

---

# Trust&Go Step by Step Guide - Loading Manifest to AWS-IoT

---

## Table of Contents

<b>1</b>	<b><i>Introduction</i></b> .....	<b>3</b>
1.1	<i>Getting started with Jupyter Notebook Tutorials</i> .....	3
1.1.1	Starting Jupyter Notebook.....	3
1.2	<i>Jupyter Notebook Basics</i> .....	3
1.2.1	The Notebook dashboard .....	3
1.3	<i>Introduction to Jupyter Notebook GUI</i> .....	4
<b>2</b>	<b><i>Jupyter Notebook Tutorials</i></b> .....	<b>6</b>
<b>3</b>	<b><i>Manifest Generation Notebook</i></b> .....	<b>7</b>
<b>4</b>	<b><i>Loading Manifest to AWS-IoT</i></b> .....	<b>9</b>
4.1	<i>CryptoAuth TrustPlatform Factory reset</i> .....	13

# 1 Introduction

This document explains step by step process involved in uploading a manifest file to AWS cloud. If you are already familiar with Jupyter Notebook you can skip this section and move to Section 2.

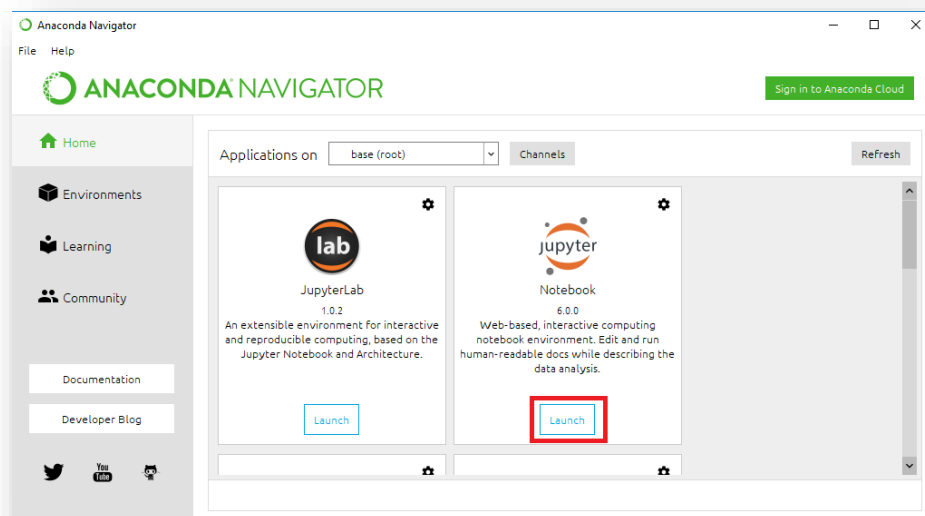
## 1.1 Getting started with Jupyter Notebook Tutorials

Jupyter Notebook is open source web application which allows you to create documents that contain code that you can execute in place as well as narrative text. It provides GUI elements, ability to execute code in place, ability to add images and gives it the look and feel that normal code files lack.

Jupyter notebooks are mainly used to explain/evaluate code in an interactive way.

### 1.1.1 Starting Jupyter Notebook

Jupyter notebook can be launched from the Anaconda Navigator main window.



## 1.2 Jupyter Notebook Basics

It is recommended to become familiar with Jupyter basic concepts with the online documentation, <https://jupyter-notebook.readthedocs.io/en/stable/examples/Notebook/Notebook%20Basics.html>

Some of the content is duplicated here for convenience. The online documentation should always be used as a reference.

### 1.2.1 The Notebook dashboard

When you first start the notebook server, your browser will open Notebook dashboard. The dashboard serves as a home page for the notebook. Its main purpose is to display the Notebooks and files in the current directory.

For example, here is a screenshot of the Jupyter dashboard. The top of the notebook list displays clickable breadcrumbs of the current directory. By clicking on these breadcrumbs or on sub-directories in the notebook list, you can navigate your file system.

