



Digital ID Certificates User Guide



September 2011

Revision 4

Table of Contents

1. Introduction.....	3
2. NRC's Use of Digital ID Certificates	3
3. Requesting an NRC Approval Code	3
4. Digital ID Certificate Enrollment Steps.....	5
5. Digital ID Certificate Installation Steps.....	11
6. Digital ID Certificate Export (Backing Up)	13
<i>6.1 Mozilla Firefox Users Only</i>	<i>18</i>
7. Digital ID Certificate Import	21
<i>7.1 Mozilla Firefox Users Only</i>	<i>26</i>
8. Digital ID Certificate Viewing Steps.....	28
9. Digital ID Certificate Renewal.....	31
10. Digital ID Certificate Revocations	31
11. Troubleshooting	34
<i>11.1 Immediate Assistance.....</i>	<i>34</i>
<i>11.2 Trusted Sites</i>	<i>34</i>
<i>11.3 Enabling ActiveX Controls and Plug-ins</i>	<i>35</i>
<i>11.4 Apple Macintosh Users.....</i>	<i>38</i>

The screen prints presented in this document may vary in appearance from what is displayed for you. This is dependant on the type of Web Browser and Version you use.

The actions outlined within this guidance document are to be followed as best as possible.

1. Introduction

The U.S. Nuclear Regulatory Commission (NRC) requires individuals and organizations to have digital ID certificates in order to submit and/or view documents electronically. The Electronic Information Exchange (EIE) system was the first NRC system requiring digital IDs. This system supports several document submission forms used by different program areas at the NRC. The NRC is developing more applications, which will require digital certificates for access.

2. NRC's Use of Digital ID Certificates

Seven different EIE programs require NRC customers to use digital ID certificates. Those submitting documents to the NRC must determine which program will meet their needs and contact the appropriate program's staff to get approval to participate. The applications using EIE digital ID certificates are:

- ① Adjudicatory (Electronic Hearing Docket and DDMS)
- ② Code Development System
- ③ Criminal History
- ④ Emergency Response Data System (ERDS)
- ⑤ Fitness for Duty (FFD)
- ⑥ General Form
- ⑦ Record Classification Action (RCA)

The Criminal History Program supports nuclear power plant requests for FBI background investigations of their staff. Fingerprints and other personal data are transmitted via this program. Participants in this program need to be sponsored by a nuclear power plant and must be included on the Criminal History Program's access list.

The Adjudicatory Proceedings Program (which involves any case being brought before the NRC) uses digital ID certificates and various access lists to enable hearing participants to submit and view appropriate hearing materials. Access rights to hearing materials are controlled based upon the sensitivity of documents and other factors judged appropriate. Documents associated with various adjudicatory hearings will have lists of people who may have various access rights to hearing documents.

The General Form Program is less restrictive and is functionally like an electronic mailbox for incoming documents from various individuals representing many public and corporate entities. This form allows people to submit digitally signed documents to the NRC for a variety of purposes.

There are three steps to get a VeriSign Digital ID from the NRC:

- ① Request an NRC Approval Code, (see [Section 3](#))
- ② Enroll for your Digital ID certificate on-line (see [Section 4](#)), and
- ③ Install your Digital ID certificate (see [Section 5](#)).

3. Requesting an NRC Approval Code

To request an NRC Approval Code, you must first determine which NRC program meets your needs. Each program area will want basic information from you including your name,

email address, phone number, organization, role in the organization and reason for submitting documents to the NRC.

Criminal History Program:

- ♦ Call: (301) 492-3531 or
- ♦ Email the NRC's Criminal History Program staff at: CrimHist.Resource@nrc.gov

Adjudicatory Proceedings Program:

- ♦ Call: (301) 415-1677 or
- ♦ Email the NRC's Office of the Secretary staff at: HearingDocket@nrc.gov

NRC General Form Program:

- ♦ Call (toll-free): (866) 672-7640 or
- ♦ Email the NRC's General Form Program staff at: General.FormResource@nrc.gov

Records Classification Action:

- ♦ Call: (301) 415-2165 or
- ♦ Email: RCAAdmin@nrc.gov

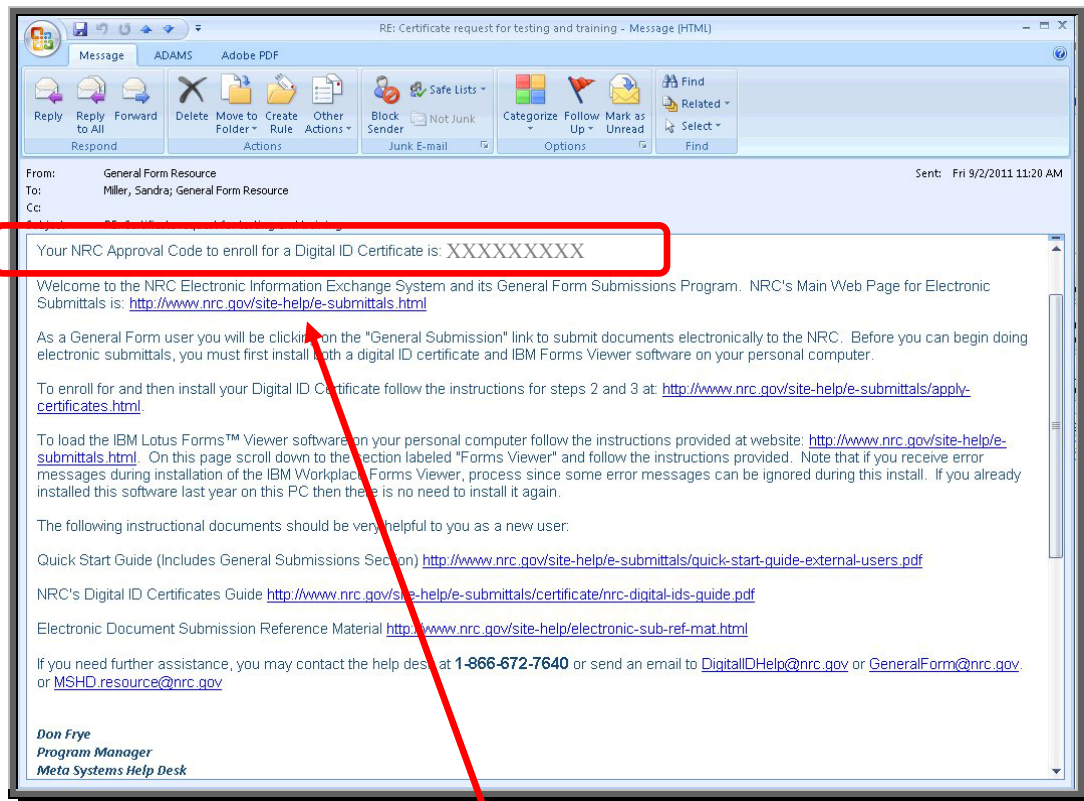
ERDS:

- ♦ Email the NRC's ERDS staff at: ERDS.Resource@nrc.gov

Fitness for Duty Reporting:

- ♦ Call: (301) 415-5949 or
- ♦ Email the Fitness for Duty Reporting staff: FitnessForDuty.Resource@nrc.gov

After submitting your request you will receive an email message with the NRC Approval Code:

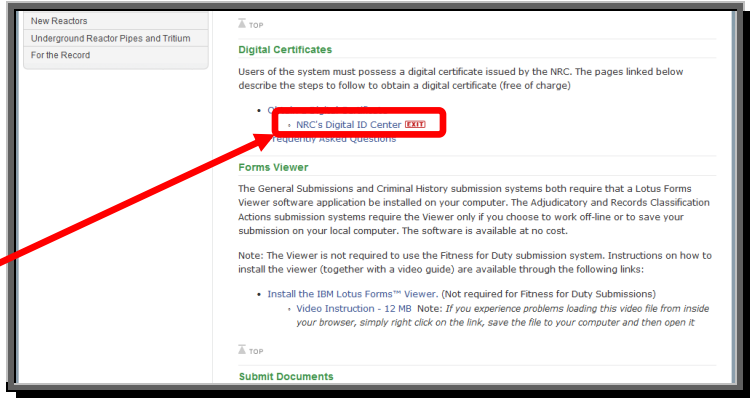


Click on the <http://www.nrc.gov/site-help/e-submittals.html> link provided in the email.

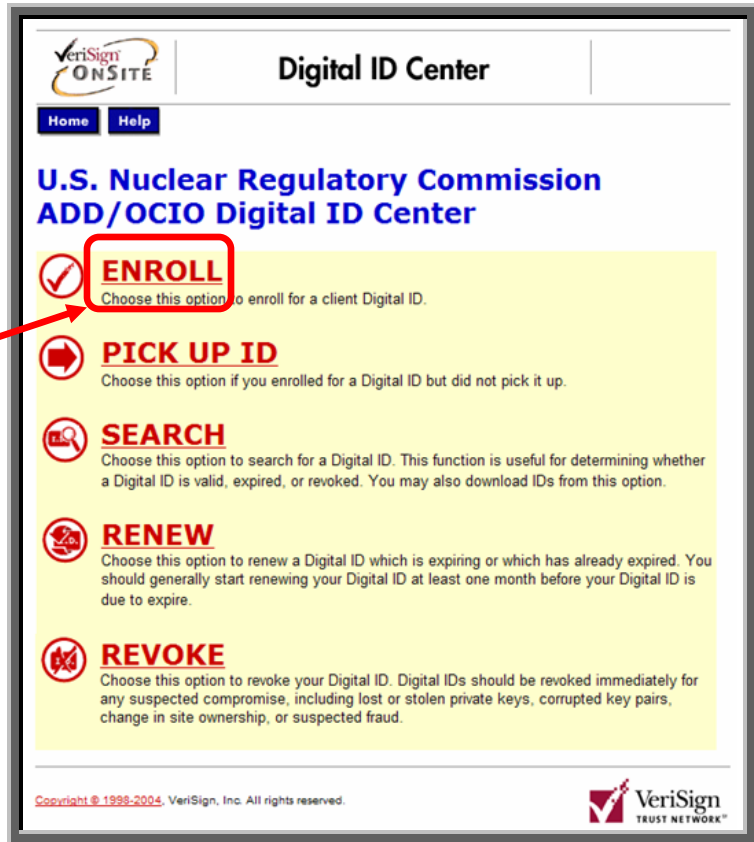
4. Digital ID Certificate Enrollment Steps

From the “*Electronic Submittal’s*” Webpage (<http://www.nrc.gov/site-help/e-submittals.html>), scroll down to the **Digital Certificates** Section. Click on the link:

- [NRC's Digital ID Center](#) **EXIT**



Select **ENROLL**.



The Enrollment Form will be displayed.

Complete the form, populating all required fields, annotated with a **blue** asterisk(*) and **(required)**.

First Name: * (required) Nickname or middle initial allowed (Example: Jack B.)
Last Name: * (required) (example -- Doe)
Your E-mail Address: * (required) (example -- jbdoe@verisign.com)
Title: * (Example: Programmer)
NRC Certificate Approval Code: (required)
Organization Name: (required)
Phone Number: (required)
Enter Challenge Phrase: (required) Do not use any punctuation.

Include your middle initial after your first name as in "John D".

The email address you enter will be stored on your digital ID certificate and has multiple uses including:

- ① It is used to send your certificate to you
- ② It must match the email address stored in NRC access list(s)
- ③ It is used to send your annual renew reminder messages

The challenge is simply a one word password you can easily remember. The challenge phrase rules are:

- ① 1 to 32 characters long
- ② Only letters, numbers and/or spaces
- ③ Case and space sensitive (avoid trailing blanks)
- ④ Spaces and numbers are not required
- ⑤ Punctuation is not allowed

The "Optional: Enter Comments" can be ignored since this is not used by the NRC.

Select the **Submit** button.

Challenge Phrase
The Challenge Phrase is a unique phrase that protects you against unauthorized action on your Digital ID. Do not share it with anyone. *Do not lose it.* You will need it when you want to revoke or renew your Digital ID.

Enter Challenge Phrase: (required)
Do not use any punctuation.

Optional: Enter Comments
In some cases, your administrator will instruct you to enter *Shared Secret* information (known only to you and the administrator) in this field. The administrator uses this shared secret to verify that it really is *you* submitting the application. This comment will not be included in your Digital ID.

