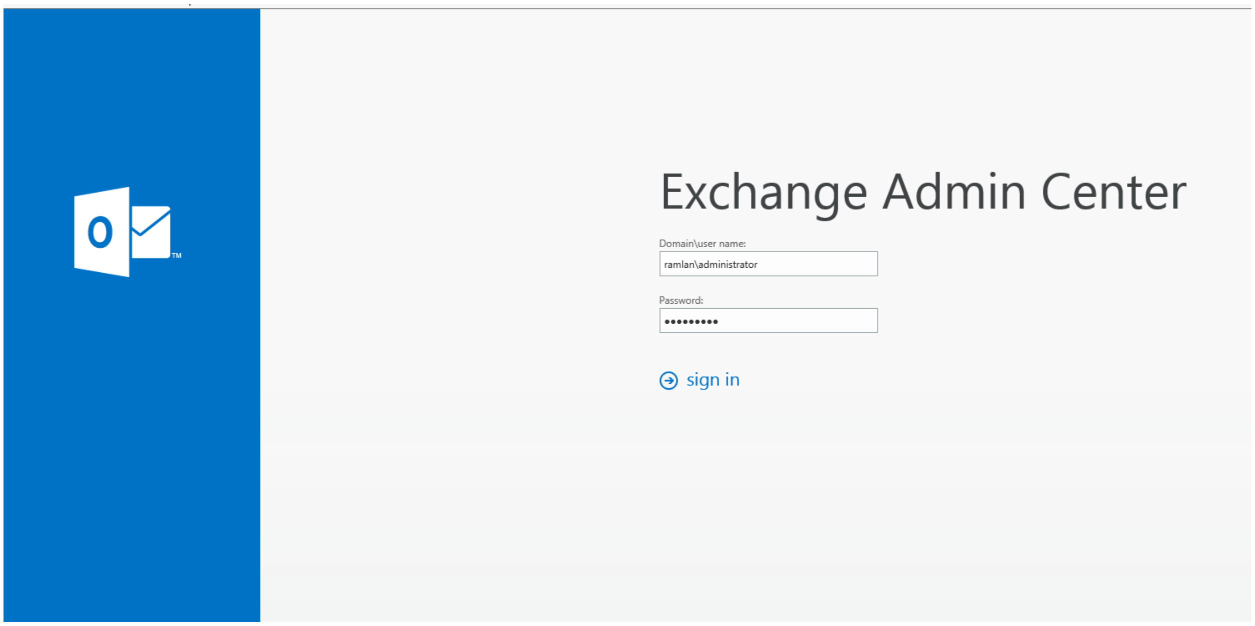
How to update the certificate on Exchange Server 2019

In this post, I will show you the steps involved to renew the certificate that is about to expire or expired on Exchange Server 2019.

This is my home lab that is running Exchange Server 2019. The SSL certificate is Comodo and is about to expire on 5th May 2019. So, I need to renew the certificate and will take screen shot of the whole process for anybody that needs to carryout at home lab or in production.

Open Exchange Administrative Center (ECP) web link and login to the server.

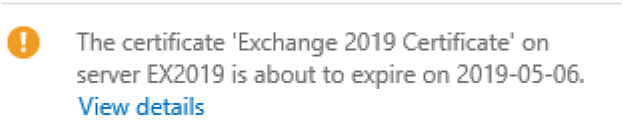


Exchange Admin Center

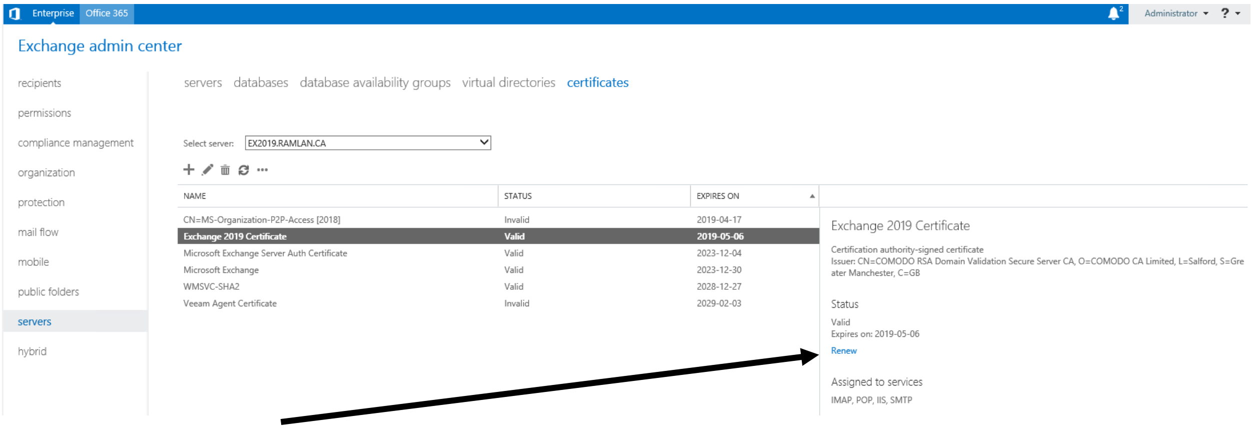
Domain\user name: ramlan\administrator

Password: •••••••••

See below message that pops up giving us a notification error that certificate is about to expire.



The certificate 'Exchange 2019 Certificate' on server EX2019 is about to expire on 2019-05-06.



Select server: EX2019.RAMLAN.CA

NAME	STATUS	EXPIRES ON
CN=MS-Organization-P2P-Access [2018]	Invalid	2019-04-17
Exchange 2019 Certificate	**Valid**	**2019-05-06**
Microsoft Exchange Server Auth Certificate	Valid	2023-12-04
Microsoft Exchange	Valid	2023-12-30
WMSVC-SHA2	Valid	2028-12-27
Veeam Agent Certificate	Invalid	2029-02-03

Exchange 2019 Certificate

Certification authority-signed certificate
Issuer: CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, S=Greater Manchester, C=GB

