COMODO
Creating Trust Online®

Comodo Antispam Gateway

Software Version 1.10

Administrator Guide

Guide Version 1.10.050213

Comodo Security Solutions
1255 Broad Street
STE 100
Clifton, NJ, 07013

Table of Contents

1 Introduction to Comodo Antispam Gateway 4
1.1 Release Notes 5
1.2 Purchasing License 7
1.3 Adding more Users, Domains or Time to your Account 7
1.4 License Information 11
2 Getting Started 14
2.1 Incoming Filtering Configuration 14
2.1.1 Configuring Your Mail Server 14
2.1.2 Configuring MX Record 15
2.1.2.1 Updating MX Records in Windows 2003/2008 Server 16
2.1.2.2 Updating MX Records on a host using BIND (and the 'named' daemon) 16
2.1.2.3 Updating MX Records for Comodo DNS 16
2.1.2.4 Updating MX Records for GoDaddy 19
2.1.2.5 Updating MX Records for Enom 20
2.1.2.6 Updating MX Records for Network Solutions 21
2.1.2.7 Updating MX Records for Yahoo! Small Business 21
2.1.2.8 Updating MX Records for 1and1 22
2.1.2.9 Updating MX Records for 4D Web Hosting 22
2.1.2.10 Updating MX Records for DNS Park 23
2.1.2.11 Updating MX Records for DreamHost 23
2.1.2.12 Updating MX Records for DynDNS 23
2.1.2.13 Updating MX Records for IX Web Hosting 24
2.1.2.14 Updating MX Records for No-IP 24
2.1.2.15 Updating MX Records in CPanel 25
2.2 Outgoing Filtering Configuration 27
2.2.1 Per-User Authentication 27
2.2.2 Outgoing Smarthost setup 28
2.2.2.1 Configuring QMail to use a Smarthost 28
2.2.2.2 Configuring PostFix to use a Smarthost 29
2.2.2.3 Configuring Sendmail to use a Smarthost 29
2.2.2.4 Configuring Exchange 2000/2003 to use a Smarthost 30
2.2.2.5 Configuring Exchange 2007/2010 to use a Smarthost 30
2.2.2.6 Configuring Exim to use a Smarthost 31
2.2.2.6.1 Configuring Exim / cPanel to use a Smarthost 32
2.2.2.6.2 Configuring Exim / Directadmin to use a Smarthost 34
3 The Administrative Interface 34
3.1 Logging-in to the Administrative Interface 36
3.2 The Dashboard Area 36
3.2.1 Domain Management 37
3.2.1.1 Adding Domains 39
3.2.1.2 Deleting Domains 41
3.2.1.3 Editing Domains 42
3.2.1.4 Managing Domain 43
3.2.1.4.1 Incoming 44

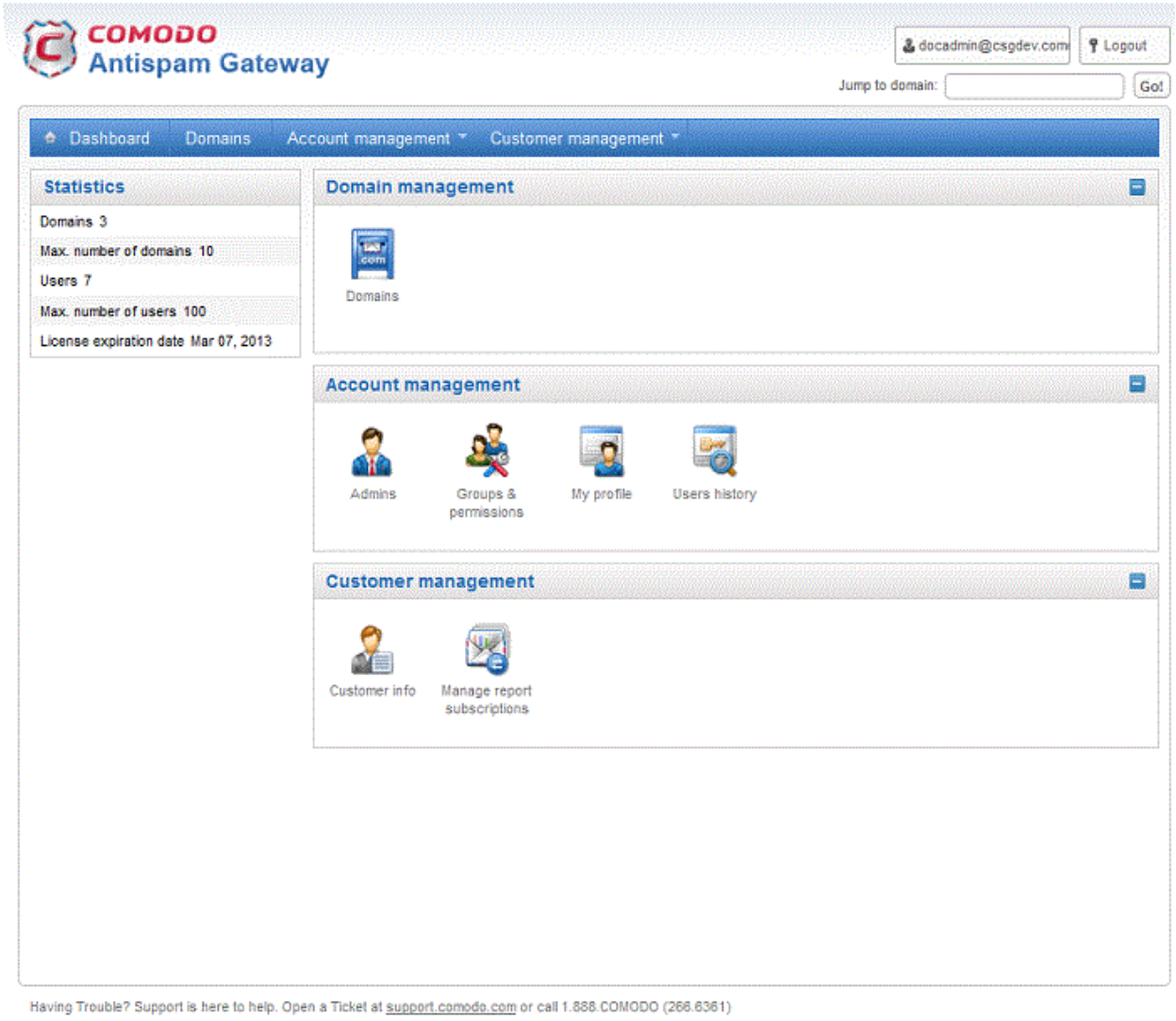
3.2.1.4.2 Outgoing 68
3.2.1.4.3 Email Management 78
3.2.1.4.4 Whitelist / Blacklist 97
3.2.1.4.5 Account Management 113
3.2.1.4.5.1 User Account Management 114
3.2.1.4.5.2 Viewing User History 128
3.2.1.4.5.3 Importing Users from LDAP 130
3.2.2 Administrator Account Management 138
3.2.2.1 Administrators 139
3.2.2.2 Groups & Permissions 143
3.2.2.3 My Profile 149
3.2.2.3.1 Changing Password of the Administrator 149
3.2.2.3.2 Change Settings 150
3.2.2.4 User History 150
3.2.3 Customer Management 150
3.2.3.1 Viewing Customer Information 151
3.2.3.2 Managing Subscriptions for Reports 153
4 CASG Reports - An Overview 156
4.1 Quarantine Report 156
4.2 Domain Statistics Report 157
Appendix 1 – CASG Error Codes 159
About Comodo 160

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



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.

- Purchasing License - How to purchase CASG licenses.
- Adding More Users, Domains Or Time To Your Account - Describes how to obtain domains, add more users to your account.
- License Information - Describes how to keep track of subscription status and various license related alerts.
- Getting Started - Describes how to configure your mail server with the CASG service
  - Incoming Filtering Configuration
  - Outgoing Filtering Configuration
- The Administrative Interface - Provides a snapshot of main functional areas of CASG.
  - Logging-in to the Administrative Interface - How to login into the CASG interface.
  - The Dashboard Area - Describes briefly about Domain management, Account management, Customer management and Statistics area.
  - Domains - Detailed explanation on how to add domains, edit domain and manage domains. This section also deals with adding users to whitelist and blacklist.
  - 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

1.1 Release Notes

Version History	
Version Number	**List of Changes**
Version 1.10	• 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	• 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 • Added user login audits, including name of user, IP, logged time and session duration
Version 1.8	• Added option for administrators to configure idle session timeout period • Various bug fixes
Version 1.7	• 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	• 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	• 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	• 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 • Added ability for administrators to view quarantined email message content through a new CASG window
Version 1.3	• 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	• Added licensing options • Fixed various bugs
Version 1.1	• 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	• Added Mail Quarantine feature • Added Whitelist / Blacklist pages • Added Domain management feature • Added Customer management • Added Account management

1.2 Purchasing License

In order to get started with CASG, you must first purchase the service then configure the service. You have the option to purchase multiple licenses for single or more domains. The number of users and domains that are allowed for all the licenses purchased will be added and displayed in the **Customer Info** page. Follow the 'Buy Now' link on the website to purchase Antispam Gateway. Your Comodo Antispam Gateway account will be created once the signup process is complete - please refer to the email you receive after signup or activation. You can now login into the account with your username and password.

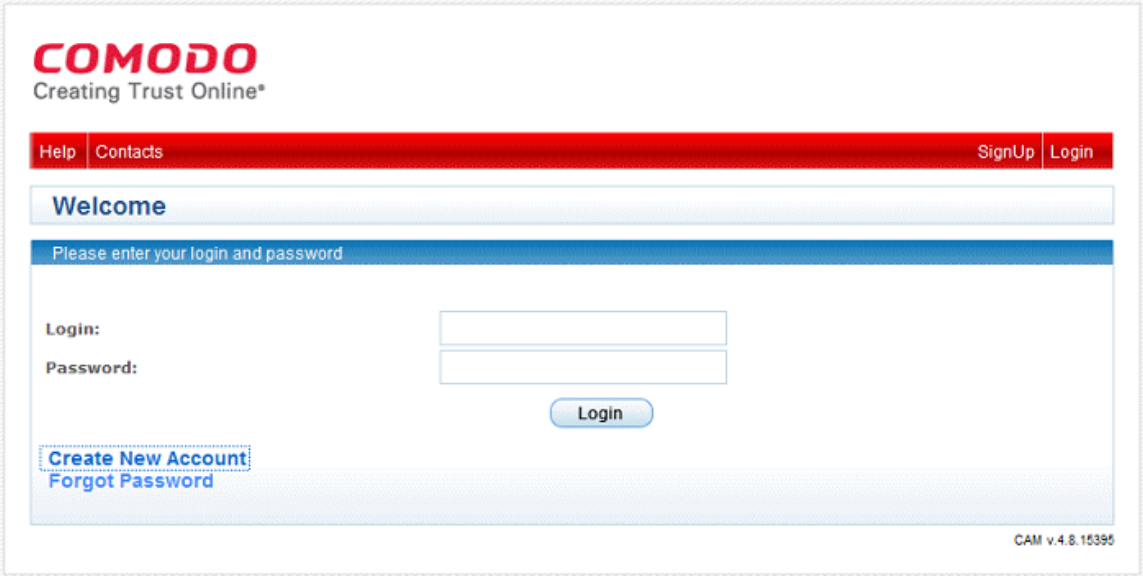
You can view the license details in the main interface after activation. See the section '**License Information**' for more details.

1.3 Adding more Users, Domains or Time to your Account

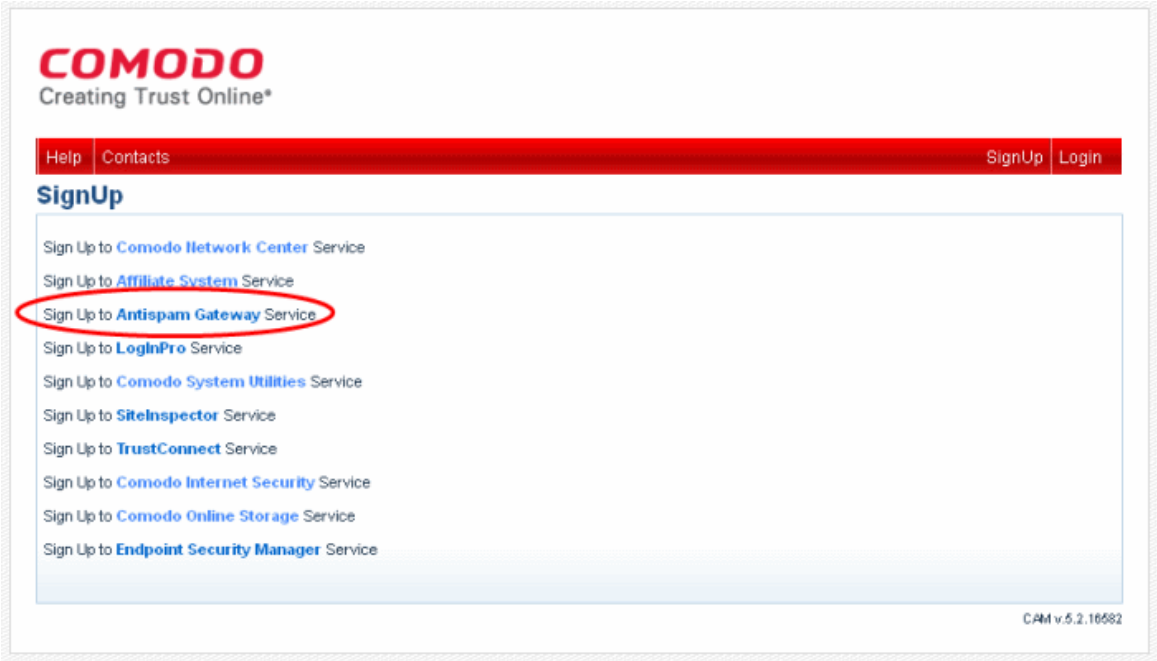
New users, domains and license term extensions as well as multiple licenses can be added to your account by logging into your CAM account at **https://accounts.comodo.com/** . Please read on for a step-by-step guide to this process.

To create CAM account

Visit the Comodo Accounts Manager page at **https://accounts.comodo.com/.** The 'Register or Log In' page will be displayed.



Click 'Create New Account' link. The Signup page for all the services offered by Comodo will be displayed.



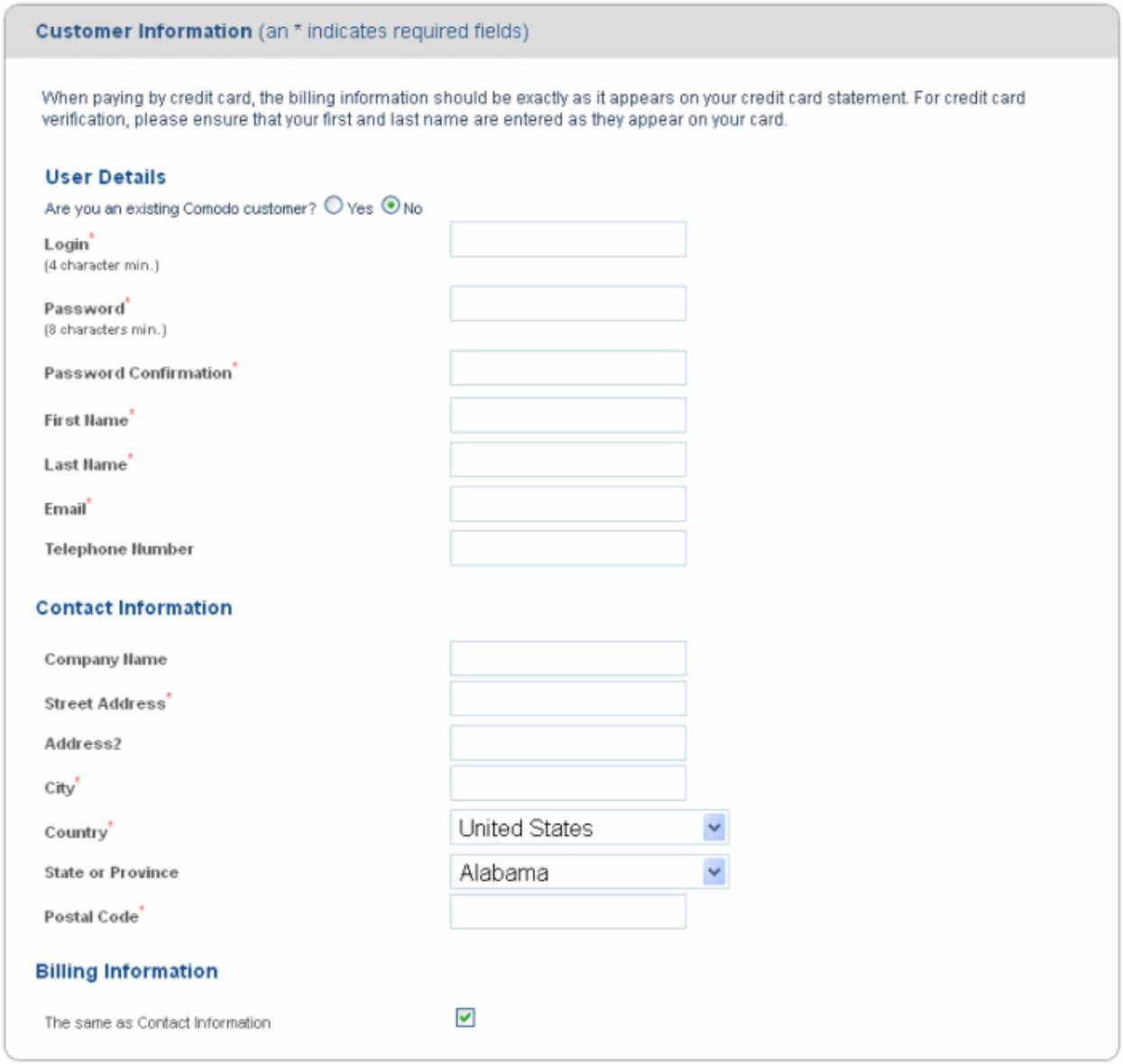
Click 'Sign Up to Antispam Gateway' link. Select the subscription package you want to use from the list displayed. You have the option to purchase single domain license or multi-domain license:

- **Single Domain License** - One email domain, for example, xyz.com or abc.xyz.com, can be configured along with a total number of licensed users.
- **Multi-domain License** - More than one email domains, for example, xyz.com, abc.xyz.com, abc.org and so on, can be configured according to the license along with a total number of licensed users for all CASG-managed domains.

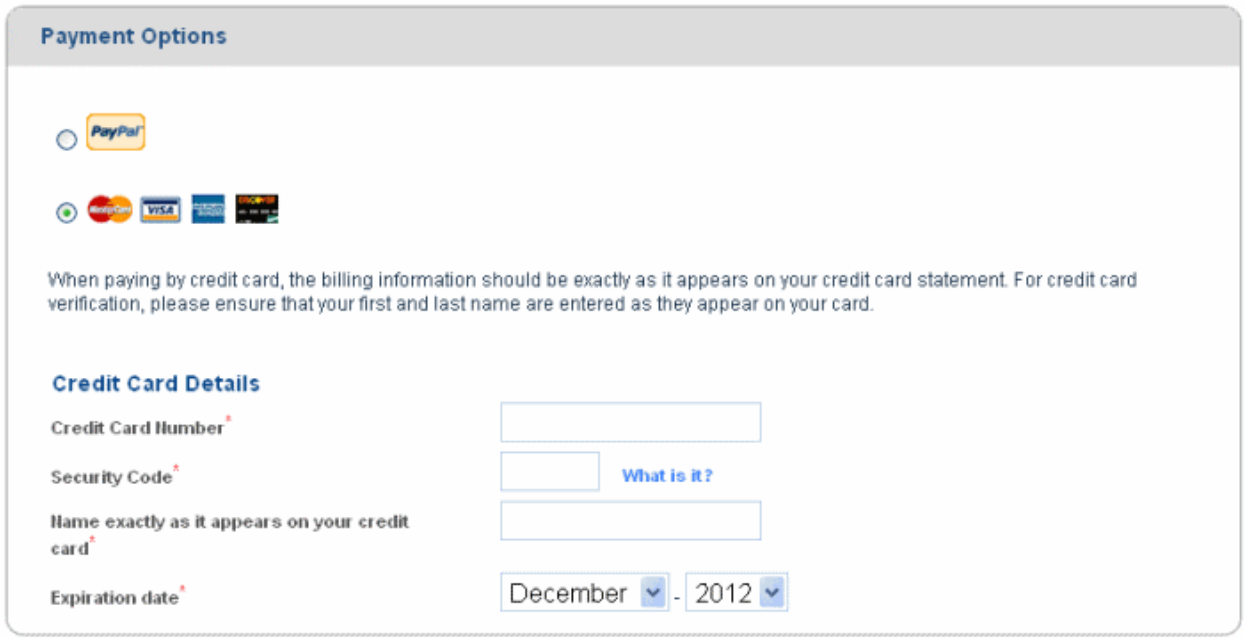
Enter the User Details and Contact Information in the respective sections.

If you already having an account with Comodo, check 'Yes' box. You will only need to enter your Email Address/Login ID , Password, and Contact Information.

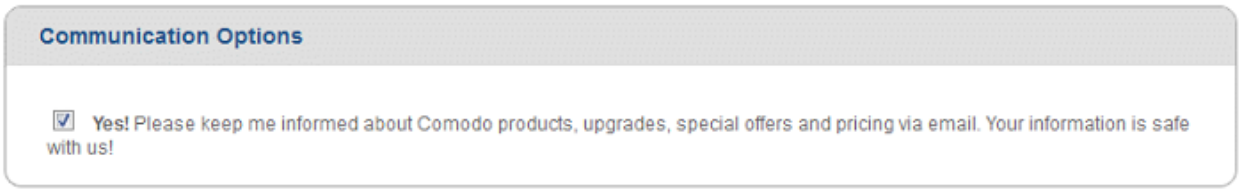
Note: Fields marked with * are mandatory.



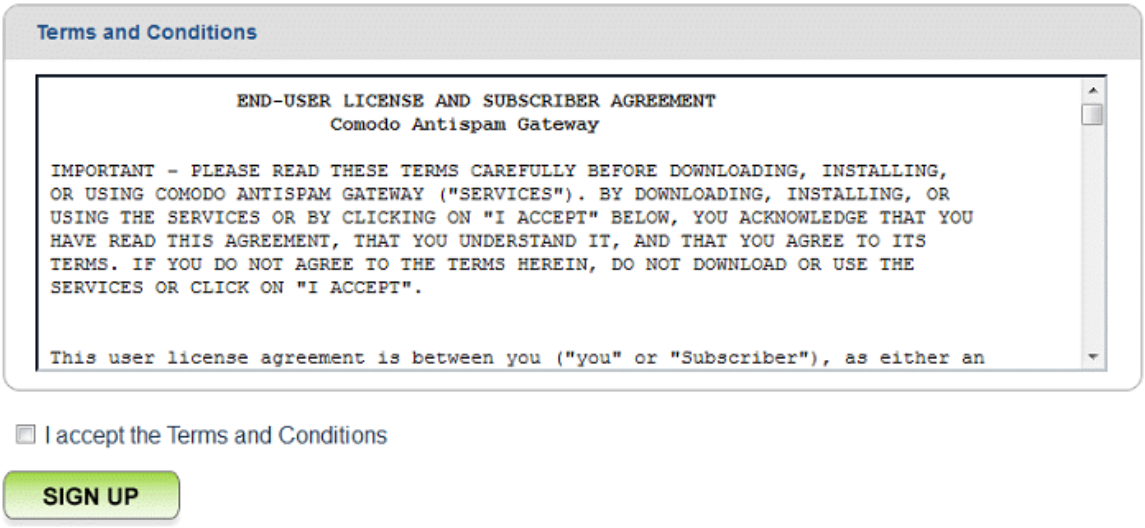
Select the payment method and enter the details.



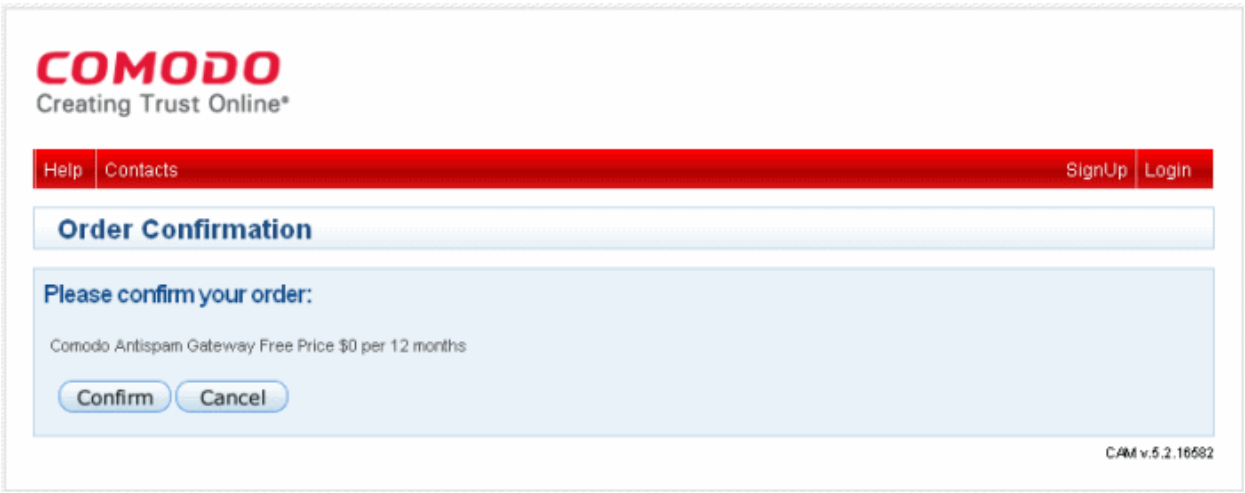
Check the box if you want to be informed about Comodo products updated via mail.



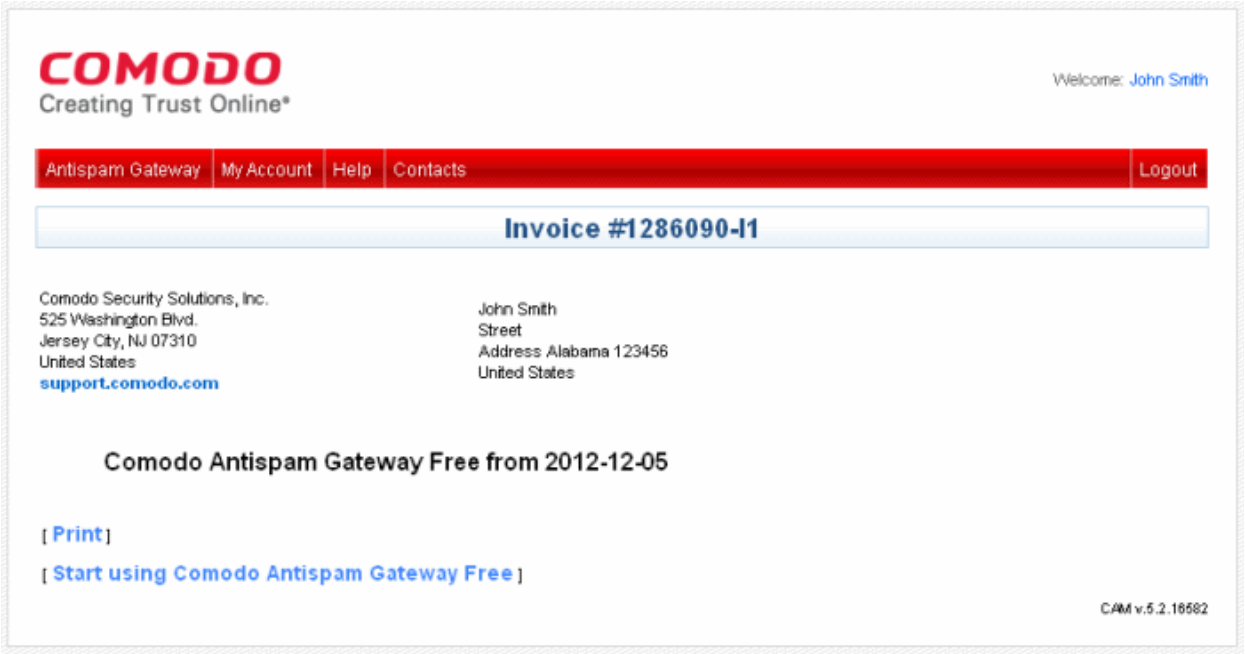
Read the 'End User License and Subscriber Agreement' and accept to it by selecting 'I accept the Terms and Conditions' checkbox. Click 'Sign Up'.



Click the Confirm /Cancel button in the Order confirmation dialog.



The assigned invoice will be displayed.

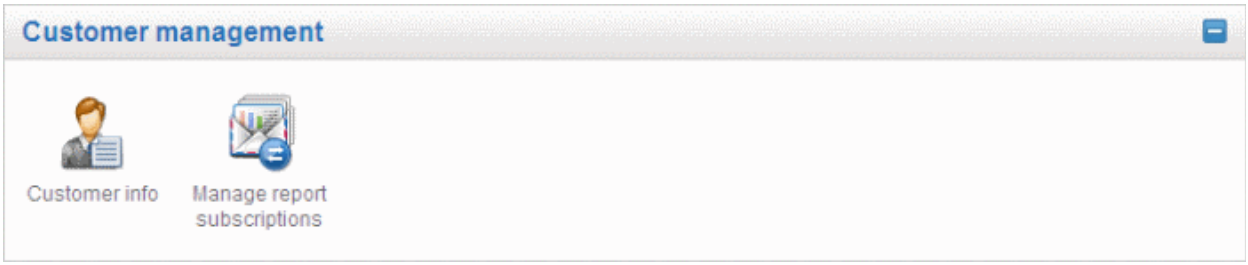


After purchasing a CASG license, you will automatically become an administrator in CASG. Repeat the process for purchasing another CASG license. The number of users and domains that are allowed for all the licenses purchased will be added and displayed in the Customer Info page.

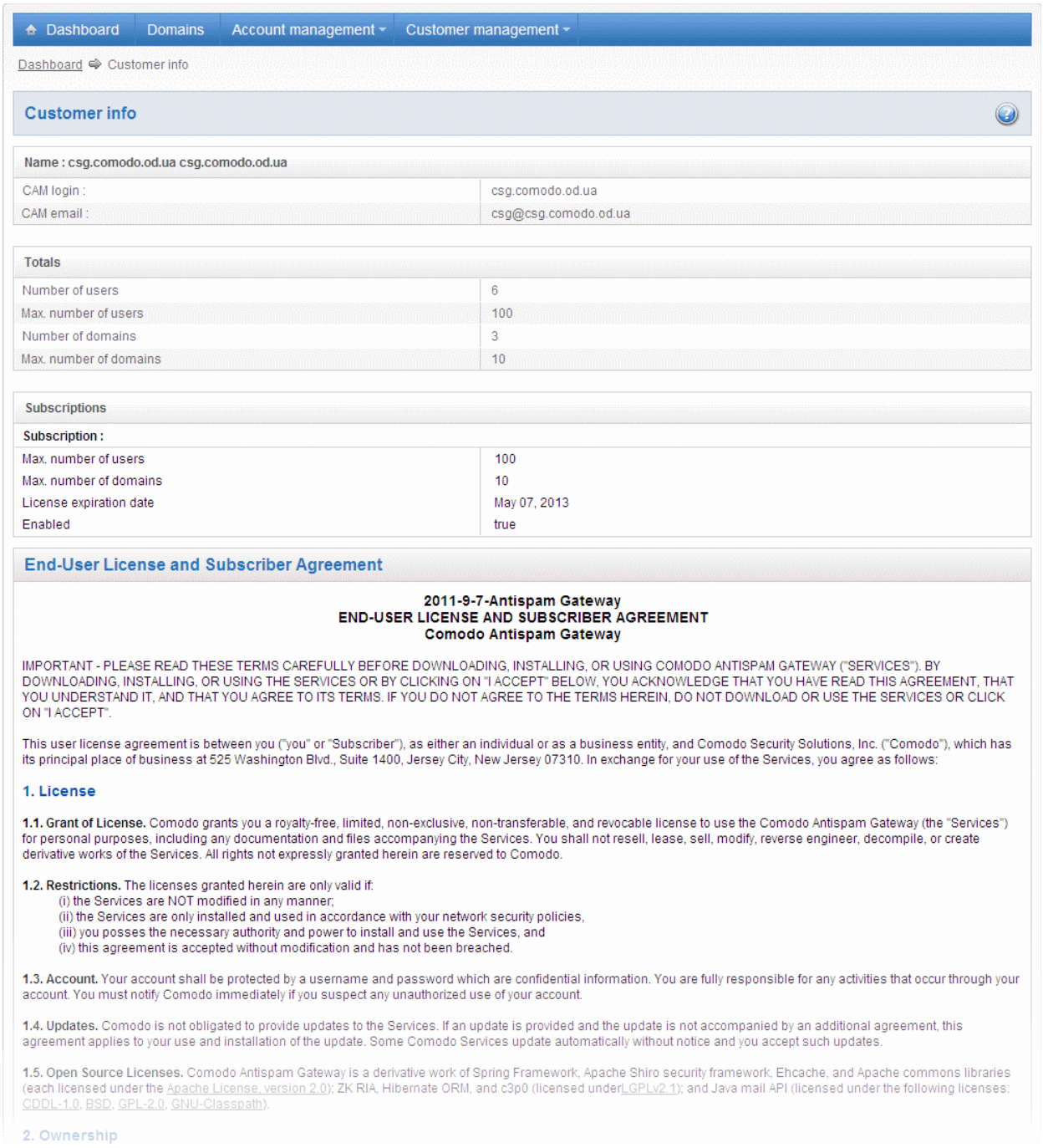
1.4 License Information

After purchasing/licensing has been completed, 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).

You can view your account status in the 'Customer Management' area in the main interface.



- Click 'Customer Info' from the 'Customer management' drop-down menu from the menu bar or the icon in the 'Customer management' configuration area.
- The image below shows an example of Customer Info who has purchased multiple licenses.



In the 'Customer Info' panel you will find the details of subscription(s) for your account. For multiple licenses, the number of users and domains that are allowed for all the licenses purchased will be added and displayed at the bottom most subscription column.

- **Name:** Displays the name of the account.
- **CAM Login**: Displays the login user name for the account in Comodo Accounts Manager (CAM) at https://accounts.comodo.com. The administrator can use this login username to log in to CAM for purchasing additional licenses and renewal of existing licenses.
- **CAM email**: Displays the email address for the account as registered at CAM.

Account Summary

- **Number of Users**: Displays the number of users for all the domains belonging to the account.
- **Max. Number of Users:** The maximum number of users that can be added as per all the subscriptions made for the account, that is, number of users cannot exceed the number given in this field for all domains included.

- **Number of Domains:** Displays the number of domains belonging to that account.
- **Max. Number of Domains:** The maximum number of domains that can be configured as per all the subscriptions made for the account.

Details on Subscriptions

- **Max. Number of Users**: The maximum number of users that can be added for the account as per the specific subscription, that is, number of users cannot exceed the number given in this field for all domains included.
- **Max. Number of Domains**: The maximum number of domains that can be configured as per the specific subscription.
- **License Expiration Date:** Provides details about the expiry date of the license for the specific subscription.
- **Enabled:** Displays whether the subscription is active or not.

End-User License and Subscriber Agreement

- **End-User License and Subscriber Agreement:** Displays the complete End-User License and Subscriber Agreement.

The 'Customer Info' panel alerts the administrator about license(s) expiration date and if Domain/Users limit is exceeded.

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,

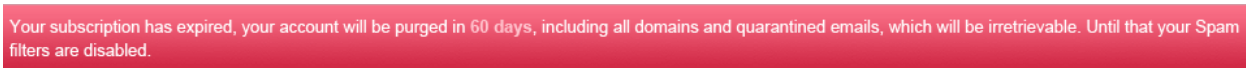
Your Comodo Antispam Gateway account is due to expire in 5 days.

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 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.



Note: The period after which all domains and quarantined emails for your account that will purged depends on the settings configured in CASG.

During the configured period after license expiry, your emails will continue to be delivered to your domain via CASG but without any spam filtering. During this period, you cannot add new domains and new users. Option to enable quarantine is also disabled and incoming Spam detection settings screen for every domain in your account will display that Quarantine is disabled. After the configured period, all domains and quarantined mails in CASG for your account will be purged.

Users of the account can use the service normally during this period. After the configured period, if an user tries to login with his/her credentials, 'Your login or password is incorrect' message will be displayed.

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 3. 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 5. 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 Getting Started

Once an account with Comodo for CASG has been created, the next step is configuring your mail server with the CASG service and setting up incoming and outgoing filtering. Click on the links below for more details.

- 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

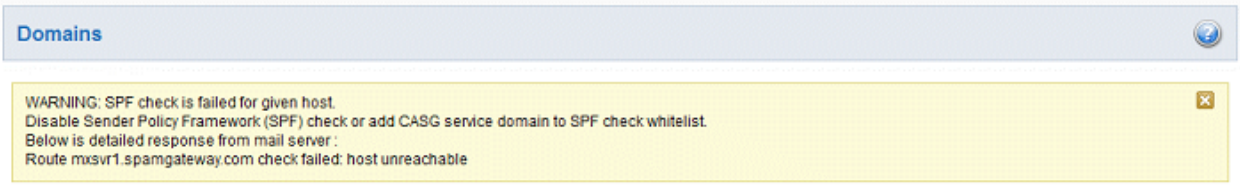
2.1.1 Configuring Your Mail Server

Step 1: Disable Sender Policy Framework (SPF) check or add CASG service domains to SPF check whitelist.

The CASG service domains are:

- mxsrv1.spamgateway.comodo.com
- mxsrv2.spamgateway.comodo.com

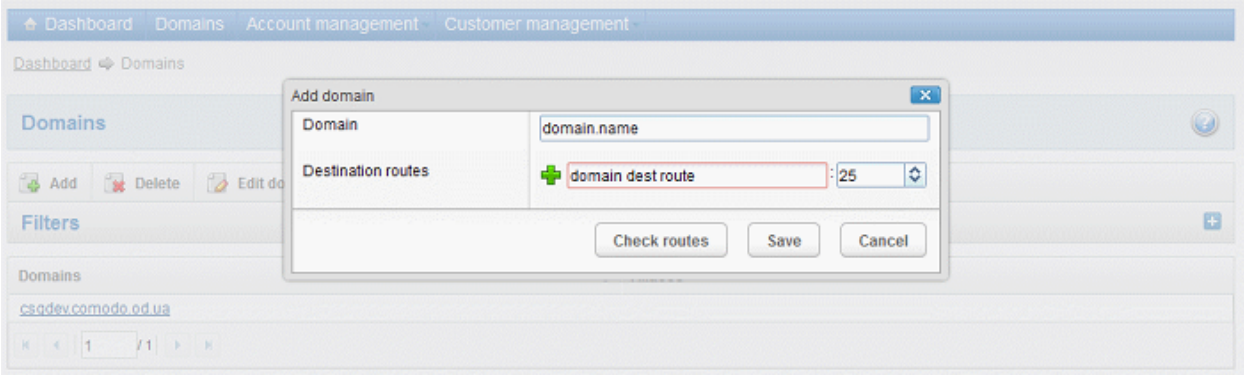
If the above step is not carried out, the following error message may appear while adding a domain.



Step 2: Add your domain to CASG service.

To add domain:

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



Step 3: Point mail server MX records to CASG service domain. See the next section 'Configuring MX Record' for more details.

2.1.2 Configuring MX Record

The next important 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 primary 'mxsrv1.spamgateway.comodo.com' and secondary 'mxsrv2.spamgateway.comodo.com'. If third-party MX servers are being used, then point the records to 'mxsrv{1,2}.spamgateway.comodo.com'.

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 Updating MX Records in Windows 2003/2008 Server

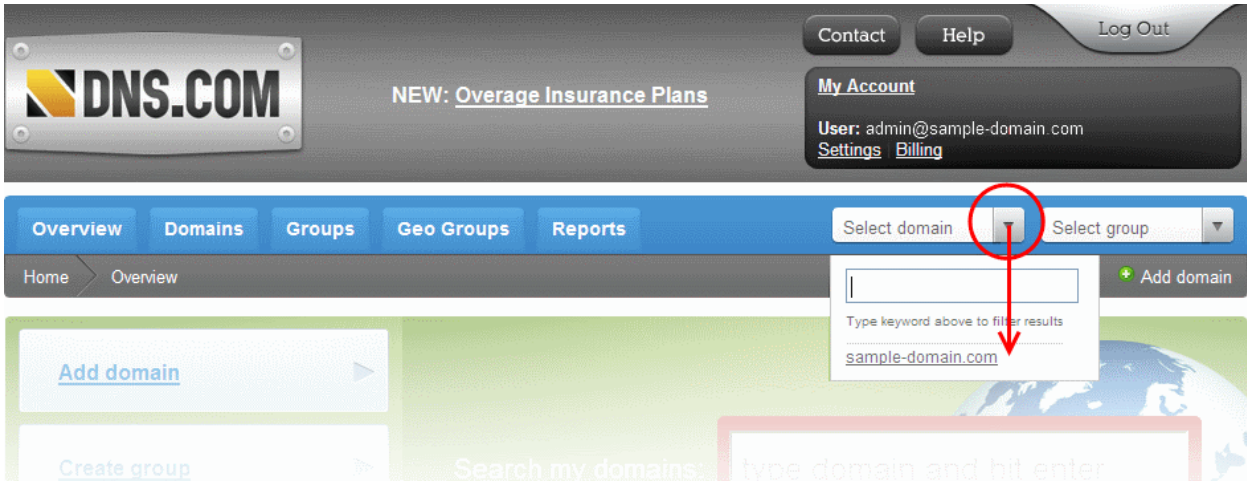
1. Open Control Panel by clicking Start > Control Panel and click 'Administrative Tools'.
2. Select 'DNS'.
3. Open the 'Forward Lookup Zones' folder.
4. To back up the current configuration, right-click the sub-folder for the mail domain you are configuring, select 'export' from the context sensitive 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. Enter a new record for primary mail server with a lowest priority number and enter its FQDN value as mxsrv1.spamgateway.comodo.com and click OK.
8. Enter a new record for secondary mail server with the next lowest priority number and enter its FQDN value as mxsrv2.spamgateway.comodo.com and click OK.
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 Updating MX Records on a host using BIND (and the 'named' daemon)

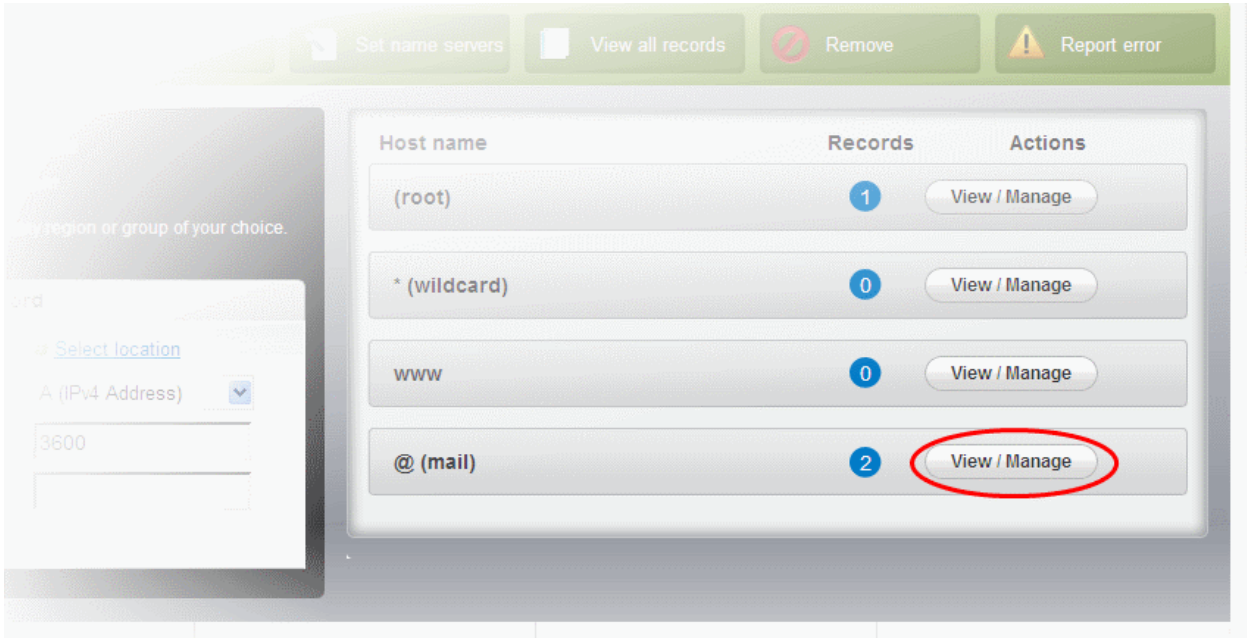
1. Make a backup copy of the zone file (or named.conf) that you intend to edit for MX record updates.
2. Open the Zone file for the mail domain you are configuring (or go to the part of named.conf being used for that zone)
3. Delete all the existing “MX” lines for that domain.
4. Enter a new “IN MX” record with the lowest preference value and enter the host name as “mxsrv1.spamgateway.comodo.com” for the primary mail server.
5. Enter a new “IN MX” record with the next lowest preference value and enter the host name as “mxsrv2.spamgateway.comodo.com” for the secondary mail server.
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 Updating MX Records for Comodo DNS

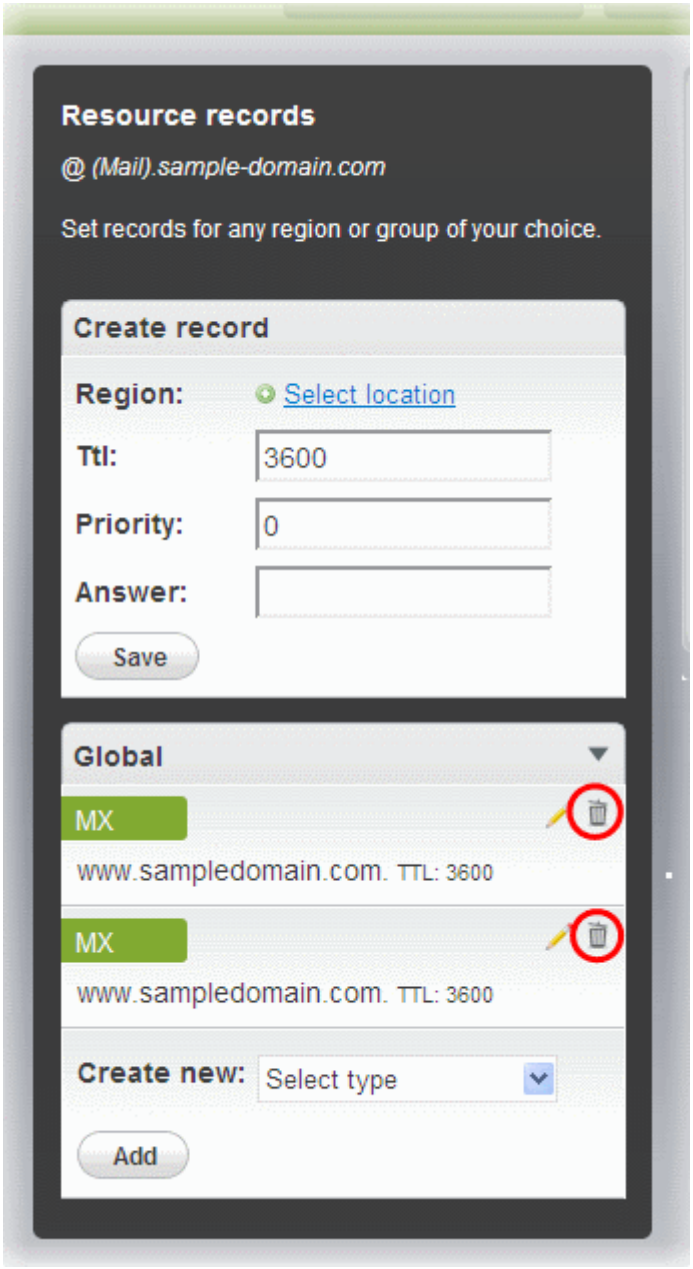
1. Log in to DNS.com administrative console at https://dns.com/login/ by entering your login email address and password.
2. Select the domain for which you want to update the MX records, from the "Select domain" drop down menu.



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 thrash 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 “mxsrv1.spamgateway.comodo.com” in the 'Answer' field
    - Click '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 “mxsrv2.spamgateway.comodo.com” in the 'Answer' field.
    - 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.

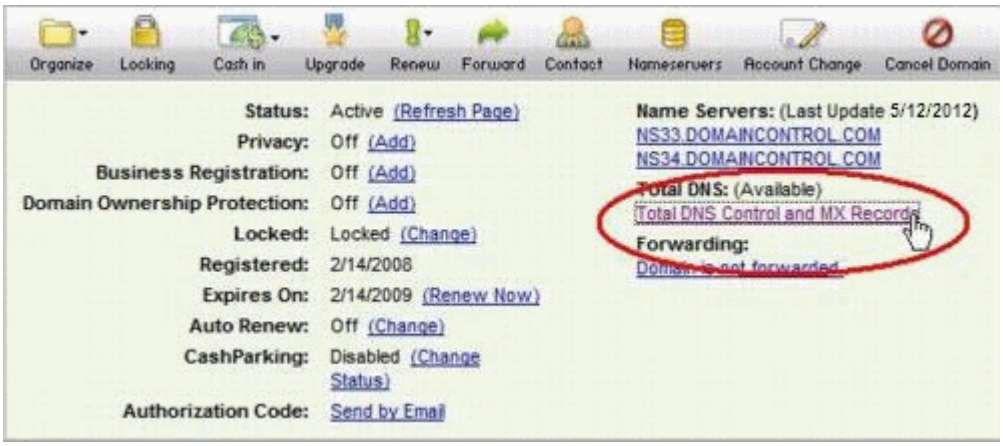
Setup should now be complete and mail filtering effected on all configured domains. If you experience problems, please open a ticket at support.comodo.com or call 1.888.COMODO (2666.6361) and have your account number ready. We have experienced

technicians on hand to help troubleshoot any configuration issues.

2.1.2.4 Updating 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.

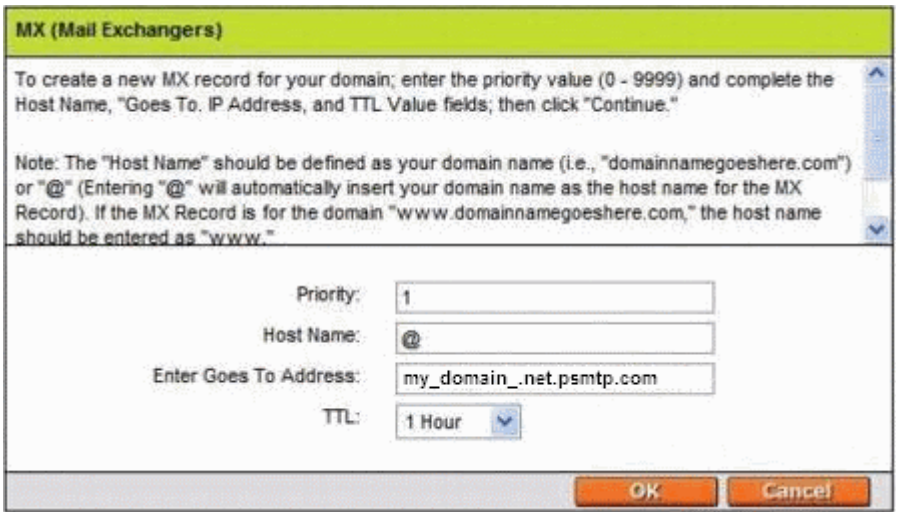
3. Select the domain for which you want to update the MX records, from the 'Domain Name' column.
4. Click 'Total DNS Control and MX Records' from the Details page.



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.

6. 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 “mxsrv1.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 “mxsrv2.spamgateway.comodo.com”.
- 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 Updating MX Records for Enom

1. Log in to Enom administrative console at https://www.enom.com/login.aspx by entering your 'Login ID', 'Password' and clicking 'Login'.
2. Click the 'Domains' tab and select 'My Domain Names'. 'Manage Domains' page will be opened
3. Choose the domain for which the MX records are to be updated.
4. Select the + icon under the 'Total DNS Control' list in the 'Domain Details' panel. A sub-list will appear.
5. 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 “mxsrv1.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 “mxsrv2.spamgateway.comodo.com”.
- 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 Updating 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.

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

Priority	Mail Server
1	mxsrv1.spamgateway.comodo.com
2	mxsrv2.spamgateway.comodo.com

7. 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 Updating MX Records for Yahoo! Small Business

1. 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'.
2. Click 'Domain' from he tool bar.
3. Click 'Manage Advanced DNS Settings'.
4. Click 'Change MX Records'.
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 '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.

6. Enter the MX record for primary email server as “mxsrv1.spamgateway.comodo.com” in the first open text box.
7. Set the priority for the primary email server as “1”
8. Enter the MX record for secondary email server as “mxsrv2.spamgateway.comodo.com” in the second open text box.
9. Set the priority for the secondary email server as “2”
10. 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 Updating 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	mxsrv1.spamgateway.comodo.com
MX 2/Prio	mxsrv2.spamgateway.comodo.com

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 Updating 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	mxsrv1.spamgateway.comodo.com
Secondary	mxsrv2.spamgateway.comodo.com

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 Updating 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 “mxsrv1.spamgateway.comodo.com” and click 'Update'
   - Replace the hostname at 2nd priority row with “mxsrv2.spamgateway.comodo.com” and click 'Update'
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 Updating 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 two text boxes, enter:
   - “mxsrv1.spamgateway.comodo.com”
   - “mxsrv2.spamgateway.comodo.com”
6. 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 Updating 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 “mxsrv1.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 “mxsrv2.spamgateway.comodo.com”
    - 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 Updating 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'.
8. 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	mxsrv1.spamgateway.comodo.com
Leave Blank	2	mxsrv2.spamgateway.comodo.com

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 Updating MX Records for No-IP

1. Log in to No-IP administrative console at https://www.no-ip.com/login/ by entering your login email address and password.
2. Click 'Host/Redirects' from the left hand side navigation.
3. Click 'Modify' beside the domain name for which the MX records are to be updated.
4. Navigate to 'Mail Options' section at the bottom of the page
5. Replace the MX record entry at the first field with “mxsrv1.spamgateway.comodo.com”
6. Replace the MX record entry at the second field with “mxsrv2.spamgateway.comodo.com”
7. Delete the other MX records.

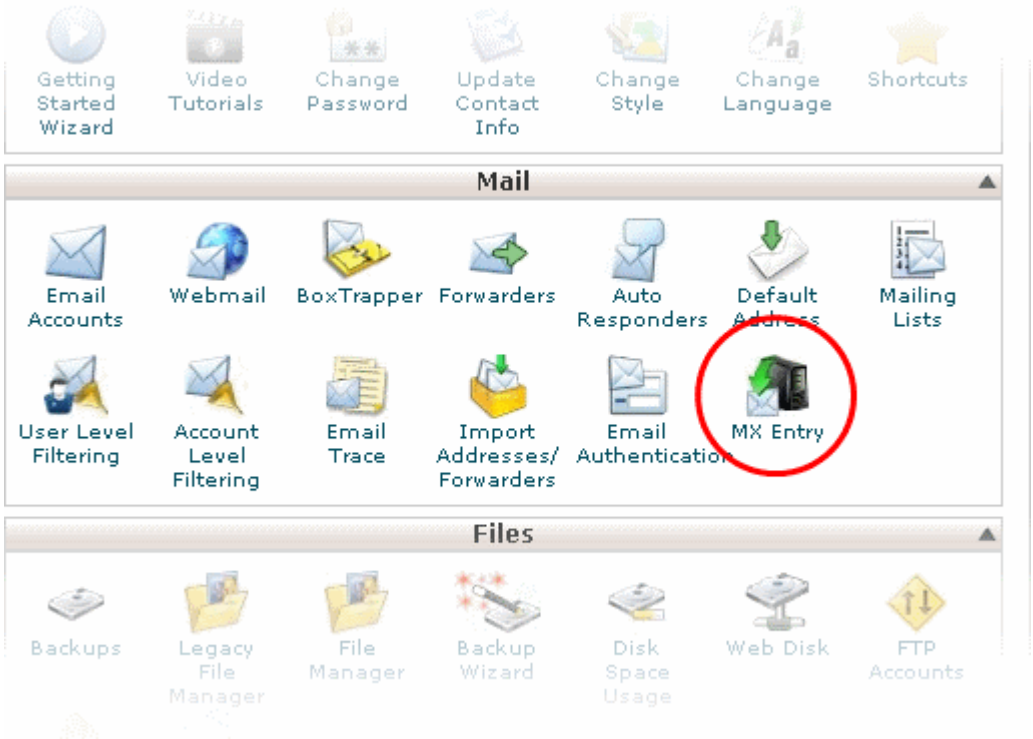
Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Edit the 'MX Records to set the priority with higher numbers like 10, 20 and so on for the existing records. You can delete these records at a later time after your changes have taken effect.

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 Updating MX Records in CPanel

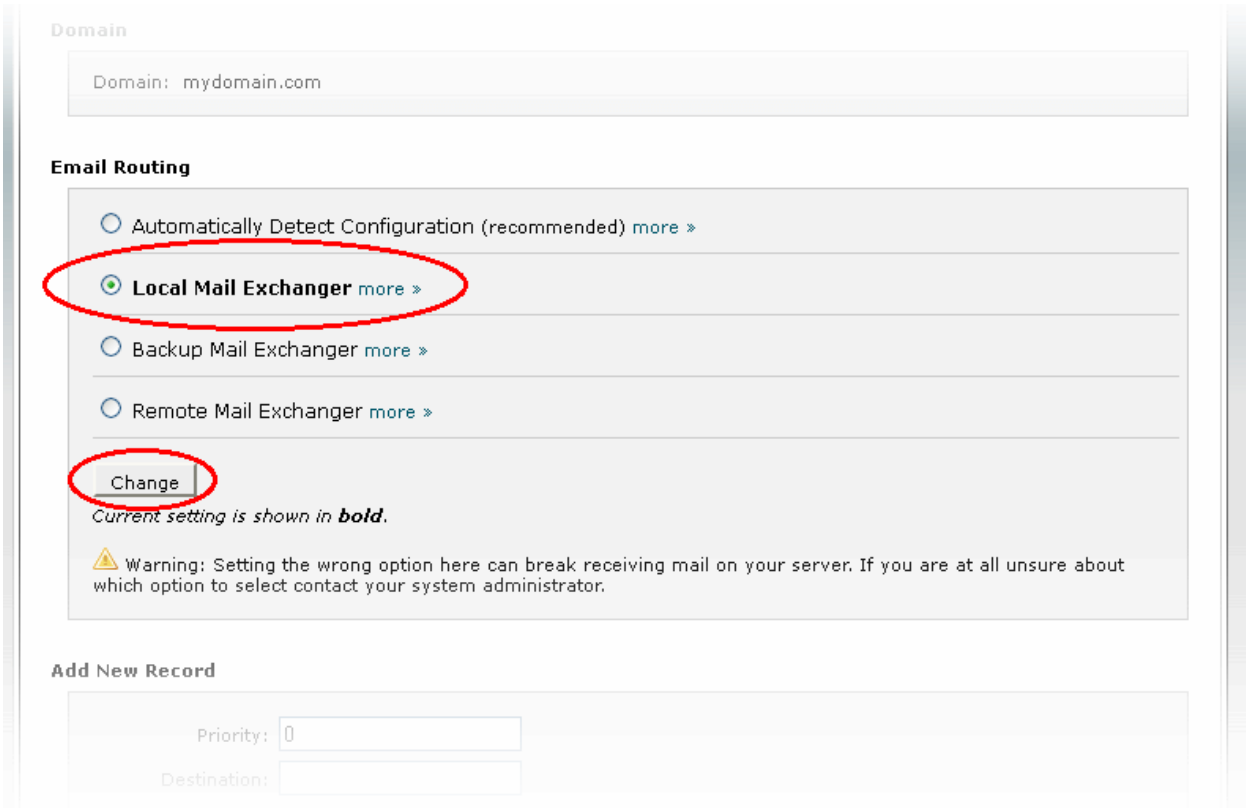
This section explains how to update MX records for your domain if you or your web hosting service provider use CPanel as webhosting control interface.

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

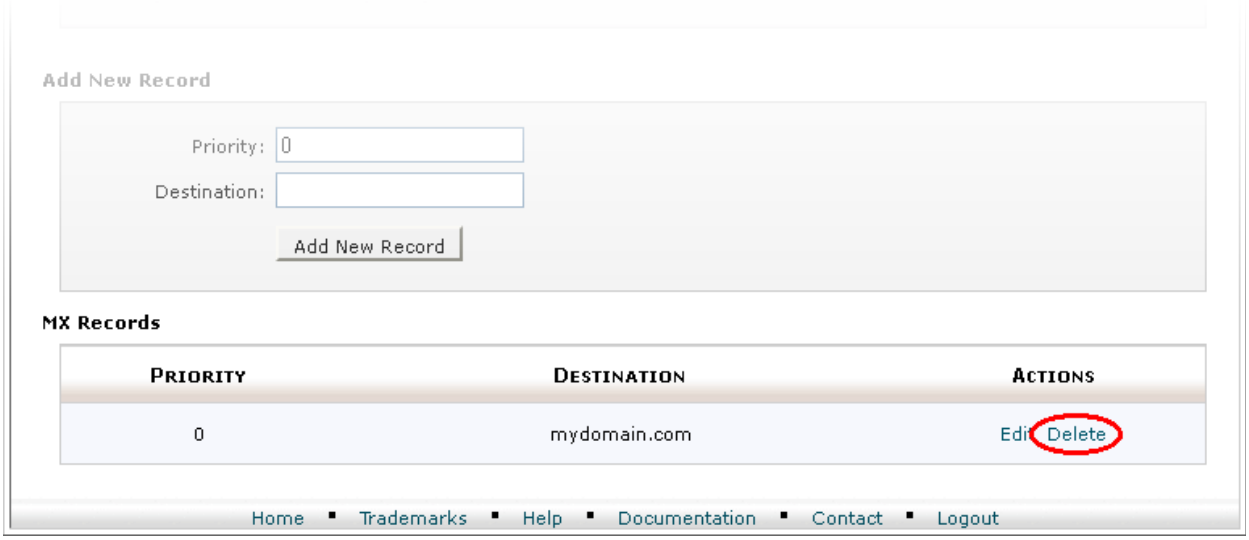


The MX Entry Maintenance panel will be opened.

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.

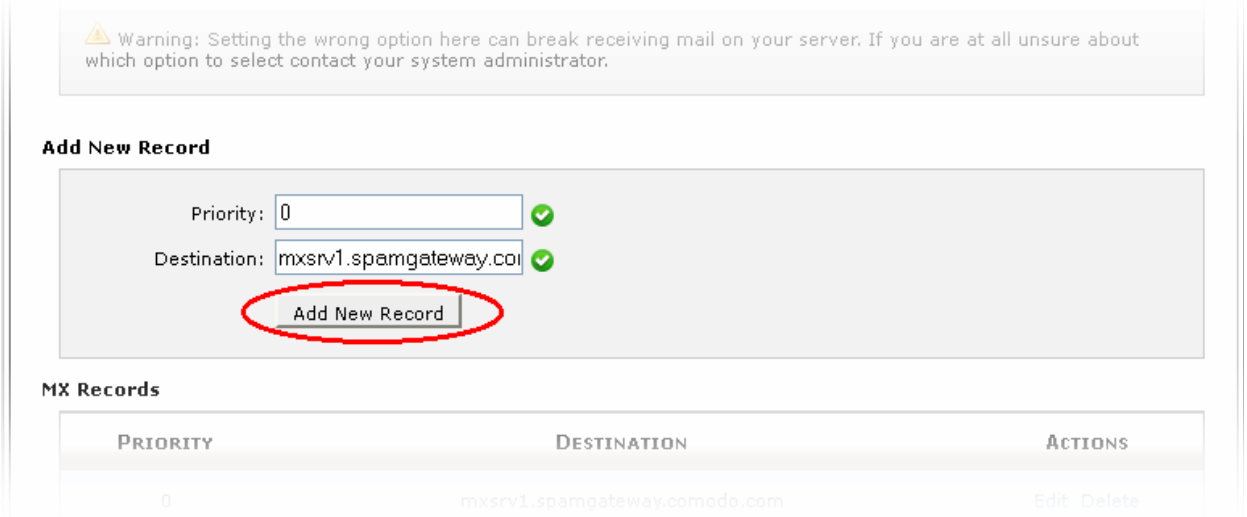


5. Delete the entries under 'MX Records' by clicking the 'Delete' links



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 “mxsrv1.spamgateway.comodo.com” in the Destination field
   - Click 'Add New record'. The new MX Record pointing to CASG service will be added



7. Set the secondary mail server under 'Add New Record'
    - Enter '1' in Priority field
    - Enter “mxsrv2.spamgateway.comodo.com” in the Destination field
    - Click 'Add New record'. The new MX Record pointing to CASG service will be added

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

CASG allows you to configure outgoing filter that is independent of incoming email filtering. 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 the following links for more details.

- Per-user authentication
- Outgoing Smarthost setup

Note: You can use only one of the methods, Per-user authentication or Outgoing Smarthost setup, for outgoing email filtering.

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.

- Configuring QMail
- Configuring PostFix
- Configuring Sendmail
- Configuring Exchange 2000/2003
- Configuring Exchange 2007/2010
- Configuring Exim
    - Configuring Exim / cPanel
    - Configuring Exim / Directadmin

2.2.2.1 Configuring 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 'mxsrv1.spamgateway.comodo.com' on port 587 as outgoing server:

echo ":mxsrv1.spamgateway.comodo.com:587" > /var/qmail/control/smtproutes

This command will set qmail that all your mails will be routed to mxsrv1.spamgateway.comodo.com:587 (**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.

echo "example.com:mxsrv1.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 Configuring PostFix to use a Smarthost

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:

relayhost = mxsrv1.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**:

example.com smtp:mxsrv1.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 trough the Smarthost.

2.2.2.3 Configuring Sendmail to use a Smarthost

Routing all mails to a smarthost :

Edit**/etc/sendmail.cf** and add the following line:

DSmxsrv1.spamgateway.comodo.com

Restart Sendmail.

2.2.2.4 Configuring Exchange 2000/2003 to use a Smarthost

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 **mxsrv1.spamgateway.comodo.com.**
- 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 Configuring Exchange 2007/2010 to use a Smarthost

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 **mxsrv1.spamgateway.comodo.com** (you need to use port 587).

If you have more then 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 smarthost with Username 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'.
- Enter **mxsrv1.spamgateway.comodo.com**, **mxsrv2.spamgateway.comodo.com** in the FQDN section.
- Click 'Change' under the smart-host authentication.
- Select '**Basic Authentication**' and tick the TLS box .
- Add your newly created username and password.
- Click 'OK '.

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 Configuring Exim to use a Smarthost

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 mxsrv1.spamgateway.comodo.com::587
  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 mxsrv1.spamgateway.comodo.com::587 ;

domain.example.org mxsrv1.spamgateway.comodo.com::587
```

Restart Exim for the changes to take effect.

2.2.2.6.1 Configuring 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 mxsrv1.spamgateway.comodo.com::587

smarthost_regular:
  driver = manualroute
  domains = !+local_domains
  transport = remote_smtp_smart_regular
  route_list = $domain mxsrv1.spamgateway.comodo.com::587
```

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 trough 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 = "* mxsrv1.spamgateway.comodo.com::587 byname"
host_find_failed = defer
no_more
```

Add a Transport to the Transport Configuration Box.

