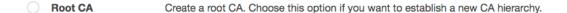
Step 1: Select CA type

- 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

Select the certificate authority (CA) type

ACM helps you create a private subordinate CA.



Subordinate CA Create a subordinate CA. Choose this option if you want to make a CA that is

subordinate to an existing CA. You can use this option to create issuing CAs as well

as intermediate CAs.



Step 1: Creating a subordinate issuing CA

 \triangle

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

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.

Certificate authority name. Max length of 64 characters.

Organization (O)* mycompany Company name. Max length of 64 characters. Organization Unit (OU)* payroll 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* seattle City. Max length of 128 characters. Common Name (CN)* acmsubordinateca g1

Step 2 : Fill in the subordinate CA parameters

*At least one subject name is required



Cancel

Previous

Next



Create CA

Step 1: Select CA type

Step 2: Configure CA subject name

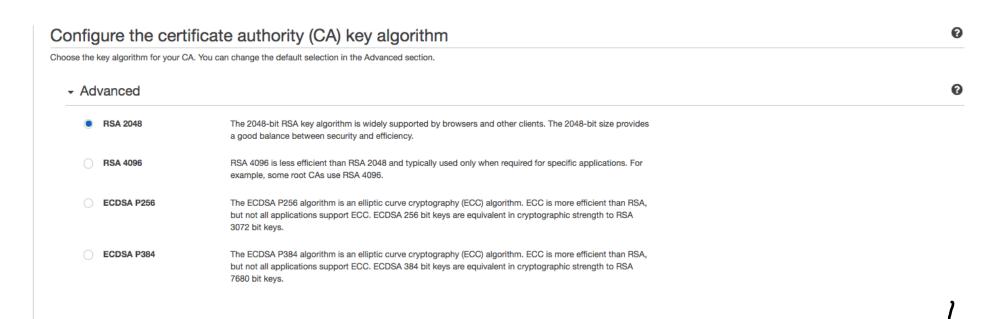
Step 3: Configure CA key algorithm

Step 4: Configure revocation

Step 5: Add tags

Step 6: Configure CA permissions

Step 7: Review



Step 3: Choose the CA key algorithm



Cancel

Previous



Create CA

Step 1: Select CA type

Step 2: Configure CA subject name

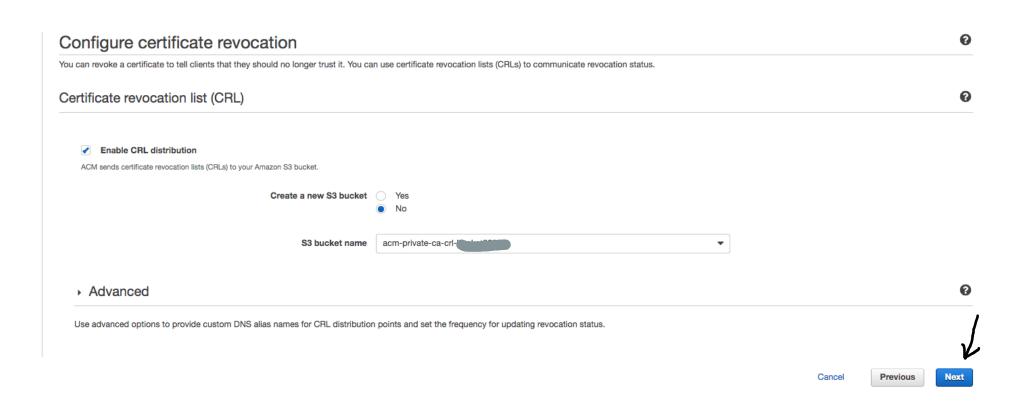
Step 3: Configure CA key algorithm

Step 4: Configure revocation

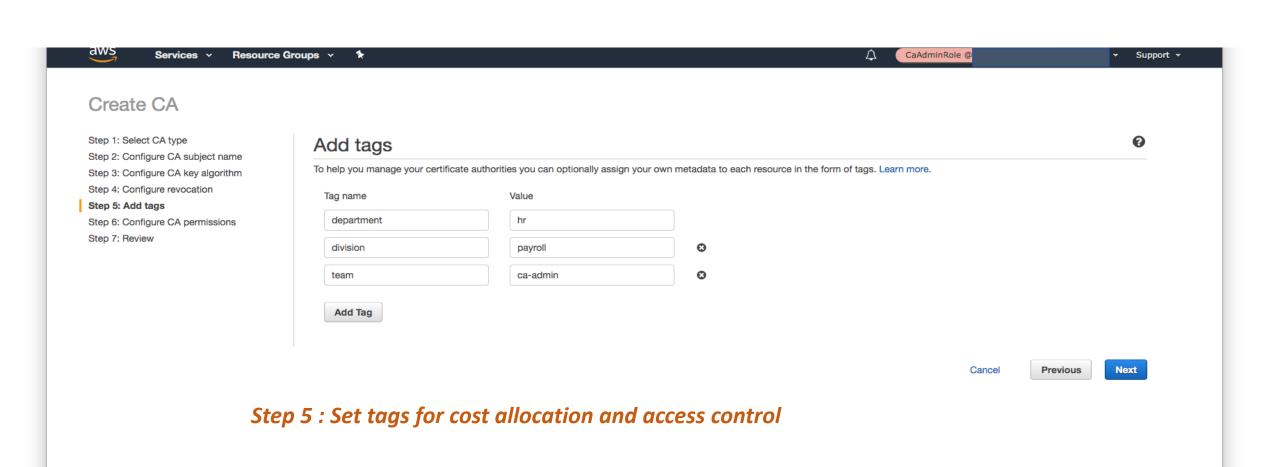
Step 5: Add tags

Step 6: Configure CA permissions

Step 7: Review



