Wireless Test Solutions

Onboarding Tool and Generic Client (OTGC) for OCF

User Manual

DEKRA Testing and Certification, S.A.U.
Parque Tecnológico de Andalucía
C/ Severo Ochoa, 2 & 6
29590 Málaga - Spain
☎. +34 952 61 91 00
Fax. +34 952 61 91 13
e-mail: terd_wts_support.es@dekra.com
web: www.dekra-product-safety.com/wireless

VERSION CONTROL

Version	Date	Change log
1.0	2018-05-24	Initial version
1.1	2018-10-02	Update Android section to FFP. Include Linux section.

Disclaimer

© 2018 DEKRA Testing and Certification, S.A.U. Please note that use of this document is conditioned by the following:

The information in this document is subject to change by DEKRA Testing & Certification, S.A.U. without notice.

Contents in this document are considered to be reliable and trustable by DEKRA at the time of publication but it is not guaranteed. Use of this document is at the reader's sole risk. Under no circumstances shall DEKRA be liable for any direct, indirect, incidental, special or consequential damages arising from any error or omission in this document.

No warranties express or implied, are given by DEKRA. All implied warranties, including implied warranties of merchantability, fitness for a particular purpose, and non-infringement are disclaimed and excluded by DEKRA.

The document does not constitute an endorsement, recommendation or guarantee of any of the products (hardware or software) mentioned. The document does not guarantee that there are no errors of defects in the products or that the products will meet the reader's expectations needs or specifications, or that they will operate without interruption.

This document does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this document.

TABLE OF CONTENTS

TABLE OF FIGURES

1 SCOPE

The present document is the User Manual of the Onboarding Tool and Generic Client (OTGC) for Open Connectivity Foundation (OCF). This document describes how to use the Full Function Product (FFP) version of the OTGC, which is currently formed by an Android application and a Linux application. In subsequent revisions of this document, iOS and Universal Windows Platform (UWP) versions will be added.

In section 0, this document specifies the user instructions of the Android application.

In section 0, this document shows how the Linux application can be used.

2 REFERENCES

[1] "https://openconnectivity.org/specs/OCF_Security_Specification.pdf," [Online].

3 DEFINITIONS AND ABBREVIATIONS

3.1 DEFINITIONS

Access Management Service (AMS)

Service implemented by an OCF Client that provisions access policies to other OCF Devices in order to allow or deny access to their resources. [1]

Credential Management Service (CMS)

Service implemented by an OCF Device that is authorized to provision credentials to other OCF Devices. [1]

Device Ownership Transfer Service (DOXS)

Service implemented by an OBT in order to manage the ownership of the devices in its network. [1]

Generic Client (GC)

An OCF Client that is able to manipulate all kind of OCF Servers.

OCF Server

A sensor or actuator capable of generating a measurement or performing an action.

OCF Client

A device capable of scanning and controlling OCF Servers.

OCF Device

A device (Server or Client) that can be incorporated into an OCF network created by an Onboarding Tool (OBT). An OBT can own an OCF Device using different Ownership Transfer Methods (OTMs).

Offboarding

Process that consists in releasing an OCF device owed by the OTGC.

Onboarding Tool and Generic Client (OTGC)

A logical entity that implements the functions of an OBT and a GC.

Onboarding

Process that consists in owning an OCF device by the OTGC.

Onboarding Tool (OBT)

A logical entity within a specific Internet of Things (IoT) network that establishes ownership for a specific device and helps bring the device into operational state within that network. An OBT shall implement DOXS and could implement AMS and CMS functionalities too. [1]

3.2 ABBREVIATIONS

For the purposes of the present document, the following abbreviations apply:

ACL	Access Control List
AMS	Access Management Service
CMS	Credential Management Service
CTT	Conformance Test Tool
DOTS	Device Owner Transfer Service
FFP	Full Function Product
GC	Generic Client
IoT	Internet of Things
OBT	Onboarding Tool
OCF	Open Connectivity Foundation
OTGC	Onboarding Tool and Generic Client
OTM	Ownership Transfer Method
RFNOP	Ready for Normal Operation
RFOTM	Ready for OTM
UWP	Universal Windows Platform

4 USER INSTRUCTIONS

4.1 OVERVIEW

The OTGC application is a tool that allows the following main actions:

1. Scan all visible OCF devices.
2. Act as DOXS and onboard OCF devices owning them by different OTMs.
3. Act as DOXS and offboard OCF devices whenever the user wants.
4. Act as GC and control OCF Servers, previously onboarded or allowed by Access Control List (ACL).
5. Act as CMS and provision credentials.
6. Act as AMS and provision access control policies.

An OCF device, i.e., bulb, fan, blind, temperature sensor, etc. can be owned and manipulated. OTGC application allows Generic Client features, like retrieving the temperature detected by a sensor, configuring the air conditioning, increasing the temperature or turning on/off the light with a simple click.

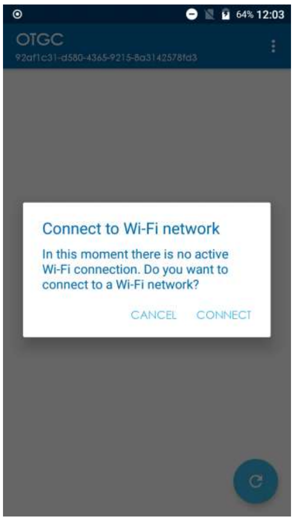
The OTGC application also allows getting information about de devices owned by introspecting them.

It can also act as AMS to provision an access control policy to permit to an OCF Client to control an OCF server or act as CMS to provision a credential to permit to an OCF client to authenticate with an OCF server.

4.2 ANDROID

4.2.1 WI-FI SCANNING

When OTGC starts, it checks if there is an active Wi-Fi connection on the device. If no connection is established, a dialog window opens in order to enable Wi-Fi on the device (if turned off) and connects it to a network as shown in Figure 1.



