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.
1.2	2018-11-30	Include Universal Windows Platform section. Include iOS section.
1.3	2019-03-04	Add pairwise devices and link device to a role section (Phase 1-Ext).
1.4	2019-10-08	Add Phase 2 scope for Android and Linux platforms: - IoTivity-Lite core migration. - Trust anchor management. - Different IPv6 scopes for the discovery process. Update screenshots. Changed RFOTM and RFNOP sections by OBT and Client modes. Added CTT section.
1.5	2019-12-02	Add onboarding of multiple devices in Onboard section.

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 Android, iOS, Linux and Windows 10 applications.

In section 4.2, this document specifies the user instructions of the Android application.

In section 4.3, this document shows how the Linux application can be used.

In section 4.4, this document shows how the Windows 10 application can be used.

In section 4.5, this document includes the user instructions of the iOS version.

In section 5, this document provides useful information to perform CTT testing.

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.

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

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.

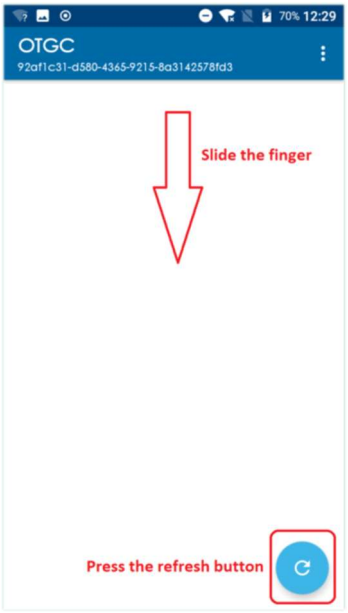

Figure 2: Empty devices list screen, Android.

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.
- Yellow: owned-by-other state. The device belongs to another owner but OTGC has certain level of access (depending on access policies) to secure resources.

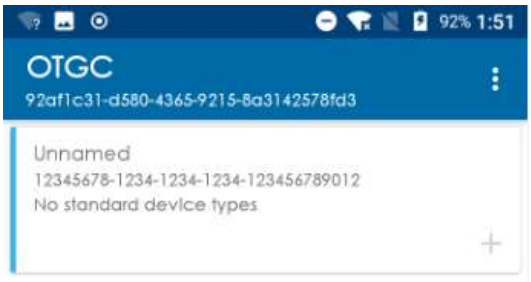

Figure 3: Devices list with an OCF device detected, Android.

OTGC v2.x.x, based on IoTivity-Lite, can discover devices using different multicast IPv6 scopes. These scopes determine the number of hops between routers to find the device in a discovery process. By default, “Link-Local” is selected and that means only one hope is made in a discovery process. Clicking on the three dots menu at top-right and selecting the “Settings” option and then “Discovery” option, the OTGC will show settings about discover process. As Figure 4 shows, the multicast IPv6 scope options are:

- Link-Local scope.
- Site-Local scope.
- Realm-Local scope.

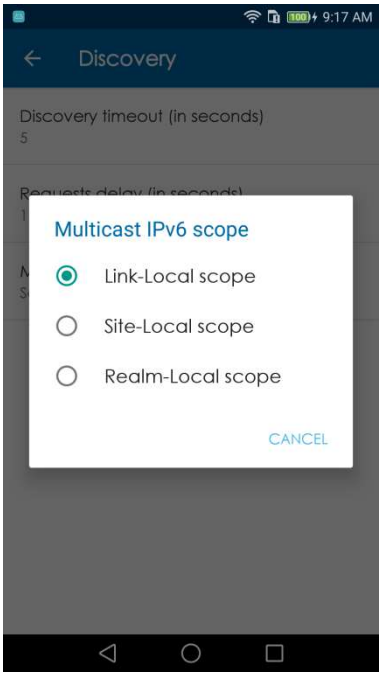

Figure 4: Multicast IPv6 scopes, Android.

4.2.3 ONBOARD A DEVICE

OTGC can only onboard an unowned device in OBT mode. Unowned devices can be onboarded by clicking on the plus icon that appears next to the device identifier, as shown in Figure 5.

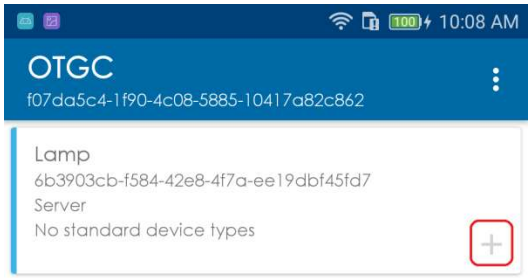

Figure 5: Onboard button, Android.

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.

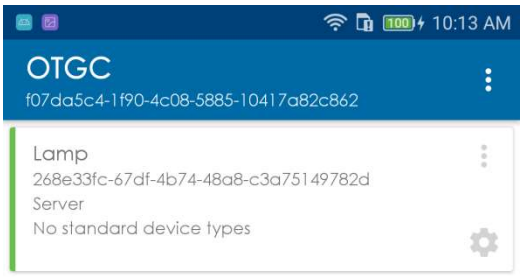

Figure 6: Owned-by-self device, Android.

OTGC v2.x.x, based on IoTivity-Lite can onboard multiple devices at the same time. To select multiple devices, make a long click on a device and select all unowned devices which are going to be onboarded. If all selected devices are unowned (listed in blue color), the “Onboard” button will appear in the menu as Figure 7 shows and, by clicking on this button, the OTGC will onboard all selected devices. Otherwise, if the state of some of the devices is different than unowned (blue color), the “Onboard” button will not appear as Figure 8 shows. OTGC will try first to onboard by PKI (user certificate). If this OTM is not supported by the device, OTGC will retry the onboarding by using Random PIN. If this OTM is also not supported by the device, Just Work OTM will be used.

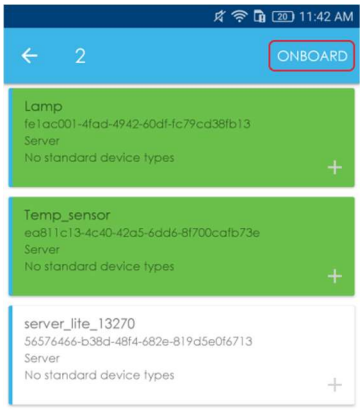

Figure 7: Onboard multiple unowned devices, Android.

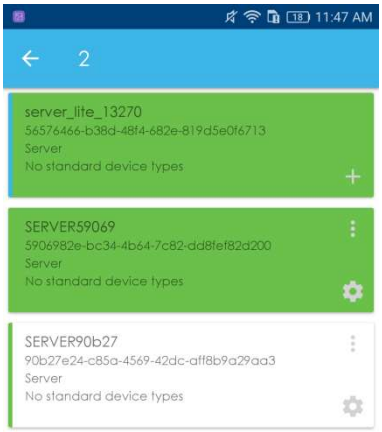

Figure 8: Onboard button is not shown with an owned device selected, Android.

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.

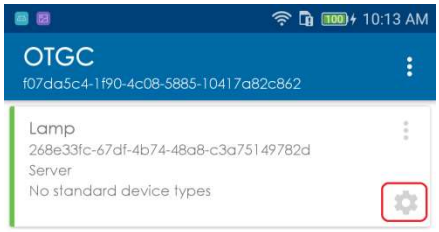

Figure 9: Generic Client button.

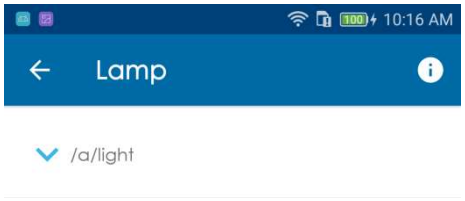

Figure 10: Resources in an OCF Server, Android.

As shown above in Figure 10, 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.

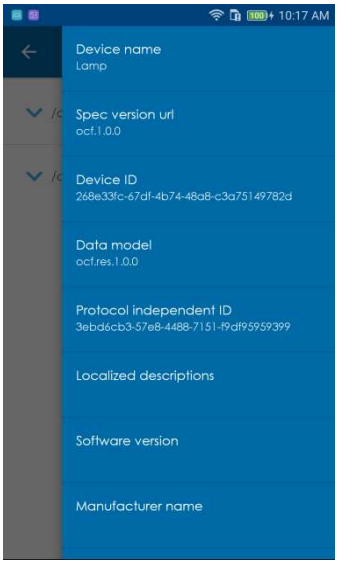

Figure 11: Device information panel, Android.

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 12, the OTGC lists the currently installed credentials. A credential can be deleted by clicking the trash icon.

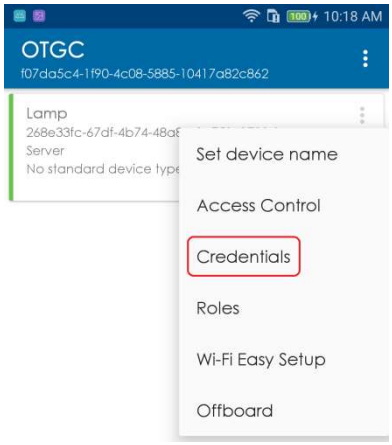

Figure 12: Credentials option, Android.

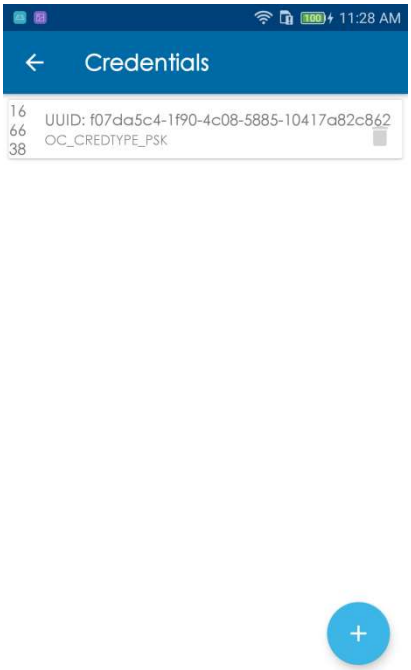

Figure 13: Currently installed credentials list, Android.

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 13 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 14 shows.

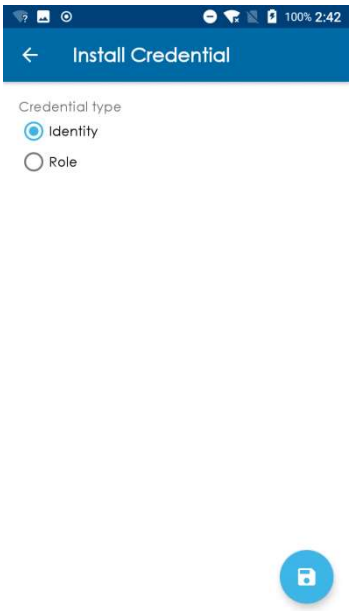

Figure 14: Provision a new credential, Android.

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 16.

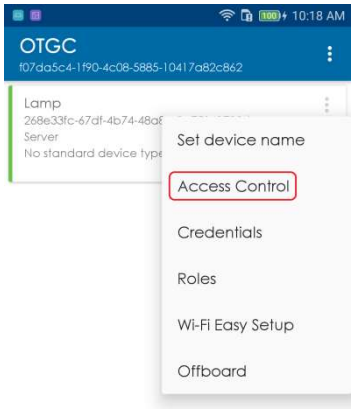

Figure 15: Access Control option, Android.

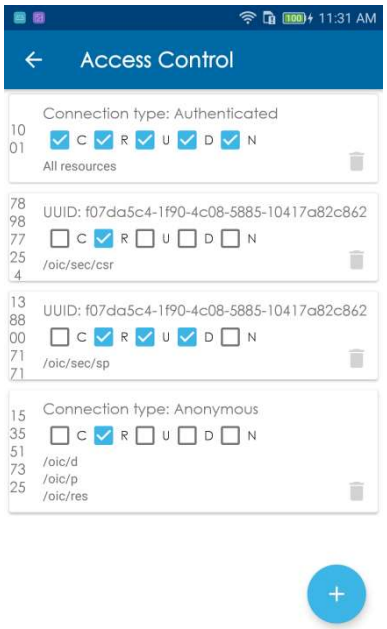

Figure 16: Access control list, Android.

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 16 and a new screen appears with a form to fill (Figure 17). 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.

Figure 17: Provision a new access control policy, Android.

4.2.7 PAIRWISE A DEVICE

The OTGC can pairwise a client and a server, which they are both owned by it, to allow the client device to manage the server. To pairwise the devices, make a long click to select them. Once, there are a client and a server both selected, the pairwise button will be enabled, as shows Figure 18:

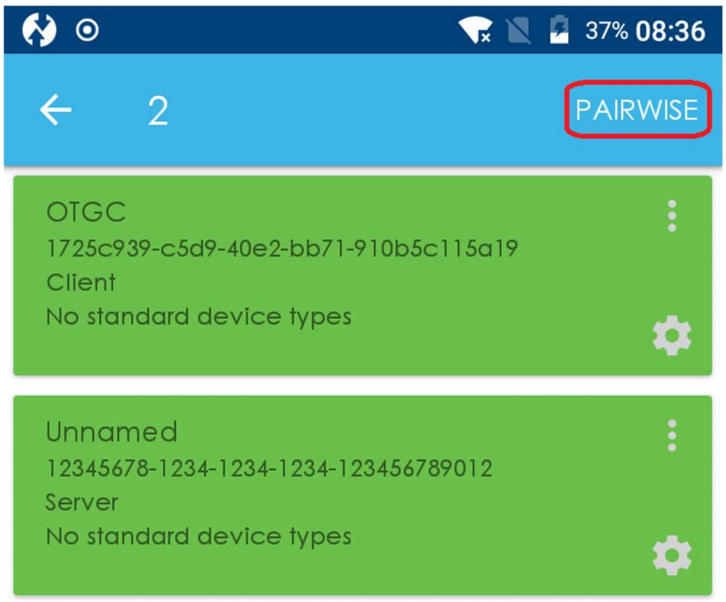

Figure 18: Pairwise devices, Android.

If the selected devices are already linked, then the unlink button will be enabled and the pairwise button will be disabled, as shows Figure 19:

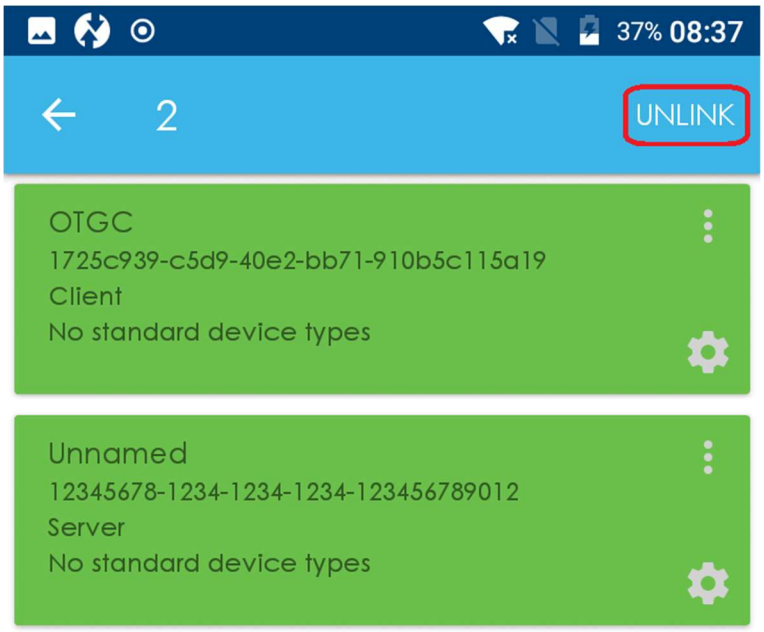

Figure 19: Unlink devices, Android.

The “Link” or “Unlink” button will not be displayed in the following situations:

- The role of a device appears as “Unknown”, instead of “Client” or “Server”.
- The selected devices are not a Client and a Server.
- The Client or the Server has not been owned by the OTGC.
- User selects more than 2 devices.

4.2.8 LINK DEVICE TO A ROLE

The OTGC can add or remove its owned devices to a specific role to allow a group of OCF Clients to interact with a group of OCF Servers, which have the same role. In this context, a “role” is like a “group”.

By clicking on the “Roles” button, the OTGC displays the current linked roles. An existing role can be deleted by clicking on the trash icon, as shows Figure 21.

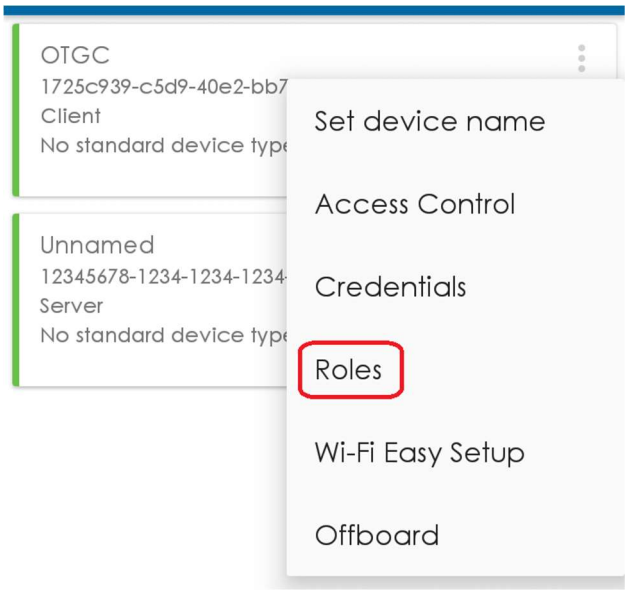

Figure 20: Roles option, Android.

Figure 21: Linked role list, Android.

To add a role, click on the right-button and a pop-up appears with a form to fill, as shows Figure 22. The following fields need to be provided:

- Role ID: role identification (i.e. “Family”).
- Role Authority: the authority for the role (i.e. “owner”).

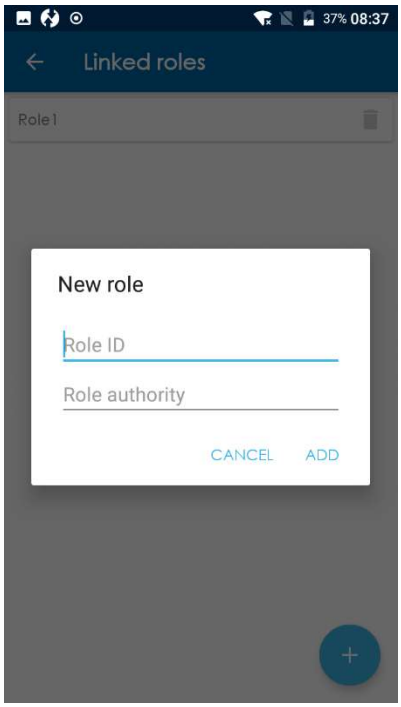

Figure 22: Link device to a role, Android.

Users can create the same role certificate (i.e. “Family”) in all onboarded OCF Clients and OCF Servers to be all in the same group. In this way, all OCF Servers in the same group (Role ID) can be controlled by all OCF Clients in that group.

4.2.9 OFFBOARD A DEVICE

An OCF device owned by the OTGC can be unowned by clicking on the “Offboard” option, as shows Figure 23. If the action succeeds, the device changes its state to unowned.

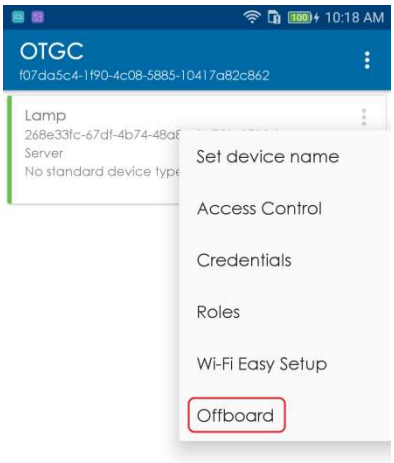

Figure 23: Offboard an owned device, Android.