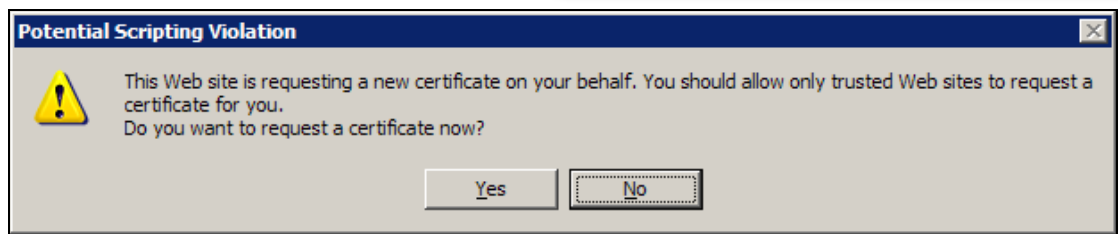
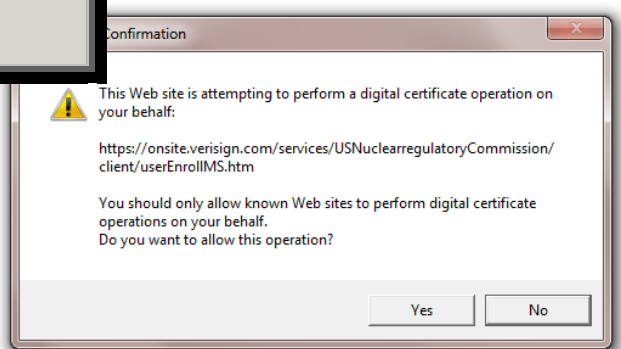
If all the information above is correct, click **Submit** to continue.

Submit **Cancel**

Copyright © 1998-2004, VeriSign, Inc. All rights reserved. VeriSign TRUST NETWORK™

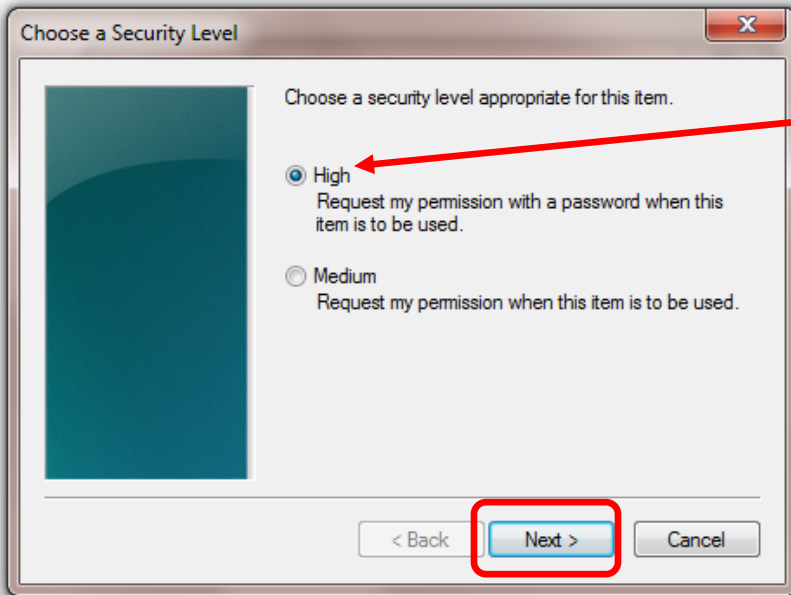


Any dialogue boxes which appear, select **OK** and/or **Yes**:



Select the button.

Set Security Level...



Select

High

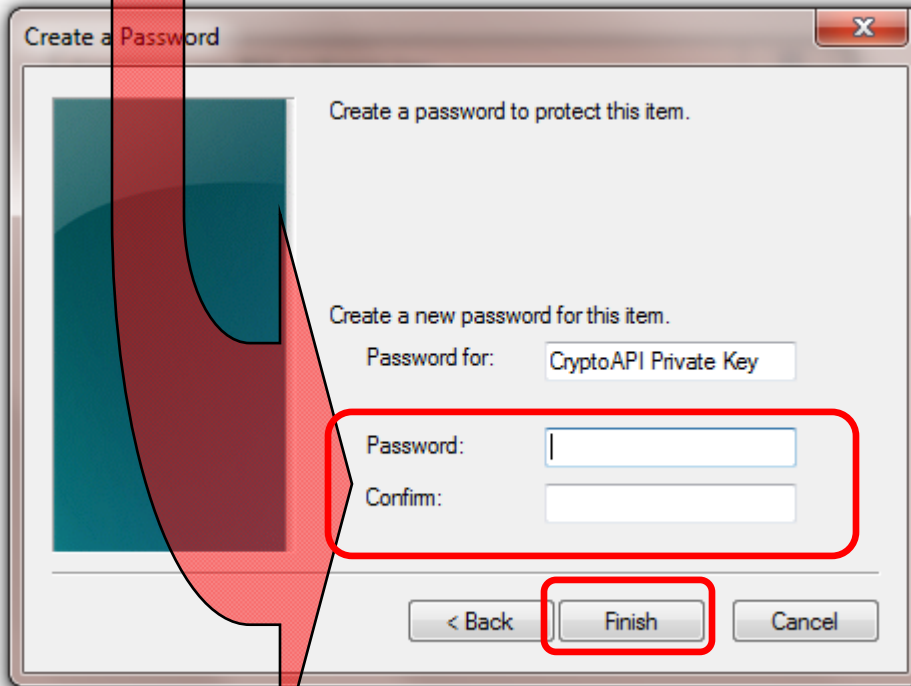
Then select the

Next >

button.

Enter the password twice (as a suggestion, use the same password used for the challenge phrase, see [Page 6](#).)

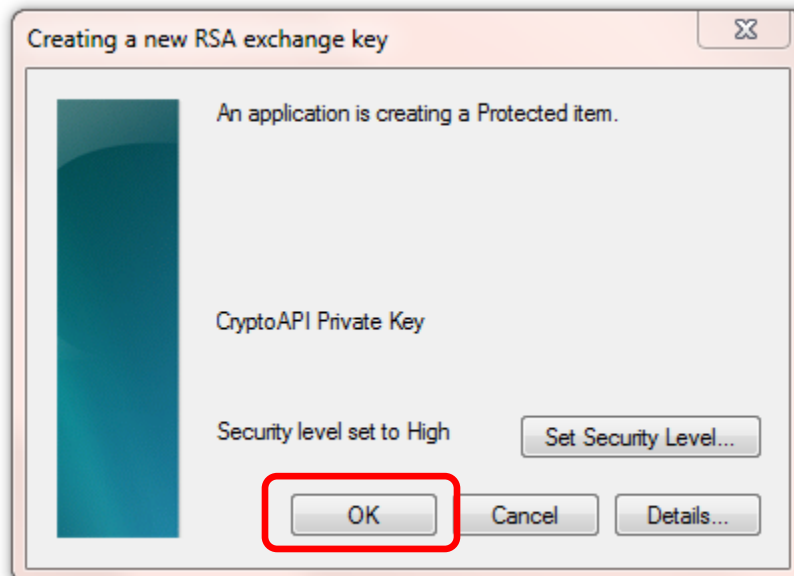
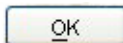
Note: *Commit to memory* this password as it will be necessary to enter this password each time you use the certificate. If a certificate password is forgotten, it cannot be reset. A new certificate must be requested.



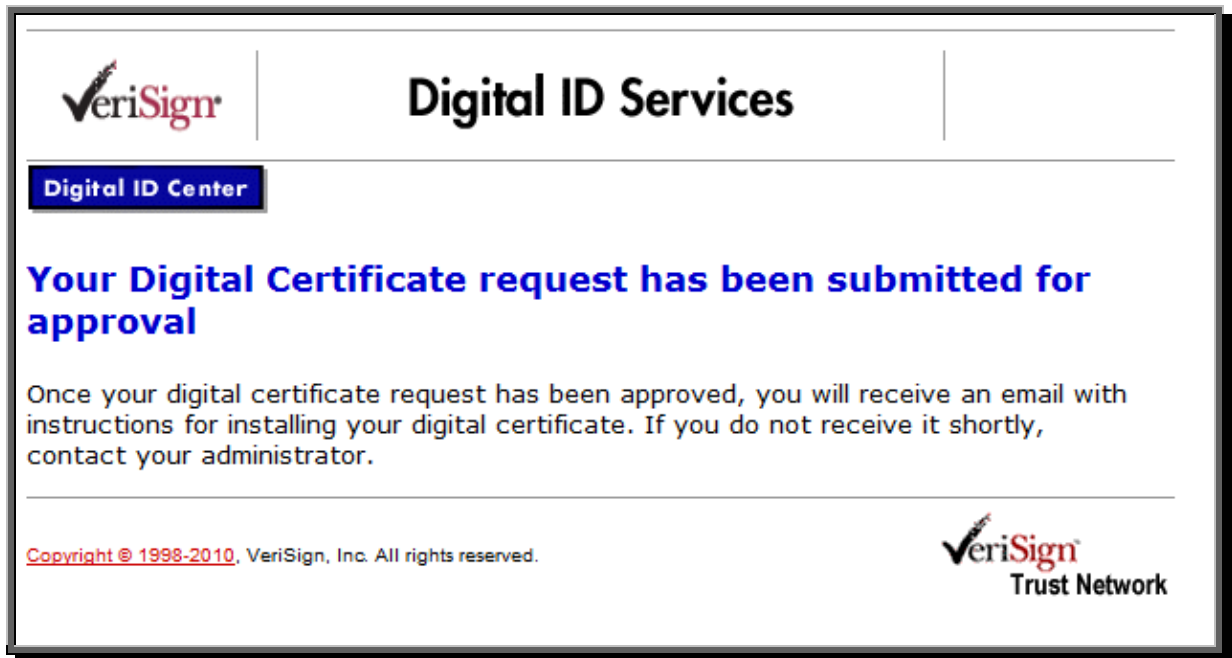
Click on the **Finish** button.

The Security level is now set to **High**.

Click on the **OK** button.



You have now successfully requested your digital ID certificate. A notification will appear to [Look in Your E-mail](#).



The screenshot shows a web page titled "Digital ID Services" with the VeriSign logo in the top left. Below the title is a blue button labeled "Digital ID Center". The main heading reads "Your Digital Certificate request has been submitted for approval". Below this, a paragraph states: "Once your digital certificate request has been approved, you will receive an email with instructions for installing your digital certificate. If you do not receive it shortly, contact your administrator." At the bottom left, there is a copyright notice: "Copyright © 1998-2010, VeriSign, Inc. All rights reserved." At the bottom right, the VeriSign Trust Network logo is displayed.

Within minutes you should receive an email acknowledging receipt of your enrollment request.

Within several hours (Eastern Standard Time business hours) your request should be reviewed and approved or disapproved. You should then receive a second email. The approval email's subject is: "Your Digital ID is ready".

Follow the instructions in this document for installing a digital ID certificate (see [Digital ID Certificate Installation Steps](#)).



IMPORTANT:

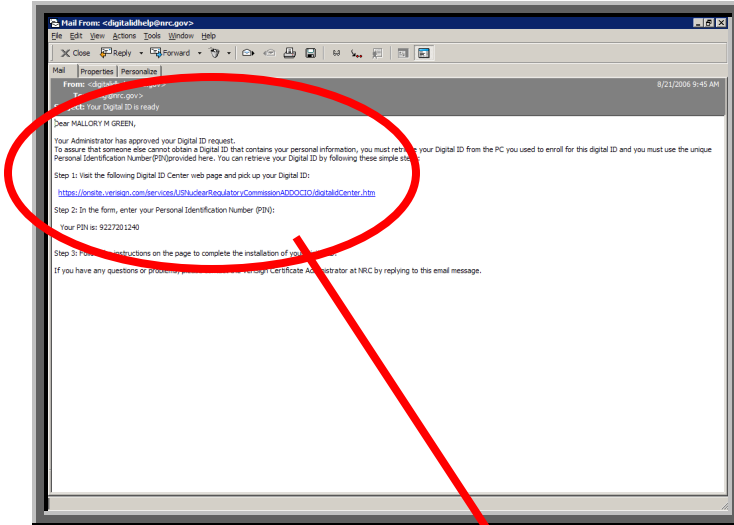
You must pick up your digital ID certificate from the same PC where you enrolled. This is a security precaution imposed by VeriSign. Therefore only enroll from a PC where you receive email for the email address to be associated with your certificate

If you have not received an approval or rejection email within two business days, send an email to DigitalIDHelp@nrc.gov or call (866) 672-7640.

