

**Trust-Fi User Guide**

**September 8, 2020**

Copyright © 2020 ICTK Holdings Co., Ltd. All Rights Reserved

Table of Contents

[Trust-Fi OTA update 3](#_Toc50472464)

[Setting Trust-Fi OTA 8](#_Toc50472465)

[Starting Trust-Fi OTA 9](#_Toc50472466)

[Wifi disconnect error 10](#_Toc50472467)

Trust-Fi OTA update

Trust-Fi now supports secure Over-the Air firmware updates with Amazon. With ICTK’s PUF based-security chip, Trust-Fi authenticates and securely deploy new firmware images to the IoT device.

Connect to AWS IoT Core with MQTT and TLS

\* Implementation based on MQTT version 3.1.1 and TLS 1.2 with

ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 cipher suite.

\* private key and certificates are encrypted in HW-based security chip, supports enhanced secured

working structure.

Configuring Amazon Web Services for OTA updates

1. Log in to the [AWS Management Console](https://aws.amazon.com/console/)
2. Create S3 bucket  where the OTA update files are stored.
3. Use the bucket name starts ‘afr-ota’ ex. afr-otaXXXXX
4. Sign in to IAM service and make sure user has proper role to access IoT and S3
5. Create OTA Update Service role and select type of trusted entity as ‘IoT’ , click next.
6. For your OTA update Service role, attach below policies

https://docs.aws.amazon.com/ko\_kr/freertos/latest/userguide/create-service-role.html

* 1. OTA update policy – AmazonFreeRTOSOTAUpdate
  2. IAM role for OTA update

1. Apply permission to IAM user for with S3 bucket and OTA Update Service role

<https://docs.aws.amazon.com/ko_kr/freertos/latest/userguide/create-ota-user-policy.html>

1. Apply permission to IAM user for Code Signing for IoT

https://docs.aws.amazon.com/freertos/latest/userguide/code-sign-policy.html

On the Device Side

1. Configure the device with proper Wi-fi information and application specific settings in order to connect with the AW IoT message broker

