

### Step 1:

- **Navigate to: https://<Your ALB DNS>**
- **Validation of ALB identity will fail as the browser doesn't have the root certificate in its trust store**

## Private CAs

### Create CA

**Actions**

	CA common name	Organization	OU	Type	Status
	Test Root	Test		Root	Deleted
	acmpcasubordinateca g1	mycompany	hr	Subordinate	Active
	acmpcaroot g1	mycompany	hr	Root	Active

### Status

### CA certificate

### Revocation configuration

## Tags

### Permissions

## Subject

Organization (O)	mycompany
Organization Unit (OU)	hr
State or province name	washington
Locality name	seattle
Common Name (CN)	acmpcaroot g1

## CA certificate validity

Not after	2029-08-20 15:26:20UTC
Expires in	3652 Days

### Additional information

Signature algorithm	SHA256WITHRSA
Serial number	

### Certificate body

-----BEGIN CERTIFICATE-----

MTIDjTCCAnWgAwISAgIRAJDjMRrmWov20Zib0FJWdEmwDQYJKoZInvcNAQELBQAw  
YDETBEGA1UECAwKd2FzaGluz3RvbjEQAQA4GA1UEBwwHc2VhdHRsZTESMBAGA1UE  
CgwJbXJjb21wYW5wMQswCQYDVQQLDAJocjEWMBQGA1UEAwwNYWYwNtCGNhcm9vdCBn  
MTAeFw0xOTA4MjAxNDIzMjBhFw0yOTA4MjAxNTIzMjBhMGAxEzARBGNVBAgMCndh  
c2hpbmd0b24xEDA0BgNVBAcMB3NlYXR0bGUxJzAQBGNVBAoMCW15Y29tCGFueTEL  
MAKGA1UECwwaHGFifjAUBGNVBAAMDWFjYXBxJzA3VjB3QgzZEWggEiMA0GCSqGSIb3  
DQEBAQUAA4IBDwAwGGAkAIAoAIBQCDmTvmq1cYv3cJQmw0mKsYkRoPABXjYdBEfPy  
Uwd8n9N2ntZ9lWqcvg+FGOCzeE3+Uowag7AGyKhknpWpJauJZGUNvn5SLYdvkvaRw  
lzQTYbH6KXM7bXE1kIU2ppw9JsUUNwcMTWbf1PLd2ODZjh5p8qbcnGQWG+8khk5



[Export Certificate body to a file](#)

### Step 2:

- Under ACM > Private CAs
- Select Root CA
- Click “Export Certificate body to a file”
- Certificate.pem will be saved to your laptop

- People
- Autofill
- Appearance
- Search engine
- Default browser
- On startup

Advanced

Extensions



About Chrome

## Privacy and security

## Sync and Google services

More settings that relate to privacy, security, and data collection



## Allow Chrome sign-in

By turning this off, you can sign in to Google sites like Gmail without signing in to Chrome