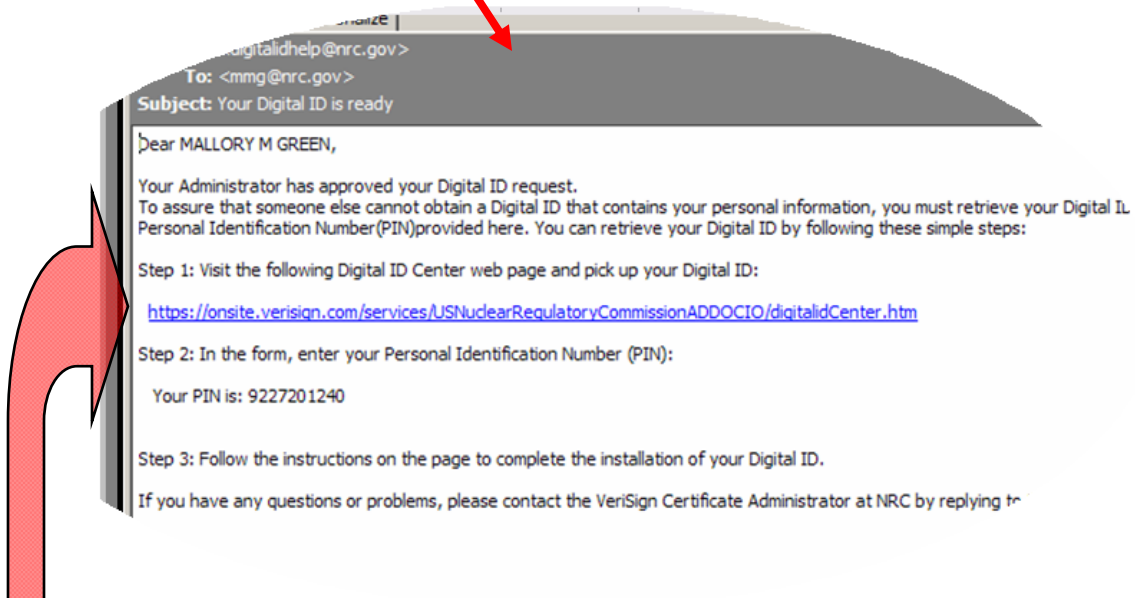
5. Digital ID Certificate Installation Steps

You will receive a “Your Digital ID is ready” email, if your digital ID certificate request is approved.

Open the “Your Digital ID is ready” email message.

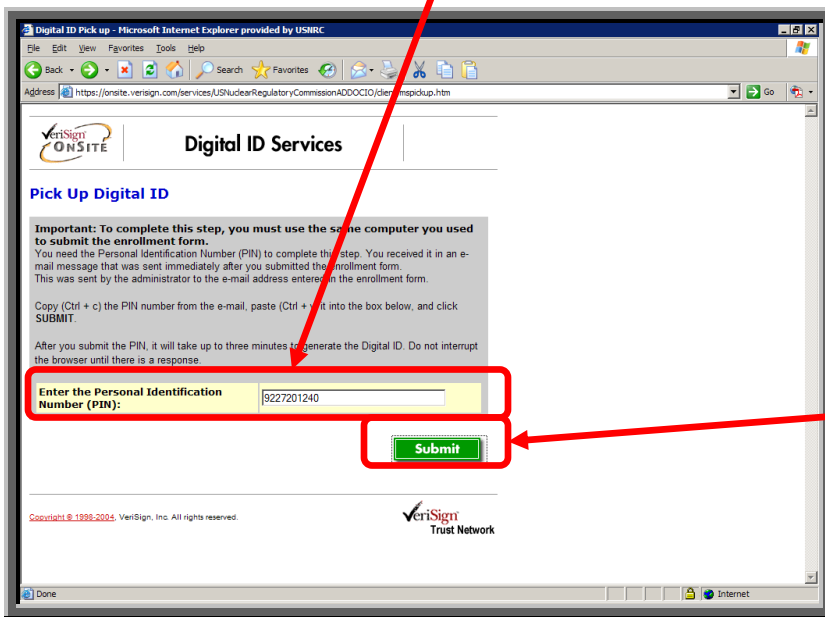


Copy the PIN (provided in Step 2 of the email message). An easy copying method is to highlight the PIN then right-mouse click and select the “Copy” option.



Next, click on the link (provided in Step 1 of the e-mail message), which takes you to NRC’s Digital ID Center’s **PICK UP ID** web page.

Click within the **Enter the Personal Identification Number (PIN)** field and paste the PIN into the field.



Click on the



button.



Did you receive a *Potential Scripting Violation* dialogue box?

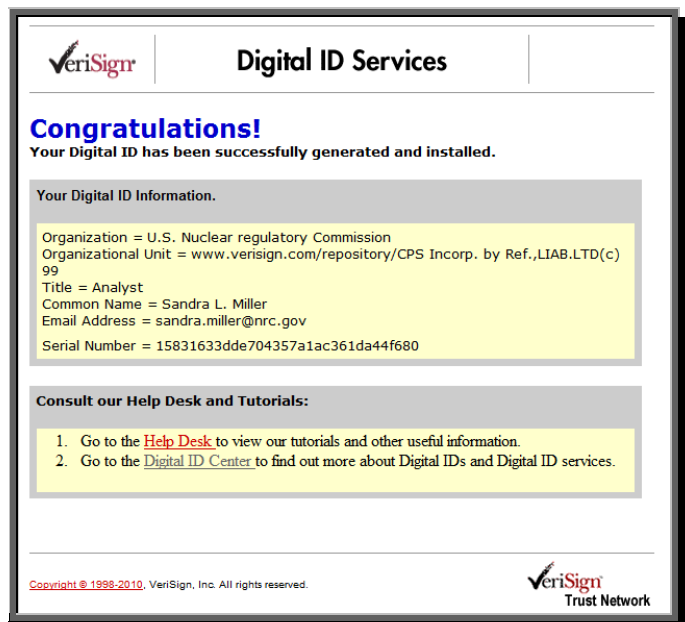
Yes Click on the button, then continue with the instructions below.

No Continue with the instructions below.



You will receive a **Congratulations!** screen telling you that your digital ID certificate have been successfully generated and installed.

It is highly recommended to *immediately* export (i.e., back-up) your certificate!



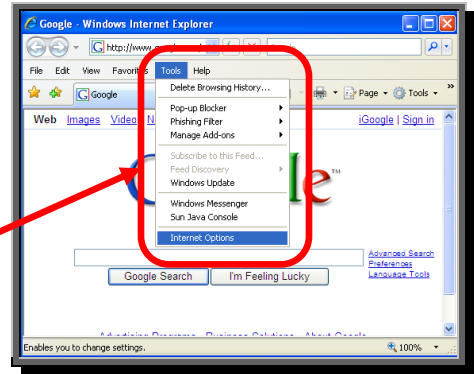
6. Digital ID Certificate Export (Backing Up)

Backing up (exporting) is essential for maintaining a copy of your certificate.

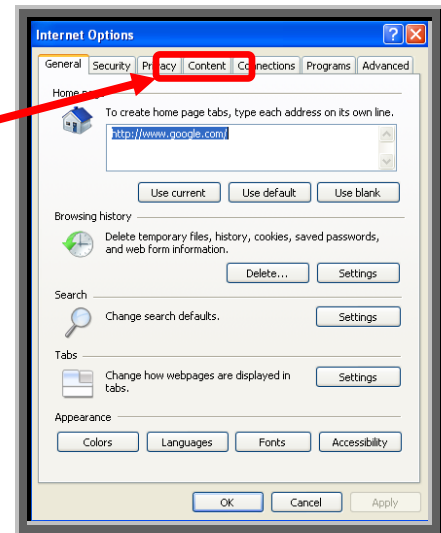
The certificate can be exported from one computer and imported onto another computer.

Open your Internet Explore browser.

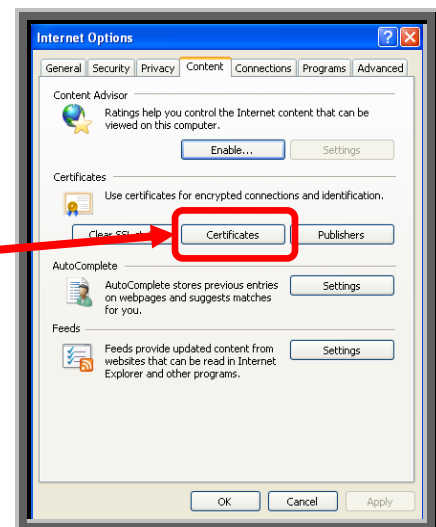
Click on the **Tools** menu option.
Select **Internet Options**.



Click on the **Content** tab.



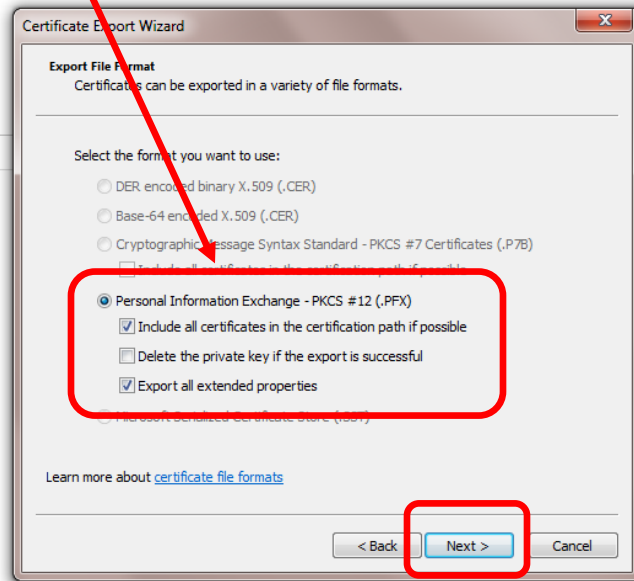
Click on the **Certificates** button.



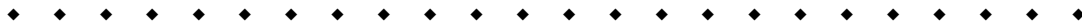
Select the following three items:

- Personal Information Exchange - PKCS #12 (.PFX)
- Include all certificates in the certification path if possible
- Delete the private key if the export is successful
- Export all extended properties

Note: **DO NOT** delete the private key and **DO NOT** proceed until you verify the **three** items only are selected to ensure the export process is successful!

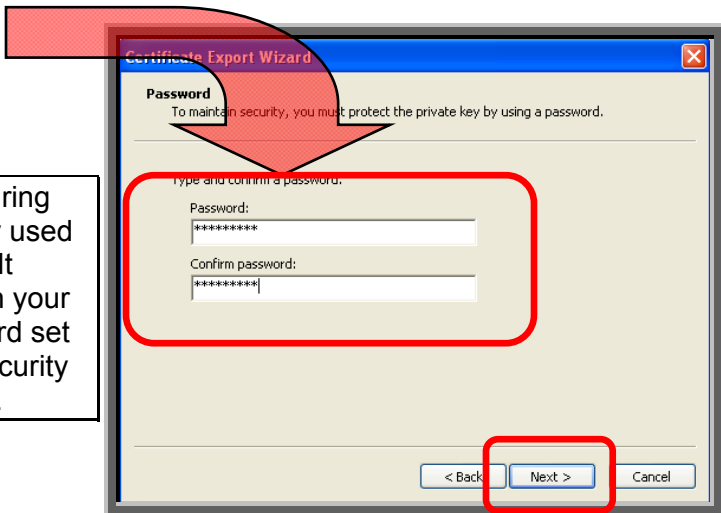


Select .



Type in an export/import password twice (as a suggestion, use the same password used for the challenge phrase, see [Page 6.](#))

Note: This password is created during the export process and only used during the import process. It should not be confused with your digital ID certificate password set immediately after setting security to “High” for your certificate.



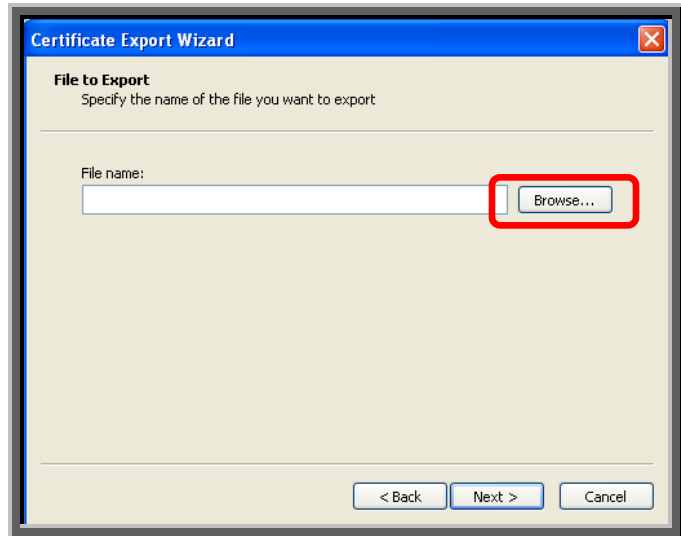
Select .

Select the button to navigate to the appropriate file path location of where the certificate is to be stored.

Suggestions are:

- ♦ Removable media (i.e., memory stick)
- ♦ Network Drive (i.e., H:/ drive or above.)

You may also email the certificate to yourself as an attachment, then save to a email folder (any computer you are able to access your email, you will then be able to access your certificate.)



Type the certificate name within the **File name** field.

