



ADVANCED ELECTRONIC SOLUTIONS

AVIATION SERVICES

COMMUNICATIONS AND CONNECTIVITY

MISSION SYSTEMS

CAES Secure Email Guide *for External Users*

Contents

Introduction	2
Organizational Level Secure Email	2
PGP Global Directory, and PGP Universal Server	2
Delivery Options.....	3
Delivery Option Recommendation	3
Delivery Options Explained	4
Getting Started.....	5
Enrolling as an External User	5
Configuring Symantec Encryption Satellite Delivery Option	7
Uninstalling Symantec Encryption Satellite	12
Configuring Key or Digital ID/Certificate Delivery Option	13
Configuring Your Account using a PGP Public Key	13
Configuring Your Account using an S/MIME (X509) Public Key	19
Using Your CAES Secure Email Portal.....	24
Appendix A.....	26
Exporting your S/MIME Certificate	26
Exporting your PGP Key (from PGP Desktop)	29
Troubleshooting.....	30
All my emails from CAES are “Secure Web Messenger”	30
I forgot my password for the CAES Secure Web Messenger”	31

Introduction

Managing and securing electronic information has become both a highly visible, and a highly regulated activity. Creating, implementing, and enforcing corporate security policies governing email has become critical to mitigating risk for all organizations. To ensure the security of sensitive email, CAES has implemented a secure email system, powered by Symantec's PGP Universal technology. This document outlines how to set up your email account to work with the CAES Secure Email system.

One of the advantages of the PGP Universal technology is its flexibility. Accordingly, you will need to choose one (1) method of interacting with the CAES Secure Email system. Depending upon the "delivery option" chosen, it may be desirable, or even necessary, to enlist the help of your local IT department to assist with the configurations described in this document.

Organizational Level Secure Email

Organizations that have a company-wide secure email system in place may prefer to configure secure email at the directory server level, rather than at the individual email address level. This higher level configuration would negate the need to perform any of the configurations in this document.

PGP Global Directory, and PGP Universal Server


If you use PGP Desktop software, and have uploaded your PGP key to the PGP Global Directory, you will only need to add the CAES keyserver in your PGP Desktop client (page 13). If you have not uploaded your key to the PGP Global Directory, you will follow the instructions for the Key or Digital ID/Certificate Option (page 12)

If your company uses PGP Universal Server, and has published the LDAP keyserver to the Internet following PGP guidelines, you should not need to perform any of the configurations in this document.

Delivery Options

Delivery Option Recommendation

The table below shows the recommended delivery option based on your current environment. All delivery options are explained in detail in the next section. Please note that your delivery option can be changed in the future.

 <p>1 – Choose your option below and... 2 – Choose your email environment to the right, then find your recommended Delivery Option.</p>	<p>I/My company uses Secure Email technology today and therefore I have a PGP Key or S/MIME certificate</p>	<p>I/My company does NOT use Secure Email technology today</p>
<p>I can install programs on my computer AND I want to configure my computer to integrate fully with CAES Secure Email</p>	<p>Key or Digital ID/Certificate</p> <p>Other possible options: Symantec Web Email Protection, Regular Email</p>	<p>Symantec Encryption Satellite</p> <p>Other possible options: Symantec Web Email Protection, Regular Email</p>
<p>I can install programs on my computer however, I DO NOT want to configure anything on my computer</p>	<p>Key or Digital ID/Certificate</p> <p>Other possible options: Symantec Web Email Protection, Regular Email</p>	<p>Regular Email</p> <p>Other possible options: Symantec Web Email Protection</p>
<p>I cannot install programs on my computer</p>	<p>Key or Digital ID/Certificate</p> <p>Other possible options: Symantec Web Email Protection, Regular Email</p>	<p>Regular Email</p> <p>Other possible options: Symantec Web Email Protection</p>

Delivery Options Explained

The delivery options dictate how you will interact with the CAES Secure Email system. They are listed in the same order here as they are listed on the website when you are asked to choose:

- **Symantec Web Email Protection**
 - CAES will create a secure webmail account on our Secure Email servers for you. You will need to log into the secure website ONLY for secure emails received from CAES. ***You will continue to receive non-secure email from CAES in your normal mail application.*** Sending a secure email to CAES requires logging in to the secure website.
- **Symantec Encryption Satellite**
 - Symantec Encryption Satellite is a Windows application that can be installed (if you are allowed) on your computer. You will not need to log into the secure website to send or receive secure email with CAES. This option may require additional configuration of your email client and/or assistance from your IT department.
- **Key or Digital ID/Certificate**
 - This option is for users/companies that already use Secure Email technology. CAES supports both S/MIME (X509) Certificates and PGP keypairs. After uploading your public key to the CAES servers, you will use your mail client to exchange secure email with CAES just as you have previously with other email recipients.
- **Regular Email**
 - This option is recommended for users that are unsure of what to choose. CAES will create a secure webmail account on our Secure Email servers for you. You will need to log into the secure website ONLY for secure emails received from CAES. ***You will continue to receive non-secure email from CAES in your normal mail application.*** Sending a secure email to CAES requires logging in to the secure website.

Getting Started

Enrolling as an External User

In order to choose your delivery option, you must enroll with the CAES PGP Universal server as an external user. This process is performed only once and begins when you receive your first "Secure Email" from CAES. This is actually a notification from CAES that you have received a secure email and it is waiting for you on your newly created secure mailbox on the CAES PGP servers. The notification will look as follows:

From: "Doe, John (SSA R4)" <john.doe@cobhamaes.com>
Date: March 17, 2020 at 10:33:25 AM EDT
To: Jane Smith <janesmith@gmail.com>
Subject: PGP Universal Secured Message from the CAES Secure Email system

You have received a PGP Universal Secured Message from:


Doe, John (SSA R4) <john.doe@cobhamaes.com>

To read this message securely, please click this link:

<https://keys.cobhamna.com/b/b.e?r=janesmith%40gmail.com&n=Jlcm1ZqBZXfbXin7shohbA%3D%3D>

Click here to
enroll as an
external user

- The link will bring you to the CAES Secure Email servers where you will be asked to create a passphrase for your account. Please read and follow the recommendations for protecting your passphrase. Enter your chosen password twice, and click CONTINUE.



You have received an encrypted message from Cobham

Please create a passphrase to secure future messages delivered to you.

This server requires your passphrase to meet the following requirements:

- They must be at least 8 characters long.
- It must include an uppercase letter, a lowercase letter, a digit and a punctuation mark.

For example, "kittycat" is not a valid passphrase, but "k1ttYc@t" is a valid passphrase.

Here are some recommendations for protecting your passphrase:

- Use an easy to remember passphrase that you don't need to write down.
- Don't use obvious passphrases that can be easily guessed.
- Don't make your passphrase a single word.
- Don't use famous quotations.

Passphrase:

Confirm Passphrase:

Copyright © 2014 Symantec Corporation. All Rights Reserved.

- You will now be prompted to select your Delivery Option. Please refer to the “[Delivery Options](#)” section of this document for a more detailed explanation. This selection can be changed later from your CAES Secure Email settings page:

Settings Help Logout

COBHAM Symantec

Message Delivery Options

Please select how you would like to receive future messages from Cobham.

☐ **Symantec Web Email Protection (Recommended)**
I want to use the passphrase I just entered to exchange messages with Cobham securely on this Web site.
☒ Save a copy of all outgoing messages in my "Sent" messages folder.

☐ **Symantec Encryption Satellite**
I want to install a small background service on my computer to automatically secure messages I exchange with Cobham.

☐ **Key or digital ID/certificate** (Select this option if you are an advanced user.)
I have an OpenPGP Key or digital ID/certificate (X.509, S/MIME) that I want to use to secure messages I exchange with Cobham.

☒ **Regular Email**
I want to receive as many messages as possible via normal email. Some messages may still be delivered via other means because of higher security needs.

Choose Option

Copyright © 2014 Symantec Corporation. All Rights Reserved.

- If you selected **Symantec Web Email Protection** or **Regular Email**:
 - YOU ARE FINISHED.** You will be brought to your CAES Secure Webmail Inbox. Proceed to the “Using Your CAES Secure Email Portal” section for more information.
- If you selected **Symantec Encryption Satellite** or **Key or Digital ID/Certificate**:
 - Proceed to the next section(s) in this document to continue your configuration.
 - NOTE: If you selected Key or Digital ID/Certificate, you will need to have your public key available. Please see Appendix A for assistance if necessary**