- Wifi configuration command

*AT+WIFI\_SSID\_STA=wifi\_SSID*

*AT+ WIFI\_PW\_STA=wifi \_PW*

- AWS configuration command

*AT+AWS\_EP=aws\_host\_url*

*AT+AWS\_PN=port\_number*

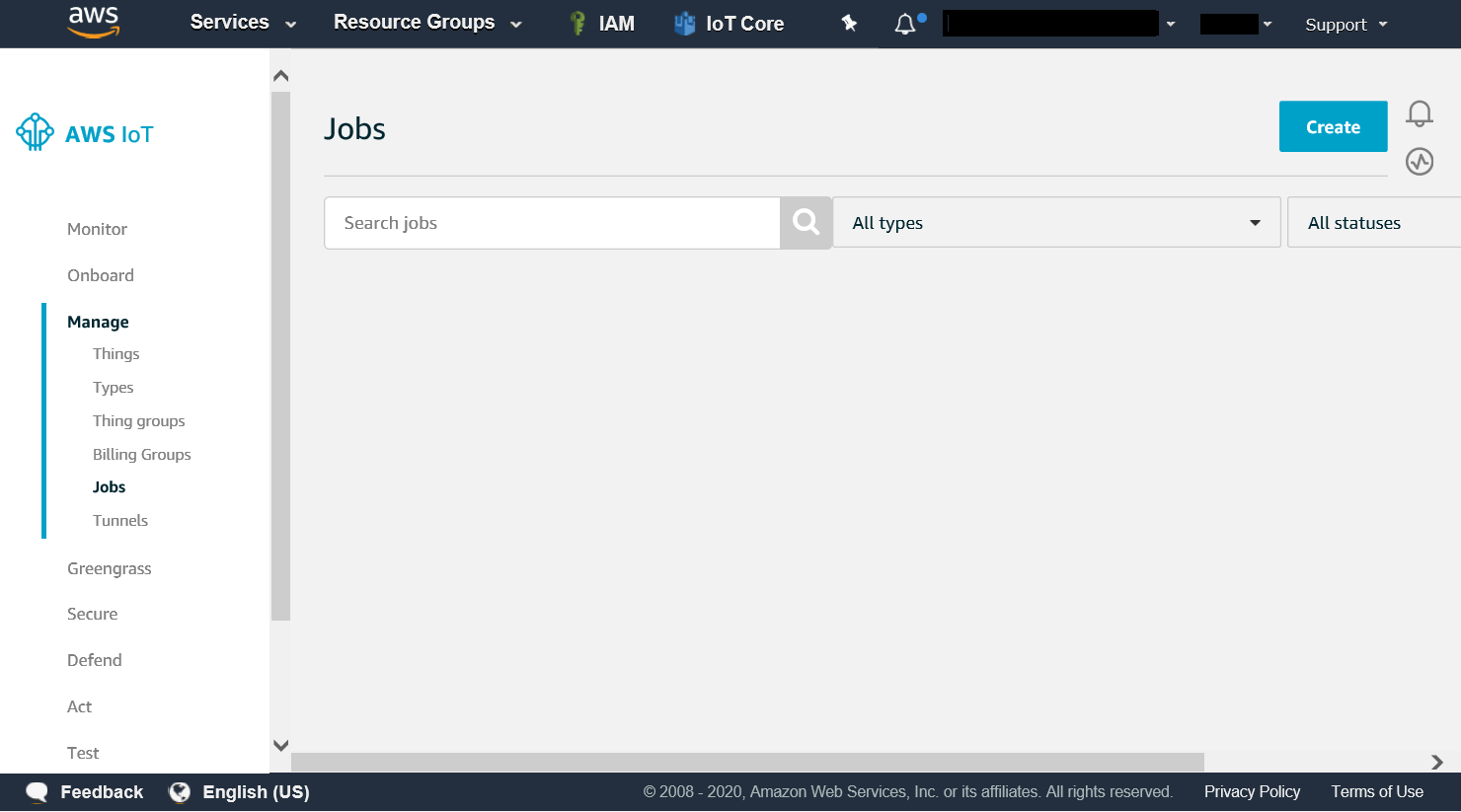
*AT+AWS\_TN=thing name*

*AT+AWS\_CID=cleintID*

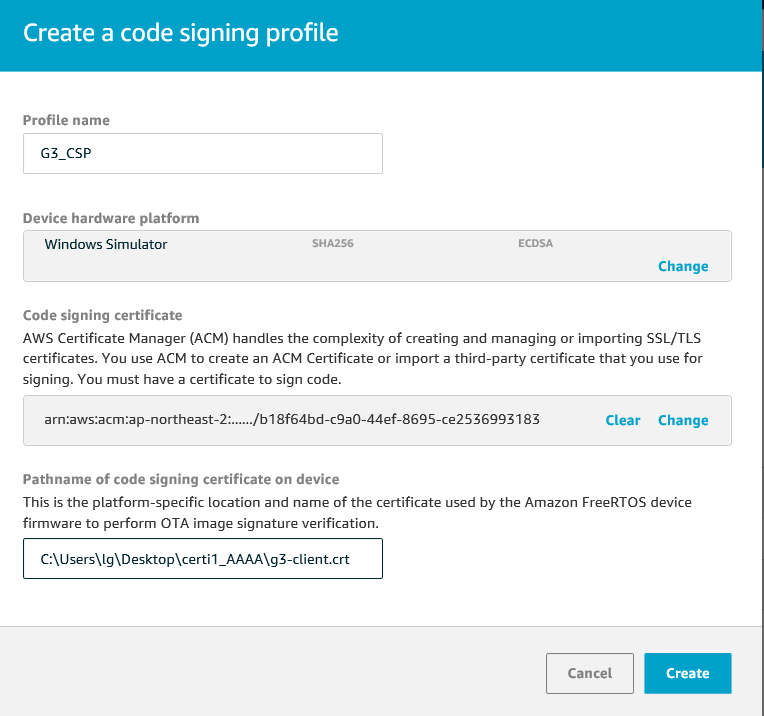
1. Trust-Fi contains amazon root CA, client certificate and private key already installed in PUF chip. The basic certificate is installed, but can be renewed or added upon request.
2. Make sure Code Singing Key is stored in G3 for verification for secure boot and update