4.2.10 WI-FI EASY SETUP

This WES mechanism is only available in OTGC v1.x.x, based on IoTivity classic. OTGC v2.x.x, based on IoTivity-Lite, does not support WES.

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 24).
4. Introduce the credentials of the network the new device is going to connect to (see Figure 25).
5. Connect to the network and scan it to verify that the device has connected properly.

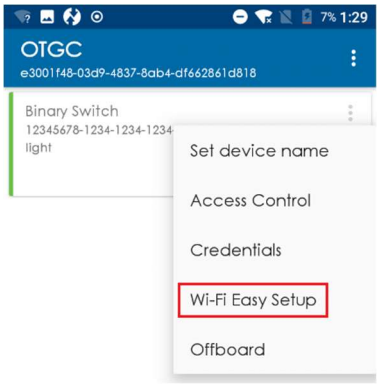

Figure 24: “Wi-Fi Easy Setup” option, Android.

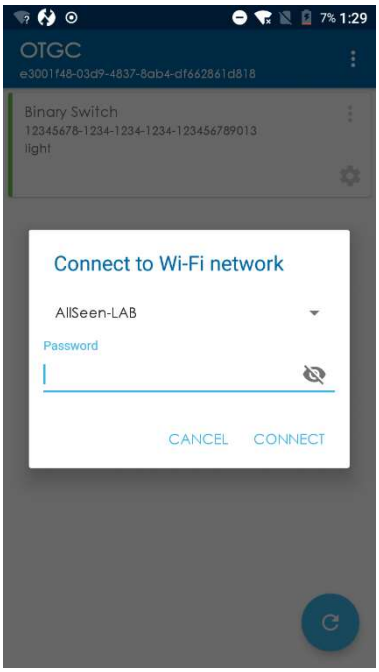

Figure 25: Input Wi-Fi credentials dialog, Android.

4.2.11 RESET OTGC

Reset the OTGC to its default values can be achieved by clicking the “Reset” option placed on the toolbar as Figure 26 shows.

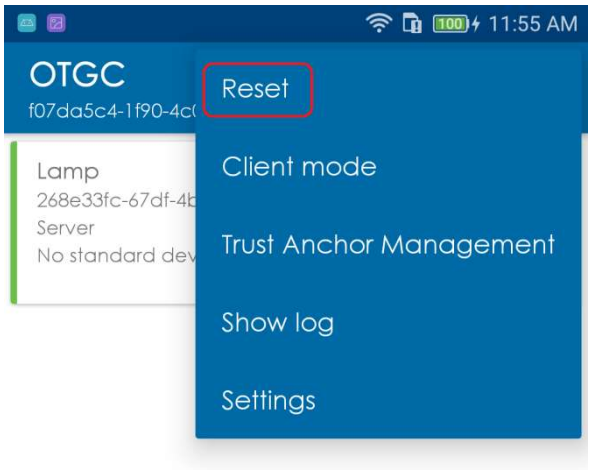

Figure 26: Reset OTGC, Android.

When the “Reset” button is clicked, the OTGC returns to its default values but it stays in the same mode (“OBT mode” or “Client mode”). By default, the OTGC starts in “OBT mode”. OTGC in “Client mode” does not allow any OBT action. This “Client mode” is needed, for example, to run CTT client test cases. See next sections for additional details.

4.2.12 OBT MODE

When the OTGC is in OBT mode, it is able to onboard/offboard devices and to provision ACEs and credentials to devices that are owned by it.

The OBT mode is enabled by default when the OTGC application is installed. Also, it can be enabled by clicking on the “OBT mode” button on the toolbar when the OTGC is in Client mode as Figure 27 shows.

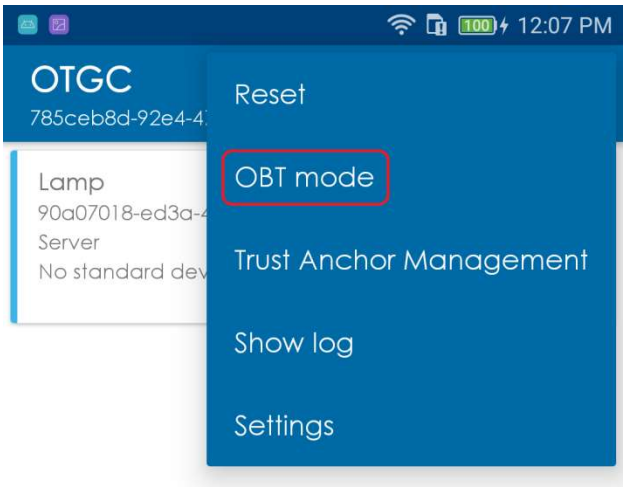

Figure 27: Change to OBT mode, Android.

Before to change the mode, an advice message will be shown to confirm that all linked devices will be deleted as Figure 28 shows.

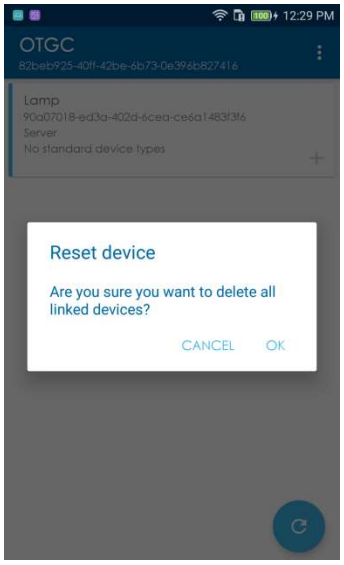

Figure 28: Advice message before to change the mode, Android.

4.2.13 CLIENT MODE

When the OTGC is in Client mode, it is not able to onboard/offboard devices, so if it tries to onboard a device while it is in Client mode, an error message appears as Figure 29 shows.

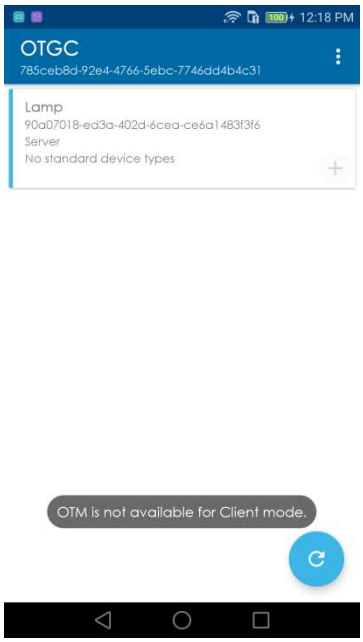

Figure 29: Error message in Client mode for the OTM, Android.

The Client mode can be enabled by clicking on the “Client mode” button on the toolbar when the OTGC is in OBT mode as Figure 30 shows.

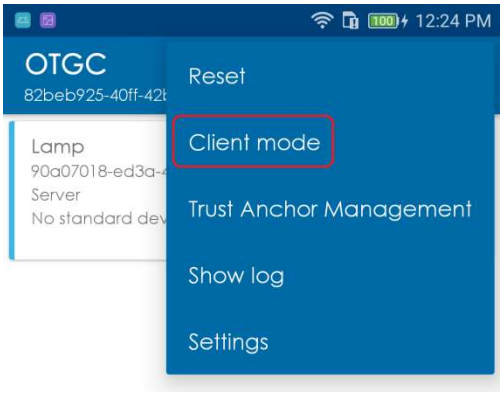

Figure 30: Change to Client mode, Android.

As discussed in section 4.2.12, an advice message will be shown to confirm that all linked devices will be deleted.

4.2.14 TRUST ANCHOR MANAGEMENT

In OTGC v2.x.x, based on IoTivity-Lite, a trust anchor certificate can be added into the credentials or an existing trust anchor can be removed from the credentials through the “Trust Anchor Management” option.

Click on the three dots at top-right menu and select the “Trust Anchor Management” option as Figure 31 shows and the OTGC will show a list of existing trust anchor certificates, as Figure 32 shows:

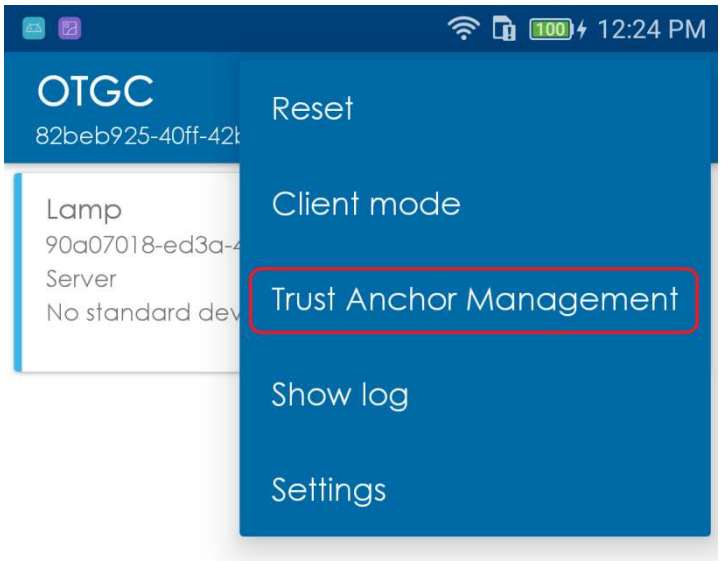

Figure 31: Trust Anchor Management, Android.

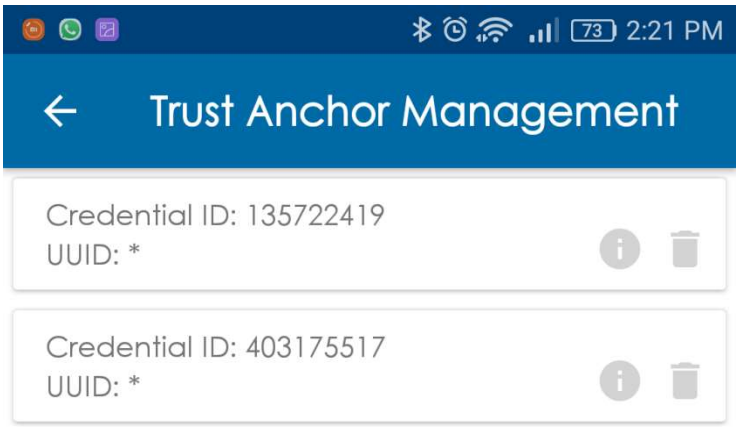

Figure 32: Trust anchor certificate list, Android.

To add a new one, click on the plus button, as Figure 33 shows, and select a root certificate in PEM format from the device storage, as Figure 34 shows.

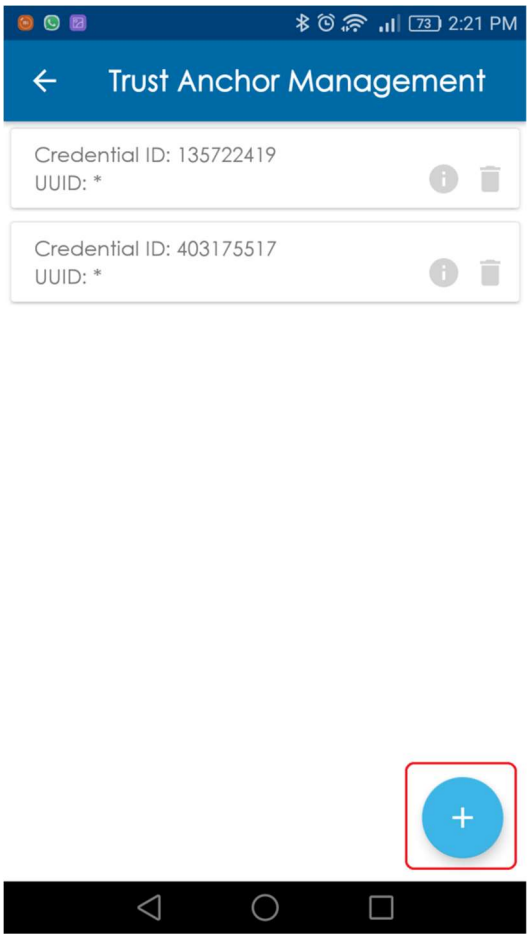

Figure 33: Add new trust anchor certificate, Android.

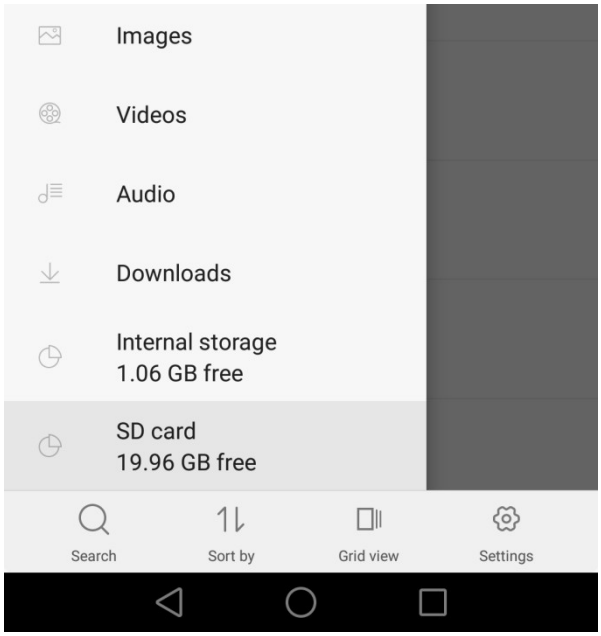

Figure 34: Device storage to select a root certificate, Android.

To see the information of the root certificate, click on the information button as Figure 35 shows, and the information of the certificate will show, as Figure 36 shows.

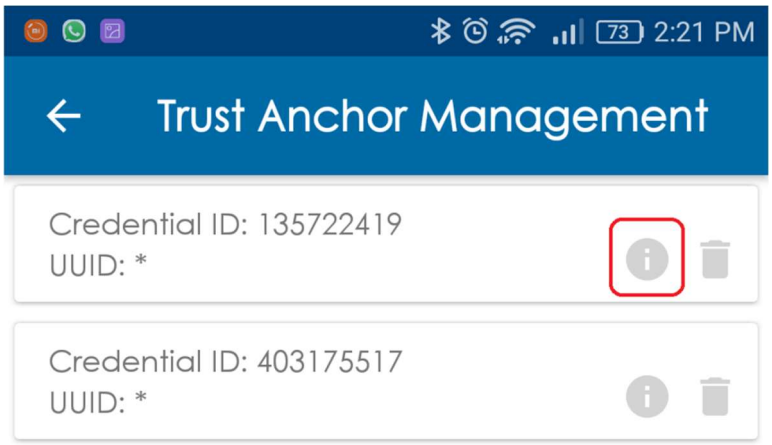

Figure 35: Show information of a trust anchor certificate, Android.

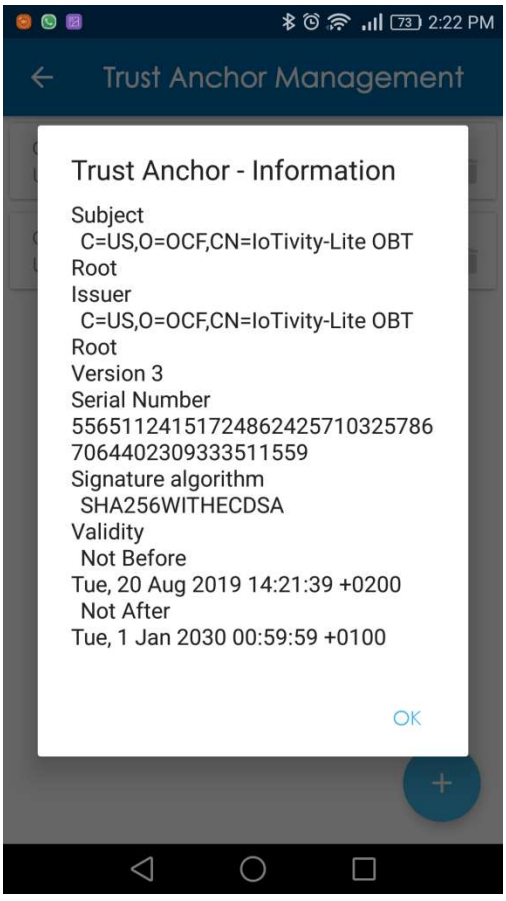

Figure 36: Information of a trust anchor certificate, Android.

To remove a certificate, click on the trash button, as Figure 37 shows.

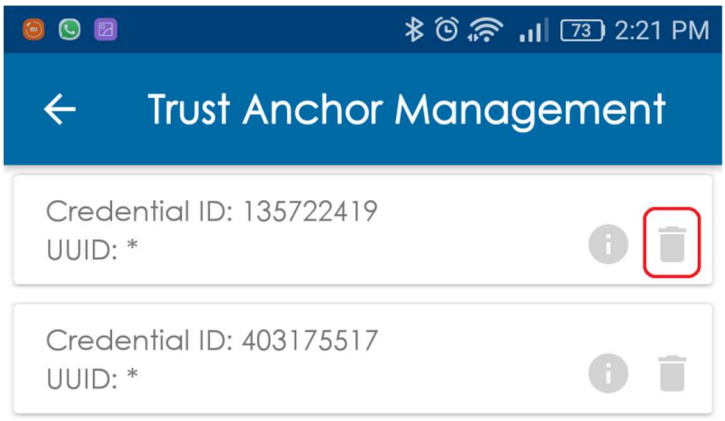

Figure 37: Remove a trust anchor certificate, Android.

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 38 shows.

Figure 38: Scan devices, Linux.

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

OTGC v2.x.x, based on IoTivity-Lite, can discover devices using different multicast IPv6 scopes. Clicking on “File” option and selecting “Settings” option, the OTGC will show settings about Discovery. As **¡Error! No se encuentra el origen de la referencia.** shows, the multicast IPv6 scope can be the followings:

- Link-Local scope
- Site-Local scope
- Realm-Local scope

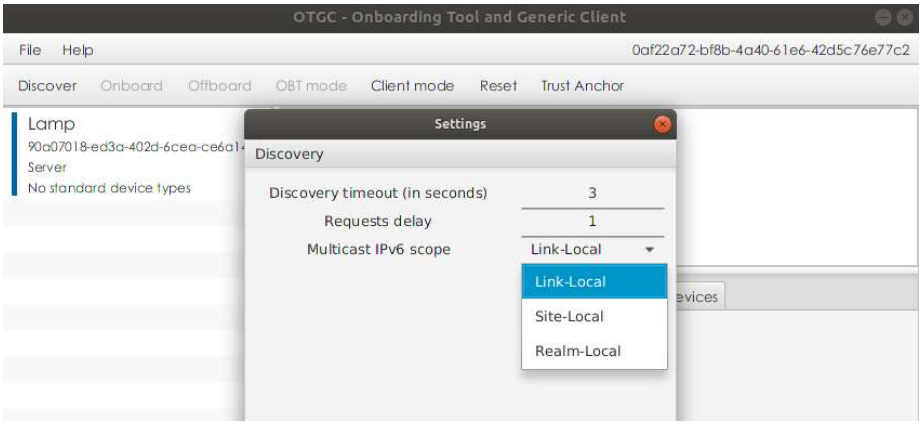

Figure 39: Multicast IPv6 scopes, Linux.

4.3.2 ONBOARD A DEVICE

OTGC can only onboard an unowned device in OBT mode. To onboard a device, select it from the devices list and click the “Onboard” button in the navigation bar, as Figure 40 shows.

