

**C·O·M·O·D·O**

™

Creating Trust Online

Comodo SecureEmail

**User Guide**

## Table of Contents

<b>1 Introduction To SecureEmail.....</b>	<b>4</b>
1.1 System Requirements.....	4
<b>2 Installing SecureEmail.....</b>	<b>7</b>
<b>3 Certificate Sign Up Wizard.....</b>	<b>11</b>
3.1 Starting Certificate Sign-up Wizard.....	11
3.2 Automatic Installation.....	16
3.3 Installation Via Collection Email.....	17
<b>4 Sending and Receiving Encrypted Mail.....</b>	<b>19</b>
4.1 Sending Encrypted Email Messages.....	19
4.2 Receiving Messages Encrypted with a Single-Use Certificate.....	19
4.3 Install Comodo SecureEmail to Decrypt and Read the Message.....	20
4.4 Decrypt and Read the Message Using Comodo's Secure Web Reader Service.....	21
<b>5 Purchase Commercial Email Certificates.....</b>	<b>23</b>
5.1 Purchasing the Certificates Using the E-PKI Manager.....	23
<b>6 Configuring SecureEmail.....</b>	<b>29</b>
6.1 Summary.....	29
6.2 Security Settings.....	31
6.2.1 Default Level Settings.....	32
6.2.2 Custom Level Settings.....	35
6.3 Certificate Update Emails.....	46
6.4 Certificate Settings.....	48
6.5 Protocols.....	54
6.5.1 Configuring SecureEmail for SSL connections.....	60
6.6 Email Folders Scanning.....	65
6.7 General.....	66
<b>7 Repairing SecureEmail.....</b>	<b>69</b>
<b>8 Uninstalling SecureEmail.....</b>	<b>72</b>
<b>FAQ.....</b>	<b>75</b>
<b>Glossary.....</b>	<b>84</b>
<b>Appendix 1 - Comodo ePKI Manager – Overview.....</b>	<b>94</b>

**Appendix 2 - Notes on 32 bit/64 bit Editions..... 98**

**Appendix 3 - Default Security Profiles..... 100**

## 1 Introduction To SecureEmail

Unsecured email messages are rather like sending a postcard written in pencil – they can be intercepted, read or edited by anyone along the way. To avoid this, every message sent should be encrypted and signed using a digital certificate. Unfortunately, the concepts and the steps involved with setting up such a system are often difficult to understand and implement. Not only does a user have to find a trusted CA and sign-up for a certificate - they also need to understand complexities such as creating a certificate request; how to import the certificate into Windows and finally how to configure their mail client to use this certificate.

That's why Comodo developed SecureEmail, the install-and-forget PKI based application that can automatically encrypt and sign all your outgoing messages. Featuring full compatibility with Outlook, Thunderbird and other major mail clients, it features a built-in wizard that allows users to easily download then setup a Comodo email certificate. Users will benefit from the security of automatic encryption and signing of their email while the application handles

difficult or hard to remember processes such as public-key exchange. Network administrators looking to implement total client-to-client email security may consider Comodo SecureEmail as a complement to gateway encryption applications which overlook the vulnerability of emails being exchanged within the network.



### 1.1 System Requirements

<b>Comodo SecureEmail - 32 bit version:</b>	<b>Comodo SecureEmail - 64 bit Version:</b>
<p><b>Operating Systems</b> Windows Vista 32 bit Windows XP (SP2) 32 bit Windows 2000 (SP4)</p> <p>64 MB RAM 20 MB Hard Disk Space</p>	<p><b>Operating Systems</b> Windows Vista 64 bit Windows XP (SP2) 64 bit</p> <p>64 MB RAM 30 MB Hard Disk Space</p>

#### Supported Email Clients:

- Outlook 2000 and above
- Outlook Express 5/5 and above
- Thunderbird 1.5 and above
- Windows Mail
- Incredimail
- Windows Live Mail
- Eudora

**NOTE:** This list of supported clients are those that SecureEmail is confirmed to support. Because it is positioned at the network layer, SecureEmail **should** work with all POP/SMTP/IMAP clients. For more details, see this [FAQ](#).

This guide is intended to take the user through the installation, configuration and use of Comodo SecureEmail and Comodo SecureEmail Pro.

['Installing SecureEmail'](#) - A brief outline of the installation procedure.

['Certificate Sign Up Wizard'](#) - Guidance on how to apply for and install a Comodo Email Certificate.

[Purchase Commercial Email Certificates](#) – Guidance on how to apply for and install a Comodo Email Certificate for use in corporate environment.

['Sending and Receiving Encrypted Mail'](#) - A brief overview of the application in operation.

['Configuring SecureEmail'](#) - Detailed help on every category of configuration, including:

- [Summary](#)
- [Security Settings](#)
- [Certificate Update Emails](#)
- [Certificates](#)
- [Protocols](#)
- [Email Folder Scanning](#)
- [General](#)

[Repairing SecureEmail](#) - A brief outline of the procedure of repairing SecureEmail installed in your system.

[Uninstalling SecureEmail](#) - A brief outline of the procedure of uninstalling SecureEmail installed in your system.

This guide also contains the following sections to enrich your knowledge on SecureEmail.

[FAQ](#) - At the back of this guide which contains answers to the most commonly asked questions.

[Appendix 1 Comodo EPKI Manager – Overview](#)

[Appendix 2 Notes on 32 bit and 64 bit editions](#)

[Appendix 3 Default Security Profiles of Comodo SecureEmail](#)

## **'Home' Edition VS Pro Edition**

There are two versions of the application, one for home and personal use and one for corporate use (Comodo SecureEmail Pro).

The only functional difference between the two is that the Pro version can be configured to encrypt and decrypt messages using certificates from *any* vendor whereas the Home version can only encrypt/decrypt using a Comodo email certificate.

### **Home and Personal Users:**

- Before you can begin using SecureEmail to sign and encrypt your mail, you need to install a [free Comodo email certificate](#).

- If you want to use a non-Comodo/3rd party email certificate to encrypt and decrypt your mails(e.g. Thawte, Verisign) , then you need to download and install SecureEmail Pro.

#### **Corporate users:**

- If you wish to use SecureEmail to sign and encrypt mail in a corporate environment then you need to sign up for an [E-PKI account](#) to purchase Comodo Corporate Email Certificates (starting from as little as \$7.20 per year) .
- If you want to use a non-Comodo/3rd party email certificate to encrypt and decrypt your mails(e.g. Thawte, Verisign) , then you need to download and install SecureEmail Pro.

**Note:** Both versions of SecureEmail require a Comodo certificate to **digitally sign** mail. If you wish to use a non-Comodo certificate as your encryption certificate alongside a Comodo signing certificate then you need to install SecureEmail Pro.

#### **Support**

The fastest way to get further assistance on Comodo SecureEmail is by joining Comodo Forums, a message board exclusively created for our users to discuss anything related to our products.

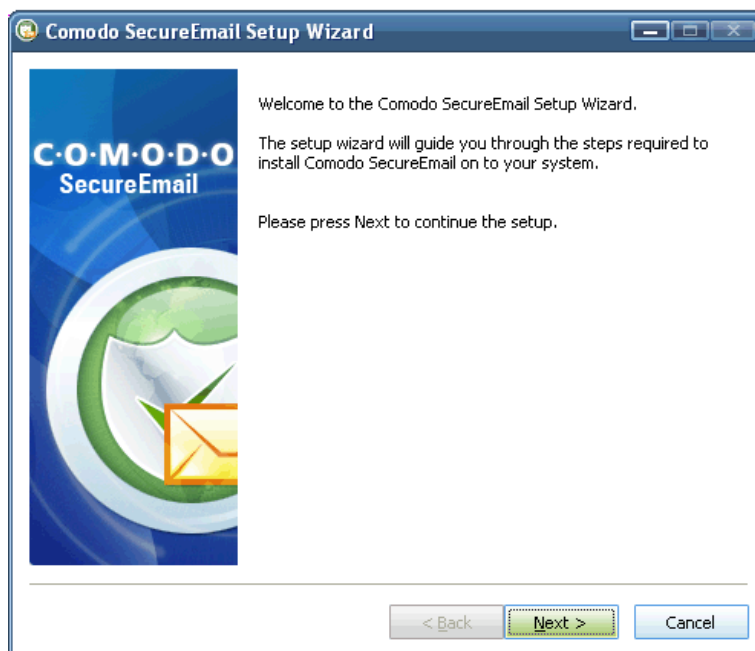
You'll benefit from the expert contributions of developers and fellow users alike and we'd love to hear your thoughts and suggestions.

Register free at <http://forums.comodo.com>.

## 2 Installing SecureEmail

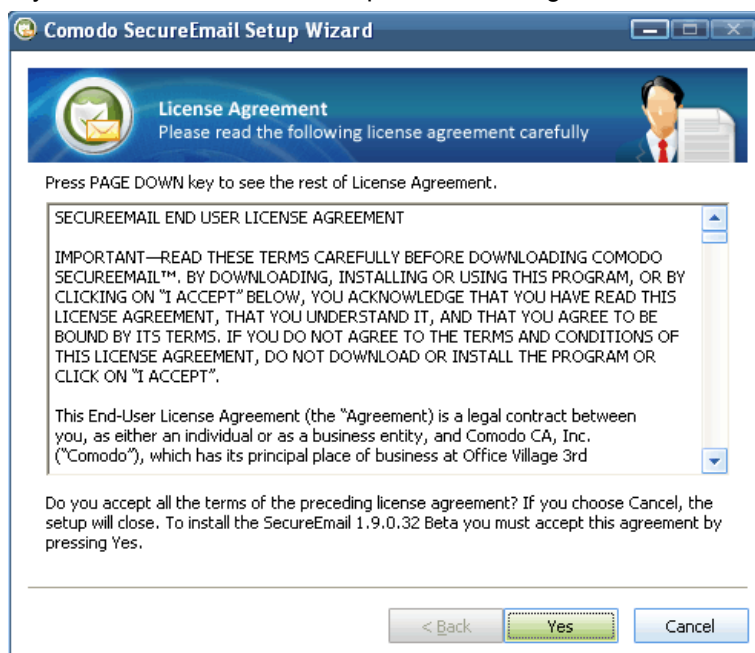
After downloading the Comodo SecureEmail setup file to your local hard drive, double click on Setup.exe to start the installation wizard.

If you already have Comodo SecureEmail installed in your system, clicking the setup.exe starts the repair/uninstall wizard. Refer [Repairing SecureEmail](#) for more details.



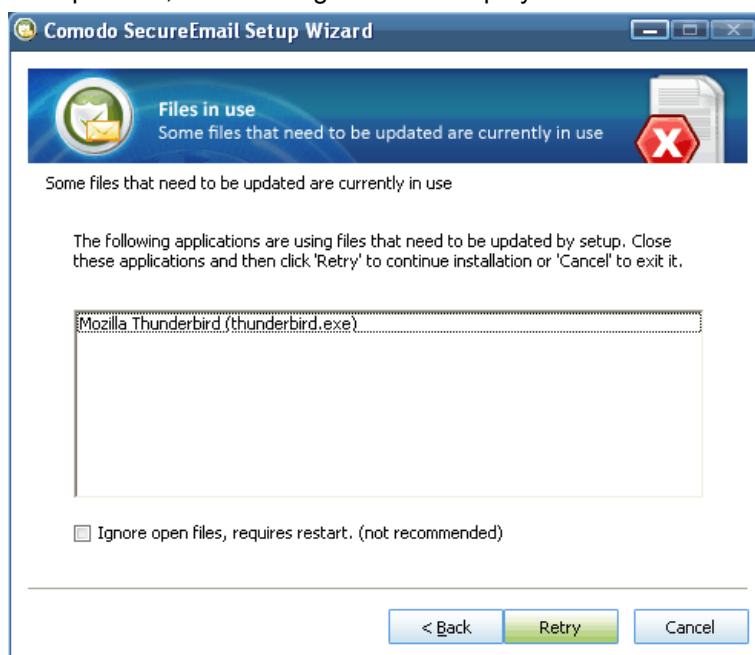
### End User License Agreement

In order to finalize installation, you must first read and accept the license agreement:



Click 'Yes' to accept and continue installation. Click 'Cancel' to decline and exit the installation.

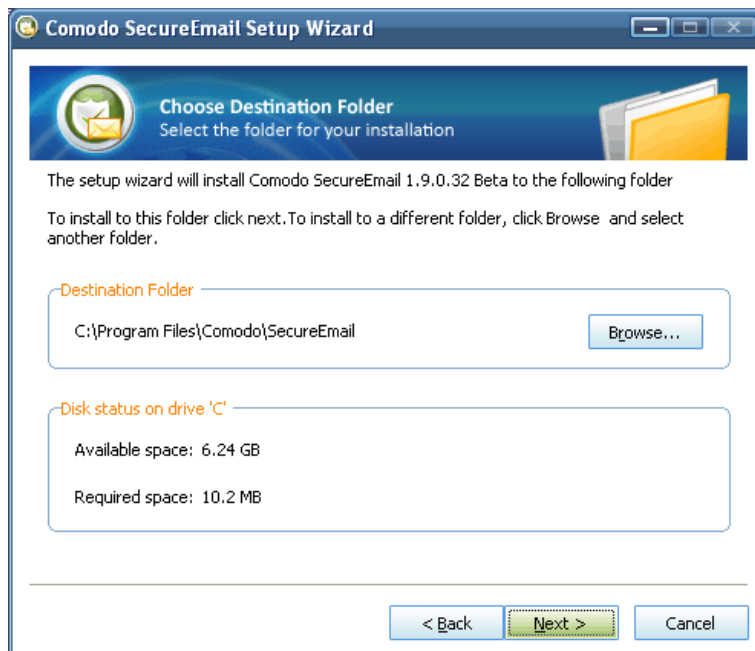
Please ensure that all other Windows programs are closed before continuing with the installation. If you have your mail client open during this installation process, the following screen is displayed.



Close your email client and click Retry.

**Note:** If you do not have your email client open, this dialog is not displayed and the installation moves to the next step.

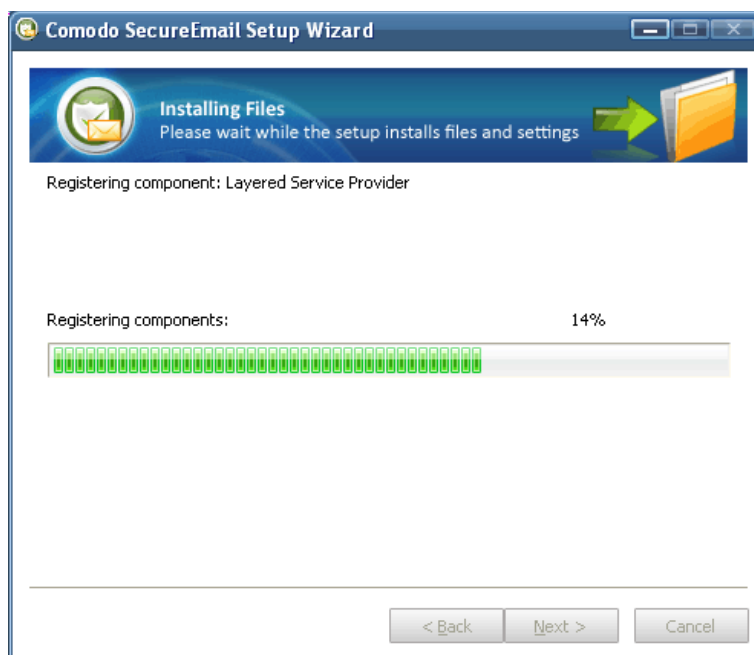
### Selecting Destination Folder



By default, Comodo SecureEmail is installed to C:\Program Files\Comodo\SecureEmail. To install to a different directory, click BROWSE. Navigate to the folder where you want to install Comodo SecureEmail, click open and click 'Next' to continue.

### Set-up Progress

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



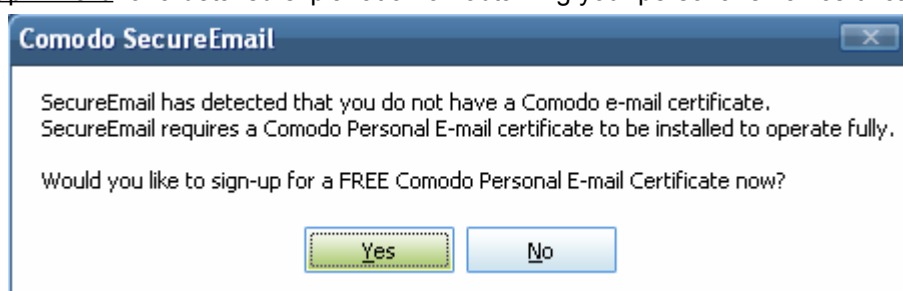
If installation fails for some reason, an appropriate message box is displayed followed by Rollback wizard page, showing rollback progress, followed by one more final wizard page.

### Certificate Sign-up Notification

If you are installing Comodo SecureEmail for the first time, you will be prompted for signing-up for free email certificate from Comodo during the progress of installation.

This certificate will be used to sign your outgoing mails and to decrypt your incoming mails using your private key. Signing the mail ensures authenticity and integrity and encrypting the mail ensures privacy. You can sign-up for this free email certificate at this moment or you can sign-up later.

See [Certificate Sign Up Wizard](#) for a detailed explanation on obtaining your personal email certificate.



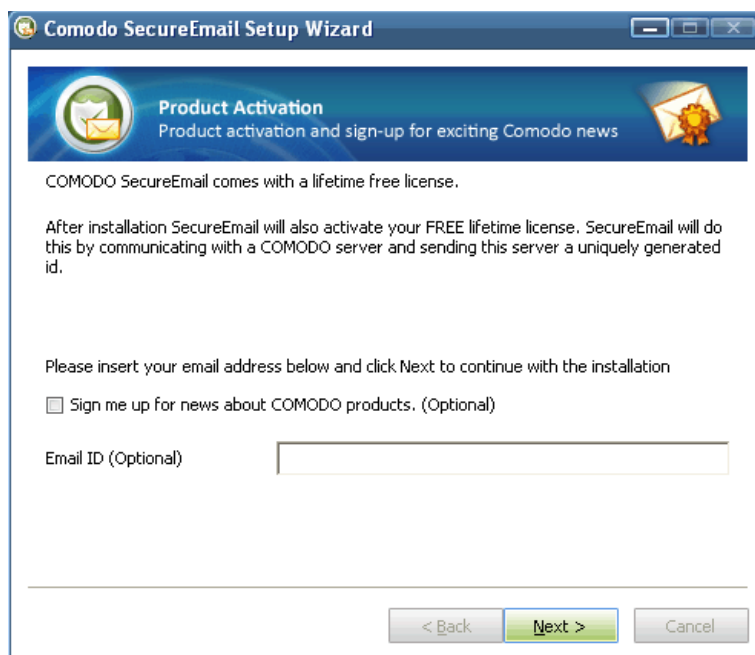
Click Yes, if you wish to sign-up for your certificate now or NO to sign-up later. The installation process will continue.

**Note:** If you already have your email certificate installed in your system, this dialog is not displayed and the installation moves to the next step.

### Product Activation

If you wish to sign up for news about Comodo products then enter your email address in the space provided.

Click 'Next' to finalize the installation wizard.



### Installation Complete and Restart

A confirmation dialog box will be displayed indicating successful completion and telling you that you should restart your system so that the updates can take effect. Please save any unsaved data and click Finish. If you wish to restart later, uncheck the box before clicking 'Finish'.

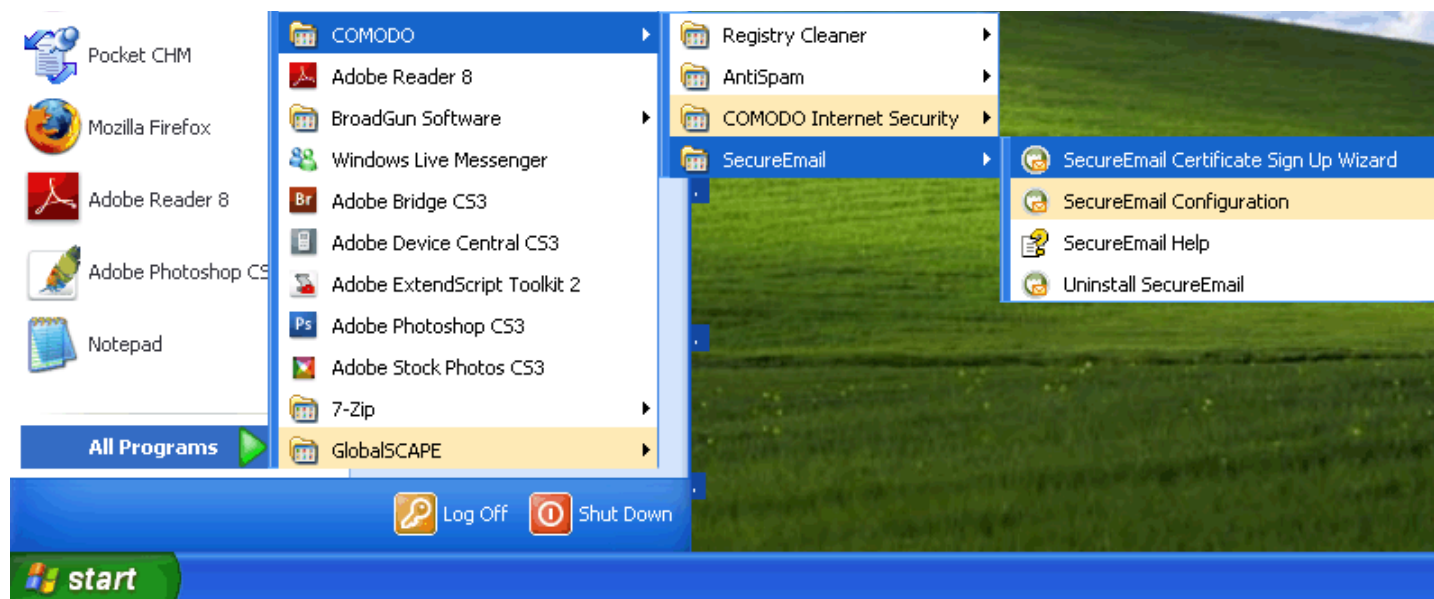


## 3 Certificate Sign Up Wizard

If you want to use SecureEmail to encrypt and sign emails then the first thing you need is a digital email certificate.

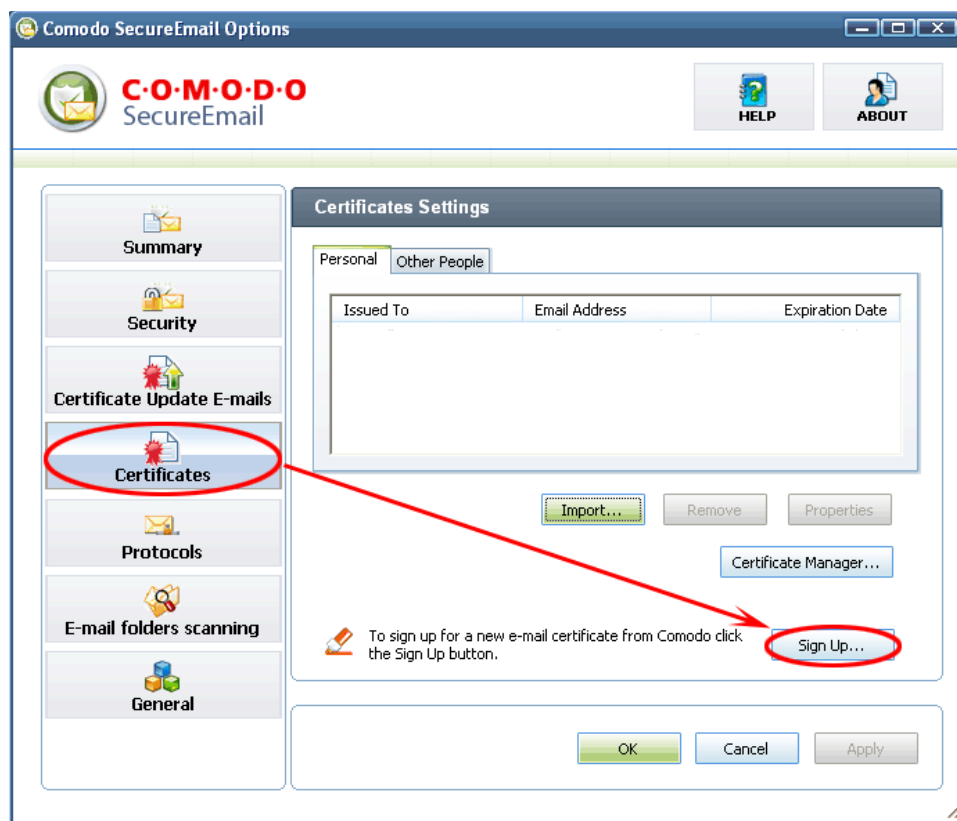
### 3.1 Starting Certificate Sign-up Wizard

At the Windows start menu, click: Start - Programs - Comodo - SecureEmail.

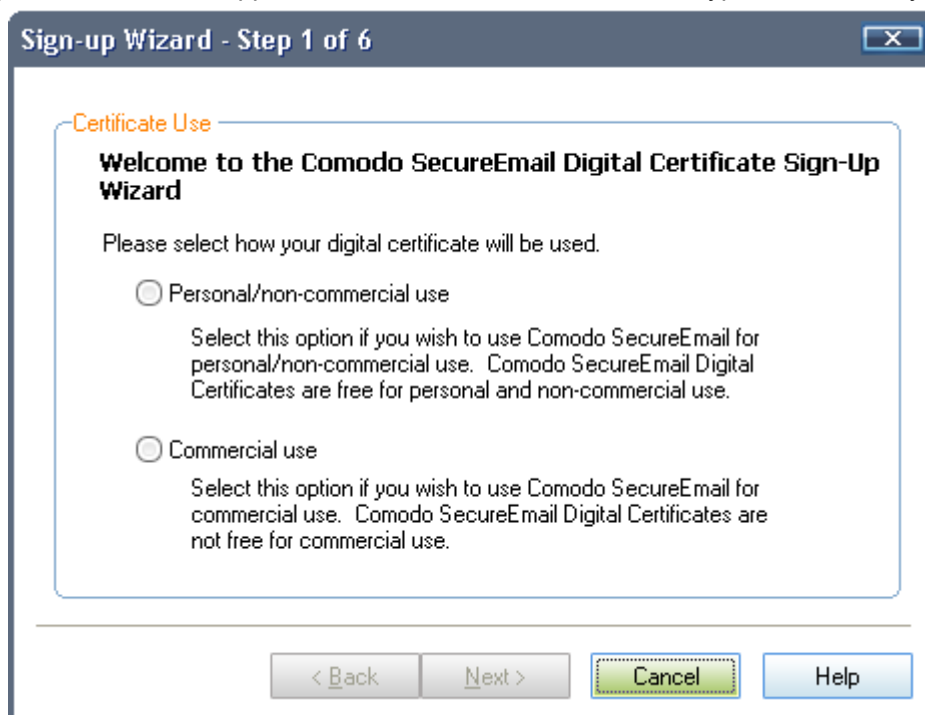


The wizard can now be accessed using two methods:

- By simply choosing 'SecureEmail Certificate Sign Up Wizard' (shown above). In which case you will go straight into the ordering process.
- Via the SecureEmail interface by clicking 'SecureEmail Configuration' (see graphic below). You then need to click the 'Certificates' button followed by 'Sign Up' . Once again, this will start the ordering process



1. The first stage of the certificate application wizard is to determine which type of certificate you require.



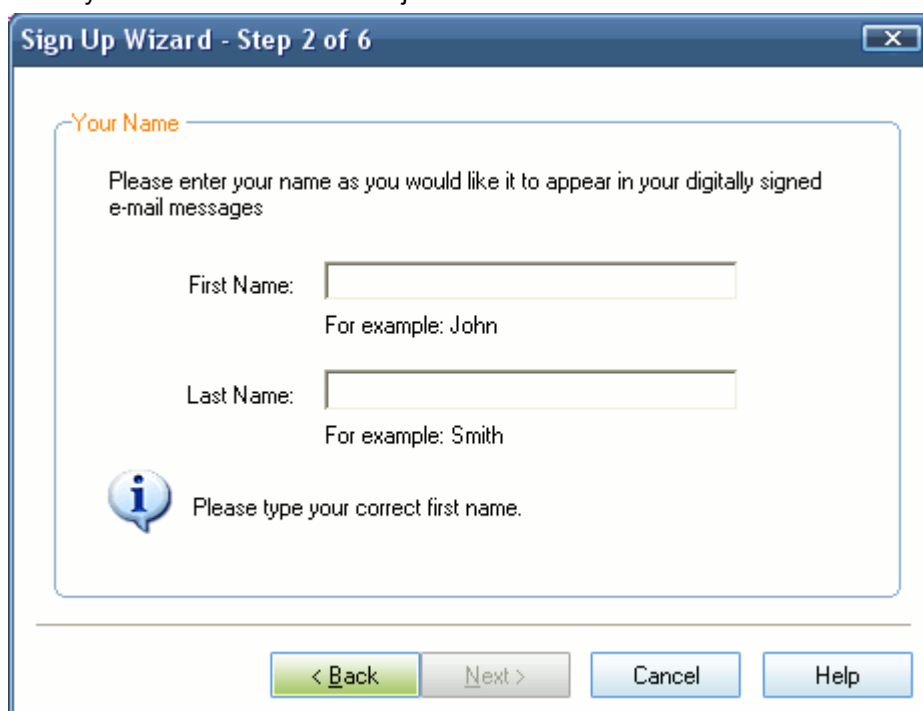
- **Personal/non-commercial use** - select this option if you are a home user and require a free Comodo Email certificate. Applications for free email certificates are carried out entirely within the SecureEmail interface. Users choosing this option will continue straight onto Step 2 of the wizard

- **Commercial use** - Select this option if you wish to use the application with Comodo Corporate Email certificates.

Unlike free certificates, Corporate certificates are applied for and issued using the Comodo E-PKI interface.

