

COMODO
Creating Trust Online®



Comodo Antispam Gateway

Software Version 2.12

Administrator Guide

Guide Version 2.12.060320

Comodo Security Solutions
1255 Broad Street
Clifton, NJ, 07013

Table of Contents

1 Introduction to Comodo Antispam Gateway.....	4
1.1 Release Notes.....	5
1.2 Purchase License.....	8
1.3 License Information.....	14
2 Get Started.....	17
2.1 Incoming Filtering Configuration.....	17
2.1.1 Configure Your Mail Server.....	17
2.1.2 Configure MX Record.....	18
2.1.2.1 Update MX Records in Windows 2003/2008 Server.....	19
2.1.2.2 Update MX Records on a host using BIND (and the 'named' daemon).....	19
2.1.2.3 Update MX Records for Comodo DNS.....	20
2.1.2.4 Update MX Records for GoDaddy.....	23
2.1.2.5 Update MX Records for Enom.....	24
2.1.2.6 Update MX Records for Network Solutions.....	25
2.1.2.7 Update MX Records for Yahoo! Small Business.....	26
2.1.2.8 Update MX Records for 1and1.....	27
2.1.2.9 Update MX Records for 4D Web Hosting.....	27
2.1.2.10 Update MX Records for DNS Park.....	28
2.1.2.11 Update MX Records for DreamHost.....	28
2.1.2.12 Update MX Records for DynDNS.....	29
2.1.2.13 Update MX Records for IX Web Hosting.....	29
2.1.2.14 Update MX Records for No-IP.....	30
2.1.2.15 Update MX Records in CPanel.....	30
2.2 Outgoing Filtering Configuration.....	33
2.2.1 Per-User Authentication.....	33
2.2.2 Outgoing Smarthost Setup.....	33
2.2.2.1 Configure QMail to use a Smarthost.....	34
2.2.2.2 Configure PostFix to use a Smarthost.....	35
2.2.2.3 Configure Sendmail to use a Smarthost.....	35
2.2.2.4 Configure Exchange 2000/2003 to use a Smarthost.....	36
2.2.2.5 Configure Exchange 2007/2010 to use a Smarthost.....	36
2.2.2.6 Configure Exchange 2013/2016 to use a Smarthost.....	37
2.2.2.7 Configure Office 365 to use a Smarthost.....	38
2.2.2.8 Configure Exim to use a Smarthost.....	47
2.2.2.8.1 Configure Exim / cPanel to use a Smarthost.....	47
2.2.2.8.2 Configure Exim / Directadmin to use a Smarthost.....	49
2.2.3 DNS Configuration.....	50
3 Login to the Admin Console.....	50
4 The Admin Console.....	51
5 The Dashboard Area.....	52
6 Domain Management.....	54
6.1 Add a Domain.....	56
6.2 Delete Domains.....	59
6.3 Edit Domains.....	59

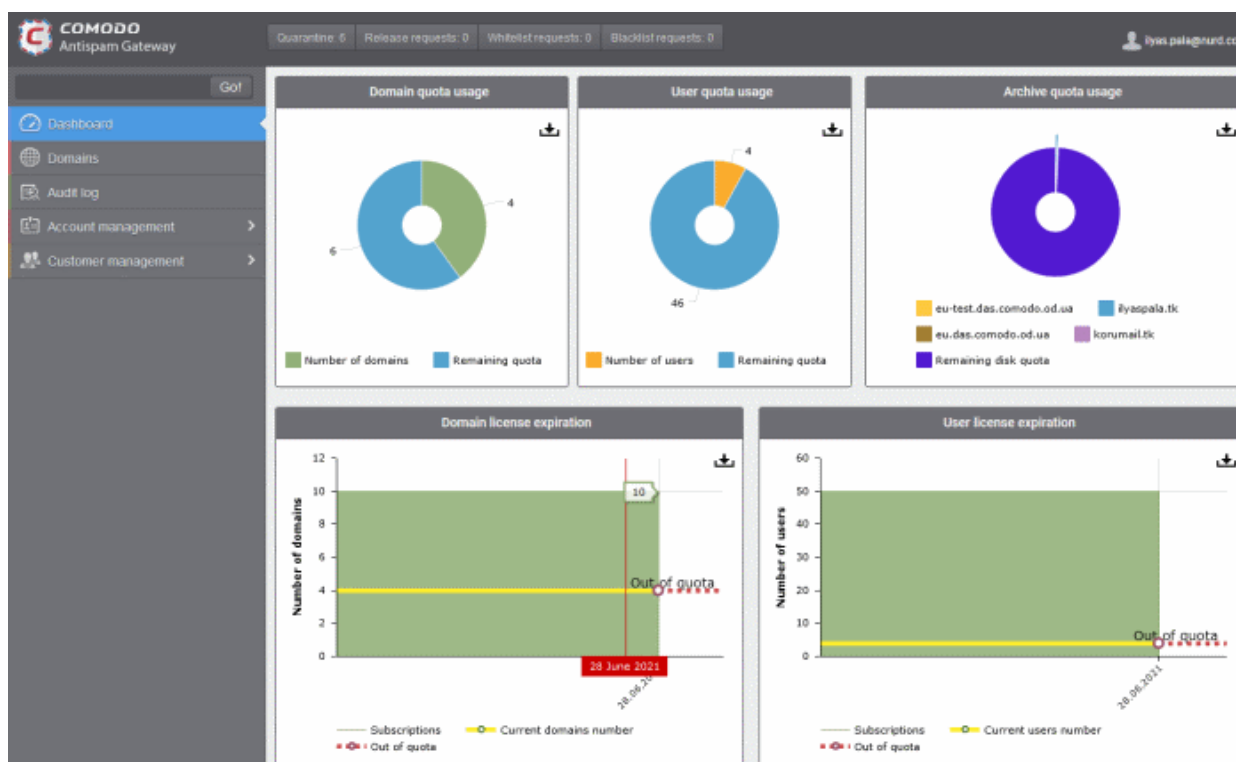
6.4	Validate Domains.....	61
6.5	Manage a Domain.....	62
6.5.1	Domain Dashboard.....	63
6.5.2	Incoming.....	66
6.5.3	Outgoing.....	130
6.5.4	Email Management.....	146
6.5.5	Domain Audit Log.....	171
6.5.6	Domain Rules.....	179
6.5.7	Account Management.....	222
6.5.7.1	User Account Management.....	223
6.5.7.2	Manage User auto-import.....	244
6.5.7.3	View User History.....	246
6.5.7.4	Import Users from LDAP.....	249
7	Audit Log.....	260
8	Administrator Account Management.....	268
8.1	Administrators.....	269
8.2	User Groups & Permissions.....	276
8.3	Admin Groups & Permissions.....	282
8.4	My Comodo Account.....	292
8.5	My Profile.....	293
8.6	Users History.....	294
9	Customer Management.....	295
9.1	End User License and Subscriber Agreements.....	295
9.2	View License Information.....	296
9.3	Manage Report Subscriptions.....	297
9.4	Notification Email Settings.....	300
10	CASG Reports - An Overview.....	300
10.1	Quarantine Report.....	301
10.2	Domain Statistics Report.....	302
10.3	Auto-Imported Users Report.....	303
10.4	Quarantine Release Report.....	304
10.5	Reported Spam Report.....	305
	Appendix 1 - CASG Error Codes.....	307
	Appendix 2 - CASG Comparison Table.....	308
	Appendix 3 - Troubleshooting LDAP.....	309
	Appendix 4 - Useful Links.....	309
	About Comodo Security Solutions.....	311

1 Introduction to Comodo Antispam Gateway

Comodo Antispam Gateway (CASG) is an enterprise email filtering solution that blocks spam, email-borne viruses and other unwanted mail from reaching user in boxes. CASG can be quickly configured for any email system and can be up and running in no time.

Features and benefits include:

- Antispam protection for incoming mails
- Antispam protection for outgoing mails
- Enhances productivity of employees and servers
- Intuitive web interface facilitates easy use and configuration
- Easy management of domains email restrictions
- Whitelist / blacklist recipients and senders
- Archiving incoming mails



Guide Structure

This guide is intended to take you through the configuration and use of **Comodo Antispam Gateway** and is broken down into the following main sections. The guide can be navigated using the bookmark links on the left.

- **Release Notes** - A list of new features that have been appeared in the CASG.
- **Purchase License** - How to purchase CASG licenses.
- **License Information** - Describes how to keep track of subscription status and various license related alerts.

- **Get Started** - Describes how to configure your mail server with the CASG service
 - **Incoming Filtering Configuration**
 - **Outgoing Filtering Configuration**
- **Login to the Admin Console** - How to login into the CASG interface.
- **The Admin Console** - Provides a snapshot of main functional areas of CASG.
- **The Dashboard Area** - Describes briefly about Domain management, Account management, Customer management and Statistics area.
- **Domain Management** - Detailed explanation on how to add domains, edit domain and manage domains. This section also deals with adding users to whitelist and blacklist and view log reports.
- **Audit Log** - Detailed explanation on how to view and export log reports for all the domains in the account.
- **Administrator Account Management** - Detailed explanation on how to add new administrators and change login passwords, subscription to periodical reports and configure language for messages from CASG.
- **Customer Management** - Provides information on accounts.
- **CASG Reports - An Overview** - An Overview of the Domain and Quarantine summary reports periodically generated and sent to the administrators and users by CASG.
- **Appendix 1** - CASG Error Codes
- **Appendix 2** - CASG Comparison Table
- **Appendix 3** - Troubleshooting LDAP
- **Appendix 4** - Useful Links

1.1 Release Notes

Version History	
Version Number	List of Changes
Version 2.12	<ul style="list-style-type: none"> • Various Bug Fixes
Version 2.11	<ul style="list-style-type: none"> • Added Domain control validation feature. Admins have to prove domain ownership.
Version 2.10	<ul style="list-style-type: none"> • System log search optimization • Added filters on Blacklist / Whitelist / Rules pages
Version 2.9	<ul style="list-style-type: none"> • Added new blacklisting option by Comodo Real-time Blackhole List (RBL).
Version 2.8	<ul style="list-style-type: none"> • Added 'Domain Rules' feature to define rules for whitelisting, blacklisting and forwarding mails and filtering mails based on TLD names of email domains • Added ability for users to view quarantined mails received at their Alias email addresses
Version 2.6	<ul style="list-style-type: none"> • Added ability to assign the language for outgoing and received messages • Added Spam trap email for administrators • Added Sites filtering option for administrators • Added 'Non human' and 'Public email' that allow to more accurately filter spam for this type of email address.
Version 2.4	<ul style="list-style-type: none"> • Added ability to create Domain Rules rules for adding senders to whitelist/blacklist • Added ability for admins and users to add senders to whitelist/blacklist from the Archive interface

	<ul style="list-style-type: none"> • Added 'Quarantine release' and 'Report spam' reports for administrators • Geolocation restriction feature added that allows to create access control policies • Added ability to forward mails from one user to another user in the same domain
Version 2.2	<ul style="list-style-type: none"> • Added 'User auto-import report' for administrators. The report contains information about all auto-imported users under each domain. • Added notification for user-auto-import events • Added ability to specify blacklist/whitelist senders by TLD • Added ability to import sender whitelists/blacklists per user from CSV file. • End users can reply to emails from mail archive • End users will be notified when emails are quarantined that were addressed to them. They can open the quarantined email by clicking the link in the notification email.
Version 2.1	<ul style="list-style-type: none"> • Added more audit events • Added Users auto import • Added Relay restrictions
Version 2.0	<ul style="list-style-type: none"> • New user interface • Added Domain Audit Log feature, which enable administrators to view the events for selected domains in customer's account • Customers can purchase storage space for archiving incoming mails • Added more audit events • Added ability to whitelist / blacklist senders for each user • Various bug fixes
Version 1.12	<ul style="list-style-type: none"> • Added Audit Log feature, which enable administrators to view the events for all the domains in customer's account • Various bug fixes
Version 1.11	<ul style="list-style-type: none"> • Added ability to assign group permissions for administrators • Added ability to login to CASG service via CAM credentials • Administrators can unlock users immediately who were locked out after three unsuccessful attempts to login • Added ability to customize notification emails • Added ability to configure number of users for each domain belonging to an account • Various bug fixes
Version 1.10	<ul style="list-style-type: none"> • Added ability to import users from Active Directory server of Domain, through LDAP • Added ability to administrators to receive quarantine request emails through alternative email address(es) • Added ability to export configured Recipient Whitelist, Sender Whitelist, Recipient Blacklist and Sender Blacklist to CSV files
Version 1.9	<ul style="list-style-type: none"> • Added ability to assign group permissions to multiple users and filtered users • Added a user ability to search for logs of all domain • Added 'Reset to default' button for Incoming Spam Detection settings • Added 'Include results from the last minutes' parameter to the Incoming & Outgoing Log search pages

	<ul style="list-style-type: none"> Added user login audits, including name of user, IP, logged time and session duration
Version 1.8	<ul style="list-style-type: none"> Added option for administrators to configure idle session timeout period Various bug fixes
Version 1.7	<ul style="list-style-type: none"> Added option to purchase multiple licenses for single domain or multiple domains Added new feature - Groups & Permissions. Allows administrators to create groups and configure permission levels for each group. Ability for administrators to add users to groups with preset policies. Users in Power group can release quarantined emails without administrator's approval Added ability for administrators to blacklist senders from Quarantine interface New option for administrators to import users to whitelist / blacklist from csv format files Added ability for administrators to import aliases from csv format files Added new options for report generation - Ability for administrators to receive global reports for all domains and domain level report for selected domain Login As button removed disabling an administrator to login as another administrator Email size restriction - Administrators to contact Comodo if more than 250 MB email size is required Various bug fixes
Version 1.6	<ul style="list-style-type: none"> Added Released Emails, Blacklisted Emails and Whitelisted Emails features in Email Management Added ability for administrators to release or reject users' request to release quarantined emails Added ability for administrators to accept or reject users' request to add senders to whitelist or blacklist Email notifications to administrators and users for requests such as to release quarantined mails, add senders to whitelist or blacklist Added ability for administrators to prioritize domain routes using drag and drop feature New option for administrators to set number of quarantined mails to be displayed per page New option to stop empty reports from being sent to recipients Right-click options to open links in new tab or new window Various bug fixes
Version 1.5	<ul style="list-style-type: none"> Added outgoing (SMTP) user management support Added email aliases support Added the ability for administrators to clear outgoing domain callout cache Added the ability for administrators to search for a specific outgoing email message
Version 1.4	<ul style="list-style-type: none"> Added periodical Domain and Quarantine summary reports feature Added ability for administrators to set language for messages displayed/sent by CASG according to their location Added automatic locking feature - the CASG account will be locked if the administrator/user login attempts fail for set number of times due to incorrect entry of username/password

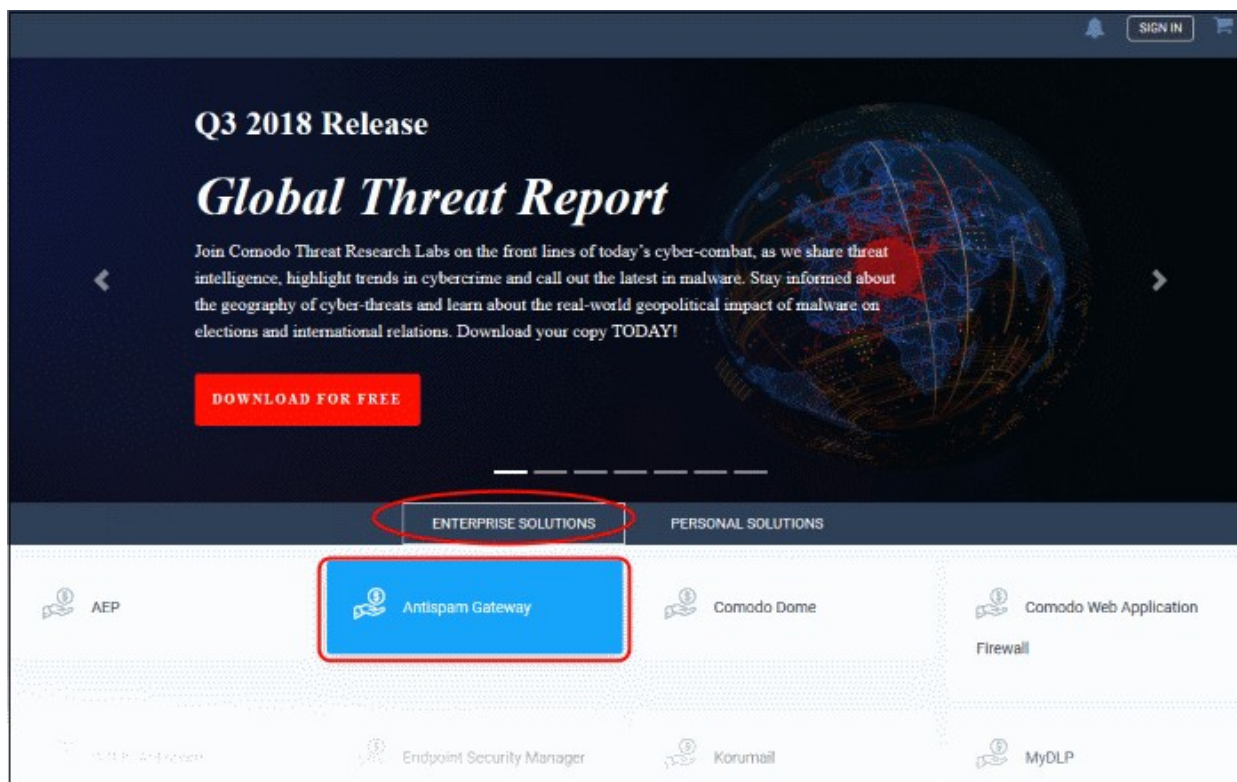
	<ul style="list-style-type: none">• Added ability for administrators to view quarantined email message content through a new CASG window
Version 1.3	<ul style="list-style-type: none">• User interface improvements• Embedded links to on-line help• Ability to configure the number of days for which logs are available• New options for domain settings• Various bug fixes
Version 1.2	<ul style="list-style-type: none">• Added licensing options• Fixed various bugs
Version 1.1	<ul style="list-style-type: none">• Added ability for administrators to view email message content through the CASG interface• Added ability to report spam in multiple formats to Comodo for potential global blacklisting• Added ability to quickly switch the domain that is currently being managed• Added ability to reset 'Blocked Extensions' list to default values
Version 1.0	<ul style="list-style-type: none">• Added Mail Quarantine feature• Added Whitelist / Blacklist pages• Added Domain management feature• Added Customer management• Added Account management

1.2 Purchase License

- In order to use CASG, you must first purchase a license for the service.
- You have the option to purchase multiple licenses for single or multiple domains.

Purchase a new license

- Login to your Comodo account at <https://cam.comodo.com/>
- Select the 'Enterprise Solutions' tab
- Click the 'Antispam Gateway' tile



- Select the product you want to purchase

A screenshot of the 'Sign Up to Antispam Gateway' form. The form includes a 'Currency' dropdown set to 'USD'. Below this are tabs for 'Base', 'Domains', 'Users', and 'Archive Space'. The 'Product' dropdown is set to 'Comodo Antispam Gateway (50 Users, 2 Domains, 0 Archive Space)'. The 'Region' dropdown is set to 'EU'. There are three tabs for 'Term of product': 'FIXED', 'MONTHS', and 'YEARS'. Under 'MONTHS', there are buttons for '1', '3', and '6', with '1' selected. Under 'YEARS', there are buttons for '1', '2', '3', '4', and '5'. The 'PRODUCT TITLE' is 'Comodo Antispam Gateway (50 Users, 2 Domains, 0 Archive Space)'. The 'Regular Price' is '\$25.00'. The 'Total Amount' is '\$25.00'. There is a checkbox labeled 'I have read and accept Test' which is checked. At the bottom, there are two buttons: 'Add To Basket' and 'Direct Signup'.

- **Product** - Select 'Base' then choose a license from the drop-down
 - You can also buy licenses for additional domains, users and / or storage space. Click the respective tab and select the required license.
 - After selecting your licenses, agree to terms and conditions then click 'Add to Basket'.
- **Region** - Select the region closest to you. We will set up your instance in this zone to improve performance.
- **Term of Product** - The longer the license term, the more money you save. For example, a 1 domain/5 user/1 month license costs \$7 per month. However, a 1 domain/5 user/1 year license costs only \$36, a saving of \$48 per year.
- Agree to the terms and conditions
- Click 'Direct Signup' if you choose a single product, or click the shopping cart at top-right
- Click 'Next'

The screenshot shows a checkout page with a progress bar at the top. The progress bar has three steps: 'Review Products' (active, indicated by a blue dot), 'User Details', and 'Payment Details'. Below the progress bar, the text reads 'You are purchasing following products:'. A table lists the purchased products:

Product Title	Period	Description	Price
Comodo Antispam Gateway (50 Users, 2 Domains, 0 Archive Space)	per month		\$25.00

Below the table, the total amount is displayed as **Total Amount: \$25.00**. There is a link 'Clear my shopping cart' and a 'Next' button.

- Complete all fields on the enrollment form:

Review Products User Details Payment Details

New user Existing user

Details

Email

Password

Confirm Password

First Name

Last Name

Contact Information

Country

State

City

Street Address

Postal Code

Previous Next

- **New user** - If you don't have a Comodo account, enter your details to create a new account
- **Existing user** - If you already have a Comodo account, enter your username and password
- Click 'Next'
- Review your details then click 'Next' again:

Review Products User Details Payment Details 0

Billing Address:

Street address:

Street address (2):

City:

Postal Code:

Country

State

Company Name:

- Finally, review your order then enter your payment details:

Review Products User Details Payment Details

Your purchase:
(you still can change it on the first step)

Product Title	Period	Description	Price
Comodo Antispam Gateway (50 Users, 2 Domains, 0 Archive Space)	per month		\$25.00





* After 1 months the product will be renewed at the full price of \$25.00 per month

Total Amount: **\$25.00**

Auto-renew this orders. You can disable this option later at any time.
 Yes! Please keep me informed about Comodo products, upgrades, special offers and pricing via email. Your information is safe with us!

Payment information

CREDIT CARD DETAILS



USE EXISTING

Name on card

Card number

Expiry Date **Security code**

🔒 Signup

Previous

- **Auto renew this order** – Deposited funds are withdrawn from your account to renew the order at the end of the subscription period. If you do not have funds in your account then your card is charged.
- **News about Comodo products** - Select to subscribe for Comodo newsletters and communications.
- **Payment type:**
 - Purchase Order – Enter the details
 - Credit Card – Enter your card details
- Click 'Signup'

Congratulations, you've successfully purchased following products:

Order Number: 741840-139

Product Name:	Comodo Antispam Gateway
License Key:	[REDACTED]
Subscription ID:	23f0dd2d19
Invoice Number:	741840-179
Order Amount:	\$25.0
Order Date:	2020-01-03
Subscription expires on:	2020-02-03

[My Licenses](#)

- Your account is created and your licenses are now active. You will also receive a confirmation email with your order details.
- The confirmation email contains the Antispam Gateway URL. Please visit this URL to login.
 - You can view your license details in the main interface after activation. See **'License Information'** for more information.
 - The number of users and domains allowed by all your licenses combined is shown in the **License Management** page.

1.3 License Information

After purchasing your license, we advise you to keep track of your usage limits and the number of days remaining on your license(s) to avoid service interruptions. You have the option to upgrade or downgrade your license as per your requirements. You will begin to receive license renewal reminders via email before the expiration of license(s).

View license information

- Log in to Comodo Antispam Gateway
- Click 'Customer management' > 'License Management' on the left
- The image below shows a customer who has purchased multiple licenses:

Quarantine: 0 Release requests: 0 Whitelist requests: 0 Blacklist requests: 0 My Account

Dashboard / License Management

License Management

Name : ak_customer1 ak_customer1
 CAM login : ak_customer1
 CAM email : alexander.kravchenko@comodo.od.us

Totals

Number of users : 2
 Max. number of users 55
 Number of domains 4
 Max. number of domains 7
 Disk quota (GB) 0.004
 Disk space 46.32 KB

Subscriptions

Reminder

Max. number of users	Max. number of domains	License expiration date	Disk quota (GB)	Enabled
50	2	Apr 18, 2017	0	true
3	3	Mar 23, 2117	3	true
1	1	Apr 29, 2017	1	true
1	1	Apr 29, 2017	0	true

- **Max. number of users** - Total users on all licenses combined.
- **Max. number of domains** - Total domains licensed on all licenses combined.

Name

- The name of the account is displayed at the title bar
- **CAM Login:** Login username for Comodo Accounts Manager (CAM) at <https://accounts.comodo.com>. You can login to CAM to purchase or renew licenses.
- **CAM email:** Email address for the account as registered in CAM.

Totals

- **Number of users:** The total number of active users across all your domains.
- **Max. number of users:** Total users you can add (all licenses combined). You cannot exceed this number of users without purchasing additional licenses.
- **Number of domains:** The number of domains enrolled for account.
- **Max. number of domains:** The total number of domains you are licensed for across all licenses.
- **Disk quota:** Total storage space available to archive incoming messages.
- **Disk space:** How much storage space you are currently using to archive mails.

Subscriptions

The following details are available for each subscription:

- **Max. number of users:** Total number of users that can be added to the account on the license.
- **Max. number of domains:** Total number of domains that can be added on the license.
- **License expiration date:** The date till which the license is valid.
- **Disk quota:** Total storage space available on the license.
- **Enabled:** States whether the subscription is active or not.

The 'Reminder' button allows you to choose an email address to receive license expiry reminders, and to specify the period of time before expiry that you wish to receive them. Please note this button will be available if you have

logged in to CASG using CAM account credentials.

Administrators will start receiving license renewal reminders via email 30 days (default) before your license(s) are due to expire.

Note: The number of days before expiration of license that you start to receive license renewal reminders and the number of reminders per day that you receive depends on the settings configured in CASG.

An example of license renewal reminder is shown below:

Dear Customer,

Your Comodo Antispam Gateway account is due to expire in 5 days.

Please renew your subscription using your [account](#) page or contact support.

Please note that on 03-06-2012 your account will be suspended for 60 days and after that all your data will be eliminated.

If you have multiple licenses and if one of them has expired, then the number of domains and users allowed for that license will be deducted from the total number of allowed domains and users. No error message will be displayed if the usage is still limited within the total domains and users allowed for the remaining license(s).

An alert will be displayed at the top of the interface on the day when all the license(s) have expired. An example of the message is shown below.

Your subscription has expired, your account will be purged in 60 days, including all domains and quarantined emails, which will be irretrievable. Until that your Spam filters are disabled.

Your subscription has expired, your account will be purged in 60 days, including all domains and quarantined emails, which will be irretrievable. Until that your Spam filters are disabled.

- There is a grace period of 60 days after license expiry to allow customers time to renew.
- During this time, your emails will continue to be delivered to your domain through CASG but without any spam filtering. You also cannot add new domains or users and cannot enable quarantine.
- Otherwise, you can login in and view/use the service normally.
- After the grace period expires, all domains and quarantined mails in your account will be purged and you will not be able to log into the account.

Administrators can upgrade or downgrade his/her account using Comodo Accounts Manager (CAM) at <https://accounts.comodo.com/account/login>. You can use the login details provided at the time of purchasing the service.

Note: Any license upgrade or downgrade for your account will not be effected immediately. However, the changes will be reflected in the interface after a certain period of time depending on the settings configured in CASG.

After downgrading your existing account or after a license has expired, if the number of domains and / or users is more than permitted, an upgrade subscription message will be displayed at the top of the CASG interface. Some examples of alert messages are shown below:

- When the domain limit is exceeded:

Your domain limit exceeded by 1. Please lower number of your domains or buy new subscription.

You will not be able to add new domains until some of the current domains are removed. CASG filter will continue to function and you can add new users.

- When the user limit is exceeded:

Your user limit exceeded by 2. Please lower number of your users or buy new subscription.

You will not be able to add new users until some of the current users are removed. CASG filter will continue to function and you can add new domains.

2 Get Started

After creating your account, the next step is configuring your mail server to work with the CASG service.

There are two service servers, one in the US and other in the EU. You should use the server best suited to your location and your requirements. The CASG service URLs are:

European Union

- mxpool1.spamgateway.comodo.com
- mxpool2.spamgateway.comodo.com

United States

- mxpool1.us.spamgateway.comodo.com

The following sections explain how to configure CASG for your environment:

- **Incoming Filtering Configuration**
 - **Configuring your mail server**
 - **Configuring MX record**
- **Outgoing Filtering Configuration**
 - **Per-user authentication**
 - **Outgoing Smarthot setup**

2.1 Incoming Filtering Configuration

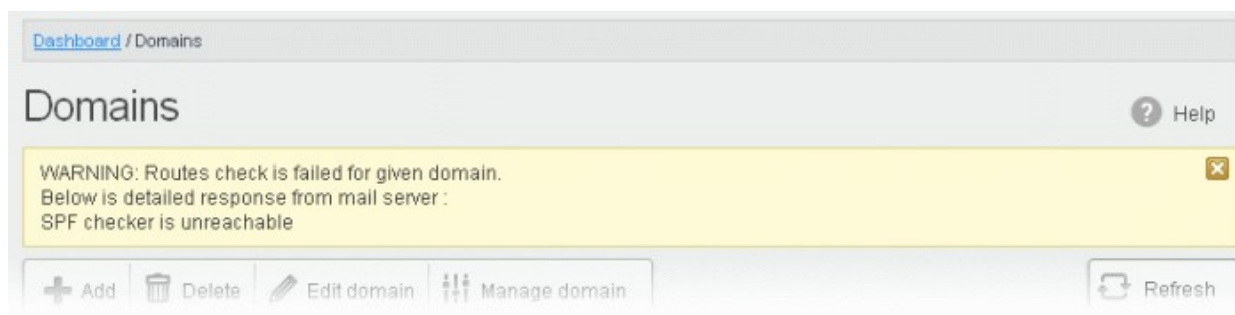
This section explains how you have to configure your mail server and point your domain MX records to CASG service.

- **Configuring your mail server**
- **Configuring MX record**

2.1.1 Configure Your Mail Server

Step 1: Disable Sender Policy Framework (SPF) checks, or add **CASG service domains** to the SPF whitelist.

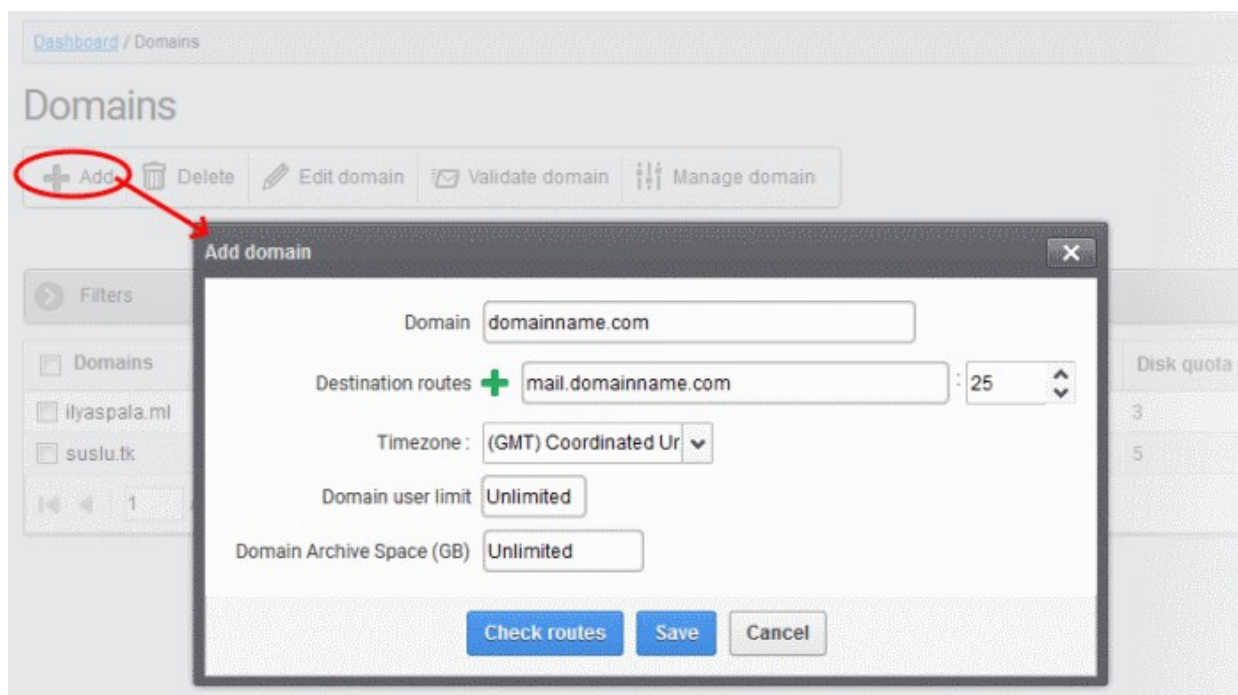
- If you don't do one of the above, you may get an error message when you add a domain:



Step 2: Add your domain to the CASG service.

To add a domain:

- **Login** to CASG system, go to **domain management** and **add domain**.



Step 3: Point mail server MX records to the **CASG service domain**. See '[Configure MX Record](#)' for more details.

2.1.2 Configure MX Record

- The next step is to update the Mail Exchange (MX) records of your domain to point to the CASG service domain.
- Please ensure that you replace your old domain MX records with **CASG service domains** according to your preferred region.

Background Note: The MX record is responsible for specifying the mail server to relay the incoming and outgoing email messages of a domain. A domain can have several MX records, each pointing to a mail server, with defined priority order. When an email is passed to/from your domain, the mail is handled by the first available mail server as per the priority. You can define new MX records or change the priority of them depending on how you want the mails to/from your domain has to be processed.

This section explains how to update your MX records so that all mails to/from your domain are passed through the CASG spam filtering service. Click the following links for detailed explanations based on the DNS software/web hosting service you use.

- [Windows Server 2003/2008](#)
- [BIND \(and the "named" daemon\)](#)
- [Comodo DNS](#)
- [GoDaddy](#)
- [Enom](#)
- [Network Solutions](#)
- [Yahoo! SmallBusiness](#)
- [1and1](#)
- [4D Web Hosting](#)
- [DNS Park](#)

- **DreamHost**
- **DynDNS**
- **IX Web Hosting**
- **No-IP**
- **Cpanel**

2.1.2.1 Update MX Records in Windows 2003/2008 Server

1. Open Control Panel by clicking Start > Control Panel and click 'Administrative Tools'.
2. Select 'DNS'.
3. Open the 'Forward Lookup Zones' folder.
4. To back up the current configuration, right-click the sub-folder for the mail domain you are configuring, select 'export' from the context sensitive menu and save the configuration in a safe location.
5. Open the zone/domain sub-folder for that mail domain.
6. Delete all the existing MX records in that zone/domain.
7. Create a new record for your primary mail server. Enter the FQDN of your preferred **CASG service domain**. CASG primary service domains are:

EU: mxpool1.spamgateway.comodo.com
US: mxpool1.us.spamgateway.comodo.com

Assign a priority of 1 as this is your primary service.

Click OK to save your record.

8. Create a new record for your secondary mail server. Enter the FQDN of your preferred **CASG service domain**. CASG secondary service domains are:

EU: mxpool2.spamgateway.comodo.com

Please note there is no secondary service domain for the US based service. Leave it blank.

Assign a priority of 2 as this is your secondary service.

Click OK to save your record.

9. Right-click the zone/domain folder and select 'Properties' from the pop-up menu.
10. Select the 'Start of Authority (SOA)' tab, click the 'Increment' button and click 'ok'.

2.1.2.2 Update MX Records on a host using BIND (and the 'named' daemon)

1. Make a backup copy of the zone file (or named.conf) that you intend to edit for MX record updates.
2. Open the Zone file for the mail domain you are configuring (or go to the part of named.conf being used for that zone)
3. Delete all the existing "MX" lines for that domain.
4. Enter a new "IN MX" record with the lowest preference value and enter the FQDN of your preferred **CASG service domain**.

CASG primary service domains are:

EU: mxpool1.spamgateway.comodo.com
US: mxpool1.us.spamgateway.comodo.com

Assign a priority of 1 as this is your primary service.

5. Enter a new "IN MX" record with the next lowest preference value and enter the FQDN of your preferred CASG service domain.

CASG secondary service domains are:

EU: mxpool2.spamgateway.comodo.com

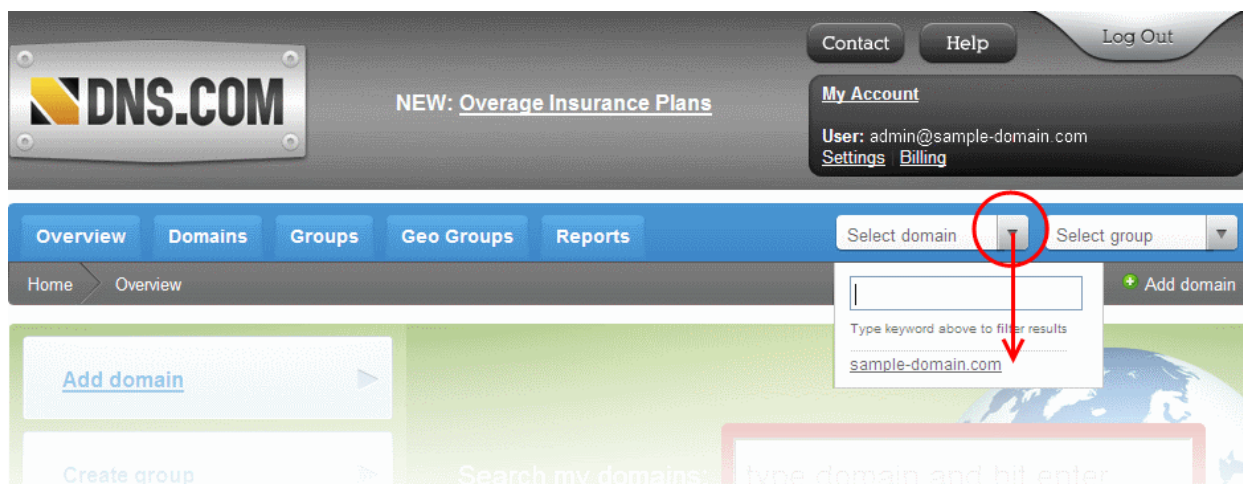
Please note there is no secondary service domain for the US based service. Leave it blank.

Assign a priority of 2 as this is your secondary service.

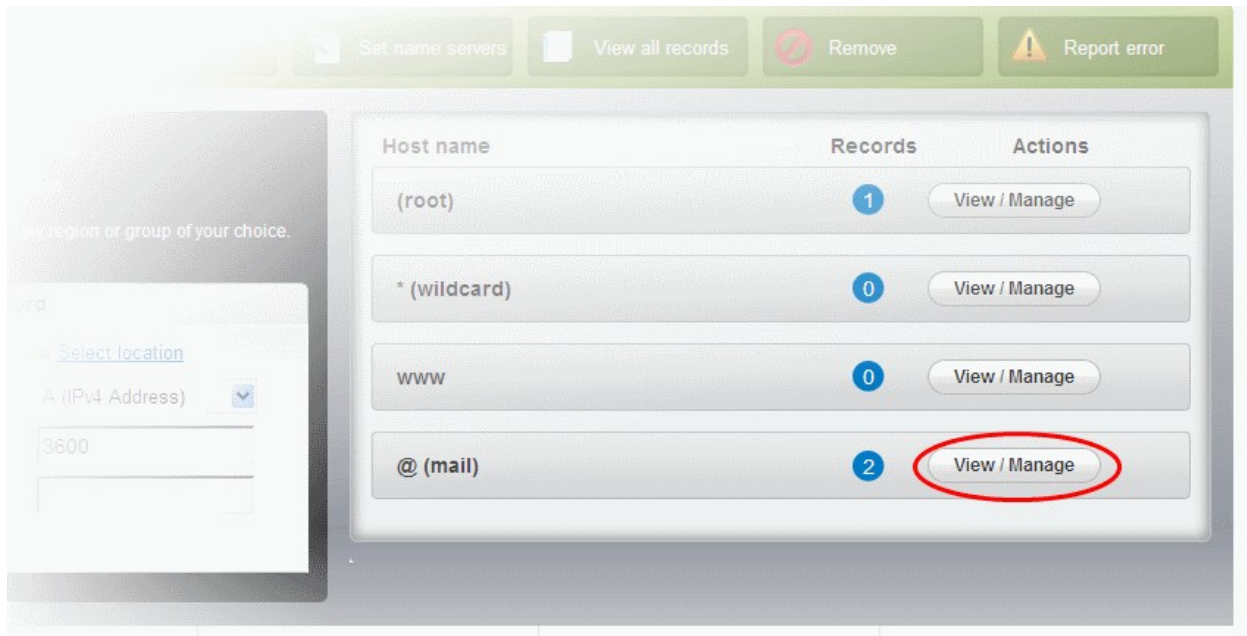
6. Find the "@ IN SOA" record and increment the serial number (on the second line of the record).
7. Save the file and check it with named-checkconf.
8. Restart the 'named' daemon.

2.1.2.3 Update MX Records for Comodo DNS

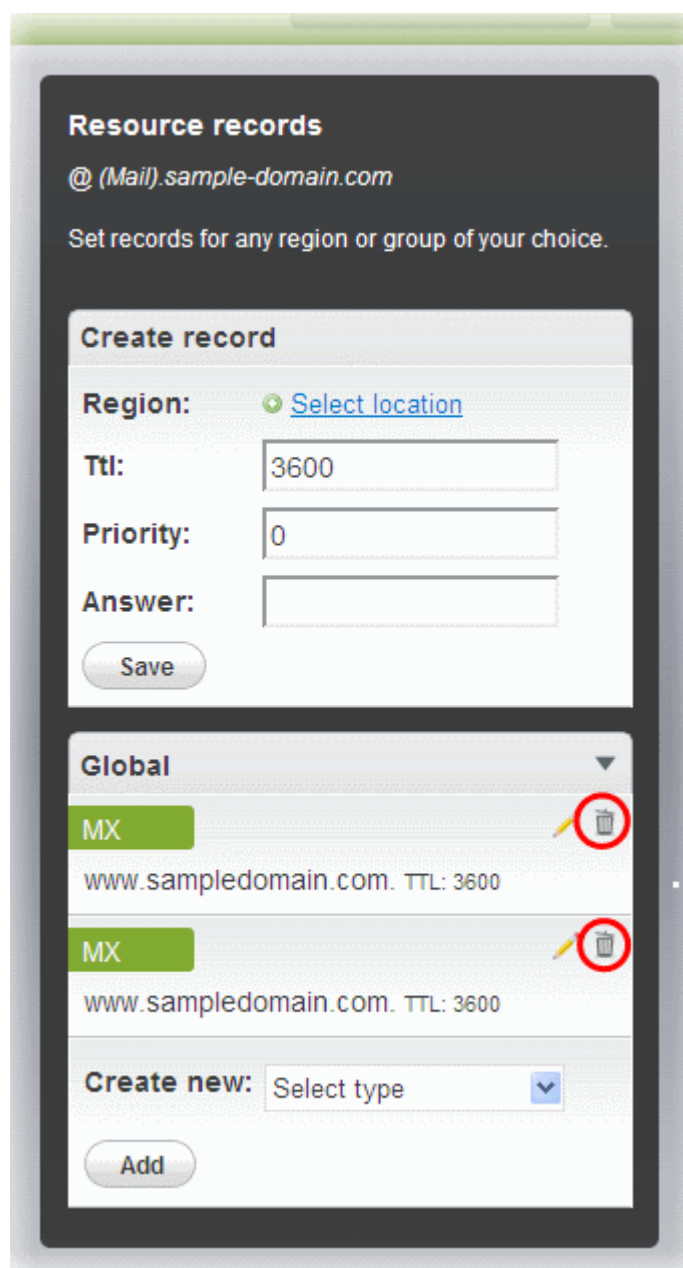
1. Log in to DNS.com administrative console at <https://dns.com/login/> by entering your login email address and password.
2. Select the domain for which you want to update the MX records, from the "Select domain" drop down menu.



3. Click the "View / Manage" button beside the row labeled "@ (mail)".



The existing MX records will be displayed at the left hand side pane.



4. Delete the existing records by clicking the trash can icons.
5. Set the primary mail server. Under 'Create Record':
 - Enter TTL as 3600 (secs)
 - Enter "1" in the 'Priority' field to set higher priority for the primary server
 - Enter the FQDN of your preferred **CASG service domain** in the 'Answer' field
CASG primary service domains are:
EU: mxpool1.spamgateway.comodo.com
US: mxpool1.us.spamgateway.comodo.comClick 'Save'
6. Again click the "View / Manage" button beside the row labeled "@ (mail)" and set the secondary mail server. Under 'Create Record':
 - Enter TTL as 3600 (secs)
 - Enter "2" in the 'Priority' field to set lower priority for the secondary server
 - Enter the FQDN of your preferred **CASG service domain** in the 'Answer' field

CASG secondary service domains are:

EU: mxpool2.spamgateway.comodo.com

Please note there is no secondary service domain for the US based service. Leave it blank.

- Click 'Save'

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

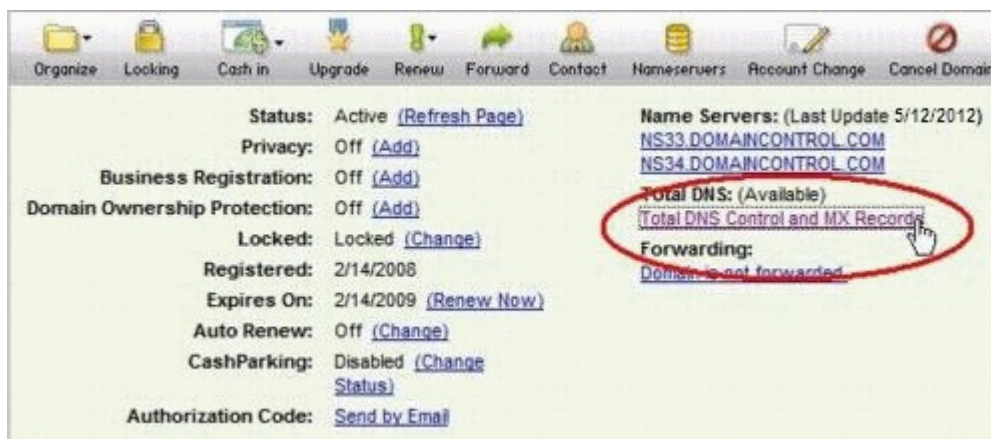
Setup should now be complete and mail filtering effected on all configured domains. If you experience problems, please open a ticket at support.comodo.com or call 1.888.COMODO (2666.6361) and have your account number ready. We have experienced technicians on hand to help troubleshoot any configuration issues.

2.1.2.4 Update MX Records for GoDaddy

1. Log in to GoDaddy administrative console at <http://www.godaddy.com>, by entering your customer number or login name, entering your password, and clicking the 'Secure Login' button.
2. Click 'My Domains' from the 'Domains' drop-down menu.



3. Select the domain for which you want to update the MX records, from the 'Domain Name' column.
4. Click 'Total DNS Control and MX Records' from the Details page.



5. Delete the existing MX records by clicking the 'X' buttons.



Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Click the 'Edit' button beside each and set the priority with higher numbers like 10, 20 and so on. You can delete these records at a later time after your changes have taken effect.

- Click 'Add New MX Record'. The interface for adding a new MX record will appear.

To set the primary server:

- Enter "1" in the 'Priority' field.
- Enter "@" in the Host Name field.
- In the 'Enter Goes To Address' field, enter the FQDN of your preferred **CASG service domain**.
CASG primary service domains are:
EU: mxpool1.spamgateway.comodo.com
US: mxpool1.us.spamgateway.comodo.com
- Select '1 week' from the TTL drop-down.
- Click 'OK'.

To set the secondary server:

- Click 'Add New MX Record' again. The interface for adding a new MX record will appear.
- Enter "2" in the 'Priority' field.
- Enter "@" in the Host Name field.
- In the 'Enter Goes To Address' field, enter the FQDN of your preferred **CASG service domain**.
CASG secondary service domains are:
EU: mxpool2.spamgateway.comodo.com
Please note there is no secondary service domain for the US based service. Leave it blank.
- Select '1 week' from the TTL drop-down.
- Click 'OK'.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.5 Update MX Records for Enom

- Log in to Enom administrative console at <https://www.enom.com/login.aspx> by entering your 'Login ID', 'Password' and clicking 'Login'.
- Click the 'Domains' tab and select 'My Domain Names'. 'Manage Domains' page will be opened
- Choose the domain for which the MX records are to be updated.
- Select the + icon under the 'Total DNS Control' list in the 'Domain Details' panel. A sub-list will appear.
- Click 'Total DNS Control And MX Records'. The 'Manage MX Records and DNS Zone File panel' will

appear.

6. Click 'Launch Total DNS Control Manager'. The 'DNS Manager' interface will appear.
7. Delete the existing MX records.

Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Click the 'Edit' button beside each and set the priority with higher numbers like 10, 20 and so on. You can delete these records at a later time after your changes have taken effect.

8. Click 'Add New MX Record'. The 'MX (Mail Exchangers) Record Wizard' will appear.

To set the primary server:

- Enter "1" in the 'Priority Value' field.
- Enter "@" in the Enter a Host Name field.
- In the 'Enter Goes To Address' field, enter the FQDN of your preferred **CASG service domain**.
CASG primary service domains are:

EU: mxpool1.spamgateway.comodo.com
US: mxpool1.us.spamgateway.comodo.com

- Select '1 week' from the TTL drop-down.
- Click 'Add'.

To set the secondary server:

- Enter "2" in the 'Priority Value' field.
- Enter "@" in the Enter a Host Name field.
- In the 'Enter Goes To Address' field, enter the FQDN of your preferred **CASG service domain**.
CASG secondary service domains are:

EU: mxpool2.spamgateway.comodo.com

Please note there is no secondary service domain for the US based service. Leave it blank.

- Select '1 week' from the TTL drop-down.
- Click 'Add'.

9. Click 'Continue'. The 'DNS Manager main page' will reappear when you've finished.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.6 Update MX Records for Network Solutions

1. Log in to Network Solutions administrative console at <https://www.networksolutions.com/manage-it/index.jsp> by entering your 'User ID', 'Password', selecting 'Manage All Services' from 'Log-in to' drop-down and clicking 'Login'.
2. Click 'Edit DNS' under 'DNS Settings'. (If this is the first time you are editing the DNS settings, then click 'Custom DNS Setting'). The 'Edit DNS' interface will appear.
3. Click 'Continue' in the 'DNS Manager-Advanced Tools'. The 'DNS Manager - Advanced Tools' interface will appear.
4. Click Add/Edit in the 'Mail Servers' panel. The 'Mail Servers' table will be displayed.
5. Delete the existing MX records.

Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Edit the 'Mail Servers' table to set the priority with higher numbers like 10, 20 and so on for the existing records. You can delete these records at a later time after your changes have taken effect.

- Update the 'Mail Servers' table with the information in the following table.

Priority	Mail Server
1	Enter the FQDN of your preferred CASG service domain . CASG primary service domains are: EU: mxpool1.spamgateway.comodo.com US: mxpool1.us.spamgateway.comodo.com
2	Enter the FQDN of your preferred CASG service domain . CASG secondary service domains are: EU: mxpool2.spamgateway.comodo.com Please note there is no secondary service domain for the US based service. Leave it blank.

- Click 'Save'.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.7 Update MX Records for Yahoo! Small Business

- Log in to Yahoo! Small Business administrative console at https://login.yahoo.com/config/login_verify2 by entering your 'Yahoo ID', 'Password' and clicking 'Sign In'.
- Click 'Domain' from the tool bar.
- Click 'Manage Advanced DNS Settings'.
- Click 'Change MX Records'.
- Delete the existing MX records.

Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Edit the 'MX Records' to set the priority with higher numbers like 10, 20 and so on for the existing records. You can delete these records at a later time after your changes have taken effect.

- Enter the MX record for primary email server with the FQDN of your preferred **CASG service domain** in the first open text box.
CASG primary service domains are:
EU: mxpool1.spamgateway.comodo.com
US: mxpool1.us.spamgateway.comodo.com
- Set the priority for the primary email server as "1"
- Enter the MX record for secondary email server with the FQDN of your preferred **CASG service domain** in the second open text box.
CASG secondary service domains are:
EU: mxpool2.spamgateway.comodo.com
Please note there is no secondary service domain for the US based service. Leave it blank.
- Set the priority for the secondary email server as "2"
- Click 'Submit'.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.8 Update MX Records for 1and1

1. Log in to 1and1 administrative console at <http://www.1and1.com/login> by entering your 'Customer ID' (Account Number or Domain name), 'Password' and clicking 'Login'.
2. Click 'Administration' tab
3. Click 'Domains'. The 'Domain Overview' page will appear.
4. Choose the domain for which the MX records are to be updated.
5. Select 'Edit DNS Settings' from the DNS menu.
6. Click 'Advanced DNS Settings' and choose 'Other mail server' from the options.
7. Delete the existing MX records.

Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Edit the 'MX Records to set the priority with higher numbers like 10, 20 and so on for the existing records. You can delete these records at a later time after your changes have taken effect.

8. Enter the MX 1/Prio and MX 2/Prio fields with the following information.

MX 1/Prio	Enter the FQDN of your preferred CASG service domain . CASG primary service domains are: EU: mxpool1.spamgateway.comodo.com US: mxpool1.us.spamgateway.comodo.com
MX 2/Prio	Enter the FQDN of your preferred CASG service domain . CASG secondary service domains are: EU: mxpool2.spamgateway.comodo.com Please note there is no secondary service domain for the US based service. Leave it blank.

9. Click 'OK'.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.9 Update MX Records for 4D Web Hosting

1. Log in to your 4D Web Hosting administrative console at <https://members.4dwebhosting.com/> by entering your 'Username', 'Password' and clicking 'Login'.
2. Click 'Configure'.
3. Click 'MX Records' from the Configuration options.
4. Replace the top two records with the following:

Primary	Enter the FQDN of your preferred CASG service domain . CASG primary service domains are: EU: mxpool1.spamgateway.comodo.com US: mxpool1.us.spamgateway.comodo.com
Secondary	Enter the FQDN of your preferred CASG service domain . CASG secondary service domains are: EU: mxpool2.spamgateway.comodo.com

Please note there is no secondary service domain for the US based service. Leave it blank.
--

5. Click 'Update MX Records'.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.10 Update MX Records for DNS Park

1. Log in to DNS Park administrative console at <https://www.dnspark.net/signin.php>.
2. Click 'DNS Hosting' from the left hand side navigation.
3. Choose the domain for which the MX records are to be updated.
4. Click 'Mail Records (MX)'.
5. Under 'MX Resource records',
 - Replace the hostname at 1st priority row with the FQDN of your preferred **CASG service domain** and click 'Update'
CASG primary service domains are:
EU: mxpool1.spamgateway.comodo.com
US: mxpool1.us.spamgateway.comodo.com
 - Replace the hostname at 2nd priority row with the FQDN of your preferred **CASG service domain** and click 'Update'
CASG secondary service domains are:
EU: mxpool2.spamgateway.comodo.com
Please note there is no secondary service domain for the US based service. Leave it blank.
6. Delete other existing MX records.

Tip: If you do not want to delete these records at this time, you can do it later, after your changes have taken effect.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.11 Update MX Records for DreamHost

1. Log in to DreamHost administrative control panel at <https://panel.dreamhost.com/> by entering your email address/Web ID and Web panel password.
2. Click 'Mail' from the left hand side navigation and select 'MX' from the options.
3. Click 'Edit' beside the domain name for which the MX records are to be updated.
4. Delete all existing MX records under 'Custom MX Records'.
5. In the first text box, enter the FQDN of your preferred **CASG service domain**
CASG primary service domains are:
EU: mxpool1.spamgateway.comodo.com
US: mxpool1.us.spamgateway.comodo.com
6. In the second text box, enter the FQDN of your preferred **CASG service domain**
CASG secondary service domains are:
EU: mxpool2.spamgateway.comodo.com
Please note there is no secondary service domain for the US based service. Leave it blank.

7. Click 'Update your custom MX records now!'

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.12 Update MX Records for DynDNS

1. Log in to DynDNS administrative console at <https://account.dyn.com/entrance/> by entering your Username and password.
2. Click 'My Services'.
3. Click 'Custom DNS' beside the domain for which the MX records are to be updated, under 'Zone Level Services'.
4. Select all the entries under 'Mail eXchanger Records' and click 'Delete MX'.
5. Click 'Add New MX'.
6. Set the primary mail server:
 - Enter the FQDN of your preferred **CASG service domain**
CASG primary service domains are:
EU: mxpool1.spamgateway.comodo.com
US: mxpool1.us.spamgateway.comodo.com
 - Select '5' for preference to set higher priority for the primary server
 - Click 'Modify MX'
 - Click 'Return to...'
7. Set the secondary mail server
 - Enter the FQDN of your preferred **CASG service domain**
CASG secondary service domains are:
EU: mxpool2.spamgateway.comodo.com
Please note there is no secondary service domain for the US based service. Leave it blank.
 - Select '10' for preference to set lower priority for the secondary server
 - Click 'Modify MX'
 - Click 'Return to...'

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.13 Update MX Records for IX Web Hosting

1. Log in to IX Web Hosting administrative control panel at <https://manage.ixwebhosting.com/index.php> by entering your login email address and password.
2. Click 'Manage' under 'Hosting Account'.
3. Choose the domain for which the MX records are to be updated.
4. Disable the existing MX records by clicking the 'On' button.
5. Click 'Edit' next to 'DNS Configuration'.
6. Delete the existing MX records.

Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Edit the 'MX Records to set the priority with higher numbers like 10, 20 and so on for the existing records. You can delete these records at a later time after your changes have taken effect.

7. Click 'Add DNS MX Record'.

- Enter the primary and secondary mail servers one by one as given in the table below. Click 'Submit' after entering each record.

Name	Data	Data (Second box)
Leave Blank	1	Enter the FQDN of your preferred CASG service domain . CASG primary service domains are: EU: mxpool1.spamgateway.comodo.com US: mxpool1.us.spamgateway.comodo.com
Leave Blank	2	Enter the FQDN of your preferred CASG service domain . CASG secondary service domains are: EU: mxpool2.spamgateway.comodo.com Please note there is no secondary service domain for the US based service. Leave it blank.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.14 Update MX Records for No-IP

- Log in to No-IP administrative console at <https://www.no-ip.com/login/> by entering your login email address and password.
- Click 'Host/Redirects' from the left hand side navigation.
- Click 'Modify' beside the domain name for which the MX records are to be updated.
- Navigate to 'Mail Options' section at the bottom of the page
- Replace the MX record entry at the first field with the FQDN of your preferred **CASG service domain**
CASG primary service domains are:
EU: mxpool1.spamgateway.comodo.com
US: mxpool1.us.spamgateway.comodo.com
- Replace the MX record entry at the second field with the FQDN of your preferred **CASG service domain**
CASG secondary service domains are:
EU: mxpool2.spamgateway.comodo.com

Please note there is no secondary service domain for the US based service. Leave it blank.
- Delete the other MX records.

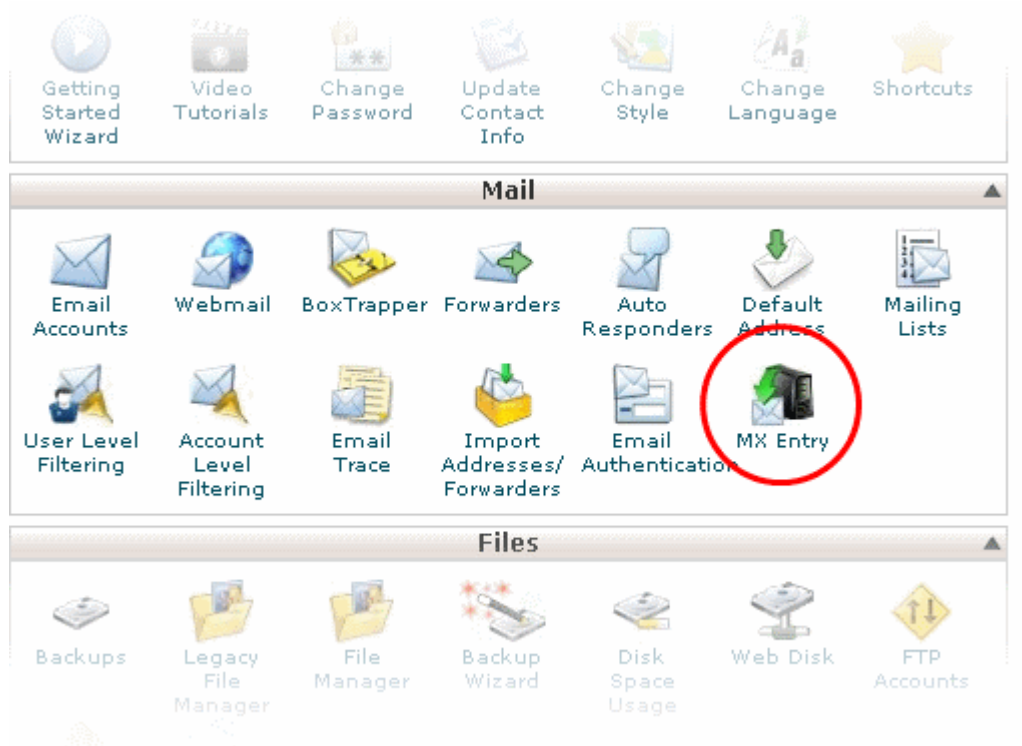
Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Edit the 'MX Records' to set the priority with higher numbers like 10, 20 and so on for the existing records. You can delete these records at a later time after your changes have taken effect.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.15 Update MX Records in CPanel

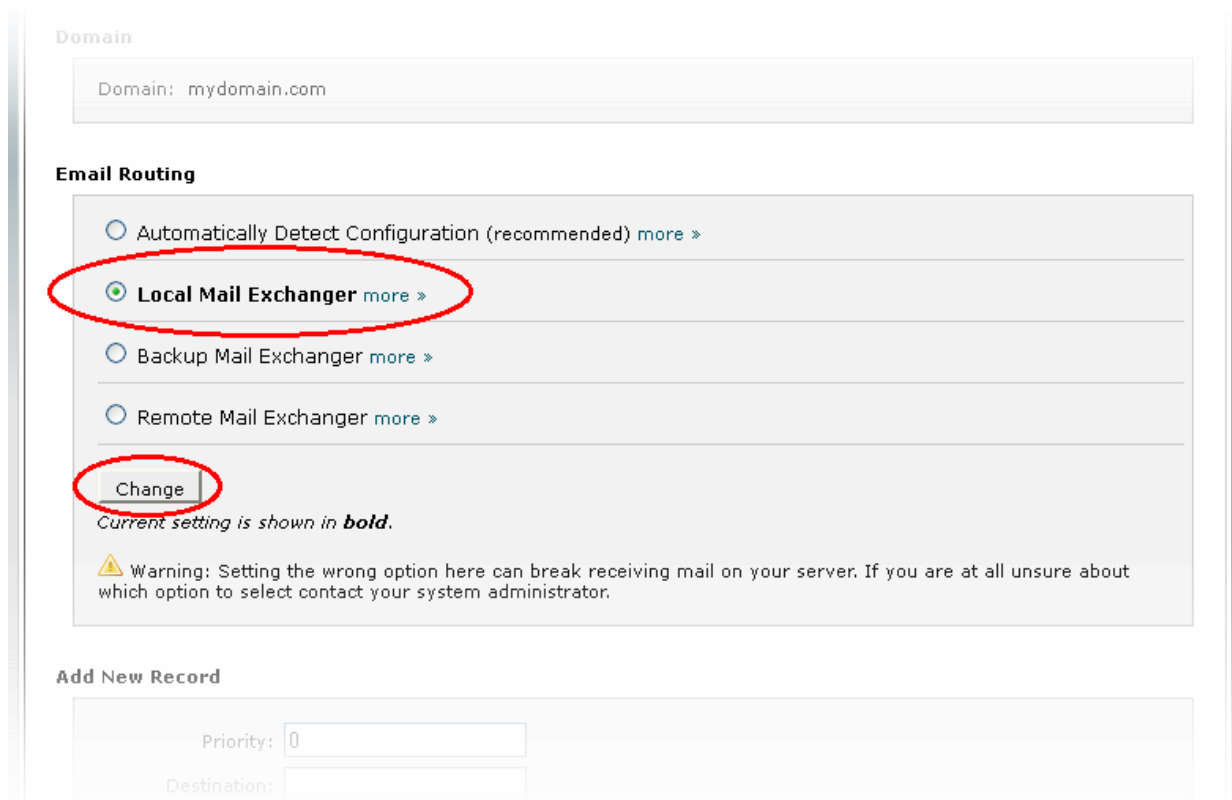
This section explains how to update MX records for your domain if you or your web hosting service provider use CPanel as webhosting control interface.

- Login to your administrative console. CPanel will be opened.
- Click 'MX Entry' icon under 'Mail'



The MX Entry Maintenance panel will be opened.

3. Select the domain for which the MX record has to be changed from the Domains area.
4. Ensure that 'Local Mail Exchanger' option is selected under 'Email Routing'. If not, select the option and click the 'Change' button.



5. Delete the entries under 'MX Records' by clicking the 'Delete' links

Add New Record

Priority:

Destination:

MX Records

PRIORITY	DESTINATION	ACTIONS
0	mydomain.com	Edit Delete

Home ▪ Trademarks ▪ Help ▪ Documentation ▪ Contact ▪ Logout

Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Click 'Edit' and set the priority with higher numbers like 10, 20 and so on. You can delete these records at a later time after your changes have taken effect.


6. Set the primary mail server under 'Add New Record'

- Enter '0' in Priority field
- Enter the FQDN of your preferred **CASG service domain** in the Destination field
CASG primary service domains are:

EU: mxpool1.spamgateway.comodo.com

US: mxpool1.us.spamgateway.comodo.com

- Click 'Add New record'. The new MX Record pointing to CASG service will be added

 Warning: Setting the wrong option here can break receiving mail on your server. If you are at all unsure about which option to select contact your system administrator.

Add New Record

Priority: ✓

Destination: ✓

MX Records

PRIORITY	DESTINATION	ACTIONS
0	mxsrv1.spamgateway.comodo.com	Edit Delete

7. Set the secondary mail server under 'Add New Record'

- Enter '1' in Priority field
- Enter the FQDN of your preferred **CASG service domain** in the Destination field
CASG secondary service domains are:
EU: mxpool2.spamgateway.comodo.com
Please note there is no secondary service domain for the US based service. Leave it blank.
- Click 'Add New record'. The new MX Record pointing to CASG service will be added

Priority:

Destination:

MX Records

PRIORITY	DESTINATION	ACTIONS
0	mxsrv1.spamgateway.comodo.com	Edit Delete
1	mxsrv2.spamgateway.comodo.com	Edit Delete
10	mydomain.com	Edit Delete

[Home](#) ▪ [Trademarks](#) ▪ [Help](#) ▪ [Documentation](#) ▪ [Contact](#) ▪ [Logout](#)

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.2 Outgoing Filtering Configuration

You can configure an outgoing filter that is independent of the incoming filter. You can set up outgoing email filter for each user, or if that is too cumbersome, you can set up the filtering server as a smarthost.

Click the following links for more details.

- [Per-user authentication](#)
- [Outgoing Smarthost setup](#)
- [DNS Configuration](#)

Note: You can use only one of the methods, [Per-user authentication](#) or [Outgoing Smarthost setup](#), for outgoing email filtering. But [DNS configuration](#) is mandatory.

2.2.1 Per-User Authentication

To set up outgoing filtering for a user, make sure that the user is a valid outgoing user. This can be done in the **Outgoing** section of the **Manage Domain** interface. You can also configure outgoing user to represent an IP address and anybody from this configured IP can send mail. To add an outgoing user, click 'Users' and 'Add' in the 'Outgoing users' interface. You can also import users from CSV file or from Incoming users. See the section **Users** to know how to configure an outgoing user.

2.2.2 Outgoing Smarthost Setup

If you use a dynamic IP or you are unable to get the proper PTR records set up then you might need to consider using a smarthost. In this case all outgoing messages would be sent to CASG mailserver and the actual recipient would be contacted by CASG mailserver itself. Please note that for smarthost option, email user authorization should be handled on your side, either by IP address or by using SMTP AUTH.

A smarthost allows an SMTP server to route email to an intermediate mail server. This can ease mail server management.

This enables you to route messages over a connection that may be more direct or less costly than other routes. The smart host is similar to the route domain option for remote domains. The difference is that, after a smart host is designated, all outgoing messages are routed to that server. With a route domain, only messages for the remote domain are routed to a specific server. If you set up a smart host, you can still designate a different route for a remote domain. The route domain setting overrides the smart host setting.

You can route all incoming / outgoing messages for remote domains through a smarthost instead of sending them

directly to the domain to reduce e-mail spam from the recipient's mail server via the default SMTP port.

There are two service servers, one in the US and other in the EU. You should provide the hostname of the ASG server that you are using as your preferred **CASG service domain**. The CASG service URLs are:

European Union

- mxpool1.spamgateway.comodo.com
- mxpool2.spamgateway.comodo.com

United States

- mxpool1.us.spamgateway.comodo.com

The following sections explain how to configure outgoing smarthost:

- **Configure QMail to use a Smarthost**
- **Configure PostFix to use a Smarthost**
- **Configure Sendmail to use a Smarthost**
- **Configure Exchange 2000/2003 to use a Smarthost**
- **Configure Exchange 2007/2010 to use a Smarthost**
- **Configure Exchange 2013/2016 to use a Smarthost**
- **Configure Office 365 to use a Smarthost**
- **Configure Exim / cPanel to use a Smarthost**
 - **Configure Exim / cPanel to use a Smarthost**
 - **Configure Exim / Directadmin to use a Smarthost**

2.2.2.1 Configure QMail to use a Smarthost

Routing all mails to a smarthost

The file where SMARTHOST relaying to smarthost settings are kept is named `smtproutes` and is usually found in `/var/qmail/control/`. We use the hostname 'mxpool1.spamgateway.comodo.com' (**EU based server**) and `mxpool1.us.spamgateway.comodo.com` (**US based server**) on port 587 as outgoing server:

European Union

```
echo: mxpool1.spamgateway.comodo.com:587" > /var/qmail/control/smtproutes
```

United States

```
echo: mxpool1.us.spamgateway.comodo.com:587" > /var/qmail/control/smtproutes
```

This command will set qmail that all your mails will be routed to `mxpool1.spamgateway.comodo.com:587` or `mxpool1.us.spamgateway.comodo.com:587` according to your preferred routing (**will remove other existing lines**).

Routing all mails for a specific domain to a smarthost :

Note: The information below relates to a very specific customer requirement and is not recommended for most deployments. A configuration like this can cause problems which will be hard to troubleshoot. Unless you are sure you need to use this setup, please explore the other available options for routing mail.

European Union

```
echo "example.com: mxpool1.spamgateway.comodo.com:587" >> /var/qmail/control/smtproutes
```

United States

```
echo "example.com: mxpool1.us.spamgateway.comodo.com:587" >> /var/qmail/control/smtproutes
```

This will route outgoing email to "example.com" via the smarthost. (rest of the lines will be kept).

2.2.2.2 Configure PostFix to use a Smarthost

You should provide the hostname of the ASG server that you are using as your preferred **CASG service domain**.

Routing all mails to a smarthost :

These instructions assume the **postfix** config files live in **/etc/postfix/main.cf**

In **/etc/postfix/main.cf** add the line:

European Union

```
relayhost = mxpool1.spamgateway.comodo.com:587
```

United States

```
relayhost = mxpool1.us.spamgateway.comodo.com:587
```

Routing all mails for a specific domain to a smarthost :

Note: The information below relates to a very specific customer requirement and is not recommended for most deployments. A configuration like this can cause problems which will be hard to troubleshoot. Unless you are sure you need to use this setup, please explore the other available options for routing mail.

Add a line to **/etc/postfix/transport**:

European Union

```
example.com smtp: mxpool1.spamgateway.comodo.com:587
```

United States

```
example.com smtp: mxpool1.us.spamgateway.comodo.com:587
```

generate a postmap file :

```
postmap hash:/etc/postfix/transport
```

To use the transport file, add or edit a line in **/etc/postfix/main.cf**:

```
transport_maps = hash:/etc/postfix/transport
```

Restart Postfix and all mail. The mail for selected domains should go through the Smarthost.

2.2.2.3 Configure Sendmail to use a Smarthost

You should provide the hostname of the ASG server that you are using as your preferred **CASG service domain**.

Routing all mails to a smarthost :

* Edit sendmail configuration sendmail.mc file

```
vi /etc/mail/sendmail.mc
```

* Append or modify macro that read as follows:

For US customers:

```
define(`RELAY_MAILER_ARGS', `TCP $h 587')dnl
```

```
define(`SMART_HOST', `mxpool1.us.spamgateway.comodo.com') dnl
```

For EU customers:

```
define(`RELAY_MAILER_ARGS', `TCP $h 587')dnl
define(`SMART_HOST', `mxpool1.spamgateway.comodo.com') dnl
```

* Regenerate a new sendmail.cf config file with m4 command:

```
m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

* Restart sendmail service:

```
/etc/init.d/sendmail restart
```

OR

```
systemctl restart sendmail
```

2.2.2.4 Configure Exchange 2000/2003 to use a Smarthost

You should provide the hostname of the ASG server that you are using as your preferred **CASG service domain**.

Routing all mails to a smarthost :

- In the Exchange System Manager, expand the Administrative Groups container.
- Expand the desired administrative group, and expand the Routing Groups container.
- Expand the routing group you need to work with, right-click the Connectors folder, and select New.
- Select SMTP Connector.
- On the General tab, enter a name to identify the connector.
- Select Forward All Mail Through This Connector To The Following Smart Hosts, and enter **mxpool1.spamgateway.comodo.com** (for EU based ASG server) or **mxpool1.us.spamgateway.comodo.com** (for US based ASG server)
- Default SMTP Server -> Properties -> Delivery Tab -> Outbound Connections -> TCP Port set to 587.

Routing all mails for a specific domain to a smarthost :

Note: The information below relates to a very specific customer requirement and is not recommended for most deployments. A configuration like this can cause problems which will be hard to troubleshoot. Unless you are sure you need to use this setup, please explore the other available options for routing mail.

Do all steps mentioned **above** and continue on with the following:

- Under Local Bridgeheads, click Add, and select the SMTP server that will become the SMTP bridgehead for its routing group.
- On the Address Space tab, click Add, select SMTP, and click OK.
- In the E-Mail Domain box, add the name of the remote location's e-mail domain (e.g., **example.com**), and click OK.
- Click OK three times to exit the SMTP connector configuration.
- Restart the Microsoft Exchange Routing Engine service and the SMTP service.

2.2.2.5 Configure Exchange 2007/2010 to use a Smarthost

You should provide the hostname of the ASG server that you are using as your preferred **CASG service domain**.

Routing all mails to a smarthost :

A Send Connector must already have been created and configured correctly on the Hub Transport server.

- Open Exchange Management Console.

- Click on the '+' next to Organization Configuration.
- Select Hub Transport and select the 'Send Connectors' tab.
- Right-click on the existing Send Connector, select 'Properties' and go to the Network tab.
- Select "Route mail through the following smart hosts:" and click 'Add'.
- Enter **mxpool1.spamgateway.comodo.com** (for EU based ASG server) or **mxpool1.us.spamgateway.comodo.com** (for US based ASG server) - you need to use port 587 for both.

If you have more than one Smarthost, repeat the previous two steps.

The changes to the Send Connector will take effect immediately without you having to reboot the server or restart any services.

In order to change the port to 587 you will have to issue the following command in the Exchange Powershell Console:

```
Set-SendConnector -identity "NAME OF CONNECTOR" -Port:587
```

Restart the transport service.

Routing all mails to a smart host with Username-Password or IP based Authentication:

A Send Connector must already have been created and configured correctly on the Hub Transport server.

- Open Exchange Management Console.
- Click on the + next to Organization Configuration.
- Select Hub Transport and select the 'Send Connectors' tab.
- Right-click on the existing Send Connector, select 'Properties' and go to the 'Network' tab.
- Select "Route mail through the following smart hosts:" and click 'Add'.
- In the FQDN section enter **mxpool1.spamgateway.comodo.com**, **mxpool2.spamgateway.comodo.com** (for EU based ASG server) or **mxpool1.us.spamgateway.comodo.com** (for US based ASG server)
- Click 'Change' under the smart-host authentication.
 - For Basic Authentication
 - Select 'Basic Authentication' and tick the 'Basic Authentication over TLS' box.
 - Add your username and password that was previously created in **CASG Outgoing Users** configuration page.
 - Click 'OK'
 - For IP based Authentication
 - Select 'None'
 - Click 'OK'
 - Then add outbound IP of your Exchange Server in **CASG Outgoing Users** configuration page

The changes to the Send Connector will take effect immediately without you having to reboot the server or restart any services.

In order to change the port to 587 you will have to issue the following command in the Exchange Powershell Console:

```
Set-SendConnector -identity "NAME OF CONNECTOR" -Port:587
```

Restart the transport service.

2.2.2.6 Configure Exchange 2013/2016 to use a Smarthost

You should provide the hostname of the DAS server that you are using as your preferred **CASG service domain**.

Routing all mails to a smarthost :

A 'send connector' must already have been created and configured correctly on the hub transport server.

- Open 'Exchange Admin Center' (EAC).

- Select 'Mail flow' on the left then click 'Send Connectors'.
- Select the existing send connector to view its properties.
- Click 'Delivery'
- Select "Route mail through the following smart hosts:" under 'Specify how to send mail with this connector' and click the '+' button to add the smart host name.
- Enter mxpool1.spamgateway.comodo.com (for EU based CASG server) or mxpool1.us.spamgateway.comodo.com (for US based CASG server) in the 'add smart host' dialog.

If you have more than one smarthost, repeat the previous three steps.

- If you need to route all mails to the smart host with Username-Password or IP based Authentication, continue with the following settings:
 - For Basic Authentication
 - Select 'Basic Authentication' under Smart host authentication
 - Tick the 'Offer basic authentication only after starting TLS' box
 - Add your username and password that was previously created in **CASG Outgoing Users** configuration page
 - Click 'Save'
 - For IP based Authentication
 - Select 'None'
 - Click 'Save'
 - Then add outbound IP of your Exchange Server in **CASG Outgoing Users** configuration page
- Under 'Address Space', click the '+' button in the 'Add Domain' window
 - Select 'SMTP' for 'Type'
 - Enter '*' in the Fully Qualified Domain Name (FQDN) field
 - Click 'Save'
- Under 'Source Server', click '+' in the 'Select a server' window.
 - Select a mailbox server that will be used to send email to the internet via the 'Client Access' server
- Click 'Finish'

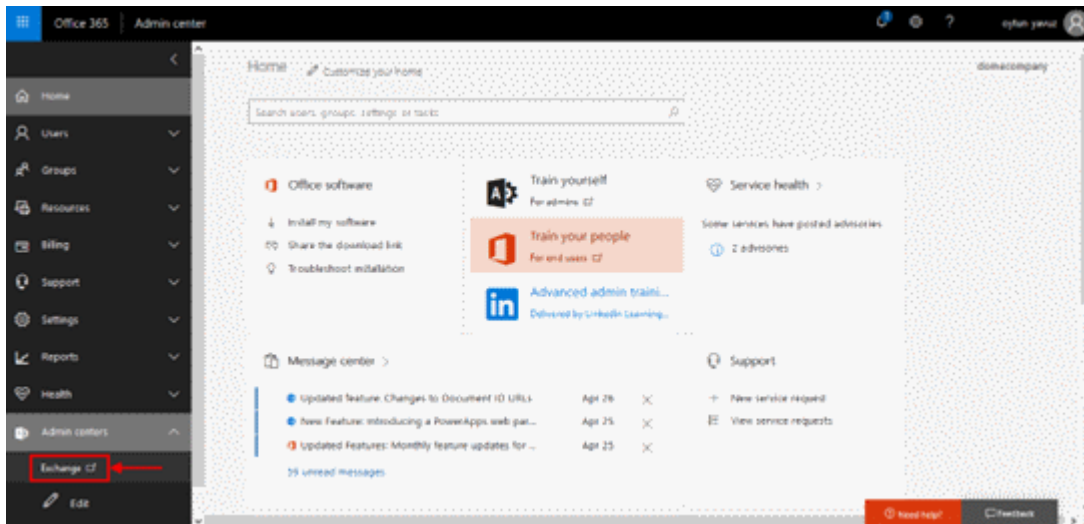
The changes you've made will take effect straight away without requiring a reboot or restarting any services.

2.2.2.7 Configure Office 365 to use a Smarthost

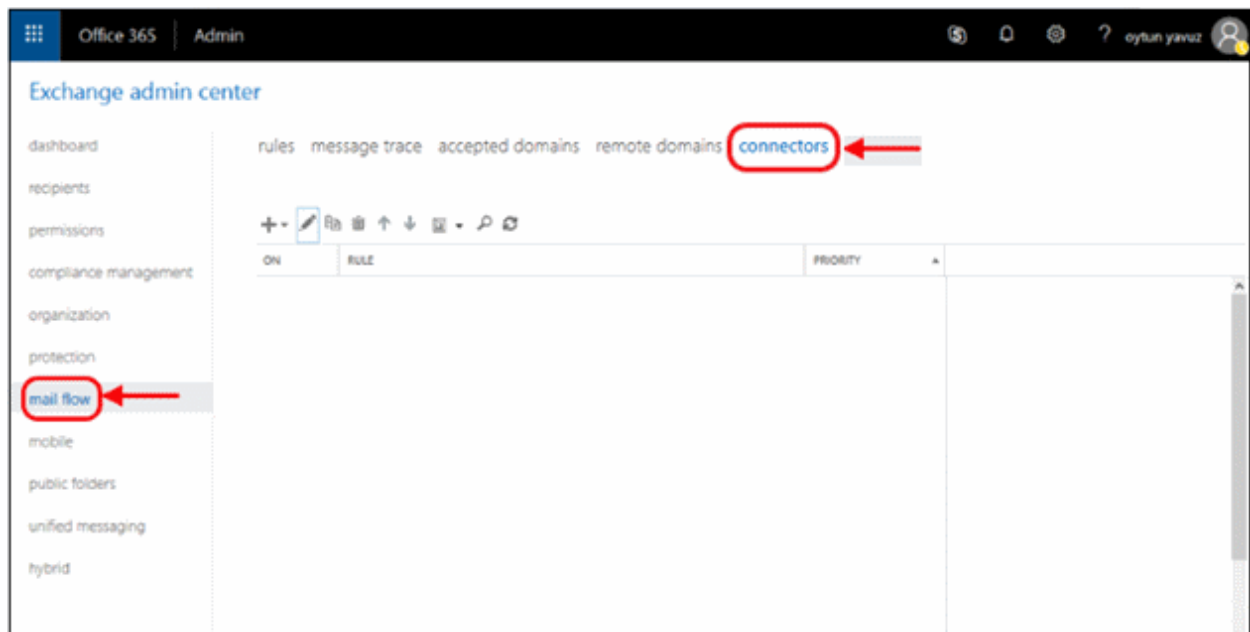
- Note – Make sure you have activated Office 365 in CASG. Go to 'Outgoing' > 'Office 365 Activation' then complete the activation procedure. [Click here](#) for more information.

Set up outbound mail in Office 365:

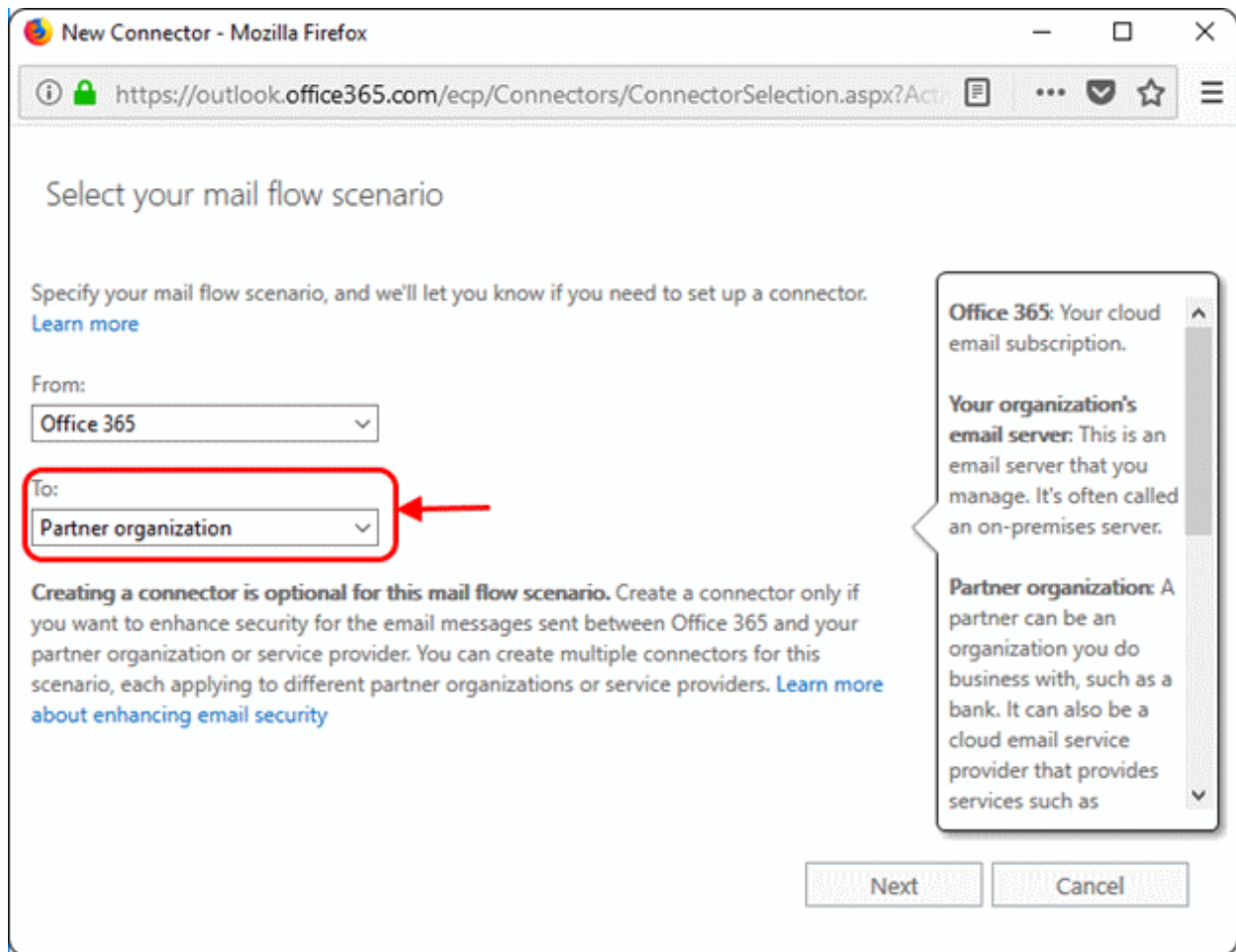
- Login to your Microsoft Office 365 administrator center account
 - Click 'Admin' from the left-menu
 - Click 'Exchange':



- Click 'mail flow' on the left
- Click 'connectors' in the top navigation:



- Add an 'Outbound Connector':
 - Select 'Office 365' in the 'From' drop-down menu
 - Select 'Partner Organization' in the 'To' drop-down menu:



- Click 'Next'
- Enter a descriptive name for the outbound connector in the 'Name' field
- Click 'Next'

New Connector - Mozilla Firefox

https://outlook.office365.com/ecp/Connectors/InboundPartnerConnector.as...

New connector

This connector enforces routing and security restrictions for email messages sent from your partner organization or service provider to Office 365.

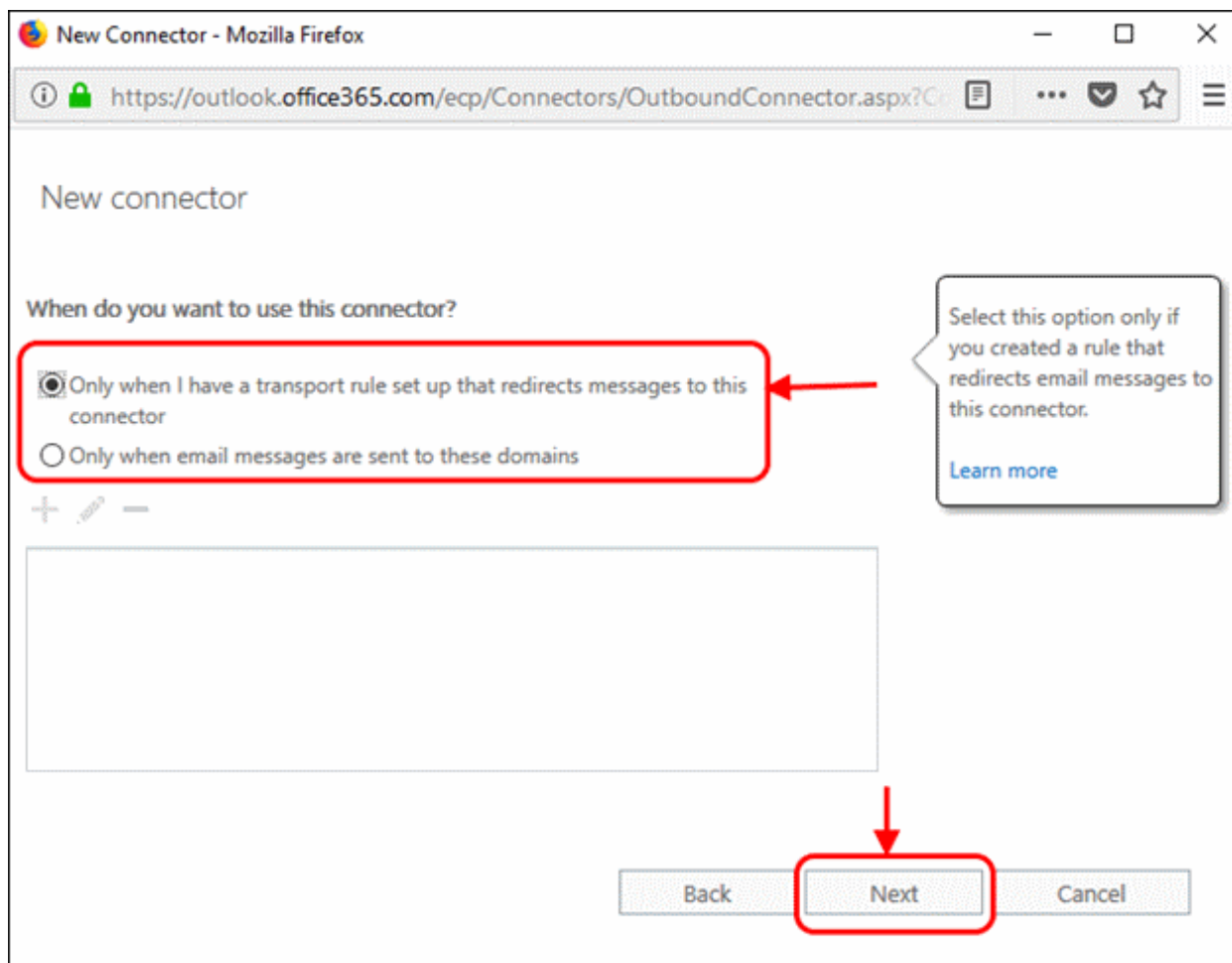
*Name:
Dome Antispam Integration

Description:

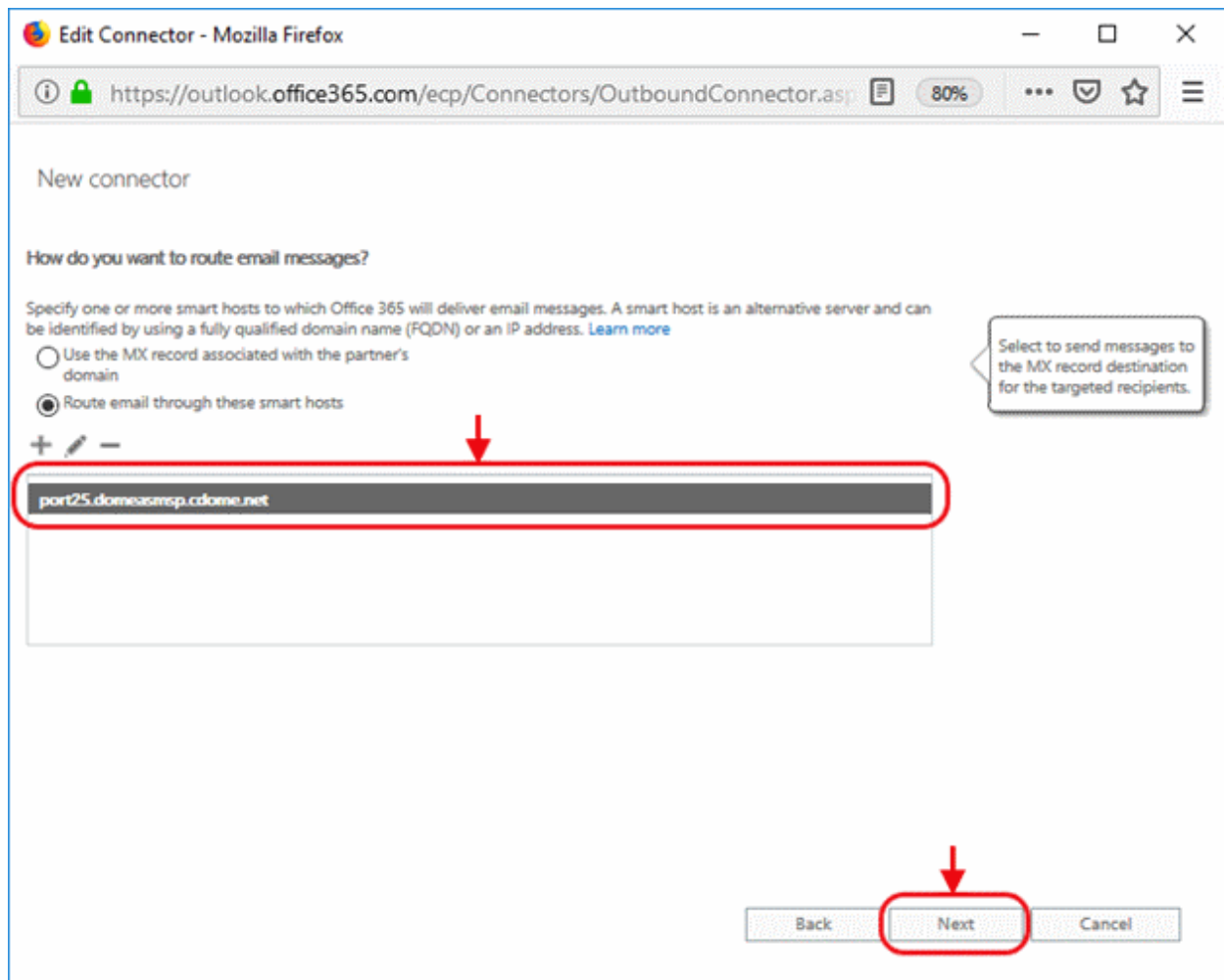
What do you want to do after connector is saved?
 Turn it on

Next Cancel

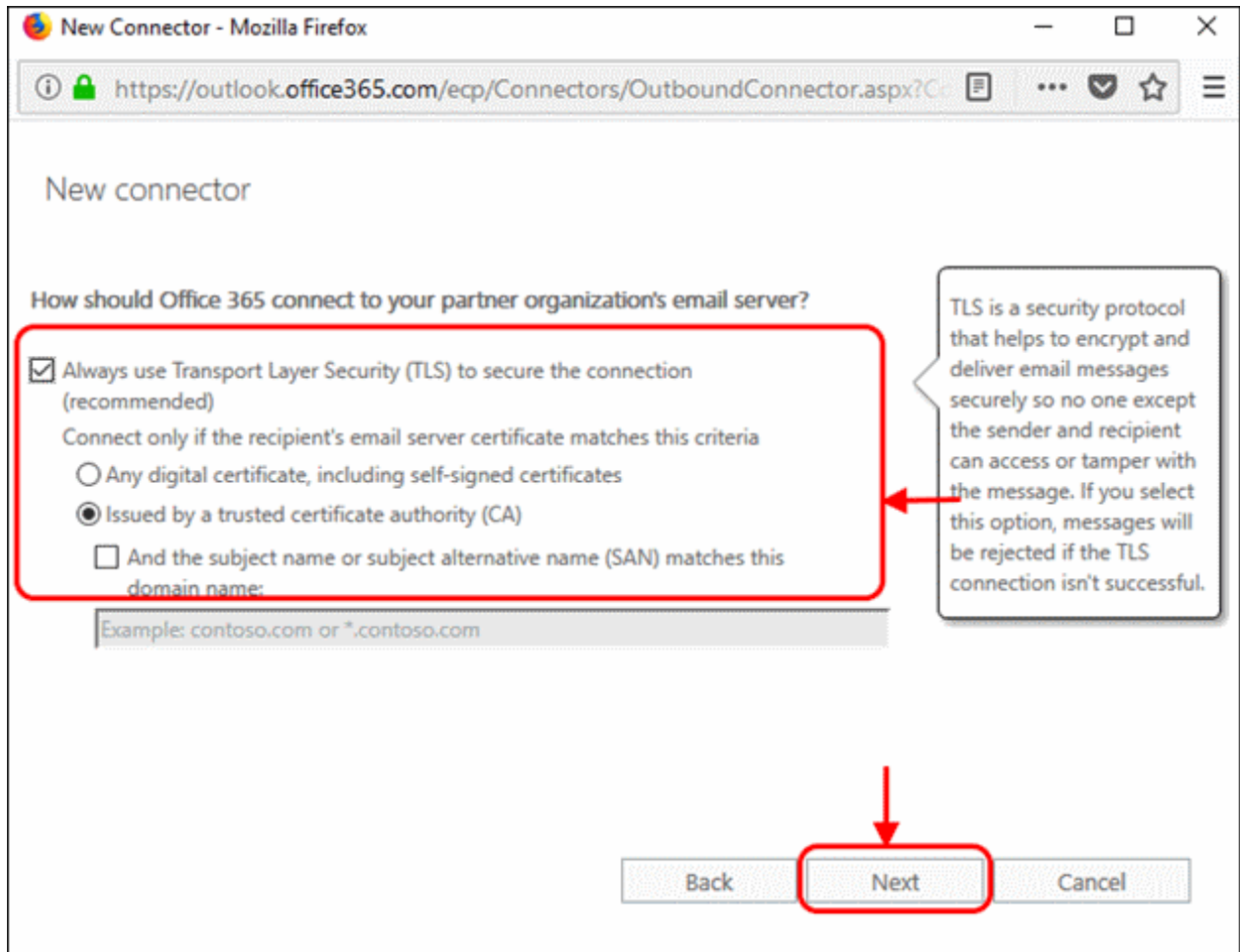
- **'When do you want to use this connector?'** - Select 'Only when I have a transport rule set up that redirects messages to this connector'
 - Click 'Next'



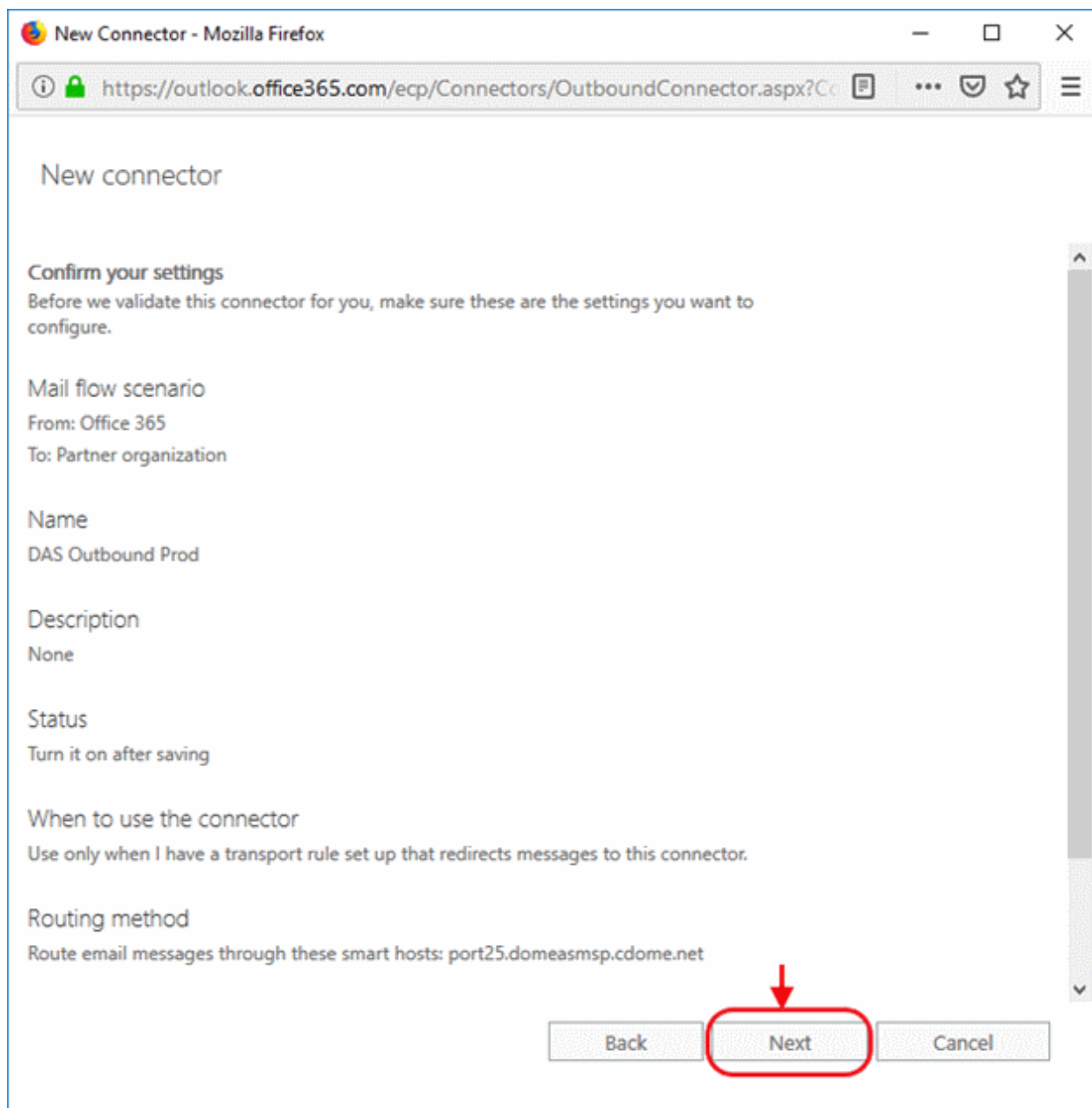
- **'How do you want to route email messages'**
 - Select 'Route email through these smart hosts'
 - Click + sign to add smart host as **port25.domeasmsp.cdome.net** in the opening page and click Save.
- Page will be updated as below.
- Click 'Next'.



- 'How should Office 365 connect to your partner organization's email server?' - Select:
 - 'Always use Transport Layer Security (TLS) to secure the connection'
AND
 - 'Issued by a trusted certificate authority'.This will make sure the connection to the mail server is securely encrypted and authentic.
- Click 'Next'



- Review your settings. Check all information in the confirmation screen is as it should be, then click 'Next':



- **'Validate this connector'** - Add an email address at which you can receive mail in the field provided, then click 'Validate'.

New connector

Validate this connector

We'll validate this connector for you to make sure it works as expected, but first you'll need to provide one or more email addresses so we can send a test message.

Specify an email address for your partner domain. You can add multiple addresses if your partner has more than one domain.

+ ✎ -

admin@ityaspala.ml

Specify the email address or addresses you want to use to validate this connector.

Back Validate Cancel

- If you receive the validation email to the specified email address, then the STATUS will change to "Succeeded". This means that Office 365 connector can connect to your smart host.
- Click 'Save' to complete connector configuration.

New connector

Validation Result

This connector works as expected. Connectivity is good, and a test email was sent to the email address you specified.

✎

TASK	STATUS
Check connectivity to "port25.domeasmsp.cdome.net"	Succeeded
Send test email	Succeeded

Back Save Cancel

2.2.2.8 Configure Exim to use a Smarthost

You should provide the hostname of the ASG server that you are using as your preferred **CASG service domain**.

Routing all mails to a smarthost :

To configure the mailserver Exim, edit your Exim configuration file (e.g. `/etc/exim/exim.conf`).

Add in the routers section (after **begin routers**):

```
spamgateway_smarthost_router:
  driver = manualroute
  transport = spamgateway_smarthost_transport
  route_list = $domain mxpool1.spamgateway.comodo.com::587 (for EU based ASG
server) or $domain mxpool1.us.spamgateway.comodo.com::587 (for US based ASG
server)
  no_more
```

Make sure the local mail route is before smarthost, if you don't want local mail to be forwarded. Add in the transports section (after **begin transports**):

```
spamgateway_smarthost_transport:
  driver = smtp
  hosts_require_tls = *
```

Routing all mails for a specific domain to a smarthost:

Note: The information below relates to a very specific customer requirement and is not recommended for most deployments. A configuration like this can cause problems which will be hard to troubleshoot. Unless you are sure you need to use this setup, please explore the other available options for routing mail.

Put the domain in place of the `$domain` value in the `route_list` (above). For multiple domains you can use:

```
route_list = domain.example.com mxpool1.spamgateway.comodo.com::587 ;
domain.example.org mxpool1.spamgateway.comodo.com::587 (for EU based ASG
server)
```

or

```
route_list = domain.example.com mxpool1.us.spamgateway.comodo.com::587 ;
domain.example.org mxpool1.us.spamgateway.comodo.com::587 (for US based ASG
server)
```

Restart Exim for the changes to take effect.

2.2.2.8.1 Configure Exim / cPanel to use a Smarthost

Routing all mails to a smarthost :

Go to the "Exim Configuration Editor" in WHM. Choose "Advanced Editor". Add in the routers section (after **begin routers**, and after the **democheck: router** block):

```
smarthost_dkim:
  driver = manualroute
  domains = !+local_domains
  require_files = "+/var/cpanel/domain_keys/private/${sender_address_domain}"
  transport = remote_smtp_smart_dkim
  route_list = $domain mxpool1.spamgateway.comodo.com::587 (for EU based ASG
server) or $domain mxpool1.us.spamgateway.comodo.com::587 (for US based ASG
server)
```

```
smarthost_regular:
  driver = manualroute
```

```
domains = !+local_domains
transport = remote_smtp_smart_regular
route_list = $domain mxpool1.spamgateway.comodo.com::587 (for EU based ASG
server) or $domain mxpool1.us.spamgateway.comodo.com::587 (for US based ASG
server)
```

Then add in the transports section (after begin transports):

```
remote_smtp_smart_dkim:
  driver = smtp
  hosts_require_tls = *
  interface = ${if exists {/etc/mailips}{${lookup{$sender_address_domain}
lsearch*/etc/mailips}{$value}{}}{}}
  helo_data = ${if exists {/etc/mailhelo}{${lookup{$sender_address_domain}
lsearch*/etc/mailhelo}{$value}{$primary_hostname}}}{$primary_hostname}}
  dkim_domain = $sender_address_domain
  dkim_selector = default
  dkim_private_key = "/var/cpanel/domain_keys/private/${dkim_domain}"
  dkim_canon = relaxed

remote_smtp_smart_regular:
  driver = smtp
  hosts_require_tls = *
  interface = ${if exists {/etc/mailips}{${lookup{$sender_address_domain}
lsearch*/etc/mailips}{$value}{}}{}}
  helo_data = ${if exists {/etc/mailhelo}{${lookup{$sender_address_domain}
lsearch*/etc/mailhelo}{$value}{$primary_hostname}}}{$primary_hostname}}
```

Save the configuration. All the outgoing mail will be relayed through the filterserver and accept original and DKIM signed emails.

Routing all mails to a smarthost with SMTP Authentication:

- Go to the "Exim Configuration Editor" in WHM.
- Choose "Advanced Editor". do not include "**begin authenticators**".
- Otherwise, simply append our 4 lines and leave out our "**begin authenticators**".

```
begin authenticators

spamgateway_login:
  driver = plaintext
  public_name = LOGIN
  client_send = : username@example.com : yourUserPassword
```

Add a Router in the Router Configuration Box.

```
send_via_spamgateway:
  driver = manualroute
  domains = ! +local_domains
  transport = spamgateway_smtp
  route_list = "* mxpool1.spamgateway.comodo.com::587 byname" (for EU based
ASG server)or "* mxpool1.us.spamgateway.comodo.com::587 byname" (for US based
server)
  host_find_failed = defer
  no_more
```

Add a Transport to the Transport Configuration Box.