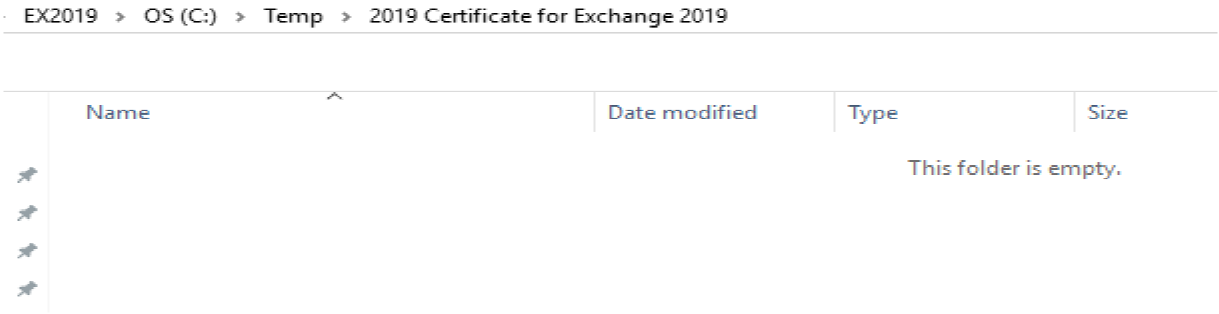
Status

Valid
Expires on: 2019-05-06

Assigned to services

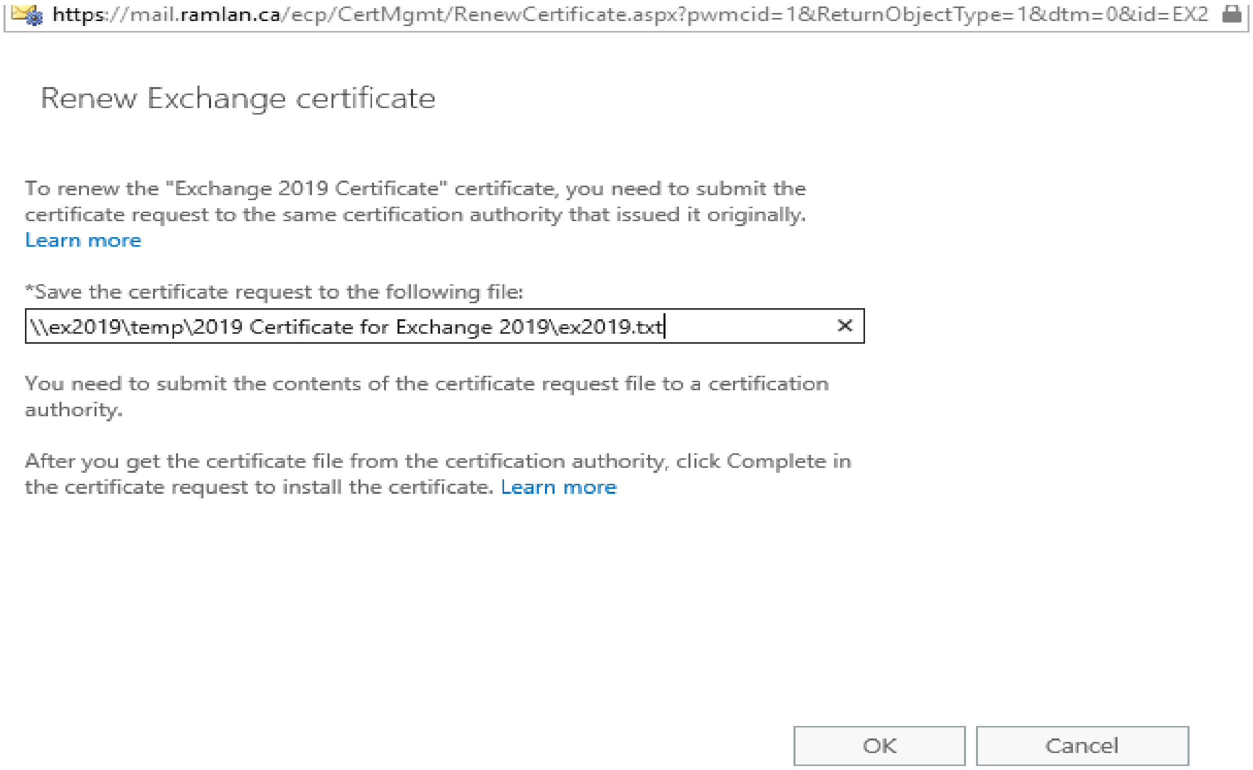
IMAP, POP, IIS, SMTP

I am going to save the certificate request here


EX2019 > OS (C:) > Temp > 2019 Certificate for Exchange 2019
Name
Date modified
Type
Size

This folder is empty.

Give certificate a name. I will call it as ex2019.txt


https://mail.ramlan.ca/ecp/CertMgmt/RenewCertificate.aspx?pwmcid=1&ReturnObjectType=1&dtm=0&id=EX2
OK
Cancel

Renew Exchange certificate

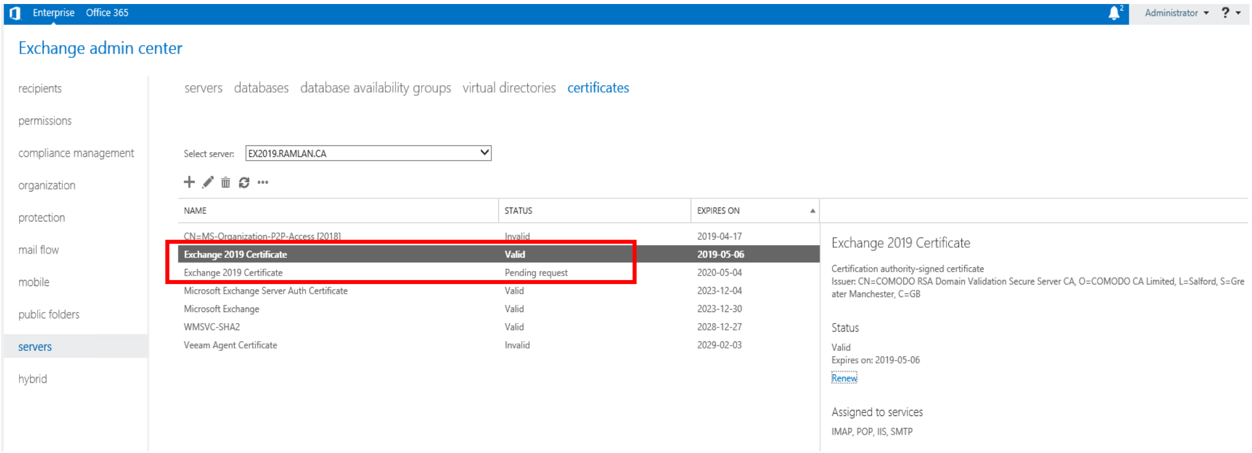
To renew the "Exchange 2019 Certificate" certificate, you need to submit the certificate request to the same certification authority that issued it originally. Learn more

*Save the certificate request to the following file:

\\ex2019\temp\2019 Certificate for Exchange 2019\ex2019.txt

You need to submit the contents of the certificate request file to a certification authority.

After you get the certificate file from the certification authority, click Complete in the certificate request to install the certificate. Learn more



Select server: EX2019.RAMLAN.CA

NAME	STATUS	EXPIRES ON
CN=MS-Organization-P2P-Access [2018]	Invalid	2019-04-17
Exchange 2019 Certificate	Valid	2019-05-06
Exchange 2019 Certificate	Pending request	2020-05-04
Microsoft Exchange Server Auth Certificate	Valid	2023-12-04
Microsoft Exchange	Valid	2023-12-30
WMSVC-SHA2	Valid	2028-12-27
Veeam Agent Certificate	Invalid	2029-02-03

Exchange 2019 Certificate

Certification authority-signed certificate
Issuer: CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, S=Greater Manchester, C=GB

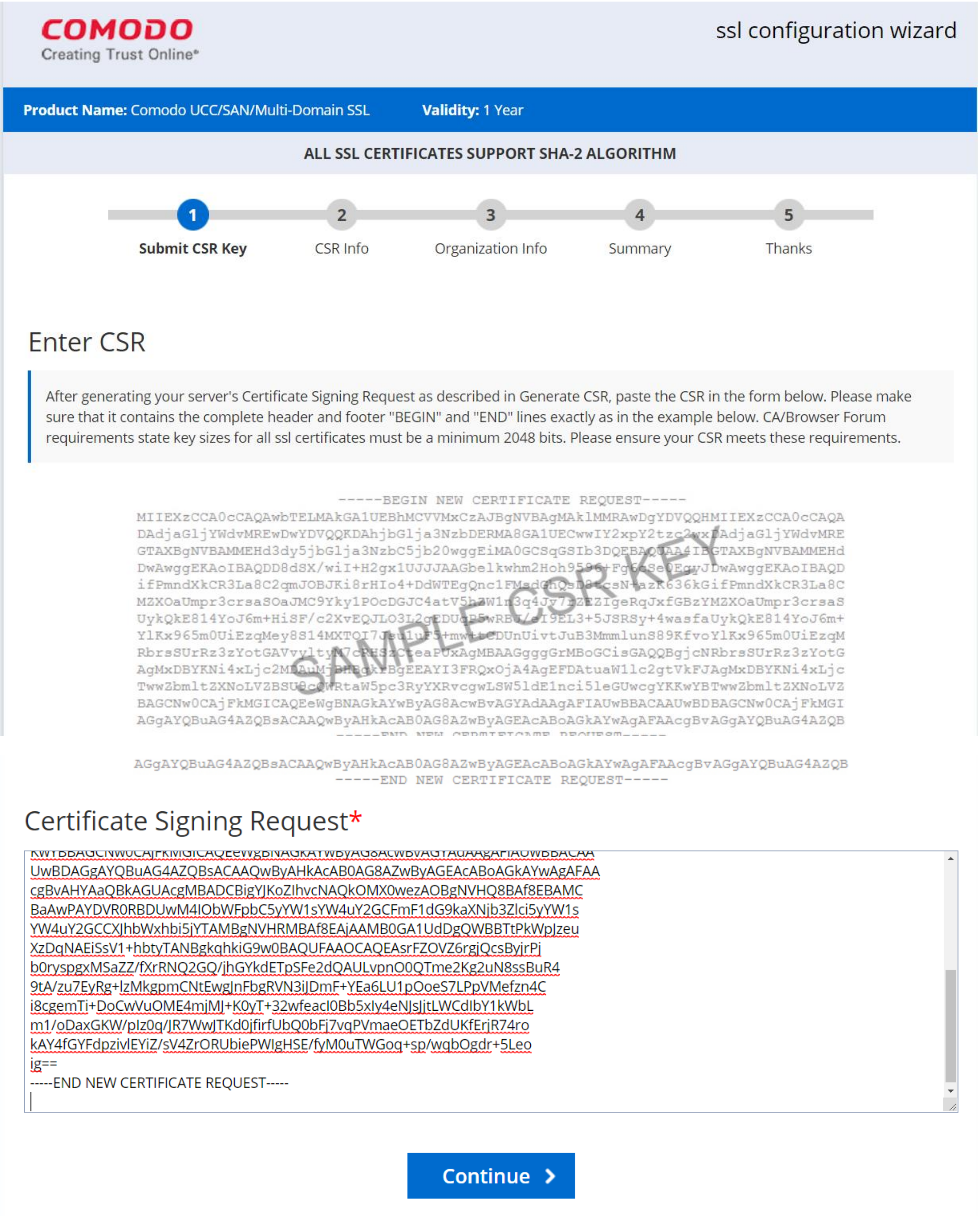
Status

Valid
Expires on: 2019-05-06
Renew

Assigned to services

IMAP, POP, IIS, SMTP

Now we have to take ex2019.txt file to SSL2BUY site to submit certificate request.



