



In this article

Prerequisites

- Step 1: Log in with RDP into Windows Server 2019
- Step 2: Download Let's Encrypt client
- Step 3: Run Win-acme Let's Encrypt client
- Step 4: Create a batch file
- Step 5: Issue certificate
- Step 6: Enable SSL if it's not enabled yet
- Step 7: Configure SSL for the newly issued certificate.
- Step 8: Verify that SSL is working



Install Let's Encrypt with Apache 2.4 on Windows Server 2019

Find answers to frequently asked questions here.



[Support](#) ▶ [Initial Setup](#) ▶ Install Let's Encrypt with Apache 2.4 on Windows Server 2019

Estimated reading time: 3 min

Introduction

In this article, we will help you to configure a Let's Encrypt client on Windows Server 2019 and how you can enable and configure your SSL certificate on your Apache webserver.

Prerequisites

- VPS or Dedicated Server with Windows Server 2019 installed.
- You must be logged in via Remote Desktop Protocol as an administrative user.
- Installed Apache 2.4 in `C:\Apache24`
- A domain name pointed towards your VPS or Dedicated server. In this tutorial, we will use `s30426.hosted-by-snel.com`. Replace all occurrences of `s30426.hosted-by-snel.com` with your actual domain name.

Step 1: Log in with RDP into Windows Server 2019

Connect to your server with the login credentials which you can find in your [client area](#).

Step 2: Download Let's Encrypt client

We will use Win-acme for issuing an SSL certificate. Visit the website of Win-acme to download the latest version. Extract the download zip to `C:\win-acme`

Step 3: Run Win-acme Let's Encrypt client

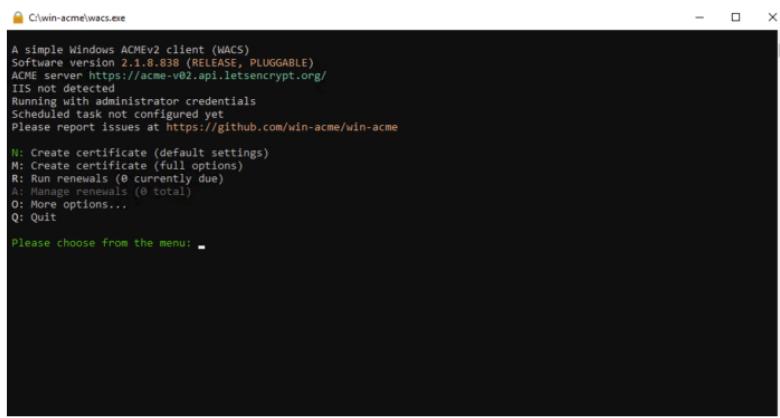
Start `wacs` with administrator permission. If Microsoft Defender SmartScreen is enabled it will ask your permission.



Click on `More info`. A new button will appear and click on `Run anyway`.



Win-acme will start



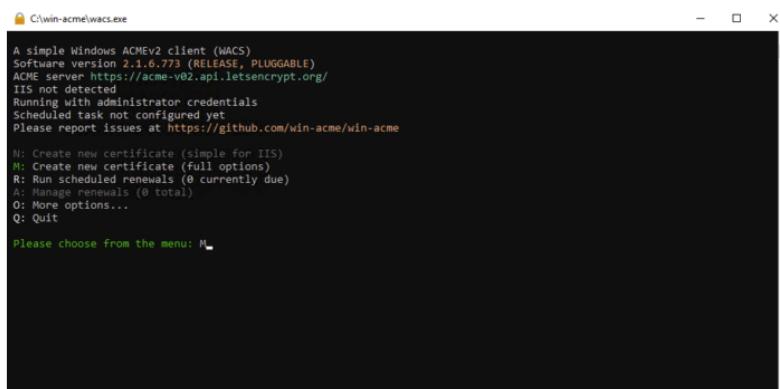
Step 4: Create a batch file

Create the following filename `C:\win-acme\Scripts\RestartApache.bat`

```
net stop "Apache2.4" & sc start "Apache2.4"
```

Step 5: Issue certificate

Enter `M` in the command prompt en hit enter.



