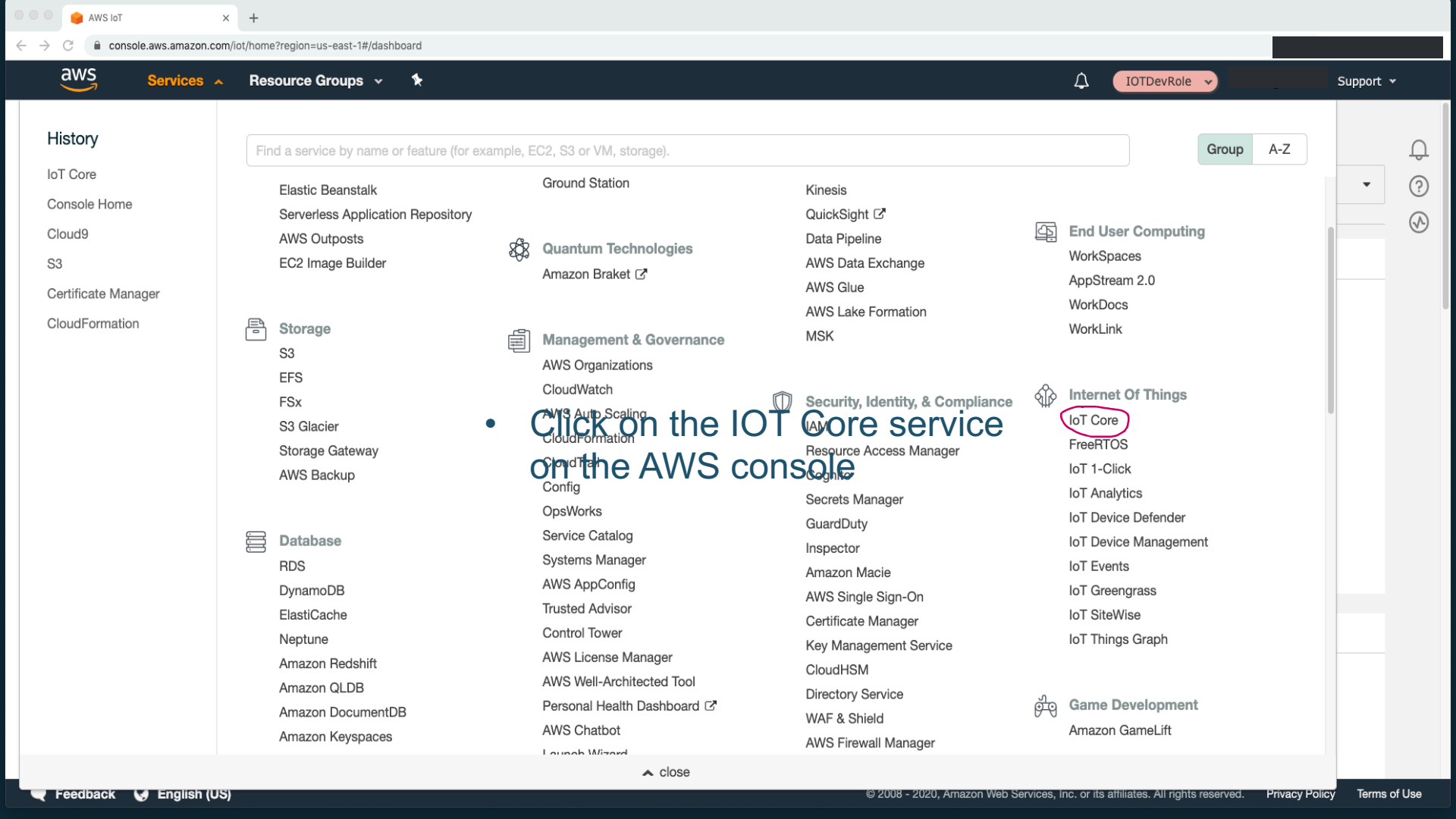


- Click on the IOT Core service on the AWS console

AWS IoT

console.aws.amazon.com/iot/home?region=us-east-1#/cacertificatehub

aws | Services | Resource Groups | IOTDevRole | Support

AWS IoT

- Monitor
- Onboard
- Manage
- Greengrass
- Secure
  - Certificates
  - Policies
  - CAs
  - Role Aliases
  - Authorizers
- Defend
- Act
- Test

