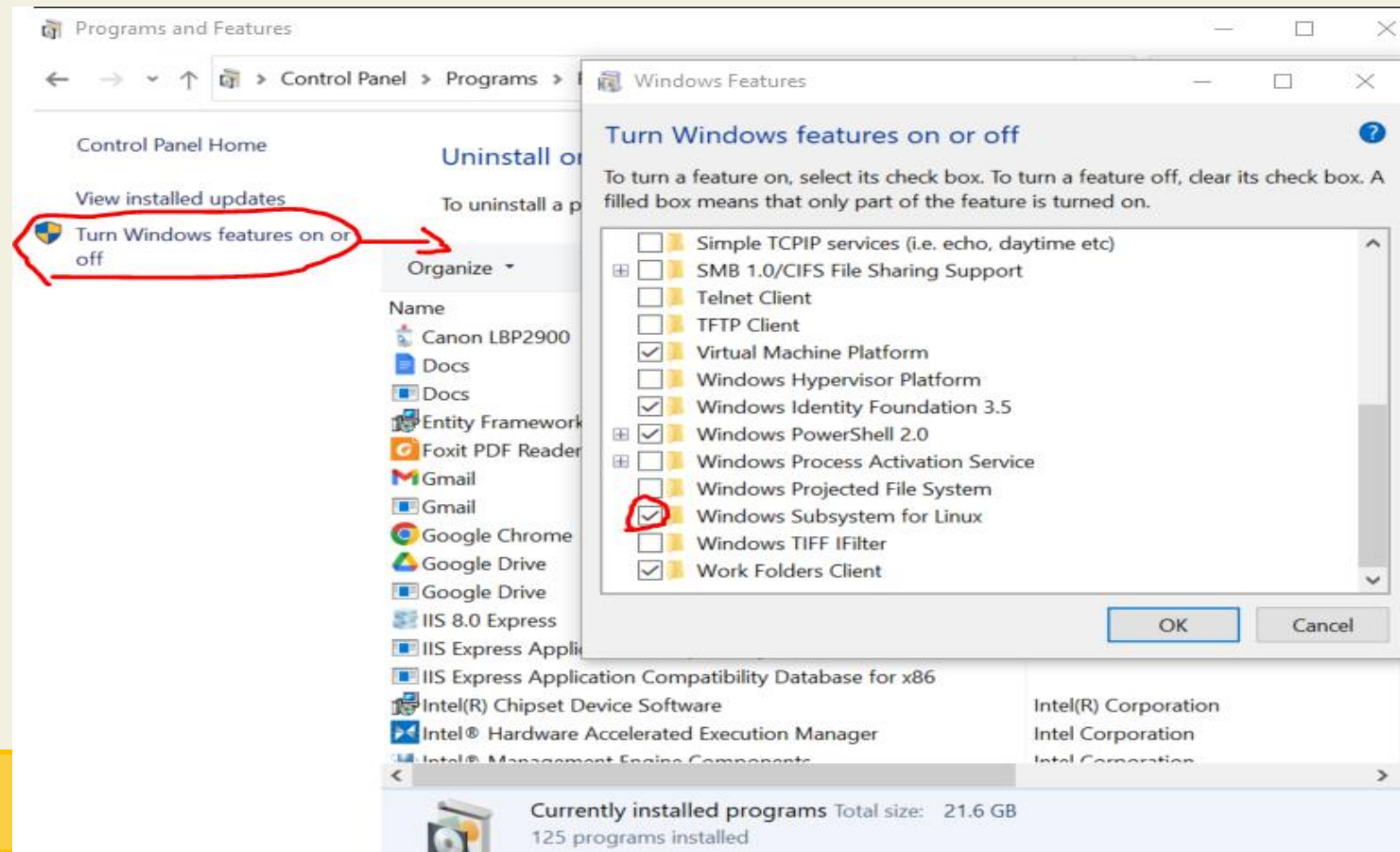


THỰC HÀNH SSL

Các bước thực hành

- Trường hợp máy tính Ubuntu: Không cần phải thực hiện các bước cài đặt dưới
- Máy tính Windows: chuẩn bị môi trường như sau:
 - + Tiến hành cài đặt WSL (Windows Subsystem Linux)
 - + Cài đặt Ubuntu trên Windows
 - + Tạo một website localhost đơn giản (chỉ cần heading)
 - + Tạo CA và add CA vào trình duyệt
 - + Cài đặt Https

