DOCUMENT NO.	*SPP-1027*
DOCUMENT NAME	*INTERNET EXPLORER CERTIFICATE ENROLLMENT PROCEDURES*

REVISION LEVEL	2
REVISION DATE	AUGUST 24TH, 2010
OWNER	JOEL FRIEDMAN, CSO

REVISION LEVEL	HISTORY	REVISION DATE
A	Initial Release	May 30th, 2008
2	Updated to current template and revision numbering convention	August 24th, 2010

INTRODUCTION 4

SCOPE 4
RELATED DOCUMENTS 4
TERMS AND DEFINITIONS 4
RESPONSIBLE PARTIES 4

1 INTERNET EXPLORER ENROLLMENT METHOD 5

1.1 IMPORTANT NOTES 5
1.2 ENROLLMENT STEPS 5

INTRODUCTION

SCOPE

This document details specific procedures required to enroll for an Internet Explorer certificate.

RELATED DOCUMENTS

SPP-1000	PCI Information Security Services Policy

TERMS AND DEFINITIONS

<Term>	<Def>

RESPONSIBLE PARTIES

CSO	Chief Security Officer
SEC ENG	Security Engineer

1 INTERNET EXPLORER ENROLLMENT METHOD

1.1 IMPORTANT NOTES

A. You must not clear your browser cache until your certificate has been successfully installed. You will receive a browser message stating that your certificate was installed successfully.
B. You must use Internet Explorer as your browser to enroll for a certificate.

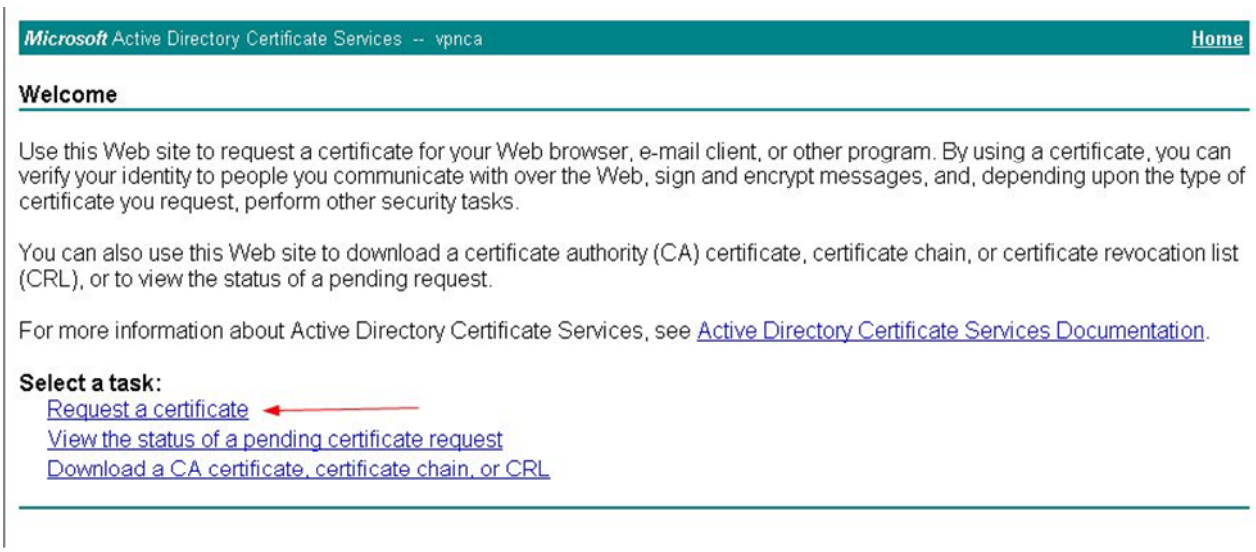
1.2 ENROLLMENT STEPS

A. Browse to http://vpnca.datapipe.net/certsrv using Internet Explorer as your browser.

NOTE: This will not work with any other web browser.

Your browser may warn you that an ActiveX control is needed to advance and may prompt you to install. If this happens, choose 'Yes' to install the ActiveX control. It is Ok to accept any warnings that may appear.

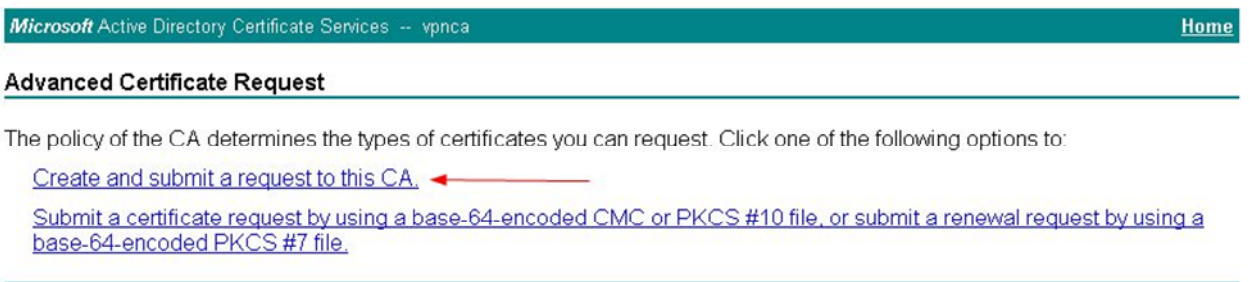
B. On the home page under Select a Task, choose 'Request a certificate'.