```
spamgateway_smtp:
driver = smtp
hosts = mxsrv1.spamgateway.comodo.com
hosts_require_auth = mxsrv1.spamgateway.comodo.com
hosts_require_tls = mxsrv1.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
```

2.2.2.6.2 Configuring 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 mxsrv1.spamgateway.comodo.com::587
  no_more
```

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

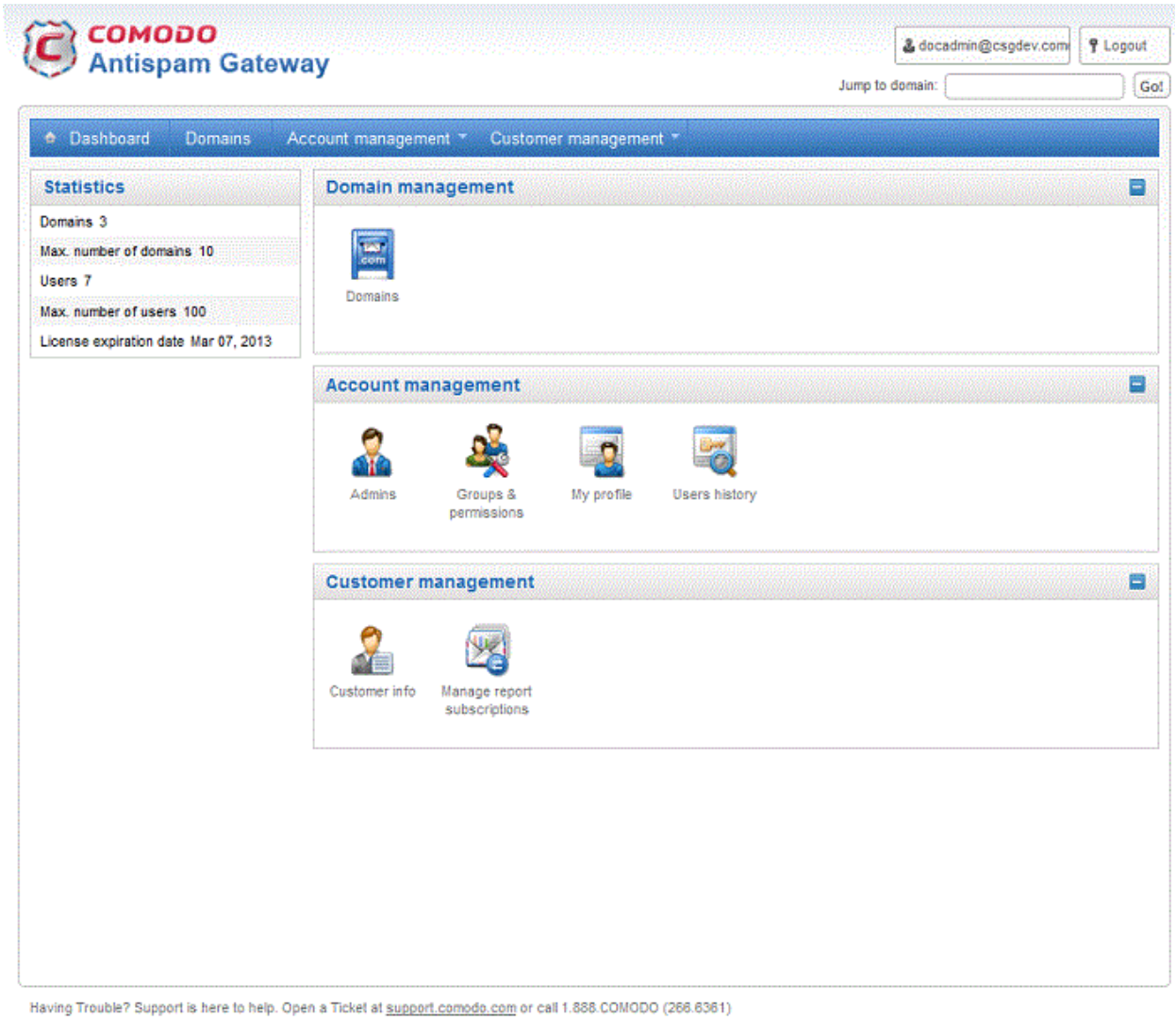
```
 spamgateway_smarthost_transport:
  driver = smtp
  hosts_require_tls = *
```

Restart Exim.

3 The Administrative Interface

The Dashboard area of Comodo Antispam Gateway (CASG) allows administrators to take overall control of domain, account and customer management.

The interface is divided into three areas - Domain Management, Account Management and Customer Management. Each of these areas can accessed by clicking the respective links in the top navigation. Clicking 'Dashboard' will return you to a summary page that displays a choice of these three areas. The left side of the interface displays statistics relevant to the specific task at hand. Within these three main areas, there are a number of other functions that enable the administrator to add domains, edit domains, add administrators and many more. At the top right of the interface, login details of the administrator is displayed. An administrator who manages many accounts can easily jump to a particular account by entering the domain name in the 'Jump to domain' box and then clicking the 'Go' button. The image below shows the admin interface after logging in.



Main Functional Areas

- **Domain Management** - Provides a snapshot of domains in CASG for your account and serves as a launchpad for adding, deleting, editing and managing domains. In this area the administrators can set filters, view quarantined mails, set email restrictions. See **Domain Management** for more details.
- **Account Management** - Enables the administrator to add other administrators, delete or edit an existing administrators. Currently logged in administrator also can change his/her password, manage their subscription to periodical domain and quarantine summary reports in this area. An administrator also can create groups and permissions can be configured for these groups. Users then can be added to these groups that will impose a common permission policy for these users. The administrators can also view a user history for *all* domains within a particular date range. See **Account Management** for more details.
- **Customer Management** - Enables the administrator to view the details of the customer such as name, maximum number of users, maximum number of domains, license expiration date and whether the customer is enabled or not. Also the administrator can manage the subscription of periodical domain and quarantine summary reports for the customer, set the language for the messages sent from CASG according to the location of the administrators. See **Customer Management** for more details.
- **Statistics** - Displays the Statistics for the current customer. If you select 'Manage Domain' in the Domains Management area this block will contain the statistics for the current domain.

Note: You can navigate the interface either by using the drop-down menus in the menu bar or the icons in the main configuration area.

Clicking the **support.comodo.com** link at the bottom of interface takes you to the Comodo support web page, an online knowledge base and support ticketing system. The fastest way to get further assistance in case you find any problem using CASG.

3.1 Logging-in to the Administrative Interface

As CASG is a web application, you can login into your account using any Internet browser by entering https://antispamgateway.comodo.com/admin/ in the address bar of the browser.

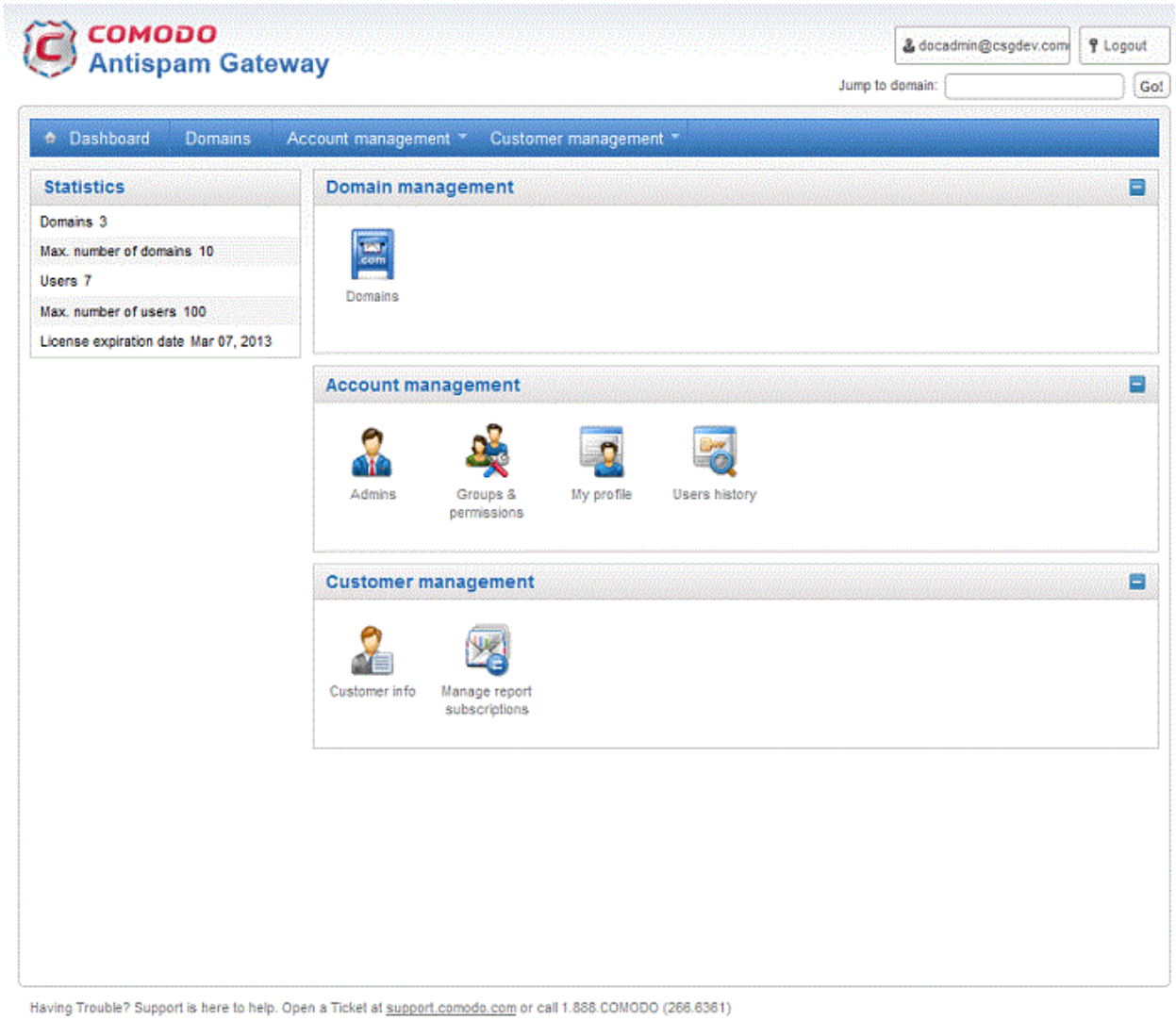
- Login to the interface with your CASG username and password.

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.

3.2 The Dashboard Area

The Dashboard area of CASG has three main functional areas and in the left side of the administrative interface is Statistics, which provides details of a selected task.



- **Domain Management** - Provides a snapshot of domains in CASG for your account and serves as a launchpad for adding, deleting, editing and managing domains. In this area the administrators can set filters, view quarantined mails, set email restrictions. See **Domain Management** for more details.
- **Account Management** - Enables the administrator to add other administrators, delete or edit an existing administrators. Currently logged in administrator also can change his/her password, manage their subscription to periodical domain and quarantine summary reports in this area. An administrator also can create groups and permissions can be configured for these groups. Users then can be added to these groups that will impose a common permission policy for these users. See **Account Management** for more details.
- **Customer Management** - Enables the administrator to view the details of the customer such as name, maximum number of users, maximum number of domains, license expiration date and whether the customer is enabled or not. Also the administrator can manage the subscription of periodical domain and quarantine summary reports for the customer, set the language for the messages sent from CASG according to the location of the administrators. See **Customer Management** for more details.
- **Statistics** - Displays the Statistics for the current customer. If you select 'Manage Domain' in the Domains Management area this block will contain the statistics for the current domain.

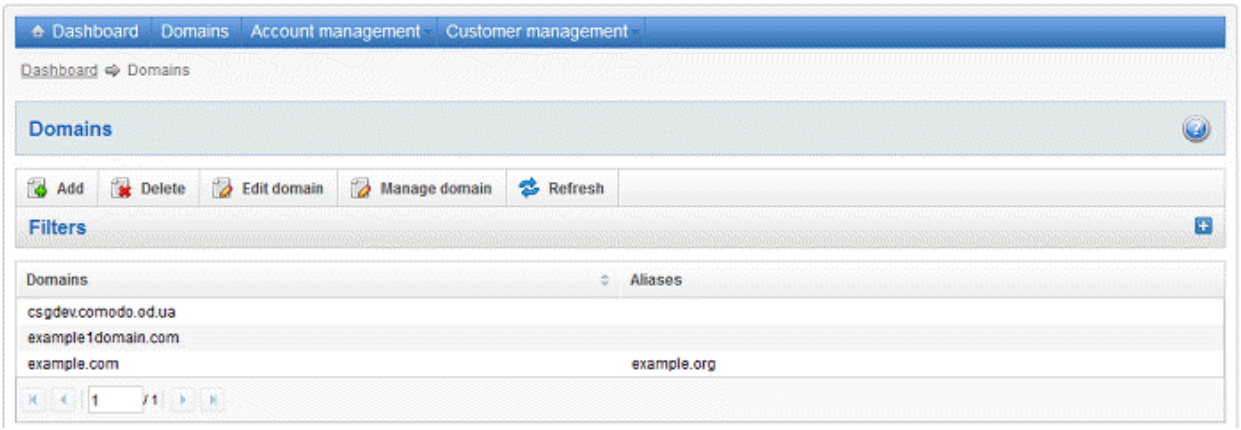
Various interfaces will display a help button at the top right side of the interface. Clicking on this help button will take you to the respective help page of CASG online help guide for more detailed explanation.

3.2.1 Domain Management

As the name suggests, the The 'Domains' area of the interface allows administrators to perform domain management tasks such as adding, deleting editing a domain. Various settings such as email size restrictions and extensions of attached files in emails can be configured for any listed domain.

Tip: CASG also periodically generates Domains reports containing a summary of all the mail activities for the domain. The reports are sent to the administrators through email. Administrators can configure for such reports through **Dashboard** > **Account Management** > **Admin** > **Add Administrators** or **Edit Administrators**. Refer to **CASG Reports - An Overview** for more details.

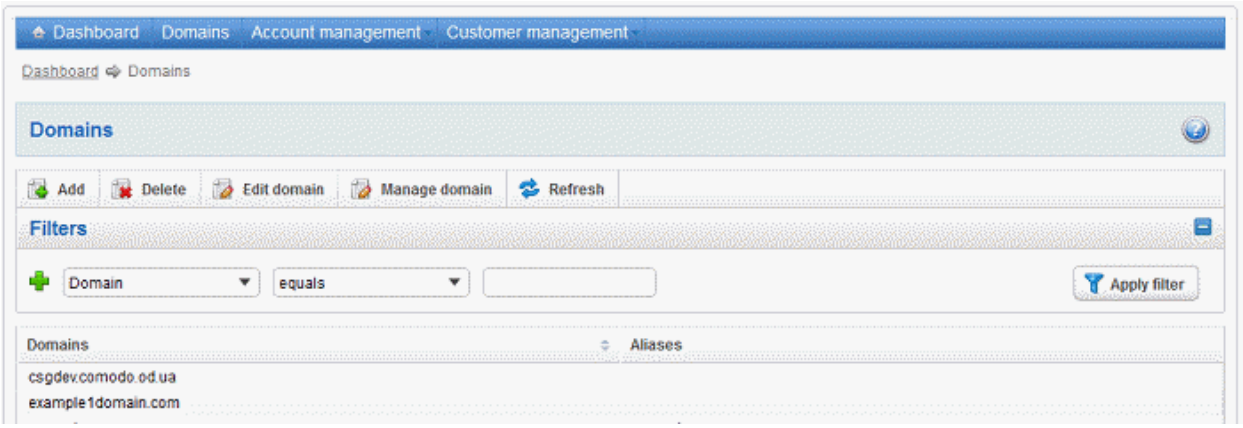
Click the Domains icon in the main configuration area or the 'Domains' tab in the menu bar to open the Domains area.



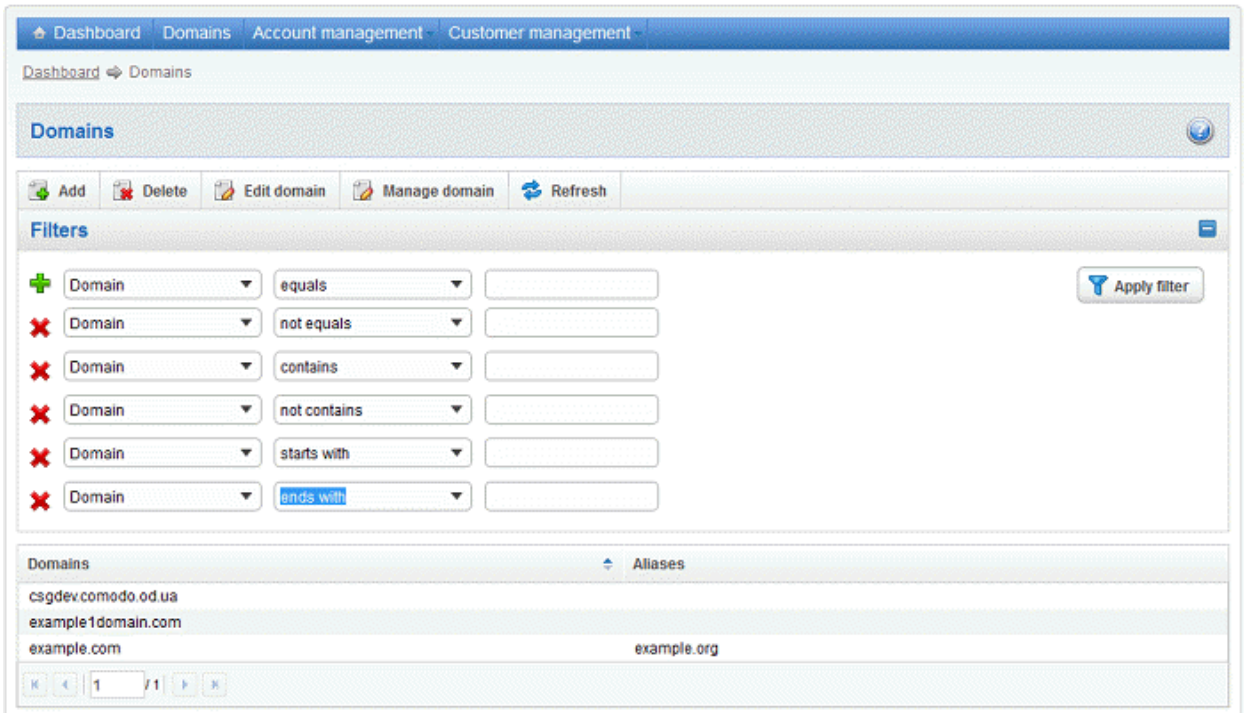
The list of domains that are configured will be displayed.

Using Filter options to search particular domain(s)

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



You can refine your search much further by clicking ✚ to add more filters.



You can remove a filter by clicking the ✖ icon beside it.

- Type the text in the third field box(es) and click 'Apply Filter'.

The application will search the domains column according to the filter(s) set and display the result.

Following are the options available in the filters area:

- **Domain:** Since here there is only 'Domains' column, there is no option in this text box.
- **Equals:** Displays the domain name that was entered in full in the text box.
- **Contains:** Displays all domain name(s) that contains the words entered in the text box.
- **Not Contains:** Displays all domain(s) that does not contain the words entered in the text box.
- **Starts With:** Displays all domain(s) that starts with the words entered in the text box.
- **Not Equals:** Displays all domain name(s), except the one entered in the text box.
- **Ends With:** Displays all the domain(s) that ends with the words entered in the text box.

Click anywhere on the Filters tab to close the filters area.

Click the Refresh button to display all the domains.

Note: To display all the domains after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

Click the following links to know how to:

- Add a domain
- Delete a domain
- Edit a domain
- Manage a domain

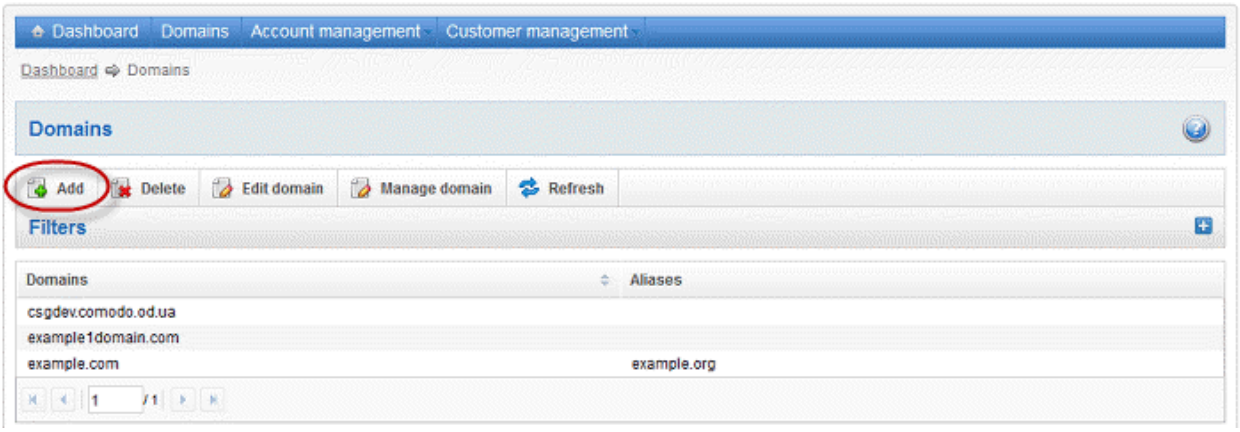
3.2.1.1 Adding Domains

From this interface you can add domains and the destination routes for respective domains. The number of domains that you

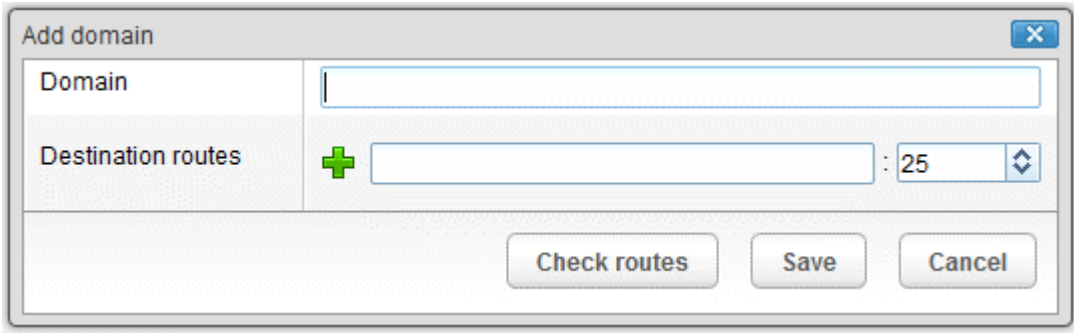
can add depends on the plan that you have subscribed.

To add a domain

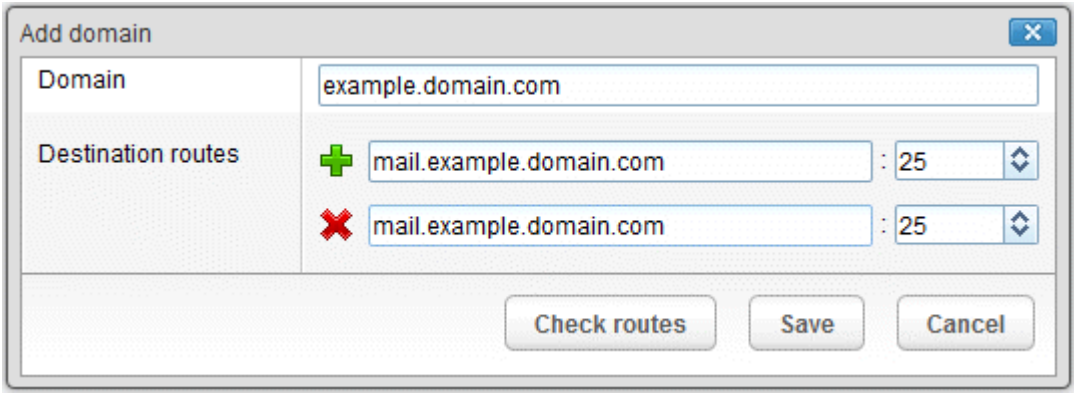
- Click the 'Add' button in the Domains interface



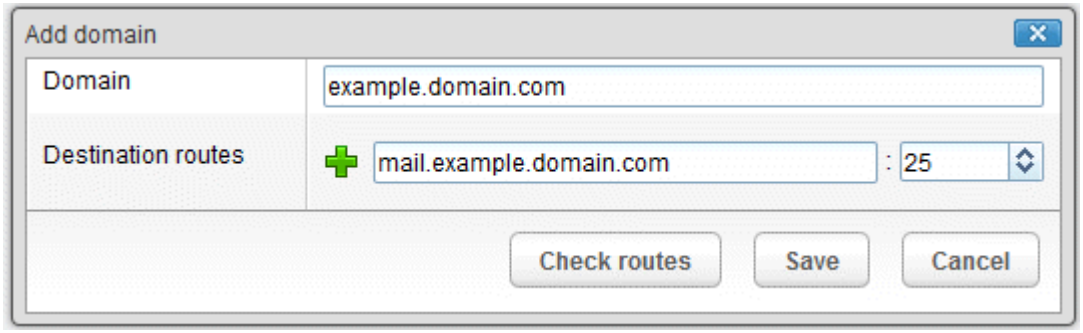
The 'Add domain' dialog will open.



- Enter a valid domain name in the 'Domain' field.
- Enter the final mail server destination route in the 'Destination routes' field. This is where the mails will be delivered from CASG after appropriate filtering of mails. The default port is 25.
- If you want additional routes to be included for the filtered mails to be delivered in case of failure of the first route, click beside the 'Destination routes' field to add more alternative destination routes.



- Click the 'Check routes' button to let CASG automatically get the destination routes information from DNS. If the result contains mxsrv1.spamgateway.comodo.com then it means that DNS MX record was already updated to work with Antispam Gateway server and you must fill 'Destination routes' field with your real MX record, for example mail.exampledomain.com.
- Click 'Save' to add the configured domains.



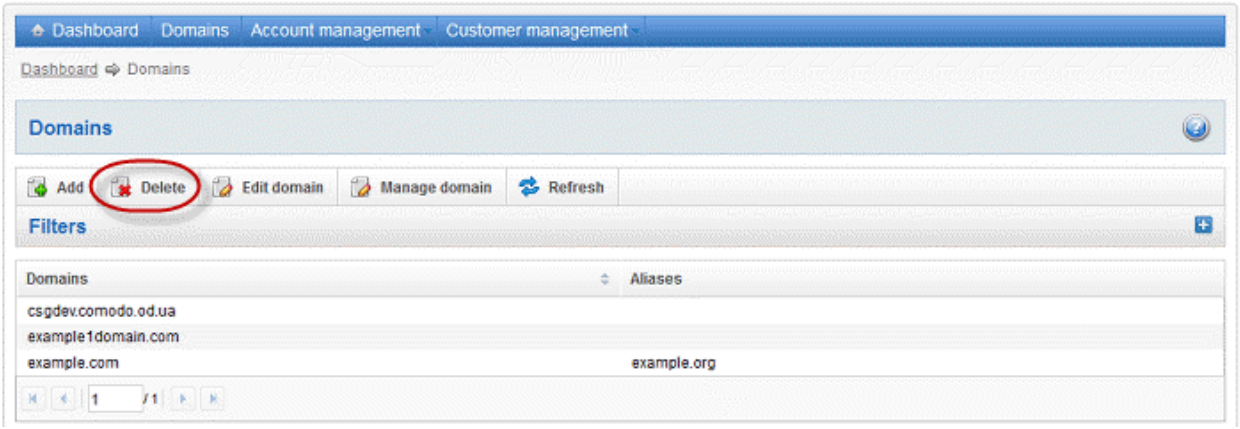
Note: When you create a new domain, email addresses 'abuse@addeddomain' and 'postmaster@addeddomain' will be added by default in Recipient Whitelist. **Click here** for more details.

3.2.1.2 Deleting Domains

If you want to delete a domain for which emails are being routed via CASG, this can be done in this interface.

To delete a domain

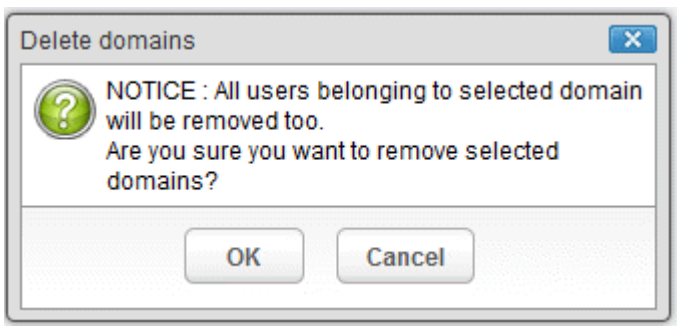
- Select the domain(s) that you want to delete from the interface.



- Click the "Delete' button

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

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



- Click 'OK' to confirm.

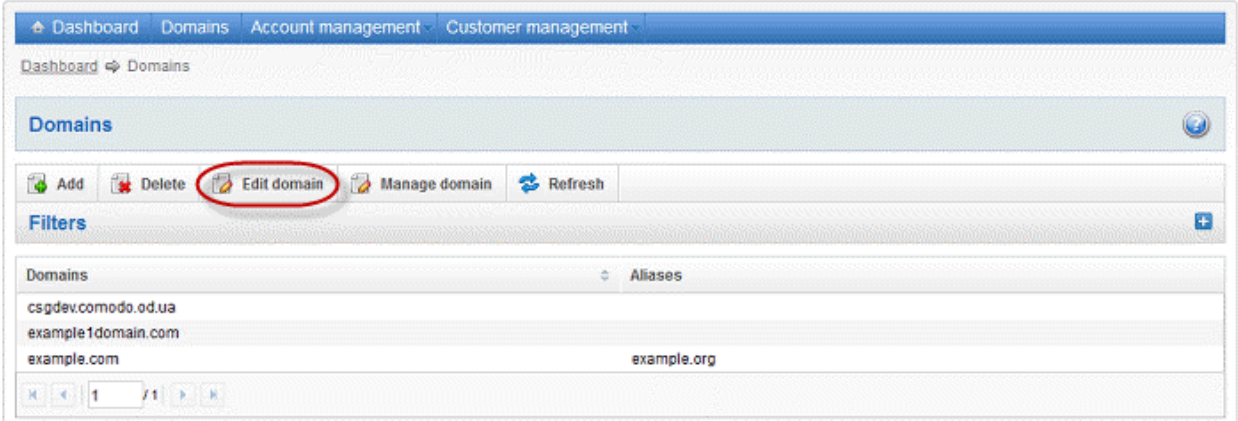
The selected domain(s) will be deleted.

3.2.1.3 Editing Domains

You can change the destination routes of a configured domain and check routes for the edited domain. Please note that the name of the domain cannot be edited.

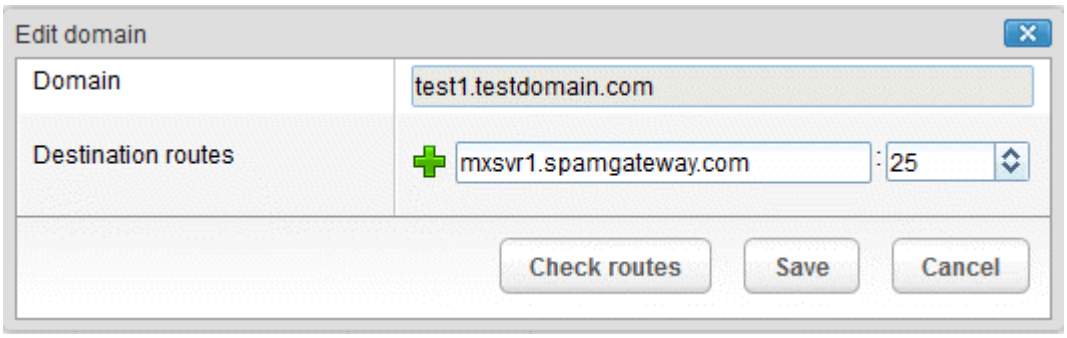
To edit a domain

- Select the domain that you want to edit from the interface



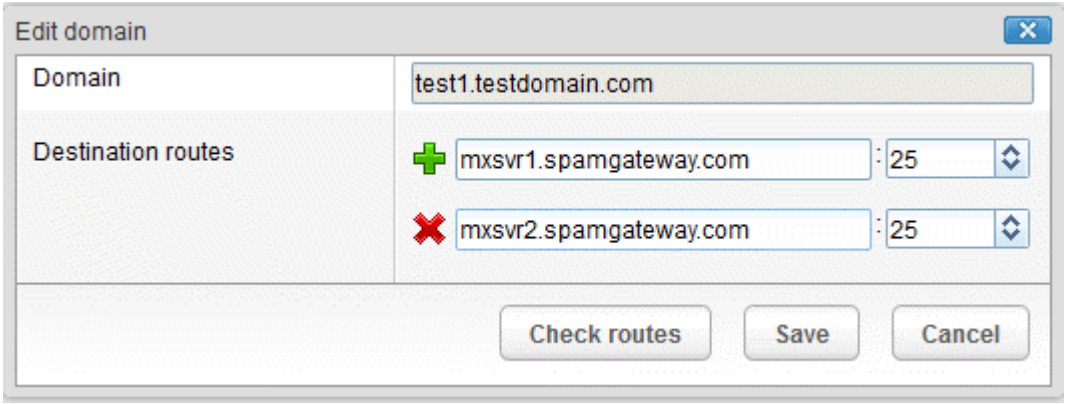
- Click the 'Edit domain" button

The Edit domain dialog will be displayed. Please note that the domain name is not editable.



From here you can add another destination route, change the primary destination route or delete additional destination routes.

- Click in the 'Destination route' field to edit it.
- Click beside the 'Destination routes' field to add more alternative destination routes.



- Click to remove alternative destination routes.
- Click the 'Check routes' button to let CASG automatically get the destination routes information from DNS. If the result contains mxsrv1.spamgateway.comodo.com then it means that DNS MX record was already updated to work with

Antispam Gateway server and you must fill 'Destination routes' field with your real MX record, for example mail.testdomain.com.

- Click 'Save' to confirm the changes.

3.2.1.4 Managing Domain

In this area, an administrator can configure various settings for a selected domain. This interface allows the administrator to view quarantined mails, set email restrictions, add users as recipient whitelist or blacklist and add new users. In the left side of the interface, the Statistics column displays the details such as number of users, email size restriction and information on daily activities for the selected domain.

This section is divided into five main subsections namely, Incoming, Outgoing, Email management, Whitelist / Blacklist and Account management. Click on the respective tab to expand or close the subsection in the interface.

To manage a domain

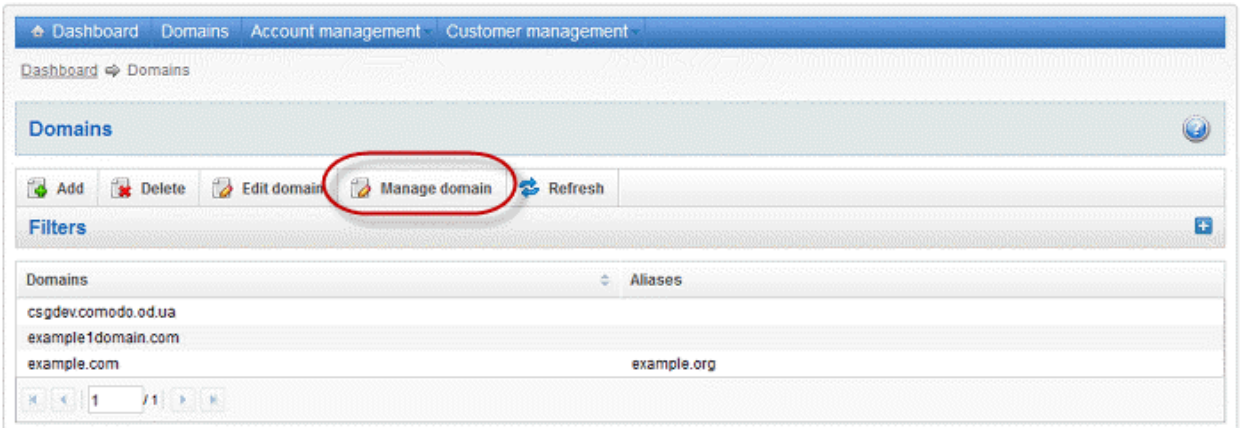
- Select the domain that you want to manage from the interface and click the 'Manage Domain' button.

  or

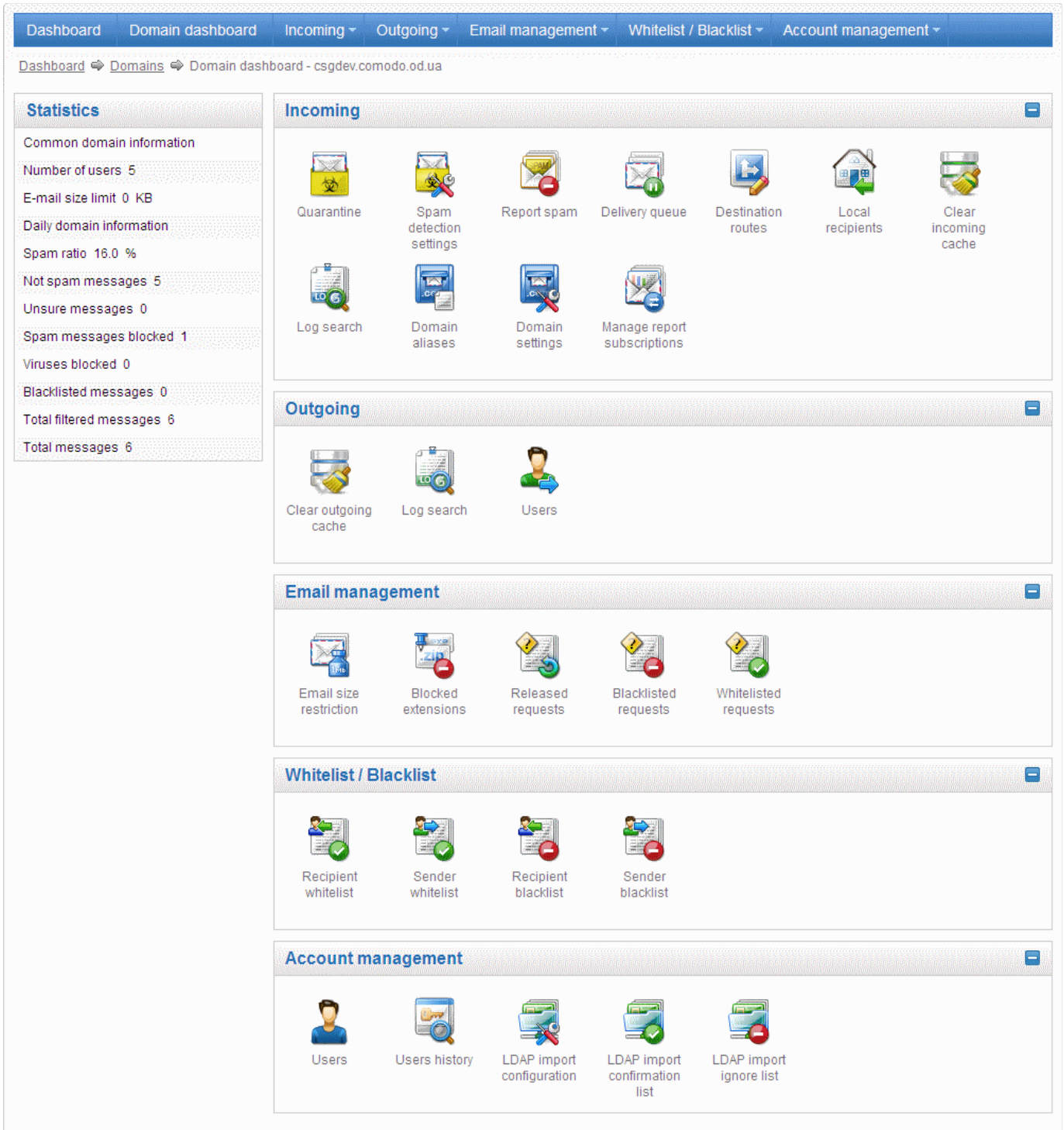
- Click on the domain name in the 'Domains' column.

  or

- Right-click on the domain name in the 'Domains' column to open in a new tab or window.



The configuration interface for the selected domain will open.

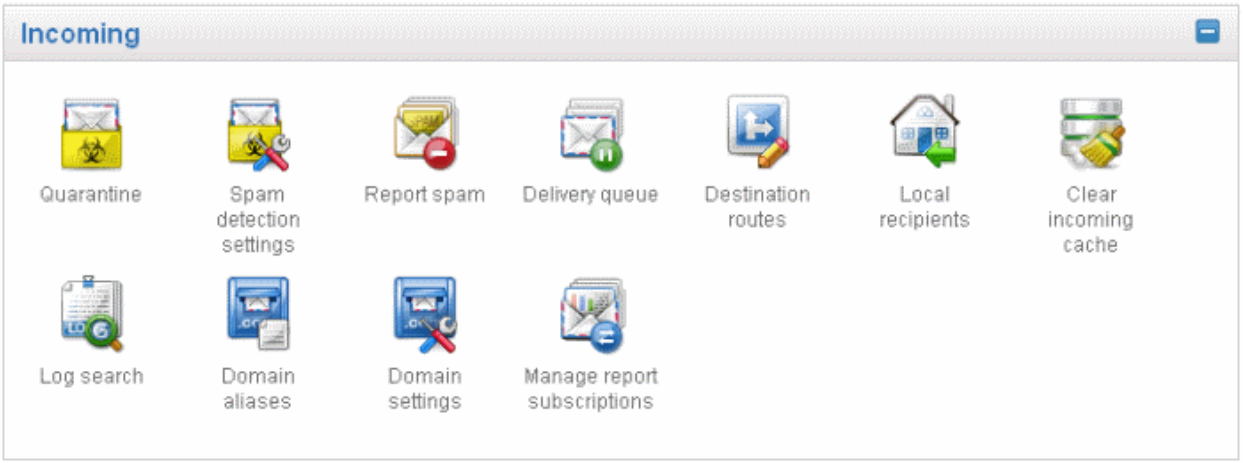


Click on the following links for more details on the subsections:

- Incoming
- Outgoing
- Email Management
- Whitelist / Blacklist
- Account Management

3.2.1.4.1 Incoming

In the 'Incoming' area of the Manage Domain section, you can view quarantined mails, configure incoming Spam detection settings, set alert heading for spam mail, add local email recipients and more.



Click the following links for more details:

- Quarantine
- 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

Quarantine

In this area, an administrator can view the list of all the quarantined emails and their headers, of all the users for the selected domain. The administrator can also choose to release quarantined emails to the intended recipient after ascertaining that particular email is not actually a spam. The administrator also can delete a selected or all the spam mails from this interface.

Tip: CASG also periodically generates Quarantine reports containing a summary of mails identified as spam or malicious that were moved to quarantine automatically. The reports are sent to the administrators through email. Administrators can configure for such reports through Dashboard > Account Management > Admin > Add Administrators or Edit Administrators. Refer to CASG Reports - An Overview for more details.

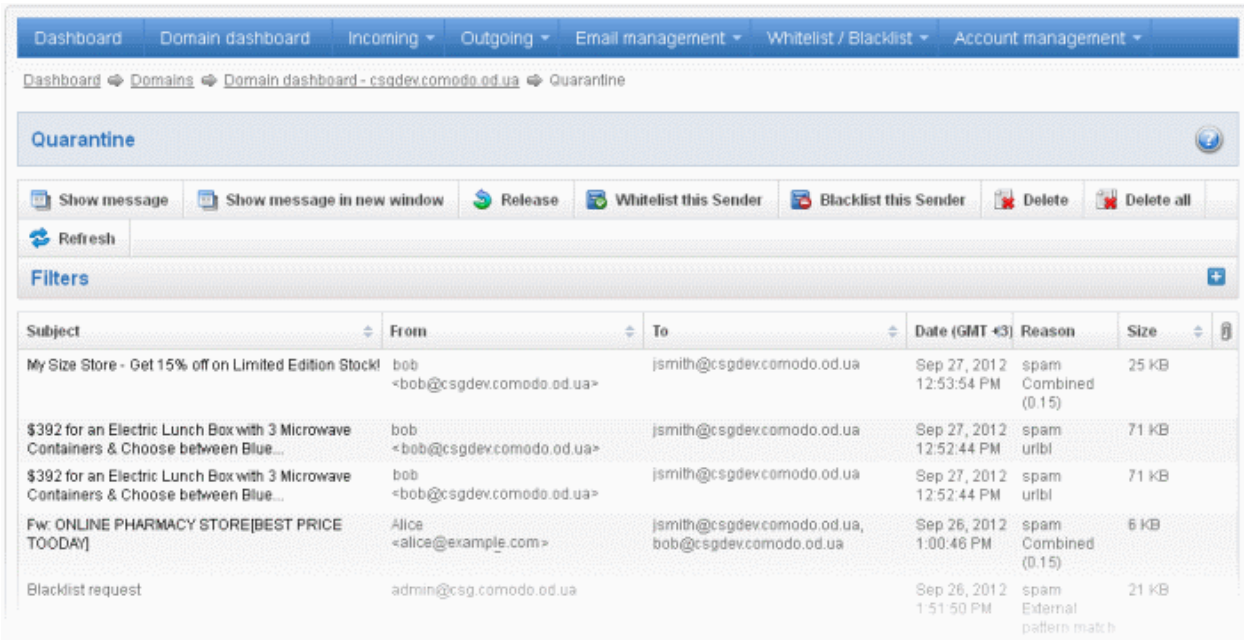
To open the quarantined email interface:

- Click 'Quarantine' from the 'Incoming' drop-down menu in the menu bar or the icon in the 'Incoming' configuration area.

Or

- Right-click on the icon and select to open in a new window or a new tab.

The quarantined email area of the selected domain will open:



The list of quarantined emails is displayed with six columns providing information about the subject, the sender, details of the recipients, the date it was sent and the size of the email. The last column indicates whether there is any attachment in the mails. You can set the number of entries to be displayed per page at the bottom.

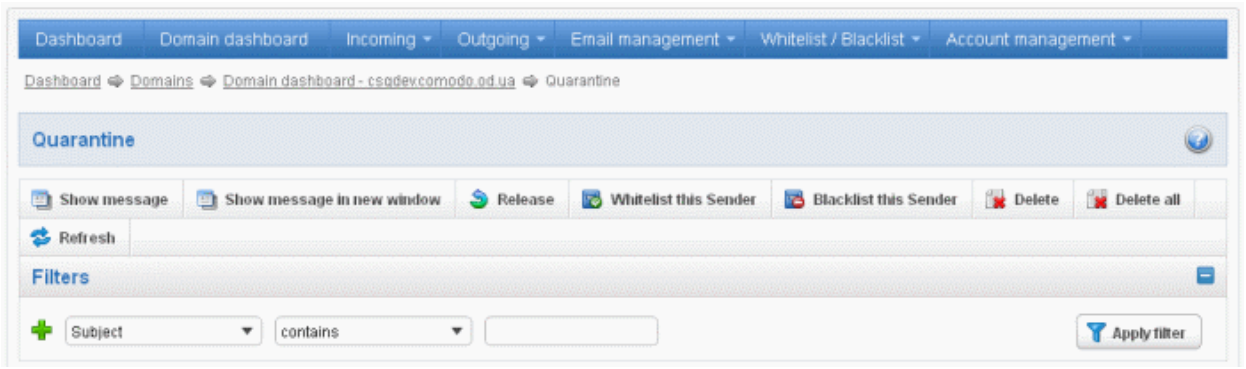
Select the number from the drop-down and click the 'Refresh' button or just wait for few seconds. The number of entries as selected per page will be displayed.

Sorting the Entries

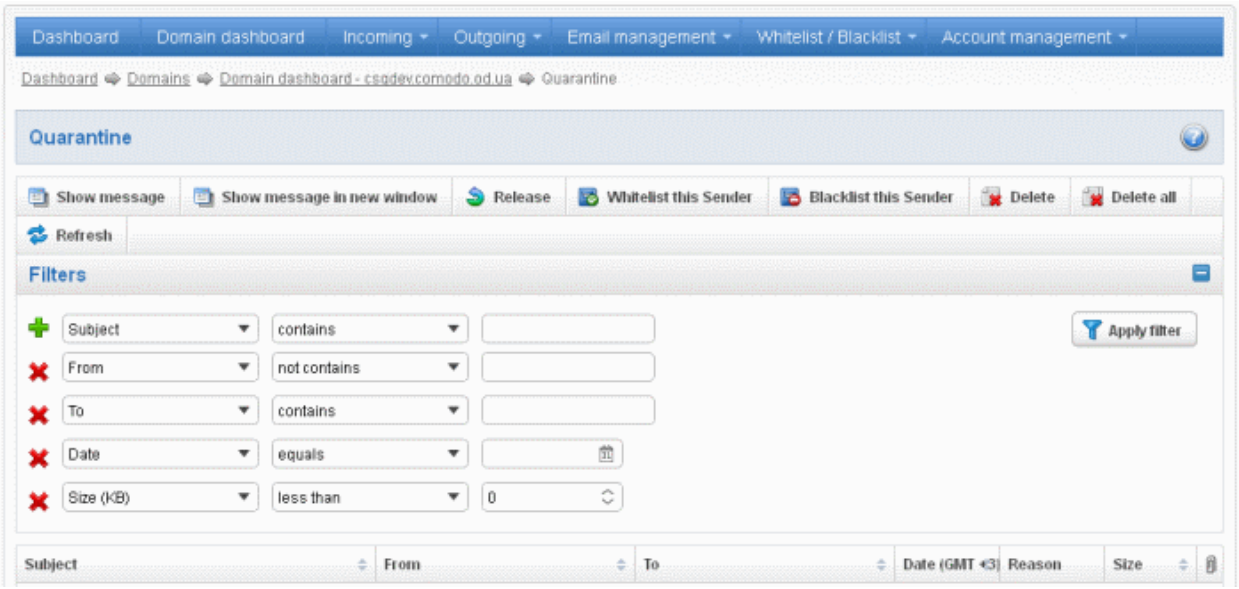
Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Using Filter option to search quarantined emails

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



You can refine your search much further by clicking ➕ to add more filters.



You can remove a filter by clicking the ✖ icon beside it.

- Type the text in the third field box(es) and click 'Apply Filter'

The application will search the respective column(s) according to the filter(s) set and display the result.

Following are the options in the first drop-down in the filters area:

- **Subject:** Displays the result based on the text entered in the text box for the 'Subject' column
- **From:** Displays the result based on the text entered in the text box for the 'From' column
- **To:** The results are filtered based on the text entered in the text box for the 'To' column

When you select any one of the above options in the first drop-down, the following filters are available in the second drop-down:

- **Contains:** Displays all quarantined mails that contain the words entered in the text box
- **Not Contains:** Displays all quarantined emails that don't contain the words entered in the text box

Other options available in the first drop-down in the filters area:

- **Date:** Displays the results according to the selected date in the third box from the calendar
- **Size (KB):** Displays the results according to size of the mail selected or entered in the third box

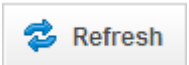
When you select 'Date' option in the first drop-down, the following filters are available:

- **Equals:** Displays the quarantined emails that have the same date as the selected date in the third box from the calendar
- **Less than:** Displays the quarantined emails with dates less than the selected date in the third box from the calendar
- **Greater than:** Displays the quarantined emails with dates greater than the selected date in the third box from the calendar

When you select 'Size (KB)' option in the first drop-down, the following filters are available:

- **Less than:** Displays the quarantined emails with size less than the selected or entered size in the third box
- **Greater than:** Displays the quarantined emails with size greater than the selected or entered size in the third box

Click anywhere on the Filters tab to close the filters area.

Click the 

button to display all the quarantined emails.

Note: To display all the quarantined emails after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

Viewing 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:

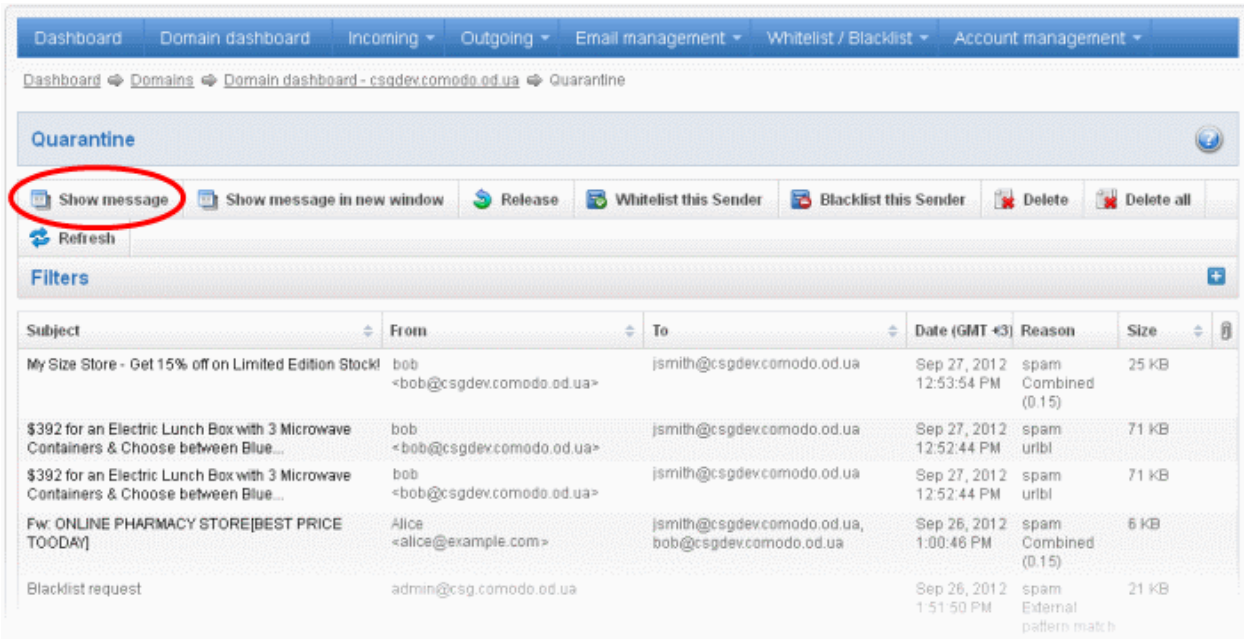
- In the same CASG window
- In a new CASG window

To view details of quarantined mails in the same CASG window:

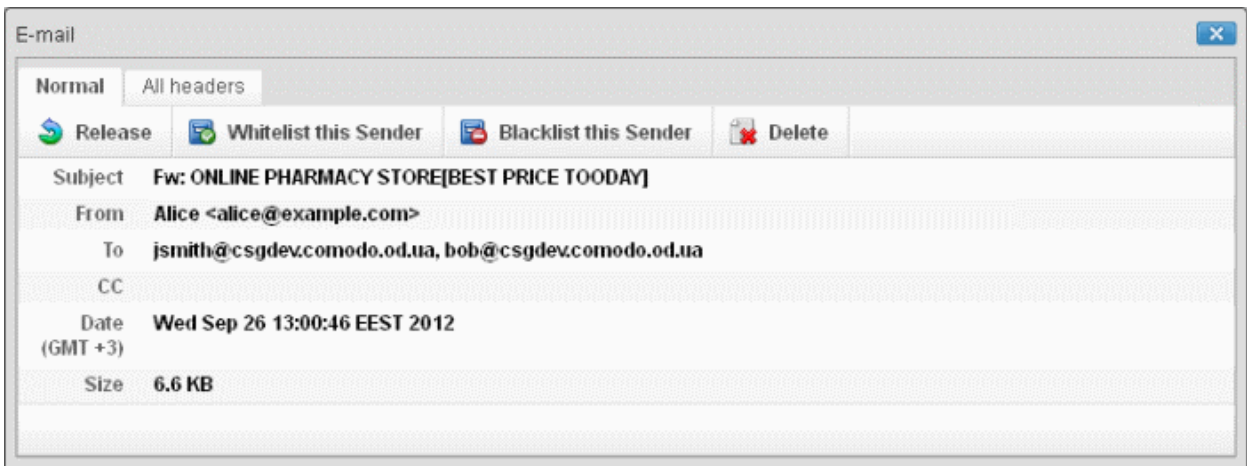
- In the quarantined email area, select the mail that you want to view and click the 'Show Message' button.

or

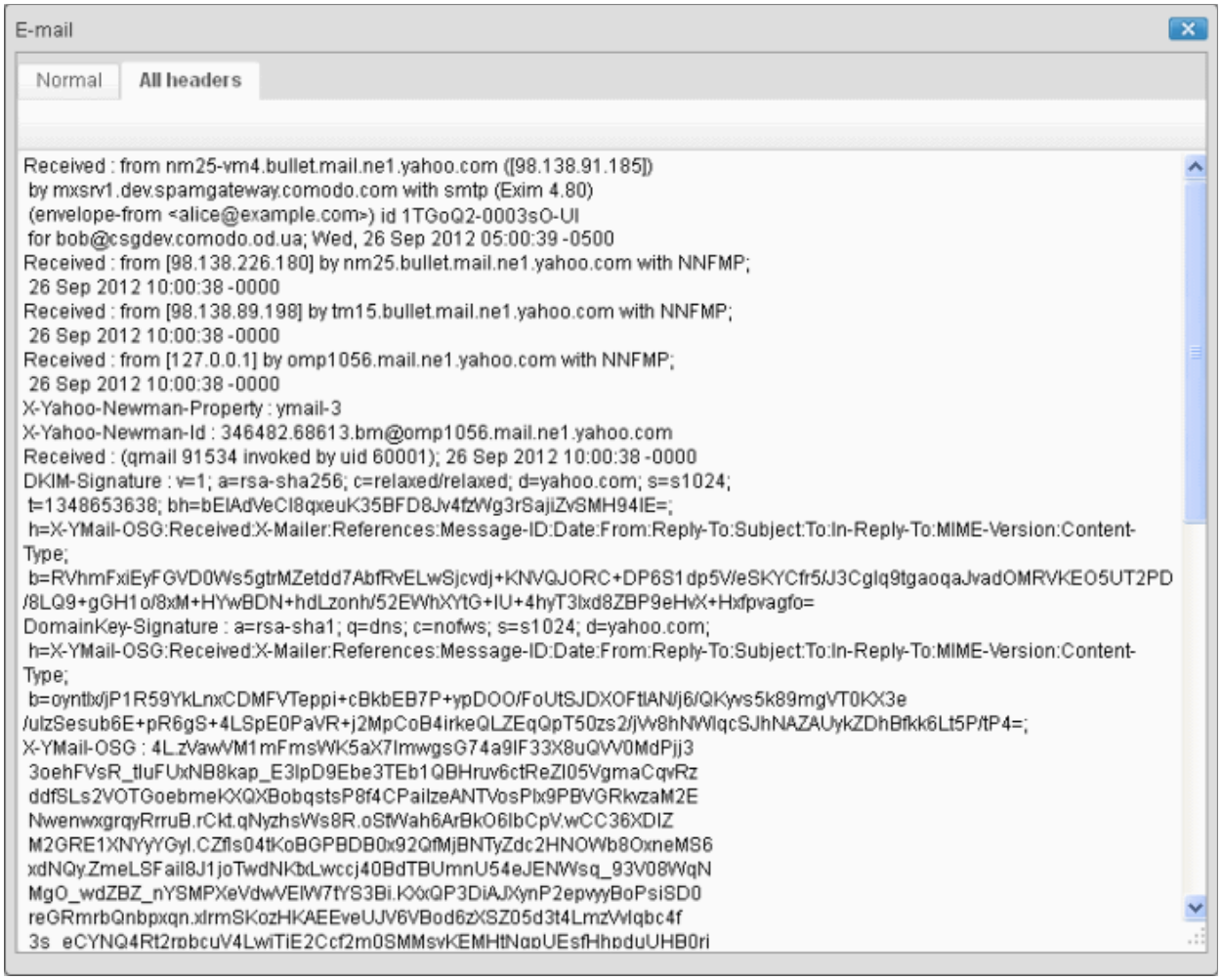
- Click on the email link in the subject column that you want to view its details.



The details of the selected email will be displayed.



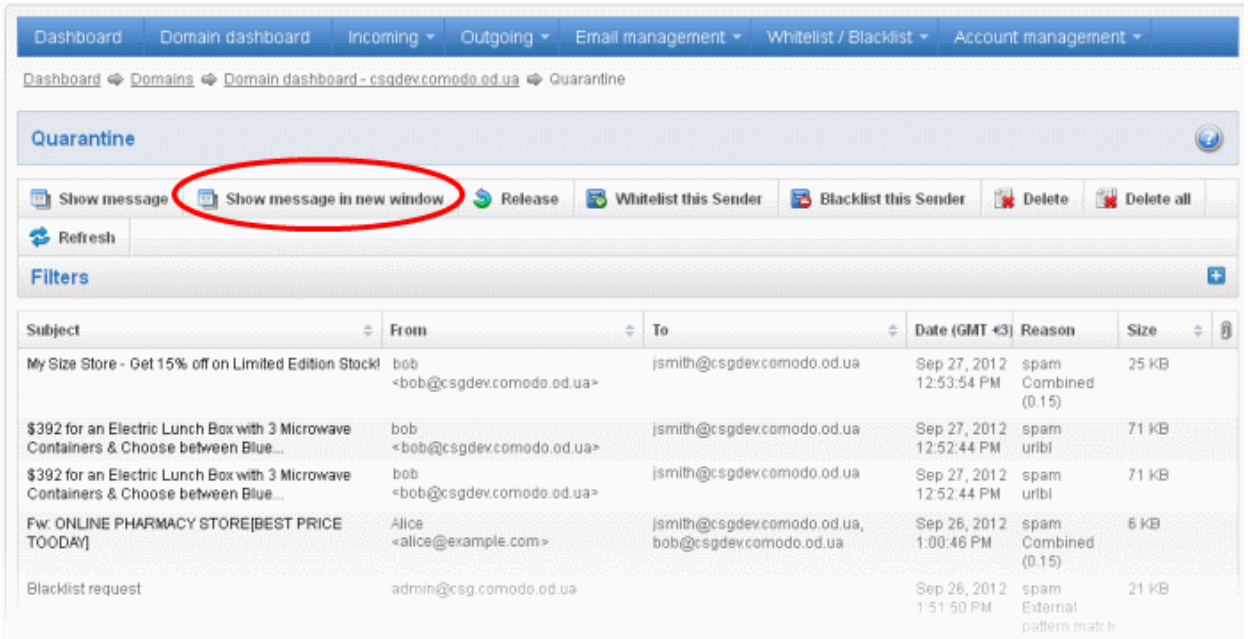
To view the email headers, which contain the tracking information of the mail detailing the path it has crossed before reaching the recipient, click 'All headers' tab. The headers give full details of the sender, route, recipient, sent date, mail type and so on and enable you to check the authenticity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



Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either release the mail or delete it. Click the 'Whitelist this sender' tab to add the sender to '**Sender Whitelist**' if you desire or 'Blacklist this Sender' to add this sender to **Sender Blacklist**. Refer to the section '**Whitelist / Blacklist**' for more details.

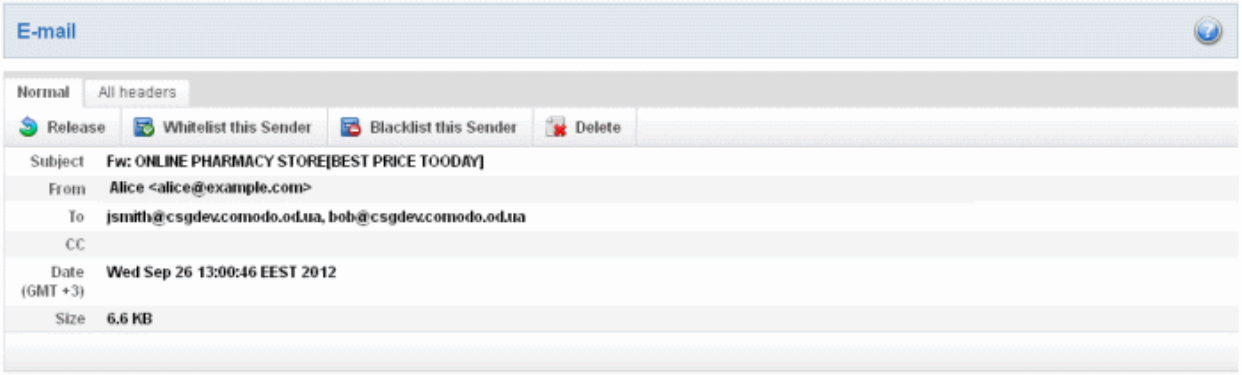
To view the details of a quarantined mail in a new CASG window

- In the quarantined email 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.



The browser will 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'.

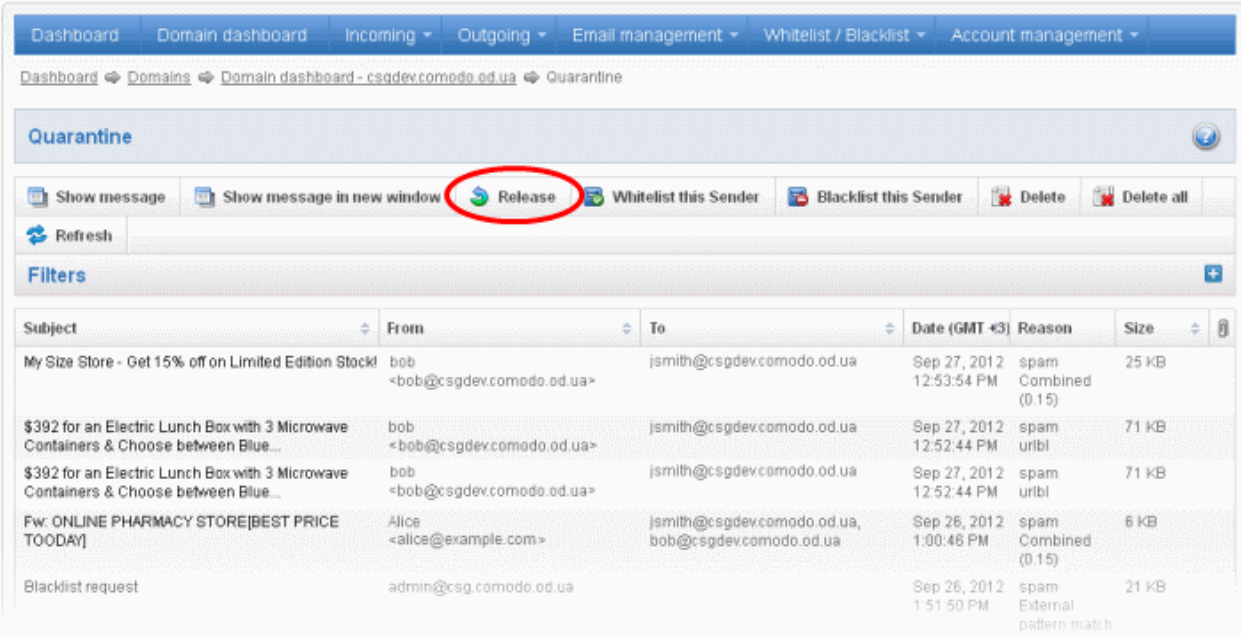
The details of the selected mail will be displayed in a new CASG window.



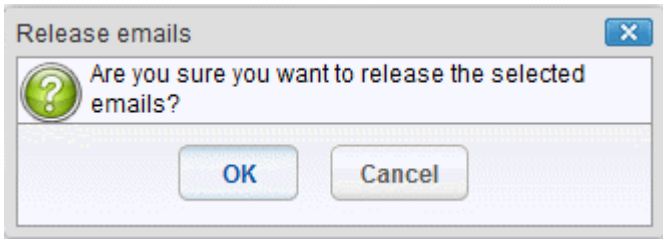
To release a quarantined mail:

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.



