RYZ014

Firmware Over-the-Air Upgrade

Contents

1. Introduction

This document details the FOTA mechanisms supported on RYZ014. It is also possible to perform local firmware upgrade using the UART connection. See the Software Upgrade Procedure application note for more details.

2. Definitions

Term	Description
FOTA	Firmware (Update) Over The Air
OPBL	OTP Primary Boot Loader
FPBL	Flash Primary Boot Loader
PSI	Platform Specific Information
mTools	Manufacturing tool: specific firmware image embedding manufacturing functions
FFF	Firmware From Flash
FFH	Firmware from Host – allows loading a firmware file via UART
Updater	Independent firmware used for update process
DUP	Device Upgrade Package
SBL	Secondary bootloader

3. FOTA Overview

The FOTA service stems from the requirement to allow reliable remote upgrades of cellular modems used in widely deployed consumer devices, throughout their lifetime.

This mandatory feature must be provided in all countries where the cellular module operates.

FOTA is required in the following cases :

1. Critical network update that requires a modem preliminary upgrade – Operator driven
2. Software update – Business and customer quality driven:
   - Security patch
   - Software ‘bugfix’ or evolution
   - Beta testers software update during product early qualification prior to commercial launch

There are two possible ways to trigger a FOTA on RYZ014 module:

- With the proprietary AT command, AT+SQNSUPGRADE. In this mode, the FOTA happens at the device’s initiative. The software image is hosted on the customer’s server. Please refer to the ***AT Commands Use Cases*** document for more information.
- Using an AVSystem solution to trigger FOTA on LwM2M. In this mode, the network schedules the FOTA. Renesas provides for the device to download and install the new software image.

4. FOTA on LwM2M

4.1 Architecture

Four main actors take part in the FOTA process:

- The modem provider (Renesas)
- The device maker (ODM)
- The end-product operator (OEM)
- The FOTA service provider (AVSystem)

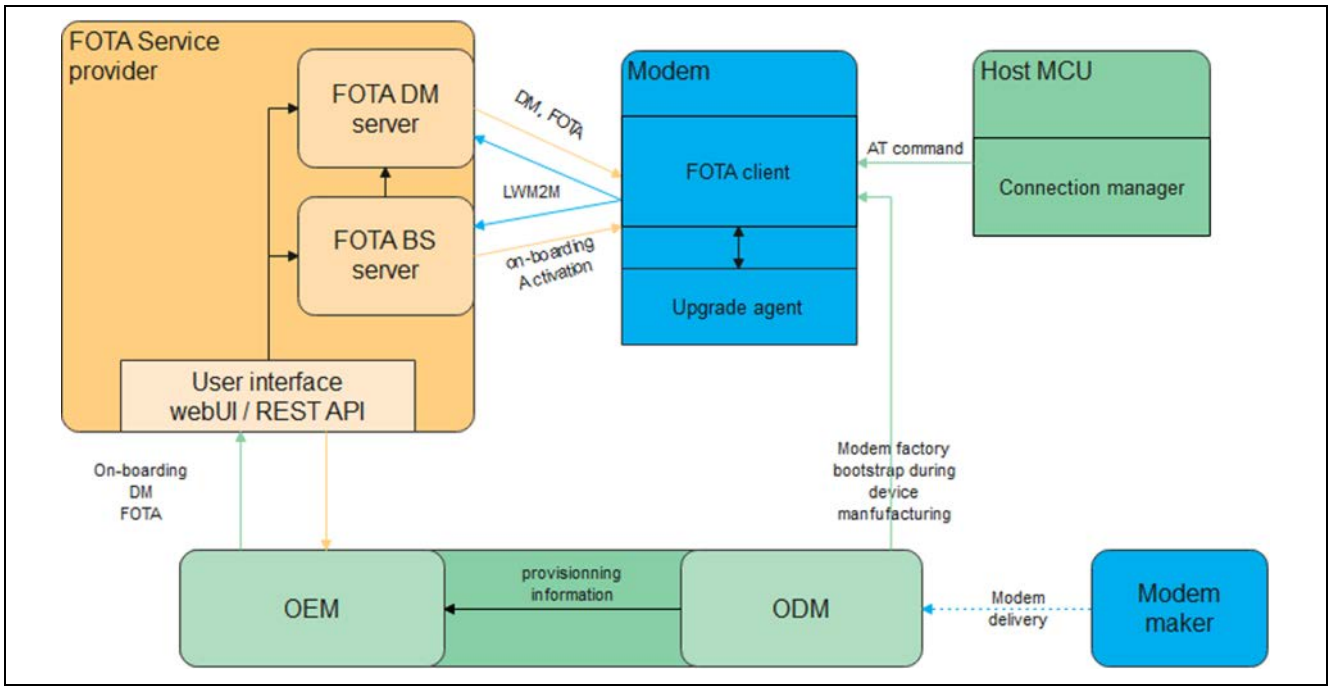

Figure 1. FOTA Process

The OEM is responsible for performing modem provisioning during end-device manufacturing (see section 10) and for 'on-board' modem information to FOTA service provider (see). The OEM also qualifies and approves the updated software and launches the FOTA operation.

The FOTA service provider must setup a FOTA server available 24/7 and always reachable by a large amount of FOTA clients.

4.2 Overview

To perform a FOTA on LwM2M:

- During the manufacturing stage:
  - Configure the LwM2M bootstrap server settings on the device (see section 4.3.1)
  - Add the device to the inventory on the AVSystem bootstrap server (see section 4.3.2)
  - Register the device to the server (see section 4.3.3)
- Manage the client on the server, that is, schedule an upgrade (see section 4.4)
- Execute the FOTA procedure (see section 4.5)

4.3 FOTA Activation During Manufacturing

To use FOTA on LwM2M feature, the LwM2M client must be registered at the *Coiote IoT Device Management* portal and provisioned with the *AVSystem* by its Bootstrap URI. Please refer to the Coiote website for more detail information. The activation of the FOTA service on a specific device follows a specific process detailed in the following figure.

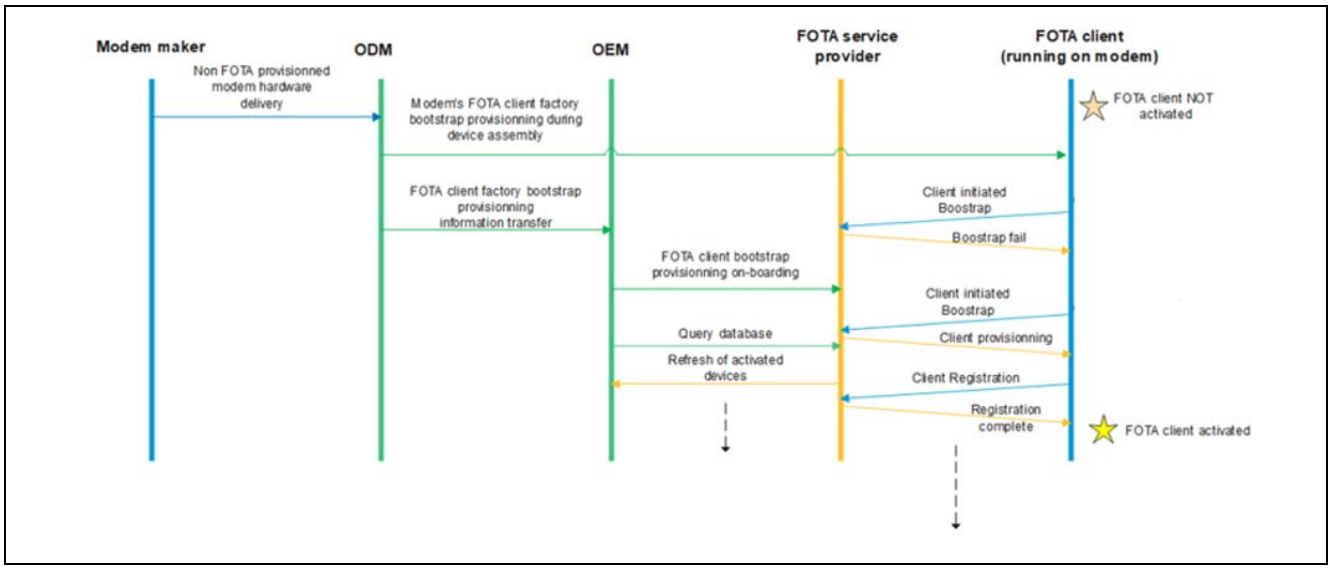

Figure 2. FOTA Service Process on a Specific Device

4.3.1 Start the LwM2M Client on the Module

The FOTA client on each module must be provided the following information:

- The endpoint URI:
  - For example, coaps://eu.iot.avsystem.cloud:5694
- The PSK key identity:
  - This field must be written as `urn:imei:<IMEI>` where `<IMEI>` is the IMEI of the module (output by the command `AT+CGSN`).
- The PSK secret:
  - Must be a random/unique 32-byte (256-bit) key written in hexadecimal encoding.
  - See the section 4.3.1.1 Key Generation below for more details

The module must also be registered with the LwM2M server before being shipped (see section 4.3.2, Adding the Device to the Inventory and section 4.3.3, Register the Device). Please double check for all parameters correctness.

4.3.1.1 Key Generation

To generate a strong, 32-byte, base64 encoded, pre-shared secret, either:

- Use the `openssl` command line utility provided in the OpenSSL software distribution. Use a *Xterm* under *Linux*™, *Terminal* under *MacOS*™, or *PowerShell* under *Windows*™:

```
> openssl rand -hex 32

e9891e446e07ba10519059db4ad9eb1b02c83d08dd80102982c27ec9e1bdebde
```

  This command outputs a 32-byte pre-shared secret encoded using *base64*.

- Use the `psktool` utility provided with the *GNUTLS* suite. This command requires a username (prepended to the generated key) and a filename to write the key into:

```
> psktool -u DV0 -p pskfile.txt -s 32

Generating a random key for user ‘DV0'

Key stored to pskfile.txt

> more pskfile.txt

DV0:caf23b8150cd4d93f23d917acf93c00cec79fab86aef370382330e68413b201b
```

- On *Linux* and *MacOS*, it is also possible to use the `shasum -a 256` utility with `/dev/random` (*MacOS*™) or `/dev/urandom` (*Linux*™) as a source of random bytes:

```
> head -c 4096 /dev/random | shasum -a 256

62ea8b6c8da61fe5b0867eb6cad81fd4e8d9a356bda79be5b311a068eda93962  -
```

4.3.1.2 Device Configuration

Once the keys are generated, the PSK key and the bootstrap server information must be written to the device. Then the LwM2M service must be enabled.

In the following table, the module is assumed to be running in ‘standard’ operating mode.