- An overview of the functionality of the E-PKI manager can be found in the appendix to this help guide [here](#).
- A guide to applying for a corporate email certificate using the E-PKI management interface can also be found in this guide in the section [Purchase Commercial Email Certificates](#)
- Selecting the 'Commercial Use' option takes you to the corporate landing page at <http://secure-email.comodo.com/corporate.html> where you can sign up for an E-PKI account or find out more details. Existing E-PKI account holders can also log into their accounts from this page.
- If you wish to purchase and use corporate certificates, but currently have the Home version of SecureEmail installed, then we recommend you *also* take the opportunity to download and install the Pro version whilst at <http://secure-email.comodo.com/corporate.html>. The Pro version offers greater flexibility to business users because it supports the use of non-Comodo certificates for the purposes of encryption/decryption. This can be particularly beneficial to organizations and users that already have (or expect to receive) email certificates from a wider range of certificate vendors (for example, Thawte or Verisign email certificates). Note -You must have a Comodo certificate installed to Digitally Sign emails using either Comodo SecureEmail Pro or Home.
- Although the application process differs depending on whether you want a commercial or free certificate, the certificate installation process is identical for both types. Once you have successfully applied for and purchased a corporate certificate using the steps outlined above you should skip to the last section on this page: [Completing The Certificate Installation](#).

2. Stages 2 and 3 are where we gather data that will be included in your email certificate. Firstly, you need to enter your first and last names and then click 'Next'. The name you enter here is the name that will be displayed as the 'Common Name' of your email certificates 'Subject' field.



3. Next, enter your email address.

This the address that your certificate will be issued for (it will form the 'Email Address' of your certificate's 'Subject' field). It is also the address we will deliver your certificate to. After we deliver your certificate, you will be able to send secured emails for this address.

**Sign-up Wizard - Step 3 of 6**


**E-mail address:**

Your e-mail address is the address that Comodo CA will issue your e-mail certificate to. You can use the e-mail certificate to send secured e-mails for this address.

Note: You will need a certificate for each e-mail address you want to secure.

E-mail address:

For example: someone@comodo.com

 Please enter your valid e-mail address.

< Back   Next >   Cancel   Help

4. Please read the Subscriber Agreement. To accept and continue, click 'Next'. If you do not accept the agreement, click 'Cancel' to terminate the ordering process.

**Sign-up Wizard - Step 4 of 6**

**Subscriber Agreement**

Secure Email Certificate Subscriber Agreement:  
Digital Certificate Subscriber Agreement ('Agreement')

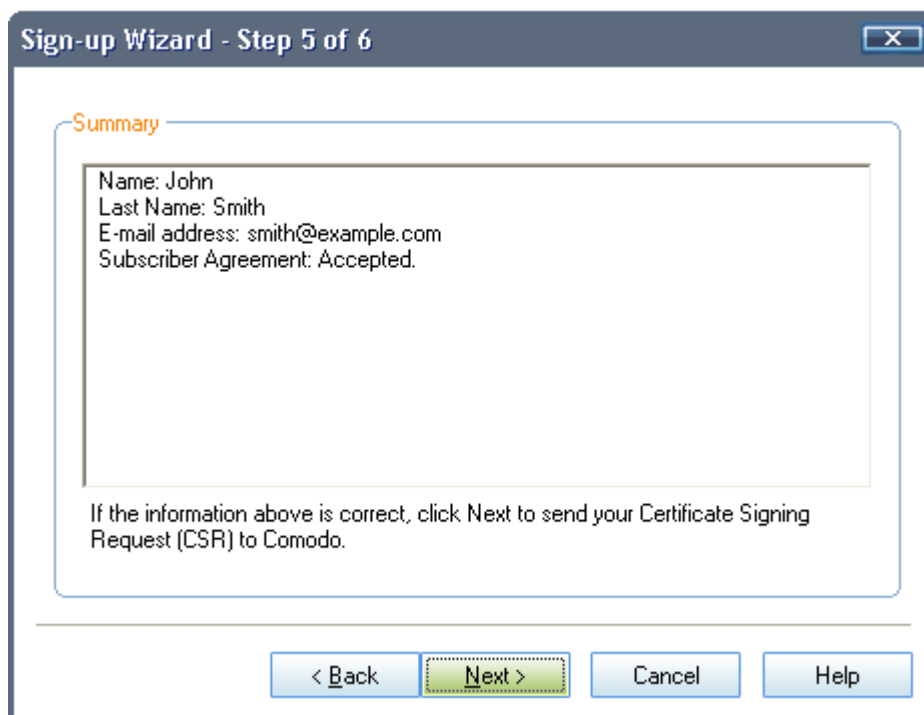
1 Application of Terms  
1.1 These terms and conditions and schedules thereto, set out below govern the relationship between you (the 'Subscriber') and Comodo Limited ('Comodo').

2 Definitions and Interpretations  
2.1 In this Agreement, unless the context requires otherwise, the following terms and expressions shall have the following meanings:  
'Business Day' means Monday to Friday inclusive excluding any days on which the banks in London are closed for business (other than for trading in Euros);  
'Certificate Period' means the time period during which a Digital Certificate remains valid and may be used as set out in the Schedule;

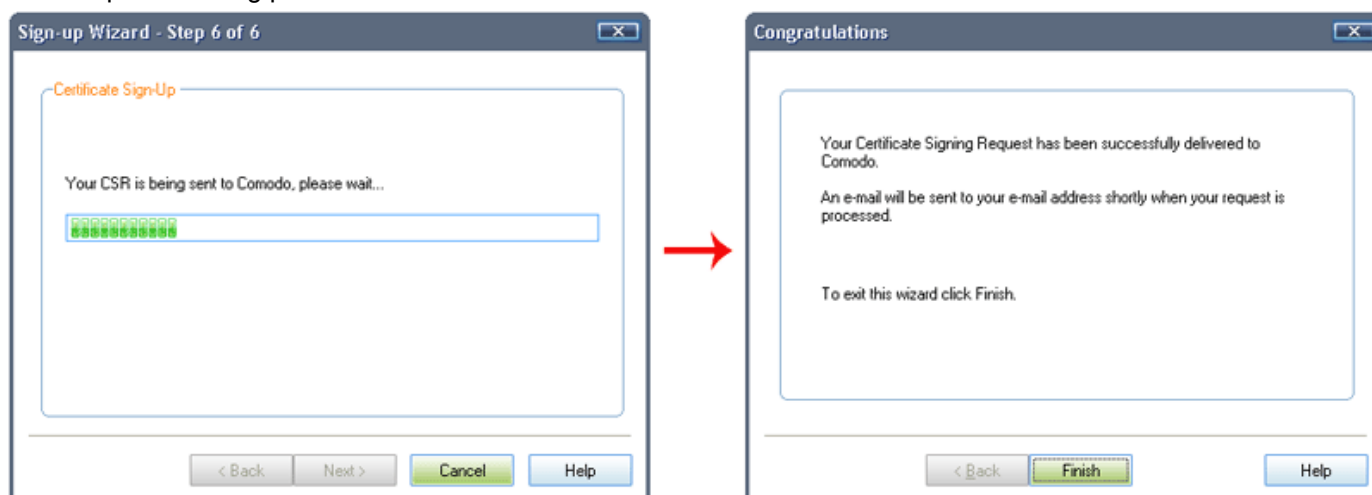
I accept the terms of the subscriber agreement

< Back   Next >   Cancel   Help

- Step 5 is a summary of the data you have provided so far. These are the details that will be used to generate the certificate signing request (CSR) that will provision your free certificate. Please check that they are correct before clicking 'Next'.



- The final stage is the actual submission of your certificate signing request to the Comodo servers. After successfully completing the submission procedure, you will see a confirmation screen informing you that your request is being processed.



## Completing the Installation of Your Certificate

There are two possible routes that can be taken to install your certificate:

- Automatic Installation** - In the majority of cases your certificate will be detected and automatically installed by Comodo SecureEmail within minutes.

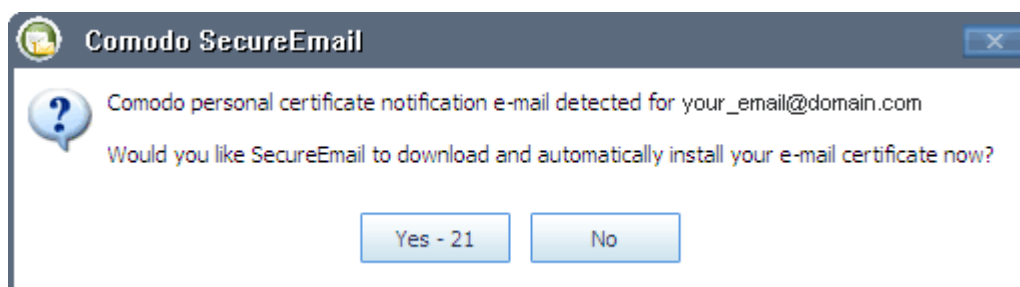
NOTE: Your certificate will be detected and automatically installed by Comodo SecureEmail ONLY IF your email client is running.

2) **Installation Via notification Email** - if you don't yet have SecureEmail installed or for some reason missed the automated installed process then Comodo will send you a notification email explaining how to collect and install your certificate.

### 3.2 Automatic Installation

---

Firstly, SecureEmail will detect the certificate notification email and alert you with the following message:



After verifying that the email address displayed is the same as the one you specified in [step 3](#), you should click 'Yes'. *(If you click 'No' then you abort the automatic installation. However, a notification mail will still be sent to the email address specified - allowing you to install at a later time.)*

### 3.3 Installation Via Collection Email

**C·O·M·O·D·O**  
Creating Trust Online™

Tel Sales : [+1 888 266 6361](tel:+18882666361)  
Fax Sales : [+1.201.963.9003](tel:+12019639003)

---

Dear [Your First Name and Last Name](#)

**Congratulations** - Your Comodo FREE Personal Secure Email Certificate is now ready for collection! You are almost able to send secure email!

Simply click on the button below to collect your certificate.

[Click & Install Comodo Email Certificate](#)

**Note:-** If the above button does not work, please navigate to [http://secure-email.comodo.com/collect/CSESecureEmailCertificate\\_Collec2.html](http://secure-email.comodo.com/collect/CSESecureEmailCertificate_Collec2.html)

Then enter the Collection Password which is:

**X x X x X x X x X x X**

Your Comodo FREE Personal Secure Email Certificate will then be automatically placed into the Certificate store on your computer.

Click "Yes" if you see a "Potential Scripting Violation" window asking "Do you want this Program to add Certificates now?"

**Note:-** We strongly recommend that you export your certificate to a safe place in case you need to reload it later. For details, please see [http://www.instantssl.com/ssl-certificate-support/server\\_faq/ssl-email-certificate-faq.html](http://www.instantssl.com/ssl-certificate-support/server_faq/ssl-email-certificate-faq.html).

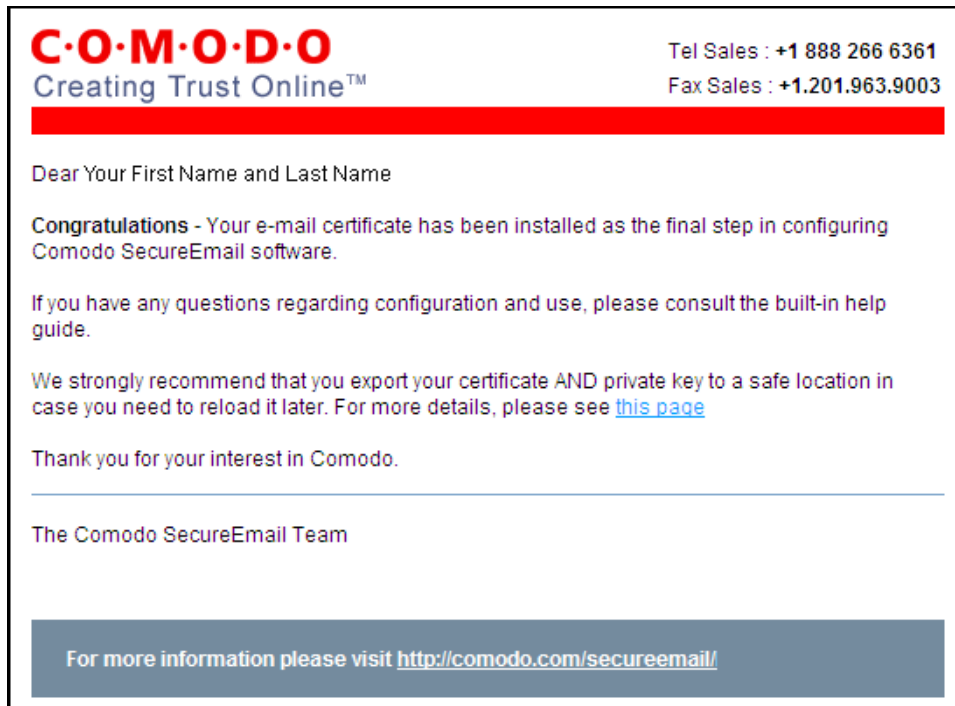
Setup and configuration of the application of SecureEmail are covered in the built-in help guide. If further assistance is required, users are encouraged post questions on our community forums at <http://forums.comodo.com> or to submit a support ticket at <http://support.comodo.com>

Thanks for doing your part to help make the online world more trusted and verified.

If you chose 'No' at the Automatic Installation prompt then you will shortly receive a notification mail containing details on how to 'manually' collect and install your certificate:

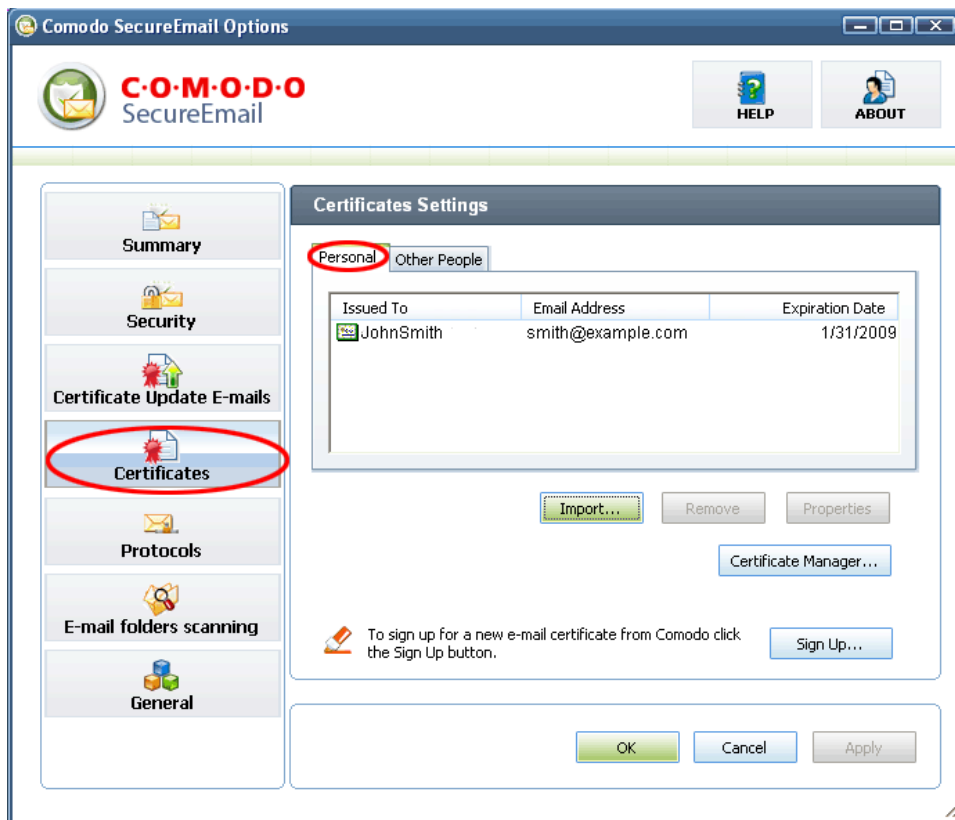
- Selecting 'Click and Install Comodo Email Certificate' will automatically fetch and install your certificate from the Comodo servers.
- Alternatively, navigate to [http://secure-email.comodo.com/collect/CSESecureEmailCertificate\\_Collec2.html](http://secure-email.comodo.com/collect/CSESecureEmailCertificate_Collec2.html) and enter your email address and the collection password to manually download your certificate.
- The collection email that is sent to Corporate Email customers is cosmetically different but functionally identical to the email shown above.

Once your certificate has been installed, you will receive a confirmation email.



Your certificate appears in the list of certificates in 'Certificates' tab of SecureEmail program. SecureEmail can now use this certificate to encrypt and digitally sign your emails.

**NEXT:** All users are now advised to familiarize themselves with the configuration and usage of the application. If you want to use SecureEmail to encrypt and sign emails then the first thing you need is a digital email certificate.



## 4 Sending and Receiving Encrypted Mail

---

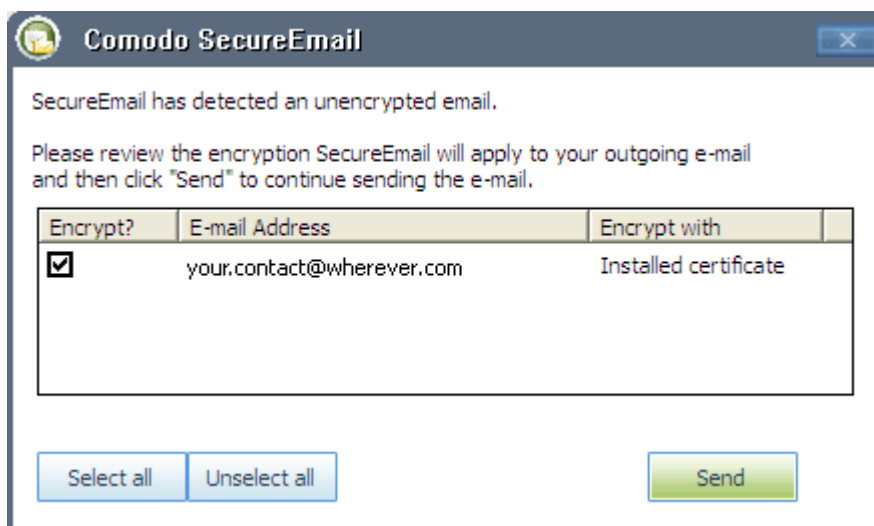
### 4.1 Sending Encrypted Email Messages

---

SecureEmail can encrypt emails for a recipient whether or not their certificate is installed on your system (subject to your [preferences](#).)

If you encrypted the email using your contact's 'regular' email certificate, then their client will automatically decrypt it. If, however, you do not have your contact's certificate, SecureEmail can generate a single-use certificate to encrypt the email. Emails encrypted with a single use certificate are attached to a non-encrypted email containing instructions of where to download SecureEmail to decrypt the attachment. The single use certificate is simultaneously uploaded to the SecureEmail Server so that your recipient can download it to decrypt the message.

SecureEmail can be configured to automatically encrypt and digitally sign all outgoing emails. Alternatively, you can configure it to prompt you if it detects that you are trying to send out an unencrypted mail (as shown below)



- For an outline of available encryption and Digital Signing options, see [Security Settings](#).
- For an outline of the recipient's experience and the choices available to them, see [Receiving Encrypted Messages](#).

### 4.2 Receiving Messages Encrypted with a Single-Use Certificate

---

As outlined in the [Security Settings](#) section of this guide, SecureEmail allows you to encrypt messages using a contact's email certificate or with a 'Single Use' certificate. This section deals with your contact's experience upon receipt of a message encrypted with such a single use certificate.

Firstly, they will receive a notification email similar to one shown below:

TEst [Inbox](#)

☆ [J.Smith](#) to me

[show details](#) 5:05 pm (0 minutes ago) [Reply](#)

**C.O.M.O.D.O**  
Creating Trust Online™

Tel Sales : +1 888 266 6361

Fax Sales : +1.201.963.9003

Dear [test@comodo.com](mailto:test@comodo.com)

You have been sent a **secure e-mail** message from [J. Smith](#) with the subject:

**Subject: TEst**

You can reach [J. Smith](#) by replying directly to this e-mail message.

If you are unsure about how to access this message, please read the information below.

**This e-mail has been secured using the Comodo Secure E-Mail Service.**

Secure e-mail messages differ from typical e-mail messages in that their contents are encrypted and therefore much more secure. In order to read a secure e-mail message you must first decrypt it. Comodo offers you two options for doing this.

- If you are using just about any e-mail software package for Microsoft Windows and are likely to be receiving more secure e-mail messages from [J. Smith](#) or other senders, you should download and install (at no cost) your own version of Comodo Secure E-Mail. [Click here for more information](#) or to download Comodo Secure E-Mail
- If you are using web-based e-mail or a non-Windows operating system for e-mail, you can view your message on a secure website designed expressly for this purpose. Simply forward this e-mail to [secure-read@secure-email.comodo.com](mailto:secure-read@secure-email.comodo.com) and you will receive a return e-mail that provides access to that website. There is no cost for accessing this website.

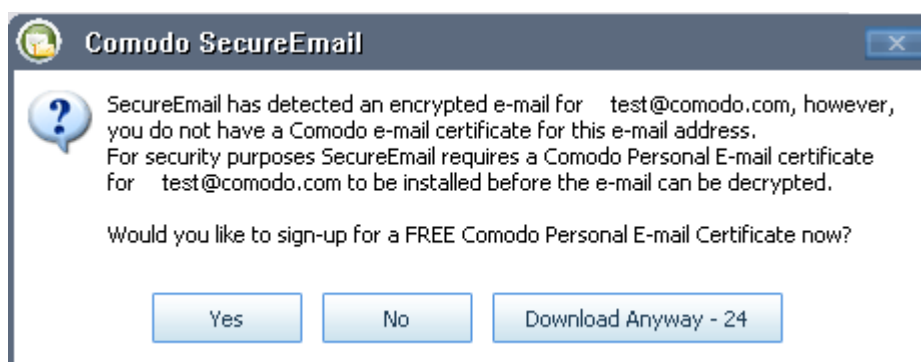
For more information please visit <http://www.secure-email.comodo.com>

The body of this mail explains that they have two main options for decrypting and reading the message:

- [Install Comodo SecureEmail to decrypt and read the message](#) (download links are provided)
- [Decrypt and read the message using Comodo's Secure Web Reader Service](#)

### 4.3 Install Comodo SecureEmail to Decrypt and Read the Message

Once the user has installed SecureEmail, it will prompt them to sign up for a Comodo email certificate (if they don't already have one). This is important as it is used by SSL client authentication to securely download the single-use-certificate to decrypt the email. (see graphic below)



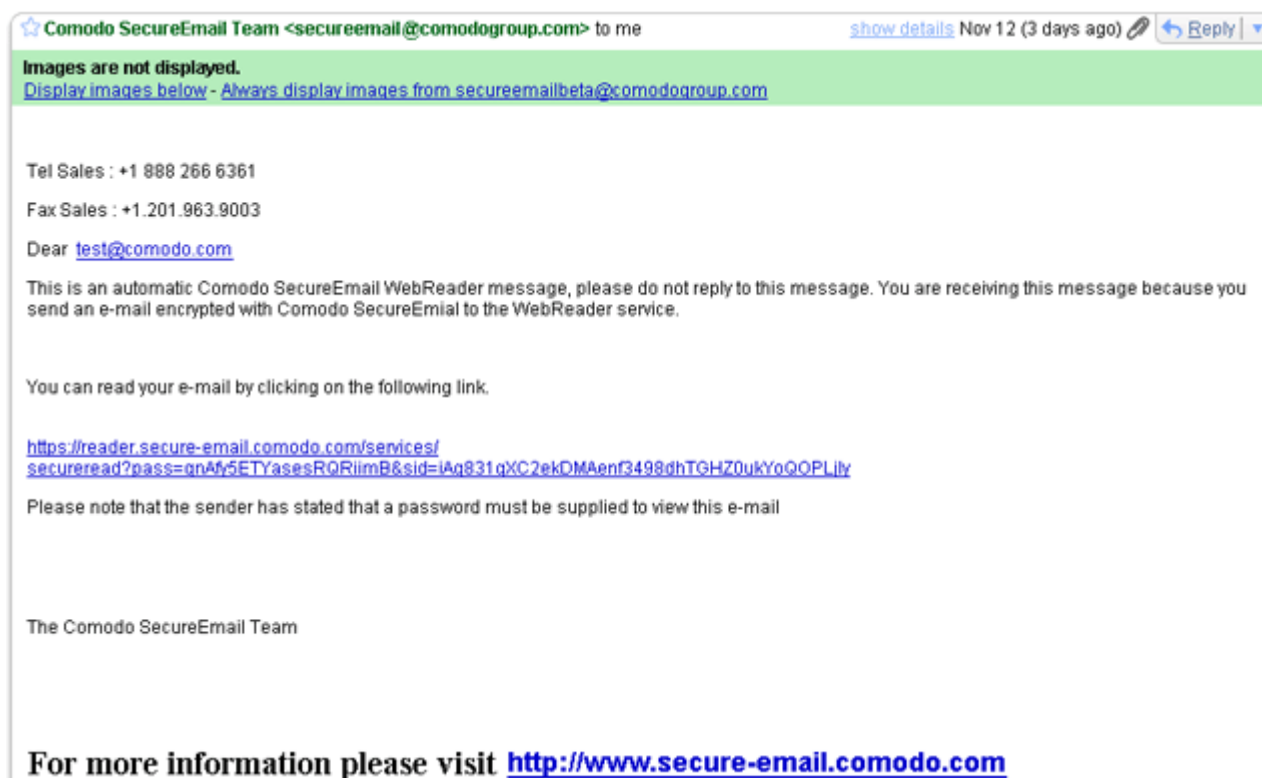
The Comodo server ensures this is a secure transaction by verifying that the certificate sent via this SSL client authentication has the same email address that the original email was sent to. The email will then be automatically

decrypted by SecureEmail and delivered back into your contact's inbox. SecureEmail will also send their new email certificate back to you by sending you a signed email. See [Certificate Update Emails](#) for more details on this process.

#### 4.4 Decrypt and Read the Message Using Comodo's Secure Web Reader Service

If your contact does not want to download and install SE then they have the option (if allowed in [encryption settings](#)) to use the Web Reader service. The process they will follow is:

- After receiving the [notification email](#) they simply need to forward it to **secure-read@secure-email.comodo.com**.
- After forwarding the mail, the server will send them another email message containing a link to our Web Reader service where they can securely view the message. (shown below)



- Your recipient clicks on the link to visit the Web Reader server which will decrypt the message and display it over a secure SSL connection. (see below)



SecureEmail: WebViewer

Delete

From: John Smith  
Sent: Tue Sep 04 04:59:58 -0400 2007  
To: test@comodo.com  
Subject: test



Signed by: John Smith

more

Hi,  
this is test encrypted message.

With best regards,  
John Smith

## 5 Purchase Commercial Email Certificates

---

If you wish to use SecureEmail to sign and encrypt mail in a corporate environment then you need to sign up for an [E-PKI account](#) to purchase Comodo Corporate Email Certificates (starting from as little as \$7.20 per year).

This page explains how E-PKI account holders can apply for , purchase and issue Comodo Corporate certificates using the E-PKI management interface.

### Background:

- To start the Comodo SecureEmail certificate sign up wizard, see the instructions [here](#).
- To begin the commercial certificate sign up process, select 'Commercial Use' at Step one of the wizard shown [here](#).
- To find out more about the features and benefit of Comodo E-PKI Manager, or [Appendix 1 of this guide](#) or visit the [Comodo Website](#)
- To open a new E-PKI account or to log into an existing account, [click here](#)

### 5.1 Purchasing the Certificates Using the E-PKI Manager

---

1. Existing E-PKI account holders and Comodo customers wishing to add E-PKI functionality to their accounts [should login here](#) (new customers should click the 'GO!' button' to begin enrollment)

## Enterprise PKI Manager (E-PKI) Area

### New Enterprise SSL Customers:

Click here if you have not previously purchased any Enterprise SSL products, or you have only purchased Enterprise SSL products on behalf of your clients.

**GO!**

---

### Existing Enterprise SSL Customers (including Existing E-PKI Account Holders):

Login below if you have previously purchased any Enterprise SSL products (excluding any orders placed on behalf of your clients) or you already have an Enterprise SSL E-PKI Account:

Username:

Password:

2. Once logged into the Comodo management system, select the "EPKI Manager" link. This will open the E-PKI management interface. On the left hand side, under 'Customer Order Options' is a list of purchasable products. Choose 'Corporate SecureEmail Certificate' (as shown below).

## Management

### My Account Summary:

Status	Active
Verification Level	Class 3

Options [▶Change Password](#)

Support [▶Buy FastTrack SSL Support](#)  
FastTrack SSL Support gives you your SSL order, including dedicated toll free).

### My Account Areas:

[Reseller](#) Manage customer orders placed

[Web Host Reseller](#) Place orders on behalf of customers through your Web Host Reseller Account

[E-PKI Manager](#) Place orders through your E-PKI Manager

[SSL Certificates](#) Manage your SSL certificates

[CVCs](#) Manage your Content Verification Certificates

[TrustLogos](#) Manage your TrustLogos

[IdAuthority](#) Add / Update details of your website(s) in the IdAuthority

- [GoldSSL Certificate](#)
- [PlatinumSSL Certificate](#)
- [PlatinumSSL Wildcard Certificate](#)
- [PlatinumSSL Legacy Certificate](#)
- [PlatinumSSL Legacy Wildcard Certificate](#)
- [PlatinumSSL SGC Certificate](#)
- [PlatinumSSL SGC Wildcard Certificate](#)

[Corporate Secure Email Certificate](#)

### Management Facilities:

[User Management](#)

### Reporting Facilities:

[Run report on your Orders](#)

Welcome:  
h@example.com  
Comodo CA

Account Options

Management

Logout

**SELECT E-PKI MANAGER**

**AND IN THE LIST OF THE CERTIFICATES  
CHOOSE 'CORPORATE SECURE EMAIL CERTIFICATE'**

- As the Administrator you will be make an application for a SecureEmail Certificate for your employees. You can only make such applications for domains Comodo have validated as owned by your business. Validation of your business and domain is a one-time event. After successful validation of domain ownership you can issue as many email certificates as you require to email addresses on that domain.

