

Public Cert in Exchange

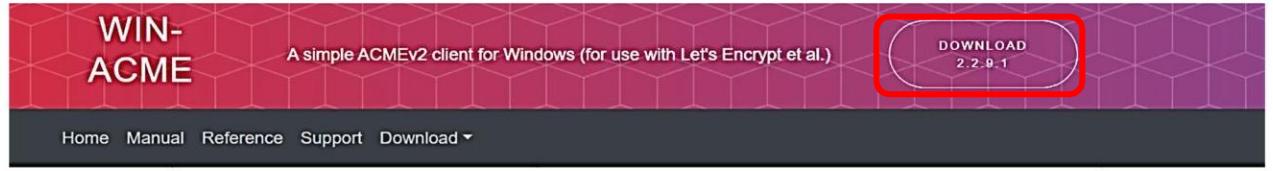
- ❖ Install Let's Encrypt Free Certificate with win-acme on Windows IIS

1. Download Let's Encrypt Client “win-acme” as it is command-line based application.

Link 1: <https://www.win-acme.com/>

Link 2: [Releases · win-acme/win-acme \(github.com\)](https://github.com/win-acme/win-acme/releases/download/v2.2.9.1701/win-acme.v2.2.9.1701.x64.pluggable.zip)
(<https://github.com/win-acme/win-acme/releases/download/v2.2.9.1701/win-acme.v2.2.9.1701.x64.pluggable.zip>)

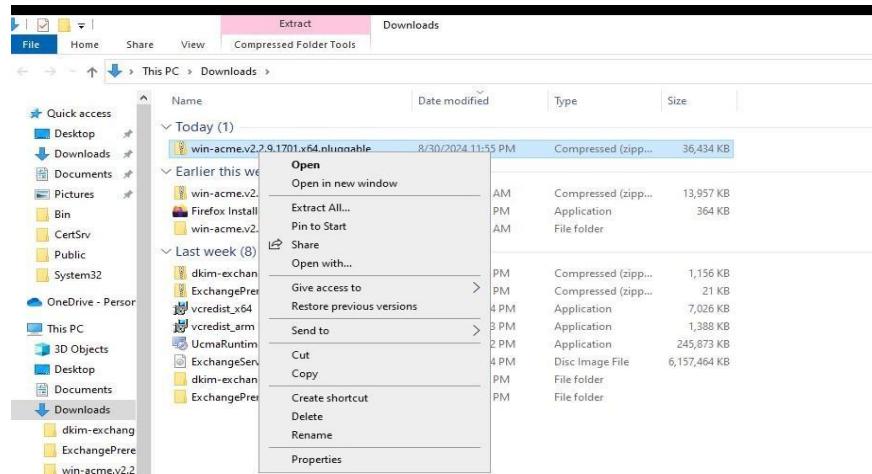
- Click on Download then it will be automatically downloading start



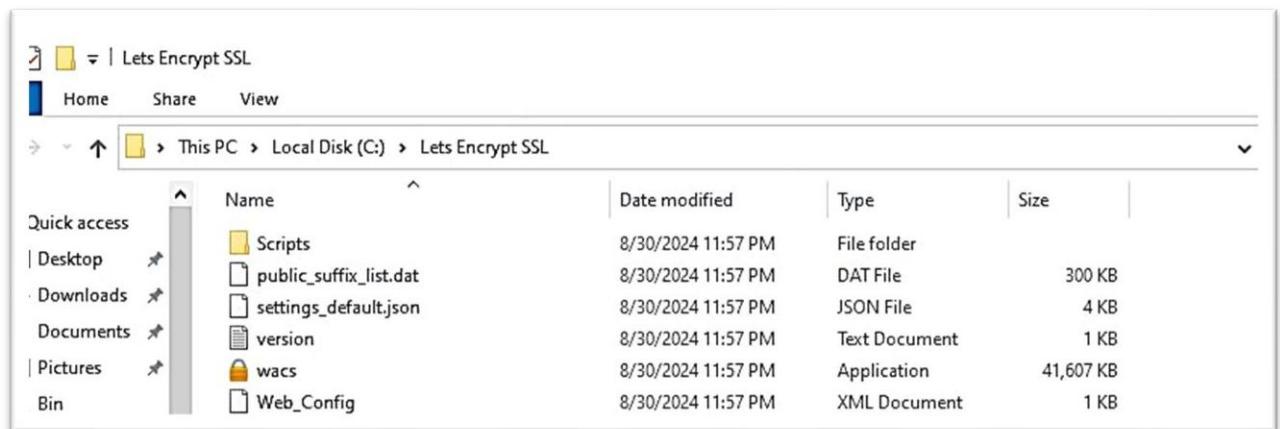
The screenshot shows the official website for WIN-ACME. At the top right, there is a large red "DOWNLOAD" button with the text "2.2.9.1" underneath it. This button is highlighted with a red oval. Below the header, there is a navigation bar with links: Home, Manual, Reference, Support, and Download. The main content area has a pink header with the text "WIN-ACME" and "A simple ACMEv2 client for Windows (for use with Let's Encrypt et al.)". The main text in the body says: "This is a ACMEv2 client for Windows that aims to be very simple to start with, but powerful enough to grow into almost every scenario." Below this, there is a bulleted list of features:

- A very simple interface to create and install certificates on a local IIS server
- A more advanced interface for many other use cases, including Apache and Exchange
- Automatically creates a scheduled task to renew certificates when needed
- Get certificates with wildcards (*.example.com), international names (证书.example.com), OCSP Must Staple extension (optional).
- Re-use private keys for DANE, use EC crypto or bring your own CSR
- Advanced toolkit for DNS, HTTP and TLS validation: SFTP/FTPS, acme-dns, Azure, Route53, Cloudflare and many more...
- Store your certificates where and how you want them: Windows, IIS Central Store, .pem files, .pfx file or KeyVault
- Compatible with all popular ACME services, including Let's Encrypt, ZeroSSL, DigiCert, Sectigo, Buypass, Keyon and others...
- Completely unattended operation from the command line
- Other forms of automation through manipulation of .json files
- Write your own Powershell .ps1 scripts to handle installation and validation
- Build your own plugins with C#

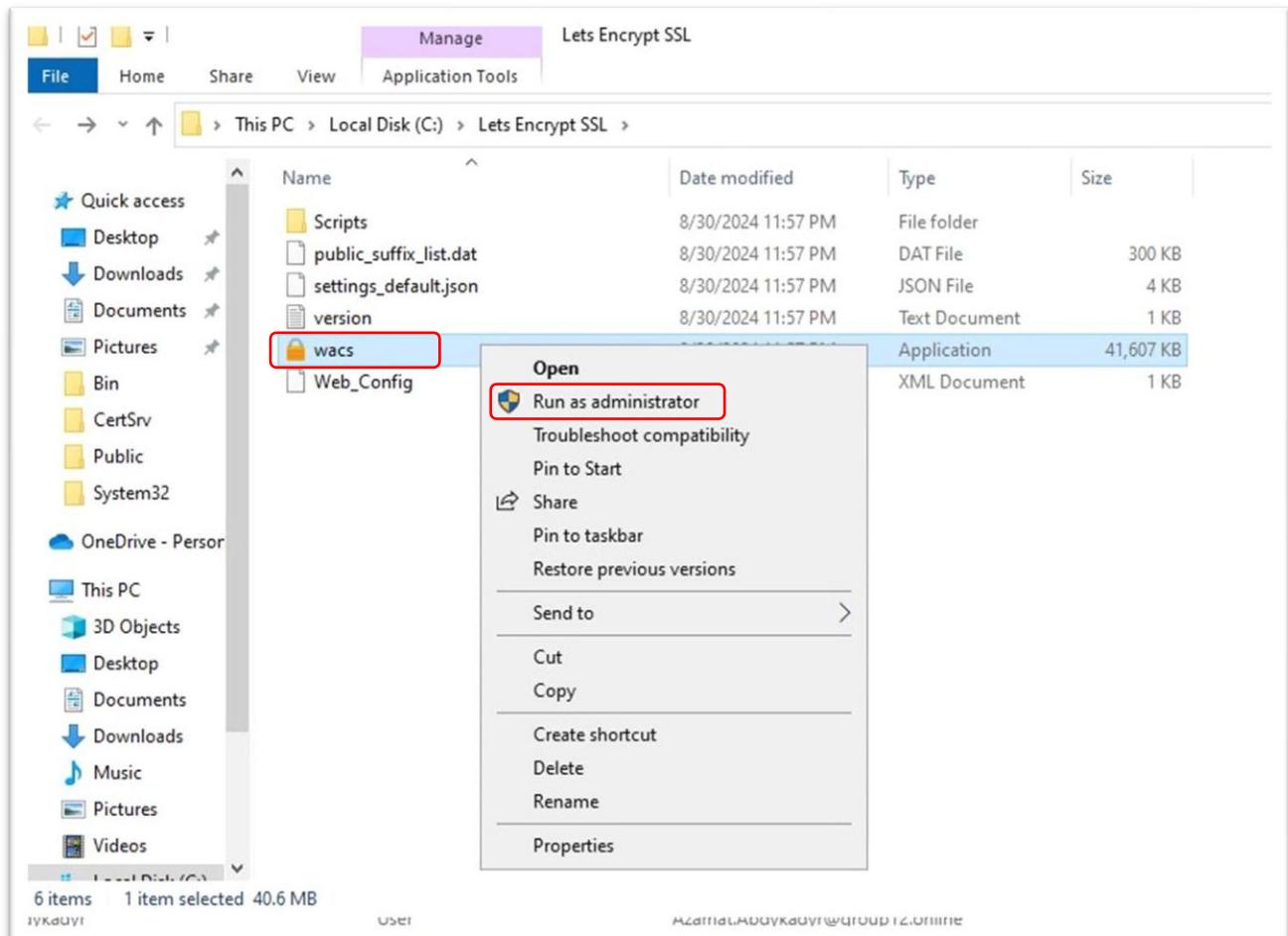
- Go to Download folder and Extract All win-acme downloaded folder.