C. Select 'advanced certificate request'.



D. Select 'Create and submit a request to this CA'.



E. Under Identifying Information section enter the following **mandatory** fields:

1. Your Full Name
2. Email address
3. Company
4. *Department

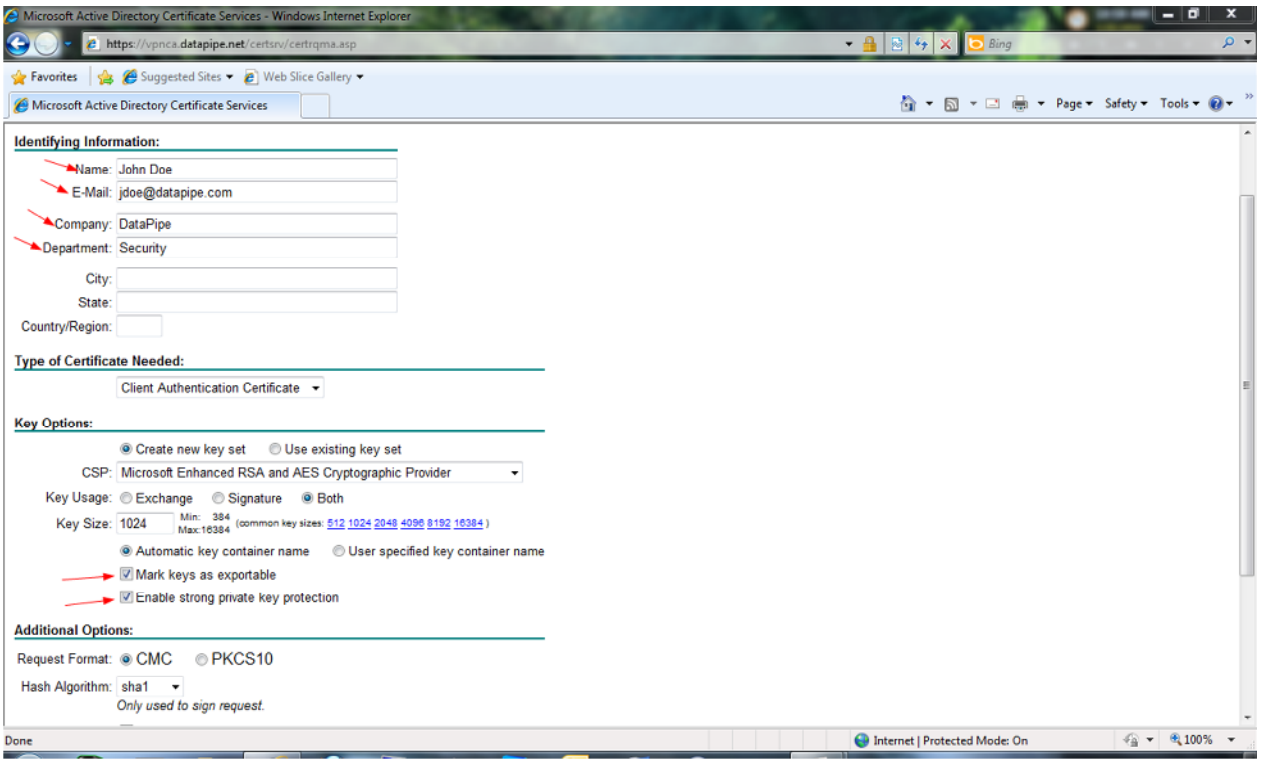
All other attributes are considered optional and do not need to be entered.

NOTE: The Company and Department attributes must be entered exactly as they were provided in the VPN Authorization Worksheet that was submitted to Datapipe. If you are enrolling for a certificate and do know if you are currently listed on the VPN Authorization Worksheet, or do not know the appropriate department and company attributes, please ask your manager for this information. If Datapipe receives a certificate enrollment request which does not exist or match the VPN Authorization Worksheet exactly, the request will be denied.

F. For Re-enrollment Only

To view your existing certificate attributes, please click on the certificates tab in the Cisco VPN client. Locate your certificate and double click it to bring up its properties. The "Subject" line contains your OU (Department) and O (Company) attributes. Please use these same values in the certificate enrollment forms.

G. Under Key Options, check '**Mark keys as exportable**' and '**Enable Strong Key Protection**'. Leave the rest of the options as the default and click Submit. Please see the screenshot below for an example of what the enrollment form should look like after you are finished filling it out.



H. After you submit your certificate you should see a pop up that states: 'Creating a new RSA exchange key'. Select 'Set Security Level'.



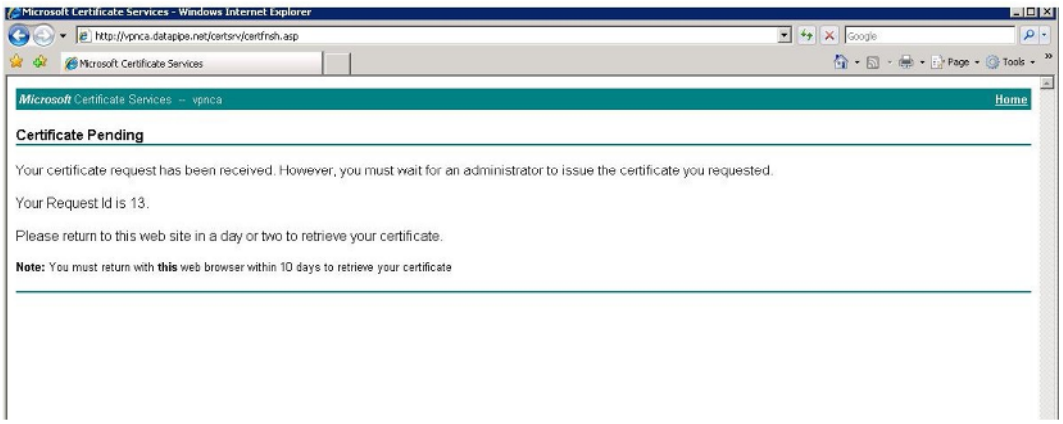
I. Select 'High' and click 'Next'.



