



# HTTPS: Create a TLS Certificate

We will walk you through the process of creating a TLS certificate in this lesson.

## We'll cover the following ^

- Objective
- Steps
- Creating the certificate

## Objective#

- Migrate our endpoint from HTTP to HTTPS.

## Steps#

- Manually create a TLS certificate.

As things stand, our application is responding to unencrypted HTTP traffic. In the real world, we want to protect any data as it traverses the network. To do that, we must encrypt our traffic and serve it over HTTPS.

We'll also take this as an opportunity to practice the two-phase change process discussed in Multi-phase deployments (<https://www.educative.io/courses/good-parts-of-aws/m2v7M6Bp0qr>) to give the chance to anyone using our HTTP endpoint to migrate to HTTPS before we turn off HTTP.



# Creating the certificate#

Requesting a certificate is an infrequent operation that requires human intervention for validation (or more automation than makes sense, for a process that happens only once). Therefore, we're going to create our certificate manually. To start, let's visit the AWS Certificate Manager (ACM) console (<https://console.aws.amazon.com/acm>) and hit *Request a certificate*. Then, let's select the public certificate option.

Choose **Import a certificate** to import an existing certificate instead of requesting a new one. [Learn more.](#)

**Import a certificate**

## Request a certificate

Choose the type of certificate for ACM to provide.

- ☒ **Request a public certificate** - Request a public certificate from Amazon. By default, public certificates are trusted by browsers and operating systems.
- ☐ **Request a private certificate** - No Private CAs available for issuance. [Learn more.](#)

[Cancel](#)

**Request a certificate**

Request a Certificate

Next, let's enter our bare domain (e.g., `the-good-parts.com`) as well as a wildcard version of the domain (e.g., `*.the-good-parts.com`). The wildcard will cover our prod and staging subdomains.



## Request a certificate

### Step 1: Add domain names

Step 2: Select validation method

Step 3: Add Tags

Step 4: Review

Step 5: Validation

AWS Certificate Manager logs domain names from your certificates into public certificate transparency (CT) logs when renewing certificates. You can opt out of CT logging. [Learn more](#)

You can use AWS Certificate Manager certificates with other [AWS Services](#).

### Add domain names



Type the fully qualified domain name of the site you want to secure with an SSL/TLS certificate (for example, `www.example.com`). Use an asterisk (\*) to request a wildcard certificate to protect several sites in the same domain. For example: `*.example.com` protects `www.example.com`, `site.example.com` and `images.example.com`.

Domain name\*

Remove

the-good-parts.com

\*.the-good-parts.com



Add another name to this certificate

You can add additional names to this certificate. For example, if you're requesting a certificate for `"www.example.com"`, you might want to add the name `"example.com"` so that customers can reach your site by either name. [Learn more](#).

### Add Domain Names

Now, we must validate that we control the domain.

## Request a certificate

Step 1: Add domain names

### Step 2: Select validation method

Step 3: Add Tags

Step 4: Review

Step 5: Validation

### Select validation method

Choose how AWS Certificate Manager (ACM) validates your certificate request. Before we issue your certificate, we need to validate that you own or control the domains for which you are requesting the certificate. ACM can validate ownership by using DNS or by sending email to the contact addresses of the domain owner.

#### ☒ DNS validation

Choose this option if you have or can obtain permission to modify the DNS configuration for the domains in your certificate request. [Learn more](#). [Learn more](#).

#### ☐ Email validation

Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for the domains in your certificate request. [Learn more](#). [Learn more](#).

Cancel

Previous

Next



## Select Validation Method

If you chose *DNS validation*, you will reach a *Validation* step that asks you to add a CNAME record to your DNS hosted zone. If you registered your domain through Route 53, you can simply click the *Create record in Route 53* button to complete the validation process. Otherwise, you have to add the requested record to your DNS hosting service.

Step 2: Select validation method

Step 3: Add Tags

Step 4: Review

**Step 5: 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

▼ the-good-parts.com

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
_84ef0baccdf6ba5741476954d30fbed5.the-good-parts.com.	CNAME	_1c9e37d93d92bff6646ace8c972cf2b7.mzlfexyx.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](#).

