# Table of Contents

1 Introduction to Comodo Dome Antispam - MSP ................................................................. 4  
  1.1 Purchasing License .................................................................................................. 5  
  1.2 Add More Users, Domains or Time to your Account .............................................. 16  
  1.3 License Information .............................................................................................. 20  

2 Getting Started ............................................................................................................ 23  
  2.1 Incoming Filtering Configuration ............................................................................. 23  
  2.1.1 Configure Your Mail Server ................................................................................ 24  
  2.1.2 Configure MX Record ......................................................................................... 24  
  2.1.2.1 Update MX Records in Windows 2003/2008 Server ....................................... 25  
  2.1.2.2 Update MX Records on a host using BIND (and the 'named' daemon) ............... 25  
  2.1.2.3 Update MX Records for Comodo DNS ............................................................ 26  
  2.1.2.4 Update MX Records for GoDaddy ................................................................. 29  
  2.1.2.5 Update MX Records for Enom ................................................................. 30  
  2.1.2.6 Update MX Records for Network Solutions .................................................. 31  
  2.1.2.7 Update MX Records for Yahoo! Small Business .......................................... 32  
  2.1.2.8 Update MX Records for 1and1 ................................................................. 33  
  2.1.2.9 Update MX Records for 4D Web Hosting .................................................... 33  
  2.1.2.10 Update MX Records for DNS Park ............................................................ 34  
  2.1.2.11 Update MX Records for DreamHost ......................................................... 34  
  2.1.2.12 Update MX Records for DynDNS ............................................................ 35  
  2.1.2.13 Update MX Records for IX Web Hosting .................................................. 35  
  2.1.2.14 Update MX Records for No-IP ................................................................. 36  
  2.1.2.15 Update MX Records in CPanel .............................................................. 37  

2.2 Outgoing Filtering Configuration .............................................................................. 39  
  2.2.1 Per-User Authentication ....................................................................................... 40  
  2.2.2 Outgoing Smarthost setup .................................................................................. 40  
  2.2.2.1 Configure QMail to use a Smarthost .............................................................. 41  
  2.2.2.2 Configure Postfix to use a Smarthost ............................................................. 41  
  2.2.2.3 Configure Sendmail to use a Smarthost ........................................................ 42  
  2.2.2.4 Configure Exchange 2000/2003 to use a Smarthost ..................................... 42  
  2.2.2.5 Configure Exchange 2007/2010 to use a Smarthost ..................................... 43  
  2.2.2.6 Configure Exchange 2013/2016 to use a Smarthost ..................................... 44  
  2.2.2.7 Configure Exim to use a Smarthost ............................................................ 44  
     2.2.2.7.1 Configure Exim / CPanel to use a Smarthost ........................................... 45  
     2.2.2.7.2 Configure Exim / Directadmin to use a Smarthost .................................... 47  

3 The Admin Console ..................................................................................................... 48  
  3.1 Log in to the Admin Console .................................................................................. 49  
  3.2 The Dashboard Area .............................................................................................. 50  
  3.2.1 Domain Management ......................................................................................... 52  
     3.2.1.1 Domains ..................................................................................................... 52  
     3.2.1.1.1 Add a Domain ....................................................................................... 54  
     3.2.1.1.2 Deleting Domains .................................................................................. 58
1 Introduction to Comodo Dome Antispam - MSP

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

Features and benefits include:

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

Guide Structure

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

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

## 1.1 Purchasing License

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

You can purchase the license(s) in two ways:

- **Through Comodo Accounts Manager**
- **Through Comodo One - MSP interface**

**Comodo Accounts Manager**

- Click the 'Buy Now' link on the website or directly visit
  https://accounts.comodo.com/spamgateway/management/signup
Select 'Dome Antispam' product and subscription term

Select the subscription package you want from the list. You have the option to purchase a 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 domain. For example, you can configure xyz.com, abc.xyz.com, abc.org along with a total number of licensed users across all your domains.

Select the number of additional domains/users to be covered and archive space requirements

Select your region

Enter your contact details and billing address details under 'Customer Information'
If you already have a Comodo account, select ‘Existing Comodo User’ and enter your username and password

If you don't have a Comodo account, select ‘New Comodo User’ and enter your details to create a new account

Complete the payment details section
Select the checkbox under Communication Options if you want to subscribe for newsletters from Comodo.
Read the 'End User License/Subscriber Agreement' and tick the checkbox to agree.

Click 'Continue'. After your order has been successfully processed, you will see the following order confirmation screen:

- Click 'Place Order'
Your account will be created and your licenses are now active. You will also receive a confirmation email with your order details.

You can login to CDAS - MSP through the URL contained in the confirmation mail.

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

The number of users and domains allowed by all your licenses combined is shown in the Customer Info page.

**Comodo One - MSP interface**

- Login to your Comodo One - MSP account and click 'Store'
Click 'Get Module' in the Comodo Dome Antispam tile

You will be taken to the subscription page.

Your login username will be pre-populated and cannot be changed.

Enter your Comodo One account password in the 'Password' field and click 'Login'
Any licenses you have already purchased will be listed in the next step.

- Click 'Buy Now' to subscribe for a new license

**Select the license type:**

- **Single Domain License** - One email domain. For example, xyz.com or abc.xyz.com, can be configured. You can also select how many users you want to license.
- **Multi-Domain License** - More than one email domain. For example, you can configure xyz.com, abc.org, abc.xyz.com etc. You can also select how many users you want to license.

**Select the license term**

- Click 'Next'
Enter your contact details and billing address details under 'Customer Information'.

Click the 'End User License/Service Agreement' link to read the EULA for Dome Antispam. Accept the agreement by selecting the checkbox.

Click 'Next'

The next step allows you to enter your payment card information.
Enter your credit card/debit card details and click 'Next'.

The 'Order Confirmation' screen will be displayed:

- Review your order and click 'Next'

Your order summary will be displayed.
Click 'Next' to view your license details.

Instructions

You've successfully purchased subscription shown below:

Dome Antispam

Comodo Dome Support Team is currently in progress of provisioning your Dome Antispam instance. This operation may take at least 2 business days to finalize.

Once provisioning is complete, you will receive your Dome Antispam Service URL from Comodo Dome Support Team via an e-mail. Please put that URL into the popup that appears once you click Dome Antispam Module under Licensed Applications.

For questions and assistance please contact:

domesupport@comodo.com

Thank you being part of the community.
The Comodo One Team

Click 'Finish'
You can login to CDAS - MSP from the Comodo One console by selecting 'Applications' > 'Dome Antispam'.

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

The number of users and domains allowed by all your licenses combined is shown in the Customer Info page.

### 1.2 Add More Users, Domains or Time to your Account

Visit [https://accounts.comodo.com/spamgateway/management/signup](https://accounts.comodo.com/spamgateway/management/signup)

Please read on for a step-by-step guide to this process.

1. **License Selection**
2. **Confirmation**
3. **Order Summary**

**Comodo Sign-Up Page**

- Please select currency that will be used for purchase (note that not all products can be available in currencies other than US Dollar)
- Select 'Dome Antispam' product and subscription term
- To add additional domains, users and/or archive space, choose your requirements from the respective drop-downs without selecting a base package.
- Select the region in which you want to use the license (choose the region closest to your company network). If you choose EU, your service will use our EU servers. If you choose US, your service will use our US servers.
- Enter your contact details and billing address details under 'Customer Information'
### Customer Information (an * indicates required fields)

#### User Details
- **Are you an existing Comodo customer?**
  - Yes
  - No
- **Email**
- **Password**
  (8 characters min.)
- **Password Confirmation**
- **First Name**
- **Last Name**
- **Telephone Number**

#### Contact Information
- **Company Name**
- **Company Website**
- **Street Address**
- **Address2**
- **City**
- **Country**
  - United States
- **State or Province**
  - Unknown
- **Postal Code**
- **Billing Email (non required)**

#### Billing Information
- The same as Contact Information

- Select ‘Existing Comodo User’ and enter your username and password

**Note:** Fields marked with * are mandatory.

- Select your payment method and complete the required payment fields:
If you want to be kept informed about Comodo products and updates, select the 'Communication Options' checkbox:

**Communication Options**

- Yes! Please keep me informed about Comodo products, upgrades, special offers and pricing via email. Your information is safe with us!

**Terms and Conditions**

END-USER LICENSE AND SUBSCRIBER AGREEMENT

Comodo Antispam Gateway

IMPORTANT – PLEASE READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING, OR USING COMODO ANTISPAM GATEWAY ("SERVICES"). BY DOWNLOADING, INSTALLING, OR USING THE SERVICES OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT DOWNLOAD OR USE THE SERVICES OR CLICK ON "I ACCEPT".

This user license agreement is between you ("you" or "Subscriber"), as either an individual or an entity, and Comodo Security Solutions Inc. ("Comodo").
• Read the 'End User License/Subscriber Agreement' and tick the checkbox to agree
• Click 'Continue'. After your order has been successfully processed, you will see the following order confirmation screen:

Your order summary will be displayed.
• Your account will be created and your licenses are now active. You will also receive a confirmation email with your order details.

• You can login to CDAS - MSP through the URL contained in the confirmation mail.

• You can view your license details in the main interface after activation. See ‘License Information’ for more information.

• The number of users and domains allowed by all your licenses combined is shown in the Customer Info page.

### 1.3 License Information

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

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

- Log in to Comodo Dome Antispam - MSP
- Click 'License Management' from the 'Customer management' drop-down menu on the left
The image below shows an example of a customer who has purchased multiple licenses:

- The 'License Management' panel shows details about your CDAS subscription(s).
- 'Max. number of users' shows the total number of users allowed by all licenses combined.
- 'Max. number of domains' shows the total number of domains allowed by all licenses combined.

**Name**
- The name of the account is displayed in the title bar.
- **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.

**Totals**
- **Number of users**: The total number of enrolled users belonging to all the domains.
- **Max. number of users**: The total 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**: The number of domains enrolled for account.
- **Max. number of domains**: The total number of domains that can be added as per all the subscriptions made for the account.
- **Disk quota**: Displays the total storage space allotted in CDAS server for archiving incoming messages as per all the subscribed packages, in GB.
- **Disk space**: Displays the storage space used by the archived mails in the CDAS server.

**Subscriptions**
The following details are displayed for each subscription:
- **Max. number of users**: The maximum number of users that can be added to the account as per the 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 added as per the subscription.
• **License expiration date**: The date till which the license is valid for the subscription.

• **Disk quota**: The maximum storage space allotted for mail archive in the CDAS server, as per the subscription.

• **Enabled**: Displays whether the subscription is active or not.

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

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

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

An example of license renewal reminder is shown below:

**Dear Customer,**

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

Please renew your subscription using your account page or contact support.

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

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

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

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

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

Administrators can upgrade or downgrade his/her account using Comodo Accounts Manager (CAM) at [https://accounts.comodo.com/account/login](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 CDAS.

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 CDAS interface. Some examples of alert messages are shown below:

• When the domain limit is exceeded:

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

You will not be able to add new domains until some of the current domains are removed. CDAS filter will continue to...
function and you can add new users.
  • When the user limit is exceeded:

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

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

## 2 Getting Started

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

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

**European Union**
- mxpool1.spamgateway.comodo.com
- mxpool2.spamgateway.comodo.com

**United States**
- mxpool1.us.spamgateway.comodo.com

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

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

### 2.1 Incoming Filtering Configuration

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

- **Configure your mail server**
- **Configure MX record**

#### 2.1.1 Configure Your Mail Server

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

If the above step is not carried out, the following error message may appear while adding a domain.
Step 2: Add your domain to CDAS service.
To add domain:
- Login to CDAS system, go to domain management and add domain.

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

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

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

This section explains how to update your MX records so that all mails to/from your domain are passed through the CDAS 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
2.1.2.1 Update MX Records in Windows 2003/2008 Server

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

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

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

   Click OK to save your record.

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

   EU: mxpool2.spamgateway.comodo.com

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

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

   Click 'OK' to save your record.

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

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

1. Make a backup copy of the zone file (or named.conf) that you intend to edit for MX record updates.
2. Open the Zone file for the mail domain you are configuring (or go to the part of named.conf being used for that zone)

3. Delete all the existing "MX" lines for that domain.

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

   CDAS primary service domains are:
   EU: mxpool1.spamgateway.comodo.com
   US: mxpool1.us.spamgateway.comodo.com

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

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

   CDAS secondary service domains are:
   EU: mxpool2.spamgateway.comodo.com
   Please note there is no secondary service domain for the US based service. Leave it blank.

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

6. Find the "@ IN SOA" record and increment the serial number (on the second line of the record).

7. Save the file and check it with named-checkconf.

8. Restart the 'named' daemon.

2.1.2.3 Update MX Records for Comodo DNS

1. Log in to DNS.com administrative console at https://dns.com/login/ by entering your login email address and password.

2. Select the domain for which you want to update the MX records, from the "Select domain" drop down menu.

3. Click the "View / Manage" button beside the row labeled "@ (mail)".
The existing MX records will be displayed at the left hand side pane.
4. Delete the existing records by clicking the 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 the FQDN of your preferred CDAS service domain in the 'Answer' field
   
   CDAS primary service domains are:
   EU: mxpool1.spamgateway.comodo.com
   US: mxpool1.us.spamgateway.comodo.com

   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 the FQDN of your preferred **CDAS service domain** in the 'Answer' field
  
  CDAS secondary service domains are:
  
  EU: mxpool2.spamgateway.comodo.com
  
  Please note there is no secondary service domain for the US based service. Leave it blank.

• Click 'Save'

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

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

### 2.1.2.4 Update MX Records for GoDaddy

1. Log in to GoDaddy administrative console at [http://www.godaddy.com](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.
6. Click 'Add New MX Record'. The interface for adding a new MX record will appear.

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.

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

To set the secondary server:
- Click 'Add New MX Record' again. The interface for adding a new MX record will appear.
- Enter "2" in the 'Priority' field.
- Enter "@" in the Host Name field.
- In the 'Enter Goes To Address' field, enter the FQDN of your preferred CDAS service domain. CDAS secondary service domains are:
  - EU: mxpool2.spamgateway.comodo.com
  - US: mxpool1.us.spamgateway.comodo.com
- Please note there is no secondary service domain for the US based service. Leave it blank.
- Select '1 week' from the TTL drop-down.
- Click 'OK'.

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

2.1.2.5 Update MX Records for Enom

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 the FQDN of your preferred **CDAS service domain**.
  
  CDAS primary service domains are:
  
  EU: mpxpool1.spamgateway.comodo.com
  US: mpxpool1.us.spamgateway.comodo.com

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

**To set the secondary server:**
- Enter "2" in the 'Priority Value' field.
- Enter "@" in the Enter a Host Name field.
- In the 'Enter Goes To Address' field, enter the FQDN of your preferred **CDAS service domain**.
  
  CDAS secondary service domains are:
  
  EU: mpxpool2.spamgateway.comodo.com

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

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

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

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

### 2.1.2.6 Update MX Records for Network Solutions

1. Log in to Network Solutions administrative console at [https://www.networksolutions.com/manage-it/index.jsp](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.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Mail Server</th>
</tr>
</thead>
</table>
| 1       | Enter the FQDN of your preferred **CDAS service domain**.
          | CDAS primary service domains are:
          | EU: mxpool1.spamgateway.comodo.com
          | US: mxpool1.us.spamgateway.comodo.com |
| 2       | Enter the FQDN of your preferred **CDAS service domain**.
          | CDAS secondary service domains are:
          | EU: mxpool2.spamgateway.comodo.com
          | Please note there is no secondary service domain for the US based service. Leave it blank. |

7. Click 'Save'.

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

### 2.1.2.7 Update MX Records for Yahoo! Small Business

1. Log in to Yahoo! Small Business administrative console at [https://login.yahoo.com/config/login_verify2](https://login.yahoo.com/config/login_verify2) by entering your 'Yahoo ID', 'Password' and clicking 'Sign In'.

2. Click 'Domain' from the toolbar.

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 with the FQDN of your preferred **CDAS service domain** in the first open text box.

   CDAS primary service domains are:
   EU: mxpool1.spamgateway.comodo.com
   US: mxpool1.us.spamgateway.comodo.com

7. Set the priority for the primary email server as "1"

8. Enter the MX record for secondary email server with the FQDN of your preferred **CDAS service domain** in the second open text box.

   CDAS secondary service domains are:
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 Update MX Records for 1and1

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

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

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

<table>
<thead>
<tr>
<th>MX 1/Prio</th>
<th>Enter the FQDN of your preferred CDAS service domain. CDAS primary service domains are: EU: mxpool1.spamgateway.comodo.com US: mxpool1.us.spamgateway.comodo.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>MX 2/Prio</td>
<td>Enter the FQDN of your preferred CDAS service domain. CDAS secondary service domains are: EU: mxpool2.spamgateway.comodo.com Please note there is no secondary service domain for the US based service. Leave it blank.</td>
</tr>
</tbody>
</table>

9. Click 'OK'.

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

2.1.2.9 Update MX Records for 4D Web Hosting

1. Log in to your 4D Web Hosting administrative console at https://members.4dwebhosting.com/ by entering your 'Username', 'Password' and clicking 'Login'.
2. Click 'Configure'.
3. Click 'MX Records' from the Configuration options.
4. Replace the top two records with the following:
5. Click ‘Update MX Records’.
The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.10 Update MX Records for DNS Park

2. Click ‘DNS Hosting’ from the left hand side navigation.
3. Choose the domain for which the MX records are to be updated.
4. Click ‘Mail Records (MX)’.
5. Under ‘MX Resource records’,
   • Replace the hostname at 1st priority row with the FQDN of your preferred **CDAS service domain** and click 'Update'
     CDAS primary service domains are:
     EU: mxpool1.spamgateway.comodo.com
     US: mxpool1.us.spamgateway.comodo.com
   • Replace the hostname at 2nd priority row with the FQDN of your preferred **CDAS service domain** and click 'Update'
     CDAS secondary service domains are:
     EU: mxpool2.spamgateway.comodo.com
     Please note there is no secondary service domain for the US based service. Leave it blank.
6. Delete other existing MX records.

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

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

2.1.2.11 Update MX Records for DreamHost

1. Log in to DreamHost administrative control panel at https://panel.dreamhost.com/ by entering your email address/Web ID and Web panel password.
2. Click ‘Mail’ from the left hand side navigation and select ‘MX’ from the options.
3. Click ‘Edit’ beside the domain name for which the MX records are to be updated.
4. Delete all existing MX records under ‘Custom MX Records’.
5. In the first text box, enter the FQDN of your preferred **CDAS service domain**
   CDAS primary service domains are:
   EU: mxpool1.spamgateway.comodo.com
   US: mxpool1.us.spamgateway.comodo.com

6. In the second text box, enter the FQDN of your preferred **CDAS service domain**
   CDAS secondary service domains are:
   EU: mxpool2.spamgateway.comodo.com
   Please note there is no secondary service domain for the US based service. Leave it blank.

7. Click 'Update your custom MX records now!'
   The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

### 2.1.2.12 Update MX Records for DynDNS

2. Click 'My Services'.
3. Click 'Custom DNS' beside the domain for which the MX records are to be updated, under 'Zone Level Services'.
4. Select all the entries under 'Mail eXchanger Records' and click 'Delete MX'.
5. Click 'Add New MX'.
6. Set the primary mail server:
   - Enter the FQDN of your preferred **CDAS service domain**
     CDAS primary service domains are:
     EU: mxpool1.spamgateway.comodo.com
     US: mxpool1.us.spamgateway.comodo.com
   - Select '5' for preference to set higher priority for the primary server
   - Click 'Modify MX'
   - Click 'Return to...

7. Set the secondary mail server
   - Enter the FQDN of your preferred **CDAS service domain**
     CDAS secondary service domains are:
     EU: mxpool2.spamgateway.comodo.com
     Please note there is no secondary service domain for the US based service. Leave it blank.
   - Select '10' for preference to set lower priority for the secondary server
   - Click 'Modify MX'
   - Click 'Return to...

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

### 2.1.2.13 Update MX Records for IX Web Hosting

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Data</th>
<th>Data (Second box)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leave Blank</td>
<td>1</td>
<td>Enter the FQDN of your preferred CDAS service domain. CDAS primary service domains are: EU: mxpool1.spamgateway.comodo.com US: mxpool1.us.spamgateway.comodo.com</td>
</tr>
<tr>
<td>Leave Blank</td>
<td>2</td>
<td>Enter the FQDN of your preferred CDAS service domain. CDAS secondary service domains are: EU: mxpool2.spamgateway.comodo.com Please note there is no secondary service domain for the US based service. Leave it blank.</td>
</tr>
</tbody>
</table>

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

2.1.2.14 Update MX Records for No-IP

1. Log in to No-IP administrative console at [https://www.no-ip.com/login/](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 the FQDN of your preferred CDAS service domain
   CDAS primary service domains are:
   EU: mxpool1.spamgateway.comodo.com
   US: mxpool1.us.spamgateway.comodo.com
6. Replace the MX record entry at the second field with the FQDN of your preferred CDAS service domain
   CDAS secondary service domains are:
   EU: mxpool2.spamgateway.comodo.com
   Please note there is no secondary service domain for the US based service. Leave it blank.
7. Delete the other MX records.
2.1.2.15 Update MX Records in CPanel

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

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.

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

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.
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 the FQDN of your preferred CDAS service domain in the Destination field

   CDAS primary service domains are:
   - EU: mxpool1.spamgateway.comodo.com
   - US: mxpool1.us.spamgateway.comodo.com
7. Set the secondary mail server under ‘Add New Record’
   a. Enter ‘1’ in Priority field
   b. Enter the FQDN of your preferred **CDAS service domain** in the Destination field
      CDAS secondary service domains are:
      EU: mxpool2.spamgateway.comodo.com
      Please note there is no secondary service domain for the US based service. Leave it blank.
   c. Click ‘Add New record’. The new MX Record pointing to CDAS 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

CDAS 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 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 CDAS mailserver and the actual recipient would be contacted by CDAS mailserver itself. Please note that for smarthost option, email user authorization should be handled on your side, either by IP address or by using SMTP AUTH.

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

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

You can route all incoming / outgoing messages for remote domains through a smarthost instead of sending them directly to the domain to reduce e-mail spam from the recipient's mail server via the default SMTP port.

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

**European Union**
- mxpool1.spamgateway.comodo.com
- mxpool2.spamgateway.comodo.com

**United States**
- mxpool1.us.spamgateway.comodo.com

The following sections explain how to configure outgoing smarthost:

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

**Routing all mails to a smarthost**

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

**European Union**

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

**United States**

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

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

**Routing all mails for a specific domain to a smarthost :**

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

**European Union**

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

**United States**

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

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

### 2.2.2.2 Configure PostFix to use a Smarthost

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

**Routing all mails to a smarthost :**

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

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

**European Union**

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

**United States**

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

**Routing all mails for a specific domain to a smarthost :**

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

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

**European Union**
example.com  smtp: mxpool1.spamgateway.comodo.com:587

**United States**
example.com  smtp: mxpool1.us.spamgateway.comodo.com:587

generate a postmap file:
postmap hash:/etc/postfix/transport

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

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

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

### 2.2.2.3 Configure Sendmail to use a Smarthost

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

**Routing all mails to a smarthost**:

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

**European Union**
DSmxpool1.spamgateway.comodo.com

**United States**
Dsmxpool1.us.spamgateway.comodo.com

Restart Sendmail.

### 2.2.2.4 Configure Exchange 2000/2003 to use a Smarthost

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

**Routing all mails to a smarthost**:

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

**Routing all mails for a specific domain to a smarthost**:

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

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

2.2.2.5 Configure Exchange 2007/2010 to use a Smarthost

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

Routing all mails to a smarthost:

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

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

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

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

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

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

Restart the transport service.

Routing all mails to a 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’.
- In the FQDN section enter mxpool1.spamgateway.comodo.com, mxpool2.spamgateway.comodo.com (for EU based DAS server) or mxpool1.us.spamgateway.comodo.com (for US based DAS server)
- 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 Configure Exchange 2013/2016 to use a Smarthost

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

**Routing all mails to a smarthost:**

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

- Open ‘Exchange Admin Center’ (EAC).
- Select ‘Mail flow’ on the left then click ‘Send Connectors’.
- Select the existing send connector to view its properties.
- Select “Route mail through the following smart hosts:” under ‘Specify how to send mail with this connector’ and click the '+' button to add the smart host name.
- Enter `mxpool1.spamgateway.comodo.com` *(for EU based CDAS server)* or `mxpool1.us.spamgateway.comodo.com` *(for US based CDAS server)* in the ‘add smart host’ dialog.

