## ONE Mail Partnered – Client Deployment Guide

Instructions for Microsoft Exchange 2000/2003 Server

Version: 1.3

## **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.

## **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	4
2.0	Intended Audience	4
3.0	Overview	4
4.0	Creating CSR(s)	5
	4.1 Generating a CSR	5
	4.2 Send the CSR to eHealth Ontario	11
5.0	Receive the Certificates	11
6.0	Installing an Exchange Certificate	12
7.0	Verifying the Exchange certificate installation	15
8.0	Install eHealth Ontario's CA Root certificate	19
9.0	Setup SMTP Connector to ONE Mail Partnered Service	26
	9.1 Setup SMTP Connector on Exchange 2000/2003	26
	9.2 Setup SMTP Connector on Exchange 2000/2003	35

## 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 <b>Default SMTP</b> Virtual Server
4. Right click on the <b>SMTP virtual</b> server and select <b>Properties</b>	4. Right click and select <b>Properties</b> .
5. Select Access tab and click on Certificate	5. Select <b>Access</b> tab and click on <b>Certificate</b>

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

늘 Exchange Syster Default !	SMTP Virtual Server Properties		? × ×
C Eile Action ⊻i Genera ← → C II	al Access Messages Delivery		
First Organization	nable anonymous access and edit the thentication methods for this resource.	Authentication	
Servers SEHMPN1C Vir Queue Birch S	cure communication ew or set the secure communications ethod used when this virtual server is	<u>C</u> ertificate	
i i i i i i i i i i i i i i i i i i i	<sup>C</sup> Welcome to the Web Server Ce	ertificate Wizard.	×
📄 💮 Pu		Welcome to the	e Web Server
EG HT Gr ⊕-G IM IP		Certificate Wiza	ard
E I I I I I I I I I I I I I I I I I I I		This wizard helps you create certificates used in secure W between your server and a c	and administer server 'eb communications lient.
Gr	a Barbara and	Status of your Web Server:	
		Your Web Server doesn't have and you don't have any pend Certificate Wizard will help yo certificate for this Web Serve existing certificate.	ve a certificate installed ding requests. nu to create a new r or attach to an
		To continue, click Next.	
		< <u>B</u> ack	Next> Cancel

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

IS Certificate Wizard	
Server Certificate These are the methods for assignir	ng a certificate to a Web site.
Select the method you want to use	e for this web site:
Create a new certificate.	
C Assign an existing certificate	
Import a certificate from a Key I	Manager backup file.
Import a certificate from a .pfx f	file
C Copy or Move a certificate from	n a remote server site to this site.
	< <u>B</u> ack <u>N</u> ext> Cancel

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

IIS Certificate Wizard			×
Delayed or Immediate Request You can prepare a request to be sent I immediately.	ater, or you can se	end one	
Do you want to prepare a certificate re immediately to an online certification au • Prepare the request now, but send	quest to be sent la uthority? it later	iter, or do you wan	t to send it
$\bigcirc$ Send the request immediately to an	n online certification	n authority	
	< <u>B</u> ack	<u>N</u> ext >	Cancel

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

Type a name fo	r the new certificate. The name should be easy fo	or you to refer to and
emember. Name:		
<enter th="" your<=""><th>organization nam e here&gt;</th><th></th></enter>	organization nam e here>	
The bit length o	f the encryption key determines the certificate's er	ncryption strength.
The bit length o The greater the Jecrease perfo Bit lengt <u>h</u> :	f the encryption key determines the certificate's er bit length, the stronger the security. However, a mance.	ncryption strength. greater bit length may
The bit length o The greater the decrease perfo Bit lengt <u>h</u> : Select crvp	f the encryption key determines the certificate's er bit length, the stronger the security. However, a mance. 1024	ncryption strength. greater bit length may

 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

C	ertificate Wizard
rg	ganization Information Your certificate must include information about your organization that distinguishes it from other organizations.
	Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department. For further information, consult certification authority's Web site. Organization:
	<enter here="" name="" organization="" your=""></enter>
	Droanizational unit
	<enter e="" here="" nam="" organizational="" unit="" your=""></enter>
	< <u>B</u> ack <u>N</u> ext> Cancel

