

Index

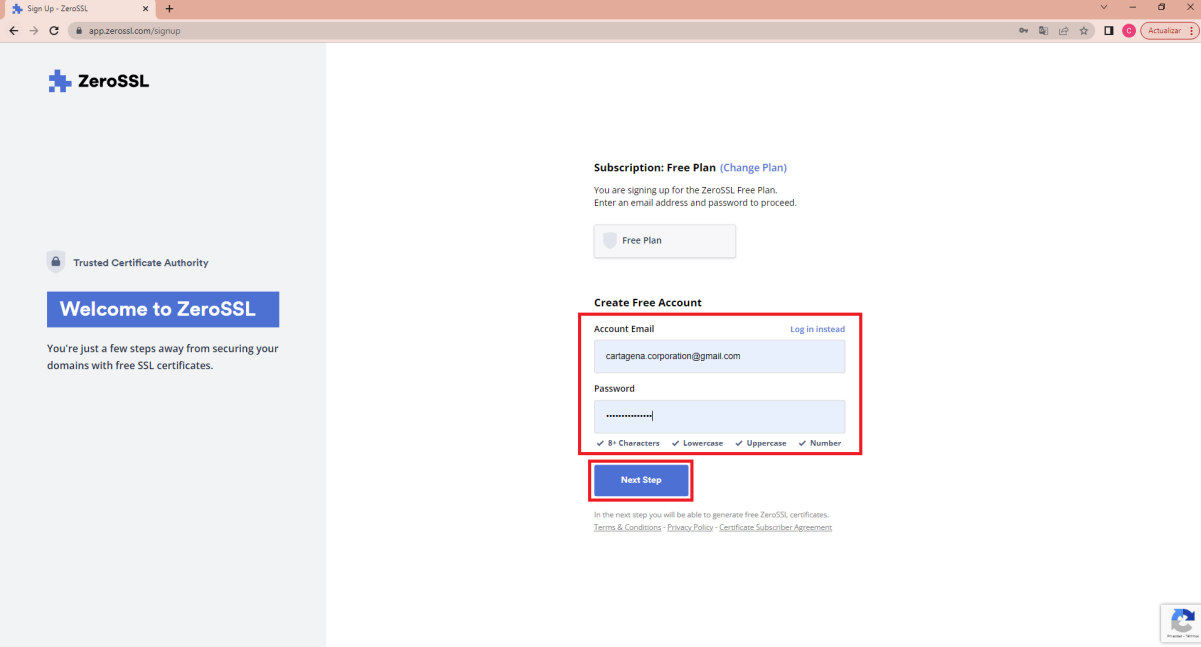
Requirements.....	2
Registro.....	3
Create an SSL Certificate.....	4
Verifying the ownership of the domain.....	7
Downloading the certificate.....	10
Installing the Certificate.....	12
Installing Open SSL.....	12
Converting from .crt to .pfx.....	13
Uploading the certificate to IIS.....	16
Adding the certificate to a website.....	18

Requirements

You have to had already bought a domain, for example saludtic.com, and you will need to have access to the email admin@saludtic.com

Registro

Get into <https://app.zeross.com/signup>, add mail and password, and then click on “Next Step”



The screenshot shows the ZeroSSL signup page in a web browser. The browser's address bar displays 'app.zeross.com/signup'. The page features the ZeroSSL logo and a 'Welcome to ZeroSSL' message. A 'Trusted Certificate Authority' badge is visible. The 'Subscription: Free Plan' section indicates the user is signing up for the Free Plan. The 'Create Free Account' section contains a red-bordered box around the 'Account Email' and 'Password' fields. The 'Account Email' field contains 'cartagena.corporation@gmail.com'. The 'Password' field is masked with dots. Below the password field, there are four checkmarks indicating password requirements: '8+ Characters', 'Lowercase', 'Uppercase', and 'Number'. A 'Next Step' button is located below the password field. At the bottom, there is a note about generating free ZeroSSL certificates and links to 'Terms & Conditions', 'Privacy Policy', and 'Certificate Subscriber Agreement'.

Sign Up - ZeroSSL

app.zeross.com/signup

Actualizar

ZeroSSL

Trusted Certificate Authority

Welcome to ZeroSSL

You're just a few steps away from securing your domains with free SSL certificates.

Subscription: Free Plan ([Change Plan](#))

You are signing up for the ZeroSSL Free Plan.
Enter an email address and password to proceed.

Free Plan

Create Free Account

Account Email [Log in instead](#)

cartagena.corporation@gmail.com

Password

.....

✓ 8+ Characters ✓ Lowercase ✓ Uppercase ✓ Number

Next Step

In the next step you will be able to generate free ZeroSSL certificates.
[Terms & Conditions](#) - [Privacy Policy](#) - [Certificate Subscriber Agreement](#)

Create an SSL Certificate

click on New Certificate

The screenshot shows the ZeroSSL dashboard in a web browser. The browser's address bar displays 'app.zerossl.com/dashboard'. The ZeroSSL logo is in the top left, and the user's email 'cartagena.corporation@gmail.com' is in the top right. A sidebar on the left contains links to 'Dashboard', 'Certificates', and 'Developer'. The main content area is titled 'Dashboard' and includes a 'Get Premium SSL' button. A 'Welcome to your dashboard' message is followed by a row of five status cards: 'Expiring Soon', 'Draft', 'Issued', 'Pending Validation', and 'Expired', each with a 'View All' link. Below these is a 'Your Subscription' section showing '0 / 3' 90-Day Certificates and '0 / 0' 1-Year Certificates, with a link to 'please upgrade your account'. The 'Create SSL Certificate' section explains that ZeroSSL allows creating certificates within minutes and highlights a red-bordered 'New Certificate' button. The 'Developer' section mentions unlimited access to the REST API and provides links to 'Developer Section' and 'API Documentation'. An 'Ayuda' button is in the bottom right corner.

Dashboard - ZeroSSL

app.zerossl.com/dashboard

ZeroSSL

Help Center Partner Program cartagena.corporation@gmail.com CA

Get Premium SSL

Dashboard

Certificates

Developer

Dashboard

Welcome to your dashboard

Thank you for your trust in ZeroSSL. Below you will find usage statistics, a short account summary as well as other resources to help you manage your SSL certificates.

Expiring Soon View All →

Draft View All →

Issued View All →

Pending Validation View All →

Expired View All →

Your Subscription

You can find your credits & usage on the right. For unlimited certificates and access to advanced SSL management tools, [please upgrade your account](#).

0 / 3 90-Day Certificates

0 / 0 1-Year Certificates

Create SSL Certificate

ZeroSSL lets you create SSL certificates within just a few minutes, supporting both 90-day and 1-year certificates. To create a certificate, click on the right.

New Certificate

Developer

You have unlimited access to our REST API, which lets you integrate ZeroSSL into your application and automate SSL certificate management.

