

# CareExchange.in

**GOOD TO KNOW** Adding Domain in Existing Hybrid Configuration

## How to Use a Self Signed Certificate in Exchange 2010

February 22, 2012 Certificates, Exchange 2010

Article Updated : Using a internal windows CA certificate with Exchange 2010

Using a Self Sign Certificate can Manage Owa alone, But Issuing a Internal Windows CA Certificate can serve all type of Clients

We can use a internal windows CA certificate with Exchange 2010 to avoid Cert Errors

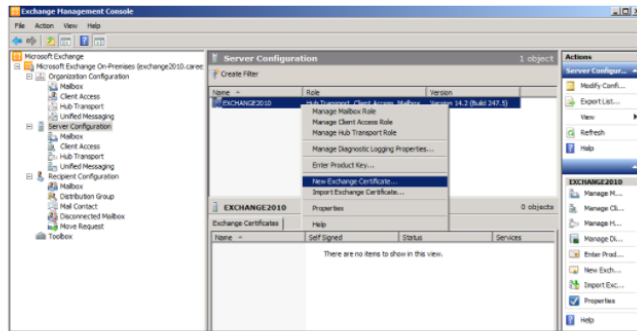
Something which you need to know is , Using a Internal Windows CA Certificate you need to install the certificates on every machine you use and Mobile devices other wise you will end up in a certificate error in the IE

So that's why people prefer going for a 3rd party certificate to overcome it.

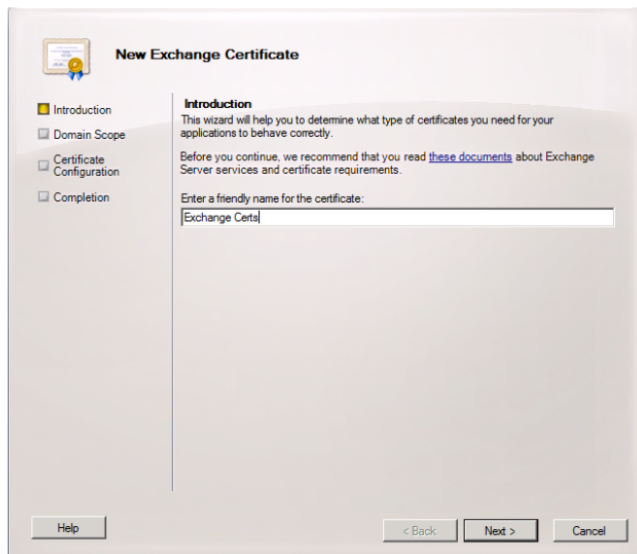
In this article We Will Learn issuing a Internal Windows CA Certificate , for this to be used Externally you need to have a CNAME record in your public DNS pointing to your Public IP NAT to your CAS

First we will learn how to Export a Certificate request file from Exchange 2010 .

### Step 1:



Type a Friendly Name :



Wild Card is used if you are going to manage more URLs .For Example : \*.Domain.com

- 750 Subscribers
- 1,130 Fans
- 64 Followers

### EMAIL SUBSCRIPTION

Subscribe via email.

Recent Popular Comments Tags

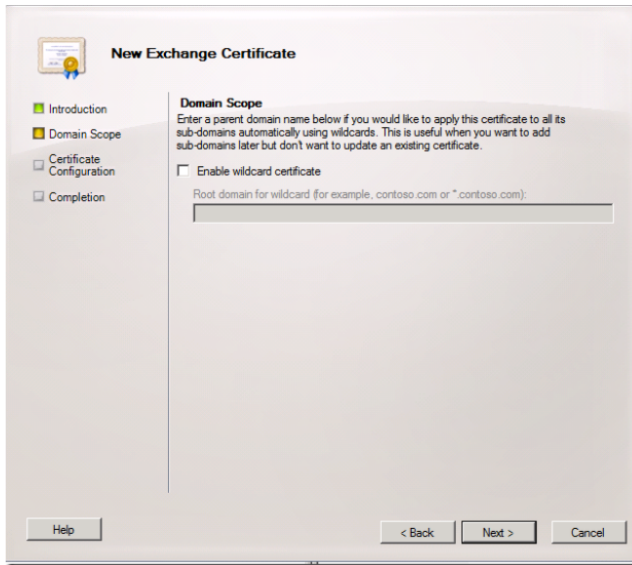
- Configuring NTP with Master Clock in Isolated Network 3 weeks ago
- VMware Windows 2012 R2 template configuration-Recommended 4 weeks ago
- IIS Installation failed-Reserved for use by another transaction 4 weeks ago
- Removing DHCP Server on Windows Server 4 weeks ago
- vSphere Client 500 SSO Error:null 4 weeks ago

