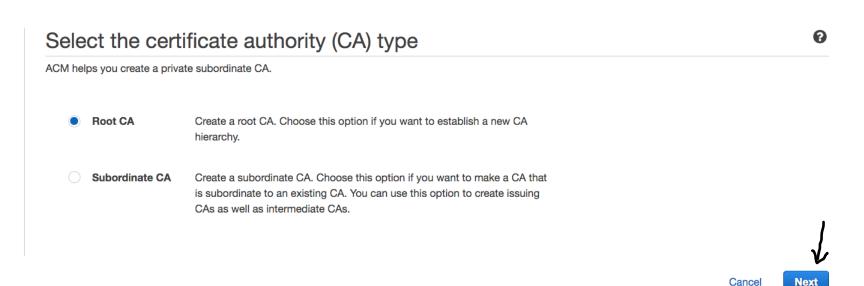
### Step 1: Select CA type

- Step 2: Configure CA subject name
- Step 3: Configure CA key algorithm
- Step 4: Configure revocation
- Step 5: Add tags
- Step 6: Configure CA permissions
- Step 7: Review



Step 1 : Creating a Root CA



### UICALC UM

Step 1: Select CA type

### Step 2: Configure CA subject name

Step 3: Configure CA key algorithm

Step 4: Configure revocation

Step 5: Add tags

Step 6: Configure CA permissions

Step 7: Review

# Configure the certificate authority (CA) name

Subject distinguished name Value

0

Name your CA using the distinguished name (DN) format. The name is used as the subject in the CA certificate and as the issuer in certificates that the CA issues. These names cannot be changed later.

# Organization (O)\* mycompany Company name. Max length of 64 characters. Organization Unit (OU)\* Company subdivision. Max length of 64 characters. Country name (C)\* United States (US) Two letter country code State or province name\* washington Full name. Max length of 128 characters Locality name\* City. Max length of 128 characters. Common Name (CN)\* acmpcaroot g1 Certificate authority name. Max length of 64 characters.

**Step 2 : Configure the Root CA parameters** 

\*At least one subject name is required



Cancel

Previous



Step 1: Select CA type

Step 2: Configure CA subject name

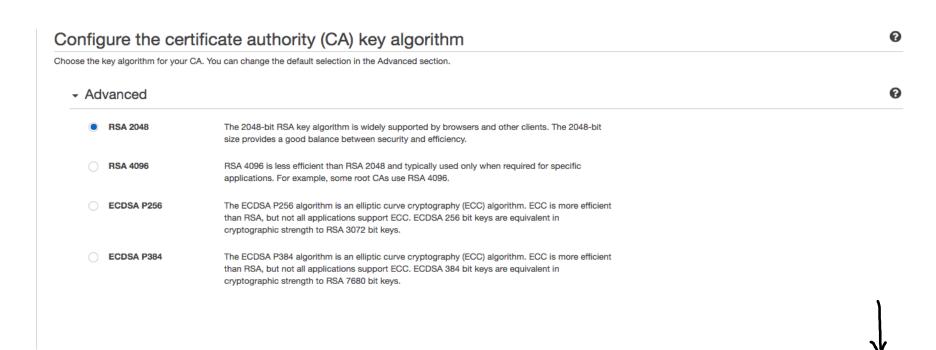
Step 3: Configure CA key algorithm

Step 4: Configure revocation

Step 5: Add tags

Step 6: Configure CA permissions

Step 7: Review



Cancel

Previous

Step 3 : Select RSA 2048 as the CA key algorithm

Step 1: Select CA type

Step 2: Configure CA subject name

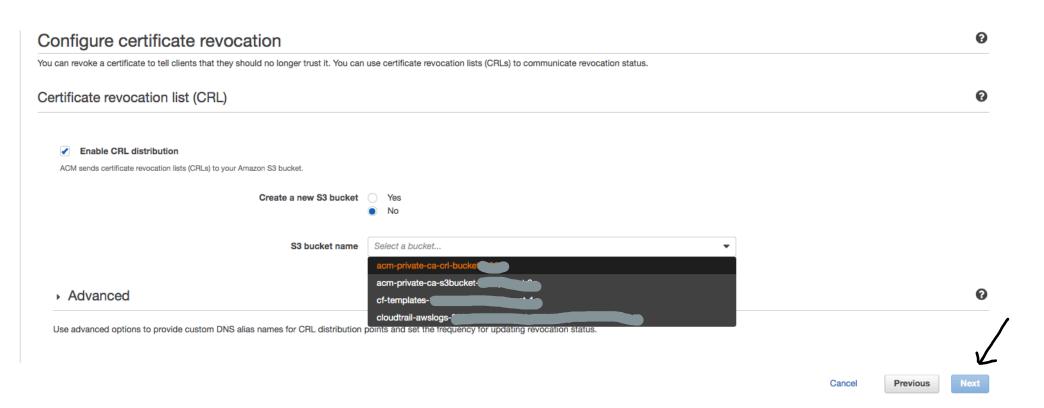
Step 3: Configure CA key algorithm

Step 4: Configure revocation

Step 5: Add tags

Step 6: Configure CA permissions

Step 7: Review



# Step 4:

- Enable Certificate Revocation List (CRL) Distribution
- Select the existing S3 buckets whose name starts with the prefix acm-private-ca-crl