- Cài đặt Ubuntu sử dụng chung với Windows: Bật Windows Subsystem Linux
- Có 02 cách thực hiện:
- Cách 1: Control Panel → Programs (Uninstall) → Turn Windows features on or off → chọn Windows Subsystem for Linux



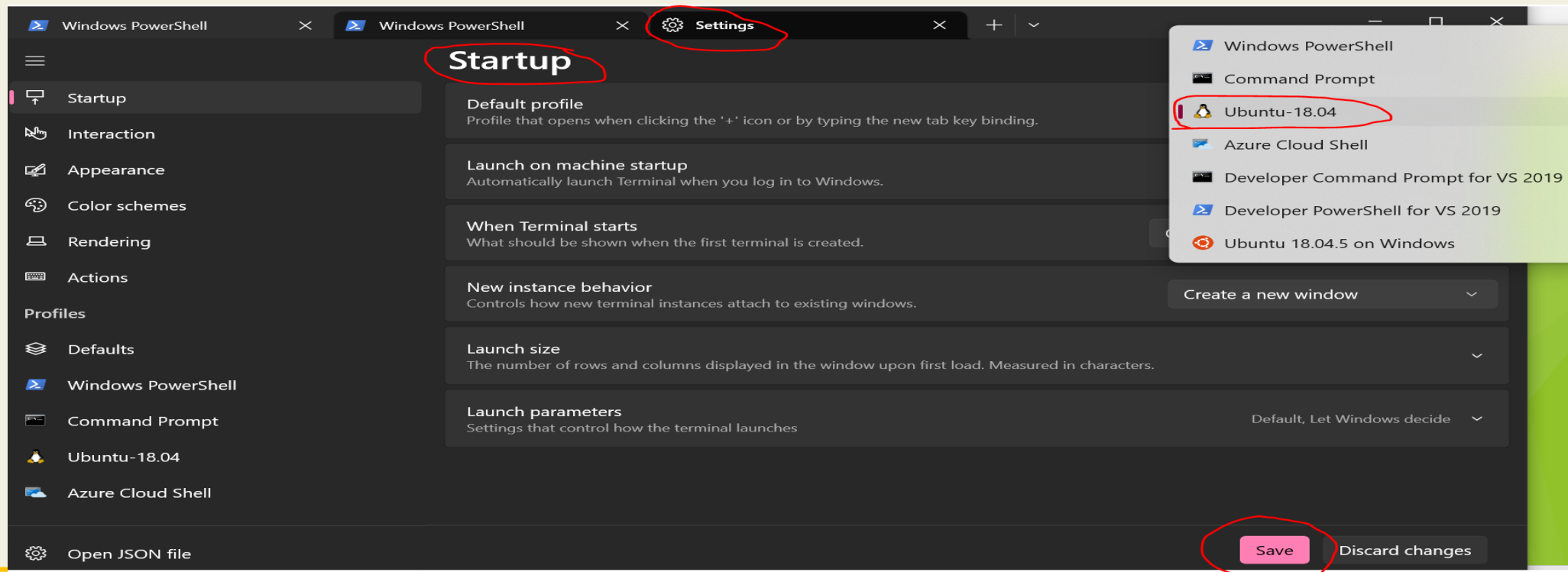
Cài đặt Ubuntu sử dụng chung với Windows: Bật Windows Subsystem Linux (WSL)

Có 02 cách thực hiện:

❑ **Cách 2:** Cài đặt WSL từng bước theo hướng dẫn tại: <https://learn.microsoft.com/en-us/windows/wsl/install-manual>

