COMODO
Creating Trust Online®

Comodo AntiSpam

Software Version 2.7

User Guide

Guide Version 2.7.092611

Comodo Security Solutions,
525 Washington Blvd.,
Jersey City, NJ 07310

Table of Contents

1.Comodo AntiSpam - Introduction **3**
2.Passcode Authentication Technology **4**
3.Installing Comodo AntiSpam **4**
3.1.Initializing and Activating Comodo AntiSpam 8
3.2.The AntiSpam Icon 12
4.A Quick Tour of Comodo AntiSpam **13**
4.1.The Main Configuration Screen 13
4.2.The Quarantine Database 14
4.3.The Authentication Database 16
4.4.Configured Email Accounts 20
4.5.Server Synchronization 21
5.Policy **22**
6.Using the Quarantine Database **24**
6.1.Setting the QDB Hold -Time 24
6.2.Using the QDB Reminder 25
6.3.Allowing/Blocking Senders & Domains From the QDB 25
6.4.Manually Deleting Spam from the QDB 26
6.5.Reporting Messages as Spam 27
7.Using the Authentication Database **27**
7.1.Adding/Removing Allowed or Blocked Addresses to the ADB 29
7.2.Importing Your Address Book to the ADB 30
7.3.Exporting Addresses from the ADB 31
8.Managing Email Accounts **32**
8.1.Email Account Settings 33
9.Advanced Settings **34**
9.1.Server Synchronization 35
9.2.Passcode Authentication 37
9.3.Miscellaneous 38
About Comodo **41**

1.Comodo AntiSpam - Introduction

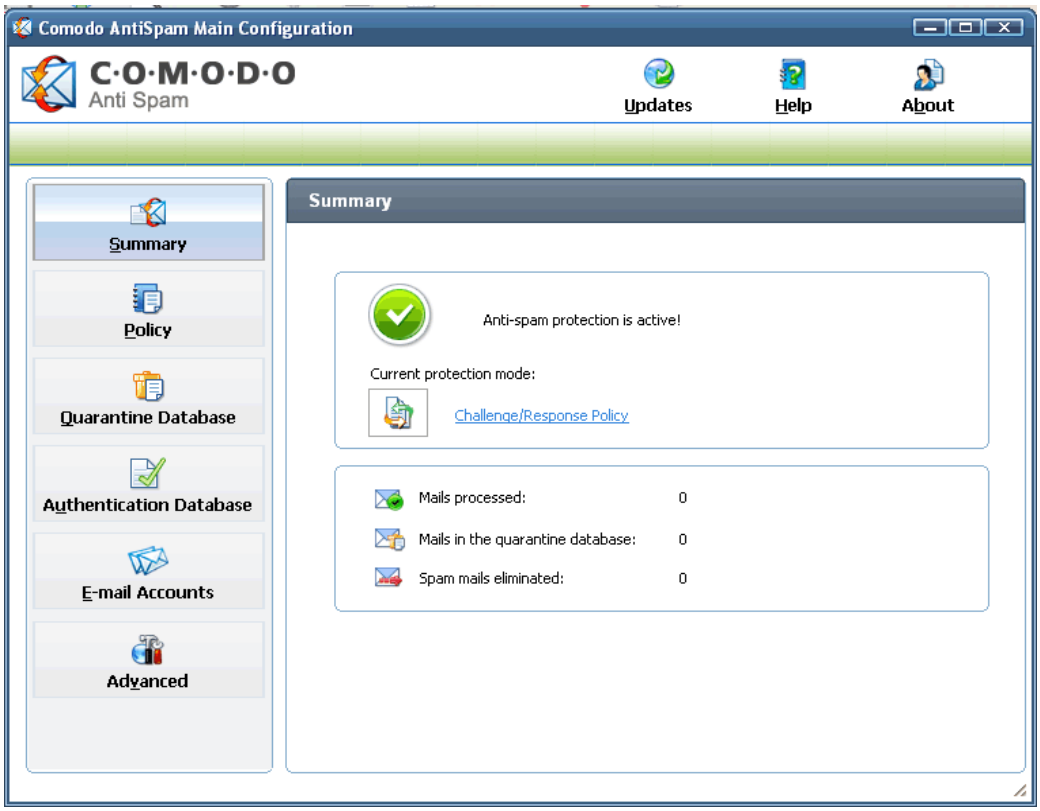
We are all too familiar with the world-wide plague of spam. Spam messages are commonly sent by advertisers trying to sell their products and services. But majority of the messages are unsolicited, annoying and build up junk in the email box. Spam messages are also used by criminals for committing various sorts of fraud, spreading viruses, luring people for illegal activities, identity theft, phishing etc.

Spammers come up with clever ways to beat the run-of-the-mill passive spam filters, which scan the content of incoming email messages to determine whether they are spam or not. Spammers use cryptic characters in the subject and body of spam emails for camouflage, making them to appear genuine.

Comodo AntiSpam is different. It doesn't look at the content of the email to determine whether it is spam or not. Rather, this patent-pending product authenticates the SENDER of each incoming email message, providing the most powerful measure of AntiSpam protection available.

During installation, your email address book is imported by Comodo AntiSpam to form a foundation of **allowed** senders. If an email arrives from an unknown sender, Comodo AntiSpam automatically sends a **challenge** message to that sender asking them to reply with your AntiSpam Passcode. The AntiSpam Passcode is sent along with the **challenge** message in a graphical form, text form or even the sender is asked to enter the passcode agreed mutually between the two parties (sender and you) beforehand, as specified by the you. When the reply message is received and the passcode is found to be correct, that sender's original email and all subsequent email from that sender are passed to your inbox.

Comodo AntiSpam supports Outlook, Outlook Express, Eudora, Netscape Messenger, Opera or any email application accessing POP3 email accounts.



Comodo AntiSpam provides the following features:

- Spam Elimination using Passcode Authentication Technology, which is an active filtering algorithm that authenticates the SENDER of each incoming email message, eliminating spam once and for all!
- **Plug and Play operation:** Simply install AntiSpam and then begin enjoying spam free email.
- AntiSpam operates in the background, so you don't have to change a thing about how you access your email.
- **Authentication Database (ADB):** The Authentication Database stores email address of your friends and foes (spammers being the foes). **Click here for more details.**
- **Quarantine Database (QDB):** The Quarantine Database allows you to view the messages, which are pending authentication. You can authorize or block emails directly from the Quarantine Database. **Click here for more details.**

- **Supported Email Accounts:** POP/SMTP. The next release will include IMAP, Exchange and AOL.
- **Supported Email Programs:** Outlook Express, Outlook, Eudora, Netscape Messenger and any other POP/SMTP enabled email program.
- **Address Import facility:** Import your address book into the Authorization Database.
- Spam Reporting Mechanism built into the **Passcode Authentication Technology.**
- **Server Synchronization:** Access you email from any computer with AntiSpam installed and you never lose the current state of your Passcode Authentication.
- Support for distribution lists.
- Support for automated e-commerce receipt messages.

2.Passcode Authentication Technology

Comodo AntiSpam uses an **AntiSpam Passcode** to authenticate people sending you email. Requests to check mail generated by the email client are intercepted by Comodo AntiSpam, running on your computer. AntiSpam then retrieves mail from the server and authenticates the sender of each message. If the sender of a particular message is allowed, it is immediately passed to your inbox. If the sender of a particular message is blocked the email message is either immediately deleted or is stored in the Quarantine Database for a prescribed period of time, whichever you choose. If the sender of a particular message is unknown, the email message is temporarily stored in the Quarantine Database and a special AntiSpam Alert message is automatically sent back to the sender of that message. The AntiSpam Alert message asks the sender reply, typing your AntiSpam Passcode in the reply. The AntiSpam Passcode is sent along with the AntiSpam Alert in the form of a graphical attachment. The idea behind sending the AntiSpam Passcode as a graphical attachment is to require a human to read the passcode and then type it in the reply. When the AntiSpam Alert reply is received by AntiSpam and the passcode is found to be correct, the original email message is immediately passed to your inbox and an entry is made into an Authentication Database (ADB) allowing all subsequent email from that particular sender. If the AntiSpam Alert reply is found to contain an incorrect passcode, the process is repeated for a configurable number of authentication attempts.

3.Installing Comodo AntiSpam

Before installing Comodo AntiSpam, save all of your work and close any open applications.

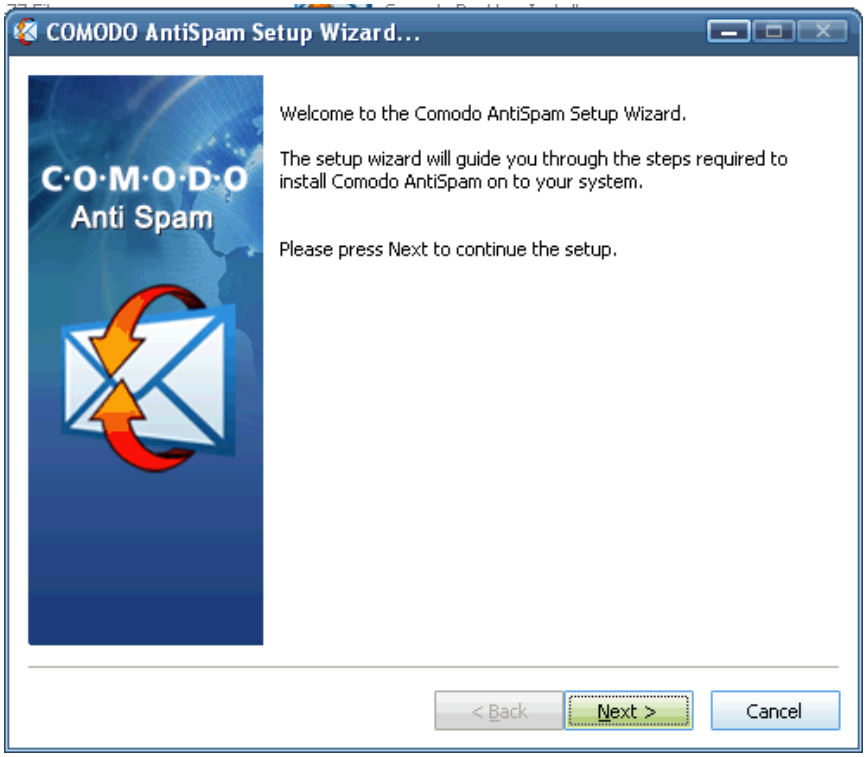
Before you install Comodo AntiSpam, read the installation instructions carefully and also review the system requirements listed in this chapter.

Installation Process

To install, download the Comodo AntiSpam setup files to your local hard drive (setup.exe can be downloaded from **http://www.comodoantispam.com/**).
Next, double click on the setup file to start the installation wizard and follow the process as below.

STEP 1: Welcome Dialog box

The set up program starts automatically and the Welcome wizard is displayed. At this time, you may cancel the install process or continue with the Comodo AntiSpam Setup program. Click 'Next' to continue.



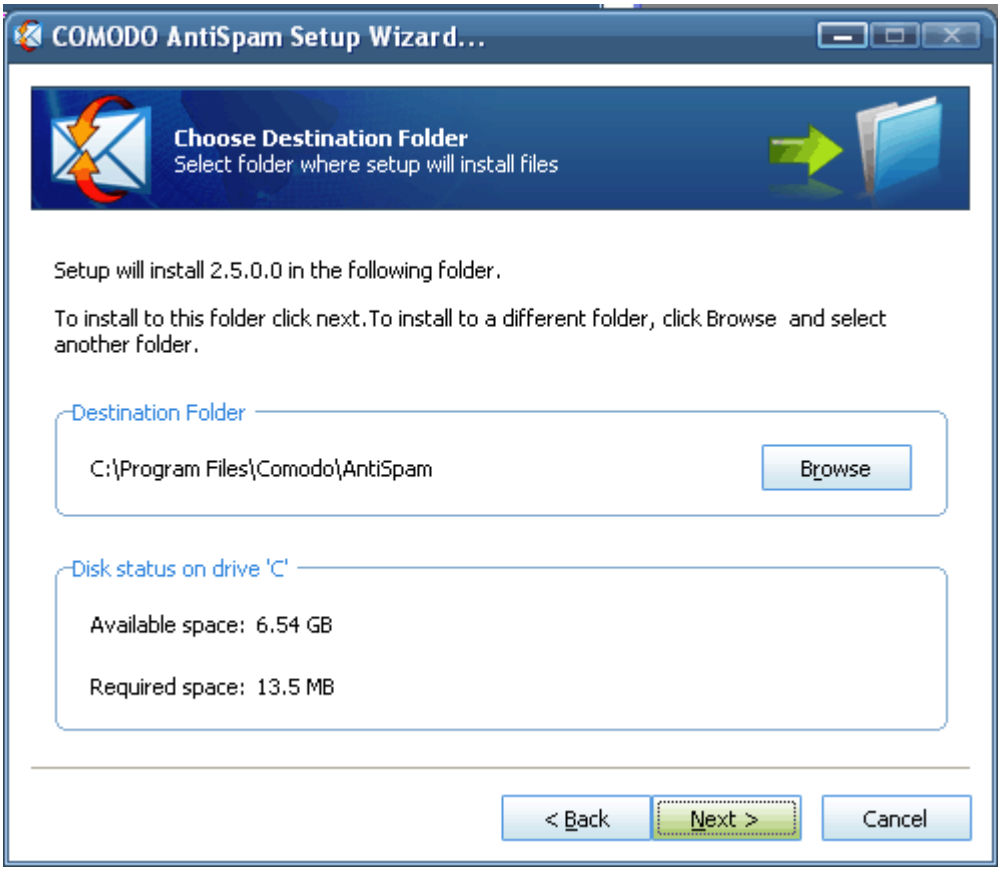
STEP 2: License Agreement

When Comodo AntiSpam is installed for the first time, you must complete the initialization phase by reading and accepting the license agreement. After you read the End-User License Agreement, click 'Yes' to continue installation. If you decline, you cannot continue with the installation.

STEP 3: Location Destination Folder

On the Destination Wizard page, confirm the location of the AntiSpam installation files. To install the program in the default destination location, click 'Next'. The default destination directory is the

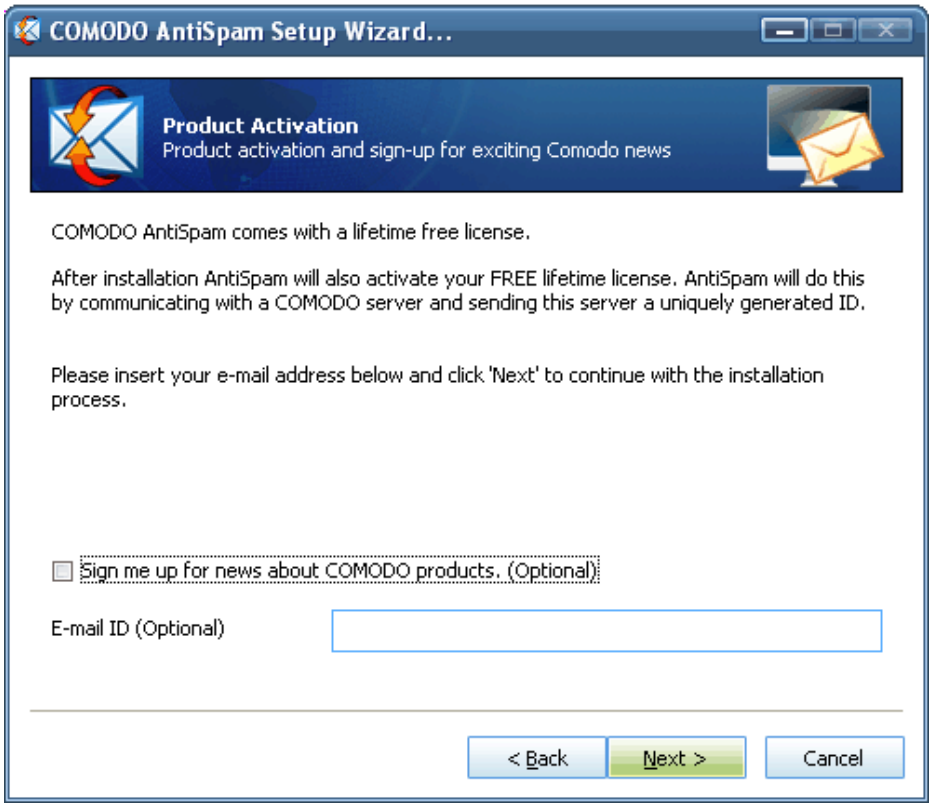
C:\Program Files\Comodo\AntiSpam.



If you do not wish to install the AntiSpam files in the default location, to install to a different folder, click BROWSE and select another folder. Click 'OK' to continue with the installation process.

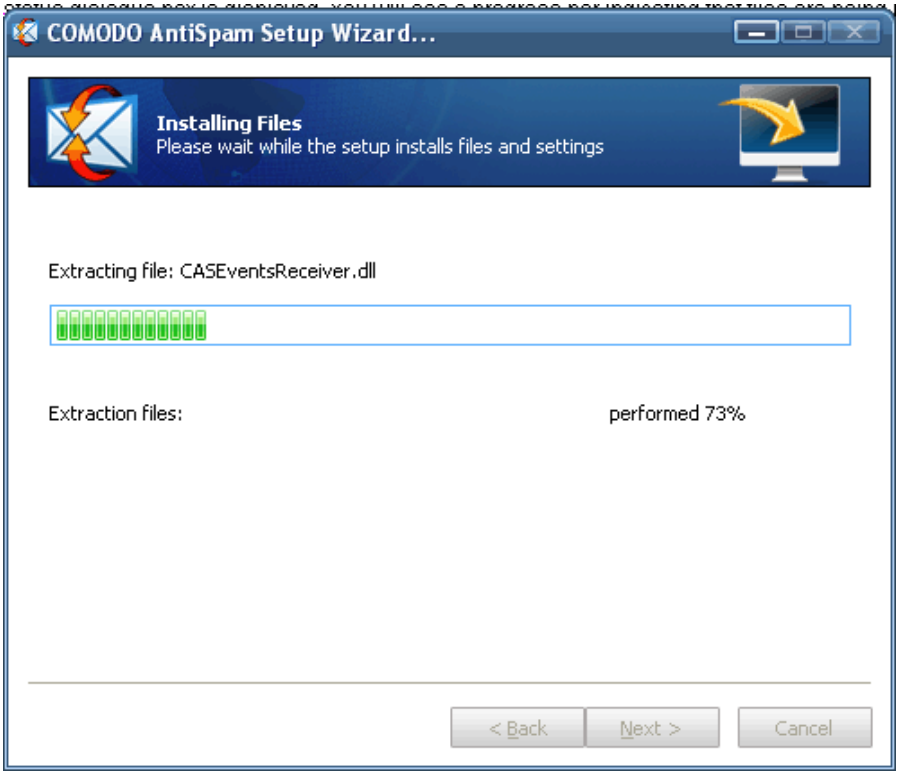
STEP 4: License Activation

If you would like to receive news about Comodo products, product updates and special offers, then enter your email address at the following screen - check the box stating 'Sign me up for news about COMODO products'. If not, simply click 'Next'.



