

Carillon eShop User's Guide



Contents

1	Introduction	3
2	HOW-TO: SET UP A CA CERTIFICATE CHAIN (TRUST CHAIN) IN WINDOWS 10	4
2.1	Installing the Carillon CA Trust Chain	5
2.1.1	Download & Install the Carillon Root CA Certificate	5
2.1.2	Download & Install Carillon Intermediate CA Certificate	9
2.1.3	Validate the Root Certificate Thumbprint.....	14
2.2	Installing the Boeing Trust Chain.....	16
2.2.1	Download Boeing Certificates.....	16
2.2.2	Install the Boeing Root CA Certificate.....	17
2.2.3	Install Boeing Intermediate CA Certificate.....	21
2.3	Verifying the Trusted Site and Validating the EVSSL.....	26
3	CERTIFICATE RETRIEVAL PROCESS	30
4	THE ACKNOWLEDGING PROCESS	39
5	HOW TO EXPORT ID, SIG, & ENC CERTIFICATES	43
5.1	Export ID, SIG & ENC Certificates from Your Personal Store	43
5.2	Deletion of Certificates from Hard Drive.....	48
5.3	To Import Certificates	48
5.4	Setting Up Access to the Carillon LDAP Proxy	52
5.5	Confirming LDAP is Properly Configured.....	55
6	HOW TO USE YOUR CERTIFICATES IN OUTLOOK	57
6.1	Setting up Outlook or Office 365 to use your Certificates	57
6.2	Signing and Encrypting E-mail	62
7	NETWORK ADMINISTRATOR TROUBLESHOOTING	64
7.1	Test link to the Carillon LDAP Proxy	64
8	CUSTOMER SERVICE	66





1 Introduction

This document serves as a guide to assist you through the various steps that need to be performed using the Carillon eShop Interface: from downloading the Carillon CA Certificate Chain (Trust Chain), retrieving and acknowledging your certificates, through to setting up Outlook in order to be able to use these certificates on your computer or laptop.

PLEASE NOTE:

The instructions in this handbook are typical guidelines of how to download and install CA certificates on your system. There may be some variance between what is presented here, and what your own system will display. Should you have any issues after you have completed these steps, please contact your System Administrator.

Please be aware that you may require Administrator rights to perform these actions. If you do not have Administrator rights on your workstation, seek assistance from your System Administrator to help with this setup.





2 HOW-TO: SET UP A CA CERTIFICATE CHAIN (TRUST CHAIN) IN WINDOWS 10

This section describes the steps for installing the Carillon Trust Chain and the Boeing Trust Chain on a Windows 10 computer or laptop. We refer to the Carillon CA and Boeing Trust Chains as our principle examples because these are the ones we use for Carillon CA issued certificates purchased from our Carillon eShop.

Installing the appropriate Trust Chain certificates on your computer or laptop ensures that your personal certificates will then be correctly installed, recognized and trusted by your applications, such as your web browser or email client.

You will need to first download the **Carillon Trust Chain** certificates. These trust chain certificates are required in order to validate the certificates that will be purchased from the Carillon Certificate eShop.

The **Carillon Trust Chain** is comprised of the following two certificates:

The <https://pub.carillon.ca/CACerts/CISRCA1.cer> (Root Certificate); and

the Carillon PKI Services CA 1 <https://pub.carillon.ca/CACerts/CISCA1.cer> (Intermediate or Signing Certificate).

These certificates can also be downloaded directly from the Carillon PKI public repository website: <https://pub.carillon.ca/> by clicking on the **DER** button for each certificate.

If you are using these certificates as part of the Boeing supply chain, you need to download the **Boeing Trust Chain** certificates. The Boeing Trust Chain certificates are required for secure email communication between Boeing and its partners.

The **Boeing Trust Chain** is comprised of the following two certificates:

The Boeing Root CA certificate (The Boeing Company Root Certificate Authority.crt); and

The Boeing Secure Messaging G2 certificate (Boeing Secure Messaging G2.crt)

These certificates can be downloaded individually from the Boeing PKI public repository website: <http://www.boeing.com/crl/>



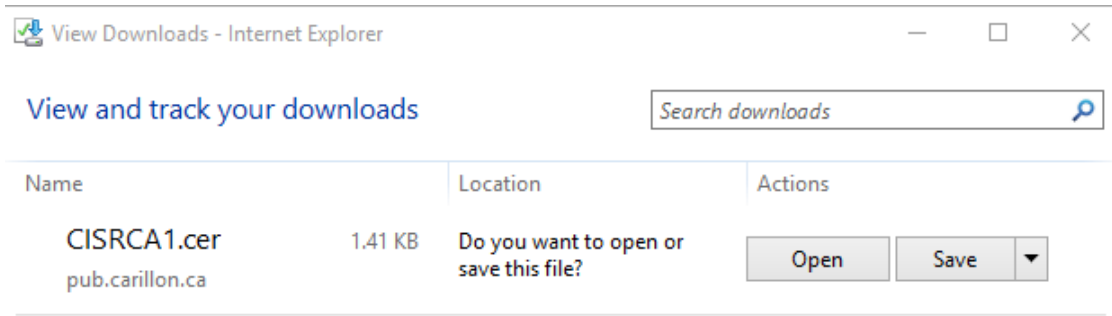


2.1 Installing the Carillon CA Trust Chain

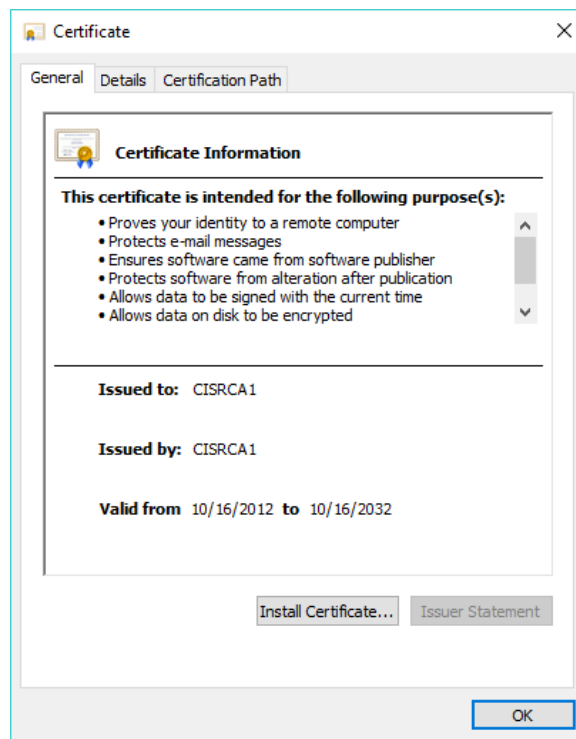
2.1.1 Download & Install the Carillon Root CA Certificate

The following link: <https://pub.carillon.ca/CAcerts/CISRCA1.cer> will bring you to your View Downloads – Internet Explorer window.

1. Under name **CISRCA1.cer** (Root CA) file; click on the **Open** button.

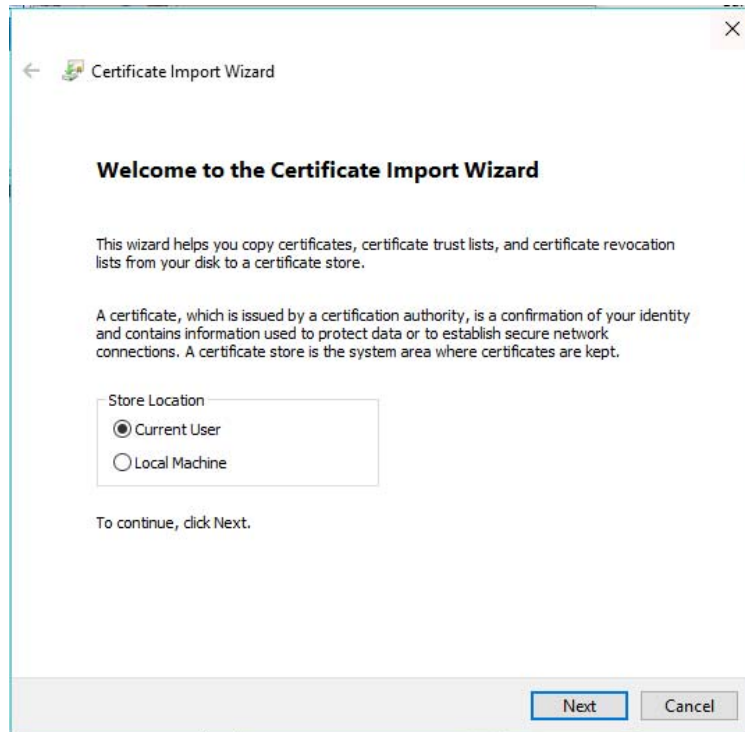


2. The **Certificate** window will appear; click on the **Install Certificate** button.

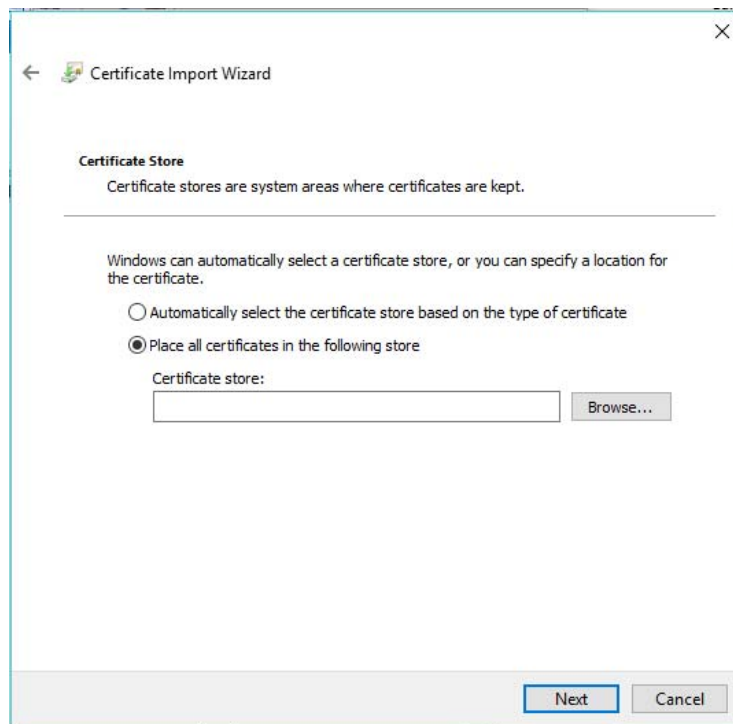




3. The following **Certificate Import Wizard** window will appear, click the **Next** button.

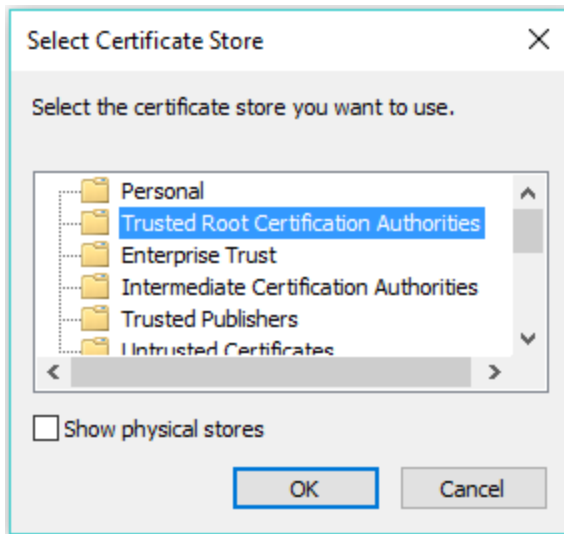


4. Select the **Place all certificates in the following store** option and then click the **Browse** button.

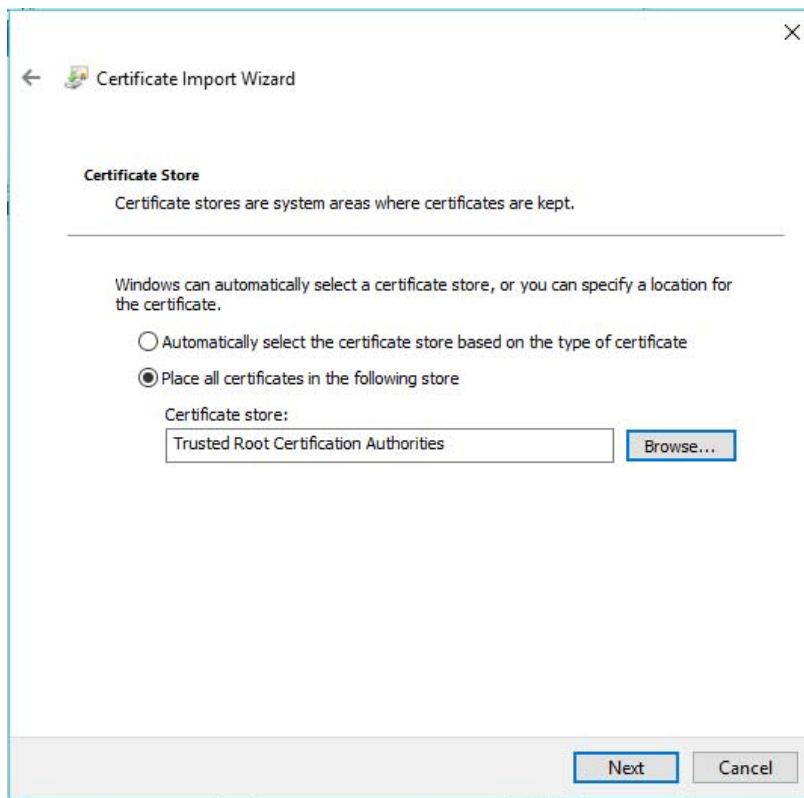




5. Click on **Trusted Root Certification Authorities** and then click **OK**.

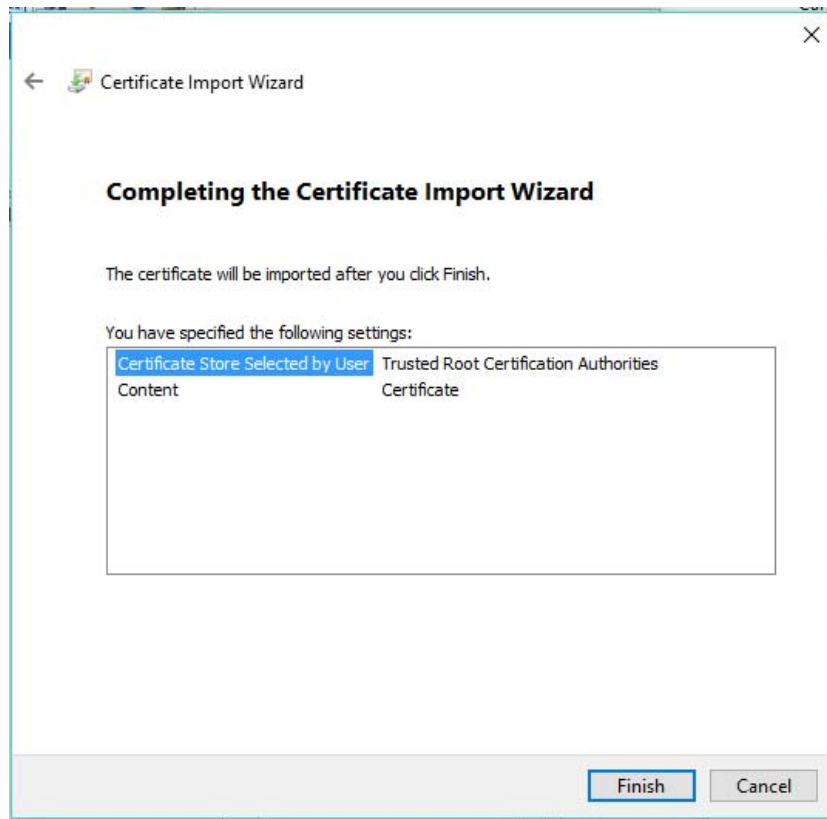


6. The following information will appear in the **Certificate Store** window, click on the **Next** button.





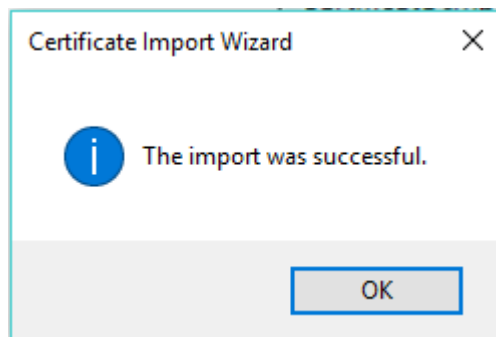
7. The following window will appear, click on the **Finish** button.



NOTE:

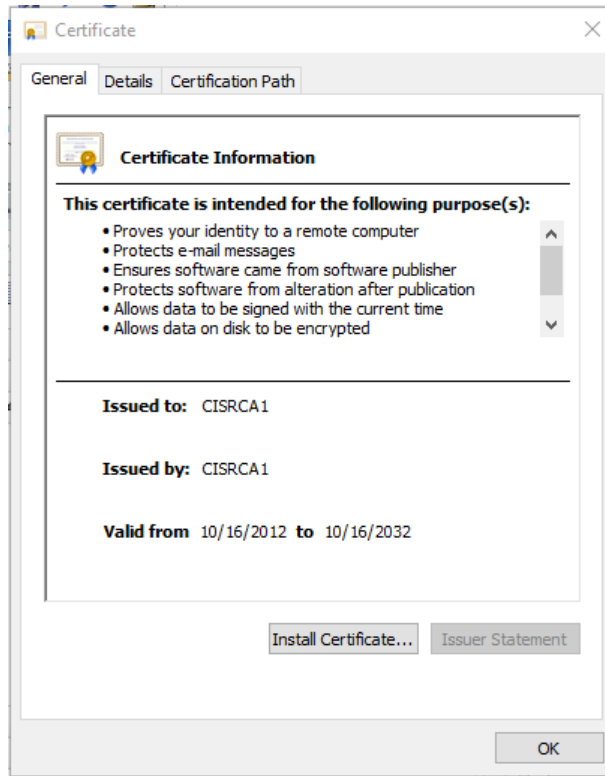
Throughout the installation of the Trust Chain, you will get Security Warning pop-ups. This is normal as you are installing the certificates for the first time. It is okay to trust and install these certificates.

8. The **Certificate Import Wizard** pop-up will appear advising the Import was successful; click the **OK** button to complete the installation of the Carillon Root CA Certificate.





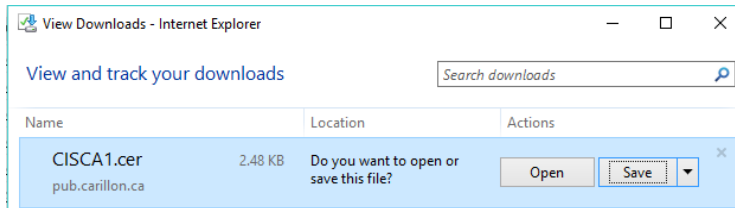
9. Click **OK** to close the certificate windows, and click **Close** on the downloads window.



2.1.2 Download & Install Carillon Intermediate CA Certificate

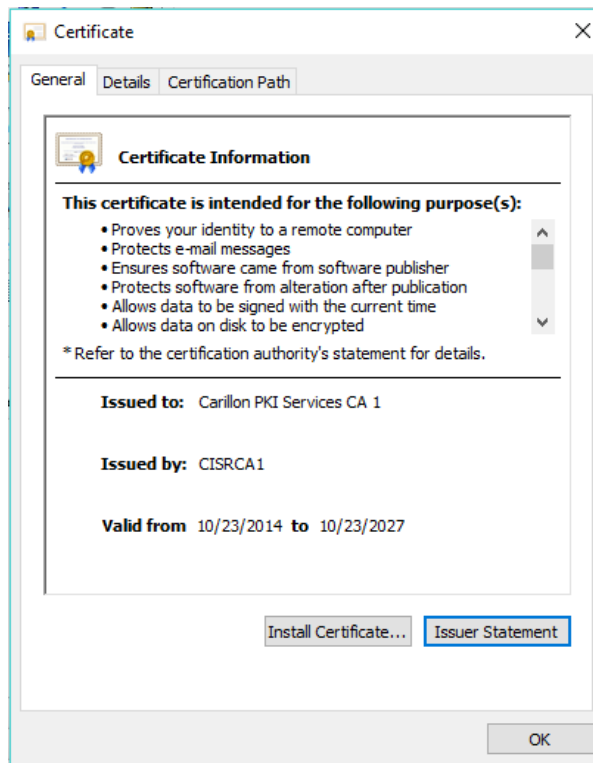
The following link: <https://pub.carillon.ca/Cacerts/CISCA1.cer> will bring you to your View Downloads – Internet Explorer window.