J. Enter a complex password that you can remember, and then click 'OK'. You will be asked for this password every time you VPN via the Cisco VPN client. It is important to note that Datapipe cannot recovery this password. Select 'Finish' – then 'OK'.

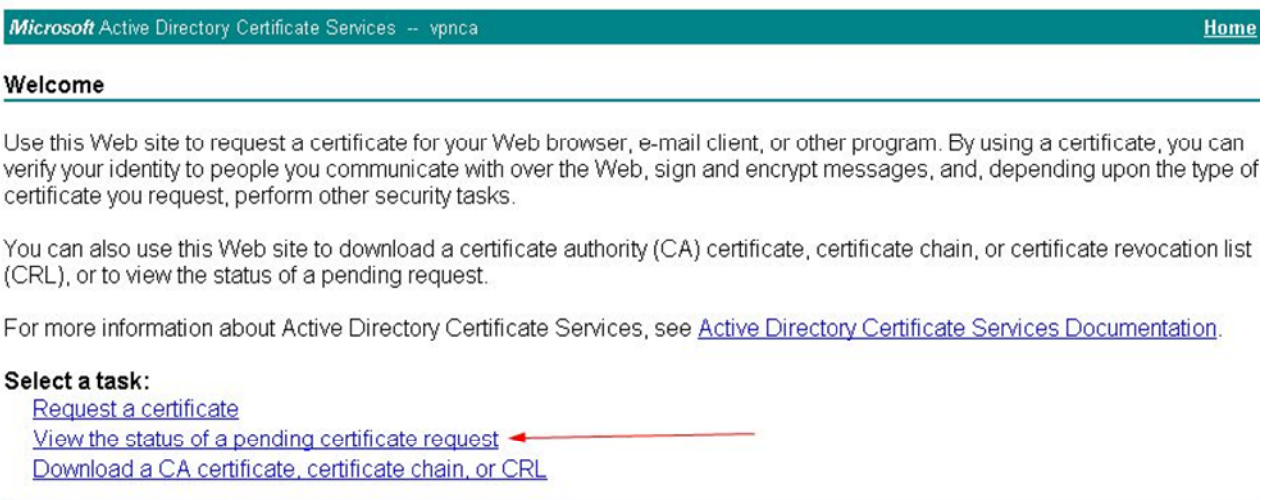


K. Your certificate request is now pending. You will get redirected to a confirmation page like the screenshot below. You will also receive an email from a member of the security department once your certificate has been approved. This may take up to one business day.

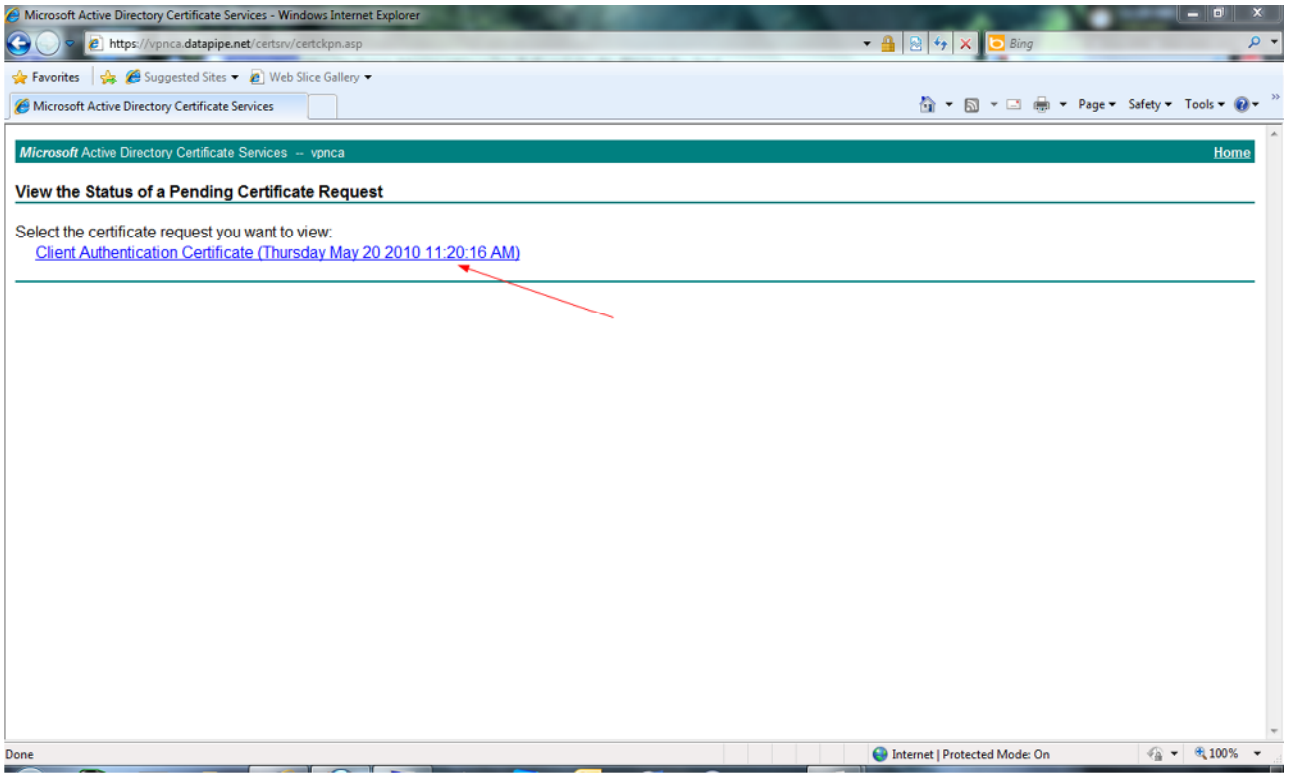


IMPORTANT: Please remember to not clear your browser cache until you have successfully installed your certificate.