Step 4: Enable CRL distribution .Select the preexisting bucket with prefix acm-private-ca-crl



Cancel

Previous

Next

Create CA

Step 1: Select CA type

Step 2: Configure CA subject name

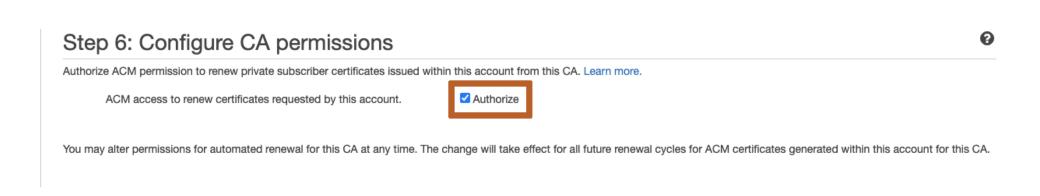
Step 3: Configure CA key algorithm

Step 4: Configure revocation

Step 5: Add tags

Step 6: Configure CA permissions

Step 7: Review



Step 6 : Let's authorize the subordinate CA to manage renewals for any private certs that are signed by this subordinate CA

Review your choices. Learn more. Step 3: Configure CA key algorithm CA type Step 6: Configure CA permissions CA type Subordinate CA subject name 🧪 Organization (O) mycompany Organization Unit (OU) payroll Country name (C) United States (US) State or province name washington Locality name seattle Common name (CN) acmsubordinateca g1 Key algorithm 🧪 Key algorithm RSA Key size 2048 Revocation / CRL distribution DNS name used in certificates CRL distributions will be available here acm-private-ca-cri-CRL distributions will be updated every 7 Days Tags 🧪 department hr division payroll team ca-admin CA permissions / ACM authorization for renewals Granted Click to confirm you understand that you will be charged a monthly fee for the operation of your Private CA until you delete it. You will not be charged for the operation of the CA during the first 30 days for the first Private CA created in your account. You will be charged for the private certificates you issue. Learn more. You must select the check box to continue. Step 7: Confirm that all the information is correct and click confirm and create