Connect to Wi-Fi network

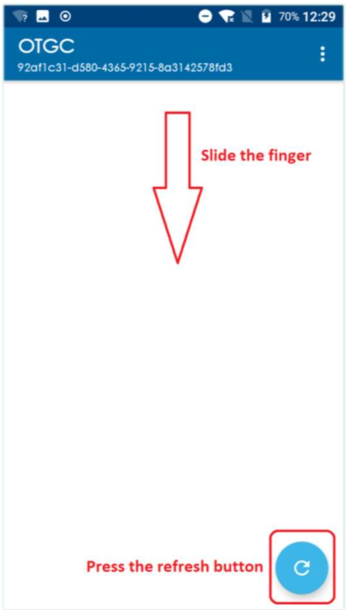
In this moment there is no active Wi-Fi connection. Do you want to connect to a Wi-Fi network?

Figure 1: “Connect to Wi-Fi network” dialog.

4.2.2 DEVICE SCANNING

When an active Wi-Fi connection exists and the OTGC starts, all visible OCF devices can be scanned. In order to do that, there are two possibilities:

1. Click the refresh button at bottom.
2. Slide the finger from top to bottom.



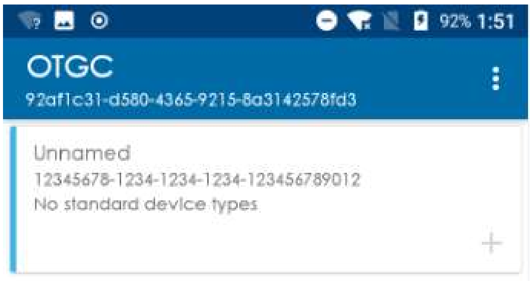
OTGC

92af1c31-d580-4365-9215-8a3142578fd3

Figure 2: Empty devices list screen.

When the scan finishes, OTGC lists all OCF devices it finds, with different color depending on the state of the device:

- Blue: unowned state. The device has no owner and can be incorporated to an OCF network.
- Green: owned-by-self state. The device belongs to the OTGC, which is the owner.
- Orange: owned-by-other state. The device belongs to another owner.



OTGC

92af1c31-d580-4365-9215-8a3142578fd3

Unnamed

12345678-1234-1234-1234-123456789012

No standard device types

Figure 3: Devices list with an OCF device detected.

4.2.3 ONBOARD A DEVICE

OTGC can only onboard an unowned device. Unowned devices can be onboarded by pressing on the plus icon that appears next to the device identifier, as shown in Figure 4.

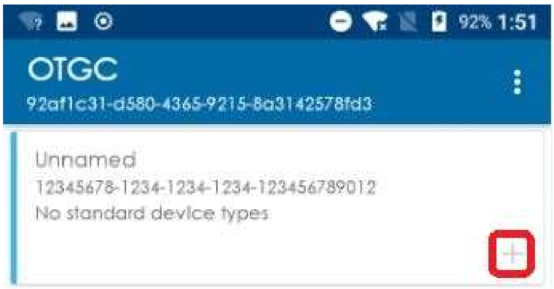

OTGC
92af1c31-d580-4365-9215-8a3142578fd3
Unnamed
12345678-1234-1234-1234-123456789012
No standard device types

Figure 4: Onboard button.

When the onboard process finishes and is successful, the recently onboarded device changes its state to owned-by-self (green). If ownership transfer fails, the OTGC shows an error message.

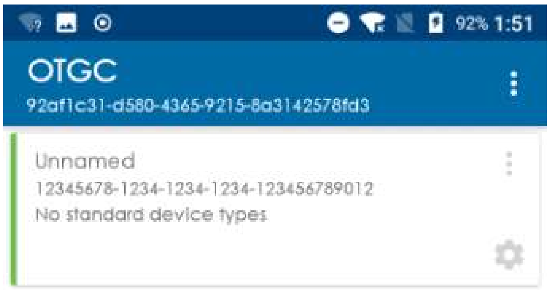
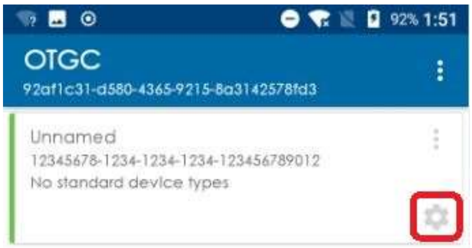

OTGC
92af1c31-d580-4365-9215-8a3142578fd3
Unnamed
12345678-1234-1234-1234-123456789012
No standard device types

Figure 5: Owned-by-self device.

4.2.4 MANAGE A DEVICE

The OTGC acts as GC on OCF devices that are owned by it. If the OCF device is owned by other OBT an access control policy has to be provisioned to it in order to make possible to the OTGC to interact with its resources.

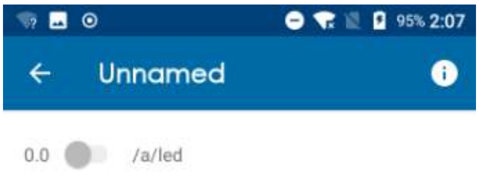
To access to the GC options, press the gear icon and a new screen appears showing all the resources the device implements. If the OTGC has not permissions, it shows an error message.



OTGC
92af1c31-d580-4365-9215-8a3142578fd3

Unnamed
12345678-1234-1234-1234-123456789012
No standard device types

Figure 6: Generic Client button.