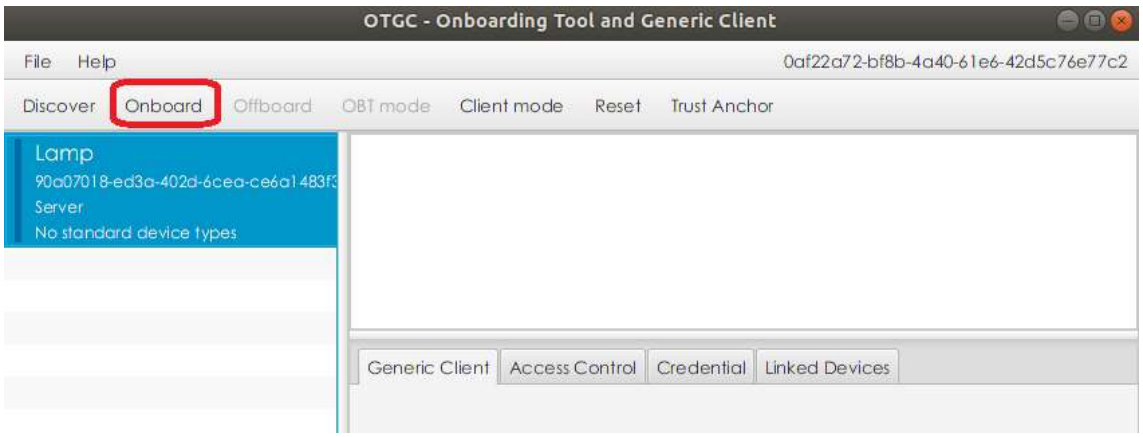

Figure 40: Onboard a device, Linux.

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.

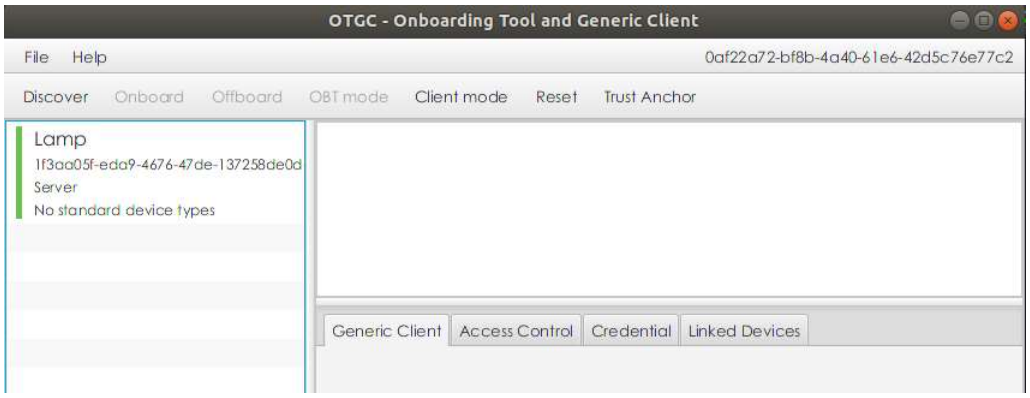

Figure 41: Devices list with an owned device, Linux.

OTGC v2.x.x, based on IoTivity-Lite can onboard multiple devices to the same time. To select multiple devices, keep pressed “Ctrl” and select all unowned devices which are going to be onboarded. If all selected devices are unowned (listed in blue color), the “Onboard” button will be enabled in the menu as Figure 42 shows and, by clicking on this button, the OTGC will onboard all selected devices. Otherwise, if the state of some of the devices is different to unowned (blue color), the “Onboard” button will be disabled as Figure 43 shows. OTGC will try first to onboard by PKI (user certificate). If this OTM is not supported by the device, OTGC will retry the onboarding by using Random PIN. If this OTM is also not supported by the device, Just Work OTM will be used.

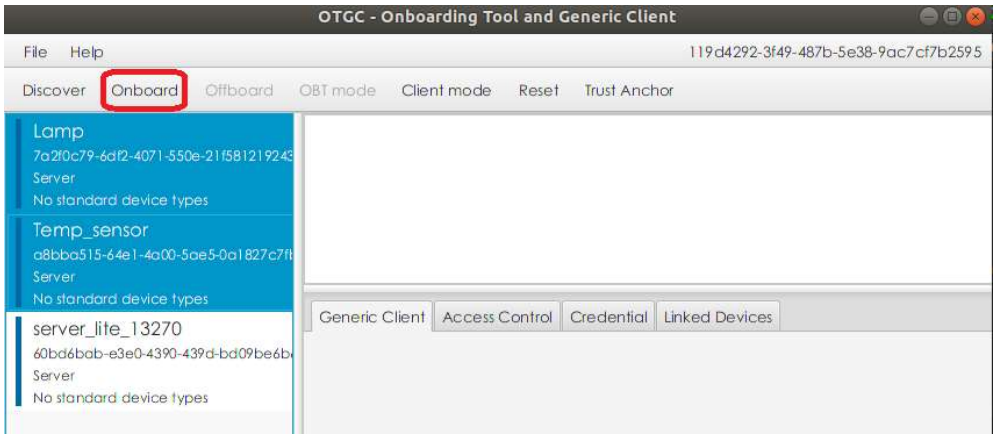

Figure 42: Onboard multiple unowned devices, Linux.

Figure 43: Onboard button is disabled with an owned device selected, 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 44.
- Device resources: see Figure 44.
- Access control list: see Figure 45.
- Credentials: see Figure 46.
- Link device: see Figure 47.

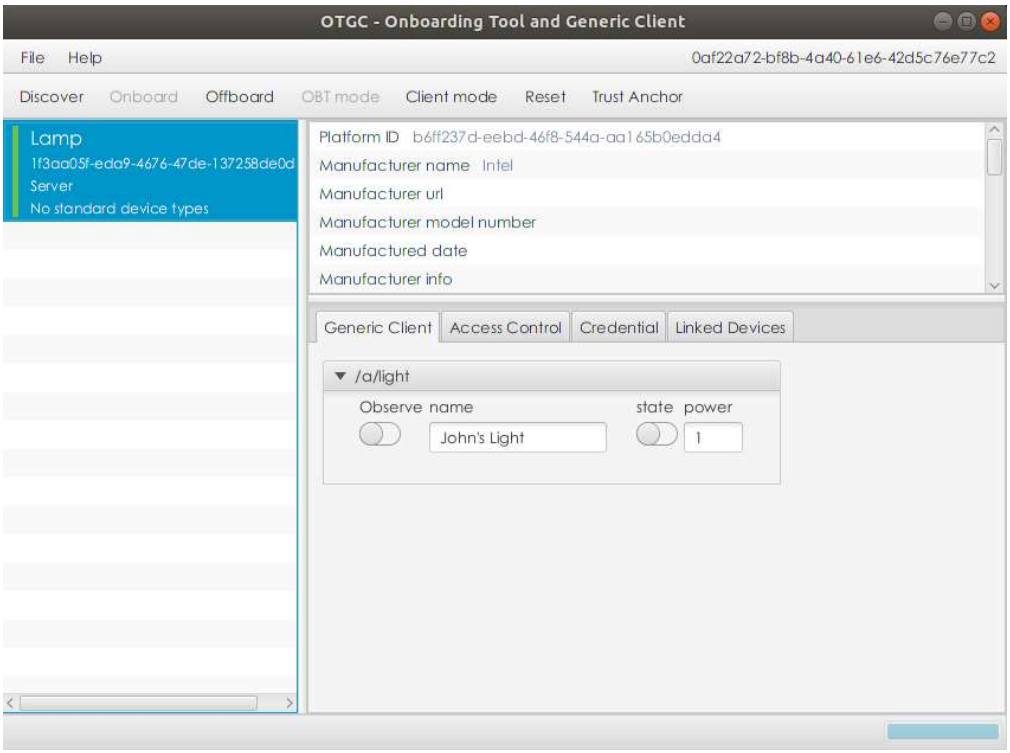

Figure 44: Device information and Generic Client, Linux.

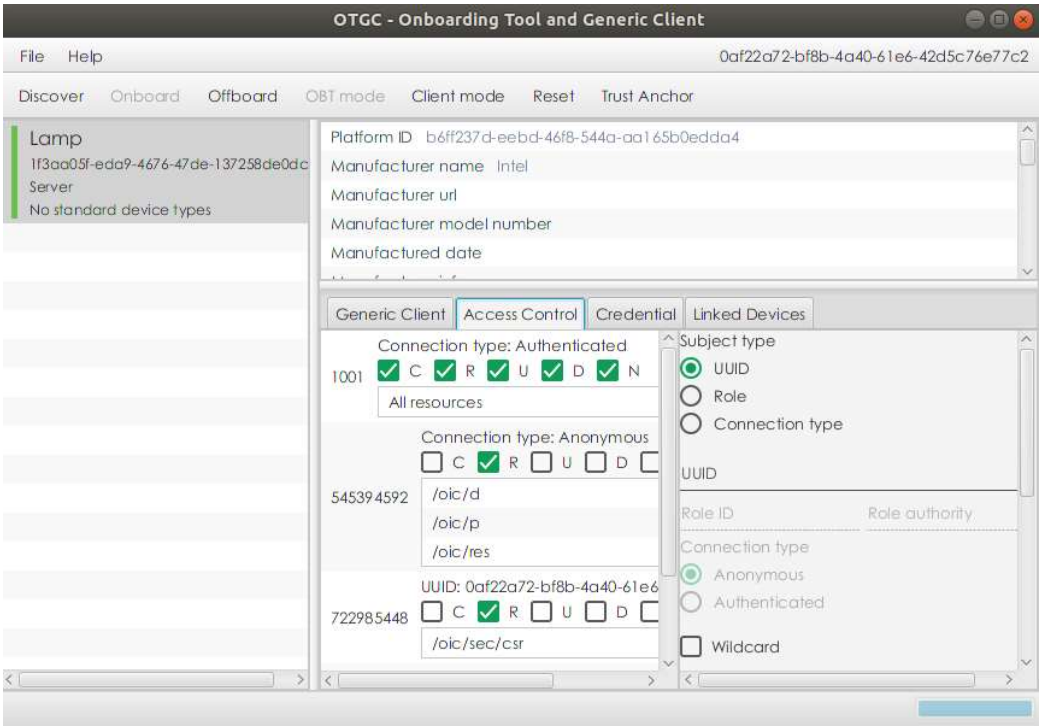

Figure 45: Access control, Linux.

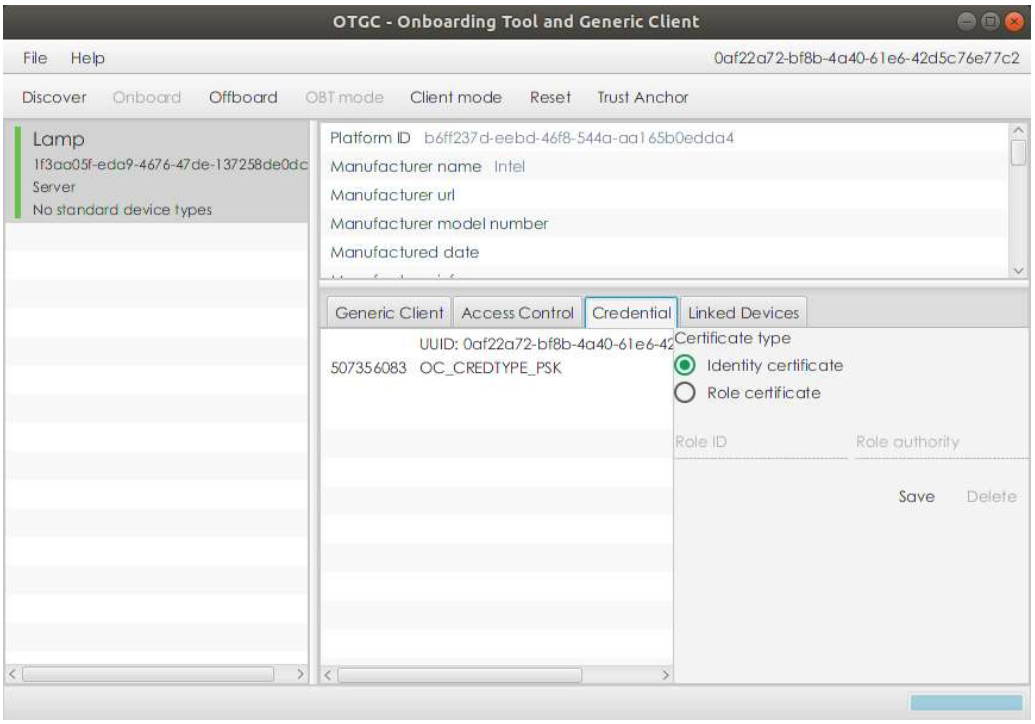

Figure 46: Credentials, Linux.

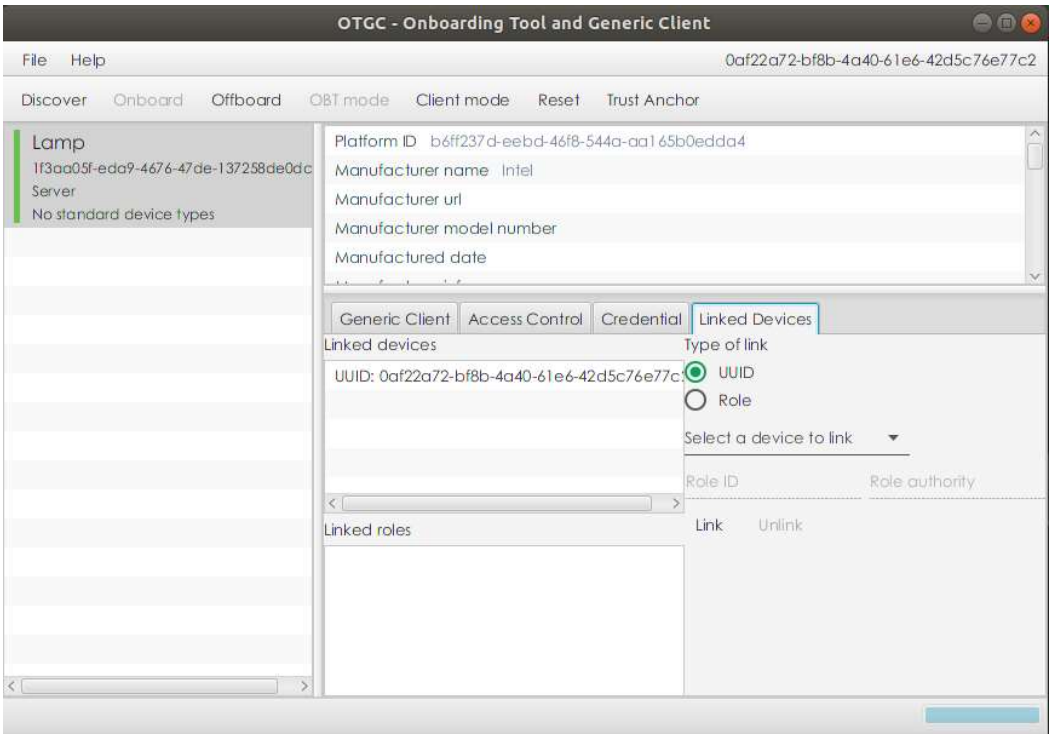

Figure 47: Link devices, Linux.

As Figure 45 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 46 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.

As Figure 47 shows, when “Linked Devices” tab is selected, the OTGC allows pairwise a client with a server or to link the selected device to a role by clicking on “Link” button. To delete a linked device or linked role, select it on the list and click on “Unlink” button. For more information about pairwise devices or link device to a role, go to section 4.2.7 or 4.2.8 of this document, respectively.

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 48 shows. After that, the device will change its state to unowned.

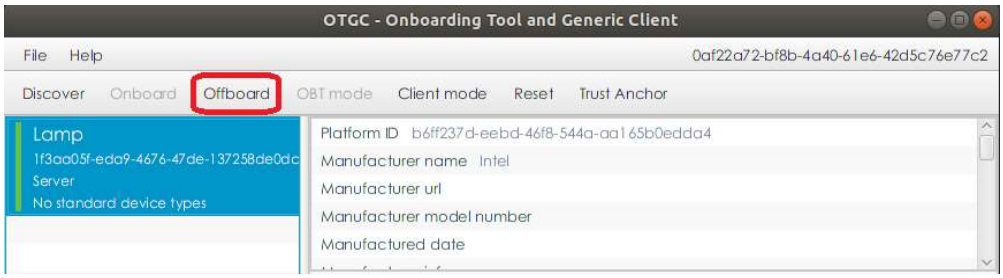

Figure 48: Offboard a device, Linux.

4.3.5 RESET OTGC

To reset the OTGC to its default values, it can be achieved by clicking on the “Reset” button in the options sited on toolbar (see Figure 49).

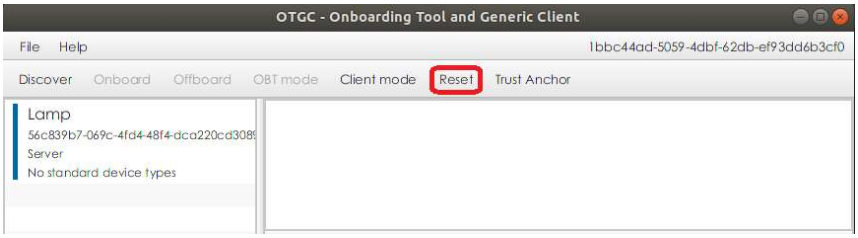

Figure 49: Reset OTGC, Linux.

4.3.6 OBT MODE

When the OTGC is in OBT mode, it is able to onboard/offboard devices and to provision ACEs and credentials to devices that they are owned by it.

The OBT mode is enabled by default when the OTGC application is installed. Also, it can be enabled by clicking in the “OBT mode” button on the toolbar when the OTGC is in Client mode as Figure 50 shows.

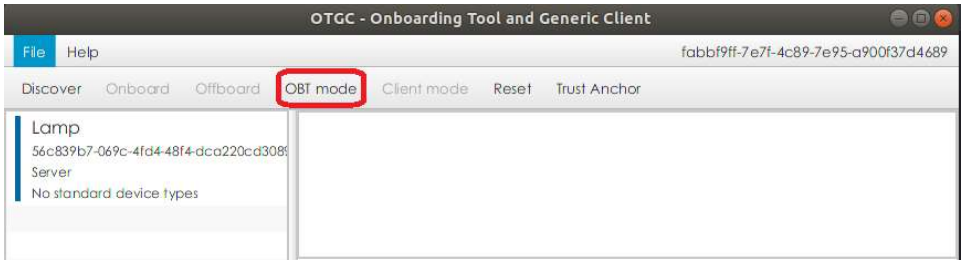

Figure 50: Change to OBT mode, Linux.

Before to change the mode, an advice message will be shown to confirm that all linked devices will be deleted as Figure 51 shows.

Figure 51: Advice message to change the mode, Linux.

4.3.7 CLIENT MODE

When the OTGC is in Client mode, it is not able to onboard/offboard devices, so if it tries to onboard a device while it is in Client mode, an error message appears as Figure 52 shows.