Software

Settings

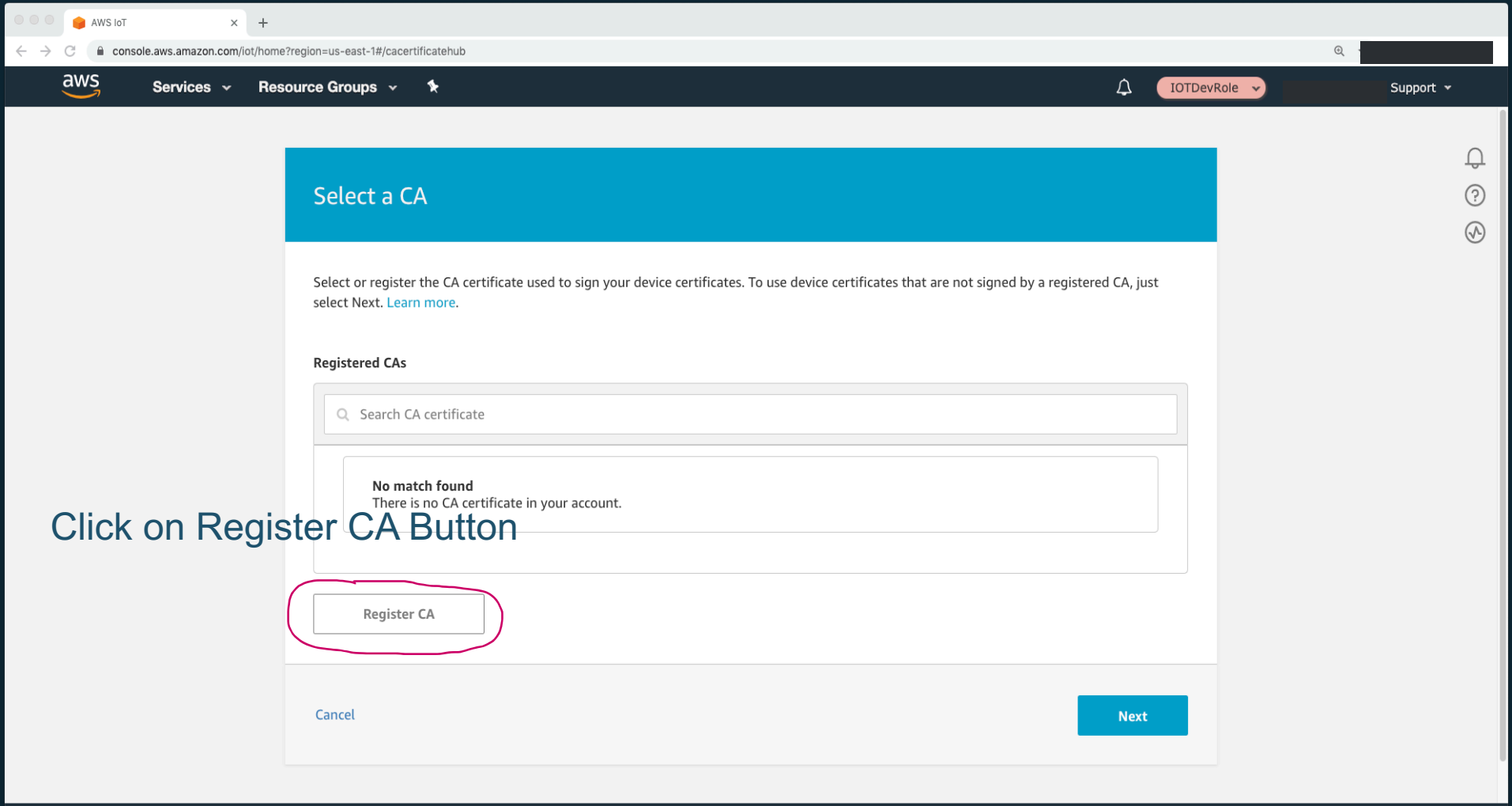
Under Secure -> Select CAs

Click on Register a CA Button

You don't have any CAs yet