Product Name: Comodo UCC/SAN/Multi-Domain SSL **Validity:** 1 Year

ALL SSL CERTIFICATES SUPPORT SHA-2 ALGORITHM

Enter CSR

After generating your server's Certificate Signing Request as described in Generate CSR, paste the CSR in the form below. Please make sure that it contains the complete header and footer "BEGIN" and "END" lines exactly as in the example below. CA/Browser Forum requirements state key sizes for all ssl certificates must be a minimum 2048 bits. Please ensure your CSR meets these requirements.

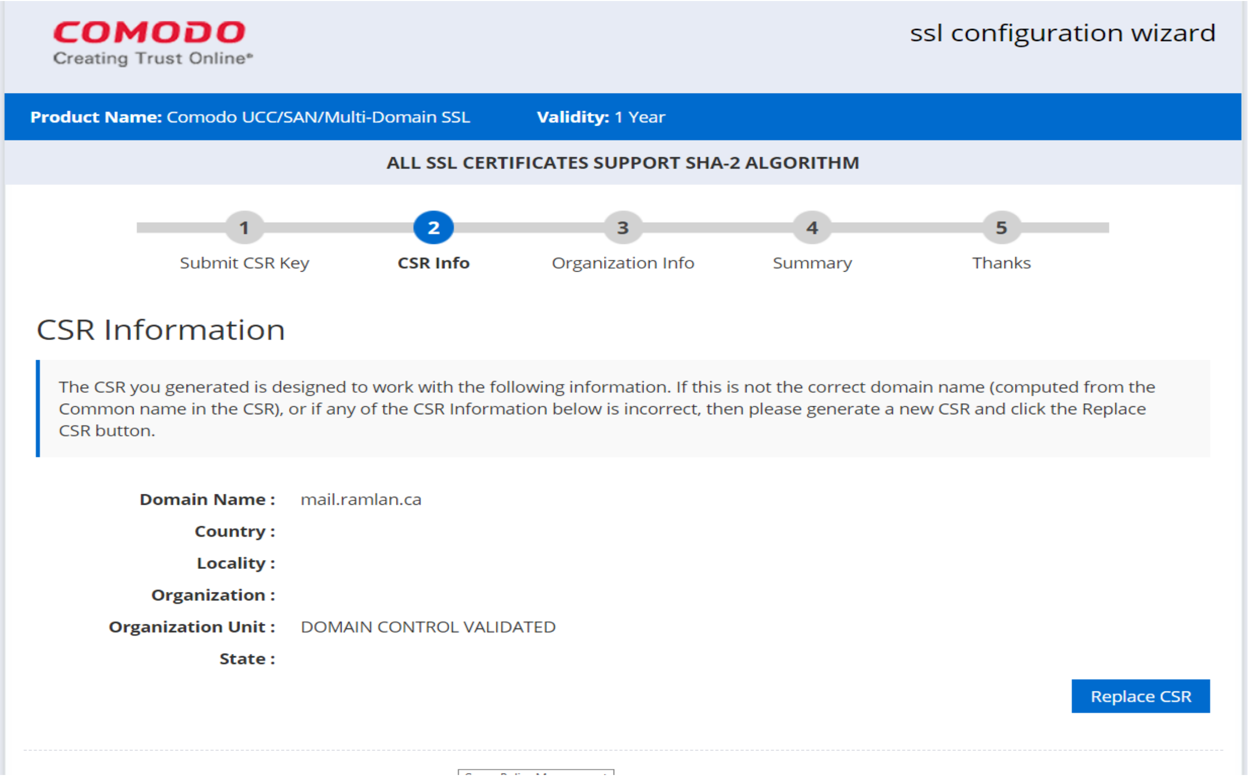
```
                  -----BEGIN NEW CERTIFICATE REQUEST-----
MIIEXzCCA0cCAQAwbTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAklMMRAwDgYDVQQHMIIEXzCCA0cCAQA
DAdjaGljYWdvMREwDwYDVQQKDAhjbGlja3NzbDERMA8GA1UECwwIY2xpY2tzc2wxDAdjaGljYWdvMRE
GTAXBgNVBAMMEHd3dy5jbGlja3NzbC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBGTAXBgNVBAMMEHd
DwAwggEKAoIBAQDD8dSX/wiI+H2gx1UJJJAAGbelkwhm2Hoh9596+Fg6cSe0EgyJDwAwggEKAoIBAQD
ifPmndXkCR3La8C2qmJOBJKi8rHIo4+DdWTEgQnc1FMsdGhQsD8tcsN+azK636kGifPmndXkCR3La8C
MZXOaUmpr3crsaSOaJMC9Yky1POcDGJC4atV5hZW1n3q4Jy7rZEZIgeRqJxfGBzYMZXOaUmpr3crsaS
UykQkE814YoJ6m+HiSF/c2XvEQJLO3L2gEDUqR5wRBU/eI9EL3+5JSRSy+4wasfaUykQkE814YoJ6m+
YlKx965m0UiEzqMey8S14MXTOI7Jsu1uF5+mw+tCDUnUivtJuB3MmmlunS89KfvoYlKx965m0UiEzqM
RbrsSUrRz3zYotGAVvyltyM7cRHSzCteaP0xAgMBAAGgggGrMBoGCisGAQQBgjcNRbrsSUrRz3zYotG
AgMxDBYKNi4xLjc2MDAuMjBHBgkrBgEEAYI3FRQxOjA4AgEFDAtuaW1lc2gtVkFJAgMxDBYKNi4xLjc
TwwZbmltZXNoLVZBSU8cQWRtaW5pc3RyYXRvcgwLSW5ldE1nci5leGUwcgYKKwYBTwwZbmltZXNoLVZ
BAGCNw0CAjFkMGICAQEeWgBNAGkAYwByAG8AcwBvAGYAdAAgAFIAUwBBACAAUwBDBAGCNw0CAjFkMGI
AGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAGgAYQBuAG4AZQB
```

AGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAGgAYQBuAG4AZQB

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

Certificate Signing Request*

```
KWYBBAGCNw0CAjFkMGICAQEeWgBNAGkAYwByAG8AcwBvAGYAdAAgAFIAUwBBACAA
UwBDAGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFAA
cgBvAHYAaQBkAGUAcgMBADCBigYJKoZIhvcNAQkOMX0wezAOBgNVHQ8BAf8EBAMC
BaAwPAYDVR0RBDUwM4IObWFpbC5yYW1sYW4uY2GCFmF1dG9kaXNjb3Zlci5yYW1s
YW4uY2GCCXJhbWxhbi5jYTAMBgNVHRMBAf8EAjAAMB0GA1UdDgQWBBTtPkWpJzeu
XzDqNAEiSsV1+hbtyTANBgkqhkiG9w0BAQUFAAOCAQEAsrFZOVZ6rgjQcsByjrPj
b0ryspgxMSaZZ/fXrRNQ2GQ/jhGYkdETpSFe2dQAULvpnO0QTme2Kg2uN8ssBuR4
9tA/zu7EyRg+lzMkgpmCNtEwgJnFbgRVN3iJDmF+YEa6LU1pOoeS7LPpVMefzn4C
i8cgemTi+DoCwVuOME4mjMJ+K0yT+32wfeacl0Bb5xly4eNJsJjtLWCdlbY1kWbL
m1/oDaxGKW/plz0q/JR7WwJTKd0jfirfUbQ0bFj7vqPVmaeOETbZdUKfErjR74ro
kAY4fGYFdpzivlEYiZ/sV4ZrORUbiePWlgHSE/fyM0uTWGoq+sp/wqbOgdr+5Leo
ig==
-----END NEW CERTIFICATE REQUEST-----
```