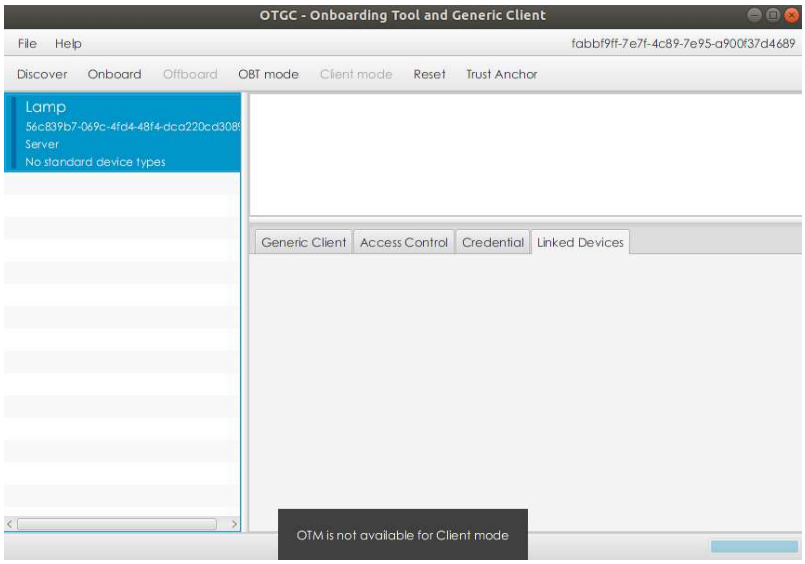

Figure 52: Error message in Client mode for OTM, Linux.

The Client mode can be enabled by clicking in the “Client mode” button on the toolbar when the OTGC is in OBT mode as Figure 53 shows.

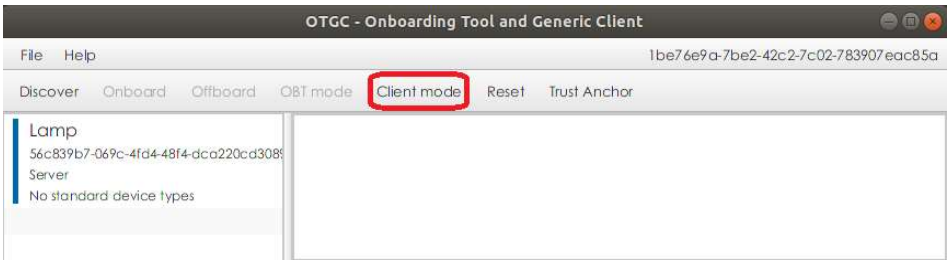

Figure 53: Change to Client mode, Linux.

As discussed in section 4.3.6, an advice message will be shown to confirm that all linked devices will be deleted.

4.3.8 TRUST ANCHOR MANAGEMENT

In OTGC v2.x.x, based on IoTivity-Lite, a trust anchor certificate can be added into the credentials or an existing trust anchor can be removed from the credentials through the “Trust Anchor” option.

Click on the “Trust Anchor” option as Figure 54 shows and the OTGC will show a list of existing trust anchor certificates, as Figure 55 shows.

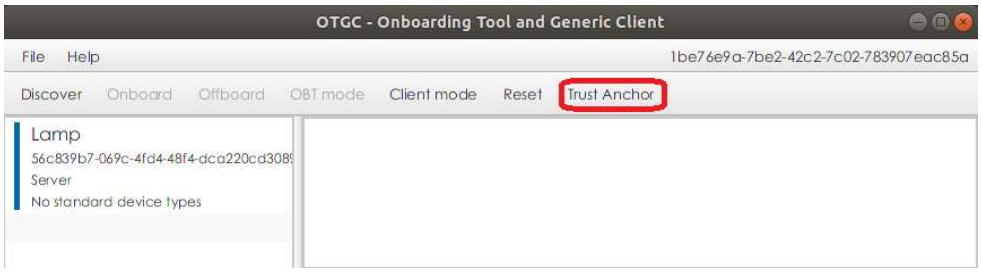

Figure 54: Trust Anchor Management, Linux.

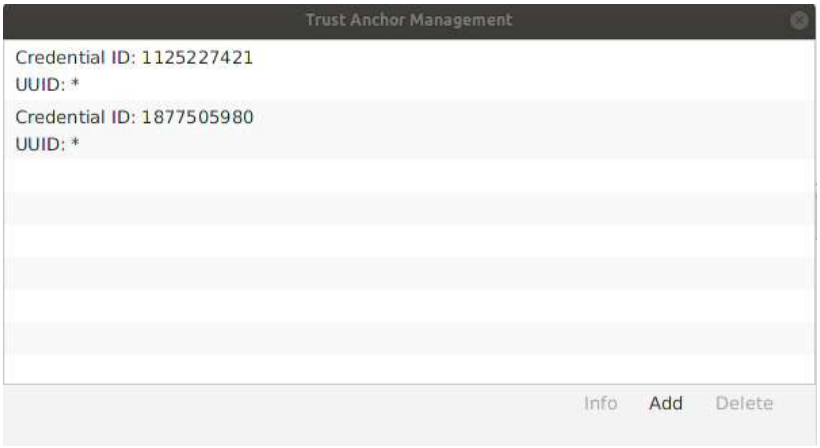

Figure 55: Trust anchor certificate list, Linux.

To add a new one, click on the “Add” button and select a root certificate in PEM format from the device storage, as Figure 56 and Figure 57 show.

Figure 56: Add new trust anchor certificate, Linux.

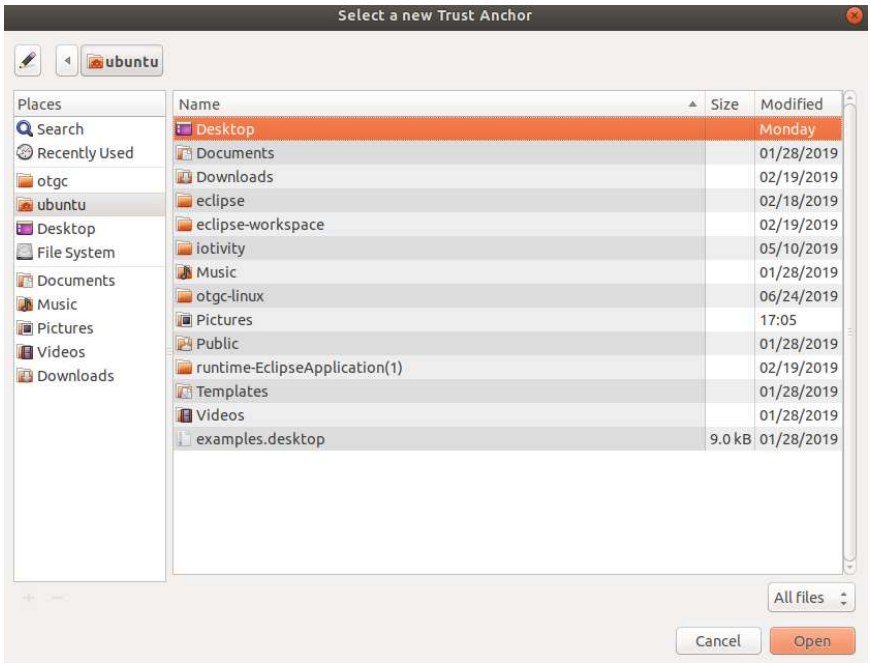

Figure 57: Device storage to select a root certificate, Linux.

To see the information of the root certificate, select a certificate and click on the information button, as Figure 58 shows, and the information of the certificate will show, as Figure 59 shows.

Figure 58: Show information of a trust anchor certificate, Linux.

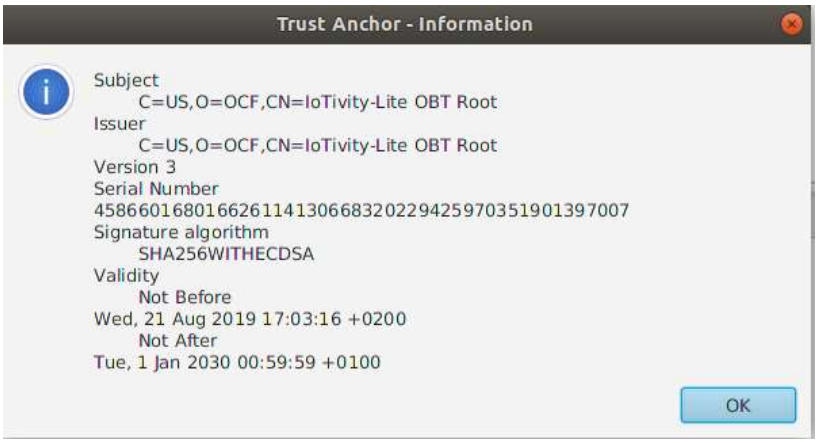

Figure 59: Information of a trust anchor certificate, Linux.

To remove a certificate, select a certificate and click on the trash button, as Figure 60 shows.

Figure 60: Remove a trust anchor certificate, Linux.

4.4 UWP

This OTGC version is not available for OTGC v2.x.x, based on IoTivity-Lite.

4.4.1 SCANNING DEVICES

When the OTGC starts, it automatically scans all visible OCF devices. To scan devices at any time, the “Scan” button in the command bar can be pressed to refresh the device list, as Figure 61 shows:

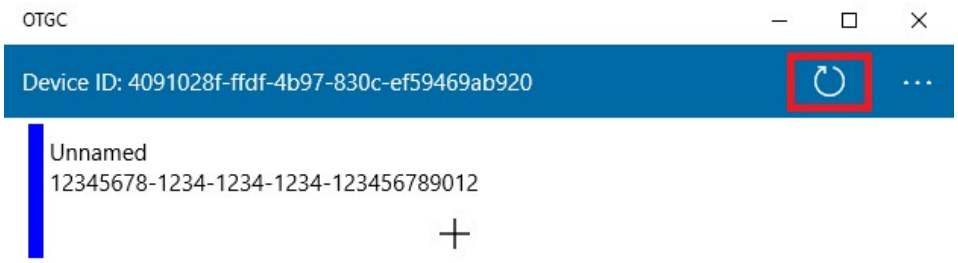

Figure 61: Scan devices, Windows 10.

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

4.4.2 ONBOARD A DEVICE

OTGC can only onboard an unowned device. To onboard a device, press on the plus icon that appears under the device identifier, as shown in Figure 62.

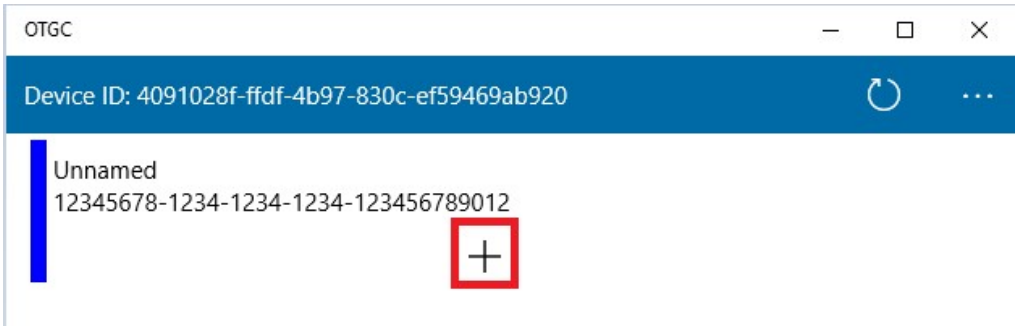

Figure 62: Onboard a device, Windows 10.

When a device is successfully onboarded, its state changes to owned-by-self (green) as shown in Figure 63.

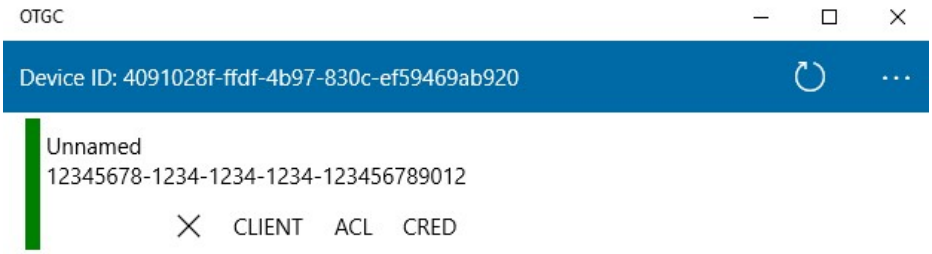

Figure 63: Owned-by-self device, Windows 10.

4.4.3 MANAGE A DEVICE

When the OTGC acts as GC, it can manage OCF devices that are owned by it. If the OCF device is owned by other OCF Client an access control policy has to be provisioned to it in order to allow to the OTGC to manage its resources.

To access to the GC, press on the “Client” button as Figure 64 shows and, depending on the window size, all resources that the OCF Server implements will appear in a new screen or will appear in the Client tab to the right of the device list as shown in Figure 65 and Figure 66.

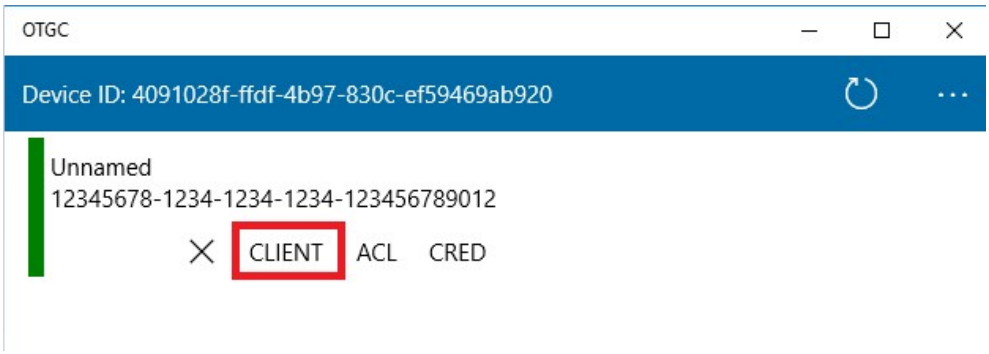

Figure 64: Generic Client button, Windows 10.

Figure 65: Generic Client tab, Windows 10.

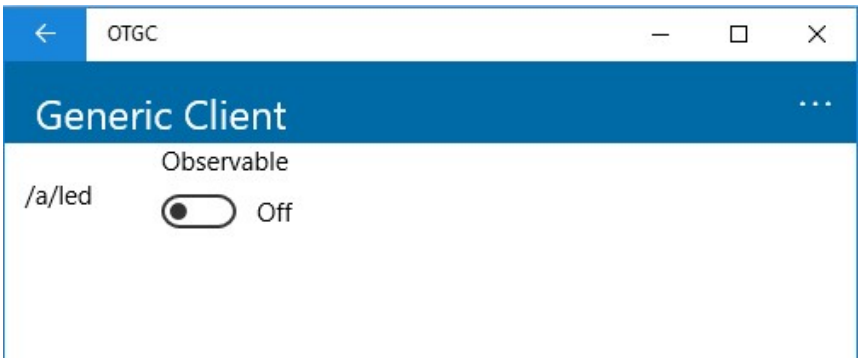

Figure 66: Generic Client screen, Windows 10.

4.4.4 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 “Cred” button as Figure 67 shows, the OTGC shows the currently installed credentials, depending on the window size, in a new screen as shown in Figure 69 or in the “Credentials” tab at right of the device list as shown in Figure 68. A credential can be deleted pressing on the trash icon.

Figure 67: Credential button, Windows 10.

Figure 68: Credentials tab, Windows 10.

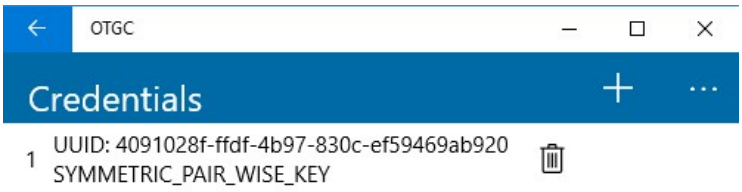

Figure 69: Credentials screen, Windows 10.

To provision some of the credentials listed in the section 4.2.5 for the owned device, at right of the credential list, select the type of the credential to provision and click on the “Add” button at bottom, as shown in Figure 68. In case to be in the credential screen, a pop-up where a new credential can be provisioned appears after pressing the plus icon, as shown in Figure 70.

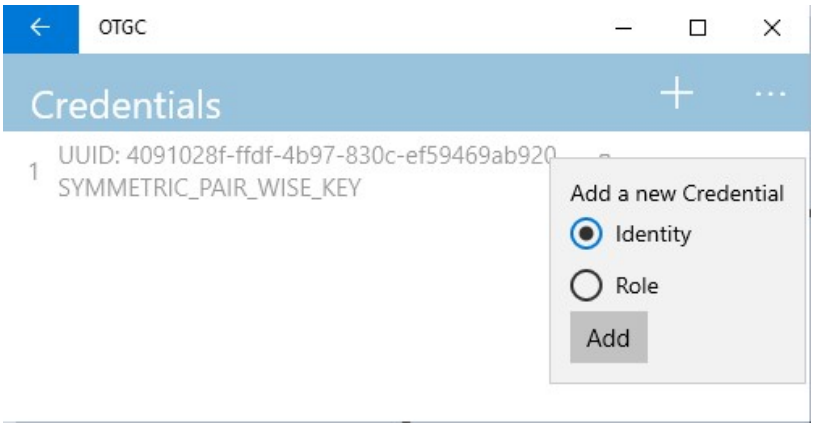

Figure 70: Add a new credential in Credentials screen, Windows 10.

4.4.5 ACCESS CONTROL LIST

When the OTGC acts as AMS, it is able to retrieve the installed 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 “ACL” button as Figure 71 shows, the OTGC will show the currently installed access control policies, depending on the window size, in a new screen (Figure 69) or in the “Access Control” tab at right of the device list (Figure 72). An access control policy can be deleted, pressing on the trash icon.

Figure 71: Access control list button, Windows 10.

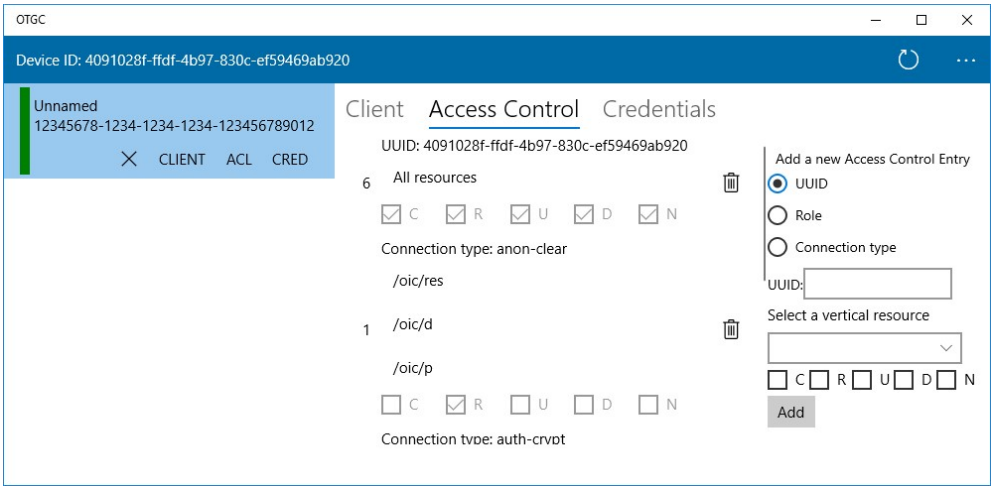

Figure 72: Access control tab, Windows 10.