Command	Response	Comment
AT+SQNCTM?	+SQNCTM: standard OK	Check the operator mode
AT+SQNAUTOCONNECT=1	OK	Automatic attach To add/edit/delete LwM2M accounts the LwM2M client must be started after reboot. It is done after AT+CFUN=1 command.
AT+CFUN=5	OK	Enter manufacturing mode
AT+SQNDMCFG=”standard”,"service",1	OK	Start LwM2M automatically
AT+SQNDMCFG="standard","server",100,"60","coaps://eu.iot.avsystem.cloud:5694","1","bs"	OK	Configure the bootstrap server. In this example, the AVSystem Bootstrap URI is: coaps://eu.iot.avsystem.cloud:5694 The server’s hold-off timer value is set to 60 s.
AT+SQNDMCFG="standard","psk",100,"urn:imei:015770000031766","87493467538357"	OK	Configure the PSK previously generated. Endpoint Client Name is “urn:imei:<IMEI>”. PreSharedKey (PSK) is a string in HEX format.
AT^RESET	OK +SHUTDOWN +SYSSTART	Reset to validate the changes

The LwM2M client's endpoint name which is used for registration on the server contains the prefix urn:imei: (for 'standard' operator mode) and the IMEI, resulting in the string: urn:imei:015770000031766.

Command	Response	Comment
AT+CGSN	015770000031766 OK	Get the IMEI

Note: Do not mix up the Endpoint Name with the PSK ID in the LwM2M account (AT+SQNDMCFG). They usually have the same value, but their roles are different.

4.3.1.3 Create a Restoration Point

The configuration must be saved in case it would need to be restored after a factory reset.

Command	Response	Comment
AT+CFUN=5	OK	Enter manufacturing mode
AT+SQNFACTORYSAVE="oem"	OK	

4.3.2 Adding the Device to the Inventory

This section assumes the existence of an AVSystem account for the feature, and the availability of an access to the Coiote IoT Device Management.

After logging to the **Coiote IoT Device Management**, go to **Device Inventory**:

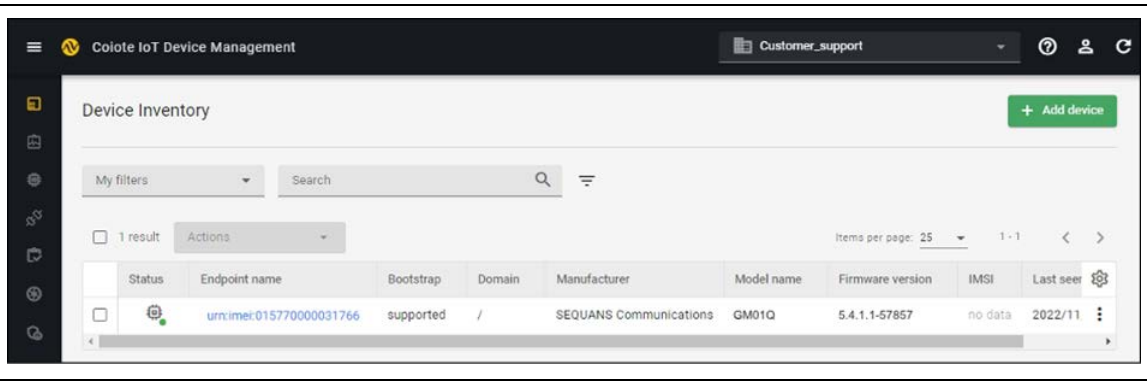

Figure 3. Device Inventory in the Coiote IoT Device Management System

Delete the device if the endpoint name is already registered (optional step):

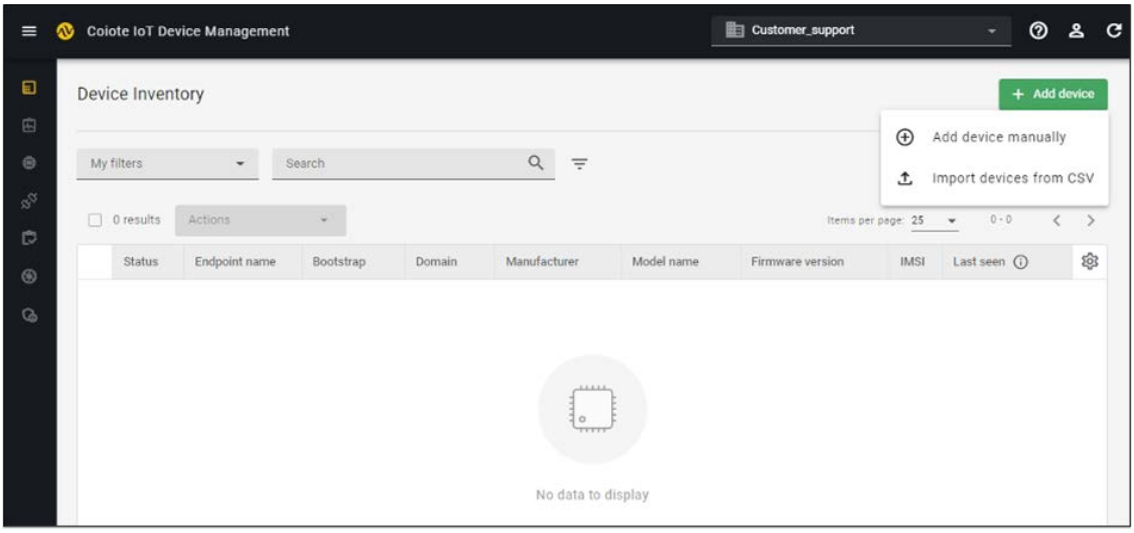

Figure 4. Deleting Device in the Coiote IoT Device Management System

Click the '**Add device'** button and choose the '**Add device manually**' option:

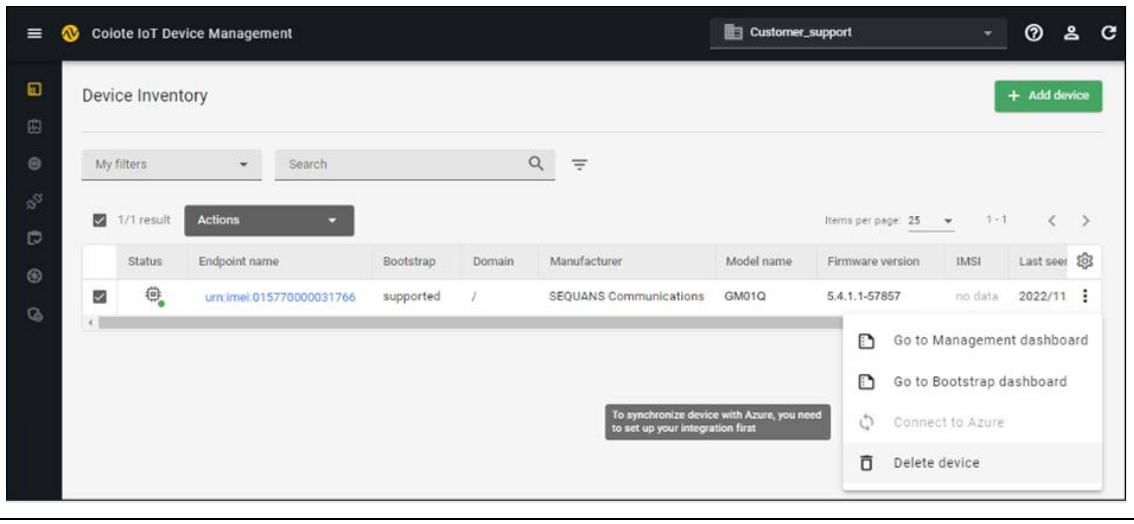

Figure 5. Adding Device Manually in the Coiote IoT Device Management System

Note: Use the 'Search' field to check if an Endpoint with the same name is already registered. If so, delete it to use the new PSK identities.

Choose '**via the Bootstrap server**' option:

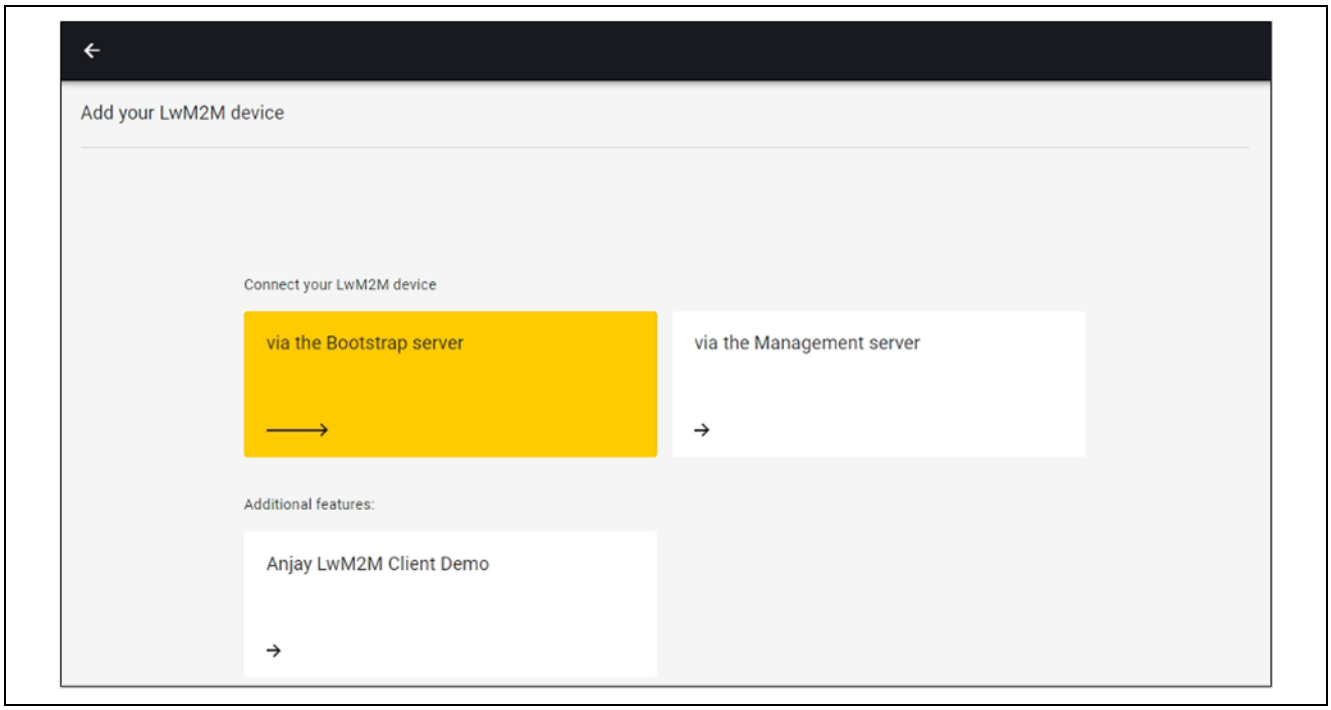

Figure 6. Choosing Option for Connecting through the Bootstrap Server

Enter the client's endpoint name, security mode, key identity and PSK key in hexadecimal format:

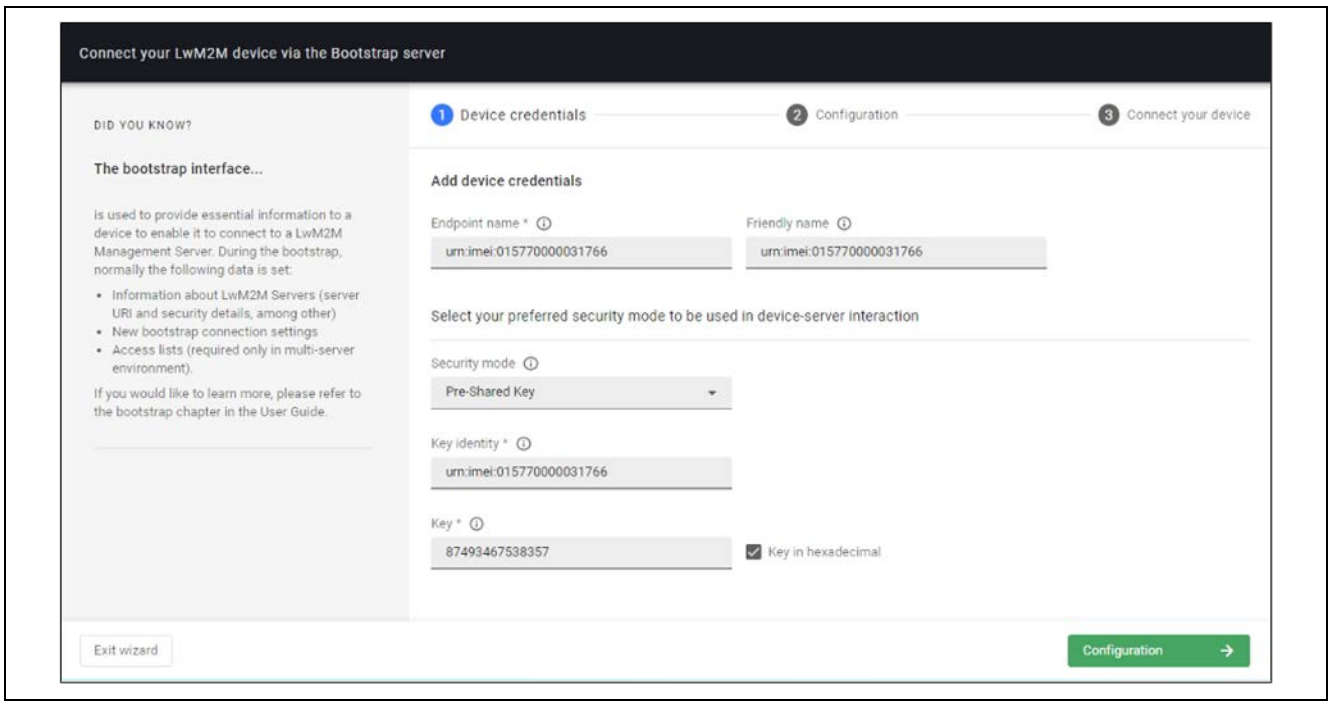

Figure 7. Adding Device Credentials

Choose '**This Coiote DM Management Server PSK**' option, then click the '**Add device**' button:

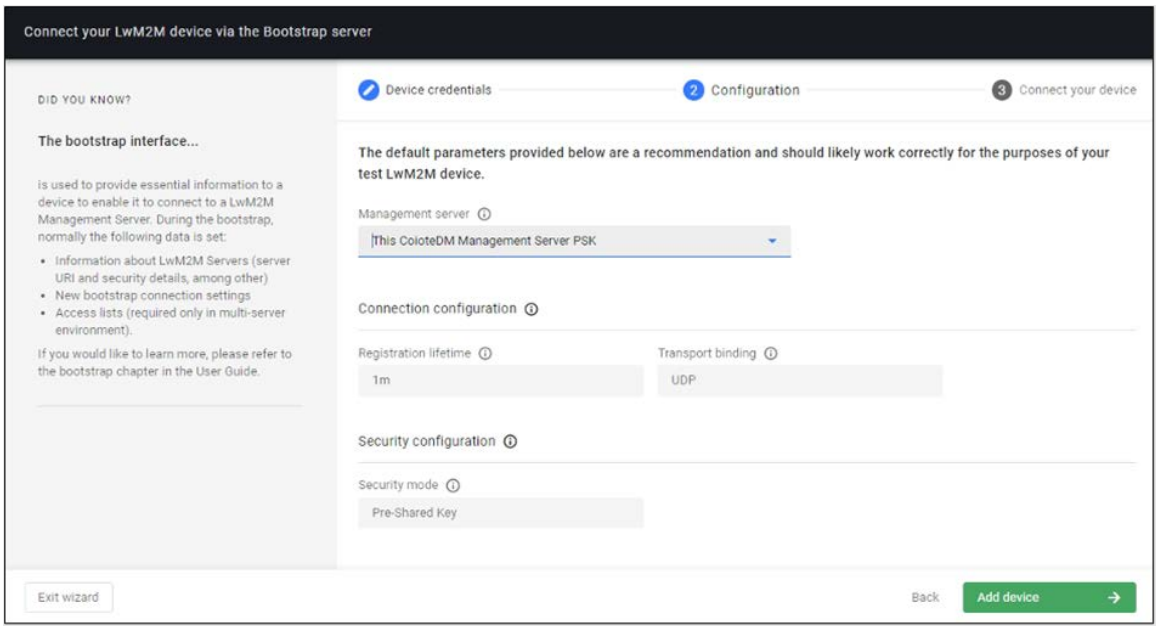

Figure 8. Choosing 'Coiote DM Management Server PSK' Option

Confirm the device creation.

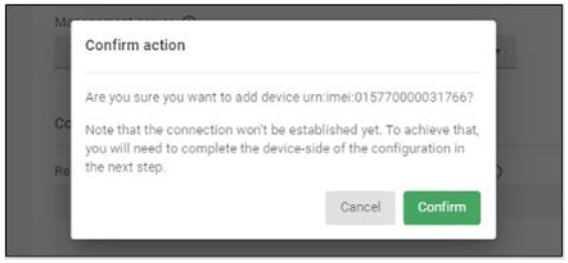

Figure 9. Confirming the Device Creation

Click on the '**Go to device'** button to advance to the Bootstrap profile management page:

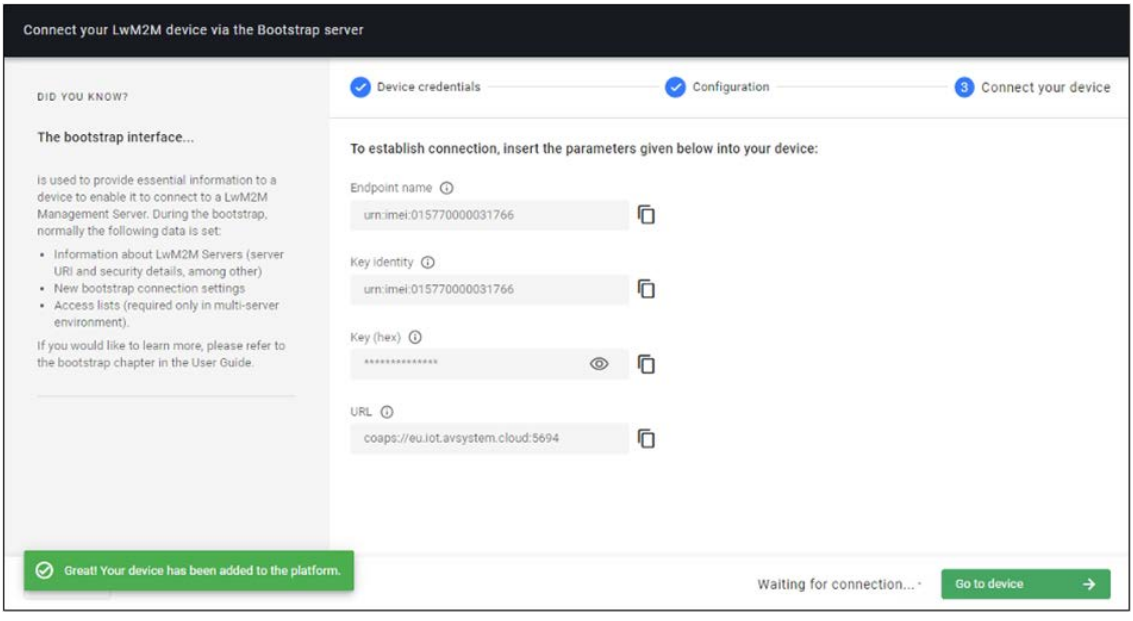

Figure 10. Going to the Bootstrap Profile Management Page

Click the '**Go to the previous version**' to revert to a previous, more stable version of the web interface (if need be).

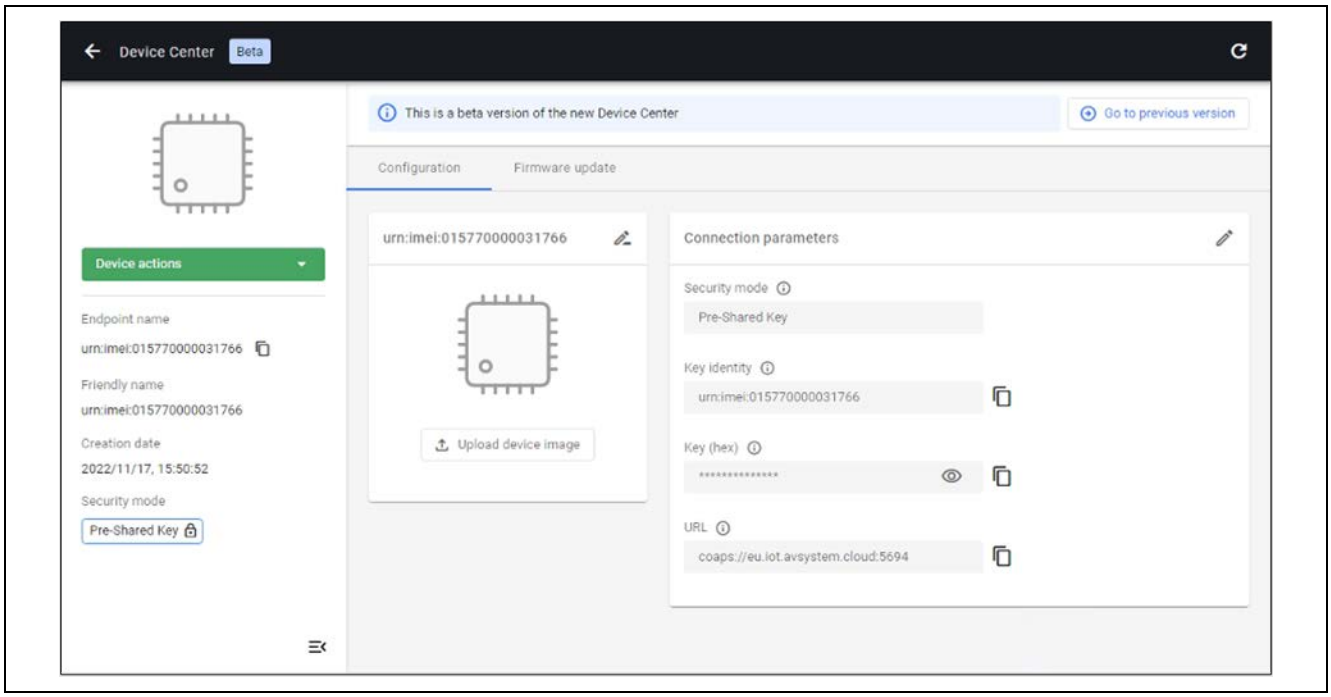

Figure 11. Going to the Previous Version of the Web Interface

4.3.3 Register the Device

In the example below, the LwM2M client is configured in 'Auto' mode. In this mode, after attaching to the network, the device contacts the bootstrap server if the server hold-off timer has expired to check for a pending update. This is the recommended setting.