- **Step 1:** Mở PowerShell as Administrator và thực hiện lệnh: `dism.exe /online /enable-feature /featurename:Microsoft-Windows-Subsystem-Linux /all /norestart`
- **Step 2:** Kiểm tra các yêu cầu để chạy WSL 2.
 - Điều kiện: Hệ điều hành Windows 10 trở lên: Với x64 thì version 1903, Build 18362.1049 trở lên; Với ARM64 thì version 2004 và Build 19041 trở lên
- **Step 3:** Bật các thuộc tính máy ảo. Tại PowerShell thực hiện lệnh: `dism.exe /online /enable-feature /featurename:VirtualMachinePlatform /all /norestart`
- **Step 4:** Tải Linux kernel với gói mới nhất
 - Tại đây: https://wslstorestorage.blob.core.windows.net/wslblob/wsl_update_x64.msi
 - Sau khi tải về nên restart lại máy và cài đặt file tải về.
- **Step 5:** Thiết lập WSL 2 như một phiên bản mặc định bằng lệnh sau trong PowerShell: `wsl --set-default-version 2`
- **Step 6:** Cài đặt phiên bản Linux phù hợp: ví dụ chọn Ubuntu 18.04LTS
 - Để thuận tiện nên cài đặt Windows Terminal sử dụng, bằng cách tải tại store của Windows

- Sau đó mở cửa sổ Ubuntu và chúng ta sẽ dùng các câu lệnh bình thường như trên HĐH ubuntu. Tại đây thiết lập username và password
- Để thiết lập user về root thì tại PowerShell thực hiện lệnh: `ubuntu1804 config --default-user root`



Chuyener ve root tren power shell:
ubuntu config --default-user root

Tạo CA cho trình duyệt

1-Tạo cặp khóa private key:

- `openssl genrsa -des3 -out rootCA.key 2048`

Sau đó nhập pass cho khóa:

```
Enter pass phrase for rootCA.key:
140648370914624:error:28078065:UI routines:UI_set_result_ex:result too small:../crypto/ui/ui_lib.c:905
:You must type in 4 to 1023 characters
Enter pass phrase for rootCA.key:
Verifying - Enter pass phrase for rootCA.key:
root@Leanh:/mnt/d/thuchanhssl_anninhmang# |
```

