AN234322

Getting started with AIROC™ IFW56810-00 single-band Wi-Fi 4 Cloud Connectivity Manager

About this document

Scope and purpose

This document guides the user to set up and connect the AWS IoT ExpressLink IFW56810-00 Cloud Connectivity Manager module to the AWS IoT Core in a few simple steps without involving any firmware development. This document also provides an overview of the module, the evaluation kit, steps to connect to the AWS Cloud, and usage of the AT command set.

Intended audience

Customers who are new to IoT and/or require a turnkey solution to get their products connected to the cloud.

Table of contents

Table of contents

1 Overview

AIROC™ IFW56810-00 Single-band Wi-Fi 4 Cloud Connectivity Manager Module (CCM) is a configurable Wi-Fi connectivity module that provides a simple, secure, plug-and-play solution for connecting products to AWS IoT cloud services. The IFW56810-00 CCM module is preprogrammed with a tested secured firmware and supports an easy-to-use AT command interface for configuration, and provides end-to-end security.

- The device identity certificate is built into the module and can run only Infineon-signed firmware.
- The module connects to the cloud using secure connections.
- Devices are managed securely in the cloud.

The IFW56810-00 CCM module features a 1x1 single-band (2.4 GHz) device operating at 20-MHz channels supporting IEEE 802.11 b/g/n. See the datasheet for details.

The host processor system interacts with the IFW56810-00 CCM module through AT commands over UART. The IFW56810-00 CCM module handles all networking-related operations to connect to the AWS IoT Core through MQTT over Wi-Fi.

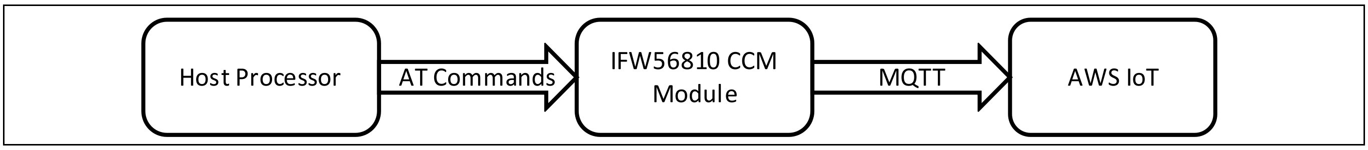


Figure 1 System architecture for products using the IFW56810-00 CCM module

2 Kit contents

- IFW956810 single-band Wi-Fi 4 Cloud Connectivity Manager evaluation kit to evaluate the IFW56810-00 single-band Wi-Fi 4 Cloud Connectivity Manager Module
- USB Type-A (male) to Type-C (female) cable
- Quick start guide