Developer Section

API Documentation

Ayuda

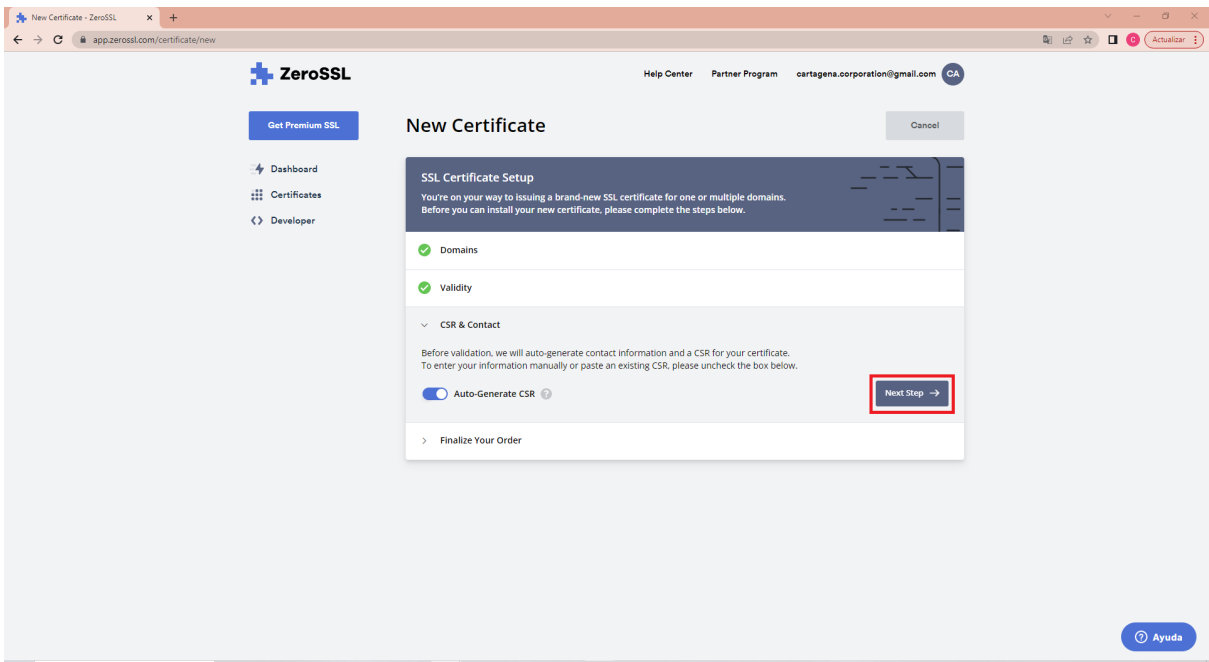
Then you need to add the domain that you already bought in godaddy or another domain seller, then “Next Step”

The screenshot shows the ZeroSSL 'New Certificate' setup page. The 'Domains' section is active, displaying a list of domains: 'saludtic2.com' and 'www.saludtic2.com', both marked with green checkmarks. A red box highlights the 'Next Step' button. The page also includes a sidebar with 'Dashboard', 'Certificates', and 'Developer' options, and a top navigation bar with 'Help Center', 'Partner Program', and 'cartagena.corporation@gmail.com'.

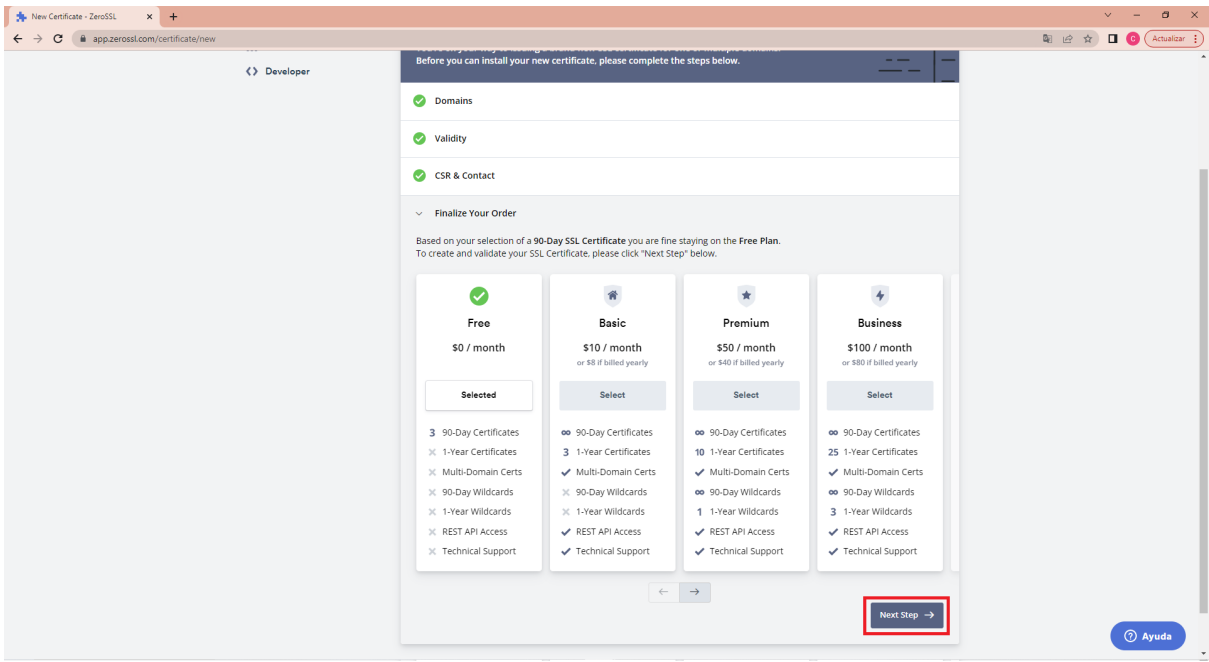
The 90 days certificates are **free**

The screenshot shows the ZeroSSL 'New Certificate' setup page. The 'Validity' section is active, displaying two options: '90-Day Certificate' (selected) and '1-Year Certificate'. A red box highlights the 'Next Step' button. The page also includes a sidebar with 'Dashboard', 'Certificates', and 'Developer' options, and a top navigation bar with 'Help Center', 'Partner Program', and 'cartagena.corporation@gmail.com'.

Leave the next option just as it is



The same here



Verifying the ownership of the domain

You will need to add the email admin of the domain that you bought, In the [video tutorial](#) there is an explanation in spanish about how to verify the domain without an admin email (Because you usually have to pay to have an email of your domain)