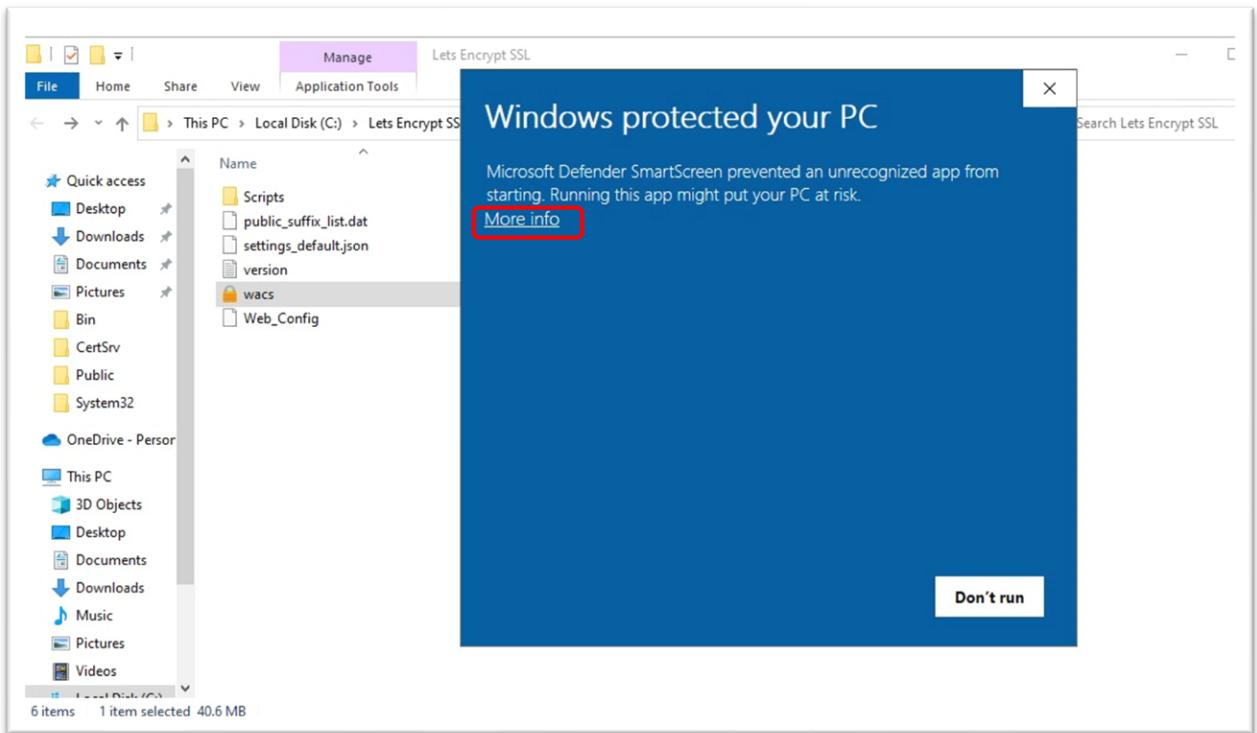
- Make a New Folder on drive C: like (Lets Encrypt SSL) then copy extracted all file or folder and paste on new folder