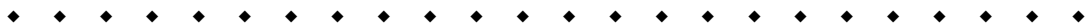
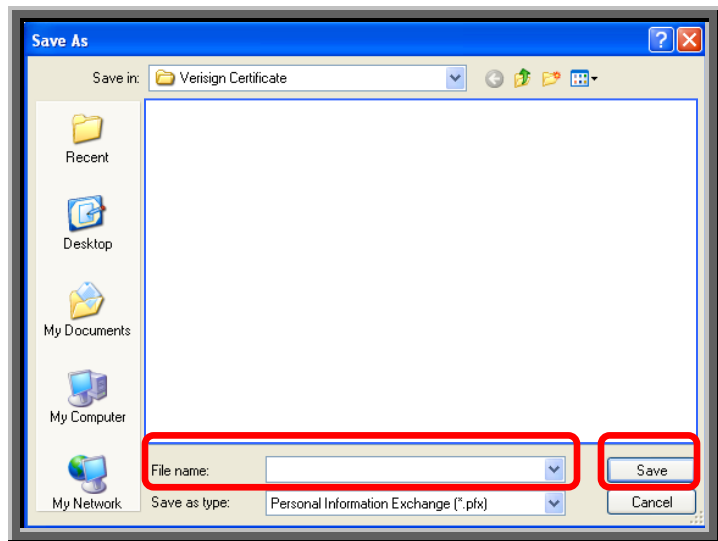
Suggested file name:

Your name, NRC, and the expiration date of the certificate.
Example:

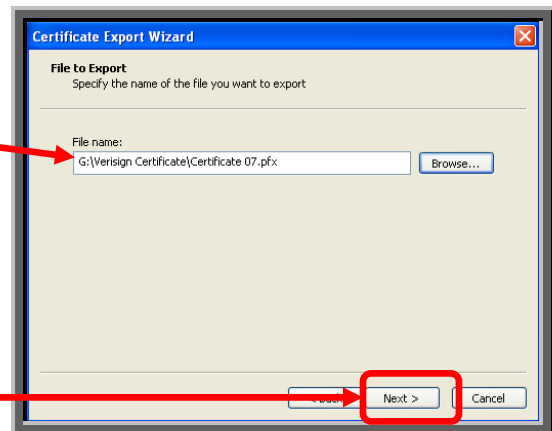
John Smith NRC 01NOV2012

The certificate file's extension is Personal Information Exchange (*.pfx).

Select .



The **File name** field will populate with the file path selection made.



Select the button.



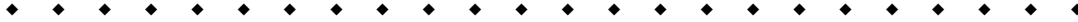
At the *Completing the Certificate Export Wizard* dialogue box, select the **Finish** button.



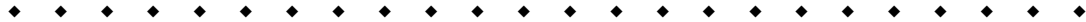
Within the **CryptoAPI Private Key** field, enter the certificate password.



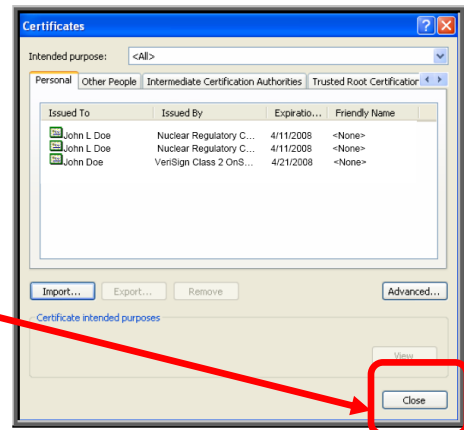
Select the **OK** button.



A dialogue box will appear with the message that the export was successful. Select the **OK** button.



To complete the exporting process, select **Close**.



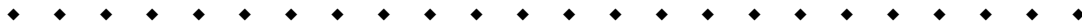
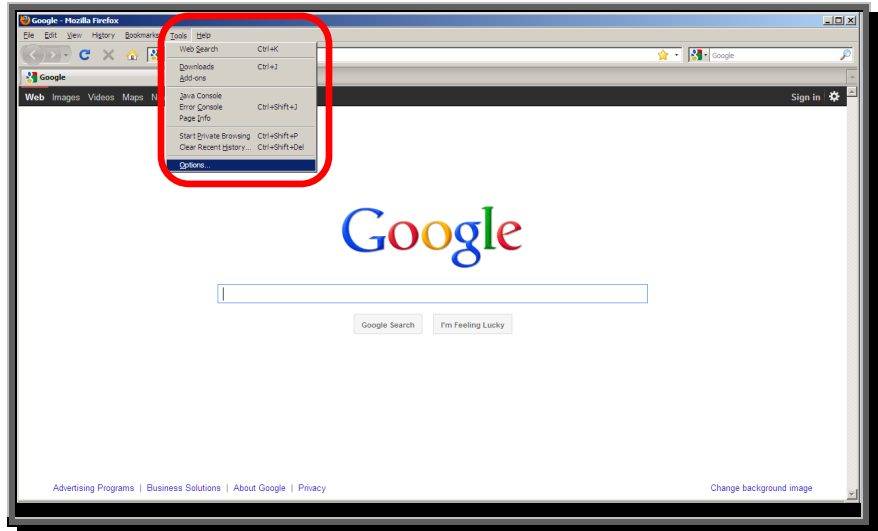
6.1 Mozilla Firefox Users Only

The following Certificate Back-up instructions are to aid users of Mozilla Firefox as their Web Browser:

Open Mozilla Firefox.

Select: **Tools**.

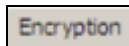
Scroll down and select: **Options**.



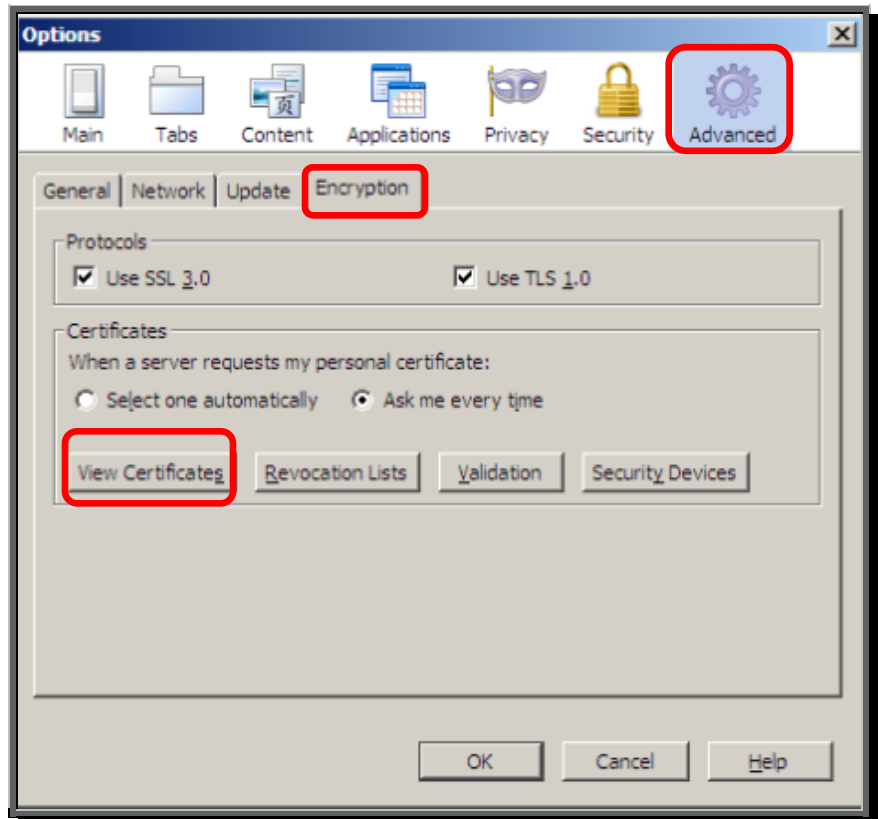
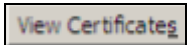
Select the icon.

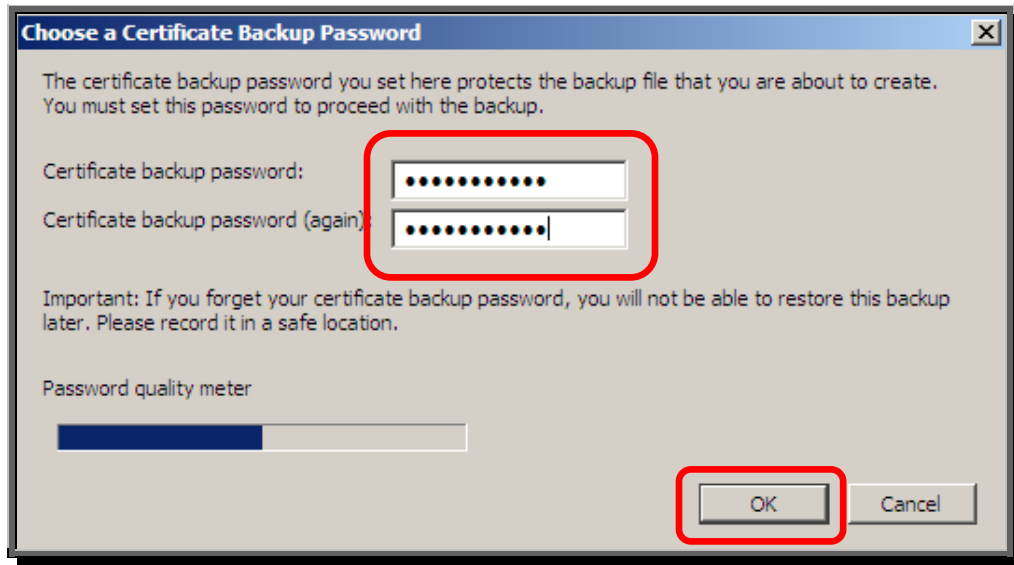


Select the tab.



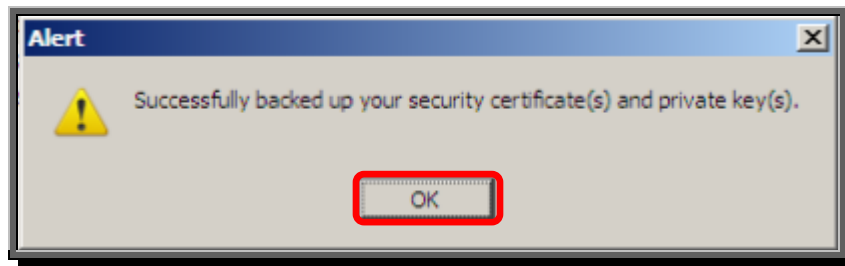
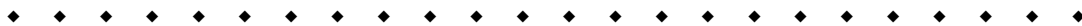
Select





Enter a password twice (as a suggestion, use the same password used for the challenge phrase, see [Page 6.](#))

Select .



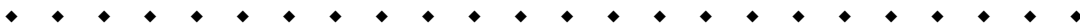
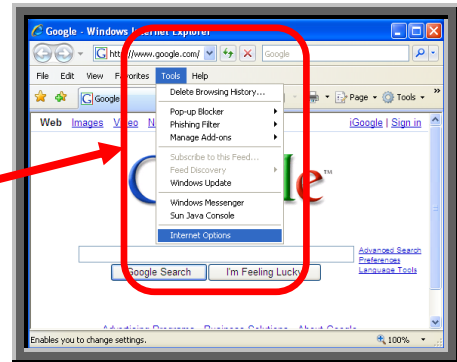
The backup is successful. Select the button.

Select at the next two dialogue boxes to exit.

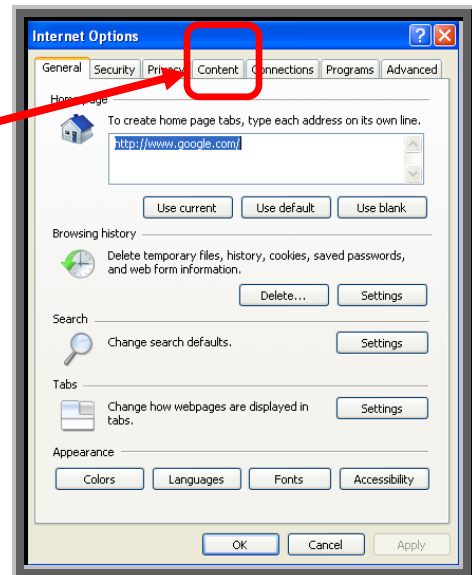
7. Digital ID Certificate Import

A certificate may be imported (copied) to a multiple number of computers. To import the certificate to a different computer (from where it was received), first open Internet Explorer browser.

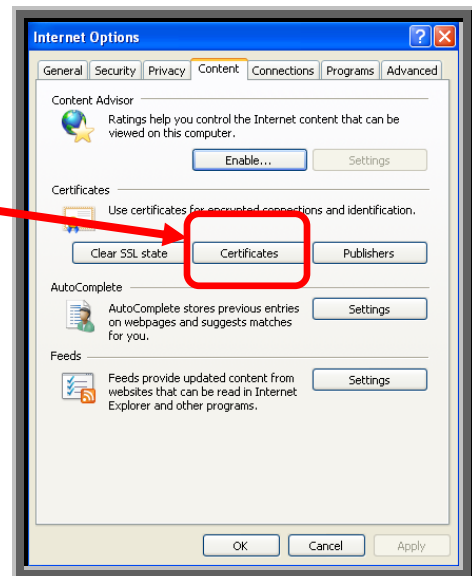
Select the **Tools** menu option. From the drop-down list, select **Internet Options**.



