Importing and Using your Email or Personal Authentication certificate with Windows Live Mail

- If you originally applied for the certificate on the same computer as your Windows Live Mail then it should already be installed. You can skip straight to 'Signing and Encrypting'.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides using one of the browsers listed on the CPAC main page. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then follow the 'import' instructions in this document.

Importing your certificate into Windows Live Mail

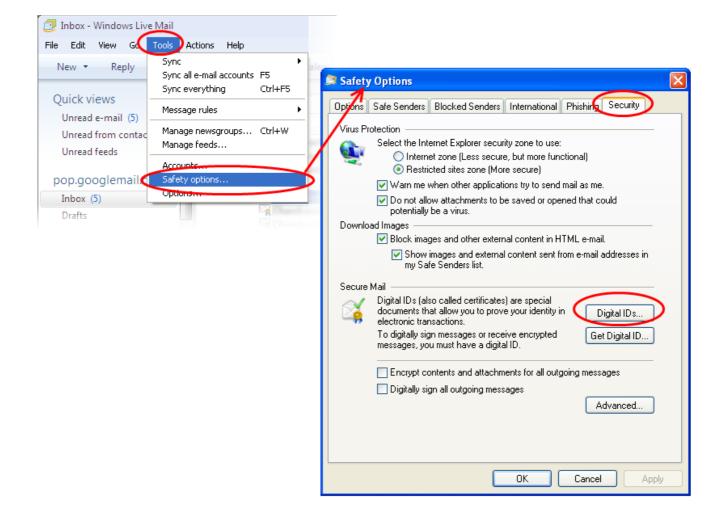
Signing and Encrypting mails

Importing your Certificate into Windows Live Mail:

- 1. Open Windows Live Mail and click **'Tools'** > **'Safety Options...'**. (If the menu bar is not displayed, click on the Menus icon in the tool bar and choose **Show menu bar** from the drop-down.)
- 2. Select the 'Security' tab and then click the 'Digital IDs' button.



Creating Trust Online™



3. In the Certificates interface, make sure the 'Personal' tab is selected, click 'Import' and then click 'Next'.

2

сомодо

Creating Trust Online[™]

Certificates	? 🔀
Intended purpose: <a>	
Personal Other People Intermediate Certification Authorities	Trusted Root Certification
Issued To Issued By Expiration	D Friendly Name
Import Export Remove	<u>A</u> dvanced
Certificate Import Wizard	Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. To continue, click Next.
	< Back Next > Cancel

4. Click 'Browse' in the next step and navigate to the location of your PKCS12 certificate file.

COMODO Creating Trust Online[™]

Certificate Import Wizard		
File to Import Specify the file you want to import.		
File name:		
Note: More than one certificate can be stored in a single file in the following formats:		
Personal Information Exchange- PKCS #12 (.PFX,.P12)		
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)		
Microsoft Serialized Certificate Store (.SST)		
< <u>B</u> ack <u>N</u> ext > Cancel		

5. Now you need to change type of the file, select '**Personal Information Exchange (.p12)'** from the drop down box, locate your certificate file (.p12) and click '**Open'** (see below).

4



Open				? 🗙
Look in:	🚞 certs	O Ø	🔊 🔁	
D Recent	🔊 alice_cert			
Desktop				
My Documents				
My Computer				
	File name:		~	Open
My Network	Files of type:	Personal Information Exchange (*.pfx;*.p12)	~	Cancel
		X.509 Certificate (*.cer;*.crt) Personal Information Exchange (*.pfx;*.p12) Certificate Trust List (*.stl) Certificate Revocation List (*.crl) Microsoft Serialized Certificate Store (*.sst) PKCS #7 Certificates (*.spc;*.p7b) All Files (*.*)		

6. Click **Next**. To complete the installation process, you are required to enter the PIN (password) you set up for the certificate during the enrollment process. If you have forgotten your password, contact your system administrator who will be able to reset it for you.

COMODO Creating Trust Online[™]

Certificate Import Wizard	
Password To maintain security, the private key was protected with a password.	
Type the password for the private key.	
Password:	

Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.	
✓ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.	
< <u>B</u> ack <u>N</u> ext > Cancel	

7. Click **Next**. You will be prompted to choose the certificate store for your certificate. Unless your administrator has specified otherwise, you should leave this at the default **Place all certificates in the following store** option.

