

***eHealth Ontario***

# ONE® Mail Partnered – Client Deployment Guide

Instructions for Microsoft Exchange  
2010 Server

Version: 1.2

Document ID: 3235

Document Owner: ONE Mail Product Team

## **Copyright Notice**

Copyright © 2014, eHealth Ontario

## **All rights reserved**

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of eHealth Ontario. The information contained in this document is proprietary to eHealth Ontario and may not be used or disclosed except as expressly authorized in writing by eHealth Ontario.

## **Trademarks**

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

## 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
0.01	2010-02	Initial draft Ognjen Andrijasevic	Ognjen Andrijasevic
1.0	2010-05	Reviewed version with changes recommended by David Thabet	Ognjen Andrijasevic
1.1	2010-05	Added Appendix A – Known Issues	Ognjen Andrijasevic
1.2	2013-05	Updated for Internet Deployments	SMI Team

## Document ID

3235

## Document Sensitivity Level

Medium

# Contents

<b>Contents</b>	<b>1</b>
<b>1.0 Introduction</b>	<b>2</b>
<b>2.0 Intended Audience</b>	<b>2</b>
<b>3.0 Overview</b>	<b>2</b>
<b>4.0 Creating CSR(s)</b>	<b>3</b>
4.1 Generating a CSR .....	4
4.2 Send the CSR to eHealth Ontario.....	6
<b>5.0 Receive the Certificates</b>	<b>7</b>
<b>6.0 Install SSHA CA Root certificate</b>	<b>8</b>
<b>7.0 Installing an Exchange Certificate</b>	<b>14</b>
<b>8.0 Verifying the Exchange certificate installation</b>	<b>16</b>
<b>9.0 Setup Receive Connector</b>	<b>18</b>
<b>10.0 Setup Send Connector</b>	<b>23</b>
<b>11.0 Post Configuration Changes</b>	<b>32</b>
<b>12.0 Appendix A - Known Issues</b>	<b>34</b>

# 1.0 Introduction

This document describes the steps required to connect Microsoft Exchange Server 2010 to ONE Mail Partnered product for secure e-mail routing:

- Generate a request for a PKI certificate
- Install SSHA CA Root certificate
- Install the created 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 2010 installed on Windows Server 2008 R2.

---

**NOTE:** There is possibility to simplify process of migration from previous versions, if you have our certificate installed on your old server, and that certificate is exportable. In that case, you can export that certificate, and install it to new server, and skip steps related to generating new request and installing new certificate.

It is important to understand that we generated certificate for your organization, not for your server. Single certificate can be installed on multiple servers in your organization.

---

## 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 SSHA CA Trusted Root certificate**
7. **Install the certificate.** This should be done on the same machine where the CSR was created.
8. **Enable only this certificate for SMTP service.**
9. **Setup Send Connector on Exchange Server 2010**
10. **Setup Default Receive Connector on Exchange Server 2010**

## 4.0 Creating CSR(s)

---

**Note:** Even in MS Exchange Server 2010 you will find GUI for Certificate Management, few important features are not possible to be configured in GUI and that is a reason why instructions are still provided for MS Exchange Shell.

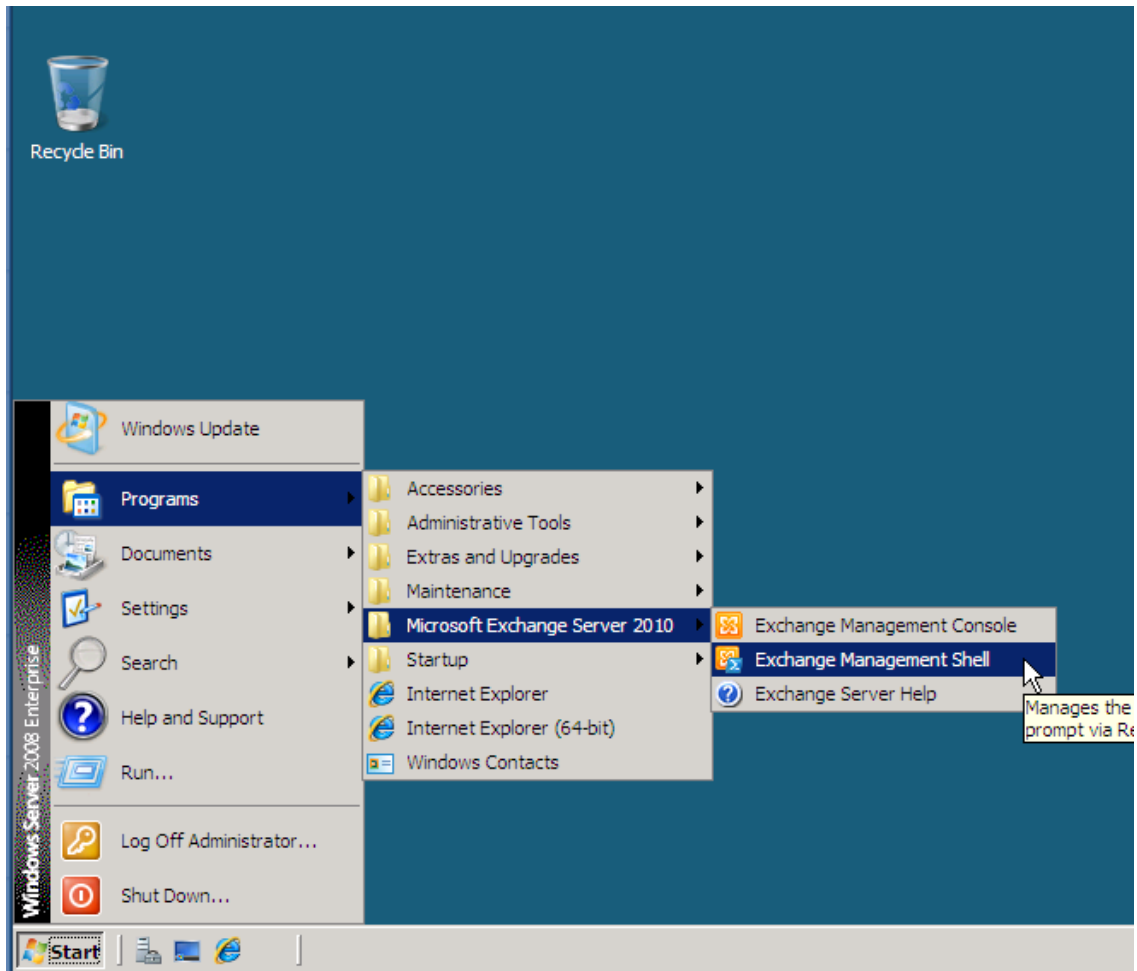
**Note:** For each request to be generated you require the corresponding Reference Number (example: 8934282) for this identity. These are obtained from the eHealth Ontario Deployment Team. A unique Reference Number is required for each certificate that is to be created.

---

## 4.1 Generating a CSR

To generate a CSR for Microsoft Exchange 2010 use Exchange Management Shell, as explained below:

- Login to your Microsoft Exchange 2010 gateway server
- Click **Start > Programs > Microsoft Exchange Server 2010 > Exchange Management Shell**



- The shell windows will be displayed

```
Machine: EXCH2K10.mpn2k10.poc

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 #51:

Want to know which mailboxes a specific Active Directory user has permissions to? Type:

$Mailboxes = Get-Mailbox -ResultSize Unlimited
$Mailboxes | Get-MailboxPermission -User <Active Directory User> ! Format-Table Identity, AccessRights, Deny

Caution: This command enumerates all the mailboxes in your organization. If you have lots of mailboxes, you may want to
target specific mailboxes.

VERBOSE: Connecting to EXCH2K10.mpn2k10.poc
VERBOSE: Connected to EXCH2K10.mpn2k10.poc.
[PS] C:\Windows\system32>
```

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

**New-ExchangeCertificate -GenerateRequest -PrivateKeyExportable \$true -KeySize 1024 -SubjectName "C=CA,S=ON, O=<Your\_Organization\_Name>,CN=<Reference Number>" -DomainName <YourPrimarySMTPDomainName> | Out-File "C:\Cert\CSR.txt"**

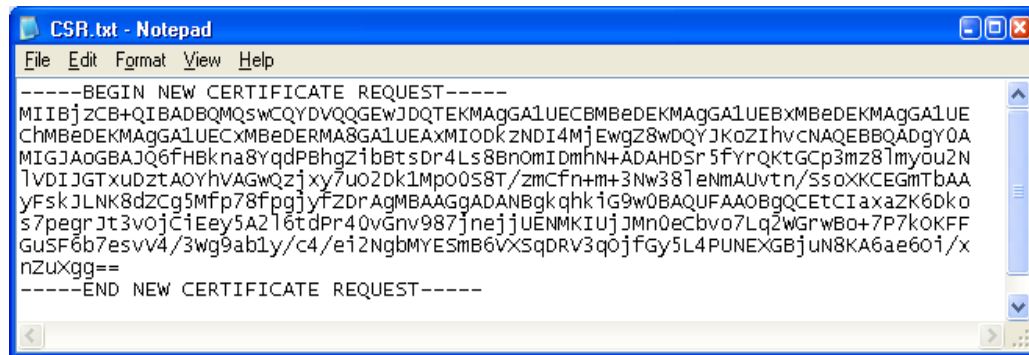
```
Machine: EXCH2K10.mpn2k10.poc

[PS] C:\Windows\system32>New-ExchangeCertificate -GenerateRequest -PrivateKeyExportable $True -KeySize 1024 -SubjectName
"C=CA,S=ON,O=eHealth Ontario ONE Mail Dev Lab,CN=123456" -DomainName eHoDevLab.on.ca ! Out-File "C:\Cert\CSR.txt"
[PS] C:\Windows\system32>
```