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

- Select ‘Basic Authentication’ under ‘Smart host authentication’ and enter the username and password of your CDAS-MSP account
- Under ‘Address Space’, click the '+' button in the ‘Add Domain’ window
  - Select ‘SMTP’ for ‘Type’
  - Enter '*' in the Fully Qualified Domain Name (FQDN) field
  - Click ‘Save’
- Under ‘Source Server’, click '+' in the ‘Select a server’ window.
  - Select a mailbox server that will be used to send email to the internet via the ‘Client Access’ server
  - Click ‘Finish’

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

### 2.2.2.7 Configure Exim to use a Smarthost

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

**Routing all mails to a smarthost:**

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

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

```
spamgateway_smarthost_router:
    driver = manualroute
    transport = spamgateway_smarthost_transport
    route_list = $domain mxpool1.spamgateway.comodo.com::587 (for EU based CDAS server) or $domain mxpool1.us.spamgateway.comodo.com::587 (for US based CDAS server)
    no_more
```
Make sure the local mail route is before smarthost, if you don't want local mail to be forwarded. Add in the transports section (after `begin transports`):

```plaintext
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:

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

Restart Exim for the changes to take effect.

### 2.2.2.7.1 Configure Exim / cPanel to use a Smarthost

Routing all mails to a smarthost:

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

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

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

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

```plaintext
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}{$primary_hostname}}}{{primary_hostname}{{primary_hostname}}}$
  dkim_domain = $sender_address_domain
```

Comodo Dome Antispam MSP Admin Guide | © 2017 Comodo Security Solutions Inc. | All rights reserved
dkim_selector = default
dkim_private_key = "/var/cpanel/domain_keys/private/${dkim_domain}"
dkim_canon = relaxed

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

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

Routing all mails to a smarthost with SMTP Authentication:

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

begin authenticators

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

Add a Router in the Router Configuration Box.

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

Add a Transport to the Transport Configuration Box.

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

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

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

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

```plaintext
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:

```plaintext
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:

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

2.2.2.7.2 Configure Exim / Directadmin to use a Smarthost

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

```plaintext
spaghateway_smarthost_router:
    driver = manualroute
    domains = ! +local_domains
    ignore_target_hosts = 127.0.0.0/8
    condition = "${perl{check_limits}}"
    transport = spaghateway_smarthost_transport
    route_list = $domain mxpool1.spaghateway.comodo.com::587 (for EU based DAS server) or $domain mxpool1.us.spaghateway.comodo.com::587 (for US based DAS server)
    no_more
```

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

```plaintext
spaghateway_smarthost_transport:
    driver = smtp
    hosts_require tls = *
```

Restart Exim.
The Admin Console

The admin console is the nerve center of Comodo Dome Antispam - MSP (CDAS), allowing you to add domains, add administrators and users, manage accounts and more.

Once logged-in, admins can navigate to different areas of the console by clicking the tabs in the left menu.

Main Functional Areas

- **Dashboard** - View graphical summaries of domain quota usage, user quota usage, archive quota usage, details of domain and user license expiration. See The Dashboard Area for more details.
- **Domains** - Configure your CDAS protected domains. The area allows you to add, remove, edit and manage domains. Admins can set filters, view quarantined mails, set email restrictions, view logs, accept blacklist requests and more. See Domain Management for more details.
- **Audit Log** - View records of actions initiated by users and administrators for all domains belonging to an account. See Audit Log for more details.
- **Account Management** -
  - Add edit or delete administrators
  - Change admin password
  - Manage subscriptions to domain and quarantine summary reports.
  - Create user and administrator groups / Configure user and group permissions
  - View user history for your domains within a particular date range.
• See **Account Management** for more details.

**Customer Management** -
• Activate or deactivate customers
• View and manage customer details such as name, maximum number of users, maximum number of domains, incoming archive space and license expiration date
• Manage subscriptions to domain and quarantine summary reports for a customer
• Configure email template settings for messages sent from CDAS.

• See **Customer Management** for more details.

Click the [support.comodo.com](http://support.comodo.com) link at the bottom of interface to visit the Comodo support portal - an online knowledge base and support ticketing system. This is the fastest way to get assistance with any CDAS issues you my encounter.

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

## 3.1 Login to the Admin Console

As CDAS is a web application, you can login into your account using any internet browser. The login URL depends on the **CDAS service domain** that you subscribed for:

- EU CDAS - https://domeasmsp.cdome.net/admin/login.zul
- US CDAS - https://us-domeasmsp.cdome.net/admin/login.zul

• Login to the interface with your CDAS username and password.

In order to ensure safety, CDAS will lock the account if the login attempts fail for more than three attempts due to incorrect username or password.

To unlock the account the administrator can contact their Comodo Account Manager.

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

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

3.2 The Dashboard Area

The dashboard contains important statistics and charts about your Dome Antispam deployment. You can export any chart as a pdf by clicking the download icon in the top right corner of each panel.

Domain Quota Usage

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

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

- Place your mouse cursor over any chart sector to view more details.
- Click an item in the legend to add or remove it from the chart.
**User Quota Usage**
Number of users protected by spam filtering and the number remaining on your current license.

Each user that you protect with spam filtering will take one user from the pool remaining on your license.
- Place your mouse cursor over any chart sector to view more details.
- Click an item in the legend to add or remove it from the chart.

**Archive Quota Usage**
The quantity of mail archive space already used and the amount remaining on your current license.
- Place your mouse cursor over any chart sector to view more details.
- Click an item in the legend to add or remove it from the chart.

**Domain License Expiration**
Quantity of domains and domain license expiry dates.
- **Y axis** - Domain count
- **X axis** - Timeline
- **Green bars** - Total number of domains allowed by all unexpired licenses.
- **Yellow line** - Actual number of domains active on your account.
- **Out-of-quota** - Shown if the actual number of domains is greater than the total allowed by your licenses.
- **Red line** - Date when a license is due to expire.

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

- The 'Domains' area allows admins to configure your domains for spam protection. You can add, delete, edit, validate and manage domains.
- You can configure policy settings such as email size restrictions and permitted file-extensions for attachments.
- You can also view logs of all configuration changes.

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

3.2.1.1 Domains

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

- Click 'Domains' on the left to open the 'Domains' area.
- The interface opens with a list of all domains that you have added to CDAS - MSP:
Use the following links for more help:

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

Sort Entries

Click the domain column heading to switch the sorting of the entries based on the ascending/descending order of the entries.

Use 'Filter' options to search particular domain(s)

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

To add more filters, click +
To remove a filter, click the icon beside it.

Available filters are:

- **Domain**: Will execute a search of domain names according to the text in the 3rd field and the condition selected in column 2.
- **Activated**: Will execute a search of activated/not activated domains. Use the conditions in column 2 and the checkbox to determine whether you want to search for activated or not activated domains.
- **Aliases**: Will execute a search of domain name aliases according to the text in the 3rd field and the condition selected in column 2.

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

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

Click 'Apply Filter' after selecting the filters.

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

Click the 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.

### 3.2.1.1 Add a Domain

From this interface, administrators with appropriate privileges can add domains, configure the number of users for each domain and the destination routes for respective domains. The number of domains that you can add depends on your subscription plan.

**To add a domain**

- Click the 'Domains' menu item on the left
• Click the 'Add' button

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 CDAS 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.
• The 'Timezone' drop-down allows you to choose the zone for the domain. CDAS will use the selected time-zone for events which concern that domain. Specifically, the quarantine list, archive list, log search, reports and report subscriptions.

• Click the 'Check routes' button to let CDAS automatically get the destination routes information from DNS. If the result contains CDAS service domain details (mxpool1.spamgateway.comodo.com for EU based service or mxpool1.us.spamgateway.comodo.com for US based service) then it means that DNS MX record was already updated to work with Dome Antispam server and you must fill 'Destination routes' field with your real MX record, for example mail.exampledomain.com.

• Enter the maximum numbers of users that can be added for this domain in the 'Domain user limit' field. Leaving this setting as 'Unlimited' will allow you to add up to, but not exceed, the maximum number of users permitted by your current license. The maximum number of users for a selected domain can also be configured in the 'Domain Settings' area.

• The domain entered in the 'Destination routes' field is tested to ensure the route is valid.
- Click 'Proceed' to save a domain.

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

- Click 'Save' to add the configured domains.

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

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

If you have already configured the domain's MX record for CDAS before adding the domain to the CDAS interface, then only the success message will be displayed. See 'Configuring MX Record' for details about configuring MX records and 'Validating Domains' for details about domain validation.
3.2.1.1.2 Deleting Domains

To delete a domain

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

**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.

3.2.1.1.3 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

- Click the 'Domains' menu item on the left
- Select the domain that you want to edit
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 and reconfigure the maximum number of users for that domain.

- 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 CDAS automatically get the destination routes information from DNS. If the result contains CDAS service domain details (mxpool1.spamgateway.comodo.com for EU based service or mxpool1.us.spamgateway.comodo.com for US based service) then it means that DNS MX record was already updated to work with Dome Antispam server and you must fill 'Destination routes' field with your real MX record, for example mail.testdomain.com.

• If required, edit the maximum of number of users that can be added for this domain in the 'Max. number of users' field. Leaving this setting as 'Unlimited' will allow you to add up to, but not exceed, the maximum number of users permitted by your current license.

• The domain entered in the 'Destination routes' field is checked by Comodo Dome Antispam diagnostic tool to assure the destination route is entered by administrator correctly.

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

• Click 'Save' to confirm the changes.

### 3.2.1.1.4 Validating Domains

All domains in CDAS MSP have to be validated in order to demonstrate your ownership of the domains. This can be done in two ways:

• The first method is to configure the MX record for the domain to the CDAS service before adding the domain in the CDAS interface. When you add this domain it will be automatically validated since only a person in control of the domain is able to modify MX records. See **'Configuring MX Record'** for details about configuring MX record to CDAS.

• The second method is to add the domain to CDAS first then validate ownership by providing an authentication code sent to postmaster@your_domain.com

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

To validate a domain

- Click the 'Domains' menu item on the left
- Select the domain that you want to validate
- Click the 'Validate domain' button
- The 'Validate domain' dialog will open:

A mail containing the validation code will have been sent to postmaster@your-domain.com immediately after adding a domain.

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

CDAS will verify the code and, if successful, the domain will be activated:
Non-validated domains should be validated within 24 hours or they will be automatically removed from the interface.

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

3.2.1.1.5 Manage a Domain

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

**To manage a domain**

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

- The configuration tabs for the selected domain will open on the left.
- By default, the 'Domain dashboard' for the selected domain will be displayed.
Click the following links for more details:

- Domain Dashboard
- Incoming
- Outgoing
- Email Management
- Domain Audit Log
- Domain Rules
- Account Management

### 3.2.1.1.5.1 Domain Dashboard

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

**To open a domain dashboard**

- Click the 'Domains' menu on the left
- Select the domain that you want to manage
- Click the 'Manage Domain' button
- Alternatively, click on the domain name in the 'Domains' column

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

The dashboard of the selected domain will be displayed:

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

- **Quarantine** - Quarantined mails of all users of the selected domain. See [Quarantine](#) for more details.
- **Release requests** - Requests from users on the selected domain to release quarantined mails. See [Released Requests](#) for more details.
- **Whitelist requests** - Requests from users on the selected domain to whitelist the senders of quarantined mails. See [Whitelisted Requests](#) for more details.
- **Blacklist requests** - Requests from users on the selected domain to blacklist the senders of quarantined mails. See [Blacklisted Requests](#) for more details.
The 'Mails Statistics' area provides a graphical as well as pie chart representation of the mails that were blocked, viruses blocked and more.

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

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

- Place your mouse cursor over a graph to view the space used on a specific date. See Managing Archived Mails for more details.

The 'Delivery queue statistics' area provides details of filtered mails that are queued in CDAS servers for delivery at a later time.

- It also displays the average time of queued mails for the previous day in CDAS servers before delivery. See Delivery Queue for more details.
3.2.1.1.5.2 Incoming

The 'Incoming' area allows you to view quarantined mails, configure incoming spam detection settings, set spam alert headings, add local email recipients and more.
Click the following links for more details:

- Quarantine
- Managing Archived Mails
- Incoming Spam detection settings
- Report Spam
- Delivery Queue
- Destination Routes
- Local Recipients
- Clear incoming cache
- Log search
- Domain aliases
- Domain settings
- Manage report subscriptions
- Relay restrictions
- Geolocation restrictions

Comodo Dome Antispam MSP Admin Guide | © 2017 Comodo Security Solutions Inc. | All rights reserved
Comodo Dome Antispam MSP - Administrator Guide

- Relay Restrictions
- Geolocation Restrictions

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

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

**To open the quarantined email interface**
- Click ‘Quarantine’ on the ‘Incoming’ drop-down menu on the left

The quarantined email area will open:
Sort the Entries
- Click any column heading to sort entries in ascending/descending order.

Use the ‘Filter’ option to search quarantined emails
- Click anywhere on the ‘Filters’ tab to open the filters area.

To add more filters, click +

To remove a filter, click the icon beside it.
Available filters are:

- **Subject**: Will execute a search of subject according to the text entered in the text box (column 3) and the condition selected in column 2.
- **From**: Will execute a search of senders according to the text entered in the text box (column 3) and the condition selected in column 2.
- **To**: Will execute a search of users according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Reason**: Will execute a search of quarantined mails according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Recipient**: Will execute a search of recipients according to the text entered in the text box (column 3) and the condition selected in column 2.

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

- **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**: Will execute a search of mail received dates according to the date selected in the calendar box (column 3) and the condition selected in column 2.
- **Size (KB)**: Will execute a search of mails according to the size selected or entered in third field (column 3) and the condition selected in column 2.

If 'Date' is selected, the following conditions 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

If 'Size' is selected, the following conditions 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 'Apply Filter' after selecting the filters.

Click anywhere on the 'Filters' 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 then click the 'Refresh' button.

### View Details of Quarantined Mails

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

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

**To view details of quarantined mails in the same CDAS window**

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

The details of the selected email will be displayed.

• Click 'All headers' to view the email headers which contain the tracking information of the mail detailing the path it has crossed before reaching the recipient. The headers give full details of the sender, route, recipient, sent date, mail type and so on and enable you to check the authenticity of the mail.
Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either release the mail or delete it.

- Click 'Whitelist this sender' to add the sender to **Sender Whitelist**
- Click 'Blacklist this Sender' to add this sender to **Sender Blacklist**. See **Whitelist / Blacklist** for more details.

**To view the details of a quarantined mail in a new CDAS window**

- Select the mail that you want to view in the quarantined email area
- Right-click on the email link in the subject column and select to open in a new tab or new window.
The browser may display a warning pop-up window notification. Click the 'Options'> then select 'Allow pop-ups for...' to allow to open new message in a new window. Click again 'Show message in new window'.

The details of the selected mail will be displayed in a new CDAS 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 confirm the release of the selected email.

- Click 'OK' to confirm the release

The email will be released to the address 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
- Click 'More actions' > 'Whitelist this Sender'.
An alert will be displayed.

- Click 'OK' to confirm to add the sender to whitelist. See '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
- Click 'More actions' > 'Blacklist this Sender'.

A confirmation will be displayed:
• Click 'OK' to confirm to add the sender to blacklist. See 'Sender Blacklist' for more details.

To delete a quarantined mail

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

A confirmation request will be displayed:

• Click 'OK' to delete the selection email.

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

• To delete all the quarantined mails, click 'More actions' > 'Delete all'.
An alert will be displayed to confirm the deletion.

![Delete emails dialog]

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

**Managing Archived Mails**

CDAS is capable of storing a copy of all incoming mails for all domains belonging to an account. A customer can purchase the archive storage space via Comodo Accounts Manager (CAM).

From the archived mails interface, an administrator with appropriate privileges can view details of the message, report spam, resend emails if required, retain messages from being removed, add the sender to Domain Rules and delete messages. The archived messages can be deleted manually or can be automated to be cleaned periodically. The settings for auto cleanup can be configured in the Domains Settings interface.

**To open the archived email interface:**

- Click the 'Archive' from the 'Incoming' drop-down on the left.
The archived email area of the selected domain will open:

**Sorting the Entries**

Click 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.

**Page Filter**

The page filter on the top-right has three options:
- **Show archive**: Lists only the archived mails
- **Show reported as spam**: Lists mails that are reported as spam
- **Show archive and reported as spam**: Lists both archived mails and mails that are reported as spam

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

### Using Filter option to search archived emails

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

To add more filters, click `➕` for narrowing down your search.

To remove a filter, click the `➖` icon beside it.

Available filters are:

- **Subject**: Will execute a search of subject according to the text entered in the text box (column 3) and the condition selected in column 2.
- **From**: Will execute a search of senders according to the text entered in the text box (column 3) and the
To: Will execute a search of users according to the text entered in the text box (column 3) and the condition selected in column 2.

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

- **Contains:** Displays all archived mails that contain the words entered in the text box
- **Not Contains:** Displays all archived 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:** Will execute a search of mail received dates according to the date selected in the calendar box (column 3) and the condition selected in column 2.
- **Size (KB):** Will execute a search of mails according to the size selected or entered in third field (column 3) and the condition selected in column 2.
- **Attachments:** Will execute a search of mails according to the checkbox status (column 3) whether enabled or disabled. If enabled, all archived mails with attachments will be displayed.
- **Marked as retained:** Will execute a search of mails according to the checkbox status (column 3) whether enabled or disabled. If enabled, all archived mails that are marked as retained will be displayed.

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

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

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

- **Less than:** Displays the archived emails with size less than the selected or entered size in the third box
- **Greater than:** Displays the archived emails with size greater than the selected or entered size in the third 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' to close the filters area.

Click the [Refresh](button to display all the archived emails.

**Note:** To display all the archived 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.

**View Details of Archived Mails**

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

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

**To view details of archived mails in the same CDAS window:**

- In the archived 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.

**To view the details of archived mails in a new CDAS window**

- In the archived email area, select the mail that you want to view, right-click on the email link in the subject column and select to open in a new tab or new window.
The browser may display a warning pop-up window notification. Click the 'Options' > 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 CDAS window.

To report archived mails as spam

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

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

Comodo Dome Antispam MSP Admin Guide | © 2017 Comodo Security Solutions Inc. | All rights reserved
An alert will be displayed to confirm selected email as spam.

Click 'OK' to confirm.

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

**To add a sender to whitelist**

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

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

An alert will be displayed to confirm adding the sender to whitelist.
• Click 'OK' to confirm to add the sender to whitelist. Refer the section 'Sender Whitelist' for more details.

To add a sender to blacklist

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

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

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

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

To resend emails from archive

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

• Select the mail that you want to resend and click 'Resend email'.
An alert will be displayed to confirm resending emails.

![Resend email(s) dialog]

- Click 'OK' to confirm.

A success message will be displayed.

To delete archived mails

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

An alert will be displayed to confirm deletion.

![Delete emails dialog]
• Click 'OK' to confirm.

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

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

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

To exclude mails from auto-clean operations

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

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

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

• Click 'OK' to confirm.
A confirmation dialog will be displayed and the retained messages are indicated by the anchor icons under the Actions column.

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

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

- Click 'OK' to confirm.
A confirmation dialog will be displayed and the anchor icons under the Actions column are no longer displayed indicating their unretained status.

**Incoming Spam detection settings**

The 'Incoming Spam Detection Settings' interface allows administrators to configure how mails are to be classified as 'spam', 'probable' and 'safe'.

- CDAS enforces several rules on mail envelope, header and content as each message passes through its spam filters.
- Each rule addresses a specific spam attribute and will assign a score to each mail based on the degree to which the mail exhibits that attribute.
- A message's total spam score depends on the weighted value of all rules combined.

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

**To configure incoming spam detection settings**

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

The incoming spam detection settings interface for the selected domain will open:
• **Quarantine enabled** - Selecting this option will move incoming mails identified as spam as per the 'Spam threshold setting' to Quarantine. If disabled, emails that are identified as 'Spam' will not be quarantined but will be delivered with the subject line as set in the 'Probable Spam notation / Spam Notation' fields. Messages identified as 'probable spam' based on the 'Probable spam threshold setting' are always sent to the recipient (and never quarantined) even if this option is enabled.

• **Days saved** - Enter the number of days that you want mails to be retained in quarantine. The maximum number of days that can be set is 9999. Quarantined mails that are not checked, released or deleted within the stipulated days will be automatically deleted from quarantine.

• **Spam threshold** - Enter any value between 0.1 and 1.0. All mails that are having a score value above that value will be identified as spam and quarantined automatically as explained above. Please note this value should be always higher than 'Probable spam threshold' value.

• **Spam notation** - The prefix that will be appended to the subject line of all 'Spam' emails sent to users. For example, "<Spam> Order two Rolex watches and get a free carton of Viagra" - where <Spam> is the text entered in the 'Spam notation' field. Note - this only applies IF quarantine has been disabled (i.e. if the 'Quarantine Enabled' box is not checked).

• **Probable spam threshold** - Enter any value between 0.0 and the value entered in Spam threshold field. All mails that are having a score value above that is set in this field will be identified as unsure mails and will be delivered to recipients with the subject line as set in the 'Probable Spam notation / Spam Notation' field.

• **Probable spam notation** - The prefix that will be appended to the subject line of all 'probable spam' emails sent to users. For example, "<Potentially Spam> Cheap deals on Dell computers" - where <Potentially Spam> is the text entered in the 'Probable spam notation' field.

• **Quarantine response** - Choose the response to be sent by CDAS to the SMTP server that delivered a message in the event that a mail is identified as spam.

  • **Rejected** - Will inform the SMTP server that the email has been rejected by CDAS and placed in quarantine.
  • **Accepted** - The email has passed the CDAS spam filters and detected as a spam will be placed in quarantine in silent mode.

• **Spam email** - Displays the email address to which the mails reported as spam from the 'Report Spam' interface and the 'Archive' interface will be forwarded. By default, mails reported as spam by the administrators will be forwarded to spam@antispamgateway.comodo.com for analysis by experts at Comodo. Once a reported mail is confirmed as spam, Comodo will update its mail filters to quarantine similar mails in future. Refer to the explanations under Managing Archived Mails and Report Spam for more details on forwarding the suspicious mails for analysis.

• **Notify user about new quarantine message** - Select this option if you wish CDAS to send a notification email to the intended recipient, if a spam email addressed to the recipient is intercepted by CDAS and moved to Quarantine. The notification email will contain a link to the...
email and a link for the user to login to the CDAS User interface.

- The recipient will be able to click the link to directly read the email, without logging-in to CDAS. The lifetime of the link is one day. If the user has not clicked the link within a day, the link will expire.
- If the user needs to respond to or delete the quarantined email, the user can click the next link to login to CDAS, view their quarantined mails and carry out their desired actions.

**Suspicious attachment notation** - The prefix that will be appended to the subject line of all mails identified with suspicious attachments like malware and macros and forwarded to the recipient or to a different email address, configured in the Domain Rules. Refer to the explanation under Rules in the section Domain Rules for more details. For example, “[Suspicious attachment] Your lucky draw” - where [Suspicious attachment] is the text entered in the ‘Suspicious attachment notation’ field.

- **Comodo RBL** - Comodo's Real-time Blackhole List (RBL) is a blacklist of locations which are known to send spam. This list is continuously updated by Comodo.
  - **Quarantine message** - If the IP address of the message sender is in the RBL, then the incoming email will be quarantined.
  - **Reject message** - If the IP address of the message sender is in the RBL, then the incoming email will be rejected.
  - **Disabled** - CDAS filters will not check Comodo RBL.
  - **Reject emails contains credit card number** - If enabled, emails that contain credit card numbers will be rejected. Credit card numbers have a certain structure that CDAS filters can recognize, so emails containing random numbers will not be rejected.

- Click ‘Save’ for your settings to take effect.
- To restore the settings to default, click ‘Reset to Default’.

**Report Spam**

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

Users can also report spam by forwarding unsolicited messages to spam@antispamgateway.comodo.com.

**To report a spam mail**

- Click 'Incoming' on the left then select 'Report spam'.
The 'Report Spam' interface will open:

- Click the 'Upload' button

Navigate to the location where the suspected email(s) is/are stored in your system. Select the mail that you want to report as spam and click 'Open'. The maximum size of the file that can be uploaded is 9 MB.
Note: Make sure to upload the file in email format only and size should not exceed 9 MB. Otherwise, the following warning message will be displayed.

The mail will be processed for uploading...

... and success message will be displayed.

Spam reported successfully
• Click the button to close the message.

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

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

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

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

The ‘Incoming Delivery Queue’ interface allows you to view queued mails and to manually force CDAS to retry delivery.

**To manually force-deliver emails in queue**

• Click ‘Incoming’ > ‘Delivery queue’ in the left-hand menu:

The ‘Incoming Delivery Queue’ interface of the selected domain will open:
Sort the Entries

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

Use the ‘Filter’ option to search queued emails

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

To add more filters, click +
You can remove a filter by clicking the icon beside it.

Available filters are:

- **Queue ID**: Will execute a search of Queue ID according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Queue name**: Will execute a search of Queue name according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Recipient**: Will indicate the email address of the recipient that is in the delivery request.
- **Message size**: Will execute the message size settings according to the number selected in the 'Filters'.
- **Subject**: Will execute a search of subject according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Last action**: Will execute a search of Last action according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Server name**: Will execute a search of Server name according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Delay reason**: Will indicate the reason an email is queued and cannot be delivered immediately.

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

- **Contains**: Displays all queued mails that contain the words entered in the text box
- **Equals**: Displays the queued emails that have the same words as entered in the text box
- **Not Equals**: Displays the queued emails that do not have the words entered in the text box
- **Not Contains**: Displays all queued emails that don't contain the words entered in the text box
- **Starts With**: Displays all queued mails that starts with the words entered in the text box.
- **Ends With**: Displays all queued mails that ends with the words entered in the text box.

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

- **Sender**: Will execute a search of senders according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Recipient**: Will execute a search of users according to the text entered in the text box (column 3) and the condition selected in column 2.
• **Message size**: Will execute a search of mails according to the size selected or entered in third field (column 3) and the condition selected in column 2.

If ‘Sender’ and/or ‘Recipient’ option is selected, the following conditions are available:

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

If ‘Message Size’ is selected, the following conditions are available:

- **Less than**: Displays the queued emails with size less than the selected or entered size in the third box
- **Greater than**: Displays the queued emails with size greater than the selected or entered size in the third 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 [Refresh] button to display all the queued emails.

**Note**: To display all queued emails, first click anywhere on the ‘Filters’ stripe to close the filters area then click ‘Refresh’.

**To force retry queued emails**

- 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, select the checkbox beside ‘Queue id’ and click the ‘Force retry’ button.

**Note**: Frozen emails can’t be force delivered from CDAS interface.

**View Headers of Queued Emails**

- Select an email from the delivery queue and click the ‘Show headers’ button.
View Results of Routes Availability Diagnostics of an Email

- Select an email from the delivery queue and click the 'Delivery diagnostic' button.
Configure Delivery Queue Alerts

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

You can specify 2 possible criteria that will trigger notifications:

- **If queue contains more than 'n' items** - CDAS will send a notification mail if the number of queued mails reaches or exceeds the number specified in this field.

- **If email remains in the queue for more than n hour(s)**: CDAS will send a notification mail when the oldest mail in the queue exceeds the age you specify (max age = 72 hours).

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

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

**Destination Routes**

- CDAS delivers incoming mails to the pre-configured next destination email server, if there is a temporary problem with the primary email destination server.

- If the failure is permanent, for example, unable to resolve hostname, CDAS will try to deliver through the next alternative route.

The 'Destination Routes' interface allows administrators to specify additional destination routes for the domain, for use as alternative destination routes.

**To add additional destination routes**

- Click 'Incoming' > 'Destination routes' in the left-hand menu
The 'Destination routes' interface 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 domain entered in the 'Destination routes' field is checked by Comodo Dome Antispam diagnostic tool to ensure the destination route is valid.

Click 'Proceed' to save a domain.

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 priority' button to confirm the changes.

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

**Local Recipients**

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

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

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

**To add local recipients**

- Click 'Incoming' on the left then select 'Local recipients'.
The 'Local Recipients' configuration area for 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 the recipient's in the E-mail field

• Click the 'Save' button

Repeat the process till you have added all users.

To remove a local recipient

• Select the user that you want to delete and click the 'Delete' button
• Click 'OK' to confirm.

The selected recipient will be deleted from the list

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

**To import local recipients from a CSV file**

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

user1
user2
user3

• Click the 'Import from CSV file' to import new users from a CSV file.
• Click 'Upload', navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.

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

• If you want to remove the upload from the queue, click the 'Remove import task' button. The 'Remove import task' deletes only the remaining part of an in-progress task.

On completion of the upload process, the results will be displayed.
The local recipients from .csv file will be uploaded and the administrator who carried out the task will receive a notification about the import task completion.

**Clear Incoming Cache**

- When an email for a certain recipient is permanently rejected by the destination server with a 5xx error code, the destination address of the recipient is considered invalid and all emails sent to the recipient will be rejected.

- CDAS filtering servers caches this information locally for up to two hours. The CDAS interface allows you to clear the call-out cache without waiting for the servers to clear it.

**To clear incoming cache**

- Click 'Incoming' on the left then select 'Clear incoming cache'.
The 'Clear incoming cache' interface will open:

- Click the 'Clear' button

The callout cache for the incoming domain is cleared.
• Click the button to close the notification.

Log Search

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

To search logs for incoming mails

• Click ‘Incoming’ on the left then select ‘Log search’.
The 'Log search (incoming)' interface for the selected domain will open:
• **Date range:** Select the date range for which you want to search the log file. The date range for which the log search can be processed depends on the settings configured in Domain Settings > Log retention period.

• **Message ID:** Enter a unique message identifier (**optional**)

• **Sender:** Enter a sender email address in this field.

• **Recipient:** Enter the email address in this field (for example, ‘testuser1’).

• **Sender IP:** Enter the IP address of the sender.

• **Sender host:** Enter the sender host name.

• **Predicate:** You have the option to select either ‘AND’ or ‘OR’ in the drop-down. When you choose ‘AND’ option, all the entered search terms will be searched together and when you choose ‘OR’ option, the application will search any of the search items entered.

• **Include results from the last minutes:** If selected, CDAS will include messages that are currently being migrated from the filtering server to the logging server in the search results.

• Click the ‘Search’ button.

CDAS will search for the entered terms and display the results.
Domain Aliases

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

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

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

To add domain aliases

- Click 'Incoming' > 'Domain aliases' in the left-hand menu
The 'Domain Aliases' interface will open:

- Click the 'Add' button to add a domain alias. The 'Add domain alias' dialog box will open.
- Enter the domain alias name in the 'Alias' field.
• Click the 'Save' button. The domain will be added to the main domain as alias and will be listed in the interface.

To delete a domain alias,

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

The selected domain alias will be deleted from the list.

**Domain Settings**

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

**To configure domain settings**

• Click 'Incoming' > 'Domain settings' in the left-hand menu
The 'Domain Settings' interface of the selected domain will open:
- **Maximum bounces**: Enter the maximum number of message bounces that each recipient in the selected domain can receive per hour (messages from postmaster addresses or with an empty envelope sender). Please note that if the number of bounces exceeds the limit set in this field, the messages are not quarantined but are permanently rejected and will not be received later. You can set this to a low value if users at the selected domain do not send mails to invalid addresses frequently. By default this field is set to 6000.

- **Log retention period**: All spam and non-spam email connections to a domain are logged in the CDAS server. By default the storage period of this log is 30 days. You can store the log for a longer period by entering the number of days that you want to store in the field. After the end of set period, the log data will be moved to a separate storage and cannot be retrieved.

- **Maximum days to retry**: If the destination route has temporary problems, the messages are queued and automatically retried at fixed intervals for the number of days entered in the field. Even after this period if the emails cannot be delivered, they are bounced to the sender. By default, this is set to 4 days, the main reason being that the senders should be aware that his/her messages are not being delivered for 4 days.

- **Change locale for system messages**: Choose the language used for messages sent to domain administrators.

- **Max. number of users**: Enter the maximum of users that can be added for this domain. Leaving this setting as 'Unlimited' will allow you to add up to, but not exceed, the maximum number of users permitted by your current license. This can also be done while creating a domain or in the editing domain interface.

- **Enable archive cleanup**: Allows you to enable or disable the auto-clean up of archived incoming mails in the archive storage. This option is available for customers that has purchased archive storage from Comodo.

- **Retain Archived Items for**: Allows you to set the period in months or days, for which the archived mails should be retained in the archive storage, if you have enabled archive clean-up. The messages that are older than the period set in this field will be purged automatically.

- **Enable user auto-login**: If enabled, end-users can login into their CDAS account without entering their credentials. On first login, the users will be asked to confirm their auto login. The users can also change the settings on their 'My Profile' page. The users' credentials will be stored in the browser’ as auto-login cookie.
and will be valid for the number of days that is entered in the next field 'Days before cookie expiration'.

- **Days before cookie expiration**: Enter the validity period in days of the auto-login cookie for end-users. This is only relevant if you have enabled user-auto-login. Upon expiry of the cookie, users need to provide login credentials to access their CDAS account. The validity period starts after each successful user login.

- **Email for license notification**: Enter the email address for receiving license notifications for this domain. You can enter different email addresses for different domains for receiving notifications with respect to CDAS license. If the field is left blank, then license notifications will be sent to admins’ registered email address in Comodo Accounts Manager (CAM).

- **Timezone**: Allows you to choose the zone for the domain, depending on the location from which it is hosted. CDAS will use the selected time-zone for events which concern that domain, especially for maintaining the quarantine list, archive list, log search, reports and report subscriptions.

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

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

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

**Manage Report Subscriptions for Selected Domain**

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

- See CDAS Reports - an Overview for more information on reports.

**To access Manage report subscriptions interface**

- Click 'Incoming' on the left then choose 'Manage report subscriptions'.
The 'Manage report subscriptions' interface will open:
• **Report recipients** - Enter the email addresses of the domain administrators to whom the reports should be sent. You can enter multiple addresses separated by a comma.

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

• The interface lets you configure the delivery schedule for each type of report.

• Click on the respective strip to expand the configuration pane for a report type.

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

• **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 CDAS. Refer to CDAS Reports - An Overview for more details.
• **Domain Statistics Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly will contain a detailed statistics of number of users, mails that have been received at and sent from the domain, number of spams identified and blocked and so on. Refer to [CDAS Reports - An Overview](#) for more details.

• **Users auto-import report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly will contain details of new users that were auto-imported based on incoming mails received for them at the mail server. For more details on configuring CDAS for auto-importing new users, refer to the section [Managing User Auto-import](#). For more details on the reports, refer to the section [CDAS Reports - An Overview](#).

• **Quarantine Release Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly will contain a detailed statistics of the quarantined mails that are released by the administrator to the recipient. Refer to [CDAS Reports - An Overview](#) for more details.

• **Reported Spam Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly will contain a detailed statistics of the mails that are reported as spam by administrators and users. Refer to [CDAS 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**
  - **Domain Statistics Report**
  - **User Auto-Import Report**
  - **Quarantine Release Report** and
  - **Reported Spam Report**

**Quarantine 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
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.

User Auto-Import 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.

**Quarantine Release Report**

![Quarantine Release Report](image)

• **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.

**Reported Spam Report**

![Reported Spam Report](image)

• **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.
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.
  
  • Click the 'Reset settings to default' button to disable all the reports. The 'Report Recipients' field will not be cleared.

**Relay Restrictions**

• The 'Relay restrictions' interface lets you specify message transfer agents (MTA), mail servers, or other mail relays from which incoming mail should be accepted or rejected.

• For example, a business that has regional offices can configure their regional systems to accept only incoming emails from email servers at the home office.

• Administrators can define organization names from which mails should be accepted or rejected. CDAS parses the mail headers of each incoming mail to ensure the existence of an MTA IP address or FQDN of the organization before accepting the mail. If you don't know the name of an organization, you can search for it using the 'Lookup' feature. Enter the IP address of the sender domain.

**To add a relay restriction rule**

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


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