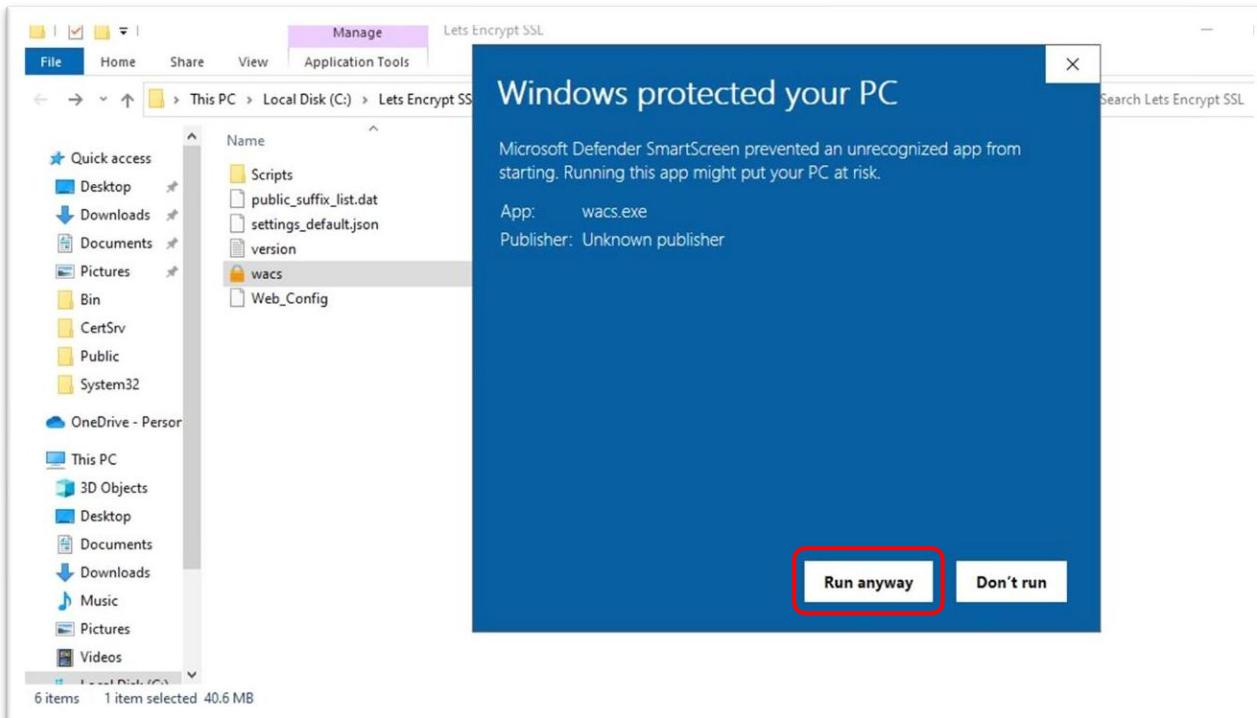
- Run wacs with as administrator



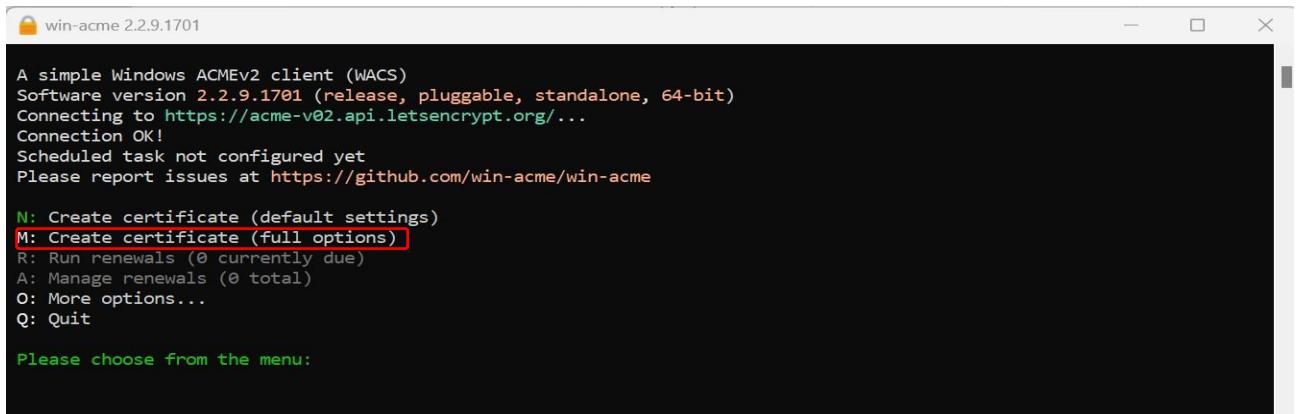
➤ Click on More info



➤ Click on Run anyway



- Choose **Create Certificate (full options)** for M then press Enter

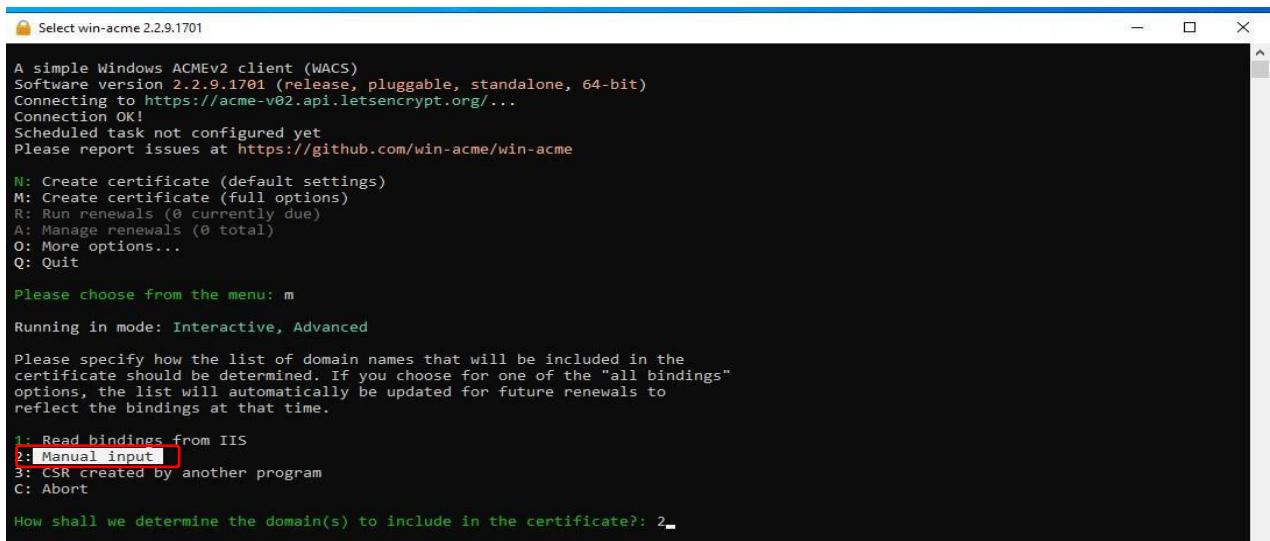


```
A simple Windows ACMEv2 client (WACS)
Software version 2.2.9.1701 (release, pluggable, standalone, 64-bit)
Connecting to https://acme-v02.api.letsencrypt.org/...
Connection OK!
Scheduled task not configured yet
Please report issues at https://github.com/win-acme/win-acme

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (0 currently due)
A: Manage renewals (0 total)
O: More options...
Q: Quit

Please choose from the menu:
```

- Choose **Manual input** for 2 then press Enter



```
Select win-acme 2.2.9.1701

A simple Windows ACMEv2 client (WACS)
Software version 2.2.9.1701 (release, pluggable, standalone, 64-bit)
Connecting to https://acme-v02.api.letsencrypt.org/...
Connection OK!
Scheduled task not configured yet
Please report issues at https://github.com/win-acme/win-acme

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run 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.

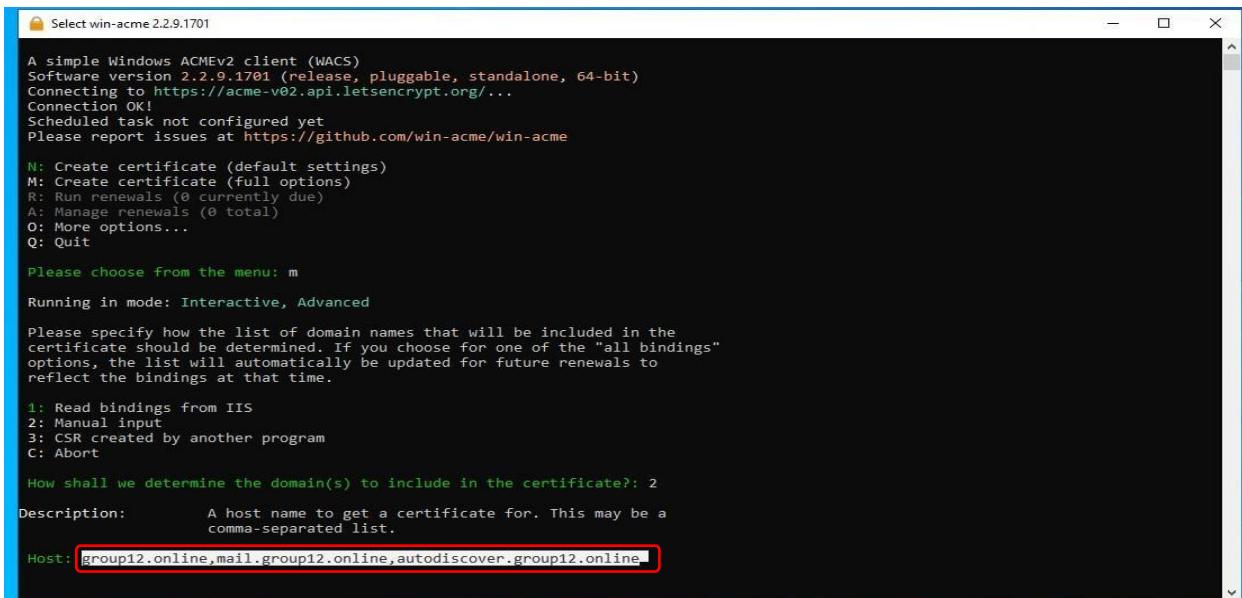
1: Read bindings from IIS
2: Manual input
3: CSR created by another program
C: Abort

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

- Write Host name

(in my case: group12.online,mail.group12.online,Autodiscover.group12.online)

- Press Enter



```
Select win-acme 2.2.9.1701

A simple Windows ACMEv2 client (WACS)
Software version 2.2.9.1701 (release, pluggable, standalone, 64-bit)
Connecting to https://acme-v02.api.letsencrypt.org/...
Connection OK!
Scheduled task not configured yet
Please report issues at https://github.com/win-acme/win-acme

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run 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: Read bindings from IIS
2: Manual input
3: CSR created by another program
C: Abort

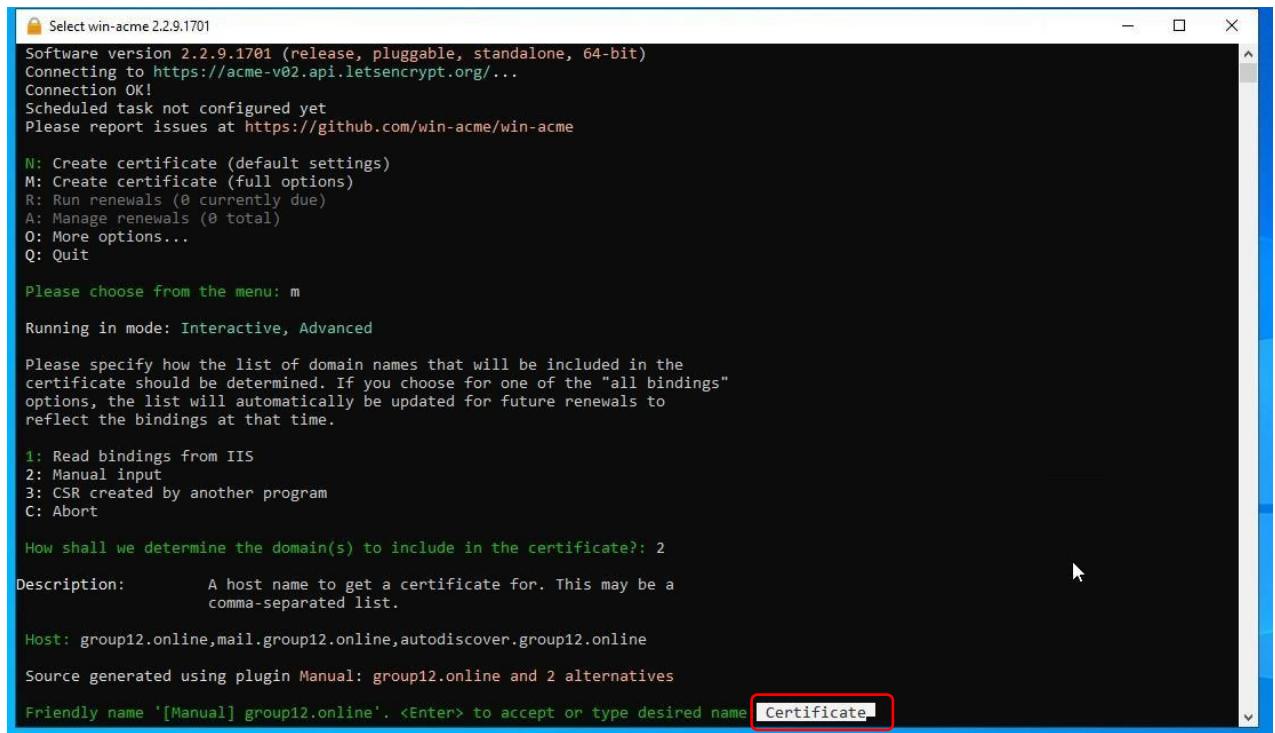
How shall we determine the domain(s) to include in the certificate?: 2

Description:      A host name to get a certificate for. This may be a
                  comma-separated list.