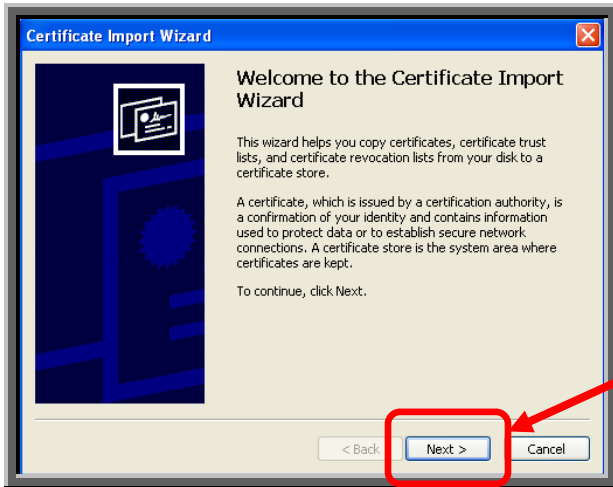
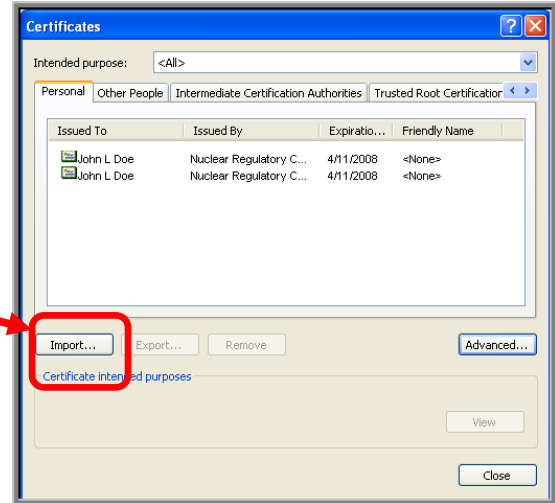
Select the **Content** tab.



Select the **Certificates** button.



Select the **Import...** button.

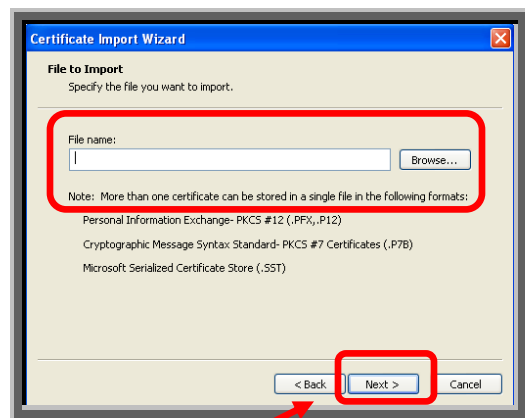


A *Certificate Import Wizard* dialogue box will appear. Select the **Next >** button.



Enter the directory where the certificate is stored **or** select the **Browse...** button to navigate to the file path location of the certificate.

Note: If browsing to locate the certificate, within the **Files of Type** field (at the bottom of the *Open* dialogue box), using the drop-down menu, you must select "**Personal Information Exchange (*.pfx)**" in order to see the certificate file you are looking for.

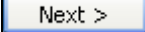


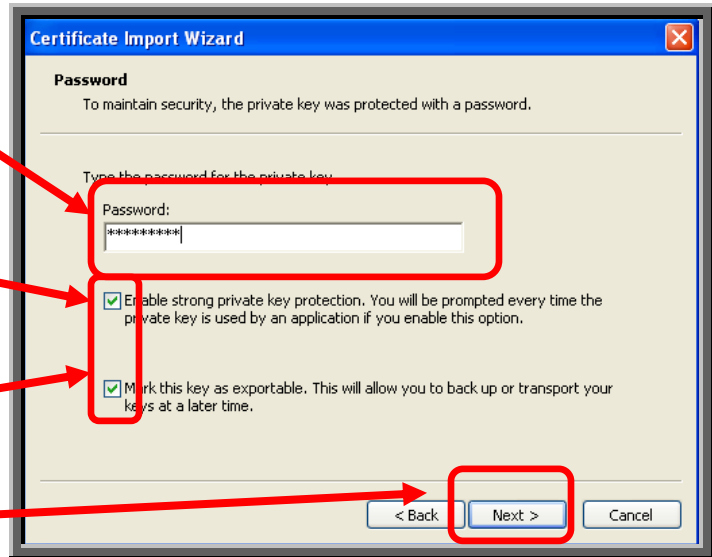
After the **File name:** field is populated, select the **Next >** button.

Enter the export/import password created during the certificate export process.

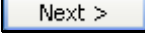
Check (☑) the "Enable strong private key protection" option.

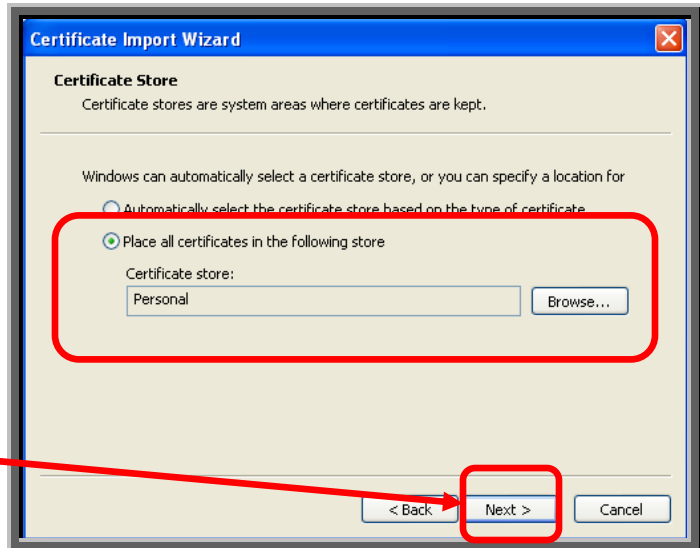
Check (☑) the "Mark the private key as exportable" option.


Select the  button.

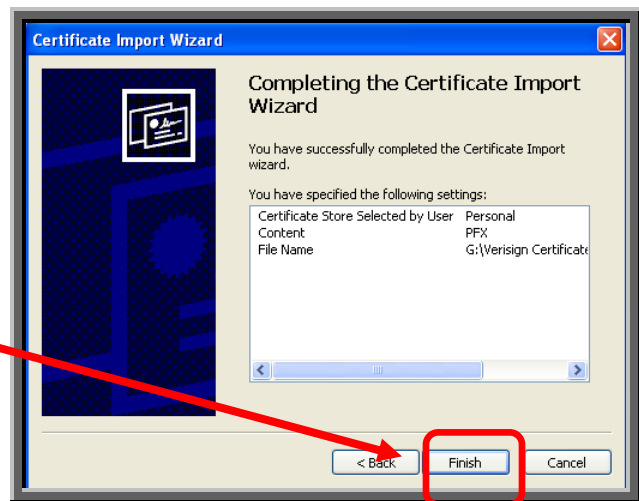


Make sure the radio button is selected (☉) for "Place all certificates into the following store" with the Certificate Store: field populated with "Personal".

Select the  button.



The *Completing the Certificate Import Wizard* dialogue box will appear. To exit, select the  button.



The Security Level must be set to High.
Select the **Set Security Level...** button.



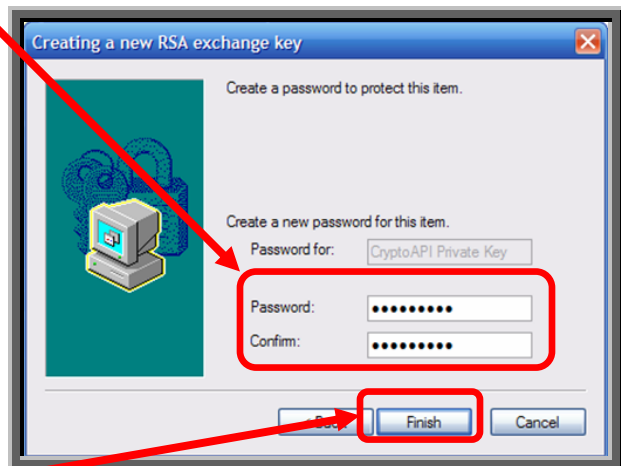
Select the **“High”** (High) radio button. This will activate password protection for your digital ID certificate.

Select the **Next >** button to continue.



Enter the **new password twice**.

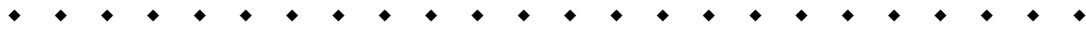
Note: *Commit to memory* this password as it will be necessary to periodically enter this password every time you use it, during the life of the certificate. If a certificate password is forgotten, it cannot be reset. A new certificate must be requested.



Select the **Finish** button.

The Security level reveals it is now set to High.

Select

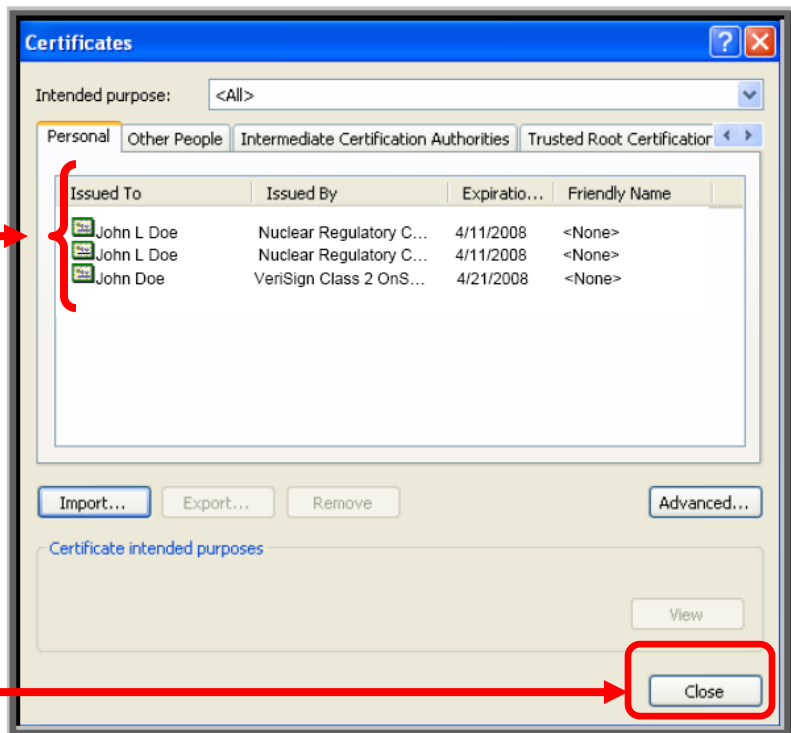


The message will appear that the import was successful. Select the button.



The newly imported certificate will be displayed within the Personal tab.

To complete the importing process, select the button.



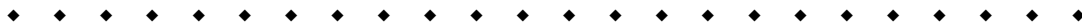
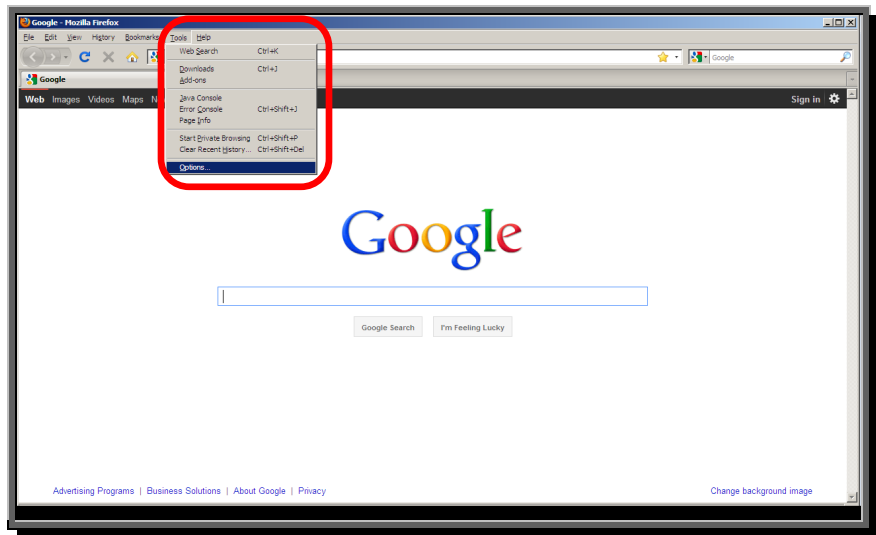
7.1 Mozilla Firefox Users Only


The following Certificate Import instructions are to aid users of Mozilla Firefox as their Web Browser:

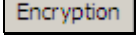
Open Mozilla Firefox.

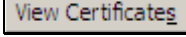
Select: **Tools**.

