

SENTEC AGENT SETUP INSTRUCTIONS

A. TO CONSIDER BEFORE SETTING UP

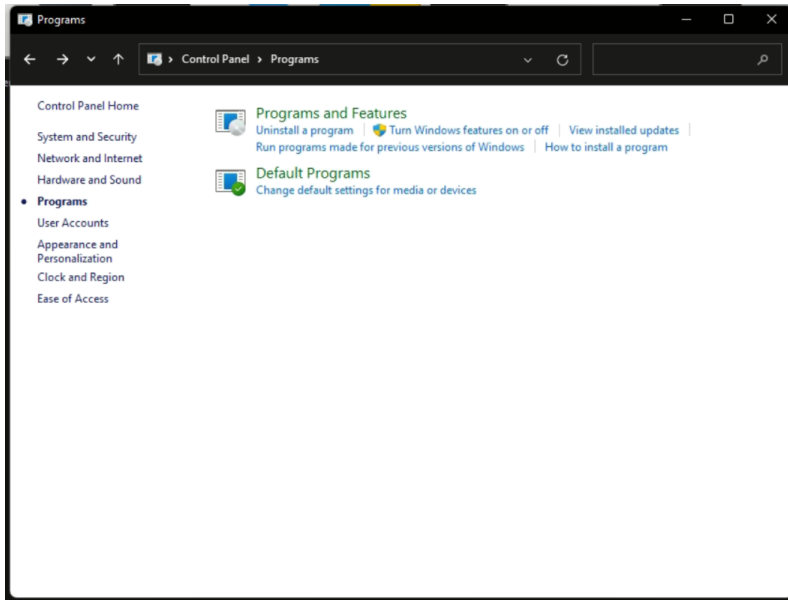
How to decide where we should install Sentec Agent

1. Ideally we want to only have one Sentec Agent service installed in a windows computer for one hotel, that is a computer server. This way, all other computers that need to perform printing or keycard writing tasks, will request into computer Server to perform those tasks. Because of limitations of how Sentec Agent installed on one computer can't access the keycard encoder and / or printer attached to another computer via USB, the ideal computer Server is the *computer who connects to all keycard encoders and has access to all printers needed*. For most cases this is the FO computer. If it is possible to opt for this option, we will need to ask for a specific subdomain for Sentec Agent service to the Sentec IT Team. This way we will have a specific subdomain such as <https://astoncilegon.agent.pms.sentec.io/> to access the service, and we will need to create self-signed certificate for the subdomain, and install SSL Certificate in other computers (clients) who access the service.
2. If it is not possible to execute the first option. We can install one Sentec Agent service for printing tasks in POS on one computer, and one Sentec Agent service for each computer that will be used to perform keycard writing tasks. This option will mostly *fit for certain cases that for some reasons, it's not possible to have one computer server for keycard and printing but still want to lessen the amount of computers used as a Sentec Agent server by making printing tasks served from one server* .
We will need to setup the service in one of POS computer that act as POS Sentec Agent Server using its IP as service url eg. <https://10.100.1.15/> and then create and bind a self-signed certificate to the url and install it in client computers.
We also need to setup the service in each of FO computer to perform keycard writing tasks using localhost and specific port as service url eg. <https://localhost:5000/> and then create and bind a self-signed certificate to the url.
3. For Sentec Agent service that only needed for just one computer (there is no need to share the service into other computers) then we need to setup the service in each of computer desired with localhost and specific port as service url eg. <https://localhost:5000/> and then create and bind a self-signed certificate to the url.

