

# Quick Start Guide

## Getting Started

### Confirm Device is within Scope of ioXt Android profile:

- Device must run the Android operating system
- Device must qualify under the GMS certification process, or equivalent

### Gather the following information:

#### Product Details

Image of Product to Upload  
Specific SKU  
Product Description  
Link to Webpage

#### Firmware Details

Firmware Version Number  
Firmware Update Link  
Operating System Information

## Portal Registration

### Register for the Certification Program [here](#)

- Alliance reviews the submission and sends a one-time log-in to change password (check spam folder)
- Follow the link provided in the email and set a permanent password



**Certification Program**

### Register for the ioXt Certification Program

Enter your information and an ioXt Alliance representative will contact you to begin the Certification Program.  
If you are currently not an Implementor or Contributor member with the ioXt Alliance, by registering you will be upgraded to the Implementor membership. [Click here](#) for additional information on membership levels.

Full Name

Phone

Company

## Submit Device

### 1. Add your device details:

- Select '+' and upload image of the device
- Complete the product details form including the operating system and firmware information

Profile  
Devices  
Documents

+

**Android Phone**  
Device Maker  
Certification Method: --  
Certification Type: IoT 2020 - Android  
Ecosystems: Works with Android, Works with Google Assistant  
Update

**Product Details**

Product Name  
Product SKU  
Product Description

### 2. Select the Android Profile and Certification Method:

- Select the profile within Certification Type field
- Select self-certification or Authorized lab within Certification Method

Certification Type: IoT 2020 - Android

Certification Method: Manufacturer Certified

Publication Date: Authorized Labs - Black box certified

Manufacturer Usage Description: Authorized Labs - White box certified

Cancel Next

### 3. If Selecting an Authorized Lab, complete the Security Testing Questionnaire

- After submitting the questionnaire, the Authorized Lab will complete the remainder of the portal wizard described in steps (4-6) below

**Security Testing Questionnaire**

Company Name: Device Maker

Company Address: address

Name of technical contact: Charlie Smith

Email: csmith@iott.com

Work Phone: 404-759-1812

Product Name: Android Phone

Product SKU: 1234567890

Firmware Version #: 1.0

4. If Self-Certifying, select any partner certifications applicable to device:

**Android Phone**  
Firmware Version # 1.0

**External Certifications**

Select all applicable ioXt partner certifications for this device firmware version from the list below. Click Next to skip.

**Certification Type**

Android GMS Certification

5. Submit results for the 10 Pledge steps located on the left-hand side of the dashboard:

**MANUFACTURER**

- 1 Vulnerability Reporting Program
- 2 Security Expiration
- 3 **Automatically Applied Updates**
- 4 Verified Software
- 5 Cryptography
- 6 Secured Interfaces
- 7 Security by Default
- 8 No Universal Password
- 9 Android certification
- 10 Review

**Android Phone**  
Firmware Version: # 1.0  
Certification Profile: ioXt 2020 - Android

**LEVEL 0**  
(In Progress)

Submit a Question

**Automatically Applied Updates**

Documentation is optional to progress in this questionnaire. The documentation confidentially is maintained by the Alliance, and is used to arbitrate researcher certification disputes.

	YES	NO	N/A
AA1 - Software updates are supported	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
AA2 - Software is maintained and updated	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
AA3 - Security updates are made available to impacted parties	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
AA4 - Security updates applied automatically, when device usage allows	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Previous    Exit wizard    Next

6. Review Pledge Levels:

- Carefully review device results, check 'Product Subscription Agreement' box and submit results
- Submit subscription fee payment or generate an invoice

**MANUFACTURER**

- 4 Verified Software
- 5 Cryptography
- 6 Secured Interfaces
- 7 Security by Default
- 8 No Universal Password
- 9 Android certification
- 10 **Review**

**LEVELS**

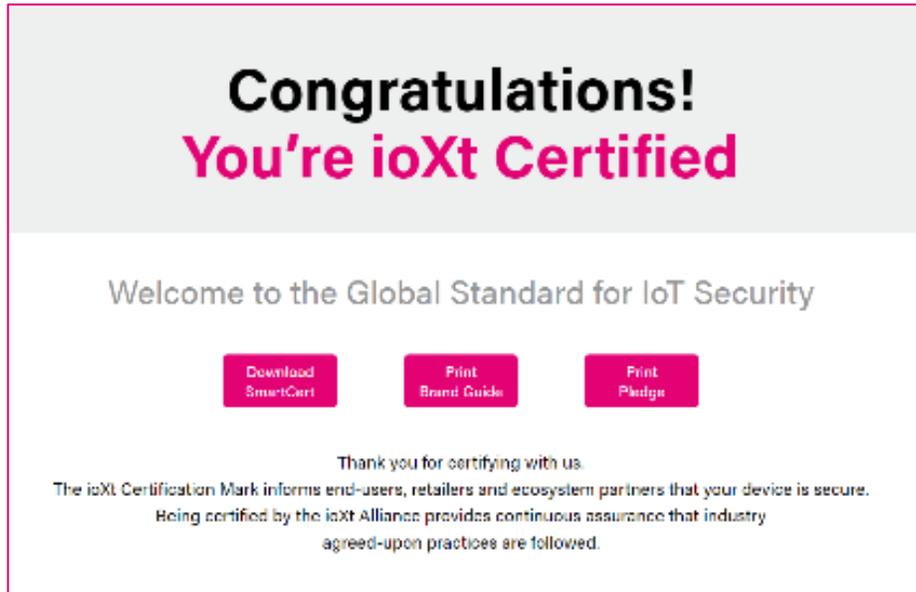
- 1) Vulnerability Reporting Program: 4
- 2) Security Expiration: 4
- 3) Automatically Applied Updates: 5
- 4) Verified Software: 6
- 5) Cryptography: 3
- 6) Secured Interfaces: 3
- 7) Security by Default: 4
- 8) No Universal Password: 4

By checking this box, I agree, to the terms and conditions set forth in the Product Subscription Agreement.

Previous    Exit wizard    Submit

## Certification

After successful payment completion or invoice creation, Certification confirmation is emailed, and collateral is immediately downloadable:



### Additional subscription benefits include:

- Ongoing certification validation
- Ongoing security alerts
- Testing by third parties through Researcher Rewards and University Rewards Programs



ioXt SmartCert Logo



Quarterly Compliance Report



Brand Guidelines