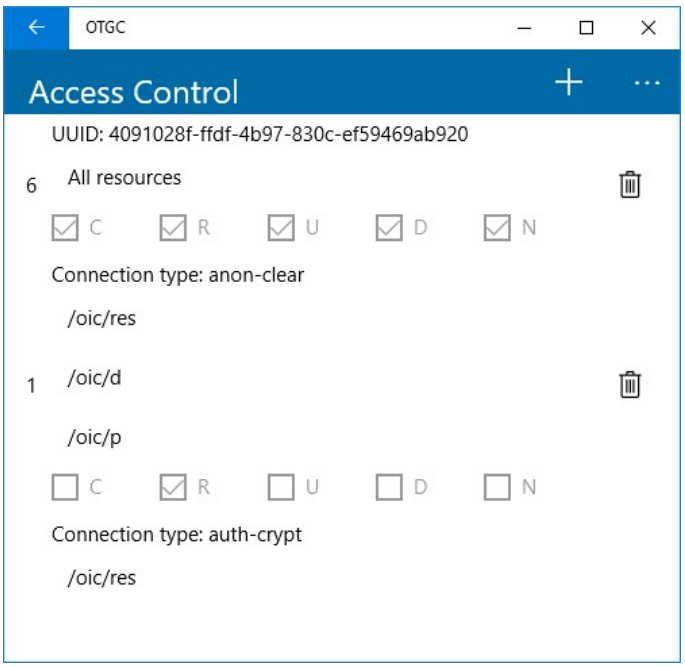

Figure 73: Access control screen, Windows 10.

To provision some of the access control policy listed in the section 4.2.6 for the owned device, at right of the credential list, select the type of the access control to provision and clicking in the “Add” button at bottom (Figure 72). In case to be in the access control screen, press the plus icon in the command bar and a pop-up will appear where a new access control policy can be provisioned (Figure 74).

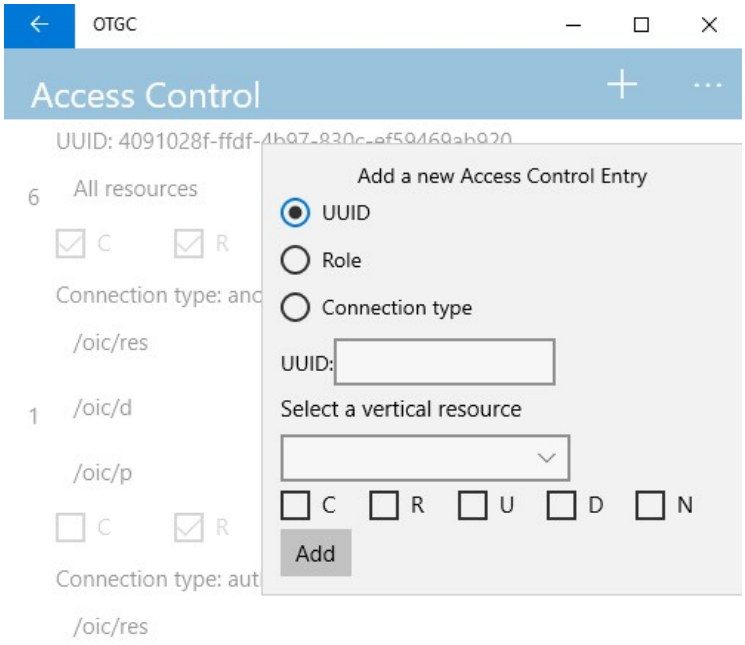

Figure 74: Add a new access control policy in Access Control screen, Windows 10.

4.4.6 LINK DEVICES

The OTGC can pairwise a client and a server or add a device to a specific role to allow the client device to manage the server. To do that, click on the “Link” button, as shows Figure 75:

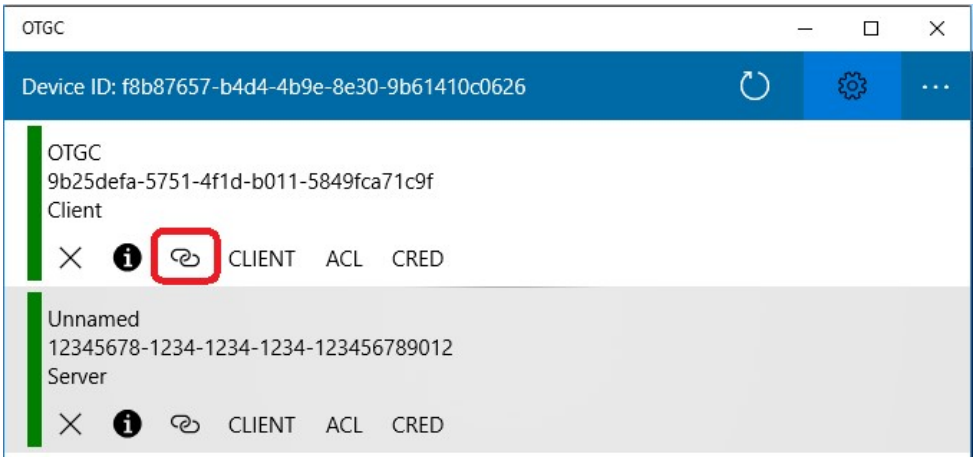

Figure 75: Link devices button, Windows 10.

Once the “Link” button is clicked, the OTGC will show the current pairwise devices and the current linked roles, depending on the window size, in a new screen (Figure 77) or in the “Linked Devices” tab at right of the device list (Figure 76). A pairwise device or linked role can be deleted, by clicking on the trash icon.

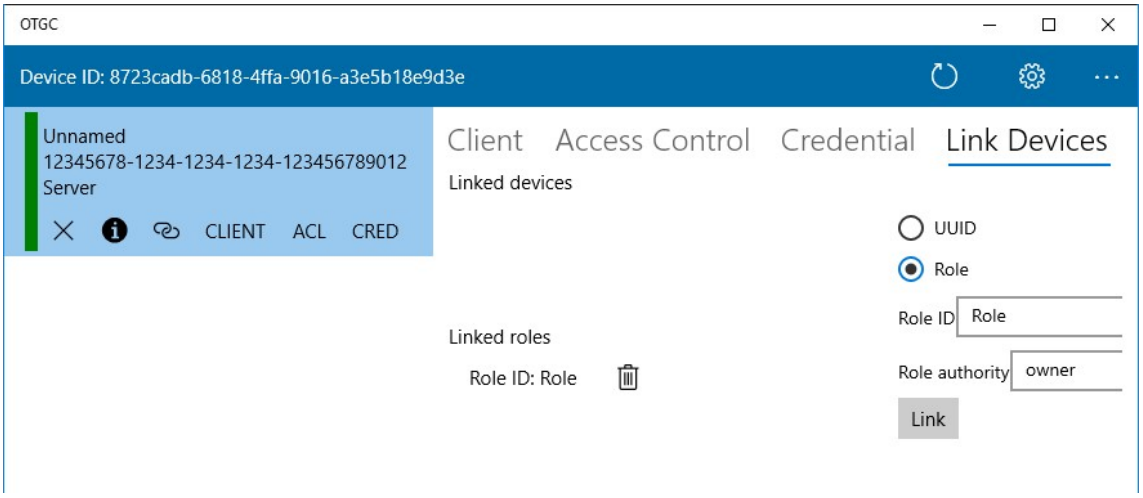

Figure 76: Link devices tab, Windows 10.

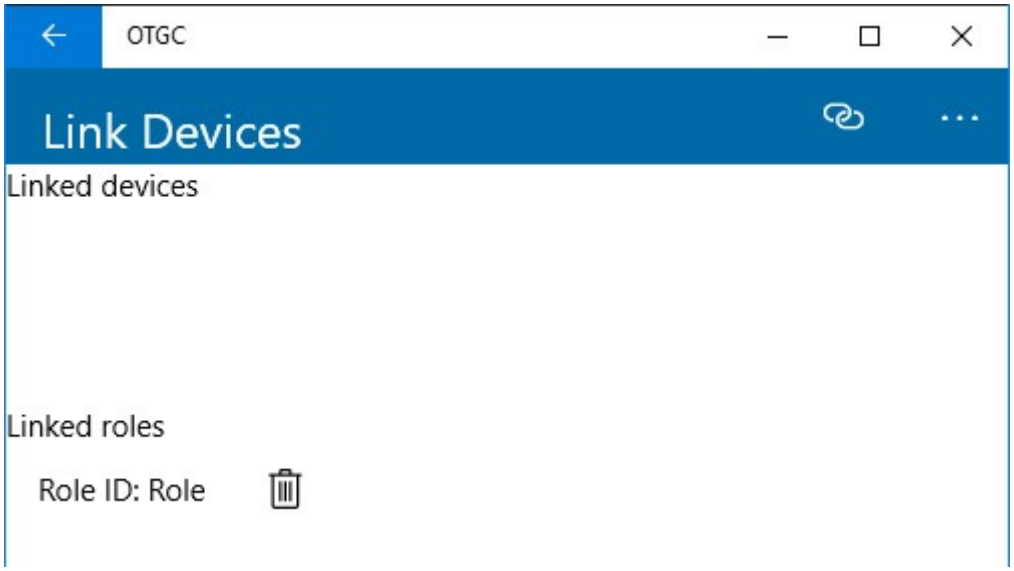

Figure 77: Link devices screen, Windows 10.

To link with a new device or to link to a new role, at right of the linked device list, select the device to link or fill the information of the role to link and click on the “Link” button at bottom (Figure 76). In case to be in the linked device screen, click on the link icon in the command bar and a pop-up will appear, where a new device or role can be linked to (Figure 78).

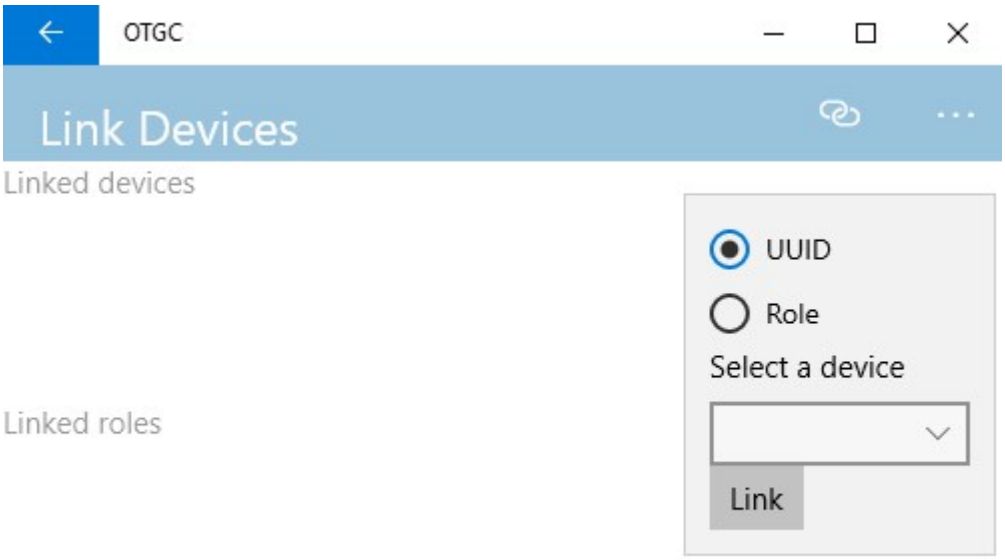

Figure 78: Link to a new device or to a new role, Windows 10.

4.4.7 OFFBOARD A DEVICE

An OCF device owned by the OTGC can be unowned by clicking on the “Cancel” icon, as shown in Figure 79. If the action succeeds, the device changes its state to unowned.

Figure 79: Offboard a device, Windows 10.

4.4.8 RESET OTGC

To reset the OTGC to its default values, it has to return to RFOTM state by clicking on “RFOTM” button in the secondary options (three dots) of the command bar as shown in Figure 80.

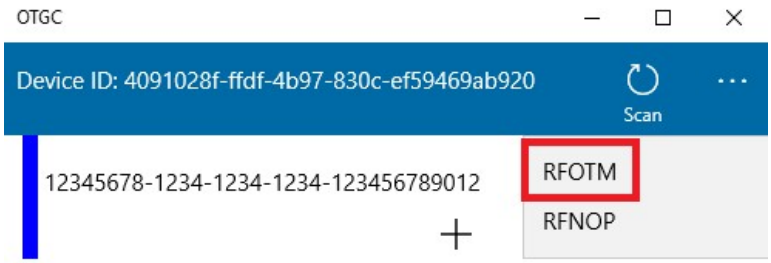

Figure 80: Reset OTGC, Windows 10.

4.4.9 OWNED OTGC BY SELF

To self-own the OTGC, click on the “RFNOP” button on the secondary options of the command bar as Figure 81 shows.

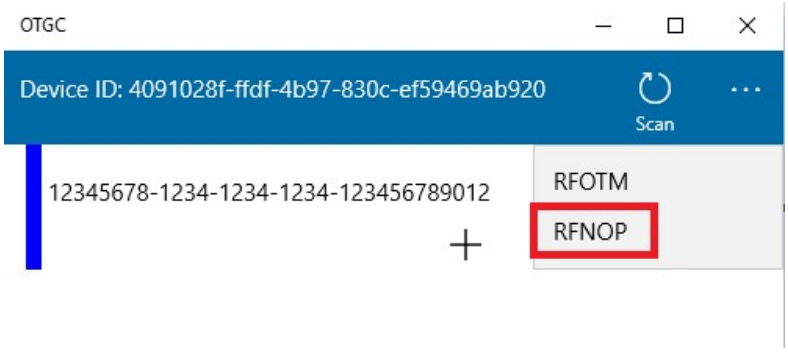

Figure 81: Self-own OTGC, Windows 10.

4.5 IOS

This OTGC version is not available for OTGC v2.x.x, based on IoTivity-Lite.

4.5.1 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 top.
2. Slide the finger from top to bottom.

Figure 82: Empty devices list screen, iOS.

When scan finishes, OTGC will show a list with OCF devices similar to the Figure 83.

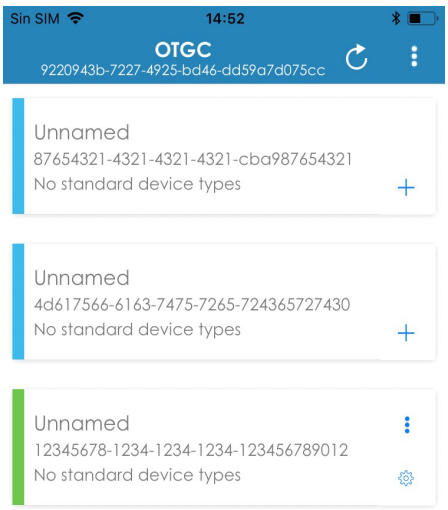

Figure 83: List with OCF devices detected, iOS.

4.5.2 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 84.

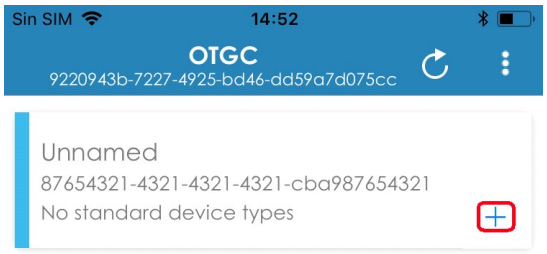

Figure 84: Onboard button, iOS.

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.

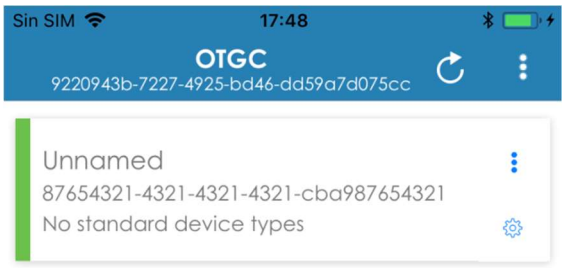

Figure 85: Owned-by-self device, iOS.

4.5.3 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.

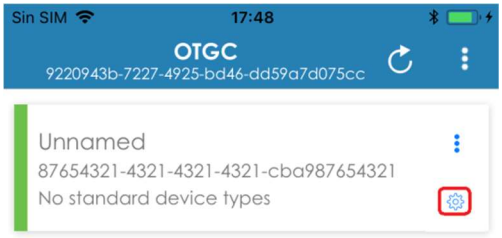

Figure 86: Generic Client button, iOS.

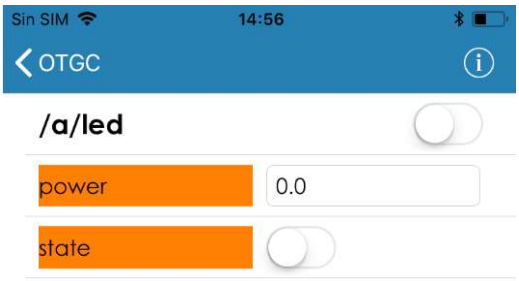

Figure 87: Resources in an OCF Server, iOS.

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.

Figure 88: Device information panel, iOS.

4.5.4 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 89, the OTGC lists the currently installed credentials. A credential can be deleted by clicking the trash icon.

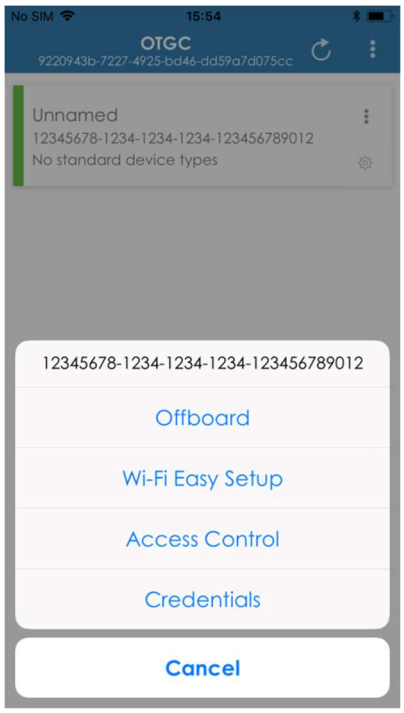

Figure 89: Credentials option, iOS.

Figure 90: Currently installed credentials list, iOS.

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

- Identity certificates.
- Role certificates.

To provision a credential, click on the plus button in the Figure 90 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 91 shows.

Figure 91: Provision a new credential, iOS.

4.5.5 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 93.

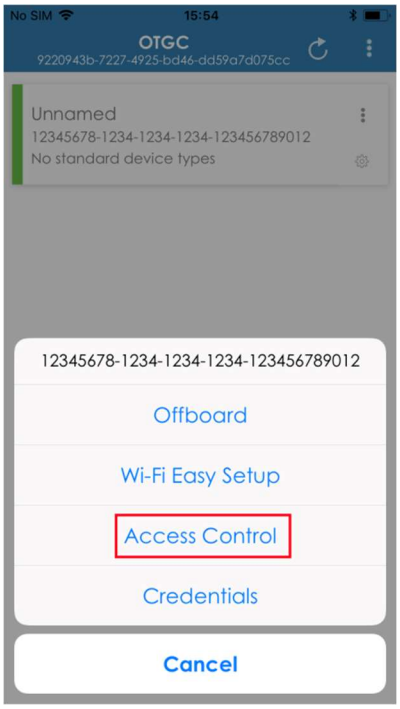

Figure 92: Access Control option, iOS.

Figure 93: Access control list, iOS.

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 top-right plus button of Figure 93 and a new screen appears with a form to fill (Figure 94). 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.

Figure 94: Provision a new access control policy, iOS.

4.5.6 OFFBOARD A DEVICE

An OCF device owned by the OTGC can be unowned by clicking on the “Offboard” option, as shows Figure 95. If the action succeeds, the device changes its state to unowned.

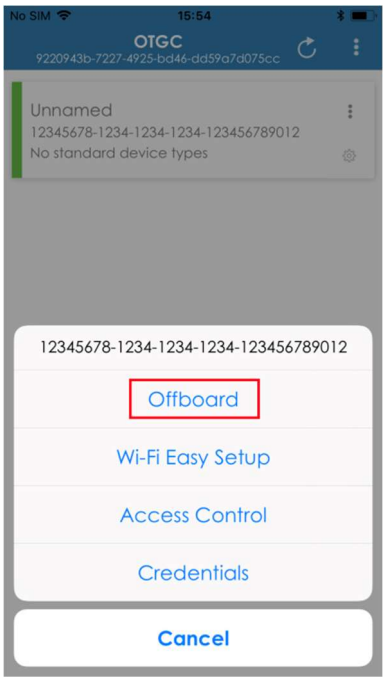

Figure 95: Offboard an owned device, iOS.