L. When you are notified via ticket or email that your certificate has been approved, click the 'Home' link on the top right of the Certificate Pending page or browse to http://vpnca.datapipe.net/certsrv using Internet Explorer on the same computer used to enroll for a certificate. On the home page, select the task: 'View the status of a pending certificate request'.



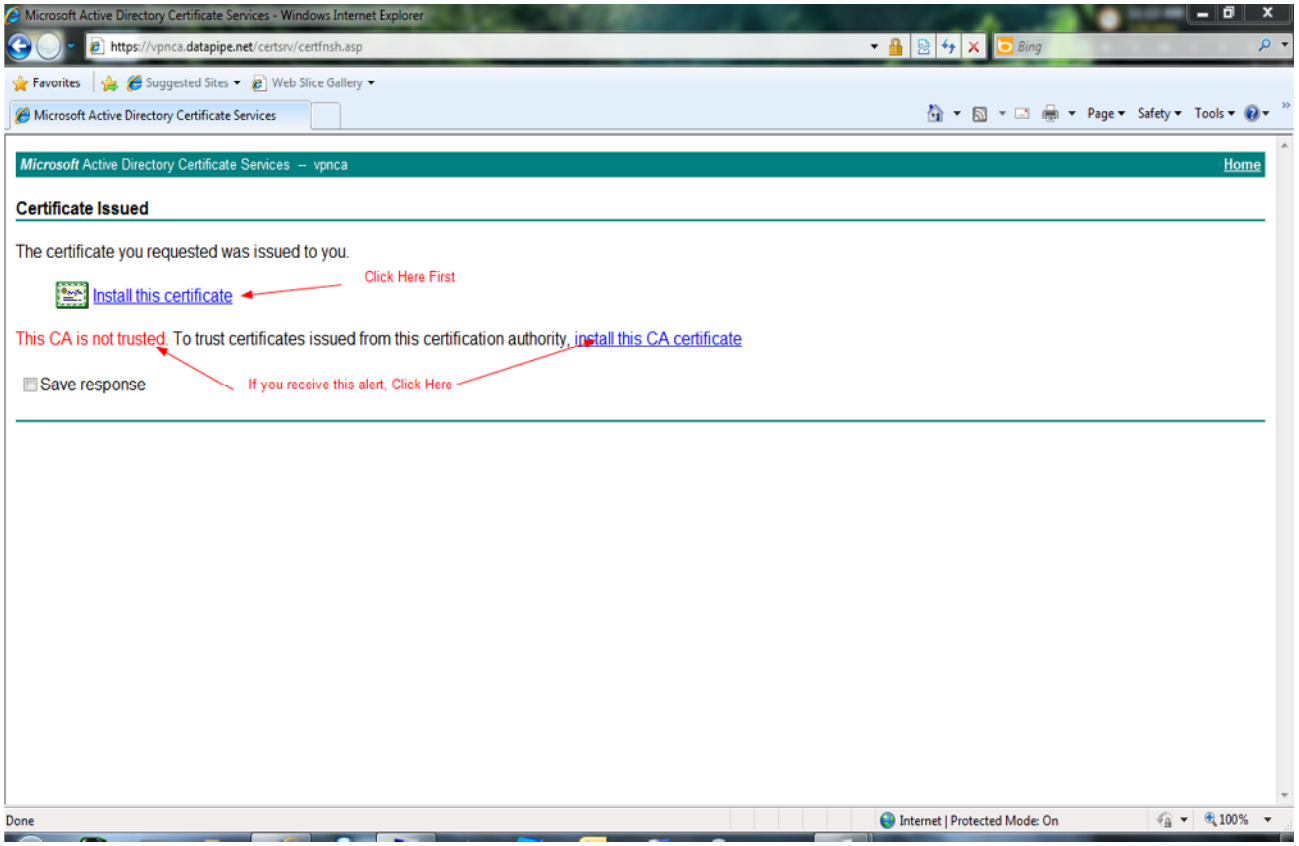
M. You will see something similar to the screenshot below. Click on the certificate request you want to install.



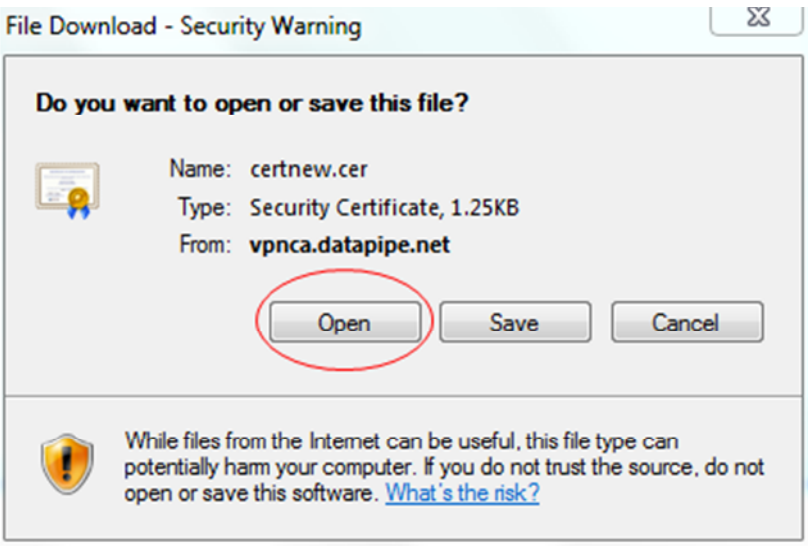
N. Click on 'Install this certificate' and you will be asked for your approval. Answer 'Yes' to all warnings. You should receive confirmation that your certificate has been installed successfully.