## Send a "Do Not Track" request with your browsing traffic



## Allow sites to check if you have payment methods saved



## Preload pages for faster browsing and searching

Uses cookies to remember your preferences, even if you don't visit those pages



## Manage certificates

Manage HTTPS/SSL certificates and settings



## Manage security keys

Reset security keys and create PINs



## Site Settings

Control what information websites can use and what content they can show you



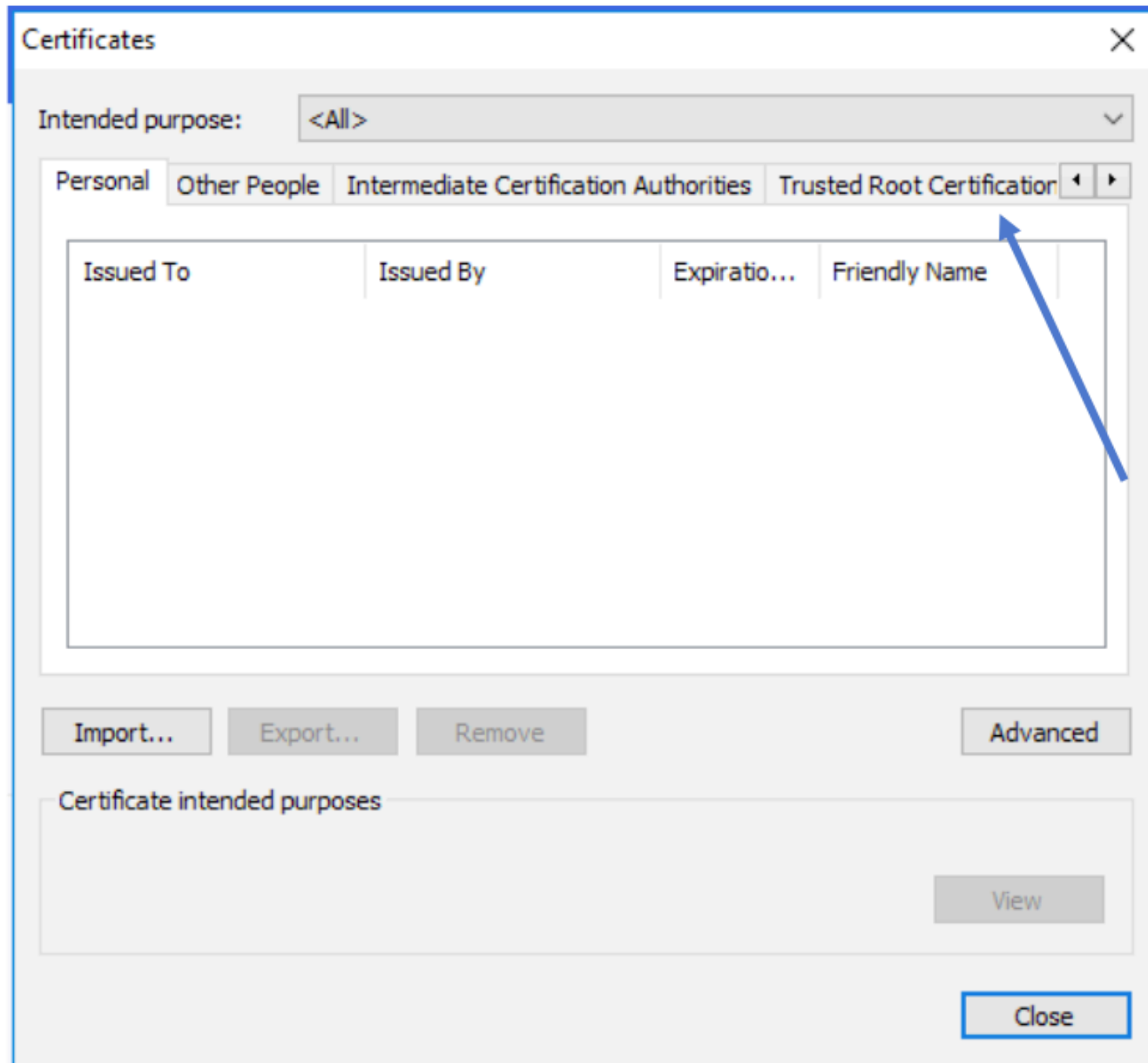
## Clear browsing data

Clear history, cookies, cache, and more



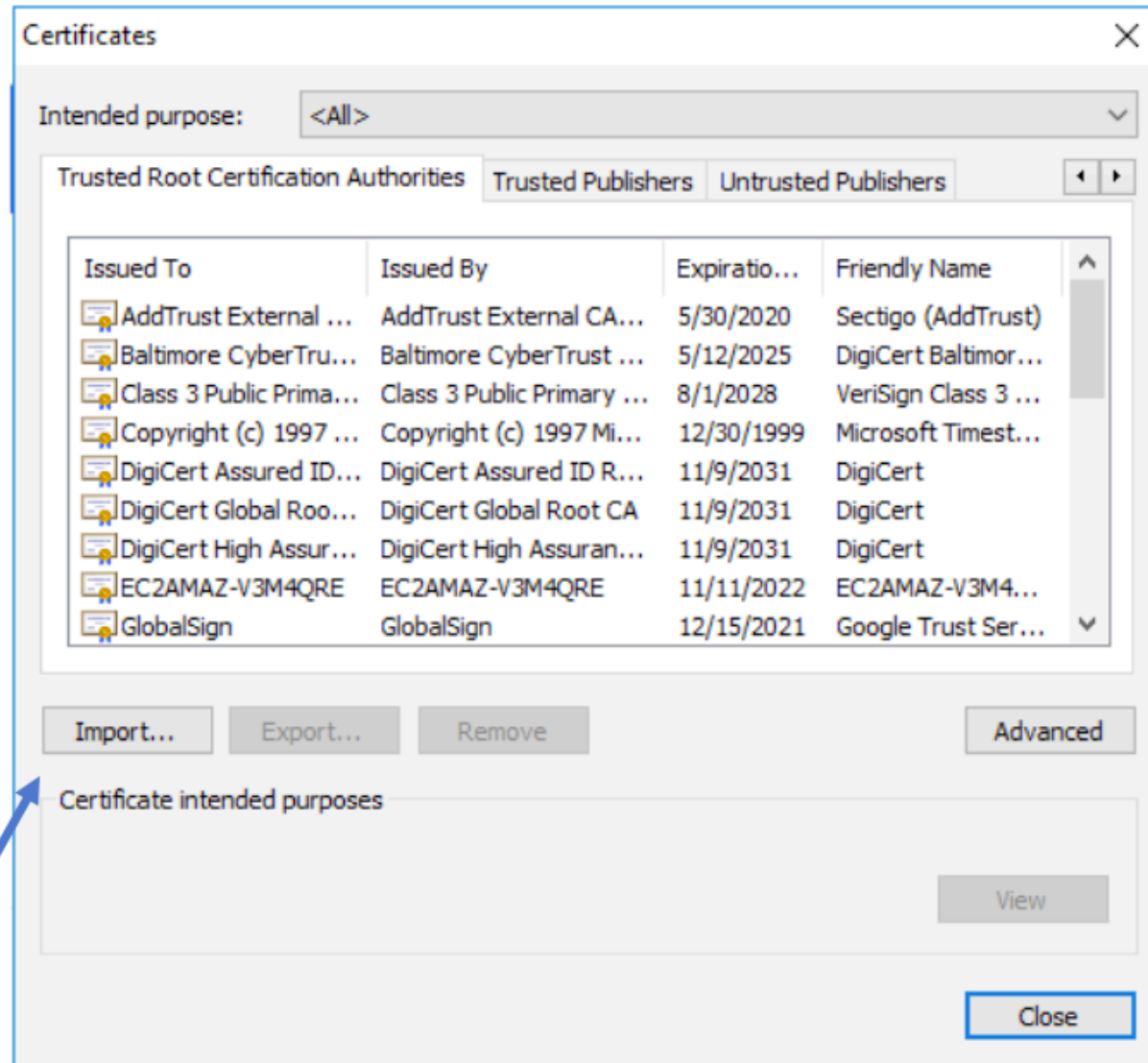
## Step 3:

- Go to Settings
- Search 'certificates'
- Click the expand button



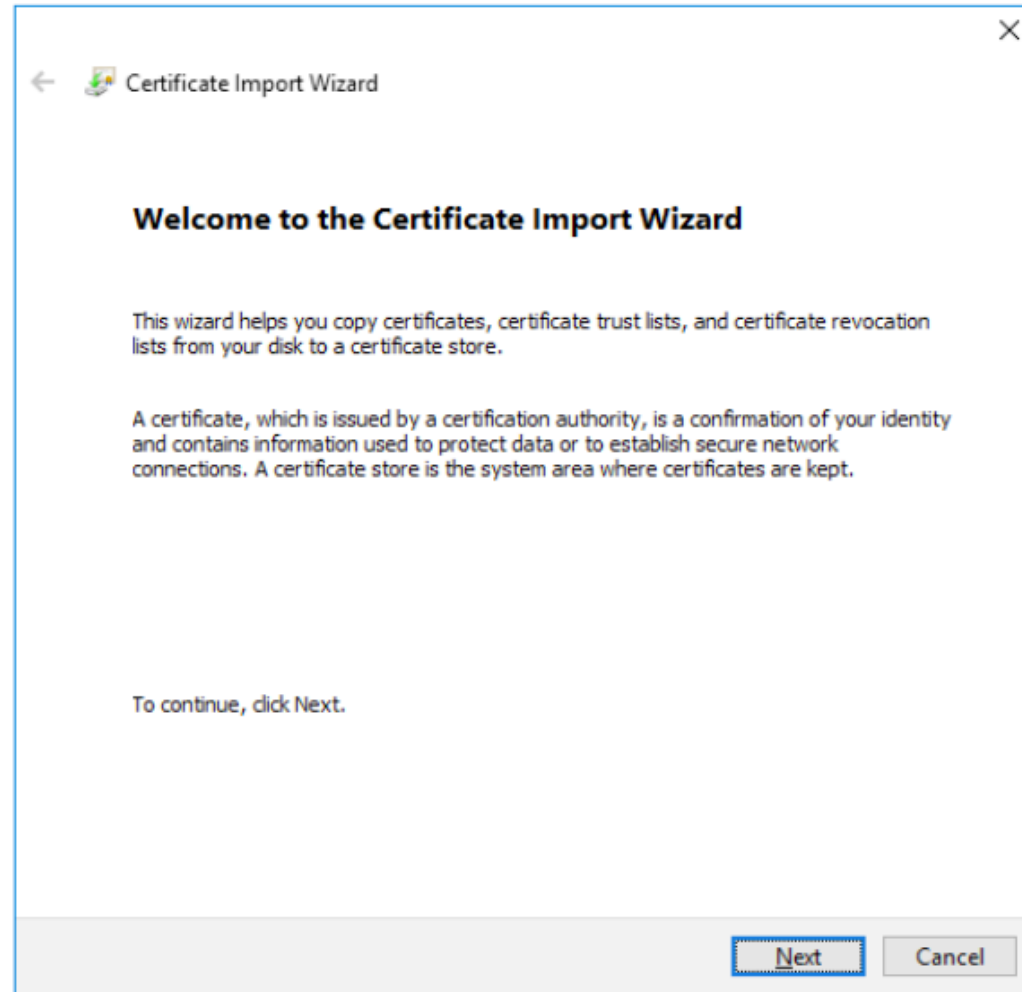
**Step 4:**

- **Click on 'Trusted Root Certification Authorities'**




### Step 5:

- Click on 'Import'



- Step 6:**
- Click 'Next'