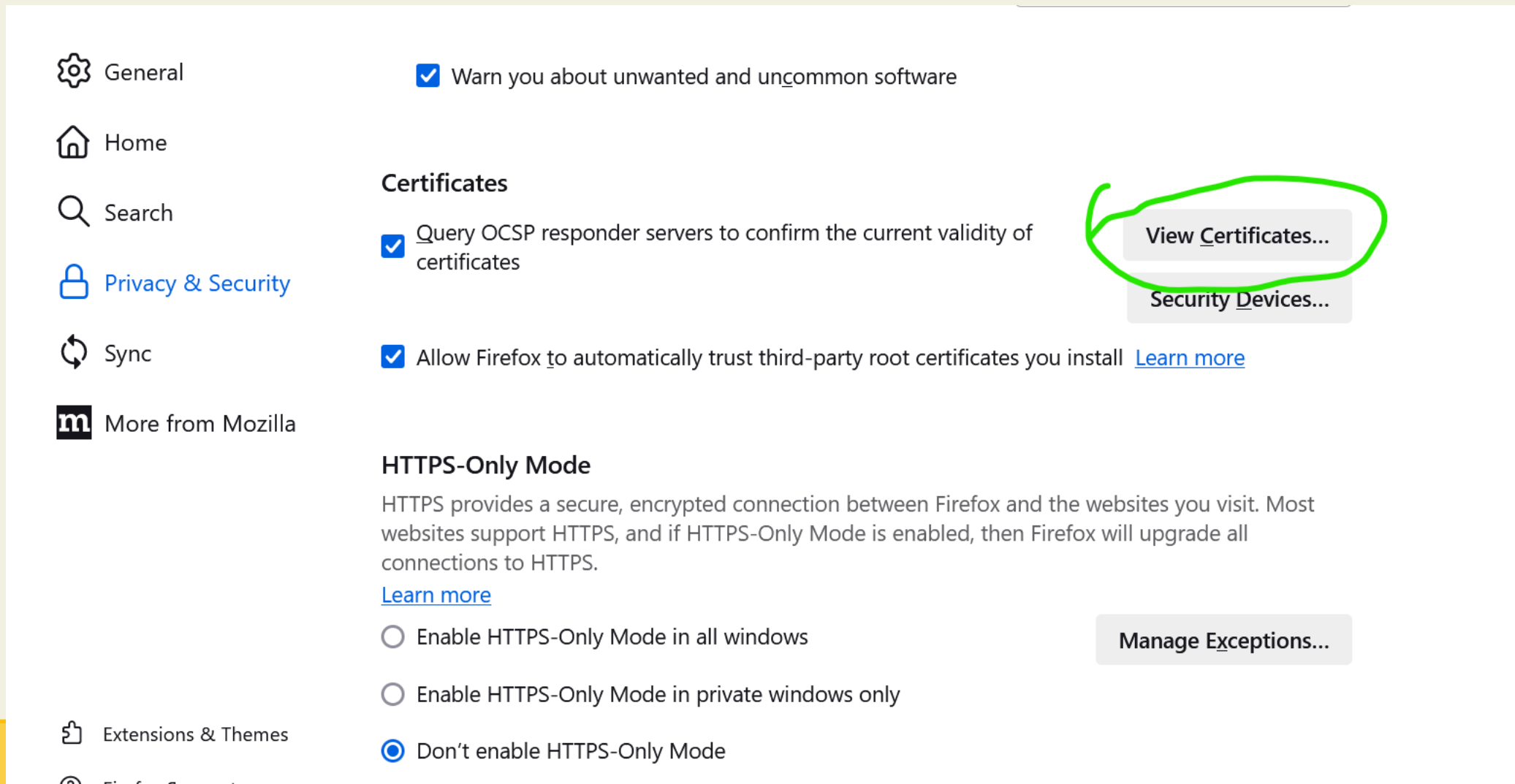
Tạo CA cho trình duyệt

2- Tạo CA:

`openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1825 -out rootCA.pem`

```
root@Leanh:/mnt/d/thuchanhssl_anninhmang# openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1825 -out rootCA.pem
Enter pass phrase for rootCA.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:VN
State or Province Name (full name) [Some-State]:HN
Locality Name (eg, city) []:NamTuLiem
Organization Name (eg, company) [Internet Widgits Pty Ltd]:HAUI
Organizational Unit Name (eg, section) []:FIT_HAUI
Common Name (e.g. server FQDN or YOUR name) []:AnhLe
Email Address []:anninhmang123@gmail.com
root@Leanh:/mnt/d/thuchanhssl_anninhmang#
```


Cài đặt CA cho trình duyệt



The screenshot shows the 'Privacy & Security' settings page in a Firefox browser. The left sidebar contains navigation links: General, Home, Search, Privacy & Security (highlighted), Sync, and More from Mozilla. The main content area is divided into sections: 'Certificates' and 'HTTPS-Only Mode'. In the 'Certificates' section, there are three checked options: 'Warn you about unwanted and uncommon software', 'Query OCSP responder servers to confirm the current validity of certificates', and 'Allow Firefox to automatically trust third-party root certificates you install'. A green circle highlights the 'View Certificates...' button. Below it is the 'Security Devices...' button. The 'HTTPS-Only Mode' section includes a description of HTTPS and a 'Learn more' link. At the bottom, there are three radio button options for enabling HTTPS-Only Mode, with 'Don't enable HTTPS-Only Mode' selected. A 'Manage Exceptions...' button is also visible.

General ☒ Warn you about unwanted and uncommon software

Home

Search

Privacy & Security

Sync

m More from Mozilla

Certificates

☒ Query OCSP responder servers to confirm the current validity of certificates

☒ Allow Firefox to automatically trust third-party root certificates you install [Learn more](#)

View Certificates...

Security Devices...