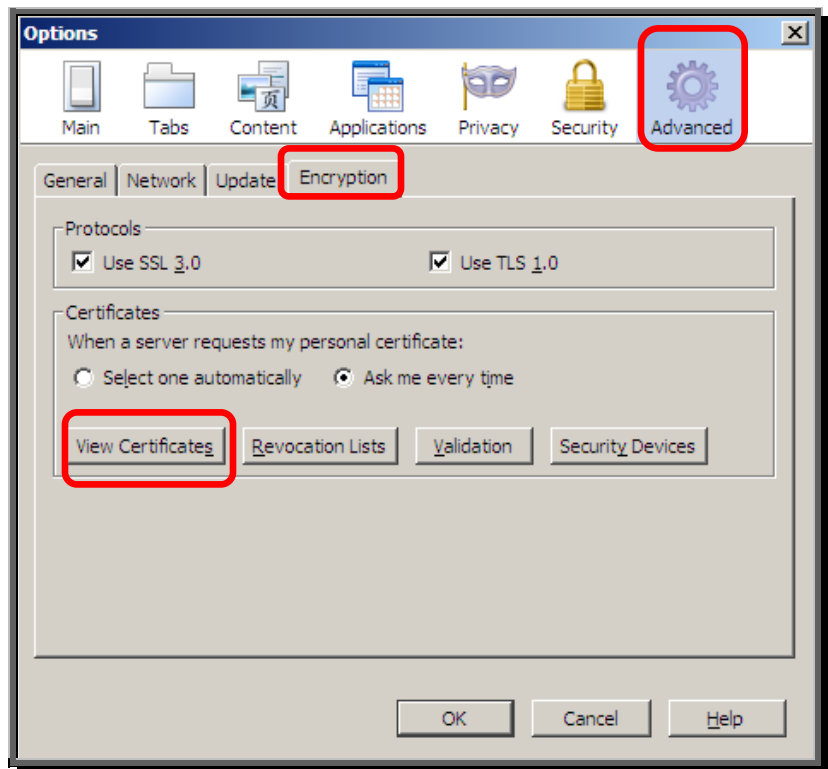
Scroll down and select: **Options**.



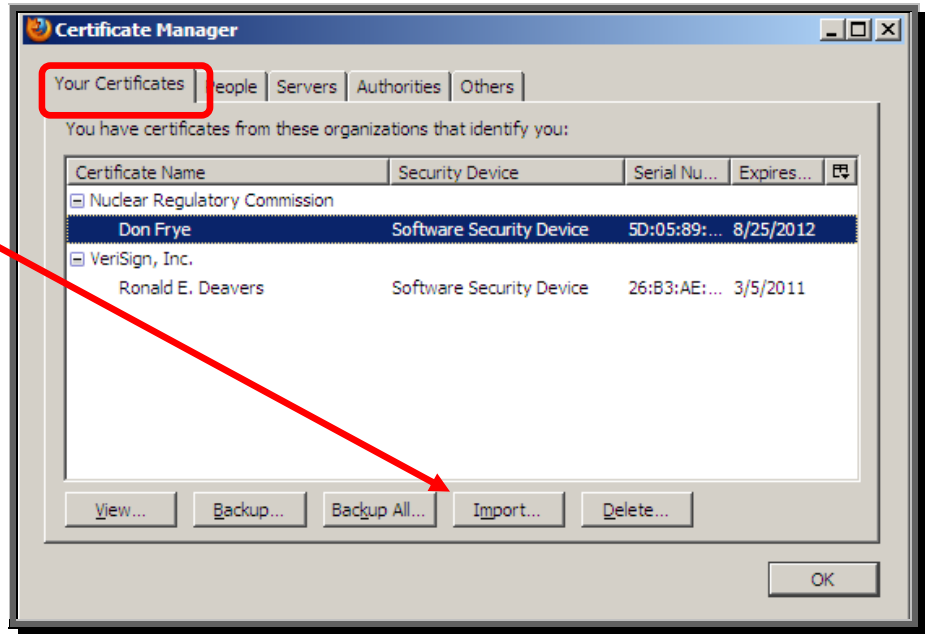
Select the  icon.

Select the  tab.

Select the  button.



From "Your Certificates" tab, select the **Import...** button.

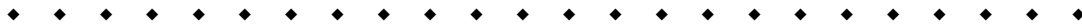
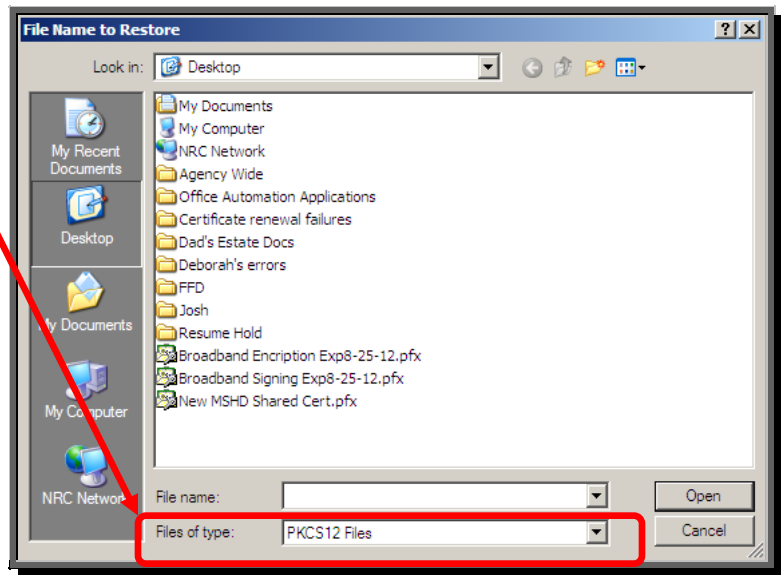
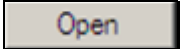


Verify the File type is at the default of PKCS12 Files.

This will ensure the correct certificate file

Navigate to the Certificate you want to Import.

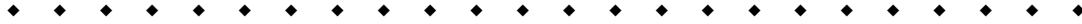
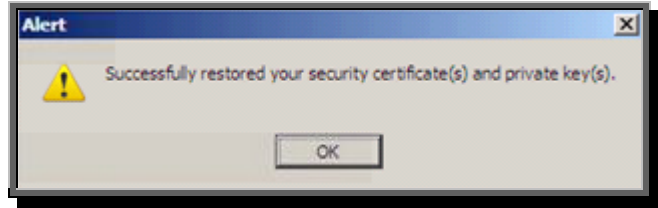
Select the certificate file you want to import, then select



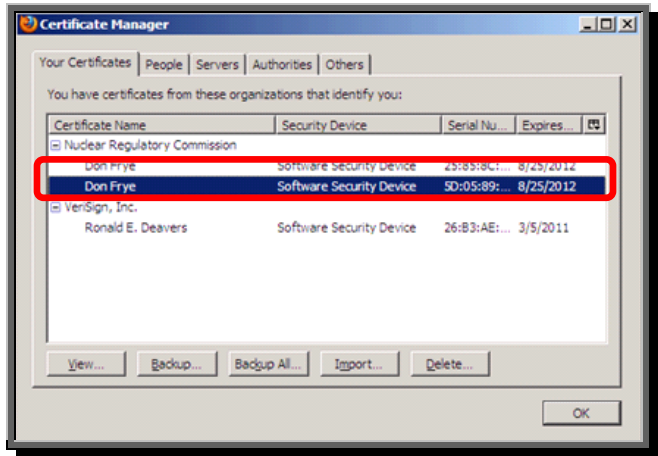
Enter the certificate password, then select



At the confirmation dialogue box, select **OK**.

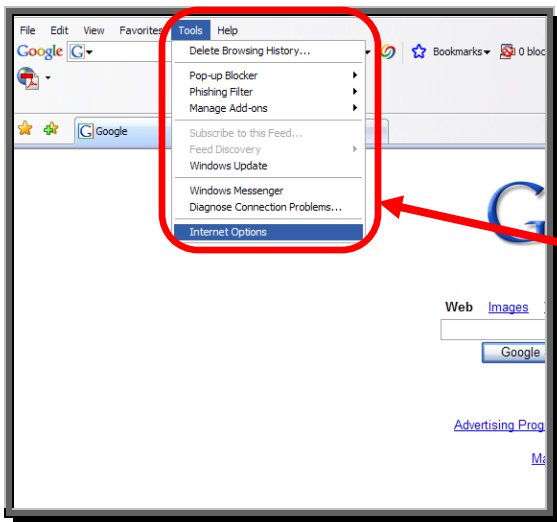


Verify the newly installed certificate is listed.



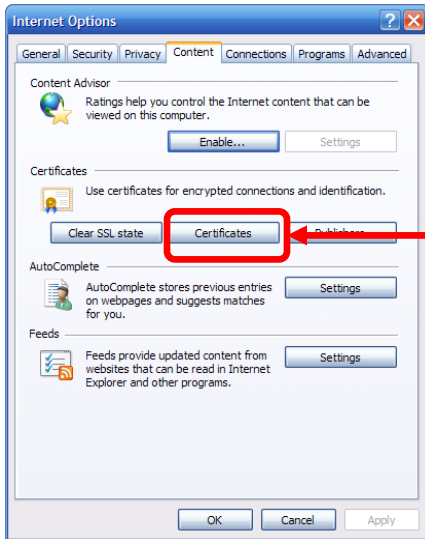
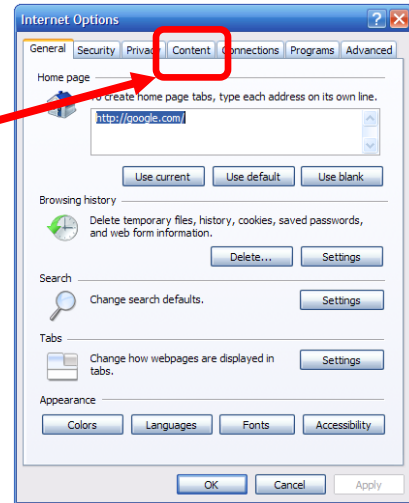
8. Digital ID Certificate Viewing Steps

Your VeriSign digital ID certificate is installed into your browser. The following steps reflect viewing via the Explorer browser Version 6.0. On your PC the steps may be somewhat different depending upon your browser, browser version, browser setting, operating system and operating system settings.



Open Internet Explore and click on the **Tools** tab. From the drop-down menu select **Internet Options**.

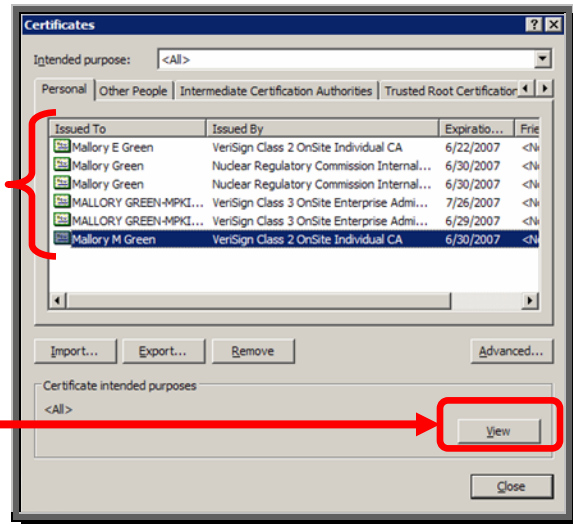
Select the **Content** tab in the Internet Options window.



Click on the **Certificates** button.

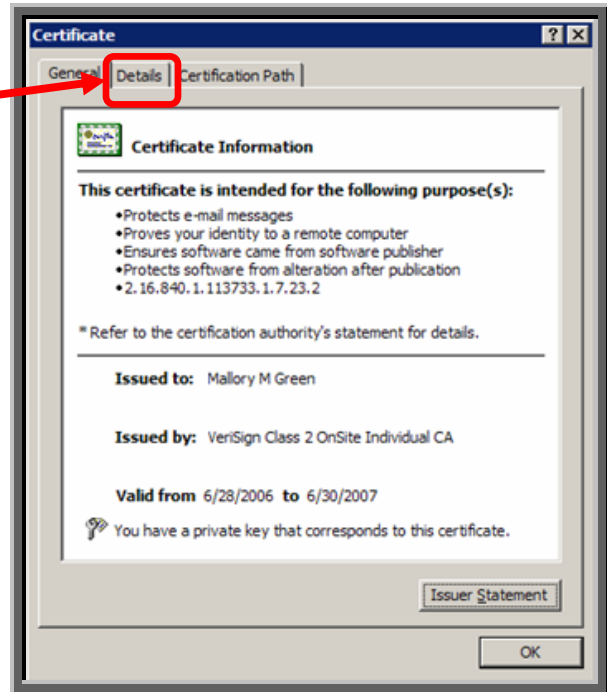


Choose a certificate to view by clicking on the desired certificate.

