

How to install Let's Encrypt for Exchange Server 2019

In this post, I will show you how to complete Let's Encrypt SSL Certificate for Exchange Server 2019. As of now, I have a valid SSL Certificate from SSL2BUY 3rd Party. This certificate is going to expire on 3rd May 2020. So, I am going to try Let's Encrypt SSL Certificate which is **FREE** and is valid for 90 days with auto renewal through Windows Scheduler.

servers databases database availability groups virtual directories certificates


Select server: EX2019.RAMLAN.CA

+ - ✖ 🔄 ...

NAME	STATUS	EXPIRES ON	
CN=MS-Organization-P2P-Access [2018]	Invalid	2019-10-14	
CN=MS-Organization-P2P-Access [2019]	Invalid	2020-04-22	
Exchange 2019 Certificate	Valid	2020-05-03	Exchange 2019 Certificate
Microsoft Exchange Server Auth Certificate	Valid	2023-12-04	Certification authority-signed certificate Issuer: CN=Sectigo RSA Domain Validation Secure Server CA, chester, C=GB
Microsoft Exchange	Valid	2023-12-30	
WMSVC-SHA2	Valid	2028-12-27	
Veeam Agent Certificate	Invalid	2029-02-03	

Status
Valid
Expires on: 2020-05-03
[Renew](#)

Assigned to services
IMAP, POP, IIS, SMTP



I will be requesting Let's Encrypt certificate for these domains.

- Mail.ramlan.ca
- Ramlan.ca
- Autodiscover.ramlan.ca

This certificate will be assigned for these services

- IIS
- SMTP
- POP
- IMAP

I have already configured Exchange Server 2019 with Virtual directories. If you need help check this link <https://practical365.com/exchange-server/powershell-script-configure-exchange-urls/>


servers databases database availability groups virtual directories certificates

Select server: All servers

Select type: All

🔍 🗑 🔄

NAME	SERVER	TYPE	VERSION	LAST MODIFIED TIME	
Autodiscover (Default Web Site)	EX2019	Autodiscover	Version 15.2 (Build 595.3)	2018-12-31 12:09 AM	
ecp (Default Web Site)	EX2019	ECP	Version 15.2 (Build 595.3)	2018-12-31 9:42 AM	
EWS (Default Web Site)	EX2019	EWS	Version 15.2 (Build 595.3)	2018-12-31 9:42 AM	
mapi (Default Web Site)	EX2019	Mapi	Version 15.2 (Build 595.3)	2018-12-31 9:42 AM	
Microsoft-Server-ActiveSync (Default Web Site)	EX2019	EAS	Version 15.2 (Build 595.3)	2018-12-31 9:42 AM	
OAB (Default Web Site)	EX2019	OAB	Version 15.2 (Build 595.3)	2018-12-31 9:42 AM	
owa (Default Web Site)	EX2019	OWA	Version 15.2 (Build 595.3)	2018-12-31 9:42 AM	owa (Default Web Site)
PowerShell (Default Web Site)	EX2019	PowerShell	Version 15.2 (Build 595.3)	2018-12-31 12:10 AM	Website: Default Web Site Authentication: Basic, FBA Outlook Web App version: Exchange2013 External URL: https://mail.ramlan.ca/owa



The virtual directory is pointing to **MAIL.RAMLAN.CA**

Other Requirements for Let's Encrypt:

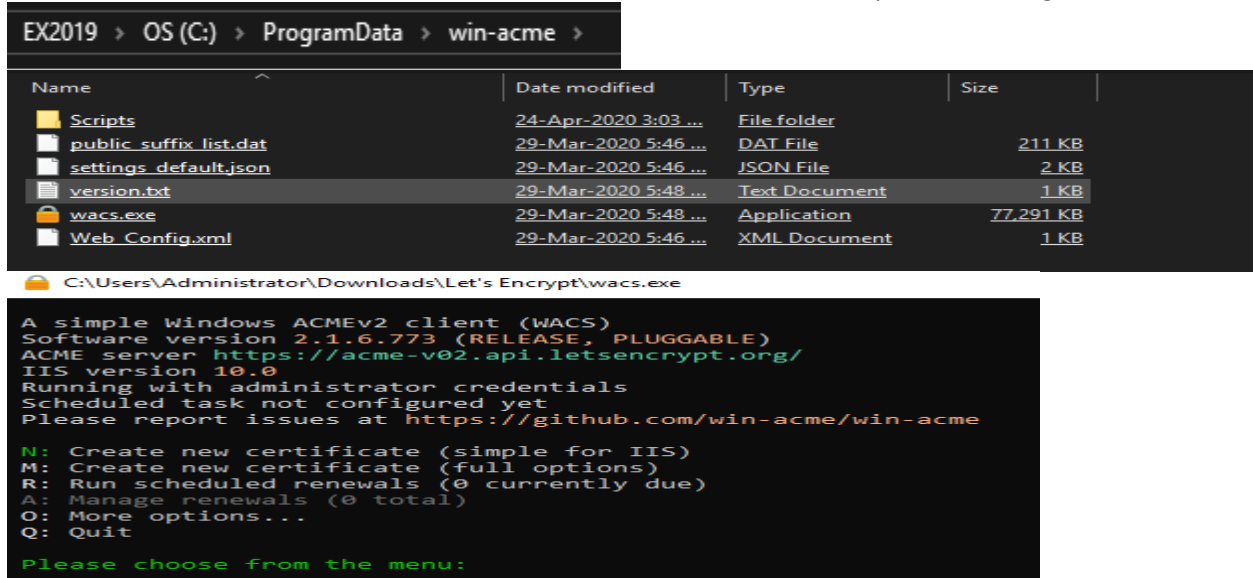
1. Download ACME v2 from below link

I was able to download Let's Encrypt ACME file from here. The version, I am using is v2.1.6.773

<https://www.win-acme.com/>



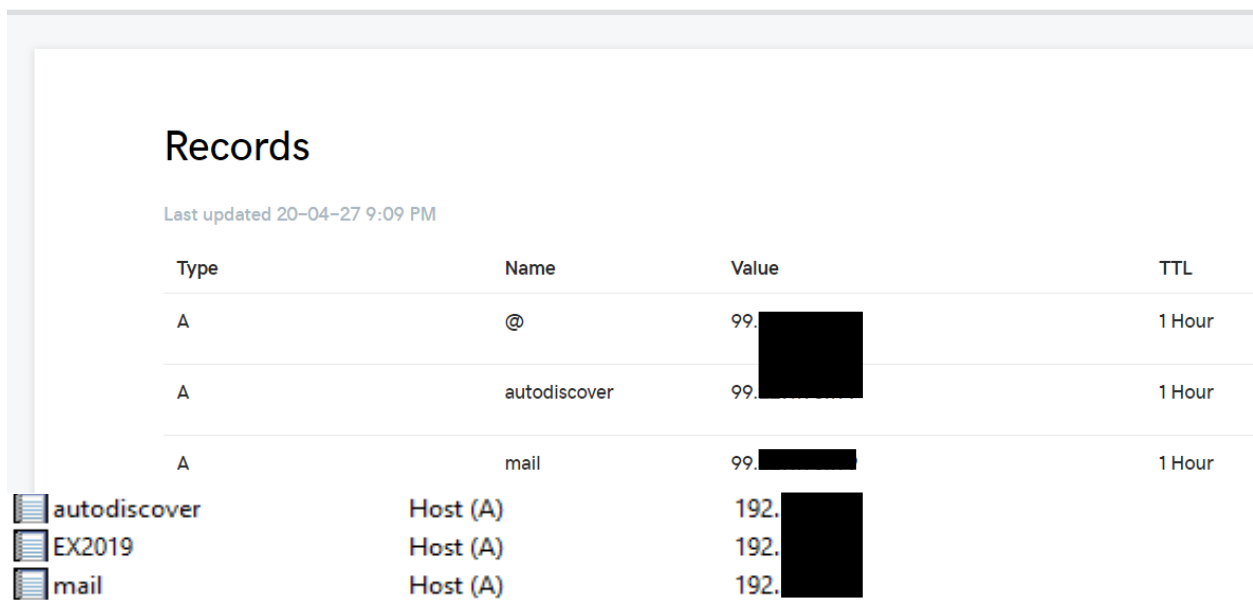
Extract files and copy to Exchange Server to the root (C:\) and keep extra copy of the files in Downloads folder as well. After that run wacs.exe as Admin so it will create necessary folder in ProgramData.