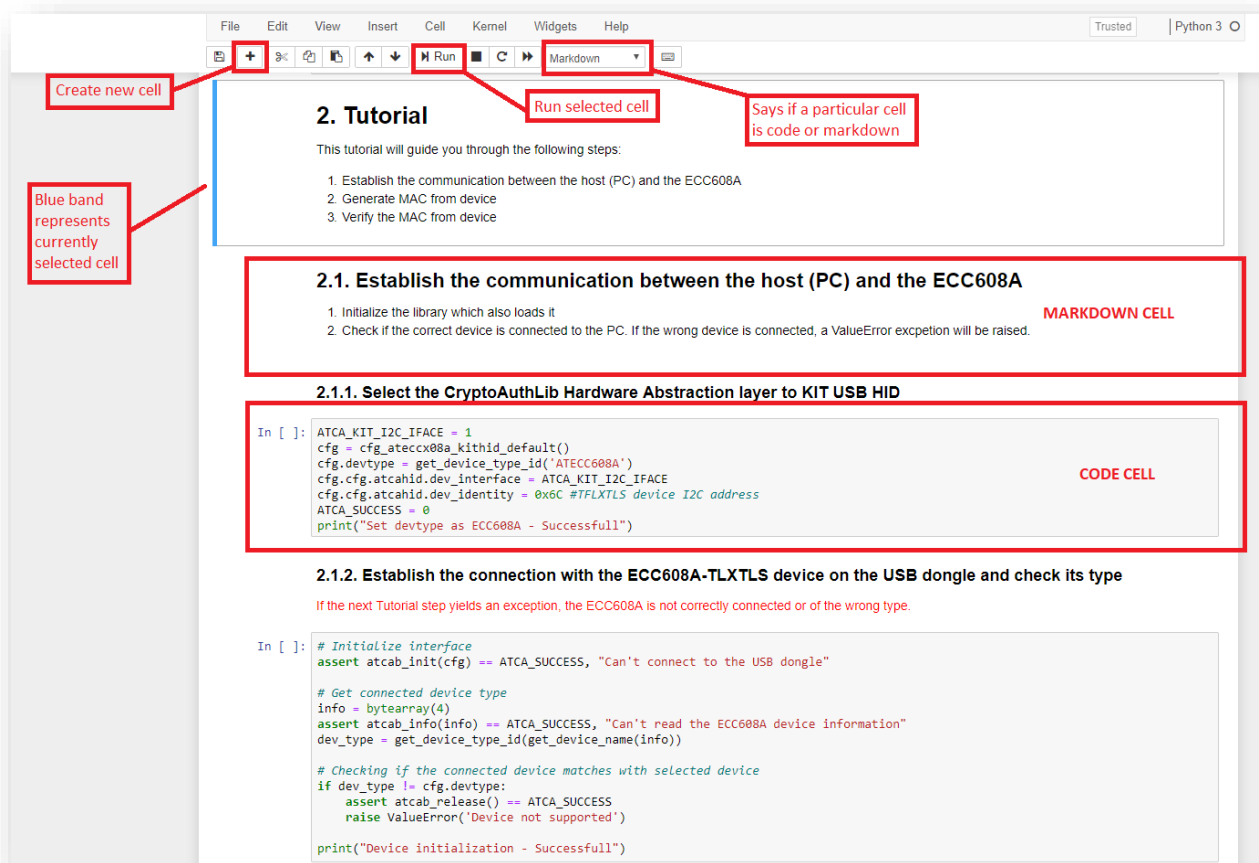


### 1.3 Introduction to Jupyter Notebook GUI.

Jupyter Notebooks contain cells where you can either write code or markdown text. Notebooks contain multiple cells, some set as code and others markdown. Code cells contain code that can be executed live, and markdown contains text and images to explain the code.

Below image shows some options in a typical Jupyter Notebook. Individual cells can be executed by pressing on the RUN button as shown in the below image.

All cells in the Notebook can be executed in order by **Kernel->Restart & Run All**.



To run all cells in sequence.



## 2 Jupyter Notebook Tutorials

The TrustPlatform Design Suite comes with a Notebook Tutorials to easily prototype popular use cases for TrustFLEX and Trust&GO devices. Here are the available Jupyter Notebook Tutorials.

<b>Jupyter Notebook Tutorials</b>	<b>Relative Path</b>	<b>Applicable devices</b>
Manifest Generation	TNGTLS_Manifest_Generation\notebooks\TNGTLS Manifest File Generation.ipynb	Trust&GO
AWS IOT with TNG-TLS	TFLXTLS_resource_generation\Crypto Resource Generator.ipynb	Trust&GO
Resource Generation	TFLXTLS_Use_Cases\notebooks\accessory-authentication\Accessory Authentication.ipynb	TrustFLEX
Accessory Authentication	TFLXTLS_Use_Cases\notebooks\aws-iot\aws-iot with ECC608A-TLFXTLS.ipynb	TrustFLEX
AWS Custom PKI	TFLXTLS_Use_Cases\notebooks\firmware-validation\Firmware Validation with ECC608A-TFLXTLS Tutorial.ipynb	TrustFLEX
Firmware Validation	TFLXTLS_Use_Cases\notebooks\ipprotection\IP Protection with ECC608A-TFLXTLS Tutorial.ipynb	TrustFLEX
IP Protection	TFLXTLS_Use_Cases\notebooks\public-key-rotation\Public Key Rotation with ECC608A-TFLXTLS Tutorial.ipynb	TrustFLEX
Secure Public Key Rotation	TNGTLS_Manifest_Generation\notebooks\TNGTLS Manifest File Generation.ipynb	TrustFLEX

### 3 Manifest Generation Notebook

Trust&GO device is one of the three devices available in the Trust Platform USB Dongle Board.

