



COMODO
Creating Trust Online®

COMODO DOME
A N T I S P A M


Comodo Dome Antispam

Software Version 6.7



Quick Start Guide

Guide Version 6.7.010819



Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Comodo Dome Antispam – Quick Start Guide

This tutorial briefly explains how administrators can setup and configure Comodo Antispam email filtering system.

This quick start guide will take you through the setup, initial configuration and usage of the product - click on any link to go straight to that section as per your current requirements.

- **Step 1 – Purchase License and Login to Dome Antispam**
- **Step 2 – Get Started**
- **Step 3 – Add Domains**
- **Step 4 – Add Users**
- **Step 5 – Configure SMTP Settings**
- **Step 6 – Configure Dome Antispam Security Components**
- **Step 7 – Configure Quarantine & Archive Mail Settings**
- **Step 8 – System Configuration**

Step 1 – Purchase License and Login to Dome Antispam

Purchase a License

You can set up your antispam instance on the cloud or on your premises.

- **Cloud customers**
 - Create a C1 account at one.comodo.com.
 - Click 'Store' in the top-menu then purchase a Comodo Antispam license.
 - Comodo will set up your cloud antispam instance
- **On-premise customers** – Purchase a license at <https://accounts.comodo.com/account/login>, download the antispam VMware image and deploy it.

Cloud Customers

- Purchase a Dome Antispam license from the C1 interface.
 - If you do not already have one, you can sign up for a free C1 account at <https://one.comodo.com/>
- Visit <https://one.comodo.com> and **login** to C1
- Click 'Store' on the menu bar
- Click 'Buy' on the 'Dome Antispam' tile and complete the license subscription process. **Click here** for help with the purchase process and configuring Dome Service URL settings.

On-premise Customers

- Visit <https://accounts.comodo.com/account/login> and complete the license purchase process. The license key and other details will be sent to your registered email address.
- Next, download the Dome AS VMware image:
 - HyperV Template - https://download.comodo.com/domeasg/DomeASG_hyperv.rar

Or

- ESX Template - https://download.comodo.com/domeasg/DomeASG_esx.rar
- [Click here](#) for help to deploy Dome AS on your network.
- After installation, [login](#) to Dome AS and activate your license. [Click here](#) if you need help with this.

Login to Dome Antispam

- [Cloud Customers](#)
- [On-premise Customers](#)

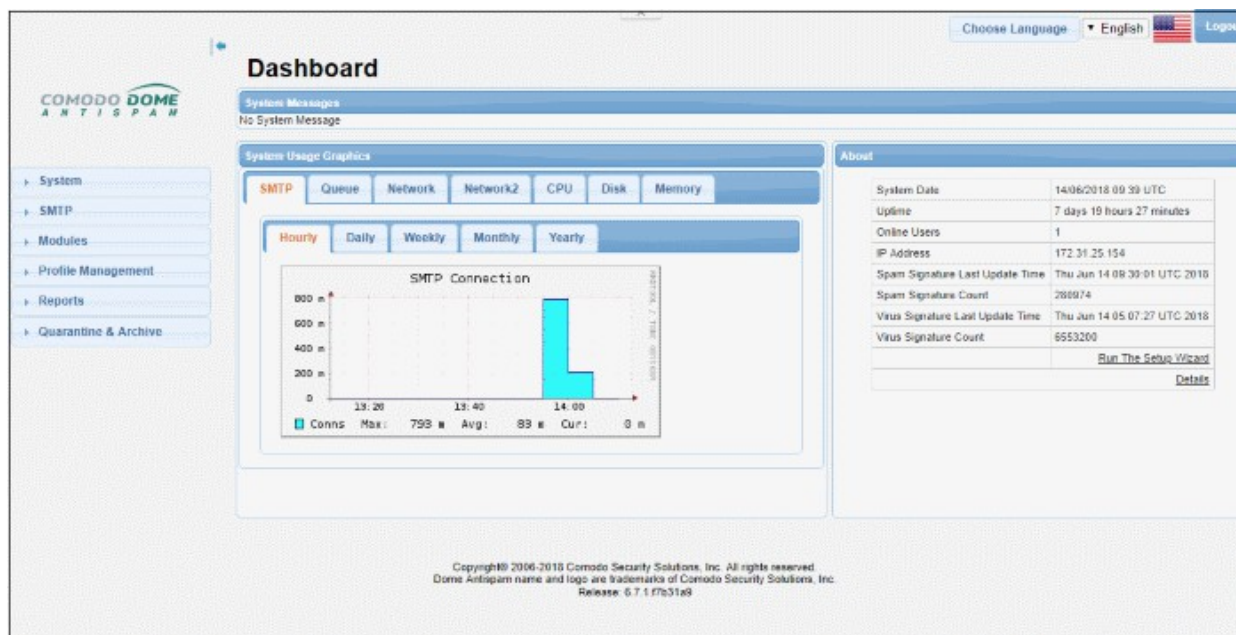
Cloud Customers

- [Login](#) to your C1 account at <https://one.comodo.com>
- Click 'Applications' > 'Dome Antispam' in the C1 menu

On-premise Customers

- The IP address of your instance was configured during Dome AS deployment. For example: <https://ip-address:8443>
- Login using any web-browser. Default credentials:
 - Username: admin
 - Password: admin

Dome Antispam will open at the dashboard:



Step 2 – Get Started

Cloud Customers

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

- Incoming Filter Configuration
 - Comodo will set up your antispam instance. After this is done, you will receive a mail that contains your account and service URL details. If you think there is a delay in this process, contact Comodo support at domesupport@comodo.com
 - Change your incoming mail server domain mx records to point to Dome Antispam. Mail will be directed to your domain after passing through antispam filtering.

