COMODO
Creating Trust Online®

Comodo Two Factor

Software Version 2.8

How To Set Up Extra Security For Your Account

Guide Version 2.8.071813

Comodo Group Inc.
1255 Broad Street
STE 100
Clifton, NJ 07013

Table of Contents

1. How To Set Up Extra Security For Your Account

1.1. Overview

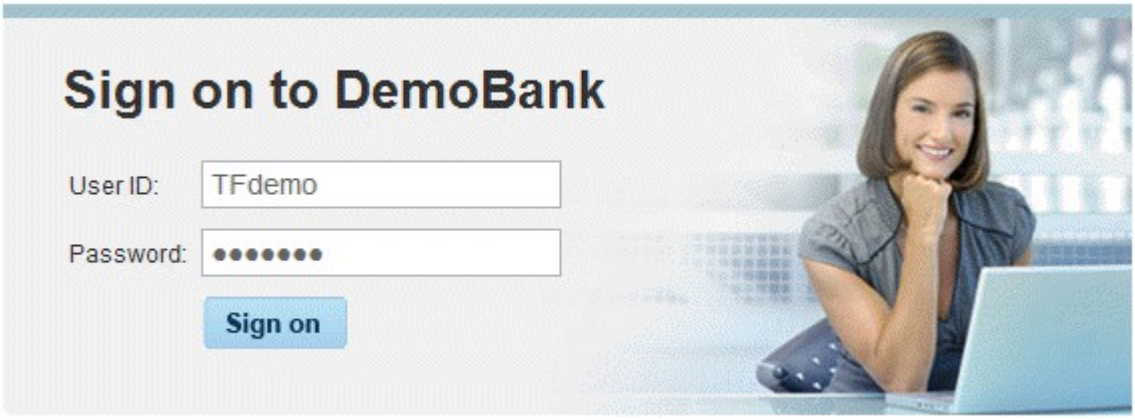
This short tutorial shows you how it's easy to add extra security when you log into your secure website or service account (for example, your online banking account) - and why we recommend that you add it to protect yourself against identity theft and fraud.

You can add it no matter where you access your secure account e.g. online banking, at home, in the office or any other personal computer - in fact you can add this superior level of protection to any computer you want, anywhere in the world.

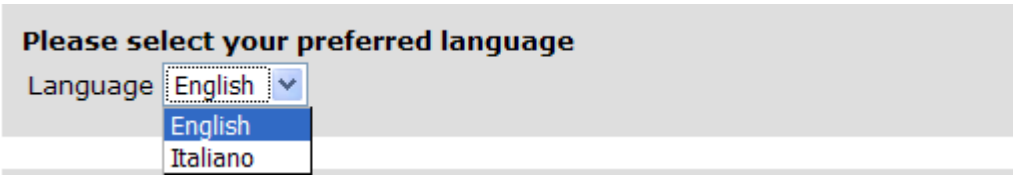
The process consists of three main parts:

(i) Selecting your preferred language
(ii) Setting up contact phone numbers and email address
(iii) Installing your personal digital certificate or security cookies onto your browser.

1. Start by logging in to your secure website as usual with your User ID and password.

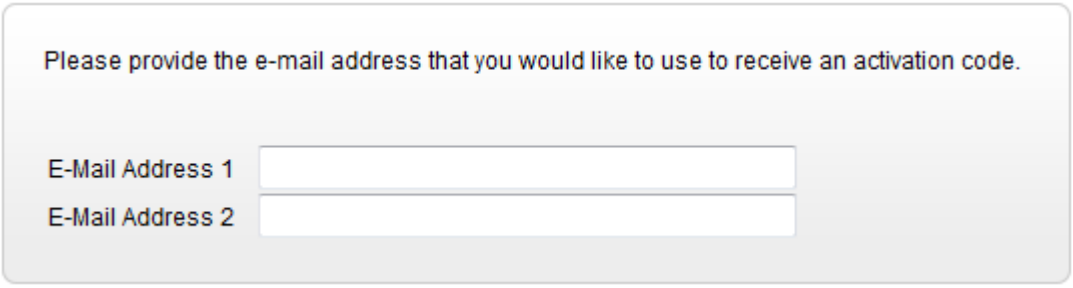


2. Next, select your preferred language from the Language drop-down menu. All the user interaction pages will be displayed in the selected language.

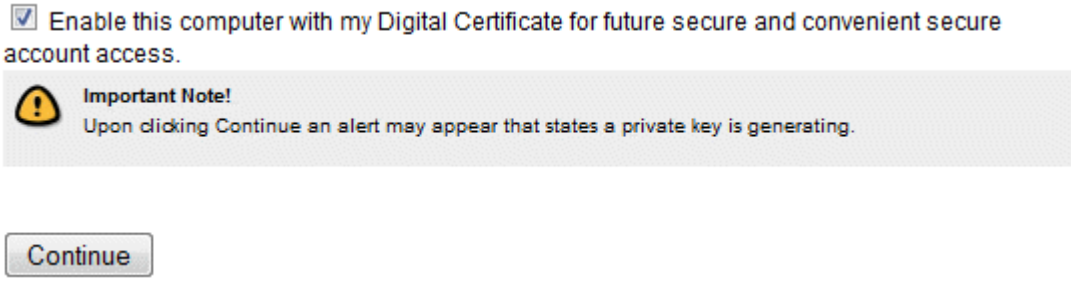


3. Next, we need you to supply us with contact phone numbers, which can be used to contact you:

4. In the form below phone numbers please provide the email address(es), that will be used to contact you in case you decide to reset your security settings.

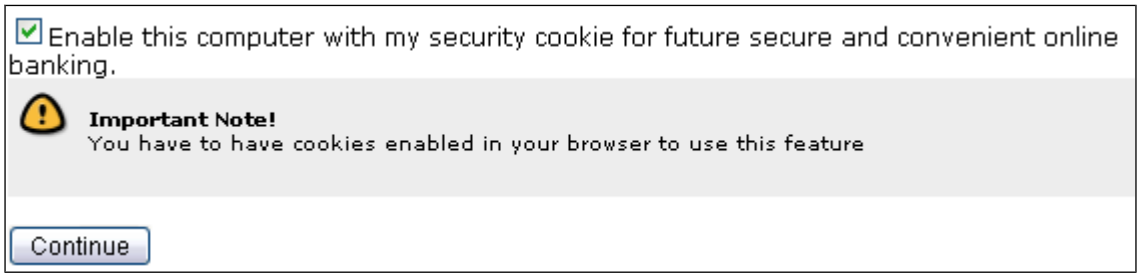


5. Finally, check the box ***'Enable this computer with my Digital Certificate for future secure and convenient on-line banking'***.



OR

'Enable my security cookie for future secure and convenient online banking' (see '**How to Enable Cookies**' section).



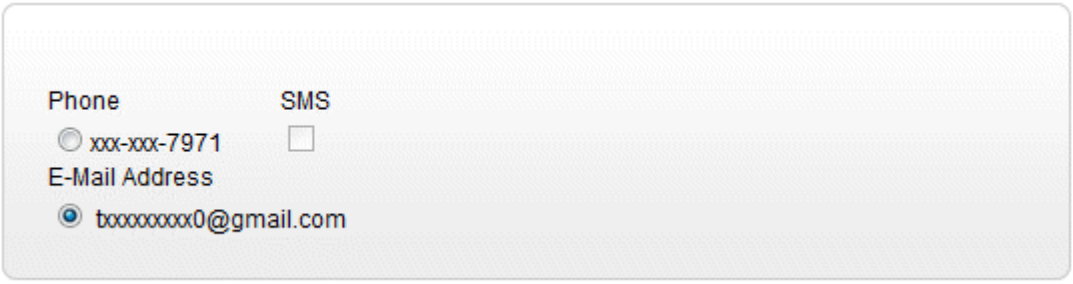
- Click 'Continue'.

Note: Digital Certificate OR Security Cookie Mode depends from your secure website's configuration options.

When logging in from an unregistered computer (such as a public or infrequently used computer) or when you login from a computer that you have not yet registered, you will be asked to select from your list of phone numbers and email addresses. We will then contact you and supply you with one-time password that will allow you to log into your account. You will also be given the opportunity to install an authentication certificate on the particular computer you are using so that you do not need to go through a similar activation procedure next time.

Note: This stage is very important. If you do not check this option, you will not install the extra security measures and will need to answer one of your security questions the next time you log into your account.

If you did not install a digital certificate on your computer you will be prompted to choose one of your contact phone numbers or email address the next time you log in. (see below)



We will then contact you and supply you with an account access activation code.

6. The final stage of the procedure is to install a digital certificate on your computer. This digital certificate will be used to identify and authenticate you to your secure website every time you log on to our website - meaning you enjoy a faster, more secure on line account access experience.

   Before generation and installation of the certificate you need to agree to the certificate subscriber agreement:

   The installation varies depending on which browser you are running:

- **Click here if you are running Internet Explorer**
- **Click here if you are running Internet Explorer 7 on Vista**
- **Click here if you are running Firefox**
- **Click here if you are running Opera**

- **Click here if you are running Safari**
- **Click here if you are running Google Chrome**

1.2. Installing Your Certificate on Internet Explorer

7. Internet Explorer automatically installs your certificate, so you need only select 'Yes' at both Windows dialog boxes as shown.

Selecting "Yes" at the first dialog will instruct your browser to contact a trusted certificate authority and automatically download and install your certificate.

Internet Explorer will then ask you for permission to add the new certificate into the master certificate store.

Your browser will now automatically download and install your certificate.

That's it! The next time you log into your account, our servers will automatically detect this certificate on your computer - meaning we identify you as the true owner of your account by recognizing not only your User ID and Password, but your computer as well.

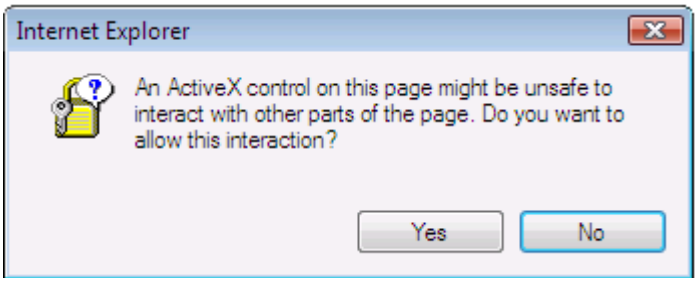
This security works in background mode and is 100% transparent you log straight in as you've always done without answering any extra security questions.

If you need to login from a different computer than the one you have added, you will be asked to answer one of the security questions that you set up earlier. Once inside your account, you'll then be prompted to install a digital certificate on that computer too.

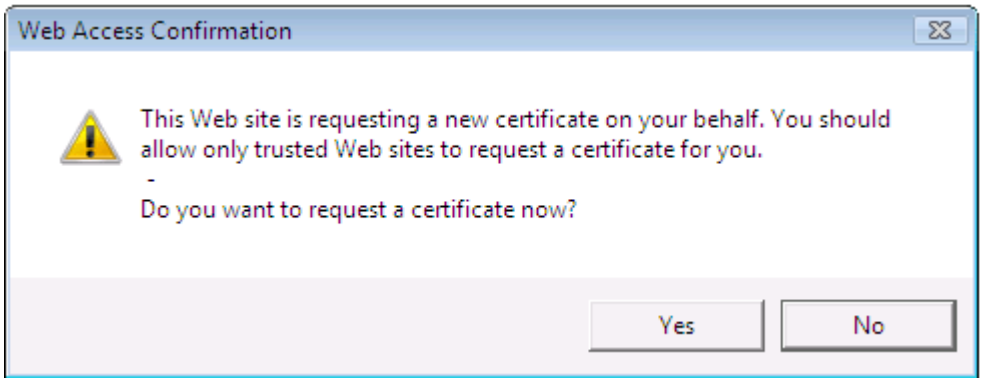
1.3. Installing Your Certificate on Internet Explorer 7 on Vista

7. This browser provides automatic installation of the certificate. You should only confirm getting and adding of it.

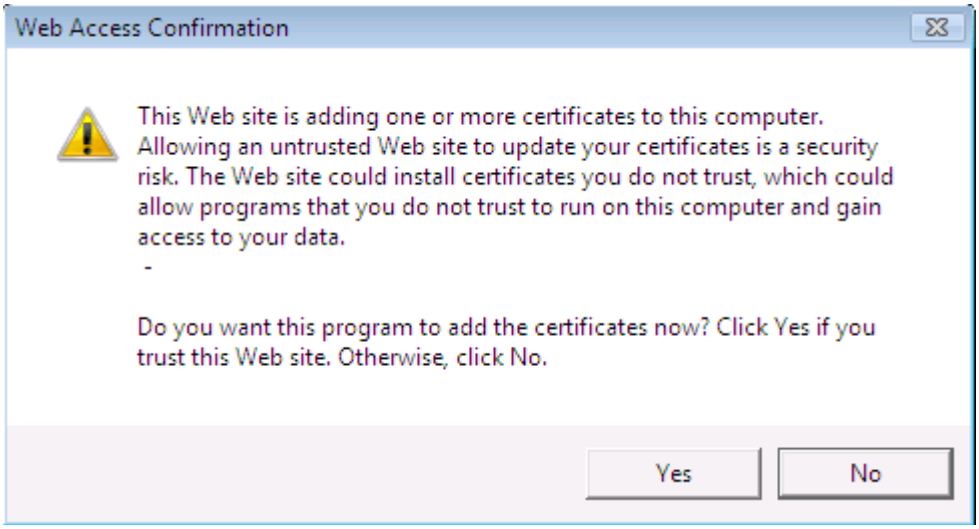
   Internet Explorer 7 may prompt you to enable ActiveX controls on your computer. To install your certificate, you will need click on 'Yes' to allow ActiveX interaction.



8. Next, IE7 will ask you to confirm your certificate request. Click 'Yes':



9. Now you need to import your new certificate into IE's master certificate store. Confirm this process by clicking the 'Yes' button:



Your browser will now automatically download and install your certificate.

That's it! The next time you log into your account, our servers will automatically detect this certificate on your computer - meaning we identify you as the true owner of your account by recognizing not only your User ID and Password, but your computer as well.

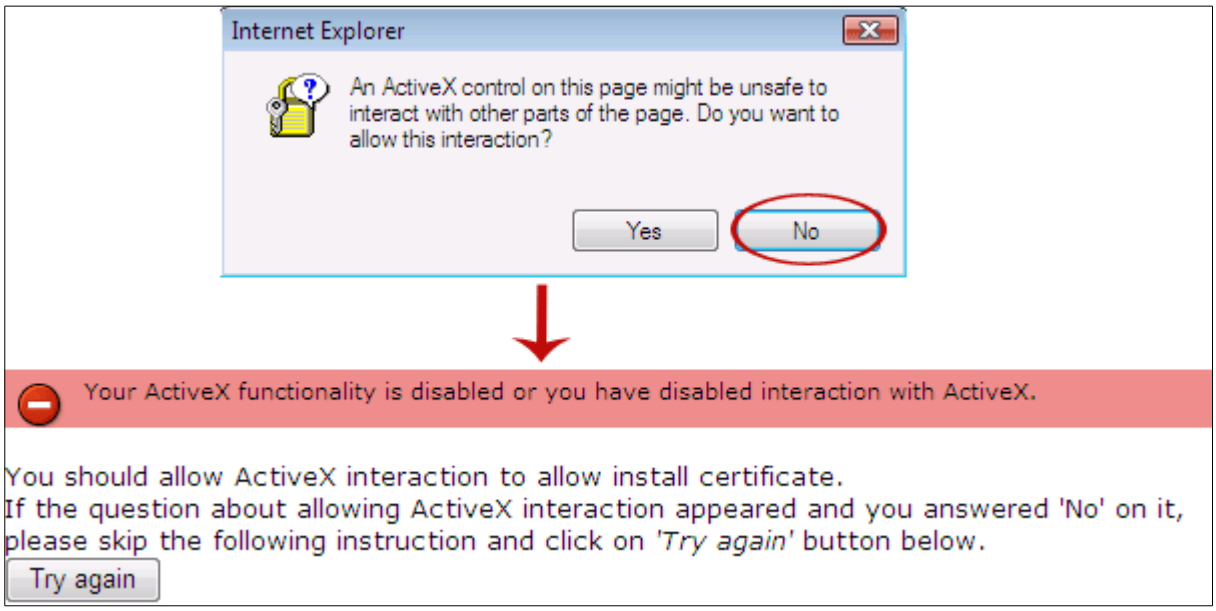
This security works in background mode and is 100% transparent you log straight in as you've always done without answering any extra security questions.

If you need to login from a different computer than the one you have added, you will be asked to answer one of the security questions that you set up earlier. Once inside your account, you'll then be prompted to install a digital certificate on that computer too.

1.3.1. Important Note

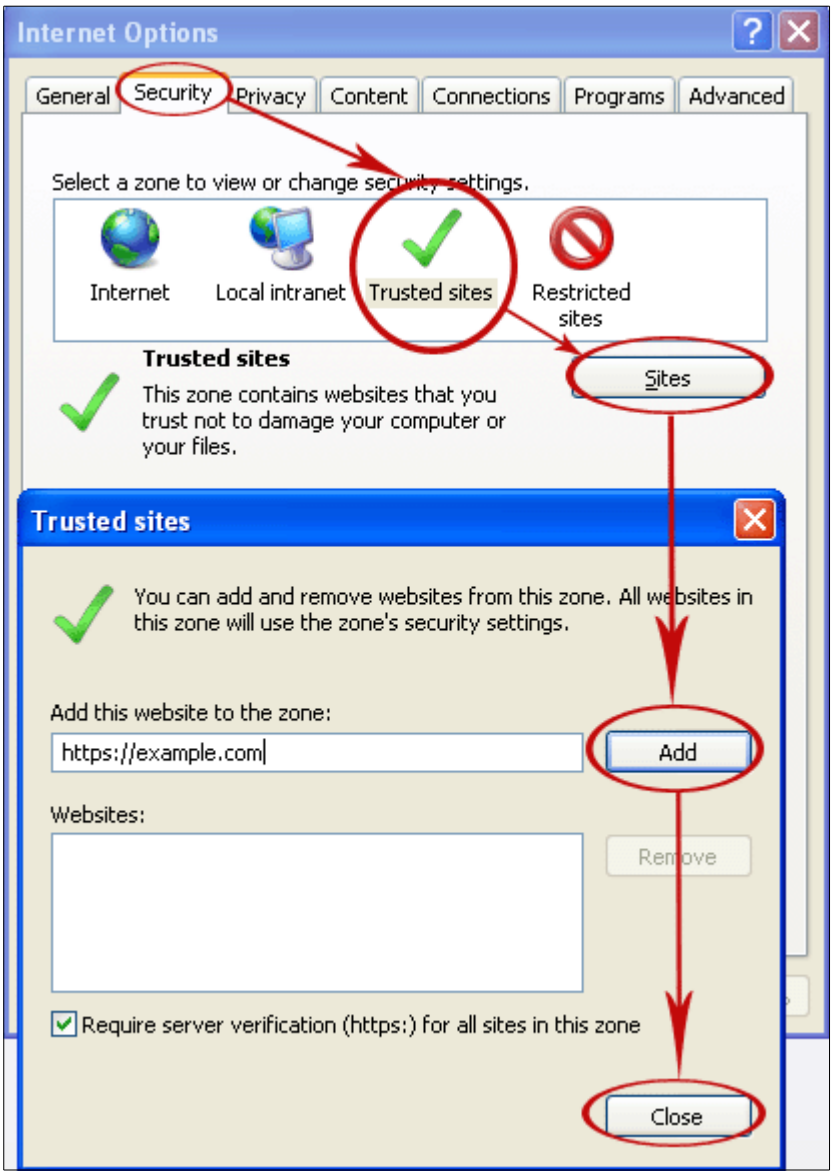
If your ActiveX interaction was disabled or you have clicked 'No' instead of allowing interaction, you will be prompted to change settings for ActiveX interaction and to try once more.

i. **You didn't allow interaction (selected 'No').** Follow these instructions:



ii. **Your interaction is disabled**. Follow these instructions:

- Open Internet Explorer and click 'Tools' then 'Internet Options' in the main tool bar. This will open the IE 'Internet Options' window.
- Next, click the 'Security' button then click the 'Trusted sites' category. This will enable 'Sites' button, click on it.
- In pop up window 'Trusted site' enter site's URL and click on 'Add' button. Click 'Close' when done.



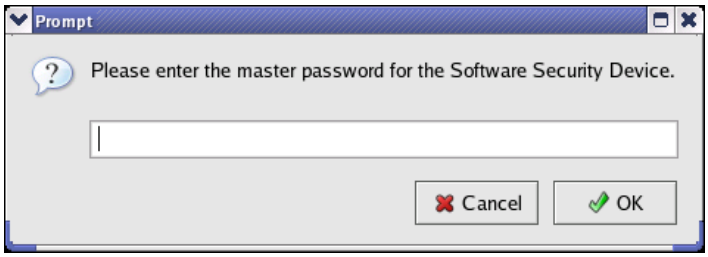
Next, you will be prompted to start again, sign-on and to install certificate. Click on 'Start again' button.