### CATEGORIES

Categories

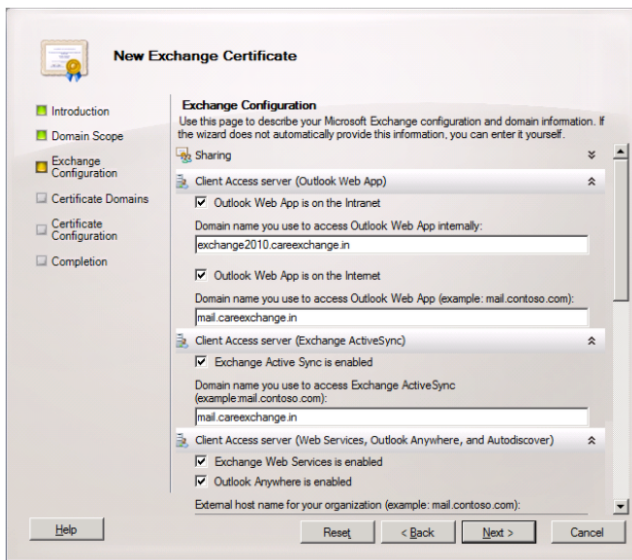
### FIND US ON FACEBOOK



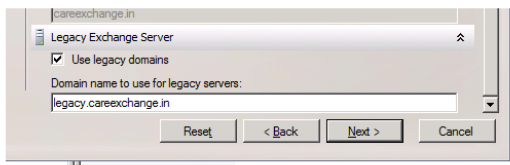


**Step 2:**

Assign the required Services for your Exchange , Give a Tick Mark

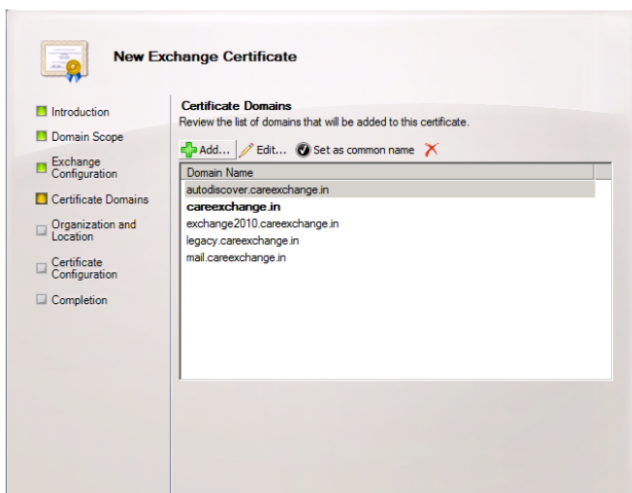


You will opt for it if you are planning for Coexistence in OWA in Exchange 2003 and Exchange 2010

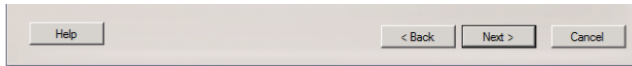


**Step 3:**

You will see the collection for URL'S







Step 4:

Fill out the Form - And set the location for the Cert Request file

**New Exchange Certificate**

- Introduction
- Domain Scope
- Exchange Configuration
- Certificate Domains
- Organization and Location**
- Certificate Configuration
- Completion

**Organization and Location**  
Use this page to enter the name of your organization, organizational unit, location, and certificate request file path.

Organization: CareExchange  
 Organization unit: Exchange Team  
 Location:   
 Country/region: United States  
 City/locality: New York  
 State/province: New York  
 Certificate Request File Path: C:\Users\administrator\CAREEXCHANGE\Desktop\Exchange Cert.req

Specify the name of the request file in the text box below. Use the Browse button to select the folder where you want the request file to be created. The name must end with the extension ".req".

Help < Back Next > Cancel

**New Exchange Certificate**

- Introduction
- Domain Scope
- Exchange Configuration
- Certificate Domains
- Organization and Location
- Certificate Configuration
- Completion**

The wizard completed successfully. Click Finish to close this wizard.  
 Elapsed time: 00:00:03  
 Summary: 2 item(s), 2 succeeded, 0 failed.

```
new -ca:ca\exchange\exchange -newkey:exchange -newcert:exchange -newreq:exchange -newkeyexportable:exchange -newkeysize:2048 -subjectname "C=US,S=New York",L="New York",O="CareExchange",OU="Exchange Team",CN="careexchange.in" -domainname "exchange2010.careexchange.in" -mail "careexchange.in" -autodiscover "careexchange.in" -legacy "careexchange.in" -server "EXCHANGE2010"
```

Elapsed Time: 00:00:03

Write file Completed

Exchange Management Shell command completed:  
 Write binary stream into the file  
 C:\Users\administrator\CAREEXCHANGE\Desktop\Exchange Cert.req.  
 Elapsed Time: 00:00:00

