eHealth Ontario

ONE® Mail Partnered – Client Deployment Guide

Instruction for Microsoft Exchange Server 2007

Version: 1.6

Document ID: 3234

Document Owner: ONE Mail Product Team

Ontario
eHealth Ontario

Copyright Notice

All rights reserved

Trademarks

Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

APPROVER(S)	TITLE/DEPARTMENT	APPROVED DATE
ONE Mail Product Team	ONE Mail Product Team	2013-06-28

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.0	2008-08	Initial draft (Anatoly Kurdin) certificate	Anotoly Kurdin
1.1	2008-09	Initial draft (Ognjen Andrijasevic) connectors	Ognjen Andrijasevic
1.2	2008-09	Corrected document based on input from Alias Downey, David Thabet and Anatoly Kurdin	Anotoly Kurdin
1.3	2008-09	Integrated changes requested by Deployment team, related to adding new Send and Receive Connectors, instead modifying exiting ones	Ognjen Andrijasevic
1.4	2010-05	Added parameter in CSR to make private key exportable	
1.5	2012-06	Removed section for disabling SMTP service on other certificates, moved section for setting up Receive Connector before section for setting up Send Connector, added STOP message after configuration of Receive Connector	Ognjen Andrijasevic
1.6	2013-05	Updated for Internet Deployments	SMI review/addition

Document ID

3234

Document Sensitivity Level

Medium

Contents

1.0 Introduction

This document describes the steps required to connect Microsoft Exchange Server 2007 to ONE Mail Partnered product for secure e-mail routing:

- Generate a request for a PKI certificate
- Install the created certificate
- Install SSHA 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 2007 (with or without Service Packs 1, 2 or 3) installed on Windows Server 2003 or Microsoft Exchange Server 2007 SP1, SP2 or SP3 installed on Windows Server 2008.

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 is 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 SSHA CA Trusted Root certificate**

8. **Setup Default Receive Connector on Exchange Server 2007**

9. **Setup Send Connector on Exchange Server 2007**

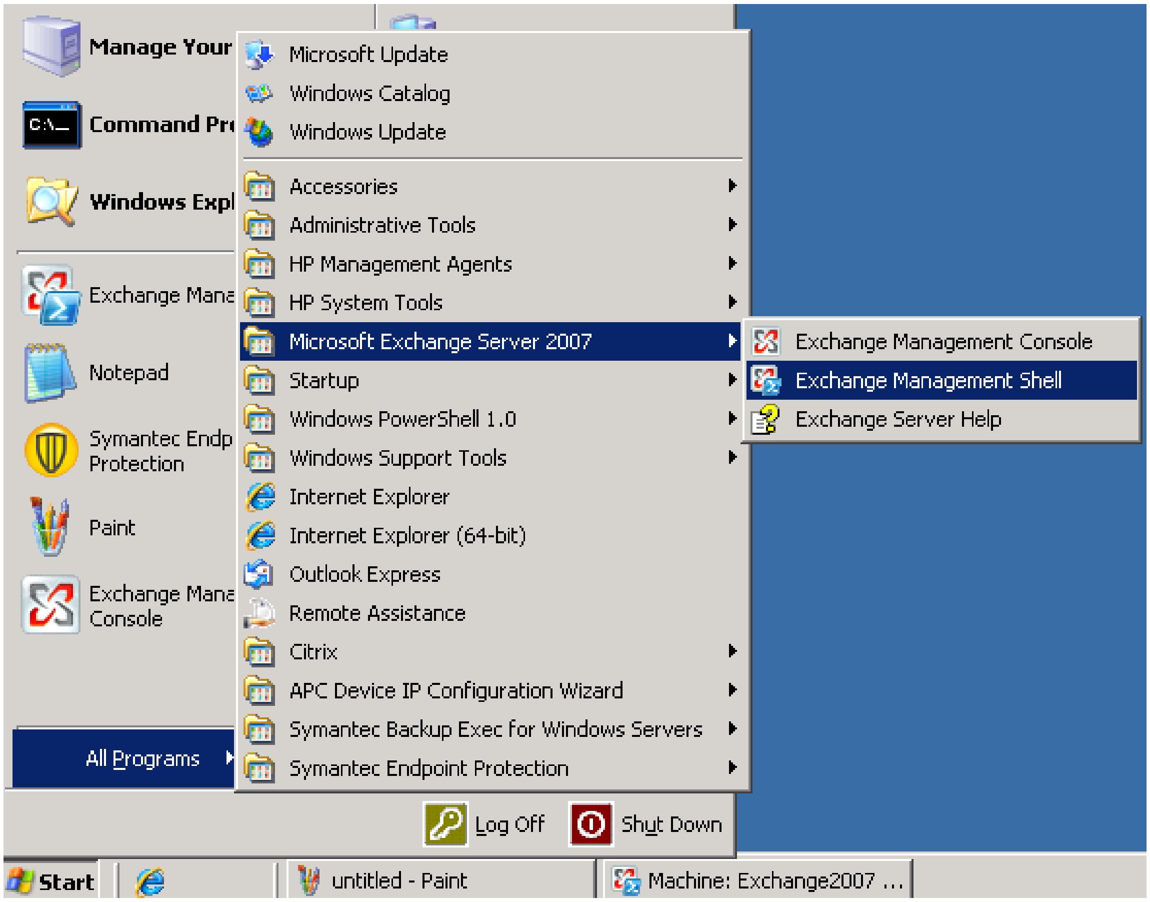
4.0 Creating CSR(s)

> Note: **Note:** 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.

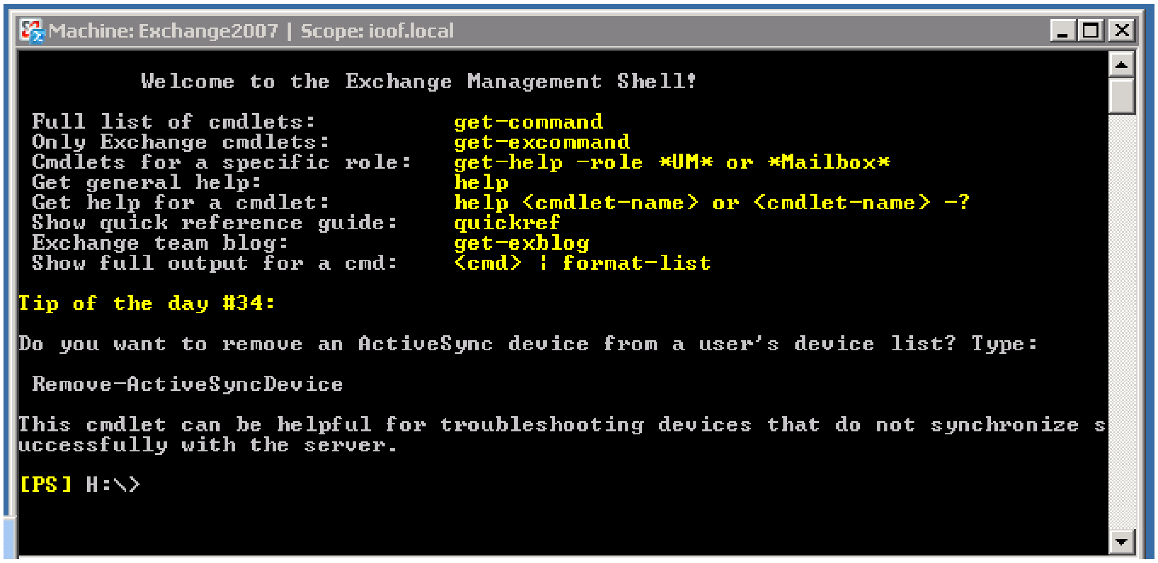
4.1 Generating a CSR

To generate a CSR for Microsoft Exchange Server 2007 use Exchange Management Shell, as explained below:

- Login to your Microsoft Exchange Server 2007 host server
- Click **Start** > **Programs** > **Microsoft Exchange Server 2007** > **Exchange Management Shell**



- The shell windows will be displayed



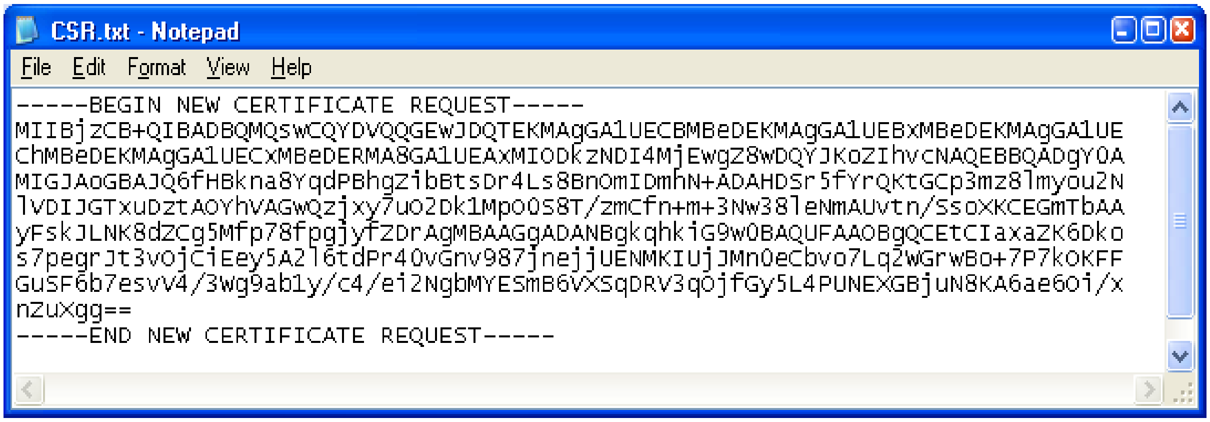
```
         Welcome to the Exchange Management Shell!

 Full list of cmdlets:          get-command
 Only Exchange cmdlets:         get-excommand
 Cmdlets for a specific role:   get-help -role *UM* or *Mailbox*
 Get general help:              help
 Get help for a cmdlet:         help <cmdlet-name> or <cmdlet-name> -?
 Show quick reference guide:    quickref
 Exchange team blog:            get-exblog
 Show full output for a cmd:    <cmd> | format-list

Tip of the day #34:

Do you want to remove an ActiveSync device from a user's device list? Type:

 Remove-ActiveSyncDevice

This cmdlet can be helpful for troubleshooting devices that do not synchronize s
uccessfully with the server.

[PS] H:\>
```

- Type-in the following **command** and press “Enter”

```
New-ExchangeCertificate -GenerateRequest: $True –PrivateKeyExportable $true -
DomainName <Your_Domain_Name> -SubjectName
"C=CA,O=<Your_Organization_Name>,ST=ON,CN=<Reference Number>" -Keysize 1024 -Path
"C:\CSR.txt"
```

Note: New-ExchangeCertificate utility requires the user to enter at least one **Domain Name**. This name is supposed to be added to the certificate **Alternative Subject Name List**. Currently, SSHA Certificate Authority **does not support** alternative subject name certificate property. As a result, the value provided for this field will be ignored by SSHA CA. However, to meet the utility requirement **you need to provide a valid domain name**.

- If the command is successfully executed open the created file specified in the **-Path** parameter. The file should have a similar content:



