

COMODO
CYBERSECURITY



Comodo Secure Email Gateway MSP

Software Version 2.12

Quick Start Guide

Guide Version 2.12.051520

Comodo Security Solutions
1255 Broad Street
Clifton, NJ, 07013

Comodo Secure Email Gateway MSP - Quick Start Guide

This tutorial briefly explains how to setup and configure Comodo Secure Email Gateway – MSP (CSEG) email filtering system.

The guide assumes that you have already obtained a license. Please [click here](#) if you need help to purchase a license.

The guide will take you through the setup, initial configuration and usage of the product. Click any link to go to the section with which you need help.

- [Step 1 - Login to the Admin console](#)
- [Step 2 - Configure your mail server to work with the CSEG service](#)
- [Step 3 - Add domains](#)
- [Step 4 - Validate domains](#)
- [Step 5 - Add administrators](#)
- [Step 6 - Add incoming users](#)
- [Step 7 - Add outgoing users](#)
- [Step 8 - Manage configuration and settings](#)
- [Step 9 - View reports](#)

Step 1 - Login to the Admin console

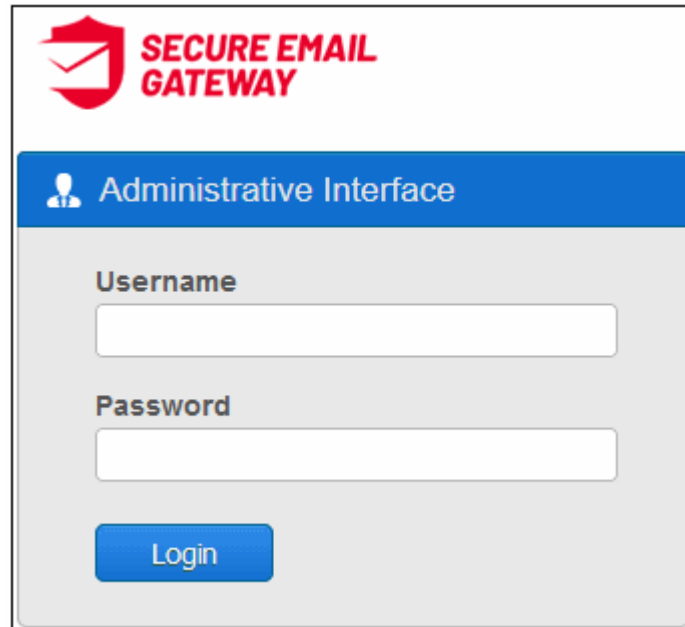
You can login to the admin console directly at your service URL, or you can login via the Comodo One (C1) / Dragon / ITarian portal.

- [Direct login](#)
- [Login via C1 / Dragon / ITarian](#)

Direct Login

You can login at your service URL using any internet browser. The URL depends on the region that hosts your data:

- EU - <https://domeasmsp.cdome.net/admin/login.zul>
- USA - <https://us-domeasmsp.cdome.net/admin/login.zul>