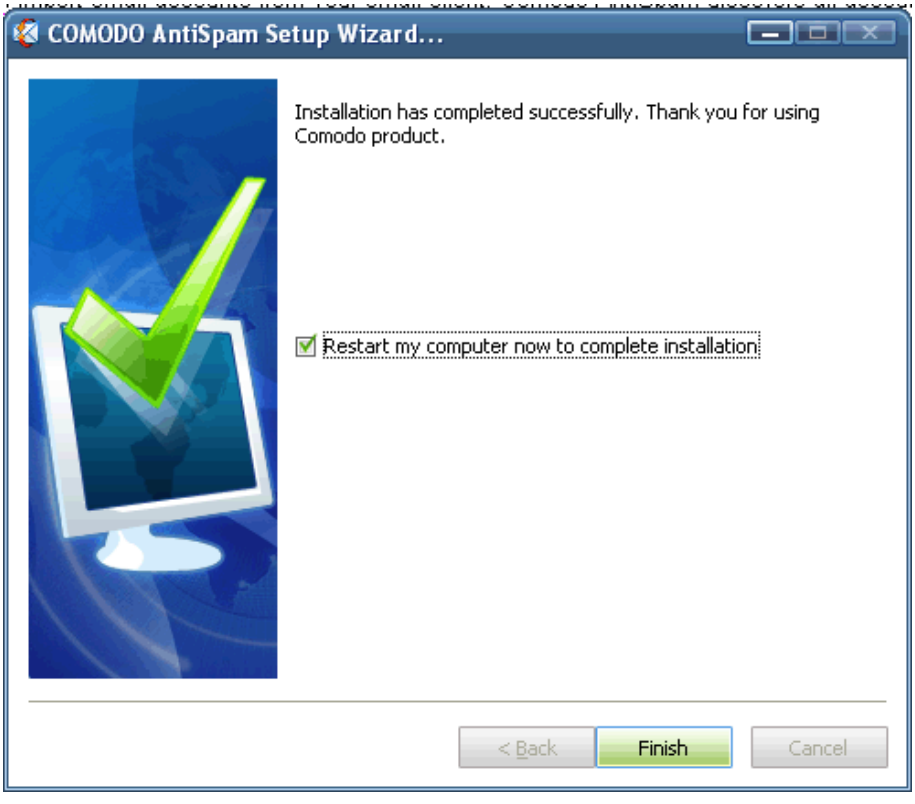
STEP 5: Set Up Status Box

A setup status dialog box is displayed. You will see a progress bar indicating that files are being installed.



STEP 6: Restart your system

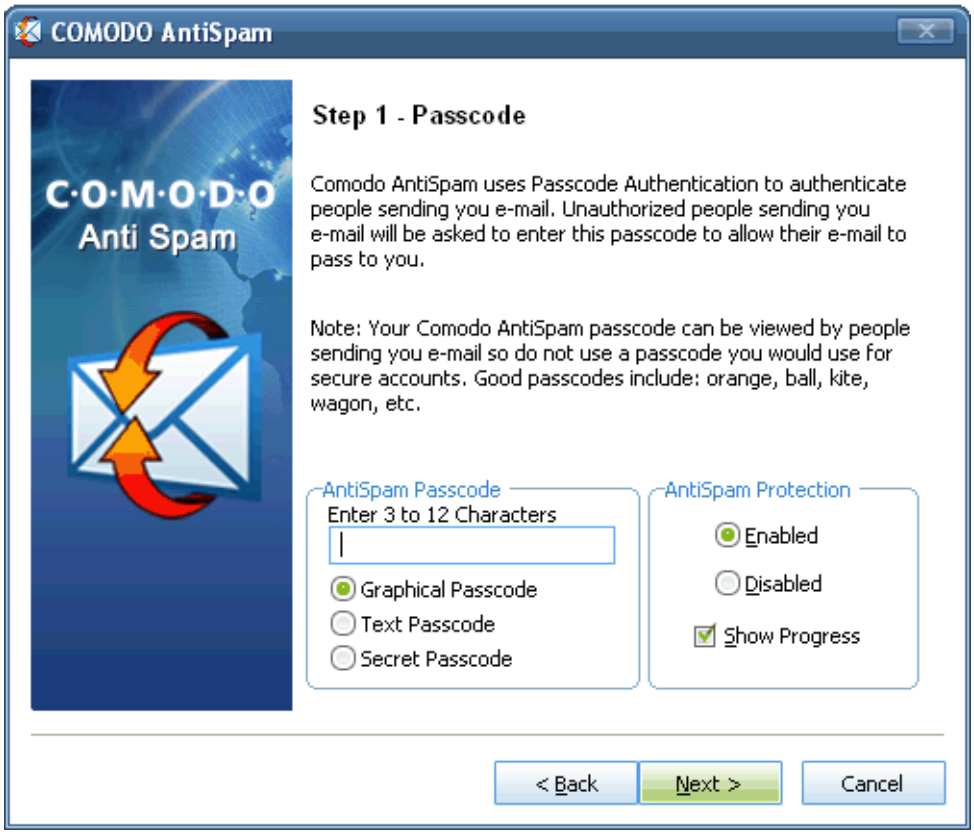
Your system must be restarted in order to finalize the installation. Please save any unsaved data and Click 'Finish' to reboot. Uncheck the 'Restart Now' option If you would rather reboot at a later time.



3.1. Initializing and Activating Comodo AntiSpam

The first time your computer boots up with Comodo AntiSpam installed, you will be prompted to configure Comodo AntiSpam.

Step 1 : Selecting Your AntiSpam Passcode



The first initialization screen is where you enter your AntiSpam Passcode. Your Passcode is visible to unauthorized senders. Therefore, you should not use a Passcode or password that you also use for any secure account access (bank, website passwords, etc). Examples of good AntiSpam Passcodes include: BLUE, orange, poodle, LIGHT,… Your AntiSpam Passcode is not case-sensitive.

Note: Please ensure that the **AntiSpam Passcode** which you enter in the **Configuration** screen does NOT match with the following keywords: Comodo, AntiSpam, Computer, Passcode, Email, Spam, Spammer, Alert, Authentication, Technology and Junk and should NOT be your name or email address.

After entering your passcode, select the manner in which your passcode has to be sent to the unknown sender for authentication. See **Passcode Authentication Technology** for more details.

If you select:

Graphical Passcode - The image of the passcode is sent. This means that the sender has to identify the characters from the image and type the passcode in order to respond to the challenge/response mail.

Text Passcode - The passcode is sent in a text format. The sender can simply click reply, as the passcode will already be in the mail, or can copy it from the mail in order to respond to the challenge/response mail.

Secret Passcode - The passcode is not sent with the challenge response mail. The sender has to type the passcode that he/she has acquired from the recipient beforehand by some other method of communication in order to respond to the challenge/response mail.

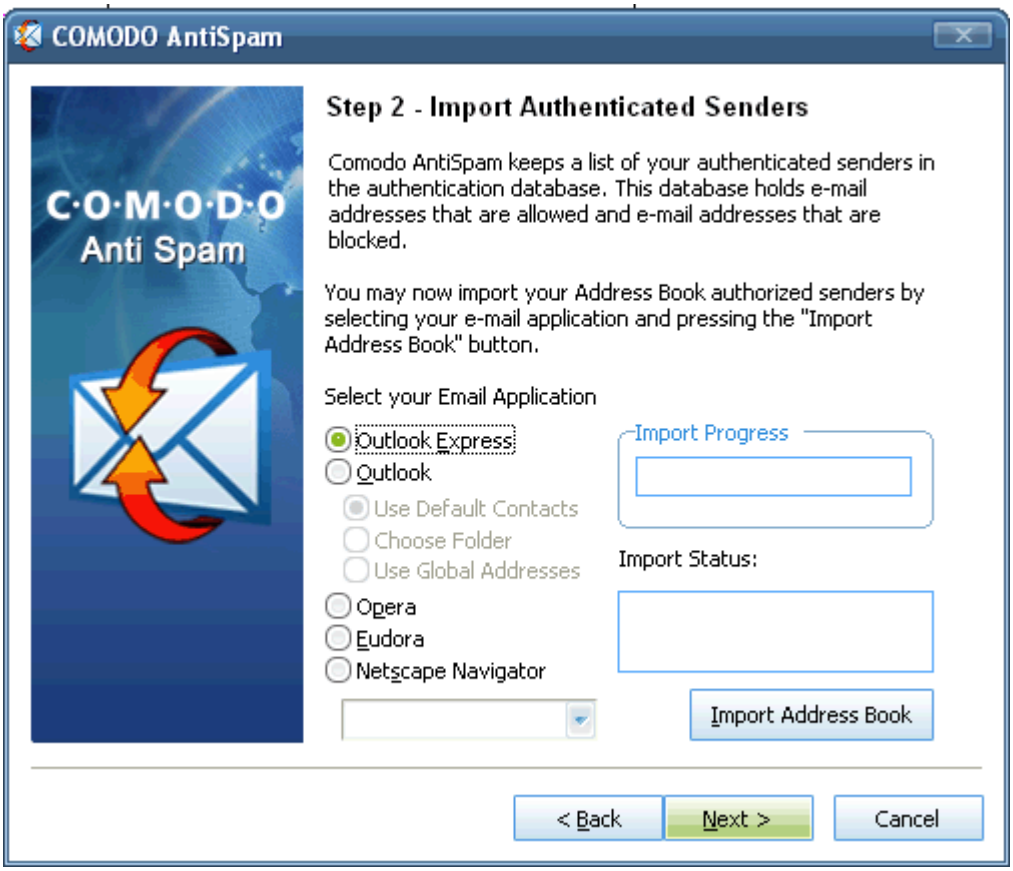
AntiSpam Protection

You can also Enable/Disable AntiSpam protection by selecting **Enabled** or **Disabled** in this interface.

Selecting **Show Progress** in this interface instructs the application to show the progress of different processes like importing address databases etc.

Step 2 : Importing Your Address Book

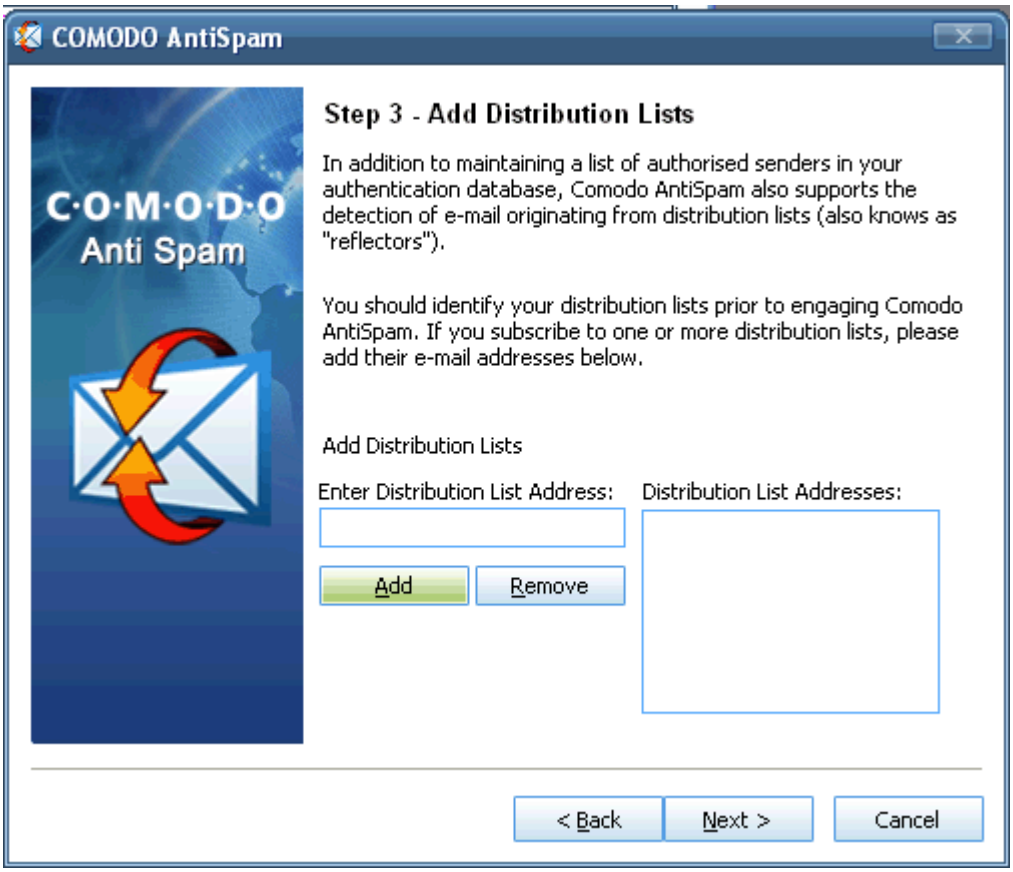
The second initialization screen is where you import your email address book. Simply select the email application you are using and press the 'Import Address Book' button. All addresses in your email address book will be imported to the Authentication Database and are designated as **Allow Email From**.



Step 3 : Adding Distribution Lists

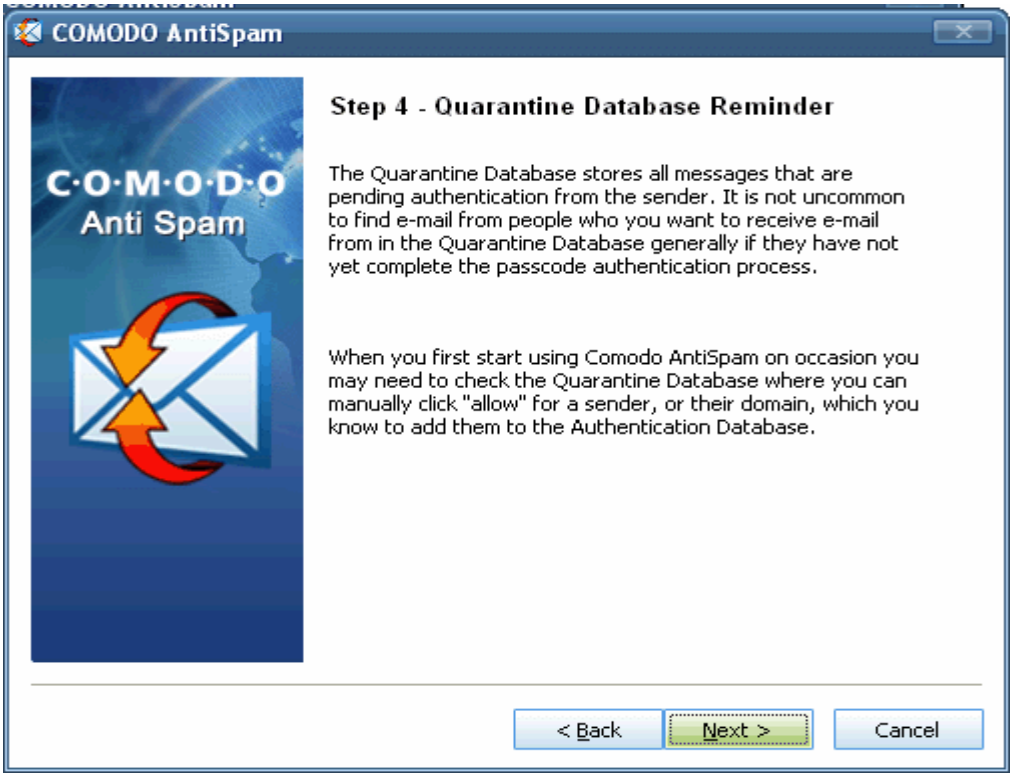
The third and final initialization screen is where you add distribution lists to the Authentication Database. If you subscribe to any email

distribution lists (also known as reflectors), it is important to enter them here. This in effect authorizes all of the subscribers to a distribution list to send you email when posting messages to the distribution list. Whenever you subscribe to a distribution list, you should add the distribution list to the Authentication Database. See **The Authentication Database** for details on how to add addresses directly to the Authentication Database.



Step 4 : Quarantine Database Reminder

Read the reminder carefully and click on 'Next' button.



Step 5 : Import Email Accounts

You can import email accounts from your email client. Comodo AntiSpam discovers all accounts of the client and provides you with possibility to import them (or some of them) into Comodo AntiSpam database.

Select the account(s) by checking the box alongside it's name and click on 'Next' button.

Configuration Complete

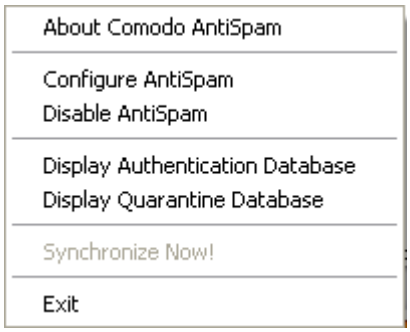
A configuration complete dialog box is displayed. Click 'Finish'.

3.2. The AntiSpam Icon

Once installed, the AntiSpam icon will appear in the system tray at the lower right-hand corner of your Windows display. This is your primary interface for configuring and managing AntiSpam. Right clicking on the icon will bring up several selections. Those are:

- **About Comodo AntiSpam**
- **Configure AntiSpam**
- **Enable/Disable AntiSpam**
- **Display Authentication Database**
- **Display Quarantine Database**
- **Synchronize Now!**
- **Exit**

The desired option is selected by left clicking on it.