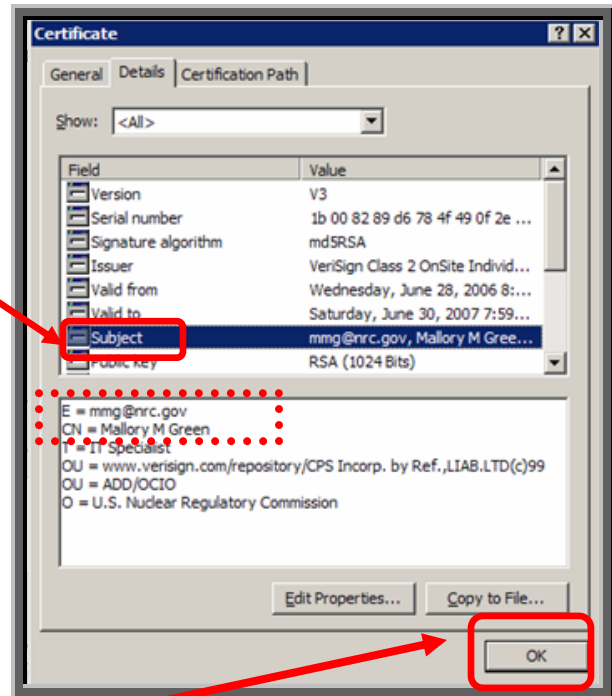


Click on the **View** button to see information about the selected certificate.

Click on the **Details** tab.



Click on the **Subject** field to see your data.



Notice that your email address is saved after E = and your name is saved after CN = in the certificates "Subject" field.

Click on the **OK** button.

9. Digital ID Certificate Renewal

The NRC issues digital ID certificates from VeriSign with a one year term. A certificate holder should receive an email message from the NRC two weeks before and then again one week before the digital ID certificate is scheduled to expire. Effective October 9, 2009 certificate holders will need to enroll for new certificates when their current certificates expire. Certificates issued prior to October 9, 2009 will no longer be renewable. These email messages will instruct the certificate holder to enroll for a new certificate and will include a link to a web address.

To enroll in a new certificate, follow the instructions provided in [Digital ID Certificate Enrollment Steps](#).

10. Digital ID Certificate Revocations

Note: To revoke certificates issued *prior to October 9, 2009*, contact the Meta-System Help Desk (toll free) at 866-672-7640 between 8:00 am to 8:00 pm EST, Monday through Friday (excluding Government holidays).

The certificate owner must remember and use the Challenge Phrase (the one-word password). The steps to revoke your digital ID certificate are:

Click on the “NRC’s Digital ID Center” link from either the “Electronic Submittals” web page (<http://www.nrc.gov/site-help/e-submittals.html>) or the “Obtain a Digital ID Certificate” web page (<http://www.nrc.gov/site-help/e-submittals/apply-certificates.html>).

Select the

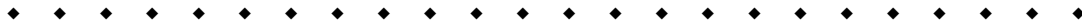
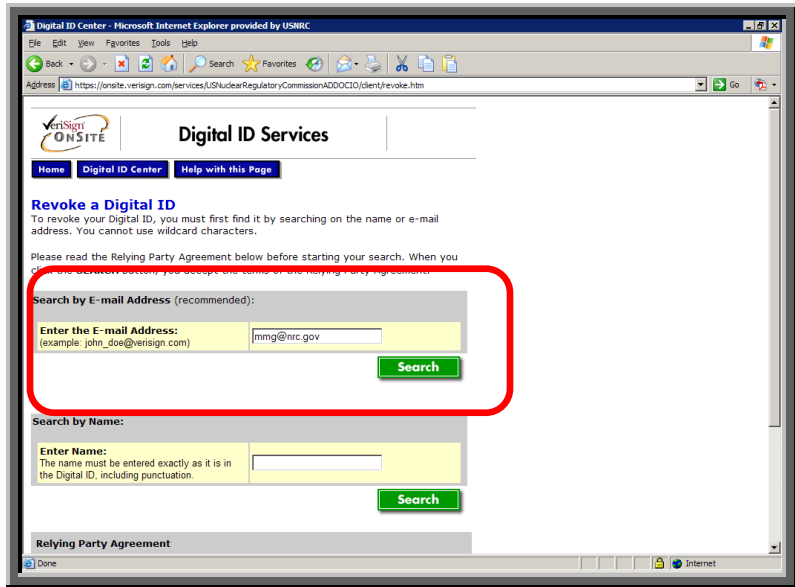
REVOKE

The screenshot shows the VeriSign Digital ID Center interface. At the top, there is a logo for VeriSign ONSITE and the text 'Digital ID Center'. Below the logo are 'Home' and 'Help' buttons. The main heading is 'U.S. Nuclear Regulatory Commission ADD/OCIO Digital ID Center'. There are five main options listed, each with an icon and a description:

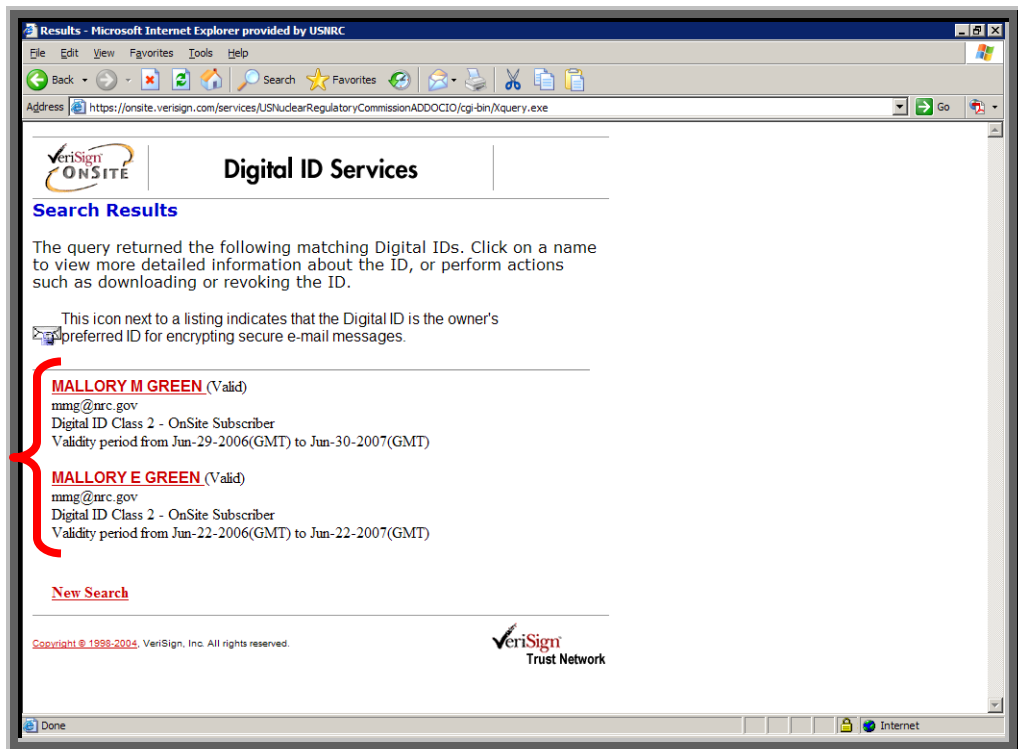
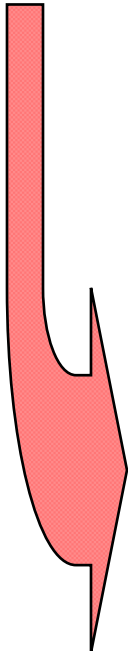
- ENROLL**: Choose this option to enroll for a client Digital ID.
- PICK UP ID**: Choose this option if you enrolled for a Digital ID but did not pick it up.
- SEARCH**: Choose this option to search for a Digital ID. This function is useful for determining whether a Digital ID is valid, expired, or revoked. You may also download IDs from this option.
- RENEW**: Choose this option to renew a Digital ID which is expiring or which has already expired. You should generally start renewing your Digital ID at least one month before your Digital ID is due to expire.
- REVOKE**: Choose this option to revoke your Digital ID. Digital IDs should be revoked immediately for any suspected compromise, including lost or stolen private keys, corrupted key pairs, change in site ownership, or suspected fraud.

The 'REVOKE' option is highlighted with a red box. At the bottom of the page, there is a copyright notice: 'Copyright © 1999-2004, VeriSign, Inc. All rights reserved.' and the VeriSign TRUST NETWORK logo.

Enter an appropriate email address or name to search for the certificate you want to revoke and press the  button.

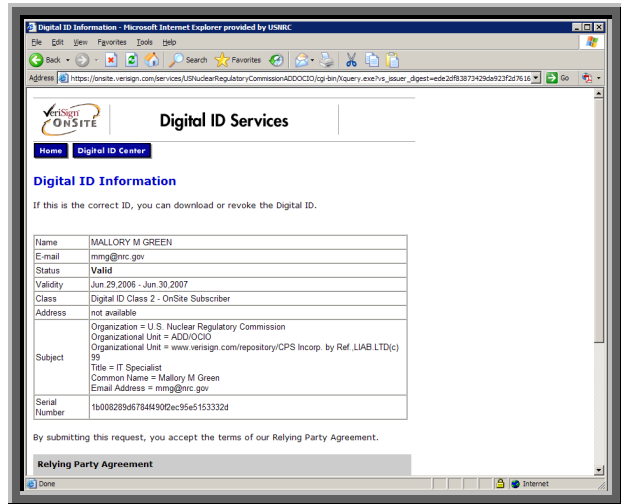


Select the applicable certificate you want to revoke.

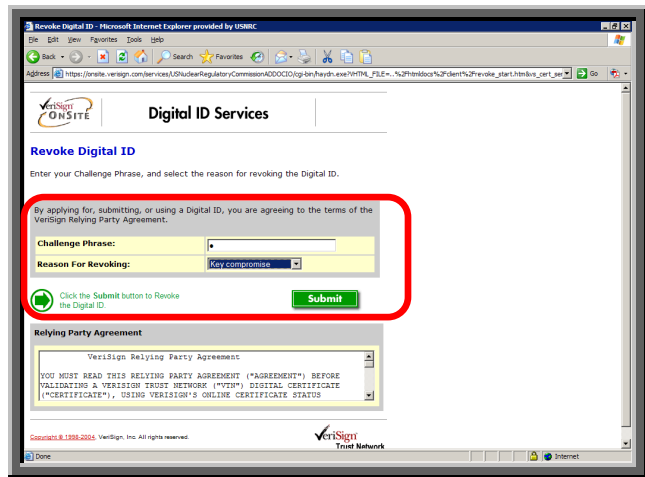


Review the data for the certificate you have chosen to revoke.

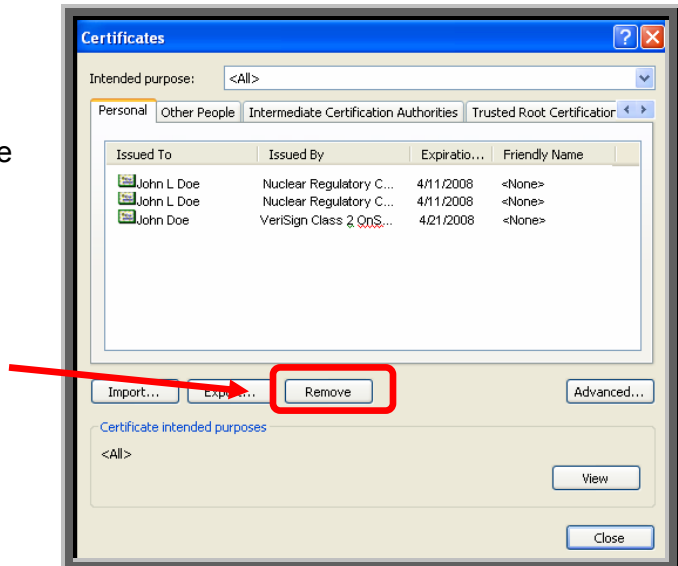
Scroll down and click on the **Revoke** button to invalidate your certificate via VeriSign.



Enter the Challenge Phrase you entered during enrollment for this digital ID certificate and then select



The steps listed in this section made your certificate invalid, however, it did not remove the certificate from your PC, therefore follow the steps within the [Digital ID Certificate Viewing Steps](#) Instructions. After locating and selecting the certificate, to remove it from your PC, select



11. Troubleshooting

11.1 Immediate Assistance

For immediate assistance, contact the NRC's Meta System Help Desk, which is available to support stakeholders (including members of the public) who submit documents electronically to the NRC and access documents through Electronic Information Exchange and the Electronic Hearing Docket.