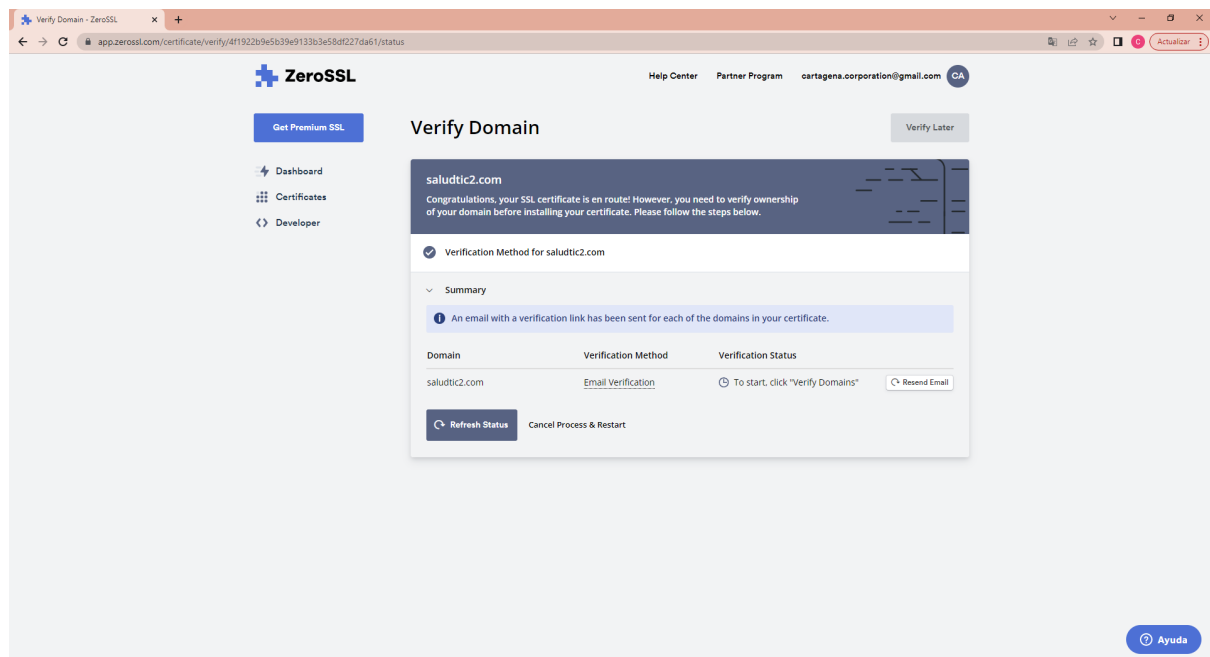
The screenshot shows the ZeroSSL 'Verify Domain' interface. A green message at the top states: 'Your certificate has been created and is ready for domain verification.' Below this, a section for 'saludtic2.com' explains that the SSL certificate is en route but ownership verification is required. Under 'Verification Method for saludtic2.com', the 'Email Verification' option is selected and highlighted with a red box. A dropdown menu shows 'admin@saludtic2.com' as the selected email address, also highlighted with a red box. Below the dropdown are radio buttons for 'DNS (CNAME)' and 'HTTP File Upload'. A 'Next Step ->' button is highlighted with a red box. The left sidebar contains links for 'Get Premium SSL', 'Dashboard', 'Certificates', and 'Developer'. The top navigation bar includes 'Help Center', 'Partner Program', and the user email 'cartagena.corporation@gmail.com'. A blue 'Ayuda' button is in the bottom right corner.

Click on verify domain

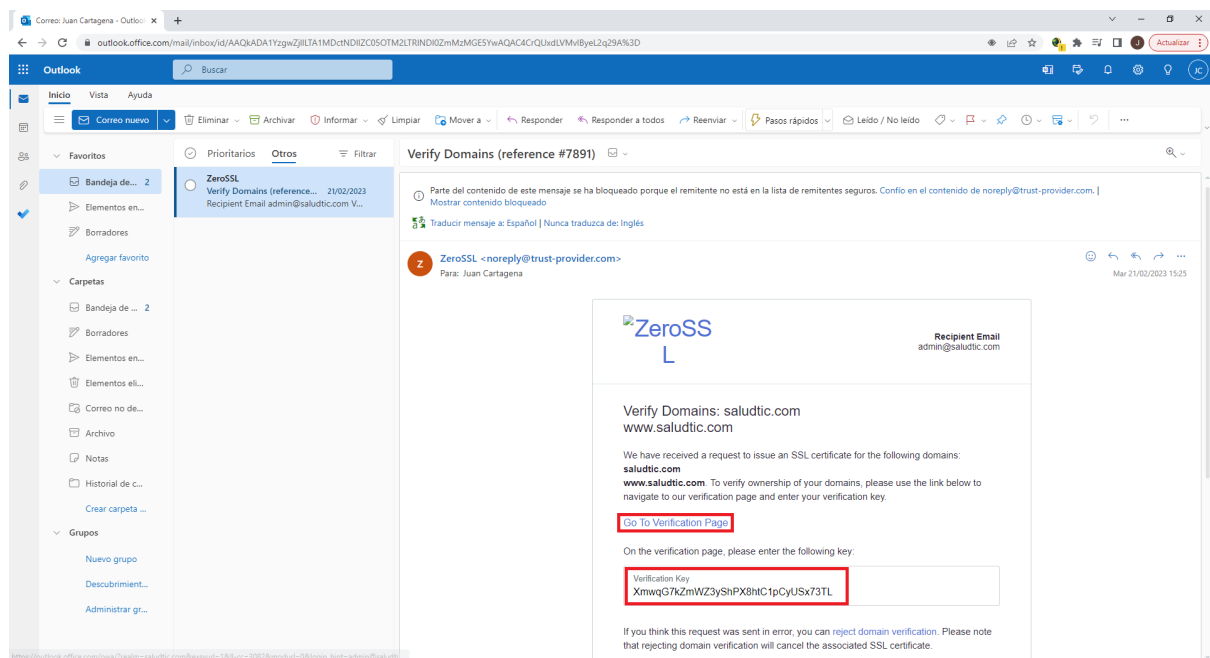
This screenshot shows the 'Finalize' step of the domain verification process. A table lists the domain 'saludtic2.com' with the 'Email Verification' method and a status of 'To start, click "Verify Domains"'. The 'Verify Domain' button is highlighted with a red box. The interface is consistent with the previous screenshot, showing the ZeroSSL logo, navigation links, and user information.

Domain	Verification Method	Verification Status
saludtic2.com	Email Verification	To start, click "Verify Domains"