1. Under name **CISCA1.cer** (Intermediate or Signing CA 1 certificate) file; click on the **Open** button.

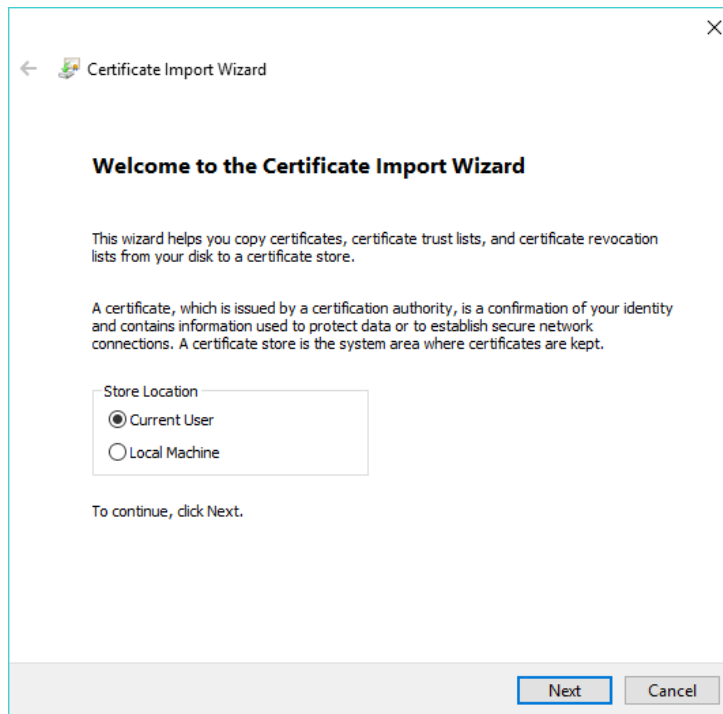




2. The Certificate window will appear; click on the **Install Certificate** button.

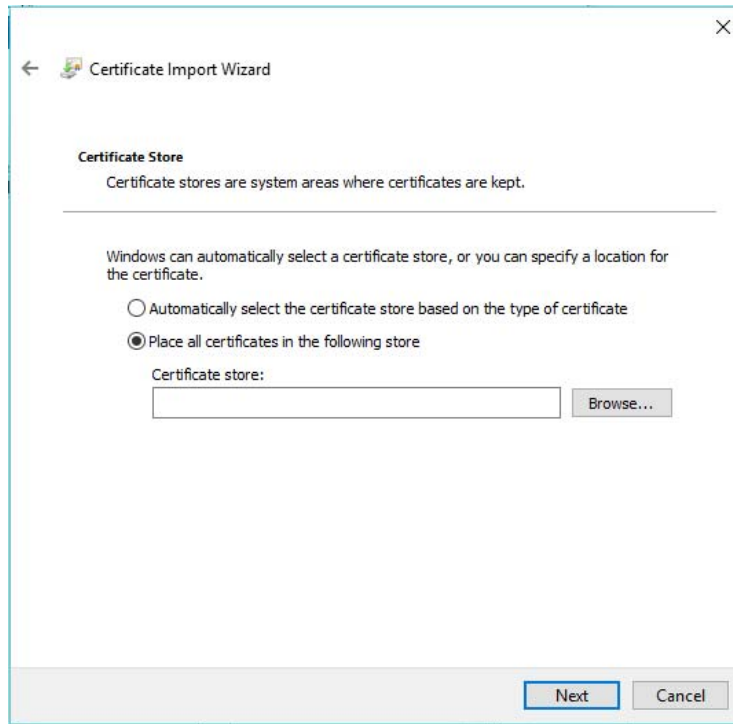


3. The following Certificate Import Welcome Wizard window will appear, click the **Next** button.

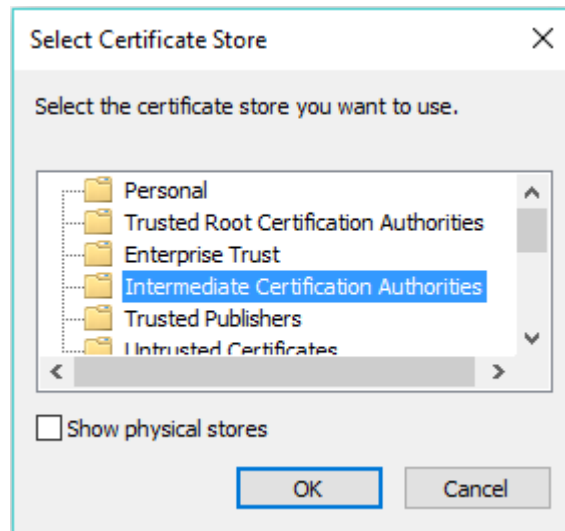




4. Select **Place all certificates in the following store** option and then click the **Browse** button.

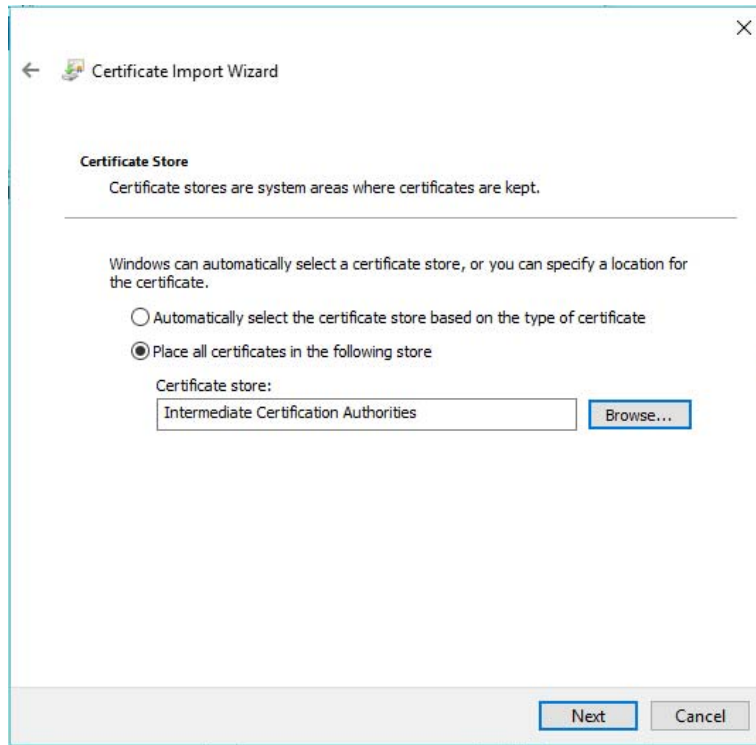


5. Click on **Intermediate Certification Authorities** and then click **OK**.

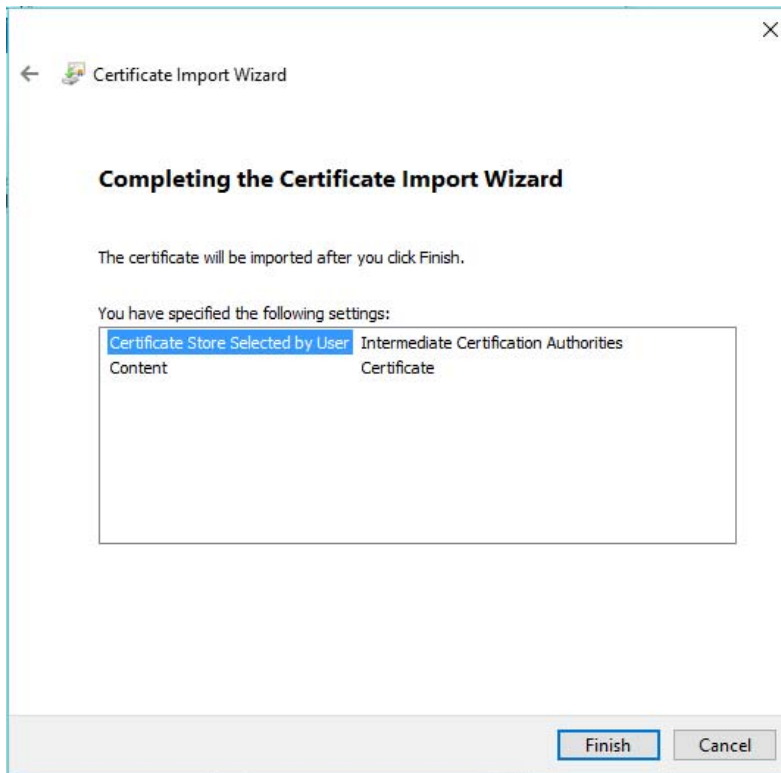




6. The following information will appear in the window, click on the **Next** button.

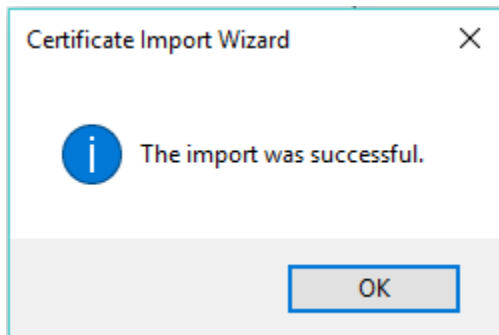


7. The following window will appear, click on the **Finish** button.





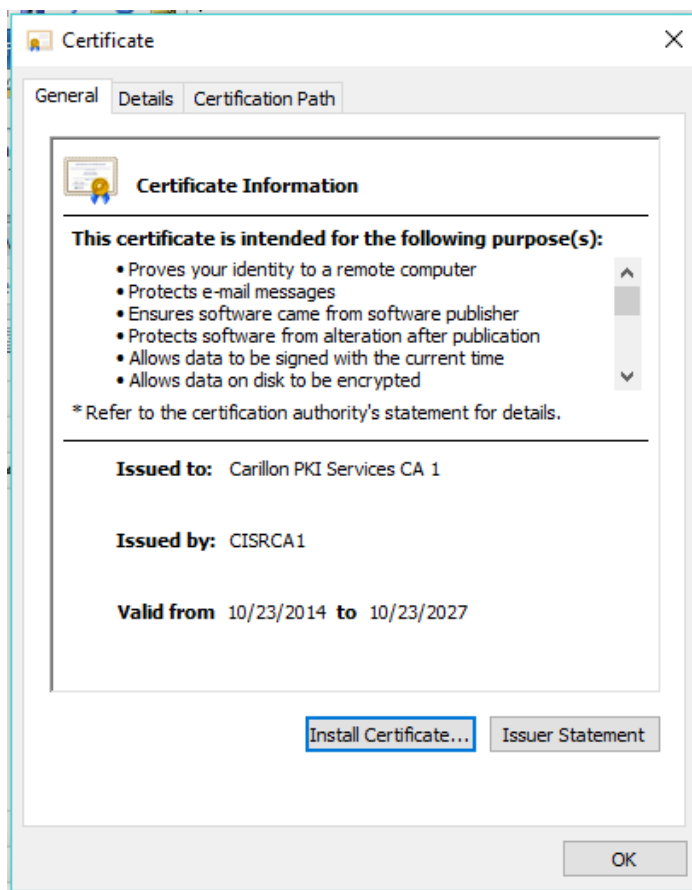
- The **Certificate Import Wizard** pop-up will appear advising the Import was successful; click the **OK** button to complete the installation of the Carillon Intermediate CA 1 Certificate.



NOTE:

Throughout the installation of the Trust Chain, you will get Security Warning pop-ups. This is normal as you are installing the certificates for the first time. It is okay to trust and install these certificates.

- Click **OK** to close the certificate windows, and click **Close** on the download window.



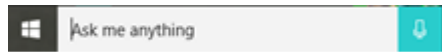


This completes the installation of the Carillon Trust Chain Certificates.

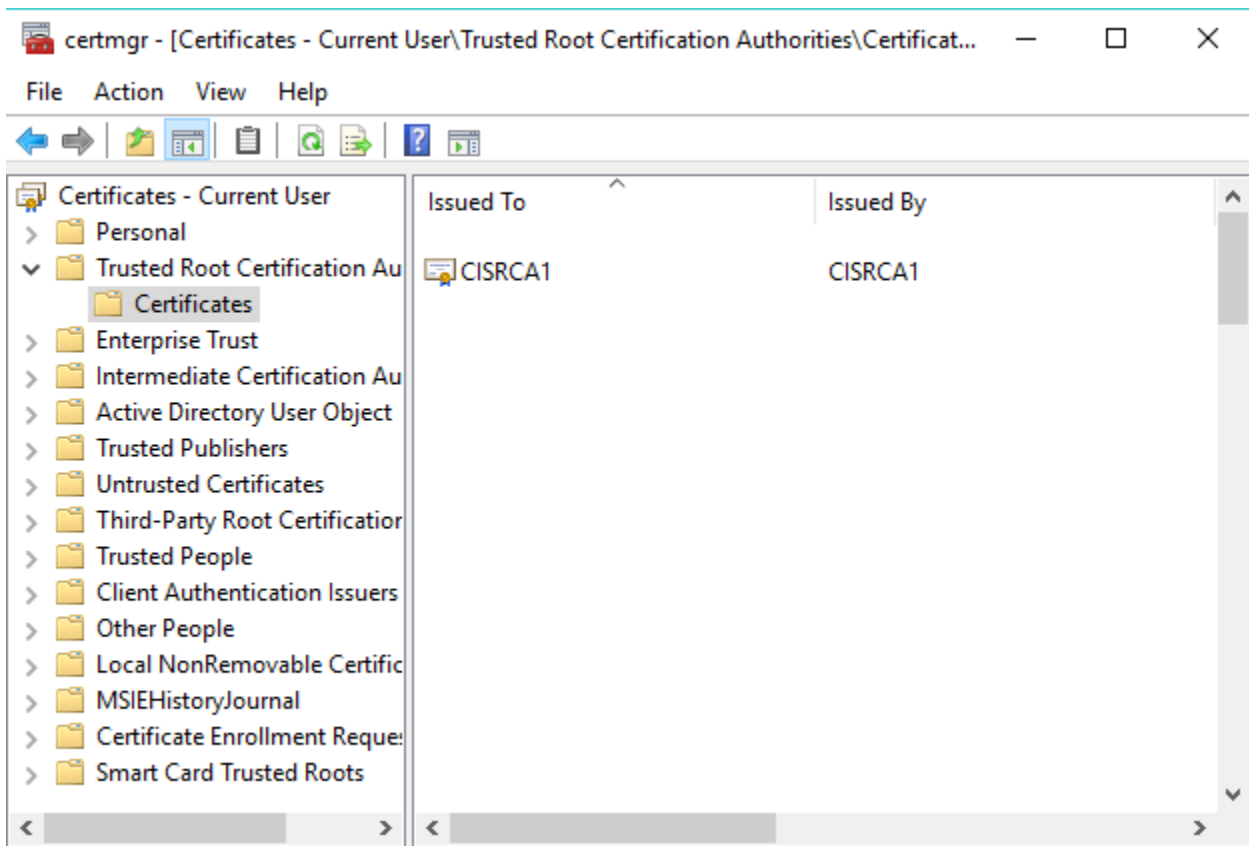
2.1.3 Validate the Root Certificate Thumbprint



1. Click on the **Start icon**:
2. Type in the Search programs and files box: **certmgr.msc** and press enter.



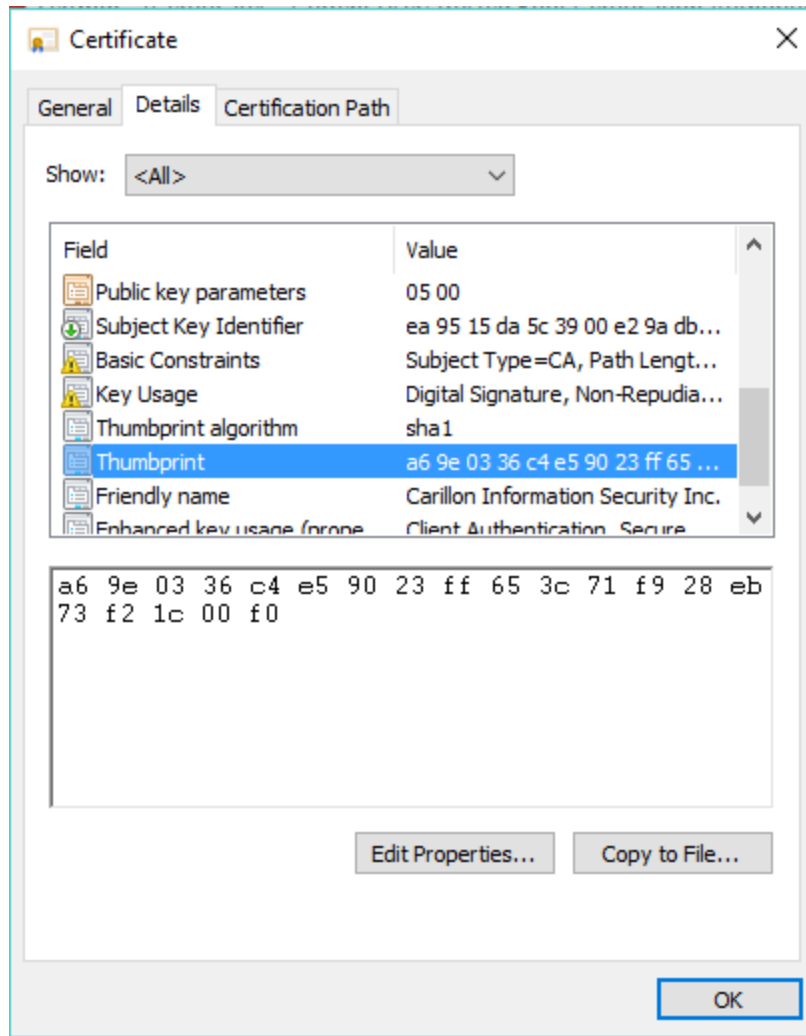
3. The certmgr window will appear. Click **Trusted Root Certification Authorities**, and then click **Certificates**. On the right panel, locate and double-click the **CISRCA1** certificate.





4. A Certificate window will open. Click the **Details** tab. In the Show: dropdown, select **<All>** in the field column, scroll down to Thumbprint. It should read:

a6 9e 03 36 c4 e5 90 23 ff 65 3c 71 f9 28 eb 73 f2 1c 00 f0.



5. Click **OK** to close the window.





2.2 Installing the Boeing Trust Chain

2.2.1 Download Boeing Certificates

1. Visit the Boeing website at the following address:

<http://www.boeing.com/crl/>

2. Under the column **Enterprise Production Authority Information** heading, download the **The Boeing Company Root Certificate Authority.crt** by **right-clicking** on the link, then in the drop-down menu select the **Save target as...** to save the file.

Boeing Class 2 Windows Machines.crt	Apr 10 05:33:06 2019 GMT
Boeing Company OSCA.cer	Nov 23 22:51:06 2016 GMT
Boeing Company OSCA.crt	Nov 23 22:51:06 2016 GMT
Boeing Company OSCA G2.crt	Dec 31 23:59:59 2020 GMT
Boeing e-Enabled Products Issuing CA(1).crt	May 1 22:37:08 2019 GMT
Boeing e-Enabled Products Issuing CA.crt	May 1 22:37:08 2019 GMT
Boeing e-Enabled Products Issuing CA G2.crt	Nov 19 20:57:18 2025 GMT
Boeing e-Enabled Products Policy CA.crt	Aug 28 23:07:56 2028 GMT
Boeing e-Enabled Products Root CA.crt	Aug 20 23:26:48 2048 GMT
Boeing Network Devices CA.crt	Oct 11 11:14:22 2016 GMT
Boeing PCA G2.crt	Sep 21 17:58:13 2029 GMT
BoeingPCAG2.p7c	Apr 30 23:59:59 2017 GMT
Boeing PCA G3.crt	Nov 29 17:20:01 2030 GMT
BoeingPCAG3.p7c	Apr 30 23:59:59 2017 GMT
Boeing PREPROD SecureBadge Medium G2.cer	Feb 1 00:12:58 2022 GMT
Boeing PREPROD SecureBadge Medium G2.crt	Feb 1 00:12:58 2022 GMT
Boeing SecureBadge Basic G2.crt	Feb 28 23:00:46 2023 GMT
Boeing SecureBadge Medium G2.crt	Feb 3 19:28:47 2022 GMT
Boeing Secure Messaging G2.crt	May 30 01:43:26 2019 GMT
Boeing SUG Root.crt	Dec 4 21:36:59 2017 GMT
saml.boeing.com.cer	Mar 25 23:59:59 2018 GMT
saml-ciefrz.boeing.com.cer	Jul 3 23:59:59 2017 GMT
saml-cie-prod.boeing.com.cer	Nov 4 23:59:59 2017 GMT
saml-cite.boeing.com.cer	Jan 13 23:59:59 2018 GMT
Secure Messaging.crt	Jan 20 19:28:53 2015 GMT
The Boeing Company Class 2 Certificate Authority.crt	Jan 11 19:02:14 2014 GMT
The Boeing Company Class 2 Certificate Authority G2.crt	Nov 15 22:15:15 2017 GMT
The Boeing Company Root Certificate Authority.crt	Dec 15 00:16:20 2021 GMT

3. Select a directory on your computer to save the file to and click the **Save** button.





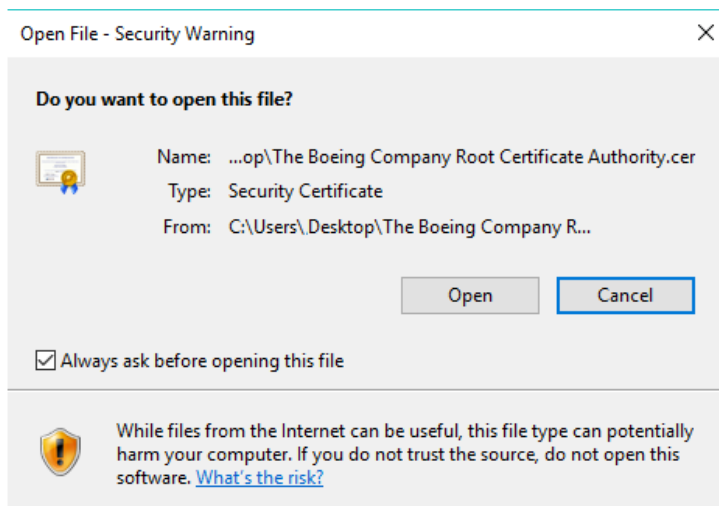
- Repeat steps 2 and 3 for the downloading of **Boeing Secure Messaging G2.crt** and **Boeing Secure Messaging G2 Exp 2019.crt** then close your browser.

Enterprise Policy Info	Document Date
Boeing_Med_Assurance_Domain_CP_v11.3.pdf	Mon Apr 3 13:03:45 2017
Boeing_SecureBadge_Medium_G2_Certificate_Templates.pdf	Thu Aug 25 08:27:05 2016
Boeing_SecureBadge_Medium_G3_Certificate_Templates.pdf	Thu Aug 25 08:26:10 2016
Enterprise Production Authority Information	Expires
Boeing_Basic_Assurance_Hardware_Root_CA.crt	Sep 18 21:47:59 2038 GMT
Boeing_Basic_Assurance_Software_Issuing_CA_G3.crt	Jun 29 22:59:40 2026 GMT
Boeing_Basic_Assurance_Software_Root_CA_G2.crt	Apr 21 20:49:09 2036 GMT
Boeing_Class_2_Windows_Machines.crt	Apr 10 05:33:06 2019 GMT
Boeing_Company_OSCA.cer	Nov 23 22:51:06 2016 GMT
Boeing_Company_OSCA.crt	Nov 23 22:51:06 2016 GMT
Boeing_Company_OSCA_G2.crt	Dec 31 23:59:59 2020 GMT
Boeing_Company_OSCA_G3.crt	Jun 1 23:00:45 2026 GMT
Boeing_e-Enabled_Products_Issuing_CA(1).crt	May 1 22:37:08 2019 GMT
Boeing_e-Enabled_Products_Issuing_CA.crt	May 1 22:37:08 2019 GMT
Boeing_e-Enabled_Products_Issuing_CA_G2.crt	Nov 19 20:57:18 2025 GMT
Boeing_e-Enabled_Products_Policy_CA.crt	Aug 28 23:07:56 2028 GMT
Boeing_e-Enabled_Products_Root_CA.crt	Aug 20 23:26:48 2048 GMT
Boeing_Mobile_Device_Issuing_CA_G1.crt	Jun 29 23:01:08 2026 GMT
Boeing_Network_Devices_CA.crt	Oct 11 11:14:22 2016 GMT
Boeing_PCA_G2.crt	Apr 30 23:59:59 2018 GMT
BoeingPCAG2.crt	Apr 30 23:59:59 2018 GMT
BoeingPCAG2.p7c	Apr 30 23:59:59 2018 GMT
Boeing_PCA_G3.crt	Apr 30 23:59:59 2018 GMT
BoeingPCAG3.crt	Apr 30 23:59:59 2018 GMT
BoeingPCAG3.p7c	Apr 30 23:59:59 2018 GMT
Boeing_SecureBadge_Basic_G2.crt	Feb 28 23:00:46 2023 GMT
Boeing_SecureBadge_Medium_G2.crt	Feb 3 19:28:47 2022 GMT
Boeing_Secure_Messaging_G2.crt	Dec 15 00:16:20 2021 GMT
Boeing_Secure_Messaging_G2_Exp_2019.crt	May 30 01:43:26 2019 GMT

You have now successfully downloaded the Boeing Trust Chain Certificates.