The procedure has to be done once after each factory reset.

Command	Response	Comment
`AT+SQNFOTACFG="standard",0,2,10,60,,60`	`OK`	• 0: LwM2M client Auto mode • 2: Report state change and intermediate error (URC) • 10: Report download progress (in 10% increments) (URC) • 60: FOTA timer 60 s for demo (max. 30 days) ,,: Download timeout (not set) • 60: Certificate ID
`AT+CFUN=1,1`	`OK`	Reset the MT prior to setting it to function level 1. A reset is needed after `SQNFOTACFG` change.
	`+SHUTDOWN` `+SYSSTART`	
	`+CEREG: 2`	Connecting to the network
	`+CEREG: 1,"0002","01A2D002",7`	Attached to the network
	`+SQNFOTA: 1`	'Onboarding' (FOTA service activation is in progress)
	`+SQNFOTA: 2`	Stopped (FOTA service is activated but not running)
	`+SQNFOTA: 3`	Idle

After the server's hold-off timer expiry.

4.4 Manage the Client on the Server

Go to the **Operation center** tab on the *Coiote IoT Device Management* server. The dashboard shows the number of activated devices (1 in this case). The device's characteristics are listed in the table:

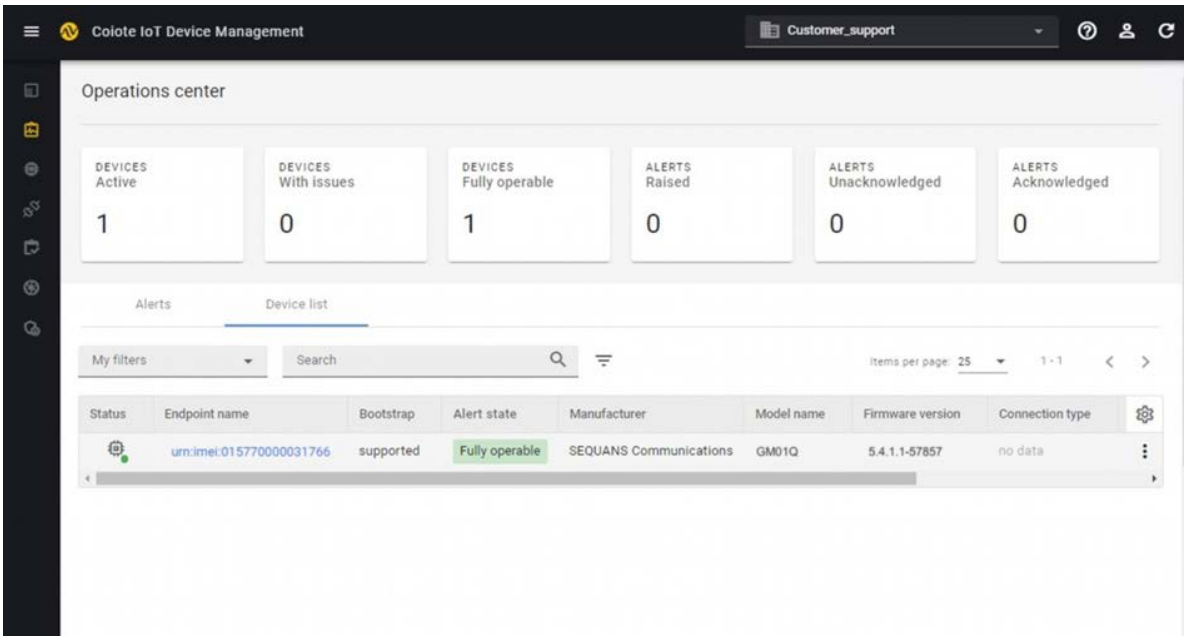

Figure 12. Viewing the Activated Devices on the Dashboard

Click on the line containing the device you want to manage and choose the '**Management'** option to manage the client.

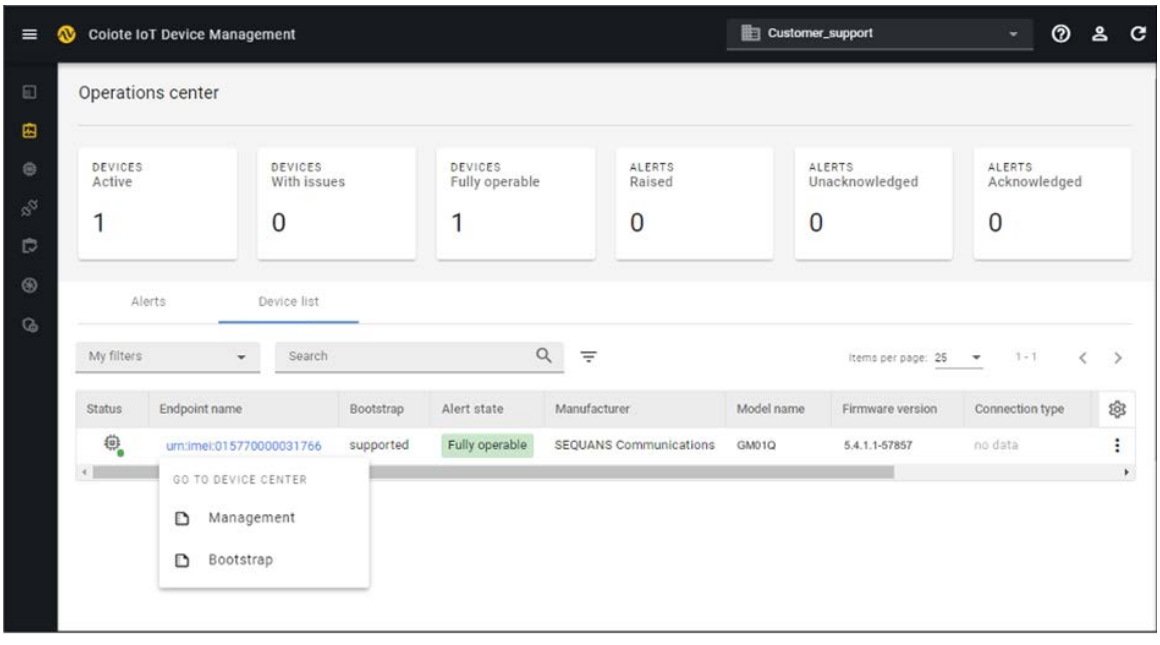

Figure 13. Managing the Client

Click on '**Go to the previous version'** to revert to a more stable web interface (if need be).

Figure 14. Going to the Previous Version of the Web Interface

Check for the client's registration in Device Management mode.

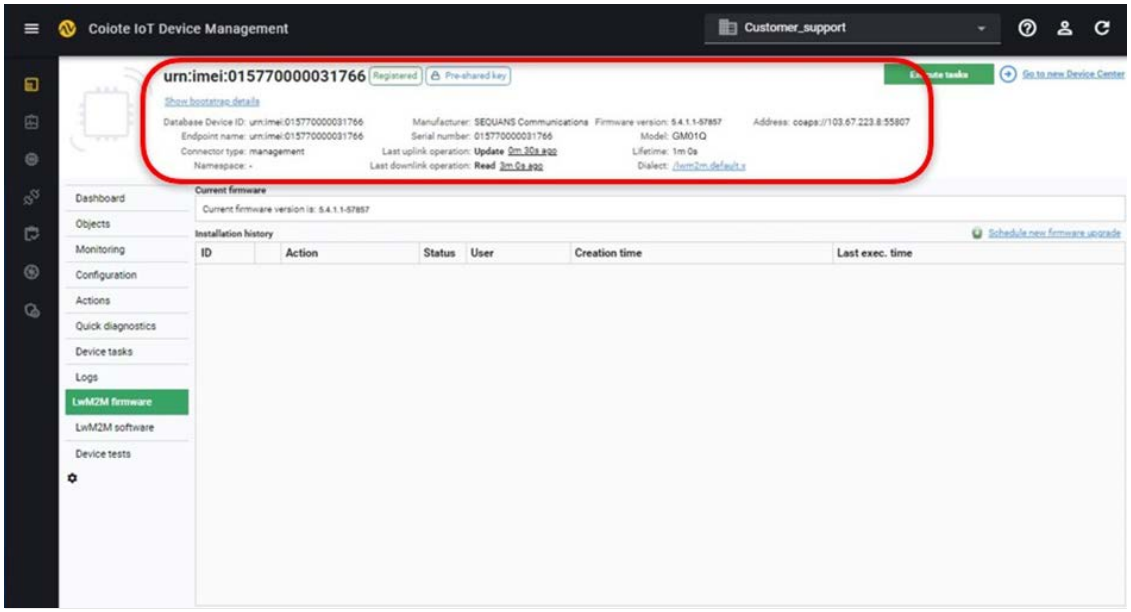

Figure 15. Checking the Client Registration in the Device Management Mode

4.4.1 Preparation

Get the official differential image delivered by Renesas or generate one following the instructions given in the ***RYZ014 System Integration Guide***.

In this chapter, the sample images are `to_LOWER_FFF_PXL.bin` which downgrades from LR5.4.1.1-57857 to LR5.4.1.1-57830, and `to_HIGHER_FFF_PXL.bin` which upgrades from LR5.4.1.1-57830 to LR5.4.1.1-57857.