Performing OTA update from AWS Console

1. Choose  IoT Core service
2. In the left navigation panel, click on Manage/Jobs



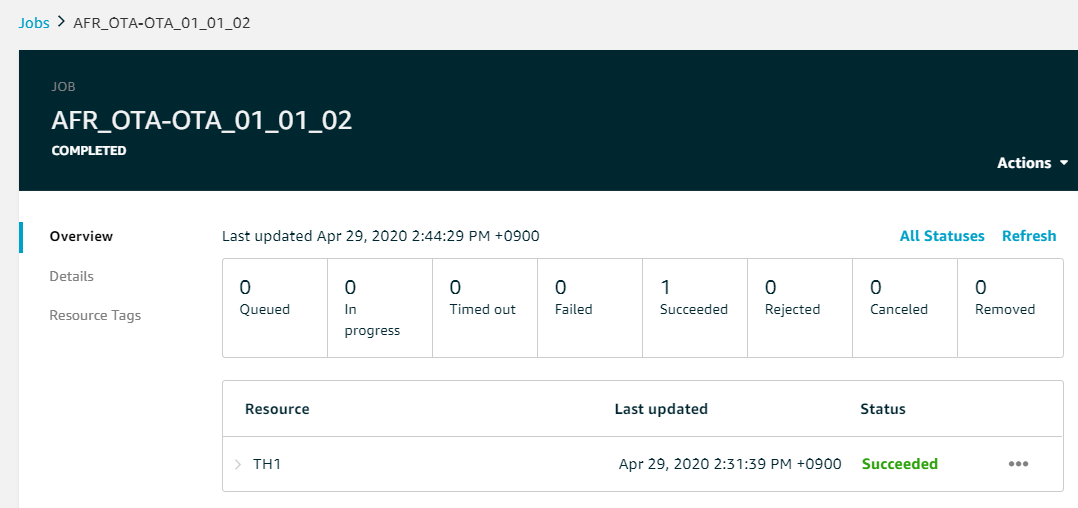
1. Click on Create button to ‘Create a FreeRTOS OTA update job ‘
2. Select devices – the one assigned for Trust-Fi
3. Choose HTTP protocol for firmware image transfer
4. Select ‘Sign a new firmware image for me’
5. Create a code signing profile
   1. Upload certification, private key and root certificate to create code signing profile.
   2. Use window simulator for this setup
   3. The pathname for code signing certification will not be used- G3 will take care of its verification. Please write down any pathname for this case.