Then request the certificate and import it, and IE automatically install your certificate.

1.4. Installing Your Certificate on Firefox

If you have never used digital certificates before, and haven't specified the password to access the certificate storage, Firefox will ask you to specify a password.

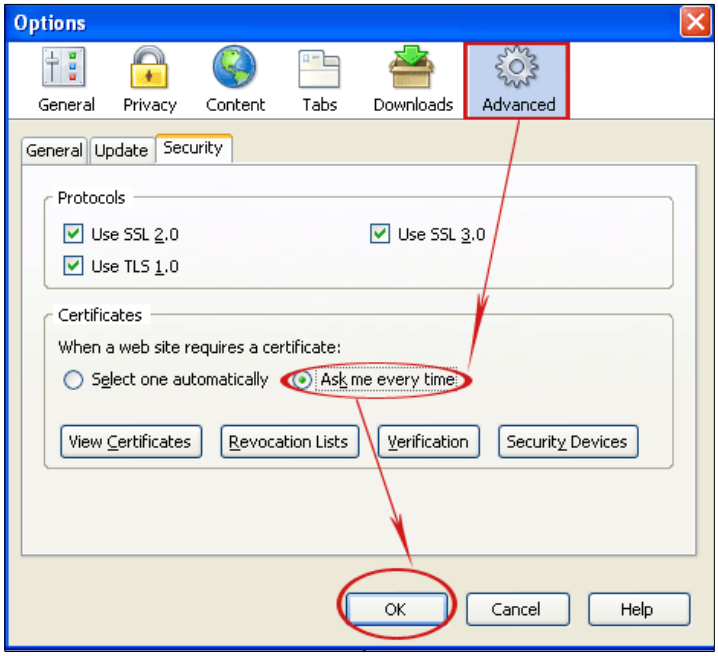
In future, Firefox will request this password to install a new certificate or to retrieve an existing certificate.



1.4.1. Note for Advanced Users

If you have more than one certificate on your PC, you need to tell Firefox to ask you which certificate it should use when accessing your secure website e.g. anybank.com. To do this:

7. Open Firefox
8. Go to Tools - Options
9. Click the 'Advanced' tab
10. Click the 'Security' sub-tab
11. Check the 'Ask me every time' radio button.
12. Click 'OK' to preserve changes.



Your browser will now automatically download and install your certificate.

That's it! The next time you log into your account, our servers will automatically detect this certificate on your computer - meaning we identify you as the true owner of your account by recognizing not only your User ID and Password, but your computer as well.

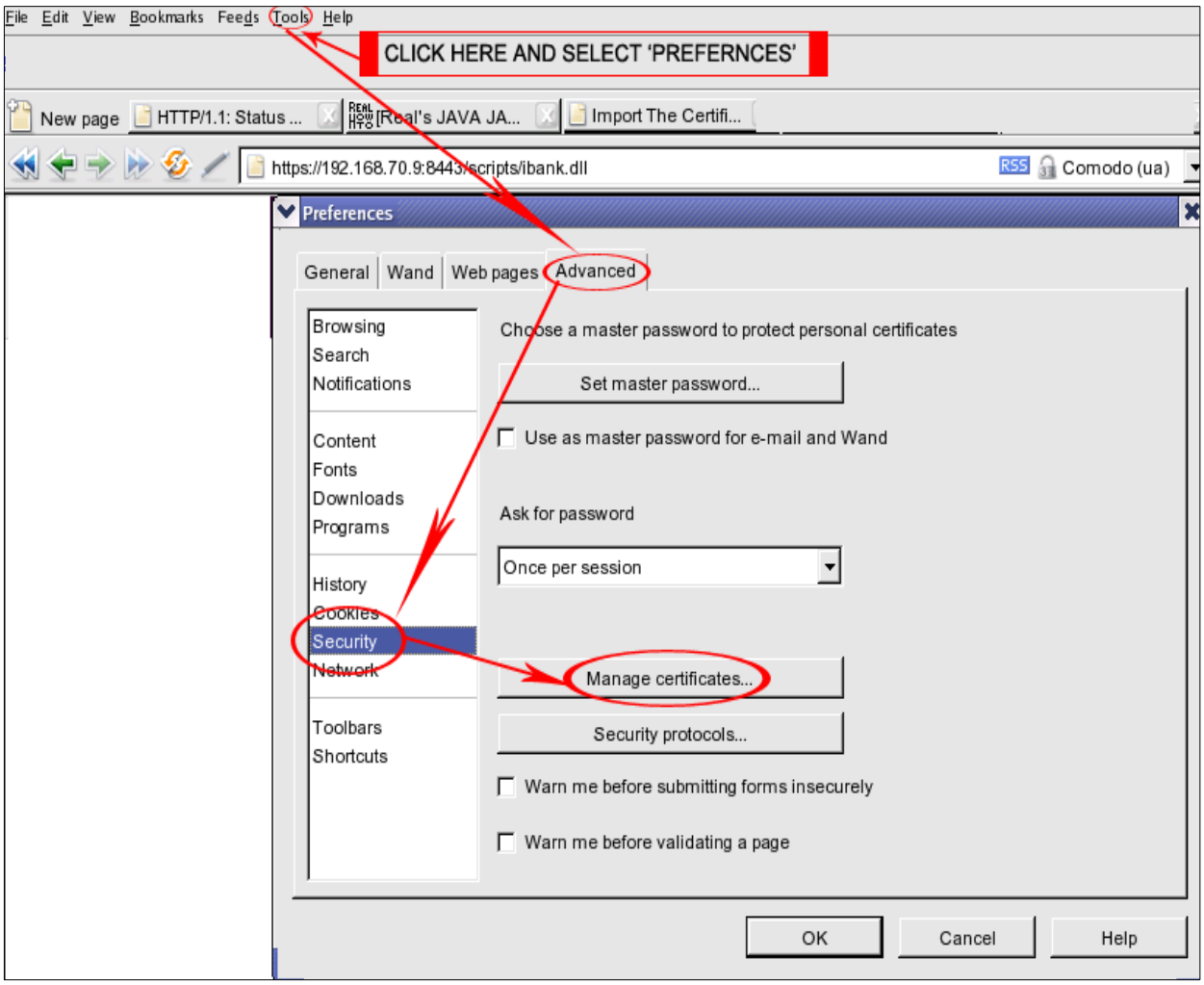
This security works in background mode and is 100% transparent you log straight in as you've always done without answering any extra security questions.

If you need to login from a different computer than the one you have added, you will be asked to answer one of the security questions that you set up earlier. Once inside your account, you'll then be prompted to install a digital certificate on that computer too.

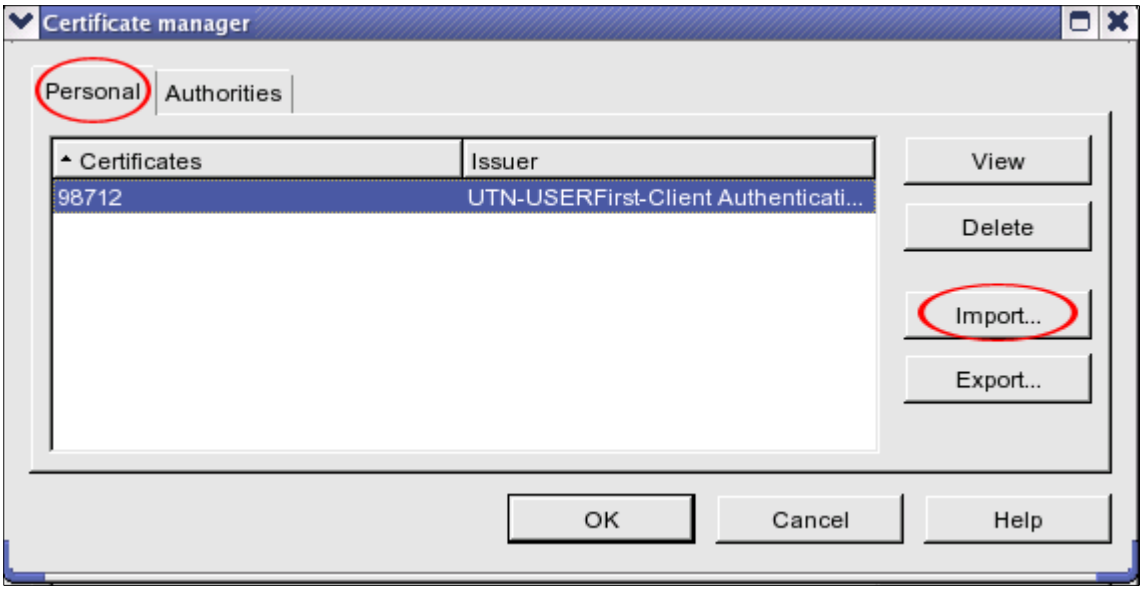
1.5. Installing Your Certificate on Opera

Unfortunately, Opera does not support automatic installation of certificates, so you first need to save the certificate to your hard drive before importing it into Opera. When asked, save the certificate file to your desktop.

7. Next comes the importing part of the installation. Whilst still in Opera select Tools / Preferences in the main menu.
8. In the pop-up window choose 'Advanced'.
9. In the drop-down list select 'Security'.
10. Click on 'Manage certificates' in the right section.



11. In the pop-up window select 'Personal'.



12. Click on 'Import' button,browse to your desktop and select the certificate file on your desktop.
13. Enter the password to access the certificate in 'Please enter the password protecting the key' field of 'Password' window.
14. Confirm the import by clicking 'OK'.

15. In the window that appears enter the password to access the certificate storage (if you've specified the password).
16. You have finished importing your new digital certificate into Opera.

Next time you log into your secure website e.g. anybank.com, Opera will ask you to specify your new digital certificate in the 'Select client certificate' window. Select the certificate which was created for you by our system.

That's it. The next time you log into your account, our servers will automatically detect this certificate on your computer - meaning we identify you as the true owner of your account by recognizing not only your User ID and Password, but your computer as well.

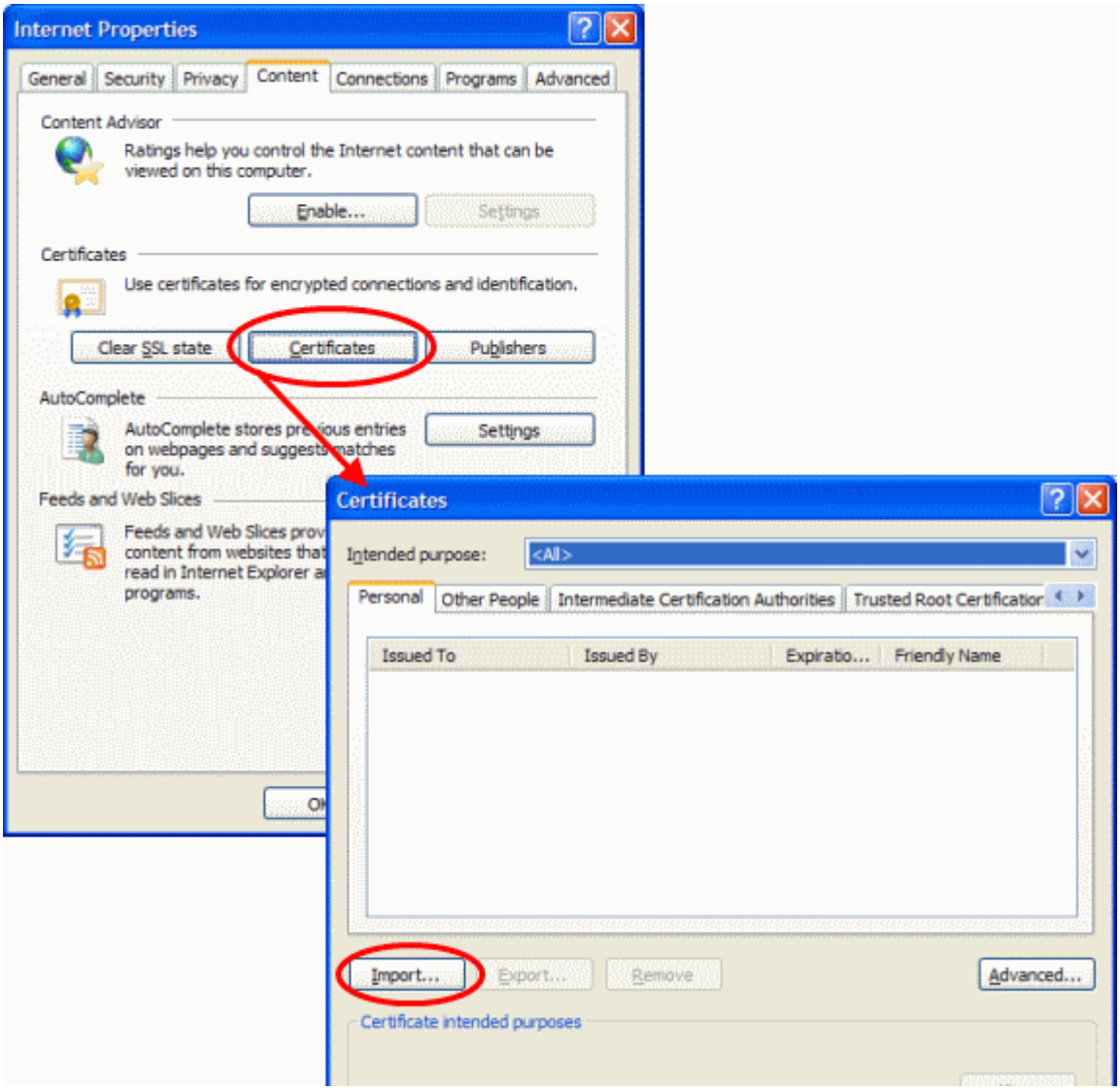
This security works in background mode and is 100% transparent you log straight in as you've always done without answering any extra security questions.

If you need to login from a different computer, you will be asked to answer one of the security questions that you set up earlier. Once inside your account, you'll then be prompted to install a digital certificate on that computer too.

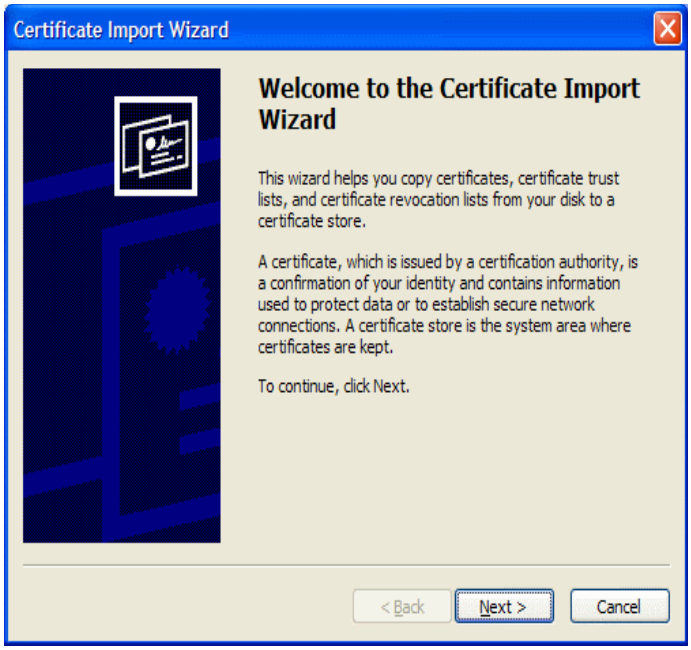
1.6. Installing Your Certificate on Safari

Unfortunately, Safari does not support automatic installation of certificates, so you first need to save the certificate to your hard drive before importing it into Safari. When asked, save the certificate file to your desktop. Also note down the password specified in the download page.

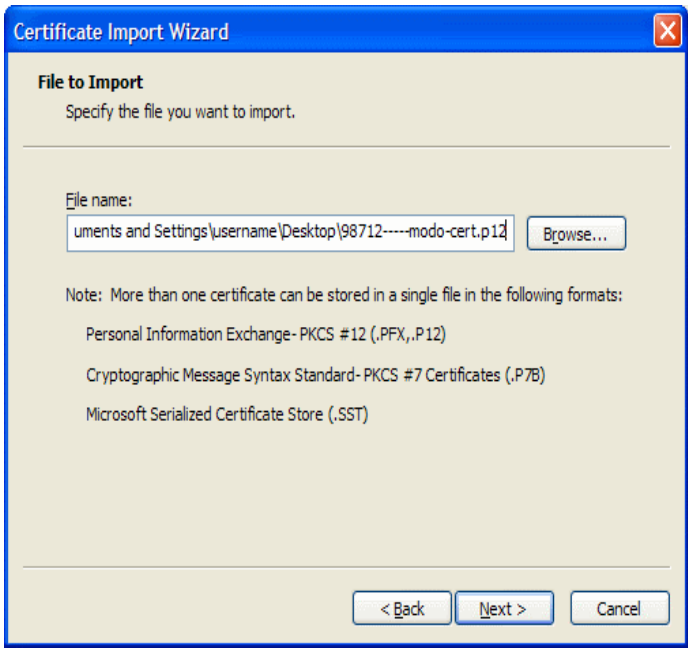
7. Next, open Control Panel from the Start Menu, click Internet Options > Content tab > Certificates > Import or simply double click on the certificate.



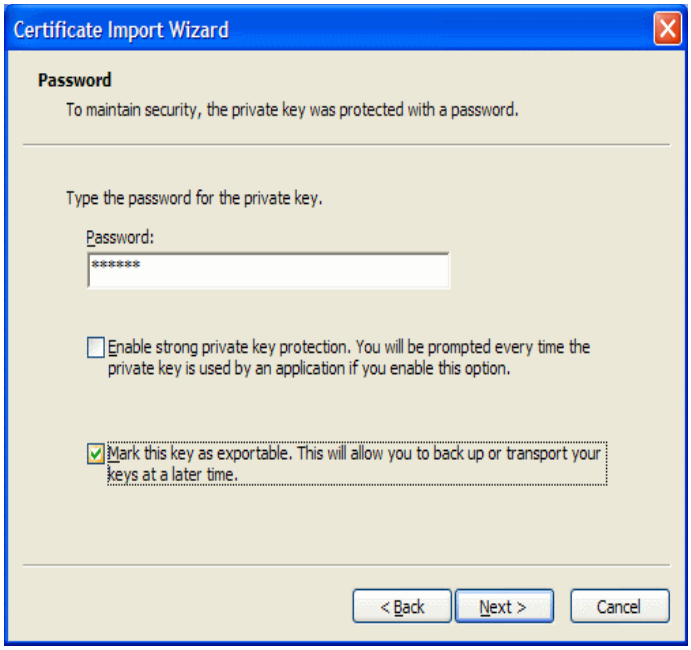
This will open the Certificate Import Wizard.



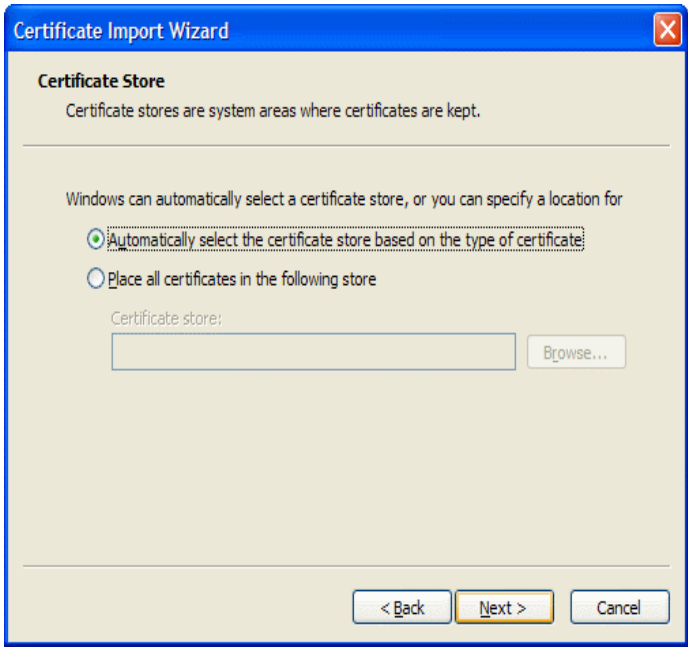
8. Click Next.



