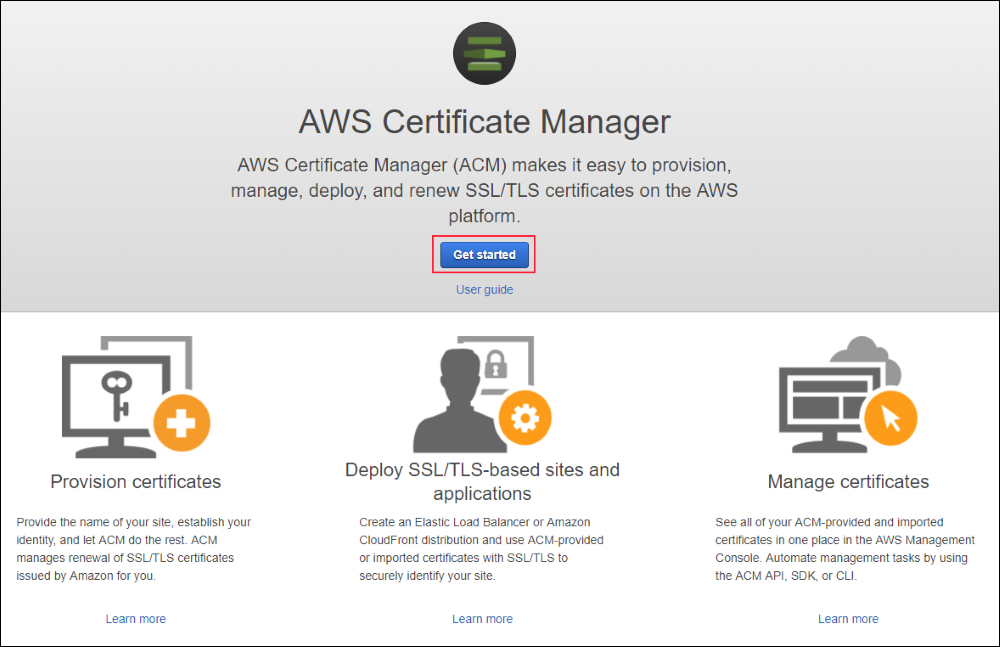
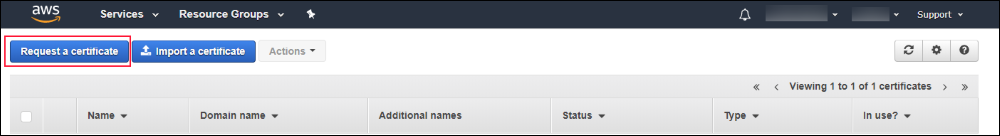
**Requesting an SSL/TLS certificate by using DNS validation**

**Step 1: Request a certificate**

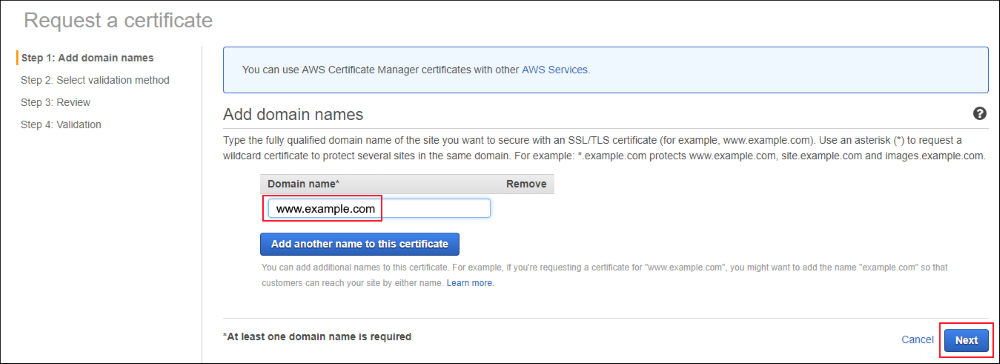
To get started, sign in to the [AWS Management Console](https://console.aws.amazon.com/console/home) and navigate to the [ACM console](https://console.aws.amazon.com/acm/home). Choose Get started to request a certificate.



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.

