

# **CWOPA Broadband Users**

---

## **Windows Operating System**

**October 2012**

### **Background**

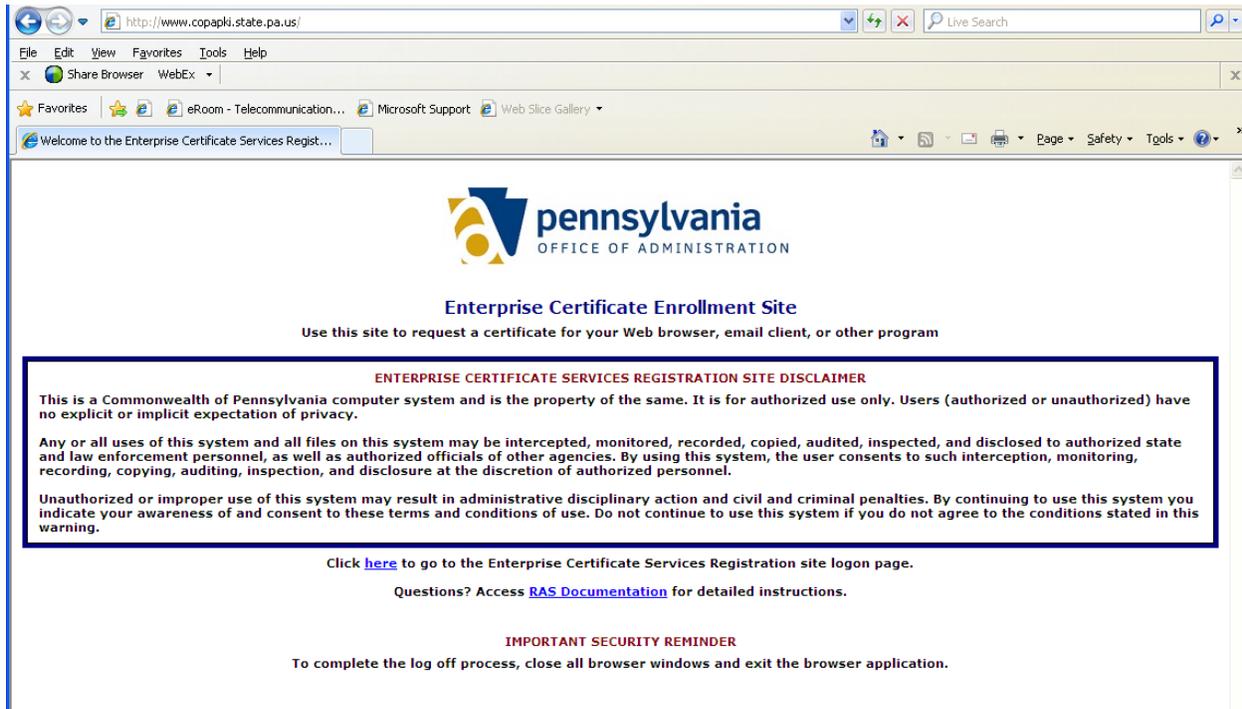
These instructions are to be used for VPN users who have been assigned a CWOPA username and password. If your machine has Internet Explorer 8 or above, begin with Section I. For versions of Internet Explorer 7 or below, start with Section II.

# Table of Contents

Section I - Internet Explorer 8 / 9 – Certificate Installation .....	2
Section II - Personal Certificate Download and Installation .....	14
Section III - Installation and Configuration of Juniper Network Connect.....	21
Section IV - Connect with Juniper Connect.....	28
Section V - Disconnect with Juniper Connect.....	32
Section VI – Technical Support.....	33

## Section I - Internet Explorer 8 / 9 – Certificate Installation

1. Open Internet Explorer, go to <https://www.icopapki.state.pa.us>
2. Click on [here](#).



The screenshot shows an Internet Explorer browser window with the address bar displaying <http://www.copapki.state.pa.us/>. The browser interface includes a menu bar (File, Edit, View, Favorites, Tools, Help), a toolbar with icons for back, forward, stop, and refresh, and a search bar labeled "Live Search". The page content displays the logo for the Pennsylvania Office of Administration, followed by the heading "Enterprise Certificate Enrollment Site" and the instruction "Use this site to request a certificate for your Web browser, email client, or other program". A prominent blue-bordered box contains the following text:

**ENTERPRISE CERTIFICATE SERVICES REGISTRATION SITE DISCLAIMER**

This is a Commonwealth of Pennsylvania computer system and is the property of the same. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized state and law enforcement personnel, as well as authorized officials of other agencies. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized personnel.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. Do not continue to use this system if you do not agree to the conditions stated in this warning.

Click [here](#) to go to the Enterprise Certificate Services Registration site logon page.

Questions? Access [RAS Documentation](#) for detailed instructions.

**IMPORTANT SECURITY REMINDER**

To complete the log off process, close all browser windows and exit the browser application.

3. Log on with the **CWOPA username** and **password** you were assigned. In the **User name:** field, be sure to precede your username with: **CWOPA\** (example: **cwopa\jsmith**)



4. Click on [Download a CA certificate, certificate chain, or CRL](#)



#### Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

#### Select a task:

[Request a certificate](#)

[Save and install the Cisco VPN Client \(Installation will restart your computer.\)](#)

[Download a CA certificate, certificate chain, or CRL](#)

5. If the Operating System on your machine is:  
**Windows XP:** Proceed to [Section A](#)  
**Windows 7:** Proceed to [Section B](#)

## Section A – XP Instructions

1. Click on [install this CA certificate chain](#)
2. Click on **Yes** button if prompted for Web site add.

Microsoft Active Directory Certificate Services – CoPA Enterprise Issuing Internal CA Home

---

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate chain](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [CoPA Enterprise Issuing Internal CA (4)]

Previous [CoPA Enterprise Issuing Internal CA (4)]

Encoding method:

DER

Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

**Potential Scripting Violation**

 This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.

Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.

3. Once you see the below screen you have successfully installed the I.E. 8/9 certificate.

Microsoft Active Directory Certificate Services – CoPA Enterprise Issuing Internal CA Home

---

**CA Certificate Installation**

The CA certificate chain has been successfully installed.

Proceed to [Section II - Personal Certificate Download and Installation](#)

## Section B – Windows 7 Instructions

### 1. Click on [Download CA certificate chain](#)

Microsoft Active Directory Certificate Services – CoPA Enterprise Issuing Internal CA Home

---

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate chain](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [CoPA Enterprise Issuing Internal CA(1)]

Previous [CoPA Enterprise Issuing Internal CA]

Encoding method:

DER

Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

---

### 2. Click **Open**

Microsoft Active Directory Certificate Services – CoPA Enterprise Issuing Internal CA Home

---

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate chain](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [CoPA Enterprise Issuing Internal CA(1)]

Previous [CoPA Enterprise Issuing Internal CA]

Encoding method:

DER

Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

0% of certnew.p7b from www.icopapki.state.pa.us ...

**File Download**

Do you want to open or save this file?