2. DNS Entry – External / Internal

DNS Management

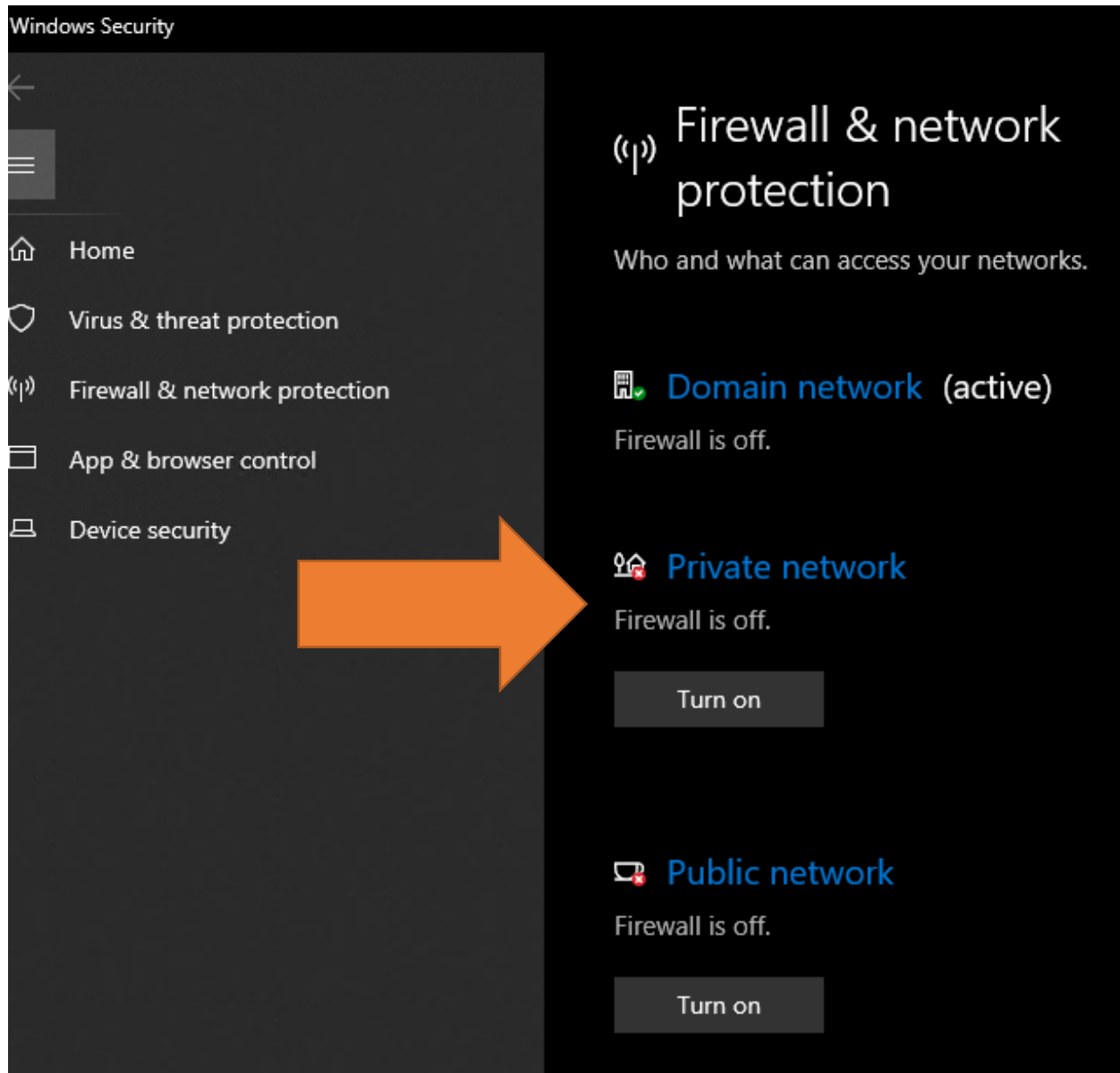
ramlan.ca



3. Port Forwarding

External			Internal				
Start Port	End Port		IP Address	Start Port	End Port	Protocol	Enable
25	to	25	192. [REDACTED]	25	to 25	Both ▼	<input checked="" type="checkbox"/>
2525	to	2525	192. [REDACTED]	2525	to 2525	Both ▼	<input checked="" type="checkbox"/>
443	to	443	192. [REDACTED]	443	to 443	Both ▼	<input checked="" type="checkbox"/>
80	to	80	192. [REDACTED]	80	to 80	Both ▼	<input checked="" type="checkbox"/>