4.4.2 Upload the Image on the Server

Log to the *Coiote IoT Device Management*, go to the '**LwM2M Firmware'** tab and click on '**Schedule New Firmware Upgrade'.**

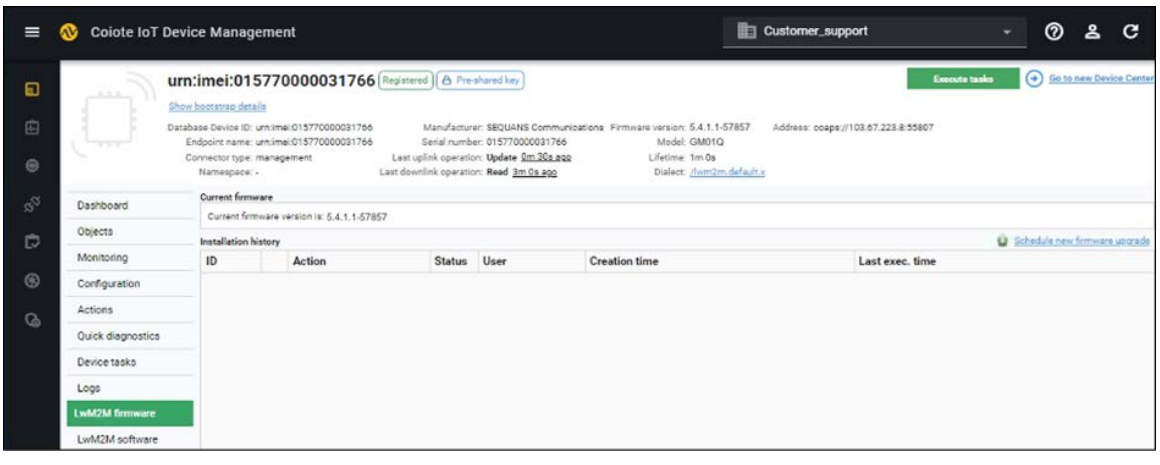

Figure 16. Navigating to the 'Schedule New Firmware Upgrade' Option

Click on '**Upload file**', select the differential dup image and then click on '**save'** to upload it.

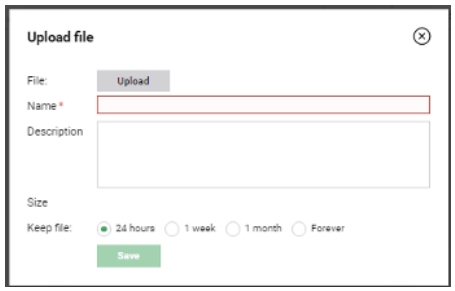

Figure 17. Uploading the Differential dup Image

Select the uploaded file, choose the image delivery method and delivery protocol, then click on **Upgrade** to begin FOTA procedure. This example uses the PULL method and the HTTP protocol.

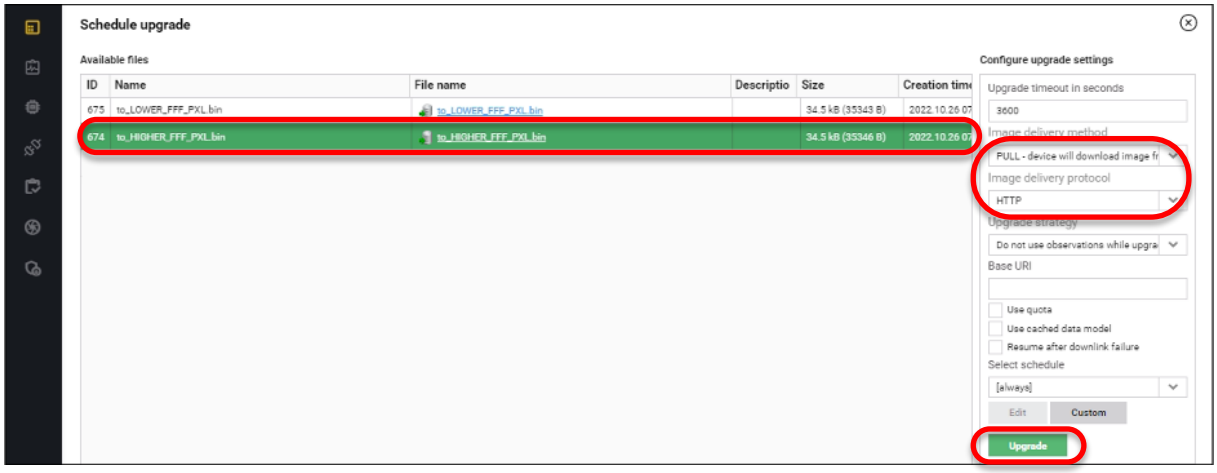

Figure 18. Beginning the FOTA Upgrade Procedure

4.5 FOTA Procedure

4.5.1 Overview

Throughout the following examples, the FOTA upgrade process is the same, but the triggers are different. This chapter details three typical use cases.

4.5.1.1 Modem (FOTA Client) Initiated FOTA

Once the FOTA client running on the modem is activated and configured in 'Auto' mode, it executes in the background and periodically checks, downloads, and installs any available upgrade package, as explained in the LwM2M specification. It also schedules the reboot sequence necessary to complete the upgrade procedure, without interaction with the host application.

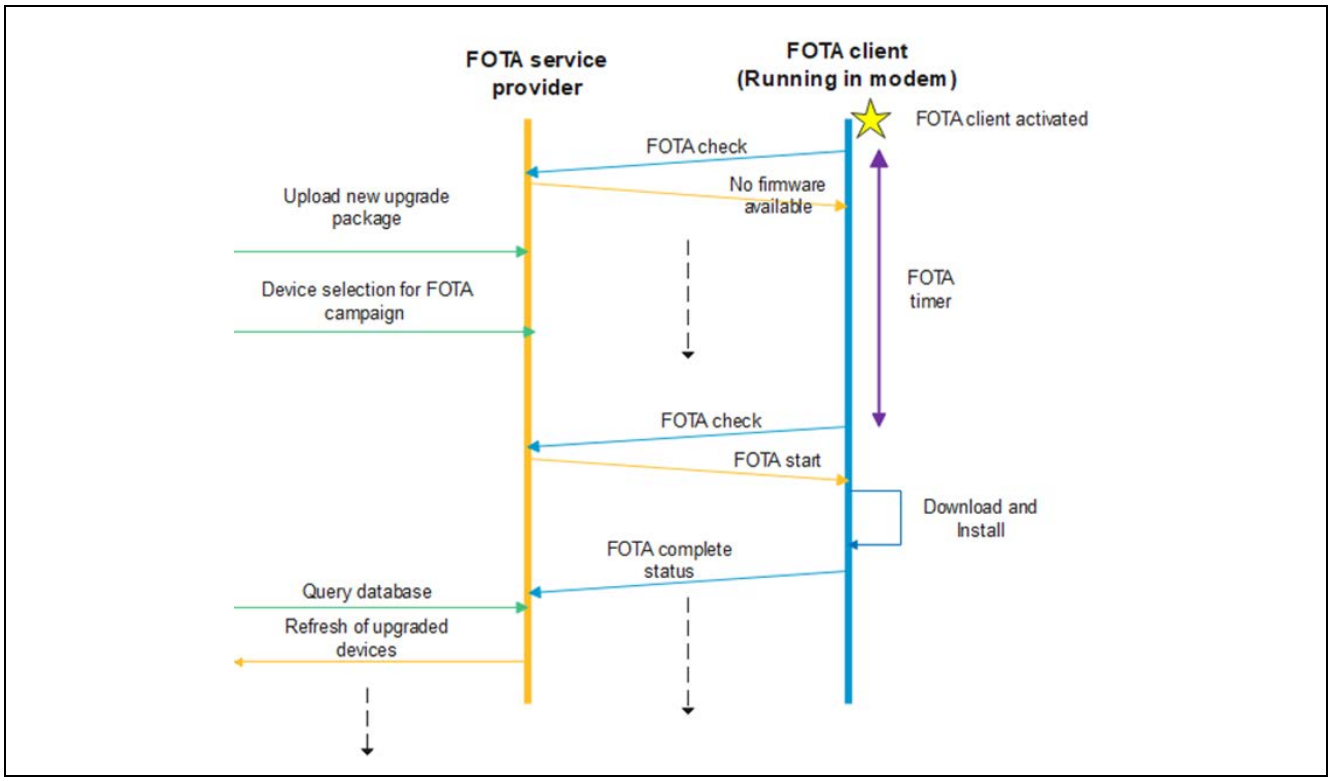

Figure 19. Modem Initiated FOTA Upgrade Procedure

The host application must process every URCs to ensure it does not power off the modem while the upgrade package is being installed.

4.5.1.2 Network Initiated Query

Once the FOTA client is activated, the server can contact the FOTA client running on the modem and ask it to check if any upgrade package is available using the process detailed below:

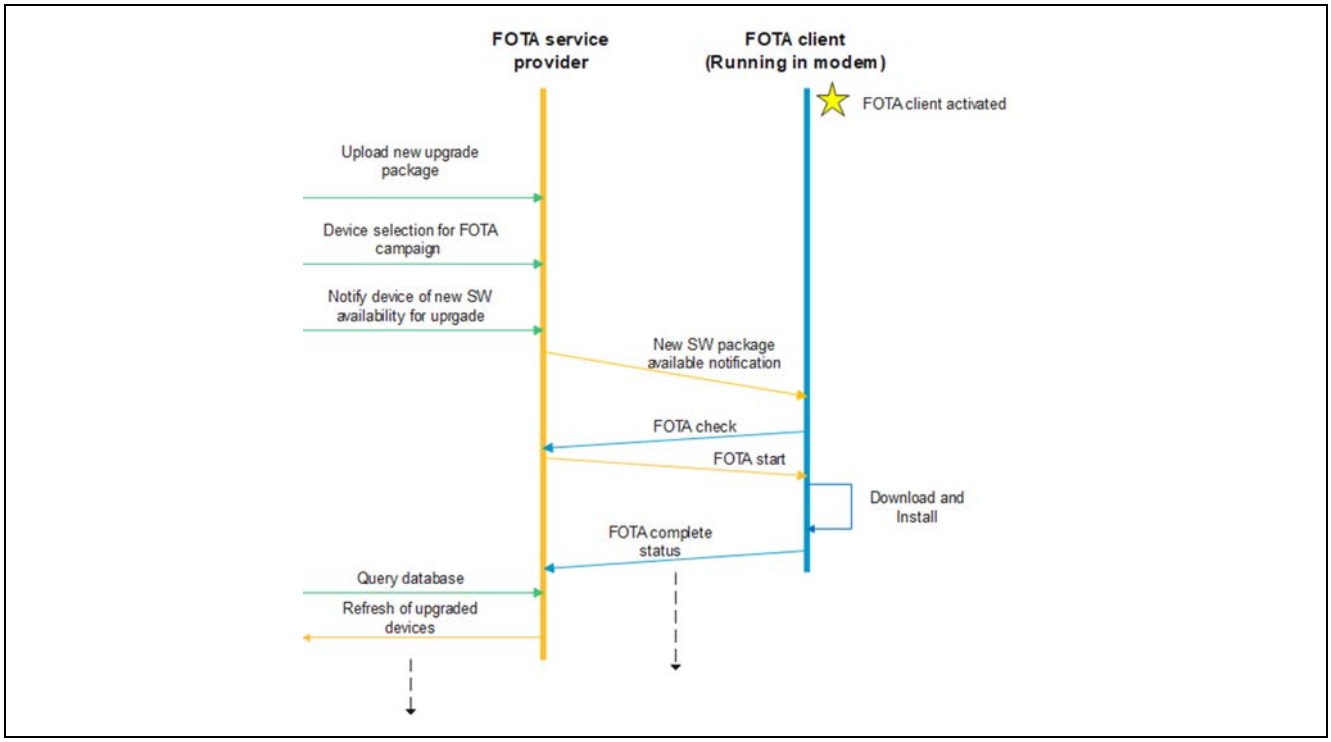

Figure 20. Checking if any Upgrade Package is Available

4.5.2 Detailed FOTA Procedure

The LwM2M client Auto mode is configured as shown above.