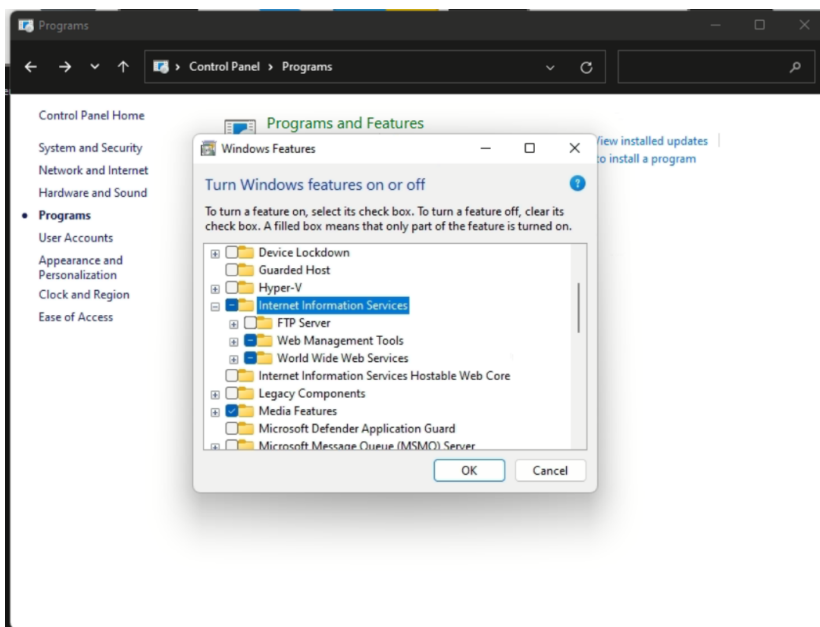
B. SETTING UP

Follow these instructions to install and setup Sentec Agent

1. Activate IIS Manager
 - a. **Control Panel** → **Programs** → **Programs and features** → **Turn windows features on or off**



b. Check **Internet Information Services** to turn on feature IIS → **OK**



2. Install **WebPlatformInstaller_x64_en-US.msi**
3. Install **dotnet-hosting-2.2.2-win.exe**
4. Install **SentecAgent.v.XX.X.X.exe**
5. Copy file **sentec-agent.db** to folder **C:\Program Files\Sentec Agent**
6. Create certificate based on where you want to bind Sentec Agent into
 - a. Open **Windows PowerShell** as Administrator
 - b. This step is for Sentec Agent served in hostname or domain, if not, skip this step. Type in command below and replace **astoncilegon.agent.pms.sentec.io** with actual hostname or domain name.

Unset

```
New-SelfSignedCertificate -DnsName astoncilegon.agent.pms.sentec.io  
-CertStoreLocation "cert:\LocalMachine\My" -TextExtension  
@("2.5.29.19={text}cA=true") -NotAfter (Get-Date).AddYears(100)
```

- c. This step is for a Sentec Agent served in a specific IP Address, if not, skip this step. Type in command below and replace 192.168.68.117 with actual IP of the computer.

Unset

```
New-SelfSignedCertificate -Subject sentec.dev -TextExtension  
@("2.5.29.17={text}DNS=sentec.dev&IPAddress=192.168.68.117", "2.5.29.19={text}cA  
=true") -NotAfter (Get-Date).AddYears(100) -CertStoreLocation  
cert:\LocalMachine\My
```

- d. This step is for a Sentec Agent served in localhost, if not, skip this step. Type in command below.

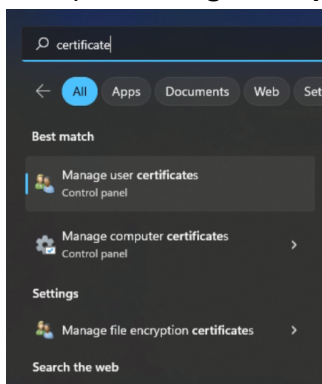
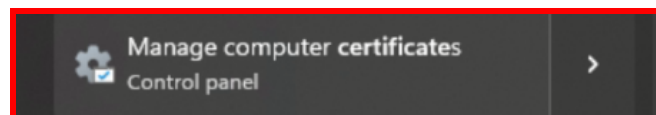
Unset

```
New-SelfSignedCertificate -DnsName "localhost" -CertStoreLocation  
"cert:\LocalMachine\My" -NotAfter (Get-Date).AddYears(100)
```