4. Firewall



Now let us start the process. Run wacs.exe as Admin

EX2019 > Downloads > Let's Encrypt >				
Name	Date modified	Type	Size	
Scripts	27-Apr-2020 2:52 ...	File folder		
public_suffix_list.dat	29-Mar-2020 5:46 ...	DAT File	211 KB	
settings.json	29-Mar-2020 5:46 ...	JSON File	2 KB	
settings_default.json	29-Mar-2020 5:46 ...	JSON File	2 KB	
version.txt	29-Mar-2020 5:48 ...	Text Document	1 KB	
wacs.exe	29-Mar-2020 5:48 ...	Application	77,291 KB	
Web_Config.xml	29-Mar-2020 5:46 ...	XML Document	1 KB	

C:\Users\Administrator.RAMLAN\Downloads\Let's Encrypt\wacs.exe

```
A simple Windows ACMEv2 client (WACS)
Software version 2.1.6.773 (RELEASE, PLUGGABLE)
ACME server https://acme-v02.api.letsencrypt.org/
IIS version 10.0
Running with administrator credentials
Scheduled task not configured yet
Please report issues at https://github.com/win-acme/win-acme
```

```
N: Create new certificate (simple for IIS)
M: Create new certificate (full options)
R: Run scheduled renewals (0 currently due)
A: Manage renewals (0 total)
O: More options...
Q: Quit
```

Please choose from the menu: m

Running in mode: Interactive, Advanced

Please specify how the list of domain names that will be included in the certificate should be determined. If you choose for one of the "all bindings" options, the list will automatically be updated for future renewals to reflect the bindings at that time.

```
1: IIS
2: Manual input
3: CSR created by another program
C: Abort
```

How shall we determine the domain(s) to include in the certificate?: 2

Type mail.ramlan.ca,ramlan.ca,autodiscover.ramlan.ca and press enter

```
Enter comma-separated list of host names, starting with the common name: mail.ramlan.ca,ramlan.ca,autodiscover.ramlan.c
a
```

Target generated using plugin Manual: mail.ramlan.ca and 2 alternatives

Suggested friendly name '[Manual] mail.ramlan.ca', press <ENTER> to accept or type an alternative: <Enter>

The ACME server will need to verify that you are the owner of the domain names that you are requesting the certificate for. This happens both during initial setup *and* for every future renewal. There are two main methods of doing so: answering specific http requests (http-01) or create specific dns records (dns-01). For wildcard domains the latter is the only option. Various additional plugins are available from <https://github.com/win-acme/win-acme/>.

```
1: [http-01] Save verification files on (network) path
2: [http-01] Serve verification files from memory
3: [http-01] Upload verification files via FTP(S)
4: [http-01] Upload verification files via SSH-FTP
5: [http-01] Upload verification files via WebDav
6: [dns-01] Create verification records manually (auto-renew not possible)
7: [dns-01] Create verification records with acme-dns (https://github.com/joohoi/acme-dns)
8: [dns-01] Create verification records with your own script
9: [tls-alpn-01] Answer TLS verification request from win-acme
C: Abort
```

How would you like prove ownership for the domain(s) in the certificate?: 2

After ownership of the domain(s) has been proven, we will create a Certificate Signing Request (CSR) to obtain the actual certificate. The CSR determines properties of the certificate like which (type of) key to use. If you are not sure what to pick here, RSA is the safe default.

- 1: Elliptic Curve key
- 2: RSA key

What kind of private key should be used for the certificate?: 2

When we have the certificate, you can store in one or more ways to make it accessible to your applications. The Windows Certificate Store is the default location for IIS (unless you are managing a cluster of them).

- 1: IIS Central Certificate Store (.pfx per domain)
- 2: PEM encoded files (Apache, nginx, etc.)
- 3: Windows Certificate Store
- 4: No (additional) store steps
- C: Abort

How would you like to store the certificate?: 3

With the certificate saved to the store(s) of your choice, you may choose one or more steps to update your applications, e.g. to configure the new thumbprint, or to update bindings.