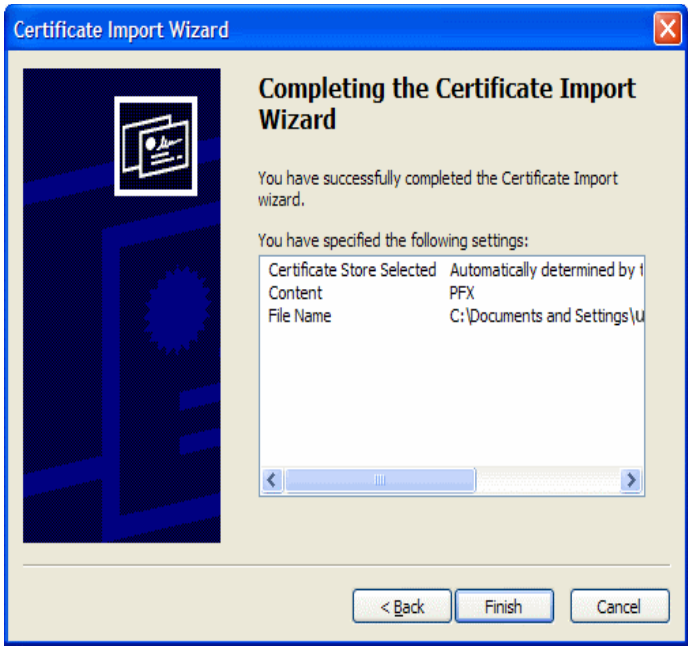
9. Click 'Browse' and navigate to your desktop and select the certificate file on your desktop and click 'Next'.



10. Enter the Password that was given in the download page and click 'Next'.



11. Select 'Automatically select the certificate store based on the type of the certificate' (default) and click 'Next'.



12. Click 'Finish'.

Import is completed and Import Success dialog will be displayed.

That's it!! The next time you log into your account, our servers will automatically detect this certificate on your computer -meaning we identify you as the true owner of your account by recognizing not only your Username and Password, but your computer as well.

This security works in background mode and is 100% transparent you log straight in as you've always done without answering any extra security questions.

If you need to login from a different computer than the one you have added, you will be asked to answer one of the security questions that you set up earlier. Once inside your account, you'll then be prompted to install a digital certificate on that computer too.

1.7. Installing Your Certificate on Google Chrome

Comodo Two Factor supports certificate installation on Google Chrome on the following operating systems:

- **Windows Operating Systems**
- **MacOS**

Note: Chrome on Linux is not yet supported for certificate installation. If you use Linux and need to set up authentication then you have two broad options:

(1) Install your certificate using a CTF supported browser such as Firefox, Opera, Safari or Internet Explorer. You must log into the secure website using this browser too.

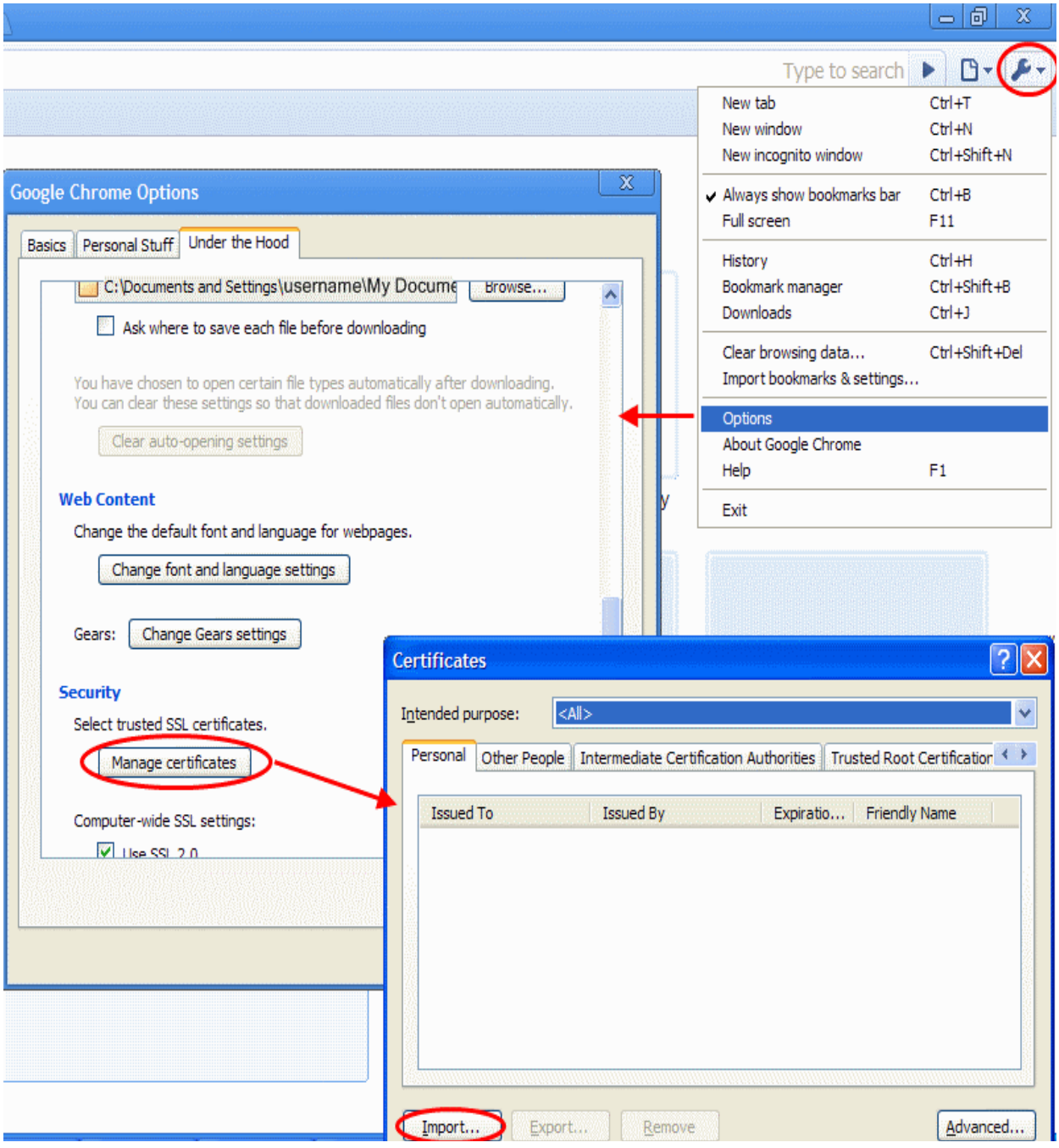
(2) Consider switching your method of authentication to secure cookies instead of certificates. CTF ***does*** support **secure cookie authentication** in Chrome on Linux (note -you may need to contact your system administrator to allow this switch).

For a complete list of browser compatibilities, see '**Table of Browsers compatibility for Client Certificate and Cookie Installation**'.

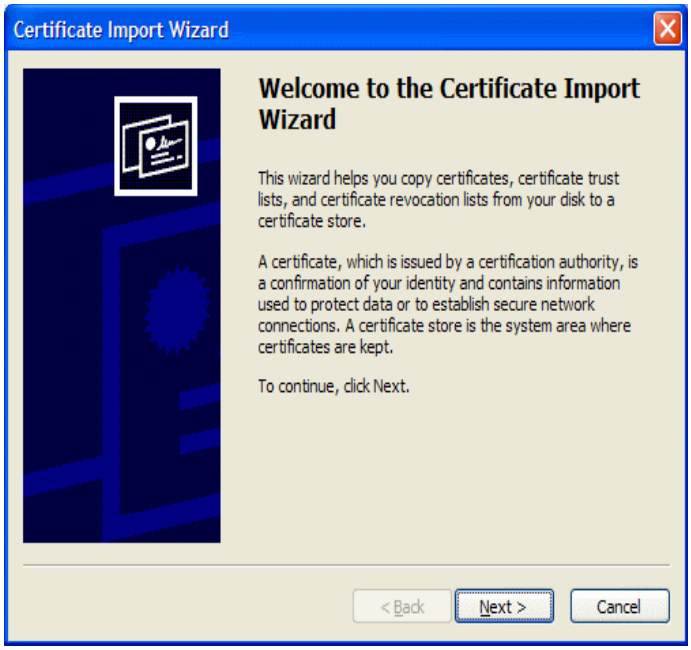
1.7.1. Installing Your Certificate on Google Chrome using Windows Operating System

Unfortunately, Chrome does not support automatic installation of certificates, so you first need to save the certificate to your hard drive before importing it into Chrome. When asked, save the certificate file to your desktop. Also note down the password specified in the download page.

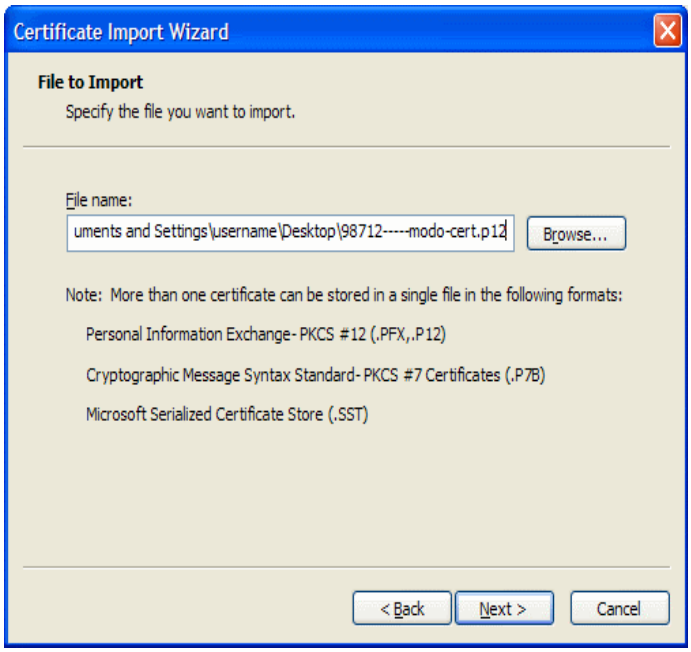
7. Next, Click on the Tools menu (Wrench icon) at the upper right corner of the Chrome browser. Click Options > Under the hood tab. Scroll down to 'Security', click Manage Certificates > Import or simply double click on the certificate.



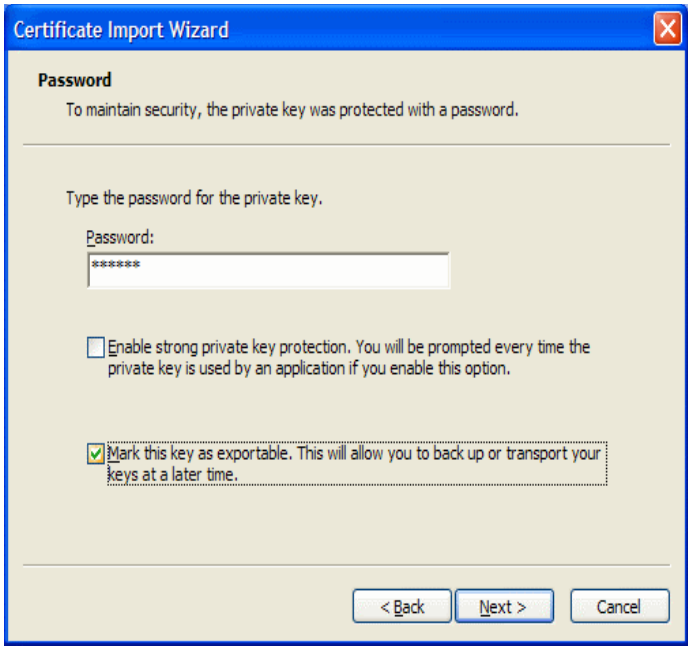
This will open the Certificate Import Wizard.



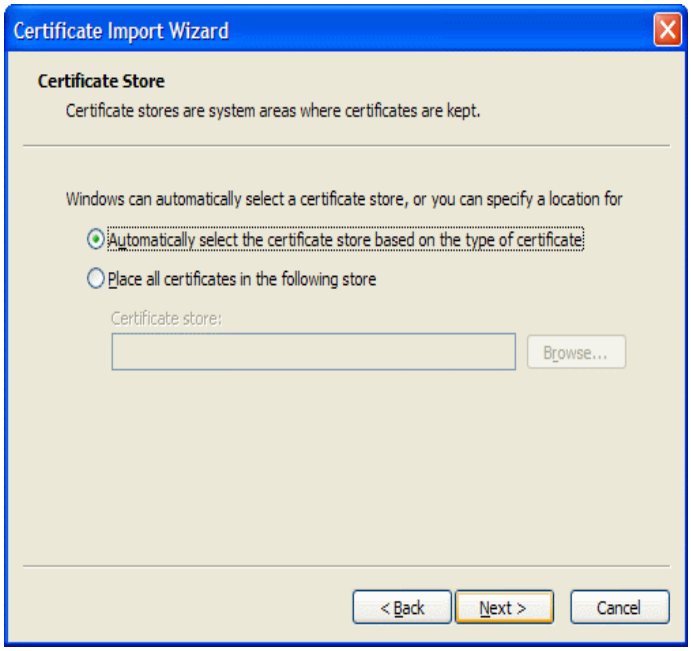
8. Click 'Next'.



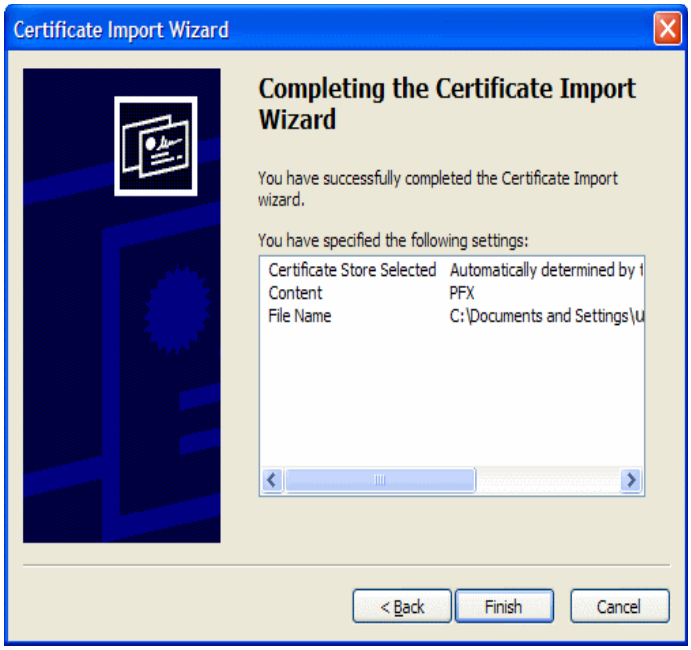
9. Click 'Browse' and navigate to your desktop and select the certificate file on your desktop and click Next.



10. Enter the Password that was given in the download page and click 'Next'.



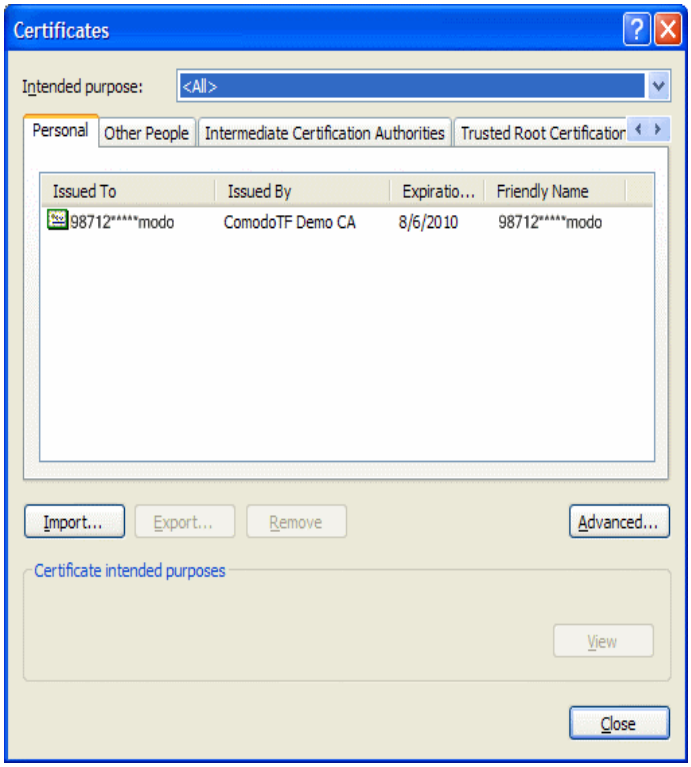
11. Select 'Automatically select the certificate store based on the type of the certificate' (default) and click 'Next'.



12. Click 'Finish'.

Import is completed and Import Success dialog will be displayed.

You can view the certificate under the personal tab of the certificate store. To view the certificate, click the Tools menu, select 'Options', click 'Under the hood' tab, scroll down to 'Security' and click 'Manage Certificates'.



That's it!! The next time you log into your account, our servers will automatically detect this certificate on your computer - meaning we identify you as the true owner of your account by recognizing not only your Username and Password, but your computer as well.

This security works in background mode and is 100% transparent you log straight in as you've always done without answering any extra security questions.

If you need to login from a different computer than the one you have added, you will be asked to answer one of the security questions that you set up earlier. Once inside your account, you'll then be prompted to install a digital certificate on that computer too.

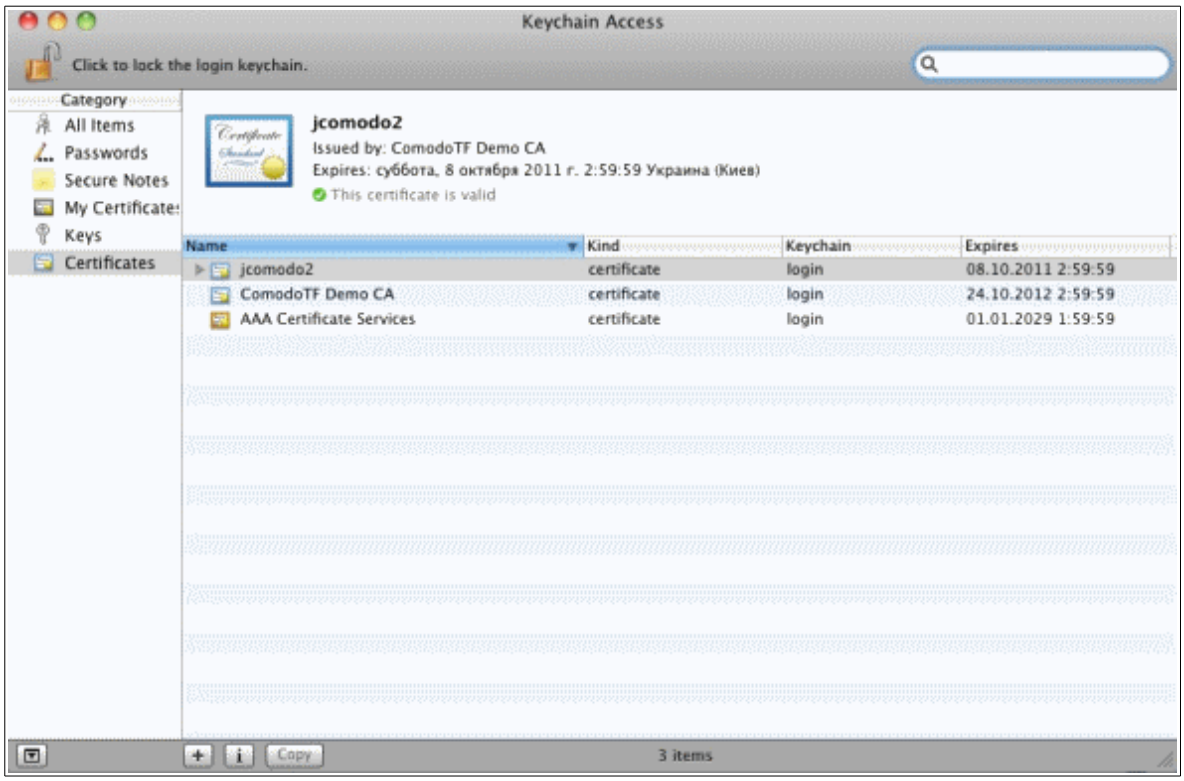
1.7.2. Installing Your Certificate on Google Chrome using MAC Operating System

Unfortunately, Chrome does not support automatic installation of certificates, so you first need to save the certificate to your hard drive before importing it into Chrome. When asked, save the certificate file to your desktop. Also note down the password specified in the download page.

7. Next, open Finder and select Applications located in PLACES. Select Utilities > Keychain Access and select File > Import Items. Select the .p12 file you previously downloaded or simply double click on the .p12 file.
8. Enter password when prompted and click 'OK'.