Following successful validation, the email certificate and application procedure is as follows:

- Administrator completes the certificate application form on behalf of the employee - providing employee name, email address and selecting the relevant security policies; (see '[Email certificate application and issuance procedure in detail](#)')
- Comodo then emails the employee with a link to begin the Certificate enrollment process – the enrollment for the Certificate must take place on the same PC on which the Certificate will be used;
- Comodo issue the Certificate which is automatically detected by and installed by the operating system on the employee's PC. If the employee has Comodo SecureEmail installed then the application will take over this aspect of the process and will place the employee's certificate in the appropriate certificate store.
- The employee is automatically redirected to the support pages for configuration and usage instructions. If the employee has Comodo SecureEmail installed then they should be instructed to consult this help guide instead.

The remainder of this page outlines this procedure in more detail.

#### 4. Email certificate application and issuance procedure in detail

After choosing 'Corporate SecureEmail Certificate' in the E-PKI manager interface (as shown earlier) you will be presented with the application form shown below:

The screenshot shows a web browser window titled "InstantSSL Security Services - Windows Internet Explorer". The address bar shows the URL: <https://secure.comodo.com/products/EPKIApplyCSE1a?SID=D5TFUj0H61sPGKVI&product=47>. The page header includes the Comodo SSL logo and contact information: "Creating Trust Online", Tel: +1 703 581 6361, Tel: +1 206 203 6361, Email: sales@comodo.com. A banner for "ESTABLISH YOUR CUSTOMER'S TRUST AND WIN THEIR BUSINESS!" is also visible. The main content area is titled "Corporate Secure Email Certificate" and includes a welcome message for "smith@example.com" from Comodo CA. The form is divided into several sections: "User Details" with fields for Email Address, First Name, and Last Name; a confirmation checkbox; "Advanced Security Options" with a dropdown for "Cryptographic Service Provider" (Microsoft Base Cryptographic Provider v1.0) and checkboxes for "Is Private Key 'User-Protected?'" and "Is Private Key 'Exportable?'"; and "Certificate validity period" with a dropdown for "Select the validity period for your Certificate." (1 year, 2 years, 3 years). The total cost is displayed as \$11.25. The form has "Cancel" and "Submit" buttons. The footer contains the copyright notice "© Copyright 2007. All rights reserved." and the date "Thursday December 20, 2007".

5. Corporate SecureEmail Certificates may only be applied for on domain names which you have a right to use. Before applying for Certificates, you must first submit the domain name for validation:

## Corporate Secure Email Certificate

Your Current Credit is: \$ **XXX.XX**

Follow the link in the first stage of enrolment to submit a domain name for validation to Comodo's IdAuthority.

### Details

Address	<input type="text"/>	<input type="text"/>	<input type="button" value="v"/>
You may only apply for Corporate Secure Email Certificates containing domain names for which your right of use has been validated. If your required domain name does not appear in the above list, you may submit it for validation by clicking <a href="#">here</a> to register an IdAutho Website.			

Follow the link in the first stage of enrollment to submit a domain name for validation to Comodo's IdAuthority. Comodo will validate ownership of the submitted domain name.

6. Once validated your domain name will appear in a selection box in the enrollment form:

## Corporate Secure Email Certificate

Your Current Credit is: \$ **XXX.XX**

### User Details

1. Email Address	<input type="text" value="smith@example.com."/>	<input type="text" value="smith.example.com"/>	<input type="button" value="v"/>
You may only apply for Corporate Secure Email Certificates containing domain names for which your right of use has been validated. If your required domain name does not appear in the above list, you may submit it for validation by clicking <a href="#">here</a> to register an IdAuthority Website.			
2. First Name	<input type="text" value="John"/>		
3. Last Name	<input type="text" value="Smith"/>		
<input type="checkbox"/>	I confirm that the above individual is an employee / authorized representative of Comodo CA and is permitted to use the above email address for email communication.		

Complete the employee details and confirm the employee is an employee or authorized representative of your company.

7. You will be asked to specify the security options for the employee's Certificate.

### Advanced Security Options

(Only applicable if the User will obtain their Certificate using Internet Explorer)

4. Cryptographic Service Provider	Microsoft Base Cryptographic Provider v1.0
5. Is Private Key 'User-Protected'?	<input type="checkbox"/>
6. Is Private Key 'Exportable'?	<input checked="" type="checkbox"/>

- **Cryptographic Service Provide (CSP):** The CSP is responsible for generating the cryptographic keys. Select from the drop down list which CSP is to be used when the employee enrolls for their Corporate SecureEmail Certificate. If the Certificate is to be generated and placed on a smart card or other security device, ensure you select the relevant CSP from the list.  
Please note that the CSP you select MUST be present on the employee's PC.
  - **Private Key User Protected:** Check this box to place additional protection on the use of the private key (signing key) associated with the employee's Certificate. Additional protection will challenge to the employee to OK the use of the Certificate every time the private key is used.
  - **Private Key Exportable:** Check this box if the private key associated with the employee's Certificate should be exportable, e.g. if the Certificate can be backed up. If you do not allow exportability and the Certificate is lost, all emails encrypted for the employee will no longer be accessible.
8. Submit the form and the issuance process will begin.

### Certificate validity period

7. Select the validity period for your Certificate:	1 year 2 years 3 years
---	------------------------------

**Total Cost: \$11.25**

Cancel

Submit

9. An email will be sent to the stated employee containing a link to a specific setup page. This page will automatically generate a Corporate SecureEmail Certificate request and submit this request to the Comodo Certification Authority. Comodo will then generate the Certificate.

Once the link has been followed, it is important that the employee keep the browser window open – the Certificate, when issued, will then automatically be installed. The browser will then automatically redirect to the support pages to assist the employee in configuration and usage.

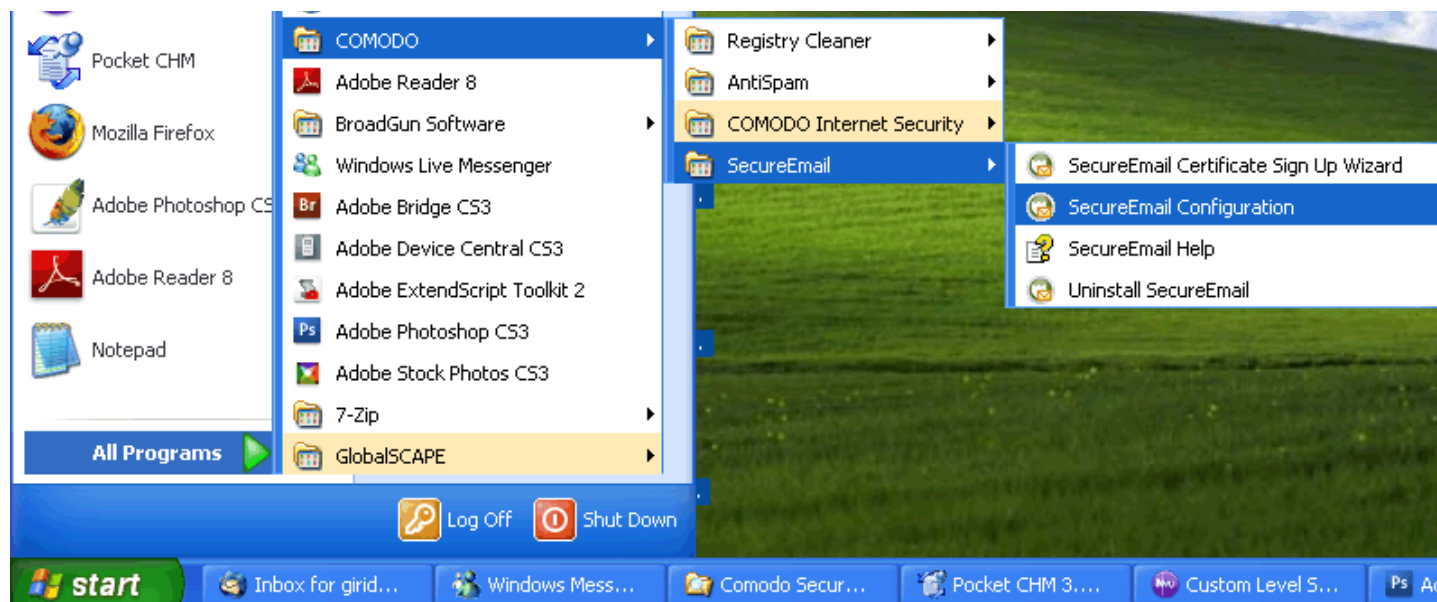
For support on configuration and installation please view:

[http://www.comodogroup.com/support/products/email\\_certs/corporate/index.html](http://www.comodogroup.com/support/products/email_certs/corporate/index.html).

10. Your account will be debited with the value of the certificate product type and validity period selected upon application of the Certificate. Upon receipt of the Certificate application the Certificate will be issued and emailed to your Account Administrator. Providing that the Certificate application contains no invalid or conflicting data, the Certificate will usually be issued within 1 hour.

## 6 Configuring SecureEmail

To configure SecureEmail options, click: Start > All Programs > Comodo > SecureEmail > Configure SecureEmail.



Secure Email configuration is divided into 7 categories. Click the links below to visit the appropriate help page.

- [Summary](#)
- [Security Settings](#)
- [Certificate Update Emails](#)
- [Certificates](#)
- [Protocols](#)
- [Email Folders Scanning](#)
- [General](#)

### 6.1 Summary

The Summary screen provides a snapshot of the configuration settings specified for the Security state, Statistics of mails processed and the version information of Comodo SecureEmail (CSE). This screen is displayed as default whenever SecureEmail Configuration is accessed from the Start Menu. The summary screen can also be viewed by clicking **Summary** tab in the main Configuration Screen.

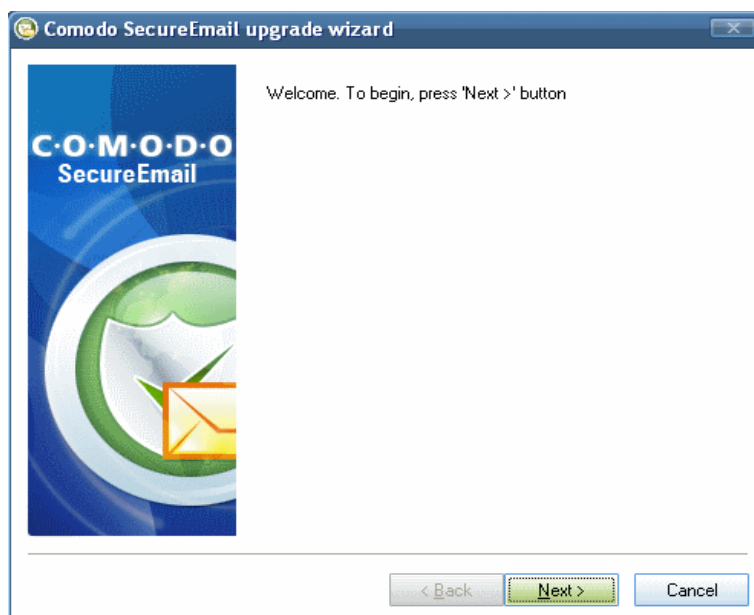


**Security State** - Displays the level of protection specified for the Encryption and Signing of the outgoing emails. See [Security Settings](#) for more details.

**Statistics** - Displays Statistics information about emails processed with the CSE. This gives the total number of mails sent and received and the relative number of mails encrypted and digitally Signed.

**Version Information** - Displays the version of CSE installed in your system and when it was last updated.

#### To manually check for updates



1. Click **Update now** button. The Upgrade Wizard is started. Click **Next**. The wizard searches for a new version.



If there is a new version available, you will be prompted to download and install the latest version of Comodo SecureEmail.

## 6.2 Security Settings

---

By Encrypting and Digitally Signing an email, your contact/recipient can verify your identity as the sender and will know that the original content of the message has not changed since it was first sent.

- Encrypting your email means that it can be deciphered and read only by the owner of the corresponding private key i.e. the intended recipient so that the confidential data sent by you cannot be stolen or modified on its way through the Internet.
- Digitally Signing your emails proves that the message and attachments really came from you and not someone masquerading as you.
- Digitally Signing your emails also ensures that the message and attachments cannot be modified or tampered with en-route through the Internet without the recipient being alerted.

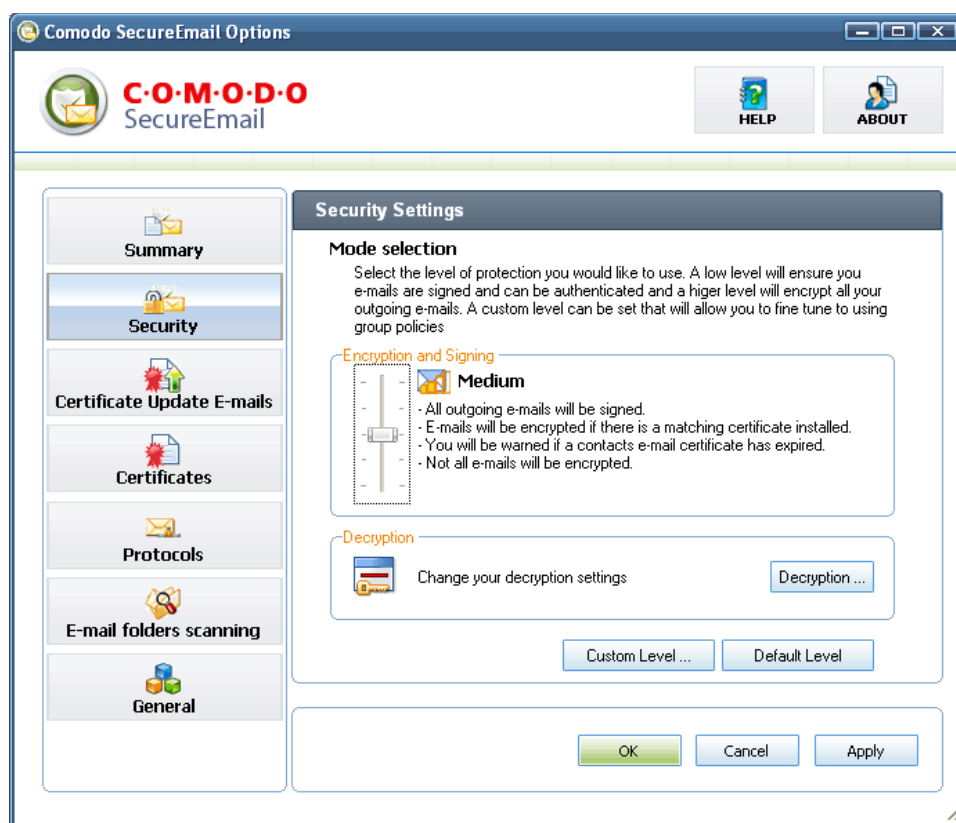
Truly secure email is therefore a combination of two equally important techniques:

**Encryption** - which ensures security of information and privacy.

**Digital Signing** - which proves that a message has not been altered during transmission and that the message came from the sender.

SecureEmail provides the ability to have all your outgoing emails *automatically* encrypted and digitally signed.

The Security Settings management interface allows you to specify the protection level for Encryption and Digital Signing the emails that you **send**. It can be accessed by clicking **Security** button in the configuration management interface.



It has the following two options:

**Default Level Settings** - Comodo SecureEmail allows users to quickly apply preset security configurations by moving the built-in security level slider. Each setting determines protection levels for Encryption, Digital Signing and Decryption. A description of the meaning of each setting is displayed alongside each setting. Clicking the 'Default Level' button in the 'Security Settings' interface will move this slider to, and implement, the 'Medium' setting. Note - using the slider to select a default security setting will implement that setting for **all** users and will over-rule any custom and group security settings.

For more details, please see '[Default Settings](#)'. For a table that specifies the precise security options implemented by each preset, see '[Appendix 3 - Default Security Profiles](#)'.

**Custom Level Settings** - The Custom level option enables advanced users to make customized configuration for Encryption, Signing and Decryption settings.

### 6.2.1 Default Level Settings

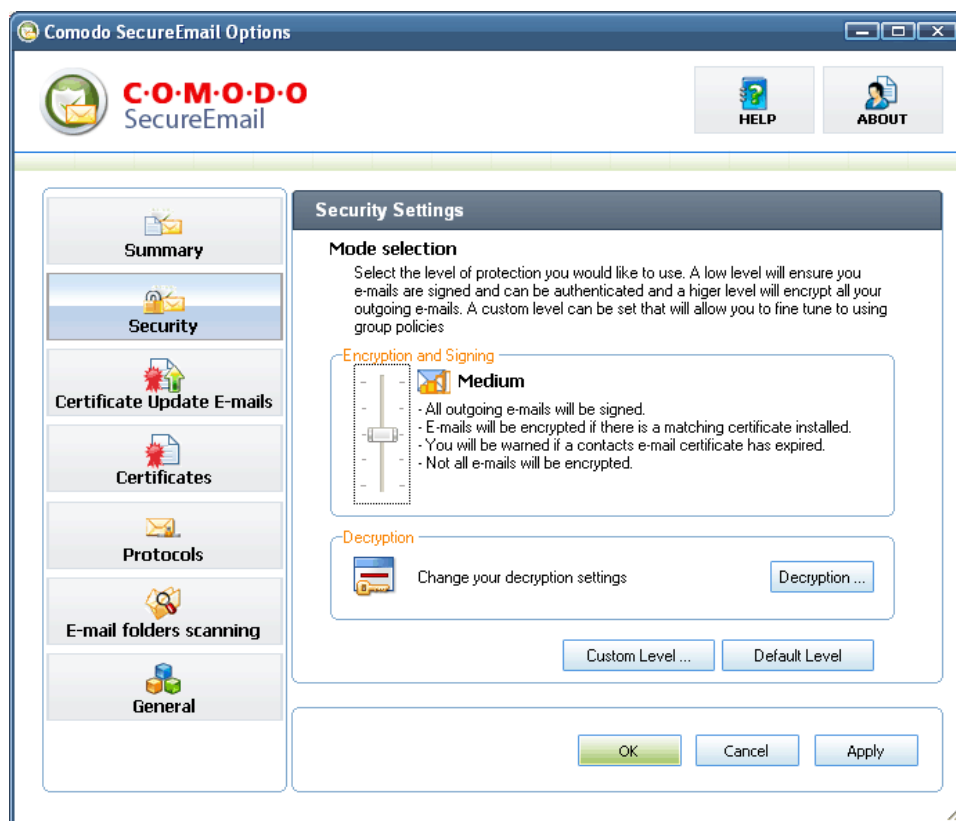
Comodo SecureEmail allows users to quickly apply preset security configurations by moving the built-in security level slider. Each setting determines protection levels for Encryption, Digital Signing and Decryption. A description of the meaning of each setting is displayed alongside each setting. Clicking the 'Default Level' button in the 'Security Settings' interface will move this slider to, and implement, the 'Medium' setting. Note - using the slider to select a default security setting will implement that setting for **All** users and will over-rule any custom and group security settings.

For a table that specifies the precise security options implemented by each preset, see '[Appendix 3 - Default Security Profiles](#)'.

By default, this settings panel is displayed if you click on the **Security** tab. If you have chosen Custom Level settings during your previous configuration set-up, you can revert to Default Level Settings panel, by clicking on **Default Level** Button.

The Default Settings Panel has the following options:

- Slider control for switching between preset protection levels ; and
- Decryption Settings.



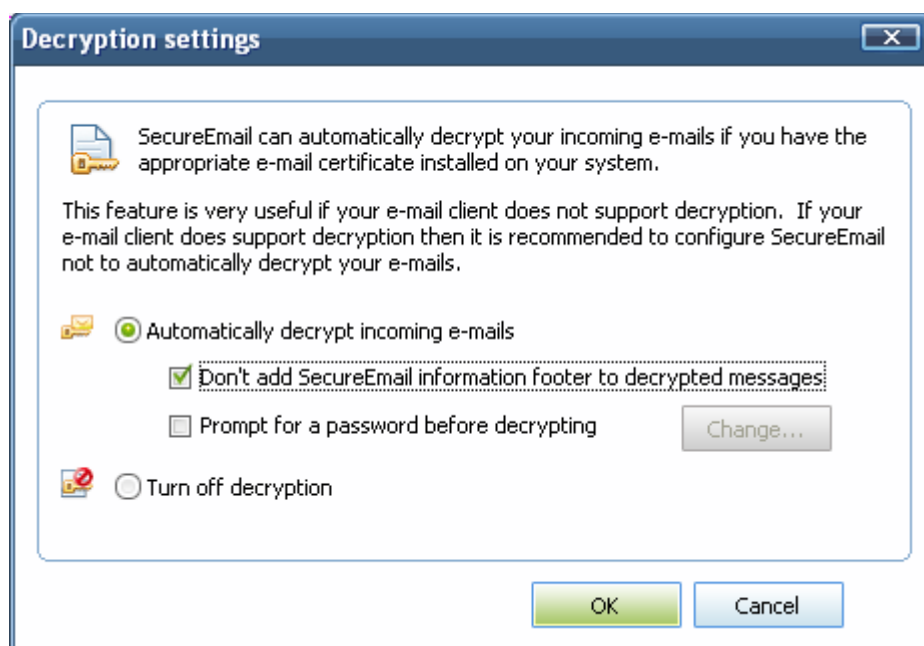
**Mode Selection Slider Control** - The slider control allows you to easily set the Security Level, with predefined Encryption, Signing and Decryption settings. It has five modes ranging from **Off** to **Very High**. Each of these levels is configured with respective specifications for Encryption, Signing and Decryption of your outgoing and incoming mails. Refer Appendix-3 Default Security Profiles for more details. The settings specified for the selected level are displayed alongside the slider.

**Decryption Settings** - All the encrypted emails that you receive are to be decrypted using your private key. The Decryption area allows you to configure CES to provide automatic decryption of your incoming emails.

This feature is highly recommended if your email client doesn't support SMIME/decryption (for example, Incredimail).

If your mail client DOES support SMIME/decryption (Outlook, Outlook Express, Thunderbird etc) then we recommend that you do not use this function\_and choose 'Turn off decryption'.

- Click on the Decryption button to access the Decryption Settings interface.



**Automatically decrypt incoming emails** - If enabled, Comodo SecureEmail will become the decryption gateway for incoming messages that have been encrypted using your email certificate.

- It will take over decryption duties if your mail client supports S/MIME.
- It will add decryption capability if you are using a mail client that does not support S/MIME (e.g. Incredimail) - i.e. SecureEmail will intercept the mail, decrypt it, then forward it to your mail client. (Users should note that this won't necessarily mean the mail is readable in non-S/MIME clients because the message may also have been signed by your contact without a clear text version attached)

You can configure the following options in here:

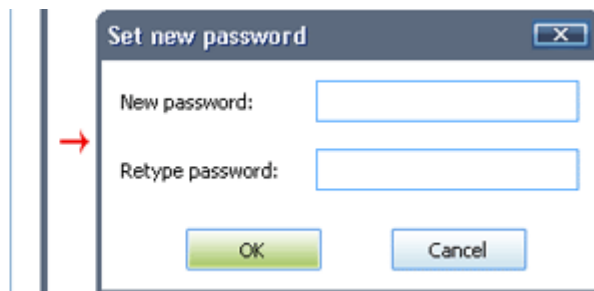
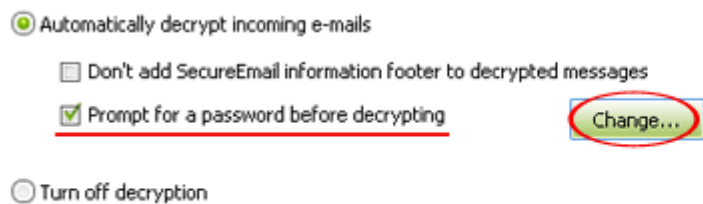
**Don't add SecureEmail information footer to decrypted messages** - By default, SecureEmail attaches an informational footer to every mail it decrypts. Uncheck to disable this feature.

**Note** - Regardless of your choice here, SecureEmail will never attach a footer to a decrypted message if the message has also been digitally signed. More info in the [FAQ](#).

**Prompt for a password before decrypting** - checking this option means SecureEmail will request a password before decrypting any messages. This adds another layer of security to your communications and is particularly useful on shared computers where the same mail client is being used for multiple mail accounts. Also, this helps prevent your messages from being compromised should an intruder gain access to your mail account settings and/or computer.

#### To set the password

1. Check the box against '*Prompt for a password before decrypting*';
2. Click on '*Change...*' button;
3. Enter and retype new password;
4. Click '*OK*' to save it.



Click 'OK' to save your preferences.

*NOTE:* The decryption options outlined on this page relate to messages that have been encrypted using your public key certificate. If you receive a message that has been encrypted using a SecureEmail 'session' certificate then SecureEmail will always intercept and decrypt it before sending your certificate back to the sender for future use. See [Certificate Update Emails](#) for more details .

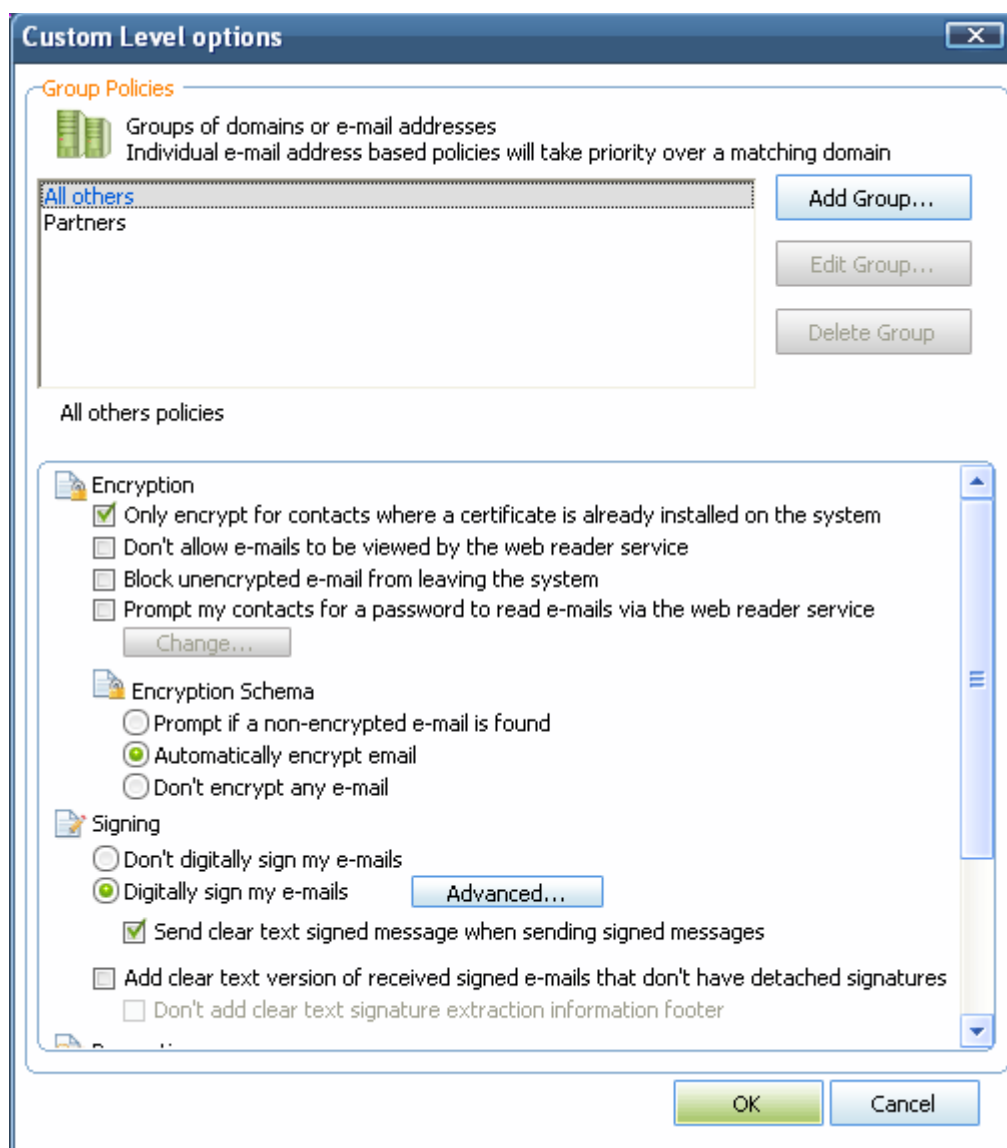
**Turn off decryption** - If enabled, no decryption will be performed by SecureEmail. Decryption duties will remain the province of your S/MIME capable mail client.

## 6.2.2 Custom Level Settings

The Custom Level Settings option in the Security Settings interface allows customized configuration of the protection levels of Encryption, Digital Signing and Decryption of your emails. Click on the **Custom Level** Button in the Security Settings interface to access Custom level options interface.