```
(for EU based ASG server)
spamgateway_smtp:
driver = smtp
hosts = mxpool1.spamgateway.comodo.com
hosts_require_auth = mxpool1.spamgateway.comodo.com
hosts_require_tls = mxpool1.spamgateway.comodo.com
```

```
(for US based server)
spamgateway_smtp:
driver = smtp
hosts = mxpool1.us.spamgateway.comodo.com
hosts_require_auth = mxpool1.us.spamgateway.comodo.com
hosts_require_tls = mxpool1.us.spamgateway.comodo.com
```

Restart Exim.

Extra: Routing all mails for a specific domain to a smarthost with individual outgoing accounts:

To be able to set custom settings/limits for outgoing users, use the information above (Routing with SMTP Authentication) with a small change. Use this:

```
client_send = :
${extract{user}}{${lookup{$sender_address_domain}lsearch{/etc/exim_spamgateway
}}}} :
```

```
${extract{pass}}{${lookup{$sender_address_domain}lsearch{/etc/exim_spamgateway
}}}}
```

instead of the **client_send** in the previous example.

To create a file called **/etc/exim_spamgateway** with the following structure, use this :

```
domain1.com:    user=user@domain1.com    pass=abc
domain2.com:    user=user@domain2.com    pass=xyz
```

Extra: Limiting Outgoing for certain domains

This option can be combined with the individual accounts configuration to restrict outgoing only to specific domains. You can add the following entry (underneath domains) in the router :

```
senders = ^.*@domain1.com : ^.*@domain2.com
```

2.2.2.8.2 Configure Exim / Directadmin to use a Smarthost

- Edit your Exim configuration file (e.g. /etc/exim.conf).
- Add in the routers section (after begin routers):

```
spamgateway_smarthost_router:
driver = manualroute
domains = ! +local_domains
ignore_target_hosts = 127.0.0.0/8
condition = "${perl{check_limits}}"
transport = spamgateway_smarthost_transport
route_list = $domain mxpool1.spamgateway.comodo.com::587 (for EU based ASG
server) or $domain mxpool1.us.spamgateway.comodo.com::587 (for US based ASG
```

```
server)
no_more
```

- This replaces the existing "lookuphost:" router which should be commented.
- Add in the transports section (after begin transports):

```
spamgateway_smarthost_transport:
driver = smtp
hosts_require_tls = *
```

Restart Exim.

2.2.3 DNS Configuration

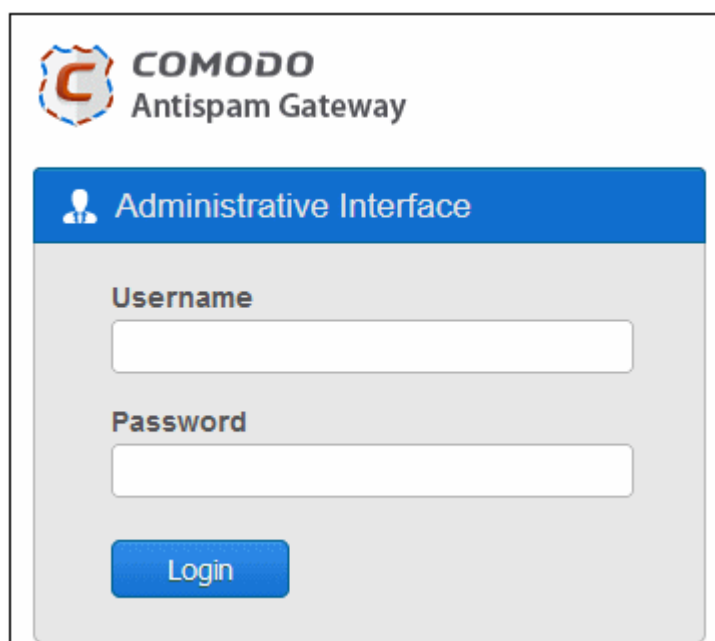
The following SPF record needs to be added to your public DNS:

```
include: _spf.antispamgateway.comodo.com
```

3 Login to the Admin Console

You can login into your CASG account using any internet browser. The login URL depends on the **CASG service domain** that you subscribed for:

- EU CASG Service domain - <https://antispamgateway2.comodo.com/admin>
- US CASG Service domain - <https://us.antispamgateway2.comodo.com/admin/>



The screenshot shows the login interface for the Comodo Antispam Gateway. At the top left is the Comodo logo, a stylized 'C' inside a gear-like shape, followed by the text 'COMODO Antispam Gateway'. Below this is a blue header bar with a white user icon and the text 'Administrative Interface'. The main content area is light gray and contains two input fields: 'Username' and 'Password'. Below the password field is a blue 'Login' button.

- Login to the interface with your CASG username and password.

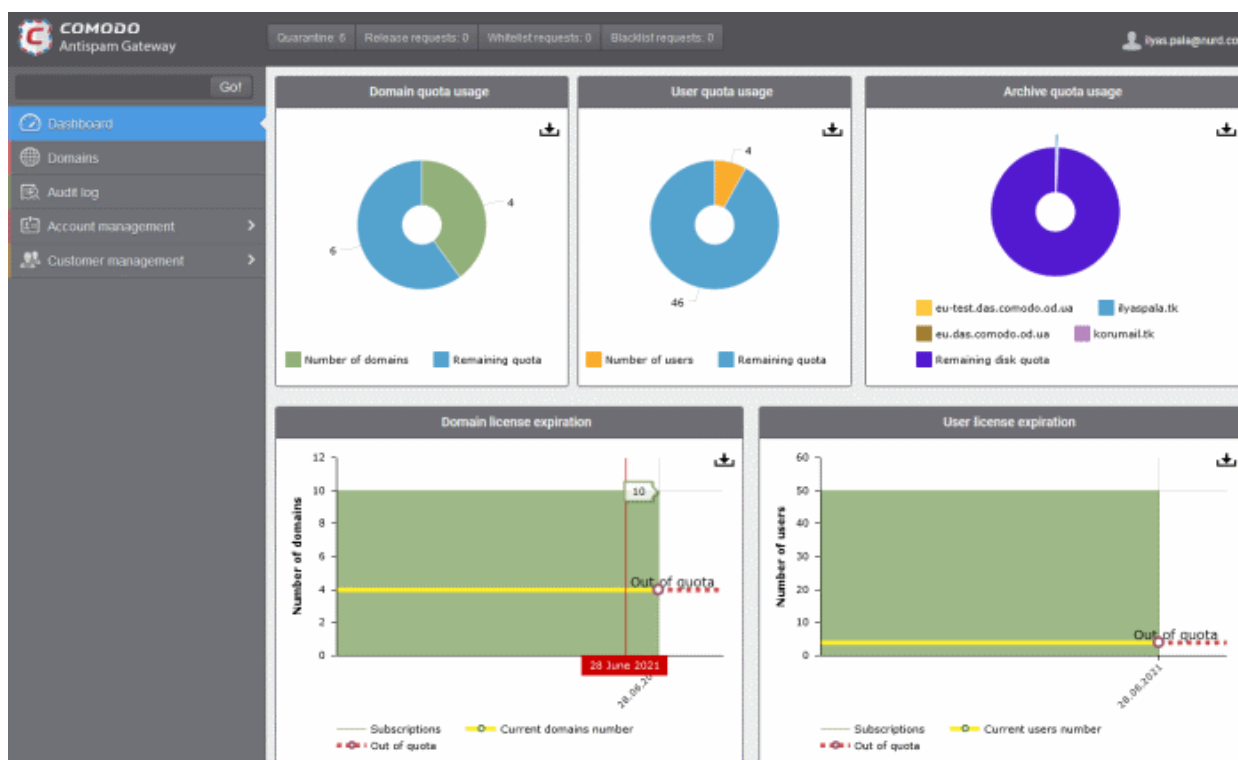
In order to ensure safety, CASG will lock the account if the login attempts fail for more than three attempts due to incorrect Username or Password. To unlock the account the administrator can contact their Comodo Account Manager.

The threshold number of unsuccessful login attempts before locking the account can also be customized by contacting the Comodo Account Manager.

Note: You can login to the interface using either the credentials created via CAM account or the administrative credentials created via the CASG interface. If you login using the CAM account credentials, an additional feature 'Login to my Comodo account' will be available in the Account management area through which you can manage your account such as subscribe for more licenses.

4 The Admin Console

The admin console is the nerve center of Comodo Antispam Gateway (CASG). It allows you to view system statistics, add domains and users, manage accounts and more.




The links on the left let you navigate to different areas of the console.

Main Functional Areas

- **Dashboard** - Charts which show current usage levels. See [The Dashboard Area](#) for more.
- **Domains** - Configure your CASG protected domains. See [Domain Management](#) for more details.
- **Audit Log** - View records of actions by users and admins. See [Audit Log](#) for more help.
- **Account Management** -
 - Add, edit or delete admins
 - Change admin password
 - Manage subscriptions to reports.
 - Create user and admin groups / Configure user and group permissions
 - View user history for your domains

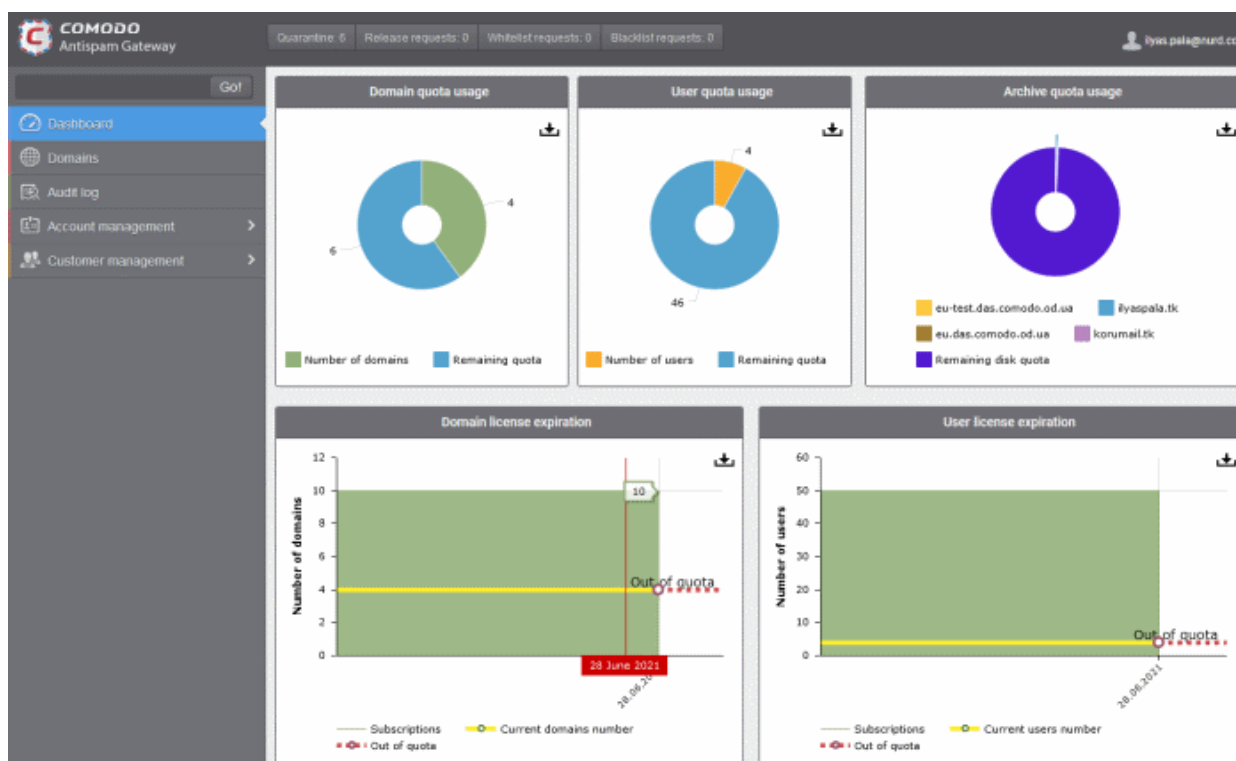
- See **Account Management** for more.
- **Customer Management** -
 - Activate or deactivate customers
 - View and manage customer details
 - Manage subscriptions to domain and quarantine reports
 - Configure mail template settings for messages sent from CASG.
 - See **Customer Management** for more.

Click the support.comodo.com link at the bottom of interface to visit the Comodo support portal - an online knowledge base and support ticketing system. This is the fastest way to get assistance with any CASG issues you my encounter.

Various areas of the application display a help button  at top-right. Click this button to open the dedicated help guide page for the area.

5 The Dashboard Area

The dashboard contains charts with data about your Antispam Gateway deployment. You can export any chart to pdf by clicking the download icon in the top-right corner of each panel.

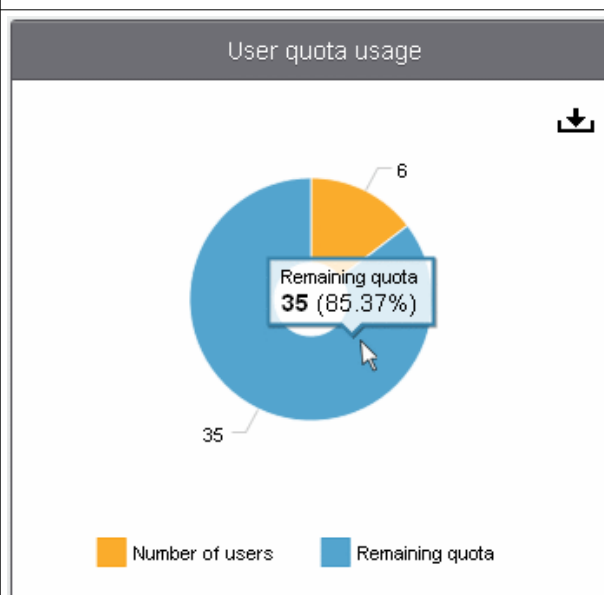
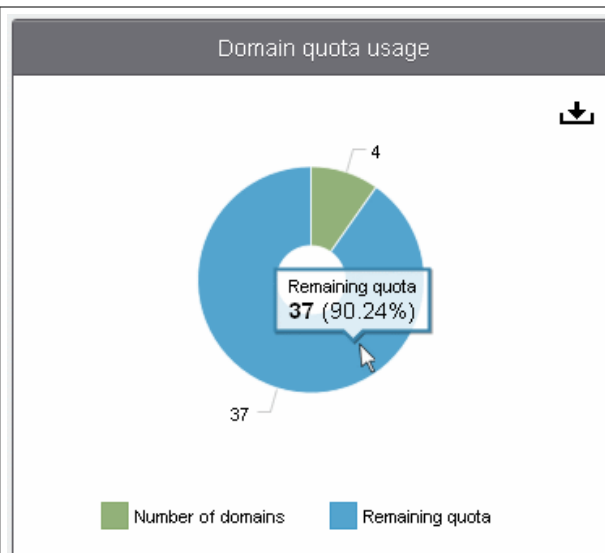


Domain Quota Usage

The number of domains used, and the number remaining on your current license.

Each domain that you set up for spam filtering will take one domain from the pool remaining on your license.

- Place your mouse cursor over any chart sector to view more details.
- Click an item in the legend to add or remove it from the chart.



User Quota Usage

Number of users protected by spam filtering, and the number remaining on your current license.

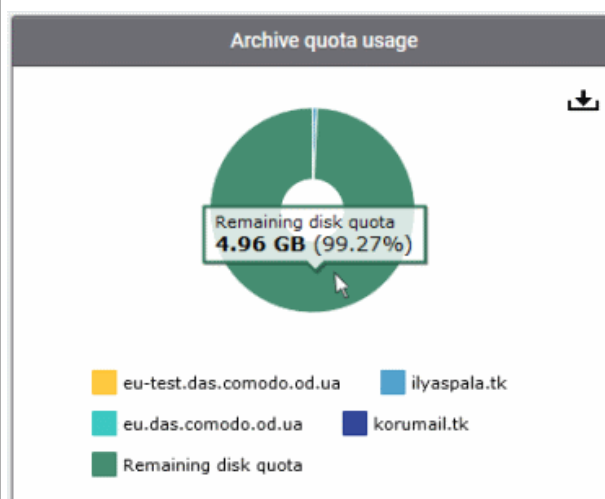
Each user that you protect with spam filtering will take one user from the pool remaining on your license.

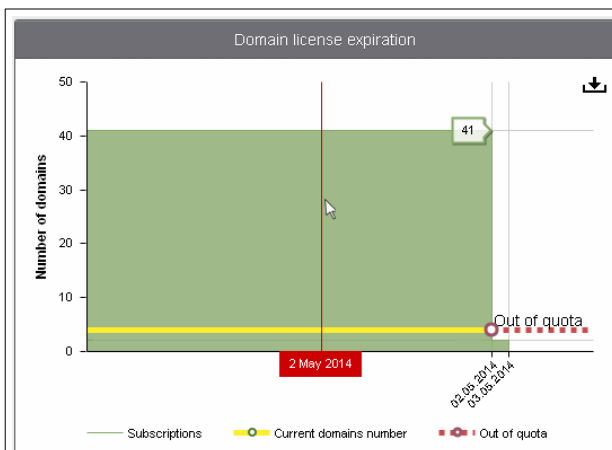
- Place your mouse cursor over any chart sector to view more details.
- Click an item in the legend to add or remove it from the chart.

Archive Quota Usage

The quantity of mail archive space already used for each domain, and the amount remaining on your current license.

- Place your mouse cursor over any chart sector to view more details.
- Click an item in the legend to add or remove it from the chart.





Domain License Expiration

Quantity of domains and domain license expiry dates.

Y axis - Domain count

X axis - Timeline

Green bars - Total number of domains allowed by all unexpired licenses.

Yellow line - Actual number of domains active on your account.

Out-of-quota - Shown if the actual number of domains is greater than the total allowed by your licenses.

Red line - Date when a license is due to expire.

Place your mouse cursor over any bar to see when the license is set to expire.

User License Expiration

Quantity of users and license expiry dates.

Y axis - User count

X axis - Timeline

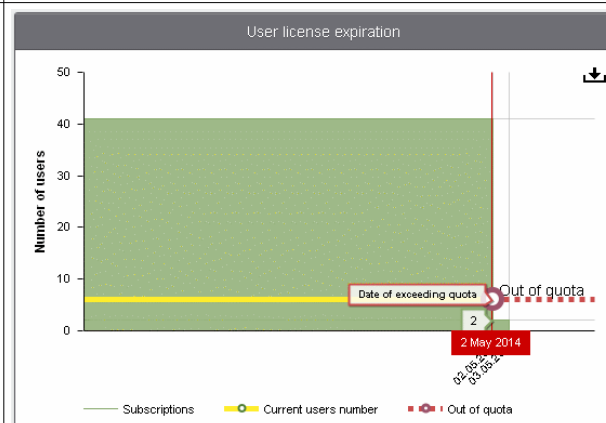
Green bars - Total number of users allowed by all unexpired licenses.

Yellow line - Actual number of users active on your account.

Out-of-quota - Shown if the actual number of users is greater than the total allowed by your licenses.

Red line - Date when a license is due to expire.

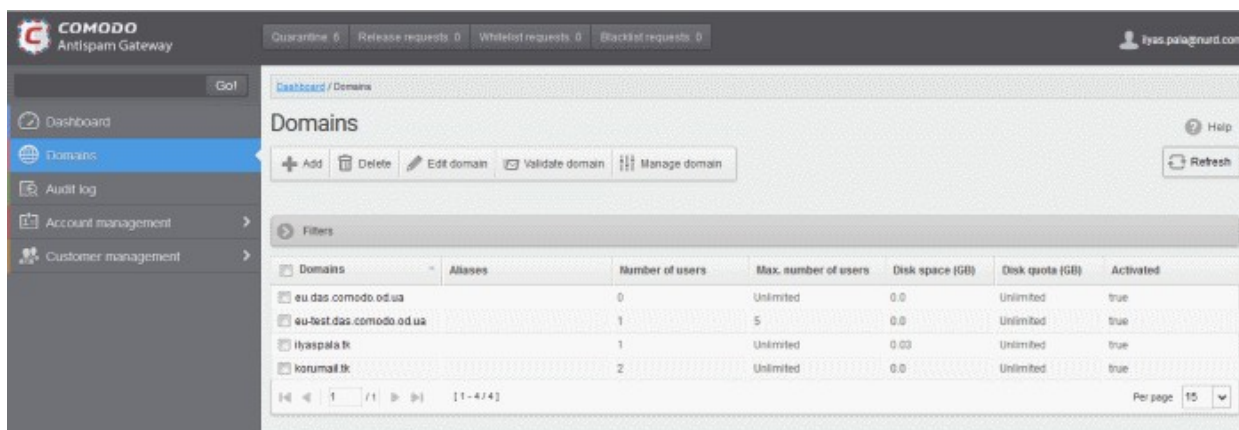
Place your mouse cursor over any bar to see when the license is set to expire.



6 Domain Management

Click 'Domains' on the left menu

- The domains area lets you configure domains for spam protection and manage them.
- You can configure policy settings such as email size restrictions, permitted file-extensions for attachments, spam detection settings and many more. See '[Manage a Domain](#)' for more details.



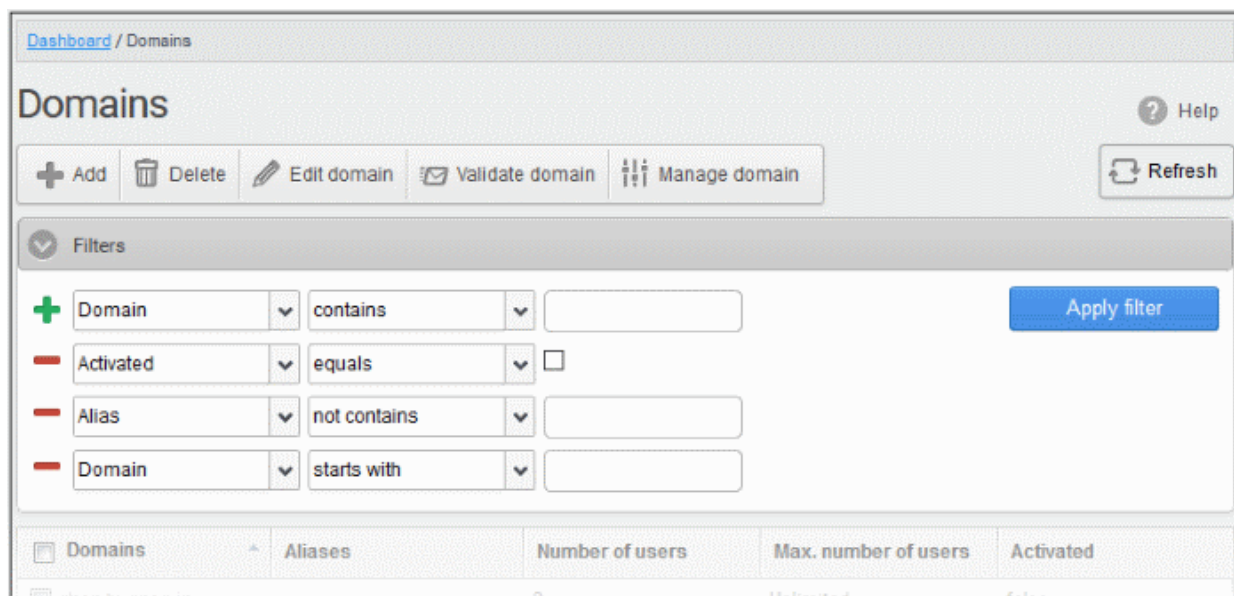
Use the following links for more help:

- [Add a domain](#)
- [Delete a domain](#)
- [Edit a domain](#)
- [Validate a domain](#)
- [Manage a domain](#)

Click the domain column header to sort domains in alphabetical order

Use filters to search particular domain(s)

- Click anywhere on the filters stripe to open it:




- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

- **Domain:** Type a domain name in the text box (column 3) and select a condition in column 2.
- **Activated:** Filter domains by their validation status
- **Aliases:** Type an alias domain name in the text box (column 3) and select a condition in column 2.

Click anywhere on the filters tab to close it. Click the 'Refresh' button to remove filters.

You can add multiple filters to the same search by clicking .

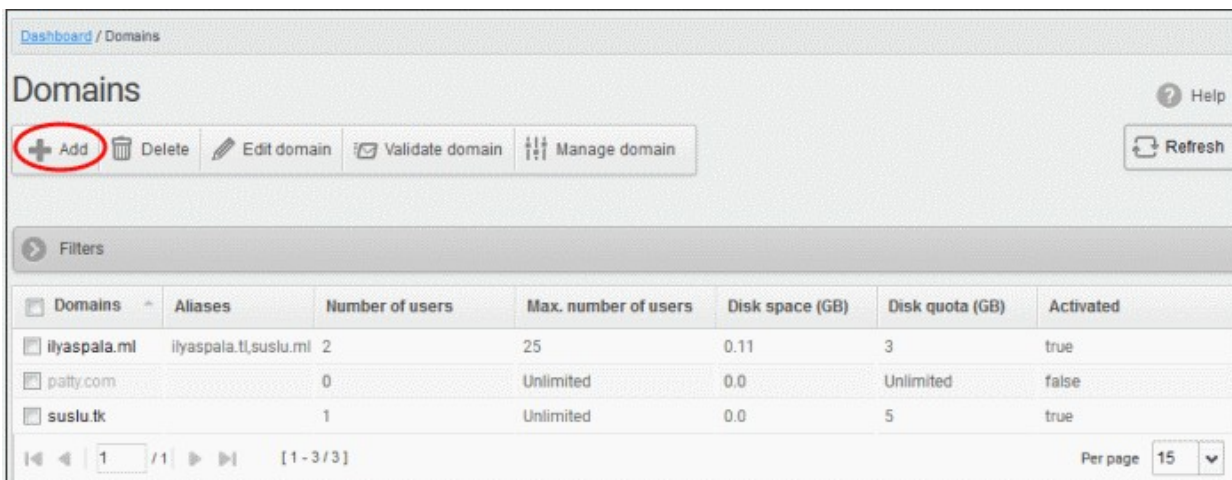
Tip: CASG can generate reports which summarize all mail activity on a domain. See [CASG Reports - An Overview](#) for more details.

6.1 Add a Domain

Admins with appropriate privileges can add domains, configure the number of users per domain, define a domain's destination route and specify archive space. The number of domains that you can add depends on your subscription plan.

Add a domain

- Click 'Domains' on the left
- Click the 'Add' button



The screenshot shows the 'Domains' management interface. At the top, there is a navigation bar with 'Dashboard / Domains' and a 'Help' icon. Below this is a toolbar with buttons for '+ Add', 'Delete', 'Edit domain', 'Validate domain', and 'Manage domain'. A 'Refresh' button is also present. Below the toolbar is a 'Filters' section. The main area contains a table with the following columns: Domains, Aliases, Number of users, Max. number of users, Disk space (GB), Disk quota (GB), and Activated. The table lists three domains: 'ilyaspala.ml', 'paity.com', and 'suslu.tk'. At the bottom, there is a pagination control showing '1 / 1' and '[1 - 3 / 3]', and a 'Per page' dropdown set to '15'.

Domains	Aliases	Number of users	Max. number of users	Disk space (GB)	Disk quota (GB)	Activated
<input type="checkbox"/> ilyaspala.ml	ilyaspala.tl,suslu.ml	2	25	0.11	3	true
<input type="checkbox"/> paity.com		0	Unlimited	0.0	Unlimited	false
<input type="checkbox"/> suslu.tk		1	Unlimited	0.0	5	true

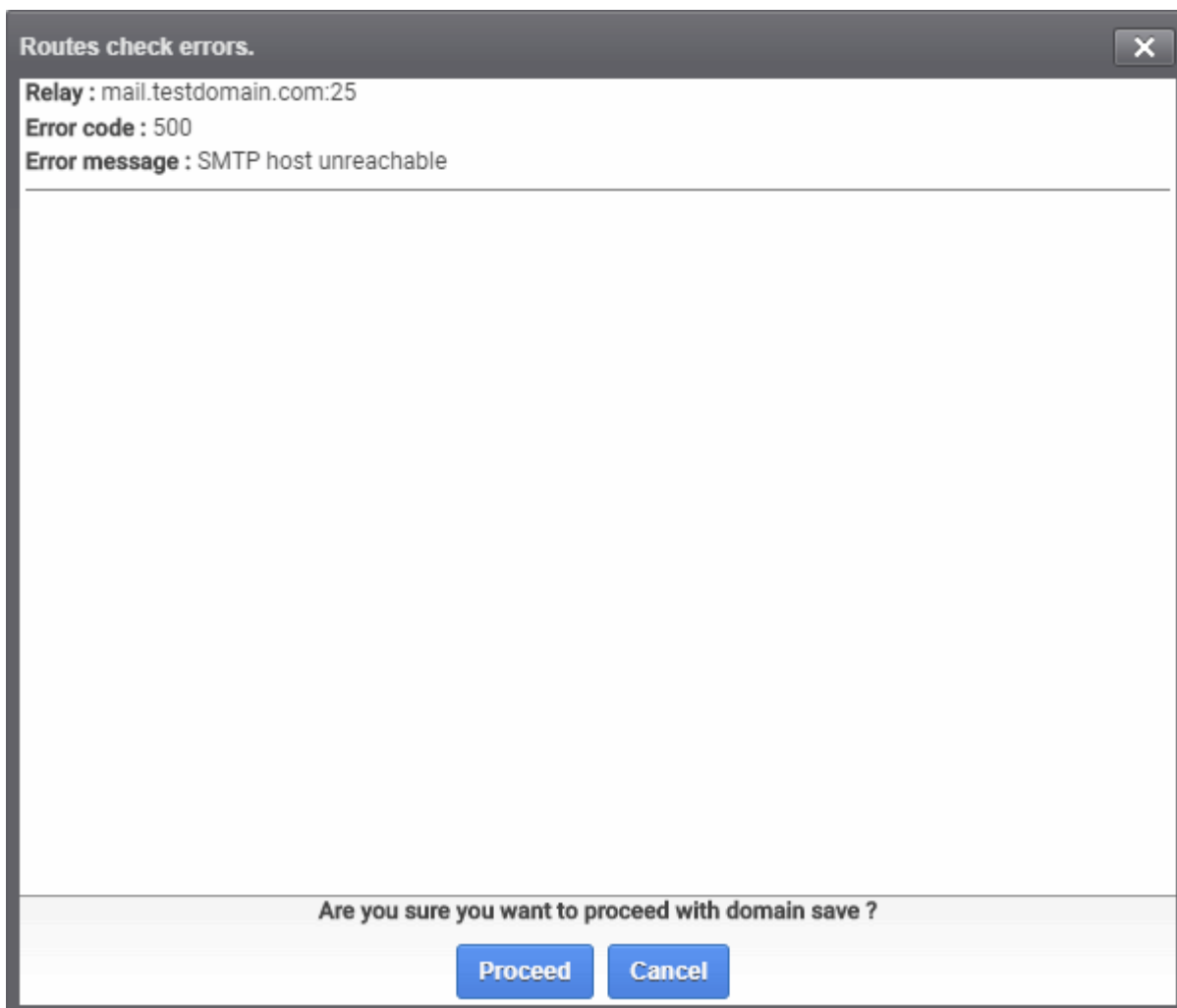
The 'Add domain' dialog will open.

The screenshot shows a window titled "Add domain" with a close button (X) in the top right corner. The window contains the following fields and controls:

- Domain:** A text input field containing "testdomain.com".
- Destination routes:** A list of two routes. The first route is "mail.testdomain.com" with a green plus icon to its left and a priority of "25" in a dropdown menu to its right. The second route is "mail1.testdomain.com" with a red minus icon to its left and a priority of "25" in a dropdown menu to its right.
- Timezone:** A dropdown menu showing "(GMT) Coordinated Ur".
- Domain user limit:** A text input field containing "Unlimited".
- Domain Archive Space (GB):** A text input field containing "Unlimited".

At the bottom of the window, there are three buttons: "Check routes" (blue), "Save" (blue), and "Cancel" (grey).

- **Domain** - Enter a valid domain name
- **Destination route** - Enter the address of the recipient mail server. This is the address to which CASG will forward mail after antispam filtering.
 - **Failover routes** - You can add additional destination routes to act as failovers. CASG will use the alternative routes if the primary route is unavailable for some reason. Click **+** to enter an additional route.
- **Timezone** - Set the zone for this domain. CASG will use this time-zone for events which concern that domain. Specifically, the quarantine list, archive list, log search, reports and report subscriptions.
- **Domain user limit** – Set the max. number of users that can be added to this domain. 'Unlimited' lets you add, but not exceed, the number of users permitted by your current license. Max. users for a domain can also be configured in the '**Domain Settings**' area.
- **Domain Archive Space** – Set the archive disk quota that this domain should use for storing mails. The disk space for all your domains cannot exceed the disk quota that you subscribed for.
- **Check Route** – Will retrieve routing information from the domain's DNS. If the result contains **CASG service domain** details (mxpool1.spamgateway.comodo.com - EU, or mxpool1.us.spamgateway.comodo.com – US), then it means your DNS MX record was already updated to work with CASG. You must enter your real MX record as the destination route. For example mail.exampledomain.com.



- Click 'Proceed' to save a domain.

Note: The number of users that you can add for all the domains belonging to your account depends on your subscription plan. For example, if the subscription plan for your account allows you to add 1000 users and you have three domains, then you can add 300 users for domain 1, 300 users for domain 2 and 400 users for domain 3. You can set any value between 0 and 999999 in the 'Max. number of users' field, but CASG checks if the total number of users for all domains is within your license limit.

- Click 'Save' to add the configured domains.

Note: When you create a new domain, email addresses 'abuse@addeddomain' and 'postmaster@addeddomain' are added by default in recipient whitelist. [Click here](#) for more details.

The following success message is displayed, along with a reminder to validate the domain within 24 hours:

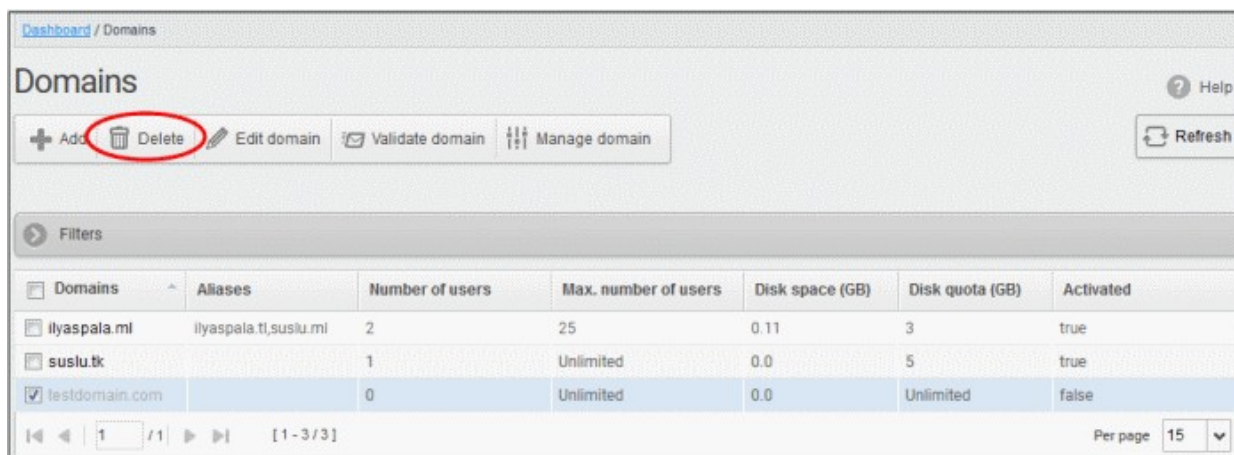
Request for domain TESTDOMAIN.COM successfully created. You have to validate your domain within 24 hours. Please follow instructions sent to postmaster@testdomain.com

If you have already configured the domain's MX record for CASG before adding the domain to the CASG interface, then only the success message is shown. See '[Configure MX Record](#)' for details about configuring MX records and '[Validate Domains](#)' for details about domain validation.

6.2 Delete Domains

Delete a domain

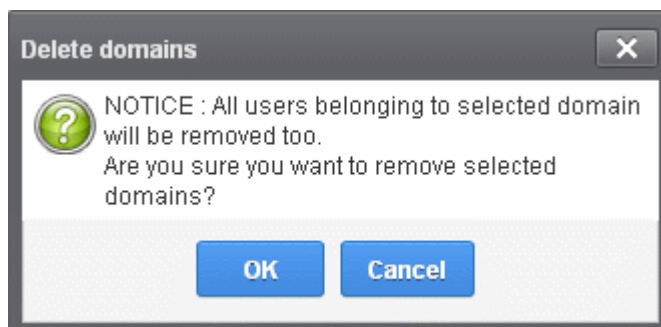
- Click the 'Domains' menu item on the left
- Select the domain(s) that you want to delete



- Click the "Delete" button

Tip: You can select multiple domains to delete by pressing and holding the Shift or Ctrl keys.

A notice is shown warning you that the users belonging to the selected domains will also be removed.



- Click 'OK' to confirm.

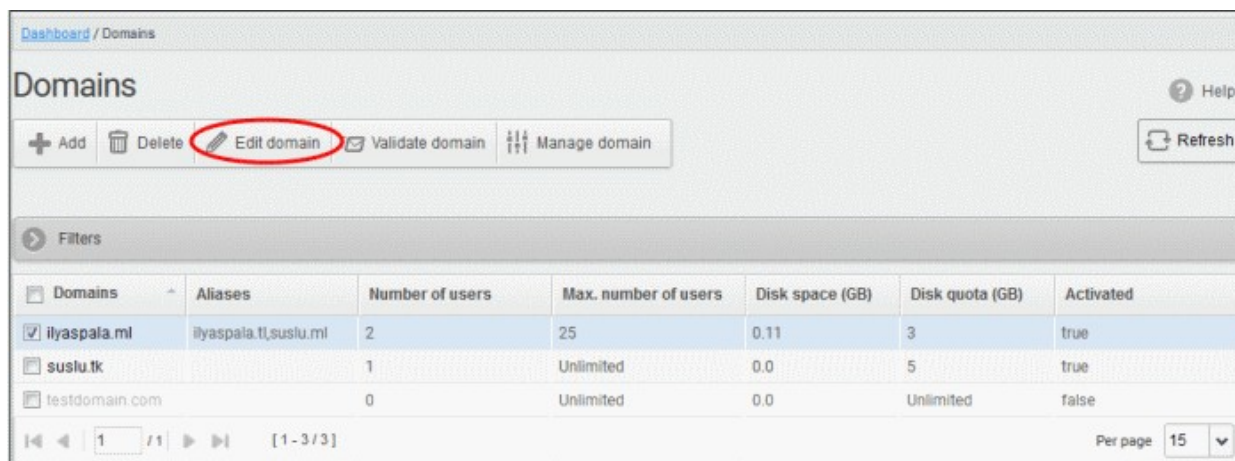
The selected domain(s) are deleted.

6.3 Edit Domains

You can change the destination route of domain, archive space and check its route. Please note that the name of the domain cannot be edited.

Edit a domain

- Click 'Domains' on the left
- Select the domain that you want to modify
- Click the 'Edit domain' button:



The 'Edit domain' dialog is shown:

- **Destination route** - Enter the address of the recipient mail server. This is the address to which CASG will forward mail after antispam filtering.
 - Failover routes - You can add additional destination routes to act as failovers. CASG will use the alternative routes if the primary route is unavailable for some reason. Click **+** to enter an additional route.
- **Timezone** - The zone for this domain. CASG will use this time-zone for events which concern that domain. Specifically, the quarantine list, archive list, log search, reports and report subscriptions.
- **Domain user limit** – The max. number of users that can be added to this domain. 'Unlimited' lets you add, but not exceed, the number of users permitted by your current license. Max. users for a domain can also be configured in the 'Domain Settings' area.
- **Domain Archive Space** – Set the archive disk quota that this domain should use for storing mails. The disk space for all your domains cannot exceed the disk quota that you subscribed for.
- **Check Route** – Will retrieve routing information from the domain's DNS. If the result contains **CASG service domain** details (mxpool1.spamgateway.comodo.com - EU, or mxpool1.us.spamgateway.comodo.com – US), then it means your DNS MX record was already updated to work with CASG. You must enter your real MX record as the destination route. For example mail.exampledomain.com.

Note: The total of users that you can add across all your domains depends on your license. You can set any value

between 0 and 999999 in the 'Max. number of users' field, but CASG checks if the total number of users for all domains is within your license limit.

- Click 'Save' to confirm the changes.

6.4 Validate Domains

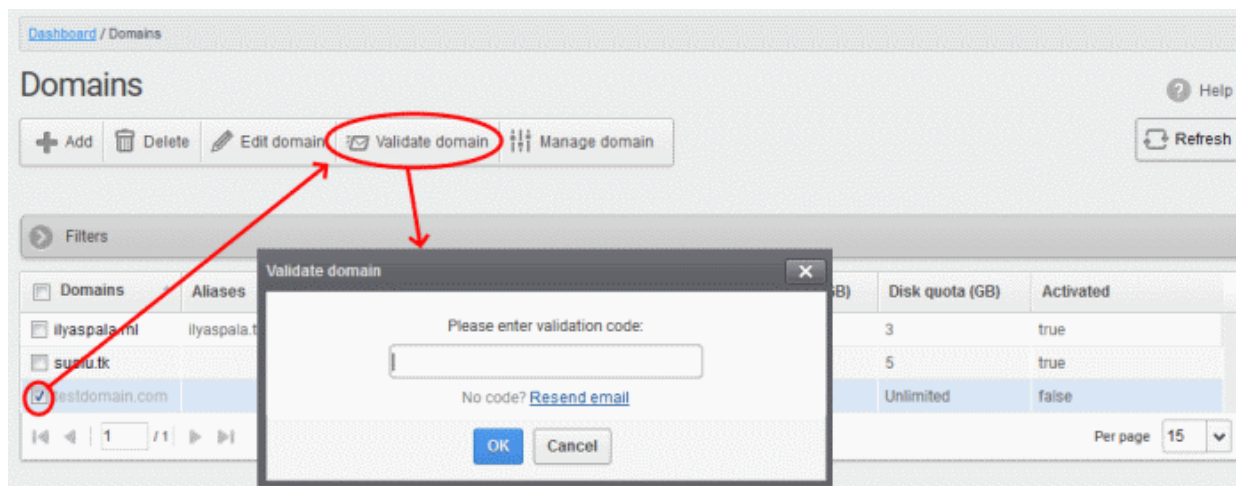
CASG requires all domains be validated in order to demonstrate your ownership of the domains. This can be done in two ways:

- The first method is to configure the MX record for the domain to the CASG service before adding the domain in the CASG interface. When you add this domain it will be automatically validated since only a person in control of the domain is able to modify MX records. See '**Configure MX Record**' for details about configuring MX record to CASG.
- The second method is to add the domain to CASG first then validate ownership by providing an authentication code sent to `postmaster@your_domain.com`

The following tutorial explains the second method. Please note that domains which have not been validated will be grayed out and marked as 'False' in the 'Activated' column.

Validate a domain

- Click the 'Domains' menu item on the left
- Select the domain and click the 'Validate domain' button
- The 'Validate domain' dialog opens:



A mail containing the validation code is sent to `postmaster@your-domain.com` immediately after adding a domain.

- Click 'Resend email' to send this mail again.
- Enter the code the field and click 'OK'

CASG will verify the code and, if successful, the domain is activated:

Dashboard / Domains

Domains

Help Refresh

+ Add Delete Edit domain Validate domain Manage domain

Filters

Domains	Aliases	Number of users	Max. number of users	Disk space (GB)	Disk quota (GB)	Activated
ilyaspala.ml	ilyaspala.tl,suslu.ml	2	25	0.11	3	true
suslu.tk		1	Unlimited	0.0	5	true
testdomain.com		0	Unlimited	0.0	Unlimited	true

1 / 1 [1-3/3] Per page 15

Non-validated domains should be validated within 24 hours or they will be automatically removed from the interface.

Note: Domain control validation (DCV) is only required for new domains added after the release of CASG version 2.10. Any domains added prior to v. 2.10 do not require DCV. Later releases may enforce DCV on all domains in stages.

6.5 Manage a Domain

- Administrators can configure various settings for a selected domain: view quarantined mails, set email restrictions, add users as recipient whitelist or blacklist, add new users and view log reports for the domain.
- This section is divided into seven main subsections. Namely, Domain dashboard, Incoming, Outgoing, Email management, Audit log, Domain Rules and Account management. Click on the respective tabs to expand or close the subsection in the left.

Manage a domain

- Click the 'Domains' menu on the left
 - Select the domain that you want to manage, then click the 'Manage Domain' button
 - Alternatively, click on the domain name in the 'Domains' column
- OR
- Right-click on the domain name in the 'Domains' column to open in a new tab or window

COMODO Antispam Gateway

Quarantine: 6 Release requests: 0 Whitelist requests: 0 Blacklist requests: 0

ilyaspala@nurd.com

Dashboard / Domains

Domains

Help Refresh

+ Add Delete Edit domain Validate domain Manage domain

Filters

Domains	Aliases	Number of users	Max. number of users	Disk space (GB)	Disk quota (GB)	Activated
eu.das.comodo.od.ua		0	Unlimited	0.0	Unlimited	true
eu-test.das.comodo.od.ua		1	5	0.0	Unlimited	true
ilyaspala.tk		1	Unlimited	0.03	Unlimited	true
korumail.tk		2	Unlimited	0.0	Unlimited	true

1 / 1 [1-4/4] Per page 15

- The configuration tabs for the selected domain will open on the left.
- By default, the 'Domain dashboard' for the selected domain is displayed.



Click on the following links for more details on the subsections:

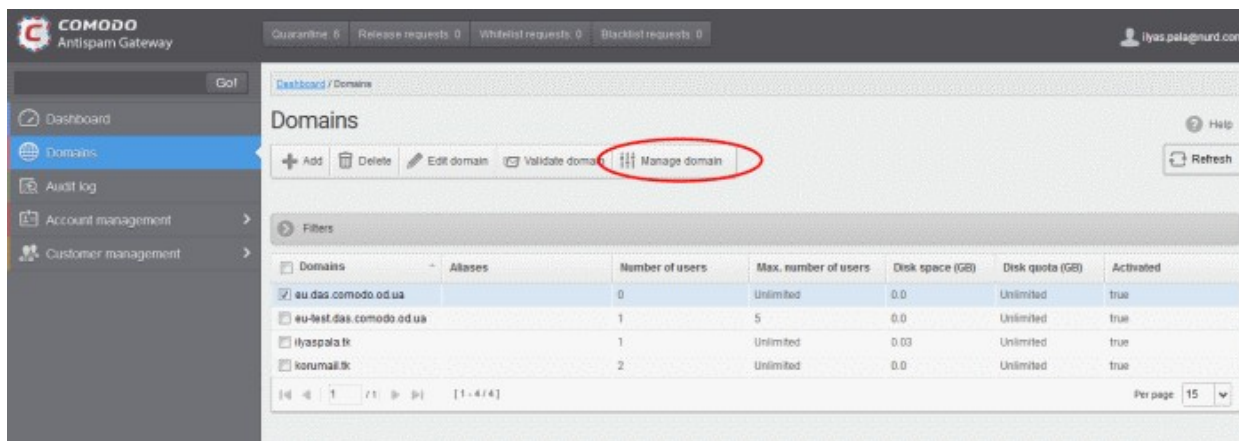
- [Domain Dashboard](#)
- [Incoming](#)
- [Outgoing](#)
- [Email Management](#)
- [Domain Audit Log](#)
- [Domain Rules](#)
- [Account Management](#)

6.5.1 Domain Dashboard

- Domain dashboards provide a fast heads-up on mail activity on your protected domains. Statistics include the number of quarantined mails, release requests, whitelist requests, blacklist requests, incoming mails archive quota usage and more.
- You can export the dashboards to image or pdf file by clicking the download icon at the top-right of each item.

Open a domain dashboard

- Click the 'Domains' menu on the left
 - Select the domain that you want to manage
 - Click the 'Manage Domain' button
 - Alternatively, click on the domain name in the 'Domains' column
- OR
- Right-click on the domain name in the 'Domains' column to open in a new tab or window



The dashboard of the selected domain is displayed:

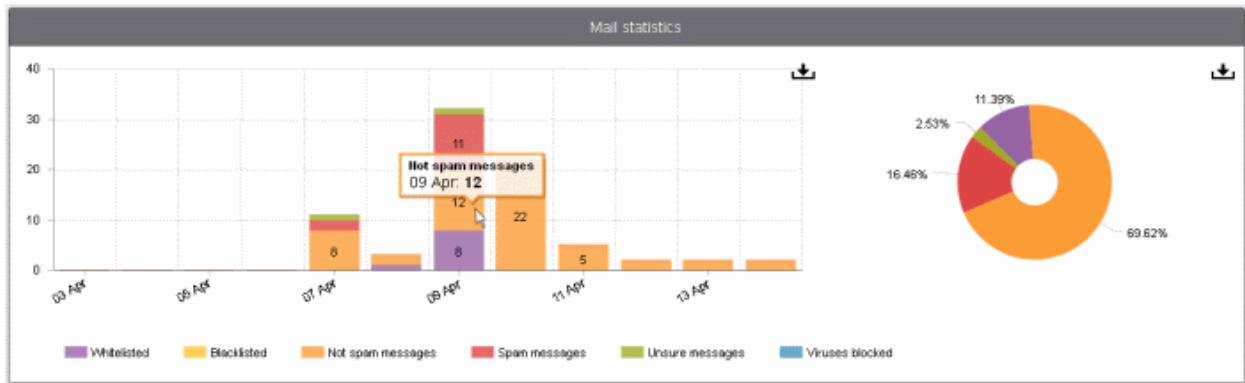


The buttons along the top of the dashboard allow you to view and take action on important items:

- **Quarantine** - Quarantined mails of all users of the selected domain. See [Quarantine](#) for more details.
- **Release requests** - Requests from users on the selected domain to release quarantined mails. See [Released Requests](#) for more details.
- **Whitelist requests** - Requests from users on the selected domain to whitelist the senders of quarantined mails. See [Whitelisted Requests](#) for more details.
- **Blacklist requests** - Requests from users on the selected domain to blacklist the senders of quarantined mails. See [Blacklisted Requests](#) for more details.

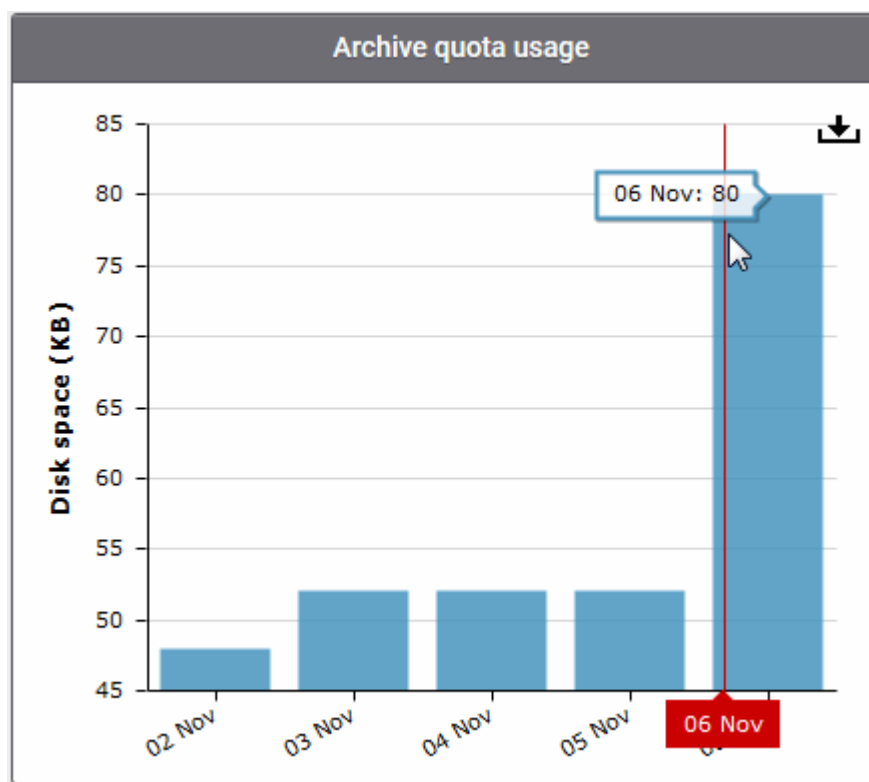
The 'Mails Statistics' area has charts to show blocked mails, blocked viruses and more.

- Place your mouse cursor over a graph to view more details.
- Click on a legend item to add or remove it from a graph.

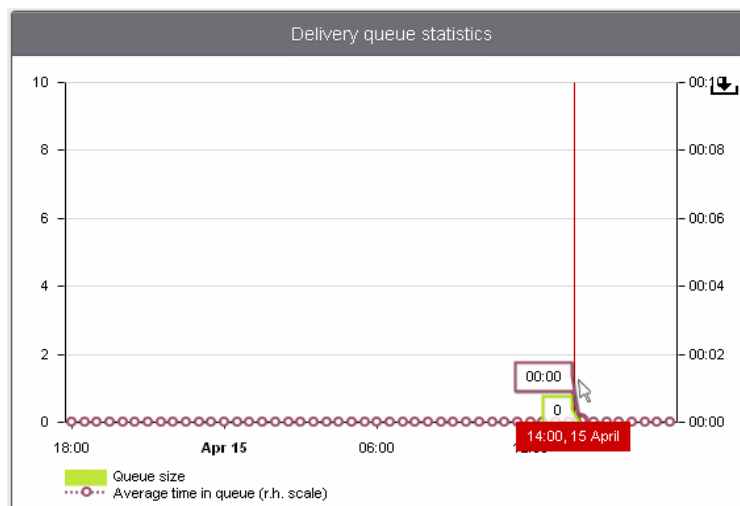


The 'Archive quota usage' area shows how much storage space has been used to archive incoming mails. The graph shows the disk space used per day for the last two weeks.

- Place your mouse cursor over a graph to view the space used on a specific date. See [Manage Archived Mails](#) for more details.

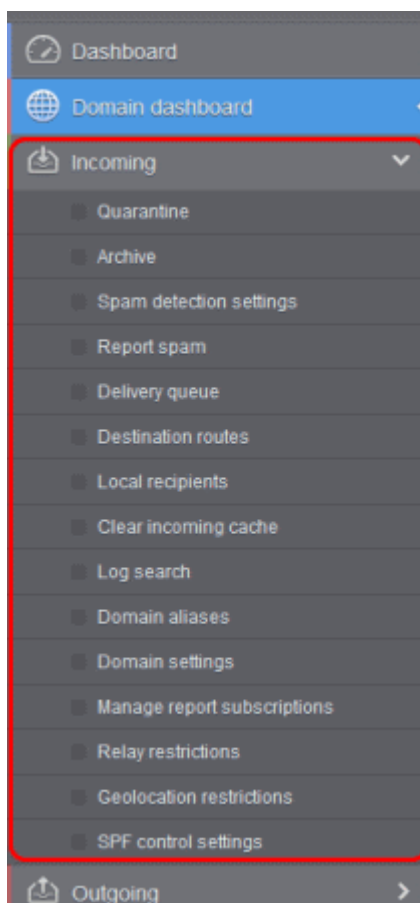


- The 'Delivery queue statistics' area provides details of filtered mails that are queued in CASG servers for delivery at a later time.
- It also displays the average time of queued mails for the previous day in CASG servers before delivery. See [Delivery Queue](#) for more details.



6.5.2 Incoming

The 'incoming' area lets you view quarantined mails, configure spam detection settings, set spam alerts, add local email recipients, and more.



Click the following links for more details:

- [Quarantine](#)
- [Manage Archived Mails](#)
- [Incoming Spam detection settings](#)

- [Report Spam](#)
- [Delivery Queue](#)
- [Destination routes](#)
- [Local Recipients](#)
- [Clear Incoming Cache](#)
- [Log Search](#)
- [Domain Aliases](#)
- [Domain Settings](#)
- [Manage Report Subscriptions for Selected Domain](#)
- [Relay Restrictions](#)
- [Geolocation Restrictions](#)
- [SPF Control Settings](#)

Quarantine

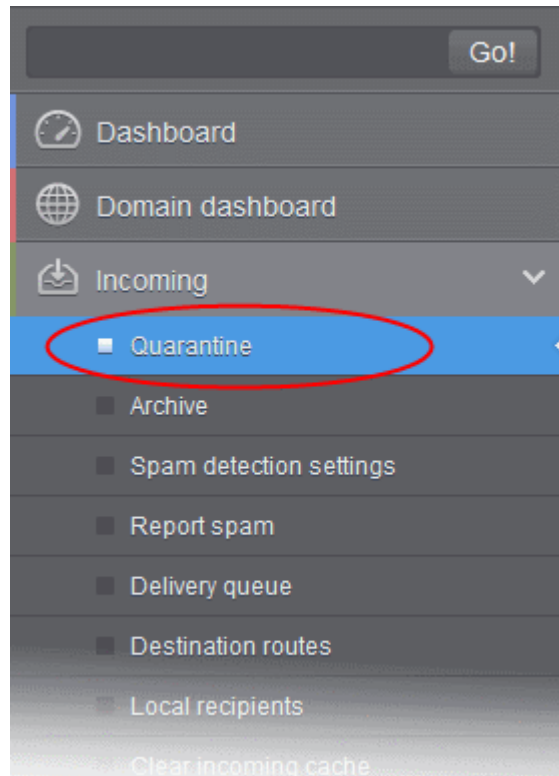
- View all quarantined emails and their headers for all users on the selected domain.
- Release quarantined emails to the intended recipient if you decide that a particular email is not spam.
- Delete selected or all spam mails

Tip: CASG periodically generates a report on all messages moved to quarantine.

- Reports are emailed to admins
- You can configure the reports in [Dashboard](#) > [Account Management](#) > [Admin](#) > [Add Administrators](#), See [CASG Reports - An Overview](#) if you need help with reports.

Open the quarantined email interface

- Click 'Quarantine' on the 'Incoming' drop-down menu on the left



The quarantined email area will open:

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Quarantine

Quarantine

[Show message](#) [Release](#) [Delete](#) [More actions](#) [Refresh](#) [Help](#)

Filters

Subject	From	To	Recipient	Date (GMT+)	Reason	Size	Actions
<input type="checkbox"/> Spam email 1	admin <demo@csg.comodo.od.ua>	demo1@docteamcasg.com	demo1@docteamcasg.com	Oct 28, 2014 1:21:46 PM	spam External pattern match (Sanesecurity.Junk.:	168 bytes	
<input type="checkbox"/> Spam email 2	admin <demo@csg.comodo.od.ua>	demo2@docteamcasg.com	demo2@docteamcasg.com	Oct 28, 2014 1:21:19 PM	spam External pattern match (Sanesecurity.Junk.:	168 bytes	

1 / 1 [1 - 2 / 2] Per page 15

- Click any column header to sort items in ascending/descending order.
- Click anywhere on the 'Filters' tab to open the filters area:

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.ed.ua / Quarantine

Quarantine

Help

Show message Release Delete More actions

Refresh

Filters


+	Subject	contains		Apply filter
-	From	contains		
-	To	contains		
-	Date	equals		
-	Size (KB)	less than	0	
-	Reason	contains		
-	Recipient	contains		

- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

- **Subject:** Type the mail subject in the text box (column 3) and select a condition in column 2.
- **From:** Enter the sender name or address in the text box (column 3) and select a condition in column 2.
- **To:** Enter the recipient name or address in the text box (column 3) and select a condition in column 2.
- **Reason:** Enter the quarantined reason in the text box (column 3) and select a condition 2.
- **Recipient:** Enter the recipient name or address in the text box (column 3) and select a condition in column 2.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

You can add multiple filters to the same search by clicking .

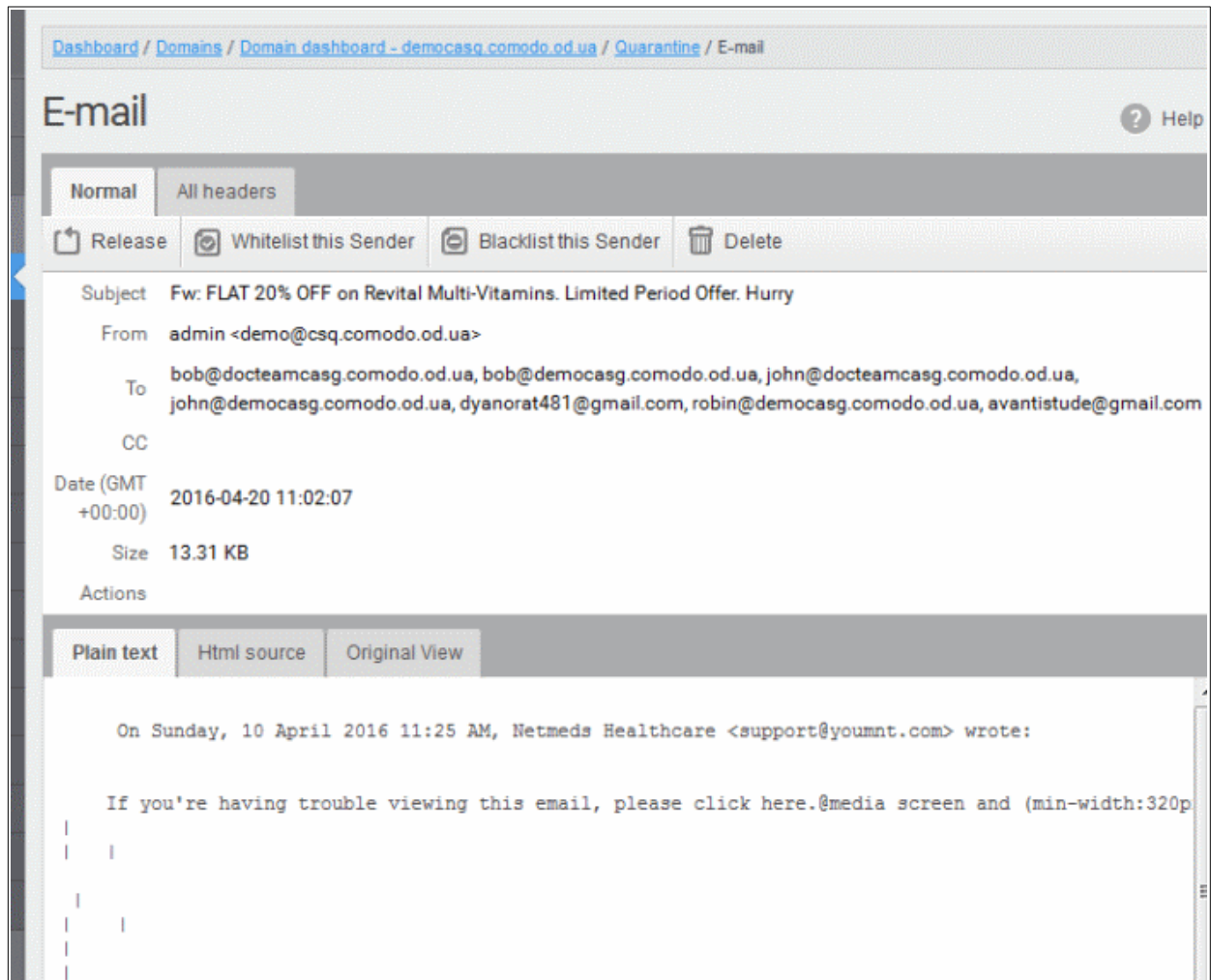
View Details of Quarantined Mails

The details like subject, sender, recipient, date and size of the mails added to the Quarantine can be viewed in two ways:

- **In the same CASG window**
- **In a new CASG window**

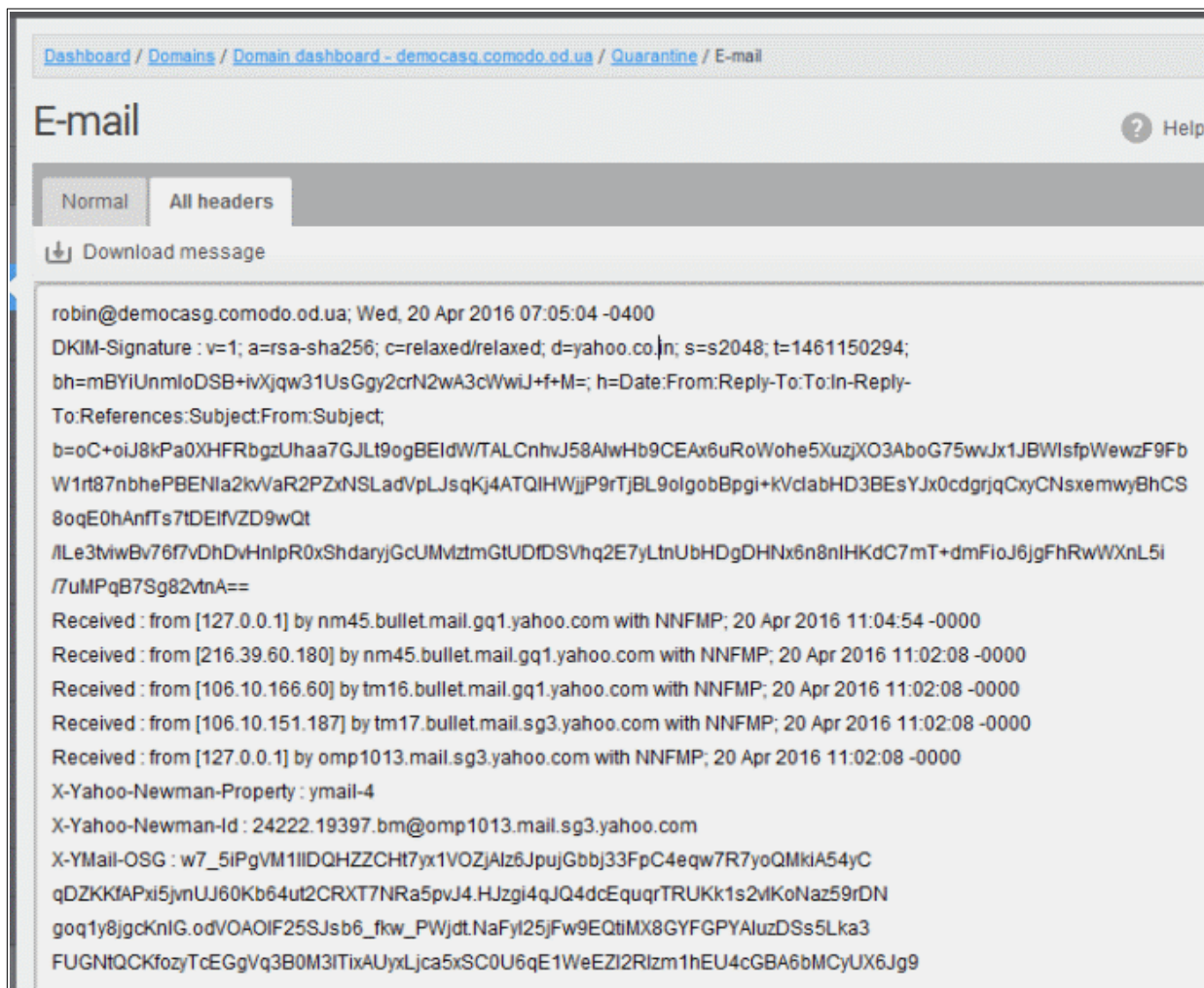
View details of quarantined mails in the same CASG window

- Select the mail that you want to view in the quarantined email area
- Click the 'Show Message' button
- OR
- Click on the email link in the subject column that you want to view its details



The details of the selected email will be displayed.

- Click 'All headers' to view the email headers which contain the tracking information of the mail detailing the path it has crossed before reaching the recipient. The headers give full details of the sender, route, recipient, sent date, mail type and so on and enable you to check the authenticity of the mail.

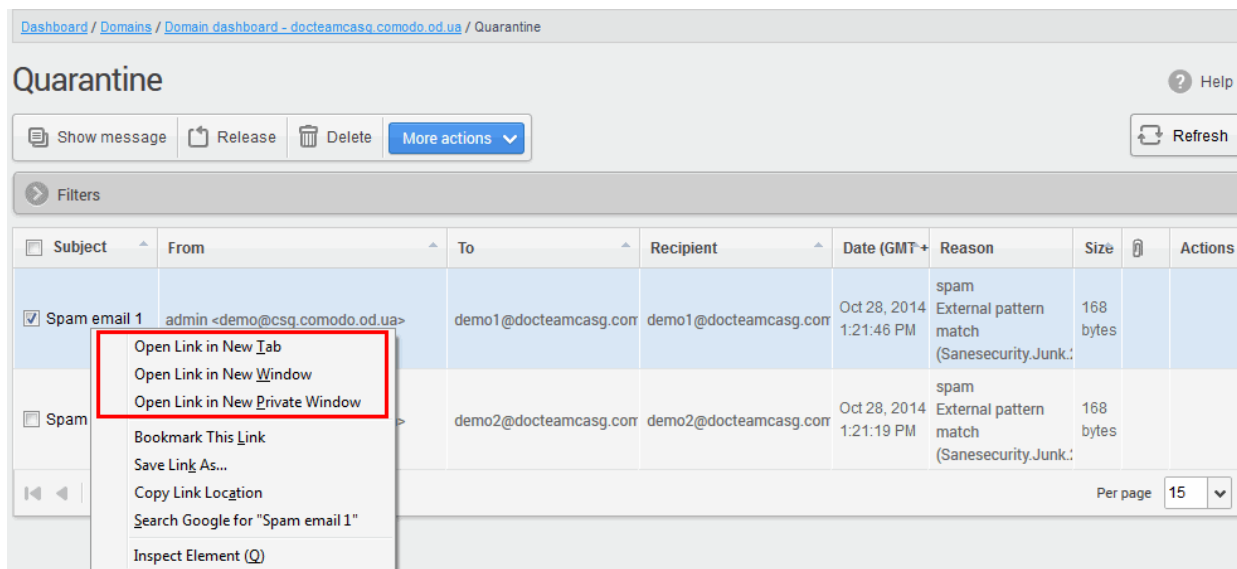


Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either release the mail or delete it.

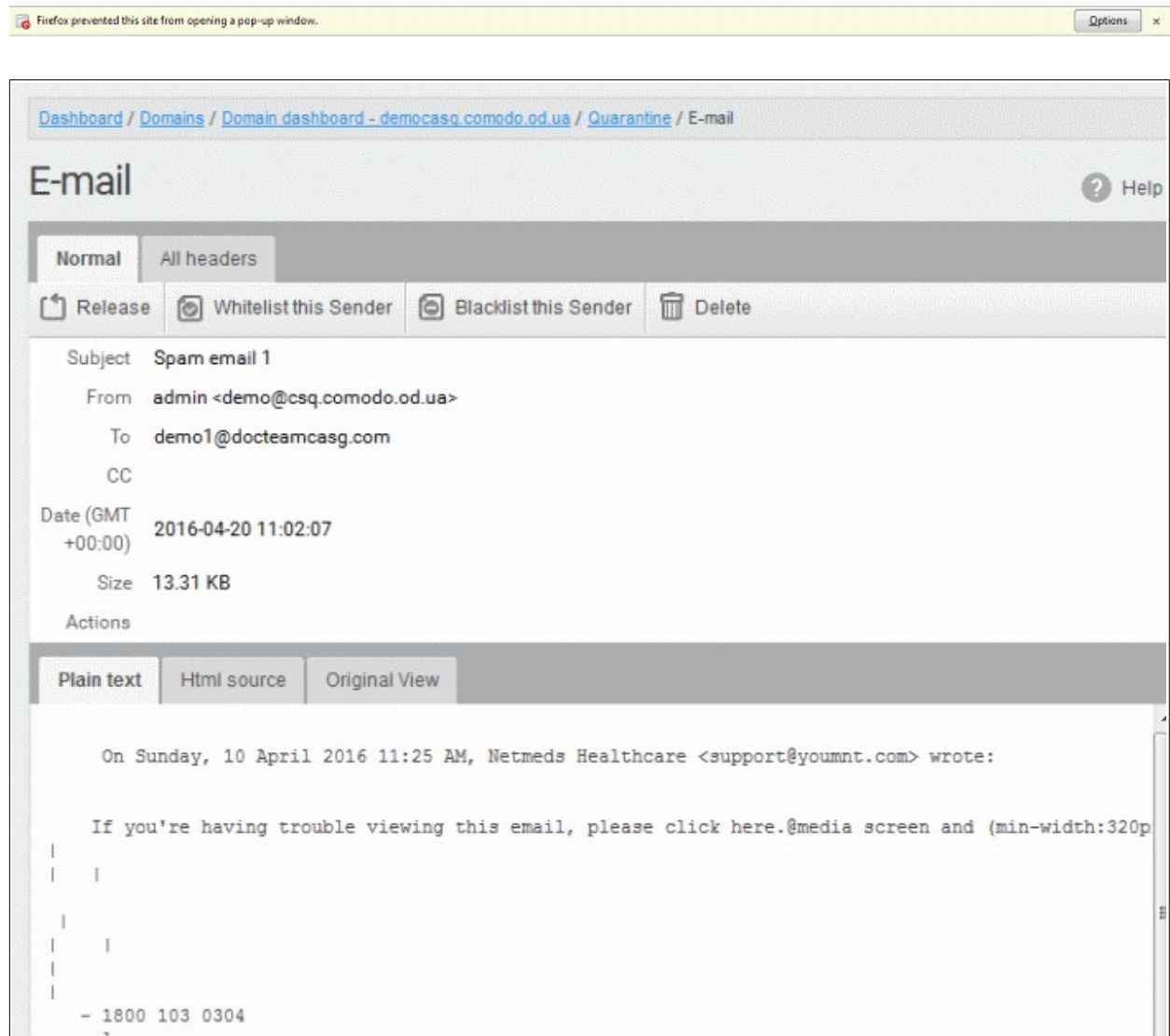
- Click 'Whitelist this sender' to add the sender to **Sender Whitelist**
- Click 'Blacklist this Sender' to add this sender to **Sender Blacklist**.

View the details of a quarantined mail in a new CASG window

- Select the mail that you want to view in the quarantined email area
- Right-click on the email link in the subject column and select to open in a new tab or new window.



The browser may display a warning pop-up window notification. Click the 'Options' > then select 'Allow pop-ups for...' to allow to open new message in a new window. Click again 'Show message in new window'.



The details of the selected mail will be displayed in a new CASG window.

Release a quarantined mail:

After viewing the details and ensuring that the selected email is not a spam you can choose to release the mail to the recipient.

- Select the mail that you want to release and click the 'Release' button.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Quarantine

Quarantine

Help

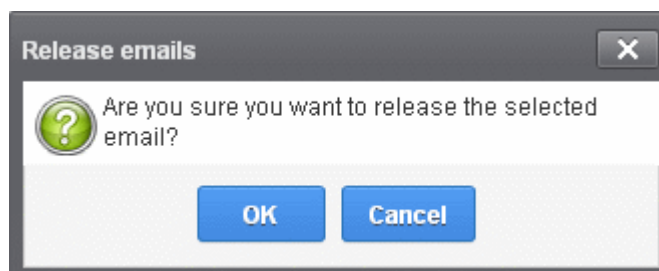
Show message Release Delete More actions Refresh

Filters

Subject	From	To	Recipient	Date (GMT +0)	Reason	Size	Actions
<input checked="" type="checkbox"/> Spam email 1	admin <demo@csg.comodo.od.ua>	demo1@docteamcasg.comod	demo1@docteamcasg.	Oct 28, 2014 1:21:46 PM	spam External pattern match (Sanesecurity.Junk.20)	168 bytes	
<input type="checkbox"/> Spam email 2	admin <demo@csg.comodo.od.ua>	demo2@docteamcasg.comod	demo2@docteamcasg.	Oct 28, 2014 1:21:19 PM	spam External pattern match (Sanesecurity.Junk.20)	168 bytes	

1 / 1 [1 - 2 / 2] Per page 15

An alert will confirm the release of the selected email.



- Click 'OK' to confirm the release

The email will be released to the addressee and the mail will no longer be in the quarantined list.

Add a sender to whitelist

After confirming that mail from a sender is not spam, admins can add them to the **Sender Whitelist**. Emails from whitelisted senders will no longer get quarantined.

- Select a mail from a sender that you want to whitelist
- Click 'More actions' > 'Whitelist this Sender'.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Quarantine

Quarantine

Help

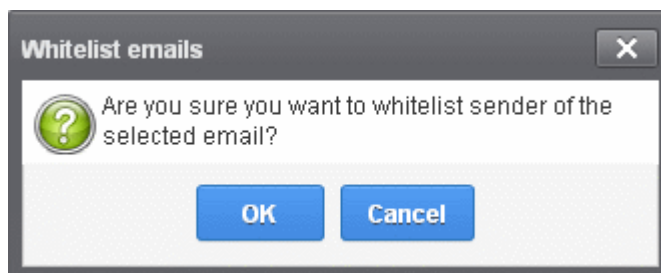
Show message Release Delete More actions Refresh

Filters

Subject	From	To	Recipient	Date (GMT +0)	Reason	Size	Actions
<input checked="" type="checkbox"/> Spam email 1	admin <demo@csg.comodo.od.ua>	demo1@docteamcasg.comod	demo1@docteamcasg.	Oct 28, 2014 1:21:46 PM	spam External pattern match (Sanesecurity.Junk.20)	168 bytes	
<input type="checkbox"/> Spam email 2	admin <demo@csg.comodo.od.ua>	demo2@docteamcasg.comod	demo2@docteamcasg.	Oct 28, 2014 1:21:19 PM	spam External pattern match (Sanesecurity.Junk.20)	168 bytes	

1 / 1 [1 - 2 / 2] Per page 15

A confirmation is shown as follows:

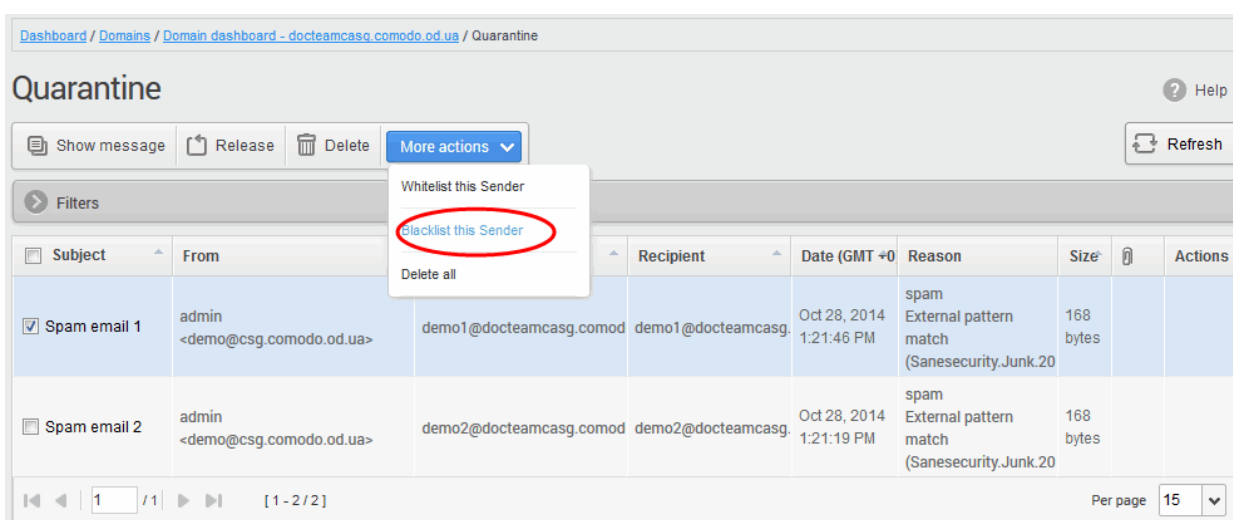


- Click 'OK' to whitelist the sender. See '[Sender Whitelist](#)' for more details.

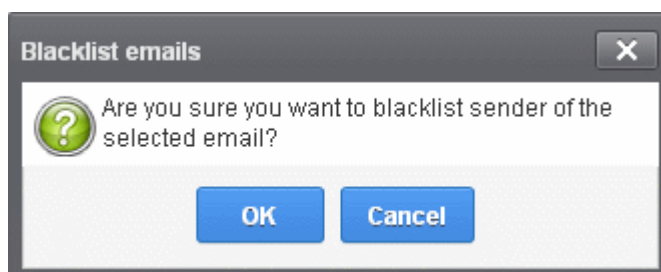
Add a sender to blacklist

Admins can add blacklist senders from the quarantine interface. Once blacklisted, all mails from the sender to the selected domain are automatically blocked.

- Select a mail from a sender you want to blacklist
- Click 'More actions' > 'Blacklist this Sender'.



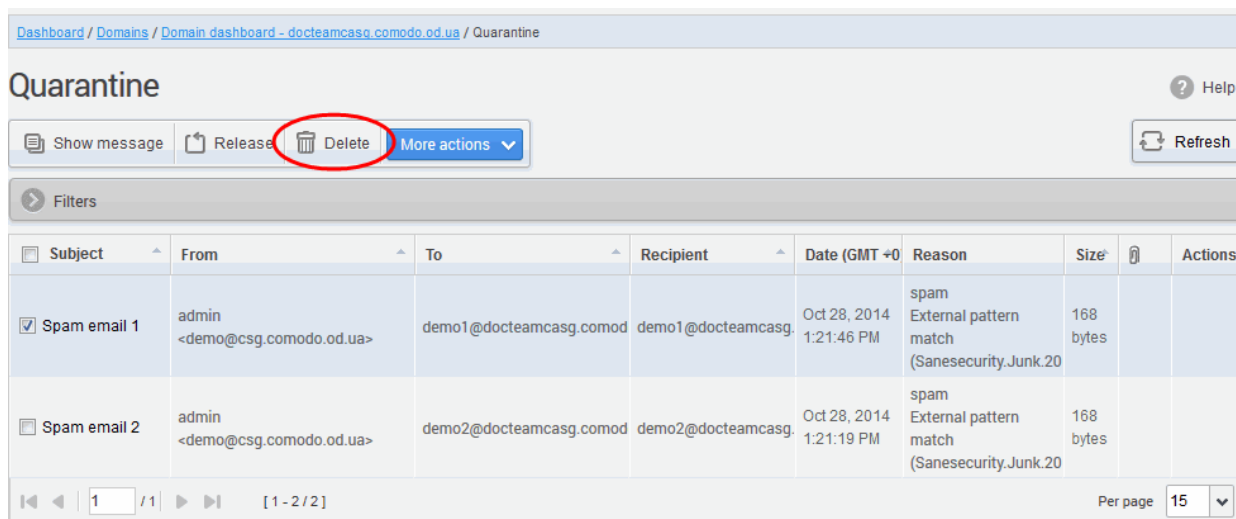
A confirmation is shown as follows:



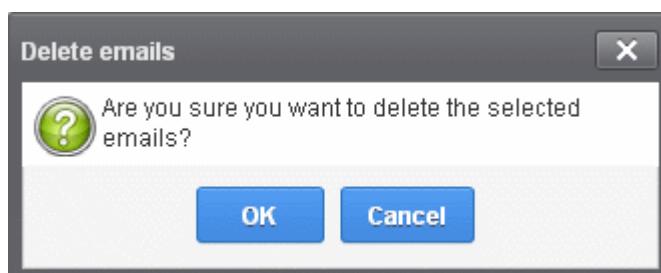
- Click 'OK' to blacklist the sender. See '[Sender Blacklist](#)' for more details.

Delete quarantined mail

- Select the mail that you want to remove
- Click the 'Delete' button

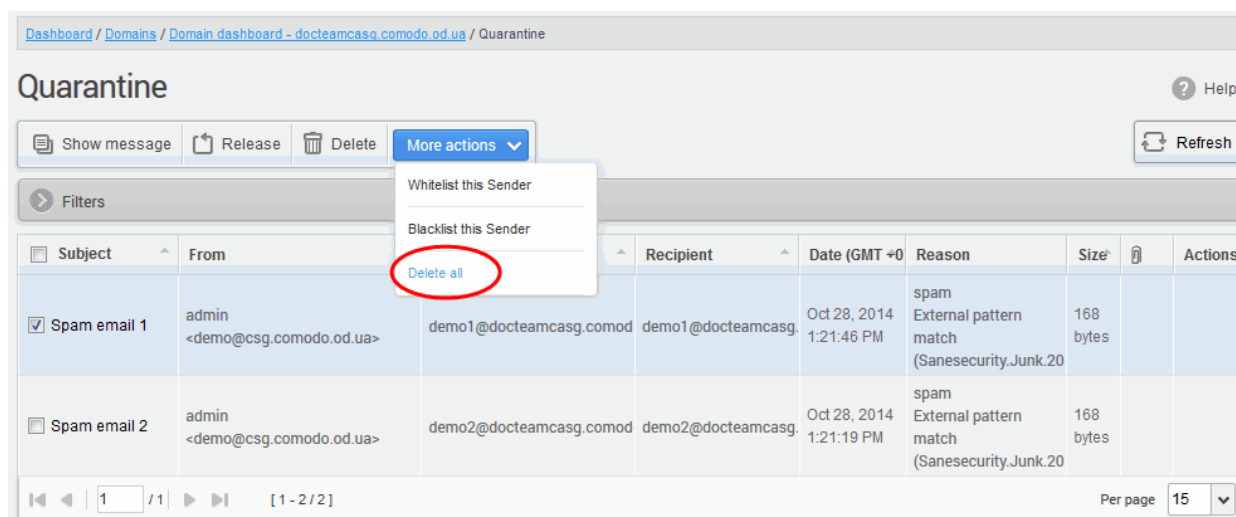


A confirmation request will be displayed:

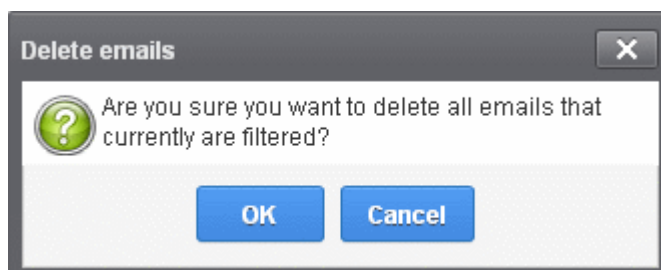


The selected mail will be deleted and will no longer be in the quarantined mail list.

- To delete all the quarantined mails, click 'More actions' > 'Delete all'.



A confirmation is shown as follows:



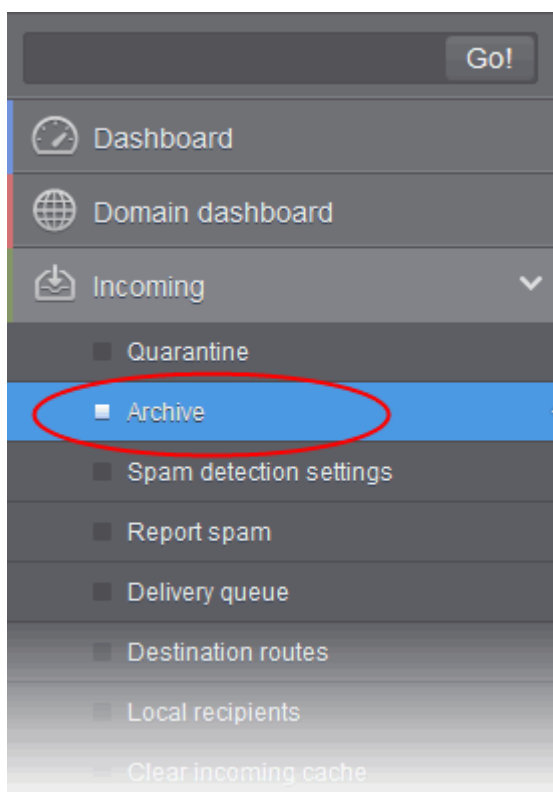
- Click 'OK' to delete all quarantined emails. All the quarantined emails for the selected domain will be deleted .

Manage Archived Mails

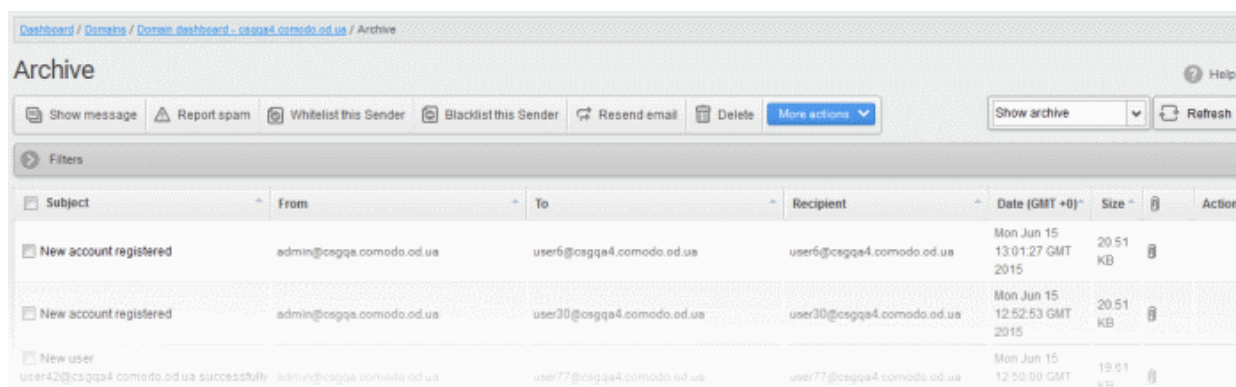
CASG can store copies of all incoming mail for all domains on an account. You can purchase storage space in Comodo Accounts Manager (CAM) at <https://accounts.comodo.com>

Open the archived mail area:

- Click 'Incoming' > 'Archive':

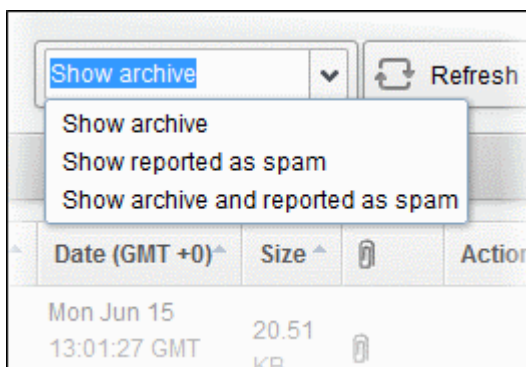


The archived email area of the selected domain will open:



Page Filter

The page filter on the top-right has three options:

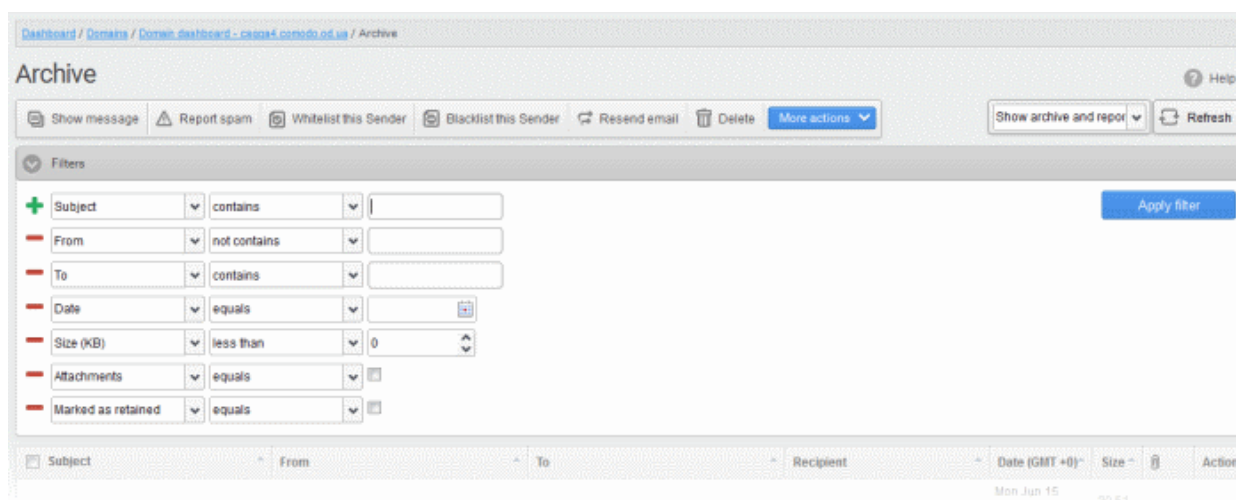


- **Show archive:** Lists only the archived mails
- **Show reported as spam:** Lists mails that are reported as spam
- **Show archive and reported as spam:** Lists both archived mails and mails that are reported as spam

Select the option from the drop-down before using the filter option described below.

Use filter option to search archived emails

- Click anywhere on the 'Filters' to open the filters area.




- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

- **Subject:** Type the email subject in the text box (column 3) and select a condition in column 2.
- **From:** Enter the sender name or address in the text box (column 3) and select a condition in column 2.
- **To:** Enter the recipient name or address in the text box (column 3) and select a condition in column 2.
- **Date:** Search by date and time mails archived. Select the date (column 3) and select a condition in column 2.
- **Size (KB):** Search archived mails by their size. Select or enter the mail size in column 3 and select a condition in column 2.
- **Attachments:** Enable or disable the checkbox (column 3) and select the condition in column 2.
- **Marked as retained:** Enable or disable the checkbox (column 3) and select the condition in column 2.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

You can add multiple filters to the same search by clicking  .

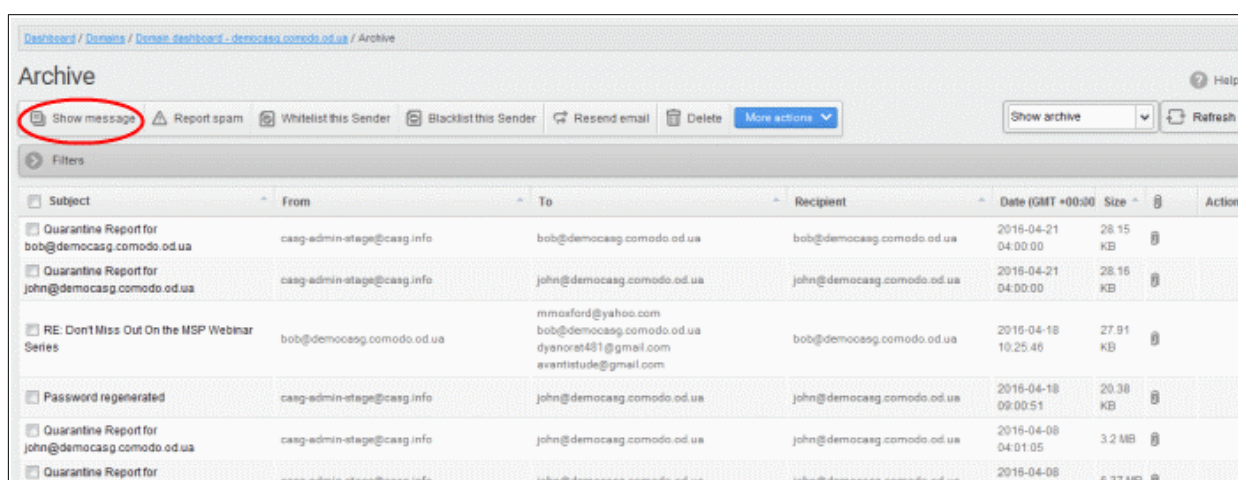
View Details of Archived Mails

There are two ways you can view the details of an archived mail:

- **In the same CASG window**
- **In a new CASG window**

View details in the same window

- Select the mail that you want to view in the 'Archive' area
- Click the 'Show Message' button
- OR
- Click on the email link in the subject column that you want to view its details.

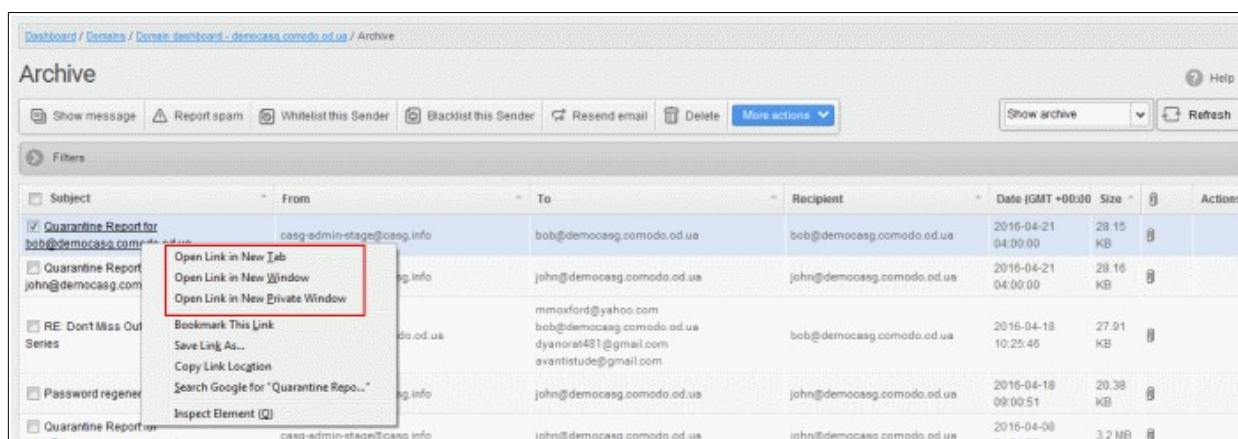


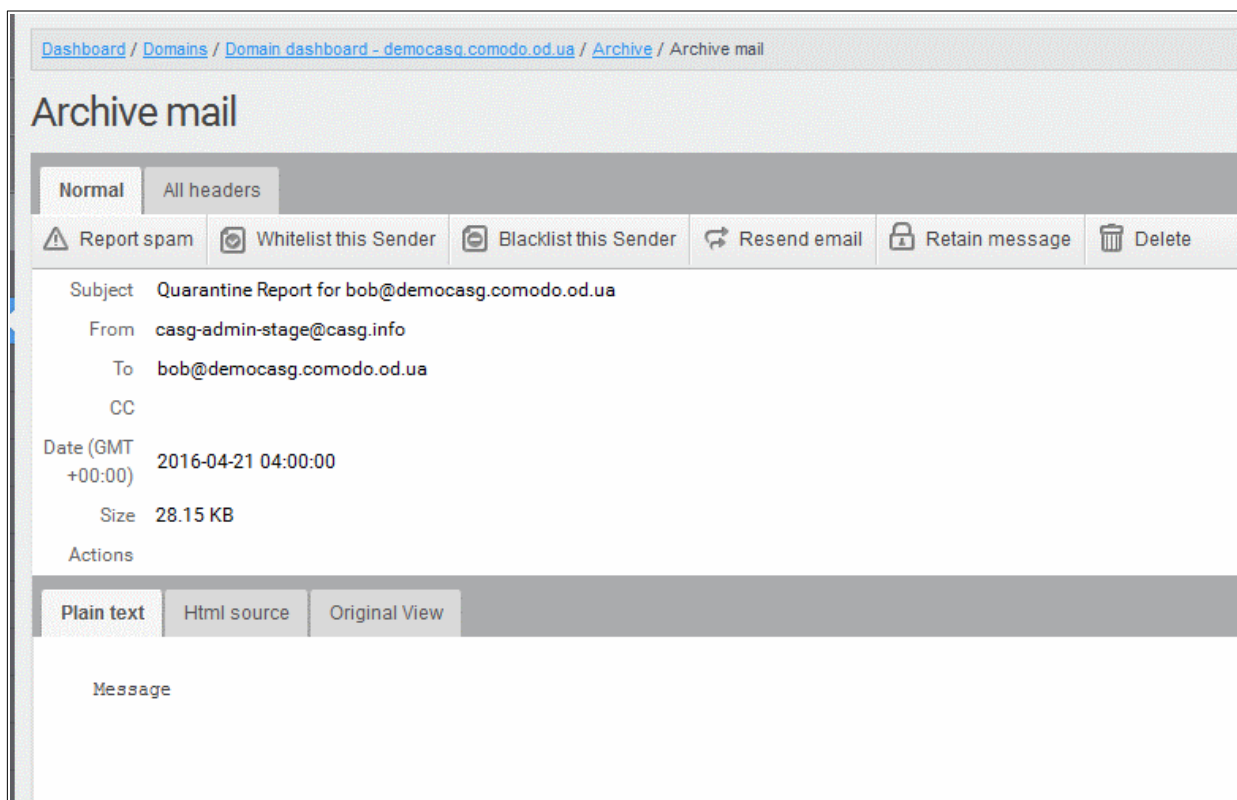
The details of the selected email will be displayed.

- Click 'All headers' to view the email headers which contain the tracking information of the mail detailing the path it has crossed before reaching the recipient. The headers give full details of the sender, route, recipient, sent date, mail type and so on and enable you to check the authenticity of the mail.

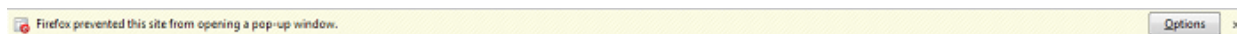
View details in a new window

- Select the mail that you want to view in the 'Archive' area
- Right-click on the email link in the subject column and select to open in a new tab or new window.

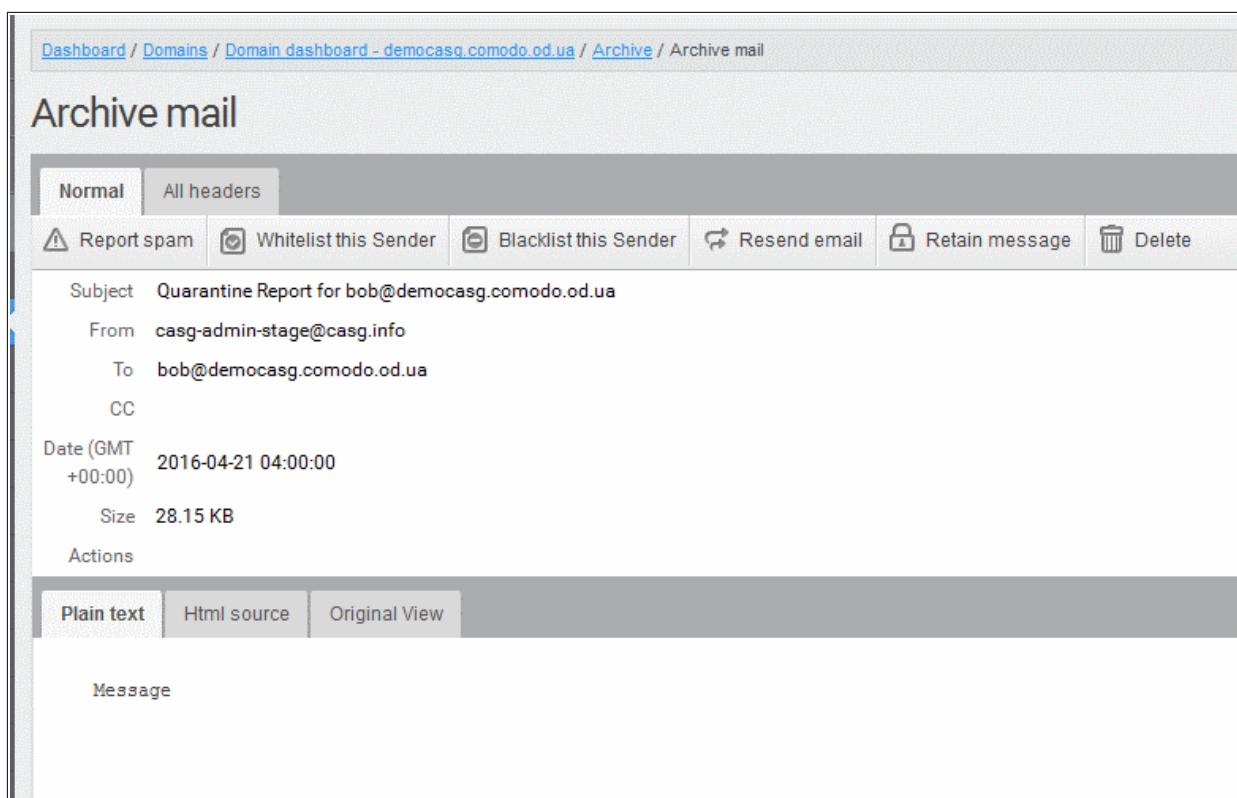




The browser may display a warning pop-up window notification. Click the 'Options' > then select 'Allow pop-ups for...' to allow to open new message in a new window. Click again 'Show message in new window'.



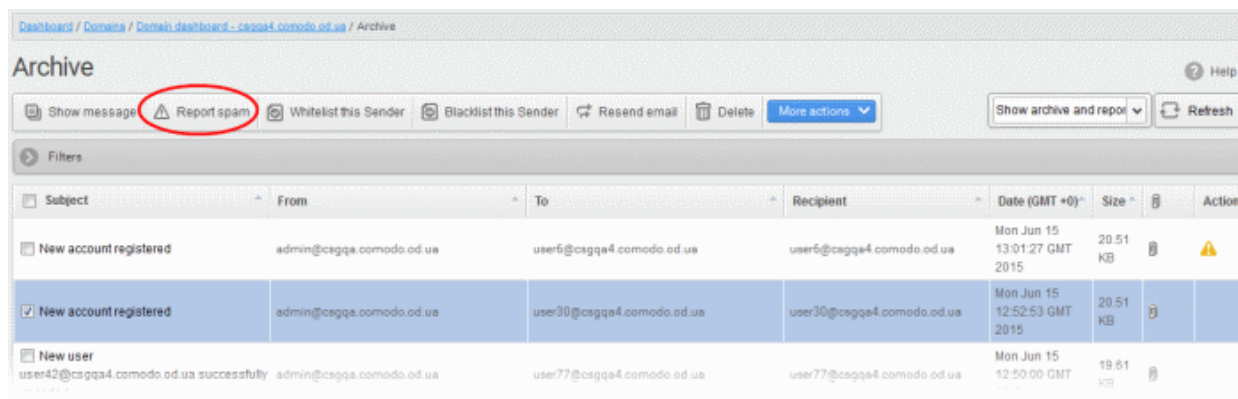
The details of the selected mail will be displayed in a new CASG window.



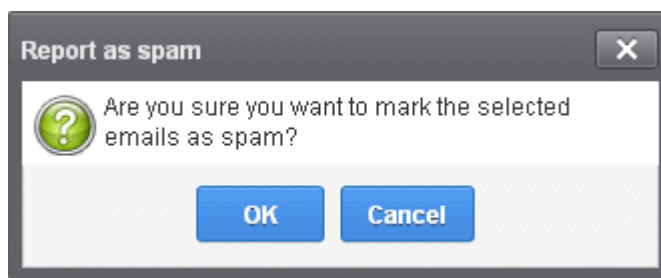
Report archived mails as spam

After viewing the details and ensuring that the selected email is a spam you can choose to report it as a spam.

- Select the mail that you want to report as spam and click 'Report spam'.



An alert will be displayed to confirm selected email as spam.



- Click 'OK' to confirm.

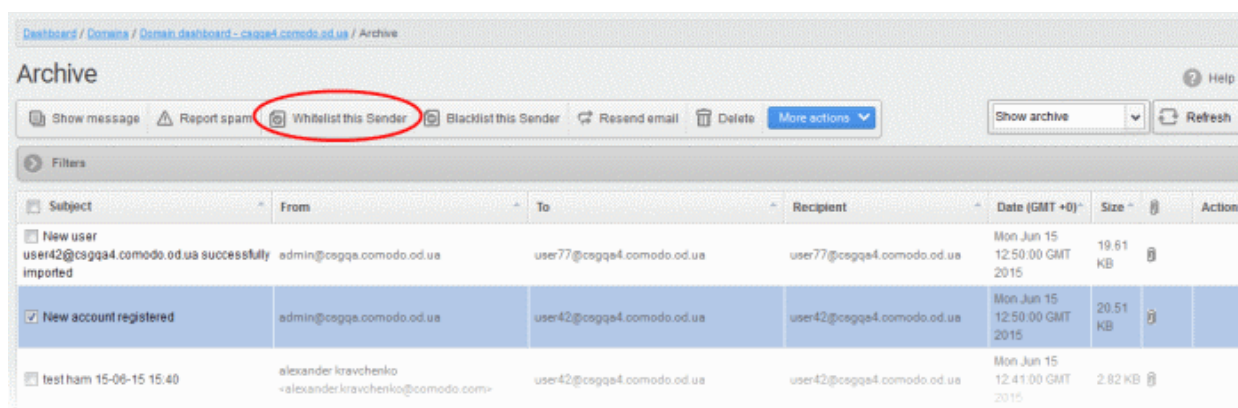


A success message will be displayed and the icon indicating the email is reported as spam will be shown under the 'Actions' column. The mail will be forwarded to the spam email address displayed in the Incoming Spam Detection Settings interface for analysis by experts. Refer to the explanation under **Incoming Spam Detection Settings** for more details.

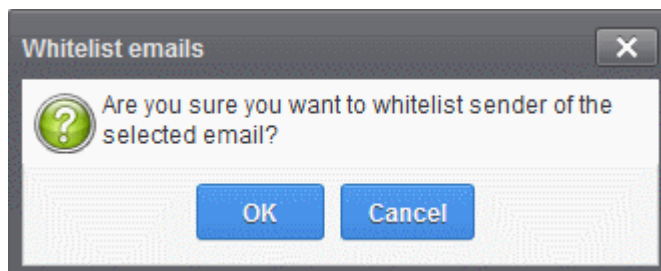
Add a sender to whitelist

Administrators can choose to add the email senders to 'Sender Whitelist' from this interface. Once added to whitelist, emails sent by these senders will not be quarantined.

- Select the mail that you want to add the sender to whitelist and then click 'Whitelist this Sender'



An alert will be displayed to confirm adding the sender to whitelist.

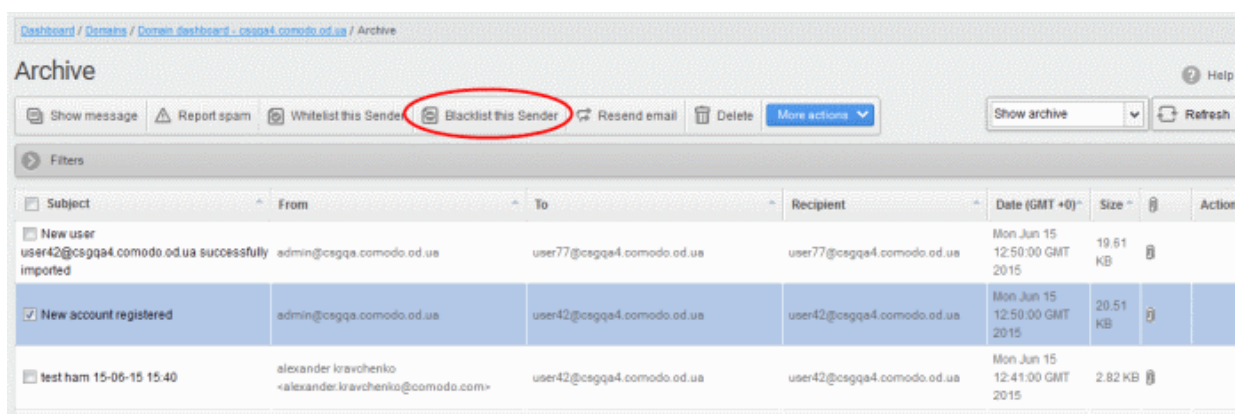


- Click 'OK' to confirm to add the sender to whitelist. Refer the section '**Sender Whitelist**' for more details.

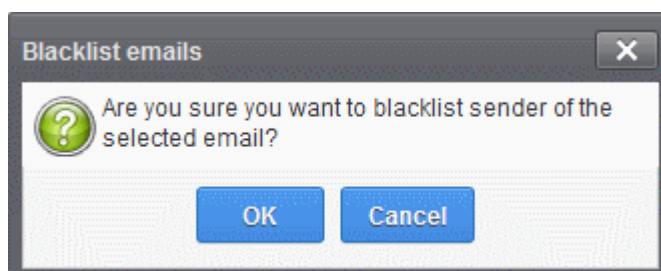
Add a sender to blacklist

Administrators can choose to add the email senders to '**Sender Blacklist**' from this interface. Once the selected senders are added to blacklist, all emails from them to the selected domain will be automatically blocked.

- Select the mail that you want to add the sender to blacklist and then click 'Blacklist this Sender'



An alert will be displayed to confirm adding the sender to blacklist.

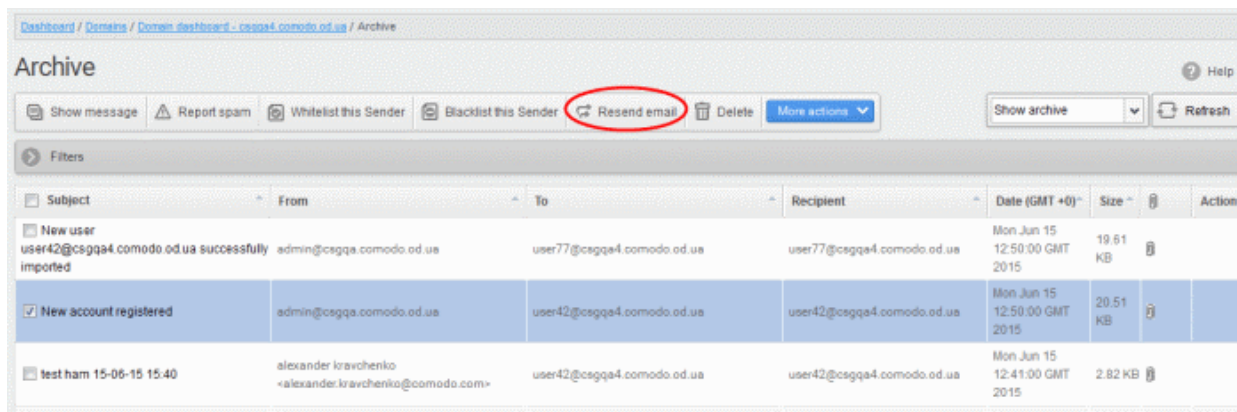


- Click 'OK' to confirm to add the sender to blacklist. Refer the section '**Sender Blacklist**' for more details.

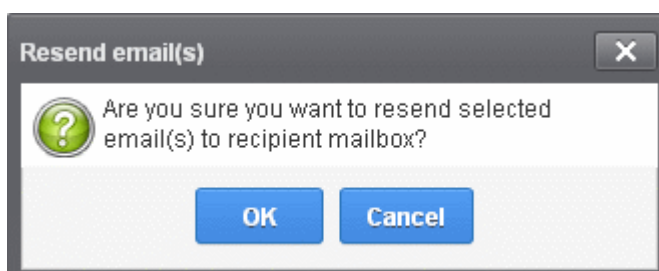
Resend emails from archive

The archived mails can be sent to the recipients if required. CASG will still retain a copy of mails in the archive even after they are sent.

- Select the mail that you want to resend and click 'Resend email'.



An alert will be displayed to confirm resending emails.



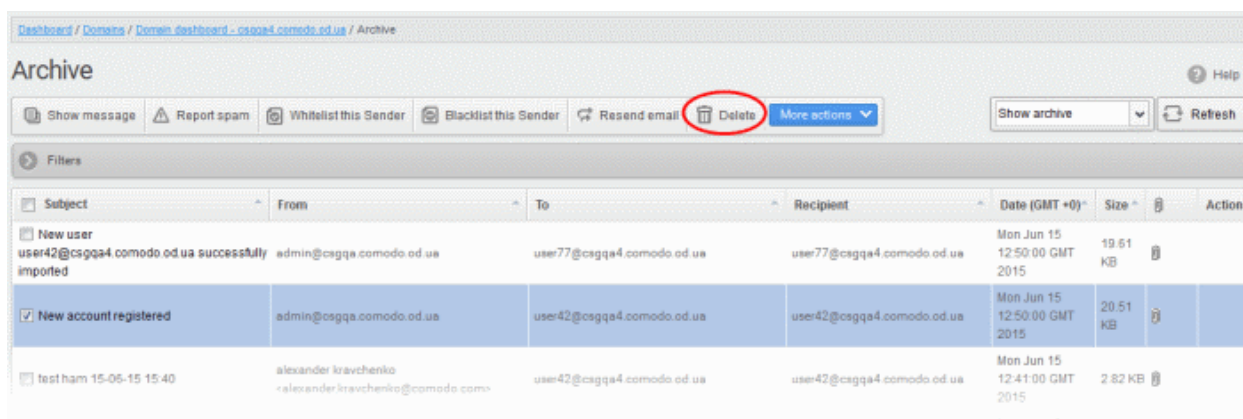
- Click 'OK' to confirm.

A success message will be displayed.

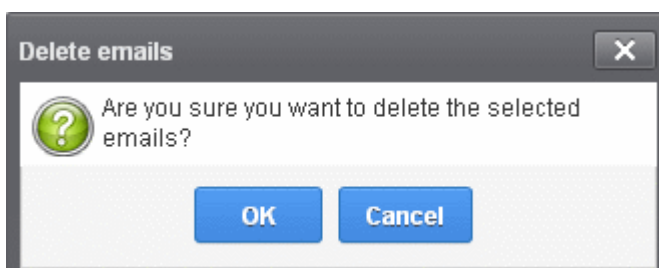


Delete archived mails

- Select the mail that you want to delete and click the 'Delete' button



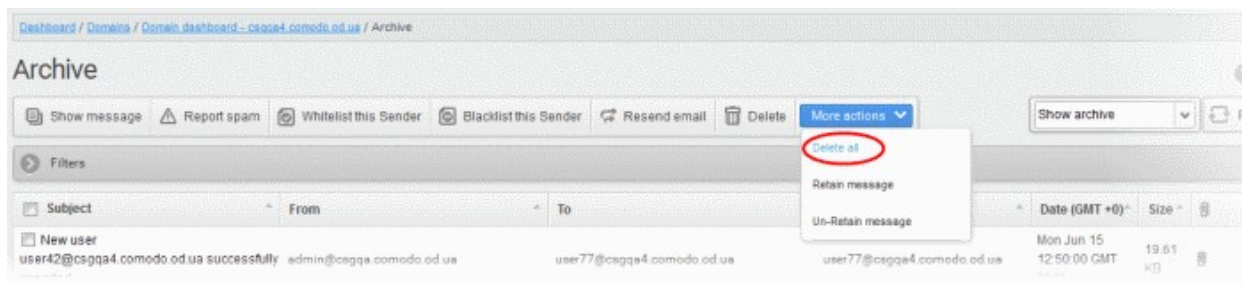
An alert will be displayed to confirm deletion.



- Click 'OK' to confirm.

The selected mail will be deleted and will no longer be in archive.

- To delete all the archived mails, click 'More actions' > 'Delete all'.

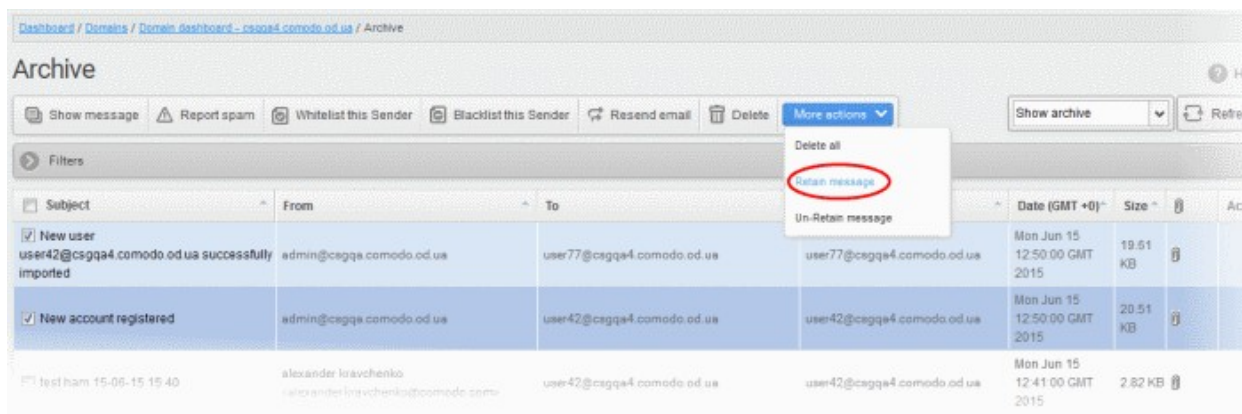


An alert will be displayed to confirm the deletion. Click 'OK' to delete all archived emails.

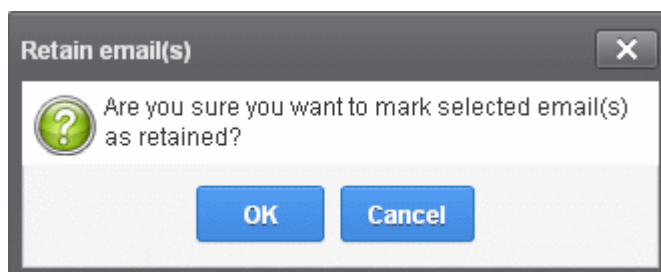
Exclude mails from auto-clean operations

CASG can be configured in the **Domain Settings** area to automatically purge emails from archive after the configured period. If administrators wants to retain email(s) from being cleared, then these mails can be marked as 'Retain message'.

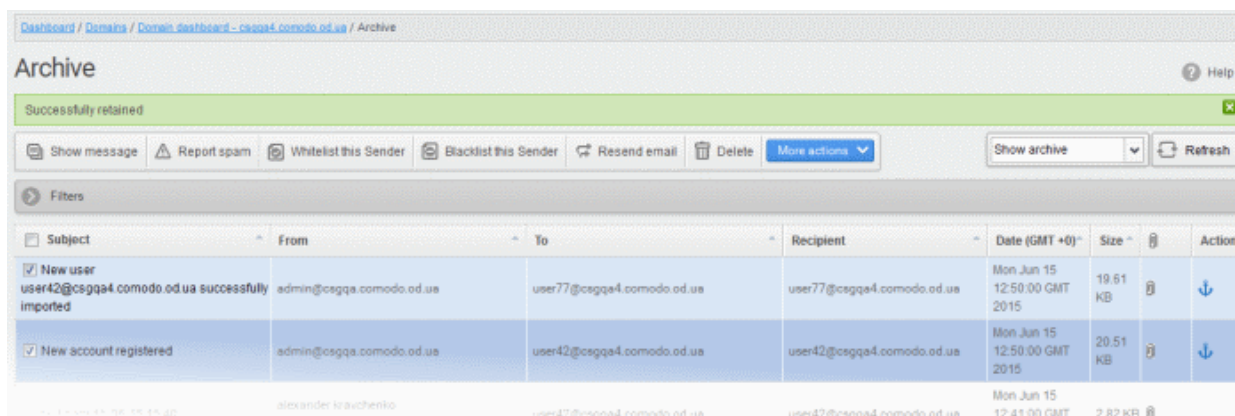
- Select the mail(s) that you want to retain and then click 'More actions' > 'Retain Message'.



An alert will be displayed to confirm retain selected email(s).

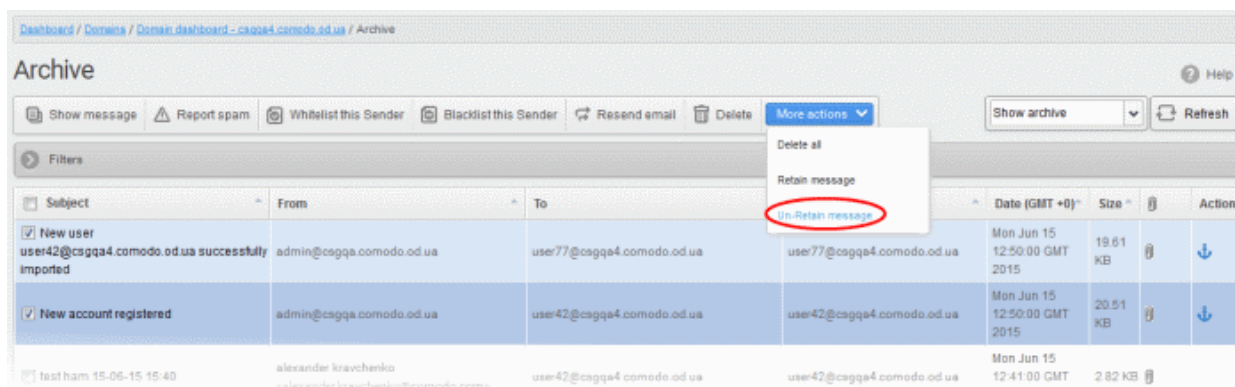


- Click 'OK' to confirm.

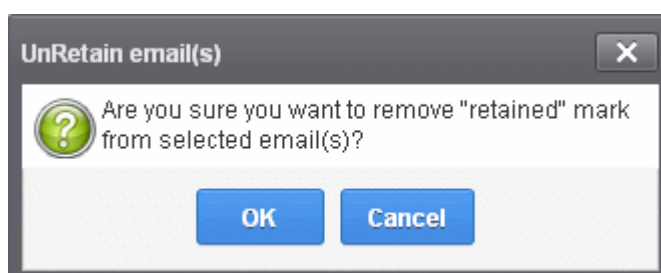


A confirmation dialog will be displayed and the retained messages are indicated by the anchor icons under the Actions column.

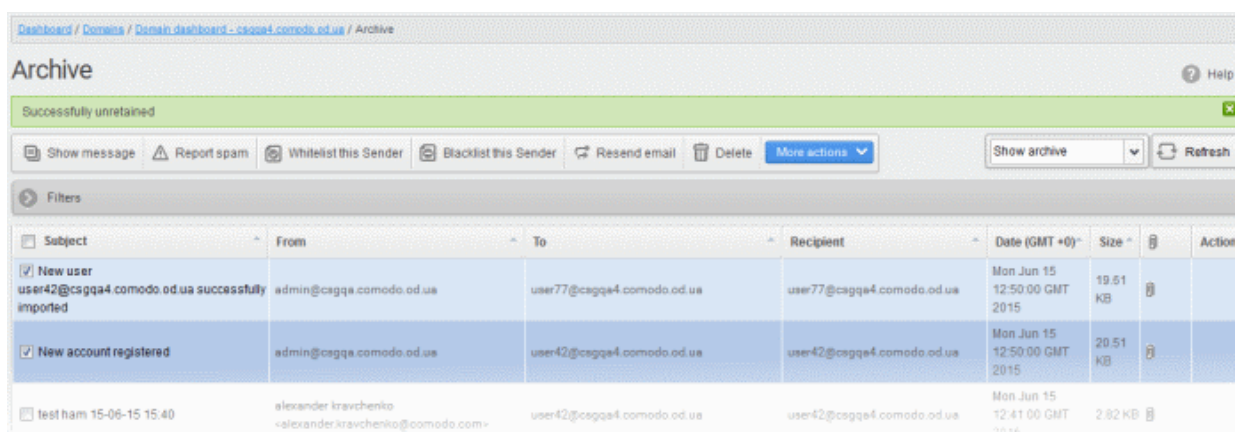
- To remove the retained status for a mail, select the retained message and then click 'More actions' > 'Un-Retain Message'.



An alert will be displayed to confirm selected email(s) from retain status.



- Click 'OK' to confirm.



A confirmation dialog will be displayed and the anchor icons under the Actions column are no longer displayed indicating their unretained status.

Incoming Spam detection settings

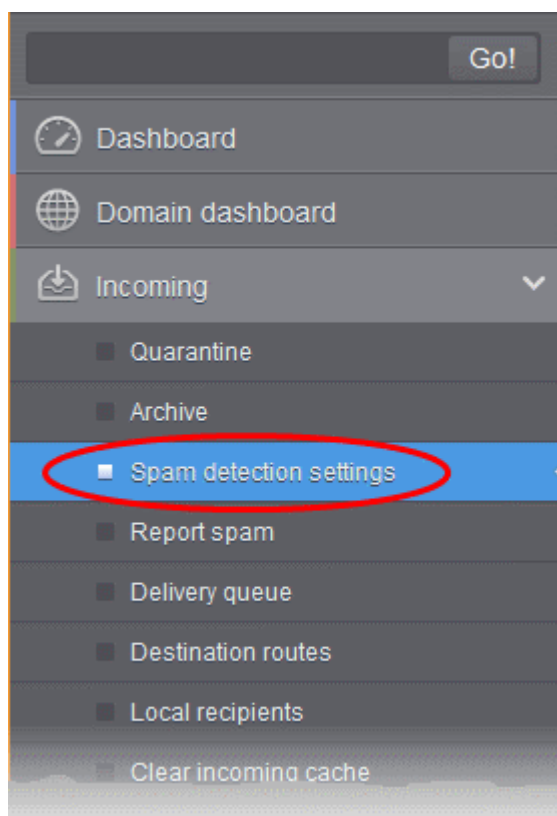
This area lets you configure the sensitivity of the spam filter, spam notation, and quarantine retention times.

- CASG runs several rules on each email as it passes through the spam filters.
- Each rule checks the mail for a specific spam attribute. The rule will assign a score to a mail based on the degree to which the mail exhibits that attribute.
- A message's total spam score depends on the weighted value of all rules combined.

For example, if you set the spam threshold to 0.33, any mail that has a score higher than 0.33 will be treated as spam and quarantined. The higher the threshold, the more likely that some spam messages may get delivered. The maximum possible threshold is 1. We advise you to test settings for a week to arrive at the best setting for your company.

Configure incoming spam detection

- Click 'Incoming' on the left and choose 'Spam detection Settings'



This opens the spam detection interface for the selected domain:

Dashboard / Domains / Domain_dashboard - ivascala.nl / Incoming Spam detection settings

Incoming Spam detection settings Help

Quarantine enabled: <input checked="" type="checkbox"/>	Days saved: 30
Spam threshold: 0.45	Spam notation: []
Probable spam threshold: 0.1	Probable spam notation: [Probable Spam]
Quarantine response: Accepted	Spam email: spam@antispamgateway.com
Notify user about new quarantine message: <input type="checkbox"/>	Suspicious attachment notation: [Suspicious attachment]
Comodo RBL: Quarantine message	Blacklist action: Reject message
Detect multiple extension attachments: <input type="checkbox"/>	Enable Containment: <input type="checkbox"/>
Remove multiple extension attachments: <input type="checkbox"/>	Reject emails contains credit card number: <input type="checkbox"/>

Save Reset to default

- **Quarantine enabled:**
 - **Enabled** - Mail identified as spam is quarantined.
 - **Disabled** - Spam is not quarantined but is delivered with a modified subject line. You can set the text which is appended to the subject line in the **Probable Spam notation / Spam Notation** fields.
 - Messages identified as 'probable spam' are always sent to the recipient, and not quarantined, even if this option is enabled. See '**Probable spam threshold setting**' to set the sensitivity.
- **Days saved** - Enter the number of days that you want mails to be retained in quarantine. The maximum number of days that can be set is 9999. Quarantined mails that are not checked, released or deleted within the stipulated days will be automatically deleted from quarantine.
- **Spam threshold** - Enter any value between 0.1 and 1.0. All mails with a score above that value are classed as spam and quarantined as explained **above**. Please note this value should be always higher than 'Probable spam threshold' value.
- **Spam notation** - The prefix that will be appended to the subject line of all 'Spam' emails sent to users. For example, "<Spam> Order two Rolex watches and get a free carton of Viagra" - where <Spam> is the text entered in the 'Spam notation' field. Note - this only applies IF quarantine has been disabled (i.e. If the 'Quarantine Enabled' box is not checked).
- **Probable spam threshold** - Enter any value between 0.0 and the value entered in **Spam threshold** field. All mails that are having a score value above that is set in this field will be identified as unsure mails and will be delivered to recipients with the subject line as set in the **Probable Spam notation / Spam Notation** field.
- **Probable spam notation** - The prefix that will be appended to the subject line of all 'probable spam' emails sent to users. For example, "<Potentially Spam> Cheap deals on Dell computers" - where <Potentially Spam> is the text entered in the 'Probable spam notation' field.
- **Quarantine response** - Choose the response to be sent by CASG to the SMTP server that delivered a message in the event that a mail is identified as spam.
- Note - If you have enabled quarantine functionality, then spam/malicious mail will be quarantined (and not delivered to the recipient) regardless of your choice here. These options merely determine what message CASG will send back to the SMTP mail server. The available options are:
 - **Rejected** - Will inform the SMTP server that the email has been rejected by CASG and placed in quarantine.
 - **Accepted** - The email has passed the CASG spam filters and detected as a spam will be placed in quarantine in silent mode.
- **Spam email** - Displays the email address to which the mails reported as spam from the 'Report Spam' interface and the 'Archive' interface will be forwarded. By default, mails reported as spam

by the administrators will be forwarded to spam@antispamgateway.comodo.com for analysis by experts at Comodo. Once a reported mail is confirmed as spam, Comodo will update its mail filters to quarantine similar mails in future. Refer to the explanations under **Manage Archived Mails** and **Report Spam** for more details on forwarding the suspicious mails for analysis.

- **Notify user about new quarantine message** - Select this option if you wish CASG to send a notification email to the intended recipient, if a spam email addressed to the recipient is intercepted by CASG and moved to Quarantine. The notification email will contain a link to the email and a link for the user to login to the CASG User interface.
 - The recipient will be able to click the link to directly read the email, without logging-in to CASG. The lifetime of the link is one day. If the user has not clicked the link within a day, the link will expire.
 - If the user needs to respond to or delete the quarantined email, the user can click the next link to login to CASG, view their quarantined mails and carry out their desired actions
- **Suspicious attachment notation** - The prefix that will be appended to the subject line of all mails identified with suspicious attachments like malware and macros and forwarded to the recipient or to a different email address, as configured in the Domain Rules. Refer to the explanation under **Rules** in the section **Domain Rules** for more details. For example, "[Suspicious attachment] Your lucky draw" - where [Suspicious attachment] is the text entered in the 'Suspicious attachment notation' field.
- **Comodo RBL** - Comodo's Real-time Blackhole List (RBL) is a blacklist of locations which are known to send spam. This list is continuously updated by Comodo.
 - **Quarantine message** - If the IP address of the message sender is in the RBL, then the incoming email will be quarantined.
 - **Reject message** - If the IP address of the message sender is in the RBL, then the incoming email will be rejected.
 - **Disabled** - CASG filters will not check Comodo RBL.
- **Blacklist action** – Specify the action if CASG detects messages from blacklisted sources such as blacklisted domains, senders, users and recipients.
 - **Reject message** – If enabled, incoming emails from blacklisted sources are rejected.
 - **Quarantine message** – If enabled, incoming emails from blacklisted sources are placed in quarantine. Response to the sender depends on the '**Quarantine response**' settings.
- **Enable Containment** – Containment is a security technology whereby email attachments with an 'unknown' trust rating are run inside a secure, sandbox environment. Note – This feature is available for EU customers. For US customers, we are in the process of migrating to a new platform. Once the process is complete, this feature will be available for US customers also.
 - Files in containment are run with heavily restricted privileges. They cannot access other processes, cannot access important system files, and cannot access user data.
 - This setting will contain unknown attachments of the following file types
- .exe, .pdf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .zip, .rar, .tar.gz, tar.bz2.
 - From the user's point-of-view, the attachment opens and runs as normal on their computer. This provides a groundbreaking combination of high security with no loss of usability.
 - Background - Each email attachment is checked by our filters and awarded a trust rating. This can be 'Safe' (the file is on our whitelist), 'Malware' (the file is on our blacklist), or 'Unknown' (the file does not yet have a trust rating).
 - Because unknown files could be malware, we run them in the container on the endpoint while we test them to establish their safety. If the tests find the file is safe then it is released from containment. If the tests find the file is harmful then it is quarantined.
 - You can disable this setting for particular users if required. See '**User Account Management**' for more info on this.
- **Detect multiple extension attachments** – Files of more than one file type or extensions. For example, 'file_name.doc.exe'. If enabled, CASG quarantines messages with these types of attachments.
- **Remove multiple extension attachments** – If enabled, message is delivered to the recipient without the attachment.
- **Reject emails contains credit card number** - If enabled, emails that contain credit card numbers are rejected. Credit card numbers have a certain structure that CASG filters can recognize, so

emails containing random numbers are not rejected.

- Click 'Save' for your settings to take effect.
- Click 'Reset to default' to undo any changes.

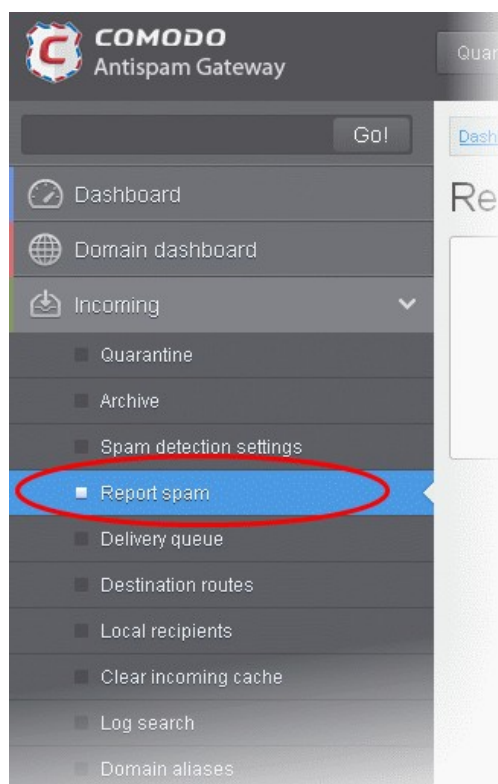
Report Spam

The 'Report Spam' feature allows you to upload and submit suspected junk emails that have got through our spam filters. Comodo will analyze reported mails and, if we confirm them as spam, will update our filters to quarantine similar mails in future. CASG accepts a range of different mail formats including .eml and .msg.

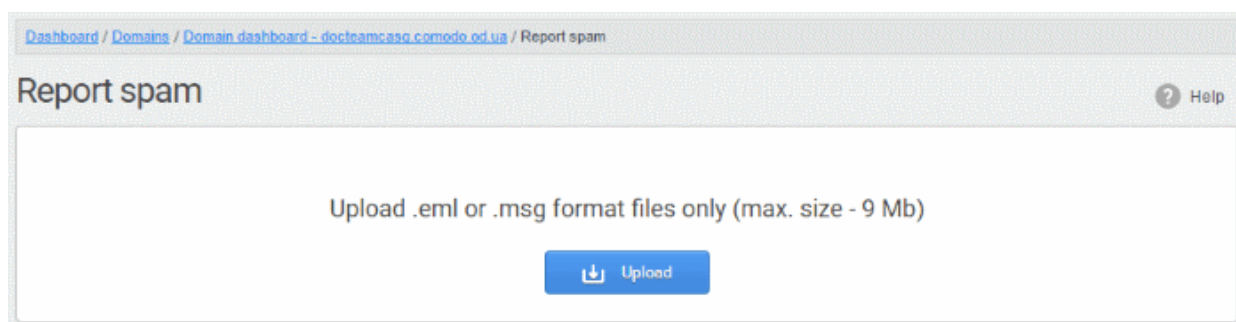
Users can also report spam by sending it to spam@antispamgateway.comodo.com. Add the spam email as an attachment in .eml or .msg format.

Report a spam mail

- Click 'Incoming' on the left then select 'Report spam'.



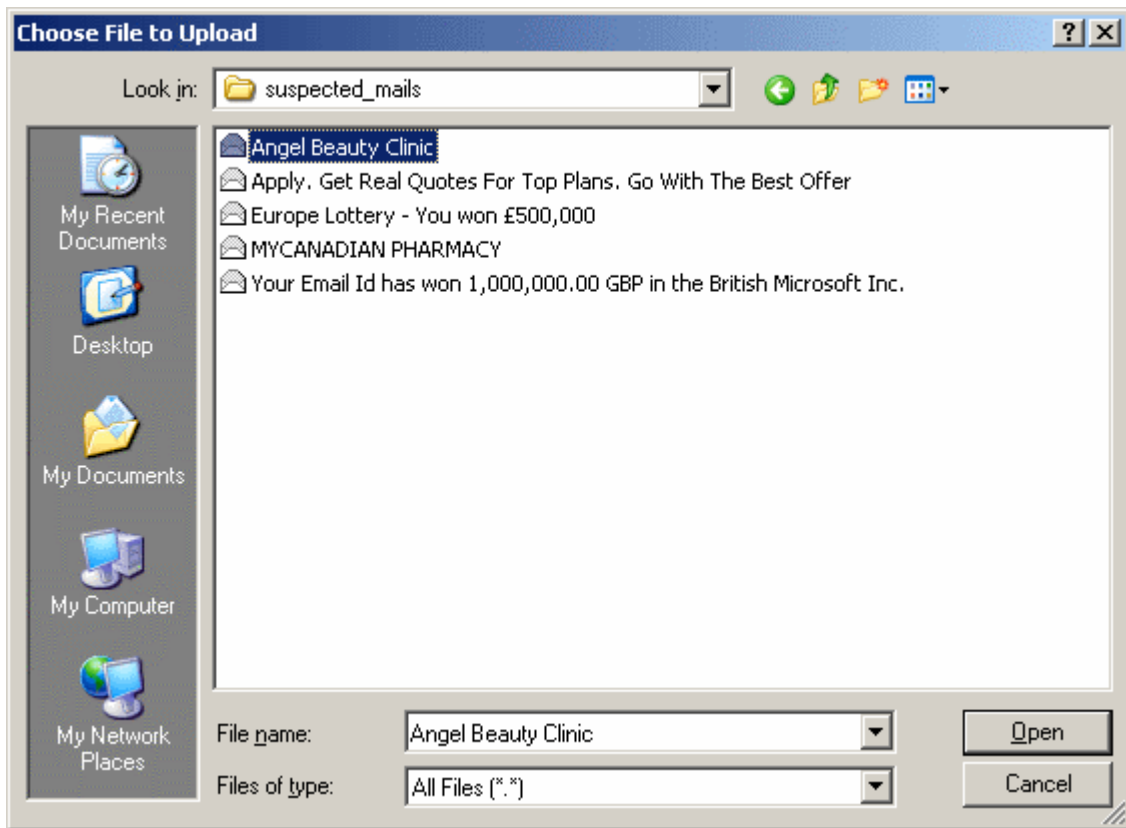
The 'Report Spam' interface will open:



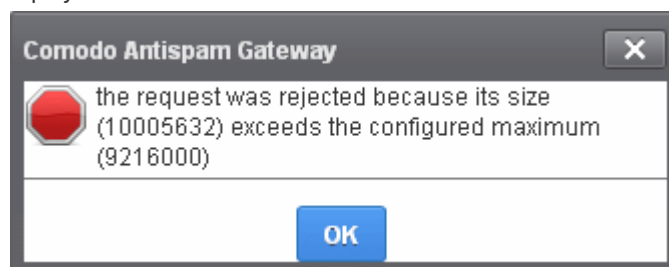
- Click the 'Upload' button

Navigate to the location where the suspected email(s) is/are stored in your system. Select the mail that you want to

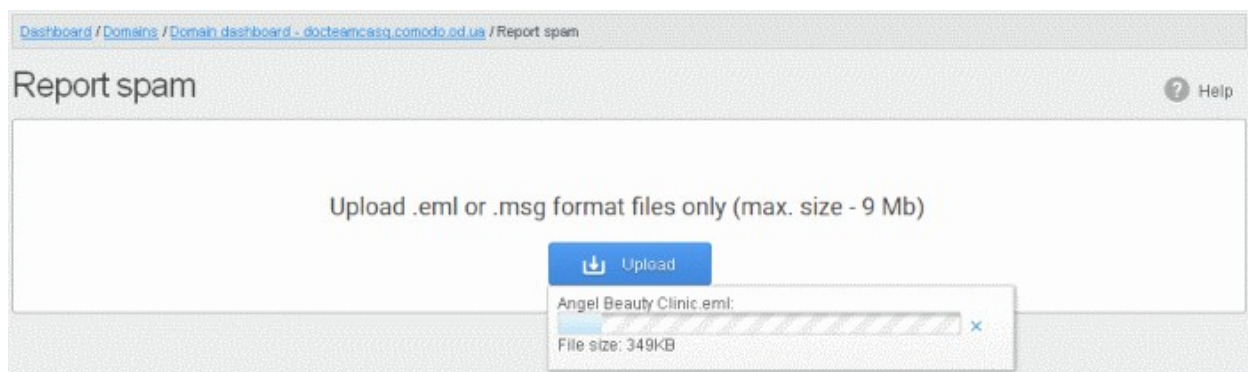
report as spam and click 'Open'. The maximum size of the file that can be uploaded is 9 MB.



Note: Make sure to upload the file in email format only and size should not exceed 9 MB. Otherwise, the following warning message will be displayed.



The mail will be processed for uploading...



... and success message will be displayed.



- Click the  button to close the message.

Delivery Queue

CASG delivers incoming emails which pass its filters directly to the destination server(s). Whenever a destination is unavailable, all filtered mails are queued on the CASG servers for delivery at a later time.

- Emails that are permanently rejected by the destination server with a 5xx error code will not be queued and are rejected by the CASG system.

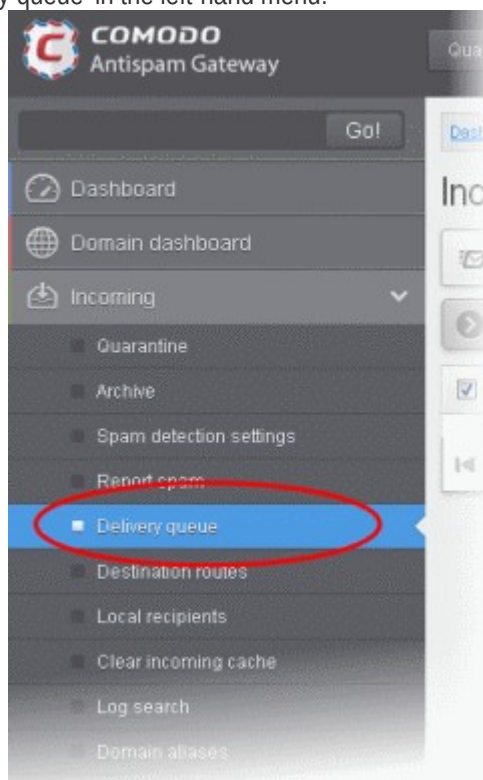
Queued messages are automatically retried for delivery for a period of time that is set in 'Maximum days to retry' in **domain settings** (for example, 4 days). The automatic retry schedule is given below:

- During the first two hours, queued messages are retried for delivery at a fixed interval of 15 minutes.
- During the next 14 hours, queued messages are retried for delivery at a variable time interval starting from 15 minutes and multiplied by 1.5 with each attempted delivery. For example, after the first 15 minutes, the subsequent attempts will be after 22.5 minutes, 34 minutes and so on.
- From 16 hours to 4 days after the delivery failure, queued messages are retried for delivery at a fixed interval of every 6 hours.
- After 4 days, all queued messages will be bounced to the respective senders. The messages will be frozen if the bounce cannot be delivered immediately and retried for delivery at a fixed time interval of 3 days for the first 21 days. At the end of this period, delivery of messages will have failed permanently.

The delivery queue area lets you view queued mails, configure queue alerts and analyze delivery diagnostics.

Manage the delivery queue

- Click 'Incoming' > 'Delivery queue' in the left-hand menu:



The 'Incoming Delivery Queue' interface of the selected domain will open:

Dashboard / Domains / Domain_dashboard_-_docteamcas.comodo.ed.us / Incoming delivery queue

Incoming delivery queue

Show headers
 Delivery diagnostic
 Alerts

Filters

<input type="checkbox"/> Queue id	In queue	Sender	Recipient	Message size	Subject	Last action	Server name	Delay reasons
<input type="checkbox"/> 3jRwrD24WTz12LF	52m	admin@antispamg	john@docteamcas	21577	New account registered	message_queue_ch	mta3.prod.casg	john@docteamcas : connect to 91.196.95.19[91.19] Connection refused
<input type="checkbox"/> 3jRwrZ1qfHzHnm5	52m	admin@antispamg	demo2@docteamc	21585	New account registered	message_queue_ch	mta1.prod.casg	demo2@docteamc : connect to 91.196.95.19[91.19] Connection refused
<input type="checkbox"/> 3jRwrY6XRgz12Lsf	52m	admin@antispamg	bob@docteamcasg	21566	New account registered	message_queue_ch	mta3.prod.casg	bob@docteamcasg : connect to 91.196.95.19[91.19] Connection refused
<input type="checkbox"/> 3jRwrY0Y1zHnly	52m	admin@antispamg	demo1@docteamc	21586	New account registered	message_queue_ch	mta1.prod.casg	demo1@docteamc : connect to 91.196.95.19[91.19] Connection refused
<input type="checkbox"/> 3jRwrH6LYpzHnn6	1h 41m	admin@antispamg	john@docteamcas	21576	New account registered	message_queue_ch	mta1.prod.casg	john@docteamcas : connect to 91.196.95.19[91.19] Connection refused

- Click any column heading to sort entries in ascending/descending order.

Use the filter option to search queued emails

- Click anywhere on the 'Filters' stripe to open the filters area.

Dashboard / Domains / Domain dashboard - docteam.das.comodo.od.ua / Incoming delivery queue

Incoming delivery queue

Help

Show headers Delivery diagnostic Alerts Refresh

Filters

+ Queue id contains

Queue name contains

Sender contains

Message size less than 0

Recipient contains

Server name contains

Apply filter

<input checked="" type="checkbox"/> Queue id	In queue	Sender	Recipient	Message size	Subject	Last action	Server name	Delay reasons
No items found								


1 / 1 Per page 15

- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

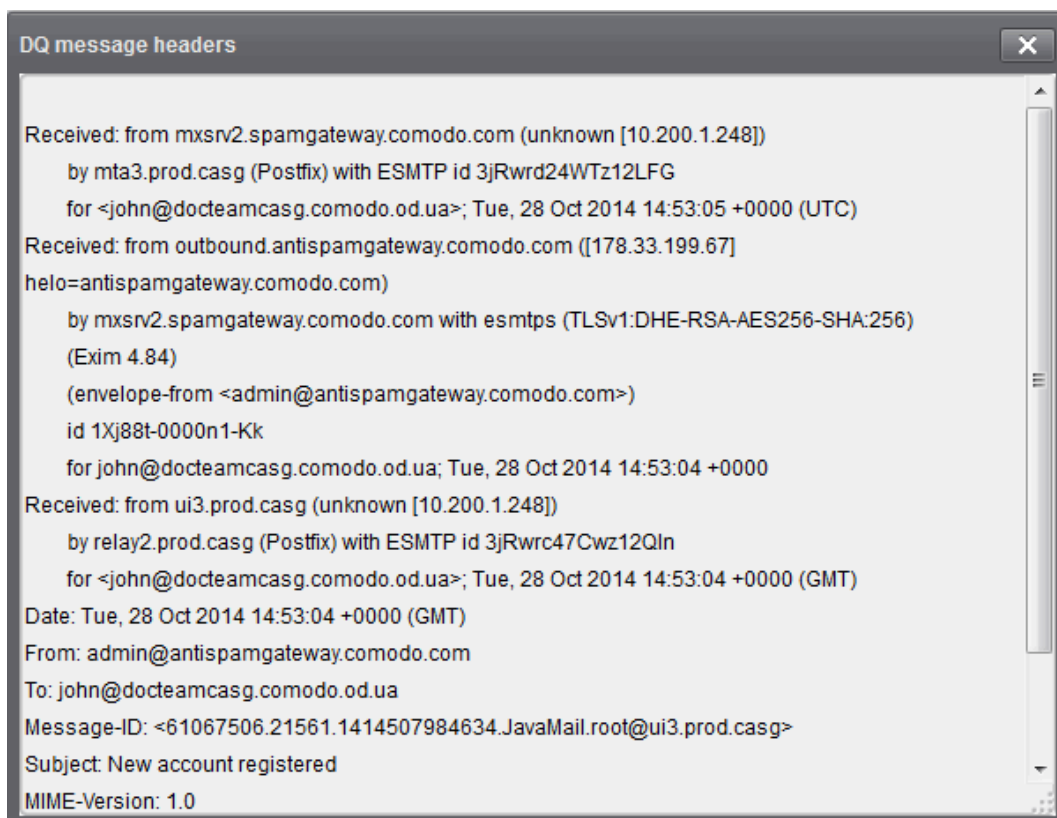
- **Queue ID:** Type a queue ID in the text box (column 3) and select a condition in column 2.
- **Queue name:** Type a queue name in the text box (column 3) and select a condition in column 2.
- **Sender:** Enter the email address of the sender in the text box (column 3) and select a condition in column 2.
- **Recipient** – Enter the email address of the recipient in the text box (column 3) and select a condition in column 2.
- **Message size:** Select the email size in column 3 and select a condition in column 2.
- **Subject:** Enter the email subject in the text box (column 3) and select a condition in column 2.
- **Last action:** Enter the latest action in the text box (column 3) and select a condition in column 2.
- **Server name:** Enter the email server name or IP in the text box (column 3) and select a condition in column 2.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

You can add multiple filters to the same search by clicking .

View headers of queued emails

- Select an email from the delivery queue and click the 'Show headers' button.

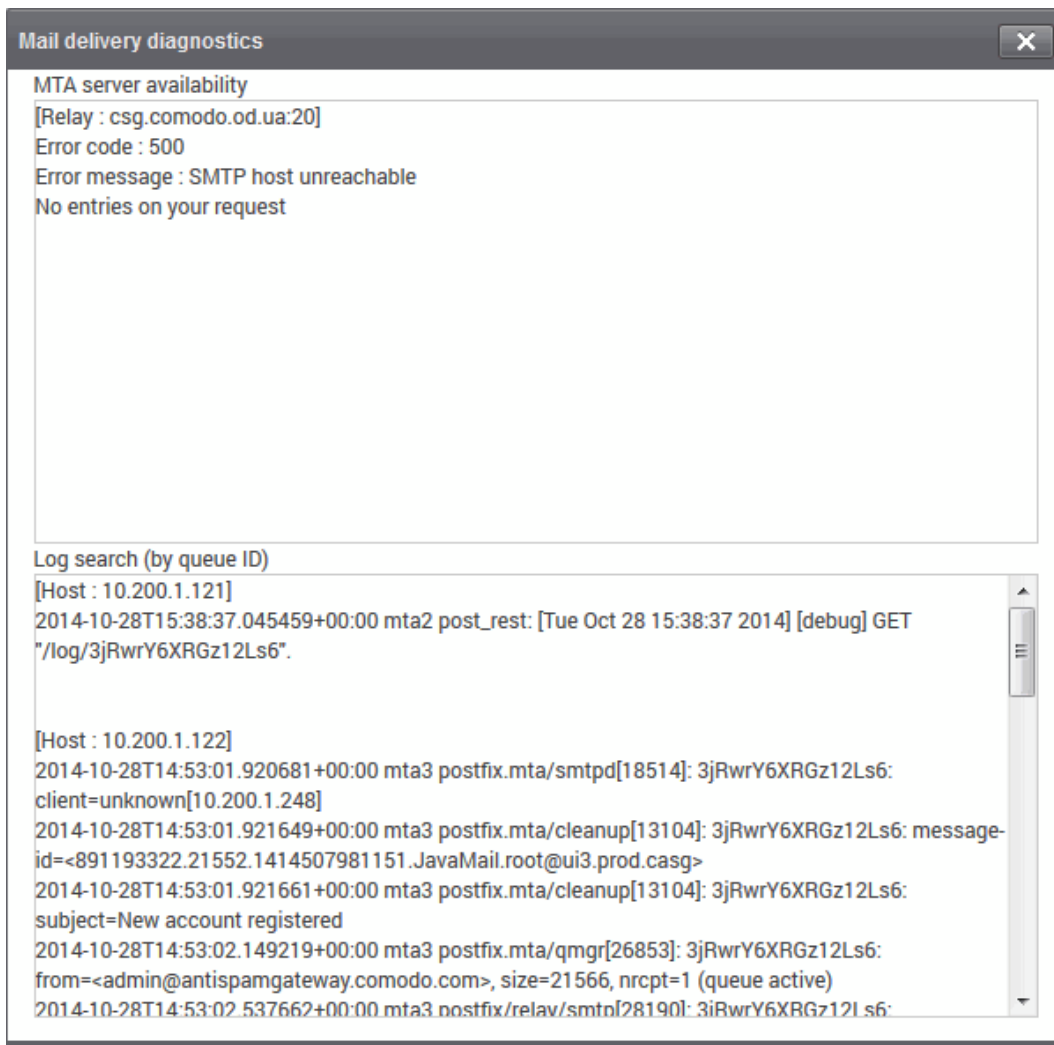