When using Auto mode, the device performs everything automatically, including triggering a FOTA check by FOTA update timer, downloading an image if available and installing it.

It is assumed that the device is already attached to the network:

Command	Response	Comment
AT+SQNFOTACFG="standard",0,2,10,60,,60	OK	0: LwM2M client Auto mode 2: Report state change and intermediate error (URC) 10: Report download progress (10% increments) (URC) 60: FOTA timer 60s for demo (max. 30 days) ,,: Download timeout (not set) 60: Certificate ID
ATI1	UE5.4.1.1 LR5.4.1.1-57857 OK	Check the current firmware version
	+SQNFOTA: 4 +SQNFOTA: 3	
	+SQNFOTA: ”available”	New software ready for upgrade
	+SQNFOTA: 4 +SQNFOTA: 3 +SQNFOTA: 5 +SQNFOTA: 5,3,0 +SQNFOTA: 5,3,10 +SQNFOTA: 5,3,20 +SQNFOTA: 5,3,30 +SQNFOTA: 5,3,40 +SQNFOTA: 5,3,50 +SQNFOTA: 5,3,60 +SQNFOTA: 5,3,70 +SQNFOTA: 5,3,80 +SQNFOTA: 5,3,90 +SQNFOTA: 5,3,100	‘Onboarding’ (FOTA service activation is in progress)
	+SQNFOTA: ”downloaded” +SQNFOTA: 6	The image is downloaded
Start the SW installation. This would take some time, keep the device powered on during the action.		
	+SQNFOTA: 7 +SQNFOTA: ”install”	Updating / Installing
	+SYSSTART +CEREG: 2	Reconnecting to the network after reboot
	+SQNFOTA: 8 +SQNFOTA: "installed", "5.4.1.1-57830"	Installed

Command	Response	Comment
	+CEREG: 1,"0002", "01A2D002",7	Reconnected to the network

You can also follow the progress on the '**LwM2M firmware**' tab on the server side.

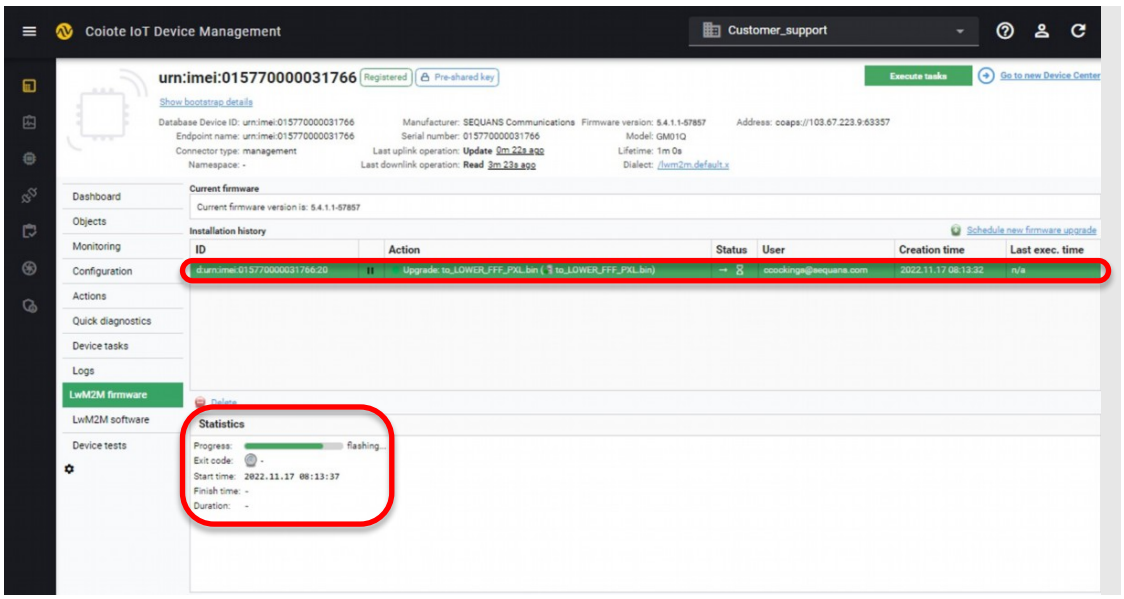

Figure 21. Viewing Upgrade Progress on the Server

4.5.3 Verify

After a successful FOTA upgrade/downgrade, the firmware version can be checked on the client side using the `ATI1` command:

Command	Response	Comment
ATI1	UE5.4.1.1 LR5.4.1.1-57830 OK	Check the current firmware version

Once the client has registered again on the server, verify that the FOTA was recorded as successful on the server side.

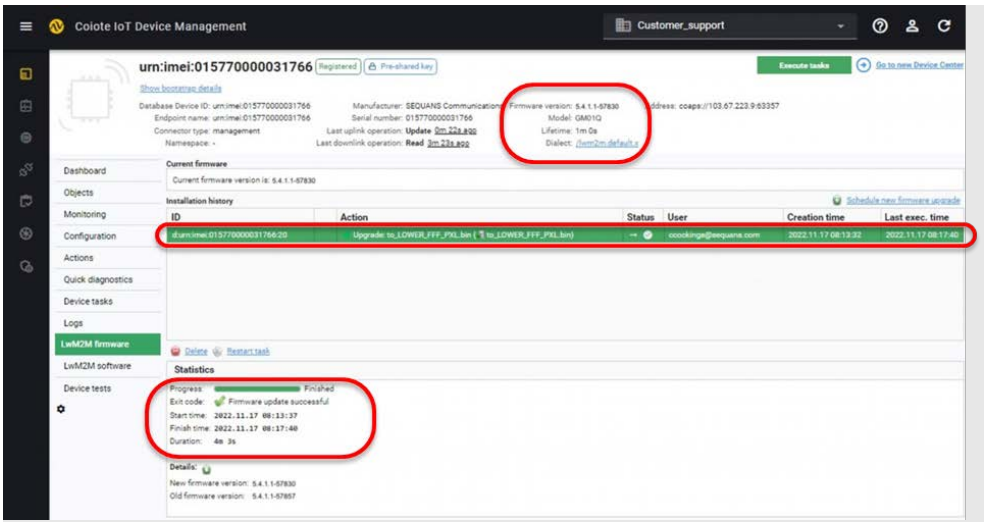

Figure 22. Verifying that FOTA was Successful

4.6 Low Power Considerations

The FOTA client allows the modem to enter Sleep and Deep Sleep modes in the following cases:

- Client state is STOPPED
- Client state is ACTIVE/IDLE

Any FOTA timer expiration will trigger FOTA client to wake up from low power modes.

4.7 Troubleshooting

Basic troubleshooting consists in parsing the +SQNFOTA URCs. These URC indicate not only the state and downloading progress, but also the cause of a raised error. Please refer to section 6, Appendix: AT Commands Description for details.

4.7.1 Wrong FOTA Image

If, during software update, you get the following log, please verify the image that has been uploaded.

```
+SQNFOTA: "downloaded"
+SQNFOTA: 6    // The FW is downloaded (software
package)
+SQNFOTA: 7    // Upgrading (software)
+SQNFOTA: "install"
+SYSSTART      // Reboot to install FW
+SQNFOTA: 3    // Idle
+SQNFOTA: 3,8  // Idle, installation failure
```

5. FOTA with AT Commands

It is also possible to perform a Firmware Over the Air (FOTA) update for the modem using firmware files from an FTP or HTTP(S) server and the AT+SQNSUPGRADE command.

In this case, specific server(s) storing the software images must be available. Since the FOTA process is a device-initiated firmware update triggered by the host system, the user must develop a host application relying on AT commands to manage the upgrade session. The modem downloads the firmware file from the specified server and updates.

Only differential FOTA upgrades are supported, which allow to upgrade the firmware to a new version or downgrade to an old version. Before firmware upgrade, the firmware package containing only the differences between the old and new firmware version must be generated. The use of a differential image reduces the amount of data transmitted and accelerates the speed of firmware upgrade.

Users need to operate the following steps to upgrade the firmware:

- Get differential firmware image from Renesas.
- Put the differential firmware image on FTP or HTTP/S server
- Execute the AT+SQNSUPGRADE command to launch the upgrade.

The module will upgrade automatically.

- The modem MUST NOT be powered down during the firmware download. Doing so will cause the download to fail, and the download will have to be restarted.
- Once the file is successfully downloaded, applying the firmware update takes a few minutes to complete. It is not recommended to power down the modem during this process. If the modem is powered down during this process, the update process pauses and then resumes once power is reapplied. This is not recommended as URC notifications about the update may be missed, the firmware update may fail and the modem resets several times during the update process.

Please refer to the *AT Command Reference Manual* for the description of the AT Commands and the *AT Commands Use Cases* application note for examples of use.

6. Appendix: AT Commands Description

6.1 AT+SQNFOTACFG: FOTA Configuration

6.1.1 Syntax

Command	Response
AT+SQNFOTACFG=<upg_profile>[,<mode>[,<report_state>[,<report_download>[,<fota_timer_sec>[,<download_to_sec>[,<certificateID>]]]]]]	OK ERROR +CME ERROR: <err>
AT+SQNFOTACFG=?	+SQNFOTACFG: 32[,(0,1)[,(0-2)[,(0-100)[,(60-32000000)[,(60-65535)[,(11-19)]]]]]] OK
AT+SQNFOTACFG?	+SQNFOTACFG: <upg_profile>,<mode>,<report_state>,<report_download>,<fota_timer_sec_requested>,<fota_timer_sec_actual>,<download_to_sec>,<certificateID> OK

6.1.2 Description

This command is used to configure FOTA client behavior.

The FOTA client relies on an upgrade service profile identified by the <upg_profile> parameter and providing following functions: device onboarding, software upgrade package availability check, software upgrade package download and optionally upgrade status reporting.

The <upg_profile> parameter references a device management service profile declared and configured separately with the AT+SQNDMCFG command under a <dmProfile> profile name equal to the <upg_profile> value.

The level of interaction with user application is configured by <mode> parameter. There is only one mode available:

- "automatic" (default): The FOTA client operates in the background, without interaction with user application.