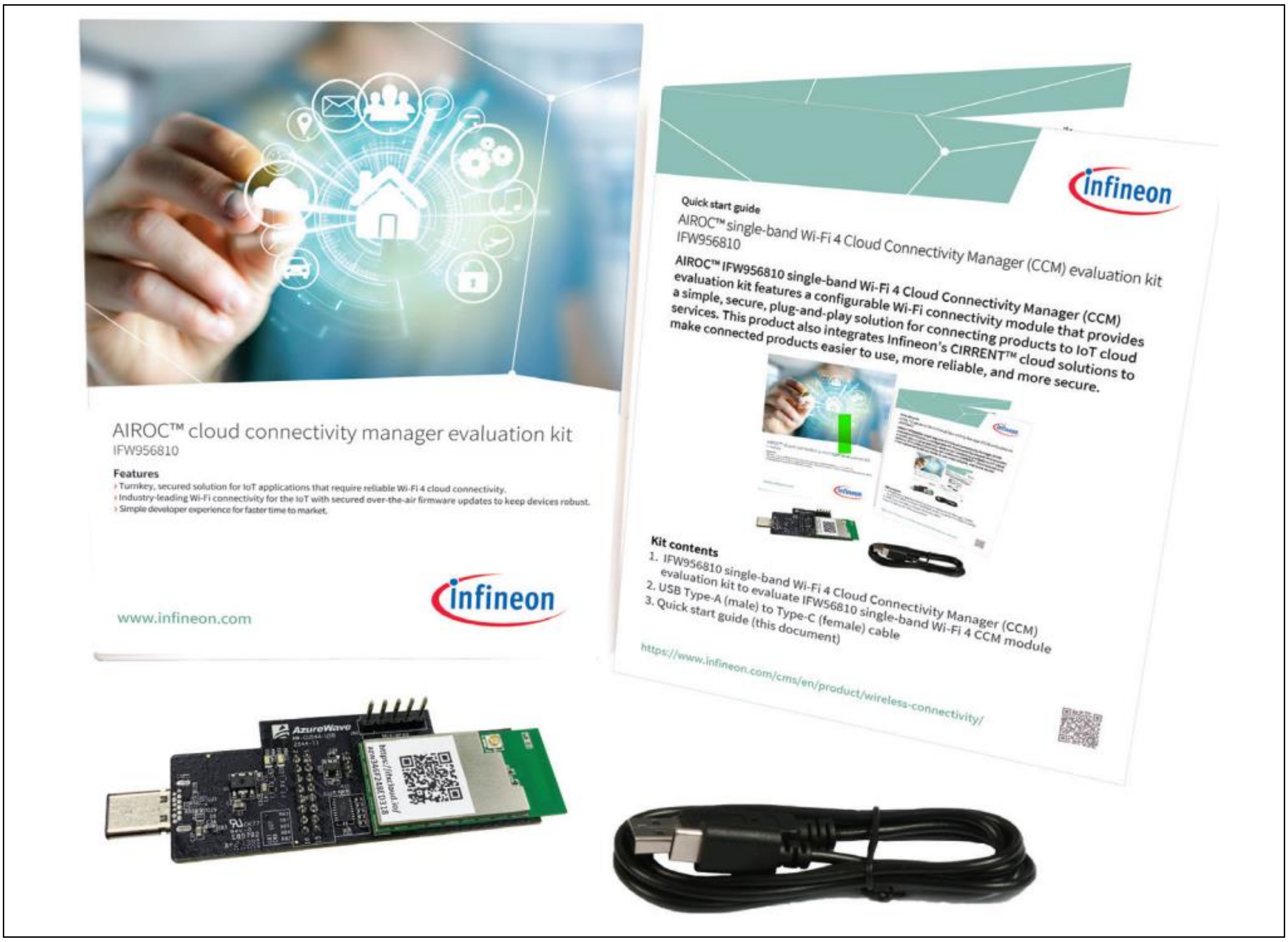

AIROC™ cloud connectivity manager evaluation kit
IFW956810
Features
Turnkey, secured solution for IoT applications that require reliable Wi-Fi 4 cloud connectivity.
Industry-leading Wi-Fi connectivity for the IoT with secured over-the-air firmware updates to keep devices robust.
Simple developer experience for faster time to market.
www.infineon.com
infineon
Quick start guide
AIROC™ single-band Wi-Fi 4 Cloud Connectivity Manager (CCM) evaluation kit
IFW956810
AIROC™ IFW956810 single-band Wi-Fi 4 Cloud Connectivity Manager (CCM) evaluation kit features a configurable Wi-Fi connectivity module that provides a simple, secure, plug-and-play solution for connecting products to IoT cloud services. This product also integrates Infineon's CIRRENT™ cloud solutions to make connected products easier to use, more reliable, and more secure.
Kit contents
1. IFW956810 single-band Wi-Fi 4 Cloud Connectivity Manager (CCM) evaluation kit to evaluate IFW56810 single-band Wi-Fi 4 CCM module
2. USB Type-A (male) to Type-C (female) cable
3. Quick start guide (this document)
https://www.infineon.com/cms/en/product/wireless-connectivity/
AzureWave

Figure 2 Kit contents

Note: *Follow the quick start guide provided along with the Kit before starting with the current document.*

3 Hardware

The IFW956810 CCM evaluation kit consists of an IFW56810-00 single-band Wi-Fi 4 Cloud Connectivity Manager module with secure processor, a PCB antenna, an FTDI chip for the USB to serial interface, and an 8x2 pin header.

