SARA-R510AWS

Application development guide

Application note



Abstract

This document provides detailed technology architecture and examples of how to use AT commands with u-blox SARA-R510AWS modules.

UBX-22017004 - R06
C1-Public

Document information

Title	**SARA-R510AWS**	
Subtitle	Application development guide	
Document type	Application note	
Document number	UBX-22017004	
Revision and date	R06	19-Sep-2024
Disclosure restriction	C1-Public	

This document applies to the following products:

Product name
SARA-R510AWS

u-blox or third parties may hold intellectual property rights in the products, names, logos, and designs included in this document. Copying, reproduction, or modification of this document or any part thereof is only permitted with the express written permission of u-blox. Disclosure to third parties is permitted for clearly public documents only.
The information contained herein is provided “as is” and u-blox assumes no liability for its use. No warranty, either express or implied, is given, including but not limited to, with respect to the accuracy, correctness, reliability, and fitness for a particular purpose of the information. This document may be revised by u-blox at any time without notice. For the most recent documents, visit www.u-blox.com.
Copyright © u-blox AG.

Contents

Document information **2**
Contents **3**
1 Introduction **5**
2 Application design and development **6**
2.1 Initial design decisions 6
2.2 Application stages 6
2.2.1 Power-on 6
2.2.2 Power-off 6
3 Local connectivity **8**
3.1 AT interface 8
3.2 AT commands response parser 8
3.3 UART configuration 8
4 MNO profiles **9**
4.1 Using MNO profiles 9
4.2 Modifiable parameters 9
4.3 MNO profile setting examples 9
4.4 AT&T profile (+DIAG MNOPROF=2) 10
4.5 Verizon profile (+DIAG MNOPROF=3) 10
4.6 T-Mobile profile (+DIAG MNOPROF=5) 10
4.7 Regulatory / Conformance profiles (+DIAG MNOPROF=0 / 201) 10
5 Network registration **11**
5.1 First time registration setup 11
5.2 PAP/CHAP Authentication 11
6 Register SARA-R510AWS with an AWS account **12**
6.1 Set up the AWS account and permissions 12
6.2 Setting up the module 12
6.3 Registering with your AWS account 13
6.4 Completion 18
7 Connect to and interact with the AWS cloud **19**
7.1 Connecting 19
7.2 Receiving data and commands from the AWS cloud 19
7.3 Sending data to the AWS cloud 20
7.4 AWS IoT Device Shadow 21
7.4.1 Enabling Device Shadow feature 22
7.4.2 Type of Shadow service 22
7.4.3 Requesting a Device Shadow document 22
7.4.4 Shadow document update 23
7.4.5 Unsubscribe Shadow Document 23
7.4.6 Delete Device Shadow 23
7.5 Embedded security 23

7.5.1 Security Certificates 24
7.5.2 AWS Device Defender 24
8 Firmware update 26
8.1 FOTA FW update 26
8.1.1 uFOTA configuration and example 26
8.2 EasyFlash 27
8.3 FOAT FW update 27
9 Host OTA FW update 28
9.1 Host OTA example 28
10 Low-power and SLEEP modes 30
11 Troubleshooting 31
11.1 Diagnostic commands 31
11.2 Unable to connect errors 31
11.3 Other troubleshooting actions 32
12 Features supported 33
Appendix 34
A LPWA technology overview 34
B Glossary 35
Related documentation 36
Revision history 36
Contact 36

1 Introduction

This document provides guidance for developing applications that interface with the u-blox SARA-R510AWS module, including examples of AT command sequences for specific use cases. This is the first document to read when working on an application built with the SARA-R510AWS.

The u-blox SARA-R510AWS IoT ExpressLink module provides communications over a cellular network anywhere that LTE Cat M1 service is available and presents a simple-to-use AT interface designed to allow resource-constrained microcontrollers to connect to AWS IoT Core.

SARA-R510AWS modules are AWS IoT ExpressLink modules based on u-blox's UBX-R5 cellular chipset, aimed at fast and easy development of secure IoT devices. By bridging the u-blox in-house chipset platform with the market-leading cloud computing services of AWS, this solution provides long-term availability and lifetime support from silicon to cloud. The embedded AWS IoT ExpressLink certified software provides a new tailored AT command set that paves the way to AWS cloud access straight out-of-the-box, which significantly reduces the time-to-market.

SARA-R510AWS modules provide AWS cloud service access without the need for the customer to integrate any additional API on their MCU; every step is handled inside the IoT modules. SARA-R510AWS modules are the perfect fit for new applications requiring reduced time-to-market as well as to renew resource-constrained legacy applications that cannot accommodate the additional code and APIs that are usually required to access AWS cloud services.

See the AWS IoT ExpressLink programmers guide [2] for detailed AT command descriptions .

The following symbols are used to highlight important information in this document:

☞ An index finger points out key information of module integration and performance.

⚠ A warning symbol indicates actions that could negatively impact or damage the module.

2 Application design and development

When designing a host application interfacing with a u-blox cellular module, consider the following points, as depicted in Figure 1:

- Split the application workflow into stages.
- Design the application to work in several modes, reflecting the lifecycle steps of the product.

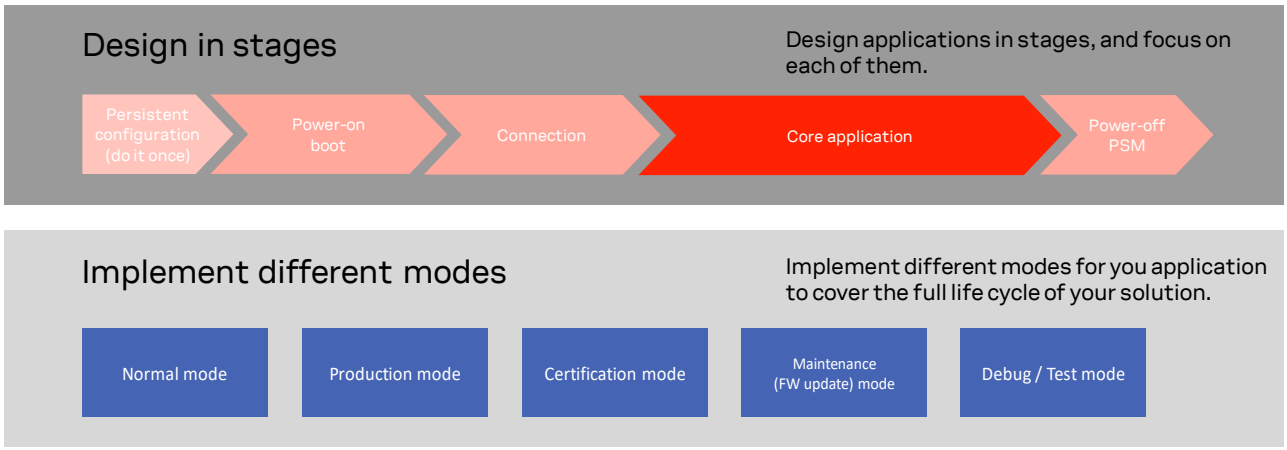


Figure 1: Application design guidelines

2.1 Initial design decisions

Some decisions shall be carefully taken at design stage as any late change could cause much effort to adapt and validate the application. For SARA-R510AWS module, the major decisions are regarding:

- The MNO profile (see section 4) to be used. This depends on the type of application and SIM card, and whether the application is for regional use or global roaming. If the SIM card belongs to an MNO for which the module has gained the type approval, the MNO profile is available in the FW and shall be used.
- Debuggability. This could be provided via test endpoints, access to the USB interface, or a prolific application log of AT commands history including diagnostic information sent by the module.

2.2 Application stages

2.2.1 Power-on

At each boot, the application shall read configurations and make sure they are correct. Module power-on time could be greater than 5 seconds due to the secure element boot time process.

It is important that the application has a robust mechanism to detect when the module is ready to communicate via AT commands at the power on. This is achieved by the host application waiting for a response to the AT command.

☞ At boot, due to security activity, the module could require up to 150 seconds for the **ThingName** or **Certificate** reading.

2.2.2 Power-off

The application can switch off the module by the **AT+SLEEP9** command. Alternatively, use the emergency shutdown described in the SARA-R5 series system integration manual [5].

☞ It is strongly recommended to maintain the **WAKE** pin asserted (low) while the application is issuing the **AT+SLEEP9** command.

3 Local connectivity

3.1 AT interface

AT communication with SARA-R510AWS is possible via the UART interface only without HW flow control. By default, the UART baud rate is set to 115200 bit/s and the formatted AT command string can be up to 9 Kbytes. Thus, the allowed AT command structure is: **AT+[up to 9 kbytes]{EOL}.**

☞ Different from what is reported in the AWS ExpressLink programmer guide [2], on SARA-R510AWS-01B-00, the formatted command string of an AT command can be up to 2 kbytes. Thus, the allowed AT commands structure is: **AT+[up to 2 kbytes]{EOL}**.

3.2 AT commands response parser

It is important that the user implements a dedicated AT parser component in the host application.

Basic guidelines:

- Use the ASCII line feed character (0x0a) or the ASCII carriage return character (0x0d) for EoL.
- Always wait for at least 20 ms for a result code before issue a new AT command.
- When the module has finished processing an AT command, it will output a final result code (either **OK** or **ERROR**) indicating that it is ready to accept a new AT command. The information text responses are issued before the result code.
- Unless otherwise specified, the maximum runtime for every AT command is 120 s to complete and return a response. This timeout is not applicable to some AT commands that are operating on the live network. Those are: **AT**, **AT+CONNECT, AT+SLEEP** and **AT+DIAG CELLS?**.

3.3 UART configuration

- End of line: line feed (i.e., 0x0a, or 0x0d)
- Local echo: yes
- Flow control: none
- Baud rate: 115200
- Bits: 8
- Parity: none
- Stop: 1

For a quick check, turn the cellular module on by pressing the **MODEM PWR_ON** button on the EVK board for around one second. In the terminal window type **AT** and then <return>, the module should answer **OK**.

4 MNO profiles

MNO profiles provide a powerful and flexible method to configure the SARA-R510AWS module to seamlessly work with the SIM of the selected network operator.