Step 1: Based on the information you provided, you must use a [Unified Communications certificate](#). Please get the certificate from a certification authority.  
 Step 2: Use the Complete Pending Request wizard to map the certificate to the certificate request created on the server.  
 Step 3: Assign the Exchange services to the certificate using the Assign Services to Certificate wizard.

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

Help < Back Finish Cancel

Step 5:

Your request file would look like this



Open it via Notepad, because we need this content to generate a Certificate

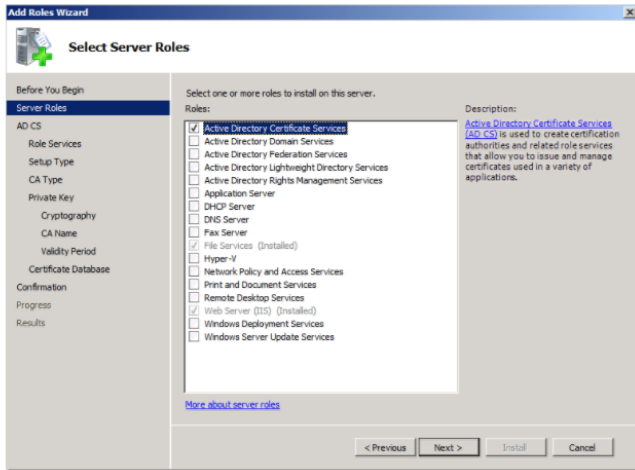
```
Exchange Cert - Notepad
File Edit Format View Help
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEHTCCA4UCAwFDEYMBYGA1UEAwPY2FyZWw4Y2hhbmd1Lm1uMRYwFAYDQQL
DA1FEgNoYw5nZSBuZWFTRUwEWDVQKDAxYXJ1R2hjaGZuZ2UxETAPBgNVBACM
CE51dyBzb3JmREwDwVQVQIDAhoZCgww9yazELMAkGA1UEBhMCVWwggE1MA0G
CSqGSIb3QDEBAQUAAIBDWAaggEKA0IBAQDRdw3qHNj9opUjwQ1NDDgYr eybXFM
VR8Z1TIV/XRqEAEQJUCs6n7QSE8ZATQVZAgLxm9HMRrBV+PpFEackSuVcpa1zy7L
YhSP2B19Y1ETr xuda+D+XWI EPGE8A1CFHDF6wDOH5q1tob3QJ0UMPhjW0A5VU
DNTB515aA2k+g/8E8CkwB4a3UuW41TsfTl i jysbg7 /pbm0C113ES892wyVUL /yE+
RFQpwk531IR1fjwYq+yxZLUAZBKRk51dyhq9I1Hsebsccr rYz /jyu1whmR3rHZS
eoa3b0TjwbDaxPx5D /PqTgZyxkn50vqkkCQBOT99tgpB01Lqw6 /mdrhfAgMBAAG
ggHAmBOGc1sGAQQBj1cNAgMxDBYKN14XL jC2WDEuJwBwBkrBgEAYI3FRQxvzBf
AgFE0BfEGNoYw5nZSBuZWFTRUwEWDVQKDAxYXJ1R2hjaGZuZ2UxETAPBgNVBACM
RVNDFEFOR0UyMDEwJW1Tl jcm9ZB2Z0LkV4Y2hhbmd1Lm1lcnZpY2IvB3N0LmV4
ZTByBgorBgEAYI3DQICMwQyYgIBAR5aAE0AaqBjAHIAbwBzAG8AZgB0ACAuBGT
AEEAIA8TAEMAaABHAG4AbgB1AGWAIBDAHIAEQBWAHQAwbWbNAHIAyQBwAGGAaQBJ
ACAUAByAG8AdgBpAGQAZQBYAwEAMIHVbgkqhkiG9w0BCQ4xgcwgCwQDgYDVROp
AQ9/BAQDAGwMI GE BgnVHREFF7B7ghx1eGNOYw5nZTIwMTAUyZFY2Ww4Y2hhbmd1
Lm1lughRtYw1S1mNRCv1eGNOYw5nZS5pboIPY2FY2Ww4Y2hhbmd1Lm1lughRdxRV
ZG1zY292ZXIuY2FY2Ww4Y2hhbmd1Lm1lughzszwdhY3kuY2FY2Ww4Y2hhbmd1Lm1l
MAWGA1udEWEb/wQMAAWhQYDR00BBYEFPKRSB6s a2X1eEMarhFJDAZYL4WEMA0G
CSqGSIb3QDEBBQUAAIBAQ5Ed7jiowqj1xhEYkIqKtXVjYTGjGQ2AVz jfQuCbnq
KLP65TNzLN2Ew5vVftajupaxZHS690J51tSol eHgaxFu4T90sY3UFydazBLUy29+
NZZvME7CmV4DCNAyOZv9FFHyUP9f eoxT0pLPC /n+3Ru /uzHUCm4OC9TiyCjLk6
1mAx9S+Hc25a1oXkvqbrvvtEvmljW8R9f09H2ht7ezWQ9PC5XSU08NUS64LF
1KBRr1cJncz1pcj11c6+mjpekVSRpyjw3TAHvnyf5kapGgub94ukkgvnyVsaerw
jddwXdr /eyxoM0jTKv20nyh1kxP51MA2LRnn5ksB/
```