```
DQ message headers
Received: from mxsrv2.spamgateway.comodo.com (unknown [10.200.1.248])
  by mta3.prod.casg (Postfix) with ESMTP id 3jRwrd24WTz12LFG
  for <john@docteamcasg.comodo.od.ua>; Tue, 28 Oct 2014 14:53:05 +0000 (UTC)
Received: from outbound.antispamgateway.comodo.com ([178.33.199.67]
  helo=antispamgateway.comodo.com)
  by mxsrv2.spamgateway.comodo.com with esmtps (TLSv1:DHE-RSA-AES256-SHA:256)
  (Exim 4.84)
  (envelope-from <admin@antispamgateway.comodo.com>)
  id 1Xj88t-0000n1-Kk
  for john@docteamcasg.comodo.od.ua; Tue, 28 Oct 2014 14:53:04 +0000
Received: from ui3.prod.casg (unknown [10.200.1.248])
  by relay2.prod.casg (Postfix) with ESMTP id 3jRwrc47Cwz12Qln
  for <john@docteamcasg.comodo.od.ua>; Tue, 28 Oct 2014 14:53:04 +0000 (GMT)
Date: Tue, 28 Oct 2014 14:53:04 +0000 (GMT)
From: admin@antispamgateway.comodo.com
To: john@docteamcasg.comodo.od.ua
Message-ID: <61067506.21561.1414507984634.JavaMail.root@ui3.prod.casg>
Subject: New account registered
MIME-Version: 1.0
```

View Diagnostics

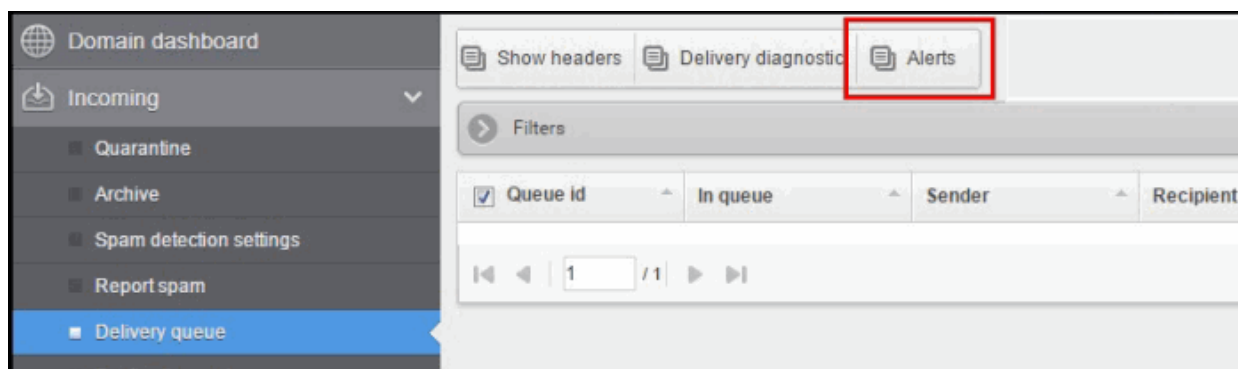
Delivery diagnostics allow mail server admins to inspect the reasons why a mail did not send correctly. These diagnostics are also useful when working with Comodo support on an issue.

- Select an email from the delivery queue then click the 'Delivery Diagnostic' button:



Configure Delivery Queue Alerts

The 'Alerts' feature lets you configure notification emails to be sent if there is a delivery delay. You will need to allow the alerting server to send you these alerts, so please add mxsrv10.antispamgateway.comodo.com [178.255.87.30] to your firewall/transport rules if necessary.



Send email alert to: Enter one or more email addresses as alert recipients.

You can specify 2 possible criteria that will trigger notifications:

- **If queue contains more than 'n' items:** CASG will send a notification mail if the number of queued mails reaches or exceeds the number specified in this field
- **If email remains in the queue for more than n hour(s):** CASG will send a notification mail when the oldest mail in the queue exceeds the age you specify (max age = 72 hours).

If you select both criteria, you will receive separate notifications for each trigger. If you uncheck both boxes, notifications will be canceled.

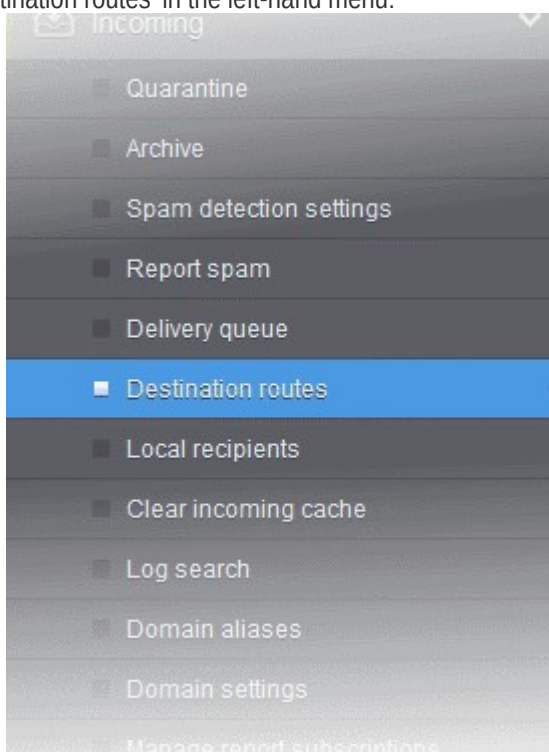
Alert frequency determines how often you will receive delivery delay notifications. Possible values are between 5-360 minutes.

Destination Routes

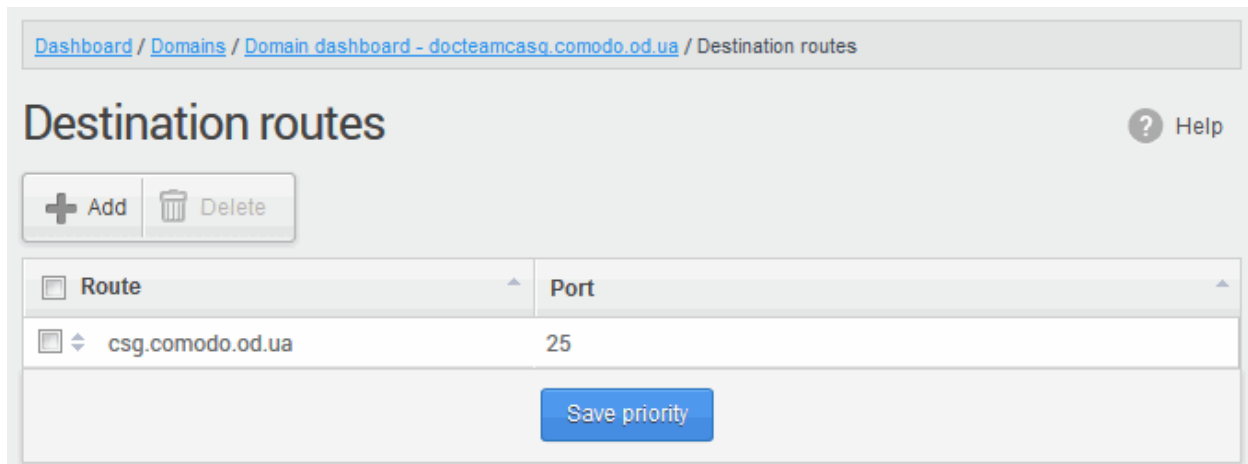
- CASG delivers incoming mail to the destination server you specify. You can also specify alternative routes which CASG will use if there is a problem with the primary route.
- Admins with appropriate permissions can add alternative routes in the **add** and **edit** domain interfaces.

Add alternative destination routes

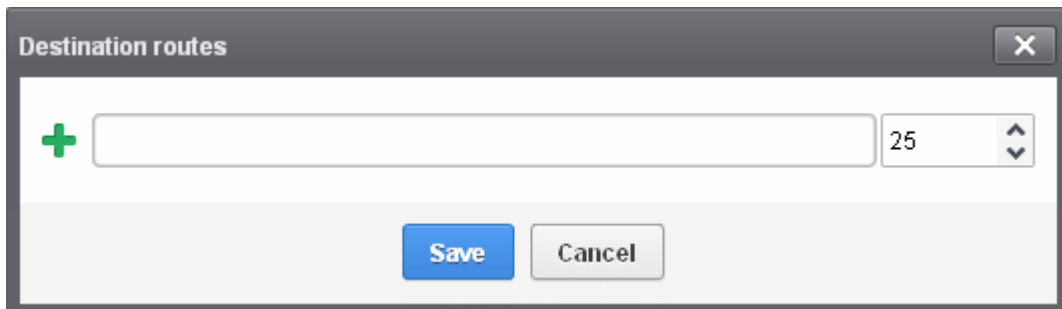
- Click 'Incoming' > 'Destination routes' in the left-hand menu:



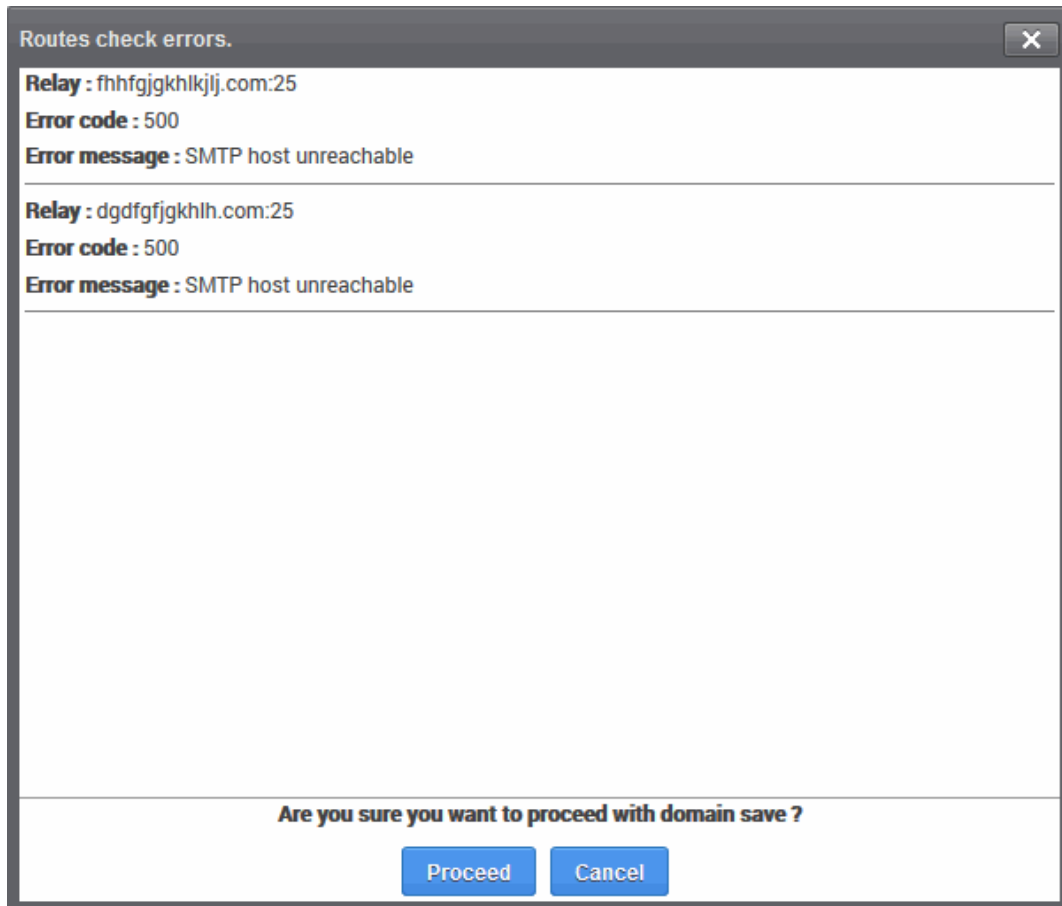
This will open the destination routes screen for the selected domain:



- Click the 'Add' button

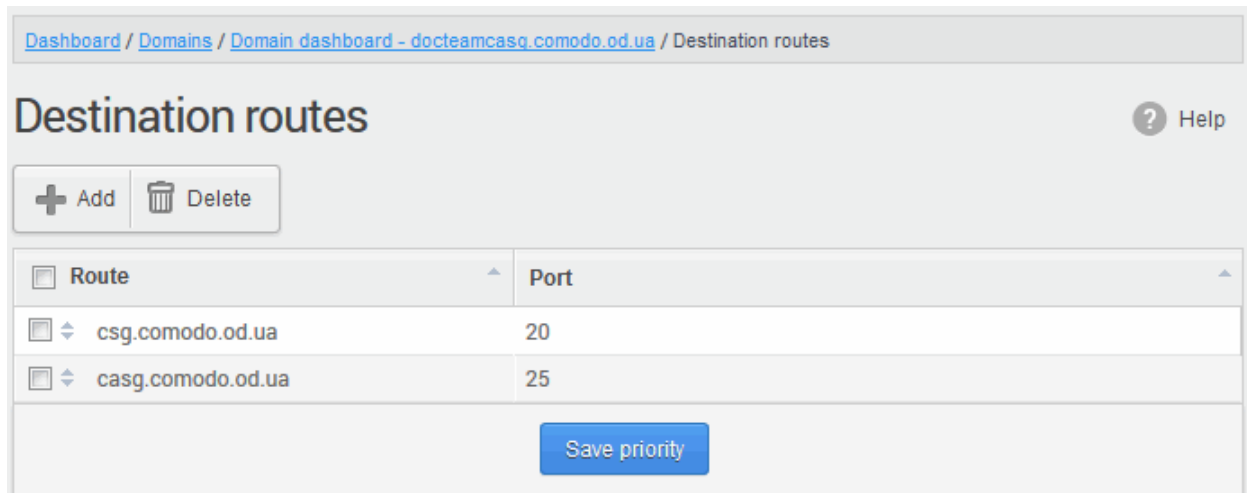


- Enter the alternative destination route (domain, IP or hostname of the SMTP server) then click 'Save'.
- CASG will test the route you enter to ensure it is valid:

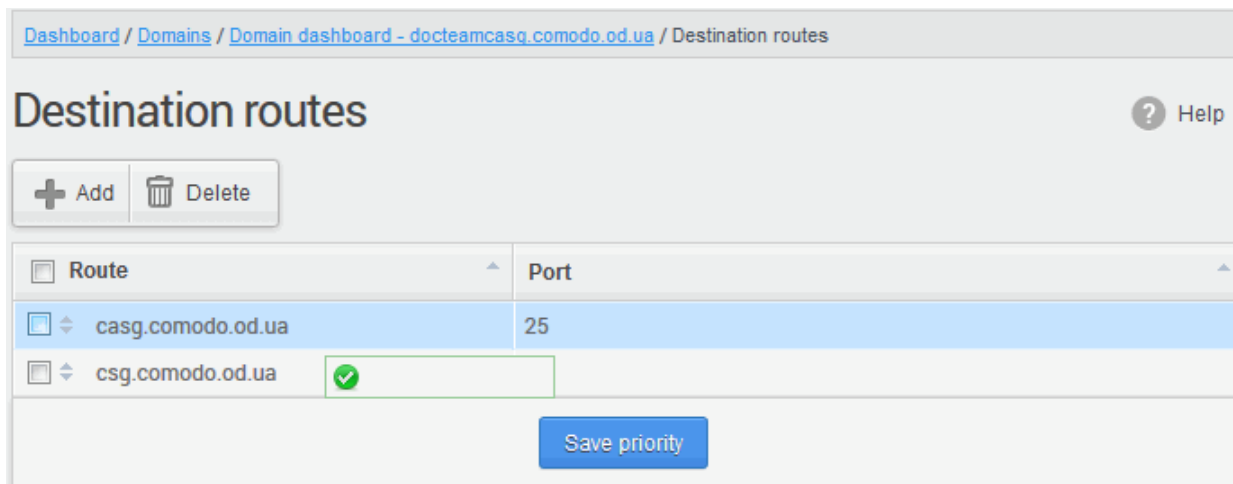


- Click 'Proceed' to save the route.

The new route is added as follows:



- Click **+** to add more alternative routes.
- CASG prioritizes the route at the top of the list, then works its way down if that route fails.
- You can re-prioritize routes by dragging and dropping them in the list.



The screenshot shows the 'Destination routes' configuration page in the Comodo Antispam Gateway administrator interface. The breadcrumb trail at the top reads: Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Destination routes. The page title is 'Destination routes' with a 'Help' icon. Below the title are 'Add' and 'Delete' buttons. A table with two columns, 'Route' and 'Port', contains two entries for 'casg.comodo.od.ua'. The first entry has a port of '25'. The second entry has a green checkmark in the 'Route' column. A 'Save priority' button is located below the table.

Route	Port
casg.comodo.od.ua	25
casg.comodo.od.ua	

- Click the 'Save priority' button to confirm the changes.

Local Recipients

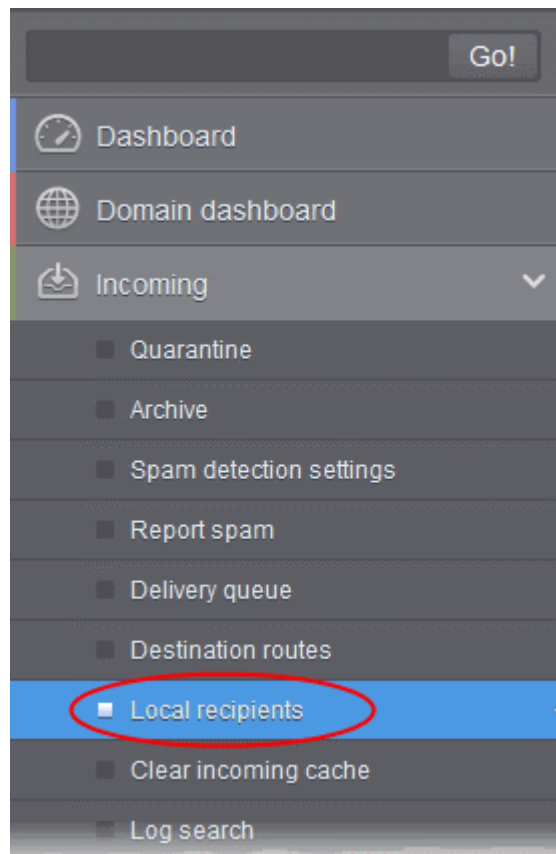
CASG can perform cached recipient call-outs to check whether recipient email addresses actually exist at the destination mail servers.

- You can configure CASG to accept mails to valid email accounts in the destination server by enabling the 'Local Recipients' feature.

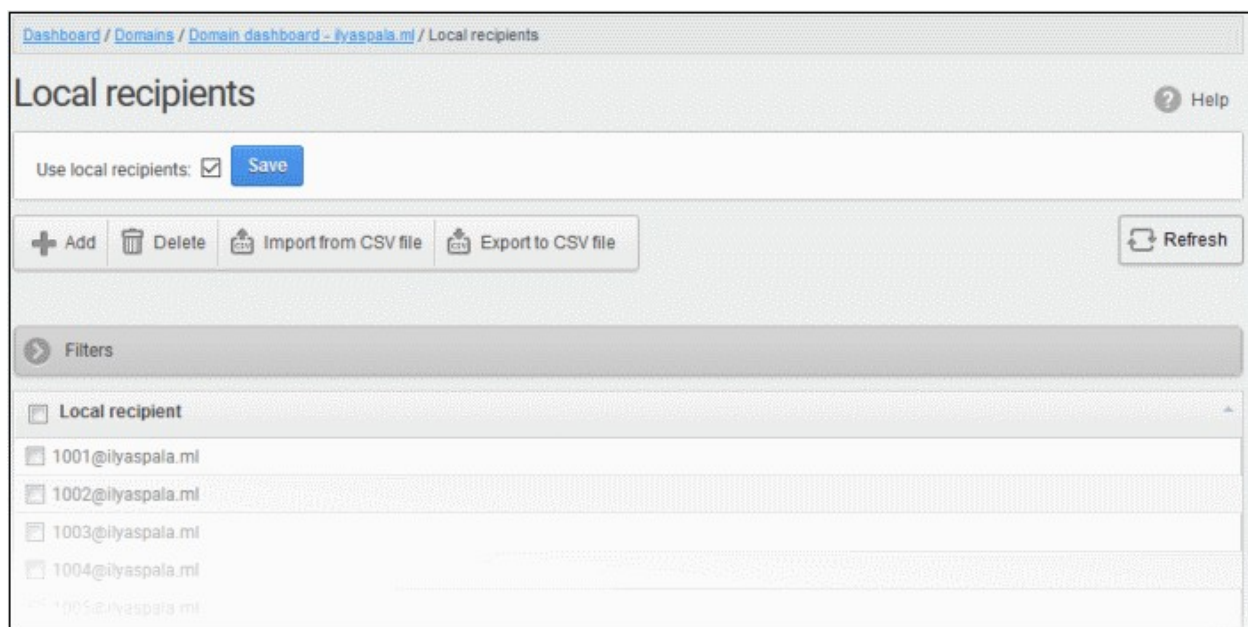
Important Note: If 'Local Recipients' feature is enabled, *all* recipients have to be added manually to the 'Local Recipients' interface. Otherwise, even valid users for that domain will not receive emails. Comodo recommends that this option should be used in specific cases only and is not required in normal circumstances.

Add local recipients

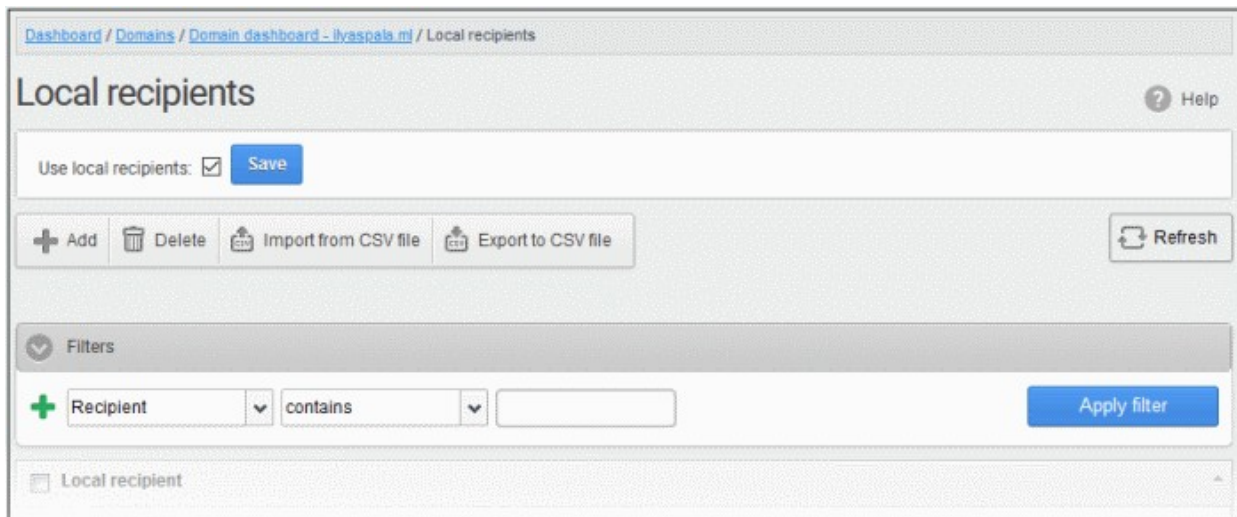
- Click 'Incoming' on the left then select 'Local recipients'.



The 'Local Recipients' configuration area for the selected domain will open:



- Click anywhere on the 'Filters' tab to open the filters area:



- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

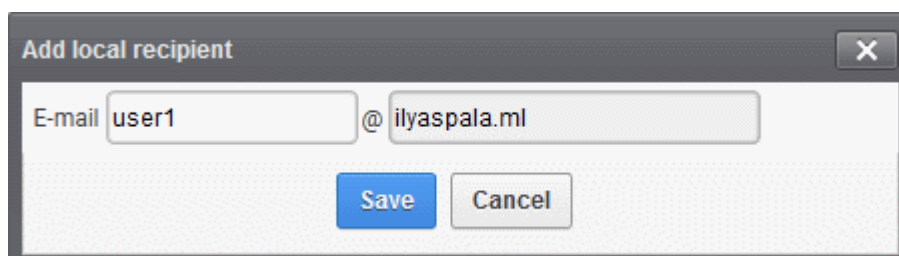
- **Recipient:** Enter the recipient name or address in the text box (column 3) and select a condition in column 2.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

Add local recipient

- Select the 'Use local recipients' check box and click the 'Save' button
- Click the 'Add' button

The 'Add local recipient' dialog box will open.



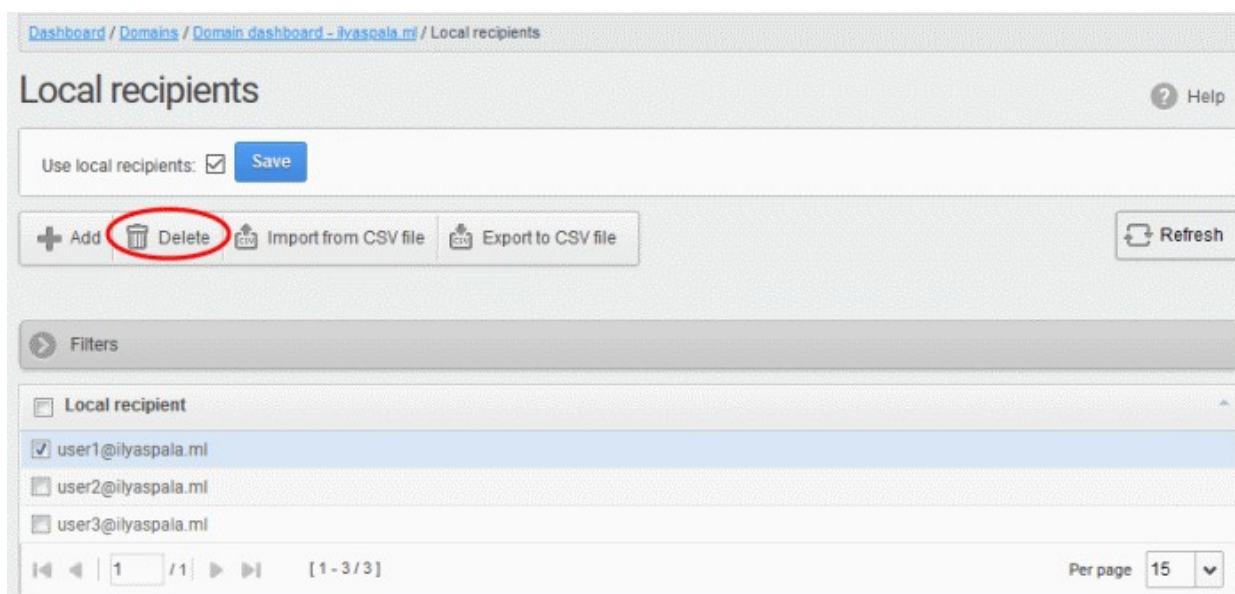
- Enter the recipient's in the E-mail field
- Click the 'Save' button

Repeat the process till you have added all users.

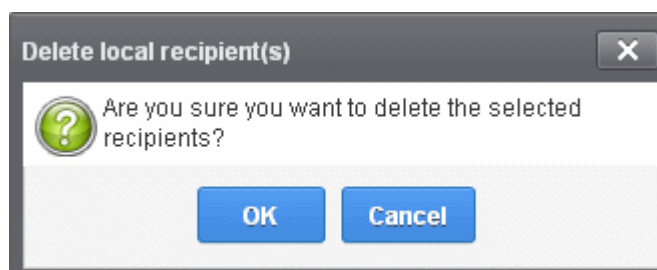


To remove a local recipient

- Select the user that you want to delete and click the 'Delete' button



- Click 'OK' to confirm.



The selected recipient will be deleted from the list

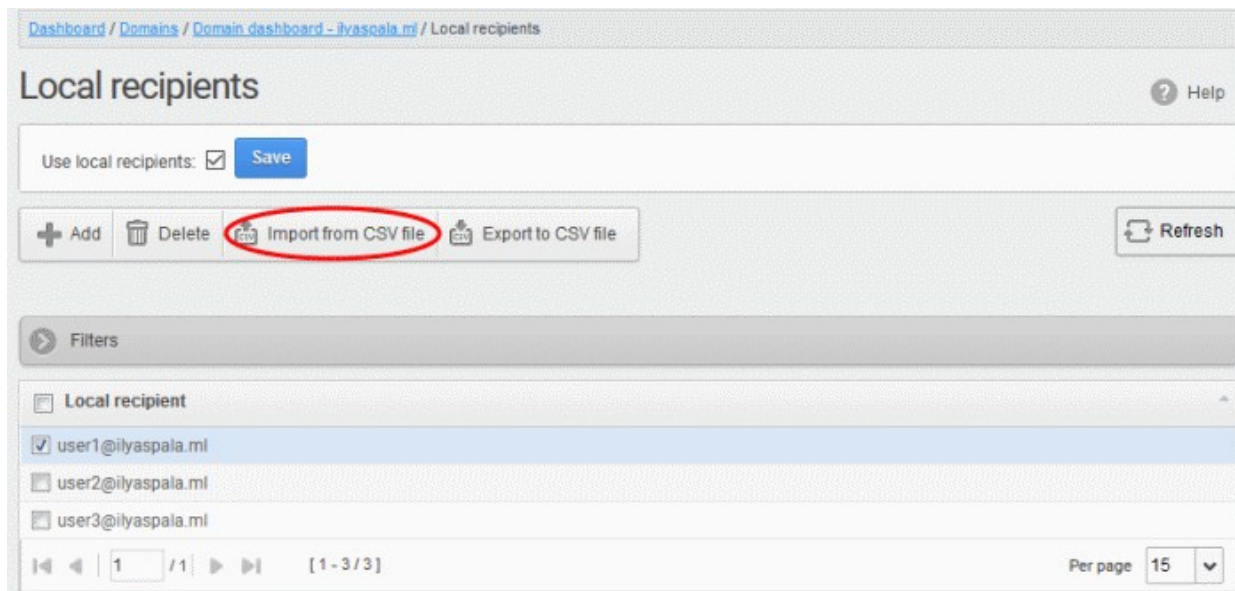
Tip: You can select multiple recipients to delete by pressing and holding the Shift or Ctrl keys.

Import local recipients from a CSV file

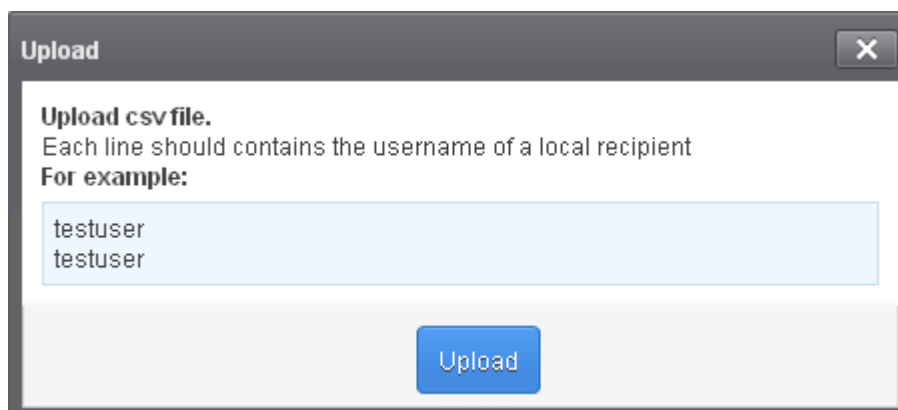
You can add many new users at a time by importing from a file. The users should be saved in separate lines as shown below:

```
user1  
user2  
user3
```

- Click the 'Import from CSV file' to import new users from a CSV file.



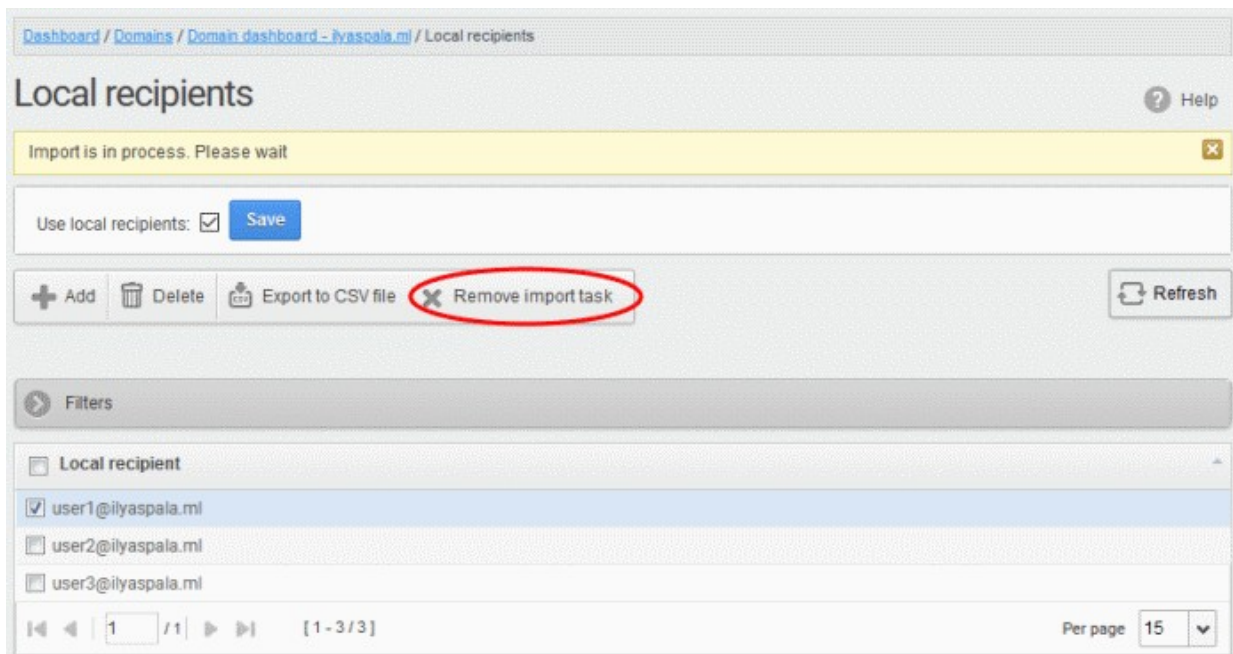
- Click 'Upload', navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.



The upload will be placed in the import tasks queue and the progress of the upload will be displayed.

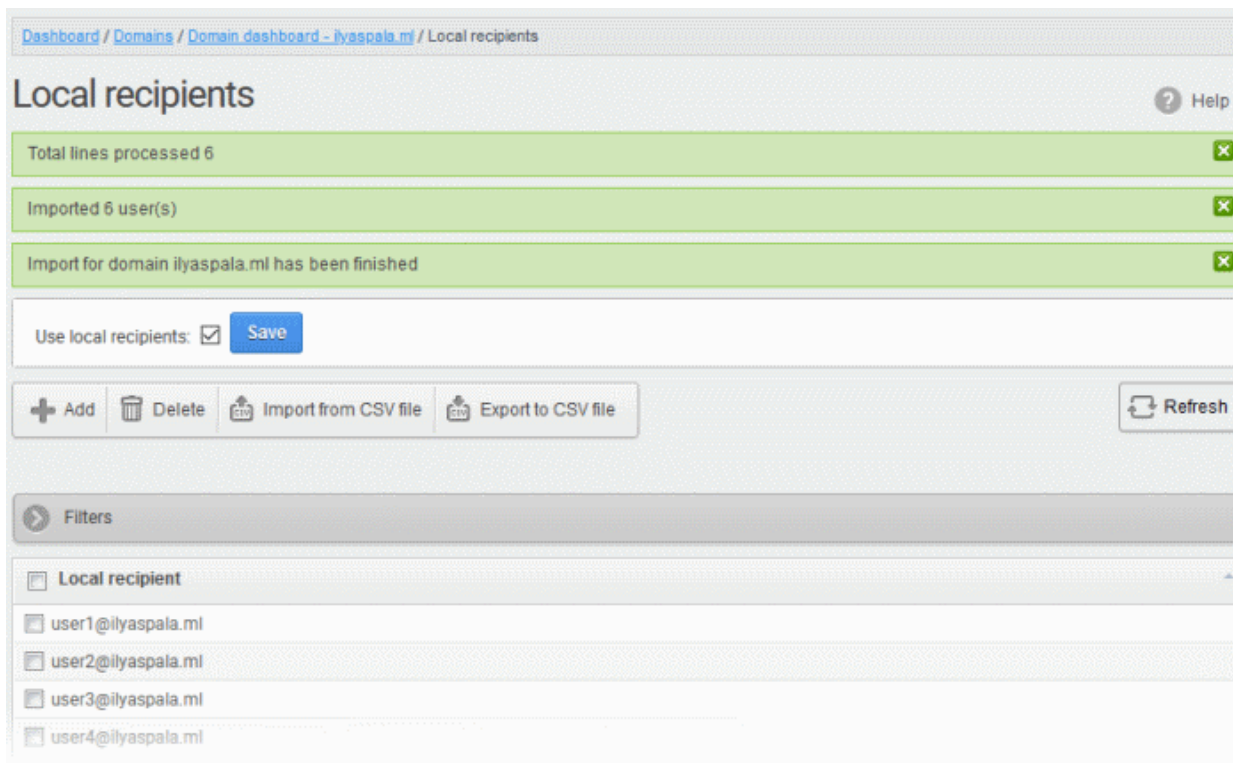
- If you want to remove the upload from the queue, click the 'Remove import task' button.

The 'Remove import task' deletes only the remaining part of an in-progress task.



The screenshot shows the 'Local recipients' page in the Comodo Antispam Gateway administrator interface. The breadcrumb trail is 'Dashboard / Domains / Domain dashboard - ilyaspala.ml / Local recipients'. The page title is 'Local recipients' with a 'Help' icon. A yellow notification bar at the top states 'Import is in process. Please wait'. Below this, there is a 'Use local recipients:' checkbox which is checked, and a 'Save' button. The main toolbar contains icons for '+ Add', 'Delete', 'Export to CSV file', and 'Remove import task' (which is circled in red), along with a 'Refresh' button. A 'Filters' section is visible below the toolbar. The main content area shows a list of local recipients under the heading 'Local recipient'. The first item, 'user1@ilyaspala.ml', is selected with a checkmark. Other items are 'user2@ilyaspala.ml' and 'user3@ilyaspala.ml'. At the bottom, there is a pagination control showing '1 / 1' and '[1 - 3 / 3]', and a 'Per page' dropdown set to '15'.

On completion of the upload process, the results will be displayed.



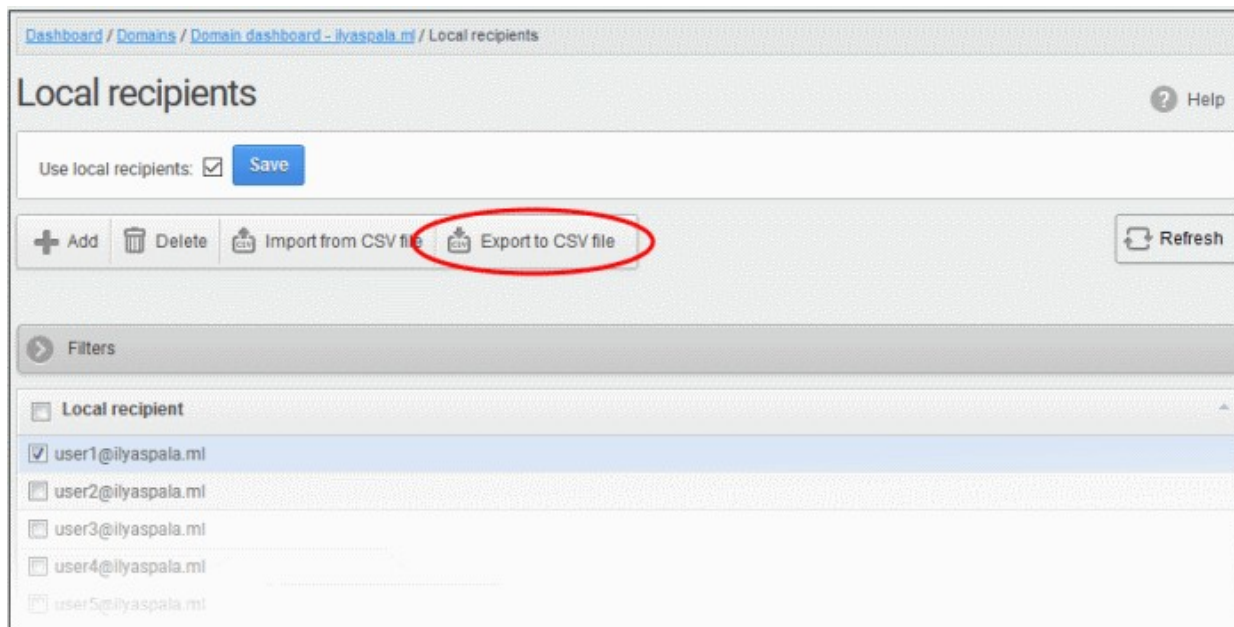
The screenshot shows the 'Local recipients' page after a successful import. The breadcrumb trail is 'Dashboard / Domains / Domain dashboard - ilyaspala.ml / Local recipients'. The page title is 'Local recipients' with a 'Help' icon. Three green notification bars at the top indicate: 'Total lines processed 6', 'Imported 6 user(s)', and 'Import for domain ilyaspala.ml has been finished'. Below these, there is a 'Use local recipients:' checkbox which is checked, and a 'Save' button. The main toolbar contains icons for '+ Add', 'Delete', 'Import from CSV file', and 'Export to CSV file', along with a 'Refresh' button. A 'Filters' section is visible below the toolbar. The main content area shows a list of local recipients under the heading 'Local recipient'. The items are 'user1@ilyaspala.ml', 'user2@ilyaspala.ml', 'user3@ilyaspala.ml', and 'user4@ilyaspala.ml'.

The local recipients from .csv file will be uploaded and the administrator who carried out the task will receive a notification about the import task completion.

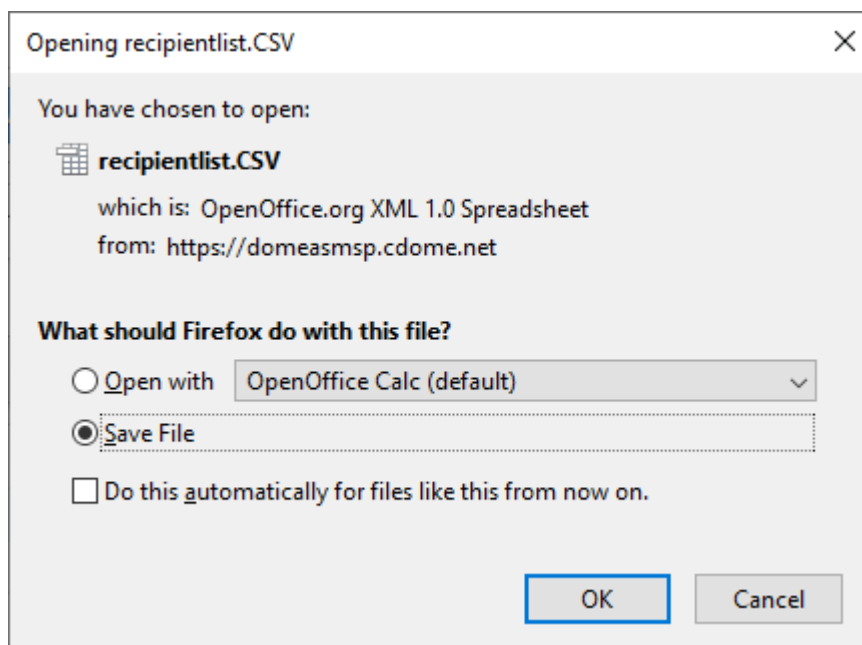
Export local recipients as a CSV file

You can save the local recipients list as a CSV file.

- Click 'More actions' > 'Export to CSV file'



The file download dialog is displayed.



- Click 'Open' to view the file with an appropriate application
- Click 'OK' to save the file to your computer.

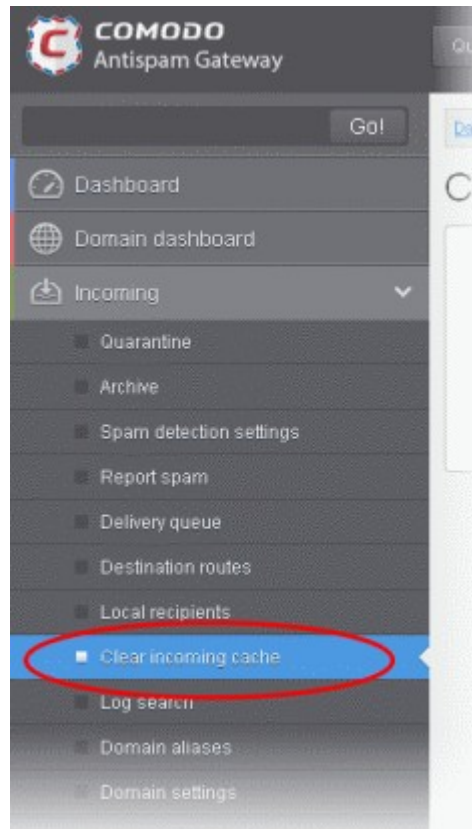
This file can be opened with Excel or Openoffice Calc.

Clear Incoming Cache

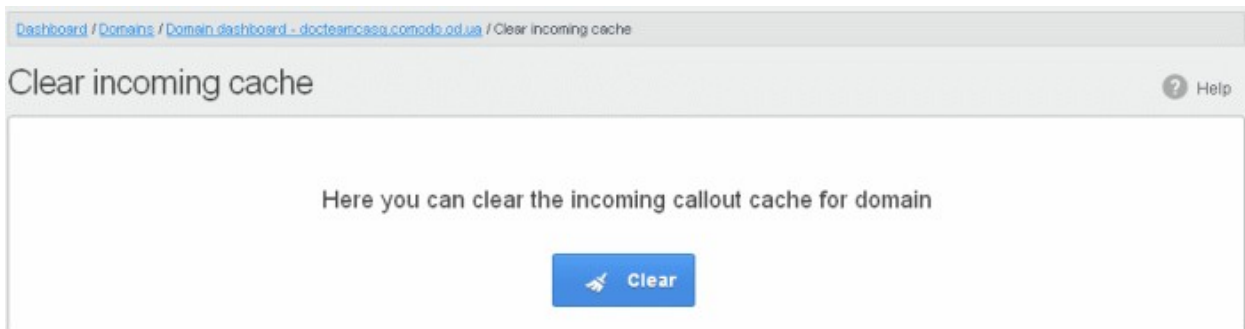
- When an email for a certain recipient is permanently rejected by the destination server with a 5xx error code, the destination address of the recipient is considered invalid and all emails sent to the recipient will be rejected.
- CASG filtering servers caches this information locally for up to two hours. The CASG interface allows you to clear the call-out cache without waiting for the servers to clear it.

Clear incoming cache

- Click 'Incoming' on the left then select 'Clear incoming cache'.

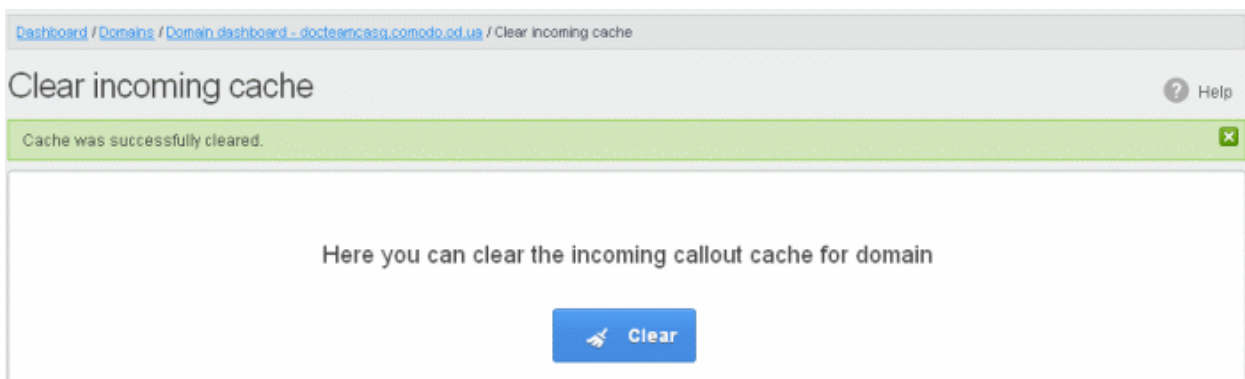


The 'Clear incoming cache' interface will open:



- Click the 'Clear' button

The callout cache for the incoming domain is cleared.



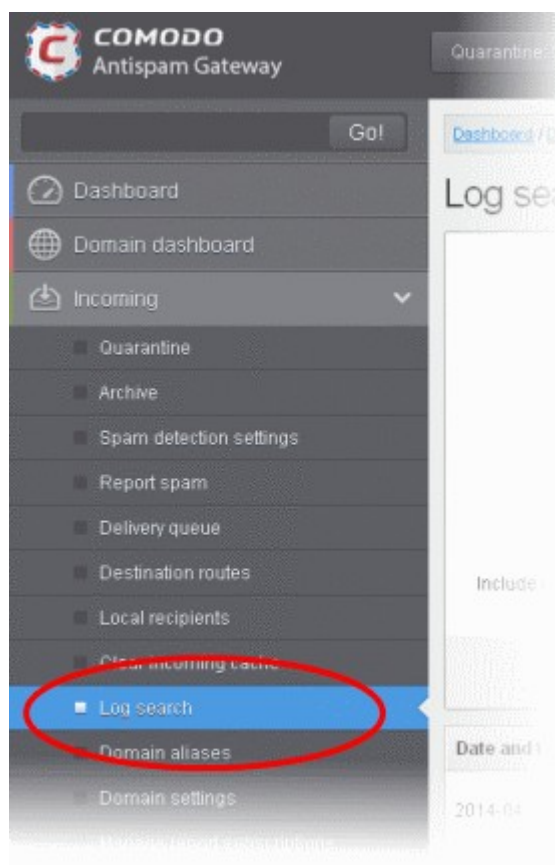
- Click the  button to close the notification.

Log Search

Log searches allow you to look for specific mails for a domain. You can refine your search by various parameters like sender, recipient and more.

Search logs for incoming mails

- Click 'Incoming' on the left then select 'Log search'.



The 'Log search (incoming)' interface for the selected domain will open:

[Dashboard](#) / [Domains](#) / [Domain dashboard - docteamcasg.comodo.od.ua](#) / [Log search \(incoming\)](#)

Log search (incoming) Help

Date range: -

Message ID:

Sender:

Recipient: @docteamcasg.comodo.od.ua

Sender IP:

Sender host:

Predicate:

Include results from the last minutes:

- **Date range:** Select the date range for which you want to search the log file. The date range for which the log search can be processed depends on the settings configured in **Domain Settings** > Log retention period.
- **Message ID** - Enter a unique message identifier (*optional*)
- **Sender:** Enter a sender email address in this field.
- **Recipient:** Enter the email address in this field (for example, 'testuser1').
- **Sender IP:** Enter the IP address of the sender.
- **Sender host:** Enter the sender host name.
- **Predicate:** You have the option to select either 'AND' or 'OR' in the drop-down. When you choose 'AND' option, all the entered search terms will be searched together and when you choose 'OR' option, the application will search any of the search items entered.
- **Include results from the last minutes:** If selected, CASG will include messages that are currently being migrated from the filtering server to the logging server in the search results.

The option "Include results from the last minutes" will slow down the search result retrieval

- Click the 'Search' button.

CASG will search for the entered terms and display the results.

Date and time	Host (Exim id)	Sender hostname	Sender	Recipient	Subject	Classification
2014-10-28 13:37:05	mxsrv1.spamgateway.cor 1Xj6xK-0008ET-B2	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo1	,DQ demo 2	Accepted Message content looked like non-spam
2014-10-28 13:37:05	mxsrv1.spamgateway.cor 1Xj6xK-0008ET-B2	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo2	,DQ demo 2	Accepted Message content looked like non-spam
2014-10-28 13:36:33	mxsrv1.spamgateway.cor 1Xj6wo-0007pb-Ag	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo1	,Re: DQ demo	Accepted Message content looked like non-spam
2014-10-28 13:36:33	mxsrv1.spamgateway.cor 1Xj6wo-0007pb-Ag	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo2	,Re: DQ demo	Accepted Message content looked like non-spam
2014-10-28 13:34:32	mxsrv2.spamgateway.cor 1Xj6up-00070G-Jb	mxsrv1.spamgateway.cor 178.33.199.65	demo@csg.comodo.od.u	demo1	,DQ demo	Rejected Rejected by relay restriction for this recipient
2014-10-28 13:34:32	mxsrv2.spamgateway.cor 1Xj6up-00070G-Jb	mxsrv1.spamgateway.cor 178.33.199.65	demo@csg.comodo.od.u	demo2	,DQ demo	Rejected Rejected by relay restriction for this recipient
2014-10-28 13:26:19	mxsrv1.spamgateway.cor 1Xj6ms-0008Pk-CK	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo2	Archive email 2	Accepted

Domain Aliases

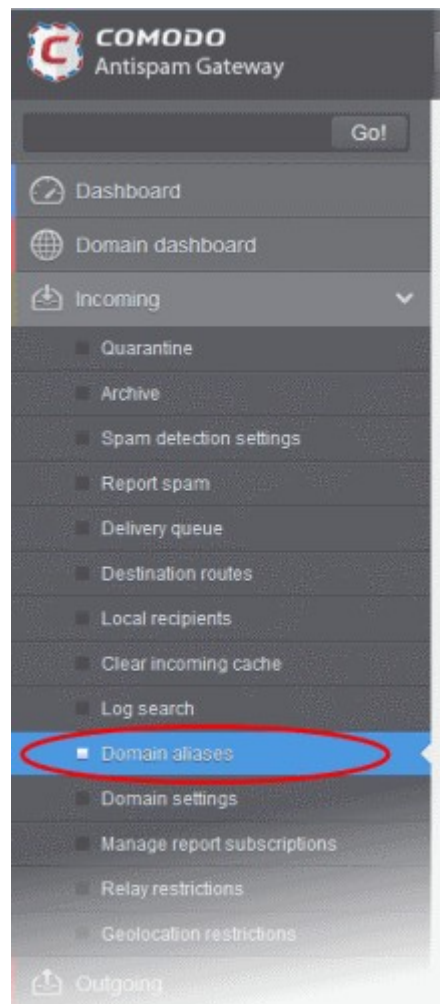
CASG lets you add multiple domains as aliases for a specific domain. Mails sent to the alias will be filtered and delivered to users at the target domain.

For example, if you add testdomain.org as an alias domain for testdomain.com, then mail sent to user1@testdomain.org will be filtered and delivered to user1@testdomain.com. The 'To:' headers in the email will still display the original recipient as user1@testdomain.org.

Note: Your MX records should be configured appropriately for the alias after adding domain aliases to CASG.

Add domain aliases

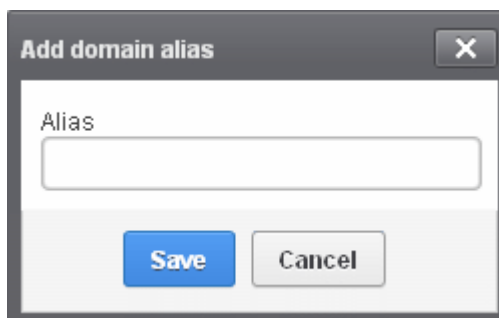
- Click 'Incoming' > 'Domain aliases' in the left-hand menu



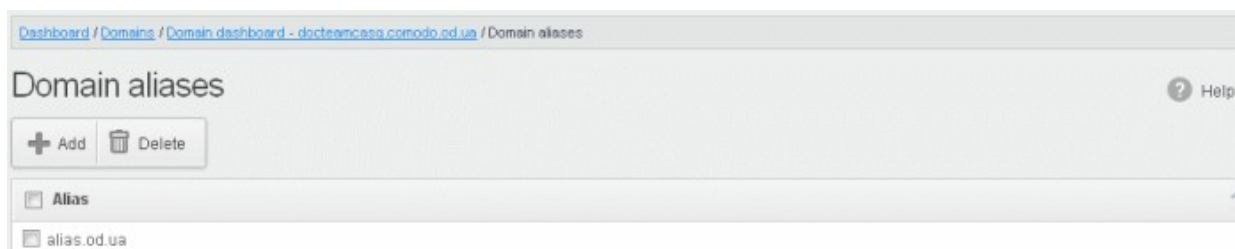
The 'Domain Aliases' interface will open:

- Click the 'Add' button to add a domain alias. The 'Add domain alias' dialog box will open
- Enter the domain alias name in the 'Alias' field



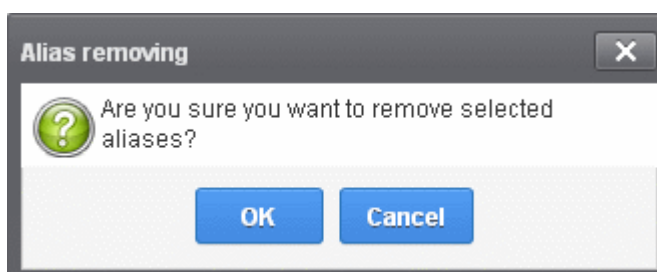


- Click the 'Save' button. The domain will be added to the main domain as alias and will be listed in the interface.



Delete a domain alias

- Select the domain alias from the list
- Click 'Delete'
- Click 'OK' to confirm the deletion.



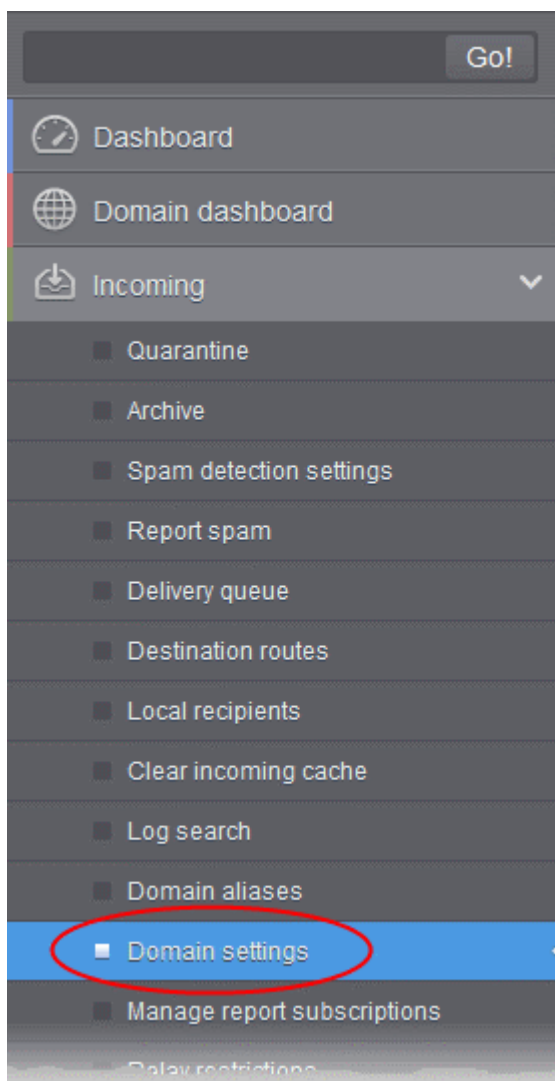
The selected domain alias will be deleted from the list.

Domain Settings

The 'Domain Settings' interface let you configure settings such as log retention period, maximum number of users and more for the selected domain.

Configure domain settings

- Click 'Incoming' > 'Domain settings' in the left-hand menu



The 'Domain Settings' interface of the selected domain will open:

Dashboard / Domains / Domain dashboard - iyaspala.nl / Domain settings

Domain settings Help

Maximum bounces:

Log retention period:

Maximum days to retry:

Max. number of users:

Enable archive cleanup:

Retain Archived items for: Months

Enable user auto-login:

Days before cookie expiration:

Email for license notifications:

Timezone:

Domain Archive Space (GB):

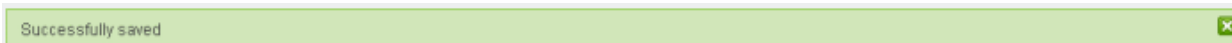
- **Maximum bounces:** Enter the maximum number of message bounces that each recipient in the selected domain can receive per hour (messages from postmaster addresses or with an empty envelope sender). Please note that if the number of bounces exceeds the limit set in this field, the messages are not quarantined but are permanently rejected and will not be received later. You can set this to a low value if users at the selected domain do not send mails to invalid addresses frequently. By default this field is set to 6000.
- **Log retention period:** All spam and non-spam email connections to a domain are logged in the CASG server. By default the storage period of this log is 30 days. You can store the log for a longer period by entering the number of days that you want to store in the field. After the end of set period, the log data will be moved to a separate storage and cannot be retrieved.
- **Maximum days to retry:** If the destination route has temporary problems, the messages are queued and automatically retried at fixed intervals for the number of days entered in the field. Even after this period if the emails cannot be delivered, they are bounced to the sender. By default, this is set to 4 days, the main reason being that the senders should be aware that his\her messages are not being delivered for 4 days.
- **Max. number of users:** Enter the maximum of users that can be added for this domain. Leaving this setting as 'Unlimited' will allow you to add up to, but not exceed, the maximum number of users permitted by your current license. This can also be done while **creating a domain** or in the **editing domain** interface.
- **Enable archive cleanup:** Allows you to enable or disable the auto-clean up of archived incoming mails in the archive storage. This option is available for customers that has purchased archive storage from Comodo.
- **Retain Archived items for:** Allows you to set the period in months or days, for which the archived mails should be retained in the archive storage, if you have enabled archive clean-up. The messages that are older than the period set in this field will be purged automatically.
- **Enable user auto-login:** If enabled, end-users can login into their CASG account without entering their credentials. On first login, the users will be asked to confirm their auto login. The users can also change the settings on their 'My Profile' page. The users' credentials will be stored in the browser as auto-login cookie and will be valid for the number of days that is entered in the next field 'Days before cookie expiration'.

- **Days before cookie expiration:** Enter the validity period in days of the auto-login cookie for end-users. This is only relevant if you have enabled user-auto-login. Upon expiry of the cookie, users need to provide login credentials to access their CASG account. The validity period starts after each successful user login.
- **Email for license notification:** Enter the email address for receiving license notifications for this domain. You can enter different email addresses for different domains for receiving notifications with respect to CASG license. If the field is left blank, then license notifications will be sent to admins' registered email address in Comodo Accounts Manager (CAM).
- **Timezone** - Allows you to choose the zone for the domain, depending on the location from which it is hosted. CASG will use the selected time-zone for events which concern that domain, especially for maintaining the quarantine list, archive list, log search, reports and report subscriptions.
- **Domain Archive Space** – Enter the archive disk space for this domain. The total disk space for all domains should not exceed the disk quota available for your account. Admins with appropriate privileges can configure this while **adding / editing** a domain.

Note: The number of users that you can add for all the domains belonging to your account depends on your subscription plan. For example, if the subscription plan for your account allows you to add 1000 users and you have three domains, then you can add 300 users for domain 1, 300 users for domain 2 and 400 users for domain 3. You can set any value between 0 and 999999 in the 'Max. number of users' field, but CASG checks if the total number of users for all domains is within your license limit.

- Click 'Reset to default' to reset default settings in CASG.
- Click the 'Save' button.

A confirmation dialog indicating the successful configuration of the domain settings will be displayed. Click 'X'.



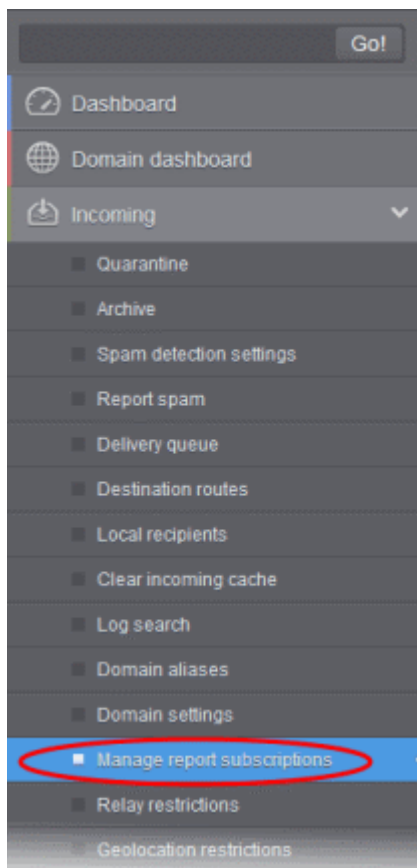
Manage Report Subscriptions for Selected Domain

Allows you to configure subscriptions to domain, user import, and quarantine reports generated for a domain. You can also specify which administrators of the domain should receive the reports.

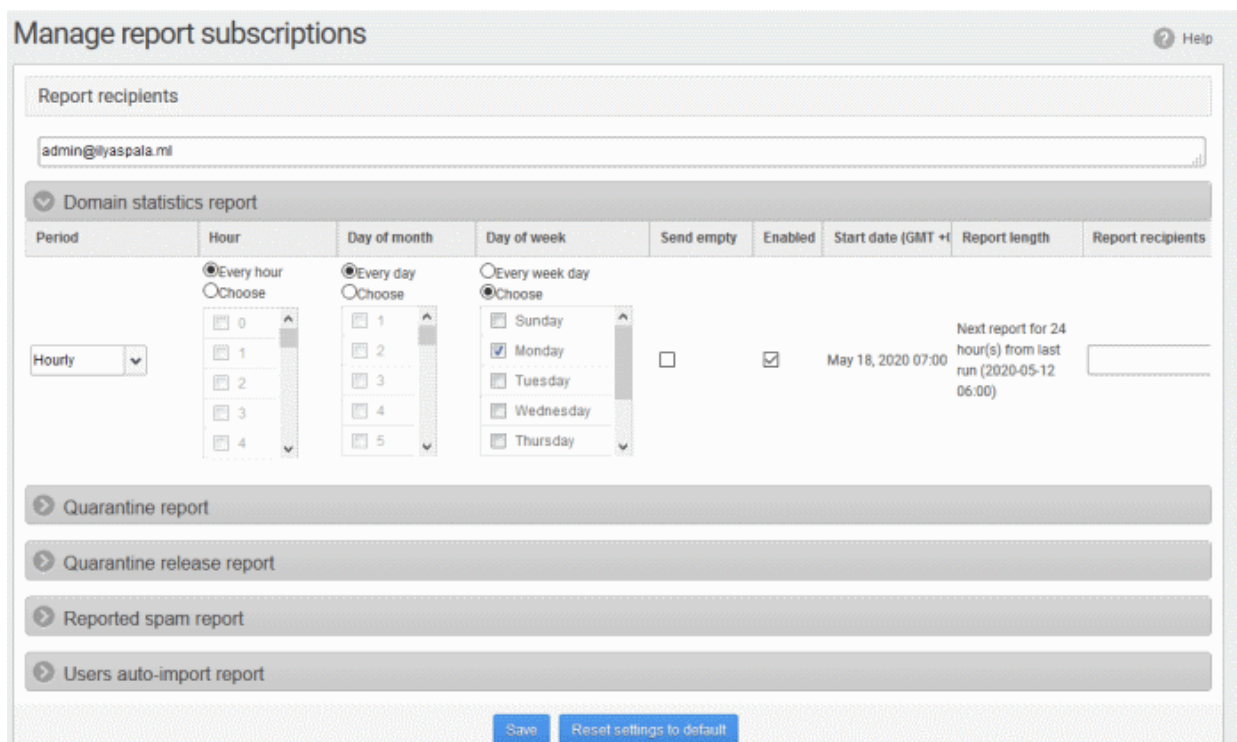
See [CASG Reports - an Overview](#) for more details on the reports.

Open manage report subscriptions interface

- Click 'Incoming' on the left then choose 'Manage report subscriptions'.



The 'Manage report subscriptions' interface will open:



- **Report recipients** (general) - Enter the email addresses of the domain administrators to whom the reports should be sent. You can enter multiple addresses separated by a comma. Note – Reports are not sent to these recipients if you configure recipients for each report type.

Note: The 'Report recipients' field will not be auto-populated as it does in the interface of **Customer Management > Manage Report Subscriptions**

- The 'manage report subscriptions' interface lets you configure the delivery schedule for each type of report.
- Click on the respective strip to expand the configuration pane for a report type.

You can configure subscriptions for five types of reports from this interface:

- **Domain Statistics Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly will contain a detailed statistics of number of users, mails that have been received at and sent from the domain, number of spams identified and blocked and so on. Refer to **CASG Reports - An Overview** for more details.
- **Quarantine Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly will contain a detailed statistics of the mails that are identified as spam or containing malicious content and moved to Quarantine of the domain automatically by CASG. Refer to **CASG Reports - An Overview** for more details.
- **Quarantine Release Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly will contain a detailed statistics of the quarantined mails that are released by the administrator to the recipient. Refer to **CASG Reports - An Overview** for more details.
- **Reported Spam Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly will contain a detailed statistics of the mails that are reported as spam by administrators and users. Refer to **CASG Reports - An Overview** for more details.
- **Users auto-import report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly will contain details of new users that were auto-imported based on incoming mails received for them at the mail server. For more details on configuring CASG for auto-importing new users, refer to the section **Manage User Auto-import**. For more details on the reports, refer to the section **CASG Reports - An Overview**.

Configure report subscriptions

- Send empty - Leave this unchecked if empty reports are not to be sent to recipients.
- Enabled – Select this so reports are generated and sent to report recipients.
- Report recipients for each report type – Enter the email address of recipients that you want the reports to be sent. You can enter multiple addresses separated by a comma. Note – If this field is configured, the recipients that you added in the general report recipients field at the top of the interface will not receive the reports.
- Select the frequency of the report to be sent to the administrators from the options for:
 - **Quarantine Report;**
 - **Domain Statistics Report;**
 - **User Auto-Import Report;**
 - **Quarantine Release Report;** and
 - **Reported Spam Report.**

Quarantine Report

- **Hour** - The reports are generated and sent to the report recipients every hour or at the selected hour(s) of the day or date chosen from 'Day of month' or 'Day of week' columns.
- **Day of month** - The reports are generated and sent to the report recipients every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports are generated and sent to the report recipients every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
- **Start date** - Displays the start date of the report generation depending on the options chosen (as per Greenwich Mean Time (GMT)).
- **Report length** - Displays the period of the report that are generated depending on the options chosen.

Domain Statistics Report

- **Period** - Enables you to set the period to be covered in the report. The report contains the statistics of all domains in the account for the past one hour, one week, one month or one year, as selected from drop-down from the scheduled report time.
- **Hour** - The reports are generated and sent to the report recipients every hour or at the selected hour(s) of the day or date chosen from 'Day of month' or 'Day of week' columns.
- **Day of month** - The reports are generated and sent to the report recipients every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports are generated and sent to the report recipients every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
- **Start date** - Displays the start date of the report generation depending on the options chosen (as per Greenwich Mean Time (GMT)).
- **Report length** - Displays the period of the report that are generated depending on the options chosen.

User Auto-Import Report

- **Hour** - The reports are generated and sent to the report recipients every hour or at the selected hour(s) of the day or date chosen from 'Day of month' or 'Day of week' columns.
- **Day of month** - The reports are generated and sent to the report recipients every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports are generated and sent to the report recipients every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
- **Start date** - Displays the start date of the report generation depending on the options chosen (as per Greenwich Mean Time (GMT)).
- **Report length** - Displays the period of the report that are generated depending on the options chosen.

Quarantine Release Report

- **Hour** - The reports are generated and sent to the report recipients every hour or at the selected hour(s) of the day or date chosen from 'Day of month' or 'Day of week' columns.
- **Day of month** - The reports are generated and sent to the report recipients every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports are generated and sent to the report recipients every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
- **Start date** - Displays the start date of the report generation depending on the options chosen (as per Greenwich Mean Time (GMT)).
- **Report length** - Displays the period of the report that are generated depending on the options chosen.

Reported Spam Report

Reported spam report							
Hour	Day of month	Day of week	Send empty	Enabled	Start date (GMT +07:00)	Report length	Report recipients
<input checked="" type="radio"/> Every hour <input type="radio"/> Choose 0 1 2 3 4	<input checked="" type="radio"/> Every day <input type="radio"/> Choose 1 2 3 4 5	<input checked="" type="radio"/> Every week day <input type="radio"/> Choose Sunday Monday Tuesday Wednesday Thursday	<input type="checkbox"/>	<input checked="" type="checkbox"/>	May 12, 2020 22:00	Next report for 1 hour(s) from last run (2020-05-12 14:00)	<input type="text"/>

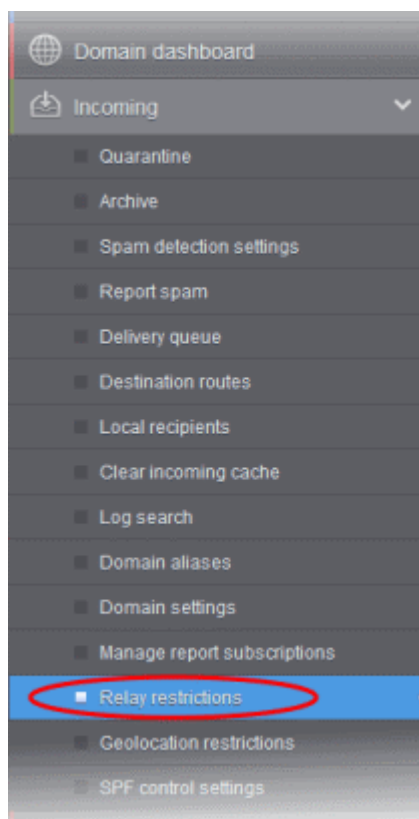
- **Hour** - The reports are generated and sent to the report recipients every hour or at the selected hour(s) of the day or date chosen from 'Day of month' or 'Day of week' columns.
- **Day of month** - The reports are generated and sent to the report recipients every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports are generated and sent to the report recipients every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
- **Start date** - Displays the start date of the report generation depending on the options chosen (as per Greenwich Mean Time (GMT)).
- **Report length** - Displays the period of the report that are generated depending on the options chosen.
- Click 'Save' for your settings to take effect.
- Click the 'Reset settings to default' button to disable all the reports. The 'Report Recipients' fields will not be cleared.

Relay Restrictions

- The 'Relay restrictions' interface lets you specify message transfer agents (MTA), mail servers, or other mail relays from which incoming mail should be accepted or rejected.
- For example, a business that has regional offices can configure their regional systems to accept only incoming emails from email servers at the home office.
- Administrators can define organization names from which mails should be accepted or rejected. CASG parses the mail headers of each incoming mail to ensure the existence of an MTA IP address or FQDN of the organization before accepting the mail. If you don't know the name of an organization, you can search for it using the 'Lookup' feature. Enter the IP address of the sender domain.

Add a relay restriction rule

- Click 'Incoming' from the left then select 'Relay Restrictions'.



The 'Relay restrictions' interface for the domain will open:

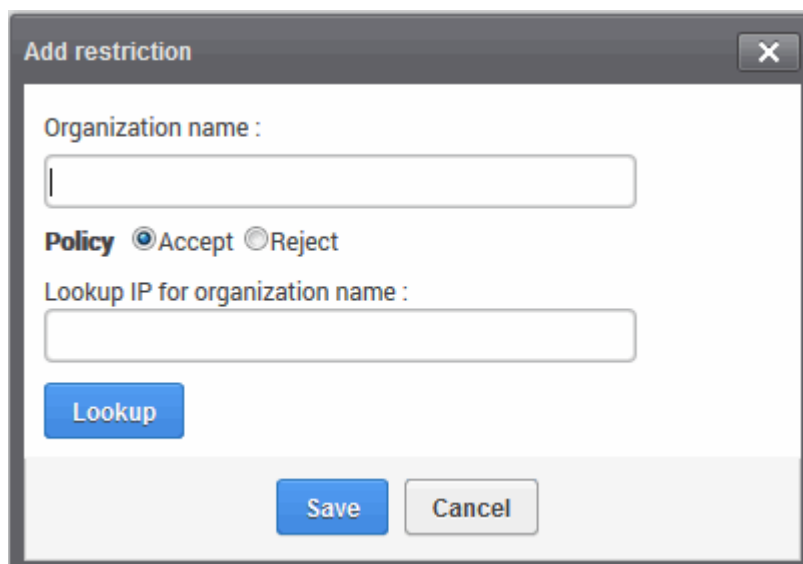
[Dashboard](#) / [Domains](#) / [Domain dashboard - demo.das.comodo.od.ua](#) / Relay restrictions

Relay restrictions

Restrict email acceptance to the following relay servers

Organization name	Policy
<input type="radio"/> Google Inc.	Accept

- Select the 'Restrict email acceptance to the following relay servers' check box
- Click the 'Add' button. The 'Add/Edit restriction' dialog will appear:



The screenshot shows a dialog box titled "Add restriction" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Organization name :". Below it is a "Policy" section with two radio buttons: "Accept" (which is selected) and "Reject". Underneath is another text input field labeled "Lookup IP for organization name :". A blue "Lookup" button is positioned below the second text field. At the bottom of the dialog, there are two buttons: a blue "Save" button and a grey "Cancel" button.

- Enter the organization name in the 'Organization name' text box
 - If you are not sure about the organization name, obtain the IP address of the mail server from any incoming mail from the organization and enter it in the 'Lookup IP for organization name' field. Click 'Lookup' to perform the search.
 - CASG will perform a lookup from WHOIS.com website and auto-populate the Organization name field.
- Choose the acceptance policy for emails from the organization's mail server:
 - Accept - All mails from the selected organizations will be accepted. Those from other organizations will be blocked.
 - Reject - All mails from the selected organizations will be blocked. Those from other organizations will be accepted.
- Click 'Save' for the rule to take effect.

Relay restrictions now enabled. ✕

- Repeat the process till you have added all the organizations.

The administrator need to add a rule for each organization from which the mails are to be accepted or rejected.

Illustrations:

1. For example, if you want to accept mails only from two domains, namely gooddomain1.com and gooddomain2.com and reject mails from all the other mail servers, create two rules, one for gooddomain1.com and other for gooddomain2.com.

- Rule 1 - Accept gooddomain1.com and block all other domains
- Rule 2 - Accept gooddomain2.com and block all other domains

Only the incoming mails from gooddomain1.com and gooddomain2.com will be accepted. Those from all the other domains will be rejected.

2. For example, if you want to block mails only from two domains, namely baddomain1.com and baddomain2.com and allow mails from all the other mail servers, create two rules, one for baddomain1.com and other for baddomain2.com.

- Rule 1 - Reject baddomain1.com and allow all other domains
- Rule 2 - Reject baddomain2.com and allow all other domains

Only the incoming mails from baddomain1.com and baddomain2.com will be blocked. Those from all the other domains will be accepted.

You can create any number of 'Allow' and 'Reject' rules. The 'Accept' rules have more priority and reject rules will be skipped in case of any rule conflict.

The incoming mails from blacklisted domains in the global or domain blacklist will be rejected even if they are accepted by the relay restrictions rules. The priority order of rules checked on allowing an email is as follows:

1. Global blacklist
2. Domain whitelist/blacklist
3. Relay restriction rules
4. Per user whitelist/blacklist

Note: The 'Relay restrictions' is disabled for TRIAL customers.

Edit Relay Restriction Rules

You can change the organization name or acceptance policy of any rule at any time.

Edit a rule

- Choose the rule to be edited and click the 'Edit' button.

The screenshot shows the 'Relay restrictions' page in the Comodo Antispam Gateway Admin interface. The page has a breadcrumb trail: Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Relay restrictions. There are three buttons: '+ Add', 'Delete', and 'Edit'. The 'Edit' button is circled in red. Below the buttons, there is a checkbox labeled 'Restrict email acceptance to the following relay servers' which is checked. A table lists the relay servers:

Organization name	Policy
<input type="radio"/> Google Inc.	Accept
<input type="radio"/> Yahoo	Accept
<input checked="" type="radio"/> Rediff.com India Limited,	Accept

The 'Rediff.com India Limited,' row is selected. A red arrow points from the 'Edit' button to the 'Add/Edit restriction' dialog box. The dialog box has the following fields and options:

- Organization name: Rediff.com India Limited,|
- Policy: Accept Reject
- Lookup IP for organization name: [empty field]
- Buttons: Lookup, Save, Cancel

The Add/Edit restriction dialog will appear.

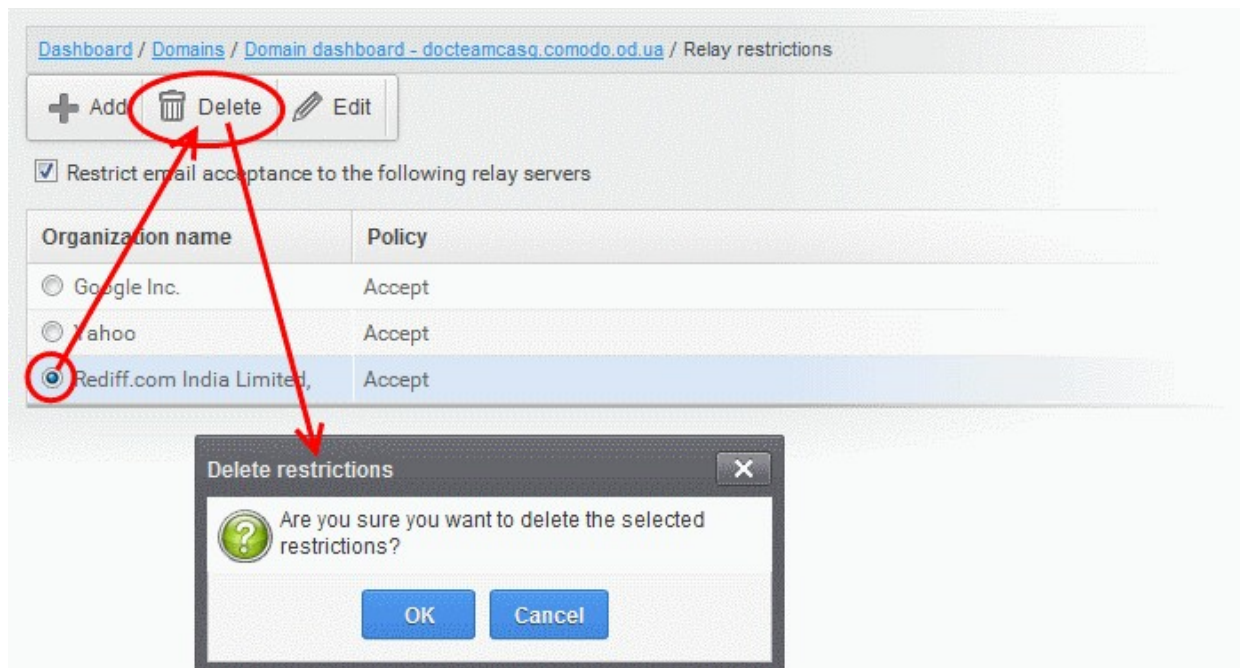
- Edit the fields and policy options as required. For more details refer to the explanation under **To add a Relay Restriction Rule**.
- Click 'Save' for your changes to take effect.

Removing Relay Restriction Rules

You can remove unwanted rules at anytime from CASG.

Remove a relay restriction rule

- Choose the rule you want to remove and click the 'Delete' button



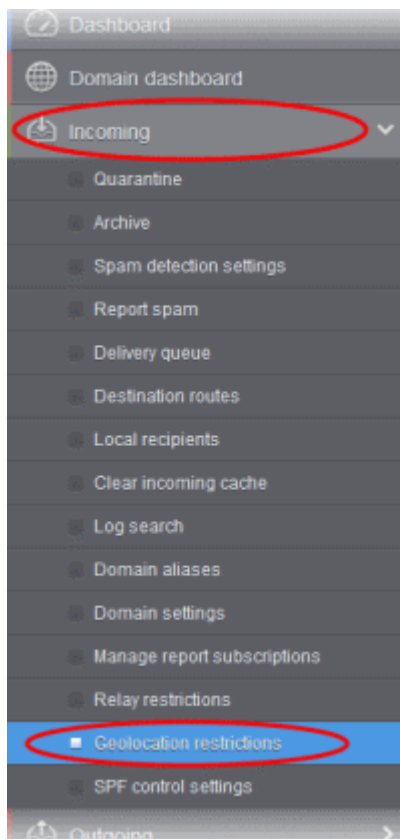
- Click 'OK' in the confirmation dialog.

Geolocation Restrictions

- You can set rules that allow or block access to the CASG console based on the country from which the connection attempt is made.
- Geolocation restriction policy applies to admins and users that has the selected domain in their user ID.

Create a geolocation policy

- Click 'Incoming' on the left then click 'Geolocation restrictions':



The 'Geolocation restrictions' interface for the domain opens:

Dashboard / Domains / Domain dashboard - iyaspala.ru / Geolocation restrictions

Geolocation restrictions

Help

+ Add Delete Edit Import from CSV file Export to CSV file

Enable geolocation restrictions

Country name	Country code	Policy
Algeria	DZ	Reject
Afghanistan	AF	Reject

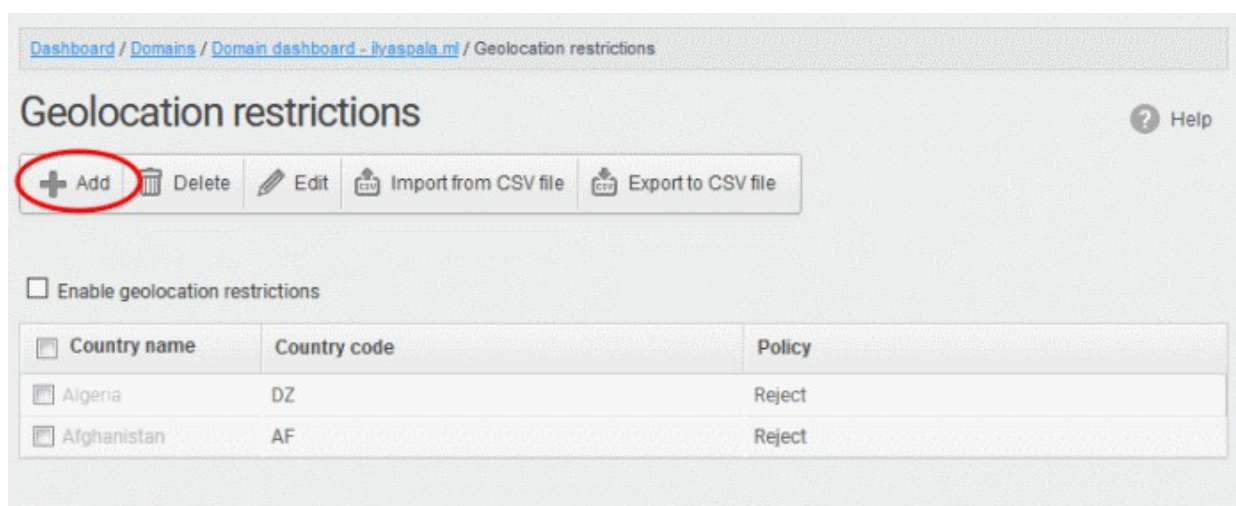
- **Enable geolocation restrictions** - Activate location based access restrictions. If enabled, administrators need to add restriction rules.

From the interface, you can:

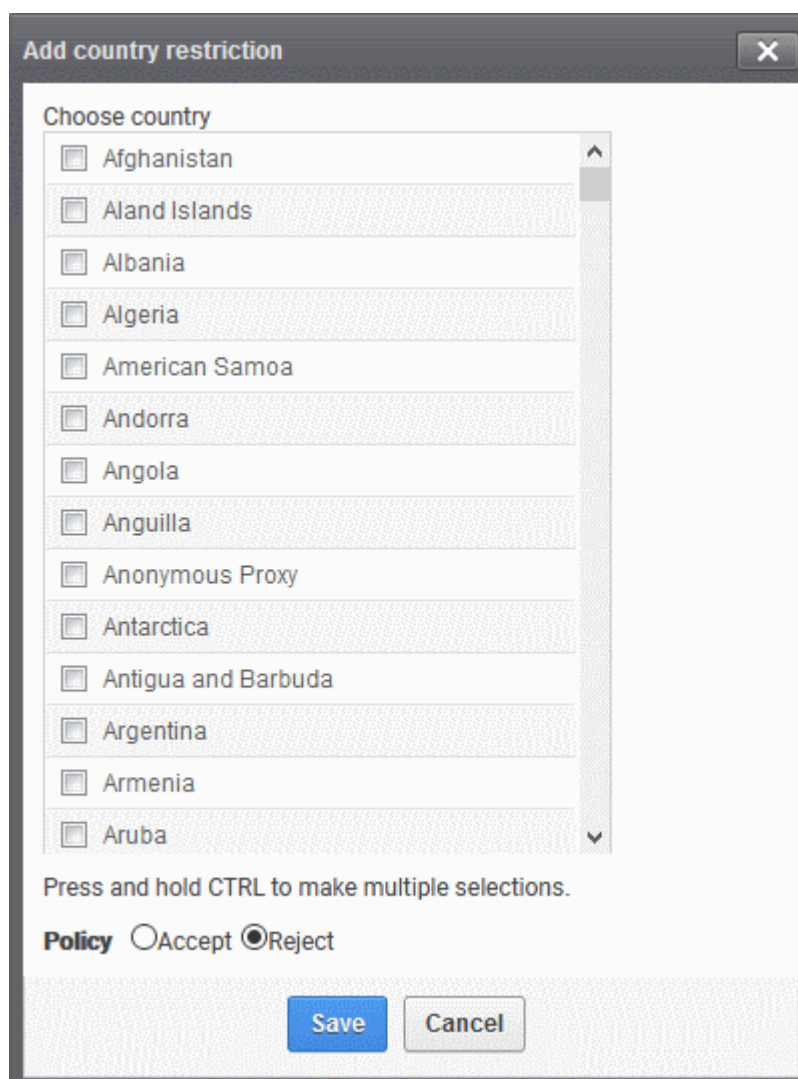
- **Add geolocation restriction rule**
- **Edit a geolocation restriction rule**
- **Delete a geolocation restriction rule**
- **Import geolocations from a CSV file**
- **Export geolocation list as a CSV file**

Add a new geolocation restriction policy

- Click the 'Add' button



The 'Add country restriction' dialog appears:

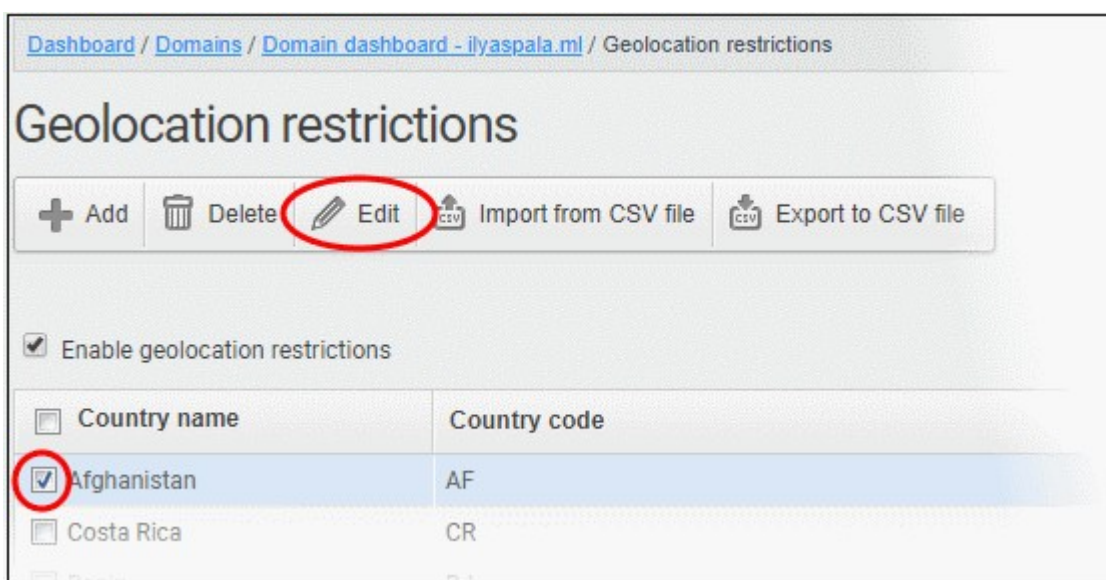


- Select the countries from the 'Choose country' drop-down
- Note – Use any one option only, select either 'Accept' or 'Reject'. 'Accept' option overrides 'Reject' option. For example, you choose to allow admins and users from US and reject from Sudan. CASG allows access from US only and denies access from *all* other countries irrespective of how many countries you rejected.

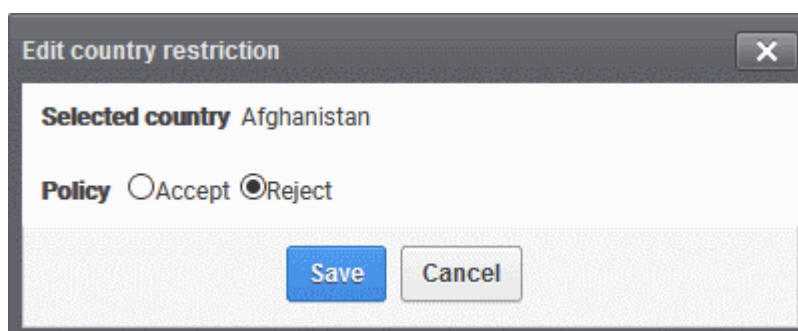
- Choose the geolocation restriction policy for accessing the CASG web interface
 - Accept - Admins and users from these countries are allowed to access the domain management interface. If you select this, admins and users from all other countries are automatically rejected from accessing CASG.
 - Reject - Admins and users from these countries are not allowed to access the domain management interface. If you select this, make sure you have not opted for 'Accept' for any country in the list.
- Click 'Save' to create the policy

Edit a geolocation restriction policy

- Select the restriction rule that you want to update and click the 'Edit' button



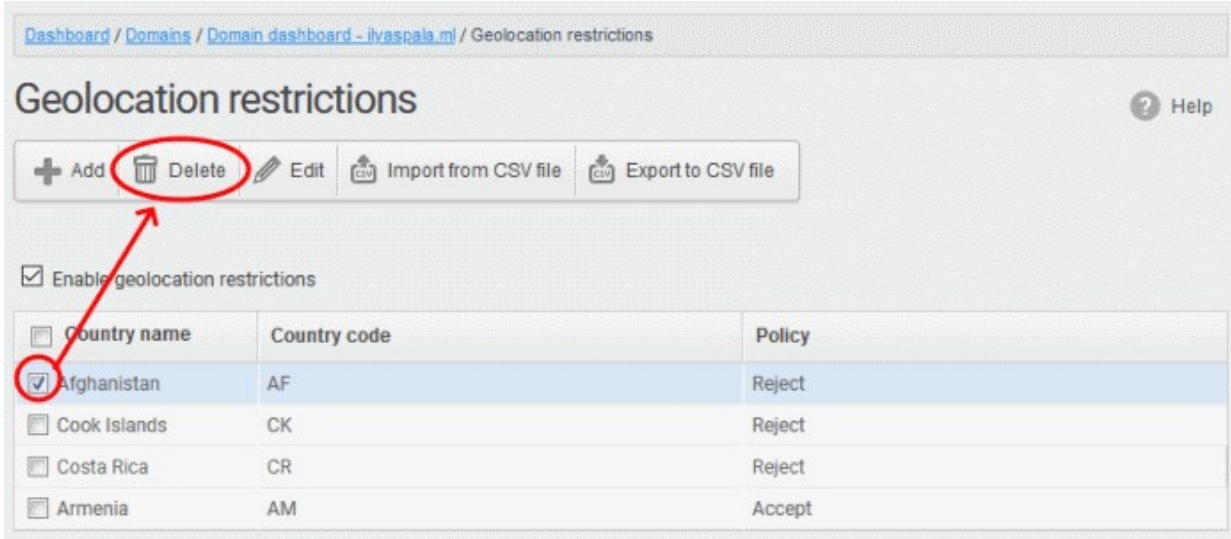
The 'Edit country restriction' dialog is shown:



- Update as required and click the 'Save' button for the changes to take effect.
- Note – Use any one option only, select either 'Accept' or 'Reject' in the list. 'Accept' option overrides 'Reject' option. For example, you choose to allow admins and users from US and reject from Sudan. CASG allows access from US only and denies access from all other countries irrespective of how many countries you rejected.

Delete a geolocation restriction policy

- Select the policy that you want to remove from the list and click the 'Delete' button



Dashboard / Domains / Domain dashboard - ilvaspala.ml / Geolocation restrictions

Geolocation restrictions

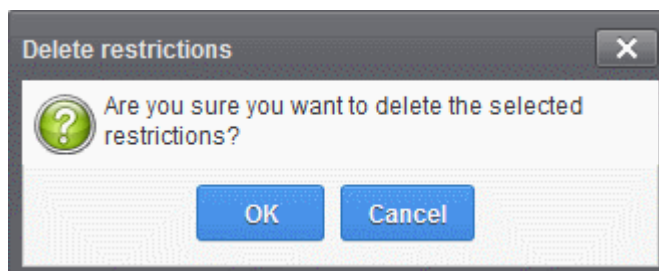
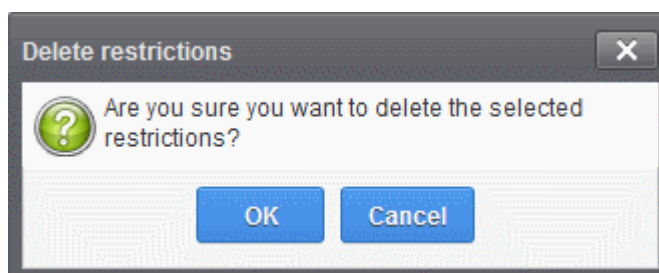
Help

+ Add Delete Edit Import from CSV file Export to CSV file

Enable geolocation restrictions

<input type="checkbox"/> Country name	Country code	Policy
<input checked="" type="checkbox"/> Afghanistan	AF	Reject
<input type="checkbox"/> Cook Islands	CK	Reject
<input type="checkbox"/> Costa Rica	CR	Reject
<input type="checkbox"/> Armenia	AM	Accept

- Click 'OK' to confirm the removal of the selected geolocation restriction rule from the list



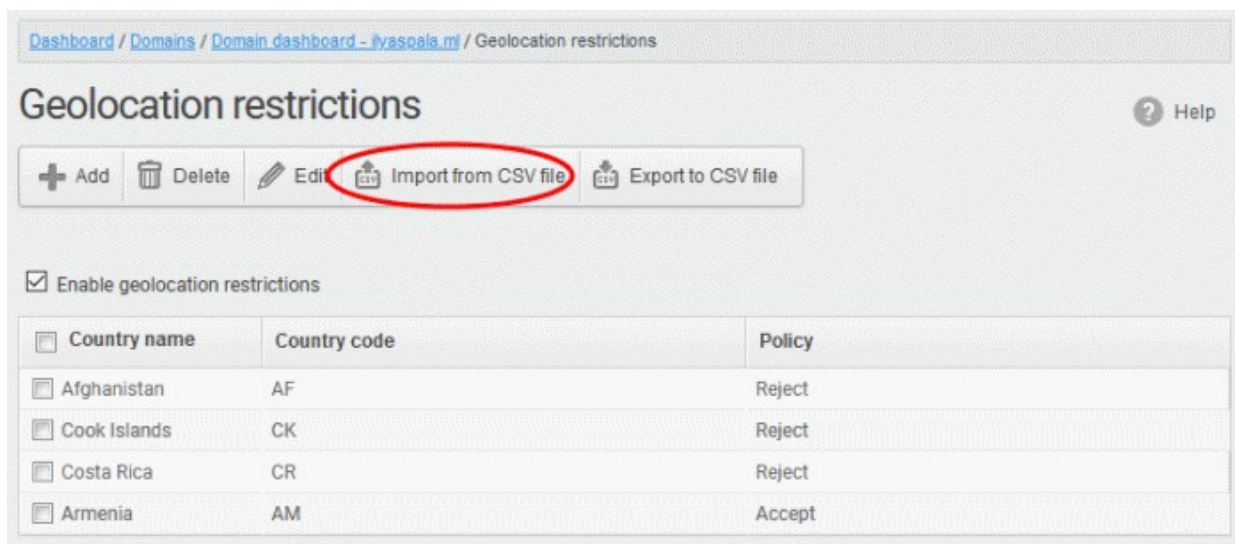
The rule will be removed from the list.

Import geolocations from a CSV file

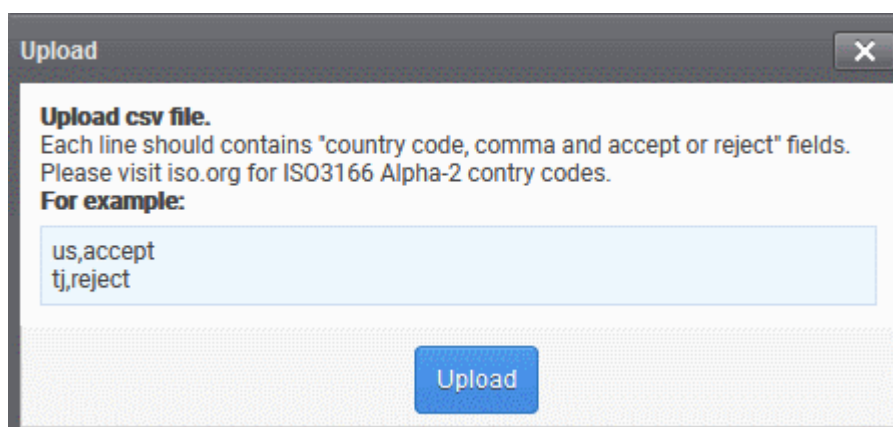
You can add many geolocations at a time by importing from a file. The country codes and values should be saved in 'comma separated value' (CSV) as shown below:

```
us,accept  
tj,reject
```

- Click 'Import from CSV file' to save countries from your CSV file

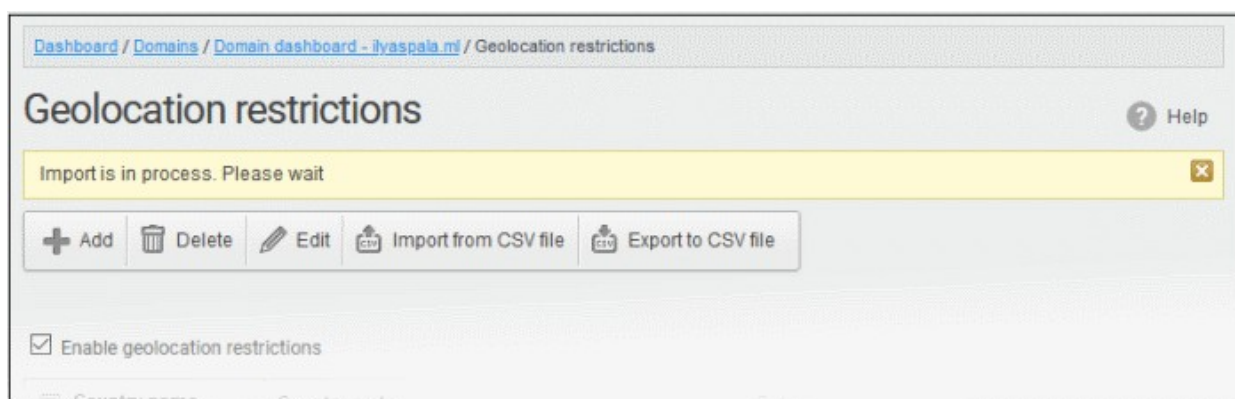


- Click 'Upload'



- Navigate to your file and click open

The import process begins...



...and when completed, the status is shown:

Dashboard / Domains / Domain dashboard - ilyaspala.ml / Geolocation restrictions

Geolocation restrictions Help

Total lines processed 5 ✕

Imported 3 user(s) ✕

Import for domain ilyaspala.ml has been finished ✕

Not imported due to duplicate 2 ✕

Enable geolocation restrictions

<input type="checkbox"/> Country name	Country code	Policy
<input type="checkbox"/> Afghanistan	AF	Reject
<input type="checkbox"/> Costa Rica	CR	Reject
<input type="checkbox"/> Benin	BJ	Reject
<input type="checkbox"/> Chad	TD	Accept

Export geolocation list as a CSV file

You can save the country list as a CSV file.

- Click 'Export to CSV file'

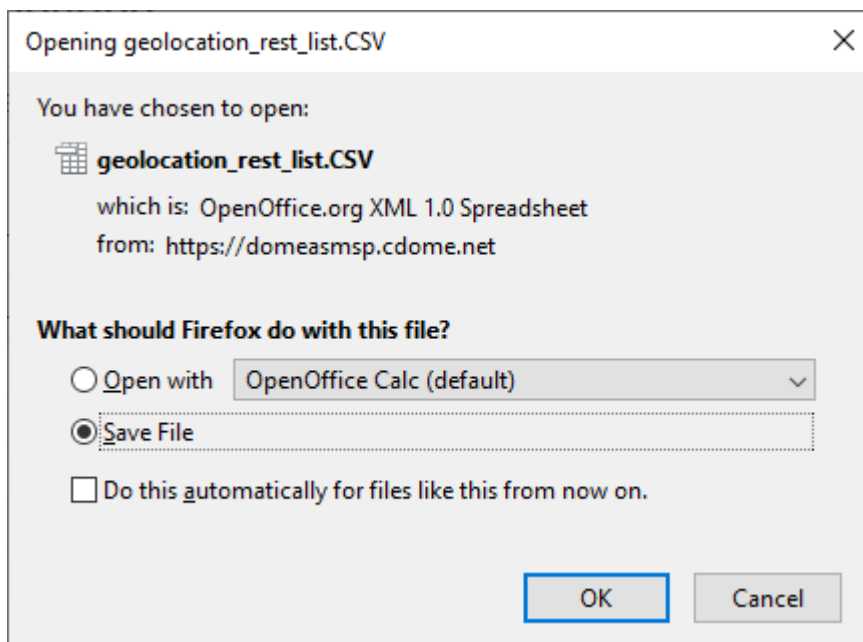
Dashboard / Domains / Domain dashboard - ilyaspala.ml / Geolocation restrictions

Geolocation restrictions Help

Enable geolocation restrictions

<input type="checkbox"/> Country name	Country code	Policy
<input type="checkbox"/> Afghanistan	AF	Reject
<input type="checkbox"/> Costa Rica	CR	Reject
<input type="checkbox"/> Benin	BJ	Reject
<input type="checkbox"/> Chad	TD	Reject
<input type="checkbox"/>		Accept

The file download dialog is displayed.



- Click 'Open' to view the file with an appropriate application
- Click 'OK' to save the file to your computer.

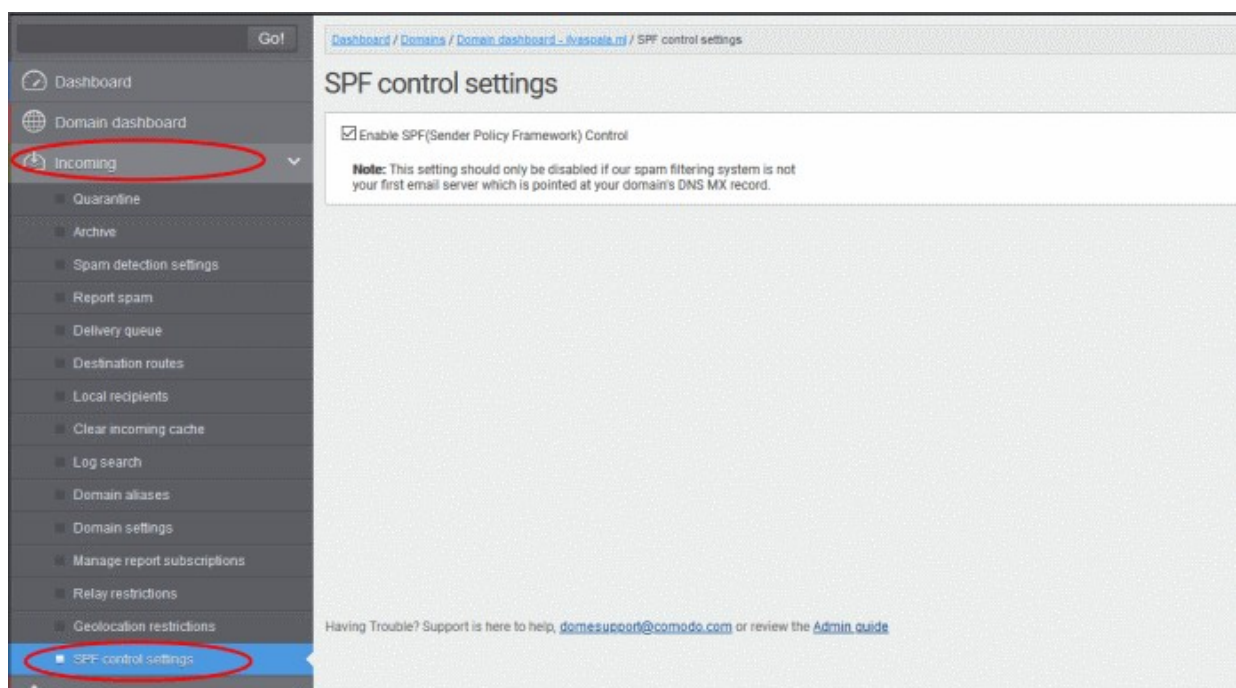
This file can be opened with Excel or Openoffice Calc.

SPF Control Settings

Sender Policy Framework (SPF) works by DNS records that specifies the authorized servers from which the emails are sent on behalf of domains. CASG is capable of checking if incoming are mails are originating from the authorized servers.

Configure SPF settings

- Click 'Incoming' on the left then click 'SPF Control Settings':



- **Enable SPF Control** – Select this to activate sender policy framework. If incoming mails are not sent from the authorized servers, the mails are rejected.

6.5.3 Outgoing

To send outgoing email, you need to add a valid user to the filter cluster. This can be done in the web interface.

The following ports are available for the outgoing service:

- SMTP AUTH: Port 25 or 587
- SMTP StartTLS Port 587
- SMTP SSL Port 465

Comodo recommends port 587. The outgoing service listens by default on all IPv4 addresses activated on the server.

- Create a separate outgoing user on the filtering cluster for each end-user to relay outgoing email. Use **automatic user locking** to close the account if abuse is detected.
- There are two methods you can for per-user authentication:
 - The first is to instruct all end-users to authenticate directly to the filter cluster for their outgoing emails.
 - The second is to configure your SMTP server to authenticate each user separately to the filter cluster for all outgoing mail.

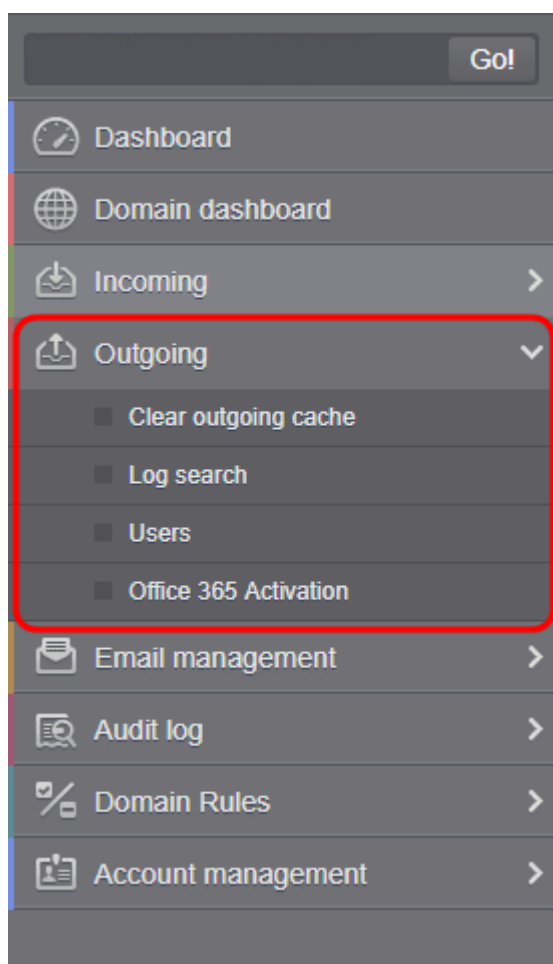
When using per-user authentication for outgoing mail, ensure you set usage limits correctly and enable automatic locking.

- If you find per-user authentication too cumbersome, you can use smarthost setup as an alternative.
- You add a single outgoing account to the filtering server and point all outgoing emails to this server, thus using the filter cluster as smarthost.
- Most email servers have a '**smarthost setting**' feature which lets you easily accomplish the task of configuring outgoing email filtering.
- Make sure to disable **automatic user locking** setting to prevent the full server account getting locked because a single user sent out spam. Also enable **block spam** so that individual spam messages will be stopped and the administrator notified.

While using smarthosting setup for outgoing mail filtering, ensure to set the limits correctly per user based on the server.

The 'Outgoing' area lets you:

- Set up spam checks on outgoing mail.
- Clear the outgoing mail server cache.
- Search for outgoing email messages.
- Integrate Office 365 with CDAS.



Click the following links for more details:

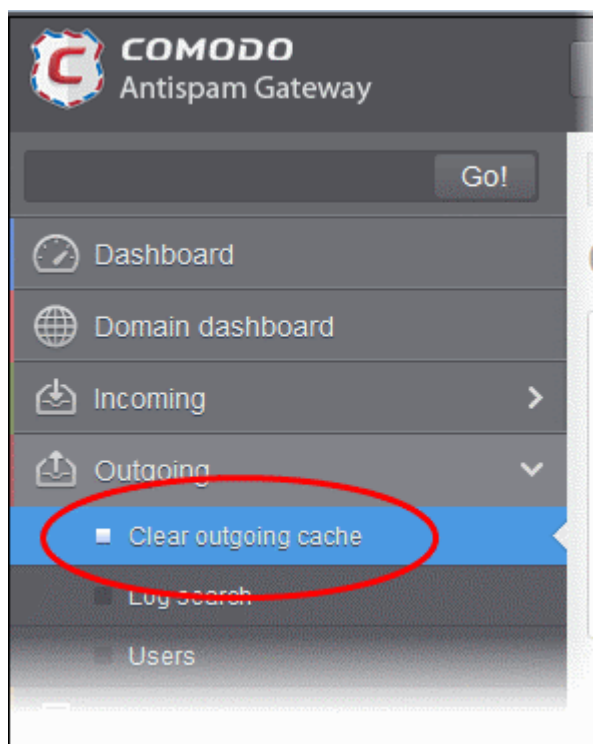
- [Clear outgoing cache](#)
- [Log search](#)
- [Users](#)
- [Office 365 Activation](#)

Clear outgoing cache

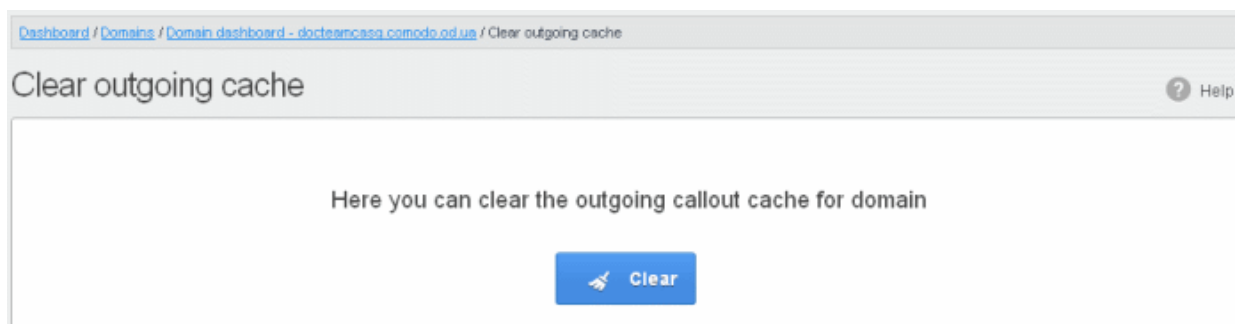
CASG checks that recipient email addresses at the destination mail server to minimize the number of recipient callouts. When an email for a certain recipient is permanently rejected by the destination server with a 5xx error code, the destination address of the recipient is considered invalid and all emails sent to the recipient are rejected. CASG caches this information locally for up to two hours. You have the option to clear the callout cache without waiting for the servers to clear it.

Clear outgoing cache

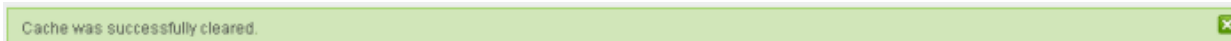
- Click 'Outgoing' > 'Clear outgoing cache':



- Click the 'Clear' button.

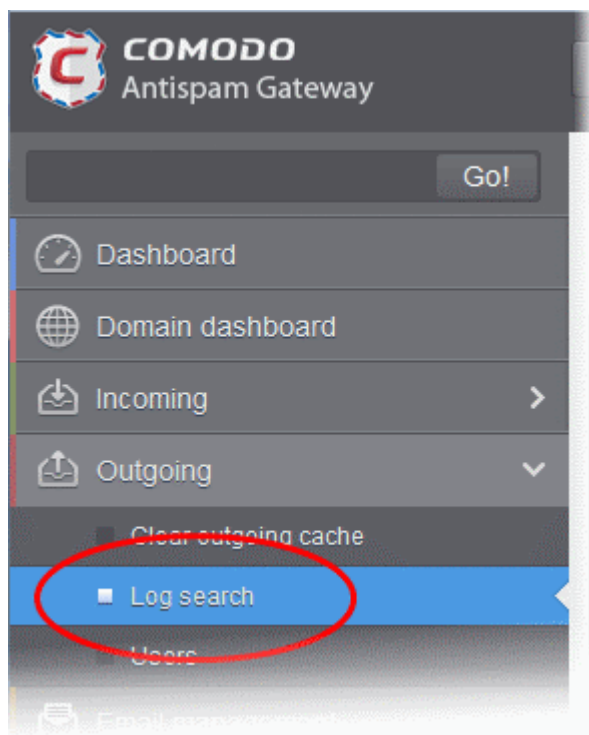


The call-out cache will be emptied:



Log search

- Click 'Outgoing' > 'Log Search':



- The 'Log Search (Outgoing)' interface is displayed:

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Log search (outgoing)

Log search (outgoing) Help

Date range: 2014-10-26 AM 11:38:40 - 2014-10-27 AM 11:38:40

Message ID:

Sender:

User: @docteamcasg.comodo.od.ua

Recipient:

Sender IP:

Sender host:

Predicate: AND

Classification: All

Include results from the last minutes:

- **Date range:** Select the date range for which you want to search the log file. The date range for which the log search can be processed depends on the settings configured in **Domain Settings** > Log retention period.

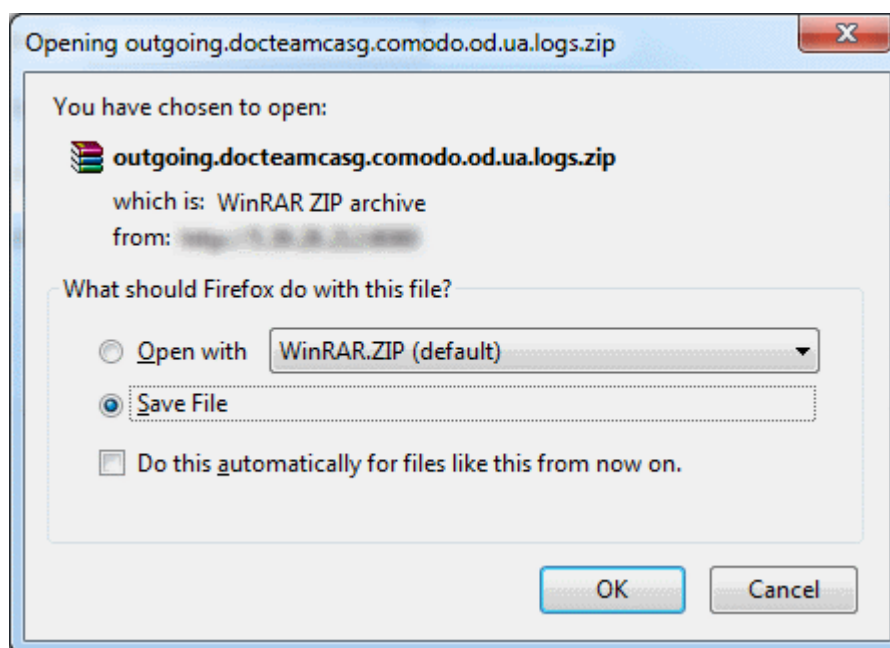
- **Message ID** - Enter a unique message identifier (*optional*)
- **Sender**: Enter the sender email address in this field.
- **User**: Enter the username of the outgoing email address for in this field (for example, 'testuser1').
- **Recipient**: Enter the email address in this field. (for example, 'testuser1@example.com').
- **Sender IP**: Enter the IP address of the sender.
- **Sender host**: Enter the sender host name.
- **Predicate**: There are two available options to select from the the drop-down: 'AND' or 'OR'
 - If 'AND' is selected - All the entered search terms will be searched together
 - If 'OR' is selected - The application will search any of the search items entered.
- **Classification**: Select the type of email that you want to search from the drop-down options.
- **Include results from the last minutes**: If selected, CASG will include messages that are currently being migrated from the filtering server to the logging server in the search results.

The option "Include results from the last minutes" will slow down the search result retrieval ✕

Click the 'Search' button. CASG will search for the entered terms and display the results.

Date and time	Host (Exim id)	Sender hostname	Sender	Recipient	Subject	Classification
2014-10-28 13:37:05	mxsrv1.spamgateway.cor 1Xj6xk-0008ET-B2	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo1	,DQ demo 2	Accepted Message content looked like non-spam
2014-10-28 13:37:05	mxsrv1.spamgateway.cor 1Xj6xk-0008ET-B2	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo2	,DQ demo 2	Accepted Message content looked like non-spam
2014-10-28 13:36:33	mxsrv1.spamgateway.cor 1Xj6wo-0007pb-Ag	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo1	,Re: DQ demo	Accepted Message content looked like non-spam
2014-10-28 13:36:33	mxsrv1.spamgateway.cor 1Xj6wo-0007pb-Ag	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo2	,Re: DQ demo	Accepted Message content looked like non-spam
2014-10-28 13:34:32	mxsrv2.spamgateway.cor 1Xj6up-00070G-Jb	mxsrv1.spamgateway.cor 178.33.199.65	demo@csg.comodo.od.u	demo1	,DQ demo	Rejected Rejected by relay restriction for this recipient
2014-10-28 13:34:32	mxsrv2.spamgateway.cor 1Xj6up-00070G-Jb	mxsrv1.spamgateway.cor 178.33.199.65	demo@csg.comodo.od.u	demo2	,DQ demo	Rejected Rejected by relay restriction for this recipient
2014-10-28 13:26:19	mxsrv1.spamgateway.cor 1Xj6ms-0008Pk-CK	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo2	Archive email 2	Accepted

- Click the 'Download' button to get a report on outgoing mail, including its delivery status.



Users

The content of outgoing emails should be checked because sending out spam / malware can damage your corporate reputation. Often the outbound email path bypasses the system that scans incoming emails from the internet, and instead sends the emails directly out to the destination. Filtering the outgoing user's mail also prevent spam from reaching end user mailboxes.

Configure User's Email Client for Outgoing Mail Filtering

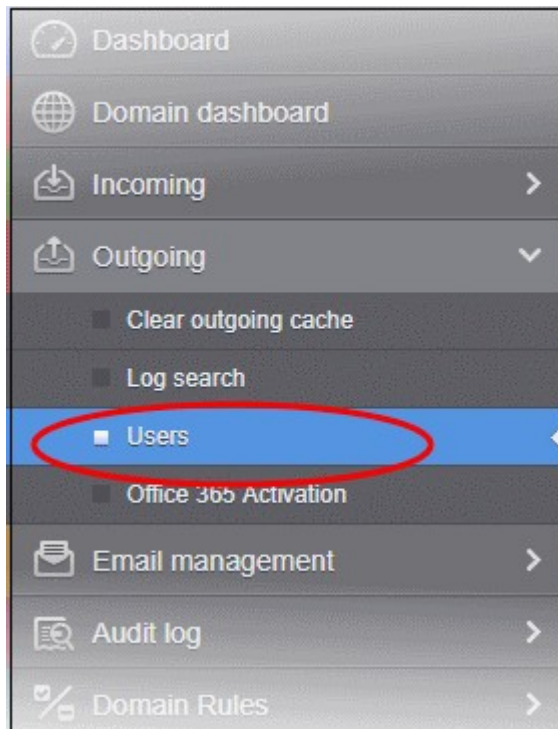
The email clients of the users added for outgoing email filtering must be configured to point to CASG service.

In the Account Settings interface of the user's email client, enter the following details:

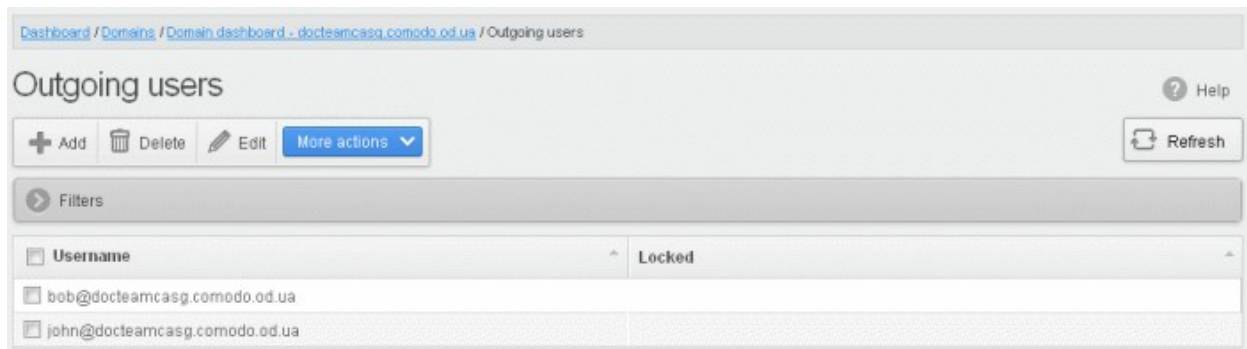
- Smtip server: mxpool1.spamgateway.comodo.com (for EU based service) or mxpool1.us.spamgateway.comodo.com (for US based service) according to your preferred **CASG service domain**.
- Connection Security: STARTTLS or SSL
- Port : 587
- Username: <username@domainname.com>

Open the outgoing users interface:

- Click 'Outgoing' > 'Users':

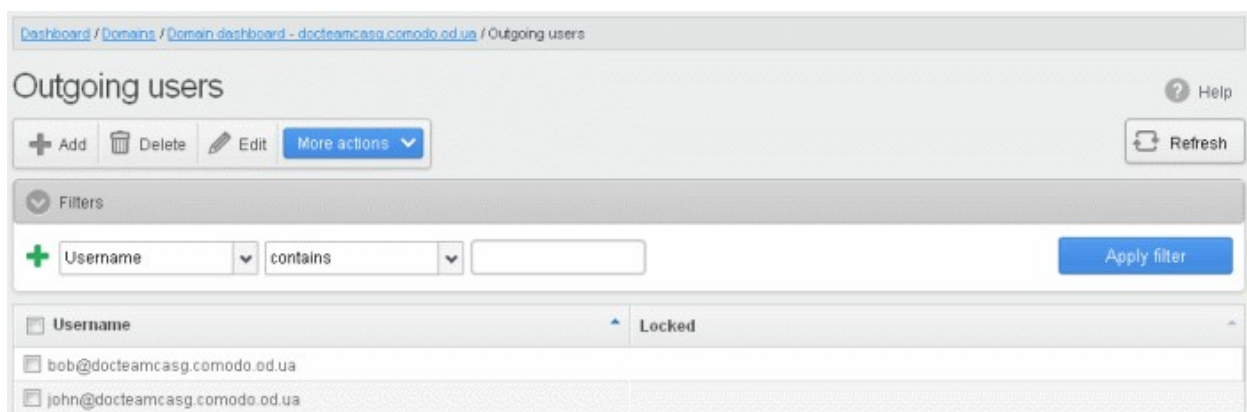


The 'Users' interface of the selected domain will be displayed:



Use filters to search for users


- Click anywhere on the 'Filters' strip to open the filters area:



You can filter results by the username:

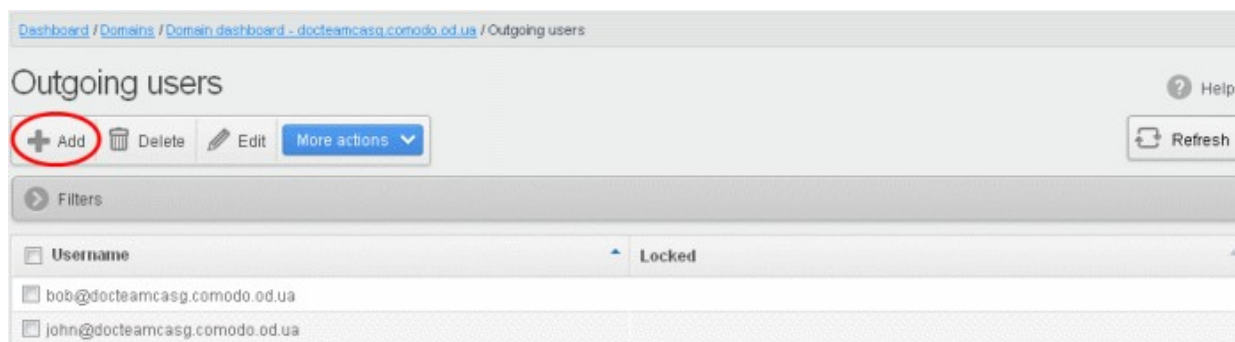
- **Username:** Type a user's email address in the text box (column 3) and select a condition in column 2.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

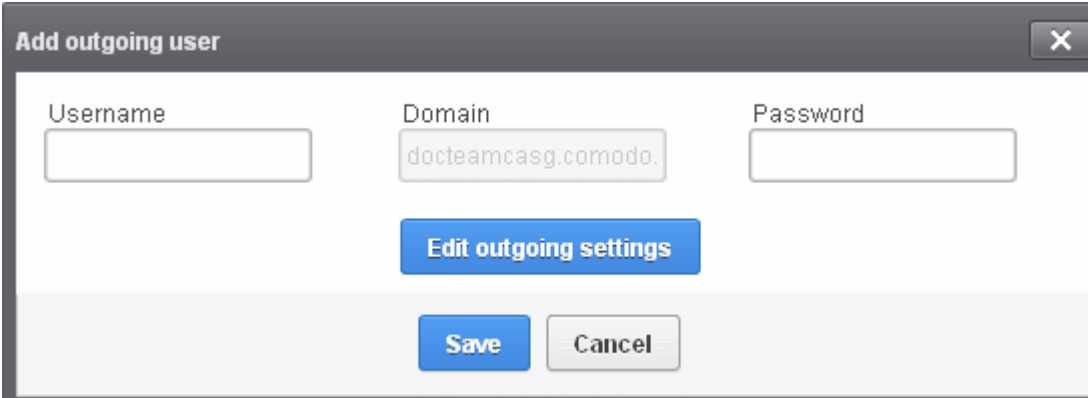
You can add multiple filters to the same search by clicking .

Add a new user

- Click the 'Add' button.



The 'Add outgoing user' dialog is displayed.



- Enter the username for the new outgoing user that will be first part of the email address. For example, testuser. The email address of the added user will be testuser@testdomain.com.
- Enter the password in the Password field. If the 'Password' field is left blank, then the 'Username' must be an IP address, and any connection from that IP will be considered authenticated without needing to use SMTP AUTH (Note: authorizing IP addresses may be disabled on the system).
- Click the 'Edit outgoing settings' button to configure outgoing settings for the user. The 'Add outgoing settings' dialog will expand:

Add outgoing user
✕

Username

Domain

Password

Automatic lock:

User lock timeout: ^ v

Maximum unlocks by timeout: ^ v

Enable outgoing limits:

Limit per month: ^ v

Limit per week: ^ v

Limit per day: ^ v

Limit per hour: ^ v

Limit per minute: ^ v

Valid sender address required:

Maximum number of recipients per day: ^ v

Invalid recipient limit: ^ v

Maximum days to retry: ^ v

Quarantine response: v

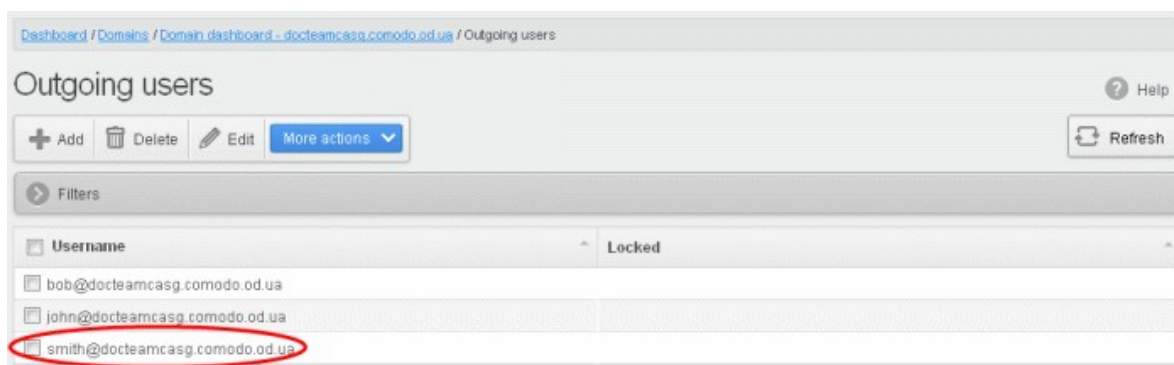
- **Automatic lock** - CASG will prevent a user from sending mail if it detects they have sent out spam or malware. You can set the length of this ban in the 'User lock timeout' field.
 - **User lock timeout** - Time in minutes that a user is banned from sending mail if CASG detects their account has sent spam. See 'Automatic lock' above.
- **Maximum unlocks by timeout** - The number of times the locked out user will be unlocked for sending out mails. After reaching the maximum limit, the user will be locked out from sending any mails till it is unlocked by the administrator.
- **Enable outgoing limits** - Activate / deactivate limits on outgoing mails.
 - **Limit per month** - The number of mails that can be sent per month
 - **Limit per week** - The number of mails that can be sent per week
 - **Limit per day** - The number of mails that can be sent per day
 - **Limit per hour** - The number of mails that can be sent per hour.
 - **Limit per minute** - The number of mails that can be sent per minute.
- **Valid sender address required** - If enabled, outgoing mails must have valid sender address.

- **Maximum number of recipients per day** - Maximum number of recipients that a user can send mails per day.
- **Invalid recipient limit:** - The number of invalid recipients that a user can send mails to.
- **Maximum days to retry** - Maximum number of days CASG will retry to send queued outgoing mails after which they are bounced to the user.
- **Quarantine response** - Determines the response that CASG will send to the SMTP server that delivered a message in the event that the mail is identified as spam.

Note: If you have enabled quarantine functionality, then spam/malicious mail will be quarantined (and not delivered to the recipient) regardless of your choice here. These options merely determine what message CASG will send back to the SMTP mail server.

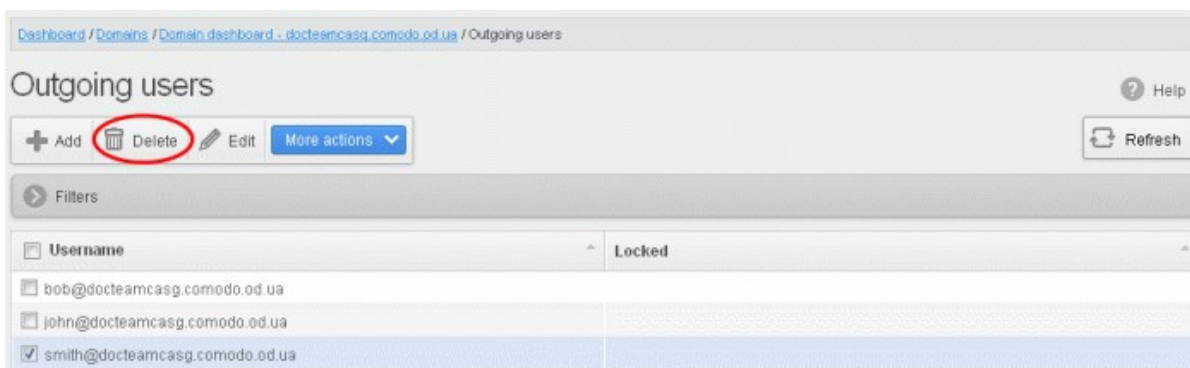
Options:

- **Rejected** - Will inform the SMTP server that the email wasn't delivered to recipient. (By default is 'Rejected'.)
 - **Accepted** - The senders will not be notified if the outgoing mails are detected as spam. They will be blocked and not delivered to recipients.
- Click the 'Save' button.

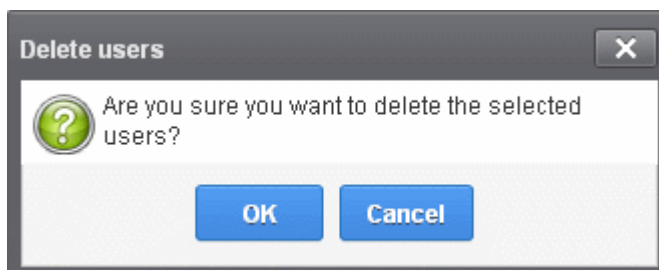


Delete an existing user

- Select the user you want to delete from the list and click the 'Delete' button.



Tip: You can select multiple users to delete by pressing and holding the Shift or Ctrl keys.

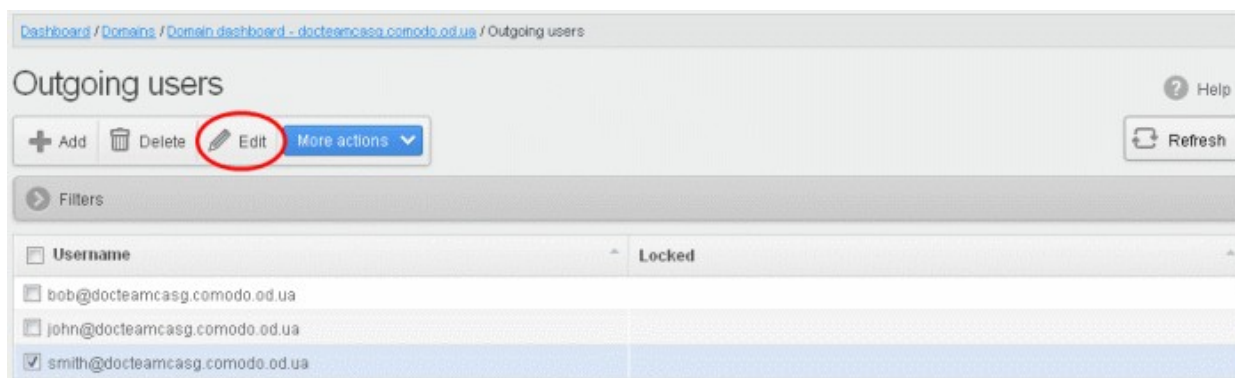


- Click 'OK' to confirm.

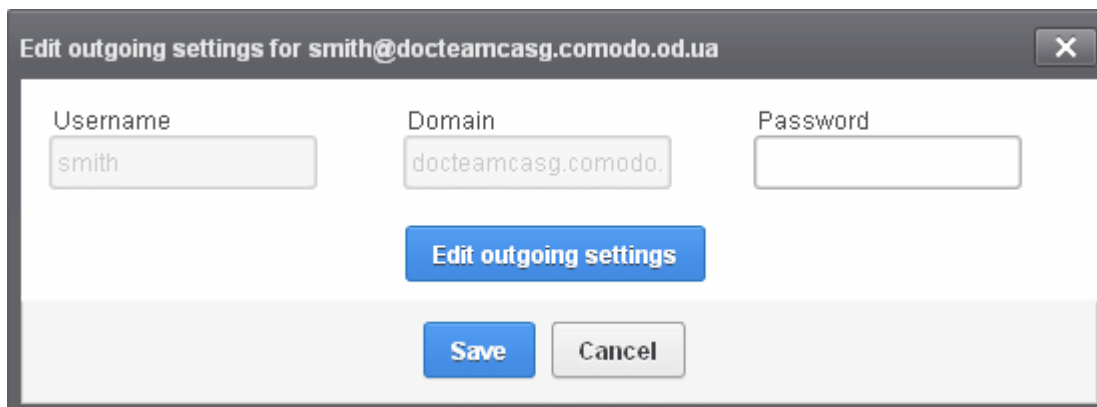
Edit an existing user

You can reset password, modify the outgoing settings configured from the 'Add outgoing user' interface.

- Select the user that you want to edit from the list and click the 'Edit' button.



- Click the 'Edit outgoing settings' button.



The 'Edit outgoing settings' is displayed.

Edit outgoing settings for testuser@demo.das.comodo.od.ua

Username: testuser Domain: demo.das.comodo.od Password: []

Edit outgoing settings

Automatic lock:

User lock timeout: 33

Maximum unlocks by timeout: 2

Enable outgoing limits:

Limit per month: 10

Limit per week: 5

Limit per day: 1000000

Limit per hour: 100000

Limit per minute: 15000000

Valid sender address required:

Maximum number of recipients per day: 10

Invalid recipient limit: 44

Maximum days to retry: 3

Quarantine response: Rejected

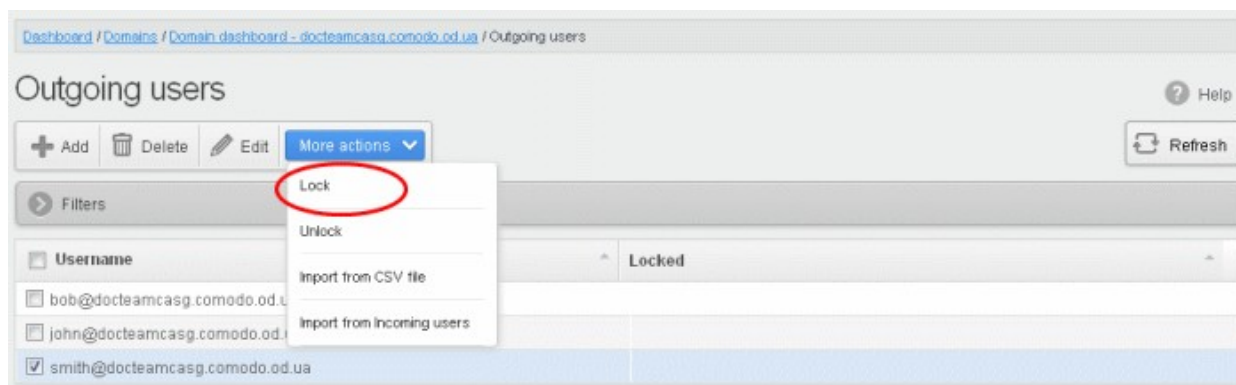
Save Cancel

- Reset the password and / or make other changes as explained in the **'Add outgoing user'** section.
- Click the 'Save' button to confirm your changes.

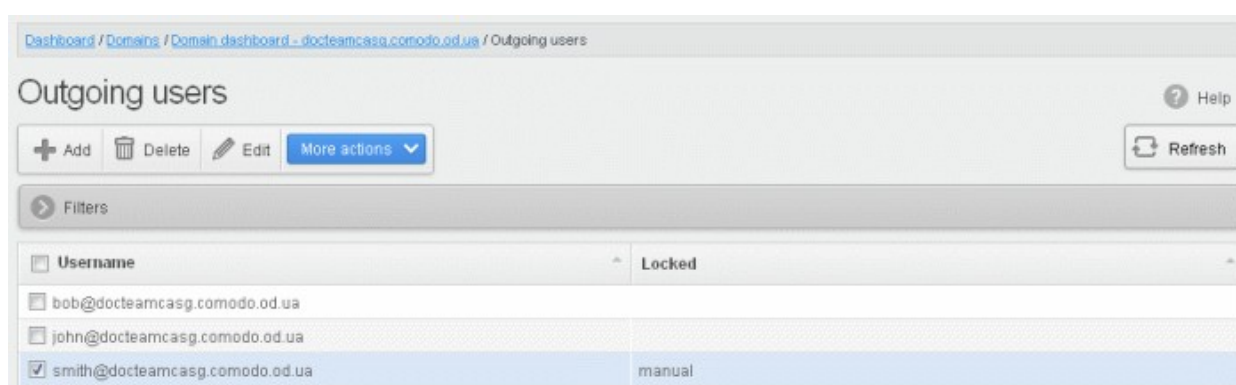
Manually lock outgoing user

Due to administrative or any other reason if you want to prevent a user from sending out mails, the Lock feature allows you to do so.

- Select the user that you want to lock, click 'More actions' drop-down > 'Lock'



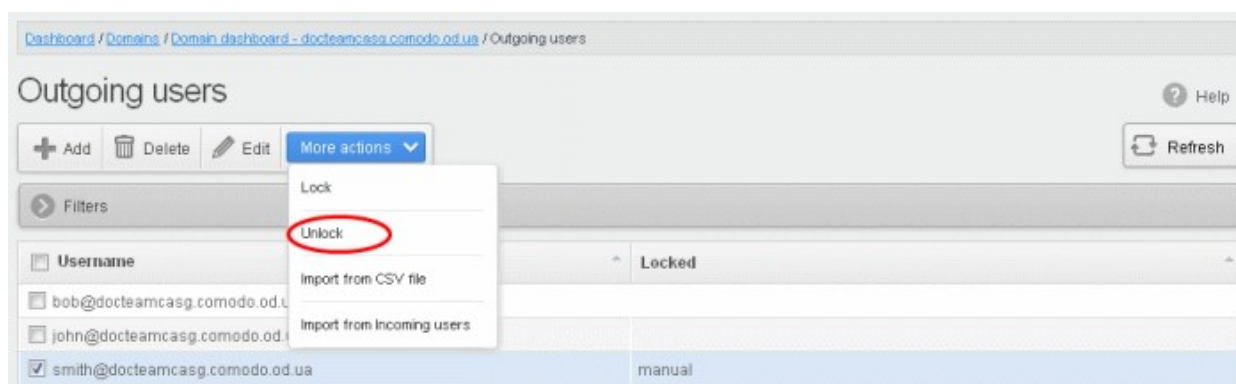
The selected user will be locked from sending mails with status 'Manual'.



Manually unlock outgoing user

A user who has been locked either manually or automatically (see [Edit outgoing settings](#)) can be unlocked from this interface.

- Select the user that you want to unlock, click 'More actions' > 'Unlock'.



The user will be unlocked and he can send mails.

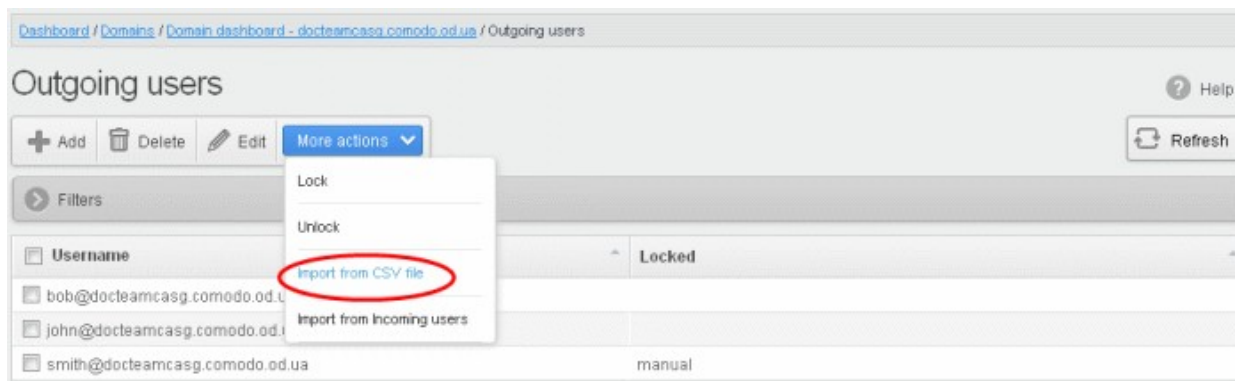
Import outgoing users from CSV file

Administrators can import many users from a file to the outgoing users list at a time. The users should be saved in the format shown below as an example:

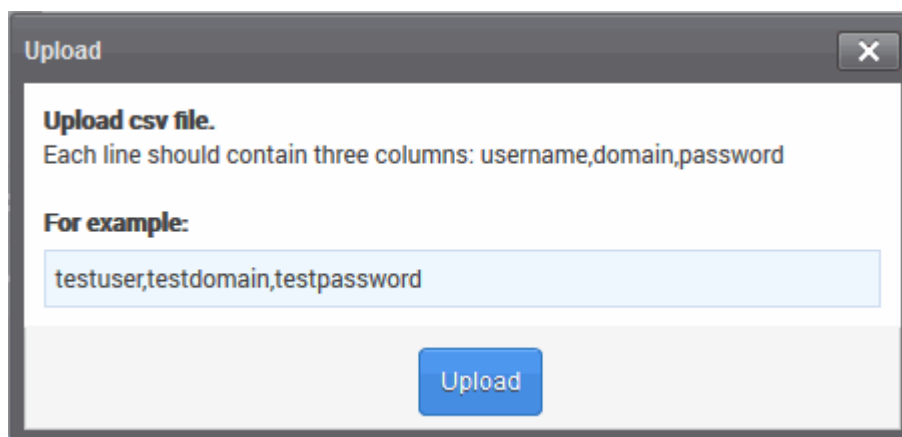
user1, domainname, password

user2, domainname, password

- To import outgoing users from a CSV file, click 'More actions' > 'Import from CSV file'

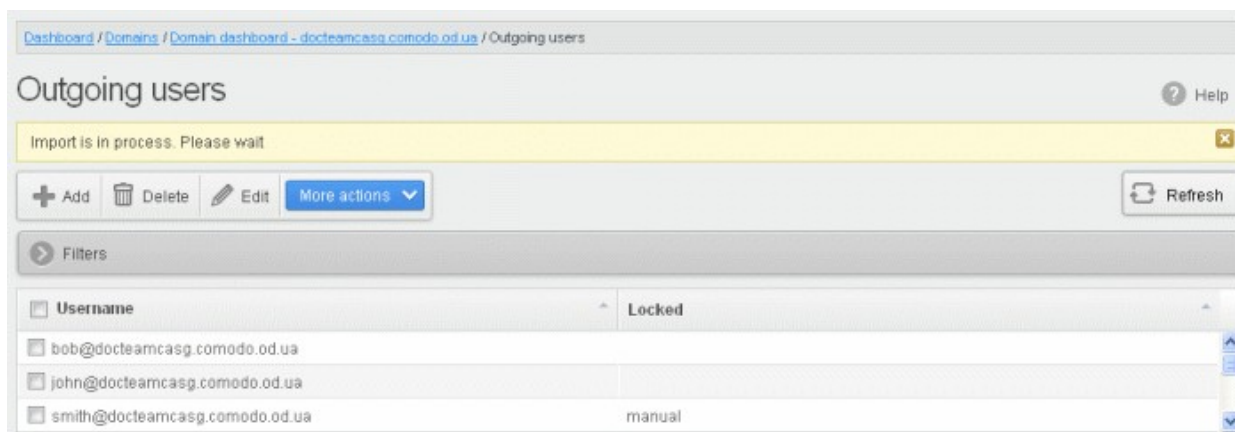


The Upload dialog will be displayed.



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

The upload progress will be displayed...



...and when completed, the results will be displayed.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Outgoing users

Outgoing users ? Help

Total lines processed 3 ✕

Imported 3 user(s) ✕

Import for domain docteamcasg.comodo.od.ua has been finished ✕

+ Add 🗑 Delete ✎ Edit More actions ▾ 🔄 Refresh

Filters

<input type="checkbox"/> Username	Locked
<input type="checkbox"/> bob@docteamcasg.comodo.od.ua	
<input type="checkbox"/> john@docteamcasg.comodo.od.ua	
<input type="checkbox"/> king@docteamcasg.comodo.od.ua	
<input type="checkbox"/> prince@docteamcasg.comodo.od.ua	
<input type="checkbox"/> queen@docteamcasg.comodo.od.ua	
<input type="checkbox"/> smith@docteamcasg.comodo.od.ua	

The administrator who carried out the task will receive a notification about the import task completion.

Import from incoming users

Administrators can add all incoming users to the outgoing users list by importing. If there is an outgoing user with the same name, the import of incoming user will be skipped.

- To import outgoing users from incoming users, click 'More actions' > 'Import from Incoming users'

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Outgoing users

Outgoing users ? Help

+ Add 🗑 Delete ✎ Edit More actions ▾ 🔄 Refresh

Filters

<input type="checkbox"/> Username	Locked
<input type="checkbox"/> bob@docteamcasg.comodo.od.ua	
<input type="checkbox"/> john@docteamcasg.comodo.od.ua	
<input type="checkbox"/> smith@docteamcasg.comodo.od.ua	

More actions menu:

- Lock
- Unlock
- Import from CSV file
- Import from incoming users**

The upload progress will be displayed...

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Outgoing users

Outgoing users ? Help

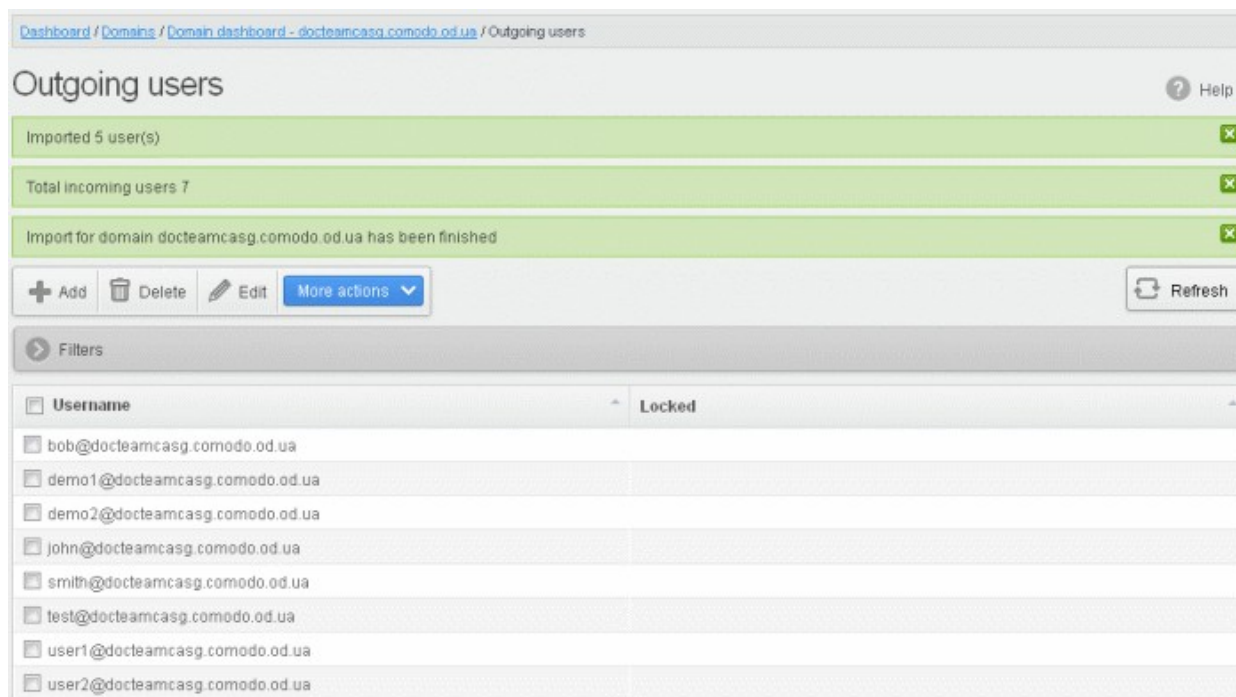
Import is in process. Please wait ✕

+ Add 🗑 Delete ✎ Edit More actions ▾ 🔄 Refresh

Filters

<input type="checkbox"/> Username	Locked
<input type="checkbox"/> bob@docteamcasg.comodo.od.ua	
<input type="checkbox"/> john@docteamcasg.comodo.od.ua	
<input type="checkbox"/> smith@docteamcasg.comodo.od.ua	

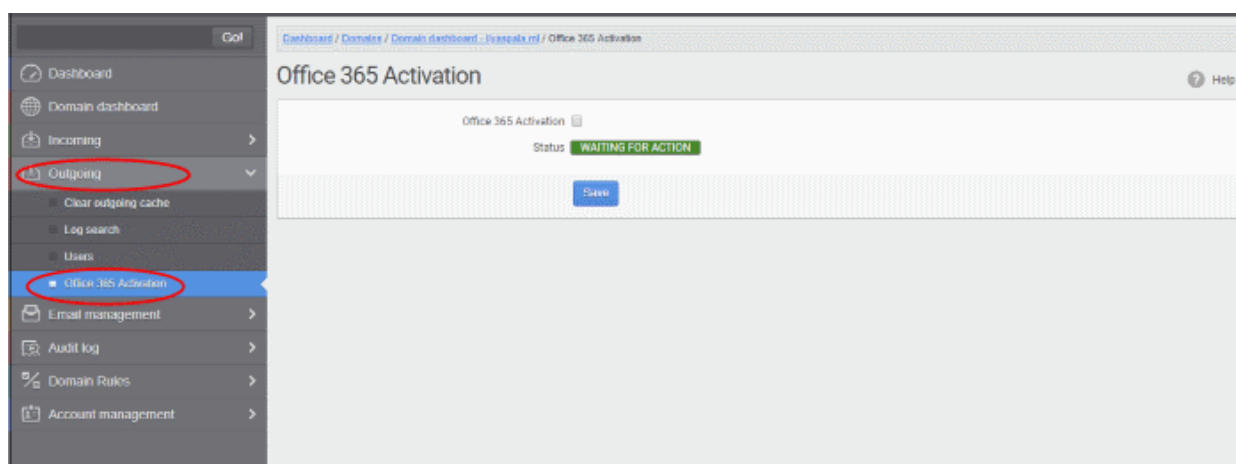
...and when completed, the results will be displayed.



The administrator who carried out the task will receive a notification about the import task completion.

Office 365 Activation

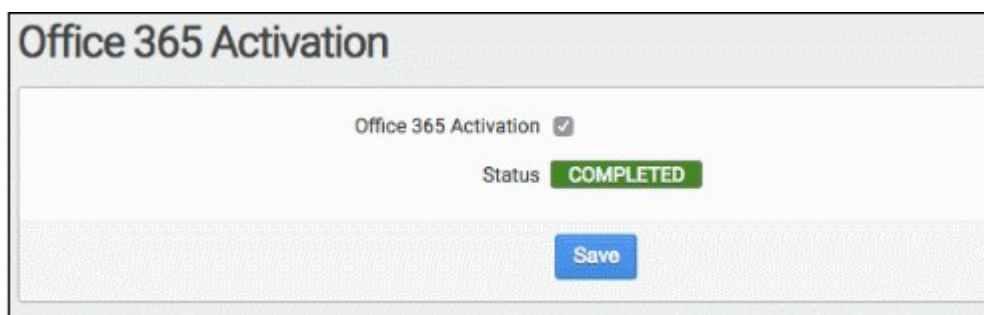
- You can integrate Office 365 with CASG so outgoing emails pass through the antispam filters
- After integration, you have to set up an 'Outbound Connector' in Office 365.
- Click 'Domains' > Select the domain you want to integrate > Click 'Manage domain'
- Click 'Outgoing' > 'Office 365 Activation' to start the integration process:



- Select 'Office 365 Activation' and click 'Save'



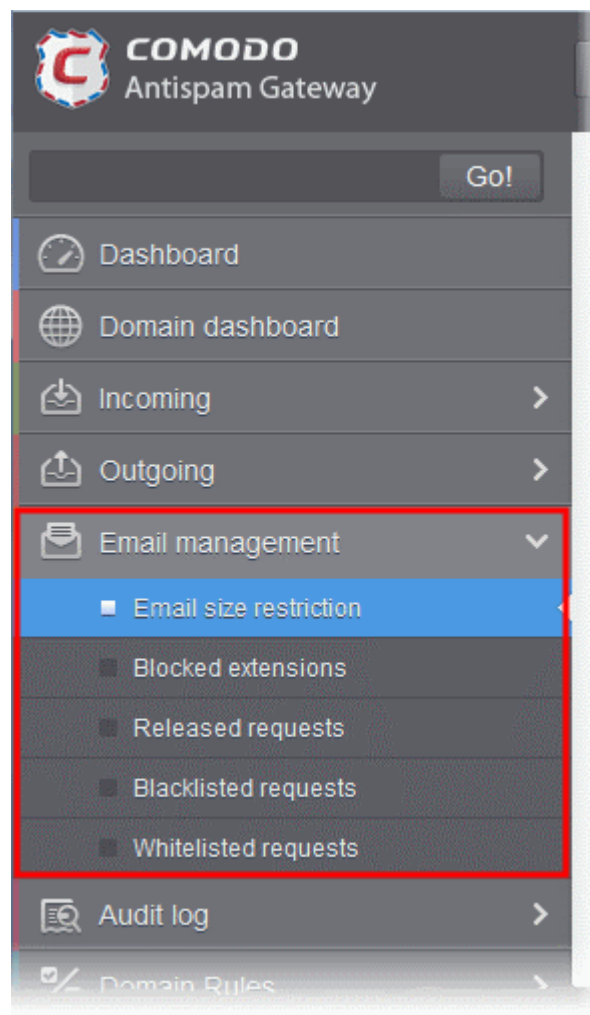
- The activation request is submitted and the status will change to 'In Progress'
- Comodo will make the necessary configuration changes. Once finished, the status will change to 'Completed'.



- The next step is for you to set up an outbound connector in your Office 365 account. This will relay and filter outgoing email traffic via CASG.
- [Click here](#) to find out how to set up an Office 365 outbound connector.

6.5.4 Email Management

- CASG lets you define the maximum size of an email and choose which file types are acceptable as attachments.
- You can also accept or reject user requests. Users can request that you release quarantined mail, or add senders to the blacklist/whitelist.



Click the following links for more details:

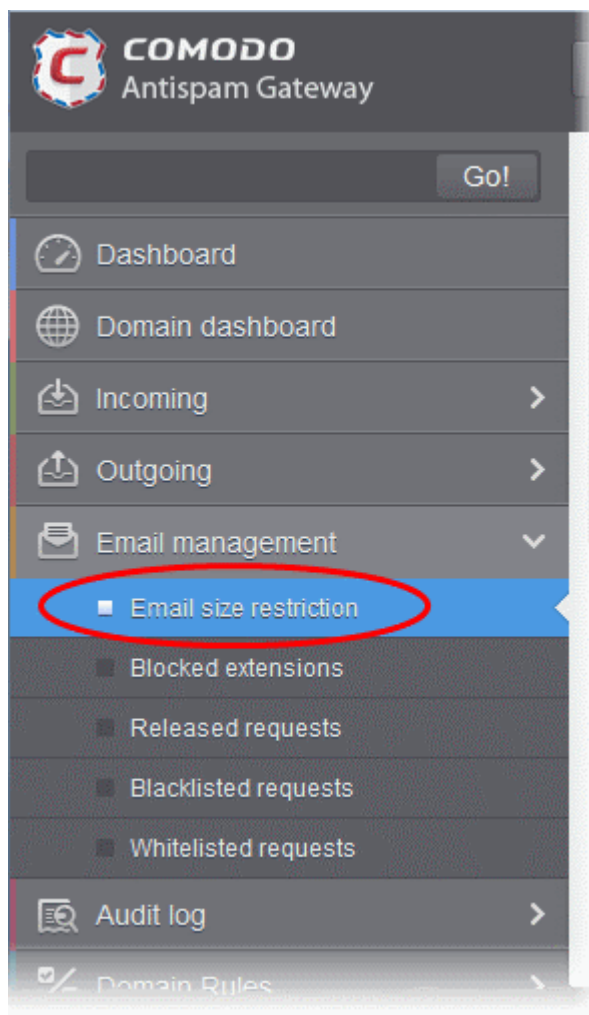
- [Email size restriction](#)
- [Blocked extensions](#)
- [Released requests](#)
- [Blacklisted requests](#)
- [Whitelisted requests](#)

Email Size Restriction

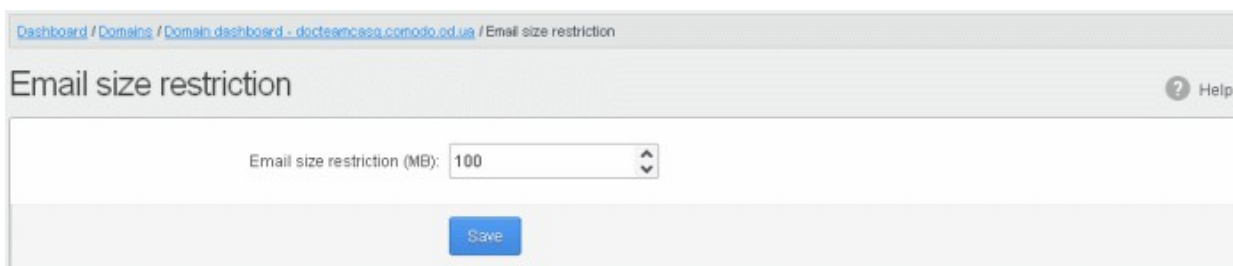
- CASG lets you set the maximum size of an email to preserve bandwidth and storage space.
- You can set the max size anywhere up to 250 MB.
- Contact your account manager if you need sizes above 250 MB. Alternatively, open a ticket at support.comodo.com or call 1.888.COMODO (266.6361). Please have your account number ready.

Set email size restriction

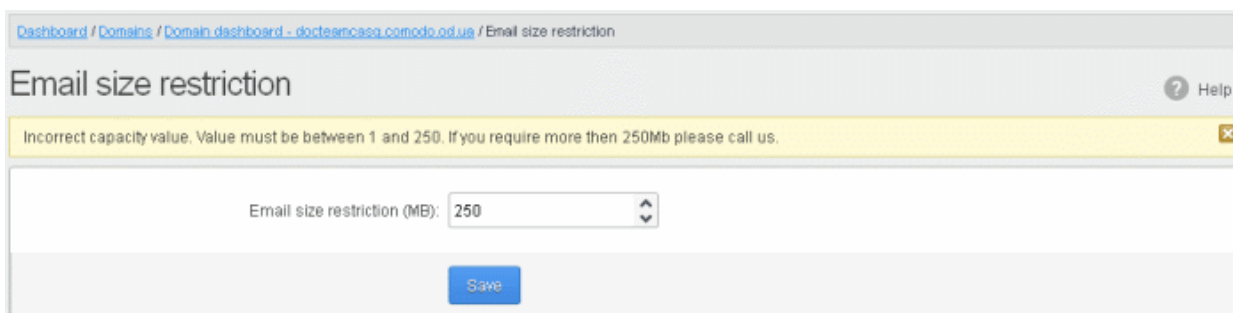
- Click 'Email management' > 'Email size restriction'



- The 'Email restrictions' interface of the domain selected will open:



- Enter the maximum allowed size (up to 250 MB) of an email. Incoming and outgoing emails larger than the value set here will be rejected.
- If you enter a value more than 250 MB, an alert will be displayed to contact your account manager at Comodo. The email size will be automatically set to 250 MB.



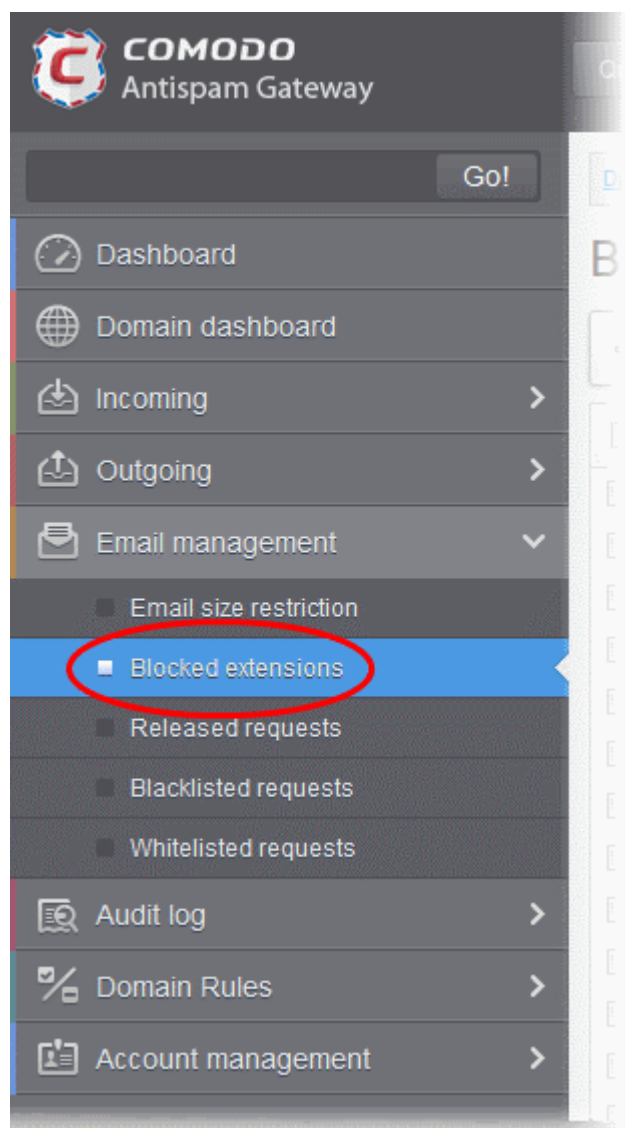
- Click 'Save' to confirm your changes.

Blocked Extensions

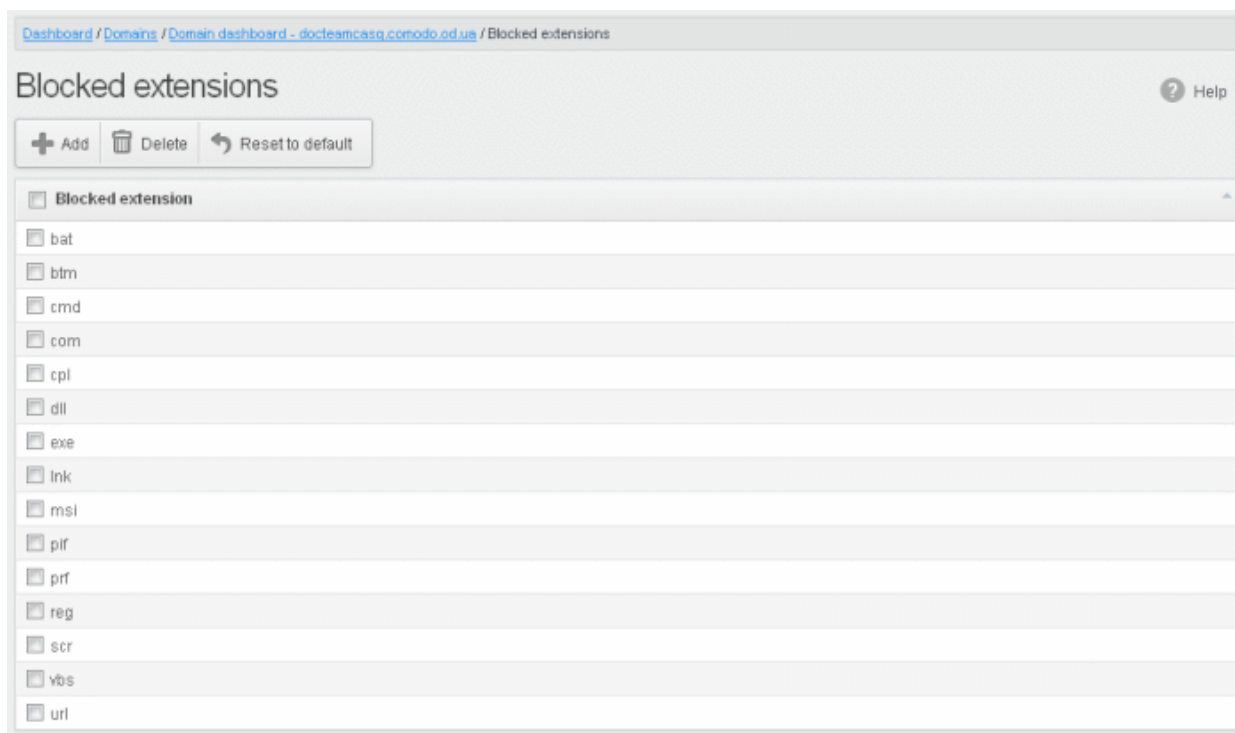
- You can automatically block email attachments with specific file extensions.
- For example, you may want to block all attachments with a .exe extension because they may contain malware. [Click here](#) to see the complete list of extensions that you can block.
- Note – If you have enabled containment in 'Incoming' > 'Spam Detection Settings', then CASG will automatically block malicious files and attachments.

Add a blocked file extension

- Click 'Email management' on the left then click 'Blocked extensions'

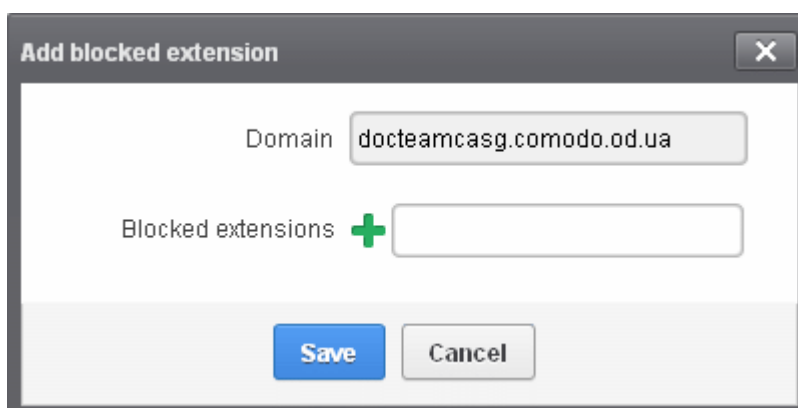


The 'Blocked extensions' interface of the domain will open:




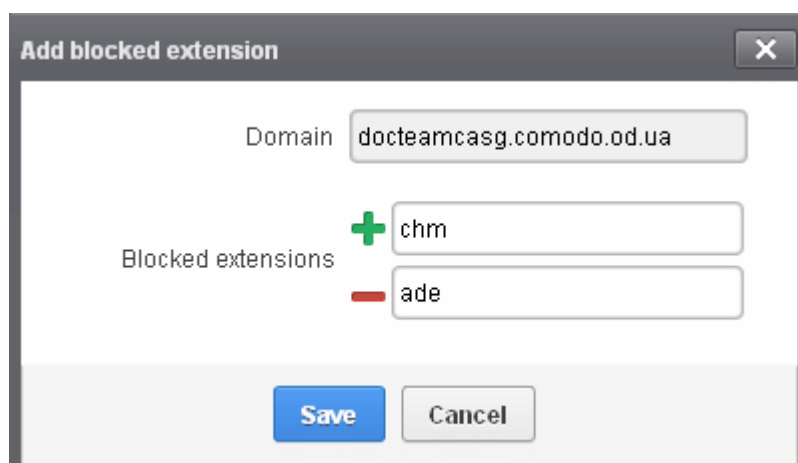
A list of default blocked extensions is displayed. You can sort the blocked extensions list alphabetically in ascending or descending order by clicking the 'Blocked extensions' title bar.

- Click the 'Add' button to include another blocked extension:



- Enter the extension name to be blocked in the text box

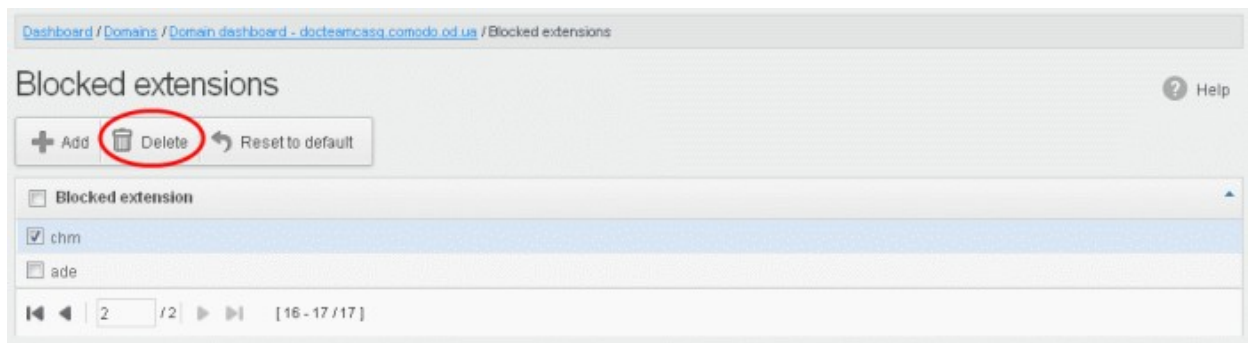
You can add many extensions at a time by clicking the  icon.



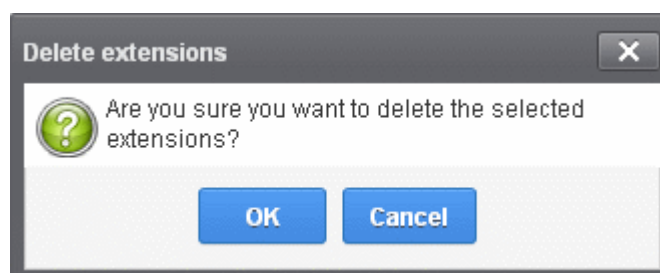
- Click the 'Save' button

The entered extensions will be added to the list.

- To delete an extension, select it from the list and click 'Delete' on the top left



An alert will be displayed to confirm to delete the selected extensions.



The selected blocked extension will be deleted from the list and email attachment with this file extension will be allowed provided it passes the size restriction filter.

- Click 'Reset to default' to restore default blocked extensions in CASG.

List of blocked Extensions

ade	csf	lib	msh	psc1	vbe
adp	dll	lnk	msh1	psc2	vbs
air	exe	mad	msh1xml	pst	vbscript
app	gadget	maf	msh2xml	reg	vsm
as	hlp	mag	mshxml	rgs	vsmacros
asf	hta	mam	msi	scf	vss
asp	html	maq	msh	scr	vst
asx	htr	mar	mst	script	vsw
bas	iim	mas	nexe	sct	vxd
bat	inf	mat	nws	sh	widget
bin	ins	mau	ocx	shb	wmd
btm	inx	mav	ops	shs	wmf
cab	isp	maw	otm	swf	wms
cer	isu	mda	paf	sys	wmz
chm	its	mdb	pcd	tmp	ws
cil	jar	mde	pif	u3p	wsc
cmd	job	mdt	prf	udf	wsf
com	js	mdw	prg	upx	wsh
cpl	jse	mdz	ps1	url	xap
crt	ksh	msc	ps1xml	vb	xml

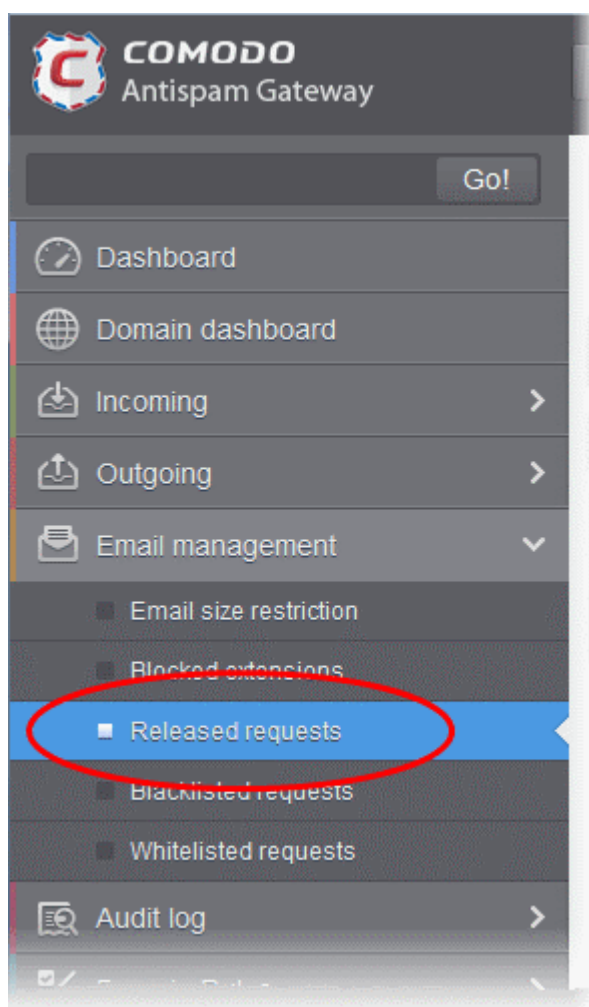
Released Requests

- Users can request that you release their quarantined emails to them. You can choose to accept or reject these requests.
- The release requests will be displayed in the interface and sent to admins whose email addresses were added to the **notification email field**
- Users who requested the release will also receive notifications.

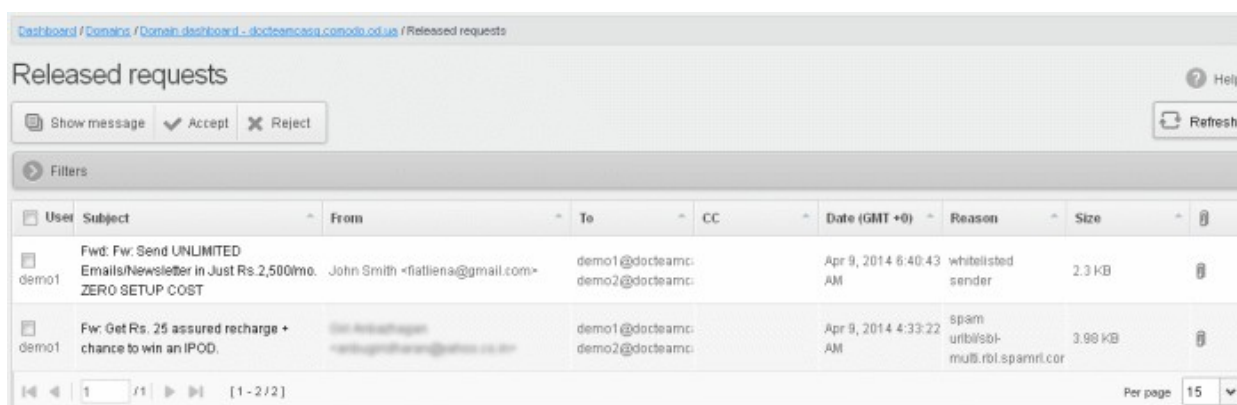
Note: Users who have been designated as 'power users' can release quarantined mails without admin approval. See **'User Groups & Permissions'** and **'Managing Permissions'** for more details.

Open the released requests interface

- Click 'Email management' on the left then click 'Released requests'



The 'Release requests' interface will open:



All current requests will be shown. Each row shows information about the requested user, subject, the sender, details of the recipients, details of recipients in CC list, the date they were sent and more.

View Details of Release Requested Mails

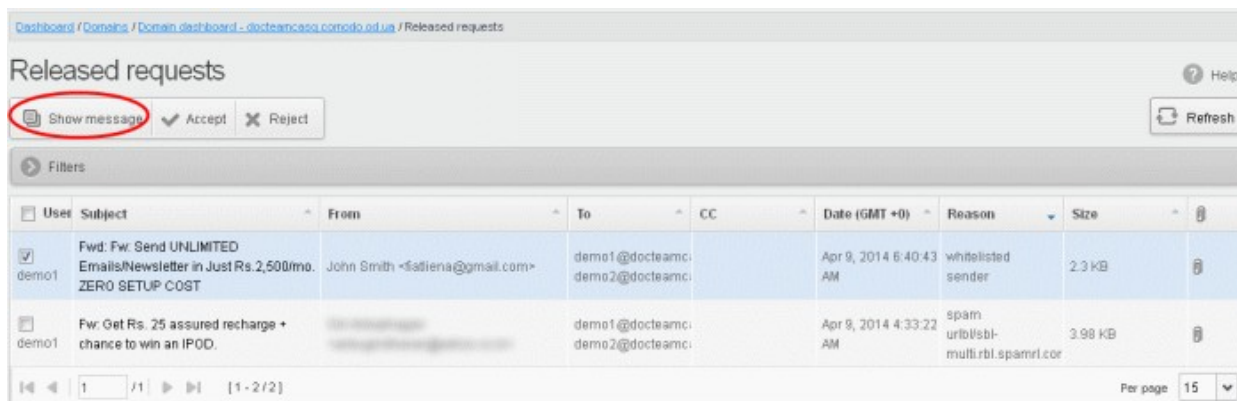
The details such as user, subject, sender, recipient, date, reason and size of the mails requested for release can be viewed in two ways:

- **In the same CASG window**
- **In a new CASG window**

View details of release requested mails in the same CASG window:

- Click 'Email Management' then 'Released requests'

- Select the mail that you want to view and click the 'Show Message' button.
- OR
- Click the email link in the subject column to view its details.



The details of the selected email will be displayed.



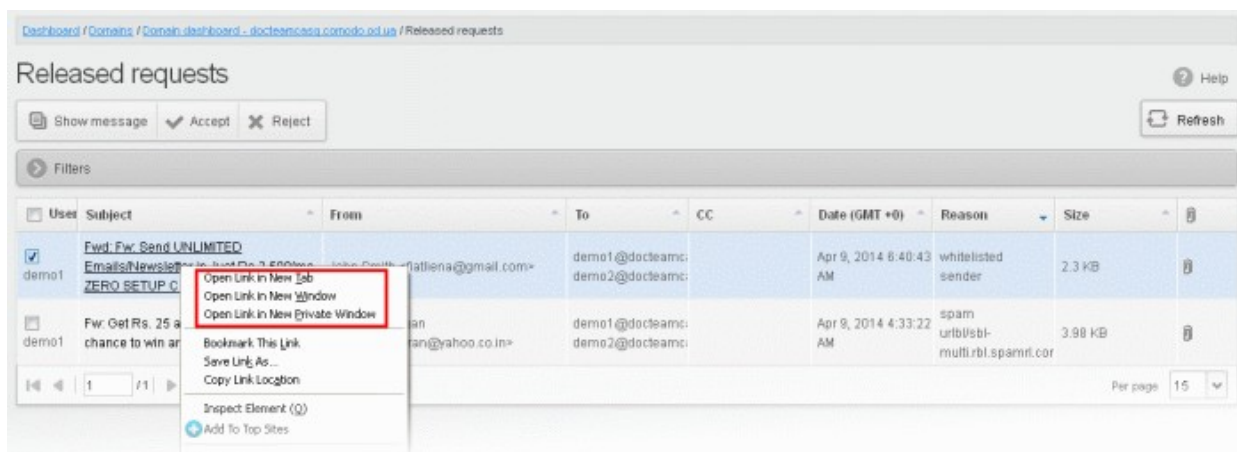
- To view email headers, which contain the tracking information of the mail details about the path it has crossed before reaching the recipient, click 'All headers' tab.

The headers give full details of the sender, route, recipient, sent date, mail type and so on and enable you to check the authenticity of the mail.

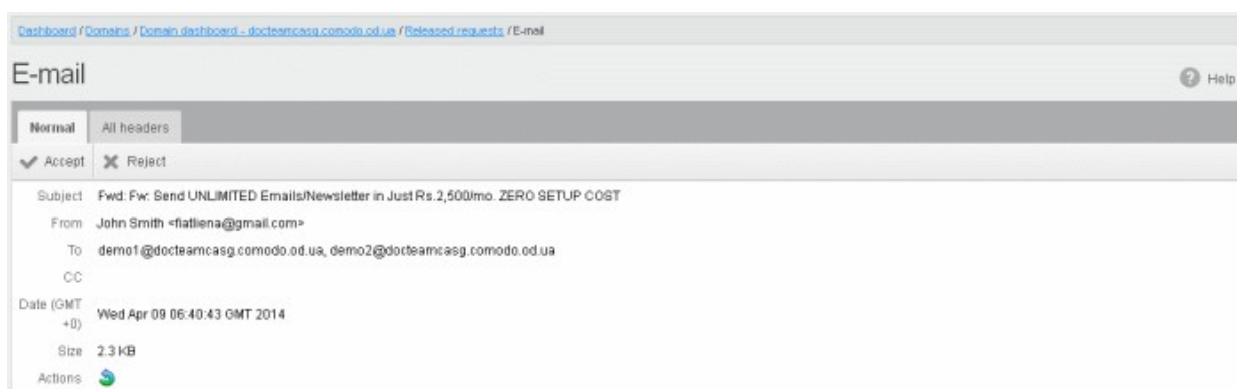
Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either **accept** the mail or **reject** it. If the mail is accepted, it will be released to the user's inbox. If it is rejected, the email will no longer be in the released emails list. Please note that emails will continue to remain in the **'Quarantined'** list irrespective of the action taken.

View details of release requested mails in a new CASG window:

- Click 'Release request' and select the mail that you want to view
- Right-click on the email link in the subject column and select 'Open link in New Tab' or 'Open Link in New Window' to open in a new tab or new window.



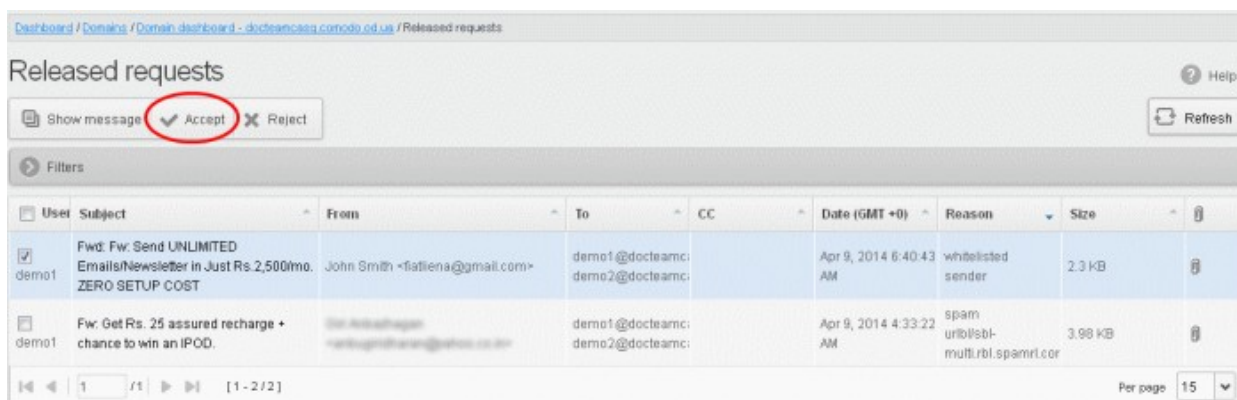
The details of the selected mail will be displayed in a new CASG window.



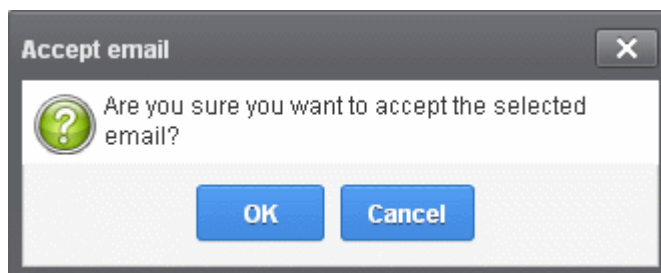
Accept the release request from users

After viewing the details and ensuring that the selected email is not a spam you can choose to release the mail to the recipient.

- Select the mail that you want to release and click the 'Accept' button.



An alert will be displayed to confirm the release of selected email to the requested user.



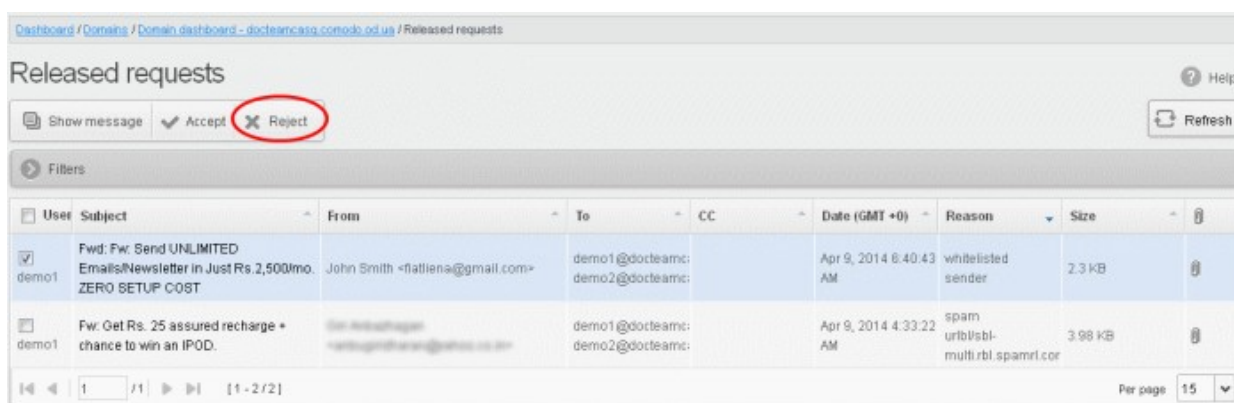
- Click 'OK' to confirm the release.

The email will be released to the user and the mail will no longer be in the released mail list. The mail will be removed from the quarantine area and it will be archived if archive space is available for the domain.

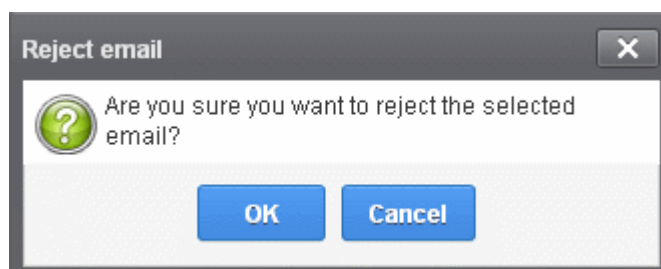
Reject the release request from users

After viewing the details of the email and if not satisfied with its authenticity you can choose to reject the request from the user.

- Select the mail that you want to reject and click the 'Reject' button.



An alert will be displayed to confirm the rejection of selected email.



- Click 'OK' to confirm the rejection.

The email will not be released to the user and the mail will no longer be in the released mail list. However, it will continue to remain in the **Quarantined** list.

Use filters to search release requests

- Click anywhere on the 'Filters' tab to open the filters area.

Released requests

Show message Accept Reject Refresh

Filters

Subject contains [] Apply filter

Subject contains []


	From	To	CC	Date (GMT +0)	Reason	Size	
demo1	John Smith <f1atiena@gmail.com>	demo1@docteamc; demo2@docteamc;		Apr 9, 2014 6:40:43 AM	whitelisted sender	2.3 KB	
	Fw: Get Rs. 25 assured recharge +	Siti Arbachagan	demo1@docteamc;	Apr 9, 2014 4:33:22	SPAM		

- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

- **Subject:** Type the email subject in the text box (column 3) and select a condition in column 2.
- **From:** Enter the sender name or address in the text box (column 3) and select a condition in column 2.
- **To:** Enter the recipient name or address in the text box (column 3) and select a condition in column 2.
- **Date:** Search by date and time mails quarantined. Select the date (column 3) and select a condition in column 2.
- **Reason:** Enter the quarantined reason in the text box (column 3) and select a condition 2.
- **Size (KB):** Search quarantined mails by their size. Select or enter the mail size in column 3 and select a condition in column 2.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

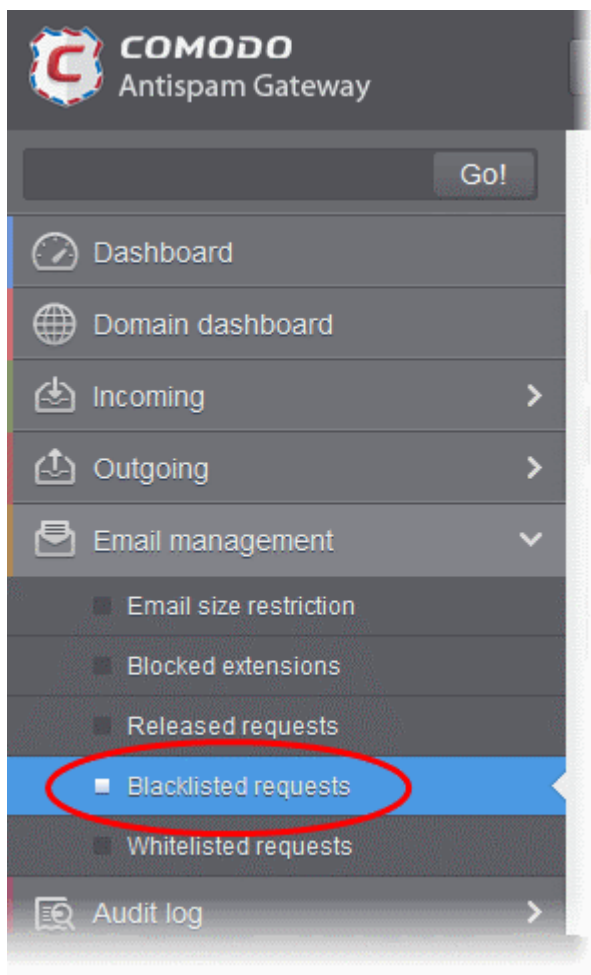
You can add multiple filters to the same search by clicking  .

Blacklisted Requests

- The 'Quarantine' interface lets users view emails intended for them but moved to quarantine.
- The interface also lets users request that senders of quarantined mails are added to the blacklist.
- The blacklist request will be sent to you via email and also added to the Email Management > Blacklist Requests interface. You can approve or reject the requests.
- Senders added to the blacklist after a request will only be blacklisted for the requester.
- Subsequent mails from the sender to the user in question will be rejected. This applies even if the sender is in the general sender whitelist.
- See [Sender Whitelist](#) and [Blacklist Senders Per User](#) for more details.

View blacklisted requests

- Click 'Email management' on the left then select 'Blacklisted requests'



The 'Blacklisted requests' interface will open:

Dashboard / Domains / Domain dashboard - docteam@comodo.net.us / Blacklisted requests

Blacklisted requests ? Help

Show message Accept Reject Refresh

Filters

<input type="checkbox"/>	User	Subject	From	To	CC	Date (GMT +0)	Reason	Size	<input type="checkbox"/>
<input type="checkbox"/>	demo1	Fwd: Fw: Send UNLIMITED Emails! Newsletter in Just Rs. 2,500/mo. ZERO SETUP COST	John Smith <fatiana@gmail.com>	demo1@docteamc: demo2@docteamc:		Apr 9, 2014 6:40:43 AM	whitelisted sender	2.3 KB	<input type="checkbox"/>
<input type="checkbox"/>	demo1	Fw: Get Rs. 25 assured recharge + chance to win an IPOD.	docteamc@docteamc.com	demo1@docteamc: demo2@docteamc:		Apr 9, 2014 4:33:22 AM	spam urlblsbi-multi.rbl.spamr1.com	3.98 KB	<input type="checkbox"/>
<input type="checkbox"/>	demo1	Fw: Register and Get Rs. 5000 to Shop Now! Introducing Pepperfry.com - India's L...	docteamc@docteamc.com	demo1@docteamc: demo2@docteamc:		Apr 9, 2014 4:32:36 AM	spam urlblim-uri.rbl.spamr1.com	3.05 KB	<input type="checkbox"/>
<input type="checkbox"/>	demo1	Fw: We have free samples for you, now try before you buy @ your doorsteps!	docteamc@docteamc.com	demo1@docteamc: demo2@docteamc:		Apr 7, 2014 6:52:31 AM	spam urlblim-uri.rbl.spamr1.com	3.02 KB	<input type="checkbox"/>
<input type="checkbox"/>	demo1	test spam email 1	docteamc@docteamc.com	demo1@docteamc:		Apr 2, 2014 2:28:40 PM	spam External pattern match (Sanesecurity.Junk)	8.16 KB	<input type="checkbox"/>

1 / 1 [1 - 5 / 5] Per page 15

The interface shows all blacklist requests from users. The list has columns which show requesting user, subject, sender, recipients, CC list, date sent, the reason they were quarantined and the size of the email. The last column shows whether there is any attachment with the mail.

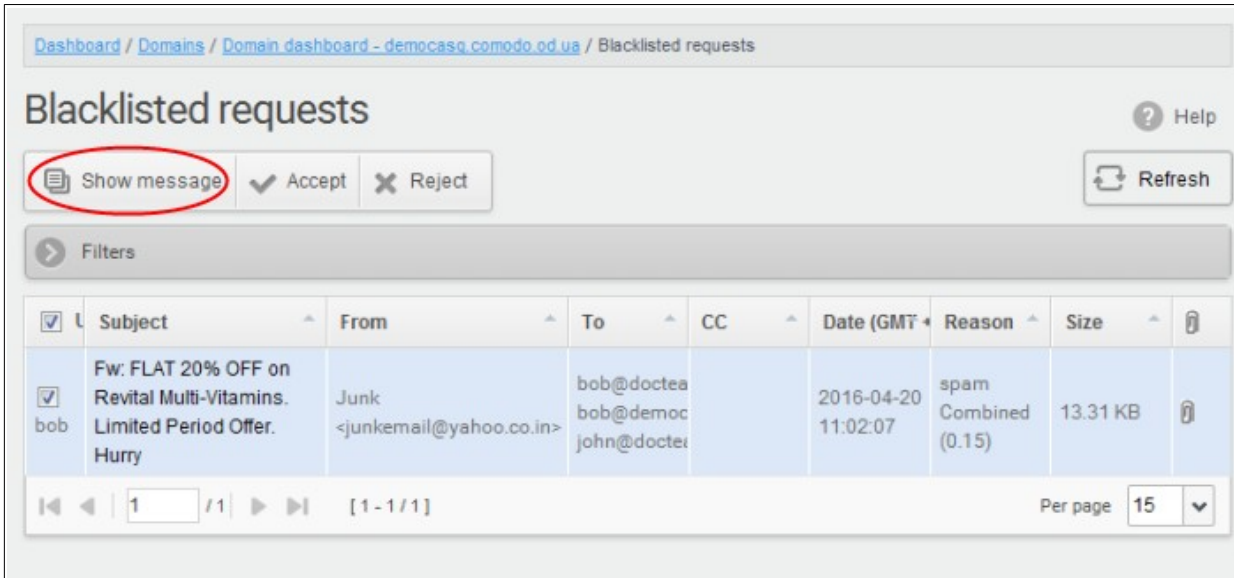
View Details of Blacklisted Requests

The details such as user, subject, sender, recipient, date, reason and size of the mails requested for blacklisting can be viewed in two ways:

- **In the same CASG window**
- **In a new CASG window**

View details of blacklisted requests in the same CASG window:

- Select the mail that you want to view and click the 'Show Message' button.
- OR
- Click on the email link in the subject column that you want to view its details.



The screenshot displays the 'Blacklisted requests' section of the Comodo Antispam Gateway. At the top, there is a breadcrumb trail: [Dashboard](#) / [Domains](#) / [Domain dashboard - democasg.comodo.od.ua](#) / [Blacklisted requests](#). Below this, the title 'Blacklisted requests' is shown with a 'Help' icon. A toolbar contains three buttons: 'Show message' (circled in red), 'Accept', and 'Reject', along with a 'Refresh' button. A 'Filters' section is visible below the toolbar. The main content is a table with the following columns: 'Subject', 'From', 'To', 'CC', 'Date (GMT)', 'Reason', 'Size', and an icon column. The table contains one entry with the following details:

<input checked="" type="checkbox"/>	Subject	From	To	CC	Date (GMT)	Reason	Size	
<input checked="" type="checkbox"/>	bob Fw: FLAT 20% OFF on Revital Multi-Vitamins. Limited Period Offer. Hurry	Junk <junkemail@yahoo.co.in>	bob@doctea bob@democ john@doctea		2016-04-20 11:02:07	spam Combined (0.15)	13.31 KB	

At the bottom of the table, there is a pagination control showing '1 / 1' and a 'Per page' dropdown set to '15'.

The details of the selected email will be displayed.

The screenshot shows the 'E-mail' interface in the Comodo Antispam Gateway. The breadcrumb trail at the top reads: Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Blacklisted requests / E-mail. The main title is 'E-mail' with a help icon. Below the title are two tabs: 'Normal' (selected) and 'All headers'. Underneath are two buttons: 'Accept' (checked) and 'Reject'. The email header information is as follows:

- Subject: Fw: FLAT 20% OFF on Revital Multi-Vitamins. Limited Period Offer. Hurry
- From: Junk <junkemail@yahoo.co.in>
- To: bob@docteamcasg.comodo.od.ua, bob@democasg.comodo.od.ua, john@docteamcasg.comodo.od.ua, john@democasg.comodo.od.ua, dyanorat481@gmail.com, robin@democasg.comodo.od.ua, avantistude@gmail.com
- CC:
- Date (GMT +00:00): 2016-04-20 11:02:07
- Size: 13.31 KB

Below the header is an 'Actions' section with three tabs: 'Plain text' (selected), 'Html source', and 'Original View'. The email content is displayed in a text area, showing a forwarded message from Netmeds Healthcare on Sunday, 10 April 2016 at 11:25 AM. The content includes a link for viewing the email on a media screen and a phone number at the bottom: 1800 103 0304.

- To view email headers, which contain the tracking information of the mail details about the path it has crossed before reaching the recipient, click 'All headers' tab.

The headers give full details of the sender, route, recipient, sent date, mail type and so on and enable you to check the authenticity of the mail.

Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either **accept** the mail or **reject** it. If the mail is accepted, it will be released to the user's inbox. If it is rejected, the email will no longer be in the released emails list. Please note that emails will continue to remain in the **Quarantined** list irrespective of the action taken.

View details of blacklisted requests in a new CASG window:

- Click 'Release request' and select the mail that you want to view
- Right-click on the email link in the subject column and select 'Open link in New Tab' or 'Open Link in New Window' to open in a new tab or new window.

Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Blacklisted requests

Blacklisted requests

Help

Show message Accept Reject Refresh

Filters

<input checked="" type="checkbox"/>	Subject	From	To	CC	Date (GMT)	Reason	Size	
<input checked="" type="checkbox"/>	Fw: FLAT 20% OFF on Revital Multi-Vitamins. Limited Period Hurry	Angel	bob@docte		2016-04-21 11:02:07	spam Combined (0.15)	13.31 KB	

Per page 15

- Open Link in New Tab
- Open Link in New Window
- Open Link in New Private Window
- Bookmark This Link
- Save Link As...
- Copy Link Location
- Search Google for "Fw: FLAT 20% OF..."
- Inspect Element (Q)

The details of the selected mail will be displayed in a new CASG window.

Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Blacklisted requests / E-mail

E-mail

? Help

Normal All headers

✓ Accept ✗ Reject

Subject Fw: FLAT 20% OFF on Revital Multi-Vitamins. Limited Period Offer. Hurry

From Junk <junkemail@yahoo.co.in>

To bob@docteamcasg.comodo.od.ua, bob@democasg.comodo.od.ua, john@docteamcasg.comodo.od.ua, john@democasg.comodo.od.ua, dyanorat481@gmail.com, robin@democasg.comodo.od.ua, avantistude@gmail.com

CC

Date (GMT +00:00) 2016-04-20 11:02:07

Size 13.31 KB

Actions

Plain text Html source Original View

On Sunday, 10 April 2016 11:25 AM, Netmeds Healthcare <support@youmnt.com> wrote:

If you're having trouble viewing this email, please click here. @media screen and (min-width:320p

|

|

|

|

- 1800 103 0304

Accept the blacklist request from users

After viewing the details, you can choose to accept the request from user to add the sender to **blacklist senders per user** list.

- Select the mail that you want to add the sender to blacklist and click the 'Accept' button.

Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Blacklisted requests

Blacklisted requests

? Help

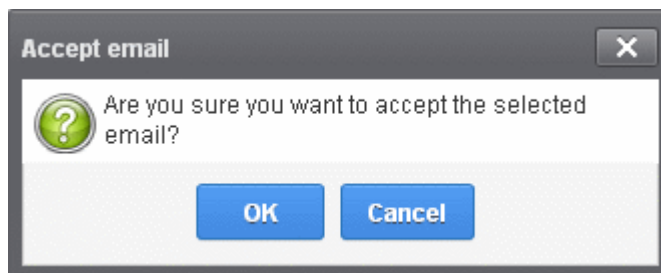
Show message Accept ✗ Reject Refresh

Filters

<input checked="" type="checkbox"/>	Subject	From	To	CC	Date (GMT)	Reason	Size	
<input checked="" type="checkbox"/>	Fw: FLAT 20% OFF on Revital Multi-Vitamins. Limited Period Offer. Hurry	Angel <angel@heaven.co.in>	bob@docte bob@dem john@doct		2016-04-21 11:02:07	spam Combined (0.15)	13.31 KB	

1 / 1 [1 - 1 / 1] Per page 15

An alert will be displayed to confirm adding the sender to '**Blacklist Senders Per User**'.



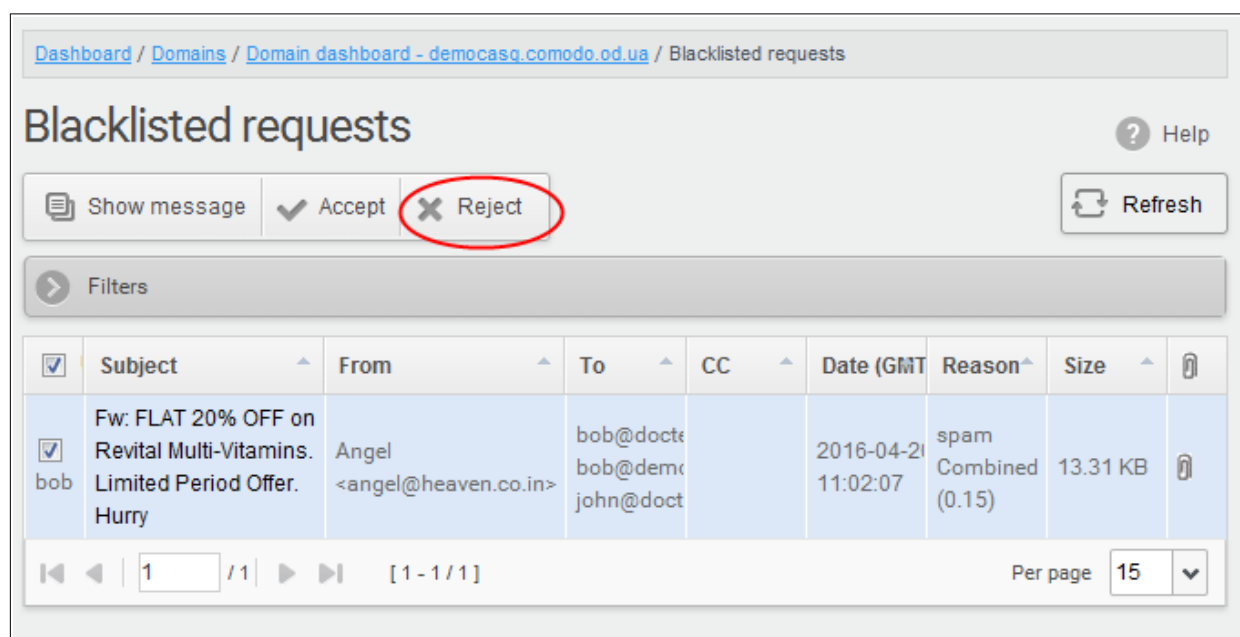
- Click 'OK' to confirm the acceptance.

The sender of the email will be added to '**Blacklist senders per user**'. See the section '**Blacklist Senders Per User**' for more details.

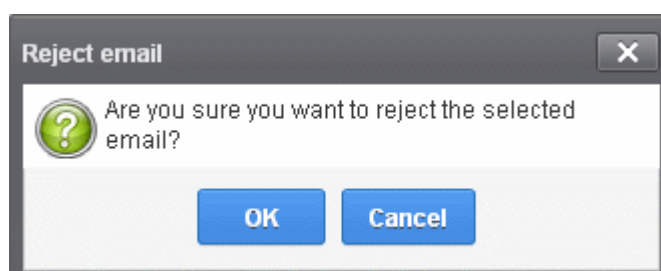
Reject the blacklist request from users

After viewing the details of the email, you can choose to reject the request from the user.

- Select the mail that you want to reject and click the 'Reject' button.



An alert will be displayed to confirm the rejection of selected email.

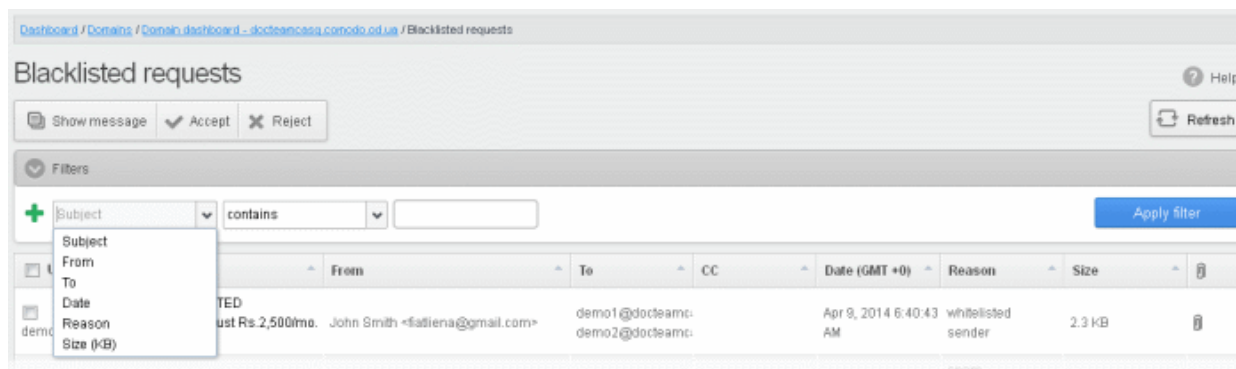


- Click 'OK' to confirm the rejection.

The sender will not be added to blacklist and the selected email will no longer be in the blacklisted emails list.

Use filters to search blacklisted requests

- Click anywhere on the 'Filters' stripe to open the filters area.




- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

- **Subject:** Type the email subject in the text box (column 3) and select a condition in column 2.
- **From:** Enter the sender name or address in the text box (column 3) and select a condition in column 2.
- **To:** Enter the recipient name or address in the text box (column 3) and select a condition in column 2.
- **Date:** Search by date and time mails quarantined. Select the date (column 3) and select a condition in column 2.
- **Reason:** Enter the quarantined reason in the text box (column 3) and select a condition 2.
- **Size (KB):** Search quarantined mails by their size. Select or enter the mail size in column 3 and select a condition in column 2.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

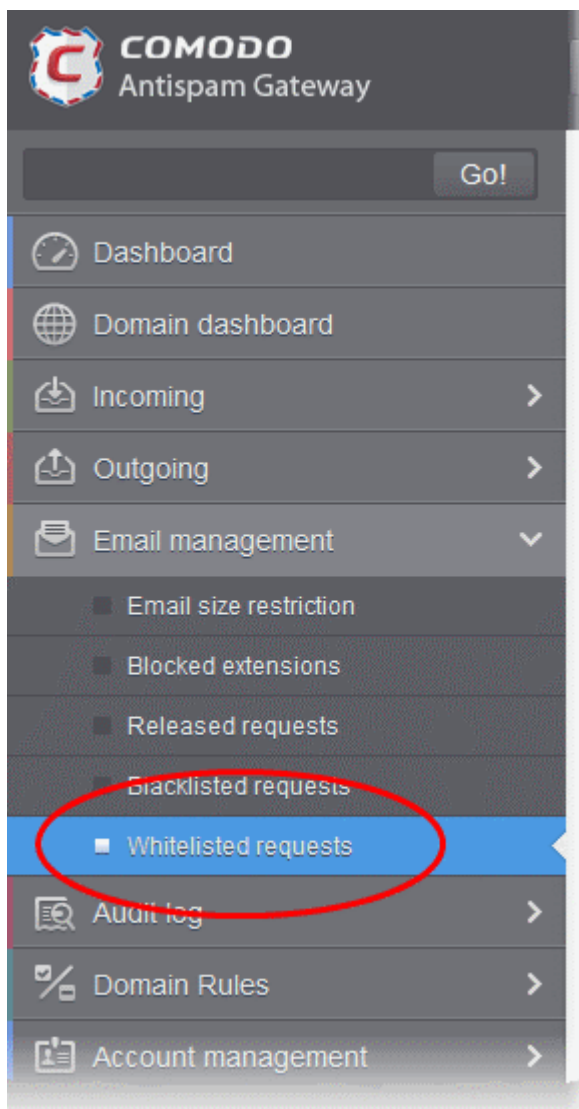
You can add multiple filters to the same search by clicking .

Whitelisted Requests

- The 'Quarantine' interface lets users view emails intended for them but moved to quarantine.
- The interface also lets users request that senders are added to the whitelist - usually because they think the mail is from a legitimate sender.
- The whitelist request will be sent to you via email and also added to the Email Management > Whitelisted Requests interface. You can approve or reject the requests.
- Senders added to the white-list after a request will only be white-listed for the requester.
- Subsequent mails from the sender to the user in question will be allowed without antispam checks.
- See [Sender Whitelist](#) and [Whitelist Senders Per User](#) for more details.

Open the whitelisted requests interface

- Click 'Email management' on the left then select "Whitelisted requests'.



The 'Whitelisted requests' interface will open:

Dashboard / Domains / Domain dashboard - docteam@comodo.od.us / Whitelisted requests

Whitelisted requests Help

Show message Accept Reject Refresh

Filters

<input type="checkbox"/>	User	Subject	From	To	CC	Date (GMT +0)	Reason	Size	<input type="checkbox"/>
<input type="checkbox"/>	demo1	Fwd: Fw: Send UNLIMITED Emails/Newsletter in Just Rs.2,500/mo. ZERO SETUP COST	John Smith <fatliens@gmail.com>	demo1@docteam.com; demo2@docteam.com;		Apr 9, 2014 6:40:43 AM	whitelisted sender	2.3 KB	<input type="checkbox"/>
<input type="checkbox"/>	demo1	Fw: Get Rs. 25 assured recharge + chance to win an IPOD.	docteam@docteam.com	demo1@docteam.com; demo2@docteam.com;		Apr 9, 2014 4:33:22 AM	spam urlblstl-multi.rbl.spam1.cor	3.98 KB	<input type="checkbox"/>
<input type="checkbox"/>	demo2	test spam email 2	docteam@docteam.com	demo2@docteam.com;		Apr 2, 2014 2:27:00 PM	spam External pattern match (SanesecurityJunk	8.18 KB	<input type="checkbox"/>

1 / 1 [1 - 3 / 3] Per page 15

The interface shows all white-list requests from users. The list has columns which show requesting user, subject, sender, recipients, CC list, date sent, the reason they were quarantined and the size of the email. The last column shows whether there is any attachment with the mail.

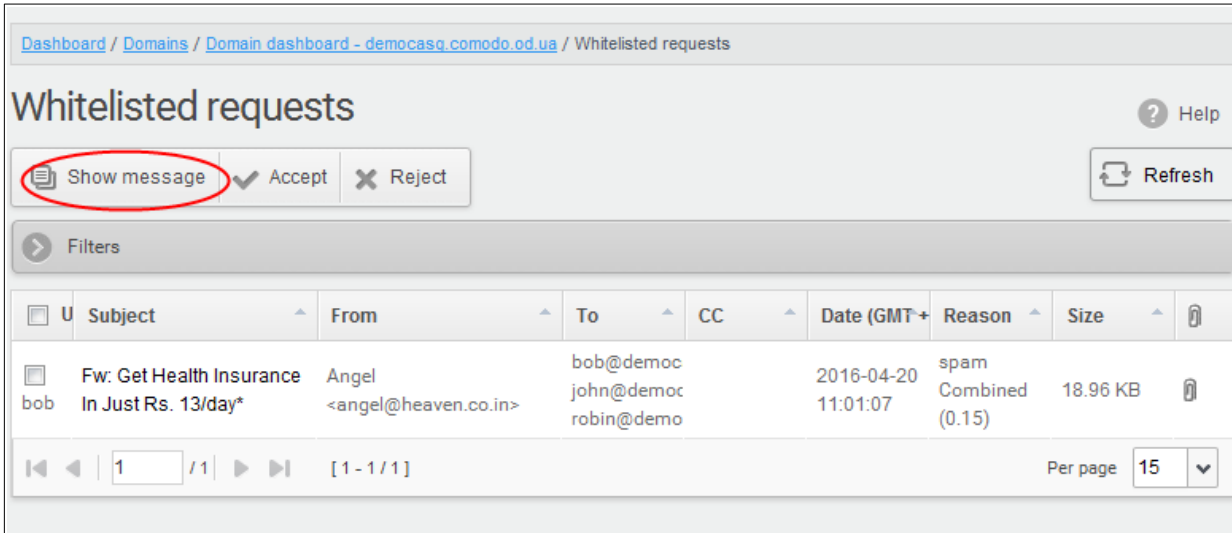
View Details of Whitelisted Requests

The details such as user, subject, sender, recipient, date, reason and size of the mails requested for whitelisting can be viewed in two ways:

- **In the same CASG window**
- **In a new CASG window**

View details of whitelisted requests in the same CASG window:

- Select the mail that you want to view and click the 'Show Message' button.
- OR
- Click on the email link in the subject column that you want to view its details.



Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Whitelisted requests

Whitelisted requests

[Show message](#) Accept Reject [Refresh](#) [Help](#)

Filters

<input type="checkbox"/>	U	Subject	From	To	CC	Date (GMT+)	Reason	Size	
<input type="checkbox"/>	bob	Fw: Get Health Insurance In Just Rs. 13/day*	Angel <angel@heaven.co.in>	bob@democ john@democ robin@demo		2016-04-20 11:01:07	spam Combined (0.15)	18.96 KB	

1 / 1 [1 - 1 / 1] Per page 15

The details of the selected email will be displayed.

Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Whitelisted requests / E-mail

E-mail ? Help

Normal All headers

✓ Accept ✗ Reject

Subject Fw: Get Health Insurance In Just Rs. 13/day*

From Angel <angel@heaven.co.in>

To bob@democasg.comodo.od.ua, john@democasg.comodo.od.ua, robin@democasg.comodo.od.ua, avantistude@gmail.com, sumeetdomestic@gmail.com, john@docteamcasg.comodo.od.ua

CC

Date (GMT +00:00) 2016-04-20 11:01:07

Size 18.96 KB

Actions

Plain text Html source Original View

On Wednesday, 20 April 2016 10:53 AM, Online Health Plan <support@indiadz.com> wrote:

If you're having trouble viewing this email, please click here.#yiv3139774641 .yiv3139774641text_box