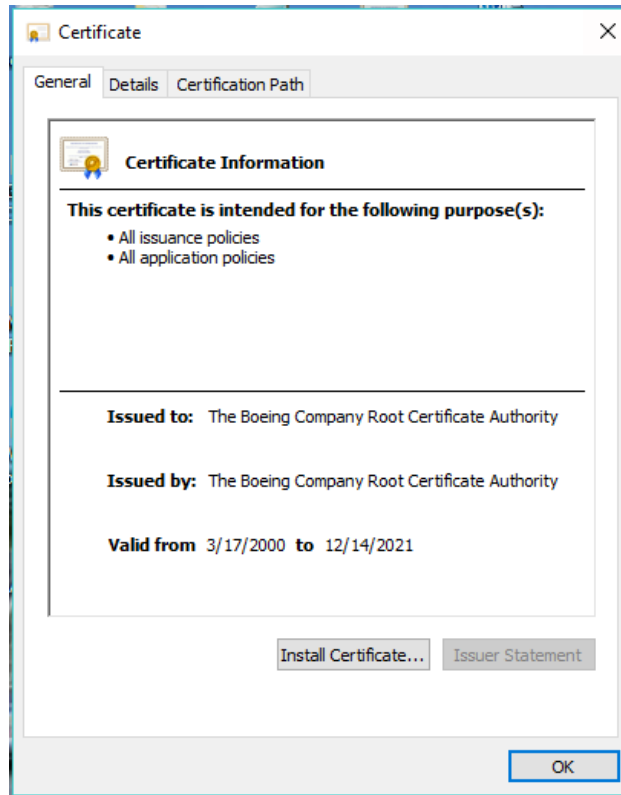
2.2.2 Install the Boeing Root CA Certificate

- Go to the folder where the Boeing Certificates were downloaded. Double-click on **The Boeing Company Root Certificate Authority** certificate and the following window will appear, click on the **Open** button:

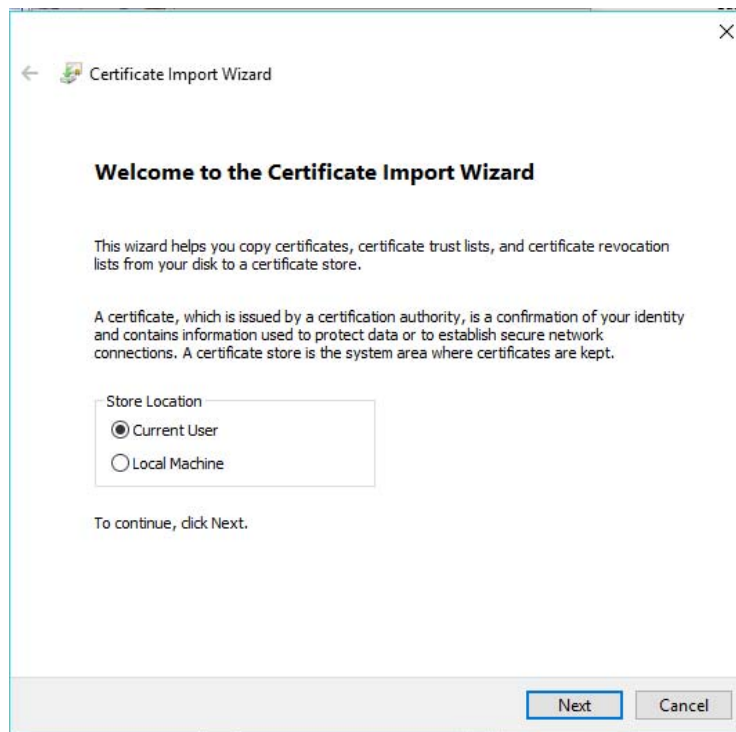




2. Click on the **Install Certificate** button.

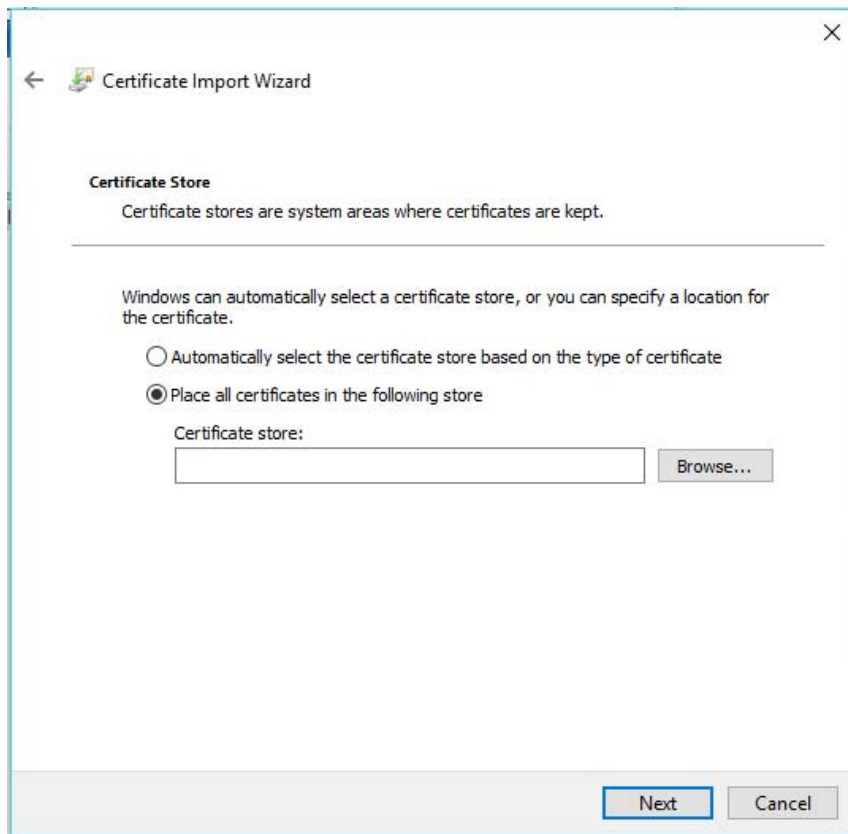


3. The following Certificate Import Wizard window will appear, click on the **Next** button.

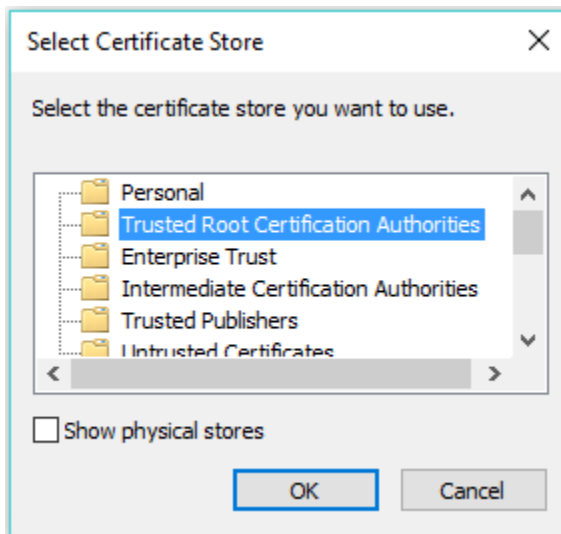




4. Select the **Place all certificates in the following store** option and the click the **Browse** button.

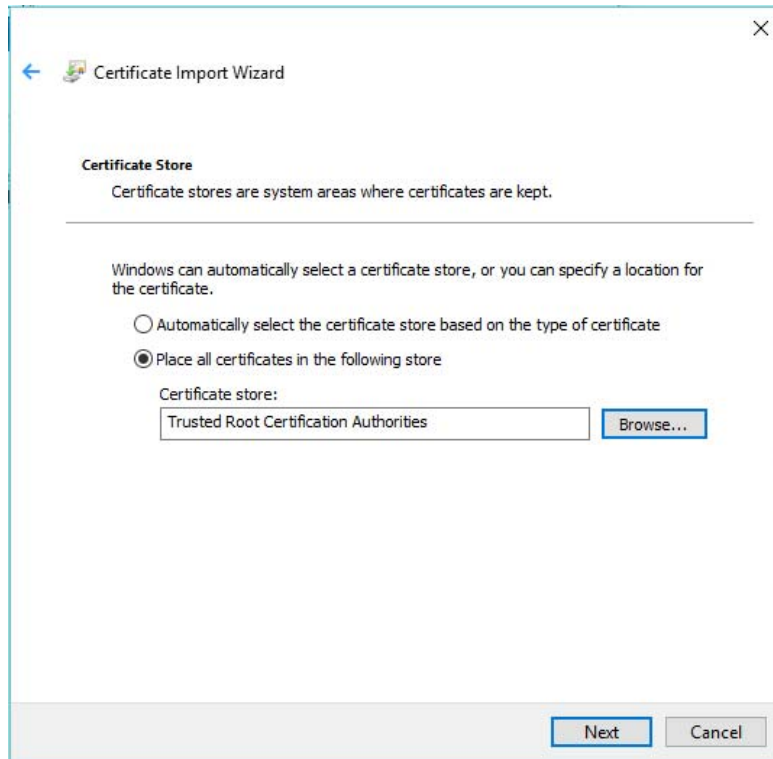


5. The following window will appear, click on **Trusted Root Certification Authorities** and then click **OK**.

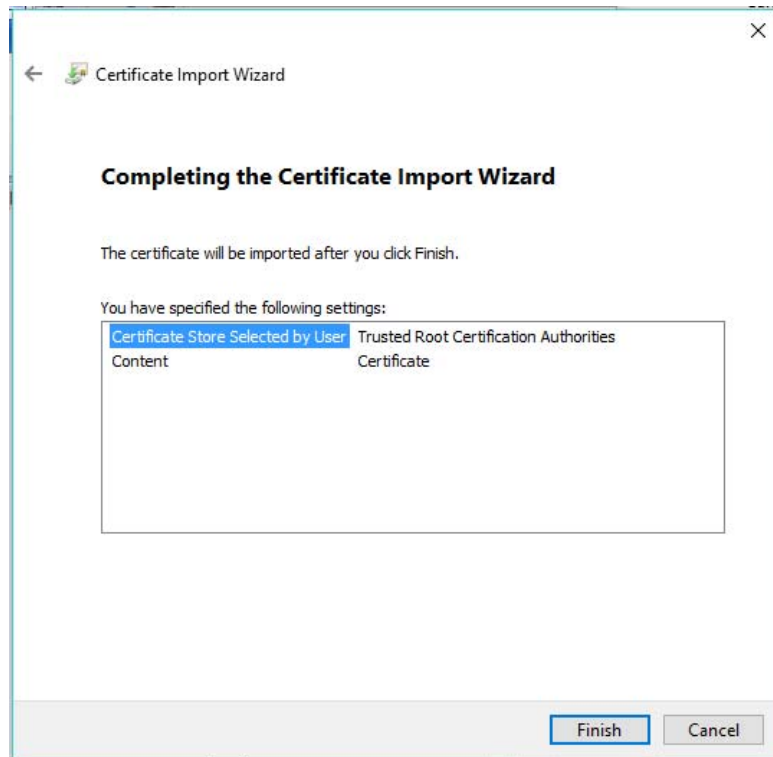




6. The following information will appear in the window, click on the **Next** button.



7. The following window will appear, click on the **Finish** button:

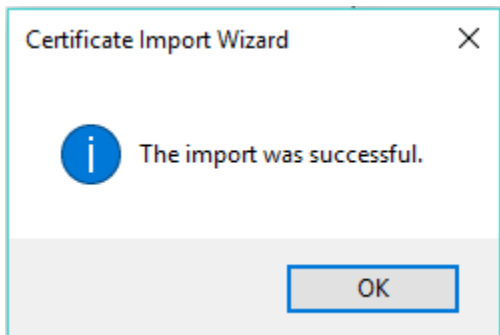




NOTE:

Throughout the installation of the Trust Chain, you will get Security Warning pop-ups. This is normal, as you are installing the certificates for the first time. It is okay to trust and install these certificates.

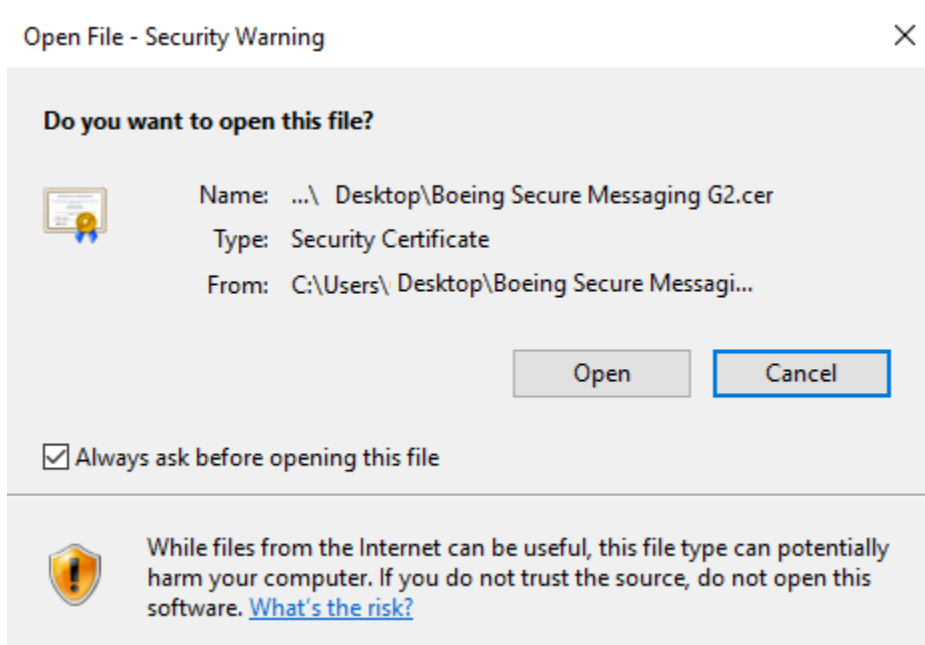
- 8. Click **OK** to complete the installation of the **Boeing Company Root Certificate Authority** certificate.



- 9. Click the **OK** button to close the Certificate window.

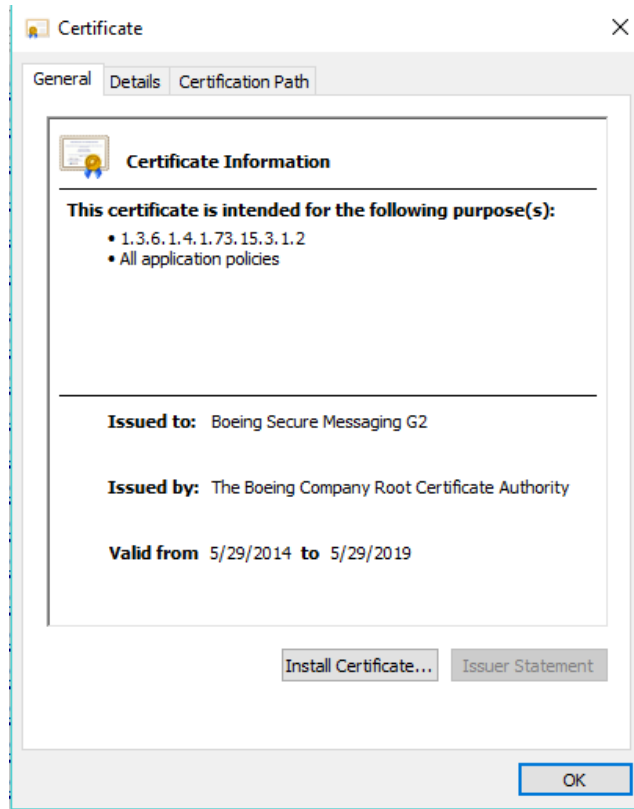
2.2.3 Install Boeing Intermediate CA Certificate

- 1. Go to the folder where the Boeing Certificates were downloaded. Double-click on the **Boeing Secure Messaging G2** certificate and the following window will appear, click on the **Open** button:

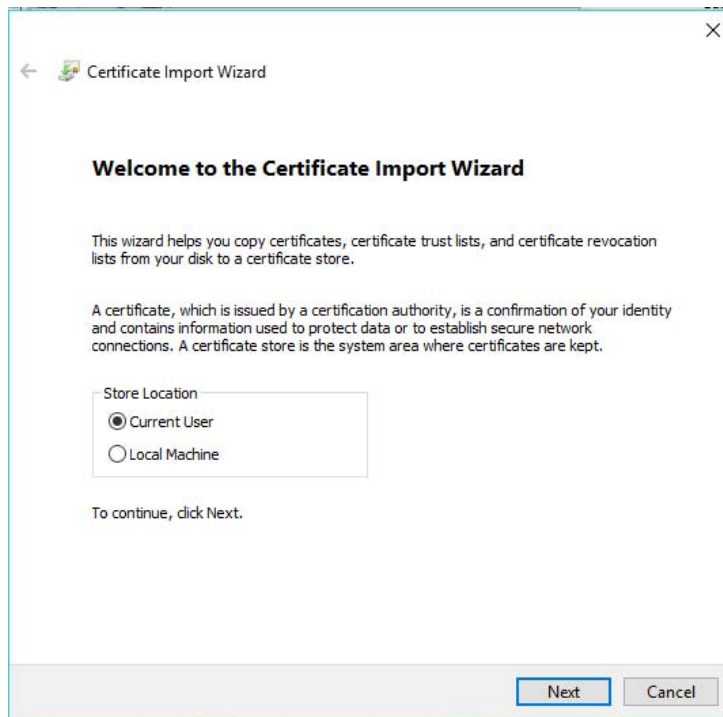




2. Click on the **Install Certificate** button.

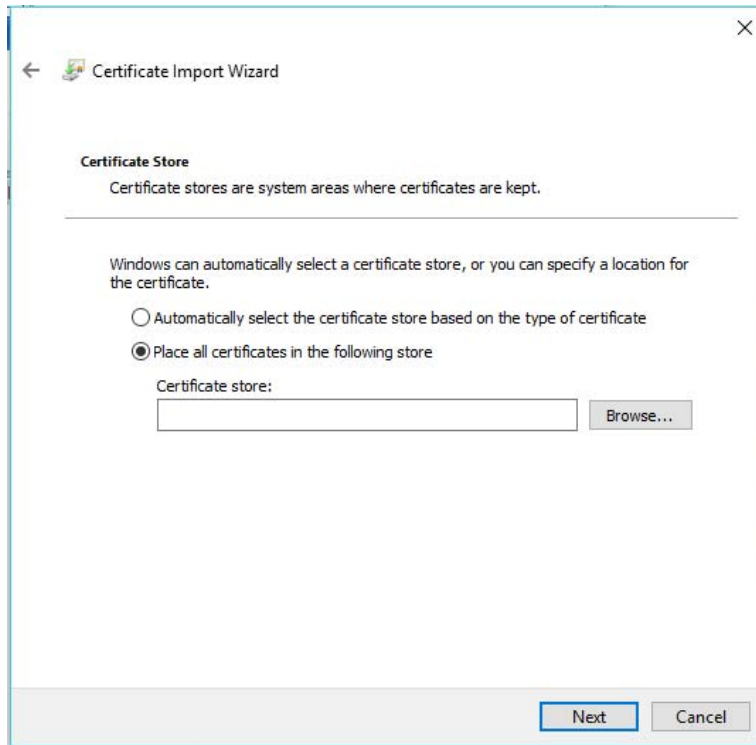


3. The following Certificate Import Wizard window will appear, click on the **Next** button.

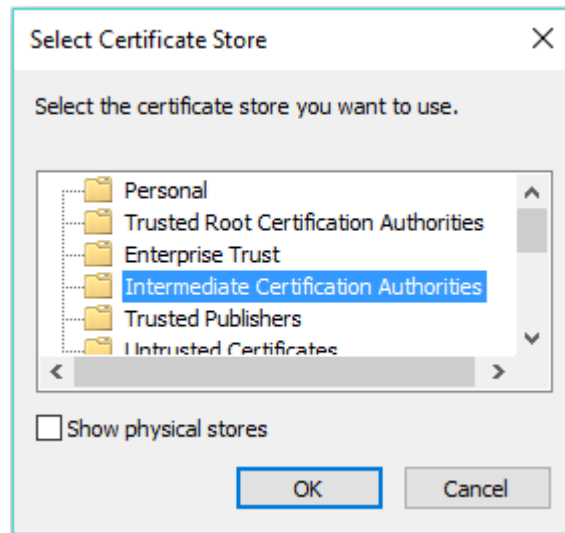




4. Select on the **Place all certificates in the following store** and then click the **Browse** button.

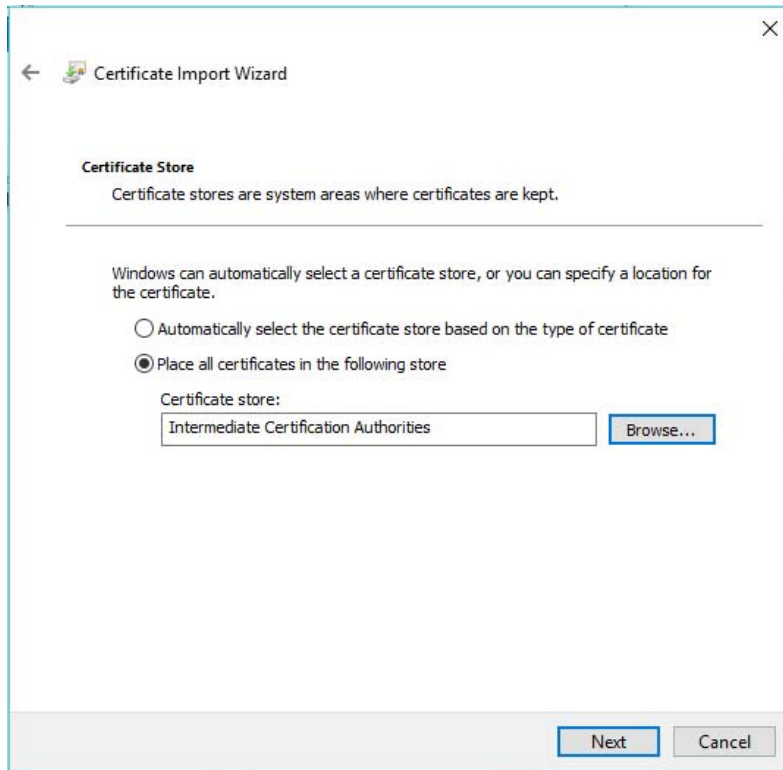


5. Click on **Intermediate Certification Authorities** and then click on the **OK** button.

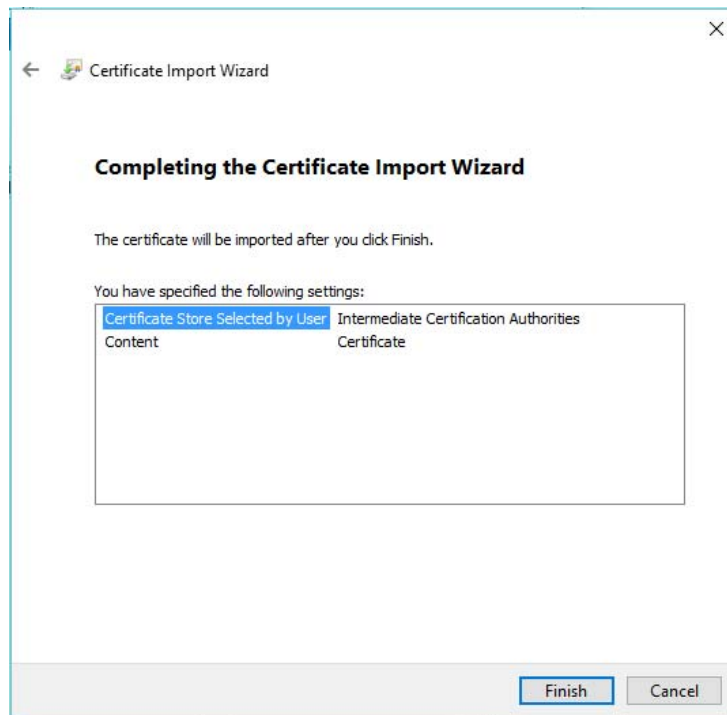




6. The following information will appear in the window, click on the **Next** button.



7. The following window will appear, click on the **Finish** button:

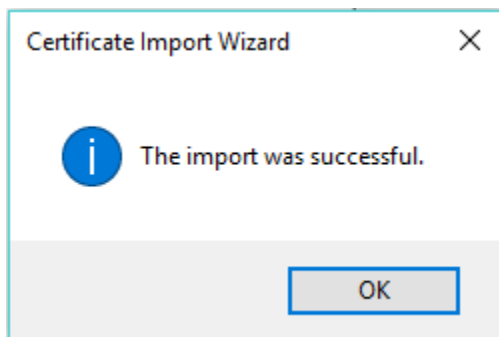




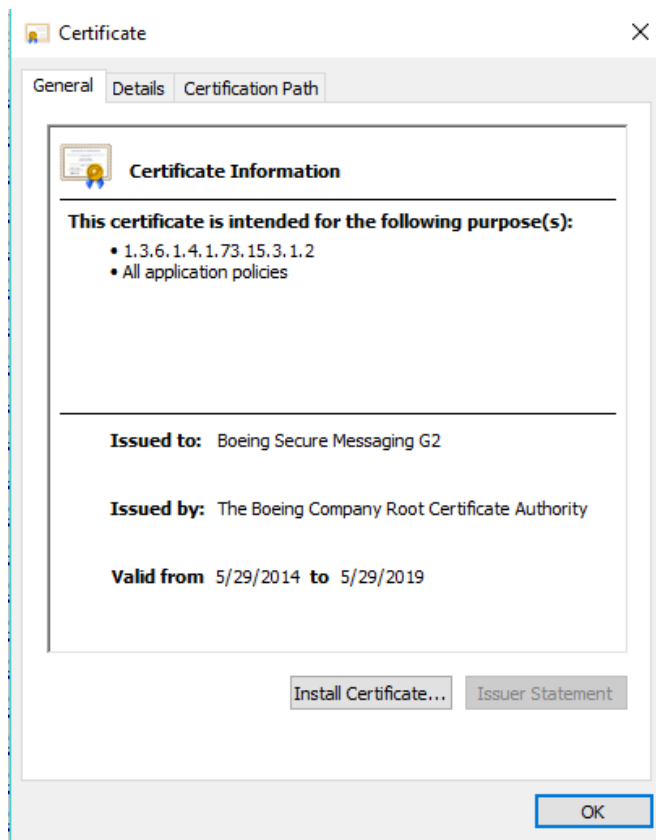
NOTE:

Throughout the installation of the Trust Chain, you may have Security Warning popups. This is normal, as you are installing the certificates for the first time. It is okay to trust and install these certificates.