The configuration settings can be done for :

- [Group Policies;](#)
- [Encryption;](#)
- [Encryption Schema;](#)
- [Digital Signing;](#)
- [Decryption;](#) and
- [Housekeeping messages.](#)



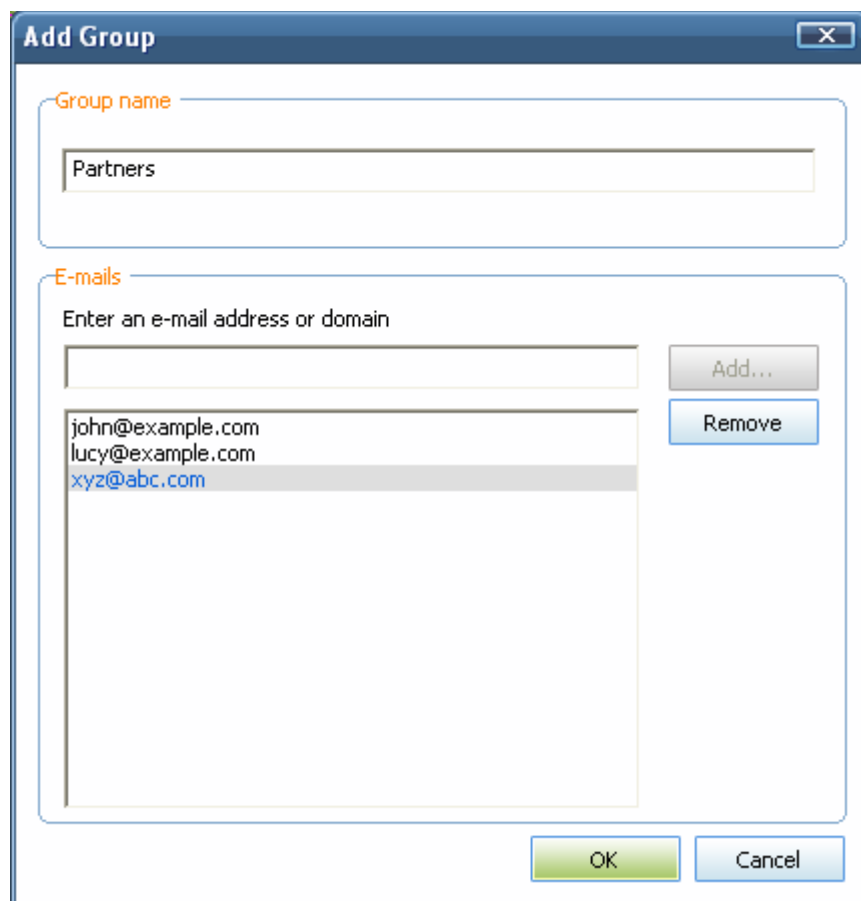
**Group Policies** - You can define groups of domains or email addresses (each group can contain 1-N number of email addresses). For each group, you can specify different protection levels, depending on the members in the group. The settings that you specify in the Custom Level Options interface, will apply for the group that is highlighted in the group policies list box.

Comodo SecureEmail has one default and unremovable group - **All other**. This group represents the email addresses which are not included in any other Group. You can specify a separate protection level configuration for this group.

### To add a new group

1. Click **Add Group**.

The following screen is displayed



2. Type a Name for the group in the Group name text box.
3. Type the email address or domain name of each contact belonging to that group in the email address box and click **Add**.

Repeat the process for adding several groups. You can also edit (i.e. add or remove contacts from a group) or delete a group from this interface.

## Encryption

There are two ways that SecureEmail can encrypt your mail - using installed certificates or by using a single-use certificate. At a basic level, all of the options detailed in this section revolve around the configuration and deployment preferences of these two encryption techniques.

- **Using Installed Certificates.** If you have your recipients email certificate installed then Comodo SecureEmail can use it to encrypt your message in the same way that your mail client would. This is the ideal way to encrypt with both parties having email certificates. SecureEmail will only encrypt with a single-use certificate if you do not have your contact's email certificate installed. For more details on certificates and certificate management, please see the 'Certificates' section.
- **Using Single-Use Certificates.** Single-Use certificates are one-time 'session' certificates that enable the encryption of messages to recipients when you do not have their 'regular' email certificate installed on your system. The encrypted email is then sent to the contact and the single-use certificate is uploaded to the

SecureEmail servers. Your recipient can decrypt and read the email either by installing a copy of SecureEmail or by using the secure [Web reader service](#). For more details, please see the section '[Receiving Encrypted Email Messages](#)'

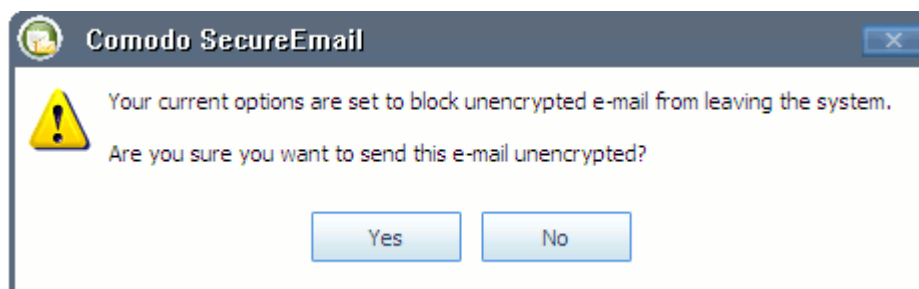
You can configure for the following in the Encryption area.

- [Only encrypt for contacts where a certificate is already installed on the system](#);
- [Don't allow emails to be viewed by the web reader service](#);
- [Block unencrypted email from leaving the system](#); and
- [Prompt my contacts for a password to read emails via the web reader service](#).

**Only encrypt for contacts where a certificate is already installed on the system** - Checking this option effectively instructs the application NEVER to encrypt using SecureEmail's single-use session certificates. Encryption will only ever be carried out using installed certificates. Your choice of whether or not to use single use certificates has an impact on other encryption options that you may have chosen on the Encryption Schema.

**Don't allow emails to be viewed by the web reader service** - Checking this box means that recipients will be not able to read your email using Comodo's web reader service. In order to view your message, they will have to download and install their own copy of Comodo SecureEmail. [Click here for more details](#) on the secure web reader service and how it integrates with Comodo SecureEmail.

**Email Firewalling - Block Unencrypted email from leaving the system** - Checking this box means that SecureEmail will prompt you if you attempt to send out an unencrypted mail.



**Prompt my contacts for a password to read emails via the web reader service** - Checking this box means that recipients must enter a password before they can read your email using Comodo's secure web reader service. [Click here for more details](#) on the secure web reader service and how it integrates with Comodo SecureEmail. Communication of this password to your recipient should be done using alternative, out-of-band mediums such as telephone, instant messenger or in person.

## Encryption Schema

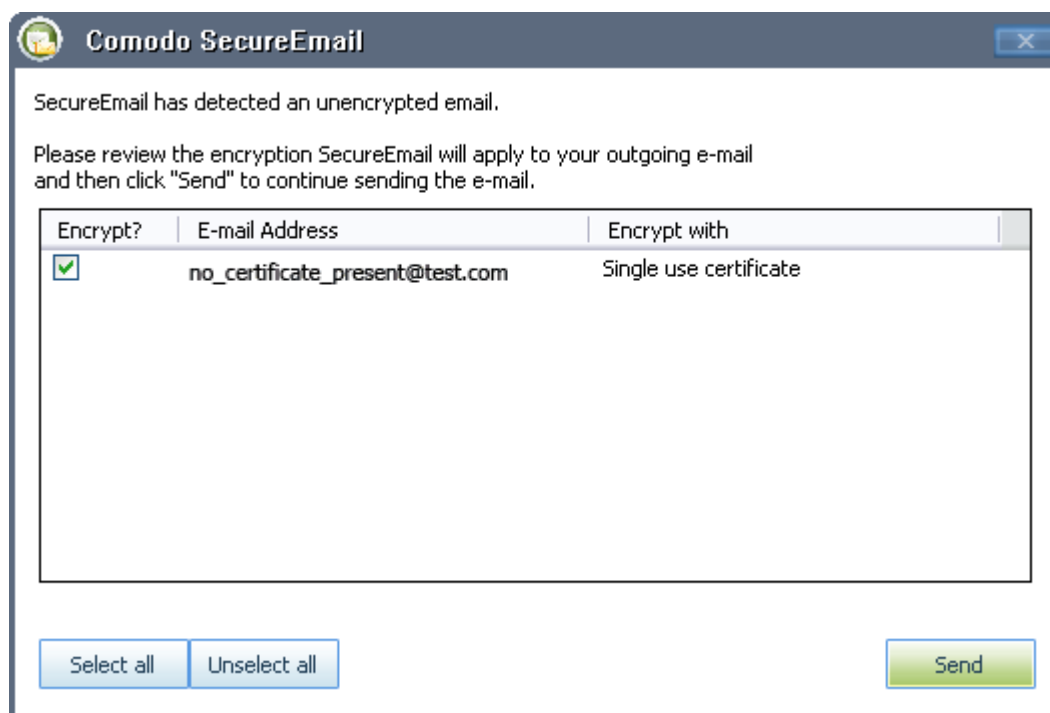
The Encryption Schema area allows for advanced settings for encryption. The settings made here have an impact on using the certificates, in combination with settings made for encryption.

You can configure for the following in the Encryption Schema area.

- Prompt if a non-encrypted email is found;
- Automatically Encrypt email; and
- Don't Encrypt any email.

**Prompt if a non-encrypted email is found** - Checking this option will display a prompt if SecureEmail detects that you are trying to send an unencrypted email. The dialog shown depends on whether or not an email certificate for the contact is present on the system.

- If you already have the recipients email certificate, the dialog asks if you want to encrypt the email using this certificate.



- Choose whether or not you wish to encrypt the message by checking/unchecking the 'Encrypt?' box at the upper left and Click 'Send' when you have made your choice.
- If you do not have an email certificate for the recipient, then the dialog will ask if you want use SecureEmail's built-in encryption functionality to encrypt the message using a single-use email certificate:
  - Choose whether or not you wish to encrypt the message by checking/unchecking the 'Encrypt?' box at the upper left and Click 'Send' when you have made your choice.

**Automatically Encrypt email** - Selecting this option will instruct SecureEmail to automatically encrypt all outgoing emails addressed to any member of the selected group:

- If you already have the recipients email certificate installed then SecureEmail will use it to encrypt the message.
- If you do not have the recipients email certificate then SecureEmail will encrypt the message using a single-use certificate. if you have enabled it.

**Note:** If you want to encrypt only using installed certificates (and never encrypt using single-use certificates) you should select Only encrypt for contacts where a certificate is already installed on the system in Encryption settings.

**Don't Encrypt Any Email** - This option turns off SecureEmail's encryption functionality only for the members of the selected group. Checking this option means all your outgoing emails will be sent in clear text. (if you choose not to encrypt your email, then it can easily be read by a third party if the message is intercepted during its passage over the Internet)

Note 1: Choosing 'Don't Encrypt Any Email' over-rides the 'Only Encrypt for contacts where a certificate is already installed on the system' option in Encryption settings.

Note 2: Disabling encryption DOES NOT prevent you from Digitally Signing messages. See the section 'Digital Signing' for more details.

The combination of the encryption setting **Only encrypt for contacts where a certificate is already installed on the system** with different options in the encryption schema are described below:

- Prompt if a non-encrypted email is found + Only encrypt for contacts where a certificate is already installed on the system: You will be prompted if you attempt to send an unencrypted message to a recipient *whether or not* you have their certificate installed. If you DO have their certificate, SecureEmail will ask you if you want to use it to encrypt the message. If you DON'T have their certificate installed then SecureEmail will provide the *option* for you to encrypt using a single-use certificate rather than as plaintext.
- Automatically Encrypt all Emails + Only encrypt for contacts where a certificate is already installed on the system: This combination means that SecureEmail will automatically encrypt all emails ONLY when you have that recipients certificate installed on your system. The application will NOT encrypt (using a single use certificate) when you attempt to send an unencrypted mail to a recipient for whom you do not have a certificate installed.
- Don't Encrypt any email + Only encrypt for contacts where a certificate is already installed on the system: SecureEmail will NOT encrypt any email at all - either using installed certificates or single use certificates, i.e. it is irrelevant whether or not you check 'Only encrypt for contacts where a certificate is already installed on the system' IF you have already selected 'Do not Encrypt any email'.

## Digital Signing

The **Signing** area in the custom level options interface allows to configure the signing options. You can configure for the following in the Signing area with respect to the selected group.

- Don't digitally sign my emails:
- Digitally sign my emails:
- Advanced Signing options:
- Add clear text version of received signed emails that don't have detached signature: and
- Don't add clear text signature extraction information footer.

**Don't digitally sign my emails** - This option means Comodo SecureEmail will not sign any of your outgoing mails. You can still encrypt your mail, but the recipient of your emails will not be able to verify you as the sender or confirm that the mail has not been tampered with.

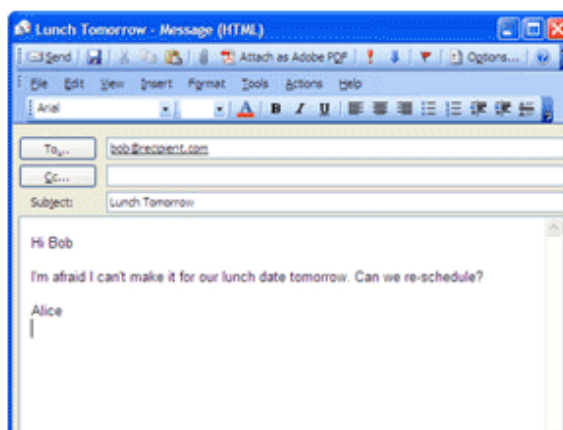
**Digitally sign my emails** - If enabled, all your outgoing emails will be signed *automatically* using your Comodo email certificate. Digitally signing your messages proves to your recipients that YOU are the sender and that contents of your message have not been altered during transit.

- **Send clear text signed message when sending signed messages**- If enabled, Comodo Secure Email will automatically send a clear text version of the message with every signed mail. This allows email clients than don't support S/MIME to view the message. This can be an especially important setting if you are sending the same signed and encrypted mail to multiple recipients - some of whom use S/MIME capable clients (such as Outlook and Thunderbird) and some that don't (such as Incredimail and Hotmail). If this box is not checked, the Incredimail/Hotmail recipient would not be able to view the signed message even if an encryption gateway had successfully decrypted it. (see example below).

## Digital Signing with clear text versions

### An example

- Alice sends a signed message to Bob
- Bob is using a non-SMIME capable client such as Yahoo mail which cannot decipher digital signatures



#### SCENARIO 1

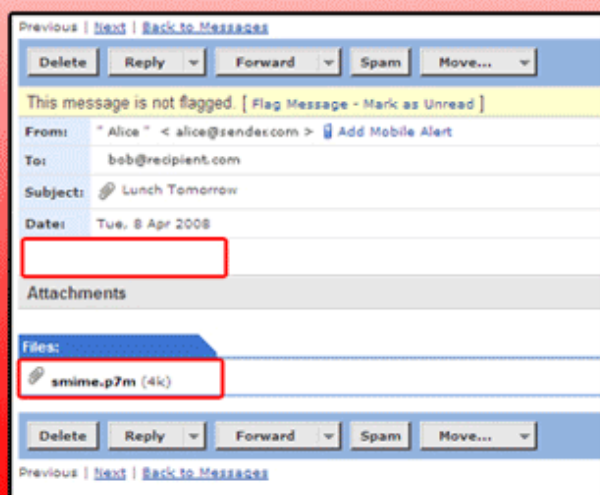
Alice does not check the 'Send Clear text...' box in the 'Digital Signatures' area of Comodo Secure Email:

Send clear text signed message when sending signed messages

#### RESULT

Alice's message and digital signature arrive as a .p7m attachment ONLY.

The message body cannot be read by Bob because his client cannot decrypt the attachment - so it appears to be a blank mail



#### SCENARIO 2

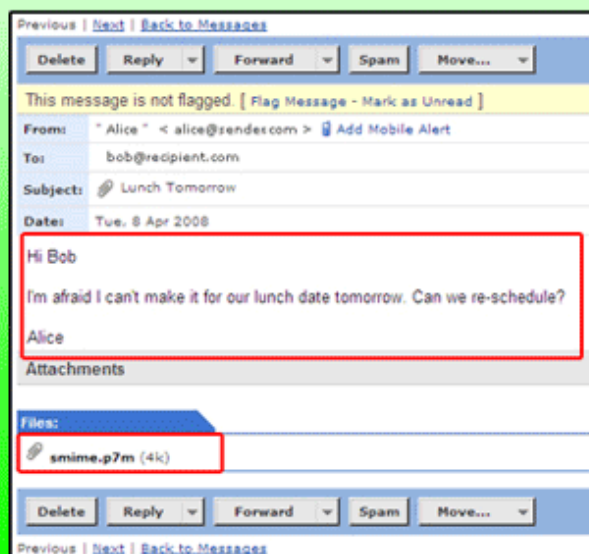
This time, Alice has the 'Send Clear text...' box checked:

Send clear text signed message when sending signed messages

#### RESULT

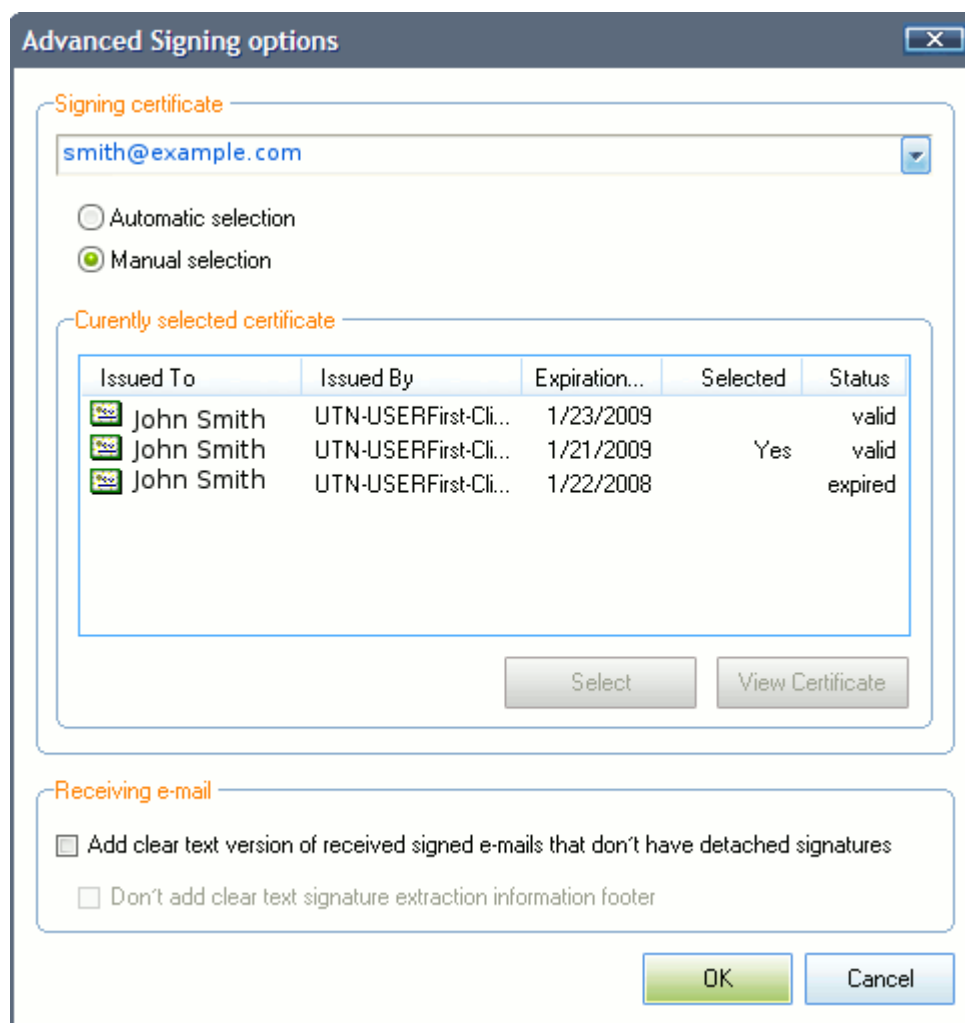
Bob's email client still cannot decipher the attachment.

However, he is still able to read the message body because Alice ALSO sent a plain text version.



Comodo recommends that users leave this option enabled. (\* Note: Sending a 'clear text' version of a digitally signed message does not compromise the security of an encrypted mail. This is because the encryption part of the equation is carried out on the message *after* it has been signed. This means the entire signed message, clear text version and all, is encrypted and can only be decrypted by the intended recipient. For more details, see this [FAQ](#))

**Advanced Signing options** - Clicking on the **Advanced** button allows you to specifically select which mail certificate to use on a per account basis, so you can have multiple accounts, each using a different certificate.



If you wish to change the certificate used for a particular mail account, then:

- First choose the desired email account from the drop-down box. This will list the certificates for that account in the 'Currently Selected Certificate' pane. All certificates present on your system are listed – including those that are expired.

Background note: You cannot choose to sign with an expired certificate! BUT you should still keep expired certificates as you will need them to decrypt old emails.

- Highlight the certificate you wish to use to sign mails for that email account. This will change the radio button from 'automatic selection' to 'manual selection'.

Background note: SecureEmail will have automatically pre-selected the appropriate certificate with which to sign based on:

(i) the mail account you are using to send the message

(ii) If you have more than one certificate per account, it selects the most recently issued certificate.

- Click 'Select'

'Yes' will appear in the 'selected' column next to the certificate you have chosen

- Click 'OK'.

NOTE 1: To sign an email with SecureEmail you need to have a Comodo certificate installed. This applies to both Pro and Home editions of the application. You can sign up for a Comodo E-Mail certificate using the built in certificate application wizard outlined on [here](#). If you wish to **encrypt** using a non-Comodo email certificate (e.g. A VeriSign or a Thawte certificate) then you must install Comodo SecureEmail Pro.

NOTE 2: To ensure smooth operation of Comodo SecureEmail, it is essential that you switch off any signing and encryption functionality that is built into your mail client.

### **Add clear text version of received signed emails that don't have detached signature**

If enabled, Comodo SecureEmail will automatically add a clear text version of any signed email's that you receive IF that mail does not have a detached signature. This will allow you to view incoming, signed emails if you are using a client that doesn't support S/MIME (for example Incredimail).

This is an especially useful setting when you consider that many of the popular mail clients that your contacts will be using to send mail to you (including Outlook) do not always attach such a clear text version to signed messages. This makes the message unreadable if you are viewing mail in a non-SMIME capable client.

For more details on the importance of clear text versions and detached signatures, see [this explanation](#) and [this FAQ](#).

### **Don't add clear text signature extraction information footer**

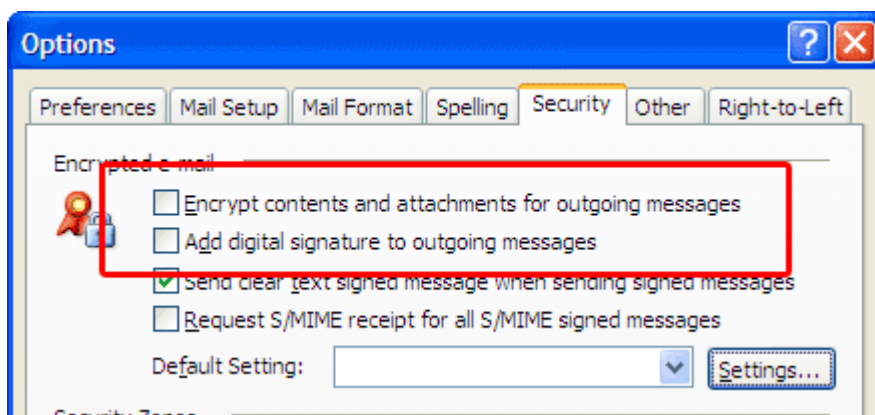
By default, SecureEmail attaches an informational footer to every plain text body that it extracts from a signature as follows

*"Clear text version of signed emails extracted by Comodo SecureEmail on [Date] at [Time]"*

If you do not want to see this message then check this box.

**IMPORTANT NOTE** - For smooth operations of SecureEmail, it is strongly recommended that you turn OFF any encryption and signing functionality in your email client as both of these duties will be performed by Comodo SecureEmail.

For example, in Microsoft Outlook, you should select **Tools > Options > Security**. Make sure the 'Encrypt Contents...' and 'Add Digital Signature...' boxes are **NOT** checked (see below).



## Decryption

The Decryption area in the custom level options interface allows you to configure the decryption settings for the mails received from the members of the selected group.

You can configure the following:

- Turn off decryption;
- Automatically decrypt incoming emails;
- Don't add SecureEmail information footer to decrypted messages; and
- Prompt for a password before decrypting.

**Turn off decryption** - If enabled, no decryption will be performed by SecureEmail. Decryption duties will remain the province of your S/MIME capable mail client.

**Automatically decrypt incoming emails** - If enabled, Comodo SecureEmail will become the decryption gateway for incoming messages that have been encrypted using your email certificate.

- It will take over decryption duties if your mail client supports S/MIME.
- It will add decryption capability if you are using a mail client that does not support S/MIME (e.g. Incredimail) - i.e. SecureEmail will intercept the mail, decrypt it, then forward it to your mail client. (Users should note that this won't necessarily mean the mail is readable in non-S/MIME clients because the message may also have been signed by your contact without a clear text version attached)

You can configure the following options in here:

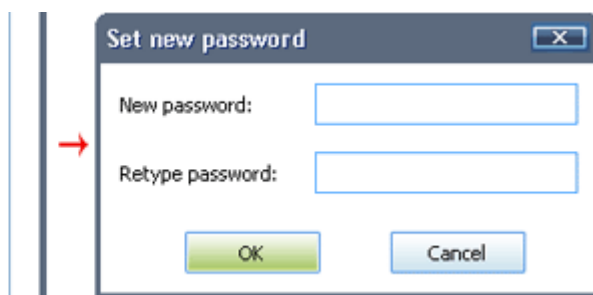
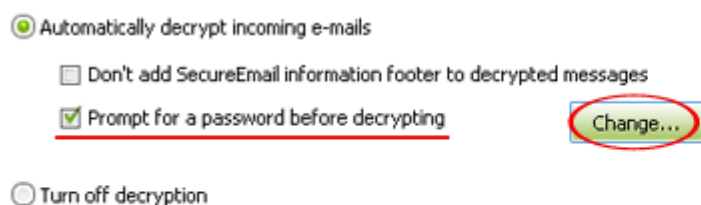
**Don't add SecureEmail information footer to decrypted messages** - By default, SecureEmail attaches an informational footer to every mail it decrypts. Uncheck to disable this feature.

**Note** - Regardless of your choice here, SecureEmail will never attach a footer to a decrypted message if the message has also been digitally signed. More info in the [FAQ](#).

**Prompt for a password before decrypting** - checking this option means SecureEmail will request a password before decrypting any messages. This adds another layer of security to your communications and is particularly useful on shared computers where the same mail client is being used for multiple mail accounts. Also, this helps prevent your messages from being compromised should an intruder gain access to your mail account settings and/or computer.

### To set the password

1. Check the box against '*Prompt for a password before decrypting*';
2. Click on '*Change...*' button;
3. Enter and retype new password;
4. Click '*OK*' to save it.



**NOTE:** The decryption options outlined on this page relate to messages that have been encrypted using your public key certificate. If you receive a message that has been encrypted using a SecureEmail 'session' certificate then SecureEmail will always intercept and decrypt it before sending your certificate back to the sender for future use. See [Certificate Update Emails](#) for more details .

### Housekeeping Messages

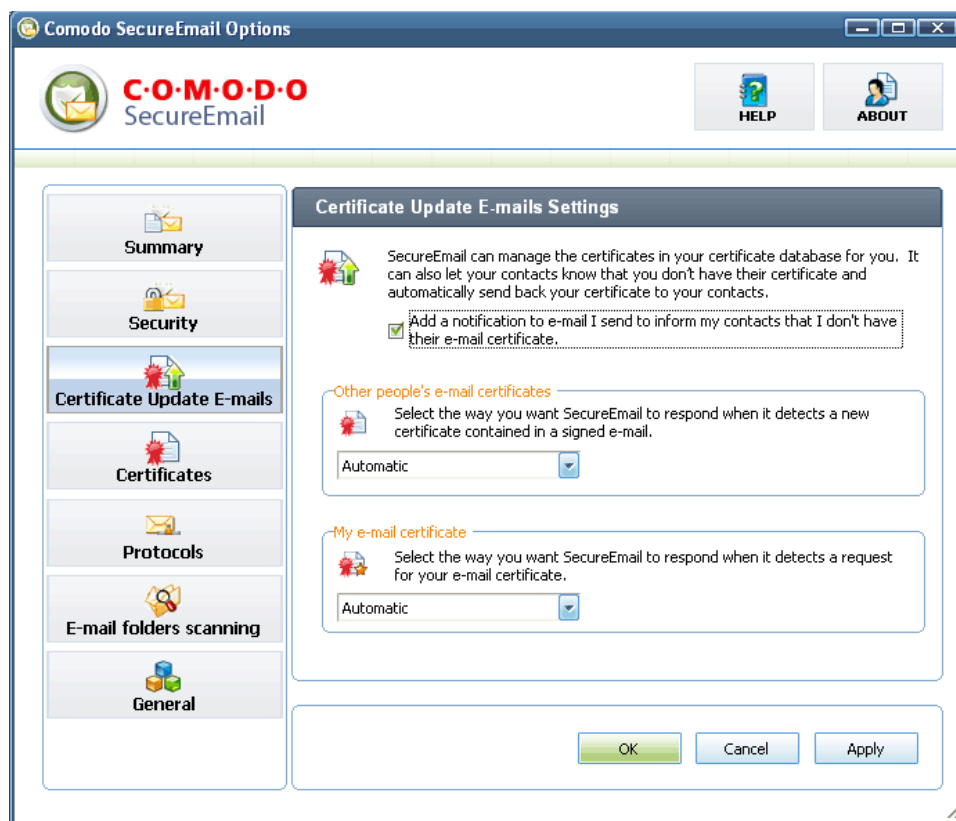
The Housekeeping Messages area in the custom level options interface allows you to configure handling of calendar messages and read receipt messages.

**Don't encrypt or sign Outlook calendar messages** - Selecting this option means that the calendar messages generated by Outlook are not encrypted.

**Don't encrypt or sign read receipt messages** - Most mail clients have an option whereby a person that has sent you an email can request that you send a short confirmation message in return stating that the message has been read. These are automated and standardized messages that contain no sensitive data and basically just state the time that the message was officially read by you. They also require no user interaction other than for you to select 'Yes' or 'No' when the request dialog box appears. Selecting this option means that these 'confirmation of read' emails will not be encrypted or signed.

## 6.3 Certificate Update Emails

Certificate Update Emails ensure both sender and recipient are updated with each others certificates - a time consuming and complex responsibility that is usually placed on the individuals involved. This area allows you to specify precisely how SecureEmail should handle these certificate exchange notifications.