- Enter routing details in 'SMTP' > 'Domains' > 'Routes'. See **Step 3** to find out how to add domain names and their corresponding routing types. If no routing is configured then the default domain routing applies.
- **Outgoing Filter Configuration**
 - The outgoing filter checks mail that is sent from your network. You can enable the feature by routing your outgoing traffic to your dome antispam service URL.
 - This service URL is same as used for incoming filtering. This URL is sent to you after Comodo finish provisioning your instance. If you have any questions or need assistance, do not hesitate to contact domesupport@comodo.com

On-premise Customers

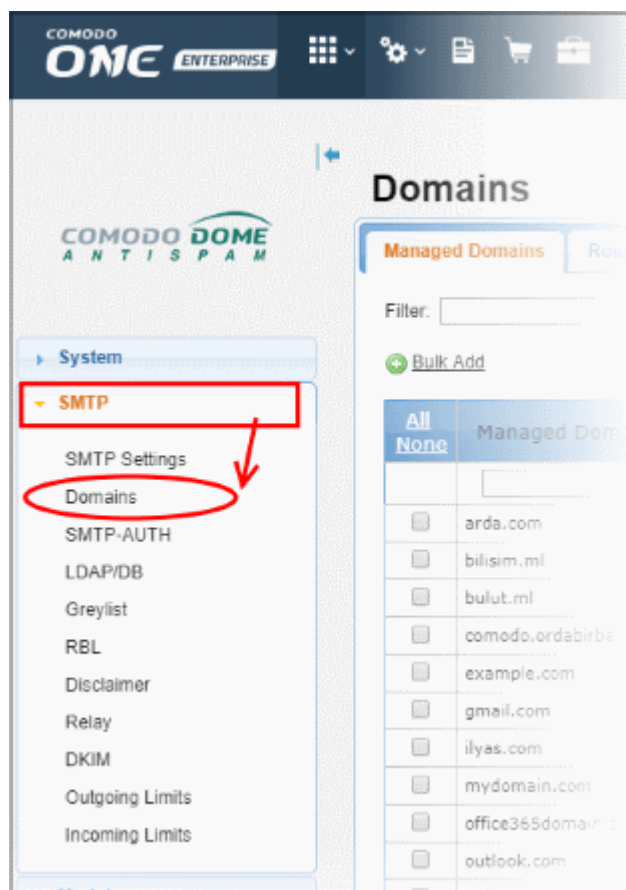
- All required configurations are done during deployment. **Click here** for help to deploy Dome AS on your premises.

Step 3 – Add Domains

The next step is to add domains which you want to protect with Dome Antispam.

To add domains:

- Click 'SMTP' > 'Domains'



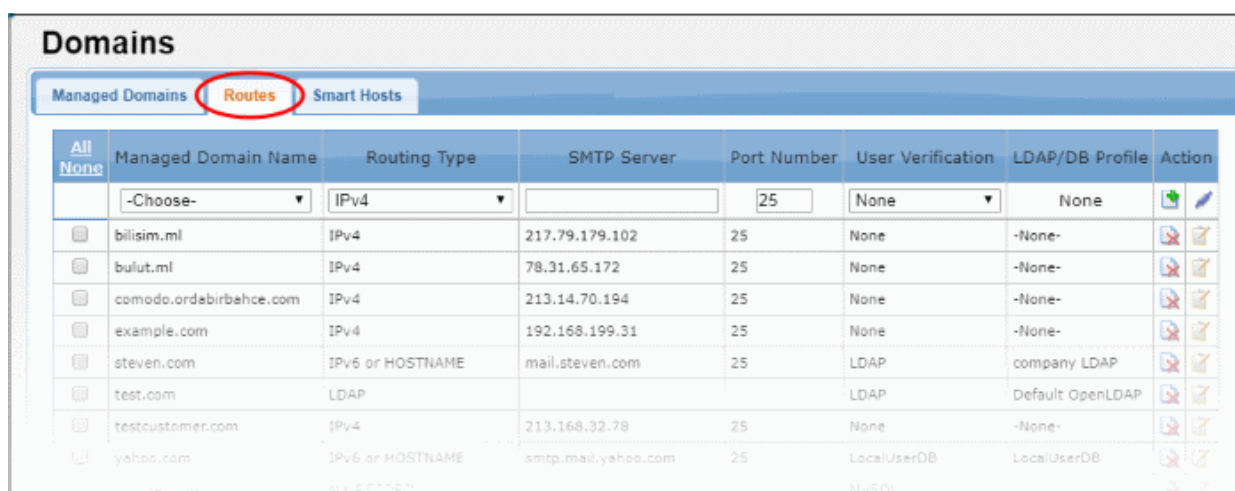
- Enter the domain name in the field under 'Managed Domain Name' column



- Click the button in the 'Action' column.
 - Alternatively, you can add multiple domains using the 'Bulk Add' link.

The next step is to define the route from Dome Antispam to your SMTP server. Dome will filter incoming mail then use this route to forward the mail to your server. If left undefined then the 'default route' will apply.

- Click 'SMTP' > 'Domains'
- Click the 'Routes' tab
- Use the drop-down menus in the top row to specify a route for the domain:



- **Managed Domain Name** - Select the domain for which you want to configure the incoming route.
- **Routing Type** – Choose the method you want to use to send mail to the SMTP server. The options available are IP4, IP6 or Hostname, MX Record and LDAP.
- **SMTP Server** – Host name or IP address of the incoming mail server. Dome Antispam will forward mail to this server after filtering.
- **Port Number** – The port number of the SMTP server through which Dome Antispam should forward mail.
- **User Verification** and **LDAP / DB Profile** - Depending on the 'User Verification' type chosen, the 'LDAP/DB Profile' column will be populated. If 'LDAP' is chosen as 'User Verification' then the LDAP profiles added in LDAP/DB section will be shown in the drop-down. Select the LDAP profile from the options.
- Click to check the connection between Dome Antispam and the remote server. The result is shown at the top.
- Click the button to save the route.