4.5.7 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 96).
4. Connect to the new network manually on your iPhone.
5. Introduce the configuration of the network the new connected (see Figure 97).
6. Scan the network to verify that the device has connected properly.

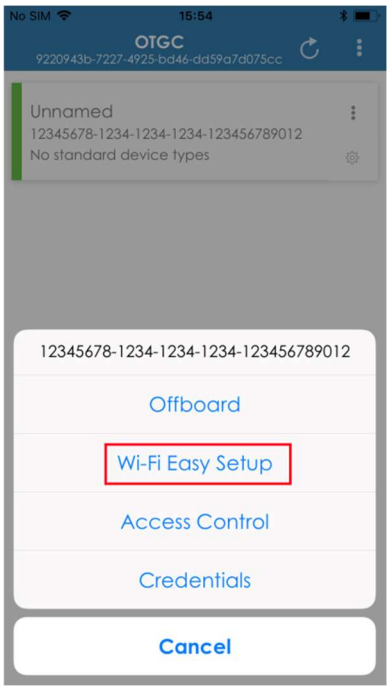

Figure 96: “Wi-Fi Easy Setup” option, iOS.

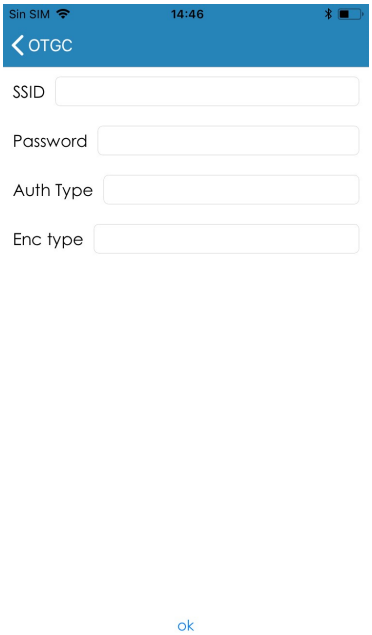

Figure 97: Input Wi-Fi credentials dialog, iOS.

4.5.8 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 98 shows.

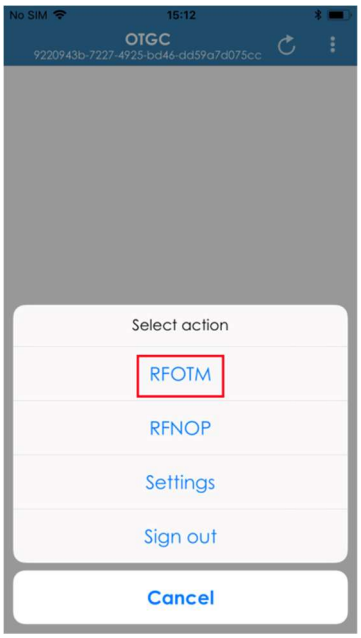

Figure 98: Reset OTGC, iOS.

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

4.5.9 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 99 shows.

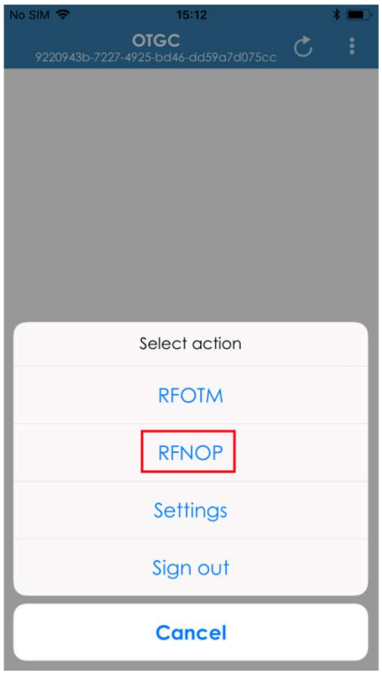

Figure 99: Self-own the OTGC, iOS.

5 ANNEX 1: RUNNING CTT TEST CASES

5.1 OBT TEST CASES

5.1.1 PRE-EXECUTION OBT TEST CASES

1. Download the EonTi and Kyrio chains from the following URL:
    a. Kyrio URL: https://testcerts.kyrio.com/#/
    b. EonTi URL: https://www.eonti.com/ocftestcerts
2. Copy the Eonti and Kyrio positive chains into:

<CTT installation folder>/Configuration/OCF/Certificates/Positive

3. Copy the Eonti and Kyrio negative chains into:

<CTT installation folder>/Configuration/OCF/Certificates/Negative

5.1.2 CT3.1.1 OBT: JUST-WORKS OTM

The goal of this test case is to verify that the OTGC is able to successfully onboard an OCF Server using Just-Works OTM.

1. Execute the test case in the CTT.
2. The test case requests to discover the CTT server and to onboard it with the OTGC, as Figure 100 shows.

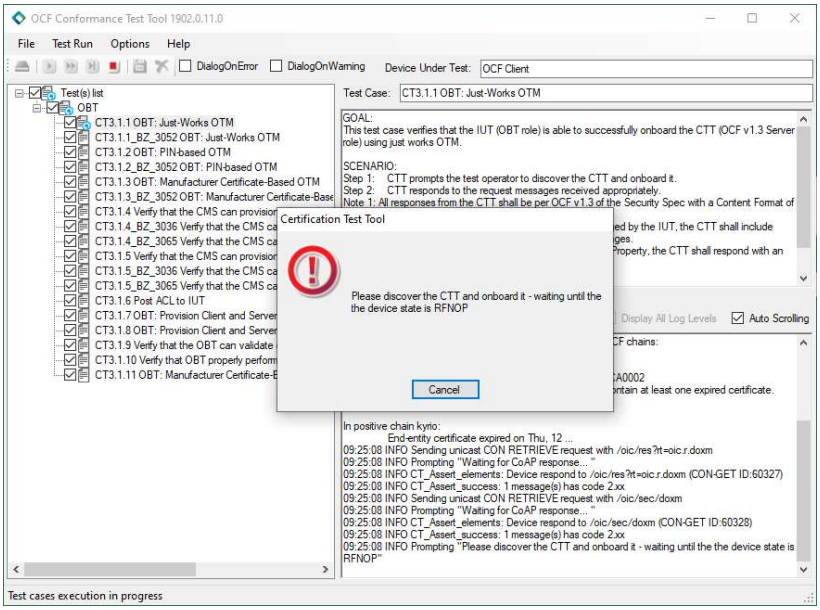

Figure 100: Discover and onboard CTT, CT3.1.1

3. Discover the devices on the OTGC clicking on the “Refresh” button at right-bottom as Figure 101 shows.

Figure 101: Scan devices on the OTGC, CT3.1.1

4. Click on the plus icon to onboard the CTT server, as Figure 102 shows.

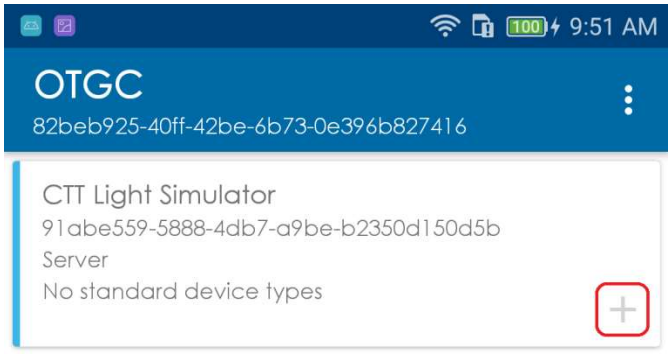

Figure 102: Onboard the CTT server, CT3.1.1

5. When the onboard process has been completed, the test case will request to confirm that the OTGC is assuming ownership of the CTT, as Figure 103 shows. Click on the “Yes” button if the CTT server appears on the OTGC as a green device (owned by the OTGC), as Figure 104 shows. Otherwise, click on the “No” button.

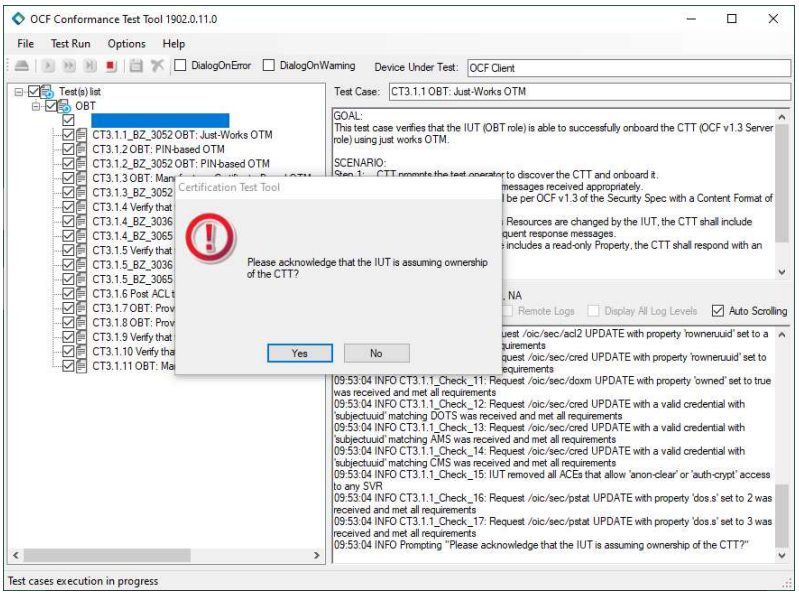

Figure 103: Confirm ownership of the CTT, CT3.1.1

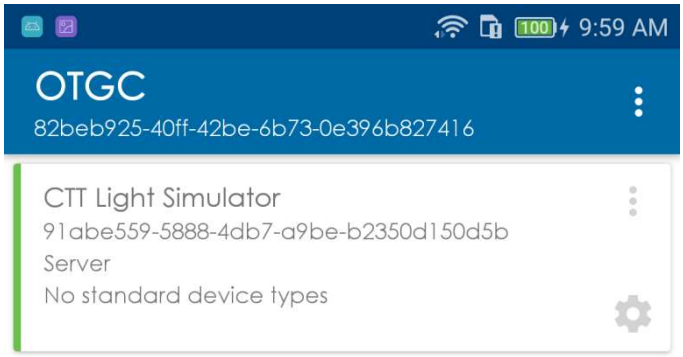

Figure 104: Owned device on the OTGC, CT3.1.1

5.1.3 CT3.1.2 OBT: PIN-BASED OTM

The goal of this test case is to verify that the OTGC is able to successfully onboard an OCF Server using PIN-based OTM.

1. Execute the test case in the CTT.
2. The test case requests to discover the CTT server and to onboard it with the OTGC using PIN XXXXXX, as Figure 105 shows.

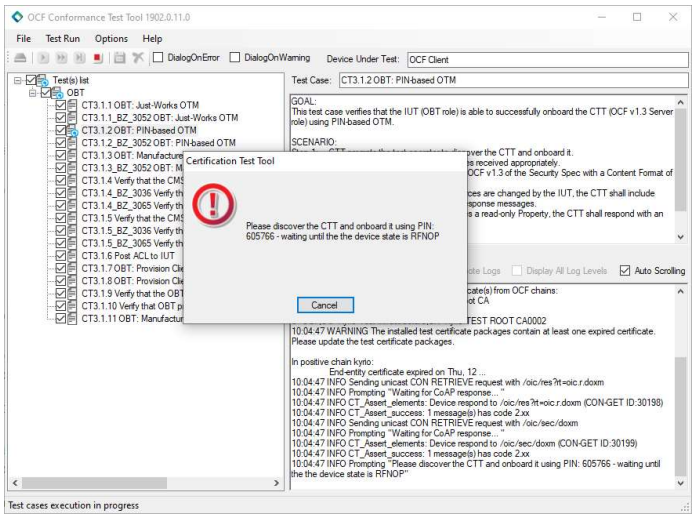

Figure 105: Discover and onboard CTT, CT3.1.2

3. Discover the devices on the OTGC clicking on the “Refresh” button at right-bottom as Figure 106 shows.

Figure 106: Scan devices on the OTGC, CT3.1.2

4. Click on the plus icon to onboard the CTT server, as Figure 107 shows.

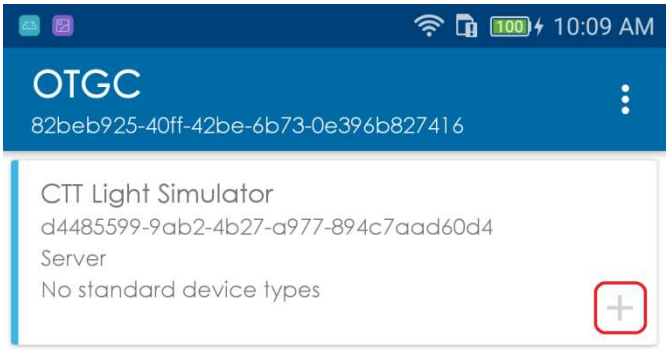

Figure 107: Onboard the CTT server, CT3.1.2

5. The onboard process will request to insert the PIN that it displayed in the step 2, as Figure 108 shows.

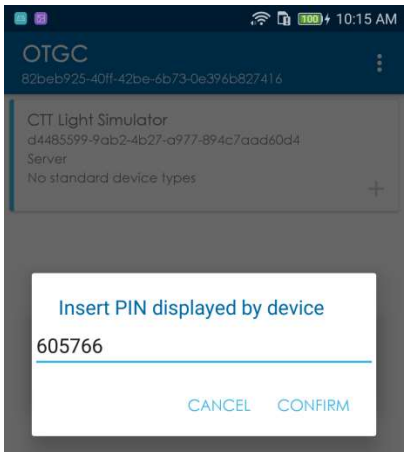

Figure 108: Insert PIN on the OTGC, CT3.1.2

6. When the onboard process has been completed, the test case will request to confirm that the OTGC is assuming ownership of the CTT, as Figure 109 shows. Click on the “Yes” button if the CTT server appears on the OTGC as a green device (owned by the OTGC), as Figure 110 shows. Otherwise, click on the “No” button.

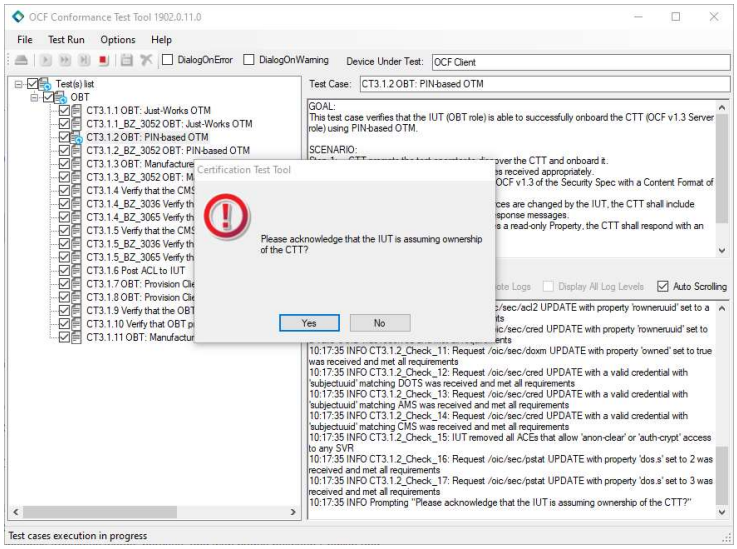

Figure 109: Confirm ownership of the CTT, CT3.1.2

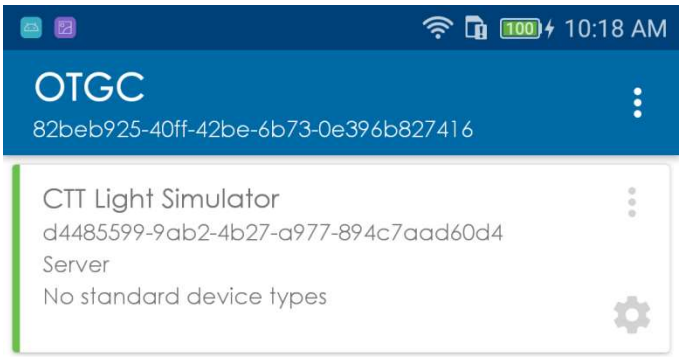

Figure 110: Owned device on the OTGC, CT3.1.2

5.1.4 CT3.1.3 OBT: MANUFACTURER CERTIFICATE-BASED OTM

The goal of this test case is to verify that the OTGC is able to successfully onboard the CTT server using manufacturer certificate-based OTM.

1. Execute the test case in the CTT.
2. The test case requests to discover the CTT server and to onboard it with the OTGC, as Figure 111 shows.

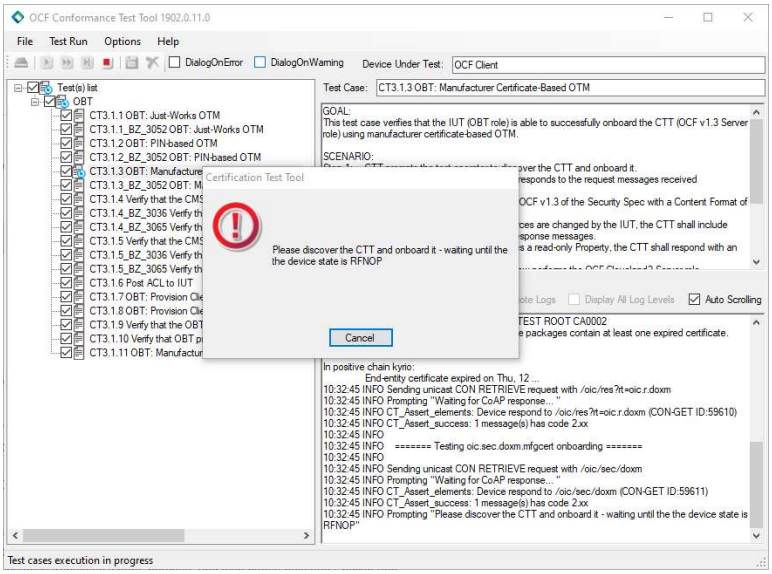

Figure 111: Discover and onboard CTT, CT3.1.3

3. Discover the devices on the OTGC clicking on the “Refresh” button at right-bottom as Figure 112 shows.

Figure 112: Scan devices on the OTGC, CT3.1.3

4. Store the Eonti Root CA and Kyrio Root CA on the OTGC (these 2 Root CAs are pre-installed in OTGC v2.x.x so this step is not really needed).
    a. Click on the three dots on the toolbar at right-top and select “Trust Anchor Management” option.

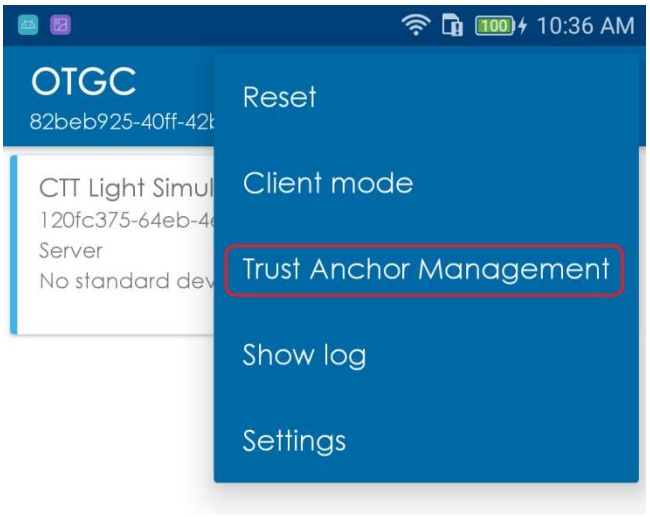

Figure 113: Trust Anchor Management, CT3.1.3

b. Click on the plus button to store a new root CA.