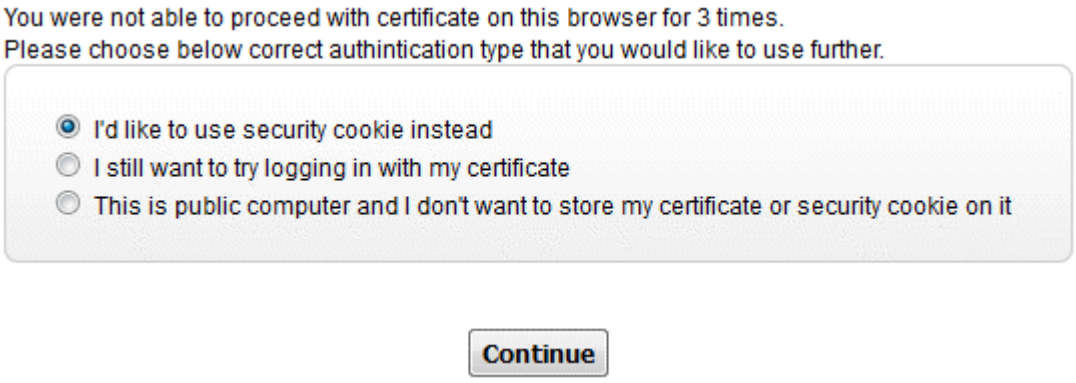
9. Next, enter the password for keychain and click 'OK'.

The Certificate will appear in the certificate list.



1.8. TroubleShooter

If you aren't able to proceed with a certificate installation for three times you will be prompted to choose one of your contact phone numbers or email address the next time you log in. But if the problems won't be eliminated, you will be prompted to use a several modes:



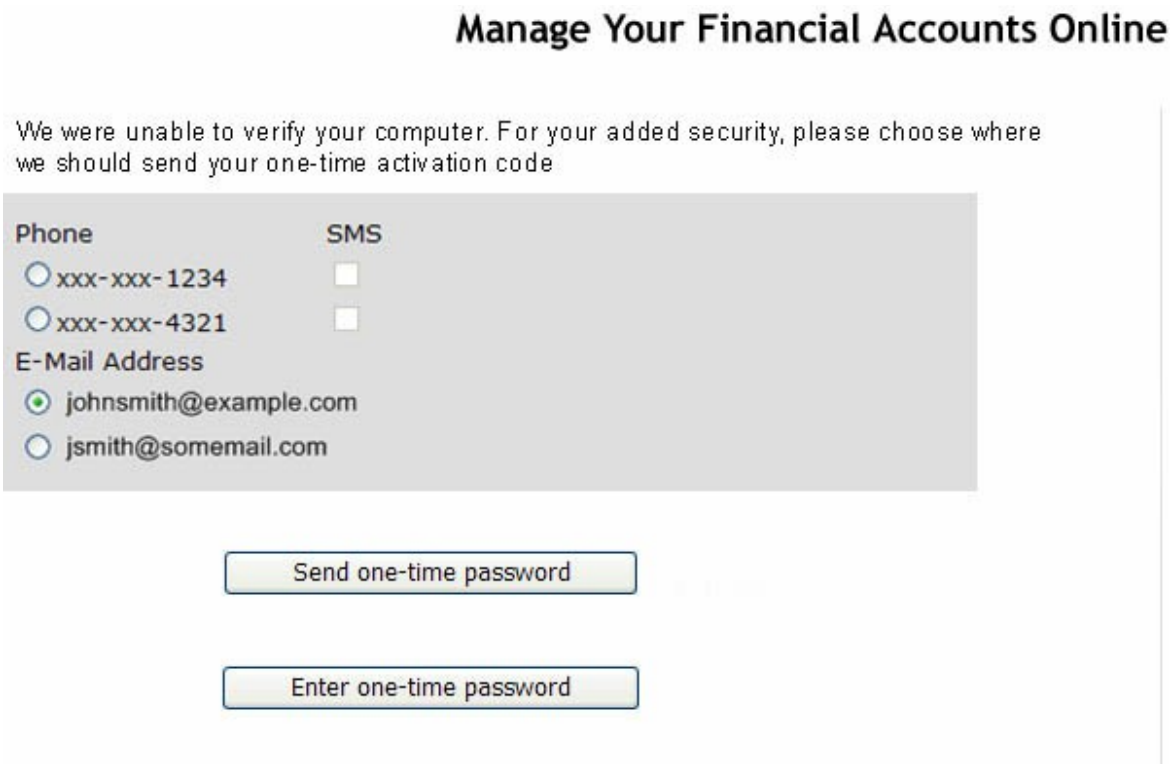
- **I'd like to user security cookie instead** - Switches this browser to COOKIE mode. Show Questions/Callback with security cookie install prompt.
- **I still want to try logging in with my certificate** - Always try to check for a certificate. This is useful for some temporary problems and when a user has two equal computers (the same versions of OS and browser). One private computer where it is safe to install certificate on and other - public where a user doesn't want to install a certificate. Show Questions/Callback with certificate install prompt in this case.
- **This is public computer and I don't want to store my certificate or security cookie on it** - Switches this browser to Question/Callback mode. Do not try to check certificate anymore on this browser. Show Questions/Callback with certificate install prompt.

2. Accessing Your Account From A Different Computer

If you have entered your regular username and password BUT our systems did not detect a security certificate or cookie on your computer then we will be unable to fully verify you as the account holder. This situation typically occurs if you are attempting to access your account from a computer other than the one you usually use.

This means you will not be able to access your account until you have entered an activation code. This activation code will be sent to the contact phone number or email address of your choice. You should have specified these contact phone numbers and email addresses when first setting up the additional security (see section **1.1. Overview**).

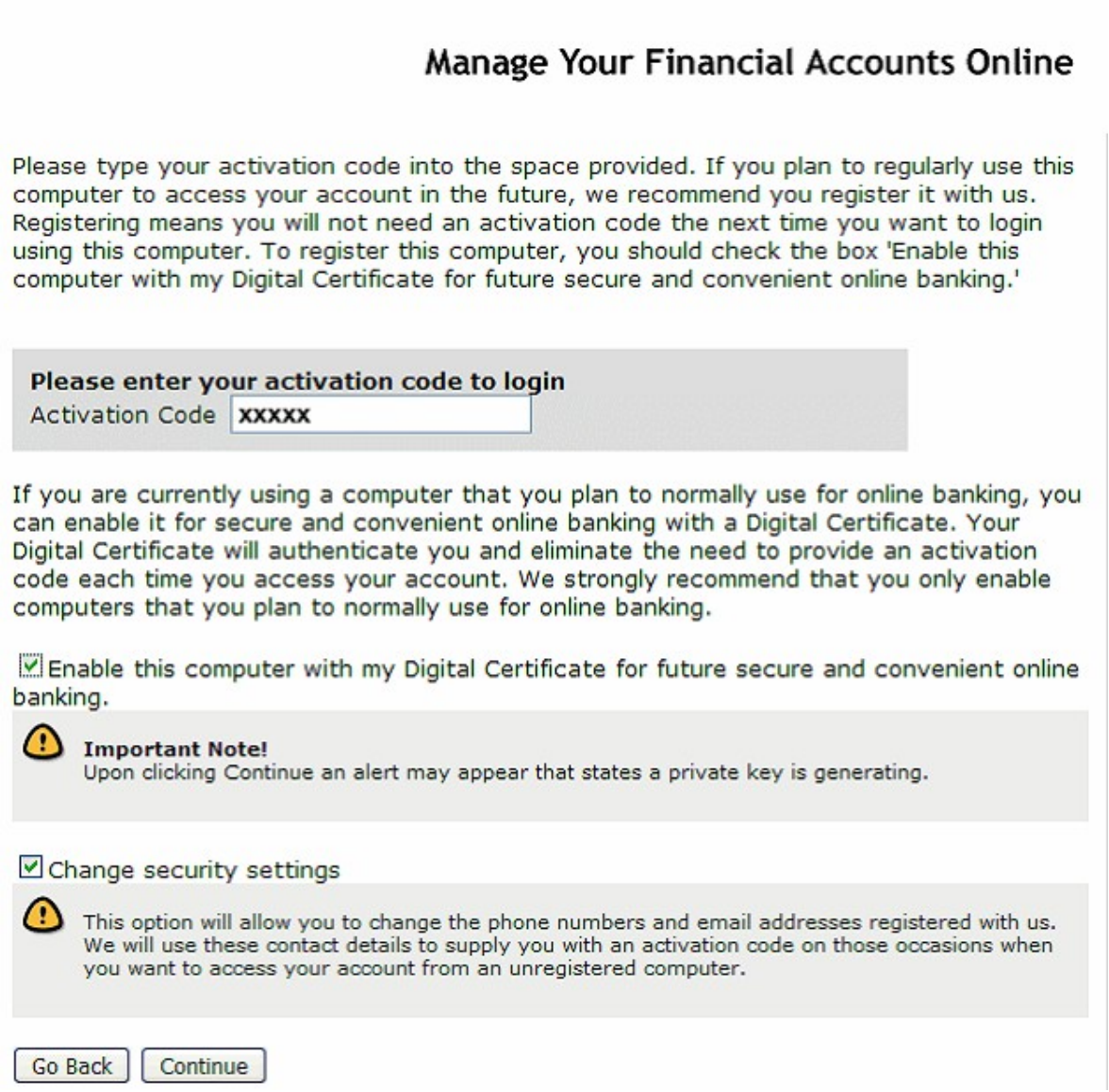
After entering your regular username and password, you will be presented with a screen similar to the following:



- If you wish to receive a phone message, simply select the radio button next to the phone number of your choice.
- If you wish to receive it via text message then check the 'SMS' box.
- If you wish to receive an email with the activation code then choose an email address instead.

Click 'Send one-time password' once you are satisfied with your choice.

After receiving the one-time code, click 'Enter one-time password' to be taken to the following screen:



- If you have received your activation code, please enter it in the field provided and click 'Continue' to log into your account. If you wish to have the code re-sent or sent to a different address then click 'Go Back' and reselect your contact address
- If you plan to regularly access your account for this computer then leave 'Enable this computer for secure and convenient banking' enabled. This will install a cookie or security certificate on the machine you are using.

Note: This is not advised if you are accessing from a public computer.

- If, having successfully answered the security question, you wish to modify your security questions and/or contact email addresses then leave 'Change Security Settings' box enabled (See **'2.1 Modifying Your Security Settings'**)

Note: If you are unable to receive the one-time password you should contact the *support department of the service that you are trying to log into* (for example, your bank). After verifying you as the account holder, the support administrator will be able to manually reset contact email address(es).

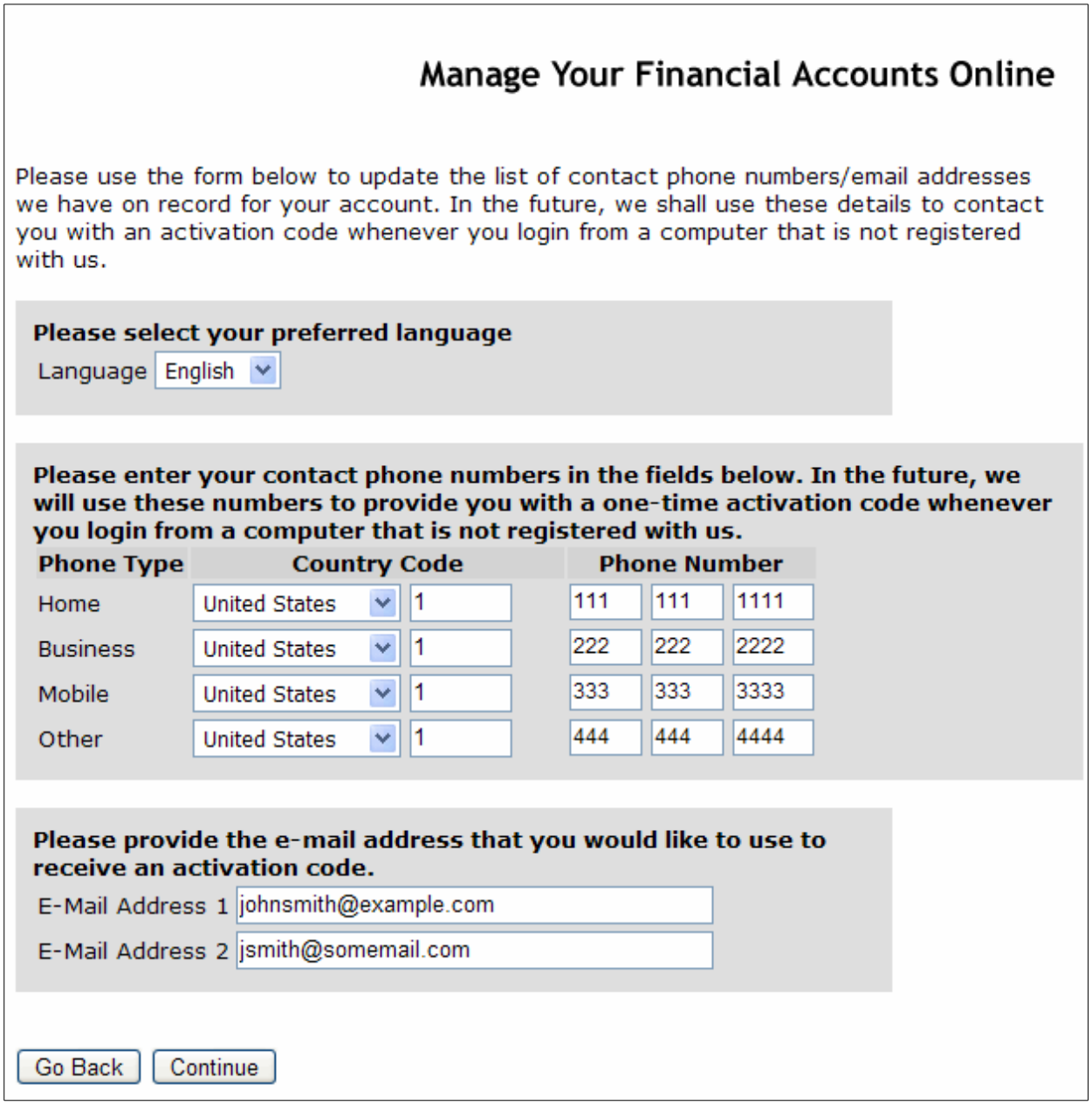
2.1. Modifying Your Security Settings

If you left 'Change Security Settings' enabled then you will be taken to a page that allows you to:

- Set the contact phone numbers and addresses that are on record for your account.

  These are the numbers and addresses to which the activation codes will be sent should this be required (for example, if our security systems cannot fully verify you as the account holder because you are attempting to access your account from a different computer). After successfully receiving and entering the one-time password you will be able to access your account. (see **'2. Accessing Your Account From A Different Computer'** for more details).

- Change language settings for this interface.



- Specify or modify the phone numbers (+ country and dialing code) and email addresses by typing in the fields provided. The next time you want to log in from a computer that does not have a security cookie/certificate, you will be presented with these numbers/addresses and asked to select the one to which we should send your activation code.
- Modify the drop down box to change the language in which this interface is displayed.
- Click 'Continue' to apply your changes and return to your main account.

3.How to Enable Cookies

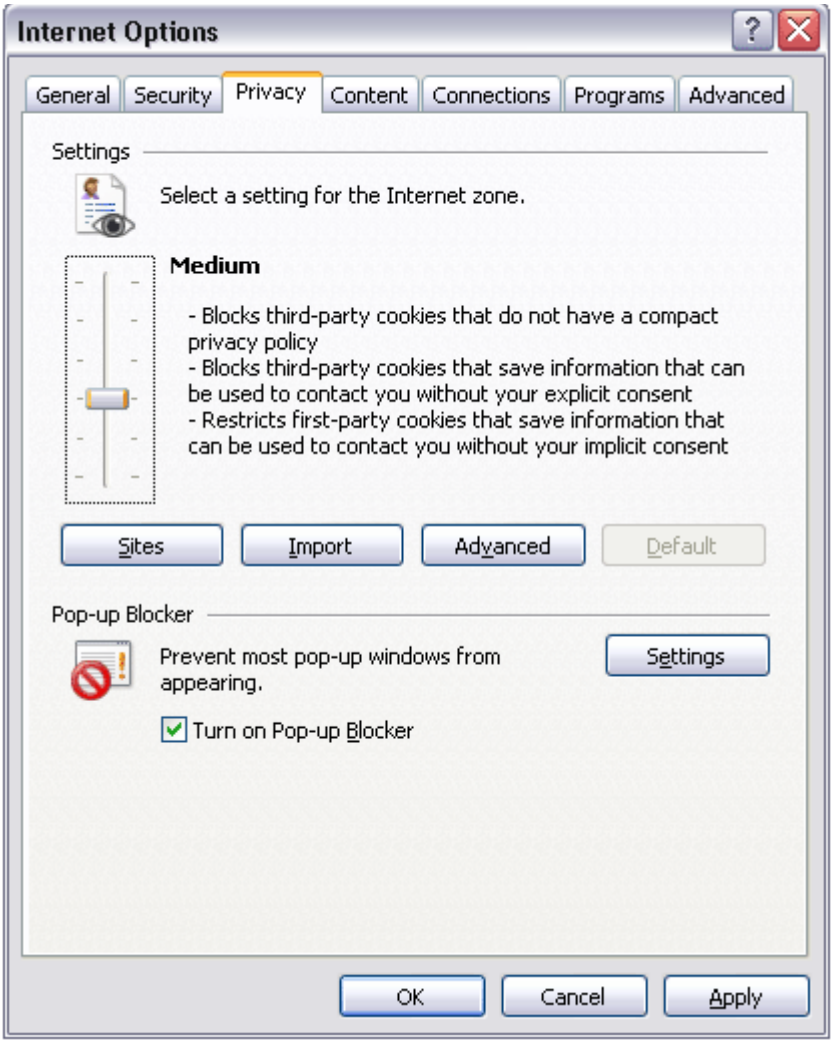
Comodo TF 'secure cookie mode' requires cookies to be enabled in your browser. In order to view step-by-step tutorial on enabling cookie, select your type of browser from the list below:

- **Enable Cookies on Internet Explorer**
- **Enable Cookies on FireFox**
- **Enable Cookies on Opera**
- **Enable Cookies on Safari**
- **Enable Cookies on Google Chrome**

3.1.Enable Cookies on Internet Explorer

To enable cookies in Internet Explorer, follow these steps:

1. From the main toolbar, select 'Tools -Internet Options - Privacy':



You need adjust the slider to the Medium- High or Lower level.

2. If you adjust the slider to the High level or higher, you need to configure Advanced Privacy Settings.
    - check the box against Override automatic cookie handling;
    - check the box against Always allow session cookies;

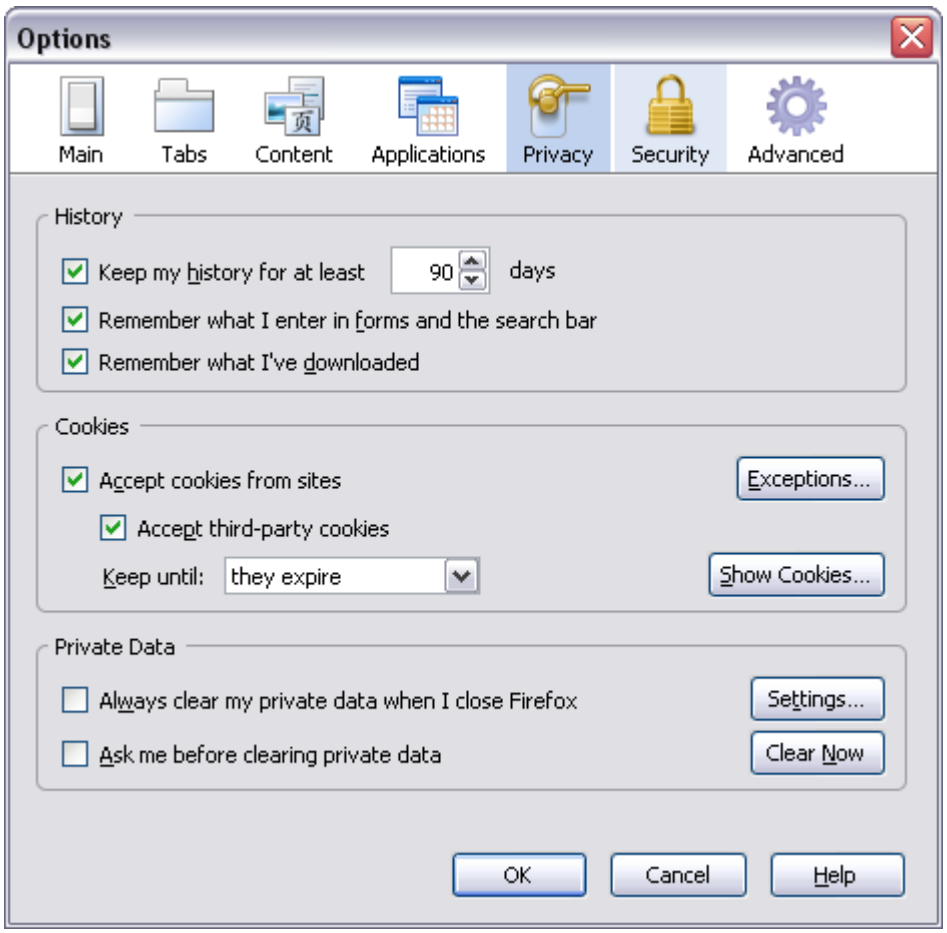
- click 'OK' to preserve changes.

