# ONE Mail Partnered – Client Deployment Guide

## Instructions for Microsoft Exchange 2000/2003 Server

Version: 1.3

# Copyright Notice



## All rights reserved



## Trademarks



## Revision History

| Date | Version | Revision |
|---|---|---|
| January 2009 | 1.0 | Initial draft (Ognjen Andrijasevic) |
| November 2014 | 1.3 | Changes to reflect new ONE Mail environment (David Thabet, ONE Mail Technical Specialist) |
| | | |
| | | |

# Table of Contents

# 1.0 Introduction

This document describes the steps required to connect Microsoft Exchange Server 2000/2003 to ONE Mail Partnered product for secure e-mail routing:

- Generate a request for a PKI certificate
- Install the created certificate
- Install eHealth Ontario CA Root certificate
- Setup Send Connector for routing e-mail to ONE Mail Partnered environment
- Setup Receive Connector for routing e-mail from ONE Mail Partnered environment to your corporate messaging system

These instructions apply to Microsoft Exchange Server 2000 (with latest Service Pack installed) installed on MS Windows Server 2000 or Microsoft Exchange Server 2003 (with latest Service Pack installed) installed on Windows Server 2000/2003. Those instructions also can be followed to configure MS Windows Server 2000/2003 IIS server configured as SMTP server to connect to eHealth Ontario's ONE Mail Partnered Service.

# 2.0 Intended Audience

This document is intended for technical personnel at eHealth Ontario client organizations who are involved in registering computer applications with eHealth Ontario. This includes:

- Application Owners
- Their delegates

# 3.0 Overview

The process of connecting to ONE Mail Partnered is as follows:

1. Register the application (for which you require a certificate) with eHealth Ontario, if this hasn't been previously done.
2. **Obtain a PKI Reference Number from eHealth Ontario**. This number will be required to create and submit your request to eHealth Ontario.

3. **Create the Certificate Signing Request (CSR)**. The CSR should be created on the machine where the certificate is to be used. The process of creating a CSR generates a matching public and private RSA key pair and stores the private key on the machine and puts the public key into the CSR.

4. **Send the CSR (with Reference Number) to the eHealth Ontario Deployment Team**

5. **Receive the created certificate back from the eHealth Ontario Deployment Team**

6. **Install the certificate**. This should be done on the same machine where the CSR was created.

7. **Install eHealth Ontario CA Trusted Root certificate**

8. **Setup Connector on Exchange Server 2000/2003 or IIS**

# 4.0 Creating CSR(s)

For each request to be generated you require the corresponding Reference Number (example: 8934282) for this identity. These are obtained from the eHealth Ontario Deployment Team. A unique Reference Number is required for each certificate that is to be created.

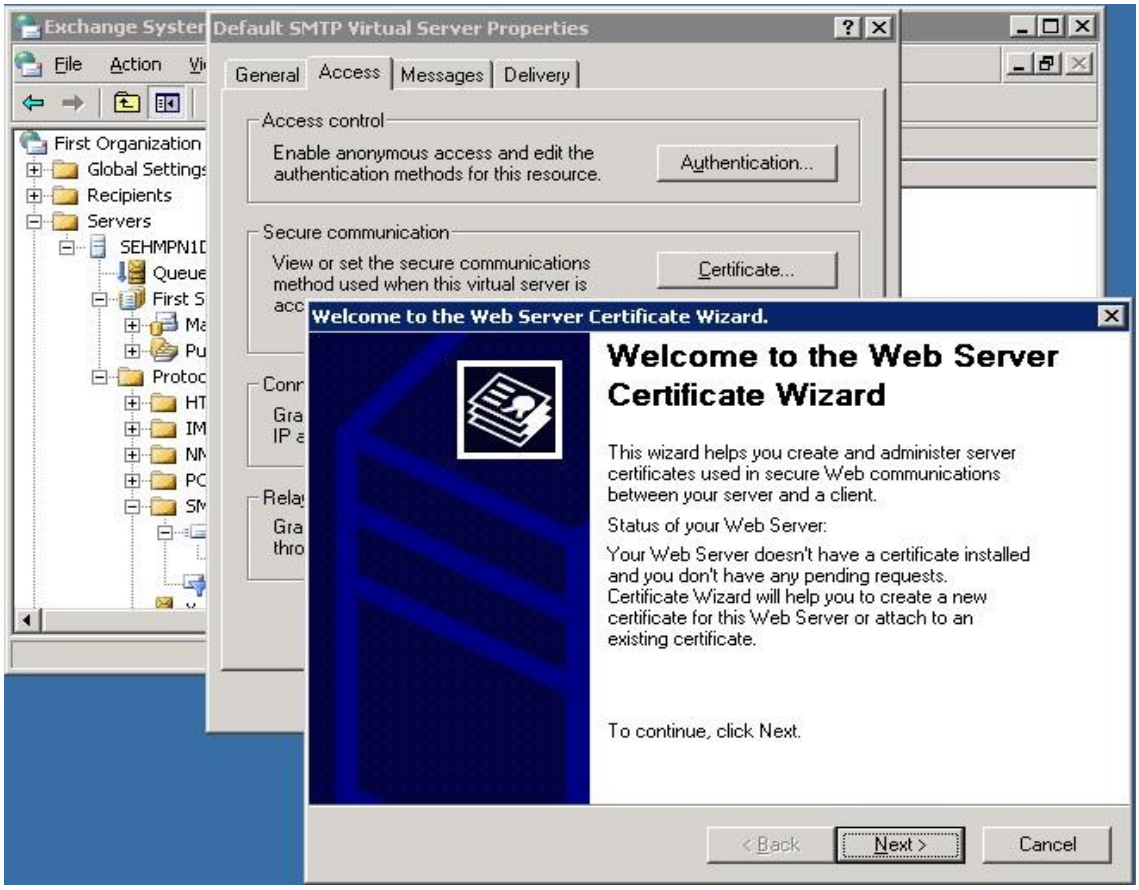
**NOTE:** It is of essential for this process to work that CSR was created on the same server where certificate will be installed. If this is not possible, please discuss the problem with eHealth Ontario's deployment team and additional processes or procedures will be followed to customize solution for that case.

## 4.1 Generating a CSR

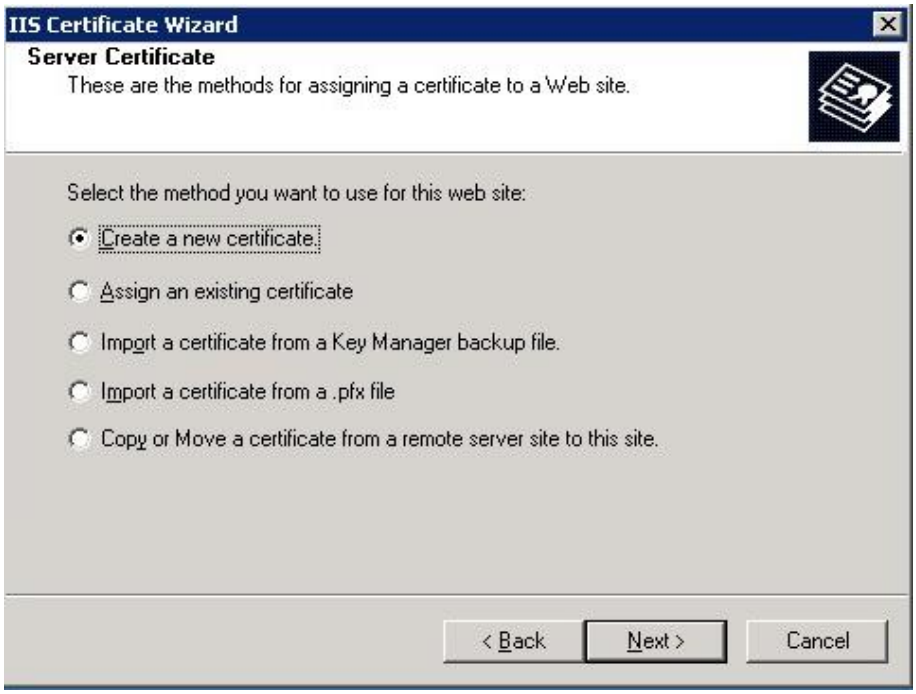
**Note:** Beginning of the process is separately described to cover different tools which are used to configure Exchange Server 2000/2003 to Web Server Certificate Wizard or MS Windows Server 2000/2003 IIS server and SMTP server to connect to same tool. Images used to describe process are generated on Exchange Server 2003 but truthfully interpret process on any other supported platform.

| The procedure for creating a CSR on an Exchange Server is: | The procedure for creating a CSR on an IIS SMTP Server is: |
|---|---|
| 1. Open Exchange System Manager | 1. Open the IIS Manager |
| 2. Expand **Servers** | 2. Select the computer |
| 3. Select the **SMTP inbound gateway Server/Protocols/SMTP** | 3. Select the **Default SMTP Virtual Server** |
| 4. Right click on the **SMTP virtual server** and select **Properties** | 4. Right click and select **Properties**. |
| 5. Select **Access** tab and click on **Certificate** | 5. Select **Access** tab and click on **Certificate** |

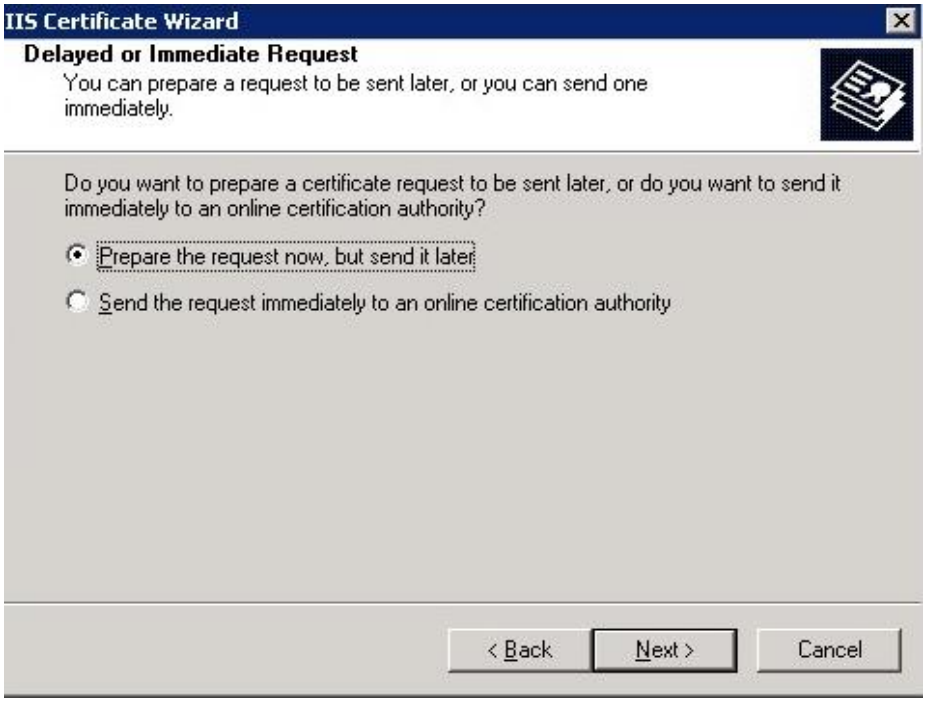
6. On the **Welcome to the Web Server Certificate Wizard** screen click on **Next** to proceed



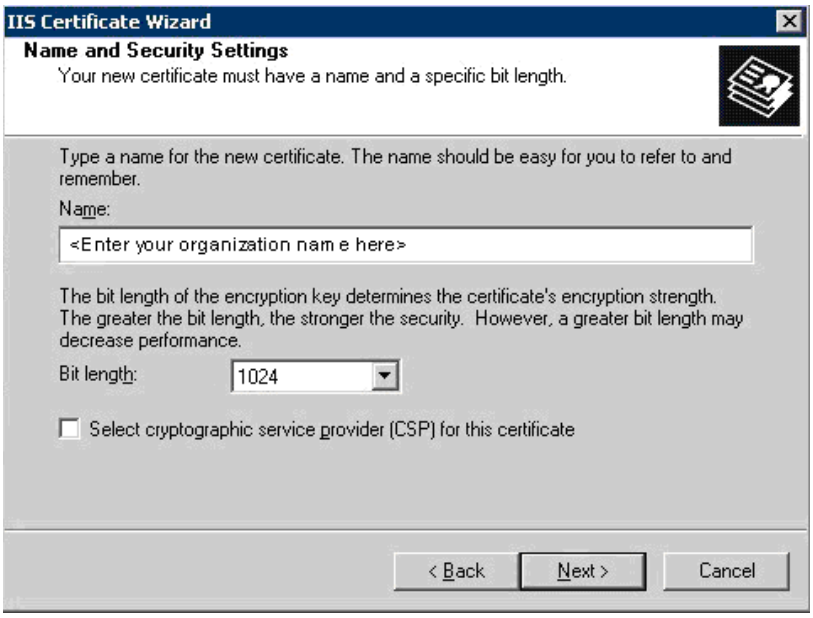
7. On **Server Certificate** screen select **Create a new certificate** and click on **Next** to proceed



