

## ARM<sup>®</sup> Cortex<sup>®</sup>-M23 32-bit Microcontroller

# Alibaba Link TEE Air on M2351 Quick Start Guide

*The information described in this document is the exclusive intellectual property of Nuvoton Technology Corporation and shall not be reproduced without permission from Nuvoton.*

*Nuvoton is providing this document only for reference purposes of NuMicro microcontroller based system design. Nuvoton assumes no responsibility for errors or omissions.*

*All data and specifications are subject to change without notice.*

For additional information or questions, please contact: Nuvoton Technology Corporation.

[www.nuvoton.com](http://www.nuvoton.com)

Table of Contents

1 OVERVIEW ..... 3

2 BUILD AND DOWNLOAD TA CODE ..... 3

3 BULID AND DOWNLOAD CA CODE ..... 12

4 EXECUTE TA AND CA CODES ..... 14

5 REVISION HISTORY ..... 15

## 1 OVERVIEW

Trusted Execution Environment (TEE) provides secure service for other rich OS on the portable device. The TEE is called Trust Application (TA) and the rich OS is called Client Application (CA). This document describes about Alibaba Link TEE Air Edition, including how to setup environment to build TA and CA codes, how to download these codes to NuMaker-FPM-M2351 board, and execution.

## 2 BUILD AND DOWNLOAD TA CODE

The Trust Application (TA) is developed in Linux and needs to be executed in M2351 Secure world. This document demonstrates how to building Alibaba Link TEE Air TA code in Ubuntu 18.04 by using GNU Arm® Embedded Toolchain version 6-2017-q2-update.

GNU Arm® Embedded Toolchain download link is as following:

<https://developer.arm.com/open-source/gnu-toolchain/gnu-rm/downloads>

### Downloading GNU Arm® Embedded Toolchain Installation File

Download Linux version of GNU Arm® Embedded Toolchain from website.

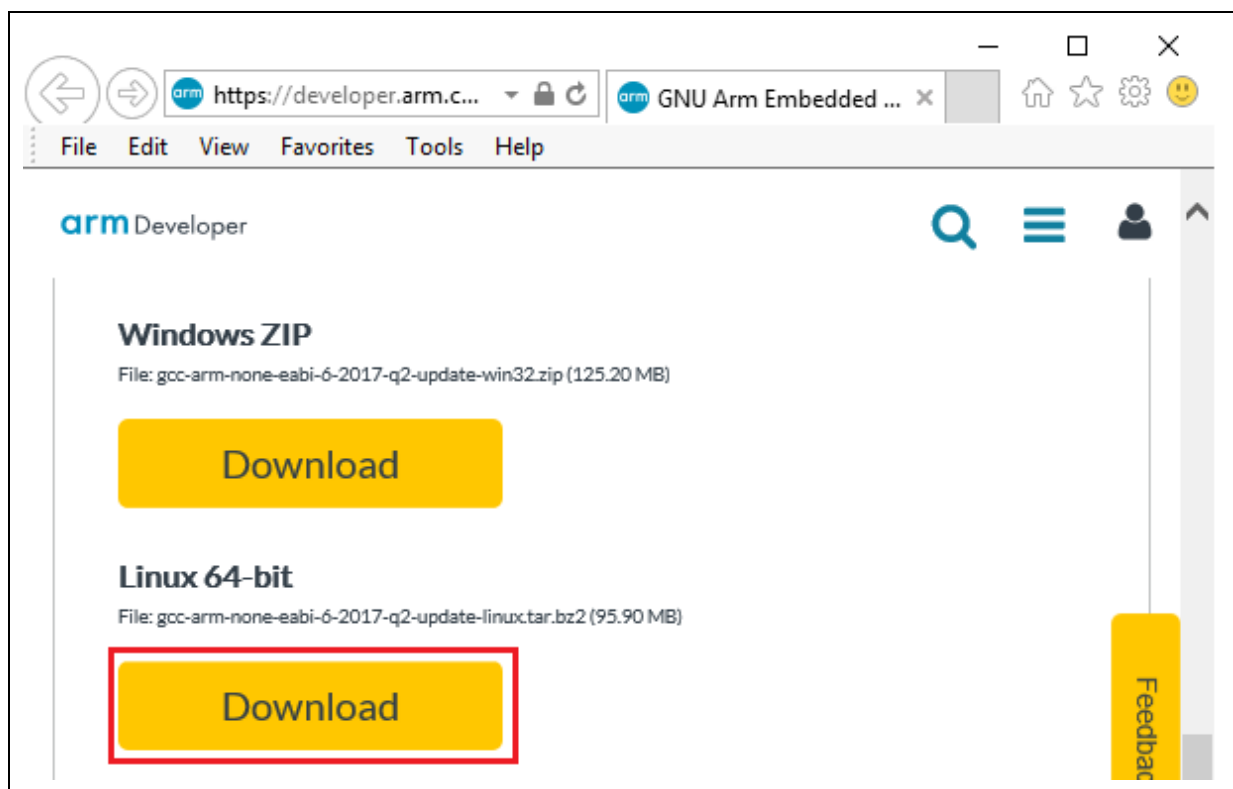


Figure 2-1 Download GNU Arm Embedded Toolchain from Website

### Install GNU Arm® Embedded Toolchain

Place downloaded file into installing folder. Right click and select “Open in Terminal” to open terminal window.