- 1: Create or update https bindings in IIS
- 2: Create or update ftps bindings in IIS
- 3: Start external script or program
- 4: No (additional) installation steps

Which installation step should run first?: 1

- 1: Default Web Site
- 2: Exchange Back End

Choose site to create new bindings: 1

- 1: Create or update ftps bindings in IIS
- 2: Start external script or program
- 3: No (additional) installation steps

Add another installation step?: 2

Full instructions: <https://www.win-acme.com/reference/plugins/installation/script>

Enter the path to the script that you want to run after renewal: ./Scripts/ImportExchange.ps1

```
{CertCommonName}:    Common name (primary domain name)
{CachePassword}:     .pfx password
{CacheFile}:         .pfx full path
{CertFriendlyName}:  Certificate friendly name
{CertThumbprint}:    Certificate thumbprint
{StoreType}:         Type of store (CentralSsl/CertificateStore/PemFiles)
{StorePath}:         Path to the store
{RenewalId}:         Renewal identifier
```

Enter the parameter format string for the script, e.g. "--hostname {CertCommonName}": '{CertThumbprint}' 'IIS,SMTP,POP,IMAP' 1 '{CacheFile}' '{CachePassword}' '{CertFriendlyName}'

```
Cached order available but not used with the --force switch.
First chance error calling into ACME server, retrying with new nonce...
Cached authorization result for autodiscover.ramlan.ca: valid
Cached authorization result for mail.ramlan.ca: valid
Authorize identifier ramlan.ca
Authorizing ramlan.ca using http-01 validation (SelfHosting)
Authorization result: valid
Requesting certificate [Manual] mail.ramlan.ca
Store with CertificateStore...
Installing certificate in the certificate store
Adding certificate [Manual] mail.ramlan.ca @ 2020-4-27 21:09:46 to store WebHosting
Installation step 1/2: IIS...
Adding new https binding *:443:mail.ramlan.ca
Our best match was the default binding and it seems there are other non-SNI enabled bindings listening to the same endpoint, which means we cannot update it without potentially causing problems. Instead, a new binding will be created. You may manually update the bindings if you want IIS to be configured in a different way.
Our best match was the default binding and it seems there are other non-SNI enabled bindings listening to the same endpoint, which means we cannot update it without potentially causing problems. Instead, a new binding will be created. You may manually update the bindings if you want IIS to be configured in a different way.
Committing 1 https binding changes to IIS
Installation step 2/2: Script...
Script ./Scripts/ImportExchange.ps1 starting with parameters 'ED1616D467357D3578BBAC34DBA98715230FA8D3' 'IIS,SMTP,POP,IMAP' 1 'C:\ProgramData\win-acme\acme-v02.api.letsencrypt.org\Certificates\kwyIQf2U00-VuGreXVSSPw-103c6b76d61ab9a89490938002dd1d65fc2ef01f-temp.pfx' 'k93ny7NrjxFXBaYPHNIsvsJTPGfJWr6FTBVSTfjMLZA=' '[Manual] mail.ramlan.ca @ 2020-4-27 21:09:46'

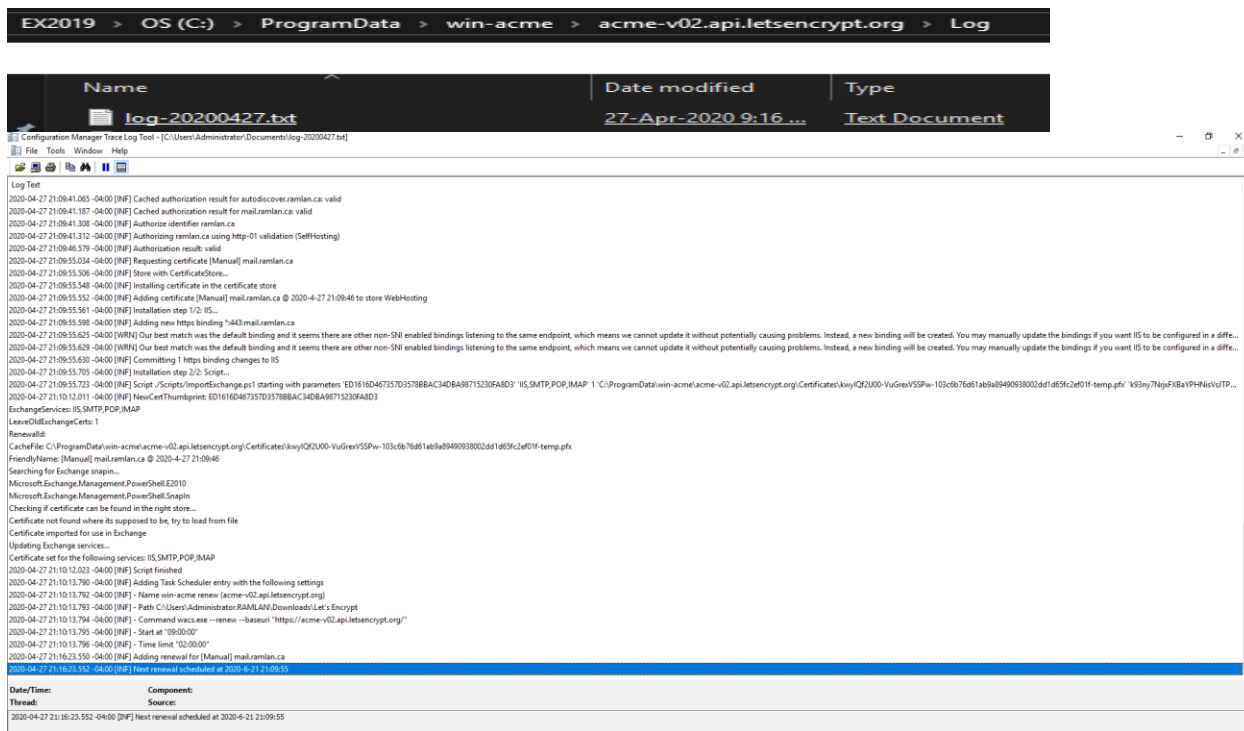
Script finished
Adding Task Scheduler entry with the following settings
- Name win-acme renew (acme-v02.api.letsencrypt.org)
- Path C:\Users\Administrator.RAMLAN\Downloads\Let's Encrypt
- Command wacs.exe --renew --baseuri "https://acme-v02.api.letsencrypt.org/"
- Start at 09:00:00
- Time limit 02:00:00

Do you want to specify the user the task will run as? (y/n*) _
```

