

# Practical: Implementing HTTPS with AWS services


## Table of Contents

- [Prerequisites and resources](#)
- [Overview of process](#)
- [Obtaining a certificate](#)
- [Integrating with API Gateway](#)
- [Integrating with Application Load Balancer](#)
- [Integrating with Cloudfront](#)

AWS provides a certificate management service that integrates with a few other services to implement HTTPS access to your application. In this practical we'll explore the workflow for implementing HTTPS on AWS API Gateway, Application Load Balancer, and CloudFront.

Note that you must use either an API gateway or an Application Load Balancer in order to add HTTPS to your application. If you don't require their service abstraction or load balancing functionality then an API Gateway is a bit easier to set up.

## Prerequisites and resources

- [AWS ACM Docs](https://docs.aws.amazon.com/acm/)  (<https://docs.aws.amazon.com/acm/>)
- Practical: AWS Route53
- Practical: AWS API Gateway
- Practical: Application load balancer and auto scaling groups

## Overview of process

1. Create a subdomain
2. Obtain a certificate
3. Link certificate to an AWS service

## Obtaining a certificate

A certificate is tied to a particular domain. Before you start, make sure that you have created a subdomain of `cab432.com` for your application. Refer to Practical: AWS Route53 if you haven't already done so.

- In the AWS console, go to the AWS Certificate Manager (ACM) page
- In the top right of the certificates list, click *Request*
- Click *Next* to accept the certificate type


- Under *Fully qualified domain name* type in your full subdomain, including the `cab432.com` part.
- Under Tags add a tag with key `qut-username` and value your QUT username like `n1234567@qut.edu.au`
- Click *Request*. You will be sent to the details page for the certificate (which has not yet been issued.)
- Click *Create records in Route53* in the *Domains* section. Since the `cab432.com` domain (and all subdomains) are managed in Route53, ACM will then create the DNS records required for domain validation.
- On the next page, again click *Create records*

At this point you will need to wait for validation, which can take a few minutes. In the list of certificates you can click the refresh button to check the status.

## Integrating with API Gateway

Skip this section if you do not want to use an API gateway. We will assume that you already have an API Gateway set up for accessing your application. If not, refer to Practical: AWS API Gateway for more details.

- Go to the details page for your API Gateway
- In the left side panel, click *Custom domain names*
- Click *Create*
- Type in the domain name that you used to create the certificate
- In the *Endpoint configuration* section, under *ACM certificate* search for the certificate that you just created. If it is not there then check that validation has succeeded.
- Under Tags add a tag with key `qut-username` and value your QUT username like `n1234567@qut.edu.au`
- Click *Create domain name*
- After creating the domain name, you will be redirected to the details page for it. Click on the *API mappings* tab and then click on *Configure API mappings*.
- Select the API that you want to associate to this domain name and then click *Save*
- Under the *Configuration* tab, you will see the *API Gateway domain name*. This is the URL that you can use to access your API over HTTPS.
- In Route53, create a CNAME or A record for your subdomain that points to the API Gateway domain name

At this point you should be able to access your application over HTTPS at `https://<your subdomain>.cab432.com`. It may take a few minutes for the DNS record to propagate (<https://www.whatsmydns.net/>  [\(https://www.whatsmydns.net/\)](https://www.whatsmydns.net/) is a useful tool to check propagation).

## Integrating with Application Load Balancer

Skip this section if you do not want to use an application load balancer. We will assume that you already have an Application Load Balancer set up for accessing your application. If not, refer to Practical: Application load balancer and auto scaling groups for more details.

- Go to the details page for your application load balancer
- In the *Listeners and rules* section, click *Add listener*
- Under *Protocol* choose HTTPS.
- Configure the target group as required for your application, similar to how you configured it when creating the ALB.
- In the *Secure listener settings* section, under *Certificate (from ACM)*, search for your certificate.
- Click *Add*
- If your subdomain name's record does not already point to this load balancer, set that up.

At this point you should be able to access your application over HTTPS at `https://<your subdomain>.cab432.com`.

## Integrating with Cloudfront

This will be discussed in the Cloudfront practical.

TEQSA PRV12079 | CRICOS 00213J | ABN 83 791 724 622