But in this case you will not be able to use Cookie Authentication Mode.

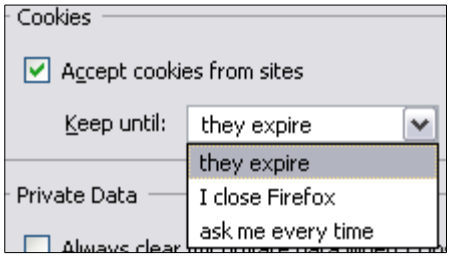
3.2. Enable Cookies on FireFox

To enable cookies in Firefox, follow these steps:

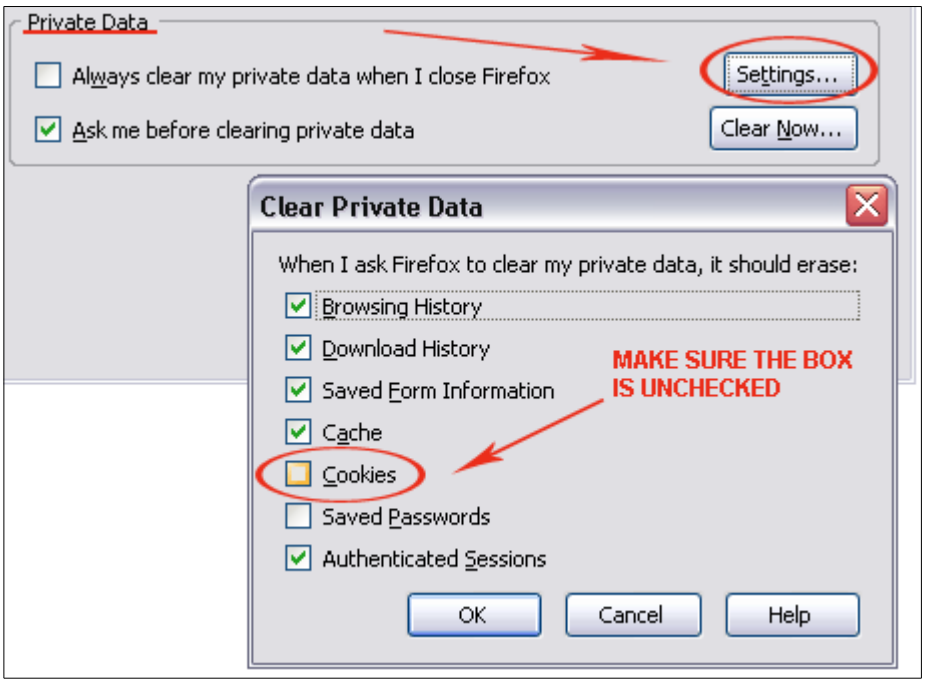
1. From the main toolbar, select 'Tools - Options - Privacy:'



2. Check the box next to 'Accept cookies from sites'. Choose 'Keep until they expire (see below)'



3. To prevent Firefox from deleting cookies during an automatic 'Clear Private Data…' operation:
   i. Click the 'Settings' button in the 'Private Data' section.
   ii. Make sure the 'Cookies' checkbox is not selected.



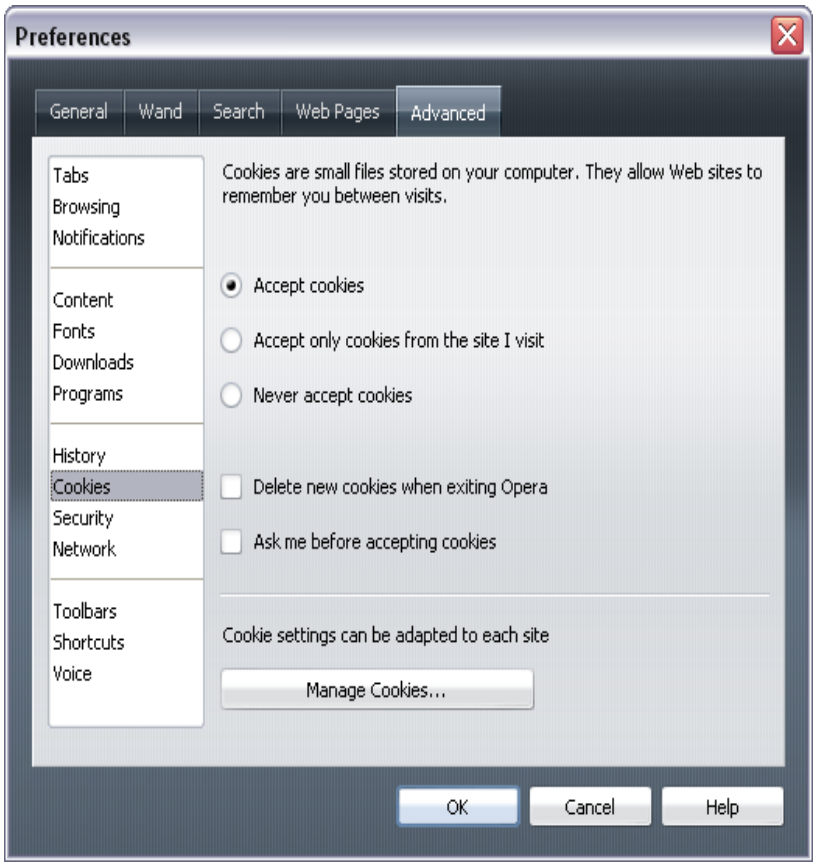
Note: This although prevents only from automatic clear, not manual.

4. Click 'OK' to confirm and save your changes.

3.3. Enable Cookies on Opera

By default, cookies are enabled in Opera. To check this setting and enable them if necessary, follow these steps:

1. From the main toolbar, select 'Tools - Preferences - Advanced - Cookies:'

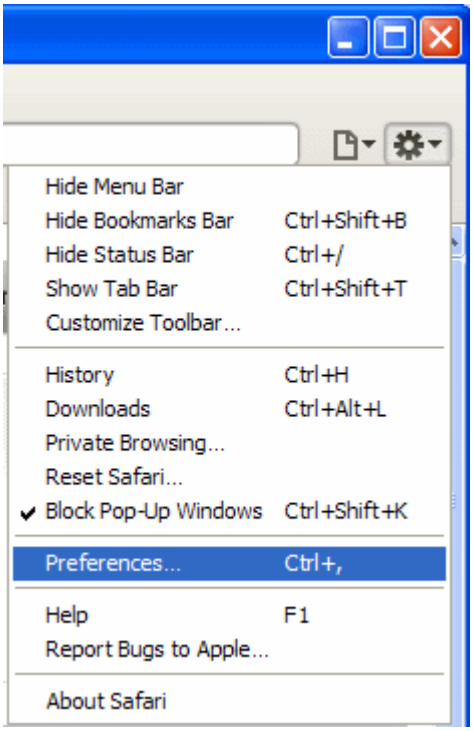


2. Select 'Accept Cookies'.
3. Click 'OK' to confirm and save your changes.

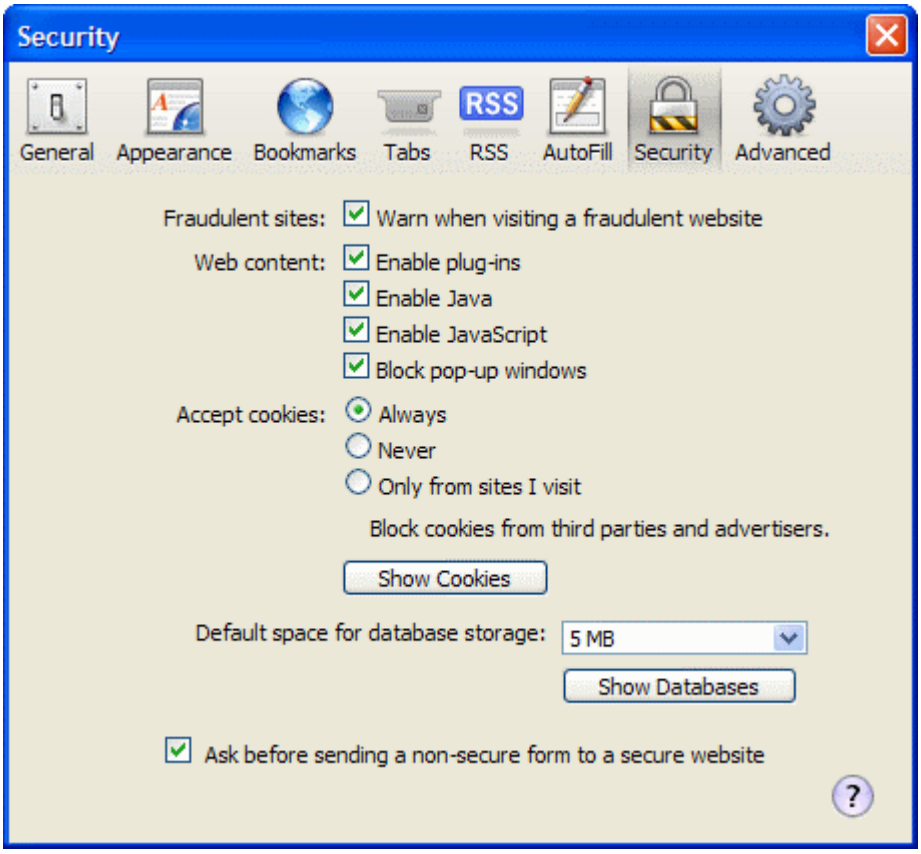
3.4. Enable Cookies on Safari

By default, cookies are enabled on Safari. To check this setting and enable them if necessary, follow these steps:

1. Click the 'Tools' button (the gear icon) at the top right corner of the Safari interface



2. Select 'Preferences' from the drop down list.
3. Select the 'Security' tab then select 'Accept cookies - always'.



4. Close the dialog to confirm and save your changes.

3.5. Enable Cookies on Google Chrome

Comodo Two Factor supports the use of cookies in Google Chrome on the following operating systems:

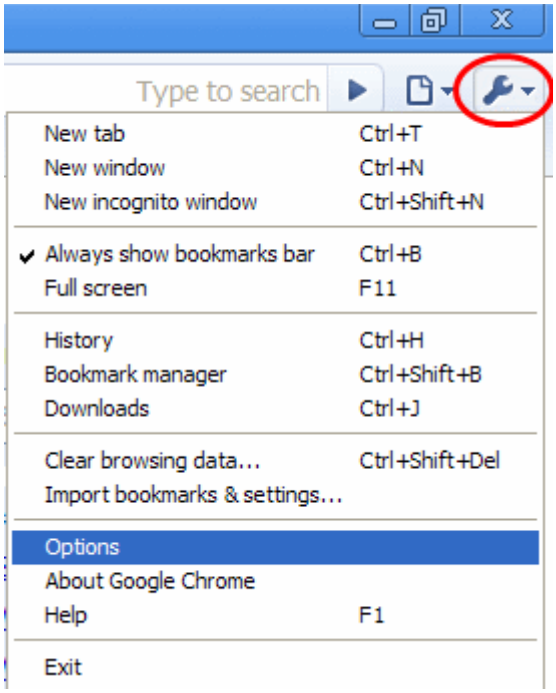
- Windows Operating Systems
- MacOS
- Linux

For a complete list of browser compatibilities, see '**Appendix 1 - Table of Browsers compatibility for Client Certificate and Cookie Installation**'

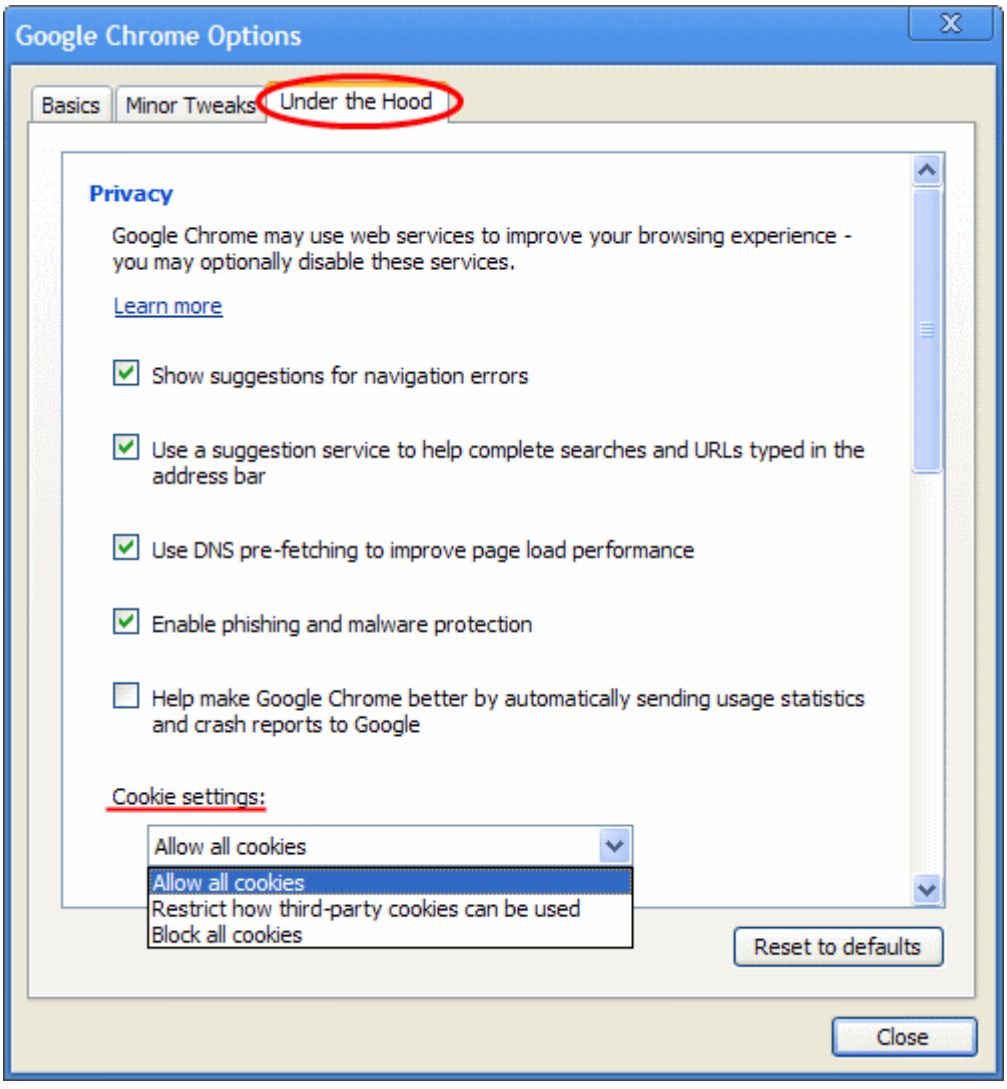
3.5.1. Enable Cookies on Google Chrome using Windows Operating System

By default, cookies are enabled in Google Chrome. To check this setting and enable them if necessary, follow these steps:

1. Click Tools button (the wrench icon) at the top right corner of the Chrome interface:



2. Select 'Options' from the drop-down list.
3. Select the 'Under the Hood' tab and select the 'Allow all cookies' option in the 'Cookie settings:' drop-down menu.



4. Click 'Close' to confirm and save your changes.

3.5.2. Enable Cookies on Google Chrome using MAC Operating System

By default, cookies are enabled in Google Chrome. To check this setting and enable them if necessary, follow these steps:

1. In the browser toolbar, click the wrench icon.

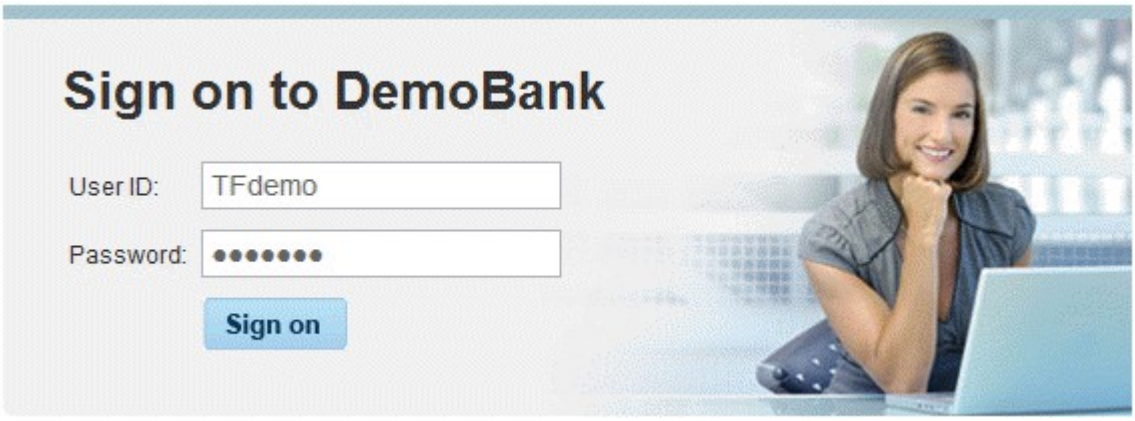
Note: If the wrench icon is not visible, click **Chrome** in the menu bar at the top of your screen.

2. Select 'Preferences' from the drop-down list.
3. Select the 'Under the Hood' tab and in the Privacy section click 'Content settings'.
4. In 'Allow cookies', select 'Allow local data to be set' to allow both the first party and third party cookies. Select the 'Block all third party cookies without exception' checkbox, if you want to allow only first party cookies and click OK.

4.How To Renew Your Digital Certificate

This tutorial shows you how to renew your digital certificate.

1. Start by logging in to your secure website e.g. anybank.com as usual with your Username and Password.



2. Next, you will be prompted to renew your digital certificate, in case your certificate expires soon:

3. Click on 'Renew Now' button. New digital certificate will be downloaded and installed into your browser. Some browsers don't provide automatic installation of the certificate, so you have to install it manually. For more info refer to sections '**Installing your certificate on Opera**', '**Installing your certificate on Google Chrome**', '**Installing your certificate on Safari**'.
4. The final stage of the procedure is to remove your OLD digital certificate from your browser.