**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, eHealth Ontario Certificate Authority **does not support** alternative subject name certificate property. As a result, the value provided for this field will be ignored by eHealth Ontario 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 | **Out-File** parameter. The file should have a similar content:





```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBjZCB+QIBADBQMqSwCQYDVQQGEWJDQTEKMAgGA1UECBMBedeKMAgGA1UEBxMBedeKMAgGA1UE
ChMBedeKMAgGA1UECxMBedeKMAgGA1UEAxMIODkZNDI4MjEwZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBA3Q6fHBkna8YqdPBhgZ1bBtsDr4Ls8BnomIDmhn+ADAHDSr5fYrQktGCP3mz8lmyou2N
lVDIJGTxuDtAOYhVAGwQzjxy7uo2Dk1Mpo0S8T/zmCfn+m+3Nw381eNmAUvtN/SsoXKCEgmTBAA
yFskJLNK8dZCg5Mfp78fpgjyFZDrAgMBAAGgADANBgkqhkiG9w0BAQUFAAOBgQCETCiaxazK6Dko
s7pegrJt3voJCiEey5A216tdPr40vGnv987jnejjUENMKIUj3Mn0eCbvo7Lq2wGrwBo+7P7kOKFF
GusF6b7esvv4/3wg9ab1y/c4/e12NgbMYESmB6vXsqDRV3q0jfGy5L4PUNEXGBjUN8KA6ae60i/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 SSHA 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
MTCCBRmgAwIBAQIEQA9vUDANBgkqhkiG9w0BAQUFADCBpjETMBEGCgmSJomT8ixk
ARkWA3NzaDEbMBkGCgmSJomT8ixkARkWC1N1YnNjcml1ZXJzMRUwEYDVQQLEWxT
U0ggU2Vydm1jZXMxETAPBgNVBAsTCFNF1Y3VyaXR5MQwwCgYDVQQLEWwNQS0kxOjA4
BgNVBAMTMVNTYXJ0IFNF5c3RlYXNzY2VyaXR5MQwwCgYDVQQAQCBZ2V3Y3kgUm9vdCB
DQSA1IFRlc3RpbmcsHhcnMDYwMjE3MDExNDQxWmcNMdkwMjE3MDExNDQxWjCBkzETMBEG
CgmSJomT8ixkARkWA3NzaDEbMBkGCgmSJomT8ixkARkWC3N1YnNjcml1ZXJzMRQw
EgYDVQQLEWwTdWJzY3JpYmVyc2ESMBAGAlUECxmJSG9zcG10YWxzMQ8wDQYDVQQLE
WwZPTFNUU1QxFTATBgNVBAsTDEFWcGxpY2F0aW9uc2ENMAsGAlUEAxMESE1TNjCB
nZANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAwmVaRaRrPLO+ZY44H2ZIX1s6jpa3
H24UDEOKYfaZ1gZesltzYDphXOMP/7ZnP350TnbiZQqpNfLqqcFQWskJSC83PEU
xMa5jjU1xTfddpGwtnYrvT+m10q3x+KGQ4y7DDtD4KSAXWkKIKndiYH9mvpq+q4X
aqHqmFN/DZw/kTECAwEAaOAcAvowggL2MASGAlUdDwQEAWIHgDarBgNVHRAEJDAi
gA8yMDA2MDI1XNzAxMDQ0MVqBDzIwMDgwMzI1MDUzNDQxWjCBxQYIKwYBBQUHAQE
EgBgwgbUwgbIGCCsGAQFUBBZACHoG1bGRhcDovL3NzaHBraTJhMDAwMXUuc3Vic2Ny
aW9wMzNoL2NuPVNTYXJ0IFNF5c3RlYXNzY2VyaXR5MQwwCgYDVQQAQCBZ2V3Y3kgUm9v
dCBDDQSA1IFRlc3RpbmcsIG91PVBLSWsgb3U9U2VjdXJpdHksIG91PVNTSCBTZXJ2
aWN1cywgZGM9U3Vic2NyaWJlcnMsIGRjPjNzad9jQU1N1cnRpZmljYXR1MIIBiGYD
VR0FBIIBgTCCAX0wgcGgg6gggbgwgUxEzARBGoJkiaJk/IsZAEZFgNzc2gx
GzAZBg9oJkiaJk/IsZAEZFgtTdWJzY3JpYmVyc2ESMBAGAlUECxmMU1N1IFN1cnRp
Y2VzMRewDwYDVQQLEWhTZW51cm10eTEMAAOGAlUECxmDUETJMTowOAYDVQQDEZFT
bWYyY2V3Y3kgUm9vdCBDDQSA1IFRlc3RpbmcsIG91PVBLSWsgb3U9U2VjdXJpdHks
IG91PVNTSCBTZXJ2aWN1cywgZGM9U3Vic2NyaWJlcnMsIGRjPjNzad9jQU1N1cnRp
ZmljYXR1UmV2b2NhdG1vbKxpC3QwHwYDVR0jBBBgwFoAU0dJQCKRd/Fk7eTuqfcpZKT5
GWRRowHQYDVR00BAYwDgtLS1NyMiADLtzKp/vfrPTThIQVMAKGA1UdEwQCAAwGQYJKo
ZIhvcNAQEBBQADggEBAB45Jjvk7Neok02/iy+hX142NV7wRR1lBmcJKLxYE3YgrGw7C7kBRjBEZbjoQy8g1Mniop8mlkA6tiJreuF2
kAxEl1lGu1DK5tqrA+1W7S3b7G5XipgC7jF8iQ9zUhb1TsflfLkZ0r/exPX3LE/P
RyEqiUBATxfC/tuwcPm4kjrGipNis+uEJAgkoOr73AlU2SL1Gf1Q+EHsyTQ2qRI/
1IDTnEACHXbgEhU4qG8p+cN2GDcN8HJUqVLGLH6G0zfp1+6rZVeHfapUqgf+hWmtX
LCjcOCVZeaS6Gpz1lbBlhRLae6glPUNQUqfX0P8dxCitvY20w0mePuikS1dFsAMZ
MGYxAA==
-----END CERTIFICATE-----

```

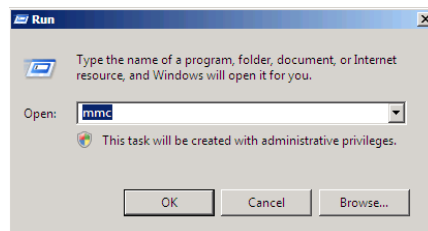
Proceed to the next section to install the certificate generated from the CSR.

## 6.0 Install SSHA CA Root certificate

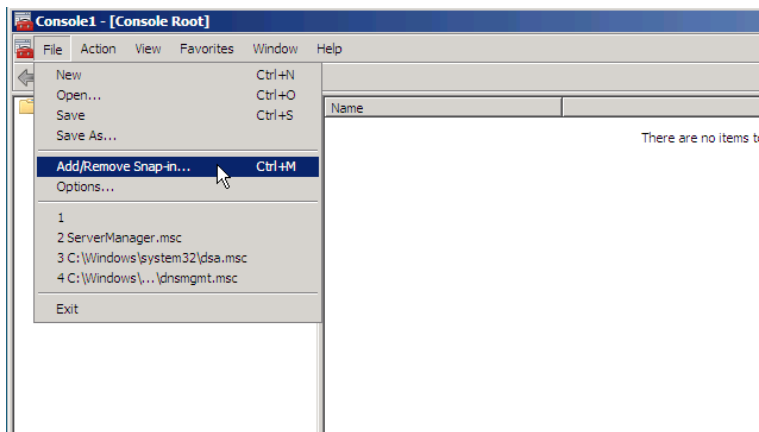
**Note:** You must also install the SSHA Root Certificate; this is not the certificate which you installed earlier in Personal Certificates storage for local computer. If you are missing this certificate in your installation package please contact eHealth Ontario and they will provide this to you.

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

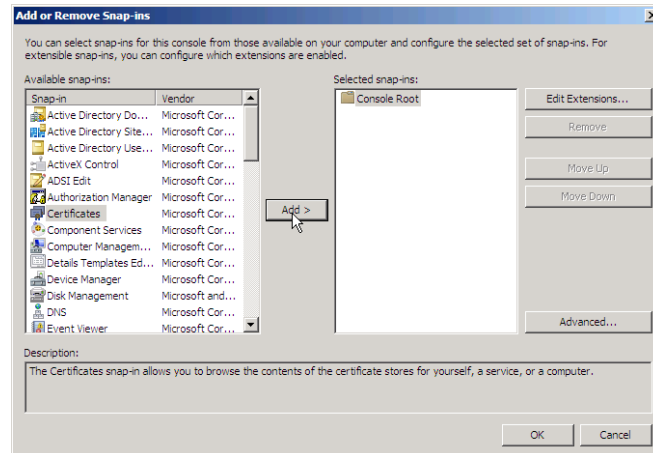
- From the **Start** menu, select **Run**. In the Run dialog box, type **mmc** and click **OK**.



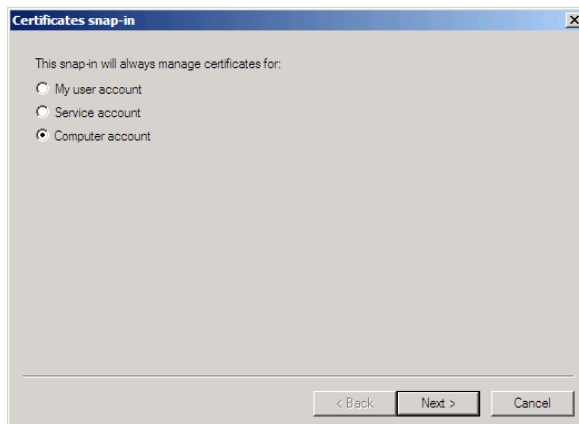
- The Microsoft Management Console is displayed. From the **File** menu, select **Add/Remove Snap-in**.



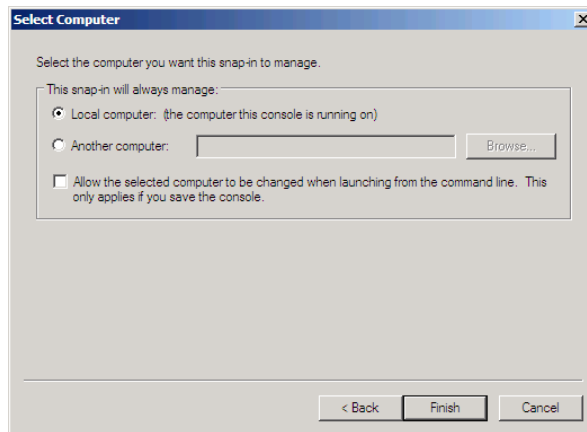
- On the Standalone tab, click **Add**. From the Available Standalone Snap-in list box, select "**Certificates**", and then click **Add**.