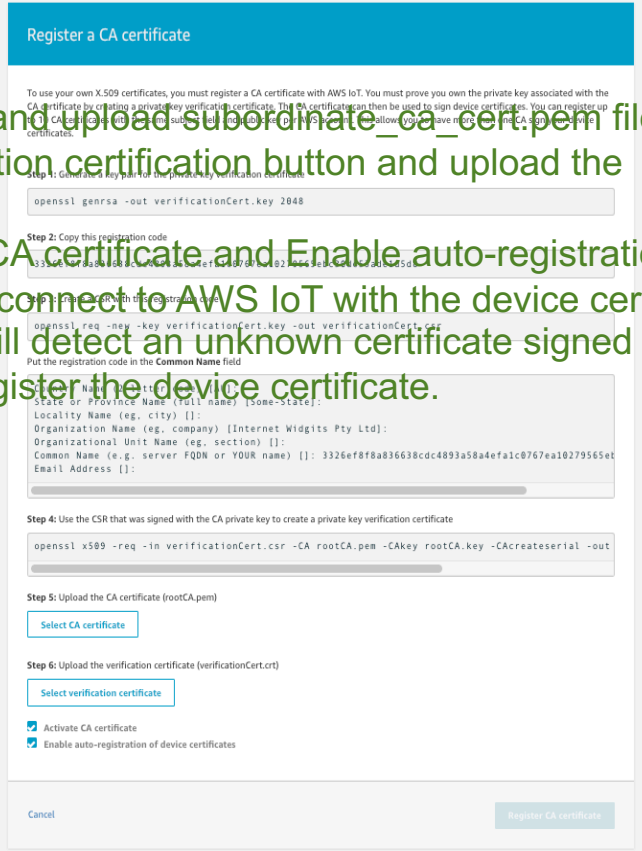
If you want to use your own device certificates, you'll need to register a CA certificate.