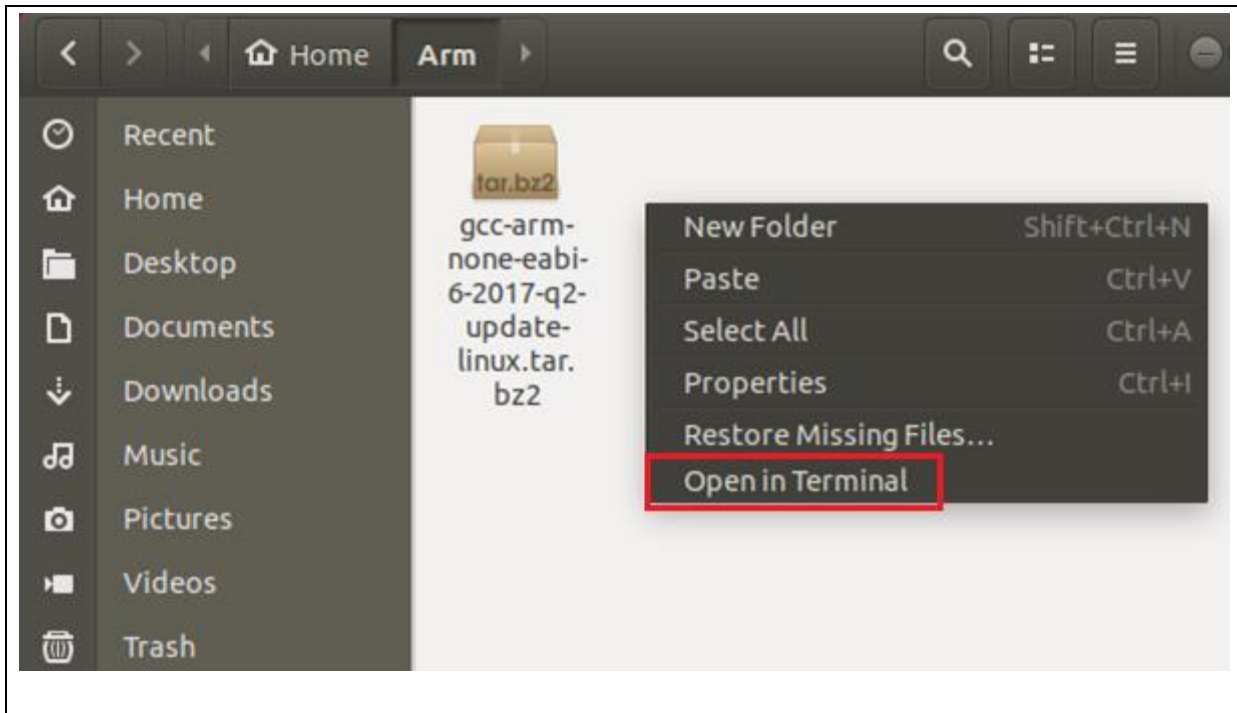


Figure 2-2 GNU Arm Embedded Toolchain Installation File

Extract installation file by using extraction command.

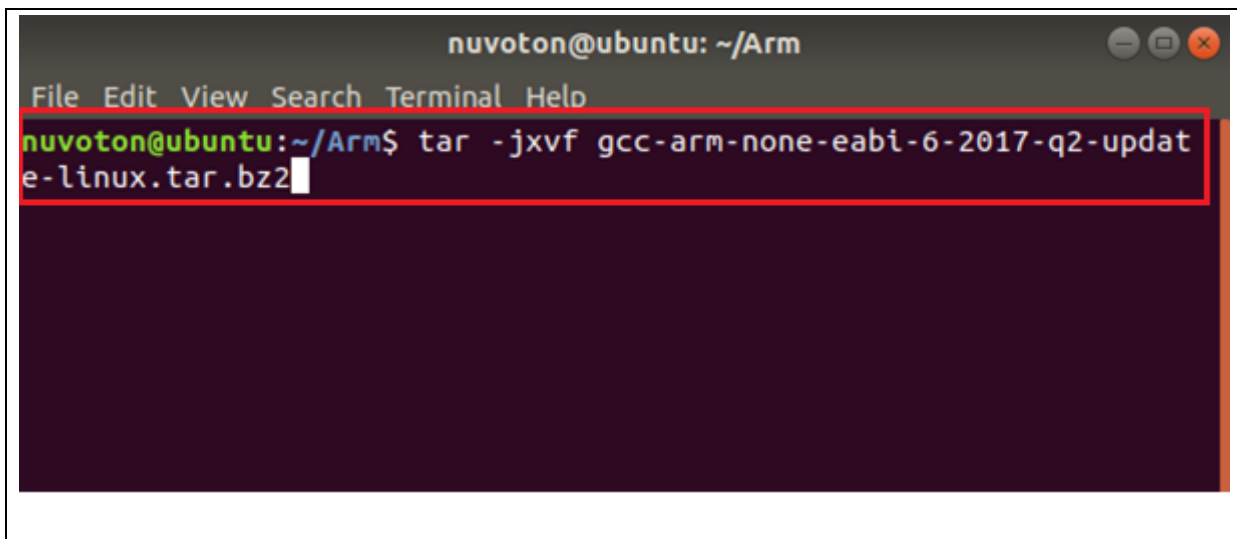


Figure 2-3 Extract GNU Arm Embedded Toolchain Installation File

The extracted file is in the same folder.

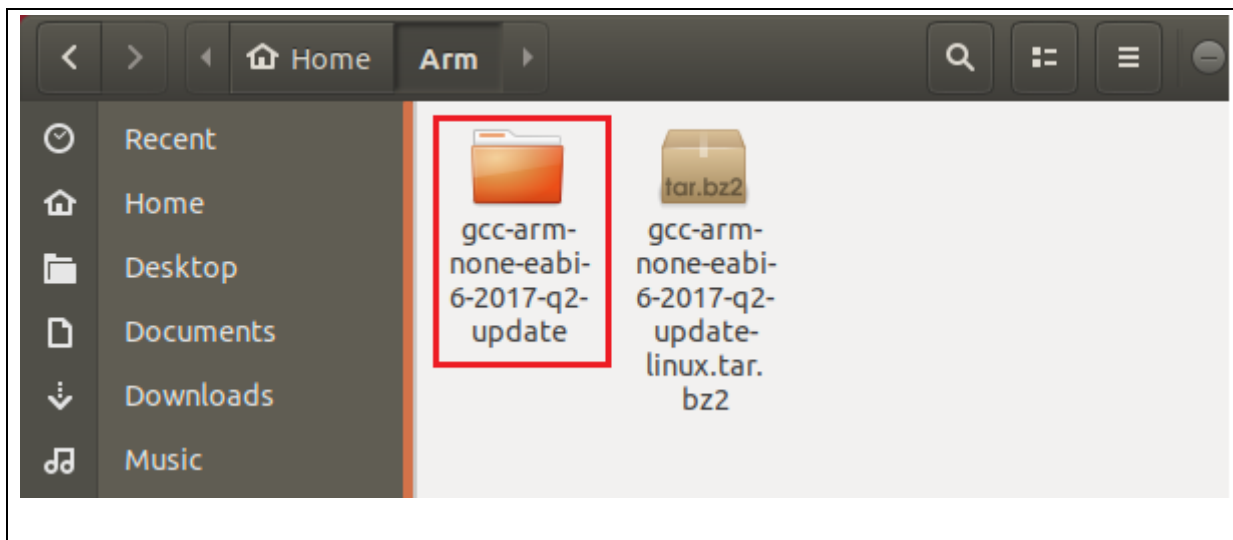


Figure 2-4 The Extracted GNU Arm Embedded Toolchain Installation File

### Add GNU Arm® Embedded Toolchain Path into Environment Variables

Use **vi** command to edit **.bashrc** file.

