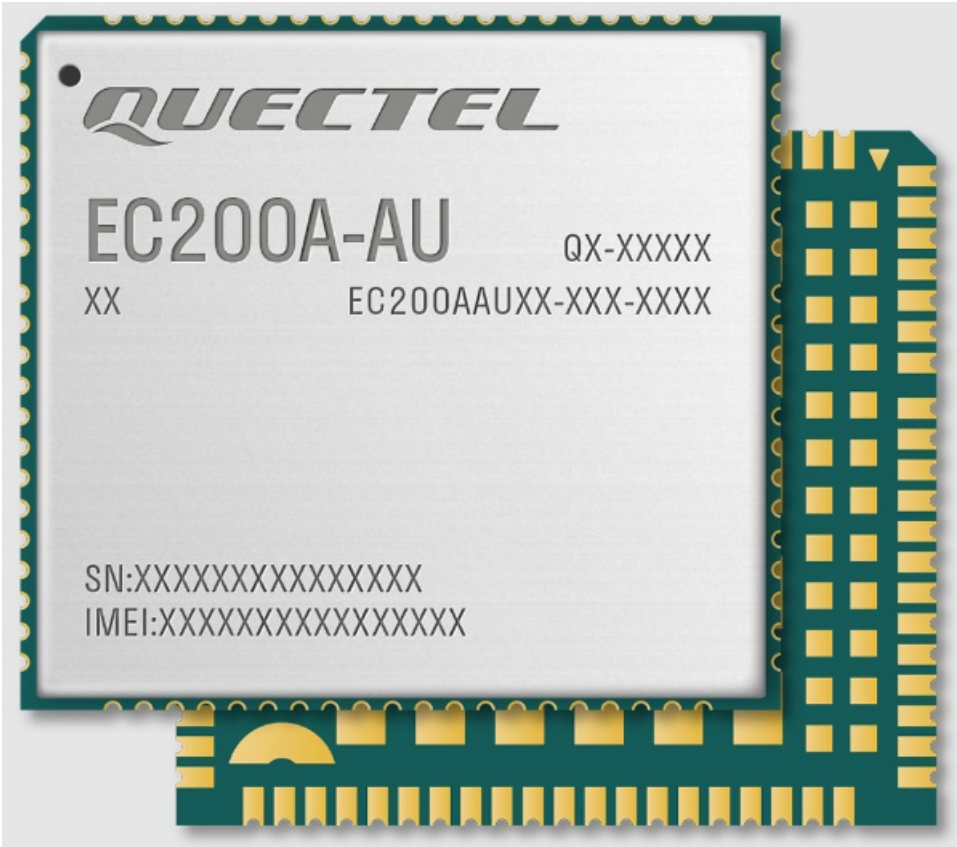


QUECTEL EC2x Series LTE Standard Module User Guide

[Home](#) » [QUECTEL](#) » QUECTEL EC2x Series LTE Standard Module User Guide 

QUECTEL EC2x Series LTE Standard Module



Contents

- [1 Legal Notices](#)
- [2 Use and Disclosure Restrictions](#)
- [3 About the Document](#)
- [4 Introduction](#)
- [5 AWS IoT Platform Access](#)
 - [5.1 Using Device Shadow Service](#)
- [6 Example](#)
- [7 Appendix A References](#)
- [8 Customer Support](#)
- [9 Documents / Resources](#)
 - [9.1 References](#)
- [10 Related Posts](#)

Legal Notices

We offer information as a service to you. The provided information is based on your requirements and we make every effort to ensure its quality. You agree that you are responsible for using independent analysis and evaluation in designing intended products, and we provide reference designs for illustrative purposes only. Before using any hardware, software or service guided by this document, please read this notice carefully. Even though we employ commercially reasonable efforts to provide the best possible experience, you hereby acknowledge and agree that this document and related services hereunder are provided to you on an “as available” basis. We may revise or restate this document from time to time at our sole discretion without any prior notice to you.

Use and Disclosure Restrictions

License Agreements

Documents and information provided by us shall be kept confidential, unless specific permission is granted. They shall not be accessed or used for any purpose except as expressly provided herein.

Copyright

Our and third-party products hereunder may contain copyrighted material. Such copyrighted material shall not be copied, reproduced, distributed, merged, published, translated, or modified without prior written consent. We and the third party have exclusive rights over copyrighted material. No license shall be granted or conveyed under any patents, copyrights, trademarks, or service mark rights. To avoid ambiguities, purchasing in any form cannot be deemed as granting a license other than the normal non-exclusive, royalty-free license to use the material. We reserve the right to take legal action for noncompliance with abovementioned requirements, unauthorized use, or other illegal or malicious use of the material.

Trademarks

Except as otherwise set forth herein, nothing in this document shall be construed as conferring any rights to use any trademark, trade name or name, abbreviation, or counterfeit product thereof owned by Quectel or any third party in advertising, publicity, or other aspects.

Third-Party Rights

This document may refer to hardware, software and/or documentation owned by one or more third parties (“third-party materials”). Use of such third-party materials shall be governed by all restrictions and obligations applicable thereto.

We make no warranty or representation, either express or implied, regarding the third-party materials, including but not limited to any implied or statutory, warranties of merchantability or fitness for a particular purpose, quiet enjoyment, system integration, information accuracy, and non-infringement of any third-party intellectual property rights with regard to the licensed technology or use thereof. Nothing herein constitutes a representation or warranty by us to either develop, enhance, modify, distribute, market, sell, offer for sale, or otherwise maintain production of any our products or any other hardware, software, device, tool, information, or product. We moreover disclaim any and all warranties arising from the course of dealing or usage of trade.

Privacy Policy

To implement module functionality, certain device data are uploaded to Quectel's or third-party's servers, including carriers, chipset suppliers or customer-designated servers. Quectel, strictly abiding by the relevant laws and regulations, shall retain, use, disclose or otherwise process relevant data for the purpose of performing the service only or as permitted by applicable laws. Before data interaction with third parties, please be informed of their privacy and data security policy.

Disclaimer

- a) We acknowledge no liability for any injury or damage arising from the reliance upon the information.
- b) We shall bear no liability resulting from any inaccuracies or omissions, or from the use of the information contained herein.
- c) While we have made every effort to ensure that the functions and features under development are free from errors, it is possible that they could contain errors, inaccuracies, and omissions. Unless otherwise provided by valid agreement, we make no warranties of any kind, either implied or express, and exclude all liability for any loss or damage suffered in connection with the use of features and functions under development, to the maximum extent permitted by law, regardless of whether such loss or damage may have been foreseeable.
- d) We are not responsible for the accessibility, safety, accuracy, availability, legality, or completeness of information, advertising, commercial offers, products, services, and materials on third-party websites and third-party resources.

Copyright © Quectel Wireless Solutions Co., Ltd. 2022. All rights reserved.