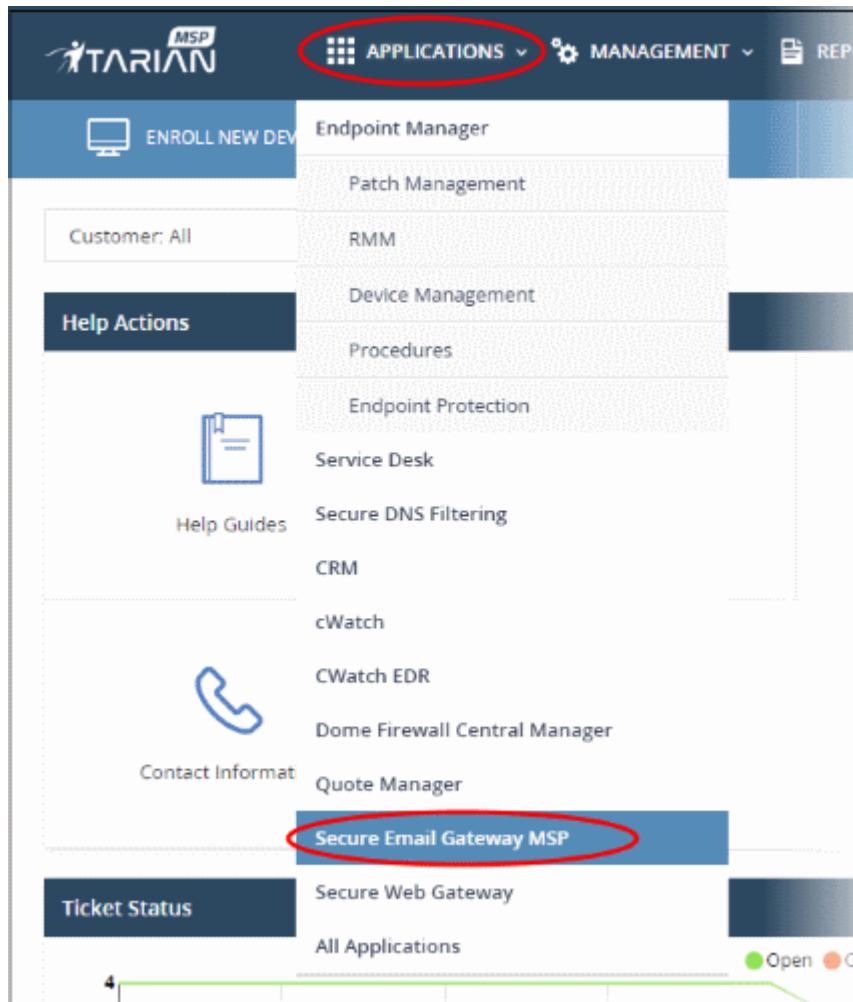


The screenshot shows the login page for the Comodo Secure Email Gateway Administrative Interface. At the top left is the logo, which consists of a red shield with a white envelope icon and the text "SECURE EMAIL GATEWAY" in red. Below the logo is a blue header bar with a white user icon and the text "Administrative Interface". The main content area is light gray and contains two input fields: "Username" and "Password". Below these fields is a blue "Login" button.

- Login to the interface with your CSEG username and password.
- Please note, your account is locked after three failed attempts login attempts. Contact your Comodo account manager if you need to unlock your account.
- To logout of the interface, close the browser window or click your username at top-right then 'Logout'

Login via Comodo One / Comodo Dragon / ITarian portal interface

- Login to your C1 / Dragon / ITarian account (ITarian portal is shown below as an example)
- Click 'Applications' > 'Secure Email Gateway MSP':



- Secure Email Gateway MSP opens at the dashboard

Step 2 - Configure your mail server to work with the CSEG service (see **Getting Started** if you need more help with this)

The next step is to setup incoming and outgoing filtering configuration.

Comodo has two Secure Email Gateway servers, one in US and other in EU. You can choose any of these locations that best suit your requirement. For example, some US customers would like to keep their data in servers that are located within their country. The details of CSEG service domains are given below:

CSEG Server Locations

European Union

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

United States

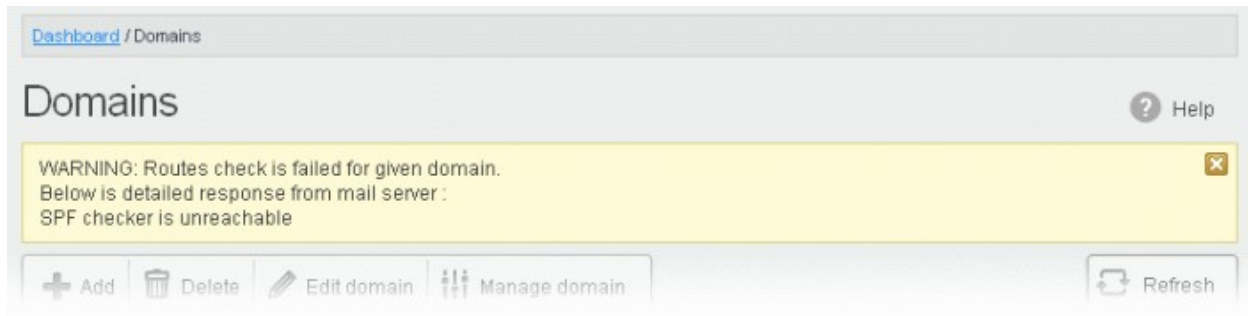
- mxpool1.us.spamgateway.comodo.com

Note – MX records

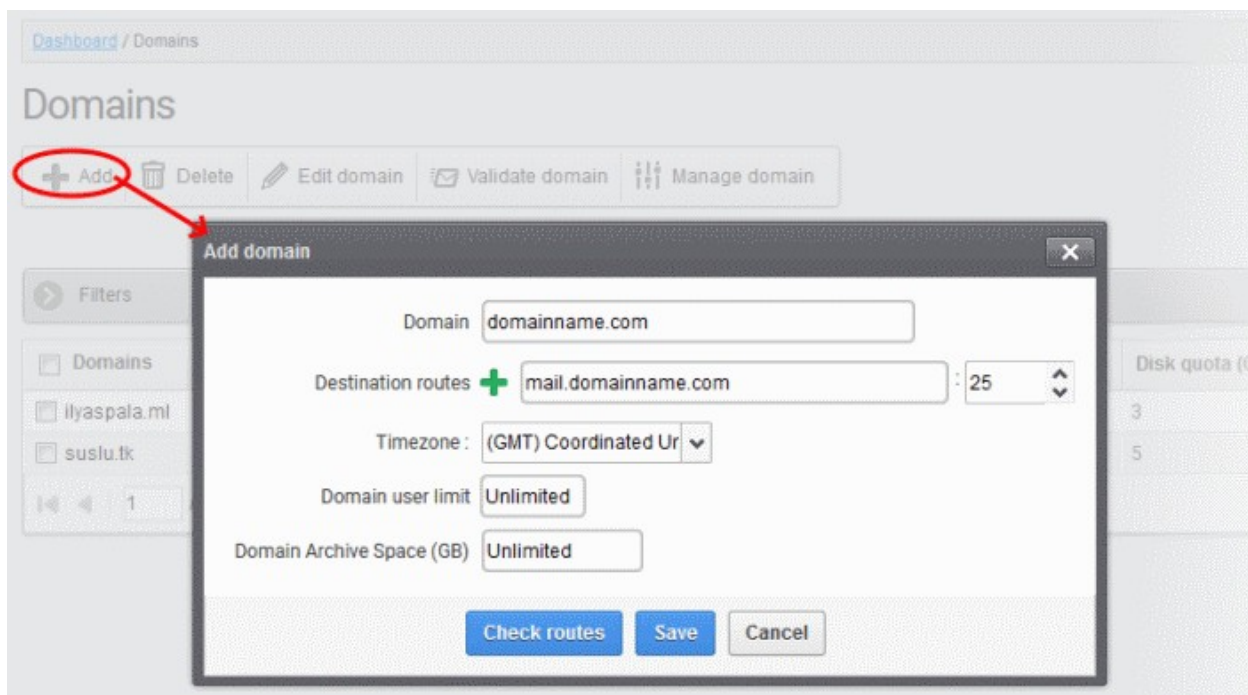
- Comodo One / Comodo Dragon / ITarian customers should use the EU or US service server URL based on their location preference during sign up.

Incoming Filtering Configuration

1. Configure your mail server – You need to disable Sender Policy Framework (SPF) checks, or add **CSEG service domains** to the SPF whitelist
 - If you don't do one of the above, you may get an error message when you add a domain:



2. Add your domain to the CSEG service - **Login** to CSEG, go to domain management and add domain.



See **Add a Domain** topic if you need more help with this.