```
Dashboard / Domains / Domain dashboard - demo.das.comodo.od.ua / Relay restrictions
```

**Relay restrictions**

- Add
- Delete
- Edit

- Restrict email acceptance to the following relay servers

<table>
<thead>
<tr>
<th>Organization name</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Inc.</td>
<td>Accept</td>
</tr>
</tbody>
</table>
Select the 'Restrict email acceptance to the following relay servers' check box
Click the 'Add' button. The 'Add/Edit restriction' dialog will appear:

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

Repeat the process till you have added all the organizations.

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

Illustrations:
1. For example, if you want to accept mails only from two domains, namely gooddomain1.com and gooddomain2.com and reject mails from all the other mail servers, create two rules, one for gooddomain1.com and other for gooddomain2.com.
   - Rule 1 - Accept gooddomain1.com and block all other domains
   - Rule 2 - Accept gooddomain2.com and block all other domains
Only the incoming mails from gooddomain1.com and gooddomain2.com will be accepted. Those from all the other domains will be rejected.
2. For example, if you want to block mails only from two domains, namely baddomain1.com and baddomain2.com and allow mails from all the other mail servers, create two rules, one for baddomain1.com and other for baddomain2.com.

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

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

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

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

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

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

**Edit Relay Restriction Rules**

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

**To edit a rule**

   • Choose the rule to be edited and click the 'Edit' button.
The Add/Edit restriction dialog will appear.

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

Removing Relay Restriction Rules
You can remove unwanted rules at anytime from CDAS.

To remove a Relay Restriction rule
- Choose the rule you want to remove and click the 'Delete' button
• Click ‘OK’ in the confirmation dialog.

**Geolocation Restrictions**

• You can set rules that allow or block access to the CDAS console based on the country from which the connection attempt was made.

**To create a geolocation policy**

• Click ‘Incoming’ on the left then click ‘Geolocation restrictions’:
The 'Geolocation restrictions' interface for the domain will open:

- **Enable geolocation restrictions** - Activate location based access restrictions. If enabled, administrators need to add restriction rules.
From this interface, you can:

- Add geolocation restriction rules
- Edit a geolocation restriction rules
- Delete a geolocation restriction rules

To add a new geolocation restriction rule

- Click the 'Add' button

The 'Add country restriction' dialog will appear.

- Select the country from the 'Choose country' drop-down
Choose the geolocation restriction policy for accessing the CDAS web interface

- Accept - Admins and users from these countries are allowed to access the domain management interface
- Reject - Admins and users from these countries are not allowed to access the domain management interface

Click 'Save' to create the policy
Repeat the process to add more rules

To edit a geolocation restriction rule
A geolocation restriction policy cannot be edited for a country. But you can change the country for the policy.

- Select the rule for which you want to change the country and click the 'Edit' button
• Select a different country from the drop-down

• Click the 'Save' button for the changes to take effect

To delete a geolocation restriction rule

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

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

The rule will be removed from the list.
3.2.1.1.5.3  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](#). The following ports are available for the outgoing service:

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

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

Create a separate outgoing user on the filtering cluster for each end-user to relay outgoing email 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**

CDAS 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. CDAS filtering servers caches this information locally for up to two hours. CDAS interface allows you to clear the callout cache without waiting for the servers to clear it.

**To clear outgoing cache**

- Click the 'Clear outgoing cache' from the 'Outgoing' drop-down on the left

The 'Clear outgoing cache' interface will be displayed:
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 allows you to search for a specific outgoing email message.

- Click the Log search form the 'Outgoing' drop-down on the left
- The 'Log Search (Outgoing)' interface will be displayed:

  - Date range: The date range for which you want to search the log file. The date range for which the log search can be processed depends on the settings configured in Domain Settings > Log retention period.
  - Message ID: A unique message identifier (optional)
• **Sender**: The sender email address in this field.

• **User**: The username of the outgoing email address for in this field (for example, ‘testuser1’).

• **Recipient**: The email address in this field. (for example, ‘testuser1@example.com’).

• **Sender IP**: The IP address of the sender.

• **Sender Host**: The sender host name.

• **Predicate**: There are two available options to select from the the drop-down: ‘AND’ or ‘OR’
  - If ‘AND’ is selected - All the entered search terms will be searched together
  - If ‘OR’ is selected - The application will search any of the search items entered.

• **Classification**: The type of email that you want to search from the drop-down options.

  - **Include results from the last minutes**: If selected, CDAS will include messages that are currently being migrated from the filtering server to the logging server in the search results.

Click the ‘Search’ button. CDAS will search for the entered terms and display the results.

### Sorting Entries

Click 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.

### Downloading the Report

- Click the 'Download' button to download the log report of sent mails for the filters entered and/or selected.
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. The values in the log report will be separated by commas. This file can be opened with Excel or Openoffice Calc for easy analysis.

**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.

**Configuring User's Email Client for Outgoing Mail Filtering**

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

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

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

**To access the 'Outgoing users' interface:**

- Click the Users' from the 'Outgoing' drop-down on the left
The 'Users' interface will be displayed:

**Sorting Entries**
Click 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' to open the filters area.
To add more filters, click + for narrowing down your search.

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 usernames(s) that starts with the words entered in the text box.
- **Ends With**: Displays all usernames(s) that ends 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' to close the filters area.
Click the Refresh button to display all the outgoing users.

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

**To add a new user**

- Click the 'Add' button at the top.
- The 'Add outgoing user' dialog will open:

  - Enter the username for the new outgoing user that will be first part of the email address. For example, testuser. The email address of the added user will be testuser@testdomain.com.
  - Enter the password in the Password field. If the 'Password' field is left blank, then the 'Username' must be an IP address, and any connection from that IP will be considered authenticated without needing to use SMTP AUTH (Note: authorizing IP addresses may be disabled on the system).
  - Click the 'Edit outgoing settings' button to configure outgoing settings for the user. The 'Add outgoing settings' dialog will expand:
• **Block outgoing spam/Automatic lock**
  - **Block outgoing spam** - Blocks all outgoing spam mails from the user.
  - **Automatic lock** - If CDAS detects spam or malicious mail from the user, it will automatically lock the user from sending mails for the period set in the 'User lock timeout' field.

• **User lock timeout** - The time in minutes the user will be locked out from sending mails after CDAS detects outgoing spam or malicious mails from the user.

• **Maximum unlocks by timeout** - The number of times the locked out user will be unlocked for sending out mails. After reaching the maximum limit, the user will be locked out from sending any mails till it is unlocked by the administrator.

• **Enable outgoing limits** - Activate / deactivate limits on outgoing mails.
  - **Limit per month** - The number of mails that can be sent per month
  - **Limit per week** - The number of mails that can be sent per week
  - **Limit per day** - The number of mails that can be sent per day
• **Limit per hour** - The number of mails that can be sent per hour.
• **Limit per minute** - The number of mails that can be sent per minute.
• **Valid sender address required** - If enabled, outgoing mails must have valid sender address.
• **Maximum number of recipients per day** - Maximum number of recipients that a user can send mails per day.
• **Invalid recipient limit** - The number of invalid recipients that a user can send mails to.
• **Maximum days to retry** - Maximum number of days CDAS will retry to send queued outgoing mails after which they are bounced to the user.
• **Quarantine response** - Determines the response that CDAS 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 CDAS will send back to the SMTP mail server.

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

• Click the 'Save' button.

To delete an existing user
• Select the user you want to delete from the list and click 'Delete' button.
Tip: You can select multiple users to delete by pressing and holding the Shift or Ctrl keys.

- Click 'OK' to confirm.

To edit an existing user

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

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

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

To manually lock outgoing user

Due to administrative or any other reason if you want to prevent a user from sending out mails, the 'Lock' feature allows you to do so.
• Select the user that you want to lock, click 'More actions' drop-down > 'Lock'
The selected user will be locked from sending mails with status 'Manual'.

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

- Select the user that you want to unlock, click 'More actions' > 'Unlock'.
The user will be unlocked and he can send mails.

**To import outgoing users from CSV file**

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

user1,domainname,password
user2,domainname,password

- To import outgoing users from a CSV file, click ‘More actions’ > ‘Import from CSV file’
• Click the 'Upload' button and navigate to the location where the file is saved and click the 'Open' button.
The upload progress will be displayed...

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

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

Import from incoming users
Administrators can add all incoming users to the outgoing users list by importing. If there is an outgoing user with the same name, the import of incoming user will be skipped.
• To import outgoing users from incoming users, click 'More actions' > 'Import from Incoming users'
The upload progress will be displayed...

...and when completed, the results will be displayed.
The administrator who carried out the task will receive a notification about the import task completion.

3.2.1.1.5.4 Email Management

- Dome Antispam allows you to configure the maximum size of each email and choose which file types are acceptable as attachments.
- You can also choose to release or reject requests from users. Users can request that you release quarantined emails or add senders to the blacklist/whitelist.
Click the following links for more details:

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

### Email Size Restriction

- CDAS lets you set the maximum size of each email to preserve bandwidth and storage space.
- Administrators can set the maximum email size anywhere up to 250 MB.
- If you require a size above 250 MB, please contact your account manager at Comodo. Alternatively, open a ticket at support.comodo.com or call 1.888.COMODO (2666.6361). Please have your account number ready.

**To set email size restriction**

- Click 'Email management' on the left and then click 'Email size restriction'
- The 'Email restrictions' interface of the domain selected will open:

![Email size restriction interface]

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

Dashboard / Domains / Domain dashboard - docteam.das.comodo.od.ua / Email size restriction

Email size restriction

Incorrect capacity value. Value must be between 1 and 250. If you require more than 250Mb please call us.

Email size restriction (MB): 250

• Click 'Save' to confirm your changes.

Blocked Extensions

• CDAS allows you to automatically block email attachments with specific file extensions.
• For example, an attachment with .exe extension may contain malicious code which could infect a recipient's computer. Click here to see the complete list of extensions that you can block.

To add blocked file extensions

• Click 'Email management' on the left then click 'Blocked extensions'
The 'Blocked extensions' interface of the domain will open:
A list of default blocked extensions is displayed. You can sort the blocked extensions list alphabetically in ascending or descending order by clicking the 'Blocked extensions' title bar.

- Click the 'Add' button to include another blocked extension:
  - Enter the extension name to be blocked in the text box

You can add many extensions at a time by clicking the + icon.
Click the 'Save' button
The entered extensions will be added to the list.

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

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

Click 'Reset to default' to restore default blocked extensions in CDAS.

List of blocked Extensions
Released Requests

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

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

To open the released requests interface

- Click 'Email management' on the left then click 'Released requests'
The 'Release requests' interface will open:

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

**View Details of Release Request 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:
To view details of release requested mails in the same CDAS window:

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

The details of the selected email will be displayed.

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

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

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

To view details of release requested mails in a new CDAS window:

- Click 'Release request' and select the mail that you want to view.
- Right-click on the email link in the subject column and select 'Open link in New Tab' or 'Open Link in New Window' to open in a new tab or new window.
The details of the selected mail will be displayed in a new CDAS 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 requested user.
Click 'OK' to confirm the release. The email will be released to the user and the mail will no longer be in the released mail list. The mail will be removed from the quarantine area and it will be archived if archive space is available for the domain.

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.

Use filters to search release requests

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:

- **Subject**: Will execute a search of subject according to the text entered in the text box (column 3) and the condition selected in column 2.
- **From**: Will execute a search of senders according to the text entered in the text box (column 3) and the condition selected in column 2.
- **To**: Will execute a search of users according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Reason**: Will execute a search of words in the reason column according to the text entered in the text box (column 3) and the condition selected in column 2.

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

- **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**: Will execute a search of mail received dates according to the date selected in the calendar box (column 3) and the condition selected in column 2.
- **Size**: Will execute a search of mails according to the size selected or entered in third field (column 3) and the condition selected in column 2.
If 'Date' is selected, the following conditions 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

If 'Size' is selected, the following conditions 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 '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 **Refresh** to display all the release requested emails.

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

**Blacklisted Requests**

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

**To view blacklisted requests**

- Click 'Email management' on the left then select 'Blacklisted requests'
The 'Blacklisted requests' interface will open:

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

**To view details of blacklisted requests in the same CDAS window:**

- Select the mail that you want to view and click the ‘Show Message’ button.

or

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

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

Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either accept the mail or reject it for blacklisting the sender. If the request is accepted, the sender will be added to 'Blacklist Senders Per User'. If it is rejected, the email will be no longer in the blacklisted requests 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 a new CDAS 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 CDAS 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 senders per user list.

- 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 'Blacklist Senders Per User'.

Click 'OK' to confirm the acceptance.

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

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.

Use Filter option to search blacklisted requests
• Click anywhere on the 'Filters' stripe to open the filters area.

To add more filters, click +

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

Available filters are:

- **Subject**: Will execute a search of subject according to the text entered in the text box (column 3) and the condition selected in column 2.
- **From**: Will execute a search of senders according to the text entered in the text box (column 3) and the condition selected in column 2.
- **To**: Will execute a search of users according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Reason**: Will execute a search of words in the reason column according to the text entered in the text box (column 3) and the condition selected in column 2.

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

- **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**: Will execute a search of mail received dates according to the date selected in the calendar box (column 3) and the condition selected in column 2.
- **Size**: Will execute a search of mails according to the size selected or entered in third field (column 3) and the condition selected in column 2.

If 'Date' is selected, the following conditions 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

If 'Size' is selected, the following conditions 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 '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 the blacklisted requests emails.

**Note**: To display all blacklist requests first click anywhere on the 'Filters' stripe to close the filters area then click 'Refresh'.

### White-listed Requests

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

**To open the whitelisted requests interface**

- Click 'Email management' on the left then select "Whitelisted requests".
The 'Whitelisted requests' interface will open:

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

**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:
To view details of whitelisted requests in the same CDAS window:

- Select the mail that you want to view and click the 'Show Message' button.

or

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

The 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 request is accepted, the sender will be added to ‘Whitelist sender per user’. If it is rejected, the email will be no longer in the whitelisted requests list. Please note that emails will continue to remain in the Quarantined list irrespective of the action taken.

To view details of whitelisted requests in new CDAS 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 CDAS window.

On Wednesday, 20 April 2016 10:53 AM, Online Health Plan <support@indiatravel.com> wrote:

If you're having trouble viewing this email, please click here.4y8y83199774641 .y881939774641text_base

The Best Hospitals are Now Affordable!
Get Health Insurance
In Just Rs. 13/day*
Get Health Insurance In Just Rs. 13/day*

Cashless Claim
Hospital Bills are directly
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 senders per user list.

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

An alert will be displayed to confirm adding the sender to 'Whitelist sender per user'.

- Click 'OK' to confirm the acceptance.

The sender of the email will be added to 'Whitelist sender per user'. See the section 'Whitelist Sender Per User' for more details.

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.

**Use Filter option to search whitelist requests**

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

To add more filters, click ⊕
You can remove a filter by clicking the icon beside it.

Available filters are:

- **Subject**: Will execute a search of subject according to the text entered in the text box (column 3) and the condition selected in column 2.
- **From**: Will execute a search of senders according to the text entered in the text box (column 3) and the condition selected in column 2.
- **To**: Will execute a search of users according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Reason**: Will execute a search of words in the reason column according to the text entered in the text box (column 3) and the condition selected in column 2.

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

- **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 start with the words entered in the text box
- **Ends with**: Displays all quarantined emails that end with the words entered in the text box

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

- **Date**: Will execute a search of mail received dates according to the date selected in the calendar box (column 3) and the condition selected in column 2.
- **Size**: Will execute a search of mails according to the size selected or entered in third field (column 3) and the condition selected in column 2.

If 'Date' is selected, the following conditions 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

If 'Size' is selected, the following conditions 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 '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 the whitelisted requests emails.

**Note:** To display all whitelist requests first click anywhere on the 'Filters' stripe to close the filters area then click 'Refresh'.

### 3.2.1.5.5 Domain Audit Log

CDAS keeps a record of actions initiated by users and administrators for a selected domain. The 'Audit Log' area allows administrators to:

- Configure and view these log reports.
- Keeps a consolidated log for all domains belonging to an account.
- To know more about consolidated log for all domains, see Audit Log for more details. This section explains about audit log for a selected domain.

Click the following links for more details:

- Audit Log Configuration
- View Domain Log

**Audit Log Configuration**

CDAS keeps a record of all actions initiated by administrators and users. However, some of the actions can be
configured not be recorded such as releasing quarantined items, updating sender whitelist and blacklist senders per user. The screen also allows administrators to add recipients to whom the notifications will be sent.

To configure audit log

- Click the ‘Configuration’ from the ‘Audit log’ drop-down on the left.

The ‘Audit Configuration’ area will be displayed:

- **Quarantined item released**
  - Create audit log entry - If enabled, CDAS records the release of quarantined mails.
  - Send notification email - If enabled, notification mails for quarantined mails release will be sent to recipients added in the ‘Notification recipient’s’ box.

- **Whitelist rules updated**
  - Create audit log entry - If enabled, CDAS records any updates to Whitelist senders per user interface.
  - Send notification email - If enabled, notification mails for updates to Whitelist senders per user interface will be sent to recipients added in the ‘Notification recipient’s’ box.

- **Blacklist rules updated**
  - Create audit log entry - If enabled, CDAS records any updates to Blacklist senders per user interface.
  - Send notification email - If enabled, notification mails for updates to Blacklist senders per user interface will be sent to recipients added in the ‘Notification recipient’s’ box.

- **Notification recipients** - Enter the email addresses of the persons to whom the email notifications for the above mentioned actions will be sent. Please note that any email addresses of the recipient’s can be entered here.
View Domain Log

The log screen allows admins with appropriate privileges to view the logs of the selected domain.

To view the audit log of the selected domain

- Click the 'Log' from 'Audit log' drop-down on the left
- The 'Audit log' screen will be displayed:

Sorting Entries

- Click 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. The sorting option is not available for 'Operation description' column.

Using Filter options to search particular event(s)

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

To add more filters, click +
Comodo Dome Antispam MSP - Administrator Guide

To remove a filter, click the icon beside it.

Available filters are:

- **Login**: Will execute a search of log entries according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Details**: Will execute a search of log entries according to the text entered in the text box (column 3) and the condition selected in column 2.

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

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

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

- **Date**: Will execute a search of log entries according to the date selected in the calendar box (column 3) and the condition selected in column 2.
- **Role**: Will execute a search of log entries according to the role selected in the third field (column 3) and the condition selected in column 2.
- **Operative description**: Will execute a search of log entries according to the action selected in the third field (column 3) and the condition selected in column 2.

If ‘Date’ is selected, the following conditions are available:

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

If ‘Role’ is selected, the following conditions are available:
Comodo Dome Antispam MSP - Administrator Guide

- **Equals:** Displays all log entries that is equal to the role selected in column 3.
- **Not Equals:** Displays all log entries that except the role selected in column 3.

If ‘Operative description’ is selected, the following conditions are available:

- **Equals:** Displays all log entries that is equal to the event selected in column 3.
- **Not Equals:** Displays all log entries that except the event selected in column 3.
- 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’ to close the filters area.
- Click the [Refresh] button to display all the entries.

**Note:** To display all the log entries 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.

The following table provides the details of actions initiated by user/administrator and shown under Operation Key and Operation Description columns in the log report:

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Operation Key</th>
<th>Operation Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DELETE_EMAIL_FROM_QUARANTINE_BY_FILTER</td>
<td>Delete quarantined messages by filter</td>
</tr>
<tr>
<td>2</td>
<td>DELETE_EMAIL_FROM_QUARANTINE</td>
<td>Delete quarantined message</td>
</tr>
<tr>
<td>3</td>
<td>RELEASE_EMAIL_FROM_QUARANTINE</td>
<td>Release quarantined message</td>
</tr>
<tr>
<td>4</td>