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBjzCB+QIBADBQMQswCQYDVQQGEwJDQTEKMAgGA1UECBMBeDEKMAgGA1UEBxMBeDEKMAgGA1UE
ChMBeDEKMAgGA1UECxMBeDERMA8GA1UEAxMIODkzNDI4MjEwgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAJQ6fHBkna8YqdPBhgZibBtsDr4Ls8BnOmIDmhN+ADAHDSr5fYrQKtGCp3mz8lmyou2N
lVDIJGTxuDztAOYhVAGwQzjxy7uO2Dk1MpO0S8T/zmCfn+m+3Nw38leNmAUvtn/SsoXKCEGmTbAA
yFskJLNK8dZCg5Mfp78fpgjyfZDrAgMBAAGgADANBgkqhkiG9w0BAQUFAAOBgQCEtCIaxaZK6Dko
s7pegrJt3vOjCiEey5A2l6tdPr40vGnv987jnejjUENMKIUjJMn0eCbvo7Lq2WGrwBo+7P7kOKFF
GuSF6b7esvV4/3Wg9ably/c4/ei2NgbMYESmB6VXSqDRV3qOjfGy5L4PUNEXGBjuN8KA6ae6Oi/x
nZuXgg==
-----END NEW CERTIFICATE REQUEST-----
```

- Complete the above procedure for each certificate you need to create, **entering a new Reference Number, and a new output file name for each request**. This will result in a new CSR each time the procedure is executed.

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 SSHA CA, it will be sent to you in a file.

Its contents will resemble the following:

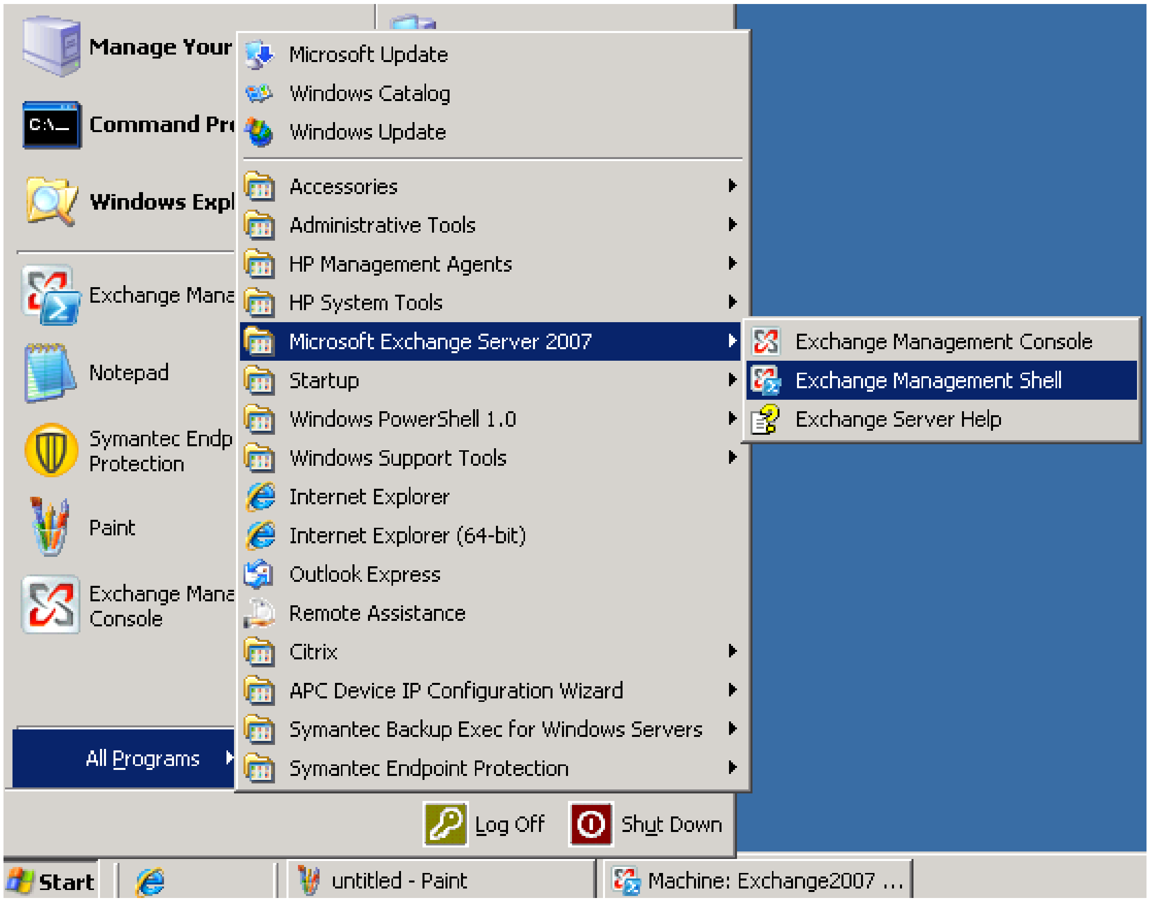
```
-----BEGIN CERTIFICATE-----
MIIGYAYJKoZIhvcNAQcCoIIGUTCCBk0CAQExADALBgkqhkiG9w0BBwGgggY1MIIG
MTCCBRmgAwIBAgIEQA9uVDANBgkqhkiG9w0BAQUFADCBpjETMBEGCgmSJomT8ixk
ARkWA3NzaDEbMBkGCgmSJomT8ixkARkWC1N1YnNjcmliZXJzMRUwEwYDVQQLEwxT
U0ggU2VydmljZXMxETAPBgNVBAsTCFNlY3VyaXR5MQwwCgYDVQQLEwNQS0kxOjA4
BgNVBAMTMVNtYXJ0IFN5c3RlbXMgZm9yIEhlYWx0aCBBZ2VuY3kgUm9vdCBDQSAt
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.

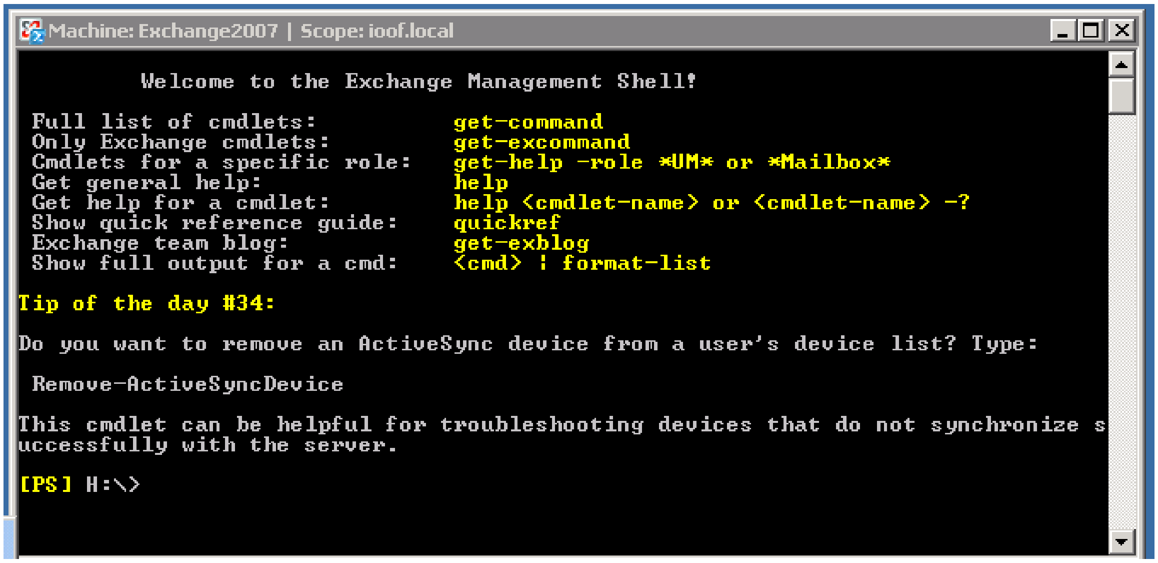
6.0 Installing an Exchange Certificate

To install the certificate received from eHealth Ontario for Microsoft Exchange Server 2007 use the Exchange Management Shell, as explained below:

- Login to your Microsoft Exchange Server 2007 host server
- Click **Start** > **Programs** > **Microsoft Exchange Server 2007** > **Exchange Management Shell**



- The shell windows will be displayed

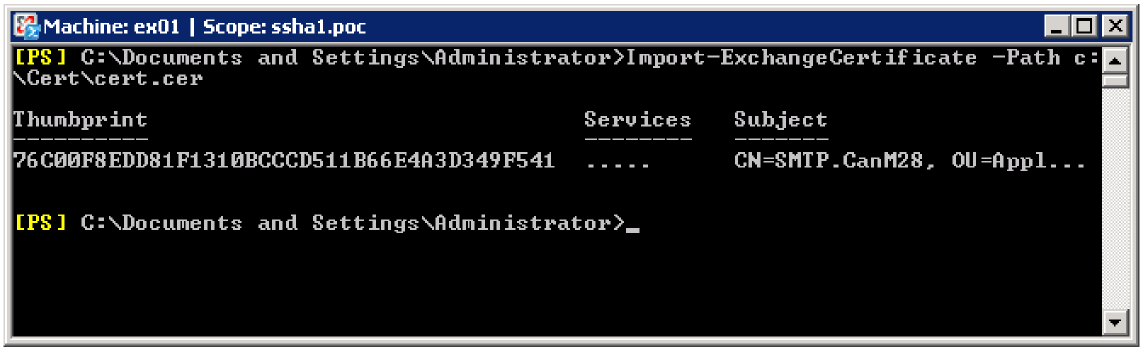


```
         Welcome to the Exchange Management Shell!

 Full list of cmdlets:          get-command
 Only Exchange cmdlets:         get-excommand
 Cmdlets for a specific role:   get-help -role *UM* or *Mailbox*
 Get general help:              help
 Get help for a cmdlet:         help <cmdlet-name> or <cmdlet-name> -?
 Show quick reference guide:    quickref
 Exchange team blog:            get-exblog
 Show full output for a cmd:    <cmd> | format-list

Tip of the day #34:

Do you want to remove an ActiveSync device from a user's device list? Type:

 Remove-ActiveSyncDevice

This cmdlet can be helpful for troubleshooting devices that do not synchronize s
uccessfully with the server.

[PS] H:\>
```

- Type-in the following command and press **Enter**

```
Import-ExchangeCertificate -Path c:\Cert\cert.cer
```

The command (if successfully executed) will install the certificate and enable it for **SMTP** service:



```
[PS] C:\Documents and Settings\Administrator>Import-ExchangeCertificate -Path c:
\Cert\cert.cer

Thumbprint                                Services   Subject
----------                                --------   -------
76C00F8EDD81F1310BCCCD511B66E4A3D349F541  .....      CN=SMTP.CanM28, OU=Appl...


[PS] C:\Documents and Settings\Administrator>_
```

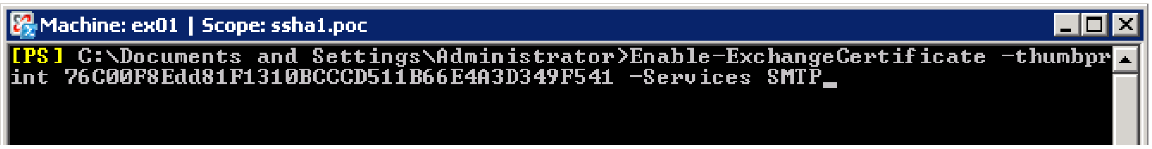
Note: **Note:** You have to specify the path and name of the certificate which was issued by eHealth Ontario for you, based on your previous CSR. Do not specify the path and name of the SSHA Root Certificate, that certificate will be installed later in another location.

- Type-in the following command and press **Enter**

```
Enable-ExchangeCertificate –Thumbprint eHealth Ontario_Certificate_ThumbPrint -
Services SMTP
```

Where *eH0_Cerificate_ThumbPrint* is thumbprint of eHealth Ontario issued certificate visible in output of previous command.

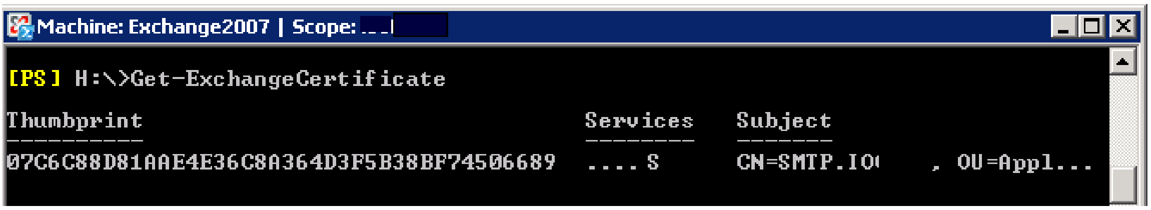
The command (if successfully executed) will enable this certificate for **SMTP** service:



```
[PS] C:\Documents and Settings\Administrator>Enable-ExchangeCertificate -thumbpr
int 76C00F8Edd81F1310BCCCD511B66E4A3D349F541 -Services SMTP_
```

7.0 Verifying the Exchange Certificate Installation

To verify the certificate installation, run *Get-ExchangeCertificate* command from Exchange Management Shell. The command should provide the certificate subject name, its thumbprint and a list of enabled services (**S - SMTP** for this example shown here).



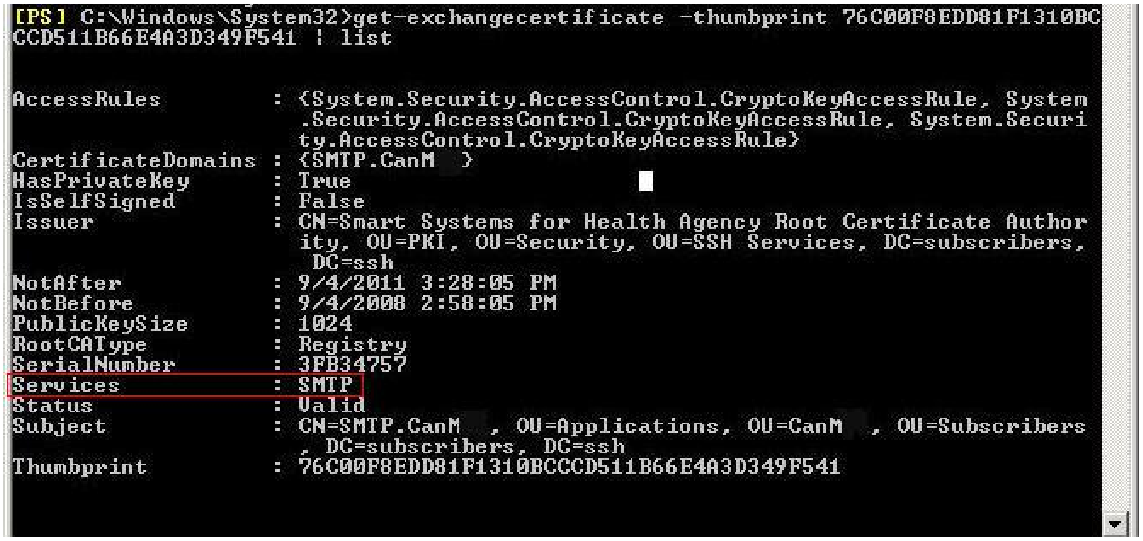
```
[PS] H:\>Get-ExchangeCertificate

Thumbprint                                Services   Subject
----------                                --------   -------
07C6C88D81AAE4E36C8A364D3F5B38BF74506689  ....S      CN=SMTP.IO[redacted], OU=Appl...
```

- Type-in the following command and press **Enter**

```
Get-ExchangeCertificate –Thumbprint eHo_Certificate_ThumbPrint |Format-List
```

Where *eHealth Ontario_Cerificate_ThumbPrint* is thumbprint of eHealth Ontario issued certificate visible in output of *Get-ExchangeCertificate* command.