Choose `manual input` in our situation, it's option 1.



Manual-input can be a different number in your setup

```
C:\win-acme\wacs.exe
IIS not detected
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: Manual input
2: CSR created by another program
C: Abort

How shall we determine the domain(s) to include in the certificate?: 1
Enter comma-separated list of host names, starting with the common name: ..
```

Enter the domain name where you want to issue a certificate. In our article it's: `s30426.hosted-by-snel.com`

```
C:\win-acme\wacs.exe
IIS not detected
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: Manual input
2: CSR created by another program
C: Abort

How shall we determine the domain(s) to include in the certificate?: 1
Enter comma-separated list of host names, starting with the common name: s30426.hosted-by-snel.com..
```

It will ask you for a friendly name, we leave it blank. Hit enter to continue.

```
C:\win-acme\wacs.exe
IIS not detected
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: Manual input
2: CSR created by another program
C: Abort

How shall we determine the domain(s) to include in the certificate?: 1
Enter comma-separated list of host names, starting with the common name: s30426.hosted-by-snel.com

Target generated using plugin Manual: s30426.hosted-by-snel.com

Suggested friendly name: '[Manual] s30426.hosted-by-snel.com', press <ENTER> to accept or type an alternative: ..
```

It will ask how you want to verify that you are the owner of that domain. In our case, `s30426.hosted-by-snel.com` is already pointing to our server and is active in Apache. In our setup, we choose option 1

`[http-01] Serve verification files on (network) path .`

```
C:\win-acme\wacs.exe
How shall we determine the domain(s) to include in the certificate?: 1
Enter comma-separated list of host names, starting with the common name: s30426.hosted-by-snel.com

Target generated using plugin Manual: s30426.hosted-by-snel.com

Suggested friendly name: '[Manual] s30426.hosted-by-snel.com', 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?: 1
```

Since we have chosen network path it will ask us for a path, in our case its `C:\Apache24\htdocs`

```

C:\Win-acme\wacs.exe
Please choose from the menu: M
[INFO] Running in mode: Interactive, Advanced
1: Manually input host names
<Enter> Abort
Which kind of certificate would you like to create?: 1
Enter comma-separated list of host names, starting with the common name: [REDACTED]
[INFO] Target generated using plugin Manual:
Suggested FriendlyName is '[Manual] reSalicesp.eu', press enter to accept or type an alternative: <Enter>
1: [dns-01] CNAME the record to a server that supports the acme-dns API
2: [dns-01] Manually create record
3: [dns-01] Run script to create and update records
4: [http-01] Host the verification file from memory (recommended)
5: [http-01] Save file on local or network path
6: [http-01] Upload verification file via WebDav path
7: [http-01] Upload verification files via FTP(S)
8: [http-01] Upload verification files via SSH-FTP
C: Abort

How would you like to validate this certificate?: 5
Path to the root of the site that will handle authentication: [REDACTED]

```

It will ask you if you want to copy the default web.config before validation. We choose **N**

```

C:\Win-acme\wacs.exe
Please choose from the menu: M
[INFO] Running in mode: Interactive, Advanced
1: Manually input host names
<Enter> Abort
Which kind of certificate would you like to create?: 1
Enter comma-separated list of host names, starting with the common name: [REDACTED]
[INFO] Target generated using plugin Manual:
Suggested FriendlyName is '[Manual] reSalicesp.eu', press enter to accept or type an alternative: <Enter>
1: [dns-01] CNAME the record to a server that supports the acme-dns API
2: [dns-01] Manually create record
3: [dns-01] Run script to create and update records
4: [http-01] Host the verification files from memory (recommended)
5: [http-01] Save file on local or network path
6: [http-01] Upload verification file to local or network path
7: [http-01] Upload verification files via FTP(S)
8: [http-01] Upload verification files via SSH-FTP
C: Abort

How would you like to validate this certificate?: 5
Path to the root of the site that will handle authentication: [REDACTED]
Copy default web.config before validation? (y/n*) [REDACTED]