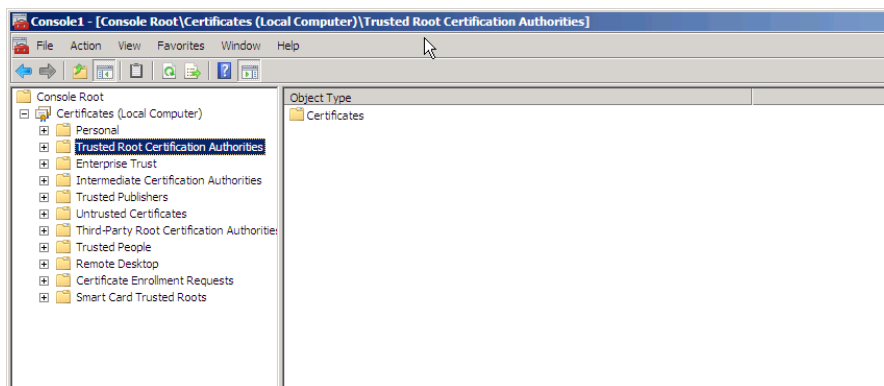
- In **Certificates snap-in** pop-up window select **Computer account** and press **Next**.



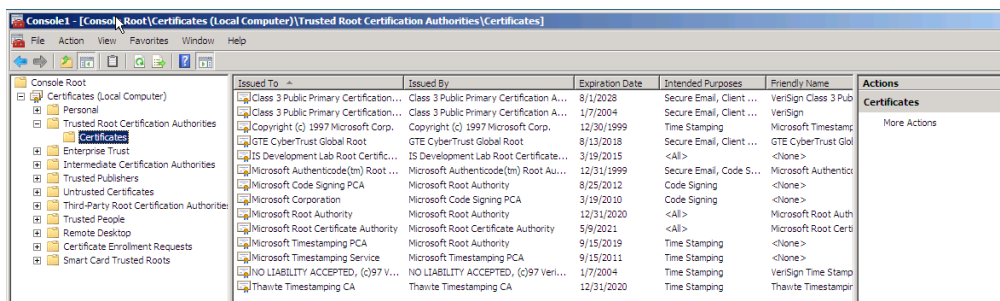
- In **Select Computer** pop-up window select **Local Computer** option and click on **Finish** button.



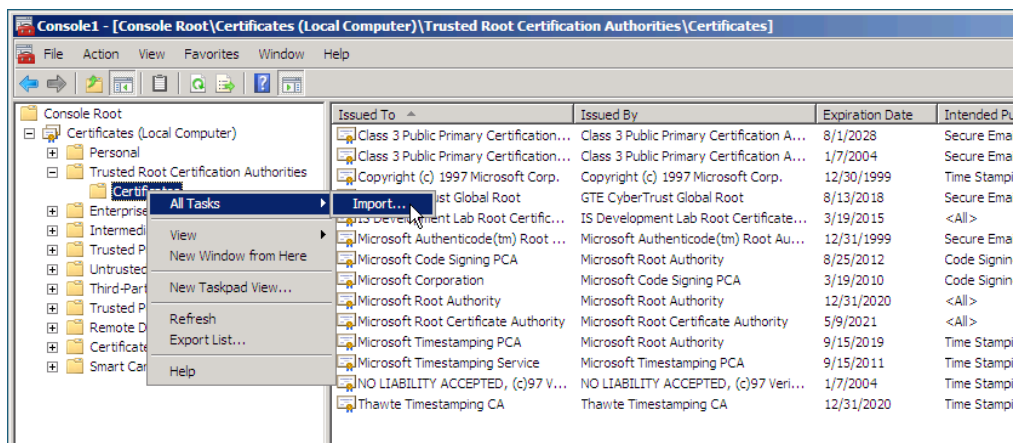
- In Stand Alone snap-in window press **Close** button and in Add/Remove window click on **OK** to exit.
- In Microsoft Management Console (**MMC**), expend the **Certificates** snap-in.



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



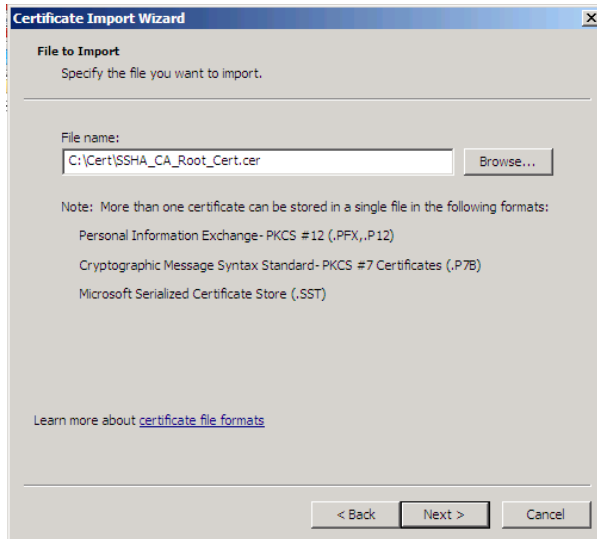
- Right click on it and select **All Task -> Import**



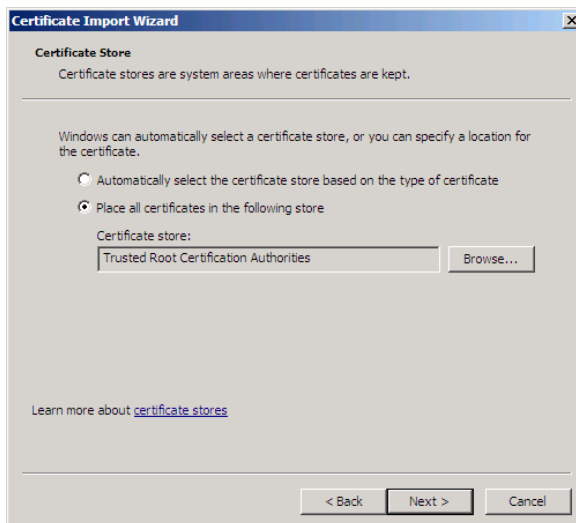
- Browse to the **SSHA CA Root certificate** received from eHealth Ontario and click **Next**



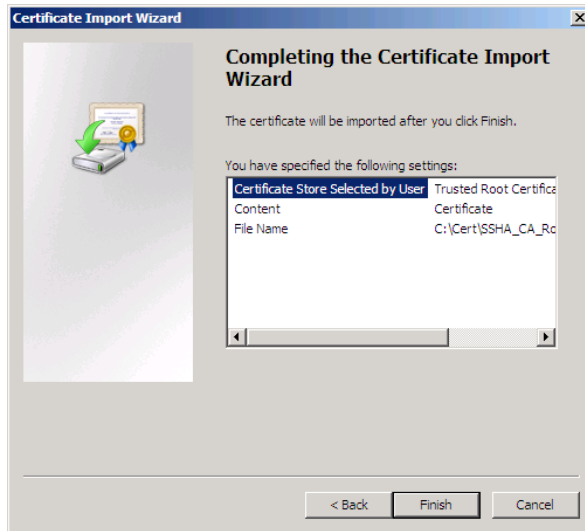
In the **File to Import** screen click on **Browse** button, select SSHA CA Root Certificate which you received from SSHA and click on **Next** to proceed.



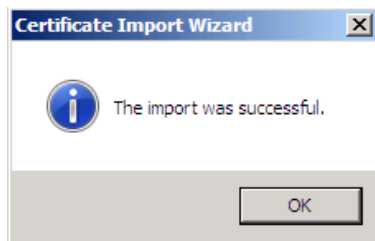
- In **Certificate Store** screen verify that **Place all certificates in the following store** and **Trusted Root Certification Authorities** options are selected and click on **Next** to proceed.



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



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



- You have successfully installed the SSHA CA Root certificate.

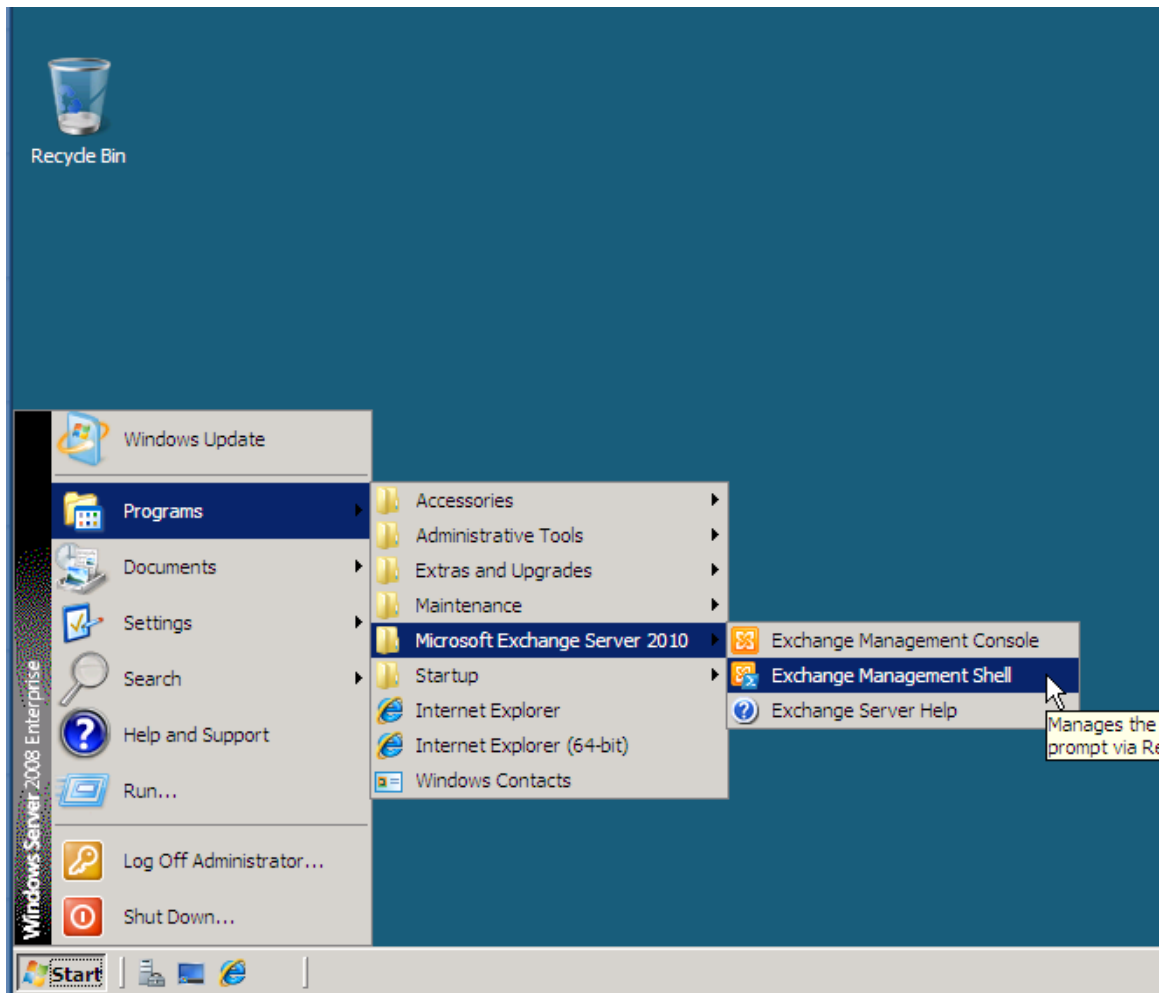




## 7.0 Installing an Exchange Certificate

To install the certificate received from eHealth Ontario for Microsoft Exchange 2010 use the Exchange Management Shell, as explained below:

- Login to your Microsoft Exchange 2010 host server
- Click **Start > Programs > Microsoft Exchange Server 2010 > Exchange Management Shell**



- The shell windows will be displayed

```
Machine: EXCH2K10.mpn2k10.poc

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 #51:

Want to know which mailboxes a specific Active Directory user has permissions to? Type:

$Mailboxes = Get-Mailbox -ResultSize Unlimited
$Mailboxes | Get-MailboxPermission -User <Active Directory User> ! Format-Table Identity, AccessRights, Deny

Caution: This command enumerates all the mailboxes in your organization. If you have lots of mailboxes, you may want to
target specific mailboxes.

VERBOSE: Connecting to EXCH2K10.mpn2k10.poc
VERBOSE: Connected to EXCH2K10.mpn2k10.poc.
[PS] C:\Windows\system32>
```

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

**Import-ExchangeCertificate -FileData ([Byte[]]\$(Get-Content -Path c:\Cert\<SSHACertFileName> -Encoding byte -ReadCount 0))**

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

```
Machine: EXCH2K10.mpn2k10.poc

[PS] C:\Windows\system32>Import-ExchangeCertificate -FileData ([Byte[]]$(Get-Content -Path c:\cert\CertMPN2K10.cer -Encoding byte -ReadCount 0))

Thumbprint                               Services    Subject
-----
083037E05E9A8CC344E40511CAG04DCDC8697545 .....      CN=mpn2k10.poc, OU=IS_Dev_Lab, O=E2k10, L=Toronto, S=ON, C=Ca

[PS] C:\Windows\system32>
```

---

**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.

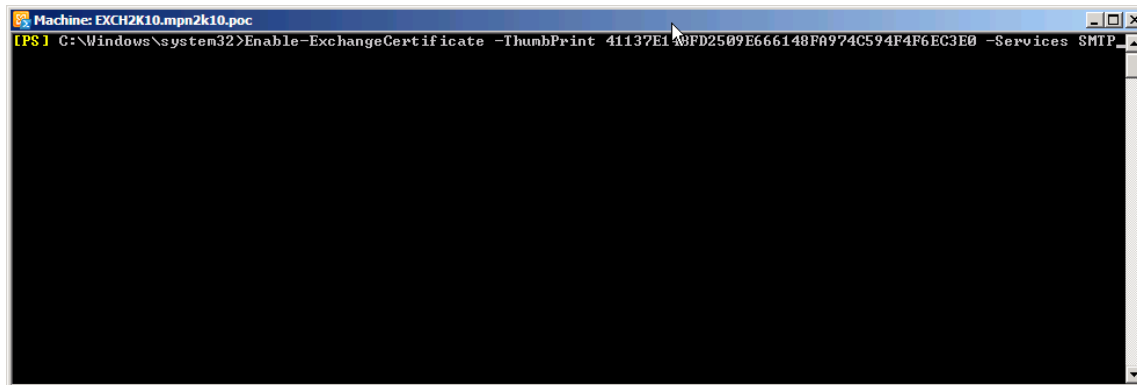
---

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

**Enable-ExchangeCertificate -Thumbprint <eHo\_Certificate\_ThumbPrint> -Services SMTP**

Where *eHo\_Certificate\_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:

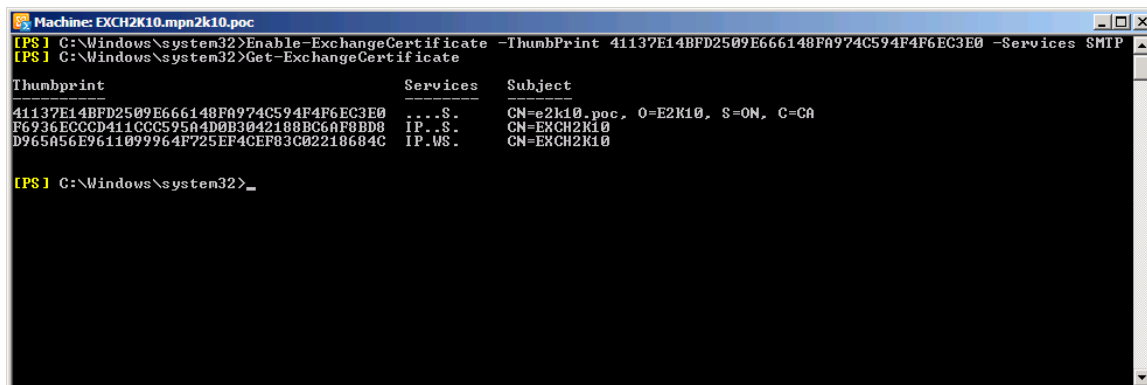


```
Machine: EXCH2K10.mpn2k10.poc
[PS] C:\Windows\system32>Enable-ExchangeCertificate -ThumbPrint 41137E14BFD2509E666148FA974C594F4F6EC3E0 -Services SMTP
```

**NOTE:** If you find that installed certificate is not associated with encryption keys please follow the steps from Appendix A to correct this problem.

## 8.0 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).



```
Machine: EXCH2K10.mpn2k10.poc
[PS] C:\Windows\system32>Enable-ExchangeCertificate -ThumbPrint 41137E14BFD2509E666148FA974C594F4F6EC3E0 -Services SMTP
[PS] C:\Windows\system32>Get-ExchangeCertificate

Thumbprint                               Services  Subject
-----
41137E14BFD2509E666148FA974C594F4F6EC3E0 ...S.    CN=e2k10.poc, O=E2K10, S=ON, C=CA
F6736ECCCD411CC595A4D0B3042188BC5AF8BD8 IP..S.    CN=EXCH2K10
D965A56E96110997964F725EF4CEF83C02210604C IP.WS.    CN=EXCH2K10

[PS] C:\Windows\system32>
```

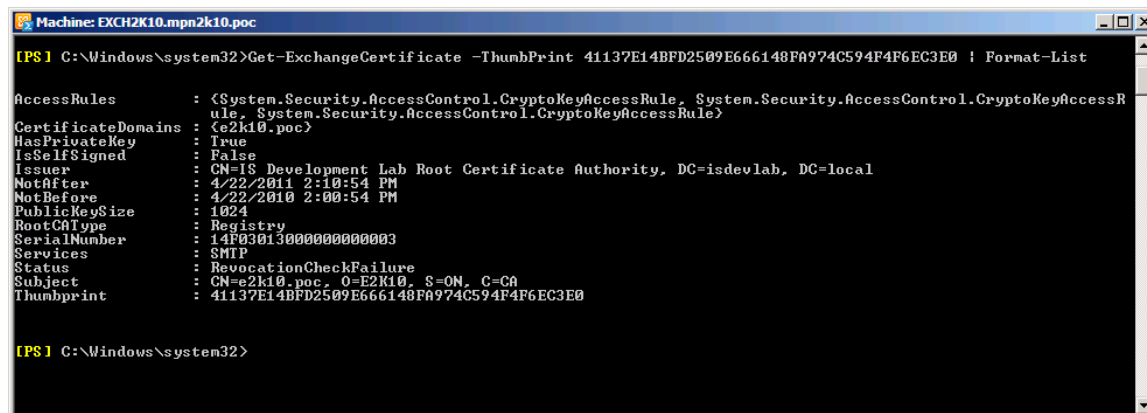
**Note:** **Important:** If you have multiple certificates in this output, please follow this procedure to verify that only the right certificate is enabled to be used by SMTP service.

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

## Get-ExchangeCertificate –Thumbprint *eHo\_Certificate\_ThumbPrint* /Format-List

Where *eHo\_Certificate\_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:



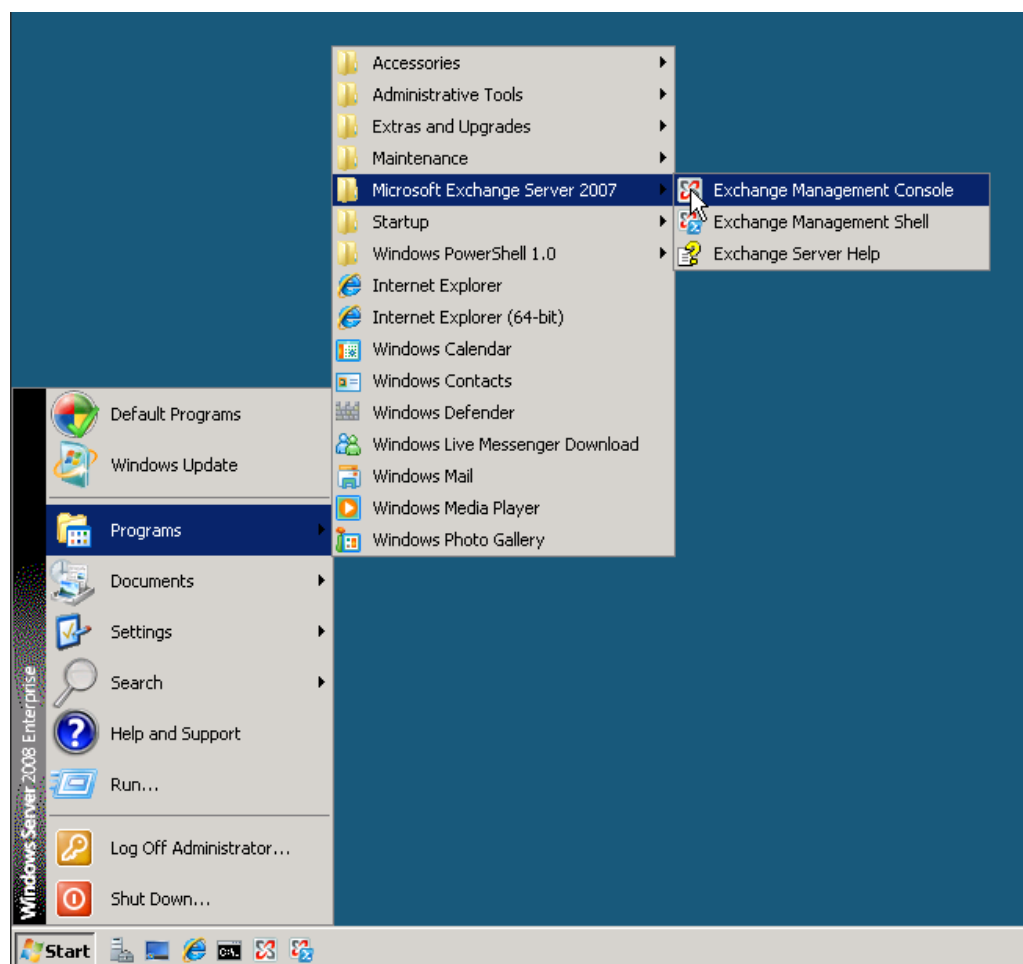
```
Machine: EXCH2K10.mpn2k10.poc
[PS] C:\Windows\system32>Get-ExchangeCertificate -ThumbPrint 41137E14BFD2509E666148FA974C594F4F6EC3E0 | Format-List
AccessRules           : <System.Security.AccessControl.CryptoKeyAccessRule, System.Security.AccessControl.CryptoKeyAccessR
CertificateDomains    : <e2k10.poc>
HasPrivateKey         : True
IsSelfSigned         : False
Issuer                : CN=IS Development Lab Root Certificate Authority, DC=isdevlab, DC=local
NotAfter              : 4/22/2011 2:10:54 PM
NotBefore             : 4/22/2010 2:00:54 PM
PublicKeySize         : 1024
RootCAType            : Registry
SerialNumber          : 14F0301300000000000003
Services              : SMTP
Status                : RevocationCheckFailure
Subject               : CN=e2k10.poc, O=E2K10, S=ON, C=CA
Thumbprint             : 41137E14BFD2509E666148FA974C594F4F6EC3E0

[PS] C:\Windows\system32>
```

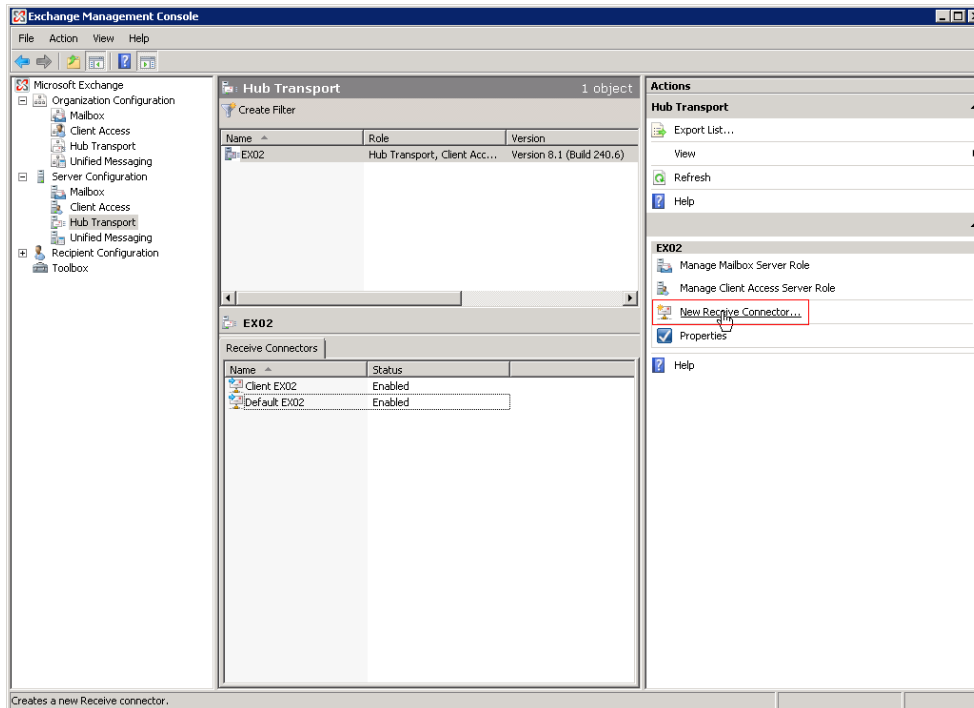
## 9.0 Setup Receive Connector

To configure a Default Receive Connector for ONE Mail Partnered environment on your Exchange Server 2010, use the Exchange Management Console as explained below:

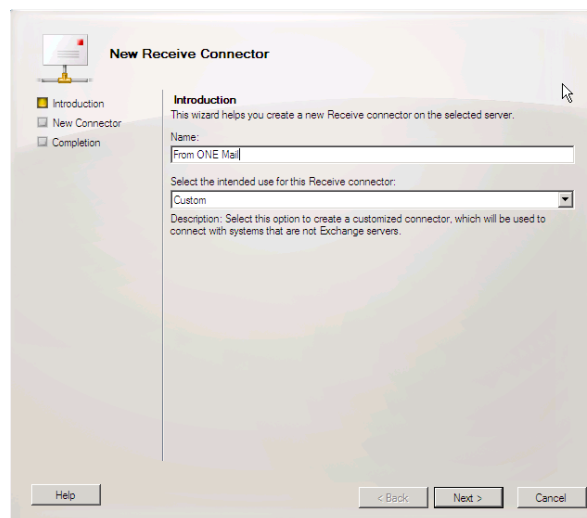
- Login to your Microsoft Exchange 2010 hub transport server.
- Click **Start > Programs > Microsoft Exchange Server 2010 > Exchange Management Console**
- **NOTE:** Screenshots are taken for this section are taken on MS Exchange Server 2007, but the functions and procedures are similar on MS Exchange Server 2010.



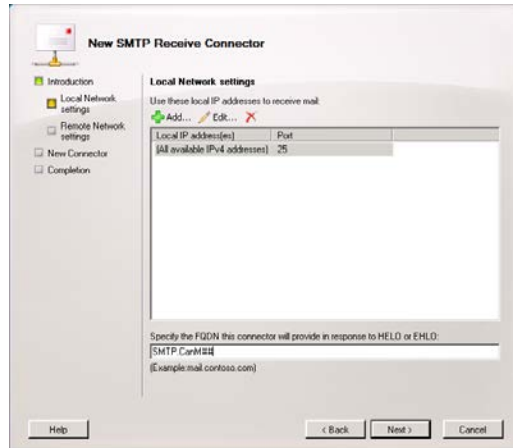
- In the left tree pane expand **Server Configuration** and select **Hub Transport** container. In upper middle pane, select your hub transport server, and in left pane, select **New Receive Connector** :



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



- 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.

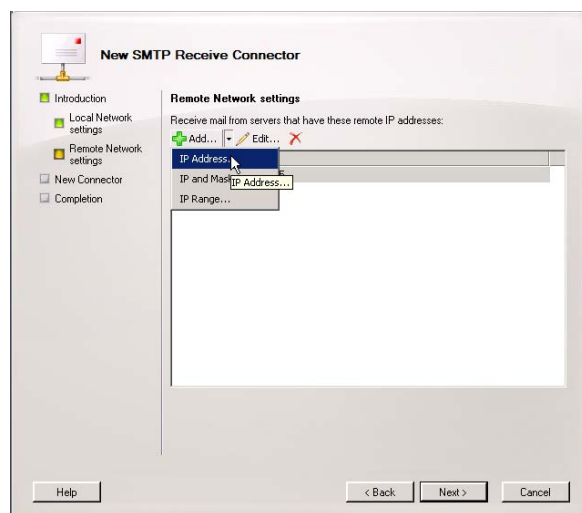


For example you can run **Get-ExchangeCertificate -ThumbPrint eHo\_Certificate\_ThumbPrint | fl** command, and in subject line find CN component of the certificate:

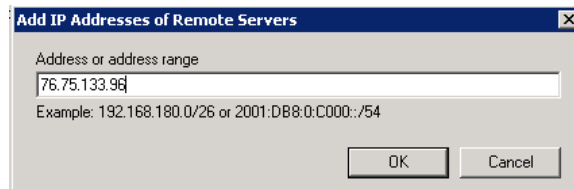
```
[PS] C:\Windows\System32>get-exchangecertificate -thumbprint 76C00F8EDD81F1310BC
CCD511B66E4A3D349F541 | list

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        : 76C00F8EDD81F1310BC00D511B66E4A3D349F541
```

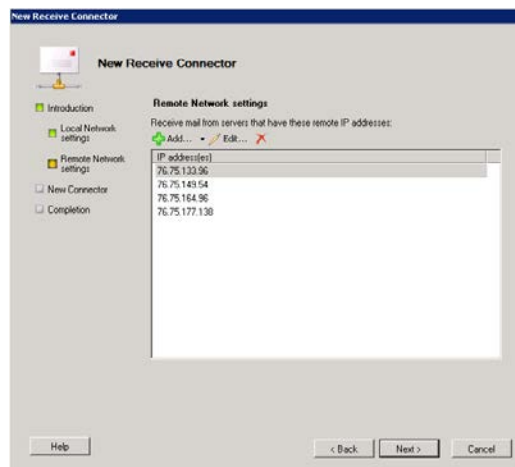
- In **Remote Network settings** window, you need to add IP address of eHealth Ontario's TLS-OUT servers here by selecting down arrow button next to **+Add** and chose **IP Address...** option.