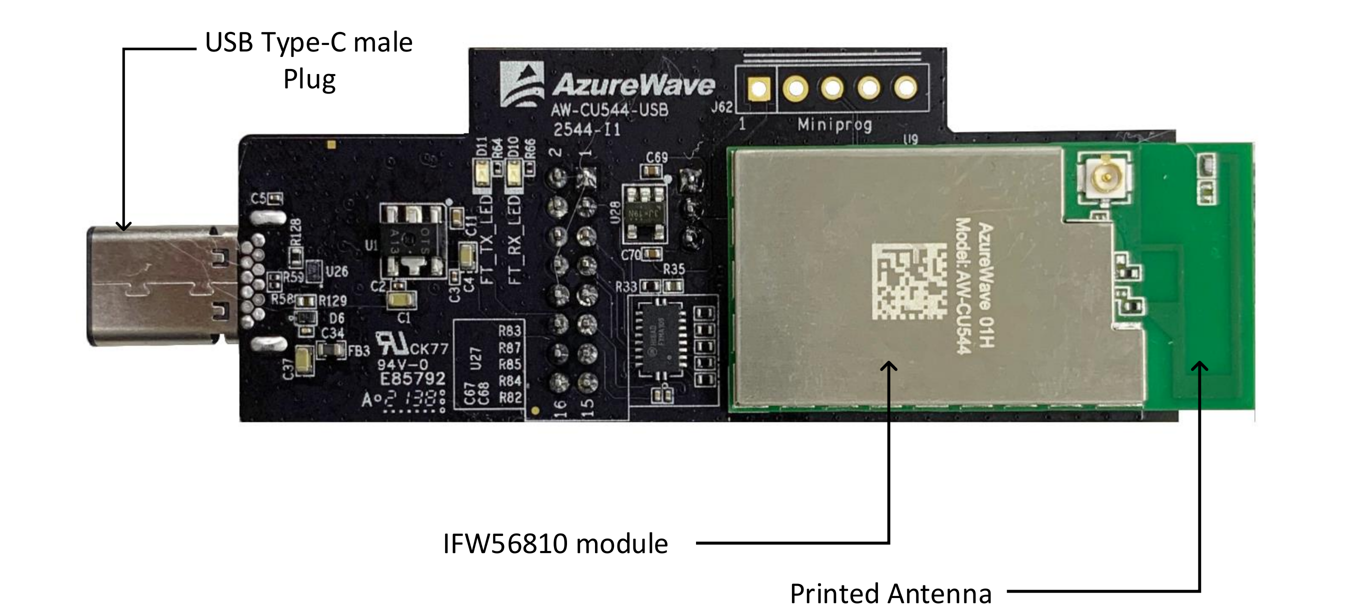


Figure 3 Top view

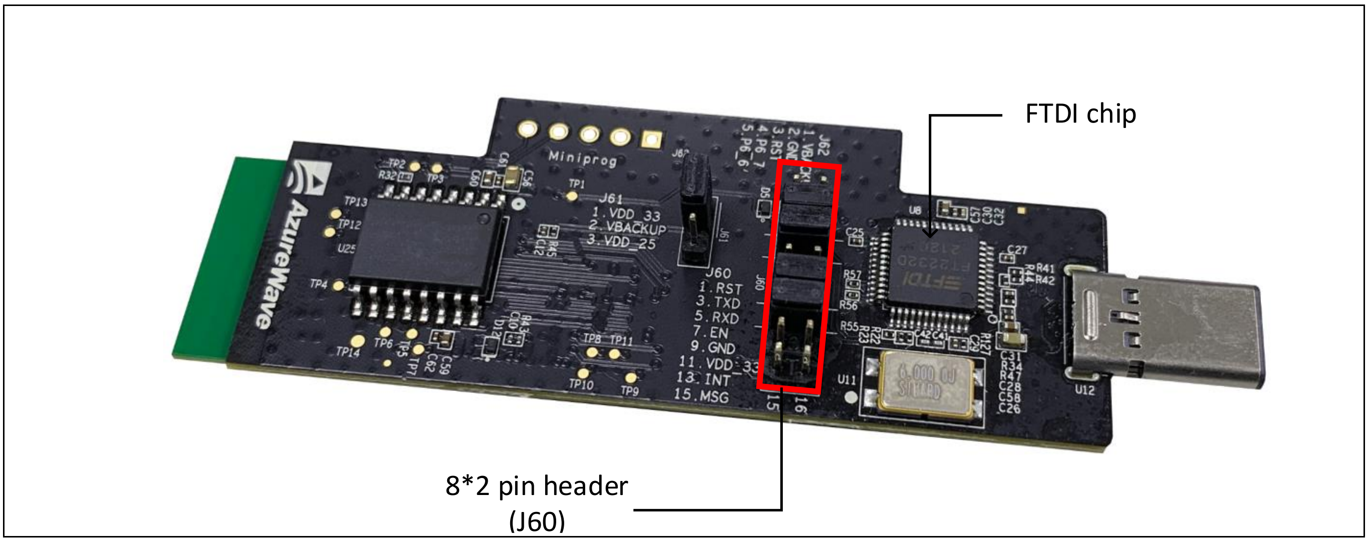


Figure 4 Bottom view

Ensure that pin 3 to pin 4, pin 5 to pin 6, pin 9 to pin 10, and pin 11 to pin 12 of header J60 are closed before connecting the USB dongle to the PC (see Figure 4). The PC can be used as a host for evaluation. AT commands can be sent through a serial terminal on the PC to the IFW956810 CCM kit.

3.1 Connect the kit to the PC

Connect the IFW956810 Single-band Wi-Fi 4 Cloud Connectivity Manager evaluation kit to the PC using either the Type-C connector or Type-A male to Type-C female cable.