Using the MNO profiles, the SARA-R5 module is dynamically configured to use the proper bands. The operator-dependent protocol stack settings must operate on the home network in full compliance with the mobile operator requirements.

With the MNO profiles, customer applications are not required to configure the module using complex and network-dependent parameters but benefit from an out-of-the-box solution that provides seamless connectivity while abstracting complexities of managing individual network configurations.

Use the **AT+DIAG MNOPROF=<mno_id>** command to select a profile for the network operator. The following section provides an example of this command. For a complete list of MNO profiles and their configuration, see Mobile Network Operator profiles appendix on the SARA-R5 series AT commands manual [6] with reference to the SARA-R510S-01B product variant.

4.1 Using MNO profiles

To configure the module to use an MNO profile, first make sure the module is de-registered from the network by issuing the **AT+DISCONNECT** command, then select the profile using the desired <MNO> value and finally software-reset the module. When the module reboots, it will use the parameters specified by the MNO.

☞ The host application shall specify an MNO profile. The default and factory-programmed MNO profile on SARA-R510AWS modules is 90 (global profile).

☞ Reboot the module with **AT+RESET** command to activate the MNO profile.

4.2 Modifiable parameters

The MNO profiles configure the module with a few parameters. The APN parameter can be overridden by the **AT+CONF APN=<apn_name>** command.

If the host application changes this parameter, it will be retained after a module reset; if the MNO profile is re-applied, after reboot the MNO profile specific settings will be restored to the factory-programmed value.

☞ Usually, the APN will be accepted also when in roaming.

For details about the settings applied by different MNO profiles, see MNO profiles appendix in the SARA-R5 series AT commands manual [6] with reference to the SARA-R510S-01B product variant.

4.3 MNO profile setting examples

De-register the module before setting MNO profile, then reboot to apply the setting.

Command	Response	Description
`AT+DISCONNECT`	`OK 0 DISCONNECTED`	De-registration of the module.
`AT+DIAG MNOPROF?`	`90`	Read the module's current MNO profile.
`AT+DIAG MNOPROF=2`	`OK Reboot the device to take effect`	Set MNO profile to AT&T.
`AT+RESET`	`OK` `Rebooting...`	Reset the module. After reboot, the MNO profile 2 settings are applied.

4.4 AT&T profile (+DIAG MNOPROF=2)

SARA-R510AWS in AT&T configuration (+DIAG MNOPROF=2) is factory-programmed with a blank string for the <APN> for default context <cid>=1: as per AT&T requirement, the user must set the custom APN (which might be different for M2M and consumer SIM cards) used for live AT&T network attach via the **AT+CONF APN=<apn_name>** set command. This setting is persistent.

4.5 Verizon profile (+DIAG MNOPROF=3)

Per Verizon requirement, the initial EPS bearer and the EPS bearers used by BIP and LwM2M are defined by default and are aligned to the entries of the VZW APN table.

SARA-R510AWS in Verizon configuration is factory-programmed with a blank string for the <APN> for default context <cid>=1. The proper APN for <cid>=1 (e.g., a static APN related to the UICC subscription) will be assigned by Verizon during the LTE attach and shall be primarily used for user data connectivity. The APN for the other <cid>s can be updated by Verizon via LwM2M provisioning. A brief description of the <cid>s in Verizon configuration is shown in the following table.

<cid> (context id)	Description
1	Initial EPS bearer, it corresponds to the first record of +VZWAPNE.
2	Corresponds to the Class 2 record of the +VZWAPNE and it is used by BIP.
3	Corresponds to the Class 3 record of the +VZWAPNE.
4	Corresponds to the Class 4 record of the +VZWAPNE and it is used for the VZW application PDN.
5, 6, 7	Correspond respectively to the Class 5, Class 6, and Class 7 records of the +VZWAPNE.

4.6 T-Mobile profile (+DIAG MNOPROF=5)

SARA-R510AWS in T-Mobile configuration (+DIAG MNOPROF=5) is factory-programmed with a blank string for the <APN> for default context <cid>=1: as per TMO requirement. The user shall set the APN used for live TMO network attach via the **AT+CONF APN=<apn_name>** set command. This setting is persistent.

AT+DIAG ULWM2MCONFIGBS=<param> command can be used to enable/disable bootstrap from SIM card to LWM2M servers.

<param>	Description
0	Disable bootstrap from SIM
1	Enable bootstrap from SIM

☞ SARA-R510AWS-00B-00 type variants doesn't support T-Mobile MNO profile.

4.7 Regulatory / Conformance profiles (+DIAG MNOPROF=0 / 201)

These MNO profiles shall be used during production or lab tests. When using these profiles, LwM2M is disabled.

From a regulatory perspective, MNO profiles do not affect the low-level RF performance of the module, which are the same regardless of the profile of choice. Some profiles, however, may enable features not available on a simulated network which are known to interfere with laboratory measurements. To reduce unexpected behavior during testing, set **AT+DIAG MNOPROF=0** or **AT+DIAG MNOPROF=201**.

5 Network registration

At power-on the module reads the information in the selected MNO profile to configure which bands to scan, the radio access technology (RAT) to use if more than one supported, and other attach parameters like APN.

The module is programmed to start up in airplane mode, so the **AT+CONNECT** command is required to trigger the network registration. Depends on the current PLMN, during the registration the device can be provisioned with the APN or the APN name must be provided by the host application as part of the persistent settings.

A new SIM can be activated after its first registration on a real network: its "profile" (i.e., the contents of the SIM files) can be remotely provisioned over the air and a registration cycle is triggered at the end of the SIM OTA procedure.

☞ The PIN lock functionality shall be disabled on the SIM card because the current product version does not allow configuring it.

5.1 First time registration setup

It is important to set the operator profile first because this operation will configure the default RAT and band mask. For details of the operator profile, see section 4.

The following example shows how to read and configure the APN.

Command	Response	Description
`AT+CONF? APN`	`OK`	Read the APN current configuration. Response is empty.
`AT+CONF APN=internet`	`OK`	Configure the APN to "internet".
`AT+CONF? APN`	`OK internet`	Read the APN current configuration.

5.2 PAP/CHAP Authentication

☞ This section is not applicable to the SARA-R510AWS-01B-00 type number.

For PAP of CHAP authentication configuration, use the **AT+CONF PDPauthtype=<auth_type>**. If the authentication is required on the initial default bearer, the setting shall be entered before issuing **AT+CONNECT** command.

Command	Response	Description
`AT+CONF PDPauthtype=1`	`OK`	Configure the PDP auth type to "PAP".
`AT+CONF? PDPauthtype`	`OK 1`	Read the current Authentication type.
`AT+CONF PDPusername=ubloxchap`	`OK`	Configure PDPauth username.
`AT+CONF? PDPusername`	`OK ubloxchap`	Read the PDP auth username.
`AT+CONF PDPpassword=ubloxpap123`	`OK`	Configure PDP auth password.
`AT+CONF? PDPpassword`	`OK ubloxpap123`	Read the PDP auth password.

<auth_type> can be one of the following:

- 0 (factory-programmed value): no authentication
- 1: PAP
- 2: CHAP
- 3: automatic selection of authentication type (none/CHAP/PAP)

6 Register SARA-R510AWS with an AWS account

6.1 Set up the AWS account and permissions

Refer to the instructions at Set up your AWS Account to:

- Sign up for an AWS account,
- Create a user and grant permissions,
- Open the AWS IoT console.

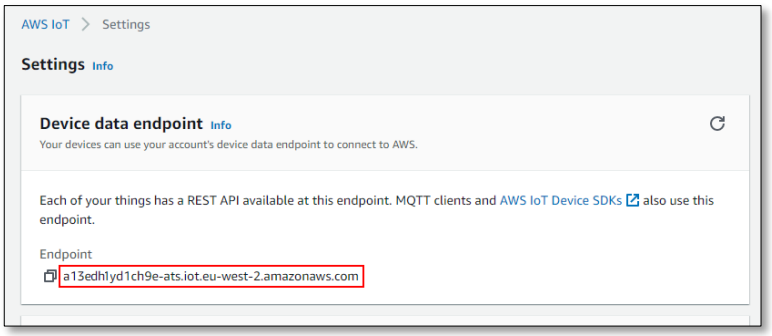
6.2 Setting up the module

Before register a cellular module with your development account for the first time, you must register it with the cellular network. Ensure that:

- A valid SIM card is inserted in the board.
- A cellular antenna is connected to the antenna connector.
- The module is in range of a cellular network that supports LTE-M.
- A serial terminal application is running on the host machine.

Then a "dummy" CONNECT is performed by the following steps:

1. In the AWS IoT Console, in **Settings** (bottom left of the navigation bar) it is reported the account "Endpoint" string from "Device data endpoint".



   Press **MODEM PWR_ON** button on the EVK board for around one second to power the cellular module on. After a short while, type an AT command in your terminal application to ensure the module is responsive.
2. As in the below example, in the terminal application, configure endpoint address with command **AT+CONF Endpoint=<endpoint_string>** then <return>.

⚠ The configuration parameter name **Endpoint** is case sensitive.

Command	Response	Description
`AT+CONF Endpoint=a13edhlydlch9e-ats.iot.eu-west-2.amazonaws.com`	`OK`	Configure the endpoint address provided by AWS.

Before proceed with the first connection attempt, it is advisable to check if the device has been already provisioned (i.e., its certificate has been already generated and downloaded on the device). Check with the **AT+CONF? Certificate pem** command. If the module is already provisioned thus responding to the command, with the internal certificate, the next step can be skipped, continue with section 6.3.

3. In the terminal application, type **AT+CONNECT** and press <return>. This command execution will take a long time and then fail. The expected response is **ERR14 2 UNABLE TO CONNECT Network registration failed**. For further details, refer to **AT+DIAG CEER** in 11.1. Proceed to register device with AWS cloud and then try to connect again.

Command	Response	Description
AT+CONNECT	ERR14 2 UNABLE TO CONNECT Network registration failed.	First connection attempt.

On this first cellular connection the module may take up to 15 minutes to find LTE-M network service. This is because the device, being new to the radio environment, must scan all the global LTE-M RF bands on each detectable cellular network. Connections shall be quicker on subsequent attempts as the module will remember how it gained service.

A data connection to the u-blox security server is required to complete this provisioning procedure. Ensure with the SIM provider that no network restrictions are limiting the data connection.

