

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/...](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

Source plugin IIS not available: No supported version of IIS detected.

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: **tot-doyu2025.ddo.jp**

Source generated using plugin Manual: tot-doyu2025.ddo.jp

Friendly name '[Manual] tot-doyu2025.ddo.jp'. <Enter> to accept or type desired name:

<Enter>

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)?: **1**

Description: Root path of the site that will serve the HTTP validation requests.

Path: **D:\WebSaver\certs**

Description: Copy default web.config to the .well-known directory.

Default: False

Argument: False (press <Enter> to use this)

Copy default web.config before validation? (y/n*) - **<Enter>**

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?: **2**

Description: .pem files are exported to this folder.

File path: **D:\WebSaver\certs**

Description: Password to set for the private key .pem file.

- 1: None
- 2: Type/paste in console
- 3: Search in vault

Choose from the menu: **1**

- 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?: **<Enter>**

Installation plugin IIS not available: No supported version of IIS detected.

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?: **3**

Terms of service:

C:\ProgramData\win-acme\acme-v02.api.letsencrypt.org\LE-SA-v1.6-August-18-2025.pd

f

Open in default application? (y/n*) - **<Enter>**

Do you agree with the terms? (y*/n) - **yes**

Enter email(s) for notifications about problems and abuse (comma-separated):

doyu2025@outlook.jp

ここまででは入力できましたが、これ以上は実際のサーバ機でないと設定できませんでした。

以下はコパイロットに聞いた入力内容です。

上記のメールアドレス入力のところから win- acme の次のステップ(手順書用)

以下は、メールアドレスを入力して Enter を押した後に win- acme が必ず実行する処理の流れです。

Let's Encrypt(win- acme)証明書発行手順書

— HTTP-01 認証方式(Apache / XAMPP 用)—

1. ACME アカウント登録

1. メールアドレス入力画面が表示される。

コード

Enter email(s) for notifications about problems and abuse (comma-separated): **doyu2025@outlook.jp**

2. 通知を受け取りたいメールアドレスを入力し、**Enter** を押す。
3. 次のメッセージが表示され、ACME アカウント登録が開始される。

コード

Registering account...

4. 利用規約への同意を求められる。

コード

Do you agree with the terms? (y*/n)

5. **y** を入力して **Enter** を押す。
6. アカウント登録完了メッセージが表示される。

コード

Account registered!

2. ドメイン認証開始 (Authorization Start)

対象ドメインの認証処理が開始される。

コード

[tot-doyu2025. ddo. jp] Authorizing...

3. HTTP-01 チャレンジ実行

win- acme は自動的に HTTP-01 を選択し、認証用ファイルを作成する。

コード

[tot-doyu2025. ddo. jp] Authorizing using http-01 validation (FileSystem)

Answer should now be browsable at:

http://tot-doyu2025. ddo. jp/. well-known/acme-challenge/xxxxxxxxxxxxxxxxxxxx
xxxx

※ xxxxxxxxxxxxxxxxxxxxxxxxxx は毎回異なるトークン。

4. 認証結果 (成功 / 失敗)

4-1. 認証成功時

コード

```
Preliminary validation succeeded  
[tot-doyu2025.ddo.jp] Authorization result: valid
```

4-2. 認証失敗時(例:DNS エラー)

コード

```
Preliminary validation failed because 'An error occurred while sending the  
request.'  
[tot-doyu2025.ddo.jp] Authorization result: invalid  
[tot-doyu2025.ddo.jp]  
{  
  "type": "urn:iETF:params:acme:error:dns",  
  "detail": "DNS problem:  
NXDOMAIN looking up A for tot-doyu2025.ddo.jp - check that a DNS record  
exists for this domain",  
  "status": 400  
}
```

※ エラー内容は状況により異なる。

5. 証明書の発行と保存(成功時のみ)

認証成功後、証明書発行処理が開始される。

コード

```
Requesting certificate [tot-doyu2025.ddo.jp]
```

選択した保存形式(PEM)に従い、証明書ファイルが出力される。

コード

```
Saving certificate to D:\WebSaver\certs  
Exporting .pem files...  
- cert.pem  
- chain.pem  
- fullchain.pem  
- privkey.pem
```

6. インストールステップ(今回はスキップ)

追加のインストール処理を選択しなかった場合：

コード

No installation steps chosen

7. 自動更新タスクの登録

Windows タスクスケジューラに自動更新タスクが登録される。

コード

Adding renewal for [tot-doyu2025.ddo.jp]

8. 完了メッセージ

全処理が完了すると、次のメッセージが表示される。

コード

Done!

以上で手順書は完成です。