HTTPS-Only Mode

HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS. [Learn more](#)

☐ Enable HTTPS-Only Mode in all windows

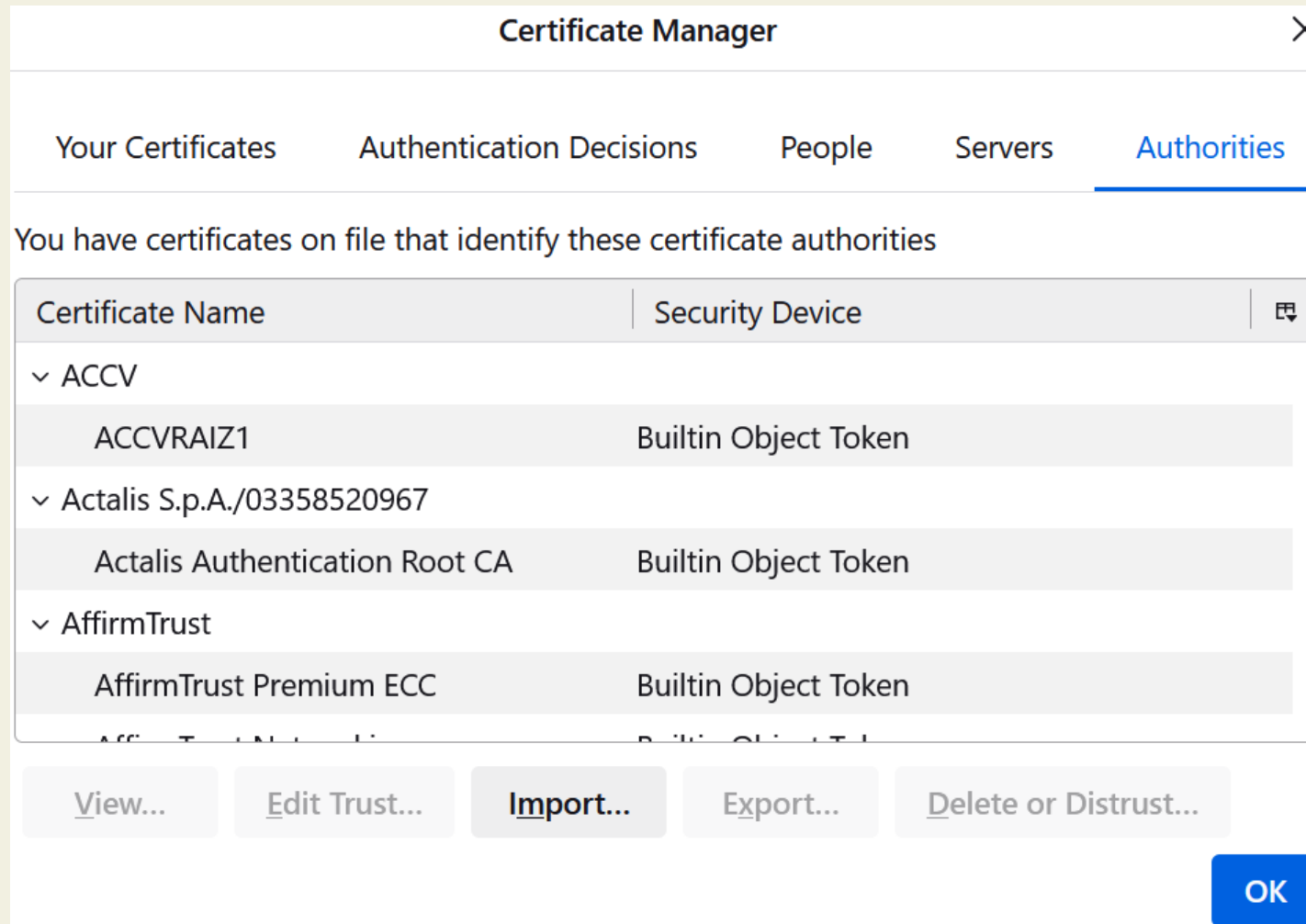
☐ Enable HTTPS-Only Mode in private windows only

