



Technical Note

TN569: Configuring Auto-Renewal Certificates on a Single Web Server in an On-Premises Symphia NowForce Installations

Publication Date: December 25, 2023

Products	Symphia NowForce On-Premises
Technical Note Type	User Guide
Exposure Level	Customer Facing
Description	This technical note provides the guidelines for configuring auto-renewal certificates on the web server in an Symphia NowForce On-Premises Installation.

Unauthorized use, duplication, or modification of this document in whole or in part without the written consent Intellicene Inc. is strictly prohibited. By providing this document, Intellicene Inc. is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice. Features listed in this document are subject to change. Contact your Intellicene representative for current product features and specifications. All marks referenced herein with the ® or TM symbol are registered trademark or trademarks of Intellicene Inc. or its subsidiaries. All rights reserved. All other marks are trademarks of their respective owners.

Contents

Contents	2
Overview	3
Prerequisites	3
Configuring Auto-Renewal SSL Certificate	4

Overview

This technical note describes how to configure a single Web Server running IIS 7.5 in your NowForce on-prem installation to automatically renew its SSL certificate. The process makes use of the open-source certificate authority, [Let's Encrypt](#) and an open-source tool [Win-Acme](#).

If your deployment contains more than one Web server, see *TN570 Configuring Auto-Renewal Certificates on Multiple Web Servers in an On-Premises Symphia NowForce Installation*.

Prerequisites

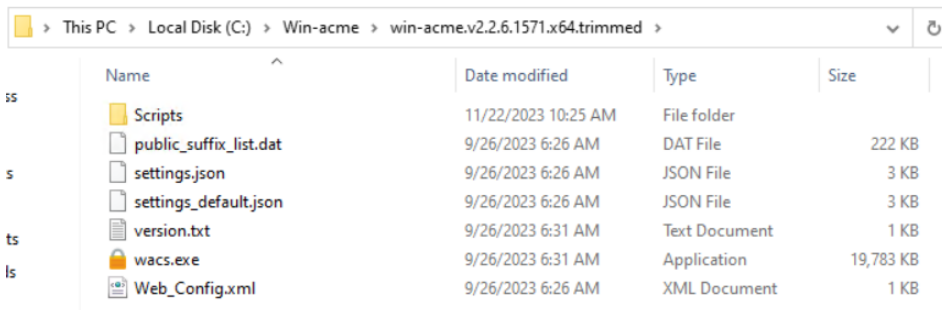
Ensure that you have all of the following prerequisites in place before you begin.

- Open port 80, and ensure that it is available and is not being used by any other process, for example IIS binding for HTTP.
- Your domain with DNS is configured for this web server .
- The IIS website with binding is configured for both HTTPS and for your domain.
- You have full administrative rights on the web server.

Configuring Auto-Renewal SSL Certificate

▼ To set auto-renewal certificate on your Windows Web Server

1. Download [Win-ACME](#) and extract the files to c:\win-acme.



A screenshot of a Windows File Explorer window showing the contents of the directory 'C:\Win-acme\win-acme.v2.2.6.1571.x64.trimmed'. The window title is 'This PC > Local Disk (C:) > Win-acme > win-acme.v2.2.6.1571.x64.trimmed'. The table below lists the files and folders in this directory.

Name	Date modified	Type	Size
Scripts	11/22/2023 10:25 AM	File folder	
public_suffix_list.dat	9/26/2023 6:26 AM	DAT File	222 KB
settings.json	9/26/2023 6:26 AM	JSON File	3 KB
settings_default.json	9/26/2023 6:26 AM	JSON File	3 KB
version.txt	9/26/2023 6:31 AM	Text Document	1 KB
wacs.exe	9/26/2023 6:31 AM	Application	19,783 KB
Web_Config.xml	9/26/2023 6:26 AM	XML Document	1 KB

2. Run wacs.exe.

```
C:\Win-acme\win-acme.v2.2.6.1571.x64.trimmed>wacs.exe

A simple Windows ACMEv2 client (WACS)
Software version 2.2.6.1571 (release, trimmed, 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
```

3. Enter n to create new certificate.

```
A simple Windows ACMEv2 client (WACS)
Software version 2.2.6.1571 (release, trimmed, 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: n

Running in mode: Interactive, Simple
```

- Select your website and binding, or alternatively choose all sites and all bindings as shown in the example below.

```
Running in mode: Interactive, Simple

Please select which website(s) should be scanned for host names. You may
input one or more site identifiers (comma-separated) to filter by those
sites, or alternatively leave the input empty to scan *all* websites.

1: demo.website.com (1 binding)

Site identifier(s) or <Enter> to choose all: <Enter>

1: sosmap.live (Site 1)

Listed above are the bindings found on the selected site(s). By default all
of them will be included, but you may either pick specific ones by typing the
host names or identifiers (comma-separated) or filter them using one of the
options from the menu.

P: Pick bindings based on a search pattern
A: Pick *all* bindings

Binding identifiers(s) or menu option: a

1: sosmap.live (Site 1)

Continue with this selection? (y*/n) - yes

Source generated using plugin IIS: sosmap.live
```

- If requested, accept terms of service and provide your email.

```
Terms of service: C:\ProgramData\win-acme\acme-v02.api.letsencrypt.org\LE-SA-v1.3-September-21-2022.pdf

Open in default application? (y/n*) - no

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

Enter email(s) for notifications about problems and abuse (comma-separated): a@a.com
```

- Review the output to confirm the tasks were successful.