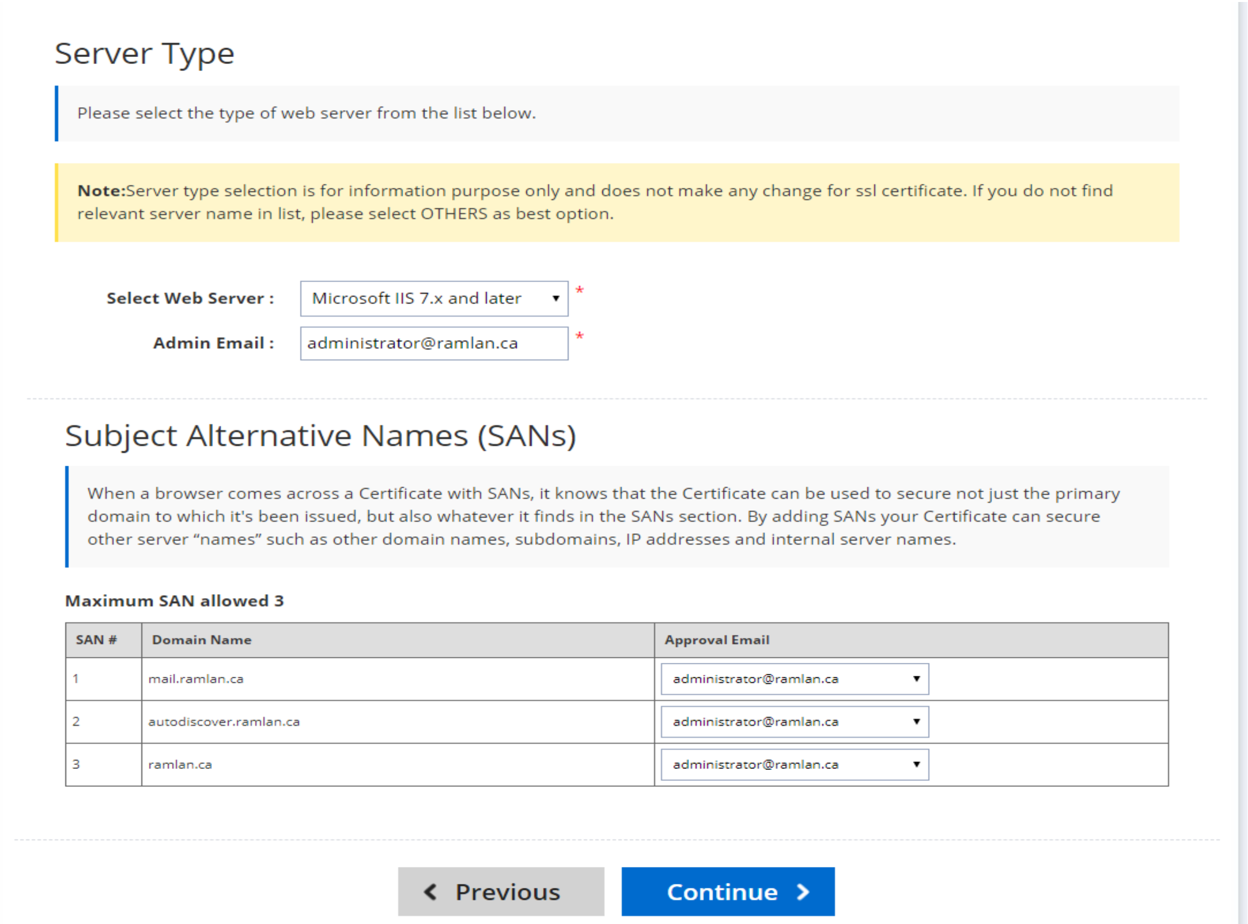
Product Name: Comodo UCC/SAN/Multi-Domain SSL **Validity:** 1 Year

ALL SSL CERTIFICATES SUPPORT SHA-2 ALGORITHM

CSR Information

The CSR you generated is designed to work with the following information. If this is not the correct domain name (computed from the Common name in the CSR), or if any of the CSR Information below is incorrect, then please generate a new CSR and click the Replace CSR button.

Domain Name :	mail.ramlan.ca
Country :	
Locality :	
Organization :	
Organization Unit :	DOMAIN CONTROL VALIDATED
State :	



Server Type

Please select the type of web server from the list below.

Note: Server type selection is for information purpose only and does not make any change for ssl certificate. If you do not find relevant server name in list, please select OTHERS as best option.

Select Web Server : Microsoft IIS 7.x and later ▾ *

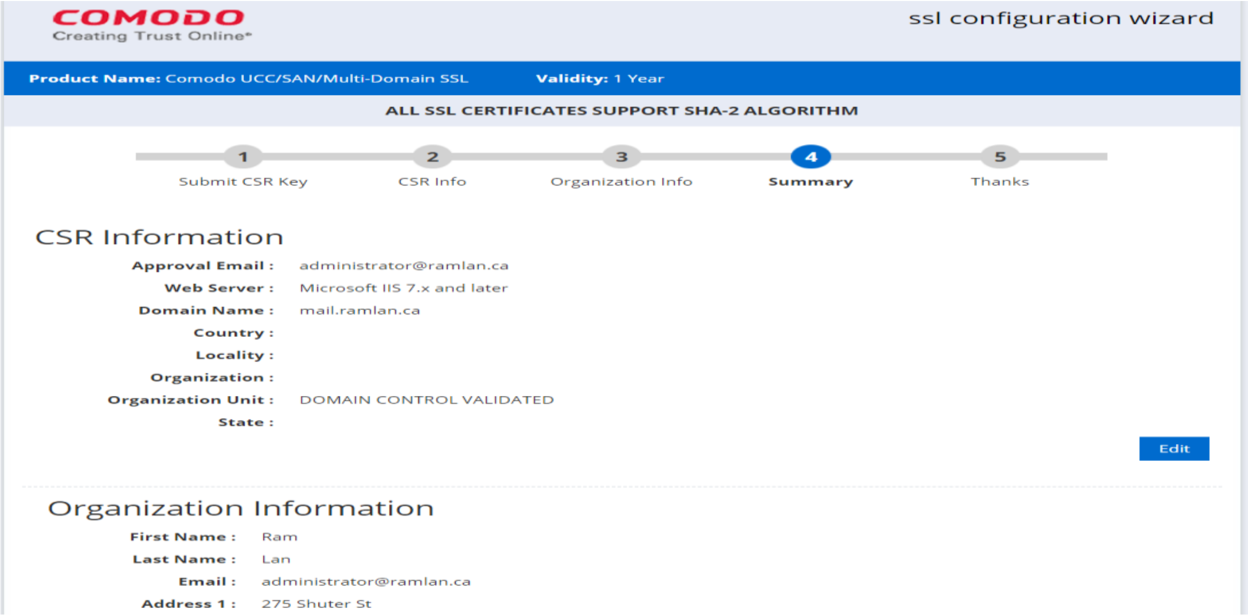
Admin Email : administrator@ramlan.ca *

Subject Alternative Names (SANs)

When a browser comes across a Certificate with SANs, it knows that the Certificate can be used to secure not just the primary domain to which it's been issued, but also whatever it finds in the SANs section. By adding SANs your Certificate can secure other server "names" such as other domain names, subdomains, IP addresses and internal server names.

Maximum SAN allowed 3

SAN #	Domain Name	Approval Email
1	mail.ramlan.ca	administrator@ramlan.ca ▾
2	autodiscover.ramlan.ca	administrator@ramlan.ca ▾
3	ramlan.ca	administrator@ramlan.ca ▾