Trust&GO devices come with pre-programmed certificates in slots 10, 11 and 12, also slots 0-4 have pre-generated private keys, other than the previously mentioned slots all the other slots are locked.

The secure element manifest format is designed to convey the unique information about a device including its unique ID (e.g. serial number), public keys, and certificates. The manifest file generated can be used to register the device to cloud providers.

By default, Jupyter starts in Users directory (\$HOME for MacOS or Linux systems). For the remainder of this document, it will be assumed that the trust\_platform folder is contained in Users directory. If this is not the case, please move trust\_platform folder to your Users directory

Within the Jupyter Dashboard, navigate trust\_platform\DesignTools\TFLXTLS\_Resource\_Generation folder to open Crypto Resource Generator.ipynb notebook



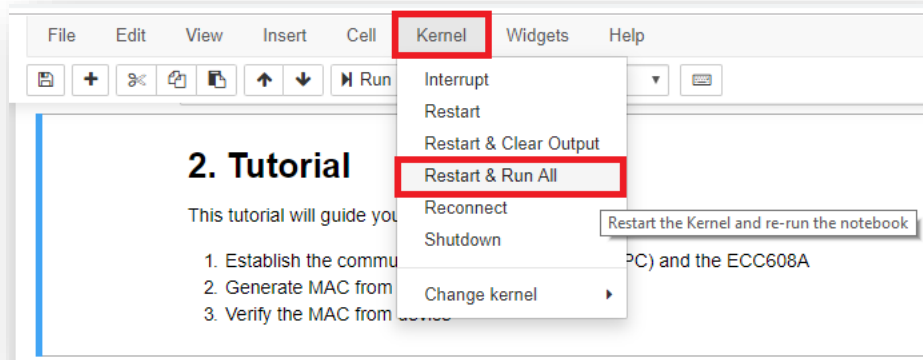
The screenshot shows the Jupyter Dashboard interface. At the top, there's a header with the Jupyter logo and 'Quit' and 'Logout' buttons. Below the header, there are tabs for 'Files', 'Running', and 'Clusters'. The 'Files' tab is active, showing a file browser. The breadcrumb path is '/ TNGTLS\_Manifest\_Generation / notebooks'. A table lists the files in the directory:

	Name	Last Modified	File size
	..	seconds ago	
<input checked="" type="checkbox"/>	TNGTLS Manifest File Generation.ipynb	4 hours ago	7.4 kB
<input type="checkbox"/>	common.py	a day ago	4.13 kB
<input type="checkbox"/>	manifest_generation_helper.py	a day ago	11.9 kB
<input type="checkbox"/>	manifest_signing_helper.py	a day ago	5.03 kB

The file 'TNGTLS Manifest File Generation.ipynb' is highlighted with a red box.

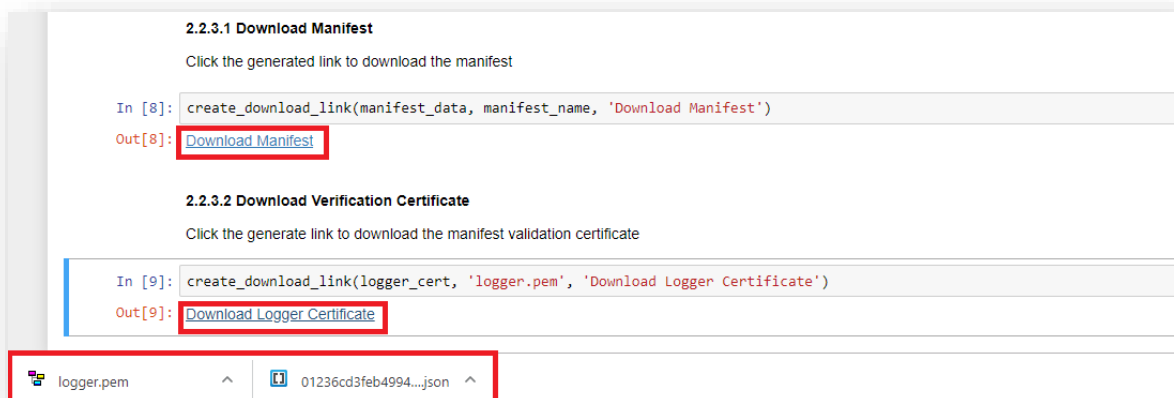
Run all cells of the TNGTLS\_Manifest\_Generation Notebook: Kernel->Restart & Run All