► \*.the-good-parts.com

Pending validation

## Create CNAME Records

It usually takes a few minutes for the certificate to be validated. Once it is validated, you should see your issued certificate in the ACM console.



« < Viewing certificates 1 to 1 > »

<input type="checkbox"/>	Name ▾	Domain name ▾	Additional names	Status ▾	Type ▾	In use? ▾	Renewal eligibility ▾
<input type="checkbox"/>	-	the-good-parts.com	*.the-good-parts.com	Issued	Amazon Issued	No	Ineligible

### Status

**Status** Issued

**Detailed status** The certificate was issued at 2019-12-19T18:16:33UTC

Domain	Validation status
▶ the-good-parts.com	Success
▶ *.the-good-parts.com	Success

[Export DNS configuration to a file](#) You can export all of the CNAME records to a file

### Details

<b>Type</b>	Amazon Issued	<b>Requested at</b>	2019-12-19T18:12:17UTC
<b>In use?</b>	No	<b>Issued at</b>	2019-12-19T18:16:33UTC
<b>Domain name</b>	the-good-parts.com	<b>Not before</b>	2019-12-19T00:00:00UTC
<b>Number of additional names</b>	1	<b>Not after</b>	2021-01-19T12:00:00UTC
<b>Additional names</b>	*.the-good-parts.com	<b>Public key info</b>	RSA 2048-bit
<b>Identifier</b>	ffa8cdd6-734a-47b2-822d-8cc398d5b6a7	<b>Signature algorithm</b>	SHA256WITHRSA
<b>Serial number</b>	0f:2b:1a:e4:9d:ef:a8:c6:d1:47:7c:be:30:97:32:1b	<b>ARN</b>	arn:aws:acm:us-east-1:154460179839:certificate/ffa8cdd6-734a-47b2-822d-8cc398d5b6a7
		<b>Validation state</b>	None

### Tags

[Edit](#)

Name

### Validated Certificate

You can also inspect the CNAME record that was added to your hosted zone in Route 53.

Dashboard

- Hosted zones
- Health checks
- Traffic flow
- Traffic policies
- Policy records
- Domains
- Registered domains
- Pending requests
- Resolver
- VPCs
- Inbound endpoints
- Outbound endpoints
- Rules

Back to Hosted Zones [Create Record Set](#) [Import Zone File](#) [Delete Record Set](#) [Test Record Set](#) [Refresh](#) [Settings](#) [Help](#)

Record Set Name  Any Type ☐ Aliases Only ☐ Weighted Only

Displaying 1 to 5 out of 5 Record Sets

<input type="checkbox"/>	Name	Type	Value	Evaluate T
<input type="checkbox"/>	the-good-parts.com.	NS	ns-1995.awsdns-57.co.uk. ns-1166.awsdns-17.org. ns-38.awsdns-04.com. ns-836.awsdns-40.net.	-
<input type="checkbox"/>	the-good-parts.com.	SOA	ns-1995.awsdns-57.co.uk. awsdns-hostmaster.ama	-
<input type="checkbox"/>	_84ef0baccdf6ba5741476954d30fbed5.the-good-parts.com.the-good-parts.com.	CNAME	_1c9e37d93d92bf6646ace8c972cf2b7.mzlfexyxx.ε	-
<input type="checkbox"/>	prod.the-good-parts.com.	A	ALIAS awsbo-loadb-1ddgvd16xei9s-615344013.us-e	No
<input type="checkbox"/>	staging.the-good-parts.com.	A	ALIAS awsbo-loadb-1sn04p0ugu5rv-1429520787.us	No

### Hosted Zone CNAME Record



Now, we will add an HTTPS endpoint to our application in the next lesson.

[← Back](#)

[Next →](#)

Custom Domains: Map our Domain to ...

HTTPS: Add an HTTPS Endpoint



Mark as Completed



Report an Issue