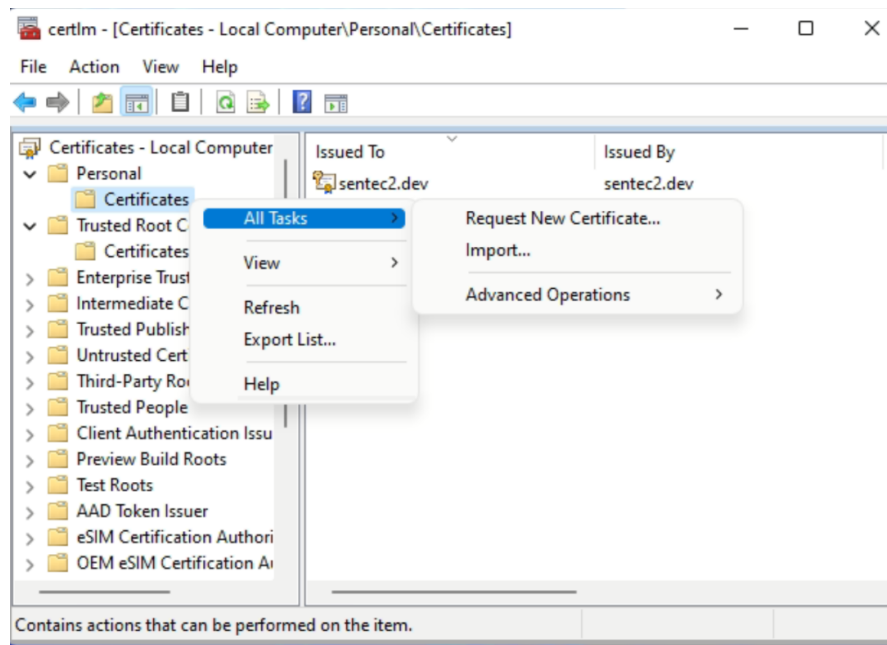
- e. Press Enter

7. Register Certificate

- a. Open **Manage Computer Certificates** from Windows App

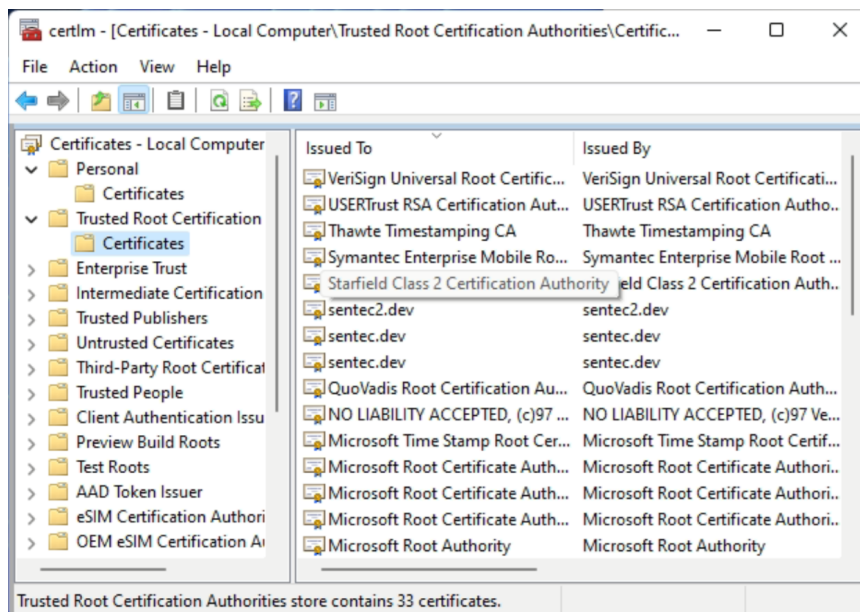


- b. Open **Personal** → **Certificates** → Right Click **All Tasks** → **Import**