**Note:** Before executing the cells on Crypto Trust Platform, its required to have factory default program running on SAMD21 of Trust Platform. Refer to [4.1 CryptoAuth TrustPlatform Factory reset](#) section for reloading default program.



The Notebook will be used to generate a manifest file which can be uploaded into the public cloud provider of your choice (Google GCP, AWS IoT and soon to be supported Microsoft Azure). TNGTLS Manifest Generation notebook needs to be run for all Trust&Go example Notebooks that require a Manifest file.

If all the steps are run without errors, you will see two download links as shown below.



Click on "Download Manifest" and "Download Logger Certificate" to download the manifest and logger file.



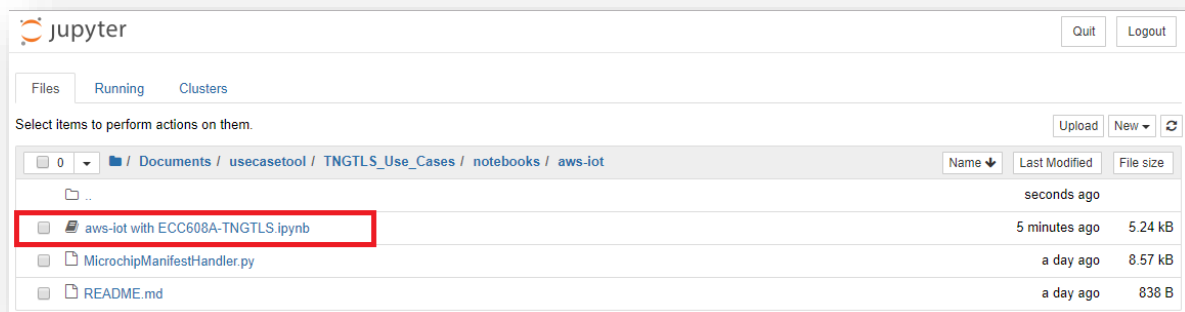
## 4 Loading Manifest to AWS-IoT

This hands-on lab is intended to demonstrate how to load a manifest file into AWS-IOT to enable device connectivity.

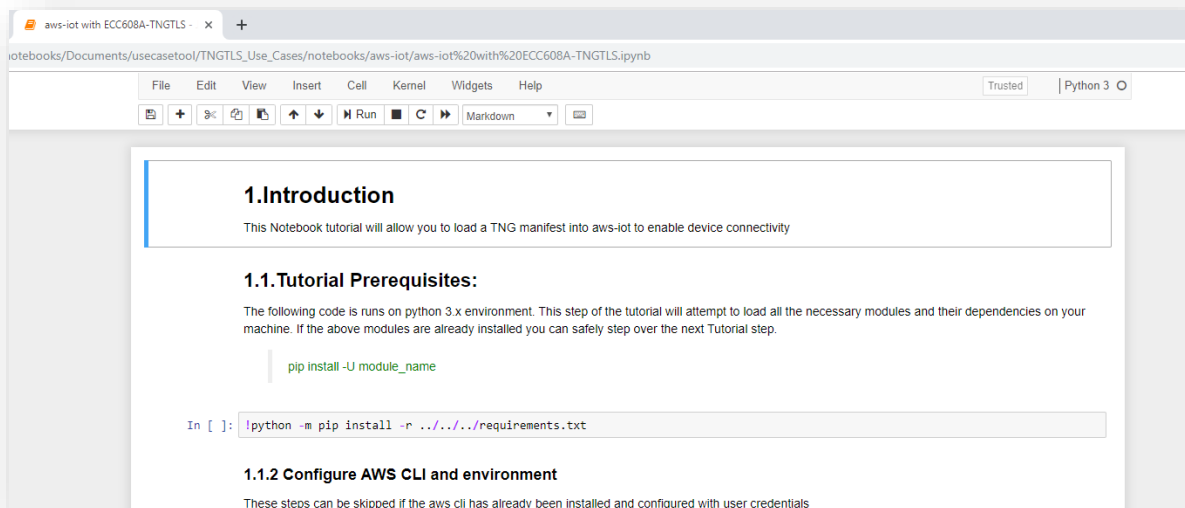
We would be using the manifest file and logger file generated in the TNGTLS Manifest File generation notebook. The Manifest file contains information about the device including serial number, public keys and certificates.