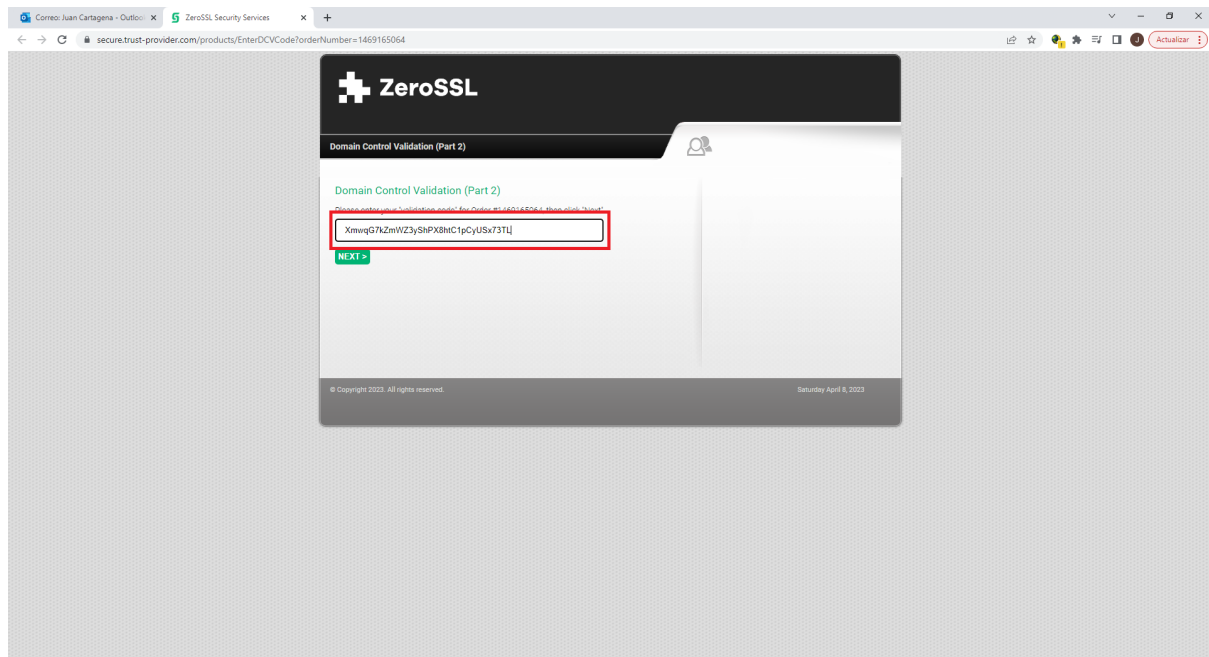
The status will change like this



Now you need to open the email inbox, you will see an email from ZeroSSL with a link to a **verification page** and a **verification key**. copy the verification key and click in the link



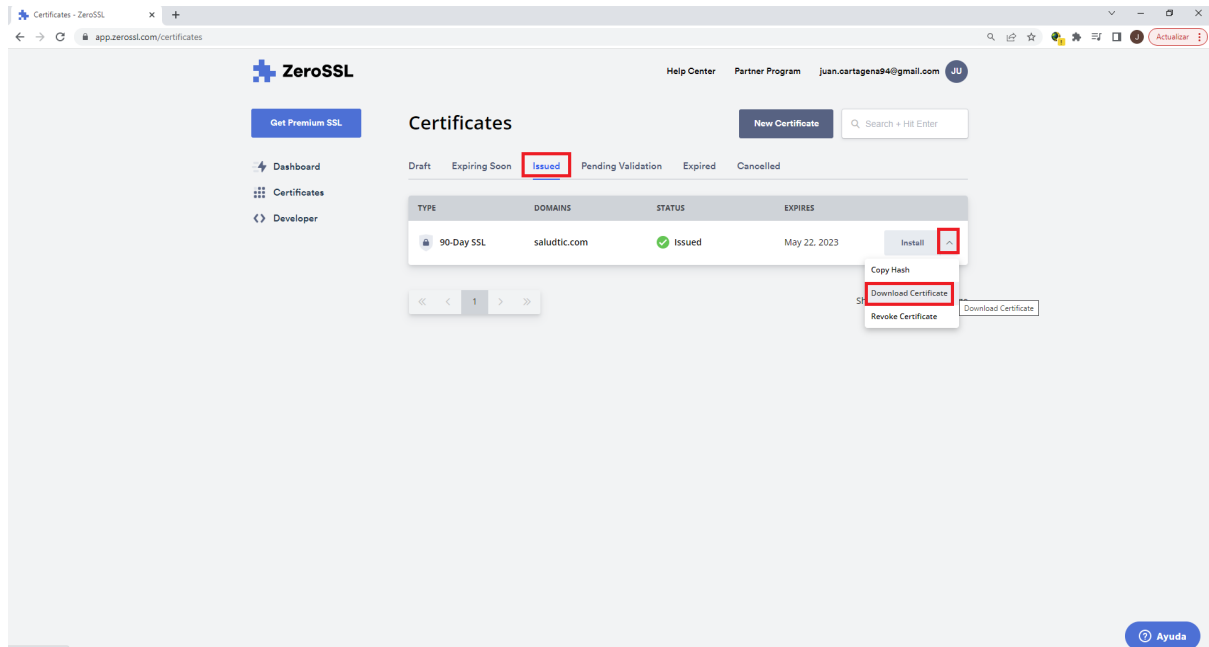
Paste the key and next



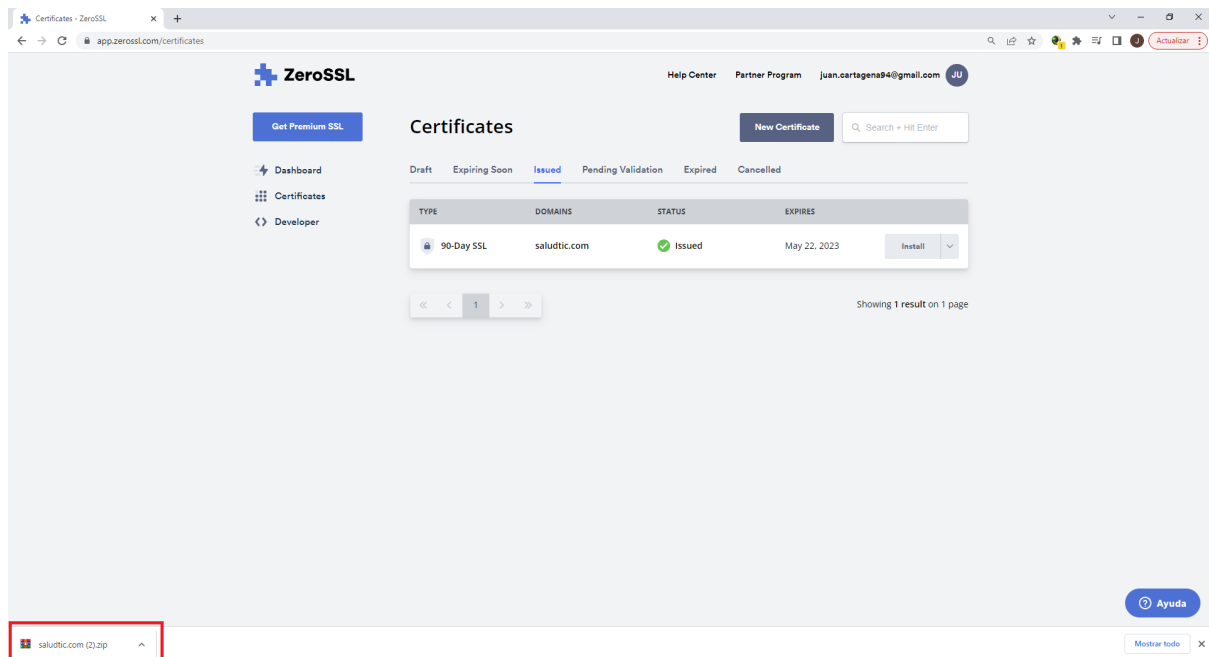
after that you will be able to see the certificate active on <https://app.zerossll.com/certificates>