The domain route will be added to the list.

Alternatively, you can define a the default route in the 'Smart Hosts' interface:

- Click SMTP > Domains > Smart Hosts tab.
- Select 'Enable Default Domain Routing' check box and provide the SMTP server details.

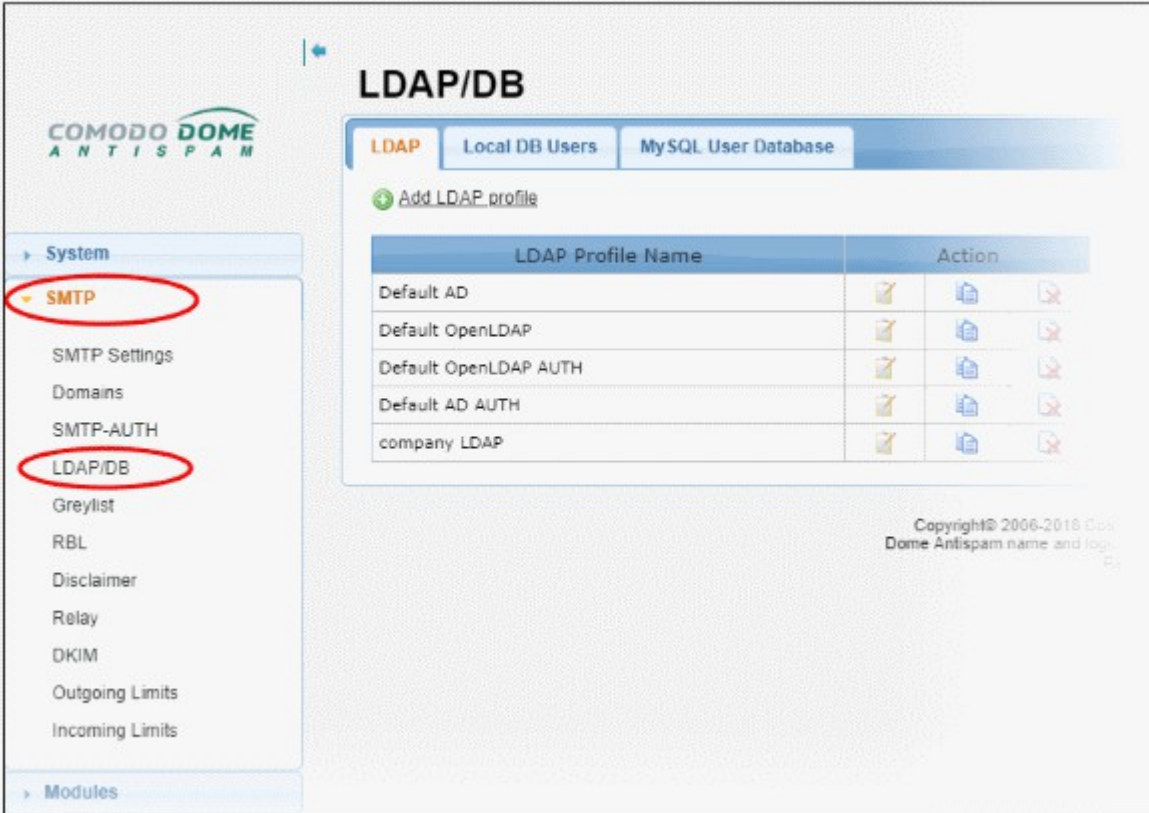
The default route will apply if you do not set a custom route for a domain. See **Default Domain Routing** for more information.

See **Manage Domains** for more details about managing domains, domain routes and smart hosts.

Step 4 – Add Users

Dome Antispam will only filter mail for valid recipients. You can add users manually and/or import users from an LDAP server / My SQL User Database.

- Click SMTP > LDAP/DB:

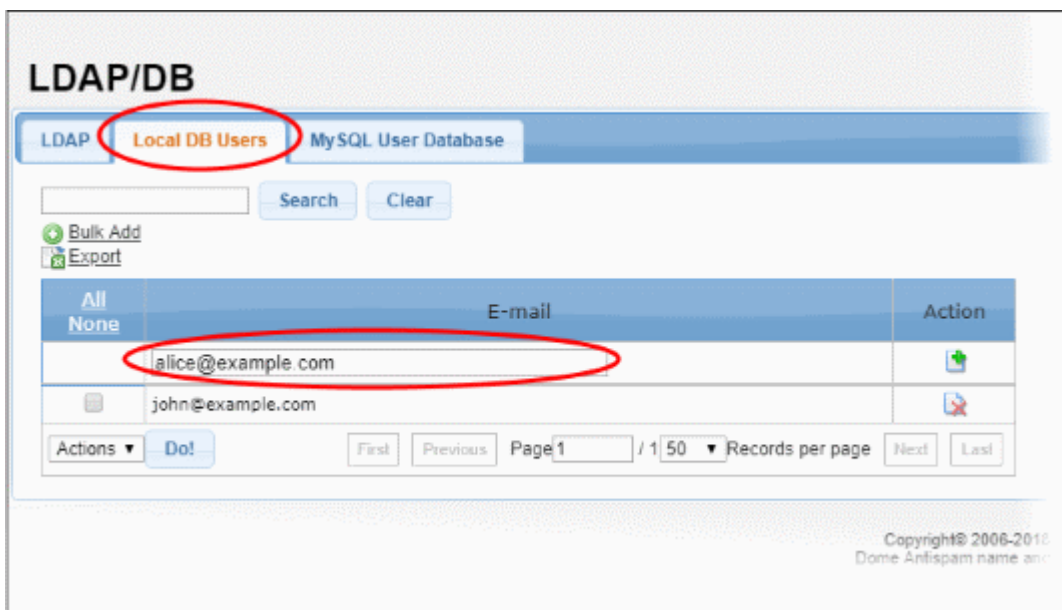



The screenshot shows the Comodo Dome Antispam web interface. On the left is a navigation menu with 'SMTP' and 'LDAP/DB' highlighted with red circles. The main content area is titled 'LDAP/DB' and has three tabs: 'LDAP', 'Local DB Users', and 'MySQL User Database'. The 'LDAP' tab is active, showing an 'Add LDAP profile' button and a table of LDAP profiles. The table has columns for 'LDAP Profile Name' and 'Action'. The profiles listed are: Default AD, Default OpenLDAP, Default OpenLDAP AUTH, Default AD AUTH, and company LDAP. Each profile has three action icons: a checkmark, a document, and a trash can. A copyright notice at the bottom right reads 'Copyright© 2006-2016 Comodo Dome Antispam name and logo'.

LDAP Profile Name	Action
Default AD	[Checkmark] [Document] [Trash]
Default OpenLDAP	[Checkmark] [Document] [Trash]
Default OpenLDAP AUTH	[Checkmark] [Document] [Trash]
Default AD AUTH	[Checkmark] [Document] [Trash]
company LDAP	[Checkmark] [Document] [Trash]

To add users manually

- Click the 'Local DB Users' tab
- Enter the user's email address as shown:



- Click the  button in the 'Action' column.
- You can add multiple users using the 'Bulk add' link.

Note – You can only add users for managed domains.

To integrate an LDAP server

- Click the LDAP tab
- Click the 'Add LDAP profile' link at the top

The screenshot shows the 'New LDAP Profile' configuration form. At the top right, there are links for 'Choose Language', 'English', and 'Logout'. The form contains the following fields and options:

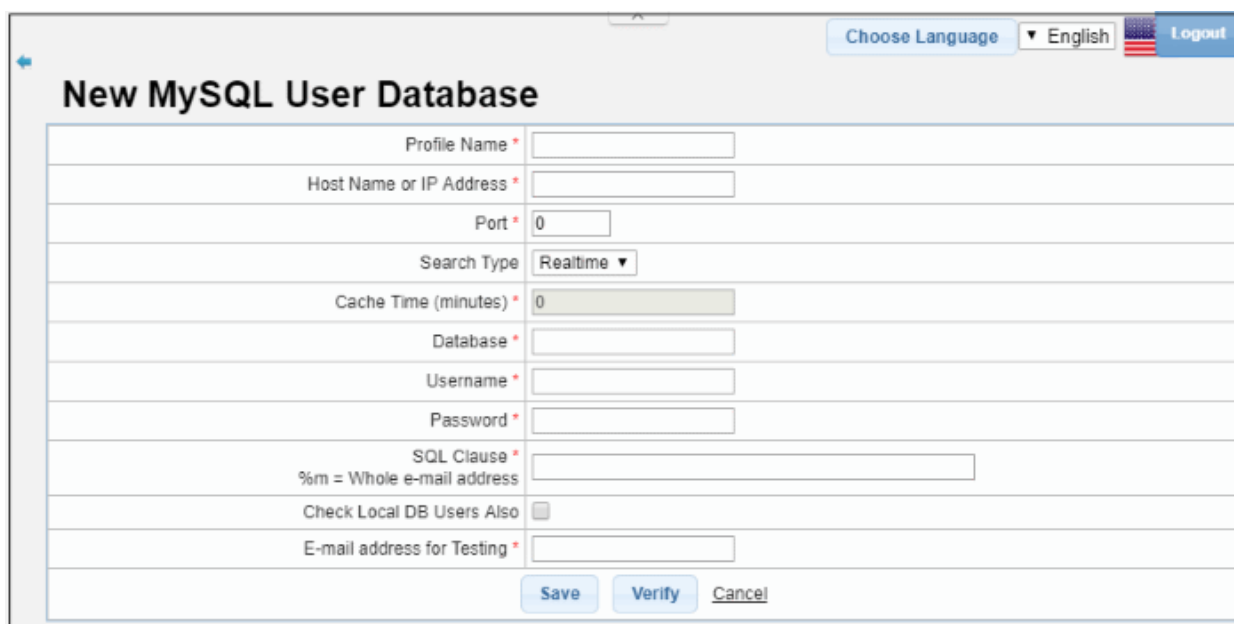
- Profile Name *
- Connection type: Plain ▼
- Host Name or IP Address *
- Port *: 389
- Host Name or IP Address (Secondary)
- Port (Secondary): 0
- Search Type: Realtime ▼
- Cache Time (minutes) *: 0
- Anonymous Access:
- Login DN *
- Password *
- Enable catch-all for this profile:
- Search Base *
- Search Pattern *
%u = "user" for "user@domain.com"
%d = "domain.com" for "user@domain.com"
%m = Whole e-mail address
- Test E-mail Address
- Email host attribute name
- Check Local DB Users Also:

At the bottom of the form are three buttons: 'Save', 'Verify', and 'Cancel'.

- Complete the profile form with the details of your LDAP server.
- Click the 'Verify' button to test the connection with the parameters you entered.
- Click the 'Save' button to apply your changes.

