


# Requesting an SSL/TLS certificate by using DNS validation

## Step 1: Request a certificate

To get started, sign in to the [AWS Management Console](#) and navigate to the [ACM console](#). Choose Get started to request a certificate.




### AWS Certificate Manager

AWS Certificate Manager (ACM) makes it easy to provision, manage, deploy, and renew SSL/TLS certificates on the AWS platform.

[Get started](#)


[User guide](#)



#### Provision certificates

Provide the name of your site, establish your identity, and let ACM do the rest. ACM manages renewal of SSL/TLS certificates issued by Amazon for you.


[Learn more](#)



#### Deploy SSL/TLS-based sites and applications

Create an Elastic Load Balancer or Amazon CloudFront distribution and use ACM-provided or imported certificates with SSL/TLS to securely identify your site.

[Learn more](#)

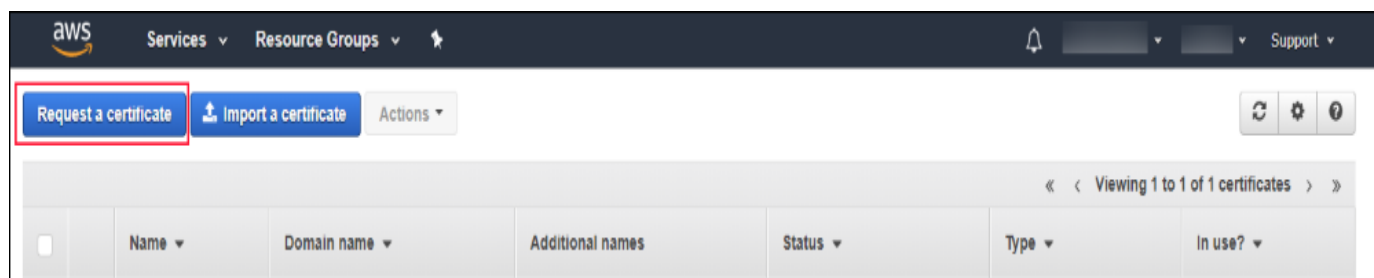


#### Manage certificates

See all of your ACM-provided and imported certificates in one place in the AWS Management Console. Automate management tasks by using the ACM API, SDK, or CLI.

[Learn more](#)

If you previously managed certificates in ACM, you will instead see a table with your certificates and a button to request a new certificate. Choose Request a certificate to request a new certificate.



Type the name of your domain in the Domain name box and choose Next. In this example, I type `www.example.com`. You must use a domain name that you control. Requesting certificates for domains that you don't control violates the [AWS Service Terms](#).

The screenshot shows the 'Request a certificate' wizard in the AWS Certificate Manager console. The wizard has four steps: Step 1: Add domain names (selected), Step 2: Select validation method, Step 3: Review, and Step 4: Validation. In Step 1, there's a light blue box with the text 'You can use AWS Certificate Manager certificates with other AWS Services.' Below this is the 'Add domain names' section. It contains a text input field with 'www.example.com' (highlighted with a red box) and a 'Remove' button. Below the input field is a blue button labeled 'Add another name to this certificate'. At the bottom of the wizard, there's a note: '\*At least one domain name is required'. To the right of this note are two buttons: 'Cancel' and 'Next' (highlighted with a red box).

## Step 2: Select a validation method

With DNS validation, you write a CNAME record to your DNS configuration to establish control of your domain name. Choose DNS validation, and then choose Review.





# Request a certificate

Step 1: Add domain names

Step 2: Select validation method

Step 3: Review

Step 4: Validation

Request in progress

A certificate request with a status of Pending validation has been created. Further action is needed to complete the validation and approval of the certificate.

## Validation

Create a CNAME record in the DNS configuration for each of the domains listed below. You must complete this step before AWS Certificate Manager (ACM) can issue your certificate, but you can skip this step for now by clicking **Continue**. To return to this step later, open the certificate request in the ACM Console.

Domain	Validation status
<div><div></div><div>www.steelcity.xyz</div></div>	Pending validation

Add the following CNAME record to the DNS configuration for your domain. The procedure for adding CNAME records depends on your DNS service Provider. [Learn more.](#)

Name	Type	Value
_ede669291a50b22db41fe58b625f521b.www.steelcity.xyz	CNAME	_0da758437f4b033c13ead76230a16ce1.acm-validations.aws

**Note:** Changing the DNS configuration allows ACM to issue certificates for this domain name for as long as the DNS record exists. You can revoke permission at any time by removing the record. [Learn more.](#)

Create record in Route 53

Amazon Route 53 DNS Customers ACM can update your DNS configuration for you. [Learn more.](#)