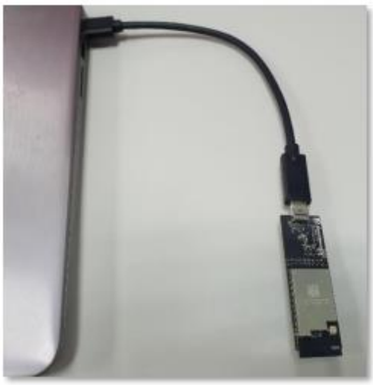


Figure 5 Connect the USB dongle to the PC

4 Setting up a serial terminal on the PC

Note: *The following instructions are only for a Windows PC.*

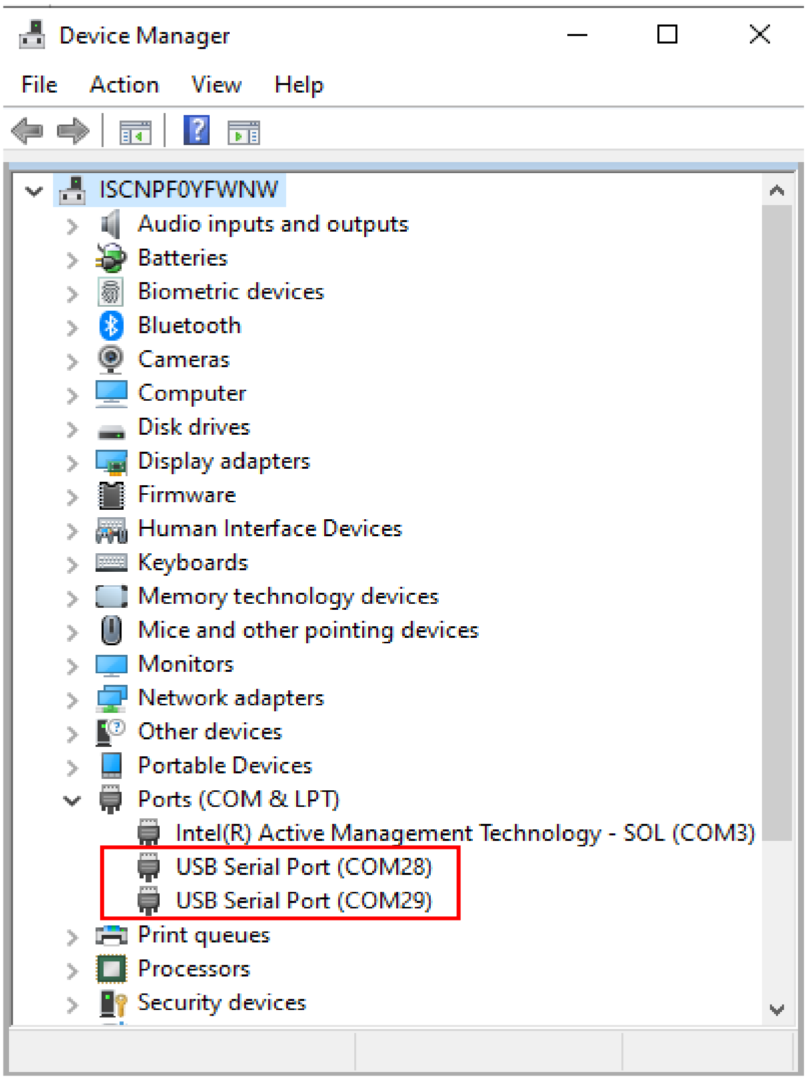
The IFW956810 CCM evaluation kit should be recognized by the PC when connected to it. If the device is recognized, the COM ports will be available in the Device Manager.

If the device is not recognized, you need to install the FTDI USB-to-UART Bridge Virtual Communication Port drivers from the VCP Drivers webpage.

4.1 Determine the COM port number

- In Windows, determine the COM port number from the Device Manager.

Note: *Use the higher-number COM port among the enumerated COM ports to communicate with the kit.*



Device Manager

File Action View Help

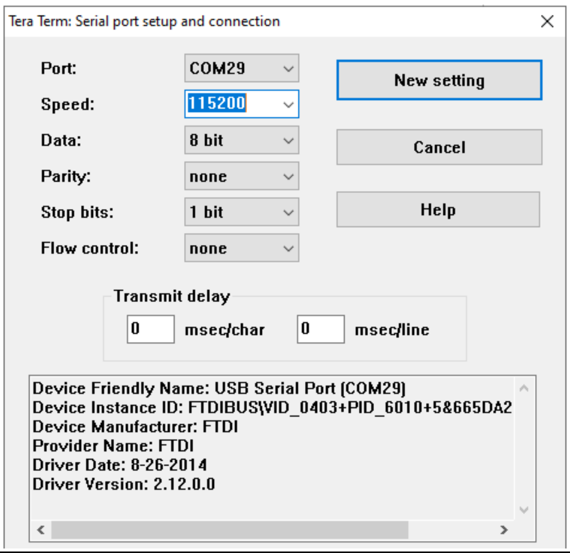
ISCNPF0YFWNW
- Audio inputs and outputs
- Batteries
- Biometric devices
- Bluetooth
- Cameras
- Computer
- Disk drives
- Display adapters
- Firmware
- Human Interface Devices
- Keyboards
- Memory technology devices
- Mice and other pointing devices
- Monitors
- Network adapters
- Other devices
- Portable Devices
- Ports (COM & LPT)
  - Intel(R) Active Management Technology - SOL (COM3)
  - USB Serial Port (COM28)
  - USB Serial Port (COM29)
- Print queues
- Processors
- Security devices

Figure 6 COM port

4.2 Serial terminal settings

Note: Tera Term is not available for Linux/macOS but there are some alternatives such as PuTTY, which have the same functionality as Tera Term, and are both free and Open Source.

1. Open a terminal such as Tera Term.
2. Choose the higher of the COM port numbers for the IFW956810 CCM evaluation kit.
3. Select **Set Up** > **Serial port.**
4. Select the following settings (see Figure 7):
   - Port: **COM29**
   - Speed: **115200**
   - Data: **8 bit**
   - Parity: **none**
   - Stop bits: **1 bit**
   - Flow control: **none**



Port: COM29
Speed: 115200
Data: 8 bit
Parity: none
Stop bits: 1 bit
Flow control: none