Among the available ExpressLink Production Onboarding procedures that are documented in the AWS Expresslink programmers guide [2], the SARA-R510AWS ExpressLink product supports only options 2, 3, 4, and 5 that are respectively, end of (assembly) line registration, end of line batch registration, just in time registration, and late-binding.

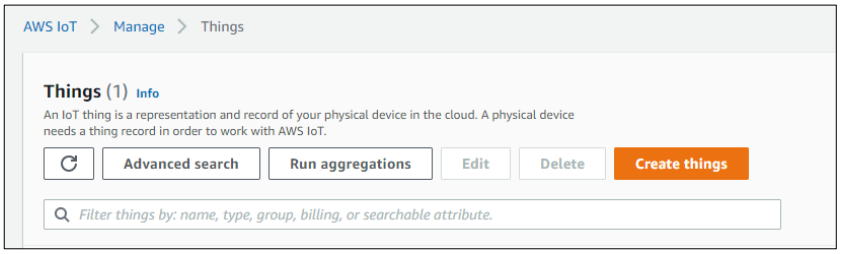
If the module is returning an error response that is different than the one shown above (e.g., just **ERR14 UNABLE TO CONNECT**), then the cellular connection has not been successful. See Section 11 for troubleshooting advice. Moreover, see a list of possible error codes in the AWS Expresslink programmers guide [2].

With these steps completed, the cellular module has successfully connected to the cellular network for the first time and registered with the necessary u-blox servers to create the certificates required to register it with your AWS account in the next steps (after which module returns **OK 1 CONNECTED** back to your **AT+CONNECT** attempts).

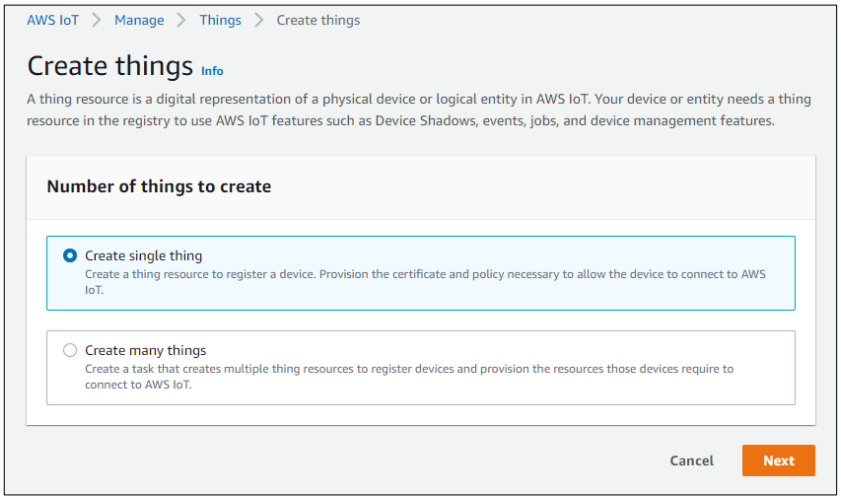
6.3 Registering with your AWS account

To create an IoT Thing and add it to your account, retrieve the u-blox AWS IoT ExpressLink SARA-R510AWS module **ThingName** and its corresponding certificate. Follow the steps below.

1. On the AWS IoT Console select **Manage** then select **Things**.



2. Click **Create things** > **Create single thing** > **Next**.

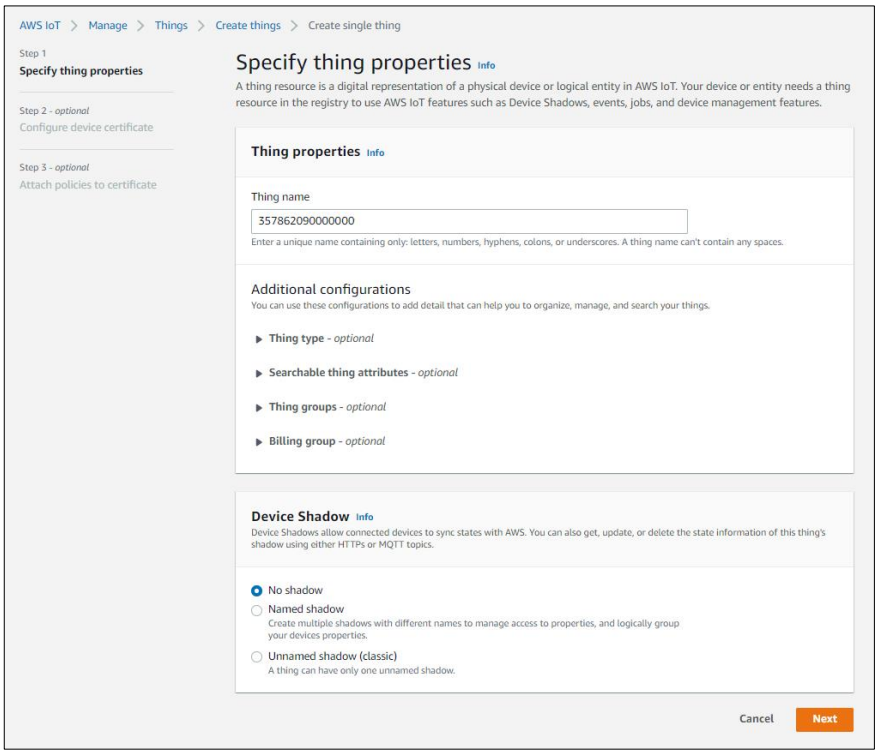


3. With the u-blox AWS IoT ExpressLink SARA-R510AWS module still switched on, in the terminal application type the command **AT+CONF? ThingName** and press <return>.

☞ The configuration parameter name **ThingName** is case sensitive.

Command	Response	Description
`AT+CONF? ThingName`	`OK 357862090000000`	Reading the ThingName current configuration.

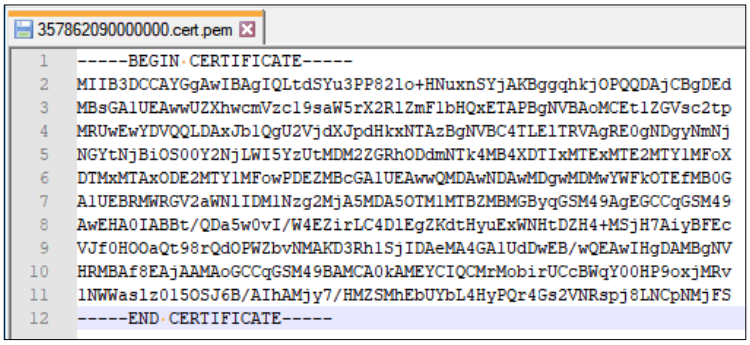
4. Copy the sequence of numeric characters (i.e., the equivalent of “357862090000000” in the image above) from the terminal. On the **Specify thing properties** page, paste the copied string from the terminal into the **Thing name** under **Thing properties** in the console. Leave the other fields as default, then click **Next**.



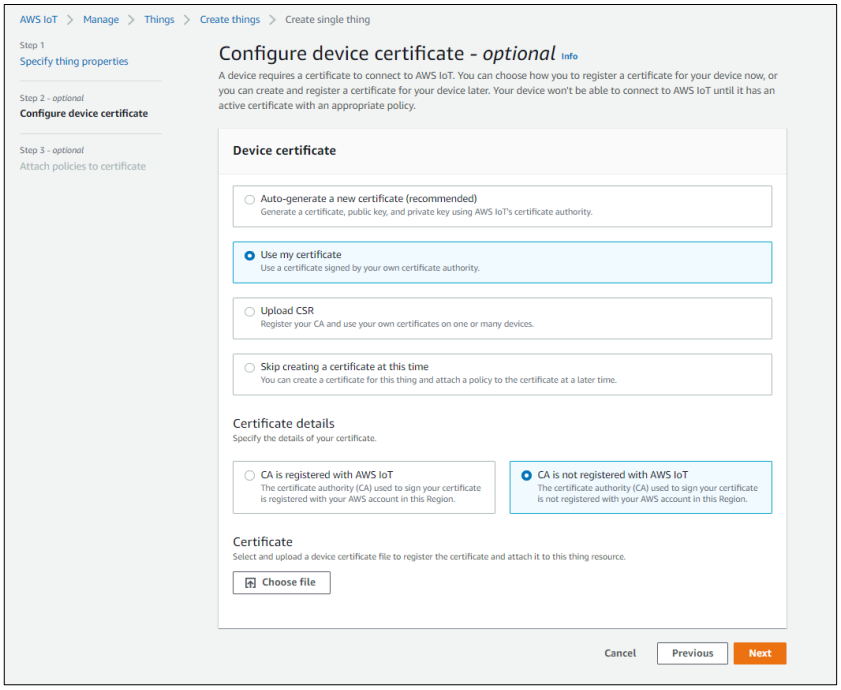
5. In the terminal application type the command **AT+CONF? Certificate pem** and press <return>.

Command	Response	Description
AT+CONF? Certificate pem	OK12 pem -----BEGIN CERTIFICATE----- MIIB3DCCAYgA... jgSubJrIqg0CAwEAAaNCMEAwDwYDQnoZsG 4q5W8LNCpNMjFS -----END CERTIFICATE-----	Read the provisioned certificate.

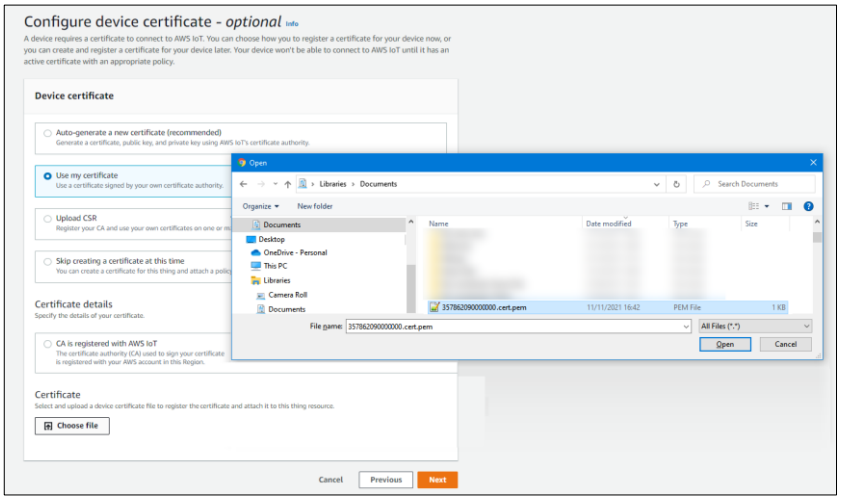
6. Copy the returned string, including **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----** but not including the line beginning with **OK**, into a text file on your host machine named "ThingName.cert.pem".