Selecting **Comodo AntiSpam** engages the **About** information screen. This screen displays version and registration information for your copy

of From this screen, you can also purchase the fully licensed product.

Selecting **Configure AntiSpam** brings up the **Main Configuration** screen that allows you to simply and completely configure AntiSpam. Once configured, AntiSpam is always there and no further action is required on your part. Each time your computer is shut down and restarted, AntiSpam returns to the same state it had prior to shutdown, providing you with continuous, transparent protection against spam. With AntiSpam installed and configured, your email client operates the same way it always has, but AntiSpam is behind the scenes protecting you from all undesirable senders.

Selecting **Disable AntiSpam** disables AntiSpam and allows all email to pass directly to your email program. This includes all quarantined messages. Clicking this selection again re-enables AntiSpam. This selection is a toggle operation between the enabled and disabled states. Once disabled, AntiSpam will stay disabled until re-enabled.

Selecting **Display Authentication Database** brings up the **Authentication Database** screen.

Selecting **Display Quarantine Database** brings up the **Quarantine Database** screen.

Selecting **Synchronize Now!** causes your AntiSpam configuration information to be sent to your email server, where it is stored as an email message. This message, when downloaded by another computer having AntiSpam installed, allows transparent spam-protected access to your email and its AntiSpam configuration. This synchronization message on the server also provides backup of your AntiSpam configuration data. If your computer crashes and you have to reinstall the AntiSpam software, the AntiSpam synchronization information will automatically update AntiSpam when you retrieve your email.

Selecting **Exit** closes the AntiSpam configuration program (closes the AntiSpam icon) but does not turn off AntiSpam Protection. To turn off AntiSpam Protection, select **Disable AntiSpam** from the main configuration screen or the AntiSpam Icon.

If you have exited the AntiSpam system tray icon, to re-open the **Main Configuration** screen again, you must open **AntiSpam Configuration** from the programs group **(Start, Programs, Comodo, Comodo AntiSpam, AntiSpam Configuration)**. This will also return the AntiSpam system tray icon to the lower right-hand corner of your Windows screen.

4. A Quick Tour of Comodo AntiSpam

When you open Comodo AntiSpam either by the clicking the icon in the Comodo AntiSpam program group or double-clicking the AntiSpam icon  running in the system tray, the **Main Configuration** screen appears.

See also:

- **The Main Configuration Screen**
- **The Quarantine Database**
- **The Authentication Database**
- **Configured Email Accounts**
- **Server Synchronization**

4.1. The Main Configuration Screen

During installation a shortcut is added to your **startup** group, which engages the C**omodo AntiSpam Main Configuration** screen. You can open the Main Configuration screen either by clicking on AntiSpam Configuration within the Comodo AntiSpam program group, or right clicking the AntiSpam icon in the system tray (lower right hand side of your screen) and selecting **Configure AntiSpam**. The **Main Configuration** screen contains the primary AntiSpam controls.

Persistent Navigation

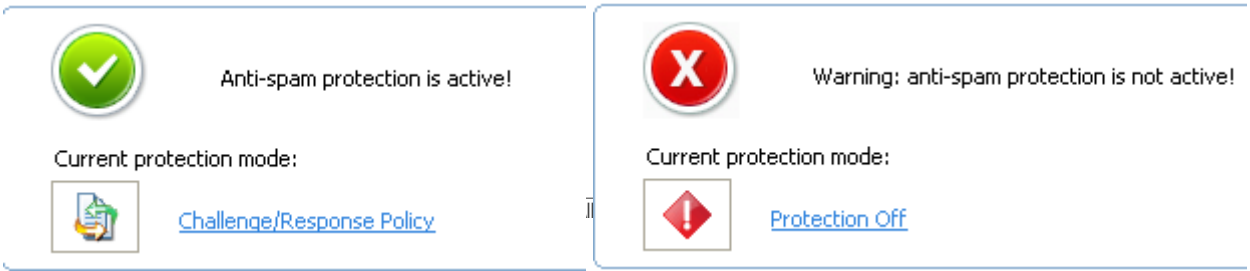
Comodo AntiSpam is divided into areas indicated by the icons at the top right hand corner and at the left side of the interface. These areas provides total control over configuration of the application. These icons are ever-present and can be accessed at all times.

- **Summary** - contains at-a-glance details of important Comodo AntiSpam settings, activity and other information. See the **'Summary'** section (below) for more details on this area.
- **Policy** - clicking this icon will take you to the protection mode configuration dialog.
- **Quarantine Database** - clicking this icon will take you to the 'Quarantine Database' configuration section. The Quarantine Database (QDB) holds all emails pending authentication.
- **Authentication Database** - clicking this icon will take you to the 'Authentication Database' configuration section. The Authentication Database (ADB) holds a list of email addresses which, have either an Allowed or Blocked designation.
- **Email Accounts** - clicking this icon will take you to the email accounts management's interface.
- **Advanced** - clicking this icon will take you to the 'Advanced Settings' section. This enables you to make settings on Passcode authentication, Server synchronization and miscellaneous settings.
- **Updates** - launches the Comodo AntiSpam updater. The updater checks for and downloads latest updates on Comodo AntiSpam from Comodo website.
- **Help** - clicking this icon will open this help guide. Each area has its own dedicated page containing detailed descriptions of the application's functionality.
- **About** - clicking this icon allows to view the 'About' information dialog. From here you can view information about the Version Number of Comodo AntiSpam that is installed on your computer.

Summary

By default, the management interface displays the 'Summary' area information. You can access this area at any time by selecting the 'Summary' tab as shown above.

Current Protection Mode - shows Comodo AntiSpam activity (Protection Enabled/ Protection Disabled).

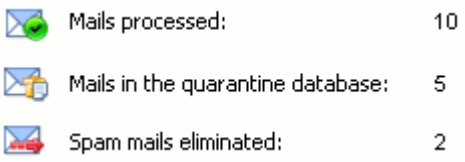


Clicking on **Challenge/Response Policy** or **Protection Off** links opens Policy configuration screen. **Click here for more details.**

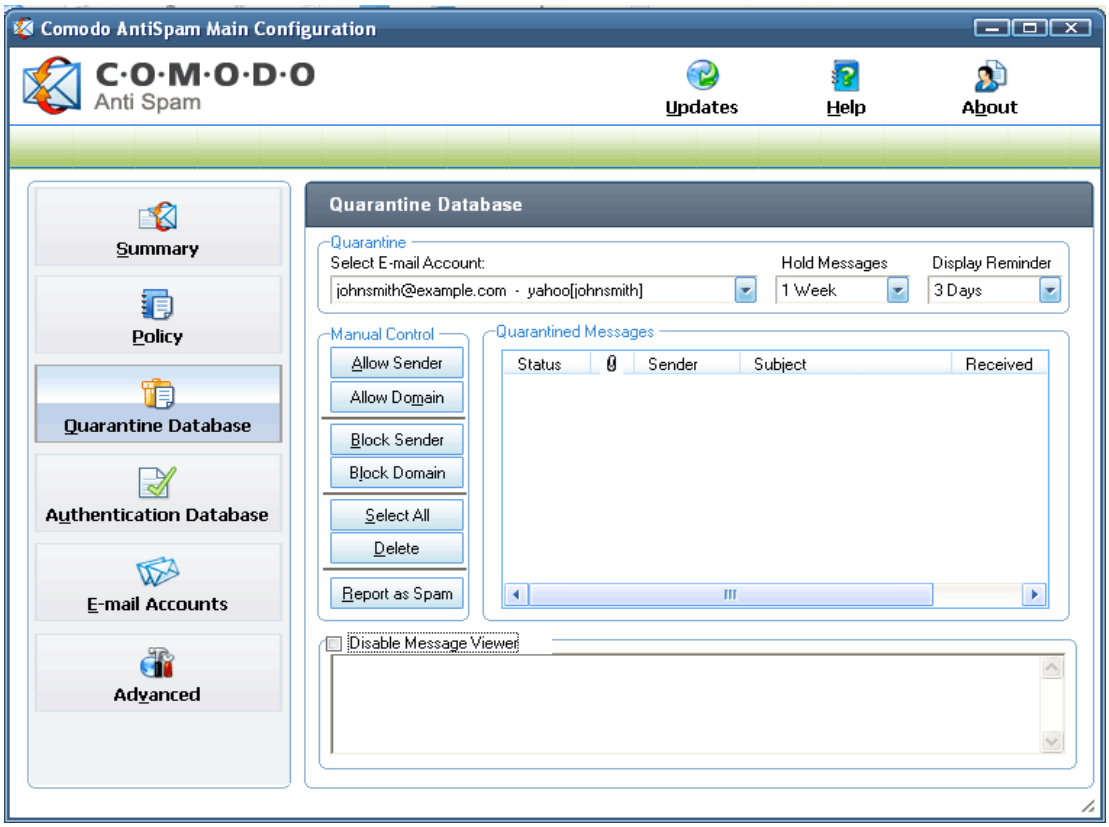
Mails processed: Shows the number of mails processed so far, from the activation.

Mails in the quarantine database: Shows the number of mails moved to quarantine database. **Click here for more details**.

Spam mails eliminated: Shows the number of mails that are eliminated by Comodo AntiSpam as they not from authenticated senders.



4.2. The Quarantine Database



Comodo AntiSpam uses the **Quarantine Database** (QDB), to hold all emails pending authentication. When you retrieve your email using your email client application (e.g. Outlook Express or Outlook), AntiSpam checks the senders email address against all email addresses in the ADB. If a match is not found, the email message is temporarily stored in the QDB and a AntiSpam Alert message is automatically sent to the sender of the unauthorized email message requesting a response containing your AntiSpam passcode. Comodo AntiSpam provides a Quarantine Database viewer where you can manually **Allow** or **Block** the senders of any or all of the email messages held in the Quarantine Database. Click on Quarantine Database to view QDB viewer.

Select Email Account: Comodo AntiSpam maintains a Quarantine Database for each of your email accounts. Use this control to select the email account for which you want view QDB.

Hold Messages: This setting can be used to specify the period of time (hold-time) for which an email is to be held quarantined from the date of receipt. On lapse of this time, the email message is deleted permanently. **Click here for more details.**

Display Reminder: Comodo AntiSpam provides a reminder to check the Quarantine Database. This setting can be used to specify the time interval between reminders. **Click here for more details.**

Quarantined Messages: The list of email messages maintained in the quarantine database is displayed here. You can individually select each mail or select all the mails to perform manual controls like 'Allow Sender', 'Block sender' and so on from this list. A preview of the selected mail is displayed in the box below. You can disable preview by selecting the check box - Disable Message Viewer.

Manual Control: The buttons in this area allows you manually specify the action to be performed on the selected mail in the Quarantined Messages list. Click:

Allow Sender - To allow all the messages from the sender of the selected message in future.

Allow Domain -To allow all the messages from the host domain of the selected message in future.

Block Sender - To block all the messages from the sender of the selected message in future.

Block Domain - To block all the messages from the host domain of the selected message in future.

Refer **Allowing/Blocking Senders and Domains from the QDB** for more details.

Select All - To select all the displayed messages for a manual control.

Delete - To delete the selected message permanently. Refer **Manually Deleting Spam from the QDB** for more details.

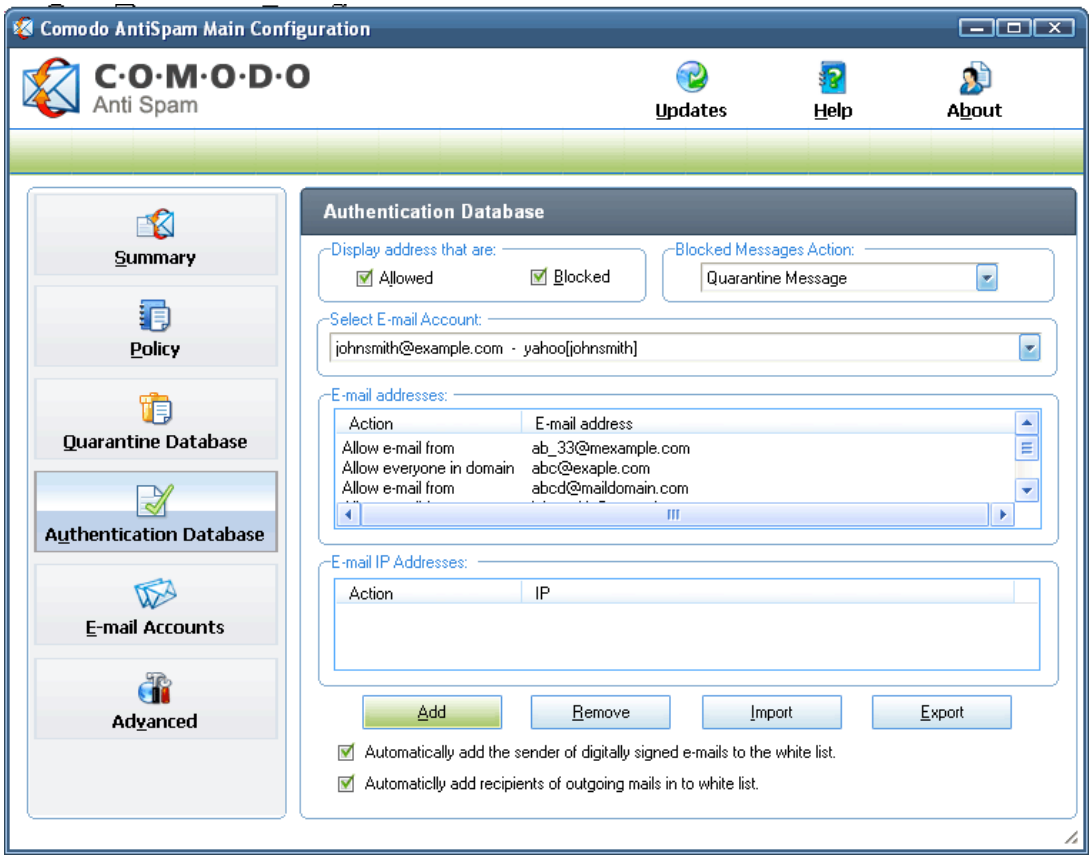
Report as Spam - To report that the selected message is a spam, to the Comodo. Refer Reporting Messages as Spam for more details.

4.3. The Authentication Database

Comodo AntiSpam uses the **Authentication Database** (ADB) to hold a list of email addresses which, have either an **Allowed** or **Blocked** designation. When you retrieve your email using your email client application (e.g. Outlook Express or Outlook), the sender of each message is checked against all email addresses in the ADB. If a match is found and it is designated **Allowed**, the email is immediately allowed to pass to your email application client. If a match is found and it is designated **Blocked**, the email either immediately deleted or is stored in the Quarantine Database for a prescribed period of time, whichever you choose. AntiSpam provides an ADB viewer where you can view, add, remove, import and export additional addresses. Click on Authentication Database to view ADB viewer.

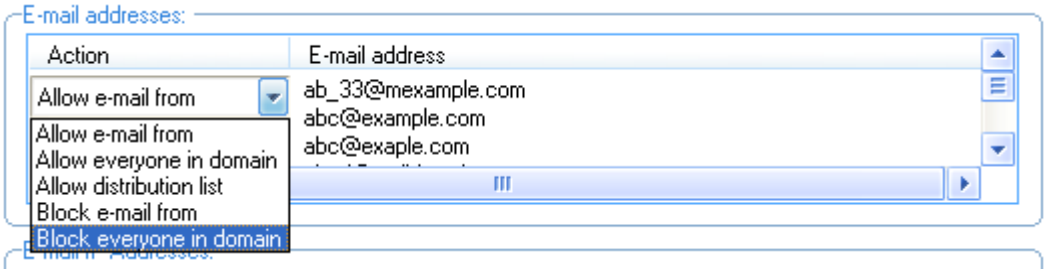
Display Addresses that are: This control allows you to specify only the selected (allowed, blocked, white list, or black list) entries for display. Anyone or both the check boxes can be selected. This feature is very useful when you are looking for a specific ADB entry. The allowed and blocked addresses are displayed as lists in the **Email addresses** and **Email IP addresses** boxes.

Blocked Messages Action: This control can be used to specify the action to be taken against the messages from blocked sources. You have two options. You can either leave them in the Quarantine Database (QDB) where they will remain for the specified quarantine period or you can have them deleted immediately by selecting the appropriate option from the drop-down menu.



Email addresses and Email IP addresses: These boxes display the list of email address entries and IP addresses with their selected actions

like Allow email from, Block email from etc. To change the action against any address entry in the list, click on the action corresponding to the entry and select an action from the available options.



Select Email Account: Comodo AntiSpam maintains a separate ADB for every email account you use. Use this control to select the email account for which you want to view the ADB.

Add: Pressing the **Add** Button brings up the **Add Email Addresses** screen where you can Add more addresses to your Authentication Database. **Click here for more details.**

Remove: Pressing the Remove Button causes the selected addresses to be deleted from the Authentication Database.

Import: Pressing the **Import** Button brings up **Import Addresses** screen where you can import white and black lists from the Comodo server or from a file located on your computer. You can store the current Authentication Database configuration using Export option as White list and Black list files and can use the saved files for restoring Authentication Database configuration when you are reinstalling or updating Comodo AntiSpam application. **Click here for more details**.