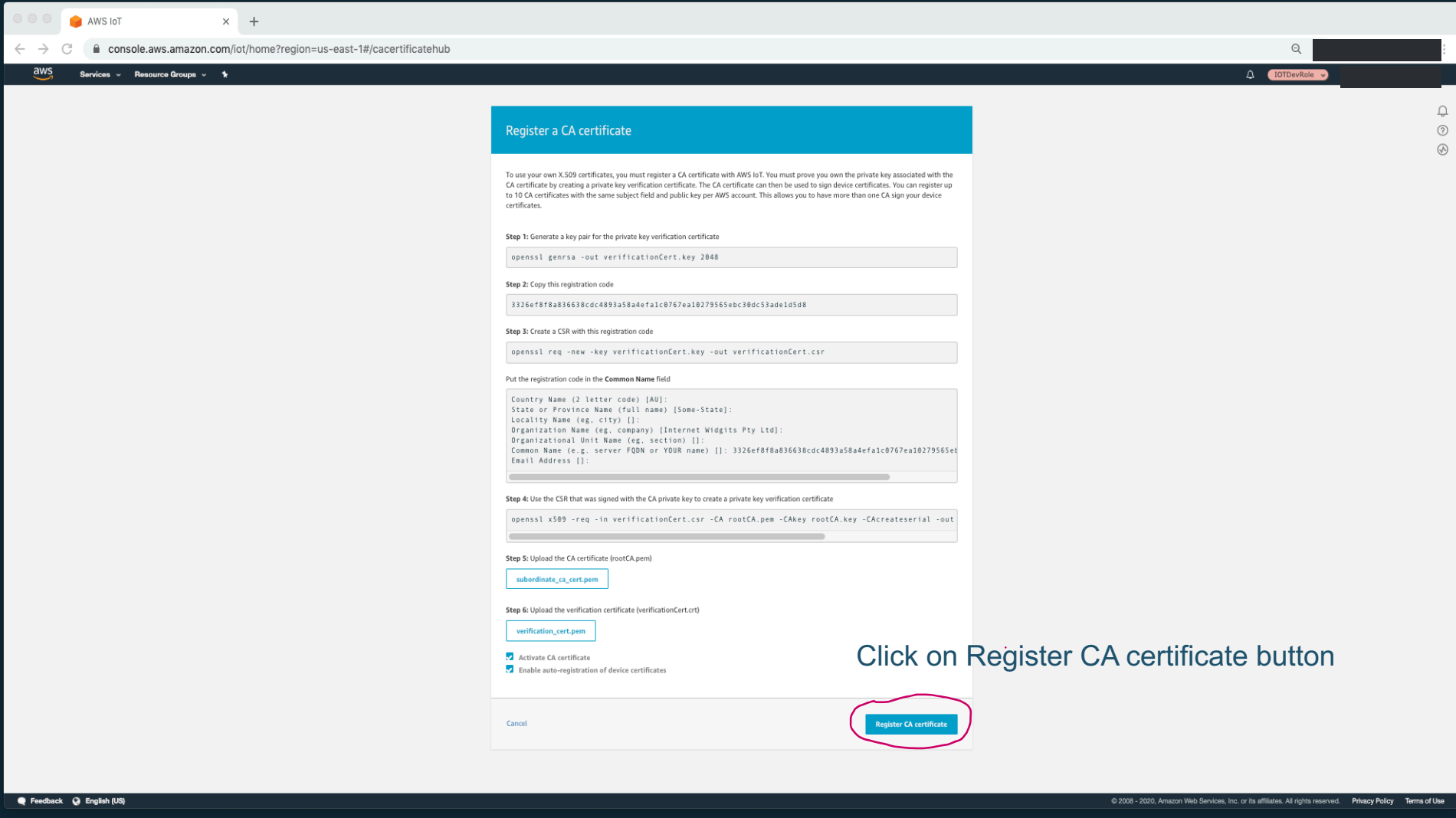
Learn more | Register a CA



Click on Register CA Button

- Skip directly to Step 5
- Click on Select CA certificate and upload subordinate_ca_cert.pem file
- In Step 6, Click Select verification certification button and upload the verification_cert.pem file
- Check the boxes for Activate CA certificate and Enable auto-registration of device certificates. When you connect to AWS IoT with the device certificate for the first time, the service will detect an unknown certificate signed by a registered CA and will auto-register the device certificate.




AWS IoT
console.aws.amazon.com/iot/home?region=us-east-1#/cacertificatehub
Services
Resource Groups
IOTDevRole
Register a CA certificate
To use your own X.509 certificates, you must register a CA certificate with AWS IoT. You must prove you own the private key associated with the CA certificate by creating a private key verification certificate. The CA certificate can then be used to sign device certificates. You can register up to 10 CA certificates with the same subject field and public key per AWS account. This allows you to have more than one CA sign your device certificates.
Step 1: Generate a key pair for the private key verification certificate
openssl genrsa -out verificationCert.key 2048
Step 2: Copy this registration code
3326ef8f8a836638cdc4893a58a4efa1c0767ea10279565ebc30dc53ade1d5d8
Step 3: Create a CSR with this registration code
openssl req -new -key verificationCert.key -out verificationCert.csr
Put the registration code in the Common Name field
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []: 3326ef8f8a836638cdc4893a58a4efa1c0767ea10279565eb
Email Address []:
Step 4: Use the CSR that was signed with the CA private key to create a private key verification certificate
openssl x509 -req -in verificationCert.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out
Step 5: Upload the CA certificate (rootCA.pem)
subordinate_ca_cert.pem
Step 6: Upload the verification certificate (verificationCert.crt)
verification_cert.pem
Activate CA certificate
Enable auto-registration of device certificates
Cancel
Register CA certificate
Click on Register CA certificate button
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use