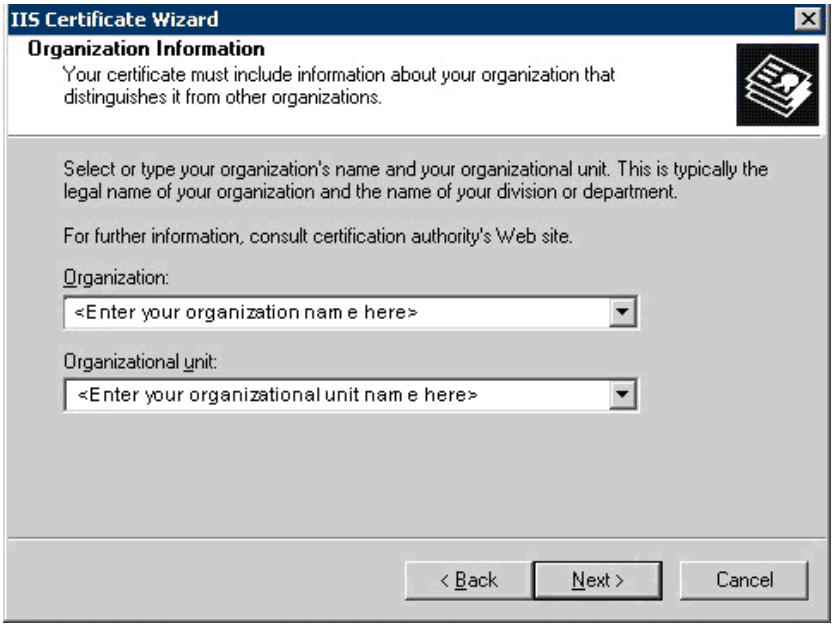

8. On **Delayed or Immediate Request** screen select **Prepare the request now, but send it later** and click on **Next** to proceed



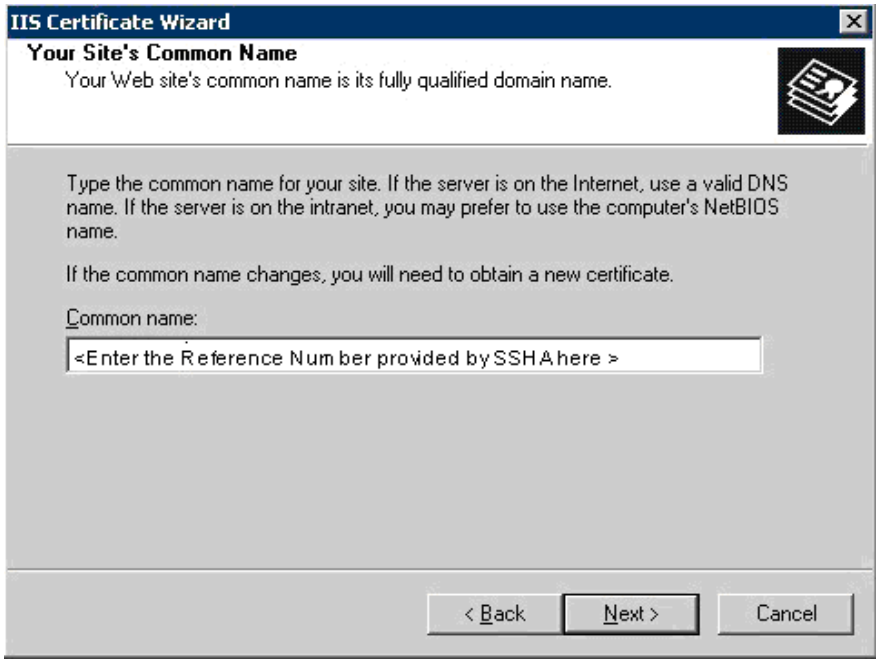
9. On **Name and Security Settings** screen enter your organization name in proper field, check that **Bit length** selected is default *1024*, and that **Select cryptographic service provider (CSP) for this certificate** check box is not selected and click on **Next** to proceed



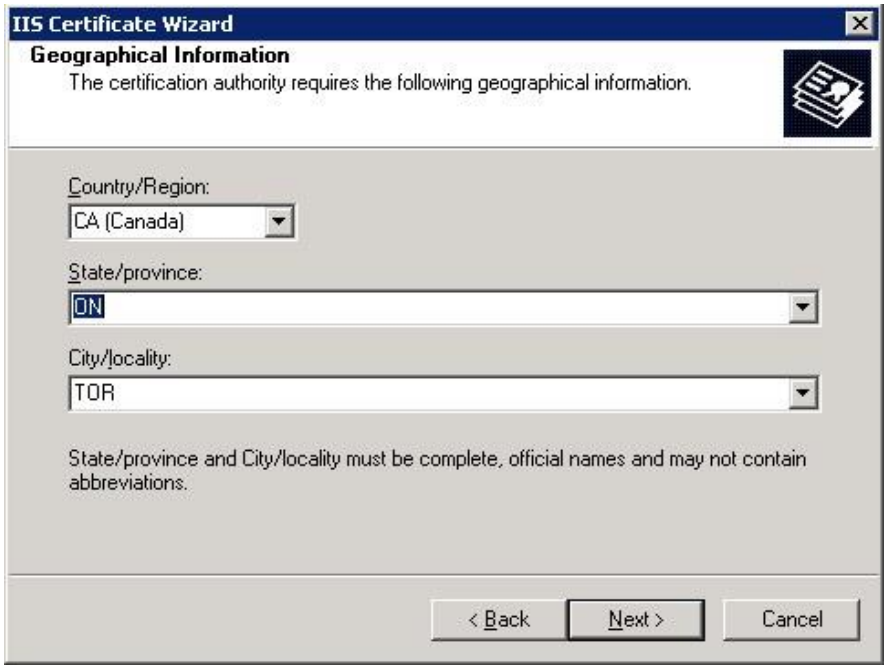

10. On **Organization Information** screen insert proper information about your organization again (**Organization** name and **Organizational Unit** name, if there no **Organizational Unit**, insert same information in both fields) and click on **Next** to proceed



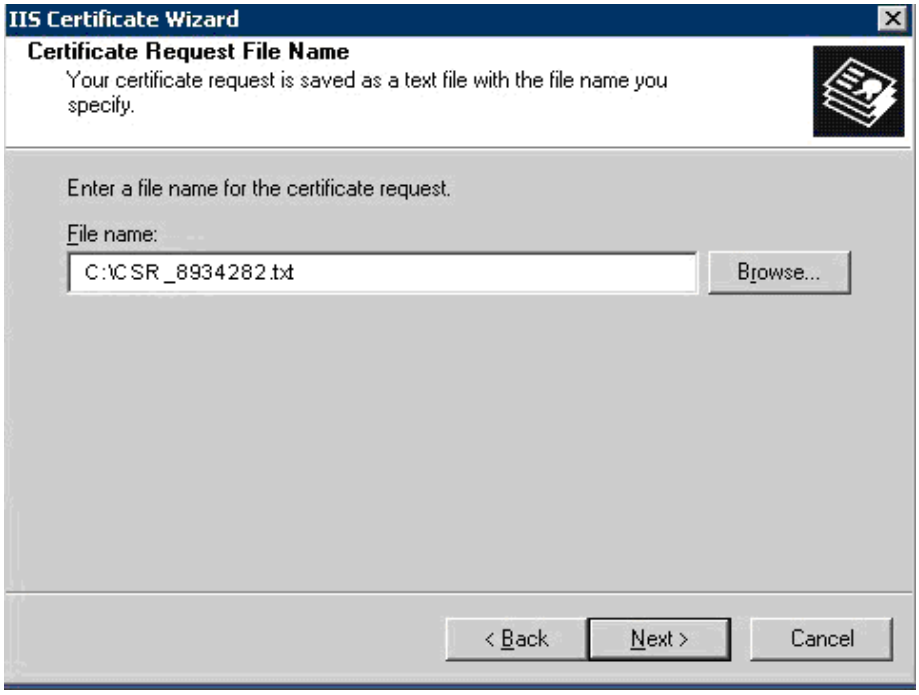
11. On **Your Site's Common Name** enter the Reference number (e.g. 8934282) provided by eHealth Ontario in the **Common name** field and click on **Next** to proceed



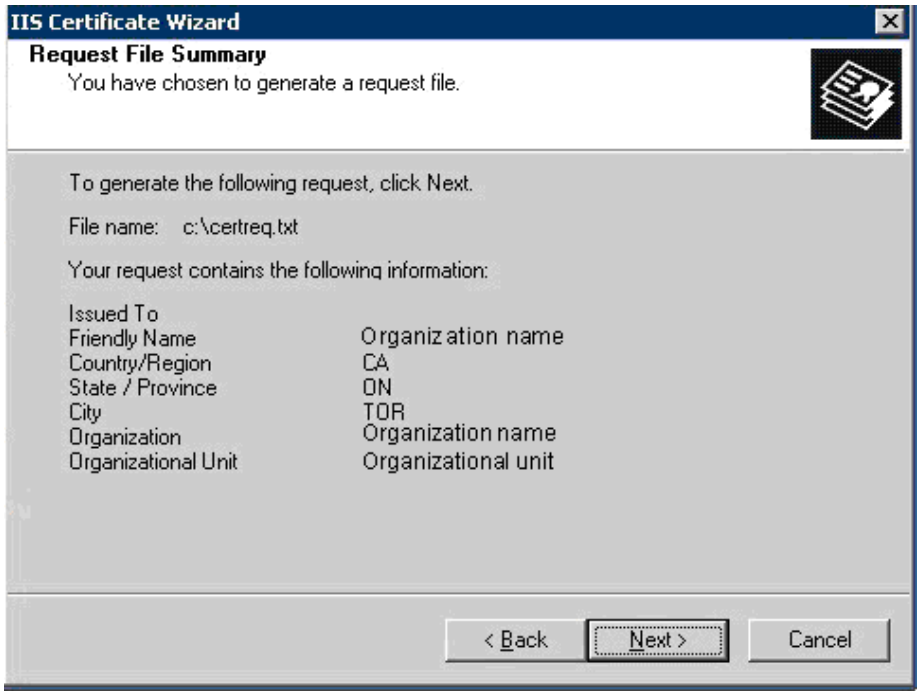

12. On the **Geographical Information** screen insert *CA (Canada)* as **Country/Region**, *Ontario* as **State/province** and proper **City/location** information in proper field. Then click on **Next** to proceed



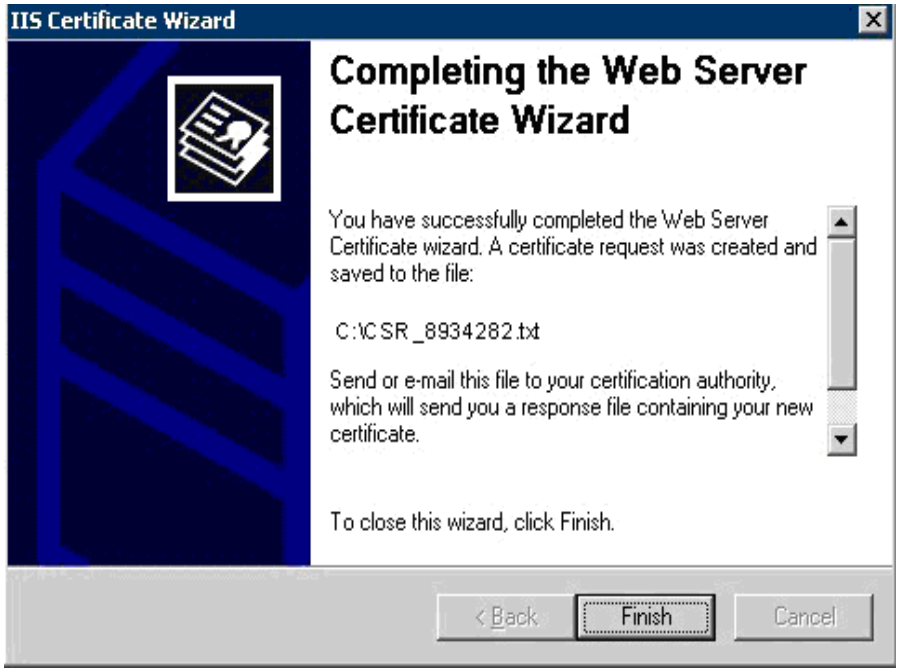
13. On **Certificate Request File Name** enter a file name in which to store the request. Use the reference number in the file name (Example: C:\CSR_8934282.txt). Click on **Next** to proceed




14. On **Request File Summary** page review all selected options and if they are right, click on **Next** to proceed



15. On the **Completing the Web Server Certificate** page click on **Finish** to exit wizard




Complete the above procedure for each certificate you need to create, **entering a new Reference Number, and Output File Name for each request**. The result each time is a CSR file.