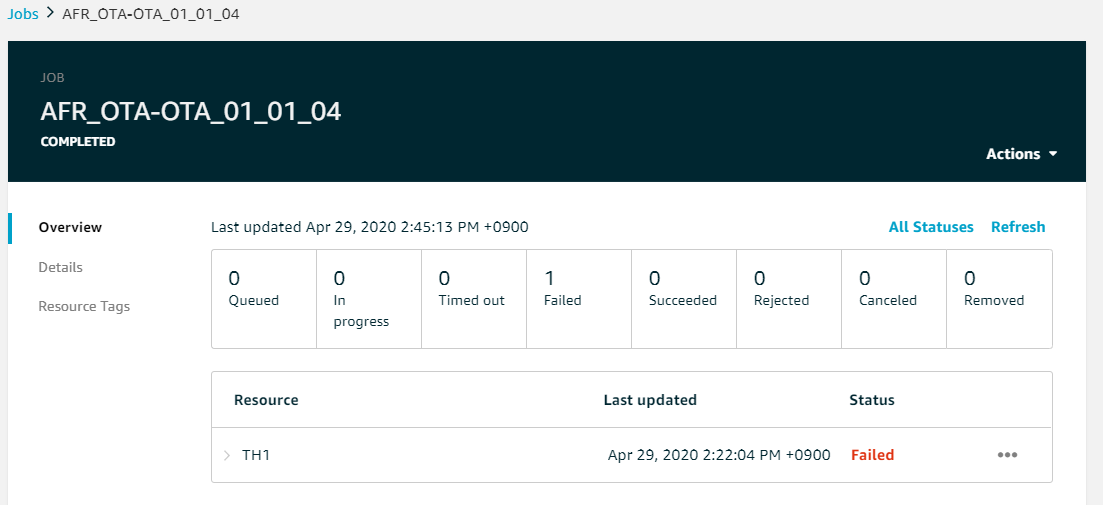


1. Select your new updated firmware from S3 bucket
2. Write down ‘/device’ on pathname of firmware image on device
3. Select the IAM role for OTA update job which we have created from step 5, configuring Amazon Web services.
4. Give your OTA update job a name and click Create. Please make sure write the version number at the end of job name. For example, OTA\_JOB\_01\_01\_03. 6-digit version number with underscore is needed to process this Trust-Fi OTA update.
5. Job will be created and queued; you can view them on your AWS console.

When Trust-Fi connected with AWS, device will perform a given job that has been listed. Job will proceed instantly if the Thing is already connected and ready for updates.

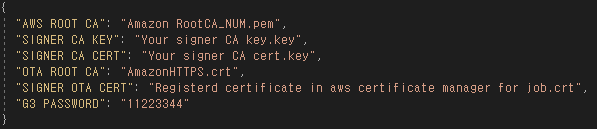
Job status and completion is shown at AWS console. When the signature cannot be verified with G3, job will be failed and firmware will keep the previous version.





Setting Trust-Fi OTA

To use Trust – Fi, you need to configure using python tool.

1. Edit the file name certi.json(AWSqual\py) in the python tools.
   1. certi.json

* The first item “AWS ROOT CA” can be downloaded from the site below, downloaded and saved in the same directory.

**[Website -** [**https://www.amazontrust.com/repository/**](https://www.amazontrust.com/repository/)**]**

* “SIGNER CA CERT & CIGNER CA KEY” is the CA registered with AWS and the private key corresponding to the CA. Likewise, save them in the same directory.
* “OTA ROOT CA” is associated with the S3 server certificate.
* “SIGNER OTA CERT” is a certificate registered in AWS Certificate Manager(ACM). If the certificate is not registered, refer to the code signing profile document below.

[[https://docs.aws.amazon.com/signer/latest/developerguide/gs-profile.html]](https://docs.aws.amazon.com/signer/latest/developerguide/gs-profile.html)

1. Run zwg3m\_certi.py and select AT UART port. This python tool write data from certi.json to Trust-Fi through opened AT port. **(The order of progress is Verifying PASSWORD → Writeing AWS ROOT CA → Writing SIGNER CA PRIVATE KEY → Writing SIGNER CA CERTI → Writing OTA ROOT CA CERTI → Writing SIGNER PUBLIC KEY: X & Y)**
2. If python exit code is 0, the setting has been completed successfully. On the contrary, if exit code isn’t 0, please check certi.json again.

Starting Trust-Fi OTA

If you run ZTP without any problems, it met all the pre-requisites of the OTA. You enter the AT command “AT+OTA\_TASK=1”, the OTA will be executed. Or there is a way to use the python tool we provide. In summary, it is as follows.

1. Entering AT command directory.

Open the AT UART port and enter “AT+OTA\_TASK=1”. If so will be started OTA task on Trust-Fi.

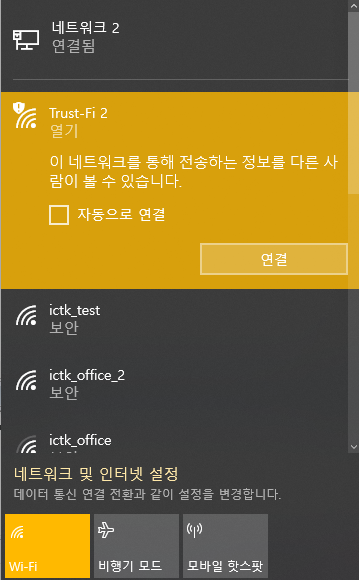
1. Running the python tool.