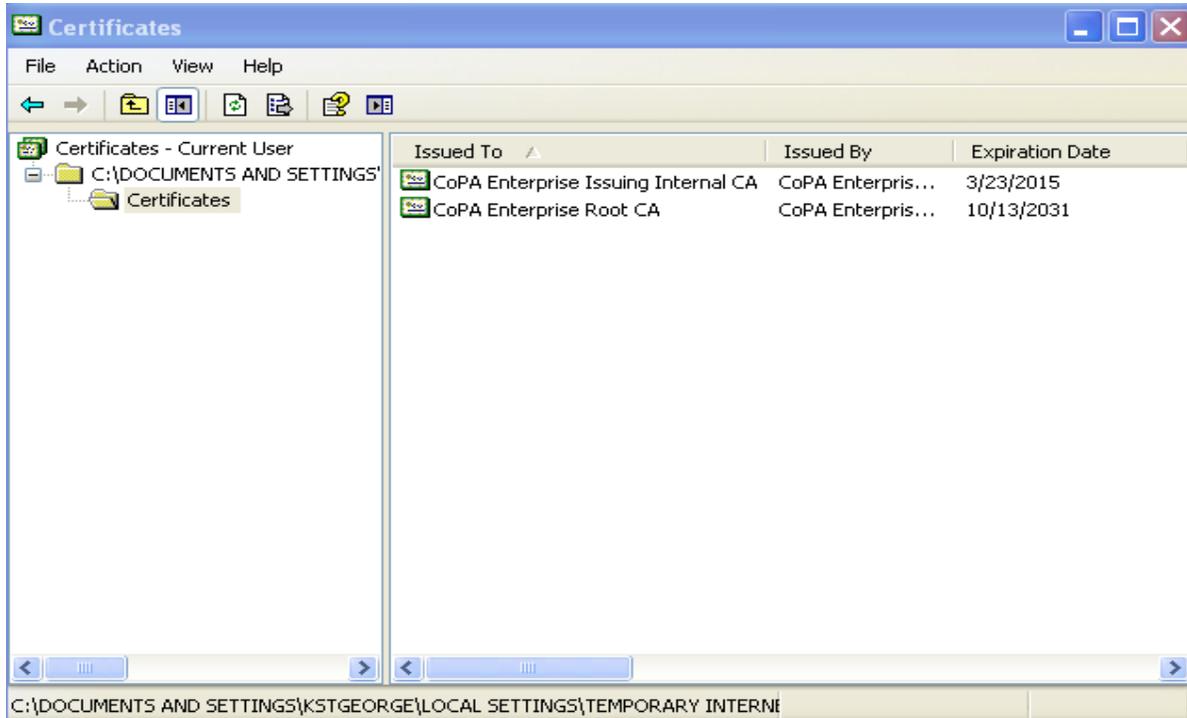
 Name: certnew.p7b  
Type: PKCS #7 Certificates, 2.00KB  
From: **www.icopapki.state.pa.us**

Always ask before opening this type of file

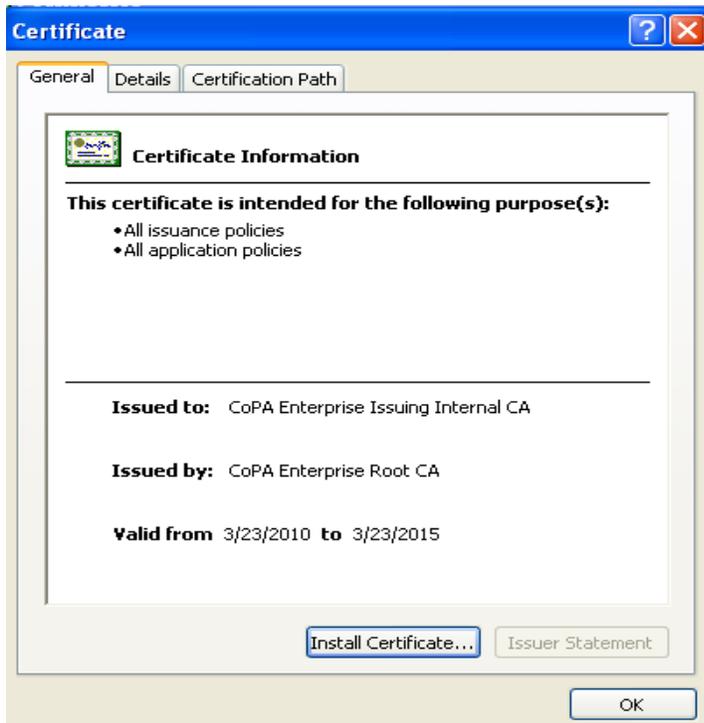
 While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. [What's the risk?](#)

---

3. The below box will pop up, **click on the + sign next to c:\documents and settings**  
Then click on **Certificates** folder, on the left side of the screen  
Next double click on **CoPA Enterprise Issuing Internal CA** on the right.



4. Click on **Install Certificate...**



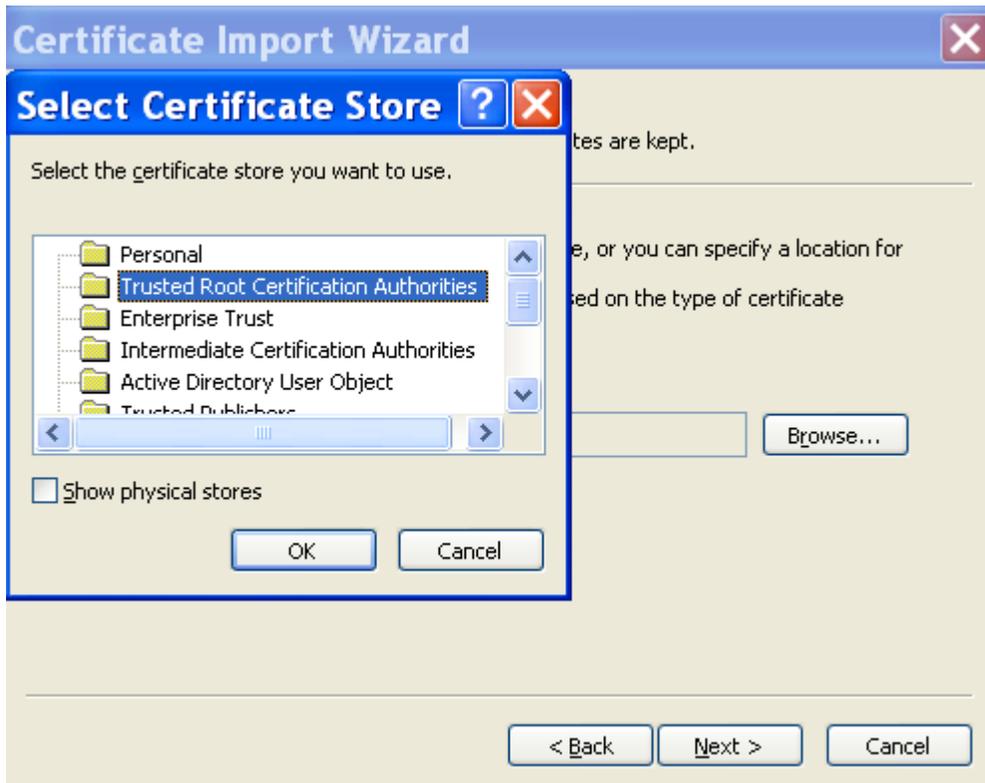
5. Click on **Next >**



6. Select **Place all certificates in the following store**  
Click the **Browse...** button.



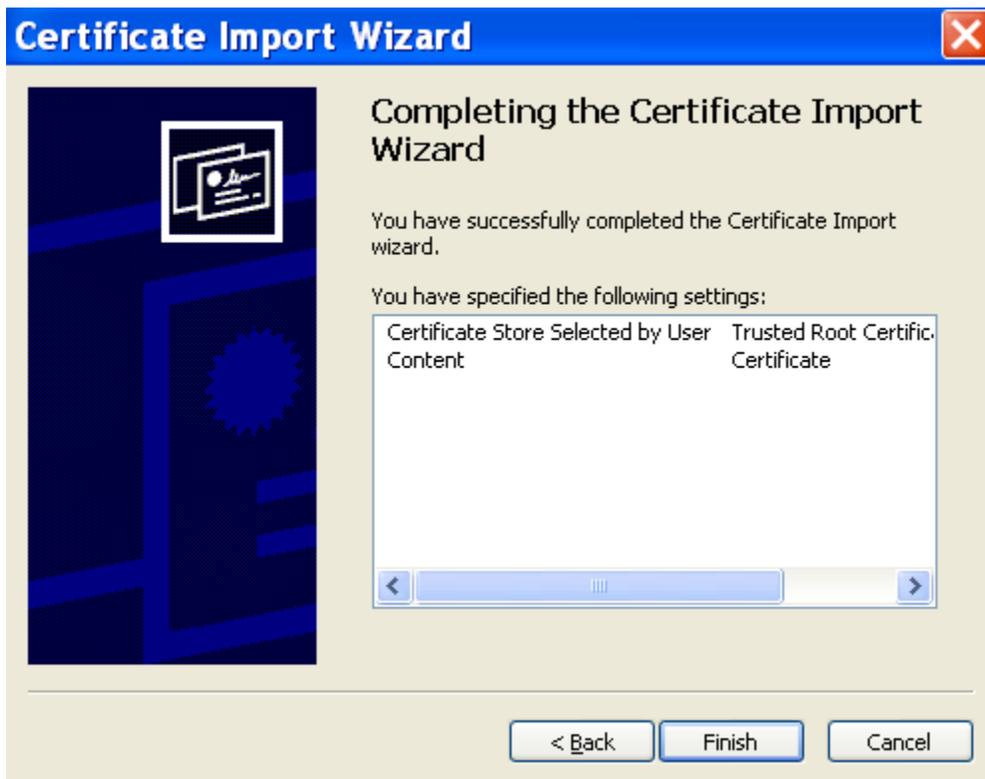
7. Select **Trusted Root Certification Authorities** and click on **OK**