Loading a manifest file to AWS\_IOT through Jupyter Notebook:

1. From the Jupyter Home page, navigate to **TNGTLS\_Use\_Cases/notebooks/aws-iot/aws-iot with ECC608A-TNGTLS.ipynb** notebook file and open it.



Opening the notebook from Jupyter home page should load the following on the browser.



2. This notebook requires user input in some of the intermediary steps so Run All option in Jupyter is not recommended. Run steps 1.1 and 1.2, these steps will install all the modules required for the Notebook and import the required modules.

3. Run step 1.3, under step 1.3 it will prompt you to enter the following details
  - a. Access key
  - b. Secret key
  - c. Region name

These details will be used to setup AWS-CLI in your PC. You can get these details from your AWS account.

The output after entering all the details will look like the image below. Credentials used in the below image should not be used, you are needed to enter the credentials tied to your own account.

```
Set the AWS access key, Secret access key and region

In [8]: access_key = input('Enter Access key\n\n')
        configure_aws_access_key(access_key)
        secret_key = input('Enter Secret access key\n\n')
        configure_aws_secret_access_key(secret_key)
        region = input('Enter region\n\n')
        configure_aws_configure_region(region)

Enter Access key

AKIAQAL5EMPTMCVSHGMN
Setting aws access key...
Done

Enter Secret access key

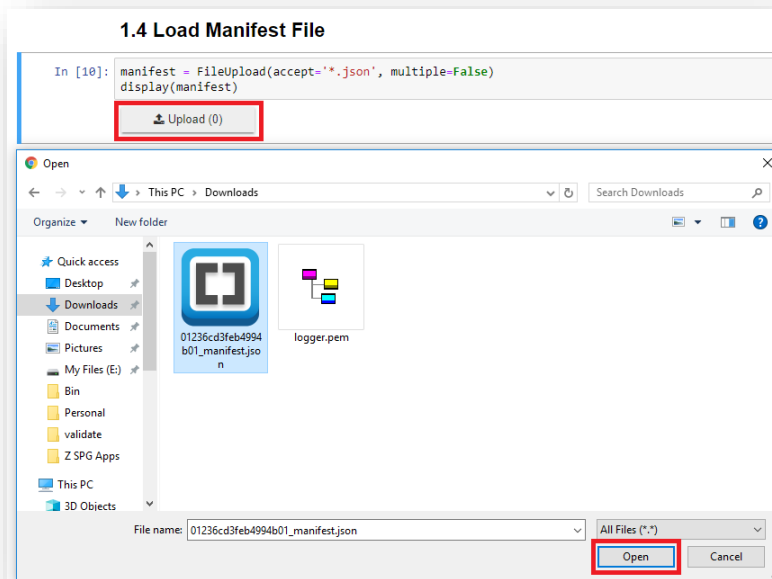
gM4oKuVl9vLvqw48IJKG7tUu/GmQ1u2jTcbjQtqy
Setting aws secret access key...
Done

Enter region

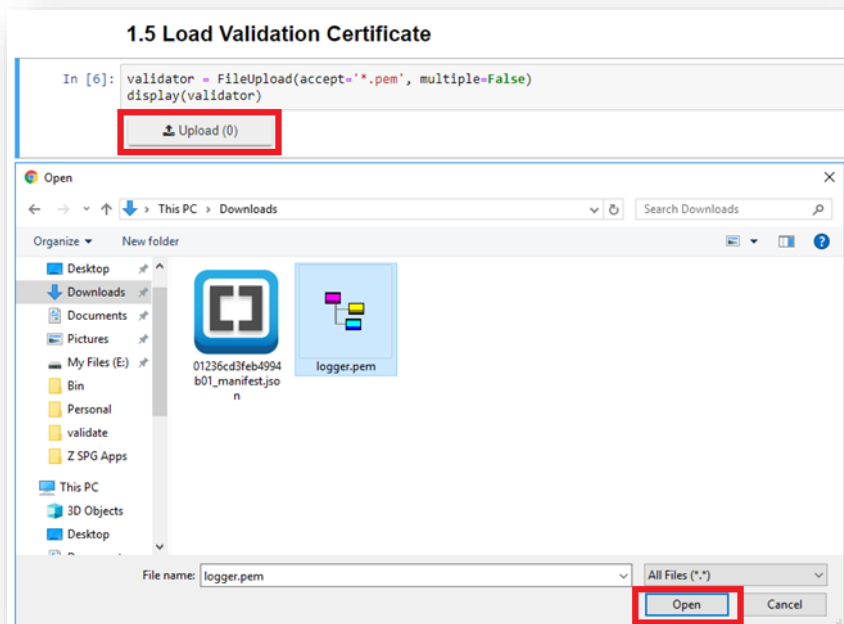
cn-north-1
Setting aws region...
Done

      Name          Value          Type    Location
      ----          -
profile            <not set>      None     None
access_key          *****HGMN shared-credentials-file
secret_key          *****Qtqy shared-credentials-file
region              cn-north-1    config-file  ~/.aws/config
```