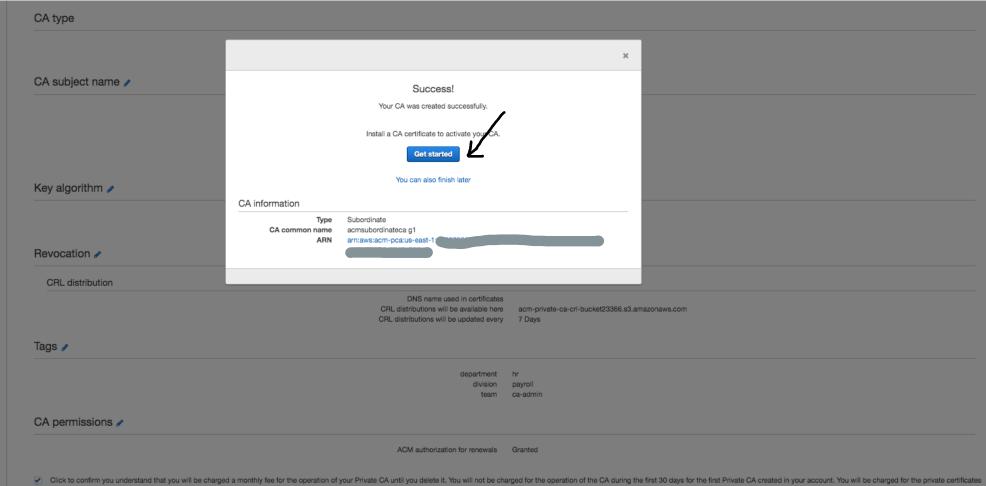
Confirm and create

Step 4: Configure revocation

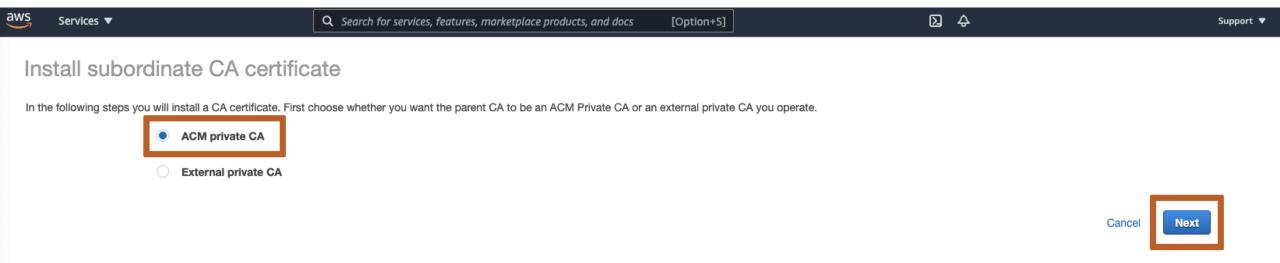
Step 5: Add tags

Step 7: Review

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



Step 8: The subordinate needs to be signed by the root CA that we created earlier. Click Get started Previous Confirm and create



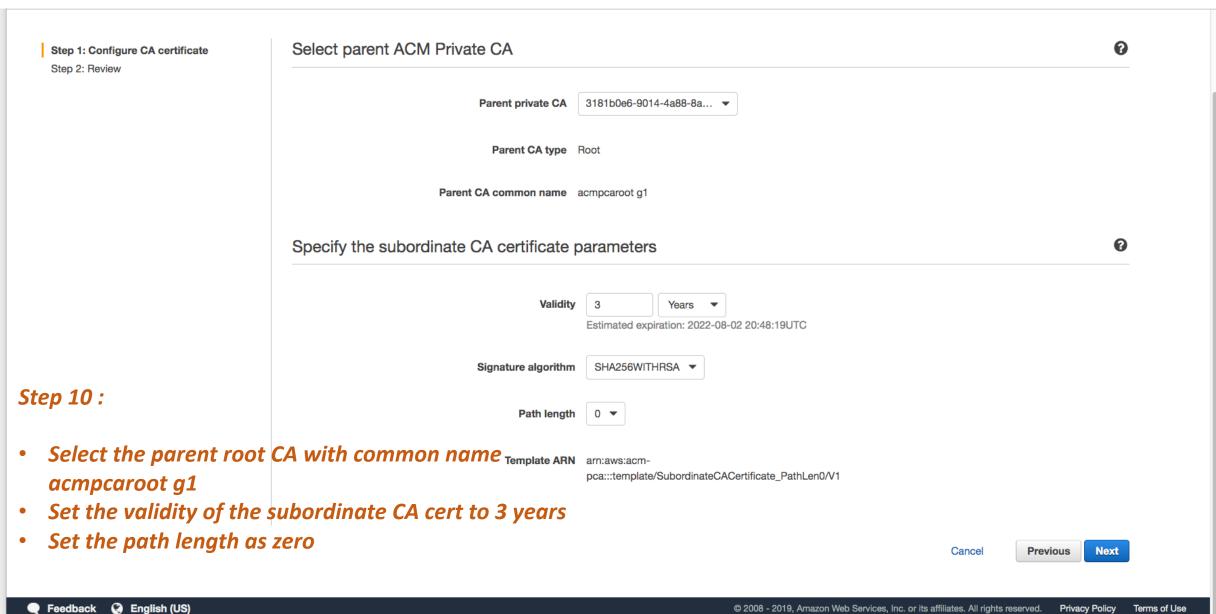
Step 9 : Signing the subordinate CA cert with the root CA that was created earlier

Quiz: (please open quiz in a new browser tab)