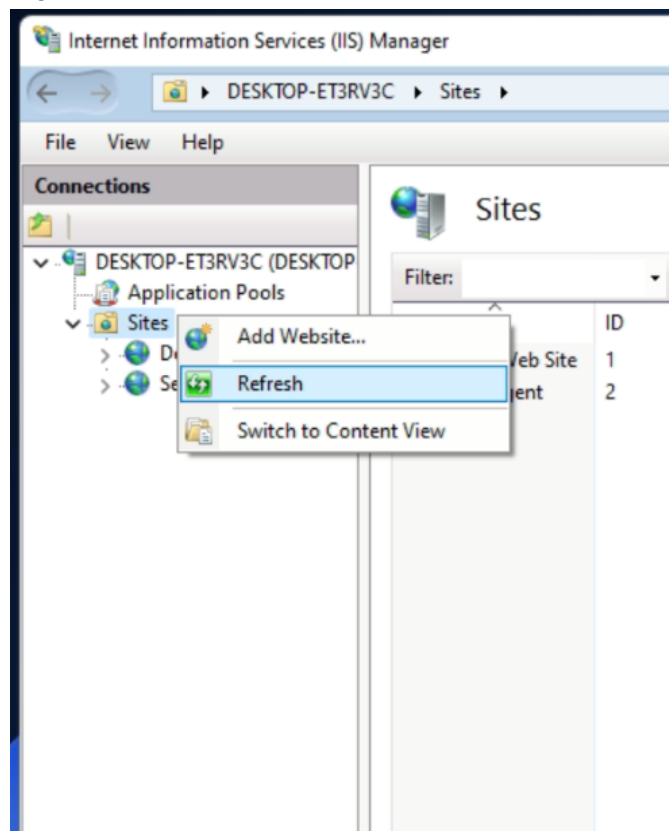


- c. Copy previously created certificate **e.g. sentec2.dev** (right click on sentec2.dev, click copy)
- d. Paste in Trusted Root Certification > Certificates (right click on Certificates folder under Trusted Root Certification, click paste)

8. Double Check **sentec2.dev** has been issued on **Trusted Root Certification**



9. Create localhost from IIS :
- a. Open IIS Manager
- Right Click on **Sites** → **Add Website**



- b. Create website with detailed below :

The 'Add Website' dialog box is shown with the following settings:

- Site name:** SentecAgent
- Application pool:** SentecAgent
- Content Directory:**
 - Physical path:** C:\Program Files\Sentec Agent
 - Pass-through authentication:** Connect as... Test Settings...
- Binding:**
 - Type:** https
 - IP address:** All Unassigned
 - Port:** 5000
 - Host name:**
 - ☐ Require Server Name Indication
 - ☐ Disable TLS 1.3 over TCP
 - ☐ Disable Legacy TLS
 - ☐ Disable OCSP Stapling
 - ☐ Disable QUIC
 - ☐ Disable HTTP/2
- SSL certificate:** localhost
- ☒ Start Website immediately