Host: group12.online,mail.group12.online,autodiscover.group12.online
```

➤ Give the accept or desired name (like: Certificate)

➤ Press Enter



```
Select win-acme 2.2.9.1701
Software version 2.2.9.1701 (release, pluggable, standalone, 64-bit)
Connecting to https://acme-v02.api.letsencrypt.org/...
Connection OK!
Scheduled task not configured yet
Please report issues at https://github.com/win-acme/win-acme

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run 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: Read bindings from 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

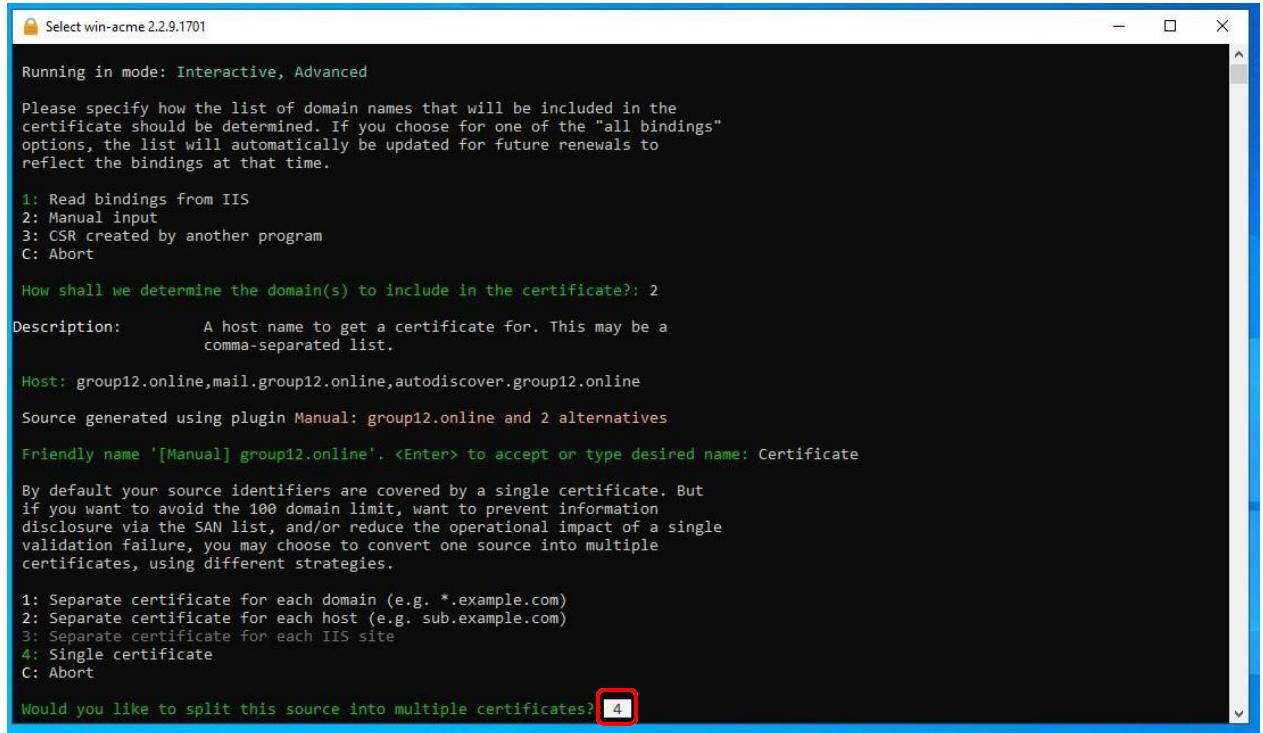
Description:      A host name to get a certificate for. This may be a
                  comma-separated list.

Host: group12.online,mail.group12.online,autodiscover.group12.online

Source generated using plugin Manual: group12.online and 2 alternatives

Friendly name '[Manual] group12.online'. <Enter> to accept or type desired name Certificate
```

➤ Choose the certificate type for 4



```
Select win-acme 2.2.9.1701
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: Read bindings from 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

Description:      A host name to get a certificate for. This may be a
                  comma-separated list.

Host: group12.online,mail.group12.online,autodiscover.group12.online

Source generated using plugin Manual: group12.online and 2 alternatives

Friendly name '[Manual] group12.online'. <Enter> to accept or type desired name: Certificate

By default your source identifiers are covered by a single certificate. But
if you want to avoid the 100 domain limit, want to prevent information
disclosure via the SAN list, and/or reduce the operational impact of a single
validation failure, you may choose to convert one source into multiple
certificates, using different strategies.

1: Separate certificate for each domain (e.g. *.example.com)
2: Separate certificate for each host (e.g. sub.example.com)
3: Separate certificate for each IIS site
4: Single certificate
C: Abort

Would you like to split this source into multiple certificates? 4
```

➤ Choose option 6 like prove ownership for the domain

```
Select win-acme 2.2.9.1701

Friendly name '[Manual] group12.online'. <Enter> to accept or type desired name: Certificate

By default your source identifiers are covered by a single certificate. But
if you want to avoid the 100 domain limit, want to prevent information
disclosure via the SAN list, and/or reduce the operational impact of a single
validation failure, you may choose to convert one source into multiple
certificates, using different strategies.

1: Separate certificate for each domain (e.g. *.example.com)
2: Separate certificate for each host (e.g. sub.example.com)
3: Separate certificate for each IIS site
4: Single certificate
C: Abort

Would you like to split this source into multiple certificates?: 4

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 identifiers the latter is the only option.
Various additional plugins are available from
https://github.com/win-acme/win-acme/.

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

How would you like prove ownership for the domain(s)? 6
```

➤ Choose option 2 of private key should be used for the certificate.

```
Select win-acme 2.2.9.1701

3: Separate certificate for each IIS site
4: Single certificate
C: Abort

Would you like to split this source into multiple certificates?: 4

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 identifiers the latter is the only option.
Various additional plugins are available from
https://github.com/win-acme/win-acme/.

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

How would you like prove ownership for the domain(s)? 6

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
C: Abort

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

- Choose option 4 to store the certificate.

```

Select win-acme 2.2.9.1701
https://github.com/win-acme/win-acme/.

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

How would you like prove ownership for the domain(s)?: 6

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
C: Abort

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 host)
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store (Local Computer)
5: No (additional) store steps

How would you like to store the certificate? 4

```

- Choose option 2 to use or type the name of another unlisted store.

```

Select win-acme 2.2.9.1701
https://github.com/win-acme/win-acme/.

5: [http] Upload verification files via WebDav
6: [dns] Create verification records manually (auto-renew not possible)
7: [dns] Create verification records with acme-dns (https://github.com/joohoi/acme-dns)
8: [dns] Create verification records with your own script
9: [tls-alpn] Answer TLS verification request from win-acme
C: Abort

How would you like prove ownership for the domain(s)?: 6

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
C: Abort

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 host)
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store (Local Computer)
5: No (additional) store steps

How would you like to store the certificate?: 4

1: [WebHosting] - Dedicated store for IIS
2: [My] - General computer store (for Exchange/RDS)
3: [Default] - Use global default, currently WebHosting

Choose store to use, or type the name of another unlisted store 2

```

- Choose option 5 to store it in another way too.

```

Select win-acme 2.2.9.1701

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
C: Abort

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 host)
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store (Local Computer)
5: No (additional) store steps

How would you like to store the certificate?: 4

1: [WebHosting] - Dedicated store for IIS
2: [My] - General computer store (for Exchange/RDS)
3: [Default] - Use global default, currently WebHosting

Choose store to use, or type the name of another unlisted store: 2

1: IIS Central Certificate Store (.pfx per host)
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store (Local Computer)
5: No (additional) store steps

Would you like to store it in another way too?: 5

```

- Choose option 1 to installation step should run first.

```

Select win-acme 2.2.9.1701

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 host)
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store (Local Computer)
5: No (additional) store steps

How would you like to store the certificate?: 4

1: [WebHosting] - Dedicated store for IIS
2: [My] - General computer store (for Exchange/RDS)
3: [Default] - Use global default, currently WebHosting

Choose store to use, or type the name of another unlisted store: 2

1: IIS Central Certificate Store (.pfx per host)
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store (Local Computer)
5: No (additional) store steps

Would you like to store it in another way too?: 5

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 bindings in IIS
2: Start external script or program
3: No (additional) installation steps

Which installation step should run first?: 1

```

- Choose option 1 to create new bindings.
- Press Enter

```

Select win-acme 2.2.9.1701
2: [My] - General computer store (for Exchange/RDS)
3: [Default] - Use global default, currently WebHosting

Choose store to use, or type the name of another unlisted store: 2

1: IIS Central Certificate Store (.pfx per host)
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store (Local Computer)
5: No (additional) store steps

Would you like to store it in another way too?: 5

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 bindings in IIS
2: Start external script or program
3: No (additional) installation steps

Which installation step should run first?: 1

This plugin will update *all* binding using the previous certificate in both
Web and FTP sites, regardless of whether those bindings were created manually
or by the program itself. Therefor you'll never need to run this installation
step twice.

During initial setup, it will try to make as few changes as possible to IIS
to cover the source identifiers. If new bindings are needed, by default it
will create those at the same site where the HTTP binding for that host was
found.

1: Default Web Site
2: Exchange Back End

Choose site to create new bindings: 1