   This procedure varies depending on which browser you are running:

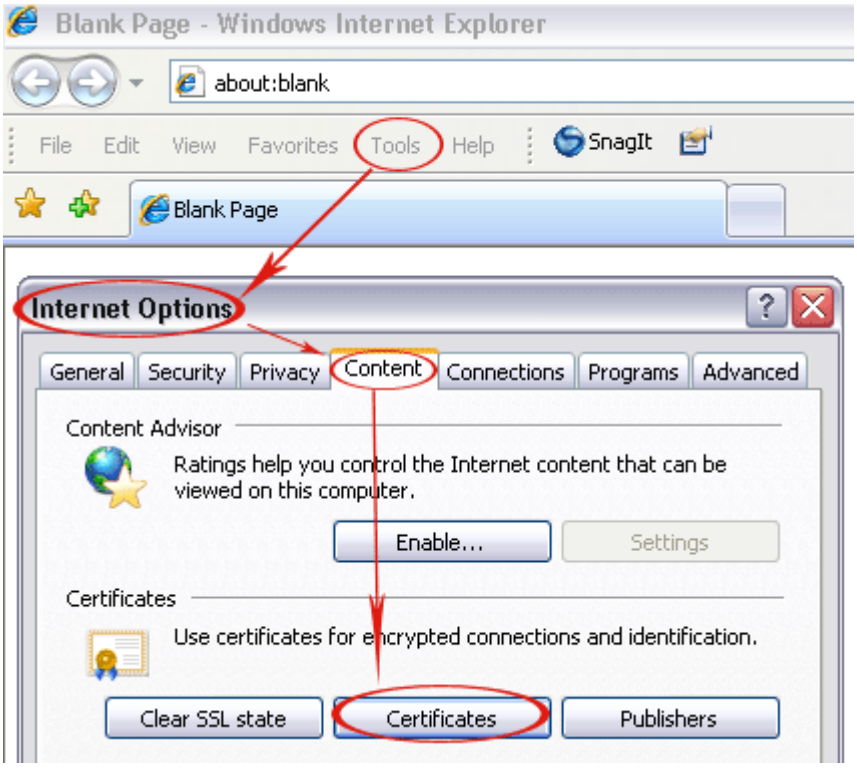
- **Click here if you are running Internet Explorer**

- **Click here if you are running Firefox**
- **Click here if you are running Opera**
- **Click here if you are running Safari**
- **Click here if you are running Google Chrome**

4.1. Removing your OLD digital certificate from Internet Explorer

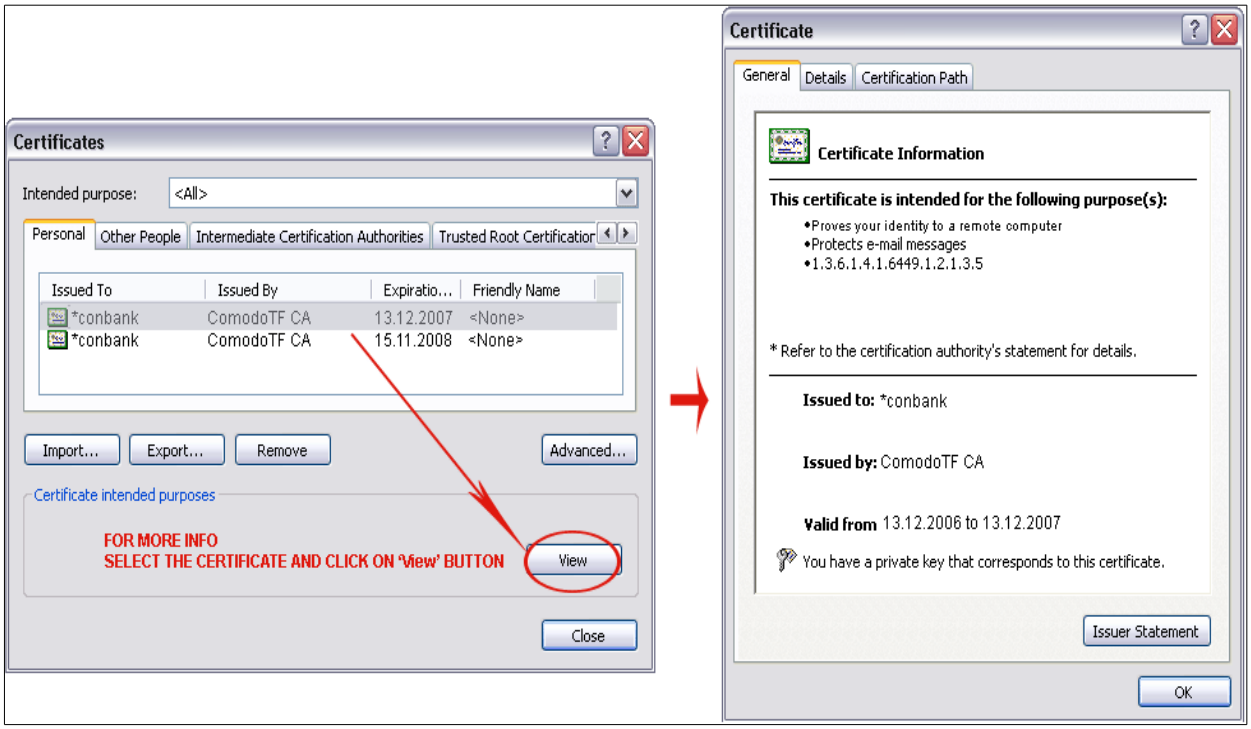
To remove your old digital certificate, click:

Tools - > Internet Options - > Content. Click on 'Certificates' button.

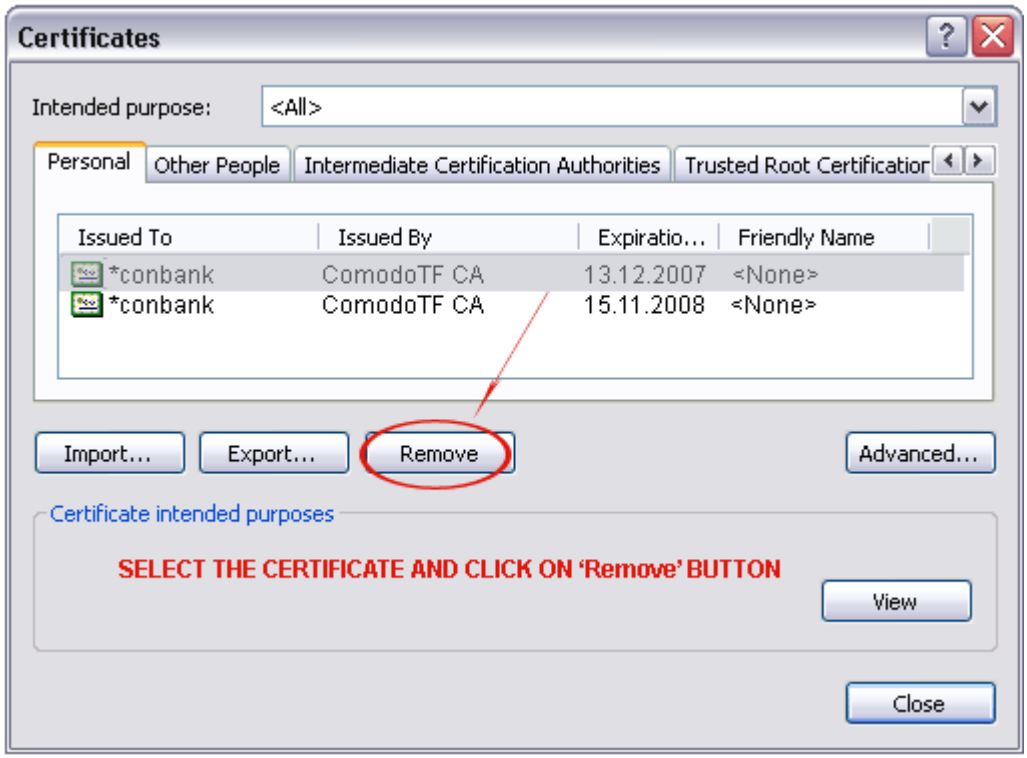


5. In certificate dialog box select your old certificate. Make sure that this is the certificate you wish to remove.

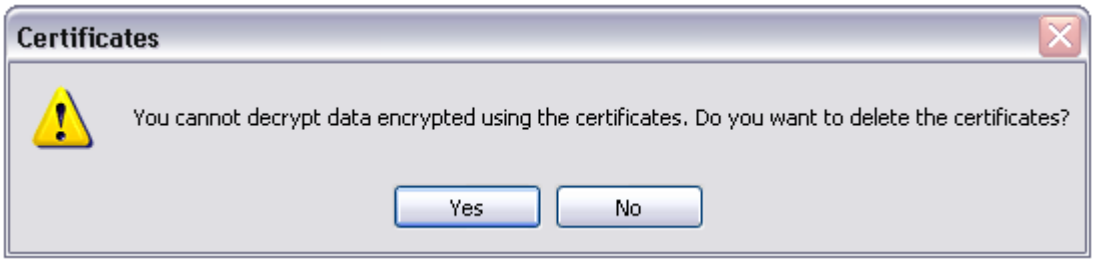
Note: To get more information about selected certificate, click on 'View' button as shown below.



6. Next, if this certificate is your OLD certificate, click the 'Remove' button:



7. Internet Explorer will then ask you for confirmation to remove the certificate:

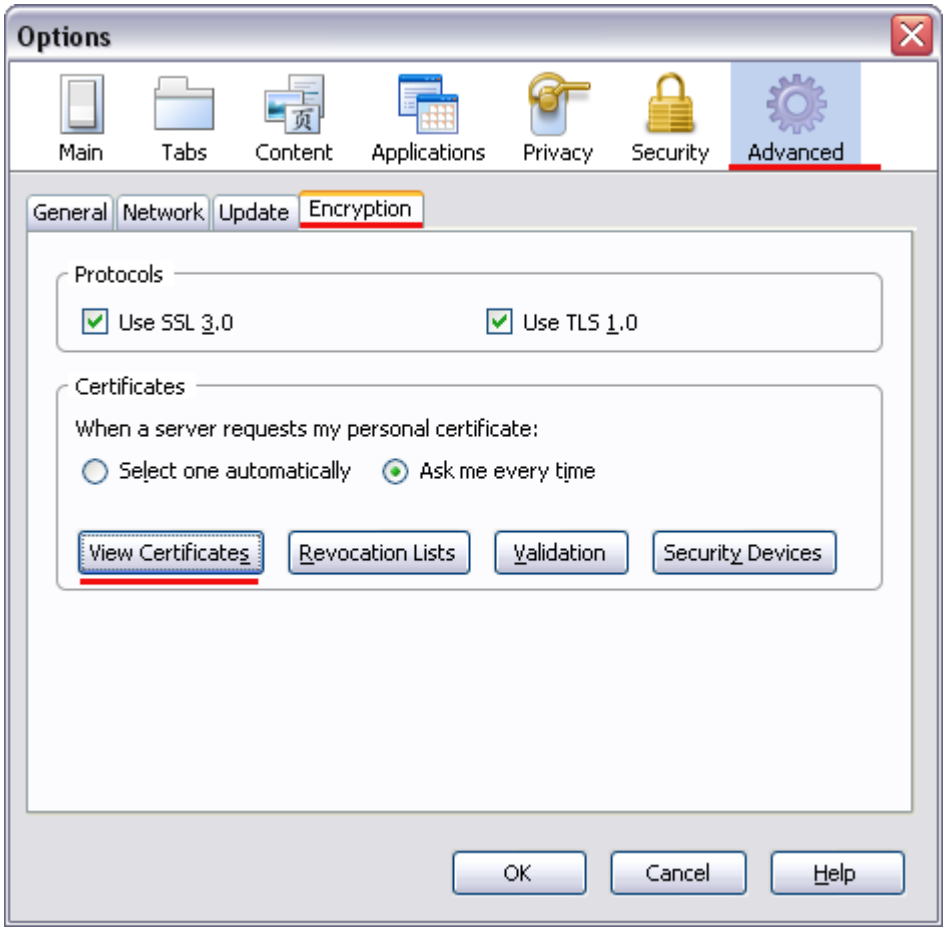


8. Click 'Yes' to confirm deletion.

4.2. Removing your OLD digital certificate from Firefox

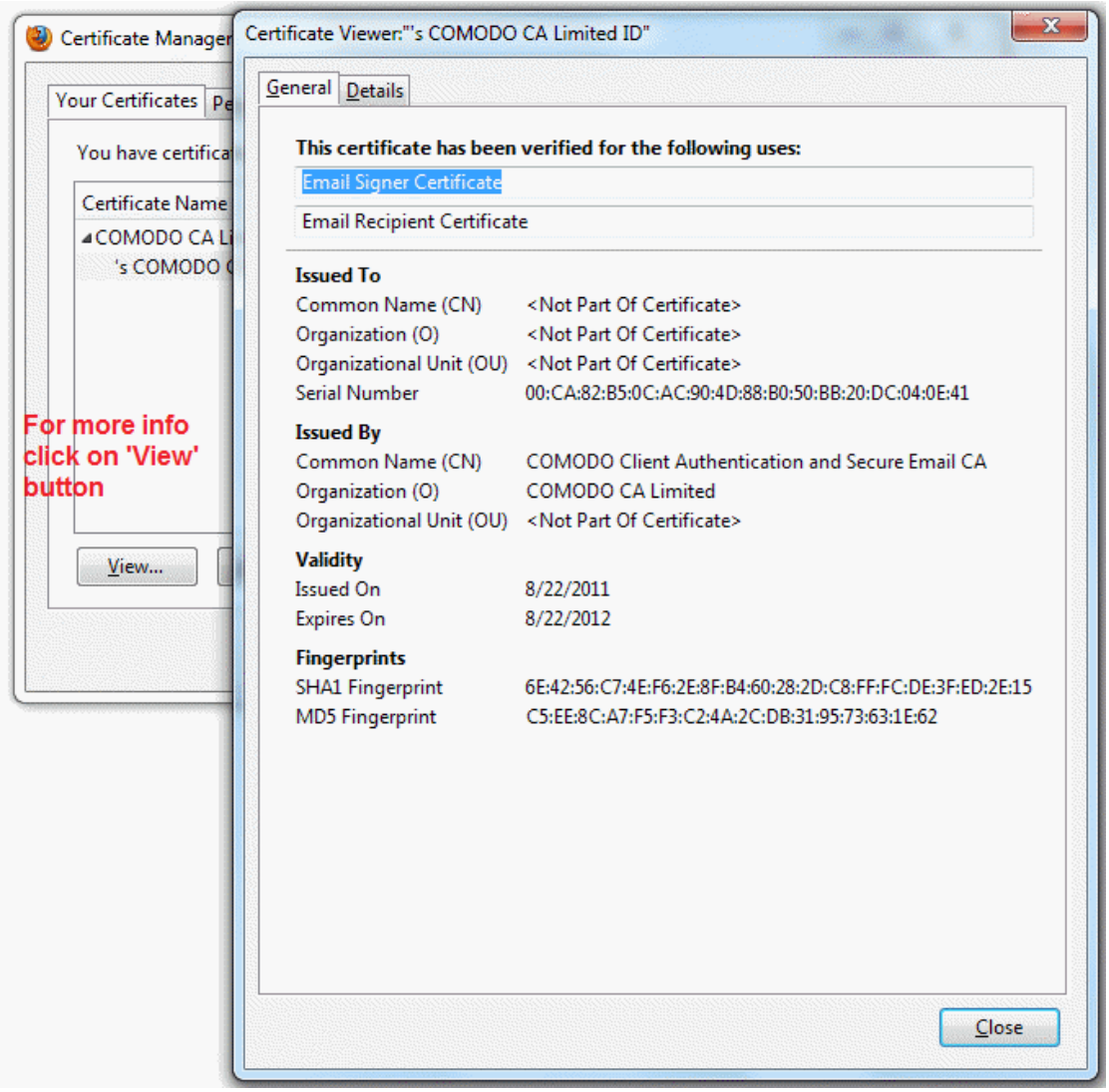
To remove your old digital certificate, click:

Tools - > Options - > Advanced - > Encryption. Click on 'View Certificates' button.

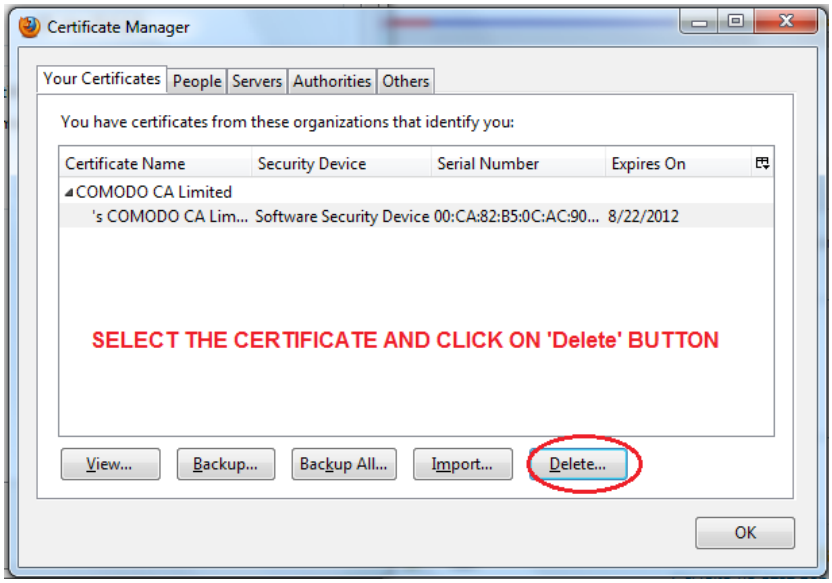


5. In the certificate dialog box select your old certificate. Make sure that this is the certificate you wish to remove.

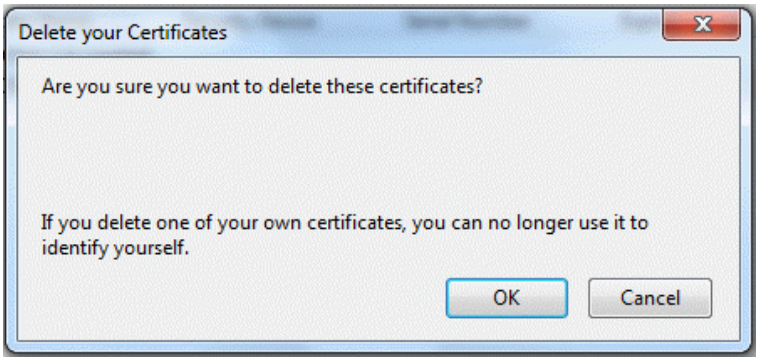
Note: To get more information about selected certificate, click on 'View' button as shown below.