- 8. Click **OK** to complete the installation of the **Boeing Secure Message G2 Certificate**



- 9. Click the **OK** button to close the certificate window.



***** Repeat steps 1 through 9 to install the Boeing Secure Messaging G2 Exp 2019.crt *****

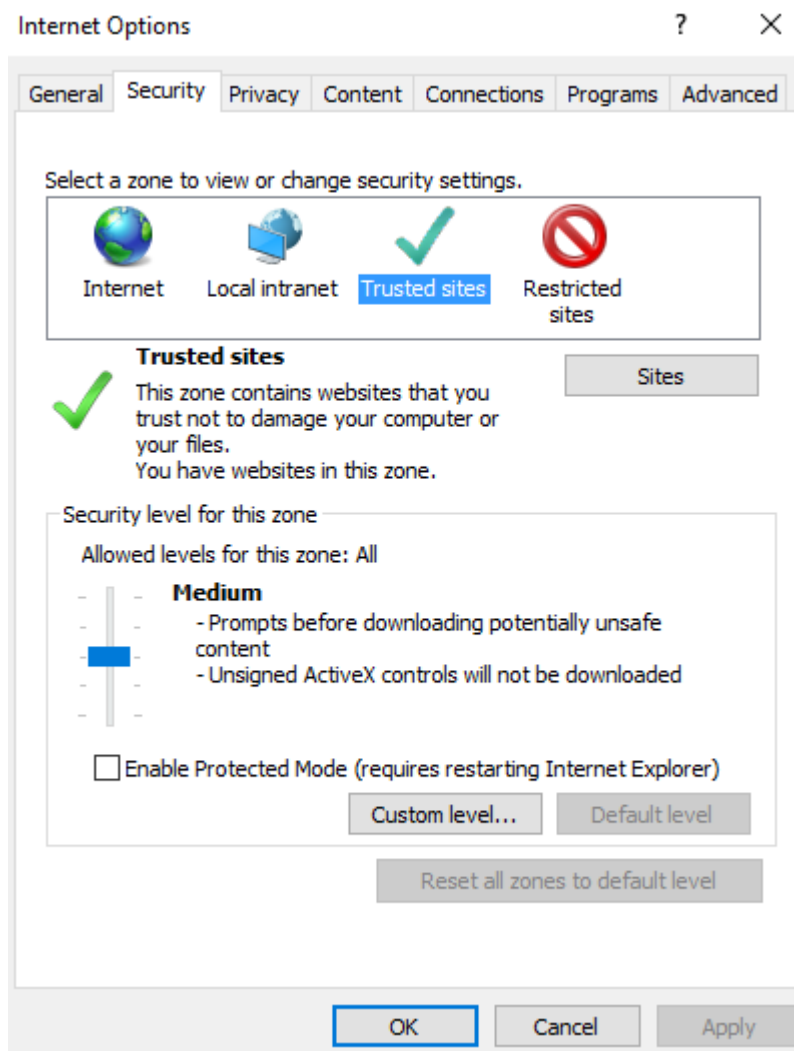




2.3 Verifying the Trusted Site and Validating the EVSSL

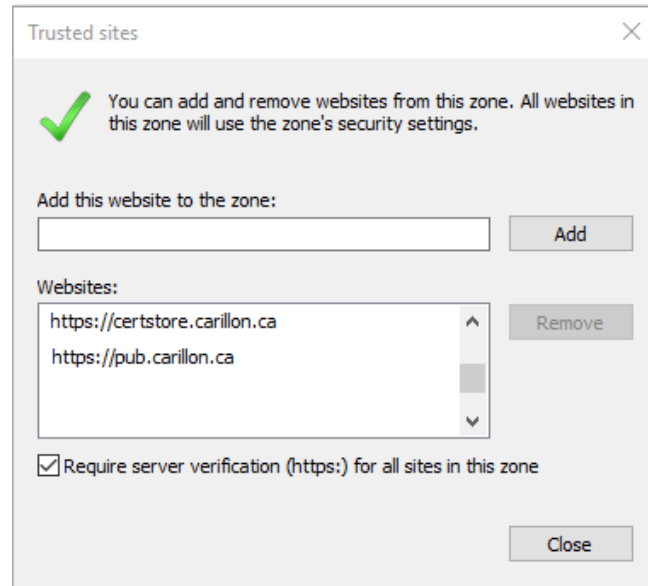
To verify if: <https://pub.carillon.ca/>; <https://www.carillon.ca> and <http://certstore.carillon.ca> are trusted sites on your computer:

1. On the web browser menu click on the **Tools** menu and select **Internet Options**. In the **Internet Options** window, select the **Security** tab.
2. Click on the **Trusted Sites check mark** then click on the **Sites** button.

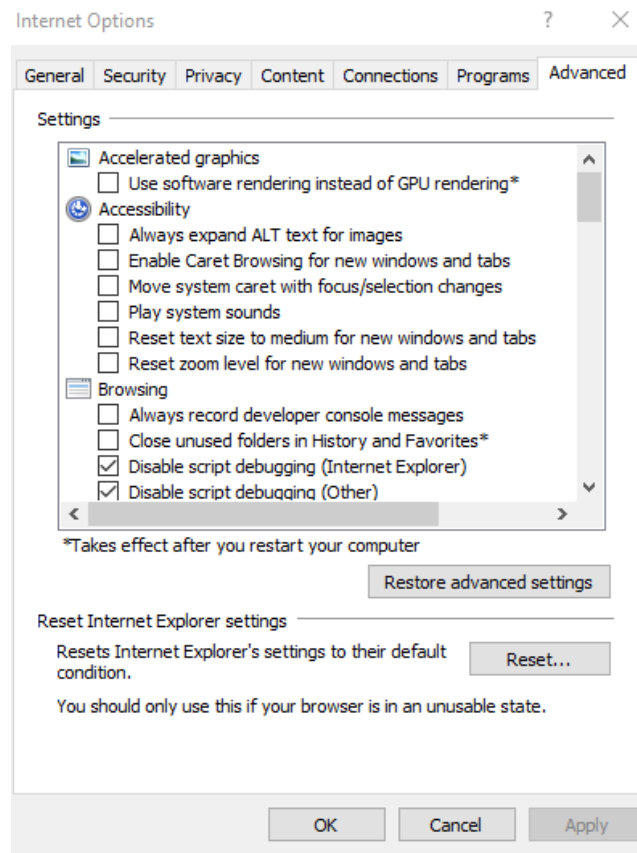




3. If in the box of **Websites** you do not see the above addresses; you will have to click on the **Add** button and add them and then click **Close** button.

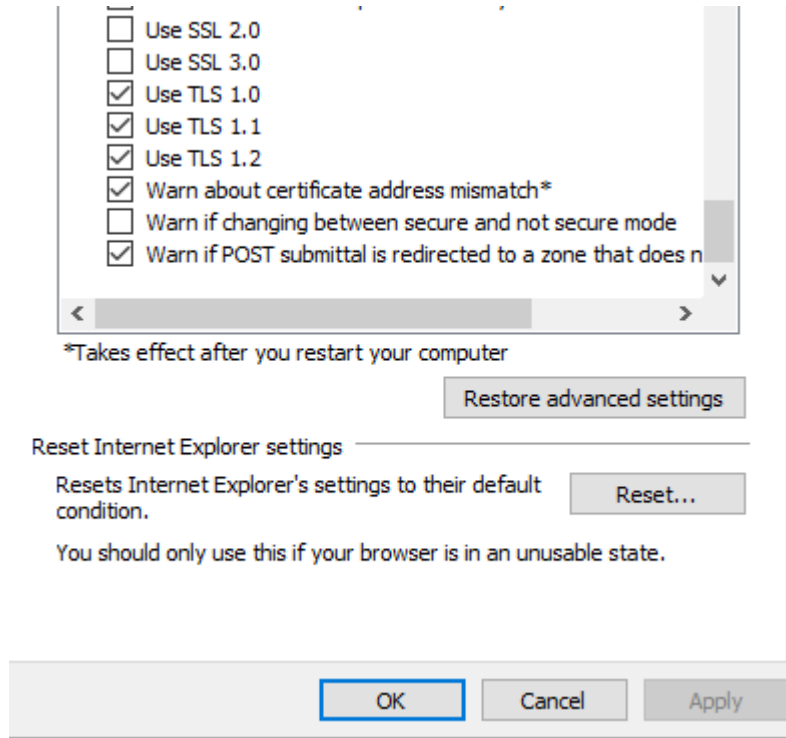


4. On the Internet Options pop-up, click on the **Advanced** tab.

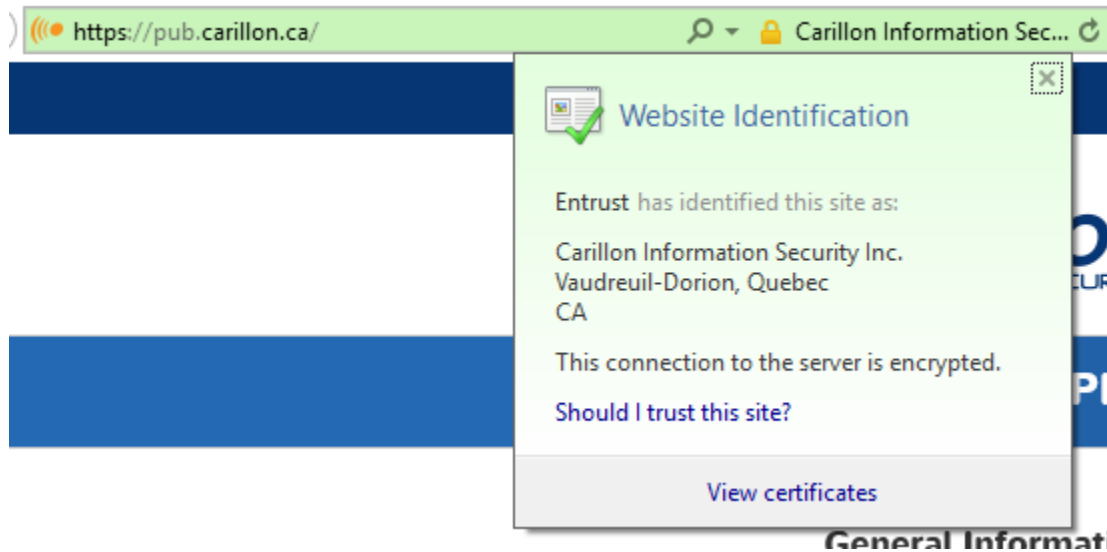




5. In the **Settings** window, scroll down to **Security** and make sure **Use SSL 2.0** and **Use SSL 3.0** are unchecked, and ensure that all the **Use TLS** options are checked, and then click the **OK** button.

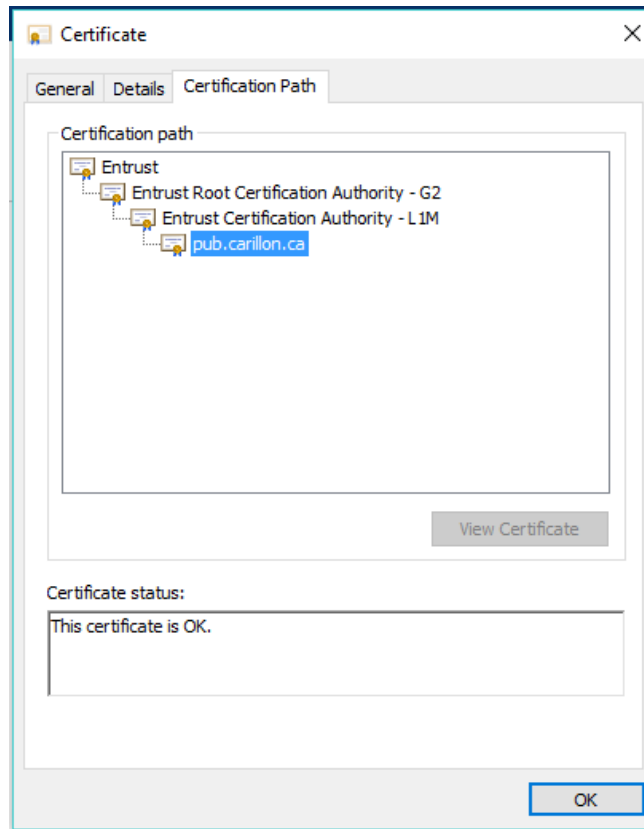


6. In the address bar, type <https://pub.carillon.ca/> and press **Enter**. There will be a lock icon as in the following screenshot. Click the **lock** and click the **View certificates** button.





7. Click the **Certification Path** tab, which shows pub.carillon.ca in the Certification path. The Certificate status should read: **This certificate is OK.**





3 CERTIFICATE RETRIEVAL PROCESS

1. You will receive a Certificate Issuance email (similar to the one below) with instructions, a link to pick up your certificates and an access code. If your email has not arrived after thirty minutes of its request; go to the following link, enter your email address, and click **Request New Access Code**.

<https://pub.carillon.ca/certserv>

Sample email:

Reply Reply All Forward

Thu 11/2/2017 7:59 AM

PKI No Reply <testing@carillon.ca>
Carillon SHA2 TEST PKI: Certificate Issuance

To Testuser Ninety-nine
Signed By testing@carillon.ca

i This message was sent with High importance.

Dear Testuser Ninety-nine:

The request for a Carillon SHA2 TEST PKI digital certificate has been approved. To proceed with the retrieval of your certificate(s), please go to the following URL:

<https://certserv.carillon.ca/certserv>

To log on:
If you already have a valid Identity certificate you will automatically be logged in, otherwise please enter your email address and the access code below:

yvfw89ymjB

If you encounter any difficulties, or have any questions, please do not hesitate to contact us at:

"PKI Help Desk" <testing@carillon.ca>
Thank you,

The Carillon SHA2 TEST PKI Team

NOTE:

Certificate Retrieval is dependent on Java to work. For the best possible results downloading and acknowledging your certificates, it is highly recommended that Internet Explorer, with the latest version of Java, be setup as your default browser on your workstation.

Should your default browser be set to anything other than Internet Explorer, you may need to export the certificates from the other browser to complete the acknowledgement process, or the process will not work altogether.

Should you encounter any issues, please do not hesitate to contact Carillon Customer Service.





- Click on the link mentioned in the email; it will bring you to the following **Certificate Services** page. Enter your email address and click on the **Submit** button.



CERTIFICATE SERVICES

- Check browser setup
- Download CA Certificate Chain

Thank you for registering for a certificate from the Carillon SHA2 TEST PKI. Log in here to generate a private key and certificate request which will then be securely transmitted to our Certificate Authority for signing.

Please enter your **email address** and the **access code** that was emailed to you.

If you have **lost** your access code, enter **only** your email address and a new code will be emailed to you.

Email Address:

SUBMIT

Please [contact us](#) if you have any questions about this service, or problems using issued certificates.

System Messages

Posted	Message
2016-05-19	If you have any questions or concerns, please contact us at customer_service@carillon.ca or 1.844.PKI.PIVI (1.844.754.7484)
Other OA	Option 2.

- Enter the **Access Code** from the email and click on the **Log In and Retrieve Certificates** button:



CERTIFICATE SERVICES

- Check browser setup
- Download CA Certificate Chain

Thank you for registering for a certificate from the Carillon SHA2 TEST PKI. Log in here to generate a private key and certificate request which will then be securely transmitted to our Certificate Authority for signing.

Please enter your **email address** and the **access code** that was emailed to you.

If you have **lost** your access code, enter **only** your email address and a new code will be emailed to you.

Email Address:

SUBMIT

Please [contact us](#) if you have any questions about this service, or problems using issued certificates.

HELLO TESTUSER NINETY NINE

You are scheduled to retrieve certificates. Please enter the access code you received by email and press the button to continue.

Access Code (from email):

LOG IN AND RETRIEVE CERTIFICATES





4. Click on the Pick up your certificates button.

WELCOME, TESTUSER NINETYNINE.

You've used a one-time password to access this page. In the future, access to this page will be supported by the Identity certificate that you will shortly be retrieving, issued by the Carillon SHA2 TEST PKI.


[Return to Main Page](#)

[Check browser setup](#)

[Download CA Certificate Chain](#)

Your certificates:

 **Identity** - - Waiting for pickup

 **Signature** - - Waiting for pickup

 **Encryption** - - Waiting for pickup

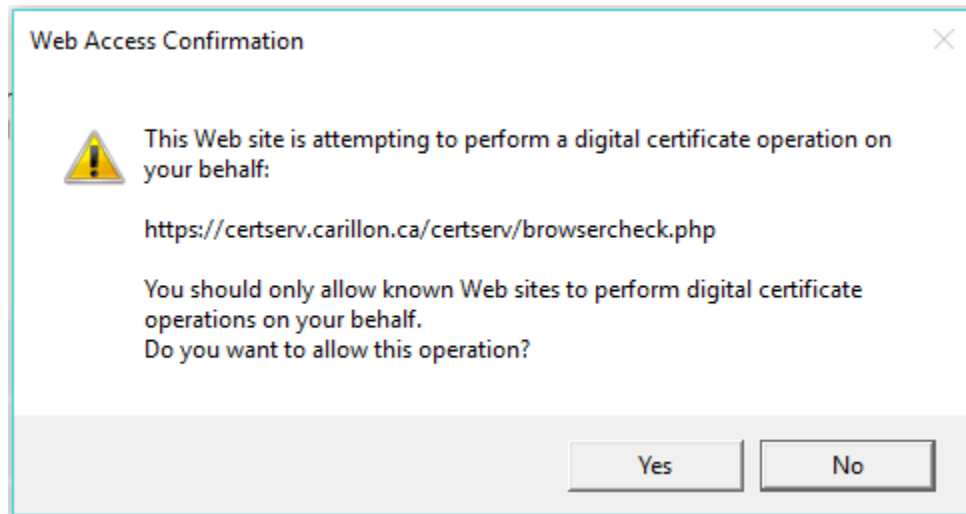
PICK UP YOUR CERTIFICATES

Encryption Key Recovery

You have (or have had in the past) encryption certificates. In order to decrypt data, you may need to recover a certificate and private key if you no longer have them. Please click the 'Encryption Key Recovery' button to access this feature.

ENCRYPTION KEY RECOVERY



5. Click **Yes**:





- 6. Your browser will be checked, then click on the Continue button.

[CONTACT](#)

CHECKING YOUR BROWSER SETUP...


Before you can retrieve your certificates, we need to ensure your web browser meets certain requirements and is correctly configured. If these tests do not succeed, unfortunately you will not be able to retrieve your certificates at this time.

Test for valid browser:	PASSED
Test for session cookies:	PASSED
Test for persistent cookies:	PASSED
Test for Java >= 1.6:	PASSED
Test for Javascript:	PASSED
Testing system time:	WARNING (Your system time is 27 seconds fast)
Test for MS enrollment object:	PASSED (CertEnroll found)
Overall result:	PASSED

This concludes the browser compatibility check. You may press "Go Back" to return to the main page.

[GO BACK](#)



It appears that you have the correct Java version installed.



[PRIVACY](#) [REPOSITORY](#)

CertServ v4.4.28 (p21439) Copyright © 2016 Carillon Information Security Inc., All rights reserved.

- 7. Read and confirm the Terms of Service and place a check in the **I hereby accept the terms of service** box and then click **Continue**.

HELLO TESTUSER NINETYNINE.

Terms of Service

By using this service, the Subscriber agrees that he has read and understood the applicable Subscriber Agreement and/or Certificate Policy, and that Certificates generated herein are to be used in accordance with those documents. Furthermore, the Subscriber, and/or the Subscriber's Employer, agrees to indemnify Carillon against any and all claims that may arise due to the Subscriber's use of this certificate.

[Subscriber Agreement](#)

Please confirm the Terms of Service:

I hereby accept the terms of service.

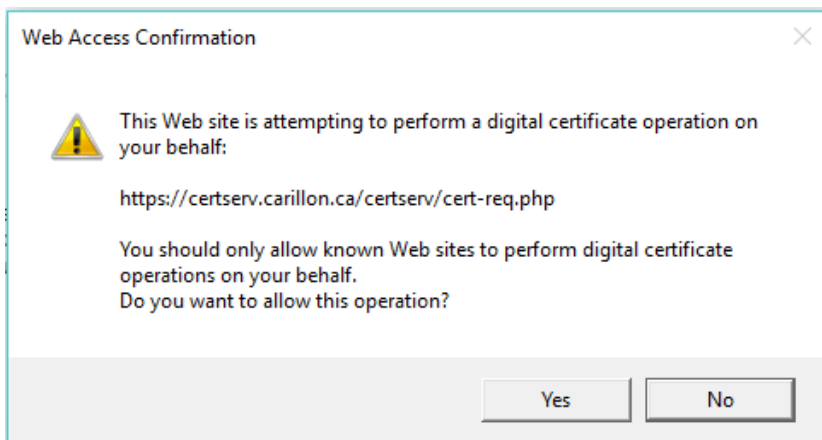
[CONTINUE](#)

- [Return to Main Page](#)
- [Check browser setup](#)
- [Download CA Certificate Chain](#)





8. Click **Yes**:



9. The following screen will appear, click on the **Continue** button.



We will generate a request for each of your certificate(s) with the following name. The certificate type will be appended to your name.

Subject:
C=CA
O=Carillon Information Security Inc.
OU=Subscribers
OU=Carillon
CN=Testuser Ninety-nine - [ID SIG or ENC]
serialnumber=4200000209

Certificates to be issued:
Identity at Basic Software 256
Signature at Basic Software 256
Encryption at Basic Software 256

- [Return to Main Page](#)
- [Check browser setup](#)
- [Download CA Certificate Chain](#)

CONTINUE

10. The generating certificates screen will appear.



PLEASE WAIT...