Buttons: OK, Cancel

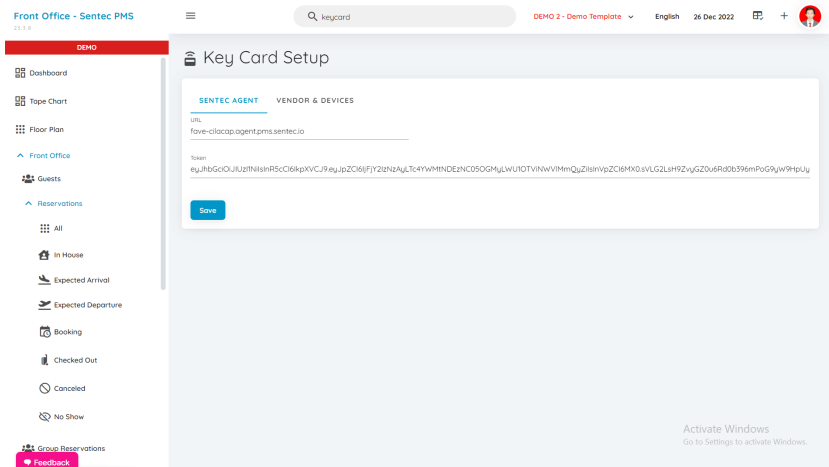
- c. Add IIS_IUSRS permission. Choose **sentec-agent** → **Edit Permissions** → **Security** → **Edit** → **Add** → **Fill out “Enter the Object Names” field with IIS_IUSRS** → **Ok All**
- d. Start IIS Service

11. Input username and password. Default username is “admin” or “Admin”, password “12345” or “123”

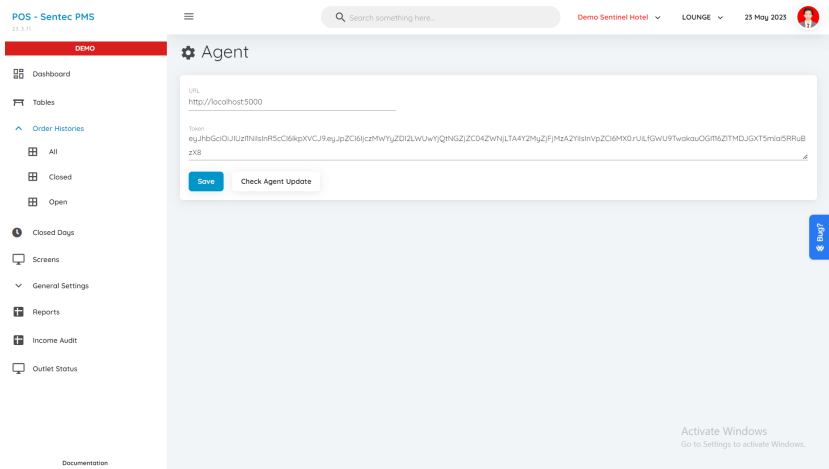
12. Copy one of the tokens listed after sign-in success

13. Open Key Card Setup menu in PMS (<https://pms.sentec.io/key-card-setup?hotelId=XXX>) and / or Agent menu in POS (<https://pos.sentec.io/agent?hotelId=XXX&outletId=YY>). Fill out the url field with the url of the service previously set up. Fill out the token field with the previously copied token. Save.