Settings Help Logout

COBHAM Symantec

Configuration Confirmation

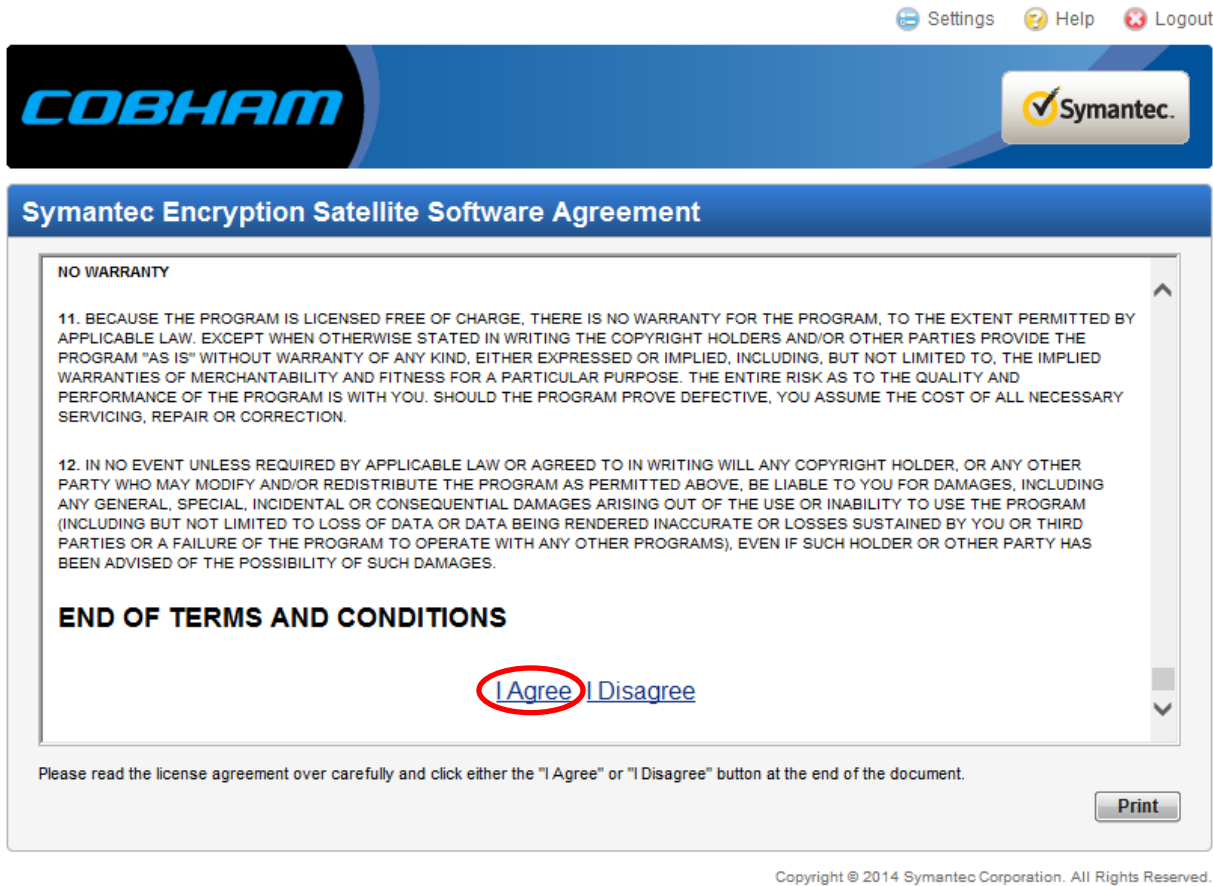
Thank you. Your delivery preference has now been set.

OK

Copyright © 2014 Symantec Corporation. All Rights Reserved.

Configuring Symantec Encryption Satellite Delivery Option

- After selecting the Symantec Encryption Satellite option, you are presented with the PGP End User License Agreement. Please read it and click **I AGREE**



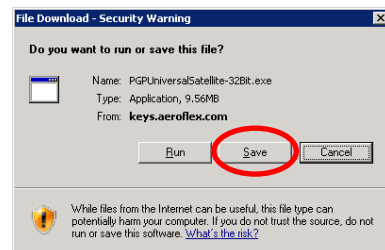
The screenshot shows the Symantec Encryption Satellite Software Agreement window. At the top, there are links for Settings, Help, and Logout. The COBHAM logo is on the left, and the Symantec logo is on the right. The main content area contains the text of the agreement, including sections on NO WARRANTY and END OF TERMS AND CONDITIONS. At the bottom, there are two buttons: "I Agree" and "I Disagree". The "I Agree" button is circled in red. Below the buttons, there is a "Print" button and a copyright notice: "Copyright © 2014 Symantec Corporation. All Rights Reserved."

- You will now be given a choice of downloads. Choose the correct version for your system and click CONTINUE



The screenshot shows the "Download Symantec Encryption Satellite" window. It has a header with COBHAM and Symantec logos. Below the header, there is a message: "Please click on an appropriate link below. Once the download has finished, click the continue button." There are three download links: "Download the Windows Satellite 32-bit Version", "Download the Windows Satellite 64-bit Version", and "Download the Mac OS X Satellite". Each link has a corresponding icon and system requirements listed below it. A red circle highlights the three download links, and another red circle highlights the "Continue" button at the bottom right. The copyright notice "Copyright © 2014 Symantec Corporation. All Rights Reserved." is at the bottom.

Select the appropriate version of the software based on your system. You will be prompted to download the application.



The screenshot shows a "File Download - Security Warning" dialog box. It asks "Do you want to run or save this file?". The file name is "PGPUniversalSatellite-32bit.exe", the type is "Application, 9.56MB", and it is from "keys.aeroflex.com". There are three buttons: "Run", "Save", and "Cancel". The "Save" button is circled in red. Below the buttons, there is a warning icon and text: "While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?"

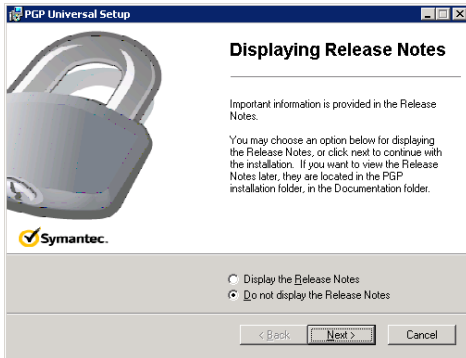
Please save it to your desktop.

- While the application is downloading, click CONTINUE. You will now be brought to your CAES Secure Email inbox to view the message that began this process.

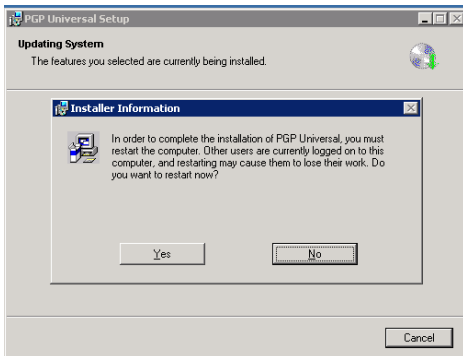


This is the actual secure message that CAES sent you. Right now it is in your CAES Secure Email account on the CAES servers, however, once you complete the Symantec Encryption Satellite configuration, you will be able to re-send this message to your normal email client.

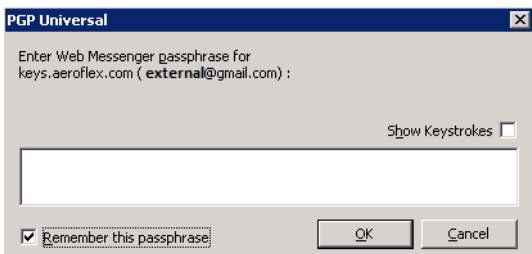
- Run the installer file for Symantec Encryption Satellite. Select not to display the Release Notes and click NEXT:



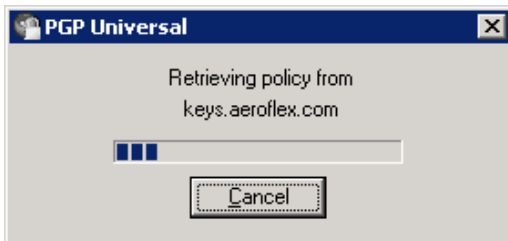
- After the installation is complete, you will be asked to reboot. Please do so:



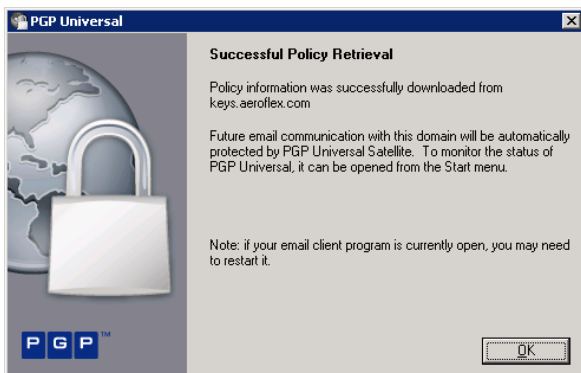
- When your computer boots back up, the PGP Universal software will prompt you to enter your CAES Secure Email passphrase that you set in the Getting Started section.
 - Enter your password, click “REMEMBER THIS PASSPHRASE”, and then click OK



- The software will now enroll with the CAES servers.

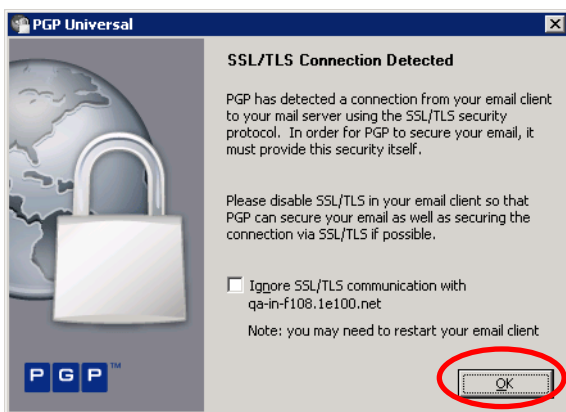


- Upon successful completion, you will see the following screen
 - **NOTE:** If you have issues enrolling, make sure your computer can communicate outbound over the Internet to keys.cobhamna.com on Port 443 (HTTPS). You may need to contact your local IT department to enable this communication.