```

It will ask what type of private key we want. We will choose option 2 **RSA key** as a private key.

```

C:\Win-acme\wacs.exe
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/johoi/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

```

Since we want to use the SSL certificate on our Apache webserver we will choose option 2

PEM encoded files (Apache, nginx, etc.) and hit enter. Once PEM is selected it will ask you where to store those files. In our case it's **C:\Apache24\conf**.

```

C:\Win-acme\wacs.exe
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?: 2
Path to folder where .pem files are stored: C:\Apache24\conf

```

We do not want to store it another way and we select option 3 **No (additional) store steps** and hit enter.

```

C:\win-acme\wacs.exe
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?: 2

Path to folder where .pem files are stored: C:\Apache24\conf

1: IIS Central Certificate Store (.pfx per domain)
2: Windows Certificate Store
3: No (additional) store steps
C: Abort

Would you like to store it in another way too?: 3

```

Once the new certificate is saved we do want to perform an extra step and choose for option 3

Start external script or program. It will ask the script path that you want to run after renewal
C:\win-acme\Scripts\RestartApache.bat.

```

C:\win-acme\wacs.exe
4: No (additional) store steps
C: Abort

How would you like to store the certificate?: 2

Path to folder where .pem files are stored: C:\Apache24\conf

1: IIS Central Certificate Store (.pfx per domain)
2: Windows Certificate Store
3: No (additional) store steps
C: Abort

Would you like to store it in another way too?: 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?: 3

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

Enter the path to the script that you want to run after renewal: C:\win-acme\Scripts\RestartApache.bat

```

Enter the following **{StoreType} {StorePath} {RenewalId}**. Once this is entered it will ask where you want to receive notification and fill in your email address.

```

C:\win-acme\wacs.exe
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?: 3

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

Enter the path to the script that you want to run after renewal: C:\win-acme\Scripts\RestartApache.bat

(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}": {StoreType} {StorePath} {RenewalId}

Enter email(s) for notifications about problems and abuse (comma separated): snel.com

Terms of service: C:\ProgramData\win-acme\acme-v02.api.letsencrypt.org\LE-SA-v1.2-November-15-2017.pdf

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

```

It will ask you if you want to open in default application choose for N and accept the terms with Y.

```

C:\win-acme\wacs.exe
3: Start external script or program
4: No (additional) installation steps

Which installation step should run first?: 3

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

Enter the path to the script that you want to run after renewal: C:\win-acme\Scripts\RestartApache.bat

(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}": {StoreType} {StorePath} {RenewalId}

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

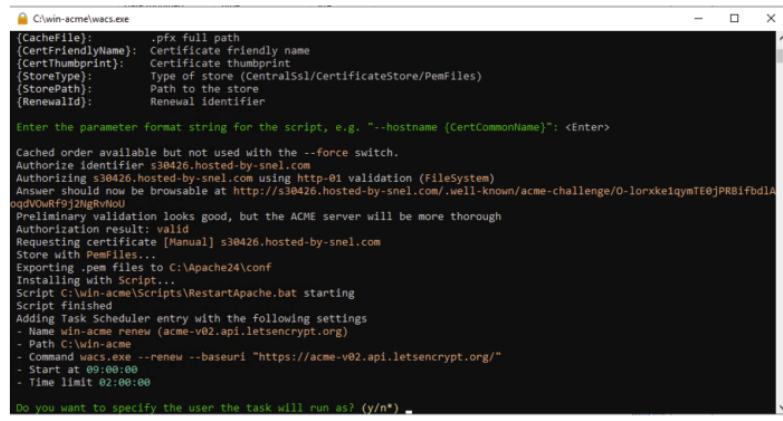
Terms of service: C:\ProgramData\win-acme\acme-v02.api.letsencrypt.org\LE-SA-v1.2-November-15-2017.pdf

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

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