To add My SQL User Database

- Click the 'My SQL User Database' tab
- Click 'Add LDAP profile' link at the top



The screenshot shows a web interface for configuring a new MySQL user database. At the top right, there are links for 'Choose Language', a dropdown menu set to 'English', and a 'Logout' button. The main heading is 'New MySQL User Database'. Below this is a form with the following fields:

Profile Name *	<input type="text"/>
Host Name or IP Address *	<input type="text"/>
Port *	<input type="text" value="0"/>
Search Type	Realtime ▼
Cache Time (minutes) *	<input type="text" value="0"/>
Database *	<input type="text"/>
Username *	<input type="text"/>
Password *	<input type="password"/>
SQL Clause *	<input type="text"/>
<small>%m = Whole e-mail address</small>	
Check Local DB Users Also	<input type="checkbox"/>
E-mail address for Testing *	<input type="text"/>

At the bottom of the form are three buttons: 'Save', 'Verify', and 'Cancel'.

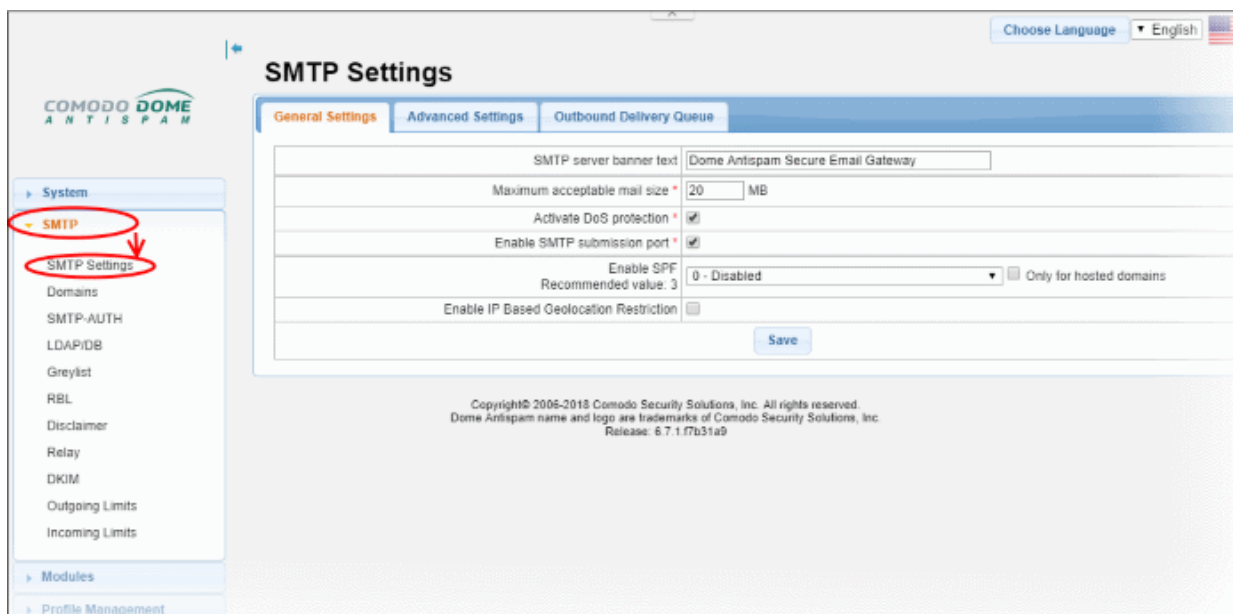
- Complete the profile form with the details of your MySQL database.
- Click the 'Verify' button to check the connection with the parameters you have specified.
- Click 'Save' to apply your changes.

See '[LDAP/Local DB/My SQL User Database](#)' if you need more help with this.

Step 5 – Configure SMTP Settings

Next, configure the SMTP settings for incoming and outgoing mails.

- Click 'SMTP' > 'SMTP Settings'



General Settings

SMTP Settings - General Settings Table of Parameters	
Parameter	Description
SMTP server banner text	The welcome message shown on the server after successfully connecting to Dome Antispam port 25
Maximum acceptable mail size (MB)	The maximum permitted size of a single email + attachments. The default value is 20 MB.
Activate DoS protection	A DoS (Denial of Service) attack occurs when a malicious actor tries to overload your mail server by bombarding it with unsolicited mail. DoS protection implements limits to help ensure your servers are not brought to a standstill by such attacks.
Enable SMTP submission port	If enabled, Dome Antispam will not accept outgoing messages from unauthenticated sources, thus helping to protect your network and users from spam emails.
Enable SPF	<p>SPF (Sender Policy Framework) is a standard designed to block the forgery of sender addresses.</p> <p>SPF values</p> <ol style="list-style-type: none"> 1. Just add received-SPF header 2. Return temporary failure in DNS query error 3. If SPF result fails (ban) then reject it (recommended) 4. If SPF result is softfail then reject it 5. If SPF result is neutral then reject it 6. If SPF result is not passed then reject it <p>You can disable SPF by selecting '0' from the list. If the check box 'Only for hosted domains' is selected, then the SPF check will be performed for outgoing mails for domains that are hosted in the network.</p>
Enable IP Based Geolocation Restriction	Sender IP based location detection. This should be enabled here in order to activate the geo location restriction settings in the incoming profiles. Mails from restricted countries list will be rejected.