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



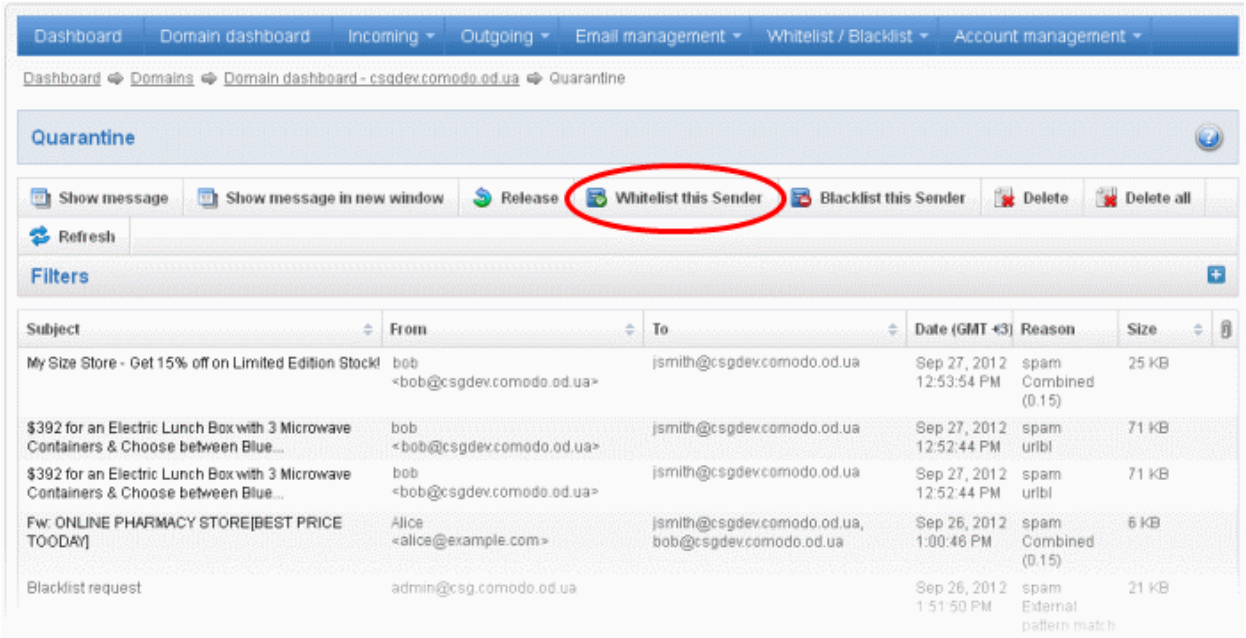
- Click 'OK' to confirm the release

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

To add a sender to whitelist

After ascertaining that emails sent by particular senders are not spam, administrators can choose to add them 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 click the 'Whitelist this Sender' button.



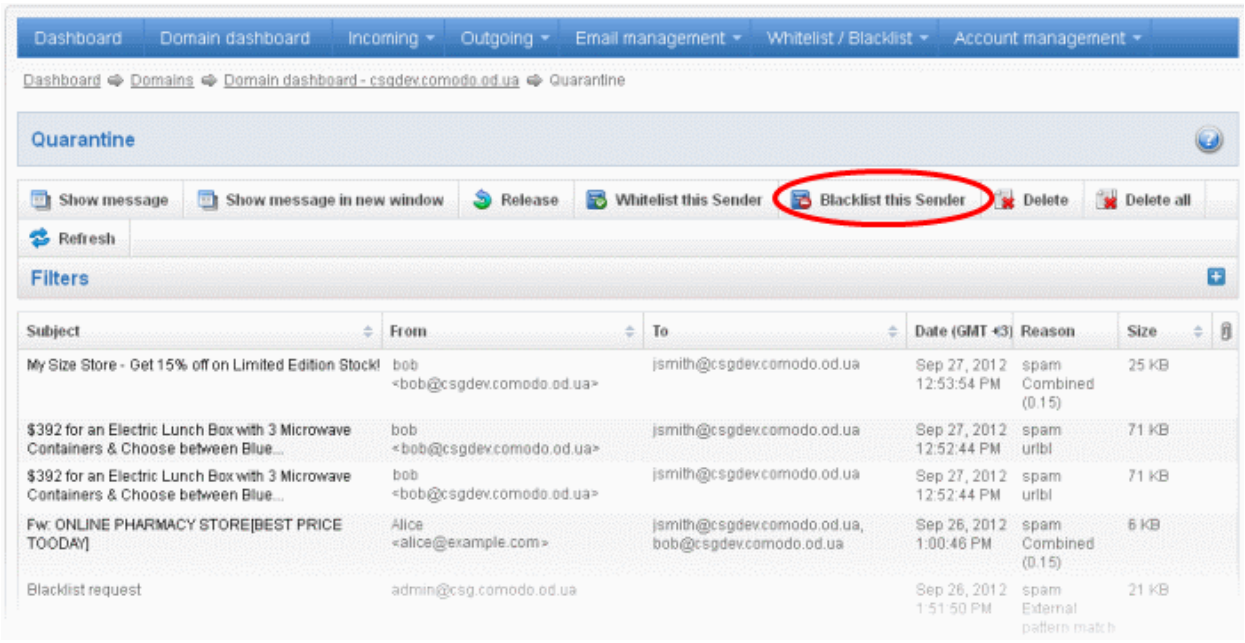
An alert will be displayed to confirm adding the sender to whitelist.

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

To add a sender to blacklist

Administrators can choose to add senders to '**Sender Blacklist**' from the Quarantine interface also. 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 click the 'Blacklist this Sender' button.

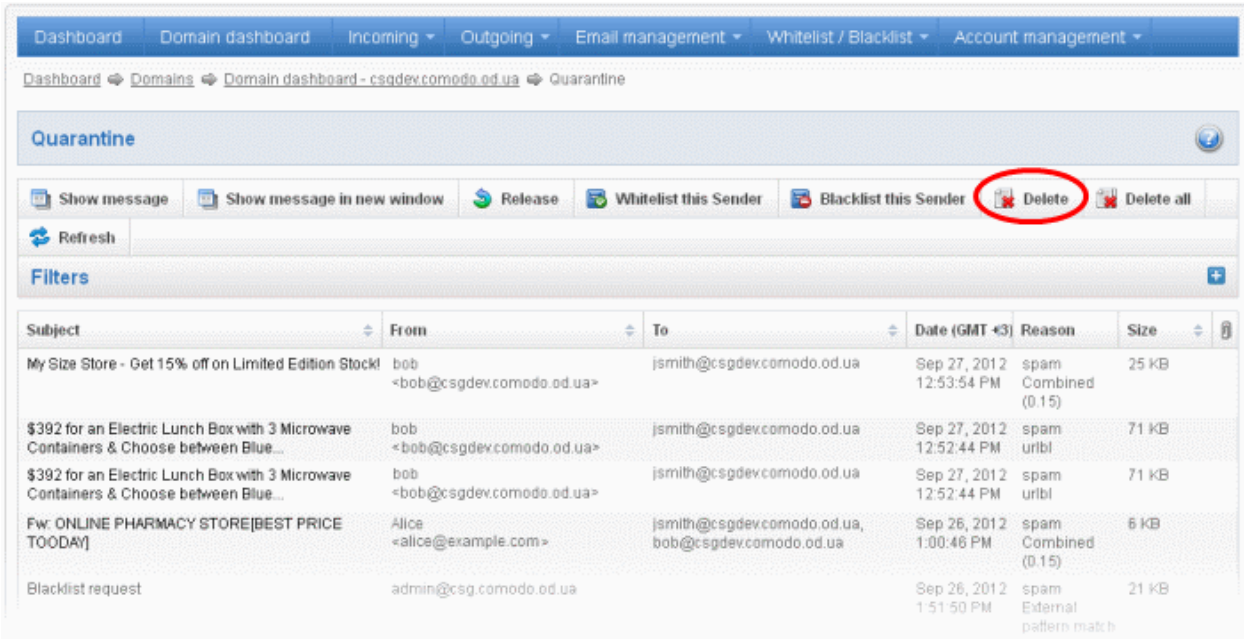


An alert will be displayed to confirm adding the sender to blacklist.

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

To delete a quarantined mail:

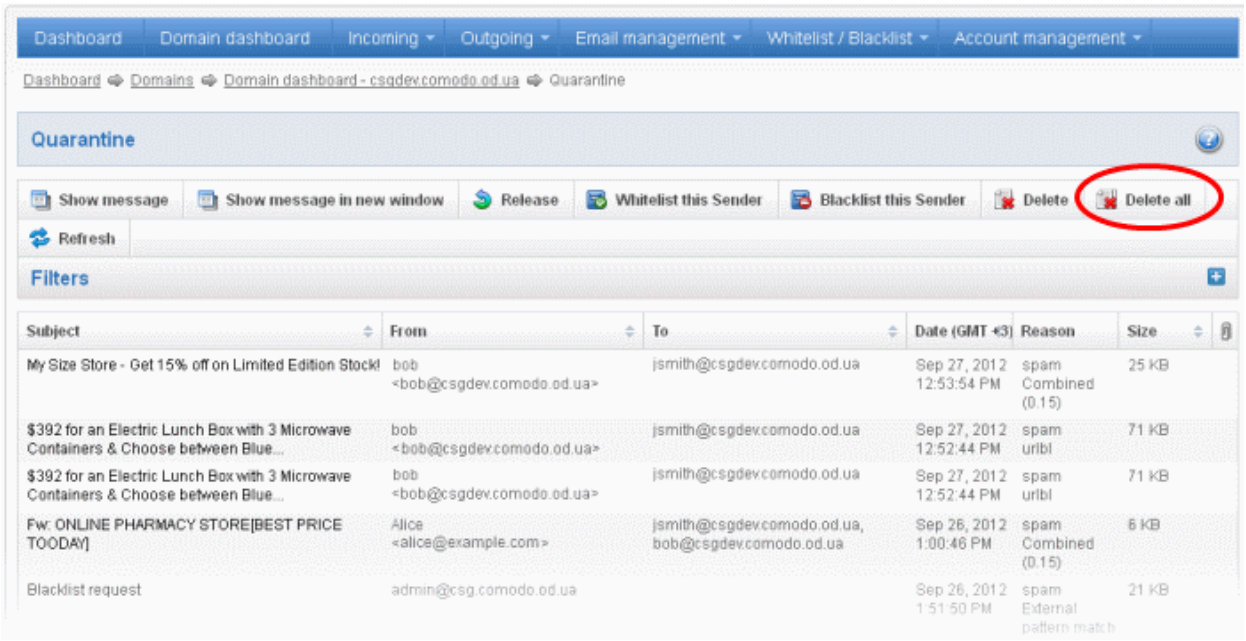
- Select the mail that you want to delete and click the 'Delete' button



An alert will be displayed to confirm the deletion. Click 'OK' to delete the selection email.

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

- Click the 'Delete All' button to remove all the quarantined emails.



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

All the quarantined emails for current domain will be deleted .

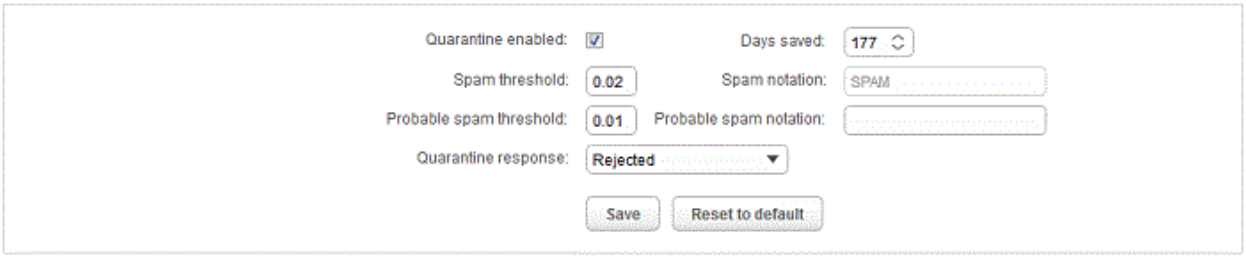
Incoming Spam detection settings

The settings made in this interface determine what kind of mails should be classified as 'spam', 'probable' and 'safe'. CASG enforces several rules to mail envelope, header and content as the emails passes through its spam filters. Each of these rules depicts some typical spam attribute, which has a numeric value on the probability that the attribute suggests spam. A message's spam score depends on the result of weighted value of all the rules combined together. For example, if you set the spam threshold as 0.33, all mails that have a score of more than 0.33 will be treated as spam and quarantined. Please note that the highest spam threshold is 1 for CASG and the higher threshold you set, it is likely that more spam messages may be delivered to the recipients. Try the settings for a week or so and after analyzing how much spam messages are being delivered to the recipients without being filtered for the current settings, you have to reconfigure the spam threshold settings accordingly.

To configure incoming spam detection settings

- Click 'Incoming spam detection settings' from the 'Incoming' drop-down menu in the menu bar or the icon in the 'Incoming' configuration area.

The incoming spam detection settings area of the selected domain will open:



- **Quarantine enabled** - Selecting this option will enable the incoming Spam detection settings that will be applied to the incoming mails and quarantined as per the spam threshold setting. If this option is not enabled, emails that are detected as 'Spam' will not be quarantined but delivered to your email server with the messages in subject line that you have set in **Probable Spam notation** / **Spam Notation**. Unsure messages are always sent to the recipient (and never quarantined) even if this option is enabled. Please see 'Unsure Notation' for more details.
- **Spam threshold** - Enter any value between 0.1 and 1.0. All mails that are having a score value above that is set in this field will be quarantined automatically as explained in the **introduction para** of this section. Please note this value should be always higher than 'Unsure threshold' value.

- **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 messages in subject line that you have set in the **Probable Spam notation** / **Spam Notation**.
- **Days saved** - Enter the number of days that you want the mails to be quarantined. The maximum number of days that can be set is 9999. The quarantined mails that are not checked, released or deleted within the stipulated days will be deleted automatically from the quarantine.
- **Probable spam notation** - The prefix that will be prepended to the subject line of all 'probable' emails sent to users. For example, "<Potentially Spam> Cheap deals on Dell computers" – where <Potentially Spam> is the 'Probable' notation'.
- **Spam notation** - The prefix that will be prepended 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 'Probable' notation'. Note - this only applies IF quarantine has been disabled (i.e. If the 'Quarantine Enabled' box is not checked).
- **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 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.
- **Reset to Default** - Reset to default all adjusted selected domain settings.

Click the 'Save' button. The incoming spam detection settings for the selected domain will be saved.

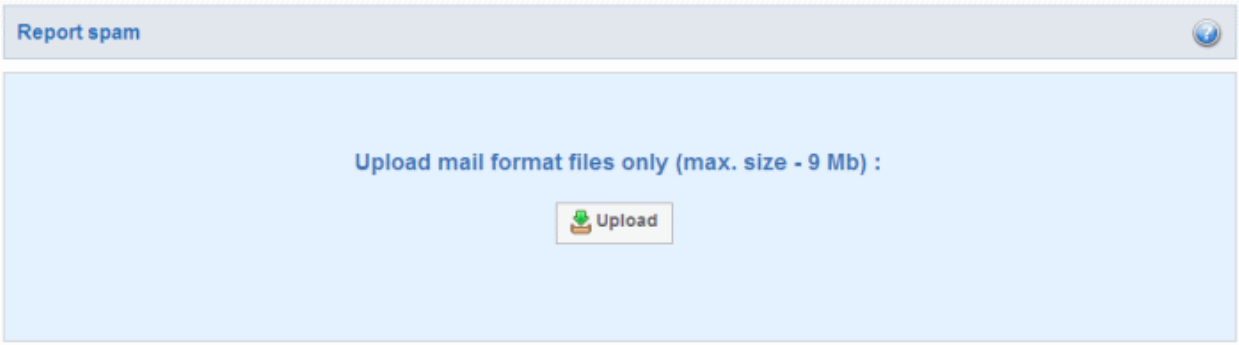
Report Spam

The Report Spam feature allows you to report suspected junk emails that have by-passed existing filters and landed in your inbox. CASG will analyze reported mails and, if found to be spam, will update its filters to quarantine similar mails in future. You can upload spam mails locally saved in your system into this area. CASG accepts a range of different mail formats, for example, .eml and .msg.

To report a spam mail

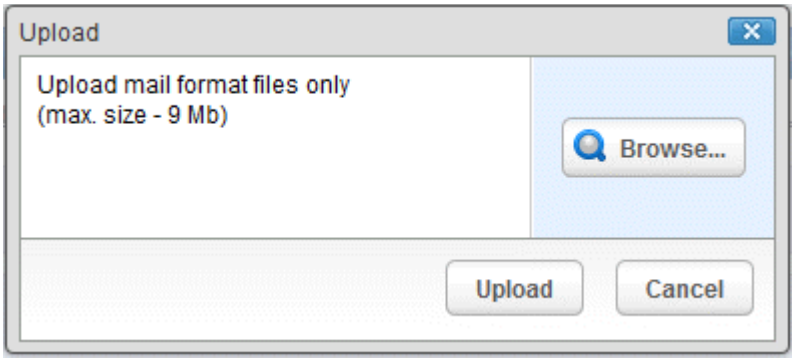
- Click 'Report spam' from the 'Incoming' drop-down menu in the menu bar or the icon in the 'Incoming' configuration area

The Report Spam interface will open.

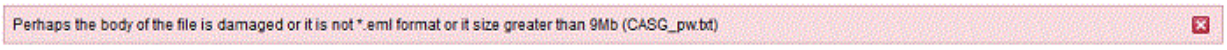


- Click the 'Upload' button

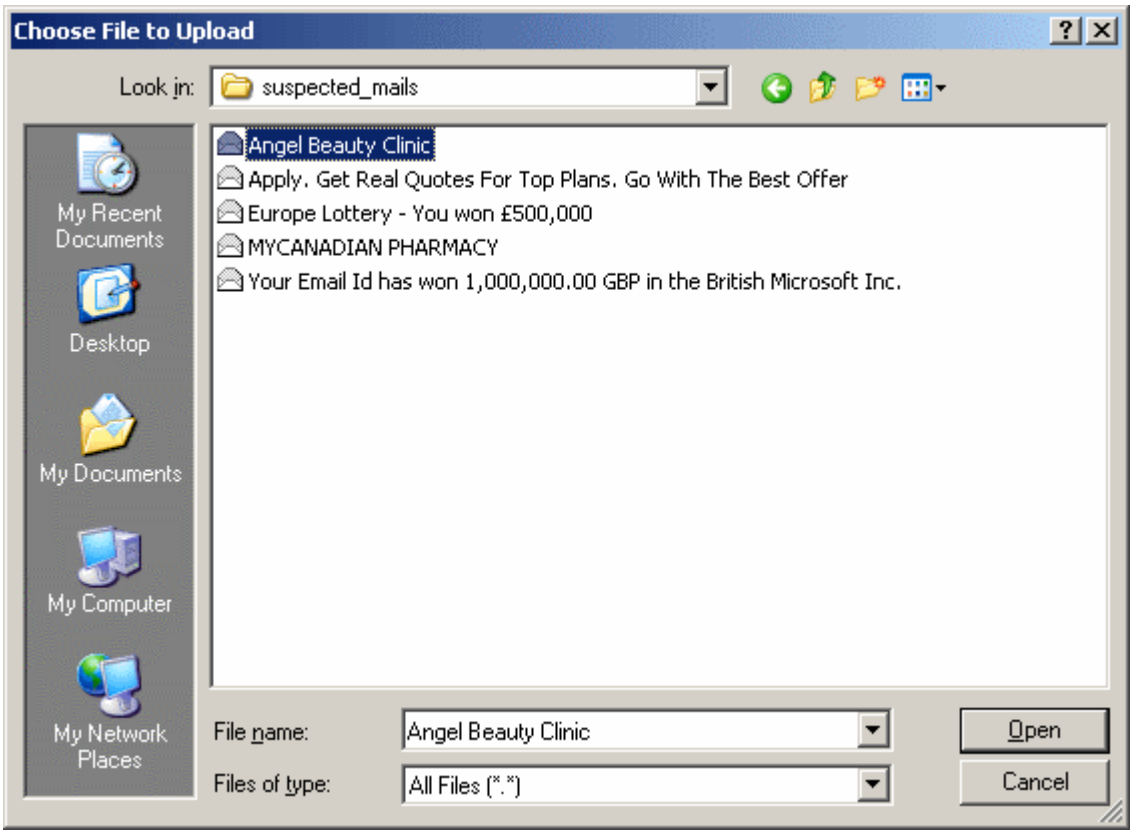
The File Upload dialog will open.



Note: Assure you will upload a correct email format and a size of the file is not greater then 9 MB. Otherwise, the following warning message will be displayed.

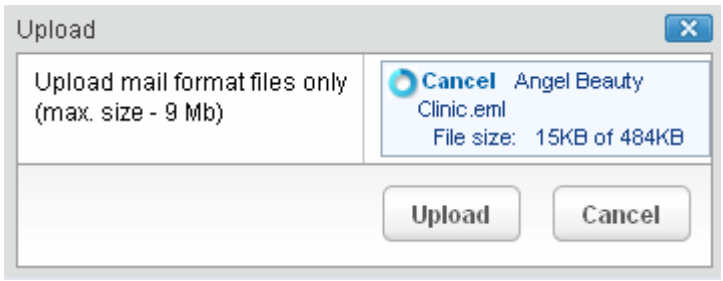


- Click Browse...

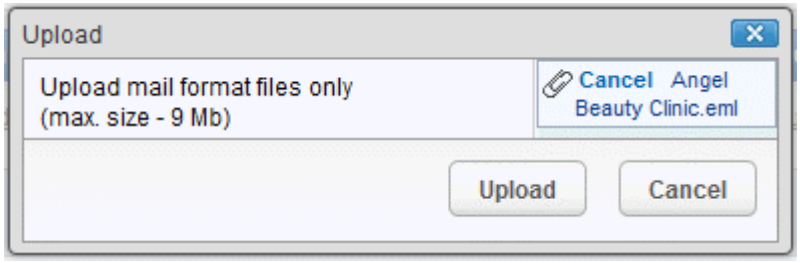


… and navigate to the location where the suspected email(s) is/are stored in your system. Select the mail that you want to report as spam and click 'Open'. The maximum size of the file that can be uploaded is 9 MB.

The mail will be processed for uploading...



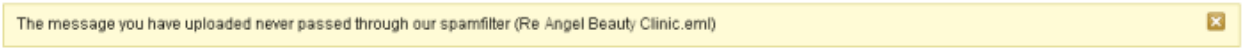
… and will be added to upload list.



- Click 'Upload'. The email will be uploaded and checked.

- Click the button to close the message.

If the mail that you have uploaded has not passed through CASG filter, the following message will be displayed.



Delivery Queue

In general, emails are delivered to the destination server directly and not stored on the filtering machines. But whenever an email destination server for an account is temporarily unavailable, all filtered mails are queued in 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 rejected by the CASG system. The queued emails can be accessed in the CASG interface and from here they can be manually force retried for delivery.

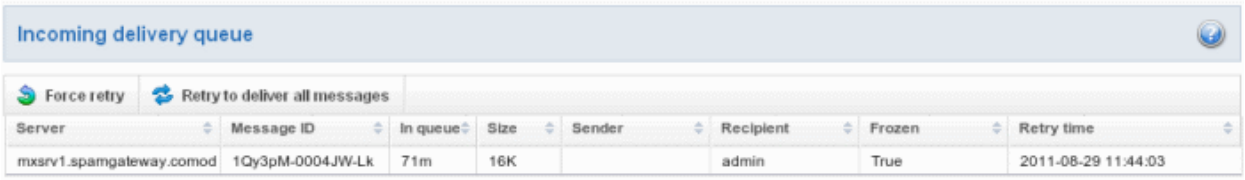
The queued messages on CASG severs are automatically retried for delivery for up to a period that is set in 'Maximum days to retry ' field in domain settings (for example, 4 days).The automatic retry schedule is given below:

- During the first two hours, the queued messages are retried for delivery at a fixed time interval of 15 minutes.
- During the next 14 hours, the 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 since the delivery failure and up to 4 days, the queued messages are retried for delivery at a fixed time interval of every 6 hours.
- After a period of 4 days, all queued messages will be bounced to 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.

To manually force-deliver emails in queue

- Click 'Delivery queue' from the 'Incoming' drop-down menu in the menu bar or the icon in the 'Incoming' configuration area

The Incoming Delivery Queue area of the selected domain will open:



- To force-deliver a single email manually, select an email from the delivery queue and click the 'Force retry' button.

- To force-deliver all email messages in the queue, click 'Retry to deliver all messages' button.

Note: Frozen emails can't be force delivered from CASG interface.

Destination Routes

If there is a temporary problem with the primary email destination server, CASG will try to deliver the filtered mails to the next destination email server that is configured. If the failure is permanent, for example, unable to resolve hostname, CASG will try to deliver through the next alternative route.

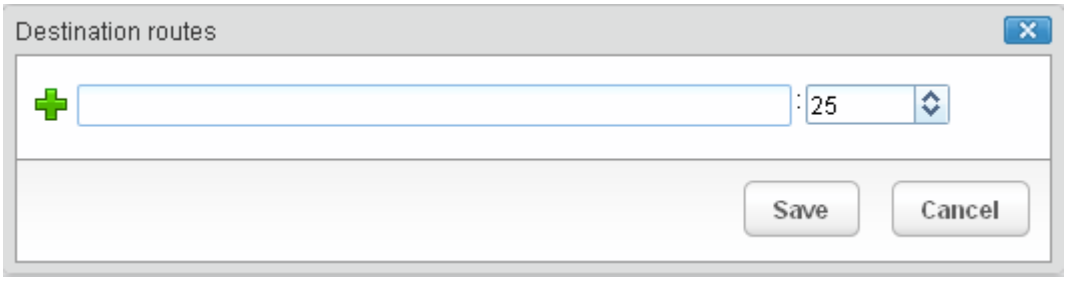
To add additional destination routes

- Click 'Destination routes" from the 'Incoming' drop-down menu in the menu bar or the icon in the 'Incoming' configuration area

The 'Destination routes' area of the selected domain will open:

- Click the 'Add' button to add another alternative destination route

The 'Destination routes' dialog box will be displayed.

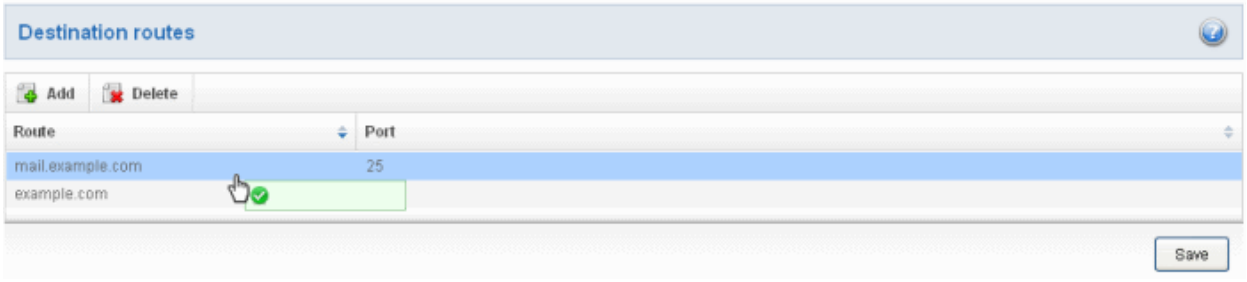


- Enter the alternative destination route and click the 'Save' button

The added route will be displayed in the list.

- If you want additional routes to be included, click to add more alternative destination routes.

You can also prioritize the routes by dragging and dropping from the list.



Click the 'Save' button to confirm the changes.

Click here for more details on how to check the routes.

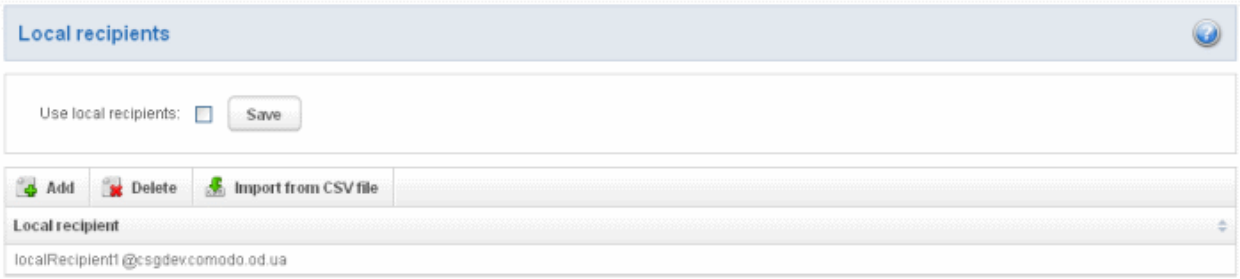
Local Recipients

CASG continuously performs a cached recipient callouts to check that recipient email addresses do actually exist in the destination mail servers. When the 'Local Recipients' option is enabled, only existing and valid email accounts in the destination server will be accepted. When this option is selected, *all the recipients* have to be added manually, else even valid users for that account will not receive emails. Comodo recommends that this option should be used in specific cases only and not required in normal cases.

To add local recipients

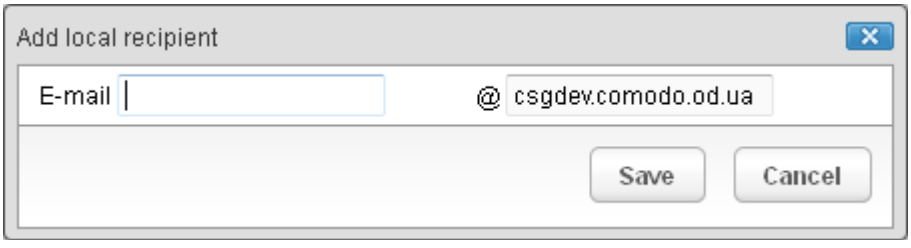
- Click 'Local Recipients' from the 'Incoming' drop-down menu in the menu bar or the icon in the 'Incoming' configuration area.

The Local Recipients configuration area of the selected domain will open:

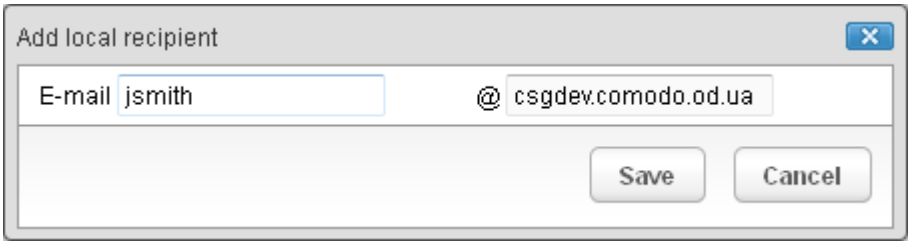


- Select the 'Use local recipients' check box and click the 'Save' button
- Click the 'Add' button

The 'Add local recipient' dialog box will open.

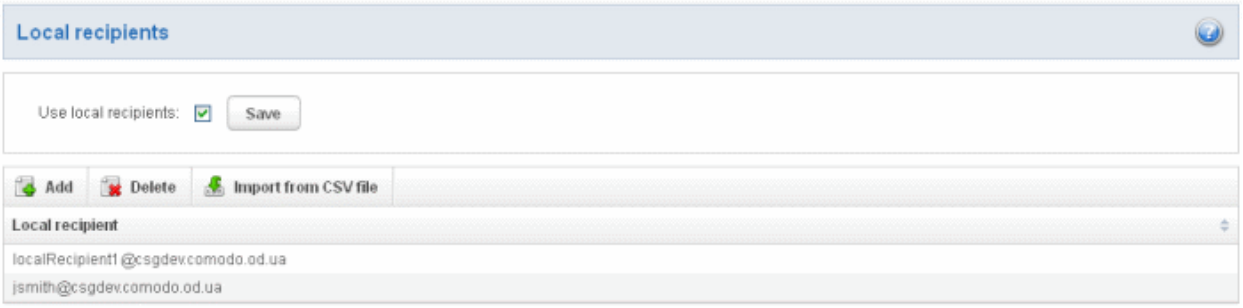


- Enter a valid user email address in the E-mail field



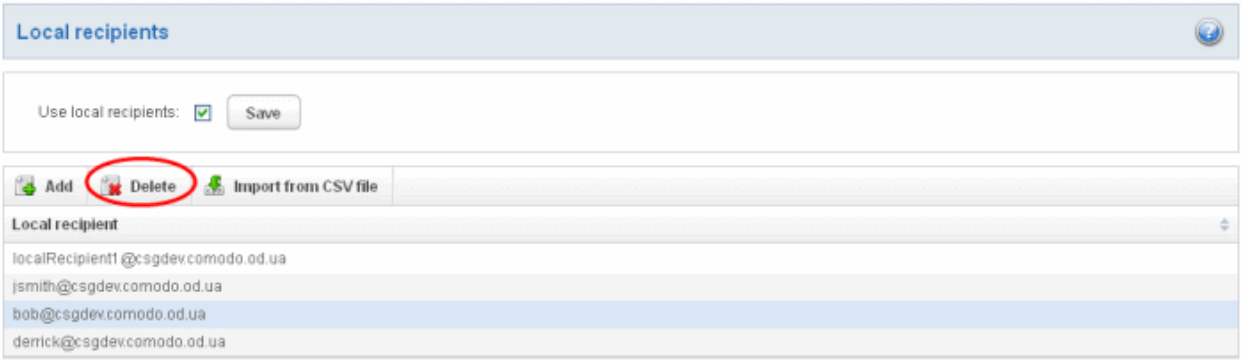
- Click the 'Save' button

Repeat the process till you have added all the users' email addresses.



To delete a local recipient

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



After clicking 'OK' in the confirmation dialog box, 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.

- To import local recipients from CSV file

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

user1
user2
user3

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

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

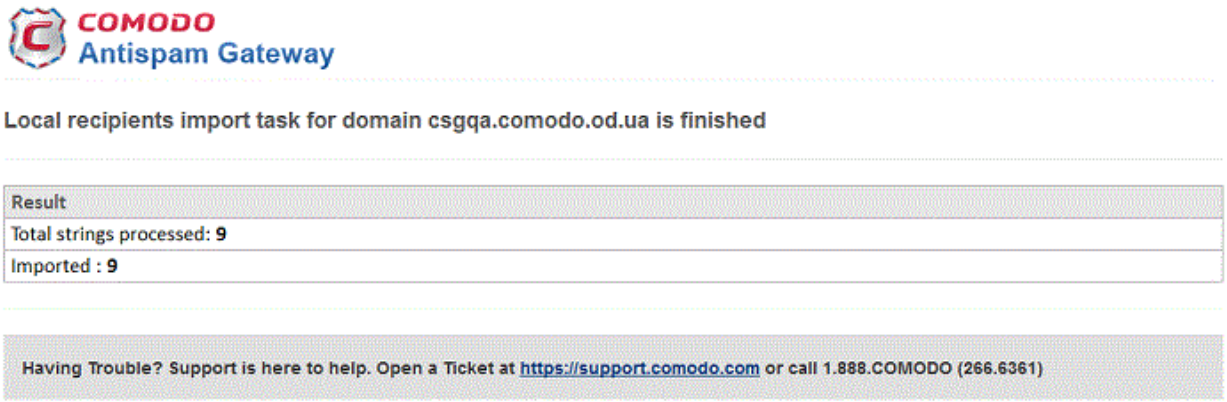
- The upload process is now ready. The maximum size of the file that can be uploaded is 9 MB. If you want to select another file, click 'Cancel' at top right side of the upload dialog. If you want to cancel the upload process, click the 'Cancel' button located at the bottom.

- Click the 'Upload' button to add new users.

The upload will be placed in 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* a remaining part of not imported task.

On completion of the upload process, refresh the browser to view the imported users.

The local recipients .csv file will be uploaded and an administrator will receive a notification about the import task completion to his email. This notification mail contains the import of local recipients data.



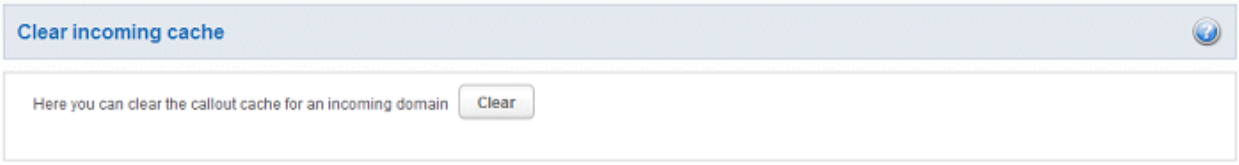
Clear Incoming Cache

CASG continuously performs a cached recipient callouts to check that recipient email addresses do actually exist in the destination mail servers. 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. CASG interface allows you to clear the callout cache without waiting for the servers to clear it.

To clear incoming cache

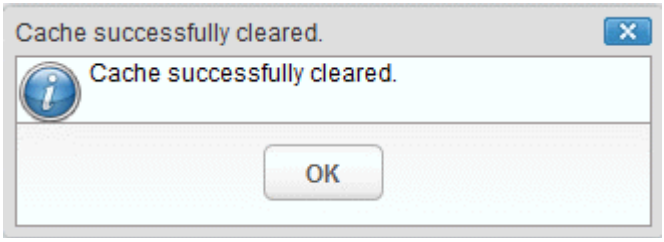
- Click 'Clear income cache' from the 'Incoming' drop-down menu in the menu bar or the icon in the 'Incoming' configuration area

The 'Clear incoming cache' area of the selected domain will open:



- Click the 'Clear' button

The callout cache for the incoming domain is cleared.



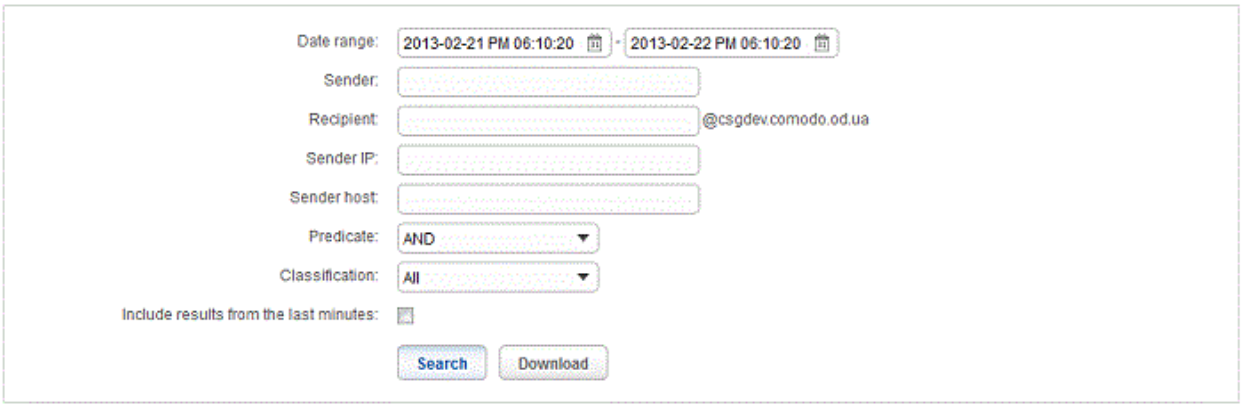
- Click 'OK' to close the 'Cache successfully cleared' dialog box.

Log Search

The Log Search option in CASG allows you to search for a specific email message.

- Click 'Log search' from the 'Incoming' drop-down menu in the menu bar or the icon in the 'Incoming' configuration area.

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



- **Date range:** Select the date range for which you want to search the log file.
- **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.
- **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.

Click the 'Search' button.

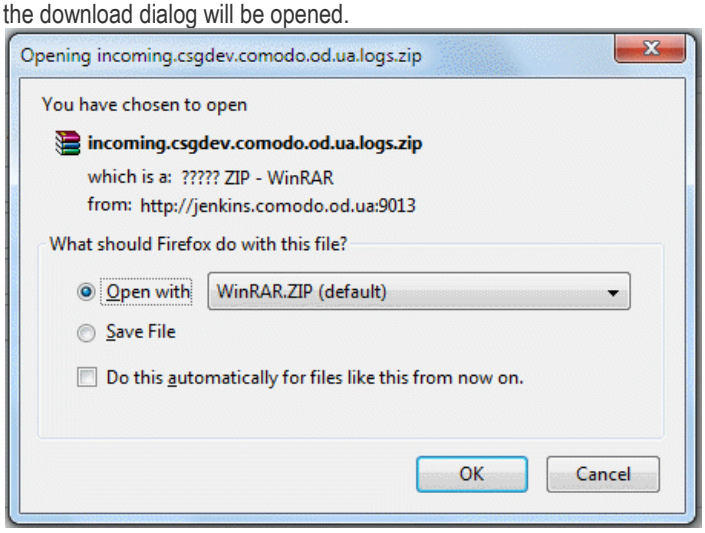
CASG will search for the entered terms and display the results.

Date and time	Host (Exim id)	Sender hostname	Sender	Recipient	Classification
2012-06-21 09:25:53	mxsrv1.dev.spamgateway.c 1ShdeA-0006nY-3g	mail.comodo.od.ua 91.196.95.17	admin@csg.comodo.od.ua	docteam	Rejected Destination address does not exist
2012-06-20 21:05:58	mxsrv1.dev.spamgateway.c 1ShS5u-0005yL-UG	mail.comodo.od.ua 91.196.95.17	admin@csg.comodo.od.ua	alex	Accepted Message content looked like non-spam
2012-06-20 21:05:12	mxsrv1.dev.spamgateway.c 1ShS5M-0005wV-Az	mail.comodo.od.ua 91.196.95.17	admin@csg.comodo.od.ua	doc.admin	Rejected Destination address does not exist

1 / 1

The **'Download'** button allows admin to retrieve from CASG a raw log of messages from the selected domain. The compressed Exim4 log containing all entries for the selected domain can be downloaded from this interface.

Press the download button, the download dialog will be opened.



You can choose to open the file by using the browse option or save the file in your system. The compressed log file will be saved in the folder that you have configured for saving download files.

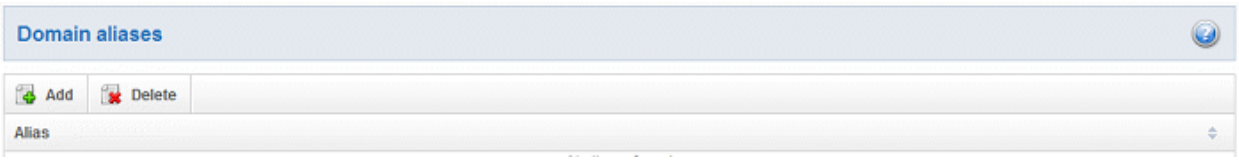
Domain Aliases

The Domain aliasing feature in CASG allows the administrator to add multiple domains as aliases for the main domain. After adding a domain alias, the MX records should be configured to activate the filtering process for this domain alias. Once this is done, mails sent to users at alias domain will be filtered and delivered to users at main domain. For example, if you add *testdomain.org* as an alias domain for the main domain *testdomain.com* and 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.*

To add domain aliases

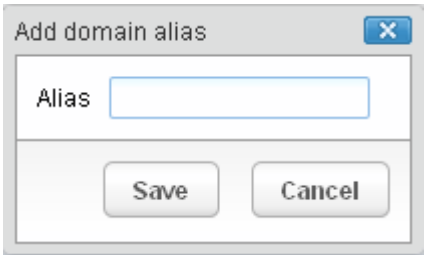
- Click 'Domain Aliases' from the 'Incoming' drop-down menu in the menu bar or the icon in the 'Incoming' configuration area

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

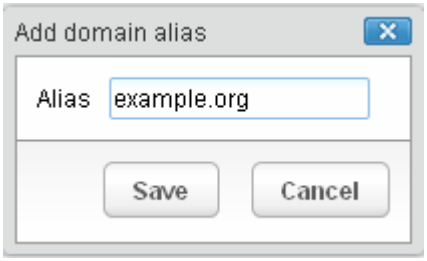


- Click the 'Add' button to add a domain alias for the selected domain

The 'Add domain alias' dialog box will open.

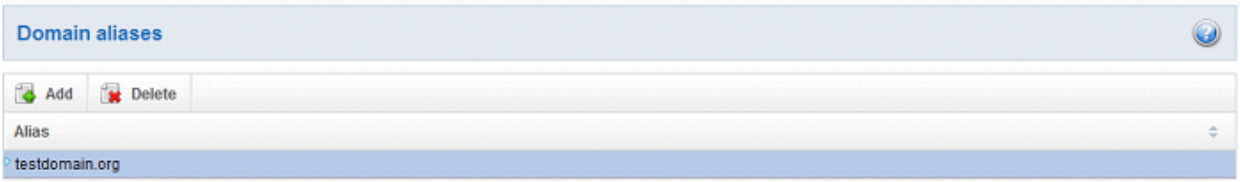


- Enter the domain alias name in the 'Alias' field

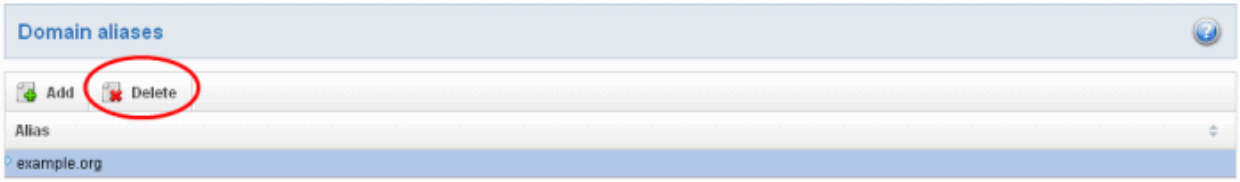


- Click the 'Save' button

The domain will be added to the main domain as alias and will be listed in the interface.



- To delete a domain alias, select the domain alias from the list and click the 'Delete' button



The selected domain alias will be deleted from the list.

Domain Settings

An administrator can configure various settings for the selected domain such as primary contact email address, the administrator's email address and maximum number of bounces allowed before being rejected.

To configure domain settings

- Click 'Domain Settings' from the 'Incoming' drop-down menu in the menu bar or the icon in the 'Incoming' configuration area

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

- **Maximum bounces:** Each recipient of the selected domain will be limited to receive only these many message bounces set in this field 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 the users at the selected domain do not send mails to invalid addresses frequently. By default this field is set to 100.
- **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 28 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.
- **Enable logging for invalid recipients:** This setting enables or disables the selected domain to log details of incoming mails addressed to incorrect recipients. This option is enabled by default.
- **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.
- **Change locale for system messages:** Select a language in what the system email notifications will be came.

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'.

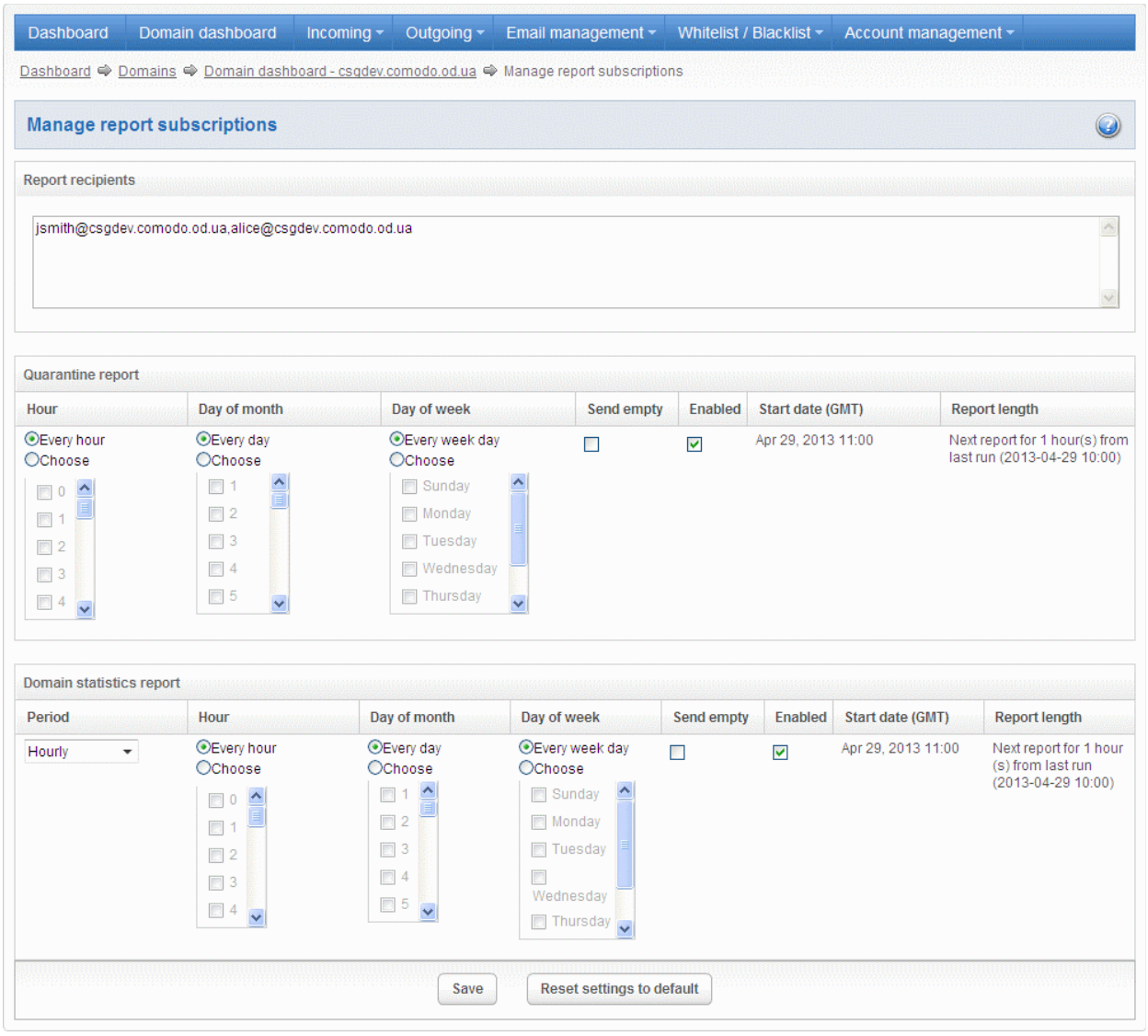
Manage Report Subscriptions for Selected Domain

The Manage report subscriptions interface accessible from the 'Incoming' configuration area of a selected domain allows the administrator to configure the subscription to the periodical Domain and Quarantine summary reports of that domain only for the administrators. Refer to CASG Reports - an Overview for more details.

To access Manage report subscriptions interface

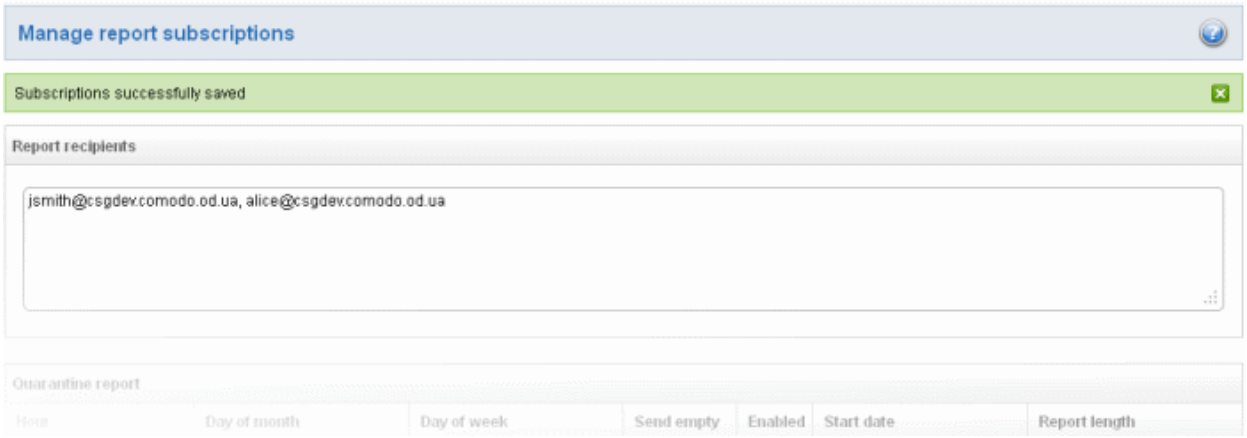
- Click 'Manage report subscriptions' icon from the 'Incoming' configuration area or click 'Manage report subscriptions' from the 'Incoming' drop-down menu in the menu bar.

The 'Manage report subscriptions' interface will be displayed:



The Report recipients field will not be auto-populated as it does in the interface of Customer Management > Managing Report Subscriptions. Enter the email address of the administrators belonging to that domain in the text field separated by a comma after each email address.

The recipients will be added and subscriptions successfully saved message will be displayed.



Clicking the 'Reset settings to default' button will disable both Quarantine and Domain statistics reports. The 'Report Recipients' field will not be cleared.

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

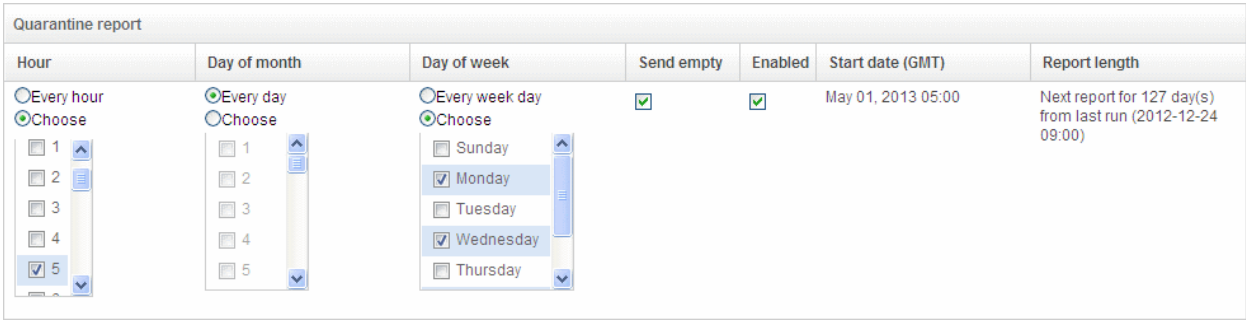
contain a detailed statistics of the mails that are identified as spam or containing malicious content and moved to Quarantine of the domain automatically by CASG. Refer to CASG Reports - An Overview for more details.

- **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. Refer to CASG Reports - An Overview for more details.

To configure the subscription of the reports

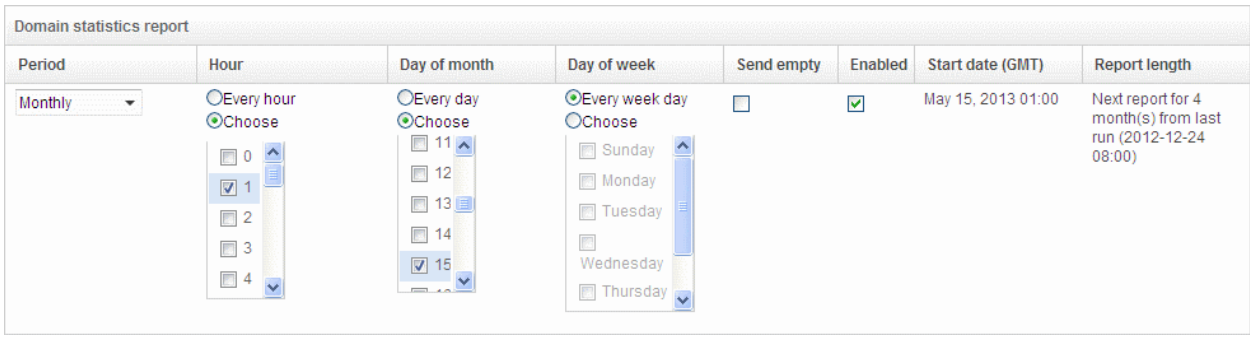
- If you want the administrators of the account to receive the periodical reports, select the 'Enabled' checkbox in the row of the respective report type. If both the reports are required, you can select both the checkboxes.
- Leave the 'Send empty' checkbox unchecked if empty reports are not to be sent to recipients.
- Select the frequency of the report to be sent to the administrators from the options for Quarantine Report and Domain Statistics Report.

Quarantine Report



- **Hour** - The reports will be generated and sent to the administrators 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 will be generated and sent to the administrators every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports will be generated and sent to the administrators 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 will be generated depending on the options chosen.

Domain Statistics Report



- **Period** - Enables you to set the period to be covered in the report. The report will 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 will be generated and sent to the administrators 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 will be generated and sent to the administrators every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports will be generated and sent to the administrators 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 will be generated depending on the options chosen.

Click 'Save' for your settings to take effect.

3.2.1.4.2 Outgoing

To be able to send outgoing email, first a valid user needs to be added to the filter cluster. This can be done from the **web interface.** By default the following port are available for the outgoing service: default recommended port 587 (supports STARTTLS/SSL). 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 and use an **"automatic user locking**" to automatically close the account in case abuse is detected. There are two methods you can make per-user authentication to work - The first method is to instruct all end-users to authenticate directly to the filter cluster for their outgoing emails or in the second method, configure your current outgoing SMTP server so that it authenticates each end-user separately to the filter cluster for all outgoing emails. If you choose the second method, how easily you can configure your SMTP server depends on the SMTP software.

While using per-user authentication for outgoing mails, ensure to set the limits correctly based on the usage of the end-user and enable automatic locking.

If you find using the per-user authentication method for outgoing mails too cumbersome to set up, the other alternative is to use smarthost setup. In this method, you add a single outgoing account either based on IP or username/password in the filtering server and point all outgoing emails to this server, thus using the filtering cluster as smarthost. Most email servers have '**smarthost setting**' feature with which you can easily accomplish the task of configuring outgoing email filtering. Make sure to disable the '**automatic user locking**' setting to prevent the full server account getting locked even if one end-user sends out spam email. Also ensure to enable '**block spam**' so that individual spam messages will be blocked and the administrator notified.

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

In the 'Outgoing' area of the Manage Domain section you can set a user account for spam checking, clear outgoing cache, search for outgoing email messages and outgoing spam checking.

Click the following links for more details:

- **Clear outgoing cache**
- **Log search**
- **Users**

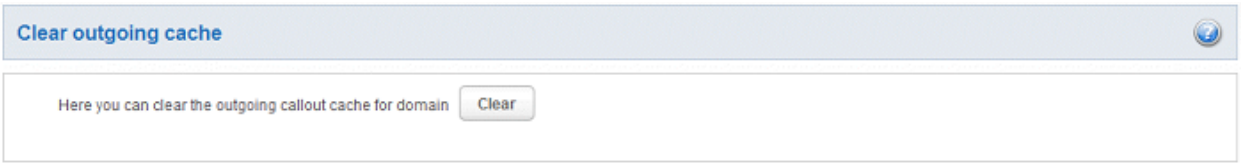
Clear outgoing cache

CASG continuously performs a cached recipient callouts to check that recipient email addresses existing/non-existing email accounts at the destination mail servers 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 will be rejected. CASG filtering servers caches this information locally for up to two hours. CASG interface allows you to clear the callout cache without waiting for the servers to clear it.

To clear outgoing cache

- Click 'Clear outgoing' from the 'Outgoing' drop-down menu in the menu bar or the icon in the 'Outgoing' configuration area.

The 'Clear outgoing cache' area of the selected domain will open:



- Click the 'Clear' button.

The callout cache for the outgoing domain is cleared.

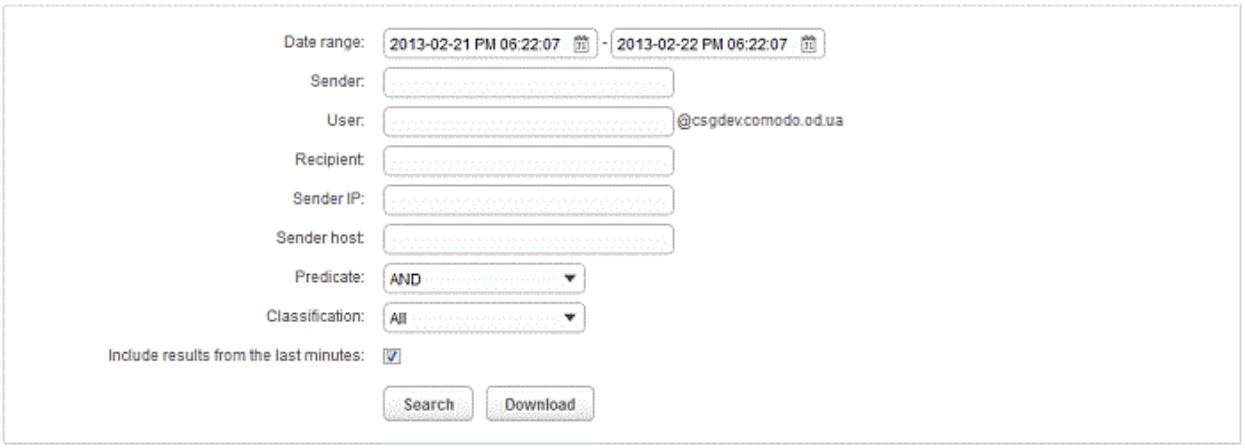
- Click 'X' to close the 'Cache successfully cleared' dialog box.

Log search

The Log Search option in CASG allows you to search for a specific outgoing email message.

- Click 'Log search' from the 'Outgoing' drop-down menu in the menu bar or the icon in the 'Outgoing' configuration area.

The 'Log Search (Outgoing)' interface of the selected domain will open:



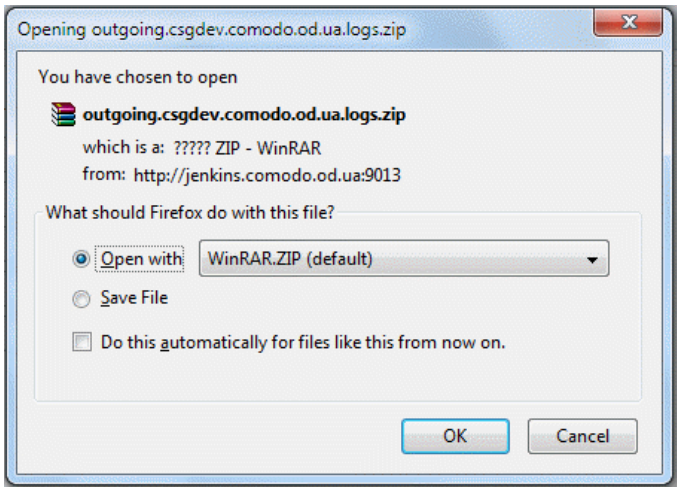
- **Date range:** Select the date range for which you want to search the log file.
- **Sender:** Enter the sender email address in this field.
- **User**: Enter the username of the outgoing email address for in this field (for example, 'testuser1').
- **Recipient:** Enter the email address in this field. (for example, 'testuser1@example.com').
- **Sender IP:** Enter the IP address of the sender.
- **Sender Host:** Enter the sender host name.
- **Predicate:** 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.
- **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.

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

Date and time	Host (Exim id)	Sender hostname	User	Sender	Recipient	Classification
2012-09-27 07:23:44	mxsrv1.dev.spamgatew 1TH8Rh-0000ym-VY	mail2.comodo.od.ua 91.196.95.33	Alice	alice@example.com	evgeniy.logvinenko@co	Accepted Message content looked like non-spam
2012-09-27 07:23:29	mxsrv1.dev.spamgatew 1TH8RJ-0000yj-94	mail2.comodo.od.ua 91.196.95.33	Tucker	tucker@example.com	evgeniy.logvinenko@co	Rejected External pattern match
2012-09-27 07:22:58	mxsrv1.dev.spamgatew 1TH8Qo-0000yQ-7v	mail2.comodo.od.ua 91.196.95.33	Tucker	tucker@example.com	evgeniy.logvinenko@co	Rejected External pattern match
2012-09-27 07:22:39	mxsrv1.dev.spamgatew 1TH8Qc-0000xc-FK	mail2.comodo.od.ua 91.196.95.33	Alice	alice@example.com	evgeniy.logvinenko@co	Accepted Message content looked like non-spam
2012-09-27 07:22:27	mxsrv1.dev.spamgatew 1TH8QS-0000xX-L6	mail2.comodo.od.ua 91.196.95.33	Alice	alice@example.com	evgeniy.logvinenko@co	Accepted Message content looked like non-spam
2012-09-27 06:53:51	mxsrv1.dev.spamgatew 1TH7yo-0008UF-Cs	mail2.comodo.od.ua 91.196.95.33	Alice	alice@example.com	evgeniy.logvinenko@co	Accepted Rejected then released
2012-09-27 06:50:28	mxsrv1.dev.spamgatew 1TH7vY-0008Oz-Ar	mail2.comodo.od.ua 91.196.95.33	Tucker	tucker@example.com	evgeniy.logvinenko@co	Rejected Blacklisted sender

The **'Download'** button allows admin to retrieve from CASG a raw log of messages from the selected domain. The compressed Exim4 log containing all entries for the selected domain can be downloaded from this interface.

Press the download button, the download dialog will open.



You can choose to open the file by using the browse option or save the file in your system. The compressed log file will be saved in the folder that you have configured for saving download files.

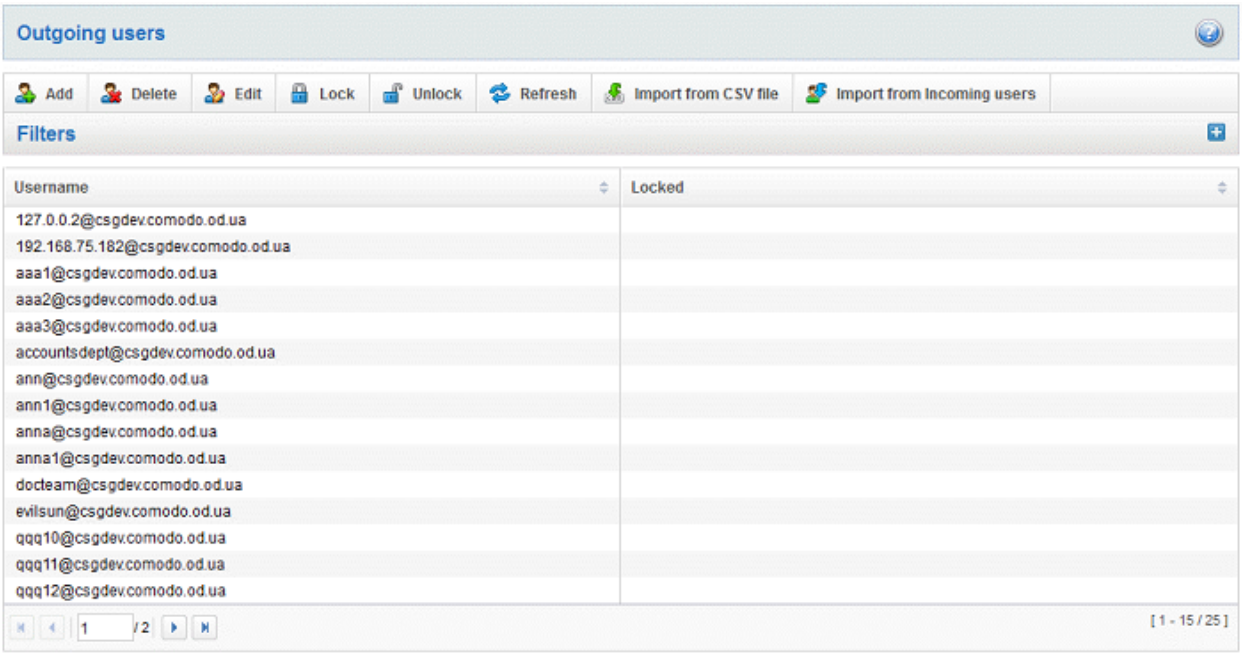
Users

Outgoing email messages should be checked for spam or malicious content because of the risk such content poses to the organization's 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.

- Click 'Users' from the 'Outgoing' drop-down menu in the menu bar or the

icon in the 'Outgoing' configuration area.