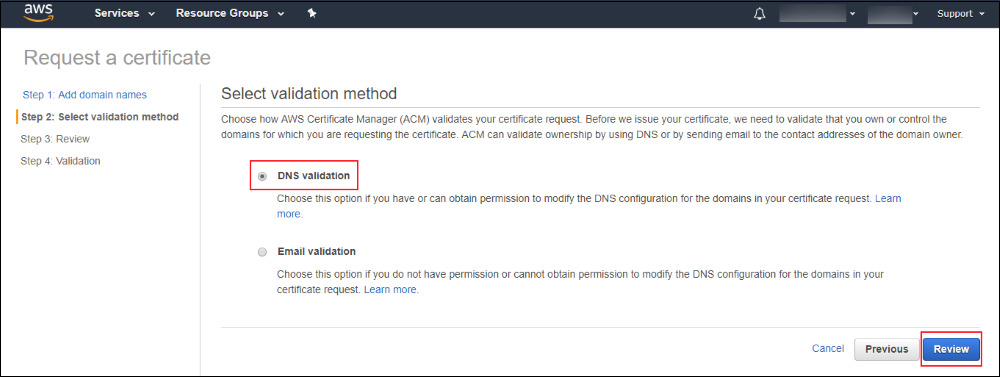


Type the name of your domain in the **Domain name** box and choose **Next**. In this example, I type www.example.com. You must use a domain name that you control. Requesting certificates for domains that you don’t control violates the [AWS Service Terms](https://aws.amazon.com/service-terms/).



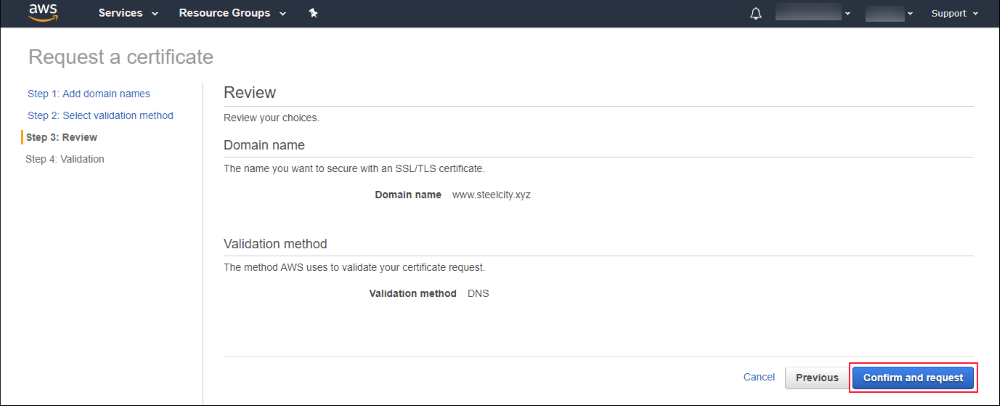
### Step 2: Select a validation method

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**.



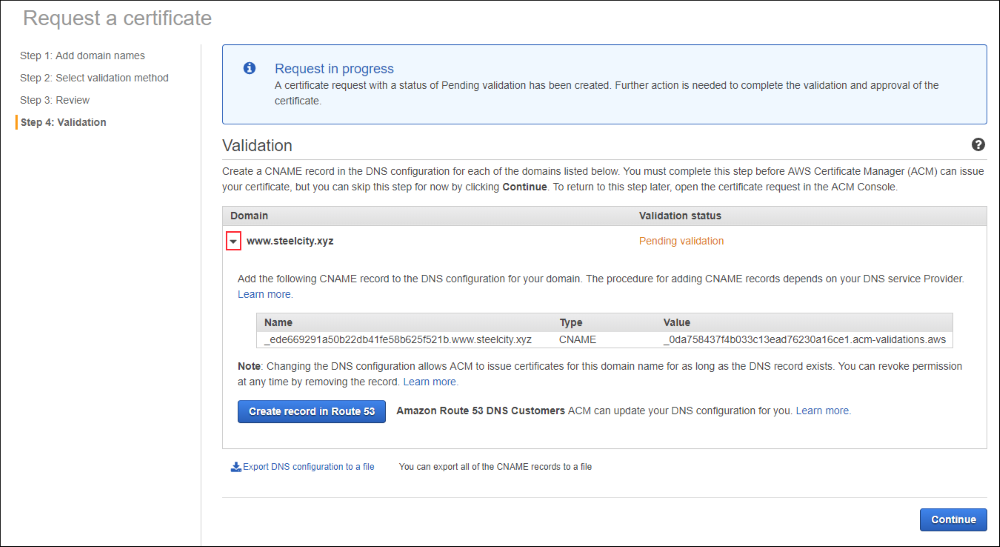
### Step 3: Review your request

Review your request and choose **Confirm and request** to request the certificate.