- **Add notification to email I send to inform my contacts that I don't have their email certificate.** - If you do not have your contacts email certificate already installed, then this setting will add a header to your outgoing emails that requests their certificate.
  - **If Your contact already has SecureEmail installed,** their installation of SecureEmail will detect the header in your email and, depending on your contact's choice in the section 'My Email Certificate', will automatically reply to you with a signed email to facilitate the certificate exchange. Similarly, the section 'Other peoples email certificates' allows you to choose how *your* installation of SecureEmail should react when it receives the reply.
- **If Your contact does not have SecureEmail installed,** the header cannot be detected. However, if you have encrypted the message with a single use certificate then your contact will receive instructions on (i) how to download their own copy of the application (ii) how to decrypt and read the mail. Once installed, their copy of SecureEmail will detect the header in your original mail and automatically reply with a signed email.

Note: This header can only be read and understood by installations of SecureEmail and you must digitally sign the outgoing mail for this setting to take effect. For security reasons, this header is not added to outgoing plain text emails. Comodo recommends that users leave this option enabled.

- **Other people's email certificates**

The drop-down options here enable you to set how you want SecureEmail to react when it detects that someone has sent you their email certificate in a signed message.

#### Other people's e-mail certificates

Select the way you want SecureEmail to respond when it detects a new certificate contained in a signed e-mail.

A screenshot of a dropdown menu. The menu is open, showing four options: 'Automatic', 'Prompt', 'Automatic', and 'Do not install'. The second 'Automatic' option is highlighted with a grey background. The dropdown arrow is on the right side of the menu.

- **Prompt** - SecureEmail will generate a pop-up dialog asking you if you want to install the sender's certificate. Clicking 'Yes' will automatically import the sender's certificate into the Window's certificate store. From this point on you can encrypt for that contact using that certificate.
- **Automatic** - SecureEmail installs the new certificate automatically. From this point on you can encrypt for that contact using that certificate.
- **Do not install** - Disregards the new certificate. User's will have to manually import any new certificates that are sent to them.

- **My email certificate**

The drop-down options here enable you to set how you want SecureEmail to react when it detects a request for your email certificate?

#### My e-mail certificate

Select the way you want SecureEmail to respond when it detects a request for your e-mail certificate.

A screenshot of a dropdown menu. The menu is open, showing four options: 'Automatic', 'Prompt', 'Automatic', and 'Do not send'. The second 'Automatic' option is highlighted with a grey background. The dropdown arrow is on the right side of the menu.

- **Prompt** - SecureEmail will generate a pop-up dialog asking you if you want to send your certificate to this contact.. Clicking 'Yes' means SecureEmail will send your certificate to the requestor in a signed email. From this point on your contact can encrypt mails sent to you using your certificate
- **Automatic** - SecureEmail sends your certificate to the requestor automatically. From this point on your contact can encrypt mails sent to you using your certificate
- **Do not send** - SecureEmail will disregard the request and will not send your certificate.

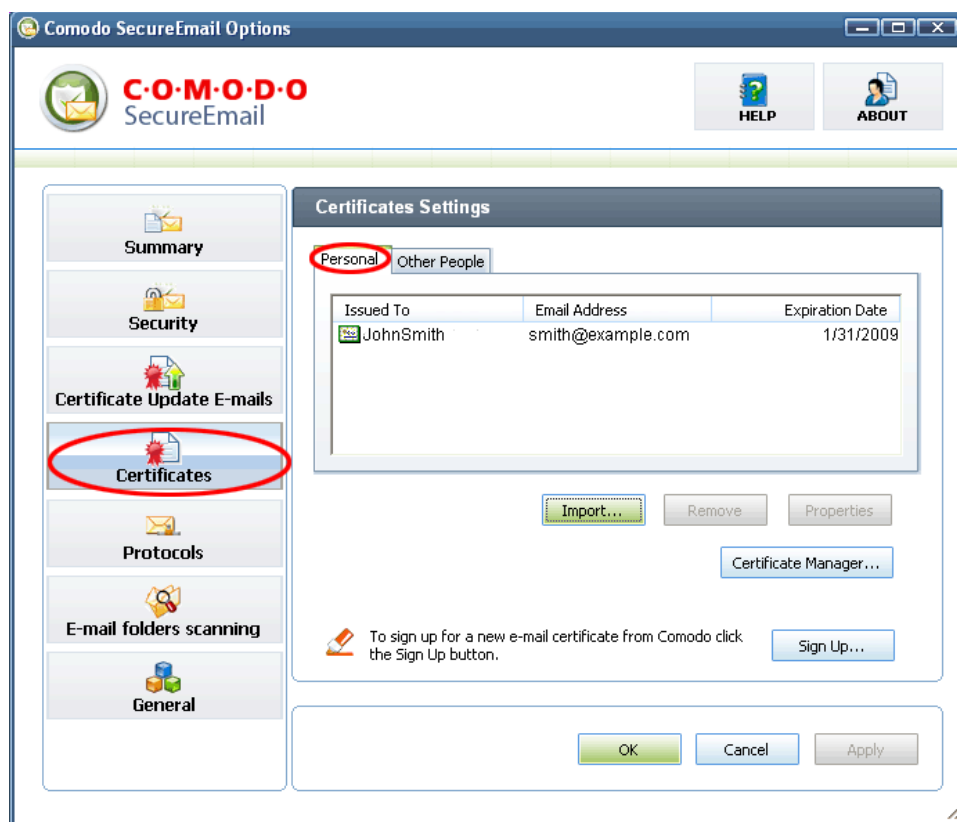
## 6.4 Certificate Settings

---

The certificate settings area provides fast, centralized management of the email certificates installed on your machine. From here you can:

- Inspect your own installed email certificates to find out details such as expiry date;
- Find out whether or not you have a recipients certificate installed on your system;
- Easily import, remove and view certificates;

- Sign up for a free Comodo email certificate; and
- Quickly Access the full Windows certificate store from within the SecureEmail interface.



### 'Personal' tab

This tab displays all your personal email certificates. Certificates listed in the 'Personal' tab can be used to digitally sign any email messages you send out to your contacts. If your email certificate is installed on other peoples systems, then they can use it to encrypt any messages they send to you. If this tab is empty, then you should click the 'Sign Up' button to download and install a free Comodo email certificate. For full details on this fast and easy process, please see '[Certificate Sign Up Wizard](#)'.

The screenshot shows the 'Certificates Settings' window with the 'Personal' tab selected. A table lists one certificate issued to JohnSmith with email address smith@example.com and expiration date 1/31/2009. Below the table are buttons for 'Import...', 'Remove', 'Properties', and 'Certificate Manager...'. At the bottom, there is a 'Sign Up...' button and a note: 'To sign up for a new e-mail certificate from Comodo click the Sign Up button.'

Issued To	Email Address	Expiration Date
JohnSmith	smith@example.com	1/31/2009

### 'Other People' tab

This tab displays other people's email certificates that are installed on your system. You can use the certificates listed in this tab to encrypt any mail that you send to that particular contact. If you do not have their certificate installed then you can still encrypt using a single-use certificate - a feature unique to Comodo SecureEmail.

The screenshot shows the 'Certificates Settings' window with the 'Other People' tab selected. A table lists one certificate issued to Lucy with email address lucy@example.com and expiration date 1/31/2009. Below the table are buttons for 'Import...', 'Remove', 'Properties', and 'Certificate Manager...'. At the bottom, there is a 'Sign Up...' button and a note: 'To sign up for a new e-mail certificate from Comodo click the Sign Up button.'

Issued To	Email Address	Expiration Date
Lucy	lucy@example.com	1/31/2009

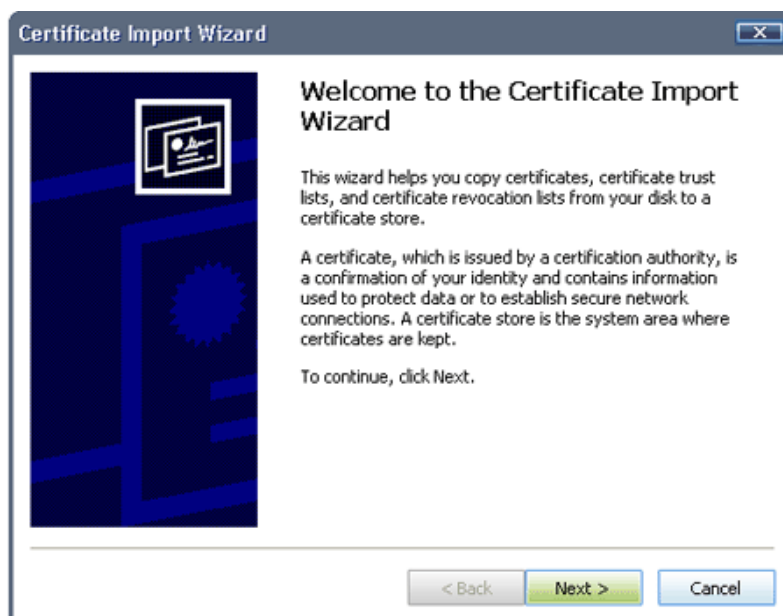
## Certificate Sign Up Wizard

Click the 'Sign Up' button to apply for a free Comodo email certificate. The wizard simplifies the whole application procedure and can be completed in minutes - requiring you to enter only your name and email address. For a complete overview of this process, see '[Certificate Sign Up Wizard](#)'.

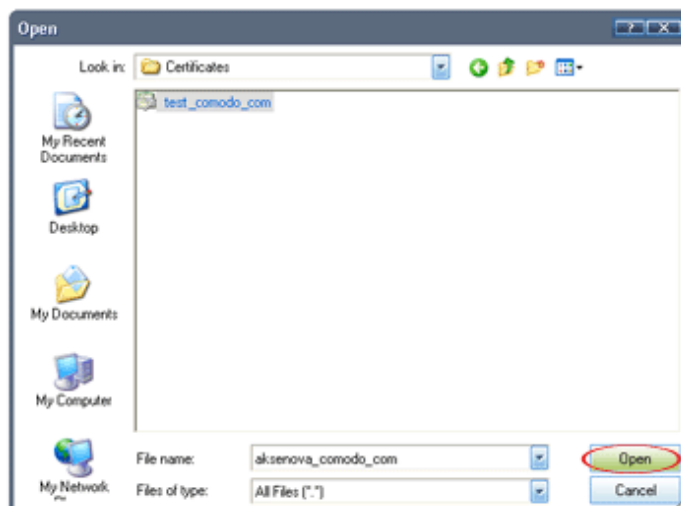
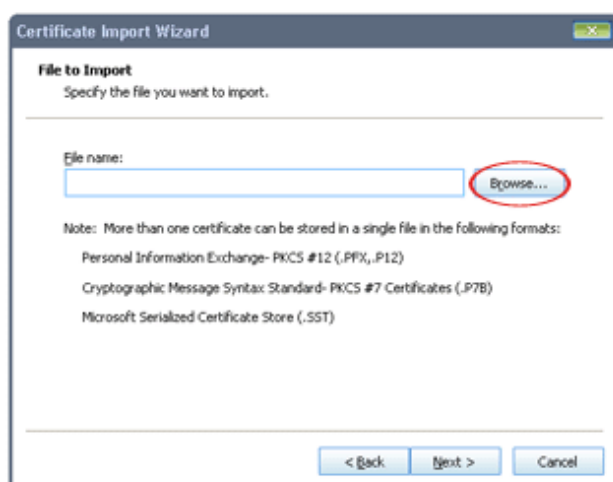
## Import Certificates into the Personal or Other People store

Comodo SecureEmail automatically imports your and other people's certificates into the appropriate store as soon as it detects them. However, there are situations when users will want to manually import certificates into the store. SecureEmail has a built in wizard that simplifies this usually complex procedure:

1. Click the '*Import*' button to launch the Certificate Import Wizard (see below). Clear instructions are provided throughout this wizard to guide you through the process.



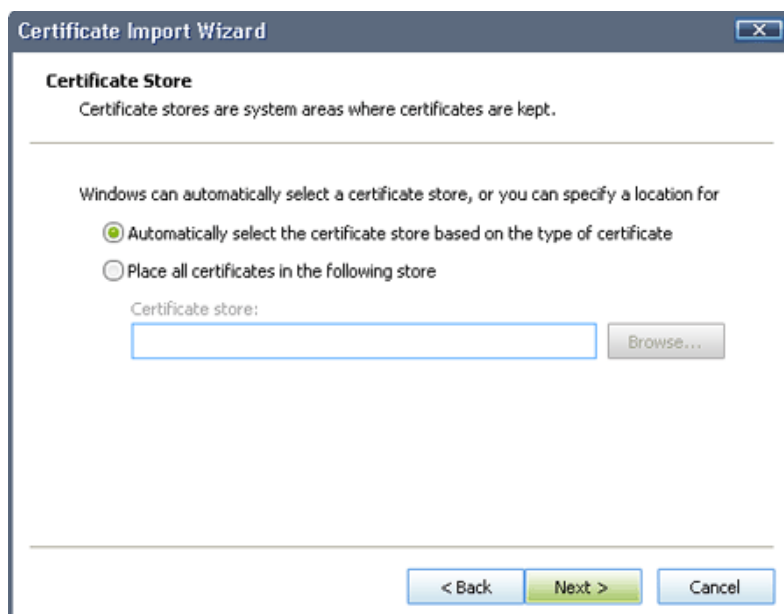
Click 'Next' to continue.



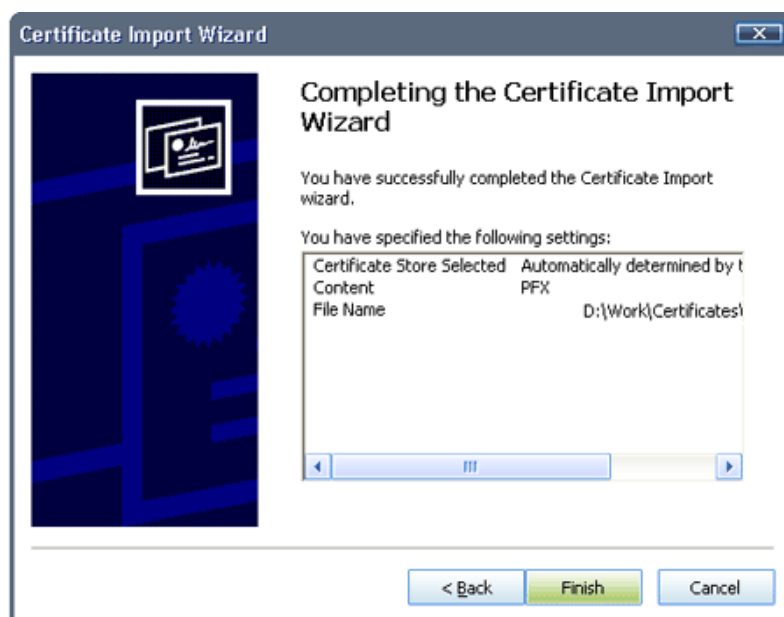
3. If the private key on the certificate is password protected (a highly recommended practice) you will need to enter it before continuing. Note - you should only see the request for a password when you are importing into the 'Personal' email store. This is because certificates in this store are used to digitally sign outgoing messages - and in order to do that, SecureEmail needs to access the private key of the certificate. It is a fundamental principle of PKI based security systems that the private key of your certificate is known and available only to you - so it is absolutely critical that your private key is password protected.



4. Select the certificate store for your certificate. It can be selected automatically (recommended for most users) or manually. (Note: If the certificate you are installing has a private key then this means it is a personal certificate and will be imported into the 'Personal Certificate' store and made available for digitally signing your email messages. If there is no private key with the certificate it is a contact's certificate and will be imported into the 'Other People's' store so you can encrypt messages to that contact)



5. Check the settings you have specified:



6. Click 'Finish' to complete the import process. The pop-up window shows you that import was successful.



7. Click 'OK'. Depending on the store you imported to, the certificate will now be visible in the 'Personal' or 'Other People' lists.

## Certificate Manager

The 'Certificate Manager...' button opens the full Windows certificate store within the SecureEmail interface - allowing fast, centralized management of every certificate type installed on your computer. Apart from the 'Personal' and 'Other People's' tabs, the Certificate Manager also displays intermediary CA certificates; trusted root certificates and trusted and untrusted publishers. You can see the exact same thing in Internet Explorer by browsing to: `Tools > Internet options > Content > Certificates`.

The full certificate manager allows you to perform all the import/remove/inspect functionality available via [Certificate Settings](#) as well as additional options such as exporting certificates and other advanced options.

## 6.5 Protocols

The 'Protocols' tab allows you to manage the ports that SecureEmail will monitor for POP, SMTP and IMAP messaging protocols.



SecureEmail will automatically import your port settings from previously configured mail accounts in Outlook, Outlook Express and Thunderbird. For all other supported and unsupported mail clients, SecureEmail uses the following default ports:

POP3 – port 110    Secure POP3 - port 995

SMTP – port 25    Secure POP3 - port 465

IMAP – port 143    Secure IMAP - port 993

For example, Incredimail is supported but SecureEmail will not automatically detect and import the port settings - rather it will use the defaults listed above. If your set-up utilizes different ports to those listed above, or if your port settings have been changed after installing SecureEmail, then you will need to manually configure them. (Tip - if SecureEmail does not seem to 'catch' either incoming or outgoing mail then it is worth checking which port numbers your mail server and mail client are using and cross reference with those specified in the 'Protocols' section).

[Click here](#) for a step-by-step guide to adding and modifying your protocol and port settings.

### **Background:**

**POP3** - (Post Office Protocol) is the standard data protocol for delivering emails across the Internet. This protocol is used for incoming emails. Major clients such as Outlook, Outlook Express and Thunderbird will, by default, use POP3 on port 110 (995 - [Secure Connection](#)) for your incoming mails. If you use Outlook, Outlook Express or Thunderbird then SecureEmail will also automatically import and monitor any non-standard ports you have specified.

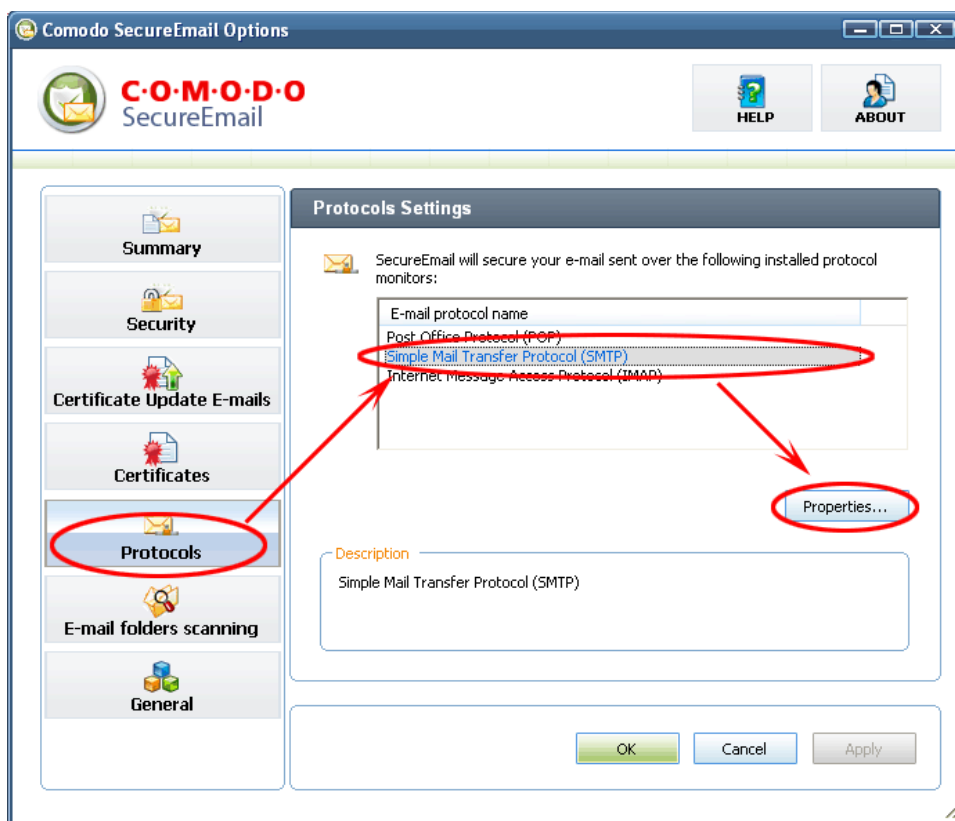
**SMTP** - (Simple Mail Transfer Protocol) is the most widely used standard for sending emails across the Internet. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified (and in most cases verified to exist) and then the message text is transferred. Major clients such as Outlook, Outlook Express and Thunderbird will be configured by default to use SMTP on server port 25 for your outgoing mails.

**IMAP** - (Internet Message Access Protocol) IMAP is an alternative method of distributing email. It is different from the standard POP3 methodology in that with IMAP, email messages are stored on the server, while in POP3, the messages are transferred to the client's computer when they are read. Thus, using IMAP allows you to access your email from more than one machine, while POP3 does not. This is important because some email servers only work with some protocols. Clients using the IMAP protocol will generally be configured to use port 143.

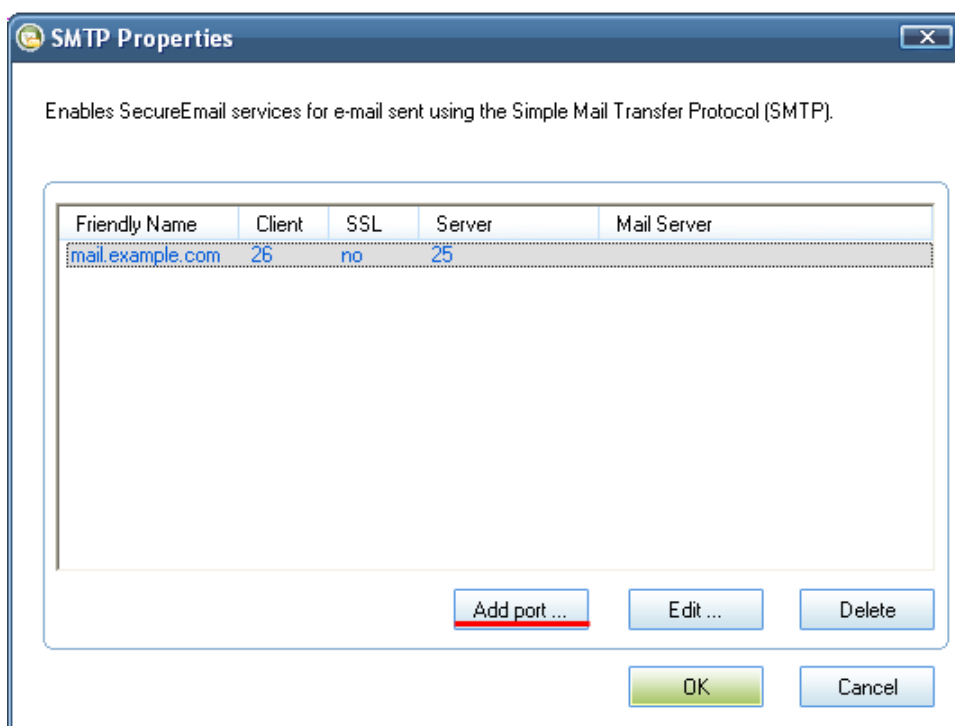
### **Addition and Modification of Monitored Ports for POP3, SMTP and IMAP**

Some email servers will be configured to send and receive through non-standard ports. If you want to have SecureEmail check messages sent through these ports, you should add these extra ports in the **Protocols** section. To add, modify or delete monitored ports.

- Click the **Protocols** button;
- Select the protocol for which you want to add or modify ports;
- Click the **Properties** button;



The following dialog will appear:



- **Add port....** will allow you to specify another port number that you want SecureEmail to monitor. Choose this if your client is configured for more than one mail account and at least one of those accounts uses a different port

to the one listed. If you only have one mail account on your client, you are advised to use the 'Edit...' button and modify the existing port number.

- **Edit....** will allow you to change the currently monitored port number for protocol.
- **Delete....** will remove the port setting - meaning SecureEmail will no longer monitor email traffic passing through the port in question.

In the form that appears enter a friendly name for the port and the port setting. In the graphic below, we have shown the dialog box for adding a port. You will see a nearly identical dialog had you chosen to 'Edit' a port.

**Add a port**

SecureEmail will monitor ports for this protocol only. If you wish to monitor the same port for other protocols you will need to add them for each protocol.

Enter a friendly name and a port number for the port setting.

Friendly Name: Thunderbird outgoing Port

Server port: 2525

Connect to the server over a secure connection (SSL)

Please enter the mail server that you are using for the secure connection. This field is required to enable CSE to correctly establish trust using the mail server's certificate.

Mail server:

Use a different e-mail client and server connection port

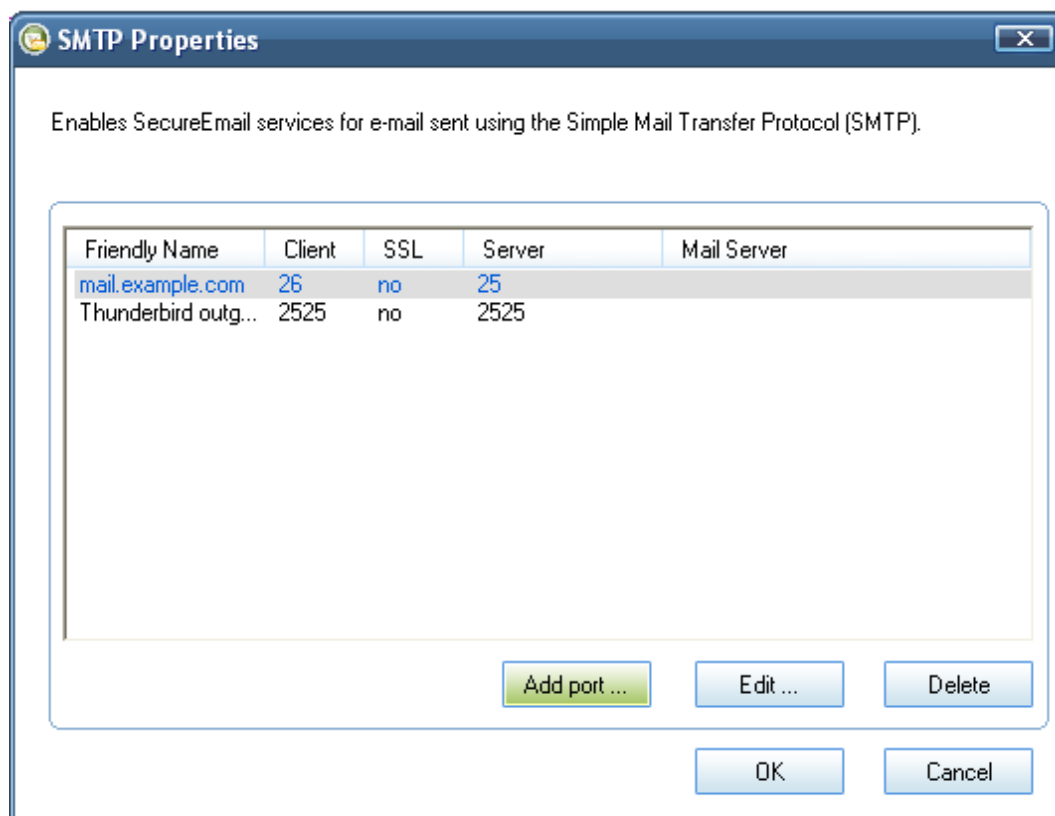
Set different e-mail client ports if you have two accounts connecting to the same server port where one or both require a secure connection. If you have more than one secure connection set a different client port for each secure connection.

E-mail Client port: 2525

OK Cancel

### To add a new port

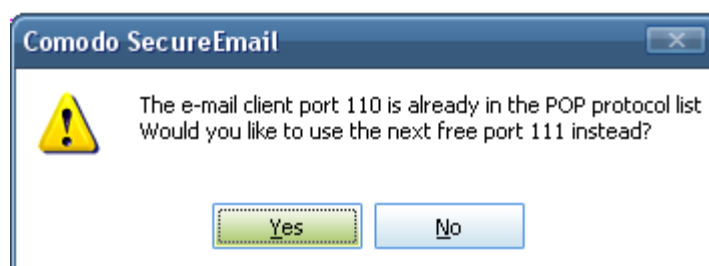
1. Enter a name (for your reference) in the **Friendly Name** text box.
2. Enter the port number you want to monitor. (To make sure that you are not entering the ports which are already in the list and used by the same or other protocols or the ports which are already monitored in another Comodo application(s) like Comodo AntiSpam, see the [notes](#) below. )
3. When finished, click **OK** . Your changes will be shown in the properties dialog (see below).

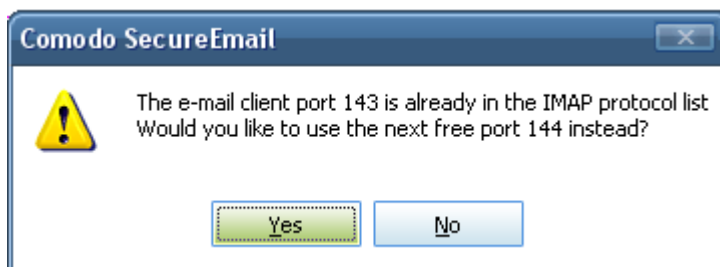
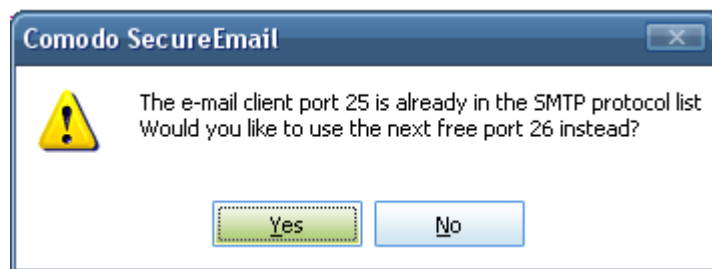


4. Click **OK** to confirm the new settings for the protocol.
5. Finally, remember to also click 'OK' when you return to the main 'Protocol Settings' area. This will instruct SecureEmail to begin monitoring the new ports.