The 'Users' interface of the selected domain will open:

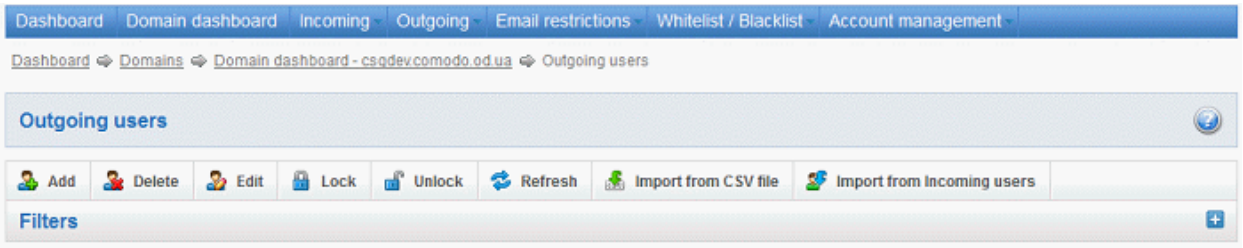


Sorting the Entries

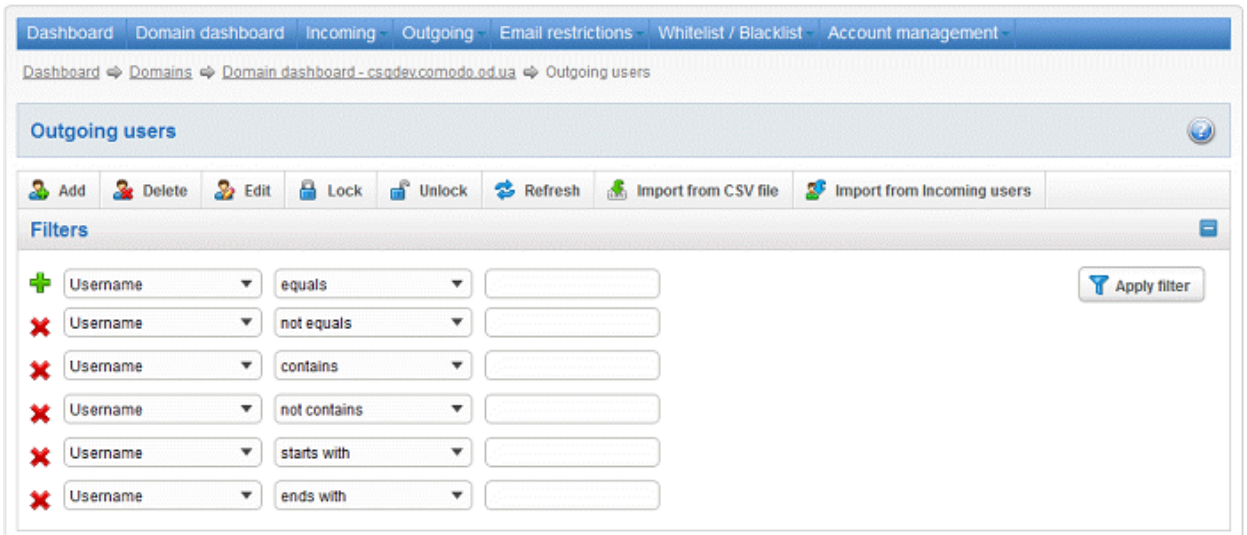
Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Using Filter option to search users

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



You can refine your search much further by clicking ✚ to add more filters.



You can remove a filter by clicking the ✖ icon beside it.

- Type the text in the third field box(es) and click 'Apply Filter'.

The application will search the respective column(s) according to the filter(s) set and display the result.

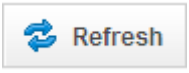
Following is the option in the first drop-down in the filters area:

Username: Displays the result based on the text entered in the text box for the 'Username' column.

The following filters are available in the second drop-down:

- **Equals:** Displays the results based on the user name that was entered in full in the text box.
- **Not Equals:** Displays all user(s), except the one entered in the text box.
- **Contains:** Displays all user(s) that contains the words entered in the text box.
- **Not Contains:** Displays all user(s) that does not contain the words entered in the text box.
- **Starts With:** Displays all user(s) that starts with the words entered in the text box.
- **Ends With**: Displays all user(s) that ends with the words entered in the text box.

Click anywhere on the Filters tab to close the filters area.

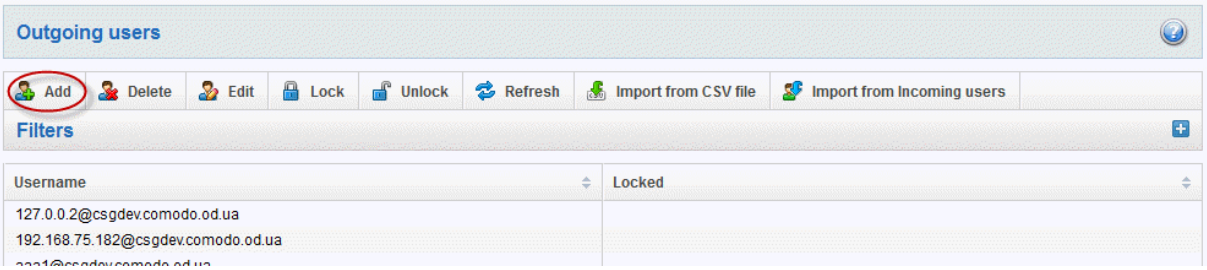
Click the 

button to display all the outgoing users.

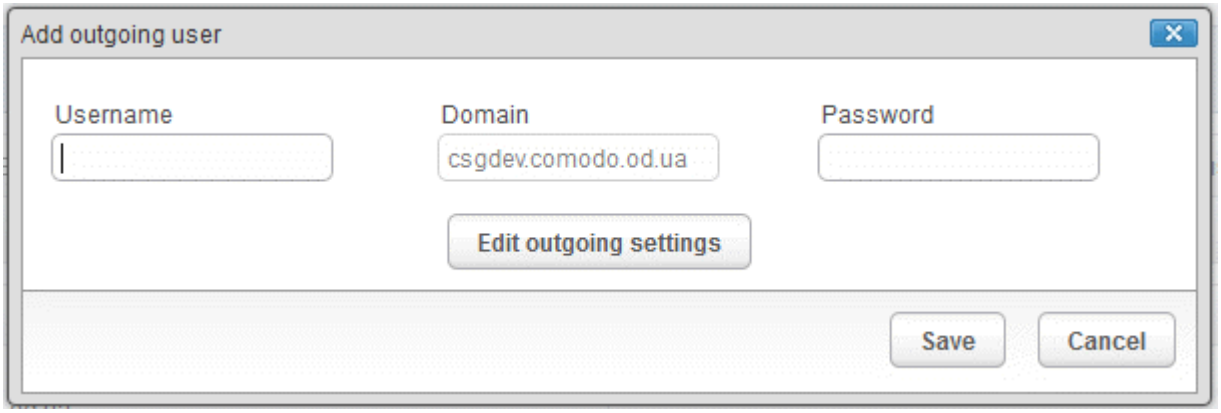
Note: To display all the users after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

To add a new user

- Click the 'Add' button.



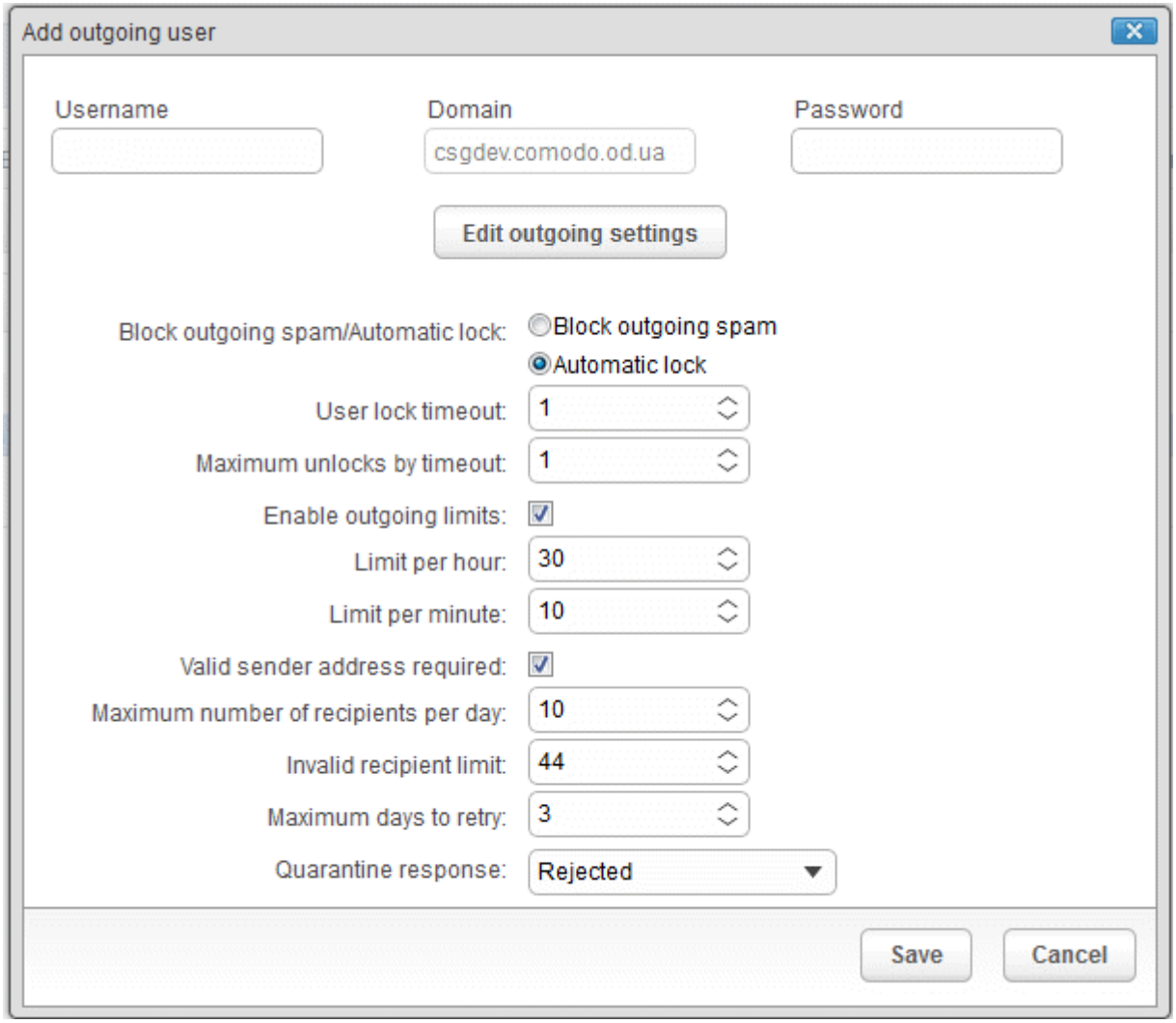
The 'Add outgoing user' dialog will open.



- Enter the username of a new 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 filed. 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' to set the outgoing user's measures. The 'Add outgoing settings' dialog will expand:



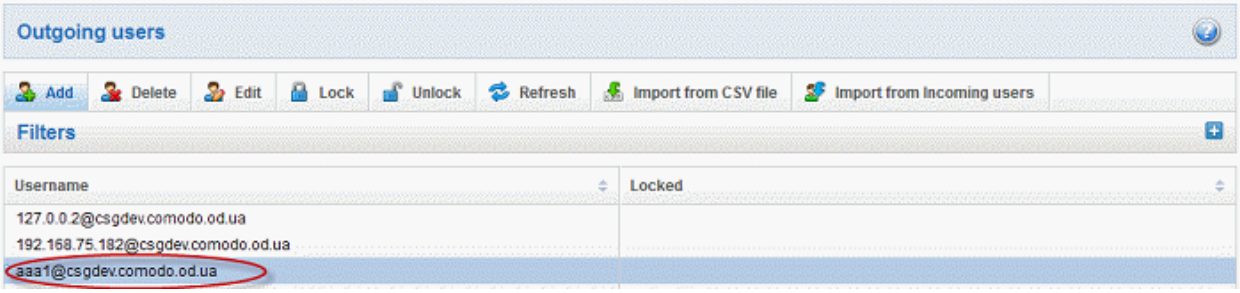
- **Block outgoing spam/Automatic lock** – Tip this setting if you wish to enable spam filtering on outgoing email / enables to automatically lock outgoing mails.
- **User lock timeout** – Allows you to to change the user lock timeout.
- **Maximum unlocks by timeout -** Change the maximum number of unlocks per user timeout.
- **Enable outgoing limits –** Allows you to activate /deactivate limits on outgoing mail.
- **Limit per hour -** The amount of outgoing mail that can be sent per hour.
- **Limit per minute** - The amount of outgoing mail that can be sent per minute.
- **Valid sender address required** – Allows you to verify that it requires a valid sender address.
- **Maximum number of recipients per day** - Allows you to configure the maximum number of recipients a sender can make per day.
- **Invalid recipient limit**: - Allows you to configure the amount of invalid recipients a sender can make per day.
- **Maximum days to retry** - The amount of days to retry with the Automatic retry schedule.
- **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:

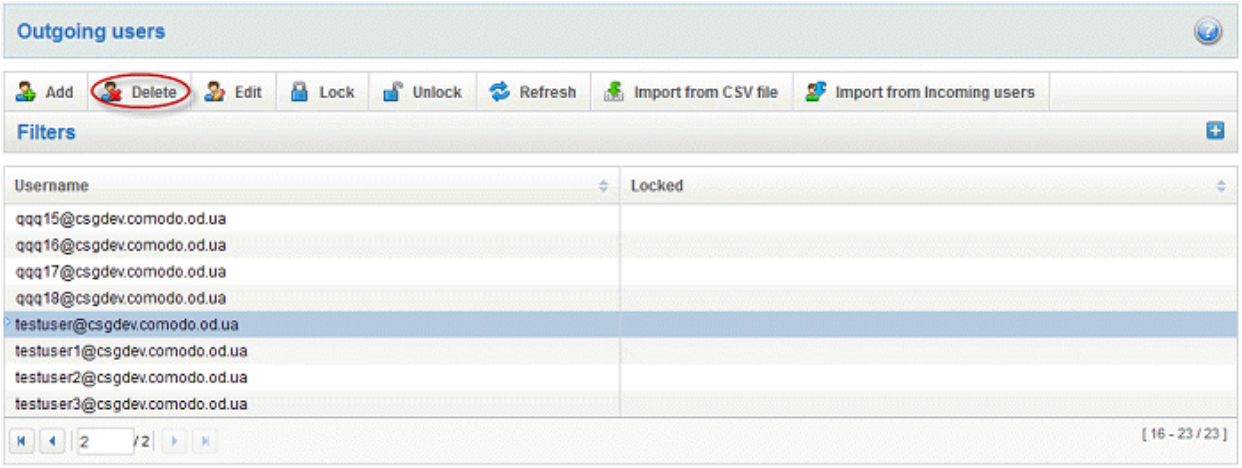
- **Rejected -** Will inform the SMTP server that the email has been rejected by CASG and placed in quarantine. (By default is 'Rejected'.)
- **Accepted -** The email has passed the CASG spam filters and detected as a spam will be placed in quarantine in silent mode.

- Click the 'Save' button.

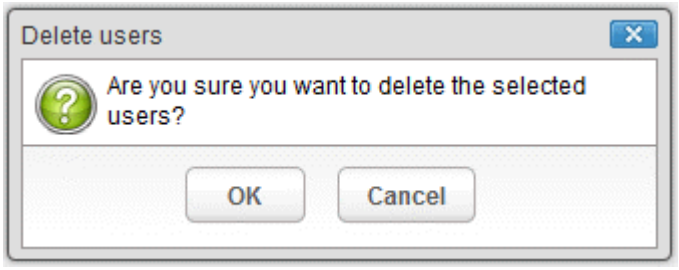


To delete an existing user

- 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.

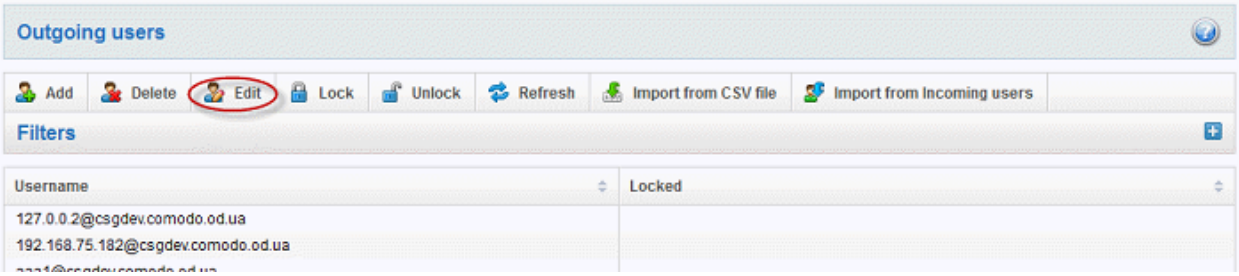


Click 'OK' to confirm your changes.

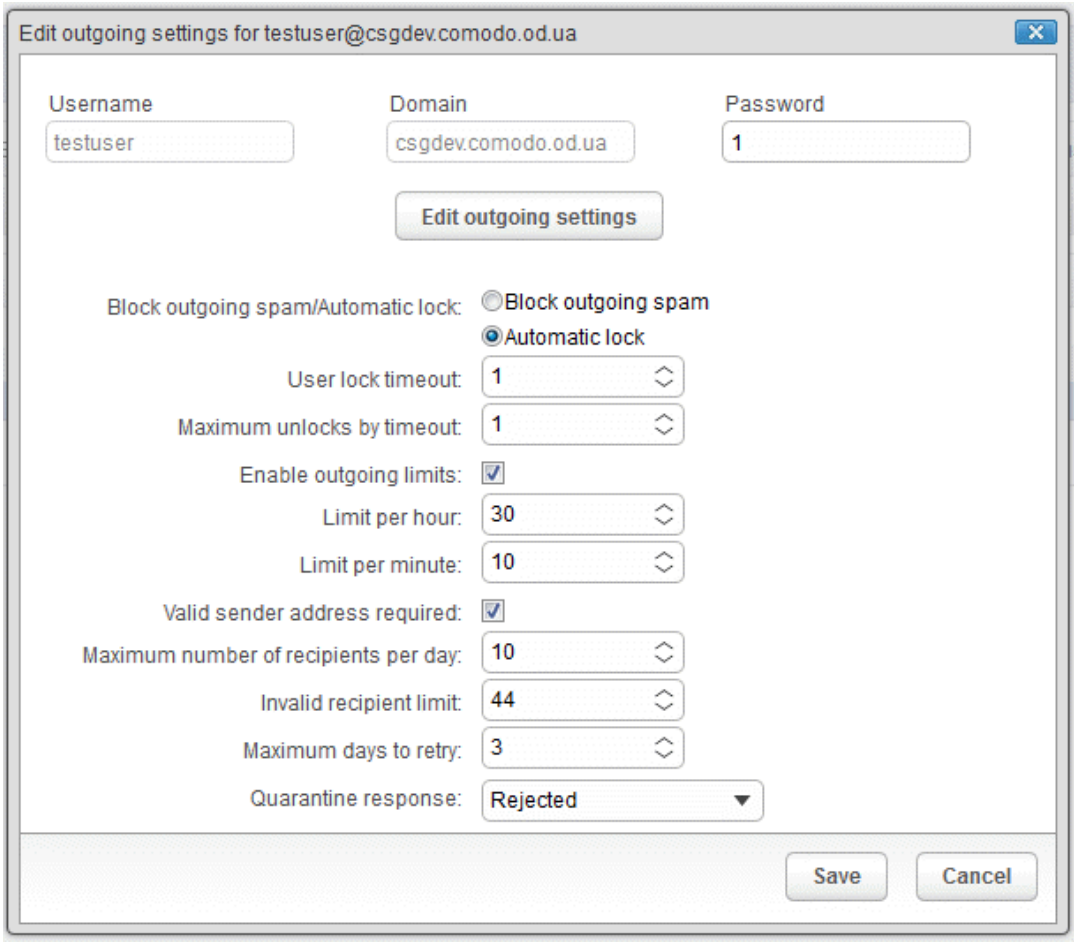
To edit an existing user

You can reset password, adjust the outgoing settings allocated from the 'Add outgoing user' interface.

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



The 'Edit outgoing settings' dialog box will be displayed.



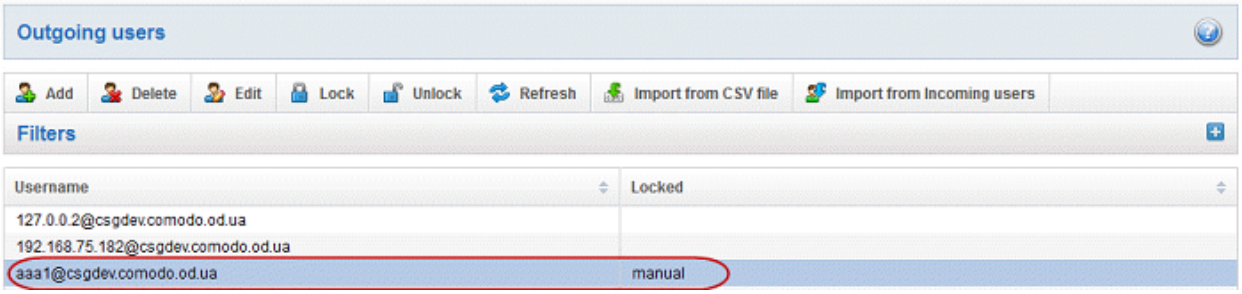
Click the 'Edit outgoing settings' button.

Reset a password in the Password field in case it is forgotten.

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

To lock / unlock user account email manually

This button prevents sending any suspicious outgoing mails manually. Select the outgoing mail and click 'Lock / Unlock' button.

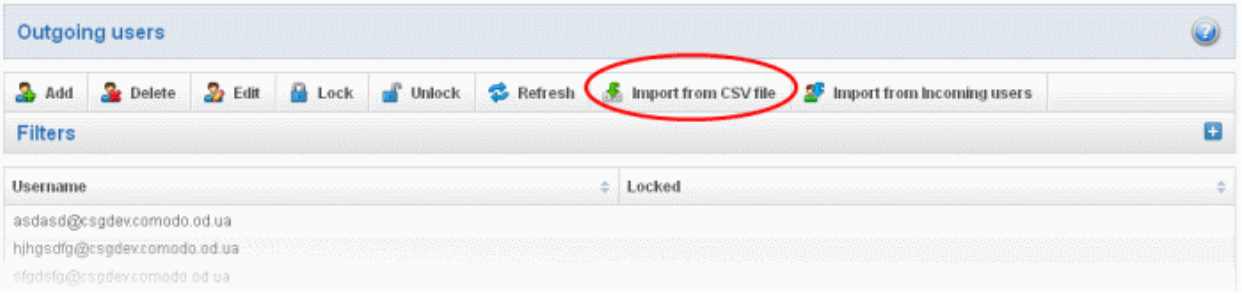


To import from CSV file

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:

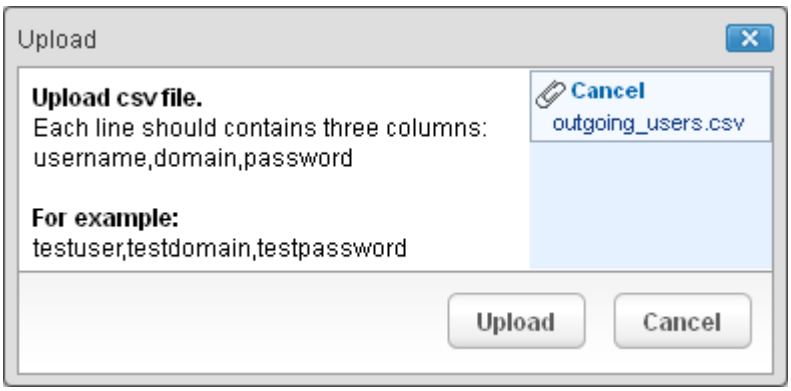
user1,domainname,password
user2,domainname,password

- Click the 'Import from CSV file' button to import outgoing users from a CSV file



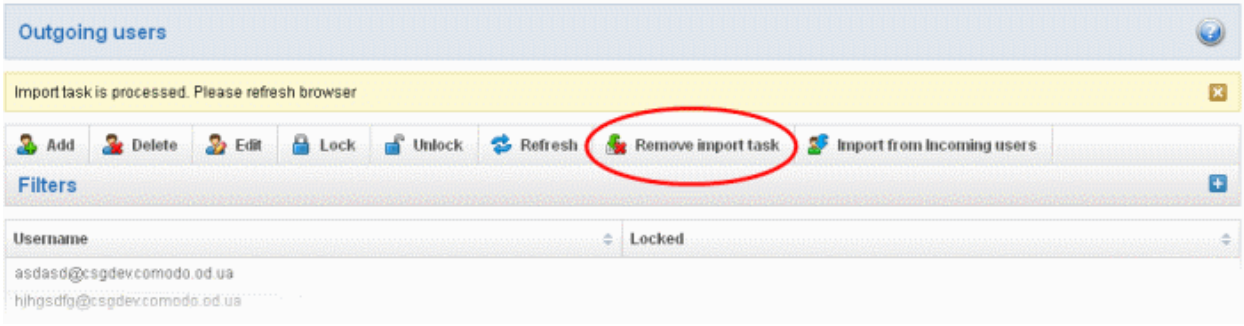
- Click 'Browse...' and navigate to the location where the file is saved and click the 'Open' button.

- The upload process is now ready. The maximum size of the file that can be uploaded is 9 MB. If you want to select another file, click 'Cancel' at top right side of the upload dialog. If you want to cancel the upload process, click the 'Cancel' button located at the bottom.



- Click the 'Upload' button to add new outgoing users.

The upload will be placed in 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* a remaining part of not imported task.



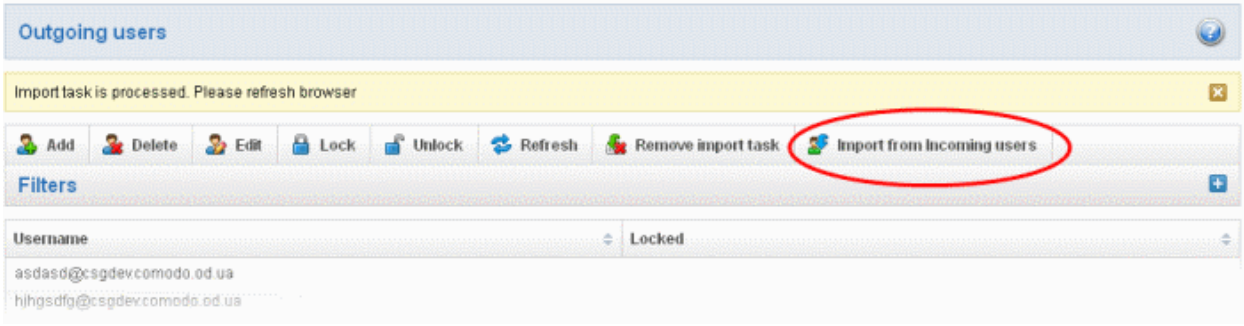
- On completion of the upload process, refresh the browser to view the imported users.

Note: During 'Import from CSV file' process the 'Import from Incoming users' will not be possible till the upload process is completed and vice-versa.

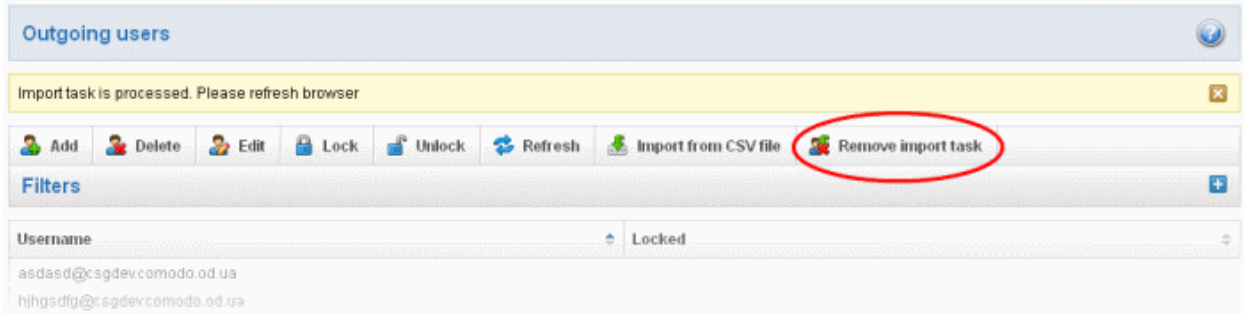
Import from incoming users

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

- Click 'Import from Incoming users' button.

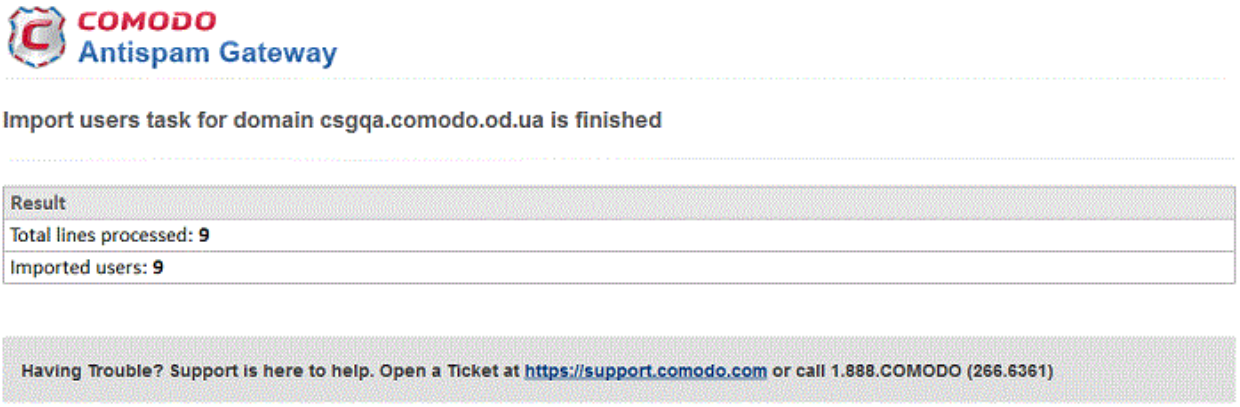


The upload will be placed in import tasks queue and the progress of the upload will be displayed. If you want to remove the upload from the queue, click the 'Remove import task' button. The 'Remove import task' deletes *only* a remaining part of not imported task.



On completion of the upload process, refresh the browser to view the imported users.

The administrator will receive a notification about the import task completion to his email. This notification mail contains the import of users data.



Configuring User's Email Client for Outgoing Mail Filtering

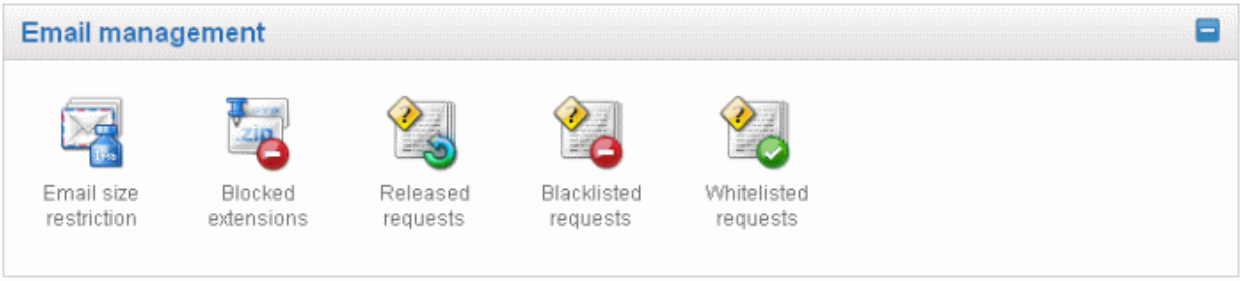
The email clients of the users added for outgoing email filtering are to configured to point to CASG service.

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

- Smtp server: mxsrv1.spamgateway.comodo.com
- Connection Security: STARTTLS or SSL
- Port : 587
- Username: <username@domainname.com>

3.2.1.4.3 Email Management

From this interface an administrator can configure the maximum size of each email and select the file types of attachments to be allowed. An administrator can also choose to release or reject requests from users for releasing quarantined emails, adding senders to blacklist and whitelist.



Click the following links for more details:

- **Email size restriction**
- **Blocked extensions**
- **Released requests**
- **Blacklisted requests**
- **Whitelisted requests**

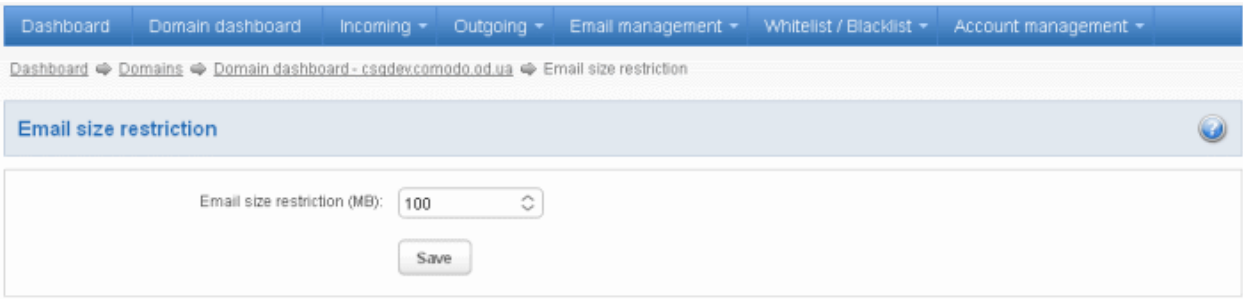
Email Size Restriction

In order to avoid your domain storage space getting used up quickly due to large size of emails, CASG allows you to set the maximum size of each email that are allowed. Administrators have a choice of restricting email size of up to 250 MB. If you require to set the size of email more than 250 MB, please contact your account manager at Comodo or please open a ticket at support.comodo.com or call 1.888.COMODO (2666.6361) and have your account number ready.

To set email size restriction

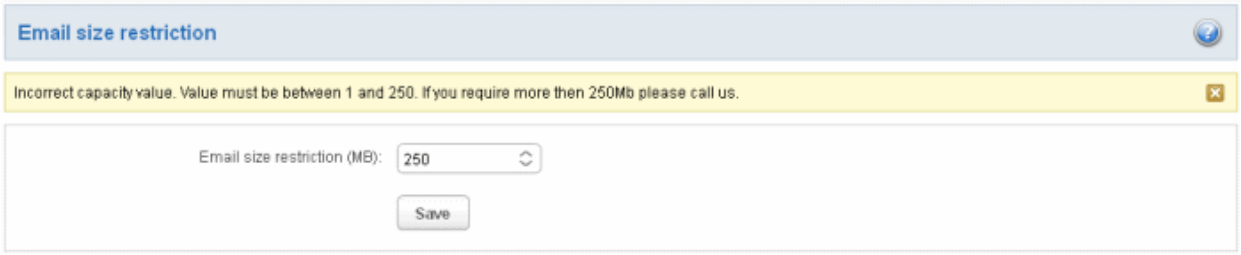
- Click 'Email size restriction' from the 'Email management' drop-down menu in the menu bar or the icon in the 'Email management' configuration area

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



- Enter the maximum allowed size (up to 250 MB) of each email that you want to set in the 'Email size restriction' field.

If you enter a value more than 250 MB, an alert will be displayed to contact your account manager at Comodo and the email size will be automatically set as 250 MB.



- If you want to set the size above 250 MB, please open a ticket at support.comodo.com or call 1.888.COMODO (2666.6361) and have your account number ready.
- Click 'Save' to confirm your changes.

Note: Incoming and outgoing emails with size more than the value set here will be quarantined.

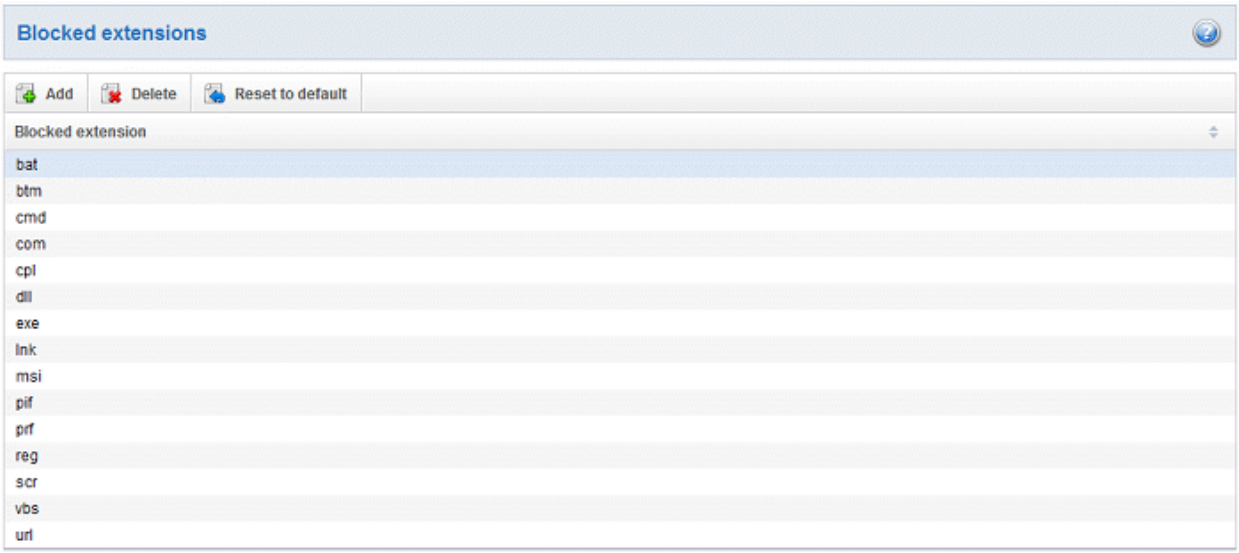
Blocked Extensions

CASG has the ability to restrict certain type of files that are attached with emails from being delivered to the recipients. For example, a file attachment with .exe extension with malicious code has the potential to run automatically while being downloaded and infect the recipient's computer.

To add file extensions to be blocked

- Click 'Blocked extensions' from the 'Email management' drop-down menu in the menu bar or the icon in the 'Email management' configuration area

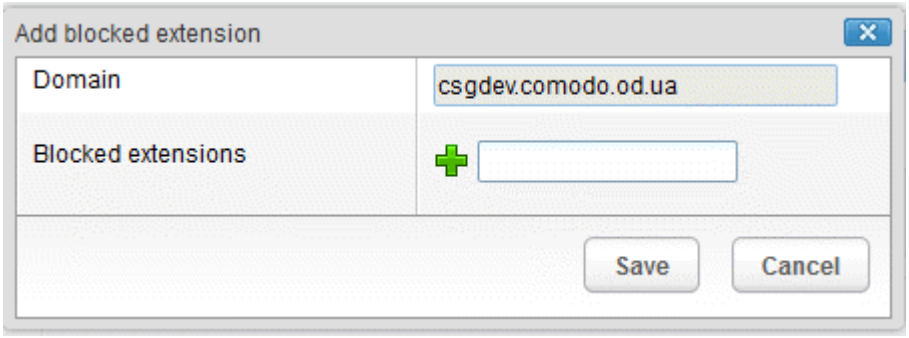
The 'Blocked extensions' interface of the selected domain will open:



The 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.

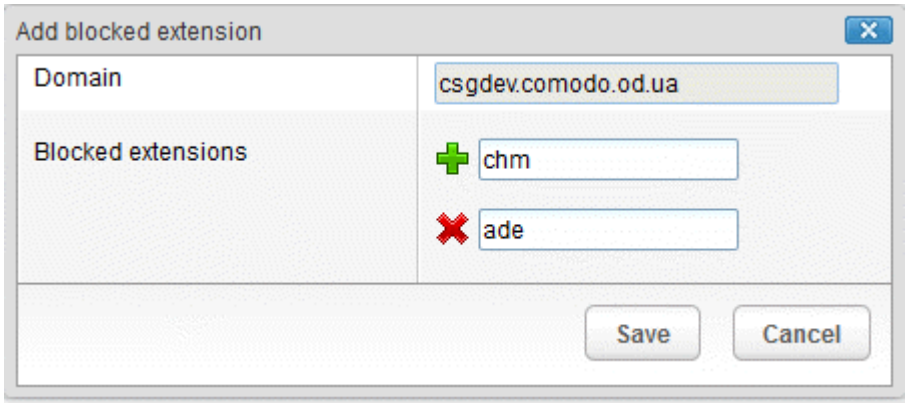
- Click the 'Add' button to include another blocked extension

The 'Add blocked extension' will be displayed.



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

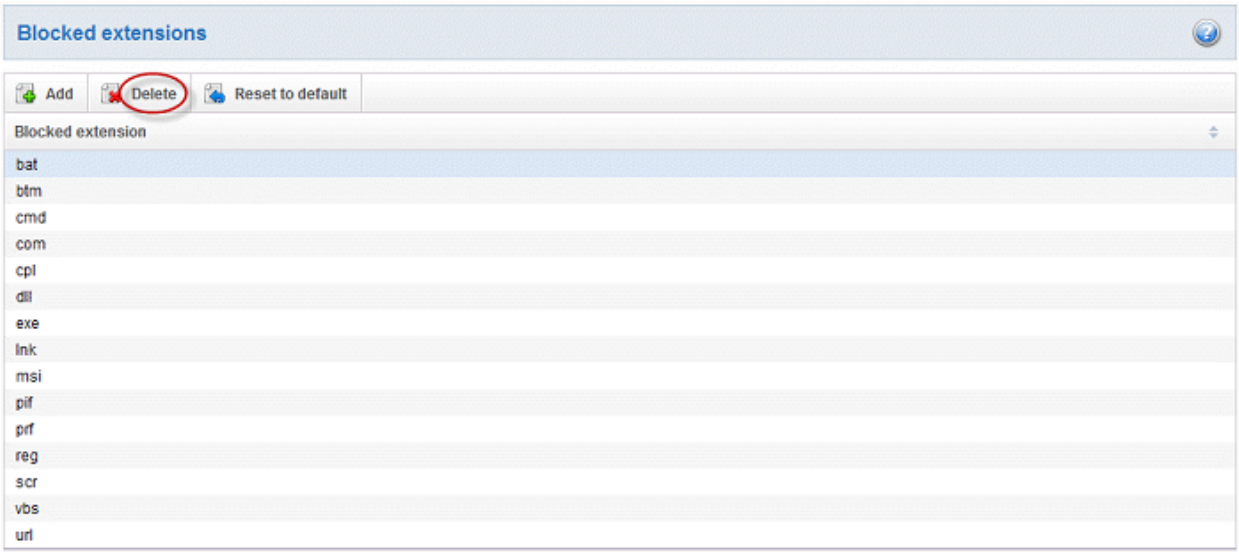
You can add many extensions at a time by clicking the icon.



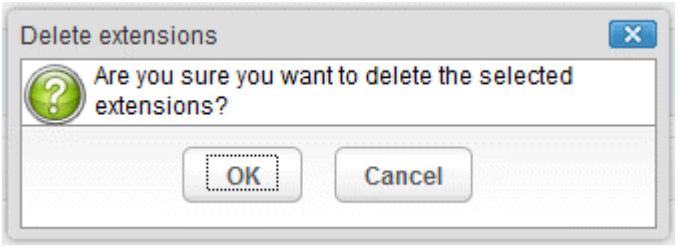
- Click the 'Save' button

The entered extensions will be added to the list.

- To delete an extension, select it from the list and click the 'Delete' button



An alert will be displayed to confirm the delete extensions.



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

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 the 'Reset to default' button to restore default blocked extensions in CASG.

Released Requests

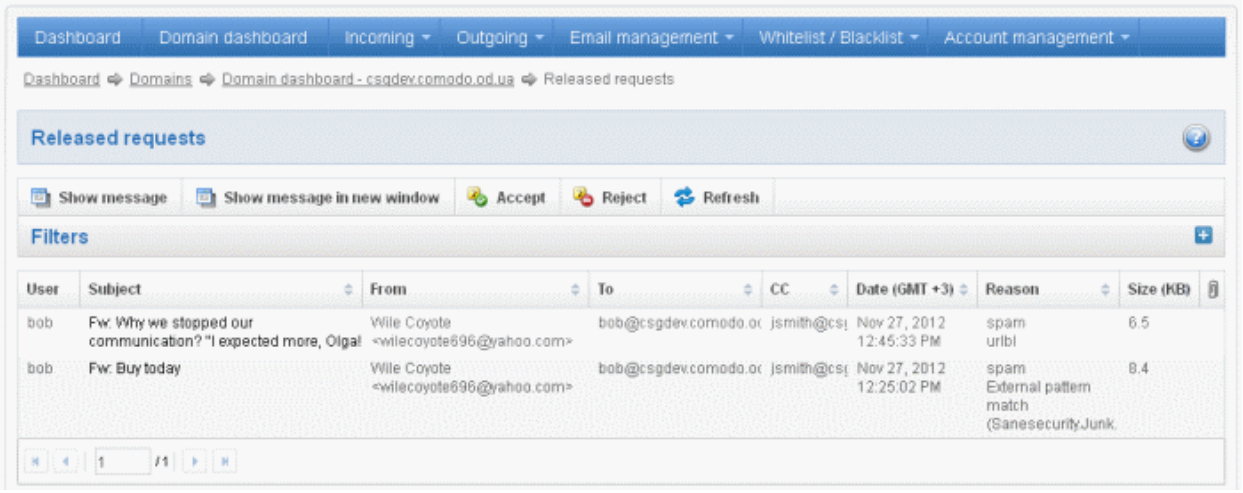
An administrator can choose to release or reject requests from users for releasing quarantined emails from their accounts. The release requests from users will be notified to all admins for that accounts via emails and will also be displayed in the interface. The users who requested for release of quarantined emails will also receive email notifications.

Note: User who have been assigned as 'Power User' can release quarantined mails without approval from the administrators. See the section '**Groups & Permissions**' and '**Managing Permissions**' for more details.

To open the released requests interface

- Click 'Released requests' from the 'Email management' drop-down menu in the menu bar or the icon in the 'Email management' configuration area

The 'Release requests' interface will open:



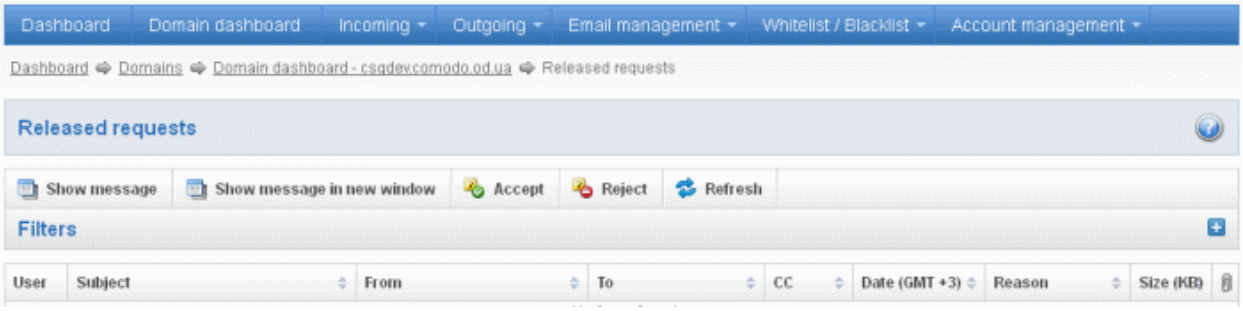
The list of emails that users requested to release will be displayed. The list contains eight columns providing information about the requested user, subject, the sender, details of the recipients, details of recipients in CC list, the date they were sent, the reason they were quarantined and the size of the email. The last column indicates whether there is any attachment in the mails.

Sorting the Entries

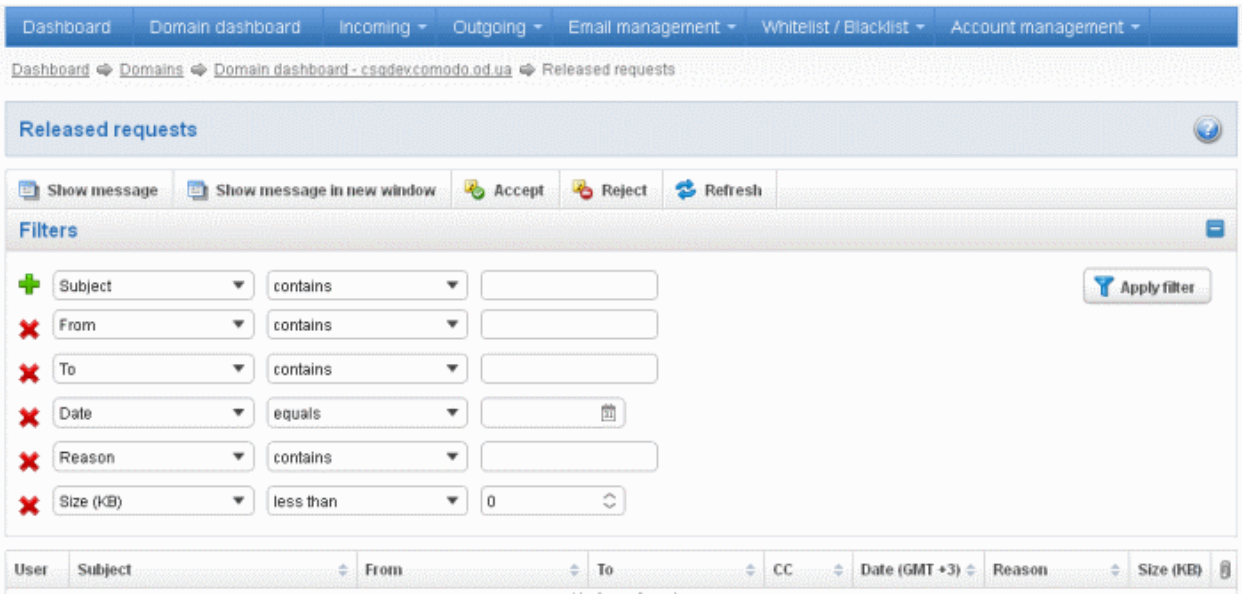
Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Using Filter option to search released requests

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



You can refine your search much further by clicking ✚ to add more filters.



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

- Type the text or select in the field box(es) and click 'Apply Filter'

The application will search the respective column(s) according to the filter(s) set and display the result.

Following are the options in the first drop-down in the filters area:

- **Subject:** Displays the result based on the text entered in the text box for the 'Subject' column
- **From:** Displays the result based on the text entered in the text box for the 'From' column
- **To:** The results are filtered based on the text entered in the text box for the 'To' column
- **Reason**: Displays a quarantined mail according to the selected reason (e.g., “Spam”, "Content", “Malicious attachment”, “Scored 0.5/1.0")

When you select any one of the above options in the first drop-down, the following filters are available in the second drop-down:

- **Contains:** Displays all quarantined mails that contain the words entered in the text box
- **Equals:** Displays all quarantined mails that contain only the words entered in the text box
- **Not Equals:** Displays all quarantined mails that do not contain only the words entered in the text box
- **Not Contains:** Displays all quarantined emails that don't contain the words entered in the text box
- **Starts with:** Displays all quarantined emails that starts with the words entered in the text box
- **Ends with:** Displays all quarantined emails that ends with the words entered in the text box

Other options available in the first drop-down in the filters area:

- **Date:** Displays the results according to the selected date in the third box from the calendar
- **Size (KB):** Displays the results according to size of the mail selected or entered in the third box

When you select 'Date' option in the first drop-down, the following filters are available:

- **Equals:** Displays the quarantined emails that have the same date as the selected date in the third box from the calendar
- **Less than:** Displays the quarantined emails with dates less than the selected date in the third box from the calendar
- **Greater than:** Displays the quarantined emails with dates greater than the selected date in the third box from the calendar

When you select 'Size (KB)' option in the first drop-down, the following filters are available:

- **Less than:** Displays the quarantined emails with size less than the selected or entered size in the third box
- **Greater than:** Displays the quarantined emails with size greater than the selected or entered size in the third box

Click anywhere on the Filters tab to close the filters area.

Click the Refresh button to display all the quarantined emails.

Note: To display all the quarantined emails after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

Viewing Details of Released 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:

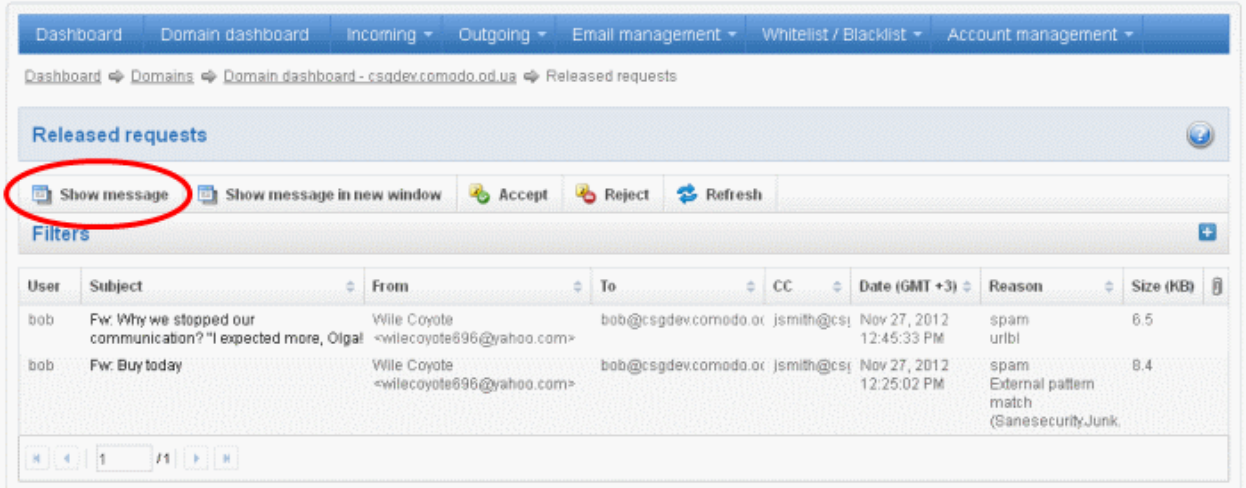
- In the same CASG window
- In a new CASG window

To view details of requested mails for release in the same CASG window:

- In the released requests area, 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.



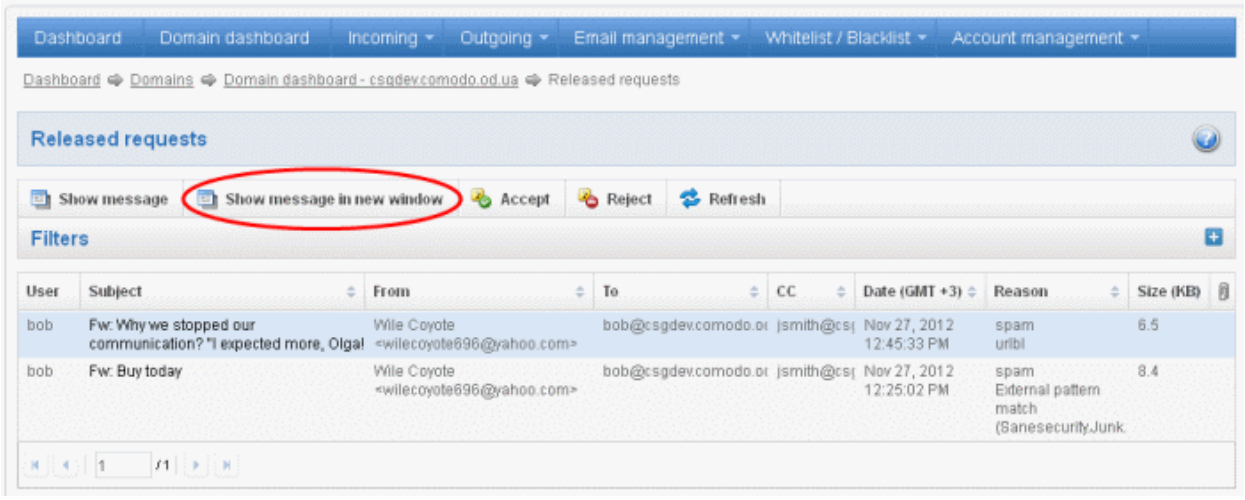
The details of the selected email will be displayed.

To view the email headers, which contain the tracking information of the mail detailing 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.

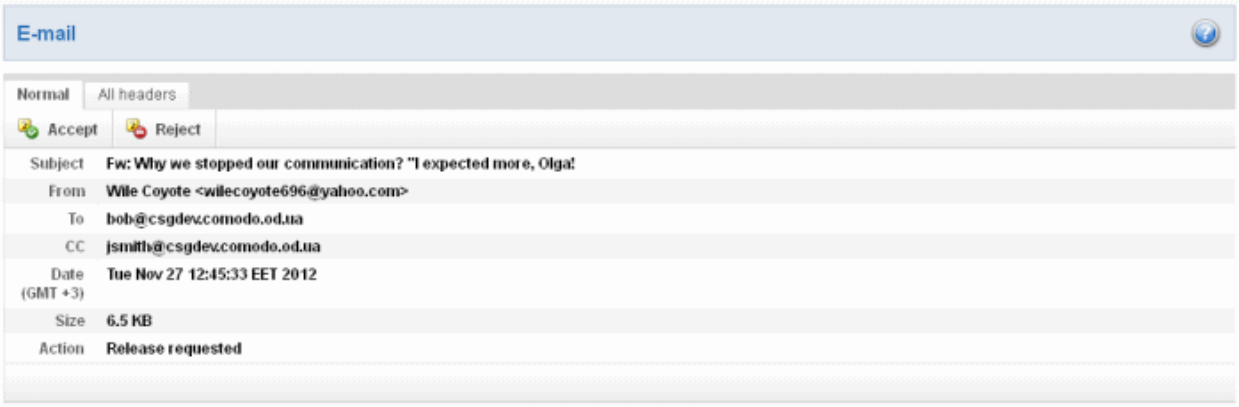
Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either **accept** the mail or **reject** it. If the mail is accepted, it will be released to the user's inbox. If it is rejected, the email will be no longer in the released emails list. Please note that emails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

To view details of requested mails for release in new CASG window:

- In the released email 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.



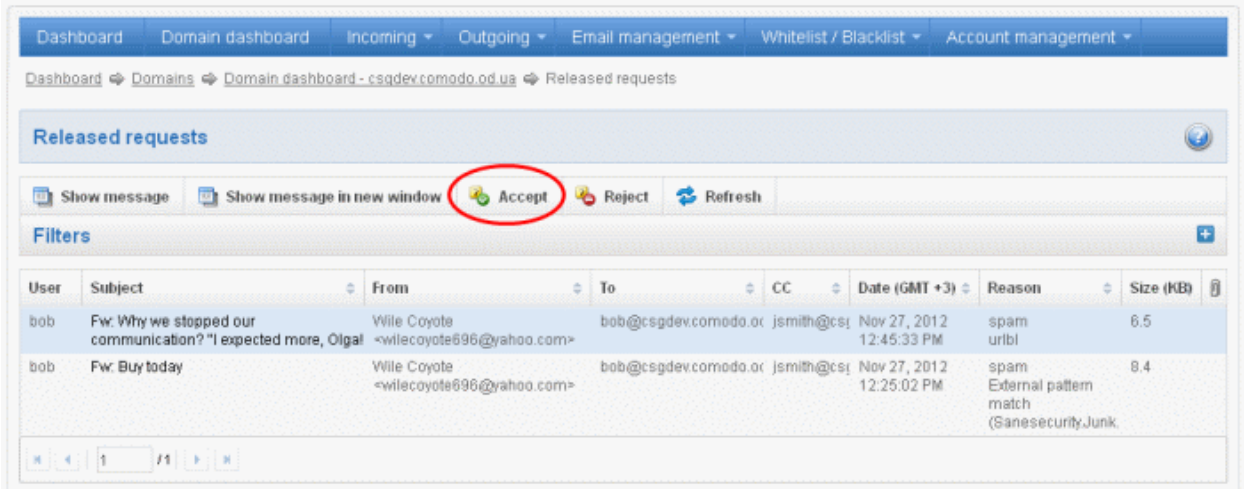
The details of the selected mail will be displayed in a new CASG window.



To 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 respective user.

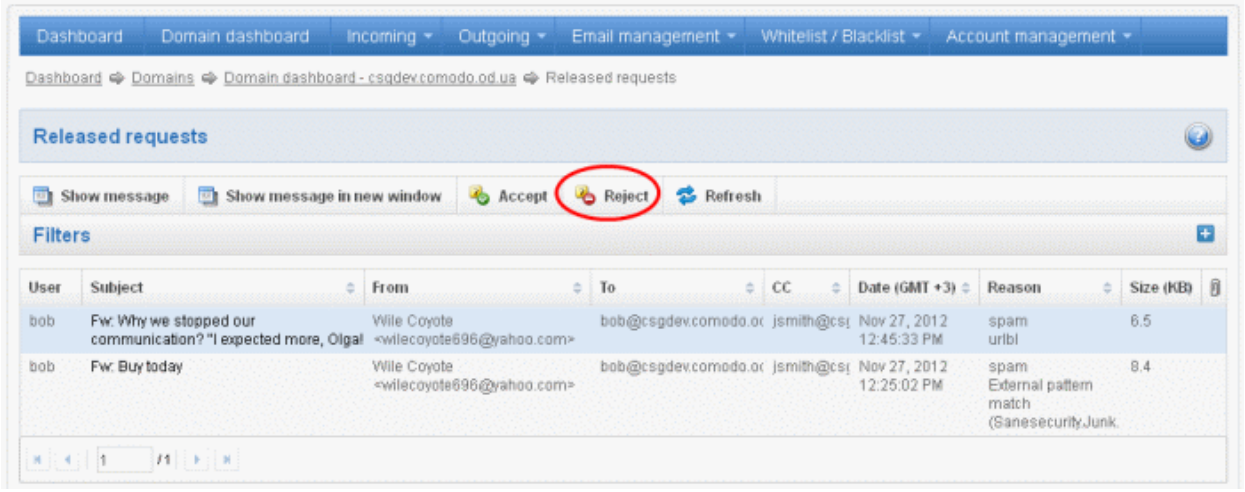
- Click 'OK' to confirm the acceptance.

The email will 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.

To 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.

Blacklisted Requests

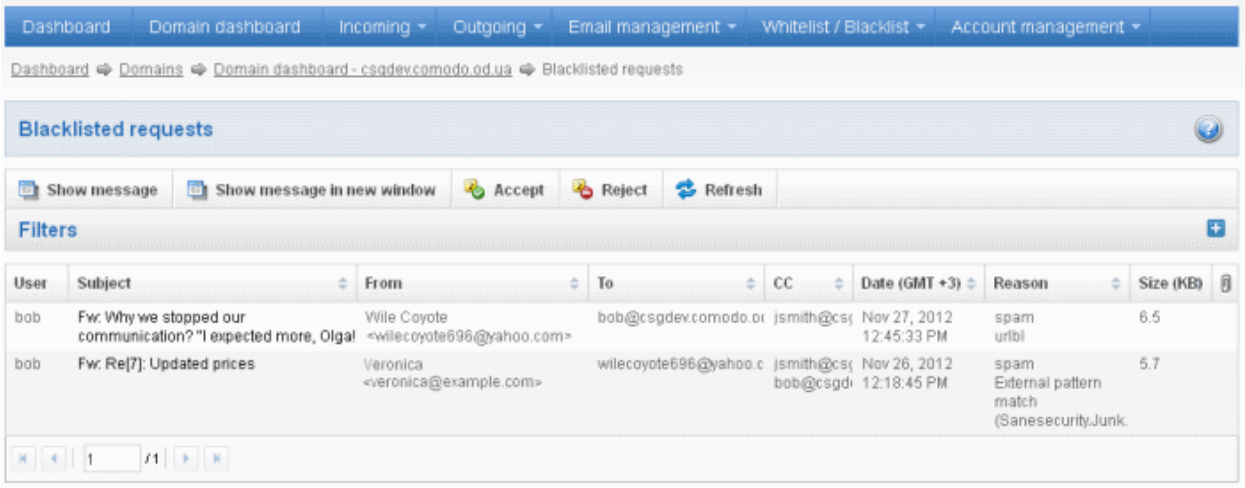
CASG allows users to send requests to their email account administrators to add senders to blacklist. Administrators in addition to receiving emails for these requests also can view the list of such requests in 'Blacklisted requests' section of the administrator interface under 'Email management' section.

To open the blacklisted requests interface

- Click 'Blacklisted requests' from the 'Email management' drop-down menu in the menu bar or the icon in the

'Email management' configuration area

The 'Blacklisted requests' interface will open:



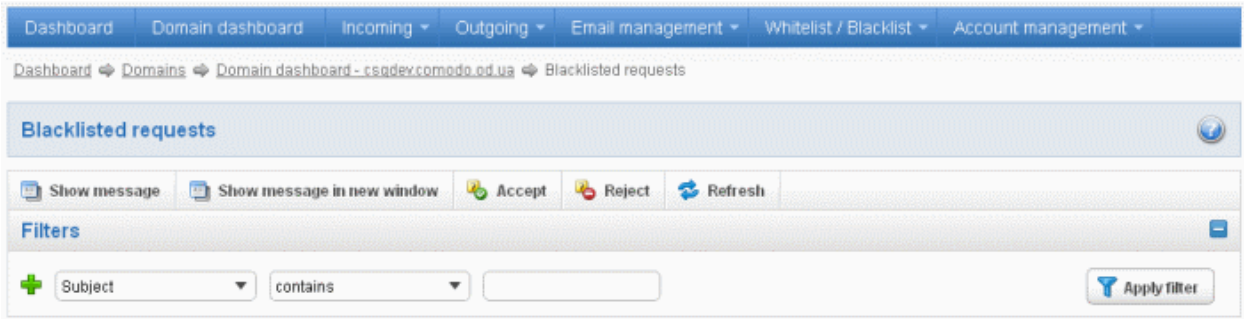
The list of emails that users requested for adding to blacklist will be displayed. The list contains eight columns providing information about the requested user, subject, the sender, details of the recipients, details of recipients in CC list, the date they were sent, the reason they were quarantined and the size of the email. The last column indicates whether there is any attachment in the mails.

Sorting the Entries

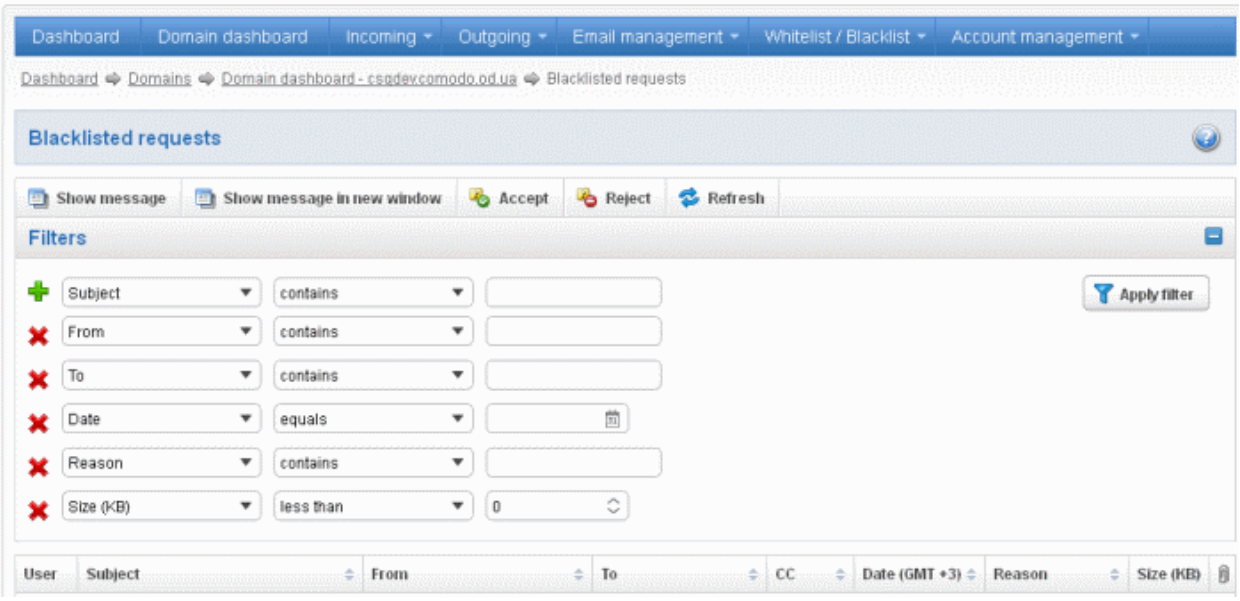
Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Using Filter option to search blacklisted requests

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



You can refine your search much further by clicking ✚ to add more filters.



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

- Type the text or select in the field box(es) and click 'Apply Filter'

The application will search the respective column(s) according to the filter(s) set and display the result.