About the Document

Revision History

Version	Date	Author	Description
—	2020-08-24	Domingo DENG	Creation of the document
1.0.0	2022-11-21	Domingo DENG	Preliminary

Introduction

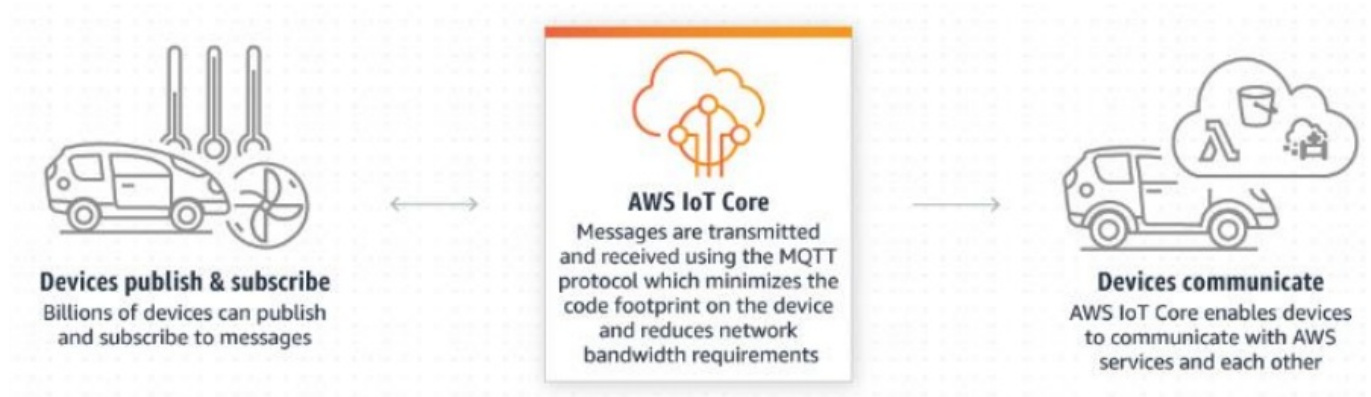
Brief Introduction on AWS IoT

AWS IoT provides secure, bi-directional communication between Internet-connected devices such as sensors, actuators, embedded micro-controllers, or smart appliances and the AWS Cloud. This enables to collect telemetry data from multiple devices, and store and analyze the data.

AWS IoT Cloud platform supports TLS dual authentication for client certificates, in which MQTT can act as a

message broker which provides a secure mechanism for devices and AWS IoT applications to publish and receive messages from each other. After importing certificates into Quectel module, the module can access to AWS IoT Cloud platform through MQTTS.

Figure 1: Communication between AWS IOT and the Device



Document Overview

This document mainly provides users with AWS IoT Cloud platform access method, including how to connect Quectel module to AWS IoT Cloud platform with MQTTS and the related AT command involved in the AWS IoT platform access process.

Applicable Modules

This document is applicable to the following Quectel modules:

- EC2x: EC25 Series/EC21 Series/EC20-CE
- EG2x: EG21-G/EG25-G/EG21-GL/EG25-GL
- EG9x: EG91 Series/EG95 Series

AWS IoT Platform Access

This chapter mainly describes AWS IoT Cloud platform access process and how to use the device shadow service after accessing the AWS IoT.

NOTE

Before using AWS IoT services, an AWS account must be created. Please refer to the AWS official website link <https://aws.amazon.com/premiumsupport/knowledge-center/create-and-activate-aws-account/> for details on how to create an AWS account.

Accessing the AWS IoT Platform

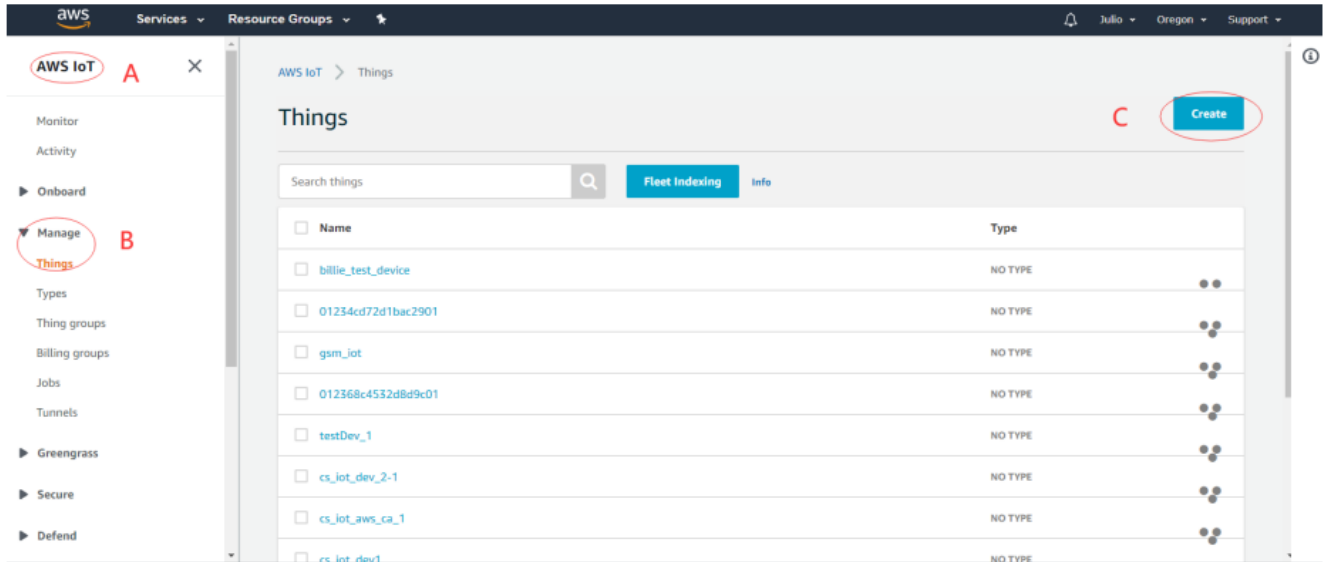
1. Register devices and get certificates