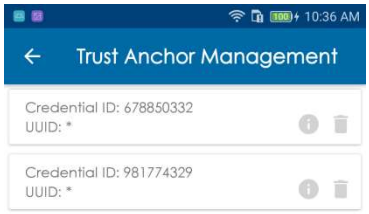

Figure 114: Add new trust anchor, CT3.1.3

c. Select the root CA to store.

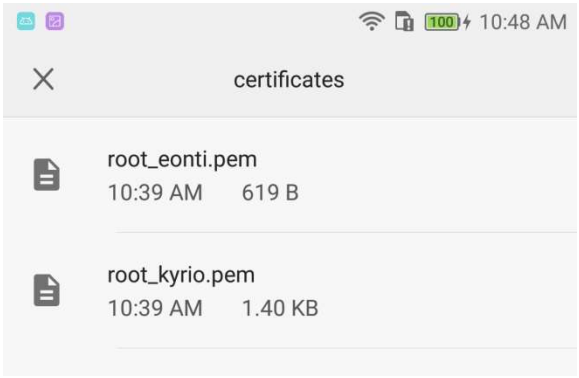

Figure 115: Select root CA to store, CT3.1.3

5. Click on the plus icon to onboard the CTT server, as Figure 116 shows.

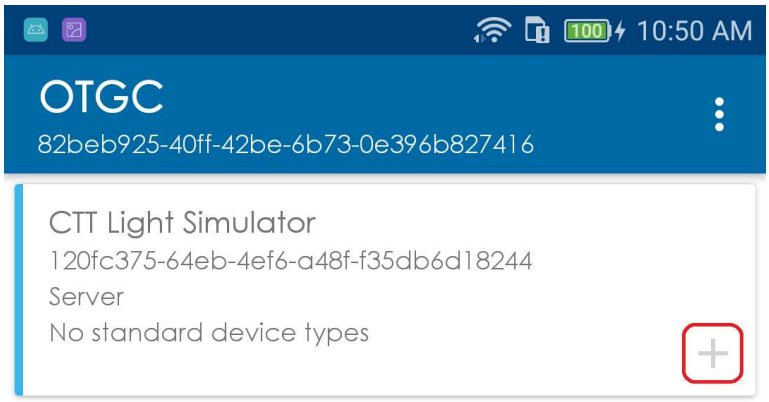

Figure 116: Onboard the CTT server, CT3.1.3

6. When the onboard process has been completed, the test case will request to confirm that the OTGC is assuming ownership of the CTT, as Figure 117 shows. Click on the “Yes” button if the CTT server appears on the OTGC as a green device (owned by the OTGC), as Figure 118 shows. Otherwise, click on the “No” button.

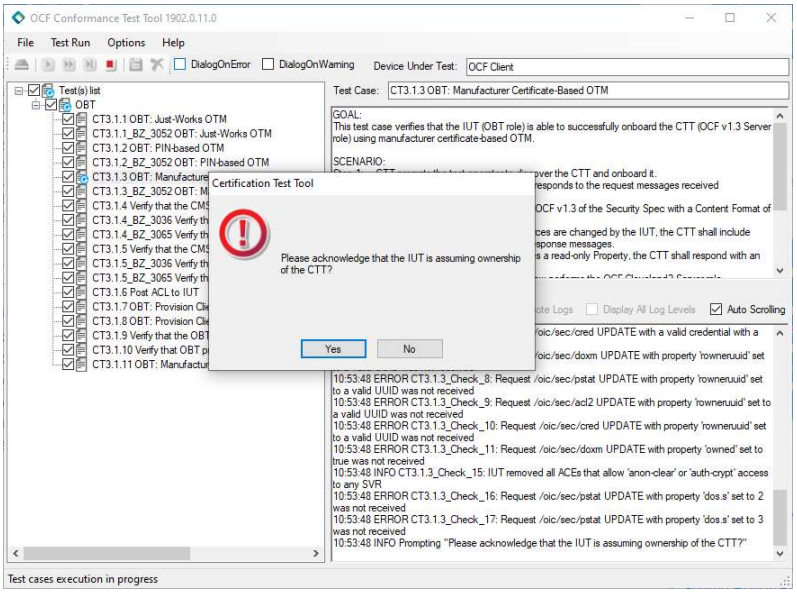

Figure 117: Confirm ownership of the CTT, CT3.1.3

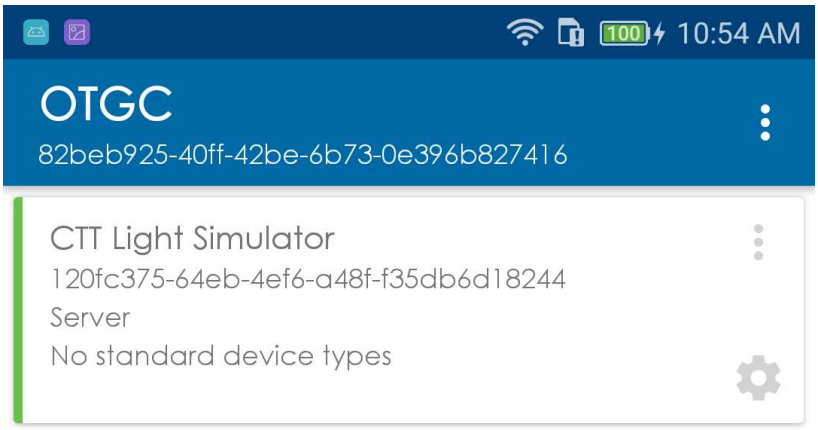

Figure 118: Owned device on the OTGC, CT3.1.3

7. Discover the devices again as in the step 4.
8. Onboard the CTT server, as in the step 6, that it has a self-signed root certificate.
9. The ownership transfer will fail.

5.1.5 CT3.1.4 CMS CAN PROVISION ROLE CREDENTIALS

The goal of this test case is to verify that the OTGC can provision a role credential to the simulated CTT client.

1. Execute the test case in the CTT.
2. The test case requests to discover the CTT client and to onboard it using any supported OTM, as Figure 119 shows.

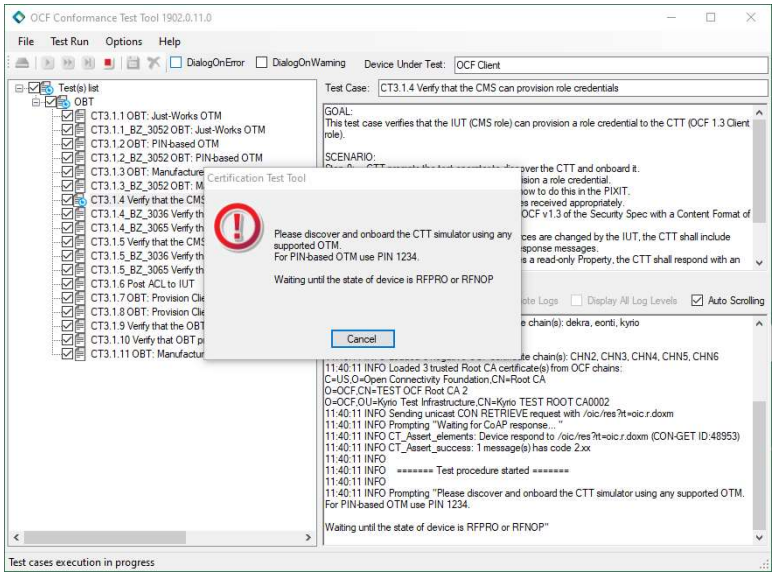

Figure 119: Discover and onboard a CTT client, CT3.1.4

3. Discover the devices on the OTGC clicking on the “Refresh” button at right-bottom as Figure 120 shows.

Figure 120: Scan devices on the OTGC, CT3.1.4

4. Click on the plus icon to onboard the CTT server, as Figure 121 shows.

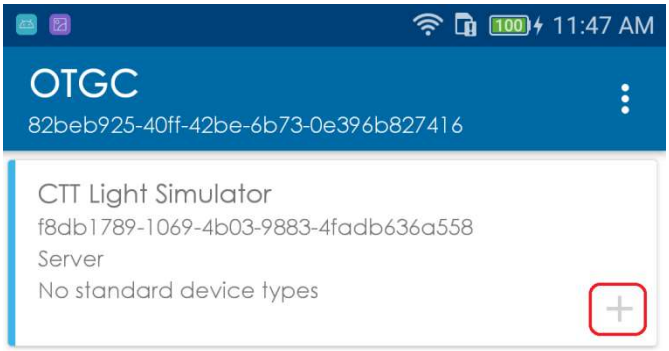

Figure 121: Onboard the CTT client, CT3.1.4

5. Select the method to do the ownership transfer.
6. When the onboard process has been completed, the test case will request to provision a role credential, as Figure 122 shows.

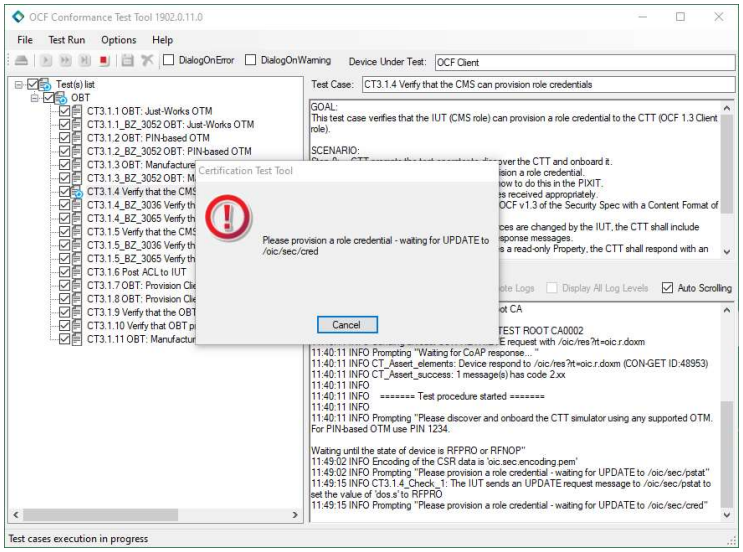

Figure 122: CTT request to provision a role credential, CT3.1.4

7. Click on the three dots of the owned device and click on the “Credentials” button, as Figure 123 shows.

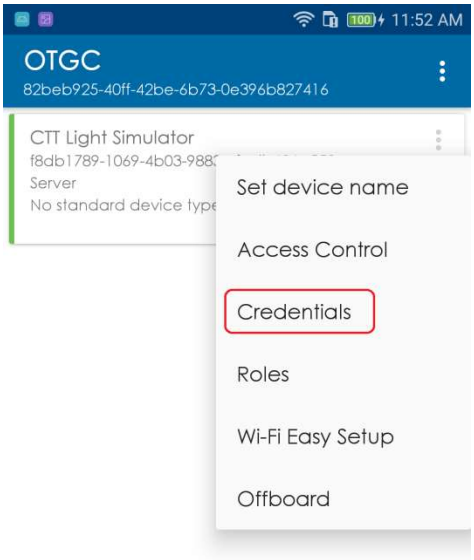

Figure 123: Select credentials on the owned device, CT3.1.4

8. Click on the plus button to store a new credential, as Figure 124 shows.

Figure 124: Add a new credential, CT3.1.4

9. Select “Identity” and click on the “Save” button, as Figure 125 shows.

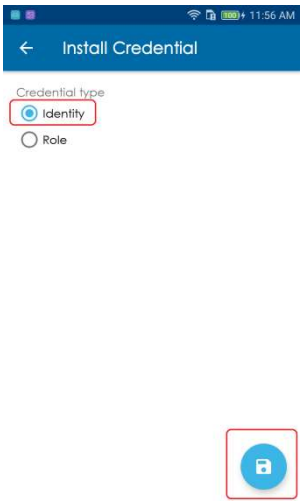

Figure 125: OTGC provisions an identity certificate, CT3.1.4

10. Click on the plus button again to store a new credential, as in the step 8.
11. Select “Role”, fill the “Role ID” and “Role Authority” fields and click on the “Save” button, as Figure 126 shows.

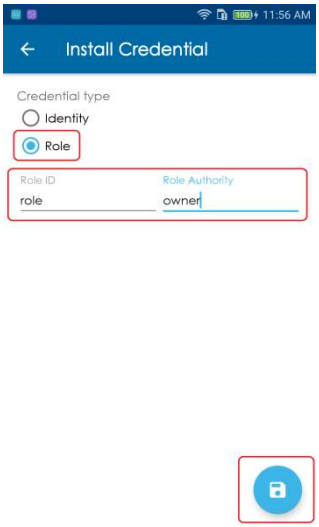

Figure 126: OTGC provisions a role certificate, CT3.1.4

5.1.6 CT3.1.5 CMS CAN PROVISION AN IDENTITY CERTIFICATE CHAIN

The goal of this test case is to verify that the OTGC can process a Certificate Signing Request from the CTT server and issue an identity certificate for it.

1. Execute the test case.
2. The test case request to discover and onboard the simulated CTT server using any supported OTM, as Figure 127 shows.

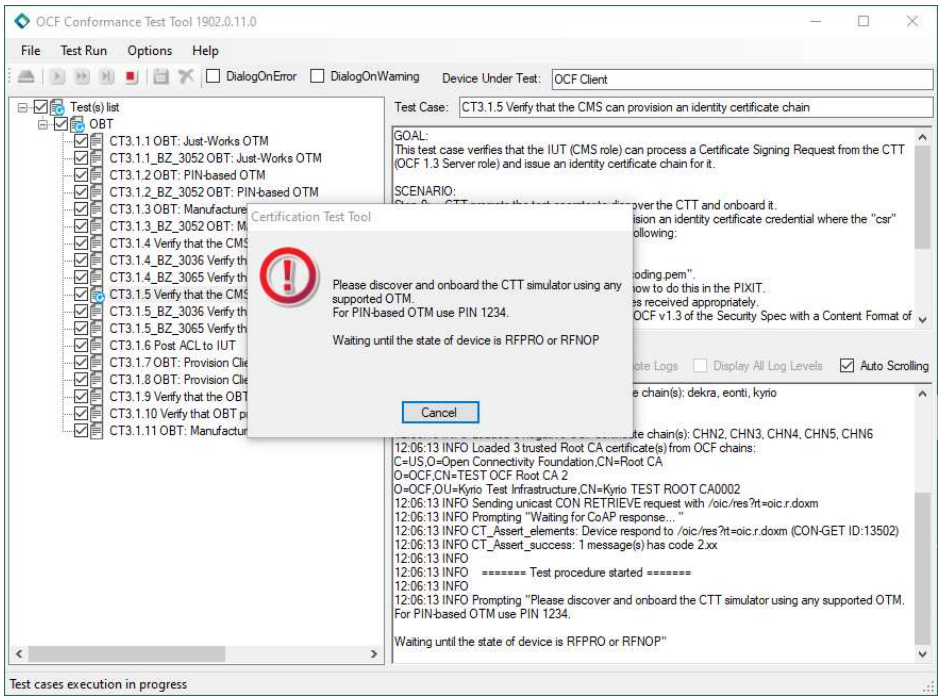

Figure 127: Discover and onboard a CTT server, CT3.1.5

3. Discover the devices on the OTGC clicking on the “Refresh” button at right-bottom as Figure 128 shows.

Figure 128: Scan devices on the OTGC, CT3.1.5

4. Click on the plus icon to onboard the CTT server, as Figure 129 shows.

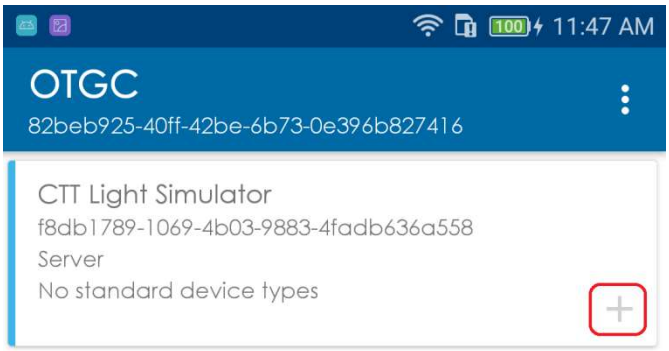

Figure 129: Onboard the CTT client, CT3.1.5

5. Select the method to do the ownership transfer.
6. When the onboard process has been completed, the test case will request to provision an identity certificate credential, as Figure 130 shows.

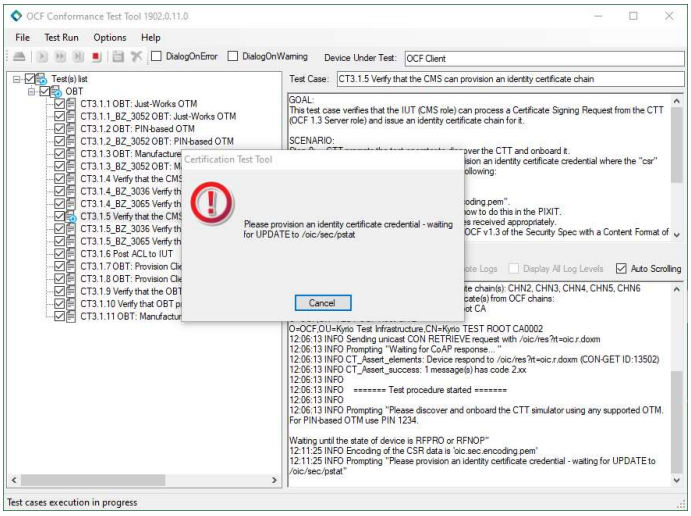

Figure 130: CTT requests to provision an identity certificate credential, CT3.1.5

7. Click on the three dots of the owned device and click on the “Credentials” button, as Figure 131 shows.

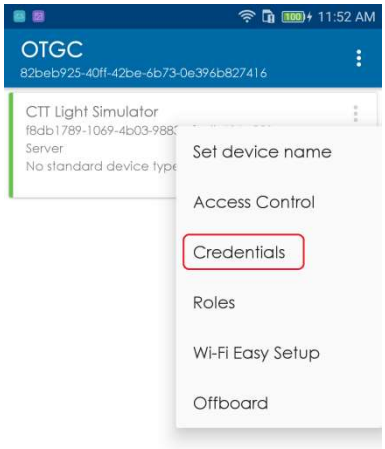

Figure 131: Select credentials on the owned device, CT3.1.5

8. Click on the plus button to store a new credential, as Figure 132 shows.

Figure 132: Add a new credential, CT3.1.5

9. Select “Identity” and click on the “Save” button, as **¡Error! No se encuentra el origen de la referencia.** shows.

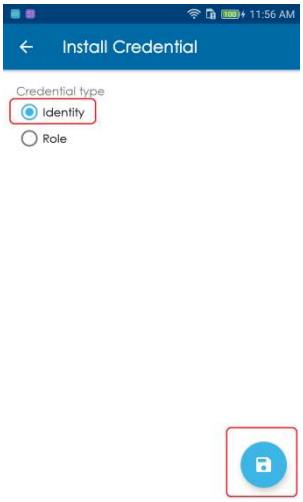

Figure 133: OTGC provisions an identity certificate, CT3.1.5

10. Wait 10 seconds to finish the test case.

5.1.7 CT3.1.6 POST ACL TO IUT

The goal of this test case is to verify that the OTGC can securely provision new ACEs to the CTT server.

1. Execute the test case.
2. The test case requests to discover the CTT server and onboard it using any supported OTM, as Figure 134 shows.