Certificate Import Wizard	×
Certificate Store	
Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for Automatically select the certificate store based on the type of certificate	
 Place all certificates in the following store 	
Certificate store:	
Personal Browse	
< <u>B</u> ack <u>N</u> ext > Cancel	

- 8. Click 'Next'.
- 9. The last step: completing the Certificate Import Wizard.



- 10.Click **Finish** to complete the process. The certificate will be imported.
- 11. Select the security level for storing the Private Key in your system and click OK.

Importing a n	ew private exchange key 🛛 🔀
	An application is creating a Protected item.
	CryptoAPI Private Key
	Security level set to Medium Set <u>Security Level</u>
	OK Cancel <u>D</u> etails

That's it. You have successfully imported your Comodo Personal Authentication certificate into your system.

Signing and Encrypting Mails

• Signing an email ensures the recipient knows the email has come from you and informs them that it has not been modified in transit.

• Encrypting an email ensures that only the recipient can read the email content and attachments.

Note: In order to encrypt mail, you must first have your recipient's email certificate in your certificate store. To obtain their certificate, you need to get your contact to send you a signed email. Upon receipt of the signed mail, their certificate will be automatically imported into your certificate store and you will be able to sign/encrypt mail to that person.

- Assign the certificate
- Signing and encrypting individual mails
- Signing and encrypting all mails by default

Assign the certificate

- 1. Right click on your email account name in Windows mail or click **'Tools' > 'Accounts...'**, select your account and click the **Properties** button.
- 2. In the Properties screen, click the Security tab.
- 3. Click **'Select'** beside the text box in the **'Signing certificate'** area and select your Comodo Personal Authentication certificate in the **'Select Digital ID'** screen. Click **'OK'**.



📮 Company (ali	cegreen) Properties 🛛 🔀
General Server	Connection Security
Signing certificate	
	ing certificate below. This will determine the digital signing messages with this account.
<u>C</u> ertificate:	Select
Encrypting prefere	ences
included with y	ryption certificate and algorithm. These are our digitally signed messages so others can send to you with these settings.
C <u>e</u> rtificate:	Seject.
Algorithm:	3DES
	Select Default Account Digital ID
	Select the certificate you want to use.
	Issued to Issued by Intended P Friendly na Expiration
	🕮 alicegre COMODO C Personal Au None 10/5/2014
	OK Cancel View Certificate

- 4. Similarly, click 'Select' beside the text box in 'Encrypting preferences' area and select the same certificate for encryption by clicking OK in the 'Select Digital ID' screen.
- 5. Click OK in the Account Properties dialog to return to Windows Live Mail.

Signing and encrypting individual mails

To sign mail:

- 1. Compose your email and attach files as usual.
- 2. In the message window, click **Tools** from the menu bar. If the menu bar is not displayed, click on the 'Menus' icon in the title bar and choose **Show menu bar**.
- 3. Check the **Digitally Sign** option from the drop-down menu and send the mail.

To encrypt mail:

- 1. Compose your email and attach files as usual.
- 2. Click **Tools** from the menu bar. If the menu bar is not displayed, click the 'Menus' icon in the title bar and choose **Show menu bar**.
- 3. Check the Encrypt option from the drop-down menu and send the mail.

Signing and Encrypting all mails by default:

- Open Windows Live Mail and click 'Tools' > 'Safety Options...'. If the menu bar is not displayed, click on the 'Menus' icon in the tool bar and choose Show menu bar.
- 2. In the Safety Options screen, click the Security tab.
- 3. Select the 'Encrypt contents and attachments for all out going messages' and/or Digitally sign all outgoing messages check-boxes as required.

Block images and other external content in HTML e-mail.		
	Show images and external content sent from e-mail addresses in my Safe Senders list.	
Secure	Mail	
	Digital IDs (also called certificates) are special documents that allow you to prove your identity in electronic transactions.	
	To digitally sign messages or receive encrypted Get Digital ID messages, you must have a digital ID.	
 Encrypt contents and attachments for all outgoing messages Digitally sign all outgoing messages Advanced 		
	OK Cancel Apply	

4. Click 'Apply' then 'OK'.

About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo Security Solutions, Inc.	Comodo CA Limited
1255 Broad Street	3rd floor, Office Village Exchange Quay
Clifton, New Jersey 07013	Trafford Road, Salford, Manchester M5 3EQ
United States	United Kingdom
Tel : +1.888.266.6361	Tel:+44 (0) 161 874 7070
Tel : +1.703.581.9361	Fax : +44 (0) 161 877 1767
Email: sales@Comodo.com	

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