```

|   |
|   |
|   | The Best Hospitals are Now Affordable |
|   | Get
|   | Health Insurance
|   | In Just
|   | Rs. 13/day* Get Health Insurance In Just Rs. 13/day*   |
|   |
|   |
|   |
|   | Get
|   | Cashless Claim
|   | Hospital Bills are directly

```

- To view email headers, which contain the tracking information of the mail details about the path it has crossed before reaching the recipient, click 'All headers' tab.

The headers give full details of the sender, route, recipient, sent date, mail type and so on and enable you to check the authenticity of the mail.

Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either **accept** the mail or **reject** it. If the request is accepted, the sender will be added to '**Whitelist sender per user**'. If it is rejected, the email will be no longer in the whitelisted requests list. Please note that emails will continue to remain in the **Quarantined** list irrespective of the action taken.

View details of whitelisted requests in new CASG window:

- In the whitelisted requests area, select the mail that you want to view and click the 'Show message in new window' button or right-click and select to open in a new tab or new window.

Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Whitelisted requests

Whitelisted requests

Help

Show message Accept Reject Refresh

Filters

U	Subject	From	To	CC	Date (GMT+)	Reason	Size	
<input type="checkbox"/>	Fw: Get Health Insurance In Just Rs. 13/day*	Angel	bob@democ john@democ robin@demo		2016-04-20 11:01:07	spam Combined (0.15)	18.96 KB	

Per page 15

- Open Link in New Tab
- Open Link in New Window
- Open Link in New Private Window
- Bookmark This Link
- Save Link As...
- Copy Link Location
- Search Google for "Fw: Get Health ..."
- Inspect Element (Q)

The details of the selected mail will be displayed in a new CASG window.

Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Whitelisted requests / E-mail

E-mail

Help

Normal All headers

Accept Reject

Subject: Fw: Get Health Insurance In Just Rs. 13/day*

From: Angel <angel@heaven.co.in>

To: bob@democasg.comodo.od.ua, john@democasg.comodo.od.ua, robin@democasg.comodo.od.ua, avantistude@gmail.com, sumeetdomestic@gmail.com, john@docteamcasg.comodo.od.ua

CC:

Date (GMT +00:00): 2016-04-20 11:01:07

Size: 18.96 KB

Actions

Plain text Html source Original View

On Wednesday, 20 April 2016 10:53 AM, Online Health Plan <support@indiadz.com> wrote:

If you're having trouble viewing this email, please click here.#yiv3139774641 .yiv3139774641text_box

| |

| The Best Hospitals are Now Affordable |

| Get

Health Insurance

In Just

Rs. 13/day* Get Health Insurance In Just Rs. 13/day* |

| |

| |

| |

| Get

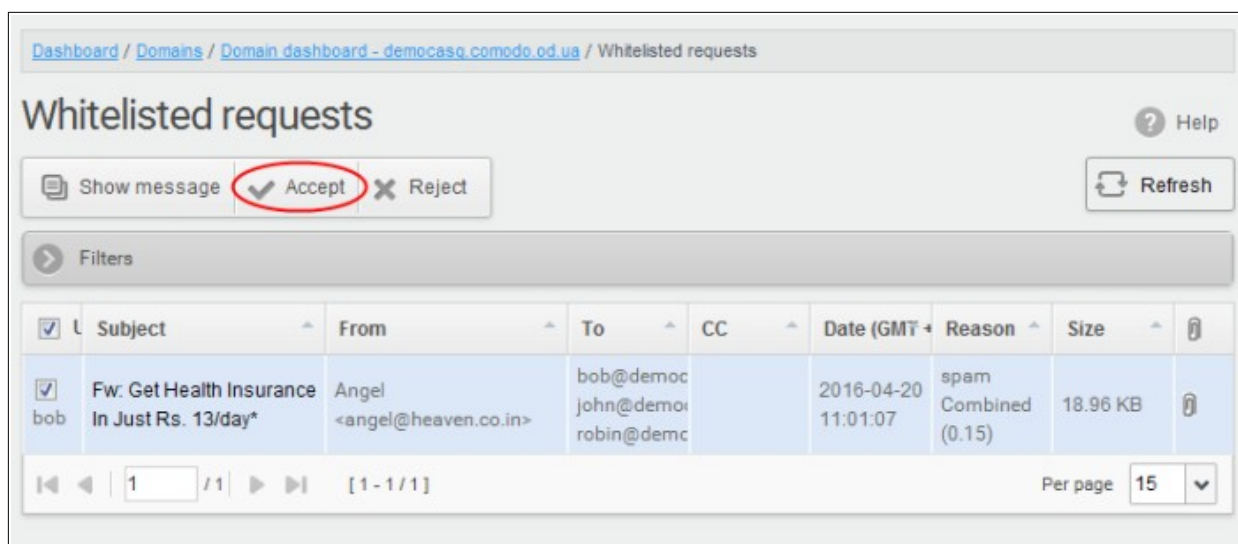
Cashless Claim

Hospital Bills are directly

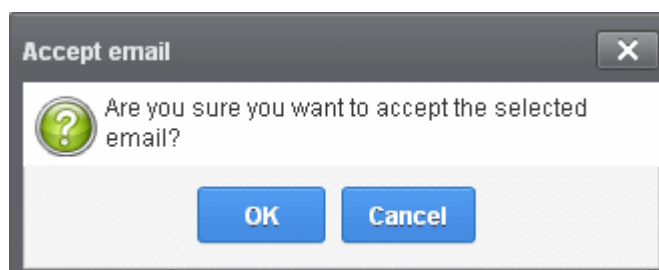
Accept the whitelist request from users

After viewing the details, you can choose to accept the request from user to add the sender to **whitelist senders per user** list.

- Select the mail that you want to add the sender to whitelist and click the 'Accept' button.



An alert will be displayed to confirm adding the sender to **'Whitelist sender per user'**.



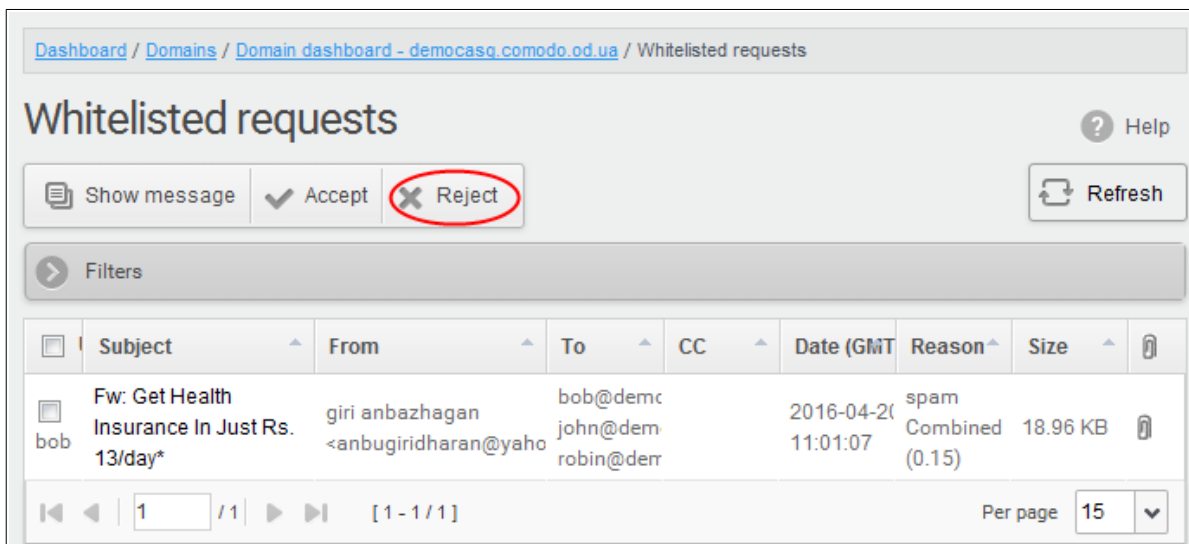
- Click 'OK' to confirm the acceptance.

The sender of the email will be added to **'Whitelist sender per user'**. See the section **'Whitelist Sender Per User'** for more details.

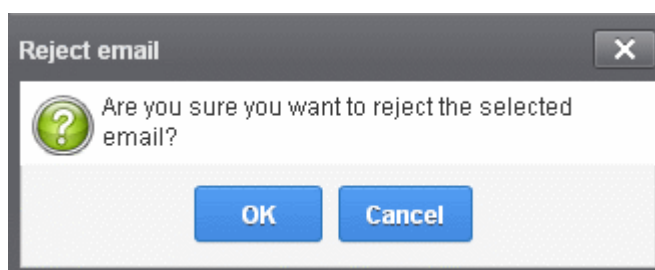
Reject the whitelist request from users

After viewing the details of the email, you can choose to reject the request from the user.

- Select the mail that you want to reject and click the 'Reject' button.



An alert will be displayed to confirm the rejection of user's request.

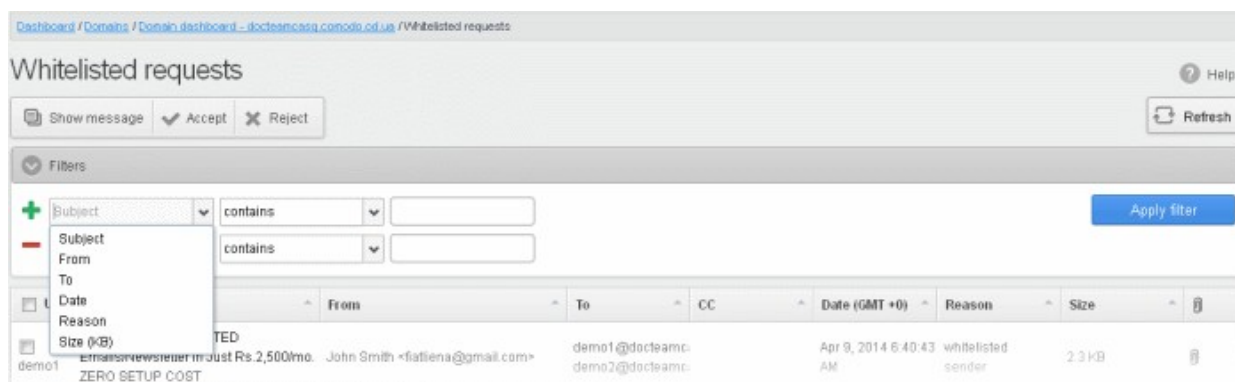


- Click 'OK' to confirm the rejection.

The sender will not be added to whitelist and the selected email will no longer be in the whitelisted requests list.

Use filters to search whitelist requests

- Click anywhere on the 'Filters' stripe to open the filters area.




- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

- **Subject:** Type the email subject in the text box (column 3) and select a condition in column 2.
- **From:** Enter the sender name or address in the text box (column 3) and select a condition in column 2.
- **To:** Enter the recipient name or address in the text box (column 3) and select a condition in column 2.

- **Date:** Search by date and time mails quarantined. Select the date (column 3) and select a condition in column 2.
- **Reason:** Enter the quarantined reason in the text box (column 3) and select a condition 2.
- **Size (KB):** Search quarantined mails by their size. Select or enter the mail size in column 3 and select a condition in column 2.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

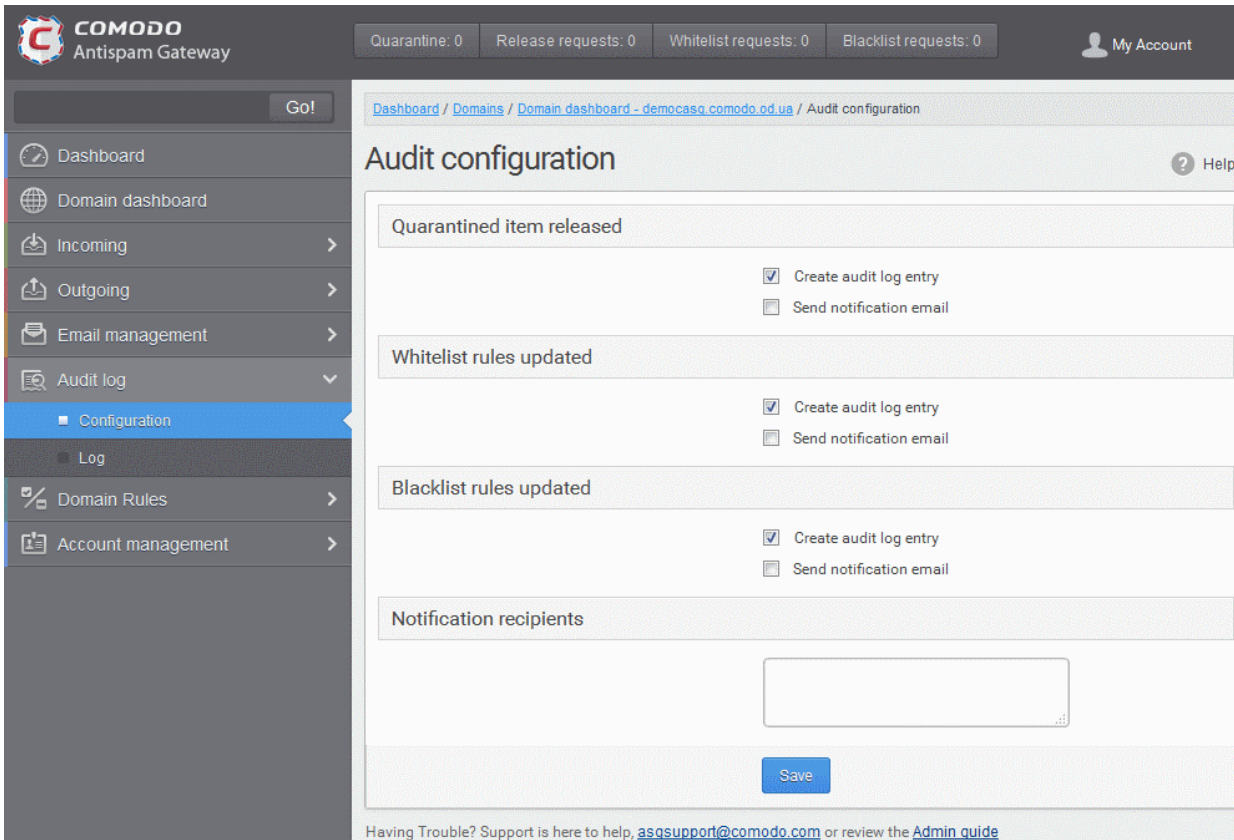
You can add multiple filters to the same search by clicking  .

6.5.5 Domain Audit Log

Domain audit logs are a record of actions by users and admins on a selected domain.

The audit log area lets you:

- Configure and view log reports.
- Keeps a consolidated log for all domains belonging to an account.
- Note. This section explains logs for individual domains. See **Audit Log** if you want a consolidated log of all domains.

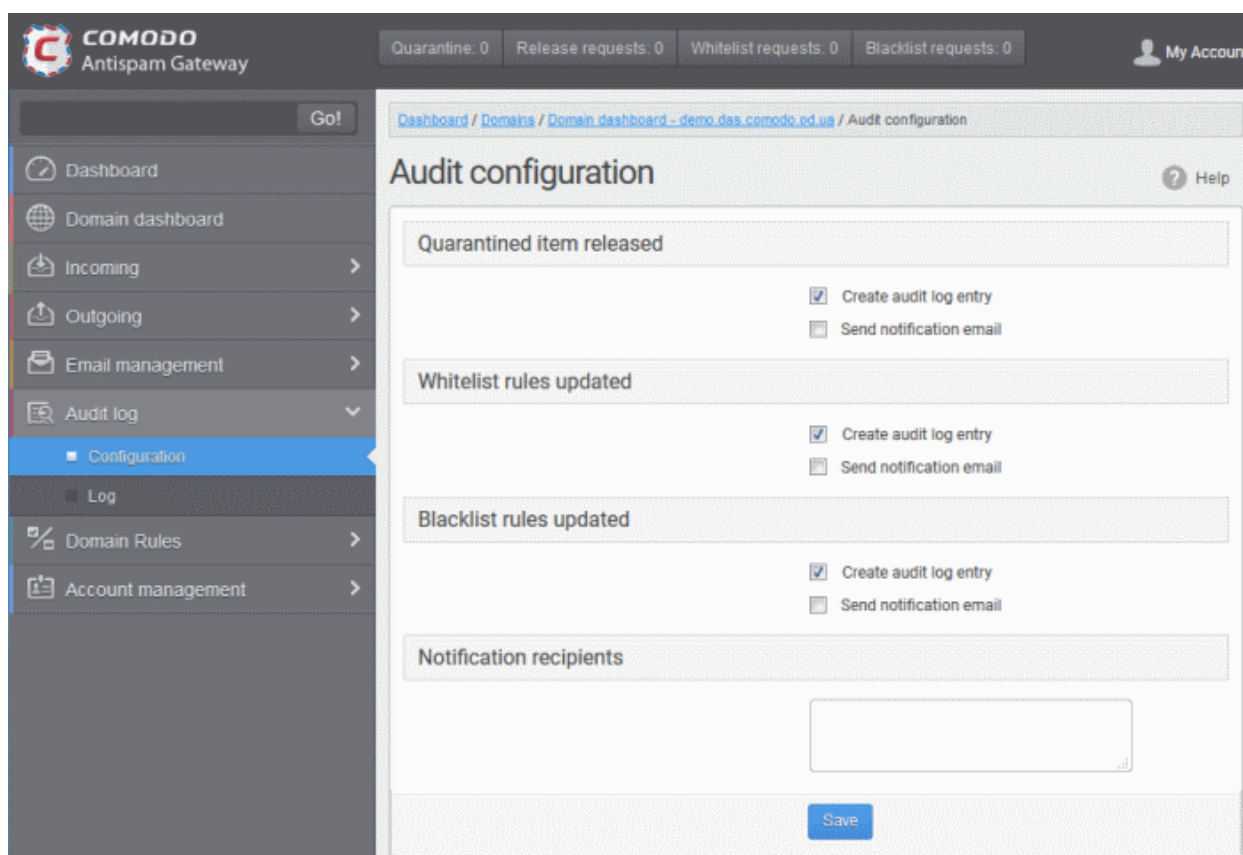


Click the following links for more details.

- [Audit Log Configuration](#)
- [View Domain Log](#)

Audit Log Configuration

- Click 'Audit log' > 'Configuration'



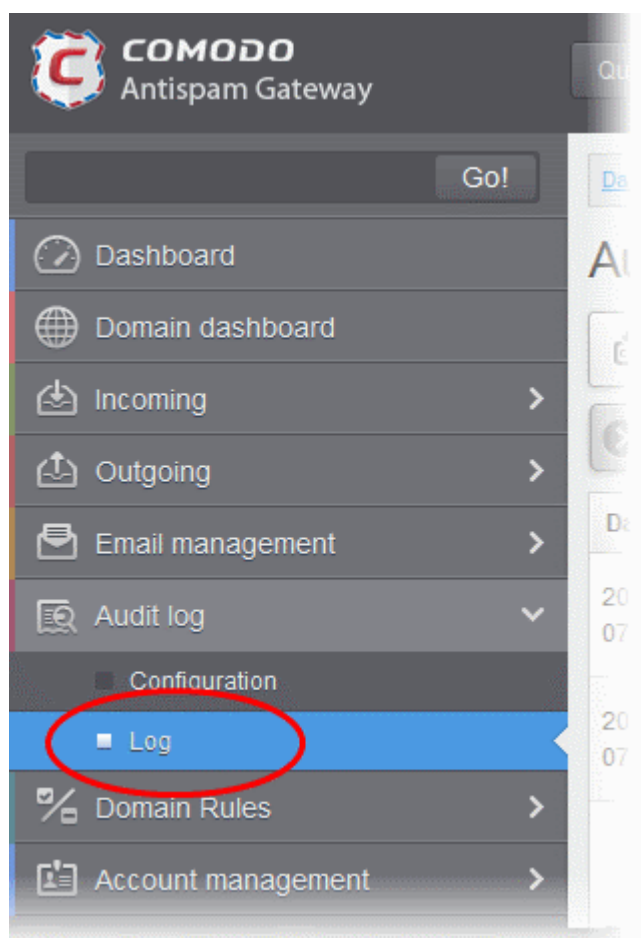
- **Quarantined item released**
 - Create audit log entry - If enabled, CASG records the release of **quarantined mails**.
 - Send notification email - If enabled, notification mails for quarantined mails release will be sent to recipients added in the 'Notification recipient's' box.
- **Whitelist rules updated**
 - Create audit log entry - If enabled, CASG records any updates to **Whitelist senders per user** interface
 - Send notification email - If enabled, notification mails for updates to **Whitelist senders per user** interface will be sent to recipients added in the 'Notification recipient's' box.
- **Blacklist rules updated**
 - Create audit log entry - If enabled, CASG records any updates to **Blacklist senders per user** interface.
 - Send notification email - If enabled, notification mails for updates to **Blacklist senders per user** interface will be sent to recipients added in the 'Notification recipient's' box.
- **Notification recipients** - Enter the email addresses of the persons to whom the email notifications for the above mentioned actions will be sent. Please note that any email addresses of the recipient's can be entered here.

View Domain Log

The log screen allows admins with appropriate privileges to view the logs of the selected domain.

View the audit log of the selected domain

- Click the 'Log' from 'Audit log' drop-down on the left



The Audit log screen will be displayed.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Audit log

Audit log

Export to CSV by filter Refresh

Filters

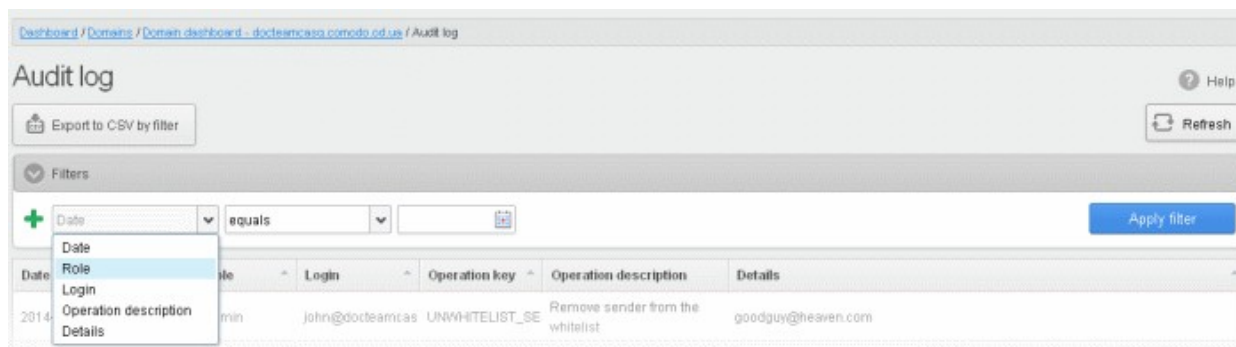
Date (GMT +0)	Role	Login	Operation key	Operation description	Details
2014-04-13 09:16:42	admin	john@docteamcas	UNWHITELIST_SE	Remove sender from the whitelist	goodguy@heaven.com
2014-04-13 08:57:07	admin	john@docteamcas	RELEASE_EMAIL_I	Release quarantined message	Recipients: demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua; Sender: [redacted]; Date: Mon Apr 07 08:52:31 GMT 2014; Subject: Fw: We have free samples for you, now try before you buy @ your doorstep!
2014-04-13 08:53:57	admin	john@docteamcas	WHITELIST_SEND	Whitelist sender	goodguy@heaven.com
2014-04-13 08:52:28	admin	john@docteamcas	UNWHITELIST_SE	Remove sender from the whitelist	someone@example.com
2014-04-13 08:50:23	admin	john@docteamcas	RELEASE_EMAIL_I	Release quarantined message	Recipients: demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua; Sender: [redacted]; Date: Mon Apr 07 08:52:31 GMT 2014; Subject: Fw: We have free samples for you, now try before you buy @ your doorstep!
2014-04-13 08:45:07	admin	john@docteamcas	BLACKLIST_SEND	Blacklist sender	devil@hell.com
2014-04-13 08:35:36	admin	john@docteamcas	WHITELIST_SEND	Whitelist sender	someone@example.com
2014-04-13 08:27:36	user	demo1	USER_BLACKLIST	Request blacklist sender for user	Recipients: demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua; Sender: John Smith <fatliona@gmail.com>; Subject: Fwd: Fw: Send UNLIMITED Emails/Newsletter in Just Rs 2,500/mo. ZERO SETUP COST, Wed Apr 09 06:40:43 GMT 2014
2014-04-13 08:25:37	admin	john@docteamcas	REJECT_WHITELI	Reject request whitelist sender for user	Recipients: demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua; Sender: John Smith <fatliona@gmail.com>; Subject: Fwd: Fw: Send UNLIMITED Emails/Newsletter in Just Rs 2,500/mo. ZERO SETUP COST, 2014-04-09 06:40:43.0

- Click any column heading to sort entries in ascending/descending order. The sorting option is not available

for the 'Operation description' column.

Use the filter options to search particular event(s)

- Click anywhere on the 'Filters' stripe to open the filters area.




- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

- **Login:** Type a user login name in the text box (column 3) and select a condition in column 2.
- **Details:** Enter the log details in the text box (column 3) and select a condition in column 2.
- **Date:** Search event logs by date and time.
- **Role:** Search event logs by user roles. Select the role (column 3) and condition in column 2.
- **Operation Description:** Select the event name (column 3) and condition in column 2.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

You can add multiple filters to the same search by clicking .

The following table show actions which are recorded in the log report:

S.No.	Operation Key	Operation Description
1	DELETE_EMAIL_FROM_QUARANTINE_BY_FILTER	Delete quarantined messages by filter
2	DELETE_EMAIL_FROM_QUARANTINE	Delete quarantined message
3	RELEASE_EMAIL_FROM_QUARANTINE	Release quarantined message
4	WHITELIST_RECIPIENT	Whitelist recipient
5	BLACKLIST_RECIPIENT	Blacklist recipient
6	UNWHITELIST_RECIPIENT	Remove recipient from the whitelist
7	UNBLACKLIST_RECIPIENT	Remove recipient from the blacklist
8	WHITELIST_SENDER	Whitelist sender
9	BLACKLIST_SENDER	Blacklist sender
10	UNWHITELIST_SENDER	Remove sender from the whitelist

11	UNBLACKLIST_SENDER	Remove sender from the blacklist
12	RESET_TO_DEFAULT_WHITELISTED_SENDERS	Reset senders whitelist
13	RESET_TO_DEFAULT_WHITELISTED_RECIPIENTS	Reset recipients whitelist
14	RESET_TO_DEFAULT_BLACKLISTED_SENDERS	Reset senders blacklist
15	RESET_TO_DEFAULT_BLACKLISTED_RECIPIENTS	Reset recipients blacklist
16	WHITELIST_SENDER_DOMAIN	Whitelist all senders of the domain
17	WHITELIST_RECIPIENT_DOMAIN	Whitelist all recipients of the domain
18	BLACKLIST_SENDER_DOMAIN	Blacklist all senders of the domain
19	BLACKLIST_RECIPIENT_DOMAIN	Blacklist all recipients of the domain
20	USER_WHITELIST_REQUEST_PER_USER	Request whitelist sender for user
21	USER_BLACKLIST_REQUEST_PER_USER	Request blacklist sender for user
22	USER_RELEASE_REQUEST	Release request
23	USER_CANCEL_WHITELIST_REQUEST_PER_USER	Cancel request whitelist sender for user
24	USER_CANCEL_BLACKLIST_REQUEST_PER_USER	Cancel request blacklist sender for user
25	USER_CANCEL_RELEASE_REQUEST	Cancel release request
26	ACCEPT_WHITELIST_REQUEST_PER_USER	Accept request whitelist sender for user
27	ACCEPT_BLACKLIST_REQUEST_PER_USER	Accept request blacklist sender for user
28	ACCEPT_RELEASE_REQUEST	Accept release request
29	REJECT_WHITELIST_REQUEST_PER_USER	Reject request whitelist sender for user
30	REJECT_BLACKLIST_REQUEST_PER_USER	Reject request blacklist sender for user
31	REJECT_RELEASE_REQUEST	Reject release request
32	SPAM_DETECTION_SETTINGS	Update spam detection settings
33	SPAM_DETECTION_SETTINGS_RESET_TO_DEFAULT	Reset spam detection settings
34	DELETE_EMAIL_FROM_ARCHIVE_BY_FILTER	Delete archived messages by filter
35	DELETE_EMAIL_FROM_ARCHIVE	Delete archived message
36	RESEND_EMAIL_FROM_ARCHIVE	Resend archived message
37	REPORTS_AS_SPAM	Reports archived message as a SPAM
38	QUARANTINE_EMAIL	Quarantine message

39	ACCEPT_AND_ARCHIVE_EMAIL	Accept and archive message
40	MARK_EMAIL_AS_SPAM	Mark message as spam
41	ACCEPT_EMAIL	Accept message
42	WHITELIST_USER_SENDER	Whitelist sender for user
43	BLACKLIST_USER_SENDER	Blacklist sender for user
44	UNWHITELIST_USER_SENDER	Remove sender from the user whitelist
45	UNBLACKLIST_USER_SENDER	Remove sender from the user blacklist
46	QUARANTINE_REPORT_SUBSCRIPTION_UPDATE	Quarantine report subscription update
47	QUARANTINE_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT	Quarantine report subscription reset to default
48	DOMAIN_STATISTICS_REPORT_SUBSCRIPTION_UPDATE	Domain report subscription update
49	DOMAIN_STATISTICS_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT	Domain report subscription reset to default
50	DOMAIN_ADD	Add domain
51	DOMAIN_DELETE	Remove domain
52	ADMIN_ADD	Add admin
53	ADMIN_EDIT	Edit admin settings
54	ADMIN_DELETE	Remove admin
55	ADMIN_UNLOCK	Unlock admin
56	ADMIN_REGENERATE_PASSWORD	Regenerate password for admin
57	ADMIN_PASSWORD_UPDATE	Update password for admin
58	SYSTEM_NOTIFICATIONS_TEMPLATE_CHANGE	System notifications template change
59	ADMIN_PERMISSIONS_GROUP_ADD	Add admin permission group
60	ADMIN_PERMISSIONS_GROUP_DELETE	Remove admin permission group
61	ADMIN_PERMISSIONS_GROUP_UPDATE	Update admin permission group
62	ADMIN_PERMISSIONS_CHANGE_DEFAULT_GROUP	Change default admin permission group
63	ADMIN_PERMISSIONS_ASSIGN_GROUP	Assign admin permission group by selection
64	REPORT_SPAM_BY_FILE	Report delivered message as spam
65	DOMAIN_DESTINATION_ROUTES_UPDATE	Update destination routes
66	DOMAIN_LOCAL_RECIPIENTS_ADD	Add local recipient
67	DOMAIN_LOCAL_RECIPIENTS_DELETE	Remove local recipient
68	DOMAIN_LOCAL_RECIPIENTS_STATE_CHANGE	Local recipients state change

69	DOMAIN_ALIASES_ADD	Add domain alias
70	DOMAIN_ALIASES_DELETE	Remove domain alias
71	DOMAIN_SETTINGS_UPDATE	Update domain settings
72	DOMAIN_SETTINGS_RESET_TO_DEFAULT	Reset domain settings to default
73	DOMAIN_RELAY_RESTRICTIONS_ADD	Add relay restriction
74	DOMAIN_RELAY_RESTRICTIONS_UPDATE	Update relay restriction
75	DOMAIN_RELAY_RESTRICTIONS_DELETE	Remove relay restriction
76	DOMAIN_RELAY_RESTRICTIONS_STATE_CHANGE	Relay restriction state change
77	DOMAIN_OUTGOING_USER_ADD	Add outgoing user
78	DOMAIN_OUTGOING_USER_SETTINGS_UPDATE	Edit outgoing user
79	DOMAIN_OUTGOING_USER_DELETE	Remove outgoing user
80	DOMAIN_OUTGOING_USER_LOCK	Lock outgoing user
81	DOMAIN_OUTGOING_USER_UNLOCK	Unlock outgoing user
82	DOMAIN_OUTGOING_USER_PASSWORD_UPDATE	Update password for outgoing user
83	DOMAIN_EMAIL_SIZE_RESTRICTION_CHANGE	Email size restriction change
84	DOMAIN_BLOCKED_EXTENSIONS_UPDATE	Update blocked extensions
85	DOMAIN_BLOCKED_EXTENSIONS_RESET_TO_DEFAULT	Reset blocked extensions to default
86	DOMAIN_AUDIT_CONFIGURATION_CHANGE	Audit configuration change
87	DOMAIN_LDAP_CONFIGURATION_CHANGE	LDAP configuration change
88	DOMAIN_INCOMING_USER_ADD	Add incoming user
89	DOMAIN_INCOMING_USER_EDIT	Edit incoming user
90	DOMAIN_INCOMING_USER_DELETE	Remove incoming user
91	DOMAIN_INCOMING_USER_UNLOCK	Unlock incoming user
92	DOMAIN_INCOMING_USER_REGENERATE_PASSWORD	Regenerate password for incoming user
93	DOMAIN_INCOMING_USER_PASSWORD_UPDATE	Update password for incoming user
94	DOMAIN_INCOMING_USER_ALIASES_UPDATE	Update incoming user aliases
95	DOMAIN_INCOMING_USER_MOVE_USER_TO_ALIAS	Move user to alias
96	DOMAIN_INCOMING_USER_MOVE_ALIAS_TO_USER	Move alias to incoming user
97	USER_PERMISSIONS_GROUP_ADD	Add user permission group

98	USER_PERMISSIONS_GROUP_DELETE	Remove user permission group
99	USER_PERMISSIONS_GROUP_UPDATE	Update user permission group
100	USER_PERMISSIONS_CHANGE_DEFAULT_GROUP	Change default user permission group
101	USER_PERMISSIONS_ASSIGN_GROUP	Assign user permission group by selection

Export Log Report to CSV

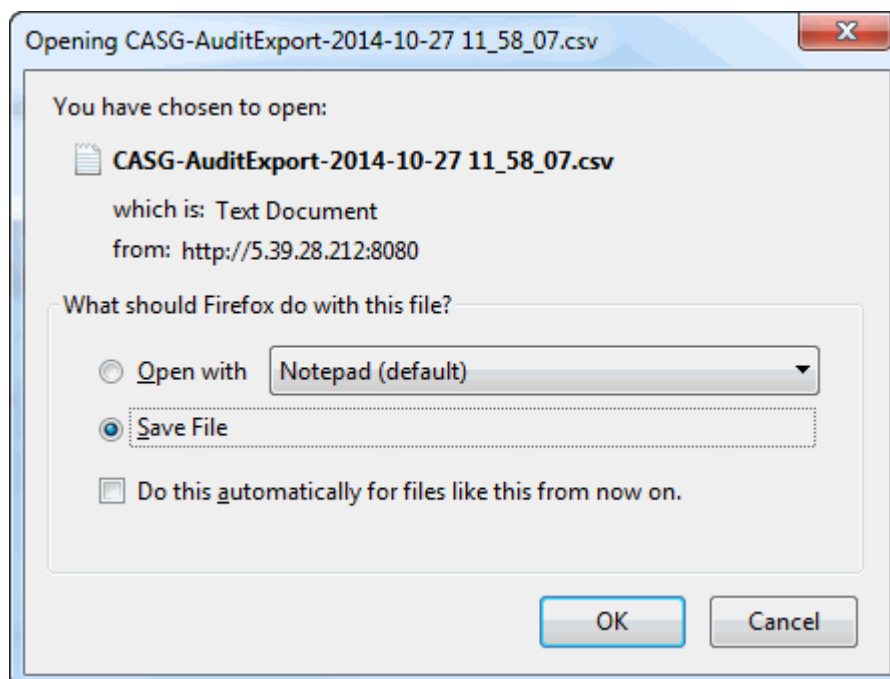
The log report can be exported to a comma separated value (CSV) file and is limited to 10,000 entries per file. If the entries exceed this value, exporting cannot be done and a warning will be displayed. Please note that exported file will display the entries in the same sorted order as in the interface.

Export log report to csv file

- Click the 'Export to CSV by filter' button.



The 'File Download' dialog will be displayed.

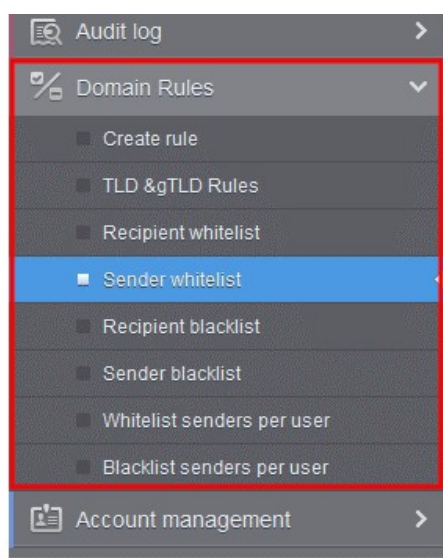


- Click 'Open' to view the file with an appropriate application
- Click 'OK' to save the file to your computer.

The values in the log report will be separated by commas and this file can be opened with Excel or Openoffice Calc for easy analysis.

6.5.6 Domain Rules

- Create granular filtering rules for each domain in order to blacklist, whitelist or forward mails.
- Rules can be based on sender, recipient, source/destination server, subject line, suspicious attachments and more.



Note: Under default conditions, CASG will filter all incoming mails to all domains that have been enabled in the 'Domains' area.

The following table offers more details on each rule type:

Rule Type	Description	Notes
Domain Rules ('Create Rule...')	Create granular rules to blacklist, whitelist or forward mail based on one or more criteria.	Criteria include sender, sender mail server, recipient, relay server, subject line and suspicious attachment.
TLD & gTLD Rules	Allow or block mails based on top level domain.	Mail from all TLDs is allowed by default. This interface allows you to block selected TLDs.
Recipient Whitelist	Always allow mail sent to these recipients.	For example, CASG will allow/block mails to/from specific_user@example.com, but will filter as normal email to/from any_other_users@example.com
Sender Whitelist	Always allow mail received from these senders.	
Recipient Blacklist	Always block mail sent to these	You can bulk import email addresses

	recipients.	from .csv or add manually.
Sender Blacklist	Always block mail received from these senders.	
Whitelist senders per user	Always allow mail from specific email addresses to specific users.	For example, CASG will allow/block mails from <code>specific_sender@example.com</code> to <code>specific_recipient@your_domain.com</code> , but will continue to filter mail from <code>specific_sender@example.com</code> to <code>everybody_else@your_domain.com</code>
Blacklist senders per user	Always block mail from specific email addresses to specific users.	You can bulk import email addresses from .csv or add manually.

General Advice

- If you are troubleshooting issues with a particular email address, please check all interfaces listed under 'Domain Rules'.
- Rule priorities can be summarized as follows:
 1. Email Size Restriction
 2. Domain Whitelist rules
 3. Sender/Recipient Whitelist
 4. Domain Blacklist rules
 5. Sender/Recipient Blacklist
 6. TLD & gTLD blacklist rule
 7. Per user White list
 8. Per user Black list
 9. Email Blocked Extensions

CASG will stop applying rules on first match (if any).
- '**Email Size Restrictions**' have a higher priority than domain rules. CASG will still block mails that exceed 'Email Size Restriction' regardless of any rules.
- '**Email Blocked Extensions**' have a lower priority than domains rules. CASG will not stop mails containing a blocked extension if there is a whitelist rule which green-lights the message.
- Whitelist domains rules take precedence over blacklist domain rules.
- Whitelist/blacklist rules in the domain rules section take precedence over 'per user' whitelist/blacklist rules.

Click the following links for more details.

- [Rules](#)
- [TLD and gTLD Rules](#)
- [Recipient Whitelist](#)
- [Sender Whitelist](#)
- [Recipient Blacklist](#)
- [Sender Blacklist](#)
- [Whitelist Senders Per User](#)

- **Blacklist Senders Per User**

Rules

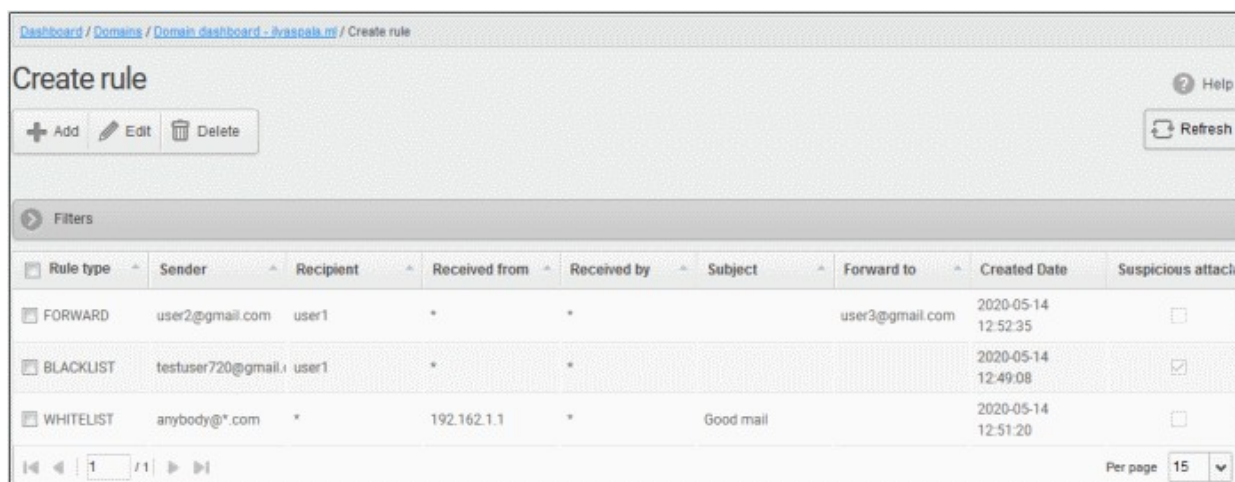
Administrators can create rules to filter inbound mails based on sender, recipient, source and relay/MTA server, subject line, attachments and so on. There are three types of filtering rules:

- **Blacklist rule** - Blocks inbound mails based on one or more filter criteria. Criteria include sender, recipient, mail servers/relays and specific subject line.
- **Whitelist rule** - Allows mails to pass through, without security checks, based on one or more filter criteria. Criteria include sender, recipient, mail servers/relays and specific subject line.
- **Forward rule** - Forwards mails based on one or more filter criteria, to a set email address. Criteria include sender, recipient, mail servers/relays and specific subject line.

For example, you can create rules to block all mails from a specific mail server, allow all mails from a specific sender to a specific recipient, forward all mails containing a specific text string in the subject line and so on.

Open the 'Create Rule' interface

- In the left-hand menu, click 'Domain Rules' > 'Create Rule'
- The 'Create Rule' interface will open:



Column Header	Description
Rule Type	Indicates whether the rule is for Blacklisting, whitelisting or forwarding.
Sender	The sender whose mails are intercepted by the rule.
Recipient	The recipient at the domain, whose mails are intercepted by the rule.
Received From	All mails sent from the external mail server indicated in this field will be intercepted by the rule.
Received by	All mails which are relayed by the servers which were indicated in this field will be intercepted by the rule.
Subject	Mails containing subject line indicated in this field will be intercepted by the rule.
Forward to	Indicates the email address to which the mails satisfying the conditions are forwarded. (Applies only to Forward Rules.)
Created date	The date and time the rule was added

Suspicious attachment	Indicates whether the rule should apply only to mails containing suspicious attachments
-----------------------	---

- Click any column header to sort rules in the ascending/descending order of the entries in that column. Does not apply to the 'Suspicious attachment' column header.


Use filters to search rules

- Click anywhere on the 'Filters' stripe to open the filters area.

The screenshot shows the 'Filters' configuration area. It has a header 'Filters' with a dropdown arrow. Below it are three filter rules, each with a plus or minus icon on the left. The first rule is 'Sender' (plus icon), condition 'contains', and value 'gabriel'. The second rule is 'Subject' (minus icon), condition 'contains', and value 'saviour'. The third rule is 'Rule type' (minus icon), condition 'equals', and value 'BLACKLIST'. An 'Apply filter' button is on the right. Below the filter rules is a table with columns: Rule type, Sender, Recipient, Received from, Received by, Subject, Forward to.

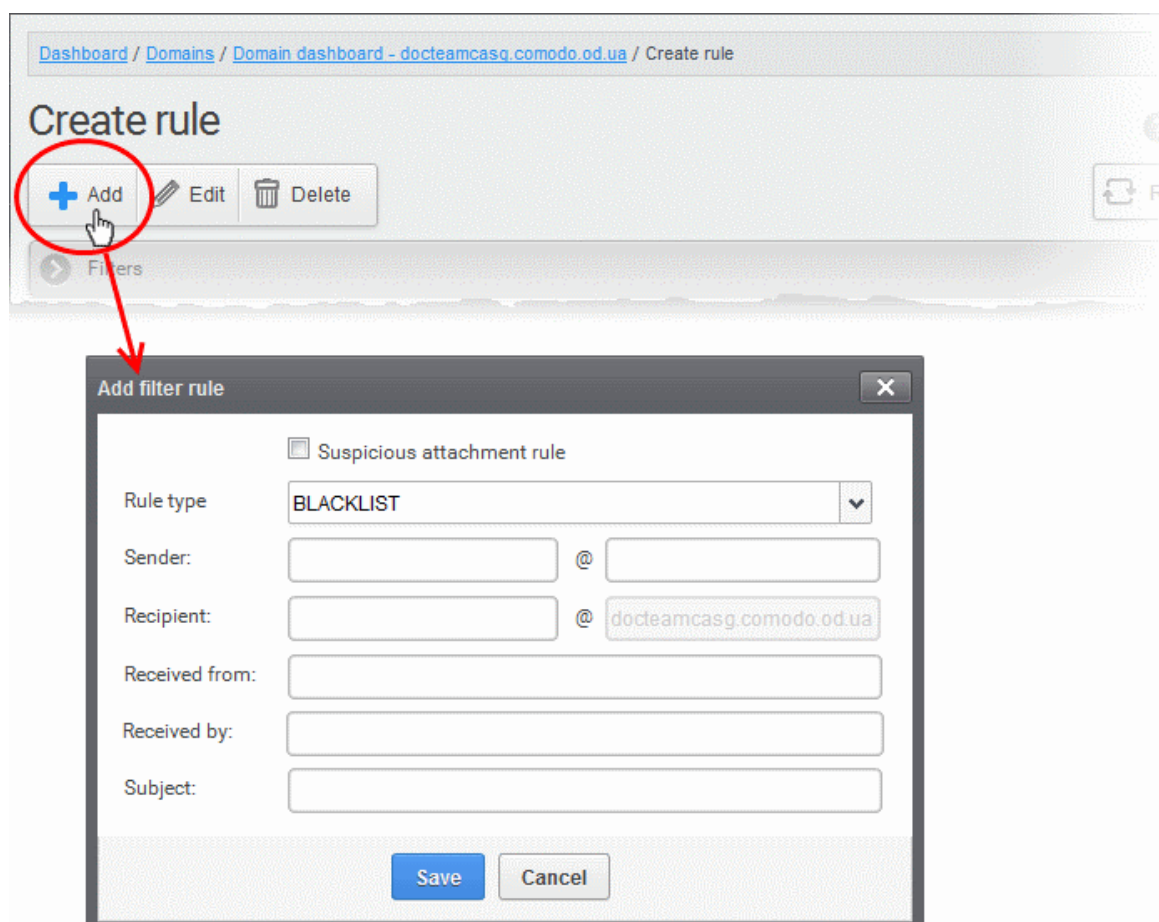
- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

- **Rule Type** – Select the rule type (column 3) and the condition in column 2.
- **Sender** – Type the sender's email address in the text box (column 3) and select the condition in column 2
- **Recipient** - Type the recipient's email address in the text box (column 3) and select the condition in column 2
- **Received from** – Type the hostname or IP address of external mail server in the text box (column 3) and select the condition in column 2
- **Received by** - Type the hostname or IP address of internal mail server in the text box (column 3) and select the condition in column 2.
- **Subject** – Enter mail subject in the text box (column 3) and select the condition in column 2
- **Forward to** – Type the forward email address in the text box (column 3) and select the condition column 2
- **Suspicious attachment rule** – Filter suspicious attachment rules based on their enabled / disabled statuses
- Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.
- You can add multiple filters to the same search by clicking  .

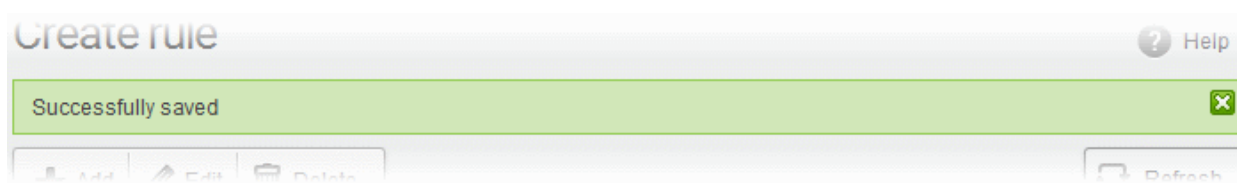
Create a new mail filter rule

- Click the 'Add' button.
- This will open the 'Add blacklist rule' dialog:



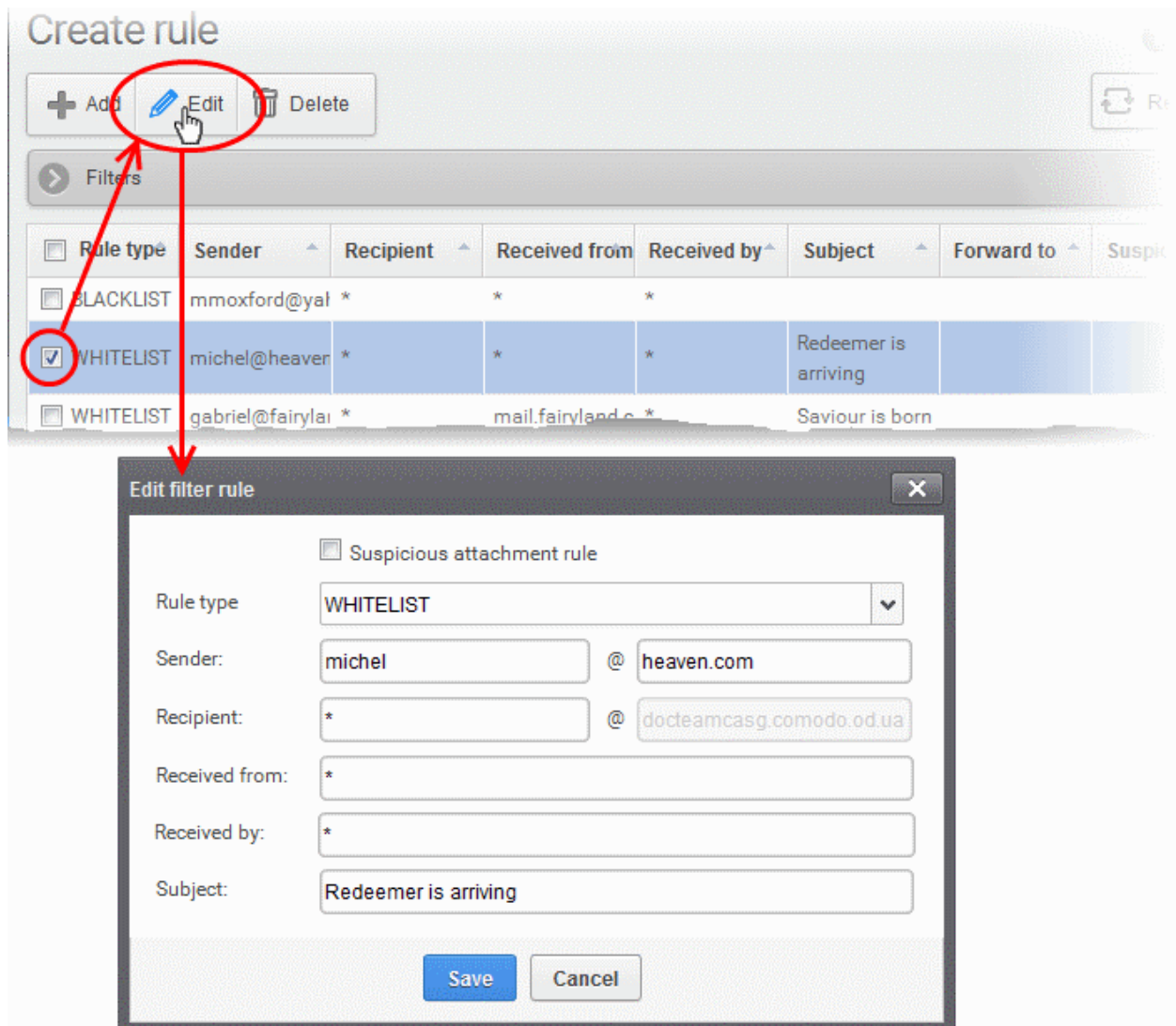
- **Suspicious attachment rule**
 - By default, all mails containing suspicious attachments will be quarantined by CASG.
 - A 'Suspicious attachment rule' lets you define specific actions if a malicious attachment is found in a mail.
 - For example, you may want mails with a suspicious attachment from a specific sender, addressed to a particular recipient to be forwarded to a certain email address.
 - Note. Enabling 'Suspicious attachment rule' means the rule only applies to mails which meet your conditions AND contain a suspicious attachment. It will not intercept mails which meet the conditions but do not contain a suspicious attachment.
- **Rule type** - Select the rule type. The available options are:
 - BLACKLIST - All mails with fields satisfying the parameters entered in the options below, will be blocked.
 - WHITELIST - All mails with fields satisfying the parameters entered in the options below, will be passed without security checks.
 - FORWARD - All mails with fields satisfying the parameters entered in the options below, will be forwarded to the email address entered in the 'Forward email' field.
- **Sender** - Enter the email address of the sender, mails sent by whom are to be intercepted by the rule. You can use wildcard characters (*, ?) to enter username/domain name in part, so that all mails containing sender address with partial text entered in this field will be intercepted. For example, entering '*@hell.com' intercepts mails from all users from the domain name 'hell.com', entering 'evilspirit@*', processes all mails with sender name 'evilspirit' from any domain and entering '*@*' intercepts all the mails with parameters entered in the fields below.
- **Recipient** - Enter the username part of the email address of the recipient, mails sent to whom are to be intercepted by the rule. The domain name part will be auto-populated with the domain name from which the rule is created. You can use wildcard characters (*, ?) to enter username in part, so that all mails containing 'To' address with partial text entered in this field will be intercepted.

- **Received from** - Enter the hostname or IP address of the external mail server, mails sent from which, are to be intercepted by the rule. You can use wildcard characters (*, ?) to enter server name in part. For example, entering 'mailxxx*' will intercept all mails that contain "mailxxx" in part in the 'Received From' field of the mail header. To specify all sender mail servers, enter just the wildcard character.
 - **Received by** - Enter the primary relay of the sending server or the MTA, mails sent through which, are to be intercepted by the rule. You can use wildcard characters (*, ?) to enter server name in part. For example, entering 'mailyyy*' will intercept all mails that contain "mailyyy" in part in the 'Received By' field of the mail header. To specify all mail servers, enter just the wildcard character.
 - **Subject** – Enter keywords that you want the rule to search for in the subject lines of emails. The rule will apply if any of these words are found. Please note the search sub-string may match values in the middle of the word. Leading and trailing spaces will be trimmed.
 - **Forward email** - This field is available only for 'FORWARD' rule. Enter the email address to which the emails containing values in the email header as configured in the fields above are to be forwarded.
- Click 'Save' to add the rule to the list of rules.



Edit a rule

- Select the rule to be edited and click the 'Edit' button from the top.

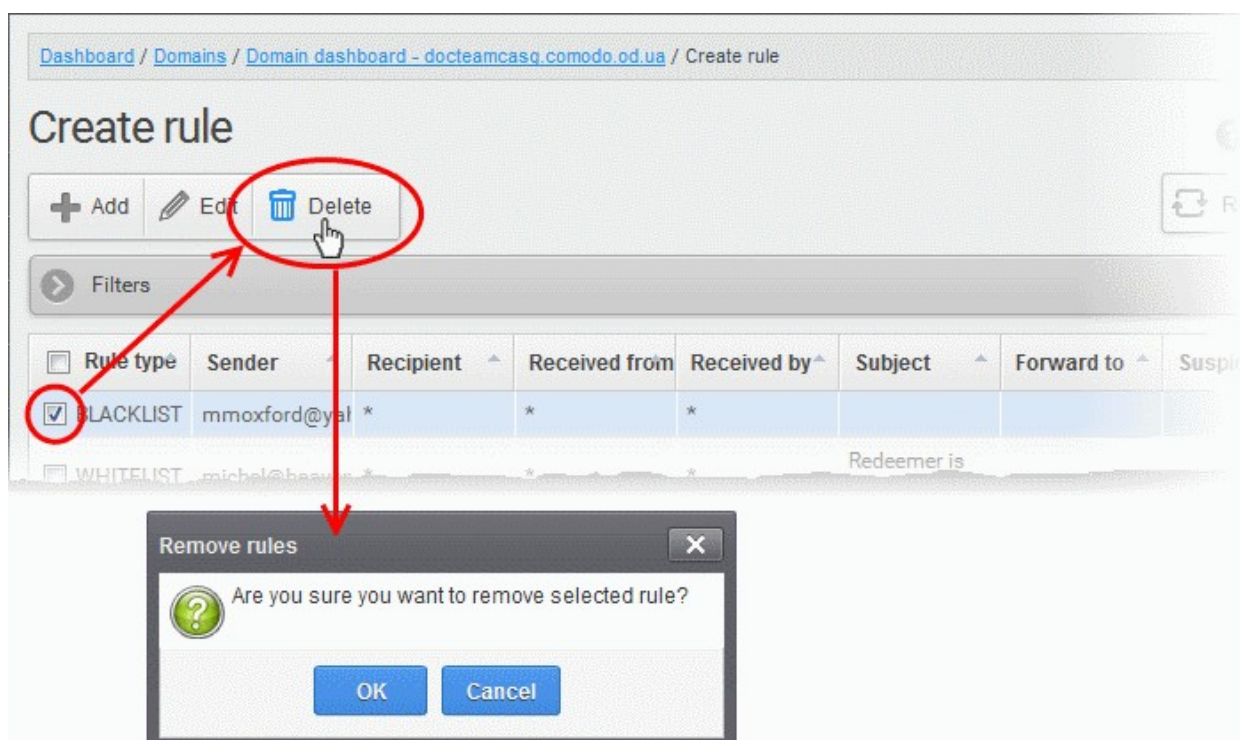


The 'Edit filter rule' dialog will appear for the rule. This dialog is similar to the 'Add rule' dialog. For descriptions of the options in this dialog, please see the explanation [above](#).

- Edit the values in the fields as required and click 'Save'.

Remove a rule

- Select the rule you want to remove and click the 'Delete' button.



A confirmation dialog will appear.

- Click 'OK' to remove the rule.

TLD and gTLD Rules

- You can allow or deny mails based on the top level domain (TLD) of the external mail server.
- By default, CASG accepts mails from all TLD names.
- You can also add custom TLDs from which you want to allow/block mail.

Open the TLD interface

- Click 'Domain Rules' > 'TLD & gTLD Rules':

Dashboard / Domains / Domain dashboard - docteamcasq.comodo.od.ua / Accepted domains

Accepted domains

<input checked="" type="checkbox"/> Australasia/Pac	<input checked="" type="checkbox"/> Asia	<input checked="" type="checkbox"/> Europe/Atle	<input checked="" type="checkbox"/> Africa/Midd	<input checked="" type="checkbox"/> Americas/C	<input type="checkbox"/> gTLD A-C	<input checked="" type="checkbox"/> gTLD D-H	<input checked="" type="checkbox"/> gTLD I-Q	<input checked="" type="checkbox"/> gTLD c R-T	<input checked="" type="checkbox"/> gTLD U-Z
<input checked="" type="checkbox"/> KIWI	<input checked="" type="checkbox"/> NAGOYA	<input checked="" type="checkbox"/> EU	<input checked="" type="checkbox"/> YT	<input checked="" type="checkbox"/> MS	<input checked="" type="checkbox"/> BAND	<input checked="" type="checkbox"/> DIGITAL	<input checked="" type="checkbox"/> KAUFEN	<input checked="" type="checkbox"/> RESTAURANT	<input checked="" type="checkbox"/> VOTING
<input checked="" type="checkbox"/> NU	<input checked="" type="checkbox"/> TOKYO	<input checked="" type="checkbox"/> GR	<input checked="" type="checkbox"/> JOBURG	<input checked="" type="checkbox"/> NYC	<input checked="" type="checkbox"/> BARGAINS	<input checked="" type="checkbox"/> DIRECTORY	<input checked="" type="checkbox"/> KITCHEN	<input checked="" type="checkbox"/> REVIEWS	<input checked="" type="checkbox"/> WANG
<input checked="" type="checkbox"/> NZ	<input checked="" type="checkbox"/> TW	<input checked="" type="checkbox"/> HAMBURG	<input checked="" type="checkbox"/> SC	<input checked="" type="checkbox"/> TC	<input type="checkbox"/> COUNTRY	<input checked="" type="checkbox"/> EDUCATION	<input checked="" type="checkbox"/> LGBT	<input checked="" type="checkbox"/> SARL	<input checked="" type="checkbox"/> WIN
<input checked="" type="checkbox"/> PH	<input checked="" type="checkbox"/> JIP	<input checked="" type="checkbox"/> IS		<input checked="" type="checkbox"/> US	<input checked="" type="checkbox"/> BIO	<input checked="" type="checkbox"/> EMAIL	<input checked="" type="checkbox"/> LIFE	<input checked="" type="checkbox"/> SCHOOL	<input checked="" type="checkbox"/> WINE
<input checked="" type="checkbox"/> PW	<input checked="" type="checkbox"/> MN	<input checked="" type="checkbox"/> IT		<input checked="" type="checkbox"/> VC	<input checked="" type="checkbox"/> BLACK	<input checked="" type="checkbox"/> ENGINEERING	<input checked="" type="checkbox"/> LIMO	<input checked="" type="checkbox"/> SERVICES	<input checked="" type="checkbox"/> WORLD
<input checked="" type="checkbox"/> SG	<input checked="" type="checkbox"/> KAN	<input checked="" type="checkbox"/> LI		<input checked="" type="checkbox"/> VEGAS	<input checked="" type="checkbox"/> BLACKFRIDAY	<input checked="" type="checkbox"/> ENTERPRISES	<input checked="" type="checkbox"/> LINK	<input checked="" type="checkbox"/> SEXY	<input checked="" type="checkbox"/> WTF
								<input checked="" type="checkbox"/> HORSE	
								<input checked="" type="checkbox"/> HOST	
								<input checked="" type="checkbox"/> HOSTING	
								<input checked="" type="checkbox"/> HAUS	
								<input checked="" type="checkbox"/> HOUSE	
								<input checked="" type="checkbox"/> HOW	

1 / 1 Per page 15

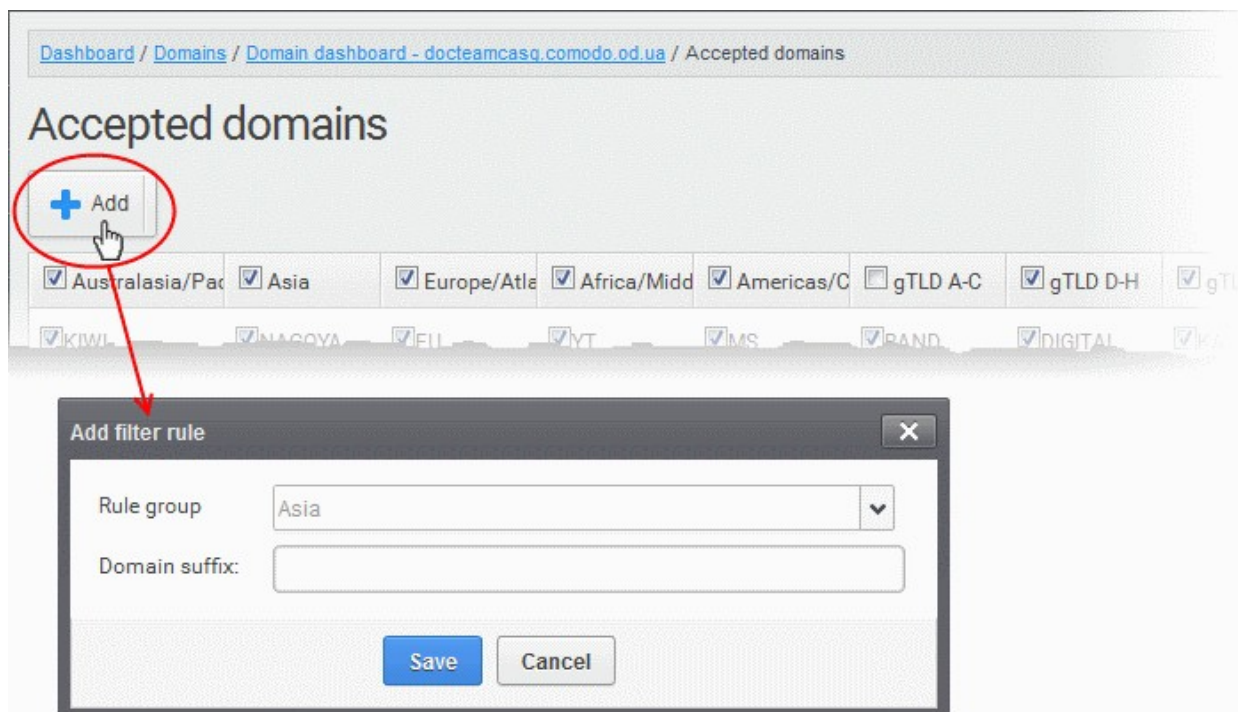
- 'Accepted domains' shows TLDs according to location, and gTLDs by alphabetical grouping. These categories are shown in the column headers and are known as 'Rule Groups'.
- All TLDs are enabled (accepted) by default.
- You can disable TLDs/gTLDs from which you do not want to accept mail.

The interface also allows you to:

- **Add new custom TLDs**
- **Configure TLD based mail filtering**

Add a new custom TLD

- Click 'Add' from the Accepted domains interface



The 'Add filter rule dialog' will appear.

- Choose the category from the 'Rule group' drop-down
- Enter the TLD name, without the '.' prefix, in the 'Domain suffix' text field
- Click 'Save' to add the TLD to the list
 - To allow the emails from mail servers with the new TLD, leave it selected
 - To block the emails from the mail servers with the new TLD, de-select it.

Configure TLD based mail filter

- Deselect TLDs from which you want to block mail. Enable TLDs from which you want to accept mail.

Recipient Whitelist

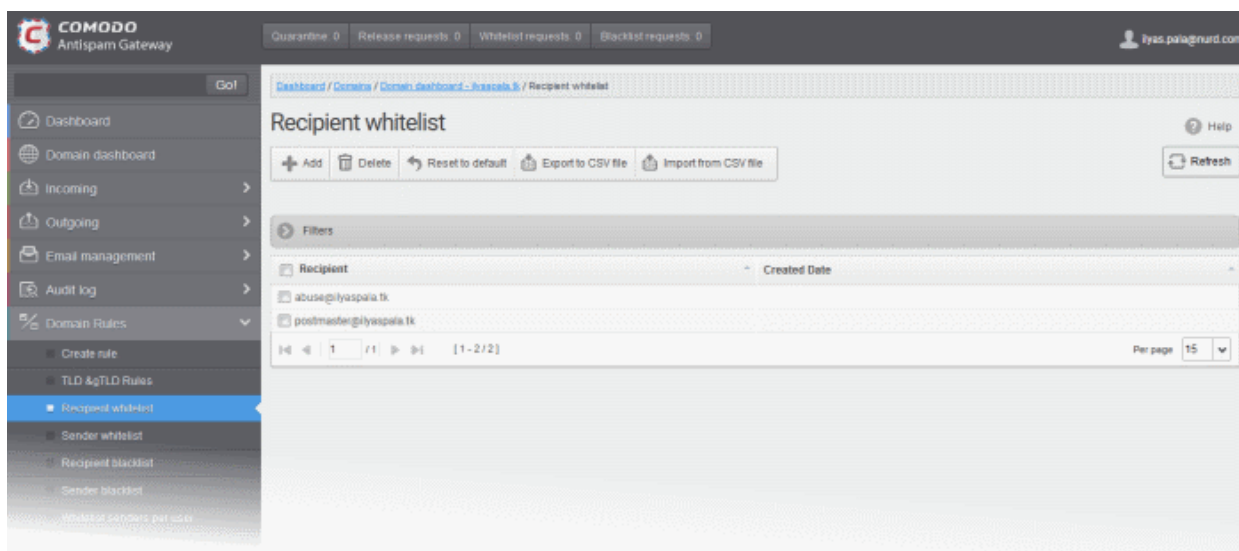
Since all filtering for whitelisted recipients is disabled, we recommend you use this option only in special circumstances. For example - abuse@domain.com and postmaster@domain.com

The recipient whitelist interface lets you:

- **Add users to recipient whitelist**
- **Export the list to CSV file for use in future**
- **Remove users from recipient whitelist**
- **Reset the list** - Delete all whitelisted recipients except the default recipients by clicking the 'Reset to default' button

Configure recipient whitelist

- Click 'Domain Rules' > 'Recipient whitelist' in the left-hand menu.



By default, the selected domain will have 'abuse' and 'postmaster' as whitelisted recipients.

- Recipient – Whitelisted recipients' mail address
- Created date – Date and time the user was added

Add Users to Recipient List

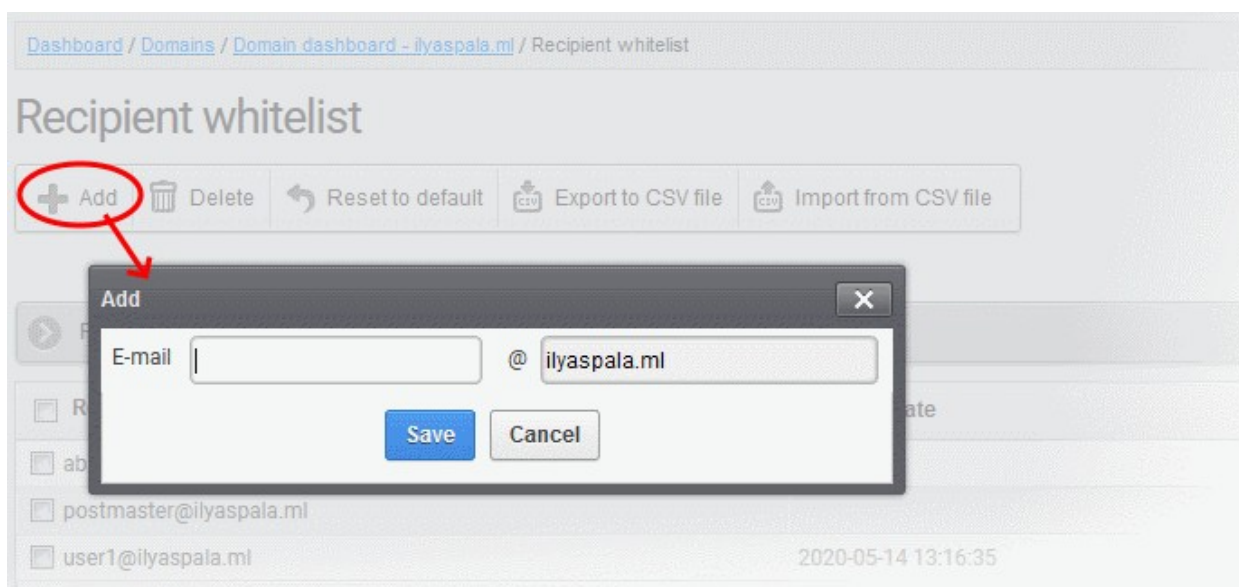
You can add recipients to the whitelist in the following ways:

- **Manually add the recipients**
- **Import recipients from a CSV file**

Manually add recipients

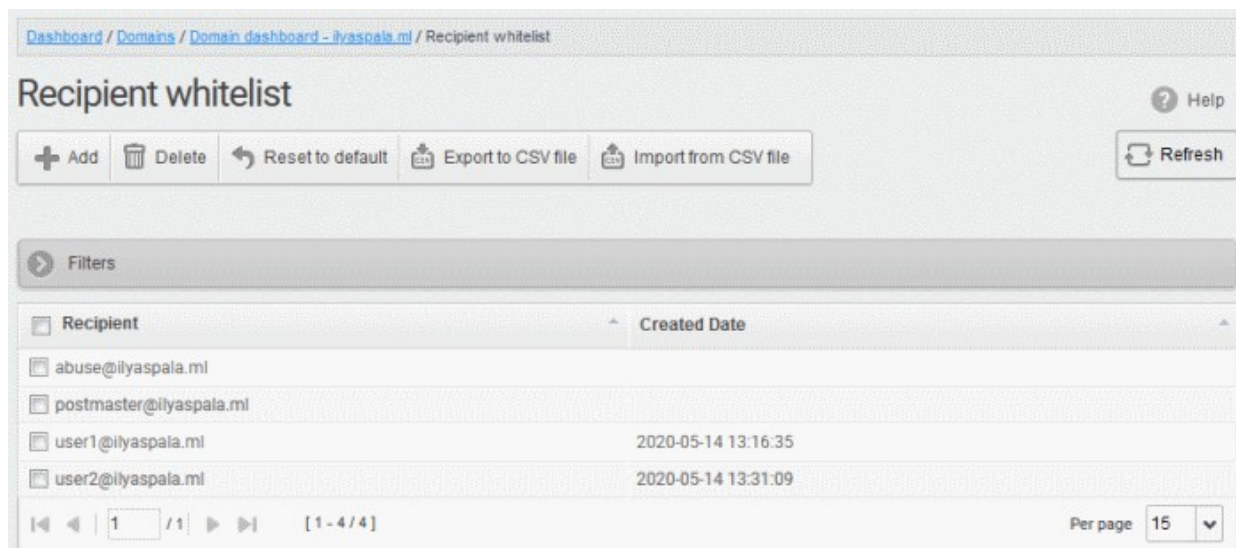
- Click 'Domain Rules' > 'Recipient whitelist' in the left-hand menu.
- Click 'Add' to add a new user to the list

The 'Add' dialog opens:



- Enter the recipient's name in the 'E-mail' text field and click the 'Save' button.
- To add a particular set of recipients to the whitelist, prefix or suffix the wildcard * in the E-mail text field. For example, enter *.stores for all the recipients in stores department to be whitelisted.
- To add a whole domain to whitelist, enter the wildcard * in the E-mail text field and click the 'Save' button. Now all the recipients in that domain will be whitelisted.

The recipient's name is added to the list.



Import users to whitelist from CSV file

Administrators can import many users to the recipient whitelist from a .csv file. Specify users in separate lines. See example below:

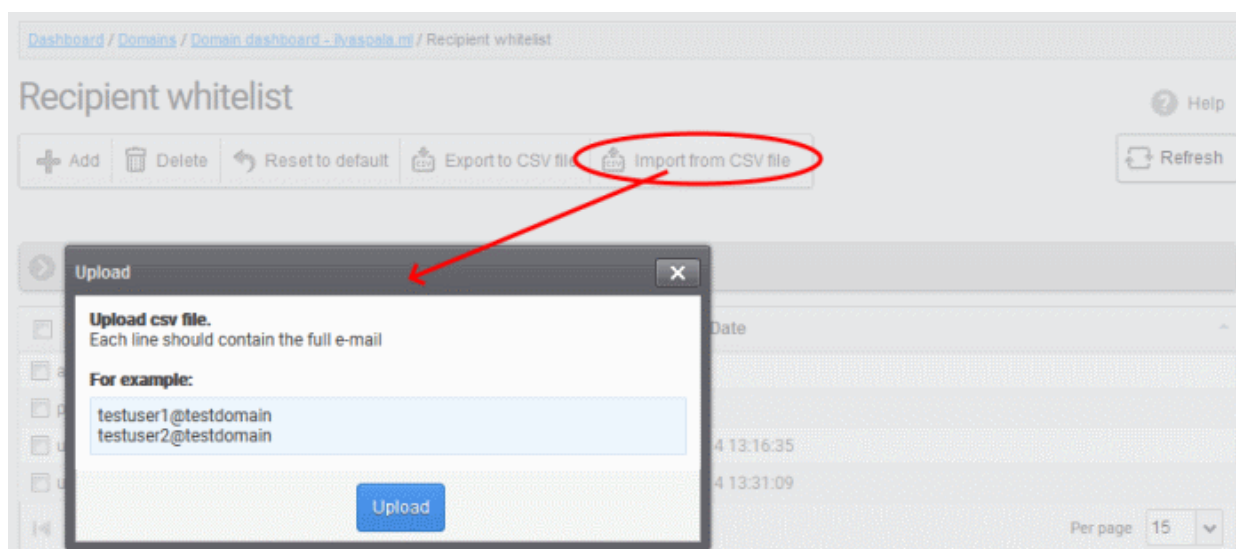
user1@testdomain.com

user2@testdomain.com

user3@testdomain.com

- Click the 'Import from CSV file' button

The 'Upload' dialog opens:



- Click the 'Upload' button and navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.

The upload is placed in import tasks queue and the progress is shown.

Remove the upload from the queue

- Click the 'Remove import task' button. If the task is in progress, 'Remove import task' deletes only the remaining part of the task.

Dashboard / Domains / Domain dashboard - ilyaspala.ml / Recipient whitelist

Recipient whitelist

Import is in process. Please wait

+ Add Delete Reset to default **Remove import task** Export to CSV file Refresh

Filters

Recipient	Created Date
abuse@ilyaspala.ml	
postmaster@ilyaspala.ml	
user1@ilyaspala.ml	2020-05-14 13:16:35
user2@ilyaspala.ml	2020-05-14 13:31:09

1 / 1 [1 - 4 / 4] Per page 15

On completion of the upload process, the users are imported and added to the list:

Dashboard / Domains / Domain dashboard - Ilyaspala.ml / Recipient whitelist

Recipient whitelist Help

Total lines processed 6

Imported 6 user(s)

Import for domain Ilyaspala.ml has been finished

+ Add Delete Reset to default Export to CSV file Import from CSV file Refresh

Filters

Recipient	Created Date
abuse@ilyaspala.ml	
postmaster@ilyaspala.ml	
user1@ilyaspala.ml	2020-05-14 13:16:35
user2@ilyaspala.ml	2020-05-14 13:31:09
user3@ilyaspala.ml	2020-05-14 14:08:53
user4@ilyaspala.ml	2020-05-14 14:08:53
user5@ilyaspala.ml	2020-05-14 14:08:53
user6@ilyaspala.ml	2020-05-14 14:08:53
user7@ilyaspala.ml	2020-05-14 14:08:53

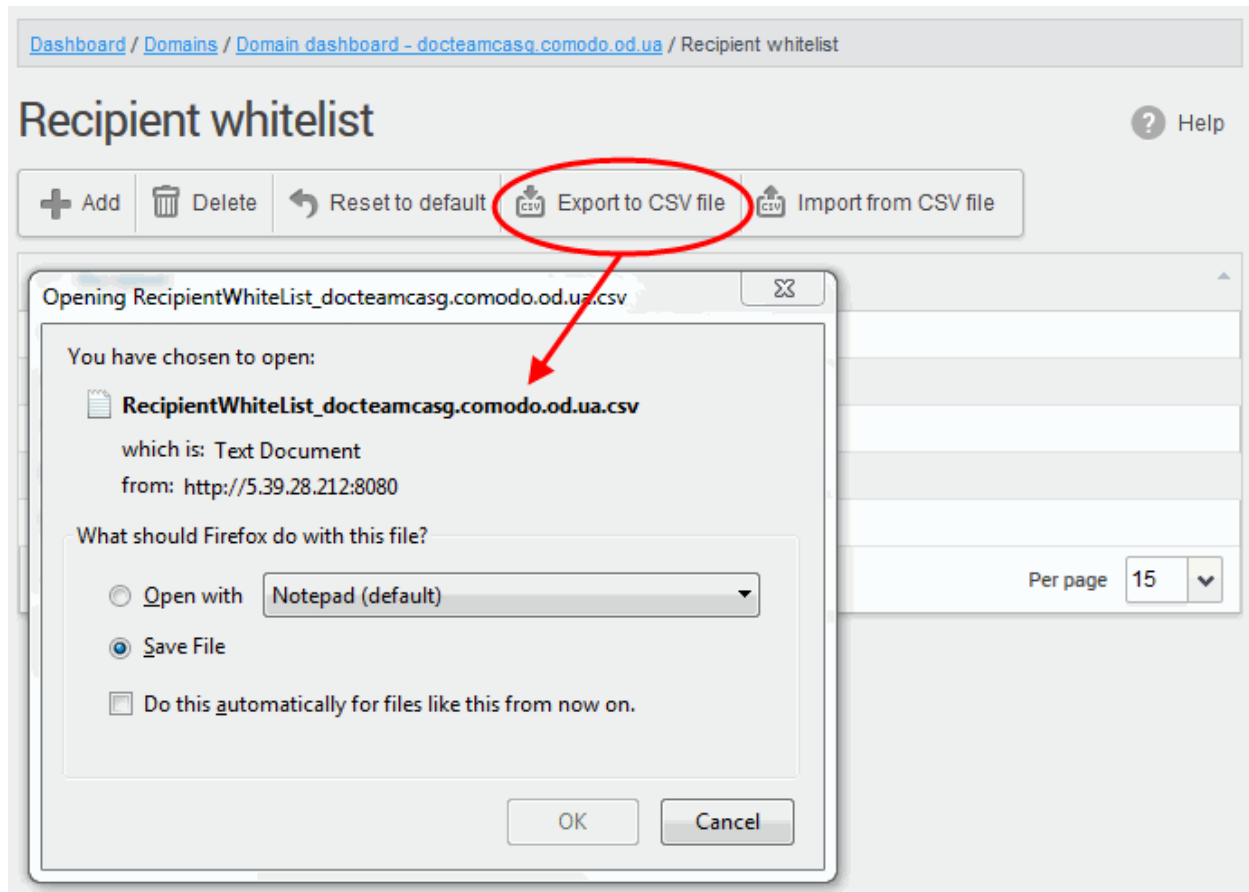
The administrator who carried out the task receives a notification about the import task completion.

Export the Recipient Whitelist to CSV file

You can save the configured recipient whitelist by exporting it as a CSV file. If required in future, administrators can import users from the csv file (for example, for a new account or after a reset).

Export the list

- Click the 'Export to CSV file' button to save the list of whitelisted recipients as a CSV file

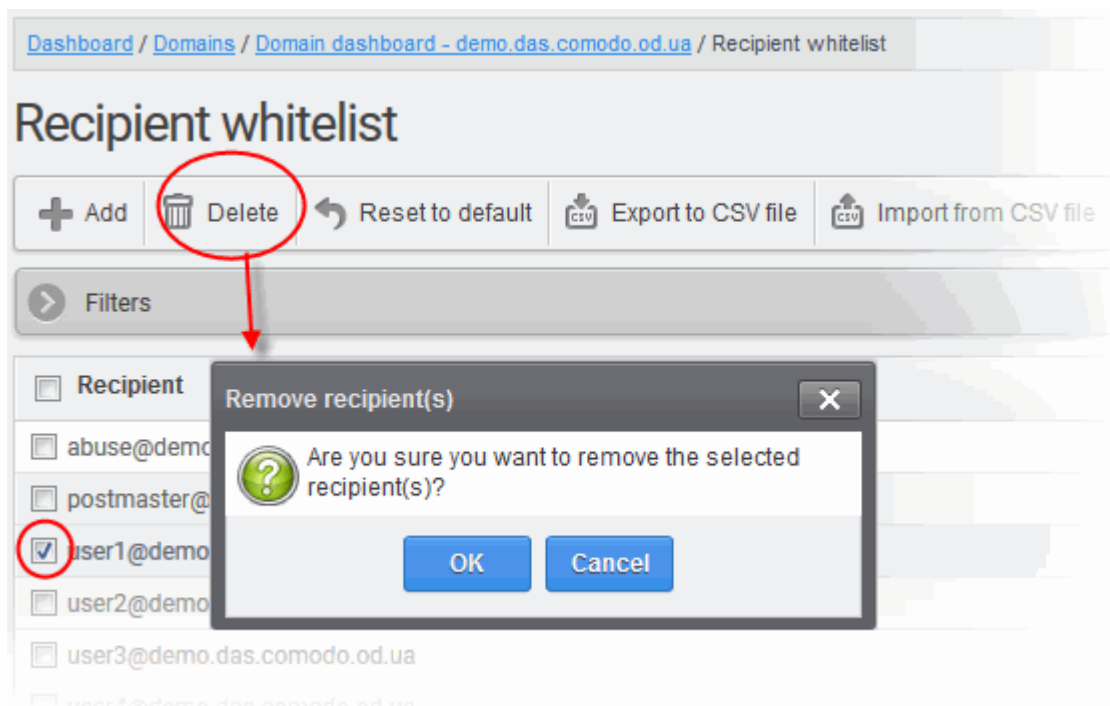


A file download dialog is displayed.

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

Delete Users from the Recipient Whitelist

- Select the recipient from the list and click the 'Delete' button



- Click 'OK' to confirm your changes

Sender Whitelist

- All filtering is disabled on mail sent by white-listed senders to recipients at the selected domain.
- The only exception is that mail from a white-listed sender which contains a suspicious attachment will still be blocked UNLESS the 'Suspicious attachment rule' is enabled. This may seem counter-intuitive on first reading.
- The following table shows how the 'Suspicious Attachment' option affects a sender white-list rule:

	Suspicious Attachment option	Suspicious file detected?	White-listing applied?
Rule Type 1	Enabled	Yes	Yes
		No	Yes
Rule Type 2	Disabled	Yes	No
		No	Yes

- Use Type 1 if you want all mails from a sender to be whitelisted and received, including those that contain suspicious attachments.
- Use Type 2 if you want to white-list all mails from a sender except those that contain suspicious attachments.

See the **Rules** section if you need more details.

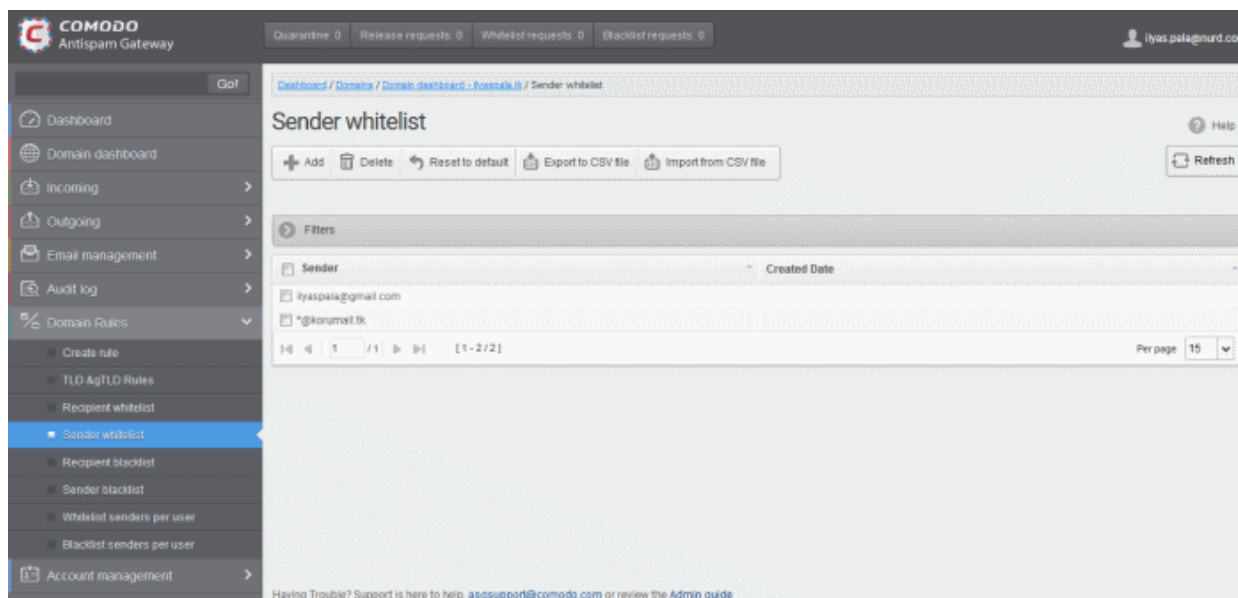
Comodo strongly recommends white-listing a sender only when the system wrongly blocks emails from a trusted sender. White-listing a sender over-rides 'Blacklist senders per user'. Refer to **Blacklist Senders Per User** for more details.

- **Add users to Sender whitelist**
- **Export the list to CSV file for use in future**
- **Remove users from Sender whitelist**
- **Reset the list** - Delete all whitelisted senders and make the list empty by clicking the 'Reset to default' button

Configure sender whitelist

- Click 'Domain Rules' > 'Sender Whitelist' in the left-hand menu.

The 'Sender whitelist' interface of the selected domain opens:



- **Sender** – Whitelisted sender email address
- **Created date** – Date and time the sender was added

Add Users to Sender Whitelist

You can add recipients to the white list in two ways:

- **Manually add senders**
- **Import senders from a CSV file**

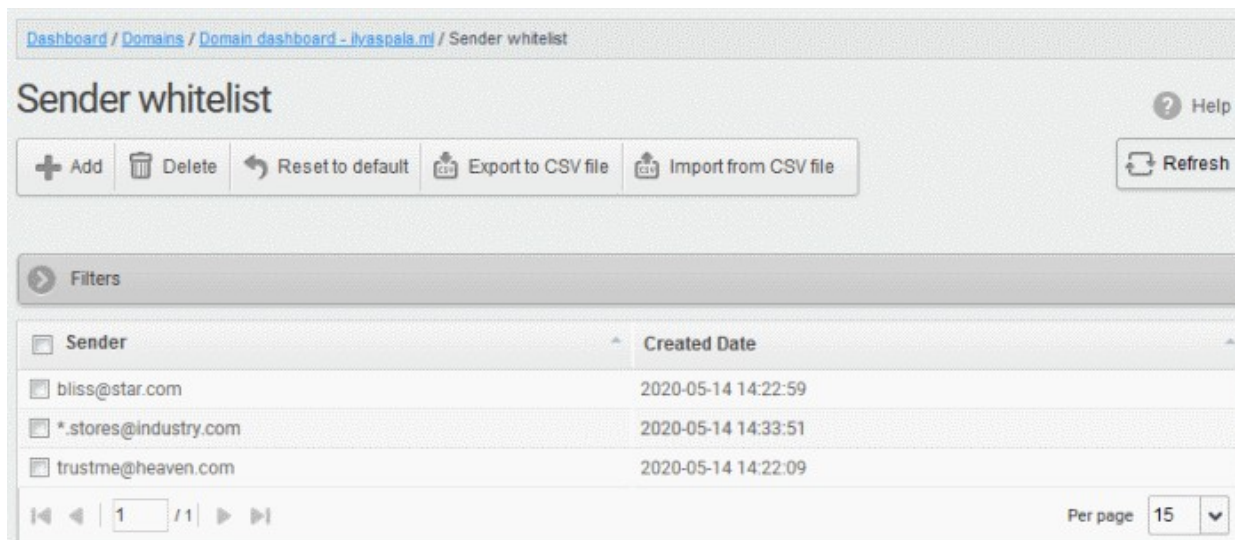
Manually add senders

- Click 'Add' to open the add whitelisted sender dialog:

- Enter the sender name in the 'E-mail' textbox and sender's email domain name after the @ symbol and click the 'Save' button. Repeat the process to add more whitelisted senders.
- To add a particular set of senders to whitelist, prefix or suffix the wildcard character * in the 'E-mail' text field and senders' email domain name after the @ symbol. For example, enter *.stores@domainname.com for all the senders in stores to be whitelisted.
- To add a specific username from any mail domain to the whitelist, enter the username in the mail text field and the wildcard character * after the @ symbol. For example, enter john@* for whitelisting the username 'john' with any email domain name.
- To add a set of users or specific username from any email domain with a specific top level domain (TLD) name like .com, .org, enter the wildcard character * or username in the Email text field and enter * followed by the TLD after the @ symbol. For example, '*@*.com' will whitelist all the senders from all the email domains ending with '.com'.
- To add a whole domain to whitelist, enter the wildcard character * in the E-mail text field and email domain after the @ symbol and click the 'Save' button. Now all the senders with the entered domain name are

whitelisted.

The senders are added to the whitelist:



Import senders to whitelist from CSV file

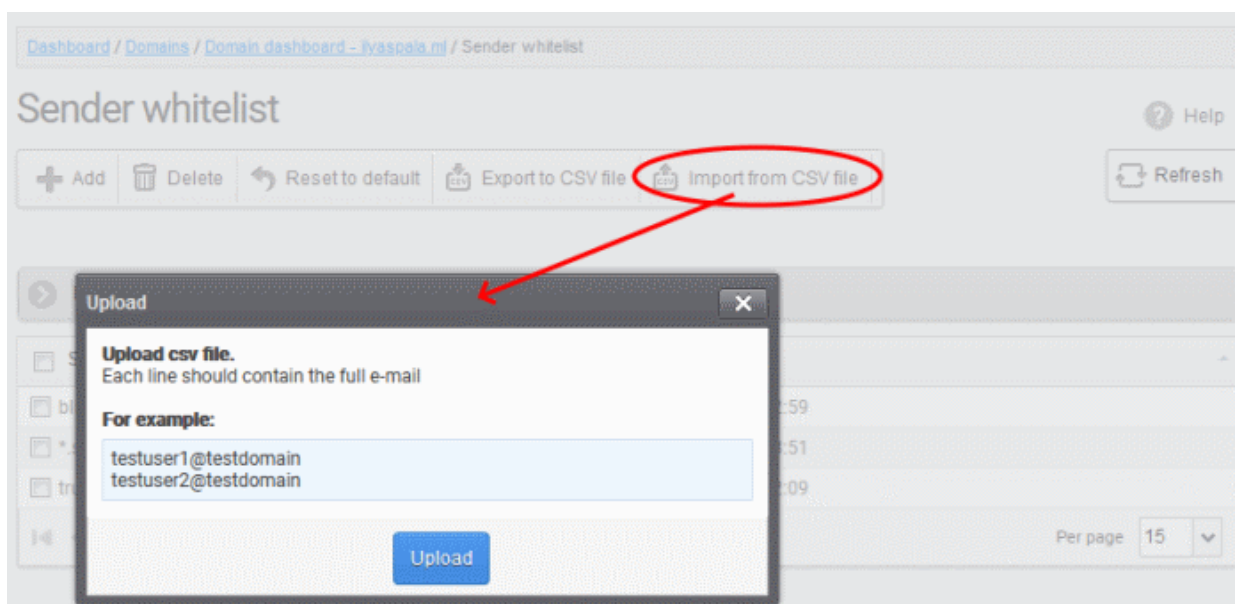
Administrators can import multiple senders from a .csv file. The senders' addresses should be saved in the following format:

sender1@domainname1.com

sender2@domainname2.com

sender3@domainname3.com

- Click the 'Import from CSV file' to import senders to whitelist from a CSV file.



- Click 'Upload', navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.

The upload is placed in import tasks queue and the progress of the upload is shown.

Remove the upload from the queue

- Click the 'Remove import task' button. The 'Remove import task' deletes only a remaining part of not imported task.

Dashboard / Domains / Domain dashboard - iyaspala.ml / Sender whitelist

Sender whitelist

Import is in process. Please wait

Filters

Sender	Created Date
<input type="checkbox"/> bliss@star.com	2020-05-14 14:22:59
<input type="checkbox"/> *.stores@industry.com	2020-05-14 14:33:51
<input type="checkbox"/> trustme@heaven.com	2020-05-14 14:22:09

Per page 15

On completion of the upload process, the result is displayed.

Dashboard / Domains / Domain dashboard - iyaspala.ml / Sender whitelist

Sender whitelist

Total lines processed 4

Imported 4 user(s)

Import for domain iyaspala.ml has been finished

Filters

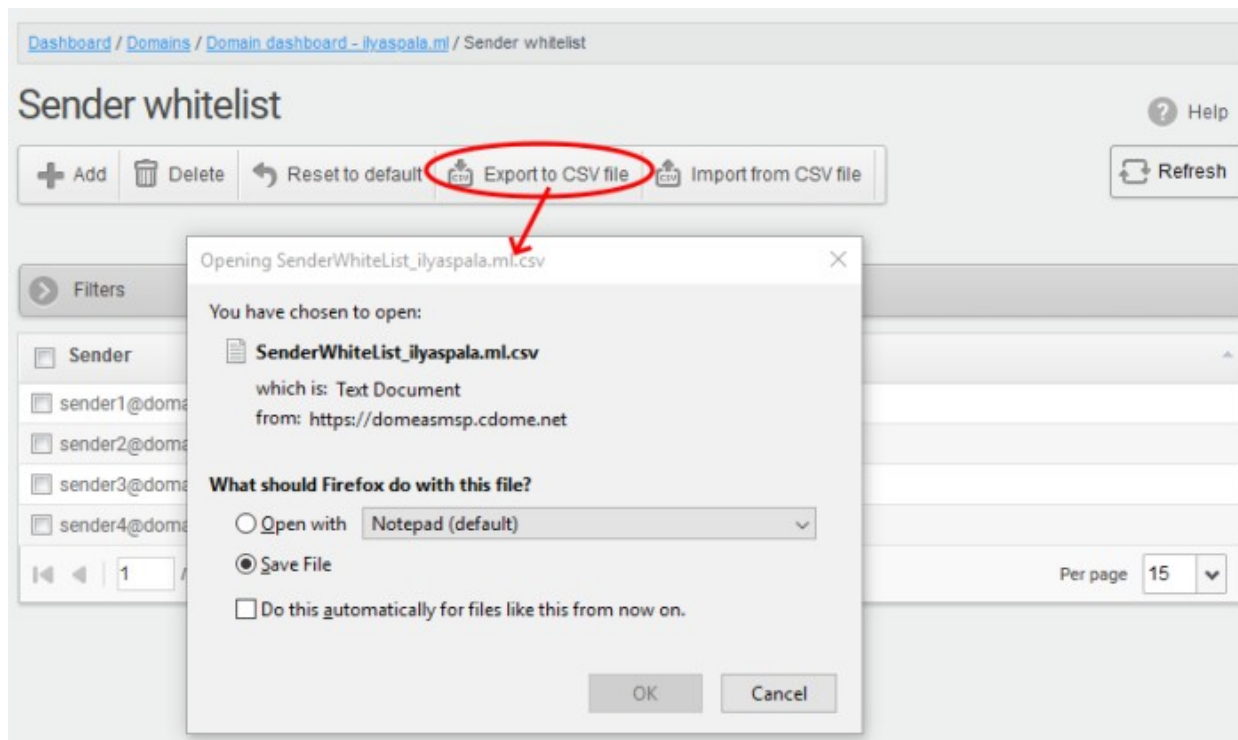
Sender	Created Date
<input type="checkbox"/> bliss@star.com	2020-05-14 14:22:59
<input type="checkbox"/> sender1@domainname1.com	2020-05-14 15:07:38
<input type="checkbox"/> sender2@domainname2.org	2020-05-14 15:07:39
<input type="checkbox"/> sender3@domainname3.in	2020-05-14 15:07:39
<input type="checkbox"/> sender4@domainname4.us	2020-05-14 15:07:39
<input type="checkbox"/> *.stores@industry.com	2020-05-14 14:33:51
<input type="checkbox"/> trustme@heaven.com	2020-05-14 14:22:09

Per page 15

The sender whietlist from .csv file is uploaded and the administrator who carried out the task receives a notification about the import task completion.

Export the Sender Whitelist to CSV file

- Click 'Export to CSV file' to save the list of whitelisted senders as a CSV file

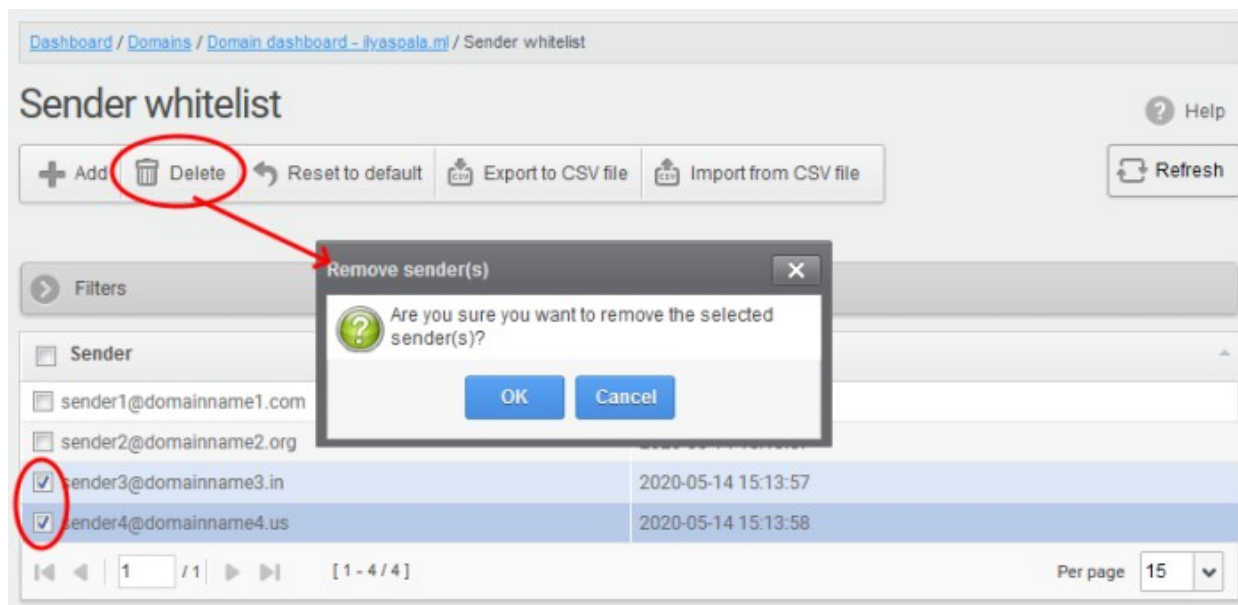


A file download dialog is displayed.

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

Delete Users from the Sender Whitelist

- Click 'Reset to default' to remove all whitelisted senders
- To remove particular sender(s) from the whitelist, select them from the list and click the 'Delete' button.



- Click 'OK' to confirm your changes.

Recipient Blacklist

- CASG will automatically block all emails to blacklisted recipients.
- Blocked messages are not quarantined and legitimate SMTP mail servers will send a bounce message to the sender.

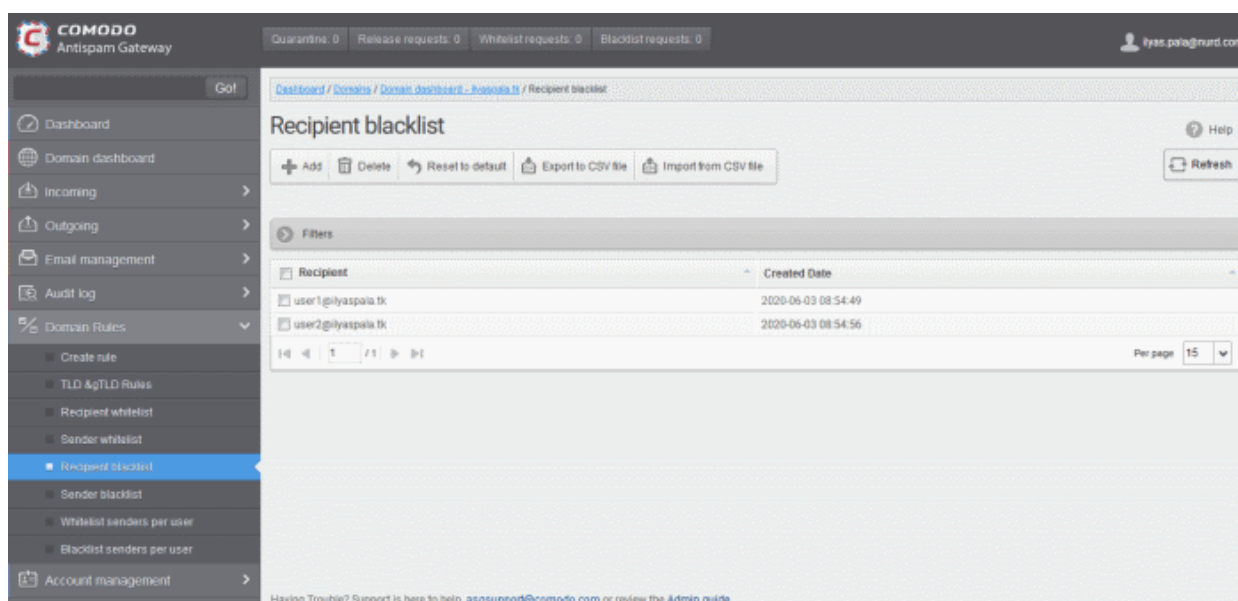
Administrators can:

- **Add users to the recipient blacklist**
- **Export the list to CSV file for use in future**
- **Remove users from recipient blacklist**
- **Reset the list** - Remove all recipients from the blacklist by clicking the 'Reset to default' button

Configure recipient blacklist

- Click the 'Recipient blacklist' from the 'Domain Rules' drop-down on the left

The 'Recipient blacklist' interface of the selected domain opens:



- **Recipient** – Blacklisted recipients' mail address
- **Created date** – Date and time the user was added

Add Users to Recipient Blacklist

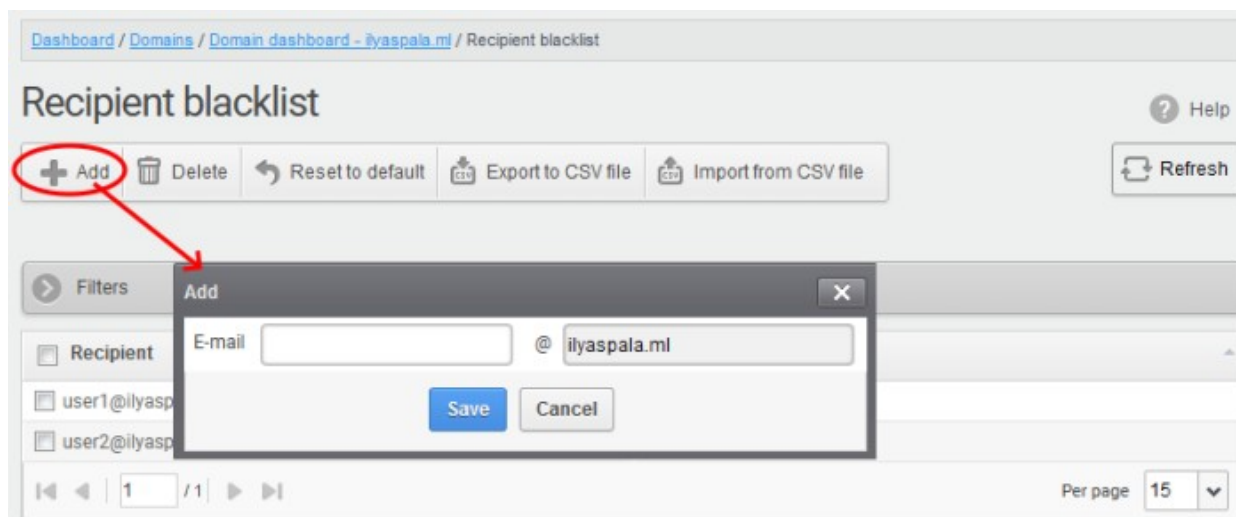
You can add recipients to the black list in the following ways:

- **Manually add the recipients**
- **Import recipients from a CSV file**

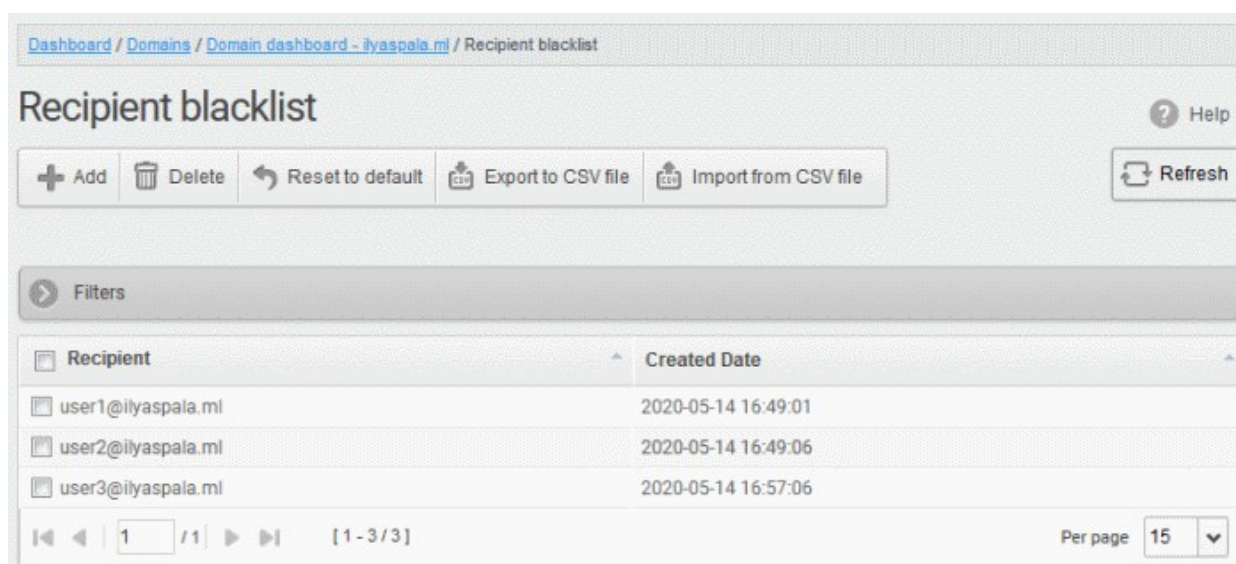
Manually add recipients

- Click 'Add' to add a new user to the list

The 'Add' dialog box opens:



- Enter the recipient name in the 'E-mail' textbox and click the 'Save' button. Repeat the process to add more recipients to blacklist.
- To add a particular set of recipients to blacklist, prefix or suffix the wildcard * in the 'E-mail' text field. For example, enter *.stores for all the recipients in stores department to be blacklisted.
- To add a whole domain to blacklist, enter the wildcard * in the 'E-mail' text field and click the 'Save' button. Now all the recipients in that domain are blacklisted.



The list of blacklisted recipients are displayed.

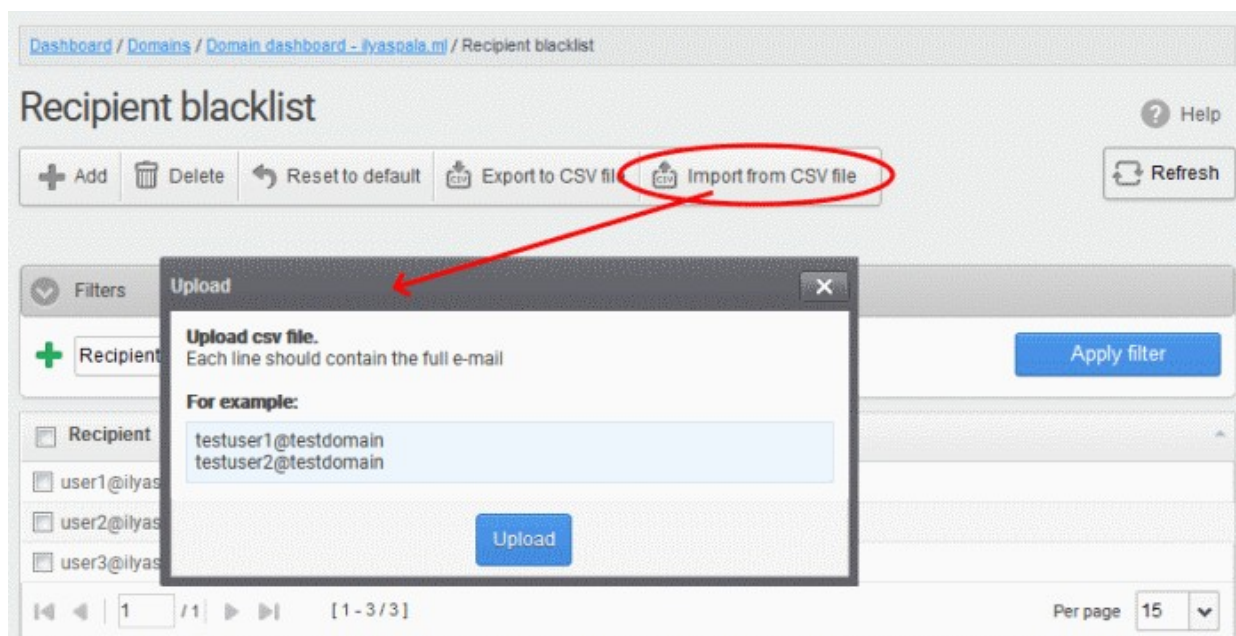
Import users to blacklist from CSV file

Administrators can import multiple users to the recipient blacklist from a .csv file. Specify users in separate lines. See example below:

```
user1@testdomain.com
user2@testdomain.com
user3@testdomain.com
```

- Click the 'Import from CSV file' button

The 'Upload' dialog opens:

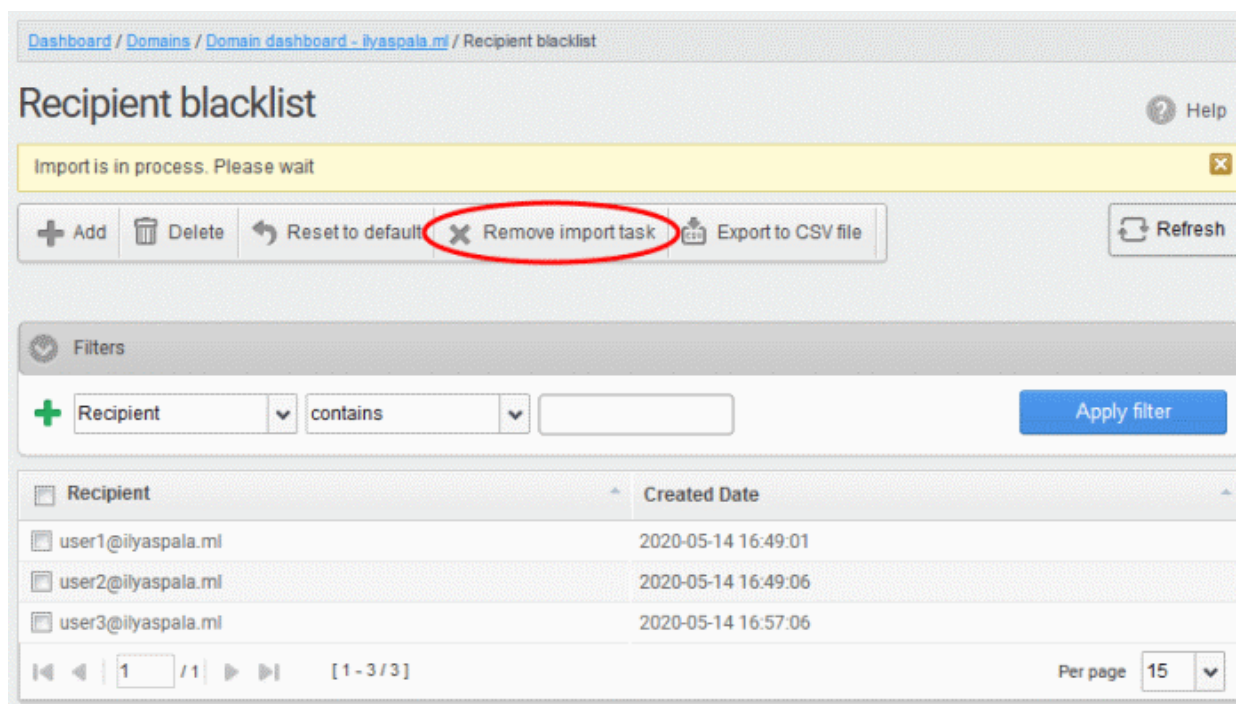


- Click 'Upload', navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.

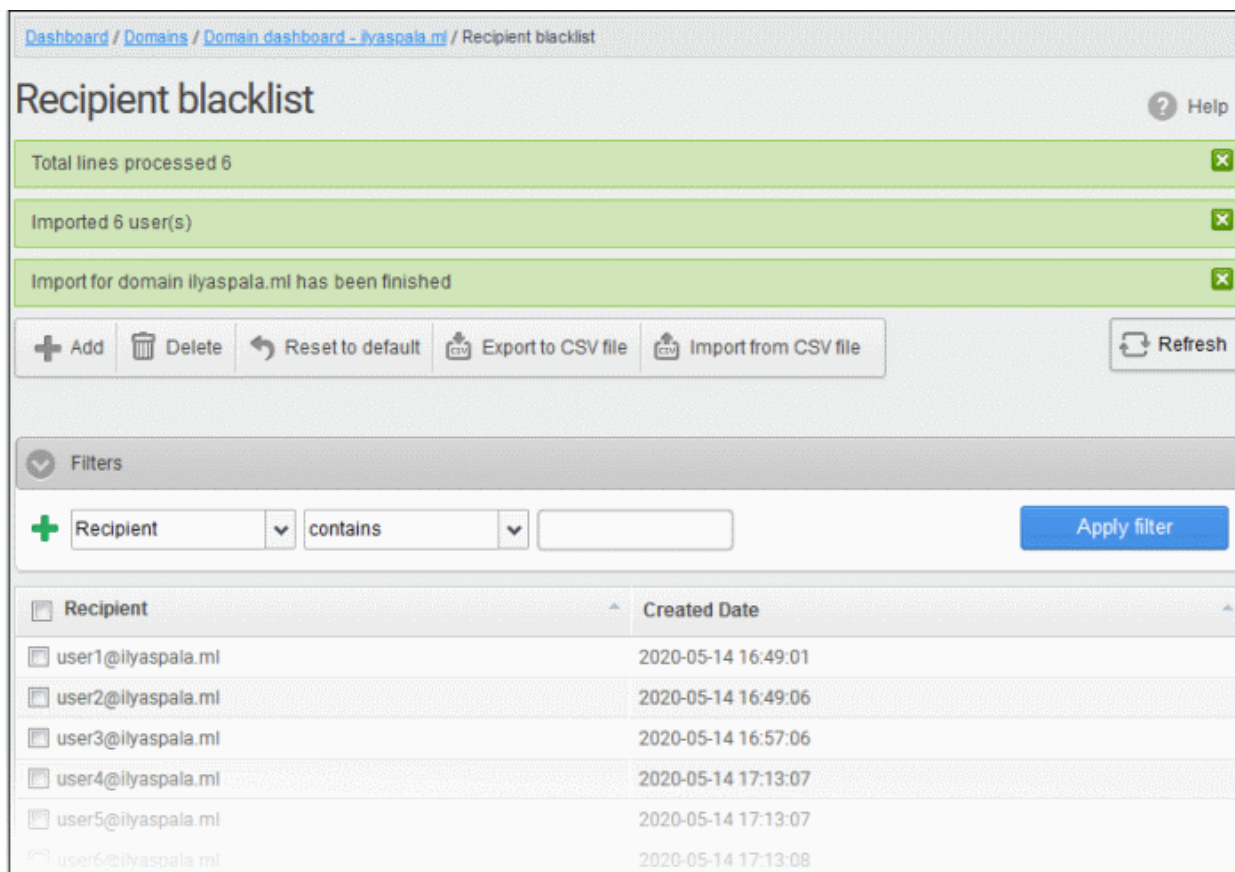
The upload is placed in import tasks queue and the progress of the upload is shown.

Remove the upload from the queue

- Click the 'Remove import task' button. 'Remove import task' deletes only the remaining part of an 'in-progress' task.



On completion of the upload process, the result is displayed.



Dashboard / Domains / Domain dashboard - ilyaspala.ml / Recipient blacklist

Recipient blacklist

Help

Total lines processed 6

Imported 6 user(s)

Import for domain ilyaspala.ml has been finished

+ Add Delete ↶ Reset to default 📄 Export to CSV file 📄 Import from CSV file Refresh

Filters

+ Recipient contains

Apply filter

Recipient	Created Date
user1@ilyaspala.ml	2020-05-14 16:49:01
user2@ilyaspala.ml	2020-05-14 16:49:06
user3@ilyaspala.ml	2020-05-14 16:57:06
user4@ilyaspala.ml	2020-05-14 17:13:07
user5@ilyaspala.ml	2020-05-14 17:13:07
user6@ilyaspala.ml	2020-05-14 17:13:08

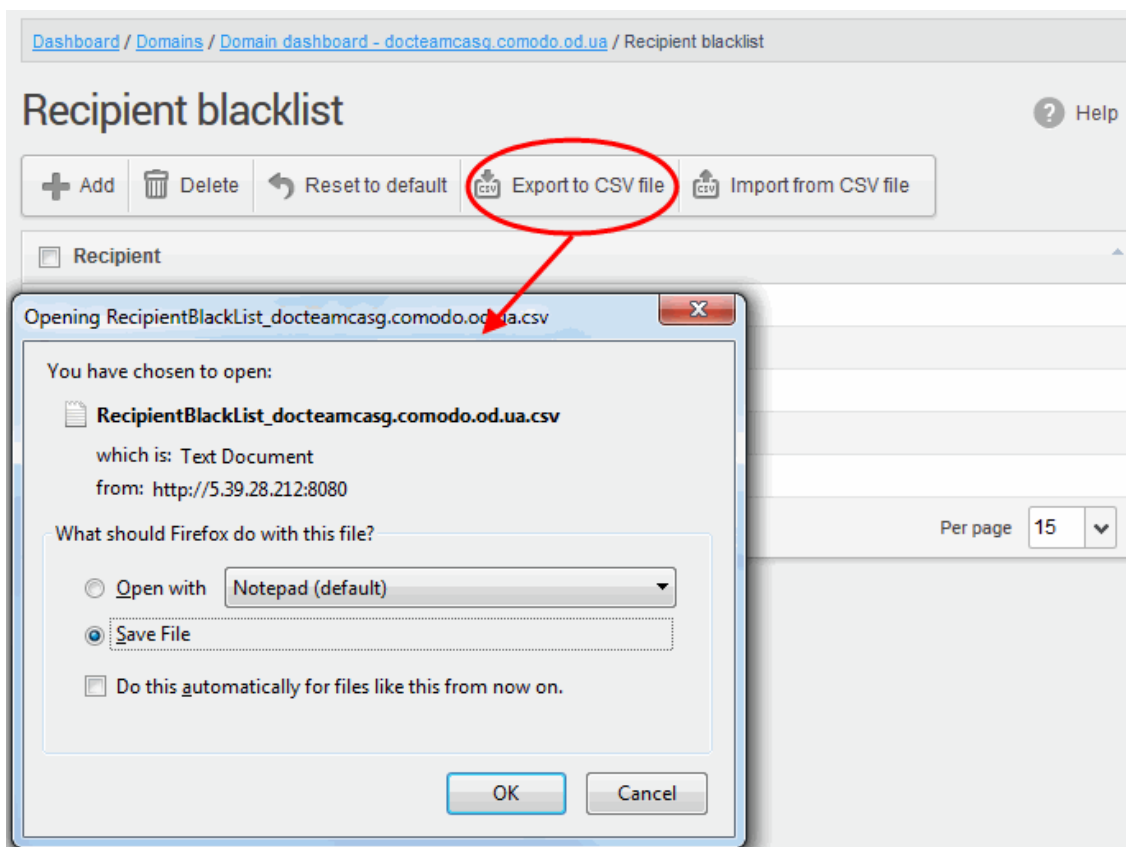
The recipient blacklist from .csv file are uploaded and the administrator who carried out the task receives a notification about the import task completion.

Export the Recipient Blacklist to CSV file

Administrators can save the recipient blacklist by exporting it as a CSV file. If required in future, the administrator can import the users from the csv file, for example for a new account or after a reset.

Export the list

- Click the 'Export to CSV file' to save the list of blacklisted recipients as a CSV file

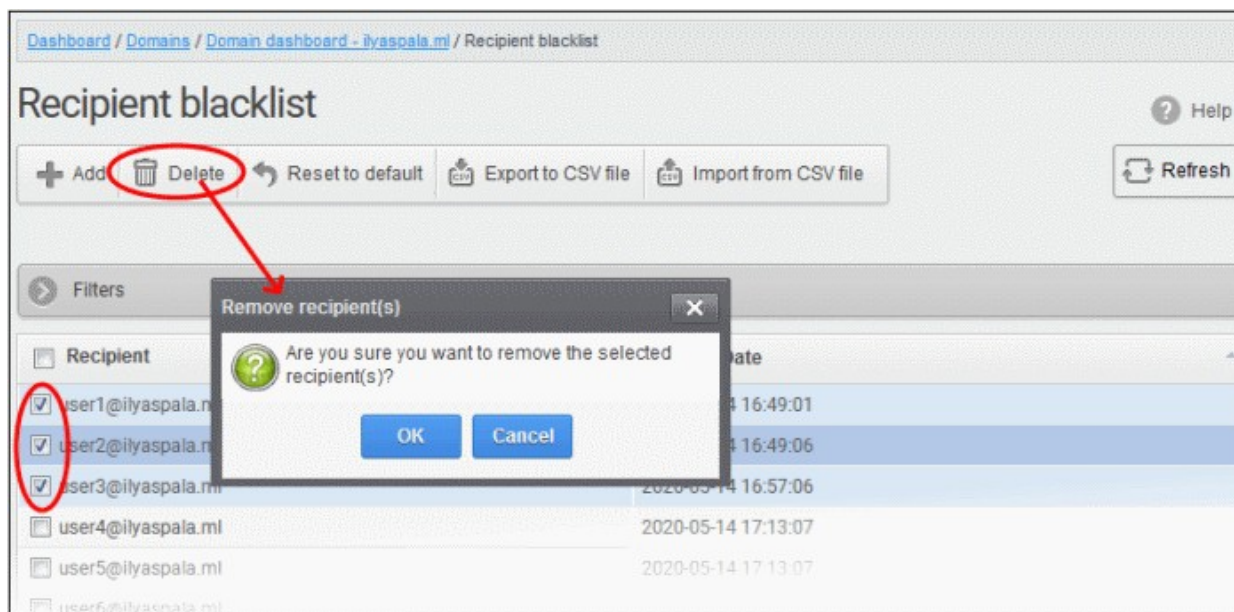


A file download dialog is displayed.

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

Delete Users from the Recipient Blacklist

- Click 'Reset to default' to remove all blacklisted recipients
- To remove recipient(s), select them from the list and click the 'Delete' button



- Click 'OK' to confirm your changes.

The user(s) are removed from the blacklist and the mails addressed to them are allowed as per the existing filter settings in CASG.

Sender Blacklist

- CASG automatically blocks all emails from blacklisted senders.
- Blocked messages are not quarantined and most mail servers will send a bounce message to the sender.

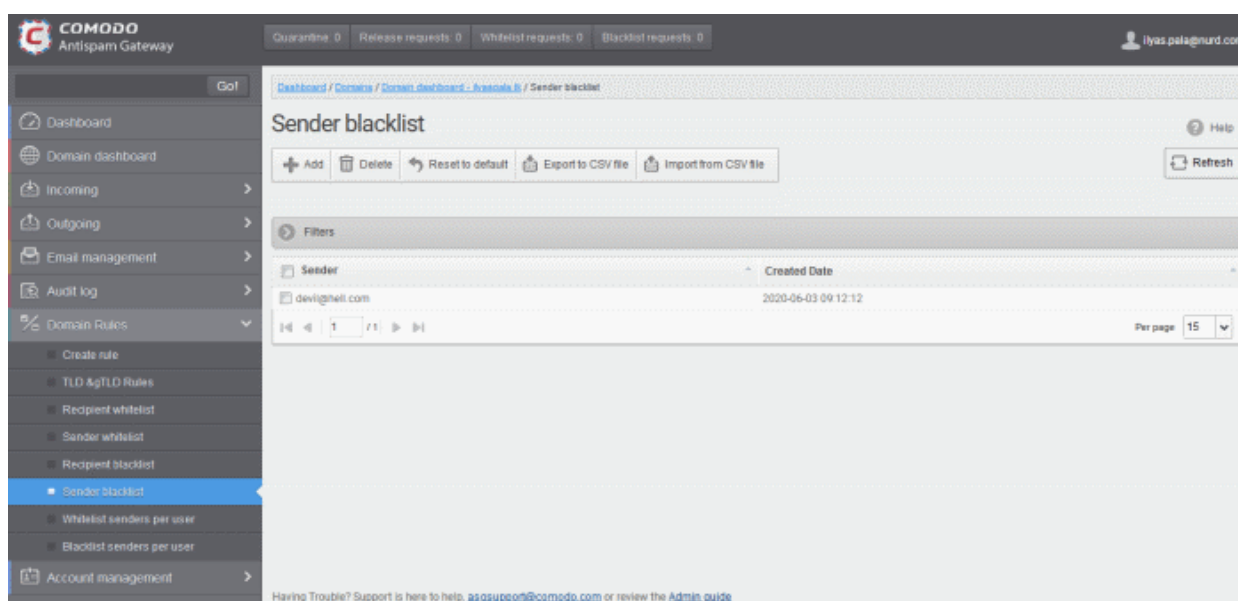
The sender blacklist interface allows admins to:

- **Add users to sender blacklist**
- **Export the list to CSV file for use in future**
- **Remove users from sender blacklist**
- **Reset the list** - Remove all senders from the blacklist by clicking the 'Reset to default' button

Configure sender blacklist

- Click the 'Sender blacklist' from the 'Domain Rules' drop-down on the left

The 'Sender blacklist' interface of the selected domain opens:



- **Sender** – Blacklisted senders' mail address
- **Created date** – Date and time the sender was added

Add Users to Senders Blacklist

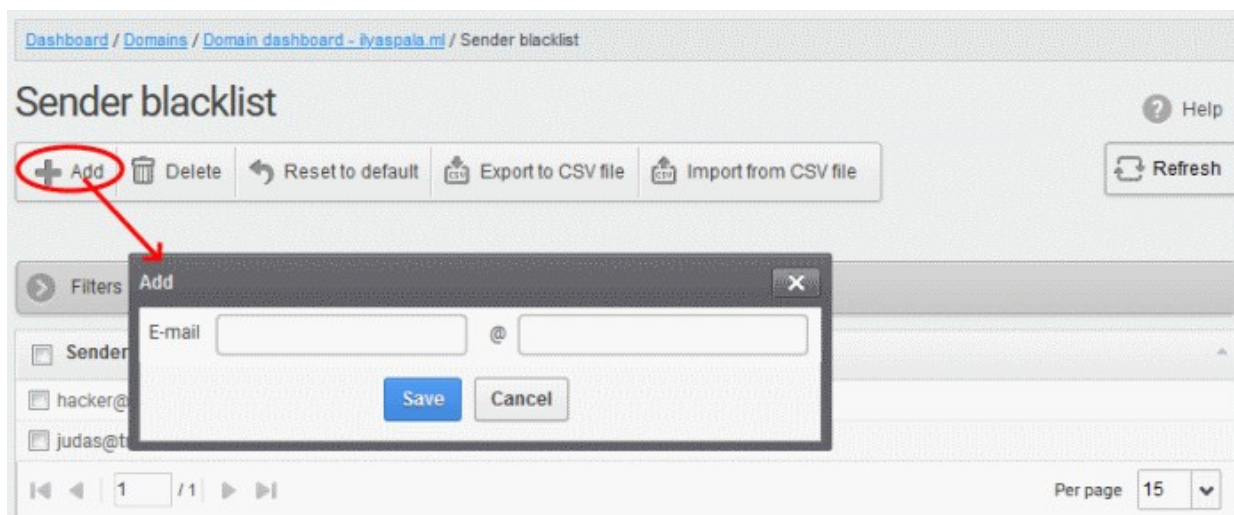
You can add senders to the blacklist in two ways:

- **Manually add the senders**
- **Import senders from a CSV file**

Manually add senders

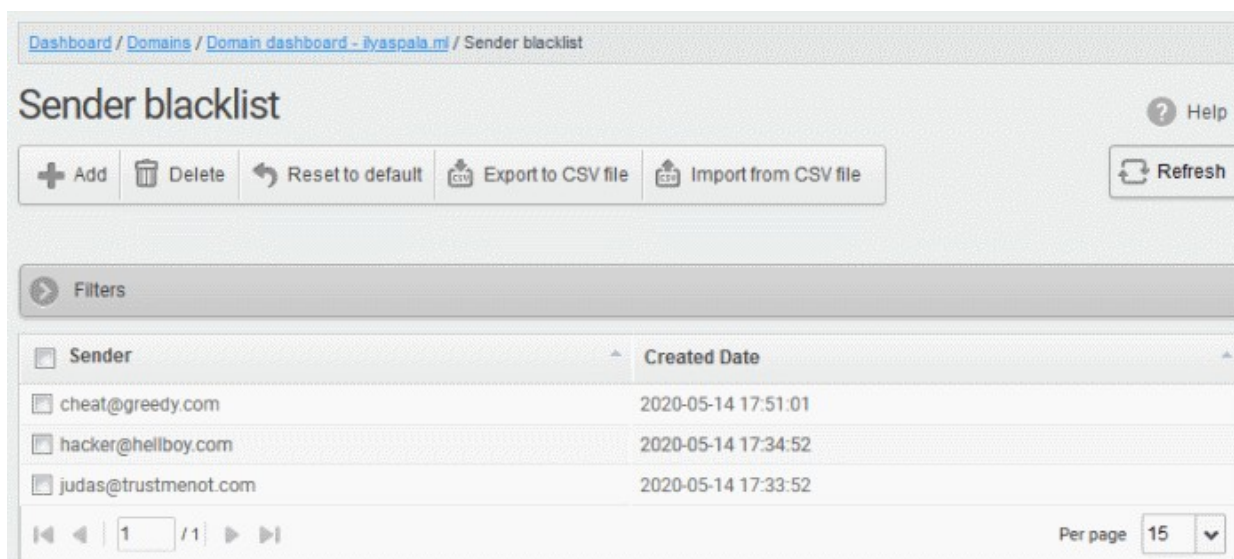
- Click 'Add' to add a new blacklisted sender

The 'Add' dialog box opens:



- Enter the sender name in the 'E-mail' textbox and sender's email domain name after the @ symbol and click the 'Save' button. Repeat the process to add more blacklisted senders.
- To add a particular set of senders to blacklist, prefix or suffix the wildcard character * in the 'E-mail' text field and senders' email domain name after the @ symbol. For example, enter *.stores@domainname.com for all the senders in stores department to be blacklisted.
- To add a specific username from any mail domain to the blacklist, enter the username in the mail text field and the wildcard character * after the @ symbol. For example, enter john@* for blacklisting the username 'john' with any email domain name.
- To add a set of users or specific username from any email domain with a specific top level domain (TLD) name like .com, .org, enter the wildcard character * or username in the Email text field and enter * followed by the TLD after the @ symbol. For example, '*@*.com' will blacklist all the senders from all the email domains ending with '.com'.
- To add a whole domain to blacklist, enter the wildcard character * in the E-mail text field and email domain after the @ symbol and click the 'Save' button. Now all the senders with the entered domain name are blacklisted.

The list of blacklisted senders are displayed.



Import senders to blacklist from CSV file

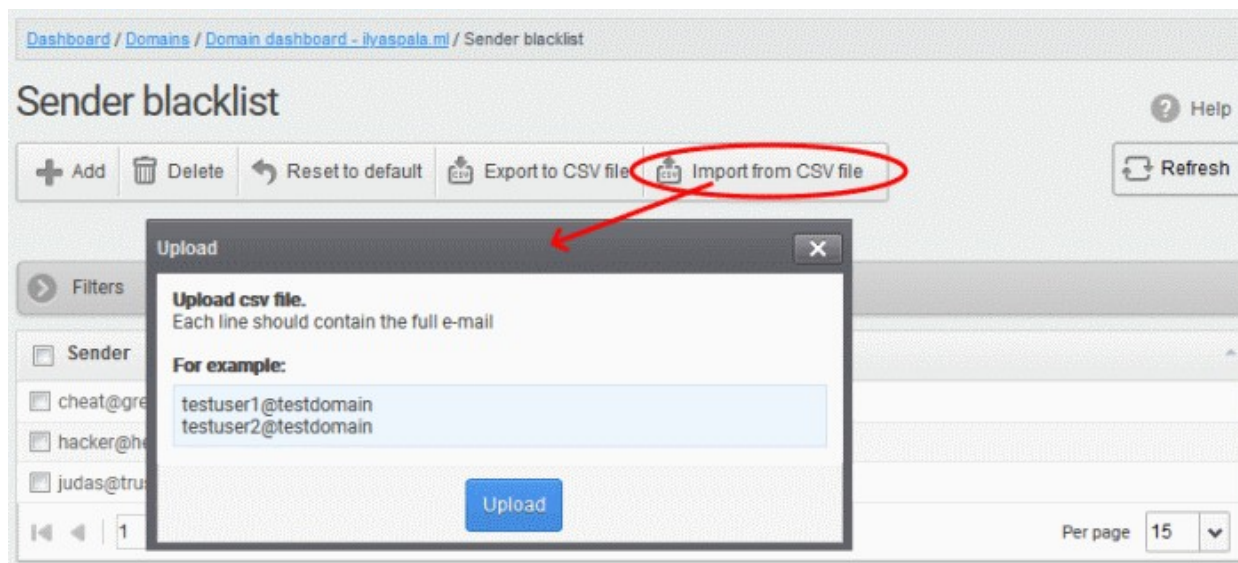
Administrators can import many senders from a file to sender blacklist at a time. The senders' address should be saved in the format shown below as an example:

sender1@domainname1.com

sender2@domainname2.com

sender3@domainname3.com

- Click the 'Import from CSV file' to add blacklist senders in bulk.

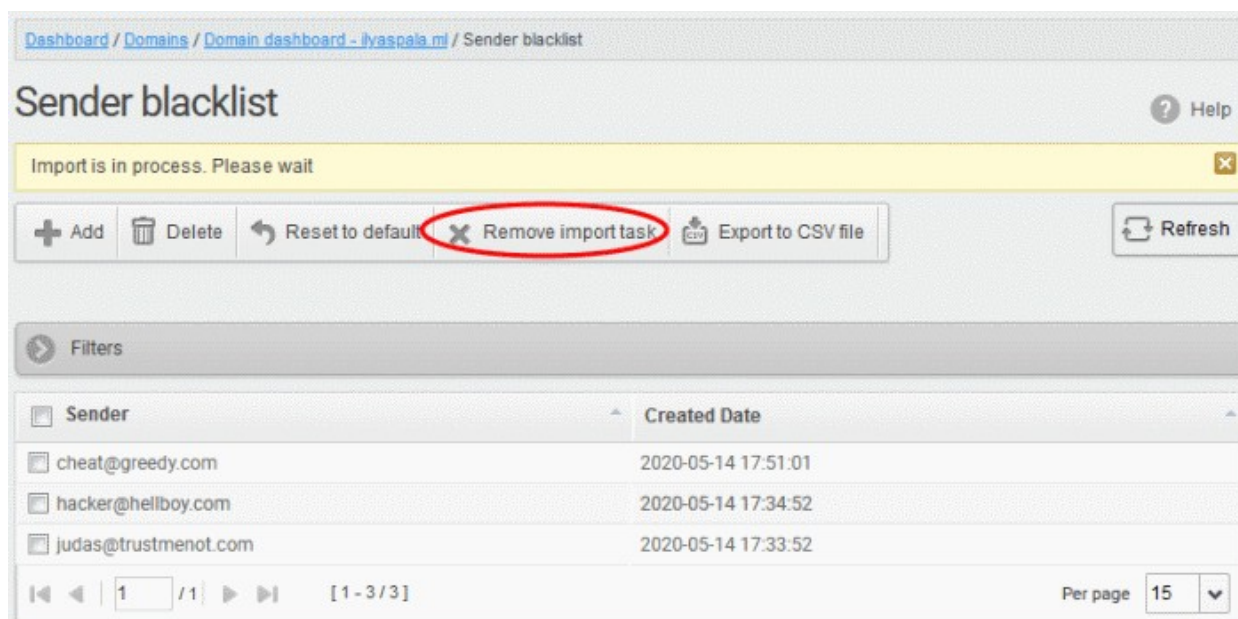


- Click 'Upload', navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.

The upload is placed in import tasks queue and the progress of the upload is shown.

Remove the upload from the queue

- Click the 'Remove import task' button. The 'Remove import task' deletes only the remaining part of not imported task.



On completion of the upload process, the result is displayed.

Dashboard / Domains / Domain dashboard - iyaspala.ml / Sender blacklist

Sender blacklist Help

Total lines processed 4 ✕

Imported 4 user(s) ✕

Import for domain iyaspala.ml has been finished ✕

[+ Add](#) [Delete](#) [Reset to default](#) [Export to CSV file](#) [Import from CSV file](#) [Refresh](#)

Filters

<input type="checkbox"/> Sender	Created Date
<input type="checkbox"/> cheat@greedy.com	2020-05-14 17:51:01
<input type="checkbox"/> hacker@hellboy.com	2020-05-14 17:34:52
<input type="checkbox"/> judas@trustmenot.com	2020-05-14 17:33:52
<input type="checkbox"/> sender1@domainname1.com	2020-05-14 18:11:27
<input type="checkbox"/> sender2@domainname2.org	2020-05-14 18:11:27
<input type="checkbox"/> sender3@domainname3.in	2020-05-14 18:11:27
<input type="checkbox"/> sender4@domainname4.us	2020-05-14 18:11:27

1 / 1 [1 - 7 / 7] Per page 15

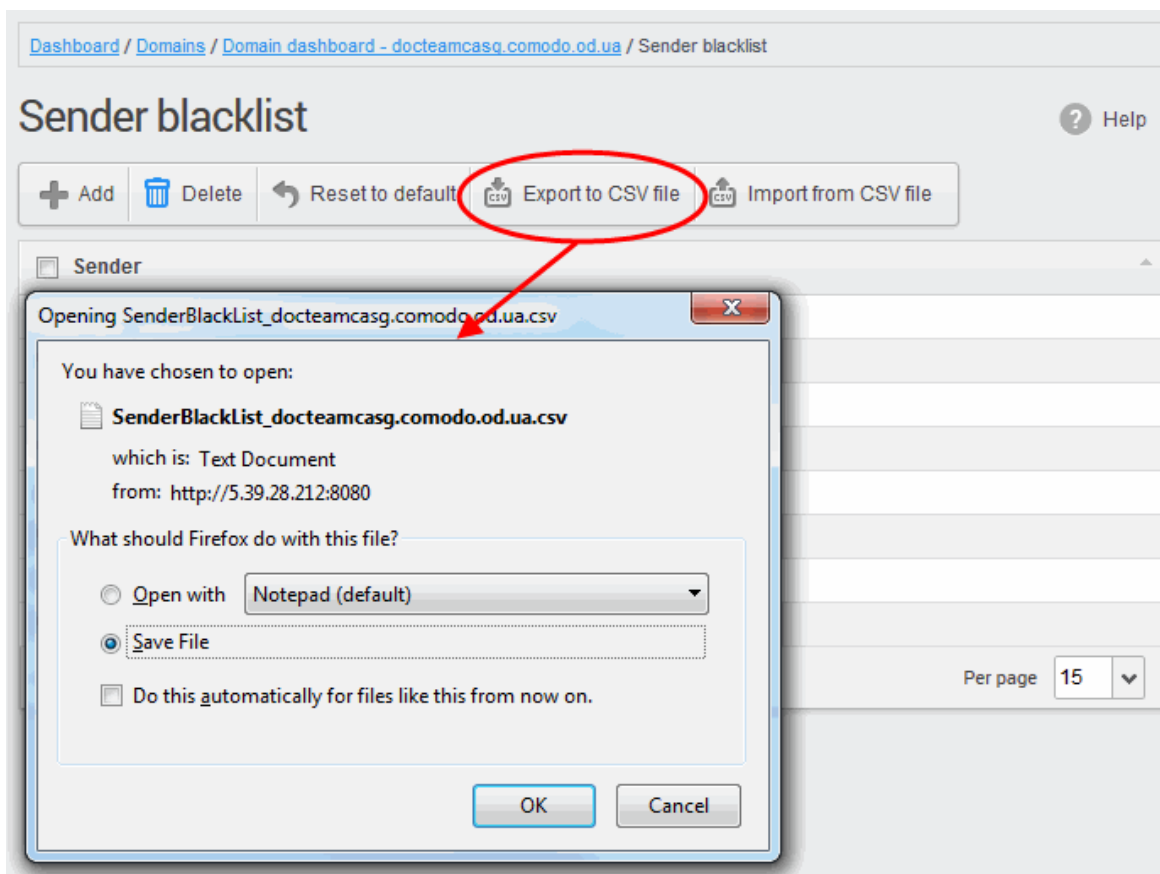
The sender blacklist from .csv file is uploaded and the administrator who carried out the task receives a notification about the import task completion.

Export the Sender Blacklist to CSV file

The administrator can save the configured sender blacklist by exporting it as a CSV file. If required in future, the administrator can import the users from the csv file, for example for a new account or after a reset.

Export the list

- Click the 'Export to CSV file' to save the list of blacklisted senders as a CSV file

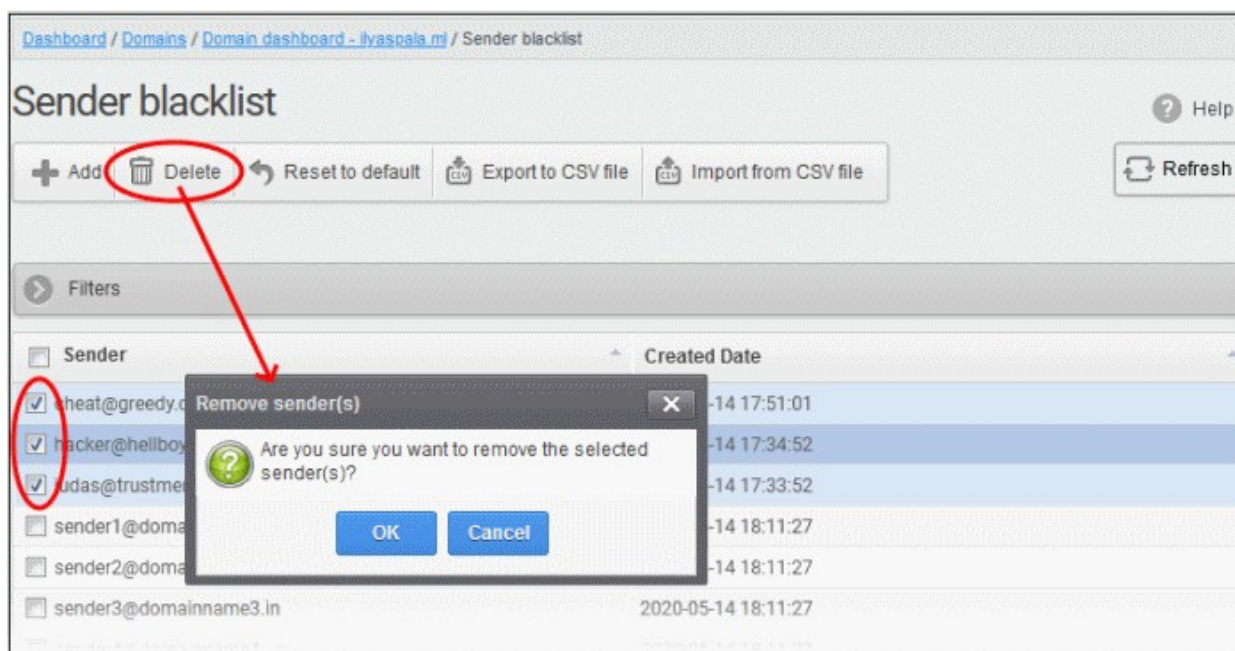


A file download dialog is displayed.

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

Delete Users from the Sender Blacklist

- Click 'Reset to default' to remove all blacklisted senders
- To remove sender(s), select them from the list and click the 'Delete' button.



- Click 'OK' to confirm your changes.

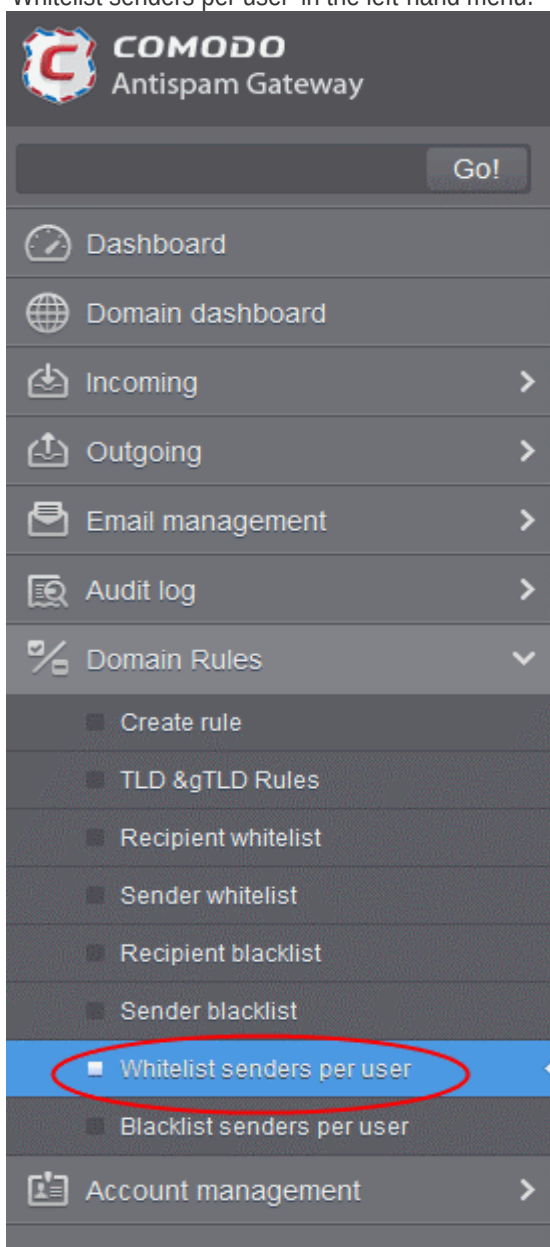
The sender(s) are removed from the blacklist. The emails from the senders are allowed as per the existing filter settings in CASG.

Whitelist Senders Per User

- Admins can permit certain senders for specific recipients - even if those senders are blacklisted elsewhere for other users.
- Senders can be manually whitelisted for a specific recipient, or can be imported from .csv. They can also be added after a user request.
- All filtering is disabled for whitelisted senders to specific recipients
- Comodo strongly recommends you only use this option after analyzing the request is genuine and warranted.

Configure sender whitelist per user

- Click 'Domain Rules' > 'Whitelist senders per user' in the left-hand menu.



The 'Whitelist senders per user' interface opens:

Dashboard / Domains / Domain dashboard - ilyaspala.mj / Whitelist senders per user

Whitelist senders per user

Help

+ Add Delete Import from CSV file Export to CSV file Refresh

Filters

Sender	Recipient	Created Date
mary@heaven.com	user2	2020-05-15 10:28:01
john@believe.me	user1	2020-05-15 10:27:38

1 / 1 Per page 15

- **Sender** – Whitelisted sender's email address
- **Recipient** – User name of the recipient
- **Created date** – Date and time the whitelist sender was added

From this interface administrators can:

- **Add senders to whitelist per user**
- **Export the list to CSV file for use in future**
- **Remove senders from Whitelist senders per user list**

Add Senders to Whitelist Per User

You can add senders to whitelist per user in the following ways:

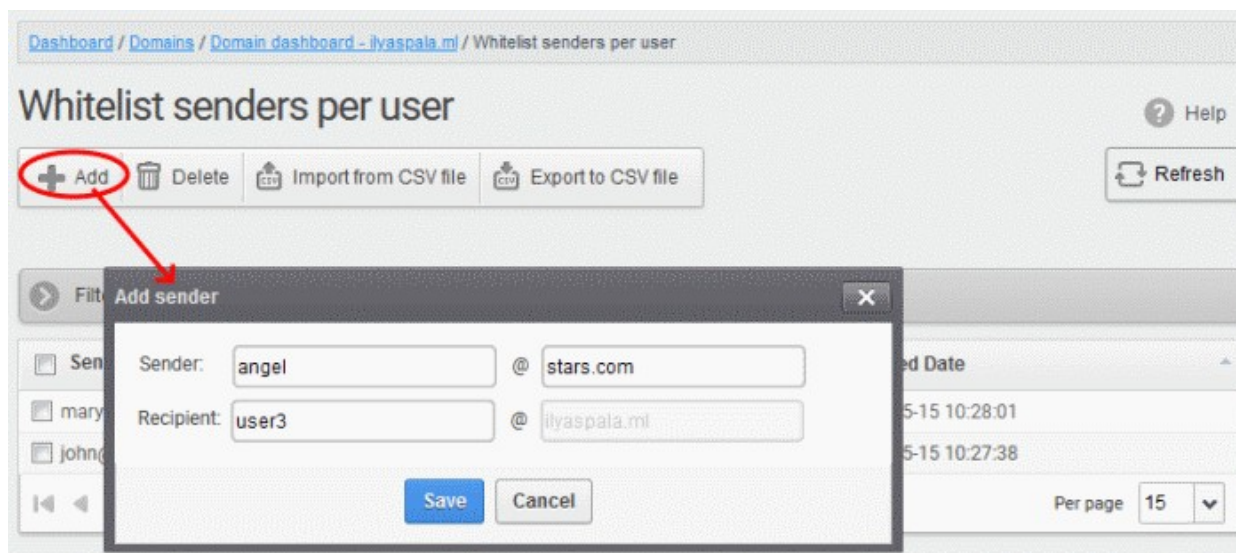
- **Manually add senders**
- **Import senders from a CSV file**
- **Add from 'Whitelist requests' from a user**

Manually add senders

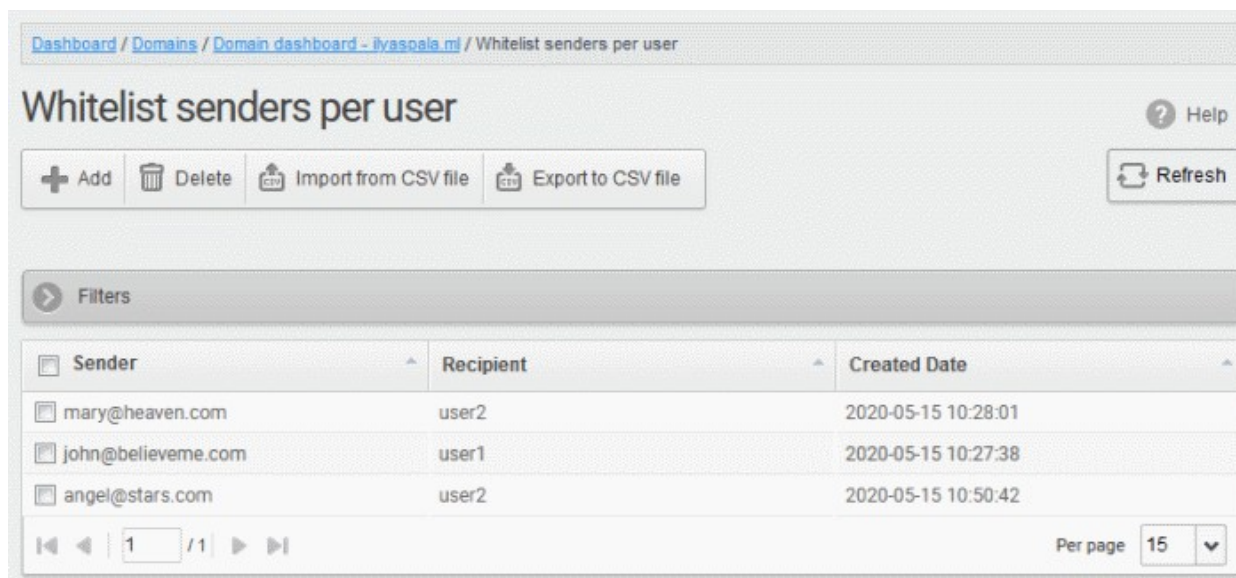
Administrators can manually specify the whitelisted sender and corresponding recipient as follows:

- Click the 'Add' button

The 'Add sender' dialog box opens:



- Sender - Enter the sender's username in the first text box and sender's email domain name after the @ symbol.
- Recipient - Enter the recipient's name in the first text box in the second row. **Note:** The recipient should be a valid user.
- Click 'Save' button. Repeat the process to add more whitelisted senders for the user.



Import senders from a CSV file

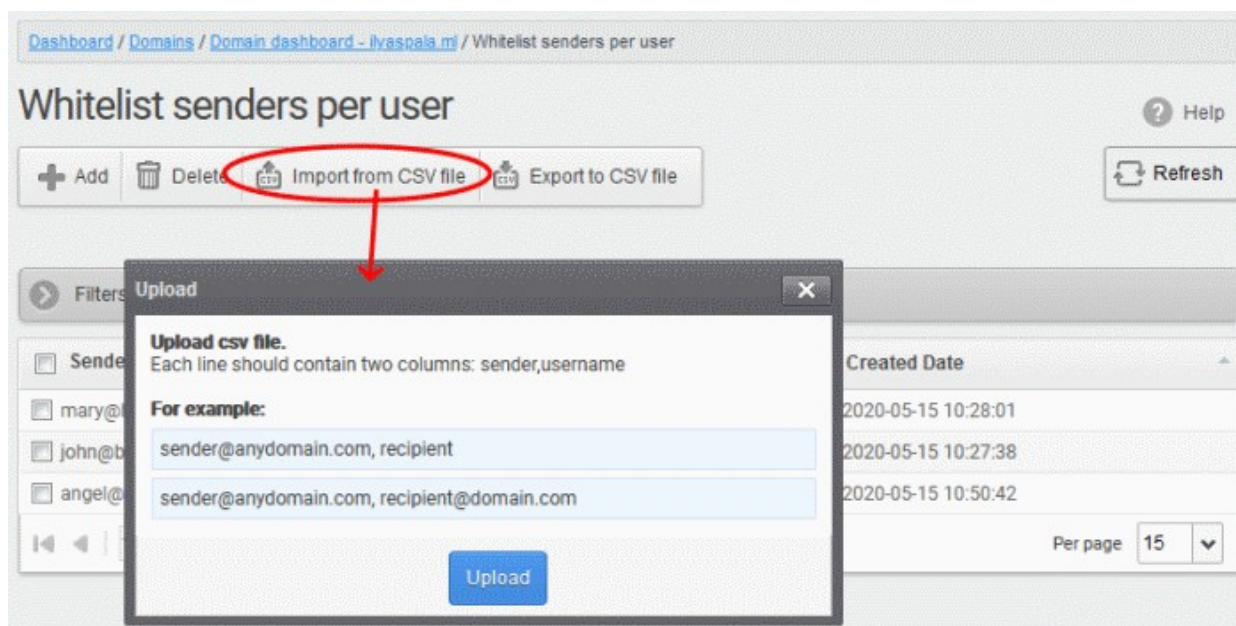
Administrators can import multiple senders at a time from a comma separated value (CSV) file to sender whitelist per user. The list of whitelisted senders and respective recipients are created using notepad or a spreadsheet application like MS Excel or OpenOffice Calc and saved in .csv format. Each line in the .csv file should contain the sender's email address and the username of the recipient or sender's email address and the recipient's email address, separated by a comma. An example is shown below:

```
sender1@anydomain.com, recipient1
sender2@anydomain.com, recipient2@domain.com
sender3@somedomain.com, recipient3
```

Import senders to whitelist from CSV file

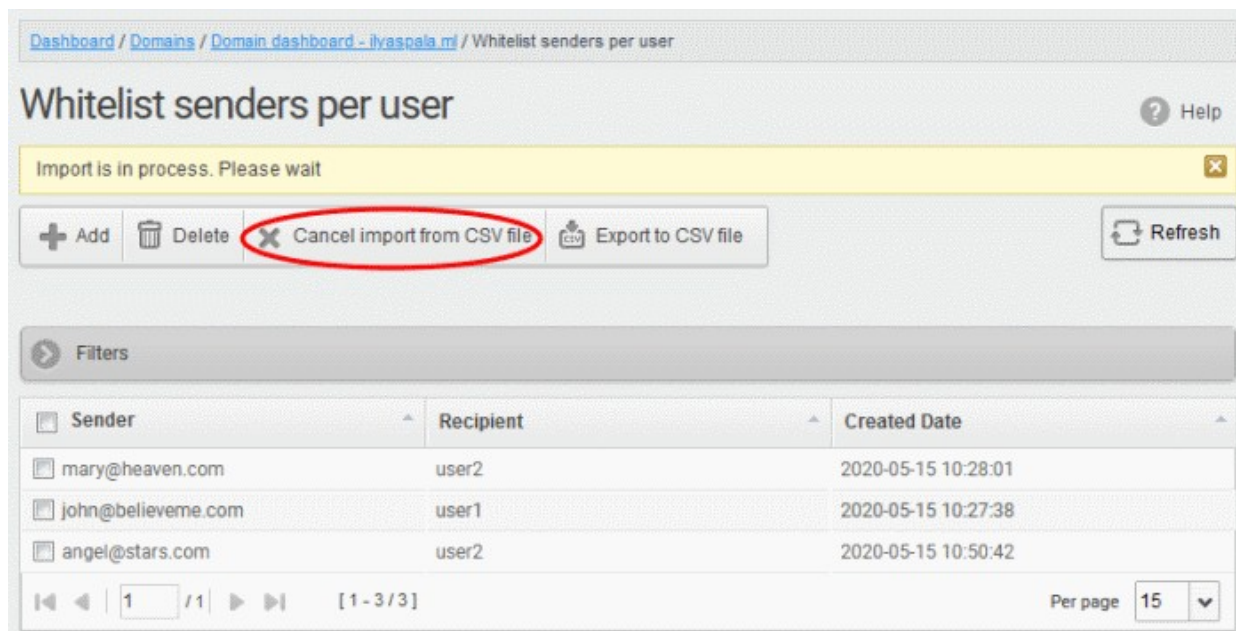
- Click the 'Import from CSV file' from the 'Whitelist senders per user' interface.

The 'Upload' dialog appears:



- Click 'Upload', navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.

The upload is placed in import tasks queue and the progress of the upload is displayed. If you want to remove the upload from the queue, click the 'Cancel import from the CSV file' button. The 'Cancel import from the CSV file' deletes only the remaining part of not imported task.



On completion of the upload process, the result is displayed.

Dashboard / Domains / Domain dashboard - ilyaspala.ml / Whitelist senders per user

Whitelist senders per user Help

Total lines processed 6 ✕

Imported 4 senders as whitelisted ✕

Import for domain ilyaspala.ml has been finished ✕

+ Add 🗑 Delete 📄 Import from CSV file 📄 Export to CSV file 🔄 Refresh

Filters

Sender	Recipient	Created Date
sender4@domainname4.us	user1	2020-05-15 12:29:47
sender3@domainname3.in	user2	2020-05-15 12:29:47
sender2@domainname2.org	user1	2020-05-15 12:29:46
sender1@domainname1.com	user2	2020-05-15 12:29:46

The sender whitelist per user from the CSV file is uploaded and the administrator who carried out the task receives a notification about the import task completion.

Add from Whitelist requests from users

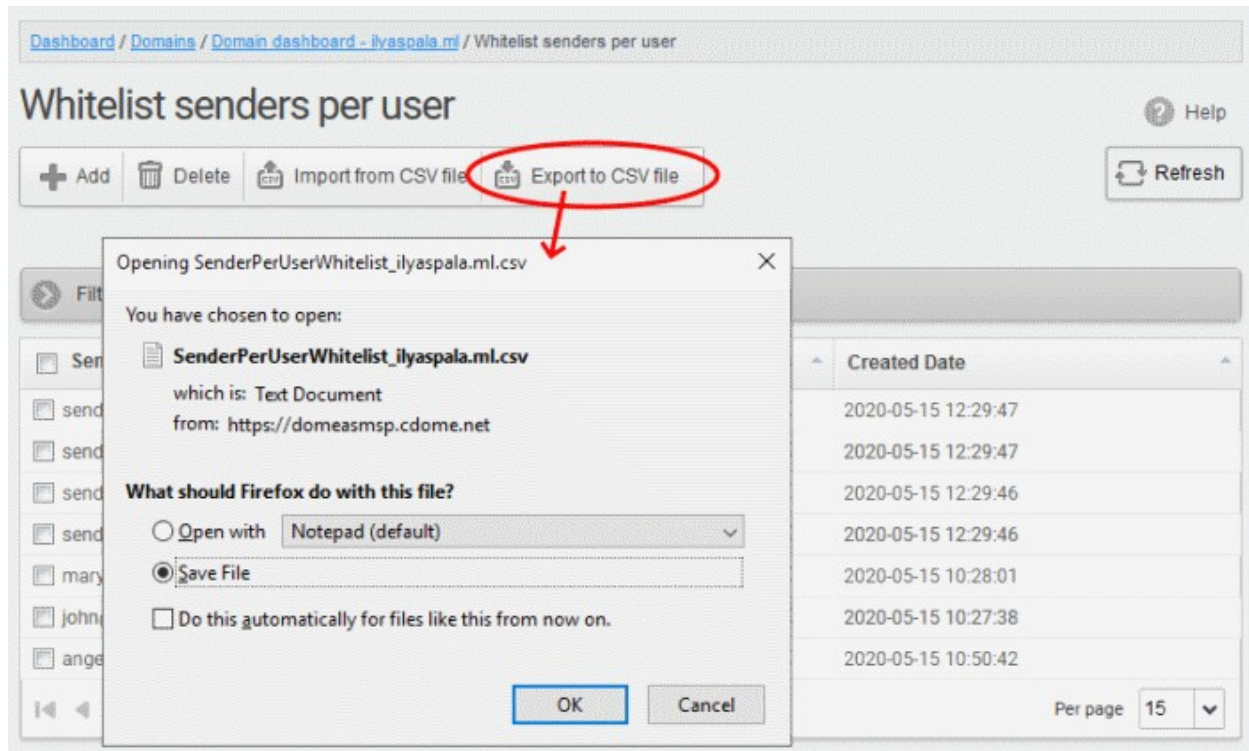
The administrator can add senders to whitelist based on the requests of the users. See [Email Management > Whitelisted Requests](#) for more details.

Export the Whitelist senders per user list to CSV file

The administrator can save the whitelist senders per user list by exporting it as a CSV file. If required in future, the administrator can import the users from the file, for example for a new account or after a reset.

Export the list

- Click the 'Export to CSV file' button to save the list

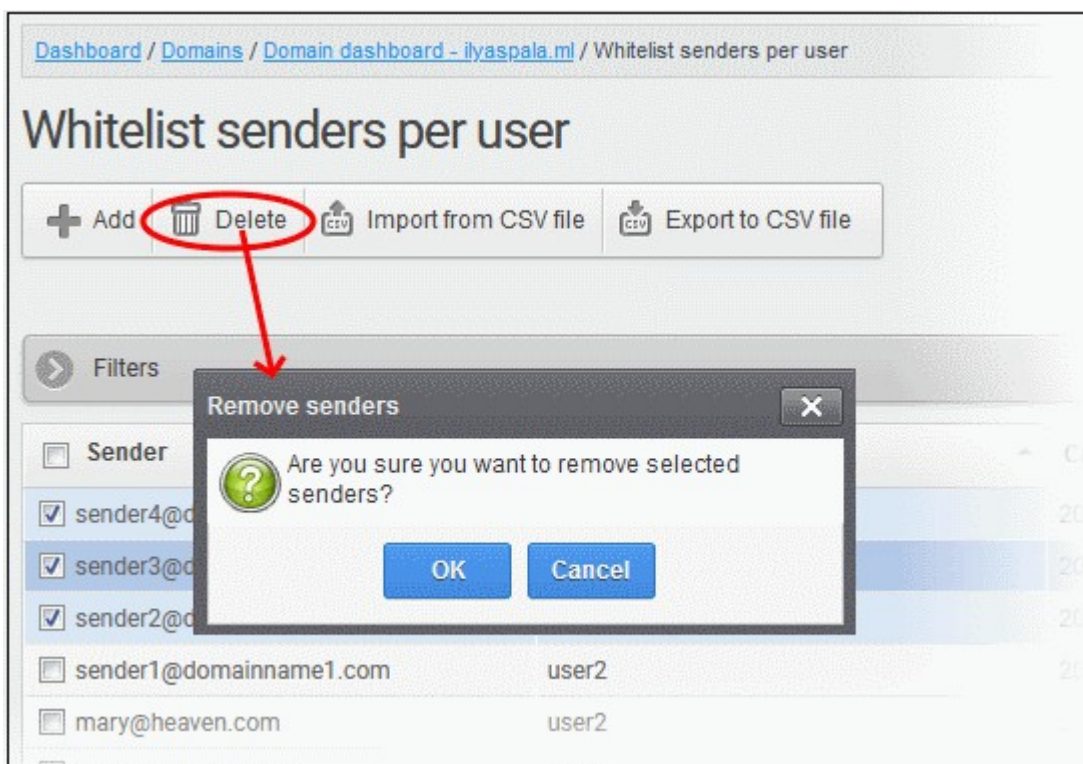


A file download dialog is displayed.

- Click 'OK' to save the file.

Delete Senders from Whitelist

- To delete sender(s) from the whitelist, select the sender(s) from the list and click the 'Delete' button.



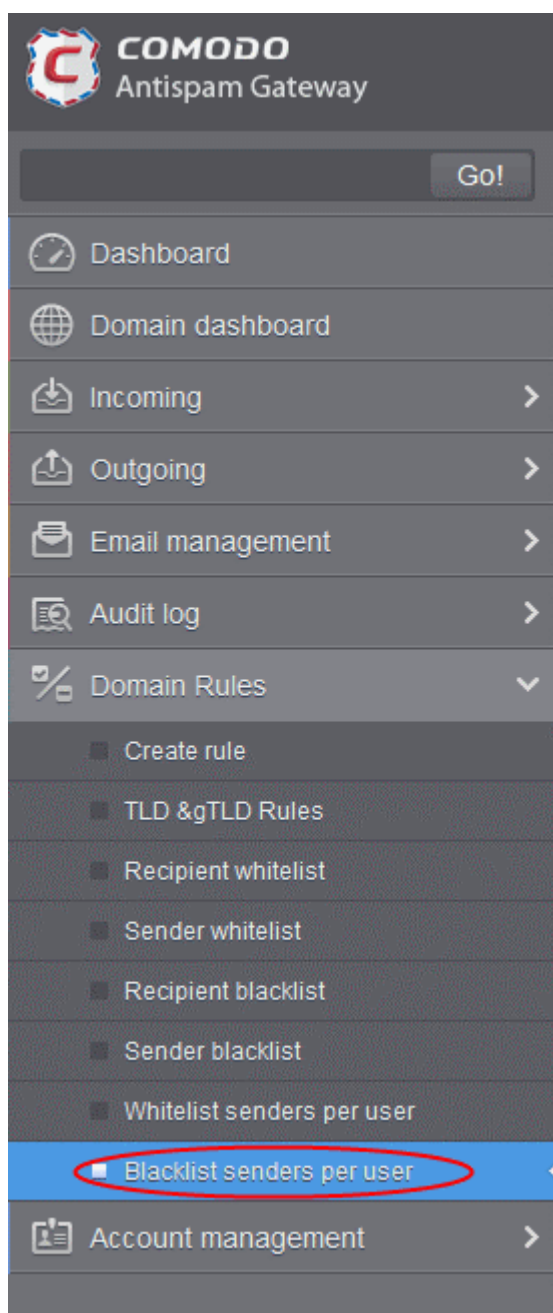
- Click 'OK' in the confirmation dialog.

Blacklist Senders Per User

- CASG allows admins to prevent certain senders from sending mail to specific users.
- This feature is useful in scenarios where you want to allow mails from a particular sender to all users in the domain but want to block the sender for a particular recipient in the domain.
- Senders can be added manually, imported from .csv and from a user request.

Configure sender blacklist per user

- Click 'Domain Rules' > 'Blacklist senders per user' in the left-hand menu:



The 'Blacklist senders per user' interface opens:

Dashboard / Domains / Domain dashboard - jvaspala.m / Blacklist senders per user

Blacklist senders per user

Help

+ Add Delete Import from CSV file Export to CSV file Refresh

Filters

Sender	Recipient	Created Date
judas@hell.com	user1	2020-05-15 13:10:48
joker@darknight.com	user2	2020-05-15 13:11:16

1 / 1 Per page 15

- **Sender** – Blacklisted sender's email address
- **Recipient** – User name of the recipient
- **Created date** – Date and time the blacklist sender was added

From this interface you can:

- **Add senders to blacklist per user**
- **Export the list to CSV file for use in future**
- **Remove senders from blacklist senders per user list**

Add Senders to Blacklist Per User

You can add senders to blacklist in three ways:

- **Manually add senders**
- **Import senders from a CSV file**
- **Add senders from 'Blacklist requests from users**

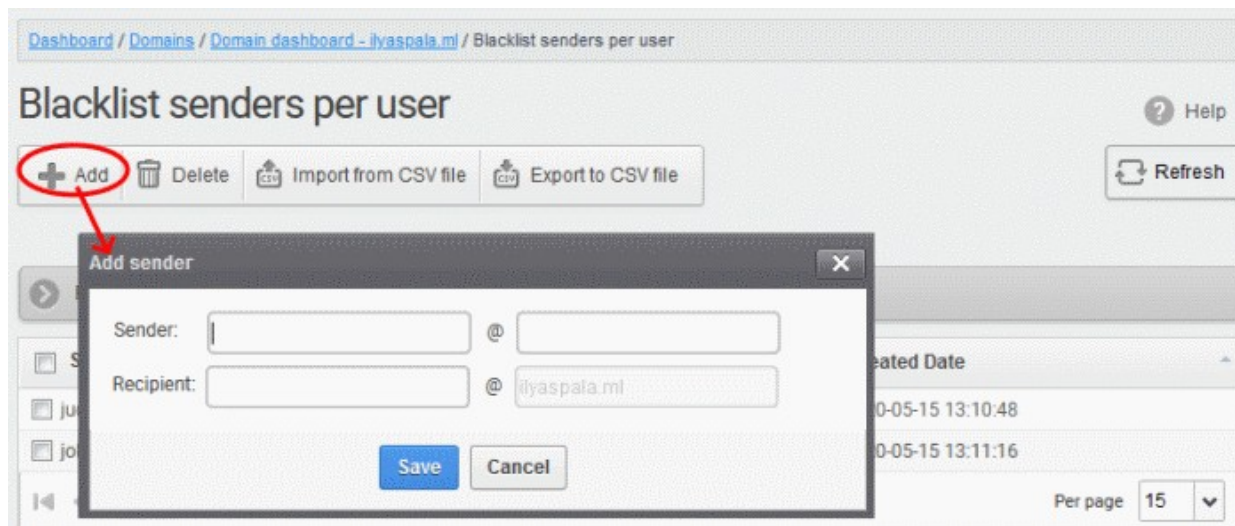
Manually add the senders

You can manually specify the senders to be blacklisted for specific recipients.

Manually add senders to blacklist per user basis

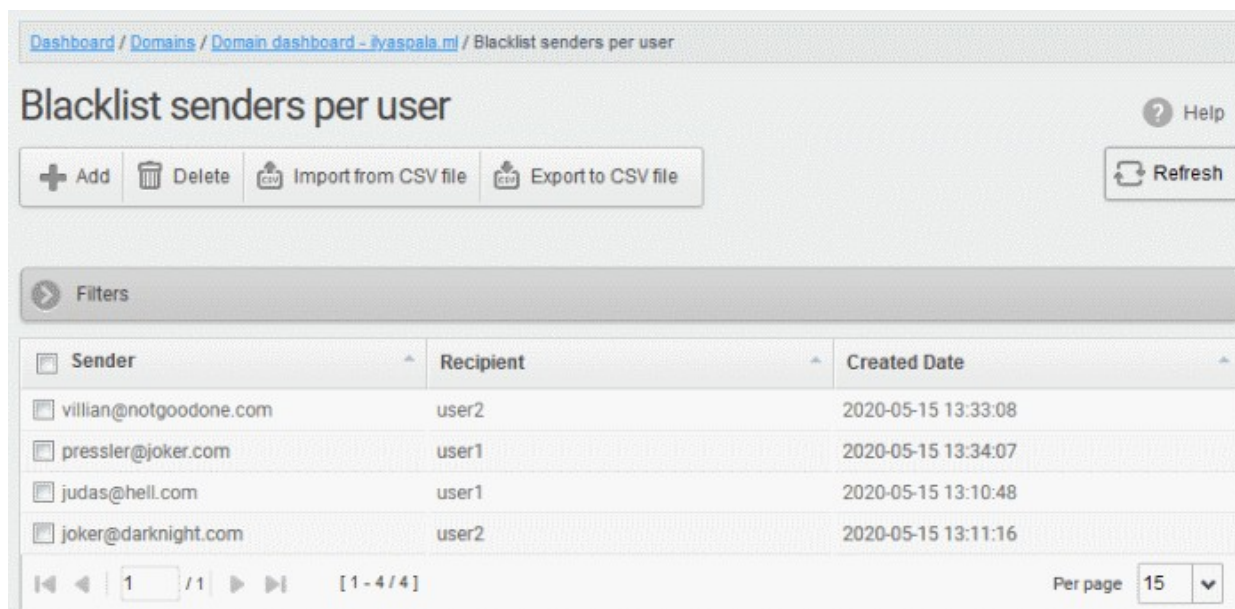
- Click the 'Add' button

The 'Add sender' dialog opens:



- Sender - Enter the sender's username in the first textbox and sender's email domain name after the @ symbol in the first row.
- Recipient - Enter the recipient's username in the first text box in the second row. **Note:** The recipient should be a valid user.
- Click 'Save' button. Repeat the process to add more blacklisted senders for the user.

The list is updated and displayed:



Import senders from a CSV file

Administrators can import multiple senders at a time from a comma separated values (CSV) file to sender blacklist per user. The list of blacklisted senders and respective recipients can be created using notepad or a spreadsheet application like MS Excel or OpenOffice Calc and saved in .csv format. Each line in the .csv file should contain the sender's email address and the username of the recipient or sender's email address and the recipient's email address, separated by a comma. An example is shown below:

sender1@anydomain.com, recipient1

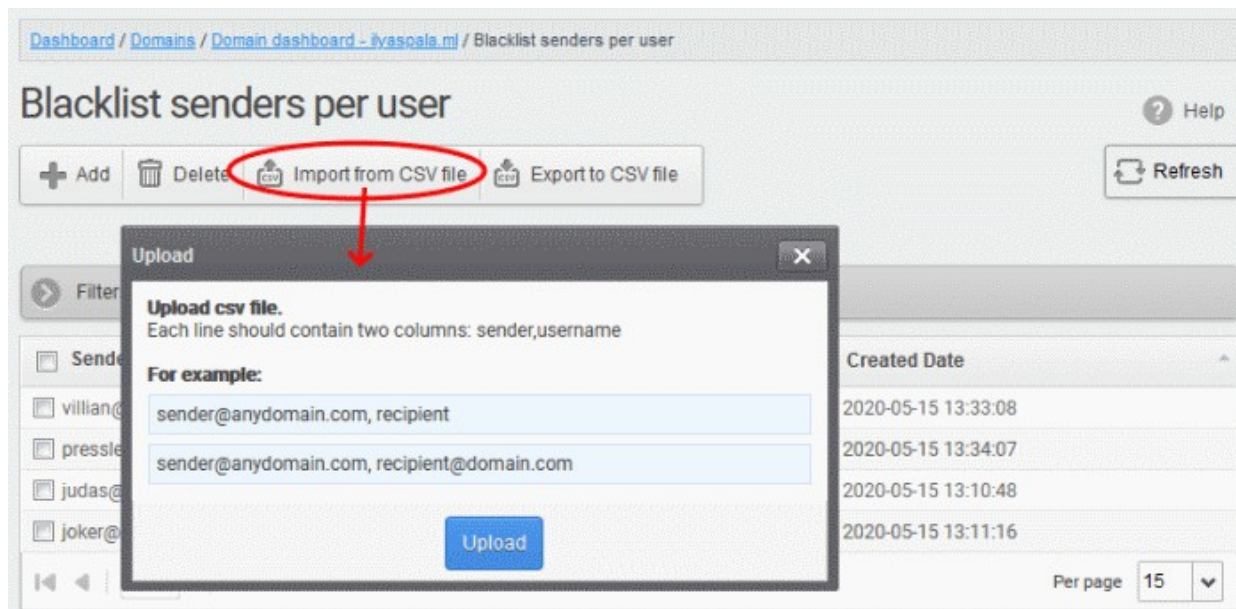
sender2@anydomain.com, recipient2@domain.com

sender3@somedomain.com, recipient3

Import senders to Blacklist from CSV file

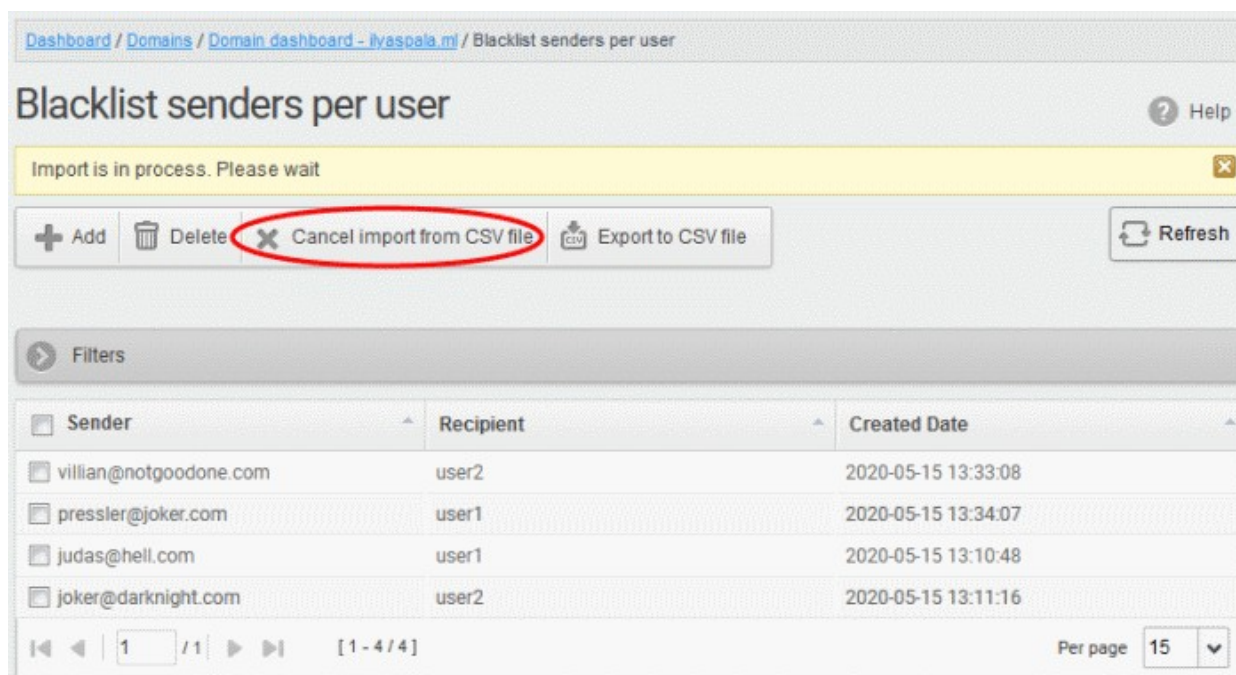
- Click the 'Import from CSV file' button from the 'Blacklist senders per user' interface.

The 'Upload' dialog appears:

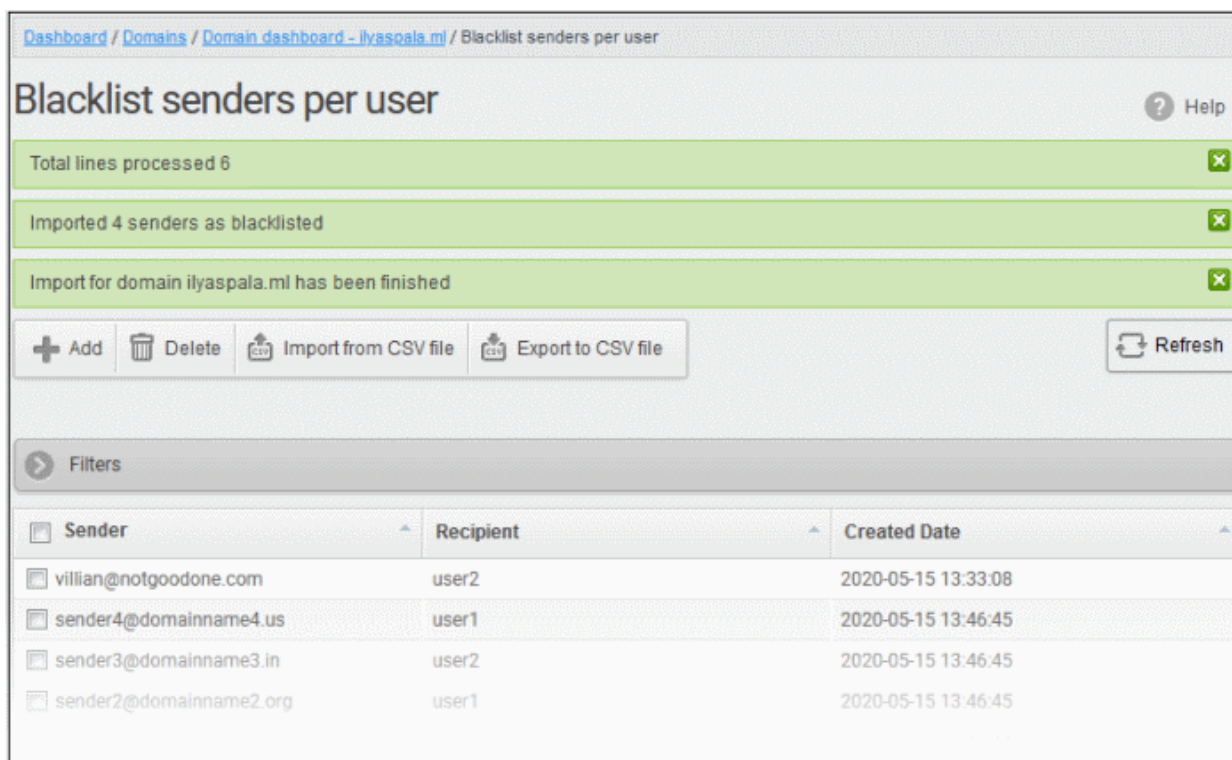


- Click 'Upload', navigate to the location where the CSV file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.

The upload is placed in import tasks queue and the progress of the upload is displayed. If you want to remove the upload from the queue, click the 'Cancel import from CSV file' button. The 'Cancel import from CSV file' deletes only the remaining part of not imported task.



On completion of the upload process, the result is displayed.



Dashboard / Domains / Domain dashboard - ilyaspala.ml / Blacklist senders per user

Blacklist senders per user Help

Total lines processed 6

Imported 4 senders as blacklisted

Import for domain ilyaspala.ml has been finished

+ Add Delete Import from CSV file Export to CSV file Refresh

Filters

Sender	Recipient	Created Date
villian@notgoodone.com	user2	2020-05-15 13:33:08
sender4@domainname4.us	user1	2020-05-15 13:46:45
sender3@domainname3.in	user2	2020-05-15 13:46:45
sender2@domainname2.org	user1	2020-05-15 13:46:45

The sender blacklist per user from the CSV file is uploaded and the administrator who carried out the task receives a notification about the import task completion.

Add senders from Blacklist requests from users

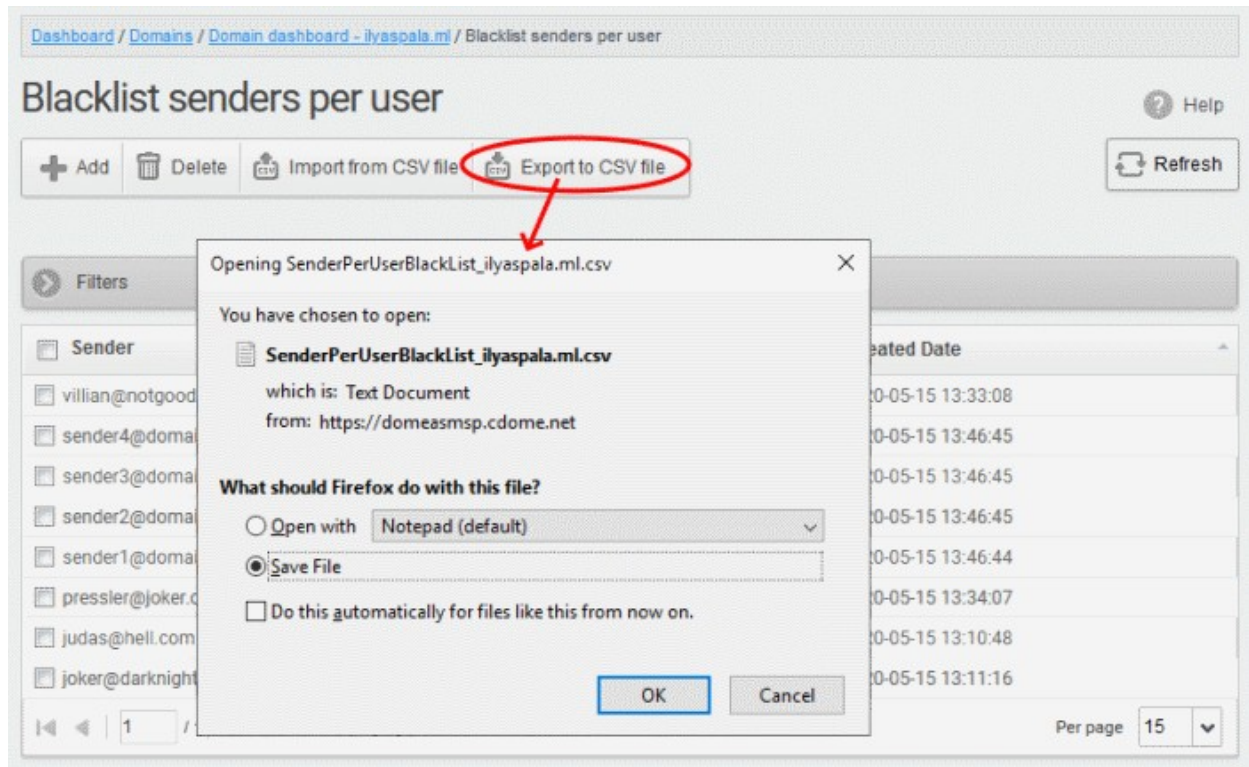
Administrators can add senders to blacklist based on the requests of the users. See [Email Management > Blacklisted Requests](#) for more details.

Export the blacklist senders per user list to a CSV file

Administrators can save the blacklist senders per user list by exporting it as a CSV file. If required in future, the administrator can import the users from the csv file, for example for a new account or after a reset.

Export the list

- Click the 'Export to CSV file' button

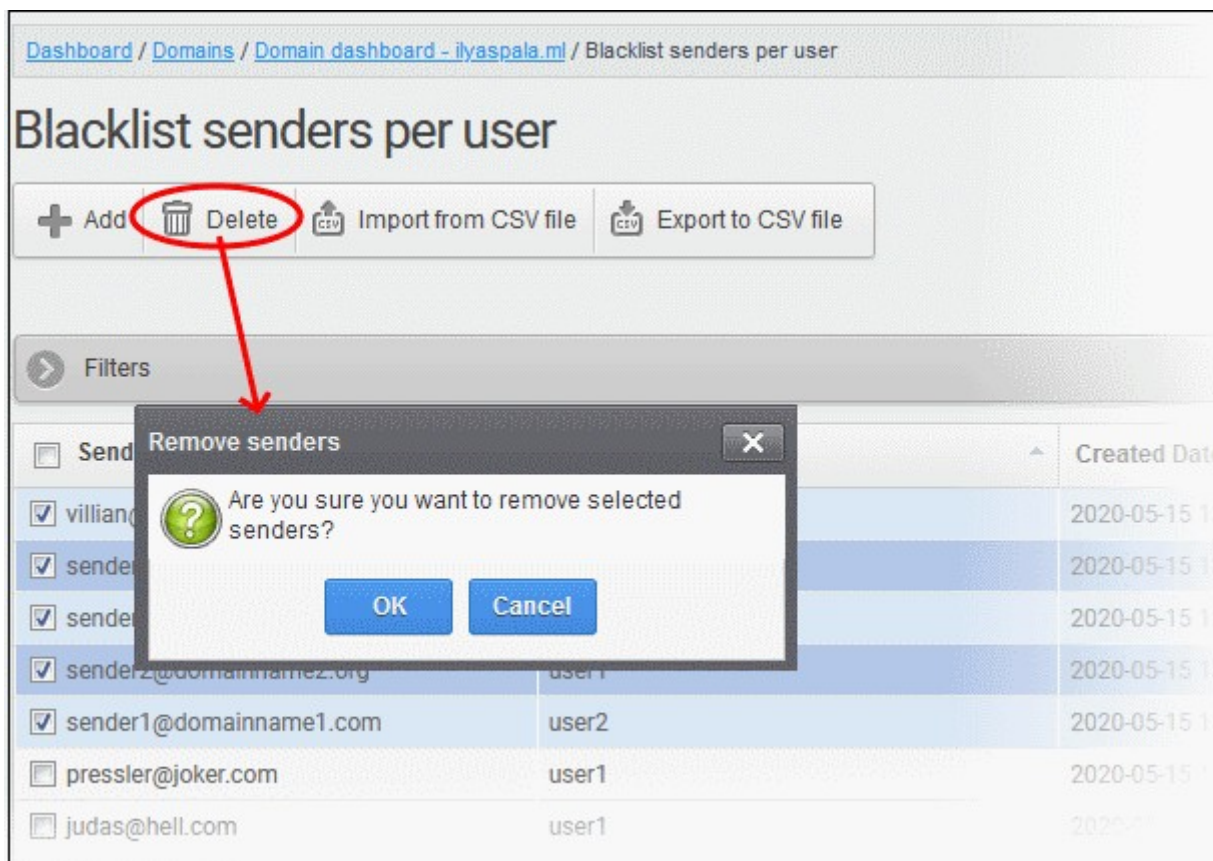


A file download dialog is displayed.

- Click 'OK' to save the file.

Delete Senders from Blacklist

- To delete sender(s) from the blacklist, select them from the list and click the 'Delete' button.



- Click 'OK' in the confirmation dialog.

6.5.7 Account Management

The 'Account Management' interface allows you to manage users for a selected domain. Admins can reset passwords for users, allow or deny access to user accounts, import users from .csv file and import users from Active Directory (AD) servers.

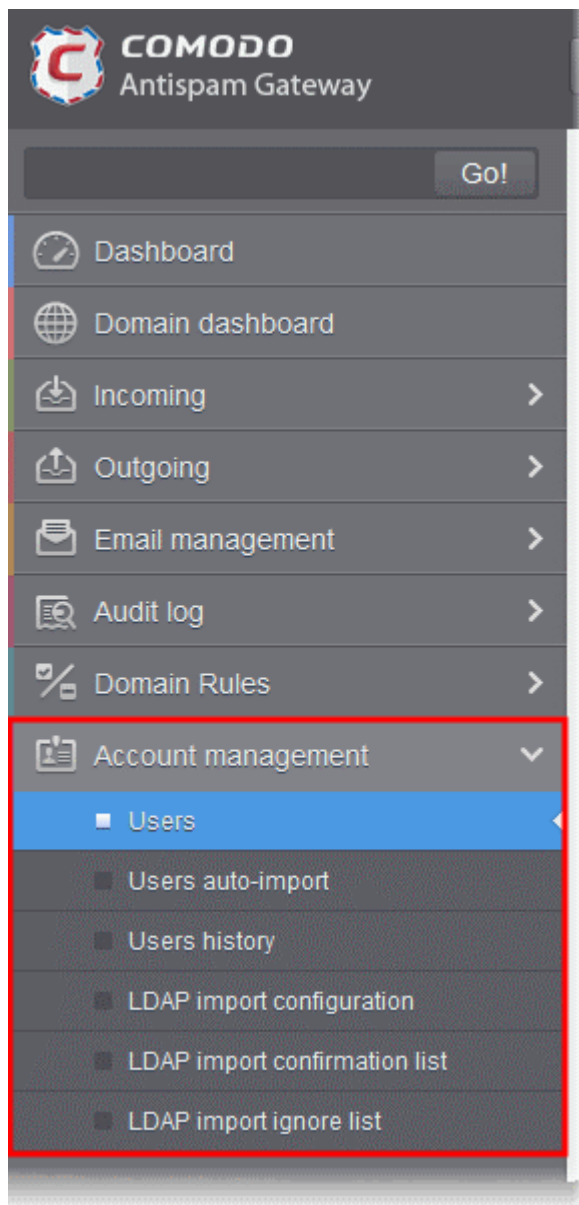
Administrators can also view users' login history. See [User History](#) for more details.

Click the following links for more details:

- [Users](#)
- [User auto-import](#)
- [Users history](#)
- [Importing Users from LDAP](#)

6.5.7.1 User Account Management

The 'Users' area lets you manage users for a selected domain. You can add/import users, delete users, edit user accounts, reset passwords and configure user permissions. You can also configure mail aliases in this interface.



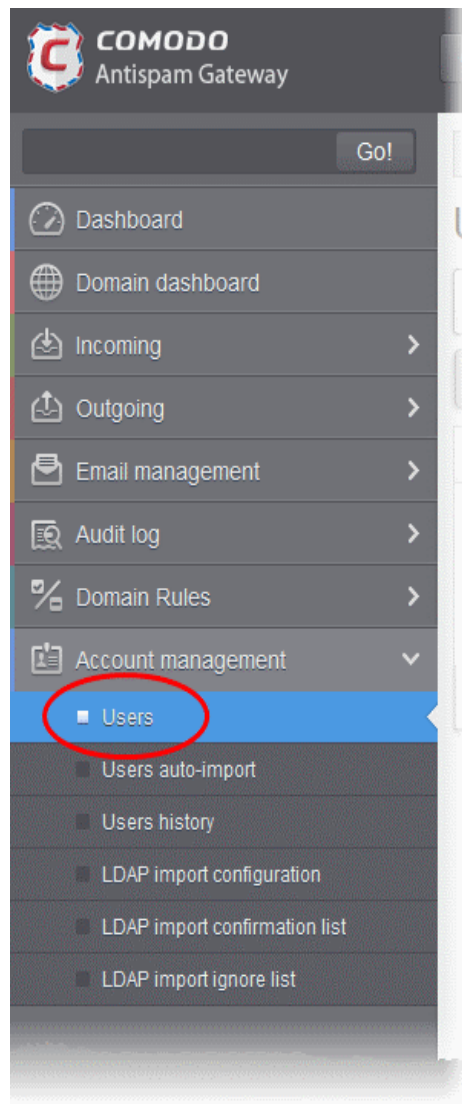
Click the following links for more details:

- [Manage Users](#)
- [Add New Users](#)
- [Delete Users](#)
- [Edit Users](#)
- [Unlock Users](#)
- [Import Users from CSV file](#)
- [Export Users to CSV file](#)
- [Manage Permissions](#)
- [Aliases](#)
- [Moving to Aliases](#)
- [Import Aliases from CSV file](#)

- **Forward mails to another user**
- **Other actions**

Manage Users

- Click 'Account management' on the left then click 'Users':



This opens the 'Users' interface of the selected domain:

- Click any column header to sort items in ascending/descending order of the entries in that column. Sorting is not available for the 'Aliases' and 'Group' columns.

Use filters to search for users


- Click anywhere on the 'Filters' stripe to open the filters area.

- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

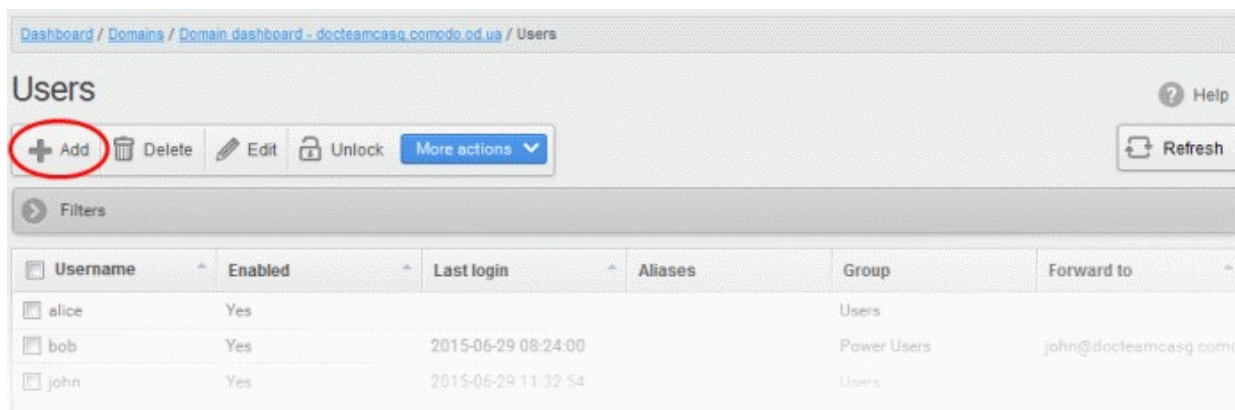
- **Username:** Type a user name in the text box (column 3) and select a condition in column 2.
- **Enabled:** Sort users by whether or not their account has been activated.
- **Last Login:** Sort users according to a specific login time. Choose the date ranges from the boxes provided.
- **Alias username:** Search users by their email alias.
- **Alias Domain:** Search users by their domain alias.
- **Forward to:** Search users by the address to which their mail is forwarded

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

You can add multiple filters to the same search by clicking .

Add a new user

- Click the 'Add' button.



This opens the new user configuration screen:

- **Username** – Type the name of the new user. This forms the first part of their email address. For example, if you type 'alice', the email address of the user will be 'alice@domainname.com'.
- **Enabled** – Clear this box to deny the new user access to CASG. The email address will still work, they just can't login to the CASG interface to, for example, check their quarantined mail. You can enable the user later if required.

You can choose to add the new user to **Recipient Whitelist** from this interface itself.

- Select the checkbox beside the 'Whitelist email' to add the user to **Recipient Whitelist**.

Admins can also determine whether users get the reports or not. By default, it is enabled.

- Deselect the 'Send quarantine reports' box to disable this option.
- Select the 'Send invitation' box to send an invitation mail to the email recipient address entered in the 'Username' text box.

The non-human and public email settings are simply markers which help Comodo to improve antispam rules and the service in general. They let us see the volume and type of spam that these types of addresses attract. These settings do not affect any technical operations, or the protection that is applied to the addresses.

Please help Comodo by telling us if the address is one, or both, of the following:

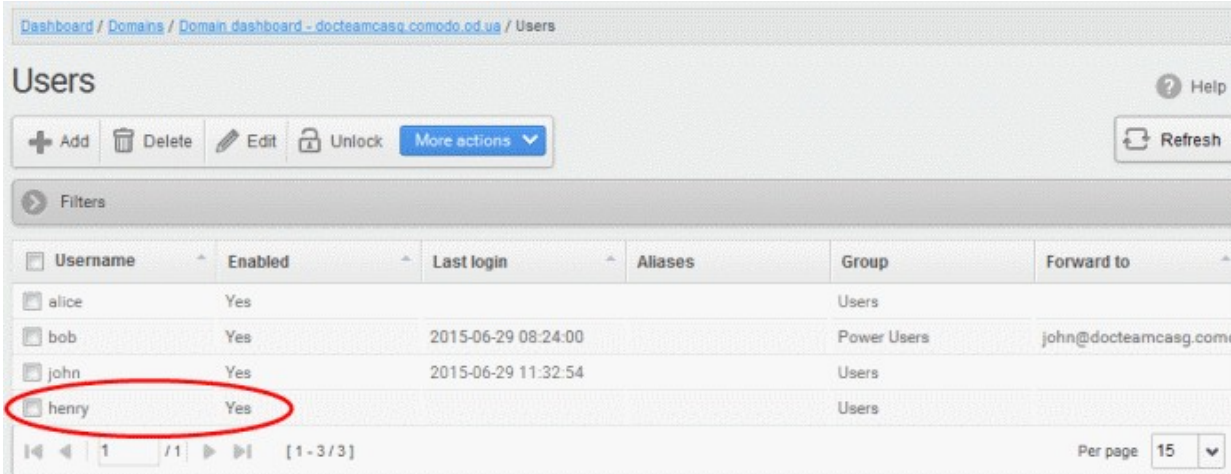
- **Non-human** – A mailing list, or other non-personal email address. For example, info@yourdomain.com or sales@yourdomain.com.
- **Public email** – A contact address that you make freely available for people to contact you. You might put this address on your website, twitter feed or Facebook page.

You can choose whether containment feature should be enabled / disabled for the user. This setting overrides the **containment settings** configured for the domain.

- Enable Containment – The options available are:
 - Enable
 - Disable
 - Use domain settings (Enable) – Applies the domain settings for containment to the user. Default value is 'Enabled' for a domain.
- Click the 'Save' button.

Note: If the user is disabled and subscribed for periodical Quarantine Reports, the subscription will also be canceled.

An email to the added user will be sent automatically containing password to access CASG. The password can be reset in the **edit interface**. The added user will be displayed in the list.



Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Users

Users

Help

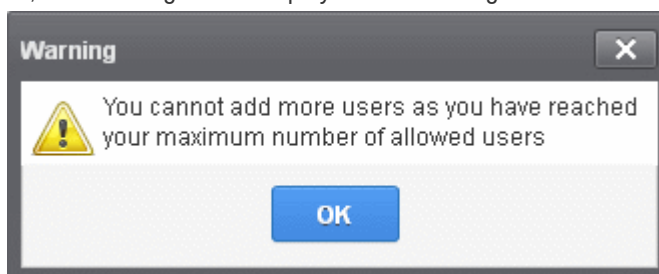
+ Add Delete Edit Unlock More actions Refresh

Filters

Username	Enabled	Last login	Aliases	Group	Forward to
alice	Yes			Users	
bob	Yes	2015-06-29 08:24:00		Power Users	john@docteamcasg.comodo
john	Yes	2015-06-29 11:32:54		Users	
henry	Yes			Users	

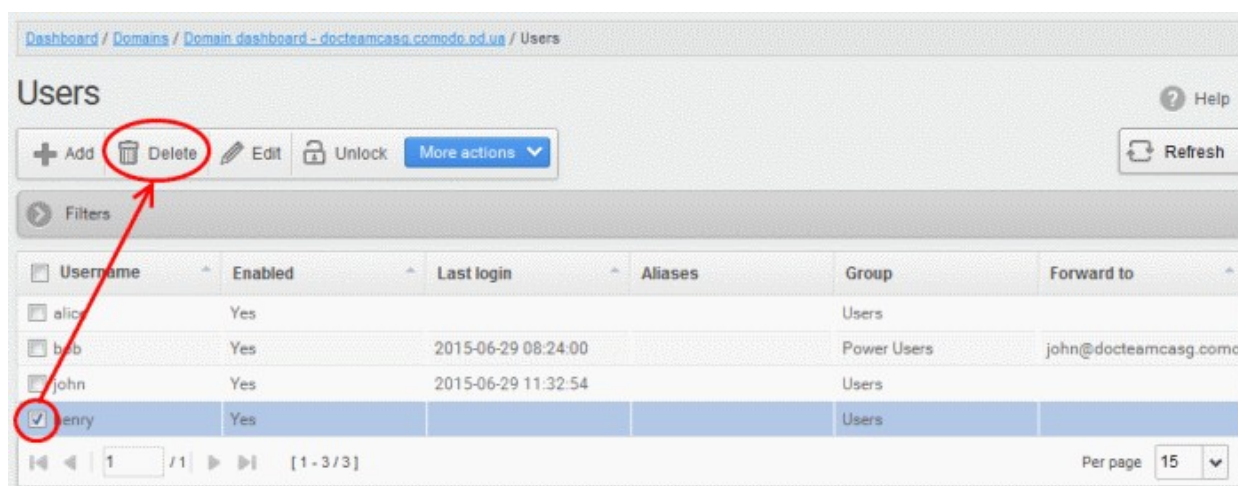
1 / 1 [1 - 3 / 3] Per page 15

Note: The number of users that can be added depends on the plan subscribed by you and the maximum number of users limit configured for the domain in the **Add Domains / Edit Domains / Domain Settings** interfaces. When you exceed the limit of users, the following will be displayed while adding a new user.

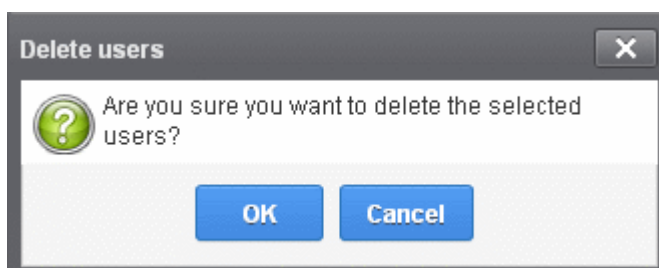


To delete an existing user

- Select the user you want to delete from the list and click the 'Delete' button



- Click 'OK' to confirm your changes.

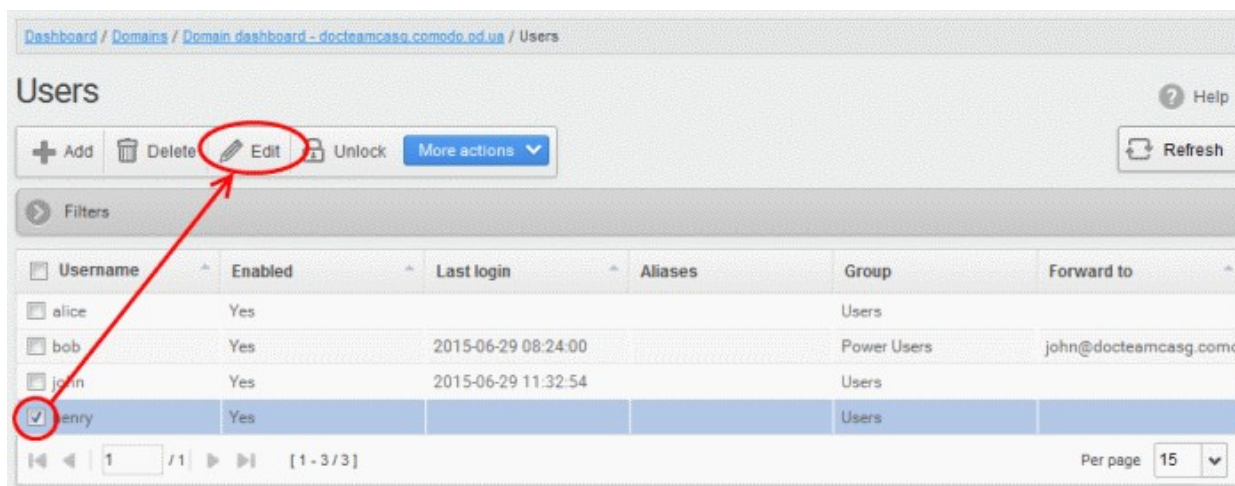


The user(s) will be removed from the list.

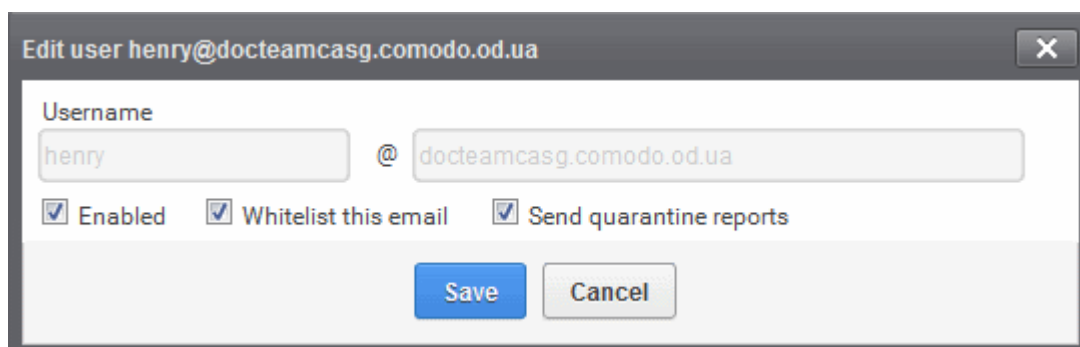
To edit an existing user

You can select to allow or deny permission for the users to access their CASG account in the edit interface as well as enable or disable quarantine report generation for the user.

- Select the user you want to edit from the list and click the 'Edit' button.



The 'Edit user' dialog box will appear.



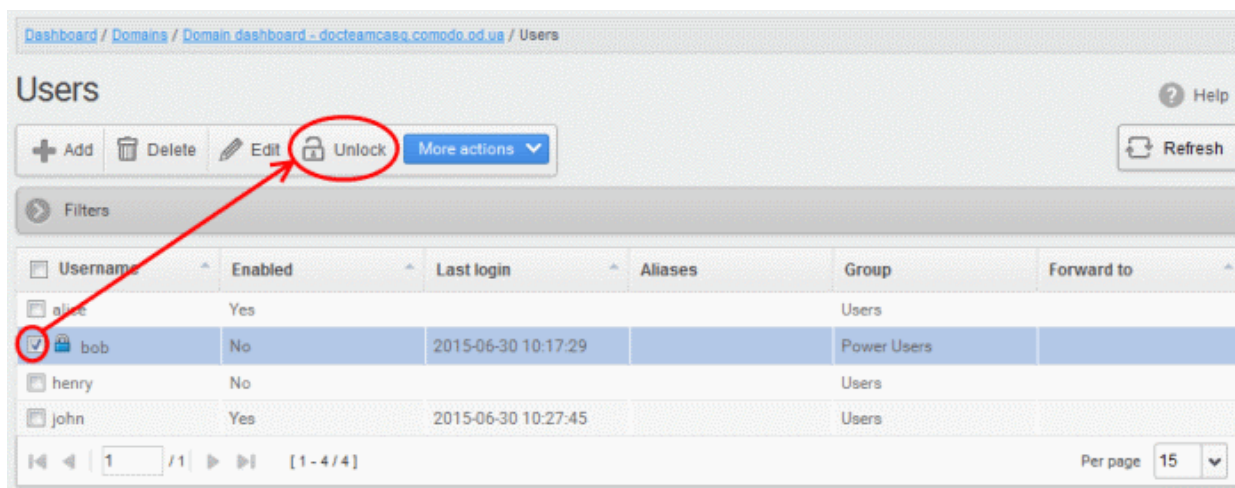
- **Enabled** - Allows the user to access the CASG interface.
- **Whitelist email** - Adds the user to the **Recipient Whitelist**.
- Disable '**Send quarantine reports**' checkbox, if you do not want the user to get quarantine reports. By default it is enabled.
- Click the 'Save' button to confirm your changes.

Note: Any active subscriptions or scheduled reports for the user will be automatically canceled if access to CASG is disabled.

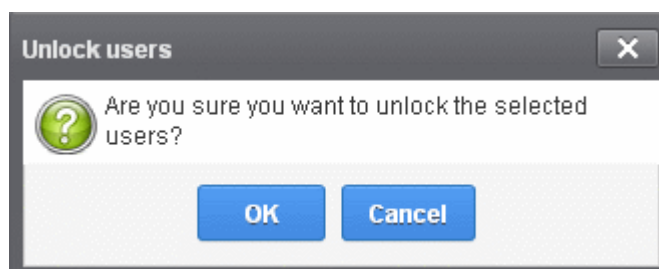
Unlock users

After 3 unsuccessful login attempts, CASG will lock a user out of their account for 30 minutes. If required, you can unlock these users immediately without waiting for the timeout to end.

Locked out users have a lock icon next to their names:



- Select the locked user from the list and click the 'Unlock' button.
- Click 'OK' in the confirmation dialog:



The user is now free to try to login again.

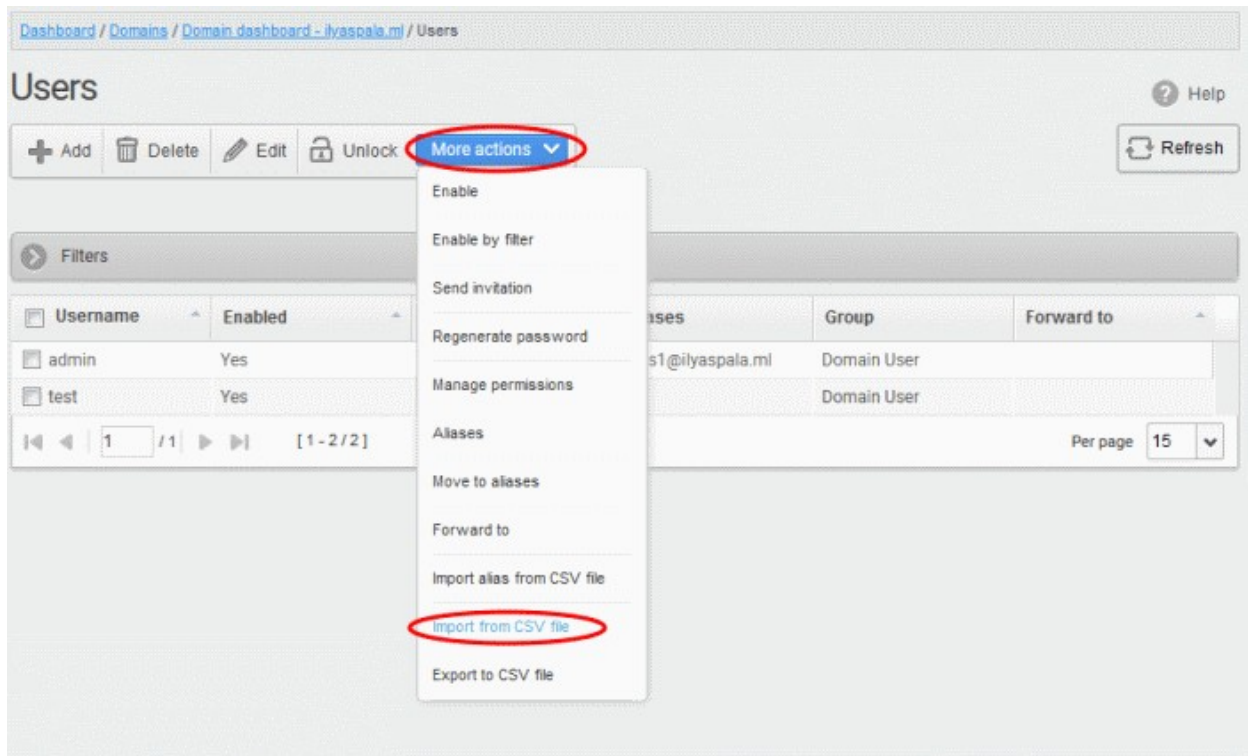
Import users from CSV file

You can add many new users at a time by importing from a file. The users should be saved in 'comma separated value' (CSV) as shown below:

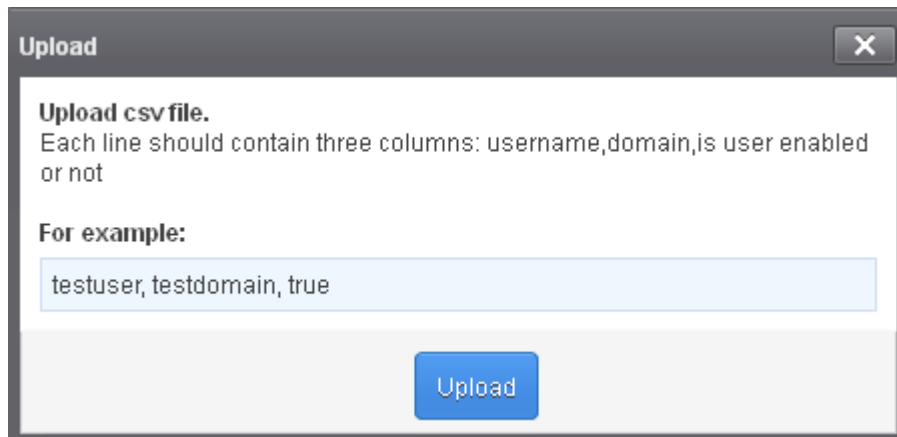
```
username1,domainname,true
```

