**Apache installation process**

Need to download apache from below link, unzip and copy where it is installing.

<https://www.apachehaus.com/cgi-bin/download.plx>

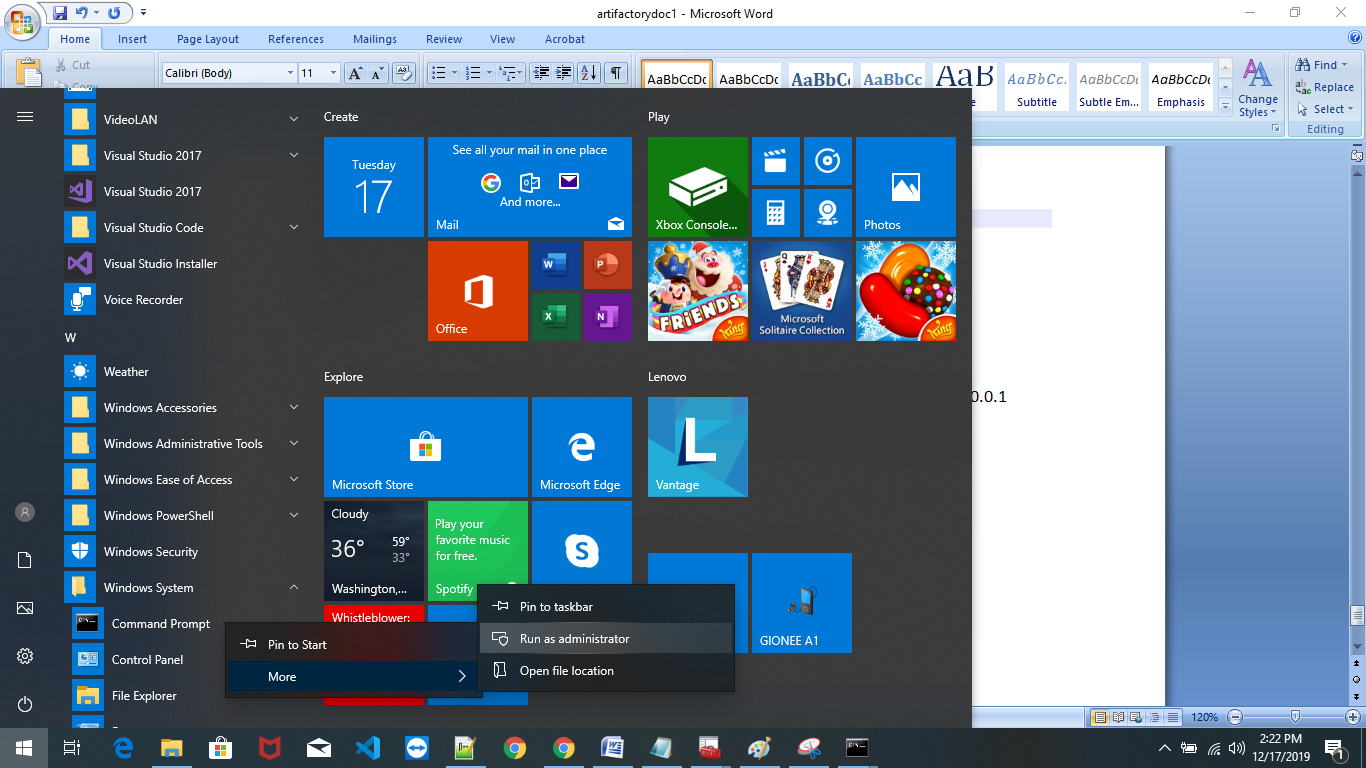
You must first install the Visual C++ Redistributable for Visual Studio 2015-2019 x86.

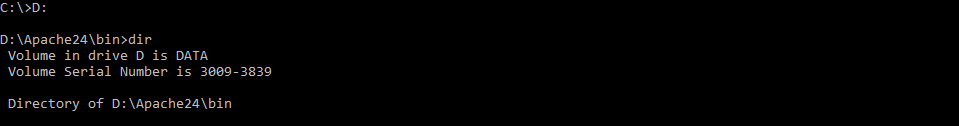
Download and Install, if you have not done so already, see:

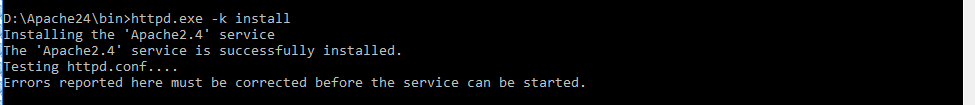
**When you unzip to an other location:**

Change Define SRVROOT "c:/Apache24” in httpd.conf, for example to "D:/Apache24"

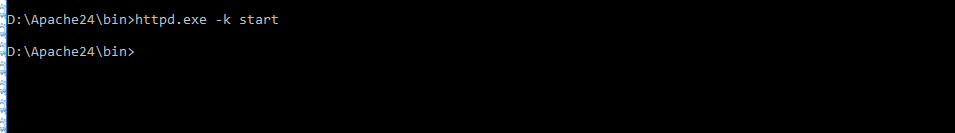
To install as a service. Open command prompt as Administrator, install and change httpd.conf file