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

5 C	ertificate Wizard
Ö	ur Site's Common Name Your Web site's common name is its fully qualified domain name.
	Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.
	If the common name changes, you will need to obtain a new certificate.
	Common name:
	<enter by="" here="" number="" provided="" reference="" ssha="" the=""></enter>
	< Back Next > Cancel

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

Country/Region:	
CA (Canada) 🗾	
State/province:	
ON	
City/Jocality:	
TOR	
State/province and City/locality abbreviations.	must be complete, official names and may not contain

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

IIS Certificate Wizard	×
Certificate Request File Name Your certificate request is saved as a text file with the file name you specify.	
Enter a file name for the certificate request.	
<u>File name:</u>	
C:\CSR_8934282.txt	B <u>r</u> owse
<u>}</u>	
< <u>B</u> ack <u>N</u> ext >	Cancel

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

IIS Re	Certificate Wizard equest File Summary You have chosen to gene	erate a request file.		×
	To generate the following	request, click Next.		
	File name: c:\certreq.txt			
	Your request contains the	following information:		
- 	Issued To Friendly Name Country/Region State / Province City Organization Organizational Unit	Organiz ation name CA ON TOR Organization name Organizational unit		
		< <u>B</u> ack	<u>N</u> ext >	Cancel

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
EgYDVQQLEwtTdWJzY3JpYmVyczESMBAGA1UECxMJSG9zcG10YWxzMQ8wDQYDVQQI
EwZPTFNUU1QxFTATBqNVBAsTDEFwcGxpY2F0aW9uczENMAsGA1UEAxMESE1TNjCE

```
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAwmVaRaRrPLO+ZY44H2ZIX1s6jpA3
H24UDEOKYfaZ1gZesltzYDphXOMp/7ZnP350TnbiZQqpNFLqqckFOWskJSC83PEU
xMa5jJU1xTfdpGWtnYrvT+mi0q3x+KGQ4y7DDtD4KSAWXkkIKndiYH9mvPBQ+q4X
aqHqmFN/DZw/kTECAwEAAaOCAvowggL2MAsGA1UdDwQEAwIHgDArBgNVHRAEJDAi
gA8yMDA2MDIxNzAxMDQ0MVqBDzIwMDgwMzI1MDUzNDQxWjCBxQYIKwYBBQUHAQEE
gbgwgbUwgbIGCCsGAQUFBzAChoGlbGRhcDovL3NzaHBraTJhMDAwMXUuc3Vic2Nv
aWJlcnMuc3NoL2NuPVNtYXJ0IFN5c3RlbXMgZm9yIEhlYWx0aCBBZ2VuY3kgUm9v
dCBDQSAtIFR1c3RpbmcsIG91PVBLSSwgb3U9U2VjdXJpdHksIG91PVNTSCBTZXJ2
aWNlcywgZGM9U3Vic2NyaWJlcnMsIGRjPXNzaD9jQUNlcnRpZmljYXRlMIIBigYD
VR0fBIIBgTCCAX0wqcGqgb6qgbukgbgwgbUxEzARBgoJkiaJk/IsZAEZFqNzc2qx
GzAZBgoJkiaJk/IsZAEZFgtTdWJzY3JpYmVyczEVMBMGA1UECxMMU1NIIFN1cnZp
Y2VzMREwDwYDVQQLEwhTZWN1cml0eTEMMAoGA1UECxMDUEtJMTowOAYDVQQDEzFT
bWFydCBTeXN0ZW1zIGZvciBIZWFsdGggQWdlbmN5IFJvb3QgQ0EgLSBUZXN0aW5n
MQ0wCwYDVQQDEwRDUkwyMIG2oIGzoIGwhoGtbGRhcDovL2NybHUuc3NoYS5jYS9j
bj1TbWFydCUyMFN5c3RlbXMlMjBmb3IlMjBIZWFsdGqlMjBBZ2VuY3klMjBSb290
JTIwQ0ElMjAtJTIwVGVzdGluZyxvdT1QS0ksb3U9U2VjdXJpdHksb3U9U1NIJTIw
U2VydmljZXMsZGM9U3Vic2NyaWJlcnMsZGM9c3NoP2NlcnRpZmljYXRlUmV2b2Nh
dGlvbkxpc3QwHwYDVR0jBBgwFoAUoDjQCKRd/Fk7eTuqfcpZKT5GWRowHQYDVR00
BBYEFDtLS1NyMiADLtzKP/vfrPTThIQVMAkGA1UdEwQCMAAwGQYJKoZIhvZ9B0EA
BAwwChsEVjcuMQMCBLAwDQYJKoZIhvcNAQEFBQADggEBAB45Jjvk7NeokO2/iy+H
X142NV7wRR11BmcJKLxYE3YgrGw7C7kBRjBEZbjoQy8g1Mniop8m1kA6tiJreuF2
kAxElilGu1DK5IqrA+1W7S3b7G5XipgC7jF8iQ9zUhblTsfLfLKZ0r/exPX3LE/P
RYeqIUbATXfc/tuwcPm4kjRigpNIs+uEJAgkoOr73A1U2SLlGf1Q+EhSyTQ2qRI/
lIDTnEACHXbgEhU4qG8p+cN2GDcN8HJUqVLG1H6GOzfp1+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 <b>Computer</b>
3. Select the SMTP inbound gateway Server/Protocols/SMTP	3. Select the <b>Default SMTP</b> Virtual Server
4. Right click on the <b>SMTP virtual</b> <b>server</b> and select <b>Properties</b>	4. Right click and select <b>Properties</b> .
5. Select <b>Access</b> tab and click on <b>Certificate</b>	5. Select <b>Access</b> tab and click on <b>Certificate</b>

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.

IIS Certificate Wizard	×