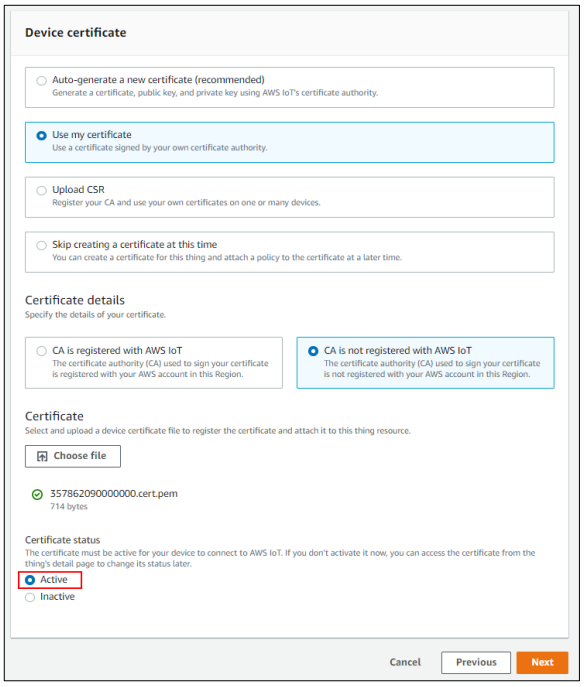
7. On the Configure device certificate page, select **Use my certificate** and choose CA is not registered with AWS IoT.



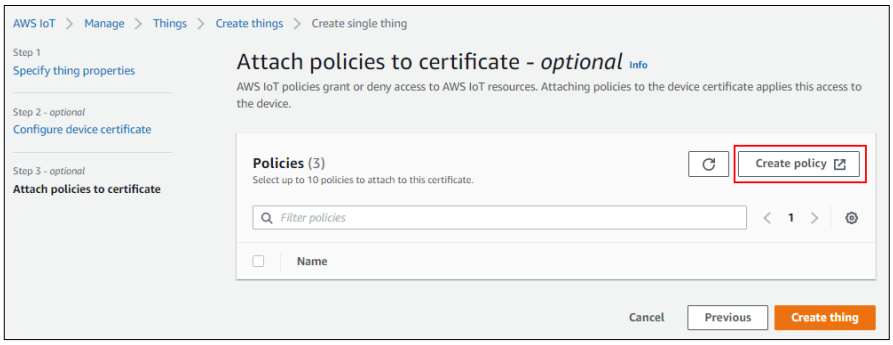
8. Under **Certificate**, select **Choose file** and upload the file "ThingName.cert.pem" from step 6.



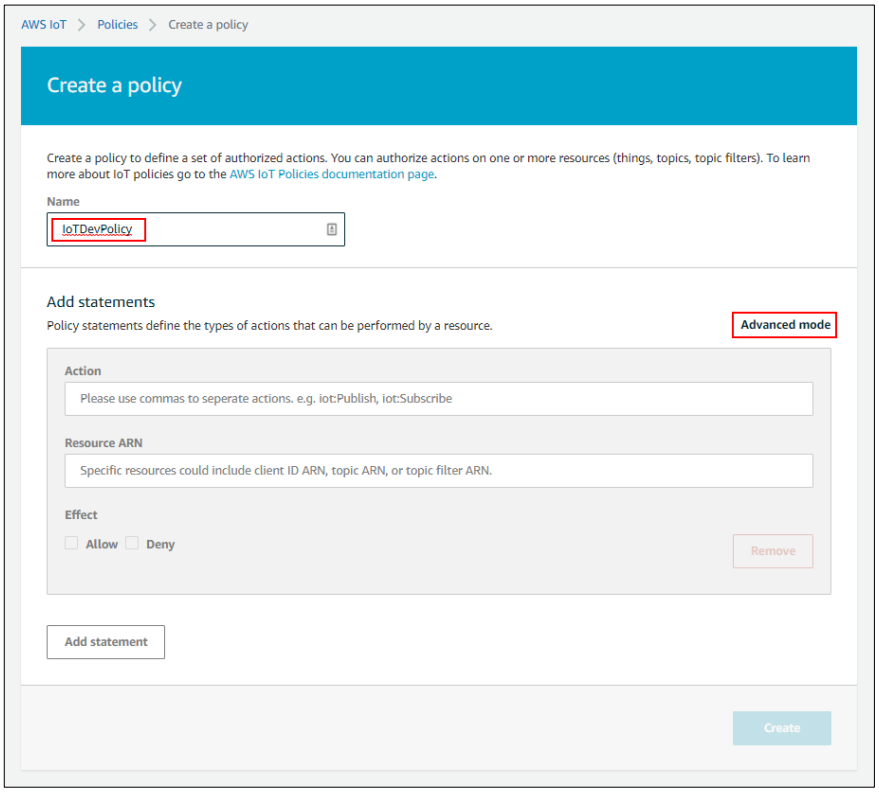
9. Under Certificate status, select **Active** and click **Next**.



10. Click **Create policy** and a new browser tab will open:



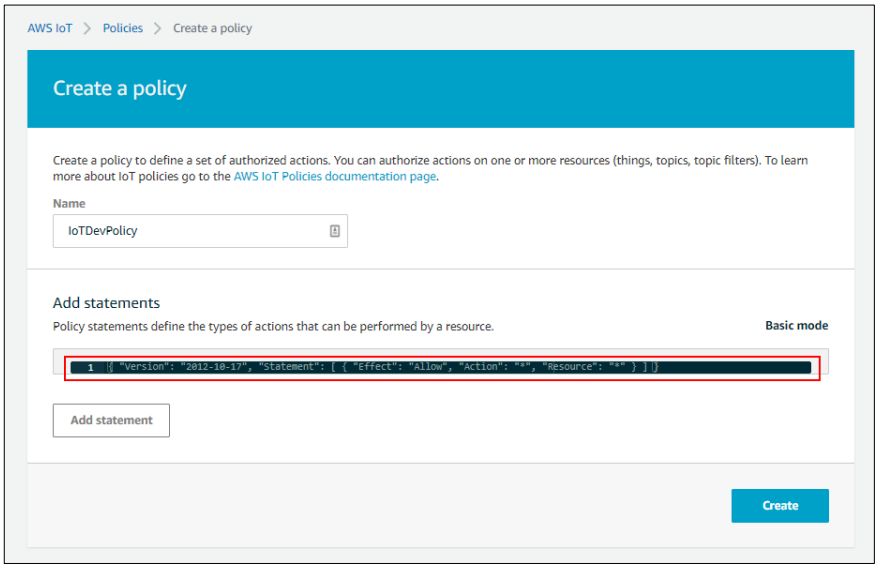
11. Type in a policy name of your choice (e.g., “IoTDevPolicy”) and click **Advanced mode**.



12. Replace the contents of the black console area that appears with the single line of text below:

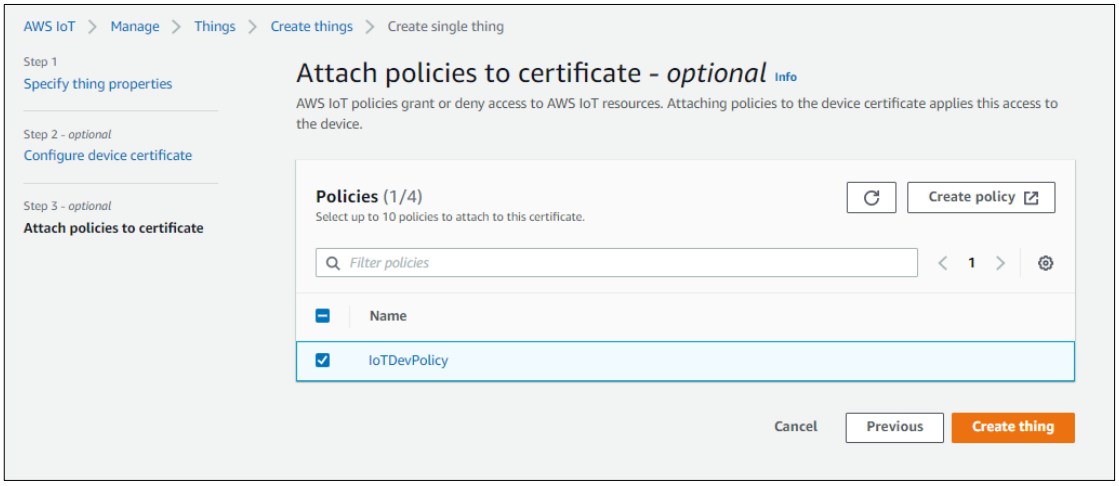
```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "*",
"Resource": "*" } ] }
```

Then click **Create** to create the policy.

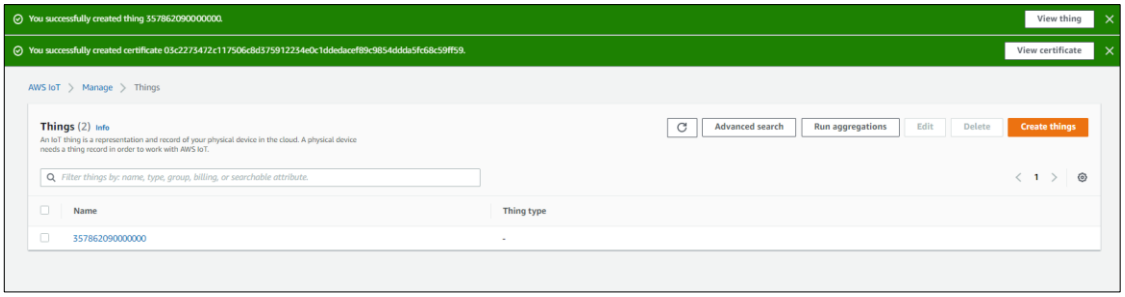


☞ The examples in this document are intended only for development environments. All devices in your fleet must have credentials with privileges that authorize only intended actions on specific resources. The specific permission policies can vary for your use case. Identify the permission policies that best meet your business and security requirements. For more information, see Example IoT Policies and Security Best Practices.