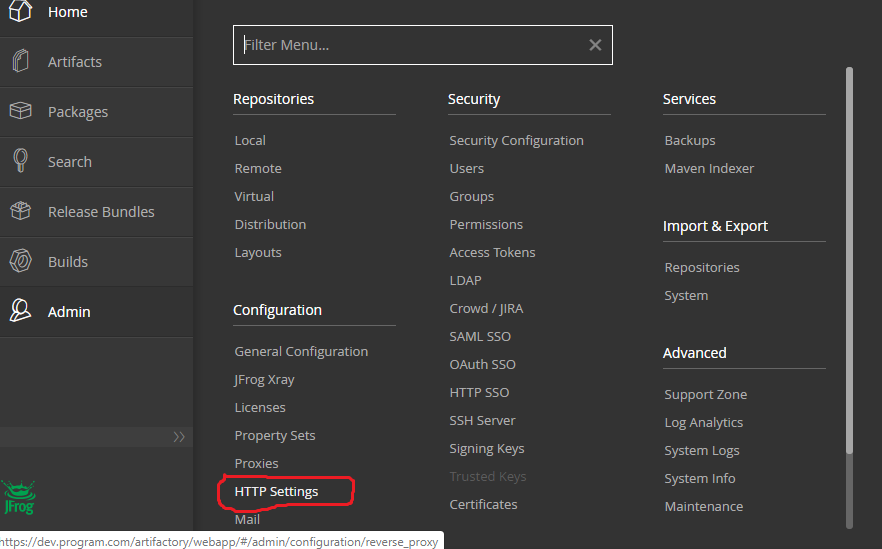


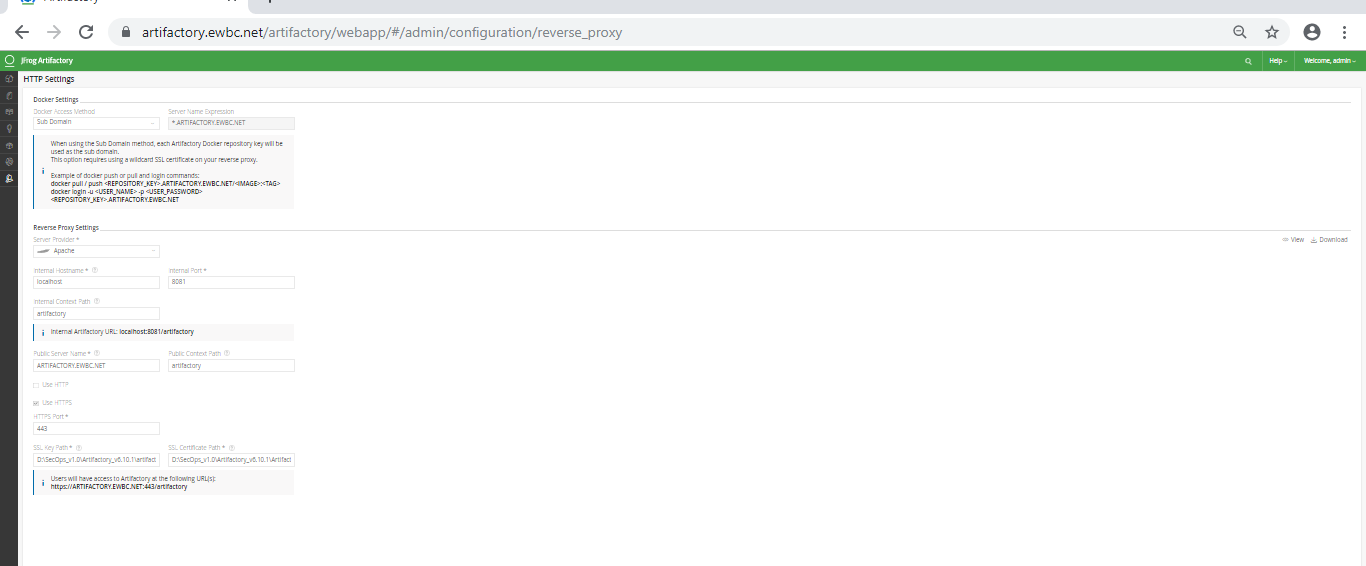


You can start/stop the service with the command:

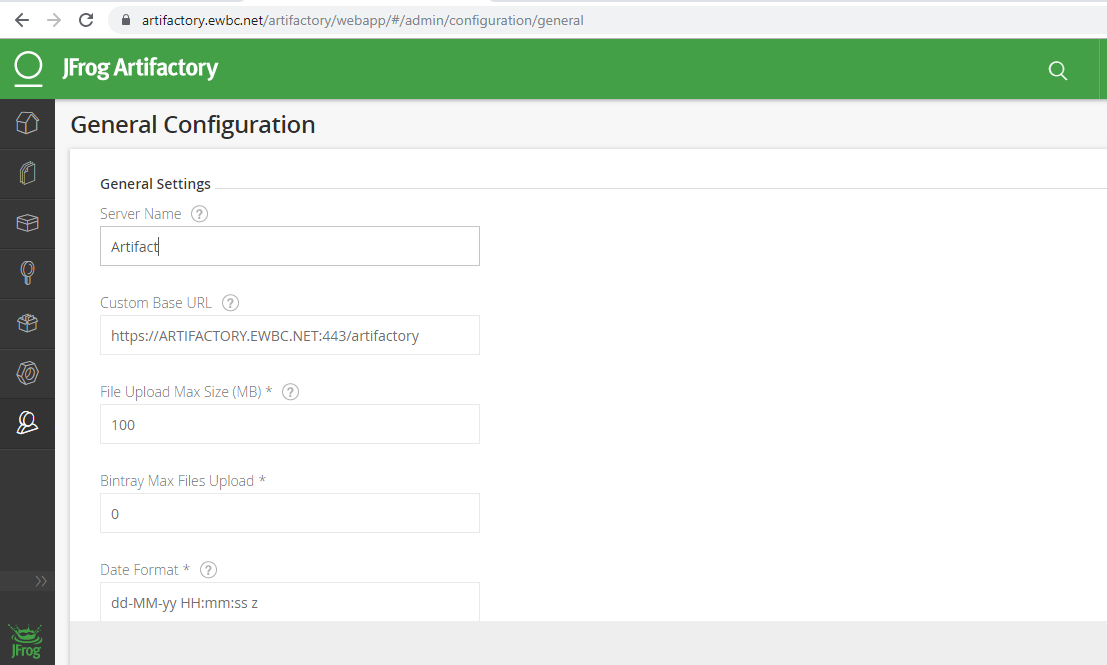


Need to connect artifactory server and click admin 🡪 Http Settings

We should click HTTP settings and provide required information ,Save , download the file and put it apache server.



We should add Custom Base URL in General Configuration so that it will redirect as default URL whenever we login.



1.We should connect jenkins server and copy .crt certifaction from artifactory server to jenkins server.

2.We should take backup **cacerts** file and add .crt cerification in java repository

keytool -importcert -keystore "C:\Program Files\AdoptOpenJDK\jdk-8.0.212.04-hotspot\jre\lib\security\cacerts" -storepass changeit -file "C:\Program Files\AdoptOpenJDK\jdk-8.0.212.04-hotspot\jre\lib\security\ARTIFACTORY.EWBC.NET.crt" -alias "servers-root"

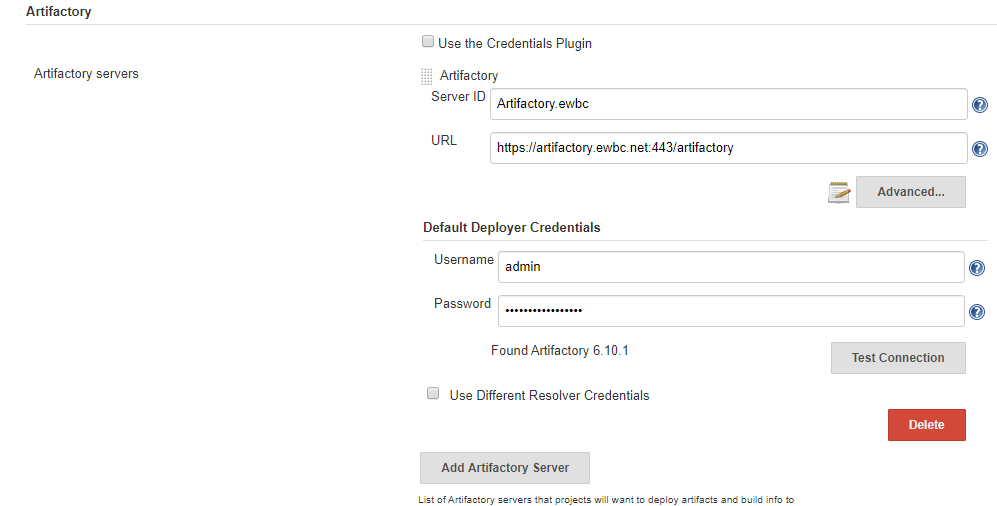
3.the above command will ask confirmation yes or No while excuting it . we should give yes so that the .crt certification will add to java **cacerts** repository.

4.We should add https url in jenkins configure system file.

[**https://artifactory.ewbc.net:443/artifactory**](https://artifactory.ewbc.net:443/artifactory)

5.Restart the jenkins server.

.



We should upload the .crt certification in personal folder of artifactory server.

**Step-by-step guide to issuing certificates on Windows so that you can run your sites in HTTPS**.

**Install OpenSSL**

**Shining Light Productions**

Visit https://slproweb.com/products/Win32OpenSSL.html and download the “Win64 OpenSSL v1.1.0l” file and run the installer.

Make sure that the “\bin\” folder of the installation folder you chose for OpenSSL is added to your system PATH environment variable, so it’s available from anywhere.

**The Three Steps to Become Your Own Certificate Authority in Windows**

In these steps, you will create a root SSL certificate that you can use to sign sites as you need.

You only need to do this first part once.

Once your root SSL is added to Windows server, you can skip to issuing certificates for all your new local domains.

**Step 1 – Create a Private Key**

We are going to create a private key called Server.key which we will use to issue the new site certificates.

I use the Apache web server, so I have created a folder called “SSL” in the Apache windows folder, and that’s where I am going to create this root key.

Open a command prompt in administrator mode and navigate to your newly created SSL folder in the Apache installation folder.