**Notes:**

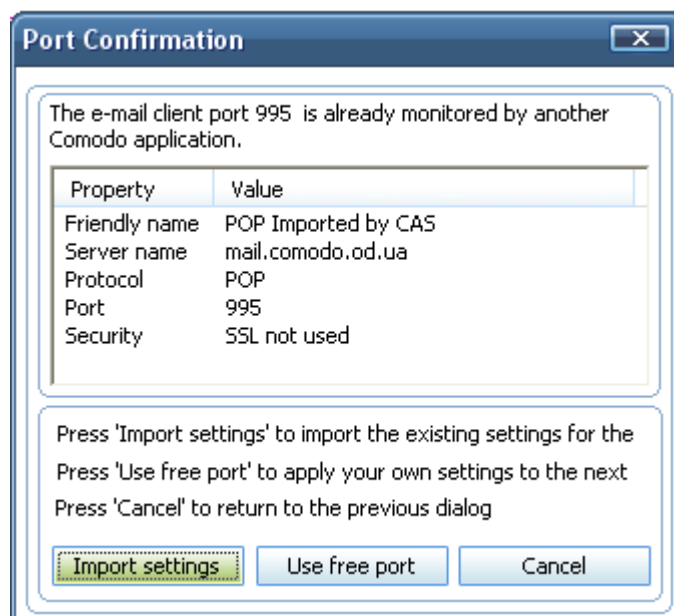
1. If you have entered a port number which already exists in the email client ports list of the same or another protocol, and clicked **OK**, one of the following dialogs will appear, as appropriate:





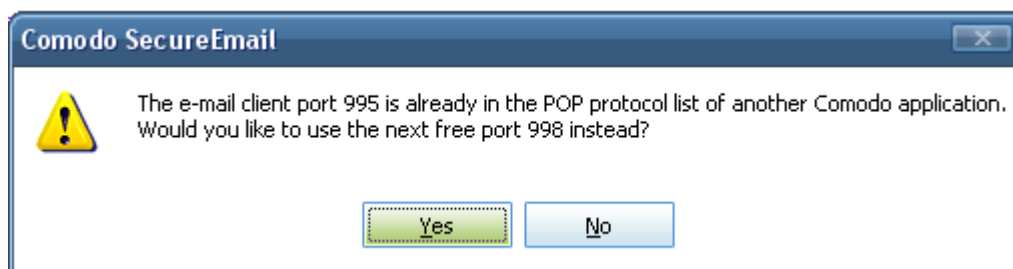
If you click **Yes**, the port with the next free email client port will be added to this protocol ports list and the 'Add a port' dialog will be closed. If you click **No**, the 'Add a port' dialog will be displayed again.

2. If you have entered a port number which is already monitored in another Comodo application(s) like Comodo AntiSpam, under the same protocol, and clicked **OK**, the following dialog will appear.



- If you click **Import settings** button, this port will be imported and added to the protocol ports list, with imported settings, and the 'Add a port' dialog will be closed.
- If you press **Use free port** button, the next free email client port will be used and the settings that you entered in 'Add a port' dialog will be added to the ports list. The 'Add a port' dialog will be closed.
- If you press **Cancel**, button. 'Add a port' dialog will be displayed again.

3. If you have entered a port number which is already monitored by a different protocol in another Comodo application, and clicked **OK**, the following dialog will appear.



- If you click **Yes**, the free port and the settings that you have entered in 'Add a port' dialog will be added in the ports list. The Add port dialog will be closed. If you click **No**, the 'Add a port' dialog will be displayed again.

These rules also apply for “**Edit a port**” dialog.

### 6.5.1 Configuring SecureEmail for SSL connections

---

If your mail server requires an SSL connection for encryption and/or user authentication purposes then you need to take the following additional steps:

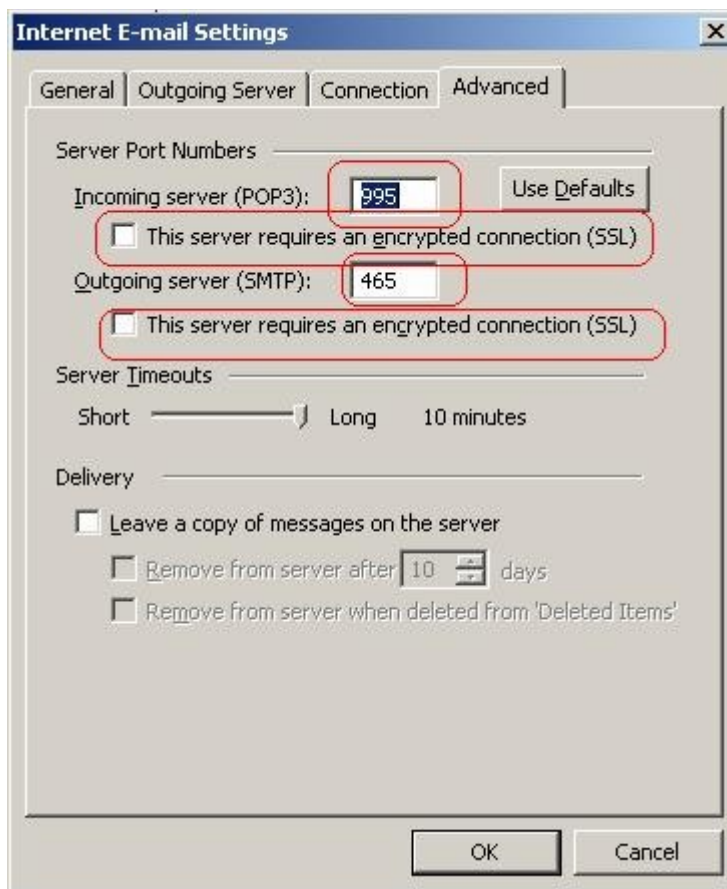
- Switch off SSL connections in your mail client .
- Make sure your mail client is configured to connect using the correct ports
- Switch on SSL connections in the 'Protocols' section of Comodo SecureEmail so it can handle the secure connection to the mail server instead of the client. ( See this FAQ for a graphical explanation of SecureEmails positioning at the network layer)

#### Switch off SSL connections in your mail client

##### To switch off SSL connections in Outlook and Outlook Express

1. Open Outlook/Outlook Express.
2. Select Tools > Email accounts....
3. Select 'View or change existing accounts'. (CSE will have imported the port settings for any existing mail account)
4. Choose the account you wish to modify and click 'Change....'
5. Click 'More Settings.....'
6. Next, click the 'Advanced' tab. Make sure:
  - Both '....encrypted connection (SSL)' boxes are **NOT** checked (see graphic below)

7. Set '995' for the POP3 port and '465' for the SMTP port. These are the most widely used default port numbers for SSL connections. (see graphic below)



### Switch on SSL connections in the 'Protocols' section of Comodo SecureEmail

To enable SSL connections in Comodo SecureEmail you need to configure both POP and SMTP in the 'Protocols' section of the application:

- Open the SecureEmail configuration interface by clicking '[Start > Comodo > SecureEmail > SecureEmail Configuration](#)'
- Click the 'Protocols' button on the left hand menu
- Choose 'Post Office Protocol (POP)' from the [list of protocols](#) and click 'Properties'
  - If you wish to modify an existing account for SSL connectivity then select the target account and click 'Edit.....'
- If you wish to add a new mail account that requires SSL connectivity, then click 'Add Port...'
- This will open the port configuration screen for that protocol (see below)

**Edit a port**

SecureEmail will monitor ports for this protocol only. If you wish to monitor the same port for other protocols you will need to add them for each protocol.

Enter a friendly name and a port number for the port setting.

Friendly Name:

Server port:

Connect to the server over a secure connection (SSL)

Please enter the mail server that you are using for the secure connection. This field is required to enable CSE to correctly establish trust using the mail server's certificate.

Mail server:

Use a different e-mail client and server connection port

Set different e-mail client ports if you have two accounts connecting to the same server port where one or both require a secure connection. If you have more than one secure connection set a different client port for each secure connection.

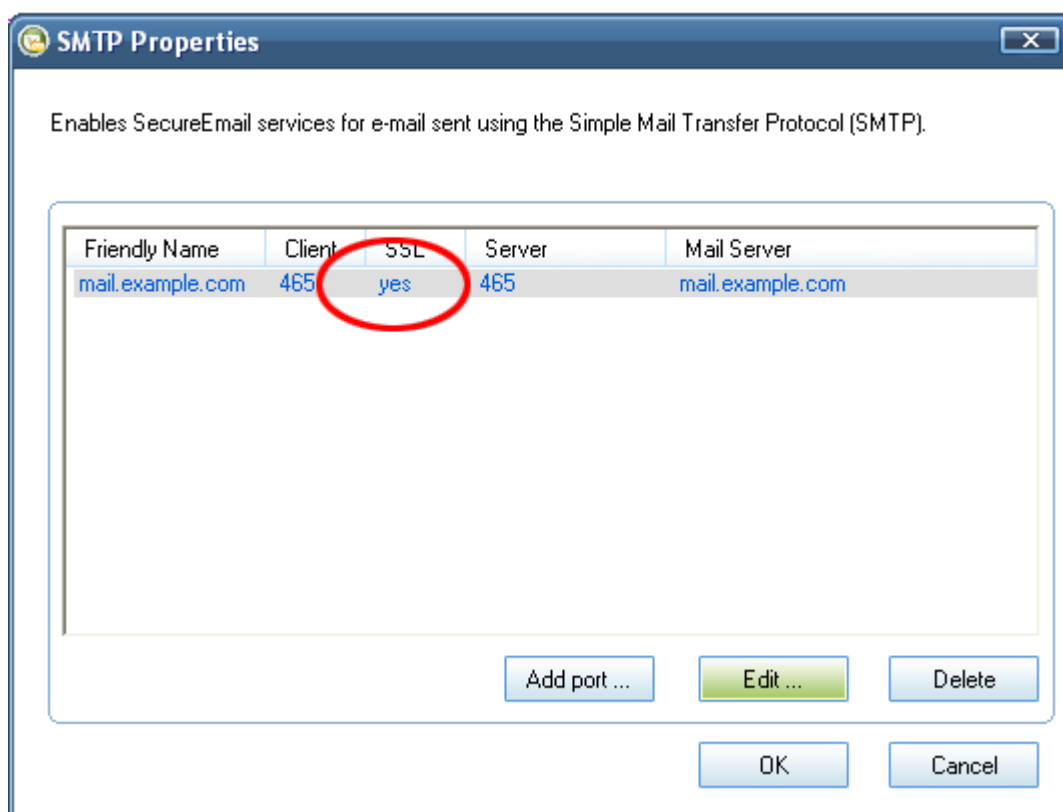
E-mail Client port:

OK Cancel

- If required, type a friendly name for the port setting (e.g. Friendly Name = 'My Secure POP Connection')
- Type '995' in the 'Server Port' field
- Check the box 'Connect to the server over a secure connection (SSL)' to enable SSL connectivity
- Next, you must enter the full name of your mail server in the 'Mail Server' field (e.g. mail.example.com). This is used to authenticate the mail server against the common name (CN) field of the mail server certificate and thus correctly establish the trust relationship. If you are 'editing' an existing port then this field will usually be pre-populated with the name of the mail server for that port. If you are adding a new port then you will need to type the name of your mail server here.
- If you have two accounts connecting to the same *server port* (for example, port 995), but only one of those accounts requires an SSL connection then you need to specify a different *email client port* for that account in order to avoid errors. To do this check the box - 'Use a different email client and server connection port' and type a (random unused) ephemeral port (1024 through 4999) number (e.g. 1994). Comodo SecureEmail will still connect to the *server port* 995 for both accounts but will only establish an SSL connection to the account with the email client port number of 1994. In addition if you have more than one secure connection set a different *email*

*client port* for each secure connection to enable Comodo SecureEmail to establish trust with the correct server certificate.

- Click 'OK' to confirm your choices. You will be returned to the 'POP3 Properties' dialog. The 'SSL' column now indicates that a secure connection is being used on the client email port for that account.

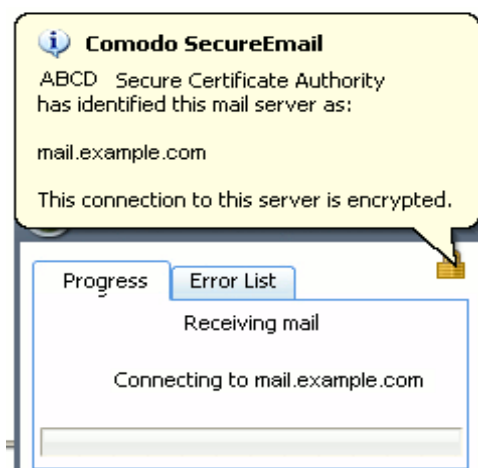


- Repeat the process for the SMTP protocol. For SMTP, you should type '465' in the 'Server Port' field.
- If necessary, repeat the process for the IMAP protocol, using '993' as the default SSL server port.

### Notification of Secure Connection

Once you have set up an SSL connection as outlined above, SecureEmail will attempt to authenticate the mail server every time you connect to it to send or receive mail. If the certificate on the mail server was issued by a trusted Certificate Authority (CA) such as Comodo or Verisign then you will see a Gold Padlock on the pop-up notification - indicating (i) you have established a secure, encrypted connection to the mail server (ii) that the company that owns the mail server has been validated by a trusted third party (a certificate authority). The image below-left shows a typical SSL connection to a mail server with a certificate issued by trusted Certificate Authority:

### Trusted Authority

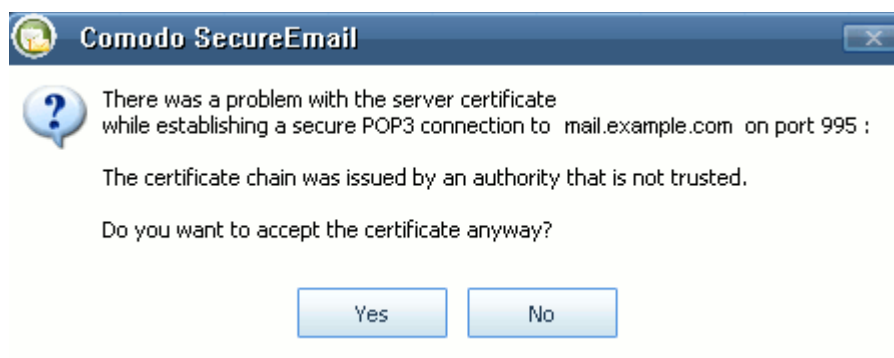


### Untrusted Authority (e.g. self signed certificates)



If the padlock has a red circle with a white exclamation mark over it then this indicates that there is a problem with the authentication process (see image above-right). This could be for many reasons, but the most likely are:

- The host names do not match. Hover your mouse over the padlock to view the mail server certificate details. Check that the host name shown here matches the one you configured in SecureEmail and your mail client.
- The certificate on the server has expired. (Comodo offer a full range of SSL certificates suitable for securing corporate mail servers - including Unified Communications Certificates for Exchange 2007 servers. See [EnterpriseSSL.com](http://EnterpriseSSL.com) for more details )
- The mail server is using a certificate signed by an untrusted certificate authority - including self signed certificates (these certificates are usually created and deployed by the mail server administrator ). The connection to the mail server is still encrypted but, because the certificate was not issued by a recognised CA, it is not possible for SecureEmail to authenticate the mail server is operated by a trustworthy organization. Comodo SecureEmail will advise you that you are about to make a secure connection to a mail server that has an untrusted certificate with the following dialog:

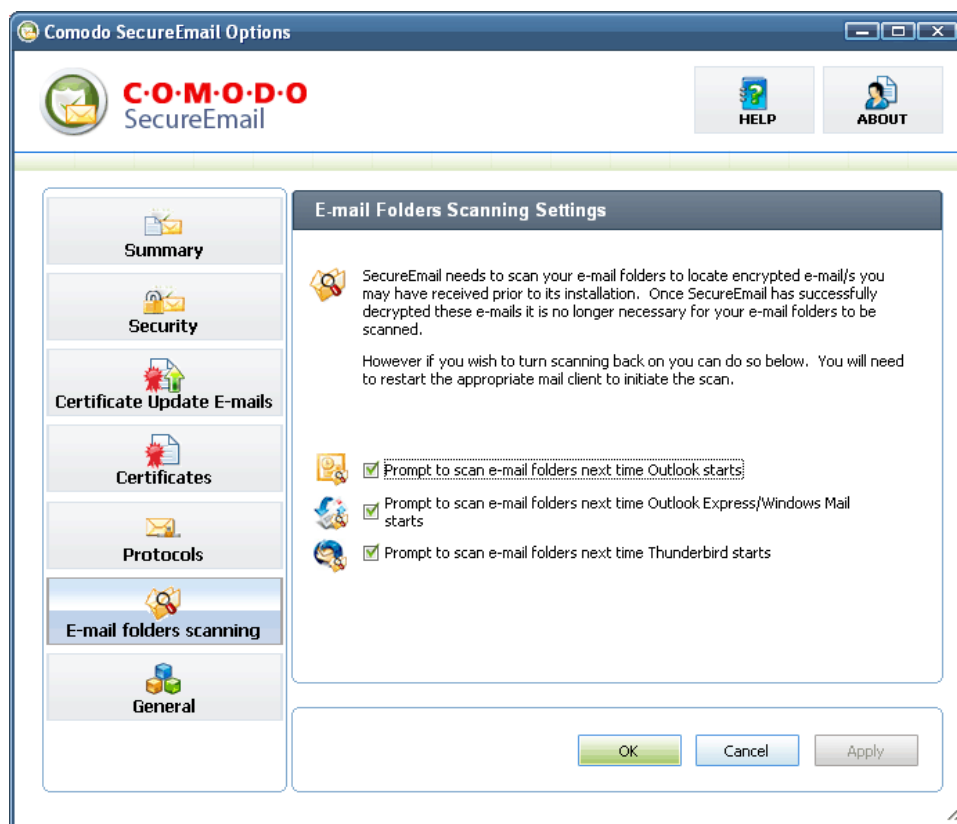


If you are sure that it is safe to connect to the mail server (for example, you have a pre-established trust relationship) then click 'Yes'. If you do not wish to connect to the mail server, click 'No'. If you are a network administrator and would like to purchase a fully trusted, Comodo SSL certificate for your company's mail server, then please visit [EnterpriseSSL.com](http://EnterpriseSSL.com).

## 6.6 Email Folders Scanning

After Comodo SecureEmail has been installed, you will be asked whether you would like to scan your inbox for encrypted messages the next time you start your mail client. Selecting 'Yes' will allow SecureEmail to detect and automatically decrypt any messages encrypted with a single use certificate that you received **before** you installed the program.

Although this is a one-off process and it should not be necessary to re-scan again, users have the option to enable recurrent scanning in the 'Email folders scanning' section of the application.



To enable this option, check the box against the email client(s) you use and click 'OK'

Make sure you click 'OK' to apply the change.

Now, every time you restart your mail client you will be prompted to confirm that you wish to scan your Inbox.



- If you wish to commence this particular scan of your Inbox, click 'Yes'
- If you wish to stop this particular scan of your Inbox, click 'No'
- If you wish to de-activate future scanning everytime your mail client is re-started, check the box '*Stop scanning email folders for SecureEmail encrypted emails*' before making your 'Yes' or 'No' choice for this particular scan.

When SecureEmail has finished scanning your inbox, it will present you with the results and ask you whether you want to scan your remaining email folders.

For example, if you have no single-use encrypted emails in your inbox you will be see the following dialog:



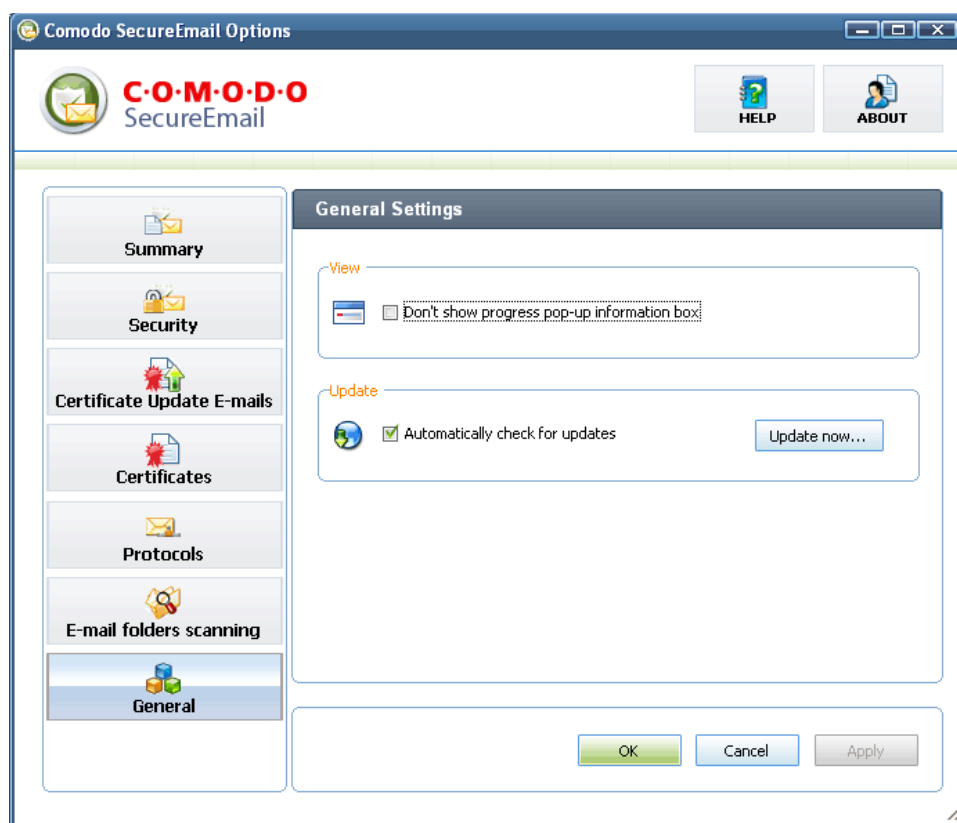
Clicking 'Yes' will begin the full scan of your remaining email folders. Click 'No' to exit the scanning wizard.

## 6.7 General

---

The 'General' management interface allows you to configure miscellaneous settings concerning the overall behavior of Comodo SecureEmail application. Click on **General** button to access this interface. The configuration settings can be done for:

- [View](#)
- [Update](#)



**Don't show progress pop-up information box** - Checking or unchecking this box determines whether or not SecureEmail should generate progress notification pop-ups like the one shown below.



Comodo advise that users leave this setting unchecked so notifications are 'Enabled'. These notifications provide a real time indicator of actions that SecureEmail is taking and can be valuable if you are attempting to troubleshoot any problems. However, should you wish to switch them off, simply check the box.

**Automatically Check For Updates** - When this setting is activated, SecureEmail will automatically connects to the Comodo servers to check for product updates in the background. If you are not currently running the latest version, you will be alerted via a message box and asked whether you wish to install the latest version of the software. Comodo advises users to leave this setting at the default of 'Enabled'.

## To manually check for updates

1. Click **Update now** button. The Upgrade Wizard is started.



2. Click **Next**. The wizard searches for a new version.



If there is a new version available, you will be prompted to download and install the latest version of Comodo SecureEmail.

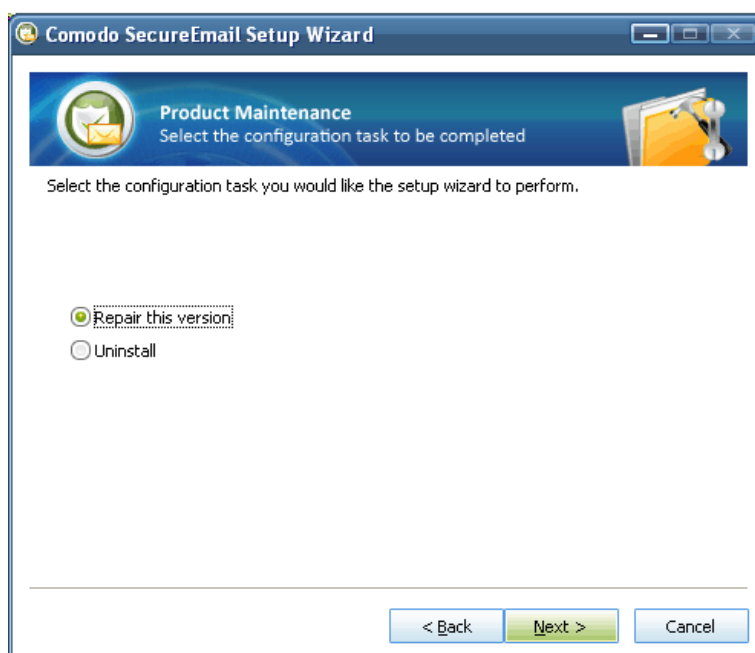
## 7 Repairing SecureEmail

Comodo SecureEmail features a repair option which allows the users to repair the application installed in their system. This is very useful the installed version of the application is not working properly for some reasons.

### Welcome Screen

To initiate the repair process, double click on Setup.exe  of the downloaded Comodo SecureEmail setup.

A welcome screen is displayed.

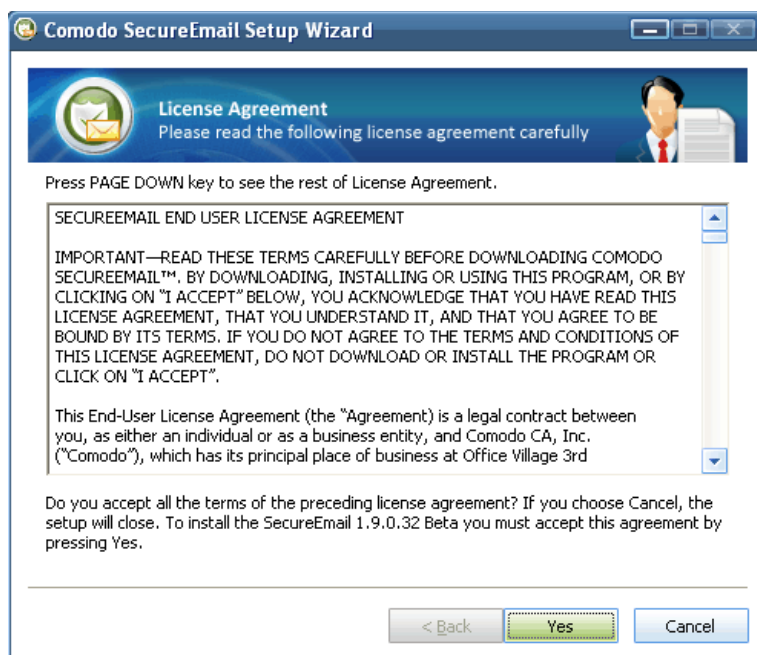


Select Repair this version if you want to repair the existing installation or select Uninstall, if you want to uninstall Comodo SecureEmail from your system and click Next.

**Note:** Selecting Uninstall and clicking Next will open the [Uninstallation wizard](#).

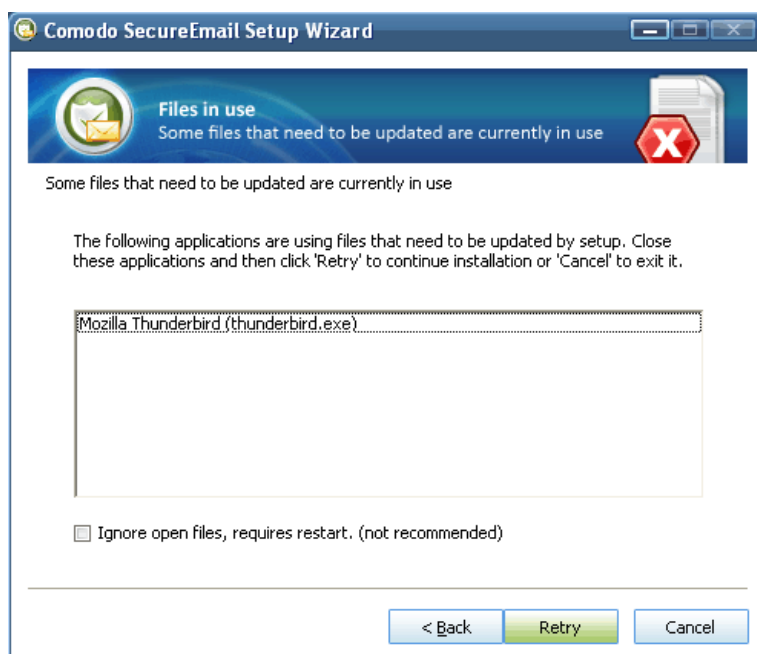
### End User License Agreement

In order to repair the installation, you must first read and accept the license agreement:



Click 'Yes' to accept and continue repairing. Click 'Cancel' to decline and exit.

Please ensure that all other Windows programs are closed before continuing with the installation. If you have your mail client open during this installation process, the following screen is displayed.

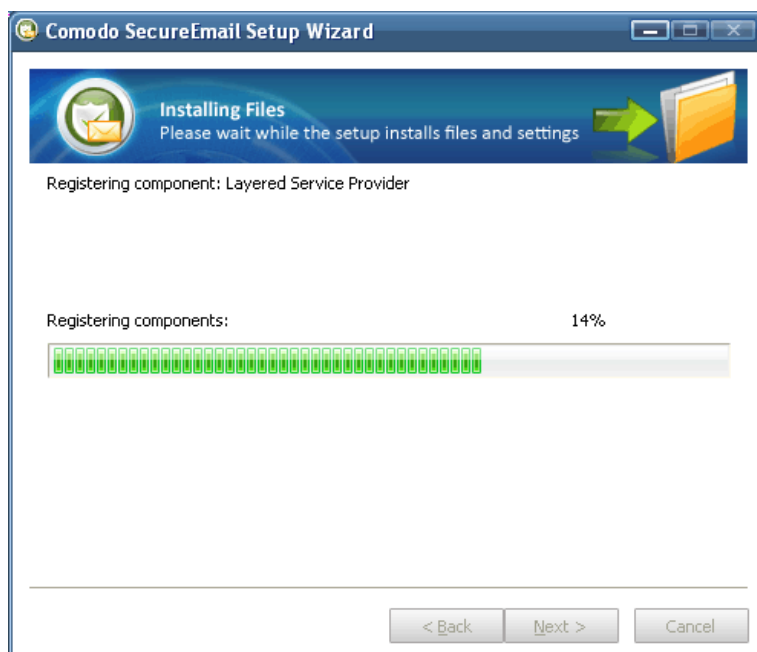


Close your email client and click Retry.