Your certificates are being generated, and will be installed when ready. This should only take a few seconds.

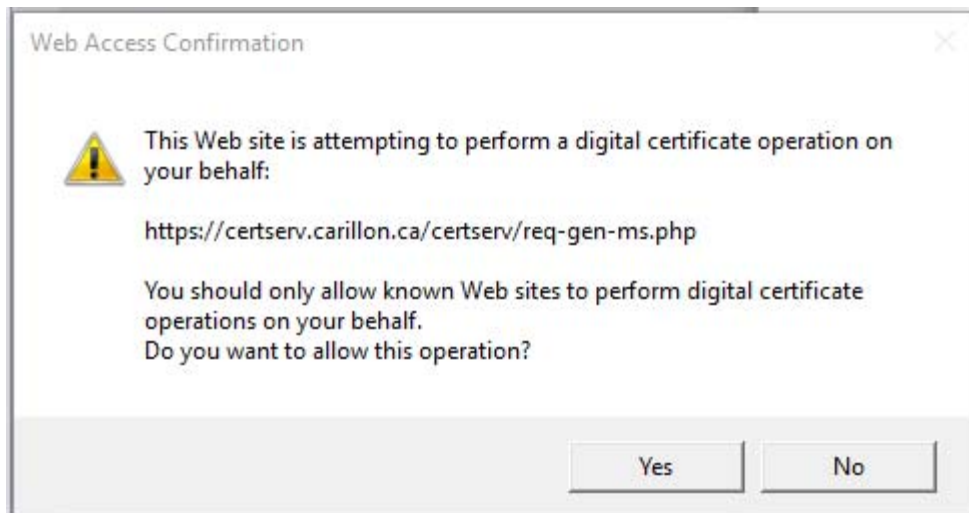
- [Return to Main Page](#)
- [Check browser setup](#)
- [Download CA Certificate Chain](#)

Fetching Signature certificate...
Fetching Encryption certificate...





11. You will have to Click **Yes** a few times:



IMPORANT NOTE:

If you have been requested for Medium level certificates (Medium Software 256) you will need to remember and enter the retrieval code you submitted on your Digital Credential Request Form (DCR).

12. Your certificates have now been retrieved and installed. Before restarting your browser, you must first download the Encryption Certificate. Click on the **DOWNLOAD CERTIFICATE** button.



ALL DONE.

Your certificates are being generated, and will be installed when ready. This should only take a few seconds.

ENCRYPTION CERTIFICATE:

This link works only **once**, please be sure to **Save the certificate** when prompted.

You will receive a password by email to unlock this file.

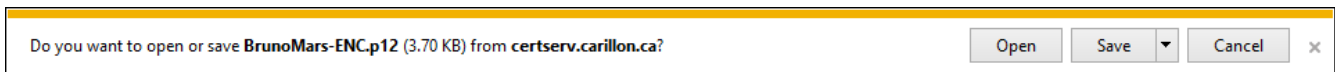
DOWNLOAD CERTIFICATE

After all certificates have been retrieved and installed, you will receive email with instructions to acknowledge your certificates.

You must RESTART YOUR BROWSER before acknowledging.

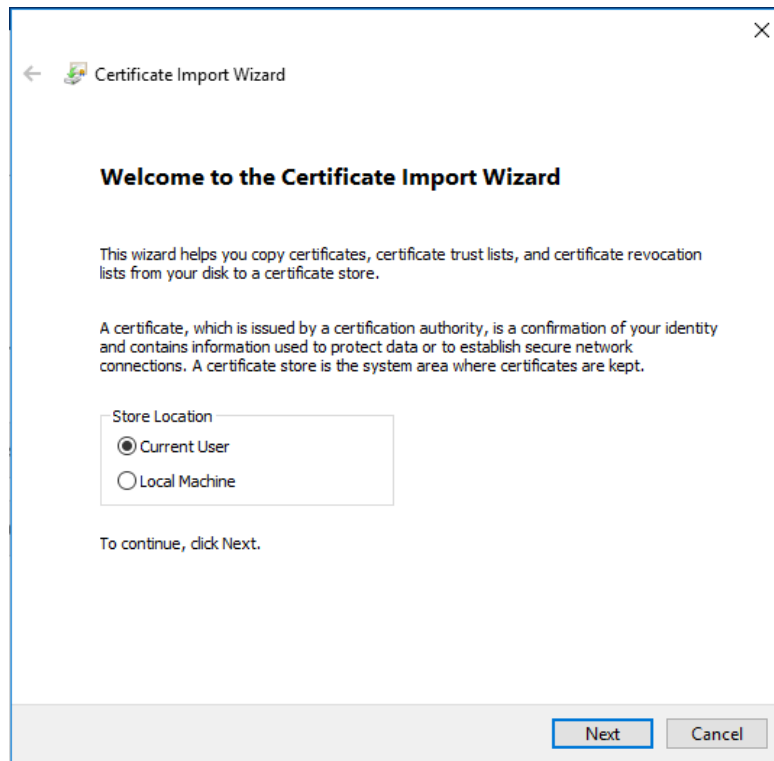
- [Return to Main Page](#)
- [Check browser setup](#)
- [Download CA Certificate Chain](#)

13. You will see a popup window at the bottom of your screen similar to the following; expand on the **Save** button and then click **Save and Open**:

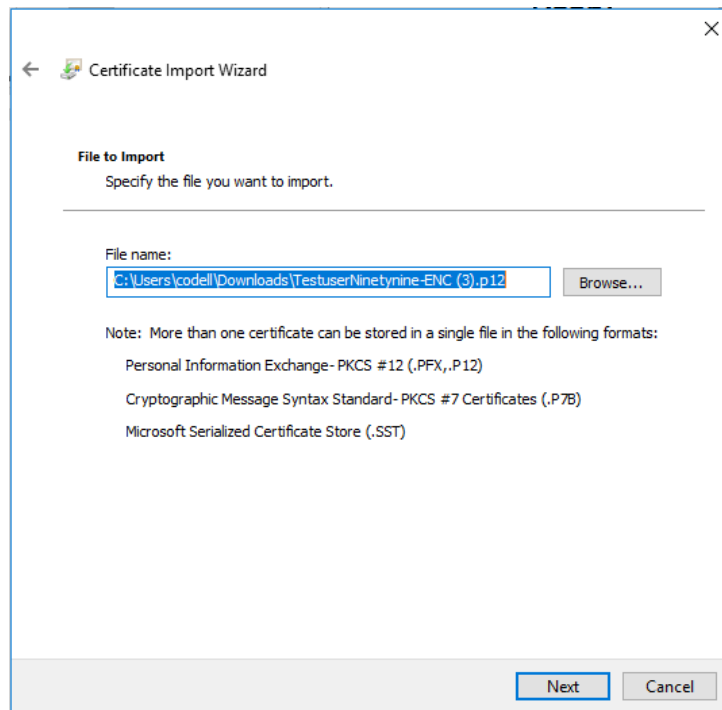




14. On the Certificate Import Wizard window, leaving the store location as Current, click next.



15. Click next on the following popup.





16. On the Private key protection popup window, enter the password (24 Alpha-Numeric password) in the Carillon PKI: Encryption Key Password email that you received.

The screenshot shows the 'Certificate Import Wizard' window. The title bar reads 'Certificate Import Wizard'. The main heading is 'Private key protection'. Below it, the text says 'To maintain security, the private key was protected with a password.' A horizontal line separates this from the next section, 'Type the password for the private key.' There is a 'Password:' label above a text input field containing 24 dots. Below the input field is a checkbox labeled 'Display Password'. Another horizontal line separates this from the 'Import options:' section. It contains three checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.' (unchecked), 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.' (unchecked), and 'Include all extended properties.' (checked). At the bottom right, there are 'Next' and 'Cancel' buttons.

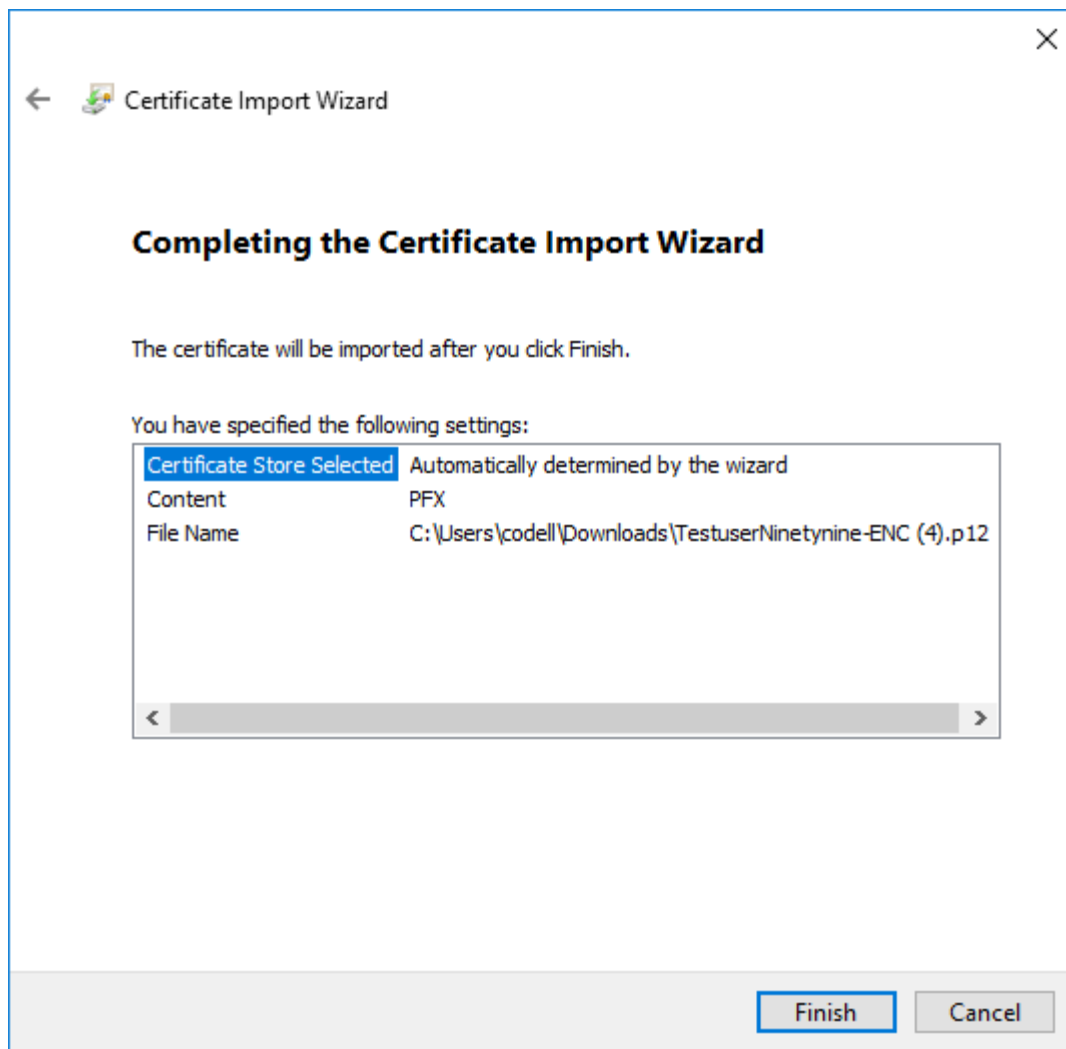
17. On the Certificate Store popup window click next, leaving the "Automatically select the certificate store based on the type of certificate" selected.

The screenshot shows the 'Certificate Import Wizard' window. The title bar reads 'Certificate Import Wizard'. The main heading is 'Certificate Store'. Below it, the text says 'Certificate stores are system areas where certificates are kept.' A horizontal line separates this from the next section, 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' There are two radio buttons: 'Automatically select the certificate store based on the type of certificate' (selected) and 'Place all certificates in the following store'. Below the radio buttons is a 'Certificate store:' label above a text input field and a 'Browse...' button. At the bottom right, there are 'Next' and 'Cancel' buttons.

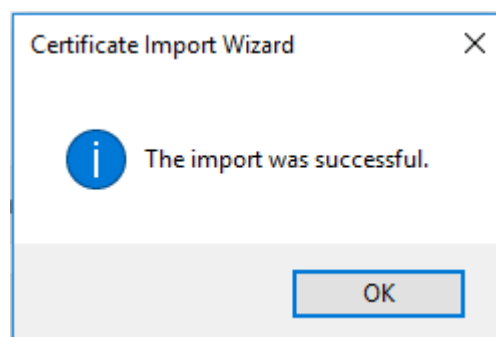




18. Click Finish on the Completing the Certificate Import Wizard popup.



19. Click OK on the Certificate Import Wizard: The import was successful popup.

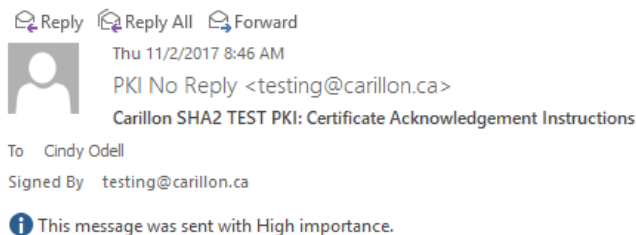




4 THE ACKNOWLEDGING PROCESS

You will receive two emails: a **Certificate Acknowledgement Instructions** email and an **Encryption Acknowledgement Code** email.

1. **OPEN** the **Certificate Acknowledgement Instructions** email (similar to the following) to acknowledge your certificates; then click on the link which will bring you to a **Windows Security** page.



Dear Testuser Ninetynine:

Thank you for retrieving your certificates from the Carillon SHA2 TEST PKI.

In order to keep and use your certificates, it is now necessary to validate that they are working properly; therefore, you must acknowledge them within 1 month of receipt.

To acknowledge your certificates, ensure that you have CLOSED all your Internet browser windows and then go to this URL:

<https://certserv.carillon.ca/certserv/acknowledge/>

IMPORTANT NOTE: If you have requested and retrieved an Encryption certificate, you will have received a second, encrypted email. This encrypted email contains a code which is needed to complete the acknowledgement for your encryption certificate.

To be able to read the encrypted email, you will need to double-click on it, so that it is opened in a separate window. It is NOT possible to read an encrypted email in the Outlook preview window.

If you encounter any difficulties, or have any questions, please do not hesitate to contact us at:

"PKI Help Desk" <testing@carillon.ca>
Thank you,

The Carillon SHA2 TEST PKI Team





2. Select your ID certificate with the Issuer: CIS and then click **OK**.



3. The following window will appear. Click on the **I acknowledge** button to acknowledge your **Signature Certificate**.



ACKNOWLEDGEMENT

Identity Certificate Acknowledgement

You have successfully generated your certificates, and used your Identity certificate to view this page. Therefore, your Identity certificate is now acknowledged.

Signature Certificate Acknowledgement

By clicking below, you will be using your Signature certificate to sign your acknowledgement of receipt of your Signature certificate.

ACKNOWLEDGE SIGNATURE CERTIFICATE

Encryption Certificate Acknowledgement

You have been sent an encrypted email with an acknowledgement code in it. Please type this code below, and click "I acknowledge".

You can also request another copy of the encrypted code by clicking "Send email again".

Acknowledgement Code:

I ACKNOWLEDGE

SEND EMAIL AGAIN

- [Return to Main Page](#)
- [Test My Certificate](#)
- [Check browser setup](#)
- [Download CA Certificate Chain](#)





4. Enter your **Acknowledgement Code** from your Encryption Acknowledgement Code email and click on the **I acknowledge** button.



ACKNOWLEDGEMENT

Identity Certificate Acknowledgement

You have successfully generated your certificates, and used your Identity certificate to view this page. Therefore, your Identity certificate is now acknowledged.

Signature Certificate Acknowledgement

Your Signature certificate has been acknowledged.

Encryption Certificate Acknowledgement

You have been sent an encrypted email with an acknowledgement code in it. Please type this code below, and click "I acknowledge".

You can also request another copy of the encrypted code by clicking "Send email again".

Acknowledgement Code:

I ACKNOWLEDGE **SEND EMAIL AGAIN**

- [Return to Main Page](#)
- [Test My Certificate](#)
- [Check browser setup](#)
- [Download CA Certificate Chain](#)





5. Your certificates have now been acknowledged.



ACKNOWLEDGEMENT

Identity Certificate Acknowledgement

You have successfully generated your certificates, and used your Identity certificate to view this page. Therefore, your Identity certificate is now acknowledged.

Signature Certificate Acknowledgement

Your Signature certificate has been acknowledged.

Encryption Certificate Acknowledgement

Your Encryption certificate has been acknowledged.

- [Return to Main Page](#)
- [Test My Certificate](#)
- [Check browser setup](#)
- [Download CA Certificate Chain](#)

6. Click on the **Return to main Page** option from the menu bar; you will now see serial numbers beside your issued certificates.



WELCOME, TESTUSER NINETYNINE.

This personalized greeting confirms the validity of your certificate, issued by the Carillon SHA2 TEST PKI.

Your certificates:

Identity -- Serial number: 020178DF4DEB6397ADCAC8FBF33E31CCA103, issued 2017-11-02 -	Revoke
Signature -- Serial number: 02013A3961698640BBB4C9F3D69028E7A02D, issued 2017-11-02 -	Revoke
Encryption -- Serial number: 02016F480E6BF48BF6880AC6A88B7329E686, issued 2017-11-02 -	Revoke

[RE-KEY ALL YOUR CERTIFICATES](#)

Encryption Key Recovery

You have (or have had in the past) encryption certificates. In order to decrypt data, you may need to recover a certificate and private key if you no longer have them. Please click the 'Encryption Key Recovery' button to access this feature.

[ENCRYPTION KEY RECOVERY](#)

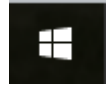
- [Return to Main Page](#)
- [Test My Certificate](#)
- [Check browser setup](#)
- [Download CA Certificate Chain](#)



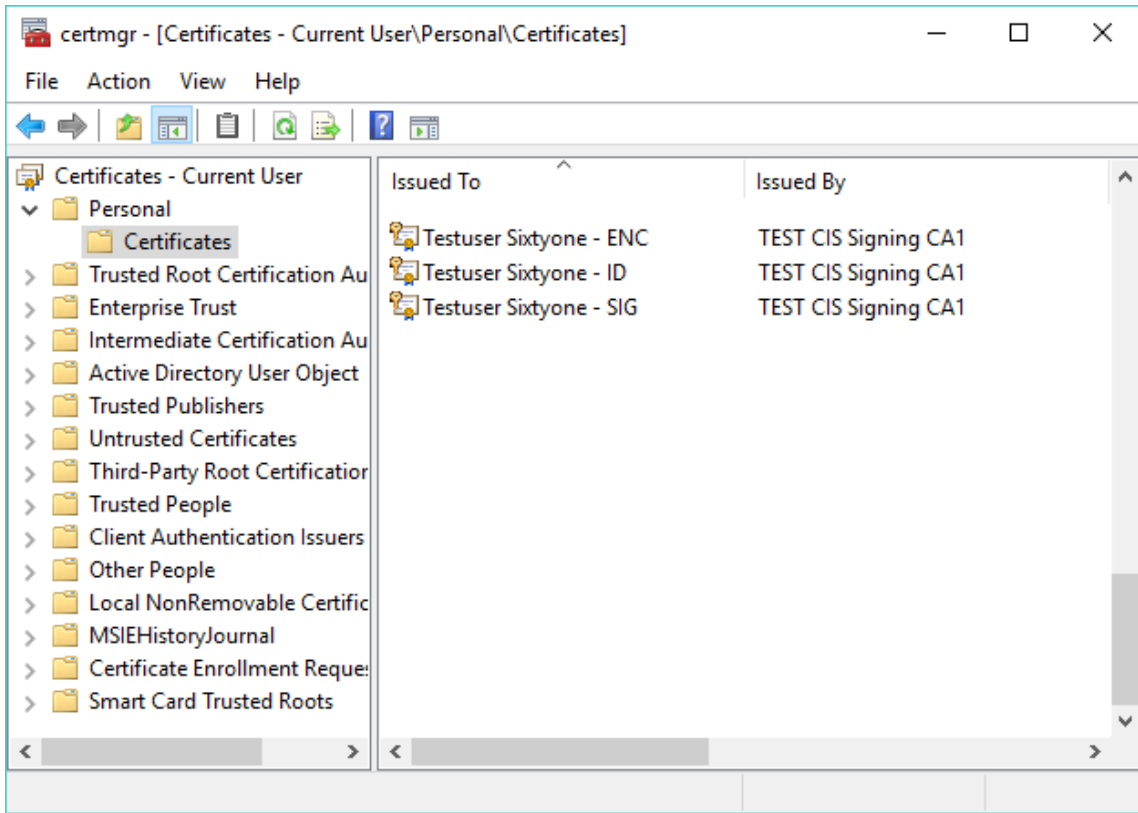


5 HOW TO EXPORT ID, SIG, & ENC CERTIFICATES

5.1 Export ID, SIG & ENC Certificates from Your Personal Store

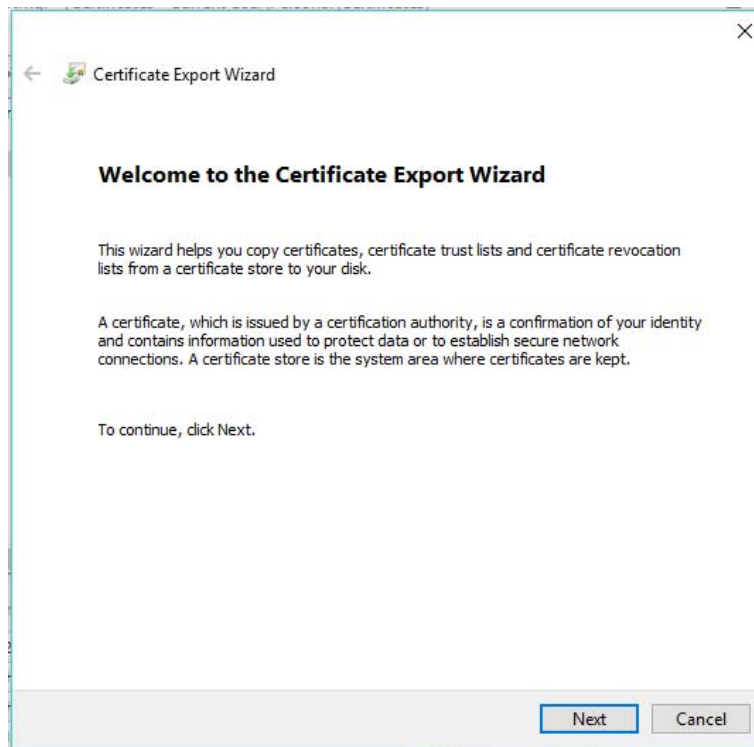


1. Click on the Start icon:
2. Type in the search box: certmgr.msc and press enter; the **certmgr – Certificates** screen will appear.
3. Under: Personal > Certificates highlight the three certificates you want to export; right click on them, then click on **All Tasks** and click on **Export**.