Product Name: Comodo UCC/SAN/Multi-Domain SSL **Validity:** 1 Year

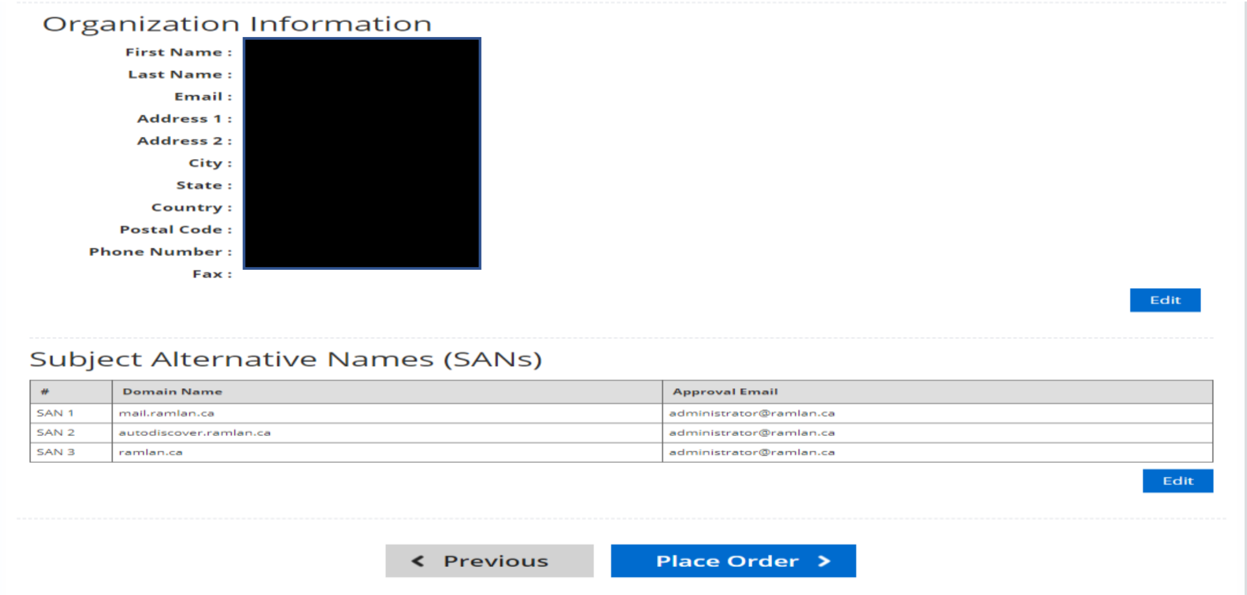
ALL SSL CERTIFICATES SUPPORT SHA-2 ALGORITHM

CSR Information

Approval Email :	administrator@ramlan.ca
Web Server :	Microsoft IIS 7.x and later
Domain Name :	mail.ramlan.ca
Country :	
Locality :	
Organization :	
Organization Unit :	DOMAIN CONTROL VALIDATED
State :	

Organization Information

First Name :	Ram
Last Name :	Lan
Email :	administrator@ramlan.ca
Address 1 :	275 Shuter St



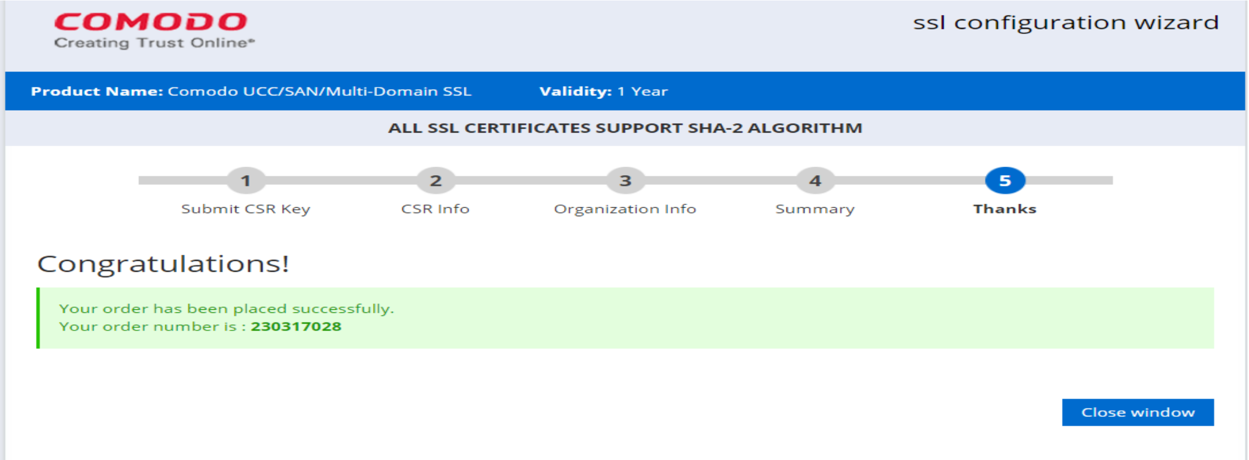
Organization Information

First Name :
Last Name :
Email :
Address 1 :
Address 2 :
City :
State :
Country :
Postal Code :
Phone Number :
Fax :

[redacted]

Subject Alternative Names (SANs)

#	Domain Name	Approval Email
SAN 1	mail.ramlan.ca	administrator@ramlan.ca
SAN 2	autodiscover.ramlan.ca	administrator@ramlan.ca
SAN 3	ramlan.ca	administrator@ramlan.ca



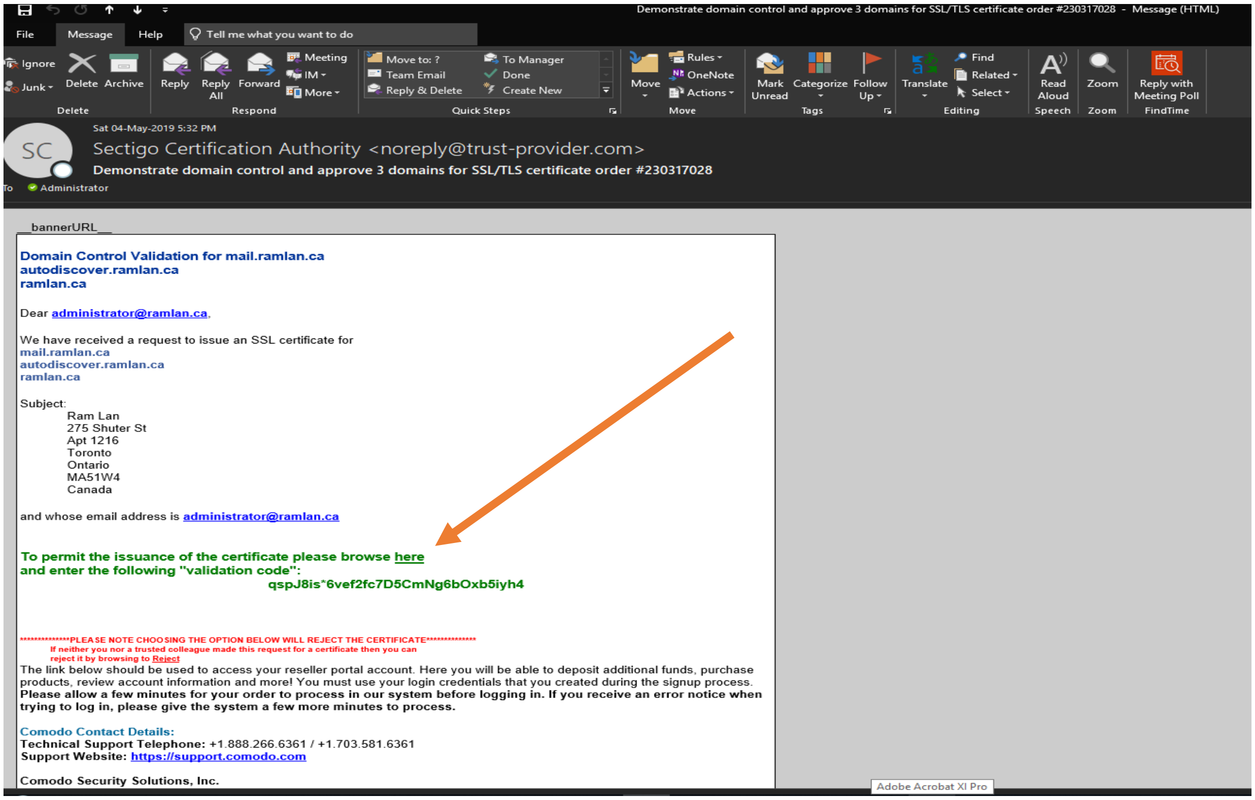
Product Name: Comodo UCC/SAN/Multi-Domain SSL **Validity:** 1 Year

ALL SSL CERTIFICATES SUPPORT SHA-2 ALGORITHM

Congratulations!

Your order has been placed successfully.
Your order number is : **230317028**

As soon as you press Place Order – You will get email from Comodo to validate the request.