**Note:** If you do not have your email client open, this dialog is not displayed and the process moves to the next step.

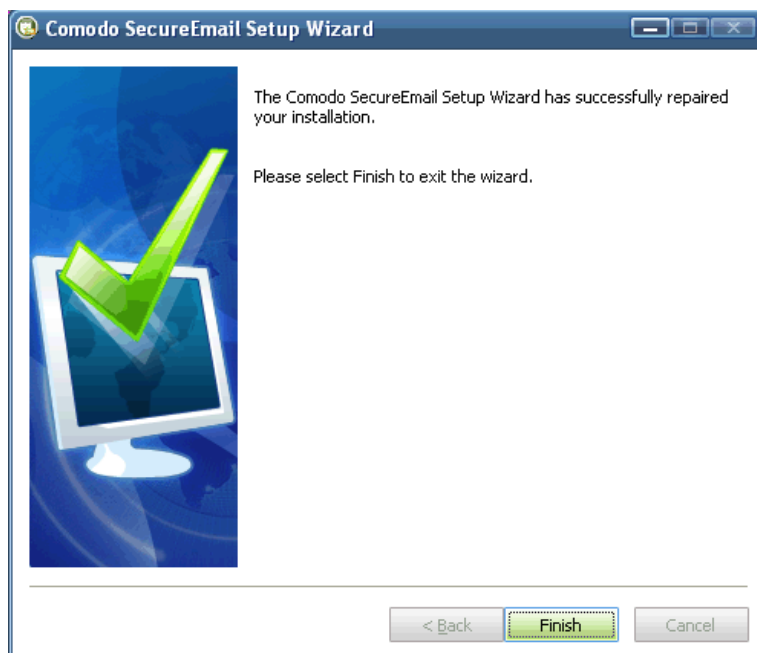
## Repair Progress

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



## Installation Complete

A confirmation dialog box will be displayed indicating successful completion. Click Finish to exit the wizard.



## 8 Uninstalling SecureEmail

---

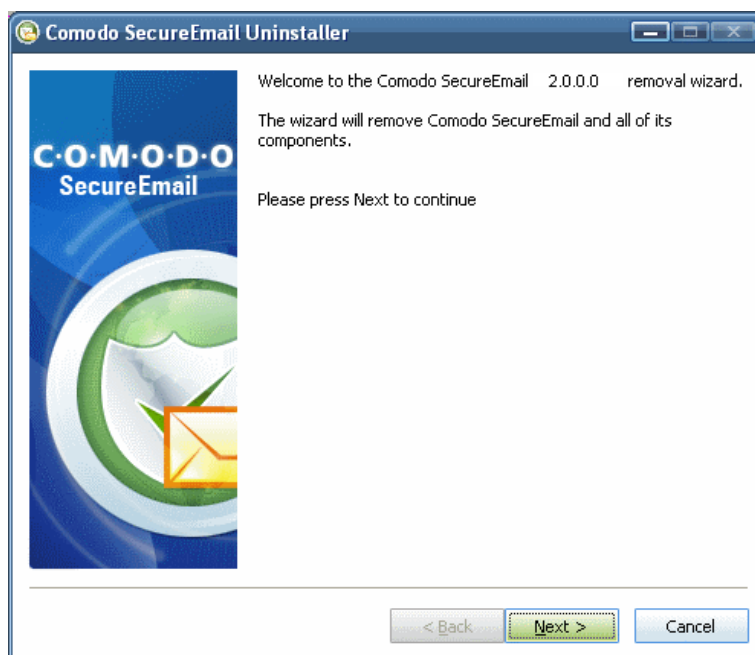
### To uninstall SecureEmail

- Click Start > Settings > Control Panel
- In the Control Panel, double-click Add/Remove Programs
- In the list of currently installed programs, click SecureEmail
- Click the 'Change/Remove' button.

**OR**

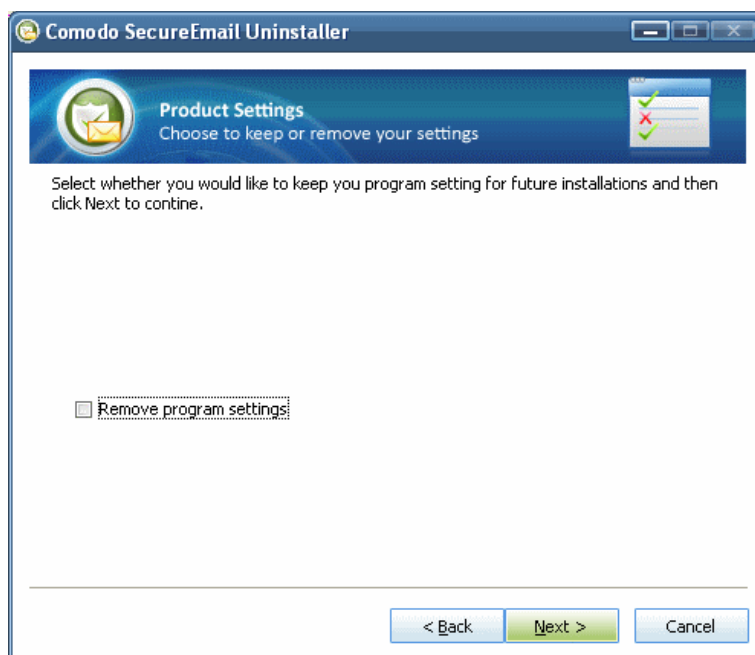
- Click Start > Programs > Comodo > SecureEmail > Uninstall SecureEmail.

A welcome screen for uninstallation is displayed.



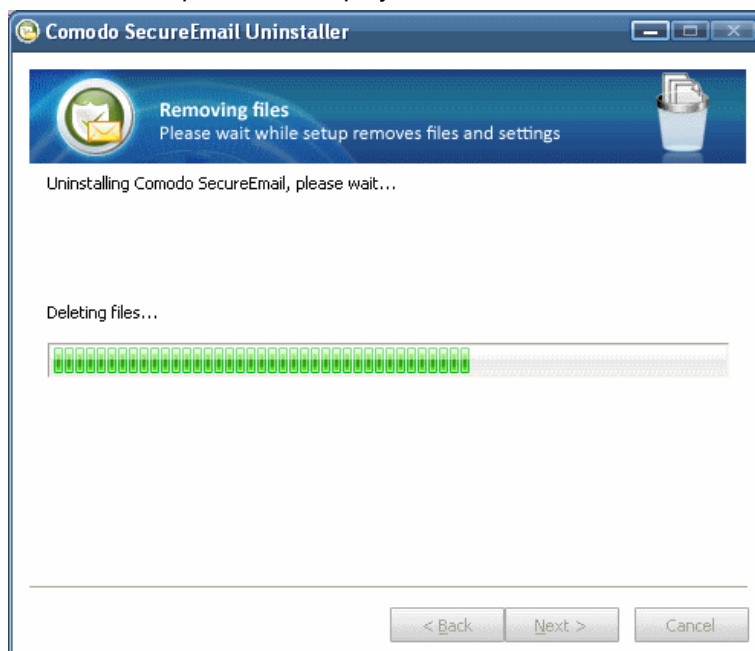
Click **Next**.

A Product settings window is displayed.

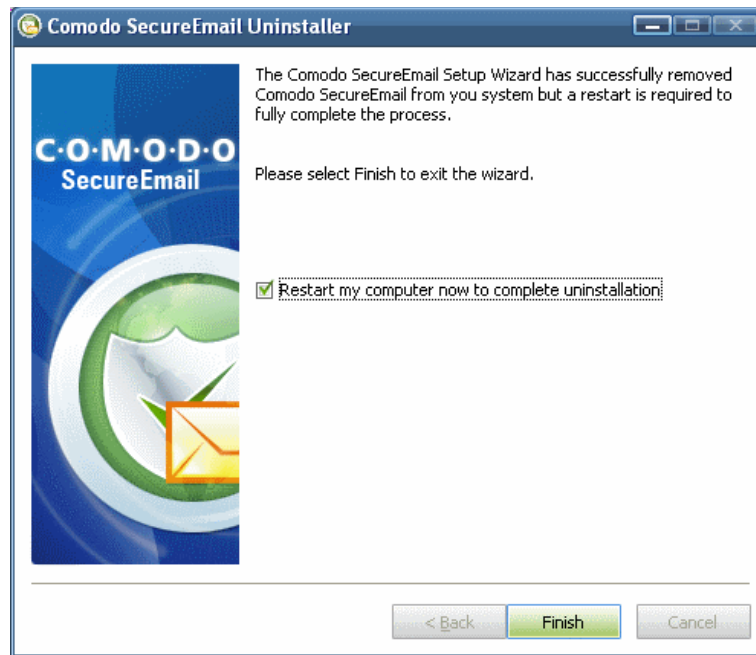


**Remove Program Settings** - The program settings for the version of Comodo SecureEmail to be uninstalled is maintained in your system, in order to aid you in configuring the application if you are going to reinstall or update the application. If you are going to reinstall or update the application, leave this option unchecked. If you are going to completely remove the application from your system, check this option and click **Next**.

A progress bar indicating the uninstallation process is displayed.



On completion, click **Next**.



Click **Finish** to complete the uninstallation process and to restart the system. If you wish to restart the system later, uncheck **Restart my computer now to complete uninstallation** and click **Finish**. The application will be completely removed only on restarting your system.

## FAQ

---

### Comodo SecureEmail mini-FAQ

- [What operating systems do SecureEmail and SecureEmail Pro support?](#)
- [Which email clients does SecureEmail support?](#)
- [Does SecureEmail work with POP/SMTP mail clients other than Outlook, Outlook Express and Thunderbird and Incredimail?](#)
- [What's the difference between the Home and Pro versions of SecureEmail?](#)
- [Will my port settings be imported into SecureEmail?](#)
- [I already have an email certificate from a vendor other than Comodo CA. Will SecureEmail work with my certificate?](#)
- [Is there any software that has compatibility issues with Comodo SecureEmail?](#)
- [How do I get a Comodo certificate?](#)
- [I've downloaded an encrypted email before I installed SecureEmail and before I had installed my Comodo CA certificate. How do I decrypt a SecureEmail email that I've already received?](#)
- [Do I have to disable encryption and signing \(S/MIME\) in my email client?](#)
- [How do I configure Secure Email to connect to an SSL secured mail server?](#)
- [Why are some mails not signed?](#)
- [Why isn't the SecureEmail auto decryption footer added to some decrypted emails?](#)
- [Where does SecureEmail store my certificate and my contacts' certificates?](#)
- [What are single-use certificates?](#)
- [How can I stop SecureEmail encrypting emails with single-use certificates?](#)
- [Why would I send a 'Clear text Attachment'? Doesn't that defeat the whole point of encryption?](#)
- [How do I back up my email certificate?](#)
- [How do I install/import my certificate again if I have saved it in Personal Information Exchange \(.pfx\) format?](#)

### What operating systems do SecureEmail and SecureEmail Pro support?

<b>32 bit versions of SecureEmail support:</b> Windows Vista Windows XP SP2 (32 bit) Windows 2000 SP4 (32 bit)	<b>64 bit versions of SecureEmail support:</b> Windows Vista (64 bit) Windows XP SP2 (64 bit)
---	---



### **Which Email clients does SecureEmail support?**

SecureEmail is confirmed to support:

- Outlook 2000 and above;
- Outlook Express 5.5 and above;
- Thunderbird 1.5 and above;
- Windows Mail;
- Incredimail;
- Windows Live Mail;
- Eudora.



### **Does SecureEmail work with POP/SMTP/IMAP mail clients other than Outlook, Outlook Express and Thunderbird and Incredimail?**

SecureEmail should work with most Windows mail clients that use POP, SMTP or IMAP messaging protocols. Users are encouraged to contact the Comodo Forums to report any problems experienced when using SecureEmail with alternative mail clients.



### **What's the difference between the Home and Pro versions of SecureEmail**

- Pro version can be configured to encrypt and decrypt messages using certificates from any vendor whereas the Home version can only encrypt/decrypt using a Comodo email certificate. This is an especially important feature in a corporate environment when employees will be likely to receive messages encrypted using email certificates from C.A.s other than Comodo.
- Pro version can only sign messages with a Comodo corporate email certificate. It cannot use Comodo free email certificates to sign messages.
- Home version can sign using Comodo free or corporate email certificates but cannot encrypt using 3rd party certificates.
- Future developments planned for the Pro version included Key ESCROW and central management of network installations.

	<i>Home Version</i>	<i>Pro Version</i>
Automatic Encryption and Signing of Email	✓	✓
Encrypt with one-time use session certificates	✓	✓
Read encrypted mails using web-reader service	✓	✓
Automatic certificate exchange and installation	✓	✓
Built-in Wizard for easy certificate sign-up	✓	✓
Automatic import of mail settings	✓	✓
Encrypt with 3rd Party Certificates	✗	✓
Sign with Comodo Free Certificates	✓	✗
Sign with Comodo Corporate Certificates	✓	✓



**Will my port settings be imported into SecureEmail?**

Yes. SecureEmail will automatically import your port settings from previously configured mail accounts in Outlook, Outlook Express , Thunderbird, Windows Mail, Windows Live Mail and Eudora . For all other supported and unsupported mail clients, SecureEmail will use the following default ports:

POP – port 110    Secure POP3 – port 995  
 SMTP – port 25    Secure POP3 – port 465  
 IMAP – port 143    Secure IMAP – port 993

If your mail set-up utilizes different ports to those listed above, then you need to configure SecureEmail accordingly. Click the 'Protocols' button in the main application interface to re-configure them.



**I already have an email certificate from a vendor other than Comodo CA. Will SecureEmail work with my certificate?**

The Pro version of the software will encrypt and decrypt with non-Comodo email certificates but requires a Comodo certificate to digitally sign messages. The home version requires a Comodo certificate for both encryption/decryption and signing.



### Is there any software that has compatibility issues with Comodo SecureEmail?

Comodo SecureEmail may not operate correctly with the following software:

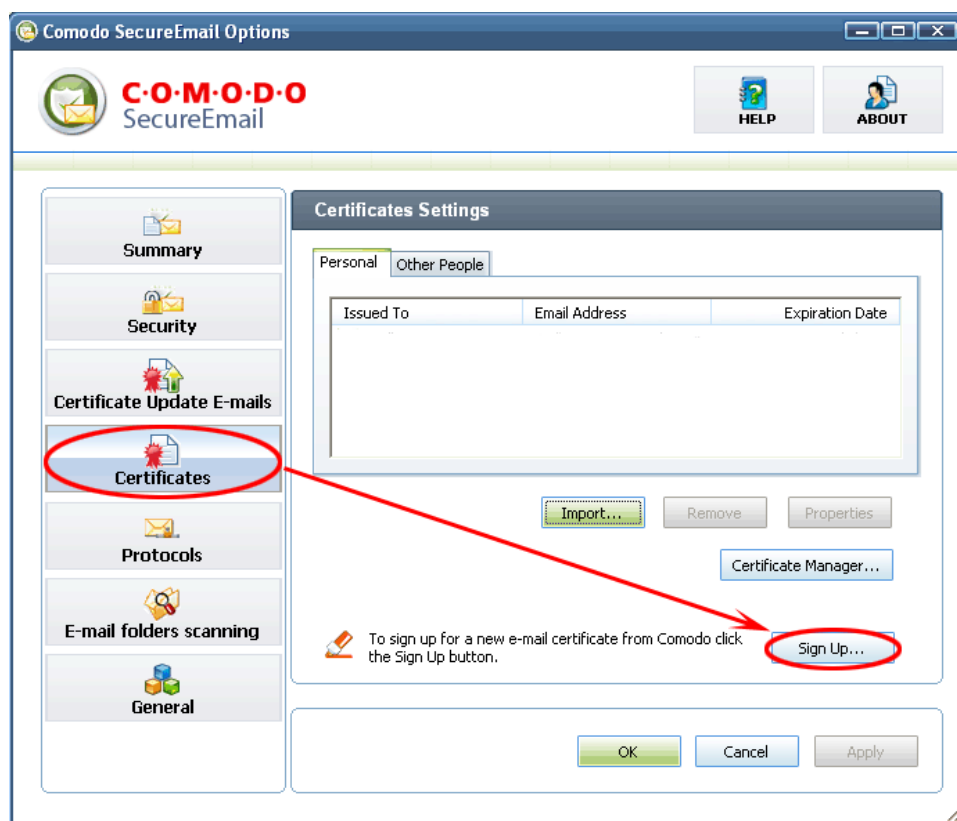
- Panda Antivirus
- Avira AntiVir Premium
- CA Internet Security Suite
- PC Tools Antivirus
- Kaspersky Internet Security 2009
- ArcaVir 2008



### How do I get a Comodo certificate?

Two options: Option 1:

Use the Sign-Up Wizard from the Certificates tab of the SecureEmail main window (see below).



Option 2: Sign up for an email certificate at the Comodo website using the following link:  
[http://www.comodo.com/products/certificate\\_services/email\\_certificate.html](http://www.comodo.com/products/certificate_services/email_certificate.html).



## I've downloaded an encrypted email before I installed SecureEmail and before I had installed my Comodo CA certificate. How do I decrypt a SecureEmail email that I've already received?

There are three choices open to you:

### **For Outlook, Outlook Express and Thunderbird (Windows only) users:**

After Comodo SecureEmail has been installed, you will be asked whether you would like to scan your inbox for encrypted messages the next time you start your mail client. Selecting 'Yes' will allow SecureEmail to detect and decrypt any pre-existing encrypted mails. Although this is a one-off process and it should not be necessary to re-scan again, users have the option to enable automatic scanning in the 'Email folders scanning' section of the application.

### **Other Windows based email client users:**

Forward the email back to yourself (the receiving email address) to enable SecureEmail to intercept it and decrypt the contents.

### **For all other users including Linux and web based email client users:**

To decrypt this email you will need to use the Comodo SecureEmail WebReader service by forwarding the email to `secure-read@secure-email.comodo.com`. You will then receive an email with full instructions of how to proceed.

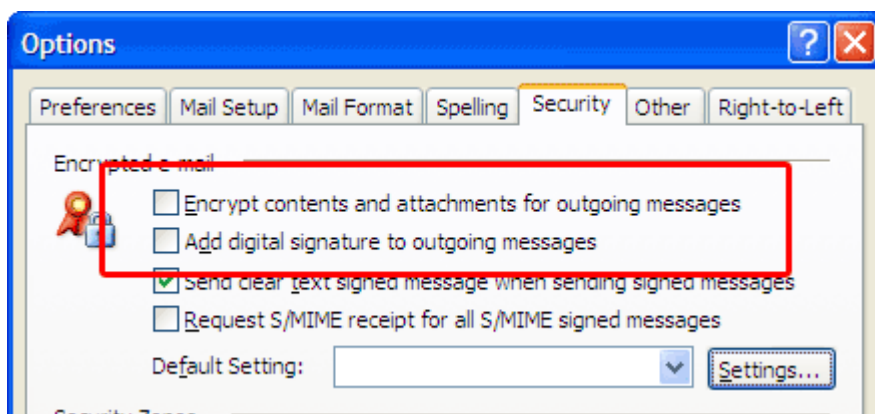


## Do I have to disable encryption and signing (S/MIME) in my email client?

Yes. For smooth operations of SecureEmail it is strongly recommended that you turn off encryption and signing in your email client as both of these duties will be performed by SecureEmail.

For example, in Microsoft Outlook, you should turn off encryption and signing by clicking:

Tools > Options > Security.

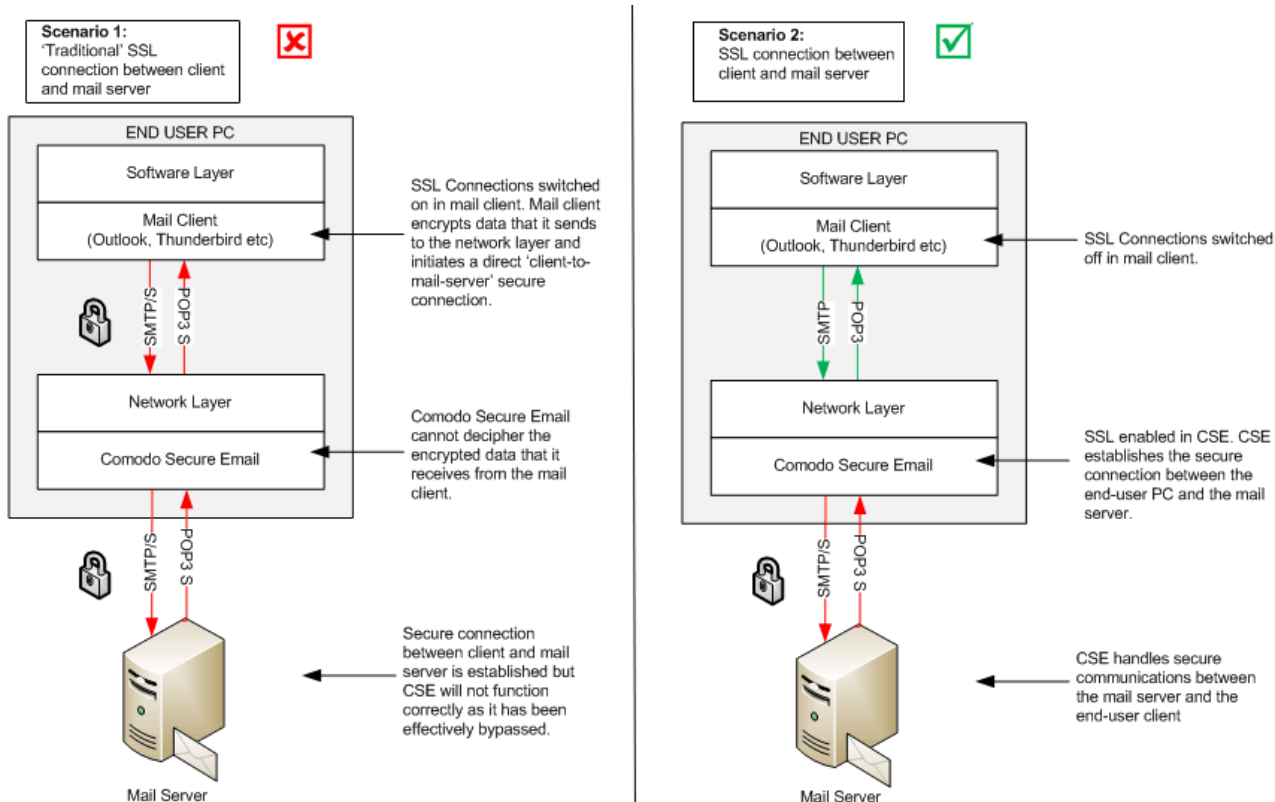


..then make sure the 'Encrypt contents...' and 'Add Digital Signature...' boxes are NOT checked (see below).



## How do I configure Secure Email to connect to an SSL secure mail server?

Because Comodo SecureEmail intercepts traffic at the network layer, you must disable SSL connections in your mail client. Next, you must enable and configure SSL port connection settings for POP3 and SMTP in the SecureEmail 'Protocols' section.



A step-by-step guide to guide to SSL connections under Comodo SecureEmail can be found in the 'Protocols' section of the main guide [here](#).



### Why are some mails not signed?

This could be because your email client has encrypted an email before SecureEmail intercepted it. Please ensure that you have turned off encryption and signing in you email client.



### Why isn't the SecureEmail auto decryption footer added to some decrypted emails?

This is probably because the email was also signed. Adding extra data to a signed email would destroy the integrity of the email's signature, making the signature invalid.



### Where does SecureEmail store my certificate and my contacts' certificates?

SecureEmail uses the standard Microsoft Windows certificate store on your computer to store certificates. You can view these from the Certificates tab in the SecureEmail main window.



### What are single-use certificates?

Single-use certificates are one-time 'session' certificates that enable the encryption of messages to recipients when you do not have their 'regular' email certificate installed on your system. The encrypted email is then sent to the contact and the single-use certificate is uploaded to the SecureEmail servers.

Your recipient then has two options to decrypt and read the email:

(1) Download and install SecureEmail themselves. (a link to the application is included in the notification email). After installation, SecureEmail will automatically scan their inbox in order to decrypt any encrypted messages and allow them to read it.

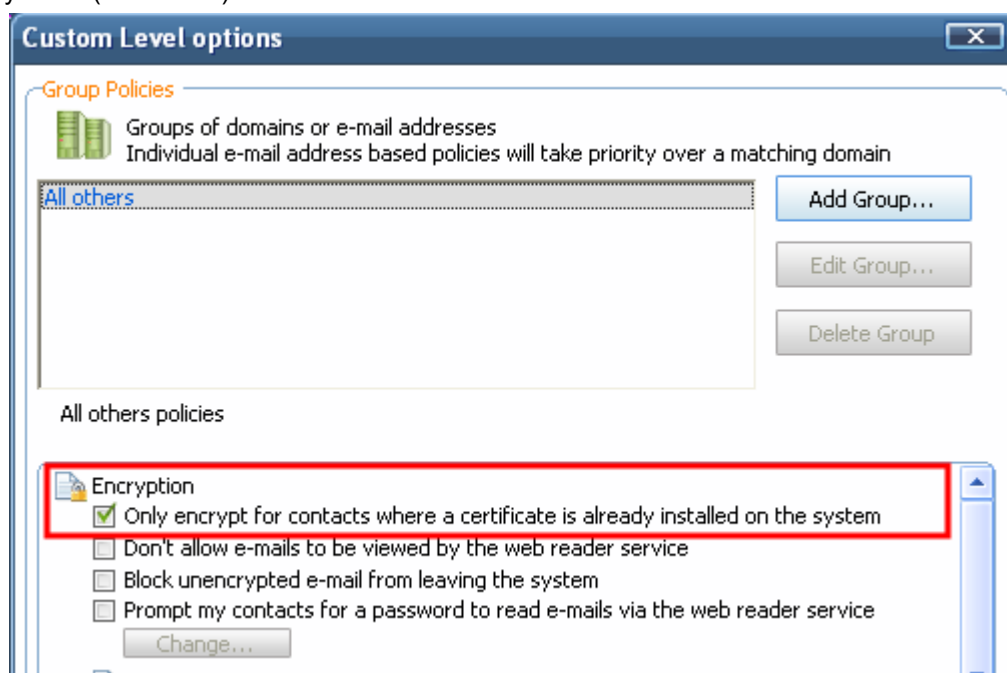
(2) They can also read the mail by simply forwarding your message to [secure-read@secure-email.comodo.com](mailto:secure-read@secure-email.comodo.com) and using Comodo's secure web reader service. Again, full instructions on this process are sent to the recipient in the initial notification email.



### How can I stop SecureEmail encrypting emails with single-use certificates?

You can stop SecureEmail encrypting with single user certificates by selecting:

Security > Custom Level > "Only encrypt for contacts where a certificate is already installed on the system" (see below)

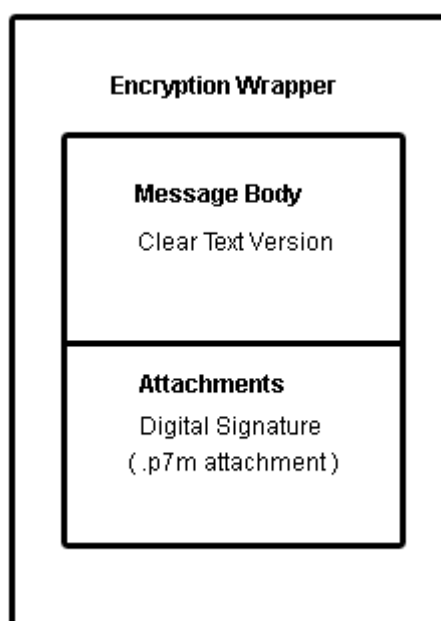


Please note that if you turn off encryption with Single Use Certificates then emails sent to contacts where a certificate is not installed will not be encrypted and will be sent in clear text.



### Why would I send a 'Clear Text' version with a signed and encrypted message? Doesn't that defeat the whole point of encryption?

When an email is digitally signed, the whole email and signature are packaged into a smime.p7m attachment. (i.e. **just** the 'Attachment' area in the diagram below is sent. The message and the digital signature are contained within the .p7m). S/MIME clients like Outlook read this attachment and display the email and signature. Non-S/MIME clients like IncrediMail won't understand what the .p7m attachment is and will show a blank mail with just the .p7m attachment.



#### *Signed and encrypted mail with 'Clear Text Enabled'*

With 'Send Clear text...' enabled, the signature and the message body are *split up* (as in the diagram). S/MIME clients will use the signature to verify the authenticity and integrity of the message whilst non-S/MIME clients will at least be able to display a plaintext version of the mail.

Sending a 'clear text' version of a digitally signed message **does not** compromise the security of an encrypted mail. This is because the encryption part of the equation is carried out on the message **after** it has been signed.

This means the entire signed message, clear text version and all, can only be accessed after the message has first been decrypted - and the only person that can perform this decryption is the intended recipient.



### How do I back up my email certificate and private key?

- Start Internet Explorer then select Tools > Internet Options > Content > Certificates
- On the 'Personal' certificates tab, click on the certificate you want to export and click the 'Export...' button
- Follow the Export wizard. When requested, select **'Yes, export the private key'**, and 'Include all certificates in the certification path, if possible.'
- Type a password which you can remember later.
- Select the save location and give the file a name, but leave the 'Type' as 'Personal Information Exchange (\*.pfx)'.
- Once finished the file and associated private key is saved as a pfx file.



### How do I install/import my certificate again if I have saved it in Personal Information Exchange (.pfx) format

- Copy the .pfx file containing your certificate to the machine on which it is to be installed then double-click the file.
- Follow the wizard and provide the password when requested.
- Let the wizard automatically select the locations for the files to be imported to.



## Glossary

---

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

### A

#### **ACK**

The acknowledgment bit in a TCP packet. (ACKnowledgment code) - Code that communicates that a system is ready to receive data from a remote transmitting station, or code that acknowledges the error-free transmission of data.

#### **Alice**

The names Alice and Bob are commonly used placeholders for archetypal characters in fields such as cryptography. Generally Alice wants to send a message to Bob.