In the **"Services"** property of this certificate you should see only SMTP service as in the example shown below:



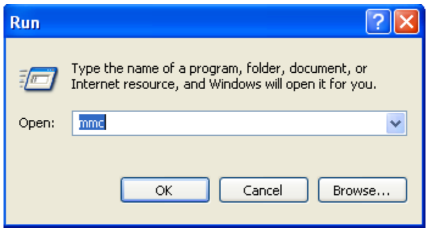
```
[PS] C:\Windows\System32>get-exchangecertificate -thumbprint 76C00F8EDD81F1310BC
CCD511B66E4A3D349F541 | list


AccessRules        : {System.Security.AccessControl.CryptoKeyAccessRule, System
                     .Security.AccessControl.CryptoKeyAccessRule, System.Securi
                     ty.AccessControl.CryptoKeyAccessRule}
CertificateDomains : {SMTP.CanM[redacted]}
HasPrivateKey      : True
IsSelfSigned       : False
Issuer             : CN=Smart Systems for Health Agency Root Certificate Author
                     ity, OU=PKI, OU=Security, OU=SSH Services, DC=subscribers,
                      DC=ssh
NotAfter           : 9/4/2011 3:28:05 PM
NotBefore          : 9/4/2008 2:58:05 PM
PublicKeySize      : 1024
RootCAType         : Registry
SerialNumber       : 3FB34757
Services           : SMTP
Status             : Valid
Subject            : CN=SMTP.CanM[redacted], OU=Applications, OU=CanM[redacted], OU=Subscribers
                     , DC=subscribers, DC=ssh
Thumbprint         : 76C00F8EDD81F1310BCCCD511B66E4A3D349F541
```

8.0 Install SSHA CA Root Certificate

Note: **Note:** You must also install the SSHA 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 **SSHA CA Root certificate** using Microsoft Management Console (**MMC**).

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

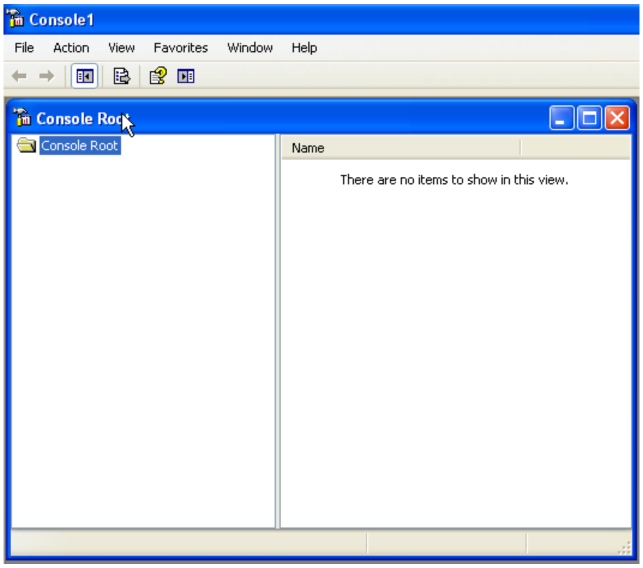


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

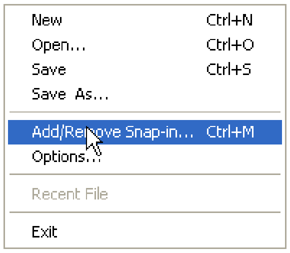
Open: mmc

- The Microsoft Management Console is displayed.

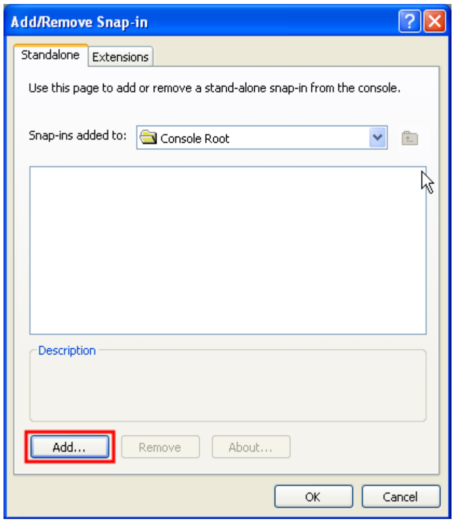


There are no items to show in this view.

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



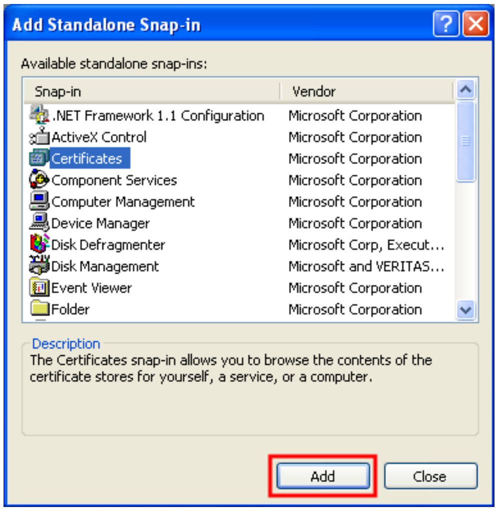
- On the Standalone tab, click **Add**.



Use this page to add or remove a stand-alone snap-in from the console.

Snap-ins added to: Console Root

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

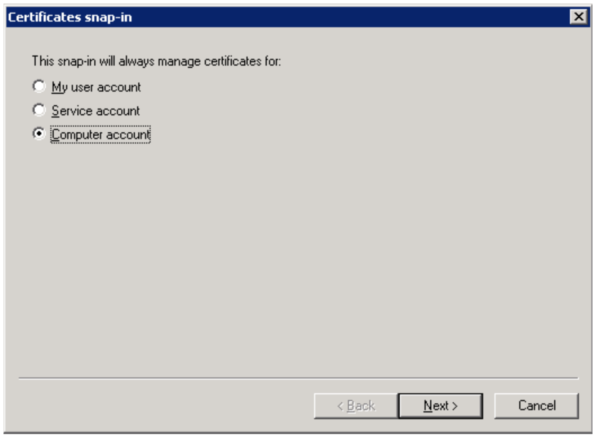


Available standalone snap-ins:

Snap-in	Vendor
.NET Framework 1.1 Configuration	Microsoft Corporation
ActiveX Control	Microsoft Corporation
Certificates	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
Disk Defragmenter	Microsoft Corp, Execut...
Disk Management	Microsoft and VERITAS...
Event Viewer	Microsoft Corporation
Folder	Microsoft Corporation

Description
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

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



Certificates snap-in

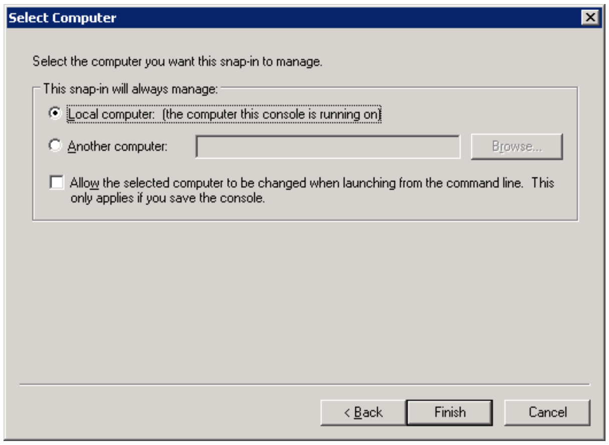
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

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



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

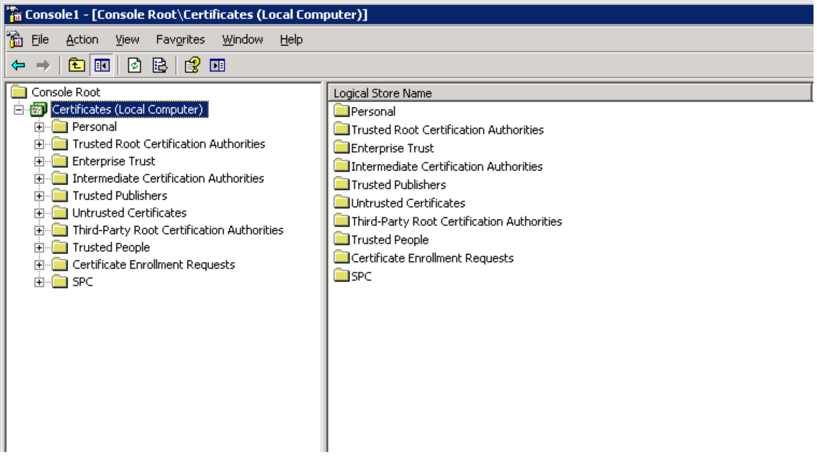
● Local computer: (the computer this console is running on)

○ Another computer:

☐ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

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

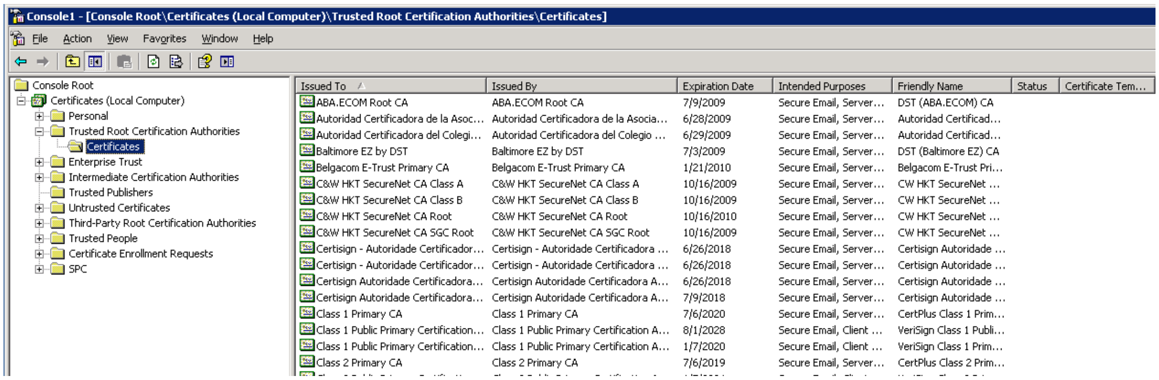
- In Microsoft Management Console (**MMC**), expend the **Certificates** snap-in.



Console1 - [Console Root\Certificates (Local Computer)]

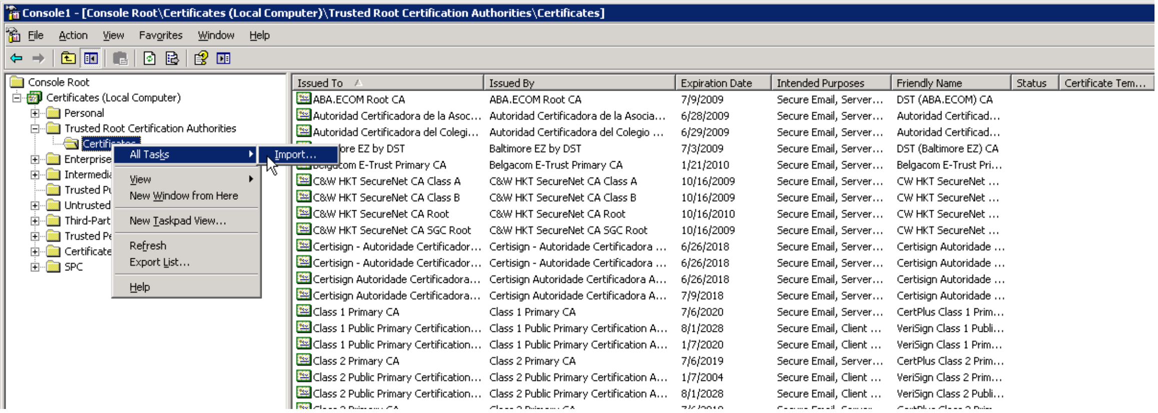
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Certificate Enrollment Requests
SPC
Logical Store Name
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Certificate Enrollment Requests
SPC

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


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Certificate Enrollment Requests
SPC