### Step 4: Submit your request

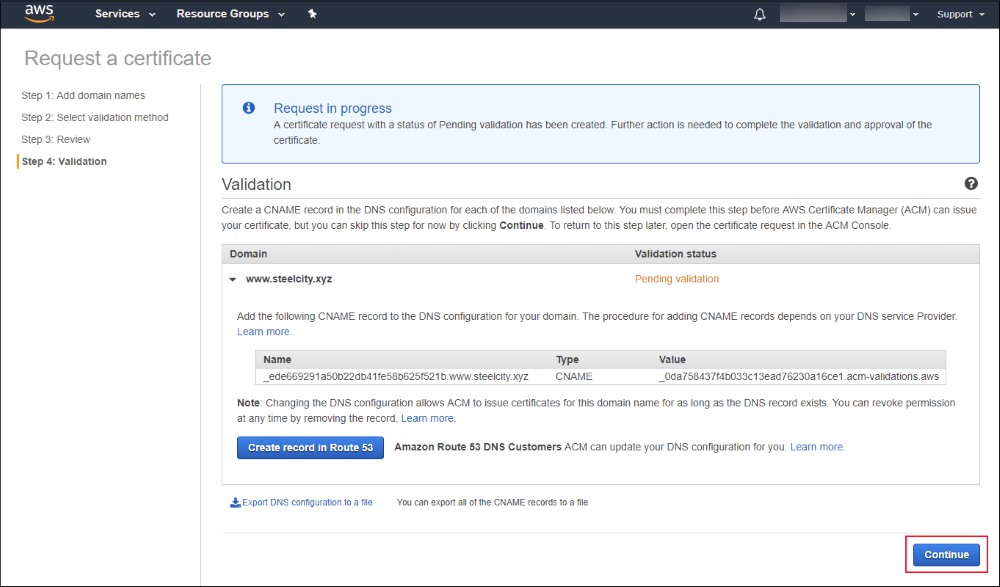
After a brief delay while ACM populates your domain validation information, choose the down arrow (highlighted in the following screenshot) to display all the validation information for your domain.



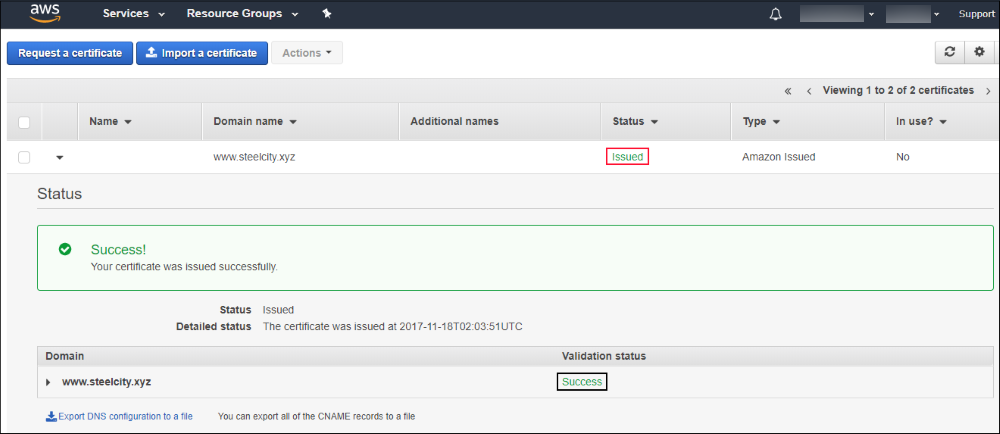
ACM displays the CNAME record you must add to your DNS configuration to validate that you control the domain name in your certificate request. If you use a DNS provider other than Route 53 or if you use a different AWS account to manage DNS records in Route 53, copy the DNS CNAME information from the 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](http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-creating.html).

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](http://docs.aws.amazon.com/acm/latest/userguide/troubleshooting.html) of the [ACM User Guide](http://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html) 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](http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https.html), [Amazon API Gateway](http://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-custom-domains.html), [Application Load Balancers](http://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html), and [Classic Load Balancers](http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/ssl-server-cert.html). Note that your certificate must be in the US East (N. Virginia) Region to use the certificate with CloudFront.