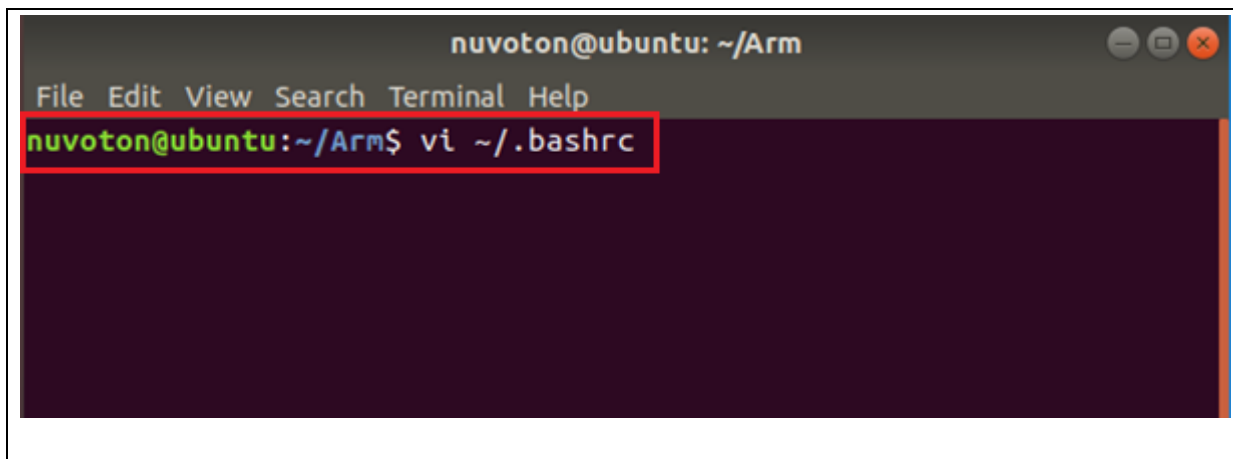
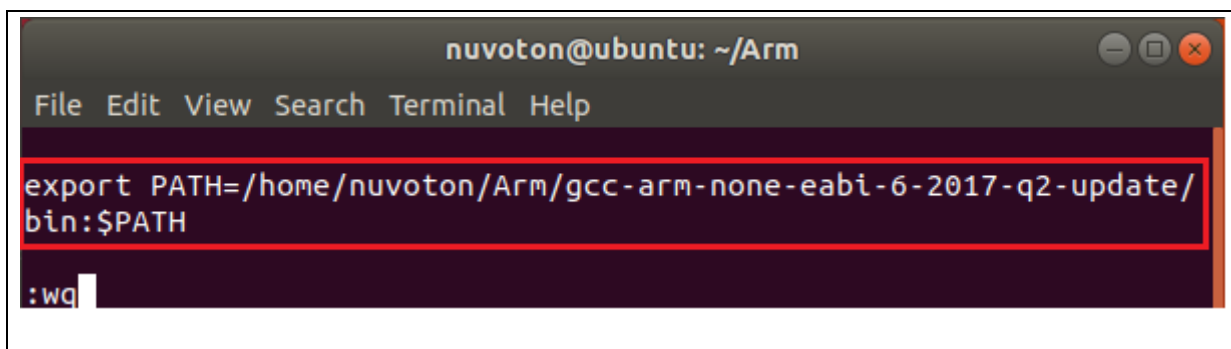


Figure 2-5 Edit .bashrc File

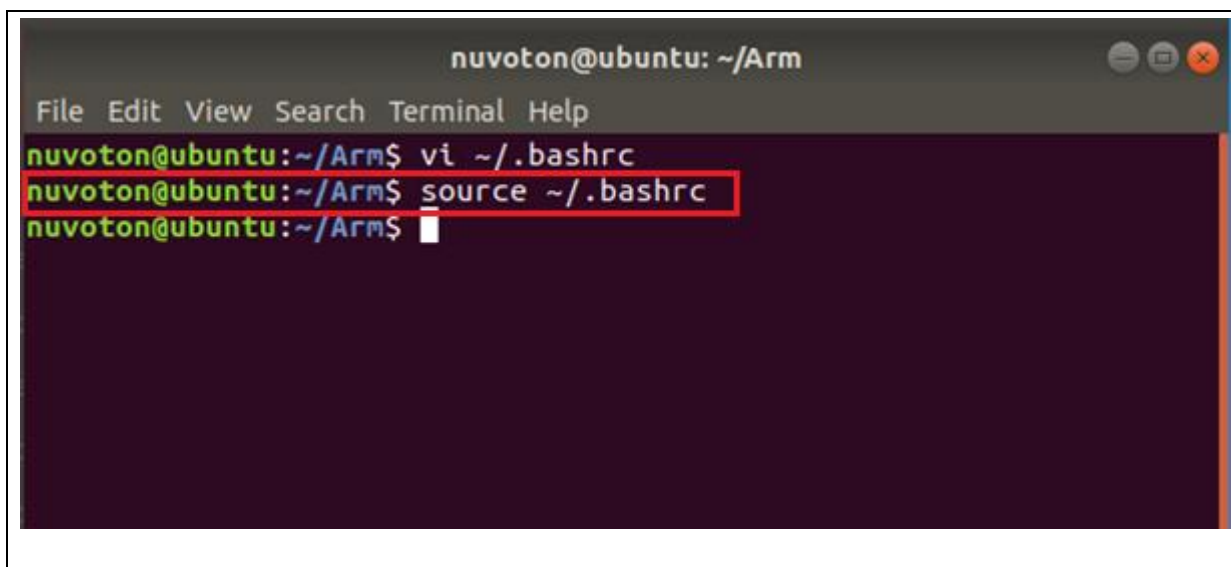
Add GNU Arm® Embedded Toolchain path at the last line of the file and remember to modify the path according to your installation location. Save the file and quit editor.



```
nuvoton@ubuntu: ~/Arm
File Edit View Search Terminal Help
export PATH=/home/nuvoton/Arm/gcc-arm-none-eabi-6-2017-q2-update/
bin:$PATH
:wq
```