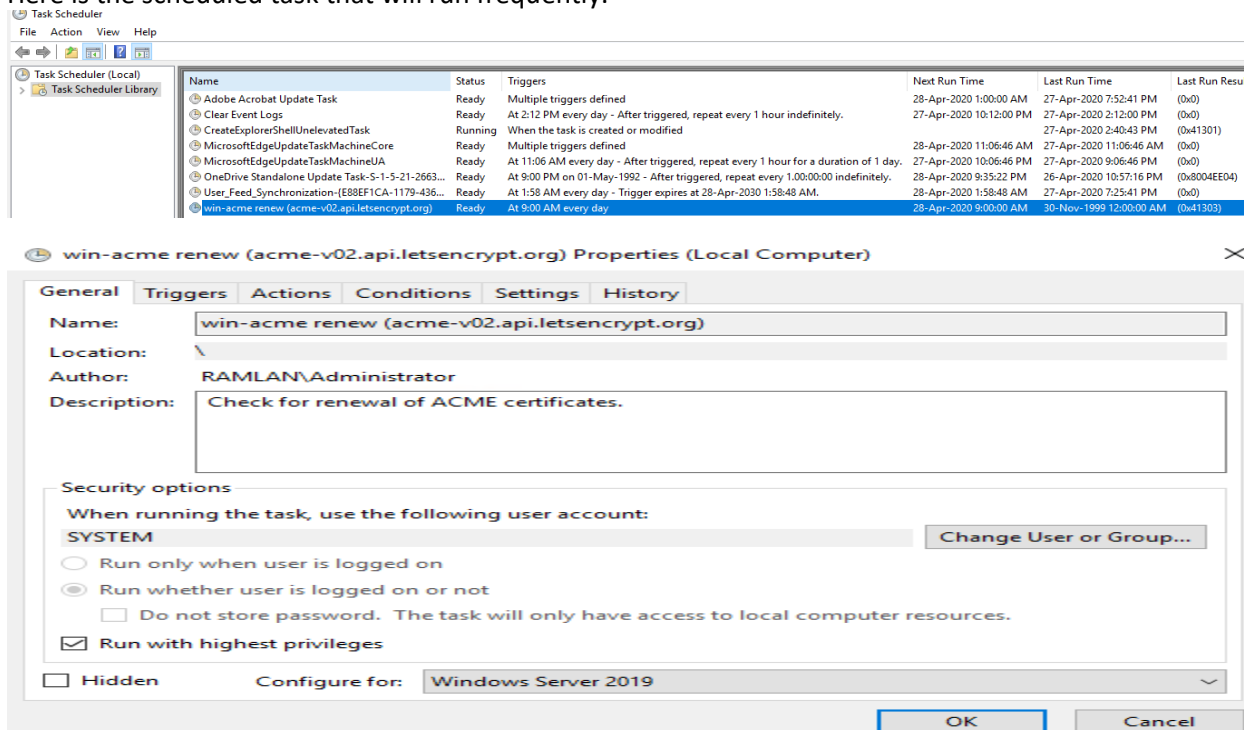
```
Do you want to specify the user the task will run as? (y/n*) - no
Adding renewal for [Manual] mail.ramlan.ca
Next renewal scheduled at 2020-6-21 21:09:55

N: Create new certificate (simple for IIS)
M: Create new certificate (full options)
R: Run scheduled renewals (0 currently due)
A: Manage renewals (1 total)
O: More options...
Q: Quit
Please choose from the menu: _
```