**Type in the following command and enter a password for the private key.**

openssl genrsa -out server.key 2048

**Step 2 – Create the Certificate File**

In this step, we are going to create a certificate file called server.crt from the private key we created in the previous step.

Note: you can choose to create a certificate file that lasts for X number of days. We’re going to choose 365 days in this example, but you can select any amount – the longer, the better.

**Type in the following command:**

openssl req -new -x509 -key server.key -out server.crt -days 365

Enter the password for the root SSL key we created in step 1.

Then, enter the information to insert in the SSL certificate:

* Two letter Country code:
* Your state or province:
* Your city:
* An organization name:
* An organizational unit name:
* A common name such as the server name or the fully qualified .domain name (FQDN): **“dev.program.com”.**
* An admin email address:

You don’t have to put your legit information in here as we’re only running SSL certificates on the local development environment, but I like to do it properly.

**Need to generate .pfx certification file**

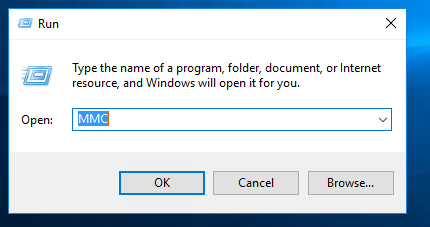
openssl pkcs12 -export -in server.crt -inkey server.key -out server.pfx

**Step 3 – Get Windows to Trust the Certificate Authority (CA)**

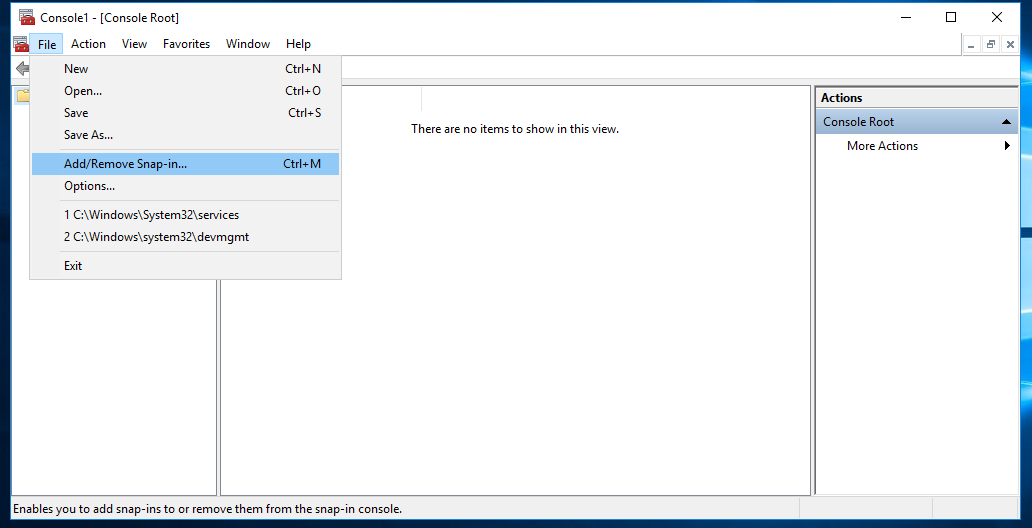
We are going to use the Microsoft Management Console (MMC) to trust the root SSL certificate.

Step 1 – Press the Windows key + R

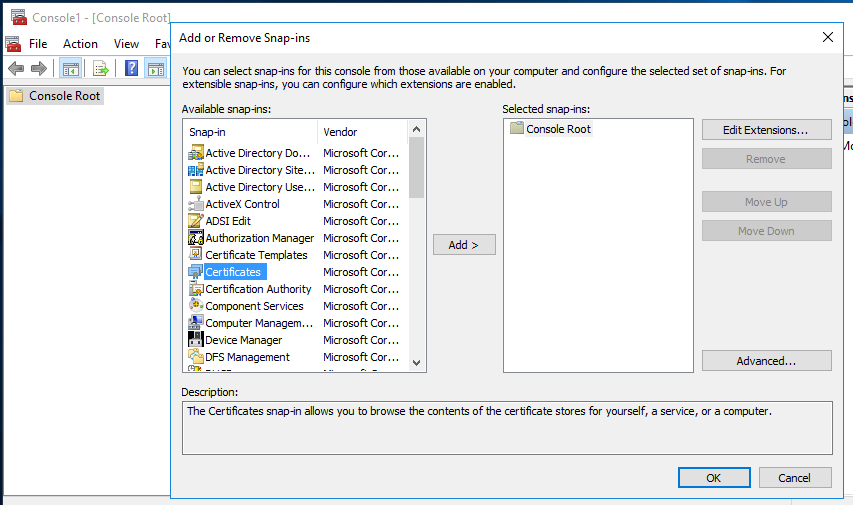
Step 2 – Type “MMC” and click “OK”