Step 2: Configure CA subject name

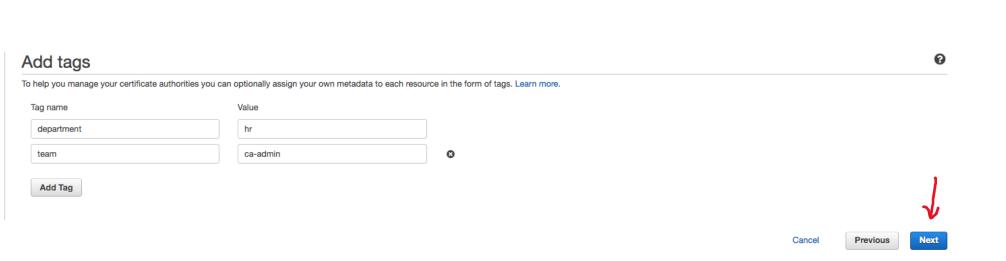
Step 3: Configure CA key algorithm

Step 4: Configure revocation

### Step 5: Add tags

Step 6: Configure CA permissions

Step 7: Review



Step 5 : Set the tags

0

## Create CA

Step 1: Select CA type

Step 2: Configure CA subject name

Step 3: Configure CA key algorithm

Step 4: Configure revocation

Step 5: Add tags

Step 6: Configure CA permissions

Step 7: Review

# Step 6: Configure CA permissions

Authorize ACM permission to renew private subscriber certificates issued within this account from this CA. Learn more.

ACM access to renew certificates requested by this account.

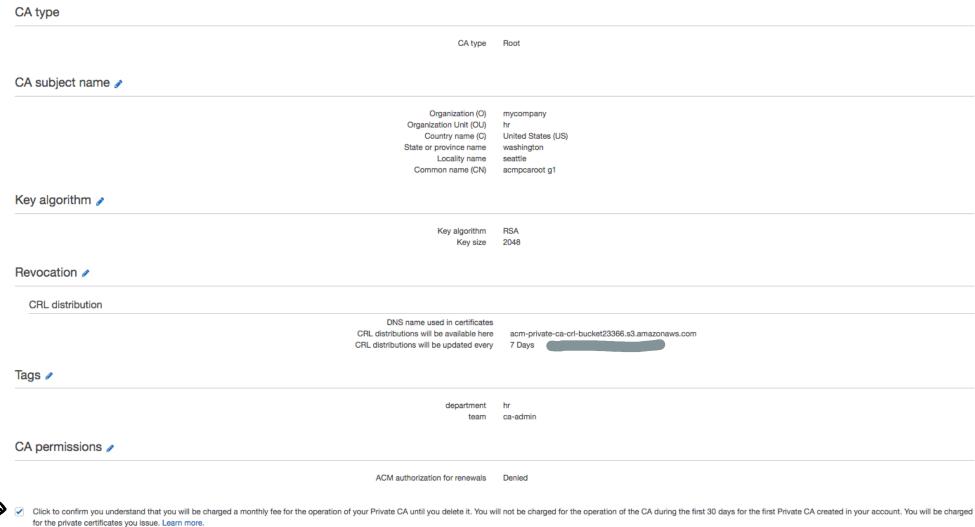


You may alter permissions for automated renewal for this CA at any time. The change will take effect for all future renewal cycles for ACM certificates generated within this account for this CA.

Cancel Previous Next

Step 6: We are not issuing end entity certs from the root CA, so Deny ACM permission for renewals

Step 4: Configure revocation Step 5: Add tags Step 6: Configure CA permissions Step 7: Review



You must select the check box to continue.