-----END NEW CERTIFICATE REQUEST-----

**Step 6:**

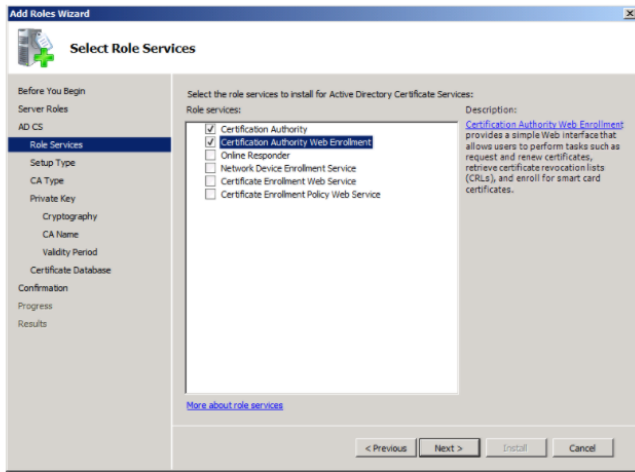
You need to have this role installed to have a Certificate Authority. It can be DC or Exchange it self

I have done this in the Exchange itself (No Harm)



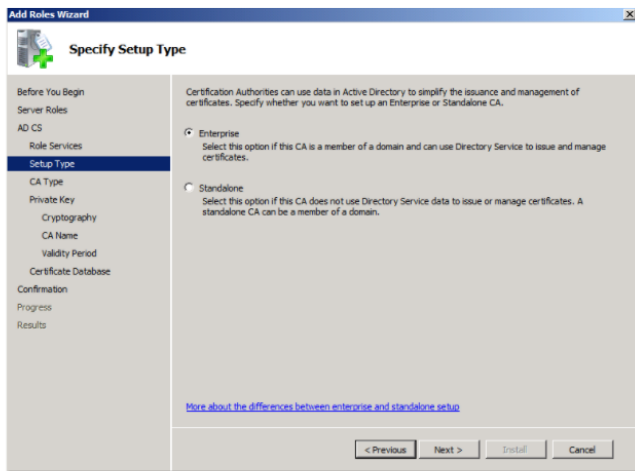
**Step 7:**

Choose : Certification authority, Certification Authority Web Enrollment



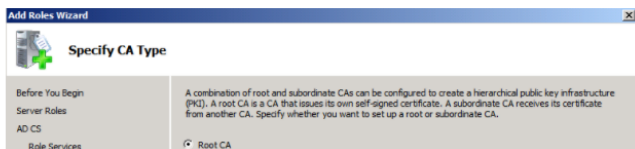
**Step 8:**

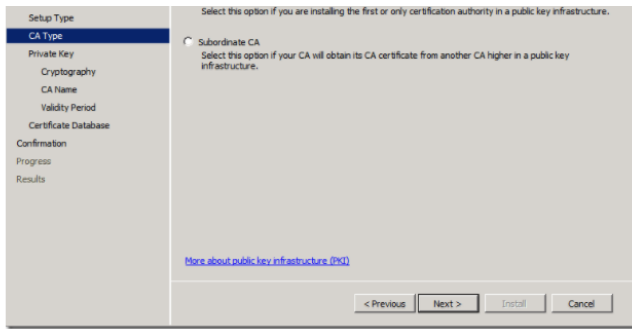
Choose Enterprise



**Step 9:**

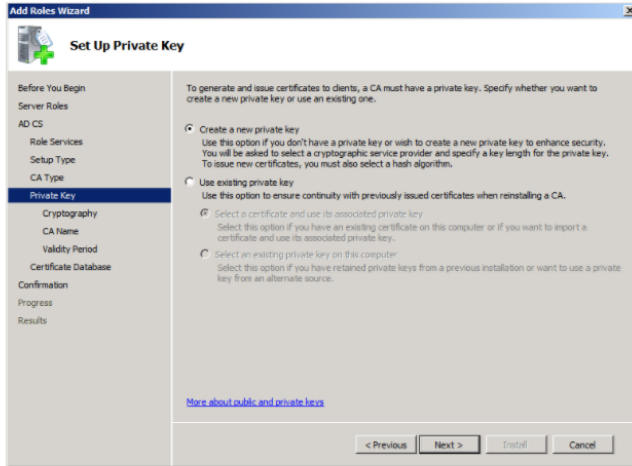
Choose Root CA





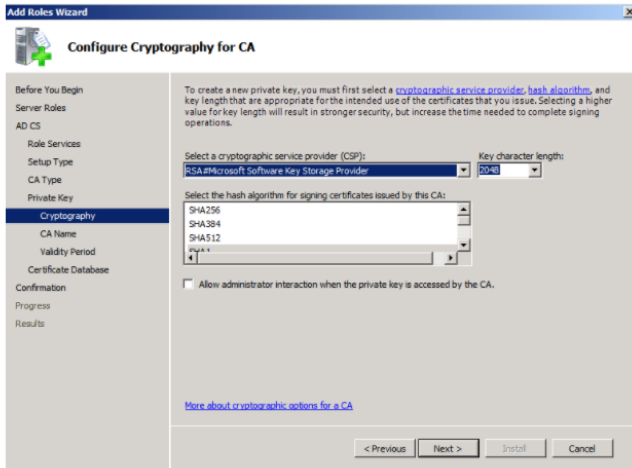
**Step 10:**

Create a new Private key



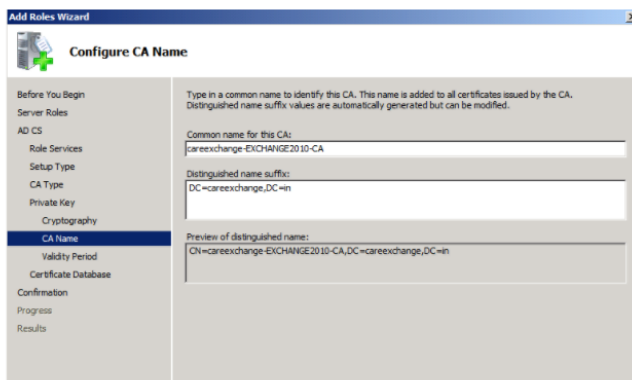
**Step 11:**

Have this Default with 2048 key Character length

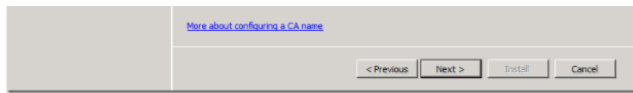


**Step 12:**

Click Next

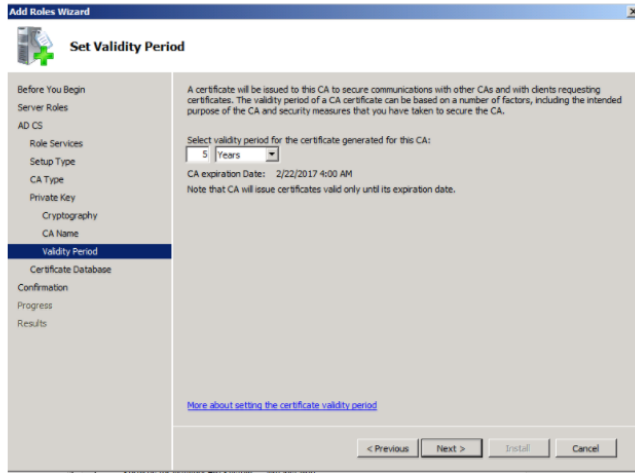




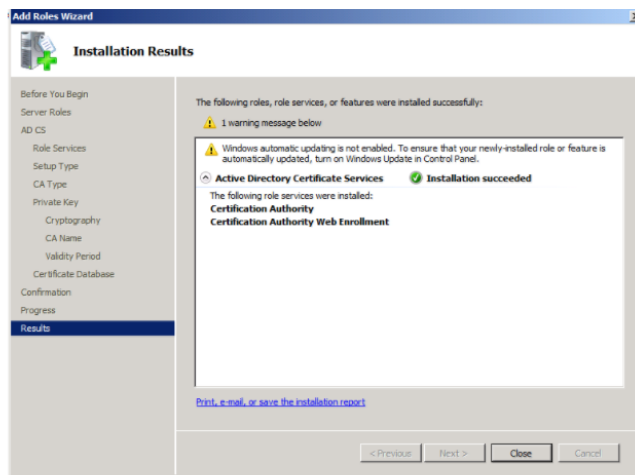


**Step 13:**

By Default Certificate is valid for 5 years , Don't make any changes on it , Click next



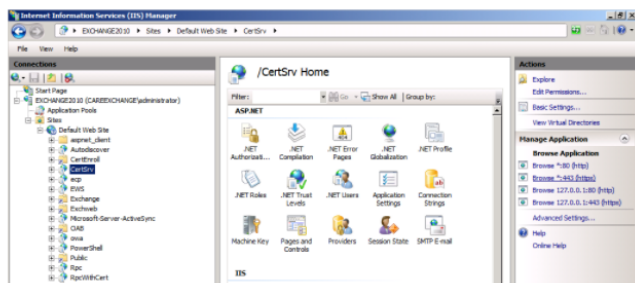
**Step 14:**



**Step 15:**

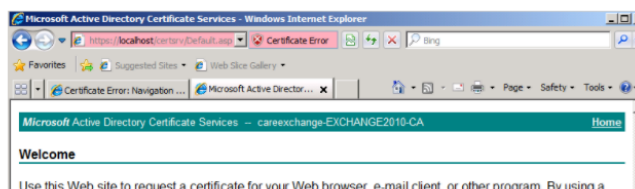
Now if you Open IIS manager , you will see "CertSrv" a Virtual Directory Created ,

Use the right side column "Browse \*.443(https)