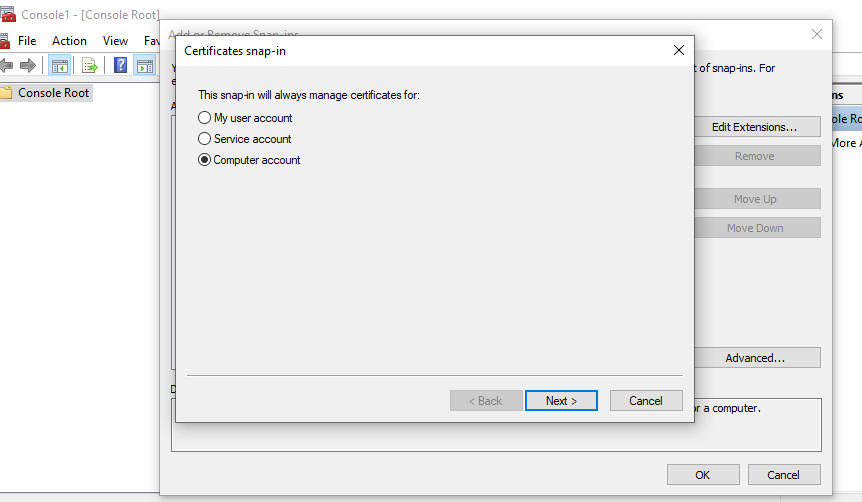
Step 3 – Go to “File > Add/Remove Snap-in”



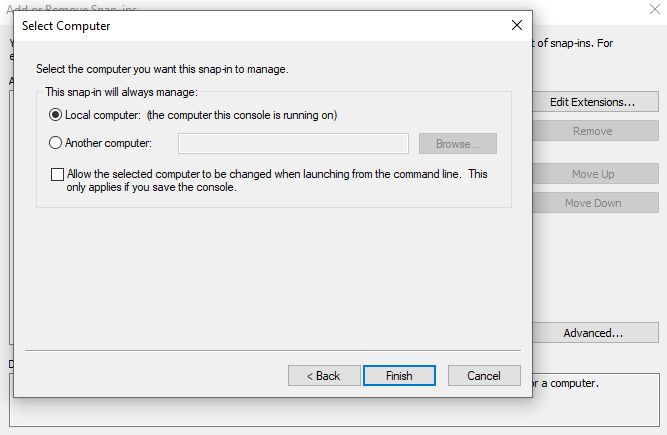
Step 4 – Click “Certificates” and “Add”



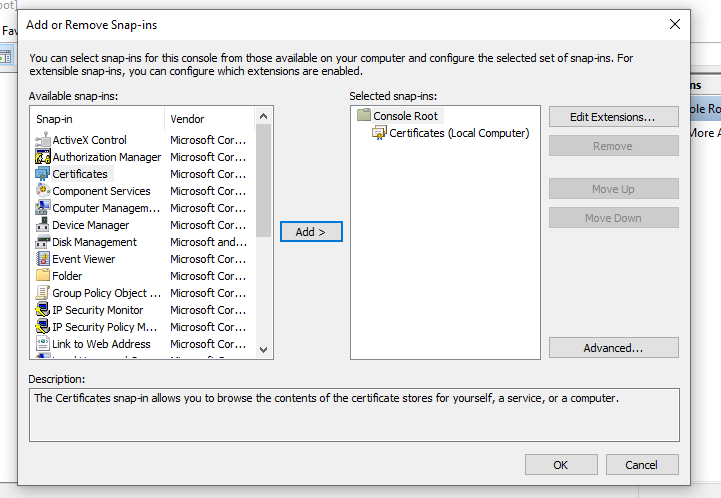
Step 5 – Select “Computer Account” and click “Next”



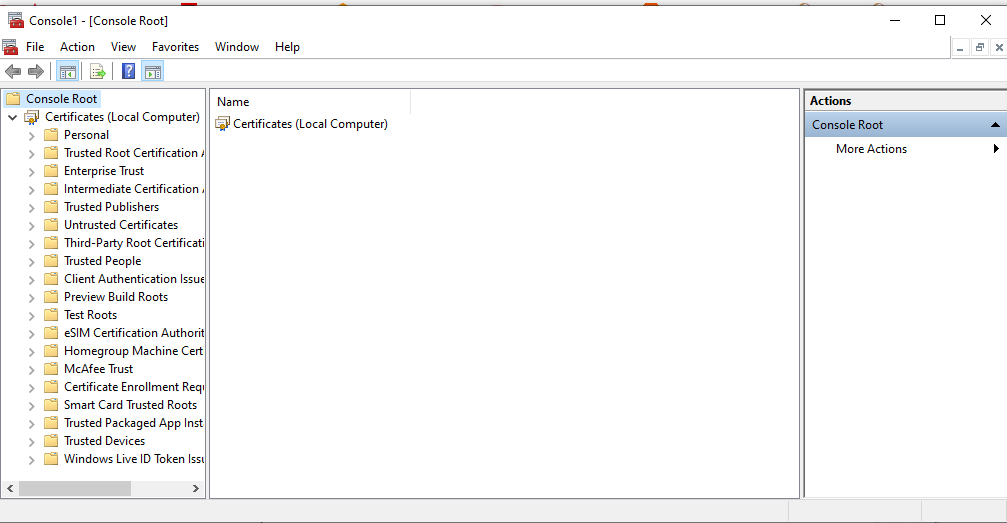
Step 6 – Select “Local Computer” then click “Finish”