<td>WHITELIST_RECIPIENT</td>
<td>Whitelist recipient</td>
</tr>
<tr>
<td>5</td>
<td>BLACKLIST_RECIPIENT</td>
<td>Blacklist recipient</td>
</tr>
<tr>
<td>6</td>
<td>UNWHITELIST_RECIPIENT</td>
<td>Remove recipient from the whitelist</td>
</tr>
<tr>
<td>7</td>
<td>UNBLACKLIST_RECIPIENT</td>
<td>Remove recipient from the blacklist</td>
</tr>
<tr>
<td>8</td>
<td>WHITELIST_SENDER</td>
<td>Whitelist sender</td>
</tr>
<tr>
<td>9</td>
<td>BLACKLIST_SENDER</td>
<td>Blacklist sender</td>
</tr>
<tr>
<td>10</td>
<td>UNWHITELIST_SENDER</td>
<td>Remove sender from the whitelist</td>
</tr>
<tr>
<td>11</td>
<td>UNBLACKLIST_SENDER</td>
<td>Remove sender from the blacklist</td>
</tr>
<tr>
<td>12</td>
<td>RESET_TO_DEFAULT_WHITELISTED_SENDERS</td>
<td>Reset senders whitelist</td>
</tr>
<tr>
<td>13</td>
<td>RESET_TO_DEFAULT_WHITELISTED_RECIPIENTS</td>
<td>Reset recipients whitelist</td>
</tr>
<tr>
<td>14</td>
<td>RESET_TO_DEFAULT_BLACKLISTED_SENDERS</td>
<td>Reset senders blacklist</td>
</tr>
<tr>
<td>15</td>
<td>RESET_TO_DEFAULT_BLACKLISTED_RECIPIENTS</td>
<td>Reset recipients blacklist</td>
</tr>
<tr>
<td>16</td>
<td>WHITELIST_SENDER_DOMAIN</td>
<td>Whitelist all senders of the domain</td>
</tr>
<tr>
<td>17</td>
<td>WHITELIST_RECIPIENT_DOMAIN</td>
<td>Whitelist all recipients of the domain</td>
</tr>
<tr>
<td></td>
<td>BLACKLIST_SENDER_DOMAIN</td>
<td>Blacklist all senders of the domain</td>
</tr>
<tr>
<td>---</td>
<td>-------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>19</td>
<td>BLACKLIST_RECIPIENT_DOMAIN</td>
<td>Blacklist all recipients of the domain</td>
</tr>
<tr>
<td>20</td>
<td>USER_WHITELIST_REQUEST_PER_USER</td>
<td>Request whitelist sender for user</td>
</tr>
<tr>
<td>21</td>
<td>USER_BLACKLIST_REQUEST_PER_USER</td>
<td>Request blacklist sender for user</td>
</tr>
<tr>
<td>22</td>
<td>USER_RELEASE_REQUEST</td>
<td>Release request</td>
</tr>
<tr>
<td>23</td>
<td>USER_CANCEL_WHITELIST_REQUEST_PER_USER</td>
<td>Cancel request whitelist sender for user</td>
</tr>
<tr>
<td>24</td>
<td>USER_CANCEL_BLACKLIST_REQUEST_PER_USER</td>
<td>Cancel request blacklist sender for user</td>
</tr>
<tr>
<td>25</td>
<td>USER_CANCEL_RELEASE_REQUEST</td>
<td>Cancel release request</td>
</tr>
<tr>
<td>26</td>
<td>ACCEPT_WHITELIST_REQUEST_PER_USER</td>
<td>Accept request whitelist sender for user</td>
</tr>
<tr>
<td>27</td>
<td>ACCEPT_BLACKLIST_REQUEST_PER_USER</td>
<td>Accept request blacklist sender for user</td>
</tr>
<tr>
<td>28</td>
<td>ACCEPT_RELEASE_REQUEST</td>
<td>Accept release request</td>
</tr>
<tr>
<td>29</td>
<td>REJECT_WHITELIST_REQUEST_PER_USER</td>
<td>Reject request whitelist sender for user</td>
</tr>
<tr>
<td>30</td>
<td>REJECT_BLACKLIST_REQUEST_PER_USER</td>
<td>Reject request blacklist sender for user</td>
</tr>
<tr>
<td>31</td>
<td>REJECT_RELEASE_REQUEST</td>
<td>Reject release request</td>
</tr>
<tr>
<td>32</td>
<td>SPAM_DETECTION_SETTINGS</td>
<td>Update spam detection settings</td>
</tr>
<tr>
<td>33</td>
<td>SPAM_DETECTION_SETTINGS_RESET_TO_DEFAULT</td>
<td>Reset spam detection settings</td>
</tr>
<tr>
<td>34</td>
<td>DELETE_EMAIL_FROM_ARCHIVE_BY_FILTER</td>
<td>Delete archived messages by filter</td>
</tr>
<tr>
<td>35</td>
<td>DELETE_EMAIL_FROM_ARCHIVE</td>
<td>Delete archived message</td>
</tr>
<tr>
<td>36</td>
<td>RESEND_EMAIL_FROM_ARCHIVE</td>
<td>Resend archived message</td>
</tr>
<tr>
<td>37</td>
<td>REPORTS_AS_SPAM</td>
<td>Reports archived message as a SPAM</td>
</tr>
<tr>
<td>38</td>
<td>QUARANTINE_EMAIL</td>
<td>Quarantine message</td>
</tr>
<tr>
<td>39</td>
<td>ACCEPT_AND_ARCHIVE_EMAIL</td>
<td>Accept and archive message</td>
</tr>
<tr>
<td>40</td>
<td>MARK_EMAIL_AS_SPAM</td>
<td>Mark message as spam</td>
</tr>
<tr>
<td>41</td>
<td>ACCEPT_EMAIL</td>
<td>Accept message</td>
</tr>
<tr>
<td>42</td>
<td>WHITELIST_USER_SENDER</td>
<td>Whitelist sender for user</td>
</tr>
<tr>
<td>43</td>
<td>BLACKLIST_USER_SENDER</td>
<td>Blacklist sender for user</td>
</tr>
<tr>
<td>44</td>
<td>UNWHITELIST_USER_SENDER</td>
<td>Remove sender from the user whitelist</td>
</tr>
<tr>
<td>45</td>
<td>UNBLACKLIST_USER_SENDER</td>
<td>Remove sender from the user blacklist</td>
</tr>
<tr>
<td></td>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>----------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>46</td>
<td>QUARANTINE_REPORT_SUBSCRIPTION_UPDATE</td>
<td>Quarantine report subscription update</td>
</tr>
<tr>
<td>47</td>
<td>QUARANTINE_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT</td>
<td>Quarantine report subscription reset to default</td>
</tr>
<tr>
<td>48</td>
<td>DOMAIN_STATISTICS_REPORT_SUBSCRIPTION_UPDATE</td>
<td>Domain report subscription update</td>
</tr>
<tr>
<td>49</td>
<td>DOMAIN_STATISTICS_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT</td>
<td>Domain report subscription reset to default</td>
</tr>
<tr>
<td>50</td>
<td>DOMAIN_ADD</td>
<td>Add domain</td>
</tr>
<tr>
<td>51</td>
<td>DOMAIN_DELETE</td>
<td>Remove domain</td>
</tr>
<tr>
<td>52</td>
<td>ADMIN_ADD</td>
<td>Add admin</td>
</tr>
<tr>
<td>53</td>
<td>ADMIN_EDIT</td>
<td>Edit admin settings</td>
</tr>
<tr>
<td>54</td>
<td>ADMIN_DELETE</td>
<td>Remove admin</td>
</tr>
<tr>
<td>55</td>
<td>ADMIN_UNLOCK</td>
<td>Unlock admin</td>
</tr>
<tr>
<td>56</td>
<td>ADMIN_REGENERATE_PASSWORD</td>
<td>Regenerate password for admin</td>
</tr>
<tr>
<td>57</td>
<td>ADMIN_PASSWORD_UPDATE</td>
<td>Update password for admin</td>
</tr>
<tr>
<td>58</td>
<td>SYSTEM_NOTIFICATIONS_TEMPLATE_CHANGE</td>
<td>System notifications template change</td>
</tr>
<tr>
<td>59</td>
<td>ADMIN_PERMISSIONS_GROUP_ADD</td>
<td>Add admin permission group</td>
</tr>
<tr>
<td>60</td>
<td>ADMIN_PERMISSIONS_GROUP_DELETE</td>
<td>Remove admin permission group</td>
</tr>
<tr>
<td>61</td>
<td>ADMIN_PERMISSIONS_GROUP_UPDATE</td>
<td>Update admin permission group</td>
</tr>
<tr>
<td>62</td>
<td>ADMIN_PERMISSIONS_CHANGE_DEFAULT_GROUP</td>
<td>Change default admin permission group</td>
</tr>
<tr>
<td>63</td>
<td>ADMIN_PERMISSIONS_ASSIGN_GROUP</td>
<td>Assign admin permission group by selection</td>
</tr>
<tr>
<td>64</td>
<td>REPORT_SPAM_BY_FILE</td>
<td>Report delivered message as spam</td>
</tr>
<tr>
<td>65</td>
<td>DOMAIN_DESTINATION_ROUTES_UPDATE</td>
<td>Update destination routes</td>
</tr>
<tr>
<td>66</td>
<td>DOMAIN_LOCAL_RECIPIENTS_ADD</td>
<td>Add local recipient</td>
</tr>
<tr>
<td>67</td>
<td>DOMAIN_LOCAL_RECIPIENTS_DELETE</td>
<td>Remove local recipient</td>
</tr>
<tr>
<td>68</td>
<td>DOMAIN_LOCAL_RECIPIENTS_STATE_CHANGE</td>
<td>Local recipients state change</td>
</tr>
<tr>
<td>69</td>
<td>DOMAIN_ALIASES_ADD</td>
<td>Add domain alias</td>
</tr>
<tr>
<td>70</td>
<td>DOMAIN_ALIASES_DELETE</td>
<td>Remove domain alias</td>
</tr>
<tr>
<td>71</td>
<td>DOMAIN_SETTINGS_UPDATE</td>
<td>Update domain settings</td>
</tr>
<tr>
<td>72</td>
<td>DOMAIN_SETTINGS_RESET_TO_DEFAULT</td>
<td>Reset domain settings to default</td>
</tr>
<tr>
<td>73</td>
<td>DOMAIN_RELAY_RESTRICTIONS_ADD</td>
<td>Add relay restriction</td>
</tr>
<tr>
<td>74</td>
<td>DOMAIN_RELAY_RESTRICTIONS_UPDATE</td>
<td>Update relay restriction</td>
</tr>
<tr>
<td></td>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>75</td>
<td>DOMAIN_RELAY_RESTRICTIONS_DELETE</td>
<td>Remove relay restriction</td>
</tr>
<tr>
<td>76</td>
<td>DOMAIN_RELAY_RESTRICTIONS_STATE_CHANGE</td>
<td>Relay restriction state change</td>
</tr>
<tr>
<td>77</td>
<td>DOMAIN_OUTGOING_USER_ADD</td>
<td>Add outgoing user</td>
</tr>
<tr>
<td>78</td>
<td>DOMAIN_OUTGOING_USER_SETTINGS_UPDATE</td>
<td>Edit outgoing user</td>
</tr>
<tr>
<td>79</td>
<td>DOMAIN_OUTGOING_USER_DELETE</td>
<td>Remove outgoing user</td>
</tr>
<tr>
<td>80</td>
<td>DOMAIN_OUTGOING_USER_LOCK</td>
<td>Lock outgoing user</td>
</tr>
<tr>
<td>81</td>
<td>DOMAIN_OUTGOING_USER_UNLOCK</td>
<td>Unlock outgoing user</td>
</tr>
<tr>
<td>82</td>
<td>DOMAIN_OUTGOING_USER_PASSWORD_UPDATE</td>
<td>Update password for outgoing user</td>
</tr>
<tr>
<td>83</td>
<td>DOMAIN_EMAIL_SIZE_RESTRICTION_CHANGE</td>
<td>Email size restriction change</td>
</tr>
<tr>
<td>84</td>
<td>DOMAIN_BLOCKED_EXTENSIONS_UPDATE</td>
<td>Update blocked extensions</td>
</tr>
<tr>
<td>85</td>
<td>DOMAIN_BLOCKED_EXTENSIONS_RESET_TO_DEFAULT</td>
<td>Reset blocked extensions to default</td>
</tr>
<tr>
<td>86</td>
<td>DOMAIN_AUDIT_CONFIGURATION_CHANGE</td>
<td>Audit configuration change</td>
</tr>
<tr>
<td>87</td>
<td>DOMAIN_LDAP_CONFIGURATION_CHANGE</td>
<td>LDAP configuration change</td>
</tr>
<tr>
<td>88</td>
<td>DOMAIN_INCOMING_USER_ADD</td>
<td>Add incoming user</td>
</tr>
<tr>
<td>89</td>
<td>DOMAIN_INCOMING_USER_EDIT</td>
<td>Edit incoming user</td>
</tr>
<tr>
<td>90</td>
<td>DOMAIN_INCOMING_USER_DELETE</td>
<td>Remove incoming user</td>
</tr>
<tr>
<td>91</td>
<td>DOMAIN_INCOMING_USER_UNLOCK</td>
<td>Unlock incoming user</td>
</tr>
<tr>
<td>92</td>
<td>DOMAIN_INCOMING_USER_REGENERATE_PASSWORD</td>
<td>Regenerate password for incoming user</td>
</tr>
<tr>
<td>93</td>
<td>DOMAIN_INCOMING_USER_PASSWORD_UPDATE</td>
<td>Update password for incoming user</td>
</tr>
<tr>
<td>94</td>
<td>DOMAIN_INCOMING_USER_ALIASES_UPDATE</td>
<td>Update incoming user aliases</td>
</tr>
<tr>
<td>95</td>
<td>DOMAIN_INCOMING_USER_MOVE_USER_TO_ALIAS</td>
<td>Move user to alias</td>
</tr>
<tr>
<td>96</td>
<td>DOMAIN_INCOMING_USER_MOVE_ALIAS_TO_USER</td>
<td>Move alias to incoming user</td>
</tr>
<tr>
<td>97</td>
<td>USER_PERMISSIONS_GROUP_ADD</td>
<td>Add user permission group</td>
</tr>
<tr>
<td>98</td>
<td>USER_PERMISSIONS_GROUP_DELETE</td>
<td>Remove user permission group</td>
</tr>
<tr>
<td>99</td>
<td>USER_PERMISSIONS_GROUP_UPDATE</td>
<td>Update user permission group</td>
</tr>
<tr>
<td>100</td>
<td>USER_PERMISSIONS_CHANGE_DEFAULT_GROUP</td>
<td>Change default user permission group</td>
</tr>
<tr>
<td>101</td>
<td>USER_PERMISSIONS_ASSIGN_GROUP</td>
<td>Assign user permission group by selection</td>
</tr>
</tbody>
</table>
Export Log Report to CSV

The log report can be exported to a comma separated value (CSV) file and is limited to 10,000 entries per file. If the entries exceed this value, exporting cannot be done and a warning will be displayed. Please note that exported file will display the entries in the same sorted order as in the interface.

To export log report to csv file

- Click the 'Export to CSV by filter' button.

The 'File Download' dialog will be displayed.

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

The values in the log report will be separated by commas and this file can be opened with Excel or Openoffice Calc for easy analysis.

3.2.1.1.5.6 Domain Rules

- Create granular filtering rules for each domain in order to blacklist, whitelist or forward mails.
- Rules can be based on sender, recipient, source/destination server, subject line, suspicious attachments and more.
**Note:** Under default conditions, CDAS will filter all incoming mails to all domains that have been enabled in the 'Domains' area.

The following table offers more details on each rule type:

<table>
<thead>
<tr>
<th>Rule Type</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Rules (‘Create Rule...’)</td>
<td>Create granular rules to blacklist, whitelist or forward mail based on one or more criteria.</td>
<td>Criteria include sender, sender mail server, recipient, relay server, subject line and suspicious attachment.</td>
</tr>
<tr>
<td>TLD &amp; gTLD Rules</td>
<td>Allow or block mails based on top level domain.</td>
<td>Mail from all TLDs is allowed by default. This interface allows you to block selected TLDs.</td>
</tr>
<tr>
<td>Recipient Whitelist</td>
<td>Always allow mail sent to these</td>
<td>For example, CDAS will allow/block mails</td>
</tr>
</tbody>
</table>
### General Advice

- If you are troubleshooting issues with a particular email address, please check all interfaces listed under 'Domain Rules'.
- Rule priorities can be summarized as follows:
  1. Email Size Restriction
  2. Domain Whitelist rules
  3. Sender/Recipient Whitelist
  4. Domain Blacklist rules
  5. Sender/Recipient Blacklist
  6. TLD & gTLD blacklist rule
  7. Per user White list
  8. Per user Black list
  9. Email Blocked Extensions

CDAS will stop applying rules on first match (if any).

- **Email Size Restrictions** have a higher priority than domain rules. CDAS will still block mails that exceed 'Email Size Restriction' regardless of any rules.
- **Email Blocked Extensions** have a lower priority than domains rules. CDAS will not stop mails containing a blocked extension if there is a whitelist rule which green-lights the message.
- Whitelist domains rules take precedence over blacklist domain rules.
- Whitelist/blacklist rules in the domain rules section take precedence over 'per user' whitelist/blacklist rules.

### Examples

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sender Whitelist</strong></td>
<td>Always allow mail received from these senders.</td>
</tr>
<tr>
<td><strong>Recipient Blacklist</strong></td>
<td>Always block mail sent to these recipients.</td>
</tr>
<tr>
<td><strong>Sender Blacklist</strong></td>
<td>Always block mail received from these senders.</td>
</tr>
<tr>
<td><strong>Whitelist senders per user</strong></td>
<td>Always allow mail from specific email addresses to specific users.</td>
</tr>
<tr>
<td><strong>Blacklist senders per user</strong></td>
<td>Always block mail from specific email addresses to specific users.</td>
</tr>
</tbody>
</table>

You can bulk import email addresses from .csv or add manually.

If you are troubleshooting issues with a particular email address, please check all interfaces listed under ‘Domain Rules’. Rule priorities can be summarized as follows:

1. Email Size Restriction
2. Domain Whitelist rules
3. Sender/Recipient Whitelist
4. Domain Blacklist rules
5. Sender/Recipient Blacklist
6. TLD & gTLD blacklist rule
7. Per user White list
8. Per user Black list
9. Email Blocked Extensions

CDAS will stop applying rules on first match (if any).

- **Email Size Restrictions** have a higher priority than domain rules. CDAS will still block mails that exceed ‘Email Size Restriction’ regardless of any rules.
- **Email Blocked Extensions** have a lower priority than domains rules. CDAS will not stop mails containing a blocked extension if there is a whitelist rule which green-lights the message.
- Whitelist domains rules take precedence over blacklist domain rules.
- Whitelist/blacklist rules in the domain rules section take precedence over ‘per user’ whitelist/blacklist rules.

Click the following links for more details.

- [Rules](#)
- [TLD and gTLD Rules](#)
- [Recipient Whitelist](#)
• Sender Whitelist
• Recipient Blacklist
• Sender Blacklist
• Whitelist Senders Per User
• Blacklist Senders Per User

Rules

Administrators can create rules to filter inbound mails based on sender, recipient, source and relay/MTA server, subject line, attachments and so on. There are three types of filtering rules:

• **Blacklist rule** - Blocks inbound mails based on one or more filter criteria. Criteria include sender, recipient, mail servers/relays and specific subject line.

• **Whitelist rule** - Allows mails to pass through, without security checks, based on one or more filter criteria. Criteria include sender, recipient, mail servers/relays and specific subject line.

• **Forward rule** - Forwards mails based on one or more filter criteria, to a set email address. Criteria include sender, recipient, mail servers/relays and specific subject line.

For example, you can create rules to block all mails from a specific mail server, allow all mails from a specific sender to a specific recipient, forward all mails containing a specific text string in the subject line and so on.

**To open the 'Create Rule' interface**

- In the left-hand menu, click 'Domain Rules' > 'Create Rule'
- The 'Create Rule' interface will open:

The 'Create Rules' interface shows all current mail filtering rules and their parameters.

<table>
<thead>
<tr>
<th>Column Header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Type</td>
<td>Whether the rule is for blacklisting, whitelisting or forwarding.</td>
</tr>
<tr>
<td>Sender</td>
<td>The sender whose mails will be intercepted by the rule.</td>
</tr>
<tr>
<td>Recipient</td>
<td>The recipient whose mails will be intercepted by the rule.</td>
</tr>
<tr>
<td>Received from</td>
<td>External mail server that sent the mail.</td>
</tr>
<tr>
<td>Received by</td>
<td>Mail server which received the mail.</td>
</tr>
<tr>
<td>Subject</td>
<td>Mails containing the subject line in this column will be intercepted by the rule.</td>
</tr>
<tr>
<td>Forward to</td>
<td>The email address to which mails satisfying the conditions are forwarded. This column only applies only to 'Forward' rules.</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Suspicious attachment</td>
<td>Whether or not the rule should apply only to mails containing suspicious attachments</td>
</tr>
</tbody>
</table>

**Sort the Entries**

- Click any column header to sort rules in the ascending/descending order of the entries in that column. Does not apply to the 'Suspicious attachment' column header.

**Use 'Filters' to search rules**

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

  - Select the field from the first drop-down, choose the condition from the second drop-down and enter the search criteria in the third field.

To add more filters, click +.

To remove a filter, click the icon beside it.

Available filters are:

- **Rule Type** - Filters rules based on type selected from the right drop-down and the condition selected in middle drop-down.
- **Sender** - Filters rules based on sender’s email address entered in part or full, in the right text field and condition chosen from the middle drop-down.
- **Recipient** - Filters rules based on recipient's user name entered in part or full, in the right text field and condition chosen from the middle drop-down.
- **Received from** - Filters rules based on hostname or IP address of external mail server entered in part or full, in the right text field and condition chosen from the middle drop-down.
- **Received by** - Filters rules based on hostname or IP address of internal mail server entered in part or full, in the right text field and condition chosen from the middle drop-down.
- **Subject** - Filters rules based on subject line entered in part or full, in the right text field and condition chosen from the middle drop-down.
- **Forward to** - Filters rules based on forward email address entered in part or full, in the right text field and condition chosen from the middle drop-down.
• **Suspicious attachment rule** - Filters rules created for suspicious attachment based on condition chosen from the middle drop-down and option from the checkbox at the right.
  - Click 'Apply Filter' after selecting the filters and selecting the conditions to view the filtered results.
  - To close the 'Filters' area, click anywhere on the 'Filters' stripe.
  - To remove the filters and to view all the rules, choose the 'Filters' area then button

**Create a new mail filter rule**
- Click the 'Add' button.
- This will open the 'Add blacklist rule' dialog:

**Suspicious attachment rule**
- By default, all mails containing suspicious attachments will be quarantined by CDAS.
- A 'Suspicious attachment rule' lets you define specific actions if a malicious attachment is found in a mail.
- For example, you may want mails with a suspicious attachment from a specific sender, addressed to a particular recipient to be forwarded to a certain email address.
- Note. Enabling 'Suspicious attachment rule' means the rule only applies to mails which meet your conditions AND contain a suspicious attachment. It will not intercept mails which meet the conditions but do not contain a suspicious attachment.

**Rule type** - Select the rule type. The available options are:
- BLACKLIST - All mails with fields satisfying the parameters entered in the options below, will be blocked.
• **WHITELIST** - All mails with fields satisfying the parameters entered in the options below, will be passed without security checks.

• **FORWARD** - All mails with fields satisfying the parameters entered in the options below, will be forwarded to the email address entered in the 'Forward email' field.

• **Sender** - Enter the email address of the sender, mails sent by whom are to be intercepted by the rule. You can use wildcard characters (*, ?) to enter username/domain name in part, so that all mails containing sender address with partial text entered in this field will be intercepted. For example, entering "@hell.com" intercepts mails from all users from the domain name 'hell.com', entering 'evilspirit@*', processes all mails with sender name 'evilspirit' from any domain and entering '*' intercepts all the mails with parameters entered in the fields below.

• **Recipient** - Enter the username part of the email address of the recipient, mails sent to whom are to be intercepted by the rule. The domain name part will be auto-populated with the domain name from which the rule is created. You can use wildcard characters (*, ?) to enter username in part, so that all mails containing 'To' address with partial text entered in this field will be intercepted.

• **Received from** - Enter the hostname or IP address of the external mail server, mails sent from which, are to be intercepted by the rule. You can use wildcard characters (*, ?) to enter server name in part. For example, entering 'mailxxx*' will intercept all mails that contain "mailxxx" in part in the 'Received From' field of the mail header. To specify all sender mail servers, enter just the wildcard character.

• **Received by** - Enter the primary relay of the sending server or the MTA, mails sent through which, are to be intercepted by the rule. You can use wildcard characters (*, ?) to enter server name in part. For example, entering 'mailyyy*' will intercept all mails that contain "mailyyy" in part in the 'Received By' field of the mail header. To specify all mail servers, enter just the wildcard character.

• **Subject** - Enter the subject line, so that the system displays all quarantined mails that contain the words entered in the text box. Please note this field doesn't support wildcards.

• **Forward email** - This field is available only for 'FORWARD' rule. Enter the email address to which the emails containing values in the email header as configured in the fields above are to be forwarded.

  • Click 'Save' to add the rule to the list of rules.

To edit a rule

  • Select the rule to be edited and click the 'Edit' button from the top.
The 'Edit filter rule' dialog will appear for the rule. This dialog is similar to the 'Add rule' dialog. For descriptions of the options in this dialog, please see the explanation above.

- Edit the values in the fields as required and click 'Save'.

**To remove a rule**

- Select the rule you want to remove and click the 'Delete' button.
A confirmation dialog will appear.
- Click ‘OK’ to remove the rule.

**TLD and gTLD Rules**

- CDAS allows administrators to restrict mails based on the top level domain name (TLD) of the external mail server.
- By default CDAS accepts mails from servers with all TLD names.
- Administrators can choose to allow mails only from selected TLDs and block mails from others.
- Administrators can also add custom TLDs and configure to accept or block mails from them.

**To open the TLD and gTLD Rules interface**

- Click ‘Domain Rules’ > ‘TLD & gTLD Rules’ in the left-hand menu.
- The TLD configuration interface will open:
The ‘Accepted domains’ interface categorizes TLDs according to location and gTLDs by alphabetical grouping. These categories are shown in the column headers and are known as ‘Rule Groups’.

- All TLDs are enabled (accepted) by default.
- You can disable TLDs/gTLDs from which you do not want to accept mail.

The interface also allows you to:

- Add new custom TLDs
- Configure TLD based mail filtering

To add a new custom TLD

- Click ‘Add’ from the Accepted domains interface
The 'Add filter rule dialog' will appear.

- Choose the category from the 'Rule group' drop-down
- Enter the TLD name, without the '.' prefix, in the 'Domain suffix' text field
- Click 'Save' to add the TLD to the list
  - To allow mail from mail servers with the new TLD, leave it selected
  - To block the mails from the mail servers with the new TLD, de-select it.

**To configure TLD based mail filter**

- Deselect TLDs from which you want to block mail. Enable TLDs from which you want to accept mail.

**Recipient Whitelist**

Since all filtering for whitelisted recipients is disabled, we recommend you use this option only in special circumstances. For example - abuse@domain.com and postmaster@domain.com

The recipient whitelist interface lets you:

- **Add users to recipient whitelist**
- **Export the list to CSV file for use in future**
- **Remove users from recipient whitelist**
- **Reset the list** - Delete all whitelisted recipients except the default recipients by clicking the 'Reset to default' button

**To configure recipient whitelist**

- Click 'Domain Rules' > 'Recipient whitelist' in the left-hand menu.

![Recipient whitelist interface](image)

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

**Add Users to Recipient List**

You can add recipients to the whitelist in the following ways:
- **Manually add recipients**
- **Import recipients from a CSV file**

To manually add recipients:

- Click 'Domain Rules' > 'Recipient whitelist' in the left-hand menu.
- Click 'Add' to add a new user to the list.

The 'Add' dialog 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 the whitelist, prefix or suffix the wildcard "*" in the E-mail text field. For example, enter "*.stores" for all the recipients in stores department to be whitelisted.
- To add a whole domain to whitelist, enter the wildcard "*" in the E-mail text field and click the 'Save' button. Now all the recipients in that domain will be whitelisted.

The recipient's name will be added to the list.
To import users from CSV file

Administrators can import many users to the recipient whitelist from a .csv file. Users should be specified in the following format:

user1@testdomain
user2@testdomain
user3@testdomain

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

The 'Upload' dialog will open:

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

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

- Click the 'Remove import task' button. If the task is in progress, 'Remove import task' deletes only the remaining part of the task.

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

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

**Export the Recipient Whitelist to CSV file**

You can save the configured recipient whitelist by exporting it as a CSV file. If required in future, administrators can import users from the csv file (for example, for a new account or after a reset).

To export the list
• Click the ‘Export to CSV file’ button to save the list of whitelisted recipients as a CSV file.

A file download dialog will be displayed.
• Click ‘OK’ and navigate to the location in your computer and save the file or the file will be downloaded to your download folder.

**Delete Users from the Recipient Whitelist**

• Select the recipient from the list and click the ‘Delete’ button.
Click 'OK' to confirm your changes.

**Sender Whitelist**

- All filtering is disabled on mail sent by white-listed senders to recipients at the selected domain.
- The only exception is that mail from a white-listed sender which contains a suspicious attachment will still be blocked UNLESS the ‘Suspicious attachment rule’ is enabled. This may seem counter-intuitive on first reading.
- The following table shows how the ‘Suspicious Attachment’ option affects a sender white-list rule:

<table>
<thead>
<tr>
<th>Rule Type 1</th>
<th>Suspicious Attachment option</th>
<th>Suspicious file detected?</th>
<th>White-listing applied?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enabled</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Rule Type 2</td>
<td>Disabled</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- Use Type 1 if you want all mails from a sender to be whitelisted and received, including those that contain suspicious attachments.
- Use Type 2 if you want to white-list all mails from a sender except those that contain suspicious attachments.

See the **Rules** section if you need more details.

Comodo strongly recommends white-listing a sender only when the system wrongly blocks emails from a trusted sender. White-listing a sender over-rules ‘Blacklist senders per user’. See **Blacklist Senders Per User** for more details.

- **Add users to Sender whitelist**
- **Export the list to CSV file for use in future**
- **Remove users from Sender whitelist**
To configure sender whitelist

- Click 'Domain Rules' > 'Sender Whitelist' in the left-hand menu.

The 'Sender whitelist' interface of the selected domain will be displayed:

Add Users to Sender Whitelist

You can add recipients to a white list in two ways:

- **Manually add senders**
- **Import senders from a CSV file**

**To manually add senders**

- Click 'Add' to open the add whitelisted sender dialog:

  ![Add whitelisted sender dialog](image)