*****NOTE:** If you DO NOT receive the message below, YOU ARE COMPLETE. Proceed to Page 10.

- After completing the enrollment, the software will detect your mail client settings. Depending on those settings, you **MAY** see a screen similar to the following:

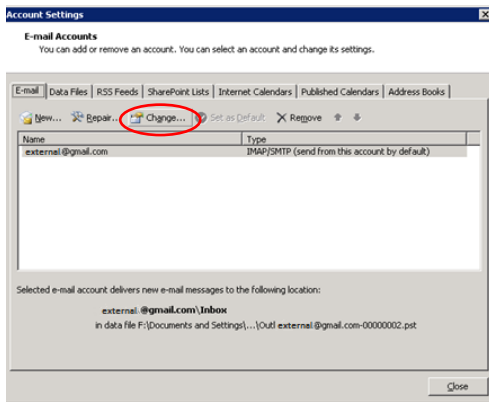


This screen indicates that further action is necessary to configure your computer. Symantec Encryption Satellite needs to perform the SSL/TLS to your mail server instead of your mail client.

Simply click OK to this message and then go into your mail client to perform the configuration.

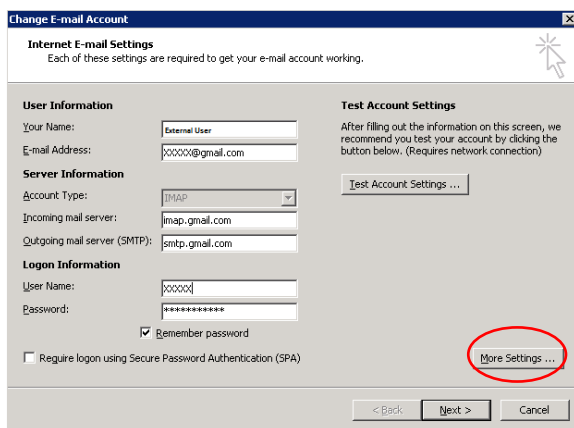
- The following screens show how to make these changes in Microsoft Outlook. For other mail clients, please refer to your user manual
 - Open Outlook and Go to "ACCOUNT SETTINGS"
 - Outlook 2007
 - Click the TOOLS menu and select ACCOUNT SETTINGS
 - Outlook 2010

- Click the FILE menu and select ACCOUNT SETTINGS
 - Select your email account and click CHANGE

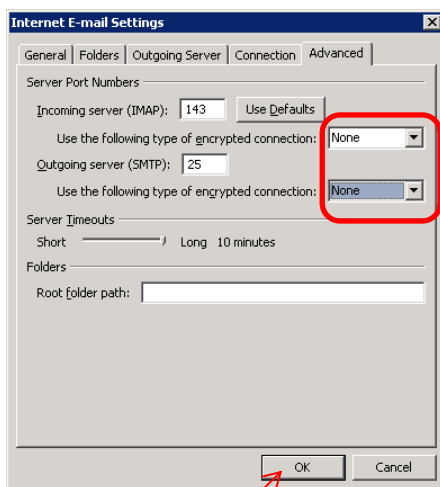


Ensure the correct email account is selected and click CHANGE

- Click the MORE SETTINGS button

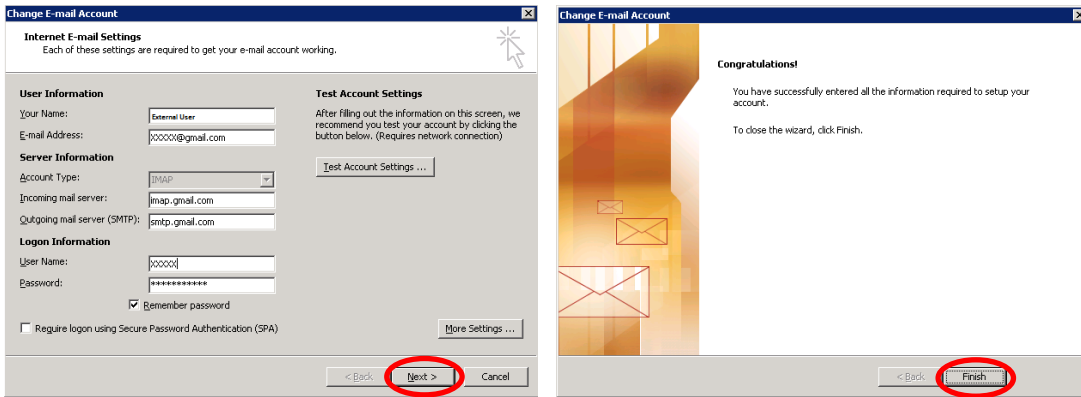


- Select the ADVANCED tab and make sure that the encryption field is set to NONE in both directions

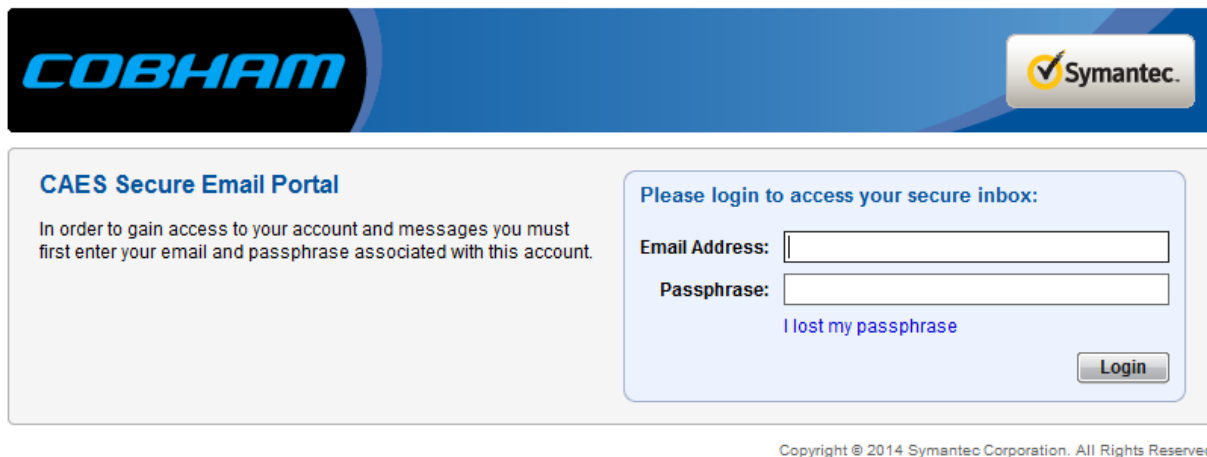


***NOTE: Notate these settings before you change them to NONE in case you uninstall PGP Universal later

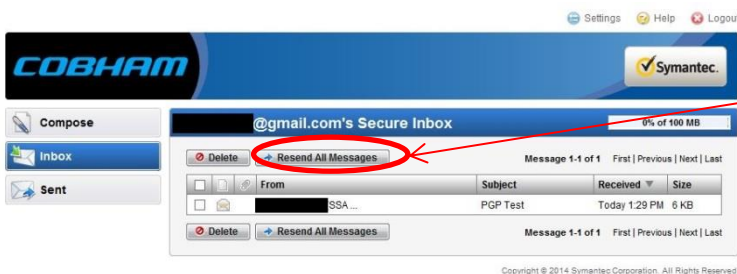
- Click OK
- Click NEXT on the CHANGE EMAIL ACCOUNT screen, then Click FINISH



- Close Outlook and then Re-Open Outlook
 - You should not receive the SSL/TLS Connection detected notification any longer.
- At this point, you have completed the configuration and can continue to use your email program normally as you always have.
- All emails from CAES that were secured PRIOR to you completing this configuration are still located in your CAES Secure Email portal.
 - Now that you have finished your configuration, you can re-send these emails through the new configuration to your normal email client.
- Log into the CAES Secure Email portal at <https://keys.cobhamna.com>



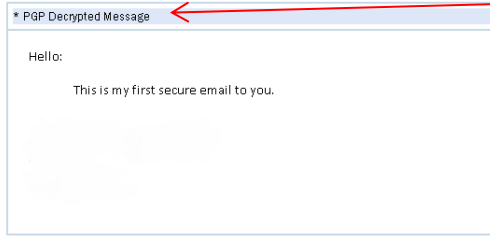
- Click on INBOX on the left hand side (if not selected already)



- The message(s) that were secured BEFORE you completed the configuration will be shown here. Click the **RESEND ALL MESSAGES** button.
- The servers will send all messages back through the system with your new PGP Satellite configuration (encrypted to your new PGP key)

- To verify that the configuration is working, go back to your email client and look at the new message(s) that have arrived. The email should look as follows:

First Message to a Non-Aeroflex user
 User, Aeroflex [AeroflexUser@aeroflex.com]
 Sent: Thu 7/12/2012 3:39 PM
 To: External@gmail.com



Notice the “PGP Decrypted” message and the blue border (annotation)

CONFIGURATION AND TESTING IS NOW COMPLETE.