#### **Attached Resource Computer NETWORK (ARCNET)**

ARCNET is a local area network (LAN) protocol, similar in purpose to Ethernet or Token Ring. ARCNET was the first widely available networking system for microcomputers and became popular in the 1980s for office automation tasks. It has since gained a following in the embedded systems market, where certain features of the protocol are especially useful.

### B

#### **Bob**

The names Alice and Bob are commonly used placeholders for archetypal characters in fields such as cryptography. Generally Bob wants to send a message to Alice.

#### **Brute-force**

Brute-force search is a trivial but very general problem-solving technique, that consists of systematically enumerating all possible candidates for the solution and checking whether each candidate satisfies the problem's statement.

#### **Bug**

Error in a program that cause problems.

### C

#### **CA - Certification Authority**

The CA is an authority trusted by one or more users to issue and manage certificates. The CA is the security solution for conducting business on the Internet. The CA ensures that electronic transactions are conducted with confidentiality, data integrity, proper user authentication, and protection against repudiation.

#### **CVSS**

CVSS refers to the Common Vulnerability Scoring System and is a vendor-neutral, industry standard that conveys vulnerability severity and helps determine urgency and priority of response. It solves the problem of multiple, incompatible scoring systems and is usable and understandable by anyone. The CVSS can be understood from the CVSS Base Vectors and CVSS Temporal Vectors.

## CVSS Base Vectors

CVSS vectors containing only base metrics take the following form:  
(AV:[R,L]/AC:[H,L]/Au:[R,NR]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]/B:[N,C,I,A])

The letters within brackets represent possible values of a CVSS metric. Exactly one option must be chosen for each set of brackets. Letters not within brackets are mandatory and must be included in order to create a valid CVSS vector. Each letter or pair of letters is an abbreviation for a metric or metric value within CVSS. These abbreviations are defined below.

Example 1: (AV:L/AC:H/Au:NR/C:N/I:P/A:C/B:C)

Example 2: (AV:R/AC:L/Au:R/C:C/I:N/A:P/B:N)

**Metric:** AV = AccessVector (Related exploit range)

**Possible Values:** R = Remote, L = Local

**Metric:** AC = AccessComplexity (Required attack complexity)

**Possible Values:** H = High, L = Low

**Metric:** Au = Authentication (Level of authentication needed to exploit)

**Possible Values:** R = Required, NR = Not Required

**Metric:** C = Conflmpact (Confidentiality impact)

**Possible Values:** N = None, P = Partial, C = Complete

**Metric:** I = IntegImpact (Integrity impact)

**Possible Values:** N = None, P = Partial, C = Complete

**Metric:** A = AvailImpact (Availability impact)

**Possible Values:** N = None, P = Partial, C = Complete

**Metric:** B = ImpactBias (Impact value weighting)

**Possible Values:** N = Normal, C = Confidentiality, I = Integrity, A = Availability

## CVSS Temporal Vectors

CVSS vectors containing temporal metrics are formed by appending the temporal metrics to the base vector. The temporal metrics appended to the base vector take the following form:

/E:[U,P,F,H]/RL:[O,T,W,U]/RC:[U,Uc,C]

Example 1: (AV:L/AC:H/Au:NR/C:N/I:P/A:C/B:C/E:U/RL:O/RC:U)

Example 2: (AV:R/AC:L/Au:R/C:C/I:N/A:P/B:N/E:P/RL:T/RC:Uc)

**Metric:** E = Exploitability (Availability of exploit)

**Possible Values:** U = Unproven, P = Proof-of-concept, F = Functional, H = High

**Metric:** RL = RemediationLevel (Type of fix available)

**Possible Values:** O = Official-fix, T = Temporary-fix, W = Workaround, U = Unavailable

**Metric:** RC = ReportConfidence (Level of verification that the vulnerability exists)

**Possible Values:** U = Unconfirmed, Uc = Uncorroborated, C = Confirmed

## D

### DHCP

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. DHCP allows devices to connect to a network and be automatically assigned an IP address.

### Debugging

The process of identifying a program error and the circumstances in which the error occurs, locating the source(s) of the error in the program and fixing the error.

### Dynamic IP

The procedure of allocating temporary IP addresses as they are needed. Dynamic IP's are often, though not exclusively, used for dial-up modems.

## E

### End User

The person who uses a program after it's been compiled and distributed.

### EPKI Manager

Enterprise Public Key Infrastructure Manager. The EPKI Manager allows you to issue bulk numbers of:

- SSL Certificates for use on domain names owned by your Company;
- SecureEmail Certificates (S/MIME) for use by employees of your Company.

Your nominated EPKI Manager Administrator(s) will be able to manage all the company's Certificates from a central web based console. Additional certificates may be purchased through the console in minutes; ensuring new servers and employee email may be secured in minutes rather than days. For more information about EPKI Manager click [here](#).

### Ethernet

Ethernet is a frame-based computer networking technology for local area networks (LANs). The name comes from the physical concept of ether. It defines wiring and signaling for the physical layer, and frame formats and protocols for the media access control (MAC)/data link layer of the OSI model. Ethernet is mostly standardized as IEEE's 802.3. It has become the most widespread LAN technology in use during the 1990s to the present, and has largely replaced all other LAN standards such as token ring, [FDDI](#), and [ARCNET](#).

## F

### Fiber-Distributed Data Interface (FDDI)

Provides a standard for data transmission in a local area network that can extend in range up to 200 kilometers (124 miles). The FDDI protocol uses as its basis the token ring protocol. In addition to covering large geographical areas, FDDI

local area networks can support thousands of users. As a standard underlying medium it uses optical fiber (though it can use copper cable, in which case one can refer to CDDI). FDDI uses a dual-attached, counter-rotating token-ring topology.

### **FS type**

type of file system.

### **FTP**

File Transfer Protocol. This is the language used for file transfer from computer to computer across the WWW. An anonymous FTP is a file transfer between locations that does not require users to identify themselves with a password or log-in. An anonymous FTP is not secure, because it can be accessed by any other user of the WWW.

In Simple words, the protocol used on the Internet for exchanging files. FTP uses the Internet's TCP/IP protocols to enable data transfer. FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server (eg, uploading a Web page file to a server).

### **G**

#### **GET**

An access method in HTTP.

#### **Graphical User Interface (GUI)**

The visual symbols and choices to control a program. Most GUI's use windows, menus, and toolbars. Most operating systems use GUI's because most users are uncomfortable with a less user friendly interface like a command line.

### **H**

#### **HackerGuardian TrustLogo**

is the daily server vulnerability assessment and certification service that delivers essential, real time verification of your security credentials directly to your website customers.

#### **HTTP**

HTTP (Hypertext Transfer Protocol) is the foundation protocol of the World Wide Web. It sets the rules for exchanges between browser and server. It provides for the transfer of hypertext and hypermedia, for recognition of file types, and other functions.

### **I**

#### **IP - Internet Protocol**

The Internet Protocol (IP) is a data-oriented protocol used by source and destination hosts for communicating data across a packet-switched Internetwork.

An IP address is a numeric address that is used to identify a network interface on a specific network or subnetwork. Every computer or server on the Internet has an IP address. It is a unique number consisting of four parts separated by dots. For example, 198.204.112.1. The address contains two pieces of information : the network portion, known as the IP network address, and the local portion, known as the local or host address.

#### **Internet Service Provider (ISP)**

A company or organization that provides the connection between a local computer or network, and the larger Internet.

## **IMAP**

Internet Message Access Protocol'. IMAP is a method of distributing email. It is different from the standard POP3 method in that with IMAP, email messages are stored on the server, while in POP3, the messages are transferred to the client's computer when they are read. Thus, using IMAP allows you to access your email from more than one machine, while POP3 does not. This is important because some email servers only work with some protocols.

## **IDS**

Software/hardware that detects and logs inappropriate, incorrect, or anomalous activity. IDS are typically characterized based on the source of the data they monitor: host or network. A host-based IDS uses system log files and other electronic audit data to identify suspicious activity. A network-based IDS uses a sensor to monitor packets on the network to which it is attached.

## **Information Security Exposure**

An information security exposure is a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.

## **K**

### **Key space**

In cryptography, an algorithm's key space refers to all possible keys that can be used to initialize it. Put in its most simplistic terms, the possibilities in the series A,B,C...Z represent a much smaller key space than AAA,AAB,AAC...ZZZ. A well-designed cryptographic algorithm should be highly computationally expensive when trying to brute-force through all possible key values.

## **L**

### **Labrea Tarpit**

A tarpit is a computer entity that will intentionally respond slowly to incoming requests. The goal is to delude clients so that unauthorized or illicit use of a fake service might be logged and slowed down. Note that some purists do not really consider a tarpit to be a honey pot, though it is certainly a fake information system resource that can delay any incoming aggressors. For example, to fight off spammers, some people run tarpits that look like open mail relays, but instead answer very slowly to SMTP commands. These are layer 7 tarpits. Other known tarpits are those that play with the TCP/IP stack in order to hold the incoming client's network socket open while forbidding any traffic over it.

The Labrea Tarpit is an excellent example that plays with the TCP/IP stack and has been used to slow down the spread of worms over the Internet.

To achieve this tarpit state, iptables accepts an incoming TCP/IP connection and then immediately switches to a window size of zero. This prohibits the attacker from sending any more data. Any attempt to close the connection is ignored because no data can be sent by the attacker to the target. Therefore the connection remains active. This consumes resources on the attacker's system but not on the Linux server or the firewall running the tarpit.

## **LAN**

A local area network (LAN) is a computer network covering a small local area, like a home, office, or small group of buildings such as a home, office, or college. Current LANs are most likely to be based on switched Ethernet or Wi-Fi technology running at 10, 100 or 1,000 Mbit/s (1,000 Mbit/s is also known as 1 Gbit/s).

## **License**

The official terms of use for a specific program. A software license is a legal document since it formally restricts the rights of the user.

## **M**

### **MAC Address**

Short for Media Access Control address, a hardware address that uniquely identifies each node of a network.

### **MessageID (MID)**

This is a unique ID generated for each email encrypted with a single use certificate.

## **N**

### **NNTP**

Network News Transfer Protocol - Refers to the standard protocol used for transferring Usenet news from machine to machine. A protocol is simply a format used to transfer data to two different machines. A protocol will set out terms to indicate what error checking method will be used, how the sending machine will indicate when it is has finished sending the data, and how the receiving machine will indicate that it has received the data.

### **Netstat**

Netstat is a command-line tool that displays a list of the active network connections the computer currently has, both incoming and outgoing. It is available on Unix, Unix-like, and Windows NT-based operating systems.

### **Network (computer)**

Networking is the scientific and engineering discipline concerned with communication between computer systems. Such networks involves at least two computers, which can be separated by a few inches (e.g. via Bluetooth) or thousands of miles (e.g. via the Internet). Computer networking is sometimes considered a sub-discipline of telecommunications.

### **Nessus**

Nessus is a comprehensive open-source vulnerability scanning program. It consists of nessusd, the Nessus daemon, which does the scanning, and nessus, the client, which presents the results to the user.

### **NIDS**

NIDS - Network-Based Intrusion Detection System. Detects intrusions based upon suspicious network traffic. A network intrusion detection system (NIDS) is a system that tries to detect malicious activity such as denial of service attacks, port-scans or even attempts to crack into computers by monitoring network traffic.

### **Nmap**

Nmap is free port scanning software designed to detect open ports on a target computer, determine which services are running on those ports, and infer which operating system the computer is running (this is also known as fingerprinting). It has become one of the most widely used tools in any network administrator's toolbox, and is used for penetration testing and general computer security.

## O

### **Operating System (OS)**

The essential software to control both the hardware and other software of a computer. An operating system's most obvious features are managing files and applications. An OS also manages a computer's connection to a network, if one exists. Microsoft Windows, Macintosh OS, and Linux are operating systems.

### **OVAL-ID**

Open Vulnerability and Assessment Language (OVAL) is an international, information security community baseline standard for how to check for the presence of vulnerabilities and configuration issues on computer systems. OVAL standardizes the three main steps of the process:

- collecting system characteristics and configuration information from systems for testing;
- testing the systems for the presence of specific vulnerabilities, configuration issues, and/or patches;
- presenting the results of the tests.

"OVAL-ID Compatible" means that a Web site, database, archive, or security advisory includes both of the following:

- OVAL-IDs used as references for security issues.
- The capability is searchable by OVAL-ID.

While it is important to the OVAL and information security communities that these types of capabilities include references to OVAL-IDs, for example, "OVAL8127", for the testing of the issues that they describe to their customers in their advisories, databases, etc., verbatim replication of OVAL definitions is not encouraged because any changes in the definition by the original author may not be brought forward to the copied version in a timely manner. For this reason, the capability must reference only OVAL-IDs and not the text of the definitions in order to be considered OVAL-ID compatible. Additionally, the ability to search through collections is required for a capability to be considered OVAL-ID compatible.

## P

### **Ping**

Ping is a computer network tool used to test whether a particular host is reachable across an IP network.

### **Plugin**

A program that allows a Web browser to display a wider range of content than originally intended. For example: the Flash plugin allows Web browsers to display Flash content.

### **PKCS**

PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA Security.

### **PKCS#10**

See RFC 2986. Format of messages sent to a certification authority to request certification of a public key. See certificate signing request.

### **PKCS#12**

Defines a file format commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.

### **PKCS#7**

See RFC 2315. Used to sign and/or encrypt messages under a PKI. Used also for certificate dissemination (for instance

as a response to a PKCS#10 message). Formed the basis for S/MIME, which is now based on RFC 3852, an updated Cryptographic Message Syntax Standard (CMS).

## **POP2**

There are two versions of POP. The first, called POP2, became a standard in the mid-80's and requires SMTP to send messages. The newer version, POP3, can be used with or without SMTP.

## **POP3**

POP3 is the abbreviation for Post Office Protocol - a data format for delivery of emails across the Internet.

## **PEM**

Privacy Enhanced Mail (PEM) is a standard for message encryption and authentication of senders.

## **R**

### **RST**

A control bit (reset), occupying no sequence space, indicating that the receiver should delete the connection without further interaction. The receiver can determine, based on the sequence number and acknowledgment fields of the incoming segment, whether it should honor the reset command or ignore it. In no case does receipt of a segment containing RST give rise to a RST in response.

## **S**

### **SecureEmail Server (SES)**

SecureEmail server used to store PKCS#12s. The server facilitates downloads of PKCS#12s and the relevant ssl client authentication.

### **Single User Certificate**

A single use certificate refers to the x.509 and associated private key generated by SecureEmail on Alice; stored on SES and downloaded by Bob after a successful SSL client authentication.

## **SMB**

A message format used by DOS and Windows to share files, directories and devices. NetBIOS is based on the SMB format, and many network products use SMB. These SMB-based networks include Lan Manager, Windows for Workgroups, Windows NT, and Lan Server. There are also a number of products that use SMB to enable file sharing among different operating system platforms.

## **S/MIME**

S/MIME (Secure / Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of email encapsulated in MIME.

## **SMTP**

Simple Mail Transfer Protocol is the most widely used standard for email transmission across the Internet. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified (and in most cases verified to exist) and then the message text is transferred.

## **SNMP**

Simple Network Management Protocol. The network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

## **SSL**

Secure Sockets Layer is commonly used protocol for managing the security of a message transmission on the Internet. Sockets refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public- and private-key encryption system, which includes the use of a digital certificate.

## **SYN**

SYN (synchronize) is a type of packet used by the Transmission Control Protocol (TCP) when initiating a new connection to synchronize the sequence numbers on two connecting computers. The SYN is acknowledged by a SYN/ACK by the responding computer.

## **STATIC IP**

An IP address which is the same every time you log on to the Internet. See [IP](#) for more information.

## **T**

### **TCP**

TCP stands for Transmission Control Protocol. TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

### **Token-Ring**

LAN technology was developed and promoted by IBM in the early 1980s and standardized as IEEE 802.5 by the Institute of Electrical and Electronics Engineers. Initially very successful, it went into steep decline after the introduction of 10BASE-T for Ethernet and the EIA/TIA 568 cabling standard in the early 1990s. A fierce marketing effort led by IBM sought to claim better performance and reliability over Ethernet for critical applications due to its deterministic access method, but was no more successful than similar battles in the same era over their Micro Channel architecture. IBM no longer uses or promotes Token-Ring. Madge Networks, a one time competitor to IBM, is now considered to be the market leader in Token Ring.

## **U**

### **User**

A person who uses a computer, including a programmer or end user.

### **User Interface (UI)**

How the user controls a program. Perhaps the simplest UI is a keyboard and command line, to enter text commands. Sometimes called a "console."

## V

### **Vulnerability**

In network security, a vulnerability refers to any flaw or weakness in the network defense that could be exploited to gain unauthorized access to, damage or otherwise affect the network.

## W

### **Web server**

The term Web server can mean one of two things:

1. A computer that is responsible for accepting HTTP requests from clients, which are known as Web browsers, and serving them Web pages, which are usually HTML documents and linked objects (images, etc.).
2. A computer program that provides the functionality described in the first sense of the term.

### **Wildcard**

Wildcards are symbols that add flexibility to a keyword search by extending the parameters of a search word. This can help if you are not certain of spelling, or only know part of a term, or want all available spellings of a word (British and American English, for example). '\*' stands for one-or-more characters (useful for all suffixes or prefixes), '#' stands for a single character, and '?' stands for numerals, zero-to-nine..

### **www**

Short for World-Wide Web. It is a global information space which people can read-from and write-to via a large number of different Internet-connected devices.

## X

### **X.509**

An internationally recognized standard for certificates that defines their required parts.

## Appendix 1 - Comodo ePKI Manager – Overview

---

### Comodo EPKI Manager

Instant security for your web operations, internal networks and employee's email.

The EPKI Manager provides instant security for your web operations, internal networks and employee's email, giving you full access to an outsourced Certificate Authority platform for all your digital certificate requirements.

When considering the implementation options for a digital certificate solution, you will make the choice to opt for an in-house PKI model, or a fully managed outsourced model. Following the in-house option will see enormous costs in time, management, legal fees, development and operational costs. To avoid such barriers for the widespread use of Certificates within an organization, Comodo has developed the enterprise class EPKI Manager - a web based console used to interface with the Comodo Certificate Authority.

- Easy to use web based console
- Issue high quality, fully trusted SSL Certificates
- Issue Corporate Secure Email Certificates quickly to employees and partners
- Create / manage "sub users" and assign specific issuance and reporting permissions to your users
- Gain savings on standard Certificate buy prices
- No extra software / hardware required
- Open an EPKI Manager account in minutes
- Full reporting / Certificate management

With the EPKI, there is no need to invest in expensive hardware, software, expertise and Certification Authority management associated with providing your own certificate solutions. The EPKI Manager allows you to issue Certificates for use within your intranets, extranets, and websites or employees email clients. Comodo already provides industry-leading prices for Certificates; however the EPKI Manager provides even greater discounts on all Certificates.

Organizations opting for the EPKI Manager can benefit from the convenience of having their nominated EPKI Manager Administrator(s) manage all the company's Certificates from a central web based console. The User Management facility allows the Administrator to create new sub-users for the EPKI Manager, each with granular permissions for issuance, revocation and reporting - allowing the enterprise to operate a distributed EPKI without the compromise of security for critical applications.

Additional certificates may be purchased through the console in minutes, ensuring new web servers, employees or internal resources may be secured in minutes rather than days.

### Secure Your Enterprise Intranets, Extranets & Websites

SSL Certificates are the industry standard technology used to secure communications between browsers and web servers, whether it via the Internet or internally through intranet or extranets. Some organizations will require multiple SSL Certificates to secure multiple servers, spanning intranets, extranets, web server operations and load balancing. To meet the needs of your organization, the EPKI Manager allows you to procure SSL Certificates on demand.

### **Secure Your Enterprise Email**

The need for email to be secure, confidential and integral is a growing concern for almost every organization. Comodo Corporate Secure Email Certificates address this critical problem and provide the ability to secure and digitally sign email and attachments using any popular mail client. The EPKI Manager provides convenient and secure access to your own web-based console to administer your Corporate Secure Email Certificates to employees and partners.

### **Assure Customers and Partners of Your Identity**

Assuring customers of your identity is an essential factor for successful online business. Certificates issued through the EPKI Manager help assure customers of your online and email identity, leading to a higher confidence in who you are. Through the user-friendly interface you can issue digital certificates to web servers, internal servers, employees and partners, certificates that in turn represent the identities and credentials of their owner. The EPKI Manager helps you achieve trust and confidence within an environment where trust and confidence is essential yet currently unavailable.

### **Fully Managed CA Operations**

Comodo operate the backend Certification Authority used to issue the SSL and Corporate Secure Email Certificates, including high availability secure redundant server systems, high speed FIPS 140-1 Level 4 signing devices, backup and customer support. All Certificates issued through the EPKI Manager are fully supported by Comodo's industry leading customer support department.

## Manage Your Enterprises Entire Certificate Requirements

SSL Certificates for websites, intranets and extranets. Corporate Secure Email Certificates for S/MIME compliant mail clients

## Issue Your Own Certificates Cost Effectively

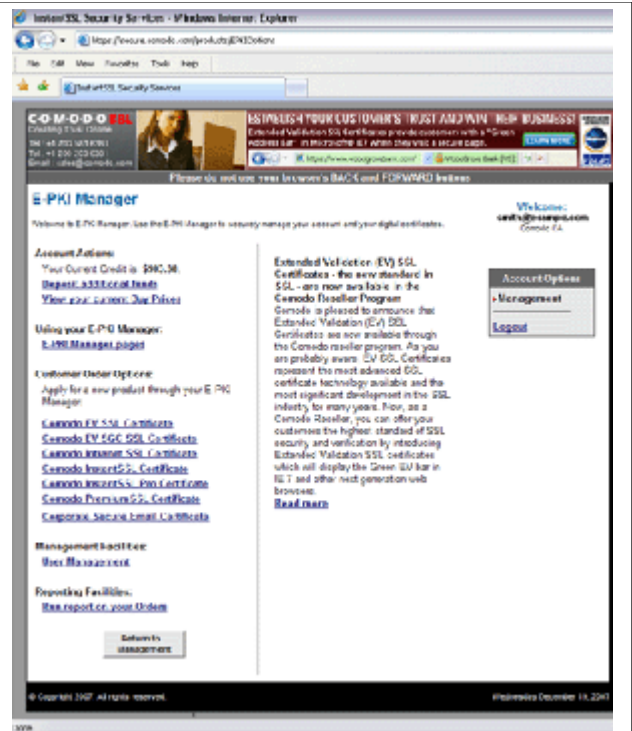
There is no need to invest in expensive hardware, software, expertise and Certification Authority management associated with providing your own certificate solutions. The EPKI Manager allows you to issue Certificates for use within your intranets, extranets, websites or employees email clients

## Web Based Interface For Easy Issuance

No set up fee is required and you can be up and running in minutes! The user-friendly web based management console gives you easy access to your Certificate management

## Granular EPKI Manager User Management

The EPKI Manager Administrator can add new users to the EPKI account, each with their own access control details and permissions. New users can have issuance abilities for SSL Certificate and/or Corporate Secure Email Certificates, access to money management facilities and access to global or local reporting facilities. This feature allows the EPKI Manager to be accessed by additional enterprise personnel, and permissions assigned accordingly.

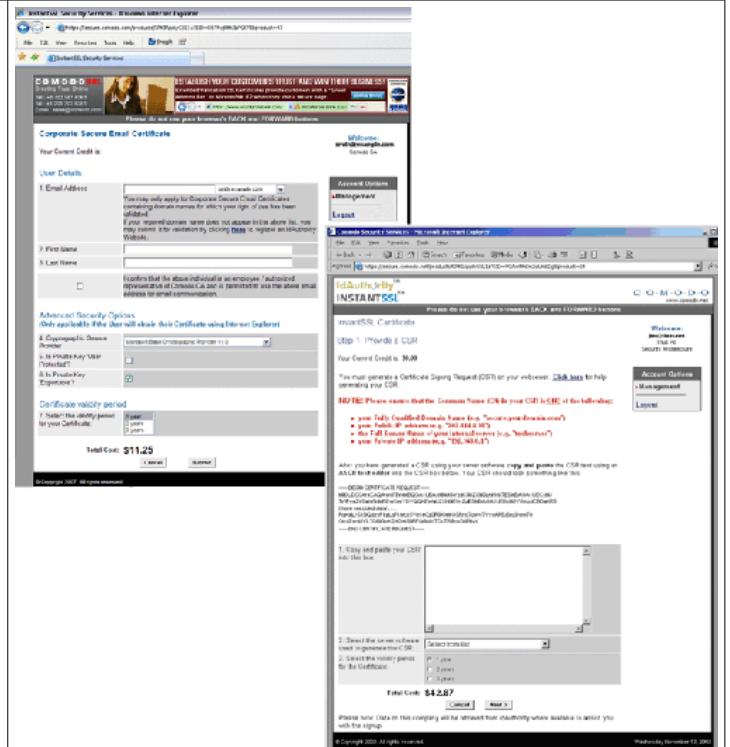


## Save Money on Your Security Requirements

Comodo already provides industry-leading prices for Certificates. Through the EPKI Manager you can take advantage of further discounts on Comodo digital certificates. Multiple Certificate requirements for distributed systems and personnel, as well as load balancing requirements, can be fulfilled quickly, easily and cost effectively.

### EPKI Manager

- Web based interface
- High availability 24/7 system
- Sub user creation and management
- Sub user certificate issuance, reporting and financial management permission assigning
- 128 bit industry standard SSL & S/MIME certificates
- Immediate issuance
- 99.3% browser ubiquity
- Standard, Intranet or Wildcard SSL Certificates available
- Corporate Secure Email Certificates available
- Full reporting facilities



## Appendix 2 - Notes on 32 bit/64 bit Editions

Windows XP 64 and Vista 64 are the 64-bit versions of the Windows XP and Vista family of Microsoft operating systems. These 64-bit versions differ from Windows XP 32 and Vista 32 in that the operating system operates in the 64-bit mode of processors that support that mode. (Those processors include AMD processors such as Athlon, Opteron and Intel 64 bit processors.)

Most, but not all, 32 bit applications will run natively under Windows XP 64 and Vista 64. However, 64 bit applications will never run under the 32 bit versions of XP and Vista.

Comodo offer 64 bit versions of SecureEmail and SecureEmail Pro for Windows XP 64 and Vista 64. There are also 32 and 64 bit versions of most major mail clients. The table and summary below provides a overview of the interoperability of these three software components (OS, Client, SecureEmail).

	<i>SecureEmail x32</i>	<i>SecureEmail x64</i>
<b>Windows XP 32-bit</b>	Will run with all 32-bit clients that SecureEmail is confirmed to support.	64 bit version of SE will not run on 32 bit operating systems.
<b>Windows XP 64-bit</b>	Will run with all 32-bit clients that SecureEmail is confirmed to support. Will not run with 64-bit clients (Microsoft Outlook Express)	Will run with all 64-bit clients that SecureEmail is confirmed to support. (Microsoft Outlook Express) Will not operate with 32-bit clients.
<b>Windows Vista 32-bit</b>	Will run with all 32-bit clients that SecureEmail is confirmed to support.	64 bit version of SE will not run on 32 bit operating systems.
<b>Windows Vista 64-bit</b>	Will run with all 32-bit clients that SecureEmail is confirmed to support. Will not run with 64-bit clients (Microsoft Windows Mail)	Will run with all 64-bit clients that SecureEmail is confirmed to support. (Microsoft Windows Mail) Will not operate with 32-bit clients

### Summary:

1. User should install 64-bit version of SecureEmail ONLY if they are going to use Microsoft Outlook Express 64-bit or Microsoft Windows Mail on Vista 64.
2. The 32 bit version of SecureEmail will run on the 64 bit operating systems ONLY if you also have the 32 bit version of a supported mail client installed. For example, the 32-bit version of SecureEmail doesn't run with Microsoft Outlook Express 64 on 64-bit operating system.

3. 64-bit version of SecureEmail doesn't install plug-ins for Mozilla Thunderbird and Microsoft Outlook (There are no 64 bit versions of Outlook/Thunderbird.)
4. It is possible to install both 64-bit and 32-bit versions of SecureEmail simultaneously on a 64 bit version of XP or Vista. Each of the installed versions will run with the correct client (so you would also need both 64-bit and 32-bit versions of your email client).

Important: In this situation, both installations ( the 32 and 64 bit versions of the SecureEmail) will share configuration settings. The configuration of the version installed first will be used by the second version installed.

## Appendix 3 - Default Security Profiles

Comodo Secure Email – Security Settings – Default security profiles

	“New Group” (default)	Off	Low	Medium	High	Very High
<b>Encryption</b>						
Only Encrypt for contacts where a certificate is already installed on the system	✓	✗	✗	✓	✓	✗
Don't allow emails to be viewed by the web reader service	✗	✗	✗	✗	✗	✓
Block unencrypted mail from leaving the system	✗	✗	✗	✗	✓	✓
Prompt my contacts for a password to read emails via the web reader service	✗	✗	✗	✗	✗	✗
<b>Encryption Schema</b>						
Prompt if a non-encrypted mail is found	✗	✗	✗	✗	✗	✓
Automatically encrypt email	✓	✗	✗	✓	✓	✗

Don't encrypt any email	x	✓	✓	x	x	x
<b>Signing</b>						
Don't digitally sign my mail	x	✓	x	x	x	x
Digitally sign my emails	✓	x	✓	✓	✓	✓
Send clear text signed message when sending signed messages	✓	x	✓	✓	✓	✓
Add clear text version of received signed emails that don't have detached signatures	x	x	x	x	x	x
Don't add clear text signature extraction information footer	x	x	x	x	x	x
<b>Decryption</b>						
Turn off decryption	✓	✓	✓	✓	✓	✓
Automatically decrypt incoming emails	x	x	x	x	x	x
Don't add SecureEmail information footer to decrypted messages	x	x	x	x	x	x
Prompt for a password	x	x	x	x	x	x

before decrypting						
<b>Housekeeping messages</b>						
Don't encrypt or sign Outlook calendar messages	✓	✓	✓	✓	✓	✗
Don't encrypt or sign read receipt messages	✓	✓	✓	✓	✓	✗
<b>You will be warned if a contacts email certificate has expired</b>	✓	✗	✗	✓	✓	✓