8. Click on **Next >**



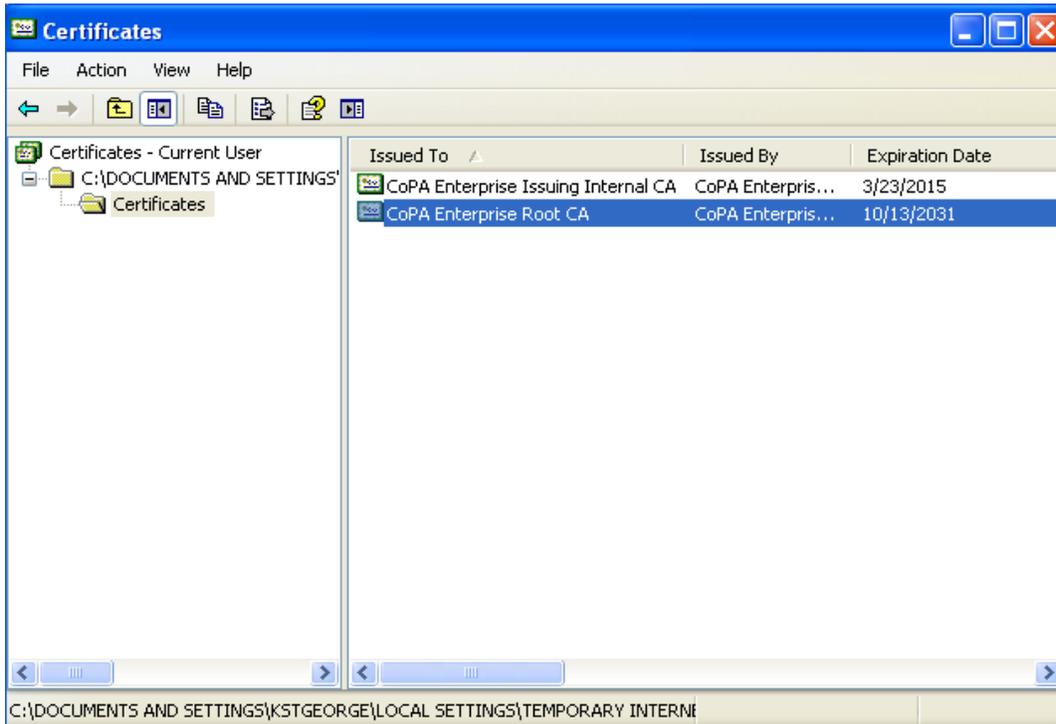
9. Click on **Finish**



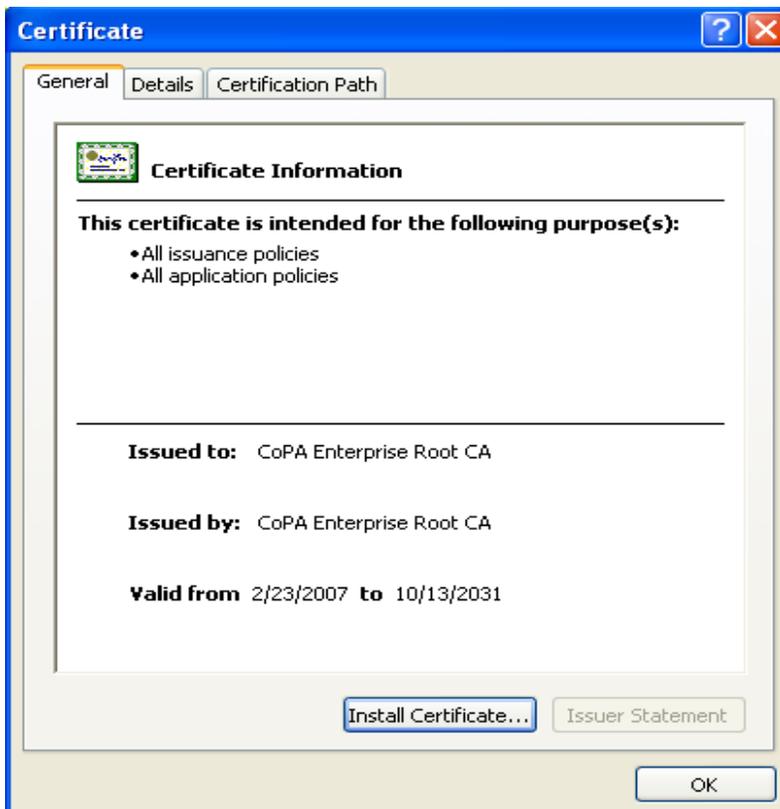
10. Click on **OK**



11. Next double click on **CoPA Enterprise Root CA**



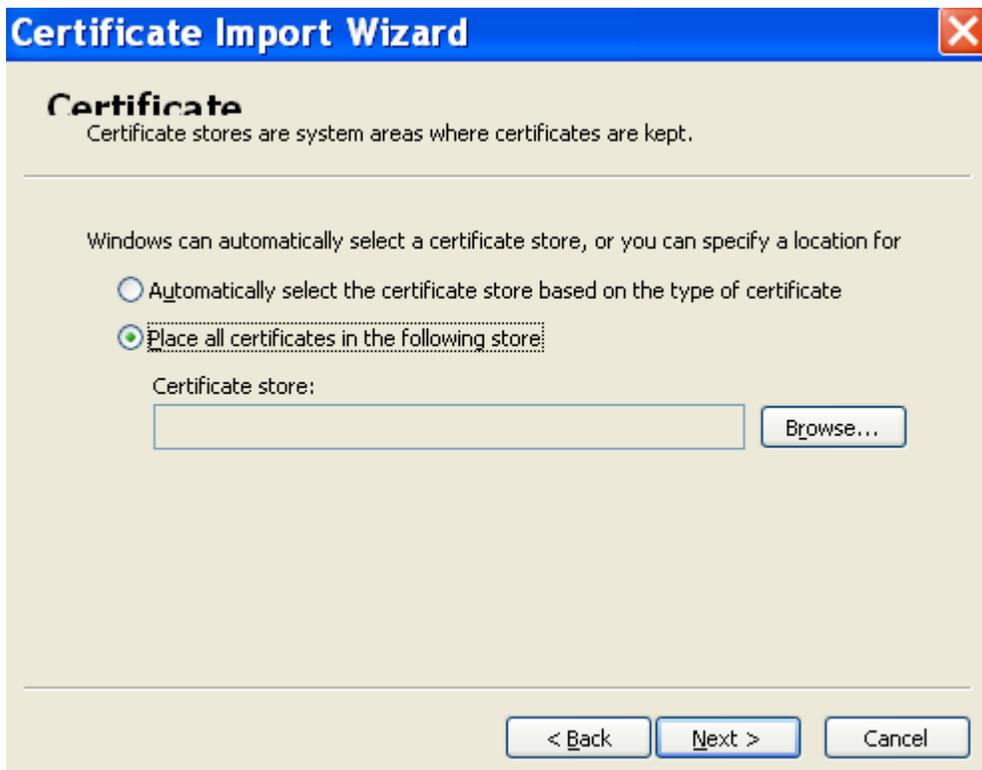
12. Click on **Install Certificate...**