3. **Configuring MX record**
 - The next step is to update the mail exchange (MX) records of your domain to point to the **CSEG service domain**.
 - Please ensure that you replace your domain's old MX records with the **CSEG service domain** according to your preferred region.

Background: MX records specify the mail server for incoming and outgoing mail on a domain. A domain can have several MX records pointing to different mail servers. When an email is passed to/from your domain, the mail is handled by the first available mail server as per your priority. You can define new MX records or change mail server priority as required.

Click the following links for detailed explanations based on the DNS software/web hosting service you use.

- **Windows Server 2003/2008**

- [BIND \(and the “named” daemon\)](#)
- [Comodo DNS](#)
- [GoDaddy](#)
- [Enom](#)
- [Network Solutions](#)
- [Yahoo! SmallBusiness](#)
- [1and1](#)
- [4D Web Hosting](#)
- [DNS Park](#)
- [DreamHost](#)
- [DynDNS](#)
- [IX Web Hosting](#)
- [No-IP](#)
- [Cpanel](#)

Outgoing Filtering Configuration

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.

1. **Per-user authentication** - To set up outgoing filtering for a user, make sure that the user is a valid outgoing user. 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 **Users** topic if you need more help with this.
2. **Outgoing Smarthost setup** – You can choose this option instead of per-user authentication method to setup outgoing filtering via CSEG. A smarthost allows an SMTP server to route email to an intermediate mail server. This can ease mail server management. In this case all outgoing messages are sent to CSEG mail-server and the actual recipient is contacted by CSEG mail-server 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.
3. **DNS Configuration** – Add this SPF record into your public DNS:

- include:_spf.antispamgateway.comodo.com

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. Click on the following links for more details:

- [Configure QMail to use a Smarthost](#)
- [Configure PostFix to use a Smarthost](#)
- [Configure Sendmail to use a Smarthost](#)
- [Configure Exchange 2000/2003 to use a Smarthost](#)
- [Configure Exchange 2007/2010 to use a Smarthost](#)
- [Configure Exchange 2013/2016 to use a Smarthost](#)
- [Configure Office 365 to use a Smarthost](#)
- [Configure Exim to use a Smarthost](#)
 - [Configure Exim / cPanel to use a Smarthost](#)

- **Configure Exim / Directadmin to use a Smarthost**

See **Getting Started** if you need more help with this.

Step 3 - Add domains (see '[Add a Domain](#)' topic if you need more help with this)

The number of domains that can be added for your account depends on the subscription plan that you have purchased.

1. Click the 'Domains' tab on the left navigation to open the Domains area.
2. Click 'Add' and in the 'Add domain' dialog, enter a valid domain name in the 'Domain' field.
3. Enter the location of your mail-server in the 'Destination route' field. This is where CSEG will send your mail after it has been processed. The default port is 25. Click **+** to enter an additional route in case the primary route is unavailable for some reason.
4. Select the timezone for the domain from the 'Timezone' drop-down.
5. Click the 'Check routes' button to get CSEG to retrieve destination route information from your DNS. If the result contains the MX URL of the **CSEG service domain**, then the DNS MX record was already updated to work with Secure Email Gateway. You must enter your real MX record in the 'Destination route' field. For example mail.exampledomain.com.
6. Enter the maximum number 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.
7. Set the archive disk quota that this domain should use for storing mails. The disk space for all your domains cannot exceed the disk quota that you subscribed for.
8. Click 'Save' to add the configured domains.