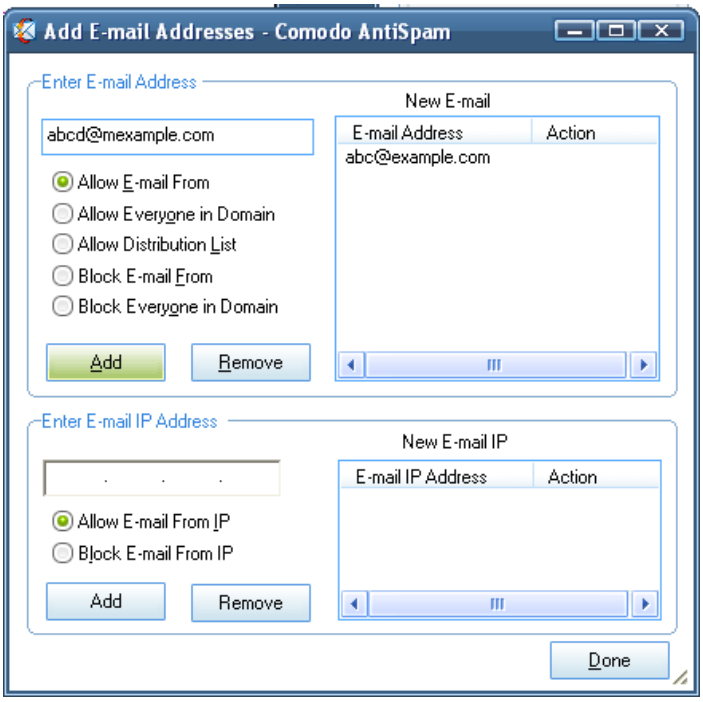
Export: Pressing the **Export** Button brings up **Export Addresses** screen where you can export addresses from your Authentication Database to local file as white listing or black listing. This helps to restore authentication database configuration when you are reinstalling or updating Comodo AntiSpam application. This also allows you to share your Authentication Database with friends, family members or colleagues. **Click here for more details.**

Automatically add the sender of digitally signed emails to the white list - Checking this box means that the sender of any email received with a digital signature is authenticated and all the mail from the same sender in future will be allowed.

Automatically add recipients of outgoing mails into white list - Checking this box means that the persons to whom you send mails are authenticated and the emails from those persons in future will be allowed.

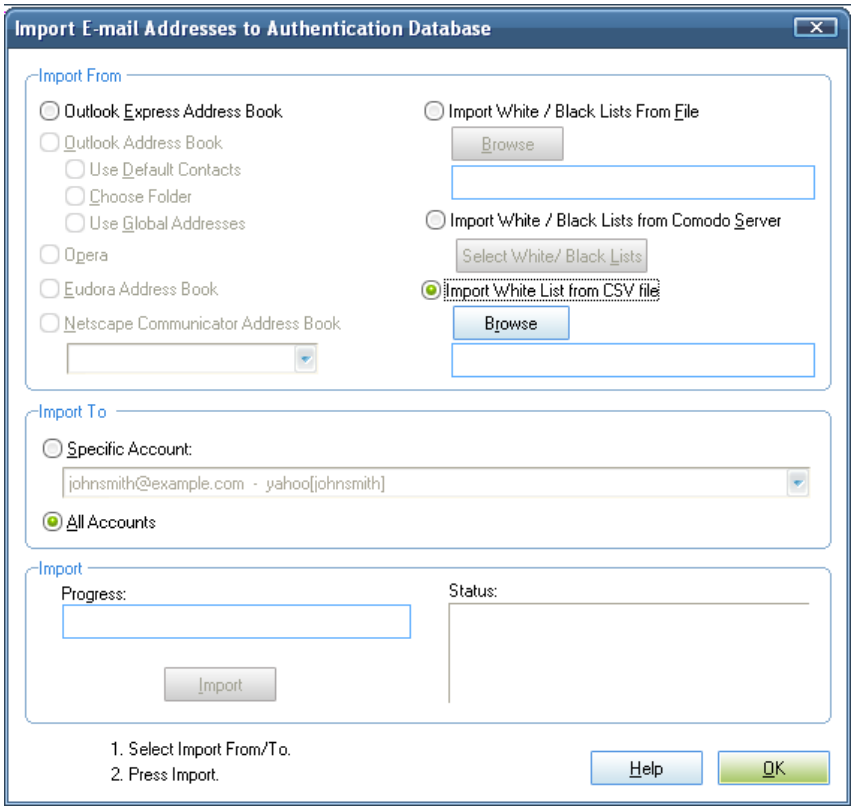
Adding Addresses to the Authentication Database

Pressing the Add button in the Authentication Database brings up the following screen where you can add new addresses. Here, you can either Allow or Block senders, domains or entire IP addresses.



Importing Addresses to the Authentication Database

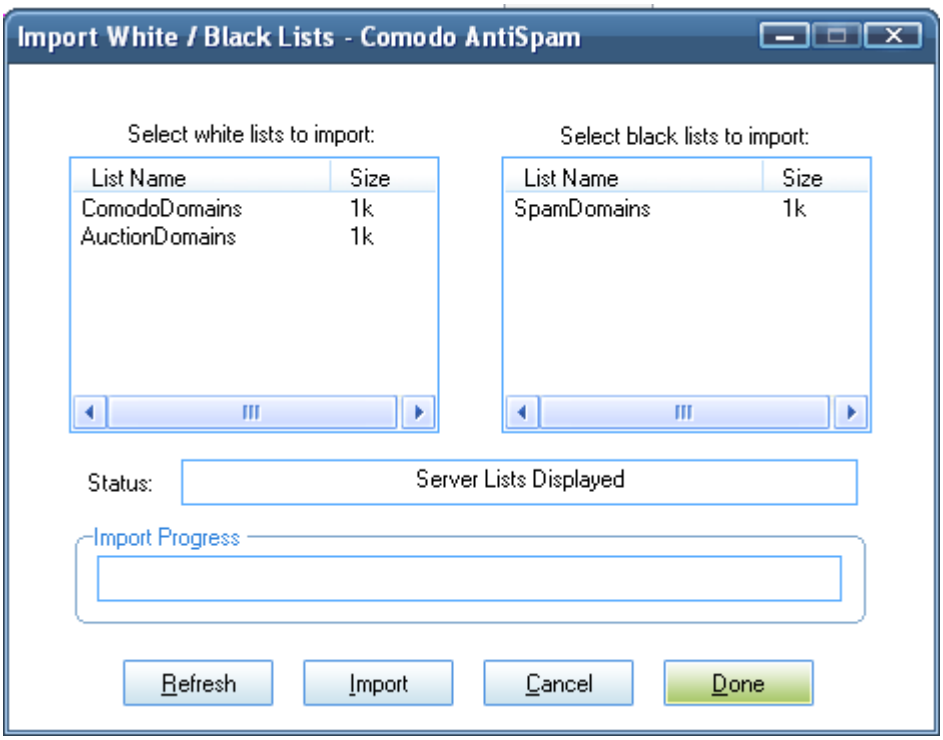
Pressing the **Import** button in the Authentication Database brings up the following screen. Here you can add addresses to you Authentication Database from various sources listed below.



You can select the source from which the authenticated addresses are to be imported in the **Import From** area. You can also select whether you want imported addresses are to be authenticated for your selected email account or all of your accounts, by using **Specific Account** or **All Accounts** options in the **Import To** area.

Lists can be imported from the following sources:

- **Import from your email client address book:** Select which email client application you are using, and press the **Import** button. Each address found in your address book is added to the ADB with **Allow Email From** status.
- **Import from White list file or Black list file stored in your computer:** Select the I**mport White/Black Lists From File** and click **Browse**. Navigate to the location in your hard drive, where you have stored your white list or black list file in the appearing explorer window and click Open. The address entries loaded from the selected list are stored in the ADB with **Allow Email From** or **Block Email From** status depending on whether those are taken from white list or black list file.
- **Import from Comodo Server:** Select the **Import White/Black Lists From Comodo Server** and click **Select White/Black Lists**. In the window that is displayed, select the white list and/or black list entries and click **Import**. The address entries loaded from the lists are stored in the ADB with **Allow Email From** or **Block Email From** status depending on whether those are taken from white list or black list.

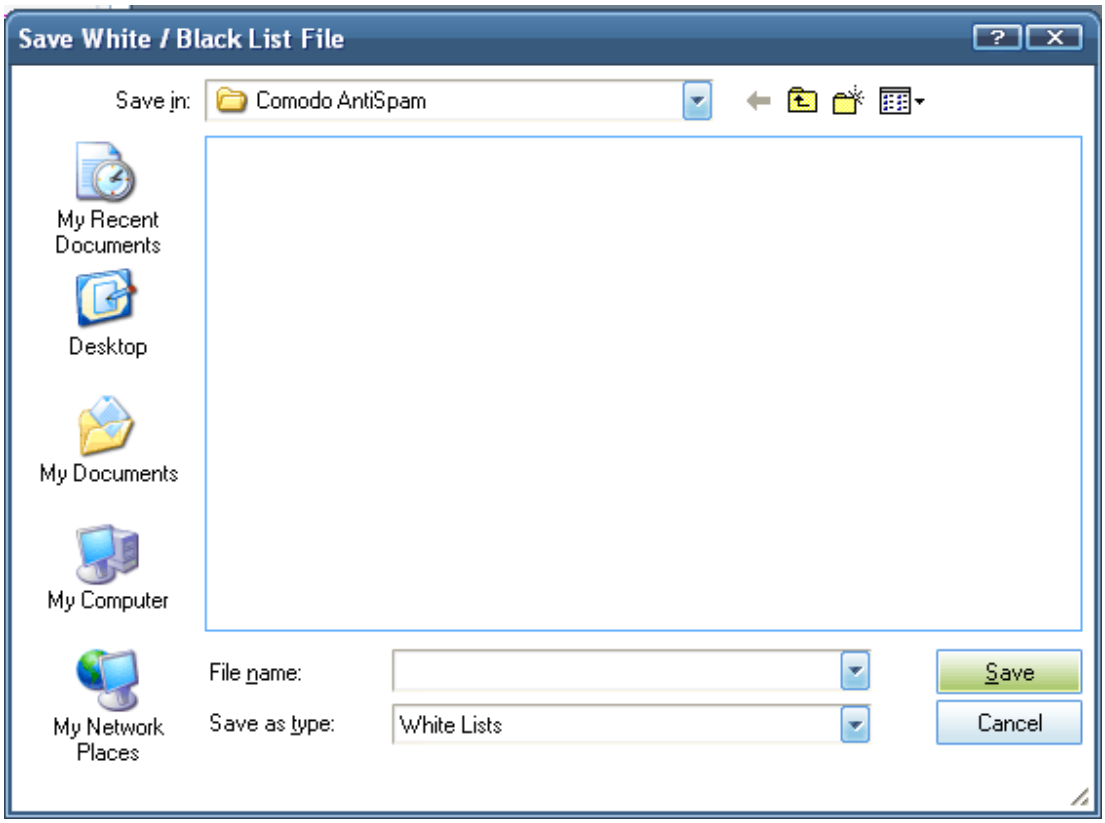


Note: You can import white-list email addresses and black-list email addresses from comodoantispam.com to add to your ADB. The black-list includes known spammer addresses that will be authenticated as blocked. The white-list addresses are trusted senders and will be authenticated as allowed.

- **Import from CSV file :** This option allows you to import the list of authenticated email address you have stored in your computer in a file of comma separated value (CSV) format. Select **White List from CSV file** and click **Browse**. Navigate to the location in your hard drive, where you have stored your CSV file. The address entries loaded from the file are stored in the ADB with Allow Email From status.

Exporting Addresses from Authentication Database to White List or Black List Files

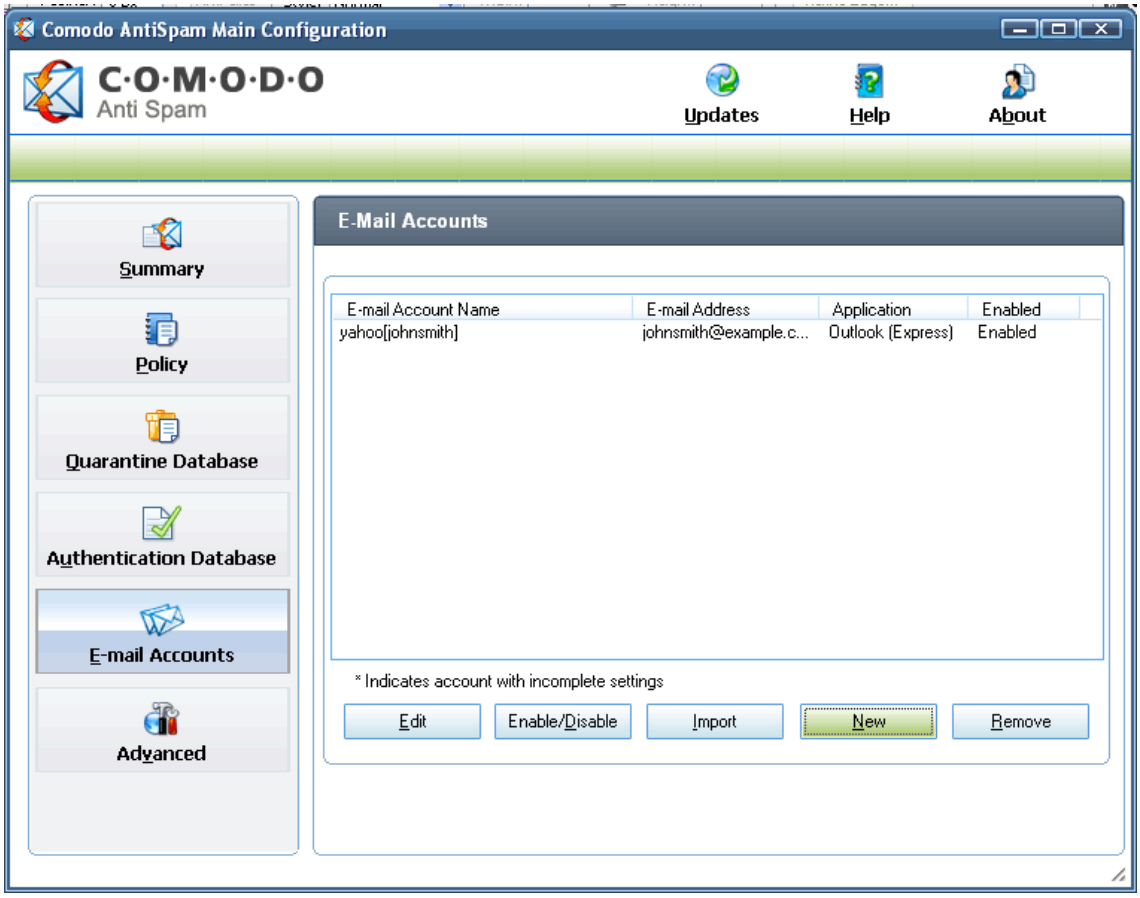
Pressing the Export button in the Authentication Database brings up the following screen.



The addresses in your authentication database are stored as white list files and black list files, depending on whether they are allowed or blocked in the location as you specify through this window.

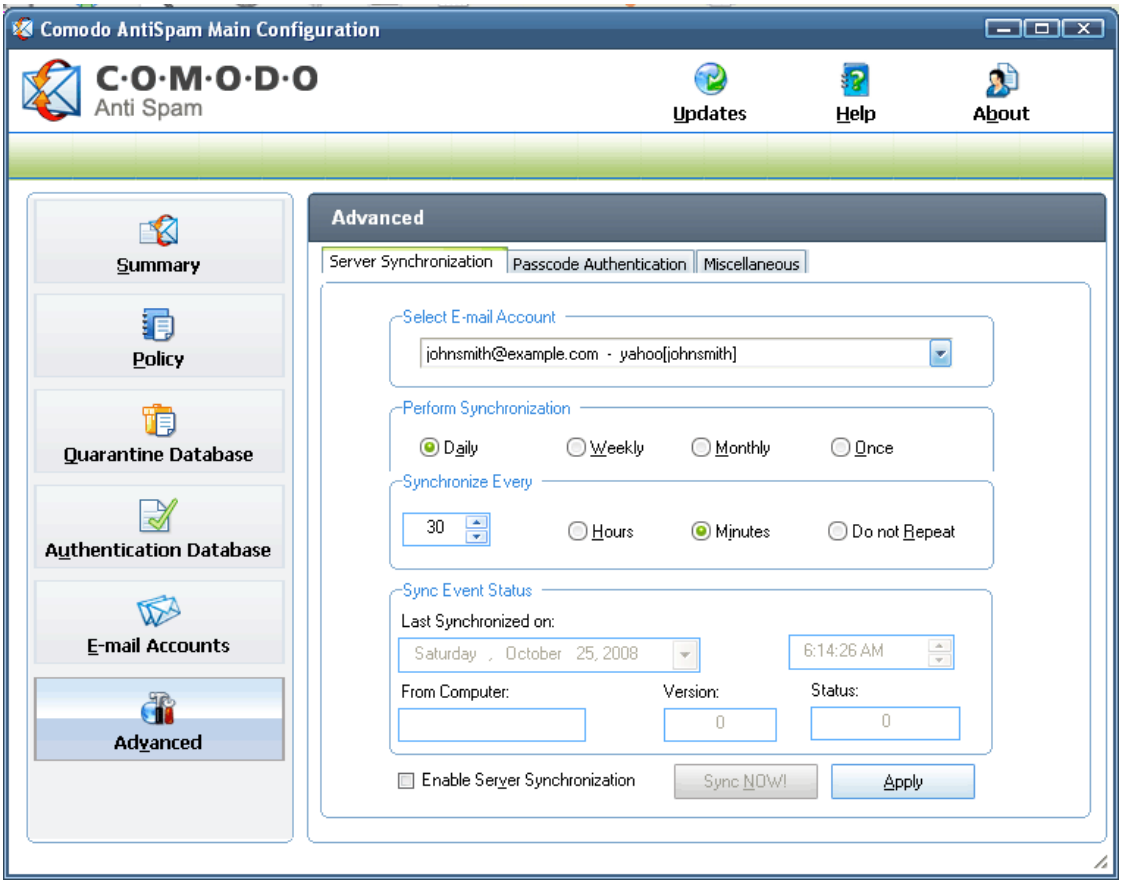
4.4. Configured Email Accounts

Pressing the **Email Accounts** button in the **Main Configuration** screen brings up the **Configured Email Accounts** screen shown below. Here you can view the accounts that Comodo AntiSpam has automatically detected. This screen allows you to optionally Add, Edit or Import email accounts.



4.5. Server Synchronization

Comodo AntiSpam provides an advanced feature, which allows you to synchronize the state of Passcode Authentication between multiple computers. If you access your email from more than one location, with **Comodo AntiSpam installed on each computer**, you will want to enable this feature to ensure the Passcode Authorization process only occurs once for each unknown sender.