**Step 16:**

You would see a page like this , Choose Request a Certificate



certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

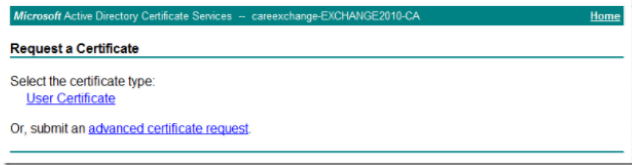
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**  
[Request a certificate](#)  
[View the status of a pending certificate request](#)  
[Download a CA certificate, certificate chain, or CRL](#)

**Step 17:**

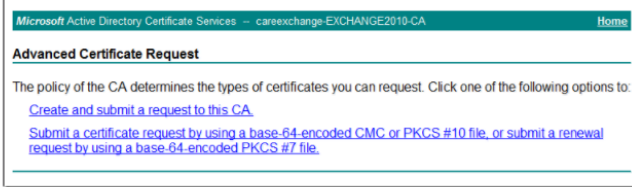
Click on Advanced Certificate Request



**Step 18:**

Choose the Second one

Submit a certificate request by using a base-64-Encoded CMC

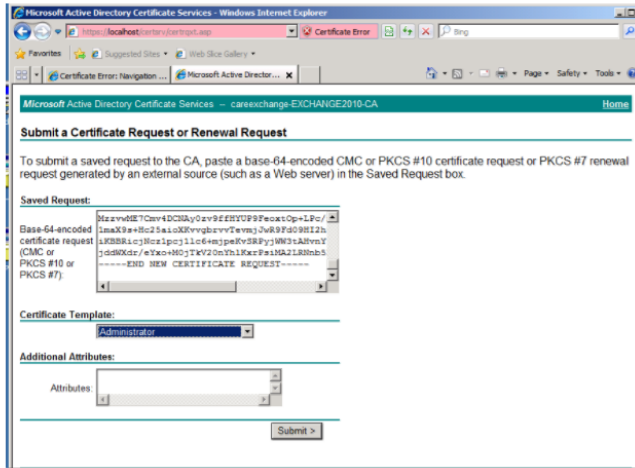


**Step 19:**

Now Copy the Note pad -

Choose Template : WebServer

NOTE \_ BELOW SCREEN SHOT \_ CHOOSE TEMPLATE \_ WEB SERVER



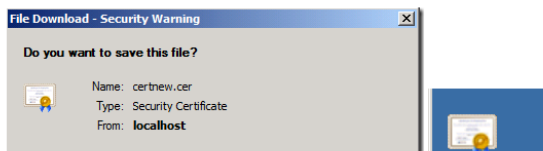
**Step 20:**

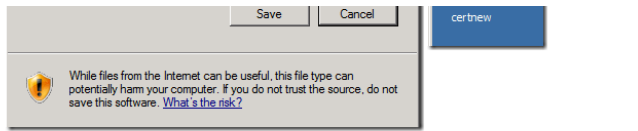
Choose "Base 64 encoded"



**Step 21:**

Save the Certificate

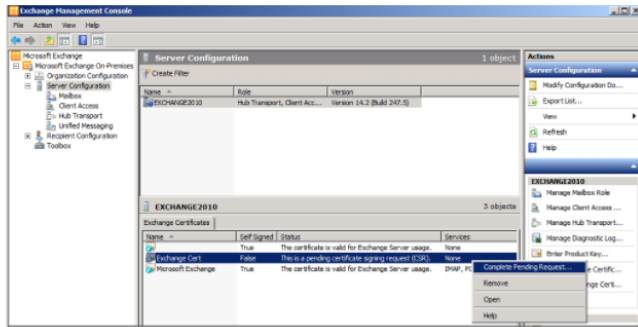




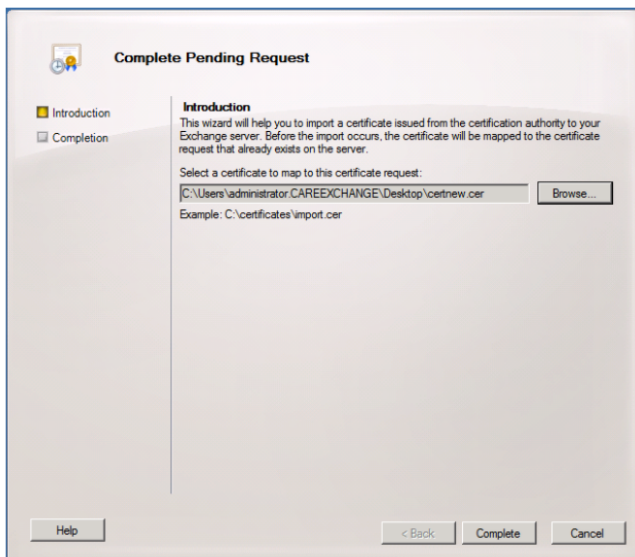
Step 22:

Now go to your EMC

Server Configuration - Complete Pending request

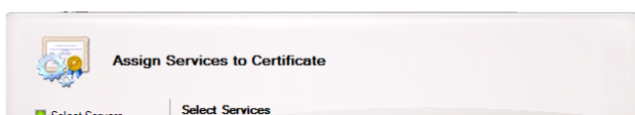
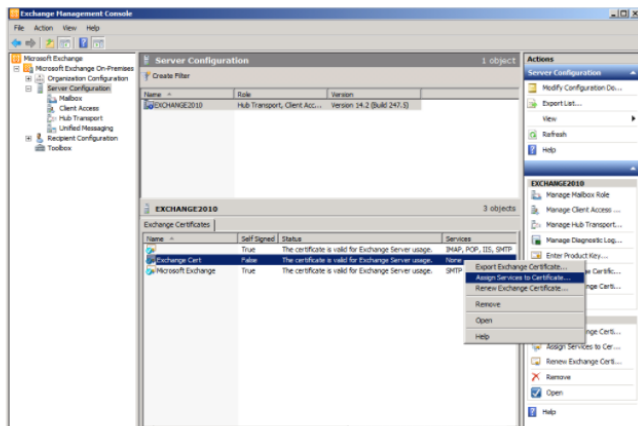


Choose the Certificate :