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

Advanced Settings

- Click the 'Advanced Settings' tab

SMTP Settings - Advanced Settings Table of Parameters	
Parameter	Description
Minimum number of filter processors	The least filter processes that the filtering engine should use. Filter processors are threads used to scan and handle mail. <ul style="list-style-type: none"> • Fewer processors = Lower resource overhead / slower performance
Maximum number of filter processors	The most filter processes that the filtering engine should use. Filter processors are threads used to scan and handle mail. <ul style="list-style-type: none"> • More processors = Higher resource overhead / better performance
Maximum number of recipients per SMTP transaction	The highest number of mailboxes to which Dome Antispam will forward mail per transaction.
Incoming SMTP session timeout (seconds)	Timeout duration of each SMTP session.
RBL Timeout (seconds)	If this time is exceeded, the RBL query is canceled and next filter is applied to the e-mail.
Early talker drop time (seconds)	After a client makes a TCP connection, SMTP servers will wait a for short time before sending a greeting message. The client replies with a HELO or a EHLO response. If the server receives the response before sending the greeting, then the client could be serving spam. The waiting time before sending the greeting is called 'Early talker drop time'. We recommend you leave the setting at the default.
Reject invalid addresses	If enabled, incoming mails with invalid address will be rejected
Queue life time (hour)	Enter the number of hours that a mail can be queued for delivery before it is bounced.
Enable tarpitting	Tarpitting helps thwart spammers by slowing the transmission of bulk emails. Tarpits slow communication times with spam servers when they send mail to several of your recipients during one session. Spammers may stop sending emails to your server if the response to their requests is very slow.
Tarpit count	Tarpitting will become active if the number of recipients exceeds the Tarpit count.
Tarpit delay (second)	The number of seconds that Tarpitting will delay the transmission response
Maximum number of SMTP sessions	Maximum number of simultaneous SMTP sessions.
Maximum number of concurrent mail delivery	Maximum number of simultaneous outgoing messages that can be sent.

Main Filter engine log level	Select the level of main filtering engine event that should be logged. Selecting 'Debug' will log all the levels.
------------------------------	---

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

Outbound Delivery Queue

You can queue outbound mails per domain so only a certain number of mails will be delivered at once.

- Click the 'Outbound Delivery Queue' tab

SMTP Settings

General Settings | Advanced Settings | **Outbound Delivery Queue**

Queue 1

Concurrence Number: 50 [Save]

Domain	Action
<input type="text"/>	
yahoo.com	

Export Import Delete all

Queue 2

Concurrence Number: 100 [Save]

Domain	Action
<input type="text"/>	
aol.com	

Export Import Delete all

Queue 3

Concurrence Number: 150 [Save]

Domain	Action
<input type="text"/>	
att.net	

Export Import Delete all

The interface has three preset delivery queues that can be configured according to your needs. You can assign as many domains as required to a particular concurrency number. You can also change the concurrency number itself if required.

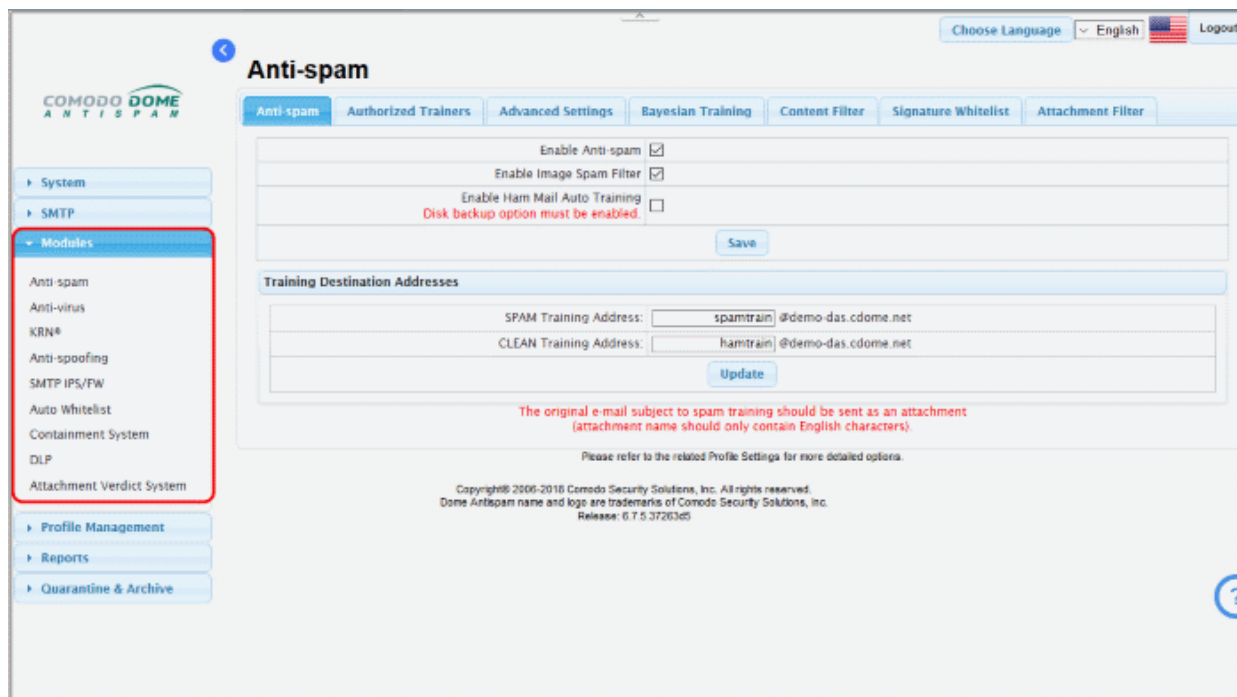
- Concurrence Number – The maximum number of emails that can be sent at once from the domain.
- To remove a domain from the list, click the button beside it.
- To remove all domains from the list, click the 'Delete all' link and confirm the removal in the 'Confirmation Dialog'.