Process a Pending Request Process a pending certificate request by retrieving the file that contains the certification authority's response.	
Enter the path and file name of the file containing the certification autho <u>P</u> ath and file name:	rity's response.
C:\Documents and Settings\Administrator\Desktop\8934282.CER	B <u>r</u> owse
< <u>B</u> ack ( <u>N</u> ext >	Cancel

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

File name: C:\Documents and Settings\Administrator\Desktop\89342 Certificate details: Issued To	
Certificate details: Issued To	282.CEF
Issued To	
Lawyed Dy Creat Cystems for Haalth Agency	
Authority Smart Systems for Health Agency	
Expiration Date 10/5/2007	
Intended Purpose Server Authentication	
Organization name	

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**.

Add/Remove Snap	in	? 🗙
Standalone Extensi	ons	
Use this page to ad	or remove a stand-alone snap-in from the conso	le.
Snap-ins added to:	Console Root	
		R.
Description		
Add	Remove About	
	ОК	ancel

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.

Local computer:	(the computer this console is running on)
C Another computer	Biowse
Allow the selecter only applies if you	d computer to be changed when launching from the command line. This I save the console.

- 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**.

Run	?X
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	mmc
	OK Cancel Browse

• The Microsoft Management Console is displayed.

🚡 Console1		
File     Action     View     Favorites     Window       ←     →     □     □     □     □	Help	
🚡 Console Roc		
Console Root	Name	
		There are no items to show in this view.

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



• On the Standalone tab, click Add.

Add/Remove Snap-in	?×
Standalone Extensions	
Use this page to add or remove a stand-alone snap-in from the conso	le.
Snap-ins added to: 🔄 Console Root 💌	£
	R
C Description	
Add Remove About	
ок с	ancel

• 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

This snap-in will always mar	nage certificates f	or:	
My user account			
Service account			
<ul> <li>Computer account</li> </ul>			

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

This snap-in will always m	anage: computer this console is running on)
C Another computer:	Browse
<ul> <li>Allow the selected c only applies if you sa</li> </ul>	omputer to be changed when launching from the command line. This we 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



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

🚡 Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]								
Ele Action View Favorites Window Help								
Console Root	Issued To 🔺	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem	
🖻 🐻 Certificates (Local Computer)	ABA.ECOM Root CA	ABA.ECOM Root CA	7/9/2009	Secure Email, Server	DST (ABA.ECOM) CA			
🗄 🖳 Personal	🖼 Autoridad Certificadora de la Asoc	Autoridad Certificadora de la Asocia	6/28/2009	Secure Email, Server	Autoridad Certificad			
Trusted Root Certification Authorities	Autoridad Certificadora del Colegi	Autoridad Certificadora del Colegio	6/29/2009	Secure Email, Server	Autoridad Certificad			
Certificates	Baltimore EZ by DST	Baltimore EZ by DST	7/3/2009	Secure Email, Server	DST (Baltimore EZ) CA			
Enterprise Trust	🖼 Belgacom E-Trust Primary CA	Belgacom E-Trust Primary CA	1/21/2010	Secure Email, Server	Belgacom E-Trust Pri			
Intermediate Certification Authorities     Trucked Dublishare	C&W HKT SecureNet CA Class A	C&W HKT SecureNet CA Class A	10/16/2009	Secure Email, Server	CW HKT SecureNet			
Industed Populations	C&W HKT SecureNet CA Class B	C&W HKT SecureNet CA Class B	10/16/2009	Secure Email, Server	CW HKT SecureNet			