Downloading the certificate

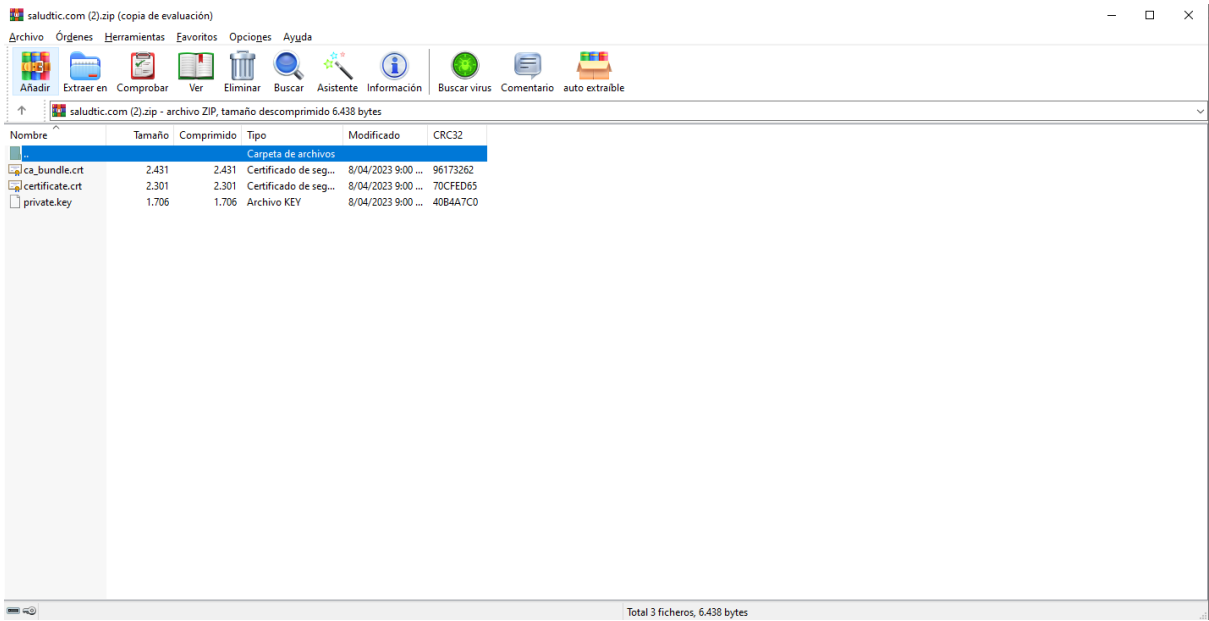
go to <https://app.zeross.com/certificates> and search the certificate on the “Issued” tab, then click on the droplist menu and “Download Certificate”



you will have a zip



In the zip you will have the .crt file, please unzip this in a folder

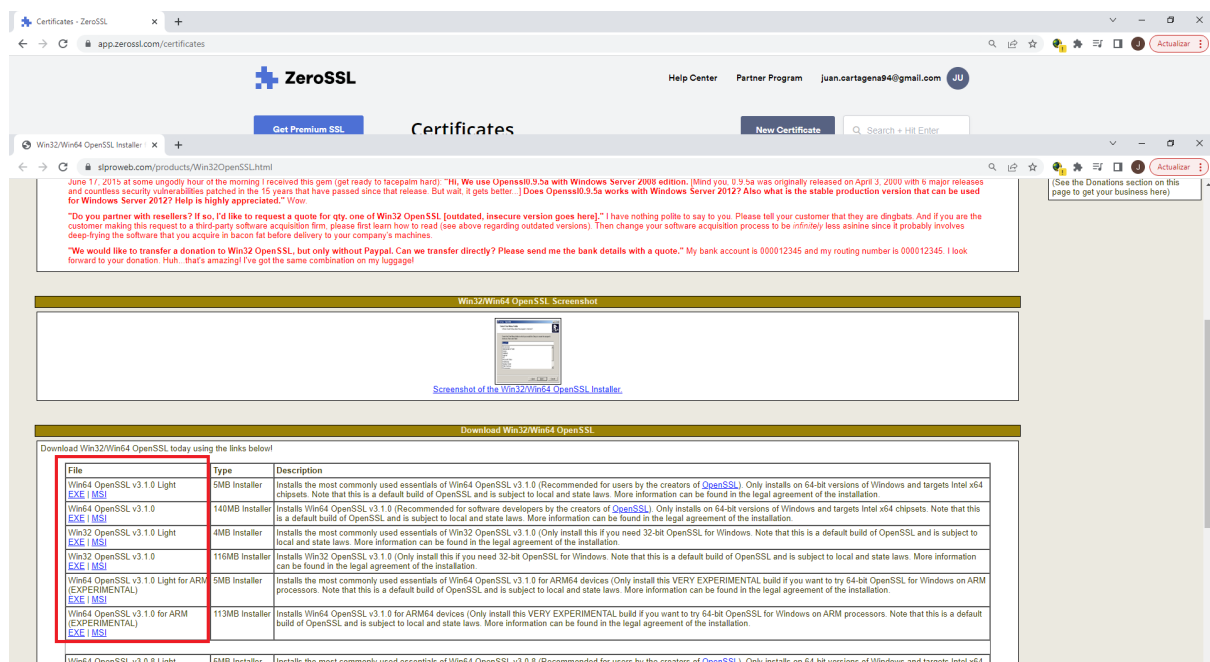


Installing the Certificate

The first step to be able to install the certificate on IIS, is to convert the file .crt to .pfx, for this we will need to instal OpenSSL, the more safety way in download the source code from <https://www.openssl.org/> and build the installer on linux, this [tutorial](#) seem to have a good explanation to do this, however for this tutorial we will trust on <https://slproweb.com/products/Win32OpenSSL.html> that offer installers already builded

Installing Open SSL

Open <https://slproweb.com/products/Win32OpenSSL.html> and download the Win64OpenSSL_Light-1_1_1t **light** version accordingly to your machine, its important that you choose the 1.1.1 version, otherwise you will have problems the moment to upload the certificates to IIS, I found this solution on [this post](#)



ZeroSSL

Help Center Partner Program juan.cartagena94@gmail.com

Get Premium SSL Certificates New Certificate

Win32/Win64 OpenSSL Installer

June 17, 2015 at some undogly hour of the morning I received this gem (get ready to takepain hard): "Hi, We use Openssl0.9.5a with Windows Server 2008 edition. (Mind you, 0.9.5a was originally released on April 3, 2000 with 6 major releases and countless security vulnerabilities patched in the 15 years that have passed since that release. But wait, it gets better.) Does Openssl0.9.5a works with Windows Server 2012? Also what is the stable production version that can be used for Windows Server 2012? Help is highly appreciated." Wow

"Do you partner with resellers? If so, I'd like to request a quote for qty. one of Win32 OpenSSL [outdated, insecure version goes here]." I have nothing polite to say to you. Please tell your customer that they are dingbats. And if you are the customer making this request to a third-party software acquisition firm, please first learn how to read (see above regarding outdated versions). Then change your software acquisition process to be infinitely less asinine since it probably involves deep-frying the software that you acquire in bacon fat before delivery to your company's machines

"We would like to transfer a donation to Win32 OpenSSL, but only without Paypal. Can we transfer directly? Please send me the bank details with a quote." My bank account is 000012345 and my routing number is 000012345. I look forward to your donation. Huh. that's amazing! I've got the same combination on my luggage!