- If the newly arrived email looks as follows, then it is not working

First Message to a Non-Aeroflex user

User, Aeroflex [AeroflexUser@aeroflex.com]

Sent: Thu 7/12/2012 3:39 PM

To: External@gmail.com

Message | Version.txt (131 B) | Message.pgp (3 KB)

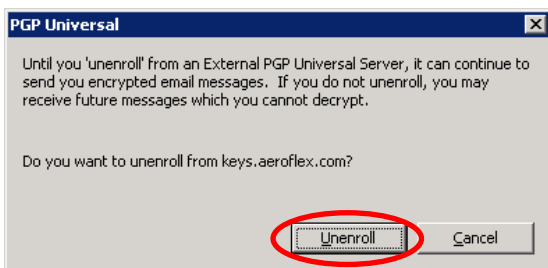
correctly:

Please reboot your computer at this point and to resend all messages again. If that fails, please contact CAES at PGP.Admins@Cobhamaes.com

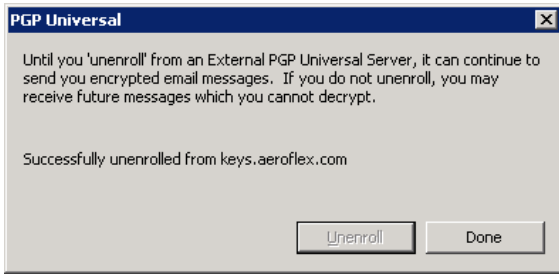
try

Uninstalling Symantec Encryption Satellite

- If for any reason you wish to uninstall Symantec Encryption Satellite (such as switching delivery options), you must un-enroll from the CAES Secure Email servers, otherwise you may continue to receive secure email from CAES that you would not be able to read.
 - Uninstalling Symantec Encryption Satellite will not have any effect on the already decrypted email in your client. You will still be able to read previously sent secure emails from CAES that were sent while you had Symantec Encryption Satellite selected as your delivery option.
- Uninstall Symantec Encryption Satellite as you would any other application
 - CONTROL PANEL > PROGRAMS AND FEATURES
- When you select to uninstall, it will prompt you to un-enroll



- After contacting the CAES Secure Email servers, you will receive the following notice:



- The program will continue to be uninstalled and you will be asked to reboot when you are finished.
- **NOTE:** If you performed the changes on the top of page 9 when you installed Symantec Encryption Satellite, be sure to set them back to their original values.

Configuring Key or Digital ID/Certificate Delivery Option

- After selecting the Key or Digital ID/Certificate option, you are presented with a screen asking you for the “public” portion of your PGP Key/Digital Certificate.

NOTE: If you need assistance exporting your Public Key, please see Appendix A of this document.

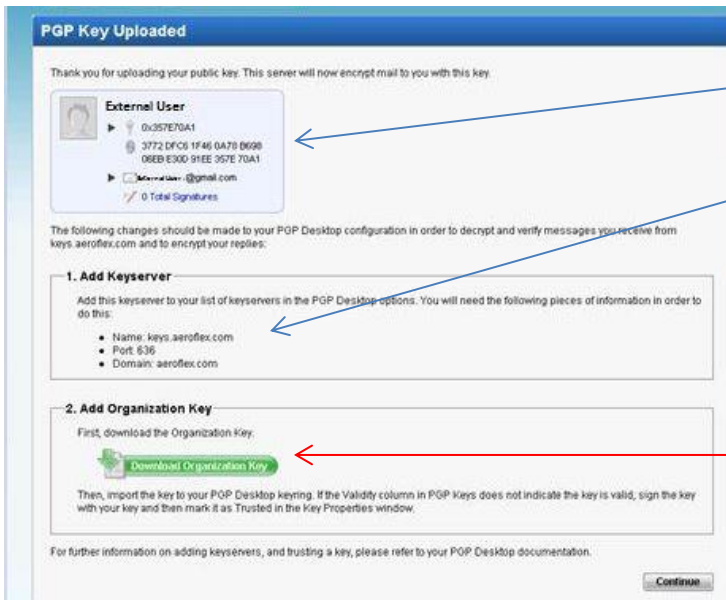
1 - Click BROWSE and select the file you exported that contains your public key

2 - Click CONTINUE

- The next screen you are presented with depends on what type (PGP or S/MIME) of public key you just uploaded. Please proceed to the appropriate section for the type of key you uploaded.

Configuring Your Account using a PGP Public Key

- After uploading your public PGP key, you are presented with the following screen and must configure a few things on your PGP Desktop software. PGP Desktop software is the only CAES supported PGP client.



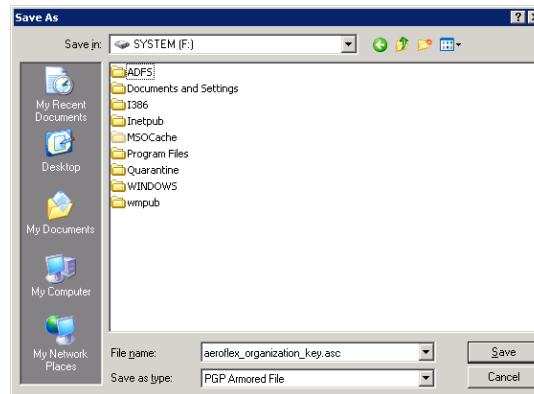
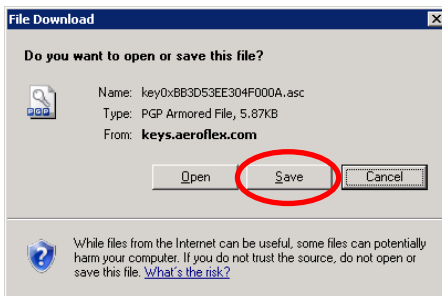
The uploaded PGP key information is displayed here. Verify it is correct

This information for CAES's PGP keyserver is needed so that you do not need to exchange public keys with CAES users. Configuring this allows PGP Desktop to search for, and find, the public keys of CAES users.

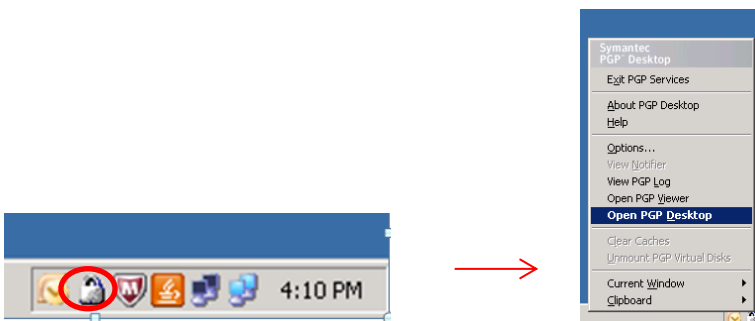
Click the **DOWNLOAD** button.

You must download CAES's organization PGP key so that you can verify and trust all CAES PGP keys for encryption with PGP Desktop.

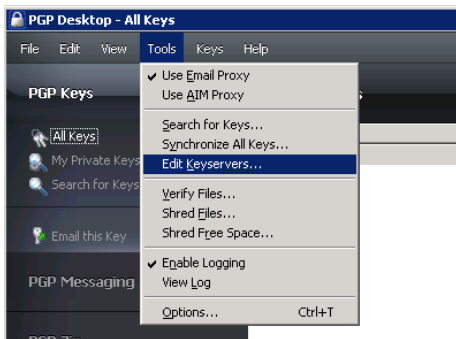
- Save the CAES organization key to a location on your computer.



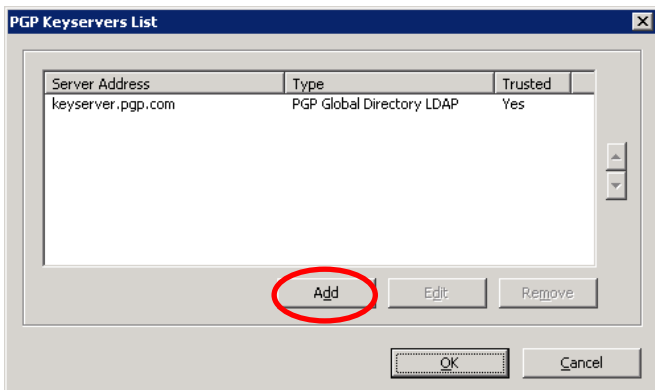
- Open your PGP Desktop software by right clicking the lock icon in your system tray



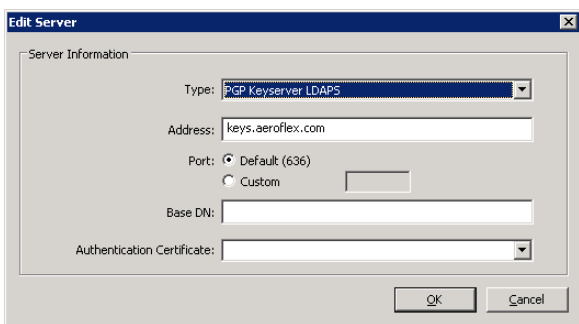
- Select the **TOOLS** menu and select **EDIT KEYSERVERS**



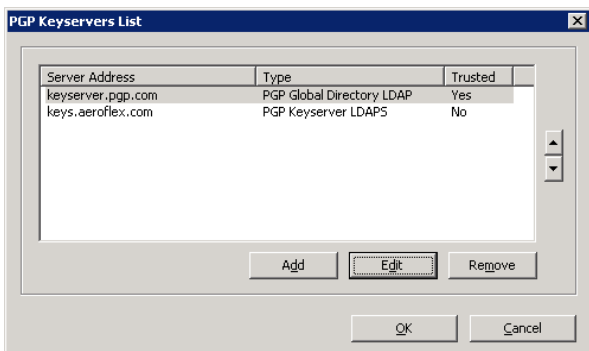
- Select ADD



- Fill out the new keyserver information as follows and then click OK:



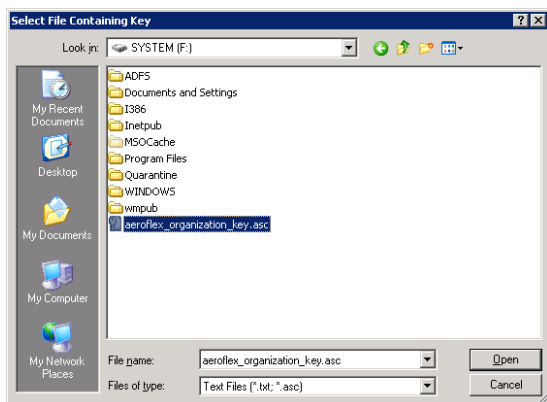
- Verify your Keyserver list now includes the keys.CobhamNA.com server
 - *You may have more servers than shown here*



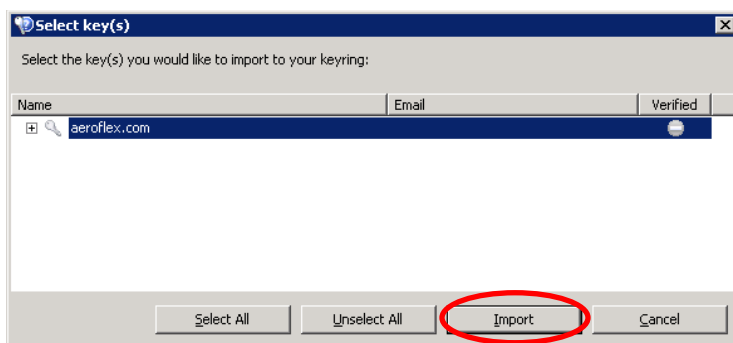
- Select the FILE menu and select IMPORT



- Browse to the CAES organization key you saved earlier and select OPEN:



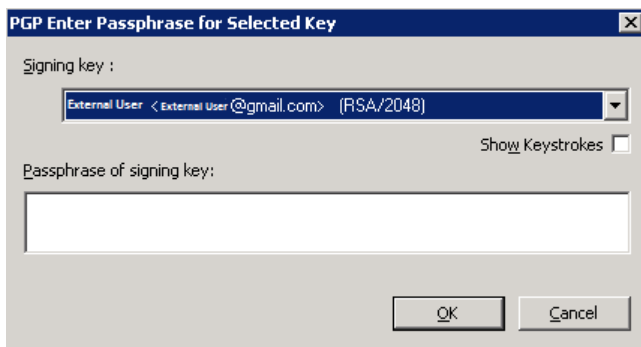
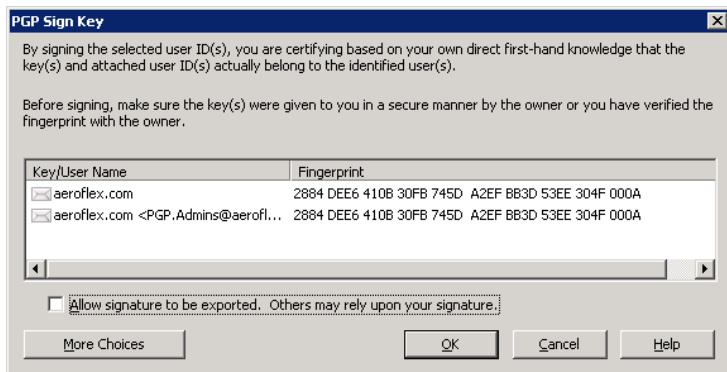
- At the Select Key screen, click IMPORT:



- Right-click the key in PGP Desktop and select SIGN

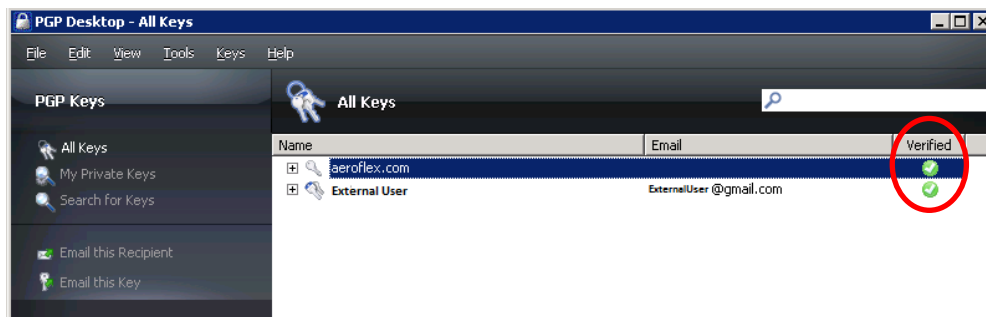


- Confirm that you want to sign the key by clicking OK (you may be asked for your personal PGP key passphrase)



NOTE: This is asking for your personal PGP key passphrase, NOT the CAES Secure Email portal passphrase. You will only see this screen if your passphrase is not cached.

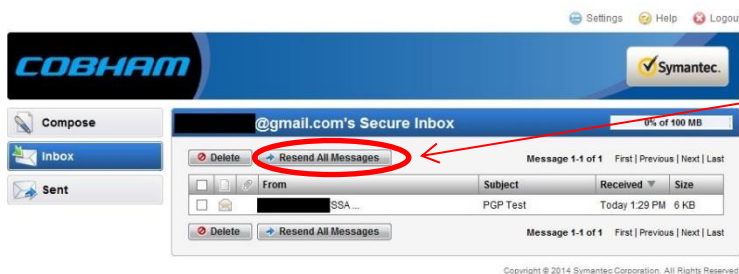
- You should now see the CAES organization key as verified



- You have completed the configuration.
- All emails from CAES that were secured PRIOR to you completing this configuration are still located in your CAES Secure Email portal.
 - Now that you have finished your configuration, you can re-send these emails through the new configuration to your normal email client.
- Log into the CAES Secure Email portal at <https://keys.cobhamna.com>

Copyright © 2014 Symantec Corporation. All Rights Reserved.

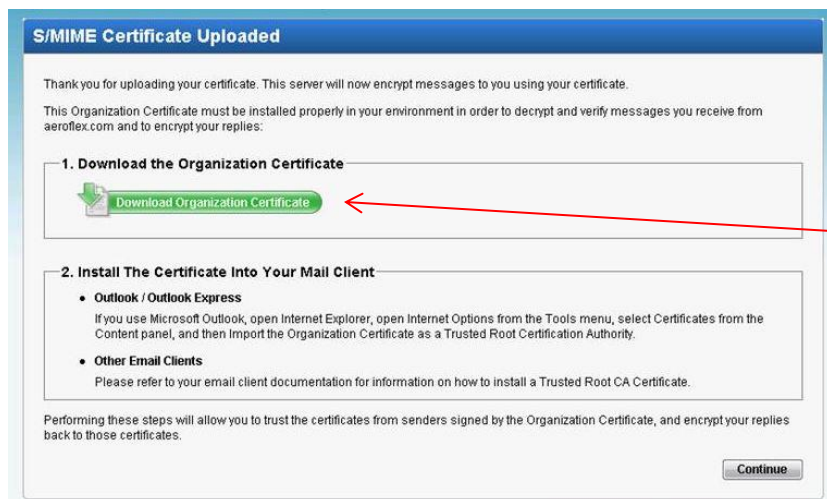
- Click on INBOX on the left hand side (if not selected already)



- The message(s) that were secured BEFORE you completed the configuration will be shown here. Click the **RESEND ALL MESSAGES** button.
- The servers will send all messages back through the system, this time encrypting to your PGP key

Configuring Your Account using an S/MIME (X509) Public Key

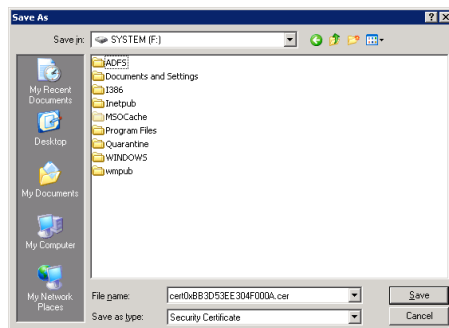
- After uploading your public S/MIME key, you are presented with the following screen and must configure a few things on your computer.



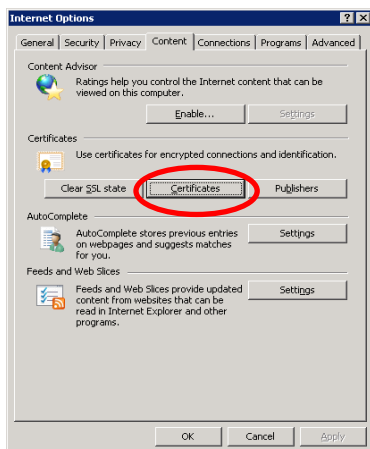
Click the **DOWNLOAD** button.

You must download CAES's Organization certificate so that your computer will trust CAES S/MIME certificates for decryption with your mail client.