```

- Choose option 2 to add another installation step.
- Press Enter

```

Select win-acme 2.2.9.1701
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store (Local Computer)
5: No (additional) store steps

Would you like to store it in another way too?: 5

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 bindings in IIS
2: Start external script or program
3: No (additional) installation steps

Which installation step should run first?: 1

This plugin will update *all* binding using the previous certificate in both
Web and FTP sites, regardless of whether those bindings were created manually
or by the program itself. Therefor you'll never need to run this installation
step twice.

During initial setup, it will try to make as few changes as possible to IIS
to cover the source identifiers. If new bindings are needed, by default it
will create those at the same site where the HTTP binding for that host was
found.

1: Default Web Site
2: Exchange Back End

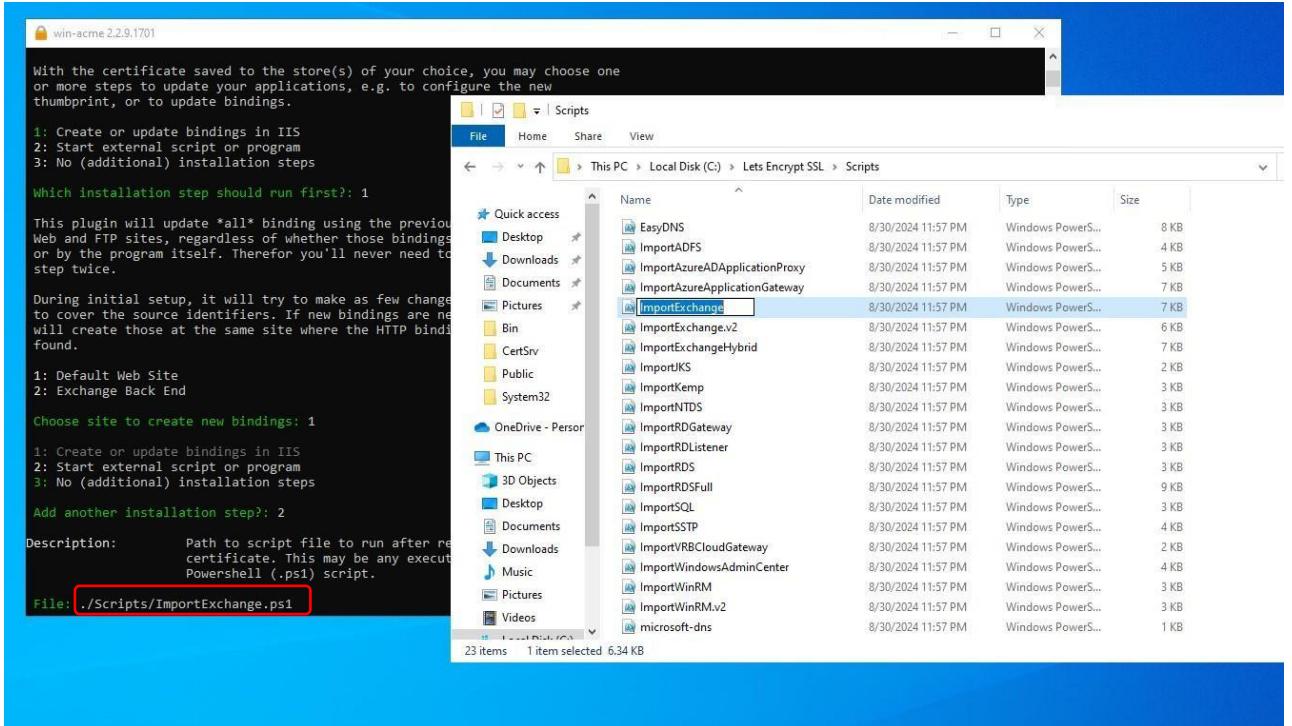
Choose site to create new bindings: 1

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

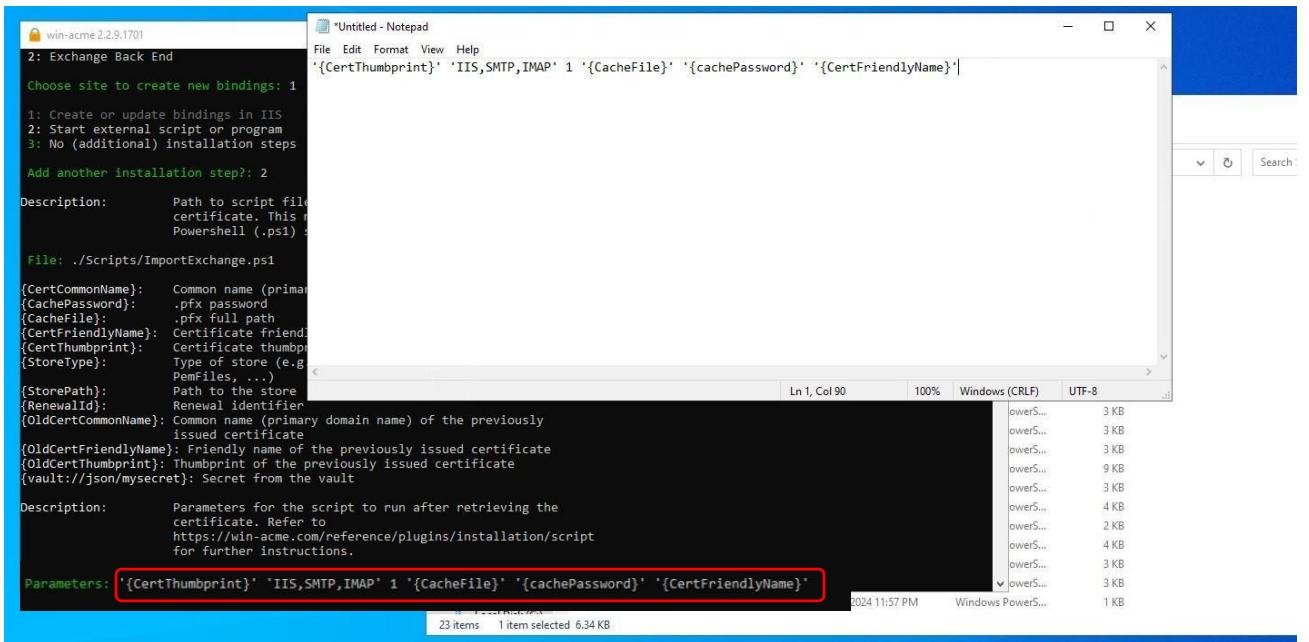
Add another installation step? 2

```

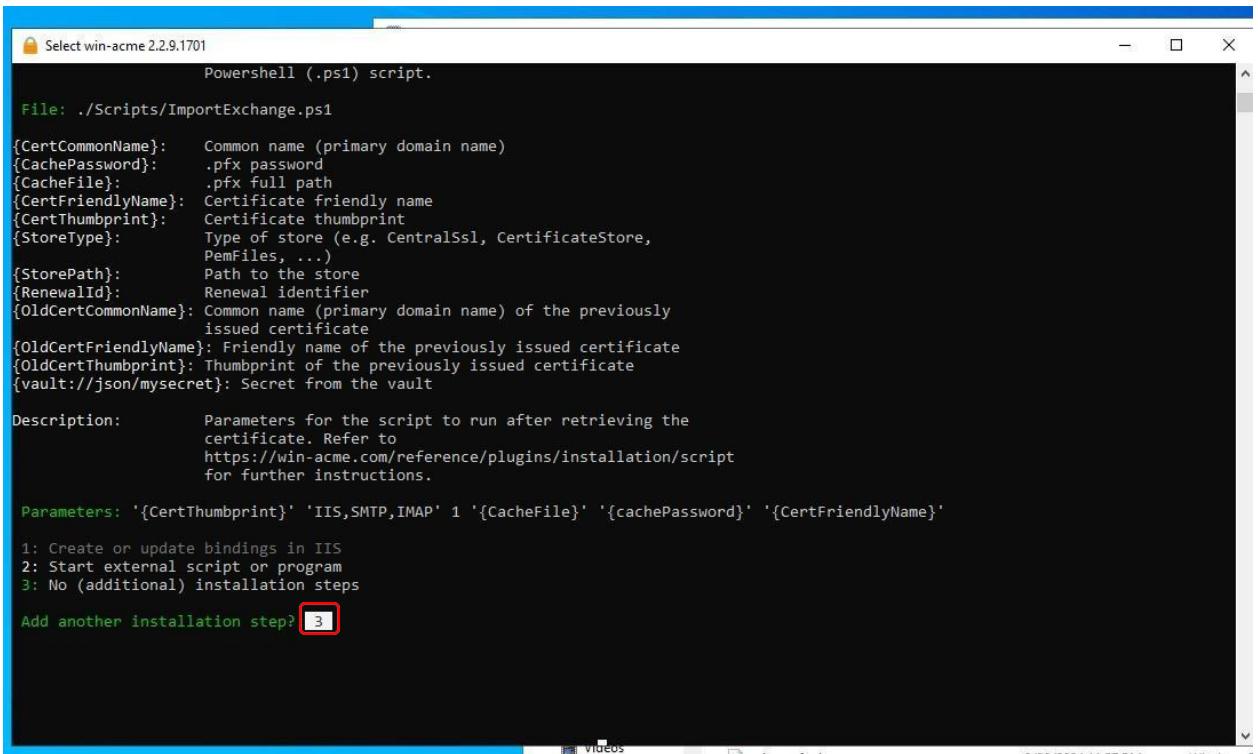
- Open Scripts on copied extracted folder then write script base description.
(like: ./Scripts/ImportExchange.ps1)
- Press Enter



- Write down parameters from scripts.
- {*CertThumbprint*} 'IIS,SMTP,IMAP' 1 '{*CacheFile*}' '{*cachePassword*}' '{*CertFriendlyName*}'
- Press Enter