Select Email Account: Select the email account to which the Server Synchronization settings are to be applied.

Note: The Enable Server Synchronization check box on the Main Configuration screen is a general enable for this feature.

Perform Synchronization: These radio buttons Enable or Disable Server Synchronization for the selected account. You can select the interval at which the server synchronization has to be carried out using the time options available in this area.

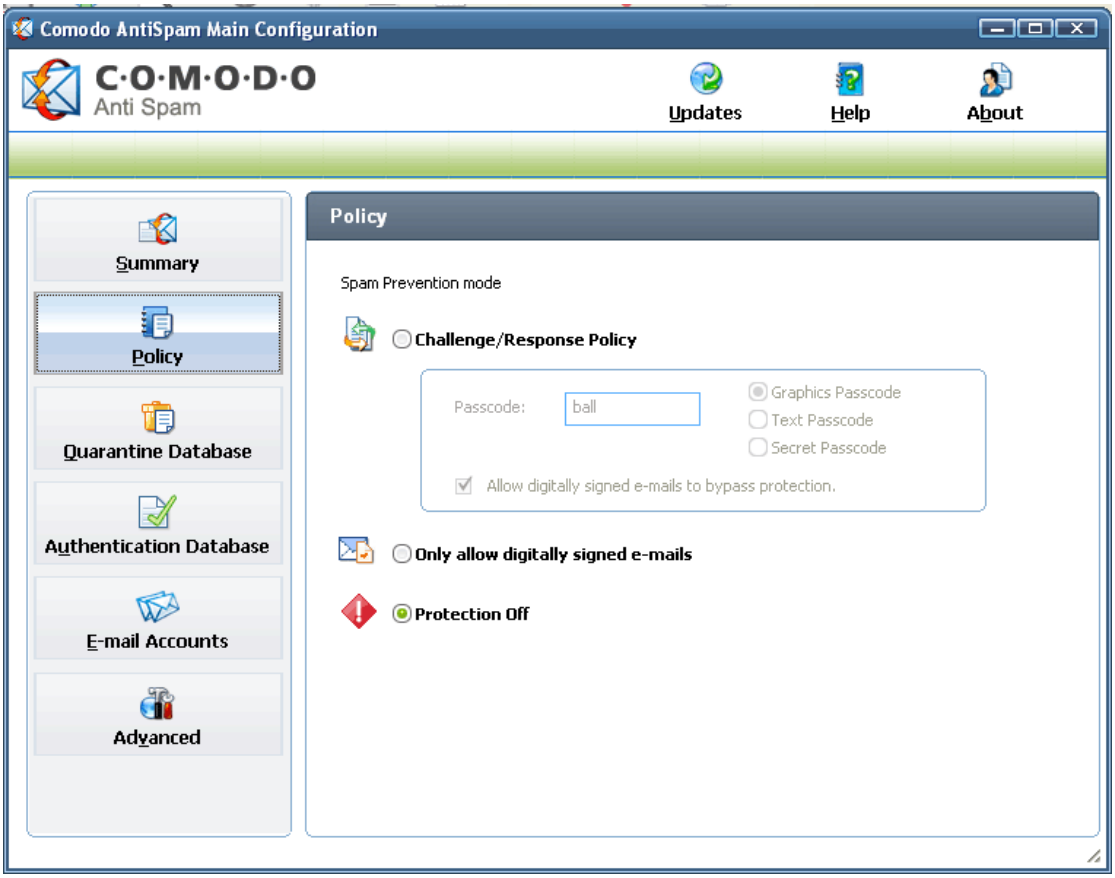
Synchronization Event Status: These fields tell you when the last synchronization event occurred, what computer generated the synchronization data, the version of the synchronization data and the operational status of the synchronization event.

Enable Server Synchronization: Checking this check box enables Server Synchronization. Server Synchronization is used if you access your email from more than one computer with AntiSpam installed on each computer. It ensures the authentication state is maintained between all computers. See **Server Synchronization** for more details on this feature.

5.Policy

The Policy management screen allows you to specify/edit configuration settings like Passcode, mode of sending the passcode in the AntiSpam alert message to the sender etc. This screen also provides option to toggle between enabling and disabling Comodo AntiSpam.

- Click on the 'Policy' tab to open Policy Management Screen.



Challenge/Response Policy: Selecting this option enables you to edit the configuration of Comodo AntiSpam.

Passcode: You can enter a new passcode or change the passcode entered previously during initialization. Examples of good passcodes include ORANGE, KITTYABC, BEACH17, ISLAND etc.

After entering your passcode, select the manner in which your passcode has to be sent to the unknown sender for authentication. See **Passcode Authentication Technology** for more details.

If you select:

Graphics Passcode - The image of the passcode is sent. This means that the sender has to identify the characters from the image and type the passcode in order to respond to the challenge/response mail.

Text Passcode - The passcode is sent in a text format. The sender can simply click reply, as the passcode will already be in the mail, or can copy it from the mail in order to respond to the challenge/response mail.

Secret Passcode - The passcode is not sent with the challenge response mail. The sender has to type the passcode that he/she has acquired from the recipient beforehand by some other method of communication in order to respond to the challenge/response mail.

Allow digitally signed emails to bypass Protection - If enabled, the messages received with the digital signature of the sender will be passed to your inbox, without being subjected to Challenge/Response policy.

Note: You should not use a passcode that you use for any secure accounts (bank, etc), as your passcode will be visible to email senders during the authentication process.

Note: Please ensure that the AntiSpam Passcode which you enter in the Configuration screen does NOT match with the following keywords: Comodo, AntiSpam, Computer, Passcode, Email, Spam, Spammer, Alert, Authentication, Technology and Junk and should NOT be your name or email address.

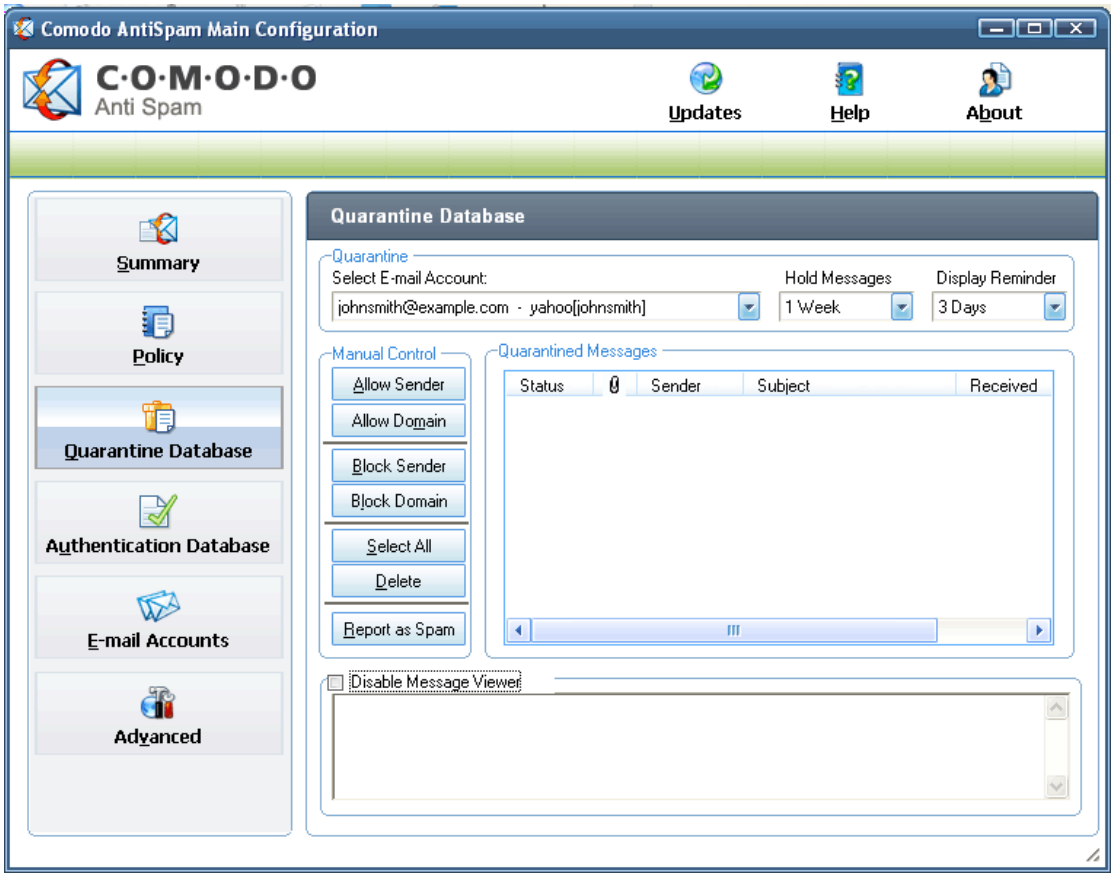
Note: AntiSpam Alert messages are sent to senders of email who are unknown to you.

Only allow digitally signed emails: If enabled, you will receive only digitally signed emails, all other emails will be blocked.

Protection Off: Selecting this option disables Comodo AntiSpam. All the mails in the quarantine database will be passed to your inbox and all the incoming mails will be allowed.

6. Using the Quarantine Database

The **Quarantine Database** screen is displayed by pressing the **Quarantine Database** button on the **Main Configuration** screen. The Quarantine Database is a temporary storage area for all emails pending authentication. A Quarantine Database is created for each of your email accounts. When you retrieve your email using your email client application (e.g. Outlook Express or Outlook), AntiSpam checks the senders email address against all email addresses in the ADB. If a match is not found, the email message is temporarily stored in the QDB and an AntiSpam Alert message is automatically sent to the sender of the unauthorized email message requesting that sender reply with your AntiSpam Passcode.



See also:

- **Setting the QDB Hold-Time**;
- **Using the Quarantine Database Reminder** ;
- **Allowing/Blocking Senders and Domains from the QDB**;
- **Manually Deleting Spam from the QDB**;
- **Reporting Messages as Spam**.

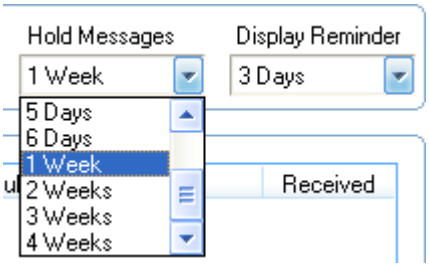
6.1. Setting the QDB Hold -Time

The messages from blocked senders specified as blocked in the Authentication database and messages which are pending for authorization are temporarily stored in the **Quarantine Database** for a user-specified period of time from the time of their receipt. On lapse of the period, the message is deleted automatically. The Hold **Messages option** in the Quarantine database management screen allows you to specify the hold-

time for each quarantined message.

To change the QDB Hold-Time

1. Open the Quarantine Database from the Main Control screen.
2. Select the Email Account for which you want to apply the current settings.
3. Click on the Hold Messages drop-down menu and select the desired setting. The default is 1 week.
4. Press OK to exit the Quarantine Database.

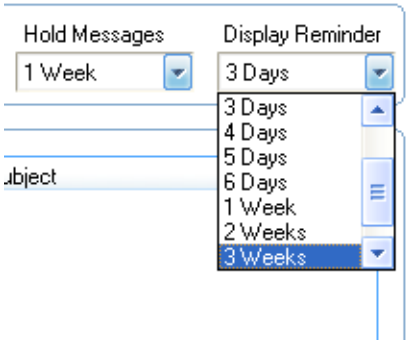


6.2. Using the QDB Reminder

Comodo AntiSpam reminds you to look through the Quarantine Database periodically. The interval of these remainders can be specified by the user using Display Remainder setting option in the Quarantine Database management screen.

To adjust this setting

1. Open the Quarantine Database from the Main Control screen.
2. Select the Email Account for which you want to apply the current settings.
3. Click on the Display Reminder drop-down menu and select the desired setting. The default is 3 days.
4. Press 'OK' to exit the Quarantine Database.



6.3. Allowing/Blocking Senders & Domains From the QDB

The Quarantined Messages box in the Quarantine Database management interface screen displays the messages in the QDB from trusted senders. This simply means that they have not yet responded to the AntiSpam Alert message with your AntiSpam Passcode. In this case you can manually allow them by pressing:

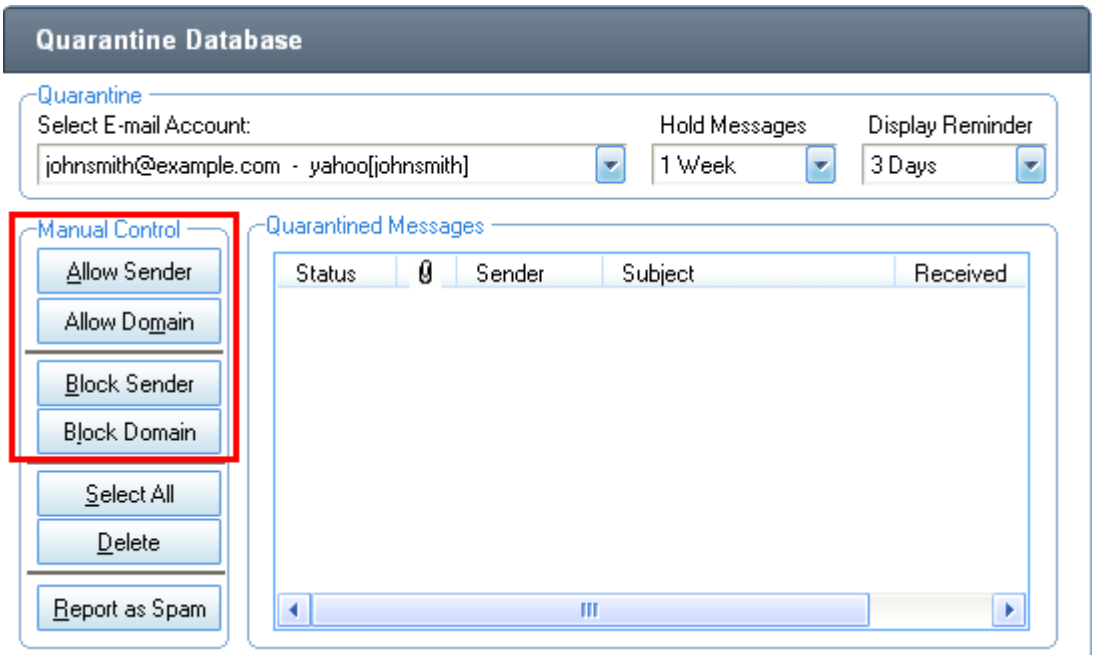
Allow Sender - To allow only that exact email address to send you email messages.

Allow Domain - To allow everyone in that senders' domain to send you email messages.

When browsing the QDB you may see annoying spam messages from the same addresses or even a single address. Generally you can leave them in the QDB and they will be deleted after the their hold-time expires. Optionally, you can manually block them by pressing:

Block Sender - To block only that exact email address from sending you email messages.

Block Domain - To block everyone in that senders' domain from sending you email messages.



6.4. Manually Deleting Spam from the QDB

Any spam message, residing in the QDB will be deleted from your mail server after the Hold-Time has elapsed, if left unattended. Optionally, you can use the **Delete** button to immediately remove any spam messages from your mail server.

To delete spam messages

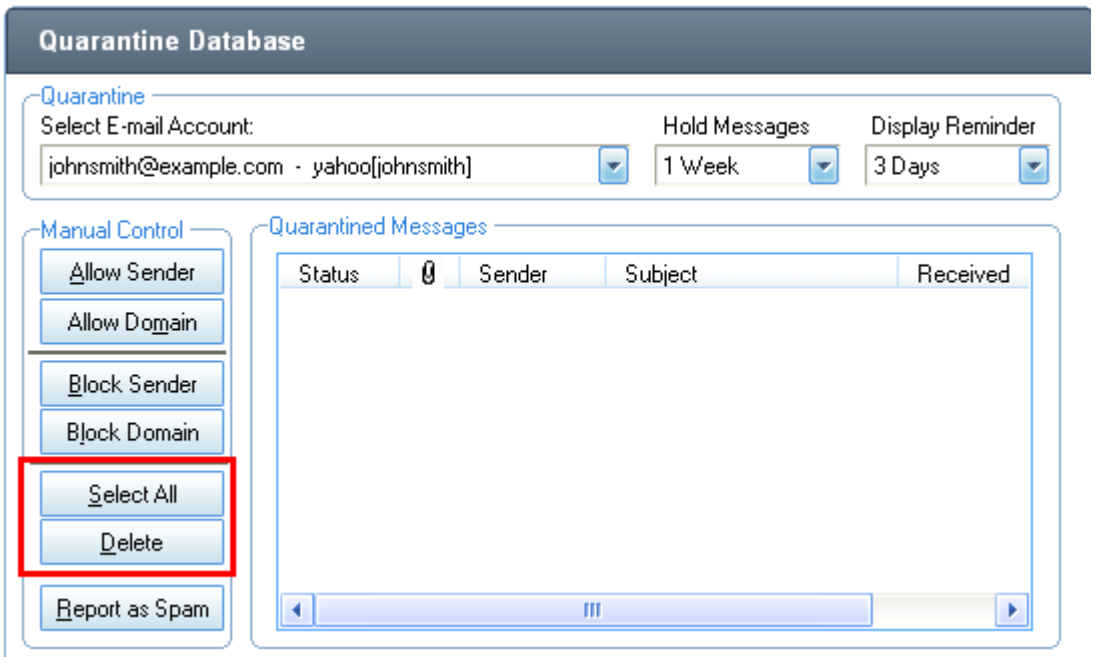
1. Open the Quarantine Database from the Main Control screen.

2. Make sure you have the correct Email Account selected in the Email Account drop-down control.

3. Select the messages you want to purge. To select more that one messages, press the control key while clicking on messages. To select all messages, press the Select All button.

4. Press the Delete button to remove the selected messages. The next time you access your email, all deleted messages will be removed from your mail server.