13. Return to the original browser tab, select the policy just created and click **Create thing** to complete your Thing creation.



14. The Thing has been successfully created in the AWS account.



15. Return to the terminal application, type the command **AT+CONNECT** then press <return>. After a short while the module should provide the response **OK 1 CONNECTED**.

Command	Response	Description
AT+CONNECT	OK 1 CONNECTED	Successful connection.

This means that the module is successfully connected to your AWS cloud account.

It is also possible to check the status of the connection with the **AT+CONNECT?** command.

Command	Response	Description
AT+CONNECT?	OK 1 1 CONNECTED CUSTOMER	Check if the application is connected and module registered to the network.

16. To close the connection, type the command **AT+DISCONNECT** in the terminal application and press <return>. After a short while the module should provide the response **OK 0 DISCONNECTED**.

Command	Response	Description
AT+DISCONNECT	OK 0 DISCONNECTED	Successful disconnection.

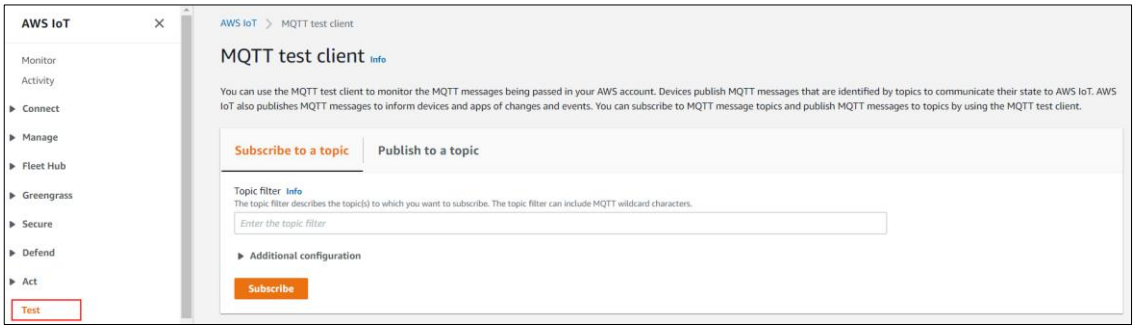
6.4 Completion

The registration of the SARA-R510AWS module as a Thing in the AWS IoT Core account is completed. The procedure is not required for every connection, as the u-blox AWS IoT ExpressLink SARA-R510AWS module will remember its configuration and will be ready to connect to AWS account automatically.

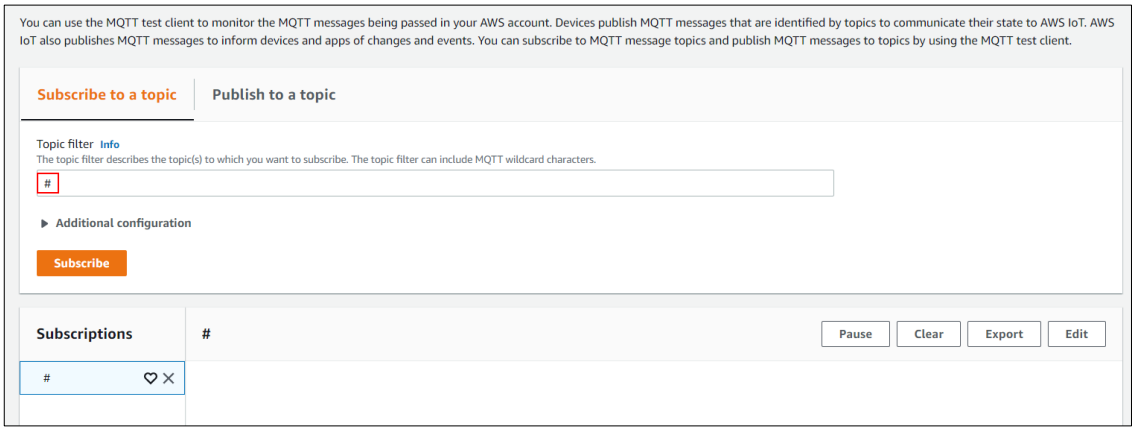
7 Connect to and interact with the AWS cloud

The MQTT client in the AWS IoT console can monitor the communication between SARA-R510AWS module and the AWS Cloud.

1. Navigate to the AWS IoT console and select **Test** from the navigation pane to open the **MQTT test client**.



2. In **Subscribe to a topic**, in **Topic filer**, enter # and click **Subscribe**.



7.1 Connecting

With the u-blox AWS IoT ExpressLink SARA-R5 module switched on, in the terminal application, establish a secure connection by typing the command **AT+CONNECT** and pressing <return>.

After a while, the module should provide the response **OK 1 CONNECTED** as displayed in the example of step 15.

⚠ Some cellular networks will refuse service to a device for a “guard time” (e.g., 1 hour) if the device is seen to connect and disconnect more than a handful of times in quick succession. Therefore, frequent connections/disconnections should be avoided.

7.2 Receiving data and commands from the AWS cloud

To receive messages on the device, in the terminal application type the command **AT+CONF Topic1=/MyTopic** and press <return>.

The module should provide the response **OK**.

Command	Response	Description
`AT+CONF Topic1=/MyTopic`	`OK`	Configuring the name of the first topic.

⚠ The **AT+CONF TopicX** command is NOT persistent across power-cycles of the device.

Next, type the command **AT+SUBSCRIBE1** and press <return>; the module should provide the response **OK**.

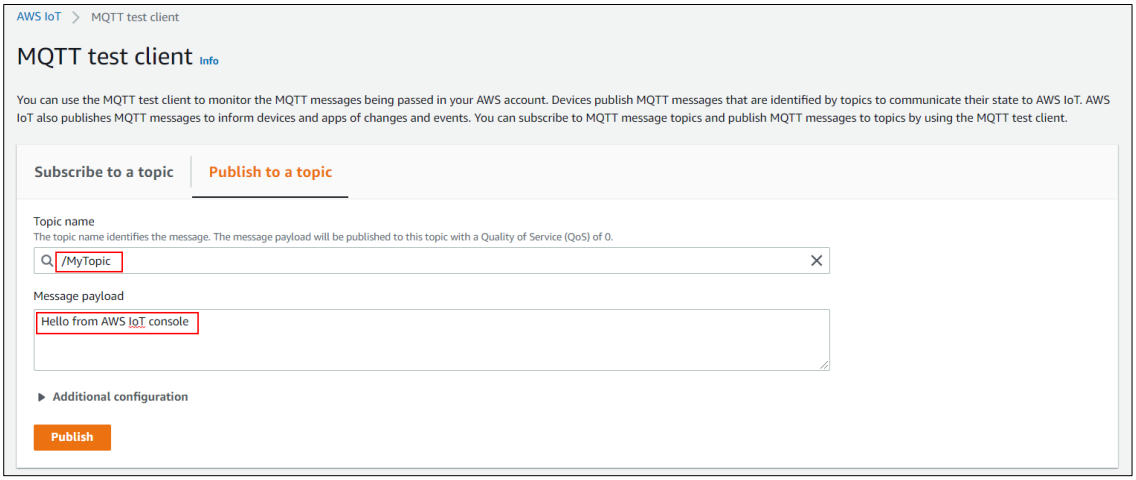
Command	Response	Description
AT+SUBSCRIBE1	OK	Subscribing to the first topic.

⚠ It is mandatory to re-subscribe after an **AT+DISCONNECT** or after powering-down the module.

If the topic subscription is no longer needed, AT+UNSUBSCRIBE# command can be used to unsubscribe from the # topic.

Command	Response	Description
AT+UNSUBSCRIBE1	OK	Unsubscribing to the first topic.

From the AWS IoT console **MQTT test client**, select **Publish to a topic**, type **/MyTopic** into the **Topic name** field (replacing the **#** that was there), under **Message payload** enter **Hello from the AWS IoT console** and then click **Publish**.



Wait for a few seconds for the message to arrive at the device (or monitor the **EVENT** pin) and then, in the terminal application, type the command **AT+GET1** and press <return>.

The module should provide the response **OK Hello from AWS IoT console**.

Command	Response	Description
AT+GET1	OK Hello from AWS IoT console	Retrieving the message from the AWS IoT console.

⚠ Incoming messages greater than 2 kB would be dropped and not delivered to the user application.

☞ The module can buffer a maximum of 50 MQTT messages.

☞ SARA-R510AWS generates SUBACK/ SUBNACK events for all subscription attempts.

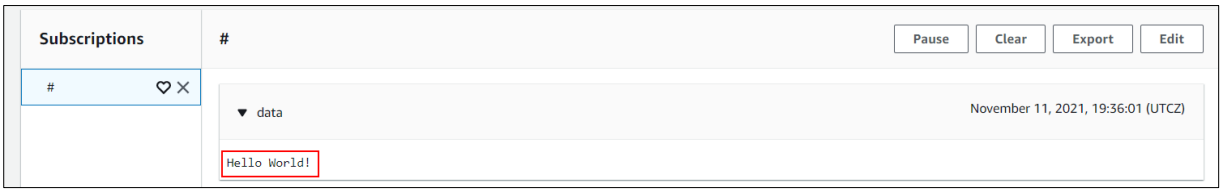
7.3 Sending data to the AWS cloud

To send a “Hello World!” message on a topic provided in the configuration dictionary (e.g., on previously configured **Topic1=/MyTopic**), in the terminal application type the command **AT+SEND1 Hello World!** and press <return>.

After a short while, the module should provide the response **OK**.

Command	Response	Description
AT+SEND1 Hello World!	OK	Successful sent “Hello World!” data to the cloud.

Then it is possible to see the **Hello World!** message appear on the AWS IoT console under the topic **/Mytopic**.



☞ In poor coverage conditions there may be up to a 30 s delay between the message arriving in the AWS IoT console and **OK** being returned in the terminal application.