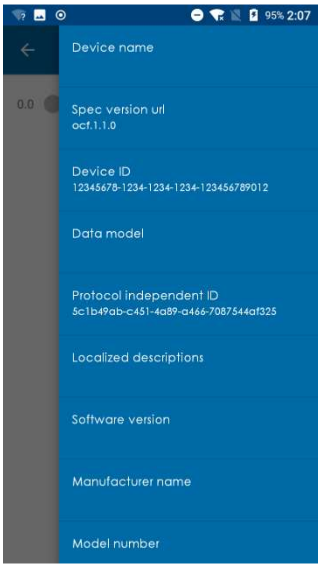


Unnamed

0.0 /a/led

Figure 7: Resources in an OCF server

As shown above in Figure 7, all resources implemented by the target device and supported by the OTGC are loaded after accessing the GC. Also, the information of the OCF device can be checked after clicking in the information icon, sited at top-right, or sliding the finger from right to left.



Device name

Spec version url
ocf.1.1.0

Device ID
12345678-1234-1234-1234-123456789012

Data model

Protocol independent ID
5c1b49ab-c451-4a89-a466-7087544af325

Localized descriptions

Software version

Manufacturer name

Model number

Figure 8: Device information panel.

4.2.5 CREDENTIALS

When the OTGC acts as CMS, it is able to retrieve the installed credentials of a certain OCF Device, delete them or provision new ones to allow the authentication between other OCF Devices and the target device.

Clicking on the “Credentials” option, as shown in Figure 9, the OTGC lists the currently installed credentials. A credential can be deleted by clicking the trash icon.

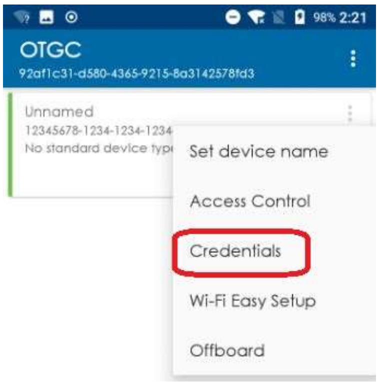


Figure 9: Credentials option.

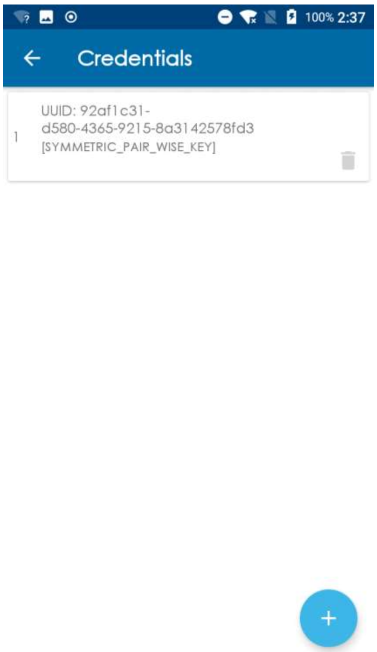
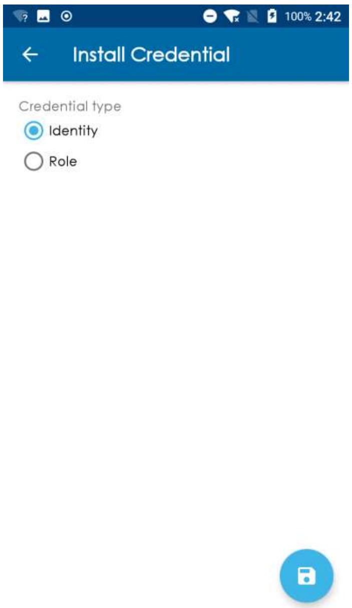

100% 2:37
Credentials
1
UUID: 92af1c31-d580-4365-9215-8a3142578fd3
[SYMMETRIC_PAIR_WISE_KEY]
+

Figure 10: Currently installed credentials list.

There are two types of credentials that the OTCG can provision:

- Identity certificates.
- Role certificates.

To provision a credential, click on the bottom-right button of Figure 10 and a new screen will load where to provision a new credential for the owned device selecting the type of the credential to provision and clicking in the save button at bottom, as Figure 11 shows.



100% 2:42

Install Credential

Credential type

● Identity

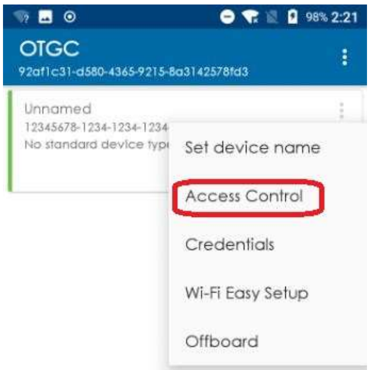
○ Role

Figure 11: Provision a new credential.

4.2.6 ACCESS CONTROL LIST

When OTGC acts as AMS, it is able to retrieve the current access control policies of a certain OCF device, delete them or provision new ones to allow other OCF Devices to interact with the target OCF Device.

Clicking on the "Access Control" button, the OTGC displays the current ACLs. An existing access control policy can be deleted by pressing the trash icon, as shows Figure 13.



98% 2:21

OTGC

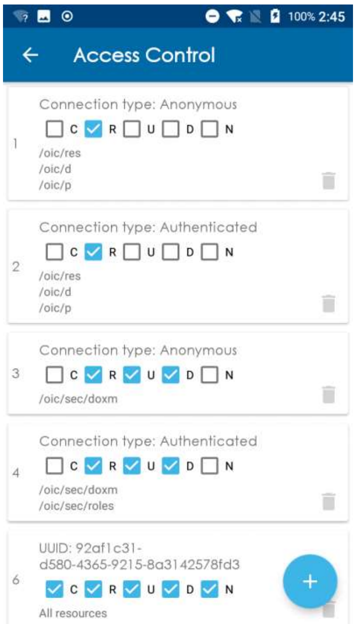
92af1c31-d580-4365-9215-8a3142578fd3

Unnamed

12345678-1234-1234-1234

No standard device typ

Figure 12: Access Control option.