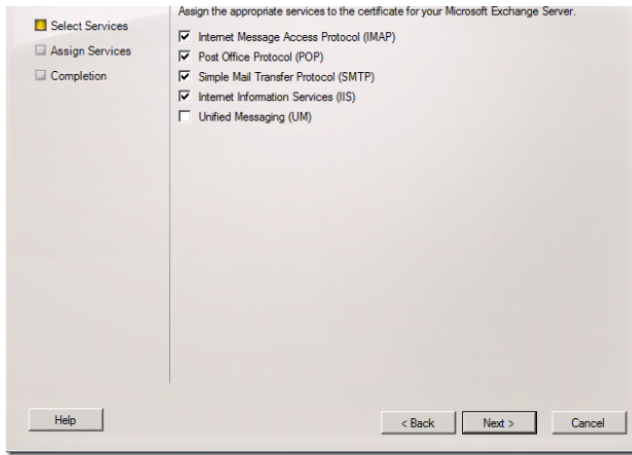


Step 23:

Now Assign Services to the Certificate







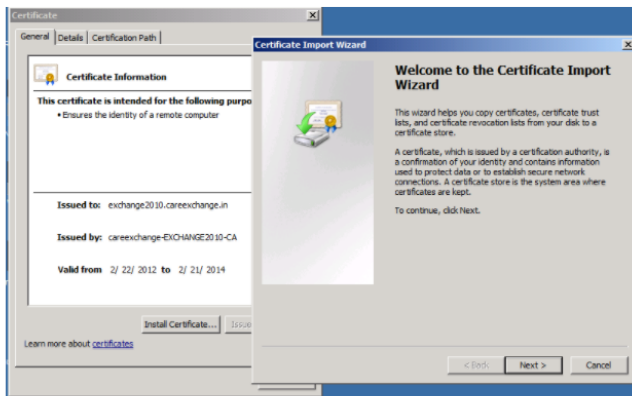
Now the Server Part is ready

Step 24:

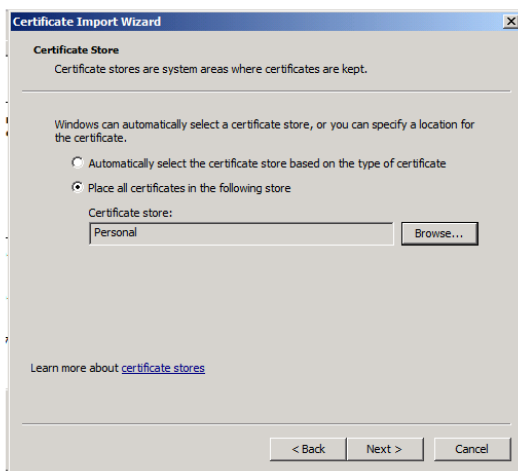
Now will learn how to install the Certificate in the Client End

Double Click on the Certificate

Click Install Certificate - Click Next -



Choose Personal -

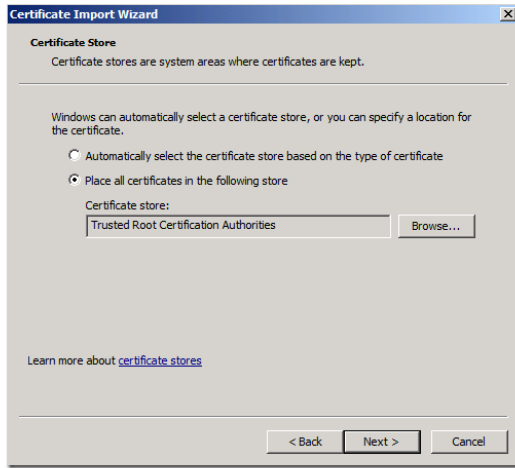


Click Next And Import will be Successful

Now Do the Same Process

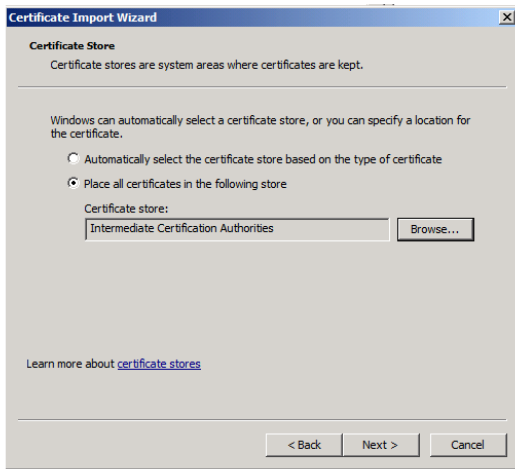
Double Click on the Certificate

Click Install Certificate - Click Next - Choose Trusted Root Certification Authorities



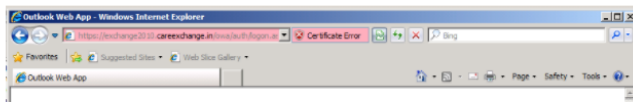
Double Click on the Certificate

Click Install Certificate - Click Next - Choose Intermediate Certification Authorities

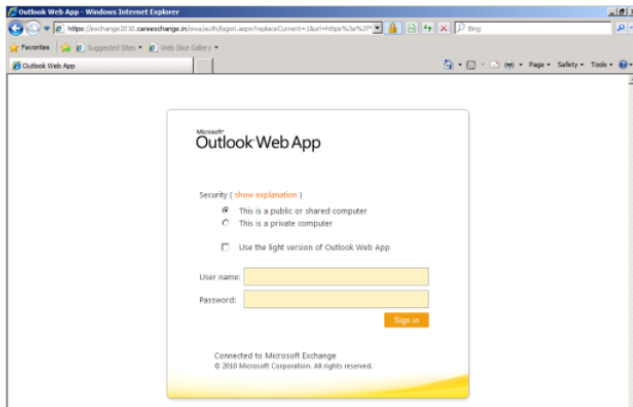


Step 25:

Before



After installing the Certificate in the Client



Great !!

Now you learnt how to Use a internal windows CA certificate with Exchange 2010

Regards

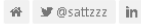
Satheshwaran Manoharan



ABOUT SATHESHWARAN MANOHARAN



Satheshwaran Manoharan is an Microsoft Exchange Server MVP , Publisher of CareExchange.in Supporting/Deploying/Designing Microsoft Exchange for some years. Extensive experience on Microsoft Technologies.