- Choose option 3 another installation step.
- Press Enter



```

Select win-acme 2.2.9.1701
PowerShell (.ps1) script.

File: ./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 (e.g. CentralSsl, CertificateStore,
Pemfiles, ...)
{StorePath}: Path to the store
{RenewalId}: Renewal identifier
{OldCertCommonName}: Common name (primary domain name) of the previously
issued certificate
{OldCertFriendlyName}: Friendly name of the previously issued certificate
{OldCertThumbprint}: Thumbprint of the previously issued certificate
{vault://json/mysecret}: Secret from the vault

Description: Parameters for the script to run after retrieving the
certificate. Refer to
https://win-acme.com/reference/plugins/installation/script
for further instructions.

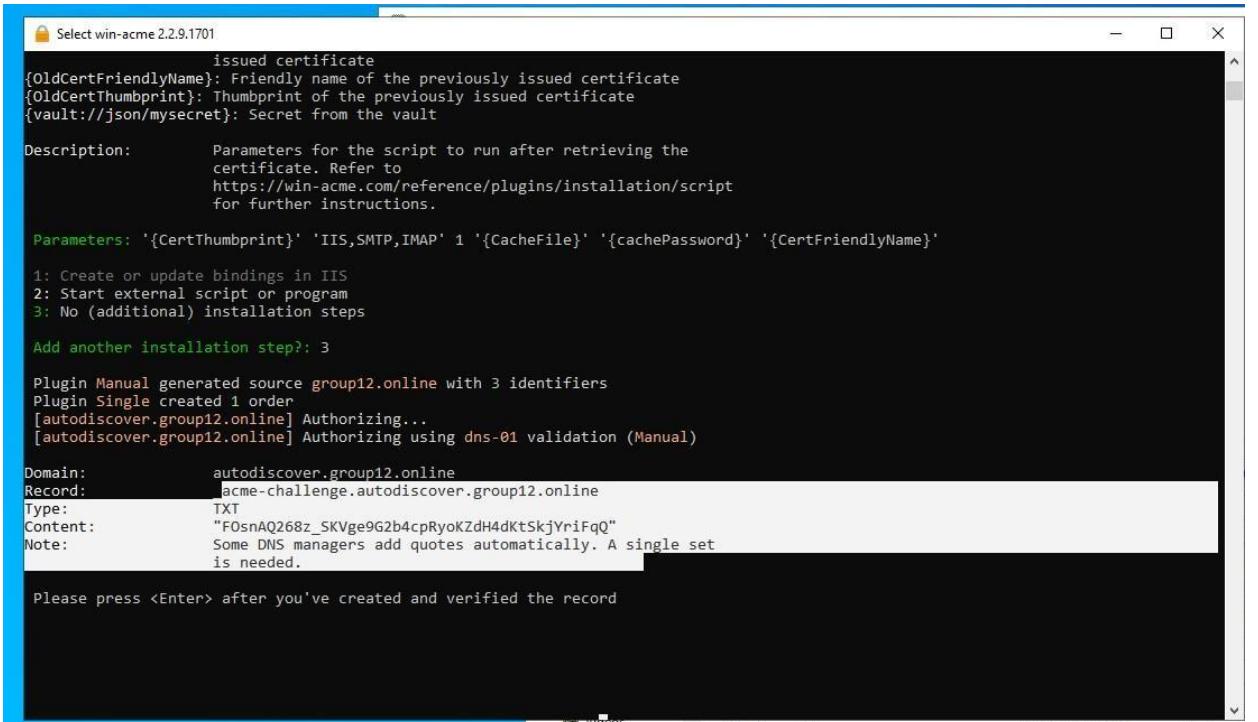
Parameters: '{CertThumbprint}' 'IIS,SMTP,IMAP' 1 '{CacheFile}' '{cachePassword}' '{CertFriendlyName}'

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

Add another installation step?: 3

```

- It will show plugin generated source for Autodiscover. After that go to your domain registrar.



```

Select win-acme 2.2.9.1701
issued certificate
{OldCertFriendlyName}: Friendly name of the previously issued certificate
{OldCertThumbprint}: Thumbprint of the previously issued certificate
{vault://json/mysecret}: Secret from the vault

Description: Parameters for the script to run after retrieving the
certificate. Refer to
https://win-acme.com/reference/plugins/installation/script
for further instructions.

Parameters: '{CertThumbprint}' 'IIS,SMTP,IMAP' 1 '{CacheFile}' '{cachePassword}' '{CertFriendlyName}'

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

Add another installation step?: 3

Plugin Manual generated source group12.online with 3 identifiers
Plugin Single created 1 order
[autodiscover.group12.online] Authorizing...
[autodiscover.group12.online] Authorizing using dns-01 validation (Manual)

Domain: autodiscover.group12.online
Record: acme-challenge.autodiscover.group12.online
Type: TXT
Content: "F0snAQ268z_SKVge9G2b4cpRyoKZdH4dKtSkjYriFqQ"
Note: Some DNS managers add quotes automatically. A single set
is needed.

Please press <Enter> after you've created and verified the record

```

- Go the DNS on your Domain and create a new TXT records

All Products and Services

Domains

group12.online
Protection Plan: None
[Upgrade Protection](#)

Websites + Marketing

DNS Manage

- Copy Record text and past in name section

Select win-acme 2.2.9.1701

Issued certificate
(OldCertFriendlyName): friendly name of the previously issued certificate
(OldCertThumbprint): thumbprint of the previously issued certificate
(Vault://Json/mysecret): Secret from the vault

Description: Parameters for the script to run after retrieving the certificate. Refer to <https://win-acme.com/reference/plugins/installation/script> for further instructions.

Parameters: '{CertThumbprint}' 'IIS,SMTP,IMAP' 1 '{CacheFile}' '{CachePassword}' '{CertFriendlyName}'

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

Add another installation step? 3

Plugin Manual generated source group12.online with 3 identifiers
Plugin Single created 1 order
[autodiscover.group12.online] Authorizing...
[autodiscover.group12.online] Authorizing using dns-01 validation (Manual)

Domain: autodiscover.group12.online
Record: _acme-challenge.autodiscover.group12.online
Type: TXT
Content: "F0snAQ268z_SKVge9G2b4cpRy0KZdH4dKSkYrIfQ"
Note: Some DNS managers add quotes automatically. A single set is needed.

Please press <Enter> after you've created and verified the record

group12.online

DNS Records Forwarding Nameservers Premium DNS Hostnames DNSSEC NEW Crypto Wallet

DNS records define how your domain behaves, like showing your website content and delivering your email.

New Records

TXT records are used to verify domain ownership, SSL verification, and email sender policies.

Type *	Name *	Value *	TTL
TXT	_acme-challenge.autodiscover.group12.online	F0snAQ268z_SKVge9G2b4cpRy0KZdH4dKSkYrIfQ	1 Hour

Add More Records Save Cancel

- Then copy content and paste it on Value section.

Select win-acme 2.2.9.1701

Issued certificate
(OldCertFriendlyName): friendly name of the previously issued certificate
(OldCertThumbprint): thumbprint of the previously issued certificate
(Vault://Json/mysecret): Secret from the vault

Description: Parameters for the script to run after retrieving the certificate. Refer to <https://win-acme.com/reference/plugins/installation/script> for further instructions.

Parameters: '{CertThumbprint}' 'IIS,SMTP,IMAP' 1 '{CacheFile}' '{CachePassword}' '{CertFriendlyName}'

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

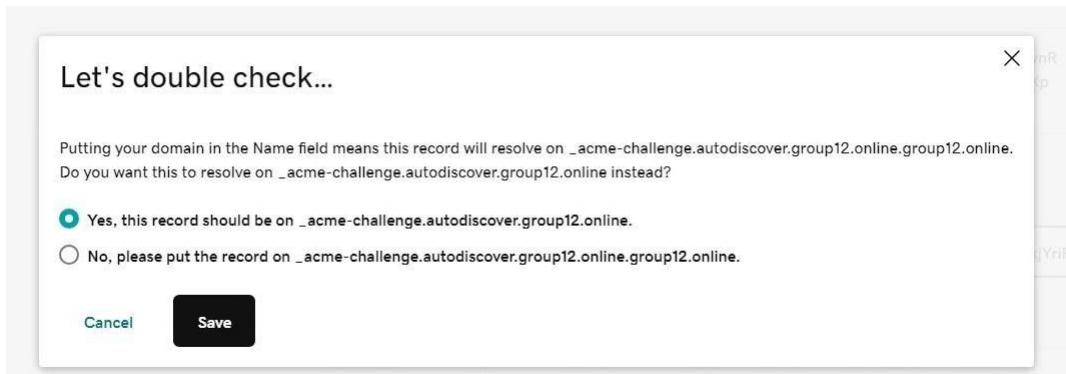
Add another installation step? 3

Plugin Manual generated source group12.online with 3 identifiers
Plugin Single created 1 order
[autodiscover.group12.online] Authorizing...
[autodiscover.group12.online] Authorizing using dns-01 validation (Manual)

Domain: autodiscover.group12.online
Record: _acme-challenge.autodiscover.group12.online
Type: TXT
Content: F0snAQ268z_SKVge9G2b4cpRy0KZdH4dKSkYrIfQ
Note: Some DNS managers add quotes automatically. A single set is needed.

Please press <Enter> after you've created and verified the record

- Then save it.



- Go back to Exchange Server Then Enter
 - choose option 2 to continue for authorization result
 - Press Enter

```
daddu.com/central/domainmanagement?domainName=group12.online
win-acme 2.2.9.1701

for further instructions.

Parameters: '{CertThumbprint}' 'IIS,SMTP,IMAP' '{CacheFile}' '{cachePassword}' '{CertFriendlyName}'

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

Add another installation step?: 3

Plugin Manual generated source group12.online with 3 identifiers
Plugin Single created 1 order
[autodiscover.group12.online] Authorizing...
[autodiscover.group12.online] Authorizing using dns-01 validation (Manual)

Domain: autodiscover.group12.online
Record: _acme-challenge.autodiscover.group12.online
Type: TXT
Content: "FOsnAQ268z_SKVgeGZb4cpRyOK2dh4dKtSkjYviFqQ"
Note: Some DNS managers add quotes automatically. A single set
      is needed.

Please press <Enter> after you've created and verified the record

[autodiscover.group12.online] [192.168.12.2] No TXT records found
[autodiscover.group12.online] [192.168.12.1] No TXT records found
[autodiscover.group12.online] Preliminary validation failed on all nameservers

The correct record has not yet been found by the local resolver. That means
it's likely the validation attempt will fail, on your DNS provider needs a
little more time to publish and synchronize the changes.

1: Retry check
2: Ignore and continue
3: Abort

How would you like to proceed?:
```

- It will take time to run command and end you authorization result: **valid**
 - Then you see instructions bellow ‘**press enter after deleted the record**’ from godaddy.com
 - Delete **TXT** record from godaddy whatever you made early.