```
username2,domainname,false
```

- To import new users from a CSV file click 'More actions' > 'Import from CSV file'

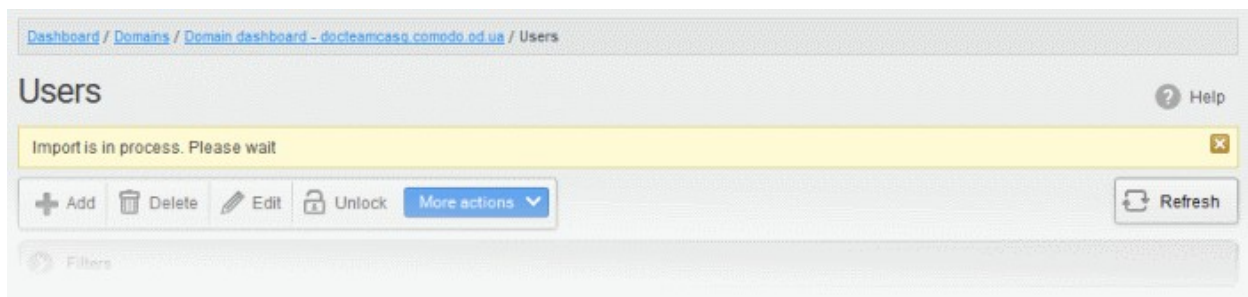


The 'Upload' dialog will be displayed.



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

The upload progress will be displayed...



...and when completed, the results will be displayed.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.ed.ua / Users

Users

Imported 1 user(s)

1 users already exist

+ Add Delete Edit Unlock More actions Refresh

Filters

Username	Enabled	Last login	Aliases	Group	Forward to
alice	Yes			Users	
bob	Yes	2015-06-30 10:17:29		Power Users	
henry	No			Users	
john	Yes	2015-06-30 10:27:45		Users	
jsmith	No			Users	

Per page 15

The administrator who carried out the task will receive a notification about the import task completion.

Note: The number of users that can be added depends on the plan subscribed by you and the maximum number of users limit configured for the domain in the **Add Domains / Edit Domains / Domain Settings** interface. CASG will stop importing users after the number of users allowed for the account is reached and a warning will be displayed.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.ed.ua / Users

Users

Imported 1 user(s)

You cannot add more users as you have reached your maximum number of allowed users by license limitation, 1 users were imported

+ Add Delete Edit Unlock More actions Refresh

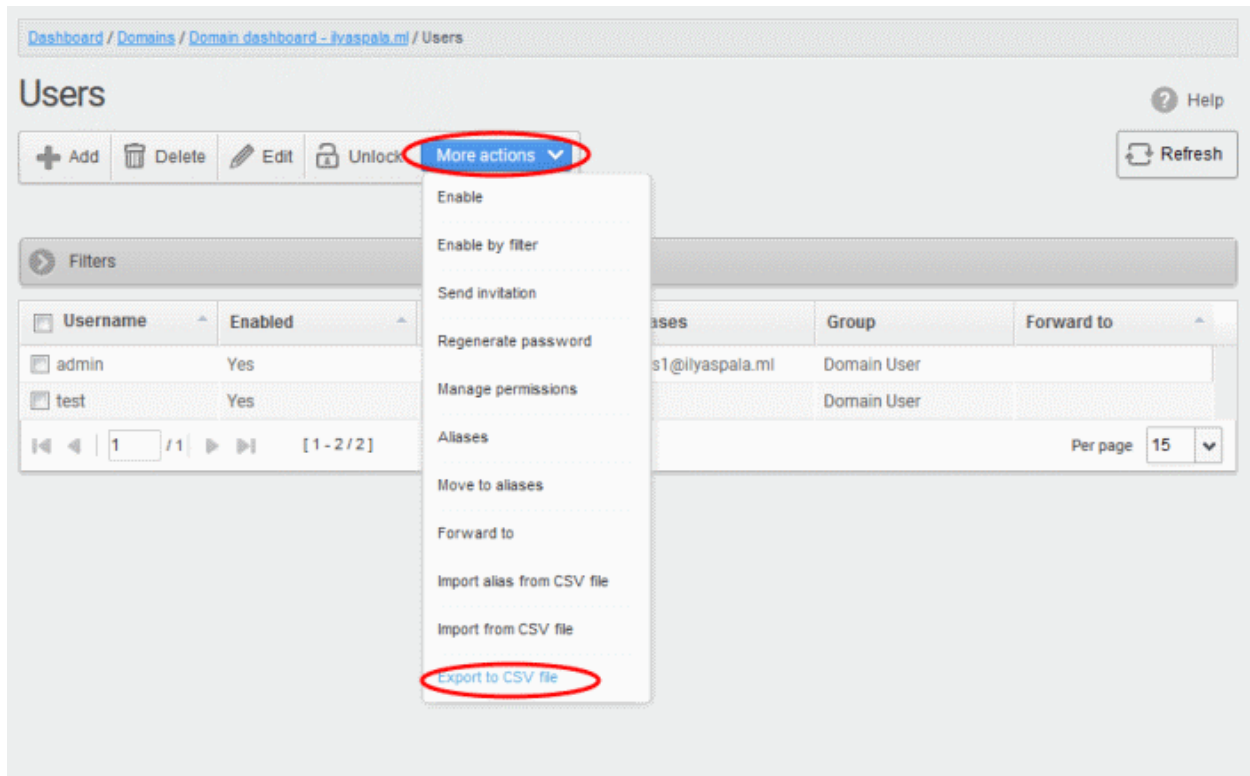
Filters

Username	Enabled	Last login	Aliases	Group	Forward to
alice	Yes			Users	

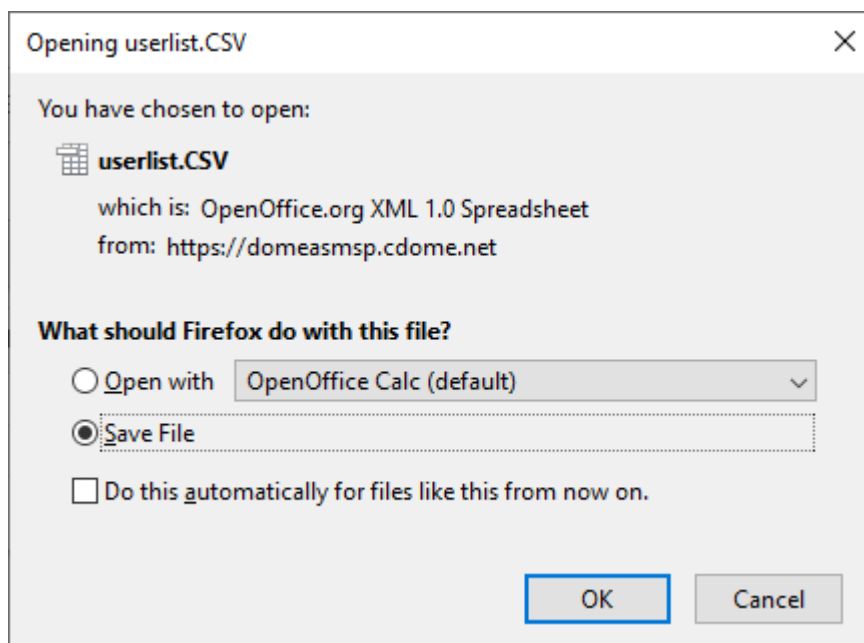
Export Users to CSV file

You can save the user list as a CSV file.

- Click 'More actions' > 'Export to CSV file'



The file download dialog is displayed.



- Click 'Open' to view the file with an appropriate application
- Click 'OK' to save the file to your computer.

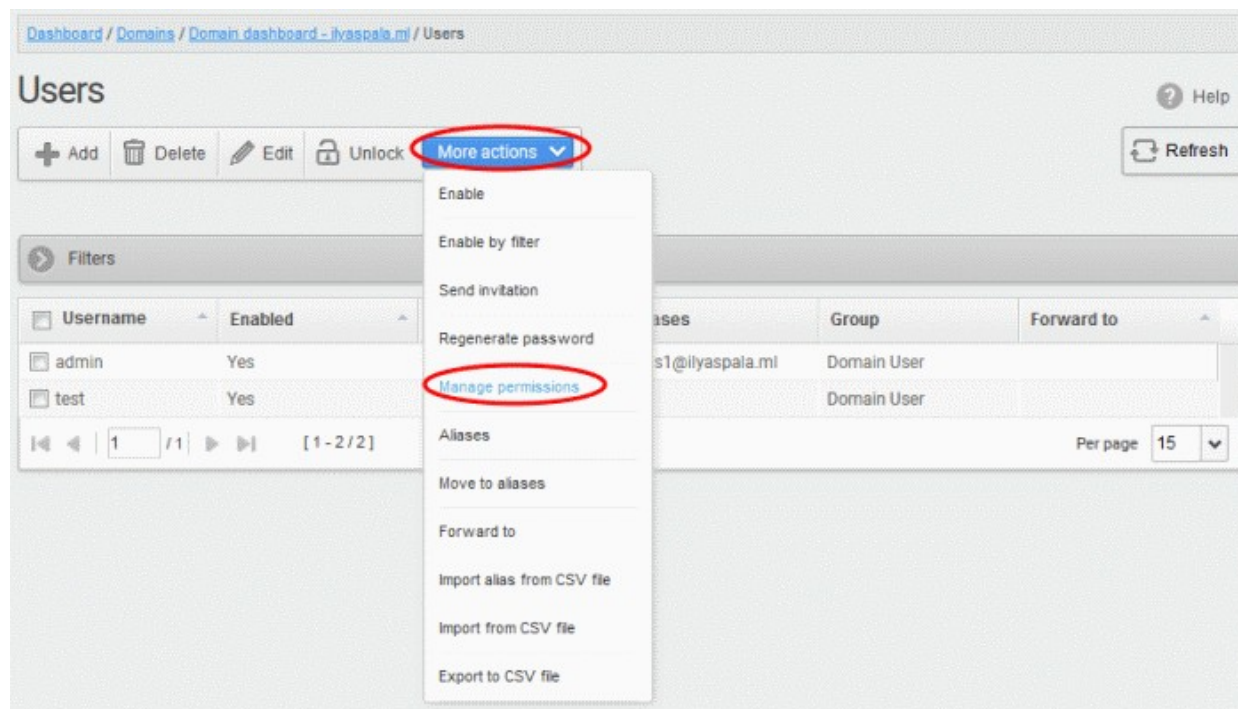
This file can be opened with Excel or Openoffice Calc.

Manage Permissions for users

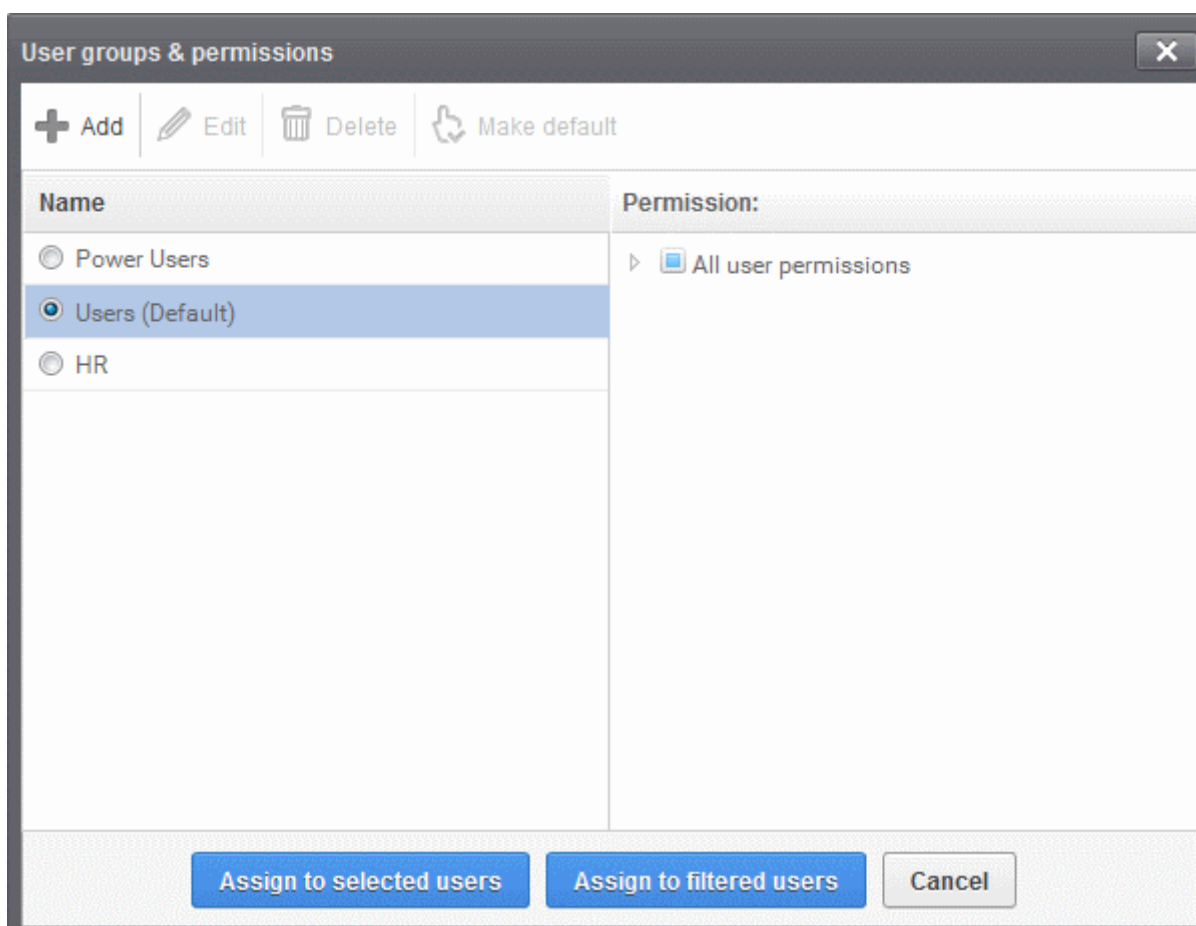
- Permissions determine what a user can and cannot do in the CASG interface.
- You can create policies which consist of a broad set of permissions, and assign them to users from this interface. See **User Groups & Permissions** for help to create groups and policies.
- New users automatically receive default permission settings.

Assign permissions for a user

- Select the user(s) and click 'More actions' > 'Manage permissions'

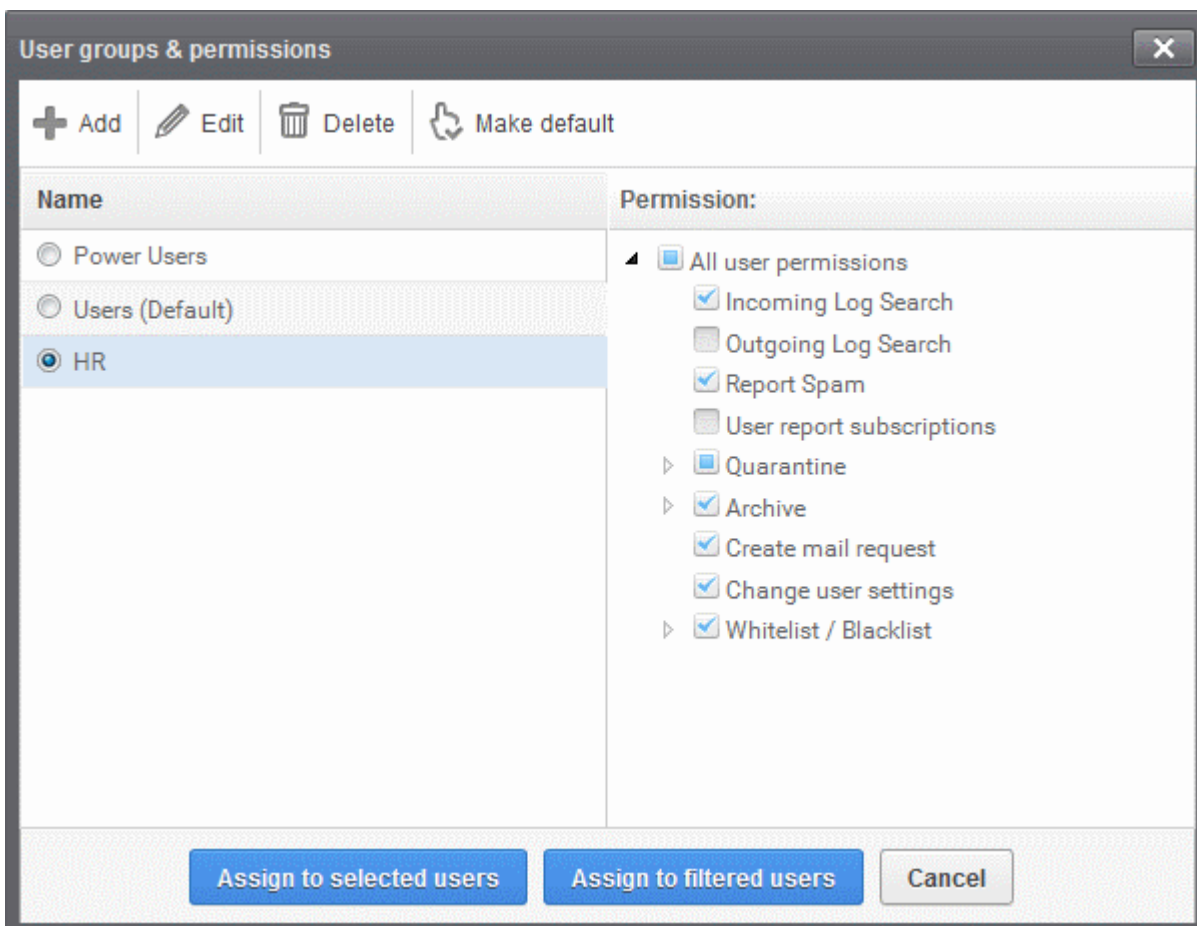


The 'User Groups & permissions' interface will appear.



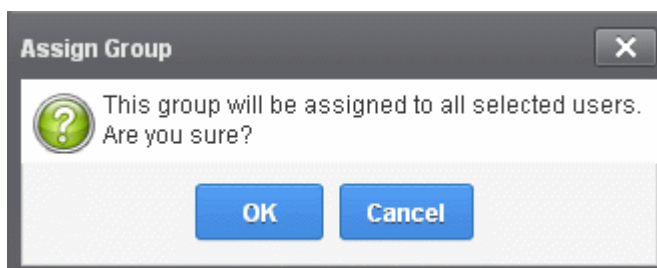
The interface displays the list of groups available with same or different permission levels for each group. By default, 'User (Default) and 'Power User' groups will be available and administrators can add, edit groups and assign permissions to users. See the section **User Groups & Permissions** for more details.

- Select the group from the list.

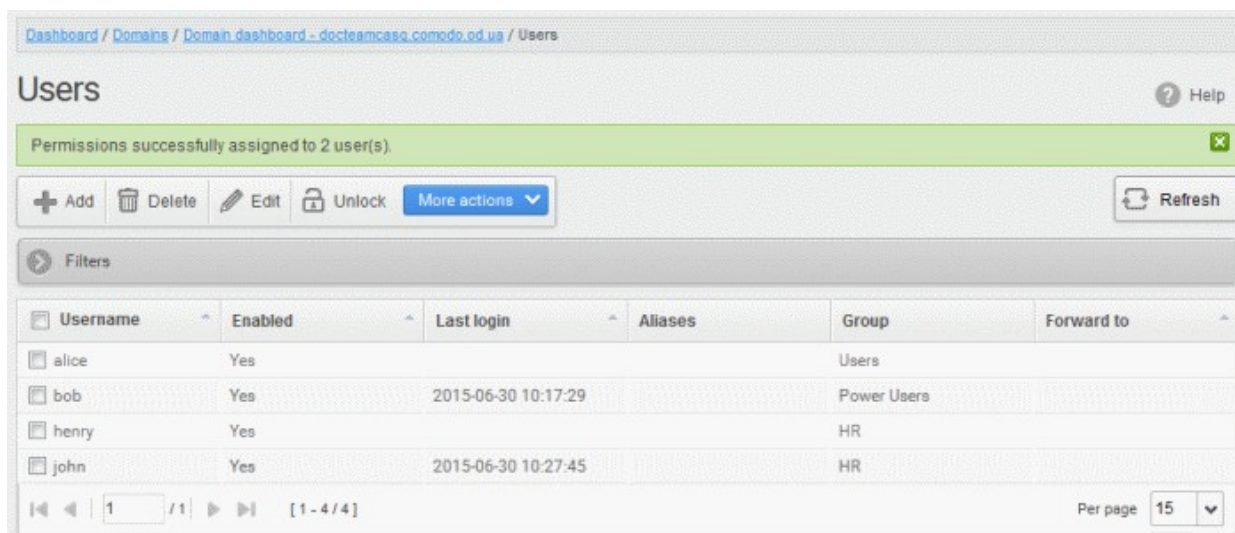


The permissions set for this group will be displayed on the right.

- Click the 'Assign to selected users' button to set permissions for selected user or multiple users.
- Click 'Assign to filtered users' button to set permissions for selected group to all users or to all users found by filter.
- Click 'OK' in the confirmation window.



The selected user(s) will be assigned to the group and successfully assigned message will be displayed.

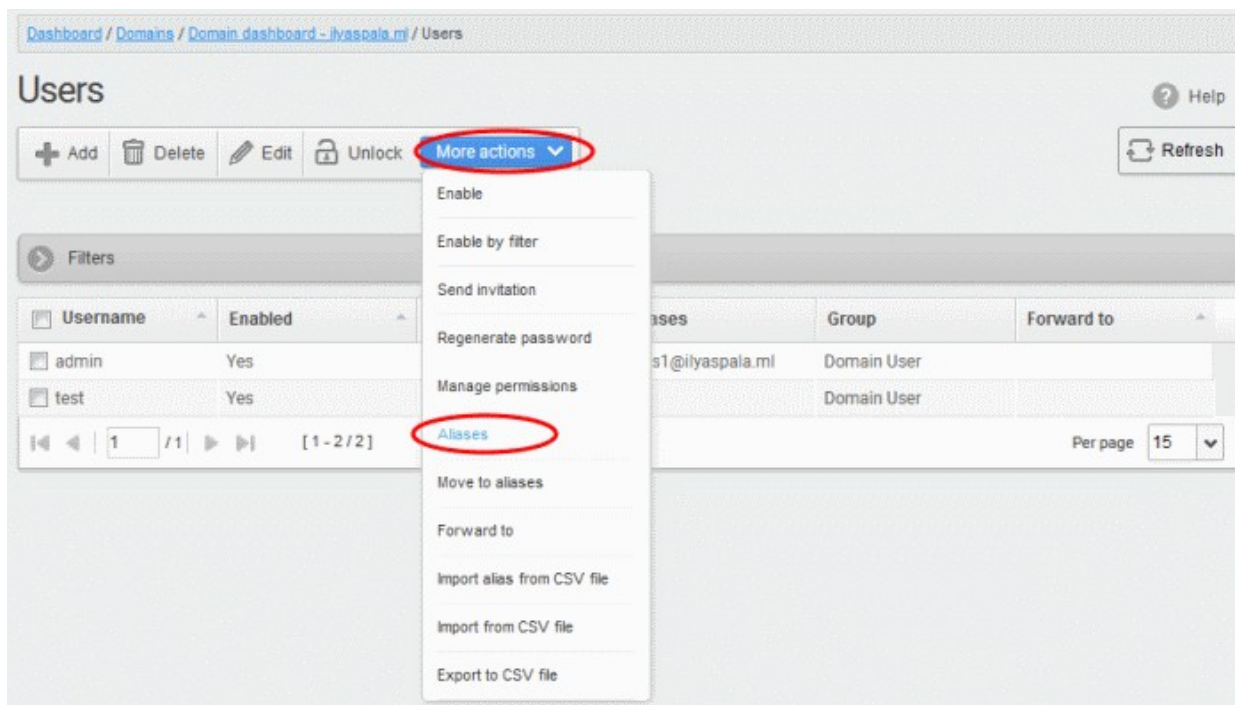


The interface also displays the new group assigned for the selected user under the 'Group' column.

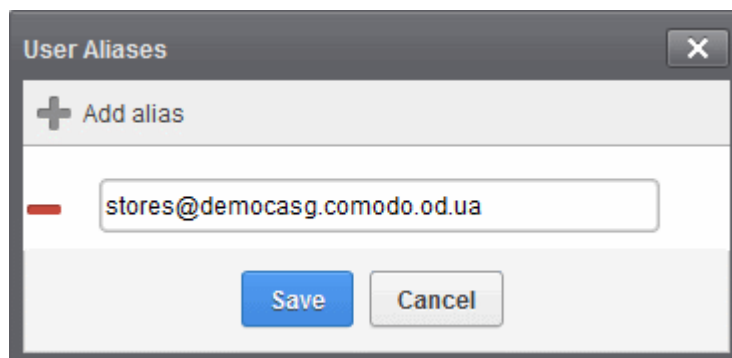
Adding the user aliases

CASG allows admins to add a user alias name to organize emails related to different groups or functions into a single email inbox automatically. The users can protect their real email address.

- Select a user and click 'More actions' > 'Aliases' to add user aliases.





- Enter the full email alias address of the user. **Note:** The alias email address must be of any domain belonging to the account.



- Click the Save button.

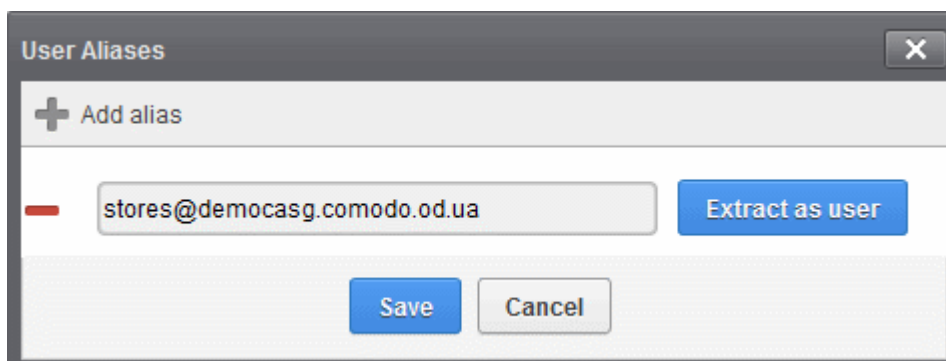
Note: Users cannot add an alias by themselves.

- To add multiple aliases click the  button.
- To remove an added alias row click the  icon beside it.

After adding a user to an alias, admins can extract him/her as a user.

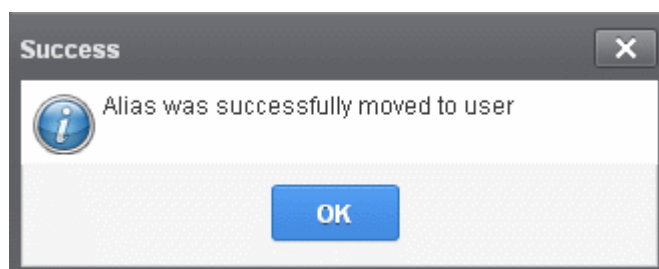
- Click the 'Aliases' button after selecting the user.

In the 'User Aliases' dialog next to the added alias row, the 'Extract as user' button will be displayed.



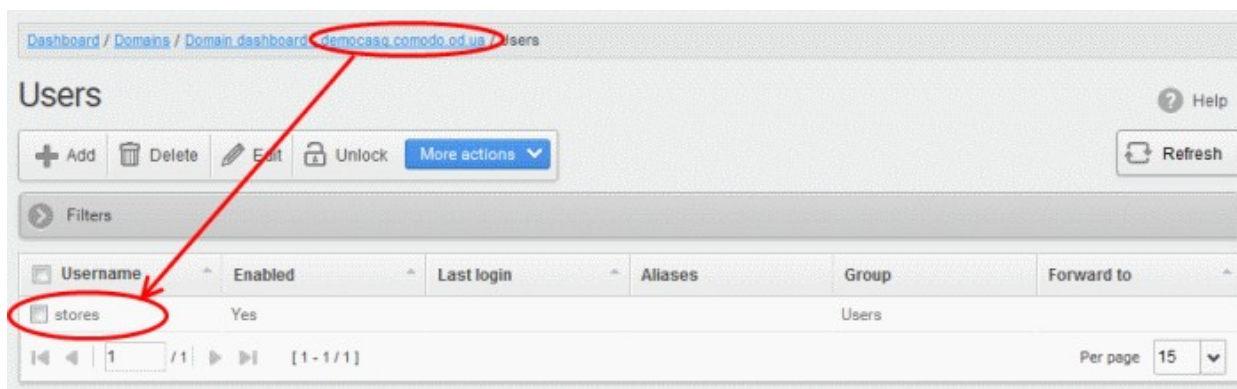
- Click the 'Extract as user' button.

The confirmation dialog will be displayed.



- Click 'OK'

The user extracted from the 'User Aliases' dialog box will be added to list of users in the respective domain added as alias and will be placed in the default group.

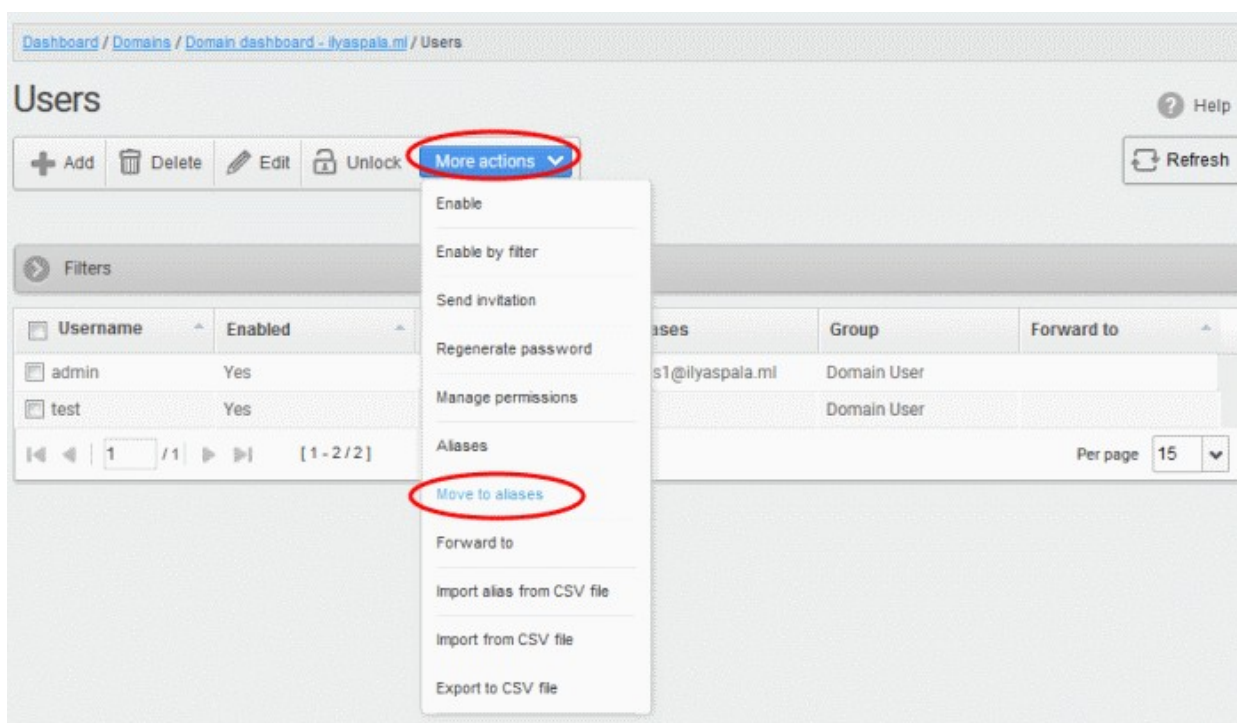


Note: The number of users that can be added for an account depends on the plan subscribed by you. When you exceed the limit of users, a warning will be displayed.

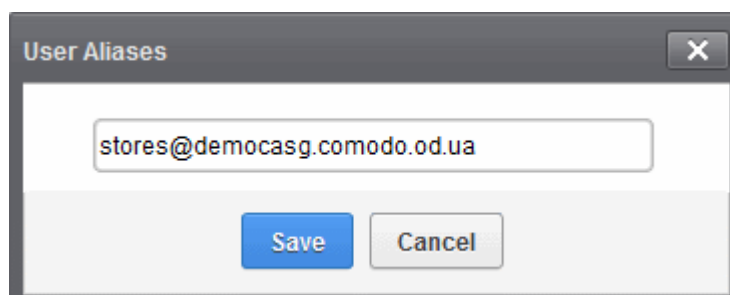
Moving user account to aliases

CASG allows admins to move an existing user as an alias for another user for any domain available in your account.

- Select the user then click 'More actions' > 'Move to aliases'

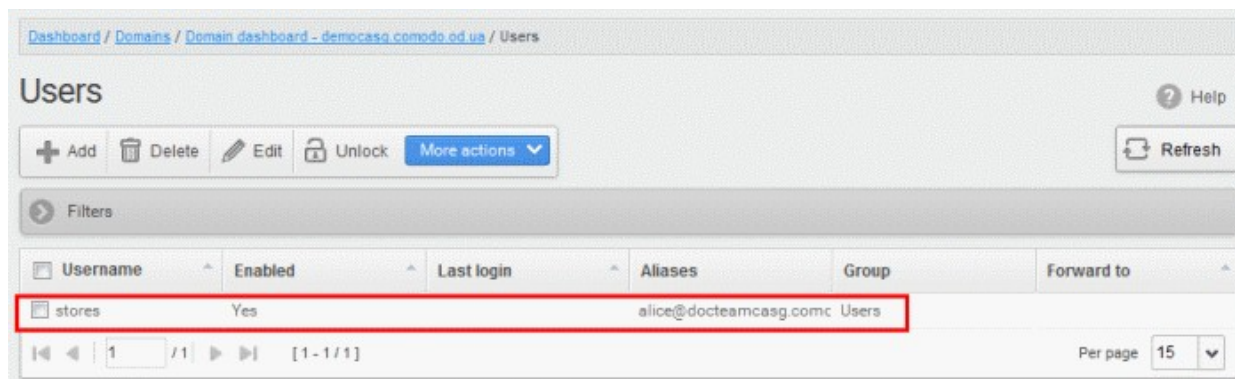


- Type the full email address of the user for whom the alias has to be added. **Note:** The user and domain should be valid and belong to your account.



- Click the 'Save' button.

Now, the selected user has become an alias of another user. (This could be for the same domain or another domain belonging to your account.)



Import alias from CSV file

You can add many aliases to existing user(s) at a time for the selected domain and / or for other domains available for your account by importing from a file. The aliases should be saved in 'comma separated value' (CSV) as shown below:

Example 1

The following example shows how you can add alias for two users for the selected domain.

```
alias@domain.com username1, username2
```

Example 2

The following example shows how you can add alias for users for the selected domain and other domains available for your account.

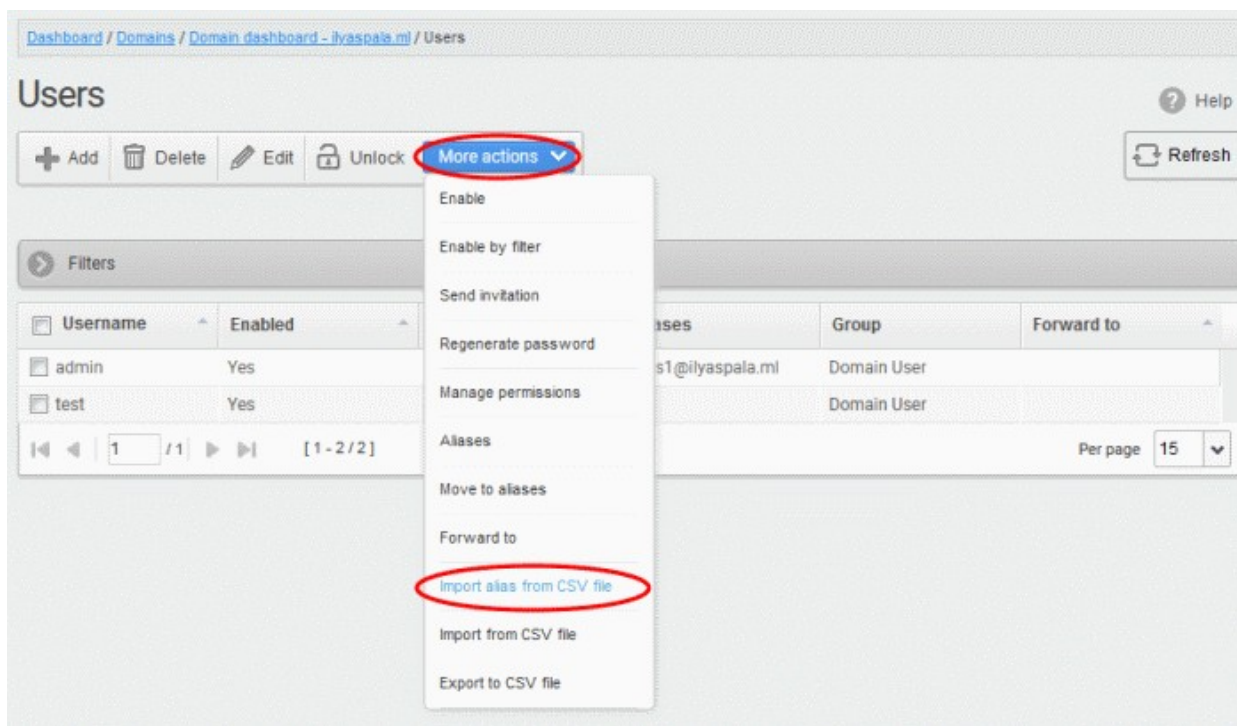
```
alias@domain.com username1, username2, username3@domain2
```

Please note that for adding many aliases at a time, each alias should be separated by a paragraph line. For example:

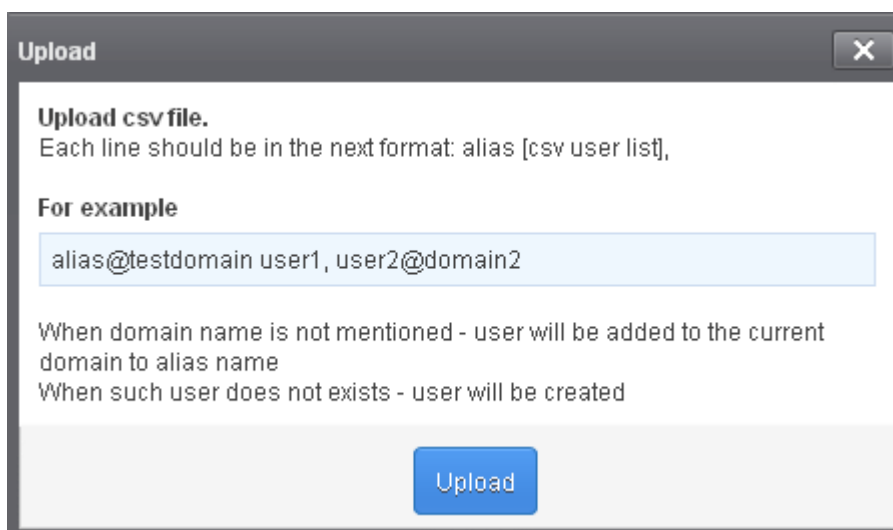
```
alias1@domain.com username1, username2
```