Below is the log you can open and check the status.



Here is the scheduled task that will run frequently.



Now we can see the certificate issued with expiry date.

servers databases database availability groups virtual directories [certificates](#)

Select server: EX2019.RAMLAN.CA

+ - ✎ 🗑️ ↺ ...

NAME	STATUS	EXPIRES ON	
CN=MS-Organization-P2P-Access [2018]	Invalid	2019-10-14	
CN=MS-Organization-P2P-Access [2019]	Invalid	2020-04-22	
Exchange 2019 Certificate	Valid	2020-05-03	
[Manual] mail.ramlan.ca @ 2020-4-27 21:09:46	Valid	2020-07-26	[Manual] mail.ramlan.ca @ 2020-4-27 21:09:46
Microsoft Exchange Server Auth Certificate	Valid	2023-12-04	Certification authority-signed certificate Issuer: CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US
Microsoft Exchange	Valid	2023-12-30	Status
WMSVC-SHA2	Valid	2028-12-27	Valid
Veeam Agent Certificate	Invalid	2029-02-03	Expires on: 2020-07-26 Renew
			Assigned to services IMAP, POP, IIS, SMTP

Use this link you can check SSL certificate status - <https://www.digicert.com/help/>

SSL Certificate Checker

If you are having a problem with your SSL certificate installation, please enter the name of your server. Our installation diagnostics tool will help you locate the problem and verify your SSL Certificate installation.

Server Address: (Ex. www.digicert.com/)

ramlan.ca

☐ Check for common vulnerabilities

CHECK SERVER

✓ DNS resolves ramlan.ca to [REDACTED]

HTTP Server Header: Microsoft-IIS/10.0

✓ TLS Certificate

Common Name = mail.ramlan.ca
Subject Alternative Names = autodiscover.ramlan.ca, mail.ramlan.ca, ramlan.ca
Issuer = Let's Encrypt Authority X3
Serial Number = 4A9E5ACE7DE7C17EEC74CBBC7CD28D45027
SHA1 Thumbprint = ED1616D467357D3578BBAC34DBA98715230FA8D3
Key Length = 3072
Signature algorithm = SHA256-RSA
Secure Renegotiation:

✓ TLS Certificate has not been revoked

OCSP Staple: Good
OCSP Origin: Good
CRL Status: Not Enabled

✓ TLS Certificate expiration

The certificate expires July 27, 2020 (90 days from today)