Figure 2-6 Add GNU Arm Embedded Toolchain Path in .bashrc File

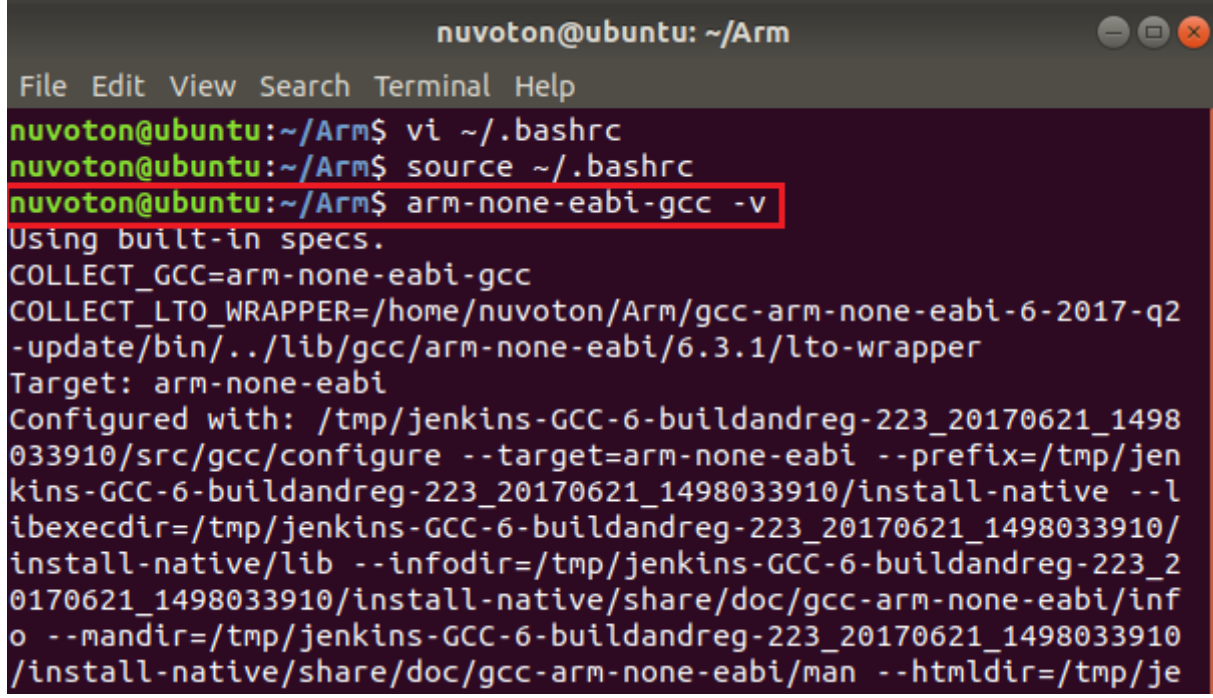
Use **source** command to make the **.bashrc** file environment variables configuration effective.



```
nuvoton@ubuntu: ~/Arm
File Edit View Search Terminal Help
nuvoton@ubuntu:~/Arm$ vi ~/.bashrc
nuvoton@ubuntu:~/Arm$ source ~/.bashrc
nuvoton@ubuntu:~/Arm$
```

Figure 2-7 Make Environment Variables Configuration Effective

Use “**arm-none-eabi-gcc -v**” command to check toolchain installation. If terminal window shows version message, the installation is successful.



```
nuvoton@ubuntu: ~/Arm
File Edit View Search Terminal Help
nuvoton@ubuntu:~/Arm$ vi ~/.bashrc
nuvoton@ubuntu:~/Arm$ source ~/.bashrc
nuvoton@ubuntu:~/Arm$ arm-none-eabi-gcc -v
Using built-in specs.
COLLECT_GCC=arm-none-eabi-gcc
COLLECT_LTO_WRAPPER=/home/nuvoton/Arm/gcc-arm-none-eabi-6-2017-q2
-update/bin/./lib/gcc/arm-none-eabi/6.3.1/lto-wrapper
Target: arm-none-eabi
Configured with: /tmp/jenkins-GCC-6-buildandreg-223_20170621_1498
033910/src/gcc/configure --target=arm-none-eabi --prefix=/tmp/jen
kins-GCC-6-buildandreg-223_20170621_1498033910/install-native --l
ibexecdir=/tmp/jenkins-GCC-6-buildandreg-223_20170621_1498033910/
install-native/lib --infodir=/tmp/jenkins-GCC-6-buildandreg-223_2
0170621_1498033910/install-native/share/doc/gcc-arm-none-eabi/inf
o --mandir=/tmp/jenkins-GCC-6-buildandreg-223_20170621_1498033910
/install-native/share/doc/gcc-arm-none-eabi/man --htmldir=/tmp/jen
```

Figure 2-8 Check Add GNU Arm Embedded Toolchain Installation

### Install Make Tool

The TA code building needs make tool. Use “**apt-get install make**” command to install make tool.

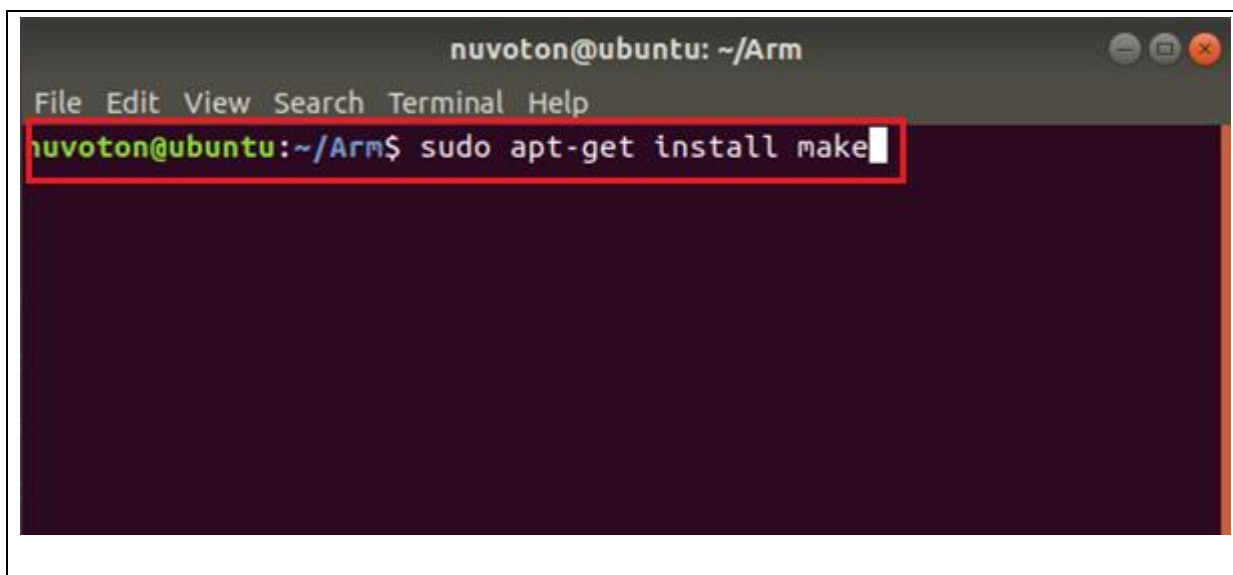


Figure 2-9 Install Make Tool

### Build TA Code

The TA code is in the following folder

**Alibaba\_Link\_TEE\_Air/FreeRTOS\_M2351/Link\_TEE\_Air\_v2.0.0.**

There is a file named “b” in “build” folder.