Third-Party Root Certification Authorities	🖼 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			
Certificate Enrolment Requests	🖼 Certisign - Autoridade Certificador	Certisign - Autoridade Certificadora	6/26/2018	Secure Email, Server	Certisign Autoridade			
E SPC	🔛 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			
	l 📾 an							

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

描 Console1 - [Console Root\Certilicates (Local Computer)\Trusted Root Certilication Authorities\Certilicates]								
📸 Eile Action View Favorites Window Help								
Console Root	Issued To 🗠	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem	
🖻 🗐 Certificates (Local Computer)	ABA.ECOM Root CA	ABA.ECOM Root CA	7/9/2009	Secure Email, Server	DST (ABA.ECOM) CA			
🗄 🧰 Personal	Autoridad Certificadora de la Asoc	Autoridad Certificadora de la Asocia	6/28/2009	Secure Email, Server	Autoridad Certificad			
Trusted Root Certification Authorities	Autoridad Certificadora del Colegi	Autoridad Certificadora del Colegio	6/29/2009	Secure Email, Server	Autoridad Certificad			
	port ore EZ by DST	Baltimore EZ by DST	7/3/2009	Secure Email, Server	DST (Baltimore EZ) CA			
Enterprise Print Solo	CA E-Trust Primary CA	Belgacom E-Trust Primary CA	1/21/2010	Secure Email, Server	Belgacom E-Trust Pri			
Trusted D	C&W HKT SecureNet CA Class A	C&W HKT SecureNet CA Class A	10/16/2009	Secure Email, Server	CW HKT SecureNet			
New Window from Here	C&W HKT SecureNet CA Class B	C&W HKT SecureNet CA Class B	10/16/2009	Secure Email, Server	CW HKT SecureNet			
Third-Part New Tacknad View	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			
Refresh	Certisign - Autoridade Certificador	Certisign - Autoridade Certificadora	6/26/2018	Secure Email, Server	Certisign Autoridade			
Export List	Certisign - Autoridade Certificador	Certisign - Autoridade Certificadora	6/26/2018	Secure Email, Server	Certisign Autoridade			
Help	Certisign Autoridade Certificadora	Certisign Autoridade Certificadora A	6/26/2018	Secure Email, Server	Certisign Autoridade			
<u></u>	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			
	🛛 🚾 desse o primeros das	dese o primero da	7/2/2010	commenced comme	couples does a pass			

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

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.	
	< Back Cancel	

• Following the Wizard select Next and Finish

Certificate Import Wizard	×			
Tok-	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.			
	< Back (Next > ) Cancel			

• 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

Specify the file you	u want to import.
Eile name:	
C:\Cert\SSHA_CA	A_Root_Cert_Production.cer
Note: More than o	one certificate can be stored in a single file in the following formats
Personal Inform	nation Exchange- PKCS #12 (.PFX,.P12)
Cryptographic M	Message Syntax Standard- PKCS #7 Certificates (.P7B)
Cryptographic M Microsoft Seriali	Message Syntax Standard- PKCS #7 Certificates (.P7B) ized Certificate Store (.SST)
Cryptographic N Microsoft Seriali	Message Syntax Standard- PKCS #7 Certificates (.P7B) ized Certificate Store (.SST)
Cryptographic N Microsoft Seriali	Message Syntax Standard- PKCS #7 Certificates (.P7B) ized Certificate Store (.SST)
Cryptographic N Microsoft Seriali	Message Syntax Standard- PKCS #7 Certificates (.P7B) ized 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 stores are	system areas where	certificates are l	kept.	
Windows can automa	tically select a certifi	cate store, or you	u can specif	y a location for
C Automatically	select the certificate	store based on th	ne type of c	ertificate
Place all certification	cates in the following	store		
Certificate sto	re:			
Trusted Rool	Certification Authori	ities		Browse