1
Connection type: Anonymous
□ C ☑ R □ U □ D □ N
/oic/res
/oic/d
/oic/p

2
Connection type: Authenticated
□ C ☑ R □ U □ D □ N
/oic/res
/oic/d
/oic/p

3
Connection type: Anonymous
□ C ☑ R ☑ U ☑ D □ N
/oic/sec/doxm

4
Connection type: Authenticated
□ C ☑ R ☑ U ☑ D □ N
/oic/sec/doxm
/oic/sec/roles

6
UUID: 92af1c31-d580-4365-9215-8a3142578fd3
☑ C ☑ R ☑ U ☑ D ☑ N
All resources

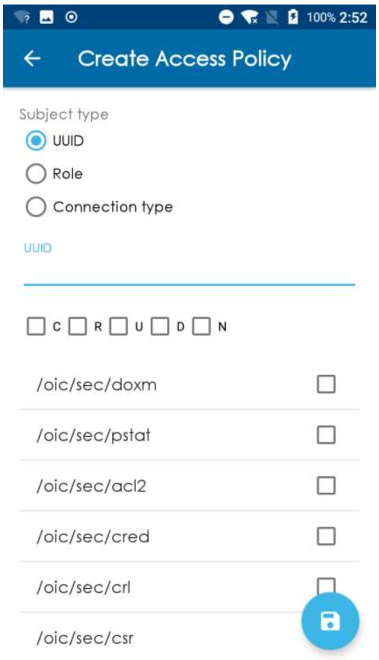
Figure 13: Access control list.

There are three types of access control policies that the OTCG can provision:

- For an UUID.
- For a role.
- For a connection type.

To provision an access control policy, click on the bottom-right button of Figure 13 and a new screen appears with a form to fill (Figure 14). The following fields can be configured:

- Subject type: kind of access control policy.
- Subject info: UUID, role identification or connection type, depending on the subject type.
- Permissions: create, retrieve, update, delete and/or notify.
- Resources: target resources of the policy to be created.



Subject type
● UUID
○ Role
○ Connection type

UUID

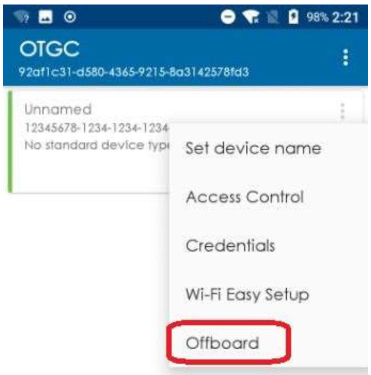
□ C □ R □ U □ D □ N

/oic/sec/doxm □
/oic/sec/pstat □
/oic/sec/acl2 □
/oic/sec/cred □
/oic/sec/crl □
/oic/sec/csr

Figure 14: Provision a new access control policy.

4.2.7 OFFBOARD A DEVICE

An OCF device owned by the OTGC can be unowned by clicking on the “Offboard” option, as shows Figure 15. If the action succeeds, the device changes its state to unowned.



Unnamed
12345678-1234-1234-1234
No standard device typ

Figure 15: Offboard an owned device.

4.2.8 WI-FI EASY SETUP

A new device may require to be connected via Wi-Fi to a network. In order to achieve that, the steps below have to be followed:

1. Connect to the Soft AP advertised by the new device.
2. Scan the network to find the new device and onboard it.
3. Click on options and select Wi-Fi Easy Setup (see Figure 16).

4. Introduce the credentials of the network the new device is going to connect to (see Figure 17).
5. Connect to the network and scan it to verify that the device has connected properly.

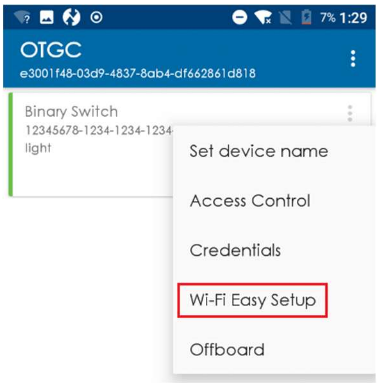


Figure 16: “Wi-Fi Easy Setup” option.

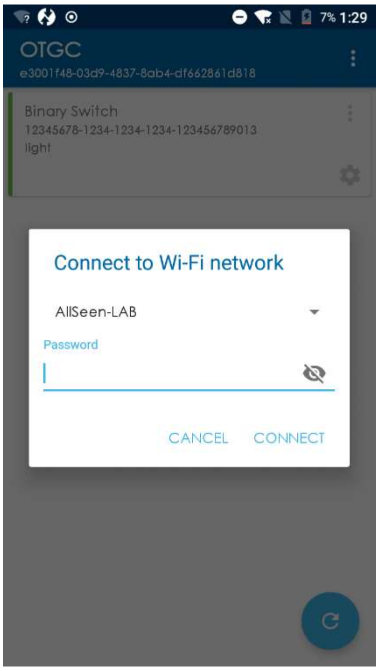


Figure 17: Input Wi-Fi credentials dialog.

4.2.9 RESET OTGC

Reset the OTGC to its default values can be achieved by clicking the Ready For Ownership Transfer (RFOTM) option placed on the toolbar as Figure 18 shows.