4. Run step 1.4, it will create Upload button. Press on that button, it will open file explorer window, there you need to navigate and choose the manifest file generated using TNG Manifest Generation Notebook.



5. Run step 1.5, it will create Upload button. Press on that button, it will open file explorer window, there you need to navigate and choose the validation certificate file generated using TNG Manifest Generation Notebook.



6. Run step 1.6, the successful completion of the step will import the certificate.

```
In [4]: manifest_data = json.loads(manifest.data[0])
validation_certificate = validator.data[0]

invoke_import_manifest('Default', manifest_data, validation_certificate)

number of certificates: 1

Loading the manifest_item
uniqueId: 01232d76543e3c1401
About to try certificate import
Response: {'ResponseMetadata': {'RequestId': 'c60038f5-5fbf-406b-b4d8-06ab5bdca2dc', 'HTTPStatusCode': 200, 'HTTPHeaders': {'date': 'Thu, 26 Sep 2019 19:46:49 GMT', 'content-type': 'application/json', 'content-length': '209', 'connection': 'keep-alive', 'x-amzn-requestid': 'c60038f5-5fbf-406b-b4d8-06ab5bdca2dc', 'access-control-allow-origin': '*', 'x-amz-apigw-id': 'ApBScE8MPHcFwOg=', 'x-amzn-trace-id': 'Root=1-5d8d15a9-cefd96acde588bf47bbdc334'}, 'RetryAttempts': 0}, 'certificateArn': 'arn:aws:iot:us-west-2:257966804464:cert/e0d8082c7b88341b5df665f2308cf98461795c3bfd4ae57b306f7239dbda474a', 'certificateId': 'e0d8082c7b88341b5df665f2308cf98461795c3bfd4ae57b306f7239dbda474a'}
Certificate import complete - returning
MANIFEST_IMPORT_SUCCESS arn:aws:iot:us-west-2:257966804464:cert/e0d8082c7b88341b5df665f2308cf98461795c3bfd4ae57b306f7239dbda474a
a      arn:aws:iot:us-west-2:257966804464:thing/01232d76543e3c1401
```

## 7. Run step 1.7, successful execution of this step verifies that the manifest was successfully uploaded, and it outputs the corresponding unique ID

```
In [5]: manifest_data = json.loads(manifest.data[0])
validation_certificate = validator.data[0]
invoke_validate_manifest_import(manifest_data, validation_certificate)

number of thingIds to check: 1

Checking the manifest_item
uniqueId: 01232d76543e3c1401
Manifest was loaded successfully
```