A. Browse to the AWS IoT console

B. In the navigation pane, choose "Manage", and then choose "Things".

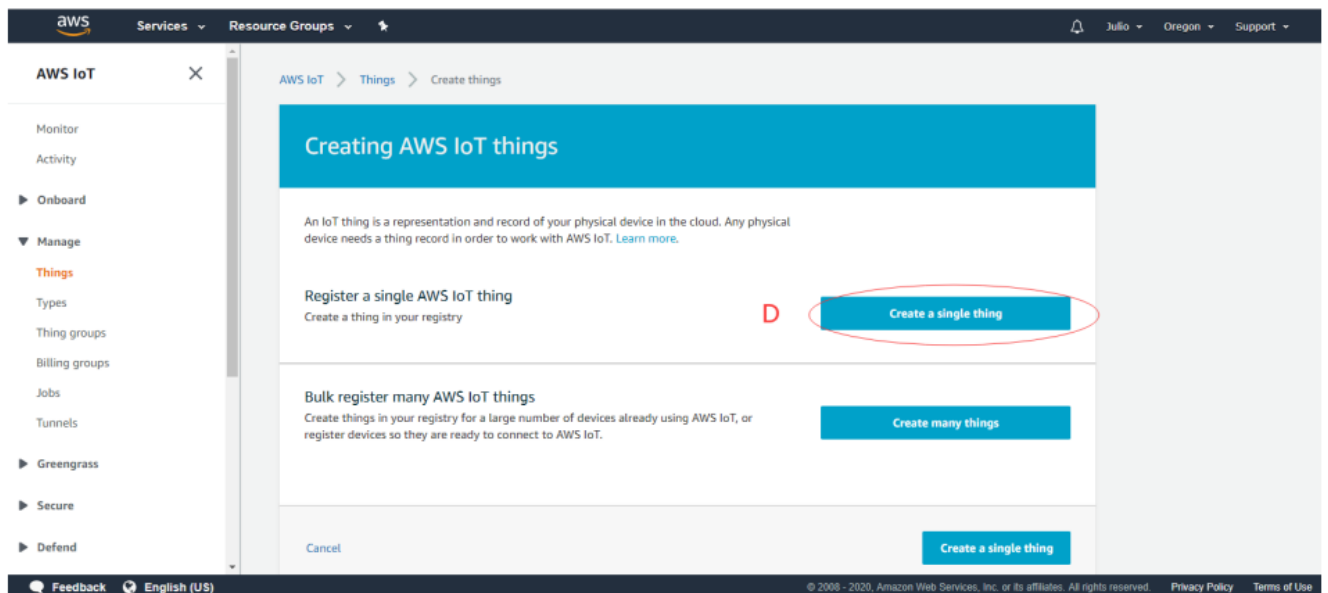
C. If you do not have any IoT things registered in your account, then you don't have any things yet page is displayed. If you see this page, choose "Register a thing". Otherwise, choose "Create".

Figure 2: Browse to the AWS IoT Console



D. On the “Creating AWS IoT things” page, choose “Create a single thing”.

Figure 3: Create a Single Thing



E. On the “Add your device to the thing registry” page, enter a name for your thing, and then choose “Next”.

Figure 4: Name Your Thing

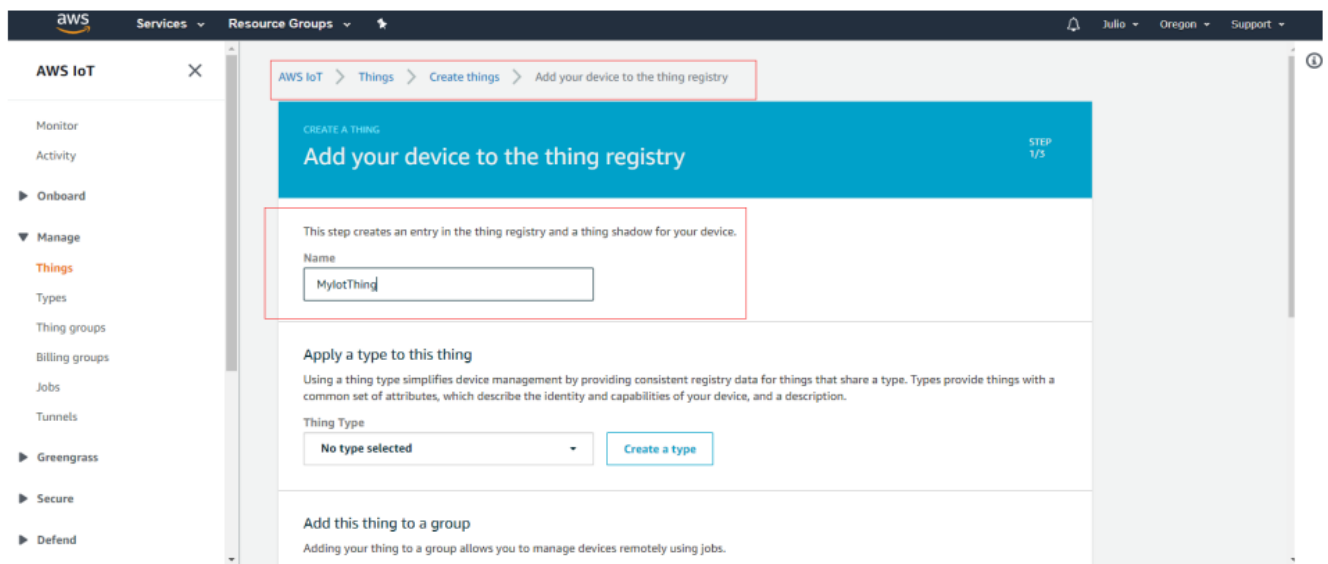
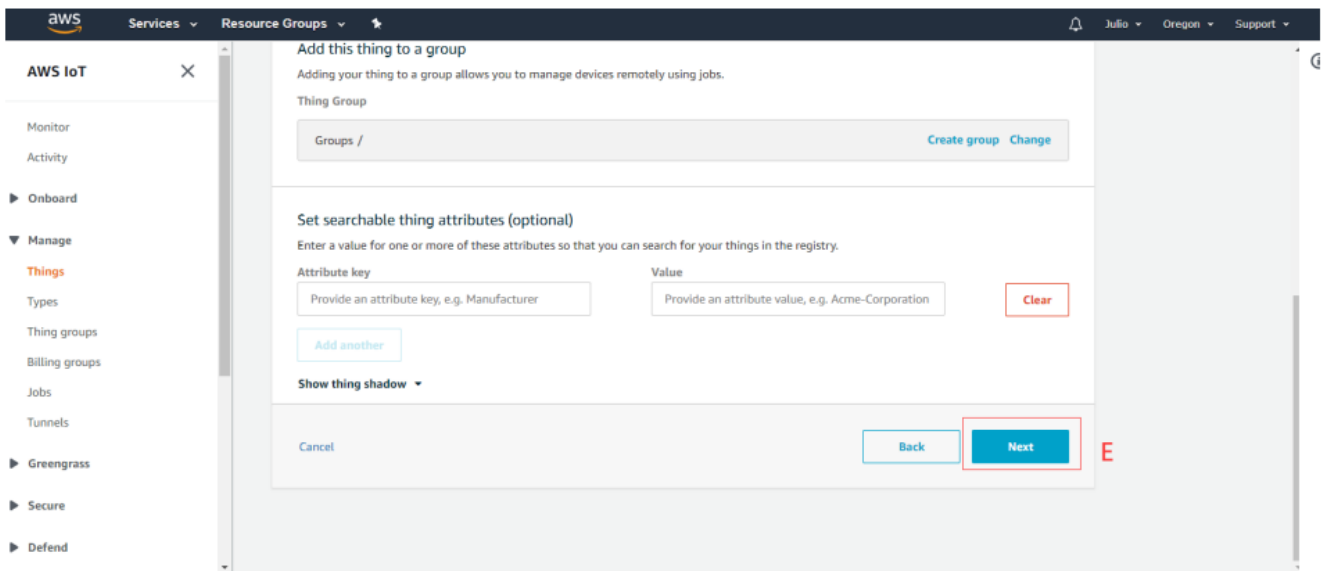
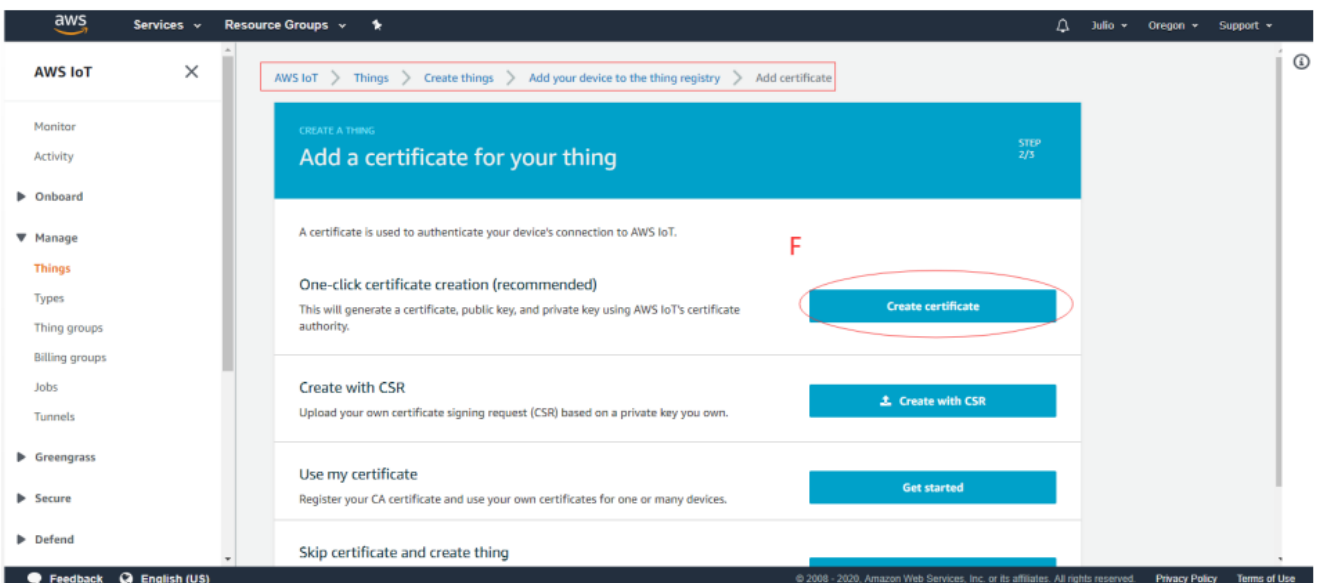