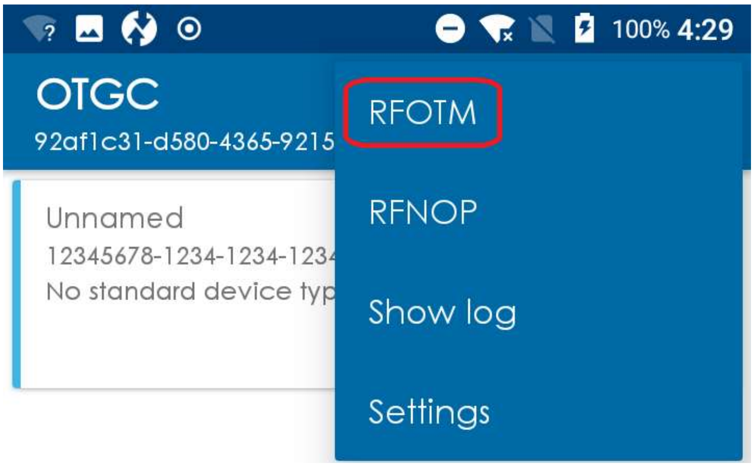


Figure 18: Reset OTGC.

This is normally done to introduce the OTGC in an OCF Network as GC instead of network owner.

4.2.10 SELF-OWN THE OTGC

To restore the OTGC to its normal operation status, click on the Ready For Normal Operation (RFNOP) button on the toolbar as Figure 19 shows.

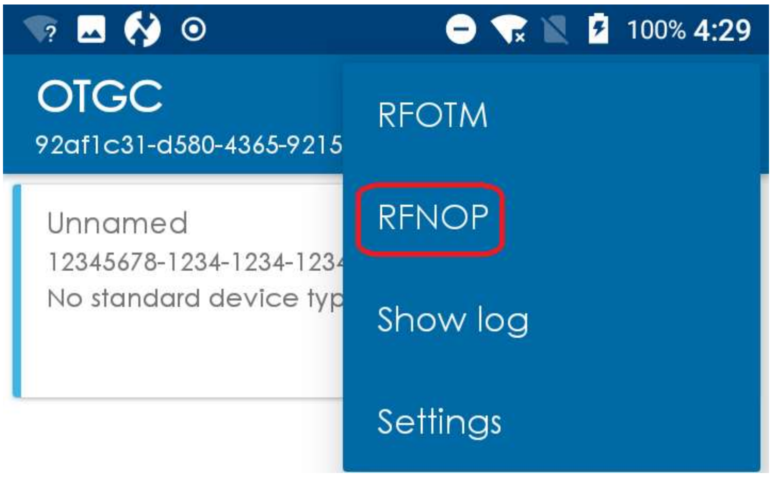


Figure 19: Self-own the OTGC.

4.3 LINUX

4.3.1 SCANNING DEVICES

When the OTGC starts, it automatically scans all visible OCF devices. To scan devices at any time, the "Discover" button in the navigation bar can be pressed to refresh the device list, as Figure 20 shows.

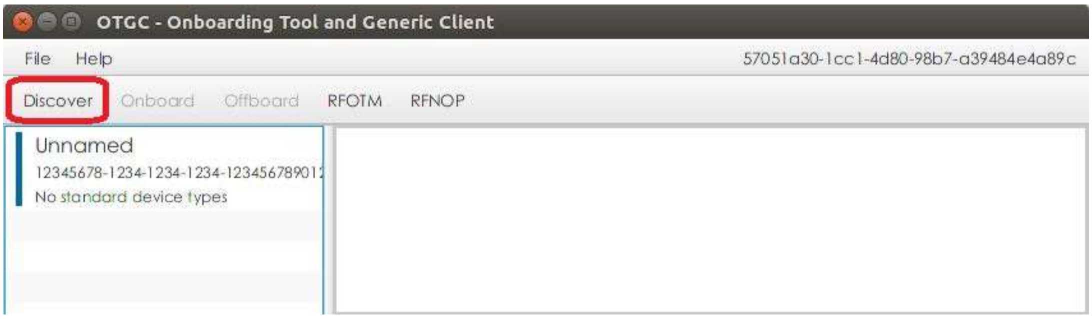


Figure 20: Scan devices in Linux.

When scan finishes, the OTGC shows a list with OCF devices similar to the specified in the section 4.2.2.

4.3.2 ONBOARD A DEVICE

OTGC can only onboard an unowned device. To onboard a device, select it from the devices list and click the "Onboard" button in the navigation bar, as Figure 21 shows.

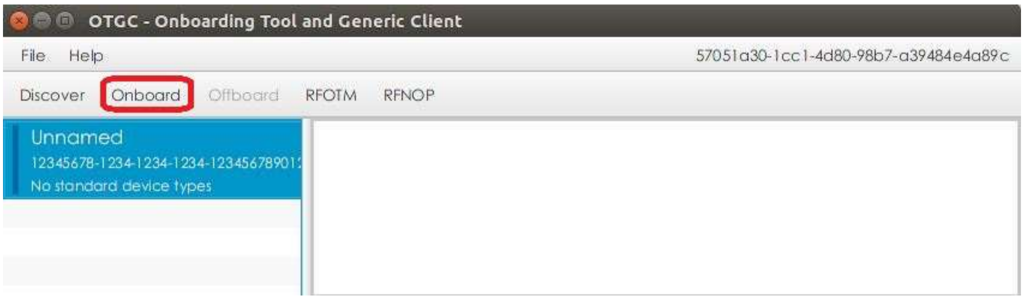
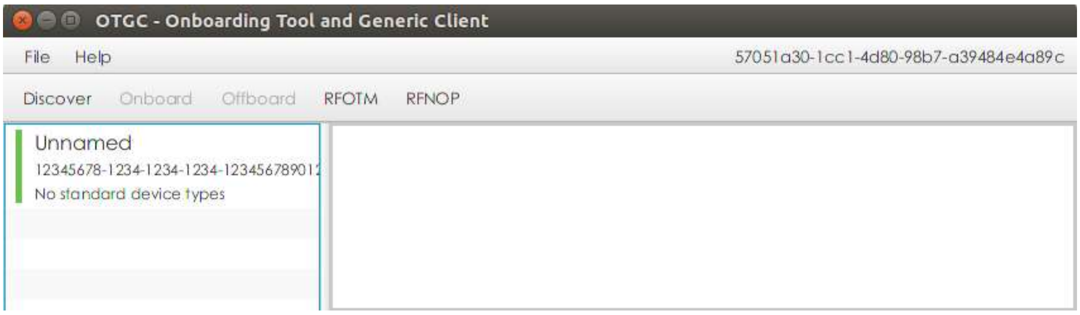


Figure 21: Onboard a device in Linux.