```
alias2@domain.com username1, username2, username3@domain2
```

- Click 'More actions' > 'Import alias from CSV file'

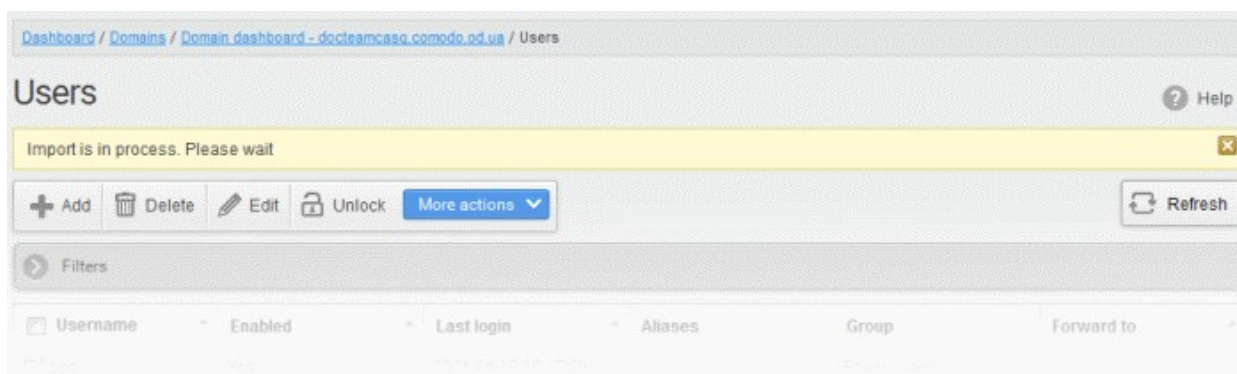


The 'Upload' dialog will be displayed.

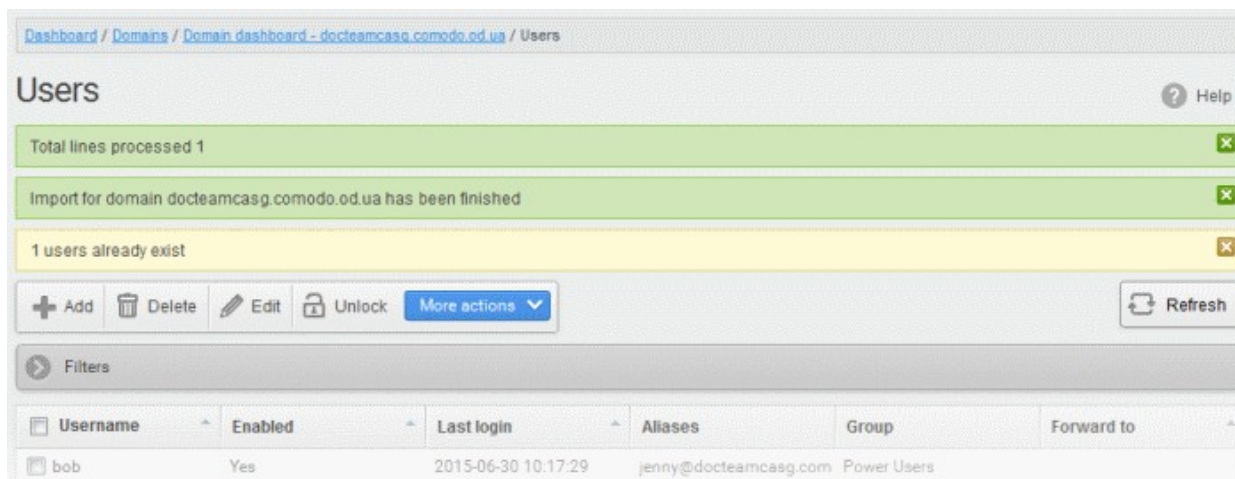


- Click the 'Upload' button and navigate to the location where the file is saved and click the 'Open' button.

The upload progress will be displayed...



...and when completed, the results will be displayed.

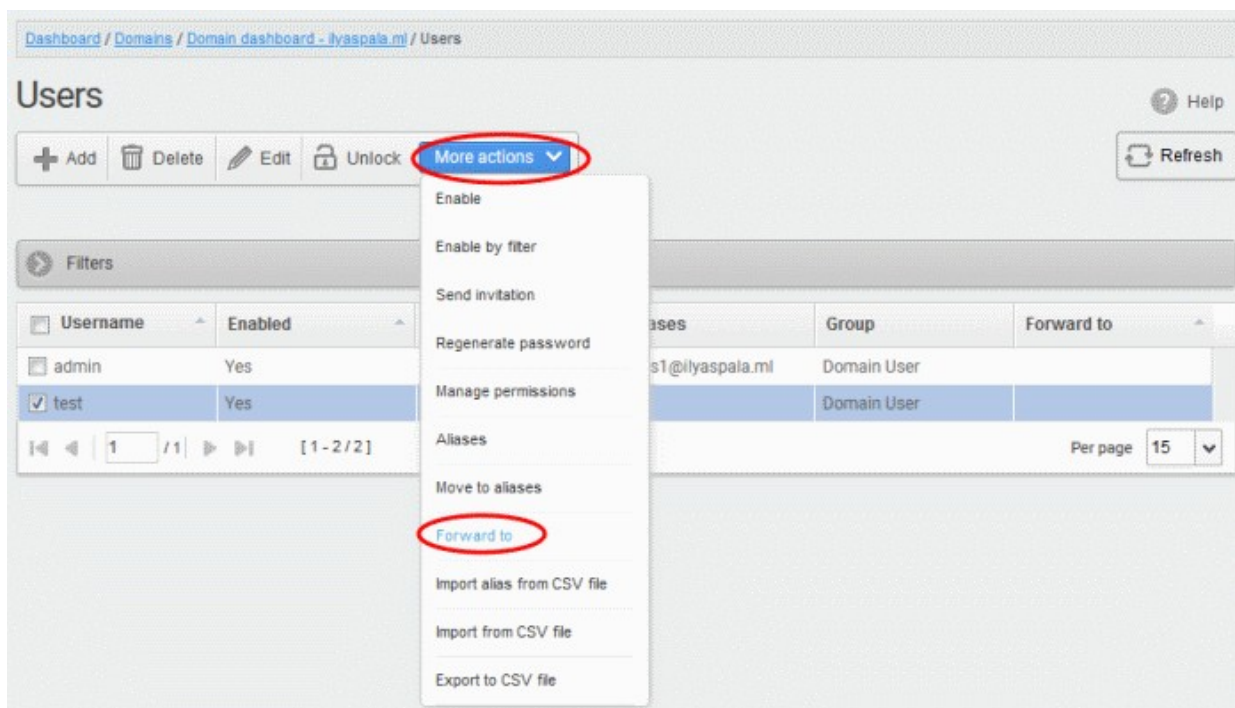


The administrator who carried out the task will receive a notification about the import task completion.

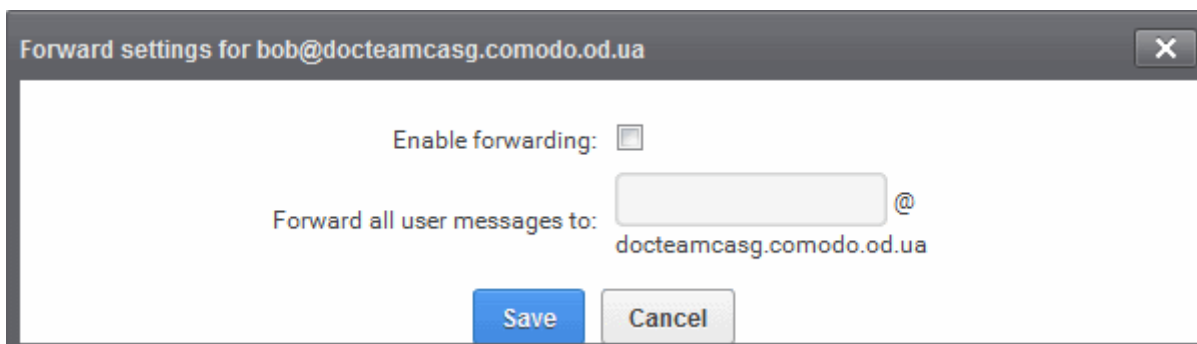
Forward mails to another user

CASG allows administrators to add a forwarding address for a user. This is useful when a user is on vacation or unavailable for sometime but the mails addressed to him should be attended immediately. Please note the forwarded user should also be in the same domain.

- Select the user whose mails have to be forwarded to another user and then click 'More actions' > 'Forward to'

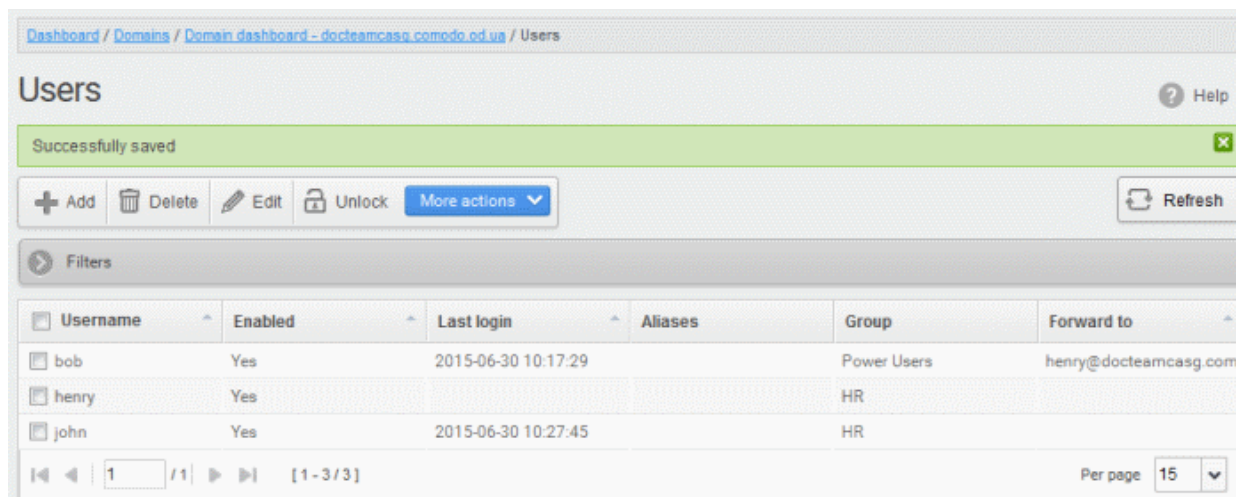


The 'Forward settings...' dialog will be displayed:

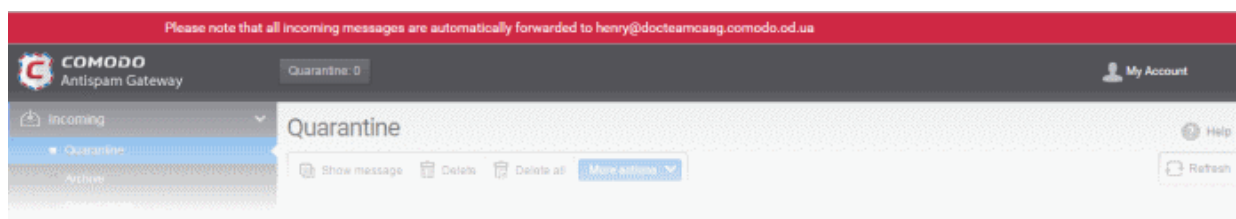


- Select the 'Enable forwarding' check box
- Enter the user name of the recipient to whom the mails have to be forwarded in the 'Forward all user messages to' field
- Click the 'Save' button

The forwarded user will be added and a success message will be displayed.

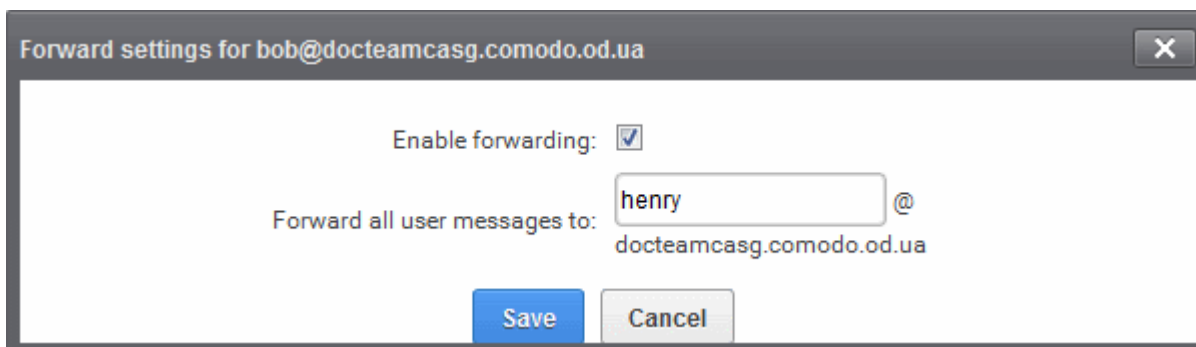


The incoming mails of the selected user will be automatically forwarded to the added user in the domain. When the selected user logs in to his/her CASG account, an alert will be displayed at the top of the interface.



- To remove the forwarded mail address for a user, select the user, click 'More actions' > 'Forward to'

The 'Forward settings...' dialog will be displayed:



- Deselect the 'Enable forwarding' check box
- Delete the username in the 'Forward all user messages to' field
- Click the 'Save' button

The forwarded user will be removed and a success message will be displayed.

Other Actions

- 'More actions' > 'Enable' - Allows user to access to CASG interface.
- 'More actions' > 'Enable by filter' - Allow CASG access to user selected by applying filter.
- 'More actions' > 'Regenerate password' - The password will be reset for the user in case it is forgotten. The new password will be sent to the user's email automatically. The user has to use this new password to access CASG.
- 'More actions' > 'Send invitation' - Send invitation to newly created users.

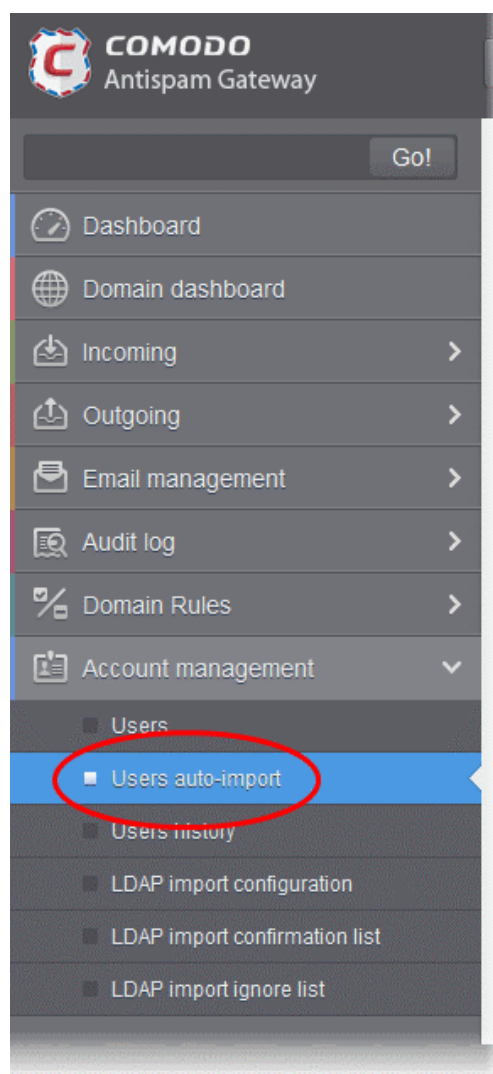
6.5.7.2 Manage User auto-import

CASG can automatically import users belonging to a managed domain after the domain receives its first email.

- Each new user will be imported in around 30 minutes and sent an invitation mail containing an activation link and credentials for their CASG account.
- New users can activate their CASG account by clicking the link in the invitation mail, or by directly logging-in to CASG with the credentials provided.
- Admins have the option to receive a notification whenever a new user is imported.

Auto-Import users

- Open the 'Domains' interface and select the domain you wish to configure
- Click the 'Manage Domain' button
- Select 'Account management' on the left then choose 'Users auto-import'



The 'Users auto-import' interface will open:

[Dashboard](#) / [Domains](#) / [Domain dashboard - docteamcasg.comodo.od.ua](#) / Users auto-import

Users auto-import

Enable auto-import

Automatically enable imported users

Send invitation to imported users

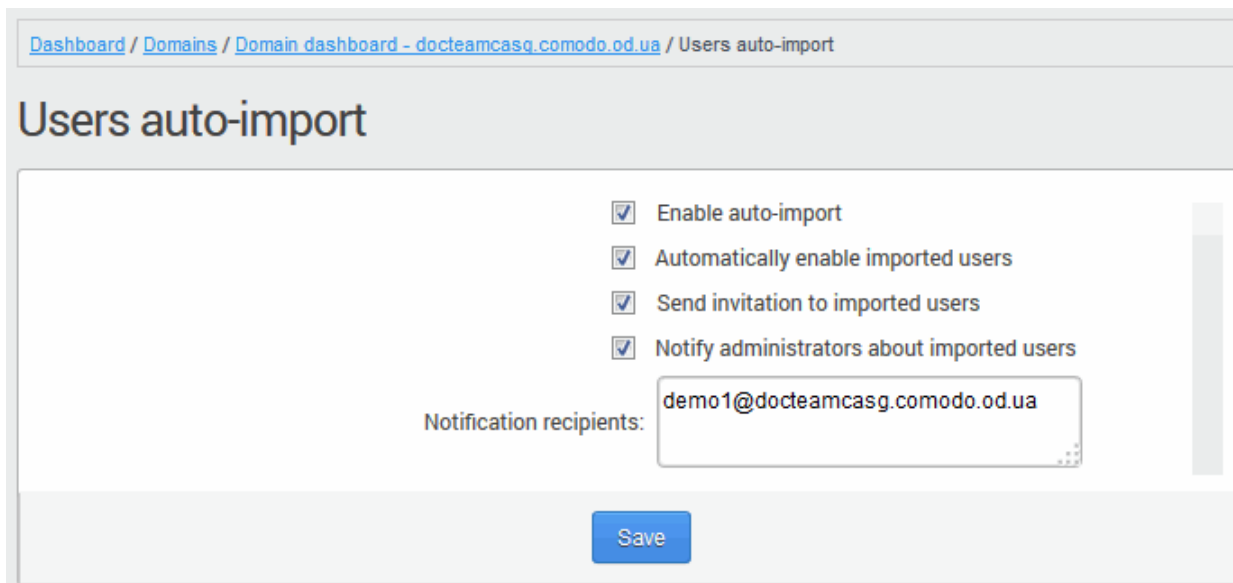
Notify administrators about imported users

Notification recipients:

- **Enable auto-import** - Select to activate the feature.
- **Automatically enable imported users** - Allows all imported users to access their CASG user account.
- **Send invitation to imported users** - Sends invitation mails to newly imported users. The mail

contains their account activation link and login credentials.

- **Notify administrators about imported users** - Select this option if admins should be notified whenever a new user is auto-imported. You can specify administrators (including self) to whom the notification mails are to be sent in the 'Notification recipients' box. The notification contains the imported user name and the domain name.
- **Notification recipients** - Enter the email addresses of admins to whom notification emails should be sent. You can enter multiple address, separated by commas.



Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Users auto-import

Users auto-import

- Enable auto-import
- Automatically enable imported users
- Send invitation to imported users
- Notify administrators about imported users

Notification recipients:

- Click 'Save' button for your settings to take effect.

Successfully saved

6.5.7.3 View User History

The 'Users History' area is a record of user activity in the CASG interface. You can filter users by IP address, last login, domain, username and/or location.

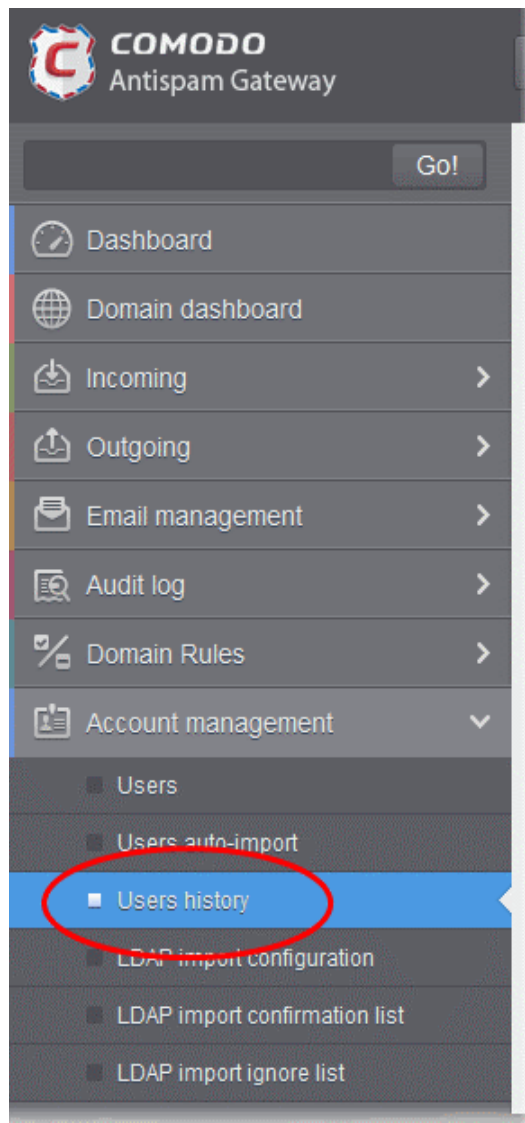
Note: This interface only shows user connections to the current domain (the domain that is shown near the top of the interface).

You can view user connections for all domains in the '**Account Management section**' (click 'Dashboard' > 'Account Management' > 'User's History').

The rest of this page explains how to access the history interface and use filters to create custom searches.

View user history

- Open the 'Domains' interface and select a domain
- Click the 'Manage Domain' button
- Click 'Account management' > 'User history'.



Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Users history ? Help

Filters

Username	Domain	IP	Location	Last login	Login duration (min)
bob	docteamcasg.comodo.od.ua	125.17.11.121	India	2015-06-29 08:24:00	Currently logged in
bob	docteamcasg.comodo.od.ua	125.17.11.121	India	2015-06-29 08:22:03	<1
john	docteamcasg.comodo.od.ua	125.17.11.121	India	2015-06-26 07:36:41	25
john	docteamcasg.comodo.od.ua	125.17.11.121	India	2015-06-26 05:57:04	1
john	docteamcasg.comodo.od.ua	125.17.11.121	India	2015-06-26 05:17:08	38

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Users history

Users history Help

Filters

Username	Domain	IP	Location	Last login	Login duration (min)
bob	docteamcasg.comodo.od.ua	125.17.11.121	India	2015-06-29 08:24:00	Currently logged in
bob	docteamcasg.comodo.od.ua	125.17.11.121	India	2015-06-29 08:22:03	<1
john	docteamcasg.comodo.od.ua	125.17.11.121	India	2015-06-26 07:36:41	25
john	docteamcasg.comodo.od.ua	125.17.11.121	India	2015-06-26 05:57:04	1
john	docteamcasg.comodo.od.ua	125.17.11.121	India	2015-06-26 05:17:08	38

- Click any column header to sort items in ascending/descending order of the entries in that column.

The sorting option is not available for 'Login Duration' column.

Use filters to search for users

- Click anywhere on the 'Filters' stripe to open the filters area.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Users history

Users history Help

Filters

+ Username contains Apply filter

- Username contains

Username
 Domain
 IP
 Location
 Last login

User	Domain	IP	Location	Last login	Login duration (min)
bob	docteamcasg.comodo.od.ua	125.17.11.121	India	2015-06-29 08:24:00	Currently logged in
bob	docteamcasg.comodo.od.ua	125.17.11.121	India	2015-06-29 08:22:03	<1

- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

- Username:** Type a user name in the text box (column 3) and select a condition in column 2.
- Domain:** Type a domain name in the text box (column 3) and select a condition in column 2.
- IP:** Type an IP address in the text box (column 3) and select a condition in column 2.
- Location:** Type a user location in the text box (column 3) and select a condition in column 2.
- Last Login:** Sorts the results based on the last login details of users.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

You can add multiple filters to the same search by clicking +.

6.5.7.4 Import Users from LDAP

In addition to manually adding users or importing them from .csv, you can also import users from the domain's Active Directory (AD) server.

- CASG uses the Lightweight Directory Access Protocol (LDAP) to import users from AD.
- CASG periodically synchronizes with the AD server to update the list of valid users.

Click the following links for more help:

- [LDAP Import Configuration](#)
- [LDAP Import Confirmation List](#)
- [LDAP Import Ignore List](#)
- [Troubleshooting LDAP](#)

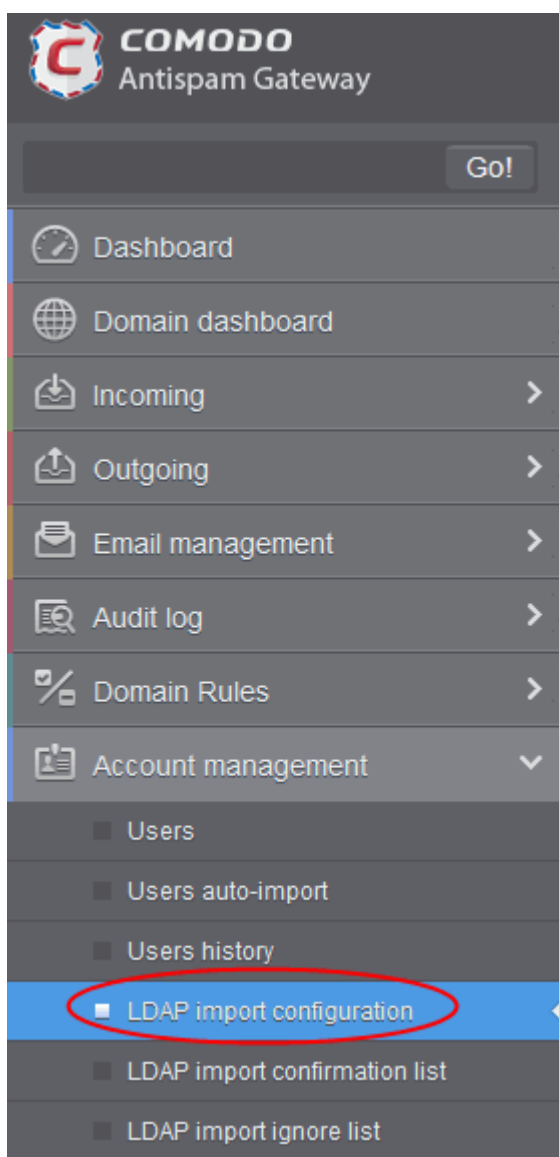
LDAP Import Configuration

The LDAP import screen lets you import users from the domain's Active Directory server.

We recommend you create a separate user account for CASG to login to the AD server, and that this account be given read-only permissions.

Configure LDAP import

- Open the 'Domains' interface
- Select the domain to which you want to import users.
- Click the 'Manage Domain' button
- Click 'Account management' > 'LDAP import configuration':



The 'LDAP import configuration' interface will open:

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / LDAP import configuration

LDAP import configuration ? Help

Connection settings

Host (IP address or name):

Port: LDAP(389) | LDAPS(636)

Use SSL to connect?: Yes

Login/Query settings

LDAP login name:

Password: Remember credentials

Synchronization interval:

BaseDN:

Filter:

Mail attribute:

Override existing records

Allow CASG to create user accounts as found on LDAP server

Allow CASG to delete user accounts not found on LDAP server

Information

Send reports: Yes

Last synchronization time (GMT):

Connection Settings

- **Host (IP Address or Name)** - Enter the hostname or external IP address of the AD server. If your organization uses the same physical server for AD and mail, then enter the details of the mail server.
- **Port** - Enter the port number of the Active Directory server.
 - 389 is the default port for non-SSL connections ('Use SSL To Connect?' box NOT checked)
 - 636 is the default port for SSL connections ('Use SSL To Connect?' box checked)
- **Use SSL To Connect?** - Select 'Yes' to use secure LDAP. You need to have an SSL certificate from a trusted certificate authority on your AD server. Self-signed certificates are not allowed.

Note: SSL access should have been enabled for the AD Server before enabling the SSL option.

Login/Query Settings

- **LDAP login name** - Account username which CASG should use to login to the AD server. Preferably, a new user account should be created especially for the CASG server. The user account should have 'read' privileges to the AD server. The username can be of the format 'username' or 'username@domainname.com'
- **Password** - Enter the password of the LDAP user account above.
- **Remember Credentials** - Enable if you want CASG server to store the username/password of the user account in order to automatically login.

Note: If you enable automatic synchronization, the 'Remember Credentials' option will not be visible because CASG will store the username and password by default. This allows CASG to connect to the AD server at the set

time interval to update the user base. The option will become visible if 'Synchronization Interval' setting is set as 'no auto updates'.

- **Synchronization interval** - This is relevant if you want CASG to connect to the AD server in order to synchronize the user base. Select the time interval at which the synchronization occurs from the drop-down. If not, select 'No auto updates'.
- **BaseDN** - Distinguished Name of the user object in Active Directory. By default, the BaseDN field will contain the Domain Component (DC) values based on the domain name for which LDAP is configured. You can add/change the values of the strings 'Container Name (CN)', 'Organizational Unit (OU)' and 'domain name' depending on the users to be imported from the Active Directory.

Example: For adding users from Container 'Users', Organizational unit 'Organization' and domain 'example.com', the administrator has to enter the following:

CN=Users, OU = Organization, DC=example, DC=com

- **Filter** - Enables the Administrator to specify filter parameters users/addresses to be imported from the AD server. Each filter parameter should be defined within parentheses. Common filter parameters are explained below:
 - (objectClass=<AD user type>)** - Specifies the user accounts to look for from the domain's Active Directory. (Default = (objectClass=User))

(mail=<domain name>) - Instructs CASG to import only the users that have a defined SMTP account within the domain. By default, the filter is pre-added with the parameter (mail=*@<current domain name>) to import the users that have email addresses on the current domain.

You can add any number of (mail=) filters if you wish to add several domain names

Example: (mail=*@domainname1.com)(mail=*@domainname2.com)

To import all email enabled users from the Active Directory irrespective of any specific domain name, enter the parameter as '(mail=*)'.

To modify a filter parameter to be exclusive rather than inclusive, add an exclamation mark (!) before the opening parenthesis of any parameter. This will instruct the query to ignore any users which fall into that category. For example, if one wanted to configure a query to find users with mail enabled at any domain EXCEPT domainname.com, the filter should include the following: (mail=*)!
(mail=*@domainname.com).

To import all email enabled users from the Active Directory irrespective of any specific domain name, enter the parameter as '(mail=*)'.

Note:

- You can only import users whose email addresses are on domains which have been added to CASG. You can view these domains in the **Domains** interface.
- You must ensure LDAP Import is enabled for the domain in the **Domain Management** area

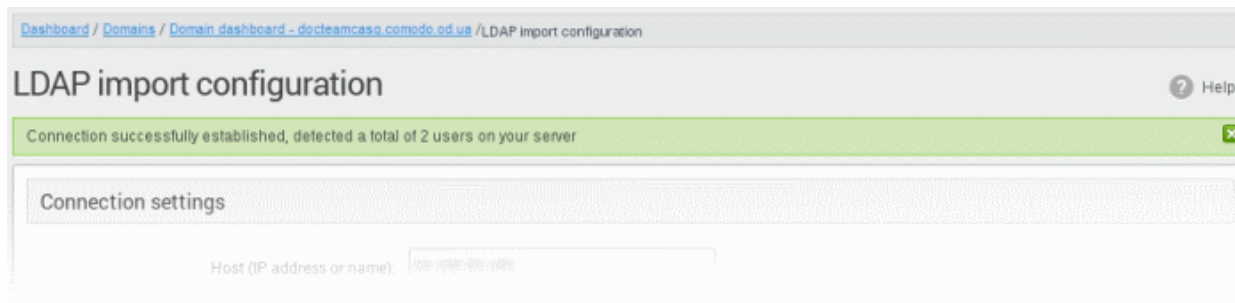
- **Mail attribute** - Enter the LDAP display name of the contact email address attribute of the AD Server. By default, this attribute name will be 'mail' for AD servers or the distinguished name (DN) or common user login name for the AD server. On other servers like Novel or OpenLDAP this attribute may be different and server specific.

Override existing records:

- **Allow CASG to create user accounts as found on LDAP server** - Select this checkbox if you wish new users added in the AD server to be automatically added to CASG during synchronization. If you do not select this option, you can manually import the new users from the [LDAP import confirmation page](#).
- **Allow CASG to delete user accounts not found on LDAP server** - Select this checkbox if you wish users removed from AD server, to be automatically removed from CASG during synchronization. If you do not select this option, you can manually remove users from the [LDAP import confirmation page](#).

Information Settings

- **Send Reports** - If enabled, CASG will send email notifications to the administrator whenever new users are created or users are removed either automatically, (if 'Allow to create users?'/ 'Allow to delete users?' are enabled) or manually from the LDAP import confirmation page.
- **Last synchronization time (GMT)** - Displays the date and time of last manual or scheduled synchronization with AD server, in GMT.
- **Notification area** - Contains information about errors that occurred during synchronization. In most cases, this will contain the same information that is provided with the "Test connection" feature. Note - this area is only visible if errors occur.
- To check the configuration and connectivity, click 'Test Connection'. If the connection is established successfully then the success message will be displayed with the total number of users detected from the AD server.



- Click 'Save' to store your configuration.
- Click 'Save and run synchronization now' to store your configuration and synchronize the CASG user base with the AD server.

LDAP Import Confirmation List

The LDAP import confirmation list interface displays the list of:

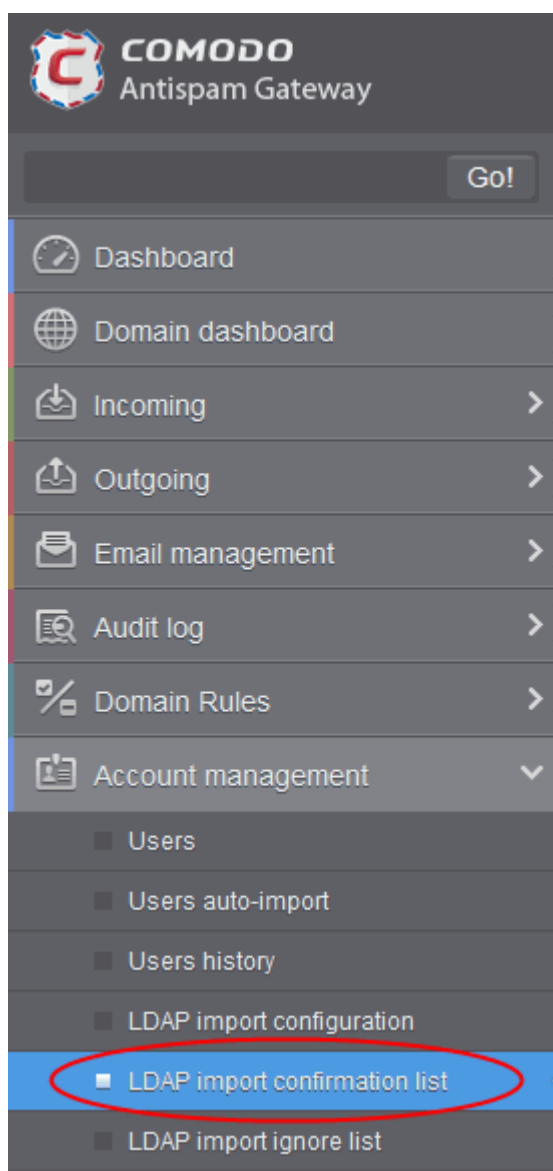
- Users created at the AD server and not yet been imported into CASG
- Users not present on AD server and not yet been removed from CASG

... if "**Allow to create users?**" / "**Allow to delete users?**" are not enabled in **LDAP import configuration interface**, along with the list of users created in CASG. The administrator can import the users created at AD server into CASG manually and remove existing users from this interface.

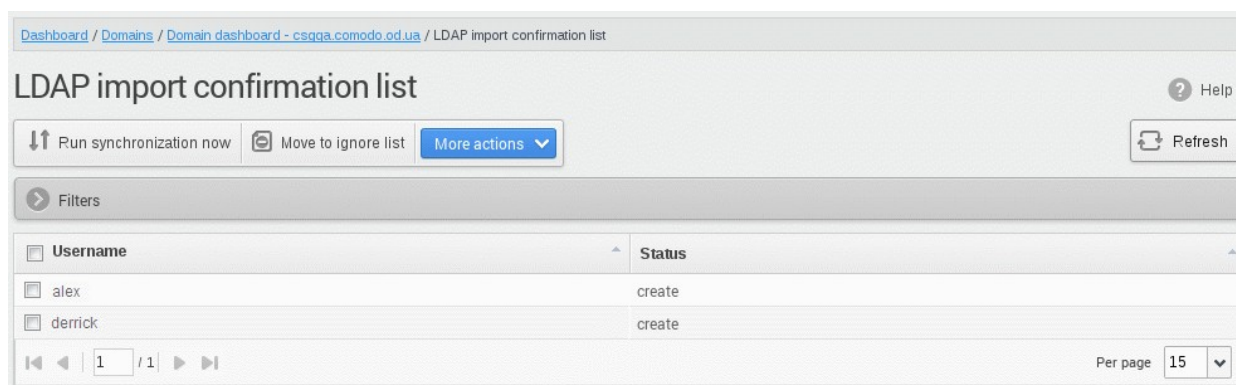
- Administrators can also initiate an on-demand synchronization from this interface.

To view LDAP import confirmation list

- Open the 'Domains' interface and select a domain
- Click the 'Manage Domain' button to open the 'Domain Management' interface.
- Click 'Account management' on the left then select 'LDAP import confirmation list'.



The 'LDAP import confirmation list' interface will open:



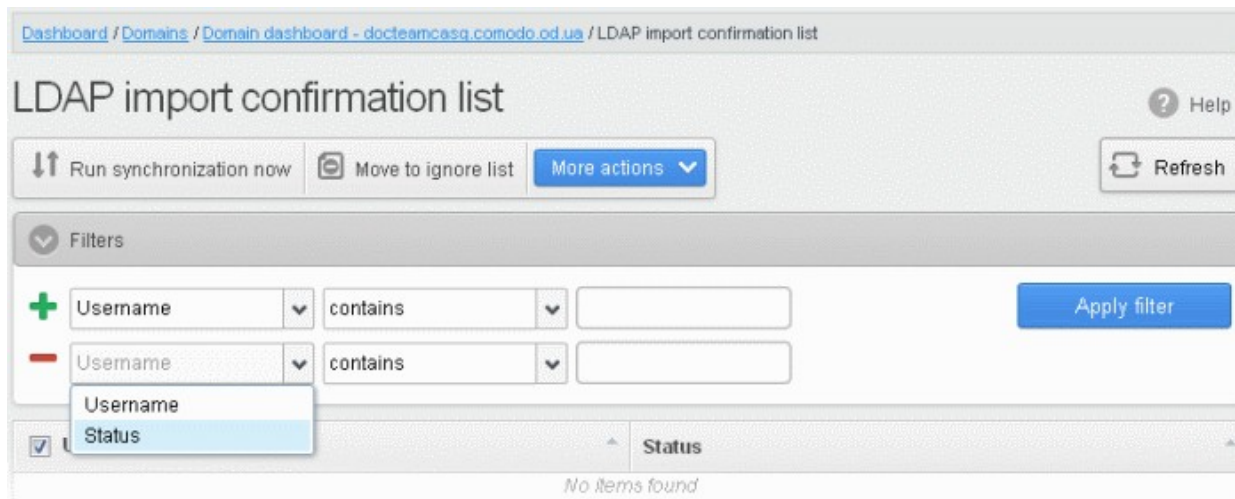
The screen shows users added to and removed from the AD server with existing users created on CASG. This list reflects the difference between CASG users and AD users, considering the **LDAP ignore list**.

- Users present in AD which are not present in CASG will have the status 'Create'
- Users not present in AD but present in CASG will have the status 'Delete'
- Click any column header to sort items in ascending/descending order of the entries in that column.

The sorting option is not available for 'Login Duration' column.

Use filters to search for users

- Click anywhere on the 'Filters' stripe to open the filters area.




- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

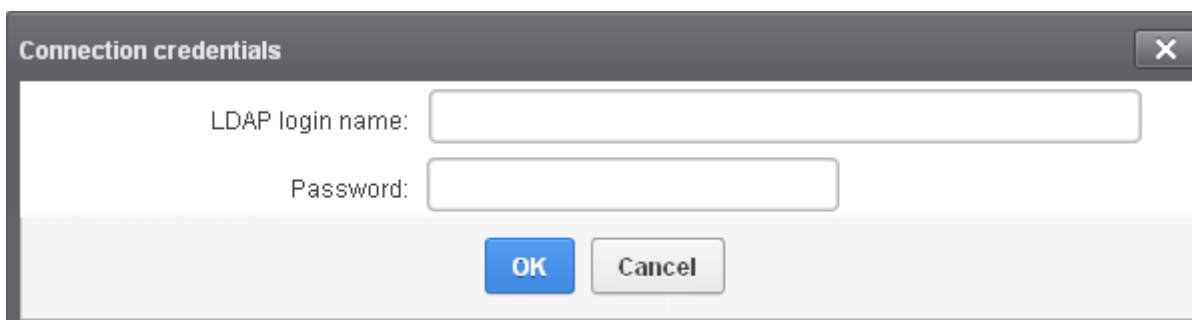
- **Username:** Type a user name in the text box (column 3) and select a condition in column 2.
- **Status:** Search users that were created per the user accounts found on LDAP server and that were deleted whose accounts not found on LDAP server. Select the condition in column 2 and the parameter in column 3.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

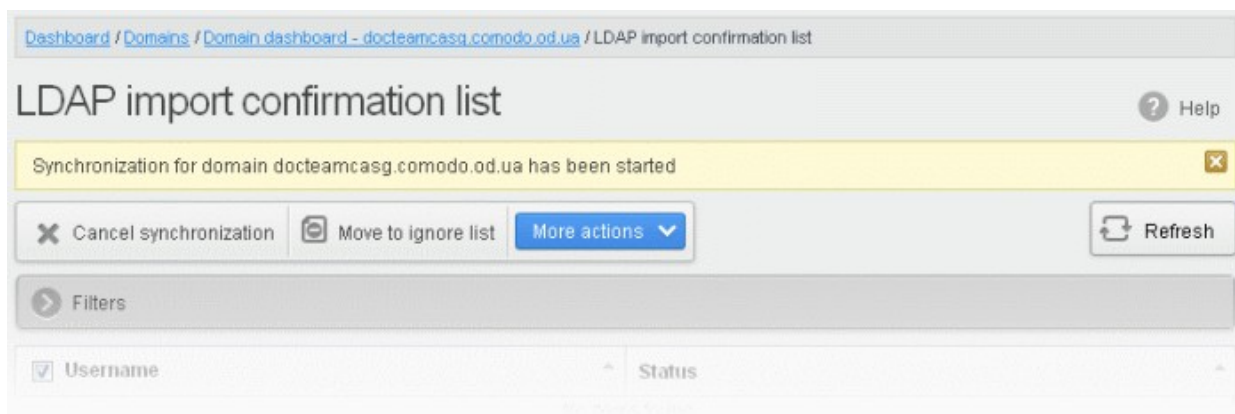
You can add multiple filters to the same search by clicking .

Run synchronization now – Manually synchronize the database

If you have not selected the option **Remember credentials** in **LDAP Import Configuration interface**, you will be asked to enter the username and password for CASG to access the AD server.



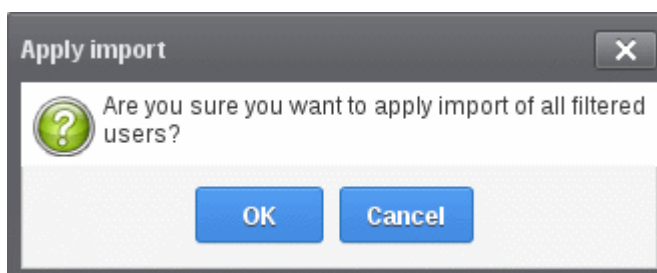
- Enter the LDAP login credentials and click 'OK'.



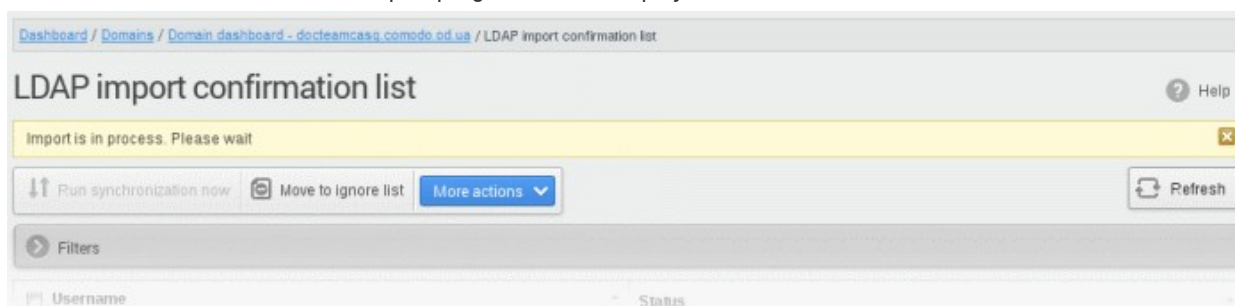
CASG will connect to your AD server to identify changes in the user database.

All users on the AD server are shown as a list.

- Click 'More actions' to select an import option.
- Click 'Ok' to confirm the import:



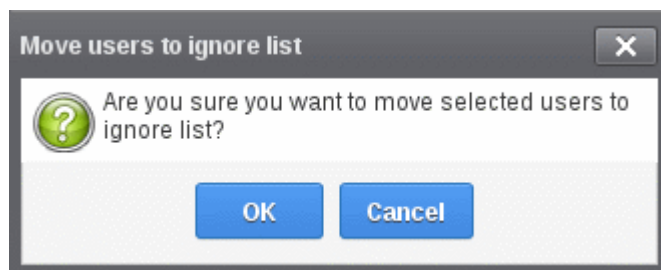
- Click 'OK'. The import progress will be displayed.



On completion, the selected users will be imported or deleted in synchronization with the AD server.

Note: The number of users that you can add for all the domains belonging to your account depends on your subscription plan. For example, if the subscription plan for your account allows you to add 1000 users and you have three domains, then you can add 300 users for domain 1, 300 users for domain 2 and 400 users for domain 3. You can set any value between 0 and 999999 in the 'Max. number of users' field in the **Add Domains / Edit Domains / Domain Settings** interface, but CASG checks if the total number of users for all domains is within your license limit.

- To move selected users to Ignore List, select the users and click 'Move to Ignore list'



... and click 'OK' in the confirmation dialog.

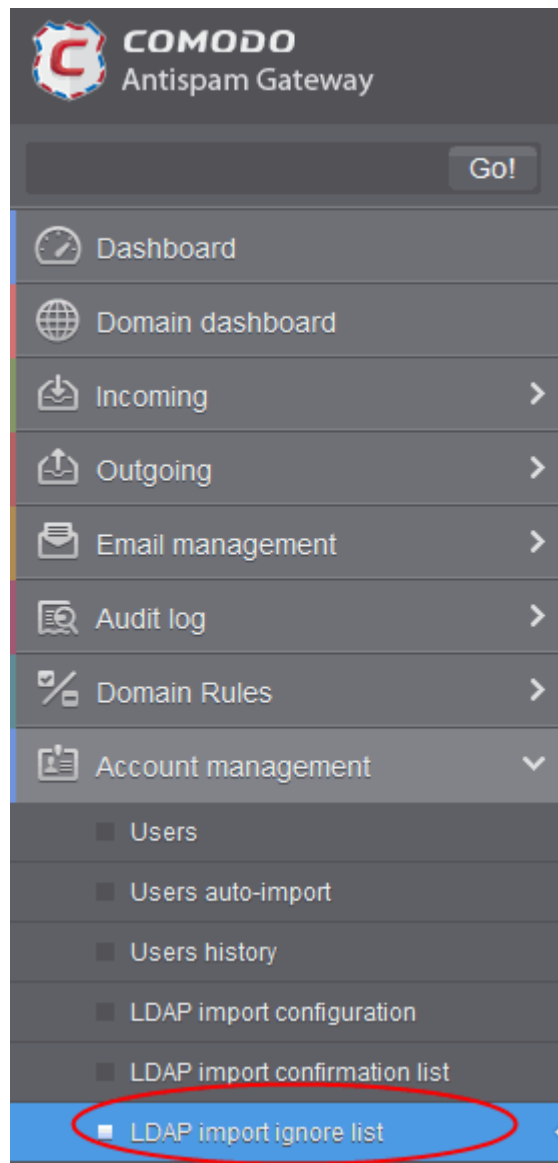
Users moved to **ignore list** will be skipped from next synchronization with the AD server.

LDAP Import Ignore List

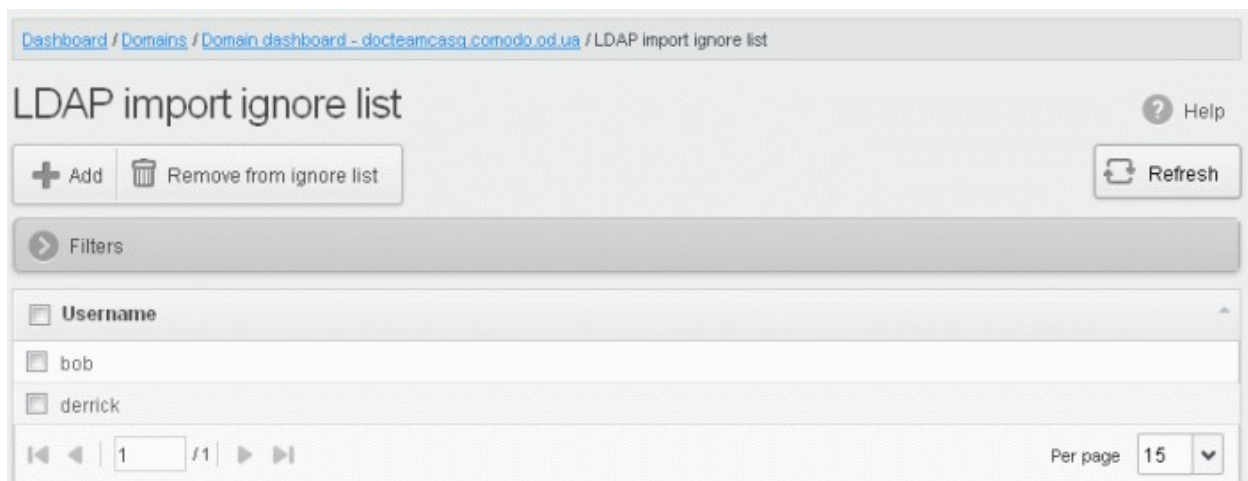
The LDAP import ignore list interface displays a list of users to be skipped from being created or deleted in CASG during synchronization with the AD server. Users can be moved to ignore list from the LDAP Import Confirmation List interface or manually added. Once added to the ignore list, the user will be skipped from the AD server from the next synchronization operation.

View LDAP import ignore list

- Open the 'Domains' interface and select the domain
- Click the 'Manage Domain' button to open the 'Domain Management' interface.
- Click 'Account management' tab > 'LDAP import ignore list' sub tab.



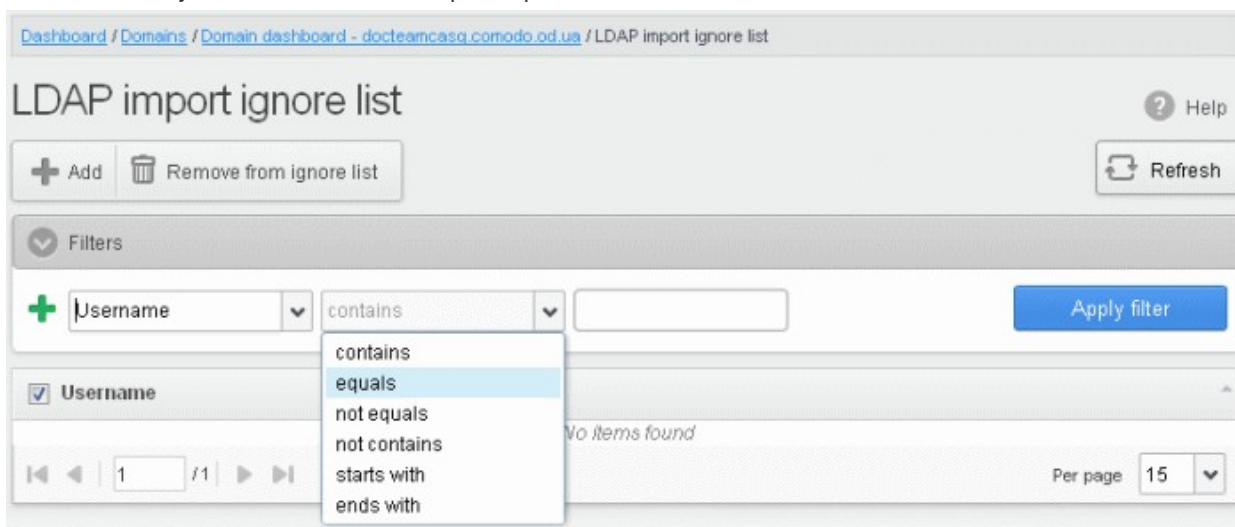
The 'LDAP import ignore list' interface will be displayed.



- Click the 'Username' column header to sort items in ascending/descending order of the usernames

Use filters to search for users


- Click anywhere on the 'Filters' stripe to open the filters area.



You can filter results by the username:

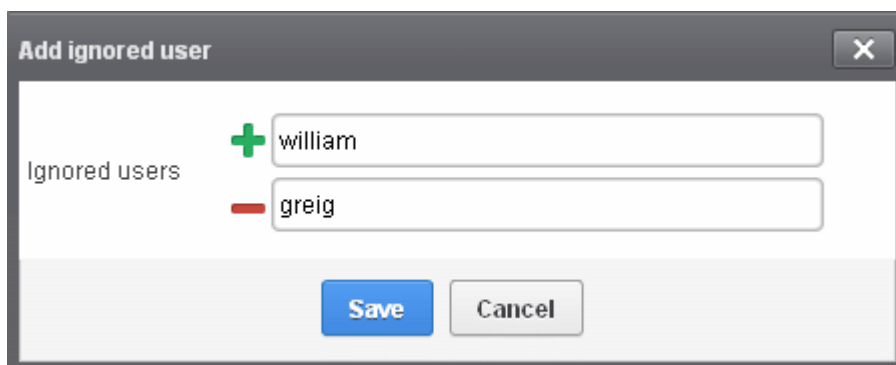
- Username:** Type a user name in the text box (column 3) and select a condition in column 2.


Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

You can add multiple filters to the same search by clicking .

Add users to ignore list

- Click 'Add'. The Add ignored user dialog will be displayed.

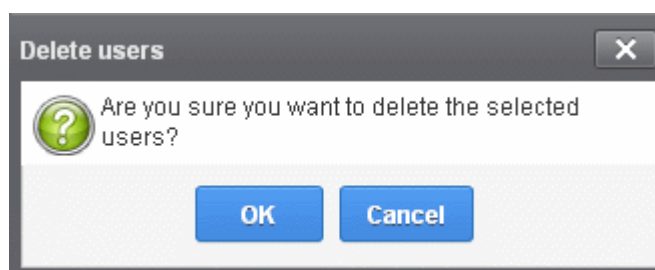


- Enter the user names to be added to the ignore list
- Click the  icon to add more users
- Click Save to add the users.

A 'Successfully added' message will be displayed at the top.

To remove the users from the ignore list

- Select the users and click 'Remove from ignore list'. A confirmation dialog will be displayed.



- Click 'OK'.

The users will be removed from the list and a 'Successfully deleted' message will be displayed at the top.

- Users removed from the ignore list will be imported to or deleted from CASG based on changes in the AD server, during the next synchronization if '**Allow to create users?'**'/**'Allow to delete users?'** are enabled in **LDAP import configuration interface**.
- Users removed from the ignore list will be listed in the LDAP import confirmation list interface based on changes in the AD server, during the next synchronization if '**Allow to create users?'**'/**'Allow to delete users?'** are not enabled in **LDAP import configuration interface**.

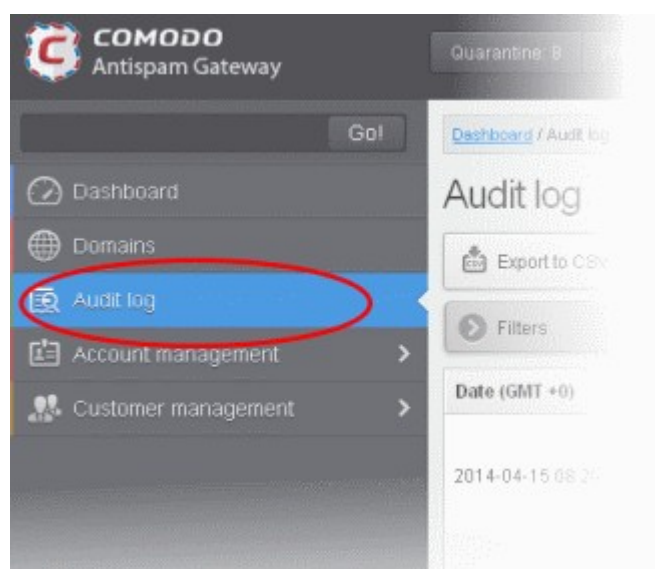
7 Audit Log

Audit logs are a record of actions taken by users and admins on domains on your account.

- This logs in this section cover all domains on the account.
- Alternatively, CASG also keeps separate logs for each domain. See **Domain Audit Log** if you want this instead.

View Audit logs

- Click 'Dashboard' > 'Audit log':



The log details for all the domains will be displayed.

Dashboard / Audit log

Audit log

Export to CSV by filter Refresh

Filters

Date (GMT +0)	Domain	Role	Login	Operation key	Operation description	Details
2014-10-28 16:30:52	docteamcasg.comodo.od.ua	system		ACCEPT_AND_ARCHIVE	Accept and archive message	Recipients: john@docteamcasg.comodo.od.ua; Sender: admin@antispamgateway.comodo.com; Date: Tue Oct 28 14:53:04 GMT 2014; Subject: New account registered
2014-10-28 16:30:51	docteamcasg.comodo.od.ua	system		ACCEPT_AND_ARCHIVE	Accept and archive message	Recipients: john@docteamcasg.comodo.od.ua; Sender: admin@antispamgateway.comodo.com; Date: Tue Oct 28 14:53:04 GMT 2014; Subject: New account registered
2014-10-28 16:30:29	docteamcasg.comodo.od.ua	system		ACCEPT_AND_ARCHIVE	Accept and archive message	Recipients: demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua; Sender: admin <demo@csg.comodo.od.ua>; Date: Tue Oct 28 13:37:58 GMT 2014; Subject: Re: DQ demo
2014-10-28 16:28:51	docteamcasg.comodo.od.ua	system		ACCEPT_AND_ARCHIVE	Accept and archive message	Recipients: demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua; Sender: admin <demo@csg.comodo.od.ua>; Date: Tue Oct 28 13:38:30 GMT 2014; Subject: DQ demo 2

- Click any column heading to sort entries in ascending/descending order. The sorting option is not available for the 'Operation description' column.

Use Filter options to search particular event(s)

- Click anywhere on the 'Filters' stripe to open the filters area.

Dashboard / Audit log

Audit log

Export to CSV by filter

Filters

+ Domain contains

- Date equals

Date Domain Role Login Operation key

2014-10-28 16:30:52 docteamcasg.comodo.od.ua system superadmin DELETE_EMAIL

- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

- **Domain:** Type a domain name in the text box (column 3) and select a condition in column 2.
- **Login:** Type a user login name in the text box (column 3) and select a condition in column 2.
- **Details:** Enter the log details in the text box (column 3) and select a condition in column 2.
- **Date:** Search event logs by date and time.
- **Role:** Search event logs by user roles. Select the role (column 3) and condition in column 2.
- **Operation Description:** Select the event name (column 3) and condition in column 2.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

You can add multiple filters to the same search by clicking .

The following table show actions which are recorded in the log report:

S.No.	Operation Key	Operation Description
1	ACCEPT_AND_ARCHIVE_EMAIL	Accept and archive message
2	ACCEPT_BLACKLIST_REQUEST	Accept blacklist request
3	ACCEPT_BLACKLIST_REQUEST_PER_USER	Accept request blacklist sender for user
4	ACCEPT_EMAIL	Accept message
5	ACCEPT_RELEASE_REQUEST	Accept release request
6	ACCEPT_WHITELIST_REQUEST	Accept whitelist request
7	ACCEPT_WHITELIST_REQUEST_PER_USER	Accept request whitelist sender for user
8	ADD_GEOLOOKUP_RESTRICTION	Add geolookup restriction
9	ADMIN_ADD	Add admin
10	ADMIN_DELETE	Remove admin
11	ADMIN_EDIT	Edit admin settings
12	ADMIN_PASSWORD_UPDATE	Update password for admin
13	ADMIN_PERMISSIONS_ASSIGN_GROUP	Assign admin permission group by selection
14	ADMIN_PERMISSIONS_CHANGE_DEFAULT_GROUP	Change default admin permission group
15	ADMIN_PERMISSIONS_GROUP_ADD	Add admin permission group
16	ADMIN_PERMISSIONS_GROUP_DELETE	Remove admin permission group
17	ADMIN_PERMISSIONS_GROUP_UPDATE	Update admin permission group
18	ADMIN_REGENERATE_PASSWORD	Regenerate password for admin
19	ADMIN_UNLOCK	Unlock admin
20	ADMIN_VIEW_MESSAGE_CONTENT	Admin view message content

21	ARCHIVE_MESSAGE	Archive message
22	BLACKLIST_DOMAIN_RULE	Blacklist domain rule
23	BLACKLIST_RECIPIENT	Blacklist recipient
24	BLACKLIST_RECIPIENT_DOMAIN	Blacklist all recipients of the domain
25	BLACKLIST_REQUEST	Blacklist request
26	BLACKLIST_SENDER	Blacklist sender
27	BLACKLIST_SENDER_DOMAIN	Blacklist all senders of the domain
28	BLACKLIST_USER_SENDER	Blacklist sender for user
29	CANCEL_BLACKLIST_REQUEST	Cancel blacklist request
30	CANCEL_WHITELIST_REQUEST	Cancel whitelist request
31	CHANGE_FORWARD_SETTINGS_FOR_INCOMING_USER	Change forward settings for incoming user
32	DELETE_EMAIL_FROM_ARCHIVE	Delete archived message
33	DELETE_EMAIL_FROM_ARCHIVE_BY_FILTER	Delete archived messages by filter
34	DELETE_EMAIL_FROM_QUARANTINE	Delete quarantined message
35	DELETE_EMAIL_FROM_QUARANTINE_BY_FILTER	Delete quarantined messages by filter
36	DOMAIN_ADD	Add domain
37	DOMAIN_ALIASES_ADD	Add domain alias
38	DOMAIN_ALIASES_DELETE	Remove domain alias
39	DOMAIN_AUDIT_CONFIGURATION_CHANGE	Audit configuration change
40	DOMAIN_BLOCKED_EXTENSIONS_RESET_TO_DEFAULT	Reset blocked extensions to default
41	DOMAIN_BLOCKED_EXTENSIONS_UPDATE	Update blocked extensions
42	DOMAIN_DELETE	Remove domain
43	DOMAIN_DESTINATION_ROUTES_UPDATE	Update destination routes
44	DOMAIN_EMAIL_SIZE_RESTRICTION_CHANGE	Email size restriction change
45	DOMAIN_INCOMING_USER_ADD	Add incoming user
46	DOMAIN_INCOMING_USER_ALIASES_UPDATE	Update incoming user aliases
47	DOMAIN_INCOMING_USER_DELETE	Remove incoming user
48	DOMAIN_INCOMING_USER_EDIT	Edit incoming user
49	DOMAIN_INCOMING_USER_MOVE_ALIAS_TO_USER	Move alias to incoming user
50	DOMAIN_INCOMING_USER_MOVE_USER_TO_ALIAS	Move user to alias
51	DOMAIN_INCOMING_USER_PASSWORD_UPDATE	Update password for incoming user

52	DOMAIN_INCOMING_USER_REGENERATE_PASSWORD	Regenerate password for incoming user
53	DOMAIN_INCOMING_USER_UNLOCK	Unlock incoming user
54	DOMAIN_LDAP_CONFIGURATION_CHANGE	LDAP configuration change
55	DOMAIN_LOCAL_RECIPIENTS_ADD	Add local recipient
56	DOMAIN_LOCAL_RECIPIENTS_DELETE	Remove local recipient
57	DOMAIN_LOCAL_RECIPIENTS_STATE_CHANGE	Local recipients state change
58	DOMAIN_OUTGOING_USER_ADD	Add outgoing user
59	DOMAIN_OUTGOING_USER_DELETE	Remove outgoing user
60	DOMAIN_OUTGOING_USER_LOCK	Lock outgoing user
61	DOMAIN_OUTGOING_USER_PASSWORD_UPDATE	Update password for outgoing user
62	DOMAIN_OUTGOING_USER_SETTINGS_UPDATE	Edit outgoing user
63	DOMAIN_OUTGOING_USER_UNLOCK	Unlock outgoing user
64	DOMAIN_RELAY_RESTRICTIONS_ADD	Add relay restriction
65	DOMAIN_RELAY_RESTRICTIONS_DELETE	Remove relay restriction
66	DOMAIN_RELAY_RESTRICTIONS_STATE_CHANGE	Relay restriction state change
67	DOMAIN_RELAY_RESTRICTIONS_UPDATE	Update relay restriction
68	DOMAIN_REQUEST_CREATED	Domain request created
69	DOMAIN_SETTINGS_RESET_TO_DEFAULT	Reset domain settings to default
70	DOMAIN_SETTINGS_UPDATE	Update domain settings
71	DOMAIN_STATISTICS_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT	Domain report subscription reset to default
72	DOMAIN_STATISTICS_REPORT_SUBSCRIPTION_UPDATE	Domain report subscription update
73	DOMAIN_VALIDATED_BY_CODE	Domain validated by code
74	DOMAIN_VALIDATED_BY_MX	Domain validated by MX
75	DOMAIN_VALIDATED_CODE_REGENERATED	Domain validation code regenerated
76	EMAIL_QUARANTINE_ALERT	Email quarantine alert
77	ENABLE_GEOLOOKUP_RESTRICTIONS	Enable geolookup restrictions
78	ENABLE_USER	Enable user
79	FORWARD_BY_RULE_EMAIL	Forward by rule email
80	FORWARD_DOMAIN_RULE	Forward domain rule
81	FORWARD_EMAIL_LOOP_EXCEPTION	Forward email loop exception
82	FORWARD_TO	Forward to

83	FORWARDED_BY_RULE_EMAIL_IS_LOOPED	Forwarded by rule email is looped
84	IMPORT_INCOMING_USER	Import incoming user
85	LICENCE IS RETORED	Licence is restored
86	LICENCE_IS_EXPIRED	Licence is expired
87	MARK_EMAIL_AS_SPAM	Mark message as spam
88	MIGRATE_DOMAIN	Migrate domain
89	NON_HUMAN_EMAIL_TYPE	Non human email type
90	PUBLIC_EMAIL_TYPE	Public email type
91	QUARANTINE_EMAIL	Quarantine message
92	QUARANTINE_RELEASE_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT	Quarantine release report subscription reset to default
93	QUARANTINE_RELEASE_REPORT_SUBSCRIPTION_UPDATE	Quarantine release report subscription update
94	QUARANTINE_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT	Quarantine report subscription reset to default
95	QUARANTINE_REPORT_SUBSCRIPTION_UPDATE	Quarantine report subscription update
96	REJECT_BLACKLIST_REQUEST	Reject blacklist request
97	REJECT_BLACKLIST_REQUEST_PER_USER	Reject request blacklist sender for user
98	REJECT_RELEASE_REQUEST	Reject release request
99	REJECT_RELEASE_REQUEST	Reject release request
100	REJECT_WHITELIST_REQUEST	Reject whitelist request
101	REJECT_WHITELIST_REQUEST_PER_USER	Reject request whitelist sender for user
102	RELEASE_EMAIL_FROM_QUARANTINE	Release quarantined message
103	REMOVE_BLACKLIST_DOMAIN_RULE	Remove blacklist domain rule
104	REMOVE_DOMAIN_BY_VALIDATION_TIMEOUT	Remove domain by validation timeout
105	REMOVE_FORWARD_DOMAIN_RULE	Remove forward domain rule
106	REMOVE_GEOLOOKUP_RESTRICTION	Remove geolookup restriction
107	REMOVE_WHITELIST_DOMAIN_RULE	Remove whitelist domain rule
108	REPLY_ON_ARCHIVED_MESSAGE	Reply on archived message
109	REPORT_SPAM_BY_FILE	Report delivered message as spam
110	REPORTED_SPAM_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT	Reported Spam report subscription reset to default
111	REPORTED_SPAM_REPORT_SUBSCRIPTION_UPDATE	Reported Spam report subscription update
112	REPORTS_AS_SPAM	Reports archived message as a SPAM
113	RESEND_EMAIL_FROM_ARCHIVE	Resend archived message

114	RESET_SPAM_DETECTION_SETTINGS_TO_DEFAULT	Reset spam detection settings to default
115	RESET_SYSTEM_NOTIFICATIONS_TEMPLATE_TO_DEFAULT	Reset system notifications template to default
116	RESET_TO_DEFAULT_BLACKLISTED_RECIPIENTS	Reset recipients blacklist
117	RESET_TO_DEFAULT_BLACKLISTED_SENDERS	Reset senders blacklist
118	RESET_TO_DEFAULT_WHITELISTED_RECIPIENTS	Reset recipients whitelist
119	RESET_TO_DEFAULT_WHITELISTED_SENDERS	Reset senders whitelist
120	SEND_INVITATION_TO_USER	Send invitation to user
121	SPAM_DETECTION_SETTINGS	Update spam detection settings
122	SPAM_DETECTION_SETTINGS_RESET_TO_DEFAULT	Reset spam detection settings
123	SYSTEM_NOTIFICATIONS_TEMPLATE_CHANGE	System notifications template change
124	TLD_DOMAIN_RULE	TLD domain rule
125	UNBLACKLIST_RECIPIENT	Remove recipient from the blacklist
126	UNBLACKLIST_SENDER	Remove sender from the blacklist
127	UNBLACKLIST_USER_SENDER	Remove sender from the user blacklist
128	UNWHITELIST_RECIPIENT	Remove recipient from the whitelist
129	UNWHITELIST_SENDER	Remove sender from the whitelist
130	UNWHITELIST_USER_SENDER	Remove sender from the user whitelist
131	UPDATE_BLACKLIST_DOMAIN_RULE	Update blacklist domain rule
132	UPDATE_FORWARD_DOMAIN_RULE	Update forward domain rule
133	UPDATE_USERS_AUTO_IMPORT_SETTINGS	Update users auto-import settings
134	UPDATE_WHITELIST_DOMAIN_RULE	Update whitelist domain rule
135	USER_BLACKLIST_REQUEST_PER_USER	Request blacklist sender for user
136	USER_CANCEL_BLACKLIST_REQUEST_PER_USER	Cancel request blacklist sender for user
137	USER_CANCEL_RELEASE_REQUEST	Cancel release request
138	USER_CANCEL_WHITELIST_REQUEST_PER_USER	Cancel request whitelist sender for user
139	USER_PERMISSIONS_ASSIGN_GROUP	Assign user permission group by selection
140	USER_PERMISSIONS_CHANGE_DEFAULT_GROUP	Change default user permission group
141	USER_PERMISSIONS_GROUP_ADD	Add user permission group
142	USER_PERMISSIONS_GROUP_DELETE	Remove user permission group
143	USER_PERMISSIONS_GROUP_UPDATE	Update user permission group
144	USER_RELEASE_REQUEST	Release request

145	USER_WHITELIST_REQUEST_PER_USER	Request whitelist sender for user
146	USERS_AUTO-IMPORT_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT	Users auto-import report subscription reset to default
147	USERS_AUTO-IMPORT_REPORT_SUBSCRIPTION_UPDATE	Users auto-import report subscription update
148	WHITELIST_DOMAIN_RULE	Whitelist domain rule
149	WHITELIST_RECIPIENT	Whitelist recipient
150	WHITELIST_RECIPIENT_DOMAIN	Whitelist all recipients of the domain
151	WHITELIST_REQUEST	Whitelist request
152	WHITELIST_SENDER	Whitelist sender
153	WHITELIST_SENDER_DOMAIN	Whitelist all senders of the domain
154	WHITELIST_USER_SENDER	Whitelist sender for user

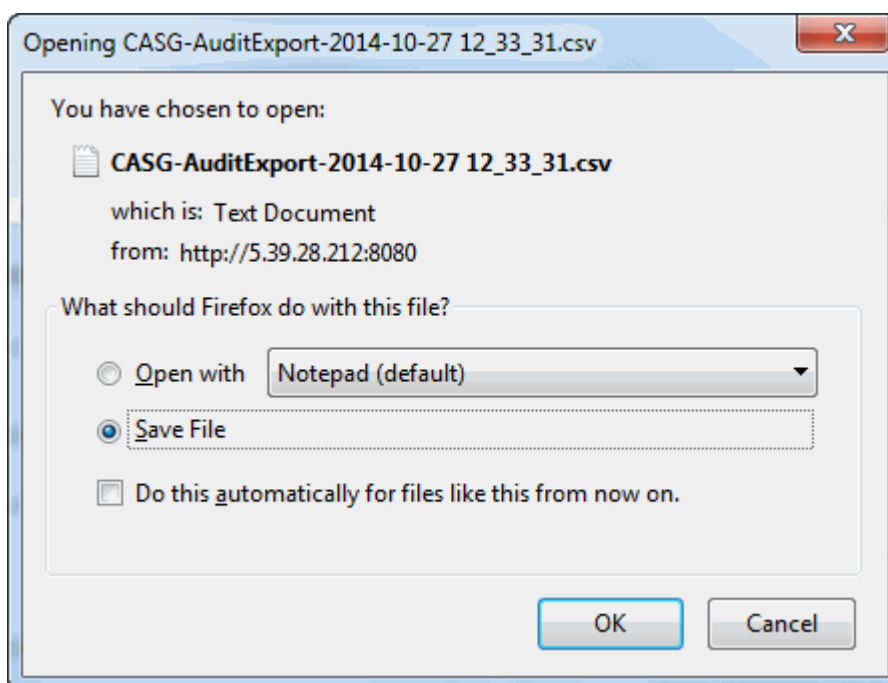
Export Log Report to CSV

The log report can be exported to a comma separated value (CSV) file and is limited to 10,000 entries per file. You will see an error if the entries exceed this value. The exported file sorts entries in the same order as they are sorted in the interface.

- Click the 'Export to CSV by filter' button.

The screenshot shows the 'Audit log' section of the Comodo Antispam Gateway interface. At the top, there is a breadcrumb 'Dashboard / Audit log'. Below it, the title 'Audit log' is displayed. A button labeled 'Export to CSV by filter' with a CSV icon is circled in red. Below the button is a 'Filters' section with a right-pointing arrow. Underneath is a table with columns: 'Date (GMT +0)', 'Domain', 'Role', 'Login', 'Operation key', and 'Opera'. The first row of data shows: '2014-04-7 12:02:13', 'csg-arch-qa.comodo.od.ua', 'superadmin', and 'DELETE, BANN, P...'. The rest of the table is partially obscured.

The 'File Download' dialog will be displayed.

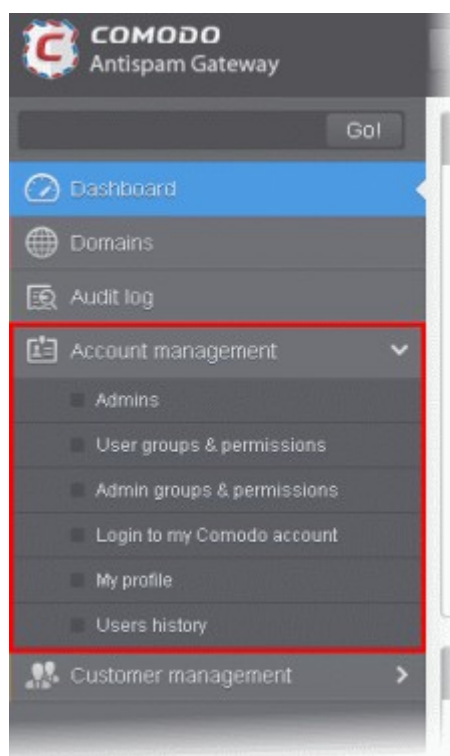


- Choose 'Open with' or 'Save File' to view / save the file with an appropriate application to your computer
- Click 'OK'

The values in the log report will be separated by commas and this file can be opened with Excel or Openoffice Calc for easy analysis.

8 Administrator Account Management

- The 'Account Management' area lets an admin with appropriate privileges add new admins for the same account.
- This area also allows you configure user permissions, reset passwords, and change login status.
- Admins who logged-in with CAM credentials will have an additional icon, 'Login to my Comodo account'.
- The items an admin sees in this area depends on their configured permissions. See '[Admin Groups & Permissions](#)' for help with this.



Click the following links for more details:

- [Manage Administrators](#)
- [User Groups & Permissions](#)
- [Admin Groups & Permissions](#)
- [Manage Comodo Account](#)
- [My Profile](#)
- [Users History](#)

8.1 Administrators

Click 'Account Management' > 'Admins'

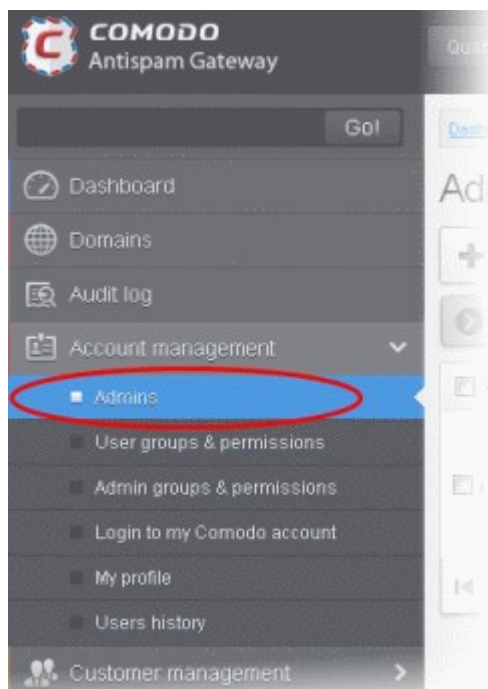
This area lets admins add or remove fellow administrators, specify their permissions and reset their passwords.

Click the following links for more:

- [Manage admins](#)
- [Add an admin](#)
- [Delete an admin](#)
- [Edit an admin](#)
- [Manage admin permissions](#)

Manage admins

- Click 'Account management' on the left and choose 'Admins'.



The admins interface shows a list of administrators, their last login time, the group to which they belong, and the domains that they can manage.

Dashboard / Admins

Admins

[+ Add](#)
[Delete](#)
[Edit](#)
[Manage permissions](#)
[Refresh](#)

Filters

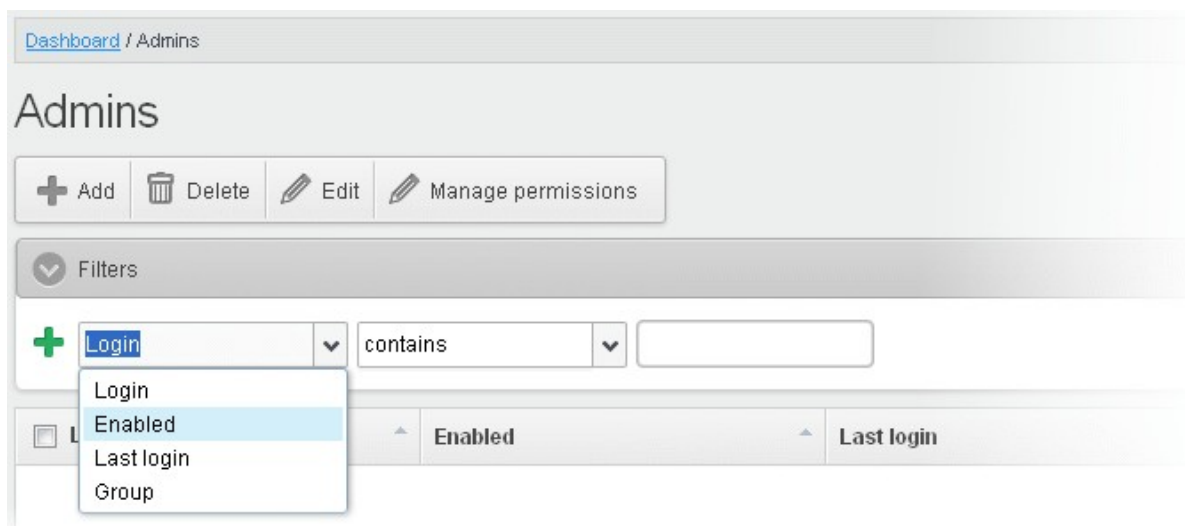
Login	Enabled	Last login	Group	Target
john@docteamcsg.comodo.od.ua	true	Apr 16, 2014 4:13:58 AM	Power Administrators	[docteamcsg.comodo.od.ua, testdomain.com, csg-arch-qa.comodo.od.ua, example.domain.com, example1.domain.com]

1 / 1 [1 - 1 / 1] Per page 15

- Click the up/down arrows in the respective column headers to sort the entries in ascending or descending order based on the login, enabled status or last login time

Use the filter option to search administrators

- Click anywhere on the 'Filters' to open the filters area.




- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

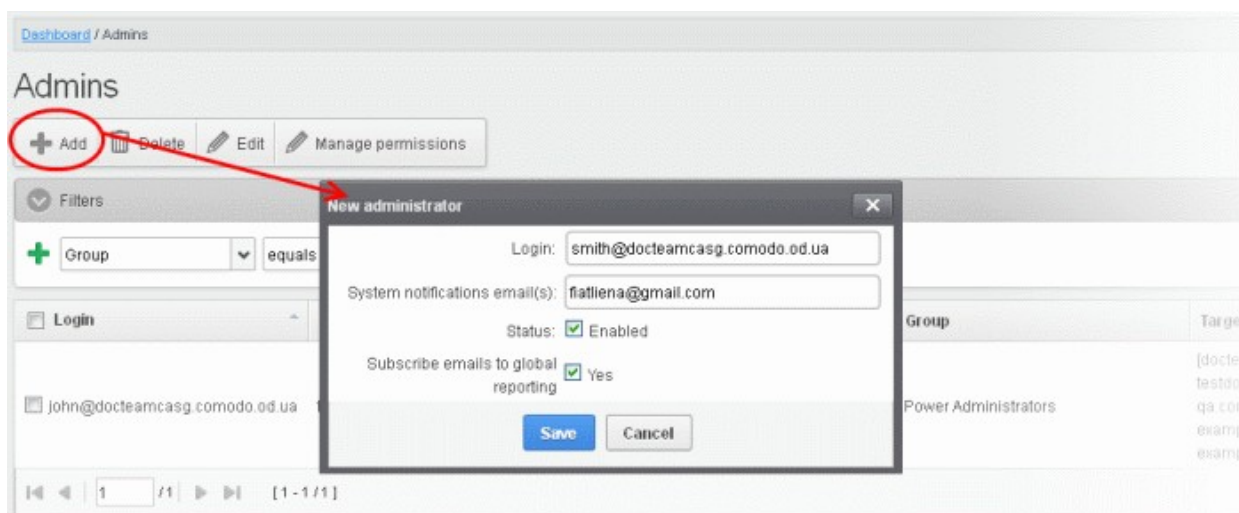
- **Login:** Type an admin login details in the text box (column 3) and select a condition in column 2.
- **Enabled:** Sorts the results based on administrators' enabled / disabled status.
- **Last Login:** Select a date in the calendar (column 3) and the condition in column 2.
- **Group:** Select an admin group in the last drop-down (column 3) and the condition in column 2.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

You can add multiple filters to the same search by clicking .

Add a new administrator

- Click the Add button.



The 'New administrator' dialog will be displayed.

- **Login** - Enter the new administrator's valid email address as login username.

- **System notifications email(s)** - Enter the email addresses at which the new administrator should receive CASG notification emails. It can be the same email address as the login name if required. You can add up to five alternative email addresses for the person. Quarantine requests and notifications are sent to the addresses specified in this field. See **Email Management** for more details.
- **Status** - Enables to change the login status of the new administrator. By default, this box is selected, that is, the new administrator can access CASG interface.
- **Subscribe emails to global reporting** - Send domain and quarantine reports to the admin at the email address used for the their username. See **CASG Reports - an Overview** for more details.
- Click the 'Save' button.

The administrator is added to the list and placed in the default group. You can modify their permissions if required (see **Manage Admin Permissions** for more). CASG will send the new admin a registration mail containing their login details. The password can be reset in the **edit interface**.

Dashboard / Admins

Admins

Filters

<input type="checkbox"/> Login	Enabled	Last login	Group	Target
<input type="checkbox"/> john@docteamcasg.comodo.od.ua	true	Apr 16, 2014 5:43:33 AM	Power Administrators	[docteamcasg.comodo.od.ua, testdomain.com, csg-arch-qa.comodo.od.ua, example.domain.com, example1.domain.com]
<input type="checkbox"/> smith@docteamcasg.comodo.od.ua	true		Power Administrators	[docteamcasg.comodo.od.ua, testdomain.com, csg-arch-qa.comodo.od.ua, example.domain.com, example1.domain.com]

/ 1 Per page 15

Delete an administrator

- Select the administrator to be removed and click 'Delete'.

Dashboard / Admins

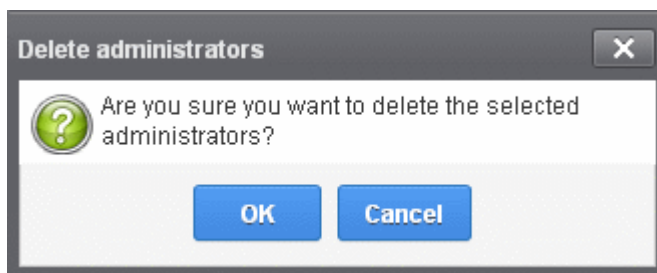
Admins

Filters

<input type="checkbox"/> Login	Enabled	Last login	Group	Target
<input checked="" type="checkbox"/> bob@casg.comodo.od.ua	true		HR	[docteamcasg.comodo.od.ua]
<input type="checkbox"/> john@docteamcasg.comodo.od.ua	true	Apr 16, 2014 6:30:50 AM	Power Administrators	[docteamcasg.comodo.od.ua, testdomain.com, csg-arch-qa.comodo.od.ua, example.domain.com, example1.domain.com]
<input checked="" type="checkbox"/> smith@docteamcasg.comodo.od.ua	true		Power Administrators	[docteamcasg.comodo.od.ua, testdomain.com, csg-arch-qa.comodo.od.ua, example.domain.com, example1.domain.com]

/ 1 Per page 15

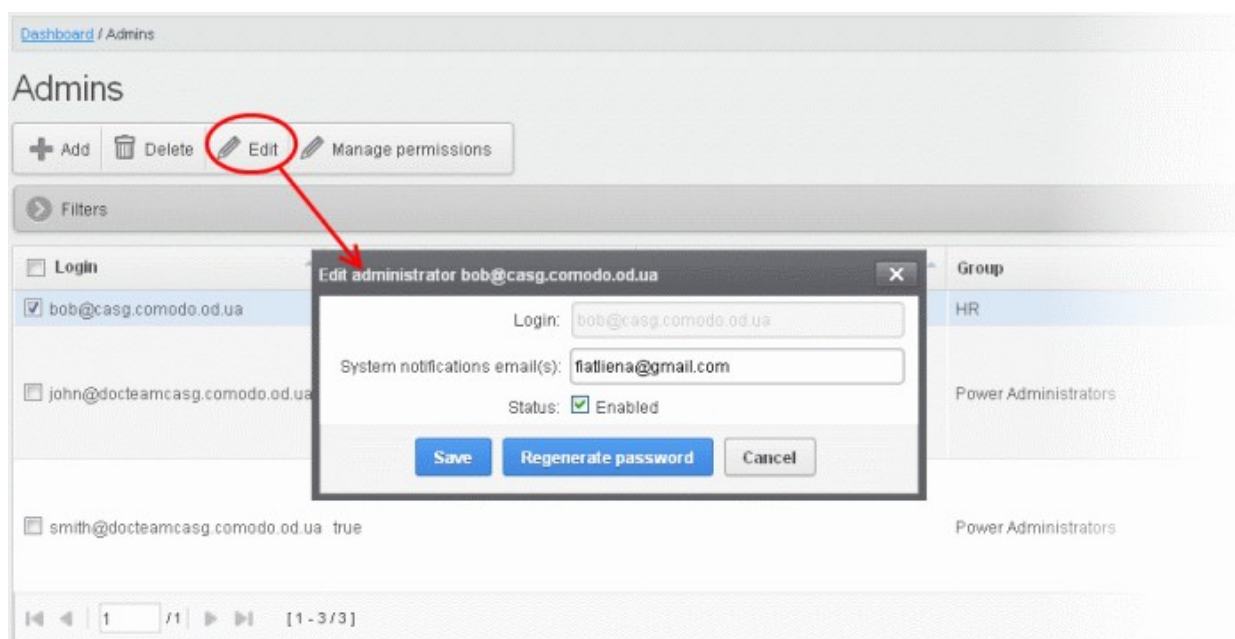
A confirm dialog is shown as follows:



- Click 'OK' to confirm the deletion.

Edit an administrator

- Select the administrator you want to edit from the list and click the 'Edit' button.



The 'Edit administrator' dialog box will be displayed.

- **System notifications email(s)** - Enter the email addresses at which the new administrator should receive CASG notification emails. It can be the same email address as the login name if required. You can add up to five alternative email addresses for the person. Quarantine requests and notifications are sent to the addresses specified in this field. See [Email Management](#) for more details.

Tip: The currently logged-in administrator can configure the Quarantine notification email address in Dashboard > Account Management > [My Profile](#) dialog.

- **Status** - Enable or disable the admin.
- **Regenerate password** - Reset the password for the administrator in case it is forgotten. The new password is sent to the administrator's email automatically. The administrator has to use this new password to access CASG
- Click the 'Save' button to confirm your changes.

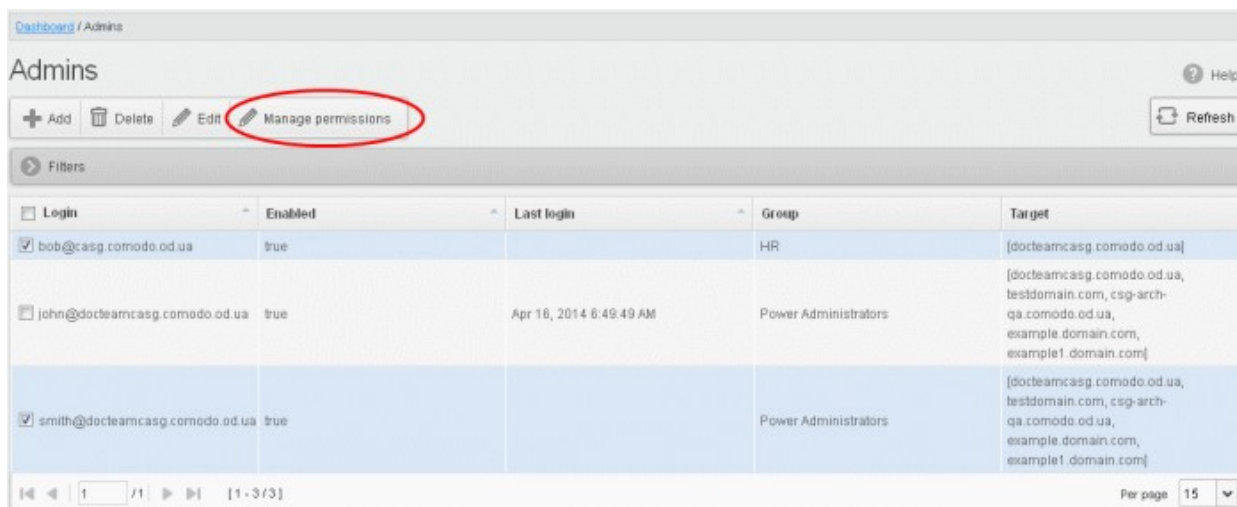
Manage admin permissions

CASG allow administrators with appropriate privileges to assign permissions for other administrators that will determine what he/she can do and cannot do while logged into their respective CASG admin interface. The administrators can create policies and assign them to other administrators from this interface. See [Admin Groups &](#)

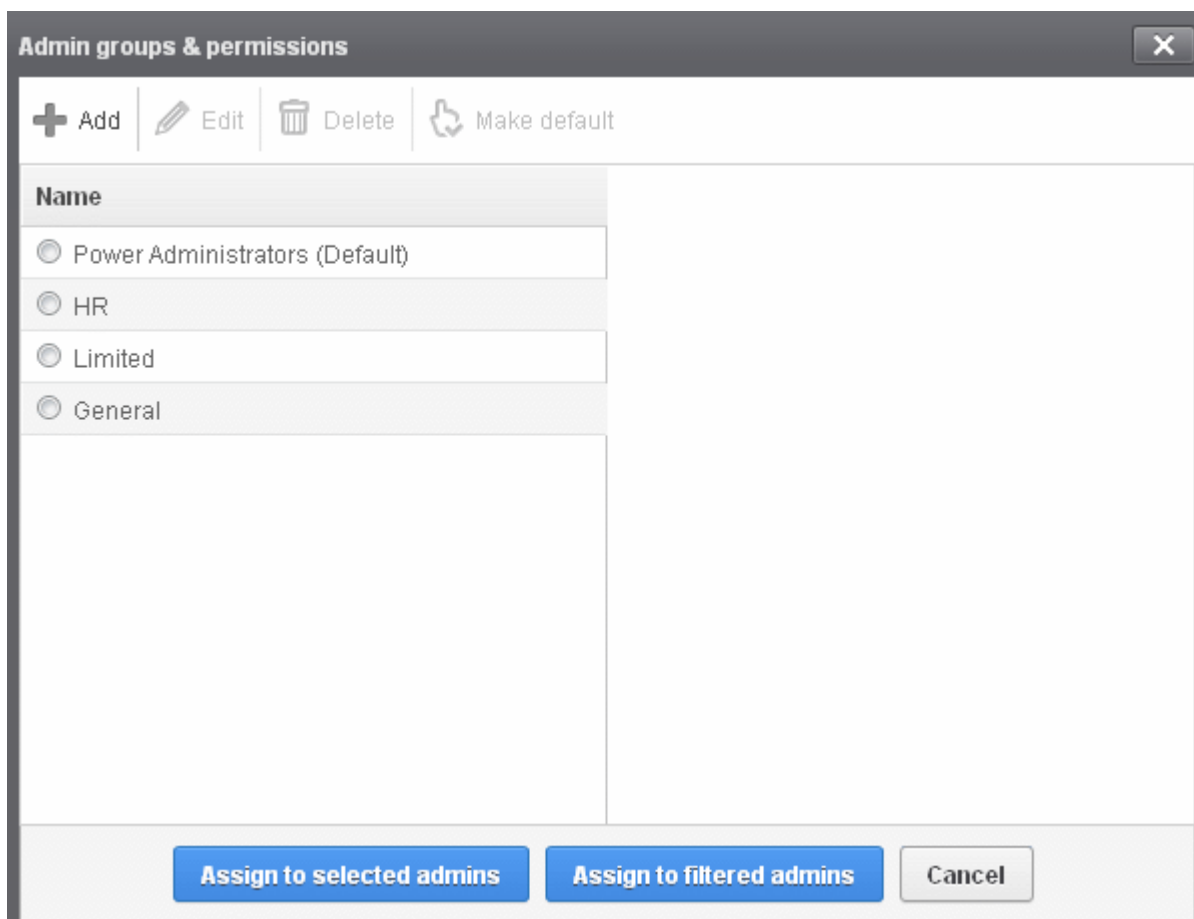
Permissions for more details on how to create groups and policies for administrators. A new administrator will be automatically assigned default permission settings.

To assign permissions for an administrator

- Select the administrator or multiple administrators that you want assign permissions and click the 'Manage permissions' button.



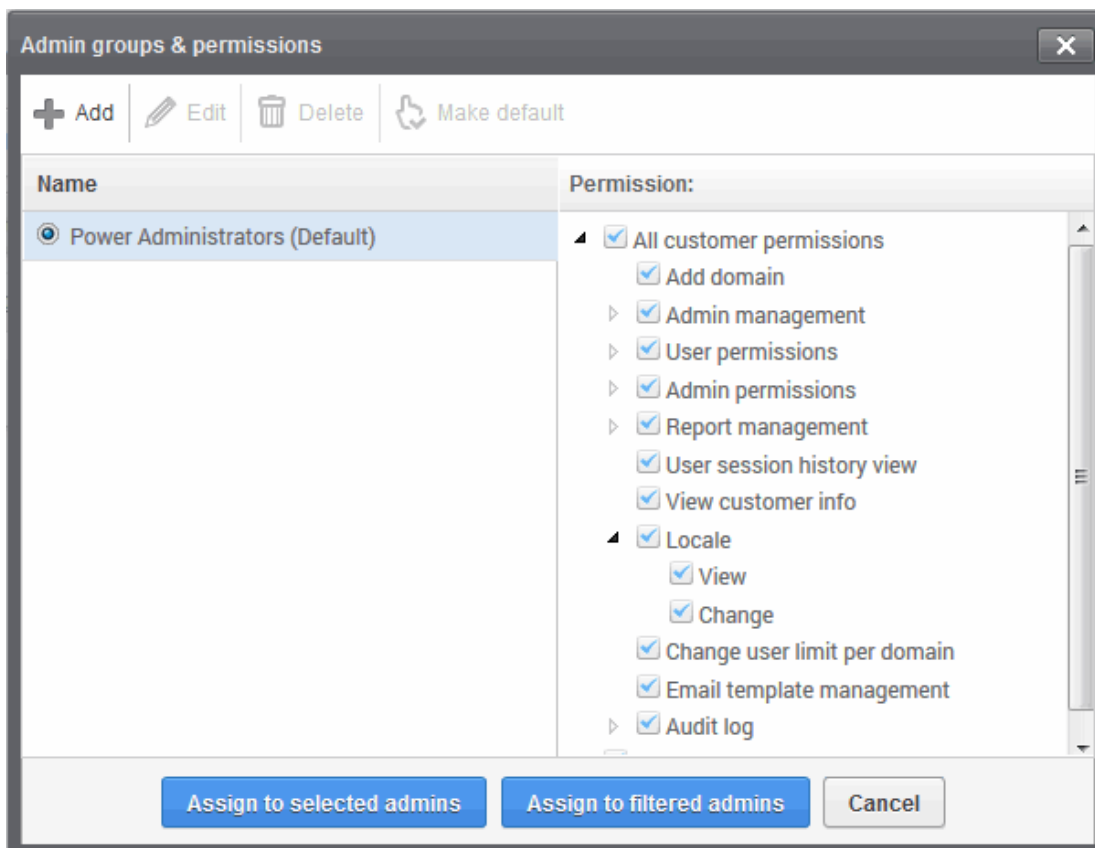
The 'Admin Groups & Permissions' interface will appear.



The interface displays the list of groups available with same or different permission levels for each group. By default, 'Power Administrators (Default) group will be available and administrators can add, edit groups and assign permissions to other administrators. See the section '**Admin Groups & Permissions**' for more details.

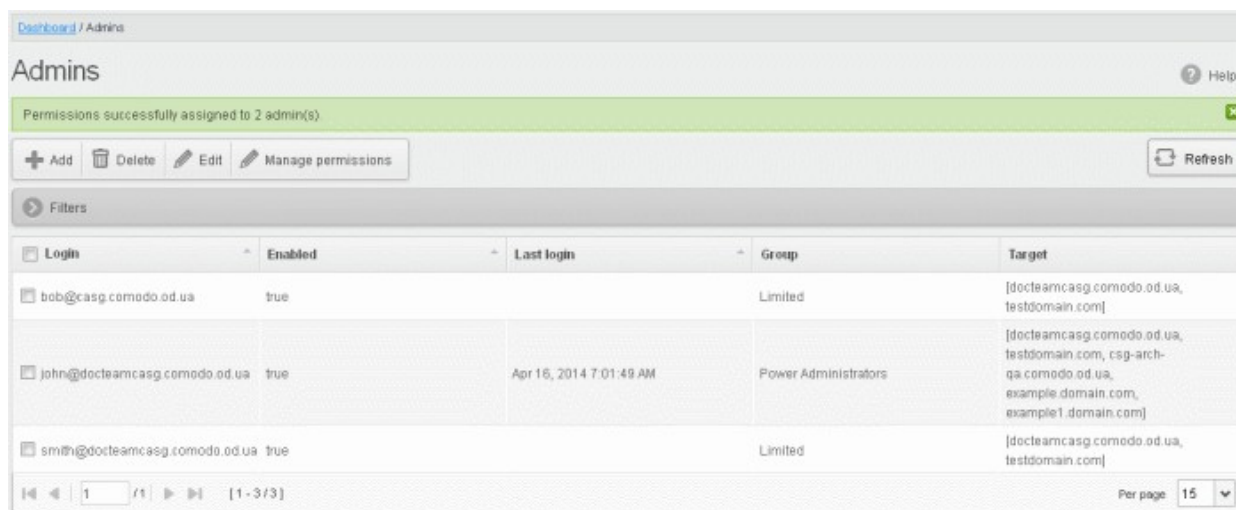
- Select the group from the list.

The permissions set for this group will be displayed on the right side.



- The permissions set for this group will be displayed on the right side.
- Click the 'Assign to selected admins' button to set permissions for selected admin(s).
- Click 'Assign to filtered admins' button to set permissions for administrators found by filter.
- Click 'OK' in the confirmation dialog.

The selected admin(s) will be added to the group and a confirmation message will be displayed.



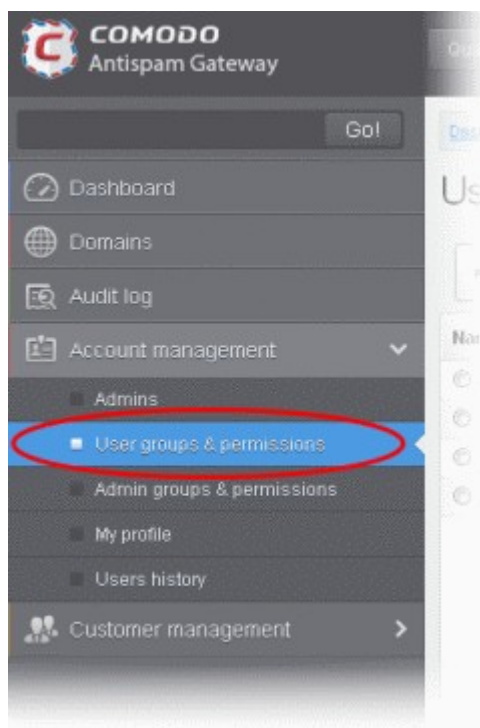
The interface also displays the new group assigned for the selected admin(s) under the 'Group' column.

8.2 User Groups & Permissions

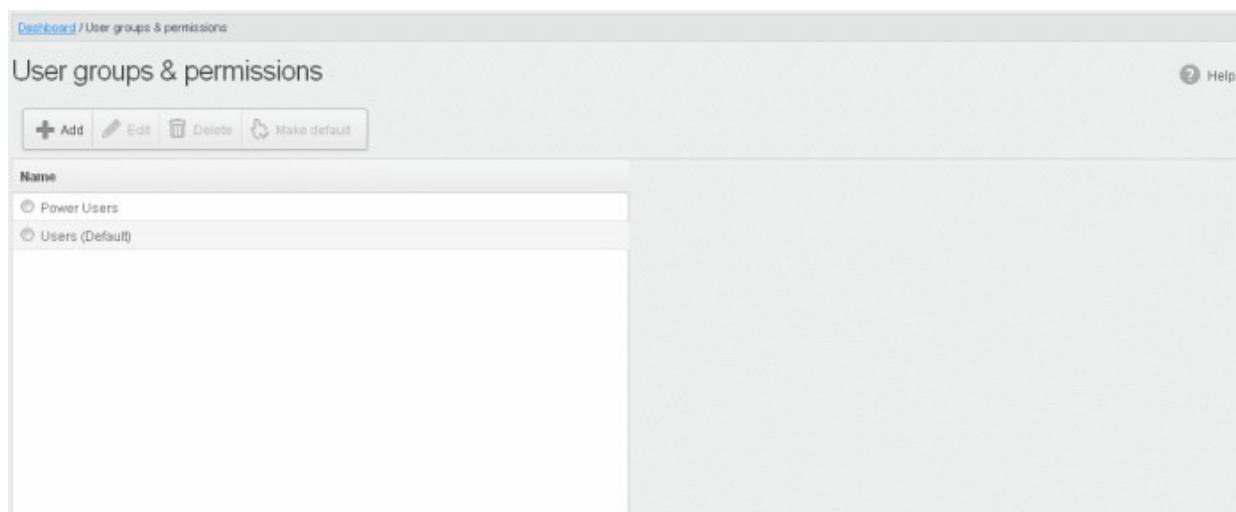
- The 'User Groups & Permissions' area lets you create email user groups and set group permissions.
- You can create multiple groups, each with different permission levels. When you assign users to a group they will inherit the permissions of the group.
- The user interface will vary according to a user's permission level. See '[Manage Permissions for Users](#)' in '[User Account Management](#)' for help with this.

Create user groups

- Click 'Account management' > 'User groups & permissions':

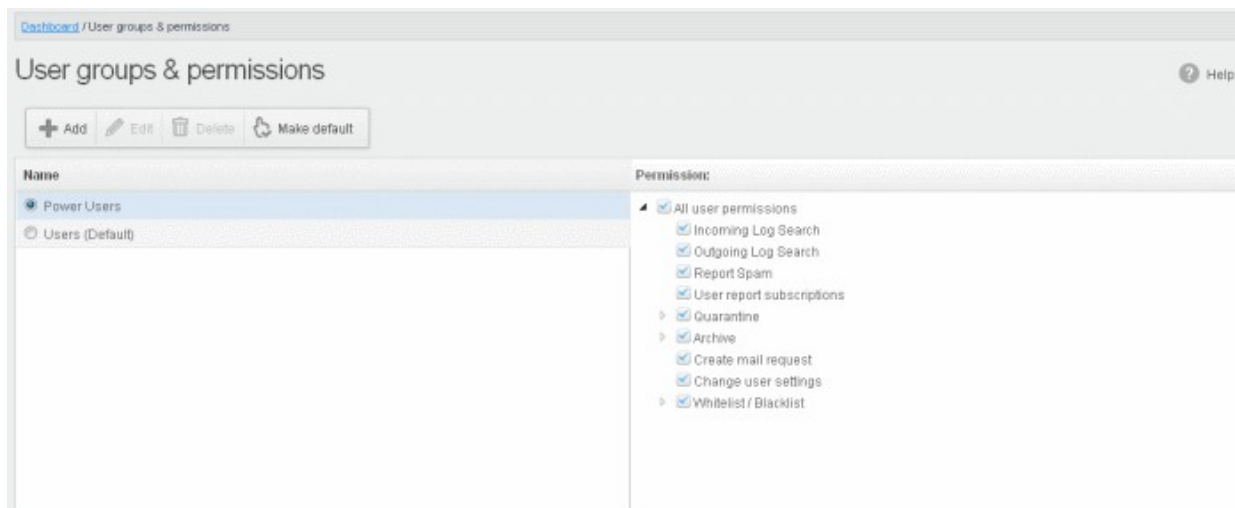


The 'User Groups & permissions' interface will be displayed.

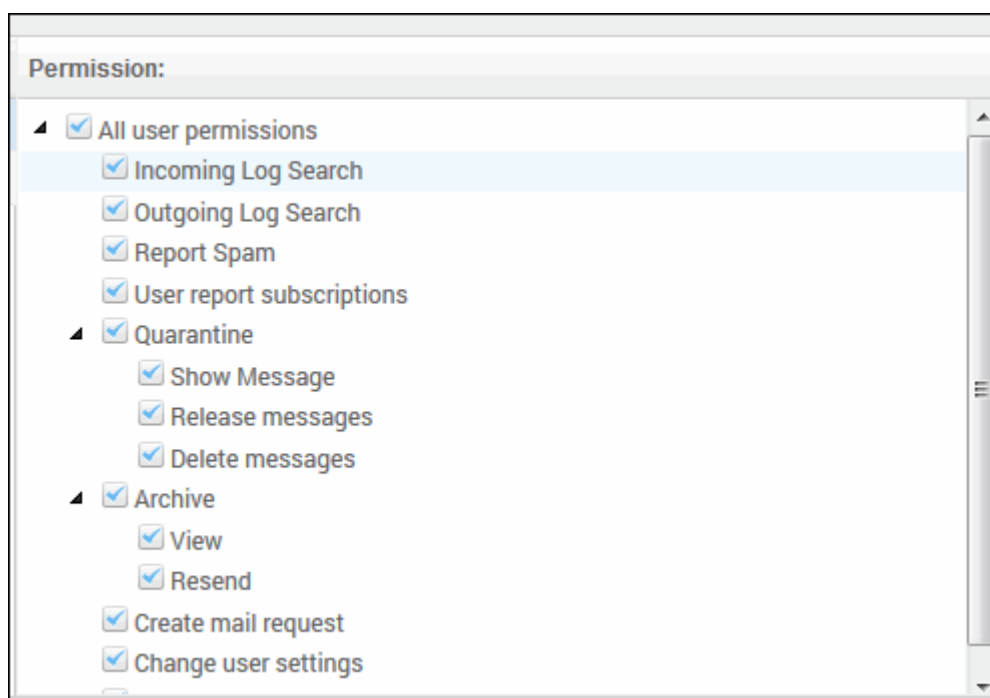


Two user groups, Power User and Users (Default), are available by default. These two groups cannot be edited or deleted.

- Click a group name to view its permissions in the right-hand pane:



- Click the arrow next to a permission to view sub-permissions:



For users in the 'Power User' group, all permission levels are enabled. The 'Release quarantine messages' option is not available to users in the regular 'Users' group. This means that if a user is assigned to the 'Power User' group, he / she can release quarantined messages from the quarantined mails list without approval from an admin. See [Released Requests](#) in '[Email Management](#)' for more details.

Permission Levels

- **Incoming Log Search** - Allows a user to search and view the log of all incoming mails.
- **Outgoing Log Search** - Allows a user to search and view the log of all outgoing mails.
- **Report Spam** - Allows a user to report a mail as spam mail.
- **User report subscriptions** - Allows a user to configure periodical quarantine report generation.
- **Quarantine**
 - **Show Message** - Allows a user to view quarantined emails in same window or separate window.
 - **Release messages** - Allows a user to release a quarantined mail without approval from the administrator.

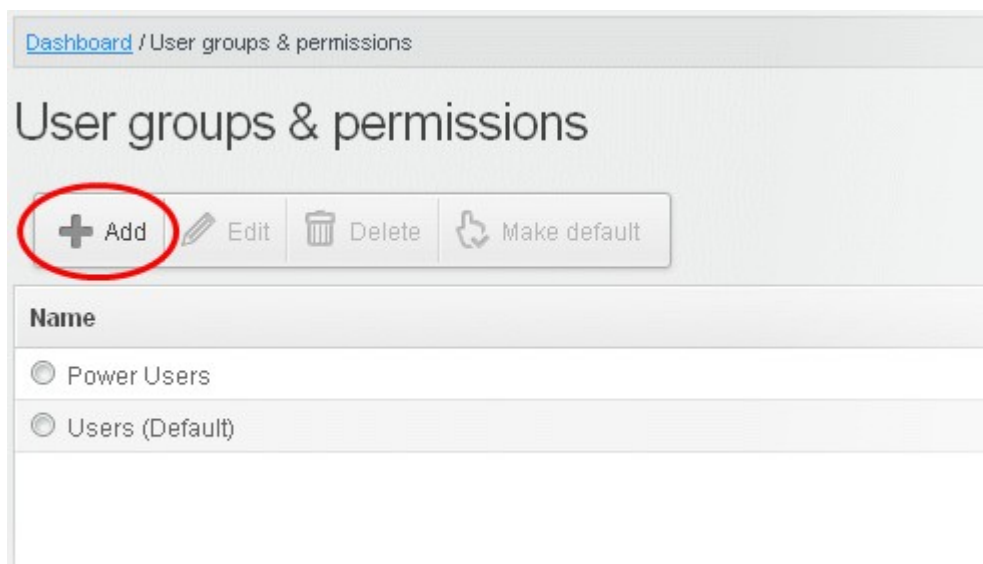
- **Delete messages** - Allows a user to delete a quarantined mail without approval from the administrator.
- **Archive**
 - **View** - Allows a user to view archived emails in same window or separate window.
 - **Resend** - Allows a user to resend archived emails to himself / herself.
 - **Reply all** - Allows a user to reply to all archive emails
 - **Forward** - Allows a user to forward an archive email composed earlier
- **Create mail request** - Allows a user to configure email request for CASG notifications.
- **Change user settings** - Allows a user to configure himself / herself as recipient whitelist.
- **Whitelist / Blacklist**
 - **Manage whitelist senders per user** - Allows a user to manage sender whitelist for his / her mail account
 - **Manage blacklist sender per user** - Allows a user to manage sender blacklist for his / her mail account

Click the following links for more details.

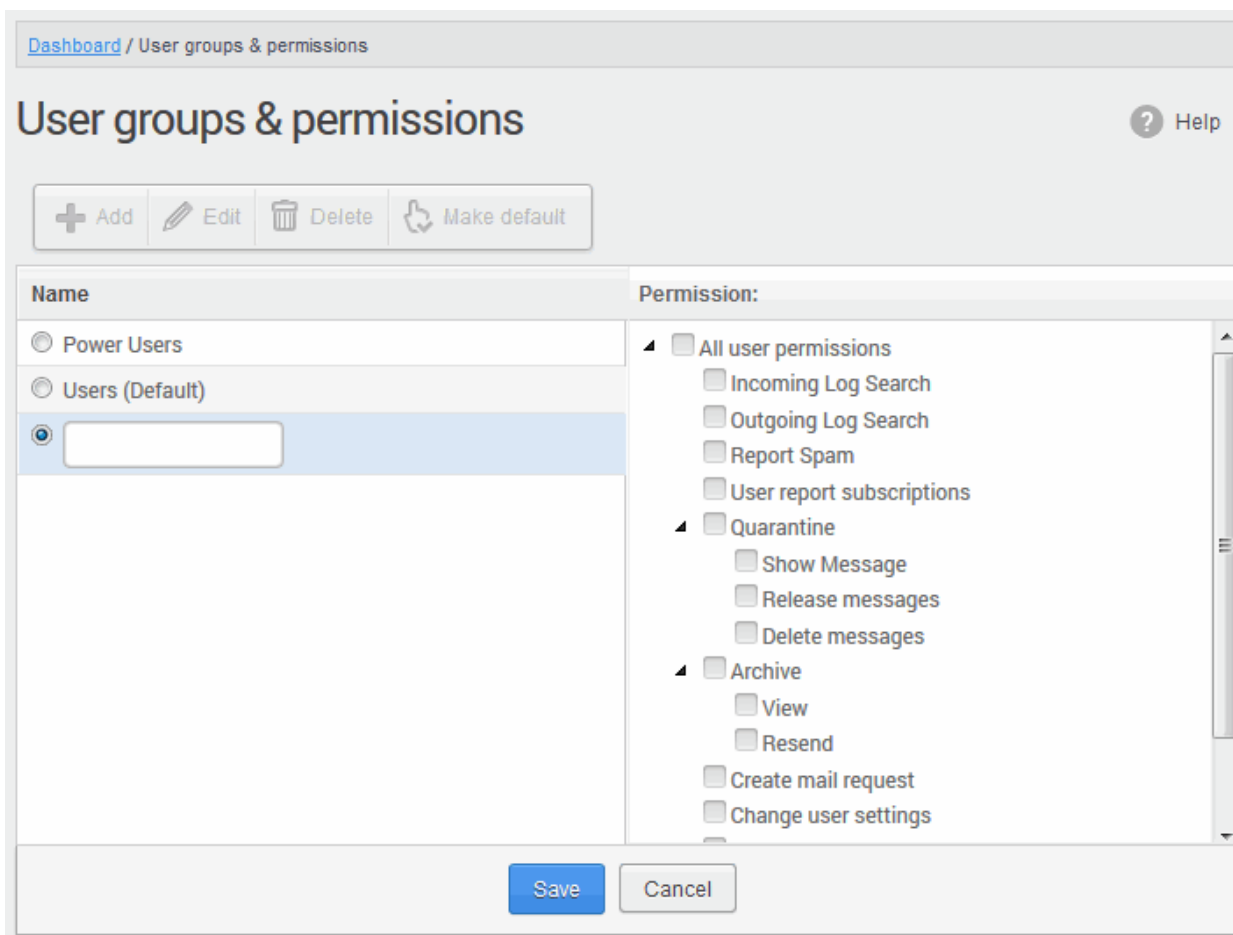
- [Add a new group](#)
- [Edit a group](#)
- [Delete a group](#)
- [Make a group as default](#)

Add a New Group

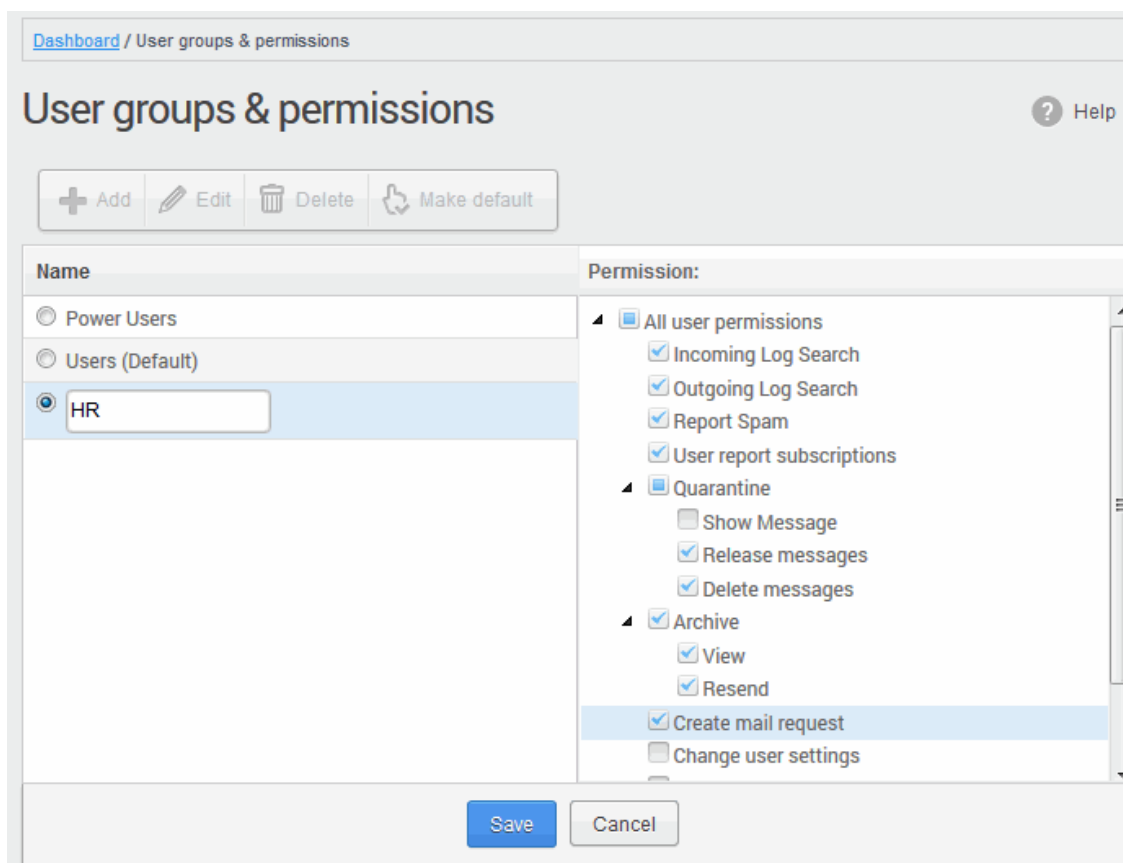
- To add a new group and configure permission levels, click the 'Add' button.



A new group creating page will be displayed.

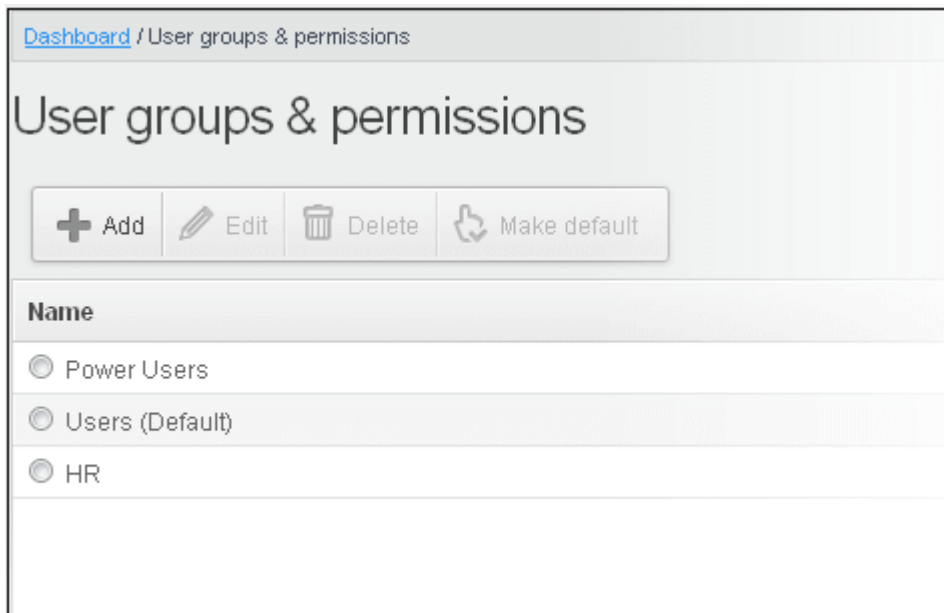


- Enter the name of the group in the text field under the 'Name' column. Note: To enable the permission levels in the right side for that group, click the 'Edit' button on the top.



- Click the 'Save' button.

The newly created group will be displayed in the interface.

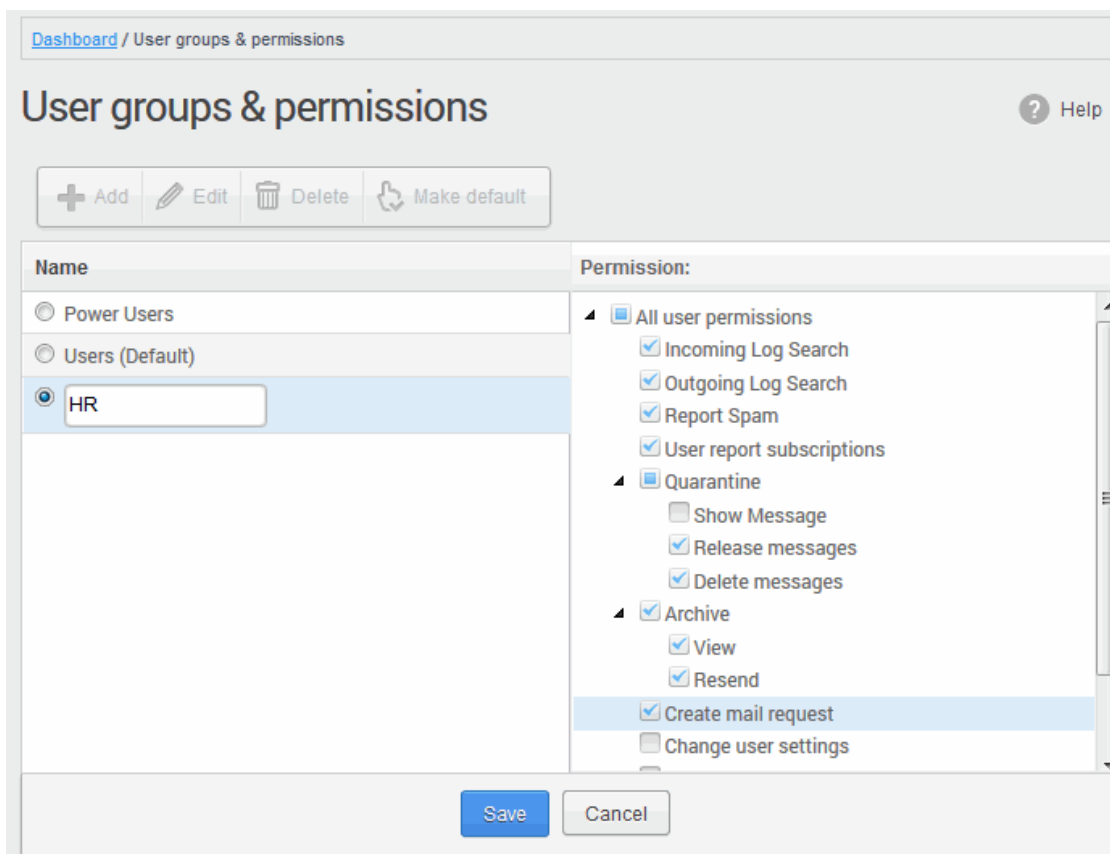


Now, users of domains belonging to the account can be assigned to this newly created group. See the section **'Managing Permissions for Users'** in **'User Account Management'** on how to add users to predefined groups.

Edit a group

You can edit the name of an existing group and / or change the permission levels.

- Select the group from the list and click the 'Edit' button.

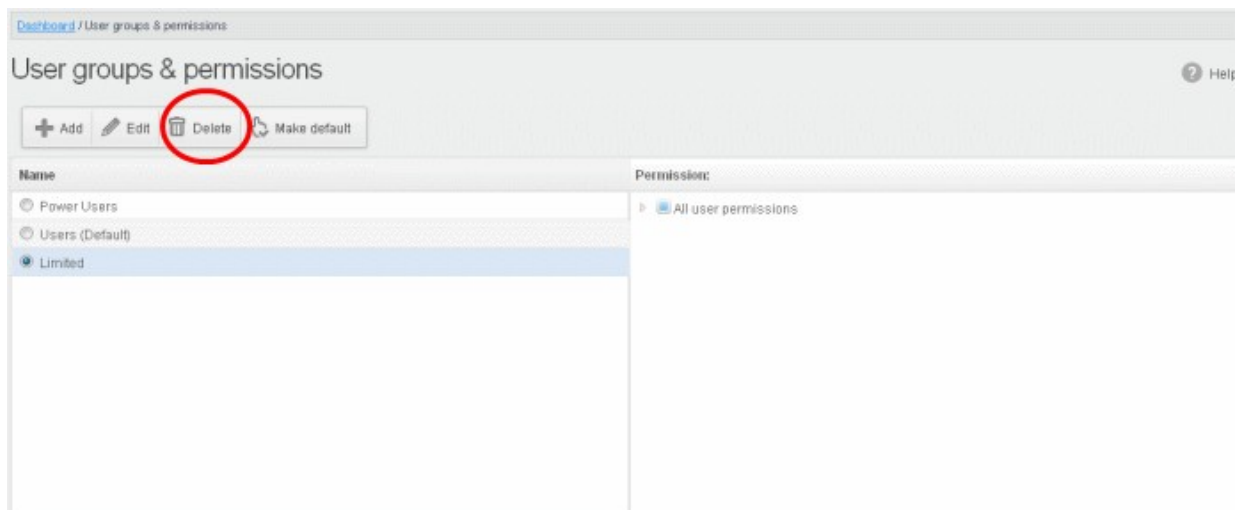


- Change the permission levels and / or the name of the group.
- Click the 'Save' button for the changes to take effect.

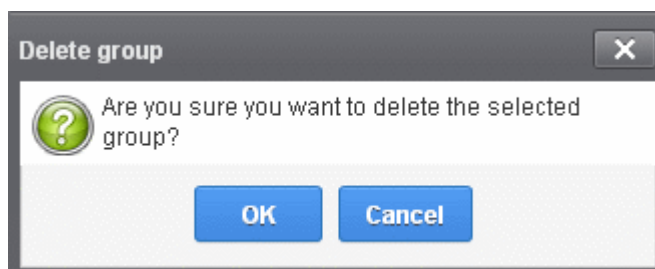
The users in the group that is edited will be automatically reassigned to the edited group.

Delete a Group

- Select a group from the list and click 'Delete'.



- Click 'OK' in the confirmation dialog.



The selected group will be deleted from the list.

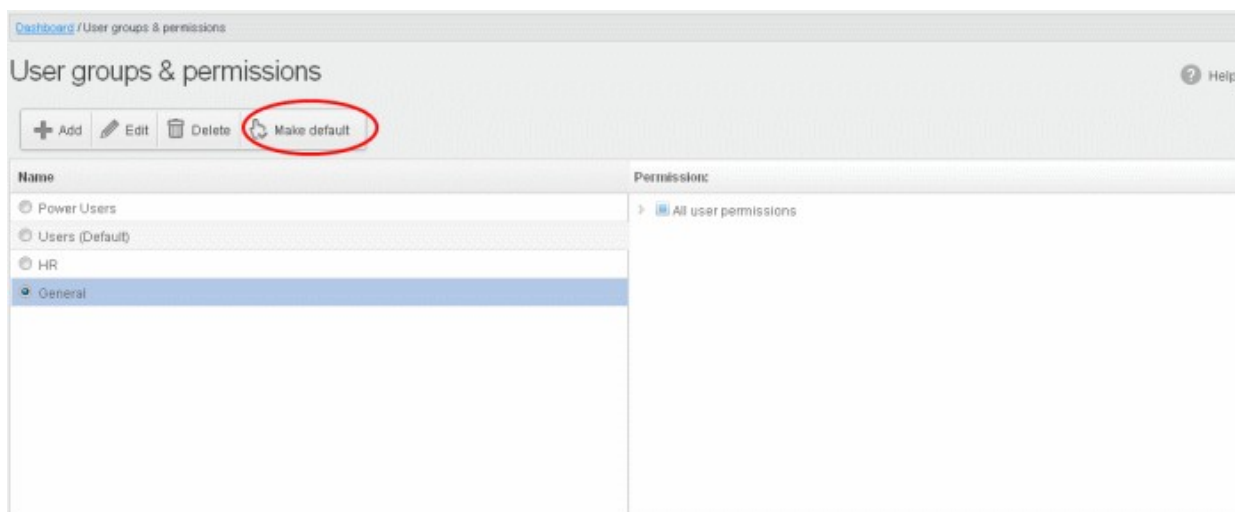
Note 1: If you delete a group, users assigned to that group will be automatically moved to default group. You have to reassign the users if required.

Note 2: If you delete a user group created by the administrator and marked as default, then the 'Users' group that was shipped with the product will be set as default. All the users from the deleted group will be automatically migrated to the 'Users' group.

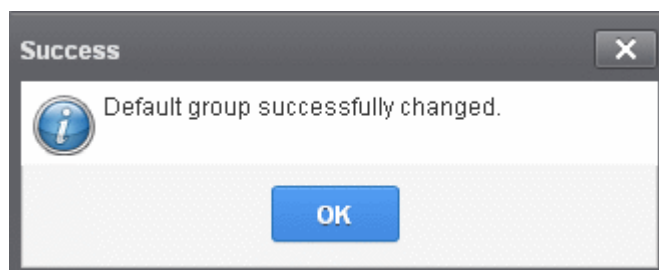
Make a Group as Default

CASG allows administrators to make an existing group as default group. Newly added users and users belonging to an existing group whose name was deleted will be automatically moved to this default group.

- Select a group from the list and click 'Make default'.

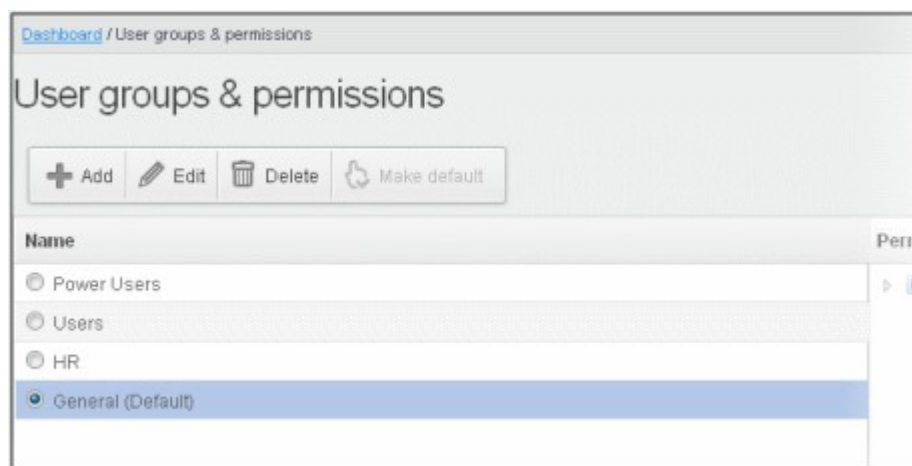


A success dialog will be displayed.



- Click 'OK'.

The selected group will be displayed as default group.



Note: If you delete a user group created by the administrator and marked as default, then the 'Users' group that was shipped with the product will be set as default. All the users from the deleted group will be automatically migrated to the 'Users' group.

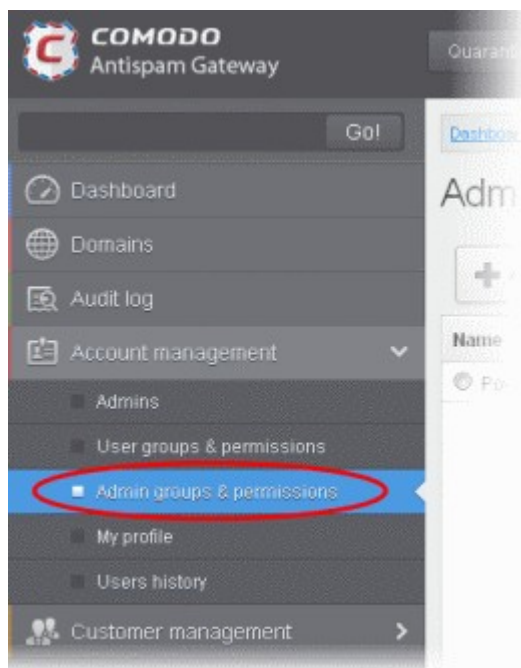
8.3 Admin Groups & Permissions

- Click 'Account management' > 'Admin groups & permissions'
- The 'Admin Groups & Permissions' area lets you create and set the privileges of admin user groups. Any users you place in an admin group will inherit the privileges of the group.

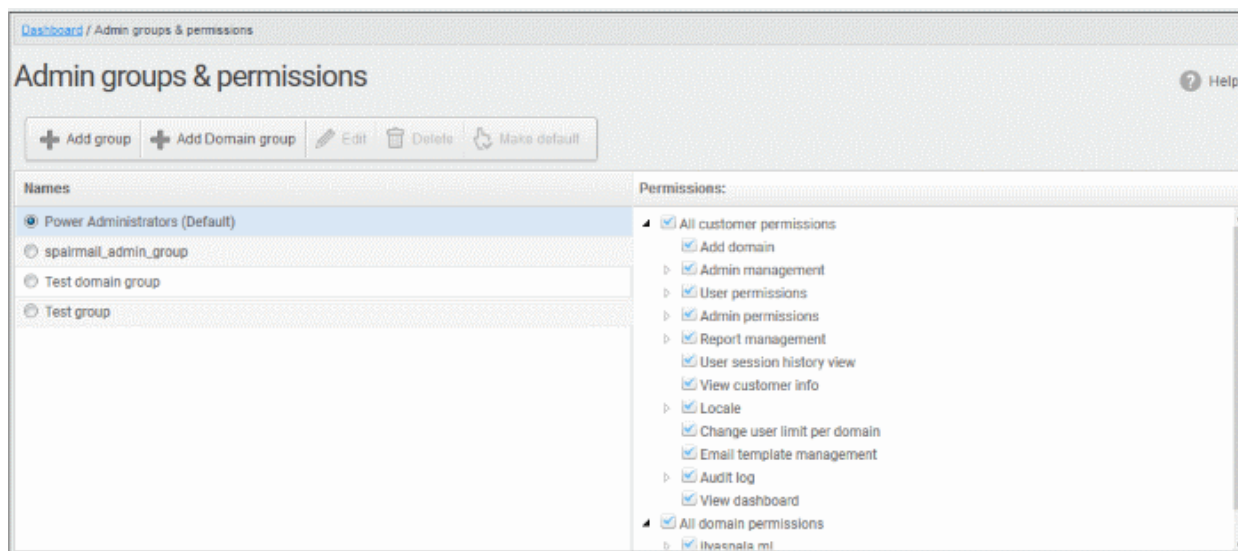
- There are two sets of permissions:
 - Customer permissions are high-level admin privileges which cover all domains on the account. For example, add domains, configure user permissions, modify email templates, view customer info, manage admins, generate reports, etc.
 - Domain permissions are technical privileges to configure and manage antispam on specific domains. For example, setup recipients, configure the delivery queue, configure whitelists and blacklists, etc.
- You can create multiple admin groups, each with different permission levels. Admin groups save time by avoiding the need to set permissions for every new administrator.
- There are two types of group you can add:
 - **Add Group** - Creates a 'blank' group with no permissions set. You add all permissions that you require.
 - **Add Domain group** - Creates a group with sufficient permissions enabled to manage a domain. This is just a time-saving feature which avoids the need to select permissions from scratch.
 - The 'Customer Permissions' tree on the right shows all privileges which are enabled by default
 - You can enable or disable these permissions as required in your custom domain group
 - Open the 'All Domain Permissions' tree to choose the domains over which group members have control. You can set permissions on a per-domain basis in here.
- The items available in the console will vary according to the permissions of the admin. See '**Manage Permissions for Administrators**' for help to add admins to predefined groups.

Create admin groups

- Click 'Account management' > 'Admin groups & permissions'



The admin groups & permissions interface is displayed.



By default, power administrators group is available. Power administrators have all customer and domain permissions enabled. You cannot edit or delete this default group.

- Tick a group from the right side to view the permission levels assigned for it.
- Click on the arrow beside a permission to display the tree structure of second level of permissions, if available.

For administrators in the 'Power Administrators' group, all permission levels will be enabled. The 'Permission' level is divided into two categories, 'All customer permissions' and 'All domain permissions'.

Customer permissions and domain permissions are two different settings. Customer permissions deals with configuring general privilege levels for the admin group. Domain permissions relates to what the admin can do in the domain(s).

- **Customer permissions** – Determines general privileges for the administrator. For example the admin can add domains, configure admin and user permissions and so on.
- **Domain permissions** – This pertains to domain level privileges. Determines what domains the admins can manage, for example, remove the domain, manage incoming and outgoing user for the domain and so on.
 - See the full list of privilege levels below.
- 'Add Domain group' allows you to create groups for domain management with predefined customer permissions. Though you can create domain management groups using 'Add group' also, this feature is useful if you want to create a large number of domain groups.

Permission Levels

- **All customer permissions** - View and manage all customer related tasks.
 - Add domain - Add new domain(s)
 - Admin management - View and manage administrators for the account.
 - View - Only view the list of administrators.
 - Unlock - Unlock previously blocked administrators.
 - Manage - Manage administrators for the account.
 - User permissions - View and manage 'User Groups & Permissions'
 - View - Only view 'User Groups & Permissions'.
 - Manage - Manage 'User Groups & Permissions'
 - Admin permissions - View and manage 'Admin Groups & Permissions'
 - View - Only view 'Admin Groups & Permissions'
 - Manage - Manage 'Admin Groups & Permissions'
 - Report management - View and manage report subscriptions

- View - Only view report subscriptions
- Change - View and manage report subscriptions
- User session history view - View user sessions history for all domains in the account.
- View customer info - View information about the customer.
- Locale - View and manage message locale set for a user
 - View - Only view message locale
 - Change - View and manage the messages locale
- Change user limit per domain - Configure the number of users for each domain in the account.
- Email template management - Edit the email template for user's notification emails.
- Audit log - Configure and view log for the permitted domain.
 - Log - View and export the log for the permitted domain.
- View dashboard – Show main customer dashboard.
- **All domain permissions** - Assign domain(s) management.
 - Assigned Domain(s) - Manage domains, incoming and outgoing users, emails, audit log and reports.
 - View - Only view the assigned domains.
 - Change - Edit the assigned domain(s)
 - Remove - Remove the assigned domain(s).
 - User Management - View and manage incoming users, outgoing users, whitelist recipients and blacklist recipients.
 - Incoming user - View, manage and unlock incoming users.
 - View - Only view list of incoming users.
 - Manage - View and manage incoming users.
 - Unlock - Unlock users immediately without waiting for the timeout period to end.
 - Change forward settings - Change forward email settings for incoming users.
 - Outgoing user - View, manage, lock/unlock and import from incoming users.
 - View - Only view list of outgoing users.
 - Manage - View and manage outgoing users.
 - Outgoing settings - Configure a list of outgoing users.
 - Lock/Unlock - Lock or unlock outgoing users from sending out mails.
 - Import from incoming - Import outgoing users from the list of incoming users.
 - Whitelist recipients - View and manage whitelist recipients.
 - View - Only view list of whitelisted recipients.
 - Manage - View and manage whitelist recipients.
 - Blacklist recipients - View and manage whitelist recipients.
 - View - Only view list of blacklisted recipients.
 - Manage - View and manage blacklist recipients.
 - Users auto-import - Automatically import all new incoming users bases on incoming email flow
 - View - Only view list of users auto-import recipients.
 - Manage - View and manage users auto-import recipients.
 - Domain geolookup restrictions - View and manage CASG web interface access control policies
 - View - Only view the access control polices
 - Manage - View and manage access control policies
 - Domain management - View and manage all domain related tasks.
 - Local recipients - View and manage local recipients.
 - View - Only view list of local recipients.
 - Manage - View and manage local recipients.
 - Domain alias - View and manage domain aliases

- View - Only view the list of domain aliases.
- Manage - View and manage domain aliases.
- Email filter settings - View and configure incoming spam detection settings.
 - View - Only view incoming spam detection settings.
 - Threshold - Configure changes for "Spam threshold" and "Probable spam threshold" fields in the Incoming Spam detection settings
 - Change - View and configure "Spam threshold" and "Probable spam threshold" fields.
- Domain settings - View and change domain settings.
 - View - Only view the list of domain settings.
 - Change - View and configure domain settings.
- Email for license notification – View and configure license expiry reminders
- Domain disk space limitation – View and configure archive storage disk space
 - View – Only view archive storage space
 - Change – View and configure archive storage space
- LDAP - View and configure LDAP settings for importing users.
 - View - Only view LDAP settings and list of imported users.
 - Change - View and configure LDAP settings for importing users.
- Quarantine - View and manage quarantined mails.
 - View - Only view the list of quarantined mails.
 - Delete - Deleted quarantined mails from the list.
 - Release - Release quarantined mails to the recipients.
 - View mail content - View the content of the quarantined mails.
- Archive - View and manage copy of incoming mails in archive.
 - View - Only view archived mails.
 - Resend - Resend archived mails to recipients.
 - Retain - Retains archived mails from being purged automatically.
 - Delete - Delete archived mails.
 - View mail content - View mail content of archived mails.
- Incoming delivery queue - View and manage queued mails.
 - View - Only view queued mails.
 - Retry - Retry to send queued mails to recipients.
 - Alerts - Queue emails notification
- Incoming Log Search - Search incoming mails log.
- Outgoing Log Search - Search sent mails log.
- Clear incoming cache - Clear incoming callout cache.
- Clear outgoing cache - Clear outgoing callout cache.
- User session history view - View user sessions history for the assigned domain(s).
- Office 365 Activation settings – View and configure Office 365 activation settings.
- SPF Control settings – View and manage sender policy framework (SPF) settings
 - View – Only view SPF settings.
 - Manage – View and configure SPF settings.
- Email Management - View and configure all Email management related settings and tasks.
 - Email size - View and configure email size settings.
 - View - Only view email size settings.
 - Change - View and configure email size settings.
 - Blocked extensions - View and manage blocked extensions.
 - View - Only view the list of blocked extensions.

- Change - View and manage blocked extensions.
- Whitelist senders - View and manage sender whitelist.
 - View - Only view sender whitelist.
 - Manage - View and manage sender whitelist.
- Blacklist senders - View and manage sender blacklist.
 - View - Only view sender blacklist.
 - Manage - View and manage sender blacklist.
- Release requests - View and manage requests from users for release of quarantined mails.
 - View - Only view the list of requests from users for release of quarantined mails.
 - Manage - View and manage requests from users for release of quarantined mails.
- Whitelist requests - View and manage requests from users to whitelist senders.
 - View - Only view the list of requests from users for adding senders to whitelist.
 - Manage - View and manage requests from users to whitelist senders.
- Blacklist requests - View and manage requests from users to blacklist senders.
 - View - Only view the list of requests from users for adding senders to blacklist.
 - Manage - View and manage requests from users to blacklist senders.
- Report spam - Upload mails to CASG for reporting them as spam.
- Create rule - Create and manage administrators rules.
 - View - Only view administrators rules.
 - Manage - View and manage administrators rules.
- Whitelist sender rule - View and manage rules for adding senders to whitelist
 - View - Only view the whitelist sender rules
 - Manage - View and manage whitelist sender rules
- Blacklist sender rule - View and manage rules for adding senders to blacklist
 - View - Only view the blacklist sender rules
 - Manage - View and manage blacklist sender rules
- Whitelist senders per user - View and manage whitelisted senders per user.
 - View - Only view list of whitelisted senders per user.
 - Manage - View and manage whitelisted senders per user.
- Blacklist senders per user - View and manage blacklisted senders per user.
 - View - Only view list of blacklisted senders per user.
 - Manage - View and manage blacklisted senders per user.
- Domain relay restrictions - View and configure email relay restriction rules
 - View - Only view relay restriction rule
 - Manage - View and manage relay restriction rules
- Audit log - Configure and view log for the permitted domain.
 - Configuration - Configure the log settings for the permitted domain.
 - Log - View and export the log for the permitted domain.
- Report management - View and configure settings for periodical domain and quarantine summary reports for the permitted domain.
 - View - Only view the configured settings for periodical domain and quarantine summary reports for the permitted domain.
 - Change - View and configure settings for periodical domain and quarantine summary reports for the permitted domain.

Default permission levels

- Add group – No permissions are enabled. You can enable permissions as per your requirement.
- Add domain group – Permissions required for domain management are enabled. You have to select the domain(s) for adding to the domain group. The following customer permissions are enabled by default:

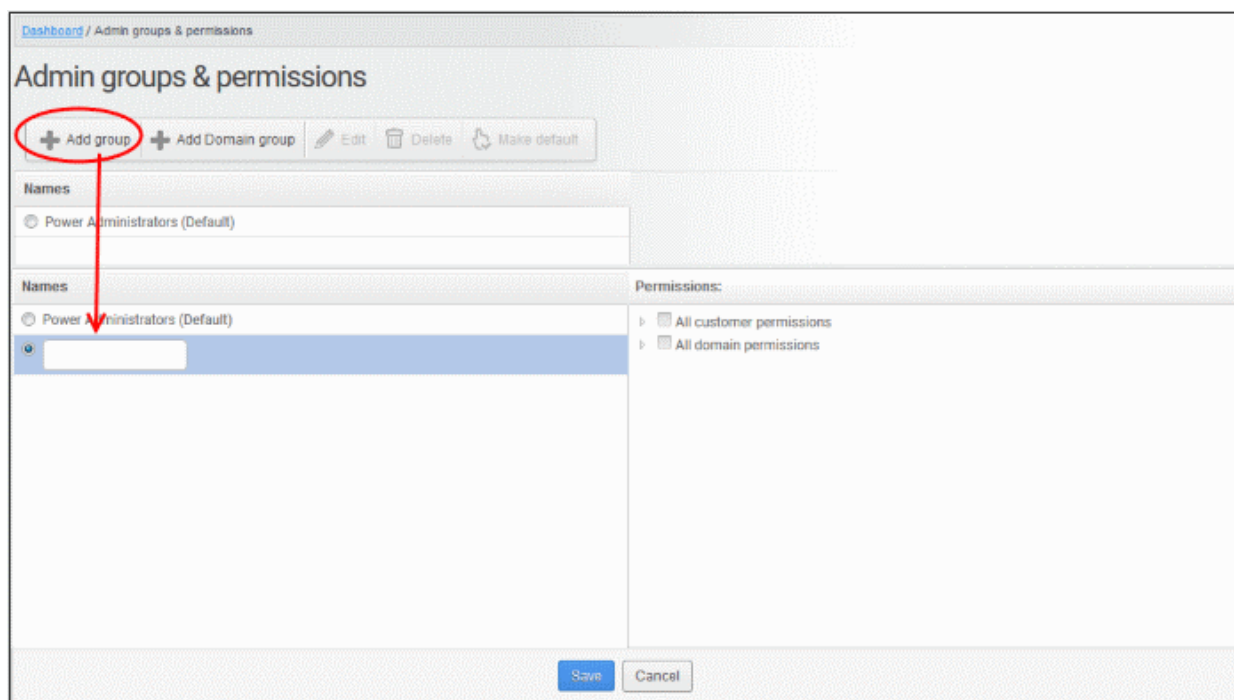
- All customer permissions
 - User permissions – View and manage
 - Report management – View and change
 - User session history view
 - Locale – View and change
 - Email template management
 - Audit log

Click the following links for more details.

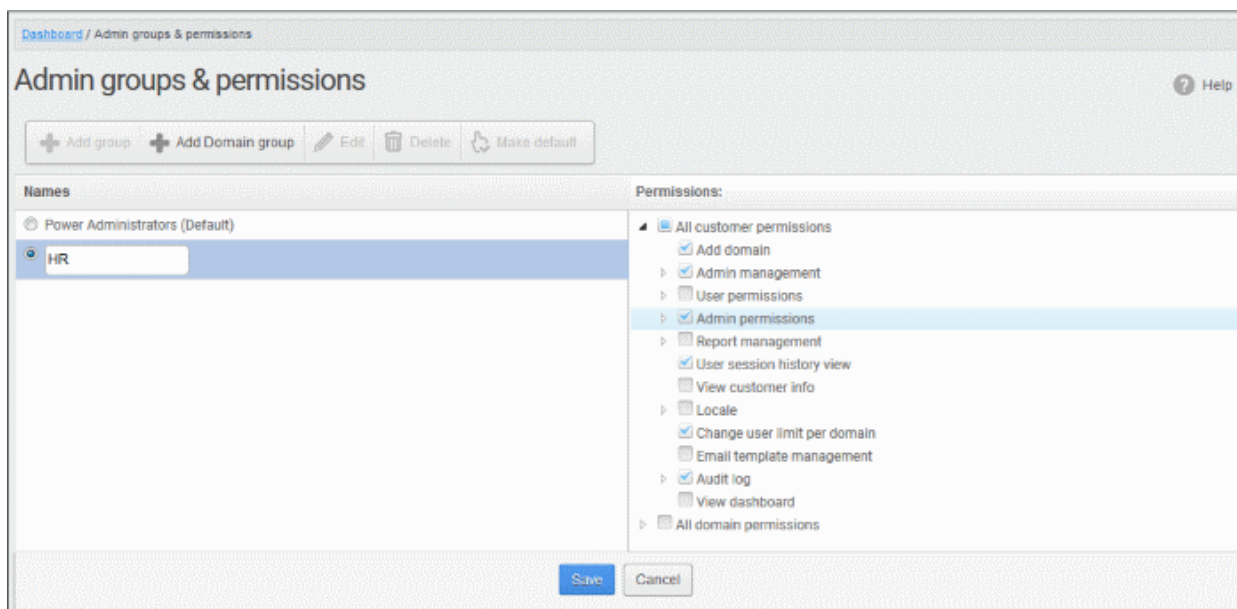
- [Add a new admin group](#)
- [Add a new domain group](#)
- [Edit an admin / domain group](#)
- [Delete an admin / domain group](#)
- [Make an admin / domain group as default](#)

Add a new admin group

- Click the 'Add group' button
- A new admin group creating field appears



- Enter the name of the group in the text field under the 'Name' column.



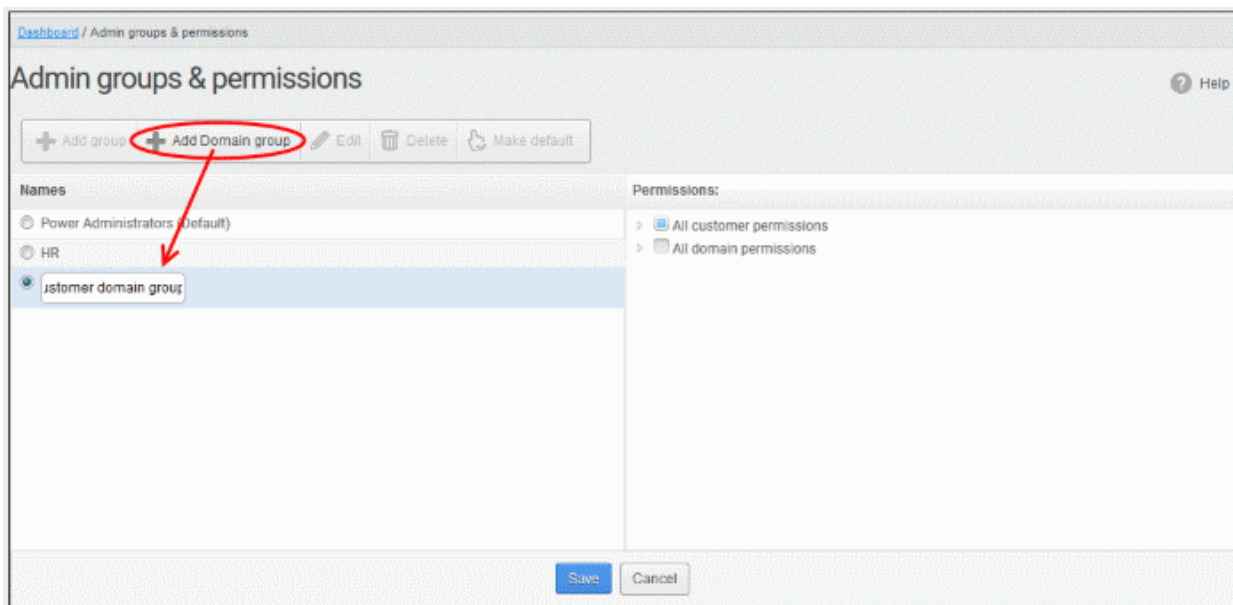
- Select the permissions for the admin group on the right.
- Click 'Save' button.

The newly created group is added.

Now, administrators belonging to the account can be assigned to this newly created group. See '[Managing Permissions for Administrators](#)' in '[Administrators](#)' on how to add users to predefined groups.

Add a new domain admin group

- Click the 'Add domain group' button
- A new domain admin group creating field appears



- Enter the domain admin group name
- Permissions:
 - All customer permissions - This group comes with predefined customer permissions that is adequate for domain management. Update if required, but not recommended. See [default permission levels](#) explained above.

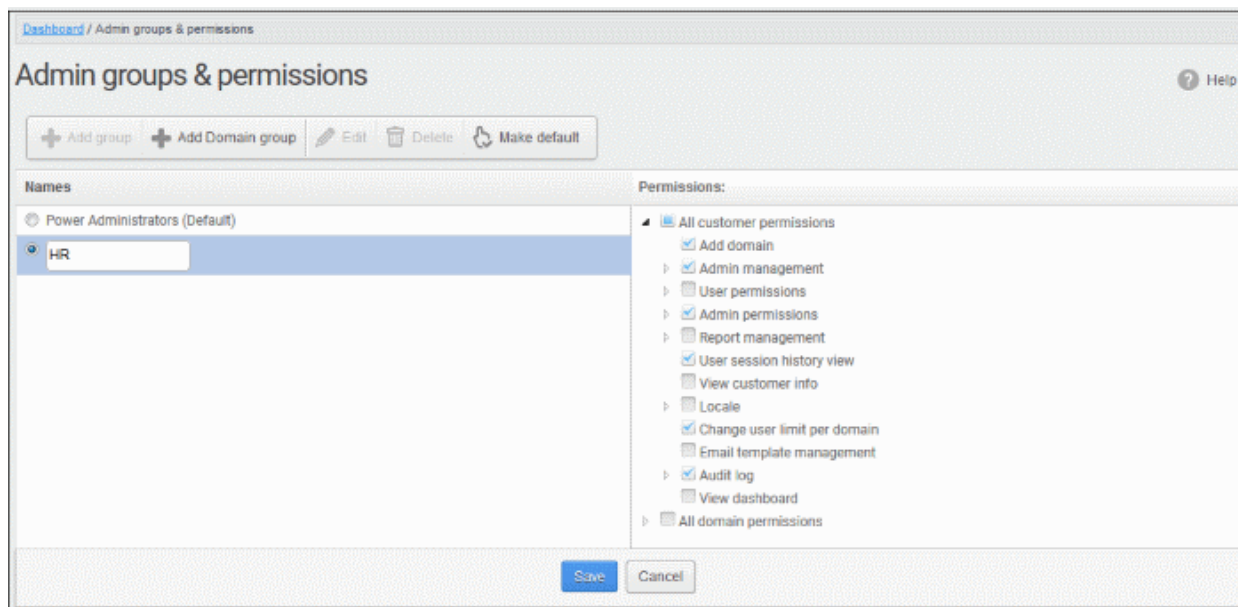
- All domain permissions - Select the domain(s) and domain permissions for the group.
- Click 'Save'

Now, administrators belonging to the account can be assigned to this newly created group. See '[Managing Permissions for Administrators](#)' in '[Administrators](#)' on how to add users to predefined groups.

Edit an admin / domain group

You can edit the name of an existing group and / or change the permission levels.

- Select the group from the list and click the 'Edit' button.

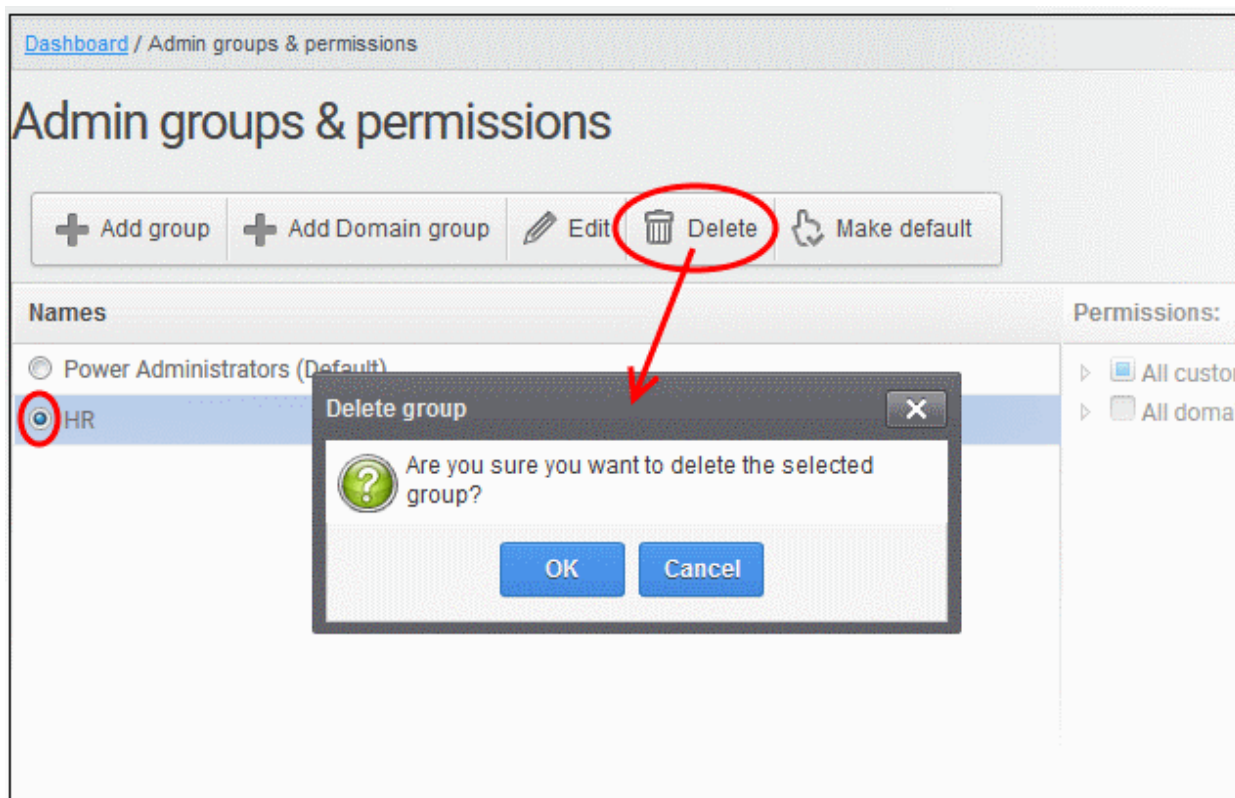


- Change the permission levels and / or the name of the group.
- Click the 'Save' button for the changes to take effect.

The admins in the group that is edited will be automatically reassigned to the edited group.

Delete an admin / domain group

- Select the group from the list and click the 'Delete' button.



- Click 'OK' in the confirmation dialog.

The selected group will be deleted from the list.

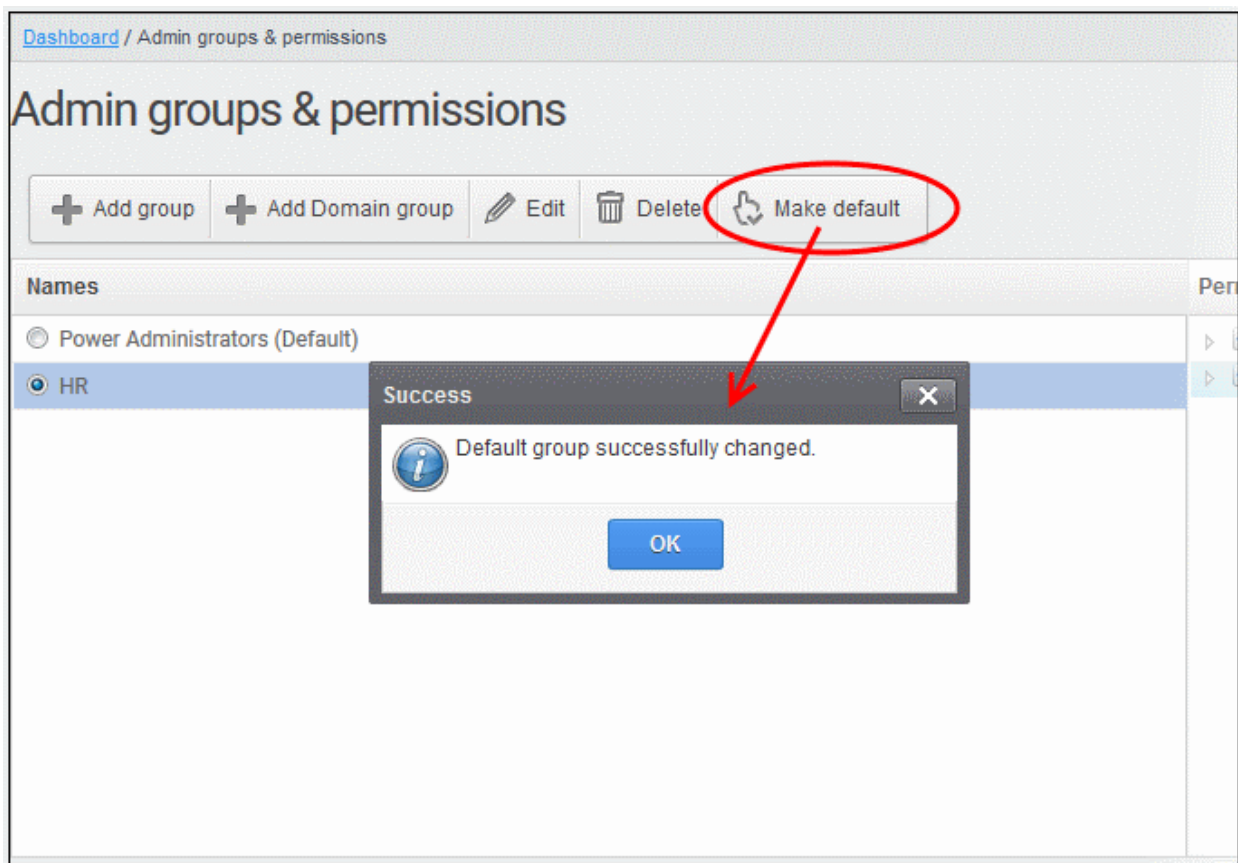
Note 1: If you delete a group, admins assigned to that group will be automatically moved to default group. You have to reassign the administrators if required.

Note 2: If you delete an admin group created by the administrator and marked as default, then the power administrators group that was shipped with the product will be set as default. All the admins from the deleted group will be automatically migrated to the power administrators group.

Make an admin / domain group as default

CASG allows administrators to make an existing group as a default group. Newly added administrators and administrators belonging to an existing group whose name was deleted will be automatically moved to this default group.

- Select a group from the list and click 'Make default'.
- A success dialog will be displayed:



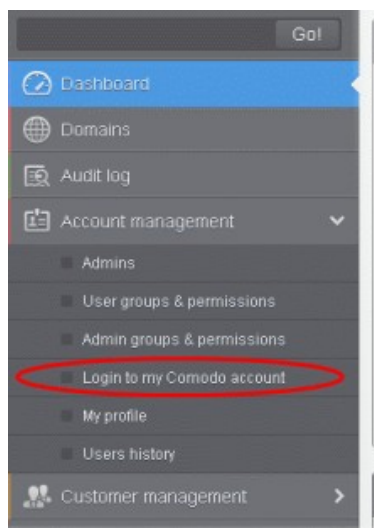
- Click 'OK'.

The selected group will be displayed as default group.

Note: If you delete an admin group created by the administrator and marked as default, then the 'Power Administrator' group that was shipped with the product will be set as default. All the admins from the deleted group will be automatically migrated to the 'Power Administrator' group.

8.4 My Comodo Account

This feature will be available in the 'Account management' if you have logged in to CASG using CAM account credentials.



- Click the 'Login to my Comodo account' to open <https://accounts.comodo.com/login> page. From here

you can:

- Add more subscriptions for CASG account
- Change your password
- Change contact information
- Sign up to other Comodo products

...and many more.

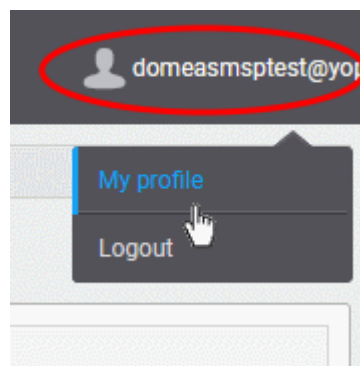
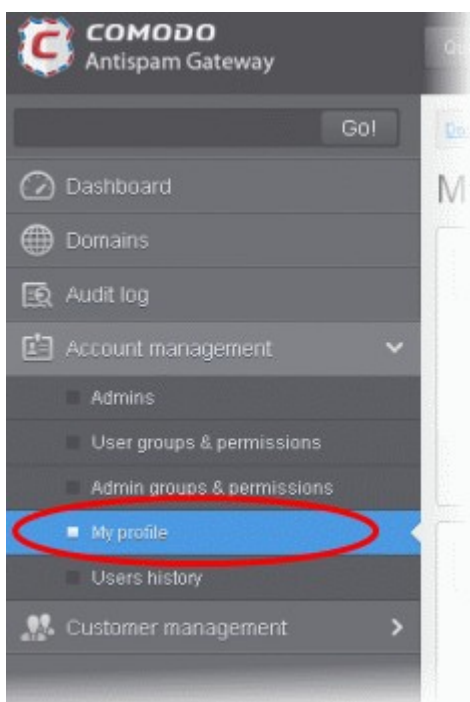
For more details on CAM account, visit our online website at help.comodo.com/topic-211-1-513-5907—Introduction-To-Comodo-Accounts-Manager.html.

8.5 My Profile

The 'my profile' interface lets currently logged-in administrator to change his login password and configure other settings.

You can open 'My profile' interface in two ways:

- Click the 'Account management' on the left to expand then 'My profile'.
- Alternatively, click the user name then 'My Profile' at the top-right.



The 'my profile' interface opens:

Dashboard / My profile

My profile Help

Change settings

Login:

CAM email:

System notifications email(s):

Number of minutes before my session expires:

Spam trap email:

Sites:

Note: The interface will vary depending whether you logged in as an admin or account admin. Account admins can change password from their CAM account.

- **Login** - The user-name of the currently active user. Administrators can use this to log in to CAM to purchase additional licenses and renew existing licenses.
- **CAM email** - The email address for the account as registered at Comodo Accounts Manager (CAM).
- **System notifications email(s)** - Enter the email addresses at which the new administrator should receive CASG notification emails. It can be the same email address as the login name and / or alternative email address(es) of up to a maximum of five. The quarantine requests from users, for blacklisting, whitelisting, or releasing quarantined emails and notifications such as of imports of users, local recipients and users via LDAP from CSV files will be sent to the email addresses specified in this field. See [Email Management](#) for more details.
- **Number of minutes before my session expires** - You can set the idle session timeout period in the box. Enter the period in minutes or increase / decrease the period by clicking the up / down arrow. The valid entry is between 1 minute and 120 minutes.
- **Spam trap email** (Optional) - If you already have a special 'spam-trap' email address then please enter it here to further improve CASG message filtering.
- **Sites** (Optional) - Enter the URLs of all websites owned by your company in order to further improve spam filtering.
- Click 'Save' for your changes to take effect.

8.6 Users History

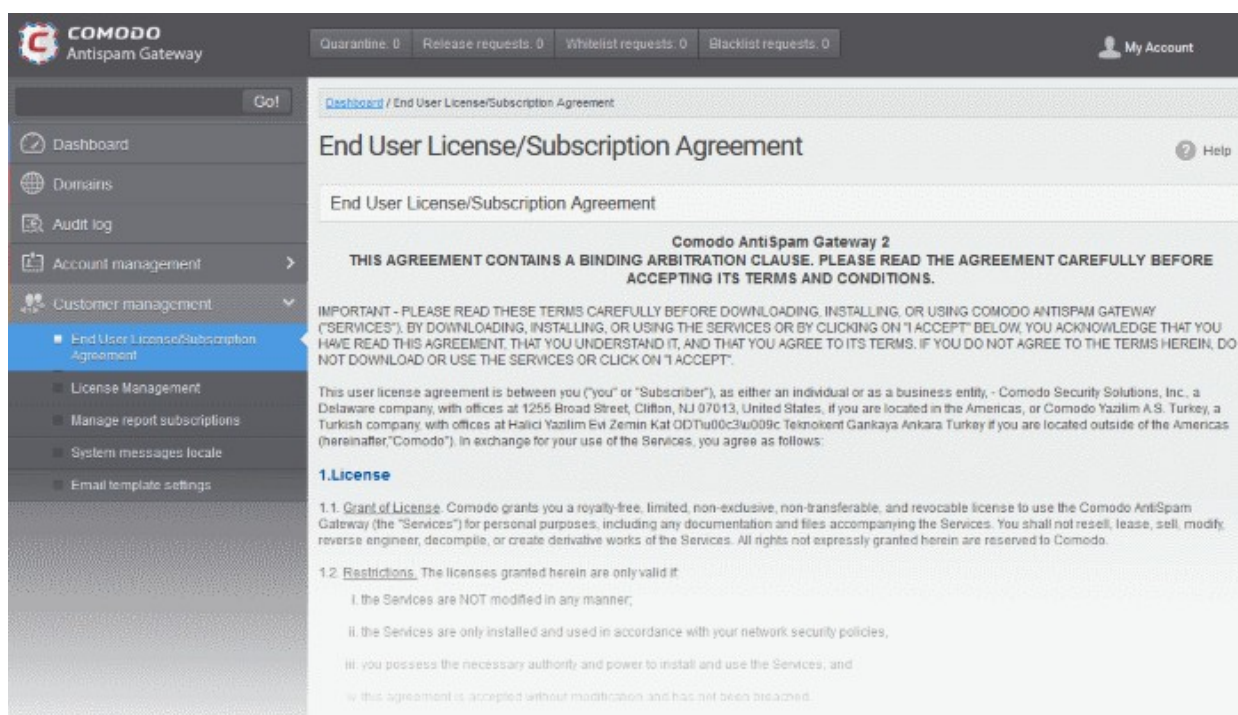
The 'Users History' area in 'Administrator Account Management' allows admins to view user history for all domains within a particular date range. From here you can filter users by IP address, last login, domain, username and/or location. By default, the most recent 15 records will be displayed.

Use of filters to create custom searches is covered in more detail [here](#).

9 Customer Management

The 'Customer Management' area allows an administrator to:

- View the details of the account they are logged into
- Create an account
- Update the product and extend your license term
- Configure subscriptions for the periodical Domain and Quarantine summary reports for domains
- Customize the 'support information' area in the notification emails that are generated for activities such as while adding a new user, password regeneration, quarantine request and quarantine report.



Click the following links for more details:

- [End user license agreements](#)
- [View license information](#)
- [Manage report subscriptions](#)
- [Notification email settings](#)

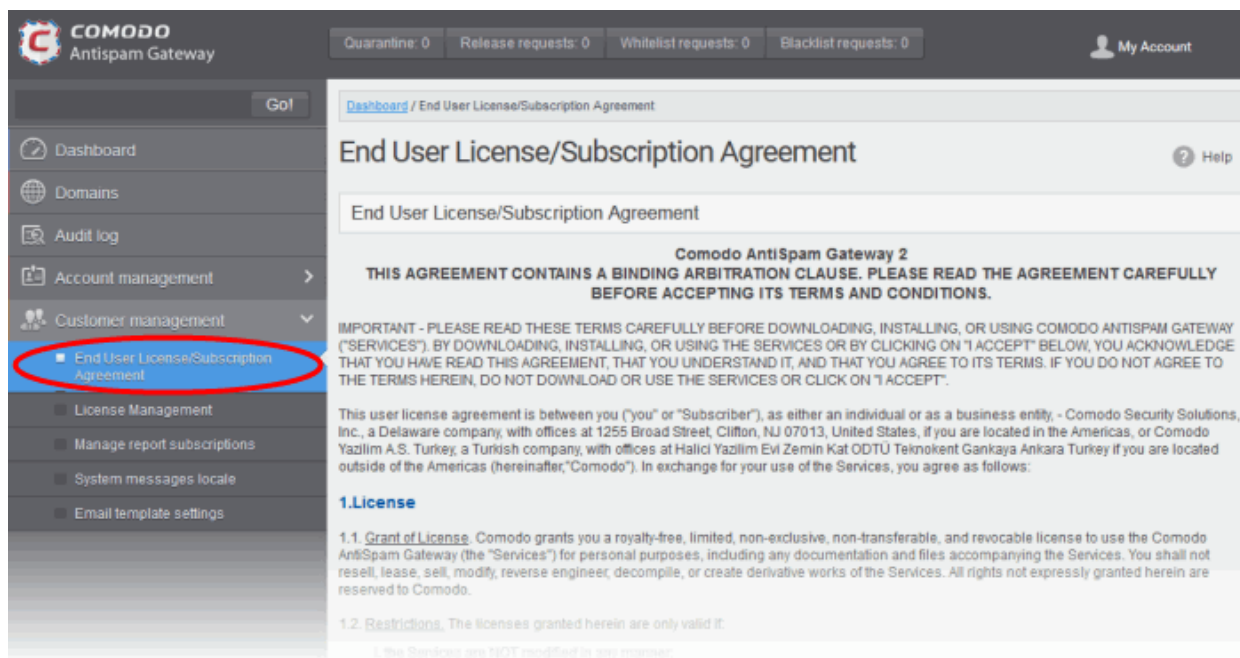
9.1 End User License and Subscriber Agreements

The 'End User License / Subscription Agreement' interface displays the complete Comodo Antispam Gateway End-User License and Subscriber Agreement.

To view End User License/Subscription Agreement

- Click 'Customer management' tab from the left hand side navigation to expand it and then click the 'End-User License/Subscriber Agreement.' tab from the sub menu.

The 'EULA/ Subscription Agreement' interface will be displayed:



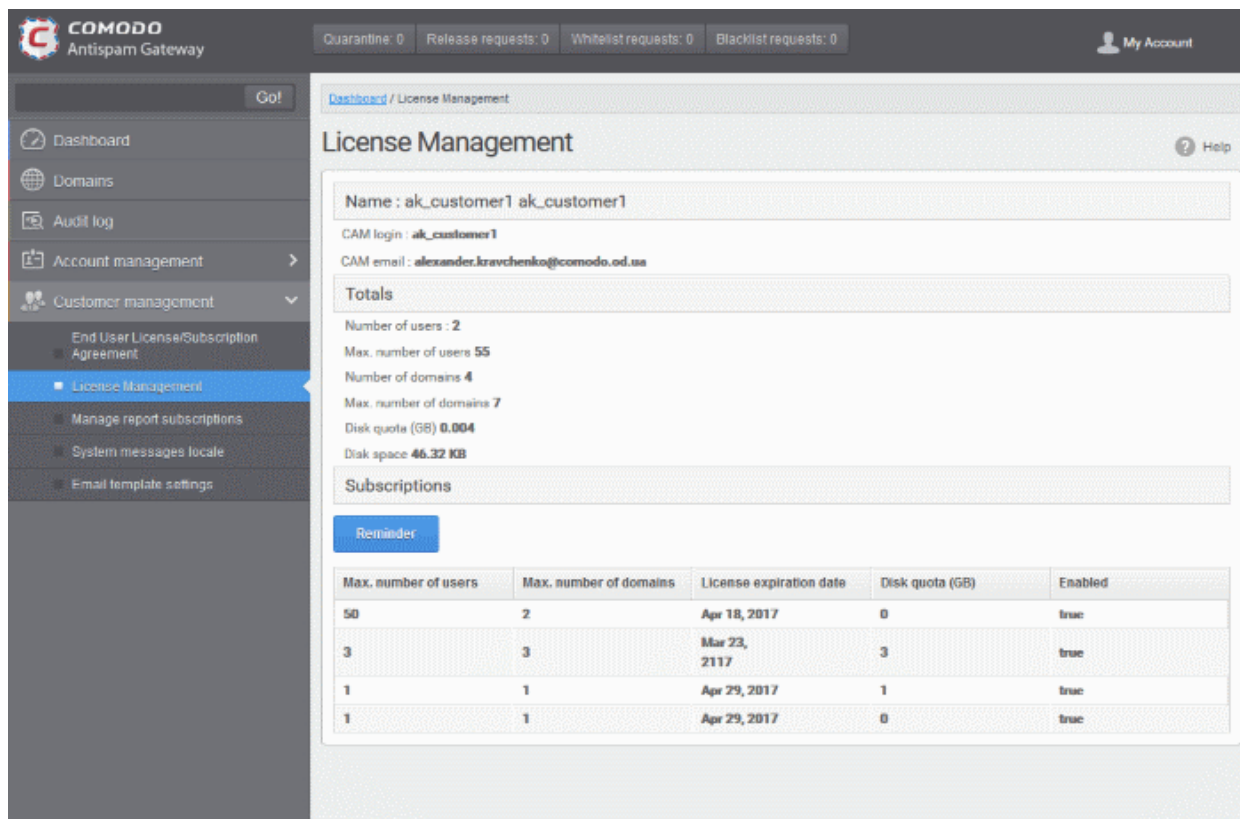
9.2 View License Information

The 'License Management' interface provides administrators with usage information.

View the license management screen:

- Click the License Management from the 'Customer management' drop-down on the left

The example below shows a customer with multiple licenses:



- **Max. number of users** - Total users on all licenses combined.
- **Max. number of domains** - Total domains licensed on all licenses combined.

Name

- The name of the account is displayed in the title bar.
- **CAM login:** Login username for Comodo Accounts Manager (CAM) at <https://accounts.comodo.com>. You can login to CAM to purchase or renew licenses.
- **CAM email:** Email address for the account as registered in CAM.

Totals

- **Number of users:** The total number of active users across all your domains.
- **Max. number of users:** Total users you can add (all licenses combined). You cannot exceed this number of users without purchasing additional licenses.
- **Number of domains:** The number of domains enrolled on the account.
- **Max. number of domains:** The total number of domains you are licensed for across all licenses.
- **Disk quota:** Total storage space available to archive incoming messages.
- **Disk space:** How much storage space you are currently using to archive mails.

Subscriptions

The following details are available for each subscription:

- **Max. number of users:** Total number of users that can be added to the account on the license.
- **Max. number of domains:** Total number of domains that can be added on the license.
- **License expiration date:** The date till which the license is valid.
- **Disk quota:** Total storage space available on the license.
- **Enabled:** States whether the subscription is active or not.

The 'Reminder' button allows you to choose an email address to receive license expiry reminders, and to specify the period of time before expiry that you wish to receive them. Please note this button will be available if you have logged in to CASG using CAM account credentials.

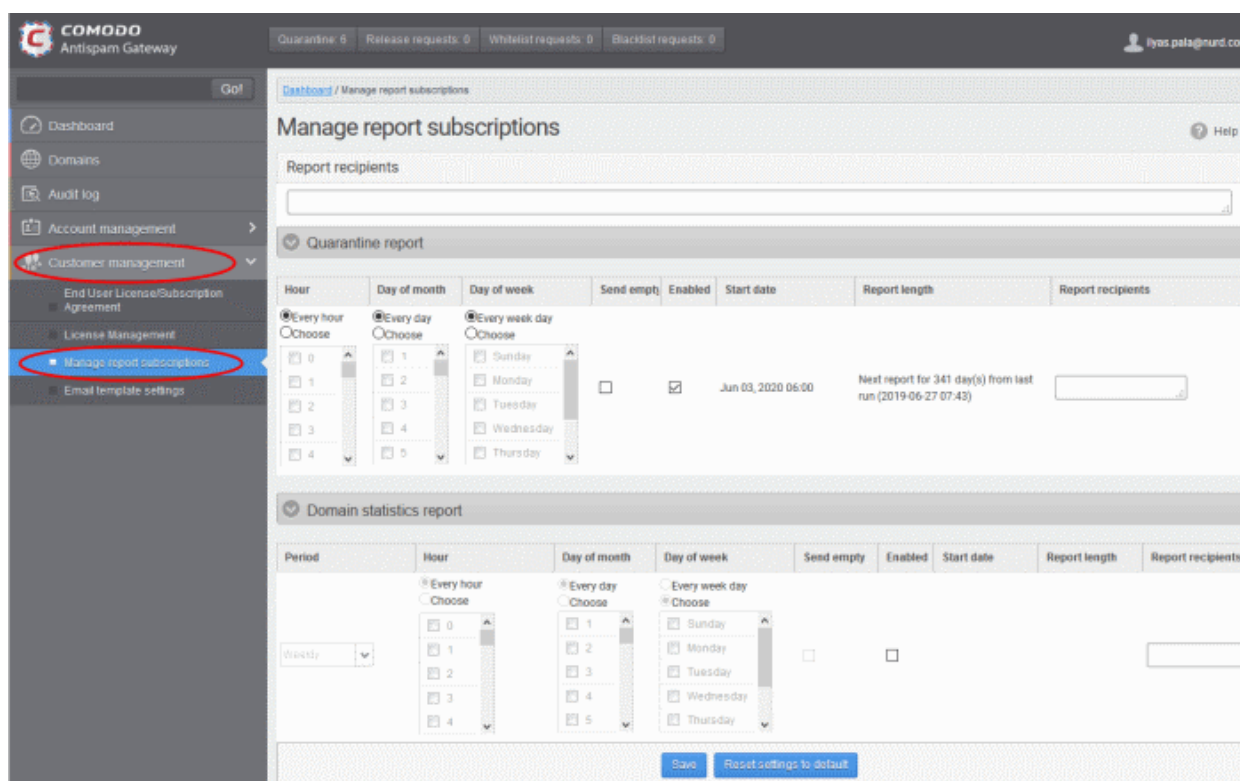
9.3 Manage Report Subscriptions

The 'manage report subscriptions' interface lets you to configure subscriptions to 'Domain' and 'Quarantine' summary reports of all enrolled domains. See [CASG Reports - an Overview](#) for more details.

Access 'manage report subscriptions' interface

- Click 'Customer management' > 'Manage report subscriptions'

The manage report interface will open:



The 'Report recipients' field at the top is auto-populated with the email addresses of all the administrators available for the account and enabled for the same, at the time of **adding them**. The report recipients can be added or removed from this interface by entering the administrator's email address or deleting them and clicking the 'Save' button at the bottom.

Note – Reports are not sent to these recipients if you configure recipients for each report type.

The administrator can configure the subscription for two types of reports from this interface:

- **Quarantine Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly, will contain a detailed statistics of the mails that are identified as spam or containing malicious content and moved to Quarantine of the domain automatically by CASG. See **CASG Reports - An Overview** for more details.
- **Domain Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly, will contain a detailed statistics of number of users, mails that have been received at and sent from the domain, number of spams identified and blocked and so on. See **CASG Reports - An Overview** for more details.

Configure the subscription of the reports

- You can expand/collapse a report configuration section by clicking on the respective strip.
- Send empty - Leave this unchecked if empty reports are not to be sent to recipients.
- Enabled – Select this so reports are generated and sent to report recipients.
- Report recipients for each report type – Enter the email address of recipients that you want the reports to be sent. You can enter multiple addresses separated by a comma. Note – If this field is configured, the recipients that you added in the general report recipients field at the top of the interface will not receive the reports.
- Select the frequency at which the reports are to be sent to the administrators.

Quarantine Report

- **Hour** - The reports are generated and sent to the report recipients every hour or at the selected hour(s) of the day or date chosen from 'Day of month' or 'Day of week' columns.
- **Day of month** - The reports are generated and sent to the report recipients every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports are generated and sent to the report recipients every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
- **Start date** - Displays the start date of the report generation depending on the options chosen (as per Greenwich Mean Time (GMT)).
- **Report length** - Displays the period of the report that are generated depending on the options chosen.

Domain Statistics Report

- **Period** - Enables you to set the period to be covered in the report. The report contain the statistics of all the domains in the account for the past one hour, one week, one month or one year, as selected from drop-down from the scheduled report time.
- **Hour** - The reports are generated and sent to the report recipients every hour or at the selected hour(s) of the day or date chosen from 'Day of month' or 'Day of week' columns.
- **Day of month** - The reports are generated and sent to the report recipients every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports are generated and sent to the report recipients every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
- **Start date** - Displays the start date of the report generation depending on the options chosen (as per Greenwich Mean Time (GMT)).
- **Report length** - Displays the period of the report that are generated depending on the options chosen.
- Click 'Save' for your settings to take effect.
- Click the 'Reset settings to default' to disable both Quarantine and Domain statistics reports. The 'Report Recipients' field will not be cleared.

9.4 Notification Email Settings

By default, all the notification mails sent to administrators and users on various events like adding a new user, password regeneration, quarantine request or periodical report mails like quarantine report will contain the links to the online help guide and Comodo support in the footer.

The 'Email template settings' area allows you customize the footer for adding their contact and support information.

To customize the notification emails

- Click the Email template settings' from the Customer management' drop-down on the left

The 'Email template settings' interface will be displayed:

The screenshot shows the 'Email template settings' page in the Comodo Antispam Gateway. The page has a dark sidebar on the left with a 'Go!' button and a list of navigation items: Dashboard, Domains, Audit log, Account management, and Customer management. The 'Email template settings' item is selected and highlighted with a red circle. The main content area is titled 'Email template settings' and includes a yellow warning box with a note: 'Note: changes below will be applied to all system notification messages sent to user'. Below the note is a checked checkbox labeled 'Change default email footer'. Underneath is a text area containing HTML code for the email footer. The code includes a link to the user guide and a support email link. At the bottom of the text area are 'Save' and 'Reset to default' buttons.

Please note the customization can be done only in html format.

- Check 'Change default email footer' box if you want to edit details.
- Edit the details in html format as per your requirement and click 'Save' button.
- Click the 'Reset to default' button to display Comodo support information in the notification emails.

10 CASG Reports - An Overview

- Comodo Antispam Gateway can generate five kinds of reports - 'Quarantine report', 'Domain statistics report', 'User import report', 'Quarantine Release Report' and 'Reported Spam Report'.
- Reports are sent via email to administrators and users as configured at scheduled times

Global Reports and Domain level Reports

1. Global reports are for all domains covered by the customer account. See '**Manage Subscriptions for Reports**' under '**Customer Management**' for more details on the account level.
2. Domain level reports are specific to a domain. See '**Manage Report Subscriptions for Selected Domain**' under '**Incoming**' section for reports on domain levels.

CASG creates five kinds of reports:

- **Quarantine Report** - Statistics about spam or malicious emails that were moved to quarantine by CASG. You can receive the report daily, weekly or monthly.
- **Domain Statistics Report** - Covers all mail activity for the domain. You can receive the report daily, weekly

or monthly.

- **Users auto-import report** - Statistics about the mail activity of new users added for each domain. User import reports are generated at the domain level and not the account level.
- **Quarantine Release Report** - Statistics about malicious or spam messages quarantined on your entire domain. These reports are generated at the domain level and not the account level.
- **Reported Spam Report** - Statistics on messages marked as spam by users. The report can be configured to be received hourly, daily, weekly or monthly by the administrator. These reports are generated at the domain level and not the account level.
- Reports can be enabled or disabled per administrator in **Dashboard > Account Management > Admin > Add Administrators** or **Edit Administrators**.

While the first two reports, Quarantine Report and Domain Statistics Report, are available for all the domains as well as for a specific domain, other reports are available for specific domains only.

10.1 Quarantine Report

The quarantine report contains a list of mails that were identified as spam or containing malicious content and were moved to quarantine automatically by CASG, with the details on sender, receiver, date and attachments. You can view the contents of a mail by clicking its subject line from the report.

- **Administrator**
 - **Domain Level** - The report generated for an administrator contains the details of the mails moved to quarantine of the selected domain.
 - **Customer Level** - The report generated for an administrator contains the details of the mails moved to quarantine of all the domains belonging to the account.
- **User** - The report generated for a user contains the details of the mails moved to quarantine of the user.

The report can be subscribed to be received hourly, daily, weekly or monthly for an administrator and daily, weekly or monthly for a user.

- **Hourly** - The reports are generated and sent every hour to the administrators through email.
- **Daily** - The reports are generated and sent daily to the administrators/user through email.
- **Weekly** - The reports are generated and sent to the administrators/user through email on every seventh day from the start date set in the 'Start date' field. The report contains details of the mails quarantined during the past seven days. The first report is sent on the start date and contains the statistics for the remaining days of the week from the day of configuration and subsequently every seven days.
- **Monthly** - The reports are generated and sent to the administrators/user through email on every 30th day from the start date set in the 'Start date' field. The report contains details of the mails quarantined during the past 30 days. The first report is sent on the start date and contains the statistics for the remaining days of the month from the day of configuration and subsequently every 30 days.

An example of a quarantine report is shown below:



Here is the quarantine report for docteamcasg.comodo.od.ua from Apr 02, 2014 14:25 to Apr 11, 2014 00:00

Subject	From	To	CC (to docteamcasg.comodo.od.ua only)	Date	Size	
test spam_email_1	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua		Wed Apr 02 14:26:40 GMT 2014	8.16 KB	
test spam_email_2	John Smith <fiatlina@gmail.com>	demo2@docteamcasg.comodo.od.ua		Wed Apr 02 14:27:00 GMT 2014	8.18 KB	
Fw: We have free samples for you, now try before you buy @ your doorsteps!	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua		Mon Apr 07 08:52:31 GMT 2014	3.02 KB	
Fw: We have free samples for you, now try before you buy @ your doorsteps!	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua		Mon Apr 07 08:52:31 GMT 2014	3.02 KB	
Fw: FOLLOW THE INSTRUCTIONS !!	John Smith <fiatlina@gmail.com>	demo2@docteamcasg.comodo.od.ua, demo1@docteamcasg.comodo.od.ua		Wed Apr 09 04:31:41 GMT 2014	231.0 KB	
Fw: FOLLOW THE INSTRUCTIONS !!	John Smith <fiatlina@gmail.com>	demo2@docteamcasg.comodo.od.ua, demo1@docteamcasg.comodo.od.ua		Wed Apr 09 04:31:41 GMT 2014	231.0 KB	
Fw: Register and Get Rs. 5000 to Shop Now! Introducing Pepperfly.com - India's Largest Home and Furniture Online Store!	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua		Wed Apr 09 04:32:36 GMT 2014	3.05 KB	
Fw: Register and Get Rs. 5000 to Shop Now! Introducing Pepperfly.com - India's Largest Home and Furniture Online Store!	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua		Wed Apr 09 04:32:36 GMT 2014	3.05 KB	
Fw: Get Rs. 25 assured recharge + chance to win an IPOC!	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua		Wed Apr 09 04:33:22 GMT 2014	3.98 KB	
Fw: Claim your exclusive rewards with the American Express Gold Card	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua		Wed Apr 09 06:33:00 GMT 2014	26.5 KB	
Fwd Fw: Send UNLIMITED Emails/Newsletter in Just Rs. 2,500/mo. ZERO SETUP COST	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua		Wed Apr 09 06:40:43 GMT 2014	2.3 KB	

Having Trouble? Support is here to help. Open a Ticket at <https://support.comodo.com> or call 1.888.COMODO (266.6361)

- Click the 'Subject' of a mail to open the mail in a new CASG window. You need to login to CASG to read the mail in the new window.

10.2 Domain Statistics Report

The domain statistics report provides details on all the mail activities on the domain. This includes information covering the number of users; mails that have been received at and sent from the domain; number of mail identified spam/malicious; number of mails blocked and so on. The report can be configured to be received hourly, daily, weekly, monthly or yearly by the administrator.

- **Domain Level** - The report contains only the details of domain statistics of the selected domain.
- **Customer Level** - The report contains the details of domain statistics of all the domains belonging to the account.

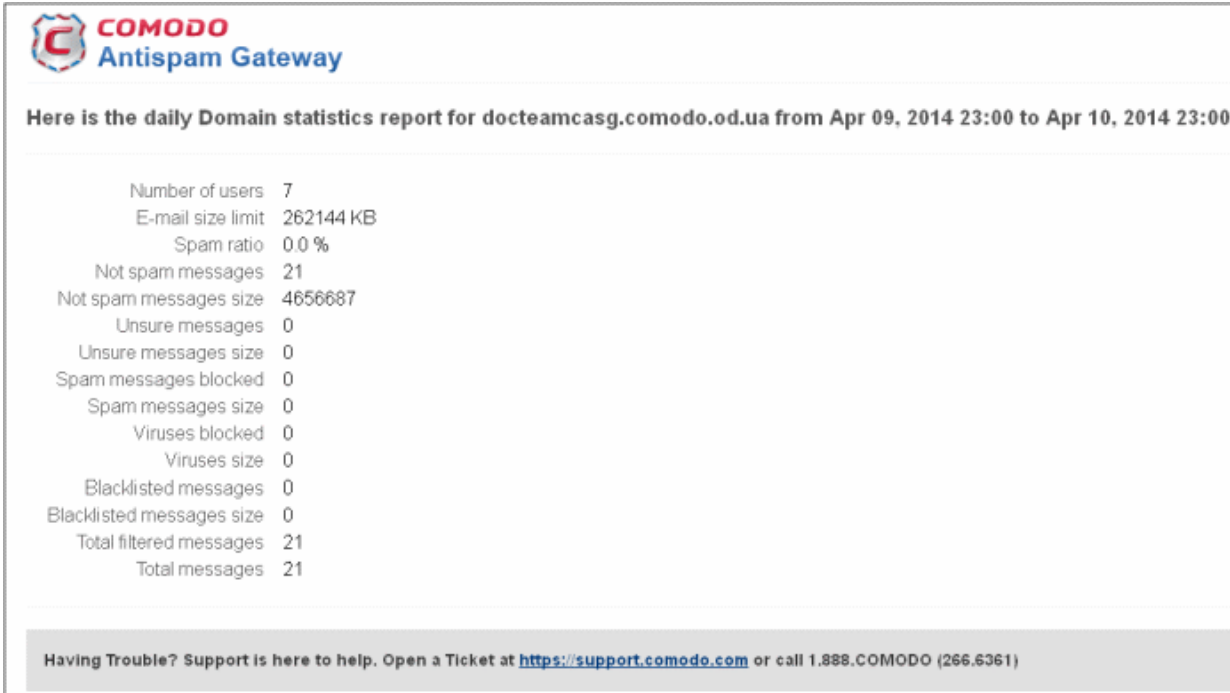
Note: The domain statistics report is available only to the administrators.

The report can be subscribed to be received hourly, daily, weekly, monthly or yearly.

- **Hourly** - Reports are generated and sent every hour to the administrators.
- **Daily** - Reports are generated and sent daily to the administrators.
- **Weekly** - Reports are generated and sent to the administrators on every seventh day from the start date set in the 'Start date' field. The report contains details of the mail activities for the domains during the past seven days. The first report is sent on the start date and contains the statistics for the remaining days of the week from the day of configuration and subsequently every seven days.
- **Monthly** - Reports are generated and sent to the administrators on every 30th day from the start date set in the 'Start date' field. The report contains details of the mail activities for the domains during the past 30 days. The first report is sent on the start date and contains the statistics for the remaining days of the month from the day of configuration and subsequently every 30 days.

- **Yearly** - Reports are generated and sent to the administrators on every 365th day from the start date set in the 'Start date' field. The report contains details of the mail activities for the domains during the past 12 months. The first report is sent on the start date and contains the statistics for the remaining months of the year from the day of configuration and subsequently every 12 months.

An example of a Domain Statistics Report is shown below:



COMODO
Antispam Gateway

Here is the daily Domain statistics report for docteamcasg.comodo.od.ua from Apr 09, 2014 23:00 to Apr 10, 2014 23:00

Number of users	7
E-mail size limit	262144 KB
Spam ratio	0.0 %
Not spam messages	21
Not spam messages size	4656687
Unsure messages	0
Unsure messages size	0
Spam messages blocked	0
Spam messages size	0
Viruses blocked	0
Viruses size	0
Blacklisted messages	0
Blacklisted messages size	0
Total filtered messages	21
Total messages	21

Having Trouble? Support is here to help. Open a Ticket at <https://support.comodo.com> or call 1.888.COMODO (266.6361)

10.3 Auto-Imported Users Report

The users auto-import report provides details on all the new users belonging to a managed domain, that were automatically imported to CASG on receiving an incoming mail addressed to them at the mail server. The auto-imported users are sent with an invitation email containing login credentials for them to access the CASG user interface. For more details on managing auto-import, see **Manage User auto-import**.

Note: The user auto-import reports are generated only for the domain level and not for the customer account level. The report is available only to the administrators.

The report contains the following details:

- Imported users count - The total number of users automatically imported into CASG for report time period.
- Enabled users count - The number of auto imported users that have activated their account by clicking the link in the invitation mail or logging-in to CASG using the credentials provided in the mail.
- Invited users count - The number of auto imported users that have been sent the invitation mails but yet to activate their account.
- User names list - The list of auto imported users.

An example of a 'Users Auto-Import Report' is shown below:



Here is the users auto-import report for `csgqa.comodo.od.ua` from Nov 21, 2014 09:00 to Nov 21, 2014 10:00

Imported users count 1
Enabled users count 1
Invited users count 0
User names list admin

For help, see the Admin guide: <http://help.comodo.com/topic-157-1-288-3192-introduction-to-comodo-antispam-gateway.html>

Having Trouble? Support is here to help. Open a Ticket at <https://support.comodo.com> or call 1.888.COMODO (256.2608)

10.4 Quarantine Release Report

The quarantine release report provides details of mails that were released from quarantine by the administrators as well as by the users with appropriate privileges. This also includes quarantine release requests accepted by administrators.

Note: The quarantine release reports are generated only for the domain level and not for the customer account level. The report is available only to the administrators .

The report can be subscribed to be received hourly, daily, weekly, monthly or yearly.

- **Hourly** - The reports are generated and sent every hour to the administrators.
- **Daily** - The reports are generated and sent daily to the administrators.
- **Weekly** - The reports are generated and sent to the administrators through email on every seventh day from the start date set in the 'Start date' field. The report contains details of the mail activities for the domains during the past seven days. The first report is sent on the start date and contains the statistics for the remaining days of the week from the day of configuration and subsequently every seven days.
- **Monthly** - The reports are generated and sent to the administrators through email on every 30th day from the start date set in the 'Start date' field. The report contains details of the mail activities for the domains during the past 30 days. The first report is sent on the start date and contains the statistics for the remaining days of the month from the day of configuration and subsequently every 30 days.
- **Yearly** - The reports are generated and sent to the administrators through email on every 365th day from the start date set in the 'Start date' field. The report contains details of the mail activities for the domains during the past 12 months. The first report is sent on the start date and will contain the statistics for the remaining months of the year from the day of configuration and subsequently every 12 months.

An example of a quarantine release report is shown below:



Quarantine release report for csgqa4.comodo.od.ua from Jul 01, 2015 09:00 to Jul 01, 2015 10:00

Date	Operation description	Login	Role	Details
Wed Jul 01 09:18:32 GMT 2015	Release quarantined message	admin1@csgqa4.comodo.od.ua	admin	Recipients: user2@csgqa4.comodo.od.ua, user3@csgqa4.comodo.od.ua, user30@csgqa3.comodo.od.ua; Sender: test@test.com; Date: null; Subject: SPAM MAIL
Wed Jul 01 09:18:49 GMT 2015	Release quarantined message	admin1@csgqa4.comodo.od.ua	admin	Recipients: user2@csgqa4.comodo.od.ua; Sender: user12@test.com; Date: null; Subject: test mail from TELNET 16-04-15 16:41
Wed Jul 01 09:42:50 GMT 2015	Release quarantined message	user1@csgqa4.comodo.od.ua	user	Recipients: user1@csgqa4.comodo.od.ua; Sender: alravchenko@csg.comodo.od.ua; Date: null; Subject: test mail 15:47

For help, see the Admin guide: <http://help.comodo.com/topic-157-1-288-3192-introduction-to-comodo-antispam-gateway.html>

Having Trouble? Support is here to help, agsupport@comodo.com or review the [Administrators Guide](#)

10.5 Reported Spam Report

The reported spam report provides details of mails that were reported as spam by the administrators as well as by the users with appropriate privileges. This also includes details of mails uploaded from the **'Report Spam'** interface.

Note: The reported spam reports are generated only for the domain level and not for the customer account level. The report is available only to the administrators .

The report can be subscribed to be received hourly, daily, weekly, monthly or yearly.

- **Hourly** - The reports are generated and sent every hour to the administrators through email.
- **Daily** -The reports are generated and sent daily to the administrators through email.
- **Weekly** - The reports are generated and sent to the administrators through email on every seventh day from the start date set in the 'Start date' field. The report contains details of the mail activities for the domains during the past seven days. The first report is sent on the start date and contains the statistics for the remaining days of the week from the day of configuration and subsequently every seven days.
- **Monthly** - The reports are generated and sent to the administrators through email on every 30th day from the start date set in the 'Start date' field. The report contains details of the mail activities for the domains during the past 30 days. The first report is sent on the start date and contains the statistics for the remaining days of the month from the day of configuration and subsequently every 30 days.
- **Yearly** - The reports are generated and sent to the administrators through email on every 365th day from the start date set in the 'Start date' field. The report contains details of the mail activities for the domains during the past 12 months. The first report is sent on the start date and contains the statistics for the remaining months of the year from the day of configuration and subsequently every 12 months.

An example of a reported spam report is shown below:



Reported Spam report for csgqa4.comodo.od.ua from Jul 01, 2015 10:00 to Jul 01, 2015 11:00

Date	Operation description	Login	Role	Details
Wed Jul 01 10:06:38 GMT 2015	Report delivered message as spam	admin1@csgqa4.comodo.od.ua	admin	Recipients: user77@csgqa4.comodo.od.ua; Sender: Dagwood Bumpsted <avantistude@gmail.com>; Date: Wed Jul 01 10:01:10 GMT 2015; Subject: Fwd: Get instant Online Personal Loan approval and disbursal in 72 hours
Wed Jul 01 10:39:03 GMT 2015	Report delivered message as spam	user77@csgqa4.comodo.od.ua	user	Recipients: user77@csgqa4.comodo.od.ua; Sender: Dagwood Bumpsted <avantistude@gmail.com>; Date: Wed Jul 01 10:01:10 GMT 2015; Subject: Fwd: Get instant Online Personal Loan approval and disbursal in 72 hours
Wed Jul 01 10:41:54 GMT 2015	Reports archived message as a Spam	user77@csgqa4.comodo.od.ua	user	Recipients: user77@csgqa4.comodo.od.ua; Sender: dagwood bumpsted <avantistude@gmail.com>; Date: Wed Jul 01 10:40:56 GMT 2015; Subject: Fwd: Zero Fees, Attractive Interest Rates and Loans upto 25L
Wed Jul 01 10:52:02 GMT 2015	Reports archived message as a Spam	user77@csgqa4.comodo.od.ua	user	Recipients: user77@csgqa4.comodo.od.ua; Sender: oxford morris minor <mmoxford@yahoo.com>; Date: Wed Jul 01 10:47:33 GMT 2015; Subject: Dr. Jones wake up now
Wed Jul 01 10:55:26 GMT 2015	Reports archived message as a Spam	user2@csgqa4.comodo.od.ua	user	Recipients: user1@csgqa4.comodo.od.ua, user2@csgqa4.comodo.od.ua; Sender: oxford morris minor <mmoxford@yahoo.com>; Date: Wed Jul 01 10:52:00 GMT 2015; Subject: Fw: Dr. Jones wake up now
Wed Jul 01 10:55:52 GMT 2015	Reports archived message as a Spam	user2@csgqa4.comodo.od.ua	user	Recipients: user1@csgqa4.comodo.od.ua, user2@csgqa4.comodo.od.ua; Sender: oxford morris minor <mmoxford@yahoo.com>; Date: Wed Jul 01 10:52:00 GMT 2015; Subject: Fw: Dr. Jones wake up now

Appendix 1 - CASG Error Codes

The most common error codes for CASG are given below:

Error Code	Description
1	Unknown error
100	Import exception
101	Wrong format
102	Wrong outgoing user format IP password. If 'password' is empty then 'username' must be IP address.
103	Communication exception
200	User limit exception
300	Spam engine exception
1000	Customer has no domains
1001	Domains mismatch
1002	Alias already exists
1003	User already exists

Appendix 2 - CASG Comparison Table

Features	Paid Version	Free Version
Number of domains and incoming / outgoing users	Depends on the subscription	5 users and 1 domain
Number of domain aliases	5	Nil
Active Directory / LDAP Synchronization	✓	✗
Create / Modify User Groups	✓	✗
Assign permissions to User Groups	✓	✗
Number of user aliases per user	5	Nil
Incoming / Outgoing email filtering	✓	✓
View all quarantined emails	✓	✓
Release quarantined emails	✓	✓
Whitelist / Blacklist quarantined emails	✓	✓
Configure spam detection settings	✓	✓
Report spam emails	✓	✓
View queued emails in Delivery Queue	✓	✓
Create local recipients	✓	✗
Clear incoming / outgoing email cache	✓	✗
Log search incoming emails	✓	✓
Log search outgoing emails	✓	✗
Create domain aliases	✓	✗
Configure domain settings	✓	✗
Configure email size restrictions	✓	✗
Configure 'Blocked extensions' settings	✓	✗
View users' release requests	✓	✗
View users' whitelist / blacklist requests	✓	✗
Whitelist / Blacklist recipients	✓	✗
Whitelist / Blacklist senders	✓	✓
View users' login history	✓	✗
Email archive	✓	✗
Number of email administrator accounts	Unlimited	1
Report management	✓	✗

Appendix 3 - Troubleshooting LDAP

This section explains how to resolve some common problems that may arise when configuring LDAP.

For full details on working with LDAP, <http://help.comodo.com/topic-157-1-288-5720-Importing-Users-from-LDAP.html>

- **Problem: Unhandled Exception:**

Solution: The exception was not classified.

- **Problem: Size limit exceeded, unable to extract more than users from server. Size limit must be increased on server side or specify more strict query**

Solution: Active Directory server has limitation on the number of search entries which may be iterated during querying. By default, Microsoft Active Directory allows only 1000 search entries. If the server received more than that, the administrator should override the default LDAP search size limit in the Active Directory, or use more strict query

- **Problem: Incorrect filter settings:**

Solution: Filter settings contain incorrect format or AD server doesn't support it.

- **Problem: Incorrect BaseDN settings: ...**

Solution: BaseDN value has incorrect format.

- **Problem: Unable to connect with provided host in BaseDN settings: ...**

Solution: Provided domain name for BaseDN setting cannot be resolved in AD forest tree. Assure a domain name is correct.

- **Problem: Unable to resolve LDAP referral, host unreachable. Users had found before referral might be imported. Possible solution is to use Global Catalog server (port 3268/3269 as default) to avoid resolving referrals.**

Solution: CASG is trying to extract as much as possible information and following referrals to resolve all search entries in a query. If the URL in the referral is unreachable by CASG then the iteration will stop. Only partial result will be provided. That occurs when an administrator uses a private domain and it cannot be accessed with only domain name (the referral contains the list of URLs of the explicit domain names but the information about servers located in the private subnet is absent). To avoid the referrals occurrence in search entries use the Global Catalog server for querying. By default, the port for this server is 3268/3269 and that depends on whether the SSL enabled or not.

- **Problem: Unknown error. Users found before error might be imported. Original exception - ...**

Solution: Search entries has been terminated within the replication process. Please contact support to find a solution.

- **If you do not know your BaseDN, here's a step-by-step guide to determining your BaseDN.**

Most organizations follow a similar convention for their determined BaseDN when the organization sets up its Active Directory. For a company with the domain of example.com, the typically BaseDN is `cn=Users,dc=example,dc=com`

Appendix 4 - Useful Links

This page contains links to external webpages which provide detailed explanations of LDAP features.

What Is the Global Catalog?

<http://technet.microsoft.com/en-us/library/cc728188%28v=ws.10%29.aspx>

Global Catalog and LDAP Searches

<http://technet.microsoft.com/en-us/library/cc978012.aspx>

LDAP Referrals

<http://technet.microsoft.com/en-us/library/cc978014.aspx>

Click the following links for more details <http://help.comodo.com/topic-157-1-288-5720-Importing-Users-from-LDAP.html>

About Comodo Security Solutions

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

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

About Comodo Cybersecurity

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

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

Email: EnterpriseSolutions@Comodo.com