• 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 Content Certificate File Name C:\Cert\SSHA_CA_R(	
	< Back Finish Cancel	

•

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

🔓 Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]						
🚡 Eile Action View Favorites Window Help						
← →   🗈 📧 👗 🗈   🗙 😰						
Console Root	Issued To 🛛 🗛	Issued By				
🖻 🐻 Certificates (Local Computer)	SERVICIOS DE CERTIFICACION - A.N.C.	SERVICIOS DE CERTIFICACION - A				
Personal	🖼 SIA Secure Client CA	SIA Secure Client CA				
Trusted Root Certification Authorities	🖼 SIA Secure Server CA	SIA Secure Server CA				
	Smart Systems for Health Agency Root Certificate Authority	Smart Systems for Health Agency Ro				
Enterprise Trust	🖼 Swisskey Root CA	Swisskey Root CA				
Trusted Publishers	🖼 TC TrustCenter Class 1 CA	TC TrustCenter Class 1 CA				
Trasted Fabilities	🖼 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.

# 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).

operties				?		
Address Space	Connected Ro	uting Groups	Delivery Res	trictions		
Content Restrict	tions Delivery Options Advanced Details					
	Ge	eneral				
M=0		0.1.1.0.1				
<u>N</u> ame:	eHelatr	n Untario Smart	Host			
smtp.tls.on	e-mail.on.ca					
Server	15.	Virtual Serve	r			
SEHMPN1DC1		Default SMT	P Virtual Server			
Add	Add <u>R</u> emove					
Do not allow		le .				
1 Do not allow	public toluer referra	15				
	OK Car	ncel /		Help		

• 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.

elatii ontario s	mart I	lost Pr	operti	ies				?
Content Restrict	ions	Deli	very Op Gene	otions eral	Ac	lvance	4	Details
Address Space	Co	nnecte	d Routi	ng Grou	ps	Delive	ery Re	estrictions
Create, modify, o		e an ad	dress <u>s</u>	pace.			L Cov	at I
Type	Addres	S					C:	st
			_					
	Mo	dify	<u> </u>	<u>ł</u> emove				
Add	<u>M</u> o pe	dify		<u>l</u> emove				
Add	<u>M</u> o pe ganizatio	dify	<u> </u>	<u>}</u> emove				
Connector scop	<u>Mo</u> pe ganizatio group	dify		<u>ł</u> emove				
Add Connector scop © Entire org © Routing g Allow message	<u>M</u> o pe ganizatiu group ges to b	dify on e relaye	d to the	<u>ł</u> emove ese dom	ains			

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

Add Address Space				? ×
<u>S</u> elect an address typ	ie:			
SMTP X400 MS CCMAIL NOTES GWISE Other				
	OK	Cancel	Help	

• 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

Internet Address Spa	ce Properties		? ×
General			
🖌 SMTP			
<u>E</u> -mail domain:	×		
<u>C</u> ost:	1		
OK	Cancel	Apply	Help

• Now your Address Space tab should look like following screen

eHelath Ontario Sn	nart Host Properties	? ×						
Content Restriction	ons Delivery Options	Advanced Details						
Address Casaa	General							
Address Space	Address Space Connected Routing Groups Delivery Restrictions							
Create, modify, or	remove an address <u>s</u> pace.							
Туре А	\ddress	Cost						
SMTP *		1						
A <u>d</u> d	Modify <u>R</u> emove							
- Connector scop	e							
Entire orga	anization							
C Routing gr	roup							
Allow message	es to be relayed to these domain:	3						
(	DK Cancel	Apply Help						

• Switch to Advanced tab and click on Outbound Security... button

eHelath Ontario Smart Host Properties ? 🗙				
General				
Address Space Connected Routing Groups Delivery Restrictions				
Content Restrictions Delivery Options Advanced Details				
Dutbound Security				
Do not send ETRN/TURN				
Request ETRN/TURN when sending messages				
Additionally request mail at specified times				
Request ETRN/TURN from different server				
<u>S</u> erver:				
Connection time:				
Bun dailu at 11:00 PM				
Specify how to request that remote servers dequeue mail				
C Issue <u>E</u> TRN				
Domains				
C Issue TURN (Requires Basic or Windows security)				