## 4.1 CryptoAuth TrustPlatform Factory reset

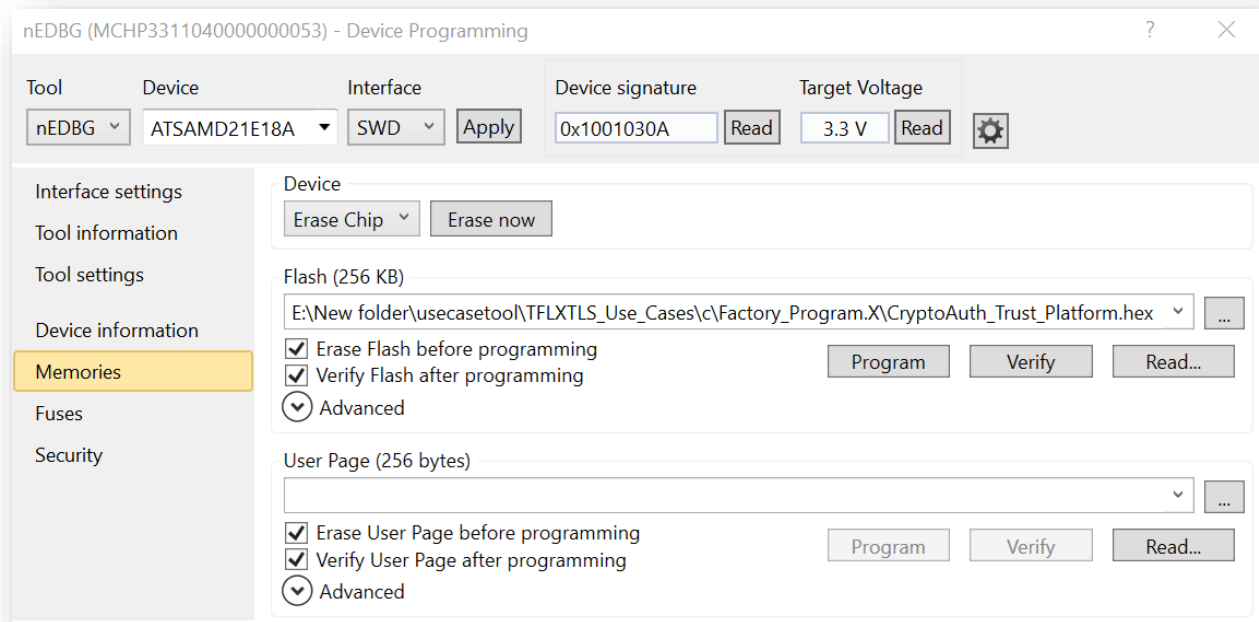
Once any of the embedded project is loaded to CryptoAuth TrustPlatform, the default program that enables interaction with TrustPlatform tools will be erased.

Before using the Platform with any other notebook or tools on PC, its required to reprogram the default .hex file. Default hex file is available at

**TFLXTLS\_Use\_Cases\c\Factory\_Program.X\CryptoAuth\_Trust\_Platform.hex**

To reprogram using Atmel Studio:

1. Navigate to AtmelStudio -> Tools -> Device Programming
2. Select Tool as nEDBG and Apply
3. Go to Memories and navigate to above path under Flash dropdown
4. Check both Erase Flash and Verify Flash
5. Click on Program



To reprogram using MPLAB:

1. Open **TFLXTLS\_Use\_Cases\c\Factory\_Program.X** project in MPLAB IDE
2. Program the Crypto Trust platform by navigating to  
**CryptoAuth\_Trust\_Platform\_Factory\_Program -> Make and Program Device**

Now, Crypto Trust Platform contains factory programmed application that enables interactions with Notebooks and/or PC tools.

---

## The Microchip Web Site

---

Microchip provides online support via our web site at <http://www.microchip.com/>. This web site is used as

a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

## Customer Change Notification Service

---

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at <http://www.microchip.com/>. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

## Customer Support

---

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support.

Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: <http://www.microchip.com/support>

## Microchip Devices Code Protection Feature

---

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.

- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as “unbreakable.”

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip’s code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

## Legal Notice

---

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY

OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer’s risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

## Trademarks

---

The Microchip name and logo, the Microchip logo, AnyRate, AVR, AVR logo, AVR Freaks, BitCloud, chipKIT, chipKIT logo, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, Heldo, JukeBlox, KeeLoq,

Kleer, LANCheck, LINK MD, maXStylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB,

OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTouch, SAM-BA, SpyNIC, SST,

SST Logo, SuperFlash, tinyAVR, UNI/O, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

ClockWorks, The Embedded Control Solutions Company, EtherSynch, Hyper Speed Control, HyperLight

Load, IntelliMOS, mTouch, Precision Edge, and Quiet-Wire are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, EtherGREEN, In-Circuit Serial Programming,

ICSP, INICnet, Inter-Chip Connectivity, JitterBlocker, KleerNet, KleerNet logo, memBrain, Mindi, MiWi, motorBench, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient

Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE,

Ripple Blocker, SAM-ICE, Serial Quad I/O, SMART-I.S., SQI, SuperSwitcher, SuperSwitcher II, Total Endurance, TSHARC, USBCheck, VariSense, ViewSpan, WiperLock, Wireless DNA, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

Silicon Storage Technology is a registered trademark of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2018, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

ISBN:

## **Quality Management System Certified by DNV**

---

### **ISO/TS 16949**

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California

and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.





# Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
<b>Corporate Office</b> 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: <a href="http://www.microchip.com/support">http://www.microchip.com/support</a> Web Address: <a href="http://www.microchip.com">www.microchip.com</a> <b>Atlanta</b> Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 <b>Austin, TX</b> Tel: 512-257-3370 <b>Boston</b> Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 <b>Chicago</b> Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 <b>Dallas</b> Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 <b>Detroit</b> Novi, MI Tel: 248-848-4000 <b>Houston, TX</b> Tel: 281-894-5983 <b>Indianapolis</b> Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 <b>Los Angeles</b> Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 <b>Raleigh, NC</b> Tel: 919-844-7510 <b>New York, NY</b> Tel: 631-435-6000 <b>San Jose, CA</b> Tel: 408-735-9110 Tel: 408-436-4270 <b>Canada - Toronto</b> Tel: 905-695-1980 Fax: 905-695-2078	<b>Australia - Sydney</b> Tel: 61-2-9868-6733 <b>China - Beijing</b> Tel: 86-10-8569-7000 <b>China - Chengdu</b> Tel: 86-28-8665-5511 <b>China - Chongqing</b> Tel: 86-23-8980-9588 <b>China - Dongguan</b> Tel: 86-769-8702-9880 <b>China - Guangzhou</b> Tel: 86-20-8755-8029 <b>China - Hangzhou</b> Tel: 86-571-8792-8115 <b>China - Hong Kong SAR</b> Tel: 852-2943-5100 <b>China - Nanjing</b> Tel: 86-25-8473-2460 <b>China - Qingdao</b> Tel: 86-532-8502-7355 <b>China - Shanghai</b> Tel: 86-21-3326-8000 <b>China - Shenyang</b> Tel: 86-24-2334-2829 <b>China - Shenzhen</b> Tel: 86-755-8864-2200 <b>China - Suzhou</b> Tel: 86-186-6233-1526 <b>China - Wuhan</b> Tel: 86-27-5980-5300 <b>China - Xian</b> Tel: 86-29-8833-7252 <b>China - Xiamen</b> Tel: 86-592-2388138 <b>China - Zhuhai</b> Tel: 86-756-3210040	<b>India - Bangalore</b> Tel: 91-80-3090-4444 <b>India - New Delhi</b> Tel: 91-11-4160-8631 <b>India - Pune</b> Tel: 91-20-4121-0141 <b>Japan - Osaka</b> Tel: 81-6-6152-7160 <b>Japan - Tokyo</b> Tel: 81-3-6880-3770 <b>Korea - Daegu</b> Tel: 82-53-744-4301 <b>Korea - Seoul</b> Tel: 82-2-554-7200 <b>Malaysia - Kuala Lumpur</b> Tel: 60-3-7651-7906 <b>Malaysia - Penang</b> Tel: 60-4-227-8870 <b>Philippines - Manila</b> Tel: 63-2-634-9065 <b>Singapore</b> Tel: 65-6334-8870 <b>Taiwan - Hsin Chu</b> Tel: 886-3-577-8366 <b>Taiwan - Kaohsiung</b> Tel: 886-7-213-7830 <b>Taiwan - Taipei</b> Tel: 886-2-2508-8600 <b>Thailand - Bangkok</b> Tel: 66-2-694-1351 <b>Vietnam - Ho Chi Minh</b> Tel: 84-28-5448-2100	<b>Austria - Wels</b> Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 <b>Denmark - Copenhagen</b> Tel: 45-4450-2828 Fax: 45-4485-2829 <b>Finland - Espoo</b> Tel: 358-9-4520-820 <b>France - Paris</b> Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 <b>France - Saint Cloud</b> Tel: 33-1-30-60-70-00 <b>Germany - Garching</b> Tel: 49-8931-9700 <b>Germany - Haan</b> Tel: 49-2129-3766400 <b>Germany - Heilbronn</b> Tel: 49-7131-67-3636 <b>Germany - Karlsruhe</b> Tel: 49-721-625370 <b>Germany - Munich</b> Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 <b>Germany - Rosenheim</b> Tel: 49-8031-354-560 <b>Israel - Ra'anana</b> Tel: 972-9-744-7705 <b>Italy - Milan</b> Tel: 39-0331-742611 Fax: 39-0331-466781 <b>Italy - Padova</b> Tel: 39-049-7625286 <b>Netherlands - Drunen</b> Tel: 31-416-690399 Fax: 31-416-690340 <b>Norway - Trondheim</b> Tel: 47-7289-7561 <b>Poland - Warsaw</b> Tel: 48-22-3325737 <b>Romania - Bucharest</b> Tel: 40-21-407-87-50 <b>Spain - Madrid</b> Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 <b>Sweden - Gothenberg</b> Tel: 46-31-704-60-40 <b>Sweden - Stockholm</b> Tel: 46-8-5090-4654 <b>UK - Wokingham</b> Tel: 44-118-921-5800 Fax: 44-118-921-5820