Whatever configured FOTA <mode>, the user application can be informed of the FOTA client activity using +SQNFOTA notifications by enabling reporting capabilities with the <report_state> and <report_download> parameters (optional parameters):

- <report_state> specifies FOTA client state change indication (+SQNFOTA) reporting level
- <report_download> specifies new firmware download progress indication reporting percentage step.

Optionally, user application can also override default FOTA client behavior by setting:

<fota_timer_sec>: Modem initiated FOTA check period (based on OMA registration lifetime resource value /1/x/1 for particular DM server). This parameter relies on server-defined registration lifetime obtained during onboarding process.

This timer is volatile and can be changed by the server at any time. If so, then the URC notification shows the new value. Also, the read command AT+SQNFOTACFG? displays both requested value and the current one.

- <download_to_sec>: Maximum time in seconds allowed for the software package download. This timeout is typically useful to prevent infinite download due to slow network or cellular connection going down during operation. Timer shall be set consistently with estimated network speed capability to avoid shutting down normal but slow updates. In case of timeout expiration during upgrade file data transfer and if download protocol supports resume function (HTTP/ HTTPS), download will be resumed next FOTA timer or next device download request. If the parameter is omitted, the download resume logic is applied.

The user can control the maximum FOTA client radio activity duration using the above timers, which may be mandatory if the device power supply architecture is only compatible with time-limited activity period.

FOTA client configuration is stored in non-volatile memory and is preserved at reboot or during a software upgrade. The configuration is updated during the next module reboot. Any kind of reboot (AT^RESET, AT+SQNSSHDN, hardware reset) is acceptable.

The read form of this command returns the FOTA client configuration applicable at next reboot (the currently active configuration is overwritten with pending changes, if any).

The test form returns values supported as a compound value.

6.1.3 Defined Values

- <upg_profile> (string): Upgrade service profile name (max. length 32 characters)
  - When upgrade service is provided by a device management service, the profile name must reference a valid device management configuration profile (see AT+SQNDMCFG).
- <mode> (num): FOTA client mode
  - 0 (default): Automatic mode with FOTA client activity managed in background without user intervention.
- <report_state> (num) [0, 1 or 2]: FOTA client state change indication (+SQNFOTA) reporting level
  - 0: Notification disabled
  - 1: State change reporting enabled
  - 2 (default) : State change and intermediate error reporting enabled
- <report_download> (num) [0..100]: Specifies software upgrade package download progress indication reporting percentage step
  - 0 (default): Do not report download progress indication
  - 1..100: Download progress indication reported at each configured percentage step
- <fota_timer_sec> (num, optional) [60..32000000]: FOTA periodic timer
  - FOTA client periodic timer used to trigger FOTA check or resume a paused FOTA activity.
  - This value is volatile and can be changed at any time by the server. The read command will display both the requested value and the value currently in use. If the value is omitted, the client will use the value provided by the server.
- <download_to_sec> (num, optional) [60..65535]: Download timeout in seconds (optional). See above for description.
- <certificateID> (num) [11..19]: Certificate index to be used for the authentication on FOTA repository server (certificate previously stored using AT+SQNSNVW="certificate" command).

6.2 AT+SQNDMCFG: Device Management

This command configures device management. <cfgGrp> identifies a configuration group set. For FOTA, three groups are mandatory:

- "service": Service main configuration
- "server": Device management server configuration
- "psk": Pre-shared key (PSK) provisioning

Configuration storage rules are unchanged:

- DM configuration profiles are stored in non-volatile memory and are preserved during device reboots, software upgrades and factory resets.
- Configuration update is done in device manufacturing mode and applied at the next module reboot. Any kind of reboot (AT^RESET, AT+SQNSSHDN, hardware reset) being acceptable.

6.2.1 Service Syntax

Command	Possible Response(s)
AT+SQNDMCFG=<dmProfile>[,<cfgGrp>[,…]]	OK +CME ERROR: <err>
AT+SQNDMCFG=<dmProfile>,"service"[,<autostart>]	OK ERROR
AT+SQNDMCFG=<dmProfile>,"service"	+SQNDMCFG=<dmProfile>,"service",<autostart> OK ERROR
AT+ SQNDMCFG=?	+SQNDMCFG=(32),"service"[,(0,1)] [...] +SQNDMCFG=(32),"server"[,(1-65535),,(256)[,[(1-8)[,(bs,dm)]]]] OK

This subcommand command is used to configure the autostart of FOTA service. If no <autostart> is provided, the response tells if the service is currently auto-started.

Test command displays the usage.

6.2.1.1 Defined values

- <dmProfile> (string): Device management server profile name (max. length 32 characters)
- <cfgGrp> (string): Device management configuration group identification
  - "service": service main configuration
  - "server": Device management server configuration
  - "psk": pre-shared key (PSK) provisioning
  - "delete-profile-config": special command group to delete the entire configuration profile
- <autostart> (num) [0 or 1]: Automatic device management startup at power-on
  - 0: LwM2M service disabled
  - 1: LwM2M service enabled

6.2.2 Server Syntax

This section extends the command with a server group. Only this extension is described here.

Command	Possible Response(s)
AT+SQNDMCFG=<dmProfile>,"server"[,<serverId>,[,<lifetimeValue>],<serverUrl>[,[<cid>][,[<serverType>]]]	OK ERROR
AT+SQNDMCFG=<dmProfile>,"server"	For each configured <serverId>: +SQNDMCFG=<dmProfile>,"server",<serverId>,<lifetimeValue>,<serverUrl>,<cid>,<server_type> OK

The write subcommand configures device management server(s) URL (<serverUrl> parameter) and PDP context identifier (<cid> optional parameter) of the APN to be used for all over the air communications. Using the command with the first two parameters only (<dmProfile>, "server") dumps all server configurations stored for identified <dmProfile>.

6.2.2.1 Defined values

- <dmProfile> (string): Device management server profile name (max. length 32 characters)
- <cfgGrp> (string): Device management configuration group identification
  - "service": service main configuration
  - "server": Device management server configuration
  - "psk": pre-shared key (PSK) provisioning
- <serverId> (num) [1..65535]: Device management short server ID
- <lifetimeValue> (num) [0..32000000]: server life time value
- <serverUrl> (string): Device management server URL (IP or Name) (Max length 256 characters)
- <cid> (num) [1..8]: PDP context identifier (optional)
  - Identifies the APN to be used for all over the air communications. By default, this is either the Internet PDN (whose effective identifier value depends on the carrier configuration profile) or the device management provider enforced PDN (ex.: the carrier device management service's special PDN).
- <serverType> (string): Server type
  - "bs": bootstrap server
  - "dm": device management server (default)

6.2.3 PSK Syntax

This section extends the command with a psk group. Only this extension is described here.

Command	Possible Response(s)
AT+SQNDMCFG=<dmProfile>,"psk",<serverId>,<pskId>,<pskSecret>	OK ERROR
AT+SQNDMCFG=<dmProfile>,"psk"	For each configured <serverId>: +SQNDMCFG=<dmProfile>,"psk",<serverId>,<pskId>,<4 first hexadecimal of pskSecret> OK

This subcommand configures the PSK identifier and secret associated to identified <dmProfile>/<serverId>. Empty <pskId> and <pskSecret> parameters to remove PSK entry.
Using only the first two parameters (<dmProfile>, "psk") dumps all the PSK configurations stored for the identified <dmProfile>. For security reason, only the first four hexadecimal of the PSK secret are displayed.

6.2.3.1 Defined values

- <dmProfile> (string): Device management server profile name (max. length 32 characters)
- <cfgGrp> (string): Device management configuration group identification
  - "service": service main configuration
  - "server": Device management server configuration
  - "psk": pre-shared key (PSK) provisioning
- <serverId> (num) [1..65535]: Device management short server ID.
- <pskId> (string): Pre-shared key identity in hexadecimal format (Max length 32 bytes = 256-bit key). Use an empty parameter to remove the PSK entry.
- <pskSecret> (string): Pre-shared key in hexadecimal format (Max length 32 bytes = 256-bit key). Use an empty parameter to remove the PSK entry.

6.2.4 delete-profile-config

This section extends the command with a *delete-profile-config* group. Only this extension is described here.

Command	Possible Response(s)
AT+SQNDMCFG=<dmProfile>,"delete-profile-config"	OK ERROR

This subcommand deletes a configuration profile in case of any mistake or misuse of the AT+SQNDMCFG command. This is important since the data are preserved at reset.

6.2.4.1 Defined values

- <dmProfile> (string): Device management server profile name (max. length 32 characters)
- <cfgGrp> (string): "delete-profile-config": deletes the entire configuration profile

6.3 AT+SQNDMCFG: LwM2M Registration Status

This command provides LwM2M Bootstrap and Device Management servers registration status. It can be used to trigger de-registration in order to save battery.

The command returns ERROR if the UE is not attached to the LTE network or if LwM2M client is not enabled.

6.3.1 Syntax

Command	Possible Response(s)
AT+SQNDMST	+SQNDMST: "bs",<Server ID>,<"bs Status">,<hold off Timer>, <bs Update Timer> ... +SQNDMST: "dm",<Server ID>,<"dm Status">,<dm Life Time>, <dm Update Timer> ... OK

6.3.2 Defined values

- <server ID> (integer [1..65535]): The server's (bootstrap or device management) short ID, as defined by the carrier.
- <bs Status> (string): Bootstrap server registration status:
  - "BS_HOLD_OFF": Waiting for hold off timer expiration before starting the bootstrap process
  - "BS_INITIATED": Bootstrap request message sent to server
  - "BS_PENDING": Bootstrap process ongoing
  - "BS_FAILING": Bootstrap error
  - "BS_FAILED": Bootstrap failed
  - "BS_FINISHING": Bootstrap finished message received from server
  - "BS_FINISHED": Bootstrap is complete
- <hold off Timer> (integer): Timer value (in seconds), defined by carrier, the UE must wait after the initial attach before starting the bootstrap process.
- <bs Update Timer> (integer): Delay (in seconds) until the bootstrap starts. If -1, the registration process is either ongoing or already complete.
- <dm Status> (string): Device Management server registration status:
  - "DEREGISTERED": Not registered
  - "REG_PENDING": Registration pending
  - "REGISTERED": Successfully registered
  - "REG_FAILED": Last registration failed
  - "REG_UPDATE_PENDING": Registration update pending
  - "REG_UPDATE_NEEDED": Registration update required
  - "DEREG_PENDING": De-registration pending
  - "REG_DISABLE": De-registration pending
  - "REG_NEEDED": New registration required
- <dm Life Time> (Integer): Registration lifetime timer (in seconds), given by the server. The registration update process starts when this timer expires. If the value is -1, the process is currently under way.
- <dm Update Timer> (Integer): Time (in seconds) remaining before the registration update starts.