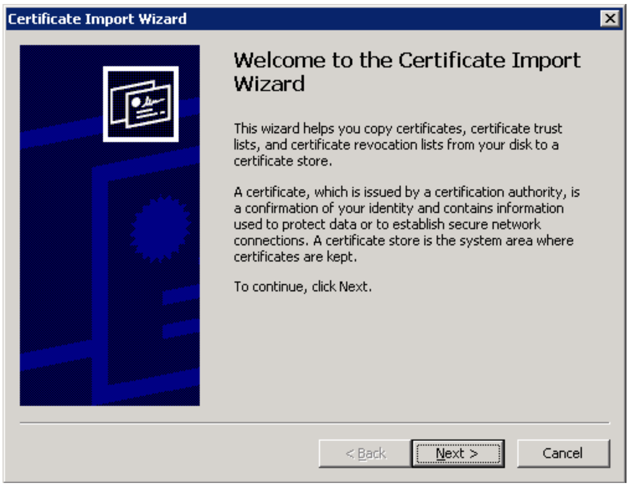
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
ABA.ECOM Root CA	ABA.ECOM Root CA	7/9/2009	Secure Email, Server...	DST (ABA.ECOM) CA		
Autoridad Certificadora de la Asoc...	Autoridad Certificadora de la Asocia...	6/28/2009	Secure Email, Server...	Autoridad Certificad...		
Autoridad Certificadora del Colegi...	Autoridad Certificadora del Colegio ...	6/29/2009	Secure Email, Server...	Autoridad Certificad...		
Baltimore EZ by DST	Baltimore EZ by DST	7/3/2009	Secure Email, Server...	DST (Baltimore EZ) CA		
Belgacom E-Trust Primary CA	Belgacom E-Trust Primary CA	1/21/2010	Secure Email, Server...	Belgacom E-Trust Pri...		
C&W HKT SecureNet CA Class A	C&W HKT SecureNet CA Class A	10/16/2009	Secure Email, Server...	CW HKT SecureNet ...		
C&W HKT SecureNet CA Class B	C&W HKT SecureNet CA Class B	10/16/2009	Secure Email, Server...	CW HKT SecureNet ...		
C&W HKT SecureNet CA Root	C&W HKT SecureNet CA Root	10/16/2010	Secure Email, Server...	CW HKT SecureNet ...		
C&W HKT SecureNet CA SGC Root	C&W HKT SecureNet CA SGC Root	10/16/2009	Secure Email, Server...	CW HKT SecureNet ...		
Certisign - Autoridade Certificador...	Certisign - Autoridade Certificadora ...	6/26/2018	Secure Email, Server...	Certisign Autoridade ...		
Certisign - Autoridade Certificador...	Certisign - Autoridade Certificadora ...	6/26/2018	Secure Email, Server...	Certisign Autoridade ...		
Certisign Autoridade Certificadora...	Certisign Autoridade Certificadora A...	6/26/2018	Secure Email, Server...	Certisign Autoridade ...		
Certisign Autoridade Certificadora...	Certisign Autoridade Certificadora A...	7/9/2018	Secure Email, Server...	Certisign Autoridade ...		
Class 1 Primary CA	Class 1 Primary CA	7/6/2020	Secure Email, Server...	CertPlus Class 1 Prim...		
Class 1 Public Primary Certification...	Class 1 Public Primary Certification A...	8/1/2028	Secure Email, Client ...	VeriSign Class 1 Publi...		
Class 1 Public Primary Certification...	Class 1 Public Primary Certification A...	1/7/2020	Secure Email, Client ...	VeriSign Class 1 Prim...		
Class 2 Primary CA	Class 2 Primary CA	7/6/2019	Secure Email, Server...	CertPlus Class 2 Prim...		

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



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
ABA.ECOM Root CA	ABA.ECOM Root CA	7/9/2009	Secure Email, Server...	DST (ABA.ECOM) CA		
Autoridad Certificadora de la Asoc...	Autoridad Certificadora de la Asocia...	6/28/2009	Secure Email, Server...	Autoridad Certificad...		
Autoridad Certificadora del Colegi...	Autoridad Certificadora del Colegio ...	6/29/2009	Secure Email, Server...	Autoridad Certificad...		
ore EZ by DST	Baltimore EZ by DST	7/3/2009	Secure Email, Server...	DST (Baltimore EZ) CA		
com E-Trust Primary CA	Belgacom E-Trust Primary CA	1/21/2010	Secure Email, Server...	Belgacom E-Trust Pri...		
C&W HKT SecureNet CA Class A	C&W HKT SecureNet CA Class A	10/16/2009	Secure Email, Server...	CW HKT SecureNet ...		
C&W HKT SecureNet CA Class B	C&W HKT SecureNet CA Class B	10/16/2009	Secure Email, Server...	CW HKT SecureNet ...		
C&W HKT SecureNet CA Root	C&W HKT SecureNet CA Root	10/16/2010	Secure Email, Server...	CW HKT SecureNet ...		
C&W HKT SecureNet CA SGC Root	C&W HKT SecureNet CA SGC Root	10/16/2009	Secure Email, Server...	CW HKT SecureNet ...		
Certisign - Autoridade Certificador...	Certisign - Autoridade Certificadora ...	6/26/2018	Secure Email, Server...	Certisign Autoridade ...		
Certisign - Autoridade Certificador...	Certisign - Autoridade Certificadora ...	6/26/2018	Secure Email, Server...	Certisign Autoridade ...		
Certisign Autoridade Certificadora...	Certisign Autoridade Certificadora A...	6/26/2018	Secure Email, Server...	Certisign Autoridade ...		
Certisign Autoridade Certificadora...	Certisign Autoridade Certificadora A...	7/9/2018	Secure Email, Server...	Certisign Autoridade ...		
Class 1 Primary CA	Class 1 Primary CA	7/6/2020	Secure Email, Server...	CertPlus Class 1 Prim...		
Class 1 Public Primary Certification...	Class 1 Public Primary Certification A...	8/1/2028	Secure Email, Client ...	VeriSign Class 1 Publi...		
Class 1 Public Primary Certification...	Class 1 Public Primary Certification A...	1/7/2020	Secure Email, Client ...	VeriSign Class 1 Prim...		
Class 2 Primary CA	Class 2 Primary CA	7/6/2019	Secure Email, Server...	CertPlus Class 2 Prim...		
Class 2 Public Primary Certification...	Class 2 Public Primary Certification A...	1/7/2004	Secure Email, Client ...	VeriSign Class 2 Prim...		
Class 2 Public Primary Certification...	Class 2 Public Primary Certification A...	8/1/2028	Secure Email, Client ...	VeriSign Class 2 Publi...		

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



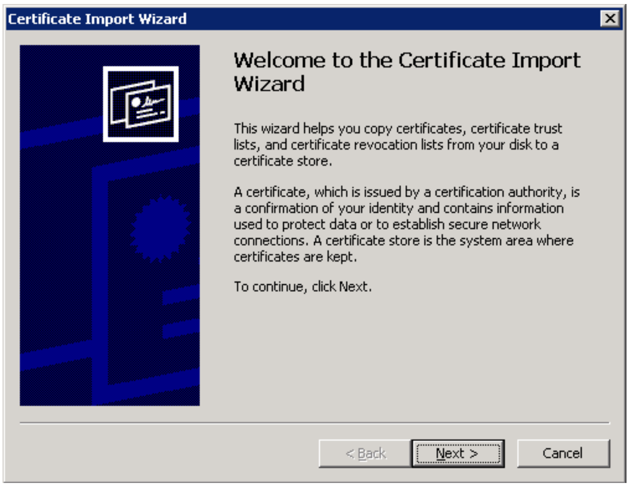
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

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



Certificate Import Wizard

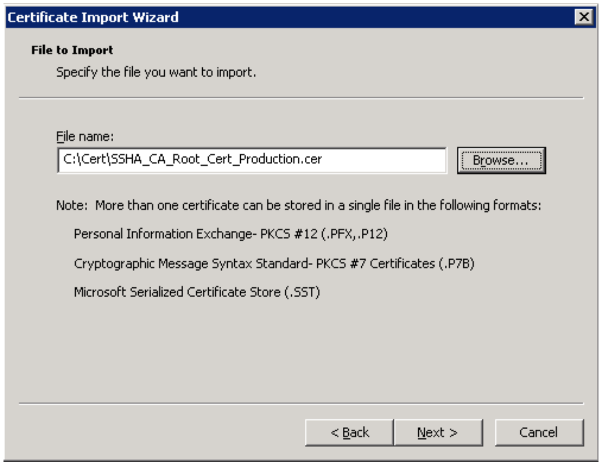
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

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



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Cert\SSHA_CA_Root_Cert_Production.cer

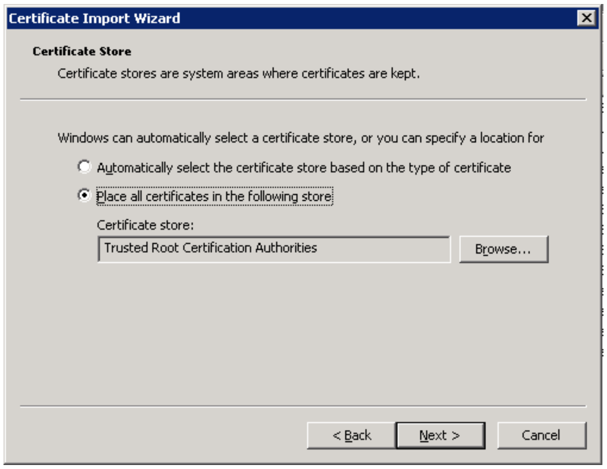
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

- 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.


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

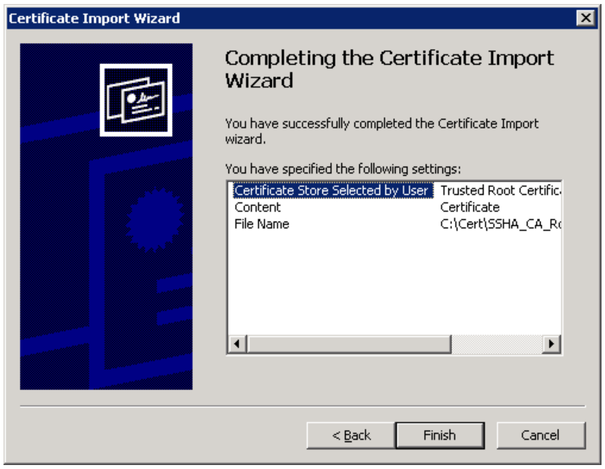
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

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


Certificate Import Wizard

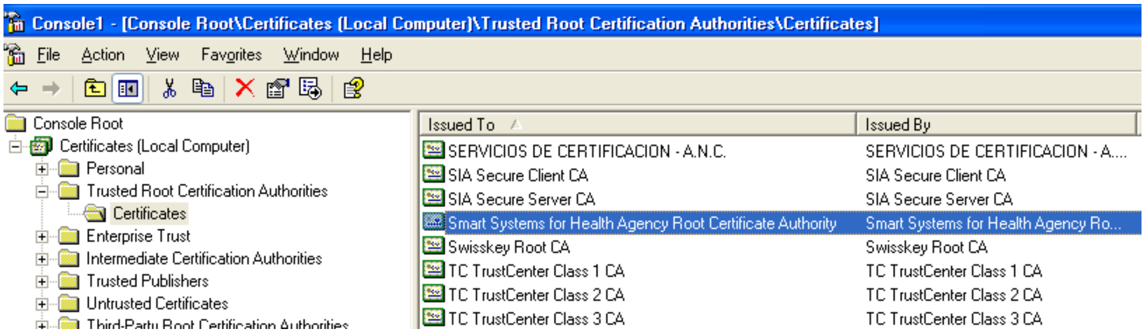
Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certific
Content	Certificate
File Name	C:\Cert\SSHA_CA_Rc

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


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities

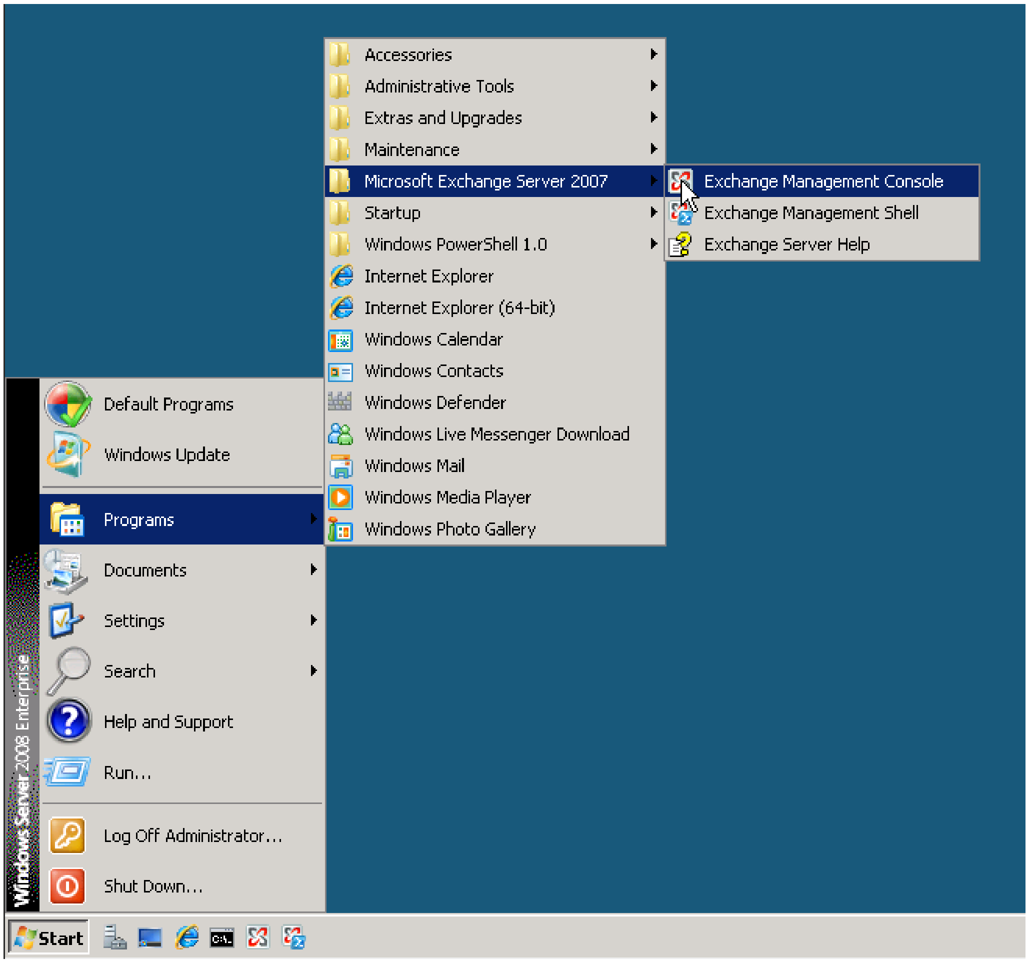
Issued To	Issued By
SERVICIOS DE CERTIFICACION - A.N.C.	SERVICIOS DE CERTIFICACION - A....
SIA Secure Client CA	SIA Secure Client CA
SIA Secure Server CA	SIA Secure Server CA
Smart Systems for Health Agency Root Certificate Authority	Smart Systems for Health Agency Ro...
Swisskey Root CA	Swisskey Root CA
TC TrustCenter Class 1 CA	TC TrustCenter Class 1 CA
TC TrustCenter Class 2 CA	TC TrustCenter Class 2 CA
TC TrustCenter Class 3 CA	TC TrustCenter Class 3 CA

- You have successfully installed the SSHA CA Root certificate.