  - Enter the sender name in the 'E-mail' text-box and sender's email domain name after the @ symbol and click the 'Save' button. Repeat the process to add more whitelisted senders.
  - To add a particular set of senders to whitelist, prefix or suffix the wildcard character * in the 'E-mail' text field and senders' email domain name after the @ symbol. For example, enter *stores.com for all the senders in stores department to be whitelisted.
• To add a specific username from any mail domain to the whitelist, enter the username in the mail text field and the wildcard character * after the @ symbol. For example, enter john@* for whitelisting the username 'john' with any email domain name.

• To add a set of users or specific username from any email domain with a specific top level domain (TLD) name like .com, .org, enter the wildcard character * or username in the Email text field and enter * followed by the TLD after the @ symbol. For example, '*@*.com' will whitelist all the senders from all the email domains ending with '.com'.

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

The list of whitelisted senders will be displayed.

![Sender whitelist](image)

To import senders to whitelist from CSV file

Administrators can import multiple senders from a .csv file. The senders' addresses should be saved in the following format:

sender1@domainname1
sender2@domainname2
sender3@domainname3

• Click the 'Import from CSV file' to import senders to whitelist from a CSV file.
• Click 'Upload', navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.

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

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, the results will be displayed.
The sender whitelist from .csv file will be uploaded and the administrator who carried out the task will receive a notification about the import task completion.

**Export the Sender Whitelist to CSV**

- Click 'Export to CSV file' to save the list of whitelisted senders as a CSV file
A file download dialog will be displayed.

- Click "OK" and navigate to the location in your computer and save the file or the file will be downloaded to your download folder.

**Delete Users from the Sender Whitelist**

- To delete a sender from the whitelist, select the sender from the list and click the 'Delete' button.
• Click ‘OK’ to confirm your changes.

**Recipient Blacklist**

• CDAS will automatically block all emails to blacklisted recipients.
• Blocked messages will not be quarantined and legitimate SMTP mail servers will send a bounce message to the sender.

Administrators can:

• **Add users to the recipient blacklist**
• **Export the list to CSV file for use in future**
• **Remove users from recipient blacklist**
• **Reset the list** - Remove all senders from the blacklist by clicking the ‘Reset to default’ button

**To configure recipient blacklist**

• Click the ‘Recipient blacklist’ from the ‘Domain Rules’ drop-down on the left

The ‘Recipient blacklist’ interface of the selected domain will be displayed:
Add Users to Recipient Blacklist

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

- **Manually add the recipients**
- **Import recipient from a CSV file**

**To manually add recipients**

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

The 'Add' 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 multiple users to the recipient blacklist from a .csv file. Users should be specified in the .csv in the format shown below:

user1@testdomain
user2@testdomain
user3@testdomain

• Click the 'Import from CSV file' button to import users to blacklist from a CSV file.
Click 'Upload', navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.

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

**To remove the upload from the queue**

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

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

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

**Export the Recipient Blacklist to CSV file**
Administrators can save the recipient blacklist by exporting it as a CSV file. If required in future, the administrator can import the users from the csv file, for example for a new account or after a reset.

**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 ‘OK’ and navigate to the location in your computer and save the file or the file will be downloaded to your download folder.

**Delete Users from the Recipient Blacklist**

- Select the recipient from the list and click the ‘Delete’ button
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 CDAS.

**Sender Blacklist**

- CDAS will automatically block all emails from blacklisted senders.
- Blocked messages will not be quarantined and most mail servers will send a bounce message to the sender.

The sender blacklist interface allows admins to:

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

**To configure sender blacklist**

- Click the 'Sender blacklist' from the 'Domain Rules' drop-down on the left

The 'Sender blacklist' interface of the selected domain will be displayed:
Adding Users to Senders Blacklist

You can add senders to blacklist in two ways:

- Manually adding the senders
- Importing from a CSV file

To manually add senders

- Click 'Add' to add a new blacklisted sender

The 'Add' dialog box will be displayed:

- Enter the sender name in the 'E-mail' textbox and sender's email domain name after the @ symbol and click the 'Save' button. Repeat the process to add more blacklisted senders.
• To add a particular set of senders to blacklist, prefix or suffix the wildcard character * in the 'E-mail' text field and senders' email domain name after the @ symbol. For example, enter *stores.com for all the senders in stores department to be blacklisted.

• To add a specific username from any mail domain to the blacklist, enter the username in the mail text field and the wildcard character * after the @ symbol. For example, enter john@* for blacklisting the username 'john' with any email domain name.

• To add a set of users or specific username from any email domain with a specific top level domain (TLD) name like .com, .org, enter the wildcard character * or username in the Email text field and enter * followed by the TLD after the @ symbol. For example, '*@*.com' will whitelist all the senders from all the email domains ending with '.com'.

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

• 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
sender2@domainname2
sender3@domainname3

• Click the 'Import from CSV file' to import senders to blacklist from a CSV file.
• Click 'Upload', navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.
The upload will be placed in import tasks queue and the progress of the upload will be displayed.

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, the results will be displayed.
The sender blacklist from .csv file will be uploaded and the administrator who carried out the task will receive a notification about the import task completion.

**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 "OK" and navigate to the location in your computer and save the file or the file will be downloaded to your download folder.

**Deleting Users from the Sender Blacklist**

- Select the sender from the list and click the 'Delete' button.
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 CDAS.

**Whitelist Senders Per User**

- Admins can permit certain senders for specific recipients - even if those senders are blacklisted elsewhere/for other users.
- Senders can be manually whitelisted for a specific recipient, or can be imported from .csv. They can also be added after a user request.
- All filtering is disabled for whitelisted senders to specific recipients.
- Comodo strongly recommends you only use this option after analyzing the request is genuine and warranted.

**To configure sender whitelist per user**

- Click 'Domain Rules' > 'Whitelist senders per user' in the left-hand menu.
The 'Whitelist senders per user' interface will be displayed:

![Whitelist senders per user interface](image)

**WhiteList senders per user**

- **Add**
- **Delete**
- **Import from CSV file**
- **Export to CSV file**

Filters

- **Sender**
  - p@eter@cioc team.das.comodo.od.ua
  - bob@doc team.das.comodo.od.ua

<table>
<thead>
<tr>
<th>Sender</th>
<th>Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>peter@cioc team.das.comodo.od.ua</td>
<td>peter</td>
</tr>
<tr>
<td>bob@doc team.das.comodo.od.ua</td>
<td>bob</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Page</th>
<th>1</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
</table>

[1-2/2]
Sort Entries

- Click any column header to sort entries in ascending/descending order of the entries in the column.

Use Filters to search senders and recipients

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

To narrow your search, add more filters by clicking +

To remove a filter, click the icon beside it.

Available filters are:

- **Sender**: Will execute a search of senders according to the text in the text box (column 3) and the condition selected in column 2.
- **Recipient**: Will execute a search of recipients according to the text in the text box (column 3) and the condition selected in column 2.

The following conditions are available:
Comodo Dome Antispam MSP - Administrator Guide

- **Equals**: Displays all senders / recipients that match the text entered in the text box.
- **Not Equals**: Displays all senders / recipients except the one entered in the text box.
- **Contains**: Displays all senders / recipients that contain the words entered in the text box.
- **Not Contains**: Displays all senders / recipients that do not contain the words entered in the text box.
- **Starts With**: Displays all senders / recipients that start with the words entered in the text box.
- **Ends With**: Displays all the senders / recipients 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' to close the filters area.

Click the **Refresh** button to display all users.

**Note**: To display all the Whitelist senders 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.

From this interface administrators can:

- Add senders to whitelist per user
- Export the list to CSV file for use in future
- Remove senders from Whitelist senders per user list

**Add Senders to Whitelist Per User**

You can add senders to whitelist in the following ways:

- Manually add senders
- Import senders from a CSV file
- Add from a 'Whitelist request' from a user

**Manually add senders**

Administrators can manually specify the whitelisted sender and corresponding recipient as follows:

- Click 'Add' to add a new sender to the list. The 'Add sender' dialog box will be displayed:
- Enter the sender's username in the email textbox and sender's email domain name after the @ symbol in the first row.
- Enter the recipient's name in the Recipient text box in the second row. **Note:** The recipient should be a valid user.
- Click 'Save' button. Repeat the process to add more whitelisted senders for the user.

The list of whitelisted senders will occur.
Import senders from a CSV file

Administrators can import a multiple senders at a time from a comma separated values (CSV) file to Sender whitelist per user. The list of whitelisted senders and respective recipients can be created using notepad or a spreadsheet application like MS Excel or OpenOffice Calc and saved in .csv format. Each line in the .csv file should contain the sender's email address and the username of the recipient or sender's email address and the recipient's email address, separated by a comma. An example is shown below:

sender1@anydomain.com, recipient1
sender2@anydomain.com, recipient2@domain.com
sender3@somedomain.com, recipient3

To import senders to whitelist from CSV file

- Click the 'Import from CSV file' from the 'Whitelist senders per user' interface.

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

The upload will be placed in import tasks queue and the progress of the upload will be displayed. If you want to remove the upload from the queue, click the 'Cancel import from the CSV file' button. The 'Cancel import from the CSV file' deletes only a remaining part of not imported task.
On completion of the upload process, the results will be displayed.

The sender whitelist per user from .csv file will be uploaded and the administrator who carried out the task will receive a notification about the import task completion.

**Add from Whitelist requests from users**

The administrator can add senders to whitelist based on the requests of the users. See Email Management > Whitelisted Requests for more details.

**Export the Whitelist senders per user list to CSV file**

The administrator can save the whitelist senders per user list by exporting it as a CSV file. If required in future, the administrator can import the users from the csv file, for example for a new account or after a reset.

**To export the list**

- Click the ‘Export to CSV file’ button to save the list of whitelisted senders per user as a CSV file
A file download dialog will be displayed.

- Click 'OK' and navigate to the location in your computer and save the file or the file will be downloaded to your download folder.

Delete Senders from Whitelist

- To delete a sender from the whitelist, select the sender from the list and click the 'Delete' button.
• Click 'OK' in the confirmation dialog.

**Blacklist Senders Per User**

• Allows admins to prevent certain senders from sending mail to specific users.
• This feature is useful in scenarios where you want to allow mails from a particular sender to all users in the domain but want to block the sender for a particular recipient in the domain.
• Senders can be added manually, imported from .csv and from a user request.

**To configure sender blacklist per user**

• Click 'Domain Rules' > 'Blacklist senders per user' in the left-hand menu:

The 'Blacklist senders per user' interface will be displayed:
Use Filters to search senders and recipients

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

To add more filters, click +

To remove a filter, click the icon beside it.

Available filters are:
Sender: Will execute a search of senders according to the text in the text box (column 3) and the condition selected in column 2.

Recipient: Will execute a search of recipients 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 senders / recipients that match the text entered in the text box.
- **Not Equals**: Displays all senders / recipients except the one entered in the text box.
- **Contains**: Displays all senders / recipients that contain the words entered in the text box.
- **Not Contains**: Displays all senders / recipients that do not contain the words entered in the text box.
- **Starts With**: Displays all senders / recipients that start with the words entered in the text box.
- **Ends With**: Displays all the senders / recipients 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 stripe to close the filters area.
- Click the button to display all users.

**Note:** To display all the Blacklist senders 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.

From this interface you can:

- Add senders to blacklist per user
- Export the list to CSV file for use in future
- Remove senders from blacklist senders per user list

**Adding Senders to Blacklist Per User**

You can add senders to blacklist in the three ways:

- Manually add senders
- Import senders from a CSV file
- Add senders from Blacklist requests from users

**Manually add senders**

The administrator can manually specify the senders to be whitelisted for specific recipients, one-by-one to be added.

**To manually add senders to blacklist per user basis**

- Click 'Add' to add a new sender to the list.

The 'Add sender' dialog box will be displayed:
Enter the sender's username in the E-mail textbox and sender's email domain name after the @ symbol in the first row.

Enter the recipient's name in the Recipient text box in the second row. **Note:** The recipient should be a valid user.

Click 'Save' button. Repeat the process to add more blacklisted senders for the user.

The list of blacklisted senders will be displayed.

---

**Import senders from a CSV file**

Administrators can import a multiple senders at a time from a comma separated values (CSV) file to Sender blacklist per user. The list of blacklisted senders and respective recipients can be created using notepad or a spreadsheet application like MS Excel or OpenOffice Calc and saved in .csv format. Each line in the .csv file should contain the sender's email address and the username of the recipient or sender's email address and the recipient's email address, separated by a comma. An example is shown below:
sender1@anydomain.com, recipient1
sender2@anydomain.com, recipient2@domain.com
sender3@somedomain.com, recipient3

To import senders to Blacklist from CSV file

- Click the 'Import from CSV file' from the 'Blacklist senders per user' interface. The 'Upload' dialog will appear.

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

The upload 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 'Cancel import from CSV file' button. The 'Cancel import from CSV file' deletes only a remaining part of not imported task.
On completion of the upload process, the results will be displayed.

The sender blacklist per user from .csv file will be uploaded and the administrator who carried out the task will receive a notification about the import task completion.

**Adding senders from Blacklist requests from users**
The administrator can add senders to blacklist based on the requests of the users. Refer to the section Email Management > Blacklisted Requests for more details.

**Exporting the Blacklist senders per user list to CSV file**

The administrator can save the blacklist senders per user list by exporting it as a CSV file. If required in future, the administrator can import the users from the csv file, for example for a new account or after a reset.

**To export the list**

- Click the 'Export to CSV file' button to save the list of blacklisted senders per user as a CSV file.

A file download dialog will be displayed.

- Click 'OK' and navigate to the location in your computer and save the file or the file will be downloaded to your download folder.

**Delete Senders from the Blacklist**

- To delete a sender from the blacklist, select the sender from the list and click the 'Delete' button.
3.2.1.1.5.7 Account Management

The 'Account Management' interface allows you to manage users for a selected domain. Admins can reset passwords for users, allow or deny access to user accounts, import users from .csv file and import users from Active Directory (AD) servers.

Administrators can also view users' login history. See User History for more details.

Click the following links for more details:

- Users
- User auto-import
- Users history
- Importing Users from LDAP

3.2.1.1.5.7.1 User Account Management

The 'Users' area allows admins with appropriate privileges to manage users for a selected domain. This includes adding/importing users, deleting users, editing user accounts, resetting passwords and configuring user permissions. Admins can also configure email aliases from this interface.

- Click 'OK' in the confirmation dialog.
Click the following links for more details:

- Managing Users
- Adding New Users
- Deleting Users
- Editing Users
- Unlocking Users
- Importing from CSV file
- Managing Permissions
- Aliases
- Moving to Aliases
- Importing Aliases from CSV file
- Forwarding mails to another user
- Other actions

**Manage Users**
• Click 'Account management' on the left then click 'Users':

The 'Users' interface of the selected domain will be displayed.
Sort the Entries

- Click any column header to sort items in ascending/descending order of the entries in that column.

The sorting option is not available for 'Aliases' and 'Group' columns.

**Use filters to search for users**

- Click anywhere on the 'Filters' stripe 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:
**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.

**Alias username:** Will execute a search of user alias name according to the text in the text box (column 3) and the condition selected in column 2.

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

- **Contains:** Displays all users with alias name(s) that contain the words entered in the text box.
- **Equals:** Displays all users with alias names that match the text entered in the text box.
- **Not Equals:** Displays all users except those with the alias name entered in the text box.
- **Not Contains:** Displays all user alias name(s) that do not contain the words entered in the text box.
- **Starts With:** Displays all user alias name(s) that start with the words entered in the text box.
- **Ends With:** Displays all the user alias name(s) that end with the words entered in the text box.

**Alias Domain:** Will execute a search of domain alias name according to the text in the text box (column 3) and the condition selected in column 2.

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

- **Contains:** Displays all users with domain alias name(s) that contain the words entered in the text box.
- **Equals:** Displays all users with domain alias names that match the text entered in the text box.
- **Not Equals:** Displays all users except those with the domain alias name entered in the text box.
- **Not Contains:** Displays all user domain alias name(s) that do not contain the words entered in the text box.
- **Starts With:** Displays all user domain alias name(s) that start with the words entered in the text box.
- **Ends With:** Displays all the user domain alias name(s) that end with the words entered in the text box.

**Forward to:** Will execute a search of forwarded to user names according to the text in the text box (column 3) and the condition selected in column 2.

When you select this option in the first drop-down, the following filters 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.

**Group:** Will execute a search of users belonging to the user group selected from the drop-down in the third column and the condition selected in column 2.

When you select this option in the first drop-down, the following filters are available:
• **Equals**: Displays all users from the group selected from the third drop-down.
• **Not Equals**: Displays all the users excluding those belonging to the group selected from the third drop-down.

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' to close the filters area.

Click the **Refresh** button to display all users.

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

**To add a new user**

• Click the 'Add' button.

The 'New user' dialog will be displayed:

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

By default, the user will be enabled.

- Clear the 'Enabled' box to deny the new user access to CDAS. 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**.

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

- Deselect the 'Send quarantine reports' box to disable this option.
- Select the 'Send invitation' box to send an invitation mail to the email recipient address entered in the 'Username' text box.
- Select 'Non human' if the address is a no-reply or common mailing list such as 'sales@...'
- Select 'Public email' if the address is published somewhere, for example on a customer facing website. Enabling this box will allow CDAS to more accurately filter spam for this type of email address.
- Click the 'Save' button.

**Note**: If the user is disabled and subscribed for periodical Quarantine Reports, the subscription will also be canceled.

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

**Note**: The number of users that can be added depends on the plan subscribed by you and the maximum number of users limit configured for the domain in the **Add Domains / Edit Domains / Domain Settings** interfaces. When you exceed the limit of users, the following will be displayed while adding a new user.

![Warning Image]
To delete an existing user

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

- Click 'OK' to confirm your changes.

The user(s) will be removed from the list.

To edit an existing user

You can select to allow or deny permission for the users to access their CDAS 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 will appear.
Enabled - Allows the user to access the CDAS interface.

Whitelist email - Adds the user to the Recipient Whitelist.

Disable 'Send quarantine reports' checkbox, if you do not want the user to get quarantine reports. By default it is enabled.

Click the 'Save' button to confirm your changes.

**Note:** Any active subscriptions or scheduled reports for the user will be automatically canceled if access to CDAS is disabled.

**To unlock users**

Users who try to login to CDAS with wrong credentials will be automatically locked after three unsuccessful attempts. They will be able to try again only after 30 minutes from the time of lockout. CDAS administrators can unlock these users immediately without waiting for the timeout period to end, so that the users can try to login again to CDAS.

The locked out users will be displayed with a lock icon beside them.

- Select the locked user from the list and click the 'Unlock' button.

A confirmation dialog will be displayed.
• Click 'OK' to unlock the selected locked user.
The user now can try to login again without waiting for the lockout time period to end.

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

• To import new users from a CSV file click 'More actions' > 'Import from CSV file'

The 'Upload' dialog will be displayed.
Click the 'Upload' button and navigate to the location where the file is saved and click the 'Open' button. The upload progress will be displayed...

...and when completed, the results will be displayed.
**Note:** The number of users that can be added depends on the plan subscribed by you and the maximum number of users limit configured for the domain in the Add Domains / Edit Domains / Domain Settings interface. CDAS will stop importing users after the number of users allowed for the account is reached and a warning will be displayed.

**Managing Permissions for users**

CDAS allows you to assign permissions to users that will determine what they can and cannot do in CDAS - MSP. Administrators can create policies and assign them to users from this interface. See 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 a user**

- Select the user(s) and click ‘More actions’ > ‘Manage permissions’

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

- Select the group from the list.
The permissions set for this group will be displayed on the right.

- Click the 'Assign to selected users' button to set permissions for selected user or multiple users.
- Click 'Assign to filtered users' button to set permissions for selected group to all users or to all users found by filter.
- Click 'OK' in the confirmation window.

The selected user(s) will be assigned to the group and successfully assigned message will be displayed.
The interface also displays the new group assigned for the selected user under the 'Group' column.

**Add the user aliases**

CDAS allows admins to add a user alias name to organize emails related to different groups or functions into a single email inbox automatically. The users can protect their real email address.

- Select a user and click 'More actions' > 'Aliases' to add user aliases.

  - Enter the full email alias address of the user. **Note:** The alias email address must be of any domain belonging to the account.
Click the Save button.

**Note:** Users cannot add an alias by themselves.

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

After adding a user to an alias, admins can extract him/her as a user.
- Click the 'Aliases' button after selecting the user.

In the 'User Aliases' dialog next to the added alias row, the 'Extract as user' button will be displayed.

- Click the 'Extract as user' button.

The confirmation dialog will be displayed.

- Click 'OK'

The user extracted from the 'User Aliases' dialog box will be added to list of users in the respective domain added as alias and will be placed in the default group.
**Note:** The number of users that can be added for an account depends on the plan subscribed by you. When you exceed the limit of users, a warning will be displayed.

### Moving user account to aliases

CDAS allows admins to move an existing user as an alias for another user for any domain available in your account.

- Select the user then click 'More actions' > 'Move to aliases'

- Type the full email address of the user for whom the alias has to be added. **Note:** The user and domain should be valid and belong to your account.
Click the 'Save' button.

Now, the selected user has become an alias of another user. (This could be for the same domain or another domain belonging to your account.)

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`

**To assign alias for users from a CSV file**

- Click 'More actions' > 'Import alias from CSV file'
The 'Upload' dialog will be displayed.

![Upload Dialog](image)

**Upload csv file.**
Each line should be in the next format: alias [csv user list].

**For example**