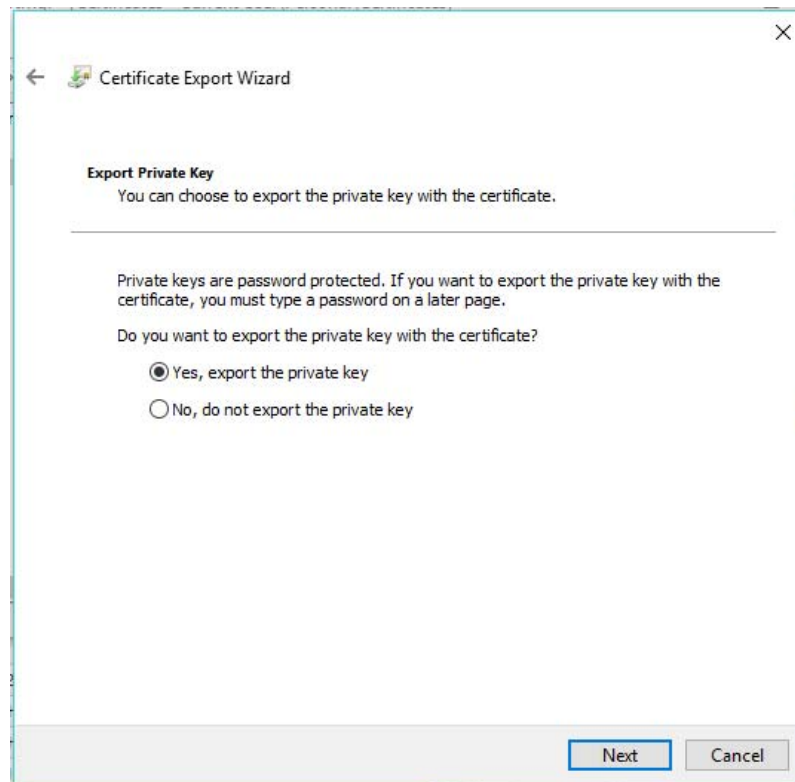




4. The Certificate Export Wizard will appear; click **Next**.



5. On the Export Private Key screen; click on **Yes, export the private key**. Click **Next**.





- The **Export File Format** screen will appear; ensure that the **Personal Information Exchange – PKCS #12(.PFX)** button is highlighted; click **Next**.

The screenshot shows the 'Certificate Export Wizard' window. The title bar reads 'Certificate Export Wizard'. Below the title bar, there is a back arrow and a small icon. The main content area is titled 'Export File Format' and contains the text 'Certificates can be exported in a variety of file formats.' Below this, there is a section 'Select the format you want to use:' with several radio button options: 'DER encoded binary X.509 (.CER)', 'Base-64 encoded X.509 (.CER)', 'Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)', 'Personal Information Exchange - PKCS #12 (.PFX)' (which is selected), and 'Microsoft Serialized Certificate Store (.SST)'. Under the 'Personal Information Exchange - PKCS #12 (.PFX)' option, there are three checkboxes: 'Include all certificates in the certification path if possible', 'Delete the private key if the export is successful', and 'Export all extended properties'. There are also two checkboxes for 'Enable certificate privacy'. At the bottom right, there are 'Next' and 'Cancel' buttons.

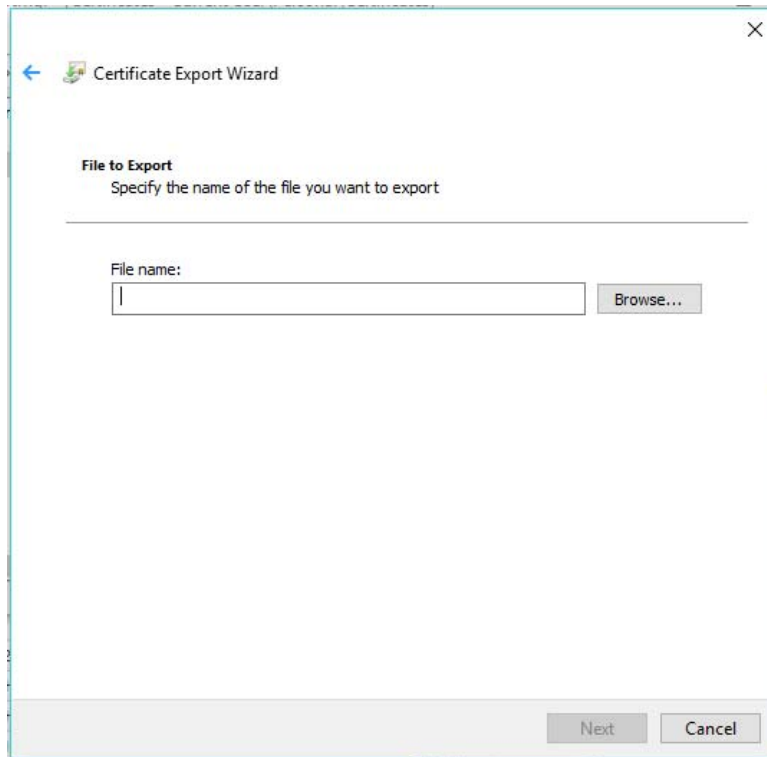
- On the **Password** Screen; create a password and retype it; then click **Next**.

The screenshot shows the 'Certificate Export Wizard' window. The title bar reads 'Certificate Export Wizard'. Below the title bar, there is a back arrow and a small icon. The main content area is titled 'Security' and contains the text 'To maintain security, you must protect the private key to a security principal or by using a password.' Below this, there is a checkbox for 'Group or user names (recommended)'. To the right of this checkbox is a list box with 'Add' and 'Remove' buttons. Below the list box, there is a checked checkbox for 'Password:'. To the right of this checkbox is a password input field with a masked password '••••••'. Below this is a 'Confirm password:' label and another password input field with a masked password '••••••'. At the bottom right, there are 'Next' and 'Cancel' buttons.

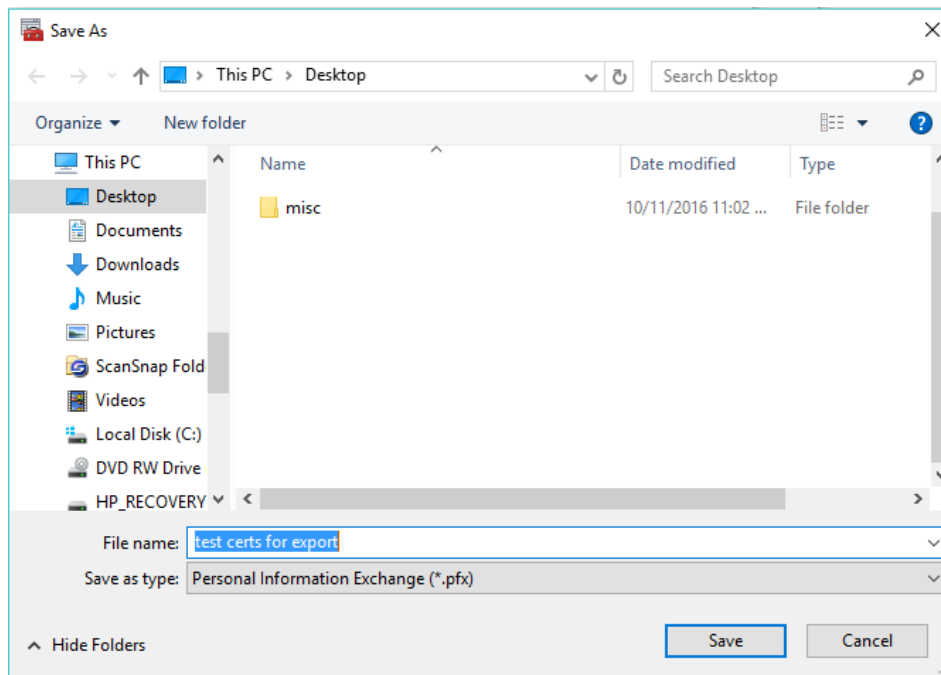




8. The **File to Export** screen will appear showing the file name to export; click **Browse**.

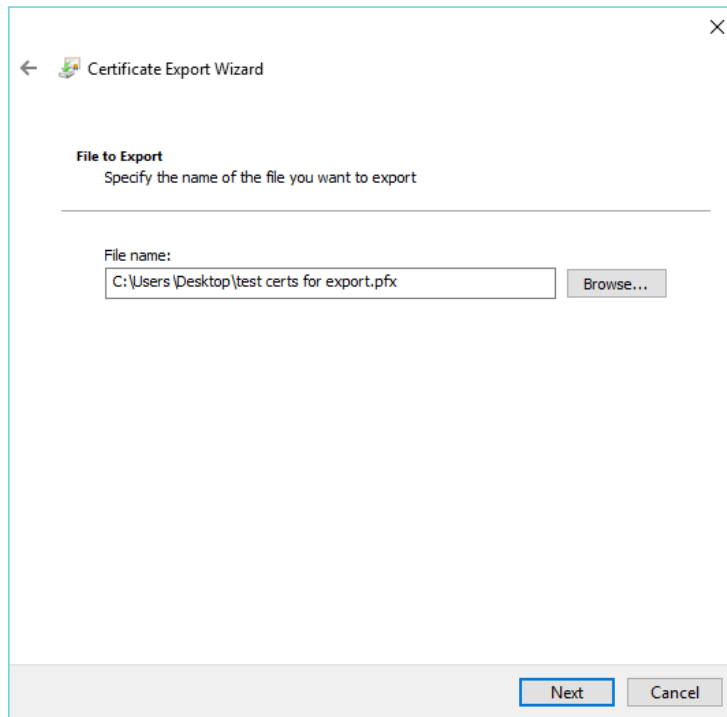


9. The **Save As** window will appear; name the file and then save it to wherever you want i.e.: desktop and then click **Save**.

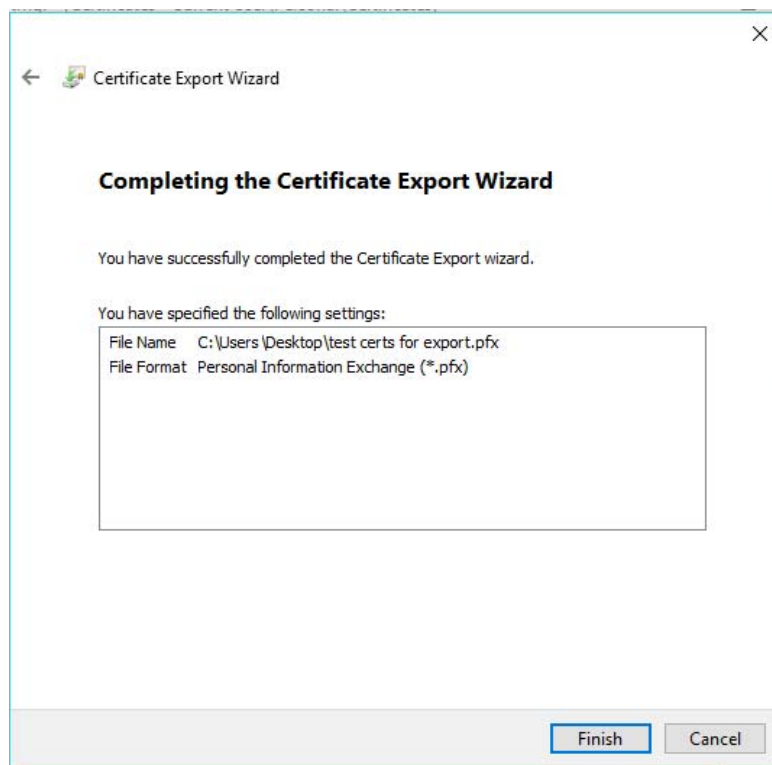




10. Click on the Next button.

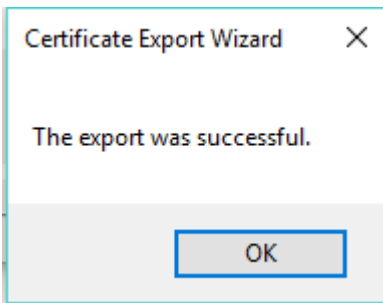


11. The Certificate Export Wizard window will appear; click **Finish**.





12. On the **Certificate Export Wizard** pop-up advising the export was successful; click **OK**.



5.2 Deletion of Certificates from Hard Drive

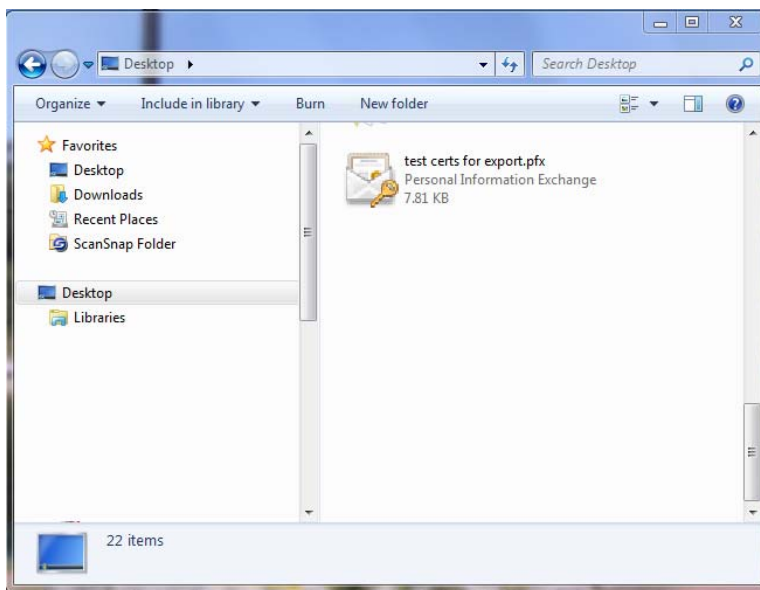
Any files containing your private key should be kept on removable media only. When first exporting your certificates, copy them to a local drive that is not accessible to a network. Import your certificates into applications as necessary, *then remove them and any related files from your machine after you're done!*

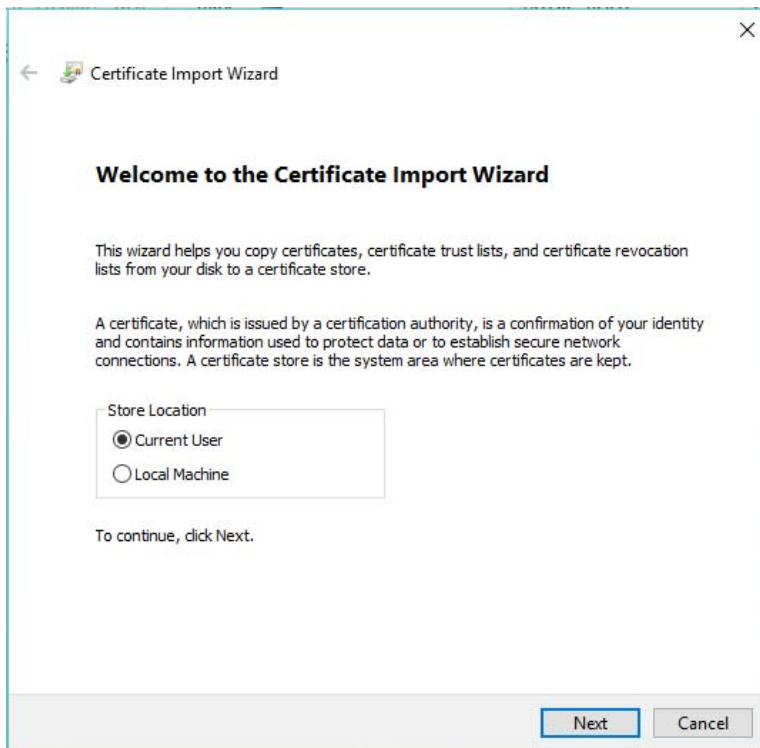
It is important to remember that all certificates exported from *your web browser* onto your computer be **DELETED**. **Failure to do so will put the security of your certificates and keys at risk.**

Also ensure that once the certificates have been deleted that your recycling bin (or trash) has been emptied.

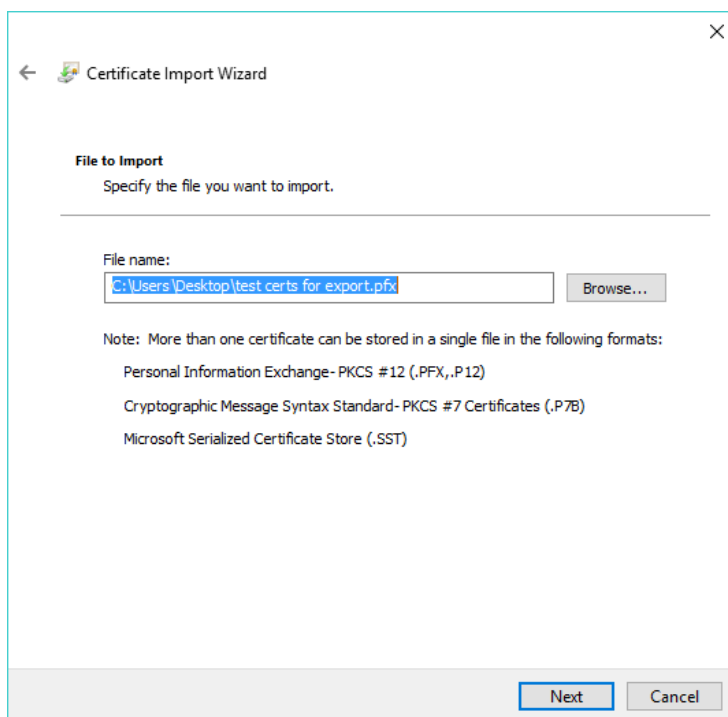
5.3 To Import Certificates

1. Double click on certificate file you saved and the Certificate Import Wizard screen will appear; click **Next**.





2. On the Certificate Import Wizard; File to Import screen; click **Next**.





3. On the **Certificate Import Wizard, Password** screen; enter the **Password** you created during export. Make sure that you check off all three boxes; especially **“Mark this key as exportable”**. This will allow you to back up or transport your keys at a later time. Click **Next**.

← Certificate Import Wizard

Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:
[.....]
 Display Password

Import options:

- Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
- Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
- Include all extended properties.

Next Cancel

4. On the Certificate Import Wizard, Certificate Store window; click on **Automatically select a certificate store based on the type of certificate**; and click **Next**.

← 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

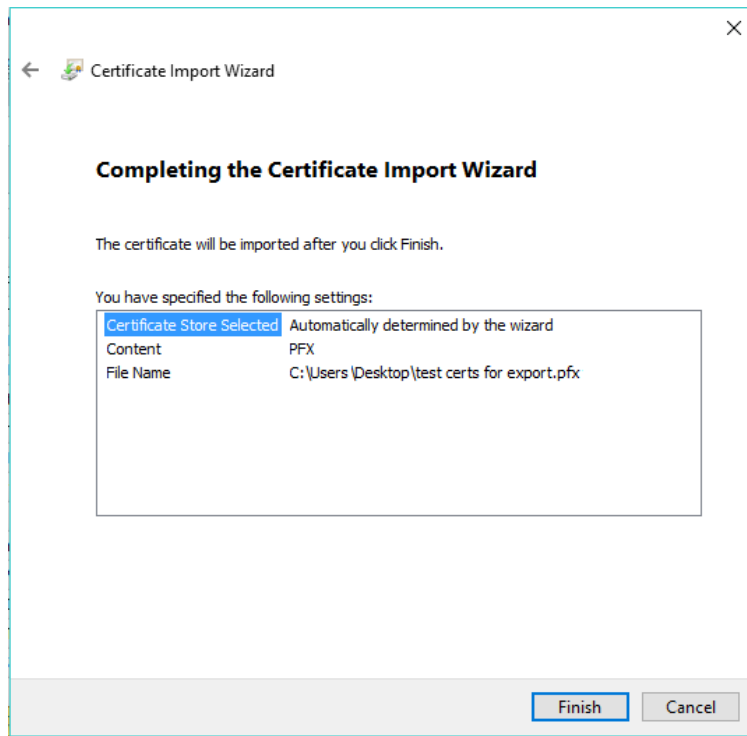
Certificate store:
[] Browse...

Next Cancel

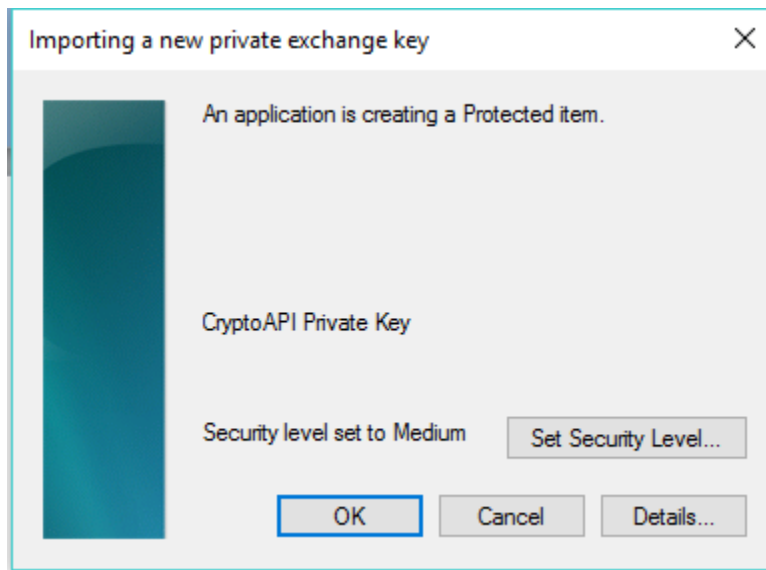




5. The Completing the Certificate Import Wizard window will appear; click **Finish**.

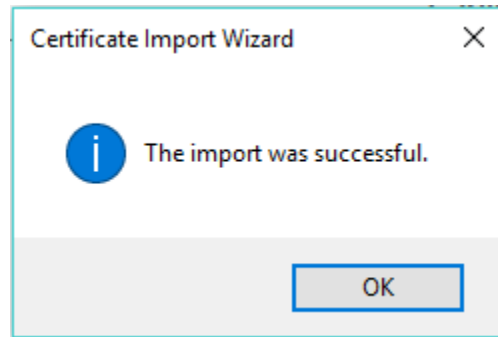


6. On the Importing a new private exchange key pop-up(s); click **OK**.





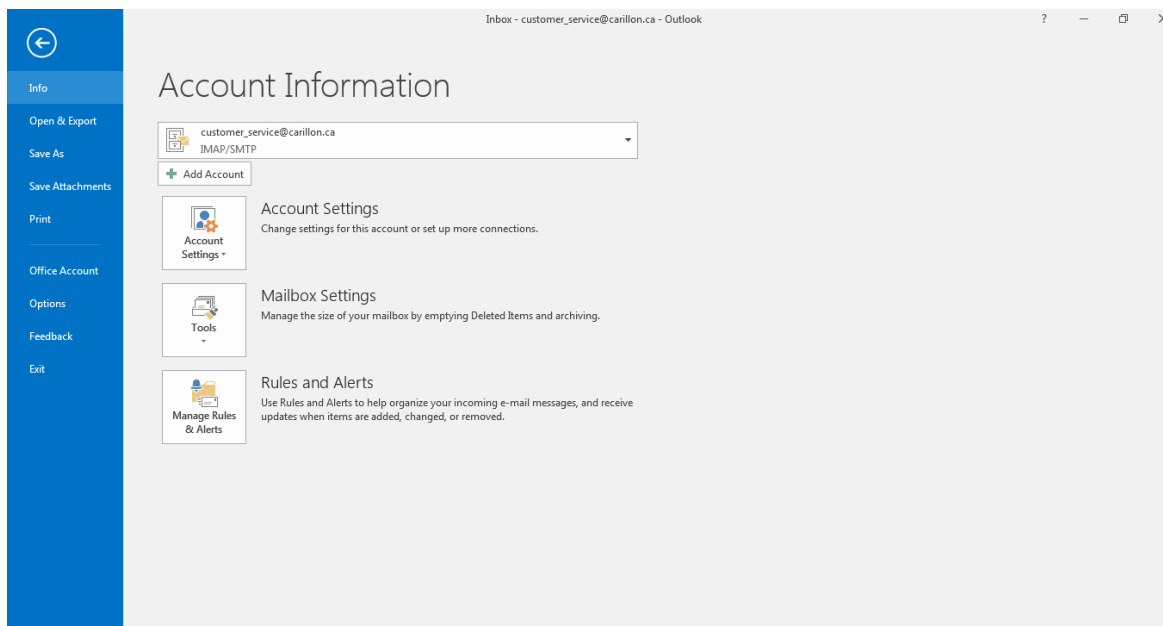
7. Click **OK** on the Import was successful pop-up.