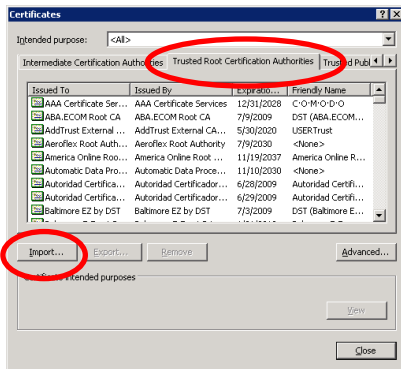
- Save the CAES Organization certificate to a location on your computer



- Open the Internet Options on the computer
 - CONTROL PANEL > INTERNET OPTIONS > CONTENT tab > CERTIFICATES



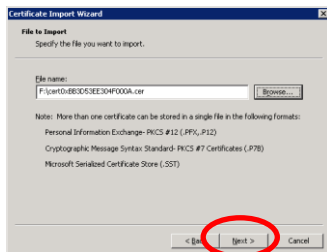
- Select the TRUSTED ROOT CERTIFICATE AUTHORITIES tab and then click IMPORT



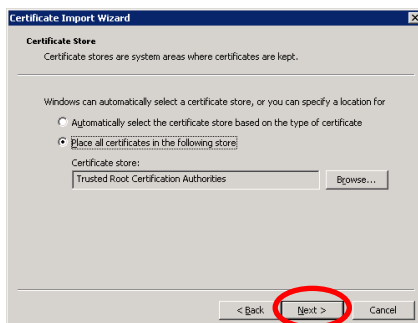
- At the WELCOME TO THE CERTIFICATE IMPORT WIZARD, click NEXT



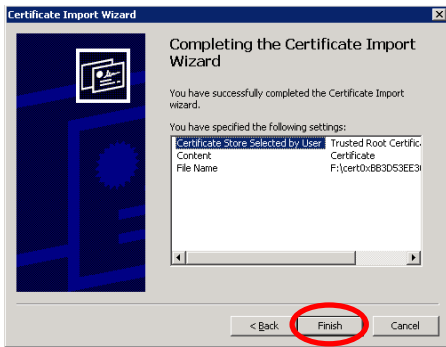
- Click BROWSE and select the CAES Organization certificate you saved earlier and then click NEXT



- Ensure the certificate will be placed into the TRUSTED ROOT CERTIFICATION AUTHORITIES and click NEXT



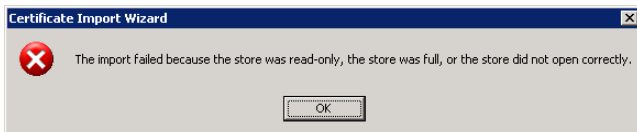
- At the COMPLETING THE CERTIFICATE IMPORT WIZARD, click FINISH



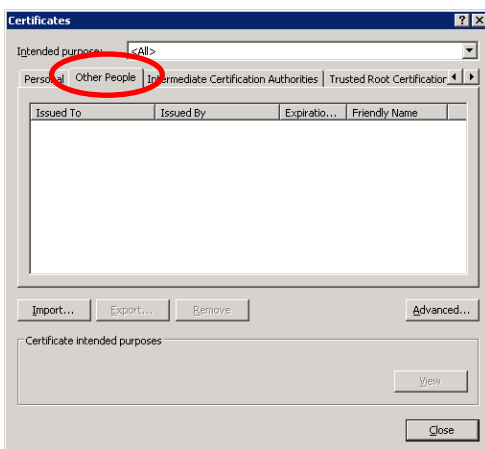
- Ensure that you receive a successful confirmation and click OK



- **NOTE: If you receive the message below:**

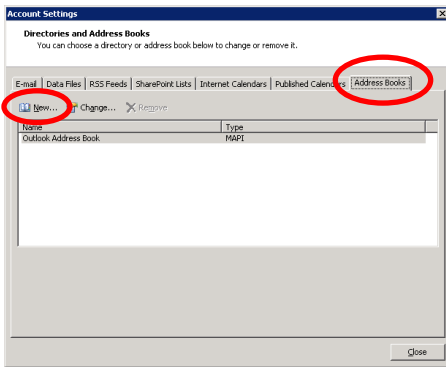


- Go back and perform the import again, this time using the OTHER PEOPLE tab:

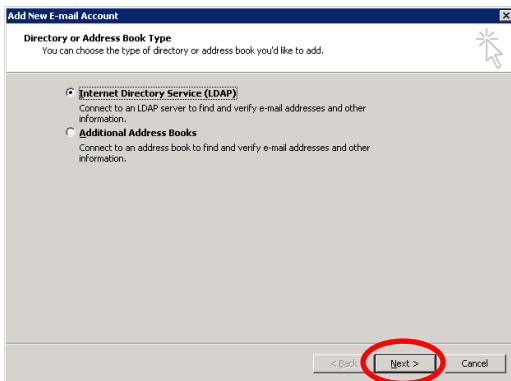


- The following configuration is optional, but recommended. It will let your email client search for CAES S/MIME certificates without you having to exchange signed emails with the CAES user.
 - The following screens show how to make these changes in Microsoft Outlook. For other mail clients, please refer to your user manual
 - Open Outlook and Go to "ACCOUNT SETTINGS"
 - Outlook 2007
 - Click the TOOLS menu and select ACCOUNT SETTINGS
 - Outlook 2010
 - Click the FILE menu and select ACCOUNT SETTINGS

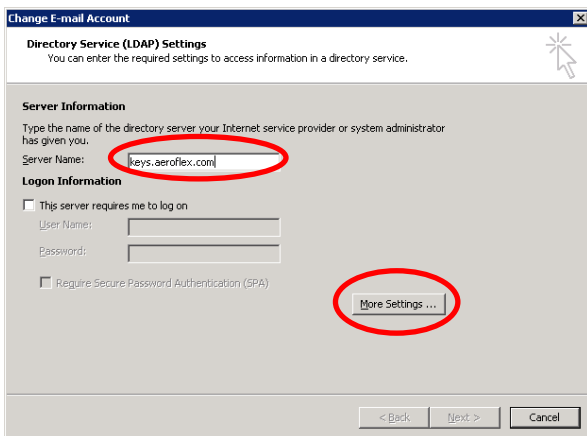
- Select the ADDRESS BOOK tab and then click NEW



- Choose INTERNET DIRECTORY SERVICE and click NEXT



- Enter keys.CobhamNA.com for the server name and then click MORE SETTINGS



- On the CONNECTION tab, fill out as follows

Microsoft LDAP Directory

Connection Search

Display Name
The display name as it appears in the Address Book
[keys.aeroflex.com]

Connection Details
Port: 636
Use Secure Sockets Layer ☒

OK Cancel Apply

- On the SEARCH tab, fill out as follows

Microsoft LDAP Directory

Connection Search

Server Settings
Search timeout in seconds: 60
Specify the maximum number of entries you want to return after a successful search: 100

Search Base
☐ Use Default
☒ Custom: o=Users

Browsing
☐ Enable Browsing (requires server support)

OK Cancel Apply

- Click OK, then click NEXT, then click FINISH, and finally click CLOSE
- Now close Microsoft Outlook and re-open it to make the new address book take effect
- You have completed the configuration.
- All emails from CAES that were secured PRIOR to you completing this configuration are still located in your CAES Secure Email portal.
 - Now that you have finished your configuration, you can re-send these emails through the new configuration to your normal email client.
- Log into the CAES Secure Email portal at <https://keys.cobhamna.com>

COBHAM Symantec

CAES Secure Email Portal

In order to gain access to your account and messages you must first enter your email and passphrase associated with this account.

Please login to access your secure inbox:

Email Address:

Passphrase:

[I lost my passphrase](#)

Login

Copyright © 2014 Symantec Corporation. All Rights Reserved.

- Click on INBOX on the left hand side (if not selected already)

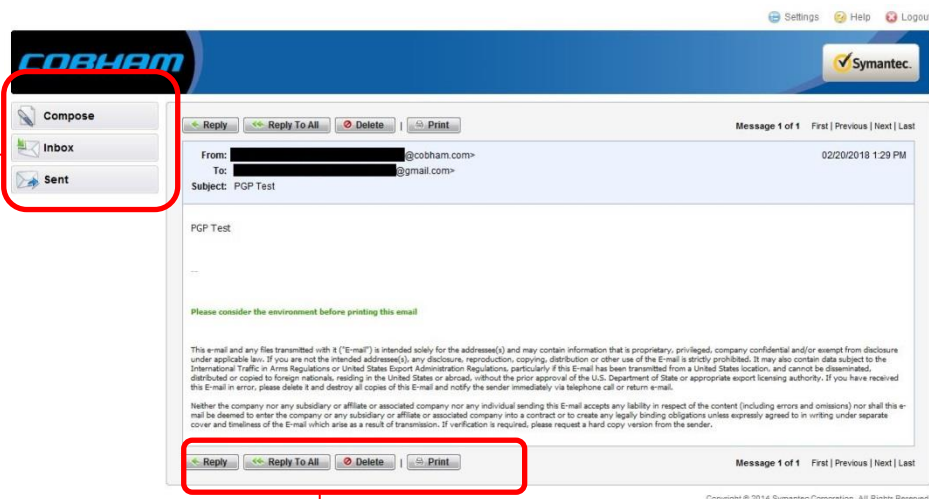


- The message(s) that were secured BEFORE you completed the configuration will be shown here. **Click the RESEND ALL MESSAGES button.**

- The servers will send all messages back through the system, this time encrypting to your S/MIME key

Using Your CAES Secure Email Portal

- The first screen you will see after selecting the Regular Email or PGP Web Messenger option, will be the original secure email sent by CAES.

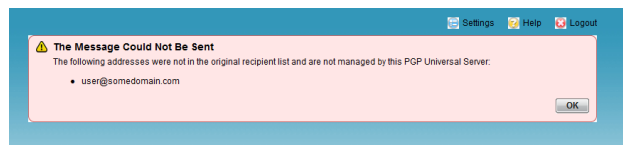


REMEMBER: Symantec Web Email:

EVERY email you receive from CAES will be a notification from the CAES Secure Email servers, and will contain a link to the corresponding message on the CAES Secure Email portal.