If the onboarding process succeeds, the list of OCF devices is refreshed and the device state changes to owned-by-self. If the process fails, the OTGC shows an error message with the cause.



57051a30-1cc1-4d80-98b7-a39484e4a89c

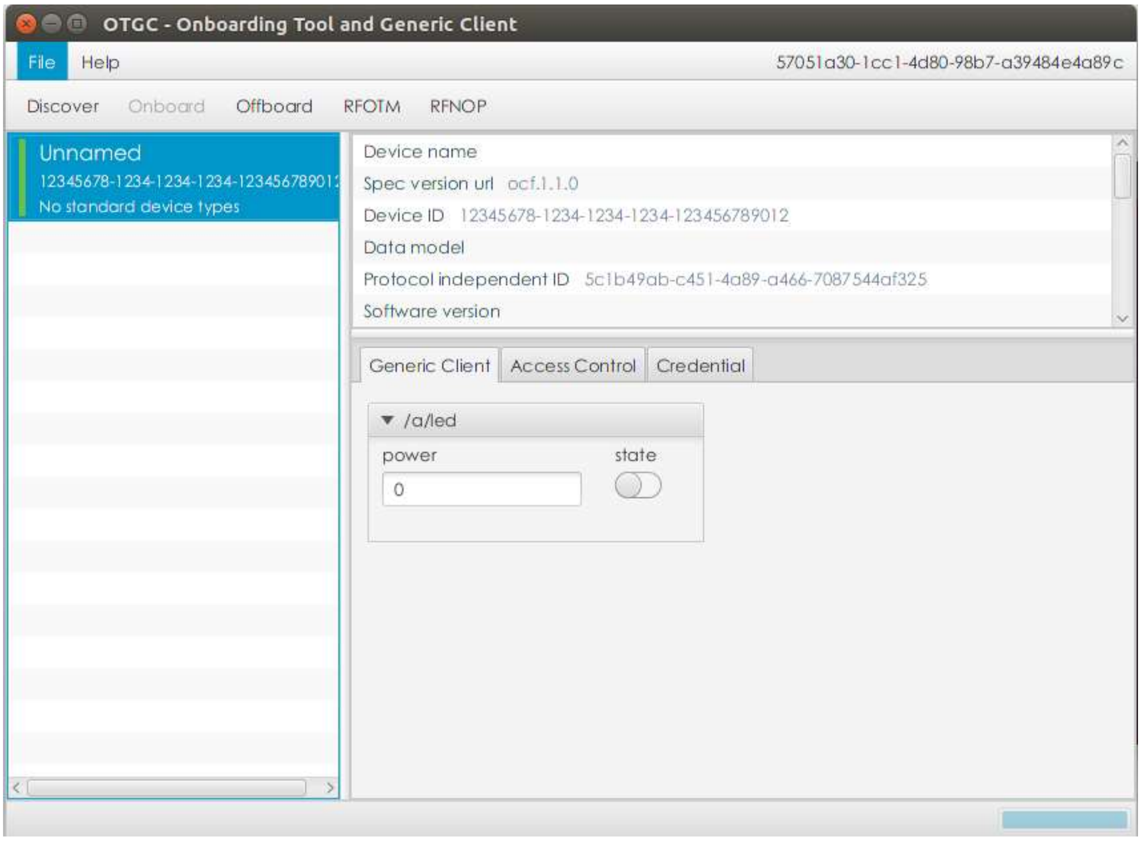
Unnamed
12345678-1234-1234-1234-12345678901
No standard device types

Figure 22: Devices list with an owned device in Linux.

4.3.3 MANAGE A DEVICE

When an owned device is selected, the following information is retrieved by the OTGC if the device allows it by access control policy:

- Device information: see Figure 23.
- Device resources: see Figure 23.
- Access control list: see Figure 24.
- Credentials: see Figure 25.