Sat 04-May-2019 5:32 PM

Sectigo Certification Authority <noreply@trust-provider.com>

Demonstrate domain control and approve 3 domains for SSL/TLS certificate order #230317028

Domain Control Validation for mail.ramlan.ca
autodiscover.ramlan.ca
ramlan.ca

Dear administrator@ramlan.ca,

We have received a request to issue an SSL certificate for
mail.ramlan.ca
autodiscover.ramlan.ca
ramlan.ca

Subject:
Ram Lan
275 Shuter St
Apt 1216
Toronto
Ontario
MA51W4
Canada

and whose email address is administrator@ramlan.ca

To permit the issuance of the certificate please browse here
and enter the following "validation code":
qspJ8is*6vef2fc7D5CmNg6bOxb5iyh4

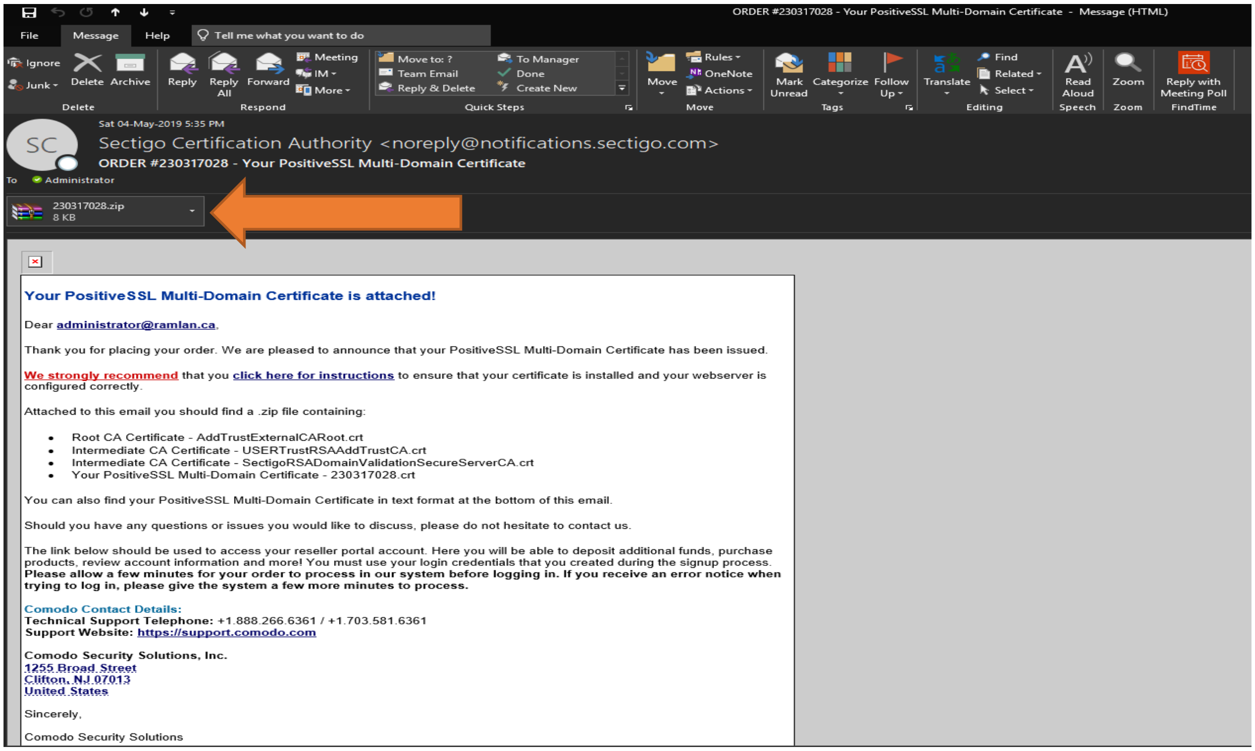
**************PLEASE NOTE CHOOSING THE OPTION BELOW WILL REJECT THE CERTIFICATE*************
If neither you nor a trusted colleague made this request for a certificate then you can
reject it by browsing to Reject

The link below should be used to access your reseller portal account. Here you will be able to deposit additional funds, purchase products, review account information and more! You must use your login credentials that you created during the signup process. **Please allow a few minutes for your order to process in our system before logging in. If you receive an error notice when trying to log in, please give the system a few more minutes to process.**

Comodo Contact Details:
Technical Support Telephone: +1.888.266.6361 / +1.703.581.6361
Support Website: https://support.comodo.com

Comodo Security Solutions, Inc.

After validation you will get email with certificate attachment.



Sat 04-May-2019 5:35 PM

Sectigo Certification Authority <noreply@notifications.sectigo.com>

ORDER #230317028 - Your PositiveSSL Multi-Domain Certificate

Your PositiveSSL Multi-Domain Certificate is attached!

Dear **administrator@ramlan.ca**,

Thank you for placing your order. We are pleased to announce that your PositiveSSL Multi-Domain Certificate has been issued.

We strongly recommend that you **click here for instructions** to ensure that your certificate is installed and your webserver is configured correctly.

Attached to this email you should find a .zip file containing:

- Root CA Certificate - AddTrustExternalCARoot.crt
- Intermediate CA Certificate - USERTrustRSAAddTrustCA.crt
- Intermediate CA Certificate - SectigoRSADomainValidationSecureServerCA.crt
- Your PositiveSSL Multi-Domain Certificate - 230317028.crt

You can also find your PositiveSSL Multi-Domain Certificate in text format at the bottom of this email.

Should you have any questions or issues you would like to discuss, please do not hesitate to contact us.

The link below should be used to access your reseller portal account. Here you will be able to deposit additional funds, purchase products, review account information and more! You must use your login credentials that you created during the signup process. **Please allow a few minutes for your order to process in our system before logging in. If you receive an error notice when trying to log in, please give the system a few more minutes to process.**

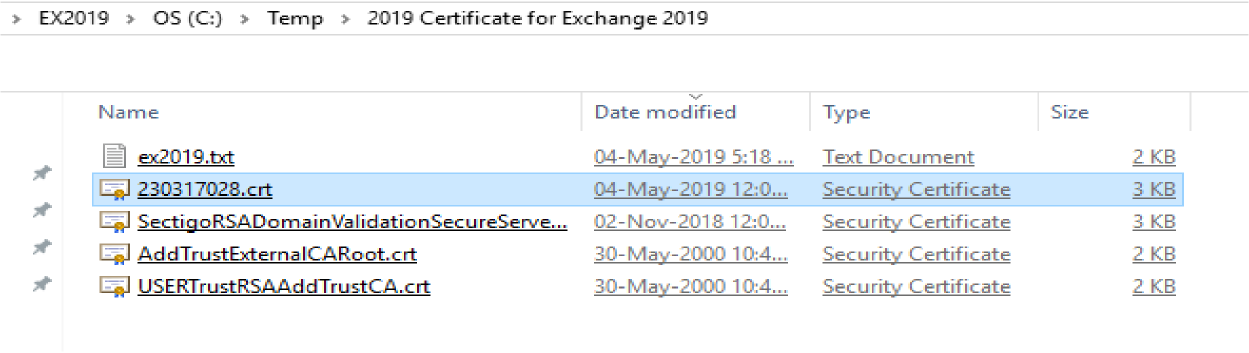
Comodo Contact Details:
Technical Support Telephone: +1.888.266.6361 / +1.703.581.6361
Support Website: https://support.comodo.com

Comodo Security Solutions, Inc.
1255 Broad Street
Clifton, NJ 07013
United States

Sincerely,

Comodo Security Solutions

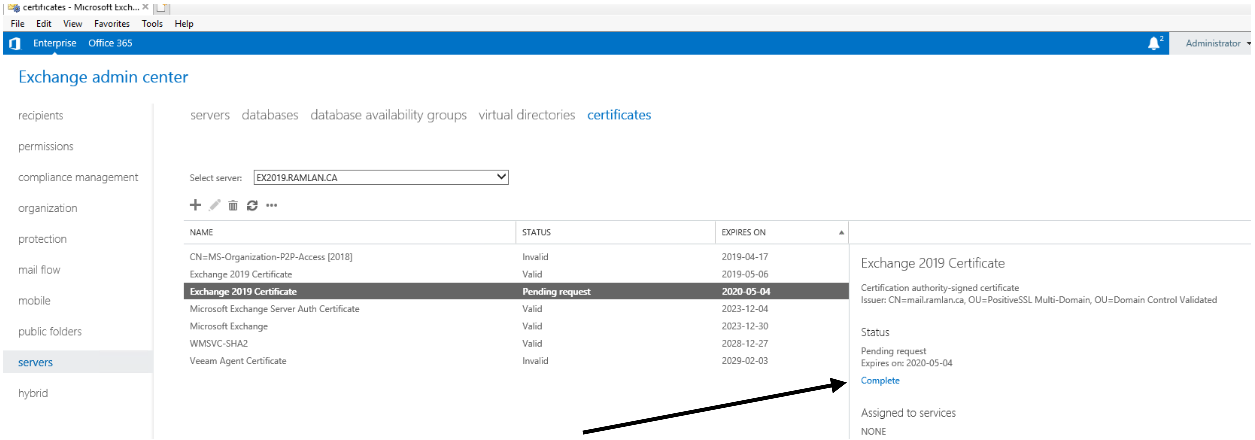
Save the file and extract the certificate. Copy the file to exchange server.