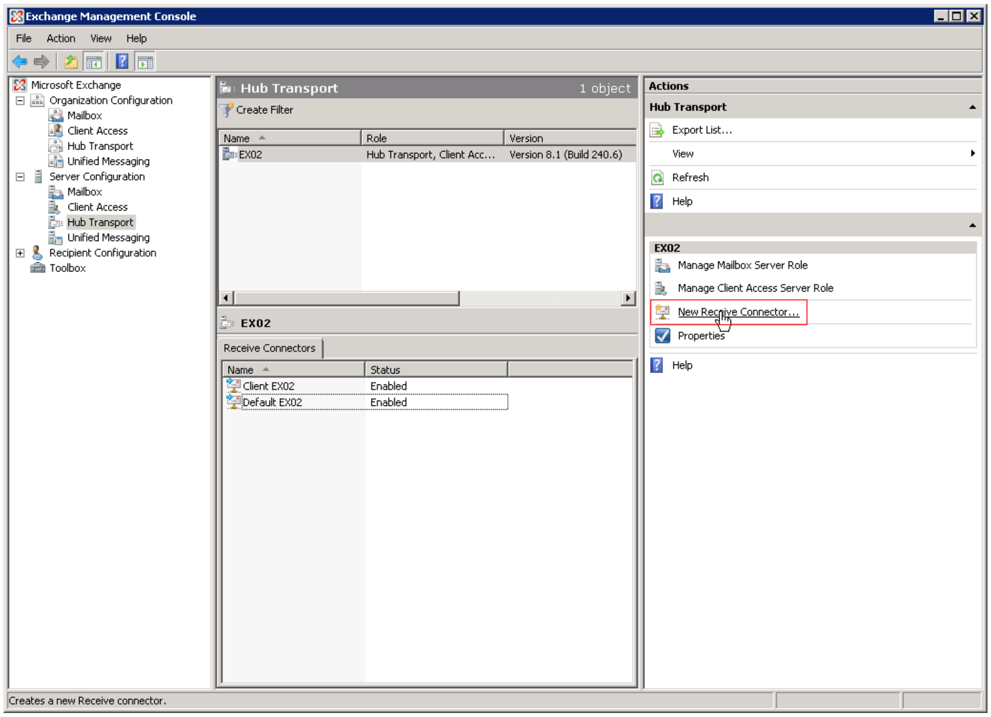
9.0 Set Up Receive Connector

To configure a Default Receive Connector for ONE Mail Partnered environment on your Exchange Server 2007, use the Exchange Management Console as explained below:

- Login to your Microsoft Exchange Server 2007 hub transport server.
- Click **Start** > **Programs** > **Microsoft Exchange Server 2007** > **Exchange Management Console**



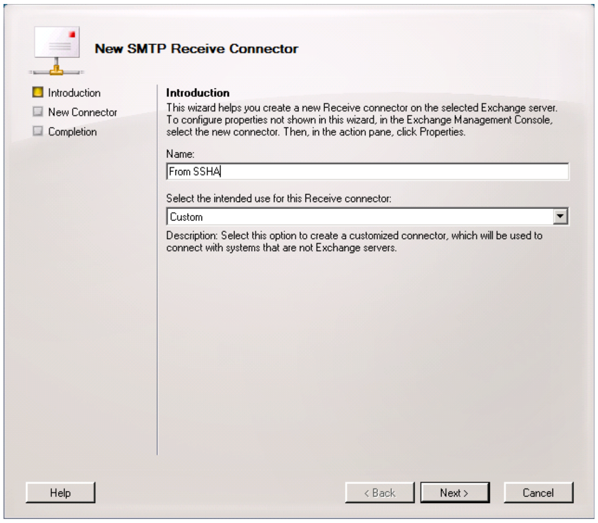
In the left tree pane expand **Server Configuration** and select **Hub Transport** container. In upper middle pane, select your hub transport server, and in left pane, select **New Receive Connector**



Name	Role	Version
EX02	Hub Transport, Client Acc...	Version 8.1 (Build 240.6)

Name	Status
Client EX02	Enabled
Default EX02	Enabled

- In **Introduction** window of wizard specify name for new connector (exp. From eHealth Ontario) and click on **Next** to proceed:



Introduction

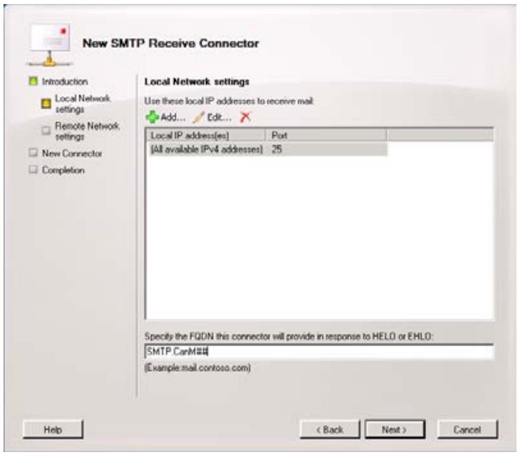
This wizard helps you create a new Receive connector on the selected Exchange server. To configure properties not shown in this wizard, in the Exchange Management Console, select the new connector. Then, in the action pane, click Properties.

Name:
From SSHA

Select the intended use for this Receive connector:
Custom

Description: Select this option to create a customized connector, which will be used to connect with systems that are not Exchange servers.

- In the **Local Network settings** window under **Specify the FQDN this connector will provide in response to HELO or EHLO:** field, specify the name which is listed in subject line of eHealth Ontario's certificate issued to your organization and click on **Next** to proceed.


New SMTP Receive Connector

Local Network settings

Use these local IP addresses to receive mail:

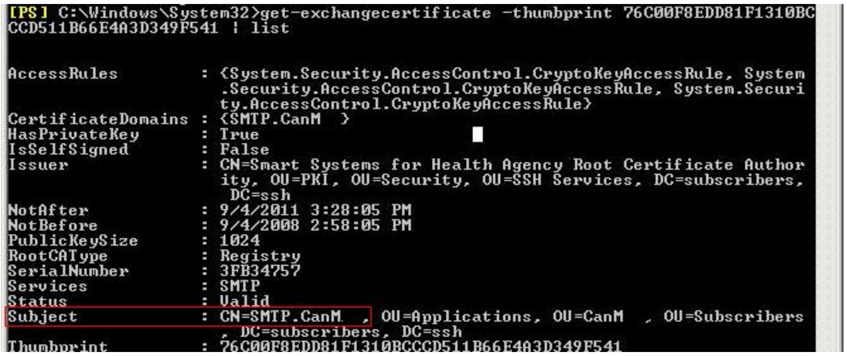
Local IP address(es)	Port
(All available IPv4 addresses)	25

Specify the FQDN this connector will provide in response to HELO or EHLO:

SMTP.CanM###

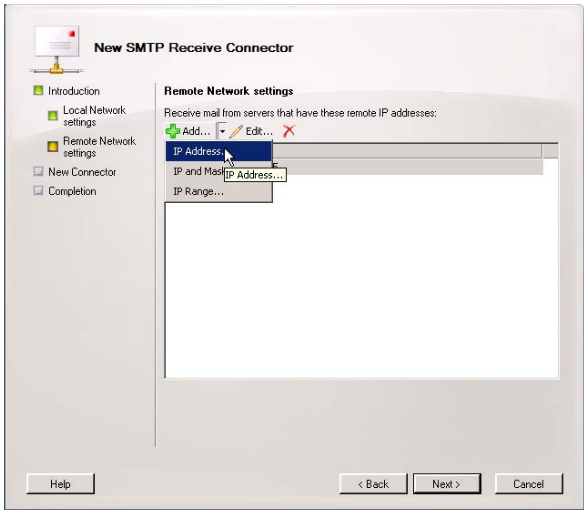
(Example:mail.contoso.com)

For example you can run **Get-ExchangeCertificate –ThumbPrint** *eHo_Certificate_ThumbPrint* **| fl** command, and in subject line find CN component of the certificate:



```
[PS] C:\Windows\System32>get-exchangecertificate -thumbprint 76C00F8EDD81F1310BC
CCD511B66E4A3D349F541 | list


AccessRules        : {System.Security.AccessControl.CryptoKeyAccessRule, System
                     .Security.AccessControl.CryptoKeyAccessRule, System.Securi
                     ty.AccessControl.CryptoKeyAccessRule}
CertificateDomains : {SMTP.CanM  }
HasPrivateKey      : True
IsSelfSigned       : False
Issuer             : CN=Smart Systems for Health Agency Root Certificate Author
                     ity, OU=PKI, OU=Security, OU=SSH Services, DC=subscribers,
                      DC=ssh
NotAfter           : 9/4/2011 3:28:05 PM
NotBefore          : 9/4/2008 2:58:05 PM
PublicKeySize      : 1024
RootCAType         : Registry
SerialNumber       : 3FB34757
Services           : SMTP
Status             : Valid
Subject            : CN=SMTP.CanM  , OU=Applications, OU=CanM  , OU=Subscribers
                     , DC=subscribers, DC=ssh
Thumbprint         : 76C00F8EDD81F1310BCCCD511B66E4A3D349F541
```

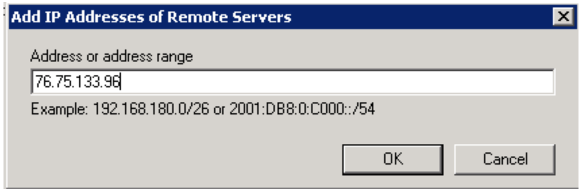
- In **Remote Network settings** window, you need to add IP address of eHealth Ontario's TLS-OUT server here by selecting down arrow button next to **+Add** and chose **IP Address...** option.


New SMTP Receive Connector

Remote Network settings

Receive mail from servers that have these remote IP addresses:

- In **Add IP Address(es) of Remote Servers** pop-up window insert IP Address of eHealth Ontario’s TLS-OUT servers and click on **OK** to exit this screen. There are 4 IPs to be added:
  - 76.75.133.96
  - 76.75.164.96
  - 76.75.149.54
  - 76.75.177.138



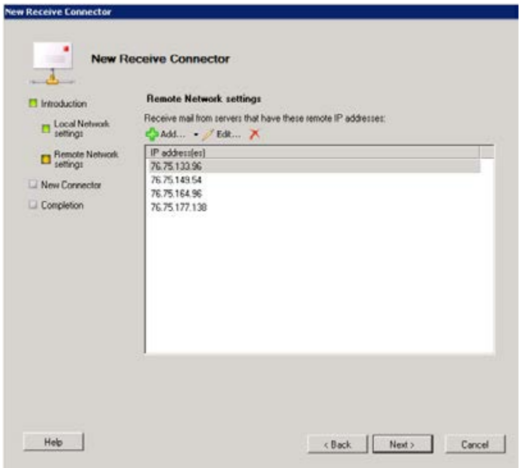
Add IP Addresses of Remote Servers

Address or address range

76.75.133.96

Example: 192.168.180.0/26 or 2001:DB8:0:C000::/54

- Remove full range of all IP v.4 addresses (0.0.0.0 – 255.255.255.255) and click on **Next** in **Remote network** window to proceed:



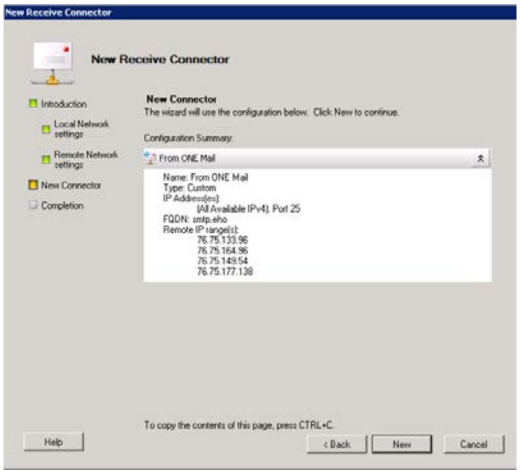
New Receive Connector

Remote Network settings

Receive mail from servers that have these remote IP addresses:

IP address(es)
76.75.133.96
76.75.149.54
76.75.164.96
76.75.177.138

- Review configuration settings in **Configuration Summary** window and click on **New** button to create connector and click on **Finish** in **Completion** window to exit:



New Receive Connector

New Connector

The wizard will use the configuration below. Click New to continue.