```
alias@testdomain user1, user2@domain2
```

When domain name is not mentioned - user will be added to the current domain to alias name.
When such user does not exist - user will be created.

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

The upload progress will be displayed.
...and when completed, the results will be displayed.

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

**Forwarding mails to another user**

CDAS allows administrators to add a forwarding address for a user. This is useful when a user is on vacation or unavailable for sometime but the mails addressed to him should be attended immediately. Please note the forwarded user should also be in the same domain.

- Select the user whose mails have to be forwarded to another user and then click 'More actions' > 'Forward to'

The 'Forward settings...' dialog will be displayed:

The 'Forward settings...' dialog will be displayed:
Select the ‘Enable forwarding’ check box

Enter the user name of the recipient to whom the mails have to be forwarded in the ‘Forward all user messages to’ field

Click the ‘Save’ button

The forwarded user will be added and a success message will be displayed.

The incoming mails of the selected user will be automatically forwarded to the added user in the domain. When the selected user logs in to his/her CDAS account, an alert will be displayed at the top of the interface.

To remove the forwarded mail address for a user, select the user, click ‘More actions’ > ‘Forward to’

The ‘Forward settings...’ dialog will be displayed:
**Comodo Dome Antispam MSP - Administrator Guide**

- Deselect the 'Enable forwarding' check box
- Delete the username in the 'Forward all user messages to' field
- Click the 'Save' button

The forwarded user will be removed and a success message will be displayed.

**Other Actions**
- To allow user to access to CDAS interface, click the 'More actions' > 'Enable'. A confirmation dialog will be displayed.
- If you want to allow access to user selected by applying filter, apply filters and click 'More actions' > 'Enable by filter'. A confirmation dialog will be displayed.
- Click the 'More actions' and select the 'Regenerate password'. The password will be reset for the user in case it is forgotten. The new password will be sent to the user's email automatically. The user has to use this new password to access CDAS. A confirmation dialog will be displayed.
- To send invitation to new created users, select users and click 'More actions' > 'Send invitation'. A confirmation dialog will be displayed.

**3.2.1.5.7.2 Manage User auto-import**

CDAS can automatically import users belonging to a managed domain after receiving the first mail addressed to the user.

- Each new user will be imported in around 30 minutes and sent an invitation mail containing an activation link and credentials for their CDAS user account.
- New users can activate their CDAS account by clicking the link in the invitation mail or by logging-in to CDAS with the credentials provided in mail.
- Administrators have the option to receive a notification whenever a new user is auto-imported into CDAS
- The 'User auto-import' interface allows administrators to enable and configure the auto-import feature.

**To access the User Auto-Import interface**

- Open the 'Domains' interface and select the domain you wish to configure
- Click the 'Manage Domain' button to open the 'Domain Management' interface.
- Select 'Account management' on the left then choose 'Users auto-import'
The 'Users auto-import' interface will open:

- **Enable auto-import** - Select this option to activate the feature.
- **Automatically enable imported users** - Allows all auto-imported users to access their CDAS user account.
- **Send invitation to imported users** - Sends invitation mails to newly imported users. The mail will contain the activation link and their login credentials.
- **Notify administrators about imported users** - Select this option if admins should be notified whenever a new user is auto-imported. You can specify administrators (including self) to whom the notification mails are to be sent in the 'Notification recipients' box. The notification contains the imported user name and the domain name.
- **Notification recipients** - Enter the email addresses of admins to whom notification emails should be sent. You can enter multiple address, separated by commas.

![Image](Dashboard/ Domains / Domain dashboard _ docleamcass.comodo.ua / Users auto-import)

- Click 'Save' for your settings to take effect.

### 3.2.1.5.7.3 View User History

The 'Users History' area contains a log of user activities on CDAS. You can filter users by IP address, last login, domain, username and/or location.

**Note:** This interface will only show user connections to the current domain (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' sub tab).

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

**To view user history**

- Open the 'Domains' interface and select a domain
- Click the 'Manage Domain' button to open the 'Domain Management' interface.
- Click 'Account management' on the left then 'Users history'.
The 'Users history' interface of the selected domain will open:

**Sort the Entries**
- Click any column header to sort items in ascending/descending order of the entries in that column.

The sorting option is not available for 'Login Duration' column.

**Use filters to search for users**
- Click anywhere on the 'Filters' stripe to open the filters area.
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 based on the search criteria entered in the third text box and the selected condition.
- **Domain**: Will execute a search of domains based on the search criteria entered in the third text box and the selected condition.
- **IP**: Will execute a search of IP Addresses based on the search criteria entered in the third text box and the selected condition.
- **Location**: Will execute a search of locations based on the search criteria entered in the third text box and the selected condition.

If any of the above options is selected in the first drop-down, the following conditions are available:

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

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

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

If 'Last Login' is selected, the following conditions are available:
• **Equals**: Displays the users whose last login is same as the selected date in the third box from the calendar.

• **Less than**: Displays the users whose last login dates are less than the selected date in the third box from the calendar.

• **Greater than**: Displays the users whose last login dates are 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' to close the filters area.

Click the [Refresh](#) button to display all the users.

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

### 3.2.1.1.5.7.4 Importing Users from LDAP

In addition to adding users manually and importing users from CSV, you can import the users from domain's Active Directory (AD) server.

• CDAS can be configured to import email users from your AD server using the Lightweight Directory Access Protocol (LDAP).

• CDAS periodically synchronizes with the AD server to automatically add or remove users based on changes made to the AD server.

Click the following links for more details:

- **LDAP Import Configuration**
- **LDAP Import Confirmation List**
- **LDAP Import Ignore List**
- **Troubleshooting LDAP**

#### LDAP Import Configuration

The LDAP Import Configuration interface allows you to configure CDAS to import users from the domain’s Active Directory server.

*Comodo strongly recommends that a separate LDAP/AD account be created for the purpose of the CDAS login and that this user account should be allocated read-only permissions.*

**To configure LDAP import**

- Open the 'Domains' interface and select the domain into which you want to import users.
- Click the 'Manage Domain' button to open the 'Domain Management' interface.
- Click 'Account management' on the left and select 'LDAP import configuration'.
The 'LDAP import configuration' interface will open:
Connection Settings

- **Host (IP Address or Name)** - Enter the hostname or external IP address of the AD server. If your organization uses the same physical server AD and the Mail Exchange server, then enter the host name or IP address of the mail server.
- **Port** - Enter the port number of the Active Directory server's LDAP port.
  - 389 is the default port for non-SSL connections ('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. To use secure LDAP, you need to install an SSL certificate from a trusted Certification Authority (CA) on your AD server. Self-signed certificates are not allowed.

**Note:** SSL access should have been enabled for the AD Server before enabling the SSL option.

Login/Query Settings

- **LDAP login name** - Account username which CDAS should use to login to the AD server. Preferably, a new user account should be created especially for the CDAS server. The user account should have 'read' privileges to the AD server. The username can be of the format 'username' or 'username@domainname.com'
- **Password** - Enter the password of the LDAP user account above.
- **Remember Credentials** - Enable this option if you wish CDAS server to store the username/password of the user account in order to automatically login.
Note: If you enable automatic synchronization, the ‘Remember Credentials’ option will not be visible because CDAS will store the username and password by default. This will allow CDAS to connect to the AD server at the set time interval to update the user base. The option will become visible if “Synchronization Interval” setting is set as ‘no auto updates’.

- **Synchronization interval** - If you wish to configure CDAS 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 CDAS 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:

- CDAS can only import LDAP users that have email addresses on domains that you have added to CDAS in the Domains interface.

- To successfully import users, you must make sure the domain of their email addresses has been added to CDAS AND that the LDAP Import is configured for each individual domain from the Domain Management are 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 CDAS to create user accounts as found on LDAP server** - Select this checkbox if you wish new users added in the AD server to be automatically added to CDAS during synchronization. If you do not select this
option, you can manually import the new users from the LDAP import confirmation page.

- **Allow CDAS to delete user accounts not found on LDAP server** - Select this checkbox if you wish users removed from AD server, to be automatically removed from CDAS 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, CDAS will send email notifications to the administrator whenever new users are created or users are removed either automatically, (if 'Allow to create users?'/ 'Allow to delete users?' are enabled) or manually from the LDAP import confirmation page.

- **Last synchronization time (GMT)** - Displays the date and time of last manual or scheduled synchronization with AD server, in GMT.

- **Notification area** - Contains information about errors that occurred during synchronization. In most cases, this will contain the same information that is provided with the "Test connection" feature. Note - this area is only visible if errors occur.

- To check the configuration and connectivity, click 'Test Connection'. If the connection is established successfully then the success message will be displayed with the total number of users detected from the AD server.

- Click 'Save' to store your configuration.

- Click 'Save and run synchronization now' to store your configuration and synchronize the CDAS user base with the AD server.

**LDAP Import Confirmation List**

The LDAP import confirmation list interface displays the list of:

- Users created at the AD server and not yet been imported into CDAS
- Users not present on AD server and not yet been removed from CDAS

... 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 CDAS. The administrator can import the users created at AD server into CDAS manually and remove existing users from this interface.

- Administrators can also initiate an on-demand synchronization from this interface.

**To view LDAP import confirmation list**

- Open the 'Domains' interface and select a domain
- Click the 'Manage Domain' button to open the 'Domain Management' interface.
- Click 'Account management' on the left then select 'LDAP import confirmation list'.
The 'LDAP import confirmation list' interface will open:

The screen shows users added to and removed from the AD server with existing users created on CDAS. This list reflects the difference between CDAS users and AD users, considering the LDAP ignore list.

- Users present in AD which are not present in CDAS will have the status 'Create'
- Users not present in AD but present in CDAS will have the status 'Delete'

Sort the Entries
Click any column header to sort items in ascending/descending order of the entries in that column. The sorting option is not available for 'Login Duration' column.

**Use filters to search for users**

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

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 third text box and the selected condition.

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

• To run a manual on-demand synchronization, click 'Run synchronization now'

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 CDAS to access the AD server.

Enter the LDAP login credentials and click 'OK'.

CDAS server will connect to your AD server and start detecting the changes in the users in the AD server.

All the users added to the AD server will be displayed as a list.

• To import or delete users selected by applying filter, apply filters as described above and click 'More actions' > 'Apply import by filter'.

• To import or delete a set of selected users, select the users and click 'More actions' > 'Apply import by selection'.
• 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 'More actions' > 'Apply import by filter'. A confirmation dialog will be displayed.

![Apply import](image1)

• Click 'OK'. The import progress will be displayed.

![LDAP import confirmation list](image2)

On completion, the selected users will be imported or deleted in synchronization with the AD server.

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

• To move selected users to Ignore List, select the users and click 'Move to Ignore list'

![Move users to ignore list](image3)

… 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 CDAS 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.
To view LDAP import ignore list

- Open the 'Domains' interface and select the domain
- Click the 'Manage Domain' button to open the 'Domain Management' interface.
- Click 'Account management' tab > 'LDAP import ignore list' sub tab.

The 'LDAP import ignore list' interface will be displayed.
Sort the Entries

- Click the 'Username' column header to sort items in ascending/descending order of the usernames.

Use filters to search for users

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

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' to close the filters area.

- Click the **Refresh** button to display all users.

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

To add users to ignore list

- Click 'Add'. The Add ignored user dialog will be displayed.
To add users to the ignore list:

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

A 'Successfully added' message will be displayed at the top.

To remove the users from the ignore list:

- Select the users and click 'Remove from ignore list'. A confirmation dialog will be displayed.
- Click OK.

The users will be removed from the list and a 'Successfully deleted' message will be displayed at the top.

- Users removed from the ignore list will be imported to or deleted from CDAS 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 Audit Log

CDAS keeps a record of actions initiated by users and administrators for all domains belonging to an account.

The 'Audit log' area allow administrators with appropriate privileges to view these log reports. CDAS also keeps logs of domains separately for each domain. For more details on selected domain audit log, see Domain Audit Log. This section explains about the consolidated log for all domains available in the account.

To view Audit log:
- Click the 'Audit log' in the 'Dashboard' area to view log details for all the domains will be displayed.
Sorting the Entries

- Click any column heading to switch the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column. The sorting option is not available for 'Operation description' column.

Using Filter options to search particular event(s)

- 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:

- **Domain**: Will execute a search of log entries according to the text entered in the text box (column 3) and the condition selected in column 2
- **Login**: Will execute a search of log entries according to the text entered in the text box (column 3) and the condition selected in column 2
- **Details**: Will execute a search of log entries according to the text entered in the text box (column 3) and the condition selected in column 2

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

- **Contains**: Displays all log entries that contain the words entered in the text box
- **Equals**: Displays all log entries that contain only the words entered in the text box
- **Not Equals**: Displays all log entries that do not contain only the words entered in the text box
- **Not Contains**: Displays all log entries that don't contain the words entered in the text box
- **Starts with**: Displays all log entries that start with the words entered in the text box
- **Ends with**: Displays all log entries that end with the words entered in the text box

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

- **Date**: Will execute a search of log entries according to the date selected in the calendar box (column 3) and the condition selected in column 2
- **Role**: Will execute a search of log entries according to the role selected in the third field (column 3) and the condition selected in column 2
- **Operation Description**: Will execute a search of log entries according to the action selected in the third field (column 3) and the condition selected in column 2

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

- **Equals**: Displays the entries that have the same date as the selected date in the third box from the calendar
- **Less than**: Displays the entries with dates less than the selected date in the third box from the calendar
- **Greater than**: Displays the entries with dates greater than the selected date in the third box from the calendar
If 'Role' is selected, the following conditions are available:

- **Equals**: Displays all log entries that is equal to the role selected in column 3
- **Not Equals**: Displays all log entries that except the role selected in column 3

If 'Operative description' is selected, the following conditions are available:

- **Equals**: Displays all log entries that is equal to the event selected in column 3
- **Not Equals**: Displays all log entries that except the event selected in column 3

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 the entries

The following table provides the details of actions initiated by user/administrator and shown under Operation Key and Operation Description columns in the log report:

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Operation Key</th>
<th>Operation Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ACCEPT_AND_ARCHIVE_EMAIL</td>
<td>Accept and archive message</td>
</tr>
<tr>
<td>2</td>
<td>ACCEPT_BLACKLIST_REQUEST</td>
<td>Accept blacklist request</td>
</tr>
<tr>
<td>3</td>
<td>ACCEPT_BLACKLIST_REQUEST_PER_USER</td>
<td>Accept request blacklist sender for user</td>
</tr>
<tr>
<td>4</td>
<td>ACCEPT_EMAIL</td>
<td>Accept message</td>
</tr>
<tr>
<td>5</td>
<td>ACCEPT_RELEASE_REQUEST</td>
<td>Accept release request</td>
</tr>
<tr>
<td>6</td>
<td>ACCEPT_WHITELIST_REQUEST</td>
<td>Accept whitelist request</td>
</tr>
<tr>
<td>7</td>
<td>ACCEPT_WHITELIST_REQUEST_PER_USER</td>
<td>Accept request whitelist sender for user</td>
</tr>
<tr>
<td>8</td>
<td>ADD_GEOLOOKUP_RESTRICTION</td>
<td>Add geolookup restriction</td>
</tr>
<tr>
<td>9</td>
<td>ADMIN_ADD</td>
<td>Add admin</td>
</tr>
<tr>
<td>10</td>
<td>ADMIN_DELETE</td>
<td>Remove admin</td>
</tr>
<tr>
<td>11</td>
<td>ADMIN_EDIT</td>
<td>Edit admin settings</td>
</tr>
<tr>
<td>12</td>
<td>ADMIN_PASSWORD_UPDATE</td>
<td>Update password for admin</td>
</tr>
<tr>
<td>13</td>
<td>ADMIN_PERMISSIONS_ASSIGN_GROUP</td>
<td>Assign admin permission group by selection</td>
</tr>
<tr>
<td>14</td>
<td>ADMIN_PERMISSIONS_CHANGE_DEFAULT_GRO UP</td>
<td>Change default admin permission group</td>
</tr>
<tr>
<td>15</td>
<td>ADMIN_PERMISSIONS_GROUP_ADD</td>
<td>Add admin permission group</td>
</tr>
<tr>
<td>16</td>
<td>ADMIN_PERMISSIONS_GROUP_DELETE</td>
<td>Remove admin permission group</td>
</tr>
<tr>
<td>17</td>
<td>ADMIN_PERMISSIONS_GROUP_UPDATE</td>
<td>Update admin permission group</td>
</tr>
<tr>
<td>18</td>
<td>ADMIN_REGENERATE_PASSWORD</td>
<td>Regenerate password for admin</td>
</tr>
<tr>
<td>19</td>
<td>ADMIN_UNLOCK</td>
<td>Unlock admin</td>
</tr>
<tr>
<td>20</td>
<td>ADMIN_VIEW_MESSAGE_CONTENT</td>
<td>Admin view message content</td>
</tr>
<tr>
<td>21</td>
<td>ARCHIVE_MESSAGE</td>
<td>Archive message</td>
</tr>
<tr>
<td>Feature Code</td>
<td>Feature Description</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>BLACKLIST_DOMAIN_RULE</td>
<td>Blacklist domain rule</td>
</tr>
<tr>
<td>23</td>
<td>BLACKLIST_RECIPIENT</td>
<td>Blacklist recipient</td>
</tr>
<tr>
<td>24</td>
<td>BLACKLIST_RECIPIENT_DOMAIN</td>
<td>Blacklist all recipients of the domain</td>
</tr>
<tr>
<td>25</td>
<td>BLACKLIST_REQUEST</td>
<td>Blacklist request</td>
</tr>
<tr>
<td>26</td>
<td>BLACKLIST_SENDER</td>
<td>Blacklist sender</td>
</tr>
<tr>
<td>27</td>
<td>BLACKLIST_SENDER_DOMAIN</td>
<td>Blacklist all senders of the domain</td>
</tr>
<tr>
<td>28</td>
<td>BLACKLIST_USER_SENDER</td>
<td>Blacklist sender for user</td>
</tr>
<tr>
<td>29</td>
<td>CANCEL_BLACKLIST_REQUEST</td>
<td>Cancel blacklist request</td>
</tr>
<tr>
<td>30</td>
<td>CANCEL_WHITELIST_REQUEST</td>
<td>Cancel whitelist request</td>
</tr>
<tr>
<td>31</td>
<td>CHANGE_FORWARD_SETTINGS_FOR_INCOMING_USER</td>
<td>Change forward settings for incoming user</td>
</tr>
<tr>
<td>32</td>
<td>DELETE_EMAIL_FROM_ARCHIVE</td>
<td>Delete archived message</td>
</tr>
<tr>
<td>33</td>
<td>DELETE_EMAIL_FROM_ARCHIVE_BY_FILTER</td>
<td>Delete archived messages by filter</td>
</tr>
<tr>
<td>34</td>
<td>DELETE_EMAIL_FROM_QUARANTINE</td>
<td>Delete quarantined message</td>
</tr>
<tr>
<td>35</td>
<td>DELETE_EMAIL_FROM_QUARANTINE_BY_FILTER</td>
<td>Delete quarantined messages by filter</td>
</tr>
<tr>
<td>36</td>
<td>DOMAIN_ADD</td>
<td>Add domain</td>
</tr>
<tr>
<td>37</td>
<td>DOMAIN_ALIASES_ADD</td>
<td>Add domain alias</td>
</tr>
<tr>
<td>38</td>
<td>DOMAIN_ALIASES_DELETE</td>
<td>Remove domain alias</td>
</tr>
<tr>
<td>39</td>
<td>DOMAIN_AUDIT_CONFIGURATION_CHANGE</td>
<td>Audit configuration change</td>
</tr>
<tr>
<td>40</td>
<td>DOMAIN_BLOCKED_EXTENSIONS_RESET_TO_DEFAULT</td>
<td>Reset blocked extensions to default</td>
</tr>
<tr>
<td>41</td>
<td>DOMAIN_BLOCKED_EXTENSIONS_UPDATE</td>
<td>Update blocked extensions</td>
</tr>
<tr>
<td>42</td>
<td>DOMAIN_DELETE</td>
<td>Remove domain</td>
</tr>
<tr>
<td>43</td>
<td>DOMAIN_DESTINATION_ROUTES_UPDATE</td>
<td>Update destination routes</td>
</tr>
<tr>
<td>44</td>
<td>DOMAIN_EMAIL_SIZE_RESTRICTION_CHANGE</td>
<td>Email size restriction change</td>
</tr>
<tr>
<td>45</td>
<td>DOMAIN_INCOMING_USER_ADD</td>
<td>Add incoming user</td>
</tr>
<tr>
<td>46</td>
<td>DOMAIN_INCOMING_USER_ALIASES_UPDATE</td>
<td>Update incoming user aliases</td>
</tr>
<tr>
<td>47</td>
<td>DOMAIN_INCOMING_USER_DELETE</td>
<td>Remove incoming user</td>
</tr>
<tr>
<td>48</td>
<td>DOMAIN_INCOMING_USER_EDIT</td>
<td>Edit incoming user</td>
</tr>
<tr>
<td>49</td>
<td>DOMAIN_INCOMING_USER_MOVE_ALIAS_TO_USER</td>
<td>Move alias to incoming user</td>
</tr>
<tr>
<td>50</td>
<td>DOMAIN_INCOMING_USER_MOVE_USER_TO_ALIAS</td>
<td>Move user to alias</td>
</tr>
<tr>
<td>51</td>
<td>DOMAIN_INCOMING_USER_PASSWORD_UPDATE</td>
<td>Update password for incoming user</td>
</tr>
<tr>
<td></td>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>52</td>
<td>DOMAIN_INCOMING_USER_REGENERATE_PASSWORD</td>
<td>Regenerate password for incoming user</td>
</tr>
<tr>
<td>53</td>
<td>DOMAIN_INCOMING_USER_UNLOCK</td>
<td>Unlock incoming user</td>
</tr>
<tr>
<td>54</td>
<td>DOMAIN_LDAP_CONFIGURATION_CHANGE</td>
<td>LDAP configuration change</td>
</tr>
<tr>
<td>55</td>
<td>DOMAIN_LOCAL_RECIPIENTS_ADD</td>
<td>Add local recipient</td>
</tr>
<tr>
<td>56</td>
<td>DOMAIN_LOCAL_RECIPIENTS_DELETE</td>
<td>Remove local recipient</td>
</tr>
<tr>
<td>57</td>
<td>DOMAIN_LOCAL_RECIPIENTS_STATE_CHANGE</td>
<td>Local recipients state change</td>
</tr>
<tr>
<td>58</td>
<td>DOMAIN_OUTGOING_USER_ADD</td>
<td>Add outgoing user</td>
</tr>
<tr>
<td>59</td>
<td>DOMAIN_OUTGOING_USER_DELETE</td>
<td>Remove outgoing user</td>
</tr>
<tr>
<td>60</td>
<td>DOMAIN_OUTGOING_USER_LOCK</td>
<td>Lock outgoing user</td>
</tr>
<tr>
<td>61</td>
<td>DOMAIN_OUTGOING_USER_PASSWORD_UPDATE</td>
<td>Update password for outgoing user</td>
</tr>
<tr>
<td>62</td>
<td>DOMAIN_OUTGOING_USER_SETTINGS_UPDATE</td>
<td>Edit outgoing user</td>
</tr>
<tr>
<td>63</td>
<td>DOMAIN_OUTGOING_USER_UNLOCK</td>
<td>Unlock outgoing user</td>
</tr>
<tr>
<td>64</td>
<td>DOMAIN_RELAY_RESTRICTIONS_ADD</td>
<td>Add relay restriction</td>
</tr>
<tr>
<td>65</td>
<td>DOMAIN_RELAY_RESTRICTIONS_DELETE</td>
<td>Remove relay restriction</td>
</tr>
<tr>
<td>66</td>
<td>DOMAIN_RELAY_RESTRICTIONS_STATE_CHANGE</td>
<td>Relay restriction state change</td>
</tr>
<tr>
<td>67</td>
<td>DOMAIN_RELAY_RESTRICTIONS_UPDATE</td>
<td>Update relay restriction</td>
</tr>
<tr>
<td>68</td>
<td>DOMAIN_REQUEST_CREATED</td>
<td>Domain request created</td>
</tr>
<tr>
<td>69</td>
<td>DOMAIN_SETTINGS_RESET_TO_DEFAULT</td>
<td>Reset domain settings to default</td>
</tr>
<tr>
<td>70</td>
<td>DOMAIN_SETTINGS_UPDATE</td>
<td>Update domain settings</td>
</tr>
<tr>
<td>71</td>
<td>DOMAIN_STATISTICS_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT</td>
<td>Domain report subscription reset to default</td>
</tr>
<tr>
<td>72</td>
<td>DOMAIN_STATISTICS_REPORT_SUBSCRIPTION_UPDATE</td>
<td>Domain report subscription update</td>
</tr>
<tr>
<td>73</td>
<td>DOMAIN_VALIDATED_BY_CODE</td>
<td>Domain validated by code</td>
</tr>
<tr>
<td>74</td>
<td>DOMAIN_VALIDATED_BY_MX</td>
<td>Domain validated by MX</td>
</tr>
<tr>
<td>75</td>
<td>DOMAIN_VALIDATED_CODE_REGENERATED</td>
<td>Domain validation code regenerated</td>
</tr>
<tr>
<td>76</td>
<td>EMAIL_QUARANTINE_ALERT</td>
<td>Email quarantine alert</td>
</tr>
<tr>
<td>77</td>
<td>ENABLE_GEOLOOKUP_RESTRICTIONS</td>
<td>Enable geolocation restrictions</td>
</tr>
<tr>
<td>78</td>
<td>ENABLE_USER</td>
<td>Enable user</td>
</tr>
<tr>
<td>79</td>
<td>FORWARD_BY_RULE_EMAIL</td>
<td>Forward by rule email</td>
</tr>
<tr>
<td>80</td>
<td>FORWARD_DOMAIN_RULE</td>
<td>Forward domain rule</td>
</tr>
<tr>
<td>81</td>
<td>FORWARD_EMAIL_LOOP_EXCEPTION</td>
<td>Forward email loop exception</td>
</tr>
<tr>
<td>Page</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>FORWARD_TO</td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>FORWARDED_BY_RULE_EMAIL_IS_LOOPED</td>
<td></td>
</tr>
<tr>
<td>84</td>
<td>IMPORT_INCOMING_USER</td>
<td></td>
</tr>
<tr>
<td>85</td>
<td>LICENCE_IS_RESTORED</td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>LICENCE_IS_EXPIRED</td>
<td></td>
</tr>
<tr>
<td>87</td>
<td>MARK_EMAIL_AS_SPAM</td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>MIGRATE_DOMAIN</td>
<td></td>
</tr>
<tr>
<td>89</td>
<td>NON_HUMAN_EMAIL_TYPE</td>
<td></td>
</tr>
<tr>
<td>90</td>
<td>PUBLIC_EMAIL_TYPE</td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>QUARANTINE_EMAIL</td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>QUARANTINE_RELEASE_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT</td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>QUARANTINE_RELEASE_REPORT_SUBSCRIPTION_UPDATE</td>
<td></td>
</tr>
<tr>
<td>94</td>
<td>QUARANTINE_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT</td>
<td></td>
</tr>
<tr>
<td>95</td>
<td>QUARANTINE_REPORT_SUBSCRIPTION_UPDATE</td>
<td></td>
</tr>
<tr>
<td>96</td>
<td>REJECT_BLACKLIST_REQUEST</td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>REJECT_BLACKLIST_REQUEST_PER_USER</td>
<td></td>
</tr>
<tr>
<td>98</td>
<td>REJECT_RELEASE_REQUEST</td>
<td></td>
</tr>
<tr>
<td>99</td>
<td>REJECT_RELEASE_REQUEST</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>REJECT_WHITELIST_REQUEST</td>
<td></td>
</tr>
<tr>
<td>101</td>
<td>REJECT_WHITELIST_REQUEST_PER_USER</td>
<td></td>
</tr>
<tr>