Export DNS configuration to a file

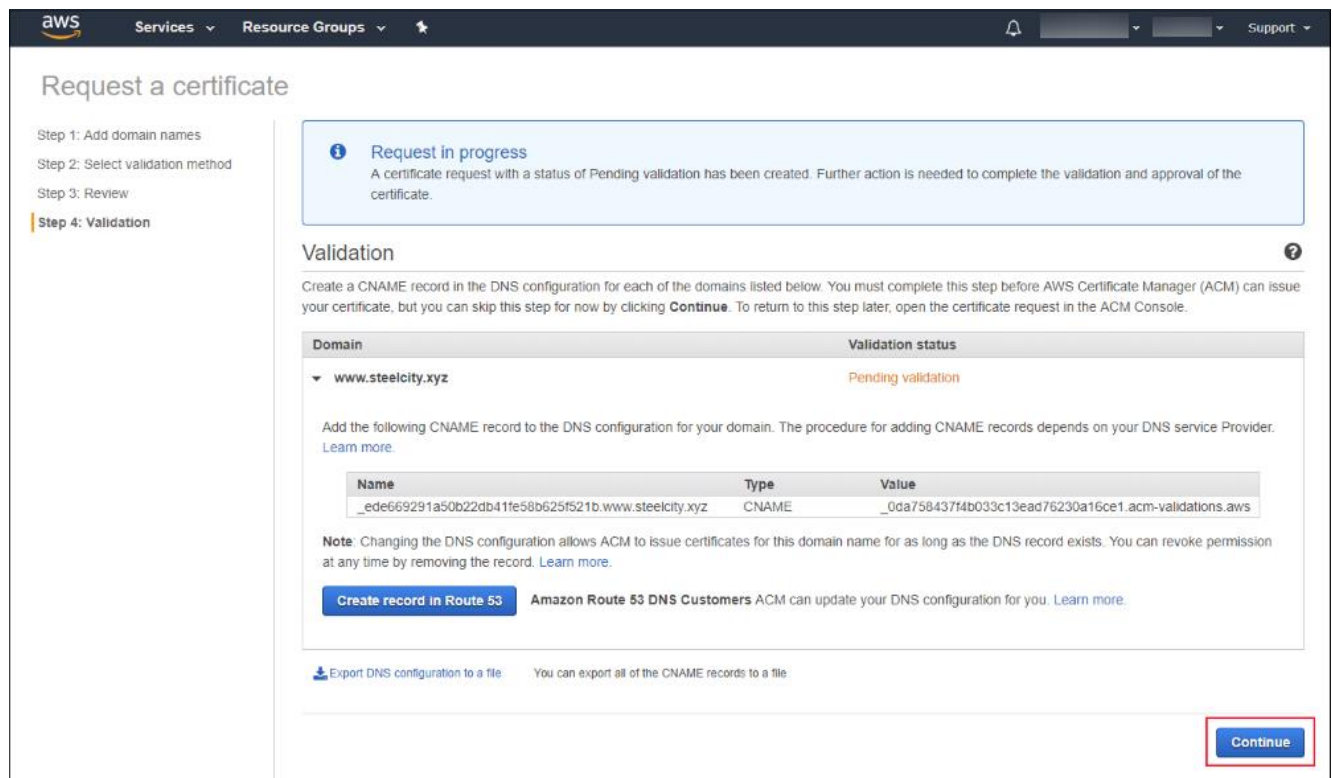
You can export all of the CNAME records to a file

Continue

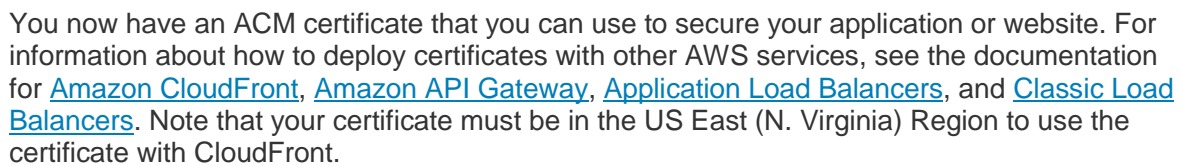
ACM displays the CNAME record you must add to your DNS configuration to validate that you control the domain name in your certificate request. If you use a DNS provider other than Route 53 or if you use a different AWS account to manage DNS records in Route 53, copy the DNS CNAME information from the validation information, or export it to a file (choose Export DNS configuration to a file) and write it to your DNS configuration. For information about how to add or modify DNS records, check with your DNS provider. For more information about using DNS with Route 53 DNS, see the [Route 53 documentation](#).

If you manage DNS records for your domain with Route 53 in the same AWS account, choose Create record in Route 53 to have ACM update your DNS configuration for you.

After updating your DNS configuration, choose Continue to return to the ACM table view.



ACM then displays a table that includes all your certificates. The certificate you requested is displayed so that you can see the status of your request. After you write the DNS record or have ACM write the record for you, it typically takes DNS 30 minutes to propagate the record, and it might take several hours for Amazon to validate it and issue the certificate. During this time, ACM shows the Validation status as Pending validation. After ACM validates the domain name, ACM updates the Validation status to Success. After the certificate is issued, the certificate status is updated to Issued. If ACM cannot validate your DNS record and issue the certificate after 72 hours, the request times out, and ACM displays a Timed out validation status. To recover, you must make a new request. Refer to the [Troubleshooting Section](#) of the [ACM User Guide](#) for instructions about troubleshooting validation or issuance failures.



You now have an ACM certificate that you can use to secure your application or website. For information about how to deploy certificates with other AWS services, see the documentation for [Amazon CloudFront](#), [Amazon API Gateway](#), [Application Load Balancers](#), and [Classic Load Balancers](#). Note that your certificate must be in the US East (N. Virginia) Region to use the certificate with CloudFront.