☞ The maximum size of MQTT messages being sent on SARA-R510AWS-01B-00 is 512 bytes and on SARA-R510AWS-01B-01 is 1024 bytes. Messages greater than these limits are dropped.

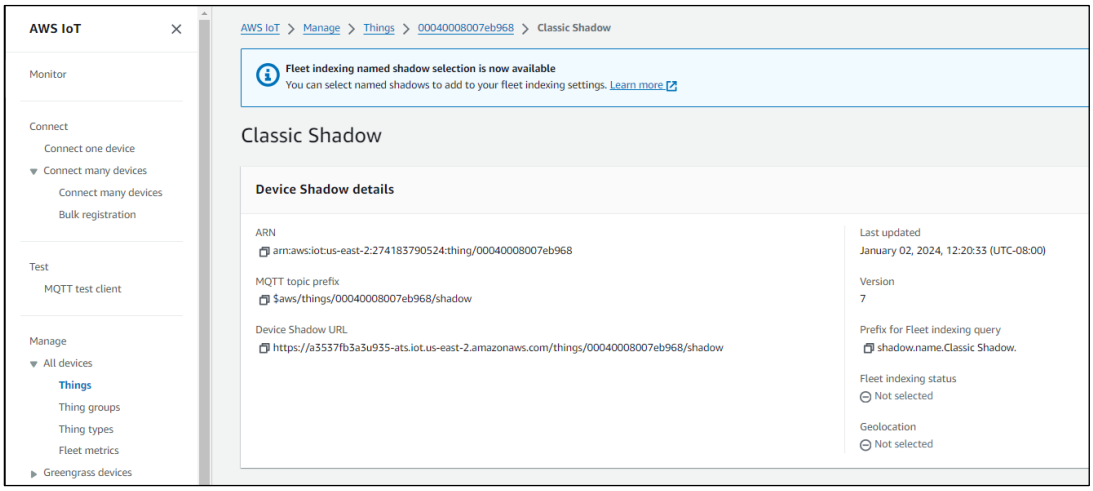
7.4 AWS IoT Device Shadow

☞ This feature is not supported on SARA-R510AWS-01B-00 type numbers.

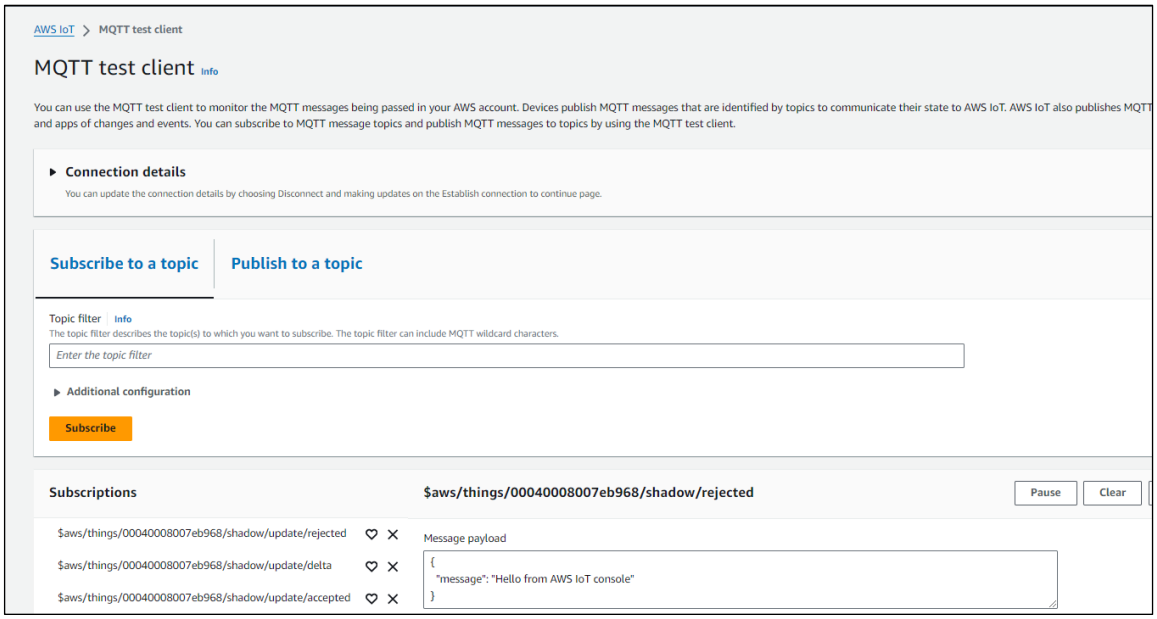
The SARA-R510AWS product supports only 2 named and 1 one unnamed Shadows.

The MQTT Test Client from the shadow details of the thing can be used to monitor the communications between the SARA-R510AWS module and the AWS Cloud.

1. Navigate to AWS IoT console and select “Things” under Manage from navigation pane and select appropriate thing name and select “Classic Shadow” under Device Shadows.



2. Select MQTT topics and click “MQTT test client”.



7.4.1 Enabling Device Shadow feature

With SARA-R510AWS module switched ON and after establishing a secured connection by the **AT+CONNECT** command, use **AT+CONF? EnableShadow** command to check if the feature is enabled. If not, the user must enable it by the following command.

Command	Response	Description
`AT+CONF EnableShadow=1`	`OK`	Successful enabled shadow feature.
`AT+CONF? EnableShadow`	`OK 0`	Reads the status of EnableShadow key. 0: Disable. 1: Enable.

7.4.2 Type of Shadow service

AWS Device Shadow service allow user to create "named" or “unnamed” shadows of each "thing" and assign a state document to each shadow. Named Shadows can be configured using **AT+CONF Shadow#=<shadowname>**.

Command	Response	Description
`AT+CONF Shadow1=testshadow`	`OK`	Mapping Shadow1 to testshadow.
`AT+CONF? Shadow1`	`OK testshadow`	Reading the Shadow1 settings.

☞ Only "named” shadows needs to be configured using above command. “Unnamed” shadows can be used directly without configuring.

7.4.3 Requesting a Device Shadow document

A "Thing" supporting shadow service will be able to keep shadow state document in sync when some change happens locally or through remote actuation. After initializing the shadow service, the state document can be obtained by using **AT+SHADOW# GET DOC** command.

Command	Response	Description
AT+SHADOW# DOC	OK	Send Request to Shadow service to retrieve shadow document for specified named shadow. ☞ If [#] index is missing, the command retrieve the “unnamed” shadow object.
AT+SHADOW# GET DOC	OK 1 {"state":{"desired":{"welcome":"aws-iot"},"reported":{"welcome":"aws-iot"}}	Read the shadow document for specified named shadow.

7.4.4 Shadow document update

Send Request to Shadow service to update shadow document for specified named shadow.

Command	Response	Description
AT+SHADOW# SUBSCRIBE	OK	Send Request to subscribe device Shadow document for selected named Shadow.
AT+SHADOW# UPDATE {"state":{"desired":{"welcome":"aws-iottt"}}}	OK	Send a request to update Shadow document for specified named shadow.
AT+SHADOW# GET UPDATE	OK 1 {“state”:{“desired”:{“welcome”:”aws-iottt”}}}	Read the response of Shadow document update for specified named shadow.
AT+SHADOW# GET DELTA	OK {"version":9,"timestamp":1704309815, "state":{"welcome":"aws-iottt"}	Read the shadow document delta for specified named shadow.

7.4.5 Unsubscribe Shadow Document

Send request to unsubscribe the shadow document.

Command	Response	Description
AT+SHADOW# UNSUBSCRIBE	OK	Send Request to unsubscribe device Shadow document for selected named Shadow.

7.4.6 Delete Device Shadow

Device Shadow can be deleted from the module by sending the **AT+SHADOW# DELETE** command.

Command	Response	Description
AT+SHADOW# DELETE	OK	Send Request to delete device Shadow for selected named Shadow.
AT+SHADOW# GET DELETE	OK 1 {"version":11,"timestamp":1704317822, "clientToken":"ExpressLink"}	Read the response of delete request for specified named shadow.

7.5 Embedded security

☞ All the communication between the ExpressLink modules and the AWS cloud is encrypted during transmission, using TLS 1.2 protocol. However, the serial interface (UART) between the host processor and the module is not encrypted. If sensitive data shall be transmitted to and from the ExpressLink module, and an unauthorized person might gain physical control of the device, we recommend implementing an additional end-to-end message encryption scheme between the host processor and the cloud application.

7.5.1 Security Certificates

There are four certificates in the configuration dictionary as per AWS specifications programmer guide document [2]. However, note that there may be some variations between the specification document and the SARA-R510AWS u-blox product.

Below are the certificates in use, and notes of the SARA-R510AWS implementation of them.

The main ExpressLink certificates are:

- Device certificate (Read only)
- RootCA (Read/Write)
- HOTA certificate (Read/Write)
- OTA certificate (Read/Write)

☞ Device certificate is read-only. A write attempt would result in “ERR12 KEY READONLY”.

☞ On SARA-R510AWS-01B-00 FW the RootCA is read-only. A write attempt would result in “ERR 12 KEY READONLY”.

☞ OTA certificate does not exist in the SARA-R510AWS configuration dictionary. Any read/write attempt would result in “ERR11 UNKNOWN KEY”.

☞ If the HOTA certificate is downloaded into the module using the command **AT+CONF HOTAcertificate=<per_certificate>{eol}**, its validation and authenticity is not checked.

7.5.2 AWS Device Defender

☞ This feature is not supported on SARA-R510AWS-01B-00 type numbers.

The Defender metrics window from the thing details can be used to monitor the device defender metrics between the SARA-R510AWS module and the AWS Cloud.

SARA-R510AWS supports following defender metrics:

Metric	Response type	Description
`Bytes Out`	`Number`	Number of bytes sent in set period.
`Messages Sent`	`Number`	Number of MQTT messages sent in defined Defender period.
`Messages Received`	`Number`	Number of MQTT messages received in defined Defender period.
`Flash Memory Writes`	`Number`	Number of file writes to flash memory in defined defender period.
`Reconnect Events`	`Flag`	Set to true if reconnect has occurred in the Defender period.
`Hard Reset Event`	`0`	This is not supported, hence the return value is set to 0.