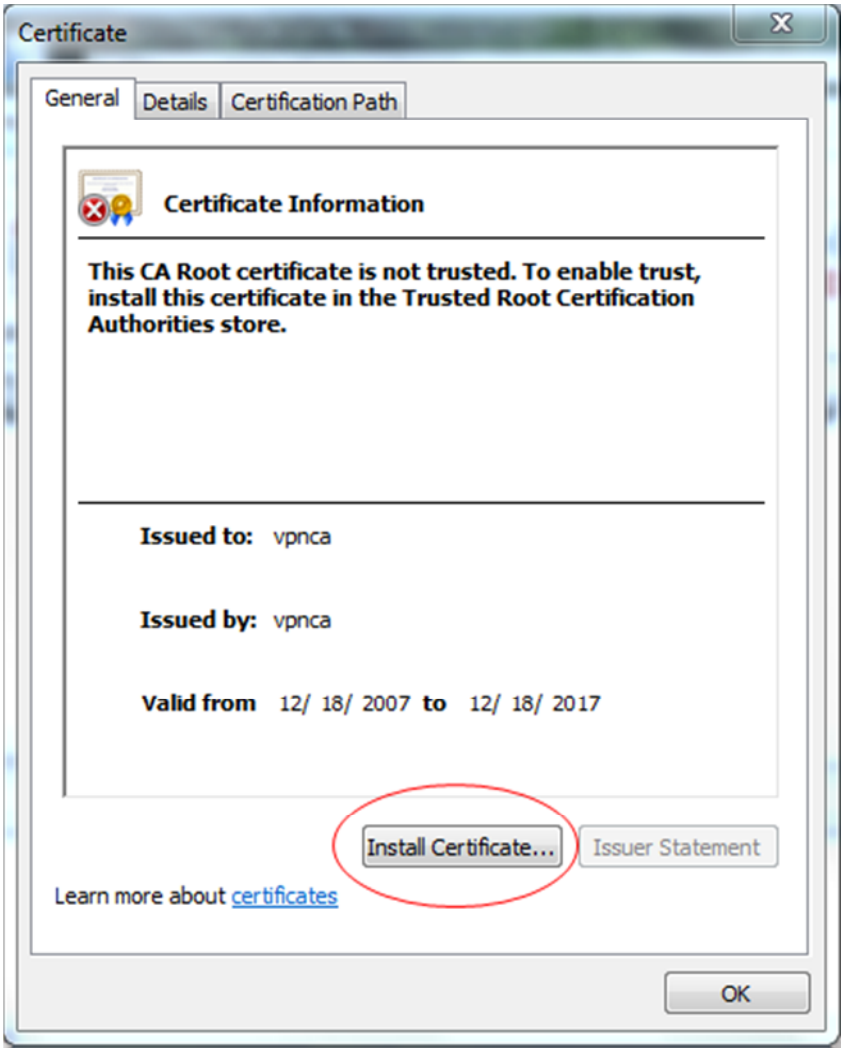


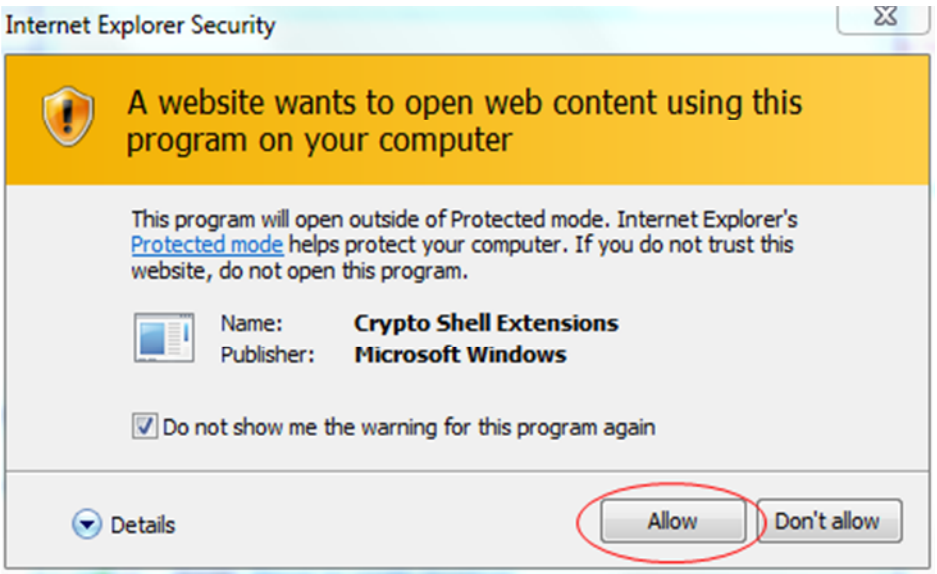
PLEASE NOTE: Some versions of Internet Explorer may alert you that 'This CA is not trusted' when you click 'Install this certificate', preventing you from installing your user certificate. If you see this message, click 'Install this CA Certificate' and navigate to the 'Trusted Root Certification Authorities' store and click 'OK'. Click 'OK' to all warning prompts until your browser tells you the CA certificate has been successfully installed. You should now be able continue install your user certificate. Screenshots detailing these steps are listed below:

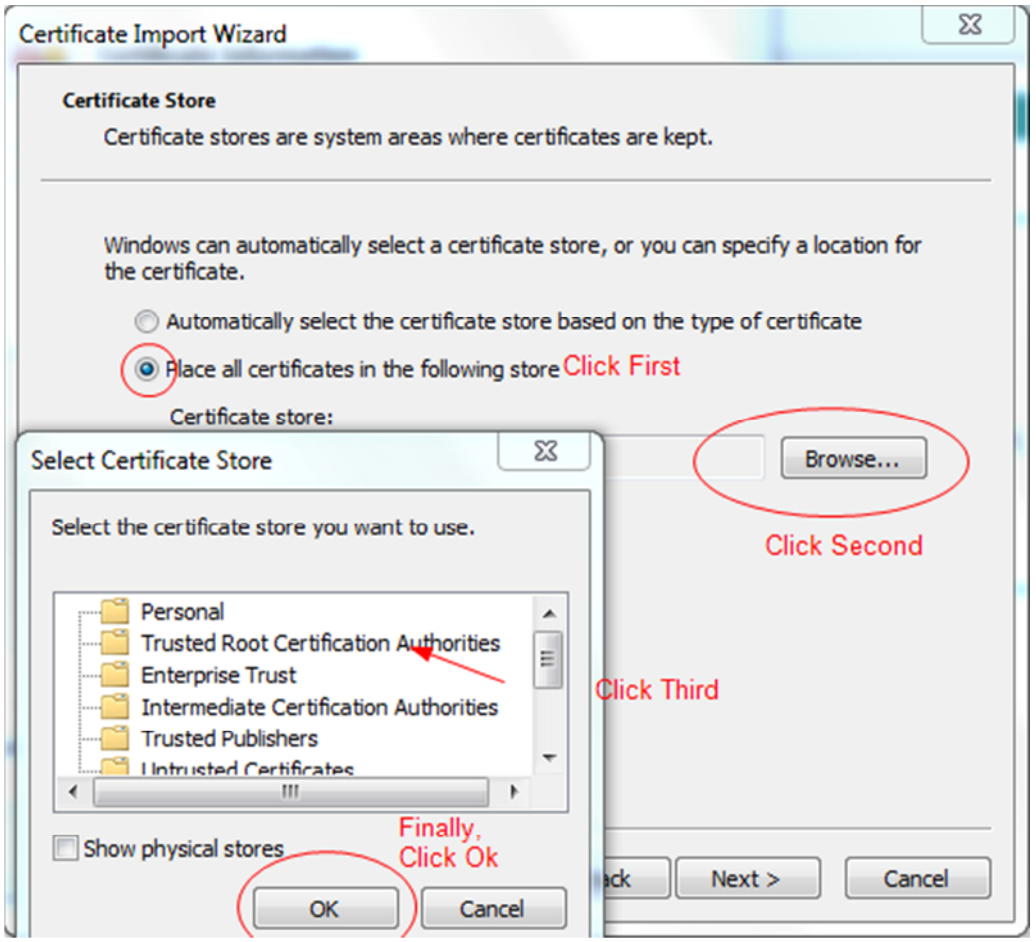


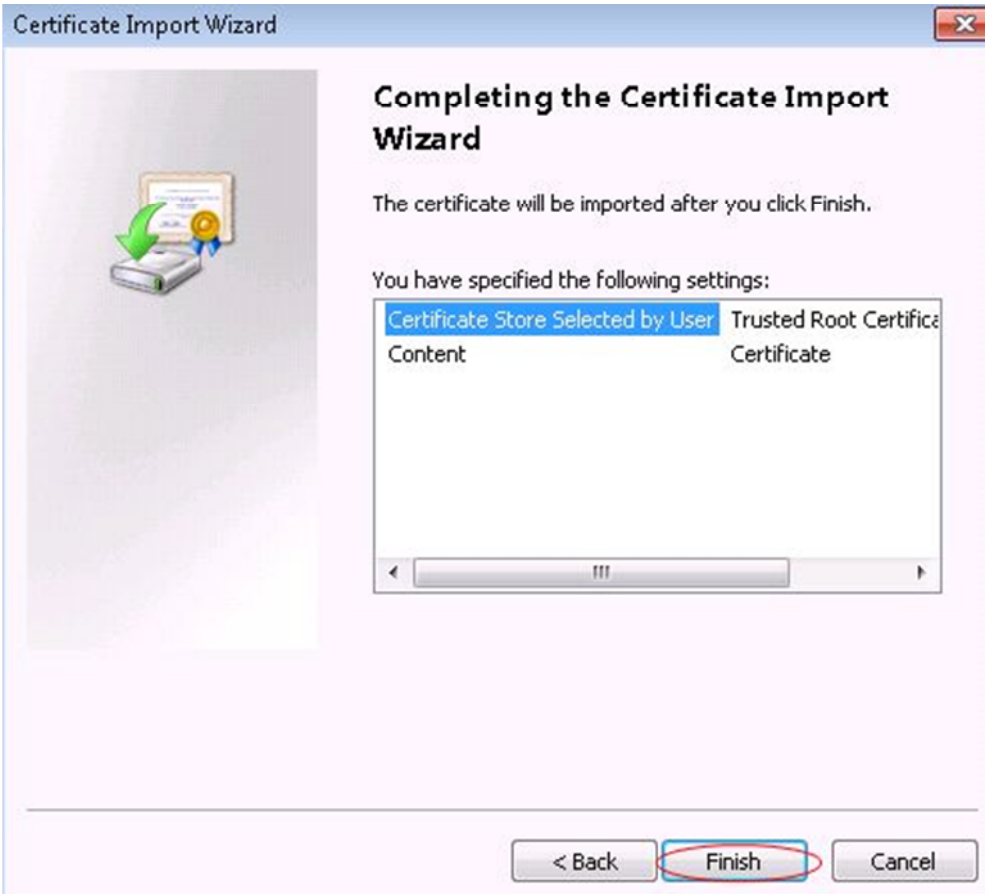
NOTE: If you are alerted to install the CA certificate first, you will receive various popup notifications, like the following screenshots below. If you do not have to install the CA certificate first, just proceed to Step Q below.