☒ Don't enable HTTPS-Only Mode

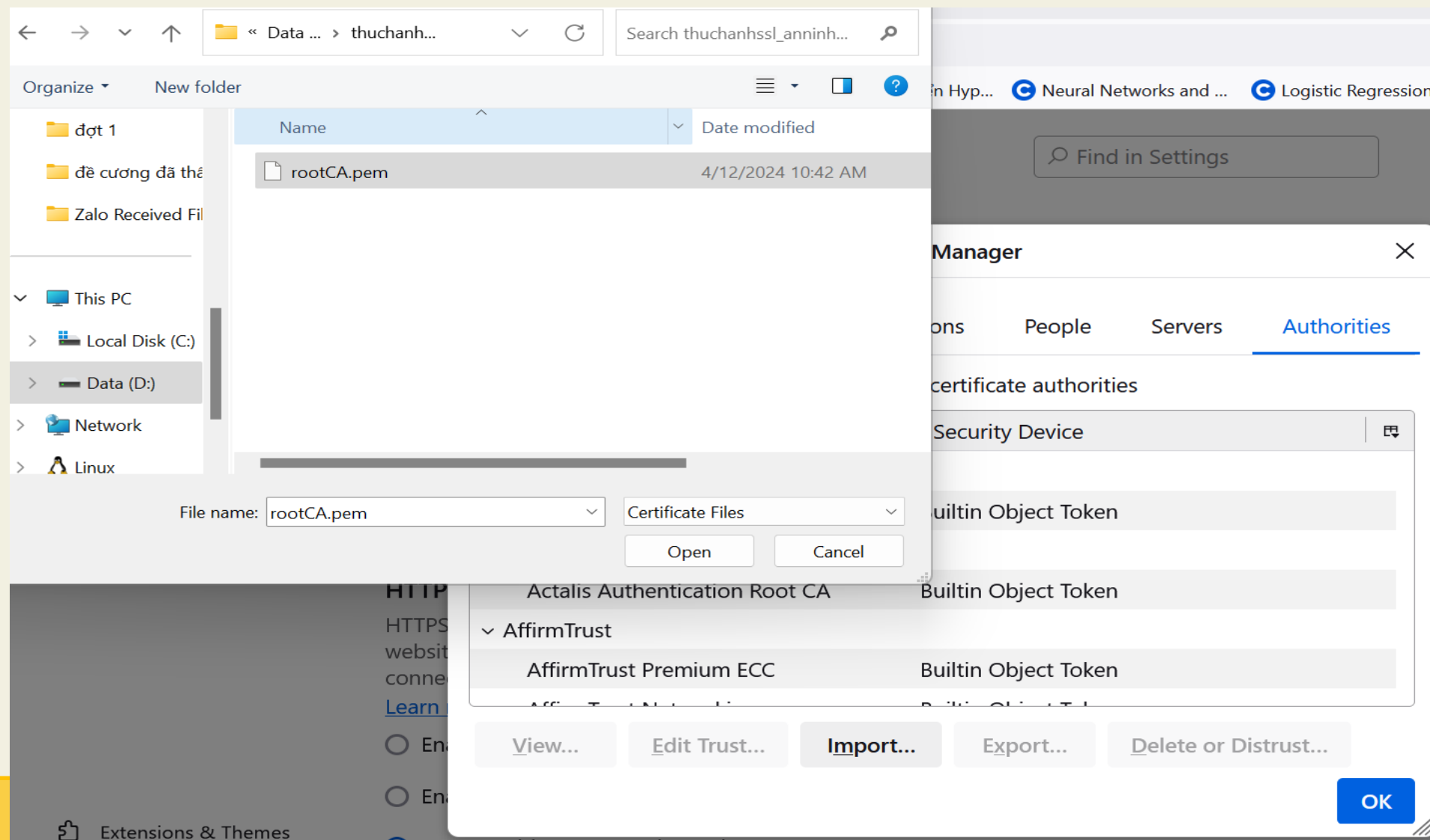
Manage Exceptions...