Figure 5: Choose “Next”



F. On the Add a certificate for your thing page, under “One-click certificate creation”, choose “Create certificate”.

Figure 6: Create Certificate



G. Download your private key and certificate by choosing the Download links for each. Note that the keys cannot be retrieved after you close this page.

H. For the root CA for AWS IoT, click on Download and select the appropriate one:

RSA 2048 bit key: Amazon Root CA 1

ECC 256 bit key: Amazon Root CA 3

Figure 7: Select the Appropriate Root CA

Amazon Trust Services Endpoints (preferred)

Note

You might need to right click these links and select **Save link as...** to save these certificates as files.

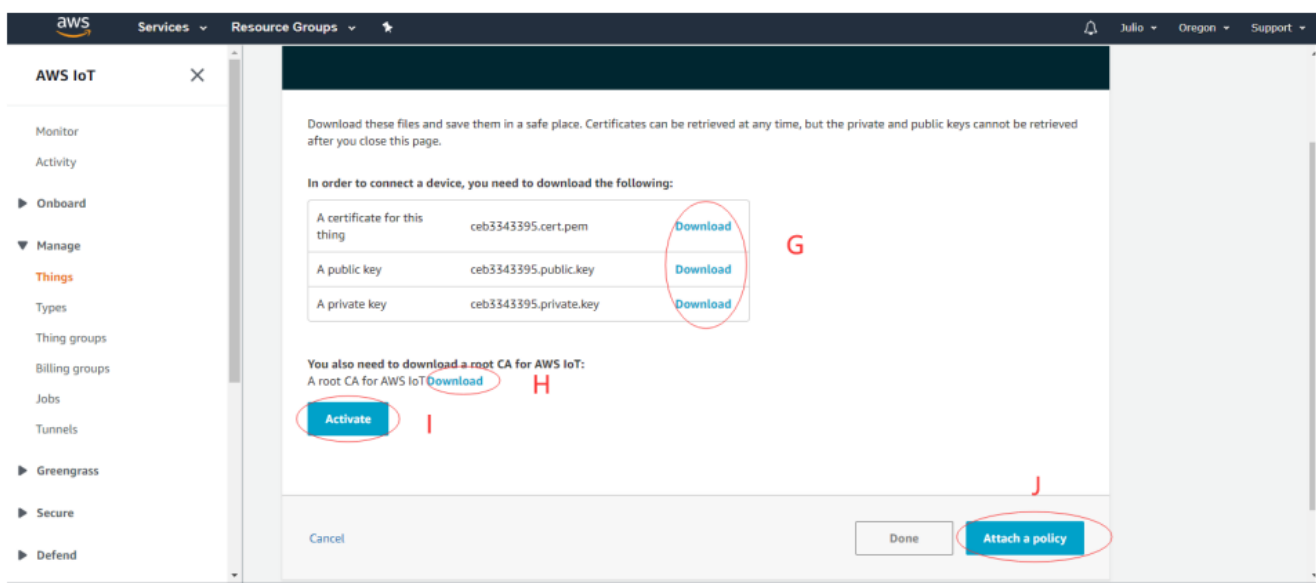
- RSA 2048 bit key: [Amazon Root CA 1](#).
- RSA 4096 bit key: Amazon Root CA 2. Reserved for future use.
- ECC 256 bit key: [Amazon Root CA 3](#).
- ECC 384 bit key: Amazon Root CA 4. Reserved for future use.

These certificates are all cross-signed by the [Starfield Root CA Certificate](#). All new AWS IoT Core regions, beginning with the May 9, 2018 launch of AWS IoT Core in the Asia Pacific (Mumbai) Region, serve only ATS certificates.

I. Choose “Activate” to activate your certificate. Certificates must be activated prior to use.

J. You can either attach an existing policy, or create one. Choose “Attach a policy” to attach a policy to your certificate that grants your device access to AWS IoT operations.

Figure 8: Download and Activate the Private Key and Certificate



Select the policy (or policies) to be attached, and choose Register thing. At this point, your device has been provisioned with AWS IoT and can begin to communicate.

