

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

Select the certificate authority (CA) type ?

ACM helps you create a private subordinate CA.

☐**Root CA**

Create a root CA. Choose this option if you want to establish a new CA hierarchy.

☒**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.

[Cancel](#)[Next](#)

Step 1 : Creating a subordinate issuing CA

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



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.

Subject distinguished name	Value
Organization (O)*	<input type="text" value="mycompany"/> <small>Company name. Max length of 64 characters.</small>
Organization Unit (OU)*	<input type="text" value="payroll"/> <small>Company subdivision. Max length of 64 characters.</small>
Country name (C)*	<input type="text" value="United States (US)"/> <small>Two letter country code</small>
State or province name*	<input type="text" value="washington"/> <small>Full name. Max length of 128 characters</small>
Locality name*	<input type="text" value="seattle"/> <small>City. Max length of 128 characters.</small>
Common Name (CN)*	<input type="text" value="acmsubordinateca g1"/> <small>Certificate authority name. Max length of 64 characters.</small>

Step 2 : Fill in the subordinate CA parameters

*At least one subject name is required



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) key algorithm ?

Choose the key algorithm for your CA. You can change the default selection in the Advanced section.

▼ Advanced ?

- ☒ **RSA 2048**

The 2048-bit RSA key algorithm is widely supported by browsers and other clients. The 2048-bit size provides a good balance between security and efficiency.
- ☐ **RSA 4096**

RSA 4096 is less efficient than RSA 2048 and typically used only when required for specific applications. For example, some root CAs use RSA 4096.
- ☐ **ECDSA P256**

The ECDSA P256 algorithm is an elliptic curve cryptography (ECC) algorithm. ECC is more efficient than RSA, but not all applications support ECC. ECDSA 256 bit keys are equivalent in cryptographic strength to RSA 3072 bit keys.
- ☐ **ECDSA P384**

The ECDSA P384 algorithm is an elliptic curve cryptography (ECC) algorithm. ECC is more efficient than RSA, but not all applications support ECC. ECDSA 384 bit keys are equivalent in cryptographic strength to RSA 7680 bit keys.

[Cancel](#)

[Previous](#)

[Next](#)

Step 3 : Choose the CA key algorithm

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 certificate revocation ?

You can revoke a certificate to tell clients that they should no longer trust it. You can use certificate revocation lists (CRLs) to communicate revocation status.

Certificate revocation list (CRL) ?

☒ **Enable CRL distribution**

ACM sends certificate revocation lists (CRLs) to your Amazon S3 bucket.

Create a new S3 bucket ☐ Yes
☒ No

S3 bucket name

acm-private-ca-crl-

Advanced ?

Use advanced options to provide custom DNS alias names for CRL distribution points and set the frequency for updating revocation status.

Cancel

Previous

Next



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

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

Add tags ?

To help you manage your certificate authorities you can optionally assign your own metadata to each resource in the form of tags. [Learn more.](#)

Tag name	Value	
<input type="text" value="department"/>	<input type="text" value="hr"/>	
<input type="text" value="division"/>	<input type="text" value="payroll"/>	✕
<input type="text" value="team"/>	<input type="text" value="ca-admin"/>	✕
<input type="button" value="Add Tag"/>		

[Cancel](#)

[Previous](#)

[Next](#)

Step 5 : Set tags for cost allocation and access control

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.

☒ Authorize

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

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

Review your choices. [Learn more.](#)

CA type

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-crl- 
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

[Cancel](#)

[Previous](#)

[Confirm and create](#)



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

CA type

CA subject name

Key algorithm

Revocation

CRL distribution

Tags

CA permissions

Success!

Your CA was created successfully.

Install a CA certificate to activate your CA.

Get started

You can also finish later

CA information

Type	Subordinate
CA common name	acmsubordinateca.g1
ARN	arn:aws:acm-pca:us-east-1:123456789012:certificate/ca-123456789012

DNS name used in certificates
CRL distributions will be available here
CRL distributions will be updated every

acm-private-ca-crl-bucket23366.s3.amazonaws.com
7 Days

department hr
division payroll
team ca-admin

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

Cancel

Previous

Confirm and create

Install subordinate CA certificate

In the following steps you will install a CA certificate. First choose whether you want the parent CA to be an ACM Private CA or an external private CA you operate.

☒ ACM private CA

☐ External private CA

Cancel

Next

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>



Step 1: Configure CA certificate

Step 2: Review

Select parent ACM Private CA



Parent private CA 3181b0e6-9014-4a88-8a... ▼

Parent CA type Root

Parent CA common name acmpcaroot g1

Specify the subordinate CA certificate parameters



Validity 3 Years ▼

Estimated expiration: 2022-08-02 20:48:19UTC

Signature algorithm SHA256WITHRSA ▼

Path length 0 ▼

Template ARN arn:aws:acm-pca:::template/SubordinateCACertificate_PathLen0/V1

Step 10 :

- **Select the parent root CA with common name `acmpcaroot g1`**
- **Set the validity of the subordinate CA cert to 3 years**
- **Set the path length as zero**

Cancel

Previous

Next

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>



Install subordinate CA certificate

Step 1: Configure CA certificate

Step 2: Review

Review and generate ?

Review your choices.

Subordinate CA certificate parameters ?

Validity	3 YEARS
Signing algorithm	SHA256WITHRSA
Path length	0
Parent CA type	Root
Parent CA common name	acmpcaroot g1

Cancel

Previous

Generate



Step 11 : Review and click Generate

✓

Success!

Your CA certificate was installed successfully.

The status of this CA is active and able to issue private certificates.

Private CAs

Create CAActions

	CA common name	Owner	Organization	OU	Type	Status
<input type="radio"/>	acmpcaroot g1	Self	mycompany	hr	Root	Active
<input checked="" type="radio"/>	acmsubordinateca g1	Self	mycompany	payroll	Subordinate	Active

StatusCA certificateRevocation configurationTagsPermissionsResource shares

StatusActive

Detailed statusAble to issue private certificates.

OwnerSelf

Details

TypeSubordinate

ARNarn:aws:acm-pca:us-[redacted]

Key algorithmRSA 2048

CRL signature algorithmSHA256WITHRSA

Created at2021-03-10 16:48:06UTC

Expiration Date2024-03-10 16:56:14UTC

Organizationmycompany

OUpayroll

CountryUS

Statewashington

Localityseattle

CA common nameacmsubordinateca g1

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