

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

*At least one subject name is required

Step 2 : Configure the Root CA parameters

Cancel

Previous

Next





Services ▾

Resource Groups ▾



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 ?

- | | |
|--|---|
| <input checked="" type="radio"/> 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. |
| <input type="radio"/> 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. |
| <input type="radio"/> 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. |
| <input type="radio"/> 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 : Select RSA 2048 as 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

Select a bucket...

acm-private-ca-crl-bucket-...

acm-private-ca-s3bucket-...

cf-templates-...

cloudtrail-awslogs-...

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 Certificate Revocation List (CRL) Distribution**
- **Select the existing S3 buckets whose name starts with the 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



Add Tag

Cancel

Previous

Next



Step 5 : Set the tags

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

In the previous step you tagged this certificate authority with the key value pair “team”:”ca-admin”. Click on the link below for the quiz :

<https://bit.ly/2To8mmf>



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: 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

CA type

CA type Root

CA subject name

Organization (O) mycompany
Organization Unit (OU) hr
Country name (C) United States (US)
State or province name washington
Locality name seattle
Common name (CN) acmpcaroot 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-bucket23366.s3.amazonaws.com
CRL distributions will be updated every 7 Days

Tags

department hr
team ca-admin

CA permissions

ACM authorization for renewals Denied

☒ 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 and create the Root CA

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	Root
CA common name	acmpcaroot g1
ARN	arn:aws:acm-pca:us-east-1:...

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
team

hr
ca-admin

ACM authorization for renewals
Denied

☒ 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 : Sign the root ca csr with the root ca's private key

Cancel Previous [Confirm and create](#)

Install root CA certificate

Step 1: Configure CA Certificate

Step 2: Review

Specify the root CA certificate parameters ?

We will activate this CA with a self-signed root CA certificate. You can always generate a new certificate later.

Validity

Years ▾

Estimated expiration: 2029-08-02 17:00:59UTC

Signature algorithm

 ▾[Cancel](#)[Next](#)

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

[Services](#) ▾[Resource Groups](#) ▾

Install root CA certificate

[Step 1: Configure CA Certificate](#)**Step 2: Review**

Review, generate, and install root CA certificate ?

Review your choices.

Validity	10 years
Signature algorithm	SHA256WITHRSA

[Cancel](#)[Previous](#)[Confirm and install](#)

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

Certificates

Certificate manager

Private certificate authority

Private CAs



Success!

Your root CA certificate was installed successfully.

The STATUS of this CA is ACTIVE and able to issue private certificates.



Private CAs

Create CA

Actions ▾



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

Status

CA certificate

Revocation configuration

Tags

Permissions

Resource shares

Status

Active

Detailed status

Able to issue private certificates.

Owner

Self

Details

Type

Root

ARN

[arn:aws:acm-pca:us](#)

Key algorithm

RSA 2048

CRL signature algorithm

SHA256WITHRSA

Created at

2021-03-10 16:18:06UTC

Expiration Date

2031-03-10 16:18:57UTC

Organization

mycompany

OU

hr

Country

US

State

washington

Locality

seattle

CA common name

acmpcaroot g1

Step 11 : You should see the root CA created with active status

Quiz : (Please open quiz in a new browse tab)

In Step 10 you clicked Confirm to install the root CA certificate. The Root CA private key is used to sign the CSR and create the root CA certificate. Click on the link below to take the quiz

<https://bit.ly/2YQr7EI>