## 4.2 Send the CSR to eHealth Ontario

Forward the **CSR/CSRs** to the eHealth Ontario Deployment Team. They will return a certificate created from the CSR and the eHealth Ontario CA Root certificate.

# 5.0 Receive the Certificates

When the certificate is created by eHealth Ontario CA, it will be sent to you in a file.

Its contents will resemble the following:


```
-----BEGIN CERTIFICATE-----
MIIGYAYJKoZIhvcNAQcCoIIGUTCCBk0CAQExADALBgkqhkiG9w0BBwGgggY1MIIG
MTCCBRmgAwIBAgIEQA9uVDANBgkqhkiG9w0BAQUFADCBpjETMBEGCgmSJomT8ixk
ARkWA3NzaDEbMBkGCgmSJomT8ixkARkWC1N1YnNjcmliZXJzMRUwEwYDVQQLEwxT
U0ggU2VydmljZXMxETAPBgNVBAsTCFNlY3VyaXR5MQwwCgYDVQQLEwNQS0kxOjA4
BgNVBAMTMVNtYXJ0IFN5c3RlbXMgZm9yIEhlYWx0aCBBZ2VuY3kgUm9vdCBDQSAt
IFRlc3RpbmcwHhcNMDYwMjE3MDEwNDQxWhcNMDkwMjE3MDEzNDQxWjCBkzETMBEG
CgmSJomT8ixkARkWA3NzaDEbMBkGCgmSJomT8ixkARkWC3N1YnNjcmliZXJzMRQw
EgYDVQQLEwtTdWJzY3JpYmVyczESMBAGA1UECxMJSG9zcGl0YWxzMQ8wDQYDVQQL
EwZPTFNUU1QxFTATBgNVBAsTDEFwcGxpY2F0aW9uczENMAsGA1UEAxMESElTNjCB
```

```
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAwmVaRaRrPLO+ZY44H2ZIX1s6jpA3
H24UDEOKYfaZ1gZesltzYDphXOMp/7ZnP350TnbiZQqpNFLqqckFOWskJSC83PEU
xMa5jJU1xTfdpGWtnYrvT+mi0q3x+KGQ4y7DDtD4KSAWXkkIKndiYH9mvPBQ+q4X
aqHqmFN/DZw/kTECAwEAAaOCAvowggL2MAsGA1UdDwQEAwIHgDArBgNVHRAEJDAi
gA8yMDA2MDIxNzAxMDQ0MVqBDzIwMDgwMzI1MDUzNDQxWjCBxQYIKwYBBQUHAQEE
gbgwgbUwgbIGCCsGAQUFBzAChoGlbGRhcDovL3NzaHBraTJhMDAwMXUuc3Vic2Ny
aWJlcnMuc3NoL2NuPVNtYXJ0IFN5c3RlbXMgZm9yIEhlYWx0aCBBZ2VuY3kgUm9v
dCBDQSAtIFRlc3RpbmcsIG91PVBLSSwgb3U9U2VjdXJpdHksIG91PVNTSCBTZXJ2
aWNlcywgZGM9U3Vic2NyaWJlcnMsIGRjPXNzaD9jQUNlcnRpZmljYXRlMIIBigYD
VR0fBIIBgTCCAX0wgcGggb6ggbukgbgwgbUxEzARBgoJkiaJk/IsZAEZFgNzc2gx
GzAZBgoJkiaJk/IsZAEZFgtTdWJzY3JpYmVyczEVMBMGA1UECxMMU1NIIFNlcnZp
Y2VzMREwDwYDVQQLEwhTZWN1cml0eTEMMAoGA1UECxMDUEtJMTowOAYDVQQDEzFT
bWFydCBTeXN0ZW1zIGZvciBIZWFsdGggQWdlbmN5IFJvb3QgQ0EgLSBUZXN0aW5n
MQ0wCwYDVQQDEwRDUkwyMIG2oIGzoIGwhoGtbGRhcDovL2NybHUuc3NoYS5jYS9j
bj1TbWFydCUyMFN5c3RlbXMlMjBmb3IlMjBIZWFsdGglMjBBZ2VuY3klMjBSb290
JTIwQ0ElMjAtJTIwVGVzdGluZyxvdT1QS0ksb3U9U2VjdXJpdHksb3U9U1NIJTIw
U2VydmljZXMsZGM9U3Vic2NyaWJlcnMsZGM9c3NoP2NlcnRpZmljYXRlUmV2b2Nh
dGlvbkxpc3QwHwYDVR0jBBgwFoAUoDjQCKRd/Fk7eTuqfcpZKT5GWRowHQYDVR0O
BBYEFDtLS1NyMiADLtzKP/vfrPTThIQVMAkGA1UdEwQCMAAwGQYJKoZIhvZ9B0EA
BAwwChsEVjcuMQMCBLAwDQYJKoZIhvcNAQEFBQADggEBAB45Jjvk7NeokO2/iy+H
X142NV7wRR1lBmcJKLxYE3YgrGw7C7kBRjBEZbjoQy8g1Mniop8m1kA6tiJreuF2
kAxElilGu1DK5IqrA+lW7S3b7G5XipgC7jF8iQ9zUhblTsfLfLKZ0r/exPX3LE/P
RYeqIUbATXfc/tuwcPm4kjRigpNIs+uEJAgkoOr73A1U2SLlGf1Q+EhSyTQ2qRI/
lIDTnEACHXbgEhU4qG8p+cN2GDcN8HJUqVLGlH6GOzfpl+6rZVeHfapUqf+hWmtX
LCjcOCVZeaS6GpzIlbBlhRLae6glPUNQUqfX0P8dxCitvY20w0mePuikS1dFsAMz
MGYxAA==
-----END CERTIFICATE-----
```


Proceed to the next section to install the certificate generated from the CSR.

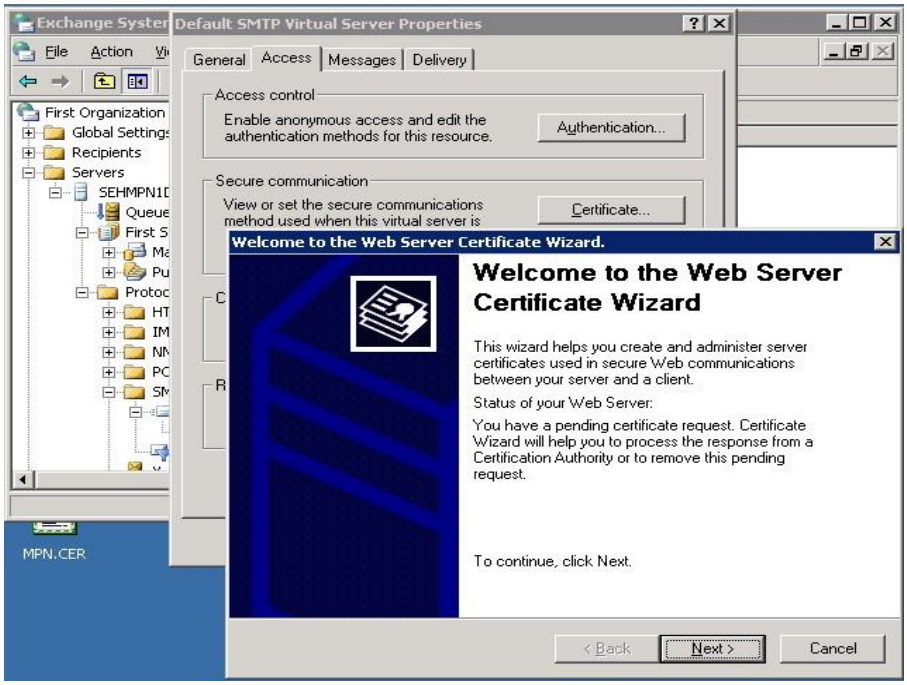
## 6.0 Installing an Exchange Certificate

**NOTE:** It is important to install certificate on the same server where CSR was generated.

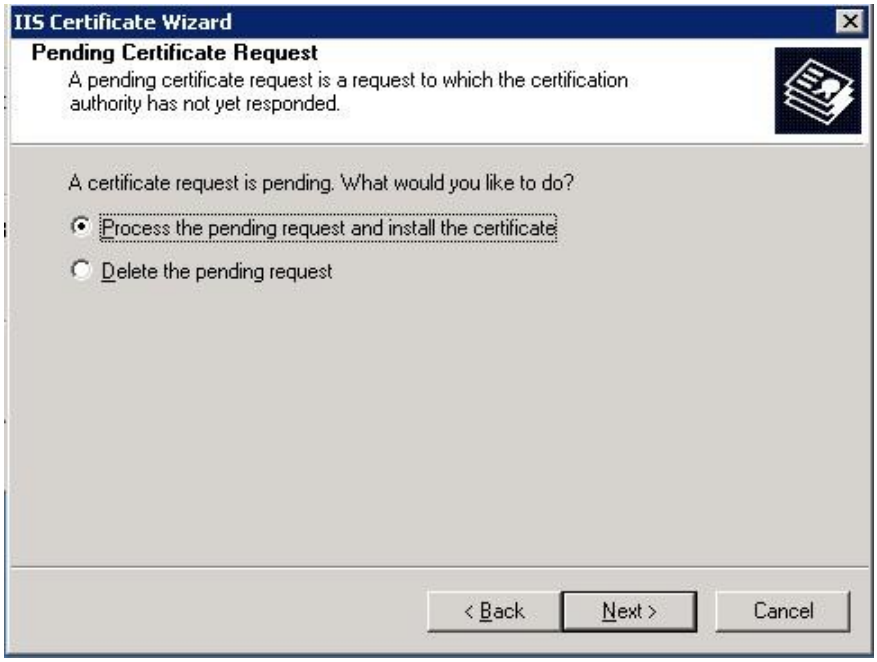
To install the certificate:

| The procedure to install certificate on an Exchange Server is: | The procedure to install certificate on an IIS SMTP Server is: |
|---|---|
| 1. Open Exchange System Manager | 1. Open the IIS Manager |
| 2. Expand **Servers** | 2. Select the **Computer** |
| 3. Select the **SMTP inbound gateway Server/Protocols/SMTP** | 3. Select the **Default SMTP Virtual Server** |
| 4. Right click on the **SMTP virtual server** and select **Properties** | 4. Right click and select **Properties**. |
| 5. Select **Access** tab and click on **Certificate** | 5. Select **Access** tab and click on **Certificate** |

6. On the **Welcome to the Web Server Certificate Wizard** screen click on **Next** to proceed

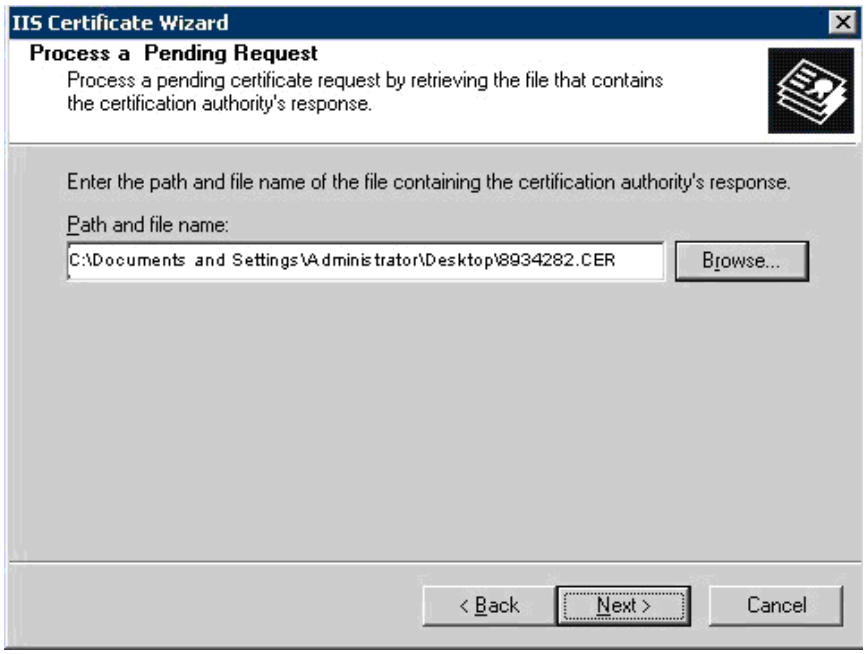



7. On **Pending Certificate Request** screen select **Process the pending request and install the certificate** option and click on **Next** to proceed

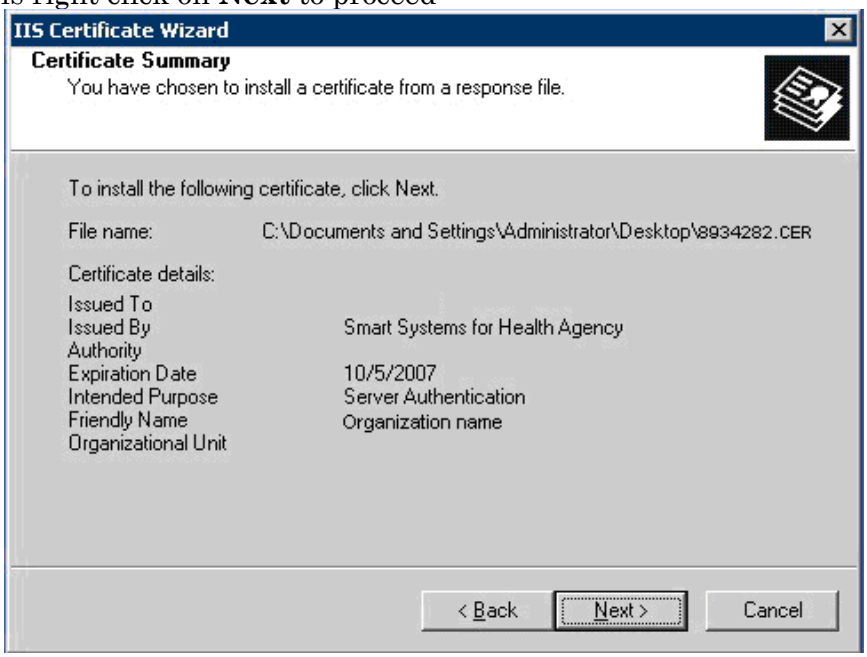


8. On Process a Pending Request screen browse and select certificate file which is send to you by eHealth Ontario's deployment team and which have name with your registration number or your organization name. Click on **Next** to proceed

NOTE: Do not select eHealth Ontario CA Root Certificate for this purpose.