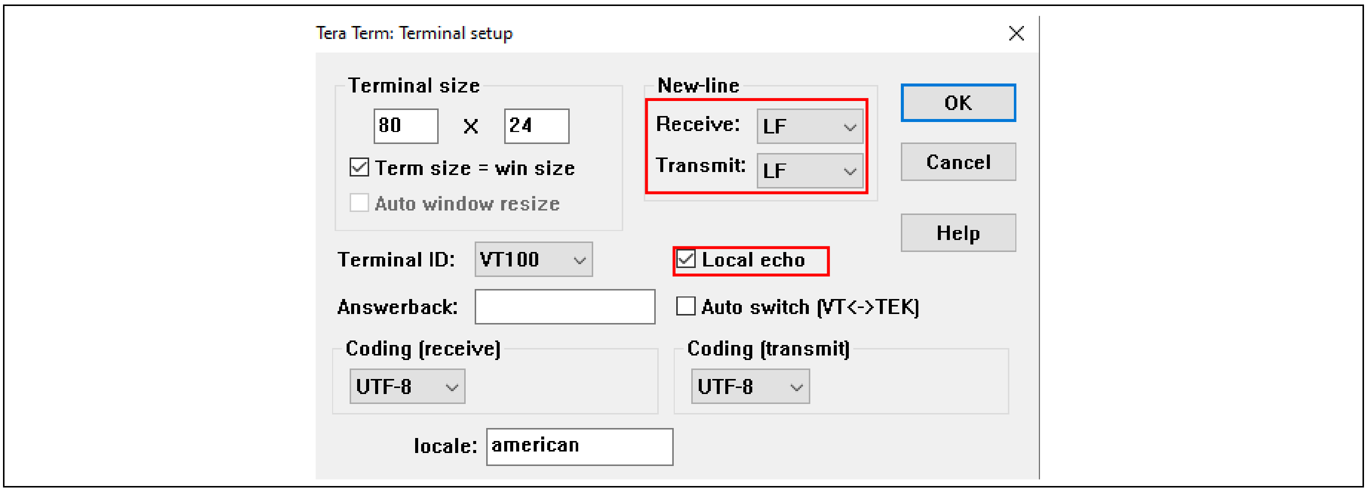
Transmit delay
0 msec/char 0 msec/line

Device Friendly Name: USB Serial Port (COM29)
Device Instance ID: FTDIBUS\VID_0403+PID_6010+5&665DA2
Device Manufacturer: FTDI
Provider Name: FTDI
Driver Date: 8-26-2014
Driver Version: 2.12.0.0

Figure 7 Serial port setup and connection

5. Select **Set Up** > **Terminal**.
6. Do the following:
   - Set **End of Line** as **Line Feed**.
   - Enable **Local Echo** to view the commands that you type on the terminal.

Setting up a serial terminal on the PC



Tera Term: Terminal setup

Terminal size

80 × 24

☑ Term size = win size

☐ Auto window resize

New-line

Receive: LF

Transmit: LF

Terminal ID: VT100

☑ Local echo

Answerback:

☐ Auto switch (VT<->TEK)

Coding (receive): UTF-8

Coding (transmit): UTF-8

locale: american

After you open the serial terminal, type the following in the serial terminal:

```
AT+CONF? About
```

Observe the following response:

```
“OK Infineon - IFW56810”.
```

5 Getting started with using an AWS account

Connect the IFW956810 single-band Wi-Fi 4 Cloud Connectivity Manager evaluation kit to the PC as mentioned in the Connect the kit to the PC section.

Follow the steps mentioned in the subsections of the Creating the AWS account and permissions section if you connect the kit for the first time. The IFW56810-00 module remembers its configuration and will be ready to connect to the AWS account automatically.

5.1 Creating the AWS account and permissions

Follow the instructions in the Amazon documentation (Set up your AWS Account) to create the account and get started:

1. Sign up for an AWS account or log in to the existing account.
2. Open the AWS IoT console.

5.1.1 AWS flow

The following steps will help you register the respective kit to the AWS account.

5.1.1.1 Create the policy

1. Open the AWS IoT Console.
2. From the left pane, select **Security**, and then select **policies**.
3. Click **Create** to create a policy. This opens a new tab.
4. Enter the policy name (e.g., “IoTDevPolicy”) and click **JSON** under policy statements tab.
5. Copy the following section into the console:

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

Note: The examples in this document are intended only for development environments. All devices in the end product 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.

6. Click **Create**.

5.1.1.2 Configure the AWS Thing

1. Open the AWS IoT Console.
2. From the left pane, select **Manage**, and then select **Things**.
3. Click **Create Things**.
4. On the **Create things** page, select **Create single thing**, and then click **Next**.
5. In the terminal application, type the following command:

```
AT+CONF? ThingName
```

6. Copy the returned string (a sequence of alphanumeric characters) from the terminal.
7. On the console, on the **Specify thing properties** page, paste the copied string from the terminal into the **Thing name** field under **Thing properties**.

8. Leave other fields at their default values, and then click **Next**.

5.1.1.3 Configure device certificate

5.1.1.3.1 Prepare device certificate

1. In the terminal application, type the following command:

   ```
   AT+CONF? Certificate pem
   ```

   You will receive the device certificate in PEM format as part of the response.

2. Copy the returned string (a longer sequence of alphanumeric symbols), and save it into a text file on your host machine as "ThingName.cert.pem".

   Replace "ThingName" with the name of the Thing obtained in the Configure the AWS Thing section.

5.1.1.3.2 Attach device certificate to the Thing

1. On the **Configure device certificate** page in the AWS Console, select **Use my certificate**, and then choose **CA is not registered with AWS IoT**.
2. Under Certificate, select **Choose file**.
3. Double-click the *ThingName.cert.pem* file created in the Prepare device certificate section.
4. Under Certificate Status, select **Active**.
5. Click **Next**.

5.1.1.4 Attach policies to certificate

1. Select the Policy created using the steps in the Create the policy section.
2. Click **Create**.

5.1.1.5 Configure endpoint

1. In the AWS IoT Console, choose **Settings**, and then copy your account endpoint string under **Device data endpoint**.
2. Type the following AT command in the serial terminal to configure the endpoint:

   ```
   AT+CONF Endpoint= endpoint copied in step 1.
   ```

   The above step replaces the configured default endpoint used for evaluating the quick connect flow .