2. Find MQTTS connection address and port of devices

A. Browse to the AWS IoT console

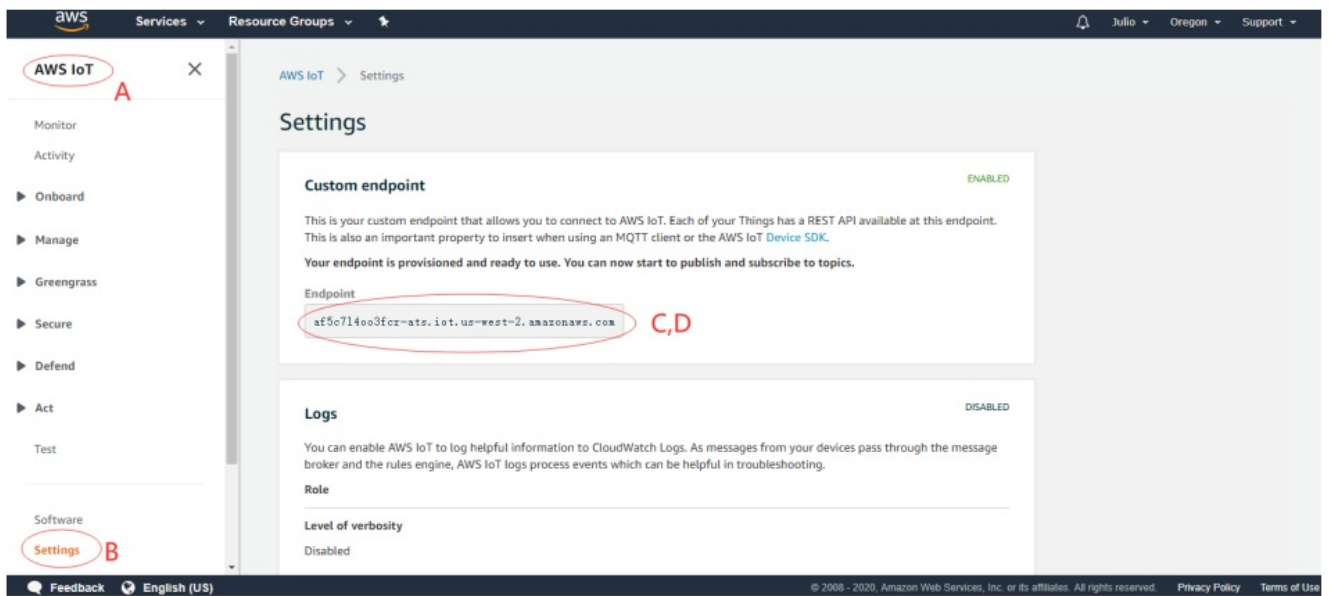
B. In the navigation pane, choose “Settings”.

C. Your AWS IoT endpoint is displayed in Endpoint. It should look like [1234567890123-ats.iot.us-east-1.amazonaws.com](#).

D. Make a note of this endpoint. Your account number and region name may be different from the example shown above.

The steps above are shown in the figure below:

Figure 9: MQTTS Connection Address



The MQTTS connection port supported by AWS IoT platform is shown as below.

Figure 10: MQTTS Connection Port

Protocols, Port Mappings, and Authentication

The following table shows each protocol supported by AWS IoT, the authentication method, and port used for each protocol.

Protocol, Authentication, and Port Mappings			
Protocol	Authentication	Port	ALPN ProtocolName
MQTT	X.509 client certificate	8883, 443 [†]	x-amzn-mqtt-ca
HTTPS	X.509 client certificate	8443, 443 [†]	x-amzn-http-ca
HTTPS	SigV4	443	N/A
MQTT over WebSocket	SigV4	443	N/A

[†]Clients that connect on port 443 with X.509 client certificate authentication must implement the [Application Layer Protocol Negotiation \(ALPN\)](#) TLS extension and use the [ALPN ProtocolName](#) listed in the [ALPN ProtocolNameList](#) sent by the client as part of the [ClientHello](#) message.

3. Import certificates and connect to AWS IoT platform

Import certificates into the module and connect the module to AWS IoT platform with AT command related to MQTTS. The process is shown as below.

Step 1: Upload the certificate files and configure TLS.

Figure 11: Certificate Files Downloaded from AWS IoT

名称	download from aws	修改日期	类型	大小
a8c6003c31-certificate.pem.crt	2020/1/10 10:20	安全证书	cc.pem	2 KB
a8c6003c31-private.pem.key	2020/1/10 16:20	私钥文件	ck.pem	2 KB
a8c6003c31-public.pem.key	2020/1/10 16:20	KEY 文件		1 KB
Amazon_Root_CA_1.pem	2020/1/10 16:22	PEM 文件	ca.pem	2 KB

Figure 12: Upload Certificate Files

COM Port Setting

COM Port: 134

Baudrate: 115200

StopBits: 1

Parity: None

ByteSize: 8

Flow Control: No Ctrl Flow

Close Port

[2020-08-23_20:39:39:717]AT+qfupl="ca.pem",1188

[2020-08-23_20:39:39:736]CONNECT

[2020-08-23_20:39:43:455]+QFUPL: 1188,2d13

[2020-08-23_20:39:43:455]OK

[2020-08-23_20:39:48:412]AT+qfupl="cc.pem",1220

[2020-08-23_20:39:48:435]CONNECT

[2020-08-23_20:39:49:910]+QFUPL: 1220,64f upload certificate to module

[2020-08-23_20:39:49:910]OK

[2020-08-23_20:39:55:060]AT+qfupl="ck.pem",1675

[2020-08-23_20:39:55:080]CONNECT

[2020-08-23_20:39:56:818]+QFUPL: 1675,632f

[2020-08-23_20:39:56:818]OK

[2020-08-23_20:40:01:761]AT+QFLST="*"

[2020-08-23_20:40:01:791]+QFLST: "UFS:ca.pem",1188

[2020-08-23_20:40:01:791]+QFLST: "UFS:cc.pem",1220

[2020-08-23_20:40:01:791]+QFLST: "UFS:ck.pem",1675

[2020-08-23_20:39:52:254]This File Size is 1675 Bytes

[2020-08-23_20:39:55:062]DCD:1 CTS:1 RI:0

[2020-08-23_20:39:56:799]DCD:0 CTS:1 RI:0

Figure 13: Configure TLS

COM Port Setting

COM Port: 134

Baudrate: 115200

StopBits: 1

Parity: None

ByteSize: 8

Flow Control: No Ctrl Flow

Close Port

[2020-08-23_20:39:56:818]+QFUPL: 1675,632f

[2020-08-23_20:39:56:818]OK

[2020-08-23_20:40:01:761]AT+QFLST="*"

[2020-08-23_20:40:01:791]+QFLST: "UFS:ca.pem",1188

[2020-08-23_20:40:01:791]+QFLST: "UFS:cc.pem",1220

[2020-08-23_20:40:01:791]+QFLST: "UFS:ck.pem",1675

[2020-08-23_20:40:01:791]OK

[2020-08-23_20:41:46:593]AT+QSSLCFG="clientkey",1,"UFS:ck.pem"

[2020-08-23_20:41:46:593]OK

[2020-08-23_20:41:47:556]AT+QSSLCFG="clientcert",1,"UFS:cc.pem"

[2020-08-23_20:41:47:556]OK

[2020-08-23_20:41:48:511]AT+QSSLCFG="cacert",1,"UFS:ca.pem"