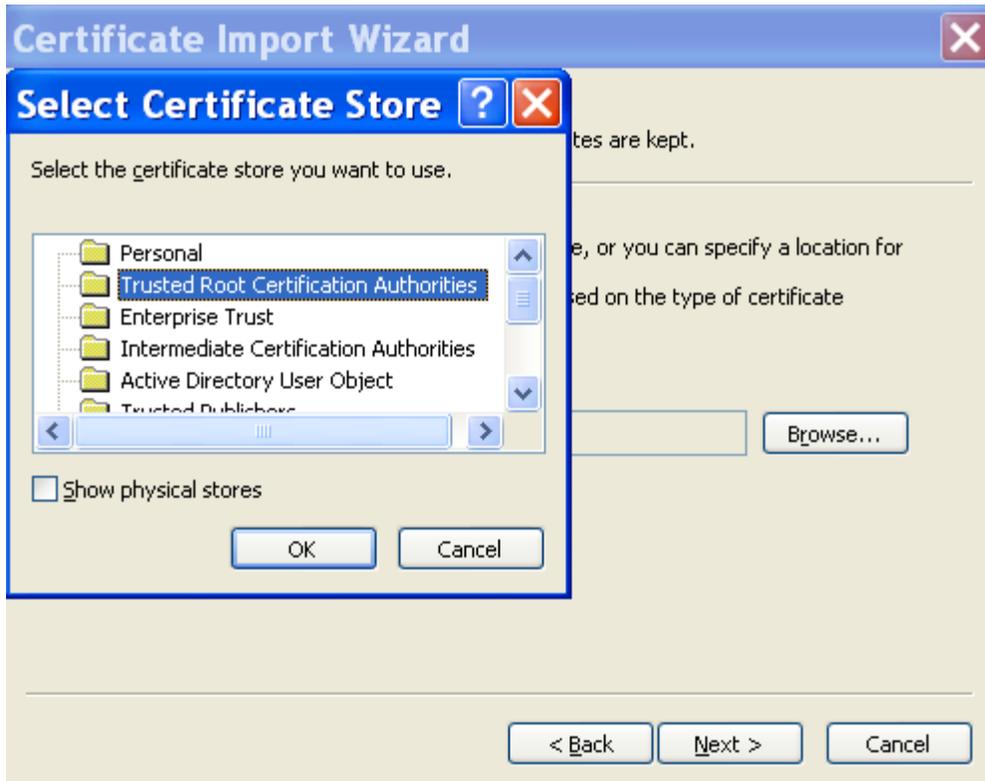
13. Click on **Next >**



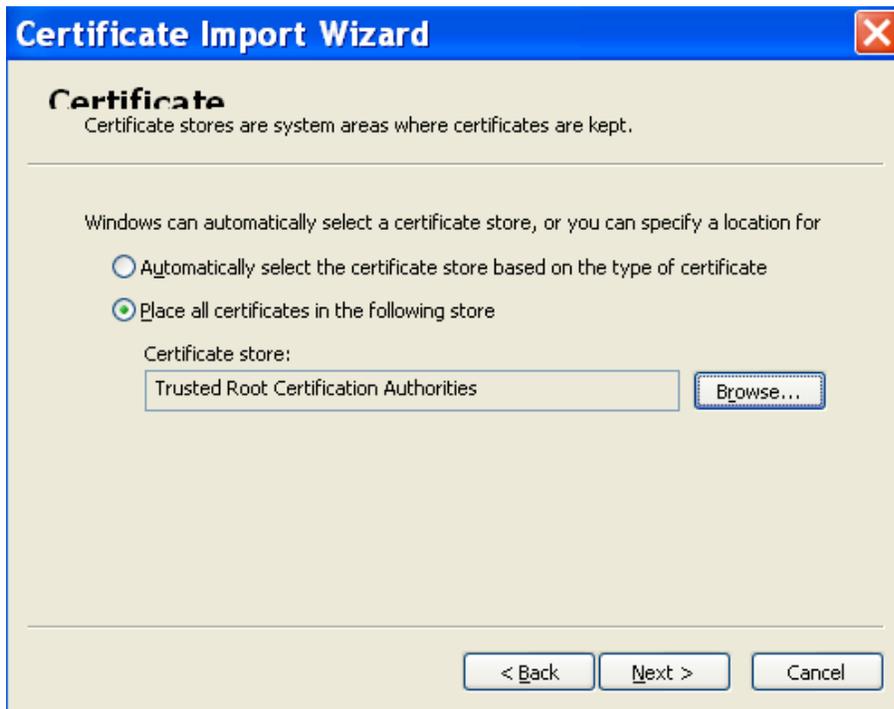
14. Select **Place all certificates in the following store**  
Click the **Browse...** button.



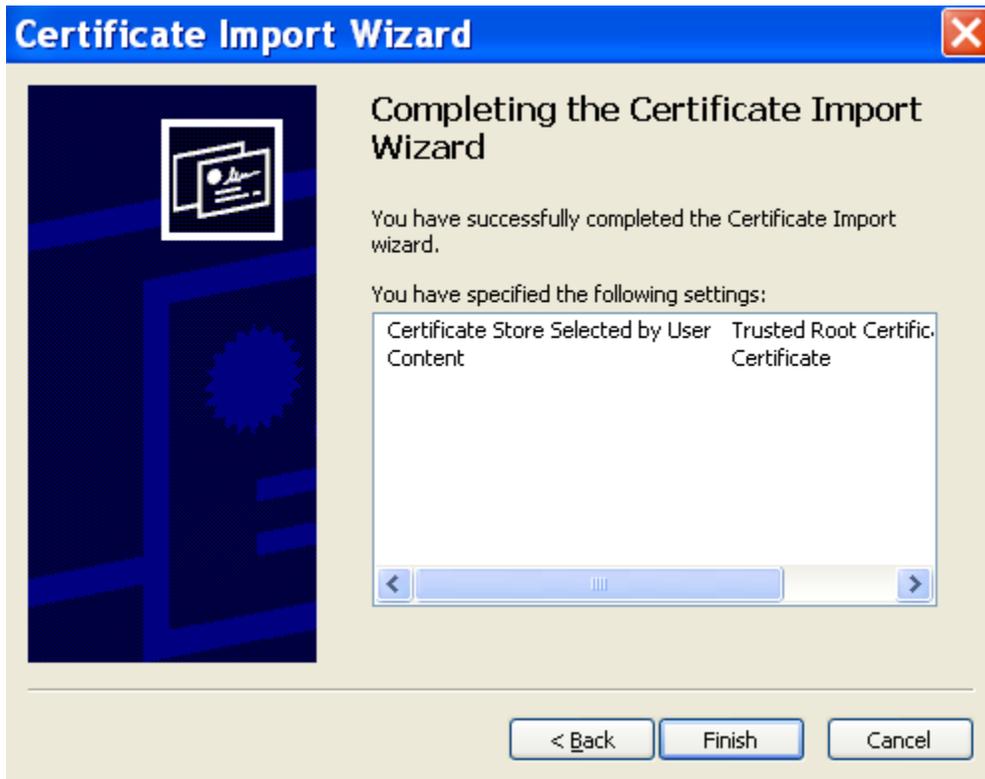
15. Select **Trusted Root Certification Authorities** and click on **OK**