Regular Email: Non-secure emails from CAES will come in to your email program. Secure email's from CAES, however, will continue to be a notification that contains the link to the corresponding message.

- From the email message, you can REPLY, REPLY ALL, DELETE, and PRINT
 - REPLY: Replies securely to the CAES user that sent the message
 - REPLY ALL: Replies securely to all recipients of the original message
 - NOTE: You cannot add any new recipients to the email unless they have an CobhamAES.com email**



- DELETE: Deletes the email message on the portal
- PRINT: Prints the message

- From the navigation bar, you can COMPOSE, go to your INBOX, and go to your SENT items folder
 - COMPOSE: Creates a new email to one or many CobhamAES.com addresses
 - INBOX: Brings you to your INBOX view. Click here when finished reading a message.
 - SENT: Brings you to your SENT ITEMS view.

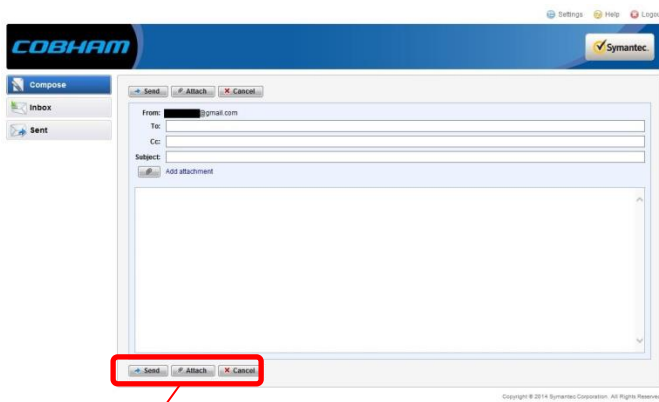
- Your INBOX view is as follows

Settings: Changes your delivery option
HELP: Displays PGP Help
LOGOUT: Logs out of the portal

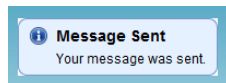
The amount of space your portal is using compared to your total allowed

You may click either the sender's name, or the subject to open the email

- The COMPOSE view is as follows



- From the COMPOSE screen, you can SEND, ATTACH, and CANCEL
 - SEND**: Sends the email. Click this when you are finished with the message. You will see:



- ATTACH**: Attaches a file to the secure email. Clicking ATTACH bring up the following screen:

1 - Click browse to select the file (15 MB max per file)

2 - Click Attach to add it to the attachment list

(If needed, highlight an attachment and click REMOVE)

3 - Click OK to complete the process or Cancel to void it

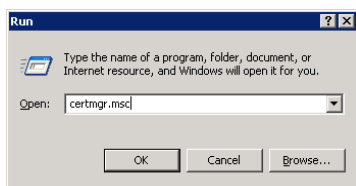
- CANCEL**: Cancels the email and returns you to your INBOX view

Appendix A

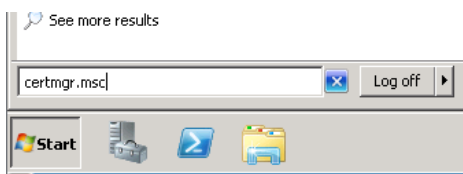
Exporting your S/MIME Certificate

This section describes how to export the public version of your S/MIME certificate from the Windows operating system. If you do not use Microsoft Windows, OR if you do not have Administrative rights on your computer, you will need to contact your local IT department for instructions on how to export your S/MIME public key.

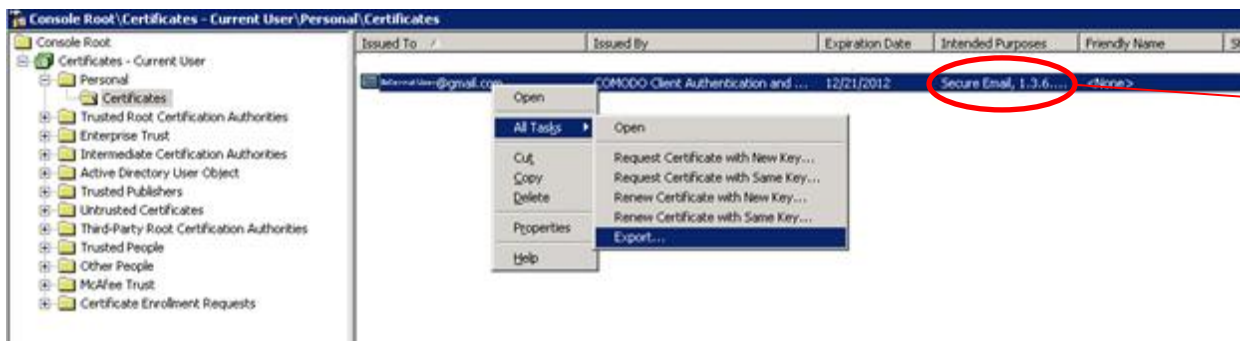
- Open the Certificates Manager
 - Windows XP - Click your START button and select RUN, then type certmgr.msc , then click OK



- Windows 7 – Click your START button and type certmgr.msc in the search bar, then hit ENTER



- Select the PERSONAL certificate store and then select the CERTIFICATES folder
 - Find your S/MIME certificate. Right click the certificate and choose ALL TASKS > EXPORT



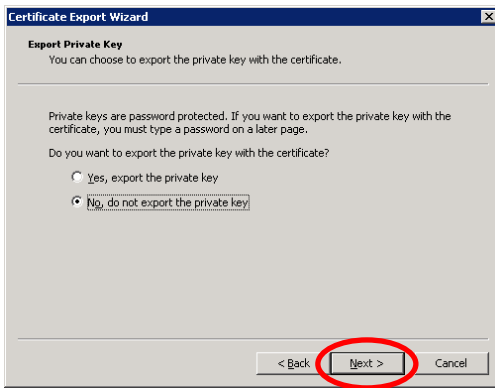
Secure Email
certificate

- At the
Welcome to
the certificate

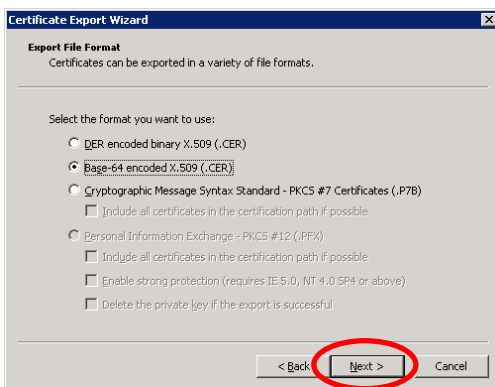
export wizard, click NEXT



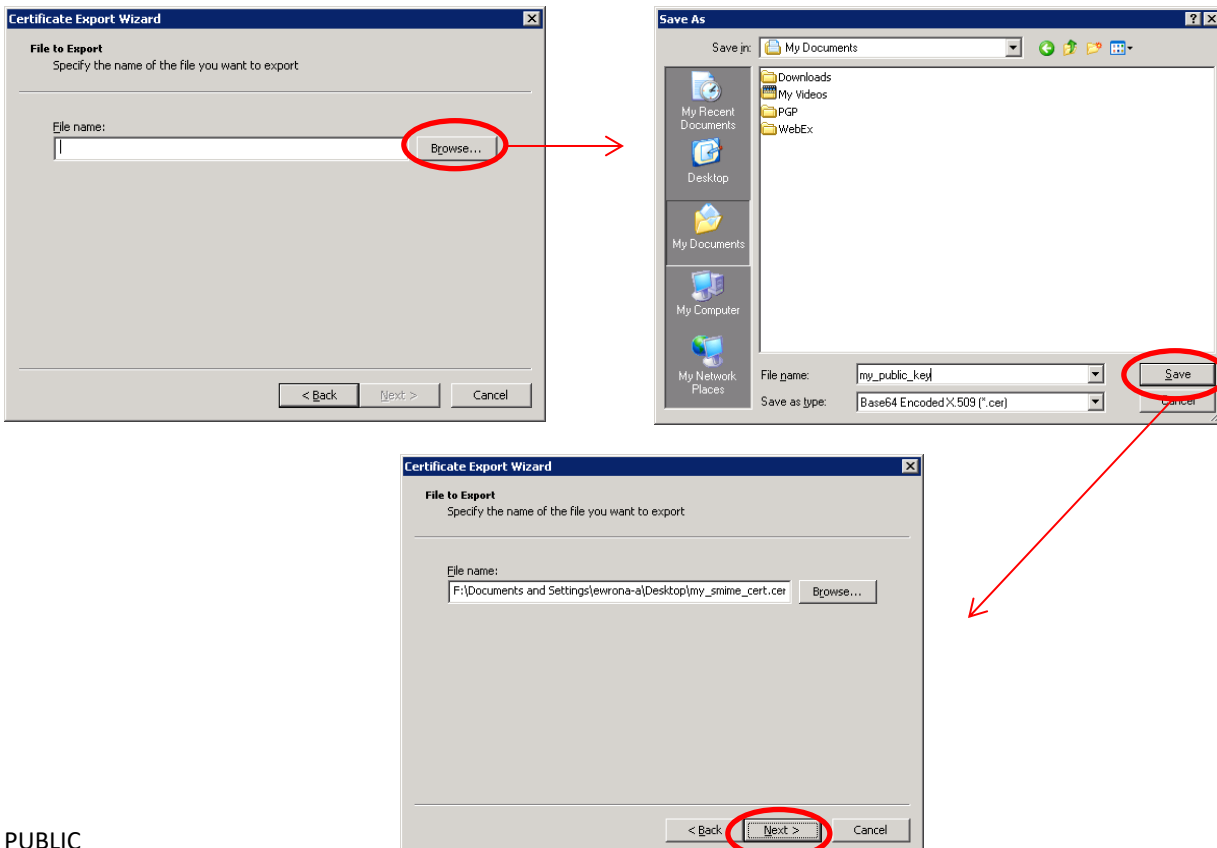
- At the Export Private Key screen, select NOT to export the private key and click NEXT



- At the Export File Format screen, choose Base-64 encoded X509 and click NEXT



- At the File to Export screen, click BROWSE. Enter a filename and location, click SAVE. Confirm and click NEXT.