[2020-08-23_20:41:48:511]OK

[2020-08-23_20:41:49:72]AT+QSSLCFG="ciphersuite",1,0xFFFF

[2020-08-23_20:41:49:72]OK

[2020-08-23_20:41:49:588]AT+QSSLCFG="seclevel",1,2

[2020-08-23_20:41:49:588]OK

[2020-08-23_20:42:59:402]AT+QMTCFG="ssl",1,1,1

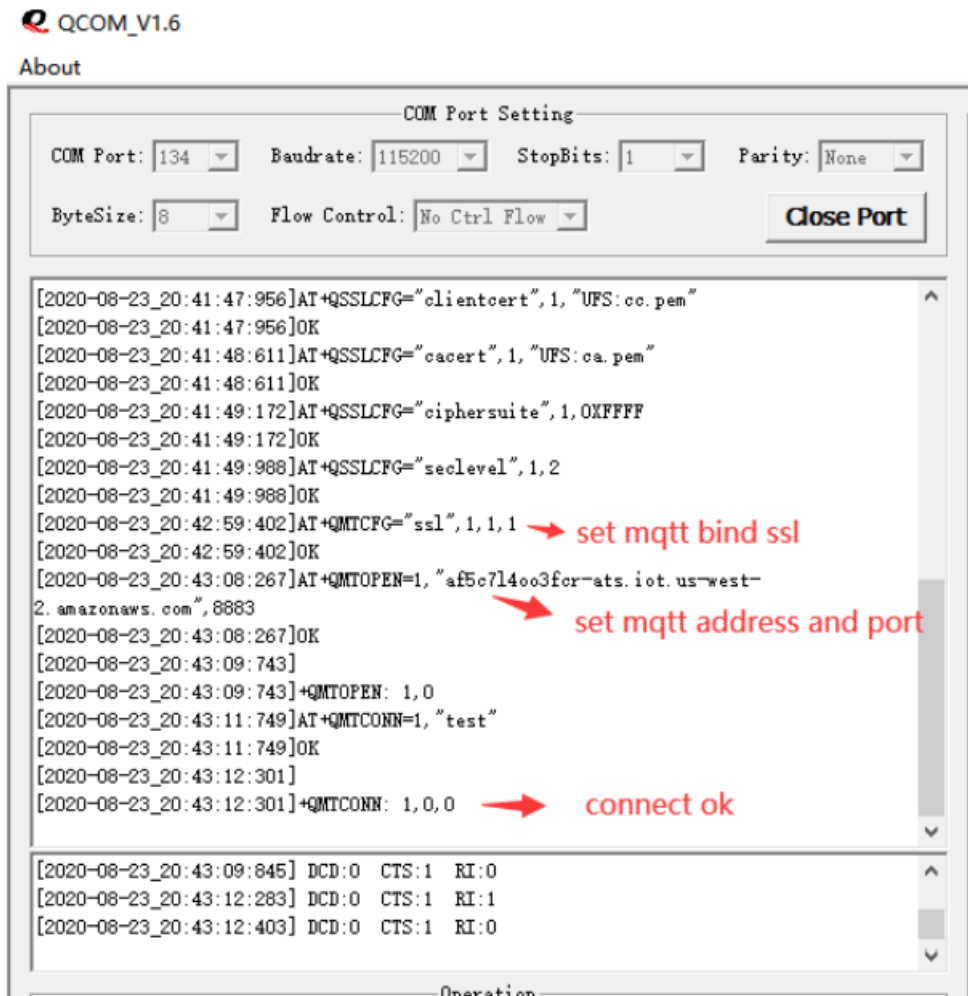
[2020-08-23_20:51:10:278]DCD:0 CTS:1 RI:0

[2020-08-23_20:51:26:380]DCD:0 CTS:1 RI:1

[2020-08-23_20:51:26:508]DCD:0 CTS:1 RI:0

Step 2: Connect to AWS IoT with MQTTS.

Figure 14: Connect to AWS IoT with MQTTS



NOTE

Some old FW required additional TLS configuration by AT command below:

AT+QSSLCFG="ignoreinvalidcertsign" and AT+QSSLCFG="ignoremulticertchainverify".

Using Device Shadow Service

Device Shadow Service

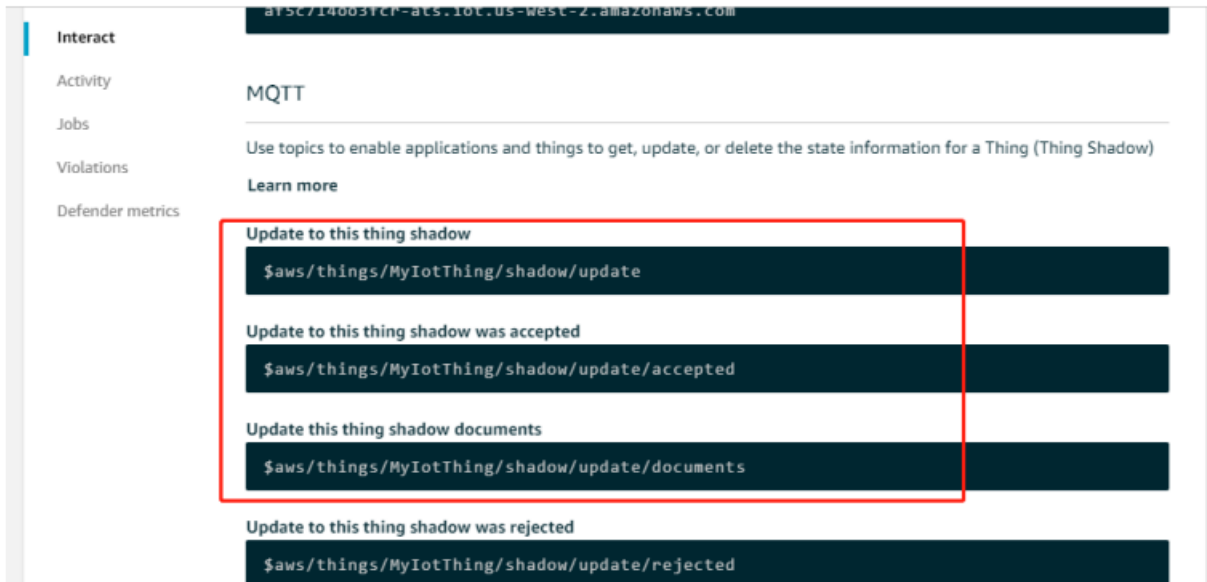
Device shadow service, provided by AWS IoT Cloud platform, maintains a shadow which is a JSON document that is used to store and retrieve current state information for each device connected to AWS IoT.

For using shadow service, please subscribe and publish topics specified by the AWS IoT in JSON format through MQTT. For details, please refer to AWS IoT official website documentation through the link <https://docs.aws.amazon.com/iot/latest/developerguide/iot-device-shadows.html>.