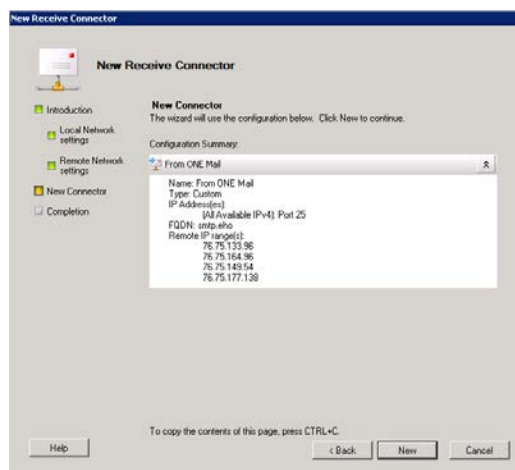
- In **Add IP Address(es) of Remote Servers** pop-up window insert IP Address of eHealth Ontario's TLS-OUT servers and click on **OK** to exit this screen. There are 4 IPs to be added:
  - 76.75.133.96
  - 76.75.164.96
  - 76.75.149.54
  - 76.75.177.138



- 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:

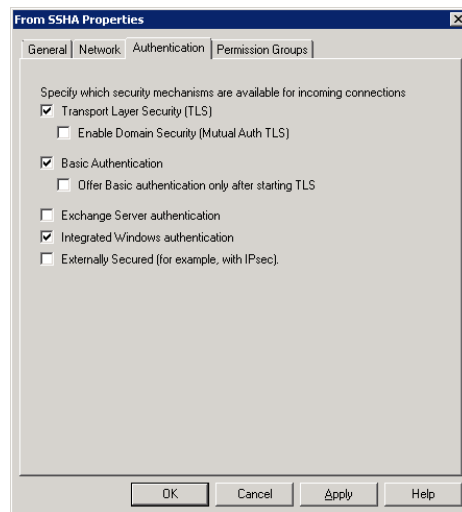


- Review configuration settings in **Configuration Summary** window and click on **New** button to create connector and click on **Finish** in **Completion** window to exit:

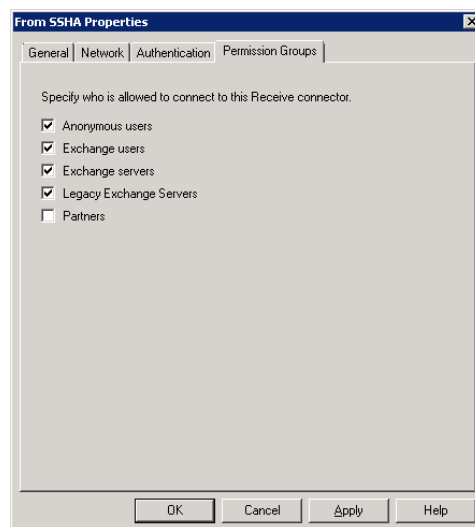




- Double click on newly created connector **From eHealth Ontario** to get properties and switch to **Authentication** tab and only select the following options:
  - Transport Layer Security (TLS)
  - Basic Authentication
  - Integrated Windows authentication



- 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**.



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

## 10.0 Setup Send Connector

To create and configure a Send Connector for the ONE Mail Partnered environment on your Exchange Server 2010 use Exchange Management Console, as explained below:

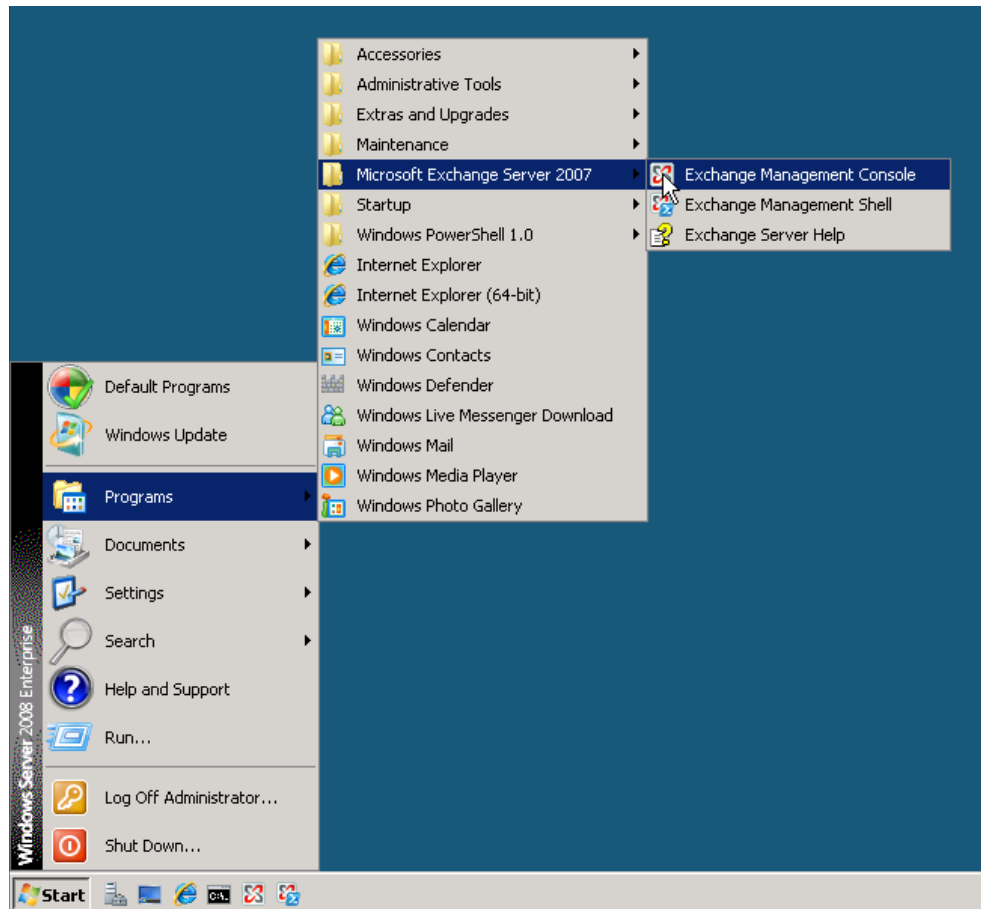
---

**Note:** Do not create this connector until “deployment date”.

**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 2010 host server.
- Click **Start > Programs > Microsoft Exchange Server 2010 > Exchange Management Console**.

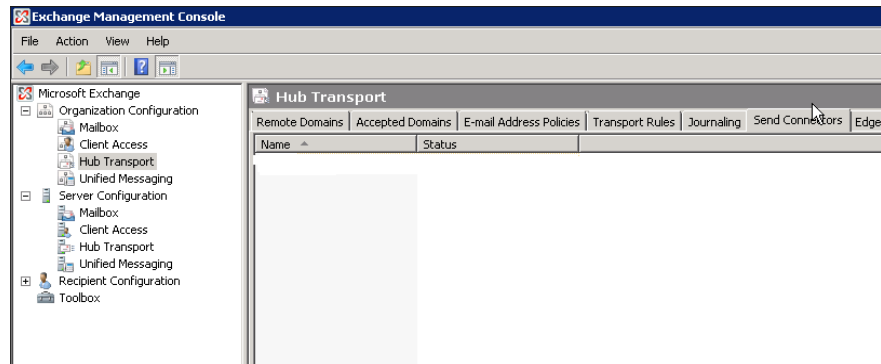


---

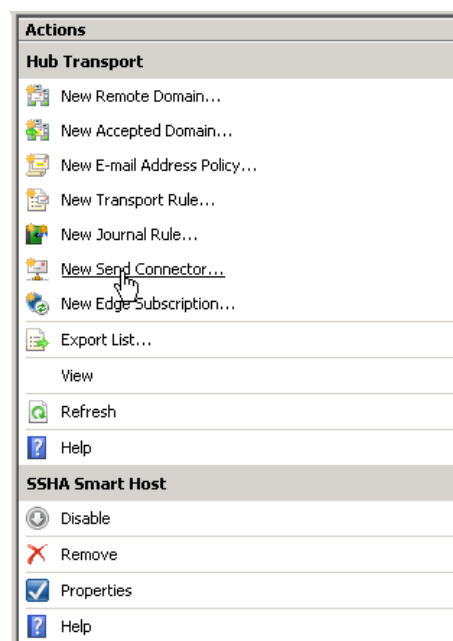
**NOTE:** Screenshots are taken for this section is taken on MS Exchange Server 2007, but the functions and procedures are similar on MS Exchange Server 2010.

---

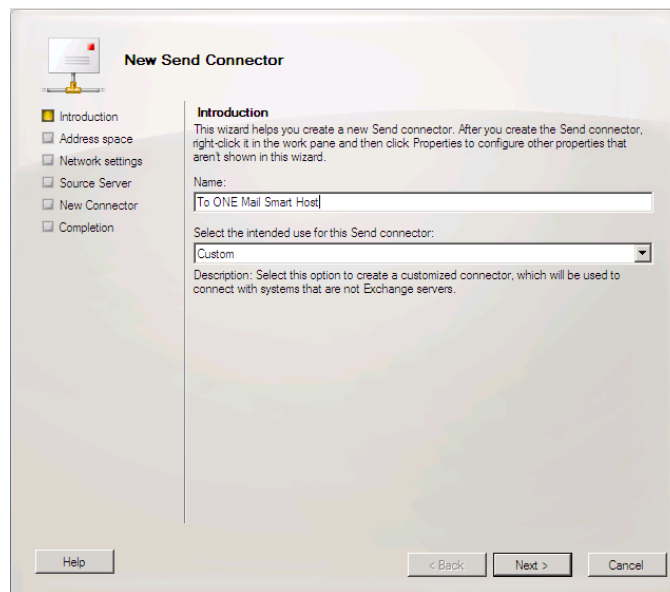
- In Exchange Management Console, in the left tree pane browse to Organization To n Configuration to Hub Transport container. Then select the **Send Connector** tab. If you have Send Connector configured to route your out-bound e-mail directly to Internet or to your previous ISP you need to delete that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



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



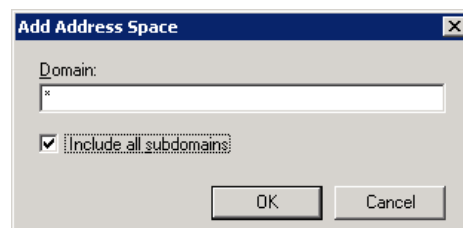
- On the **New SMTP Send Connector** introduction screen select the name of the new connector and insert in the **Name** field (ex. To ONE Mail Smart Host). From the **Select the intended use for this Send connector** drop down menu select **Custom** and press **Next**.