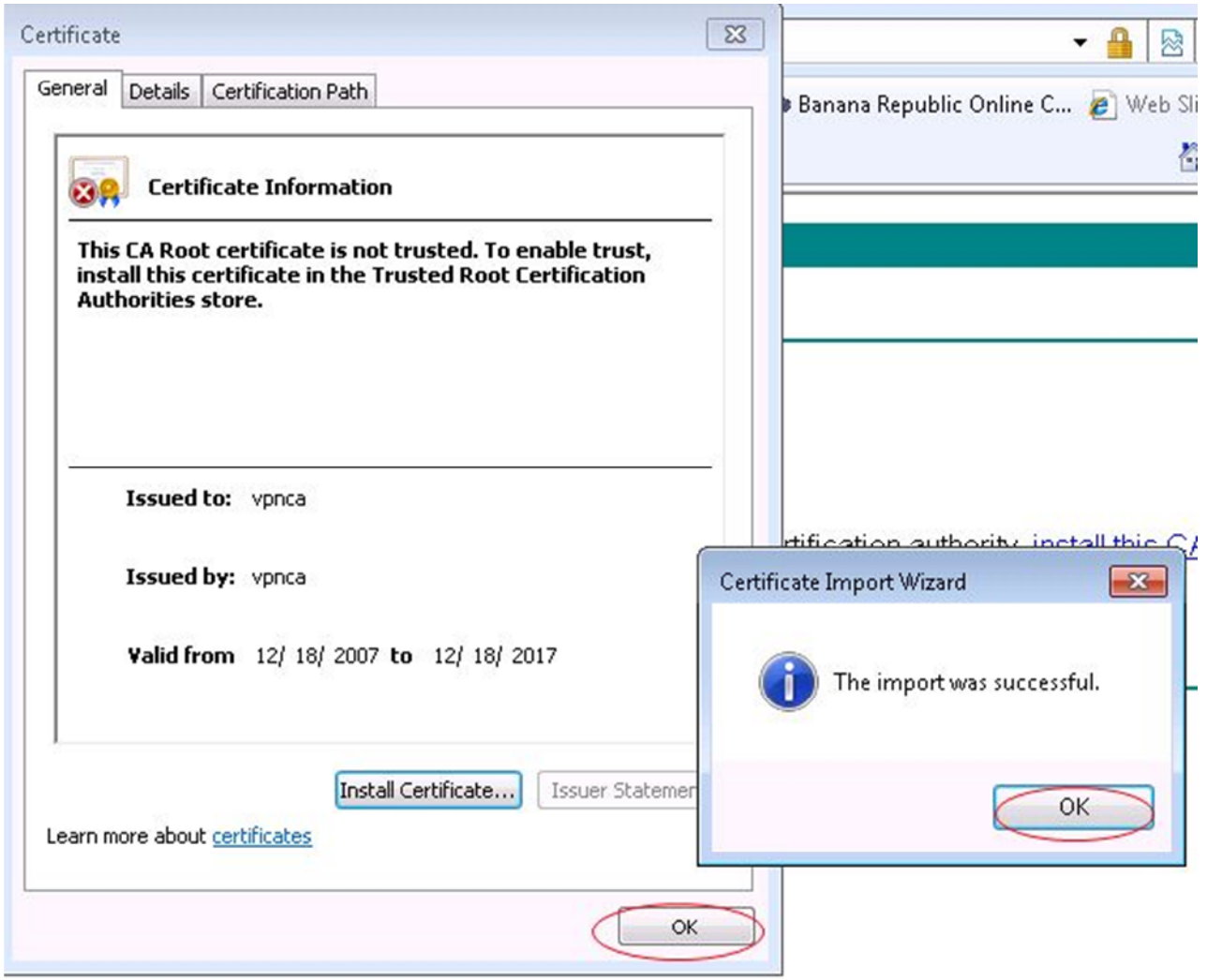

Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: vpnca
Issued by: vpnca
Valid from 12/ 18/ 2007 to 12/ 18/ 2017
Install Certificate...
Issuer Statement
Learn more about certificates
OK


Internet Explorer Security
A website wants to open web content using this program on your computer
This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust this website, do not open this program.
Name: Crypto Shell Extensions
Publisher: Microsoft Windows
Do not show me the warning for this program again
Details
Allow
Don't allow