←  Certificate Import Wizard

**File to Import**  
Specify the file you want to import.

---

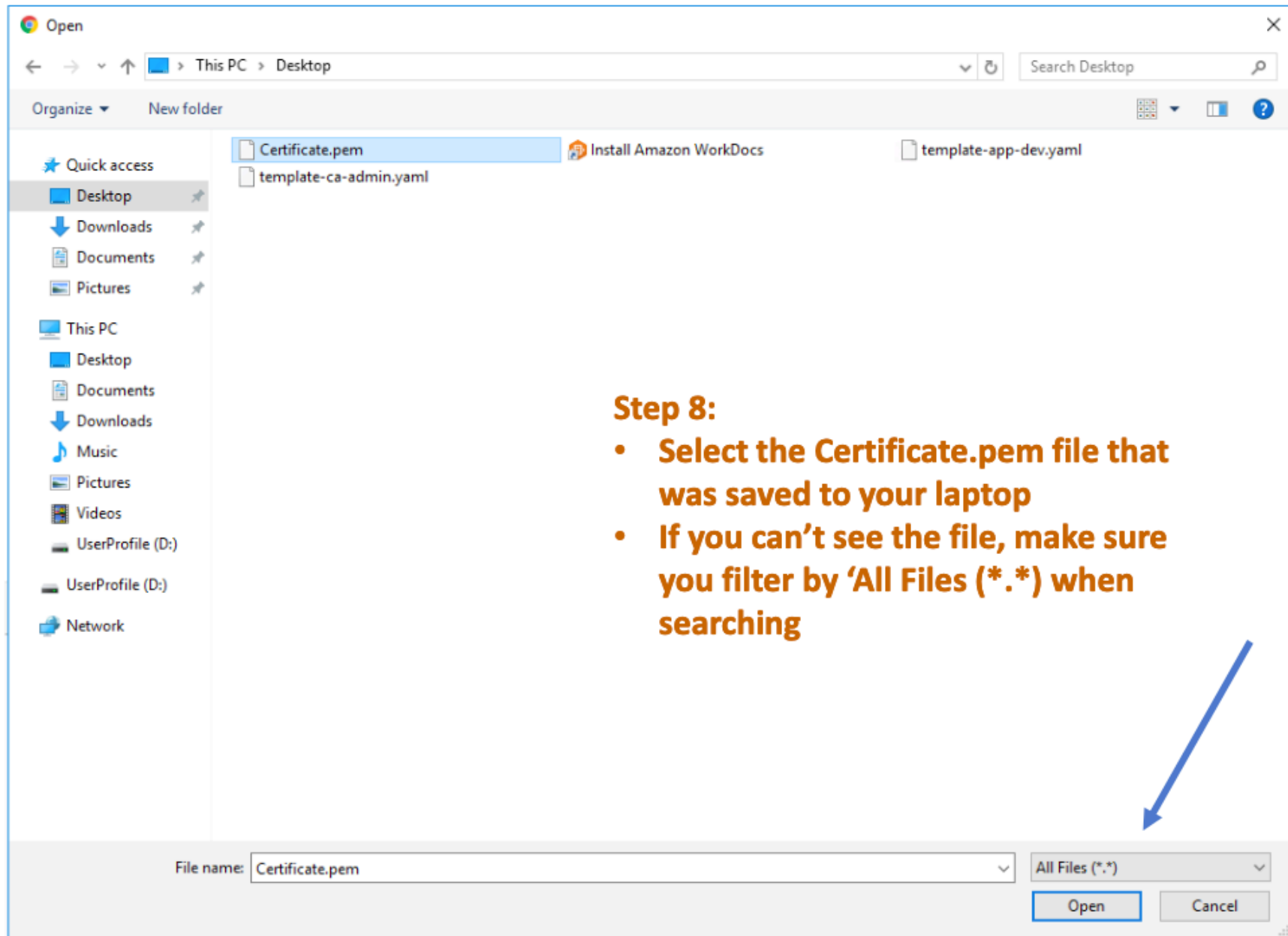
File name:

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

**Step 7:**

- Click on 'Browse'





### Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

- ☐ Automatically select the certificate store based on the type of certificate
- ☒ Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Browse...