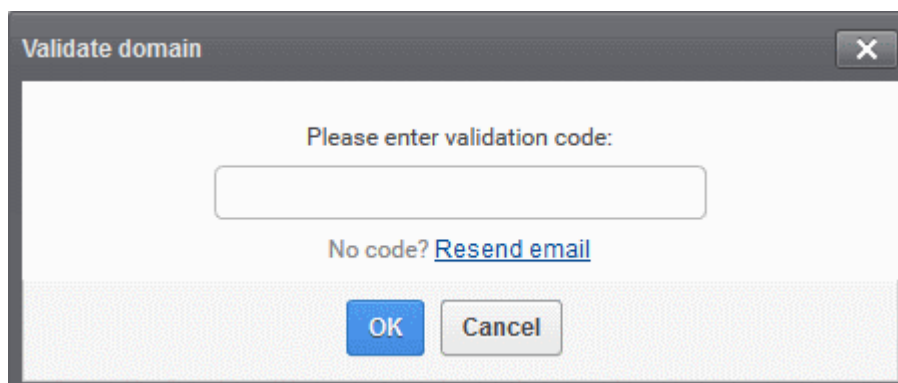
If you have already configured the MX record for the domain as explained in **Step 2** to the CSEG service before adding it to CSEG interface, then you can skip the next step and proceed to Step 5.

Step 4 – Validate Domains

You need to prove you own a domain before it can be used with CSEG. This is done by completing the domain control validation (DCV) process. There are a couple of ways to do this:

- You can complete DCV by configuring your MX record for the domain as explained in **Step 2**
 - You can complete DCV by answering a challenge-response email sent to postmaster@ on the domain in question. Follow the instructions below if you wish to use this method:
1. Click the 'Domains' tab on the left to open the 'Domains' area.
 2. Select the domain that you want to validate.
 3. Click the 'Validate domain' button

This opens the validate domain dialog:



Validate domain

Please enter validation code:

No code? [Resend email](#)

OK Cancel

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.

- Copy the code from the mail, paste it into the field provided and click 'OK'

CSEG will verify the code and, if successful, the domain is activated.

Step 5 - Add administrators (see '[Adding New Administrators](#)' if you need more help with this)

Add new administrators for a domain:

1. Click 'Admins' from the 'Account management' drop-down menu on the left navigation
2. In the Admins configuration interface, click the 'Add' button.
3. Add the new administrator by completing their user details, including login username and email address (for receiving system notifications). You can also specify whether the new admin is allowed to access the CSEG interface and whether they should have a subscription for global reporting.
4. Click the 'Save' button.

Step 6 - Add incoming users

Admins can add users manually or import user lists via .csv or Lightweight Directory Access Protocol (LDAP). To get started:

- Click 'Domain' on the left, select the domain for which you want to add users and click the 'Manage domain' button.

1. To add users manually:

- Click 'Domain' > select the domain for which you want to add users > click 'Manage domain'
- Click 'Account management' > 'Users' on the left hand menu.
- Click the 'Add' button in the 'Users' interface.
- Enter the username of the new user in the 'New User' dialog. This name becomes the first part of their email address. For example, if you add a user called 'alice', their email address is 'alice@your-domain.com'.
- The dialog also allows you to add the user to the recipient whitelist, to add them as recipients of quarantine reports, and to grant the user access to the CSEG interface.
- Click the 'Save' button.
- See '[User Account Management](#)' if you need more help with this.

2. To import users via a .csv file:

- Click 'Domain' > select the domain for which you want to add users > click 'Manage domain'
- Click 'Account management' > 'Users' on the left hand menu.
- Click 'More Actions' > 'Import from CSV file'.
- Users should be listed in the following format in the .csv file:

```
username1, domain.com, true  
username2, domain.com, false
```
- E.g. `alice,example.com,true`. True/false determines whether or not a user can access the CSEG interface.
- Click 'Upload', navigate to where your file is saved and click 'Open' to import the .csv file..
- See '[User Account Management](#)' if you need more help with this.

3. To import users via LDAP.

You can configure CSEG to import users from an AD server using the Lightweight Directory Access Protocol (LDAP). Once configured, CSEG can periodically synchronize with AD and add or remove users as their


status changes on the AD server.