16. Click on **Next >**



17. Click on **Finish**



18. Click on **OK**

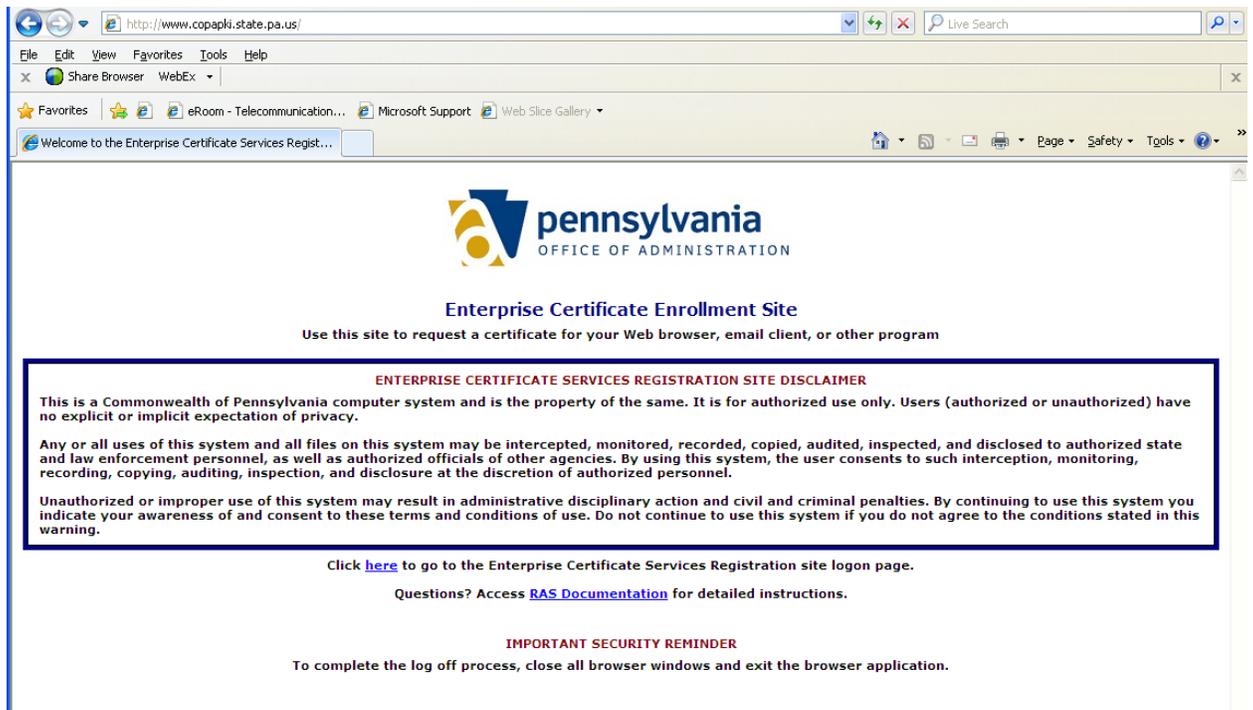


You have now completed the I.E. 8/9 Certificate installation.

Proceed to [Section II - Personal Certificate Download and Installation](#)

## Section II - Personal Certificate Download and Installation

1. Open Internet Explorer, go to <http://www.icopapki.state.pa.us>.  
**NOTE: This website can only be access if you are connected to the Commonwealth network.**
2. The *Enterprise Certificate Services Registration Site* screen is displayed.
3. Select “**Click here**” below the disclaimer box. This will allow you to request a certificate that will ensure RAS security.



4.

The screenshot shows the Internet Explorer browser window with the address bar displaying <http://www.icopapki.state.pa.us/>. The page content includes the Pennsylvania Office of Administration logo and the following text:

**Enterprise Certificate Enrollment Site**  
Use this site to request a certificate for your Web browser, email client, or other program

**ENTERPRISE CERTIFICATE SERVICES REGISTRATION SITE DISCLAIMER**  
This is a Commonwealth of Pennsylvania computer system and is the property of the same. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.  
Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized state and law enforcement personnel, as well as authorized officials of other agencies. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized personnel.  
Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. Do not continue to use this system if you do not agree to the conditions stated in this warning.

Click [here](#) to go to the Enterprise Certificate Services Registration site logon page.  
Questions? Access [RAS Documentation](#) for detailed instructions.

**IMPORTANT SECURITY REMINDER**  
To complete the log off process, close all browser windows and exit the browser application.

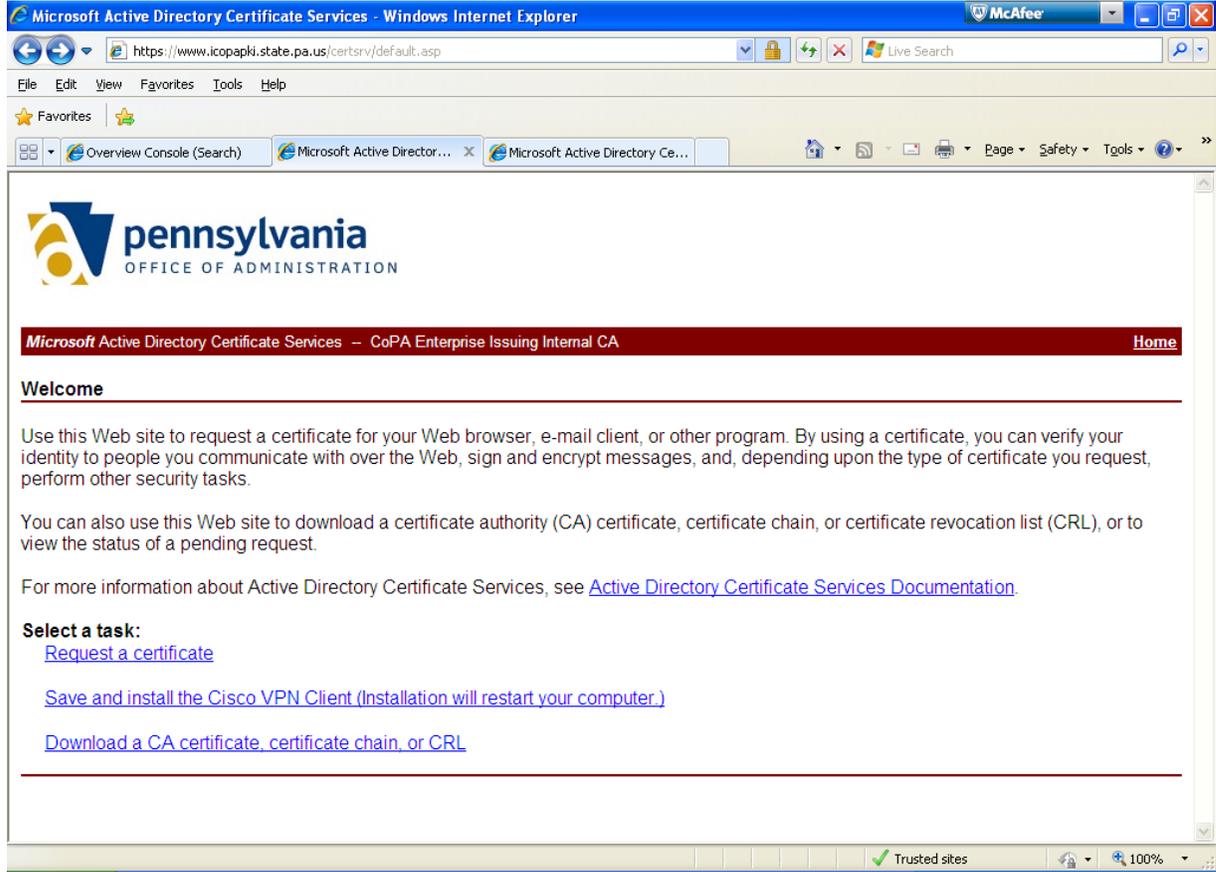
Click “**Yes**” if the *Security Alert* screen is displayed.