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



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



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

The screenshot shows the 'New SMTP Send Connector' wizard at the 'Address space' step. On the left, a navigation pane lists: Introduction (selected), Address space, Network settings, Source Server, New Connector, and Completion. The main area is titled 'Address space' and contains the instruction 'Specify the address space(s) to which this connector will route mail:'. Below this is a table with two columns: 'Domain' and 'Type'. The table contains one entry with 'smtp' in the 'Type' column. There are 'Add' and 'Remove' buttons above the table. At the bottom are 'Help', '< Back', 'Next >', and 'Cancel' buttons.

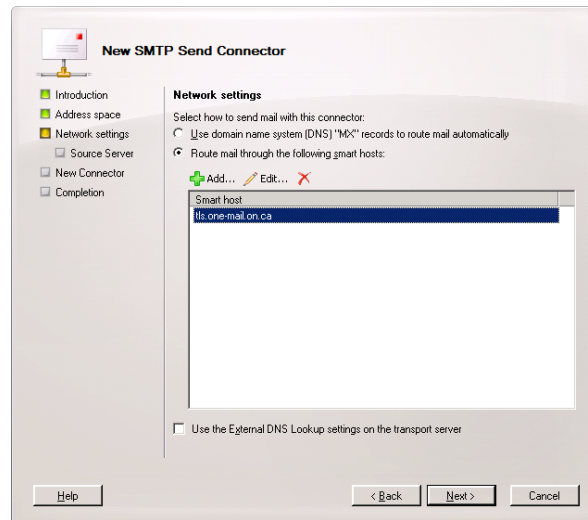
- In **Network settings** screen select option **Route mail through the following smart host:** and press the **Add** button.

The screenshot shows the 'New SMTP Send Connector' wizard at the 'Network settings' step. The navigation pane on the left is the same as the previous screen. The main area is titled 'Network settings' and contains the instruction 'Select how to send mail with this connector:'. There are two radio button options: 'Use domain name system (DNS) "MX" records to route mail automatically' (which is unselected) and 'Route mail through the following smart hosts:' (which is selected). Below the selected option is an 'Add' button and a table with one column 'Smart host'. At the bottom is a checkbox 'Use the External DNS Lookup settings on the transport server' which is unchecked. The bottom navigation buttons are 'Help', '< Back', 'Next >', and 'Cancel'.

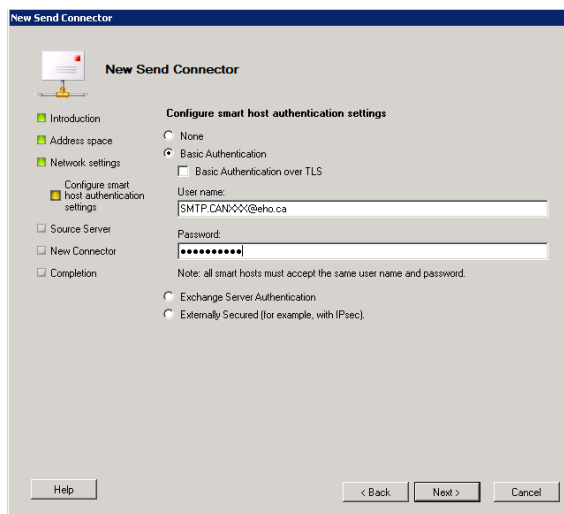
- In the **Add smart host** pop up window select **Fully qualified domain name (FQDN):** and insert eHealth Ontario's TLS-IN FQDN **smtp.tls.one-mail.on.ca** and press **OK**.

The screenshot shows the 'Add smart host' pop-up window. It has two radio button options: 'IP address:' (unselected) and 'Fully qualified domain name (FQDN):' (selected). Under 'IP address:', there is a text box with '0.0.0.0' and an example 'Example: 192.168.10.10'. Under 'Fully qualified domain name (FQDN):', there is a text box with 'smtp.tls.one-mail.on.ca' and an example 'Example: ipgateway1.contoso.com'. At the bottom are 'OK' and 'Cancel' buttons.

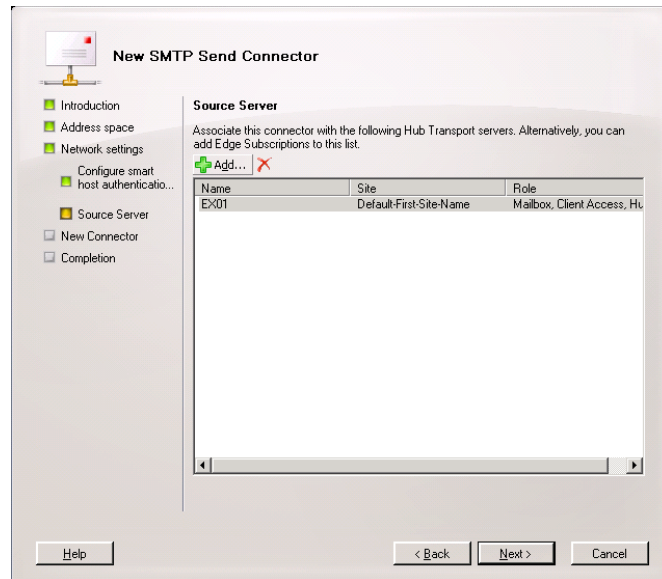
- Back in the **Network settings** screen, you will now see new smart host and press **Next** to proceed.



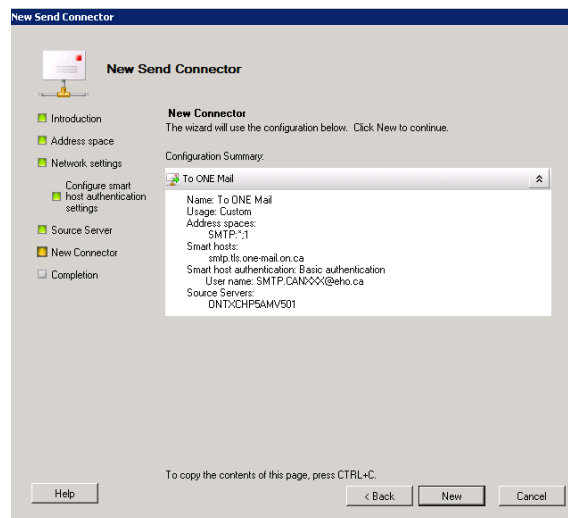
- In the **Authentication Settings** screen select only **Basic Authentication** option and insert user name and password provided by eHealth Ontario, then press **Next** to proceed.



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

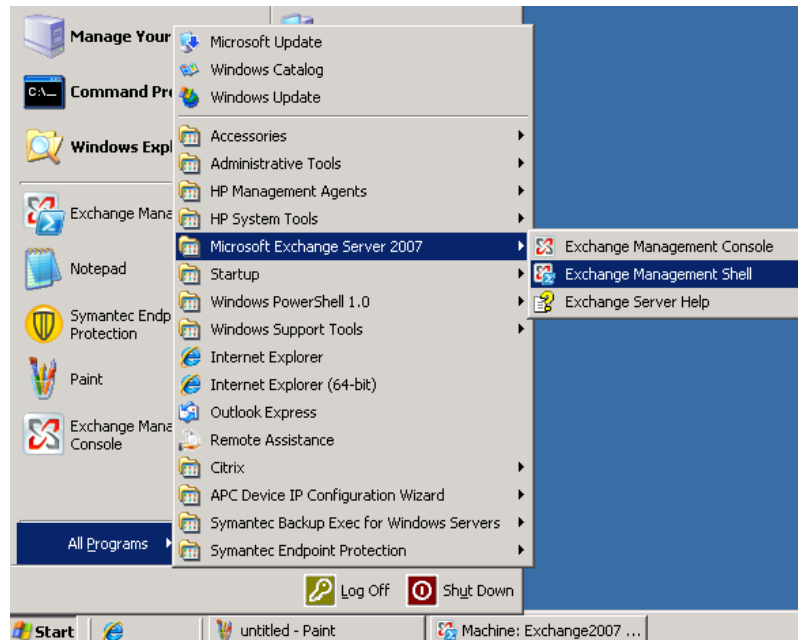


- In the **Configuration Summary** screen review selected options and press **New** to proceed.