9. On **Certificate Summary** screen review provided information and if it is right click on **Next** to proceed

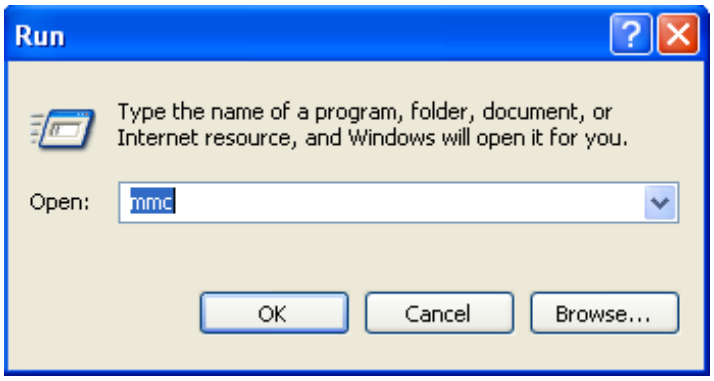


10. On **Completing the Web Server Certificate** page click on **Finish** to exit wizard

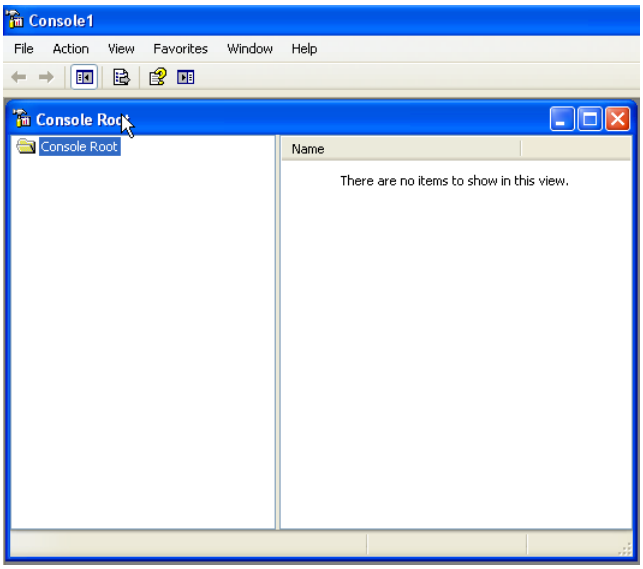

# 7.0 Verifying the Exchange certificate installation

To verify the certificate installation:

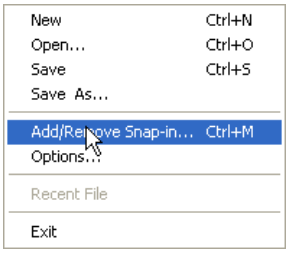
1. From the **Start** menu, select **Run**. In the Run dialog box, type **mmc** and click **OK**.



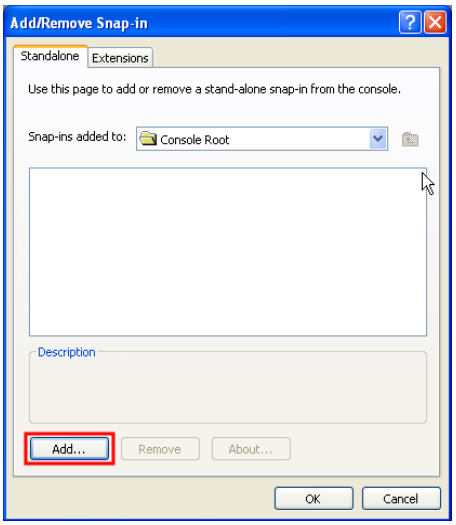

2. The Microsoft Management Console is displayed.



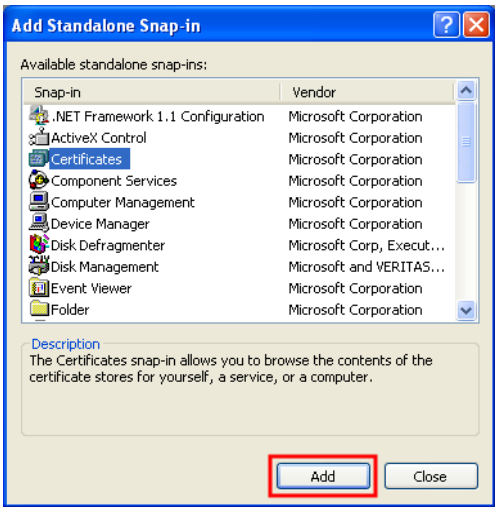

3. From the **File** menu, select **Add/Remove Snap-in**.



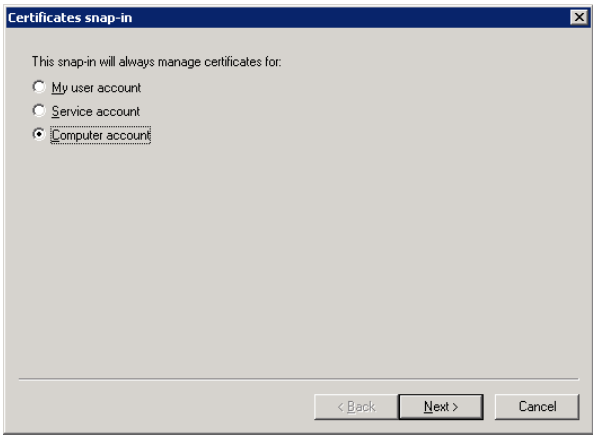

4. On the Standalone tab, click **Add**.



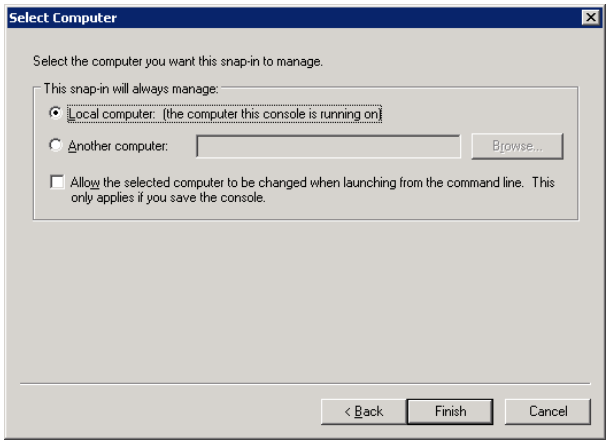

5. From the Available Standalone Snap-in list box, select "**Certificates**", and then click **Add**.




6. In **Certificates snap-in** pop-up window select **Computer account** and press **Next**.

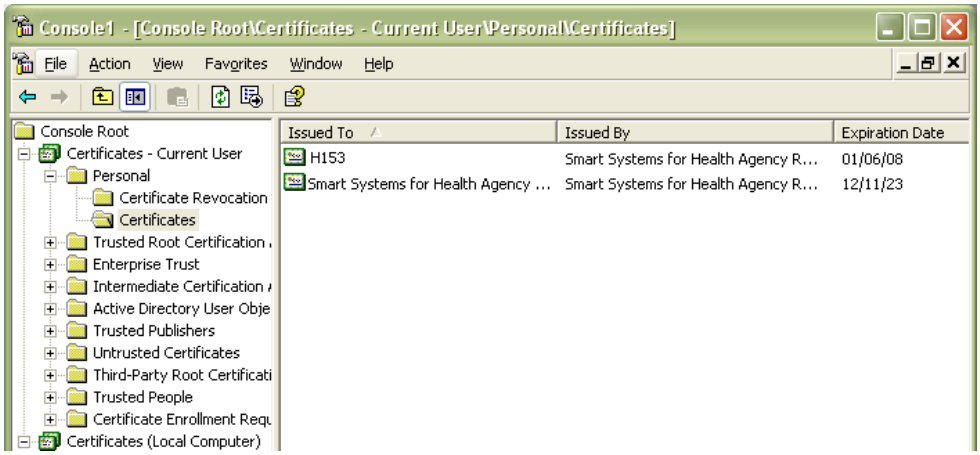



7. In **Select Computer** pop-up window select **Local Computer** option and click on **Finish** button.

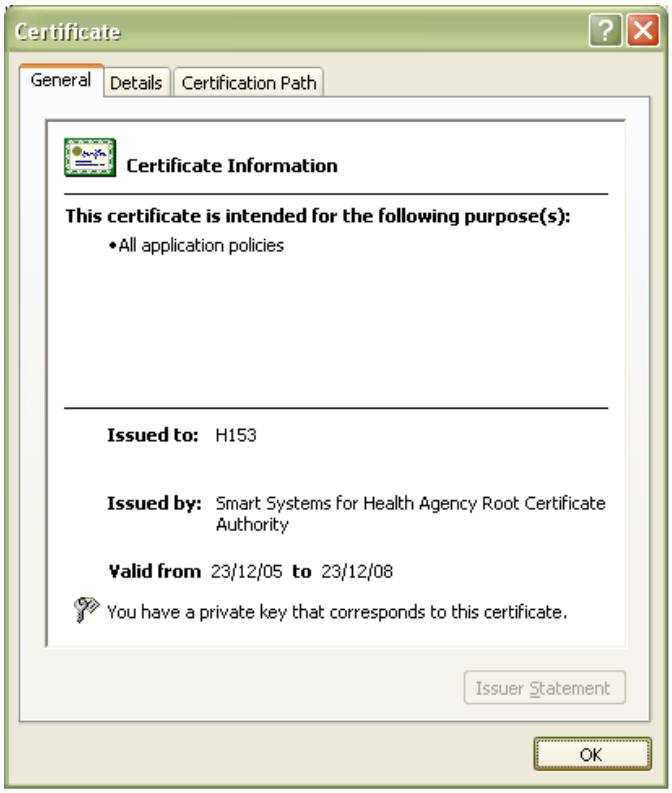


8. In Stand Alone snap-in window press **Close** button and in Add/Remove window click on **OK** to exit.

9. In the console tree, select **Personal – Certificates** container and locate new certificate **Issued By** *Smart Systems for Health Agency Root CA*.




10. Double-click the certificate generated from the CSR. The following dialog appears:



Ensure that the message "**You have a private key that corresponds to this certificate"** is displayed.

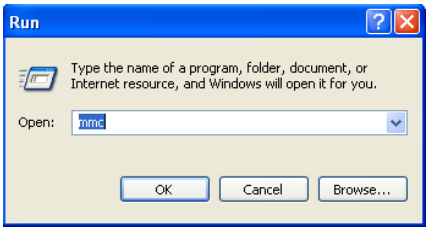
11. You have successfully installed the certificate.

# 8.0 Install eHealth Ontario's CA Root certificate

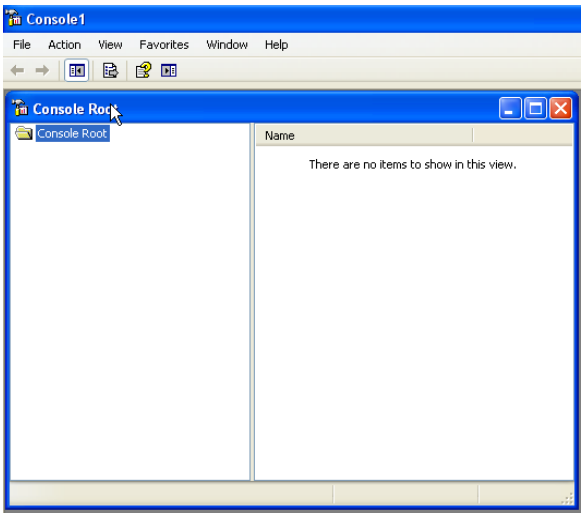
**Note:** You must also install the eHealth Ontario's Root Certificate; this is not the certificate which you installed earlier in Personal Certificates storage for local computer. If you are missing this certificate in your installation package please contact eHealth Ontario and they will provide this to you.