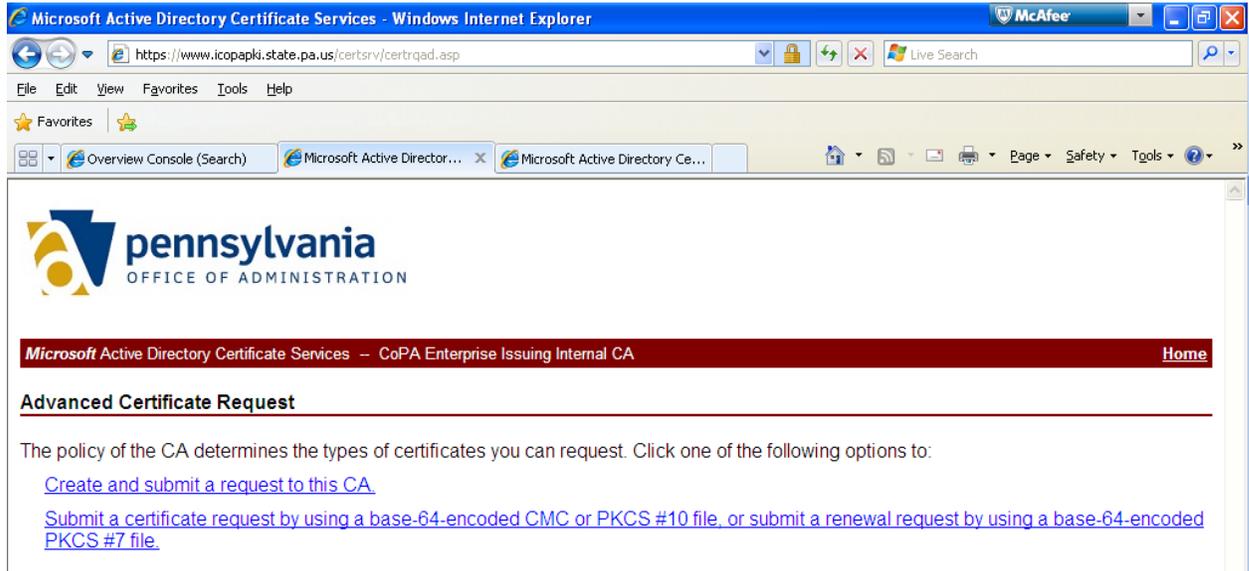
5. Enter your **CWOPA Username and Password** and then click “**OK**”.
  - a. The Username must be prefixed by **cwopa\**
  - b. Windows 2000 users **ONLY** will have the domain line displayed. Enter **CWOPA** in the domain box.



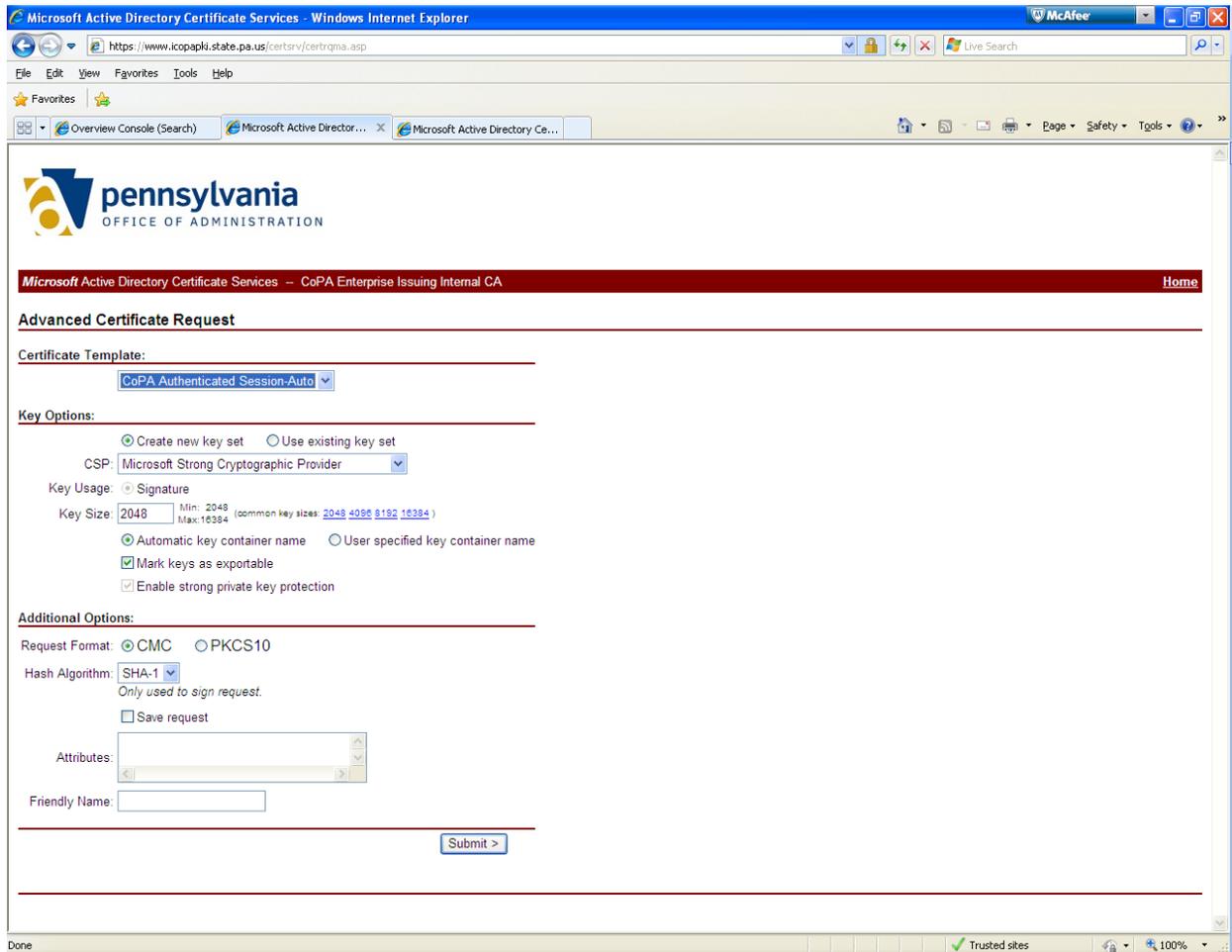
6. Select the [“Request a certificate”](#) link.



7. Select the [“Create and submit a request to this CA.”](#) link.



8. Select the following options on the *Advanced Certificate Request* screen:
  - a. In the “Certificate Template” drop-down select the template type
    - i. **“CoPA Authentication Session-Auto”**
    - ii. Select a different option if required.
  - b. In the “Key Options” drop-down make sure the following is displayed:
    - i. CSP: **“Microsoft Strong Cryptographic Provider”**
  - c. Select the **“Submit”** button to start generating the request.



9. Select **“Yes”** on the *Potential Scripting Violation* screen.



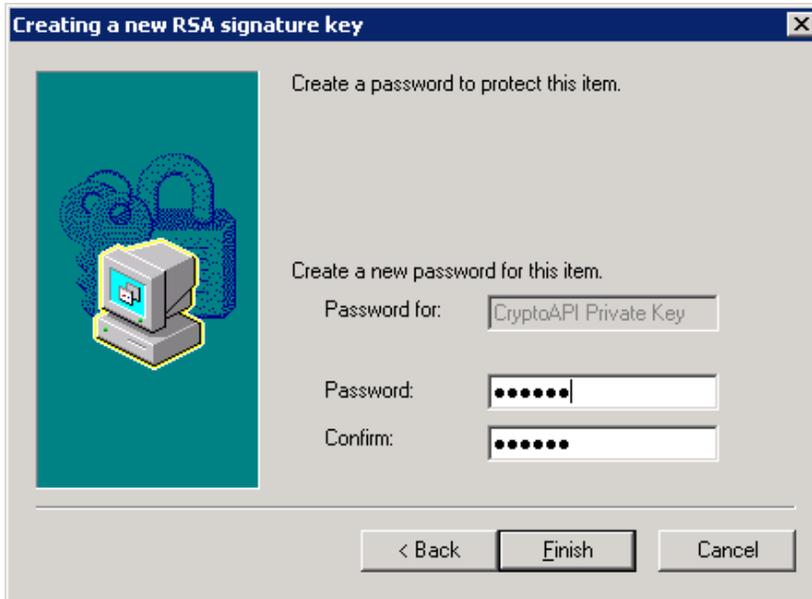
10. Select the “Set Security Level” button.



11. Select “High” to make this certificate password protected and then click “Next>”.



12. Enter the following information on the *Creating a new RSA signature key* screen and select **“Finish”** when completed.
- Enter a **unique password** in the “Password” field that will also be used through the Export and Import process. Anything alpha and/or numeric will work.
  - Re-enter** the unique password in the “Confirm” field.
  - This Password remains the same for this yearly certificate. It is important for you to remember this password. If you forget the password, it cannot be recovered or reset.