5.2 Connect the kit to Wi-Fi

A Wi-Fi onboarding mechanism is required for IoT products that do not have a display to enter Wi-Fi SSID and password.

Note: *Connect the kit only to a 2.4-GHz Wi-Fi network.*

5.2.1 Using AT commands

AT commands provide a simple method of Wi-Fi onboarding in a development environment.

Type the following commands in sequence in the terminal application:

```
AT+CONF SSID=<your router ssid>
AT+CONF Passphrase=<your router passphrase>
```

Note: *The local router's SSID and passphrase are stored securely inside the IFW56810-00 CCM module. While the SSID can be retrieved later (i.e., for debugging purposes), any attempt to retrieve the passphrase will return an error.*

5.3 Connect and interact with the AWS Cloud

Use the MQTT client in the AWS IoT Console to monitor the communication between your evaluation kit and the AWS Cloud.

1. Navigate to the AWS IoT Console (https://console.aws.amazon.com/iot/).
2. In the navigation pane, select **Test** and then click **MQTT Test Client**.
3. Navigate to the additional configuration and select Display payloads as strings (these are more accurate) under the MQTT payload display.
4. In **Subscribe to a topic** panel, enter #, and then click **Subscribe**.

5.3.1 Connect to the AWS IoT Core

Enter the following command in the serial terminal to establish a secure connection to the AWS IoT Core if you followed AWS flow

```
AT+CONNECT
```

After a few seconds, the device will connect to the AWS IoT Core and you will receive the message

```
"OK 1 CONNECTED"
```

6 AT commands to send and receive data

Wait for a response from the IFW956810 CCM evaluation kit in the serial terminal after entering each AT command.

6.1 Publish to a topic

Enter the following commands in sequence in the serial terminal:

```
AT+CONF Topic1=/MyPubTopic
AT+SEND1 hello world
```

The **Hello world** message gets dispayed on the AWS IoT console.

6.2 Subscribe to a topic

1. Enter the following commands in sequence in the serial terminal:

   ```
   AT+CONF Topic2=/MySubTopic
   AT+SUBSCRIBE2
   ```

2. Do the following on the AWS IoT Console:

   a) Select the MQTT test client and type `/MySubTopic` in the **Topic filter** and press **Subscribe** .

   b) Then go to **Publish to a topic** tab and type `/MySubTopic` in the **Topic name** field. Keep the "Hello from the AWS IoT Console" message.

   c) Click **Publish**.

3. On your serial terminal, enter the following command:

   ```
   AT+GET2
   ```

   You will receive the following message:

   "OK Hello from the AWS IoT Console".

Note: The IFW56810-00 CCM module is capable of queuing 32 MQTT messages from AWS IoT core.

7 Low-power modes

7.1 Prerequisites

Before trying the low-power modes, ensure that the IFW56810-00 CCM module is not connected to Wi-Fi. To disconnect the device. enter the following command in the serial terminal:

```
AT+DISCONNECT
```

7.2 System sleep mode

To put the IFW56810-00 CCM module to System Sleep mode for a particular duration, enter the following command:

```
AT+SLEEP <Sleep time in seconds>
```

For example, AT+SLEEP 10 puts the device in Sleep mode for 10 seconds.

Enter the following command to put the device in System Sleep mode indefinitely till it receives an external interrupt:

```
AT+SLEEP
```

In System Sleep mode the device stays in Sleep state until it receives any external interrupt.

External interrupt can be triggered through sending any AT command or using device reset (using RST pin) or triggering the WAKE (INT) pin.

7.3 Deep Sleep mode

Enter the following command to put the device in Deep Sleep mode:

```
    AT+SLEEP1
```

The device stays in Deep Sleep state until the device is reset (using the RST pin) or wake pin is triggered.

Note: *The RST pin is pulled up by a 4.7-kΩ resistor internally; deasserting the pin will reset the module.*

The Wake pin can be triggered by a falling edge (HIGH to LOW). By default, the Wake pin is in high-impedence state.

8 Performing firmware over-the-air update

8.1 Prerequisites

Get the signed updated firmware image from the ccm-ota-image-update GitHub page.

To create an OTA update role in the AWS account, see the Create an OTA Update service role webpage .

8.2 Create a firmware update job in AWS IoT

1. Open AWS IoT Console.
2. Click **Manage**, and then under **Remote actions** click **Jobs**.
3. Click **Create job.**
4. Select **Create FreeRTOS OTA Update Job**, and then click **Next**.
5. Provide a job name which is unique within your AWS account. Optionally, provide a description, and then click **Next**.
6. From the **Devices to update** drop-down list, choose the Thing name with which the IFW56810-00 CCM module is registered in the account.
7. Select **MQTT** as the transfer protocol, and deselect **HTTP** if selected.
8. Select **Use my custom signed file.**
9. On the form that appears, enter the details from the Prerequisites section. Do the following:
   - In the **signature** field, provide the base64-encoded signature for the image.
   - From the **Original hashing algorithm** drop-down list, select the hashing algorithm provided by Infineon.
   - From the **Original encryption algorithm** drop-down list, select the encryption algorithm provided by Infineon.
   - In the **Path name of code signing certificate on device**, field, enter `NA`.
10. Select **Upload a new file**.
11. Click **Choose file** and upload the image received from Infineon.
12. Do one of the following:
    - Click **Create S3 bucket** to create a new bucket for the new uploaded image.
    - Click **Browse S3** to select an existing bucket in your account.
13. Under **Path Name of file on device**, enter `NA` if the image is not targeted as an executable file within a filesystem.
14. From the **File type** drop-down list, select a value “101” to signify that it is an IFW56810-00 CCM firmware update, and not a host firmware update.
15. Choose the OTA update role created above from the **Role** drop-down list under the **IAM role** section, and then click **Next**.
16. Click **Create Job**.