6. Next, if this certificate is your OLD certificate, click the 'Delete' button:



7. Firefox will then ask you for confirmation to delete the certificate:

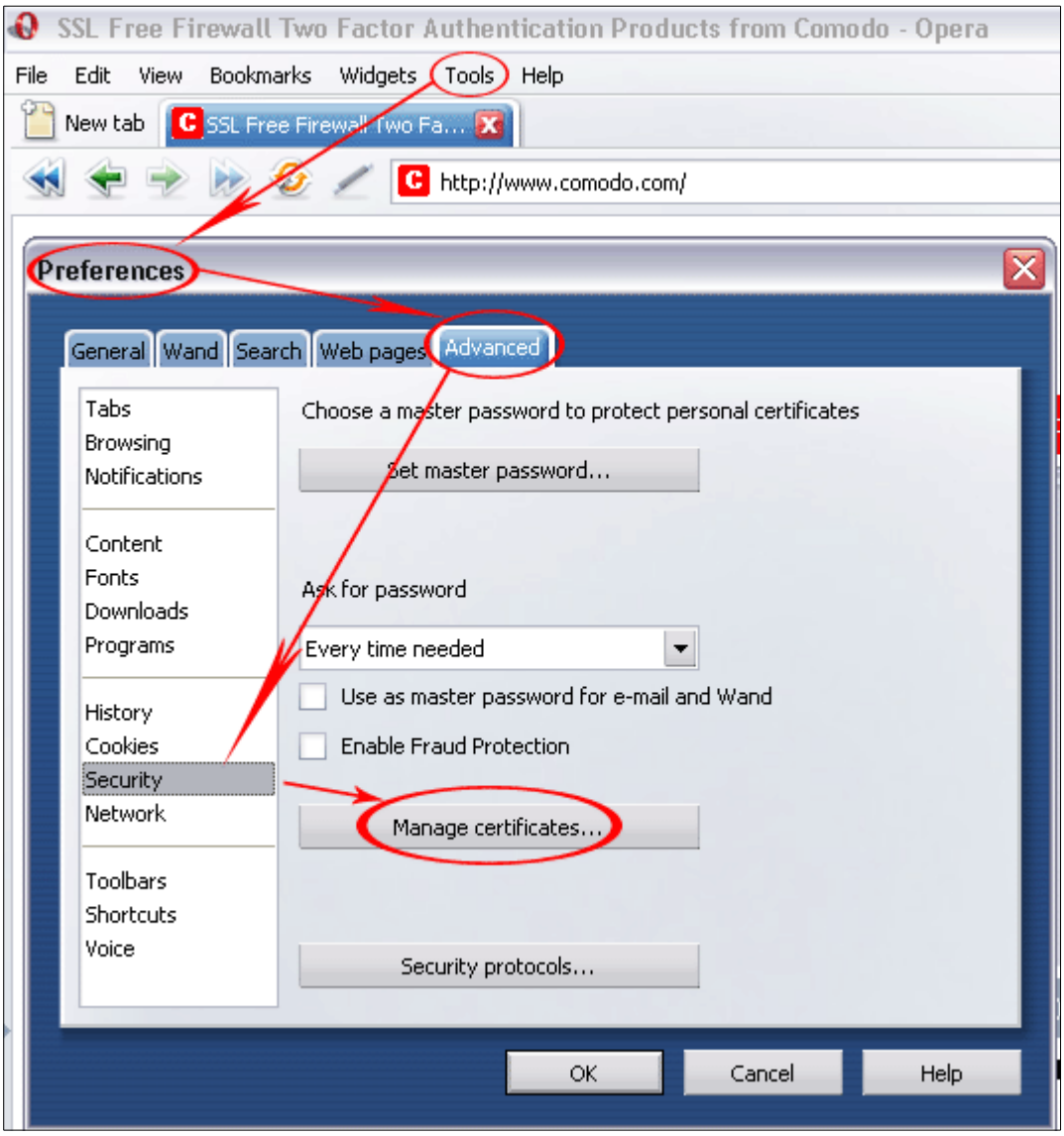


8. Click 'OK' to confirm deletion.

4.3. Removing your OLD digital certificate from Opera

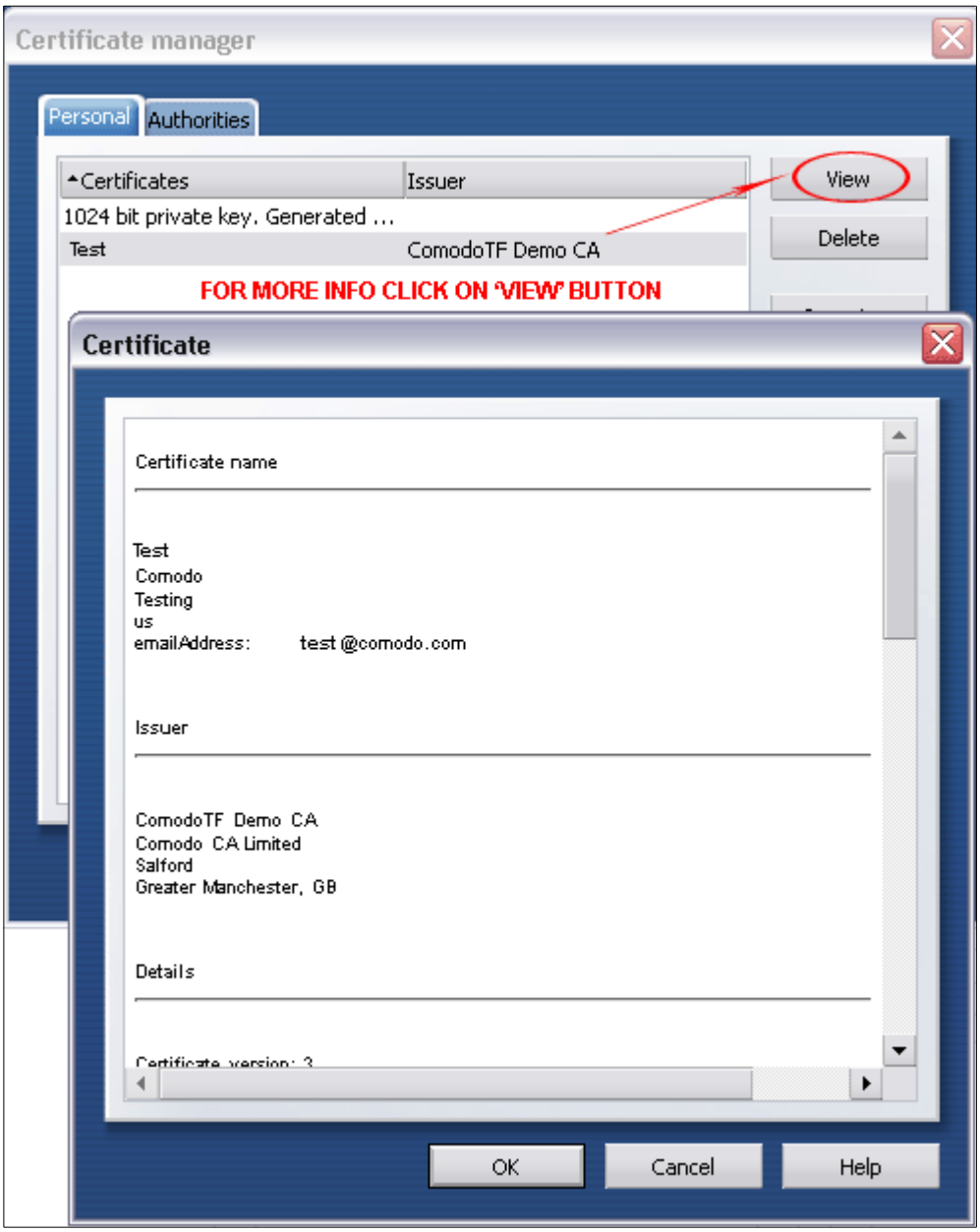
To remove your old digital certificate, click:

Tools - > Preferences - > Advanced - > Security. Click the 'Manage Certificates' button.

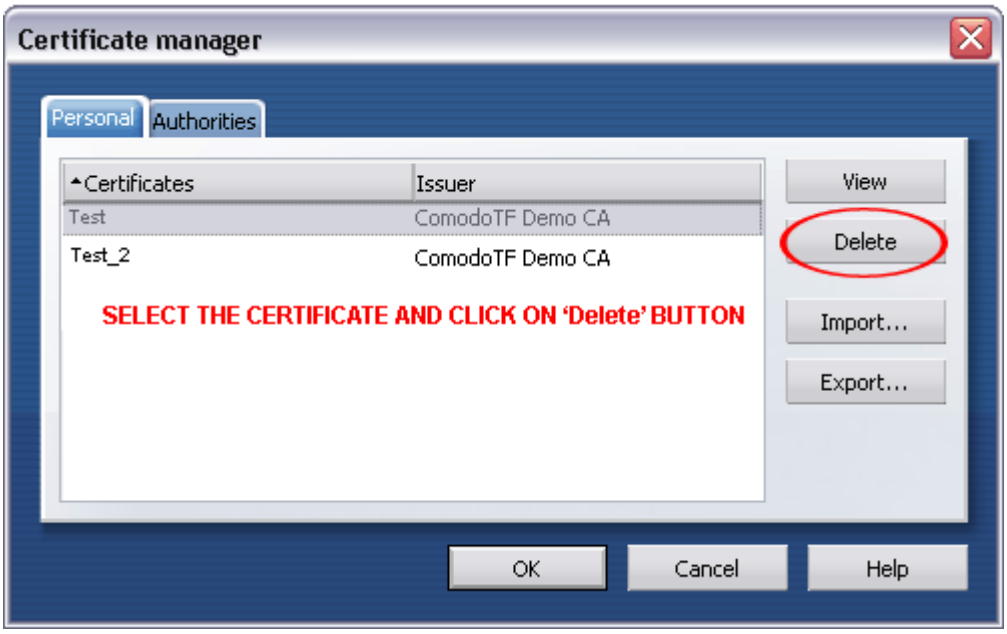


5. In the certificate dialog box select your old certificate. Make sure this is the certificate you wish to remove.

Note: To get more information about selected certificate, click on 'View' button as shown below.



6. Next, if this certificate is your OLD certificate, click the 'Delete' button:



4.4. Removing your OLD digital certificate from Safari

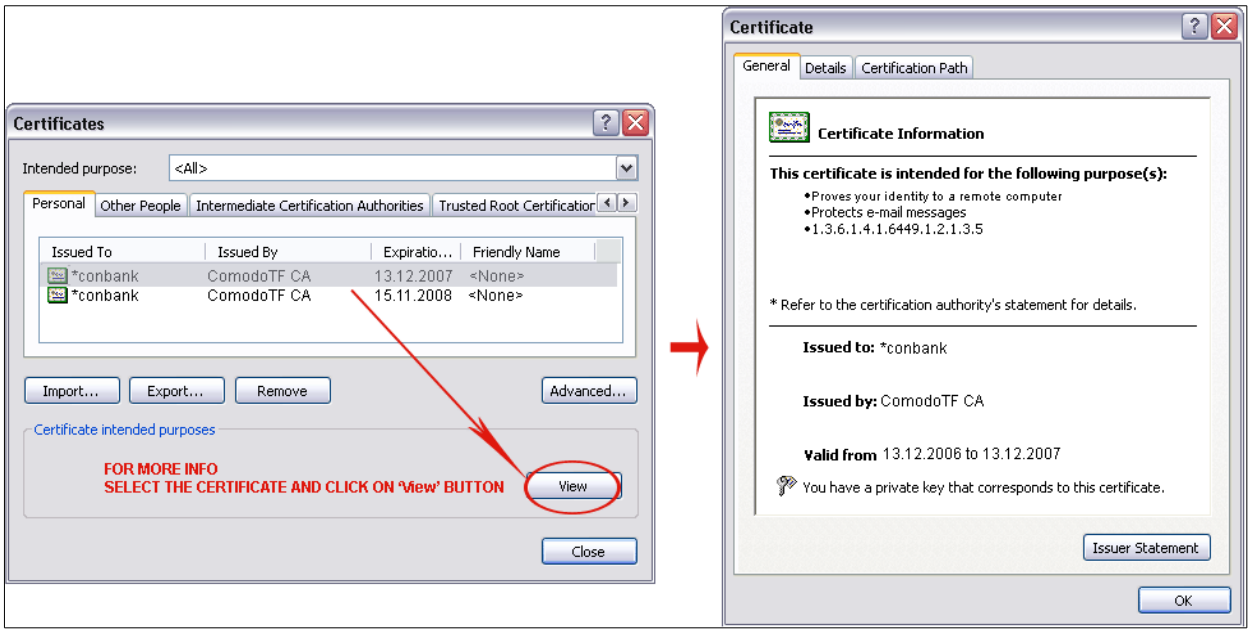
To remove your old digital certificate

Open the Control Panel from Start menu.

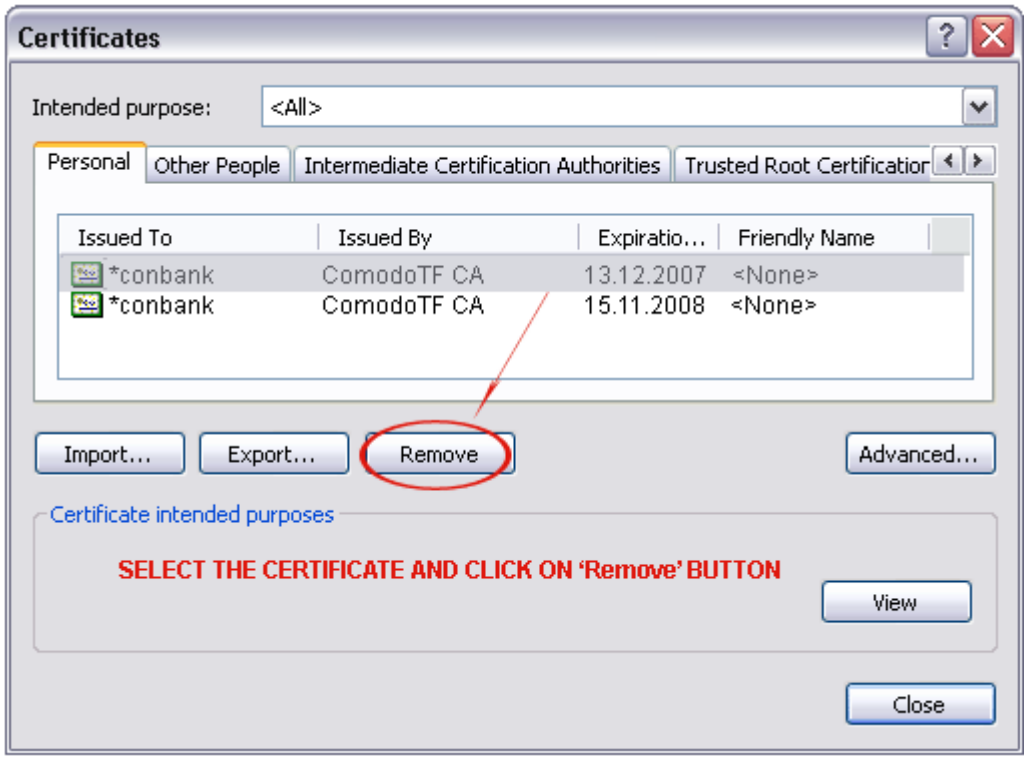
Click Internet Options > Content tab > Certificates.

5. In certificate dialog box select your old certificate. Make sure that this is the needed certificate.

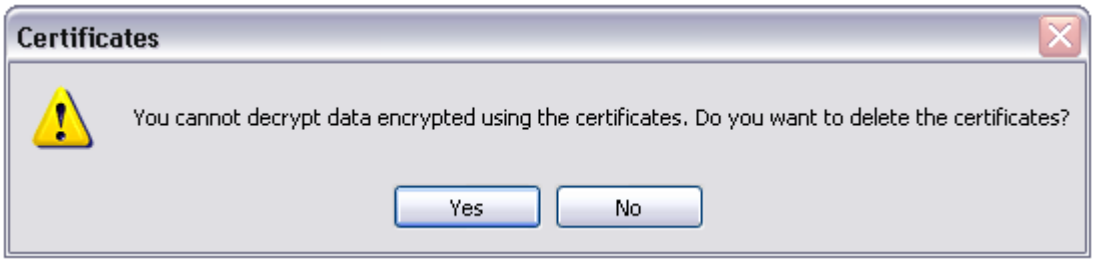
Note: To get more information about selected certificate, click on 'View' button as shown below.



6. Next, if this certificate is your OLD certificate, click on 'Remove' button:



7. You will be asked for confirmation to remove the certificate:



8. Click 'Yes' to confirm deletion.

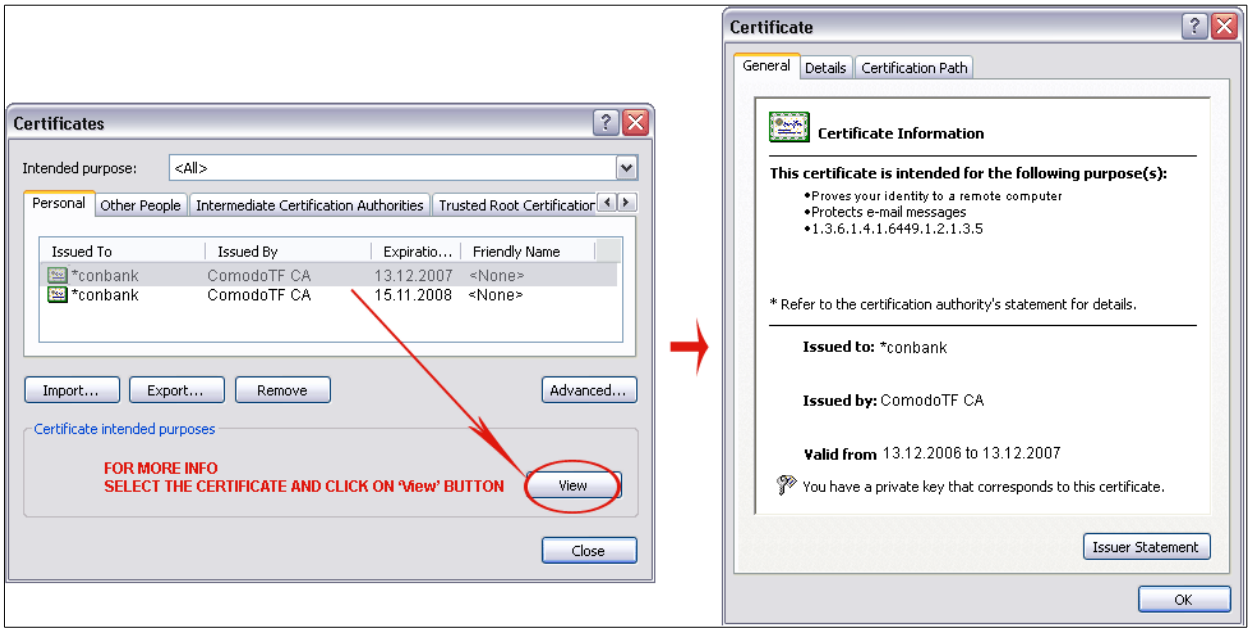
4.5. Removing your OLD digital certificate from Google Chrome

To remove your old digital certificate:

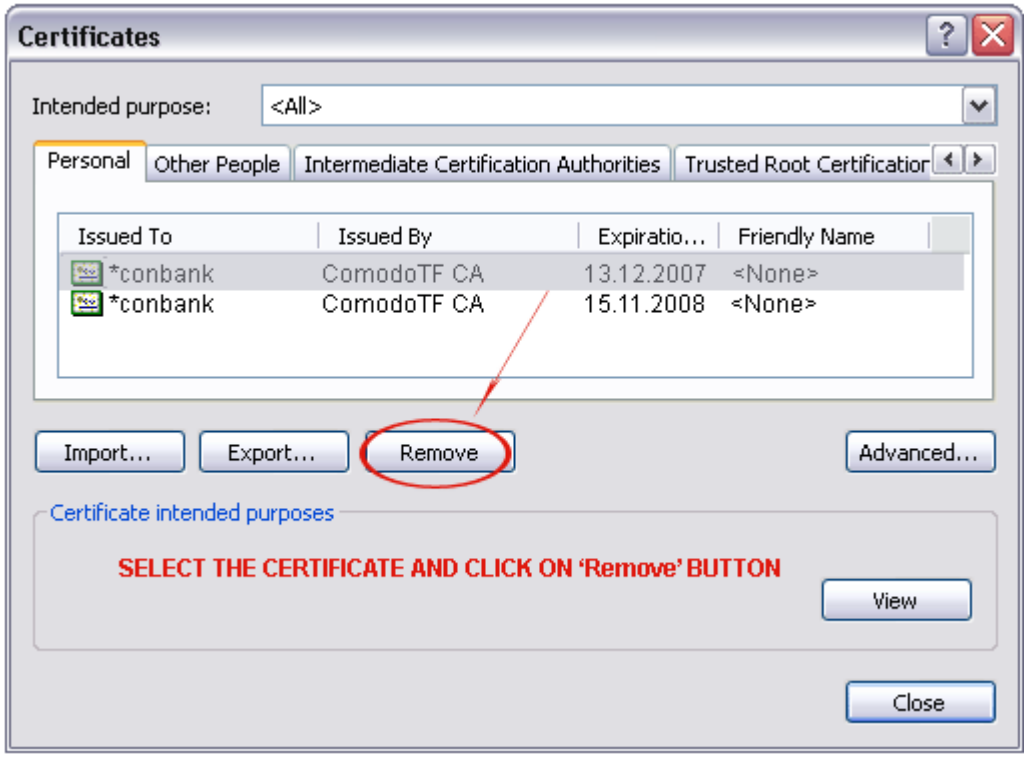
Go to the 'Tools' menu (the wrench icon), select 'Options', click 'Under the hood' tab, scroll down to 'Security' and click 'Manage Certificates'.

5. In the certificate dialog box select your old certificate. Make sure that this is the certificate you wish to remove.

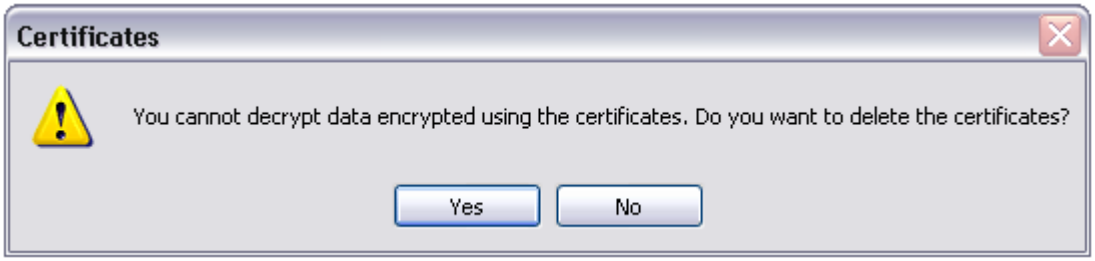
Note: To get more information about selected certificate, click on 'View' button as shown below.