Install the **eHealth Ontario CA Root certificate** using Microsoft Management Console (**MMC**).

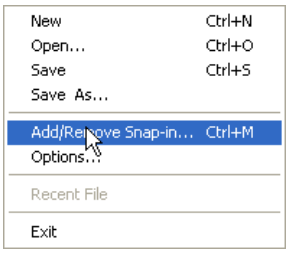
- From the **Start** menu, select **Run**. In the Run dialog box, type **mmc** and click **OK**.



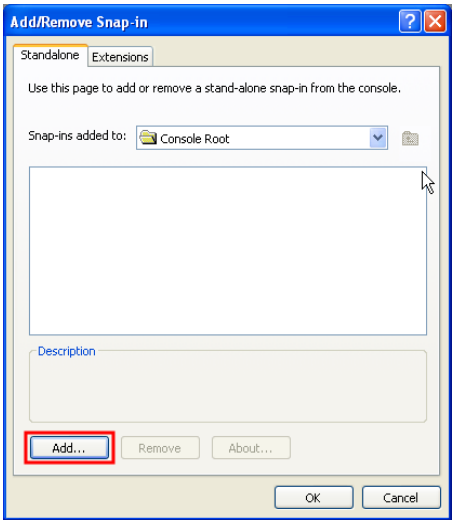

- The Microsoft Management Console is displayed.



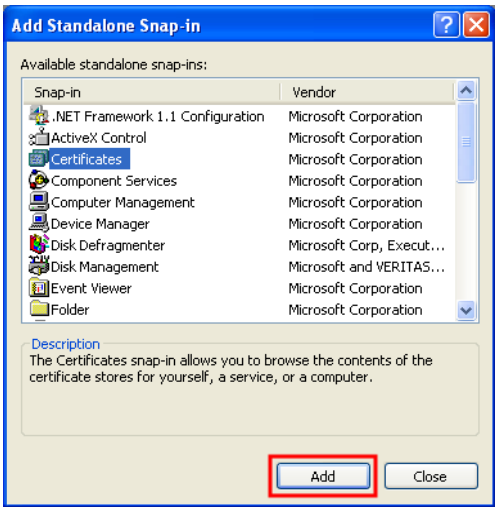

- From the **File** menu, select **Add/Remove Snap-in**.



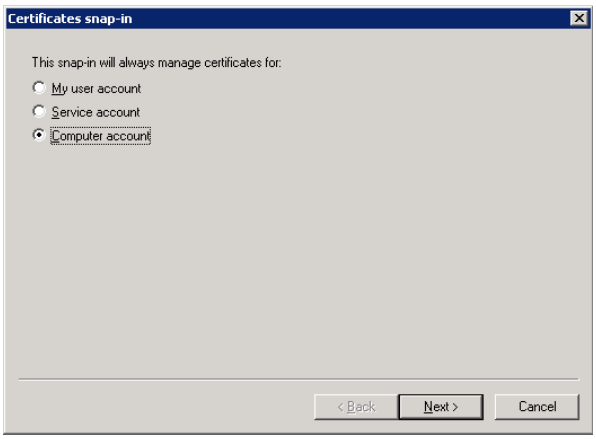

- On the Standalone tab, click **Add**.



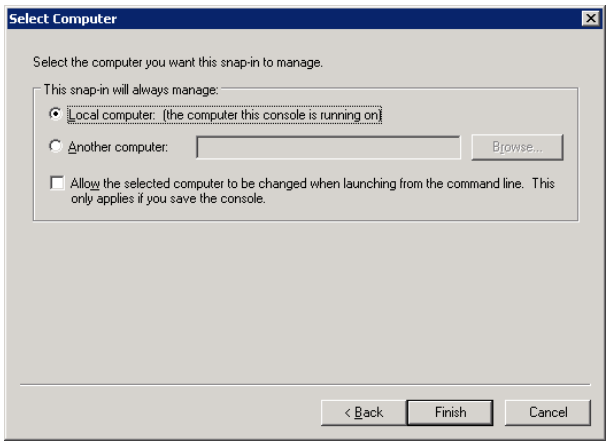

- From the Available Standalone Snap-in list box, select "**Certificates**", and then click **Add**.




- In **Certificates snap-in** pop-up window select **Computer account** and press **Next**

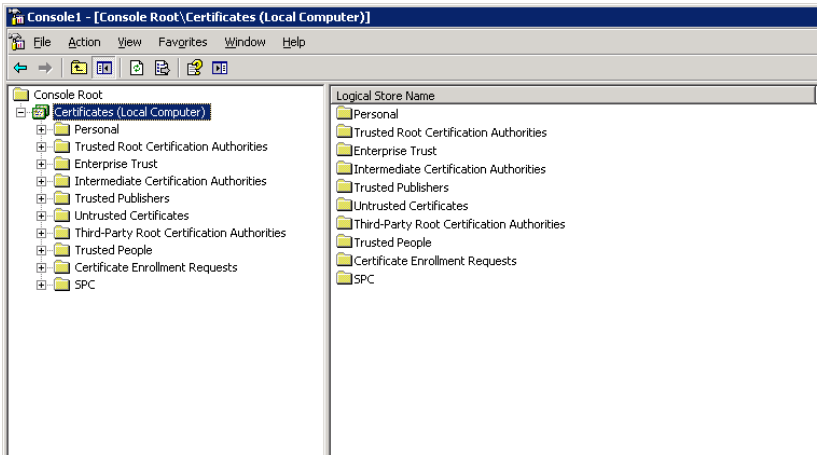



- In **Select Computer** pop-up window select **Local Computer** option and click on **Finish** button

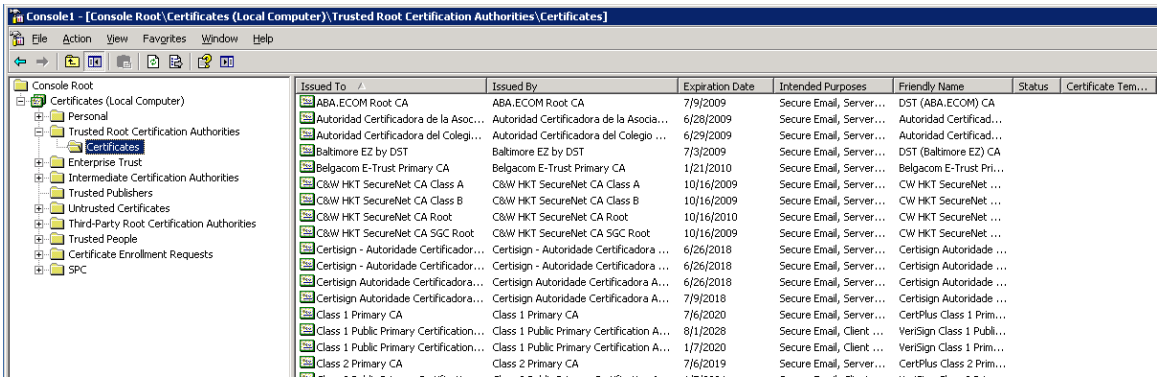



- In Stand Alone snap-in window press **Close** button and in Add/Remove window click on **OK** to exit

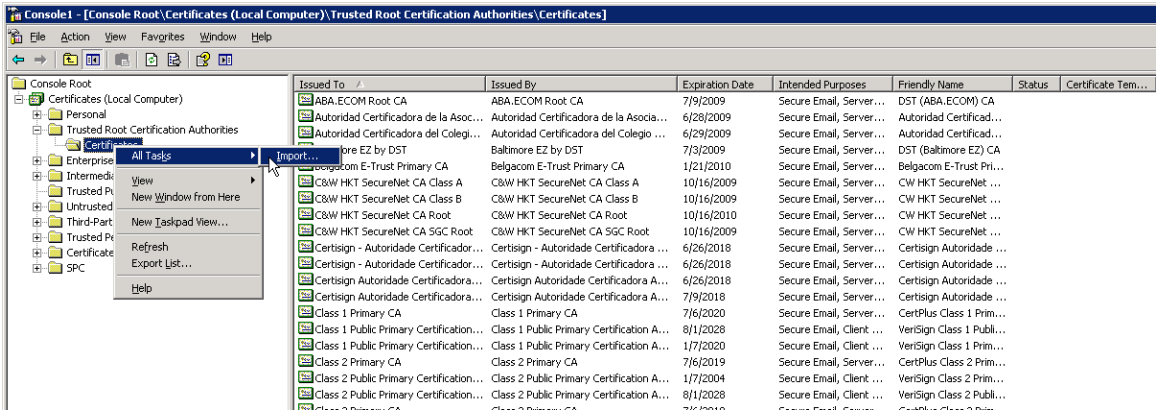
- In Microsoft Management Console (**MMC**), expend the **Certificates** snap-in



- In the console tree, select **Trusted Root Certificate Authorities – Certificates** container



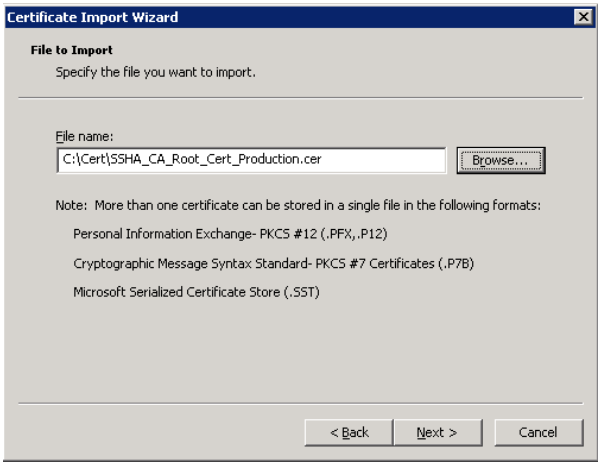

- Right click on it and select **All Task -> Import**



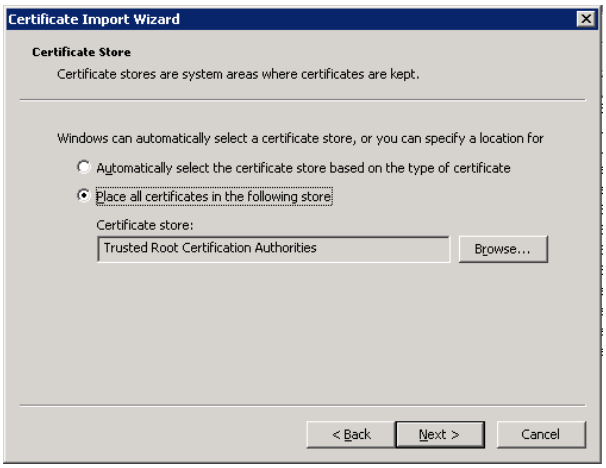

- Browse to the **eHealth Ontario CA Root certificate** received from eHealth Ontario and click **Next**


- Following the Wizard select **Next** and **Finish**

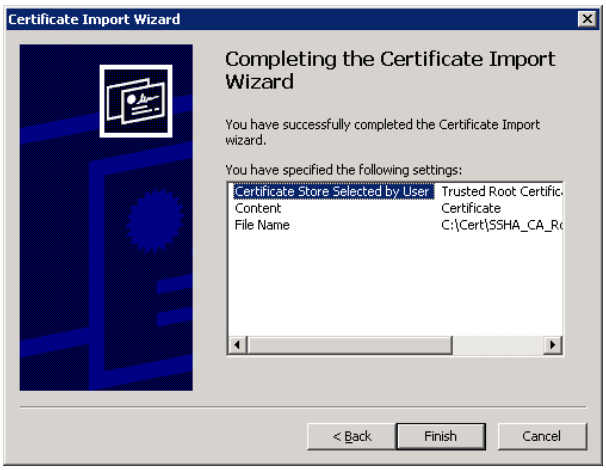

- In the **File to Import** screen click on **Browse** button, select eHealth Ontario CA Root Certificate which you received from eHealth Ontario and click on **Next** to proceed



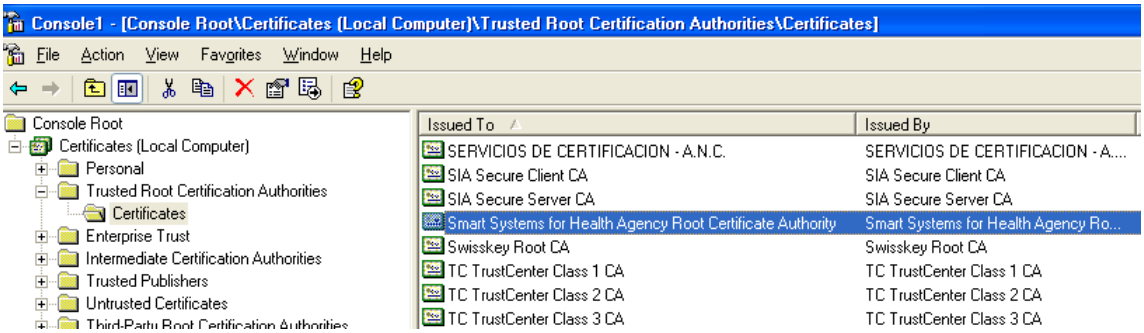

- In **Certificate Store** screen verify that **Place all certificates in the following store** and **Trusted Root Certification Authorities** options are selected and click on **Next** to proceed




- In **Completing** screen verify selected options and click on **Finish** to exit




- Open **Certificates** folder in the **Trusted Root Certificate Authorities** and verify if **EHEALTH ONTARIO CA Root certificate** is installed




- You have successfully installed the SSHA CA Root certificate.