In Step 9 you selected ACM Private CA instead of External private CA. Click on the link below for the quiz

https://bit.ly/2KqPgcm



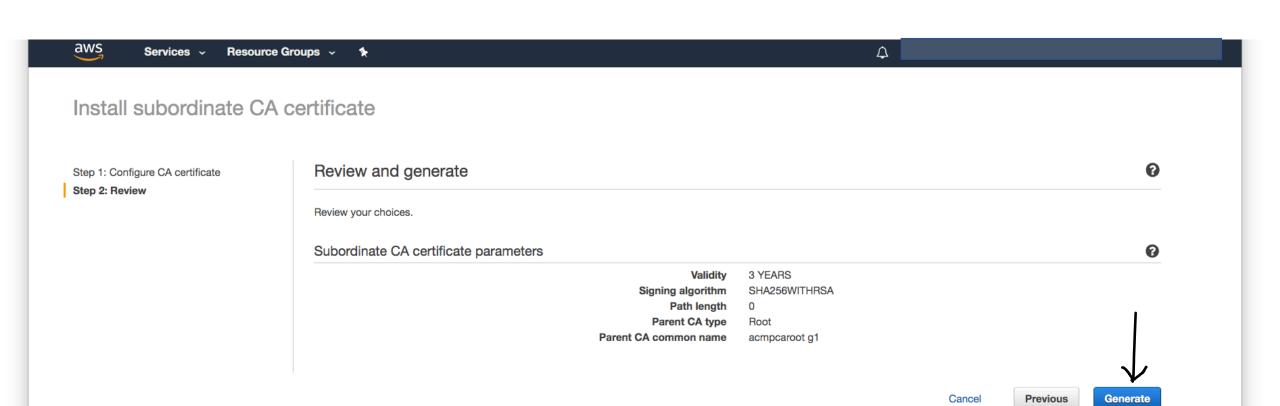


Quiz: (please open quiz in a new browser tab)

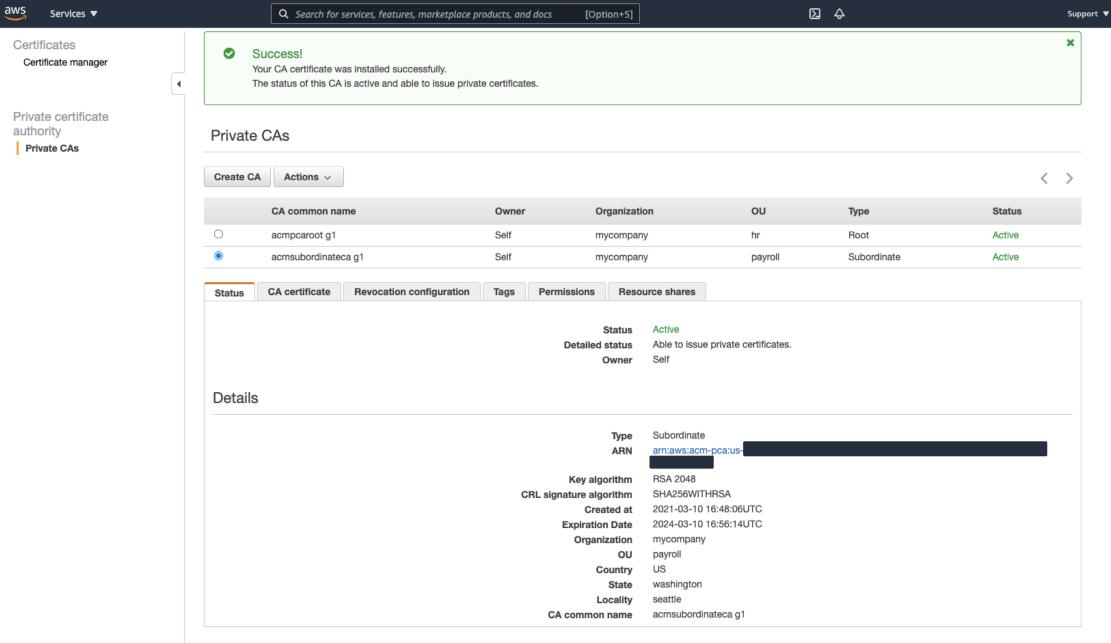
In Step 10 you set the path length as zero. Click on the link below for the quiz

https://bit.ly/2YWdJOW





Step 11 : Review and click Generate



You should see the subordinate CA with common name "acmsubordinateca g1" with status set to "Active"