Autodiscover Group 12 Online					
Record	Type	Value	ttl	Created	Actions
_autodiscover	MX	mxb.mailgun.org. (Priority: 5)		1 Hour	
_acme-challenge._autodiscover	TXT	v=spf1 include:mailgun.org ~all		1/2 Hour	
_acme-challenge._autodiscover	TXT	k1...domainkey		1 Hour	
_acme-challenge._autodiscover	TXT	FOsnAQ268z_SKVge9G2b4cpRyoKzd4dKt5kjYrifqQ		1 Hour	
_dmarc	TXT	v=DMARC1; p=quarantine; rua=mailto:dmarc-reports@group12.online; ruf=mailto:dmarc-failures@group12.online; fo=1		1/2 Hour	

- When press Enter you can see another record for domain and create a new TXT records

```
! Select win-acme 2.2.8.1701
[autodiscover.group12.online] Preliminary validation failed on all nameservers
[autodiscover.group12.online] Will retry in 30 seconds (retry 8/10)...
[autodiscover.group12.online] [192.168.12.2] No TXT records found
[autodiscover.group12.online] Preliminary validation failed on all nameservers
[autodiscover.group12.online] Will retry in 30 seconds (retry 9/10)...
[autodiscover.group12.online] [192.168.12.2] No TXT records found
[autodiscover.group12.online] [192.168.12.1] No TXT records found
[autodiscover.group12.online] Preliminary validation failed on all nameservers
[autodiscover.group12.online] Will retry in 30 seconds (retry 10/10)...
[autodiscover.group12.online] [192.168.12.2] No TXT records found
[autodiscover.group12.online] [192.168.12.1] No TXT records found
[autodiscover.group12.online] Preliminary validation failed on all nameservers
[autodiscover.group12.online] It looks like validation is going to fail, but we will try now anyway...
[HTTP] Request completed with status BadRequest
First chance error calling into ACME server, retrying with new nonce...
[autodiscover.group12.online] Authorization result: valid

Domain: autodiscover.group12.online
Record: _acme-challenge.autodiscover.group12.online
Type: TXT
Content: "F0snAQ268z_SKVge9G2b4cpRyoKZdH4dKtSkjYrifQq"

Please press <Enter> after you've deleted the record

[autodiscover.group12.online] Record F0snAQ268z_SKVge9G2b4cpRyoKZdH4dKtSkjYrifQ deleted
[group12.online] Authorizing...
[group12.online] Authorizing using dns-01 validation (Manual)

Domain: group12.online
Record: _acme-challenge.group12.online
Type: TXT
Content: "-lxa9LHztFvxGN-NXIVd_OBMkCk"
Note: Some DNS managers add quotes automatically. A single set is needed.

Please press <Enter> after you've created and verified the record
```

The screenshot shows the GoDaddy DNS Management interface for the domain group12.online. In the 'DNS Records' tab, a new record is being added. The 'Type' is set to 'TXT', the 'Name' is '_acme-challenge.group12.online', the 'Value' is '-lxa9LHztFvxGN-NXIVd_OBMkCk', and the 'TTL' is set to '1 Hour'. A red arrow points from the 'Content' field in the terminal output above to the 'Value' field in the GoDaddy interface.

```
! Select win-acme 2.2.8.1701
[autodiscover.group12.online] Preliminary validation failed on all nameservers
[autodiscover.group12.online] Will retry in 30 seconds (retry 8/10)...
[autodiscover.group12.online] [192.168.12.2] No TXT records found
[autodiscover.group12.online] Preliminary validation failed on all nameservers
[autodiscover.group12.online] Will retry in 30 seconds (retry 9/10)...
[autodiscover.group12.online] [192.168.12.2] No TXT records found
[autodiscover.group12.online] [192.168.12.1] No TXT records found
[autodiscover.group12.online] Preliminary validation failed on all nameservers
[autodiscover.group12.online] Will retry in 30 seconds (retry 10/10)...
[autodiscover.group12.online] [192.168.12.2] No TXT records found
[autodiscover.group12.online] [192.168.12.1] No TXT records found
[autodiscover.group12.online] Preliminary validation failed on all nameservers
[autodiscover.group12.online] It looks like validation is going to fail, but we will try now anyway...
[HTTP] Request completed with status BadRequest
First chance error calling into ACME server, retrying with new nonce...
[autodiscover.group12.online] Authorization result: valid

Domain: autodiscover.group12.online
Record: _acme-challenge.autodiscover.group12.online
Type: TXT
Content: "F0snAQ268z_SKVge9G2b4cpRyoKZdH4dKtSkjYrifQq"

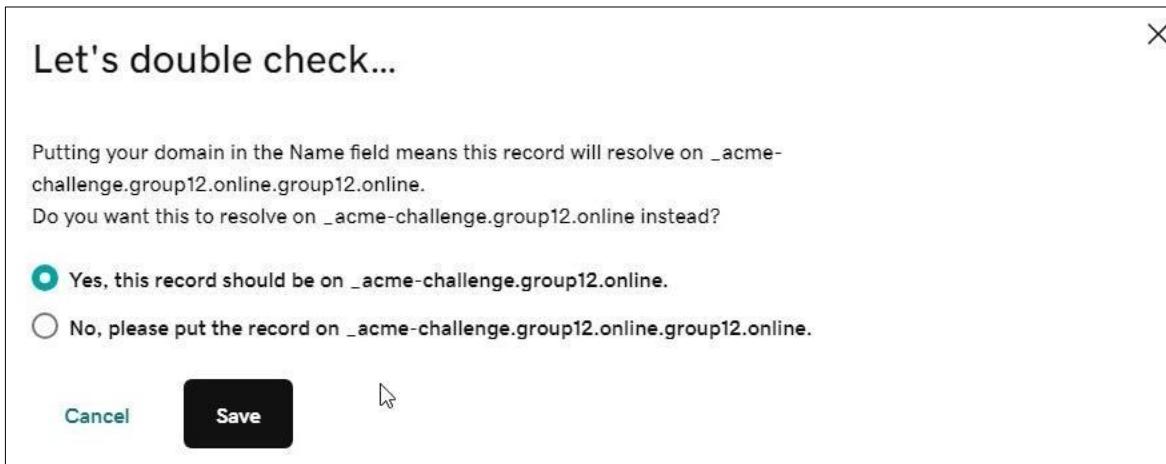
Please press <Enter> after you've deleted the record

[autodiscover.group12.online] Record F0snAQ268z_SKVge9G2b4cpRyoKZdH4dKtSkjYrifQ deleted
[group12.online] Authorizing...
[group12.online] Authorizing using dns-01 validation (Manual)

Domain: group12.online
Record: _acme-challenge.group12.online
Type: TXT
Content: "-lxa9LHztFvxGN-NXIVd_OBMkCk"
Note: Some DNS managers add quotes automatically. A single set is needed.

Please press <Enter> after you've created and verified the record
```

- Then save it.



- Go back to Exchange Server Then Enter
- Choose option 1 or either 2 to continue for authorization result
- Press Enter

```

win-acme 2.2.9.1701
Domain:          autodiscover.group12.online
Record:         _acme-challenge.autodiscover.group12.online
Type:          TXT
Content:        "F0snAQ268z_SKVge9G2b4cpRyoKZdH4dKtSkjYrIfQ"
Please press <Enter> after you've deleted the record
[autodiscover.group12.online] Record F0snAQ268z_SKVge9G2b4cpRyoKZdH4dKtSkjYrIfQ deleted
[group12.online] Authorizing...
[group12.online] Authorizing using dns-01 validation (Manual)

Domain:          group12.online
Record:         _acme-challenge.group12.online
Type:          TXT
Content:        "-lxa9LHztFvxGN-NXiVd_OBMkC0QIwXlCOY546q6Kc"
Note:          Some DNS managers add quotes automatically. A single set
               is needed.

Please press <Enter> after you've created and verified the record
[group12.online] [192.168.12.2] No TXT records found
[group12.online] [192.168.12.1] No TXT records found
[group12.online] Preliminary validation failed on all nameservers

The correct record has not yet been found by the local resolver. That means
it's likely the validation attempt will fail, or your DNS provider needs a
little more time to publish and synchronize the changes.

1: Retry check
2: Ignore and continue
3: Abort

How would you like to proceed?: 1

```



```

Select win-acme 2.2.9.1701
[group12.online] [192.168.12.2] No TXT records found
[group12.online] [192.168.12.1] No TXT records found
[group12.online] Preliminary validation failed on all nameservers
[group12.online] Will retry in 30 seconds (retry 8/10)...
[group12.online] [192.168.12.2] No TXT records found
[group12.online] [192.168.12.1] No TXT records found
[group12.online] Preliminary validation failed on all nameservers
[group12.online] Will retry in 30 seconds (retry 9/10)...
[group12.online] [192.168.12.2] No TXT records found
[group12.online] [192.168.12.1] No TXT records found
[group12.online] Preliminary validation failed on all nameservers
[group12.online] Will retry in 30 seconds (retry 10/10)...
[group12.online] [192.168.12.2] No TXT records found
[group12.online] [192.168.12.1] No TXT records found
[group12.online] Preliminary validation failed on all nameservers
[group12.online] It looks like validation is going to fail, but we will try now anyway...
[group12.online] Authorization result: valid

Domain:          group12.online
Record:         _acme-challenge.group12.online
Type:          TXT
Content:        "-lxa9LHztFvxGN-NXiVd_OBMkC0QIwXlCOY546q6Kc"
Note:          Some DNS managers add quotes automatically. A single set
               is needed.

Please press <Enter> after you've created and verified the record