# STOP

The next section of this *Client Deployment Guide* cannot be completed until your ONE Mail Partnered Deployment Date.

The following steps will be completed with the ONE Mail Technical Analyst working with you.

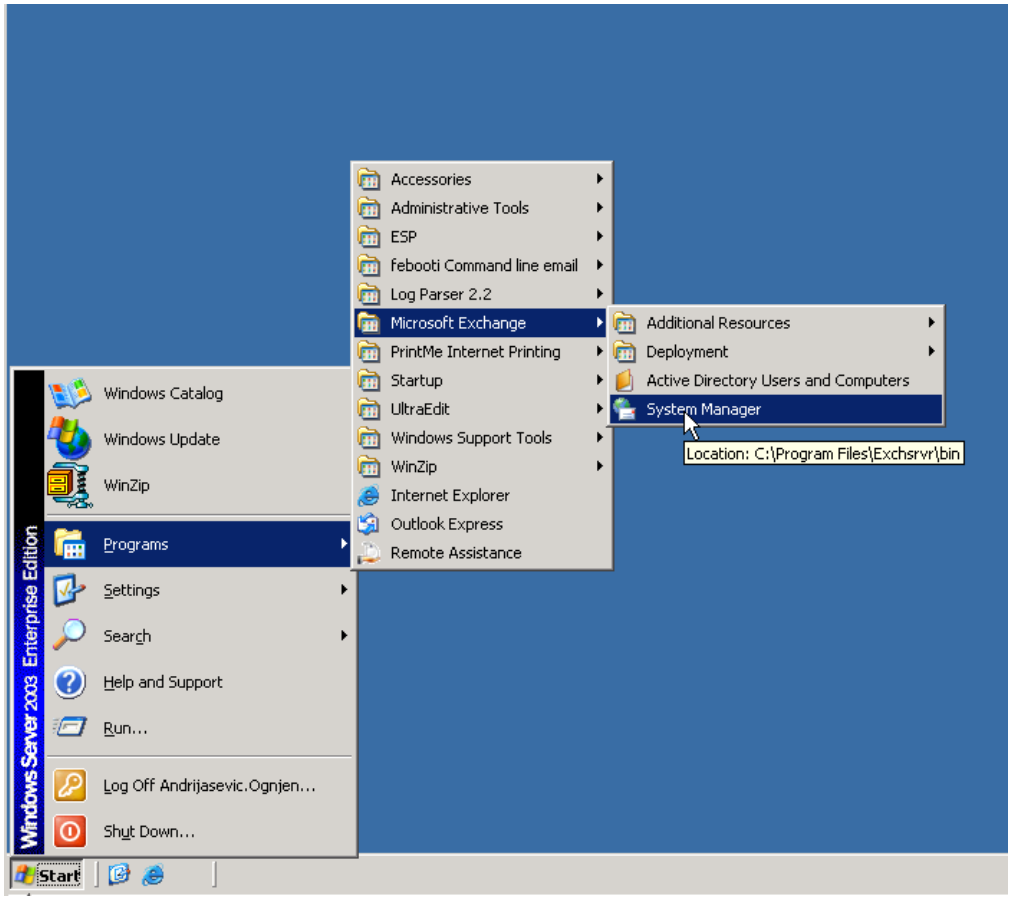
# 9.0 Setup SMTP Connector to ONE Mail Partnered Service

## 9.1 Setup SMTP Connector on Exchange 2000/2003

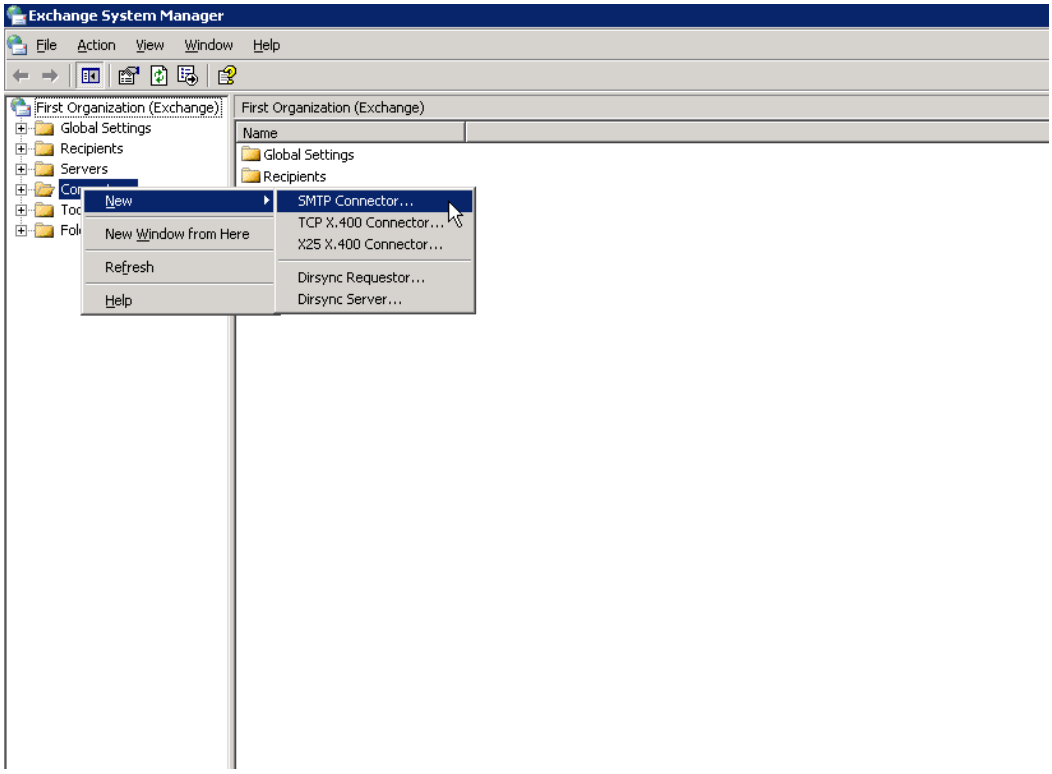
To create and configure a Connector for the ONE Mail Partnered environment on your Exchange Server 2000/2003 use Exchange System Manager Console, as explained below.

**NOTE:** If you are configuring MS Windows Server 2000/2003 IIS/SMTP server skip to chapter 9.1 Setup SMTP Connector on MS Windows Server 2000/2003.

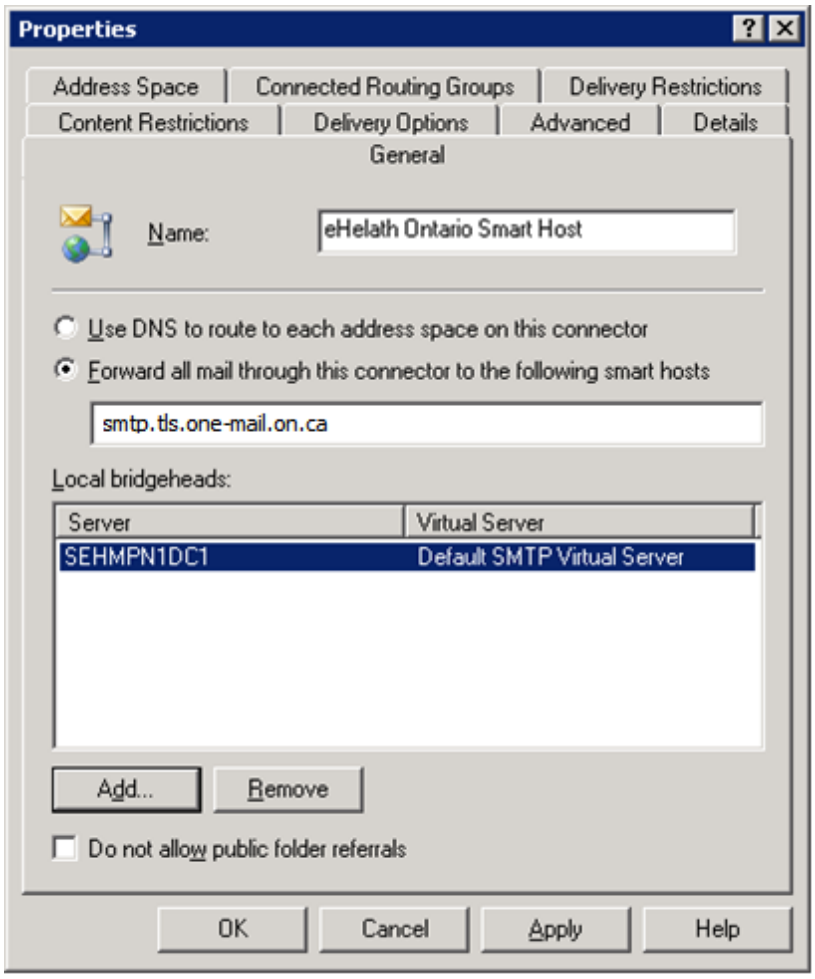
- Login to your Microsoft Exchange 2000/2003 host server.
- Click **Start** > **Programs** > **Microsoft Exchange** > **System Manager.**



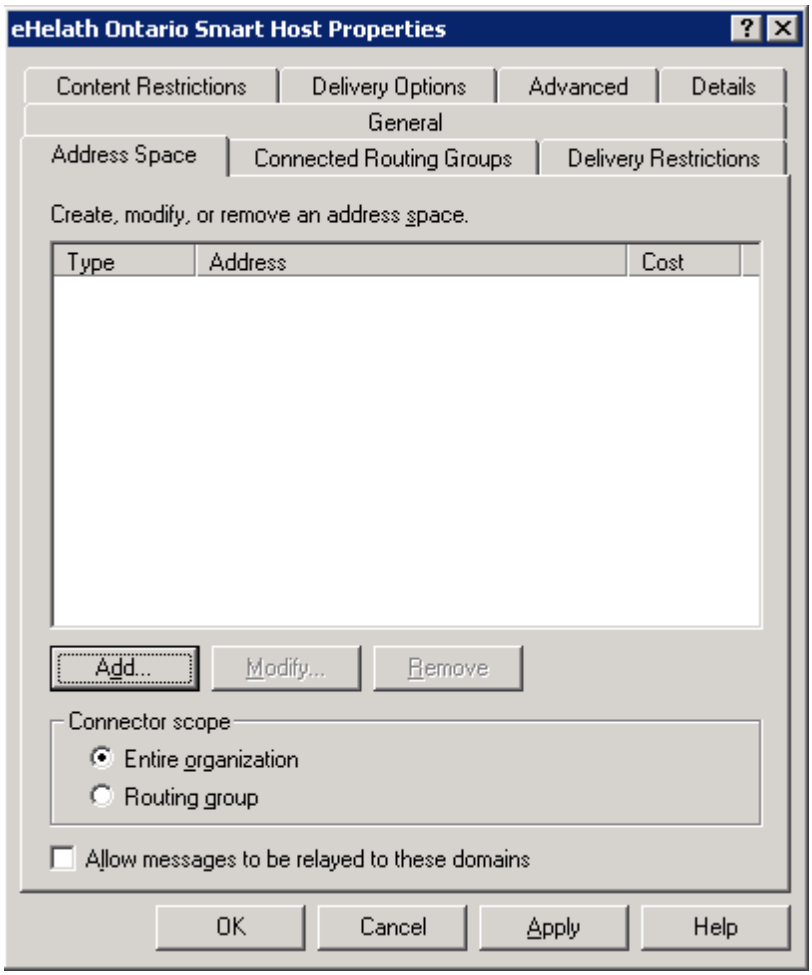
- In **Exchange System Manager** Console, in the left tree pane point to **Connectors** container, right click on it and chose **New/SMTP Connector** option to start New Connector Properties.