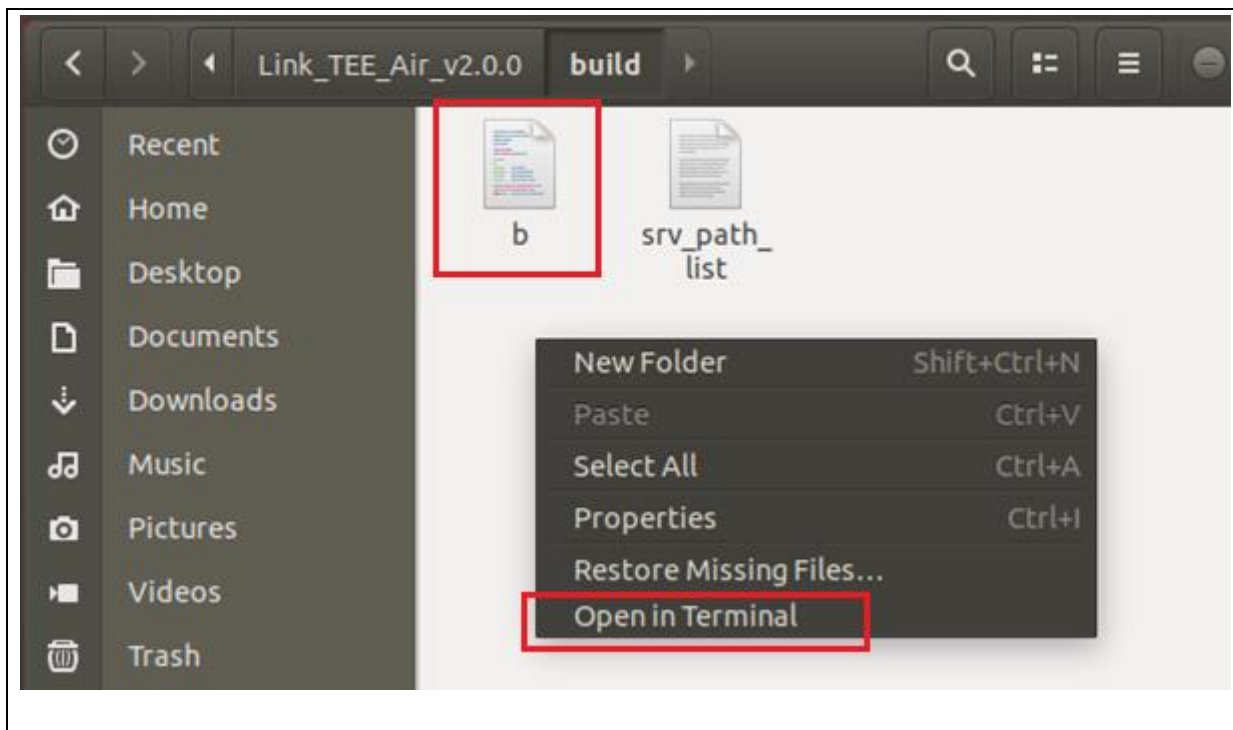


Figure 2-10 Execute b File to Build TA Code

Execute b file in terminal window.



```

nuvoton@ubuntu: ~/Alibaba_Link_TEE_Air/FreeRTOS_M2351/Link_TEE_Ai...
File Edit View Search Terminal Help
nuvoton@ubuntu:~/Alibaba_Link_TEE_Air/FreeRTOS_M2351/Link_TEE_Air
.0/build$ ./b
~/Alibaba_Link_TEE_Air/FreeRTOS_M2351/Link_TEE_Air_v2.0.0/samples
/xor/tw ~/Alibaba_Link_TEE_Air/FreeRTOS_M2351/Link_TEE_Air_v2.0.0
/build
arm-none-eabi-gcc -I. -I/home/nuvoton/Alibaba_Link_TEE_Air/FreeRT
OS_M2351/Link_TEE_Air_v2.0.0/samples/xor/tw/./inc -I/home/nuvoto
n/Alibaba_Link_TEE_Air/FreeRTOS_M2351/Link_TEE_Air_v2.0.0/samples
/xor/tw/../../../../src/tw/inc -mthumb -mcpu=cortex-m23 -mcmse -mthu
mb-interwork -Werror -O2 -Werror-implicit-function-declaration -W
strict-prototypes -Wwrite-strings -fno-builtin -DCONFIG_TW=1 -DC
ONFIG_DBG=1 -DCONFIG_MEMORY_PROFILING=0 -DCONFIG_BS_DBG=1 -DCONF
IG_CORE_DBG=1 -DCONFIG_POOL_DBG=0 -DCONFIG_TEE_API_DBG=0 -DCONF
IG_DEVICE_DBG=1 -DCONFIG_EFLASH_DRV_DBG=0 -DCONFIG_CRYPTO_DRV_DBG=0
-DCONFIG_ALI_CRYPTO_DBG=0 -DCONFIG_SUPPORT_MULTI_THREAD=0 -DCONF
IG_API_STRING=1 -DCONFIG_API_POOL=1 -DCONFIG_API_PRINTF=1 -DCONF
IG_API_CB_SUPPORT=1 -DCONFIG_API_CB_MEM=1 -DCONFIG_API_CB_FILE=0 -D
CONFIG_API_CRYPT=1 -DCONFIG_BACKTRACE=1 -DCONFIG_TEST_PERF=0 -c
xor_ta.c -o xor_ta.o
arm-none-eabi-ld -r xor_ta.o -o built-in.o
~/Alibaba_Link_TEE_Air/FreeRTOS_M2351/Link_TEE_Air_v2.0.0/build
integ-cmd = ../tools/build_tw/build_tw -s ../src/tw/platform/m235
1/sw.elf -a ../samples/xor/tw/built-in.o -o ../out/tee_tw.bin

```

Figure 2-11 Build TA Code

If building is successful, it will output the TA code binary file TEE\_tw.bin in “out” folder.



Figure 2-12 The TA Code Binary

### Download TA code

The TA code needs to download in Windows by Nuvoton NuMicro® ICP Programming Tool. Select target chip as “M2351 Series” and then click “Continue >>”.