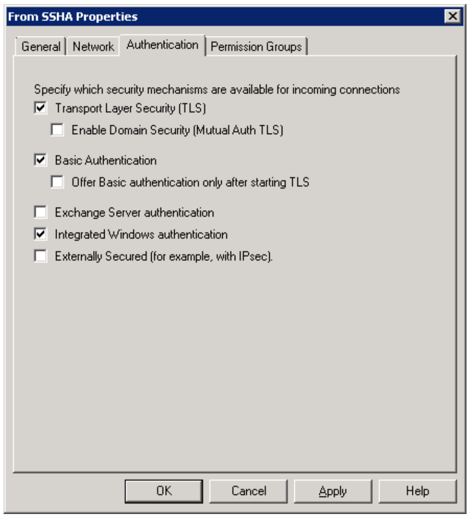
Configuration Summary:

From ONE Mail

```
Name: From ONE Mail
Type: Custom
IP Address(es):
        (All Available IPv4): Port 25
FQDN: smtp.eho
Remote IP range(s):
        76.75.133.96
        76.75.164.96
        76.75.149.54
        76.75.177.138
```

To copy the contents of this page, press CTRL+C.

- Double click on newly created connector **From eHealth Ontario** to get properties and switch to **Authentication** tab and only select the following options:
    - Transport Layer Security (TLS)
    - Basic Authentication
    - Integrated Windows authentication



Specify which security mechanisms are available for incoming connections

☑ Transport Layer Security (TLS)

☐ Enable Domain Security (Mutual Auth TLS)

☑ Basic Authentication

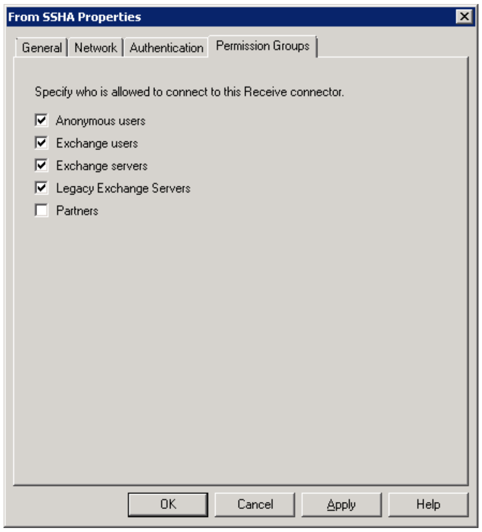
☐ Offer Basic authentication only after starting TLS

☐ Exchange Server authentication

☑ Integrated Windows authentication

☐ Externally Secured (for example, with IPsec).

- Switch to the **Permission Groups** tab and select all available permission groups except **Partners** and click on **Apply** to save changes and exit **Exchange Management Console**.



Specify who is allowed to connect to this Receive connector.

☑ Anonymous users

☑ Exchange users

☑ Exchange servers

☑ Legacy Exchange Servers

☐ Partners

- Run **Services.msc** tool and restart **Microsoft Exchange Transport** service to immediately apply all changes.

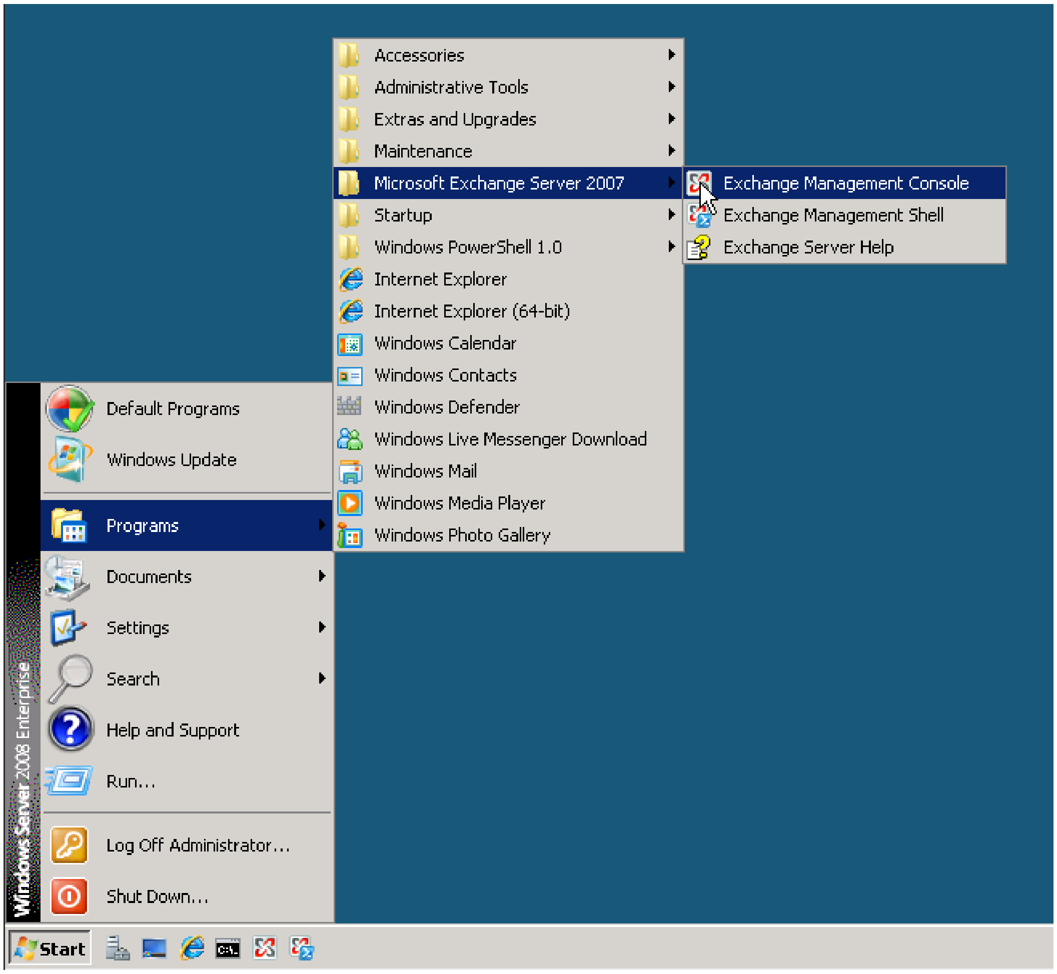
STOP: Do not complete the remainder of the configurations until the scheduled Go Live date.

10.0 Set Up Send Connector

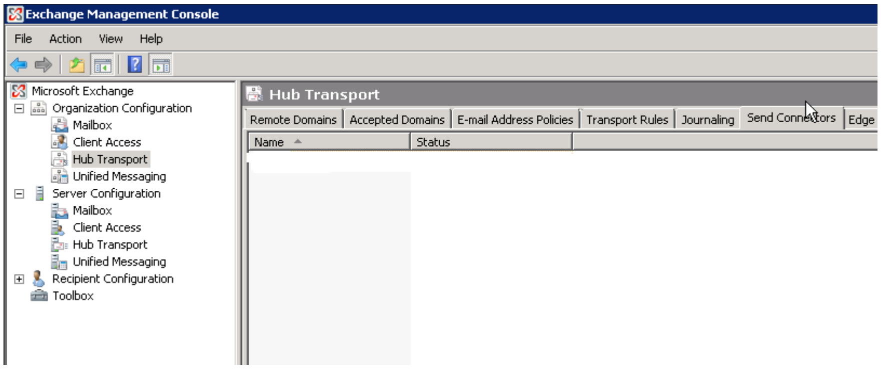
To create and configure a Send Connector for the ONE Mail Partnered environment on your Exchange Server 2007 use Exchange Management Console, as explained below:

> Note: **Note:** If you already have **Send Connector** configured on your server, please change priority of this connector to 20, by taking Properties of that Send Connector, switch to Address Space tab, edit exiting address space and change Cost value from 1 to 20. After that proceed with creation of the new Send Connector to connect to eHealth Ontario's ONE Mail Partnered program.

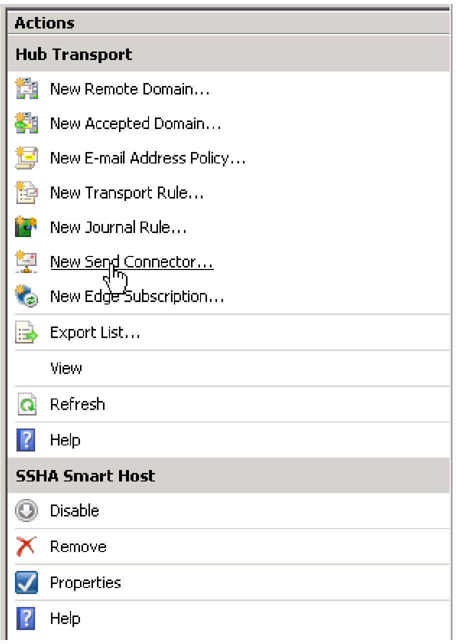
- Login to your Microsoft Exchange Server 2007 host server.
- Click **Start** > **Programs** > **Microsoft Exchange Server 2007** > **Exchange Management Console.**



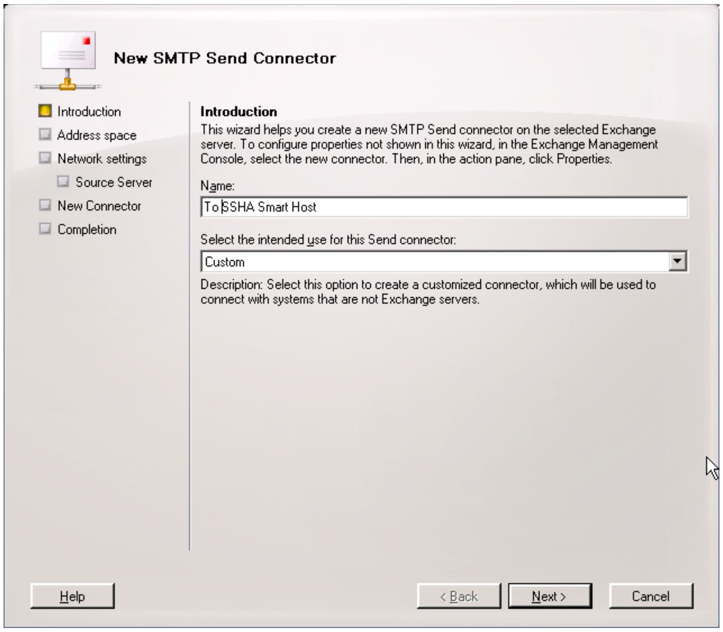
- In Exchange Management Console, in the left tree pane browse to Organization Configuration to Hub Transport container. Then select the **Send Connector** tab. If you have Send Connector configured to rout your out-bound e-mail directly to Internet, or to your previous ISP you need to delete that connector.



- To create new Send Connector, in the right action pane select **New Send Connector.**



- On the **New SMTP Send Connector** introduction screen select the name of the new connector and insert in the **Name** field (ex. To eHealth Ontario Smart Host). From the **Select the intended use for this Send connector** drop down menu select ***Custom*** and press **Next.**


New SMTP Send Connector

Introduction

This wizard helps you create a new SMTP Send connector on the selected Exchange server. To configure properties not shown in this wizard, in the Exchange Management Console, select the new connector. Then, in the action pane, click Properties.

Name:

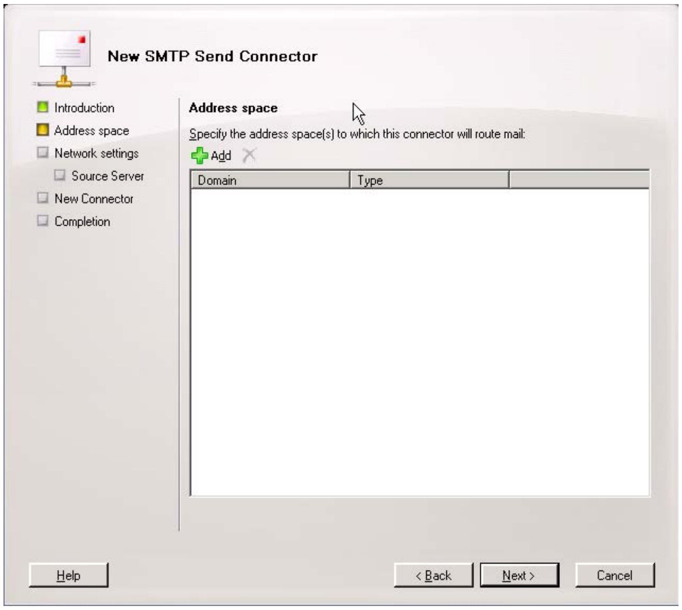
To SSHA Smart Host

Select the intended use for this Send connector:

Custom

Description: Select this option to create a customized connector, which will be used to connect with systems that are not Exchange servers.