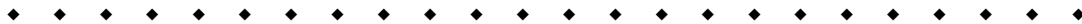
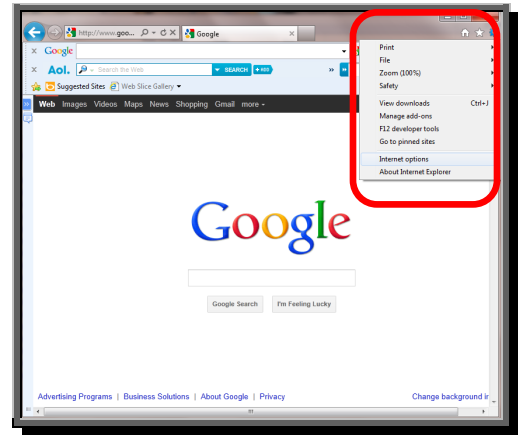
You can reach the Help Desk by telephone (toll free) at 1-866-672-7640. The Help Desk's hours of operation will be 8:00 am to 8:00 pm EST, Monday through Friday (excluding Government holidays).

11.2 Trusted Sites

Open your Web Browser.

Select **Tools**.

Scroll down and select **Internet Options**.

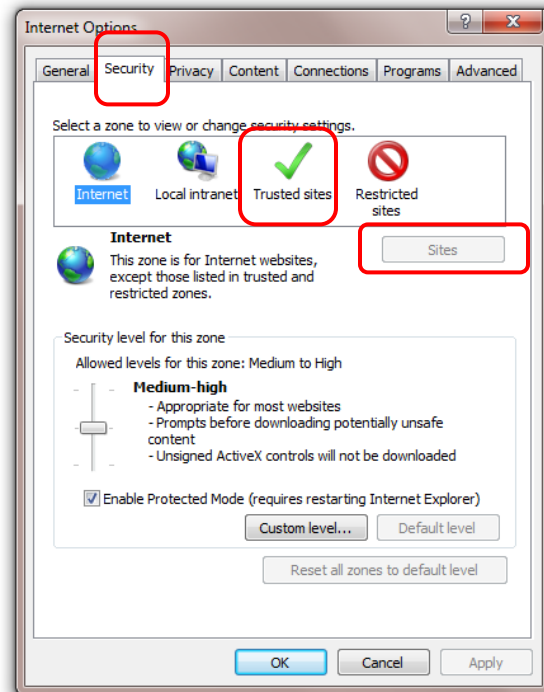


Select the **Security** Tab.




Select: **Trusted sites**

Then select:

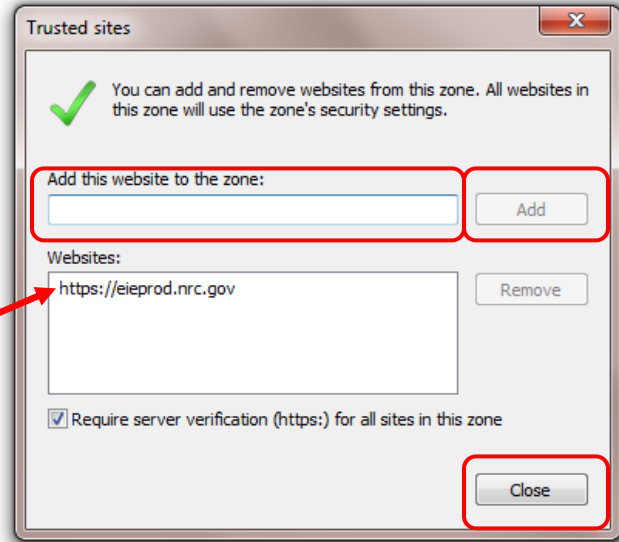


<https://eieprod.nrc.gov> MUST be displayed within the **Websites:** field (as it appears in the screen print to the right.)

If it does not, then enter it into the **Add this website to the zone:** field.

Select  (the website address will now be listed, as it appears in the screen print to the right.)

Then select: .



At the *Internet Options* dialogue box, select: .

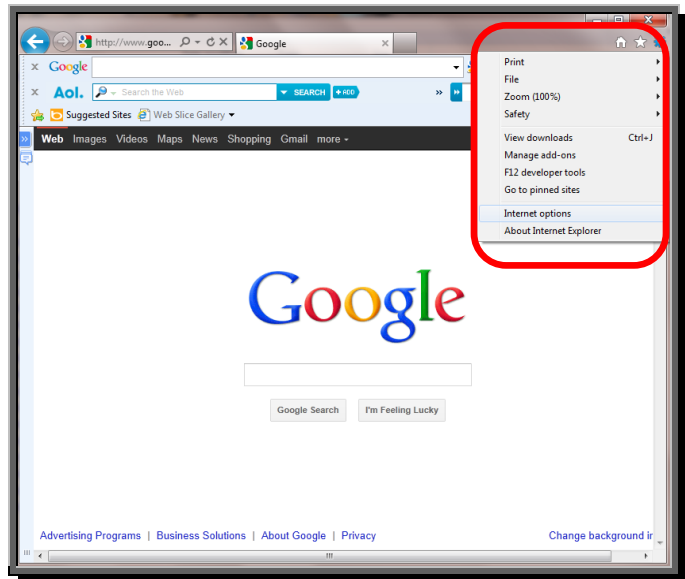
11.3 Enabling ActiveX Controls and Plug-ins

Note: You may need to contact your IT department for permission to conduct the following actions.

Open your Web Browser.

Select **Tools**.

Scroll down and select **Internet Options**.

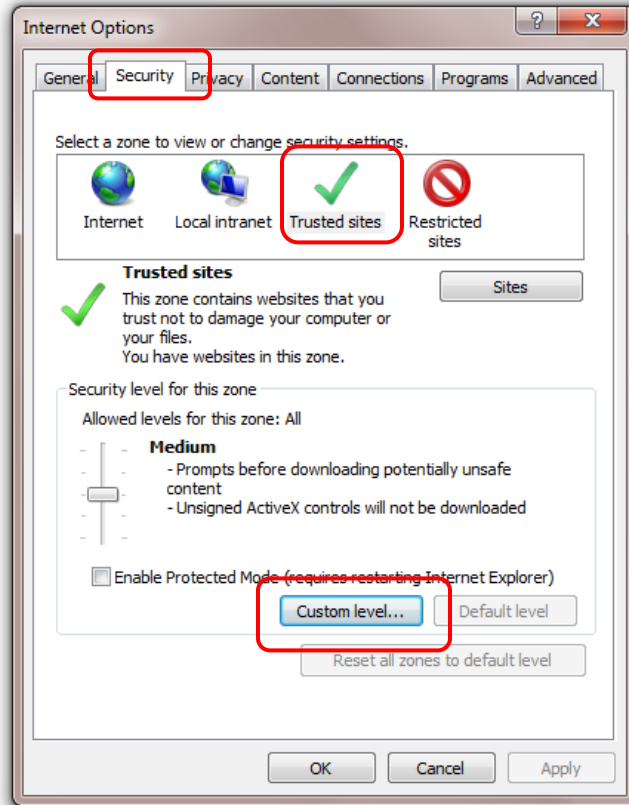
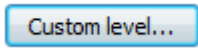


Select the **Security** Tab.



Select: **Trusted sites**

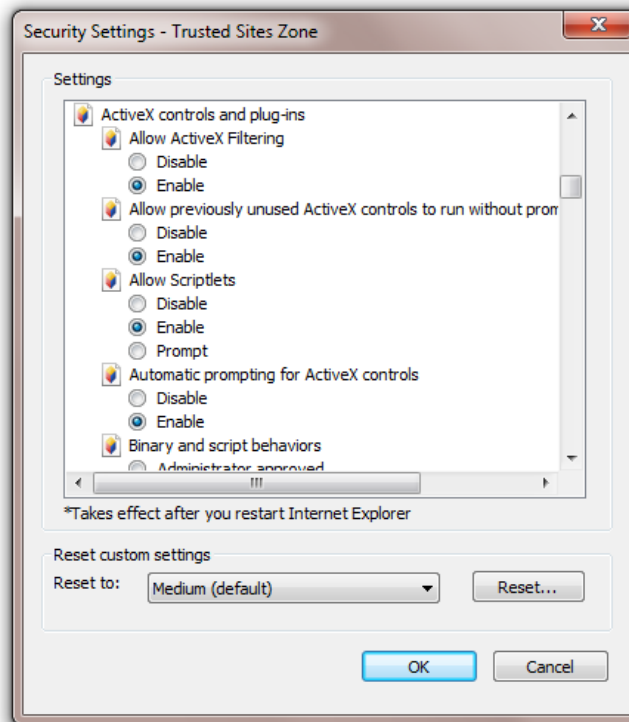
Then select:



Scroll down and locate:
ActiveX controls and plug-ins

Enable the following:

- Allow ActiveX Filtering
- Allow previously unused ActiveX controls to run without prompt
- Allow Scriptlets
- Automatic prompting for ActiveX controls

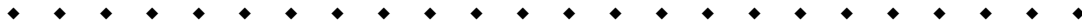
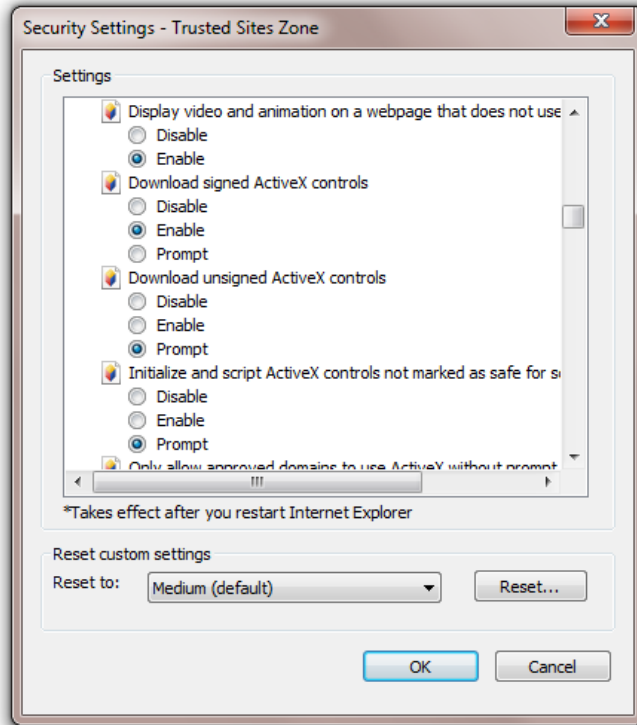


Enable the following:

- Display video and animation on a webpage that does not use external media player
- Download signed ActiveX controls

Prompt the following:

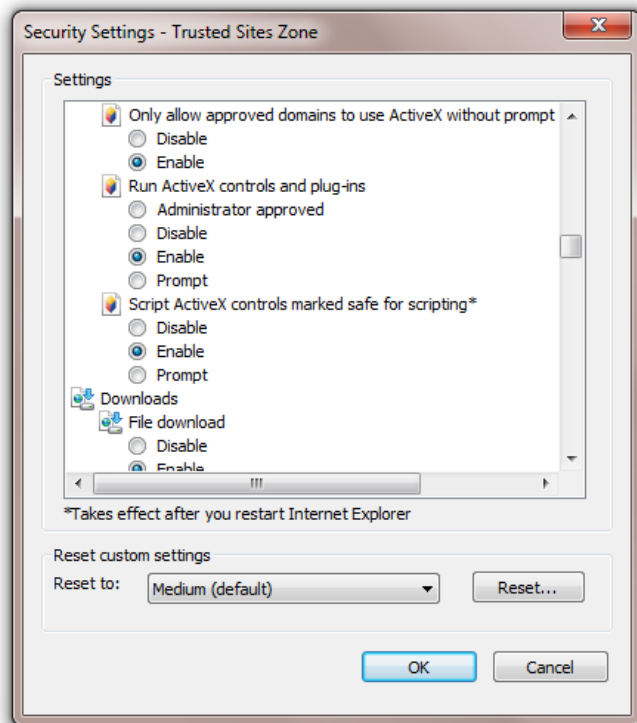
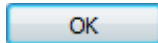
- Download unsigned ActiveX controls
- Initialize and script ActiveX controls not marked as safe for scripting



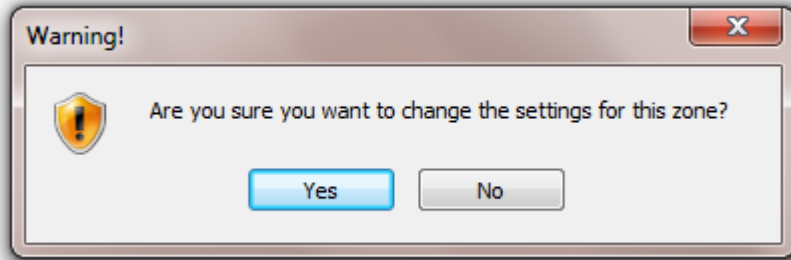
Enable the following:

- Only allow approved domains to use ActiveX without prompt
- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting

Select:



Select to change the settings.



At the *Internet Options* dialogue box, select: .

11.4 Apple Macintosh Users

Apple Macintosh computer (Mac) is not supported therefore, if you are experiencing issues, please refer to [Section 11.1](#) for Immediate Assistance.