Comodo strongly recommends that a separate LDAP/AD account be created for the purposes of the CSEG login and that this user account is allocated read-only permissions.

- Click 'Domain' > select the domain for which you want to add users > click 'Manage domain'
- Click 'Account management' > 'LDAP import configuration' on the left hand menu.
- Enter/ select the required configuration settings.
 - Click 'Save' to store these settings for later
 - Click 'Save and run synchronization now' to save your settings and import users from your AD server
- Click 'LDAP import confirmation list' (under 'Account management' on the left) to view the differences between the CSEG and AD user lists.
 - Users present in AD but not present in CSEG – click 'Create' to add them to CSEG
 - Users present in CSEG but not present in AD – click 'Delete' to remove them from CSEG
- Click 'Run Synchronization Now' to fetch the latest users from AD. All new users are displayed.
 - Click 'Apply import by filter' to import users after applying a filter of your choice
 - Click 'Apply import by selection' to manually select the users you wish to import
 - Clear all filters and click 'Apply import by filter' to import the latest user list from AD
- Click 'OK' in the confirmation dialog.

Add users to ignore list

Users in the ignore list are not added, deleted or updated when CSEG synchronizes with Active Directory.

- Click 'Account management' > 'LDAP import ignore list'
- Click 'Add'. The 'Add ignored' user dialog will open.
- Enter the users you wish to ignore. Click the  icon to add more users
- Click 'Save' to add the users to the ignore list.

See [Importing Users from LDAP](#) if you need more help with this area.

Step 7 - Add outgoing users (see '[Users](#)' topic if you need more help on this)

Outgoing emails should be checked for spam or malware because of the risk such content poses to your company's reputation. Outbound email often bypasses corporate antispam filters and goes direct to the destination. Filtering outgoing mail will prevent spam emanating from your organization.

Configuring User's Email Client for Outgoing Mail Filtering

1. The email clients of the users added for outgoing email filtering are to configured to point to CSEG service.
2. In the Account Settings interface of the user's email client, enter the following details:
 - Smtplib server: mxpool1.spamgateway.comodo.com or mxpool1.us.spamgateway.comodo.com depending on your configured **CSEG service domain**
 - Connection Security: STARTTLS or SSL
 - Port : 587
 - Username: <username@domainname.com>

To add a new user to the outgoing list

An administrator can add outgoing users manually one by one or import them as bulk via a CSV file.

1. Click the 'Users' tab from the 'Outgoing' drop-down menu on the left navigation
2. To add users manually, click the 'Add' button.
3. In the 'Add outgoing user' dialog, enter the username of the new user.

4. 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 are considered authenticated without needing to use SMTP AUTH (Note: authorizing IP addresses may be disabled on the system).
5. The 'Edit outgoing settings' allows you to configure various outgoing settings.
 - **Automatic lock** - CSEG will prevent a user from sending mail if it detects they have sent out spam or malware. You can set the length of this ban in the 'User lock timeout' field.
 - **User lock timeout** – Time in minutes that a user is banned from sending mail if CSEG detects their account has sent spam. See 'Automatic lock' above.
 - **Maximum unlocks by timeout** - The number of times the locked out user is unlocked for sending out mails. After reaching the maximum limit, the user is 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 CSEG will retry to send queued outgoing mails after which they are bounced to the user.
 - **Quarantine response** – Determines the response that CSEG 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 mails are quarantined (and not delivered to the recipient) regardless of your choice here. These options merely determine what message CSEG sends 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 are not notified if the outgoing mails are detected as spam. They are blocked and not delivered to recipients.
6. Click the 'Save' button.
 7. To add many users at a time, importing them via a CSV file is the best option. The users should be saved in 'comma separated value' (CSV) as shown below:

```
user1,domainname,password  
user2,domainname,password
```
 8. Click the 'Import from CSV file' button to import outgoing users from a CSV file.
 9. Click 'Upload' and navigate to the location where the file is saved and click the 'Open' button to add new outgoing users.
 10. Click 'Import from incoming users' to add all incoming users to the outgoing users list.