NOTES: Please be aware of the following:

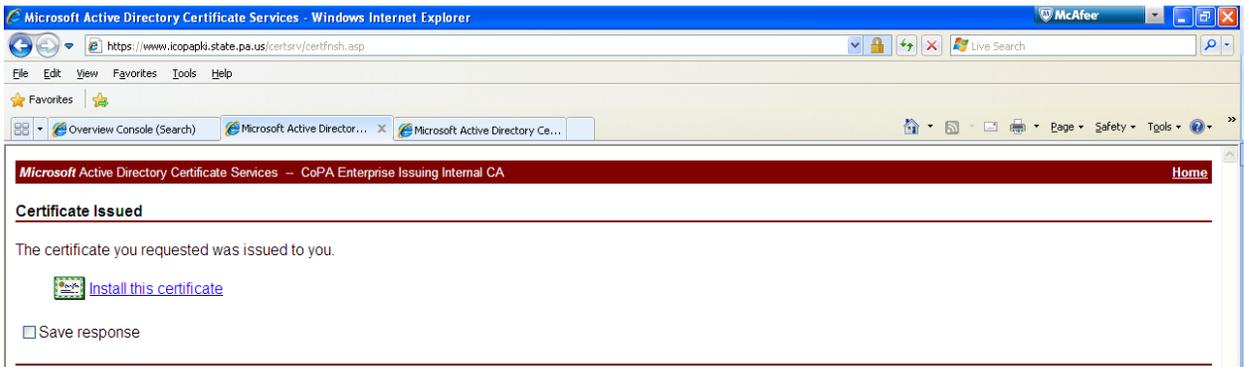
**Windows XP** - “Password for:” field = **CryptoAPI Private Key** will be displayed.

**Windows 2000** - “Password for:” field will be **empty**.

13. Select “**OK**” to confirm the setting.



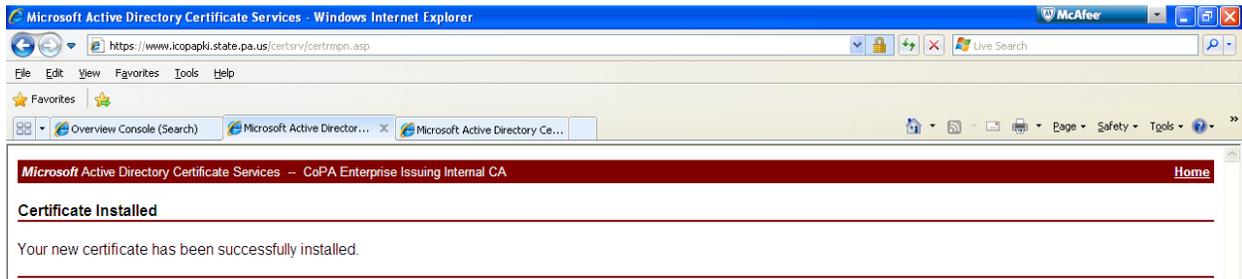
14. Select “**Install this certificate**”. It may take a few moments for the certificate icon to appear so please be patient and wait for the icon to appear before clicking the link.



15. Select “**Yes**”. The next screen may take a few minutes to appear.



16. A **“Certificate Installed”** confirmation message is displayed when the certificate has been successfully downloaded and installed. Close (X) the screen.



Proceed to [Section III - Installation and Configuration of Juniper Network Connect](#)

## **Section III - Installation and Configuration of Juniper Network Connect**

### **Background**

The Juniper Network Connect client package for Windows is a software package installed on the remote user's workstation or laptop device to provide VPN access to the secure COPA network.

### **Requirements**

In order to use these installation and configuration instructions you must have:

1. Administrator access to the laptop\workstation. This permission must be granted through your Agency's network administrators.
2. A Commonwealth Certificate and password. See [Sections I & II](#) of this document.
3. A CWOPA Username and Password

**NOTE:** The user will receive a descriptive message at the beginning of the installation process if the web browser being used does not meet the following requirements

1. Firefox - requires Java to be installed and enabled
2. Internet Explorer - the ActiveX must be enabled

## **Installation:**

1. Open an Internet browser window and navigate to <https://moose.pa.gov>.  
**NOTE:** this website **CANNOT** be accessed while logged on to the CWOPA network.
2. Enter your CWOPA Username and Password
3. Click the Realm dropdown menu to select CWOPA (for Commonwealth of PA users).  
This step ensures the correct access to your agency servers.



4. Click **Sign-in** and Network Connect launches the secure access



5. Depending upon your machine's operating system, enter your Certificate information in one following permission windows:

a. Windows XP:

1. Enter your commonwealth Certificate password
2. Do not click the check box to remember your password
3. Click **OK**

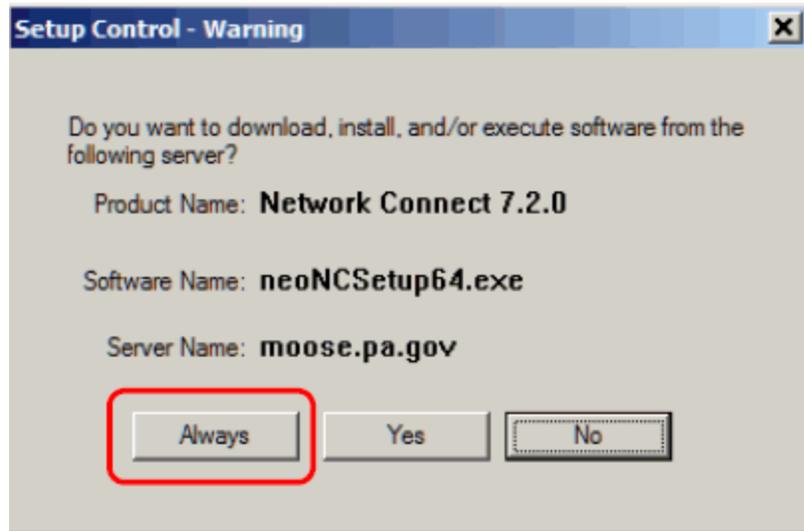


b. Windows 7

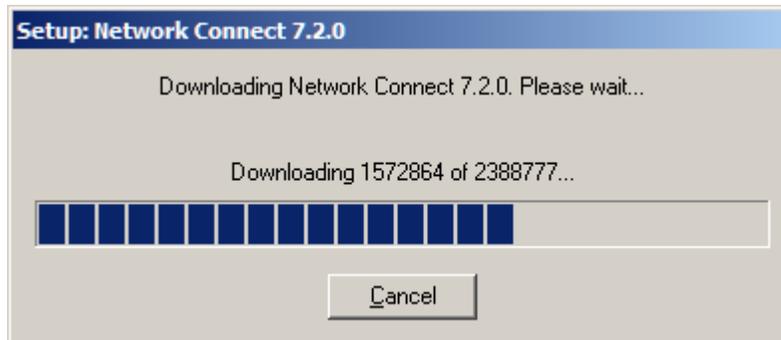
1. Select **Grant permission**
2. Enter your Commonwealth Certificate password and click **OK**



3. Click **Always** in the Setup Control window



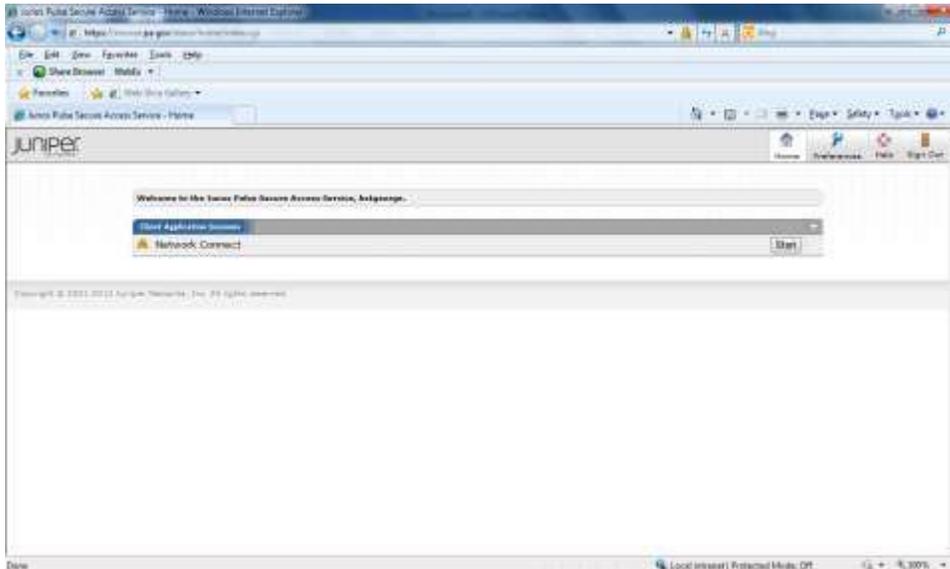
4. Juniper Network Connect downloads and installs.