5. Press 'OK' to exit the Quarantine Database.

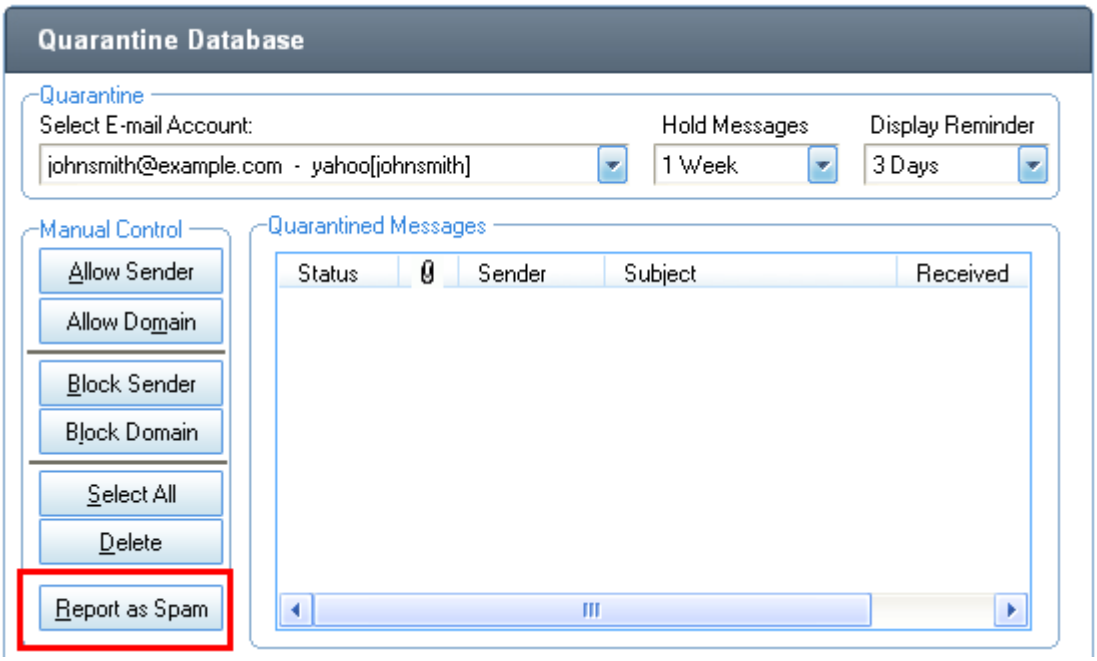


6.5. Reporting Messages as Spam

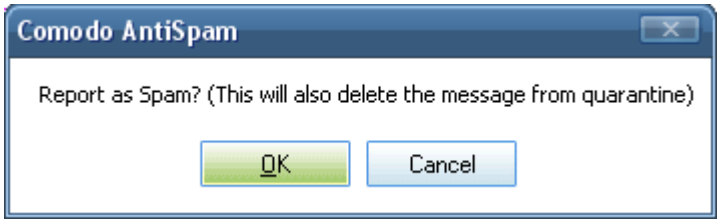
The Quarantine database management interface allows you to report the messages held in the QDB as Spam to Comodo. This can be done if you suspect a message listed in the Quarantined messages box as a spam.

To report a selected message as Spam

1. Select a message to be reported as Spam from the Quarantine Database.
2. Click 'Report as Spam'.



The following **Comodo AntiSpam** dialog box appears prompting you to report the selected message as Spam to Comodo.



3. Click **'OK'** to report the selected message as Spam or otherwise click 'Cancel'.

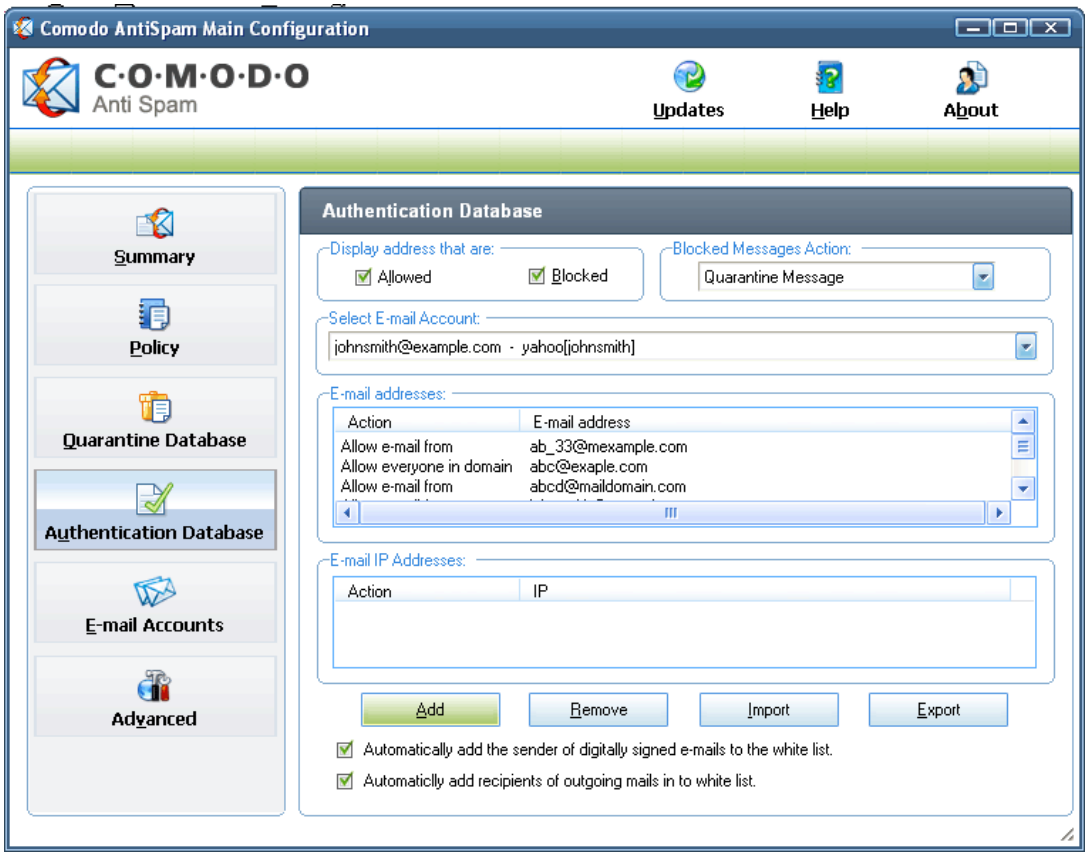
Note: A message reported as Spam to Comodo will be deleted from the Quarantine database.

7. Using the Authentication Database

The **Authentication Database** (ADB) holds a list of email addresses which, have either an **Allowed** or **Blocked** designation. When you retrieve your email using your email client application (e.g. Outlook Express or Outlook), the sender of each message is checked against all email addresses in the ADB. If a match is found and it is designated Allowed, the email is immediately allowed to pass to your email application

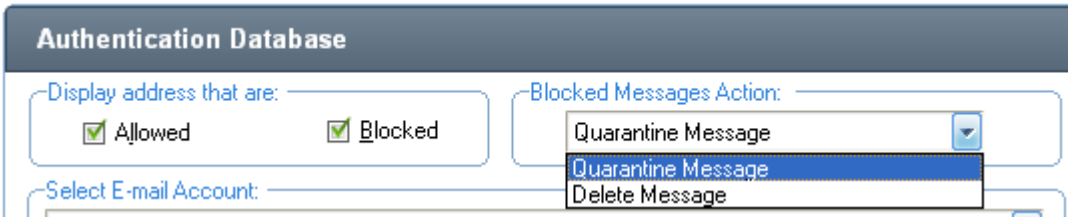
client. If a match is found and it is designated Blocked, the email either immediately deleted or is stored in the Quarantine Database for a prescribed period of time, whichever you choose.

Click on Authentication Database to view the **Authentication Database** (ADB) management interface screen. the interface screen displays a list of email addresses and email IP addresses, which are either allowed or not allowed (blocked) to send you email messages. With this interface, you can change the designation of email addresses, set the action to be taken against blocked messages, add, remove, import and export additional addresses.



Display Addresses that are: This control allows you to specify only the selected (allowed, blocked, white list, or black list) entries for display. Anyone or both the check boxes can be selected. This feature is very useful when you are looking for a specific ADB entry. The allowed and blocked addresses are displayed as lists in the **Email addresses** and **Email IP addresses** boxes.

Blocked Messages Action: This control can be used to specify the action to be taken against the messages from blocked senders. You have two options. You can either leave them in the Quarantine Database (QDB) where they will remain for the specified quarantine period or you can have them deleted immediately by selecting the appropriate option from the drop-down menu.



Select Email Account: Comodo AntiSpam maintains a separate ADB for every email account you use. Use this control to select the email account for which you want to view the ADB.

Email addresses and **Email IP addresses:** These boxes display the list of email address entries and IP addresses with their selected actions like Allow email from, Block email from etc. To change the action against any address entry in the list, click on the action corresponding to the entry and select an action from the available options.

If you select:

Allow Email From - The messages from that sender address are always allowed.

Allow Everyone in Domain - All the messages from the given domain are allowed, except if other ADB address from the same domain have Block Email From selected. In which case these individual addresses can be blocked, while allowing everyone else in the domain.

Note: Block Email From has precedence over Allow Everyone in Domain.

Allow Distribution List - All the messages from that address and the addresses in the respective distribution list, (i.e. CC addresses) are always allowed.

Note: The messages To and Cc addresses are authenticated for distribution lists, as subscribers are generally Blind Carbon Copied (Bcc).

Block Email From: If selected, messages from that sender address are always blocked.

Block Everyone in Domain: If selected, all messages from the given domain are blocked except if other ADB address from the same domain have Allow Email From selected. In which case these individual addresses can be allowed, while blocking everyone else in the domain.

Note: Allow Email From has precedence over Block Everyone in Domain.

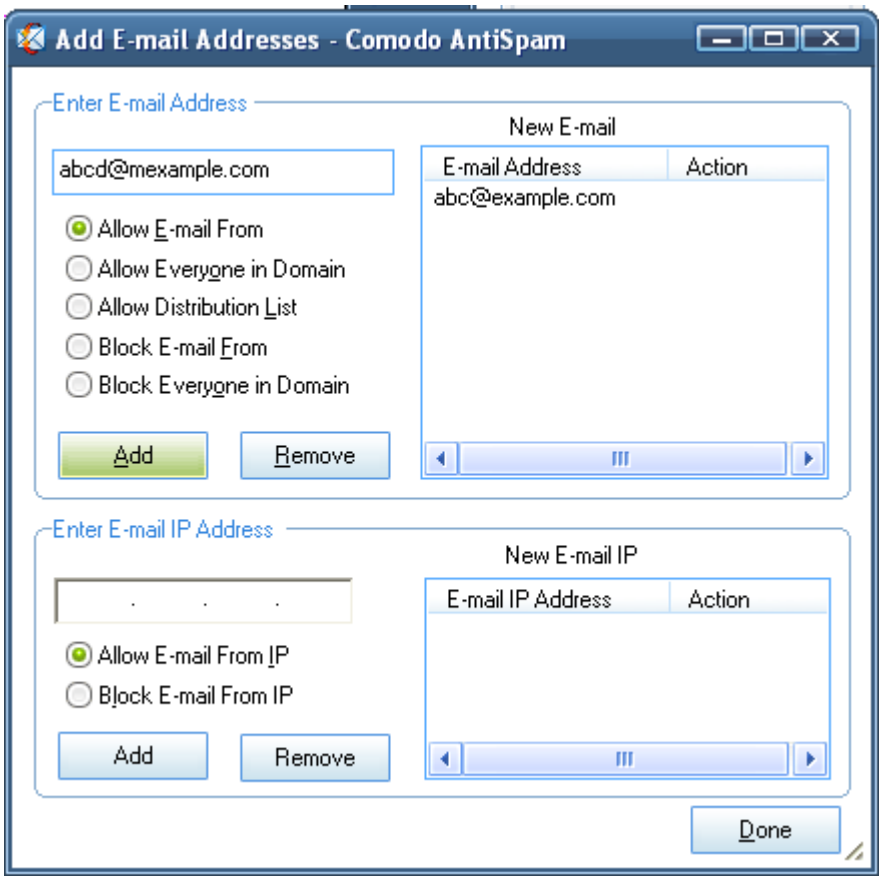
Upon successful Passcode Authentication, a new address is added to the ADB with the **Allow Email From** control.

See also:

- **Adding Allowed or Blocked Addresses to the ADB**
- **Importing Your Address Book to the ADB**
- **Exporting addresses from the ADB**

7.1. Adding/Removing Allowed or Blocked Addresses to the ADB

You can Add or Remove addresses to or from the Authentication Database manually. Generally, you would not want to Remove an address, however the control exists to do so. Click on the Add button in the Authentication Database management interface to obtain the Add Email Addresses interface.



To add an entry to the ADB

1. Type an email addresses in the Enter Email Address text box.
2. Select the action to be taken (i.e. Allow Email from, Block Email from etc.) against the typed address.
3. Click 'Add'.

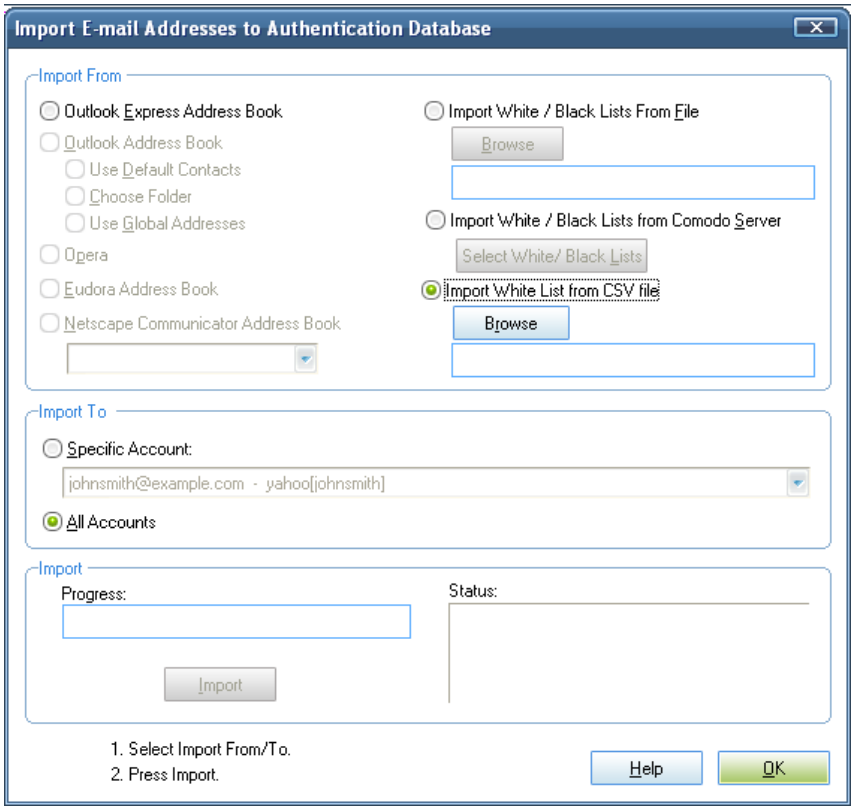
- Repeat the procedure for adding several addresses one by one.

You can see the addresses adding up in the New Email list box, as you add the email addresses one by one

- To remove an existing email address entry, select the address from the New Email list box and click **'Remove'**.
- You can follow the same steps for entering Email IP Addresses and designate respective actions.
- Click **Done** to close the **Add Email Addresses** interface.

7.2. Importing Your Address Book to the ADB

You can import the Address book maintained with your email client, white or black lists from your local file, white or black lists maintained at Comodo server and from a comma separated value (CSV) file maintained in your system into the Authentication database. Click on the **Import** button in the Authentication database management interface screen to obtain **Import Email addresses** interface.



You can select the source from which the authenticated addresses are to be imported in the Import From area. You can also select whether you want imported addresses are to be authenticated for your selected email account or all of your accounts, by using Specific Account or All Accounts options in the Import To area.

Lists can be imported from the following sources:

- **Import from your email client address book:** Select which email client application you are using, and press the **Import** button. Each address found in your address book is added to the ADB with **Allow Email** From status. Messages from any of the addresses imported are allowed to pass.

Note: If the **Import** button is not enabled, this means that your importing your email program's address book is not yet supported. Comodo AntiSpam is diligently working to support all email program address books. Check to see if this update is available by pressing the **Check For Updates** button on the **Main Configuration** screen.

- Import from White list file or Black list file stored in your computer:

Black Lists: A black list is a list of known bad (Spammer) addresses. These addresses are imported with a **Blocked** control. It is generally NOT recommended to import Black Lists, as the Passcode Authentication algorithm will quarantine unknown senders until they pass the authentication process.

White Lists: A white list is a list of trusted email addresses. These addresses are imported with an **Allowed** control. Importing white lists provides a means to allow email messages from no-respond addresses. A no-respond address is an address, which sends you email but does not receive email, like a receipt for something you bought on the Internet.

To import White list file or Black list file from your computer

1. Select the **Import White/Black Lists From File** and click **Browse**.
2. Navigate to the location in your hard drive, where you have stored your white list or black list file in the appearing explorer window and click **Open**.