The 'SMTP' section also allows you to configure other settings such as outgoing limits, incoming limits and more. See '[SMTP Configuration](#)' for more details.

Step 6 – Configure Dome Antispam Security Components

The 'Modules' section lets you configure Dome Antispam security components.

- Click 'Modules' on the left
- Help for each module is listed under the following screenshot:



Click the links below:

- [Anti-spam](#)
- [Anti-virus](#)
- [KRN](#)
- [Anti-spoofing](#)
- [SMTP IPS / FW](#)
- [Auto Whitelist](#)
- [Containment System](#)
- [DLP](#)
- [Attachment Verdict System](#)

Anti-spam

- **Anti-spam General Settings** - Enable/disable anti-spam and image filters. Ham mail = legitimate mail. Upload ham training materials help teach the antispam system to identify legitimate mail – useful if you are getting too many false-positives. The anti-spam module must be enabled in order to activate the anti-spam parameters specified in profile settings.
- **Authorized Trainers** - Define the sources from which spam training emails can be sent. Submitting sample spam emails allows the system to learn, adapt and protect against new spam types.

- **Advanced Settings** - The languages you select here will be analyzed for spam using the Bayesian spam classifier.
- **Bayesian Training** - The Bayesian engine analyzes emails for patterns which may indicate that the mail is spam. You can upload sample spam and HAM (legitimate) emails in order to 'train' the engine to provide more accurate verdicts.
- **Content Filter** – Add words that when detected in message body will be marked as spam
- **Signature Whitelist** – A list of digital signatures that came attached to white-listed emails. You can manually whitelist mails from the 'Mail Logs' interface.
- **Attachment Filter** – Define how many archive levels should be checked by Dome Antispam. For example, a zip file may contain another zip file inside it. A depth of '2' means Dome Antispam will check inside both files.

See '**Anti-Spam**' in the main user guide for more information.

Antivirus

Configure antivirus settings and select the program that should be used for AV scans.

- **General Settings** – Enable / disable anti-virus and select the virus scanner.
- **Advanced Settings** – Define scanner settings such as size of mails that should be scanned, file types that should be scanned and so on.

See '**AntiVirus**' for more information.

KRN

Korumail Reputation Network is a system which assigns a trust rating to IP addresses. It not only includes traditional features such as real-time IP blacklists but also has 'whitelist' and 'greylisting ignore' features.

- **Servers** - A newly added KRN server will be in enabled status by default. Click the 'Yes' or 'No' link under the 'Enabled' column to switch between enabled and disabled statuses.
- **Settings** – Enable / disable Reputation Network blacklist, whitelist and whitelist triplet scan.

See '**Reputation Network (KRN)**' if you need more help with this.

Anti-spoofing

Email spoofing is a technique used to forge email headers so that the message appears to originate from a source other than the true sender. You can configure the settings to check whether an email is being sent from an authorized server.

- Select 'Enable Anti-spoofing' check box
- Select the managed domain from the 'Choose Domain' drop-down and enter the IP addresses.

See '**Anti-Spoofing**' if you need more help with this.

SMTP IPS / FW

Configure the intrusion prevention system (IPS) and firewall (FW) to protect against denial of service (DoS) and SYN attacks.

- **General** – Enable / disable SMTP IPS/FW module and configure the security profile.
- **Whitelist** – Add trusted networks so they will not be filtered by the SMTP IPS module.
- **Blocked** – Add IP addresses so that mails from these sources never reach the SMTP level for processing.

- **Rate Control** - The 'Rate Control' feature protects your company from spammers that send huge amount of emails to the server in a small amount of time. Configure the rate control settings in order to automatically add IP addresses to blacklist if the set threshold is exceeded.

See '**Rate Control**' if you need more help with this.

Auto Whitelist

Configure this setting to automatically trust emails sent between specific senders and recipients.

- The threshold means how many emails must be exchanged before the remote sender is added to the whitelist. The threshold must be achieved within the 'Maximum Day Count' underneath this setting.

See '**Auto Whitelist**' if you need more help with this.

Containment System

- Protects users from zero-day malware by opening any untrusted attachments in a secure, virtual environment known as the container.
- Items in the container are not allowed to access other processes or user data and will write to a virtual hard-drive and registry.
- Dome Antispam checks the trust rating of all attachments. PDF and .exe attachments with a trust rating of 'Unknown' are removed and replaced with a link.
- The link allows recipients to download a special version of the file wrapped in Comodo's containment technology. The file will be open in a virtual container on the endpoint

DLP (Data Leak Prevention)

- Data loss prevention helps stops sensitive information from leaving your organization via email. You configure it by specifying keywords that should be monitored.
- If triggered, you can configure actions such as quarantine or block the mail.
- You specify the keywords themselves in the antispam profile.
- **DLP** – Enable / disable DLP, Incoming Profiles and Outgoing Profiles.

See '**Data Leak Prevention**' if you need more help with this.

Attachment Verdict System

Configure to submit email attachments (executable and pdf files) that are rated as 'Unknown' to Valkyrie, a file analysis and verdicting system.

- **General Settings** – Enable / disable attachment verdict system. Provide your Dome AS license key. The host name is by default set to Valkyrie.

See '**Attachment Verdict System**' if you need more help with this.

Step 7 – Configure Quarantine & Archive Mail Settings

Configure the number of days that logs and archived files should be retained in Dome Antispam.