Step 8 - Manage configuration and settings (see '**Manage a Domain**' topic if you need more help with this)

You can manage and configure various settings for a selected domain such as view quarantined mails, add users as recipient whitelist or blacklist, add new users and so on. Click the following links for more details about each activity.

- **Incoming**

- 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 for selected domain
- Relay restrictions
- Geolocation restrictions
- SPF Control Settings
- **Outgoing**
 - Clear outgoing cache
 - Log search
 - Users
 - Office 365 Activation
- **Email Management**
 - Email size restriction
 - Blocked extensions
 - Released requests
 - Blacklisted requests
 - White-listed requests
- **Domain Audit Log**
 - Audit log configuration
 - View domain log
- **Domain Rules**
 - Rules
 - TLD and gTLD rules
 - Recipient whitelist
 - Sender whitelist
 - Recipient blacklist
 - Sender blacklist
 - Whitelist senders per user
 - Blacklist Senders per user
- **Account Management**
 - User account management
 - User auto-import
 - Users history
 - Importing users from LDAP

Step 9 - View Reports

Comodo Secure Email Gateway can periodically generate different kinds of reports that are sent to administrators and users. CSEG generates two types of report - a global report for all domains belonging to the account and another

specific for a domain. The reports for these types are similar except the former will contain reports for all domains while the latter will contain reports for the selected domain.

To add new subscriber(s) in the report subscription list for a selected domain

1. Click 'Domain' > select the domain for which you want to add subscriber > click 'Manage domain'
2. Click 'Incoming' > 'Manage report subscriptions' on the left hand menu
3. Enter the full email address of the subscriber(s) in the 'Report recipients' text box. You can add multiple subscribers at a time with each email addresses separated by a comma. You can also add subscriber(s) in each report configuration area, if required.
4. Select the 'Enabled' buttons in the respective report configuration area for receiving the reports.
5. Select the frequency of the report to be sent to the subscribers from the options. (see the topic '**Manage Report Subscription for Selected Domain**' if you need more help with this)
6. Click the 'Save' button at the bottom.
7. To remove subscriber(s), just delete them in the 'Report recipients' text box and click the 'Save' button at the bottom.

The types of reports available for a selected domain are:

- **Domain statistics report**
- **Quarantine report**
- **Quarantine release report**
- **Reported spam report**
- **Users auto-import report**

To add new subscriber(s) in the report subscription list for all domains in the account

There are two methods you can add subscribers for receiving global reports.

1. At the time of adding new administrators.
 - Click 'Account management' > 'Admins' on the left hand menu
 - Click the 'Add' button.
 - After filling out other details in the 'New administrator' dialog, select the 'Subscribe emails to global reporting' check box.
 - Click the 'Save' button.
2. In the 'Manage report subscriptions' interface.
 - Click 'Customer management' > 'Manage report subscriptions' on the left hand menu
 - Enter the full email address of the subscriber(s) in the 'Report recipients' text box. You can add multiple subscribers at time with each email addresses separated by a comma. You can also add subscriber(s) in each report configuration area, if required.
 - Select the 'Enabled' buttons in the 'Quarantine report' and 'Domain statistics report' configuration area for receiving both the reports.
 - Select the frequency of the report to be sent to the subscribers from the options for Quarantine Report and Domain Statistics Report. (see the topic '**Manage Report Subscriptions**' if you need more help with this)
 - Click the 'Save' button at the bottom.

There is only one way to remove subscribers from the list.

- To remove subscriber(s), just delete them in the 'Report recipients' text box and click the 'Save' button at the bottom.

The types of global reports available for an account are:

- **Quarantine report**
- **Domain statistics report**

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit [comodo.com](https://www.comodo.com) or our [blog](#). You can also follow us on [Twitter](#) (@ComodoDesktop) or [LinkedIn](#).

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

Email: EnterpriseSolutions@Comodo.com