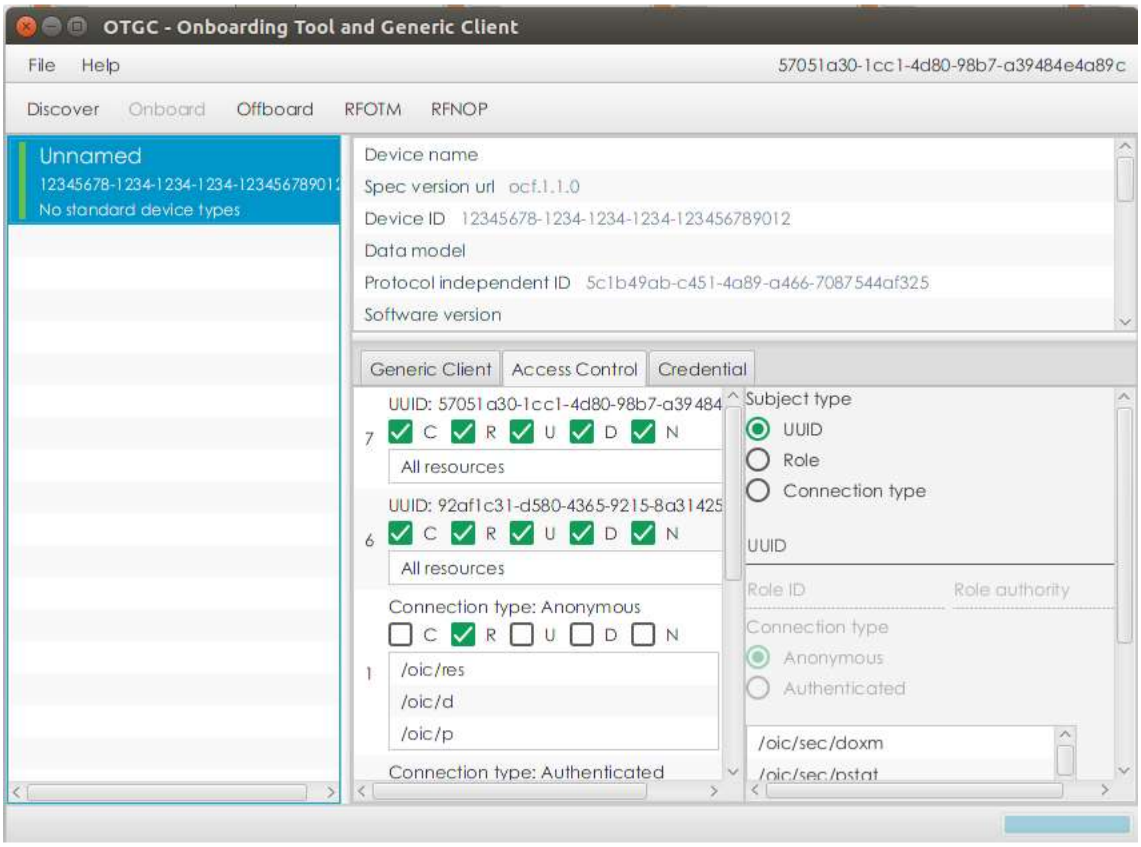
57051a30-1cc1-4d80-98b7-a39484e4a89c

Unnamed
12345678-1234-1234-1234-12345678901
No standard device types

Device name
Spec version url ocf.1.1.0
Device ID 12345678-1234-1234-1234-123456789012
Data model
Protocol independent ID 5c1b49ab-c451-4a89-a466-7087544af325
Software version

▼ /a/led
power 0
state

Figure 23: Device information and Generic Client in Linux.



57051a30-1cc1-4d80-98b7-a39484e4a89c

Unnamed
12345678-1234-1234-1234-12345678901
No standard device types

Device name
Spec version url ocf.1.1.0
Device ID 12345678-1234-1234-1234-123456789012
Data model
Protocol independent ID 5c1b49ab-c451-4a89-a466-7087544af325
Software version

7 UUID: 57051a30-1cc1-4d80-98b7-a39484
☑ C ☑ R ☑ U ☑ D ☑ N
All resources

6 UUID: 92af1c31-d580-4365-9215-8a31425
☑ C ☑ R ☑ U ☑ D ☑ N
All resources

1 Connection type: Anonymous
□ C ☑ R □ U □ D □ N
/oic/res
/oic/d
/oic/p

Connection type: Authenticated

Subject type
● UUID
○ Role
○ Connection type

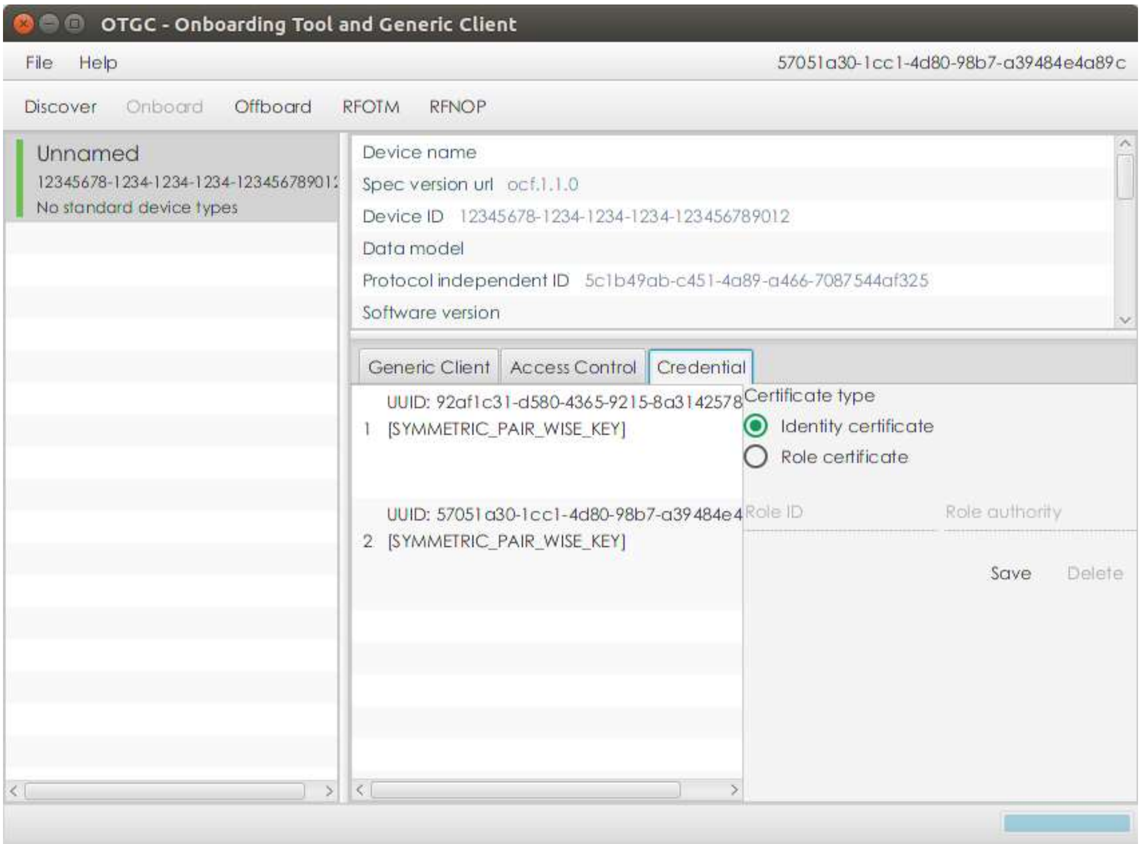
UUID

Role ID
Role authority

Connection type
● Anonymous
○ Authenticated

/oic/sec/doxm
/oic/sec/pstat

Figure 24: Access control in Linux.



