



LUNDS
UNIVERSITET

WIN-ACME

MORGAN PERSSON, LUNDS UNIVERSITET, 2022-03-29



Varför WIN-ACME

- Började med Posh-ACME för ett par år sedan
 - Stöd för många DNS-tjänster
 - Man får göra schemaläggning och installation själv
 - Måste vara rätt version av PowerShell
- Letade efter alternativ
 - Fri programvara (för Windows)
 - Gärna mer funktionalitet



WIN-ACME

- Fri programvara (Apache License 2.0)
- Många sätt att verifiera (HTTP/HTTPS/DNS/m.m.)
- Kan dela port med IIS (http.sys)
- Stöd för flera olika certifikatutfärdare (även Sectigo)
- Automatisk schemaläggning och installation
- Enkel att anpassa efter behov

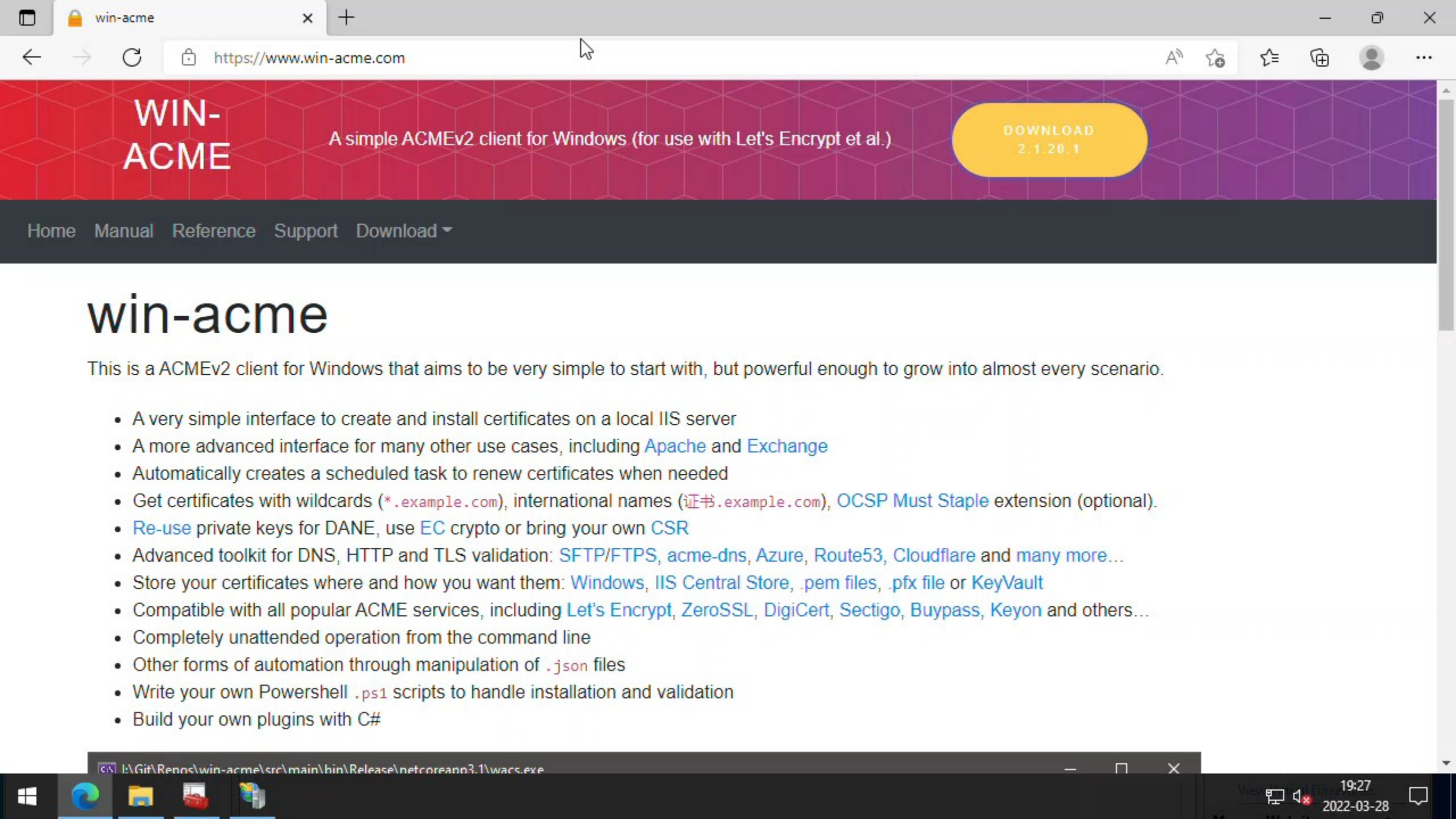
<https://www.win-acme.com>



DEMO



LUNDS
UNIVERSITET



win-acme

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.

- 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#](#)

Kommandorad

wacs.exe

--source manual

--host print.net.lth.se --friendlyname print

--store certificatestore --certificatestore My

--installation iis --installationsiteid 1



ImportRDP.ps 1

```
param([Parameter(Mandatory=$true)] $CertThumbprint)
```

```
Get-CimInstance -ClassName 'Win32_TSGeneralSetting'  
-Namespace 'root\CIMV2\TerminalServices' | Set-CimInstance  
-Property @{SSLCertificateSHA1Hash=$CertThumbprint}
```



Kommandorad (IIS och RDP)

wacs.exe

--source manual

--host print.net.lth.se --friendlyname print

--store certificatestore --certificatestore My

--installation iis,script --installationsiteid 1

--script "C:\Script\ImportRDP.ps1"

--scriptparameters "{CertThumbprint}"



Behörighet till certifikat

- Tjänster som kör under ett tjänstekonto kan behöva behörighet till certifikatet
- Går att lösa med kommandorad
`wacs --acs-fullcontrol "konto"`

<https://www.win-acme.com/manual/advanced-use/examples/exchange>



Frågor?

Morgan Persson
morgan.persson@lth.lu.se
046-222 75 14



LUNDS
UNIVERSITET