Following are the options in the first drop-down in the filters area:

- **Subject:** Displays the result based on the text entered in the text box for the 'Subject' column
- **From:** Displays the result based on the text entered in the text box for the 'From' column
- **To:** The results are filtered based on the text entered in the text box for the 'To' column
- **Reason**: Displays a quarantined mail according to the selected reason (e.g., “Spam”, "Content", “Malicious attachment”, “Scored 0.5/1.0")

When you select any one of the above options in the first drop-down, the following filters are available in the second drop-down:

- **Contains:** Displays all quarantined mails that contain the words entered in the text box
- **Equals:** Displays all quarantined mails that contain only the words entered in the text box
- **Not Equals:** Displays all quarantined mails that do not contain only the words entered in the text box
- **Not Contains:** Displays all quarantined emails that don't contain the words entered in the text box
- **Starts with:** Displays all quarantined emails that starts with the words entered in the text box
- **Ends with:** Displays all quarantined emails that ends with the words entered in the text box

Other options available in the first drop-down in the filters area:

- **Date:** Displays the results according to the selected date in the third box from the calendar
- **Size (KB):** Displays the results according to size of the mail selected or entered in the third box

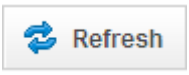
When you select 'Date' option in the first drop-down, the following filters are available:

- **Equals:** Displays the quarantined emails that have the same date as the selected date in the third box from the calendar
- **Less than:** Displays the quarantined emails with dates less than the selected date in the third box from the calendar
- **Greater than:** Displays the quarantined emails with dates greater than the selected date in the third box from the calendar

When you select 'Size (KB)' option in the first drop-down, the following filters are available:

- **Less than:** Displays the quarantined emails with size less than the selected or entered size in the third box
- **Greater than:** Displays the quarantined emails with size greater than the selected or entered size in the third box

Click anywhere on the Filters tab to close the filters area.

Click the 

button to display all the quarantined emails.

Note: To display all the quarantined emails after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

Viewing 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:

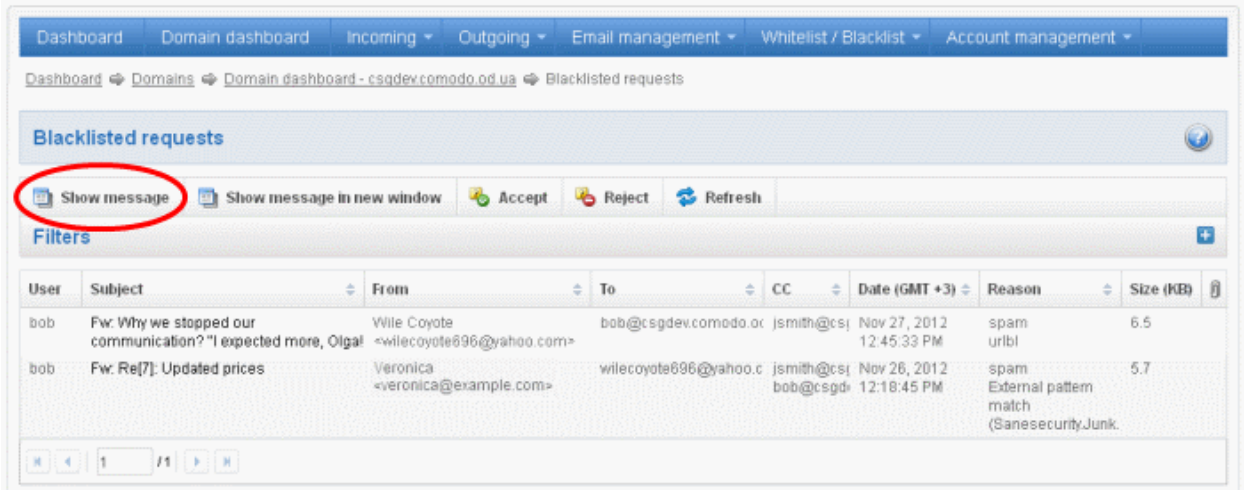
- In the same CASG window
- In a new CASG window

To view details of blacklisted requests in the same CASG window:

- In the blacklisted requests area, 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 details of the selected email will be displayed.

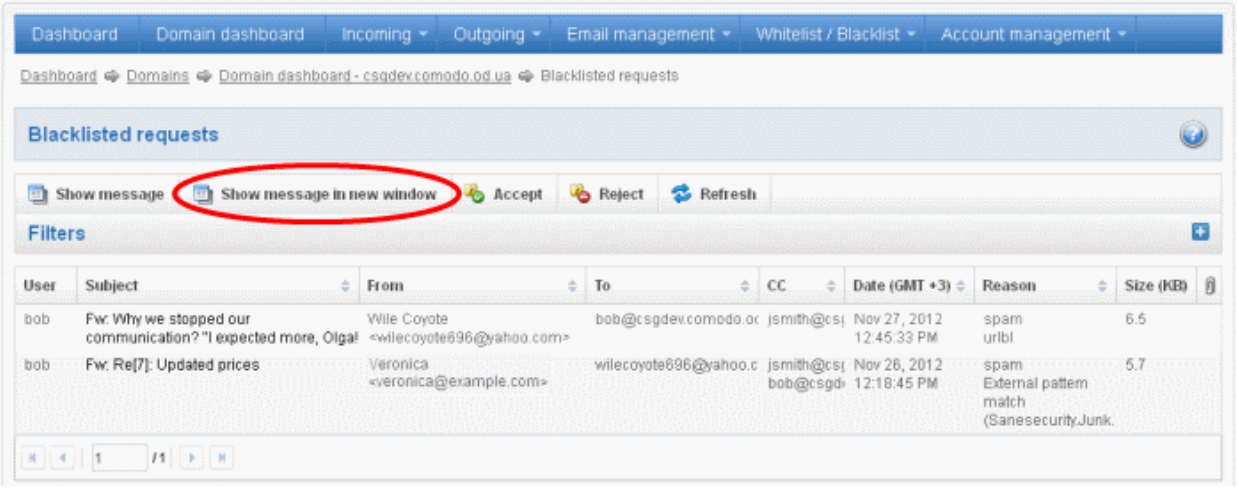
To view the email headers, which contain the tracking information of the mail detailing the path it has crossed before reaching

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.

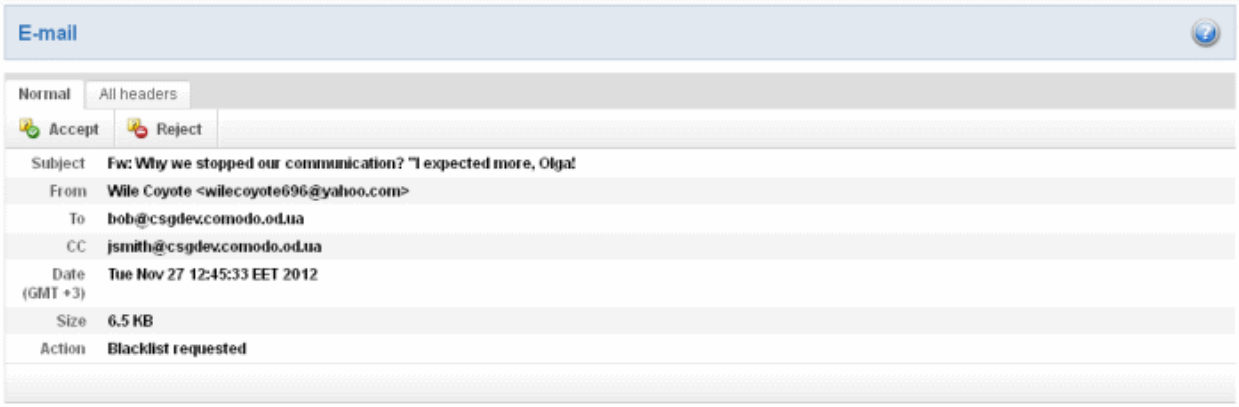
Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either **accept** the mail or **reject** it for blacklisting the sender. If the mail is accepted, the sender will be added to '**Sender blacklist**'. If it is rejected, the email will be no longer in the blacklisted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

To view details of blacklisted requests in new CASG window:

- In the blacklisted 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.



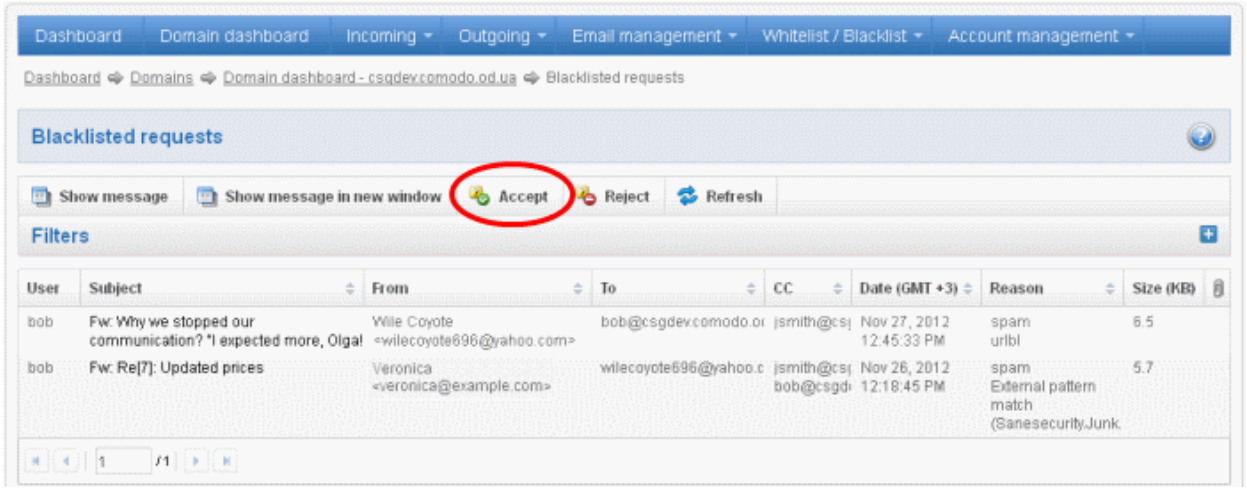
The details of the selected mail will be displayed in a new CASG window.



To 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.

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



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

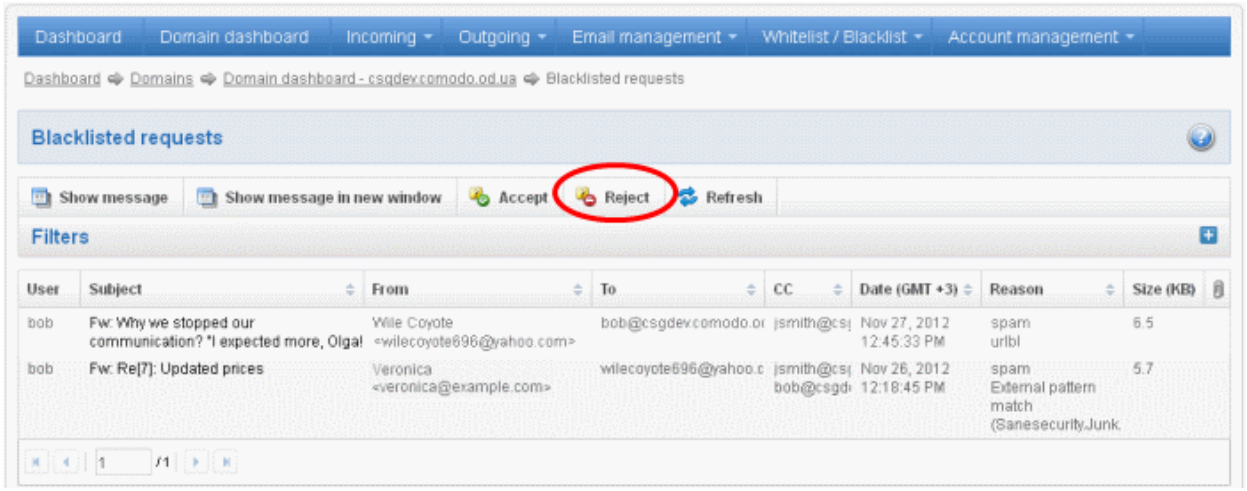
- Click 'OK' to confirm the acceptance.

The sender of the email will be added to 'Sender blacklist'. See the section '**Sender blacklist**' for more details.

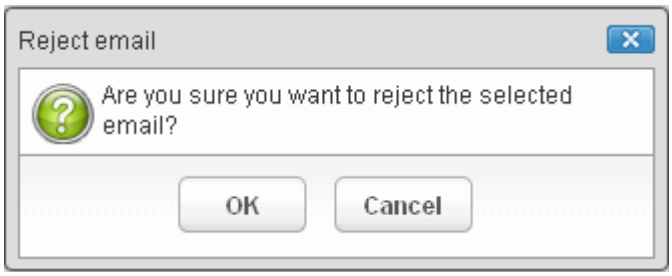
To reject the blacklist request from users

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.

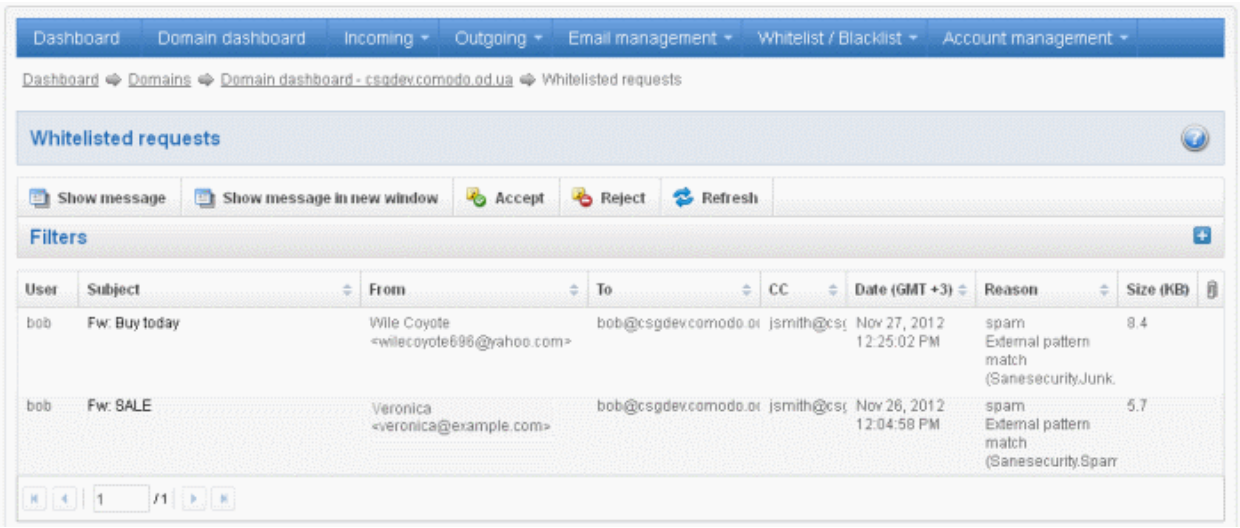
Whitelisted Requests

CASG allows users to send requests to their email account administrators to add senders to whitelist from their Quarantine interface. Administrators in addition to receiving emails for these requests also can view the list of such requests in 'Whitelisted requests' section of the administrator interface under 'Email management' section.

To open the whitelisted requests interface

- Click 'Whitelisted requests' from the 'Email management' drop-down menu in the menu bar or the icon in the 'Email management' configuration area.

The 'Whitelisted requests' interface will open:



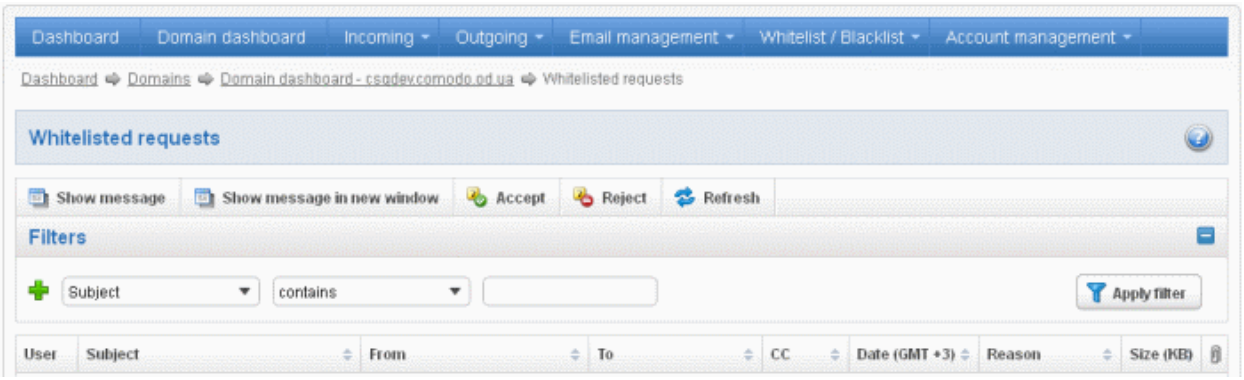
The list of emails that users requested for adding the senders to whitelist will be displayed. The list contains eight columns providing information about the requested user, subject, the sender, details of the recipients, details of recipients in the CC list, the date they were sent, the reason they were quarantined and the size of the email. The last column indicates whether there is any attachment in the mails.

Sorting the Entries

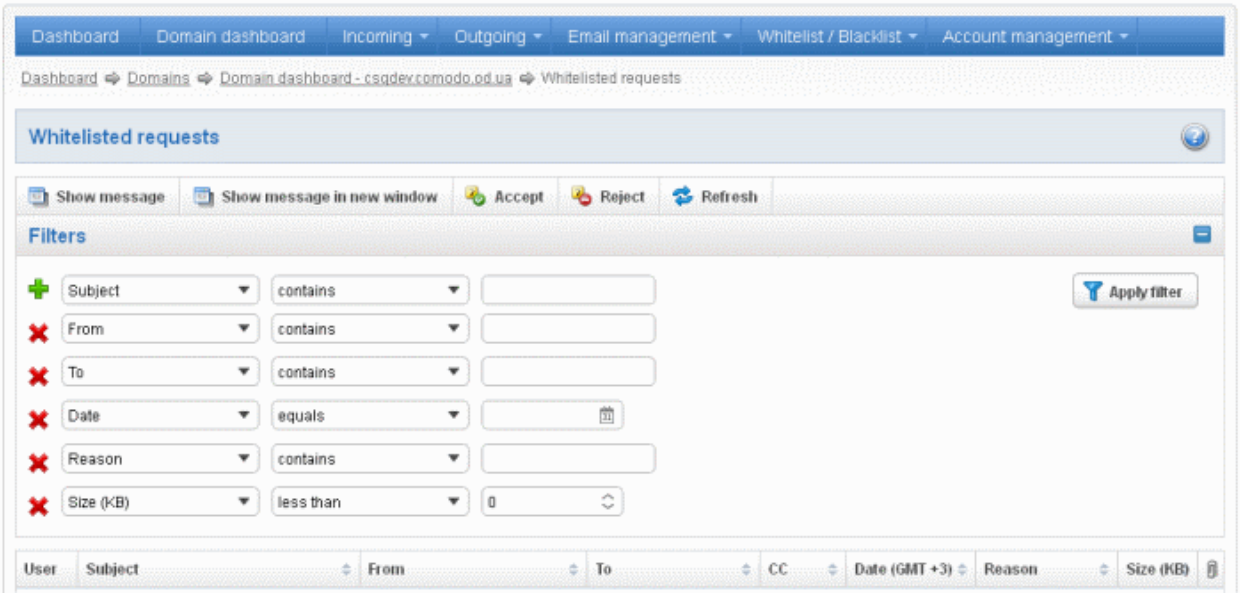
Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Using Filter option to search whitelisted requests

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



You can refine your search much further by clicking ✚ to add more filters.



You can remove a filter by clicking the ✖ icon beside it.

- Type the text or select in the field box(es) and click 'Apply Filter'

The application will search the respective column(s) according to the filter(s) set and display the result.

Following are the options in the first drop-down in the filters area:

- **Subject:** Displays the result based on the text entered in the text box for the 'Subject' column
- **From:** Displays the result based on the text entered in the text box for the 'From' column
- **To:** The results are filtered based on the text entered in the text box for the 'To' column
- **Reason**: Displays a quarantined mail according to the selected reason (e.g., “Spam”, "Content", “Malicious attachment”, “Scored 0.5/1.0")

When you select any one of the above options in the first drop-down, the following filters are available in the second drop-down:

- **Contains:** Displays all quarantined mails that contain the words entered in the text box
- **Equals:** Displays all quarantined mails that contain only the words entered in the text box
- **Not Equals:** Displays all quarantined mails that do not contain only the words entered in the text box
- **Not Contains:** Displays all quarantined emails that don't contain the words entered in the text box
- **Starts with:** Displays all quarantined emails that starts with the words entered in the text box
- **Ends with:** Displays all quarantined emails that ends with the words entered in the text box

Other options available in the first drop-down in the filters area:

- **Date:** Displays the results according to the selected date in the third box from the calendar

- **Size (KB):** Displays the results according to size of the mail selected or entered in the third box

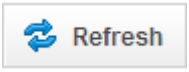
When you select 'Date' option in the first drop-down, the following filters are available:

- **Equals:** Displays the quarantined emails that have the same date as the selected date in the third box from the calendar
- **Less than:** Displays the quarantined emails with dates less than the selected date in the third box from the calendar
- **Greater than:** Displays the quarantined emails with dates greater than the selected date in the third box from the calendar

When you select 'Size (KB)' option in the first drop-down, the following filters are available:

- **Less than:** Displays the quarantined emails with size less than the selected or entered size in the third box
- **Greater than:** Displays the quarantined emails with size greater than the selected or entered size in the third box

Click anywhere on the Filters tab to close the filters area.

Click the 

button to display all the quarantined emails.

Note: To display all the whitelisted requests after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

Viewing 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:

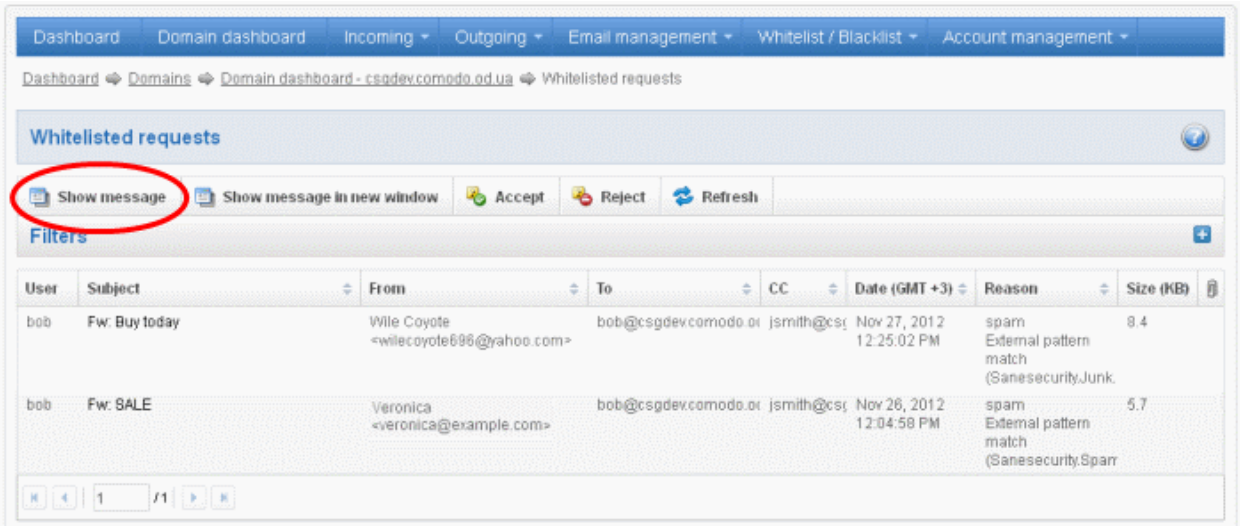
- In the same CASG window
- In a new CASG window

To view details of whitelisted requests in the same CASG window:

- In the whitelisted requests area, 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.



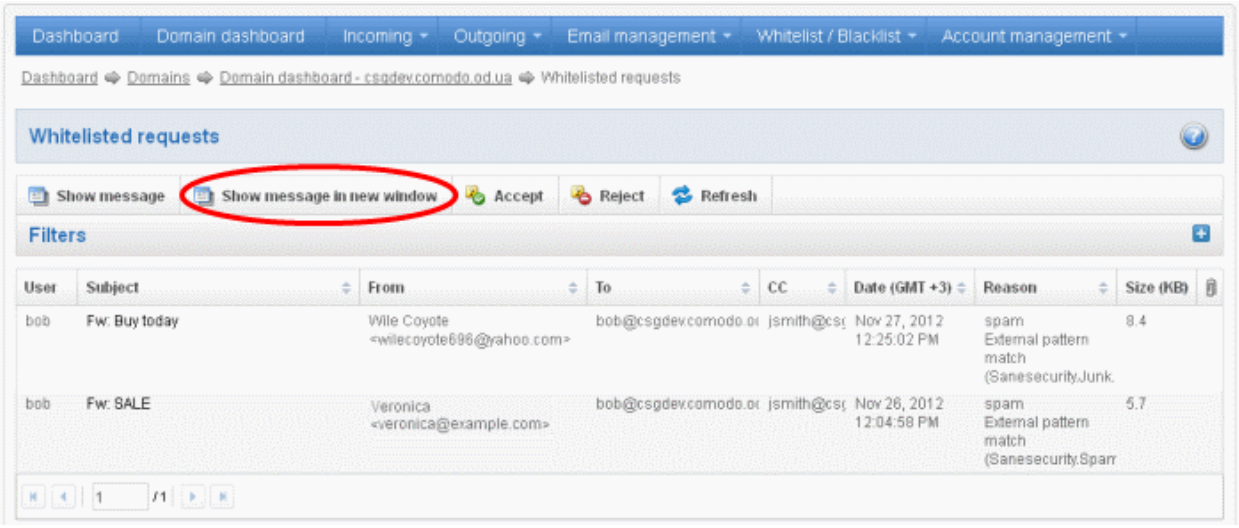
The details of the selected email will be displayed.

To view the email headers, which contain the tracking information of the mail detailing 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 for whitelisting the sender. If the mail is accepted, the sender will be added to '**Sender Whitelist**'. 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.

To 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.

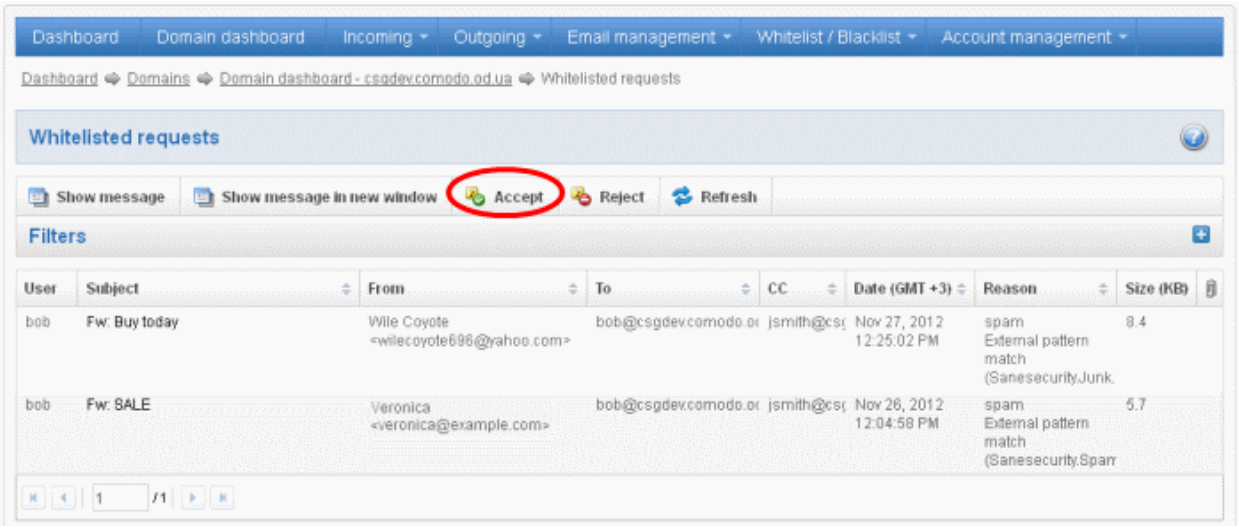


The details of the selected mail will be displayed in a new CASG window.

To 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.

- 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 '**Sender Whitelist**'.

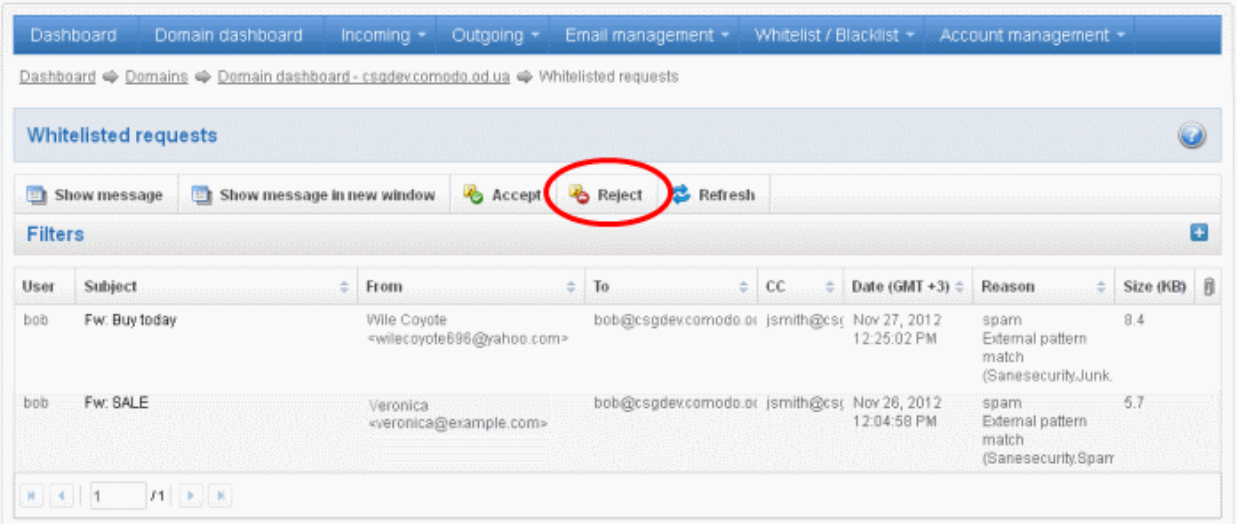
- Click 'OK' to confirm the acceptance.

The sender of the email will be added to 'Sender whitelist'. See the section '**Sender Whitelist**' for more details.

To 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.

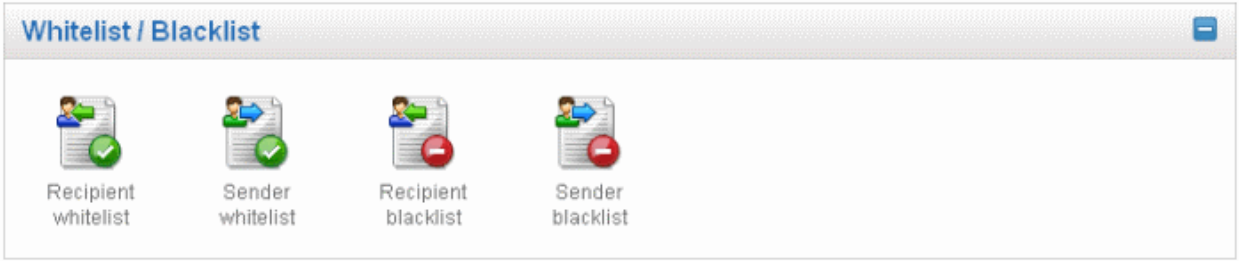
- Click 'OK' to confirm the rejection.

The sender will not be added to whitelist and the selected email will no longer be in the whitelisted requests list.

3.2.1.4.4 Whitelist / Blacklist

CASG allows the administrator of a domain to configure recipients or senders in whitelist or blacklist. While all filtering settings are disabled for whitelisted recipients, all mails sent by blacklisted senders are automatically rejected. Administrators can also choose to whitelist or blacklist a particular set of recipients/senders or a whole domain using wildcard character.

The Administrators can export the whitelists and blacklists to comma separated values CSV files, which can be used in future if the users are to be re-added to the lists.



Click the following links for more details.

- **Recipient Whitelist**
- **Sender Whitelist**
- **Recipient Blacklist**
- **Sender Blacklist**

Recipient Whitelist

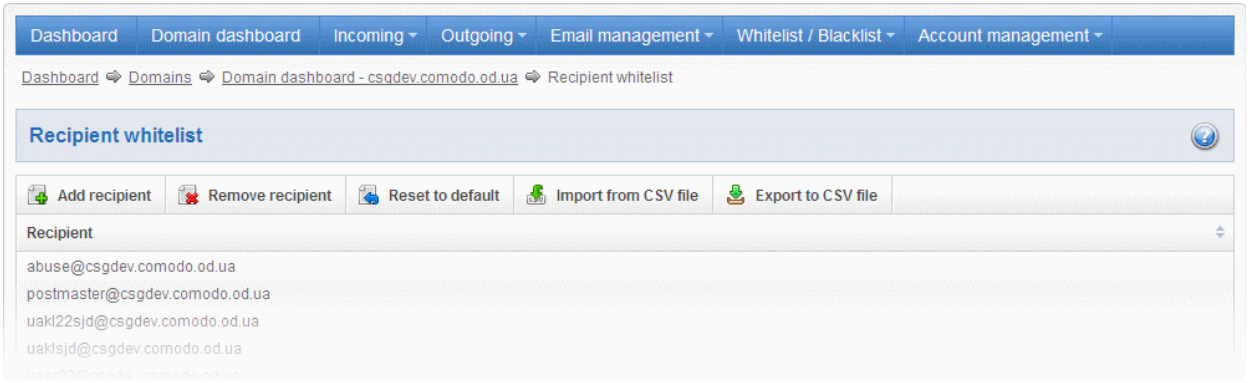
Since all filtering checks for the whitelisted recipients are disabled, CASG recommends to use the option only for certain cases such as postmaster or abuse@domain.com. The Administrator can:

- 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

To configure recipient whitelist

- Click 'Recipient whitelist' from the 'Whitelist / Blacklist' drop-down menu in the menu bar or the icon in the 'Whitelist / Blacklist' configuration area

The 'Recipient whitelist' interface of the selected domain will open:



By default, the selected domain will have 'abuse' and 'postmaster' as whitelisted recipients.

Adding Users to Recipient List

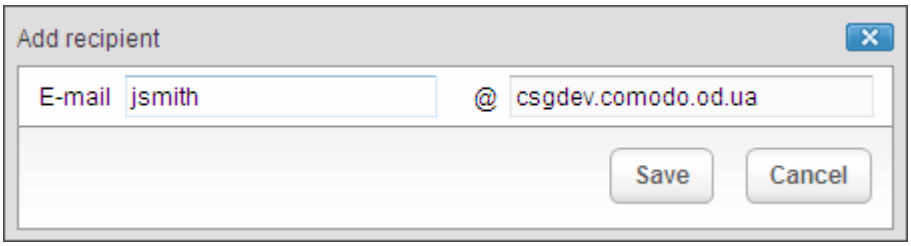
You can add recipients to white list in the following ways:

- Manually adding the recipients
- Importing from a CSV file

To manually add recipients

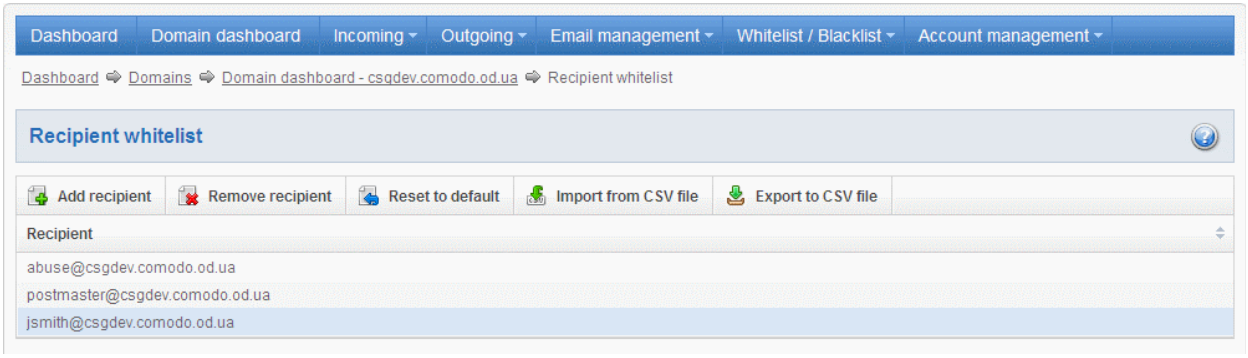
- Click 'Add recipient' to add a new user to the list

The 'Add recipient' dialog box will open.



- Enter the recipient's name in the E-mail text field and click the 'Save' button.
- To add a particular set of recipients to 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.

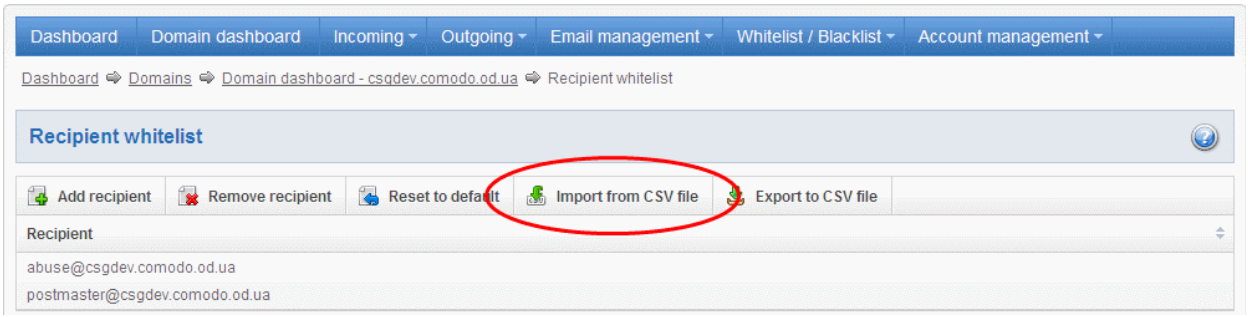
The recipient's name will be added to the list.



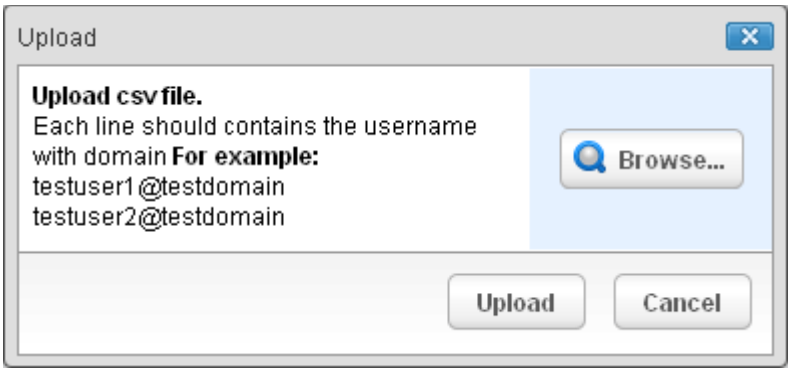
To import users to whitelist from CSV file

Administrators can import many users from a file to Recipient whitelist at a time. The users should be saved in the format shown below as an example:
user1@testdomain.com
user2@testdomain.com
user3@testdomain.com

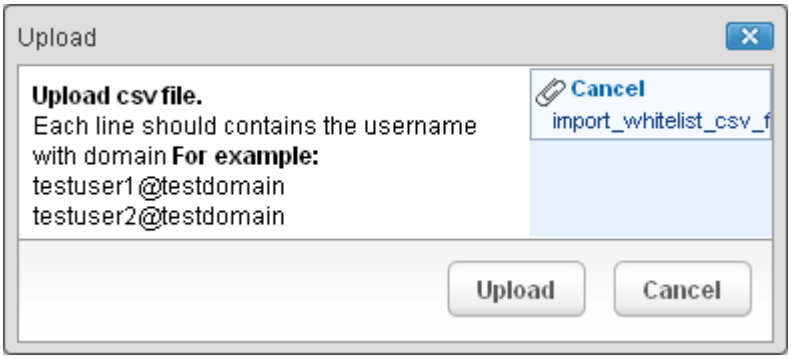
- Click the 'Import from CSV file' to import users to whitelist from a CSV file



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

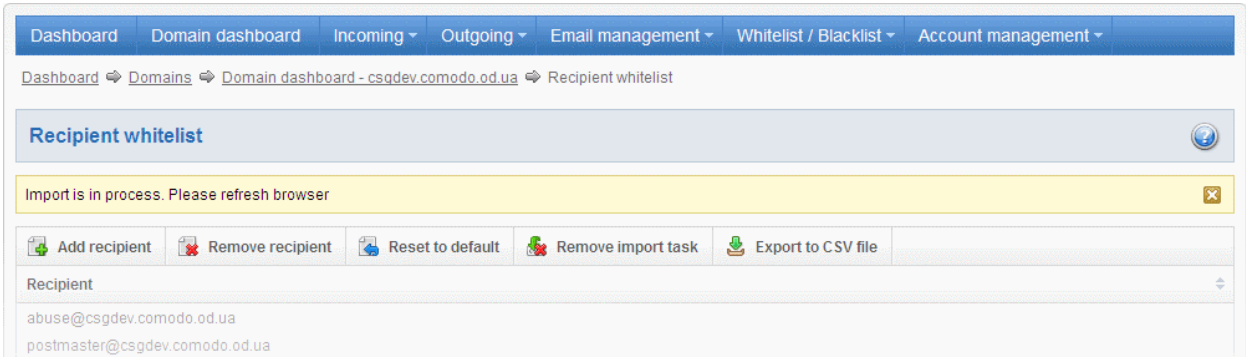


- The upload process is now ready. The maximum size of the file that can be uploaded is 9 MB. If you want to select another file, click 'Cancel' at top right side of the upload dialog. If you want to cancel the upload process, click the 'Cancel' button located at the bottom.

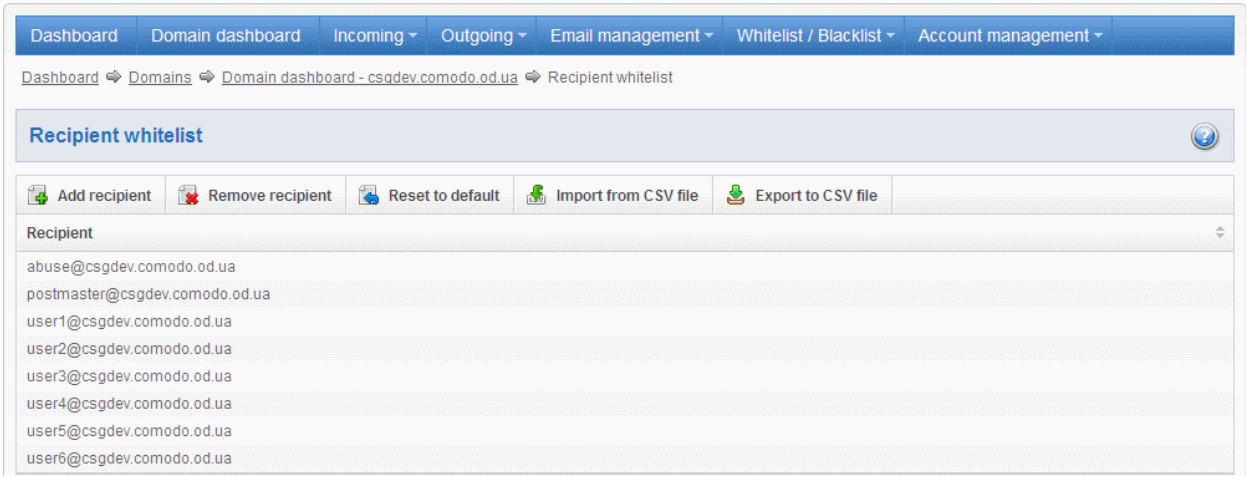


- Click the 'Upload' button to add new users.

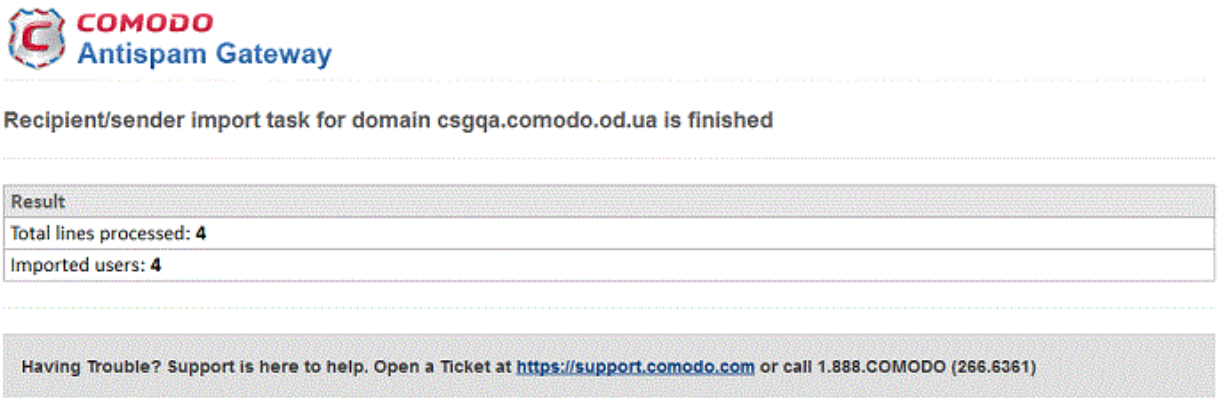
The upload will be placed in import tasks queue and the progress of the upload will be displayed. If you want to remove the upload from the queue, click the 'Remove import task' button. The 'Remove import task' deletes *only* a remaining part of not imported task.



On completion of the upload process, refresh the browser to view the imported users.



- The administrator will receive a notification about the import task completion to his email.

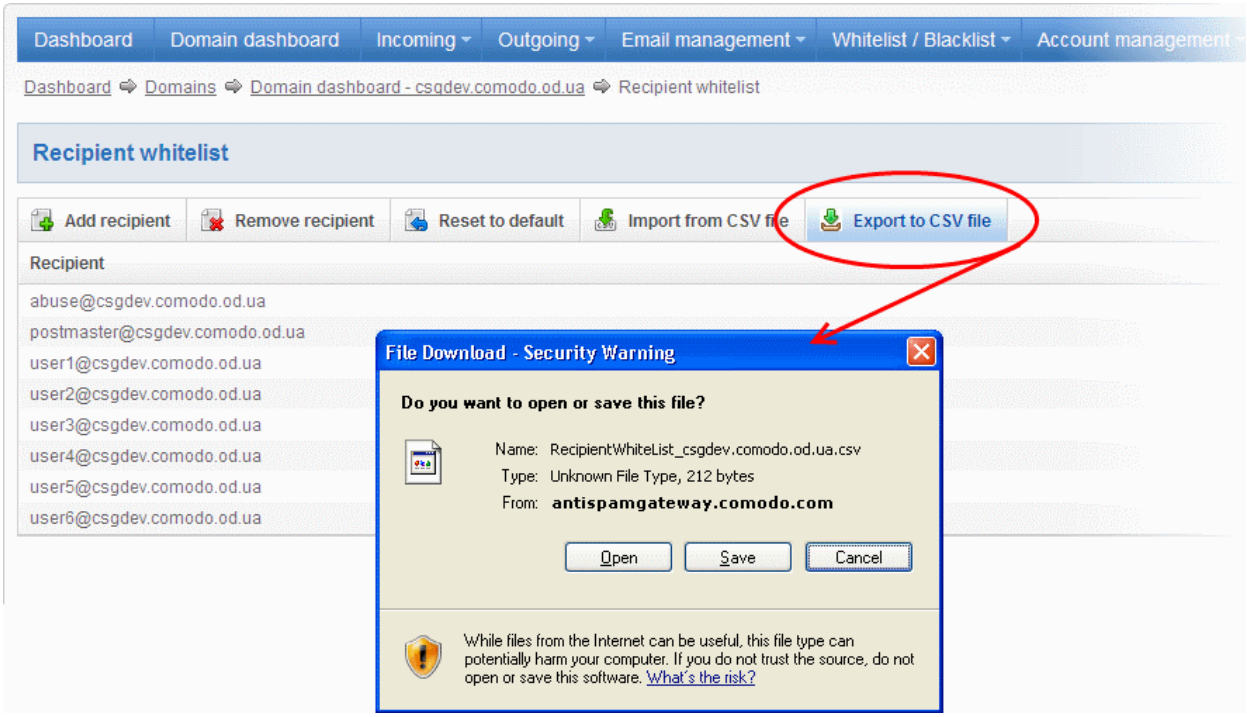


Exporting the Recipient Whitelist to CSV file

The administrator can save the configured recipient whitelist 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.

To export the list

- Click the 'Export to CSV file' to save the list of whitelisted recipients as a CSV file

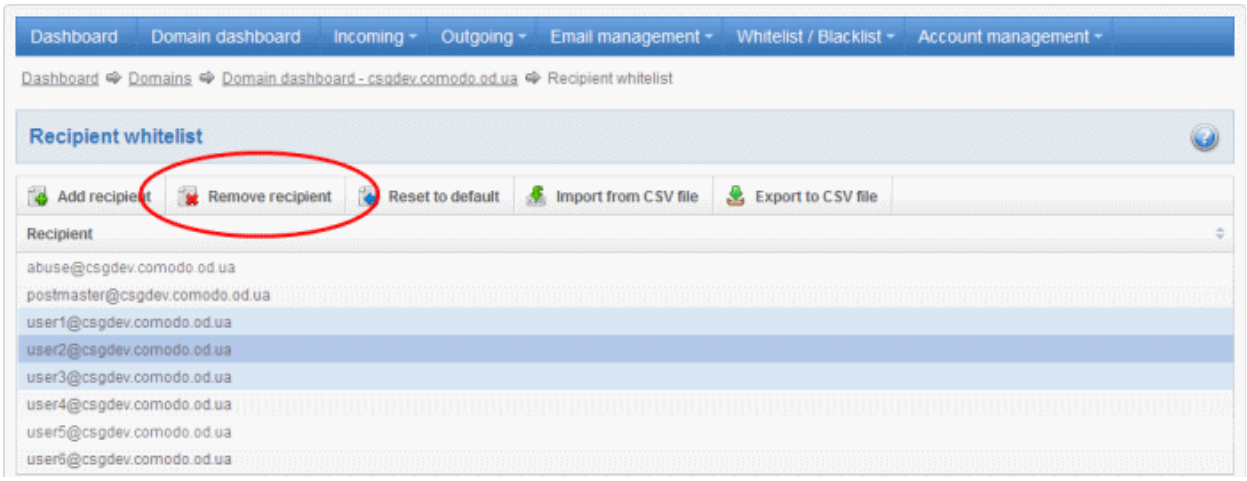


A file download dialog will be displayed.

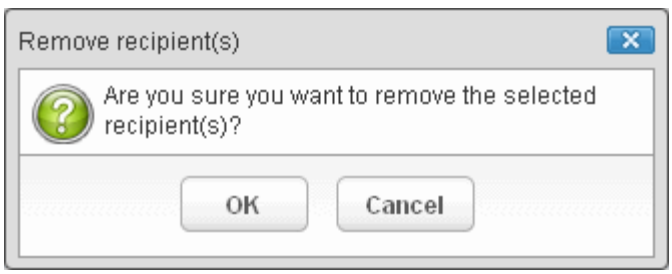
- Click 'Save' and navigate to the location in your computer and save the file.

Deleting Users from the Recipient Whitelist

- To delete a recipient from the whitelist, select the recipient from the list and click the 'Remove recipient' button



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



- Click 'OK' to confirm your changes

Sender Whitelist

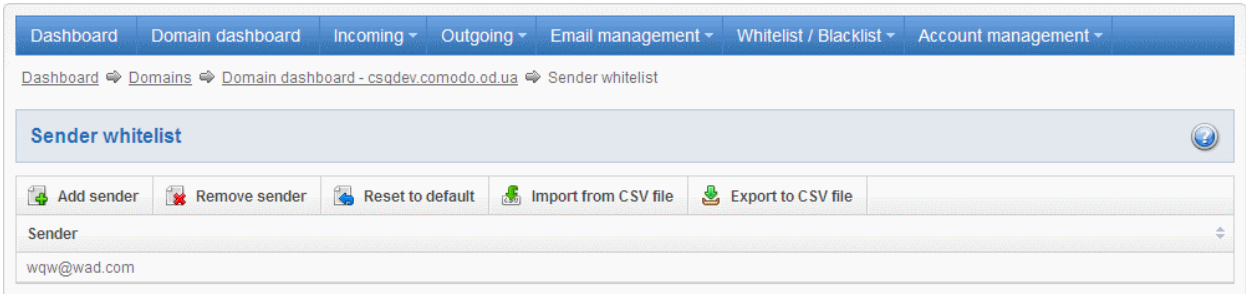
All the filtering checks for whitelisted senders to the recipients of the selected domain are disabled. Comodo strongly recommends to use this option only when the system wrongly blocks emails from a certain trusted sender. The Administrator can:

- 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

To configure sender whitelist

- Click 'Sender whitelist' from the 'Whitelist / Blacklist' drop-down menu in the menu bar or the icon in the 'Whitelist / Blacklist' configuration area

The 'Sender whitelist' interface of the selected domain will open:



Adding Users to Sender Whitelist

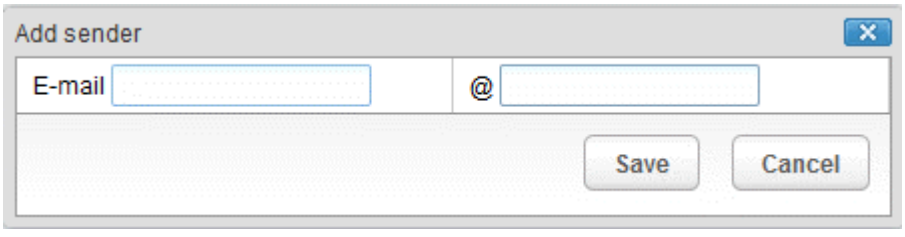
You can add recipients to white list in the following ways:

- Manually adding the senders
- Importing from a CSV file

To manually add recipients

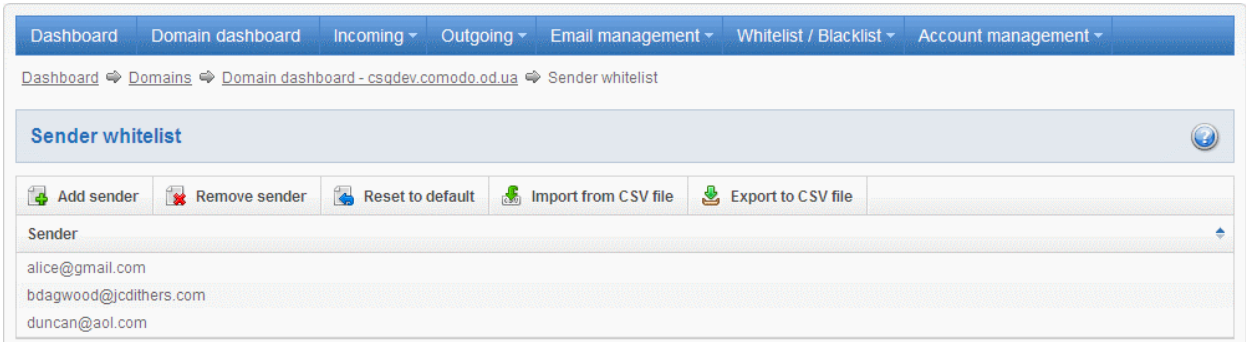
- Click 'Add sender' to add a new whitelisted sender

The 'Add sender' dialog box will open.



- 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 * in the E-mail text field and senders' email domain name after the @ symbol. For example, enter *.stores.com for all the senders in stores department to be whitelisted.
- To add a whole domain to whitelist, enter the wildcard * in the E-mail text field and email domain after the @ symbol and click the 'Save' button. Now all the senders with the domain name entered will be whitelisted.

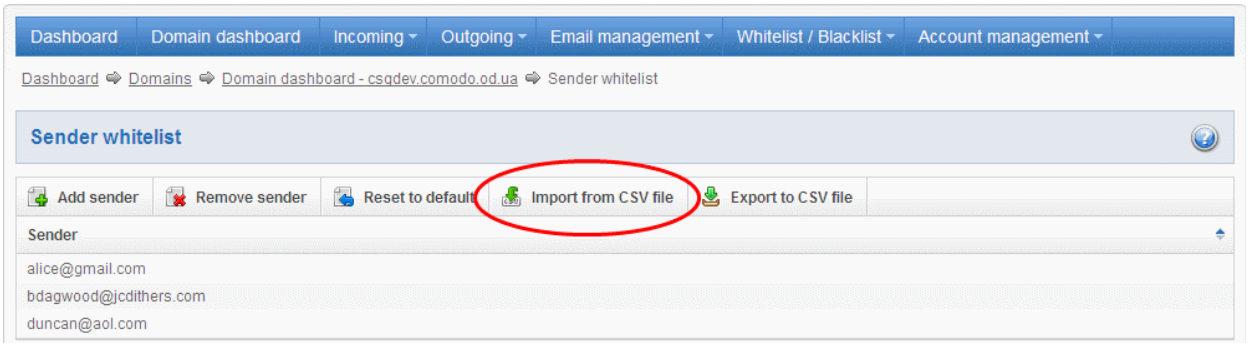
The list of whitelisted senders will be displayed.



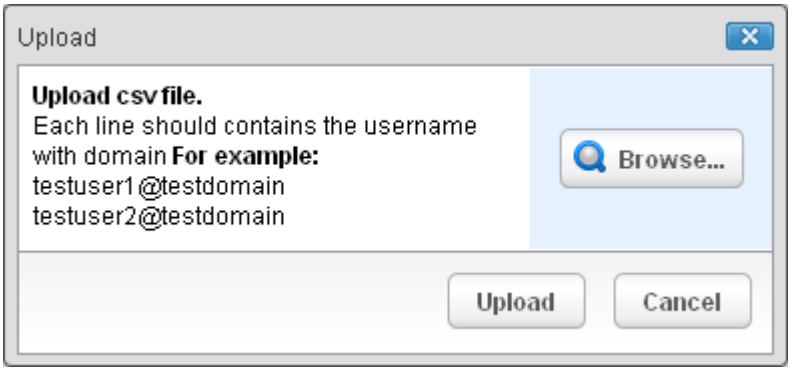
To import senders to whitelist from CSV file

Administrators can import many senders from a file to Sender whitelist 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

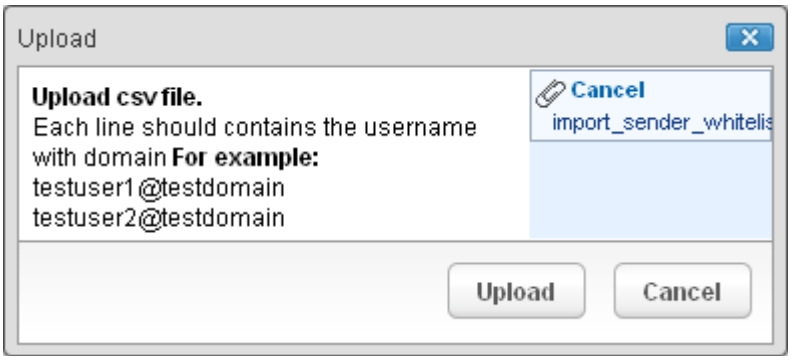
- Click the 'Import from CSV file' to import senders to whitelist from a CSV file.



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

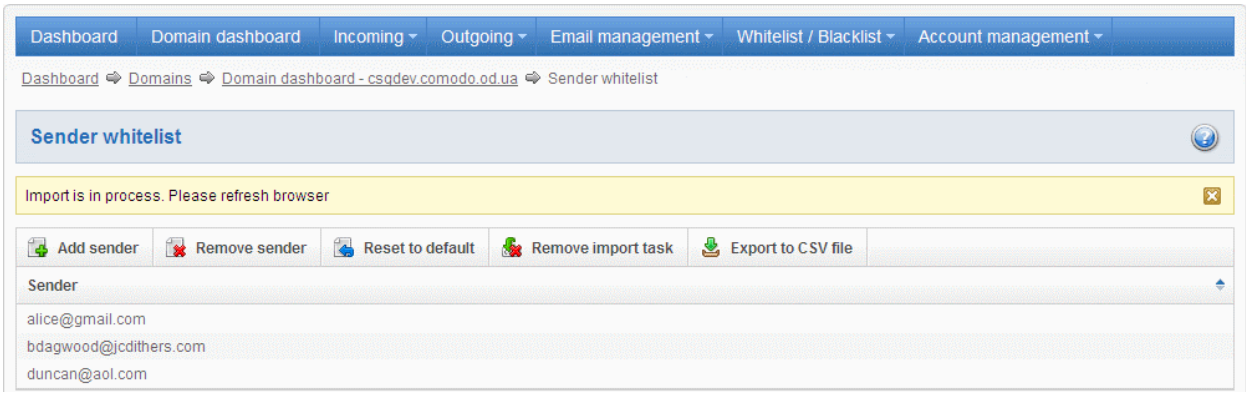


- The upload process is now ready. The maximum size of the file that can be uploaded is 9 MB. If you want to select another file, click 'Cancel' at top right side of the upload dialog. If you want to cancel the upload process, click the 'Cancel' button located at the bottom.

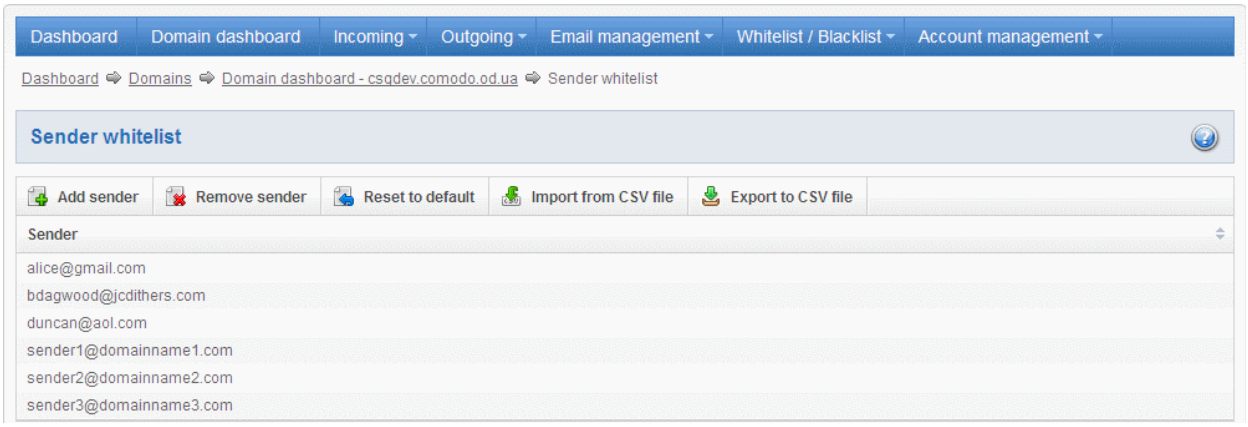


- Click the 'Upload' button to add senders.

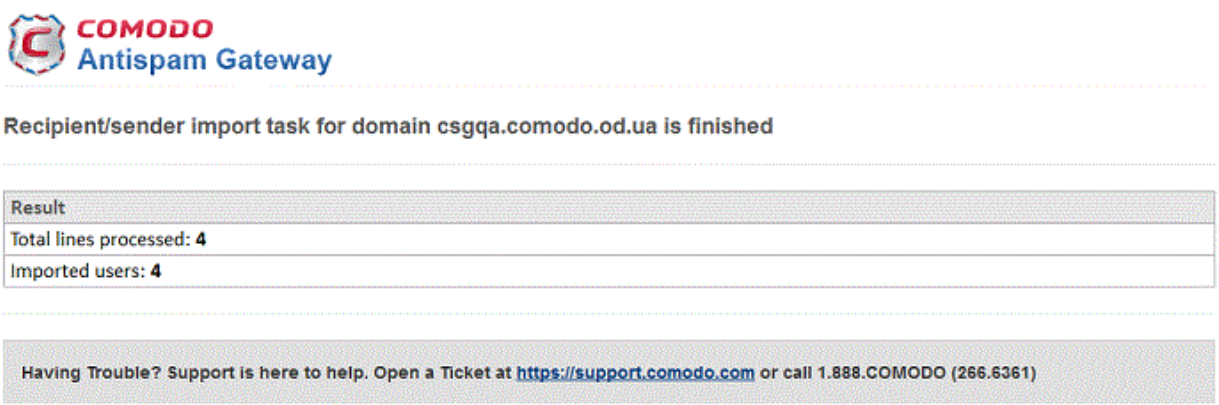
The upload will be placed in import tasks queue and the progress of the upload will be displayed. If you want to remove the upload from the queue, click the 'Remove import task' button. The 'Remove import task' deletes *only* a remaining part of not imported task.



On completion of the upload process, refresh the browser to view the imported users.



- The administrator will receive a notification about the import task completion to his email.

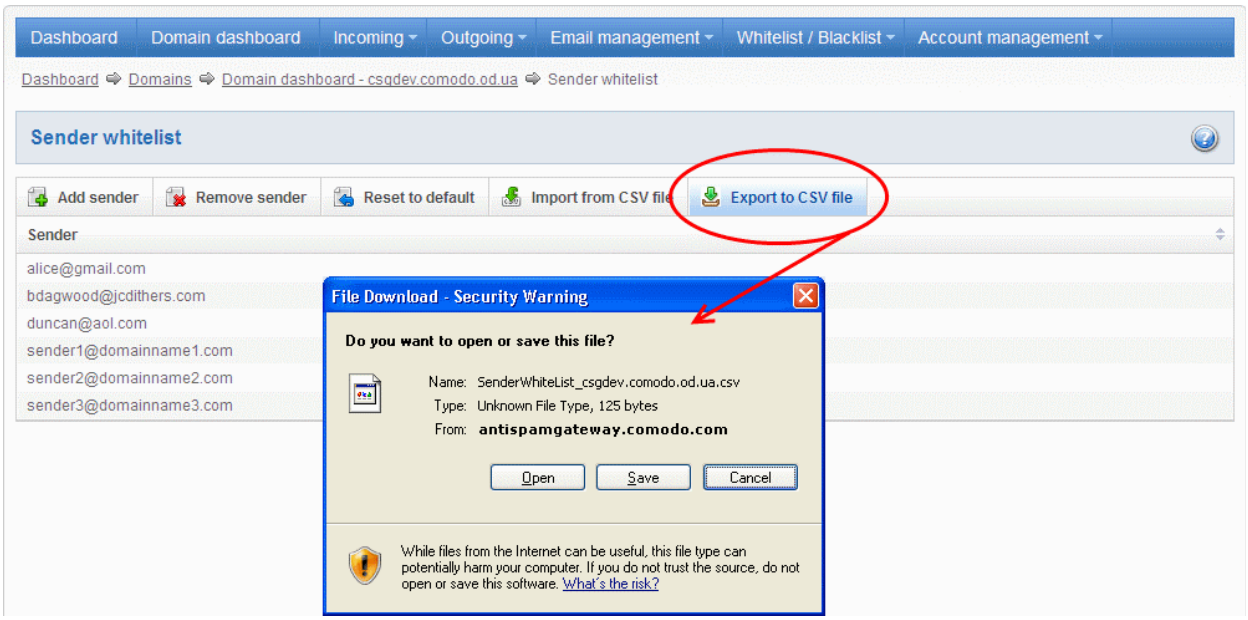


Exporting the Sender Whitelist to CSV file

The administrator can save the configured sender whitelist 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.