Previous Configure Receive Connector in Exchange 2010

Next Configuring 3rd Party Exchange Certificate in Exchange 2010

RELATED ARTICLES



Microsoft Exchange Topology Service Crashing on restart
March 28, 2017



Install and Configure Certificate Authority in Windows Server 2016
February 18, 2017



535 Authentication Credentials invalid on Outgoing mails
February 10, 2017

67 COMMENTS



single mom help March 19, 2012 at 11:09 am
Good blog! I really love how it is simple on my eyes and the data are well written. I'm wondering how I could be notified when a new post has been made. I've subscribed to your RSS feed which must do the trick! Have a great day!

Reply



tablette graphique bamboo March 22, 2012 at 7:33 pm
I've recently started a web site, the info you provide on this website has helped me greatly. Thank you for all of your time & work.

Reply



programy partnerskie July 15, 2012 at 9:38 am
Hello.This article was extremely motivating, especially since I was investigating for thoughts on this issue last Tuesday.

Reply



Abdul Simuel July 16, 2012 at 4:07 pm
I like this web site very much. Its a really nice situation to read and incur information.

Reply



Satheshwaran Manoharan October 17, 2012 at 2:57 pm
Thanks Abdul

Reply



programy partnerskie July 16, 2012 at 9:52 pm
I like what you guys are up too. Such smart work and reporting! Keep up the excellent works guys !?;ve incorporated you guys to my blogroll. I think it will improve the value of my site

Reply



Mauricio Pletz September 21, 2012 at 7:22 pm
I simply want to say I am just very new to blogging and honestly loved you're web page. Very likely I'm going to bookmark your site . You amazingly have exceptional stories. Thanks for sharing your blog.

Reply



Satheshwaran Manoharan October 17, 2012 at 2:57 pm
Thank you Mauricio

Reply



terpercaya October 4, 2012 at 3:58 am
Wow that was unusual. I just wrote an really long comment but after I clicked submit my comment didn't show up. Grrrr... well I'm not writing all that over again. Anyways, just wanted to say excellent blog!

Reply




Alva Buscarino October 17, 2012 at 4:37 am
You actually make it seem so easy together with your presentation but I find this topic to be really something that I feel I'd by no means understand. It seems too complicated and very huge for me. I am looking forward in your next put up, I'll attempt to get the hold of it!

Reply



Satheshwaran Manoharan October 17, 2012 at 2:56 pm
I have tried my best to make it . As simple Alva



 If you feel you are confused at some point . let me know. will help you to proceed further.  
Thank you

Reply



**Kurt Gargus** October 25, 2012 at 3:36 pm  
Good write-up. I'm regular visitor of one's site, maintain up the nice operate, and It's going to be a regular visitor for a long time.

Reply



**Dinesh** November 3, 2012 at 7:17 am  
Hi,  
It is a very good guide and I appreciate it. I followed your guide but still I receive certificate error on my client side. the only difference is my CA is on my primary DC. Can you help me!

Reply



**Satheshwaran Manoharan** November 5, 2012 at 11:39 pm  
What the is the Cert Error?  
Do we have Other Exchange Versions in the Environment?

Reply



**Graham** November 13, 2012 at 6:49 am  
Hi,  
It certainly is very comprehensive but unfortunately like Dinesh I also still get a certificate error. The error report is that "This certificate cannot be verified up to a trusted certification authority". When I check using MMC certificate plug-in the certificate is definitely imported into both the trusted root authority, intermediate authority and personal stores - I have tried doing the import both at user and local computer level for these options. Any suggestions will be gratefully accepted - we really cannot afford to go and buy a UCC certificate for this installation?  
Thanks,  
Graham

Reply



**Satheshwaran Manoharan** November 13, 2012 at 2:31 pm  
Can you check the Cert?  
Issued to : "Webmail.Domain.com"  
and the URL you browse "Webmail.domain.com/owa"  
  
The above "Issued to"and the URL  
webmail.domain.com  
should be the same.  
  
If it differs you will get the error

Reply



**Graham** November 14, 2012 at 8:04 am  
The certificate shows as issued to 'mail.com', issued by -CA. The URL I am accessing is https://mail.com/owa i.e. the certificate 'issued to' domain and the URL are definitely the same.  
Also if I try to connect using Outlook Anywhere (which is our real need) I get a message saying "the security certificate is not from a trusted certifying authority, which is pretty much the same error."  
Looking in the client certificate stores via MMC the certificate shows as Issued to mail.com, Issued By -CA, valid to 5 Nov 2014, Intended purposes 'server authentication', no friendly name and template 'WebServer'. It is in the personal store, the trusted root CAs, the Intermediate CAs and I also, in desperation, added it to third-party Root CAs. Still doesn't work  
Where can I look next to get this going? I am happy to upload or mail the certificate for you to have a look at if you want me to, just don't want to publish on the net for obvious reasons :).  
Thanks,  
Graham

Reply



**Graham** November 14, 2012 at 8:44 am  
The previous got a bit mangled : to be clear the certificate shows as issued to mail.{domain}.com by an authority {org}-{server}-CA. The URL being accessed is https://mail.{domain}.com/owa .

Reply



**Graham** November 14, 2012 at 8:59 am  
Thought I should also add that the clients on which I am installing the certificates are NOT members of the domain to which the server issuing them belongs. Is this perhaps of relevance?

Reply



**Satheshwaran Manoharan** November 14, 2012 at 5:59 pm  
Hi Graham  
For Outlook Anywhere Self Sign Cert Won't work. Its by design !!

Reply



**Graham** November 15, 2012 at 12:37 am  
1. My certificate still doesn't work for OWA regardless of whether or not it should work for OA.  
2. It isn't a 'self-signed' certificate it is a certificate produced by an internal CA. The two are different things. The self-signed certificate is what we replace with the generated one in step 23 - you can see in your own image that the original 'Microsoft Exchange' cert is marked in column 'Self-signed' as 'true' and this locally generated 'Exchange Cert' one is 'false'.  
3. If it REALLY won't work for OA (and I still believe it should) then a) what is the point of doing all this as all you gain is the ability to not have to ignore the certificate error to use OWA and b) you really need to make the article much more clear as to what this process is useful for.