If successful, the job will be listed with the status as “in progress”.

8.3 Monitor and apply the new firmware update for the IFW56810-00 module

The IFW56810-00 CCM module polls for firmware update jobs, receives and validates a job, and then enters a state waiting for the update to be accepted. The host application receives an OTA event indicating that a new firmware image is available for the IFW56810-00 CCM module.

The host application or the user can perform the following sequence by entering appropriate commands in the serial terminal:

1. Check the image version running on the CCM Module before doing OTA using the following AT command:

   ```
   AT+CONF? Version
   ```

2. Query the state of the job:

   ```
   AT+OTA?
   ```

   You will receive a response “OK 1”

3. Accept the new firmware update using the following command:

   ```
   AT+OTA ACCEPT
   ```

   The IFW56810-00 CCM module starts downloading the firmware update from the cloud.

4. Query the state of the job:

   ```
   AT+OTA?
   ```

   Downloading the image takes a few minutes to complete. During the OTA image download, this command returns “OK 3”. You will receive an OTA event when the download is completed the image signature is verified.

5. Check whether the OTA image is received:

   ```
   AT+OTA?
   ```

   You will receive the response “OK 4”.

6. Apply the new image received through OTA using the following:

   ```
   AT+OTA APPLY
   ```

   Now, the IFW56810-00 CCM module reboots and boots up with the new image.

7. To confirm whether the new image is updated, check the image version using the following AT command:

   ```
   AT+CONF? Version
   ```

8. Connect back to the AWS IoT using the following command:

   ```
   AT+CONNECT
   ```

The IFW56810-00 CCM module should now connect to AWS IoT, complete the self-test and mark the image as valid. This prevents further rollback to the old image.

You can check the job status by going back to the AWS IoT Console. You should see the job status as completed.

9 Performing host firmware over-the-air update

The IFW56810-00 CCM module supports the host firmware over-the-air updates. To do so, follow these steps.

Skip the prerequisites if you already have the OTA update role in the AWS account.

9.1 Prerequisites

To create an OTA update role in the AWS account, see the Create an OTA Update service role webpage.

9.2 Create a firmware update job in AWS IoT

1. Open AWS IoT Console.
2. Click **Manage**, and then under **Remote actions** click **Jobs**.
3. Click **Create job.**
4. Select **Create FreeRTOS OTA Update Job**, and then click **Next**.
5. Provide a job name which is unique within your AWS account. Optionally, provide a description, and then click **Next**.
6. From the **Devices to update** drop-down list, choose the Thing name with which the IFW56810-00 CCM module is registered in the account.
7. Select **MQTT** as the transfer protocol, and deselect **HTTP** if selected.
8. Select **Use my custom signed file.**
9. On the form that appears:
   - In the **signature** field, provide the base64-encoded signature for the image. If the image is not signed, enter `NA`.
   - From the **Original hashing algorithm** drop-down list, select the hashing algorithm. If not used, leave it as is.
   - From the **Original encryption algorithm** drop-down list, select the encryption algorithm. If not used, leave it as is.
   - In the **Path name of code signing certificate on device** field, enter `NA`.
10. Select **Upload a new file**.
11. Click **Choose file** and upload the image.
12. Do one of the following:
    - Click **Create S3 bucket** to create a new bucket for the new uploaded image.
    - Click **Browse S3** to select an existing bucket in your account.
13. Under **Path Name of file on device**, enter `NA` if the image is not targeted as an executable file within a filesystem.
14. From the **File type** drop-down list, select a value “202” to signify that it is an IFW56810-00 CCM host firmware update.
15. Choose the OTA update role created above from the **Role** drop-down list under the **IAM role** section, and then click **Next**.
16. Click **Create Job**.

9.3 Monitor and load the firmware update to the host

The host application or the user can perform the following sequence by entering appropriate commands in the serial terminal:

1. Query the state of the job:

   ```
   AT+OTA?
   ```

   You will receive a response “OK 2”

2. Accept the new firmware update:

   ```
   AT+OTA ACCEPT
   ```

The IFW56810-00 CCM module starts downloading the firmware update from the cloud

3. Query the state of the job:

   ```
   AT+OTA?
   ```

Downloading the image takes a few minutes to complete. During the HOTA image download, this command returns “OK 3”. Once the image is downloaded this command will return “OK 5”

4. The host can send the following command to the IFW56810-00 CCM module to receive the image

```
AT+OTA READ <read size>
```

This command responds with “OK {count} {data} {checksum}”

The byte count is expressed in hex (from 1 to 6 digits), each byte is then presented as a pair of hex digits (no spaces) for a total of count*2 characters followed by a checksum (4 hex digits). The reading pointer is advanced by *count* bytes.