```

Run the task under a specific user, since it requires a user with administrator permissions.



```
[CacheFile]: .pfx full path
[CertFriendlyName]: Certificate friendly name
[CertThumbprint]: Certificate thumbprint
[StoreType]: Type of store (CentralSsl/CertificateStore/PemFiles)
[StorePath]: Path to the store
[RenewId]: Renewal identifier

Enter the parameter format string for the script, e.g. "--hostname {CertCommonName}": <Enter>

Cached order available but not used with the --force switch.
Authorize identifier s30426.hosted-by-snel.com
Authorizing s30426.hosted-by-snel.com via http-01 validation (FileSystem)
Authorization result can be browsable at http://s30426.hosted-by-snel.com/.well-known/acme-challenge/O-lorxke1qymTE0jPRB1fbdlA
pgDwOkRfjzNgRvN0U
Preliminary validation looks good, but the ACME server will be more thorough
Authorization result: valid
Requesting certificate [Manual] s30426.hosted-by-snel.com
Store with PemFiles..
Exporting .pem files to C:\Apache24\conf
Installing with Script...
Script C:\win-acme\Scripts\RestartApache.bat starting
Script finished
Adding Task Scheduler entry with the following settings
- Name win-acme renew (acme-v02.api.letsencrypt.org)
- Path C:\win-acme
- 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)
```

Step 6: Enable SSL if it's not enabled yet

If SSL is already enabled for your Apache webserver you can continue to step 7. Open the httpd configuration file `C:/Apache24/conf/httpd.conf`. In the httpd.conf file changes the following lines by removing the comment sign `#`:

```
Loadmodule ssl_module modules/mod_ssl.so
Include conf/extra/httpd-default.conf
Include conf/extra/httpd-ssl.conf
```

Do an Apache configuration file check. Start command prompt with administration permission. Run the following command:

```
cd C:\Apache24\bin
httpd.exe -t
```

The output should give Syntax OK if there is no error in the configuration file.

Step 7: Configure SSL for the newly issued certificate.

Open the httpd-ssl configuration file located here `C:/Apache24/conf/extra/httpd-ssl.conf`.

Change the SSLCertificateFile:

```
SSLCertificateFile "${SRVROOT}/conf/server.crt"
```

with

```
SSLCertificateFile "${SRVROOT}/conf/s30426.hosted-by-snel.com-chain.pem"
```

Change the SSLCertificateKeyFile :

```
SSLCertificateKeyFile "${SRVROOT}/conf/server.key"
```

with

```
SSLCertificateKeyFile "${SRVROOT}/conf/s30426.hosted-by-snel.com-key.pem"
```

Change the SSLCipherSuite:

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4:!3DES
SSLProxyCipherSuite HIGH:MEDIUM:!MD5:!RC4:!3DES
```

with

```
SSLCipherSuite ECDH+AESGCM256:ECDH+CHACHA20:DH+AESGCM256:ECDH+AES256:DH+AES256:!aNULL:!MD5:!DS8
SSLProxyCipherSuite ECDH+AESGCM256:ECDH+CHACHA20:DH+AESGCM256:ECDH+AES256:DH+AES256:!aNULL:!MD5:!DS8
```

Change SSL protocol

```
SSLProtocol all -SSLv3
SSLProxyProtocol all -SSLv3
```

With

```
SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1
SSLProxyProtocol all -SSLv3 -TLSv1 -TLSv1.1
```

Change VirtualHost

```
# General setup for the virtual host
DocumentRoot "${SRVROOT}/htdocs"
ServerName www.example.com:443
ServerAdmin admin@example.com
ErrorLog "${SRVROOT}/logs/error.log"
TransferLog "${SRVROOT}/logs/access.log"
```

With

```
# General setup for the virtual host
DocumentRoot "${SRVROOT}/htdocs"
ServerName s30426.hosted-by-snel.com:443
ServerAdmin <example@example.com>
ErrorLog "${SRVROOT}/logs/error.log"
TransferLog "${SRVROOT}/logs/access.log"
```

Save the changes. Re-check the Apache configuration on the command prompt. Start command prompt with administration permission. Run de following command:

```
cd C:/Apache24/bin
httpd.exe -t
```

If everything is OK. Restart Apache webserver via command prompt. Start command prompt with administration permission. Run de following command:

```
cd C:/Apache24/bin
httpd -k restart
```

Step 8: Verify that SSL is working

Visit the website on your browser: <https://s30426.hosted-by-snel.com>

Conclusion

In this article, we described how you can install a Let's Encrypt client and configure Apache webserver on Windows to use the issued SSL certificate.

Was this article helpful?

 Like 8  Dislike 0

Views: 23370

Comments



Antonio Pereira says
Thursday, August 20th, 2020 at 15:53

Hello,

Great article it got me up and going. Is there a way to automatically renew certificates after 90 days.

Thanks

[Reply](#)



Ahmet Bas says
Thursday, August 20th, 2020 at 15:59

WinAcme will create a renewal task if you followed our article as described in step 6: "Run the task under a specific user, since it requires a user with administrator permissions.". Which will perform a restart of the Apache server after a successful renewal.

[Reply](#)



Antonio Pereira says

Friday, August 21st, 2020 at 21:15

I must of skipped that test. I see the the restartapache.bat file but its empty. Is there a way i can manually add the entries in the batch file and then i assume i will have to add a windows task scheduler to run it every 90 days.

[Reply](#)



Ahmet Bas says

Monday, August 24th, 2020 at 10:05

We created the restartapache.bat ourselves which can be found in step 4, where you can see the content of it. You can go over the process and make the changes you need to make.

[Reply](#)



Ryan says

Tuesday, November 10th, 2020 at 16:31

Forbidden

You don't have permission to access this resource.
I get this error after configuring everything right.

[Reply](#)



Irma yanet says

Monday, March 1st, 2021 at 20:35

Great !!! I configured Apache for Django and all work fine. Only I had to do a change, I removed the comment sign # at the line :
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
and all work excellent.
You don't forget to add a permit rule in windows firewall, with a port 443.

[Reply](#)



Yaniv says

Saturday, June 5th, 2021 at 16:19

Thank you! works like magic 😊

[Reply](#)



Sarooj Z says



Sarooj Z says

Monday, November 22nd, 2021 at 11:19

You are a star!

While configuring at end of step 5 I provided invalid credential and I could not set task to run automatically renew certificates. How can I go back to that step? Appriciate your assistance.

[Reply](#)

Ahmet Bas says

Monday, November 22nd, 2021 at 11:51

If you open Win-acme client and click on "More Options" you can "(Re)create scheduled task" which should help you to change values.

[Reply](#)

Sarooj Z says

Monday, November 22nd, 2021 at 12:16

Thanks so much...

[Reply](#)

Pavel says

Monday, February 28th, 2022 at 15:10

You made my day!

Thank you so much.

[Reply](#)

Raul Chiarella says

Tuesday, March 29th, 2022 at 19:19

How can i do this procedure on Windows Server Core passing parameters only?

[Reply](#)

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website



Post Comment

**Deploy your Cloud VPS
within 2 minutes**

Become a Snel.com customer today

Get started



9.8/10 Reviews

Contact us

+31 88 3 088 099

Our Products

- Domain name
- Professional Web Hosting
- Reseller Hosting
- Microsoft 365
- Managed Servers
 - Managed Cloud VPS
 - Managed Pure Performance VPS
 - Managed Azure VPS
 - Managed Dedicated Servers
- Self-managed Servers
 - Cloud VPS
 - Pure Performance VPS
 - Enterprise Dedicated Servers
 - Budget Dedicated Servers

More...

- Our Story
- Contact Us
- Reviews
- ISO Certification
- Data Center
- Network
- Snel Status
- Payment Methods
- SnelWallet
- Affiliate Program

Legal

- Service Level Agreement
- EU GDPR
- Disclaimer
- Privacy Statement
- Terms and Conditions
- Data Processing Agreement
- Acceptable Usage Policy

Blog

- Snel.com guest at Next Level RTL Z
- Switching to IPv6 is adapted slower than expected
- Which Control Panel do you need?
- Migrate to Snel.com, fast and easy!
- Attention! How chaos is growing in your server landscape

Show us some love



Stay Updated

youremail@address.com

 Sign up

Snel Status

All systems operational

Copyright © 2022 Snel.com B.V. All Rights Reserved.