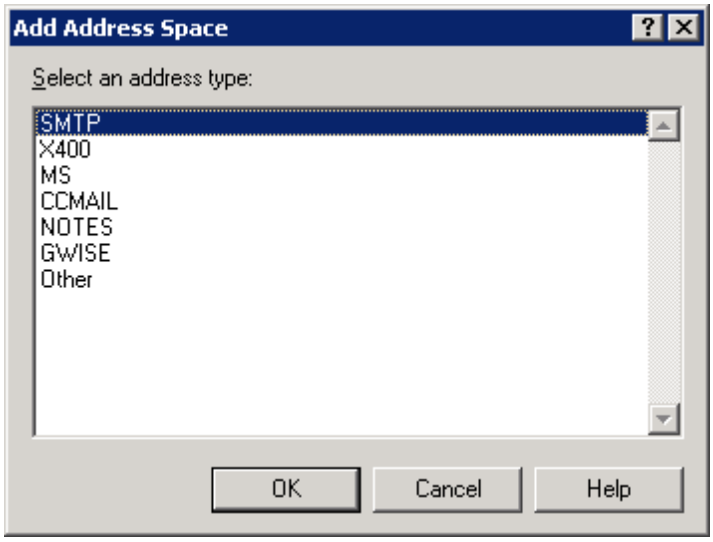

- On the **General** tab for new SMTP Connector specify the **Name** for connector (ex. eHealth Ontario Smart Host)**.** Chose option **Forward all mail through this connector to the following smart host** and specify *tls.one-mail.on.ca* FQDN for destination smart host. If **Local bridgehead** server is not selected, then click on **Add** button to specify your local gateway server as local bridgehead server (s).



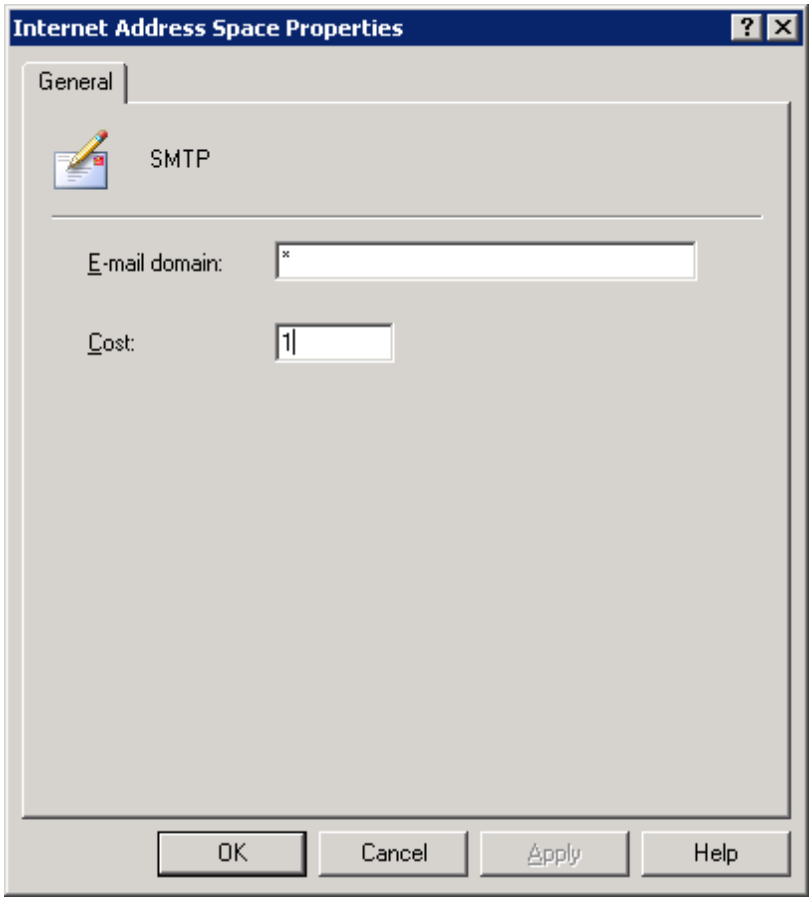

- On the **Address Space** tab of properties click on **Add** button to add ***** as connectors address space (this will setup your system to forward e-mail to all destination external SMTP domains through this connector). Check that **Entire organization** option is selected in **Connector Scope** field.



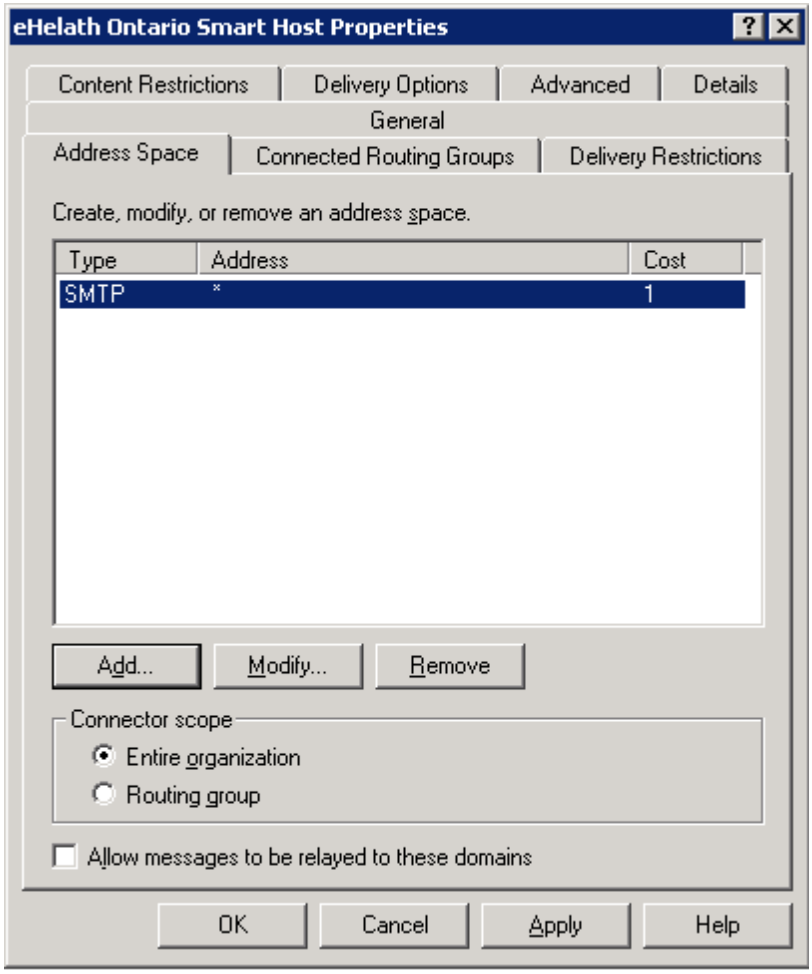

- In **Add Address Space** pop-up window select **SMTP** and click on **OK** to proceed



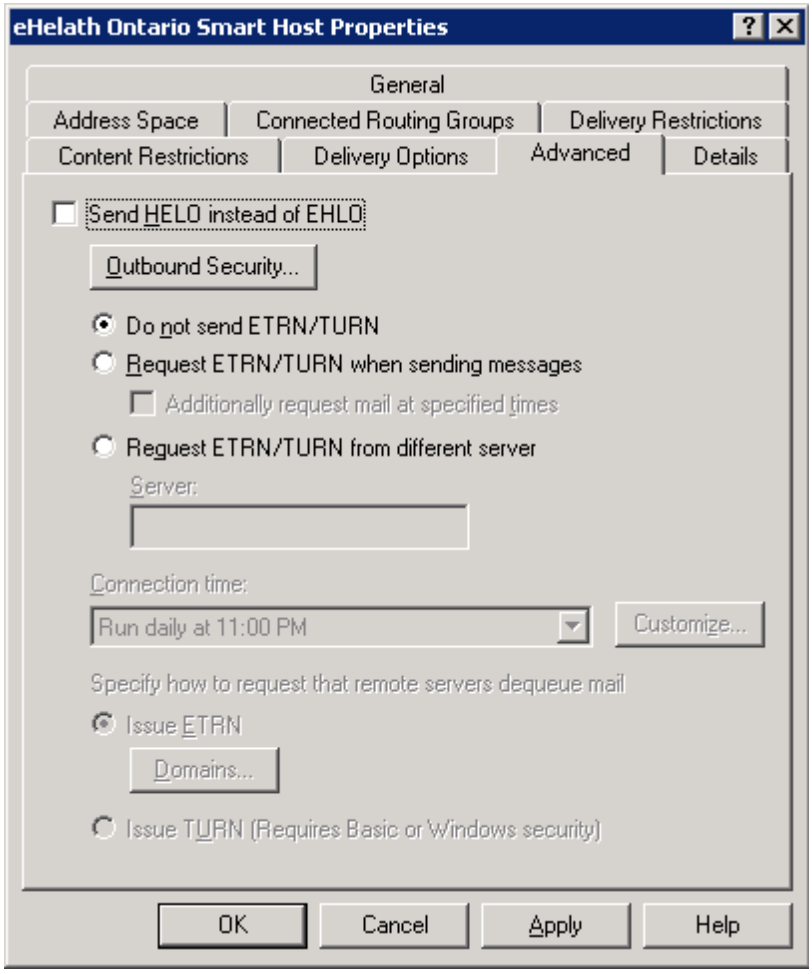
- In **Internet Address Space Properties** screen specify * as **E-mail domain** and *1* as **Cost** and click on **OK** to finish configuration of address space



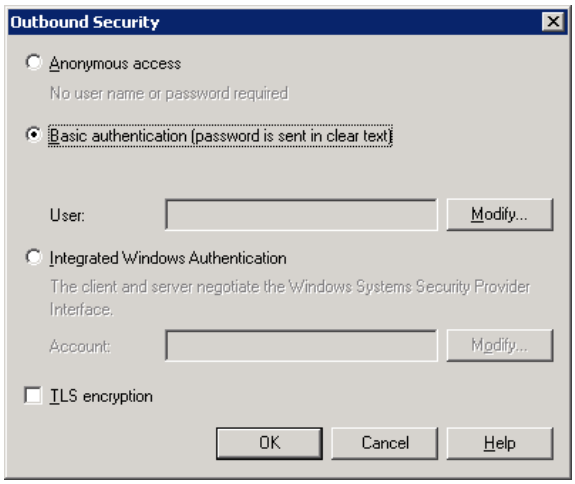

- Now your Address Space tab should look like following screen


eHelath Ontario Smart Host Properties
Content Restrictions
Delivery Options
Advanced
Details
General
Address Space
Connected Routing Groups
Delivery Restrictions
Create, modify, or remove an address space.
Type
Address
Cost
SMTP
*
1
Add...
Modify...
Remove
Connector scope
Entire organization
Routing group
Allow messages to be relayed to these domains
OK
Cancel
Apply
Help

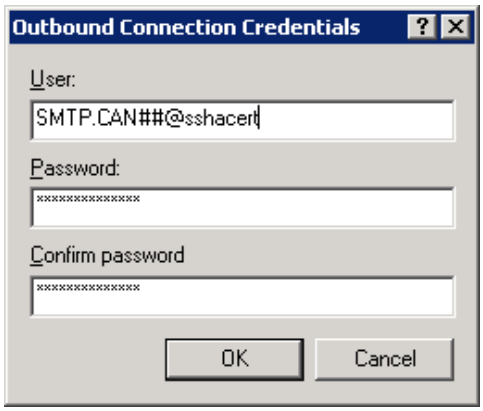
- Switch to **Advanced** tab and click on **Outbound Security…** button



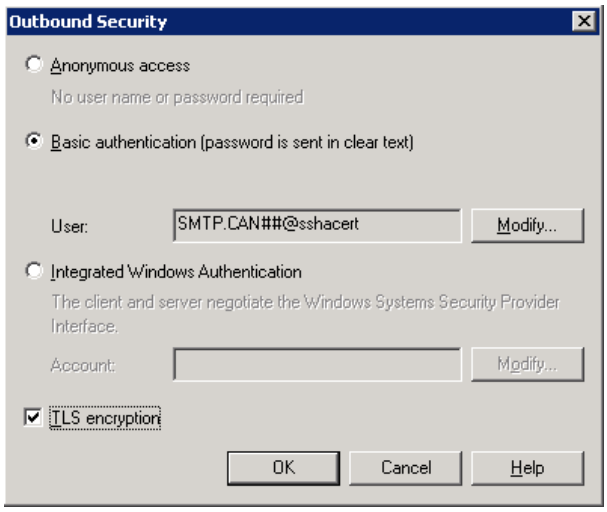

- On the Outbound Security screen select Basic authentication (password is sent in clear text) and click on Modify… button to specify user which will be used for authentication




- In **Outbound Connection Credentials** insert information about user account and password which was provided to you by eHealth Ontario's deployment team as part of deployment package. Click on **OK** to return to **Outbound Security** screen




- Select **TLS encryption** option and then click on OK to return to connector properties

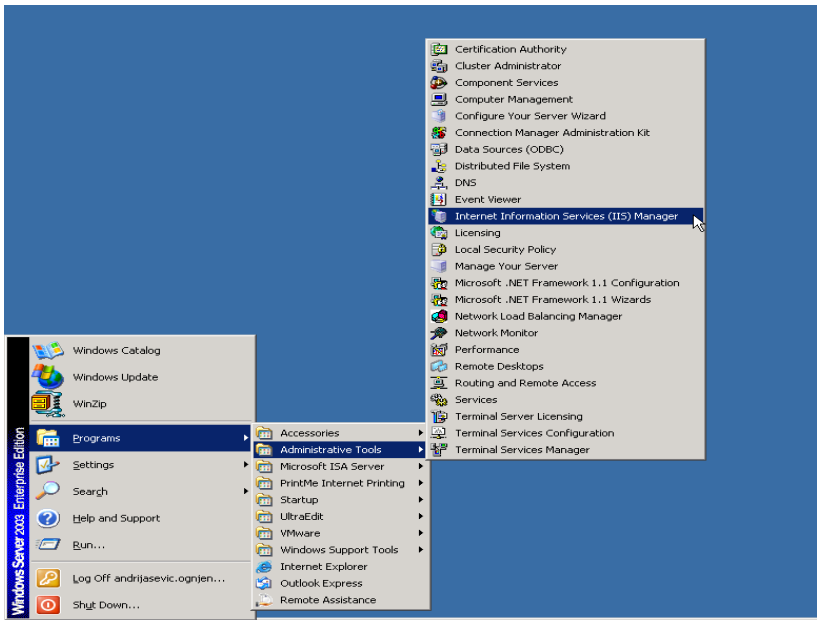



- Now you configured all necessary settings for this connector, click on **Apply** and **OK** buttons to apply all those and exit property pages.
- Open Services console and restart IIS Admin service to pick up new settings.
- Proceed with eHealth Ontario's deployment team with testing new configuration.