5.4 Setting Up Access to the Carillon LDAP Proxy

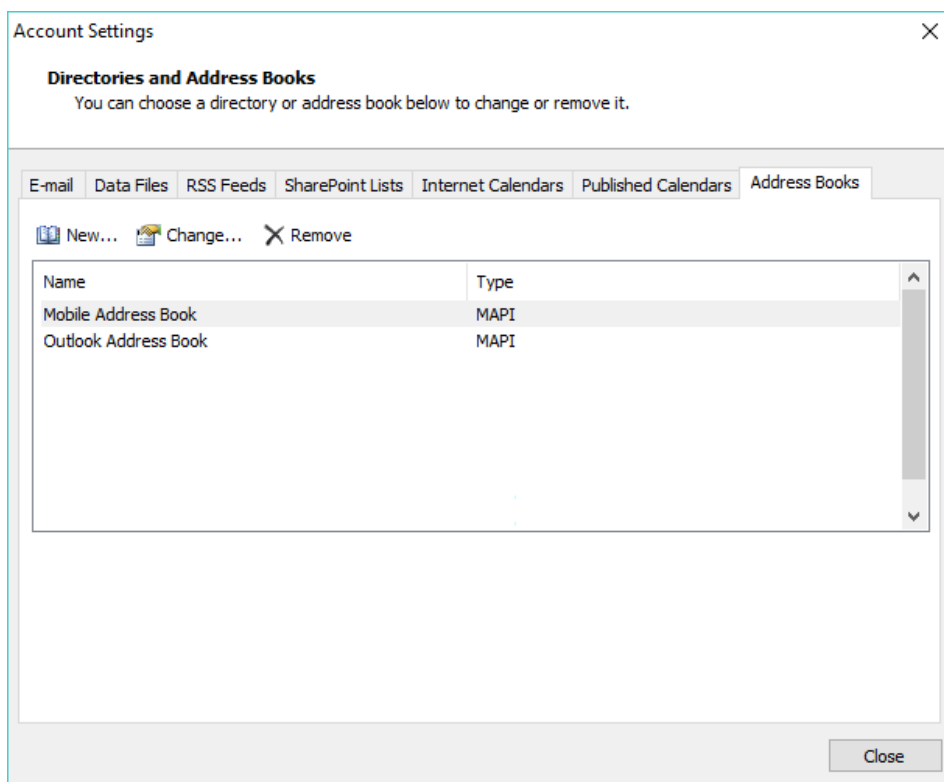
The *Carillon LDAP Proxy* is a link to a directory of recipient encryption certificates containing public encryption keys, which can then be used to encrypt email intended for the person associated with the retrieved certificates. This is done in order to avoid having to manually enter each person's certificates so that you may send/receive encrypted e-mail with them.

1. From you Microsoft Outlook page, select the **File** tab and then **Info** tab from the corresponding menu items. Click on the **Account Settings** button, and select the **Account Settings...** pop-up.

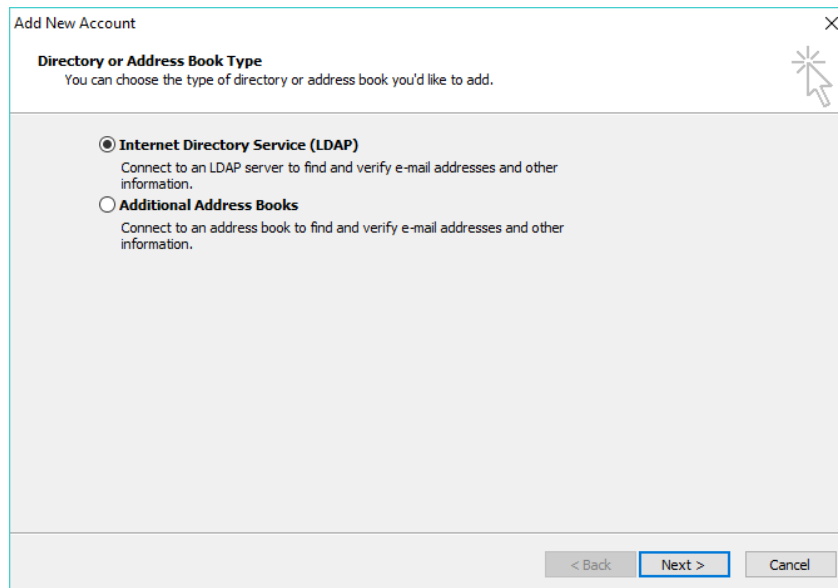




2. In the Accounts Settings window, select the **Address Books** tab and click on the **New...** button.



3. Make sure the **Internet Directory Service (LDAP)** option is selected and click the **Next** button.



4. Fill out the **Server Name** information only. The **Carillon LDAP Proxy** directory is **dir.carillon.ca**.

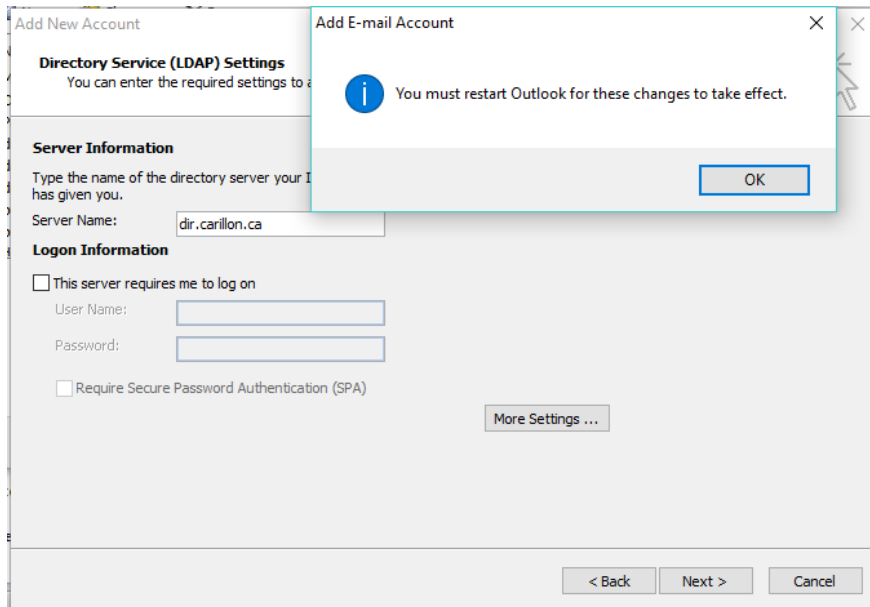




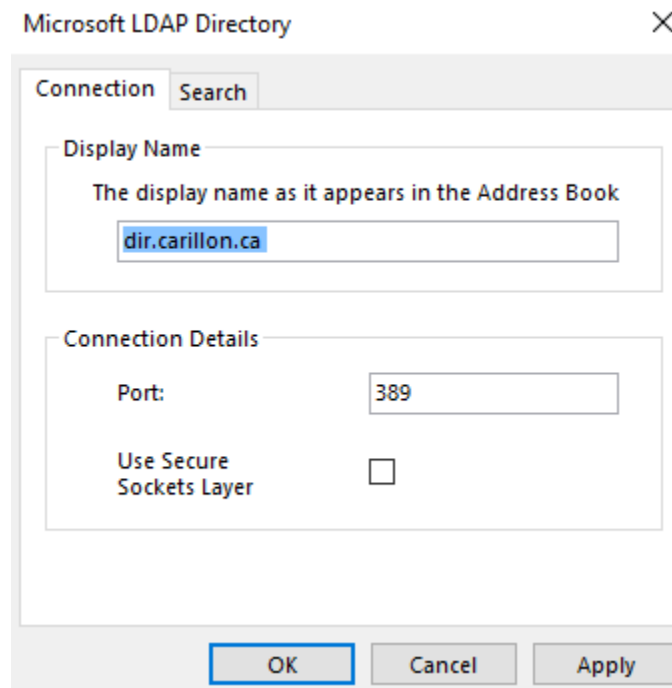
5. Click on the **More Settings** button.

NOTE:

Do not select *“This server requires me to log on”*. User Name and Password are *not* required.

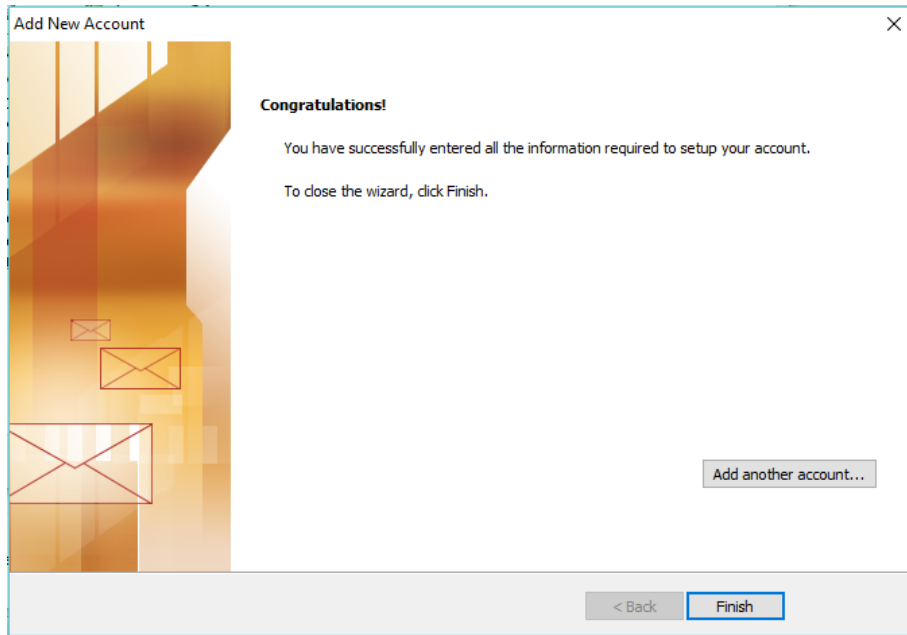


6. In the Microsoft LDAP Directory window ensure that dir.carillon.ca is the Display Name and that the Connection Details Port is set to **389**; then click **OK** or **Apply** as necessary.





7. Click the **Finish** button.



8. Click the **Close** Button.

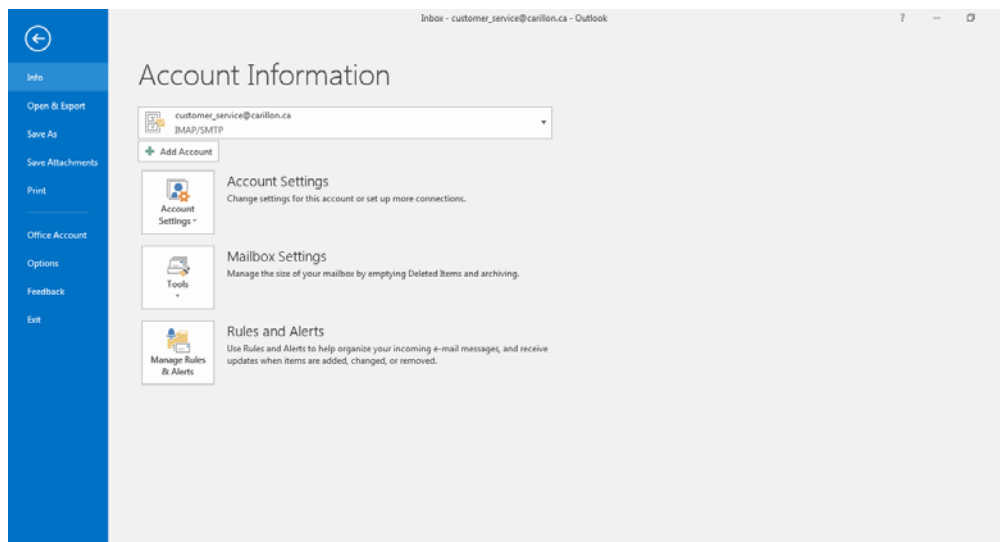
9. You will need to **RESTART** Microsoft Outlook for the email account changes to take effect.

You have now completed setting up the Carillon LDAP Proxy

5.5 Confirming LDAP is Properly Configured

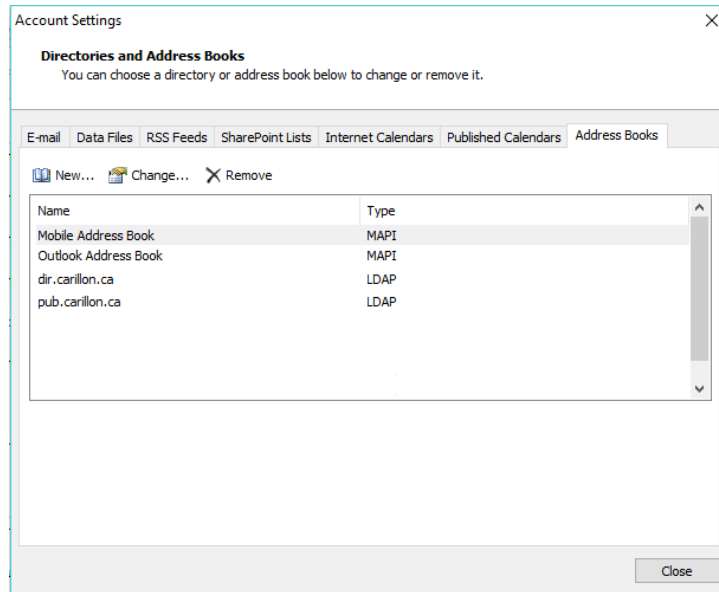
To confirm that the changes have been applied, open Outlook and select the **File** tab and **Info** tab from the corresponding menu items.

1. Click on the **Account Settings** button and select the **Account Settings...** pop-up. In the Accounts Settings window, select the **Address Books** tab.

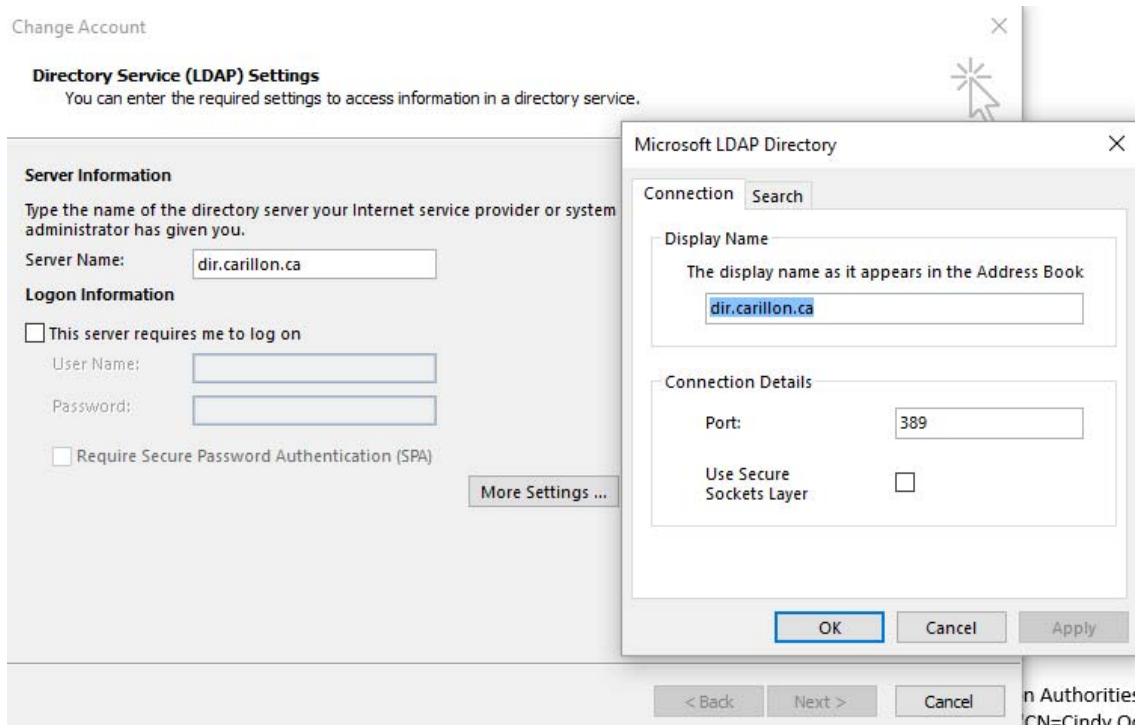




2. Your directory should appear in the list on this page. Double click on dir.carillon.ca



3. Click on More Settings
4. Verify that dir.carillon.ca is the Display Name and that the Port is 389, click OK.



5. Click the **Close** button to close the window.

You have now verified that you have access to the Carillon LDAP Proxy.





6 HOW TO USE YOUR CERTIFICATES IN OUTLOOK

This section gives step by step instructions on how to set up and use Secure Email (S/MIME) with your email client and how to properly import the certificates into the **Microsoft Office Outlook 2010** or higher and on Microsoft Office 365 email management tool. These instructions will guide you on how to set up your email account to use these certificates, as well as set up your email client to use the *Carillon LDAP Proxy* so that you can look up and find other users with whom you may wish to exchange secure email.

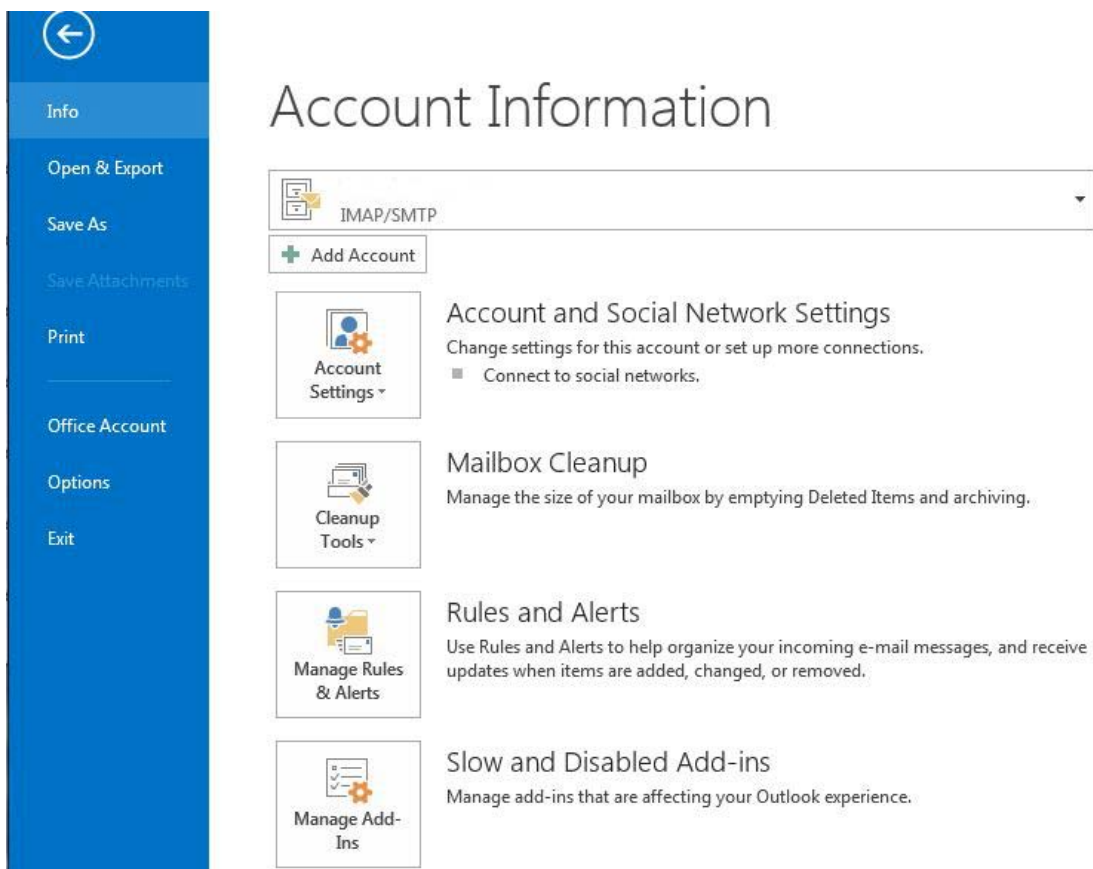
To ensure these certificates are properly recognized and trusted by your email client, be sure to install the associated Trust Chain certificates on your computer or laptop before proceeding.

NOTE:

Third party certificates aren't supported for OWA S/MIME; only Microsoft Windows Certificate Authority issued certificates are supported.

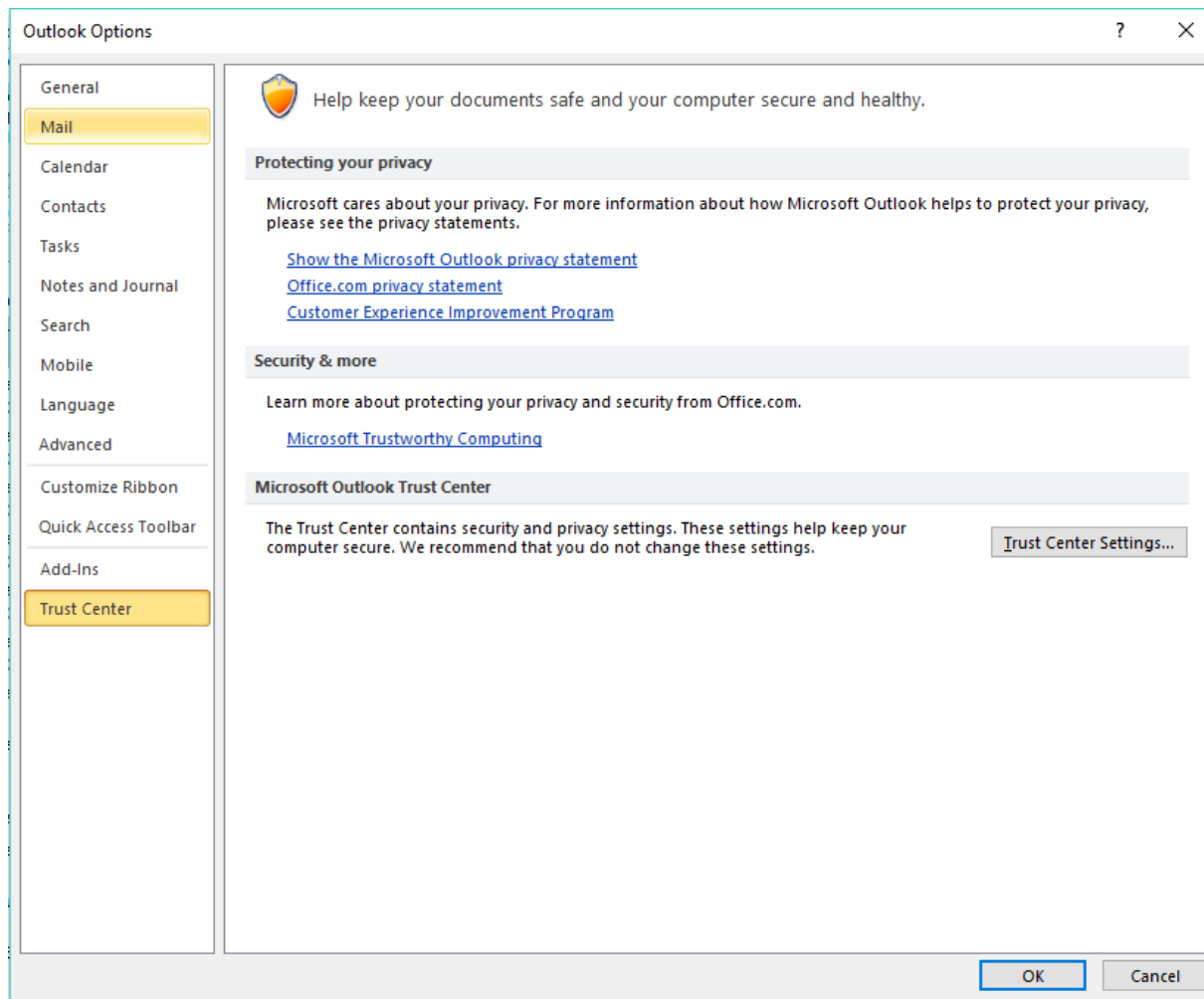
6.1 Setting up Outlook or Office 365 to use your Certificates

1. Start the email application.
2. Select the File tab and then select Options. You will see a screen similar to this one.