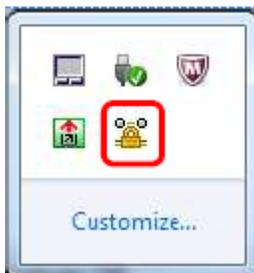
## Connection:

The Welcome screen displays and you may begin working.

**NOTE:** It is not necessary to click **Start**. Your VPN connection is already active based on the Welcome message on the screen.



The connection has now been added and your Network Connect client is available on the active system tray.



**You are now connected to your VPN session.**

## Section IV - Connect with Juniper Connect

To activate a VPN connection through the Network Connect client on a regular basis, please use the steps below:

1. Open an Internet browser window and navigate to <https://moose.pa.gov>.  
**NOTE:** This website **CANNOT** be access while logged on to the CWOPA network.
2. Enter your CWOPA Username and Password
3. Click the **Realm** drop down menu to select CWOPA. This step ensures the correct access to your agency servers.



4. Click **Sign-in** and Network Connect launches the secure access



5. Enter your Certificate information, based on your operating system, in one of the following permission windows:

**Windows XP:**

- a. Enter your Commonwealth Certificate password
- b. Do not click the check box to remember your password
- c. Click **OK**



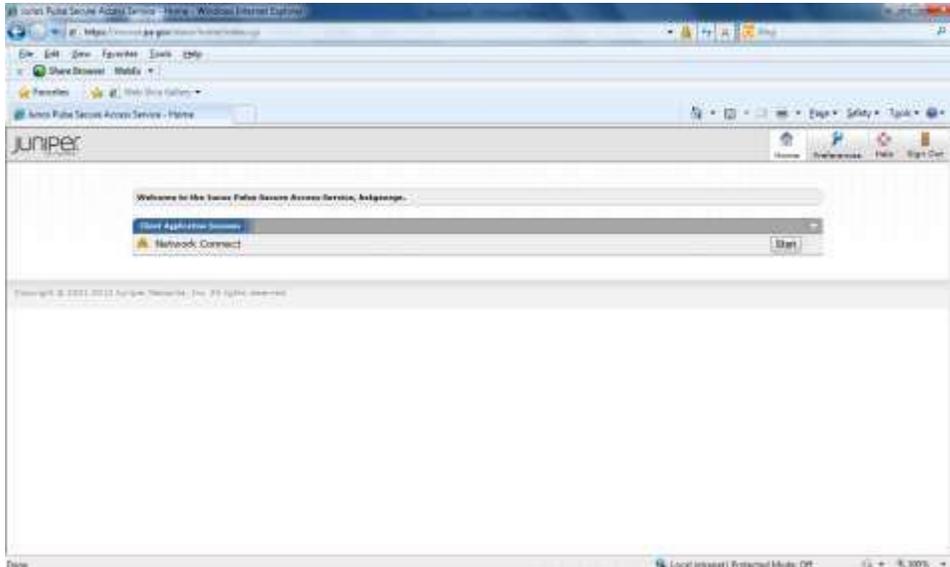
**Windows 7:**

- a. Select **Grant permission**
- b. Enter your Commonwealth Certificate password and click **OK**

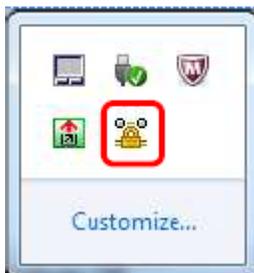


The Welcome screen displays and you may begin working.

**NOTE:** It is not necessary to click Start. Your VPN connection is already active based on the Welcome message on the screen.



The connection has now been added and the Network Connect icon displays in your system tray at the bottom of your screen, indicating a secure connection.

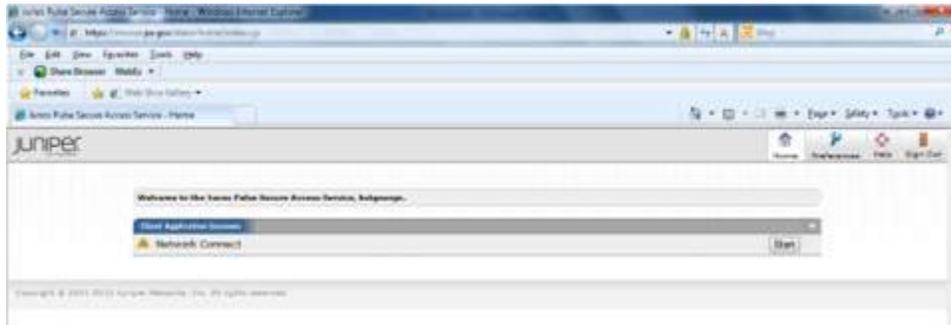


## Section V - Disconnect with Juniper Connect

### Disconnecting the VPN Session

Prior to shutting down your device, it is important to sign off of the VPN service. You have two options:

1. Open <https://moose.pa.gov>

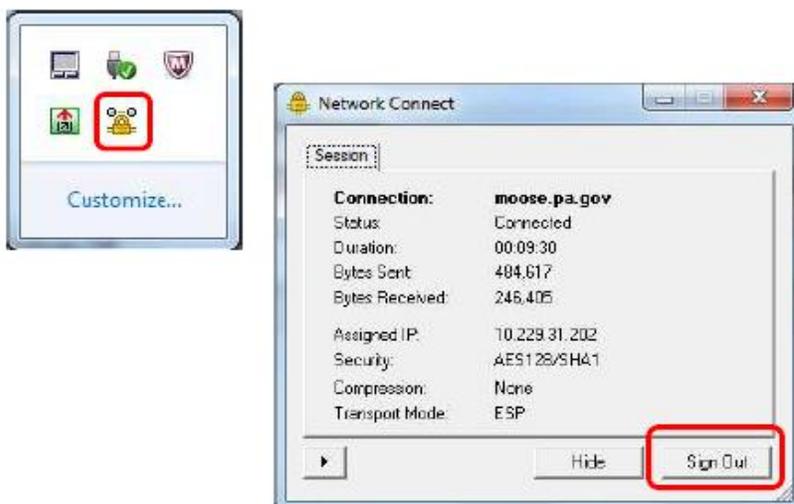


2. Click **Sign Out** in the upper right of the screen to log off your Commonwealth session



Or

1. Double click the **Network Connect icon** on your system tray at the bottom of your screen to open the Network Connect window and click **Sign Out**



## **Section VI – Technical Support**

- A. Call your agency's IT help desk if you are:
  - a. Having a problem with your CWOPA username or password.
  - b. Having a problem connecting to your agency's resources (i.e., mapped drives, RDP) once you have successfully established your VPN connection.
- B. Call the Enterprise Security Helpdesk at 717-772-8606 if you are:
  - a. Having a problem downloading your digital certificate.
- C. Call the Verizon Commonwealth Service Desk (VCSD) at 877-302-7366 if you are:
  - a. Having a problem installing the Juniper Network Connect software.
  - b. Having a problem establishing or maintaining a VPN connection with the Juniper Network Connect software.