Extensions & Themes

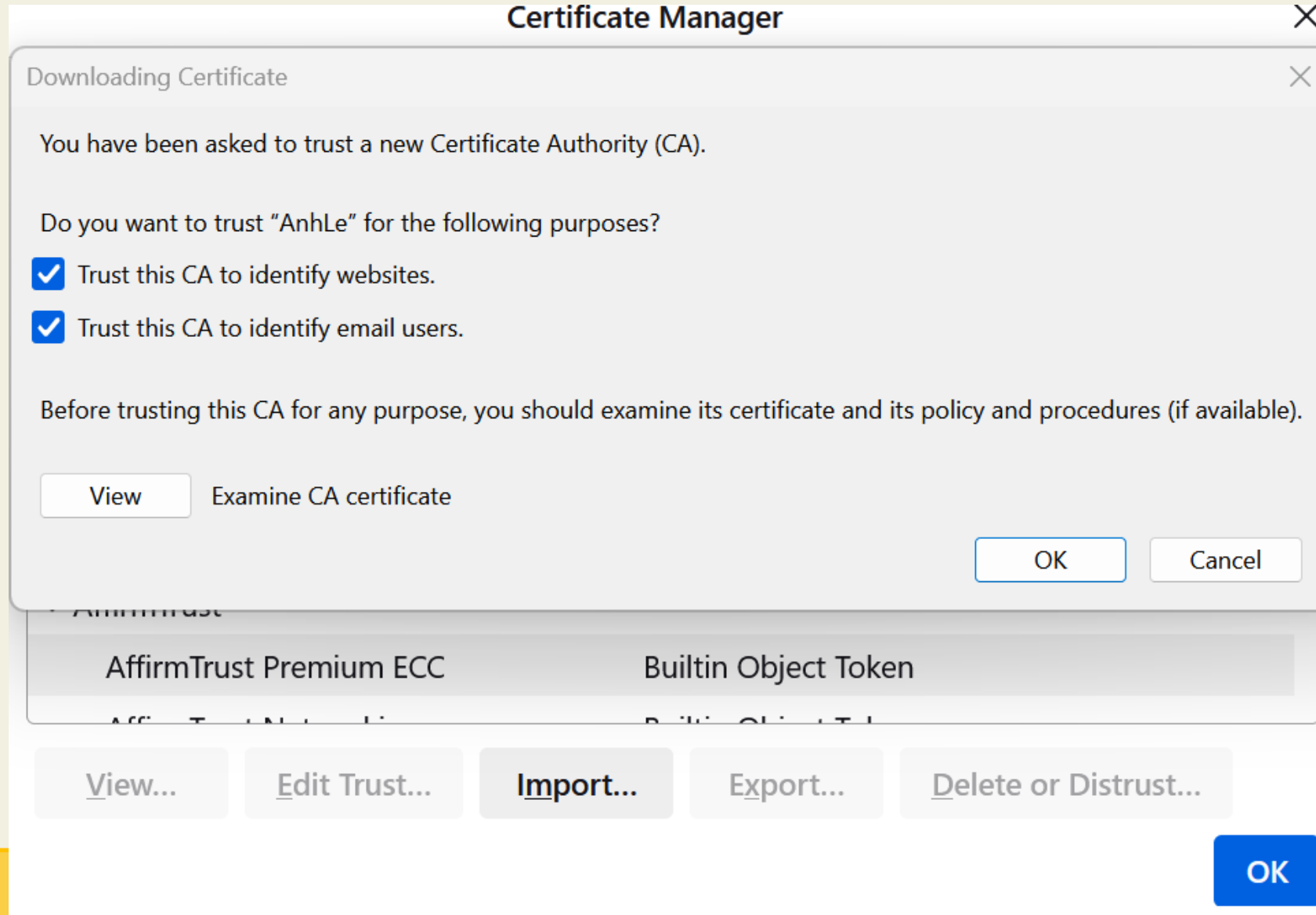
Cài đặt CA cho trình duyệt



Cài đặt CA cho trình duyệt



Cài đặt CA cho trình duyệt



Cài đặt CA cho trình duyệt

Certificate

AnhLe

Subject Name

Country	VN
State/Province	HN
Locality	NamTuLiem
Organization	HAUI
Organizational Unit	FIT_HAUI
Common Name	AnhLe
Email Address	anninhmang123@gmail.com