```

- It will take time to run command and end you authorization result: **valid**
- Then you see instructions bellow ‘**press enter after deleted the record**’ from godaddy.com
- Delete **TXT** record from godaddy whatever you made early.
- When press Enter you can see another record for mail.domain and create a new **TXT** records

```

Select win-acme 2.2.9.1701
[group12.online] [192.168.12.2] No TXT records found
[group12.online] [192.168.12.1] No TXT records found
[group12.online] Preliminary validation failed on all nameservers
[group12.online] Will retry in 30 seconds (retry 9/10)...
[group12.online] [192.168.12.2] No TXT records found
[group12.online] [192.168.12.1] No TXT records found
[group12.online] Preliminary validation failed on all nameservers
[group12.online] Will retry in 30 seconds (retry 10/10)...
[group12.online] [192.168.12.2] No TXT records found
[group12.online] [192.168.12.1] No TXT records found
[group12.online] Preliminary validation failed on all nameservers
[group12.online] It looks like validation is going to fail, but we will try now anyway...
[group12.online] Authorization result: valid

Domain:          group12.online
Record:         _acme-challenge.group12.online
Type:          TXT
Content:        "-lxa9LHztFvxGN-NXiVd_OBMkC0QIwXlCOY546q6Kc"
Please press <Enter> after you've deleted the record
[group12.online] Record -lxa9LHztFvxGN-NXiVd_OBMkC0QIwXlCOY546q6Kc deleted
[mail.group12.online] Authorizing...
[mail.group12.online] Authorizing using dns-01 validation (Manual)

Domain:          mail.group12.online
Record:         _acme-challenge.mail.group12.online
Type:          TXT
Content:        "-asp3y5RntzfPSmIbcJWl9zsZZJzkFv6TNSMnDzSss"
Note:          Some DNS managers add quotes automatically. A single set
               is needed.

Please press <Enter> after you've created and verified the record

```

The screenshot shows the GoDaddy DNS Records interface for the domain **group12.online**. The 'DNS Records' tab is selected. A red arrow points from the 'Name' input field in the 'New Records' table to the 'Name' input field in the GoDaddy interface. Another red arrow points from the 'Value' input field in the GoDaddy interface to the 'Value' input field in the 'New Records' table.

Type *	Name *	Value *	TTL
TXT	_acme-challenge.mail.group12.or	lbcJWI9zsZZJzkFv6TNSMnDzSss	1 Hour

```

Select win-acme 2.2.9.1701
[group12.online] [192.168.12.2] No TXT records found
[group12.online] [192.168.12.1] No TXT records found
[group12.online] Preliminary validation failed on all nameservers
[group12.online] Will retry in 30 seconds (retry 9/10)...
[group12.online] [192.168.12.2] No TXT records found
[group12.online] [192.168.12.1] No TXT records found
[group12.online] Preliminary validation failed on all nameservers
[group12.online] Will retry in 30 seconds (retry 10/10)...
[group12.online] [192.168.12.2] No TXT records found
[group12.online] [192.168.12.1] No TXT records found
[group12.online] Preliminary validation failed on all nameservers
[group12.online] It looks like validation is going to fail, but we will try now anyway...
[group12.online] Authorization result: valid

Domain:          group12.online
Record:         _acme-challenge.group12.online
Type:          TXT
Content:        "-lxa9LHztFvxGN-NXiVd_OBMkC0QIwXlCOY546q6Kc"
Please press <Enter> after you've deleted the record
[group12.online] Record -lxa9LHztFvxGN-NXiVd_OBMkC0QIwXlCOY546q6Kc deleted
[mail.group12.online] Authorizing...
[mail.group12.online] Authorizing using dns-01 validation (Manual)

Domain:          mail.group12.online
Record:         _acme-challenge.mail.group12.online
Type:          TXT
Content:        "-asp3y5RntzfPSmIbcJWl9zsZZJzkFv6TNSMnDzSss"
Note:          Some DNS managers add quotes automatically. A single set
               is needed.

Please press <Enter> after you've created and verified the record

```

- When you create a **txt** record **save it**.
- Come back Exchange Server and press Enter then you can see option for choose you can select **1** or **2** either.
- It will take time to run command and end you authorization result: **valid**
- Then you see instructions bellow ‘**press enter after deleted the record**’ from godaddy.com
- Delete **TXT** record from godaddy whatever you made early.
- Press Enter.

```

Select win-acme 2.2.9.1701
[mail.group12.online] Preliminary validation failed on all nameservers
[mail.group12.online] Will retry in 30 seconds (retry 5/10)...
[mail.group12.online] [192.168.12.2] No TXT records found
[mail.group12.online] [192.168.12.1] No TXT records found
[mail.group12.online] Preliminary validation failed on all nameservers
[mail.group12.online] Will retry in 30 seconds (retry 6/10)...
[mail.group12.online] [192.168.12.2] No TXT records found
[mail.group12.online] [192.168.12.1] No TXT records found
[mail.group12.online] Preliminary validation failed on all nameservers
[mail.group12.online] Will retry in 30 seconds (retry 7/10)...
[mail.group12.online] [192.168.12.2] No TXT records found
[mail.group12.online] [192.168.12.1] No TXT records found
[mail.group12.online] Preliminary validation failed on all nameservers
[mail.group12.online] Will retry in 30 seconds (retry 8/10)...
[mail.group12.online] [192.168.12.2] No TXT records found
[mail.group12.online] [192.168.12.1] No TXT records found
[mail.group12.online] Preliminary validation failed on all nameservers
[mail.group12.online] Will retry in 30 seconds (retry 9/10)...
[mail.group12.online] [192.168.12.2] No TXT records found
[mail.group12.online] [192.168.12.1] No TXT records found
[mail.group12.online] Preliminary validation failed on all nameservers
[mail.group12.online] Will retry in 30 seconds (retry 10/10)...
[mail.group12.online] [192.168.12.2] No TXT records found
[mail.group12.online] [192.168.12.1] No TXT records found
[mail.group12.online] Preliminary validation failed on all nameservers
[mail.group12.online] It looks like validation is going to fail, but we will try now anyway...
[mail.group12.online] Authorization result: valid

Domain: mail.group12.online
Record: _acme-challenge.mail.group12.online
Type: TXT
Content: "aspp3y5yRNtzfpSmHbcJWl9zsZZJzkFv6TNSMnD2Sss"

Please press <Enter> after you've deleted the record

```

- When you press the enter you can bellow screen then choose ‘**n**’ for no any specify the user the task will run as.
- Then you can see Certificate details on next screen

```

You may manually update the bindings if you want IIS to be configured in a different way.
Adding new https binding :443:group12.online
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.
Adding new http binding :443:autodiscover.group12.online
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.
Adding Task Scheduler entry with the following settings
- Name win-acme renew (acme-v02.api.letsencrypt.org)
- Path C:\lets Encrypt SSL
- Command wacs.exe --renew --baseuri "https://acme-v02.api.letsencrypt.org/"
- Start at 00:00:00
- Random delay 04:00:00
- Time limit 02:00:00
Do you want to specify the user the task will run as? (y/n*) - no

```

- Choose ‘**Q**’ for Quit

```

You may manually update the bindings if you want IIS to be configured in a different way.
Adding new https binding :443:autodiscover.group12.online
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.
Adding new https binding :443:autodiscover.group12.online
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.
Adding Task Scheduler entry with the following settings
- Name win-acme renew (acme-v02.api.letsencrypt.org)
- Path C:\lets Encrypt SSL
- Command wacs.exe --renew --baseuri "https://acme-v02.api.letsencrypt.org/"
- Start at 00:00:00
- Random delay 04:00:00
- Time limit 02:00:00
Do you want to specify the user the task will run as? (y/n*) - no
Adding renewal for Certificate
Next renewal due after 2024/01/25
Certificate Certificate created

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (@ currently due)
A: Manage renewals (t total)
O: More options...
Q: Quit

Please choose from the menu:

```

- You can check multiple way to certificate added or not here are steps:

- Open Exchange Admin Center >Certificates

The screenshot shows the Exchange Admin Center interface. On the left, there's a navigation pane with various categories like recipients, servers, and protection. The 'servers' category is selected. In the main content area, there's a table titled 'Certificates'. The first row, which has a red box around it, represents a certificate issued by 'Let's Encrypt' on August 31, 2024, valid until November 28, 2024. The table includes columns for NAME, STATUS, and EXPIRE ON.

- Open OWA and check certificate

The screenshot shows the OWA interface with a blue background featuring the Microsoft logo. Overlaid is a 'Certificate Viewer' window for 'group12.online'. The 'General' tab is selected. A red box highlights the 'Issued By' section, which shows the certificate was issued by 'R10' (Let's Encrypt). Other details shown include the common name 'group12.online', SHA-256 fingerprints, and certificate expiration dates.

- Open internet Information Services (IIS) Manager.

The screenshot shows the IIS Manager interface. The left pane shows a tree structure with 'MAIL (GROUP12.administrative)' selected. The right pane shows the 'Default Web Site Home' page. Under the 'Actions' pane, there's a 'Bindings...' button highlighted with a red box.

The screenshot shows the 'Site Bindings' page in the IIS Manager. It lists various bindings for the 'Default Web' site, including multiple entries for 'https://mail.group12.online' and one for 'http://mail.group12.online'. A red box highlights this list of bindings.