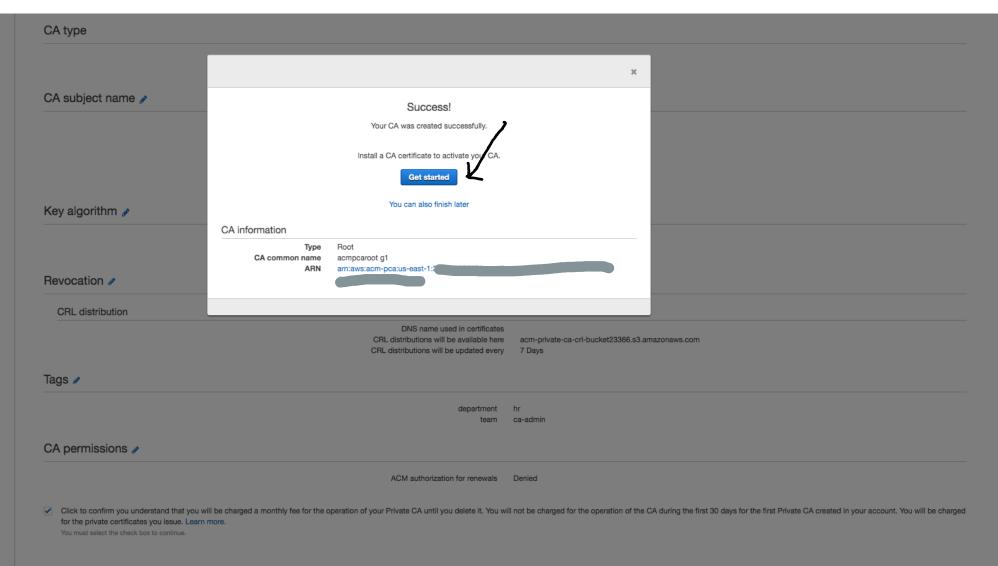
Step 7: Confirm and create the Root CA

Cancel

Step 4: Configure revocation Step 5: Add tags

Step 6: Configure CA permissions

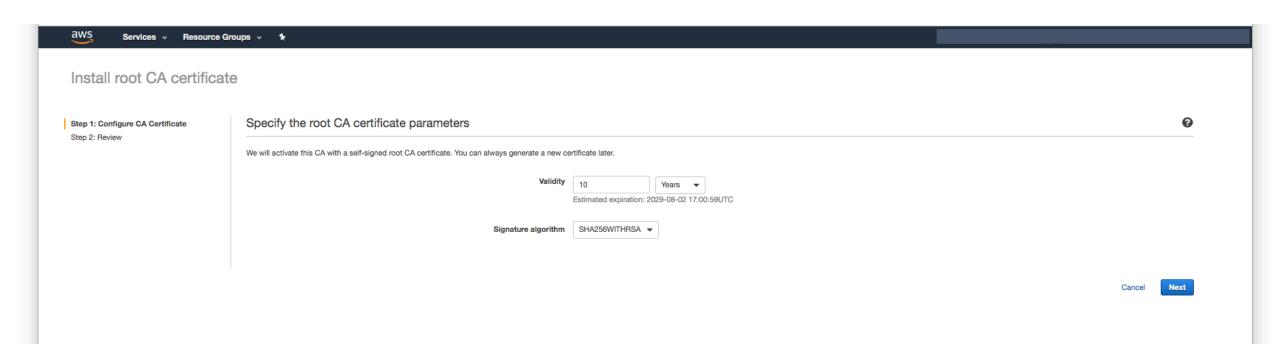
Step 7: Review



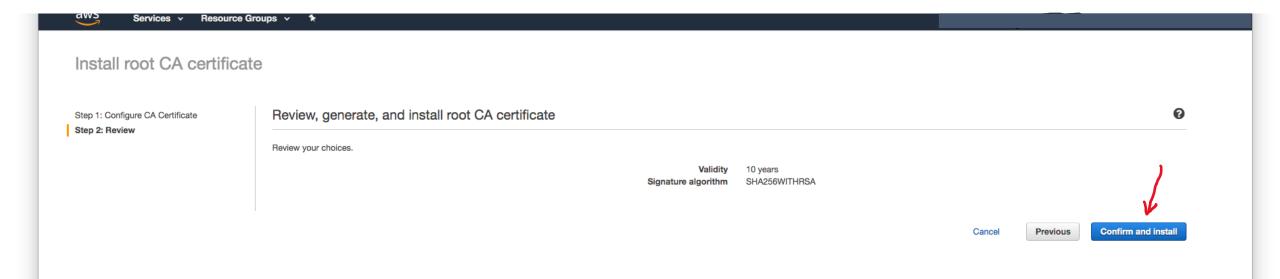
Step 8: Sign the root ca csr with the root ca's private key

cel Previous

Confirm and create



Step 9 : Set the validity period and signature algorithm for the Root CA certificate



**Step 10 : Confirm and install to create the root CA certificate** 