To export the list

- Click the 'Export to CSV file' to save the list of whitelisted senders as a CSV file

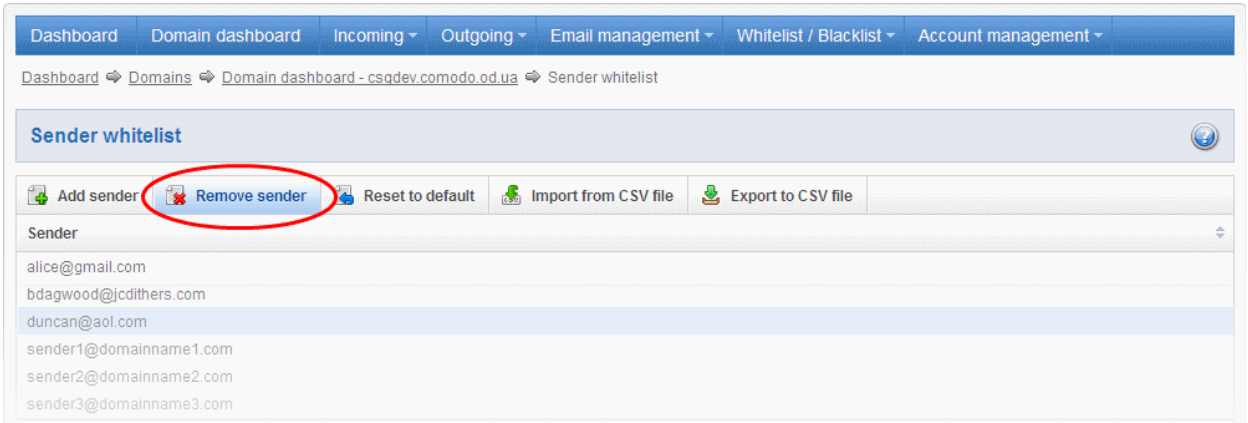


A file download dialog will be displayed.

- Click 'Save' and navigate to the location in your computer and save the file.

Deleting Users from the Sender Whitelist

- To delete a sender from the whitelist, select the sender from the list and click the 'Remove sender' button.



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

- Click 'OK' to confirm your changes.

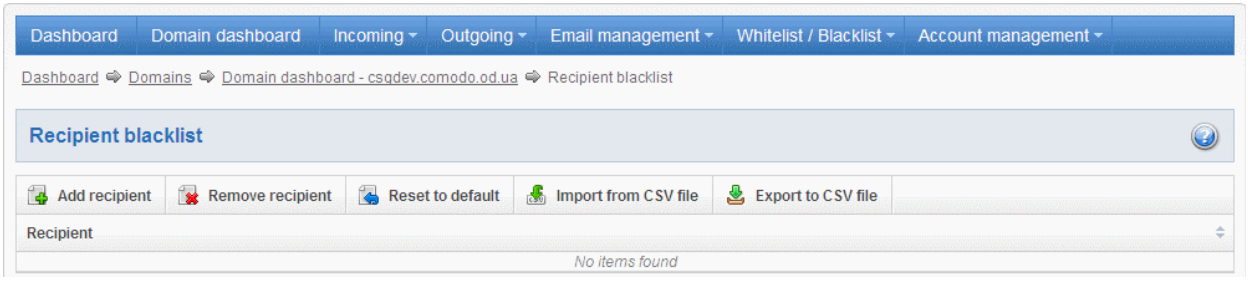
Recipient Blacklist

CASG will automatically block all emails to blacklisted recipients. Please note that the messages will not be quarantined and legitimate email sending SMTP servers will send a bounce message to the sender. The Administrator can:

- Add users to recipient blacklist
- Export the list to CSV file for use in future
- Remove users from recipient blacklist
- **Reset the list -** Delete all blacklisted senders and make the list empty by clicking the 'Reset to default' button

To configure recipient blacklist

- Click 'Recipient blacklist' from the 'Whitelist / Blacklist' drop-down menu in the menu bar or the icon in the 'Whitelist / Blacklist' configuration area



The 'Recipient blacklist' interface of the selected domain will open.

Adding Users to Recipient Blacklist

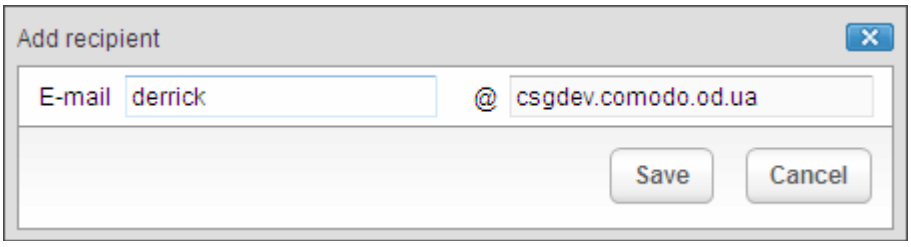
You can add recipients to the black list in the following ways:

- Manually adding the recipients
- Importing from a CSV file

To manually add recipients

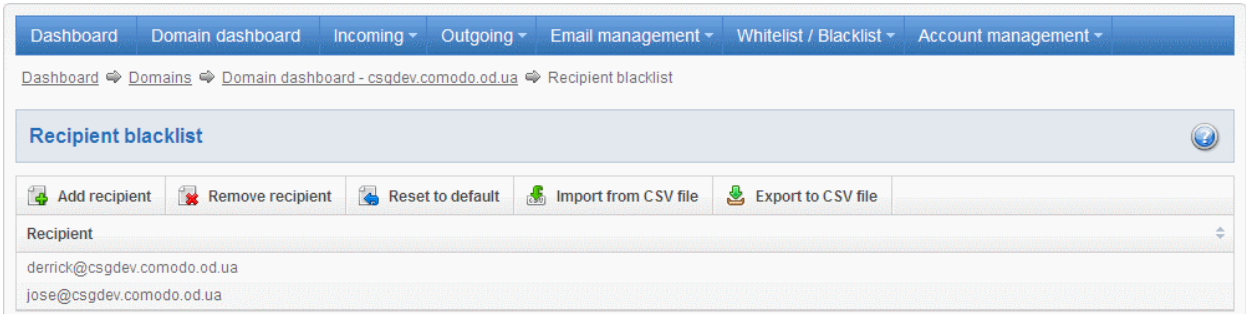
- Click 'Add recipient' to add a new user to the list

The 'Add recipient' dialog box will open.



- 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 will be blacklisted.

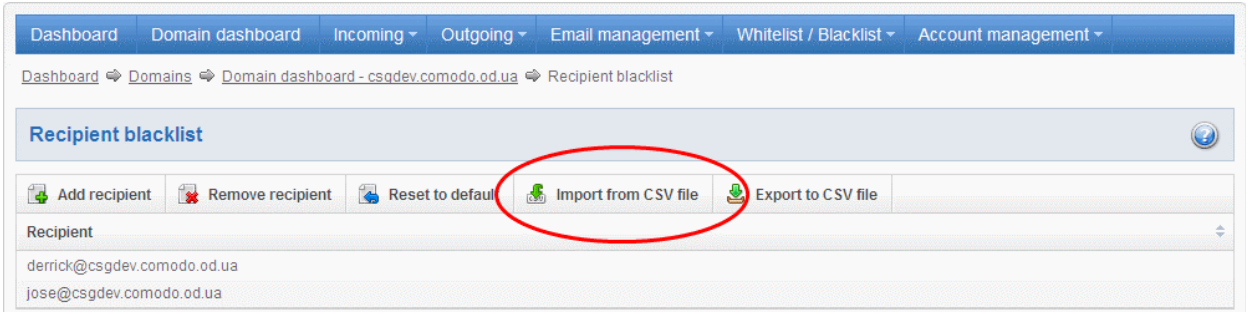
The list of blacklisted recipients will be displayed.



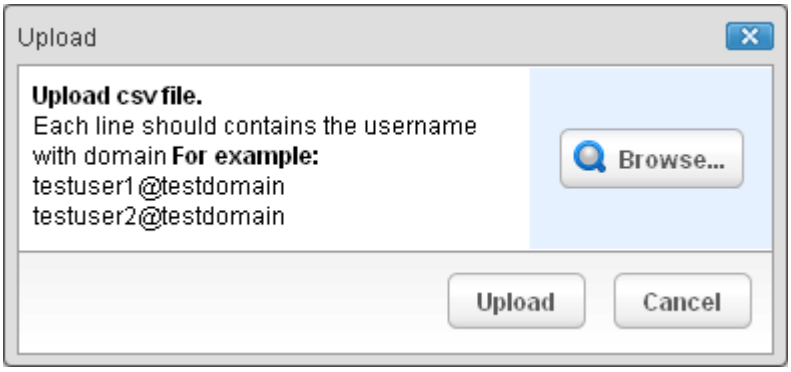
To import users to blacklist from CSV file

Administrators can import many users from a file to Recipient blacklist at a time. The users should be saved in the format shown below as an example:
user1@testdomain.com
user2@testdomain.com
user3@testdomain.com

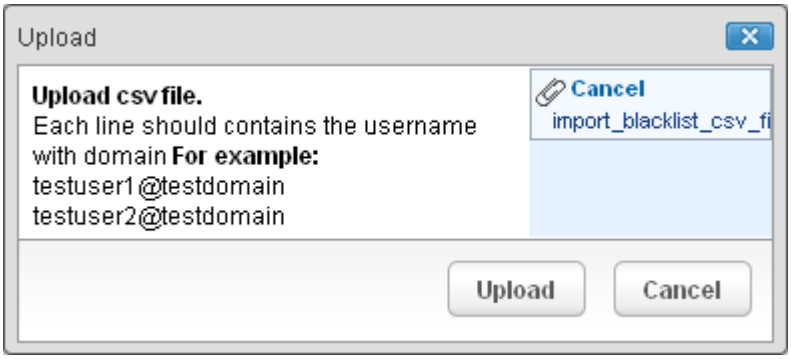
- Click the 'Import from CSV file' button to import users to blacklist from a CSV file.



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

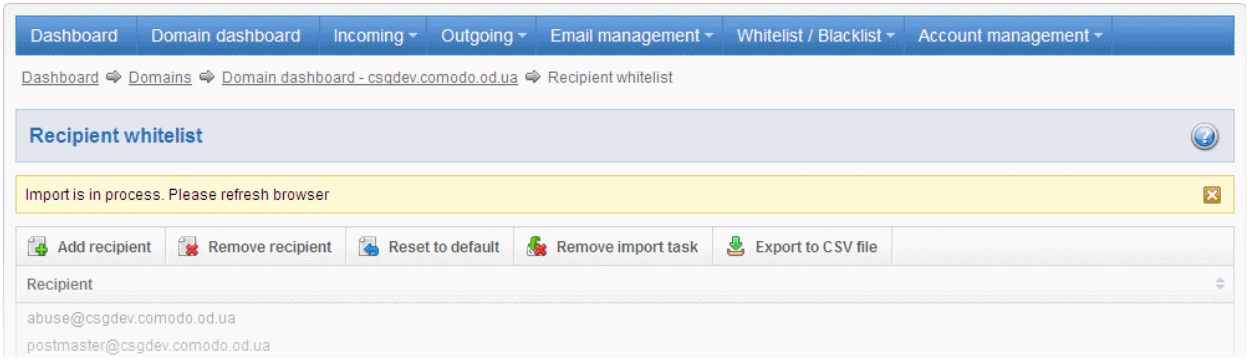


- The upload process is now ready. The maximum size of the file that can be uploaded is 9 MB. If you want to select another file, click 'Cancel' at top right side of the upload dialog. If you want to cancel the upload process, click the 'Cancel' button located at the bottom.

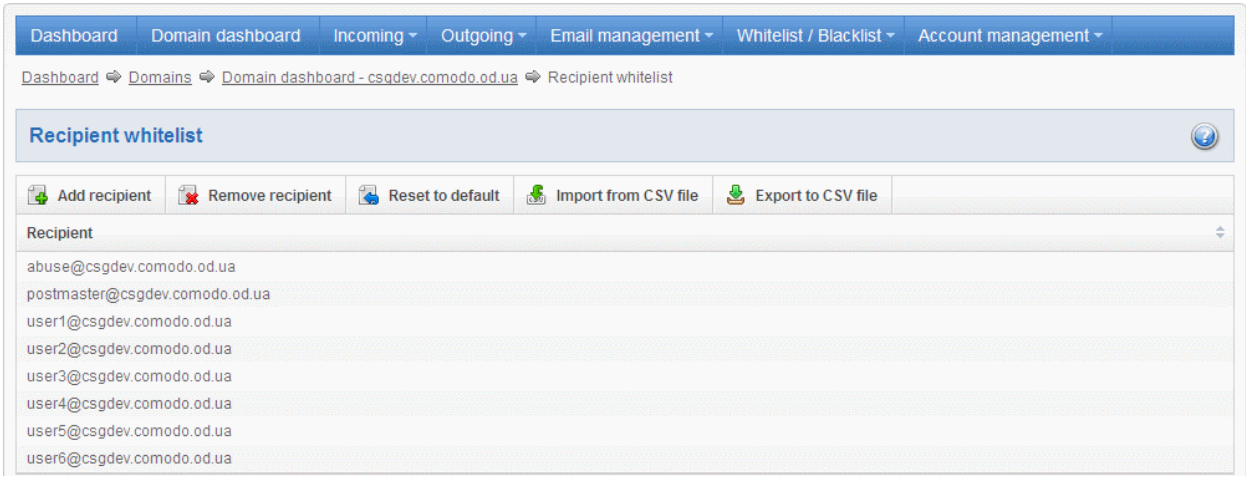


- Click the 'Upload' button to add new users.

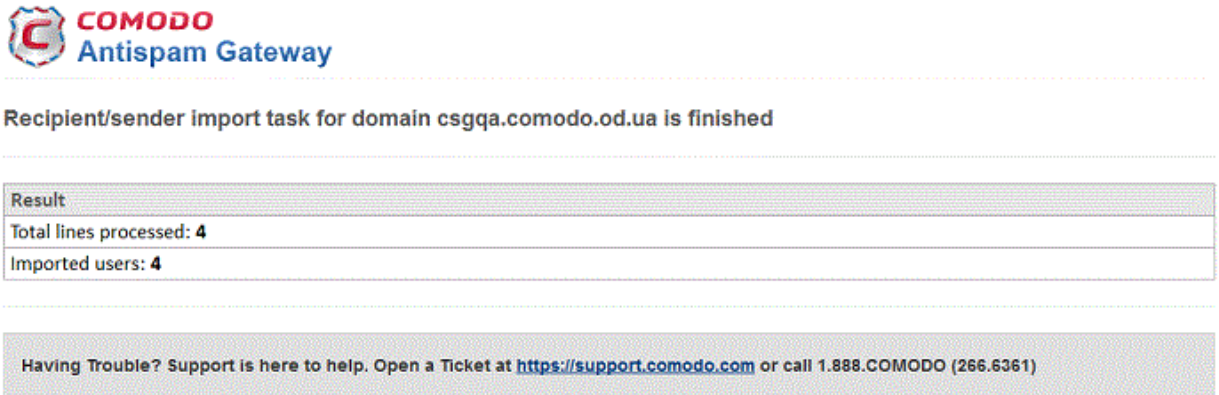
The upload will be placed in import tasks queue and the progress of the upload will be displayed. If you want to remove the upload from the queue, click the 'Remove import task' button. The 'Remove import task' deletes *only* a remaining part of not imported task.



On completion of the upload process, refresh the browser to view the imported users.



- The administrator will receive a notification about the import task completion to his email.

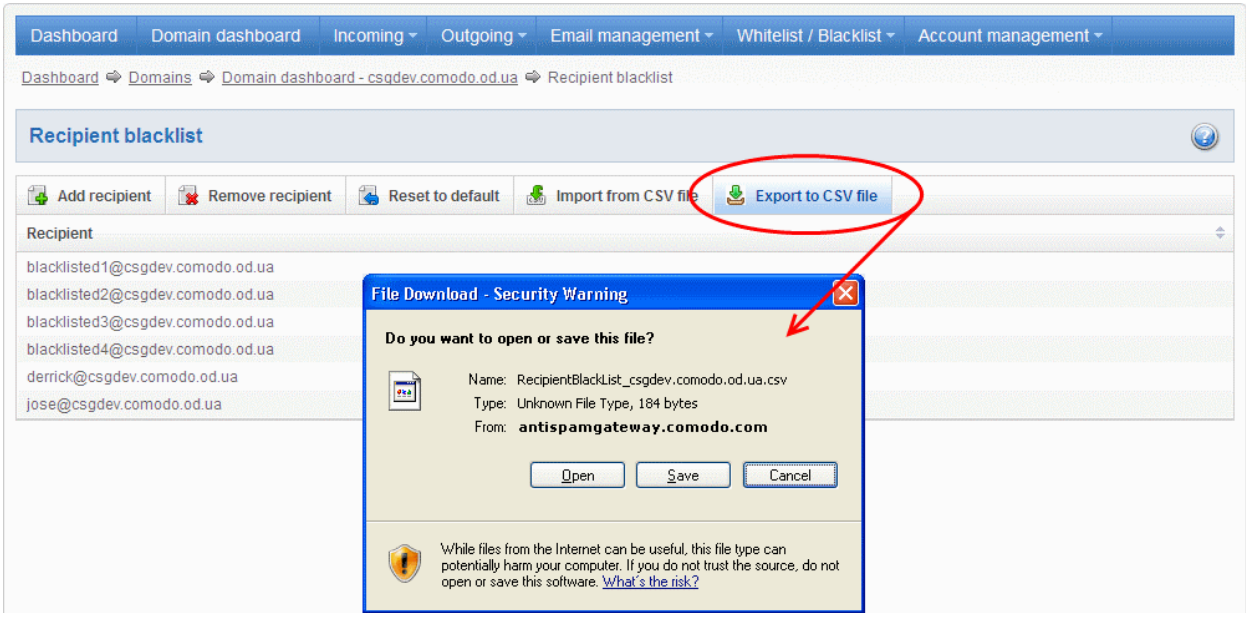


Exporting the Recipient Blacklist to CSV file

The administrator can save the configured 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.

To export the list

- Click the 'Export to CSV file' to save the list of blacklisted recipients as a CSV file

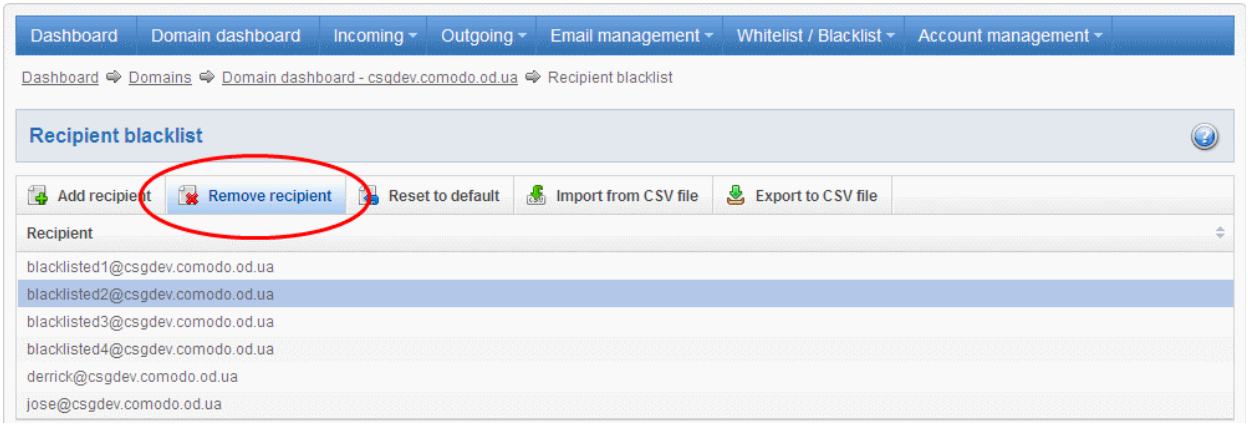


A file download dialog will be displayed.

- Click 'Save' and navigate to the location in your computer and save the file.

Deleting Users from the Recipient Blacklist

- To delete a recipient from the blacklist, select the recipient from the list and click the 'Remove recipient' button



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

- Click 'OK' to confirm your changes. The user will be removed from the blacklist and the mails addressed to the user will be allowed as per the existing filter settings in CASG.

Sender Blacklist

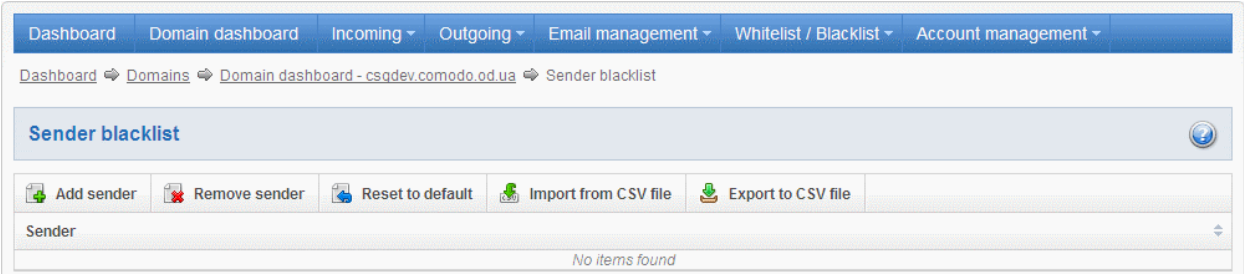
CASG will automatically block all emails from blacklisted senders. Please note that the messages will not be quarantined and legitimate email sending SMTP servers will send a bounce message to the sender. The administrator can:

- Add users to sender blacklist
- Export the list to CSV file for use in future
- Remove users from sender blacklist
- **Reset the list -** Delete all blacklisted senders and make the list empty by clicking the 'Reset to default' button

To configure sender blacklist

- Click 'Sender blacklist' from the 'Whitelist / Blacklist' drop-down menu in the menu bar or the icon in the 'Whitelist / Blacklist' configuration area

The 'Sender blacklist' interface of the selected domain will open.



Adding Users to Senders Blacklist

You can add senders to black list in the following ways:

- Manually adding the senders
- Importing from a CSV file

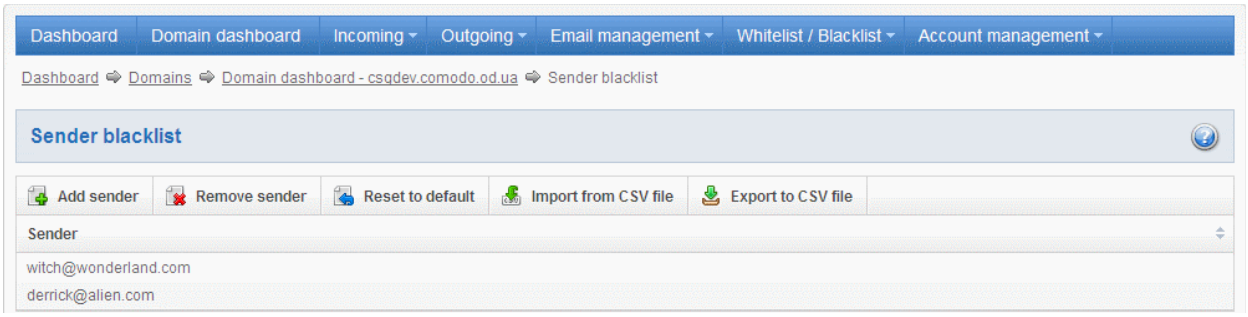
To manually add recipients

- Click 'Add sender' to add a new blacklisted sender

The 'Add sender' dialog box will open.

- 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 * in the E-mail text field and senders' email domain name after the @ symbol. For example, enter *.stores for all the senders in stores department to be blacklisted.
- To add a whole domain to blacklist, enter the wildcard * in the E-mail text field and email domain after the @ symbol and click the 'Save' button. Now all the senders with the domain name entered will be blacklisted.

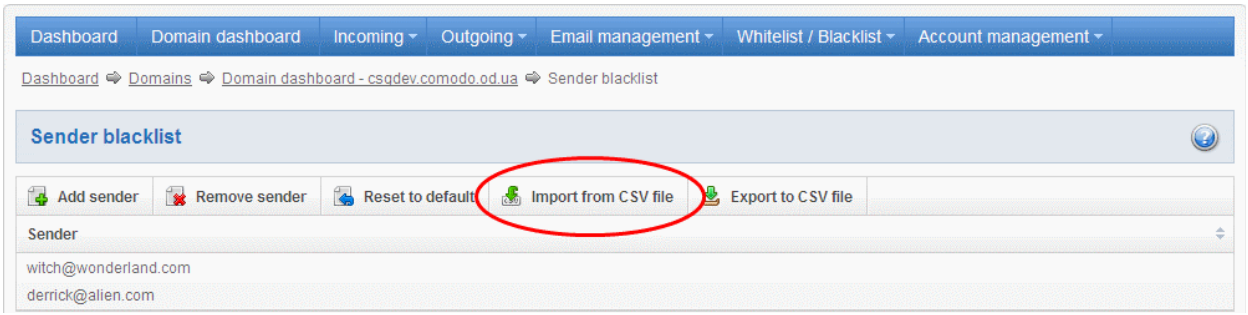
The list of blacklisted senders will be displayed.



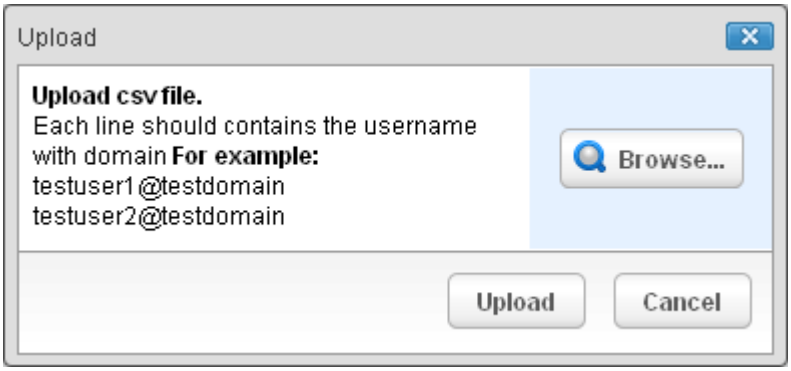
To import senders to blacklist from CSV file

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

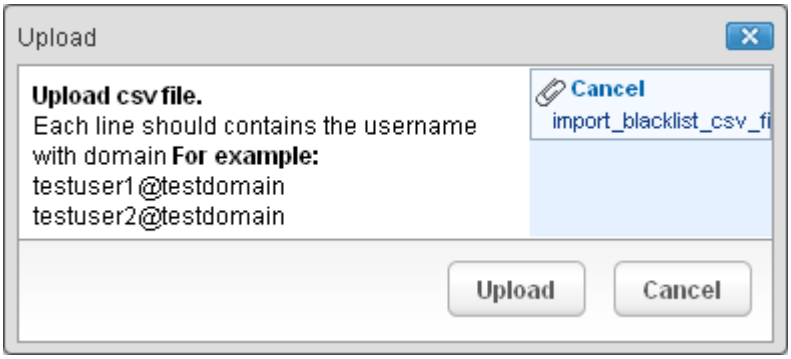
- Click the 'Import from CSV file' to import senders to blacklist from a CSV file.



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

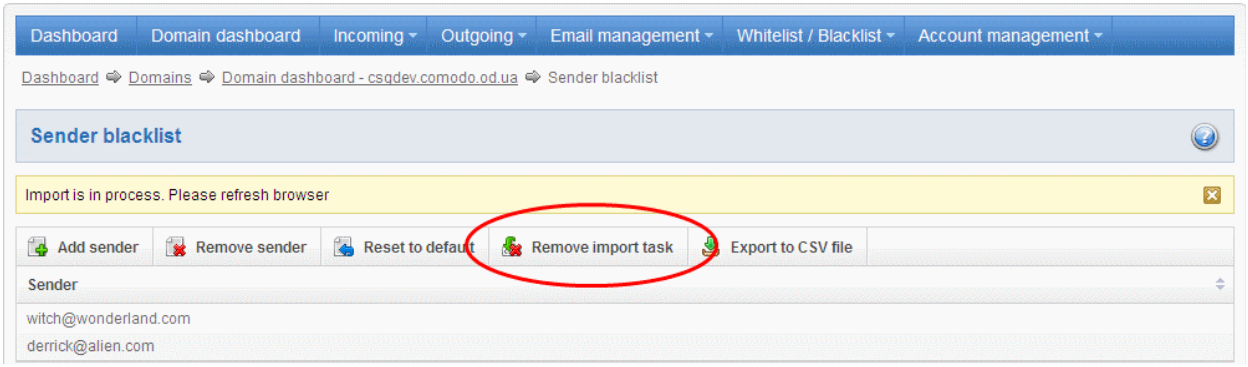


- The upload process is now ready. The maximum size of the file that can be uploaded is 9 MB. If you want to select another file, click 'Cancel' at top right side of the upload dialog. If you want to cancel the upload process, click the 'Cancel' button located at the bottom.

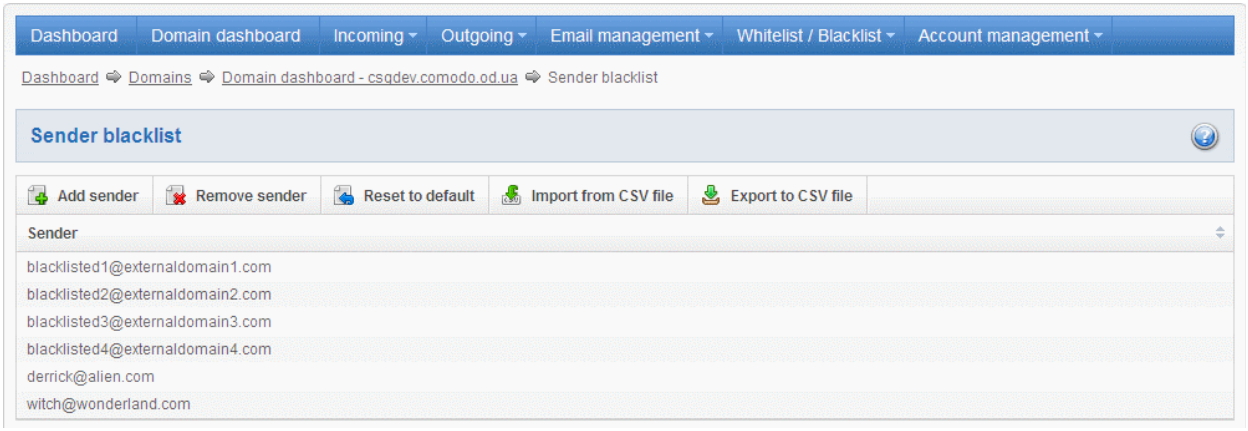


- Click the 'Upload' button to add senders.

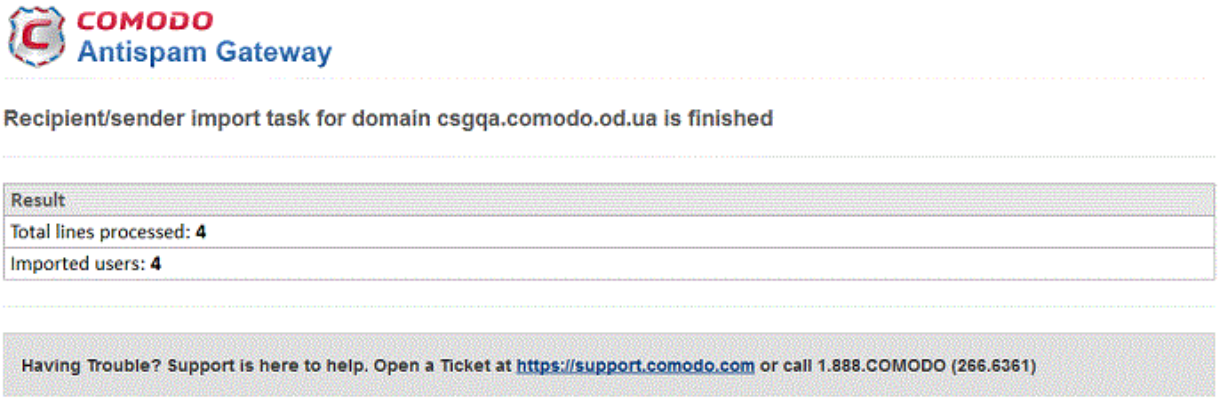
The upload will be placed in import tasks queue and the progress of the upload will be displayed. If you want to remove the upload from the queue, click the 'Remove import task' button. The 'Remove import task' deletes *only* a remaining part of not imported task.



On completion of the upload process, refresh the browser to view the imported users.



- The administrator will receive a notification about the import task completion to his email.

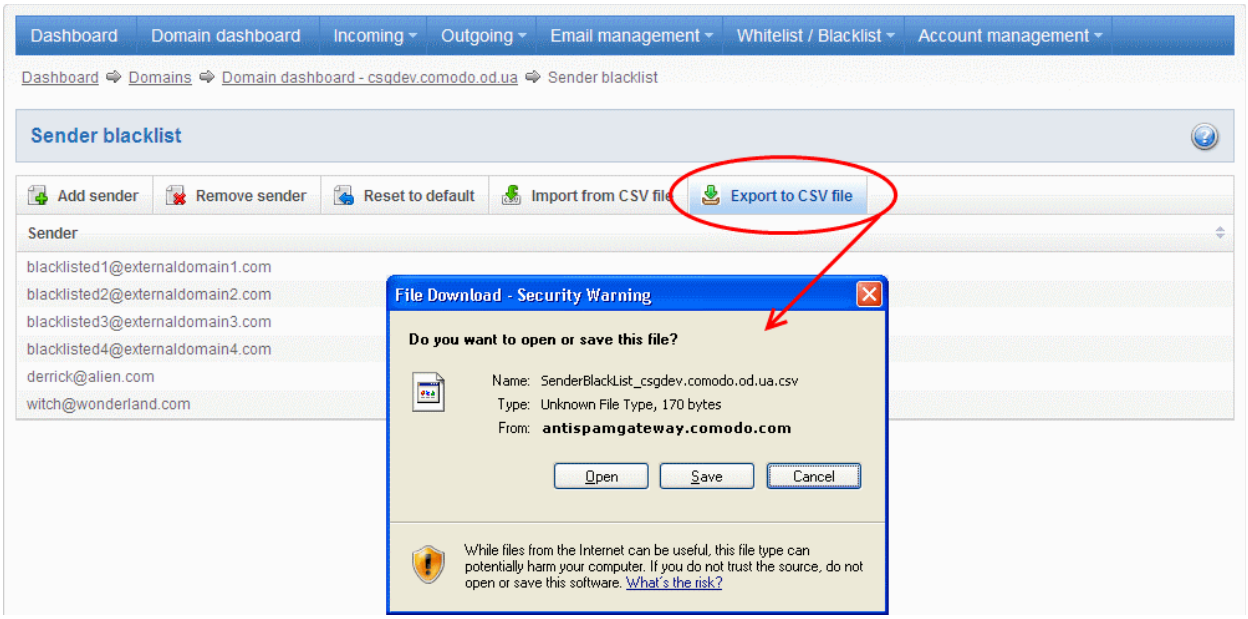


Exporting the Sender Blacklist to CSV file

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.

To export the list

- Click the 'Export to CSV file' to save the list of blacklisted senders as a CSV file

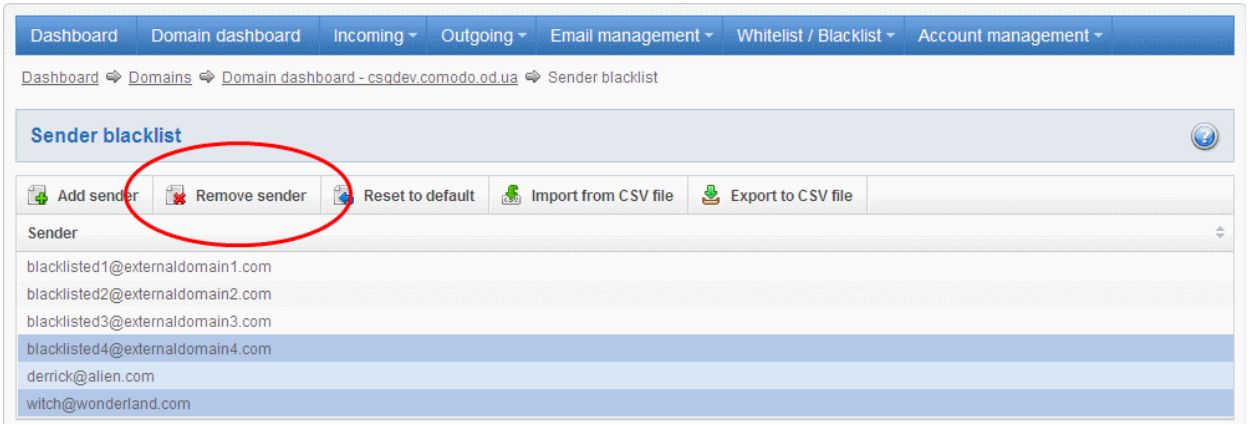


A file download dialog will be displayed.

- Click 'Save' and navigate to the location in your computer and save the file.

Deleting Users from the Sender Blacklist

- To delete a sender from the blacklist, select the sender from the list and click the 'Remove sender' button.



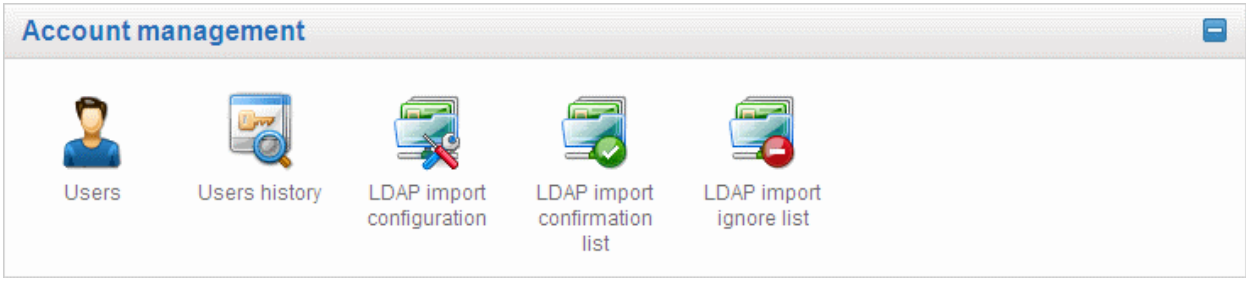
Tip: You can select multiple recipients to delete by pressing and holding the Shift or Ctrl keys.

- Click 'OK' to confirm your changes. The sender(s) will be removed from the blacklist. The emails from the senders will be allowed as per the existing filter settings in CASG.

3.2.1.4.5 Account Management

In the Account Management interface, an administrator can manage the users for the selected domain. From this interface, you

can reset passwords for users, allow or deny permission for users to access their account, can import CSV file containing the list of users, import users from your the Active Directory (AD) server of the domain through Lightweight Directory Access Protocol (LDAP), add and move your aliases. In the Users history interface, an administrator can view users login history. Refer to User History for more details.



Click the following links for more details:

- Users
- Users history
- Importing Users from LDAP

3.2.1.4.5.1 User Account Management

The 'Users' area of 'Account Management' allows administrators to manage the users for the selected domain. This includes adding/importing users, deleting user, editing user accounts, resetting passwords and configuring user permissions. Admins can also configure email aliases from this interface.

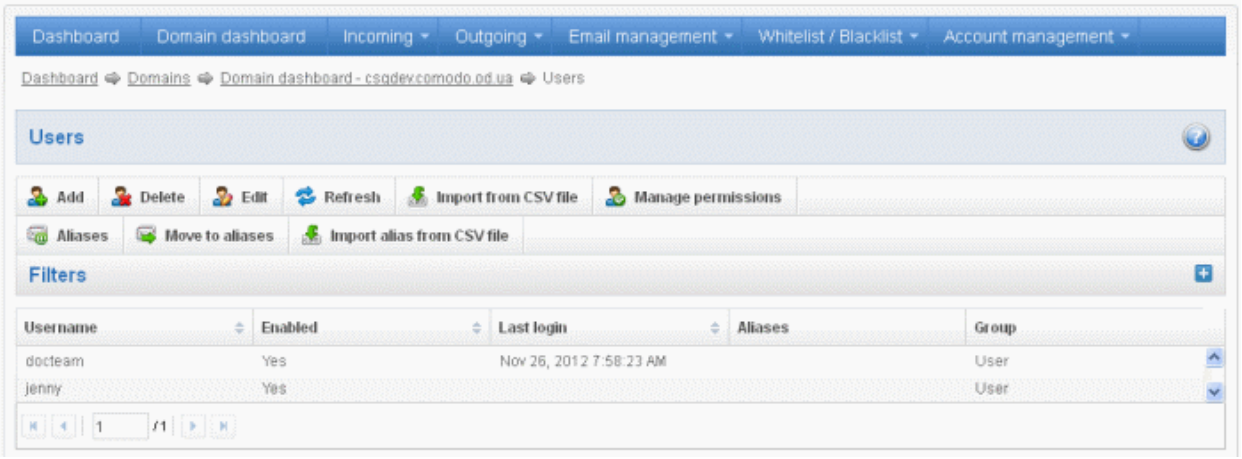
Click the following links for more details:

- Managing Users
- Adding New Users
- Deleting Users
- Editing Users
- Importing from CSV file
- Managing Permissions
- Aliases
- Moving to Aliases
- Importing Aliases from CSV file

Managing Users

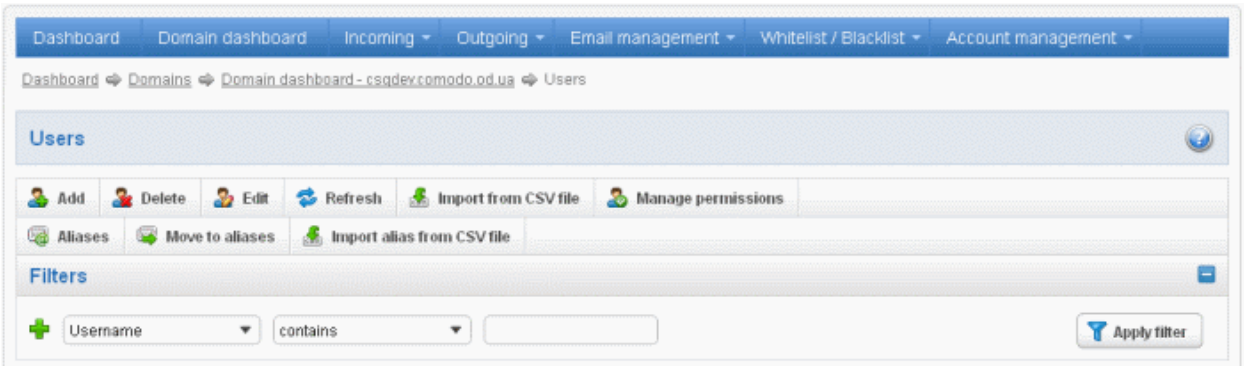
- Click 'Users' from the 'Account management' drop-down menu in the menu bar or the icon in the 'Account management' configuration area

The 'Users' interface of the selected domain will open.

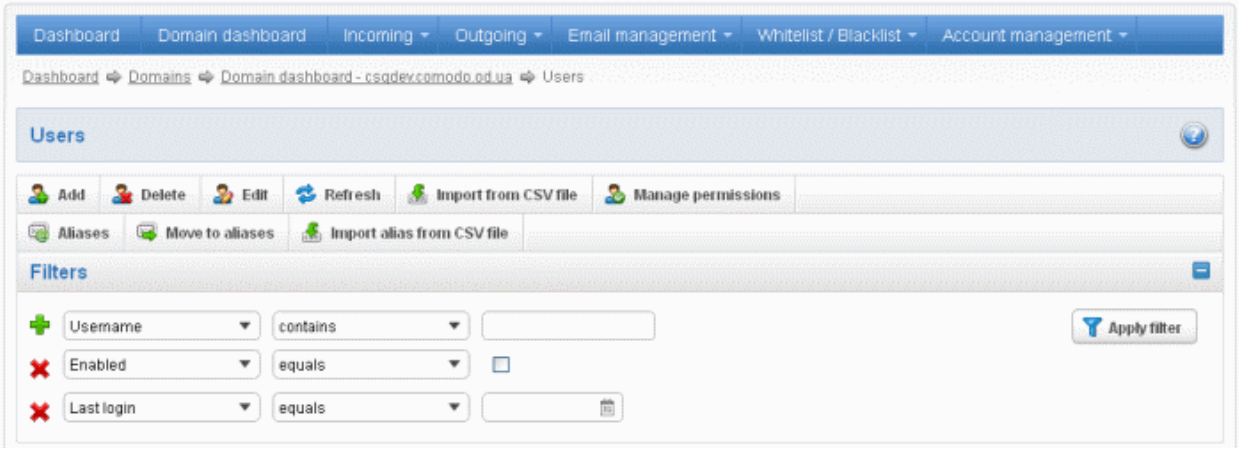


Using the filter option to search users

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



You can further refine your search by clicking ✚ to add more filters.



You can remove a filter by clicking the ✖ icon beside it.

Available filters are:

- **Username:** Will execute a search of usernames according to the text in the text box (column 3) and the condition selected in column 2.

If 'Username' is selected, the following conditions are available:

- **Equals**: Displays all usernames that match the text entered in the text box.
- **Not Equals**: Displays all users except the one entered in the text box.

- **Contains**: Displays all username(s) that contain the words entered in the text box.
- **Not Contains**: Displays all username(s) that do not contain the words entered in the text box.
- **Starts With**: Displays all username(s) that start with the words entered in the text box.
- **Ends With**: Displays all the username(s) that end with the words entered in the text box.

Other options available in the first drop-down in the filters area:

- **Enabled:** Sorts the results based on whether a user is enabled or disabled.

When you select this option in the first drop-down, 'equals' is the only option available in the second drop-down:

- **Equals:** Displays the results of enabled users when the checkbox beside it is selected. When the checkbox is not selected, it displays the list of users who are not enabled.
- **Last Login:** Sorts the results based on the last login details of users.

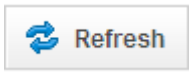
When you select this option in the first drop-down, the following filters are available:

- **Equals:** Displays the list of users whose last login date is the same as the selected date in the third box from the calendar.
- **Less than:** Displays the list of users whose last login date is less than the selected date in the third box from the calendar.
- **Greater than:** Displays the list of users whose last login date is greater than the selected date in the third box from the calendar.

Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

Click anywhere on the Filters tab to close the filters area.

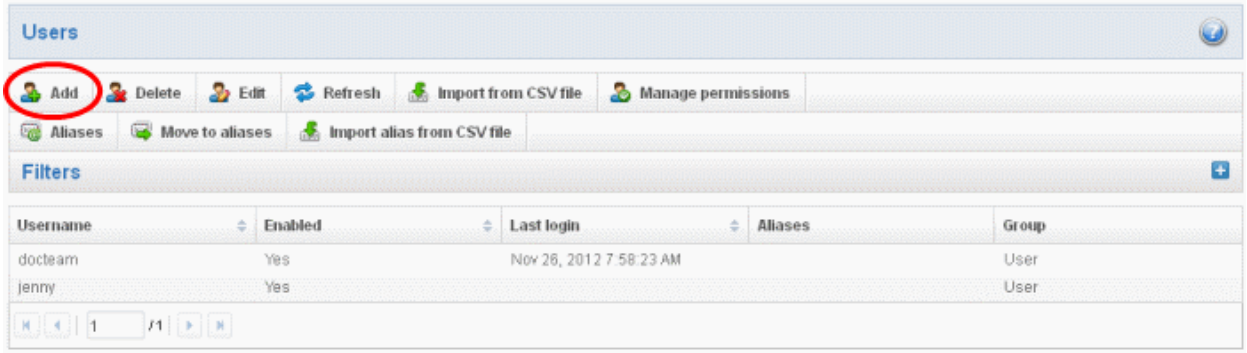
Click the 

button to display all users.

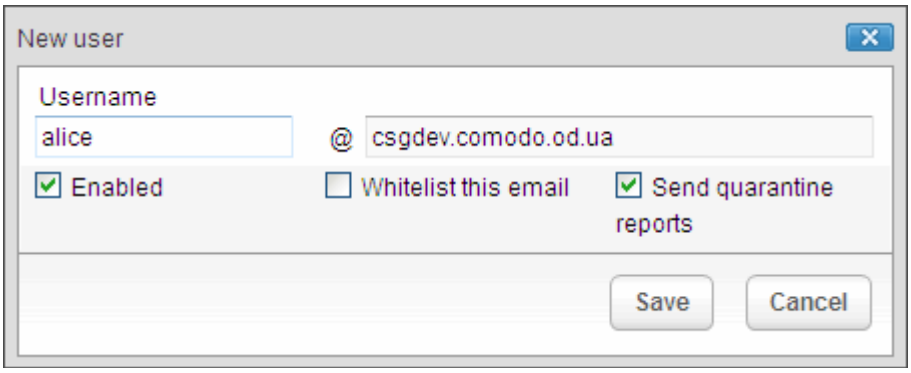
Note: To display all the users after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

To add a new user

- Click the 'Add' button.



The 'New user' dialog will open.



- Enter the username of a new user that will be first part of the email address. For example, 'alice'. The email address of the added user will be 'alice@domainname.com'.

By default, the user will be enabled. Uncheck the checkbox beside 'Enabled' to deny the new user access to CASG. You can enable the user in the **Edit user** interface later on.

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**..

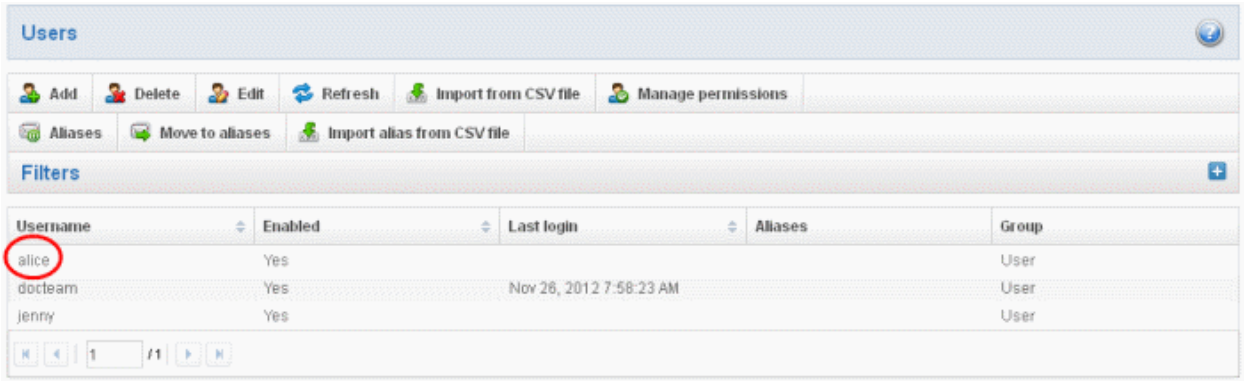
Checking 'Whitelist this email' will disable the 'Send quarantine reports' checkbox.

The administrators can also determine whether the users will get the reports or not. By default, it is enabled.

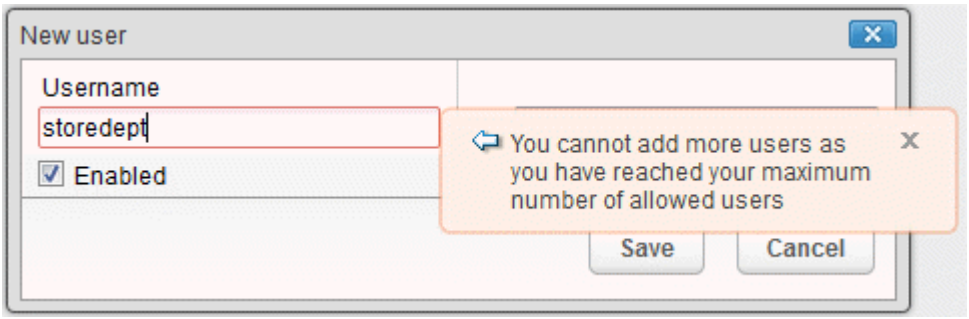
- Uncheck 'Send quarantine reports' box to disable this option.
- Click the 'Save' button.
- A green strip confirming successfully saved user will be displayed.

Note: If the user is disabled, the user will be automatically added to whitelist. All the emails from/to the user will be allowed without the filtering checks. Also, if the user has subscribed for periodical Quarantine Reports, the subscription will also be canceled. If the user is enabled, the user will be removed from the whitelist. If required, the administrator can add the user to the Recipient Whitelist by selecting the 'Whitelist this email' checkbox.

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.

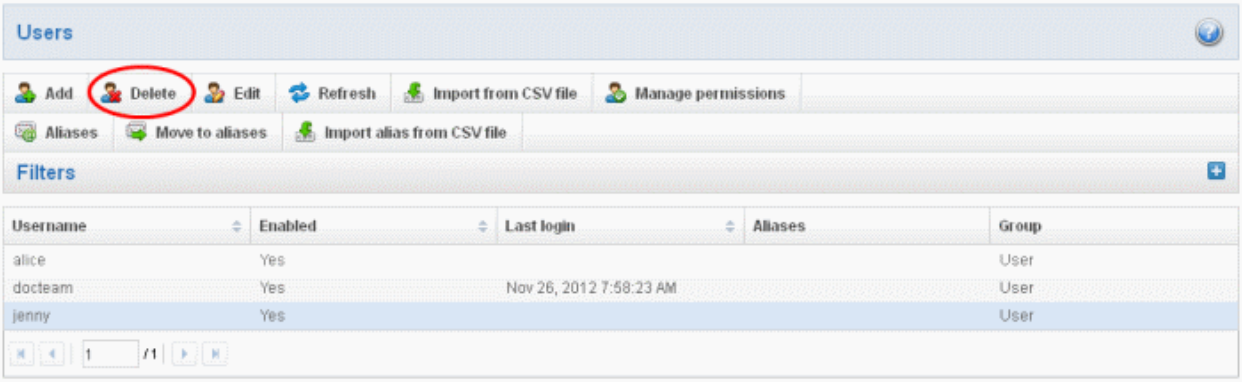


Note: The number of users for an account depends on the plan subscribed by you. When you exceed the limit of users, the following will be displayed while adding a new user.

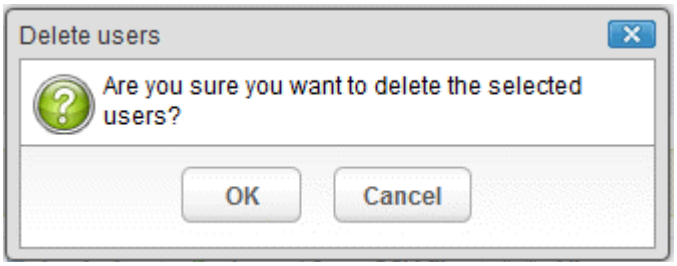


To delete an existing user

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



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



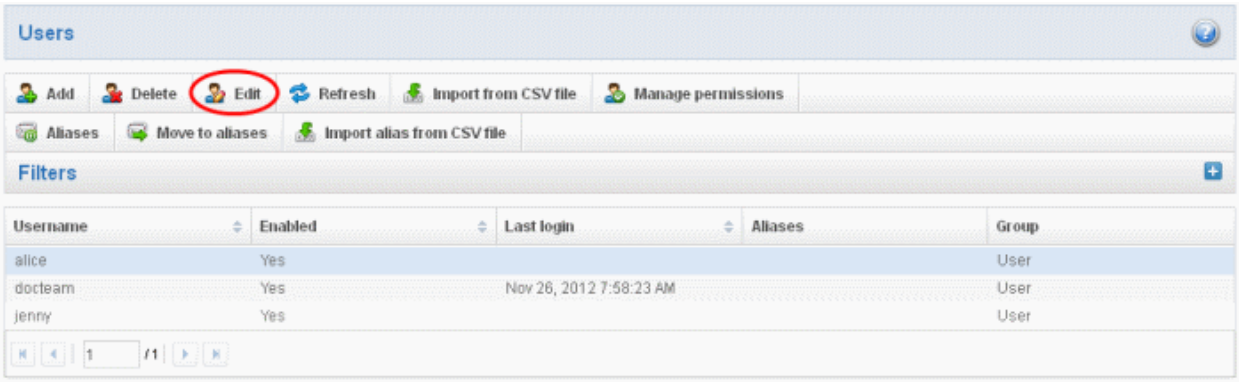
- Click 'OK' to confirm your changes.

A green strip confirming successful deletion will be appeared.

To edit an existing user

You can reset password, 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 be displayed.

- **Enabled** - Select the checkbox to allow or deny access to the CASG interface.
- **Whitelist email** - Select this checkbox to add the user to **Recipient Whitelist**.
- **Regenerate password** - Click this button to reset the password 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.
- Disable '**Send quarantine reports**' checkbox, if you do not want the user gets quarantine reports. By default it is enabled.

Checking 'Whitelist this email' will disable the 'Send quarantine reports' checkbox.

Click the 'Save' button to confirm your changes.

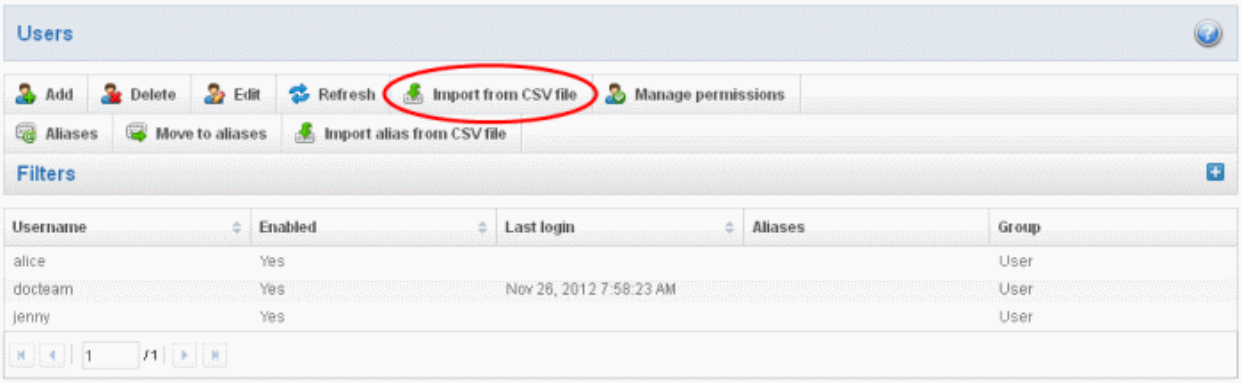
Note: If the user is disabled, the user will be automatically added to whitelist. All the emails from/to the user will be allowed without the filtering checks. Also, if the user has subscribed for periodical Quarantine Reports, the subscription will also be canceled. If the user is enabled, the user will be removed from the whitelist. If required, the administrator can add the user to the Recipient Whitelist by selecting the 'Whitelist this email' checkbox.

To import users from CSV file

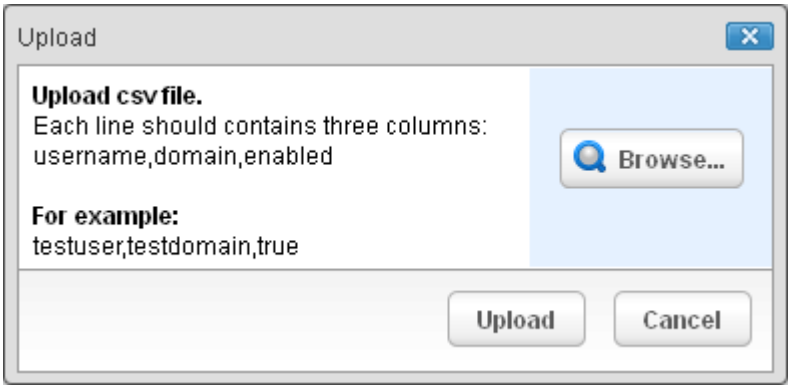
You can add many new users at a time by importing from a file. The users should be saved in 'comma separated value' (CSV) as shown below:

username1,domainname,true
username2,domainname,false

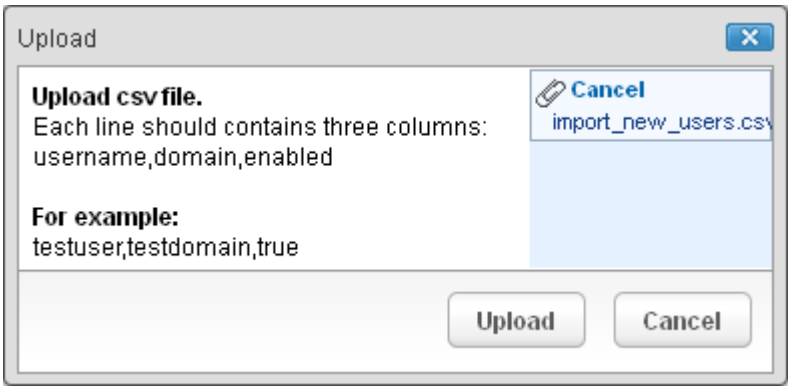
- Click the 'Import from CSV file' to import new users from a CSV file



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

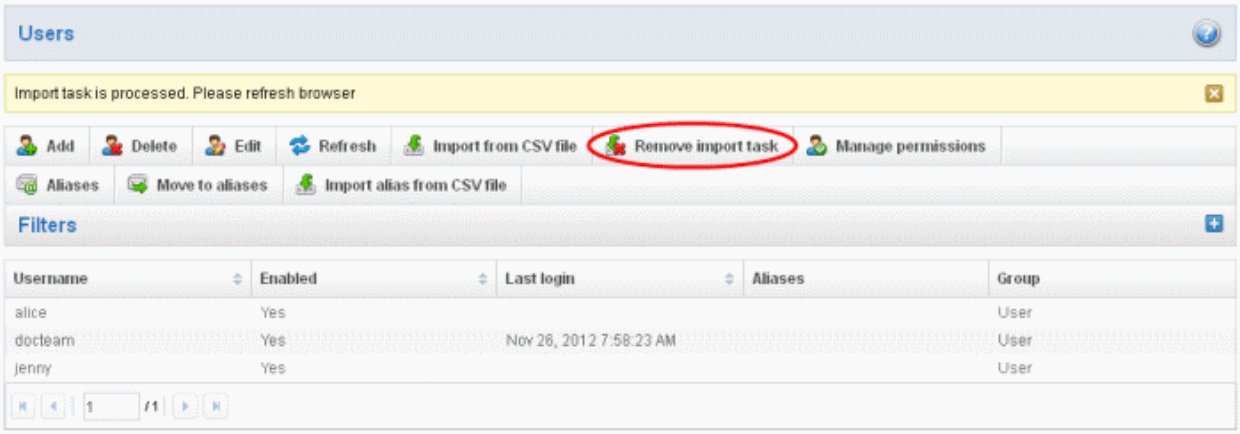


- The upload process is now ready. The maximum size of the file that can be uploaded is 9 MB. If you want to select another file, click 'Cancel' at top right side of the upload dialog. If you want to cancel the upload process, click the 'Cancel' button located at the bottom.

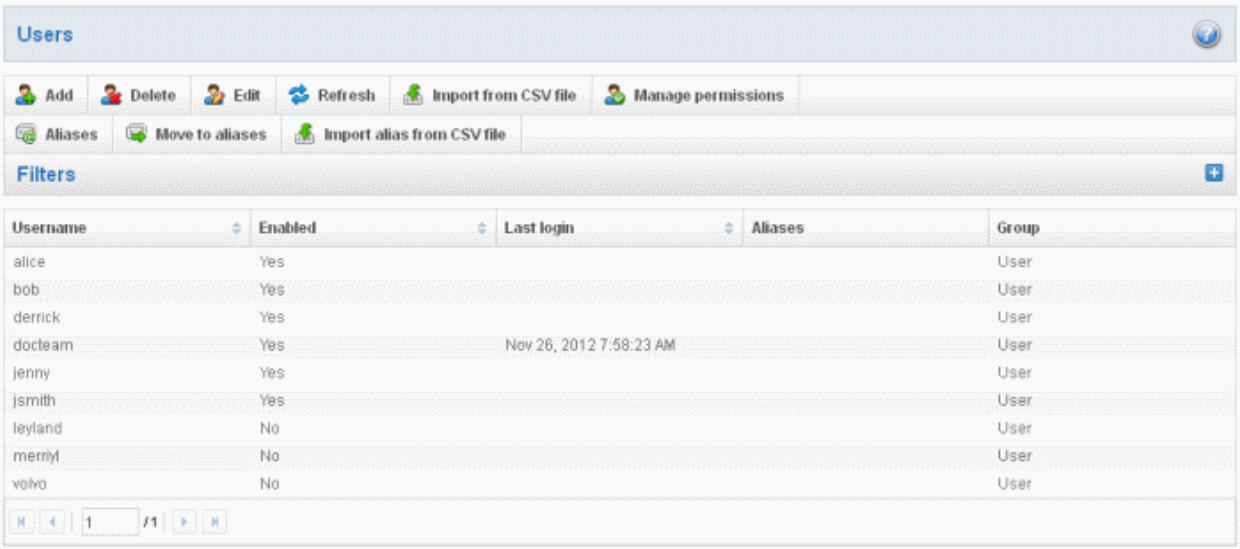


- Click the 'Upload' button to add new users.

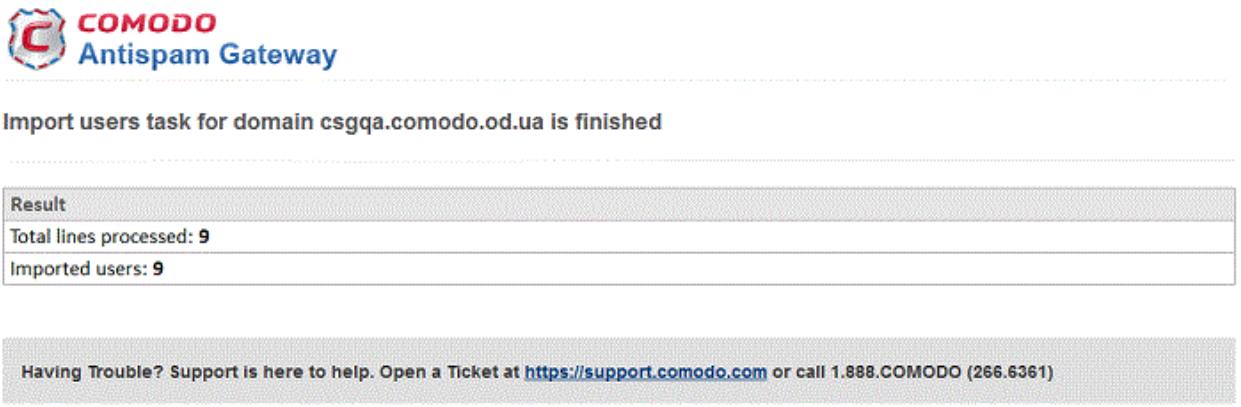
The upload will be placed in import tasks queue and the progress of the upload will be displayed. If you want to remove the upload from the queue, click the 'Remove import task from the queue' button. The 'Remove import task' deletes *only* a remaining part of not imported task.



On completion of the upload process, refresh the browser to view the imported users.



The administrator will receive a notification about the import task completion to his email.



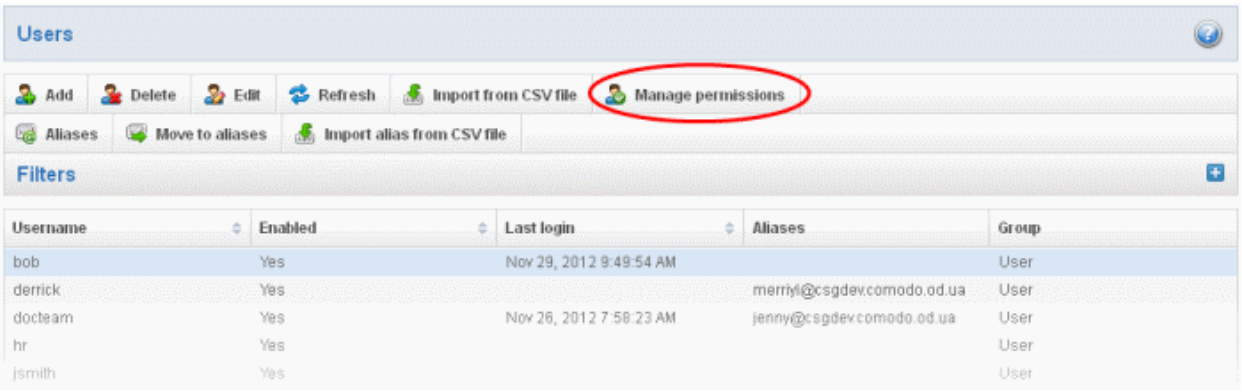
Note: During 'Import from CSV file' process the 'Import from Incoming users' will not be possible till the upload process is completed and vece-versa.