Subscribe and Publish Shadow Topics

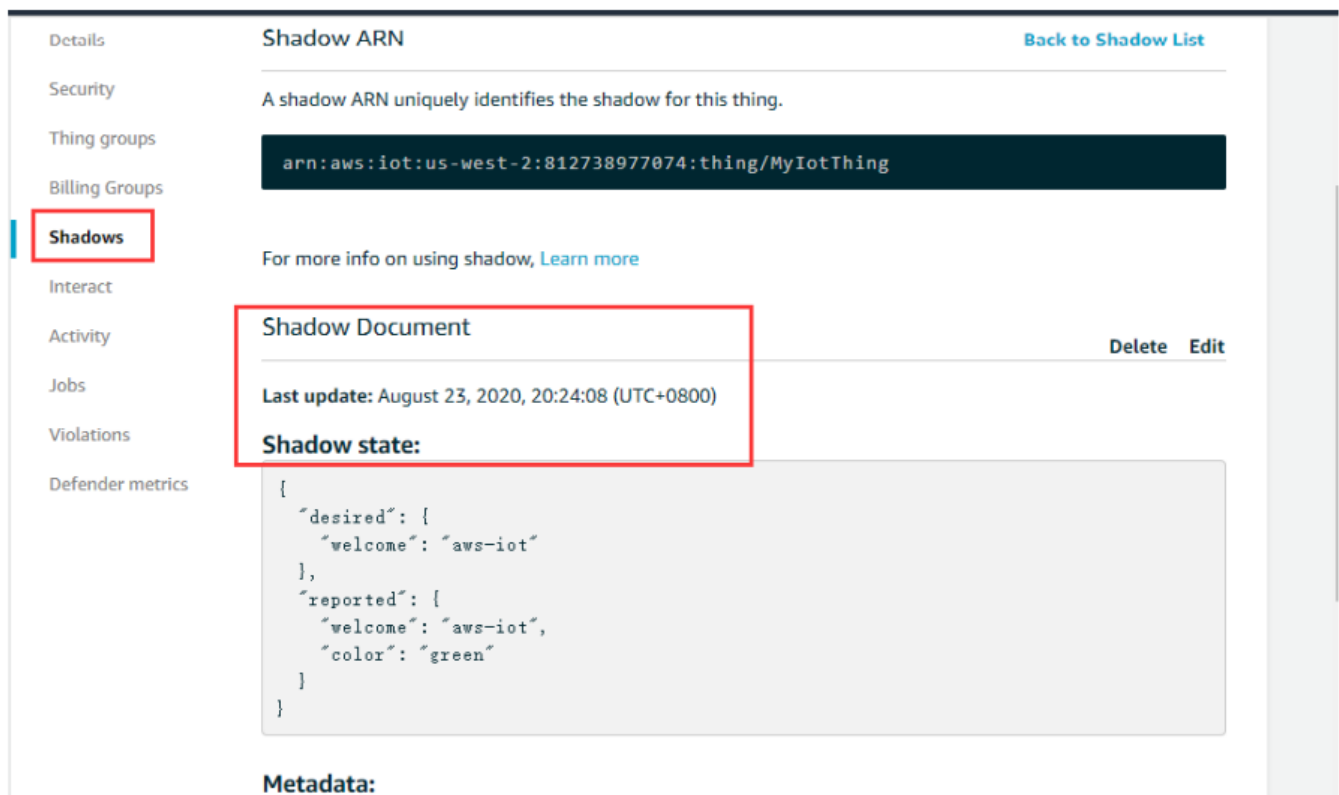
Step 1: Sign in to the AWS IoT console, search "IoT" in search bar, choose "Manage"->"Things", select the created Thing, and on the pop-up page, choose "Interact" in the Details column to view shadow topics which should be subscribed after the module accesses to AWS IoT, as shown below.

Figure 15: Shadow Topics



Step 2: On the page after clicking the created Thing, choose “Shadow” in the Details column to view shadow document where the shadow state will update when receiving messages published from devices, as shown below.

Figure 16: Shadow Document



Step 3: Modules are to subscribe and publish shadow topics, as shown below.

Figure 17: Subscribe Shadow Topics

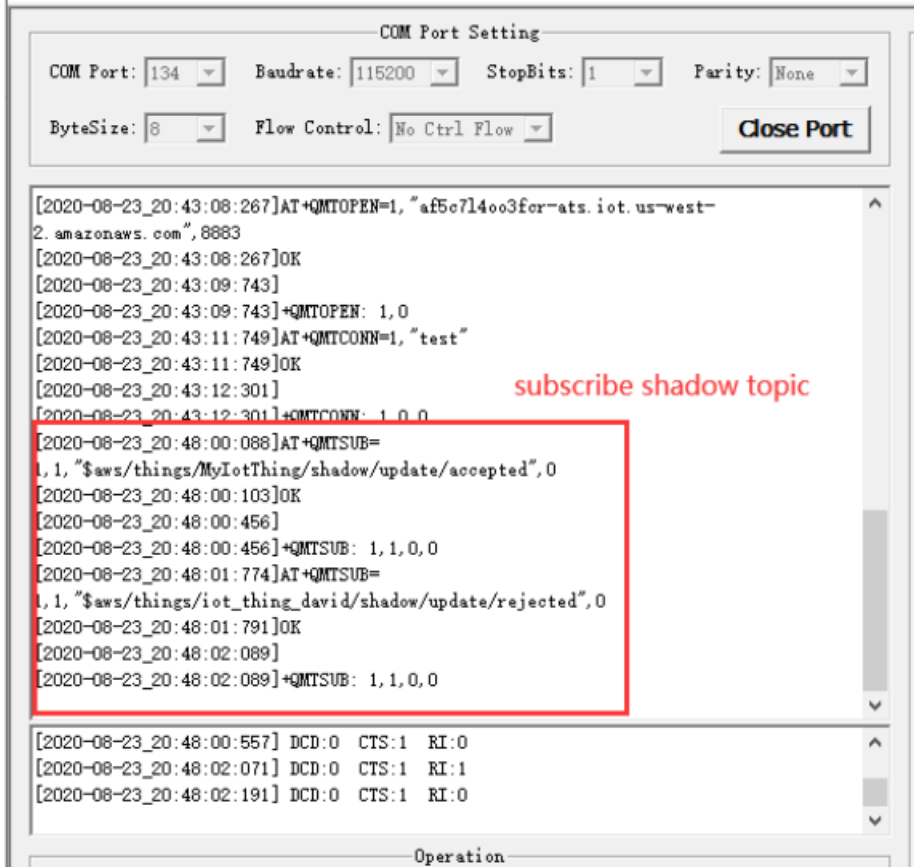
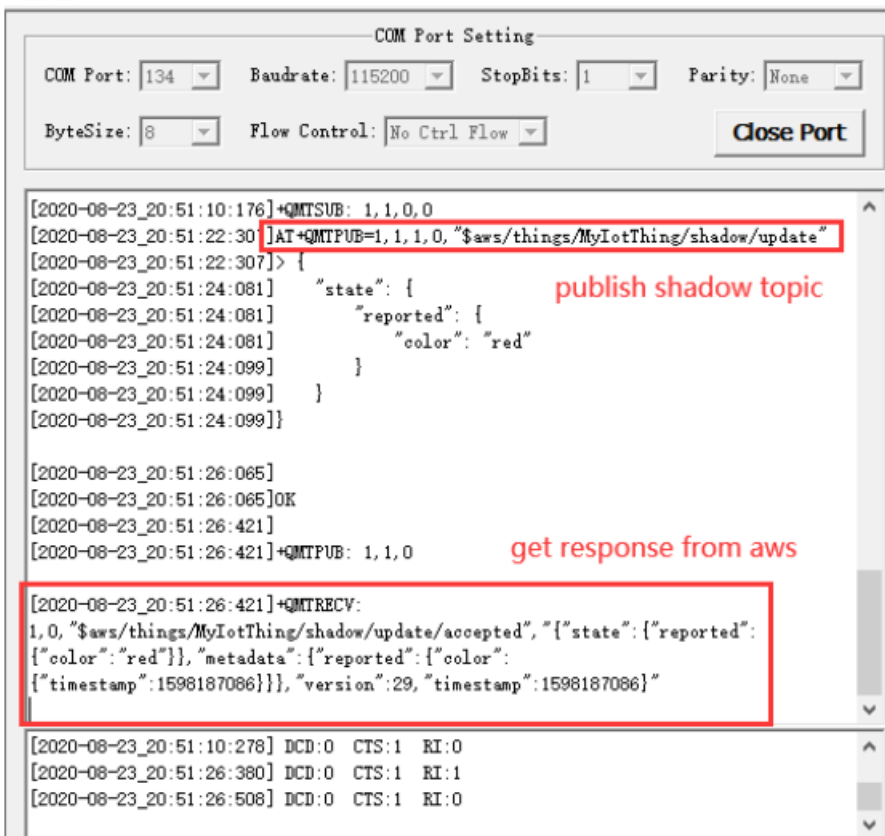