OTGC - Onboarding Tool and Generic Client

57051a30-1cc1-4d80-98b7-a39484e4a89c

Unnamed
12345678-1234-1234-1234-12345678901
No standard device types

Device name
Spec version url ocf.1.1.0
Device ID 12345678-1234-1234-1234-123456789012
Data model
Protocol independent ID 5c1b49ab-c451-4a89-a466-7087544af325
Software version

UUID: 92af1c31-d580-4365-9215-8a3142578
1 [SYMMETRIC_PAIR_WISE_KEY]

UUID: 57051a30-1cc1-4d80-98b7-a39484e4
2 [SYMMETRIC_PAIR_WISE_KEY]

Certificate type
● Identity certificate
○ Role certificate

Role ID
Role authority

Figure 25: Credentials in Linux.

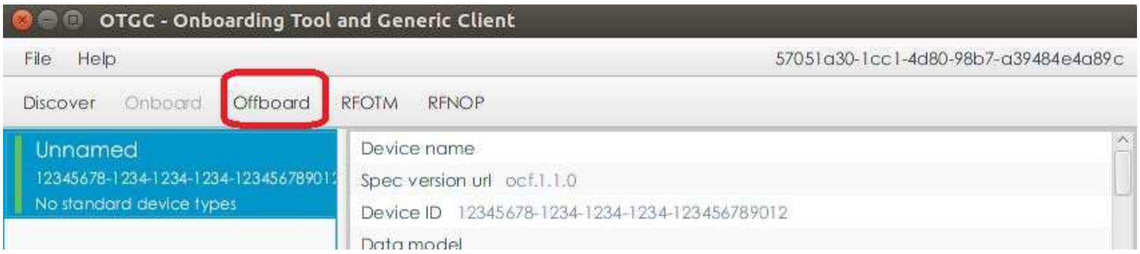
As Figure 24 shows, when “Access Control” tab is selected the OTGC allows provisioning a new access control policy selecting the type of access control and clicking on “Save” button. To delete an existing access control policy, an access control has to be selected in the access control list and click on “Delete” button. For more information about access control policies, go to section 4.2.6.

As Figure 25 shows, when “Credentials” tab is selected the OTGC allows provisioning a new credential selecting the type of credential and clicking on “Save” button. To delete an existing credential, a credential has to be selected in the credentials list and click on “Delete” button. For more information about credentials, go to section 4.2.5.

To deselect an OCF device, keep pressed “CTRL” and click in the OCF device to deselect.

4.3.4 OFFBOARD A DEVICE

An OCF device owned by the OTGC can be unowned selecting it and pressing “Offboard” button, as Figure 26 shows. After that, the device will change its state to unowned.



57051a30-1cc1-4d80-98b7-a39484e4a89c

12345678-1234-1234-1234-12345678901

No standard device types

Device name

Spec version url ocf.1.1.0

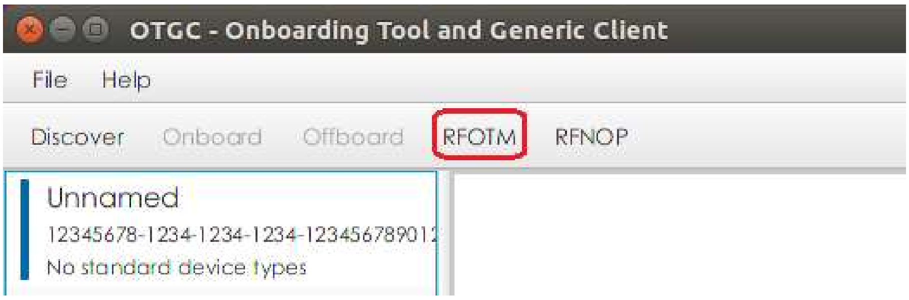
Device ID 12345678-1234-1234-1234-123456789012

Data model

Figure 26: Offboard a device in Linux.

4.3.5 RESET OTGC

To reset the OTGC to its default values, it has to return to RFOTM state by clicking on “RFOTM” button in the options sited on toolbar (see Figure 27).



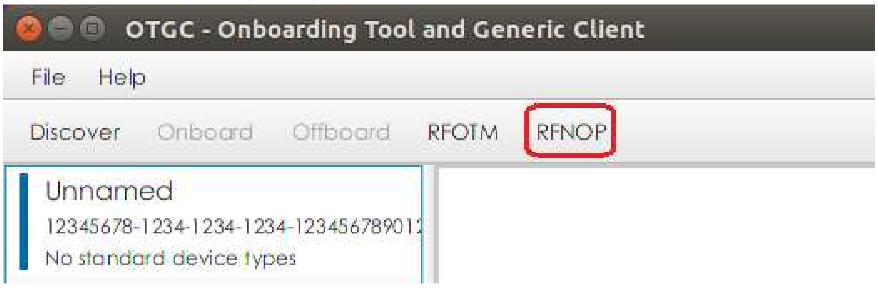
12345678-1234-1234-1234-12345678901

No standard device types

Figure 27: Reset OTGC in Linux.

4.3.6 OWNED OTGC BY SELF

To self-own the OTGC, click on the “RFNOP” button on toolbar (see Figure 28).



12345678-1234-1234-1234-12345678901

No standard device types

Figure 28: Self-own OTGC in Linux.

4.4 IOS

TBD

4.5 UWP

TBD