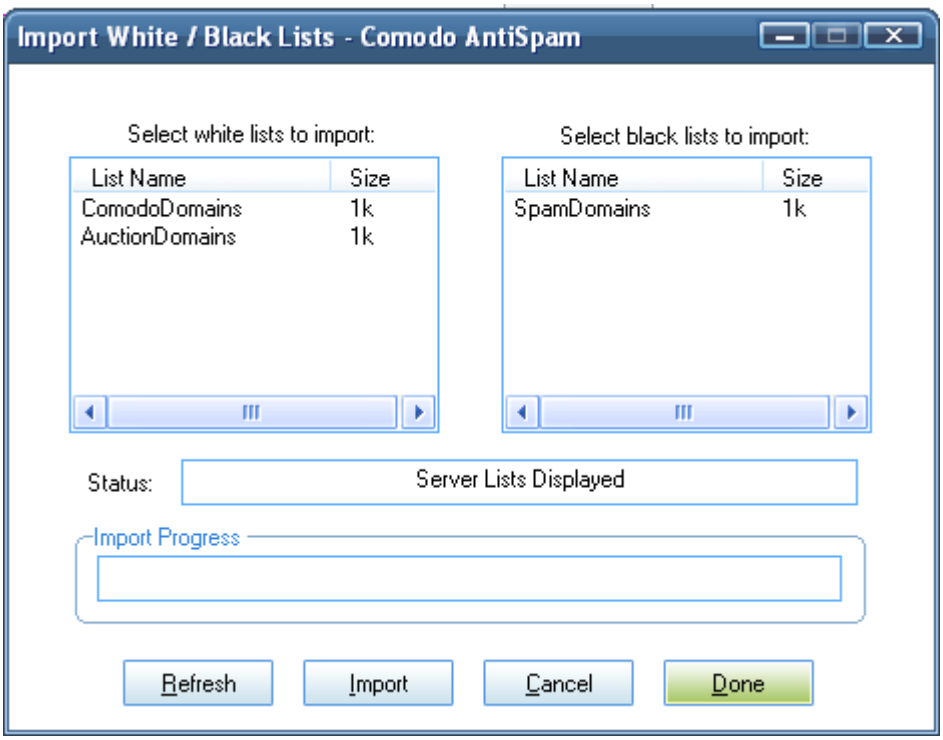
The address entries loaded from the selected list are stored in the ADB with **Allow Email From** or **Block Email From** status depending on whether that are taken from white list or black list file. This is useful when you are uninstalling and reinstalling or updating Comodo AntiSpam.

- **Import from Comodo Server:** You can import white-list email addresses and black-list email addresses from comodoantispam.com to add to your ADB. The black-list includes known spammer addresses that will be authenticated as blocked. The white-list addresses are trusted senders and will be authenticated as allowed.

To import White list file or Black list file from Comodo Server

1. Select the **Import White/Black Lists From Comodo Server** and click **Select White/Black Lists**.
2. In the window that is displayed, select the white list and/or black list entries and click **Import**.

The address entries loaded from the lists are stored in the ADB with **Allow Email From** or **Block Email From** status depending on whether that are taken from white list or black list.

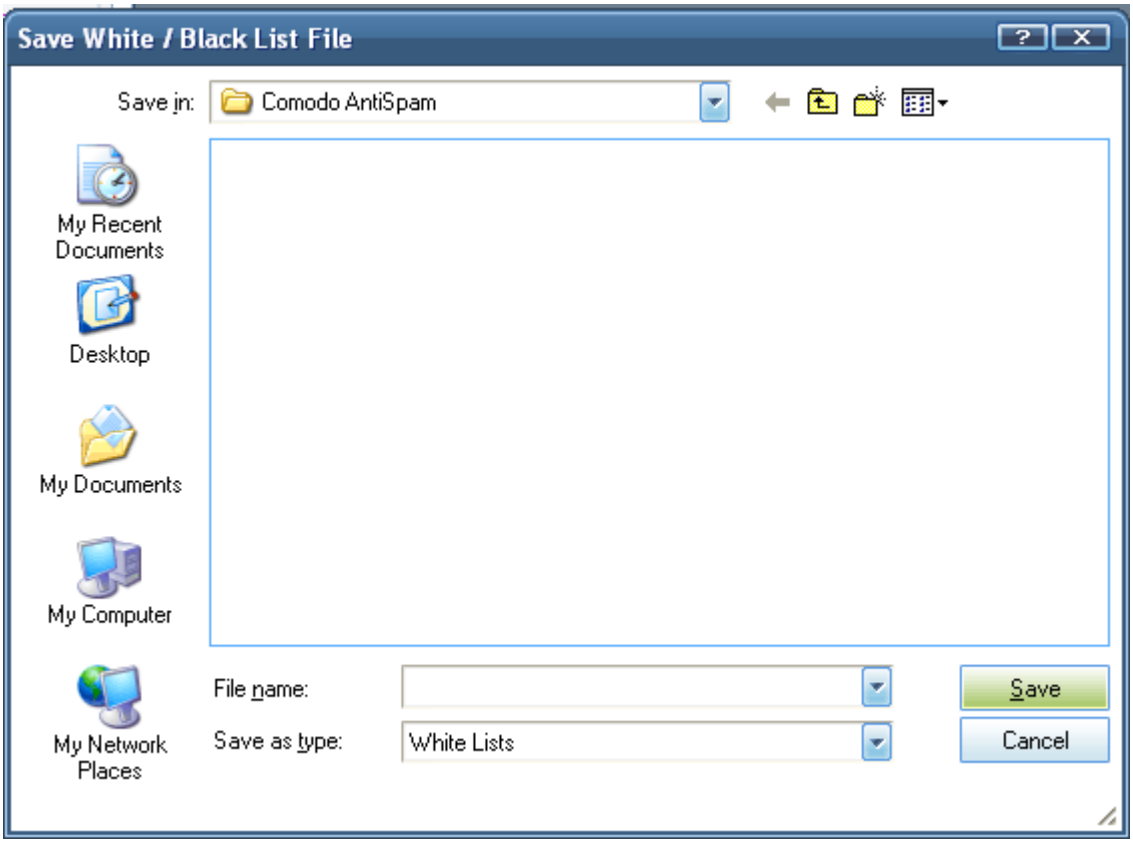


- **Import from CSV file:** This option allows you to import the list of authenticated email address you have stored in your computer in a file of comma separated value (CSV) format. Select White List from CSV file and click 'Browse'. Navigate to the location in your hard drive, where you have stored your CSV file and click 'Open'. The address entries loaded from the file are stored in the ADB with Allow Email From status.

7.3. Exporting Addresses from the ADB

You can export the Addresses maintained in your Authentication Database as a white list file or black list file and store in your system as a back-up. This is useful when you are uninstalling and reinstalling or updating Comodo AntiSpam. You can import the white list and the black list

after you reinstall or update the application. Click on the Export button in the Authentication database management interface screen to obtain Save As interface.

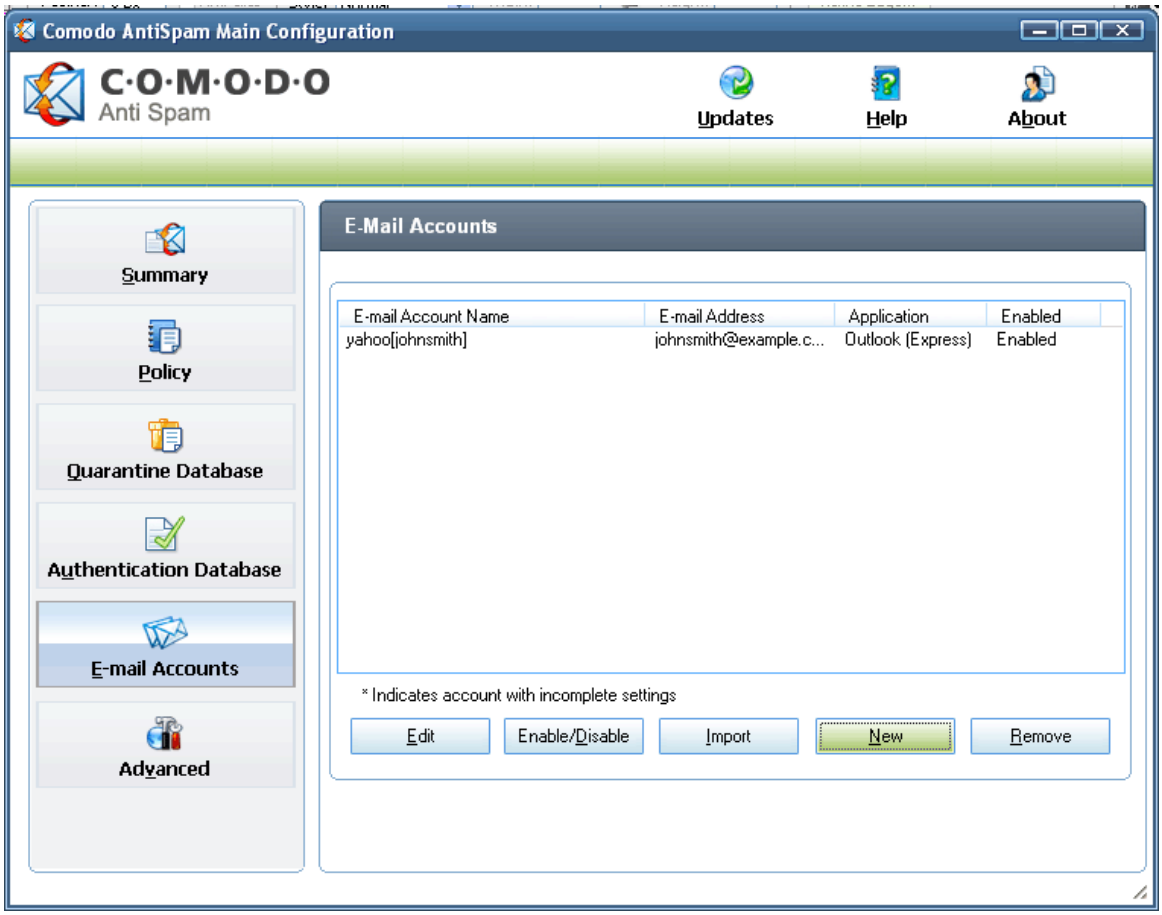


To export the addresses

1. Select the destination folder.
2. Type a file name in the File Name text box.
3. Select the file type from White Lists or Black Lists.
4. Click 'Save'.

8.Managing Email Accounts

Comodo AntiSpam automatically detects your configured email accounts. You will probably never have to manually add or edit an email account within Comodo AntiSpam. However, if for some reason AntiSpam does not recognize and email account you will be prompted to add or edit your email account information. The Email accounts management interface screen, which shows the Configured Email Accounts screen can be accessed by clicking Email Accounts button in the main configuration interface. You can edit individual account settings, if needed.



Edit: This option allows you to edit an existing email account. To edit an existing account, select the account from the displayed list and click Edit. An Email Account Settings screen with the current settings for the selected account is displayed. You can edit the settings from the window.

Enable/Disable: This control toggles between enabled and disabled states of the Comodo AntiSpam protection offered for the email account selected from the list.

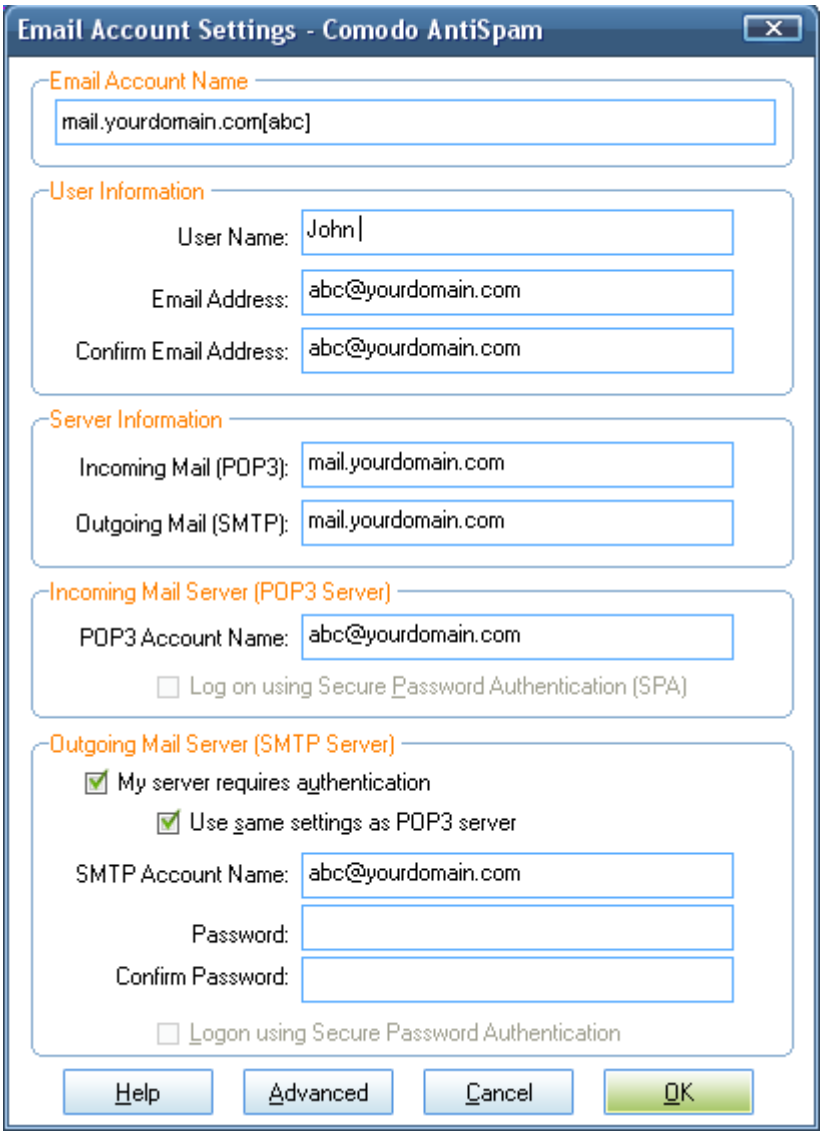
Import: This control button automatically scans the windows registry and imports all email accounts.

New: This control brings up a blank Email Account Settings screen, which guides you through the process of adding a new account.

Remove: This control removes the selected Email account from the Comodo AntiSpam protection.

8.1. Email Account Settings

The Email Account Settings screen allows you to either add or change an email account's settings.



User Name: Enter your real name here (e.g. John Smith)

Email Address: Enter the account email address here.

Confirm Email Address: Again enter the account email address here. The entry here should be the same as the Email Address entered above.

Incoming Mail Server (POP3): Enter the account POP email server address here (e.g. pop.myserver.com, mail.mydomain.com).

Outgoing Email Server (SMTP): Enter the account SMTP email server address here (e.g. smtp.myserver.com, mail.mydomain.com).

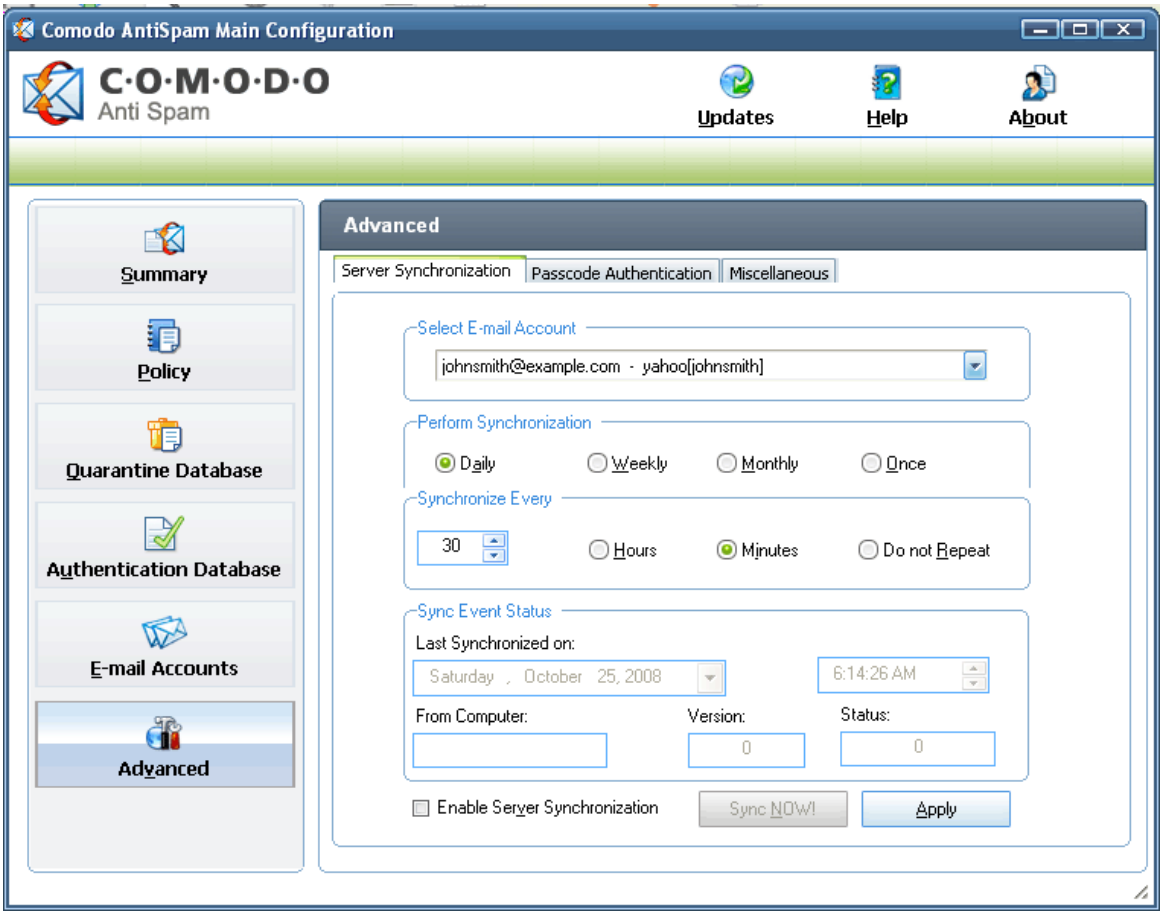
Account Name: Enter the Name Here. This is the account name you use to log into the POP server (i.e. MyUserName, MyUserName+mydomain.com).

Outgoing Mail Authentication: If your email account requires you to use email account authentication for your outgoing email (SMTP), enter your account and password in the provided fields.

9.Advanced Settings

The Advanced Settings screen allows you to fine tune Comodo AntiSpam's operation. Click on the 'Advanced' button to access the Advanced

settings screen.



The following sections describe the settings available on each of the advanced tabs.