Next

Cancel

**Step 9:**  
• Click 'Next'

## Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

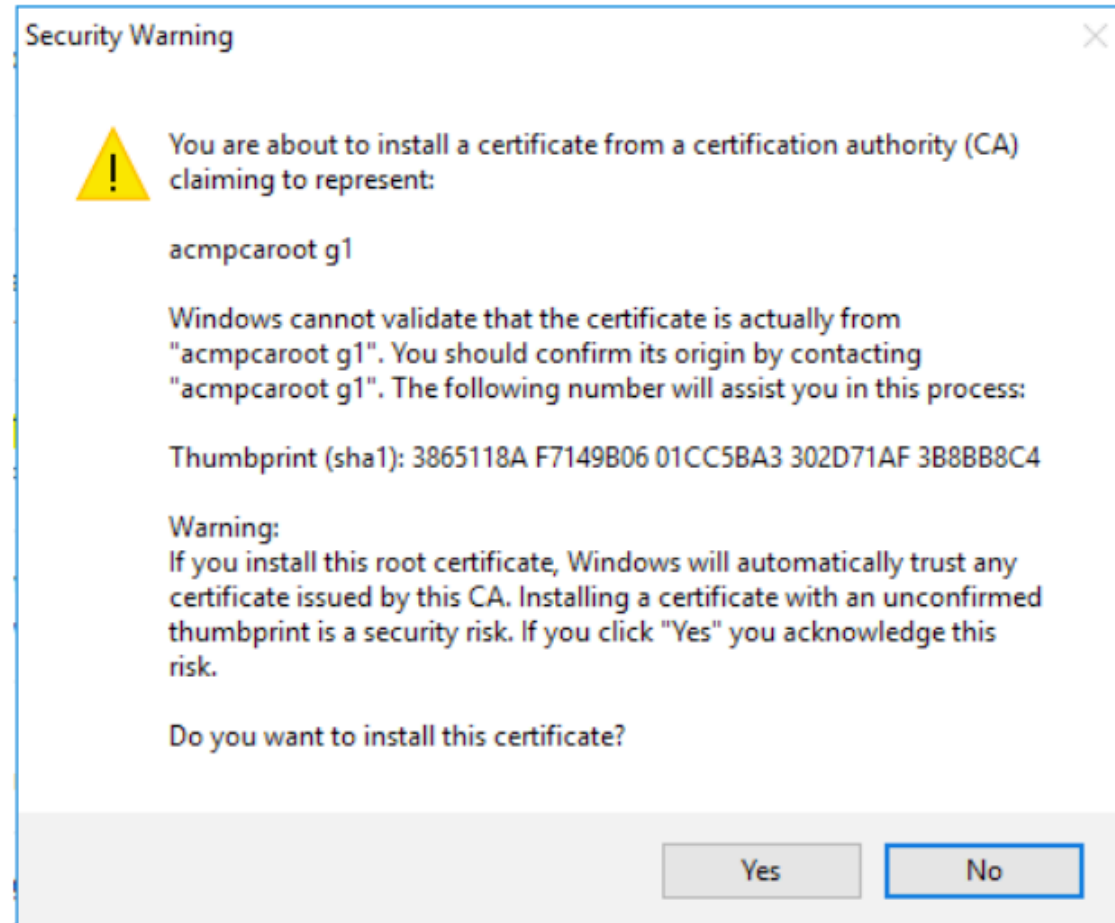
Certificate Store Selected by User	Personal
Content	Certificate
File Name	

Finish

Cancel

**Step 10:**  
• Click 'Finish'





**Step 11:**

- Click 'Yes'

Certificate Import Wizard

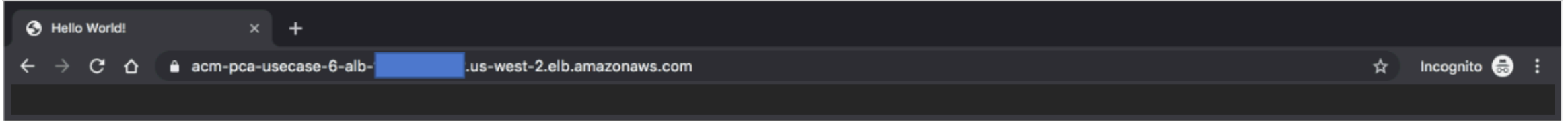


The import was successful.

OK

**Step 12:**

- **Click 'Ok'**
- **You have now imported the certificate successfully**



# Hello World!

**Step 13:**

- **Reload the webpage**
- **(You may need to clear cache)**
- **Notice the lock icon (Secure TLS Connection)**