- In the Address space screen click the **Add** button

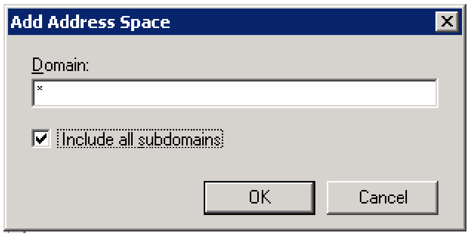


New SMTP Send Connector

Address space

Specify the address space(s) to which this connector will route mail:

- In the **Add Address Space** window type "*" in the **Domain** box and press **OK**.

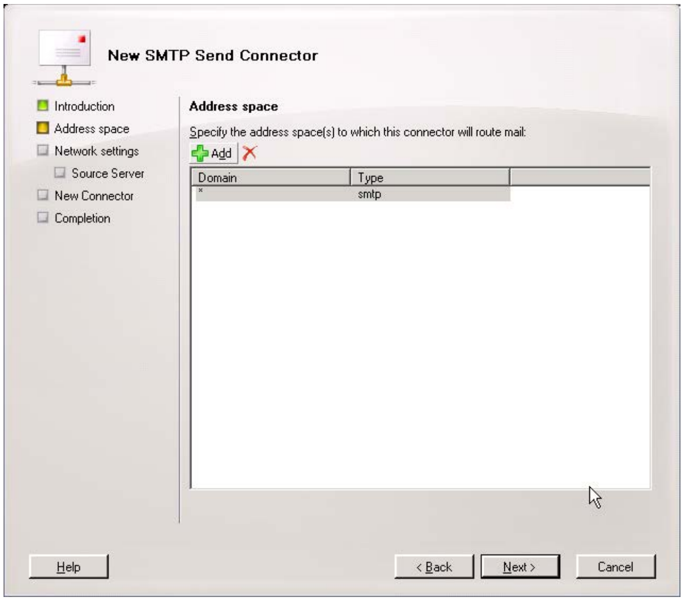


Add Address Space

Domain: *

☑ Include all subdomains

- In the **Address space** screen you will see the new address space, press **Next** to proceed:



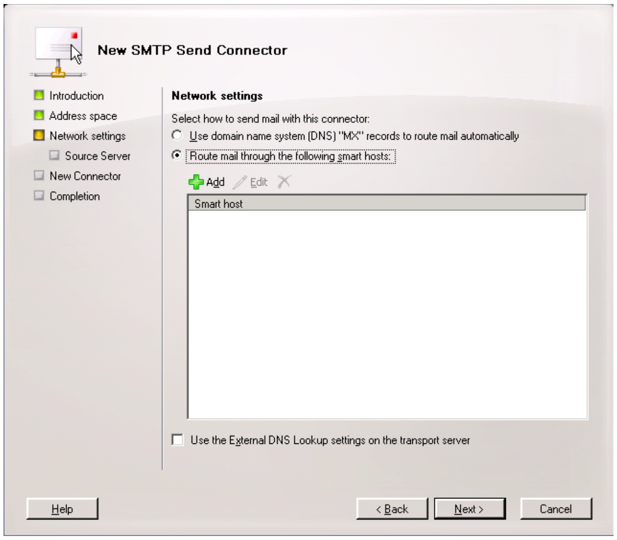
New SMTP Send Connector

Address space

Specify the address space(s) to which this connector will route mail:

Domain	Type
*	smtp

- In **Network settings** screen select option **Route mail through the following smart host:** and press the **Add** button.



New SMTP Send Connector

- Introduction
- Address space
- Network settings
  - Source Server
- New Connector
- Completion

Network settings

Select how to send mail with this connector:

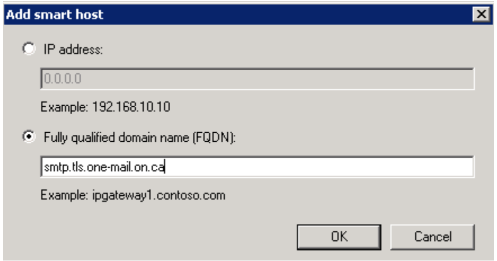
○ Use domain name system (DNS) "MX" records to route mail automatically

● Route mail through the following smart hosts:

Smart host

□ Use the External DNS Lookup settings on the transport server

- In the **Add smart host** pop up window select **Fully qualified domain name (FQDN):** and insert eHealth Ontario's TLS-IN FQDN **smtp.tls.one-mail.on.ca** and press **OK.**



Add smart host

○ IP address:

0.0.0.0

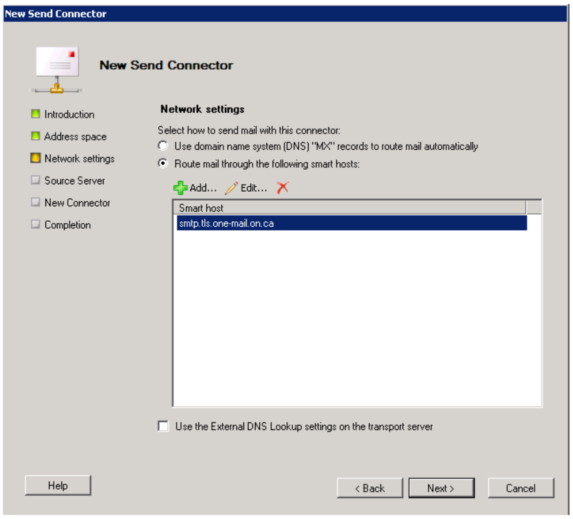
Example: 192.168.10.10

● Fully qualified domain name (FQDN):

smtp.tls.one-mail.on.ca

Example: ipgateway1.contoso.com

- Back in the **Network settings** screen, you will now see new smart host and press **Next** to proceed.



New Send Connector

Network settings

Select how to send mail with this connector:

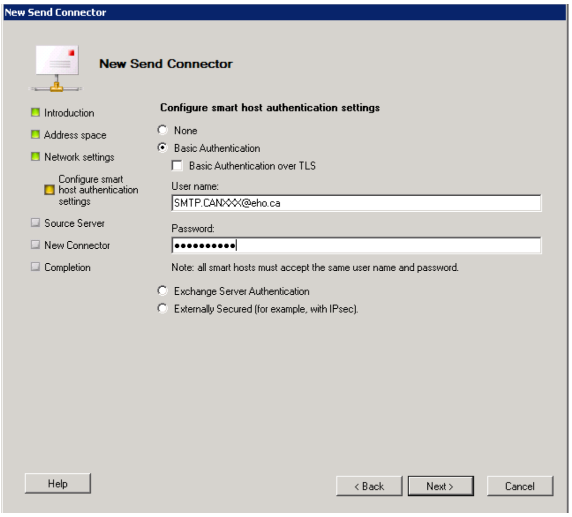
○ Use domain name system (DNS) "MX" records to route mail automatically

● Route mail through the following smart hosts:

Smart host
smtp.tls.one-mail.on.ca

□ Use the External DNS Lookup settings on the transport server

- In the **Authentication Settings** screen select only **Basic Authentication** option and insert user name and password provided by eHealth Ontario, then press **Next** to proceed.



New Send Connector

Configure smart host authentication settings

○ None

● Basic Authentication

□ Basic Authentication over TLS

User name: SMTP.CANXXX@eho.ca

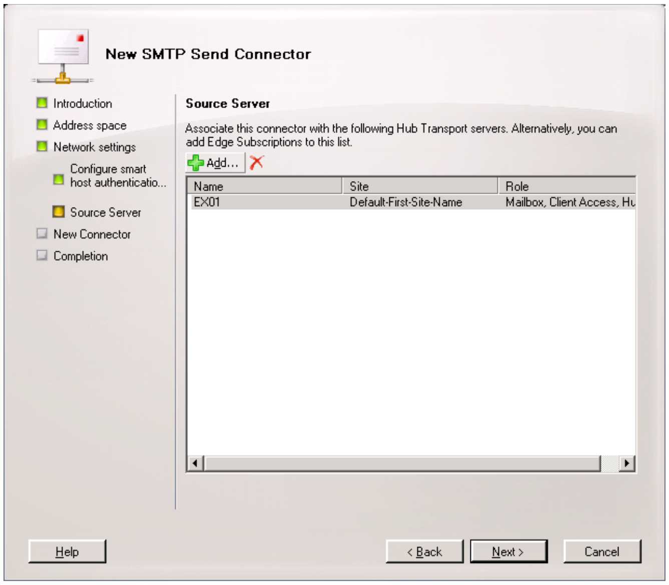
Password: ●●●●●●●●●●

Note: all smart hosts must accept the same user name and password.

○ Exchange Server Authentication

○ Externally Secured (for example, with IPsec).

- In the **Source Server** screen select only your **Hub Transport** server and press **Next** to proceed.

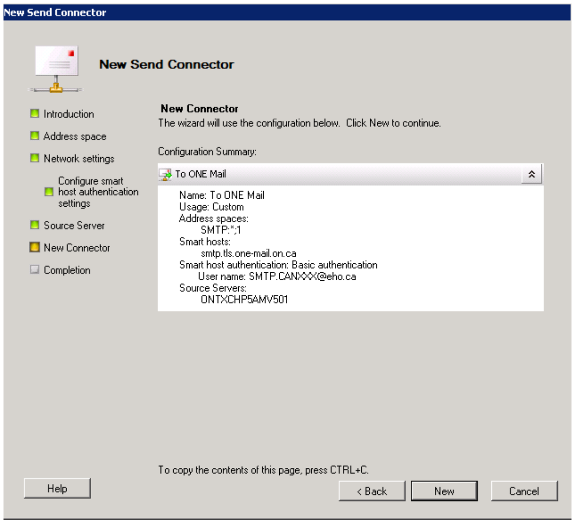


Source Server

Associate this connector with the following Hub Transport servers. Alternatively, you can add Edge Subscriptions to this list.

Name	Site	Role
EX01	Default-First-Site-Name	Mailbox, Client Access, Hu

- In the **Configuration Summary** screen review selected options and press **New** to proceed.



New Connector
The wizard will use the configuration below. Click New to continue.

Configuration Summary:

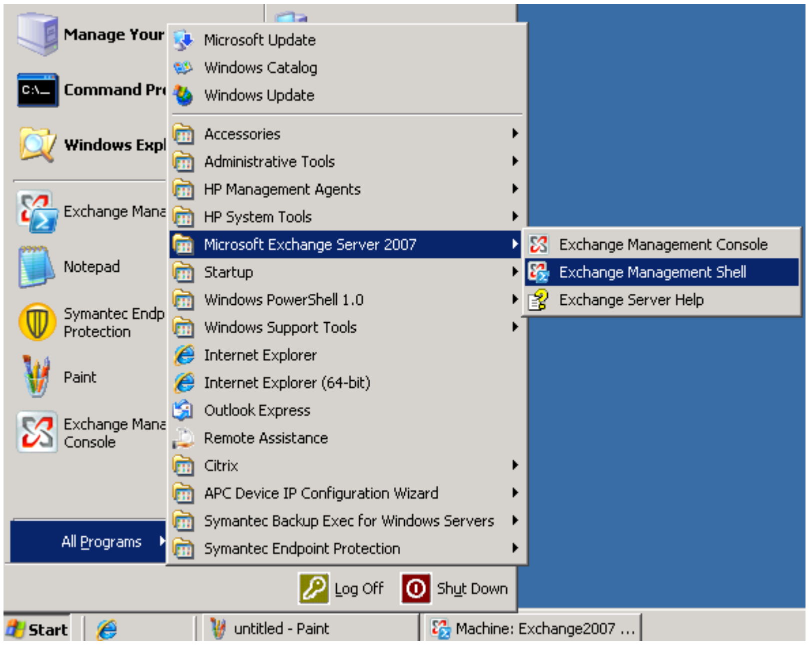
To ONE Mail

```
Name: To ONE Mail
Usage: Custom
Address spaces:
    SMTP:*;1
Smart hosts:
    smtp.tls.one-mail.on.ca
Smart host authentication: Basic authentication
   User name: SMTP.CANXXX@eho.ca
Source Servers:
    ONTXCHP5AMV501
```

To copy the contents of this page, press CTRL+C.

In the **Completion** screen press **Finish** to exit.