7.5.2.1 Enabling Device Defender

On SARA-R510AWS module, use **AT+CONF? DefenderPeriod** command to check if the feature is enabled. If not, the user must enable it by the following command.

Command	Response	Description
AT+CONF? DefenderPeriod	OK 0	Reads the Device defender period. 0: Disable. 60-3600 sec: Enable. ☞ Any value other than 0, 60-3600 will result in ERR4 PARAMETER ERROR.
AT+CONF DefenderPeriod=300	OK 0	Device defender is enabled with 300 seconds of reporting period.

8 Firmware update

☞ Application configurations such as Endpoint address and APN are erased during the FW update procedure. The application must reconfigure them once the update completed.

8.1 FOTA FW update

The FOTA FW update process uses the uFOTA client present inside the SARA-R510AWS paired with the u-blox uFOTA server.

Once the uFOTA campaign is initialized, the connection with the uFOTA u-blox server and the starting of the FW download is a transparent process. The host application will be notified of the FOTA FW update process using OTA query or by monitoring the **EVENT** pin.

The host can enable or disable the uFOTA client by the diagnostic commands listed in below table. Follow the steps below to enable the uFOTA client to register with uFOTA server and download and do a FOTA FW update.

8.1.1 uFOTA configuration and example

Command	Response	Description
AT+DIAG ULWM2M=0	OK	Enable the LwM2M client used for uFOTA update.
AT+DIAG ULWM2MCONFIGEXT	OK	Configure the LWM2M client.
AT+DIAG ULWM2MCONFIG_ENABLE=<server_id>	OK	Configure and enable the connection parameters for LwM2M server (normally id is 721). ☞ The configuration needs to be done before sending any registration request to uFOTA server.
AT+RESET	OK	Reboot the module to save the above configuration.
AT+CONNECT	OK	Register the module to the network. Now the device should automatically connect with the uFOTA server.
AT+DIAG ULWM2MREG=721	OK	Alternatively, this command can be used to force the LwM2M client registration with the u-blox uFOTA server.
AT+OTA?	OK 3	Once the download is started, the status can be checked with the OTA query command which will return OTA code: 3 (OTA in progress) The device will automatically reboot once the download is finished to perform FW integrity checks.
		If FOTA FW integrity checks pass, FW installation progress will be displayed by the +UUFWINSTALL URC's. ☞ If the FOTA FW integrity check fails, the device reboots itself and reverts to the previous FW version. Upon installation completion, the device will reboot and modem AWS AT interface will be available.
AT+CONF? Version	OK 83.16,A80.01,7686996	Check if the version has changed.
AT+CONNECT	OK	Register the module to the network, so it can report the success/failure of the uFOTA process to the uFOTA server.

8.2 EasyFlash

EasyFlash is a Windows-based application that flashes SARA-R510AWS modules via the primary UART interface. See EasyFlash use in SARA-R5 FW update application note [7].

8.3 FOAT FW update

The AT+OTW command triggers the firmware download using the Xmodem or Xmodem-1k protocol. Once downloaded the FOAT update file (.upd) via Xmodem protocol, the installation procedure starts.

After the download ends, the +UFWPREVAL URCs display the progress indication for the update file validation. The progression of the validation is incremental, but the increment can be different. The +UFWPREVAL: 100 URC may not be issued, and the module can start the installation phase issuing the +UFWUPD URC.

After the end of the update file validation:

- If the validation failed, the procedure will be suspended and a FOAT error code will be issued together with the +UFWUPD URC. The module exits from the update procedure mode and returns to the normal mode since the firmware is unchanged and usable.
- If the validation succeeded, the firmware installation procedure will start, notified by the +UFWUPD URCs.

During the update operations, the +UFWUPD URCs display the progress indication and the operation result on the serial interface set via the +UFWUPD AT command. The installation is incremental, but the increment can be different from 1.

Command	Response	Description
`AT+DIAG Version?`	`OK 83.21,A80.01,6a51c5d`	Returns current FW version of the device.
`AT+OTW`	`+UFWUPD: ONGOING`	Preparing to download the FW update file using Xmodem transfer protocol.
	`OK`	Device responds with OK after downloading the update file.

	`+UFWPREVAL: 0`
	`+UFWPREVAL: 10`
	…
	`+UFWPREVAL: 100`
	`+UFWUPD: 1`
	`+UFWUPD: 12`
	…
	`+UFWUPD: 98`
	`+UFWUPD: 100`
	`+UFWUPD: 128`
		FW update file validation started.
		
		FW update file validation completed.
		FW installation started.
		
		128 indicate FW installation completed successfully.
		
		☞ The last URC with a value greater than 100 indicates the update operation result (e.g., 128 means operation completed with success (for more details see the FOAT error result codes in [6]).

☞ SARA-R510AWS will not exit the OTW mode unless a complete file transfer and firmware installation is completed successfully. Resetting the module will not exit the XMODEM mode.

☞ The module will only recover to boot the AWS Application when the valid package is transferred and installed. SARA-R5 will remain in XMODEM mode and will keep expecting a valid package to be transferred again if the installation is failed.

9 Host OTA FW update

The HOST OTA FW update process uses the AWS IoT console to transfer the HOST FW update file to the SARA-R510AWS module. Not only the host OTA FW update file but also the AWS IoT console can be used to transfer and update the Host OTA certificate file present in the configuration dictionary of SARA-R510AWS.

The following “Reserved OTA file type codes” can be selected when starting a Job in the AWS IoT console.

Code	Description
202	Host Update
204	Host OTA certificate update

9.1 Host OTA example

The table below shows how to download the host update file or Host OTA certificate update file:

Command	Response	Description
`AT+CONNECT`	`OK`	Register the module to the network.
		Start a “job” on the AWS IoT cloud.
`AT+OTA?`	`OK 2 <filename>`	Check status using OTA query command. If a valid job document is received from AWS IoT cloud, OTA query command will return OTA code: 2 (meaning that a host OTA update is being proposed) thus showing the filename of the host OTA update filename which is received directly from AWS IoT cloud. Also the EVENT pin can be monitored to see if a job document is received.

`AT+OTA ACCEPT`	`OK`	Accept the proposed OTA job. The download of Host OTA update file will be started.
		After that:
		☞ OTA query command will return OTA code: 3 (OTA in progress).
		Once the download completed, integrity and signature validation are performed. Depending on the OTA file type used in the “job” document, SARA-R510AWS may act differently.
		• If OTA file type is 202 (Host OTA FW update file)
		  • If signature validation failed, OTA query command will return OTA code: 0 (No OTA in progress). Job status is reported as failed.
		  • If signature validation passed, OTA query command will return OTA code: 5 (A new host image has arrived).
		• If OTA file type is 204 (Host OTA certificate update file), the signature validation is performed only if there is HOTA certificate present in the configuration dictionary.
		  • If signature validation passed, Host OTA certificate update file is updated in the HOTA certificate present in the configuration dictionary.
		  • If signature validation failed, OTA query command will return OTA code: 0 (No OTA in progress).

`AT+OTA READ <num_of_bytes>`	`OK <num_of_read_bytes> <actual_data> <checksum>`	Host application can read chunks of download update file. Refer to Section 9.2.4 of AWS IoE ExpressLink programmers guide [2] for further details.
`AT+OTA SEEK <byte_address>`	`OK <byte_address>`	The host application can provide a seek offset from where to start reading the downloaded HOTA update file. Refer to the Section 9.2.5 of AWS IoE ExpressLink programmers guide [2] for further details.

Command	Response	Description
AT+OTA CLOSE	OK	Mark the job as success.
AT+OTA FLUSH	OK	Reject the proposed OTA job. A job status rejected will be reported to the AWS IoT console, while the errors will be reported using events. Eventually, it can be checked using the EVENT query command. Refer to the Section 8.2.1 of AWS IoE ExpressLink programmers guide [2] for further details.
AT+OTA?	OK 0	Query status. The OTA query command will return OTA code: 0 (which means that no OTA in progress).

10 Low-power and SLEEP modes

There are two low-power/sleep modes supported:

- **Mode 0**: Normal sleep (**AT+SLEEP0** command)
  It is called 32 kHz/UART sleep mode with cellular radio switched off. The module's state information (RAM data, configs) is retained. The module can be waked up:
  - Automatically based on the expiry of set time duration (e.g., with the **AT+SLEEP [duration]** command), or
  - By issuing an AT command, or
  - via GPIO pin (**WAKE** pin)

  This is equivalent to "AT+UPSV: 1" to allow the modem to go into sleep; and upon wake up the application autonomously set it up to "AT+UPSV: 0" to restrict the device to go into sleep again.
- **Mode 1**: Deep sleep (**AT+SLEEP1** command)
  The module is kept switched off in this mode. The module's state information is lost. The module can be waked up using the **POWER** pin (Normal Power ON procedure).

☞ On SARA-R510AWS-01B-00 product variant, **AT+SLEEP9** command is used for entering the Deep sleep.

☞ All higher SLEEP modes specified by user via **AT+SLEEP2** to **AT+SLEEP9** would be treated as **AT+SLEEP1** as per AWS Specifications.

☞ In SLEEP **Mode 0**, some initial characters on UART shall be lost when the device is waked up by AT because 115,200 (at a sensible sampling frequency) is not a multiple of the 32 kHz clock, at least not one that is within the tolerance of the UART specifications, hence the main clock has to be started when an edge is detected on the TXD line and that takes a finite amount of time.

☞ On the SARA-R510AWS-01B-01 product variant, in normal SLEEP **Mode 0**, the module cannot be waked up by using the WAKE pin or by expiry of the specified time duration if the duration is less than 6 seconds.

☞ In SLEEP **Mode 1**, "automatic wake-up of device upon user specified duration expiry" is not supported because all clocks are off in deep sleep mode.

☞ There is no use of eDRX and PSM features in this product. The module only connects to cellular network and the cloud only upon **AT+CONNECT** user command and disconnects from both upon **AT+DISCONNECT** command.

11 Troubleshooting

It is recommended to track the module status in the host application. Such diagnostic information helps to detect specific scenarios and implement proper handling in the host application.

11.1 Diagnostic commands

The SARA-R510AWS product implements some additional AT commands for diagnostic purpose.