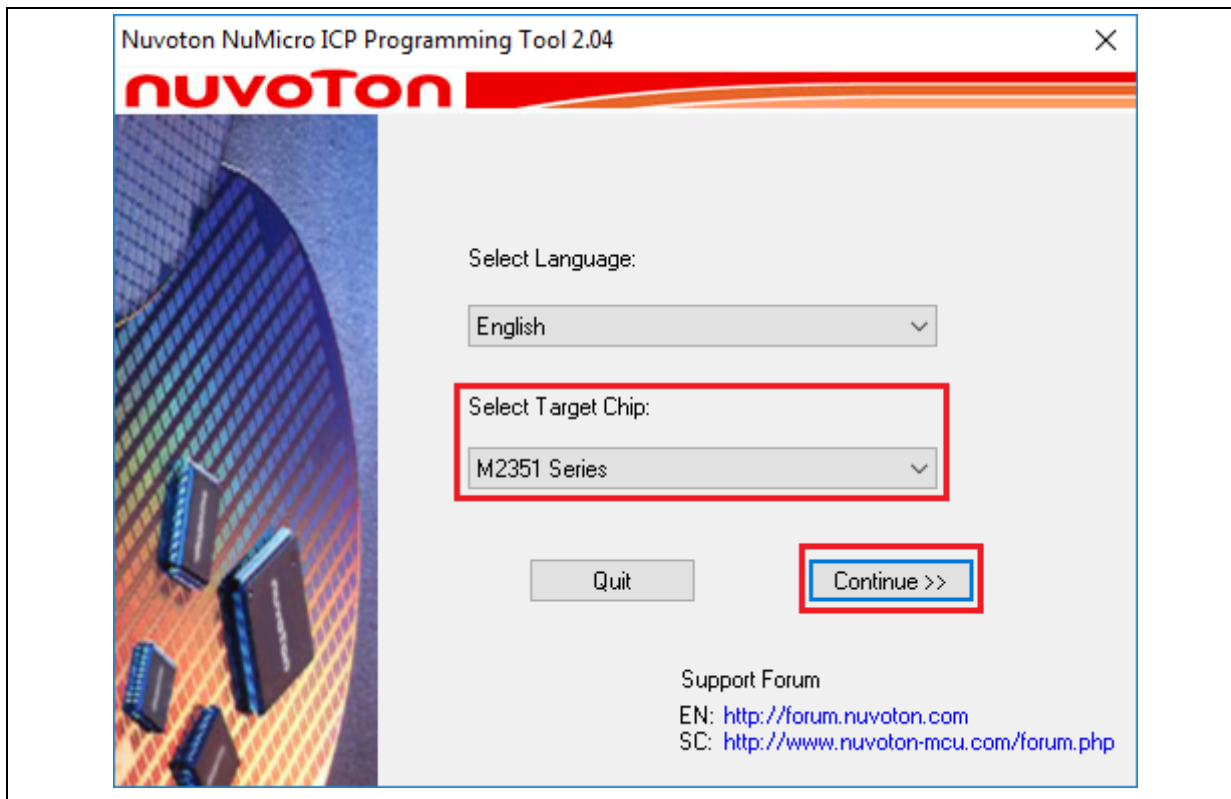


Figure 2-13 Nuvoton NuMicro ICP Programming Tool

Connect NuMaker-FPM-M2351 board with PC and click “Connect” to wait for M2351 being connected with Nu-Link.

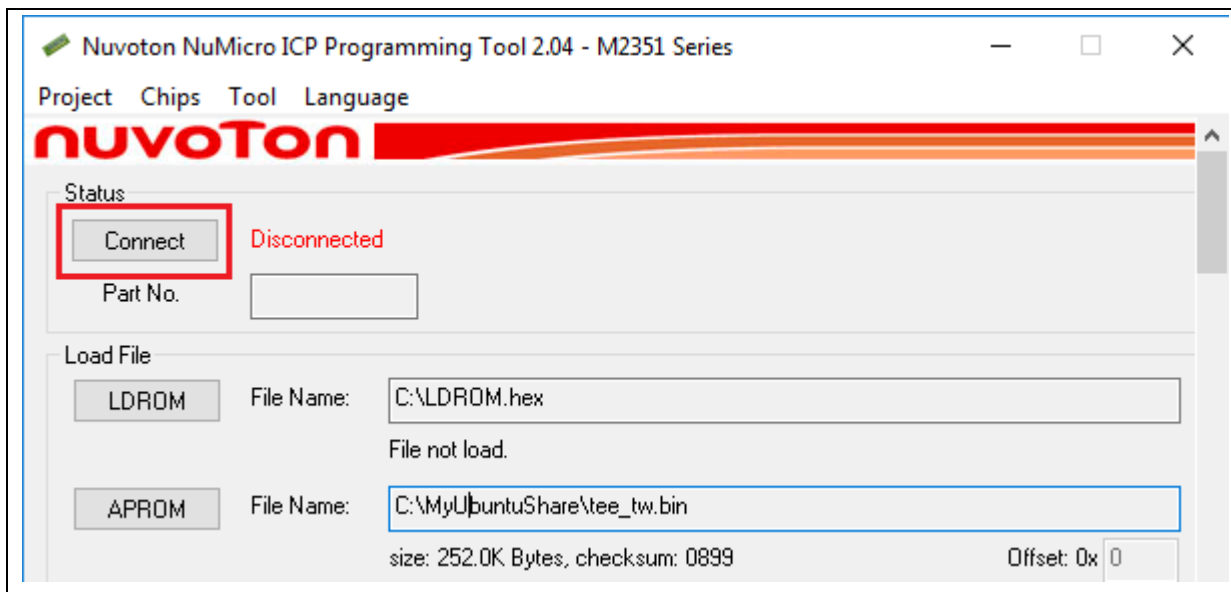


Figure 2-14 Connect NuMaker-FPM-M2351 Nu-Link

After the “Status” catalog shows M2351 is connected, user can add TEE\_tw.bin file into APROM load file. In the “Programming” catalog, select APROM checkbox. Press “Start” button to start downloading TA code.