<td>102</td>
<td>RELEASE_EMAIL_FROM_QUARANTINE</td>
<td></td>
</tr>
<tr>
<td>103</td>
<td>REMOVE_BLACKLIST_DOMAIN_RULE</td>
<td></td>
</tr>
<tr>
<td>104</td>
<td>REMOVE_DOMAIN_BY_VALIDATION_TIMEOUT</td>
<td></td>
</tr>
<tr>
<td>105</td>
<td>REMOVE_FORWARD_DOMAIN_RULE</td>
<td></td>
</tr>
<tr>
<td>106</td>
<td>REMOVE_GEOLOOKUP_RESTRICTION</td>
<td></td>
</tr>
<tr>
<td>107</td>
<td>REMOVE_WHITELIST_DOMAIN_RULE</td>
<td></td>
</tr>
<tr>
<td>108</td>
<td>REPLY_ON_ARCHIVED_MESSAGE</td>
<td></td>
</tr>
<tr>
<td>109</td>
<td>REPORT_SPAM_BY_FILE</td>
<td></td>
</tr>
<tr>
<td>110</td>
<td>REPORTED_SPAM_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT</td>
<td></td>
</tr>
<tr>
<td>111</td>
<td>REPORTED_SPAM_REPORT_SUBSCRIPTION_UPDATE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>---------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>112</td>
<td>REPORTS_AS_SPAM</td>
<td>Reports archived message as SPAM</td>
</tr>
<tr>
<td>113</td>
<td>RESEND_EMAIL_FROM_ARCHIVE</td>
<td>Resend archived message</td>
</tr>
<tr>
<td>114</td>
<td>RESET_SPAM_DETECTION_SETTINGS_TO_DEFAULT</td>
<td>Reset spam detection settings to default</td>
</tr>
<tr>
<td>115</td>
<td>RESET_SYSTEM_NOTIFICATIONS_TEMPLATE_TO_DEFAULT</td>
<td>Reset system notifications template to default</td>
</tr>
<tr>
<td>116</td>
<td>RESET_TO_DEFAULT_BLACKLISTED_RECIPIENTS</td>
<td>Reset recipients blacklist</td>
</tr>
<tr>
<td>117</td>
<td>RESET_TO_DEFAULT_BLACKLISTED_SENDERS</td>
<td>Reset senders blacklist</td>
</tr>
<tr>
<td>118</td>
<td>RESET_TO_DEFAULT_WHITELISTED_RECIPIENTS</td>
<td>Reset recipients whitelist</td>
</tr>
<tr>
<td>119</td>
<td>RESET_TO_DEFAULT_WHITELISTED_SENDERS</td>
<td>Reset senders whitelist</td>
</tr>
<tr>
<td>120</td>
<td>SEND_INVITATION_TO_USER</td>
<td>Send invitation to user</td>
</tr>
<tr>
<td>121</td>
<td>SPAM_DETECTION_SETTINGS</td>
<td>Update spam detection settings</td>
</tr>
<tr>
<td>122</td>
<td>SPAM_DETECTION_SETTINGS_RESET_TO_DEFAULT</td>
<td>Reset spam detection settings</td>
</tr>
<tr>
<td>123</td>
<td>SYSTEM_NOTIFICATIONS_TEMPLATE_CHANGE</td>
<td>System notifications template change</td>
</tr>
<tr>
<td>124</td>
<td>TLD_DOMAIN_RULE</td>
<td>TLD domain rule</td>
</tr>
<tr>
<td>125</td>
<td>UNBLACKLIST_RECIPIENT</td>
<td>Remove recipient from blacklist</td>
</tr>
<tr>
<td>126</td>
<td>UNBLACKLIST_SENDER</td>
<td>Remove sender from blacklist</td>
</tr>
<tr>
<td>127</td>
<td>UNBLACKLIST_USER_SENDER</td>
<td>Remove sender from user blacklist</td>
</tr>
<tr>
<td>128</td>
<td>UNWHITELIST_RECIPIENT</td>
<td>Remove recipient from whitelist</td>
</tr>
<tr>
<td>129</td>
<td>UNWHITELIST_SENDER</td>
<td>Remove sender from whitelist</td>
</tr>
<tr>
<td>130</td>
<td>UNWHITELIST_USER_SENDER</td>
<td>Remove sender from user whitelist</td>
</tr>
<tr>
<td>131</td>
<td>UPDATE_BLACKLIST_DOMAIN_RULE</td>
<td>Update blacklist domain rule</td>
</tr>
<tr>
<td>132</td>
<td>UPDATE_FORWARD_DOMAIN_RULE</td>
<td>Update forward domain rule</td>
</tr>
<tr>
<td>133</td>
<td>UPDATE_USERS_AUTO_IMPORT_SETTINGS</td>
<td>Update users auto-import settings</td>
</tr>
<tr>
<td>134</td>
<td>UPDATE_WHITELIST_DOMAIN_RULE</td>
<td>Update whitelist domain rule</td>
</tr>
<tr>
<td>135</td>
<td>USER_BLACKLIST_REQUEST_PER_USER</td>
<td>Request blacklist sender for user</td>
</tr>
<tr>
<td>136</td>
<td>USER_CANCEL_BLACKLIST_REQUEST_PER_USER</td>
<td>Cancel request blacklist sender for user</td>
</tr>
<tr>
<td>137</td>
<td>USER_CANCEL_RELEASE_REQUEST</td>
<td>Cancel release request</td>
</tr>
<tr>
<td>138</td>
<td>USER_CANCEL_WHITELIST_REQUEST_PER_USER</td>
<td>Cancel request whitelist sender for user</td>
</tr>
<tr>
<td>139</td>
<td>USER_PERMISSIONS_ASSIGN_GROUP</td>
<td>Assign user permission group by selection</td>
</tr>
<tr>
<td>140</td>
<td>USER_PERMISSIONS_CHANGE_DEFAULT_GROUP</td>
<td>Change default user permission group</td>
</tr>
<tr>
<td>Code</td>
<td>Function Description</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------</td>
<td></td>
</tr>
<tr>
<td>141</td>
<td>USER_PERMISSIONS_GROUP_ADD</td>
<td>Add user permission group</td>
</tr>
<tr>
<td>142</td>
<td>USER_PERMISSIONS_GROUP_DELETE</td>
<td>Remove user permission group</td>
</tr>
<tr>
<td>143</td>
<td>USER_PERMISSIONS_GROUP_UPDATE</td>
<td>Update user permission group</td>
</tr>
<tr>
<td>144</td>
<td>USER_RELEASE_REQUEST</td>
<td>Release request</td>
</tr>
<tr>
<td>145</td>
<td>USER_WHITELIST_REQUEST_PER_USER</td>
<td>Request whitelist sender for user</td>
</tr>
<tr>
<td>146</td>
<td>USERS_AUTO-IMPORT_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT</td>
<td>Users auto-import report subscription reset to default</td>
</tr>
<tr>
<td>147</td>
<td>USERS_AUTO-IMPORT_REPORT_SUBSCRIPTION_UPDATE</td>
<td>Users auto-import report subscription update</td>
</tr>
<tr>
<td>148</td>
<td>WHITELIST_DOMAIN_RULE</td>
<td>Whitelist domain rule</td>
</tr>
<tr>
<td>149</td>
<td>WHITELIST_RECIPIENT</td>
<td>Whitelist recipient</td>
</tr>
<tr>
<td>150</td>
<td>WHITELIST_RECIPIENT_DOMAIN</td>
<td>Whitelist all recipients of the domain</td>
</tr>
<tr>
<td>151</td>
<td>WHITELIST_REQUEST</td>
<td>Whitelist request</td>
</tr>
<tr>
<td>152</td>
<td>WHITELIST_SENDER</td>
<td>Whitelist sender</td>
</tr>
<tr>
<td>153</td>
<td>WHITELIST_SENDER_DOMAIN</td>
<td>Whitelist all senders of the domain</td>
</tr>
<tr>
<td>154</td>
<td>WHITELIST_USER_SENDER</td>
<td>Whitelist sender for user</td>
</tr>
</tbody>
</table>

**Export Log Report to CSV**

The log report can be exported to a comma separated value (CSV) file and is limited to 10,000 entries per file. If the entries exceed this value, exporting cannot be done and a warning will be displayed. Please note that exported file will display the entries in the same sorted order as in the interface.

**To export log report to csv file**

- Click the ‘Export to CSV by filter’ button. The ‘File Download’ will open:
Click ‘Open with’ or ‘Save File’ to view / save the file with an appropriate application to your computer.

Click ‘OK’

The values in the log report will be separated by commas and this file can be opened with Excel or Openoffice Calc for easy analysis.

3.2.3 Administrator Account Management

- The ‘Account Management’ area lets an admin with appropriate privileges to add new administrators for the same account.
- This area also allows the administrator to configure permissions for users and administrators, reset passwords and change the login status from enabled to disabled and vice-versa.
- Admins who have logged in using the CAM credentials will have an additional icon ‘Login to my Comodo account’ through which you can access your CAM account.
- If logged in as an administrator, the ‘Account Management’ area will differ depending on the privileges configured for the administrator. See ‘Admin Groups & Permissions’ for more details.
Click the following links for more details:

- Managing Administrators
- User Groups & Permissions
- Admin Groups & Permissions
- Managing Comodo Account
- My Profile
- Users History

3.2.3.1 Administrators

In this interface, an administrator with appropriate privileges can add new administrators, delete existing administrators, set permission levels as well as edit the login status and regenerate new password for existing administrators. Refer to the section 'Admin Groups & Permissions' for more details on administrative privileges.

Click the following links for more details:

- Managing Administrators
- Adding New Administrators
- Deleting Administrators
- Editing Administrators
- Managing Permissions for Administrators

Managing Administrators
Comodo Dome Antispam MSP - Administrator Guide

• Click the 'Admins' from the 'Account management' drop-down menu on the left

The 'Admins' interface displays a list of administrators with their CDAS enabled/disabled status, their last login date and time, to which group they belong and the domains that they can manage.

• Click the up/down arrows in the respective column headers to sort the entries in ascending or descending order based on the login, enabled status or last login time

Using the filter option to search administrators
• Click anywhere on the 'Filters' to open the filters area.
You can add more filters by clicking + for narrowing down your search.

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

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

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 administrator name that was entered in full in the text box.
- **Not Equals**: Displays all administrator(s), except the one entered in the text box.
- **Contains**: Displays all administrator(s) that contains the words entered in the text box.
- **Not Contains**: Displays all administrator(s) that does not contain the words entered in the text box.
- **Starts With**: Displays all administrator(s) that starts with the words entered in the text box.
- **Ends With**: Displays all administrator(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 administrator(s) who are not enabled.

- **Last Login**: Will execute a search of admins according to the date selected in the calendar (column 3) and the condition selected in column 2.

When you select this option in the first drop-down, the following filters are available:
• **Equals**: Displays the list of administrator(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 administrator(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 administrator(s) that has the last logged in on dates greater than the selected date in the third box from the calendar.

• **Group**: Will execute a search of admins according to the group selected in last drop-down (column 3) and the condition selected in column 2.

• **Equals**: Displays the results based on the group name that is selected in the drop down list from the third box.

• **Not Equals**: Displays all administrator(s), except the one selected in the drop down list from the third 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' to close the filters area.

• Click the button to display all administrators.

**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 be displayed.

• **Login** - Enter the new administrator's valid email address as login username.

• **System notifications email(s)** - Enter the email addresses at which the new administrator should receive CDAS notification emails. It can be the same email address as the login name and / or alternative email address(es) of up to a maximum of five. The quarantine requests from users, for blacklisting, whitelisting, or releasing quarantined emails and notifications such as of imports of users, local recipients and users via LDAP from CSV files will be sent to the email addresses specified in this field. See Email Management for more details.

• **Status** - Enables to change the login status of the new administrator. By default, this box is selected, that is, the new administrator can access CDAS interface.
• **Subscribe emails 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 [CDAS Reports - an Overview](#) for more details.

• Click the ‘Save’ button.

The administrator will be added to the list and be placed in the default group. The privileges to the administrator can be configured according to his/her role. See 'Managing Permissions for Administrators' for more details. An email to the added administrator will be sent automatically containing password to access CDAS. 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 delete and click 'Delete' button.

A confirm dialog will be displayed warning you that the selected administrators will be deleted.
• Click ‘OK’ to confirm the deletion.

The selected administrator(s) will be deleted from the list.

To edit an existing administrator

You can reset the password, change the CDAS notification email address(es) and allow or deny permission for the administrators to access their CDAS 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.

• **System notifications email(s)** - Enter the email addresses at which the new administrator should receive CDAS notification emails. It can be the same email address as the login name and / or alternative email address(es) of up to a maximum of five. The quarantine requests from users, for blacklisting, whitelisting, or releasing quarantined emails and notifications such as of imports of users, local recipients and users via LDAP from CSV files will be sent to the email addresses specified in this field. Refer to the section **Email Management** for more details.

**Tip:** The currently logged-in administrator can configure the Quarantine notification email address in **Dashboard > Account Management > My Profile** dialog.

• **Status** - Enables to change the login status of the administrator

• **Regenerate password** - 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 CDAS
Click the 'Save' button to confirm your changes.

Managing Permissions for Administrators

CDAS allow administrators with appropriate privileges to assign permissions for other administrators that will determine what he/she can do and cannot do while logged into their respective CDAS admin interface. The administrators can create policies and assign them to other administrators from this interface. See 'Admin Groups & Permissions' for more details on how to create groups and policies for administrators. A new administrator will be automatically assigned default permission settings.

To assign permissions for an administrator

- Select the administrator or multiple administrators that you want assign permissions and click the 'Manage permissions' button.

The 'Admin Groups & Permissions' interface will be displayed.

Assign to selected admins  Assign to filtered admins  Cancel
The interface displays the list of groups available with same or different permission levels for each group. By default, 'Power Administrators (Default) group will be available and administrators can add, edit groups and assign permissions to other administrators. See the section 'Admin Groups & Permissions' for more details.

- Select the group from the list.

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

- The permissions set for this group will be displayed on the right side.
- Click the 'Assign to selected admins' button to set permissions for selected admin(s).
- Click 'Assign to filtered admins' button to set permissions for administrators found by filter.
- Click 'OK' in the confirmation dialog.

The selected admin(s) will be added to the group and a confirmation message will be displayed.
The interface also displays the new group assigned for the selected admin(s) under the ‘Group’ column.

### 3.2.3.2 User Groups & Permissions

- The ‘User Groups & Permissions’ interface allows admins with appropriate privileges to create email user groups and to set group permissions.
- You can create multiple groups, each with different permission levels. When you assign users to a group they will inherit the permissions of the group.
- The user interface will vary according to a user’s permission level. See ‘Managing Permissions for Users’ in ‘User Account Management’ for help with this.

**To create user groups**

- Click the ‘User groups & permissions’ from the ‘Account management’ drop-down menu on the left
- The ‘User Groups & permissions’ interface will be displayed

By default, two user groups, Power User and Users (Default), will be available. These two groups cannot be either edited nor deleted.

- Click any one of them will display the permission levels assigned for the group in the right side.
Click 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 Released Requests in ‘Email Management’ for more details.

Permission Levels

- Incoming Log Search - Allows a user to search and view the log of all incoming mails.
- Outgoing Log Search - Allows a user to search and view the log of all outgoing mails.
- Report Spam - Allows a user to report a mail as spam mail.
- User report subscriptions - Allows a user to configure periodical quarantine report generation.
- Quarantine
  - Show Message - Allows a user to view quarantined emails in same window or separate window.
• Release messages - Allows a user to release a quarantined mail without approval from the administrator.
• Delete messages - Allows a user to delete a quarantined mail without approval from the administrator.
• Archive
  • View - Allows a user to view archived emails in same window or separate window.
  • Resend - Allows a user to resend archived emails to himself / herself.
  • Reply all - Allows a user to reply to all archive emails
  • Forward - Allows a user to forward an archive email composed earlier
• Create mail request - Allows a user to configure email request for CDAS notifications.
• Change user settings - Allows a user to configure himself / herself as recipient whitelist.
• Whitelist / Blacklist
  • Manage whitelist senders per user - Allows a user to manage sender whitelist for his / her mail account
  • Manage blacklist sender per user - Allows a user to manage sender blacklist for his / her mail account

Click the following links for more details.
  • Adding a new group
  • Editing a group
  • Deleting a group
  • Making a group as default

To add a new group
  • To add a new group and configure permission levels, click the 'Add' button
  • A new group creating page will be displayed.
Enter the name of the group in the text field under the 'Name' column. Note: To enable the permission levels in the right side for that group, click the 'Edit' button on the top.
• Click the ‘Save’ button.

The newly created group will be displayed in the interface with the allotted permissions to it.

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

To edit a group

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

• Select the group from the list and click the 'Edit' button.
Change the permission levels and / or the name of the group.

Click the ‘Save’ button for the changes to take effect.

The users in the group that is edited will be automatically reassigned to the edited group.

**To delete a group**

- Select the group from the list and click the ‘Delete’ button.
• Click 'OK' in the confirmation dialog.

The selected group will be deleted from the list.

**Note 1:** If you delete a group, users assigned to that group will be automatically moved to default group. You have to reassign the users if required.

**Note 2:** If you delete a user group created by the administrator and marked as default, then the 'Users' group that was shipped with the product will be set as default. All the users from the deleted group will be automatically migrated to the 'Users' group.

**To make a group as default**

CDAS allows administrators to make an existing group as default group. Newly added users and users belonging to an existing group whose name was deleted will be automatically moved to this default group.

• Select a group from the list and click the 'Make default' button.

A success dialog will be displayed.
3.2.3.3 Admin Groups & Permissions

- The 'Admin Groups & Permissions' interface allows admins with appropriate privileges to create administrator groups.
- Each group can be configured with different permission levels. This simplifies the process of configuring permission levels for each administrator. New or existing administrators belonging to the account can be simply assigned to a group with a preset policy.
- The admin interface will vary according to his/her permission level. See 'Managing Permissions for Administrators' in 'Administrators' for how to add administrators to predefined groups.

To create admin groups

- Click the 'Admin Groups & Permissions' from the 'Account management' drop-down menu on the left

The 'Admin Groups & Permissions' interface will be displayed.

**Note:** If you delete a user group created by the administrator and marked as default, then the 'Users' group that was shipped with the product will be set as default. All the users from the deleted group will be automatically migrated to the 'Users' group.
By default, Power Administrator group will be available. This default group cannot be either edited nor deleted.

- Tick a group from the right side to view the permission levels assigned for it.

- Click on the arrow beside a permission to display the tree structure of second level of permissions, if available.
For administrators in the 'Power Administrators' group, all permission levels will be enabled. The 'Permission' level is divided into two categories, 'All customer permissions' and 'All domain permissions'.

- The customer permissions deals with providing privileges for adding domains, configuring email user permissions, report management and so on.
- The domain permission level deals with providing access to particular domain(s). This is very useful if you want to restrict administrators to manage selected domains only.

**Permission Levels**

- **All customer permissions** - View and manage all customer related tasks.
  - Add domain - Add new domain(s)
  - Admin management - View and manage administrators for the account.
    - View - Only view the list of administrators.
    - Unlock - Unlock previously blocked administrators.
    - Manage - Manage administrators for the account.
  - User permissions - View and manage 'User Groups & Permissions'
    - View - Only view 'User Groups & Permissions'
    - Manage - Manage 'User Groups & Permissions'
  - Admin permissions - View and manage 'Admin Groups & Permissions'
    - View - Only view 'Admin Groups & Permissions'
    - Manage - Manage 'Admin Groups & Permissions'
  - Report management - View and manage report subscriptions
    - View - Only view report subscriptions
    - Change - View and manage report subscriptions
  - User session history view - View user sessions history for all domains in the account
  - View customer info - View information about the customer.
  - Locale - View and manage message locale sent to a user
    - View - Only view messages locale
    - Change - View and manage messages locale
  - Change user limit per domain - Configure the number of users for each domain in the account.
  - Email template management - Edit the email template for user's notification emails.
  - Audit log - Configure and view log for the permitted domain.
    - Log - View and export the log for the permitted domain.

- **All domain permissions** - Assign domain(s) management.
  - Assigned Domain(s) - Manage domains, incoming and outgoing users, emails, audit log and reports.
    - View - Only view the assigned domains.
    - Change - Edit the assigned domain(s)
    - Remove - Remove the assigned domain(s).
  - User Management - View and manage incoming users, outgoing users, whitelist recipients and blacklist recipients.
    - Incoming user - View, manage and unlock incoming users.
      - View - Only view list of incoming users.
      - Manage - View and manage incoming users.
      - Unlock - Unlock users immediately without waiting for the timeout period to end.
      - Change forward settings - Change forward email settings for incoming users
    - Outgoing user - View, manage, lock/unlock and import from incoming users.
- View - Only view list of outgoing users.
- Manage - View and manage outgoing users.
- Outgoing settings - Configure a list of outgoing users.
- Lock/Unlock - Lock or unlock outgoing users from sending out mails.
- Import from incoming - Import outgoing users from the list of incoming users.

- Whitelist recipients - View and manage whitelist recipients.
  - View - Only view list of whitelisted recipients.
  - Manage - View and manage whitelist recipients.

- Blacklist recipients - View and manage blacklist recipients.
  - View - Only view list of blacklisted recipients.
  - Manage - View and manage blacklist recipients.

- Users auto-import - Automatically import all new incoming users bases on incoming email flow
  - View - Only view list of users auto-import recipients.
  - Manage - View and manage users auto-import recipients.

- Domain geolookup restrictions - View and manage CDAS web interface access control policies
  - View - Only view the access control policies
  - Manage - View and manage access control policies

- Domain management - View and manage all domain related tasks.
  - Local recipients - View and manage local recipients.
    - View - Only view list of local recipients.
    - Manage - View and manage local recipients.
  - Domain alias - View and manage domain aliases
    - View - Only view the list of domain aliases.
    - Manage - View and manage domain aliases.
  - Email filter settings - View and configure incoming spam detection settings.
    - View - Only view incoming spam detection settings.
    - Change - View and configure "Spam threshold" and "Probable spam threshold" fields.
    - Threshold - Configure changes for "Spam threshold" and "Probable spam threshold" fields in the Incoming Spam detection settings.

- Domain settings - View and change domain settings.
  - View - Only view the list of domain settings.
  - Change - View and configure domain settings.

- LDAP - View and configure LDAP settings for importing users.
  - View - Only view LDAP settings and list of imported users.
  - Change - View and configure LDAP settings for importing users.

- Quarantine - View and manage quarantined mails.
  - View - Only view the list of quarantined mails.
  - Delete - Deleted quarantined mails from the list.
  - Release - Release quarantined mails to the recipients.
  - View mail content - Only view quarantined mails from the list.

- Archive - View and manage copy of incoming mails in archive.
  - View - Only view archived mails.
  - Resend - Resend archived mails to recipients.
  - Retain - Retains archived mails from being purged automatically.
  - Delete - Delete archived mails.
• View mail content - View mail content of archived mails.
• Incoming delivery queue - View and manage queued mails.
  • View - Only view queued mails.
  • Retry - Retry to send queued mails to recipients.
  • Alerts - Queue email notification
• Incoming Log Search - Search incoming mails log.
• Outgoing Log Search - Search sent mails log.
• Clear incoming cache - Clear incoming callout cache.
• Clear outgoing cache - Clear outgoing callout cache.
• User session history view - View user sessions history for the assigned domain(s).
• Email Management - View and configure all Email management related settings and tasks.
  • Email size - View and configure email size settings.
    • View - Only view email size settings.
    • Change - View and configure email size settings.
  • Blocked extensions - View and manage blocked extensions.
    • View - Only view the list of blocked extensions.
    • Change - View and manage blocked extensions.
  • Whitelist senders - View and manage sender whitelist.
    • View - Only view sender whitelist.
    • Manage - View and manage sender whitelist.
  • Blacklist senders - View and manage sender blacklist.
    • View - Only view sender blacklist.
    • Manage - View and manage sender blacklist.
• Release requests - View and manage requests from users for release of quarantined mails.
  • View - Only view the list of requests from users for release of quarantined mails.
  • Manage - View and manage requests from users for release of quarantined mails.
• Whitelist requests - View and manage requests from users to whitelist senders.
  • View - Only view the list of requests from users for adding senders to whitelist.
  • Manage - View and manage requests from users to whitelist senders.
• Blacklist requests - View and manage requests from users to blacklist senders.
  • View - Only view the list of requests from users for adding senders to blacklist.
  • Manage - View and manage requests from users to blacklist senders.
• Report spam - Upload mails to CDAS for reporting them as spam.
• Create rule - Create and manage administrators rules.
  • View - Only view administrators rules.
  • Manage - View and manage administrators rules.
• Whitelist sender rule - View and manage rules for adding senders to whitelist
  • View - Only view the whitelist sender rules
  • Manage - View and manage whitelist sender rules
• Blacklist sender rule - View and manage rules for adding senders to blacklist
  • View - Only view the blacklist sender rules
  • Manage - View and manage blacklist sender rules
• Whitelisted senders per user - View and manage whitelisted senders per user.
  • View - Only view list of whitelisted senders per user.
  • Manage - View and manage whitelisted senders per user.
• Blacklisted senders per user - View and manage blacklisted senders per user.
- View - Only view list of blacklisted senders per user.
- Manage - View and manage blacklisted senders per user.
- Domain relay restrictions - View and configure email relay restriction rules
  - View - Only view relay restriction rule
  - Manage - View and manage relay restriction rules
- Audit log - Configure and view log for the permitted domain.
  - Configuration - Configure the log settings for the permitted domain.
  - Log - View and export the log for the permitted domain.
- Report management - View and configure settings for periodical domain and quarantine summary reports for the permitted domain.