- Click 'Quarantine & Archive' on the left then 'Quarantine & Archive Settings'

The screenshot shows the 'Quarantine & Archive Settings' page. The sidebar on the left has a red box around the 'Quarantine & Archive' menu item. The main content area has three tabs: 'General', 'E-mail Reports', and 'Admin E-mail Reports'. The 'General' tab is selected, showing a table of settings with input fields for values like 60, 30, 60, 5, and 10. A 'Save' button is at the bottom right of the settings table.

- Click the 'General' tab

Quarantine & Archive General Settings - Table of Parameters	
Parameter	Description
Delivery Logs Deleted Time	Delivery logs are a record of incoming and outgoing mails which were accepted by mails servers. Specify the number of days these logs should be kept.
E-mail Logs Deleted Time	Mail logs are a record of all incoming and outgoing mails handled by Dome Antispam, regardless of whether the mail was accepted. Enter the number of days for which the email logs should be retained.
Archive remove interval	The number of days that Dome Antispam should store a copy of emails.
Attachment Verdict System record remove Interval	Attachment verdicts tell Dome Antispam whether or not an attachment is safe, malicious or unknown. These verdicts are awarded by Valkyrie after it has analyzed the files behavior. Enter the number of days the verdicts should be retained by Dome AS. This is for the purposes of to view log history and the analysis result. Dome Antispam asks Valkyrie verdict for each attachment regardless of prior requests.
Quarantine remove interval	Enter the number of days after which the 'Quarantined Logs' will be removed. The maximum period that can be set is 30 days.
Duration of storage of original mail and attachments on server	This setting pertains to Containment. Specify the number of days that emails including attachments should be retained on Dome AS server. The period should be between 1 and 360 days. Original emails and contained attachments are deleted after this period.

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

You can also configure the email reports settings for users to access their quarantined emails and admin email reports settings for sending reports to administrators. See '[Quarantine & Archive](#)' for more details.

Step 8 – System Configuration

After completing the initial steps explained above, you can check and configure other system settings such as GUI customization and more.

- Click 'System' on the left, then the sub-menu that you want to configure

The screenshot displays the 'Services' management page in the Comodo Dome Antispam console. On the left, a sidebar menu is visible with 'System' highlighted in red. The main content area shows a table of services with their current status and start/stop controls.

Service	Status	Start / Stop
Delivery Agent	Running (Green icon)	Stop (Red hexagon)
SMTP Service	Running (Green icon)	Stop (Red hexagon)
SMTP Submission Service	Running (Green icon)	Stop (Red hexagon)
Main Filtering Engine	Running (Green icon)	Stop (Red hexagon)
Anti-spam Engine	Running (Green icon)	Stop (Red hexagon)
Syslogd	Running (Green icon)	Stop (Red hexagon)
Snmpd Service	Running (Green icon)	Stop (Red hexagon)
Scheduler Service	Running (Green icon)	Stop (Red hexagon)

- **Services** - Start or stop various services such as delivery agent, SMTP, Snmpd, scheduler and more.
- **License** – View current license, create license requests and / or install a new license.
- **Settings** – Configure important Dome Antispam settings:
 - **General** - Enable or disable automatic upload of selected spam messages to Comodo for analysis.
 - **Cache** – Configure cache expire time for Greylist IP addresses, SMTP Auth logs and LDAP.
 - **Session** - Configure the session timeout period and the maximum number of concurrent login count to the account.
 - **GUI Customization** - Customize the look and feel of the console. You can also change the name and the logo which is displayed in the interface.
 - **Backup** – Store copies of system configuration settings and logs. You can restore your Antispam configuration from your backup at any time.
 - **Restore** - Reverts your Dome Antispam configuration and logs to a previous system state.
 - **Log Upload** – Automate the process of uploading various types of Dome Antispam logs.
 - **Postmaster** – Forward mails directed to postmaster@ to another address.
 - **SMTP TLS** – Configure to encrypt messages transmitted between Mail Transfer Agents (MTAs).
 - **Database Update** – Allows you to update virus and spam database manually.
 - **Syslog** – Forward logs to a remote server.
- **Logs** - Download logs and delete unwanted logs.
- **Tools** - Check the connectivity to the mail servers and clients. Clear the mails in the SMTP delivery queue.
- **Statistics** - View SMTP connection statistics, mail statistics and utilization statistics of hardware and software resources like network, CPU, hard disks and system memory as graphs.

See **System Configurations** for more details.

See the admin guide at <https://help.comodo.com/topic-443-1-898-11454-Mail-Logs-Report.html> for information about all the features and settings.

Dashboard – View statistics about your mail traffic and overall system details. You can also view important system messages and update the license. See <https://help.comodo.com/topic-443-1-898-11364-The-Dashboard.html> for more information.

System – Configure antispam services, upgrade license and more. See <https://help.comodo.com/topic-443-1-898-11366-System-Configurations.html> for details.

SMTP – Configure settings for incoming and outgoing mails, manage domains and more. See <https://help.comodo.com/topic-443-1-898-11367-SMTP-Configuration.html> for more information.

Modules – In this section, you can configure the core security components of Dome Antispam email defense system. See <https://help.comodo.com/topic-443-1-898-11368-Modules.html> for more details.

Profile Management – Create rules and settings that can be applied to specific domains, e-mail addresses, incoming mails and outgoing mails. See <https://help.comodo.com/topic-443-1-898-11369-Profile-Management.html> for more information.

Reports – Configure report settings and generate reports for mail logs, SMTP queue and more. See <https://help.comodo.com/topic-443-1-898-11370-Reports.html> for more details.

Quarantine & Archive – In this section, you can configure the number of days that logs and archived files should be retained. Also view the details of 'Quarantine Logs' and 'Archived Mails'. See <https://help.comodo.com/topic-443-1-898-11371-Quarantine-&-Archive.html> for more information.

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