**Chapter 7**

**AWS Creating Things, Certificates, and Policies (Video 7-4)**

Hi, I’m Alan Hawse, welcome back to WICED WiFi 101. Last time I introduced you to the wonderful world of AWS. In this video, I'm going to show you how to use the AWS web console to create things, certificates and policies.

First, I'll go to console.aws.amazon.com and login to my account. As I mentioned last time, you'll need to create your own account if you want to try this out.

Once I'm logged in I'll click on "IoT Core", then "Manage" to see the Things that are in my account.

## Things

I want to create a brand-new Thing, so I'll click on Create. I'm just going to create a single Thing for now, but you can see that AWS gives you a way to do batch operations too. And all of this can also be done programmatically - i.e. to make your company’s provisioning easier.

I'll name the Thing and leave everything else as it is and click Next.

## Certificates

I have the choice of creating a new Certificate for a new Thing, uploading one if I have my own – and remember you can create your own certificates with openSSL – or I can use a Certificate that I already have inside of AWS, or if you want, just skip the Certificate completely. I'm going to create a new Certificate for this example.

On this page, I have the option to download the certificate, public key, and private key. I also have the option to download the root CA for AWS. I will now download all of these. For the AWS Root CA certificate there are a few different choices. We will download the RootCA1, which uses an Amazon Trust Services – also known as ATS – RSA 2048 bit key.

It's VERY IMPORTANT that you download the certificates and keys before leaving this page. You won’t get another opportunity. You can get the certificates later if you need them, but once you leave this page, you will not be able to retrieve the keys, so you won't be able to use the device certificate that you just created if you don't download those keys right now.

Once I have the keys, I want to Activate the Certificate.

## Policies

Next, I need a Policy. The Policy is used to set permissions for the Thing. That is, what IoT actions it can perform and on what elements it can perform those actions. For example, a light switch would need to update the desired state of a light bulb but not the reported state, and vice versa.

If I had an existing Policy that I wanted to use I could Attach it here, but I want to create a new one, so I will click on Done, Secure, Policies, Create.

I'll give the policy a name. Under actions, I want to give this Thing permission to do any IoT function so I'll enter iot:\*. You can see that other options exist to allow only Publish, only Subscribe, and so on.

For the resource ARN I'll just put in \* and I'll check "Allow" so that it will be able to update any resource. Then I'll click on Create.

Next, I need to attach a Policy to the Certificate. If you know the number of your certificate you can get to it from Secure > Certificates. If you don't remember the number, you can go to Manage > Things, click on the Thing that you created, then Security and you will see the Certificate that you attached when you created the Thing.

Click on the Certificate and then on Actions > Attach Policy. Select the policy that you created and click "Attach".

OK, now let's make sure everything is setup the way it should be. I first click on the Thing. It has a Certificate attached to it and the Certificate is Active – that’s good. The Certificate has a Policy attached to it that allows all IoT actions on any resource. OK, that's good.

Now I have a Thing setup in AWS. It has an Active Certificate attached to it and the Certificate has a Policy that allows the actions we want. In the next video, I'll show you how to get your WICED IoT device to interact with the AWS Cloud.

As always, you should post your comments and questions in our WiFi developer community or you are welcome to email me at alan\_hawse@cypress.com or tweet me @askioexpert. Thank you.