EX2019 > OS (C:) > Temp > 2019 Certificate for Exchange 2019

Name	Date modified	Type	Size
ex2019.txt	04-May-2019 5:18 ...	Text Document	2 KB
230317028.crt	04-May-2019 12:0...	Security Certificate	3 KB
SectigoRSADomainValidationSecureServe...	02-Nov-2018 12:0...	Security Certificate	3 KB
AddTrustExternalCARoot.crt	30-May-2000 10:4...	Security Certificate	2 KB
USERTrustRSAAddTrustCA.crt	30-May-2000 10:4...	Security Certificate	2 KB

Now click to complete pending certificate



Select server: EX2019.RAMLAN.CA

NAME	STATUS	EXPIRES ON
CN=MS-Organization-P2P-Access [2018]	Invalid	2019-04-17
Exchange 2019 Certificate	Valid	2019-05-06
Exchange 2019 Certificate	**Pending request**	**2020-05-04**
Microsoft Exchange Server Auth Certificate	Valid	2023-12-04
Microsoft Exchange	Valid	2023-12-30
WMSVC-SHA2	Valid	2028-12-27
Veeam Agent Certificate	Invalid	2029-02-03

Exchange 2019 Certificate

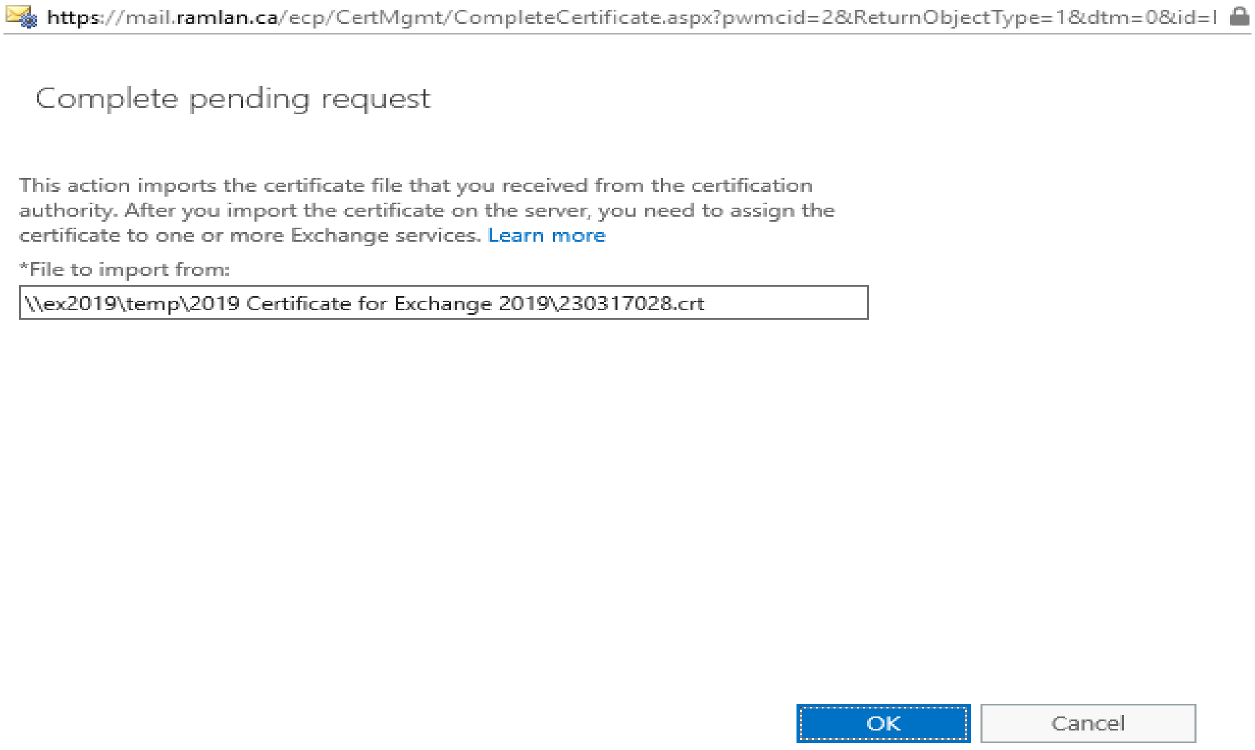
Certification authority-signed certificate
Issuer: CN=mail.ramlan.ca, OU=PositiveSSL Multi-Domain, OU=Domain Control Validated

Status

Pending request
Expires on: 2020-05-04
Complete

Assigned to services

NONE



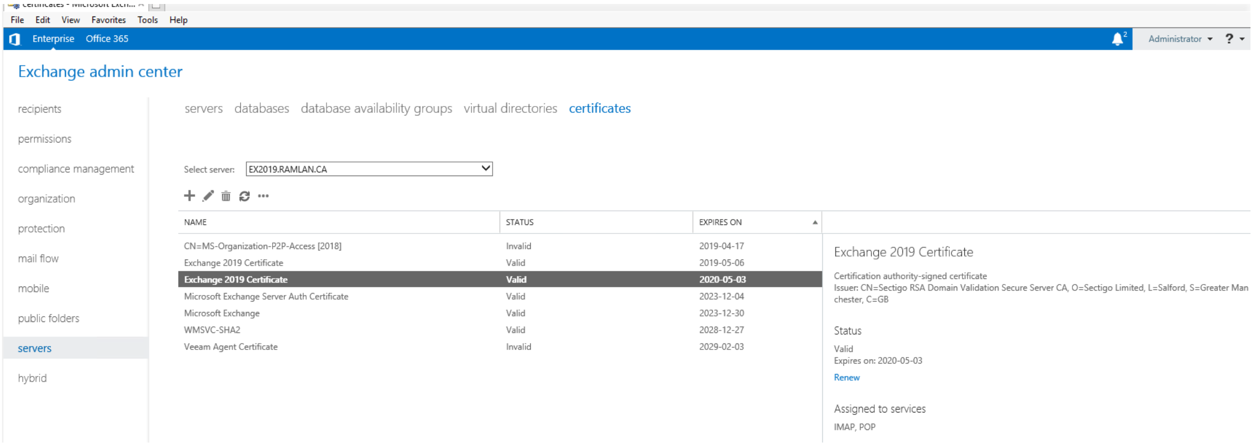
https://mail.ramlan.ca/ecp/CertMgmt/CompleteCertificate.aspx?pwmcid=2&ReturnObjectType=1&dtm=0&id=I

Complete pending request

This action imports the certificate file that you received from the certification authority. After you import the certificate on the server, you need to assign the certificate to one or more Exchange services. Learn more

*File to import from:

\\ex2019\temp\2019 Certificate for Exchange 2019\230317028.crt



Select server: EX2019.RAMLAN.CA

NAME	STATUS	EXPIRES ON
CN=MS-Organization-P2P-Access [2018]	Invalid	2019-04-17
Exchange 2019 Certificate	Valid	2019-05-06
Exchange 2019 Certificate	**Valid**	**2020-05-03**
Microsoft Exchange Server Auth Certificate	Valid	2023-12-04
Microsoft Exchange	Valid	2023-12-30
WMSVC-SHA2	Valid	2028-12-27
Veeam Agent Certificate	Invalid	2029-02-03

Exchange 2019 Certificate

Certification authority-signed certificate
Issuer: CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB

Status

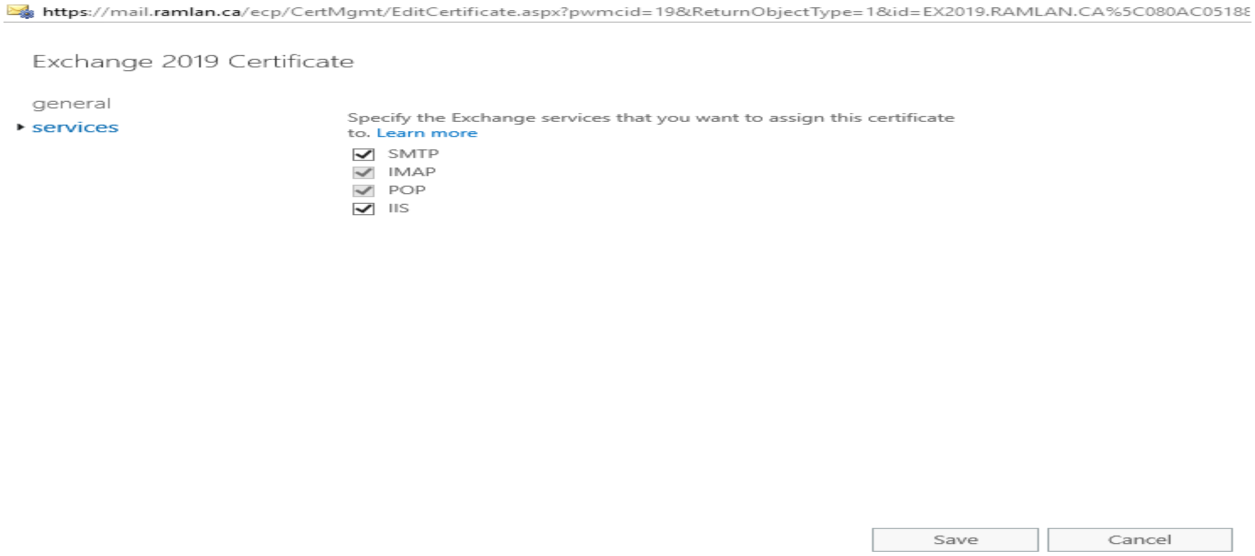
Valid
Expires on: 2020-05-03

Renew

Assigned to services

IMAP, POP

Now we have to assign the services. Click the Pencil button

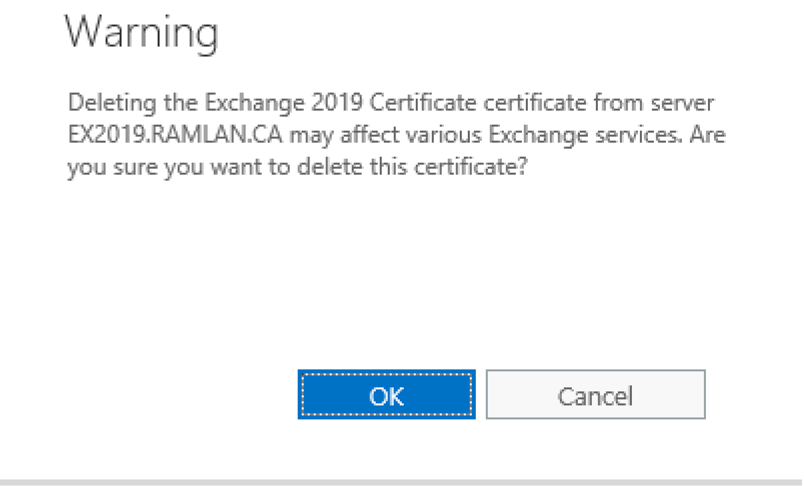

https://mail.ramlan.ca/ecp/CertMgmt/EditCertificate.aspx?pwmcid=19&ReturnObjectType=1&id=EX2019.RAMLAN.CA%5C080AC0518

Exchange 2019 Certificate

Specify the Exchange services that you want to assign this certificate to. Learn more

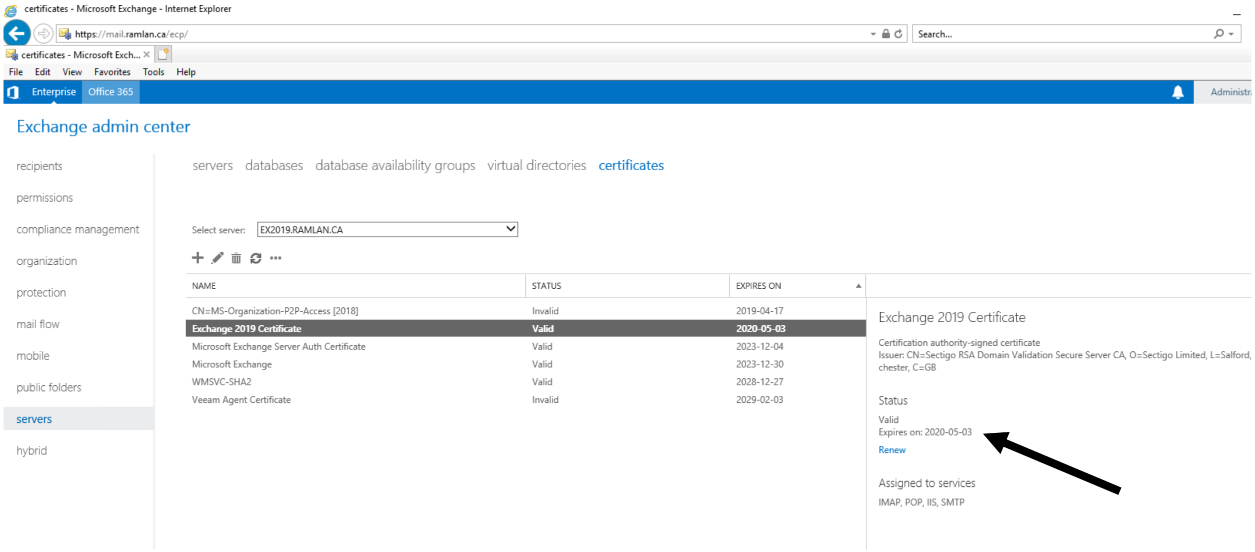
☑ SMTP
☑ IMAP
☑ POP
☑ IIS

Now we can delete the expiring certificate. Select the certificate and press delete button


Warning

Deleting the Exchange 2019 Certificate certificate from server EX2019.RAMLAN.CA may affect various Exchange services. Are you sure you want to delete this certificate?

Now we have one certificate that is valid till May 2020.


certificates - Microsoft Exchange - Internet Explorer
https://mail.ramlan.ca/ecp/
Search...
certificates - Microsoft Exch...
File Edit View Favorites Tools Help
Enterprise Office 365
Administr
Exchange admin center
recipients
permissions
compliance management
organization
protection
mail flow
mobile
public folders
servers
hybrid
servers databases database availability groups virtual directories certificates

Select server: EX2019.RAMLAN.CA

NAME	STATUS	EXPIRES ON
CN=MS-Organization-P2P-Access [2018]	Invalid	2019-04-17
Exchange 2019 Certificate	Valid	2020-05-03
Microsoft Exchange Server Auth Certificate	Valid	2023-12-04
Microsoft Exchange	Valid	2023-12-30
WMSVC-SHA2	Valid	2028-12-27
Veeam Agent Certificate	Invalid	2029-02-03

Exchange 2019 Certificate

Certification authority-signed certificate
Issuer: CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, chester, C=GB

Status

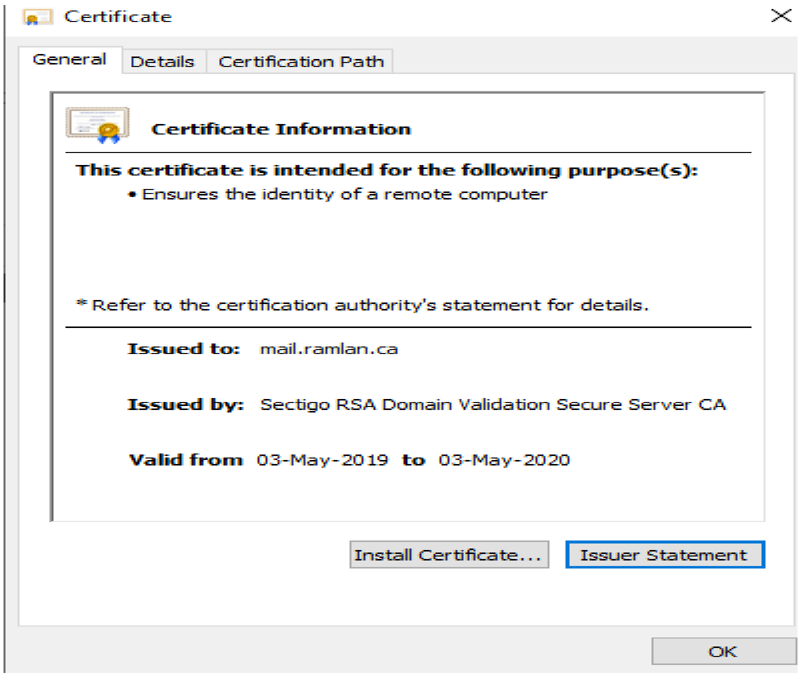
Valid
Expires on: 2020-05-03

Renew

Assigned to services

IMAP, POP, IIS, SMTP

Now login to ECP and check Padlock button – Check certificate details.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: mail.ramlan.ca

Issued by: Sectigo RSA Domain Validation Secure Server CA

Valid from 03-May-2019 to 03-May-2020

Now open Outlook 2019 to make sure users don't get any error message. So far so good for me. No errors and the renewal went without any issue.

Thanks

Ram Lan
04th May 2019