Open zwg3m\_ota\_cmd.py with python IDE and run. So will transfer AT command’s “AT+OTA\_TASK=1” to Trust-Fi on zwg3m\_ota\_cmd.py

\* But Trust-Fi’s ota memory size is maximum 1612kB. Note this point and upload it to AWS.

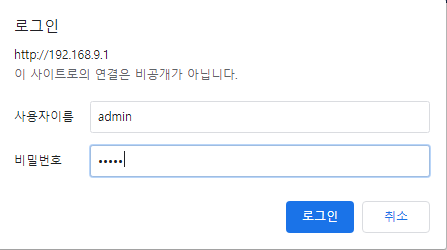
Wifi disconnect error

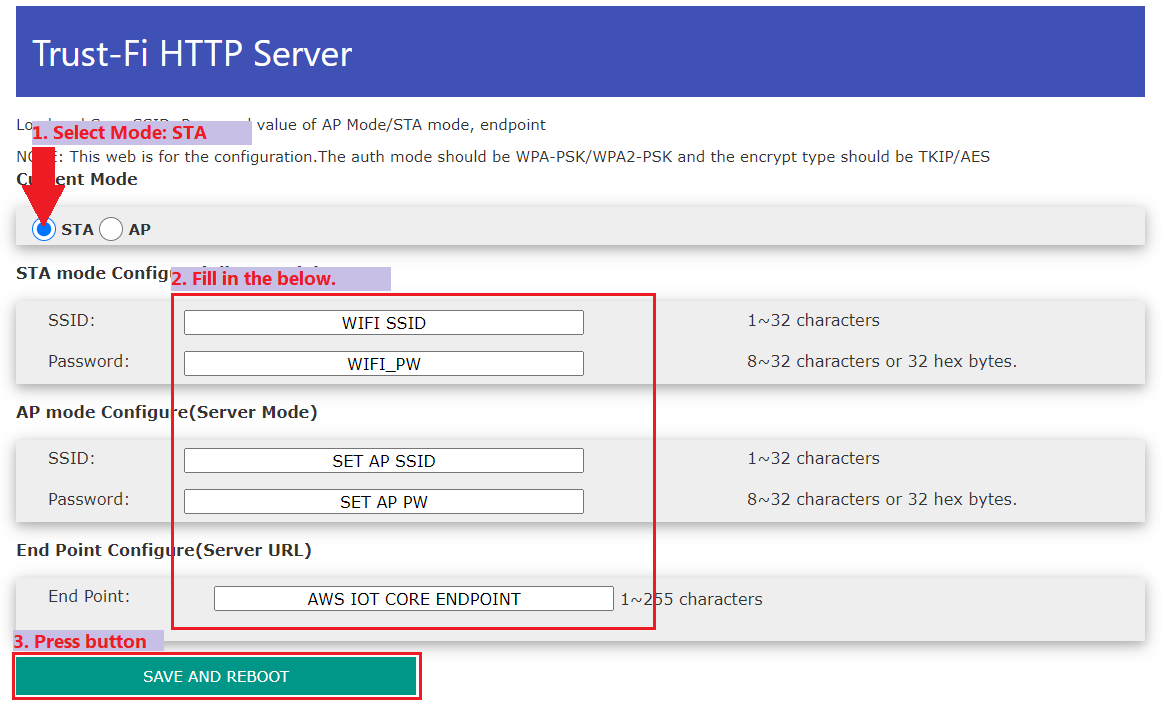
\* If you occurred wifi disconnect error, Trust-Fi is set to AP mode from STA mode. Then you will be able to connect HTTP server of Trust-Fi through wifi.

1. Connect to Trust-Fi operated AP mode trough wifi.

And approach Trust-Fi ip address.

(Default Ip address is 192.168.9.1)

Then input “admin” at UserID & PW.

1. Set the WIFI options on the HTTP server.
2. Check if Trust-Fi reboots.