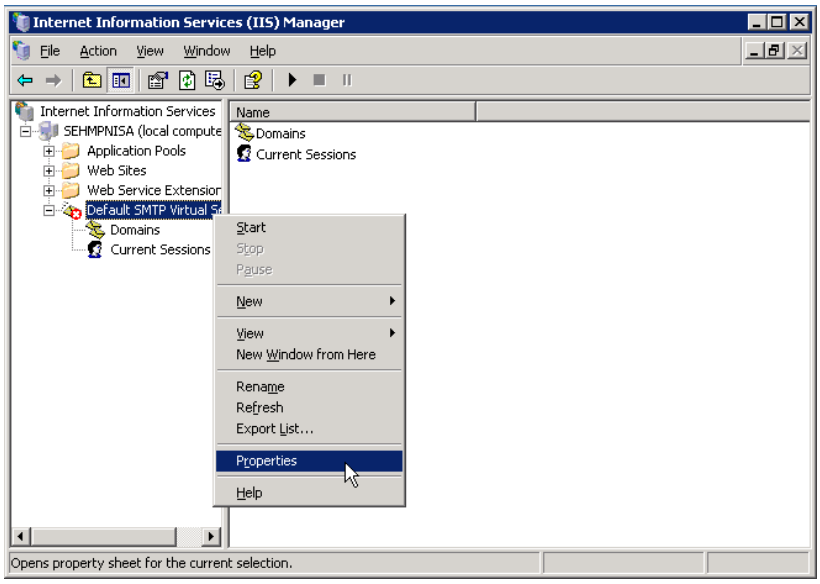
## 9.2 Setup SMTP Connector on Exchange 2000/2003

To create and configure a Connector for the ONE Mail Partnered environment on your MS Windows Server 2000/2003 use Internet Information Services Management Console, as explained below.

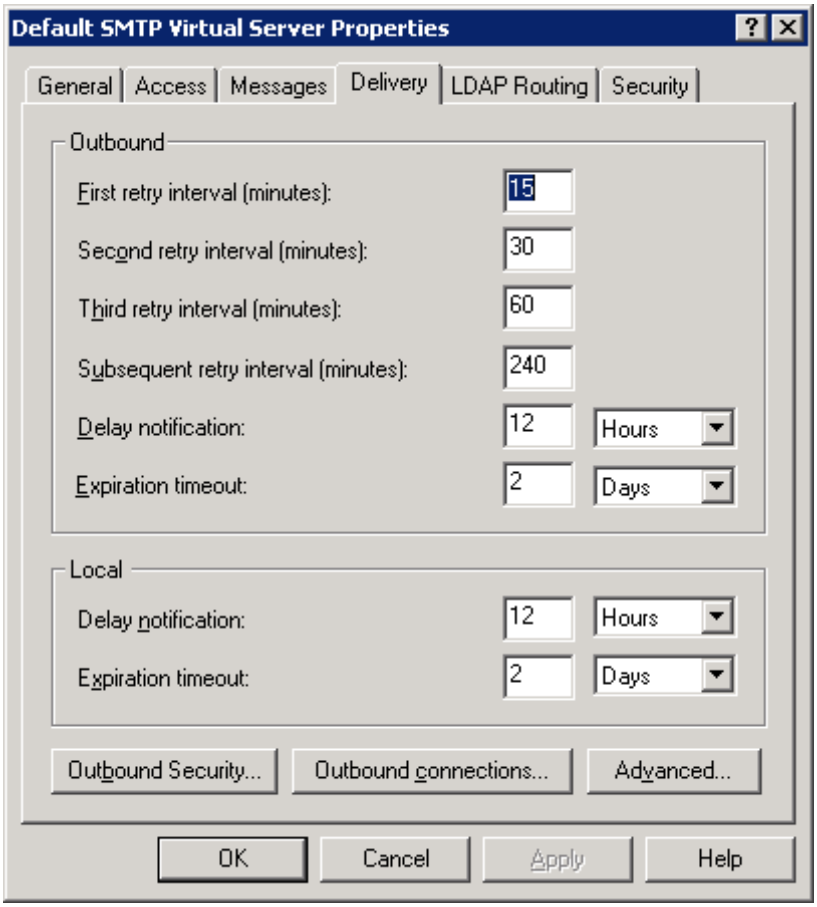
- Login to your MS Windows 2000/2003 host server.
- Click **Start** > **Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager.**




- In the left pane, expend you local server, point to **Default SMTP Virtual Server**, right click and select **Properties**

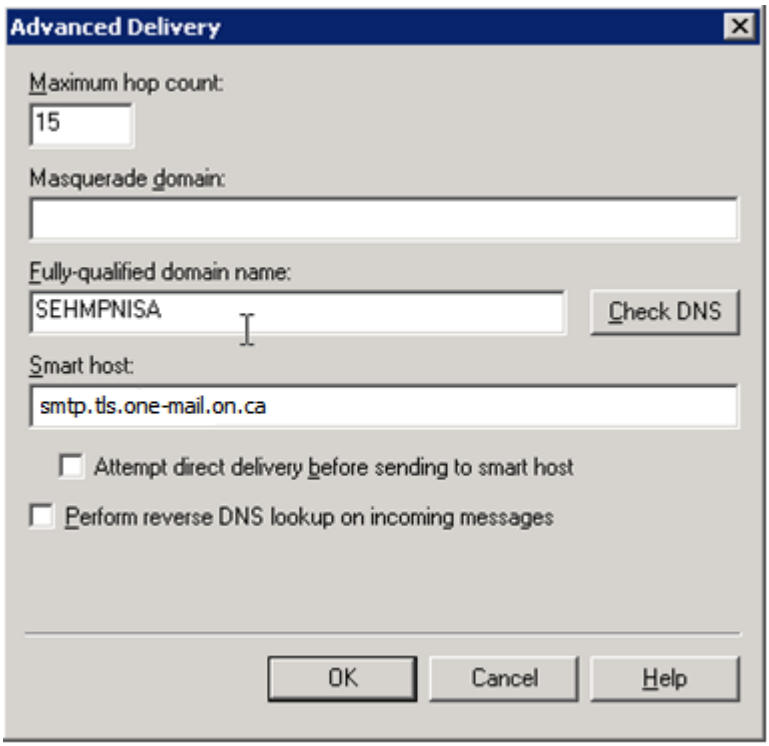



- Switch to **Delivery** tab and click on **Advanced** button

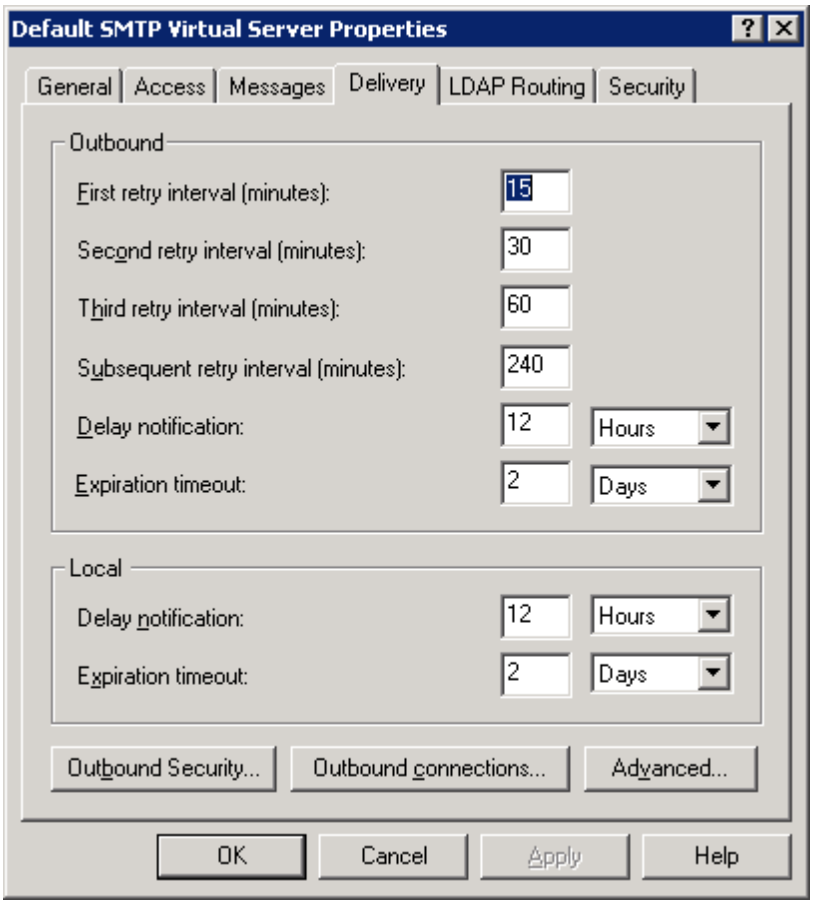



- On **Advanced Delivery** tab specify *tls.one-mail.on.ca* as **Smart Host** and check that **Attempt direct delivery before sending to smart host** and

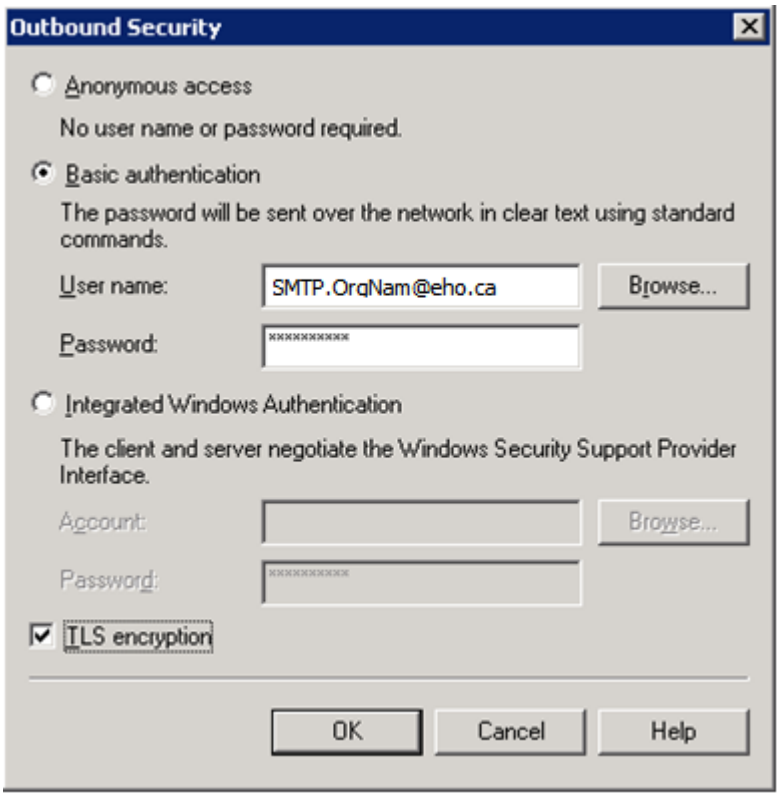
**Perform reverse DNS lookup on incoming messages** check boxes are not selected. Click on OK to return to SMTP Virtual Server Properties.




- Back on Delivery tab, now click on Outbound Security… button




- On **Outbound Security** screen select **Basic authentication** option and insert **User Name** and **Password** provided by eHealth Ontario's deployment team to you in appropriate fields. Select TLS encryption check box. Click on OK to return to SMTP Virtual Server prosperities.




- Now you configured all necessary settings for this connector, click on **Apply** and **OK** buttons to apply all those and exit property pages.
- Open Services console and restart IIS Admin service to pick up new settings.
- Proceed with eHealth Ontario's deployment team with testing new configuration.