✓ Certificate Name matches ramlan.ca



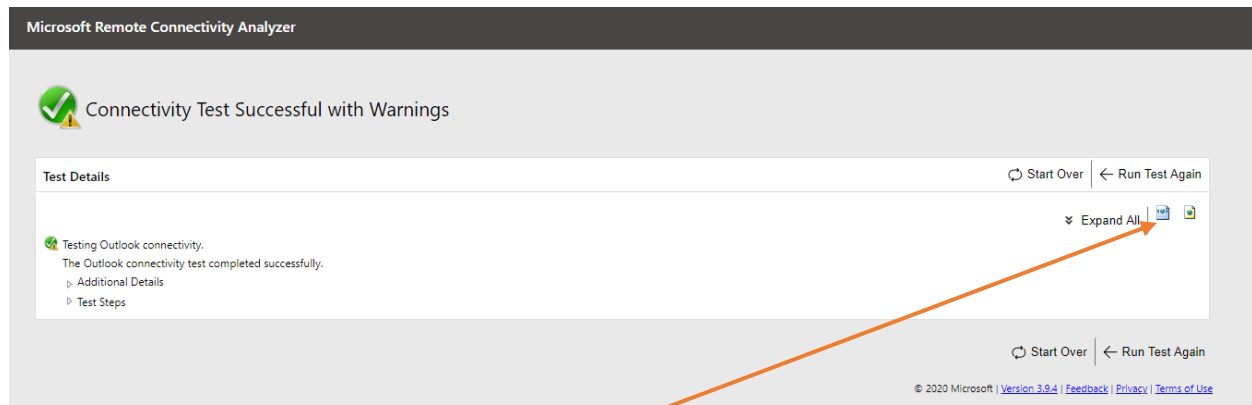
Subject mail.ramlan.ca
Valid from 28/Apr/2020 to 27/Jul/2020
Issuer Let's Encrypt Authority X3



Subject Let's Encrypt Authority X3
Valid from 17/Mar/2016 to 17/Mar/2021
Issuer DST Root CA X3

✓ TLS Certificate is correctly installed

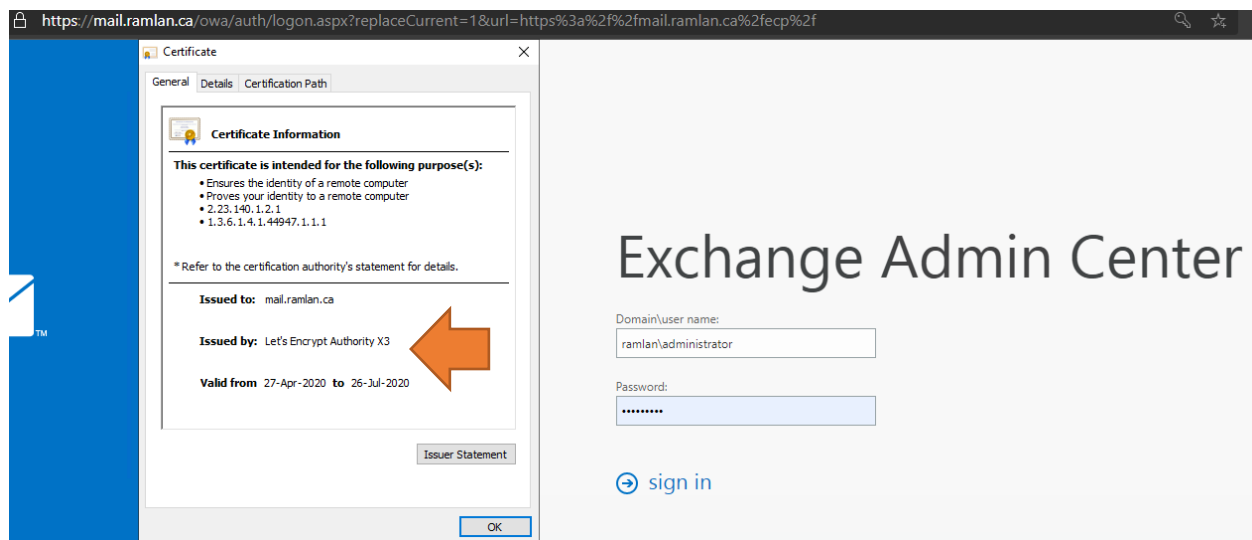
Remote Connectivity Analyzer status for Outlook connectivity.



I have exported html and xml file for above



Certificate Status.



This concludes the entire process for Let's Encrypt.

Thanks

Ram Lan
27th April 2020