Win32/Win64 OpenSSL Screenshot

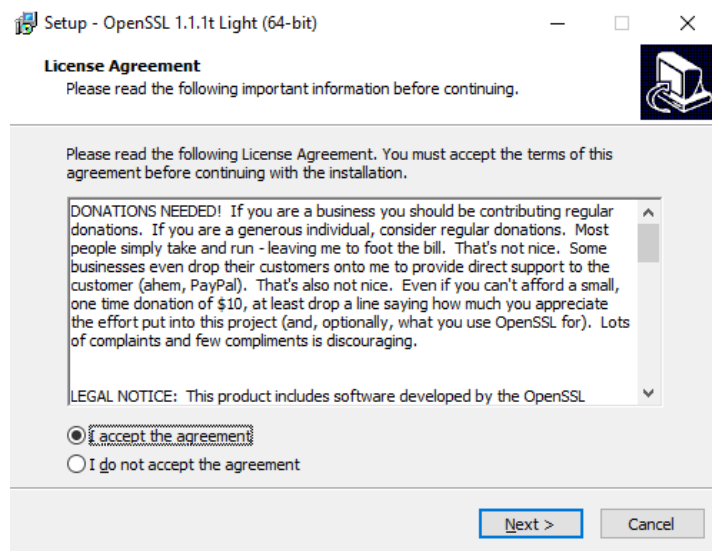
Screenshot of the Win32/Win64 OpenSSL Installer.

Download Win32/Win64 OpenSSL

Download Win32/Win64 OpenSSL today using the links below!

File	Type	Description
Win64 OpenSSL v3.1.0 Light EXE MSI	5MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v3.1.0 (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows and targets Intel x64 chipsets. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v3.1.0 EXE MSI	140MB Installer	Installs Win64 OpenSSL v3.1.0 (Recommended for software developers by the creators of OpenSSL). Only installs on 64-bit versions of Windows and targets Intel x64 chipsets. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v3.1.0 Light EXE MSI	4MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v3.1.0 (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v3.1.0 EXE MSI	116MB Installer	Installs Win32 OpenSSL v3.1.0 (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v3.1.0 Light for ARM EXE MSI	5MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v3.1.0 for ARM64 devices (Only install this VERY EXPERIMENTAL build if you want to try 64-bit OpenSSL for Windows on ARM processors. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v3.1.0 for ARM EXE MSI	113MB Installer	Installs Win64 OpenSSL v3.1.0 for ARM64 devices (Only install this VERY EXPERIMENTAL build if you want to try 64-bit OpenSSL for Windows on ARM processors. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v3.0.0 Light EXE MSI	5MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v3.0.0 (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows and targets Intel x64

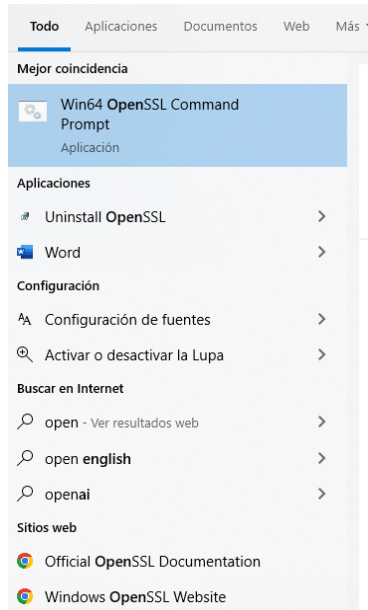
Open the installer and next next until complete.



Converting from .crt to .pfx

We will follow the next tutorials <https://www.youtube.com/watch?v=n3eMjMsb0Ng&t=103s> and [this](#)

Search for openssl in your computer



You will see a CMD shell, navigate to the location of the certificate

Win64 OpenSSL Command Prompt

Win64 OpenSSL Command Prompt

```
OpenSSL 1.1.1t  7 Feb 2023
built on: Wed Feb  8 15:15:49 2023 UTC
platform: VC-WIN64A
options: bn(64,64) rc4(16x,int) des(long) idea(int) blowfish(ptr)
compiler: cl /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_CPUID_OBJ
-DOPENSSL_IA32_SSE2 -DOPENSSL_BN_ASM_MONT -DOPENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM
-DKECCAK1600_ASM -DRC4_ASM -DMD5_ASM -DAESNI_ASM -DVPAES_ASM -DGHASH_ASM -DECP_NISTZ256_ASM -DX25519_ASM -DPOLY1305_ASM
-DUSING_V110_SDK71 -D_WINSOCK_DEPRECATED_NO_WARNINGS -D_WIN32_WINNT=0x0502
OPENSSLDIR: "C:\Program Files\Common Files\SSL"
ENGINESDIR: "C:\Program Files\OpenSSL\lib\engines-1_1"
Seeding source: os-specific

C:\Users\57321>cd Downlowads
El sistema no puede encontrar la ruta especificada.

C:\Users\57321>cd Downloads

C:\Users\57321\Downloads>cd Saldudtic
El sistema no puede encontrar la ruta especificada.

C:\Users\57321\Downloads>cd saludtic.com

C:\Users\57321\Downloads\satudtic.com>cd ..

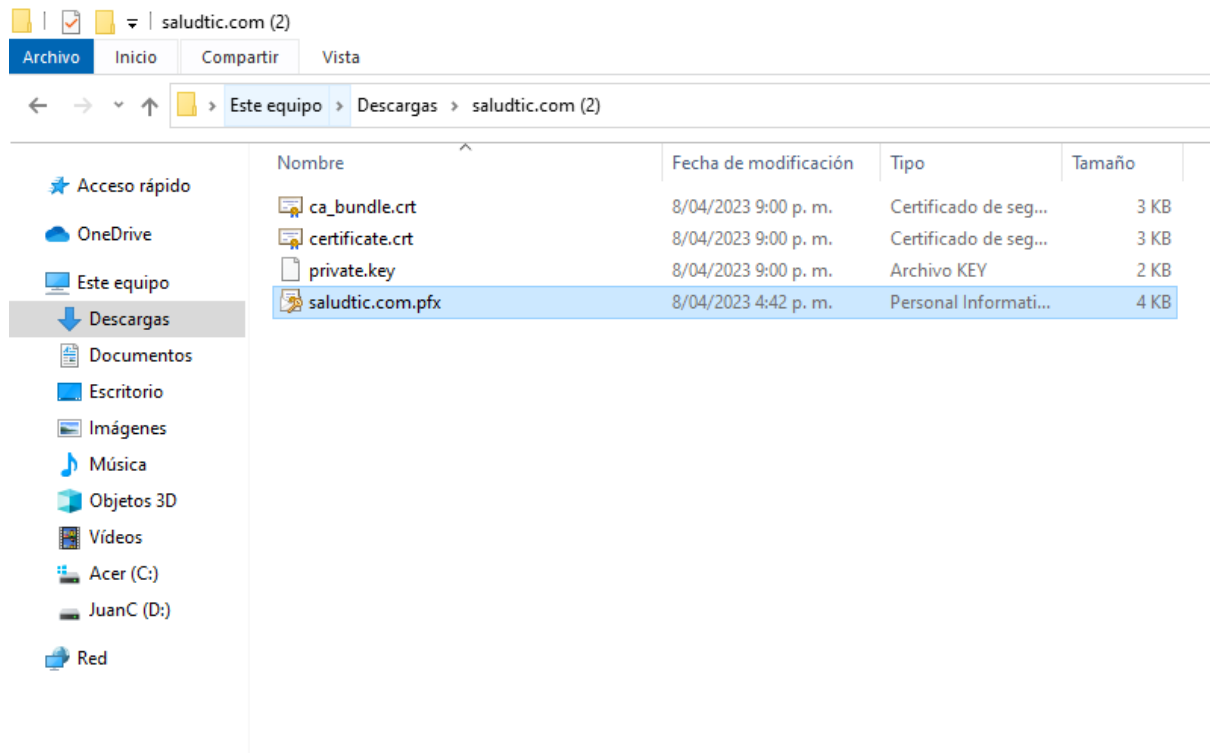
C:\Users\57321\Downloads>cd saludtic.com (2)

C:\Users\57321\Downloads\satudtic.com (2)>
```