Managing Permissions

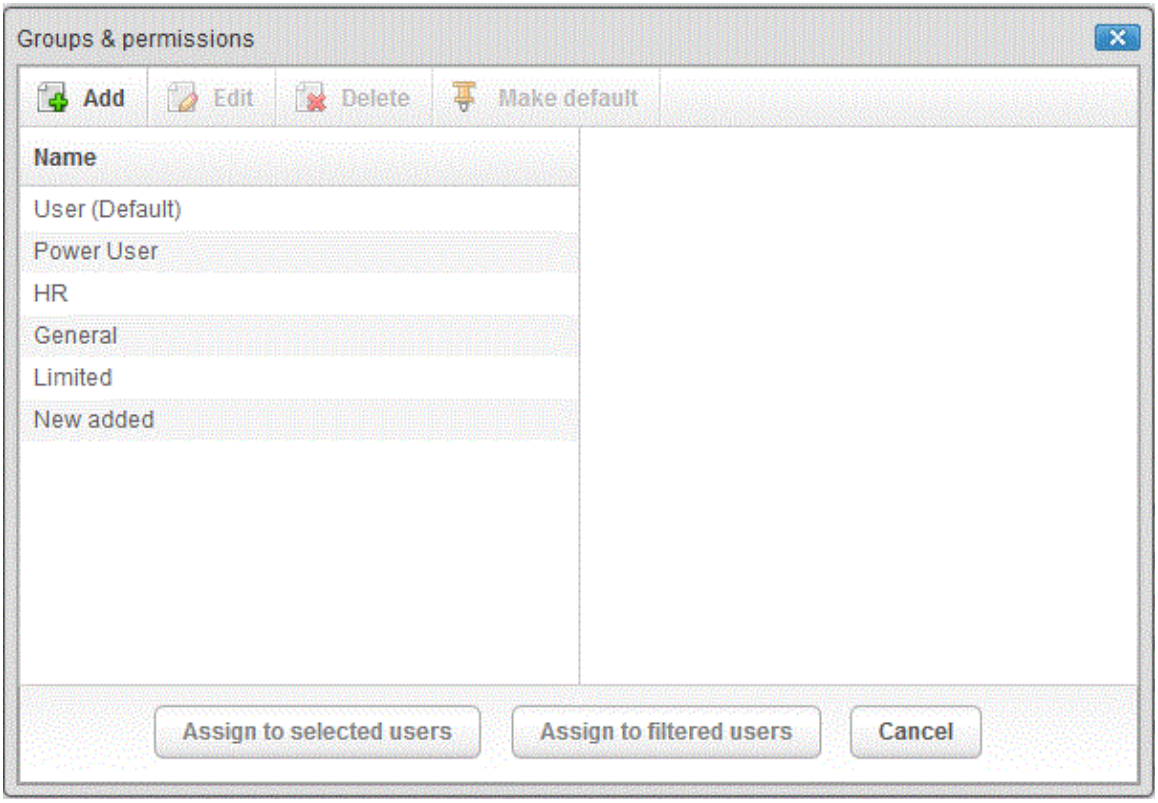
CASG allow administrators to assign permissions for users that will determine what the users can do and cannot do while logged into their respective CASG user interface. The administrators can create policies and assign them to users from this interface. See the section '**Groups & Permissions**' for more details on how to create groups and policies. A new user will be automatically assigned default permission settings.

To assign permissions for an user

- Select the user or multiple users (press Shift/CTRL + left button of the mouse) that you want assign permissions and click the 'Manage permissions' button.

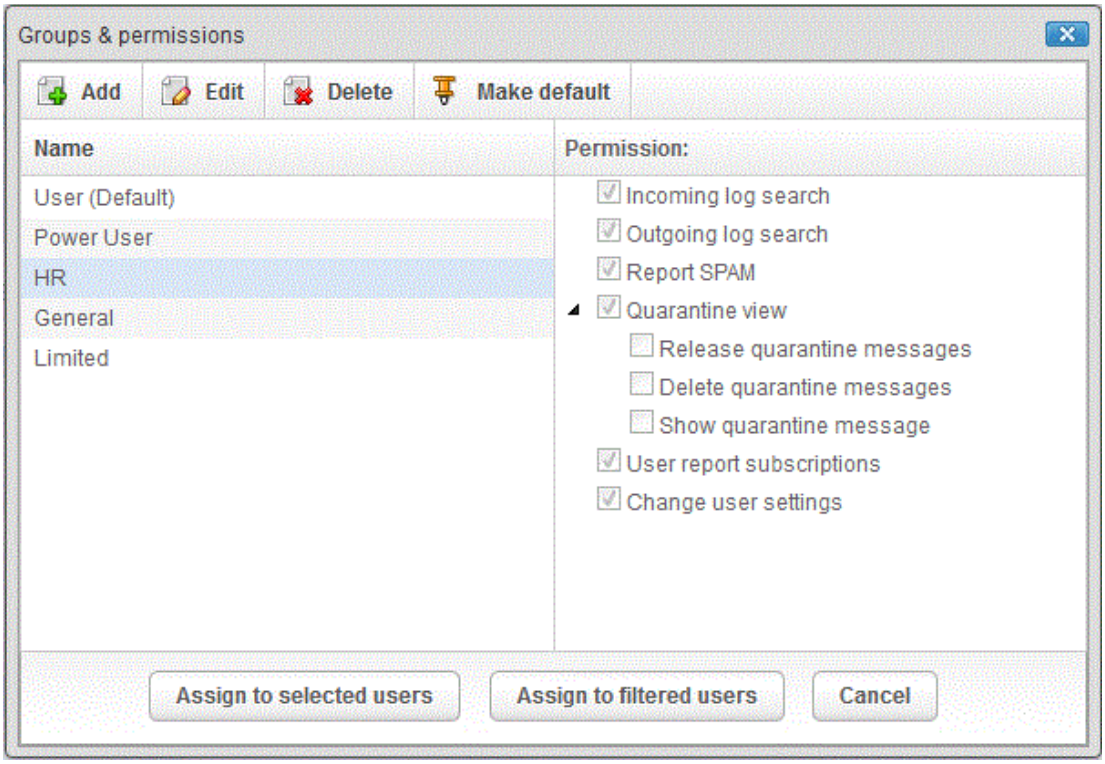


The 'Groups & permissions' interface will open.



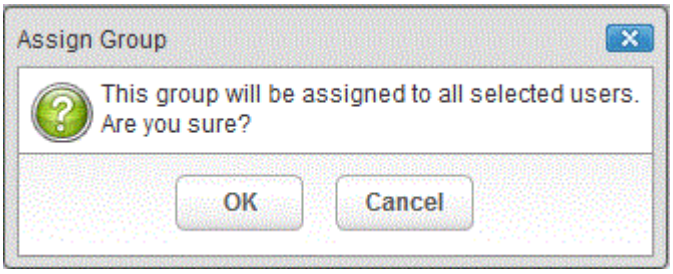
The interface displays the list of groups available with same or different permission levels for each group. By default, 'User (Default) and 'Power User' groups will be available and administrators can add, edit groups and assign permissions to users. See the section '**Groups & Permissions**' for more details.

- Select the group from the list.

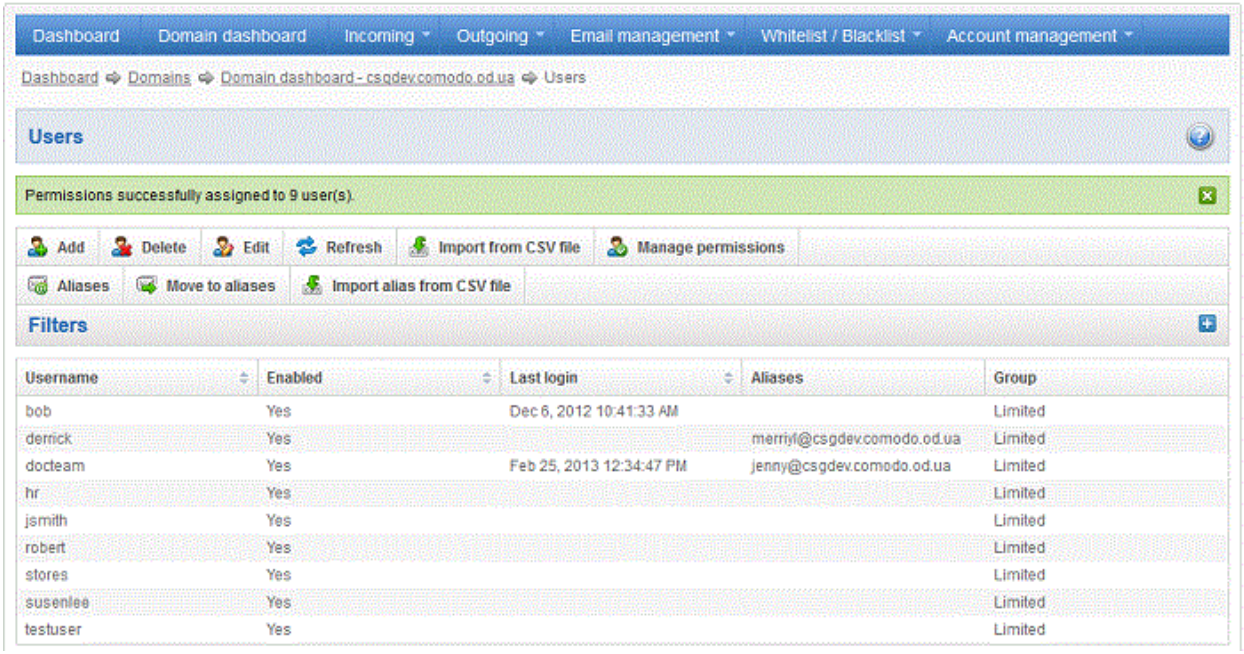


The permissions set for this group will be displayed on the right side.

- 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.



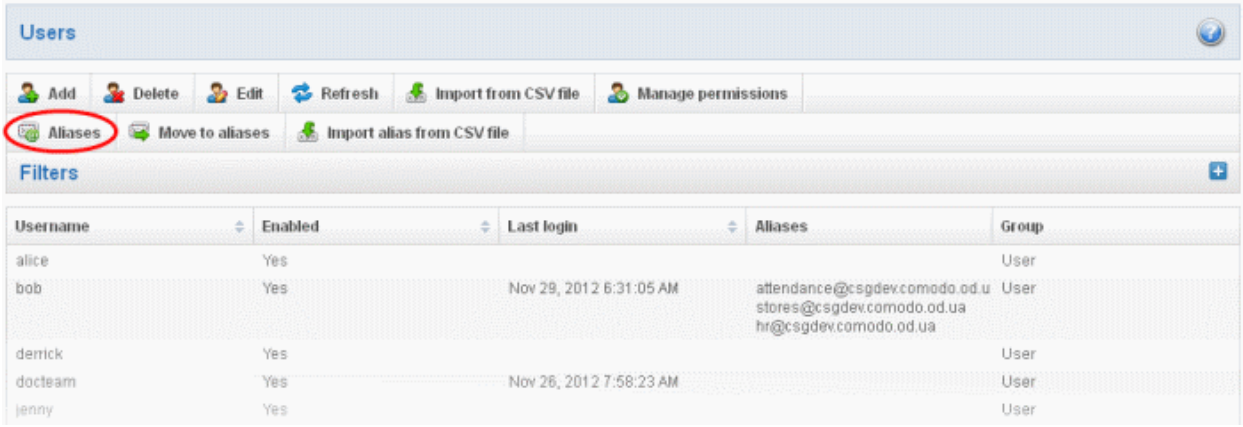
The selected user(s) will be assigned to the group and successfully assigned message will be displayed.



The interface also displays the new group assigned for the selected user under the 'Group' column.

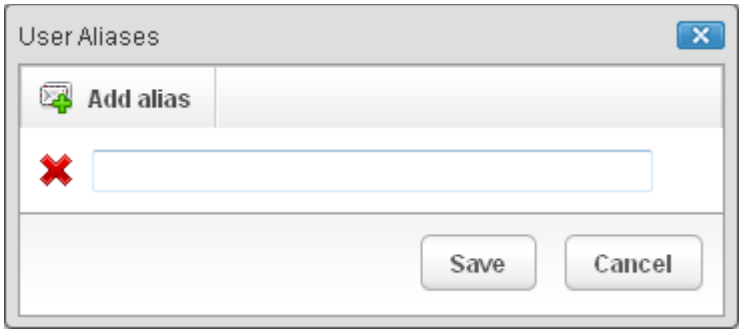
Adding user aliases

CASG allows admins to use a user alias name to organize emails related to different groups or functions into a single email inbox automatically. You can use it to protect your real email address.



- Enter the full email addresses (one per line) of the users who should receive the mail sent to the alias. (an email address of any domain on this computer can be an alias name. An user will have an access to an alias interface from the users dashboard and can work with it).
- Select an user and click 'Aliases' to add user aliases.
- Fill out the fields on the 'User Aliases' dialog, click on 'Save' to finish.

Note: A user cannot add an alias by themselves.

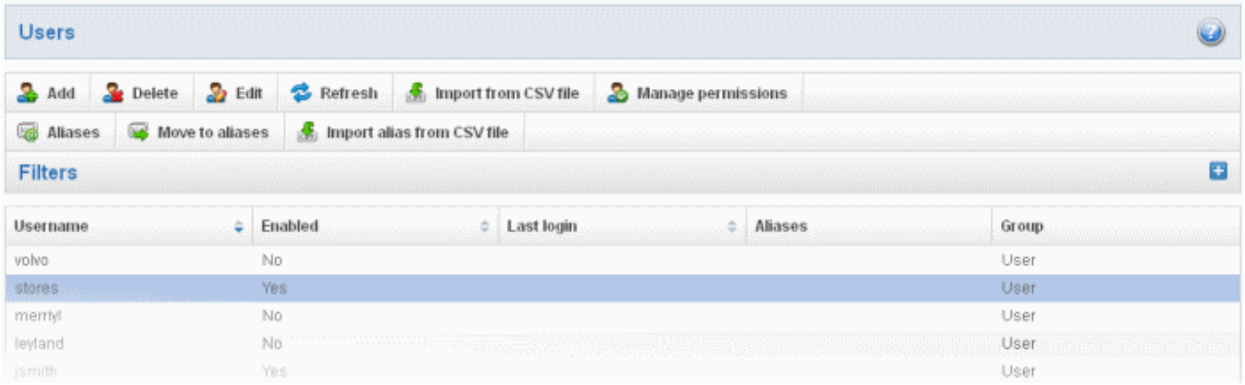


- To add multiple aliases click the Add alias button.
- To remove an added alias row click the icon beside it.

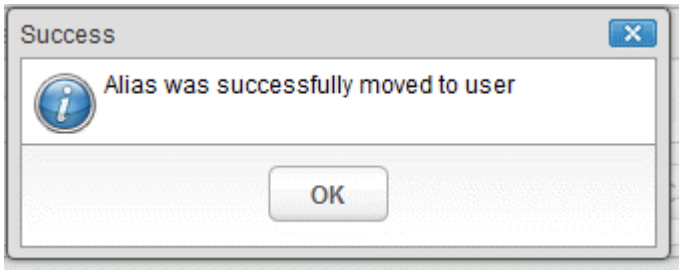
After adding an user to an alias, admin can extract him/her as user.

- Click the 'Aliases' button. 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 new user will appear in the list of the username.



A notification dialog confirming successful extraction will be displayed.

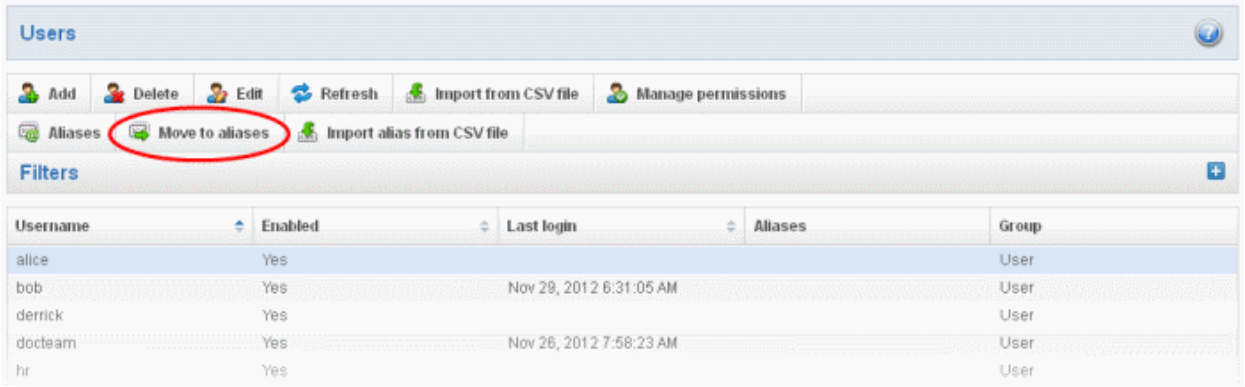


And a green strip will be appear above the user interface.

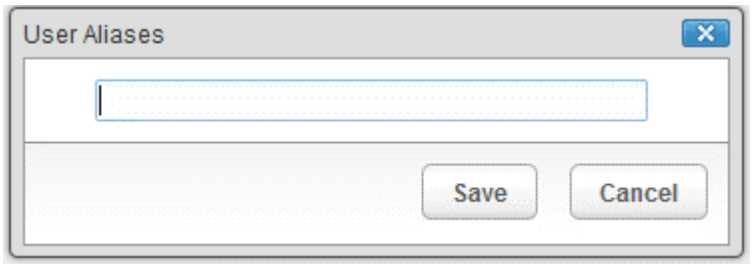
SUCCESS: Successfully saved

Moving user account to aliases

CASG allows admins to move an existing user to an alias.



- Select the user that have to be moved to an alias.
- Click the 'Move to aliases' button.
- Type a full email address of the user from your user's list.



- Click 'Save' to finish adding an alias.

Now, the selected user has become an alias of the user, whose email was entered in the input field of 'User Aliases' dialog.

Importing 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

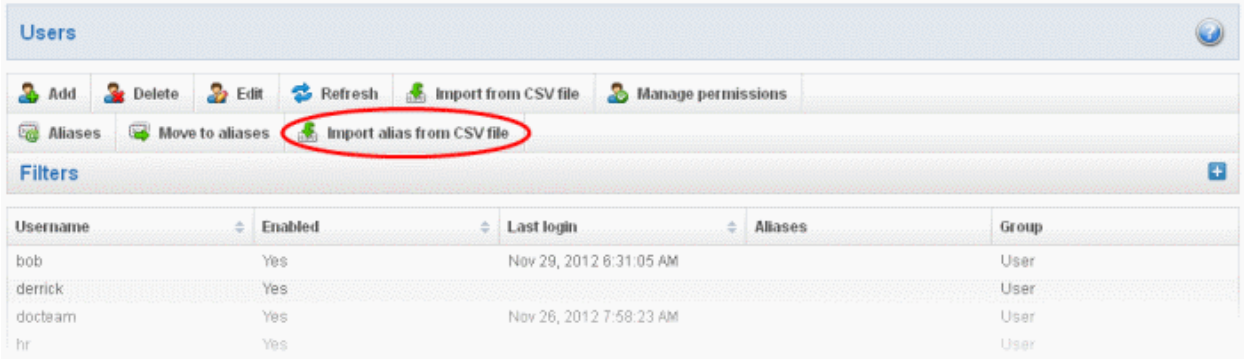
The following example shows how you can add alias for users for the selected domain and other domains available for your account.

alias@domain.com username1, username2, username3@domain2

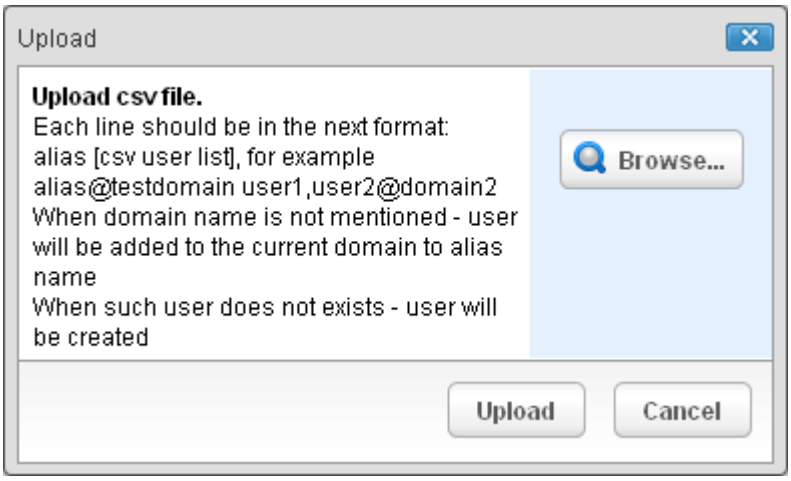
Please note that for adding many aliases at a time, each alias should be separated by a paragraph line. For example:

alias1@domain.com username1, username2
alias2@domain.com username1, username2, username3@domain2

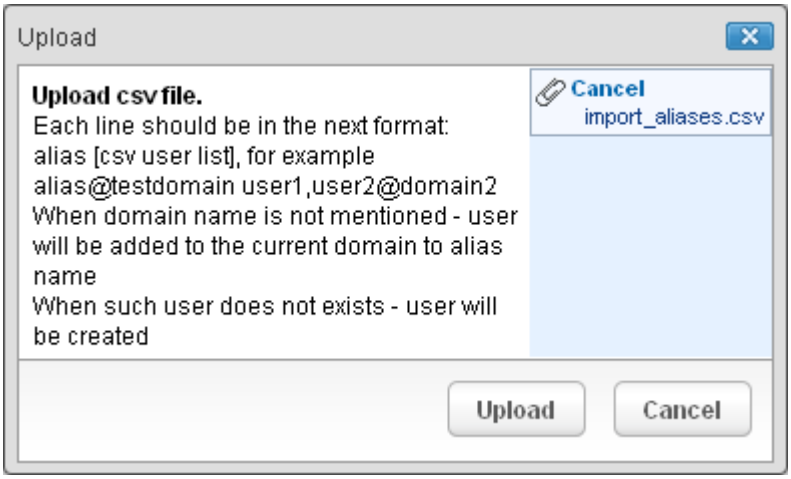
- Click the 'Import alias from CSV file' button to assign alias for users from a CSV file.



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

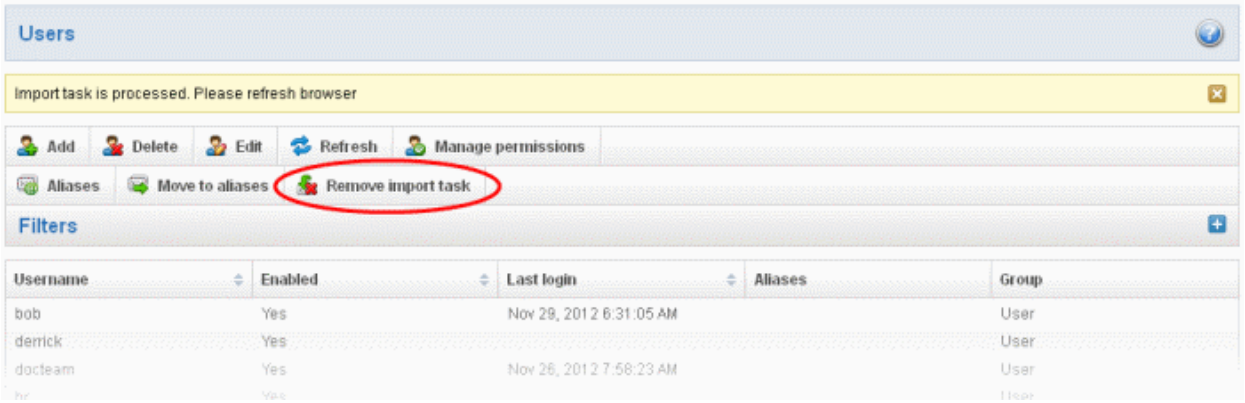


- The upload process is now ready. The maximum size of the file that can be uploaded is 9 MB. If you want to select another file, click 'Cancel' at top right side of the upload dialog. If you want to cancel the upload process, click the 'Cancel' button located at the bottom.

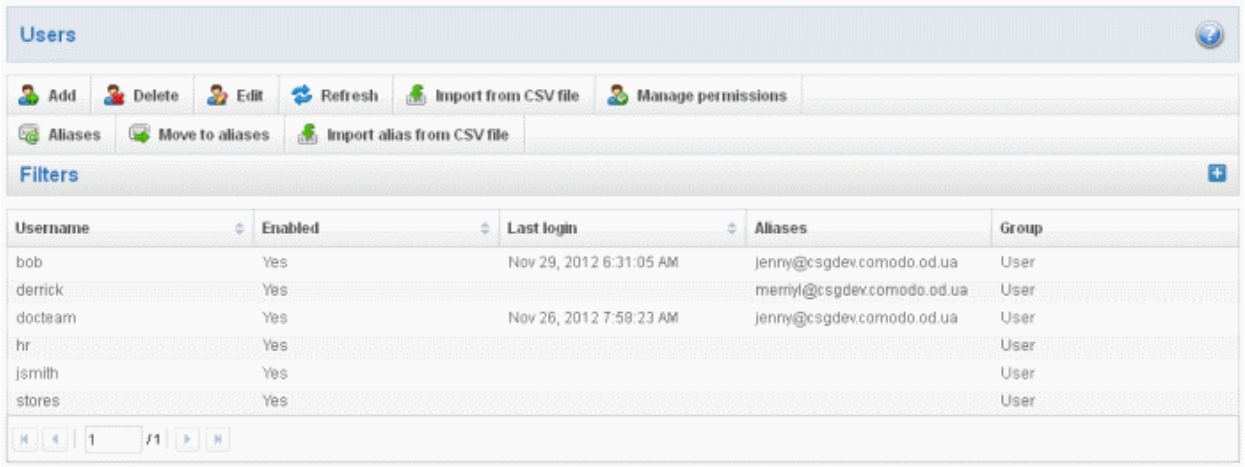


- Click the 'Upload' button.

The upload will be placed in 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.



- On completion of the upload process, refresh the browser to view the imported aliases.



3.2.1.4.5.2 Viewing User History

The 'User History' area contains a record of user account connections within a particular date range. You can filter users by IP address, last login, Domain or User name.

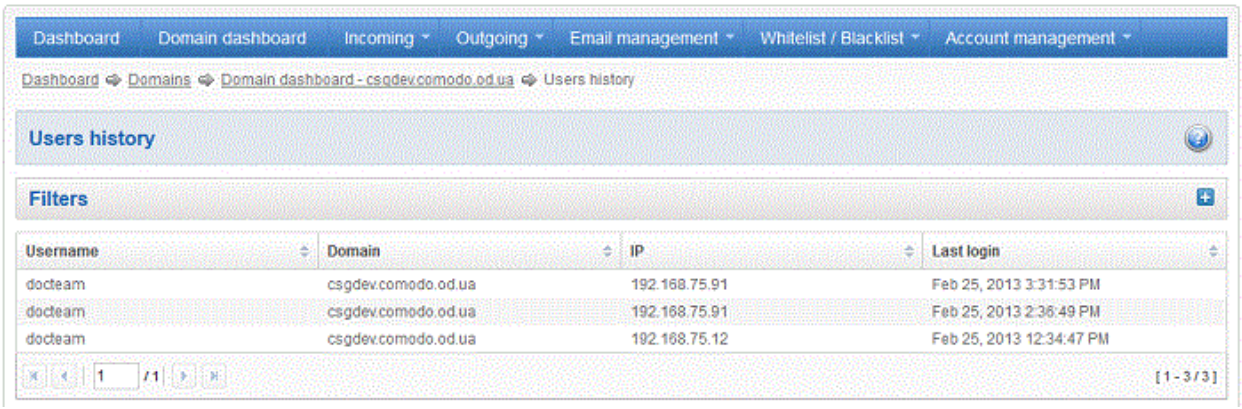
Note: This interface will show user connections to the current domain only (the domain that is shown near the top of the interface). If required, you can view user connections for all domains in the '**Account Management section**' (click 'Dashboard' then in the 'Account Management' section, click 'User's History').

The remainder of this page explains how to access the history interface and how to use filters to create custom searches.

Accessing the user history interface

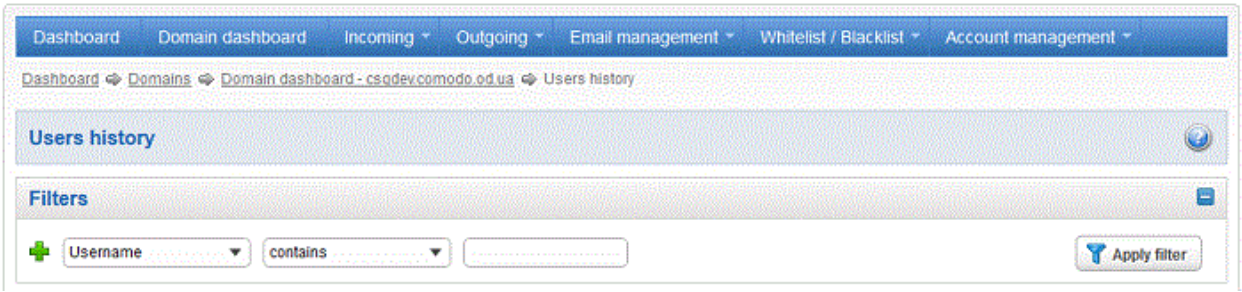
- Click 'Users history' from the 'Account management' drop-down menu in the menu bar or the icon in the 'Account management' configuration area.

The 'Users history' interface of the selected domain will open.

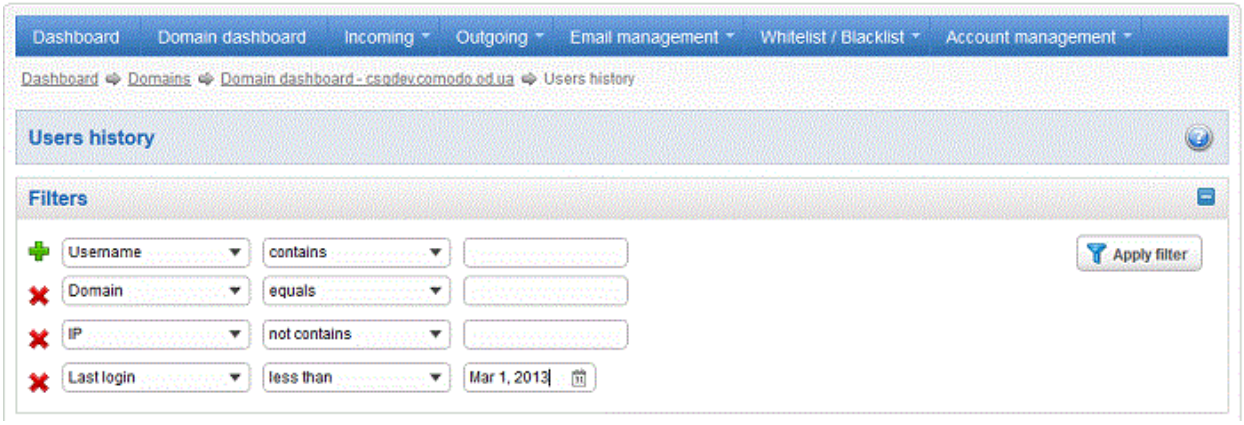


Using the filter option to search users

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



You can further refine your search by clicking to add more filters.



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

Available filters are:

Username: Will execute a search of usernames according to the text in the text box (column 3) and the condition selected in column 2.

If 'Username' is selected, the following conditions are available:

- **Equals**: Displays all usernames that match the text entered in the text box.
- **Not Equals**: Displays all users except the one entered in the text box.
- **Contains**: Displays all username(s) that contain the words entered in the text box.
- **Not Contains**: Displays all username(s) that do not contain the words entered in the text box.
- **Starts With**: Displays all username(s) that start with the words entered in the text box.

- **Ends With**: Displays all the username(s) that end with the words entered in the text box.

Other options available in the first drop-down in the filters area:

Domains: Sorts the results based on a user domains.

IP: Sorts the results based on a user domains details.

Last Login: Sorts the results based on the last login details of users.

Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

Click anywhere on the Filters tab to close the filters area.

3.2.1.4.5.3 Importing Users from LDAP

In addition to adding users manually and importing users from CSV file, CASG enables the administrators to import the users from the Active Directory (AD) server of the domain. You can configure CASG to access your AD server through Lightweight Directory Access Protocol (LDAP) to import the email users and to periodically synchronize with the AD server for automatic addition or removal of the users based on the changes made to the AD server.

Click the following links for more details:

- LDAP Import Configuration
- LDAP Import Confirmation List
- LDAP Import Ignore List

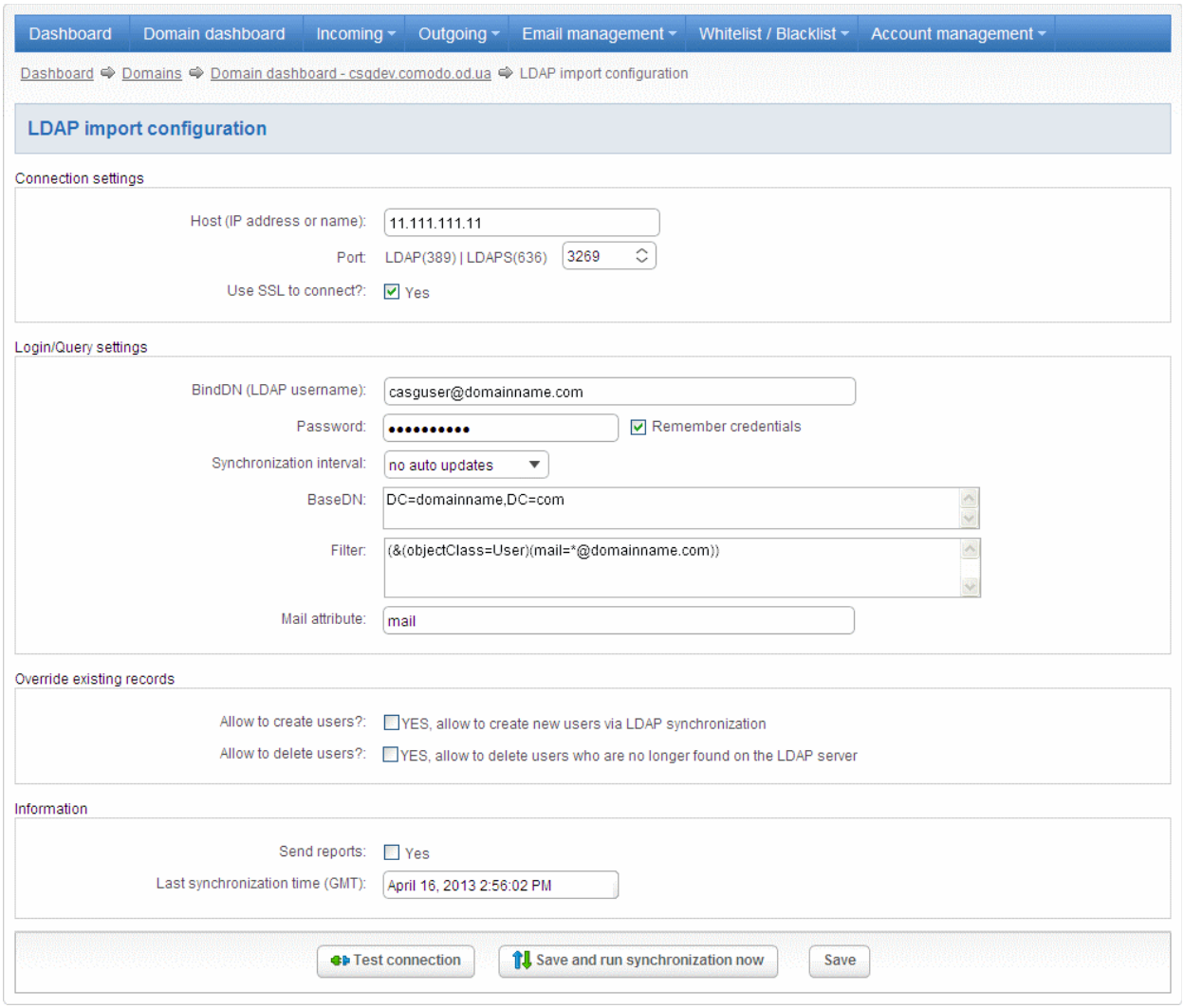
LDAP Import Configuration

The LDAP Import Configuration interface allows the administrators to configure CASG to import the email users from the Domains's Active Directory and to set for periodical synchronization. Once Active Directory has been configured, CASG imports the users into its interface and updates it periodically. For example if a new user is added in the Active Directory, CASG can automatically add the new user to CASG.

Accessing the LDAP import configuration interface

- Click 'LDAP import configuration' from the 'Account management' drop-down n the menu bar or click the icon from the 'Account management' configuration area.

The 'LDAP import configuration' interface of the selected domain will open.



Connection Settings

- **Host (IP Address or Name)** – Enter the external hostname or external IP address of the AD server. If your Organization uses the same physical server for AD server and the Mail Exchange server, then enter the host name or IP address of the mail server.
- **Port** - Enter the port number of Active Directory Server's LDAP port.
  - 389 is the default port for non-SSL connection ('Use SSL To Connect' box NOT checked)
  - 636 is the default port if SSL connection is active ('Use SSL To Connect' box checked)
- **Use SSL To Connect?** - Select the 'Yes' check box if you wish us to use secure LDAP. In order to use secure LDAP, you need to install an SSL certificate from a Certification Authority (CA) like Comodo CA in your AD server. Self Signed certificates are not allowed.

Note: SSL access should have been enabled for AD Server before opting for SSL usage.

Login/Query Settings

- **BindDN (LDAP username)** - Enter the username of the user account using which CASG server can access the AD server. Preferably, a new user account can be created for the CASG server in the AD server with a new user name and password. 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 CASG user account.
- **Remember Credentials** - Enable this option if you wish CASG server to remember the username/password of the user account, in order to automatically login.

Note: If you are configuring for automatic periodic synchronization, CASG will store the username and password by default to connect to the AD server at the set time interval to update the user base, hence the option 'Remember Credentials' will not be visible. The option will be visible for you to enable or disable if 'Synchronization Interval' setting is set as 'no auto updates'.

- **Synchronization interval** - If you wish to configure CASG to automatically connect to the AD server and synchronize the user base, select the time interval for synchronization from the drop-down. Else, 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:

- CASG can only import LDAP users that have email addresses on domains that you have added to CASG in the **Domains** interface.
- To successfully import users, you must make sure the domain of their email addresses has been added to CASG AND that the LDAP Import is configured for each individual domain from the **Domain Management Area** of the respective domain.

- **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 to create users?** – 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 to delete users?** – 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**.

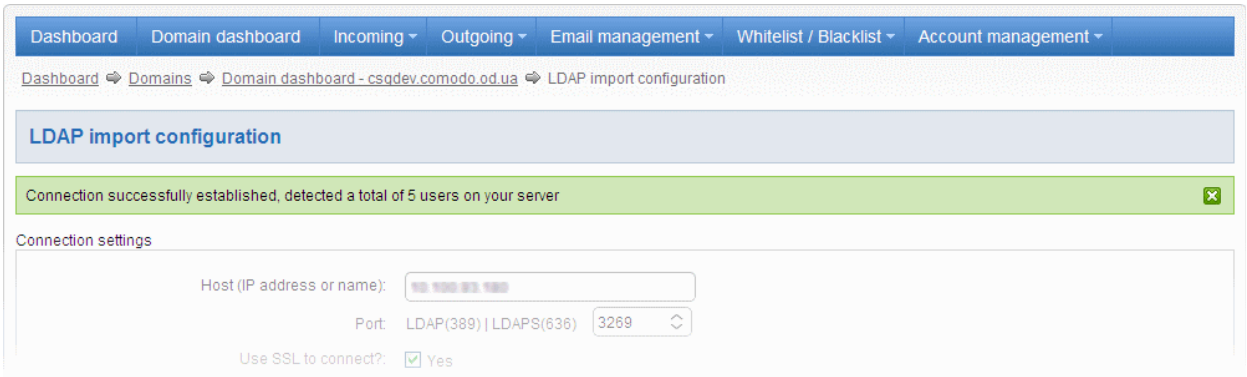
Information Settings

- **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.

- 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.



- To save your configuration, click 'Save'.
- To Save your configuration and run a manual synchronization of user base with the AD server instantly, click 'Save and run synchronization' now

LDAP Import Confirmation List

The LDAP import confirmation list interface displays the list of:

- Users created at the AD server and yet to be imported into CASG
- Users removed from AD server and yet to be removed from CASG

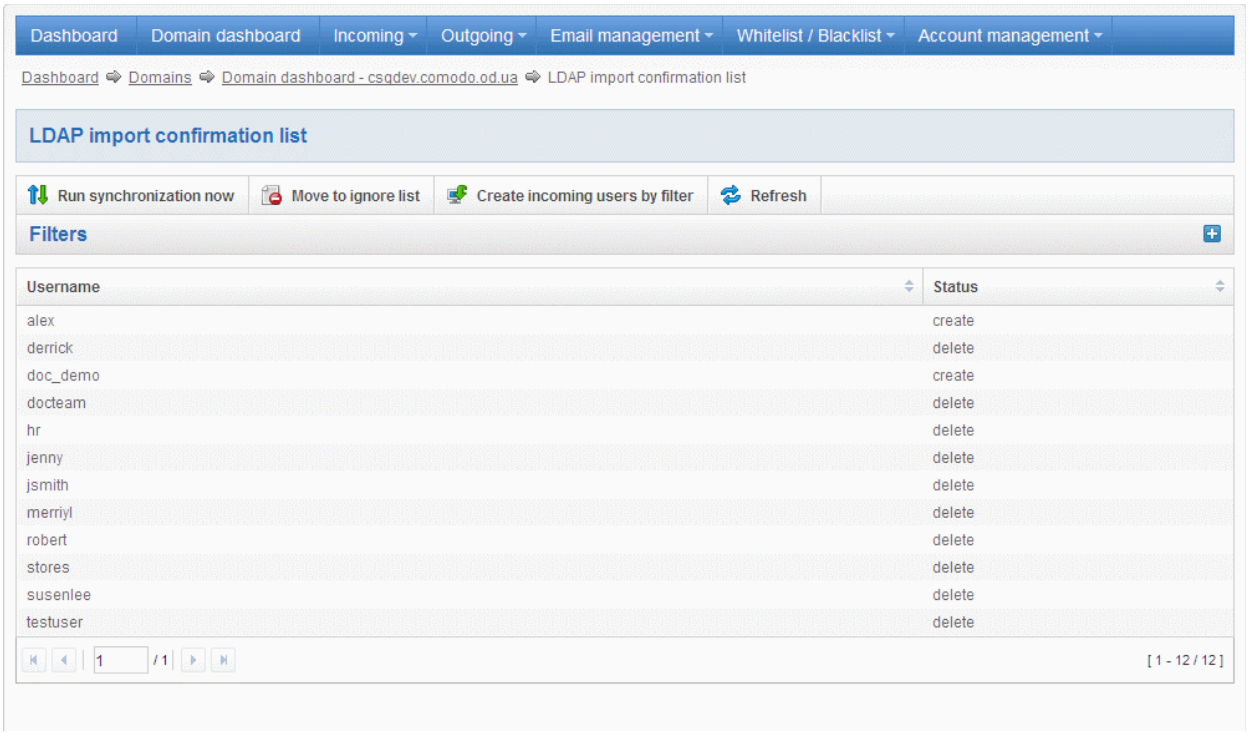
… if "**Allow to create users?' / 'Allow to delete users?**' are not enabled in **LDAP import configuration interface**, along with the list of users created in CASG. The administrator can import the users created at AD server into CASG manually and remove existing users from this interface.

Also, the administrator can initiate an on-demand synchronization from this interface.

Accessing the LDAP import confirmation list interface

- Click 'LDAP import confirmation list' from the 'Account management' drop-down n the menu bar or click the icon from the 'Account management' configuration area.

The 'LDAP import confirmation list' interface of the selected domain will open.

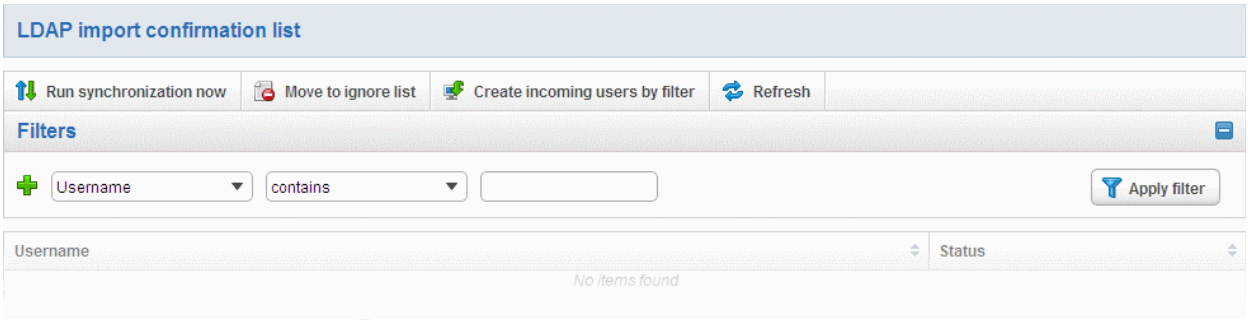


The list of users added to and deleted from the AD server with the existing users created at CASG will be displayed.

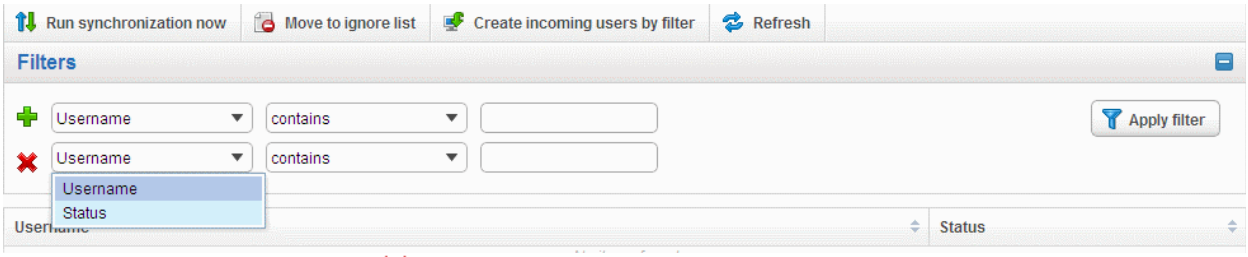
- New users added to the AD server will be displayed with the status 'Create'
- Users removed from the AD server will be displayed with the status 'Delete'

Using the filter option to search users

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



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



You can remove a filter by clicking the ✖ icon beside it.

Available filters are:

- **Username:** Will execute a search of usernames according to the text in the text box (column 3) and the condition selected in column 2.

If 'Username' is selected, the following conditions are available:

- **Equals**: Displays all usernames that match the text entered in the text box.

- **Not Equals**: Displays all users except the one entered in the text box.
- **Contains**: Displays all username(s) that contain the words entered in the text box.
- **Not Contains**: Displays all username(s) that do not contain the words entered in the text box.
- **Starts With**: Displays all username(s) that start with the words entered in the text box.
- **Ends With**: Displays all the username(s) that end with the words entered in the text box.

Other options available in the first drop-down in the filters area:

- **Status:** Sorts the results based on whether a user's status is 'Create' or 'Delete' selected from third column and condition selected from second column.

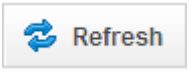
If 'Status' is selected, the following conditions are available:

- **Equals**: Displays the users whose status is as chosen in third column
- **Not Equals**: Displays the users whose status is opposite to that chosen in third column

Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

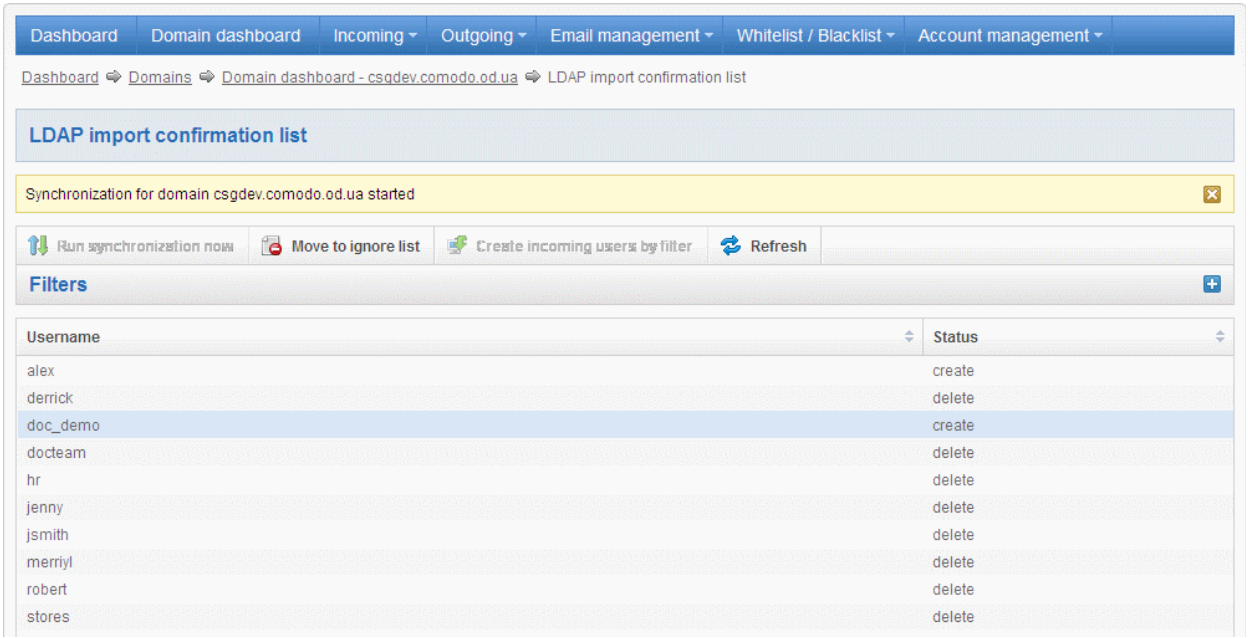
Click anywhere on the Filters tab to close the filters area.

Click the 

button to display all users.

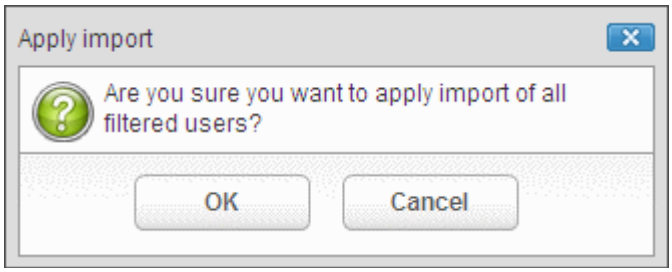
Note: To display all the users after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

- To run a manual on-demand synchronization, click 'Run Synchronization Now'

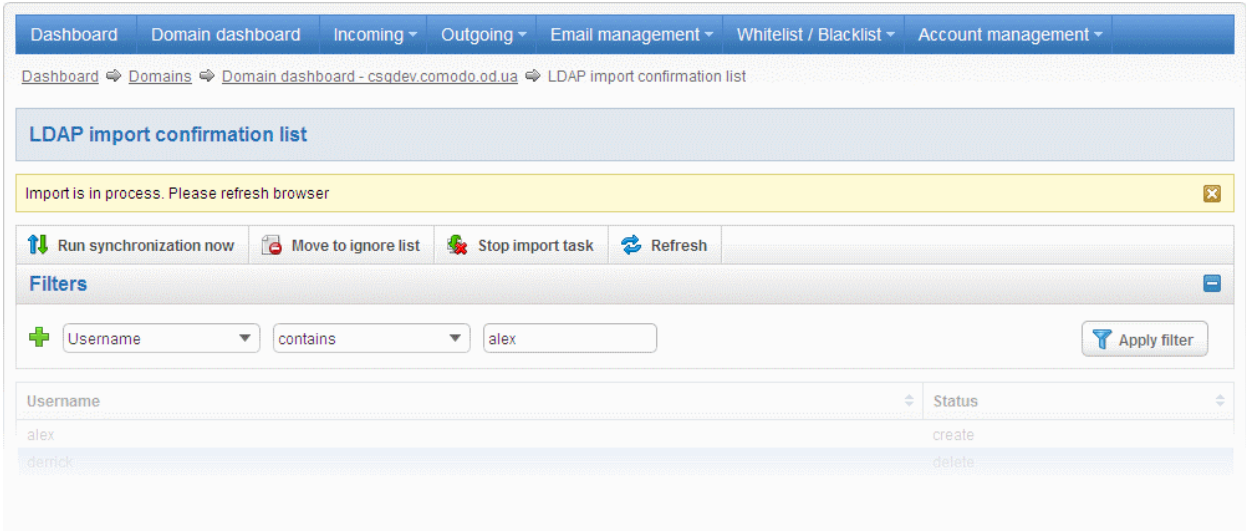


CASG server will connect to your AD server and start detecting the changes in the users in the AD server. If you have not selected the option **Remember credentials** in **LDAP Import Configuration interface**, you will be asked to enter the username and password for CASG to access the AD server.

- To import all users created at the AD server and to delete all the users removed from AD server at once, clear all the filters and click 'Create incoming users by filter'. A confirmation dialog will be displayed.

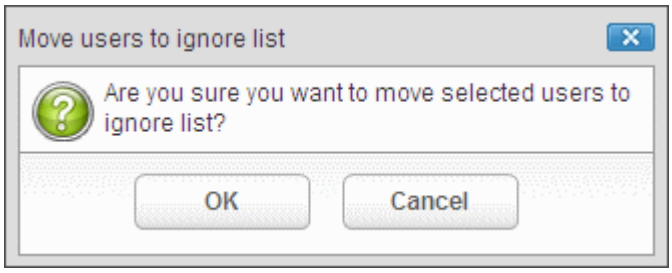


- Click OK. The import progress will be displayed.



- Refresh the browser to complete the process.

- To import selected users from the AD server or to delete selected users removed from AD server, apply filters as described above and click 'Create incoming users by filter'. A confirmation dialog will be displayed.
  - Click OK in the confirmation dialog. The users will be imported/deleted and the progress will be displayed.
  - Refresh the browser to complete the process.
- 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

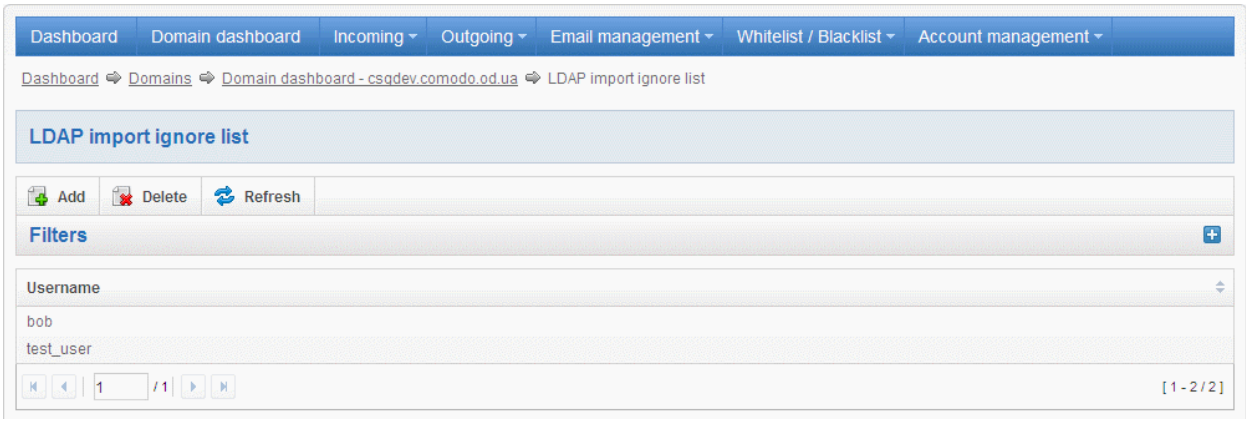
The LDAP import ignore list interface displays a list of users to be skipped from being created or deleted in CASG during synchronization with the AD server. Users can be moved to ignore list from the LDAP Import Confirmation List interface or manually added. Once added to the ignore list, the user will be skipped from the AD server from the next synchronization operation.

Accessing the LDAP import confirmation list interface

- Click 'LDAP import ignore list' from the 'Account management' drop-down n the menu bar or click the

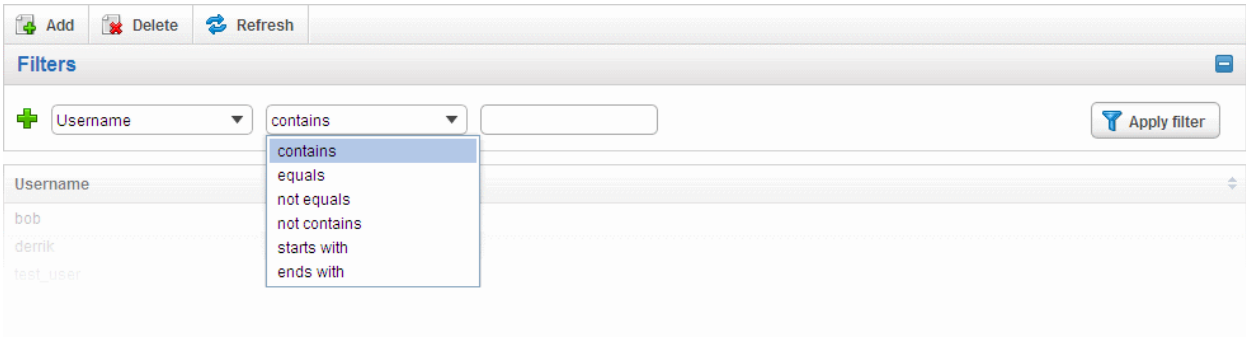
icon from the 'Account management' configuration area.

The 'LDAP import ignore list' interface of the selected domain will open.



Using the filter option to search users

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



Available filters are:

- **Username:** Will execute a search of usernames according to the text in the text box (column 3) and the condition selected in column 2.

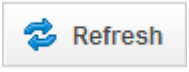
The following conditions are available:

- **Equals**: Displays all usernames that match the text entered in the text box.
- **Not Equals**: Displays all users except the one entered in the text box.
- **Contains**: Displays all username(s) that contain the words entered in the text box.
- **Not Contains**: Displays all username(s) that do not contain the words entered in the text box.
- **Starts With**: Displays all username(s) that start with the words entered in the text box.
- **Ends With**: Displays all the username(s) that end with the words entered in the text box.

Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

Click anywhere on the Filters tab to close the filters area.

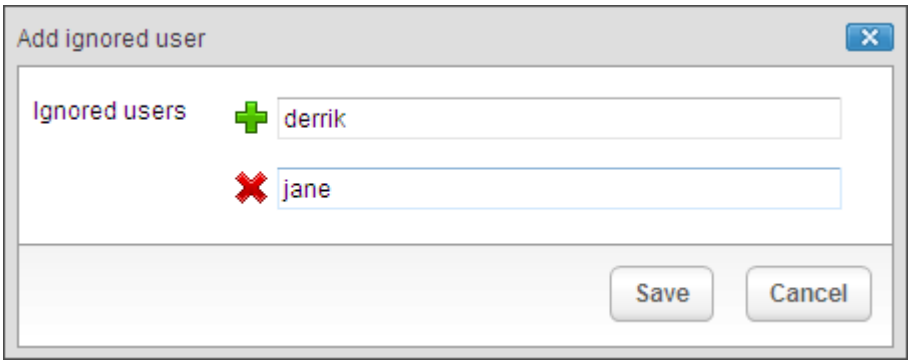
Click the 

button to display all users.

Note: To display all the users after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

To add users to ignore list

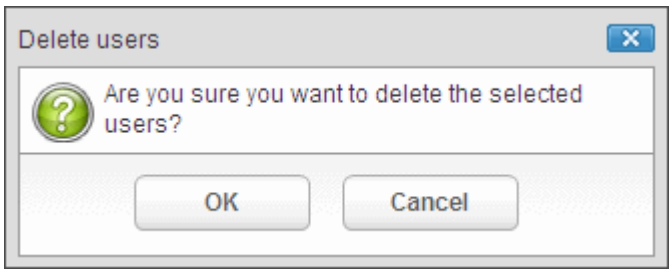
- Click 'Add'. The Add ignored user dialog will open.



- Enter the user names to be added to the ignore list
- Click the icon to add more users
- Click Save to add the users.

To remove the users from the ignore list

- Select the users and click 'Delete'. A confirmation dialog will be displayed.



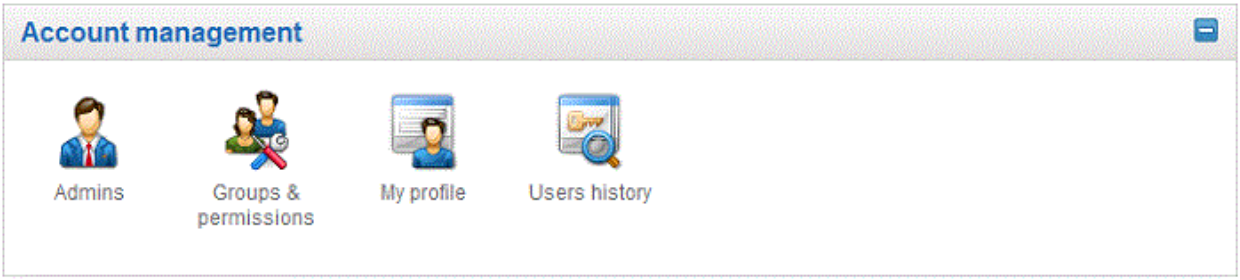
- Click OK.

The users will be removed from the list.

- 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.

3.2.2 Administrator Account Management

The Account Management area of CASG allows an administrator to add new administrators for the same account. The edit section in this area allows the administrator to reset passwords and change the login status from enabled to disabled and vice-versa.



Click the following links for more details:

- Managing Administrators
- Groups & Permissions

- My Profile
- Users History

3.2.2.1 Administrators

In this interface of the CASG, an administrator can add new administrators as well as edit the login status and regenerate new password for existing administrators.

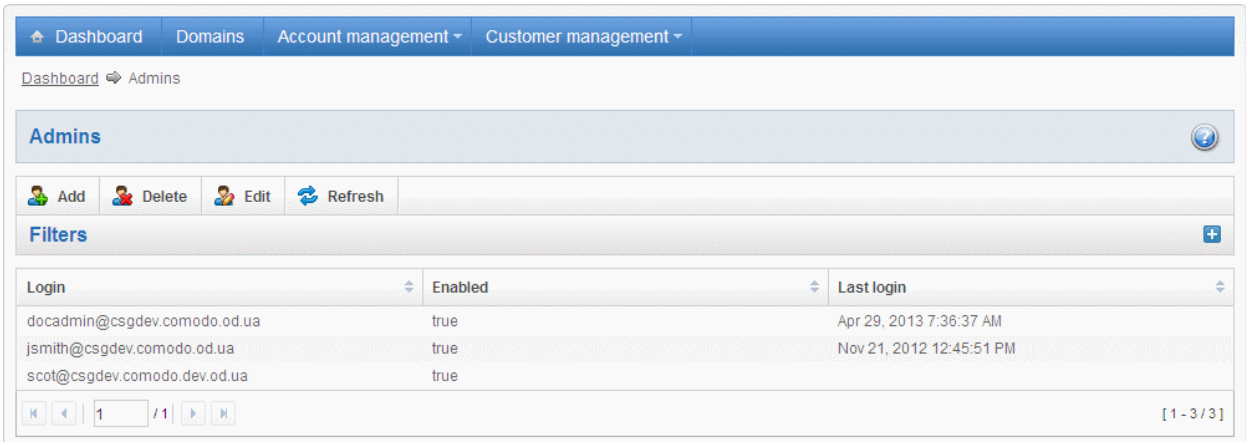
Click the following links for more details:

- Managing Administrators
- Adding New Administrators
- Deleting Administrators
- Editing Administrators

Managing Administrators

- Click 'Admins' from the 'Account management' drop-down menu from the menu bar or the icon in the 'Account management' configuration area

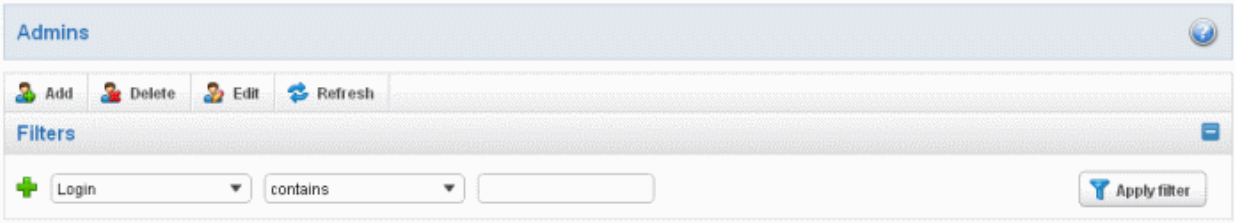
The 'Admins' configuration interface will open:



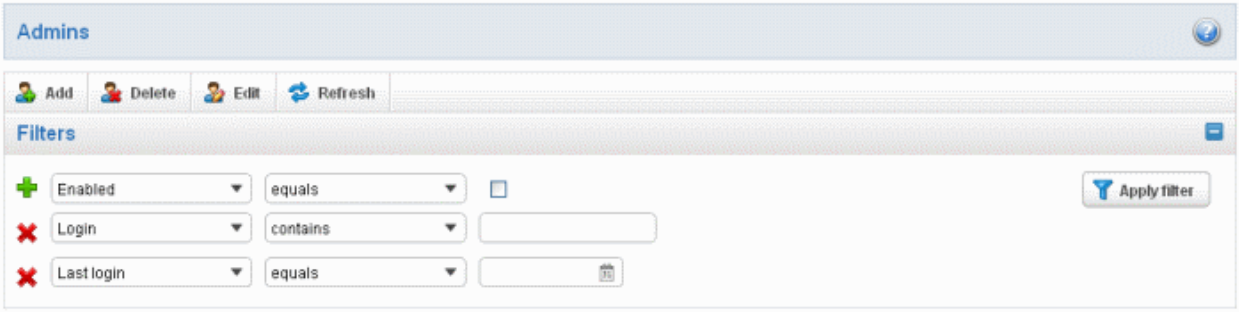
The 'Admins' interface displays a list of administrators with their CASG enabled/disabled status and their last login date and time. You can sort the entries in ascending or descending order based on the login, enabled status, report subscription status or last login time by clicking the up/down arrows in the respective column headers.

Using the filter option to search administrators

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



You can refine your search much further by clicking ✚ to add to more filters.



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

Following are the options in the first drop-down in the filters area:

- **Login:** Displays the result based on the administrator name entered in the text box.

When you select this option in the first drop-down, the following filters are available in the second drop-down:

- **Equals:** Displays the results based on the user name that was entered in full in the text box.
- **Not Equals:** Displays all user(s), except the one entered in the text box.
- **Contains:** Displays all user(s) that contains the words entered in the text box.
- **Not Contains:** Displays all user(s) that does not contain the words entered in the text box.
- **Starts With:** Displays all user(s) that starts with the words entered in the text box.
- **Ends With:** Displays all user(s) that ends with the words entered in the text box.

Other options available in the first drop-down in the filters area:

- **Enabled:** Sorts the results based on administrators' enabled / disabled status.

When you select this option in the first drop-down, 'equals' is the only option available in the second drop-down:

- **Equals:** Displays the results of enabled administrator(s) when the checkbox beside it is selected. When the checkbox is not selected, it displays the list of user(s) who are not enabled.

- **Last Login:** Sorts the results based on the last login details of user(s).

When you select this option in the first drop-down, the following filters are available:

- **Equals:** Displays the list of user(s) that has the last logged in on the same date as the selected date in the third box from the calendar.
- **Less than:** Displays the list of user(s) that has the last logged in on dates less than the selected date in the third box from the calendar.
- **Greater than:** Displays the list of user(s) that has the last logged in on dates greater than the selected date in the third box from the calendar.

Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

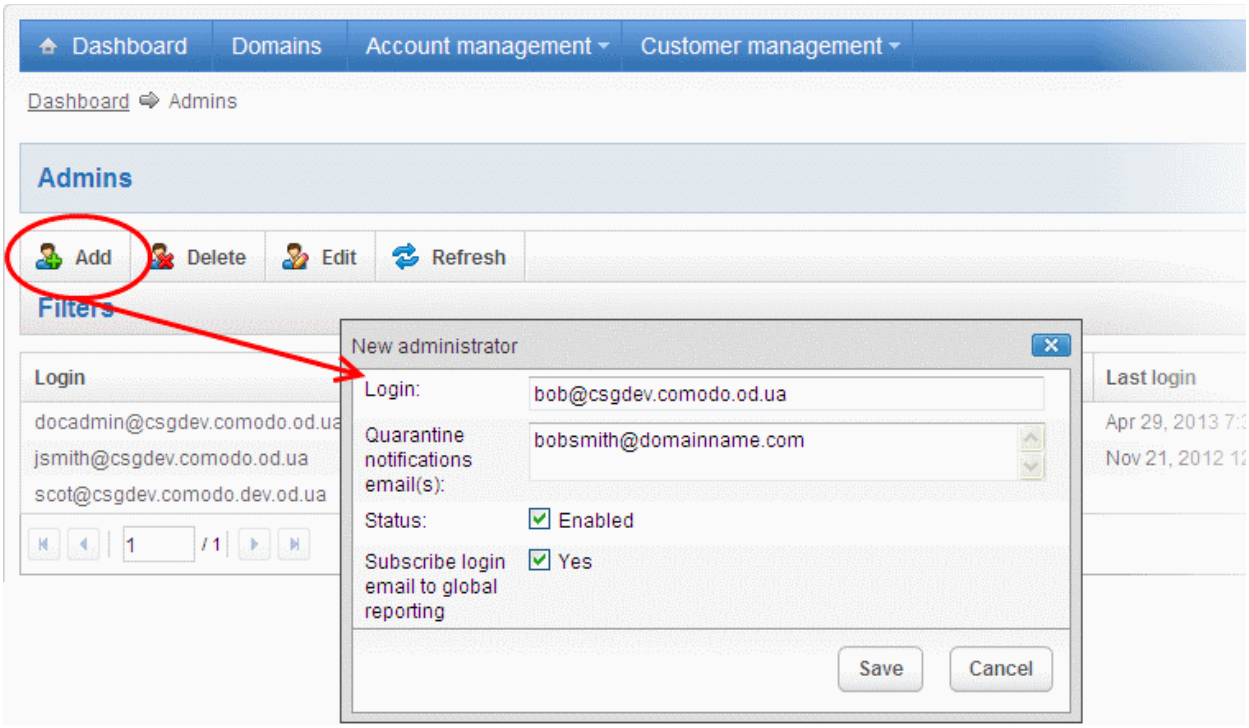
Click anywhere on the Filters tab to close the filters area.

Click the Refresh button to display all user.

Note: To display all the administrators after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

To add a new administrator

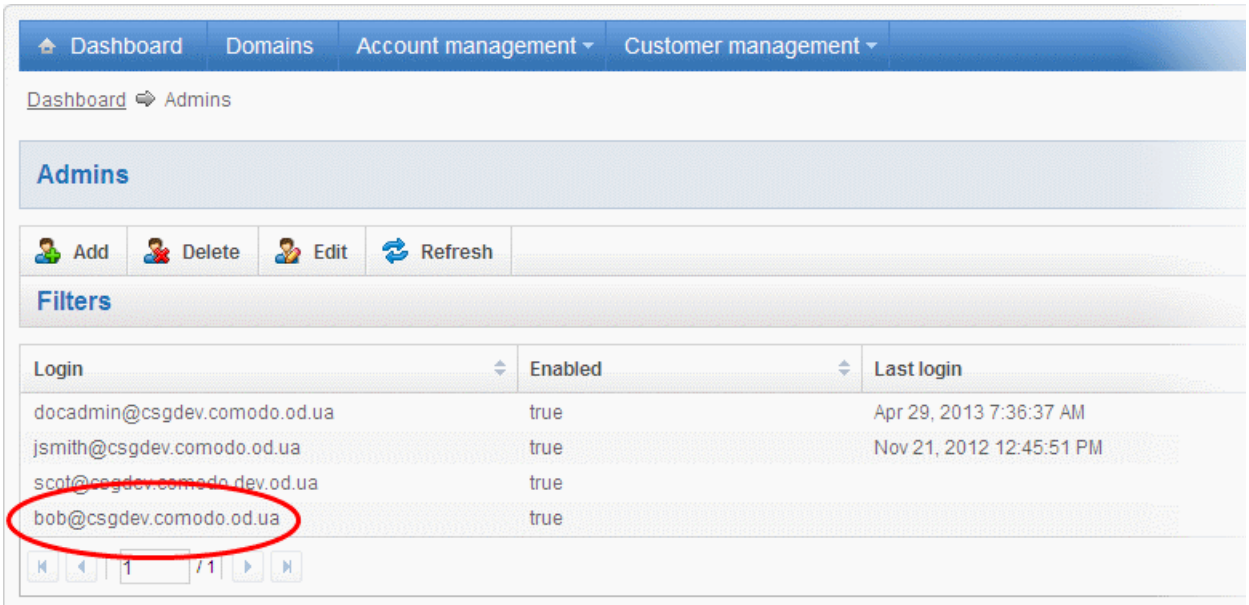
- Click the Add button.



The 'New administrator' dialog will open.

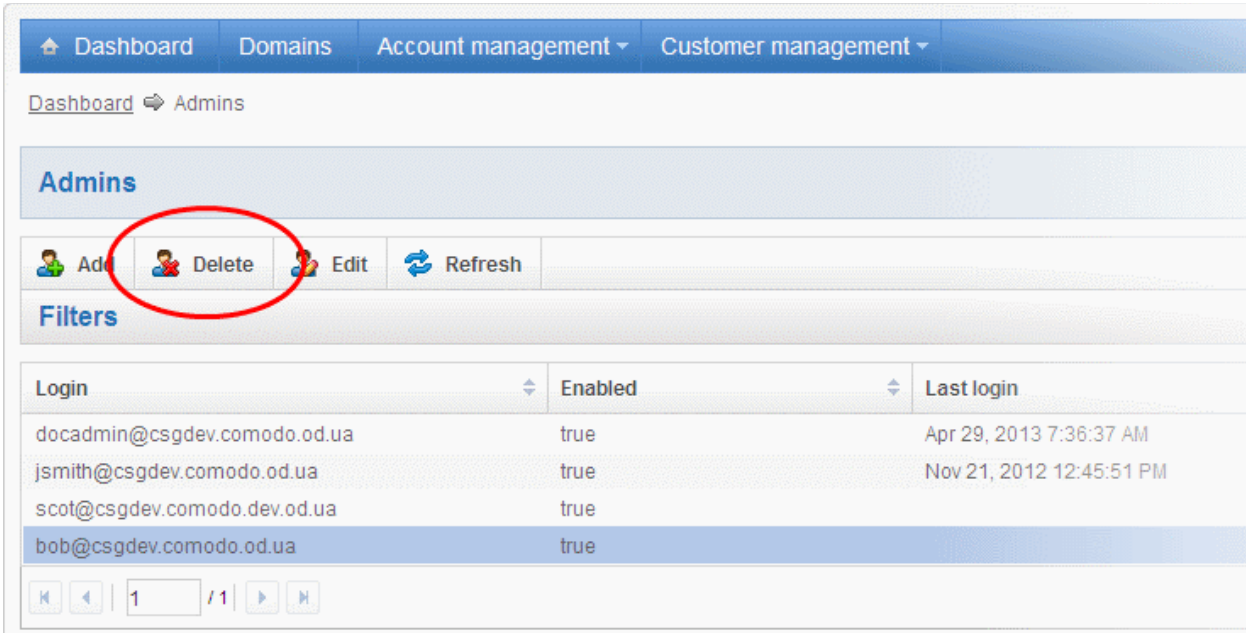
- **Login** - Enter the new administrator's valid email address as login username.
- **Quarantine notifications email(s)** - Enter the email addresses at which the new administrator should receive quarantine request emails from CASG. It can be the same email address as the login name or an alternative email address(es) of the administrator. The quarantine requests from users, for blacklisting, whitelisting, or releasing quarantined emails will be sent to the email addresses specified in this field. Refer to the section **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 login email to global reporting** – Selecting this checkbox enables the new administrator to receive the periodical domain and quarantine summary reports of all domains belonging to the account at the email address specified as login user name. Refer to **CASG Reports - an Overview** for more details.
- Click the 'Save' button.

An email to the added administrator will be sent automatically containing password to access CASG. The password can be reset in the **edit interface**. The added administrator will be displayed in the list.



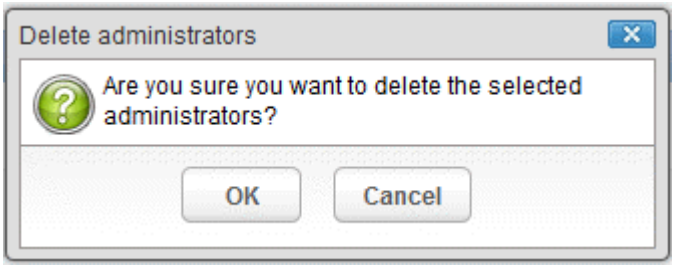
To delete an administrator

- Select the administrator to be removed and click the 'Delete' button.



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

A confirm dialog will be displayed warning you that the selected administrators will be deleted.



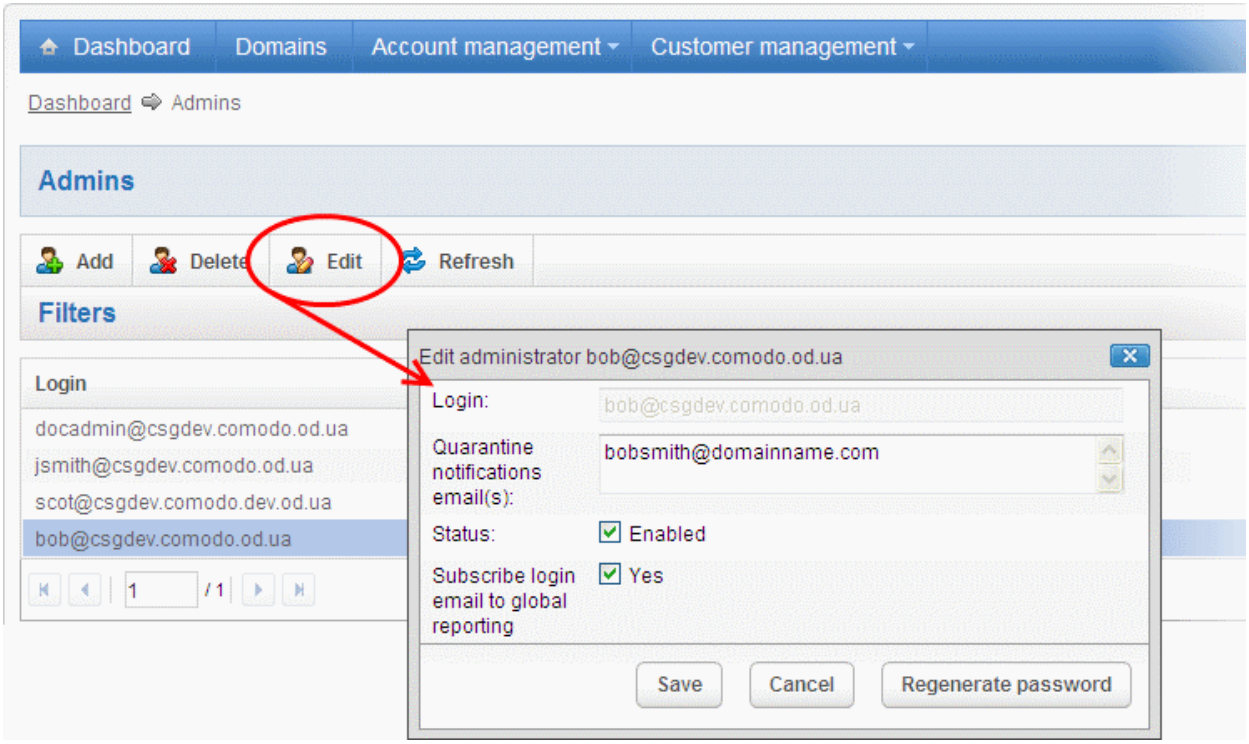
- Click 'OK' to confirm the deletion.

The selected administrator will be deleted from the list.

To edit an existing administrator

You can reset password, enable or disable global report generation and allow or deny permission for the administrators to access their CASG account in the edit interface.

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



The 'Edit administrator' dialog box will be displayed.

- **Quarantine notifications email(s)** - Enter the email addresses at which the new administrator should receive quarantine request emails from CASG. It can be the same email address as the login name or an alternative email address(es) of the administrator. The quarantine requests from users, for blacklisting, whitelisting, or releasing quarantined emails will be sent to the email addresses specified in this field. Refer to the section **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 login email to global reporting** - Selecting this checkbox enables the new administrator to receive the periodical domain and quarantine summary reports of all domains belonging to the account at the email address specified as login user name. Refer to **CASG Reports - an Overview** for more details.
- **Regenerate password** - Click this button to reset the password for the administrator in case it is forgotten. The new password will be 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.

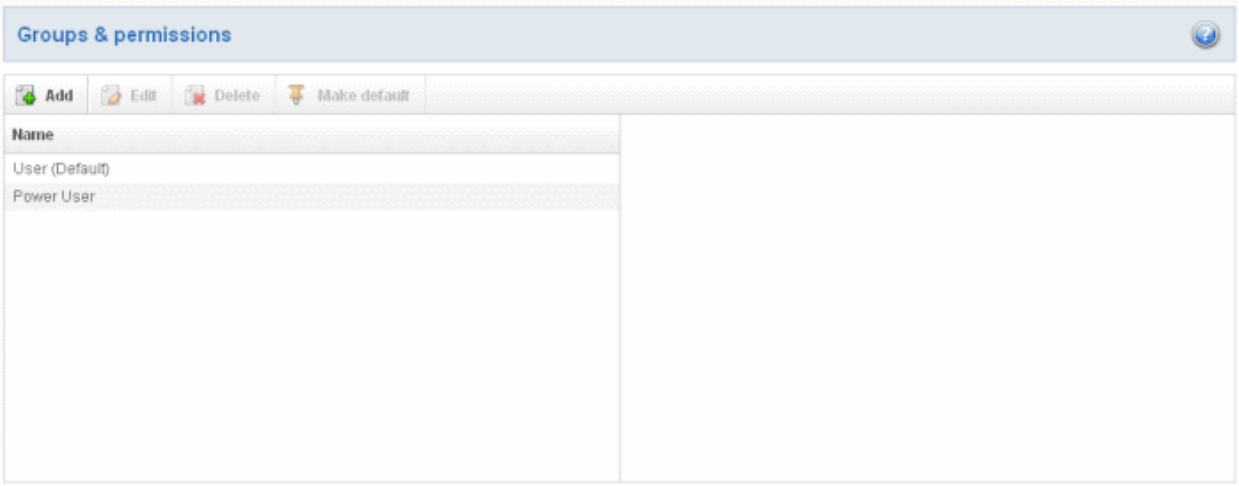
3.2.2.2 Groups & Permissions

The Groups & Permissions interface allows the administrators to create email user groups according to the needs of the organization. Each group can be configured with different permission levels. This simplifies the process of configuring permission levels for each user meaning new or existing users belonging to all domains for the account can be simply assigned a group with a preset policy. See the section '**Managing Permissions**' in '**User Account Management**' on how to add users to predefined groups.

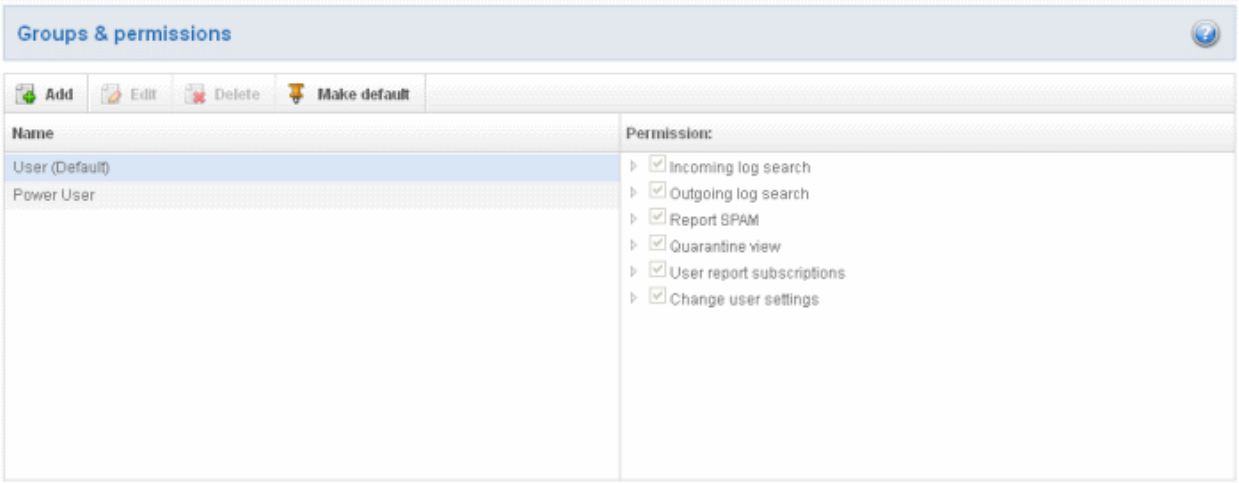
To create groups

- Click 'Groups & permissions' from the 'Account management' drop-down menu in the menu bar or the icon in the 'Account management' configuration area

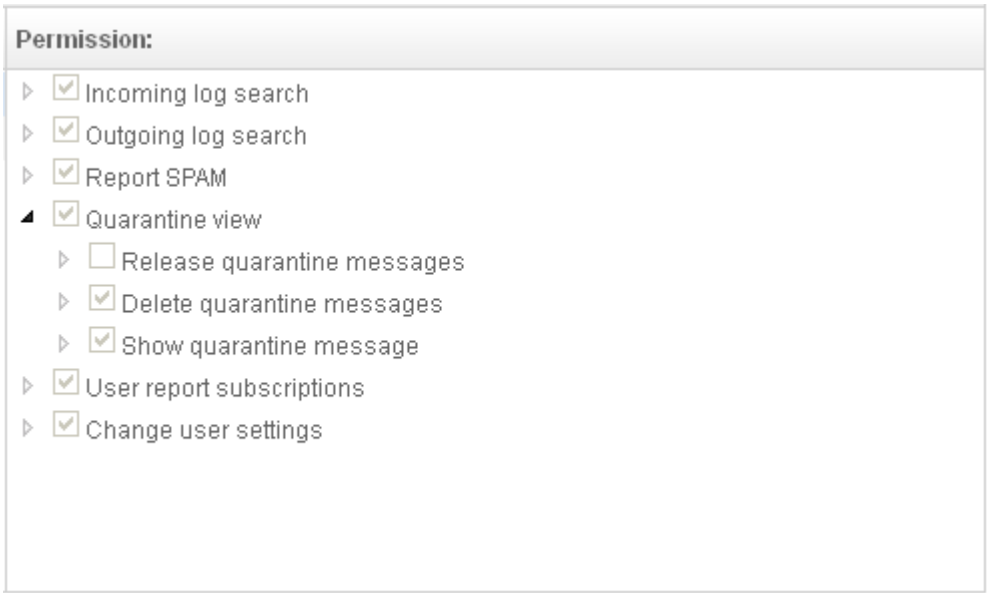
The 'Groups & permissions' interface will open.



By default, two user groups, User (Default) and Power User, will be available. These two groups cannot be either edited nor deleted. Clicking any one of them will display the permission levels assigned for the group in the right side.



Clicking on the arrow beside a permission will display the tree structure of second level of permissions, if available.



For users in the 'Power User' group, all permission levels will be enabled. The 'Release quarantine messages' option will not be 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 the administrator. See the section Released

Requests in 'Email Management' for more details.

Permission Levels

- **Incoming log search** - Allows an user to view the log of all incoming mails.
- **Outgoing log search** - Allows an user to view the log of all outgoing mails.
- **Report SPAM** - Allows an user to report a mail as spam mail.
- **Quarantine view**
  - **Release quarantine messages** - Allows an user to release a quarantined mail without approval from the administrator.
  - **Delete quarantine messages** - Allows an user to delete quarantined messages.
  - **Show quarantine messages** - Allows an user to view quarantined emails in same window or separate window.
- **User report subscriptions** - Allows an user to configure periodical quarantine report generation.
- **Change user settings** - Allows an user to configure himself / herself as recipient whitelist.

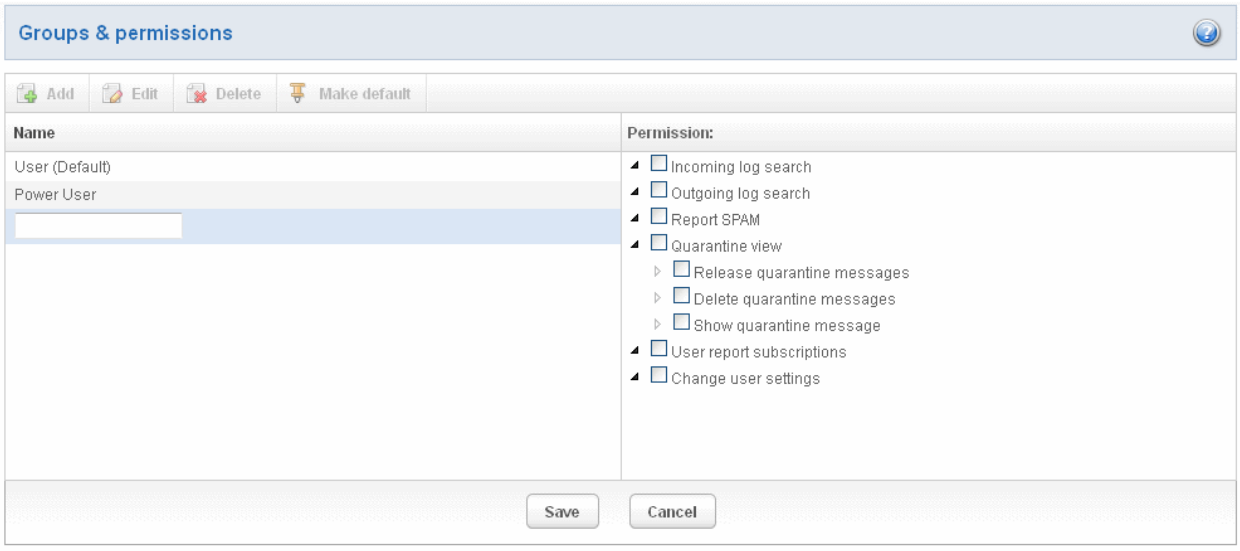
Click the following links for more details.

- Adding a new group
- Editing a group
- Deleting a group
- Making a group as default

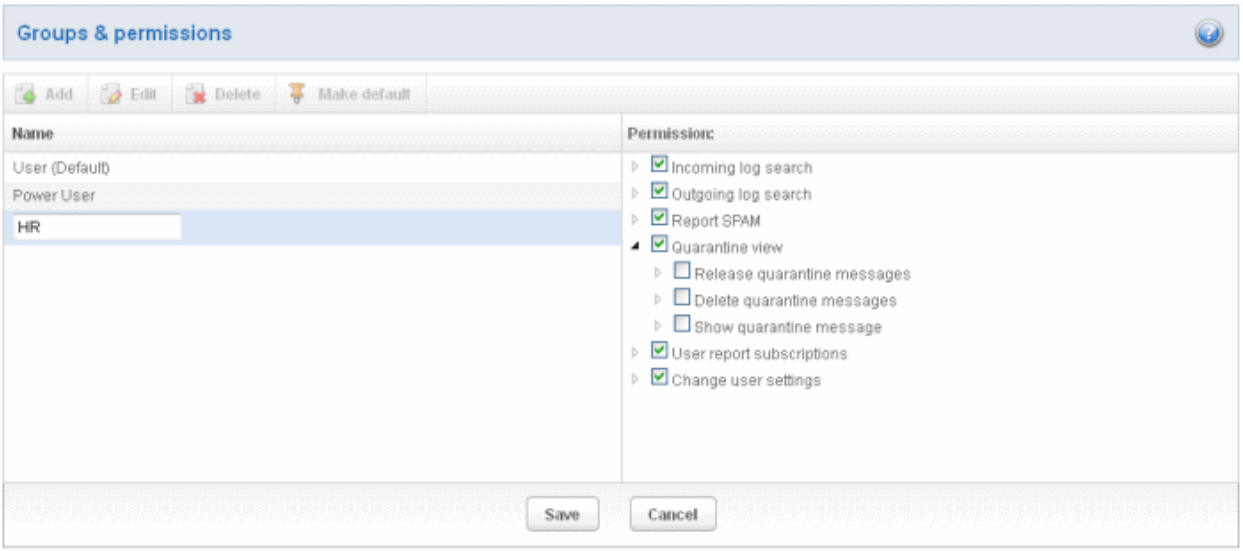
Adding a New Group

- To add a new group and configure permission levels, click the 'Add' button.

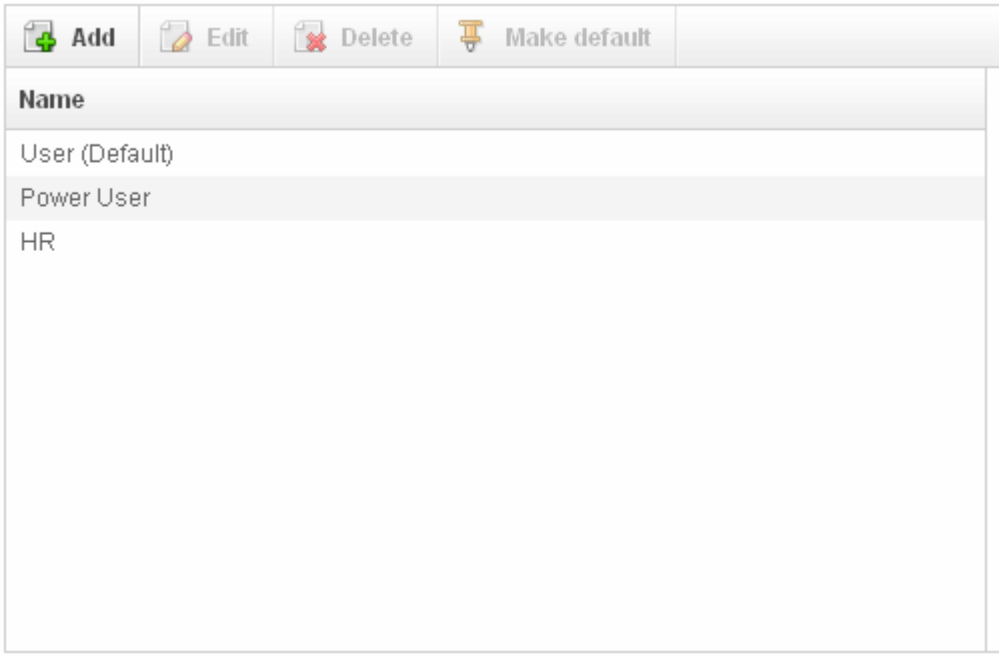
- Enter the name of the group in the text field under the 'Name' column and enable the permission levels in the right side required for that group.



- Click the 'Save' button.



The newly created group will be displayed in the interface.

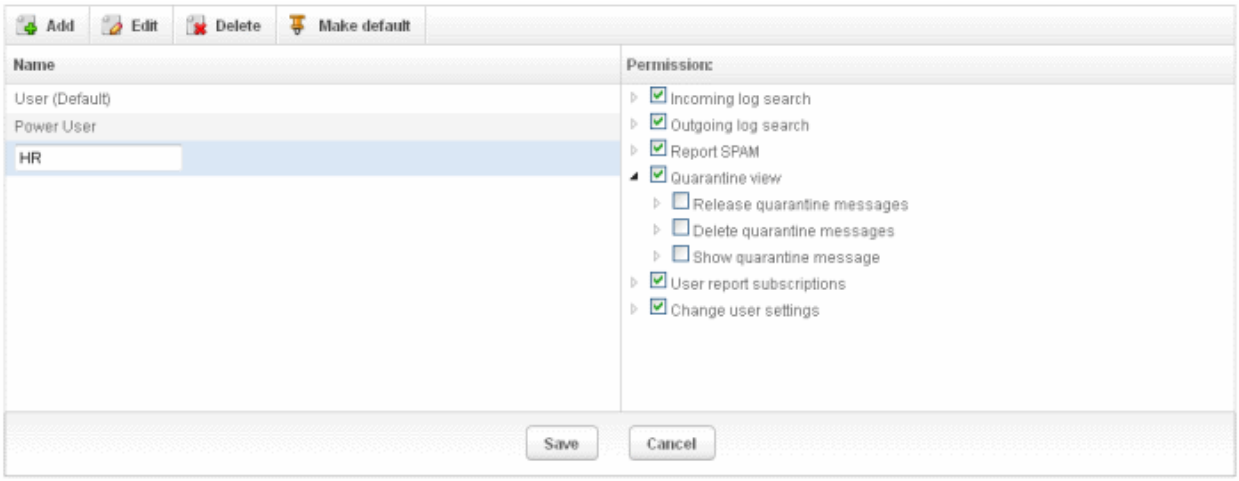


Now, users of domains belonging to the account can be assigned this newly created group. See the section '**Managing Permissions**' in '**User Account Management**' on how to add users to predefined groups.

Editing a Group

You can edit the name of an existing group and / or change the permission levels.

- To edit an existing group, select the group from the list and click the 'Edit' button.



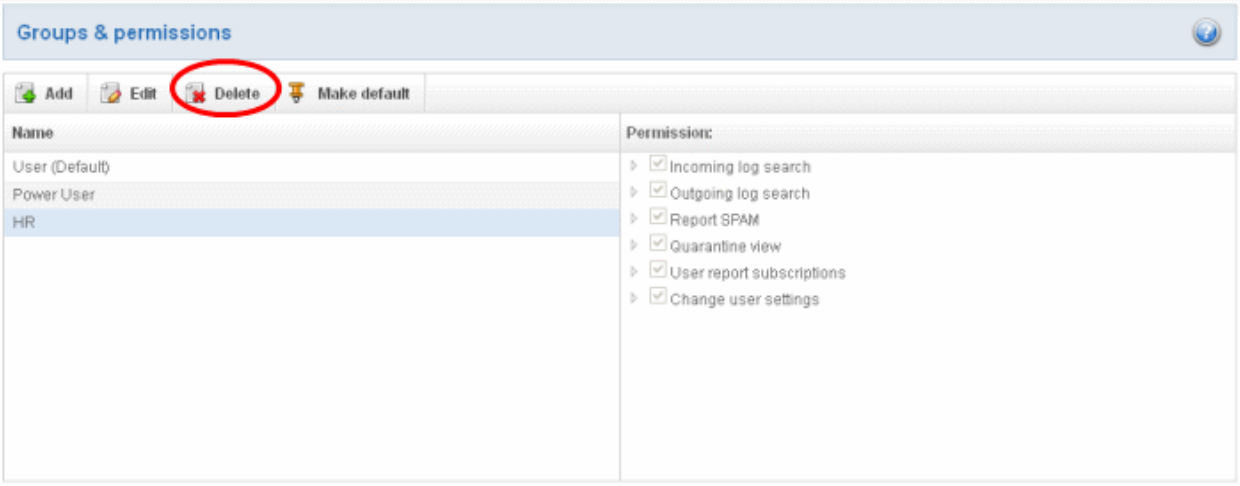
- Change the permission levels and / or the name of the group.

Note: If you change the name of a group, users assigned to that group will be automatically moved to default group. You have to reassign the users.

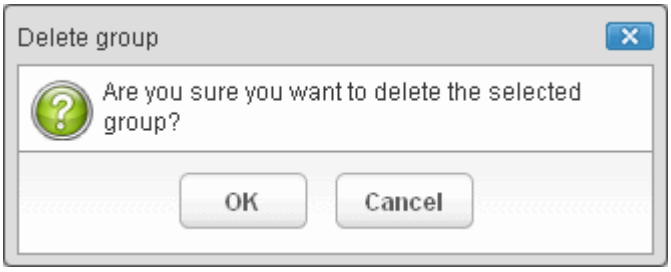
- Click the 'Save' button for the changes to take effect.

Deleting a Group

- To delete a group, select it from the list and click the 'Delete' button.



- Click 'OK' in the confirmation dialog.



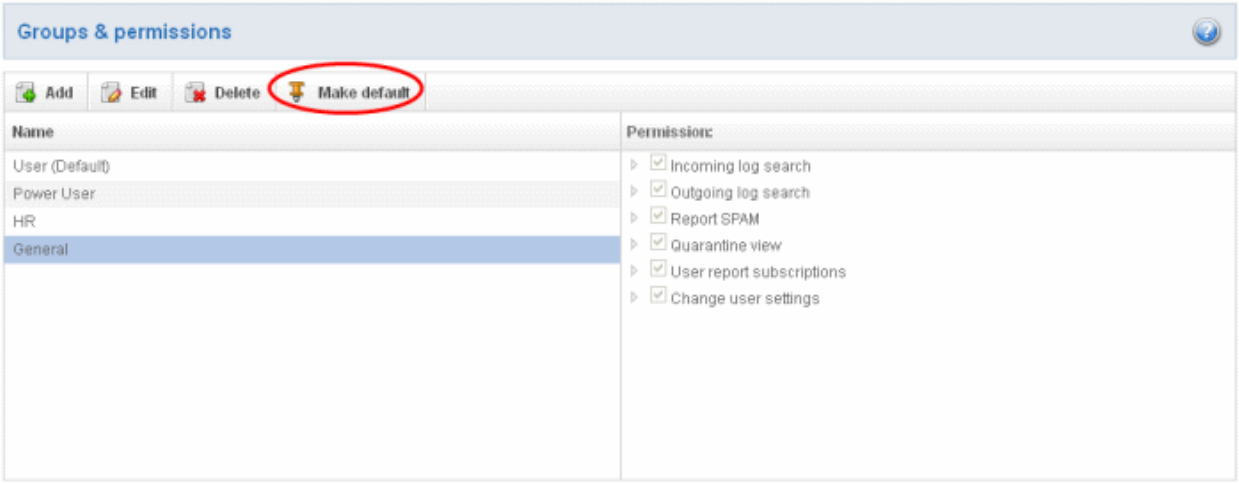
The selected group will be deleted from the list.

Note: If you delete a group, users assigned to that group will be automatically moved to default group. You have to reassign the users.

Making 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 edited or deleted will be automatically moved to this default group.

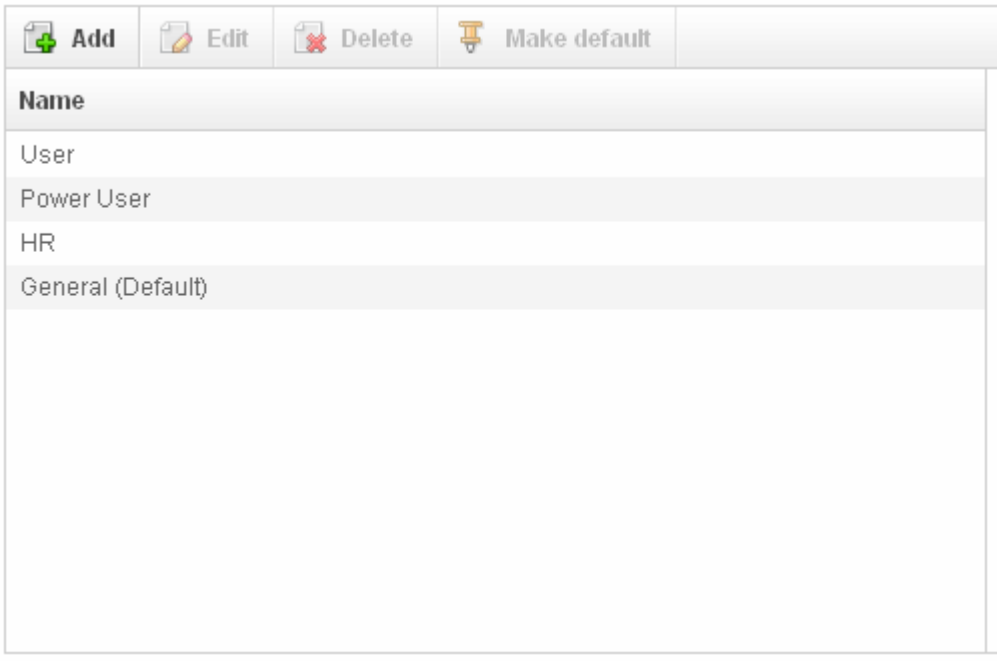
- To make an existing group as a default group, select it from the list and click the 'Make default' button.



A success dialog will be displayed.

- Click 'OK'.

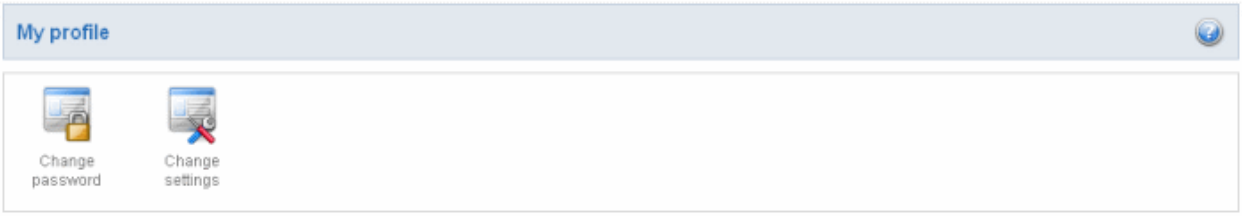
The selected group will be displayed as default group.



3.2.2.3 My Profile

The My Profile interface allows the currently logged-in administrator to change his / her login password to CASG as well as to change settings for idle session timeout and enabling / disabling subscription for the periodical domain and quarantine summary reports. Refer to **CASG Reports - An Overview** for more details.

- To access the My Profile interface, click 'My Profile' icon from the 'Account management' configuration area of the Dashboard or click 'My Profile' in the Account Management drop-down menu from the menu bar.



Click the following links for more details:

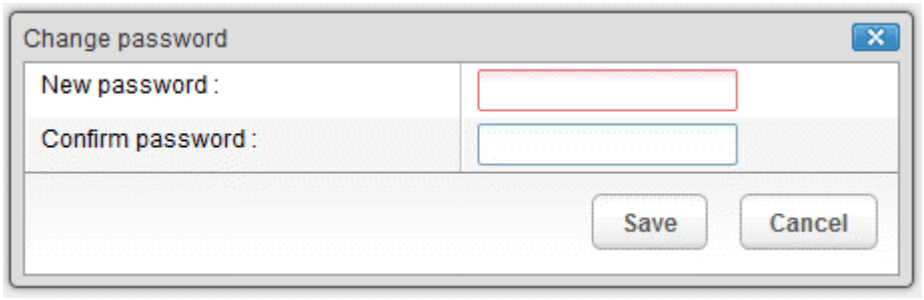
- **Changing Administrator's password**
- **Changing settings for idle session timeout and subcriptions for global summary reports**

3.2.2.3.1 Changing Password of the Administrator

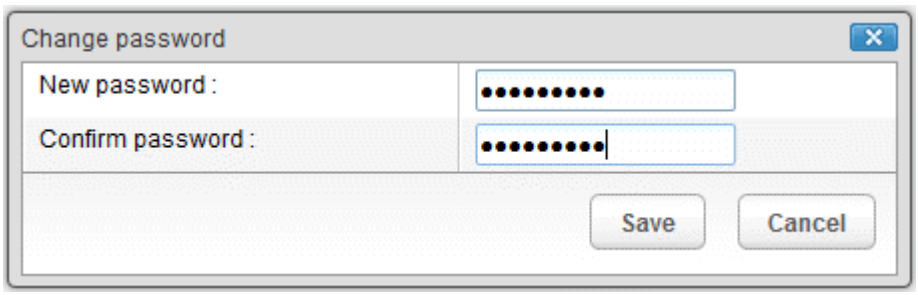
The Change Password allows the currently logged-in administrator to change his/her login password.

To change the password

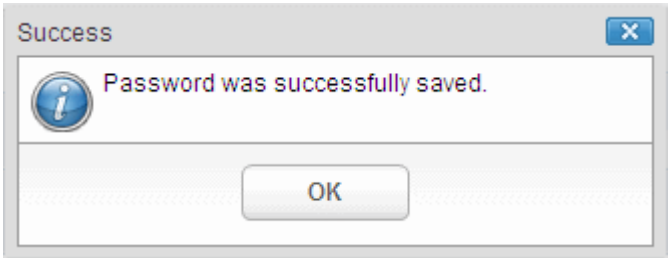
- Click the 'Change password' icon from the My Profile area. The Change Password dialog will be displayed.



- Enter the new password and confirm it in the respective text boxes.



- Click the 'Save' button.



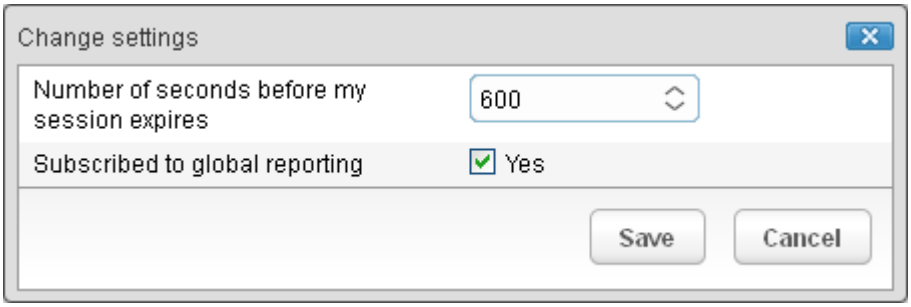
The administrator has to use the new password to login into the CASG interface.

3.2.2.3.2 Change Settings

The 'Change settings' interface allows the currently logged-in administrator to set his / her idle session timeout period as well as to enable / disable subscription for periodical domain and quarantine summary reports for all the domains in the account. Refer to CASG Reports - an Overview for more details.

To set idle session timeout and global report subscription status

- Click the 'Change settings' icon from the My Profile area. The 'Change settings' dialog will be displayed.



- **Number of seconds before my session expires** - You can set the idle session timeout period in the box. Enter the period in seconds or increase / decrease the period by clicking the up / down arrow. The valid entry is between 1 minute and 120 minutes. Please note this feature will not be available if an administrator is logged into CASG using CAM credentials.
- **Subscribed to global reporting** - Enable this check box to receive the periodical Domain Summary Report and the Quarantine Summary Report for all the domains in the account. Else deselect the check box. This can also be done in the Edit dialog in the Administrators interface.
- Click Save for your changes to take effect.

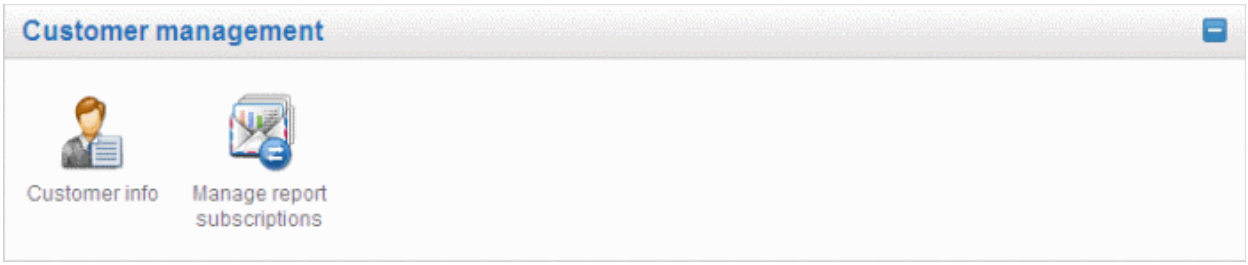
3.2.2.4 User History

The 'User History' area in 'Administrator Account Management' allows the administrators to view user history for *all* domains within a particular date range. You can filter users by IP address, last login, Domain or User name. By default, the most recent 15 records will be displayed.

Use of filters to create custom searches is covered in more detail here.

3.2.3 Customer Management

The Customer Management area of CASG allows an administrator to view the details of the account they are logged into. You can configure subscriptions for the periodical Domain and Quarantine summary reports for domains; create an account; update the product and extend your license term.



Click the links for more details:

- Viewing Customer Information
- Managing subscriptions for reports

3.2.3.1 Viewing Customer Information

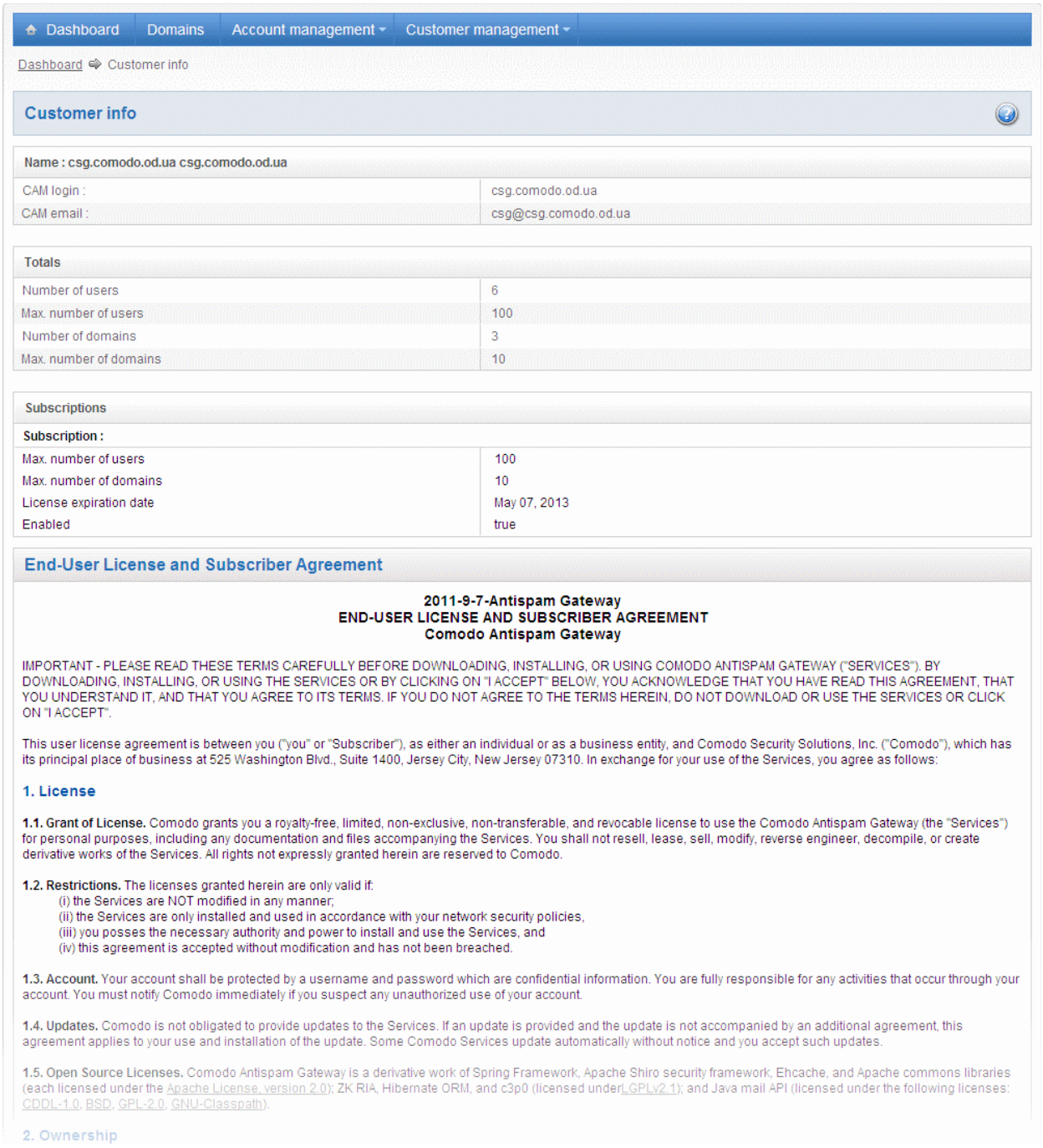
The Customer Info interface accessible from the 'Customer management' configuration area of the dashboard provides the administrator with the details like maximum number of users, domains, license term and so on of the CASG account.

To view the account Information

- Click Customer Info icon from the 'Customer management' configuration area or click 'Customer Info' from the 'Customer management' drop-down menu in the menu bar.

The 'Customer Info' interface will be displayed:

The image below shows an example of Customer Info who has purchased multiple licenses.



In the 'Customer Info' panel you will find the details of subscription(s) for your account. For multiple licenses, the number of users and domains that are allowed for all the licenses purchased will be added and displayed at the bottom most subscription column.

- **Name:** Displays the name of the account.
- **CAM Login**: Displays the login user name for the account in Comodo Accounts Manager (CAM) at https://accounts.comodo.com. The administrator can use this login username to log in to CAM for purchasing additional licenses and renewal of existing licenses.
- **CAM email**: Displays the email address for the account as registered at CAM.

Account Summary

- **Number of Users**: Displays the number of users for all the domains belonging to the account.
- **Max. Number of Users:** The maximum number of users that can be added as per all the subscriptions made for the account, that is, number of users cannot exceed the number given in this field for all domains included.
- **Number of Domains:** Displays the number of domains belonging to that account.

- **Max. Number of Domains:** The maximum number of domains that can be configured as per all the subscriptions made for the account.

Details on Subscriptions

- **Max. Number of Users**: The maximum number of users that can be added for the account as per the specific subscription, that is, number of users cannot exceed the number given in this field for all domains included.
- **Max. Number of Domains**: The maximum number of domains that can be configured as per the specific subscription.
- **License Expiration Date:** Provides details about the expiry date of the license for the specific subscription.
- **Enabled:** Displays whether the subscription is active or not.

End-User License and Subscriber Agreement

- **End-User License and Subscriber Agreement:** Displays the complete End-User License and Subscriber Agreement.

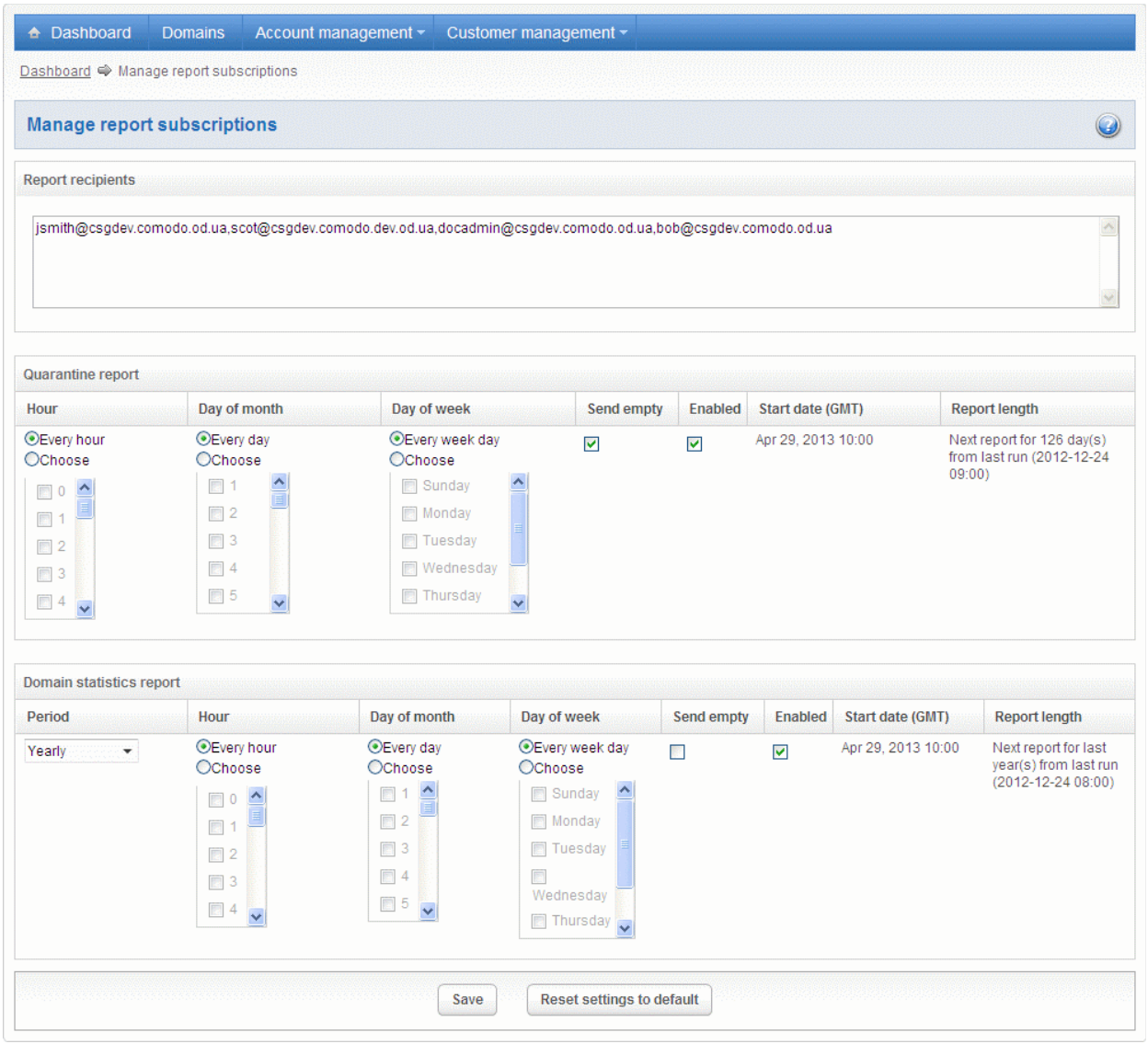
3.2.3.2 Managing Subscriptions for Reports

The Manage report subscriptions interface accessible from the 'Customer management' configuration area of the dashboard allows the administrator to configure the subscription to the periodical Domain and Quarantine summary reports of all domains for the administrators enrolled for the account. Refer to CASG Reports - an Overview for more details.

To access Manage report subscriptions interface

- Click Manage report subscriptions icon from the 'Customer management' configuration area or click 'Manage report subscriptions' from the 'Customer management' drop-down menu in the menu bar.

The 'Manage report subscriptions' interface will be displayed:



The 'Report recipients' field will be auto-populated with all the administrators available for the account.

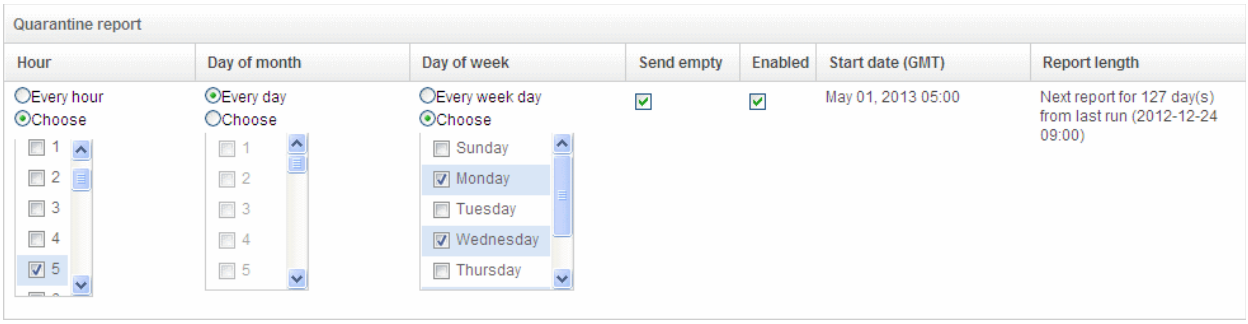
The administrator can configure the subscription for two types of reports from this interface:

- **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. Refer to 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. Refer to CASG Reports - An Overview for more details.

To configure the subscription of the reports

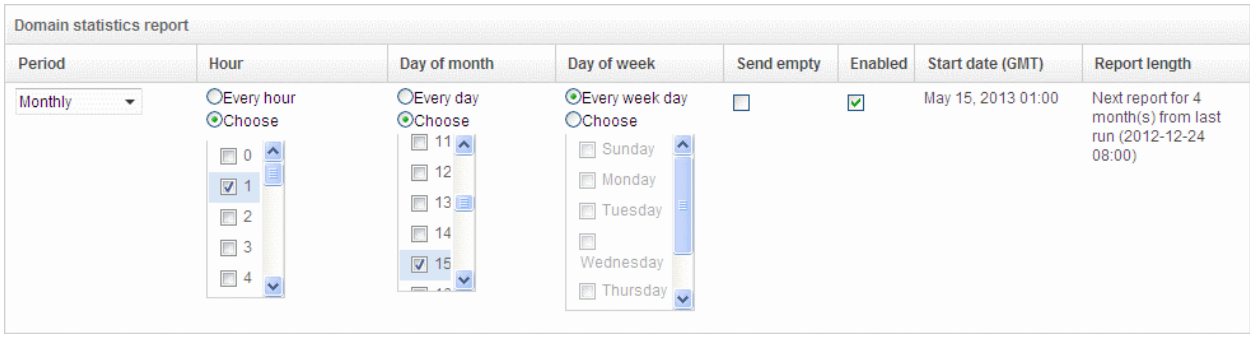
- If you want the administrators of the account to receive the periodical reports, select the 'Enabled' checkbox in the row of the respective report type. If both the reports are required, you can select both the checkboxes.
- Leave the 'Send empty' checkbox unchecked if empty reports are not to be sent to recipients.
- Select the frequency of the report to be sent to the administrators from the options for Quarantine Report and Domain Statistics Report.

Quarantine Report



- **Hour** - The reports will be generated and sent to the administrators 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 will be generated and sent to the administrators every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports will be generated and sent to the administrators 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 will be generated depending on the options chosen.

Domain Statistics Report



- **Period** - Enables you to set the period to be covered in the report. The report will 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 will be generated and sent to the administrators 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 will be generated and sent to the administrators every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports will be generated and sent to the administrators 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 will be generated depending on the options chosen.

Click 'Save' for your settings to take effect.

Clicking the 'Reset settings to default' button will disable both Quarantine and Domain statistics reports. The 'Report Recipients' field will not be cleared.

4 CASG Reports - An Overview

Comodo Antispam Gateway can periodically generate quarantine and domain reports that are sent to administrators and users. CASG generates two types of report – a global report for all domains belonging to the account and anther specific for a domain. See the section '**Managing Subscriptions for Reports**' in '**Customer Management**' for more details on customer level global reports and '**Manage Report Subscriptions for Selected Domain**' in '**Incoming**' section for reports on domain levels. The reports for these types will be similar except the former will contain reports for all domains while the latter will contain reports for the selected domain. The reports will be sent routinely at the times selected in the language set for the account.

CASG can provide two types of reports:

- **Quarantine Report** - A statistical breakdown of mails identified as spam or malicious that were moved to quarantine by CASG. The report can be configured to be received hourly, daily, weekly or monthly.
- **Domain Statistics Report** - A comprehensive report which covers all mail activity for 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 or monthly by the administrator.
- By default, global reports are enabled for new administrators. Reports can be enabled or disabled per administrator in **Dashboard** > **Account Management** > **Admin** > **Add Administrators** or **Edit Administrators**.

4.1 Quarantine Report

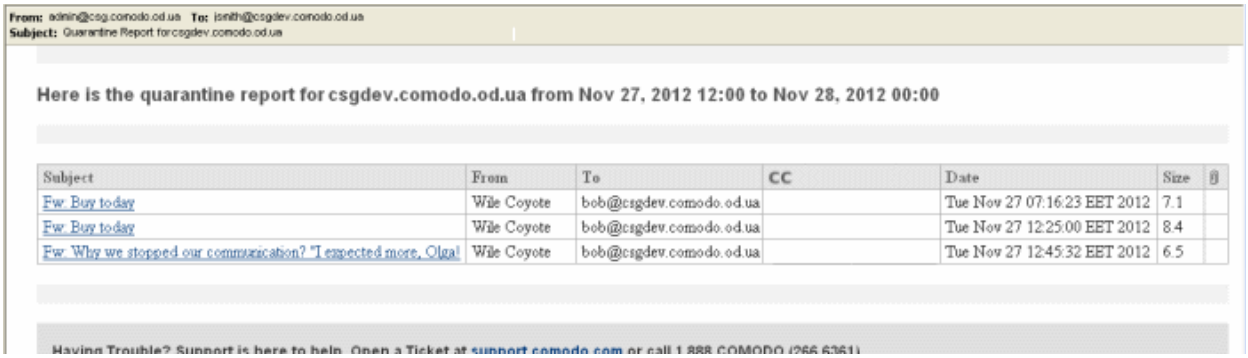
The Quarantine Report contains a list of mails that were identified as spam or containing malicious content and were moved to Quarantine automatically by CASG, with the details on sender, receiver, date and attachments. Clicking the subject line in the list will open the respective mail in a new CASG window.

- **Administrator**
  - **Domain Level** - The Report generated for an administrator will contain the details of the mails moved to quarantine of the selected domain.
  - **Customer Level** - The Report generated for an administrator will contain the details of the mails moved to quarantine of all the domains belonging to the account.
- **User** - The Report generated for a user will contain 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 an user.

- **Hourly** - The reports will be generated and sent every hour to the administrators through email.
- **Daily** -The reports will be generated and sent daily to the administrators/user through email.
- **Weekly** - The reports will be 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 will contain details of the mails quarantined during the past seven days. The first report will be sent on the start date and will contain the statistics for the remaining days of the week from the day of configuration and subsequently every seven days.
- **Monthly** - The reports will be 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 will contain details of the mails quarantined during the past 30 days. The first report will be sent on the start date and will contain 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:


From: admin@csg.comodo.od.ua To: jsmith@csgdev.comodo.od.ua
Subject: Quarantine Report for csgdev.comodo.od.ua

Here is the quarantine report for csgdev.comodo.od.ua from Nov 27, 2012 12:00 to Nov 28, 2012 00:00

Subject	From	To	CC	Date	Size	
Fw: Buy today	Wile Coyote	bob@csgdev.comodo.od.ua		Tue Nov 27 07:16:23 EET 2012	7.1	
Fw: Buy today	Wile Coyote	bob@csgdev.comodo.od.ua		Tue Nov 27 12:25:00 EET 2012	8.4	
Fw: Why we stopped our communication? "I expected more, Olga!	Wile Coyote	bob@csgdev.comodo.od.ua		Tue Nov 27 12:45:32 EET 2012	6.5	

Having Trouble? Support is here to help. Open a Ticket at support.comodo.com or call 1.888.COMODO (266.6361)

- Clicking on the 'Subject' link will open the respective mail in a new CASG window. You need to login to CASG to read the mail in the new window.

4.2 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.

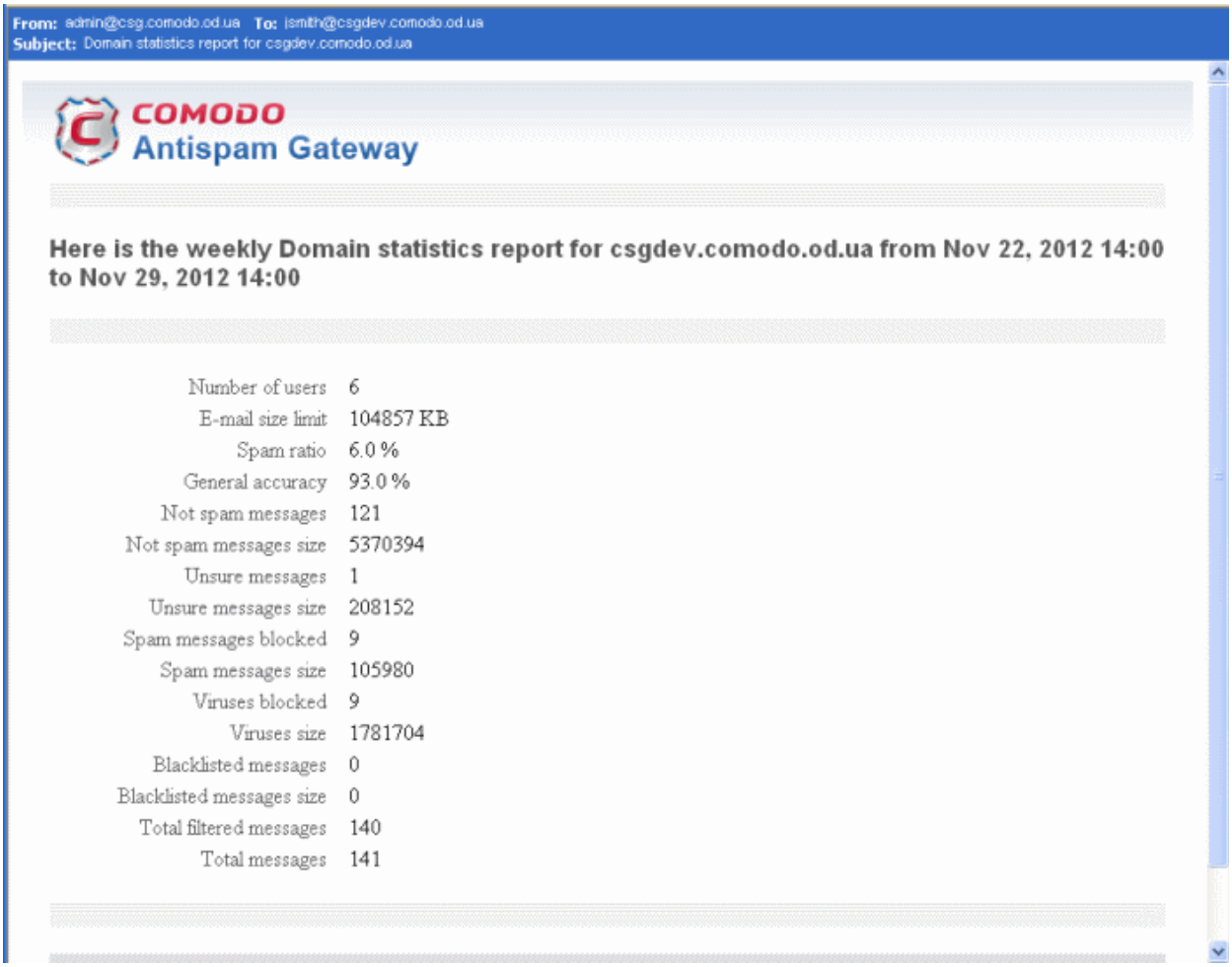
- **Domain Level** - The Report generated for an administrator will contain only the details of domain statistics of the selected domain.
- **Customer Level** - The Report generated for an administrator will contain the details of domain statistics of all the domains belonging to the account.

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** - The reports will be generated and sent every hour to the administrators through email.
- **Daily** -The reports will be generated and sent daily to the administrators through email.
- **Weekly** - The reports will be generated and sent to the administrators through email on every seventh day from the start date set in the 'Start date' field. The report will contain details of the mail activities for the domains during the past seven days. The first report will be sent on the start date and will contain the statistics for the remaining days of the week from the day of configuration and subsequently every seven days.
- **Monthly** - The reports will be generated and sent to the administrators through email on every 30th day from the start date set in the 'Start date' field. The report will contain details of the mail activities for the domains during the past 30 days. The first report will be sent on the start date and will contain the statistics for the remaining days of the month from the day of configuration and subsequently every 30 days.
- **Yearly** - The reports will be generated and sent to the administrators through email on every 365th day from the start date set in the 'Start date' field. The report will contain details of the mail activities for the domains during the past 12 months. The first report will be 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 Domain Statistics Report is shown below:


From: admin@csg.comodo.od.ua To: jsmith@csgdev.comodo.od.ua
Subject: Domain statistics report for csgdev.comodo.od.ua
COMODO
Antispam Gateway
Here is the weekly Domain statistics report for csgdev.comodo.od.ua from Nov 22, 2012 14:00 to Nov 29, 2012 14:00
Number of users 6
E-mail size limit 104857 KB
Spam ratio 6.0 %
General accuracy 93.0 %
Not spam messages 121
Not spam messages size 5370394
Unsure messages 1
Unsure messages size 208152
Spam messages blocked 9
Spam messages size 105980
Viruses blocked 9
Viruses size 1781704
Blacklisted messages 0
Blacklisted messages size 0
Total filtered messages 140
Total messages 141

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

About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

Comodo Security Solutions, Inc.

1255 Broad Street

STE 100

Clifton, NJ, 07013

United States

Tel: +1.888.256.2608

Tel: +1.703.637.9361

Email: EnterpriseSolutions@Comodo.com

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