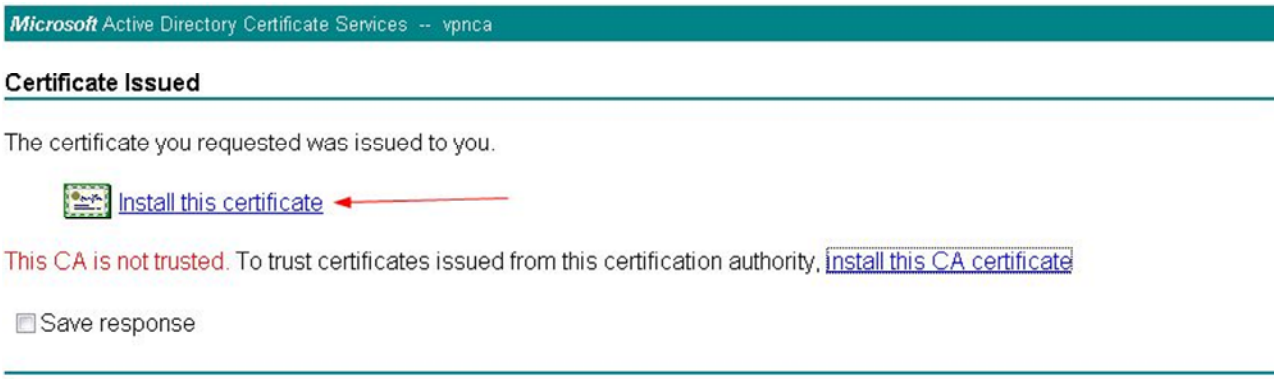

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Click First
Certificate store:
Browse...
Click Second
Select Certificate Store
Select the certificate store you want to use.
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Click Third
Show physical stores
Finally, Click Ok
OK
Cancel
Next >
Cancel


Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certifica
Content
Certificate
< Back
Finish
Cancel


Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
vpnca
Windows cannot validate that the certificate is actually from "vpnca". You should confirm its origin by contacting "vpnca". The following number will assist you in this process:
Thumbprint (sha1): FBDFBB20 971738BB 12D8B93E 1848D5D6 EBBDC1A4
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No


Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: vpnca
Issued by: vpnca
Valid from 12/ 18/ 2007 to 12/ 18/ 2017
Install Certificate...
Issuer Statemer
Learn more about certificates
OK
Banana Republic Online C...
Web Sli
Certificate Import Wizard
The import was successful.
OK

O. Upon installation of the CA certificate, you will still need to install your user certificate. Click on 'Install this certificate'.



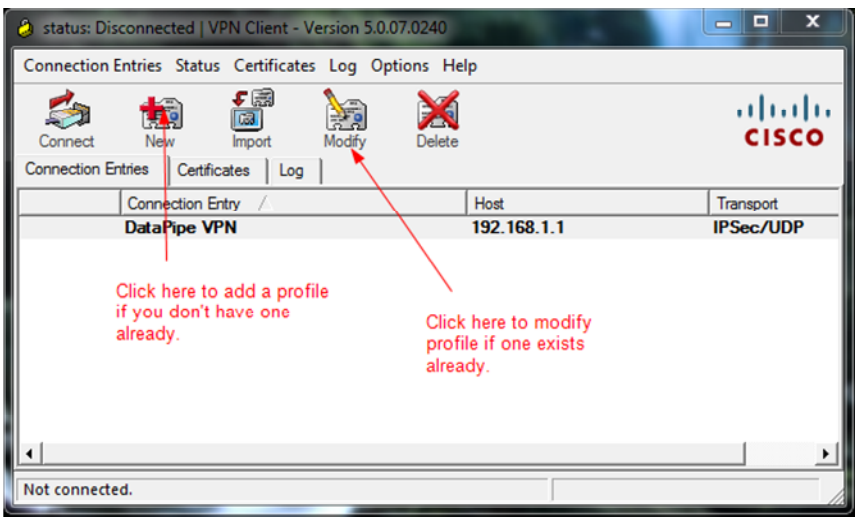
P. You should receive a confirmation similar to the one below.

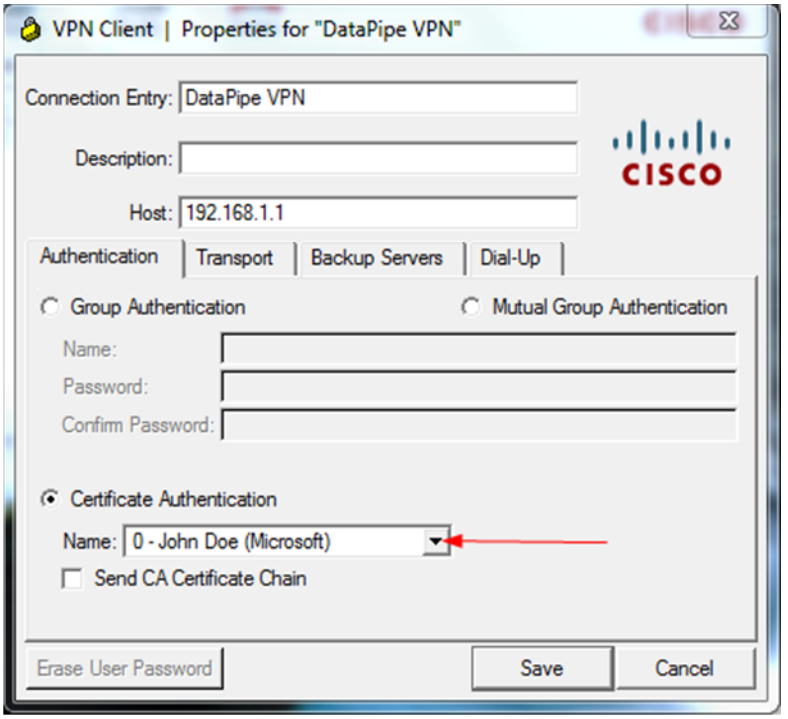


NOTE: If you receive an error, please provide Datapipe with the exact error message you have received.

Q. Open up your Cisco VPN client and right click your connection entry. If you do not have a connection entry created already, please add an entry that with a name and input your firewall IP as the host and choose 'certificate authentication'. Select your user certificate from the drop down menu that you just installed.

NOTE: If you do not know the firewall IP, please ask your manager for this information





R. Click **Save**. You should now be able to connect. If you have any problems connecting, please email tripwire@datapipe.com with the error message you received. **Finished!**