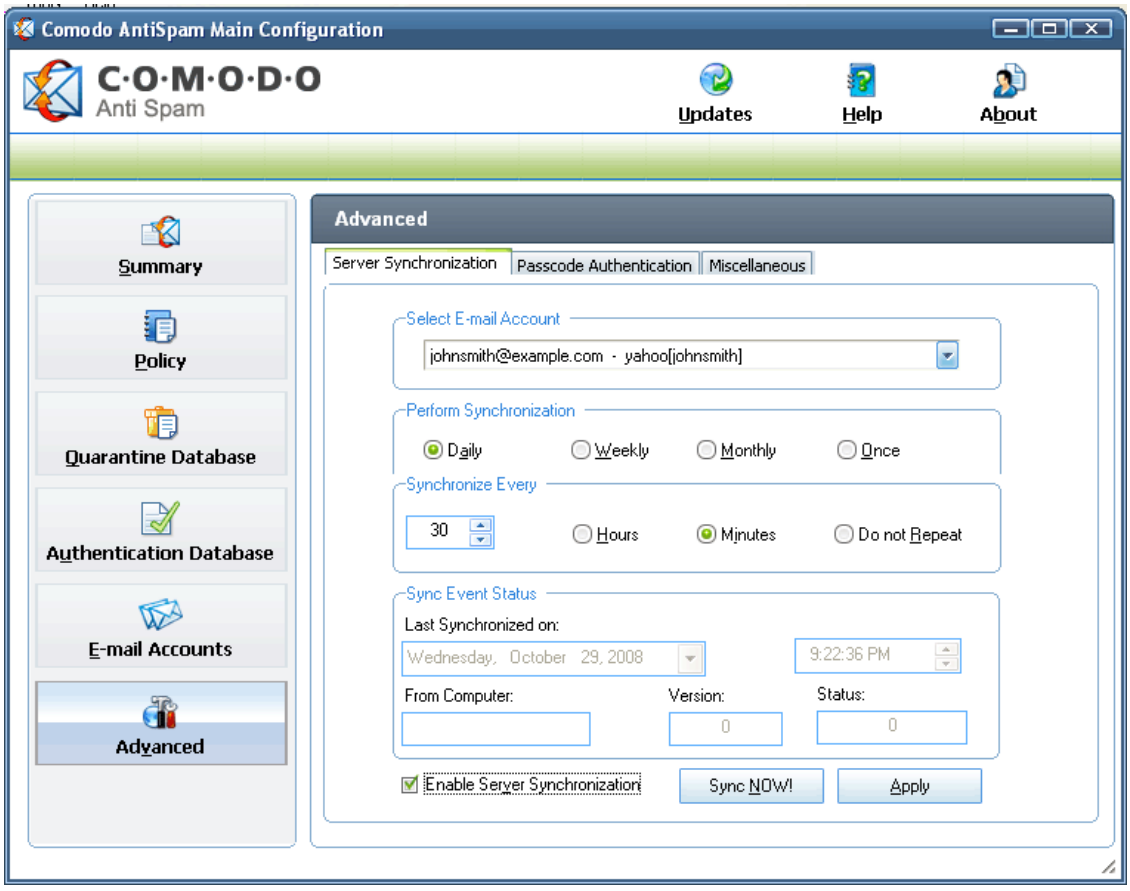
- **Server Synchronization**
- **Passcode Authentication**
- **Miscellaneous**

9.1. Server Synchronization

During the process of Passcode Authentication, each unknown sender is transitioned through multiple states of authentication. Server Synchronization allows you to save the state of each unknown sender on your email server.

Server Synchronization enables you to access your email account from multiple computers (with Comodo AntiSpam installed) while maintaining the Passcode Authentication state for unknown senders across each computer. The synchronization file is sent as an attachment to an email message to your email account (i.e. to yourself). If a synchronization message is found with a newer version, it is decompressed, decrypted, and merged into your local Comodo AntiSpam Passcode Authentication files.

Transmitting the synchronization information is quite efficient and secure. The Synchronization data is both encrypted and compressed. Click on Server Synchronization tab to access the Server Synchronization interface.


Comodo AntiSpam Main Configuration
C·O·M·O·D·O
Anti Spam
Updates
Help
About
Summary
Policy
Quarantine Database
Authentication Database
E-mail Accounts
Advanced
Advanced
Server Synchronization
Passcode Authentication
Miscellaneous
Select E-mail Account
johnsmith@example.com - yahoo[johnsmith]
Perform Synchronization
Daily
Weekly
Monthly
Once
Synchronize Every
30
Hours
Minutes
Do not Repeat
Sync Event Status
Last Synchronized on:
Wednesday, October 29, 2008
9:22:36 PM
From Computer:
Version:
Status:
0
0
Enable Server Synchronization
Sync NOW!
Apply

Configuring Server Synchronization

Mark the **Enable Server Synchronization** check box on the **Comodo AntiSpam - Advanced Settings** screen to enable this feature. The **Sync Now!** button now become active. This screen contains the controls for enabling synchronization for your individual accounts. Follow the steps given below to configure server synchronization for a given account. The following instructions must be performed on each computer you intend to access the selected email account from.

1. Make sure you have the desired **Email Account** selected in the **Select Email Account** drop-down.

2. Select whether you want synchronization to be performed Daily, Weekly, Monthly or only Once.

3. Select the start Date and Time you wish to begin synchronization.

4. If you selected to perform Synchronization Daily, now select what time interval to during the day to perform synchronization.

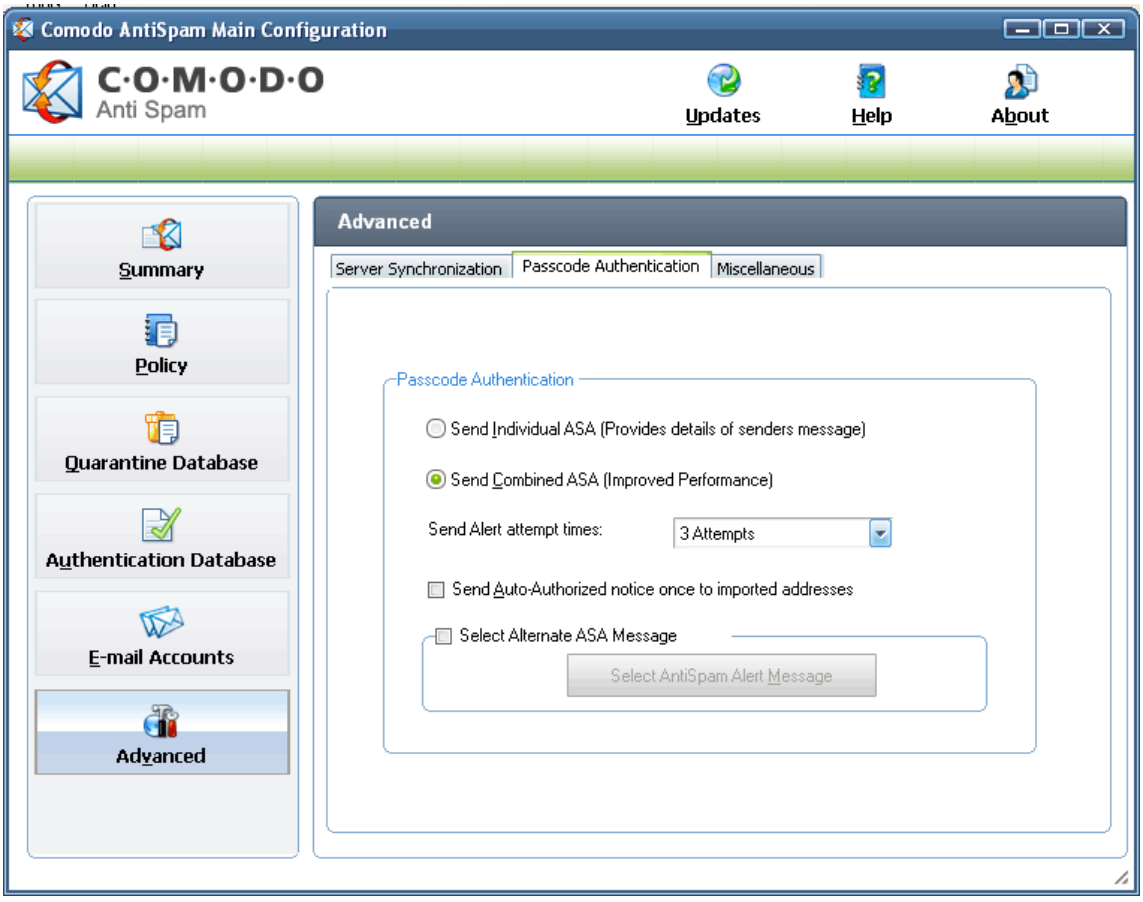
At the prescribed time interval, Comodo AntiSpam will check to see if the state of any messages' Passcode Authentication has changed. If it has, a synchronization file is compiled and sent to the email account's server.

When downloading messages to your computer, Comodo AntiSpam first checks to see if there is a newer synchronization file on the server. If it finds one, it is opened, decompressed, decrypted and merged into the local Comodo AntiSpam synchronization data.

The Sync Event Status area displays you a summary of previous synchronization processes.

9.2. Passcode Authentication

The **Passcode Authentication** interface allows to specify the settings for sending the alert message to the unknown sender for Challenge/Response in order to authenticate the sender. Click on the Passcode Authentication tab in Advanced settings interface to access Passcode authentication interface.



AntiSpam Alert (ASA) Messages

This setting controls how the ASA Messages are sent. Here you have the options to send individual ASA messages in response to each incoming message from an unknown sender or to send one ASA message to multiple senders.

For example, if you get several mails and AntiSpam finds 20 messages from unknown senders, you can have AntiSpam either send an individual ASA message to each of the 20 unknown senders or you can have AntiSpam send a single ASA message to all the 20 senders.

Note: Each of the 20 (combined) recipients cannot see who the other recipients are (this is called Blind Carbon Copying or BCC).

Send Alert attempt times: This setting controls how many times a sender is allowed to attempt passcode authentication. The default is 3. You can change the number as you wish from the drop-down.

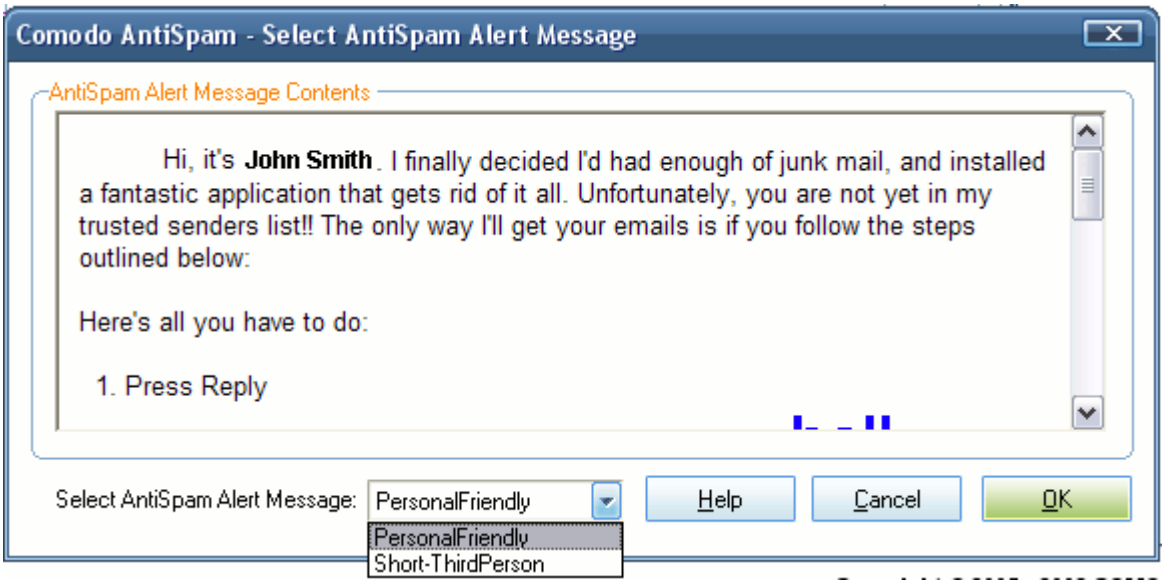
Note: AntiSpam Alert messages are sent to senders of email who are unknown to you.

Send Auto-Authorized notice once to imported addresses

This setting controls AntiSpam to sends an **Auto-Authorized** message to the sender, in response to the first email from sender whom you have imported into your Authentication Database from your email application.

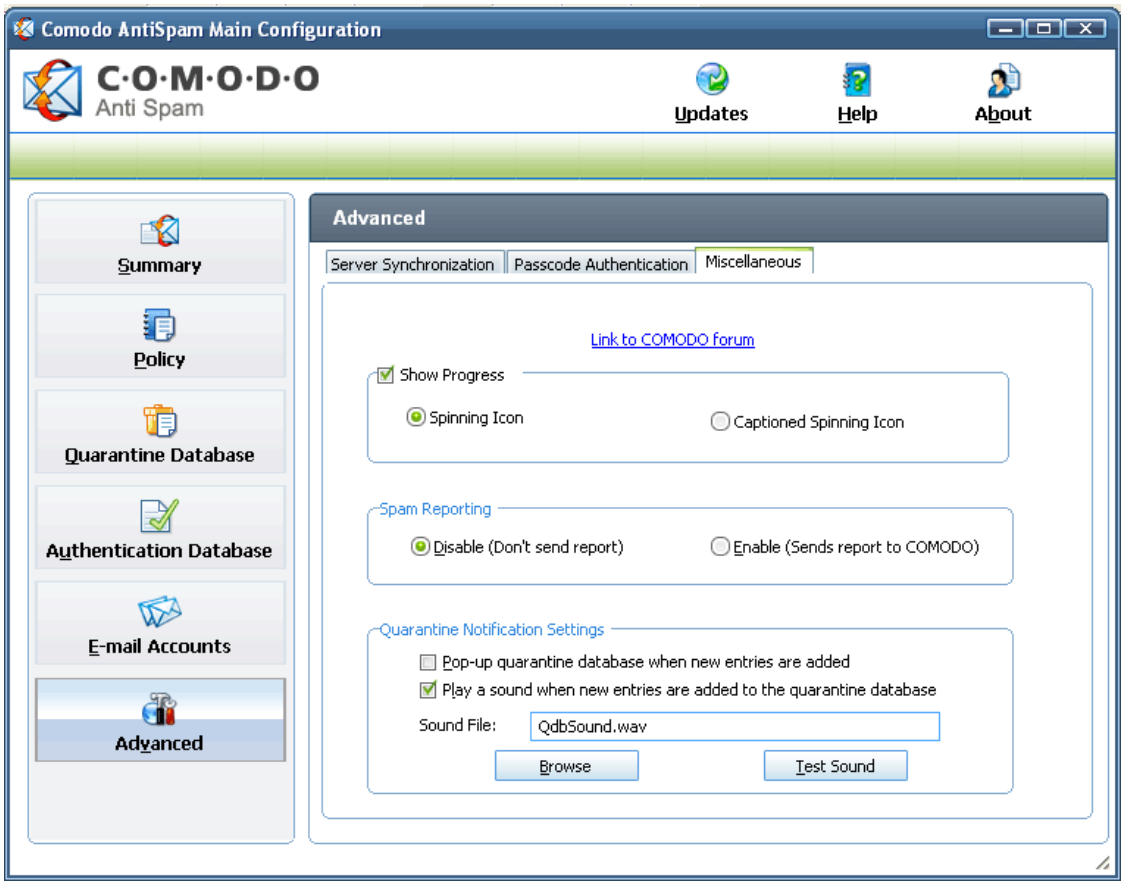
Select Alternate ASA Message

If enabled, you can select Alternate ASA Message from the suggested variants.



9.3. Miscellaneous

The Miscellaneous settings interface allows you to specify overall configurations for Comodo AntiSpam. Click on Miscellaneous tab in Advanced Settings interface to access Miscellaneous settings interface.



Link to Comodo Forum - Clicking this link leads you to AntiSpam area of Comodo Forum. You can post your questions regarding Comodo AntiSpam at the Comodo community user forum and get an answer immediately. Once registered, you'll join thousands of other users discussing all aspects of our products.

You'll benefit from the expert contributions of developers and fellow users alike and will find answers to any questions you may have. **Register at Comodo Forums Now**.

Show Progress

Checking this check box turns on the progress indicator. The progress indicator is displayed when AntiSpam is busy retrieving and authenticating your email. You have the choice of a Spinning Icon or if your operating system is Windows XP you will have and additional selection of Captioned Spinning Icon. Spinning Icon progress simply animates (spins) the AntiSpam icon running in the system tray if you hover your mouse over the spinning icon a progress caption will appear. Captioned Spinning Icon displays a progress caption during the entire time AntiSpam is processing.

Spam Reporting

If the **Spam Reporting** is enabled, Comodo AntiSpam can automatically report spam to Comodo. When AntiSpam receives any mail from an unknown sender, it stores the mail in the **Quarantine database** in the **Pending Authentication** state. It sends an AntiSpam Alert mail to that sender. If the Alert mail bounces then AntiSpam checks it against the Spam mail characteristics. If the bounced mail meets these characteristics then a spam reporting mail will be sent to Comodo with the following details:

- AntiSpam user name;
- AntiSpam email address;
- Unknown Sender's email address; and
- Unknown Sender's emails as an attachment.

Note: AntiSpam will not add the sender's email address into the Authentication Database with Blocked state.

Note: For each reported address, AntiSpam will not perform Spam reporting again.

- Select **Enable (Sends report to COMODO)** option to enable automatic Spam Reporting capability; or
- Select **Disable (Don't send report)** option to disable automatic Spam Reporting capability.

Note: By default, the Enable (Sends report to COMODO) option will be enabled.

Quarantine Notification Settings

Pop-up quarantine database when new entries are added to the QDB - Enabling this feature causes a pop-up display of the Quarantine Database (QDB), when new messages (from unknown senders) are added to it.

Play a sound when new entries are added to the quarantine database - Enabling this features produces an audible alert when new entries are added to the QDB. You can select any .wav file to be played, by clicking the Browse button and navigating to the .wav file you wish to set.

About Comodo

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

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

Comodo Security Solutions, Inc.

525 Washington Blvd. Jersey City,

NJ 07310

United States

Tel: +1.888.256.2608

Tel: +1.703.637.9361

Email: **EnterpriseSolutions@Comodo.com**

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

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