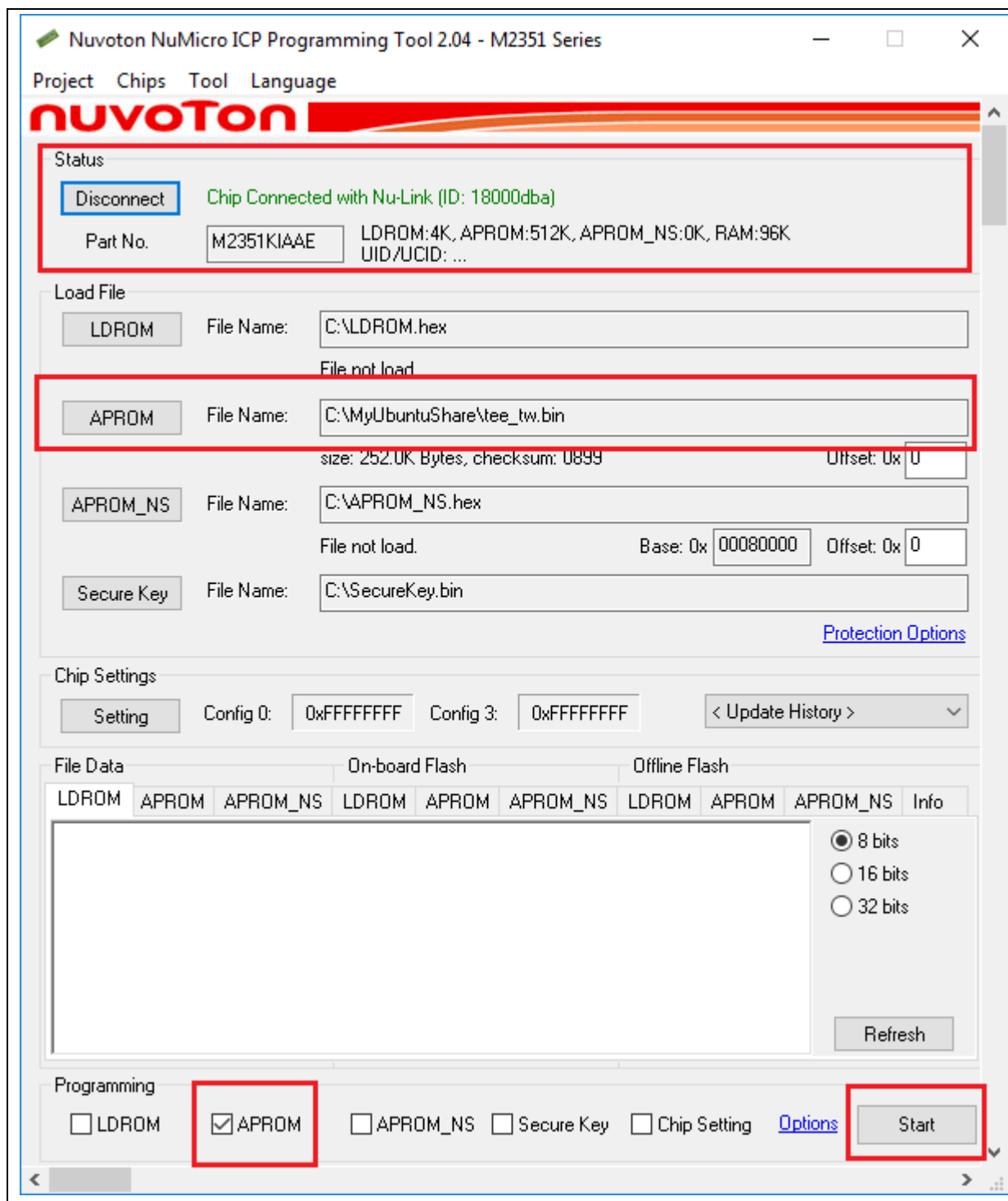


Figure 2-15 Use Nuvoton NuMicro ICP Programming Tool to Download TA Code

### 3 BULID AND DOWNLOAD CA CODE

The Client Application (CA) is developed in Windows KEIL. It is developed in M2351 Non-secure world. This document demonstrates how to building Alibaba Link TEE Air CA code in Windows 10 by using Keil®-MDK v5.23.

#### Open CA Code Project

The CA code KEIL project is in “Alibaba\_Link\_TEE\_Air/FreeRTOS\_M2351\_Demo\_M2351\_NS”.

User can open the CA code with KEIL uVision5 by double clicking the “RTOSDemo\_523.uvprojx” file.

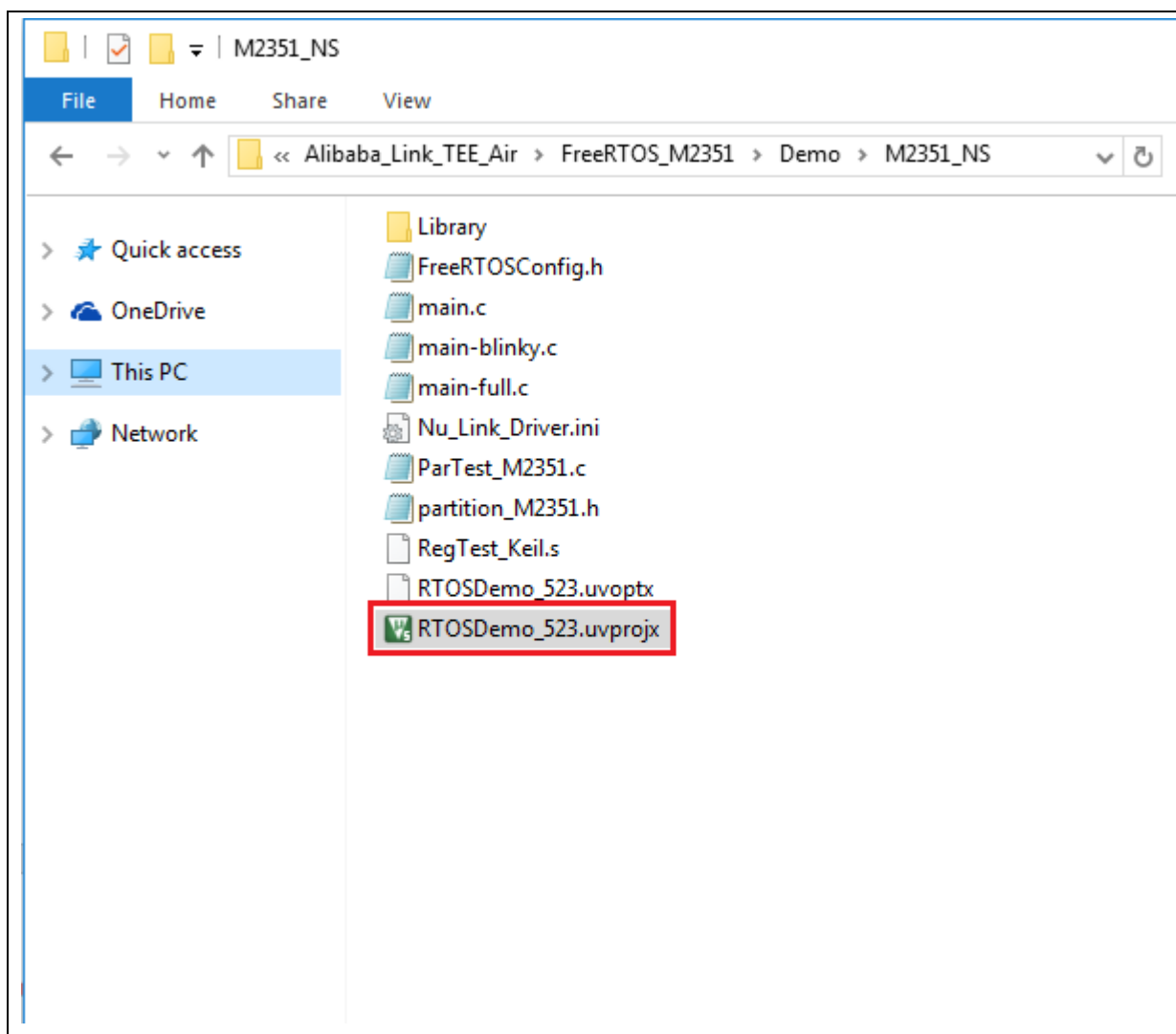


Figure 3-1 The CA Code Project

### Build CA Code

User can click the “Rebuild” icon to build the CA code in KEIL MDK.