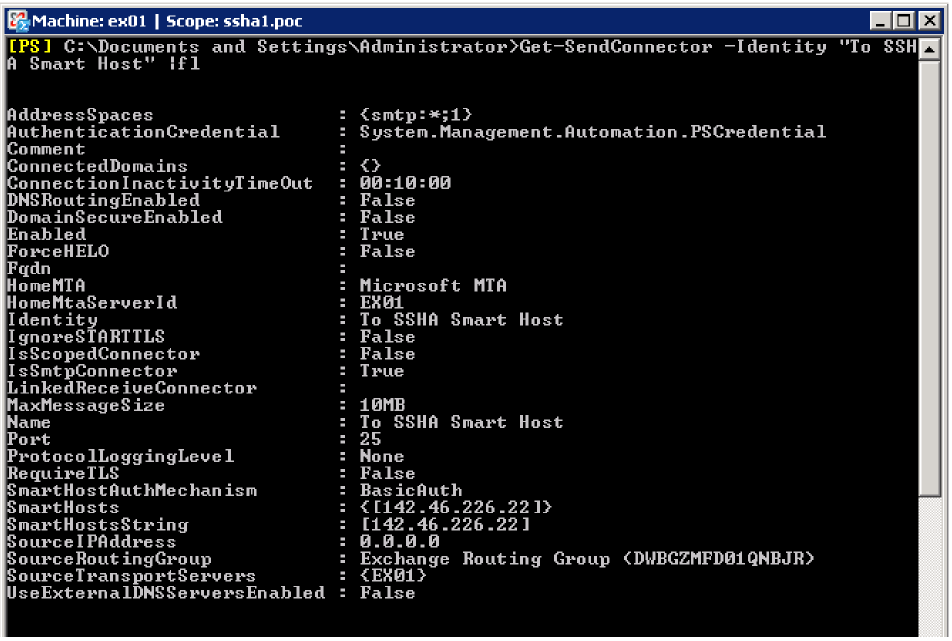
- Now open Exchange Management Shell from Start Menu.



- Then type command:

```
Get-SendConnector –Identity "Your_Send_Connector_Name" |fl
```

"*Your_Send_Connector_Name*" is the name which you specified during connection creation.



```
[PS] C:\Documents and Settings\Administrator>Get-SendConnector -Identity "To SSH
A Smart Host" |fl


AddressSpaces                : {smtp:*;1}
AuthenticationCredential     : System.Management.Automation.PSCredential
Comment                      :
ConnectedDomains             : {}
ConnectionInactivityTimeOut  : 00:10:00
DNSRoutingEnabled            : False
DomainSecureEnabled          : False
Enabled                      : True
ForceHELO                    : False
Fqdn                         :
HomeMTA                      : Microsoft MTA
HomeMtaServerId              : EX01
Identity                     : To SSHA Smart Host
IgnoreSTARTTLS               : False
IsScopedConnector            : False
IsSmtpConnector              : True
LinkedReceiveConnector       :
MaxMessageSize               : 10MB
Name                         : To SSHA Smart Host
Port                         : 25
ProtocolLoggingLevel         : None
RequireTLS                   : False
SmartHostAuthMechanism       : BasicAuth
SmartHosts                   : {[142.46.226.22]}
SmartHostsString             : [142.46.226.22]
SourceIPAddress              : 0.0.0.0
SourceRoutingGroup           : Exchange Routing Group (DWBGZMFD01QNBJR)
SourceTransportServers       : {EX01}
UseExternalDNSServersEnabled : False
```

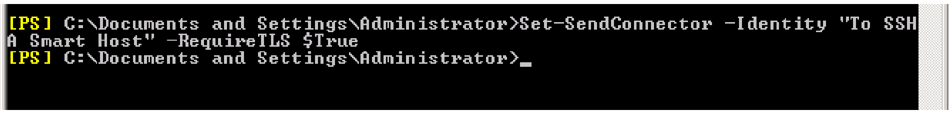
Check following fields in output:

- *IgnoreSTARTTLS* need to be *False*
- *SmartHostAuthMechanism* need to be only *BasicAuth*
- RequireTLS need to be True

Note: RequireTLS by default is **False (as you can see on previous screenshot)** and we need to change that to **True** by running following command:

```
Set-SendConnector –Identity “Your_Send_Connector_Name” –RequireTLS $True
```

Where “*Your_Send_Connector_Name*” is the name which you specified during connection creation:



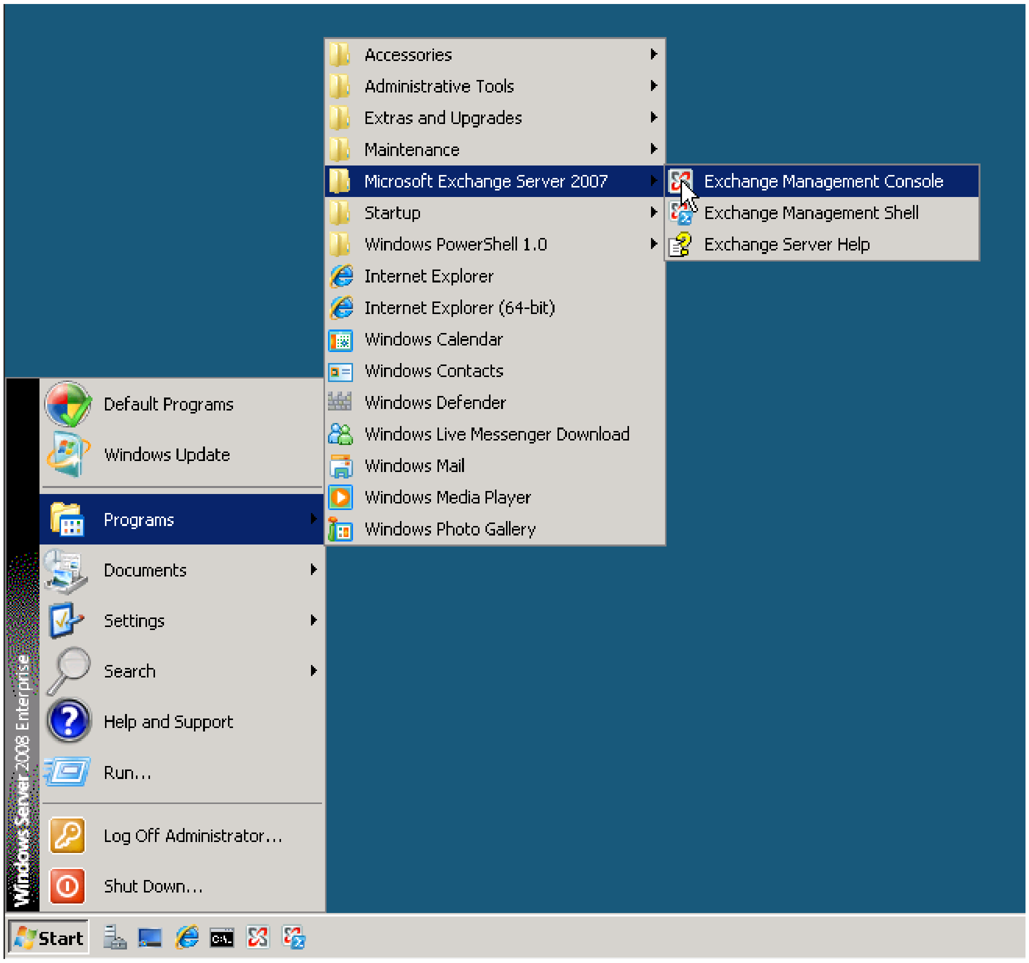
```
[PS] C:\Documents and Settings\Administrator>Set-SendConnector -Identity "To SSH
A Smart Host" -RequireTLS $True
[PS] C:\Documents and Settings\Administrator>_
```

Note: If any other two parameters are not setup as required use same command with appropriate parameters to set them.

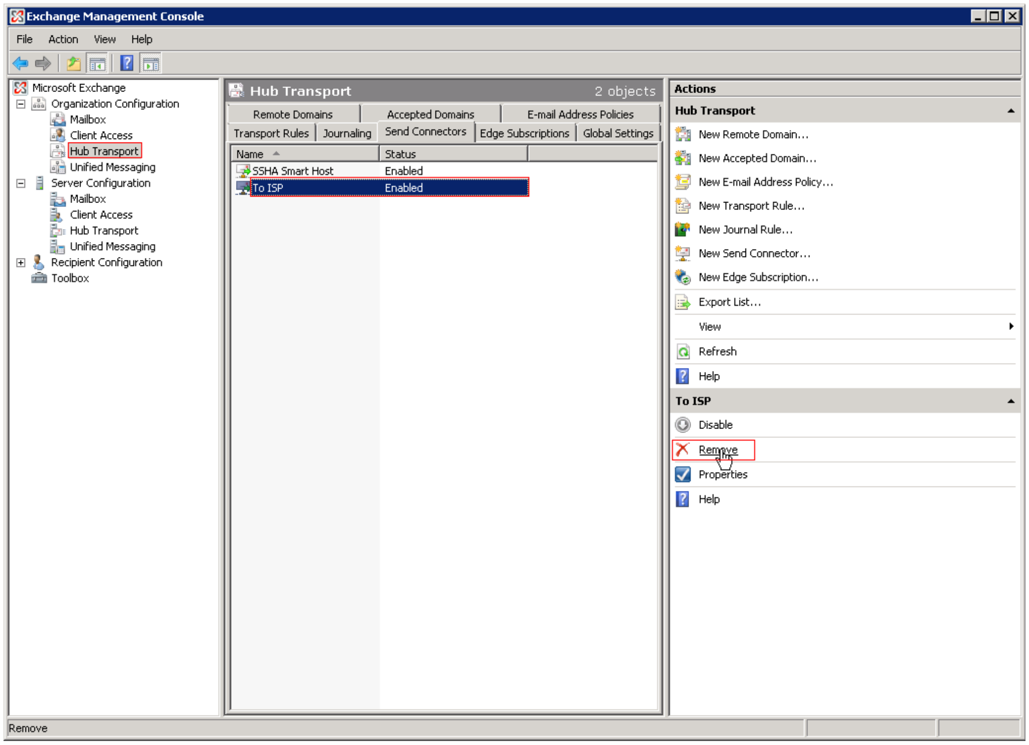
11.0 Post Configuration Changes

Once full integration with ONE Mail Partnered program is implemented and tested, and you are fully disconnected from your previous ISP service, you will need to remove all old Send and Receive Connector configurations by following these steps:

- Login to your Microsoft Exchange Server 2007 hub transport server.
- Click **Start** > **Programs** > **Microsoft Exchange Server 2007** > **Exchange Management Console**

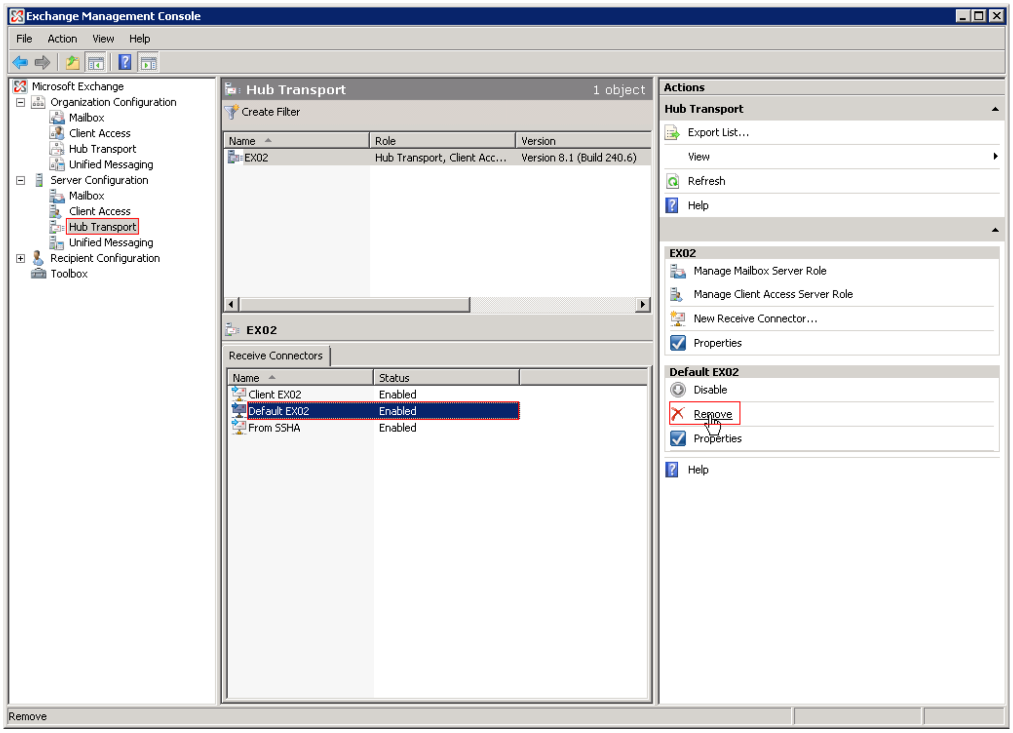


- In the left tree pane expand **Organization Configuration** and select **Hub Transport** container, in the middle pane switch to **Send Connector** tab, select old Send connector which was used to connect to ISP mail server, and in left **Action** pane select **Remove**:



Name	Status
SSHA Smart Host	Enabled
To ISP	Enabled

- In the left tree pane expand **Server Configuration** and select **Hub Transport** container, in the lower middle pane select old Receive connector which was used to receive mail from ISP mail server, and in left **Action** pane select **Remove**:



Name	Role	Version
EX02	Hub Transport, Client Acc…	Version 8.1 (Build 240.6)

Name	Status
Client EX02	Enabled
Default EX02	Enabled
From SSHA	Enabled