Note: The IFW56810-00 CCM module can read up to 2 KB at once. If the size of the host image is greater than 2 KB, the host needs to perform multiple AT+OTA READ commands with a specified read size.

10 Troubleshooting

10.1 Two COM ports enumerated when the kit is connected

The IFW956810 CCM evaluation kit has a FT2232H chip capable of supporting USB to dual-channel UART (USB serial converter A and USB serial converter B). Only USB serial converter B is configured in the kit for USB-to-UART conversion. Therefore, use the higher-number COM port among the enumerated COM ports to communicate with the kit.

10.2 Errors when commands are entered

For example:

```
AT+SUBCRIBE2
ERR3 COMMAND NOT FOUND
```

1. Make sure that the typed command is correct.
2. Note the error codes and see the AWS IoT ExpressLink Programmer's Guide for details of the error code and to determine the cause.

10.3 Change the Wi-Fi network connected

1. Execute AT+DISCONNECT on the serial terminal to disconnect from the current Wi-Fi network.
2. To configure the required Wi-Fi credentials, see Connect the kit to Wi-Fi.

10.4 ERR14 2 UNABLE TO CONNECT [Wi-Fi Connection failed] error for the AT+CONNECT command

The `AT+CONNECT` command first connects to Wi-Fi, if not already connected, and then connects to the AWS IoT Core.

1. Check the Wi-Fi connection.
2. Check the entered Wi-Fi credentials.
3. Type the following command to verify whether the kit connects to Wi-Fi:

   ```
   AT+DIAG PING 8.8.8.8
   ```

   If the connection is successful, the device will respond with “OK Received ping response in <ping latency ms>”.

10.5 ERR14 5 UNABLE TO CONNECT MQTT device authentication failure error for the AT+CONNECT command

The `AT+CONNECT` command first connects to Wi-Fi if not already connected and then connects to the AWS IoT Core.

1. Check the AWS endpoint.
2. Check the device certificate uploaded to the AWS IoT Core and the device certificate present in the CCM device.

10.6 Other supported AT commands

Use the following command to initiate a ping to a given IPv4 address from the CCM module:

```
    AT+DIAG PING X.X.X.X
```
X.X.X.X - IPv4 address

Enable the logs using the following AT command:

```
    AT+DIAG LOG 5
```

Disable the logs using the following AT command:

```
    AT+DIAG LOG 0
```

Use the following command to initiate a SCAN of nearby Wi-Fi access points with a timeout of X seconds from the CCM module:

```
    AT+DIAG SCAN X
```

Disconnects the device (if connected) and resets its internal state. Non-persistent configuration parameters are reinitialized, all subscriptions are terminated, and the message queue is emptied.

```
    AT+RESET
```

Performs a full factory reset of the ExpressLink module, including re-initializing all non-persistent configuration parameters and selected persistent parameters, and empties the message queue.

```
    AT+FACTORY_RESET
```

For more details on which configuration parameters are persistent or non-persistent, see the refer to the following:

- https://docs.aws.amazon.com/iotexpresslink/latest/programmersguide/elpg-configuration-dictionary.html#elpg-table3

11 References

For connecting the CCM IFW956810 evaluation kit to the MCU, see the following:

- How to connect the AIROC™ IFW956810 CCM evaluation kit to the MCU development system - KBA236179

See the following for code examples using CCM and CY8CKIT-062s2-43012 as the host microcontroller

- AIROC™ CCM MQTT-PUBLISH-CAPSENSE-SLIDER
- AIROC™ CCM MQTT-OTA-SUBSCRIBE
- AIROC™ CCM MQTT HELLO WORLD

See the following link for AWS ExpressLink spec.

- AWS IoT ExpressLink Programmer's Guide

See the following for the videos explaining the different sections of the GSG:

- TBD

Revision history

Document revision	Date	Description of changes
**	2021-11-29	Initial release
*A	2021-12-24	Added Infineon CIRRENT Cloud flow to register the kit to the AWS account
*B	2022-09-22	Added the following sections to showcase new features of CCM: • Quick evaluation of the CCM device • Low-power modes • Performing host firmware over-the-air update Updated the following sections as per new Infineon Cirrent Cloud ID GUI and latest CCM firmware: • Register the kit to your AWS development account • AT commands to send and receive data Added References. Updated the following sections to improve readability: • Kit contents • Troubleshooting
*C	2023-05-03	Updated the following sections to improve the readability: • Register the kit to your AWS development account • Troubleshooting Changed the module name from IFW56810 to IFW56810-00.
*D	2023-10-16	Removed Infineon CIRRENT Cloud flow.

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2023-10-16

Published by

Infineon Technologies AG
81726 Munich, Germany

Do you have a question about this document?

Email: erratum@infineon.com

Document reference
002-34322 Rev. *D

Important notice
The information contained in this application note is given as a hint for the implementation of the product only and shall in no event be regarded as a description or warranty of a certain functionality, condition or quality of the product. Before implementation of the product, the recipient of this application note must verify any function and other technical information given herein in the real application. Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind (including without limitation warranties of non-infringement of intellectual property rights of any third party) with respect to any and all information given in this application note.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

Warnings
Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.