6.3.3 Examples

```
AT+SQNDMST
+SQNDMST: "bs",100,"BS_HOLD_OFF",10,7
+SQNDMST: "dm",101,"DEREGISTERED",86400,86397

OK
```

The bootstrap process is delayed by the carrier's hold off timer. It will start in 7 seconds.

```
AT+SQNDMST
+SQNDMST: "bs",100,"BS_INITIATED",10,-1
+SQNDMST: "dm",101,"DEREGISTERED",86400,86363

OK
```

The bootstrap process is under way. The <bs Status> string can take other values during the bootstrap process.

```
AT+SQNDMST
+SQNDMST: "bs",100,"BS_FINISHED",10,-1
+SQNDMST: "dm",102,"DEREGISTERED",2592000,22
+SQNDMST: "dm",101,"REG_PENDING",86400,-1

OK
```

The bootstrap process was successful:

- Two device management servers have been set up by the bootstrap server
- Server 102 registration starts in 22 seconds
- Server 101 registration is under way. The <dm Status> string can take other values during the server registration process.

```
AT+SQNDMST
+SQNDMST: "bs",100,"BS_FINISHED",10,-1
+SQNDMST: "dm",102,"DEREGISTERED",2592000,18
+SQNDMST: "dm",101,"REGISTERED",86400,84597

OK
```

The bootstrap process was successful:

- Server 102 registration starts in 18 seconds
- Server 101 registration was successful. Registration update period is 24 h. The next registration update is scheduled in 84597 s.

```
AT+SQNDMST
+SQNDMST: "bs",100,"BS_FINISHED",10,-1
+SQNDMST: "dm",102,"REGISTERED",2592000,2587603
+SQNDMST: "dm",101,"REGISTERED",86400,81965
```

```
0K


The bootstrap process was successful:
```

- Server 102 registration was successful. Registration update period is 30 days (2,592,000 seconds). The next registration update is scheduled in 2,587,603 s.
- Server 101 registration was successful. Registration update period is 24 h. The next registration update is scheduled in 81,965 s.

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	Jan.31.23	-	Initial release

General Precautions in the Handling of Microprocessing Unit and Microcontroller Unit Products

The following usage notes are applicable to all Microprocessing unit and Microcontroller unit products from Renesas. For detailed usage notes on the products covered by this document, refer to the relevant sections of the document as well as any technical updates that have been issued for the products.

1. Precaution against Electrostatic Discharge (ESD)

   A strong electrical field, when exposed to a CMOS device, can cause destruction of the gate oxide and ultimately degrade the device operation. Steps must be taken to stop the generation of static electricity as much as possible, and quickly dissipate it when it occurs. Environmental control must be adequate. When it is dry, a humidifier should be used. This is recommended to avoid using insulators that can easily build up static electricity. Semiconductor devices must be stored and transported in an anti-static container, static shielding bag or conductive material. All test and measurement tools including work benches and floors must be grounded. The operator must also be grounded using a wrist strap. Semiconductor devices must not be touched with bare hands. Similar precautions must be taken for printed circuit boards with mounted semiconductor devices.
2. Processing at power-on

   The state of the product is undefined at the time when power is supplied. The states of internal circuits in the LSI are indeterminate and the states of register settings and pins are undefined at the time when power is supplied. In a finished product where the reset signal is applied to the external reset pin, the states of pins are not guaranteed from the time when power is supplied until the reset process is completed. In a similar way, the states of pins in a product that is reset by an on-chip power-on reset function are not guaranteed from the time when power is supplied until the power reaches the level at which resetting is specified.
3. Input of signal during power-off state

   Do not input signals or an I/O pull-up power supply while the device is powered off. The current injection that results from input of such a signal or I/O pull-up power supply may cause malfunction and the abnormal current that passes in the device at this time may cause degradation of internal elements. Follow the guideline for input signal during power-off state as described in your product documentation.
4. Handling of unused pins

   Handle unused pins in accordance with the directions given under handling of unused pins in the manual. The input pins of CMOS products are generally in the high-impedance state. In operation with an unused pin in the open-circuit state, extra electromagnetic noise is induced in the vicinity of the LSI, an associated shoot-through current flows internally, and malfunctions occur due to the false recognition of the pin state as an input signal become possible.
5. Clock signals

   After applying a reset, only release the reset line after the operating clock signal becomes stable. When switching the clock signal during program execution, wait until the target clock signal is stabilized. When the clock signal is generated with an external resonator or from an external oscillator during a reset, ensure that the reset line is only released after full stabilization of the clock signal. Additionally, when switching to a clock signal produced with an external resonator or by an external oscillator while program execution is in progress, wait until the target clock signal is stable.
6. Voltage application waveform at input pin

   Waveform distortion due to input noise or a reflected wave may cause malfunction. If the input of the CMOS device stays in the area between V_{IL} (Max.) and V_{IH} (Min.) due to noise, for example, the device may malfunction. Take care to prevent chattering noise from entering the device when the input level is fixed, and also in the transition period when the input level passes through the area between V_{IL} (Max.) and V_{IH} (Min.).
7. Prohibition of access to reserved addresses

   Access to reserved addresses is prohibited. The reserved addresses are provided for possible future expansion of functions. Do not access these addresses as the correct operation of the LSI is not guaranteed.
8. Differences between products

   Before changing from one product to another, for example to a product with a different part number, confirm that the change will not lead to problems. The characteristics of a microprocessing unit or microcontroller unit products in the same group but having a different part number might differ in terms of internal memory capacity, layout pattern, and other factors, which can affect the ranges of electrical characteristics, such as characteristic values, operating margins, immunity to noise, and amount of radiated noise. When changing to a product with a different part number, implement a system-evaluation test for the given product.

Notice

1. Descriptions of circuits, software and other related information in this document are provided only to illustrate the operation of semiconductor products and application examples. You are fully responsible for the incorporation or any other use of the circuits, software, and information in the design of your product or system. Renesas Electronics disclaims any and all liability for any losses and damages incurred by you or third parties arising from the use of these circuits, software, or information.
2. Renesas Electronics hereby expressly disclaims any warranties against and liability for infringement or any other claims involving patents, copyrights, or other intellectual property rights of third parties, by or arising from the use of Renesas Electronics products or technical information described in this document, including but not limited to, the product data, drawings, charts, programs, algorithms, and application examples.
3. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
4. You shall be responsible for determining what licenses are required from any third parties, and obtaining such licenses for the lawful import, export, manufacture, sales, utilization, distribution or other disposal of any products incorporating Renesas Electronics products, if required.
5. You shall not alter, modify, copy, or reverse engineer any Renesas Electronics product, whether in whole or in part. Renesas Electronics disclaims any and all liability for any losses or damages incurred by you or third parties arising from such alteration, modification, copying or reverse engineering.
6. Renesas Electronics products are classified according to the following two quality grades: “Standard” and “High Quality”. The intended applications for each Renesas Electronics product depends on the product’s quality grade, as indicated below.
   "Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; industrial robots; etc.
   "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control (traffic lights); large-scale communication equipment; key financial terminal systems; safety control equipment; etc.

   Unless expressly designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not intended or authorized for use in products or systems that may pose a direct threat to human life or bodily injury (artificial life support devices or systems; surgical implantations; etc.), or may cause serious property damage (space system; undersea repeaters; nuclear power control systems; aircraft control systems; key plant systems; military equipment; etc.). Renesas Electronics disclaims any and all liability for any damages or losses incurred by you or any third parties arising from the use of any Renesas Electronics product that is inconsistent with any Renesas Electronics data sheet, user’s manual or other Renesas Electronics document.
7. No semiconductor product is absolutely secure. Notwithstanding any security measures or features that may be implemented in Renesas Electronics hardware or software products, Renesas Electronics shall have absolutely no liability arising out of any vulnerability or security breach, including but not limited to any unauthorized access to or use of a Renesas Electronics product or a system that uses a Renesas Electronics product. RENESAS ELECTRONICS DOES NOT WARRANT OR GUARANTEE THAT RENESAS ELECTRONICS PRODUCTS, OR ANY SYSTEMS CREATED USING RENESAS ELECTRONICS PRODUCTS WILL BE INVULNERABLE OR FREE FROM CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, DATA LOSS OR THEFT, OR OTHER SECURITY INTRUSION (“Vulnerability Issues”). RENESAS ELECTRONICS DISCLAIMS ANY AND ALL RESPONSIBILITY OR LIABILITY ARISING FROM OR RELATED TO ANY VULNERABILITY ISSUES. FURTHERMORE, TO THE EXTENT PERMITTED BY APPLICABLE LAW, RENESAS ELECTRONICS DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT AND ANY RELATED OR ACCOMPANYING SOFTWARE OR HARDWARE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.
8. When using Renesas Electronics products, refer to the latest product information (data sheets, user’s manuals, application notes, “General Notes for Handling and Using Semiconductor Devices” in the reliability handbook, etc.), and ensure that usage conditions are within the ranges specified by Renesas Electronics with respect to maximum ratings, operating power supply voltage range, heat dissipation characteristics, installation, etc. Renesas Electronics disclaims any and all liability for any malfunctions, failure or accident arising out of the use of Renesas Electronics products outside of such specified ranges.
9. Although Renesas Electronics endeavors to improve the quality and reliability of Renesas Electronics products, semiconductor products have specific characteristics, such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Unless designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not subject to radiation resistance design. You are responsible for implementing safety measures to guard against the possibility of bodily injury, injury or damage caused by fire, and/or danger to the public in the event of a failure or malfunction of Renesas Electronics products, such as safety design for hardware and software, including but not limited to redundancy, fire control and malfunction prevention, appropriate treatment for aging degradation or any other appropriate measures. Because the evaluation of microcomputer software alone is very difficult and impractical, you are responsible for evaluating the safety of the final products or systems manufactured by you.
10. Please contact a Renesas Electronics sales office for details as to environmental matters such as the environmental compatibility of each Renesas Electronics product. You are responsible for carefully and sufficiently investigating applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive, and using Renesas Electronics products in compliance with all these applicable laws and regulations. Renesas Electronics disclaims any and all liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
11. Renesas Electronics products and technologies shall not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable domestic or foreign laws or regulations. You shall comply with any applicable export control laws and regulations promulgated and administered by the governments of any countries asserting jurisdiction over the parties or transactions.
12. It is the responsibility of the buyer or distributor of Renesas Electronics products, or any other party who distributes, disposes of, or otherwise sells or transfers the product to a third party, to notify such third party in advance of the contents and conditions set forth in this document.
13. This document shall not be reprinted, reproduced or duplicated in any form, in whole or in part, without prior written consent of Renesas Electronics.
14. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products.

(Note1) “Renesas Electronics” as used in this document means Renesas Electronics Corporation and also includes its directly or indirectly controlled subsidiaries.
(Note2) “Renesas Electronics product(s)” means any product developed or manufactured by or for Renesas Electronics.

(Rev.5.0-1 October 2020)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

Contact information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
www.renesas.com/contact/.