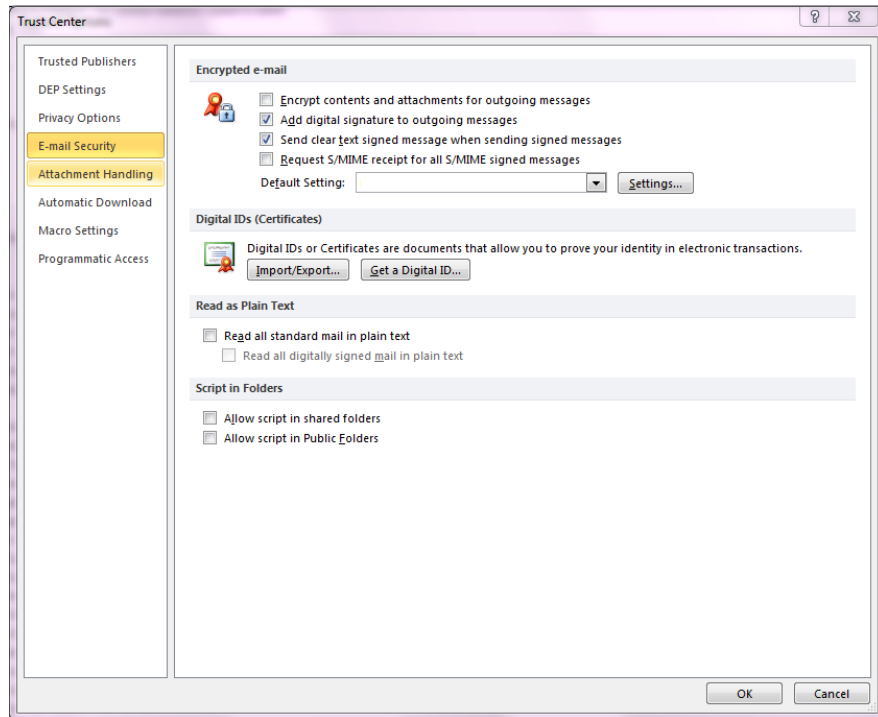


3. Select the **Trust Center tab** from the side menu, and then select the **Trust Center Settings...** button. Similarly in Office 365, select the Trust Center tab from the side menu; you will not have a Trust Center Settings button.

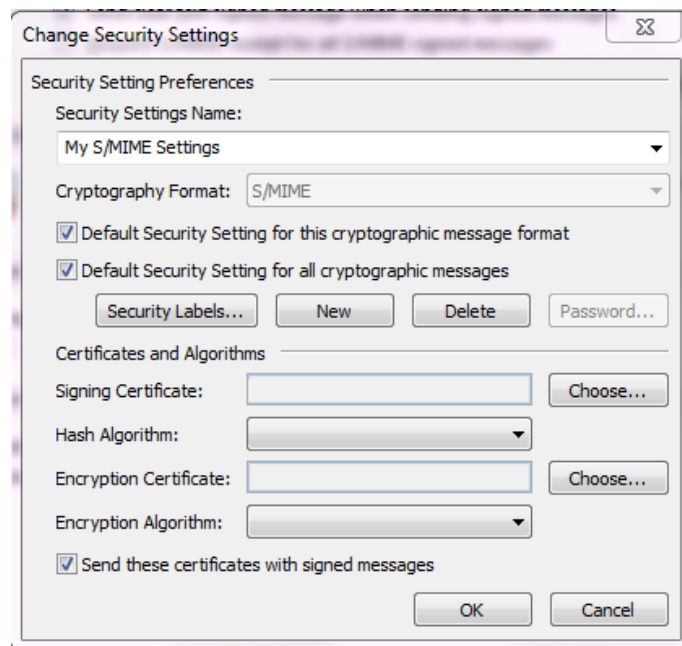




4. In the Trust Center window, under the **E-mail Security** tab, click the **Settings** button.

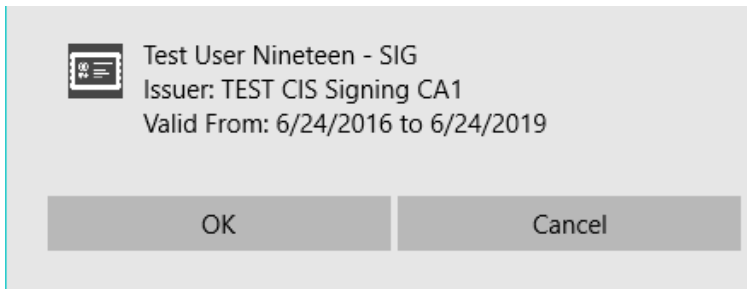


5. In the Change Security Settings window, under Security Settings Name, enter a name for your security setting (this would be a name you designate to your certificates). Under the Certificates and Algorithms section, setup your Signing certificate by clicking on **Choose**.

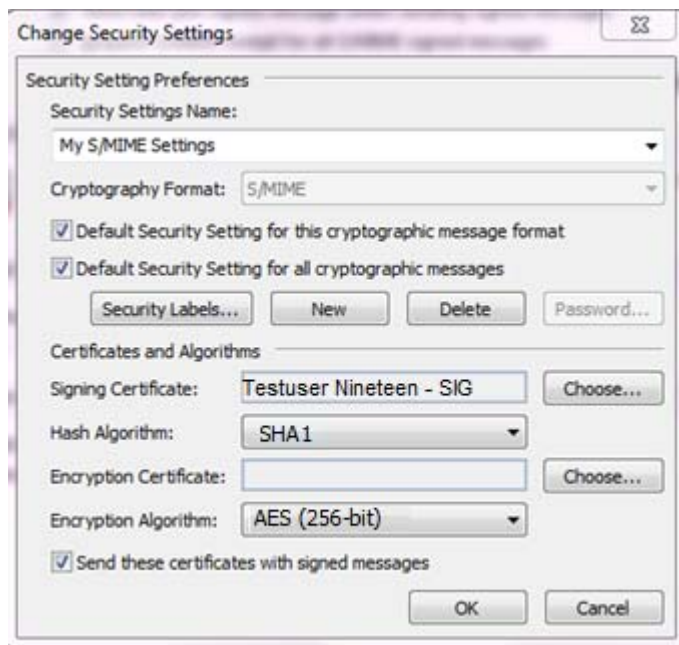




6. On the Windows Security window, select the signature certificate you wish to use (if you have more than one) and click the **OK** button.



7. For the Hash Algorithm, select SHA1.

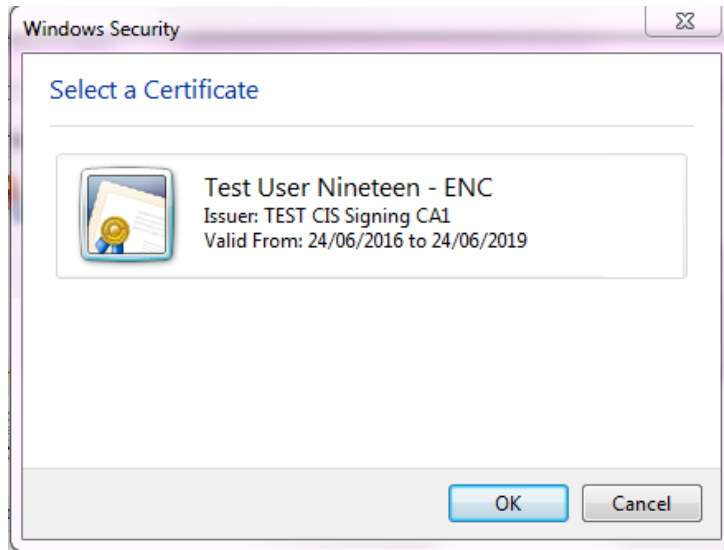


8. Setup your Encryption Certificate by clicking on **Choose**.

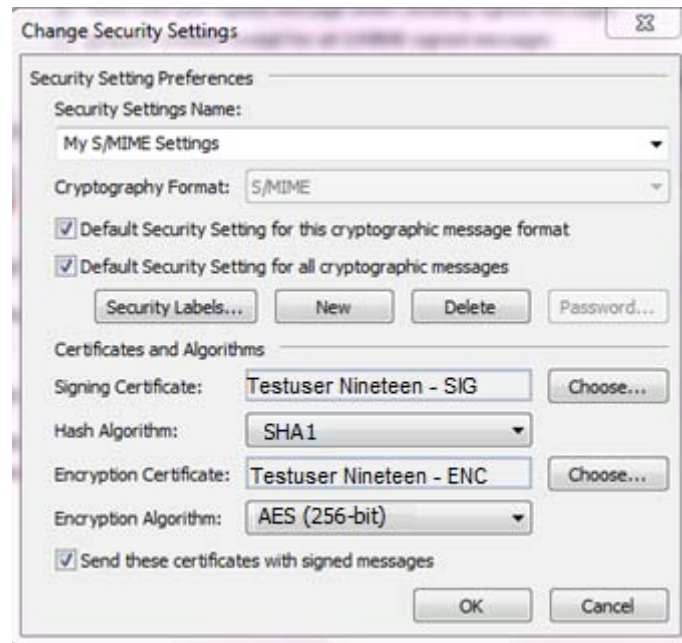




9. On the Windows Security window, select the encryption certificate you wish to use (if you have more than one) and click the **OK** button.



10. For the Hash Algorithm, select **AES (256-bit)**.



11. Click the **OK** button to complete your Personal Certificate setup.

You have now finished setting up your Personal Certificates for use in *Outlook*.





6.2 Signing and Encrypting E-mail

The reasons for digitally signing and encrypting a document are simple:

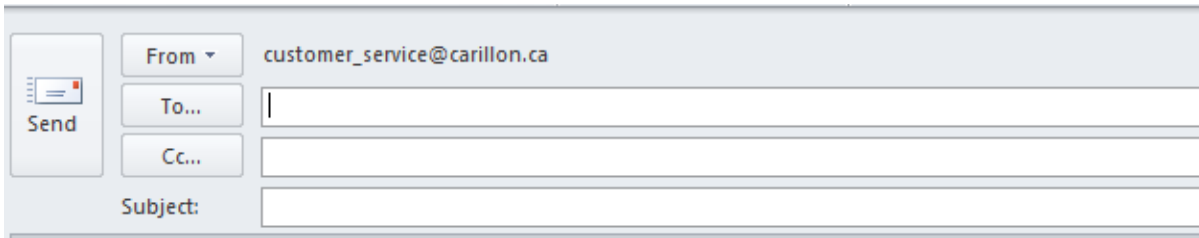
- It ensures that the document was actually sent by YOU.
- It ensures that the document wasn't modified in route.

Additionally, the reason for encrypting an email is that it ensures that no one else can read your message. To proceed:

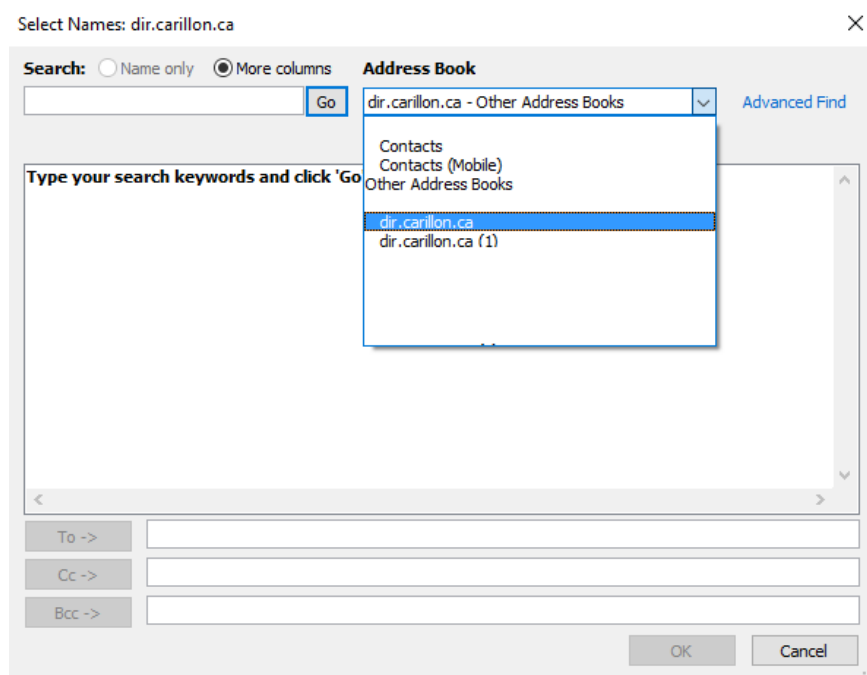
1. Open Outlook, and select **New E-mail** on the htab.



2. Click on the **To...**

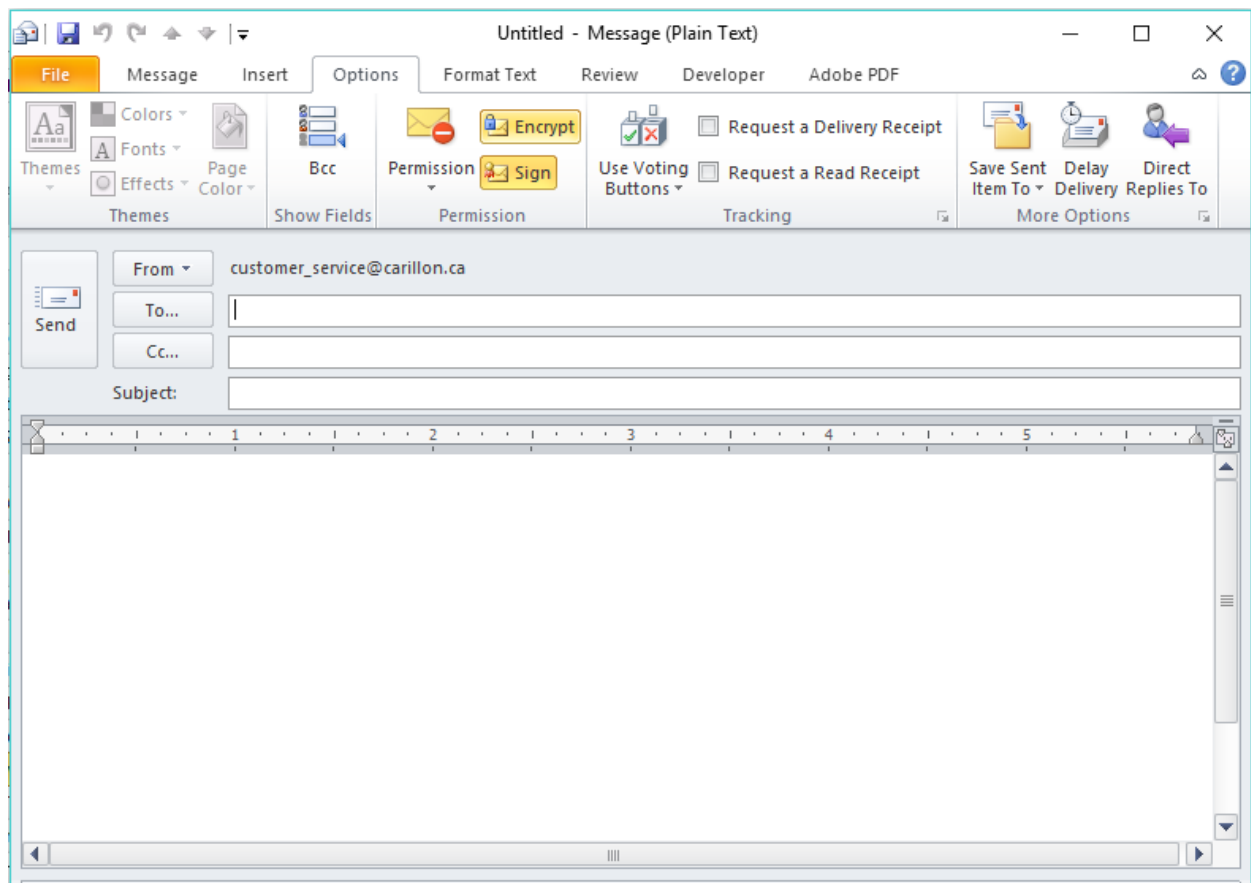


3. The **Select Names: Contact** window should pop up and from the **Address Book** drop down, select: **dir.carillon.ca**. Type in the email address in the space to the left of the **GO** button; then select **GO**.





4. The name of the person should show up in the space below with ENC beside it. Select their name, then click on the **TO**, then **OK**.
5. Fill out your email, then open the **Options** tab and ensure that the **Encrypt** and **Sign** buttons on the Permission menu are selected.
6. Click **Send** to send the digitally signed and encrypted email.



Delivered messages display the signing icon, encryption icon, or both, depending on the options you selected.

You have now successfully sent a signed and encrypted email.

NOTE:

If you are using Windows 7, recipients of your emails may not be able to read your encrypted messages if they are using an older email client.

To fix this problem, follow the steps below:

1. From the **File** menu, select **Options**, then click the **Trust Center** tab, **Trust Center** button.
2. Under the **Encrypted email** header, click the **Setting** button. Under the **Certificates and Algorithms** section, from the **Encryption Algorithm** drop-down menu, select **3DES**.
3. Click **OK**, and then click **OK** again.






7 NETWORK ADMINISTRATOR TROUBLESHOOTING

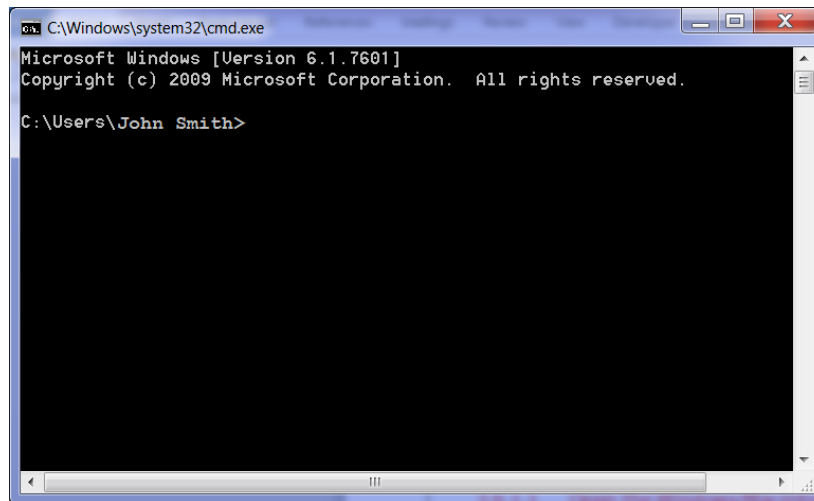
This section is to assist **Network Administrators** in diagnosing certain common problems that may occur after setting up the certificates on your system. References are made to tools that the Network Administrator will have at their disposal in order to perform these tasks.

7.1 Test link to the Carillon LDAP Proxy

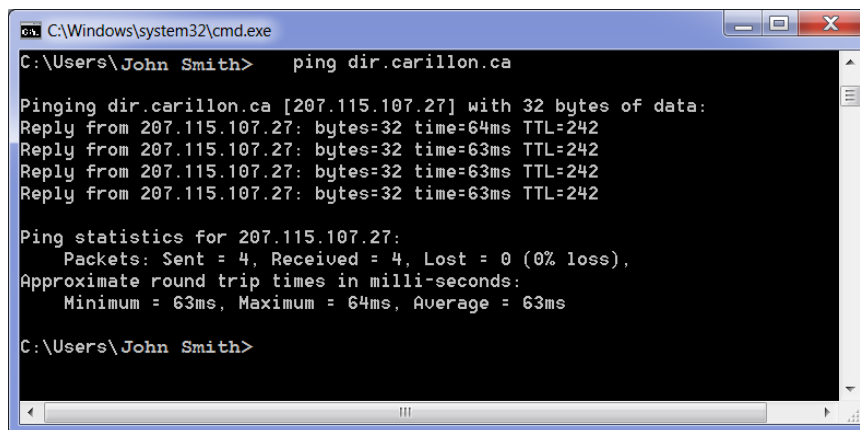
1. To test your configuration to the **Carillon LDAP Proxy**, click the Start Menu button , and in the **Search programs and files** field type **cmd** and press the [Enter] key to open the Windows Command Prompt.



2. The following window will appear; type the command: **ping dir.carillon.ca**



3. If you were successful in connecting to the directory, you should have 0% lost packets, receiving the following output:



4. If no connection was established (100% packet loss), try again.





5. Telnet to port 389 – if you get a connected message, the firewall from your organization will let the traffic through. If you get a connection denied message, please open your company firewall to allow traffic on TCP 389 to dir.carillon.ca.
6. To ensure that you can, in fact, lookup certificates, open the shell and make sure you are in the directory with *OpenLDAP* (or equivalent tool) in order to do an “ldapsearch”.
7. Then type this command:

```
ldapsearch -xh dir.carillon.ca mail=captainbob@carillon.ca
```

Where captainbob@carillon.ca is the email address of the certificates you are looking for. If the search was successful, you should see a user Certificate entry returned (a giant block of text (certificate) should be displayed.) This means the email is correct. If you're still unable to send the person email, it is likely due to their certificate being expired or revoked.

```
mail: captainbob@carillon.ca
userCertificate;binary: #_HHDCOCBq5Gaw1B2q1B1j2Aqg3qd3i1L3L=ADUFA8B7N0Dw00YUw
QQ3Rr^DQTR+N0k3A^HDCgr^Q2TyaTpxsb24g3H5mb0Jt^Y3R;+34g^8Uj630-6^e3GM5f;E;RkNCT3A1
```

If the search was not successful, the following output will be returned.

```
# LDAPv3
# base <> (default) with scope subtree
# filter: mail=badmail@carillon.ca
# requesting: ALL
#
# search result
search: 2
result: 0 Success
text: Successful
# numResponses: 1
```

This means that this email address is not in the certificate directory. Contact the owner of the email address and make sure the email address you typed in is correct. If the email address is spelled correctly, the owner does not hold a certificate and should not be communicated with.

NOTE:

You CANNOT use a directory browser to verify connectivity. The directory is configured to answer specific queries for user Certificate entries by people knowing email addresses, and to not allow for browsing. This is to ensure confidentiality.





8 CUSTOMER SERVICE

Should you require assistance at any time, please feel free to contact us and we will be happy to assist you:

Carillon Information Security Inc.,

Customer Service Group

8:00AM-8:00PM Eastern

Telephone: 1-514-485-0789

Email: customer_service@carillon.ca