6. Next, if this certificate is your OLD certificate, click on 'Remove' button:



7. You will be asked for confirmation to remove the certificate:



8. Click 'Yes' to confirm deletion.

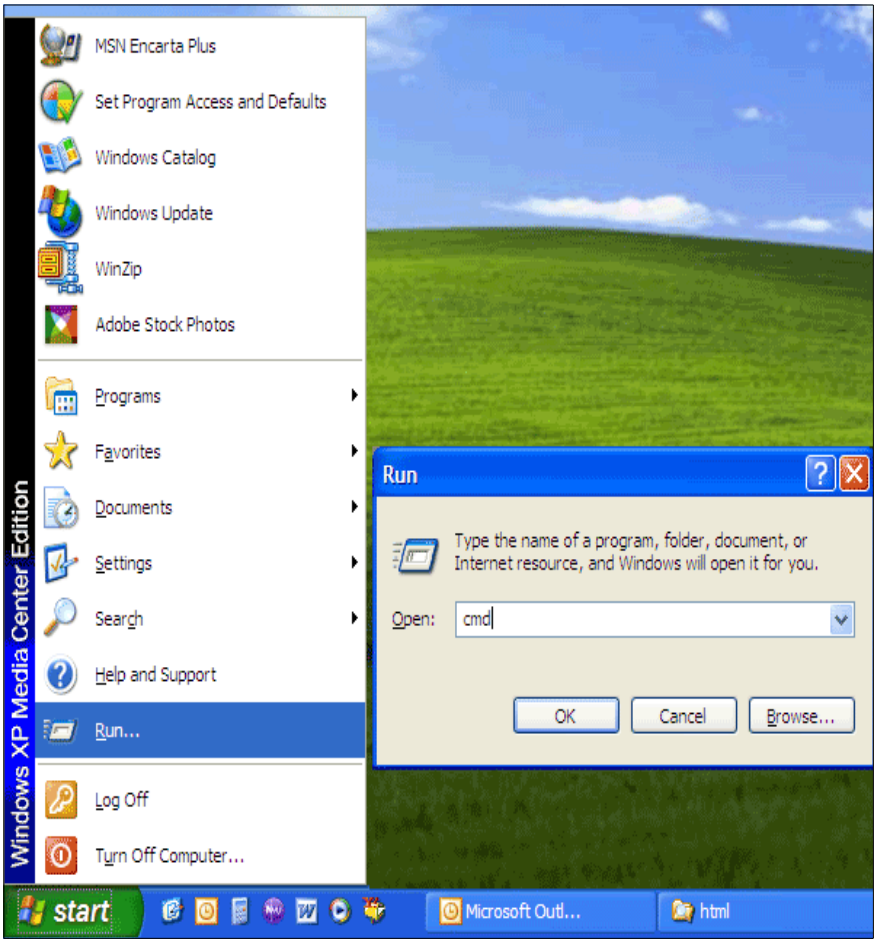
5. Troubleshooting

5.1. 'Page cannot be displayed' error in IE 6/7 after certificate has been installed

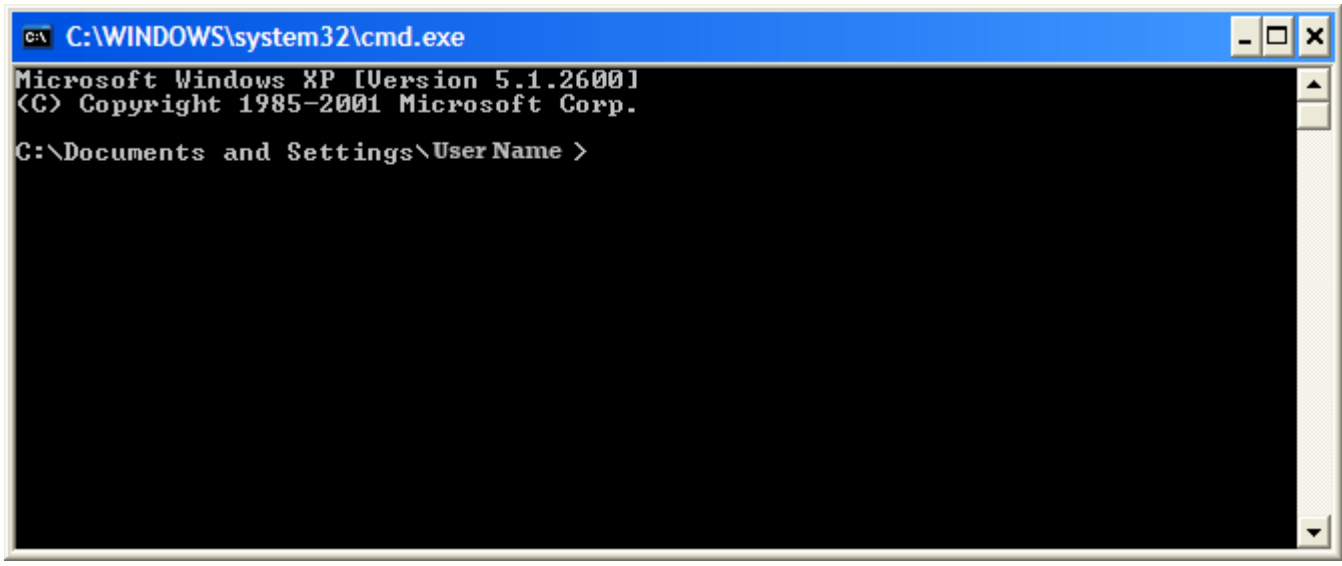
The following procedure describes how to fix the 'Page cannot be displayed' error on Windows XP/ 2000/ 2003 when using Internet Explorer 6.x/ 7.x after installing the client certificate.

To get started, you just need to complete a few, simple, step-by-step instructions.

5. Open up a command prompt window by clicking on Start > Run > . Type 'cmd' at the run menu then click the OK button (see screenshot below)



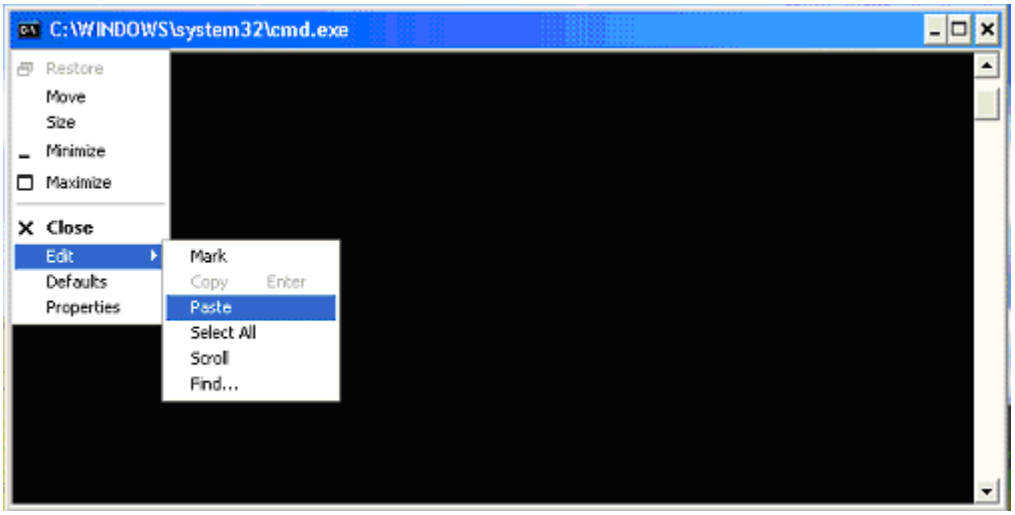
6. Click 'OK'. This will open the command line interface.



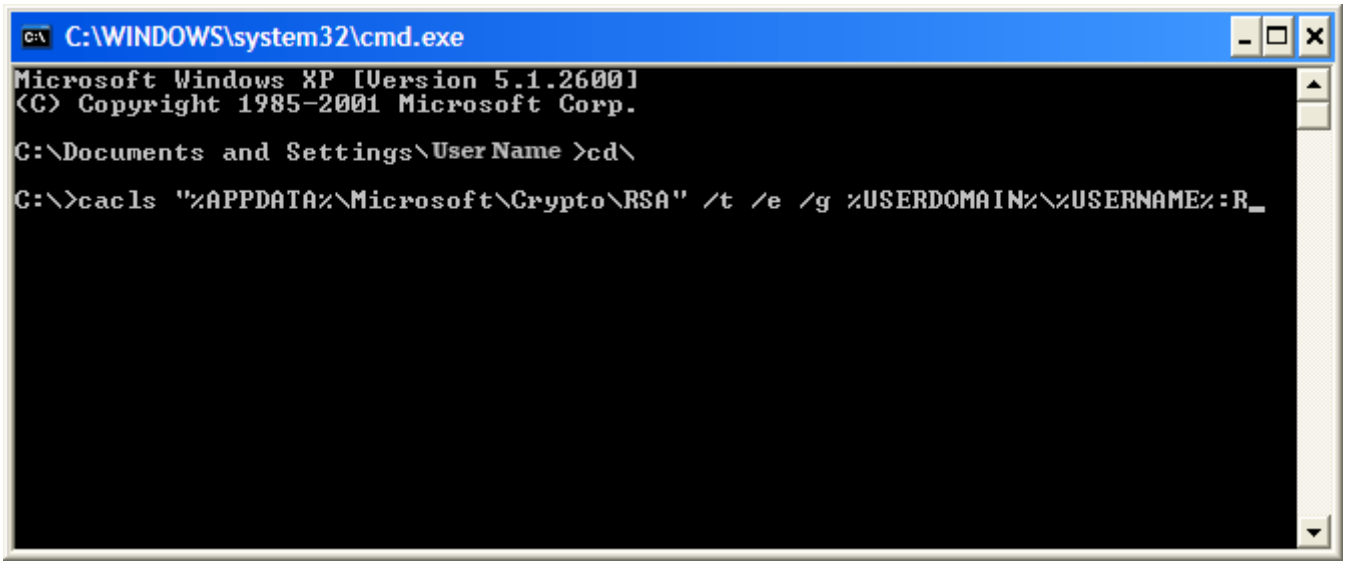
You now need to do three more actions:

- First you should type CD\ then immediately press enter. This will return you to a simple C:\> prompt
- Next , highlight the following command, right click and select 'copy'

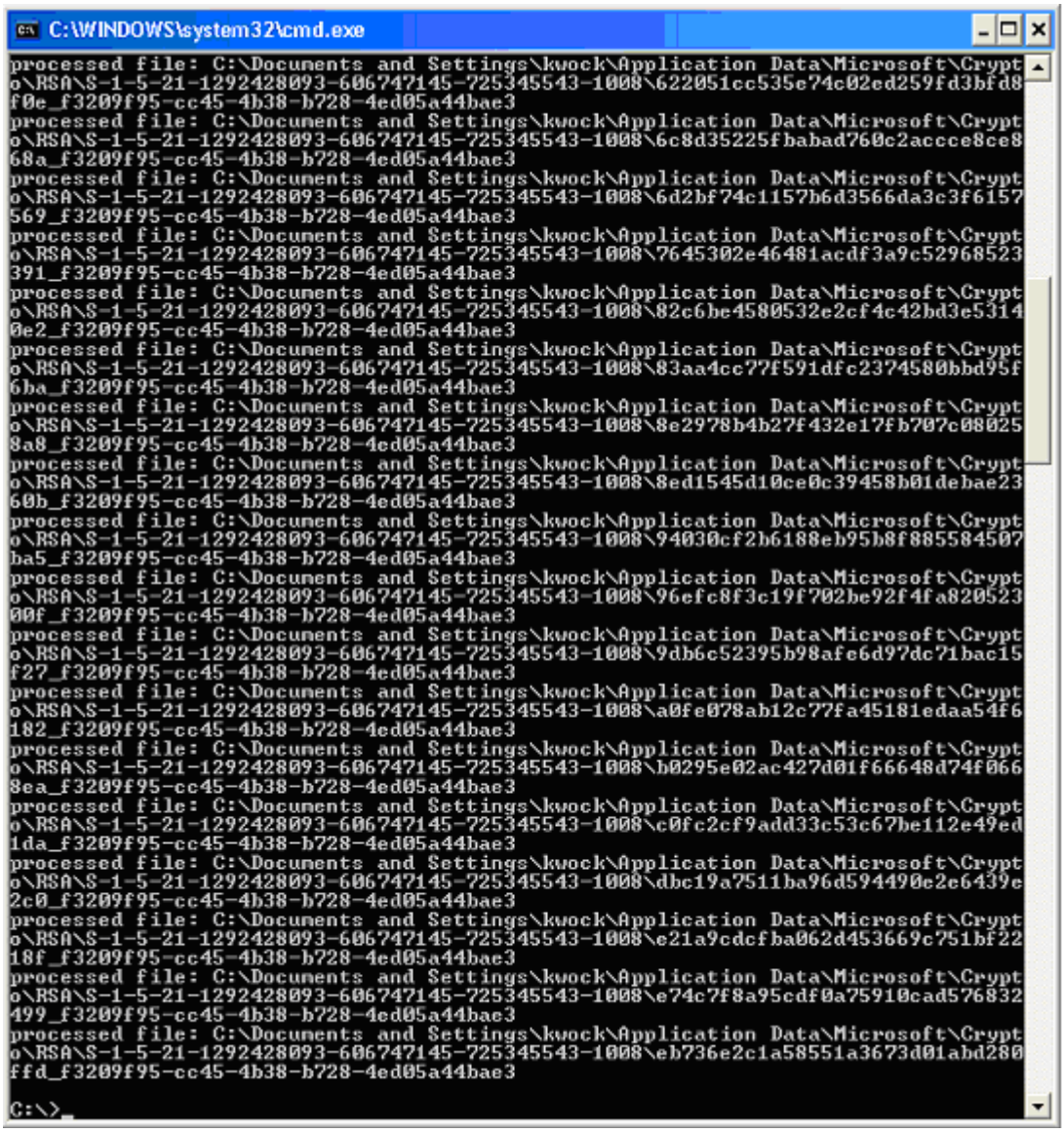
  cacls "%APPDATA%\Microsoft\Crypto\RSA" /t /e /g %USERDOMAIN%\%USERNAME%:R
- Finally, paste the line you just copied into the command line interface by clicking on the  icon at the top left and browsing to the 'paste' command as shown below:



The final command screen should look like the one shown below:



7. Press 'Enter'. You will see a screen similar to the one below:



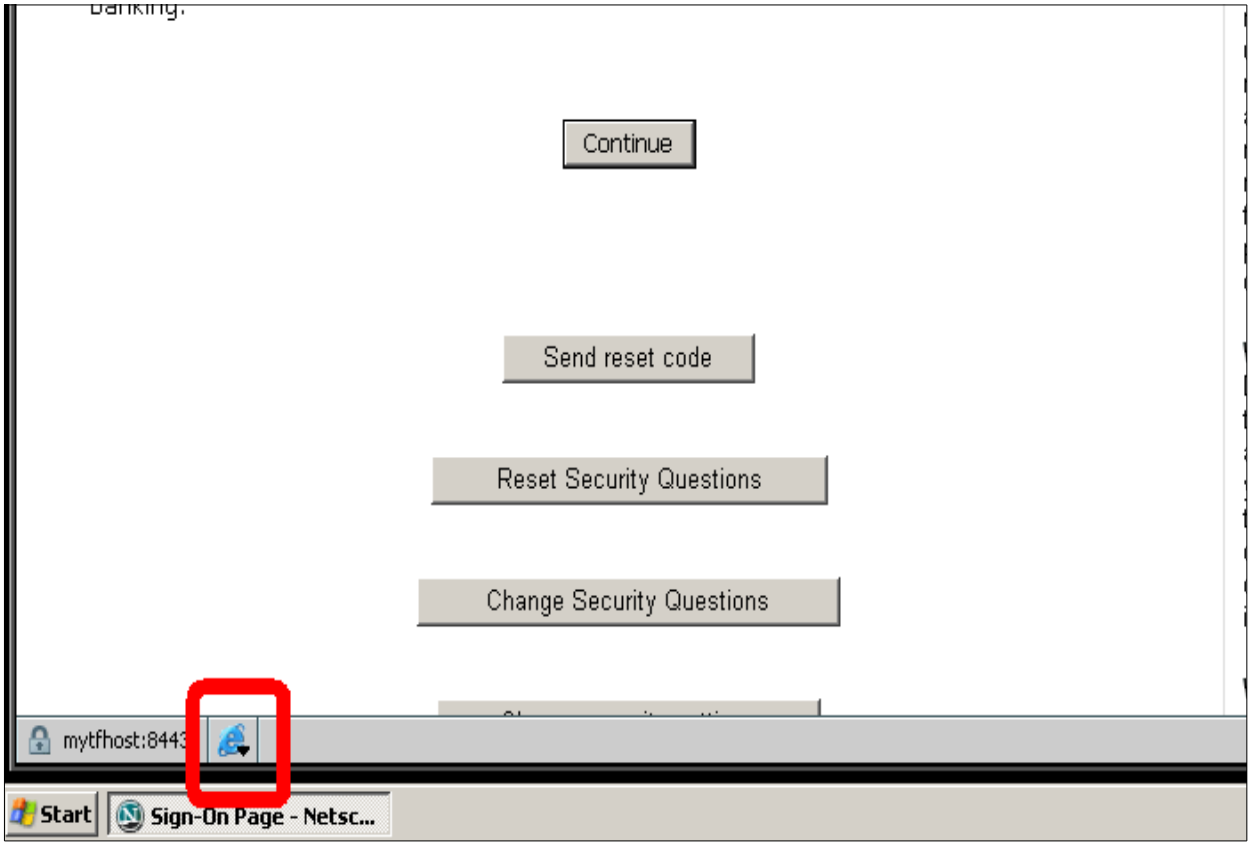
You should now be able to launch your browser and sign-in to your account.

5.2. Netscape 8.0 users running IE render mode

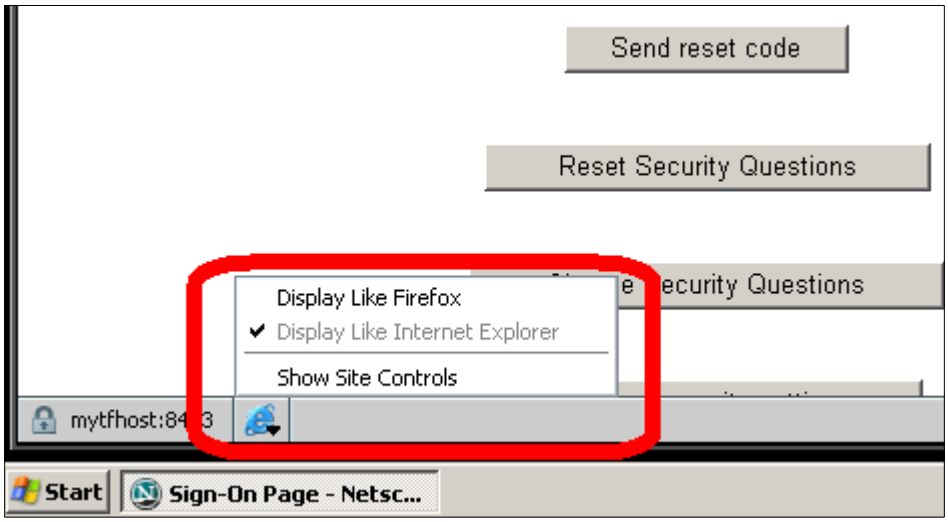
Netscape 8.0 must be running in 'Firefox Render Mode' in order to install a Comodo Client Certificate. They cannot be installed if Netscape 8.0 is running 'Internet Explorer Render Mode'.

Check which render mode you are running before setting up your questions and answers.

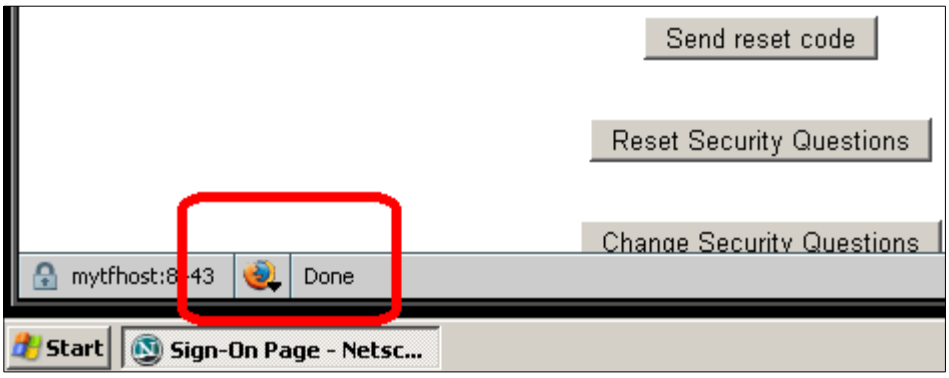
The fastest way to determine this is to look at the lower left hand corner. If the Internet Explorer logo is displayed then you are running in IE Render mode.



To change Netscape 8.0 to 'Firefox Render Mode', simply click on the small, downward facing arrow next the icon and choose 'Display like Firefox' from the menu. (As shown below)



The icon should change to a Firefox icon as shown below:



You should now go ahead and setup your security questions and answers and click the check-box for 'Enable this computer with my Digital Certificate for future secure and convenient online banking'.

Appendix 1 - Table of Browsers Compatibility for Client Certificate and Cookie Installation

Browser	Client Certificates	Secure Cookies
Internet Explorer 8		
Internet Explorer 7		
Internet Explorer 6		
Firefox 3.x		
Firefox 2.0		
Opera 9.63 and below		
Opera 9.64 and above	Certificate installation unsupported Certificate enrollment on certificates installed before update to 9.63 is supported.	
Safari 4.0		
Safari 3.0		
Blackberry		
Chrome 3.0 on Windows and Mac OS		
Chrome 3.0 on Linux		
Chrome 2.0 and below		
MS IE Mobile 6 and above		
MS IE Mobile 5	Not tested	

Browser	Client Certificates	Secure Cookies
Konqueror 4.x	✗	✓
Konqueror 3.x	✓	✓
Netscape	✓	✓
Other browsers based on IE, Safari or Firefox (AOL, OmniWeb etc.)	✓	✓

About Comodo

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

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

Comodo Group Inc.

1255 Broad Street

STE 100

Clifton, NJ 07013

United States

Tel: +1.877.712.1309

Tel: +1.703.637.9361

Email: **EnterpriseSolutions@Comodo.com**

Comodo CA Limited

3rd Floor, 26 Office Village,

Exchange Quay,

Trafford Road, Salford,

Greater Manchester M5 3EQ,

United Kingdom

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

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