a. In PMS



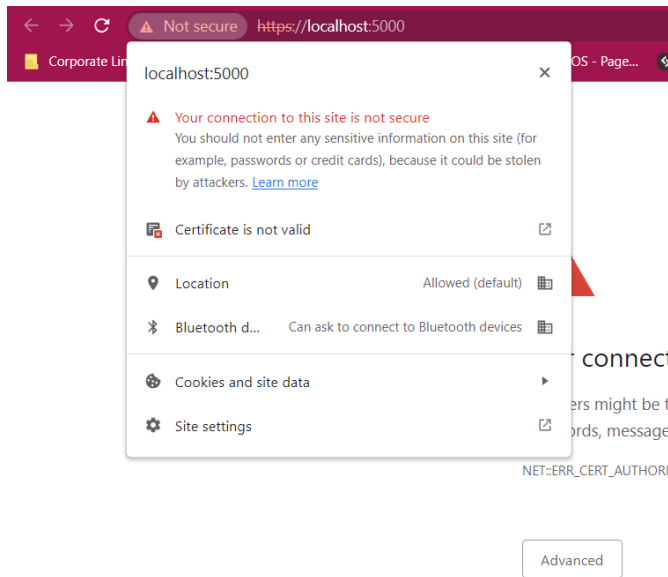
b. In POS



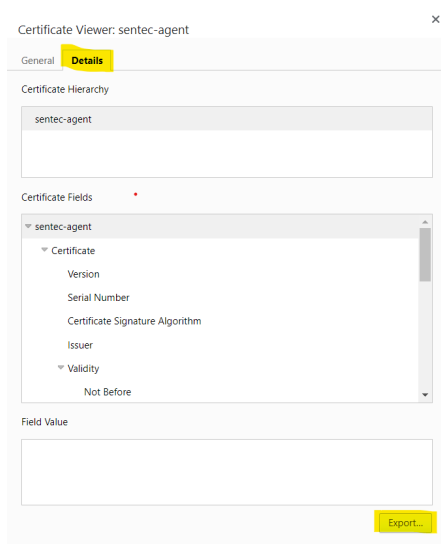
C. INSTALLING CERTIFICATE IN CLIENT COMPUTER

1. For windows computer

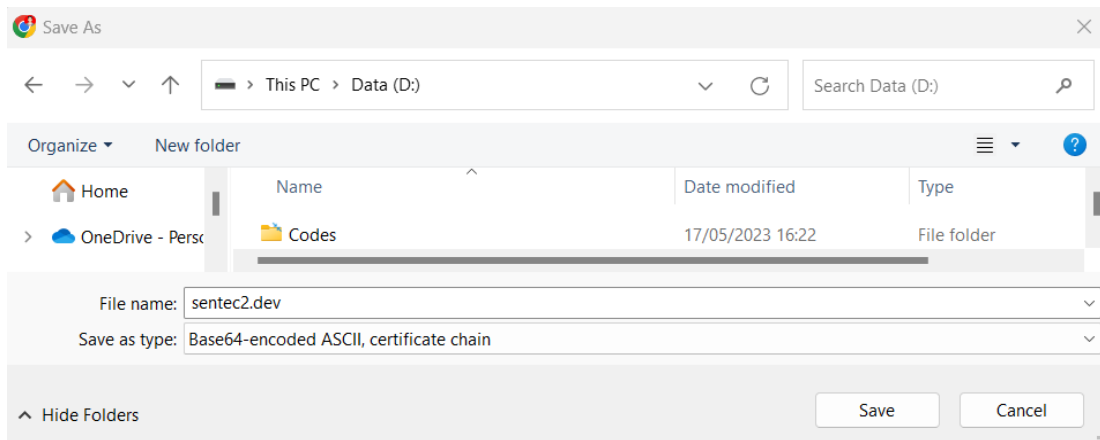
- Open browser and access the previously set up service e.g. <https://astoncilegon.agent.pms.sentec.io>
- Click on the Not Secure icon on the left of the address bar.
- Click “Certificate is not valid” option



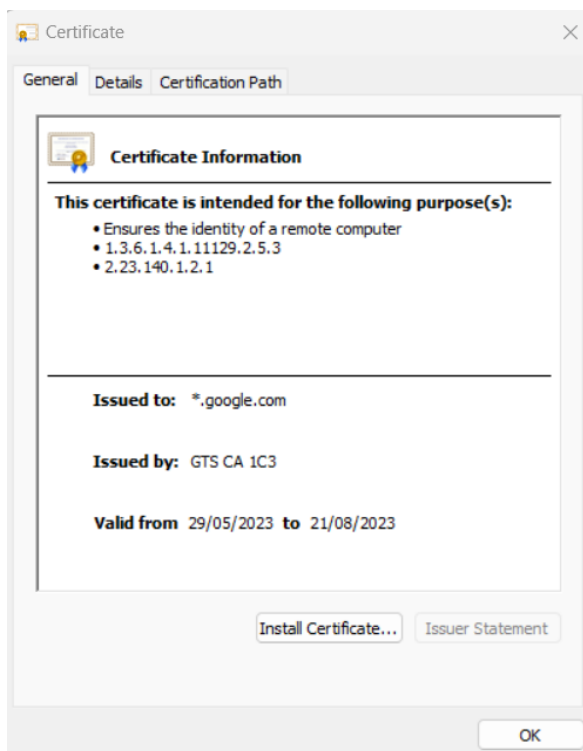
- Click on the “Detail” tab, click “Export..” button