Then paste the next instruction, you will need to add a password 2 times

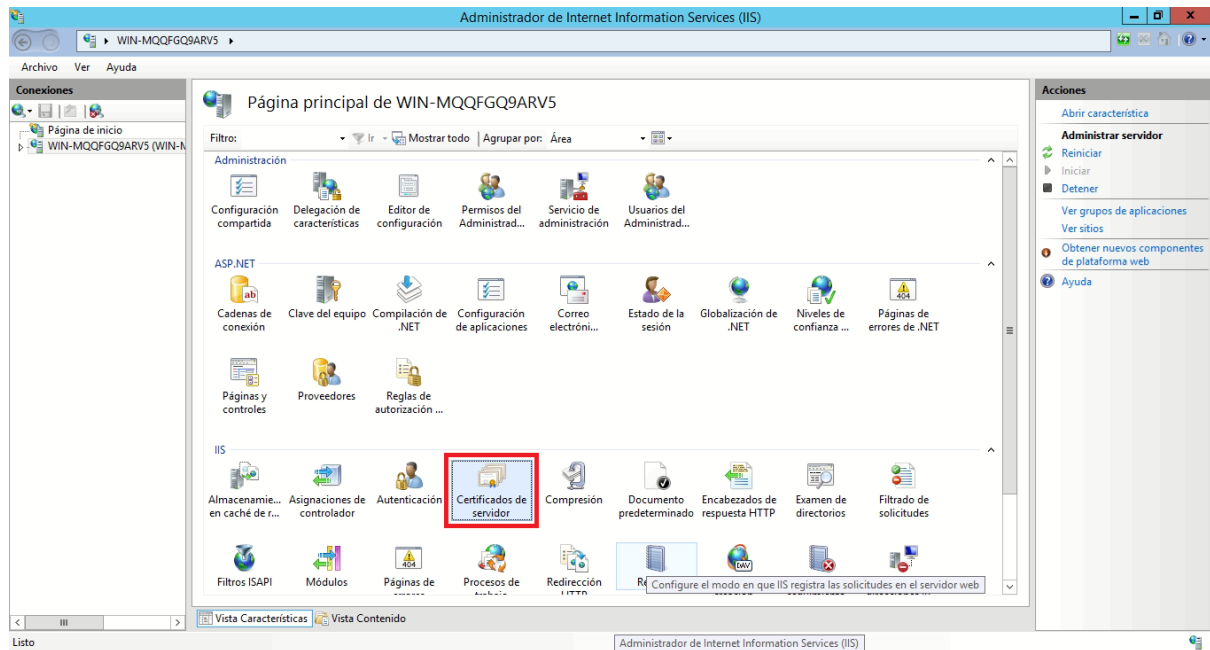
```
openssl pkcs12 -export -out saludtic.com.pfx -inkey private.key -in certificate.crt
```