• 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

Dutbound Secur	ity 🔉
C Anonymous a	ICCESS
No user nam	e or password required
<u>     Basic authen     Basic authen     Constant     </u>	ication (password is sent in clear text)
User:	<u>M</u> odify
C Integrated W	indows Authentication
The client an Interface.	d server negotiate the Windows Systems Security Provider
Account:	M <u>o</u> dify
LS encrypti	on
	OK Cancel <u>H</u> elp

• 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

Outbound Connection Credentials	? ×
<u>U</u> ser:	
SMTP.CAN##@sshacer	
Password:	
*****	
, Confirm password	
*****	
, 	
OK Car	ncel

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

D <u>Anonymous</u> No user nan	access ne or password required	
Basic auther	ntication (password is sent in clear text)	
User:	SMTP.CAN##@sshacert	<u>M</u> odify
] Integrated V	Vindows Authentication	
The client a Interface.	nd server negotiate the Windows Systems Secu	rrity Provider
Account:		M <u>o</u> dify
TLS encrypt	tion	

- 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** 

🐚 Internet Information Servic	es (IIS) Manager		
🐚 <u>F</u> ile <u>A</u> ction <u>V</u> iew <u>W</u> indov	/ <u>H</u> elp		_ 8 ×
← → 🗈 🖪 🗗 🗟	🔁 🕨 🖿 🛛		
Internet Information Services	Name Domains Current Sessions		
Domains Current Sessions	<b>Start</b> Stop P <u>a</u> use		
	New +		
	⊻iew New <u>W</u> indow from Here		
	Rena <u>m</u> e Refresh Export <u>L</u> ist		
	Properties		
<b>↓</b>			
Opens property sheet for the curren	t selection.		

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

Default SMTP Virtual Server Properties	? ×		
General Access Messages Delivery L	DAP Routing Security		
Outbound			
<u>First retry interval (minutes):</u>	15		
Second retry interval (minutes):	30		
T <u>h</u> ird retry interval (minutes):	60		
S <u>u</u> bsequent retry interval (minutes):	240		
Delay notification:	12 Hours 💌		
Expiration timeout:	2 Days 💌		
-Local			
Delay <u>n</u> otification:	12 Hours 💌		
Expiration timeout:	2 Days 💌		
Outbound Security Outbound connections Advanced			
OK Cancel	<u>Apply</u> Help		

• 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.

Advanced Delivery 🔀
Maximum hop count:
Masquerade <u>d</u> omain:
Eully-qualified domain name:           SEHMPNISA         Check DNS
Smart host: smtp.tls.one-mail.on.ca
Attempt direct delivery before sending to smart host     Reviews DNS look up on incoming measures
errorm reverse DNS lookup on incoming messages
OK Cancel <u>H</u> elp

• Back on Delivery tab, now click on Outbound Security... button

Default SMTP Virtual Server Properties	<u>?</u> ×		
General Access Messages Delivery LDA	PRouting Security		
Cutbound			
Eirst retry interval (minutes):	15		
Sec <u>o</u> nd retry interval (minutes):	30		
T <u>h</u> ird retry interval (minutes):	60		
S <u>u</u> bsequent retry interval (minutes):	240		
Delay notification:	12 Hours		
Expiration timeout:	2 Days		
Local			
Delay <u>n</u> otification:	12 Hours 💌		
Expiration timeout:	2 Days 💌		
Outbound Security Outbound <u>connections</u> Advanced			
OK Cancel	Apply Help		

• 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.

Outbound Security		×
C Anonymous access		
No user name or pas	sword required.	
Basic authentication	i i i i i i i i i i i i i i i i i i i	
The password will be commands.	sent over the network in clear text	using standard
User name:	SMTP.OrgNam@eho.ca	Browse
Password:	жинини	
C Integrated Windows	Authentication	
The client and server Interface.	r negotiate the Windows Security S	upport Provider
A <u>c</u> count:		Bro <u>w</u> se
Passwor <u>d</u> :	мининини	
✓ ILS encryption		
	OK Cancel	Help

- 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.