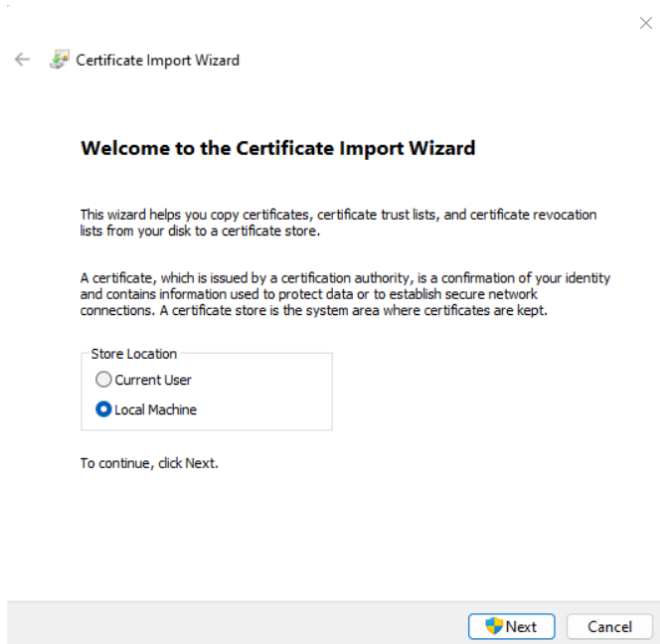
- e. Choose Base64-encoded ASCII, certificate chain in “Save as type” field. Save.



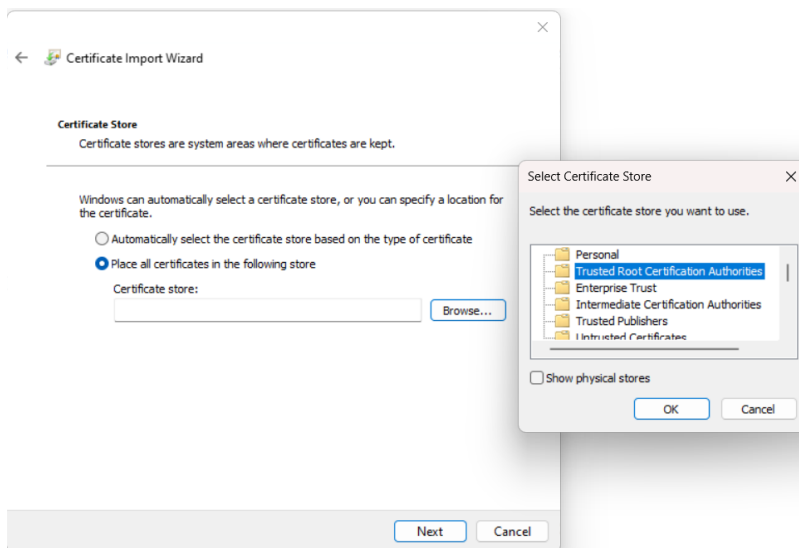
- f. Open the directory where you save the certificate. Double click on the certificate.
- g. Click on “Install Certificate”



- h. Choose “local machine”. Then click next.



- i. Choose “Place all certificates in the following store”. Then choose “Trusted Root Certification Authorities”. Click “OK” and “Next”.



- j. Click “Finish”
- k. Open browser and access the previously set up service e.g. <https://astoncilegon.agent.pms.sentec.io> again to see if it is accessible with https. Look for the lock icon on the left side of the address bar. If it is there, then the installation is complete.