**Graham** November 15, 2012 at 3:09 am  
Re: Outlook Anywhere and internal CA certificates:  
"With regards to SSL certificate support and Outlook Anywhere, the certificate type that is not supported is the certificate that Exchange generates itself using new-exchangecertificate. A CA issued certificate (whether your own or a commercial) is supported."

from  
http://social.technet.microsoft.com/Forums/en-US/exchangesvrgenerallegacy/thread/4bd74114-d146-44ad-8594-c6b58 ffe1a1



**Graham** November 15, 2012 at 8:52 am

In addition I have now exported the {org}-(server)-CA from the Trusted Root CA of the server and imported that to the Trusted Root CA of the (non-domain) client. Now OWA works as you describe, as there is a path to a trusted authority. For domain clients they may probably automatically trust the server as it is in the same domain.

The failure on OA has also changed - I am now now seeing an 'untrusted certificate error', just an issue with authentication. I will track that down and post the results.

Conclusions so far:  
Both OA and OWA should work with a INTERNALLY GENERATED certificate. OWA works with self-signed, OA doesn't.

The title of this article is wrong - it's not about using a self-signed certificate but an internal CA one - and it's a very comprehensive guide to that.



**Graham** November 20, 2012 at 3:45 am

Final Update: all working now. The authentication issue appears to have been down to switching to Kernel mode authentication for the various exchange processes at some point.

So to summarise - this detailed guide works for both OWA and OA by using an internal CA certificate, with the proviso that for non-domain member PCs you need to import the issuing server's CA certificate to the Trusted Root CA store, in addition to the Exchange certificate generated as described here.

Thanks Satheshwaran for creating this guide initially and for our exchange (pardon the pun!) regarding the differences between self-signed and internal CA generated certificates. I hope the clarification will be of value to all readers of this blog.

Regards,  
Graham



**Satheshwaran Manoharan** November 20, 2012 at 5:07 am

You are most welcome !!



**Satheshwaran Manoharan** November 15, 2012 at 4:19 pm

Hi Graham,  
Have Emailed you on this !  
Issued by Windows CA will work with Outlook anywhere  
But not a Self Sign Cert  
Thankyou !

Reply



**adatmentés** November 29, 2012 at 10:00 pm

Hi there, I found your web site via Google at the same time as searching for a related subject, your site came up, it looks great. I've bookmarked it in my google bookmarks.

Reply



**Mohammed** January 15, 2013 at 4:49 am

You are very helpfull. Keep doing the good work. It inspires the junior admis like me.

Reply



**Satheshwaran Manoharan** January 15, 2013 at 8:12 am

Sure I Will Mohammed. Thank you for your Comments

Reply



**adatmentés** January 28, 2013 at 1:18 pm

Asking questions are in fact good thing if you are not understanding something completely, except this article provides good understanding even.

Reply



**Satheshwaran Manoharan** January 28, 2013 at 6:10 pm

Thank Man !

Reply



**Jaison Joseph Samuel** January 29, 2013 at 8:40 pm

Hi Satheshwaran,  
Thank you for sharing the knowledge. I was looking for such informative articles. I am trying all sorts of tests to master the Exchange Server domain in my lab environment. Once again Thankx bro!

Reply



**Satheshwaran Manoharan** January 30, 2013 at 5:58 am

Thank you for your comments Jaison !  
You are always welcome !

Reply




**Gulab** February 1, 2013 at 1:22 pm


On step:3 You have domain mail.careexchange.in but the OWA url doesn't point to the same address. Rather then it's the FQDN of your exchange server, which is not correct.

You should be able to login to OWA using https://mail.careexchange.in/owa

Reply

 **Gulab** February 1, 2013 at 1:23 pm  
On step:3 You have domain mail.careexchange.in but the OWA url doesn't point to the same address. Rather then it's the FQDN of your exchange server, which is not correct.  
Aren't you able to login to https://mail.careexchange.in/owa or you just mentioning the server fqdn?  
You should be able to login to OWA using https://mail.careexchange.in/owa

[Reply](#)

 **Satheshwaran Manoharan** February 2, 2013 at 3:09 am  
Hi Gulab,  
I Understand. But the internal URL of my server is the FQDN of my Server. WHere the Cert has both the entries.  
So both should work right ?


[Reply](#)

 **checkwebsite** February 12, 2013 at 8:35 am  
This unique material you presents in this article is a top-notch and great matter. Captivating strategy and also structure in composition. Keep writing this kind of useful details.

[Reply](#)

 **Satheshwaran Manoharan** February 15, 2013 at 3:31 am  
Thank you !


[Reply](#)

 **yasir** February 21, 2013 at 7:29 am  
My cert is working on Server but I got an error on client PC.... i have also install to Personal,Trusted Root Certification Authorities,Intermediate Certification Authorities.....but still got an error with internet explorer 9. kindly guide me.

[Reply](#)

 **yasir** February 21, 2013 at 7:45 am  
Same the Issue facing like Graham..... email me


[Reply](#)

 **Satheshwaran Manoharan** February 22, 2013 at 10:30 am  
Use MMC and trying importing the Cert and let me know what happens


[Reply](#)

 **Terence AGius** March 5, 2013 at 6:14 am  
I have done these steps several times, yet now my exchange does not work anymore. Clients can't connect with web or outlook. So maybe article is helpful but in my case it set me back to the dark ages.


[Reply](#)

 **Satheshwaran Manoharan** March 5, 2013 at 6:18 am  
if you have had a Self Signed Cert already. After doing these steps. You have place the new cert in all your devices.  
That's the only situation where connected devices goes disconnected. and That's the disadvantage of a self signed Cert


[Reply](#)

 **Terence AGius** March 5, 2013 at 10:13 am  
Thanks for quick reply.  
But certificate does not even show on Exchange or in certificates. I confirmed that I do not have that thumbprint anywhere  
So how can I revert back..make a normal self signed certificate and leave things as they were

[Reply](#)

 **Satheshwaran Manoharan** March 6, 2013 at 1:45 am  
Go to an old client. Check what cert you had in the past. If you are using the same CA. Try using the same Cert. make sure its not expired

[Reply](#)

 **Vijay Amirtharaj** March 11, 2013 at 5:00 pm  
This is simply superb... I love this site 😊

[Reply](#)

 **Satheshwaran Manoharan** March 12, 2013 at 4:35 am  
Thank you for you comments vijay