Figure 18: Publish Shadow Topics



Step 4: Back to “Shadow Document” to view the shadow state, as shown below.

Figure 19: View Shadow State

The screenshot shows the AWS IoT console interface for a specific thing. On the left is a navigation menu with options: Details, Security, Thing groups, Billing Groups, Shadows (selected), Interact, Activity, Jobs, Violations, and Defender metrics. The main content area is titled 'Shadow ARN' with a 'Back to Shadow List' link. Below this, it explains that a shadow ARN uniquely identifies the shadow for a thing and shows the ARN: `arn:aws:iot:us-west-2:812738977074:thing/MyIotThing`. The 'Shadows' section includes a 'Learn more' link. The 'Shadow Document' section, highlighted with a red box, shows the 'Last update' timestamp: 'August 23, 2020, 20:51:26 (UTC+0800)'. Below this, the 'Shadow state' is displayed as a JSON object in a code block. The JSON shows 'desired' and 'reported' states, both with a 'welcome' field set to 'aws-iot'. The 'reported' state also includes a 'color' field set to 'red', which is highlighted with a red box.

```
{
  "desired": {
    "welcome": "aws-iot"
  },
  "reported": {
    "welcome": "aws-iot",
    "color": "red"
  }
}
```

Example

This chapter provides examples for AWS IoT platform access authentication. The following shows the whole process of accessing the AWS IoT with MQTTS.

```
//Import certificates into the module.
AT+QFUPL="ca.pem",1206
CONNECT
+QFUPL: 1206,5a63
OK
AT+QFUPL="cc.pem",1220
CONNECT
+QFUPL: 1220,3879
OK
AT+QFUPL="ck.pem",1675
CONNECT
+QFUPL: 1675,6136
OK
AT+QFLST=""
+QFLST: "UFS:ca.pem",1206
+QFLST: "UFS:cc.pem",1220
+QFLST: "UFS:ck.pem",1675
OK
//Configure TLS.
AT+QSSLCFG="clientkey",1,"UFS:ck.pem"
OK
AT+QSSLCFG="clientcert",1,"UFS:cc.pem"
OK
AT+QSSLCFG="cacert",1,"UFS:ca.pem"
OK
```

```

AT+QSSLCFG="ciphersuite",1,0xFFFF
OK
AT+QSSLCFG="seclevel",1,2
OK
//Connect to AWS through MQTTS.
AT+QMTCFG="ssl",1,1,1
OK
AT+QMTOPEN=1,"af5c7l4oo3fcr-ats.iot.us-west-2.amazonaws.com",8883
OK
+QMTOPEN: 1,0
AT+QMTCONN=1,"test"
OK
+QMTCONN: 1,0,0 //Connected to AWS IoT successfully.
//Test shadow service.
AT+QMTSUB=1,1,"$aws/things/MyIotThing/shadow/update/accepted",0
OK
+QMTSUB: 1,1,0,0
AT+QMTSUB=1,1,"$aws/things/MyIotThing/shadow/update/rejected",0
OK
+QMTSUB: 1,1,0,0
AT+QMTPUB=1,1,1,0,"$aws/things/MyIotThing/shadow/update"
> {
  "state": {
    "reported": {
      "color": "red"
    }
  }
}
OK
+QMTPUB: 1,1,0
+QMTRECV:1,0,"$aws/things/MyIotThing/shadow/update/accepted","{"state":{"reported":{"color":
:"red"},"metadata":{"reported":{"color":{"timestamp":1579138722}}},"version":15,"timestamp":1
579138722}" //Received the response from shadow service.
//Disconnect from the AWS IoT.
AT+QMTCLOSE=1
OK
+QMTCLOSE: 1,0

```

NOTE

For the details of above commands, please refer to Document [1], Document [2] and Document [3] listed in Appendix A.

Appendix A References

Table 1: Related Documents

Document Name
[1] Quectel_LTE_Standard_FILE_Application_Note
[2] Quectel_LTE_Standard_MQTT_Application_Note
[3] Quectel_EC2x&EG9x&EG2x-G&EM05_Series_SSL_Application_Note

Table 2: Terms and Abbreviations

Abbreviation	Description
AWS	Amazon
IoT	Internet of Things
MQTT(S)	Message Queuing Telemetry Transport (Security)
TLS	Transport Layer Security
SSL	Secure Sockets Layer

Customer Support

At Quectel, our aim is to provide timely and comprehensive services to our customers. If you require any assistance, please contact our headquarters: Quectel Wireless Solutions Co., Ltd.
Building 5, Shanghai Business Park Phase III (Area B), No.1016 Tianlin Road, Minhang District, Shanghai 200233, China

Tel: +86 21 5108 6236


Email: info@quectel.com

Or our local offices. For more information, please visit: <http://www.quectel.com/support/sales.htm>.

For technical support, or to report documentation errors, please visit:
<http://www.quectel.com/support/technical.htm>. Or email us at: support@quectel.com.



Documents / Resources

	<p>QUECTEL EC2x Series LTE Standard Module [pdf] User Guide</p> <p>EC2x Series LTE Standard Module, EC2x Series, LTE Standard Module, Standard Module, Module</p>
---	---

References

- [User Manual](#)