These commands are only implemented on the SARA-R510AWS product. Therefore, they are not mentioned in the AWS ExpressLink programmer guide [2] and only available in the SARA-R510AWS product documentation.

The syntax used for these diagnostic commands is **AT+DIAG {command}{eol}**. The following table reports all the available diagnostic commands:

Command	Response	Description[1]
AT+DIAG CELLS?	OK "vodafone IT","22210","CAT-M1"	Calls the AT+COPS=? to retrieve the list of available cells. A “not connected to the network” error is returned if the SARA-R510AWS module is not registered to the network.
AT+DIAG CEREG?	OK 5,327,"CAT-M1"	Calls the AT+CEREG? command to retrieve the network status.
AT+DIAG COPS?	OK "vodafone IT",222,10	Calls the AT+COPS? command to retrieve information about the network with which device is connected.
AT+DIAG CESQ?	OK -114,-10	Calls the AT+CESQ? command to retrieve the information about the network quality.
AT+DIAG Version?	OK 83.16,A80.01,7686996	Gets the firmware version (if available), and the application version.
AT+DIAG CEER	OK EMM cause,0,No cause information available	Calls the AT+CEER command to retrieve information about the last network rejection cause.
AT+DIAG NetworkBackoffTimer	OK Remaining duration:0	The information regarding the NAS BACKOFF TIMERS is returned. ☞ The command is not supported on SARA-R510AWS-01B-00 type number.

☞ Except for the **AT+DIAG Version?** command, all the other commands above may return an empty response (e.g., OK 0,0 or OK “”,0,0) if the SARA-R510AWS module is not registered (i.e., CONNECTED) to the network.

11.2 Unable to connect errors

In case of impossibility to perform a connection after the **AT+CONNECT** command, the module is reporting the message**: ERR14 {#hint} UNABLE TO CONNECT** followed by the field **[detail]**.

On the SARA-R510AWS product the possible causes of error are the following:

{#hint}	[detail]	Error description
2	Check SIM card	
2	Network registration failed. For further details, refer to AT+DIAG CEER	

[1] Additional details about the legacy AT commands reported in all the description can be found in the SARA-R5 series AT commands manual [6] with reference to the SARA-R510S-01B product variant.

{#hint}	[detail]	Error description
1	Backoff algorithm imposed delay	
2	Registered, no IP address from network	
3	ThingName is not configured	
3	Endpoint is not valid	
3	MQTT client setup failed	
4	MQTTER #<n>	Where <n> is the MQTT Error Code defined in the SARA-R5 series AT commands manual [6].

See ddditional details on the **{#hint}** parameters in the AWS IoT ExpressLink programmers guide [2].

11.3 Other troubleshooting actions

Problem	Action
Not see anything in the terminal application when type in it.	The AWS IoT ExpressLink specification does not include echoing of received characters, which is normal for a machine-oriented interface. When typing in commands manually, set “local echo” on in the terminal application to see the messages exchanged.
No response is received to any AT commands typed in the terminal application.	Make sure that the baud rate of the terminal application is set to 115200 bit/s and that AT commands are formed exactly as defined in the AWS IoT ExpressLink programmers guide [2].
The AT command **CONNECT** does not work.	Make sure that the SIM card is inserted in the board, an antenna is connected, and the module is within range of a cellular network that provides LTE-M coverage. Double check that the registration procedure of section 5 and 6 have been correctly followed, including registering of the device in the AWS account; the connection is to the endpoint of the device in that account (not just the cellular network) and so it cannot succeed until all of the registration steps have been completed. If **CONNECT** worked in the past but is now failing in the same location and after using the device for some while, it may be that the cellular network has decided to refuse service for a “guard time” (e.g. 1 hour) because the device has connected and disconnected more than a handful of times in quick succession. The only way to avoid this is avoiding many connections/disconnections).
The AT command **SEND#** returns **OK** even when I have disconnected the cellular antenna and so I am sending a message not in coverage.	Messages are queued until it is possible to send them. Once the cellular module is reconnected messages will be successfully published.
Setting a topic with the AT command **CONF TopicX** (where **X** is 1 to 16) returns an error.	While a topic is subscribed-to it cannot be modified; use the command **AT+UNSUBSCRIBE#** to unsubscribe from topic **#** before modifying it.
The AT commands **CONFMODE**, and **WHERE** do not work.	These AT commands are not supported in the SARA-R510AWS product.
Some parameters to the **CONF** command do not work.	Only parameters that are relevant to a cellular device are supported; see Section 12 for a full list.
The AT command **TIME?** does not work.	The module must be connected to the cellular network to obtain the time. If the problem happens when the module is connected, then it is possible that the cellular network in use does not support reporting of time to the mobile terminal (the feature is optional in the network).
Some downlink messages from the server are going missing.	Make sure that no downlink message exceeds 2048 bytes in size.

12 Features supported

The firmware provided on the u-blox SARA-R510AWS module does NOT support all the features of the AWS IoT ExpressLink command set. The following commands are supported:

CONNECT, **DISCONNECT**, **SLEEP**, **RESET**, **FACTORY_RESET**, **SEND#**[2], **GET**[3], **SUBSCRIBE**, **UNSUBSCRIBE**, **CONF**, **EVENT**, **DIAG**, **TIME, OTA, CONNECT!, OTW, GPIO, SHADOW, DEFENDER**.

Different from what is reported in the AWS ExpressLink programmer guide [2], on SARA-R510AWS devices, the following commands are not supported:

CONFMODE, BLE, Certificate Rotation, TopicRoot, SSID, Parse phrase, OTA certificate, WHERE.

☞ Besides the above features, SARA-R510AWS-01B-00 FW version do not support: **OTW.**

☞ OTA of the module is supported but only through u-blox uFOTA since it must work within the constraints applied by the cellular network operators. Therefore, in case of module OTA, all the OTA commands are not supported expect for the **AT+OTA?**

In SARA-R510AWS product, for the **CONF** command, only the following parameters are supported:

About, **Version**, **ThingName**, **Certificate**, **Endpoint**, **APN**, **Topic#** (where # can be an integer from 1 to 16, i.e., the maximum number of topics is 16).

☞ The power-on behavior of the module is defined by the underlying SARA-R5 HW, i.e. the module does not power on until the **PWR_ON** pin is asserted for 1 s and then released, see the SARA-R510AWS series data sheet [4] for more details; the pin MUST be released as if it is held for more than 16 s an emergency restart of the module will be performed. The **PWR_ON** pin is a toggle, i.e., if it is asserted for 1 s and then released while the module is powered on then the module will power off again. It is recommended to power the module off in this way before physically removing power.

☞ The behavior of the **RST** pin described in the AWS ExpressLink documentation is offered by the **RESET_N** pin of the module.

☞ The event queue depth is 10 events. This indicates that a maximum of 10 events can be stored or buffered by the SARA-R510AWS module at any given time. If the user does not read the events right away, they will be dropped.

[2] The maximum size of MQTT message being sent on SARA-R510AWS-01B-00 release is 512 bytes while on SARA-R510AWS-01B-01 release is 1024 bytes.
[3] The maximum message size that can be received is 2048 bytes.

Appendix

A LPWA technology overview

SARA-R510AWS module supports LTE Cat M1 low-power wide-area (LPWA) technology.

Key applications using LPWA include:

- Automotive and transportation
- Smart metering
- Smart cities
- Smart buildings
- Connected health
- Agricultural and environmental

LTE Cat M1 is a LPWA air interface that allows the connection to IoT and M2M devices with medium data rate requirements. It enables longer battery lifecycles thanks to enhanced power saving mode and extended in-building range (up to 15 dBm more than LTE, thanks to the repetitions of transmissions provided in the coverage enhancement modes), as compared to standard cellular technologies such as 2G, 3G, or LTE Cat 1.

LTE Cat M1 is part of the same 3GPP Release 13 standard that also defines Narrowband IoT (NB-IoT or LTE Cat NB1) - both are LPWA technologies in the licensed spectrum. With uplink speeds of 375 kbit/s, which can reach 1 Mbit/s on some networks thanks to protocol stack enhancements, and downlink speeds of 375 kbit/s in half duplex mode, LTE Cat M1 specifically supports IoT applications with low to medium data rate needs. At these speeds, LTE Cat M1 can deliver remote firmware updates over-the-air (uFOTA, with access to MNOs and u-blox servers via the LwM2M protocol) within reasonable timeframes, making it well-suited for critical applications running on devices that may be deployed in the field for extended periods of time.

Battery life of up to 10 years on a single charge in some use cases also contributes to lower maintenance costs for deployed devices, even in locations where end devices may not be connected directly to the power grid.

The LTE Cat M1 standard specifies connected mode mobility, which SARA-R5 supports through inter-frequency and intra-frequency handover capability, resulting in higher reliability of transmissions, particularly important in non-static usage.

B Glossary

Abbreviation	Definition
APN	Access Point Name
AWS	Amazon Web Services
EoL	End of Line
LPWA	Low-Power Wide-Area
MNO	Mobile Network Operator

Related documentation

[1] AWS IoT ExpressLink website
[2] AWS IoT ExpressLink programmers guide v1.2
[3] AWS IoT ExpressLink example code
[4] u-blox SARA-R510AWS series data sheet, UBX-22016999
[5] u-blox SARA-R5 series system integration manual, UBX-19041356
[6] u-blox SARA-R5 series AT commands manual, UBX-19047455
[7] u-blox SARA-R5 series FW update application note, UBX-20033314
[8] u-blox EVK-R5 user guide, UBX-19042592

☞ For product change notifications and regular updates of u-blox documentation, register on our website, www.u-blox.com.

Revision history

Revision	Date	Name	Comments
R01	28-Jul-2022	mreb	Initial release.
R02	30-Nov-2022	mreb	Updated document with functionalities of the Engineering Sample release.
R03	12-Apr-2023	mreb	Updated document with functionalities of the Initial Production release.
R04	05-Feb-2024	aayy	Extended document applicability to SARA-R510AWS-01B-01.
R05	12-Jul-2024	aayy	Updated the document with Device Defender details.
R06	19-Sep-2024	aayy	Added the FOAT FW update feature.

Contact

u-blox AG

Address: Zürcherstrasse 68
8800 Thalwil
Switzerland

For further support and contact information, visit us at www.u-blox.com/support.