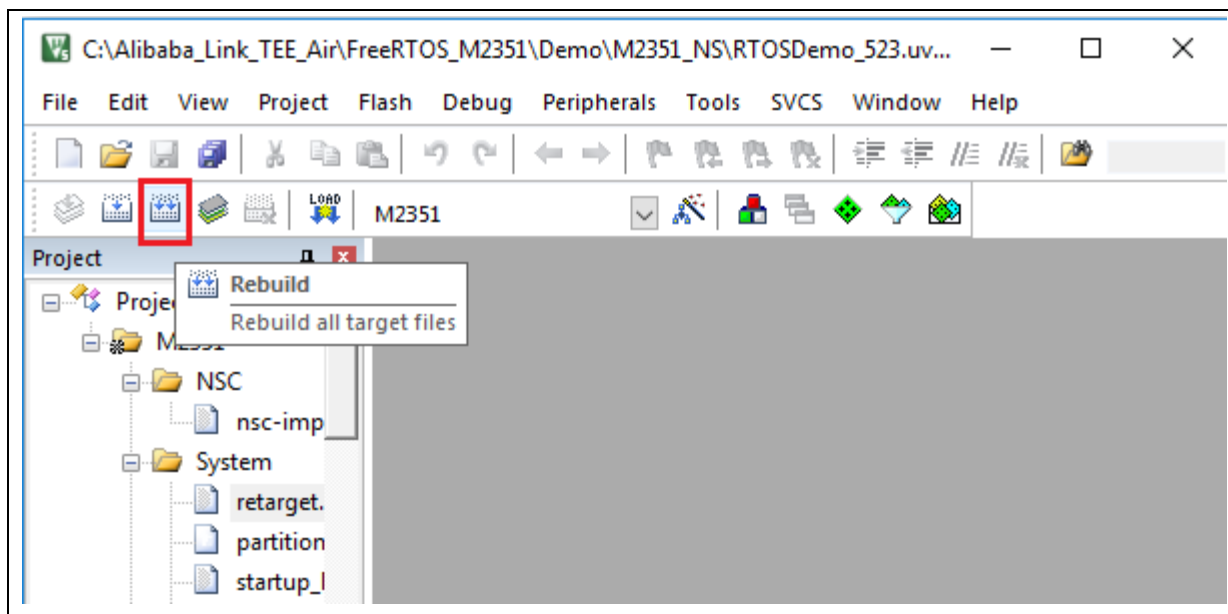


Figure 3-2 Build CA Code

### Download CA Code

User can click the “Download” icon to download the code to M2351 in KEIL MDK.

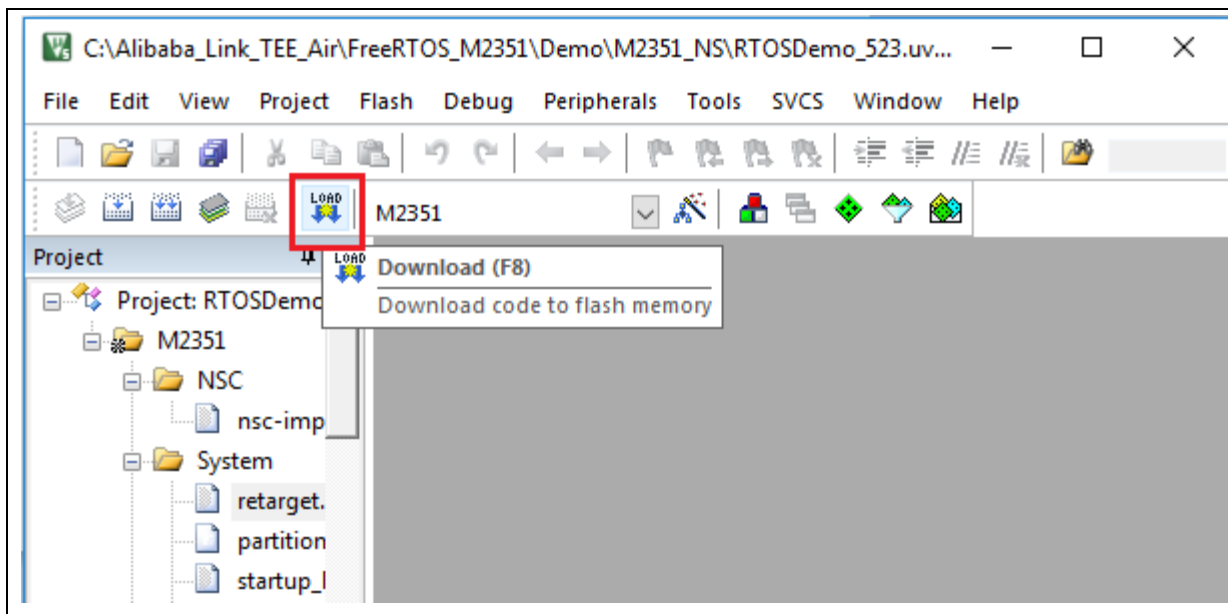


Figure 3-3 Download CA Code



## 4 EXECUTE TA AND CA CODES

After building and downloading TA and CA codes, user can press reset to execute the firmware. User can open terminal window and the debug message is shown as below.

### The TA Code Execution Debug Message

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!srv found:1871b9788a99c!!thread 2 test
a1a028eb601d53ed503
tw: TA ----- CreateEntryPoint: 0x1205d
tw: TAtw:
Welcome to ALI Cloud Link TEE
tw: #####
tw: #   AIR Edition
tw: #   version:   2.0.0
tw: #   arch:      ARM
tw: #   platform:  M2351
tw: #   project:   TOA_REF
tw: #   buildtime: 2018_8_24_15:25
tw: #####
tw:heap init
tw:device init
tw: INF device_init 420:device init!
tw: INF device_init 431:sam1 init!
tw: INF device_init 431:TRNG init!
tw: INF device_init 431:AES init!
```

Figure 4-1 The TA Code Execution Debug Message

### The CA Code Execution Debug Message

```
FreeRTOS ...
#####thread 1 test
tw: tw core: receive a msg 0x30011788
tw: INFO - srv found:1871b9788a99ca1a028eb601d53ed503
tw: TA ----- CreateEntryPoint: 0x1205d
tw: TA ----- OpenSessionEntryPoint: 0x12065
tw: tw core: receive a msg 0x30011788
tw: TA ----- InvokeCommandEntryPoint: 0x1206d
xor: a 0x00000000, b 0x00000001, xor 0x00000001
a = 0; b = 1; c = a ^ b: 1
tw: tw core: receive a msg 0x30011788
tw: TA ----- CloseSessionEntryPoint: 0x12069
xor success
#####thread 1 round success
```

Figure 4-2 The CA Code Execution Debug Message

## 5 REVISION HISTORY

Date	Revision	Description
2018.08.31	1.00	1. Initially issued.

### Important Notice

Nuvoton Products are neither intended nor warranted for usage in systems or equipment, any malfunction or failure of which may cause loss of human life, bodily injury or severe property damage. Such applications are deemed, "Insecure Usage".

Insecure usage includes, but is not limited to: equipment for surgical implementation, atomic energy control instruments, airplane or spaceship instruments, the control or operation of dynamic, brake or safety systems designed for vehicular use, traffic signal instruments, all types of safety devices, and other applications intended to support or sustain life.

All Insecure Usage shall be made at customer's risk, and in the event that third parties lay claims to Nuvoton as a result of customer's Insecure Usage, customer shall indemnify the damages and liabilities thus incurred by Nuvoton.

---

*Please note that all data and specifications are subject to change without notice.  
All the trademarks of products and companies mentioned in this datasheet belong to their respective owners.*