- 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.

```
Machine: ex01 | Scope: ssh1.poc
[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
IsSmtplibConnector      : True
LinkedReceiveConnector  :
MaxMessageSize          : 10MB
Name                    : To SSHA Smart Host
Port                    : 25
ProtocolLoggingLevel    : None
RequiresTLS             : 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:

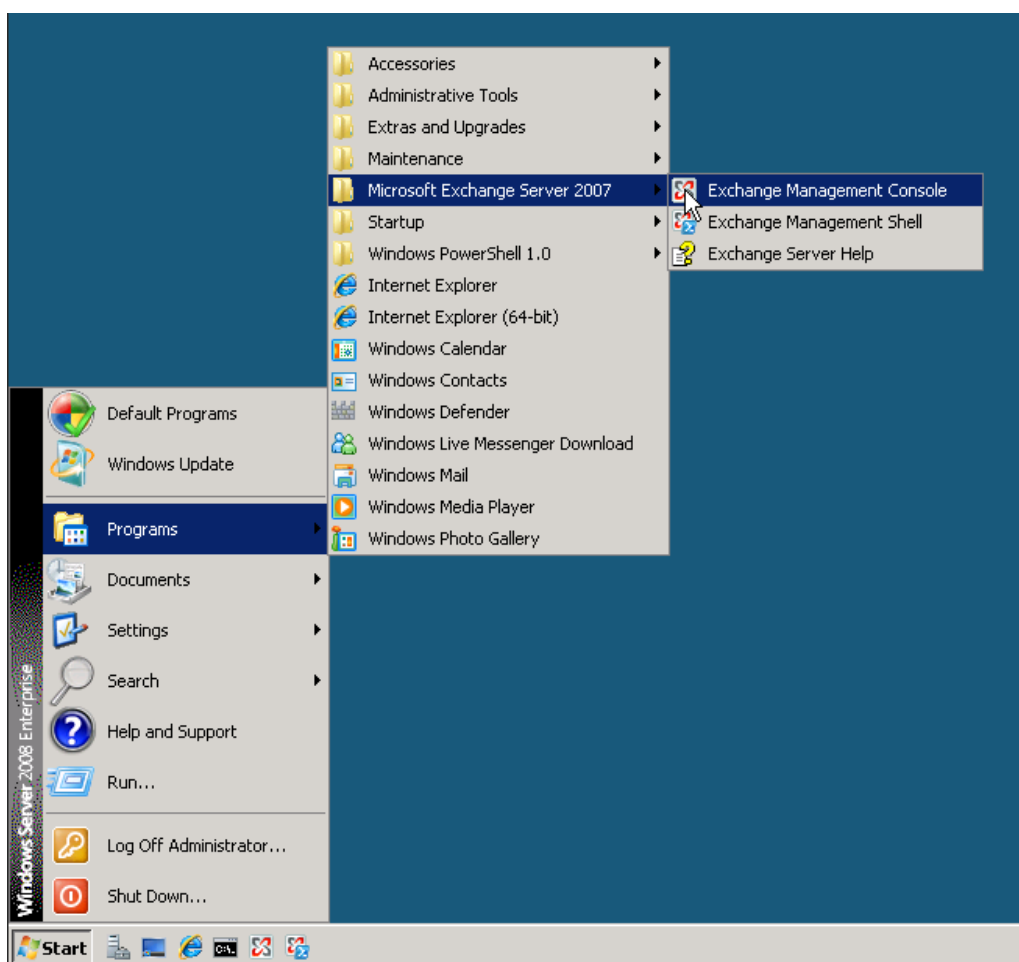
```
[PS] C:\Documents and Settings\Administrator>Set-SendConnector -Identity "To SSH
A Smart Host" -RequireTLS $True
[PS] C:\Documents and Settings\Administrator>_
```

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

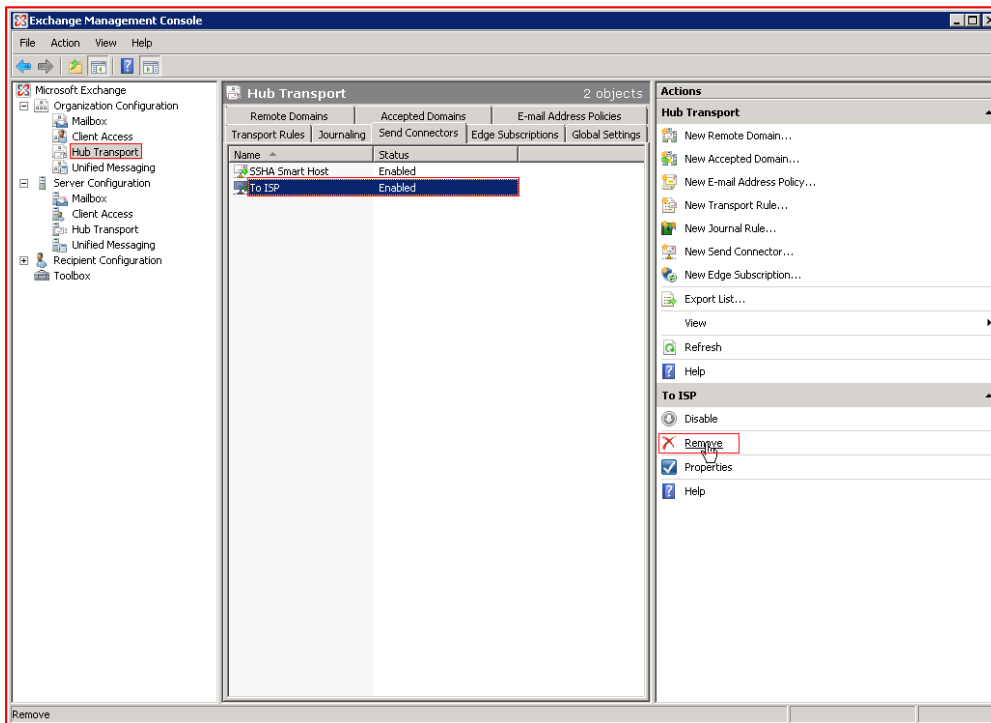
## 11.0 Post Configuration Changes

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 those steps.

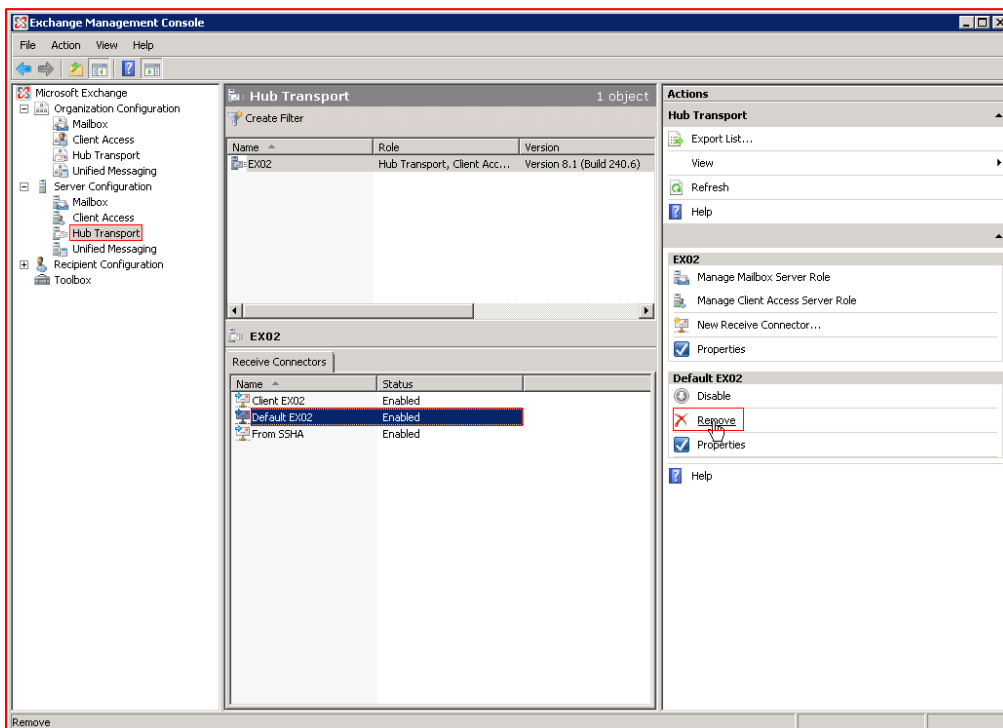
- Login to your Microsoft Exchange 2010 hub transport server.
- Click **Start > Programs > Microsoft Exchange Server 2010 > Exchange Management Console**



- 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**:



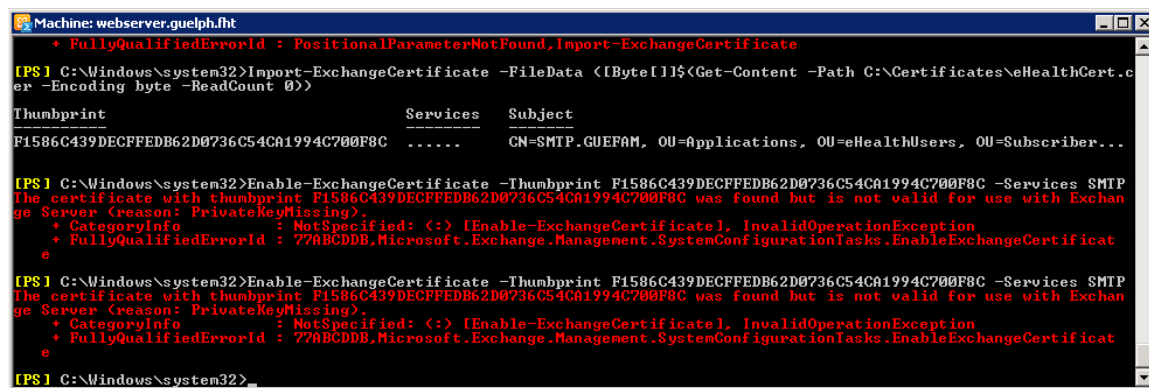
- In the left tree pane expand **Server Configuration** and select **Hub Transport** container, in the lower middle pane select old Receive connector which was used to receive mail from ISP mail server, and in left **Action** pane select **Remove**:



## 12.0 Appendix A - Known Issues

1. In case that you find that newly installed certificate is not associated with encryption keys, you will experience this error:

“The certificate with thumbprint <certificate thumbprint> was found but is not valid for use with Exchange Server (reason: PrivateKeyMissing).”



```
Machine: webserver.guelph.fht
+ FullyQualifiedErrorId : PositionalParameterNotFound.Import-ExchangeCertificate

[PS] C:\Windows\system32>Import-ExchangeCertificate -FileData ([Byte[]](Get-Content -Path C:\Certificates\MyHealthCert.cer -Encoding byte -ReadCount 0))

Thumbprint                               Services    Subject
-----
F1586C439DECFFEDB62D0736C54CA1994C700F8C ..... CN=SMTP.GUEFAM, OU=Applications, OU=eHealthUsers, OU=Subscriber...

[PS] C:\Windows\system32>Enable-ExchangeCertificate -Thumbprint F1586C439DECFFEDB62D0736C54CA1994C700F8C -Services SMTP
The certificate with thumbprint F1586C439DECFFEDB62D0736C54CA1994C700F8C was found but is not valid for use with Exchange Server (reason: PrivateKeyMissing).
+ CategoryInfo          : NotSpecified: (:) [Enable-ExchangeCertificate], InvalidOperationException
+ FullyQualifiedErrorId : 77ABCDD8,Microsoft.Exchange.Management.SystemConfigurationTasks.EnableExchangeCertificate

[PS] C:\Windows\system32>Enable-ExchangeCertificate -Thumbprint F1586C439DECFFEDB62D0736C54CA1994C700F8C -Services SMTP
The certificate with thumbprint F1586C439DECFFEDB62D0736C54CA1994C700F8C was found but is not valid for use with Exchange Server (reason: PrivateKeyMissing).
+ CategoryInfo          : NotSpecified: (:) [Enable-ExchangeCertificate], InvalidOperationException
+ FullyQualifiedErrorId : 77ABCDD8,Microsoft.Exchange.Management.SystemConfigurationTasks.EnableExchangeCertificate

[PS] C:\Windows\system32>Get-ExchangeCertificate -eHo_Certificate_ThumbPrint |Format-List
```

In that case you should run following command:

`certutil -repairstore my <serial number of certificate>`

Where <serial number of certificate> can be find by running `Get-ExchangeCertificate -eHo_Certificate_ThumbPrint |Format-List`