  - View - Only view the configured settings for periodical domain and quarantine summary reports for the permitted domain.
  - Change - View and configure settings for periodical domain and quarantine summary reports for the permitted domain.

Click the following links for more details.

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

Adding a New Admin Group

- To add a new admin group and configure permission levels, click the 'Add' button
- A new admin group creating page will be displayed
- Enter the name of the group in the text field under the 'Name' column. Note: To enable the permission levels in the right side, click the 'Edit' for that group.
Click 'Save' button.
The newly created group will be displayed in the interface.

Now, administrators belonging to the account can be assigned to this newly created group. See 'Managing Permissions for Administrators' in 'Administrators' on how to add users to predefined groups.

**Editing an admin group**

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

- Select the group from the list and click the 'Edit' button.
• Change the permission levels and / or the name of the group.
• Click the 'Save' button for the changes to take effect.

The admins in the group that is edited will be automatically reassigned to the edited group.

Deleting an admin 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 1**: If you delete a group, admins assigned to that group will be automatically moved to default group. You have to reassign the administrators if required.

**Note 2**: If you delete an admin group created by the administrator and marked as default, then the 'Power Administrator' group that was shipped with the product will be set as default. All the admins from the deleted group
will be automatically migrated to the "Power Administrator" group.

Making an admin group as default

CDAS allows administrators to make an existing group as a default group. Newly added administrators and administrators belonging to an existing group whose name was deleted will be automatically moved to this default group.

- Select a group from the list and click the 'Make default' button.
- A success dialog will be displayed:

![Admin groups & permissions]

- Click 'OK'.

The selected group will be displayed as default group.

**Note:** If you delete an admin group created by the administrator and marked as default, then the 'Power Administrator' group that was shipped with the product will be set as default. All the admins from the deleted group will be automatically migrated to the 'Power Administrator' group.

3.2.3.4 My Comodo Account

This feature will be available in the 'Account management' if you have logged in to CDAS using CAM account credentials.
Click the 'Login to my Comodo account' to open https://accounts.comodo.com/login page. From here you can:

- Add more subscriptions for CDAS account
- Change your password
- Change contact information
- Sign up to other Comodo products

...and many more.

For more details on CAM account, visit our online website at https://help.comodo.com/topic-211-1-513-5907--Introduction-To-Comodo-Accounts-Management.html

3.2.3.5 My Profile

The 'My Profile' interface lets currently logged-in administrator to change his login password to CDAS as well as to change settings for idle session timeout and CDAS notification email address.

You can open 'My profile' interface in two ways:

- Click the 'Account management' on the left to expand then 'My profile'.
- Alternatively, click 'My Account' > 'My Profile' at the top-right.
The 'My Profile' interface will open:
Note: The interface will vary depending on the login credential that you have used to access CDAS. The password can be changed after logging in to the CAM account.

To set idle session timeout and change system notifications email address

- Click the 'My profile' from the 'Account management' drop-down menu on the left

<table>
<thead>
<tr>
<th>Dashboard / My profile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>My profile</strong></td>
</tr>
<tr>
<td>Change settings</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Login:</strong> <a href="mailto:domeasmspext@yopmail.com">domeasmspext@yopmail.com</a></td>
</tr>
<tr>
<td><strong>CAM email:</strong> <a href="mailto:domeasmspext@yopmail.com">domeasmspext@yopmail.com</a></td>
</tr>
<tr>
<td><strong>System notifications email(s):</strong> <a href="mailto:domeasmspext@yopmail.com">domeasmspext@yopmail.com</a></td>
</tr>
<tr>
<td><strong>Number of minutes before my session expires:</strong> 30</td>
</tr>
<tr>
<td><strong>Interface language:</strong> English</td>
</tr>
<tr>
<td><strong>Spam trap email:</strong></td>
</tr>
<tr>
<td><strong>Sites:</strong></td>
</tr>
</tbody>
</table>

- **Login** - The user-name of the currently active user. Administrators can use this to log in to CAM to purchase additional licenses and renew existing licenses.
- **CAM email** - The email address for the account as registered at Comodo Accounts Manager (CAM).
- **System notifications email(s)** - Enter the email addresses at which the new administrator should receive CDAS notification emails. It can be the same email address as the login name and / or alternative email address(es) of up to a maximum of five. The quarantine requests from users, for blacklisting, whitelisting, or releasing quarantined emails and notifications such as of imports of users, local recipients and users via LDAP from CSV files will be sent to the email addresses specified in this field. See Email Management for more details.
- **Number of minutes before my session expires** - You can set the idle session timeout period in the box. Enter the period in minutes or increase / decrease the period by clicking the up / down arrow. The valid entry is between 1 minute and 120 minutes. Please note this feature will not be available if an administrator is logged into CDAS using CAM credentials.
- **Spam trap email** (Optional) - If you already have a special 'spam-trap' email address then please enter it here to further improve CDAS message filtering.
- **Sites** (Optional) - Enter the URLs of all websites owned by your company in order to further improve spam filtering.
- Click 'Save' for your changes to take effect.
3.2.3.6 Users History

The 'Users History' area in 'Administrator Account Management' allows admins to view user history for all domains within a particular date range. From here you can filter users by IP address, last login, domain, username and/or location. By default, the most recent 15 records will be displayed.

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

3.2.4 Customer Management

The 'Customer Management' area allows an administrator to:

- View the details of the account they are logged into
- Create an account
- Update the product and extend your license term
- Configure subscriptions for the periodical Domain and Quarantine summary reports for domains
- Customize the 'support information' area in the notification emails that are generated for activities such as while adding a new user, password regeneration, quarantine request and quarantine report.

Click the following links for more details:

- End user license agreements
- Viewing customer information
- Managing subscriptions for reports
- Configuring language for messages from CDAS
- Notification email settings
3.2.4.1 End User License and Subscriber Agreements

The 'End User License / Subscription Agreement' interface displays the complete Comodo Dome Antispam - MSP End-User License and Subscriber Agreement.

To view End User License/Subscription Agreement

- Click 'Customer management' tab from the left hand side navigation to expand it and then click the 'End-User License/Subscriber Agreement.' tab from the sub menu.

The 'EULA/ Subscription Agreement' interface will be displayed:

3.2.4.2 Viewing License Information

The 'License Management' interface provides administrators with usage information.

To view the license management screen:

- Click the License Management from the 'Customer management' drop-down on the left

The example below shows a customer with multiple licenses:
The 'License Management' panel displays 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.

From the 'License Management' panel the you can get the the details of subscription(s) for the CDAS 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**
- The name of the account is displayed in the title bar.
- **CAM login**: 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**: The email address for the account as registered at CAM.

**Totals**
- **Number of users**: The total number of enrolled users belonging to all the domains.
- **Max. number of users**: The total 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**: The number of domains enrolled for account.
- **Max. number of domains**: The total number of domains that can be added as per all the subscriptions made for the account.
- **Disk quota**: The total storage space allotted in CDAS server for archiving incoming messages as per all the subscribed packages, in GB.
- **Disk space**: The storage space used by the archived mails in the CDAS server.

**Subscriptions**
The following details are displayed for each subscription:
- **Max. number of users**: The maximum number of users that can be added to the account as per the 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 added as per the subscription.
• **License expiration date:** The date till which the license is valid for the subscription.

• **Disk quota:** The maximum storage space allotted for mail archive in the CDAS server, as per the subscription.

• **Enabled:** Displays whether the subscription is active or not.

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

### 3.2.4.3 Manage Report Subscriptions

The 'Manage report subscriptions' interface lets you to configure subscriptions to 'Domain' and 'Quarantine' summary reports of all enrolled domains. Refer to [CDAS Reports - an Overview](#) for more details.

#### To access Manage report subscriptions interface

- Click Manage report subscriptions from the 'Customer management' drop-down on the left

The 'Manage report subscriptions' interface will open:

![Manage report subscriptions interface](image)

The 'Report recipients' field will be auto-populated with the email addresses of all the administrators available for the account and enabled for the same, at the time of adding them. The report recipients can be added or removed from this interface by entering the administrator's email address or deleting them and clicking the 'Save' button at the bottom.

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 CDAS. See [CDAS Reports - An Overview](#) for more details.
• **Domain Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly, will contain a detailed statistics of number of users, mails that have been received at and sent from the domain, number of spams identified and blocked and so on. See [CDAS Reports - An Overview](#) for more details.

**To configure the subscription of the reports**

- You can expand/collapse a report configuration section by clicking on the respective strip.
- If you want the administrators 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 reports without any statistics need not to be sent to recipients.
- Select the frequency at which the reports are to be sent to the administrators.

**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.

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

### 3.2.4.4 Configure Language for Messages from CDAS

The 'System messages locale' allows the administrator to configure the language of messages displayed and sent to the administrators of the domains by CDAS, according to the location of the administrators.

**To configure for the language of messages**

- Click 'System messages locale' from the 'Customer management' drop-down menu on the left

The 'System messages locale' interface will be displayed:
• Select the language in which CDAS should display and send its messages from the 'Change locale for system messages' drop-down. The messages will be displayed/sent in the selected language to the administrators of the domain managed by the currently logged in administrator.

• Click 'Save'

• The locale successfully set message will be displayed.

3.2.4.5 Notification Email Settings

By default, all the notification mails sent to administrators and users on various events like adding a new user, password regeneration, quarantine request or periodical report mails like quarantine report will contain the links to the online help guide and Comodo support in the footer.

The 'Email template settings' area allows you customize the footer for adding their contact and support information.

**To customize the notification emails**

• Click the Email template settings’ from the Customer management' drop-down on the left

The 'Email template settings' interface will be displayed:
Please note the customization can be done only in html format.

- Check 'Change default email footer' box if you want to edit details.
- Edit the details in html format as per your requirement and click 'Save' button.
- Click the 'Reset to default' button to display Comodo support information in the notification emails.

4 CDAS Reports - An Overview


- Reports are sent via email to administrators and users as configured

Global Reports and Domain level Reports

1. Global reports are for all domains covered by the customer account. See 'Managing Subscriptions for Reports' under 'Customer Management' for more details on the account level.

2. Domain level reports are specific to a domain. See 'Manage Report Subscriptions for Selected Domain' under 'Incoming' section for reports on domain levels.

Reports will be delivered at the scheduled times in the language set for the account.

CDAS creates five kinds of reports:

- **Quarantine Report** - A statistical breakdown of mails identified as spam or malicious that were moved to quarantine by CDAS. 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.

- **Users auto-import report** - The periodical report containing details of new users that were auto-imported into
CDAS for each domain, based on incoming mails received for them at the mail server. The report can be configured to be received hourly, daily, weekly or monthly by the administrator. The user auto-import reports are generated only for the domain level and not for the customer account level.

- **Quarantine Release Report** - The periodical report containing details of mails that were released from the quarantine list by both administrators and users with appropriate privileges. The report can be configured to be received hourly, daily, weekly or monthly by the administrator. The quarantine release reports are generated only for the domain level and not for the customer account level.

- **Reported Spam Report** - A detailed report of mails that were reported as spam by administrators as well as users with appropriate privileges. The report also includes details of mails that were uploaded as spam to CDAS. The report can be configured to be received hourly, daily, weekly or monthly by the administrator. The reported spam reports are generated only for the domain level and not for the customer account level.

- Reports can be enabled or disabled per administrator in **Dashboard > Account Management > Admin > Add Administrators** or **Edit Administrators**.

While the first two reports, Quarantine Report and Domain Statistics Report, are available for all the domains as well as for a specific domain, other reports are available for specific domains only.

### 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 CDAS, with the details on sender, receiver, date and attachments. You can view the contents of a mail by clicking its subject line from the report.

- **Administrator**
  - **Domain Level** - The Report generated for an administrator 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 a 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:
• Click the ‘Subject’ of a mail to open the mail in a new CDAS window. You need to login to CDAS 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(s). This includes information covering the number of users; mails that have been received at and sent from the domain; number of mail identified as 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 administrators.

- **Domain Level** - The report will contain only the details of domain statistics of the selected domain.
- **Customer Level** - The report 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** - Reports will be generated and sent every hour to the administrators through email.
- **Daily** - Reports will be generated and sent daily to the administrators through email.
- **Weekly** - Reports will be generated and sent to the administrators 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** - Reports will be generated and sent to the administrators 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** - Reports will be generated and sent to the administrators 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:

![Domain Statistics Report Example](image)

4.3 Auto-Imported Users Report

The 'Users Auto-Import' Report provides details on all new users belonging to a managed domain, that were automatically imported to CDAS on receiving an incoming mail addressed to them at the mail server. The auto-imported users are sent with an invitation email containing login credentials for them to access the CDAS user interface. For more details on managing auto-import, refer to the section [Manage User auto-import](#).

**Note:** The user auto-import reports are generated only for the domain level and not for the customer account level. The report is available only to the administrators.

The report contains the following details:

- **Imported users count** - The total number of users automatically imported into CDAS within the report time period.
- **Enabled users count** - The number of auto imported users that have activated their account by clicking the link in the invitation mail or logging-in to CDAS using the credentials provided in the mail.
- **Invited users count** - The number of auto imported users that have been sent the invitation mails but yet to activate their account.
User names list - The list of auto imported users.

An example of a 'Users Auto-Import Report' is shown below:

Here is the users auto-import report for csgqa.comodo.od.ua from Nov 21, 2014 09:00 to Nov 21, 2014 10:00

<table>
<thead>
<tr>
<th>Imported users count</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled users count</td>
<td>1</td>
</tr>
<tr>
<td>Invited users count</td>
<td>0</td>
</tr>
<tr>
<td>User names list</td>
<td>admin</td>
</tr>
</tbody>
</table>


4.4 Quarantine Release Report

The 'Quarantine Release Report' provides details of mails that were released from quarantine by the administrators as well as by the users with appropriate privileges. This also includes quarantine release requests accepted by administrators.

**Note:** The quarantine release reports are generated only for the domain level and not for the customer account level. The report is available only to the administrators.

The report can be subscribed to be received hourly, daily, weekly, monthly or yearly.

- **Hourly** - The reports 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 Quarantine Release Report is shown below:

![Quarantine Release Report](image)

4.5 Reported Spam Report

The 'Reported Spam Report' provides details of mails that were reported as spam by the administrators as well as by the users with appropriate privileges. This also includes details of mails uploaded from the 'Report Spam' interface.

**Note:** The reported spam reports are generated only for the domain level and not for the customer account level. The report is available only to the administrators.

The report can be subscribed to be received hourly, daily, weekly, monthly or yearly.

- **Hourly** - The reports 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 Reported Spam Report is shown below:
### Reported Spam report for csgqa4.comodo.od.ua from Jul 01, 2015 10:00 to Jul 01, 2015 11:00

<table>
<thead>
<tr>
<th>Date</th>
<th>Operation description</th>
<th>Login</th>
<th>Role</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wed Jul 01 10:06:38 GMT 2015</td>
<td>Report delivered message as spam</td>
<td><a href="mailto:admin1@csgqa4.comodo.od.ua">admin1@csgqa4.comodo.od.ua</a></td>
<td>admin</td>
<td>Recipients: <a href="mailto:user77@csgqa4.comodo.od.ua">user77@csgqa4.comodo.od.ua</a>; Sender: Dagwood Bumpsted &lt;<a href="mailto:avantistude@gmail.com">avantistude@gmail.com</a>&gt;; Date: Wed Jul 01 10:01:10 GMT 2015; Subject: Fwd: Get Instant Online Personal Loan approval and disbursement in 72 hours</td>
</tr>
<tr>
<td>Wed Jul 01 10:39:03 GMT 2015</td>
<td>Report delivered message as spam</td>
<td><a href="mailto:user77@csgqa4.comodo.od.ua">user77@csgqa4.comodo.od.ua</a></td>
<td>user</td>
<td>Recipients: <a href="mailto:user77@csgqa4.comodo.od.ua">user77@csgqa4.comodo.od.ua</a>; Sender: Dagwood Bumpsted &lt;<a href="mailto:avantistude@gmail.com">avantistude@gmail.com</a>&gt;; Date: Wed Jul 01 10:01:10 GMT 2015; Subject: Fwd: Get Instant Online Personal Loan approval and disbursement in 72 hours</td>
</tr>
<tr>
<td>Wed Jul 01 10:41:54 GMT 2015</td>
<td>Reports archived message as a Spam</td>
<td><a href="mailto:user77@csgqa4.comodo.od.ua">user77@csgqa4.comodo.od.ua</a></td>
<td>user</td>
<td>Recipients: <a href="mailto:user77@csgqa4.comodo.od.ua">user77@csgqa4.comodo.od.ua</a>; Sender: dagwood bumped &lt;<a href="mailto:avantistude@gmail.com">avantistude@gmail.com</a>&gt;; Date: Wed Jul 01 10:40:56 GMT 2015; Subject: Fwd: Zero Fees, Attractive Interest Rates and Loans upto 25l.</td>
</tr>
<tr>
<td>Wed Jul 01 10:52:02 GMT 2015</td>
<td>Reports archived message as a Spam</td>
<td><a href="mailto:user77@csgqa4.comodo.od.ua">user77@csgqa4.comodo.od.ua</a></td>
<td>user</td>
<td>Recipients: <a href="mailto:user77@csgqa4.comodo.od.ua">user77@csgqa4.comodo.od.ua</a>; Sender: oxford morris minor &lt;<a href="mailto:mcoxford@yahoo.com">mcoxford@yahoo.com</a>&gt;; Date: Wed Jul 01 10:47:33 GMT 2015; Subject: Dr. Jones wake up now</td>
</tr>
<tr>
<td>Wed Jul 01 10:55:26 GMT 2015</td>
<td>Reports archived message as a Spam</td>
<td><a href="mailto:user2@csgqa4.comodo.od.ua">user2@csgqa4.comodo.od.ua</a></td>
<td>user</td>
<td>Recipients: <a href="mailto:user1@csgqa4.comodo.od.ua">user1@csgqa4.comodo.od.ua</a>, <a href="mailto:user2@csgqa4.comodo.od.ua">user2@csgqa4.comodo.od.ua</a>; Sender: oxford morris minor &lt;<a href="mailto:mcoxford@yahoo.com">mcoxford@yahoo.com</a>&gt;; Date: Wed Jul 01 10:52:00 GMT 2015; Subject: Fwd: Dr. Jones wake up now</td>
</tr>
<tr>
<td>Wed Jul 01 10:55:52 GMT 2015</td>
<td>Reports archived message as a Spam</td>
<td><a href="mailto:user2@csgqa4.comodo.od.ua">user2@csgqa4.comodo.od.ua</a></td>
<td>user</td>
<td>Recipients: <a href="mailto:user1@csgqa4.comodo.od.ua">user1@csgqa4.comodo.od.ua</a>, <a href="mailto:user2@csgqa4.comodo.od.ua">user2@csgqa4.comodo.od.ua</a>; Sender: oxford morris minor &lt;<a href="mailto:mcoxford@yahoo.com">mcoxford@yahoo.com</a>&gt;; Date: Wed Jul 01 10:52:00 GMT 2015; Subject: Fwd: Dr. Jones wake up now</td>
</tr>
</tbody>
</table>
Appendix 1 - CDAS Error Codes

The most common error codes for CDAS are given below:

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unknown error</td>
</tr>
<tr>
<td>100</td>
<td>Import exception</td>
</tr>
<tr>
<td>101</td>
<td>Wrong format</td>
</tr>
<tr>
<td>102</td>
<td>Wrong outgoing user format IP password. If 'password' is empty then 'username' must be IP address.</td>
</tr>
<tr>
<td>103</td>
<td>Communication exception</td>
</tr>
<tr>
<td>200</td>
<td>User limit exception</td>
</tr>
<tr>
<td>300</td>
<td>Spam engine exception</td>
</tr>
<tr>
<td>1000</td>
<td>Customer has no domains</td>
</tr>
<tr>
<td>1001</td>
<td>Domains mismatch</td>
</tr>
<tr>
<td>1002</td>
<td>Alias already exists</td>
</tr>
<tr>
<td>1003</td>
<td>User already exists</td>
</tr>
</tbody>
</table>
### Appendix 2 - CDAS Feature List

<table>
<thead>
<tr>
<th>Features</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of domains and incoming / outgoing users</td>
<td>Depends on the subscription</td>
</tr>
<tr>
<td>Number of domain aliases</td>
<td>5</td>
</tr>
<tr>
<td>Active Directory / LDAP Synchronization</td>
<td>✓</td>
</tr>
<tr>
<td>Create / Modify User Groups</td>
<td>✓</td>
</tr>
<tr>
<td>Assign permissions to User Groups</td>
<td>✓</td>
</tr>
<tr>
<td>Number of user aliases per user</td>
<td>5</td>
</tr>
<tr>
<td>Incoming / Outgoing email filtering</td>
<td>✓</td>
</tr>
<tr>
<td>View all quarantined emails</td>
<td>✓</td>
</tr>
<tr>
<td>Release quarantined emails</td>
<td>✓</td>
</tr>
<tr>
<td>Whitelist / Blacklist quarantined emails</td>
<td>✓</td>
</tr>
<tr>
<td>Configure spam detection settings</td>
<td>✓</td>
</tr>
<tr>
<td>Report spam emails</td>
<td>✓</td>
</tr>
<tr>
<td>View queued emails in Delivery Queue</td>
<td>✓</td>
</tr>
<tr>
<td>Force Retry (Force Deliver) selected or all queued emails in Delivery Queue</td>
<td>✓</td>
</tr>
<tr>
<td>Create local recipients</td>
<td>✓</td>
</tr>
<tr>
<td>Clear incoming / outgoing email cache</td>
<td>✓</td>
</tr>
<tr>
<td>Log search incoming emails</td>
<td>✓</td>
</tr>
<tr>
<td>Log search outgoing emails</td>
<td>✓</td>
</tr>
<tr>
<td>Create domain aliases</td>
<td>✓</td>
</tr>
<tr>
<td>Configure domain settings</td>
<td>✓</td>
</tr>
<tr>
<td>Configure email size restrictions</td>
<td>✓</td>
</tr>
<tr>
<td>Configure 'Blocked extensions' settings</td>
<td>✓</td>
</tr>
<tr>
<td>View users' release requests</td>
<td>✓</td>
</tr>
<tr>
<td>View users' whitelist / blacklist requests</td>
<td>✓</td>
</tr>
<tr>
<td>Whitelist / Blacklist recipients</td>
<td>✓</td>
</tr>
<tr>
<td>Whitelist / Blacklist senders</td>
<td>✓</td>
</tr>
<tr>
<td>View users' login history</td>
<td>✓</td>
</tr>
<tr>
<td>Email archive</td>
<td>✓</td>
</tr>
</tbody>
</table>
Appendix 3 - Troubleshooting LDAP

This section explains how to resolve some common problems that may arise when configuring LDAP.


- **Problem: Unhandled Exception:**
  Solution: The exception was not classified.

- **Problem: Size limit exceeded, unable to extract more then users from server. Size limit must be increased on server side or specify more strict query**
  Solution: Active Directory server has limitation on the number of search entries which may be iterated during querying. By default, Microsoft Active Directory allows only 1000 search entries. If the server received more than that, the administrator should override the default LDAP search size limit in the Active Directory, or use more strict query

- **Problem: Incorrect filter settings:** ...
  Solution: Filter settings contain incorrect format or AD server doesn’t support it.

- **Problem: Incorrect BaseDN settings:** ...
  Solution: BaseDN value has incorrect format.

- **Problem: Unable to connect with provided host in BaseDN settings:** ...
  Solution: Provided domain name for BaseDN setting cannot be resolved in AD forest tree. Assure a domain name is correct.

- **Problem: Unable to resolve LDAP referral, host unreachable. Users had found before referral might be imported. Possible solution is to use Global Catalog server (port 3268/3269 as default) to avoid resolving referrals.**
  Solution: CDAS is trying to extract as much as possible information and following referrals to resolve all search entries in a query. If the URL in the referral is unreachable by CDAS then the iteration will stop. Only partial result will be provided. That occurs when an administrator uses a private domain and it cannot be accessed with only domain name (the referral contains the list of URLs of the explicit domain names but the information about servers located in the private subnet is absent). To avoid the referrals occurrence in search entries use the Global Catalog server for querying. By default, the port for this server is 3268/3269 and that depends on whether the SSL enabled or not.

- **Problem: Unknown error. Users found before error might be imported. Original exception - ...**
  Solution: Search entries has been terminated within the replication process. Please contact support to find a solution.

- **If you do not know your BaseDN, here's a step-by-step guide to determining your BaseDN.**
  Most organizations follow a similar convention for their determined BaseDN when the organization sets up its Active Directory. For a company with the domain of example.com, the typically BaseDN is `cn=Users,dc=example,dc=com`
Appendix 4 - Useful Links

This page contains links to external webpages which provide detailed explanations of LDAP features.

What Is the Global Catalog?


Global Catalog and LDAP Searches


LDAP Referrals


Click the following links for more details http://help.comodo.com/topic-445-1-914-12228-Importing-Users-from-LDAP.html
About Comodo

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

Comodo Security Solutions, Inc.

1255 Broad Street
Clifton, NJ, 07013
United States
Tel: +1.888.256.2608
Tel: +1.703.637.9361
Email: EnterpriseSolutions@Comodo.com