- At the Completing the Export screen, confirm the settings and click FINISH



- You will receive the confirmation as follows




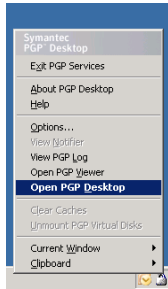
NOTE: Upload the generated file when you are asked for your key in the Enrolling as an External User section.

Exporting your PGP Key (from PGP Desktop)

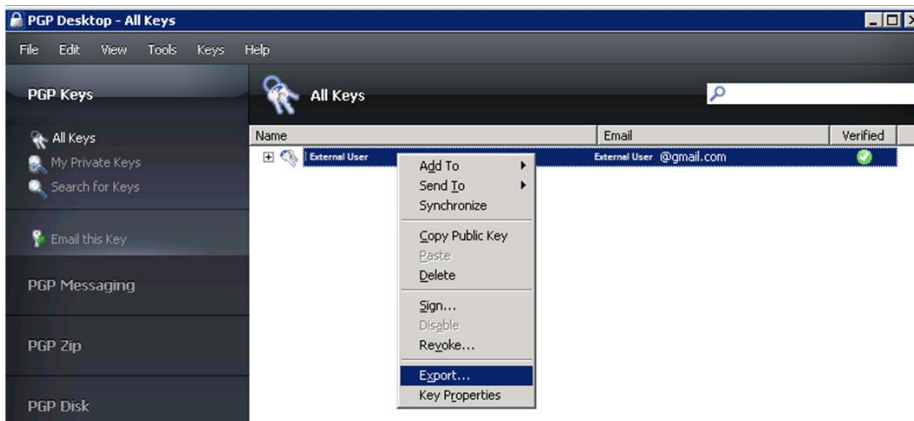
This section describes how to export the public version of your PGP key from the PGP Desktop software only. If you do not use PGP Desktop, you will need to contact your local IT department or software manual for instructions on how to export your PGP public key.

- Open PGP Desktop

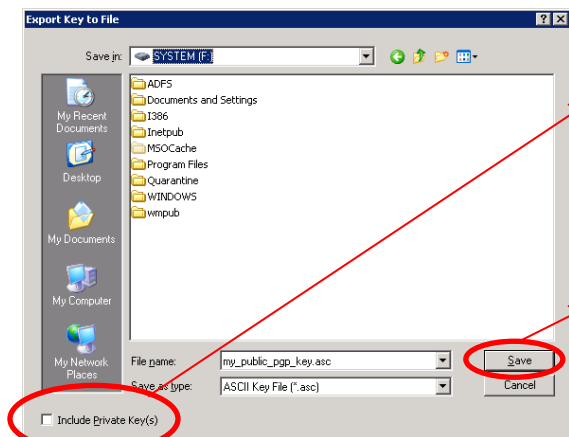
- Right click your  icon in the system tray and select Open PGP Desktop



- Click PGP KEYS on the left hand side and then right click your PGP key in the right hand pane and select EXPORT



- Select a location for the file and give it a filename. Make sure you DO NOT export the private key.



Ensure this box is NOT checked

When you click SAVE, the file is generated and saved, however, you are not given any confirmation. Upload the generated file when you are asked for your key in the Enrolling as an External User section.

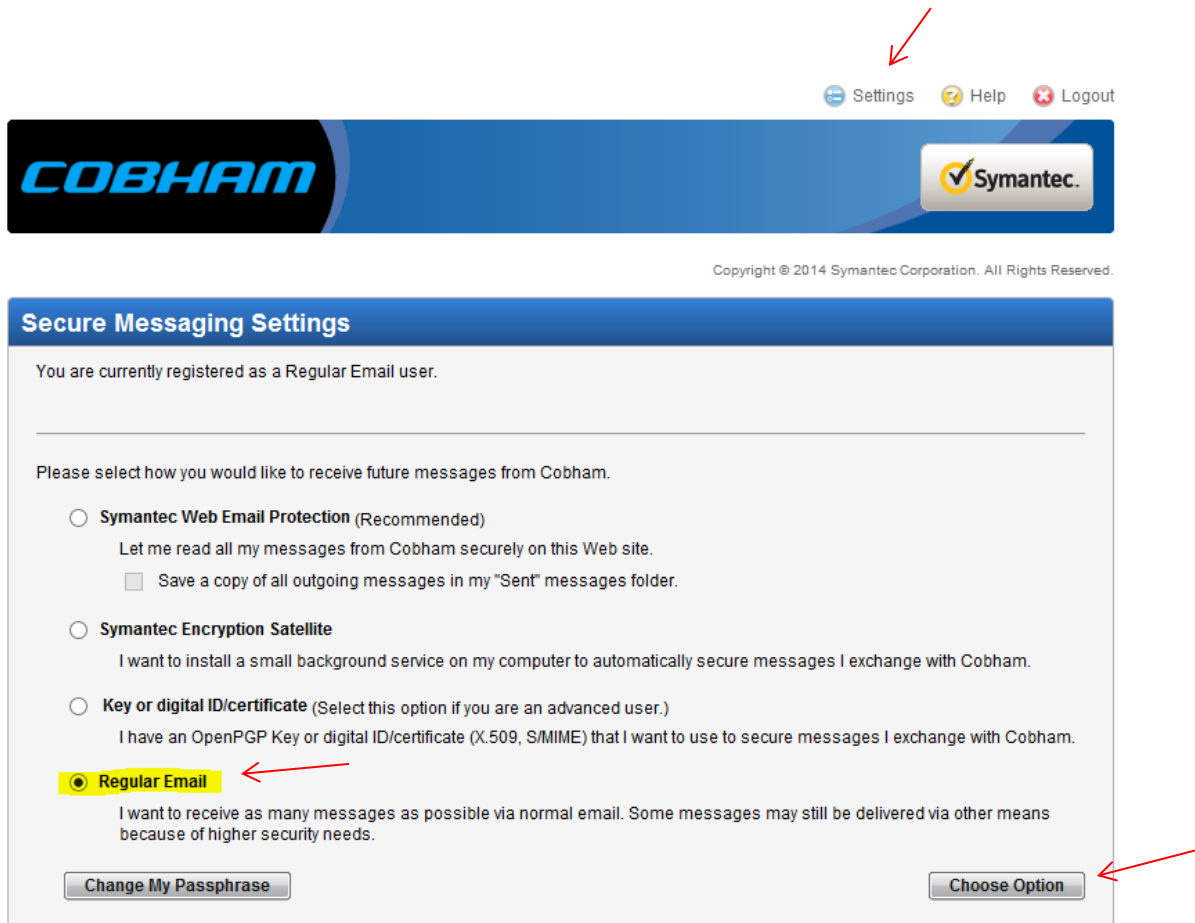
Troubleshooting

All my emails from CAES are “Secure Web Messenger”

Problem: All my emails from CAES are encrypted or only receive “Secure Web Messenger” email notices, even though the CAES sender did not encrypt the message.

Cause: Your Secure Messaging Settings are set to “Symantec Web Email Protection”

Solution: Log in to the CAES Secure Email Portal at <https://keys.cobhamna.com> and go to "Settings" and select the option for "Regular Email" and click “Choose Option”.



Settings Help Logout

COBHAM Symantec

Copyright © 2014 Symantec Corporation. All Rights Reserved.

Secure Messaging Settings

You are currently registered as a Regular Email user.

Please select how you would like to receive future messages from Cobham.

- ☐ **Symantec Web Email Protection** (Recommended)
Let me read all my messages from Cobham securely on this Web site.
☐ Save a copy of all outgoing messages in my "Sent" messages folder.
- ☐ **Symantec Encryption Satellite**
I want to install a small background service on my computer to automatically secure messages I exchange with Cobham.
- ☐ **Key or digital ID/certificate** (Select this option if you are an advanced user.)
I have an OpenPGP Key or digital ID/certificate (X.509, S/MIME) that I want to use to secure messages I exchange with Cobham.
- ☒ **Regular Email**
I want to receive as many messages as possible via normal email. Some messages may still be delivered via other means because of higher security needs.

[Change My Passphrase](#) [Choose Option](#)

I forgot my password for the CAES Secure Web Messenger”

Problem: I forgot my password to the CAES Secure Email Portal or my password has expired.

Solution: Go to the CAES Secure Email Portal at <https://keys.cobhamna.com> and click “I lost my passphrase”

- Enter the email address you originally registered on the CAES Secure Email Portal and click **Send**:

- You will receive an email with a link to reset your passphrase. If your account is in the "Locked" state, check your mailbox for the "Symantec Encryption Server Account Unlock" email from Symantec Encryption Server, and follow the instructions in the email to unlock your account
 - **Note:** if you do not receive the email within 30 minutes please check your SPAM folder and inform your IT department to allow emails from “DONOTREPLY@cobhamna.com”