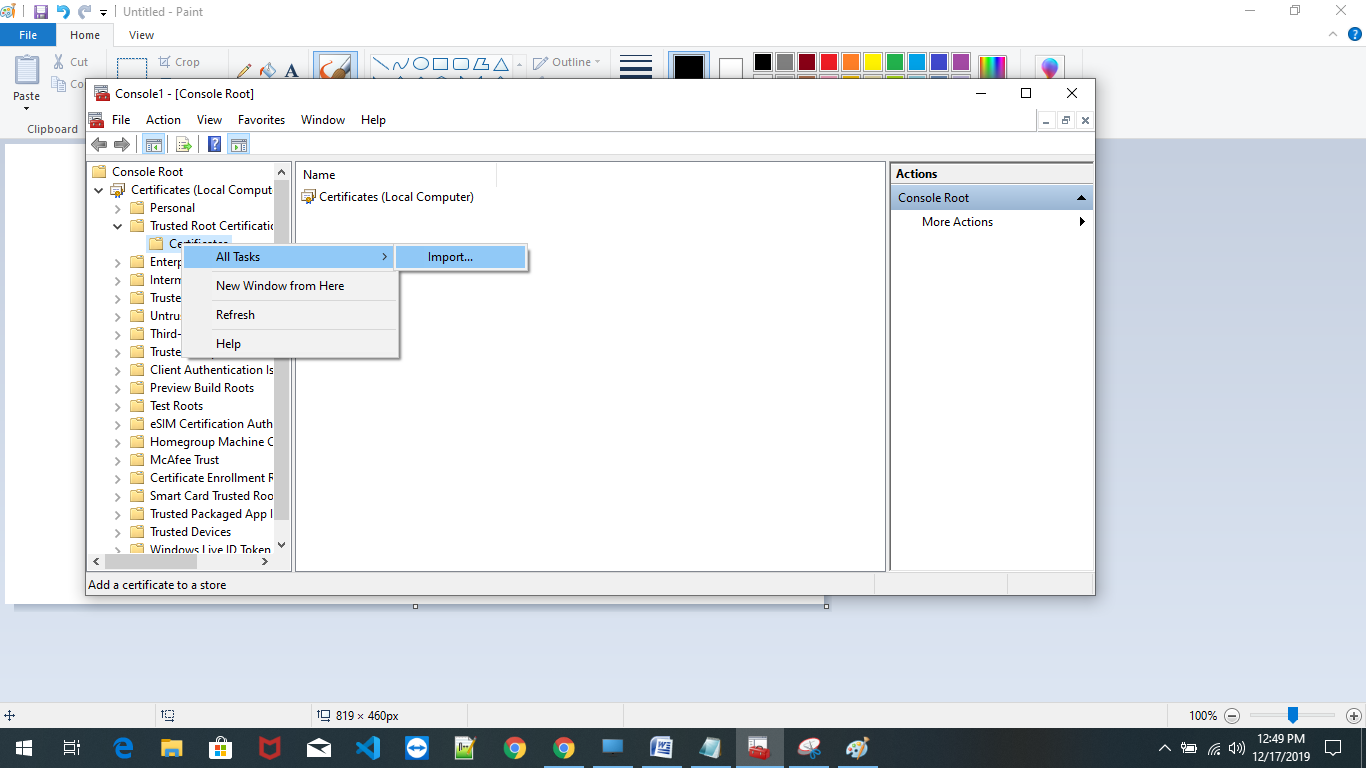
Step 7 – Click “OK” to go back to the MMC window



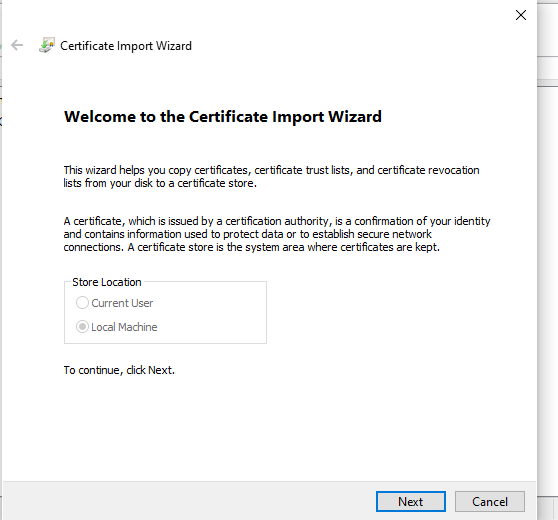
Step 8 – Double-click “Certificates (local computer)” to expand the view