Issuer Name

Country	VN
State/Province	HN
Locality	NamTuLiem
Organization	HAUI
Organizational Unit	FIT_HAUI
Common Name	AnhLe
Email Address	anninhmang123@gmail.com

Validity

Not Before	Fri, 12 Apr 2024 03:42:46 GMT
Not After	Wed, 11 Apr 2029 03:42:46 GMT

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	BC:3B:74:CF:92:42:62:68:83:50:62:89:D3:54:3C:01:42:BE:CE:5F:28:61:E8:51:1F:16:...

Miscellaneous

Serial Number	21:05:74:06:5F:FB:C6:1A:39:A0:B2:8C:9C:DE:AD:0C:94:F9:E6:9C
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	28:8B:B3:5D:99:1C:C5:F9:F1:89:D7:9D:DF:A8:DD:E3:34:16:77:ED:A7:35:32:A9:87:...
SHA-1	D7:9A:2A:6F:5F:67:C1:97:4A:9E:A8:E5:64:C8:54:77:F7:46:65:9B

- Tạo private key cho domain local (tên tùy đặt, ví dụ: test-ssl.local)
 - openssl genrsa -out test-ssl.local.key 2048
- Tạo request CSR (certificate signing request)
 - openssl req -new -key test-ssl.local.key -out test-ssl.local.csr

```
root@Leanh: /mnt/d/thuchanhssl_anninhmang# openssl req -new -key test-ssl.local.key -out test-ssl.local.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:VN
State or Province Name (full name) [Some-State]:Hanoi
Locality Name (eg, city) []:namtuliem
Organization Name (eg, company) [Internet Widgits Pty Ltd]:hau
Organizational Unit Name (eg, section) []:fit
Common Name (e.g. server FQDN or YOUR name) []:anhle
Email Address []:anninhmang123@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:1234
root@Leanh: /mnt/d/thuchanhssl_anninhmang#
```

- Tạo một file config để định nghĩa SAN (Subject Alternative Name là 1 extension của X.509) cho SSL:

- vi test-ssl.local.ext
- Paste nội dung sau vào và lưu thoát (:x!):

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation,
keyEncipherment, dataEncipherment
subjectAltName = @alt_names
```

```
[alt_names]
DNS.1 = test-ssl.local
```

- Khi đó trong thư mục có các file sau:

```
Alt optional company name [].1234
root@Leanh:/mnt/d/thuchanhssl_anninhmang# vi test-ssl.local.ext
root@Leanh:/mnt/d/thuchanhssl_anninhmang# ls
rootCA.key  rootCA.pem  test-ssl.local.csr  test-ssl.local.ext  test-ssl.local.key
root@Leanh:/mnt/d/thuchanhssl_anninhmang#
```

- Tạo CA cho domain:
 - openssl x509 -req -in test-ssl.local.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial \-out test-ssl.local.crt -days 1825 -sha256 -extfile test-ssl.local.ext

```
rootCA.key rootCA.pem test-ssl.local.csr test-ssl.local.ext test-ssl.local.key
root@Leanh:/mnt/d/thuchanhssl_anninhmang# openssl x509 -req -in test-ssl.local.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial \
> -out test-ssl.local.crt -days 1825 -sha256 -extfile test-ssl.local.ext
Signature ok
subject=C = VN, ST = Hanoi, L = namtuliem, O = hauui, OU = fit, CN = anhle, emailAddress = anninhmang123@gmail.com
Getting CA Private Key
Enter pass phrase for rootCA.key:
root@Leanh:/mnt/d/thuchanhssl_anninhmang# ls
rootCA.key rootCA.srl test-ssl.local.csr test-ssl.local.key
rootCA.pem test-ssl.local.crt test-ssl.local.ext
root@Leanh:/mnt/d/thuchanhssl_anninhmang#
```

→ Thêm HTTPS cho local domain với private key file và certificate file đã tạo

Cài đặt HTTPS với NginX