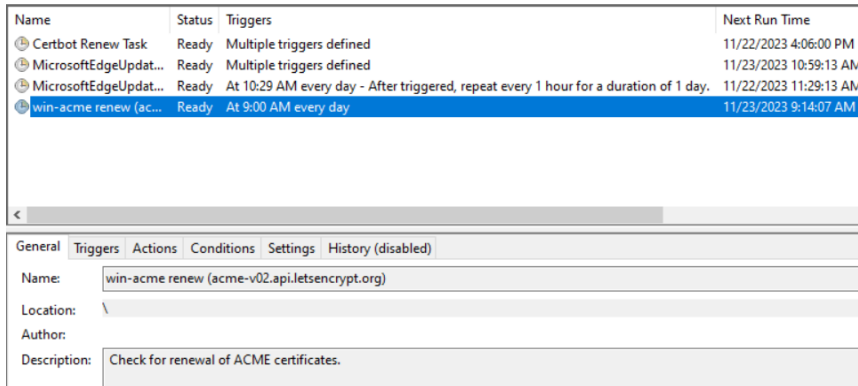
```
Plugin IIS generated source sosmap.live with 1 identifiers
Plugin Single created 1 order
[sosmap.live] Authorizing...
[sosmap.live] Authorizing using http-01 validation (SelfHosting)
[sosmap.live] Authorization result: valid
Downloading certificate [IIS] (any site), (any host)
Store with CertificateStore...
Installing certificate in the certificate store
Adding certificate [IIS] (any site), (any host) @ 2023/11/22 to store WebHosting
Installing with IIS...
Updating existing https binding sosmap.live:443 (flags: 0)
Committing 1 https binding changes to IIS while updating site 1
Adding Task Scheduler entry with the following settings
- Name win-acme renew (acme-v02.api.letsencrypt.org)
- Path C:\Win-acme\win-acme.v2.2.6.1571.x64.trimmed
- Command wacs.exe --renew --baseuri "https://acme-v02.api.letsencrypt.org/"
- Start at 09:00:00
- Random delay 04:00:00
- Time limit 02:00:00
Adding renewal for [IIS] (any site), (any host)
Next renewal due after 2024/1/16
Certificate [IIS] (any site), (any host) created
```

- From the Windows taskbar, open **Task Scheduler**.

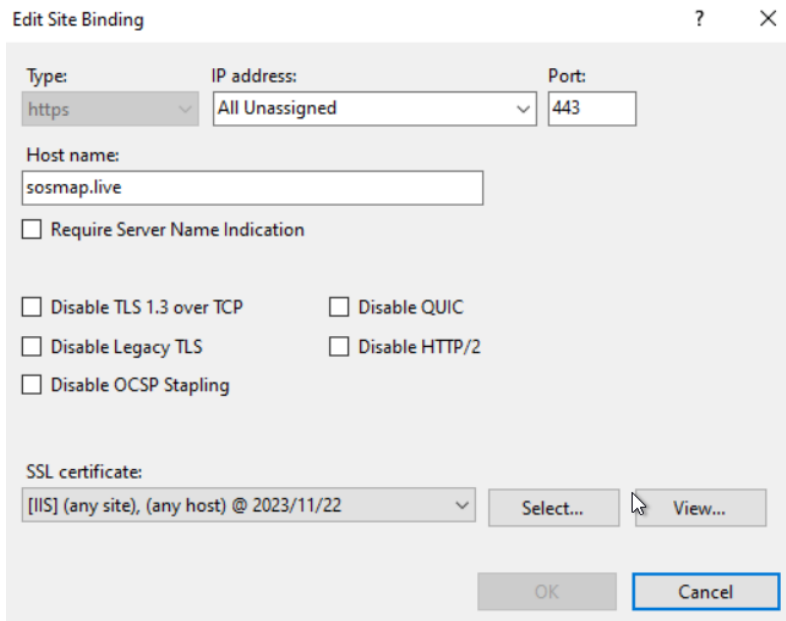
8. In **Task Scheduler Library**, stand on the task that was added **win-acme renew** and right click, select **Properties** to view the to display the task information.
9. Review the scheduled task to renew the certificate is created. Click **OK** to exit.

Note

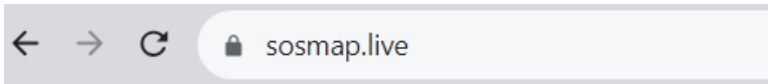
- The start time (Trigger) is set for 9 am daily.
- This task renews only when the certificate is about to expire, not every day.



10. In the Windows taskbar, open **IIS**.
11. Right-click on your **site name** and select **Edit Bindings**.
12. Double click the **site name** to display the **Edit Site Binding** window and click **View** to display the new certificate. Click **OK** to close.



- Open a Chrome browser and navigate to your website, confirm that the lock icon appears in adjacent to the site's URL. This is the indication that the site is now secured with an up to date certificate.



- Click on the  (lock icon) and navigate to **Connection is Secure** > **Certificate is valid** to display the certificate's details.

Certificate Viewer: sosmap.live ×

General Details

Issued To

Common Name (CN)	sosmap.live
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	R3
Organization (O)	Let's Encrypt
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Wednesday, November 22, 2023 at 6:09:56 PM
<u>Expires On</u>	Tuesday, February 20, 2024 at 6:09:55 PM

SHA-256 Fingerprints

Certificate	646b615a839f3d01170a6ee920d07696e23f3d803bf11abf2f1825fcd3c93856
Public Key	7772d8f55d925689576e8712698959ea7462341530b4904b0c76d5e79fb6ce6f