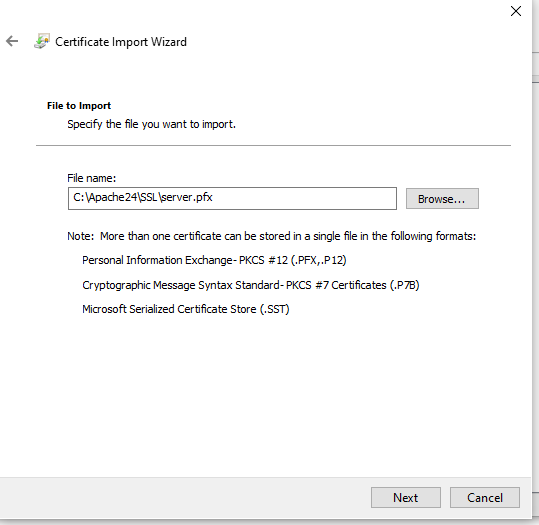


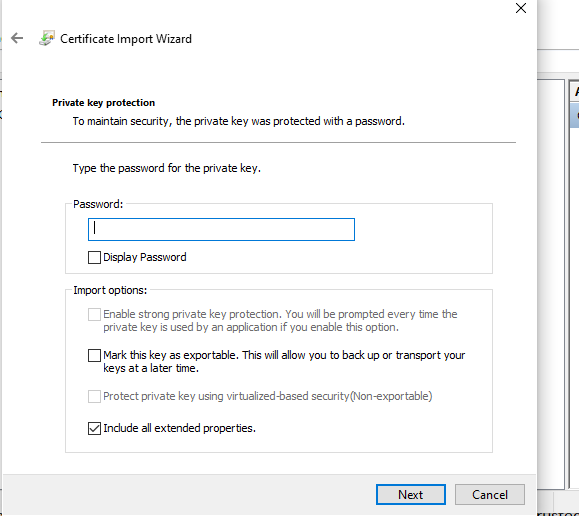
Step 9 – Select “Trusted Root Certification Authorities”, right-click “Certificates” and select “All Tasks” then “Import”



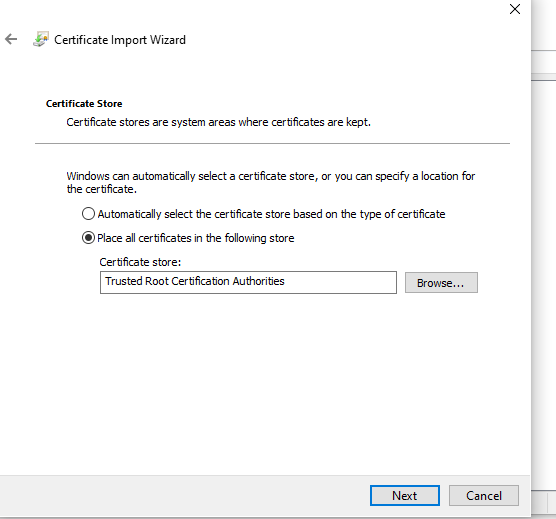
Step 10 – Click “Next” then Browse and locate the “C:\Apache24\SSL\server.pfx” file we created in step 2 and put the password .







Step 11 – Select “Place all certificates in the following store” and select the “Trusted Root Certification Authorities store”. Click “Next” then click “Finish” completing the wizard.



Browse the certificates to see yours in the list.

Now you can start issuing SSL certificates for all your local domains.

**Issuing Certificates for Local Domains**

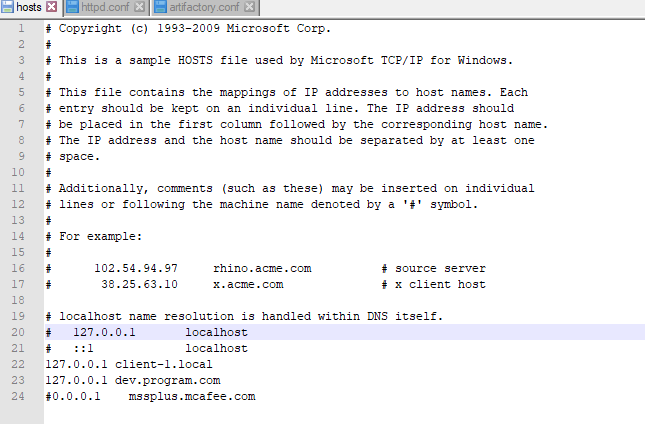
Creating a Local Domain Site

I’m not going to cover setting up the actual site in Nginx or whatever web server you use.

The first step will be to create a local domain.