after that, you will see a .pfx file in the same folder

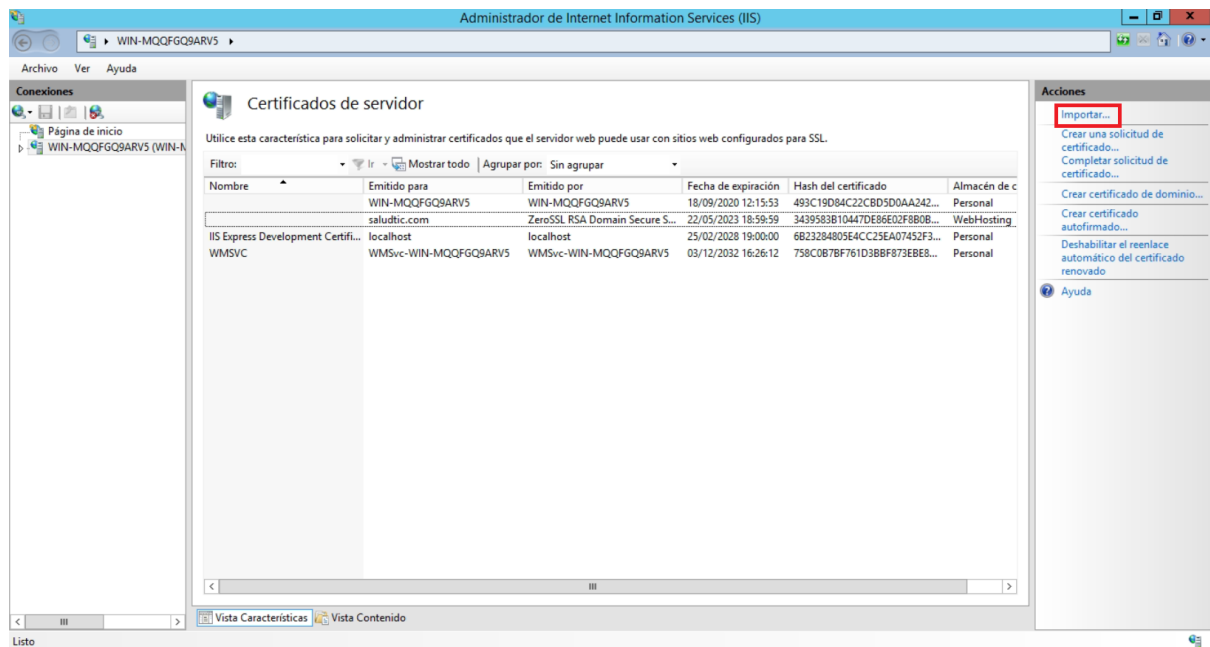


Uploading the certificate to IIS

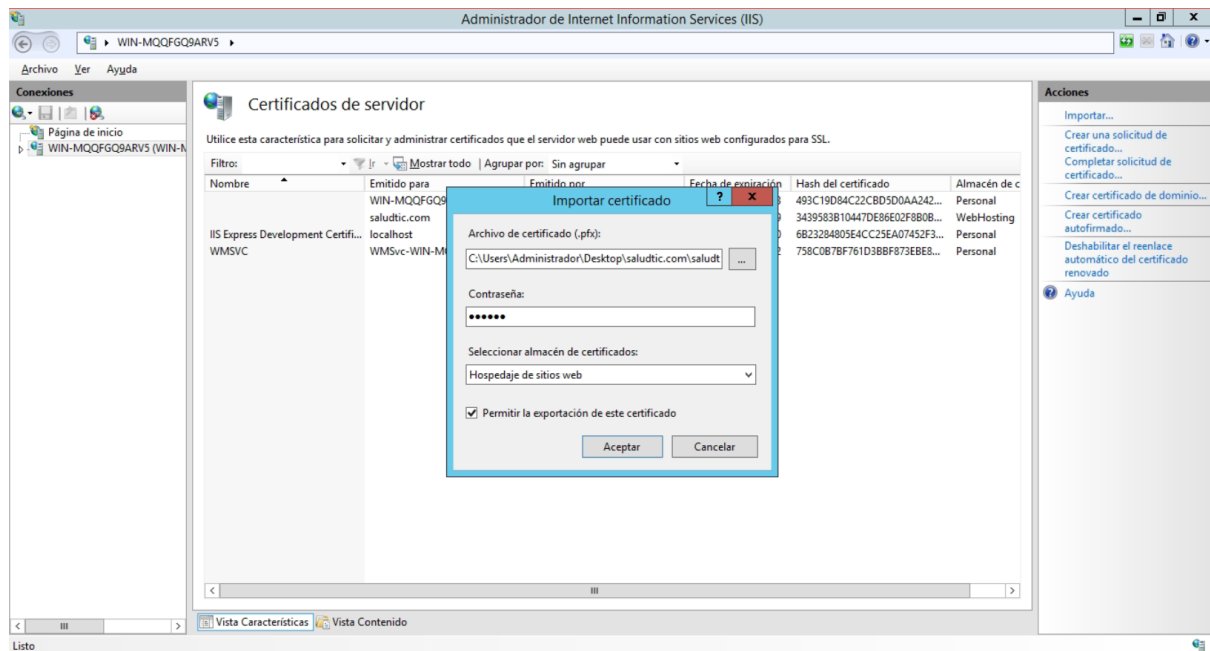
In the IIS go to “Certificados de servidor”



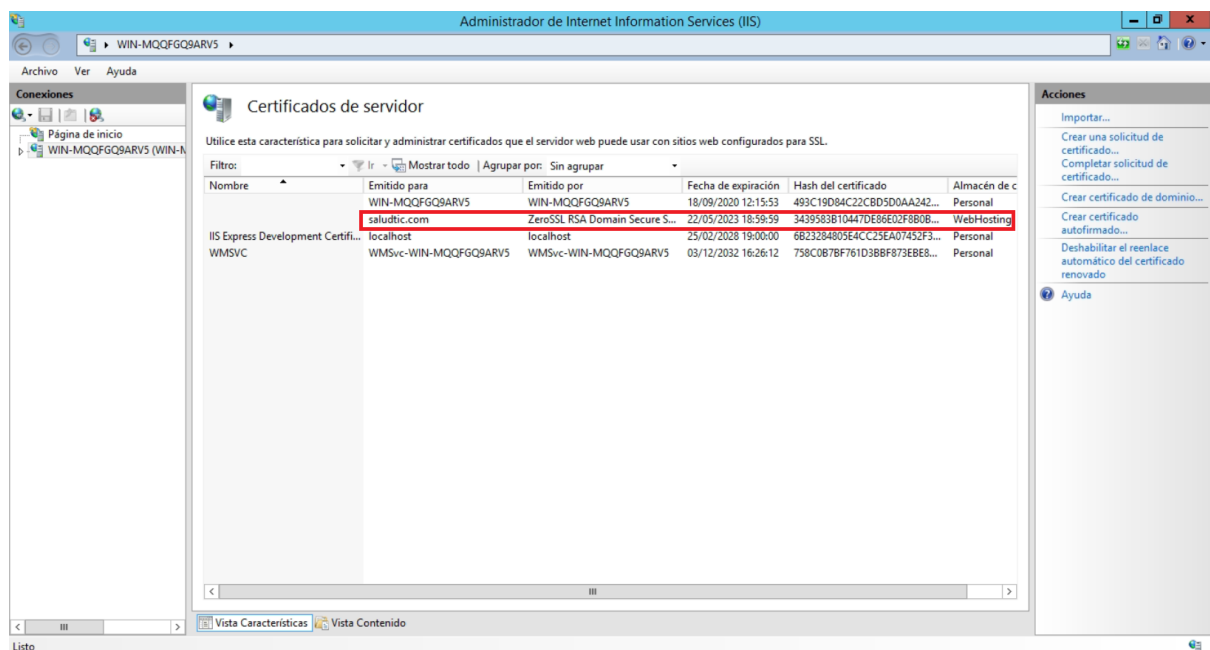
Then “Importar”



In the windows that opens, search the certificate, add the password that you chose on Openssl and select the option “Hospedaje de sitios web”

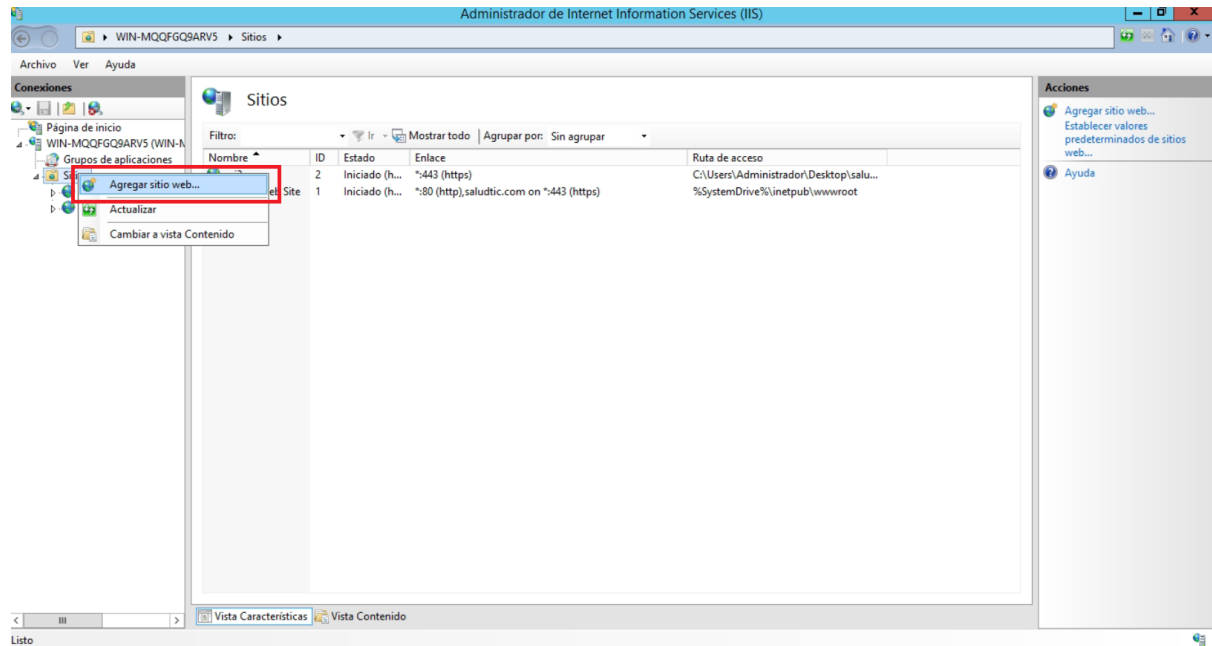


Now you should be able to see the certificate installed.



Adding the certificate to a website

Create a new site,



fill the necessary data, and choose "tipo" as HTTPS, and you should be able to see the certificate in the dropdown list