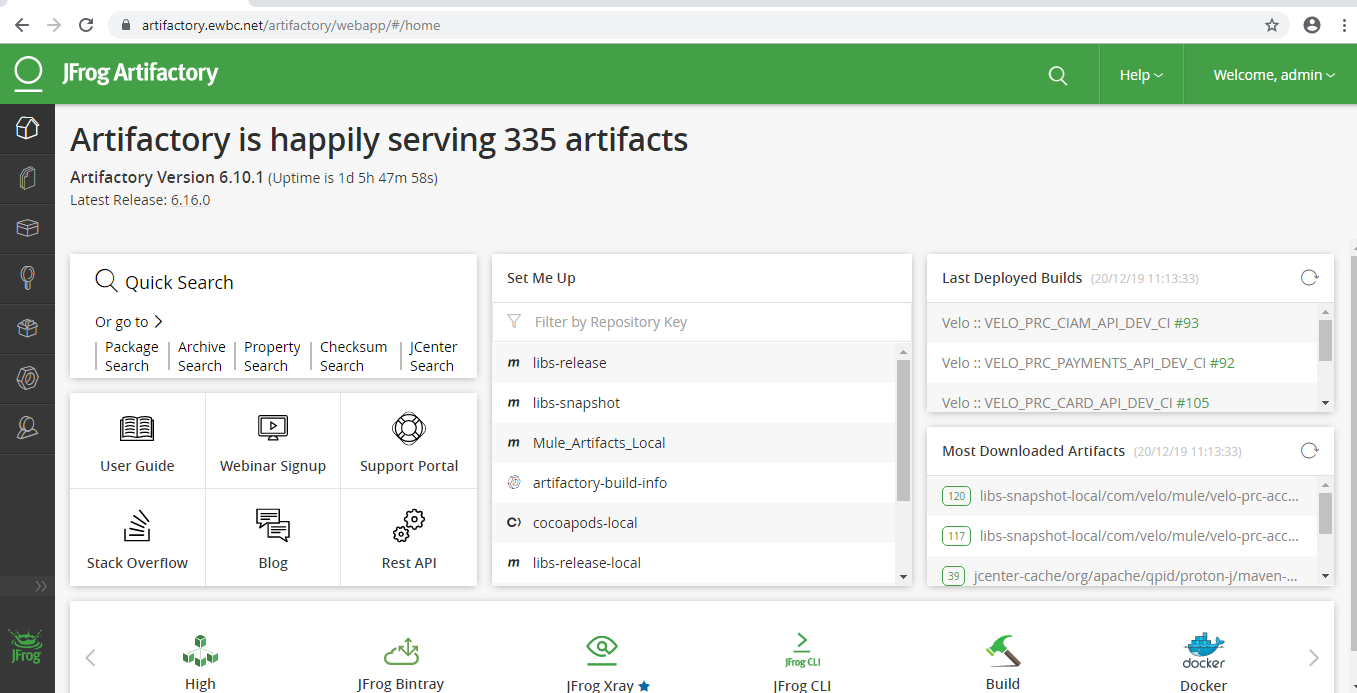
You do this in your c:\program files\windows\system32\drivers\etc\hosts file.

Here’s an example hosts file.

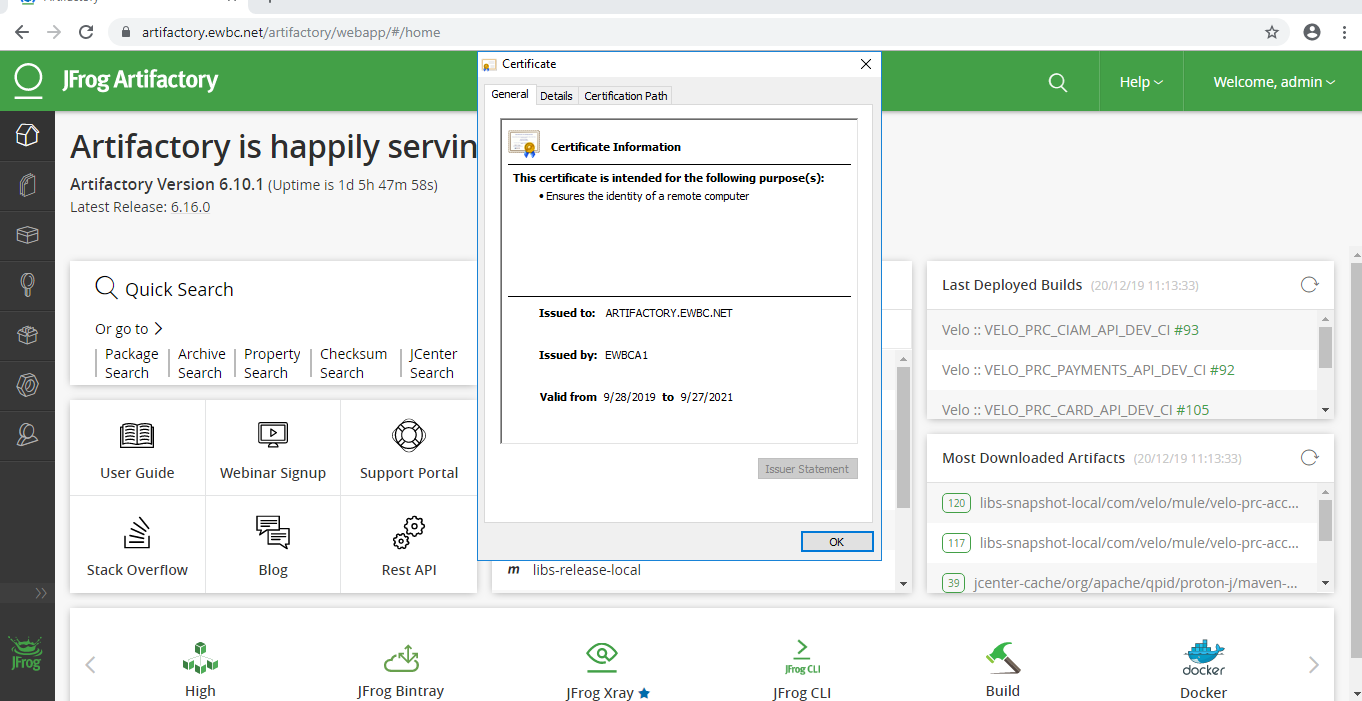


You can see that I’ve added a “dev.program.com” domain to point to IP address 127.0.0.1

So “dev.program.com” is the new website address and I want to connect to it using “https:// dev.program.com”



Check the certification



openssl genrsa -out server.key 2048

openssl req -new -x509 -key server.key -out server.crt -days 365

openssl pkcs12 -export -in server.crt -inkey server.key -out server.pfx