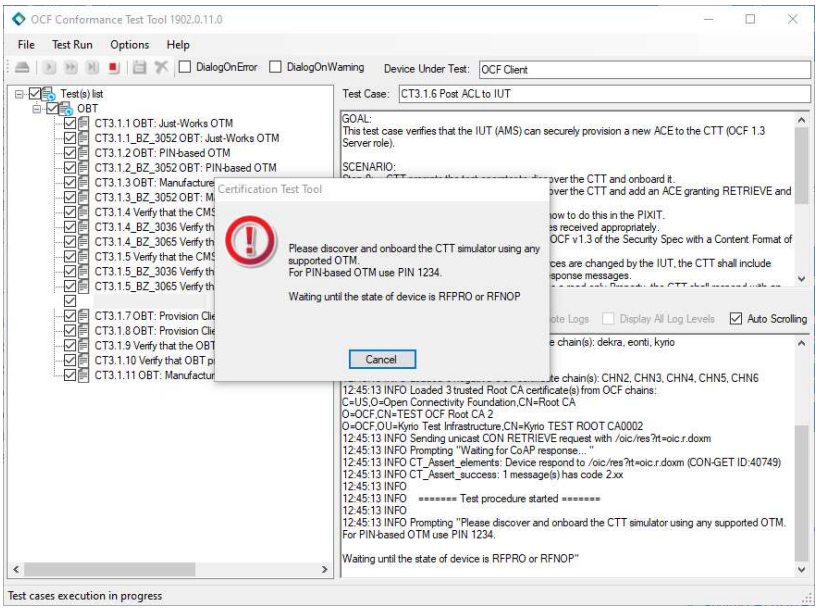

Figure 134: Discover and onboard a CTT server, CT3.1.6

3. Discover the devices clicking on the “Refresh” button at right-bottom, as Figure 135 shows.

Figure 135: Scan devices on the OTGC, CT3.1.6

4. Click on the plus icon to onboard the CTT server, as Figure 136 shows.

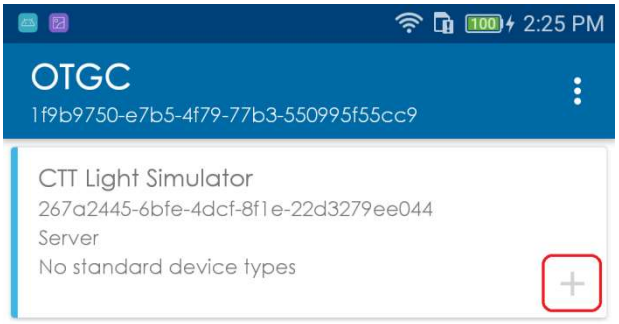

Figure 136: Onboard the CTT server, CT3.1.6

5. Select the method to do the ownership transfer.

6. When the onboard process has been completed, the test case will request to provision a new ACE that it grants RETRIEVE access to the Vertical Resource, as Figure 137 shows.

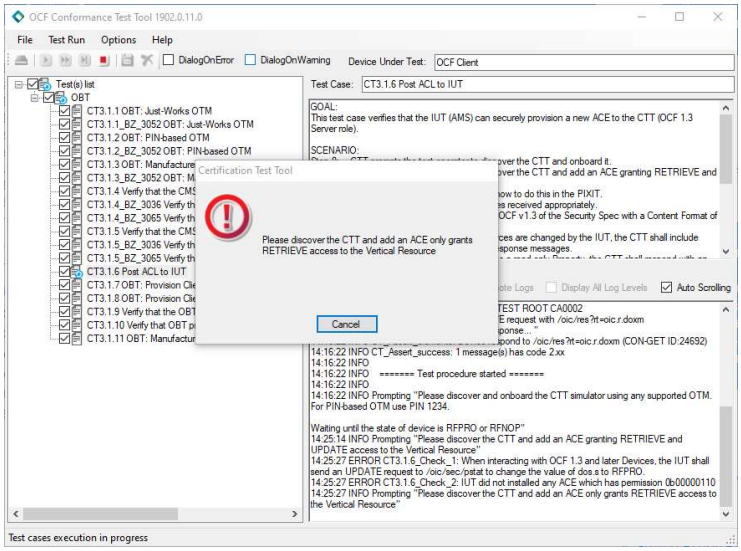

Figure 137: CTT requests to provision a new ACE, CT3.1.6

7. Click on the three dots of the owned device and click on the “Access Control” button:

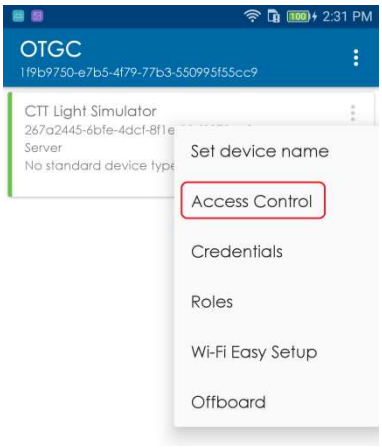

Figure 138: Select access control option on the owned device, CT3.1.6

8. Click on the plus button to add a new ACE, as Figure 139 shows.

Figure 139: Add a new ACE, CT3.1.6

9. Fill the ACE field as commented below and click on the “Save” button at right-bottom, as Figure 140 shows.
    a. Subject type: UUID
    b. UUID: <device UUID>
    c. Permits: Retrieve (R)
    d. Resources: Choose a resource

Figure 140: Provision an ACE by subject UUID, CT3.1.6

10. Delete the ACE added in the previous step clicking on the trash button, as shows.

Figure 141: Delete the ACE added, CT3.1.6

11. The test cases will request to add a new ACE that it grants RETRIEVE access to any authenticated client, as Figure 142 shows.

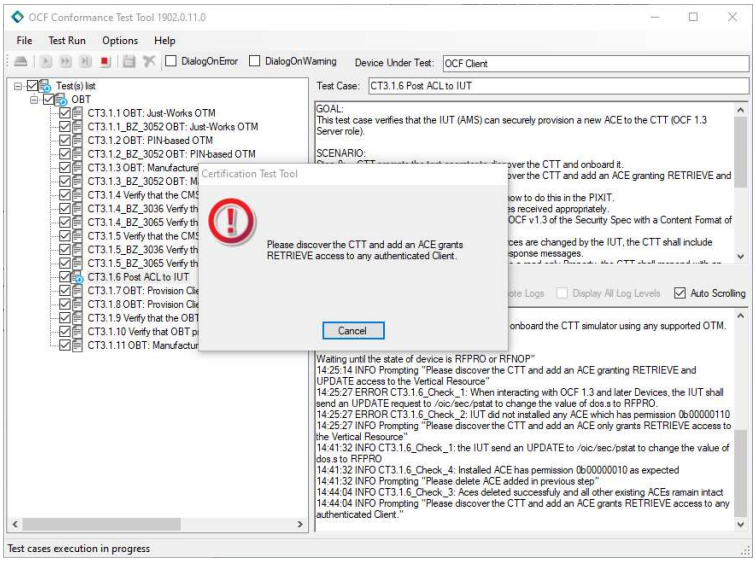

Figure 142: Provision an autheticated ACE, CT3.1.6

12. Click on the plus icon to add a new ACE, as in the step 8.
13. Fill the ACE fields as commented below and click on the “Save” button, as Figure 143 shows.
    a. Subject type: Connection type
    b. Connection type: Authenticated
    c. Permits: Retrieve (R)
    d. Resources: Choose a resource

Figure 143: Provision an ACE by connection type, CT3.1.6

14. Delete the ACE added in the previous step, as in the step 10.
15. The test case request to add a new ACE that it grants UPDATE access to "role1", as Figure 144 shows.

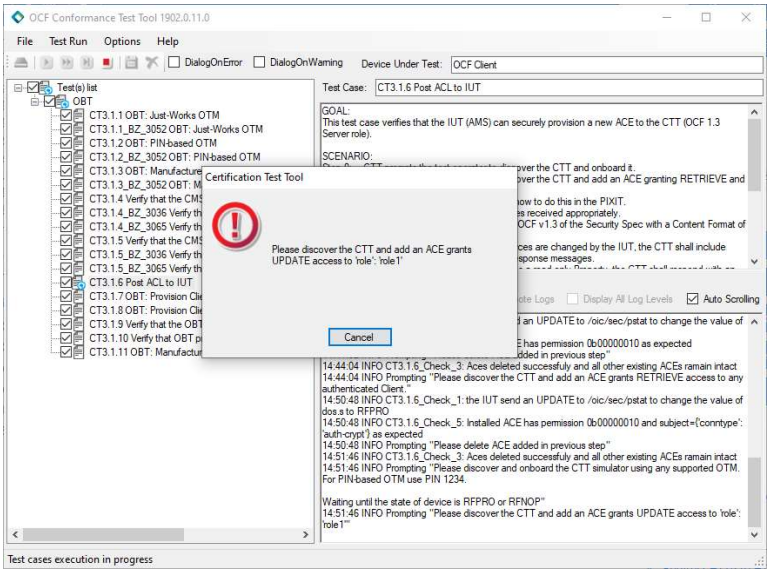

Figure 144: Provision a role ACE, CT3.1.6

16. Click on the plus button to a new ACE, as in the step 8.
17. Fill the ACE fields as commented below and click on the "Save" button, as Figure 145 shows.
    a. Subject type: Role
    b. Role ID: Role
    c. Role Authority: Authority of the role
    d. Permits: Update (U)
    e. Resources: Choose a resource

Figure 145: Provision a role ACE, CT3.1.6

18. Delete the ACE added in the previous step, as in the step 10.

5.1.8 CT3.1.7 PROVISION CLIENT AND SERVER WITH ROLES

The goal of this test case is to verify that the OTGC can onboard and provision the CTT server and the CTT client with appropriate ACEs and credentials that enable CTT client to access the resources on CTT server using roles.

1. Execute the test case.
2. The test case requests to discover the CTT client and the CTT server and onboard them using any supported OTM, as Figure 146 shows.

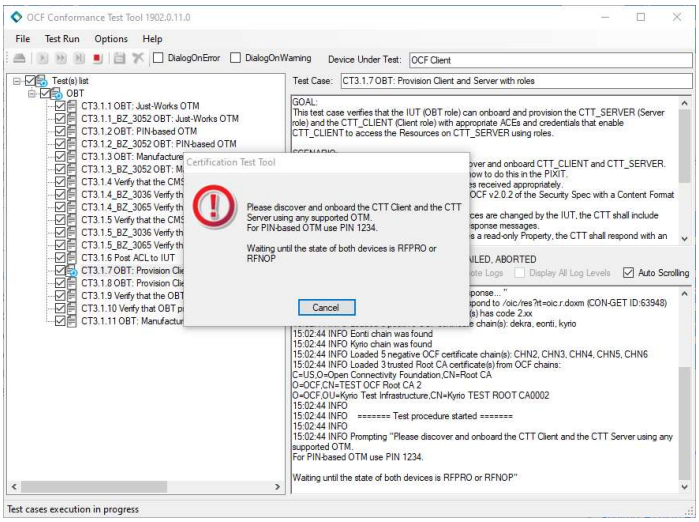

Figure 146: Discover CTT client and CTT server and onboard them, CT3.1.7

3. Discover the devices clicking on the “Refresh” button at right-bottom, as Figure 147 shows.

Figure 147: Scan devices on the OTGC, CT3.1.7

4. Onboard the CTT client and the CTT server by clicking on the plus icon, as Figure 148 shows.

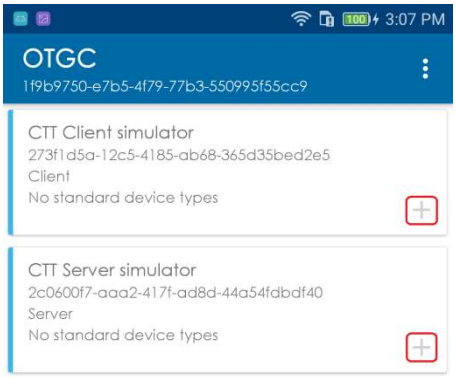

Figure 148: Onboard the CTT client and the CTT server, CT3.1.7

5. When the ownership transfer of both devices has been completed, the test case will request to provision a role credential to the CTT client and a role ACE to the CTT server, as Figure 149 shows.

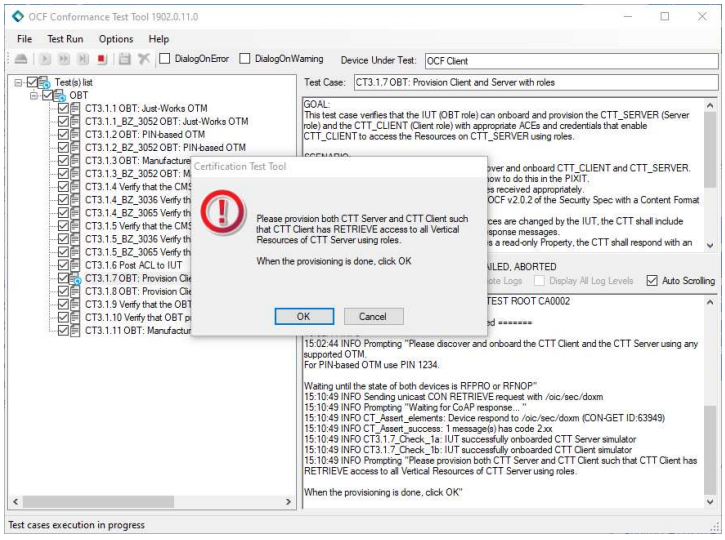

Figure 149: Provision role credential and role ACE, CT3.1.7

6. Click on the three dots on the CTT client and select the “Roles” option, as Figure 150 shows.

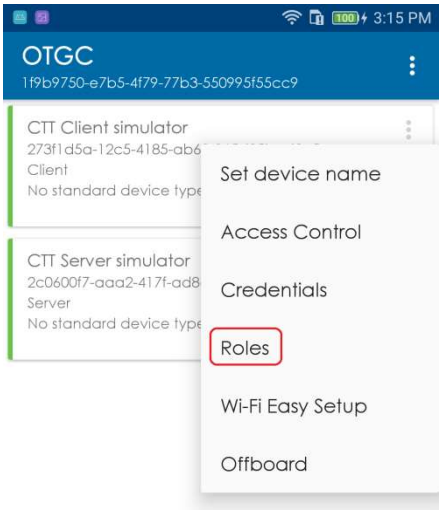

Figure 150: Add device to a role, CT3.1.7

7. Click on the plus icon to add a new role, as Figure 151 shows.

Figure 151: Add role to the CTT device, CT3.1.7

8. Fill “Role ID” and “Role authority” fields and click on the “Add” button, as Figure 152 shows.

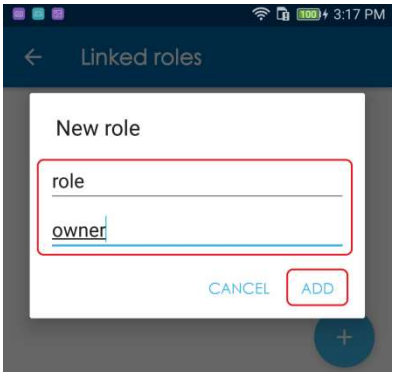

Figure 152: Add a new role, CT3.1.7

9. Click on the three dots on the CTT server and select the “Roles” option, as in the step 6.
10. Click on the plus icon to add a new role, as in the step 7.
11. Fill “Role ID” and “Role authority” fields with the same values as the step 8 and click on the “Add” button, as in the step 8.
12. Click on the “OK” button in the CTT to confirm the OTGC has provisioned to the CTT client and the CTT server.

5.1.9 CT3.1.8 PROVISION CLIENT AND SERVER WITH AUTHENTICATED ACCESS

The goal of this test case is to verify that the OTGC can onboard and provision the CTT server and the CTT client with appropriate ACEs and credentials that enable CTT client to access the resources on CTT server using wildcard ACEs and authenticated access.

1. Execute the test case.
2. The test case requests to discover the devices and onboard them using any supported OTM, as Figure 153 shows.

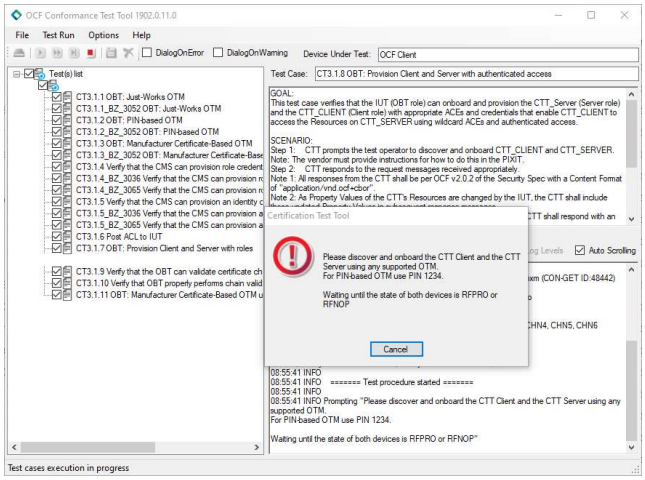

Figure 153: Discover CTT client and CTT server and onboard them, CT3.1.8

3. Discover the devices clicking on the “Refresh” button at right-bottom, as Figure 154 shows.

Figure 154: Scan devices on the OTGC, CT3.1.8

4. Onboard the CTT client and the CTT server by clicking on the plus icon, as Figure 155 shows.

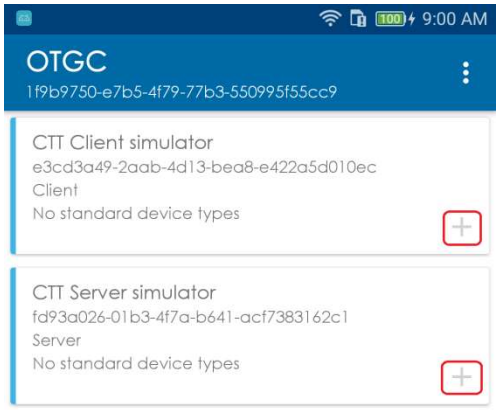

Figure 155: Onboard the CTT client and the CTT server, CT3.1.8

5. When the ownership transfer of both devices has been completed, the test case will request to provision the CTT client and the CTT server such that CTT client has RETRIEVE access to all non-configuration resources of the CTT server using its authenticated status, as Figure 156 shows.

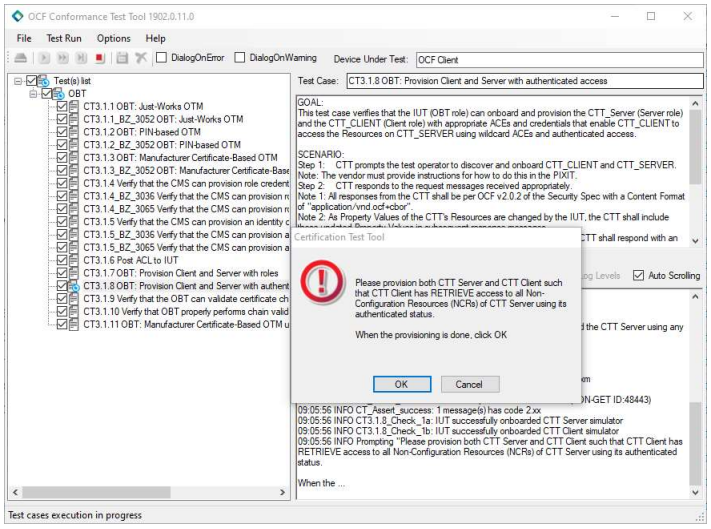

Figure 156: Provision CTT client and CTT server, CT3.1.8

6. Click on the three dots on the CTT client and select the “Credentials” option, as Figure 157 shows.

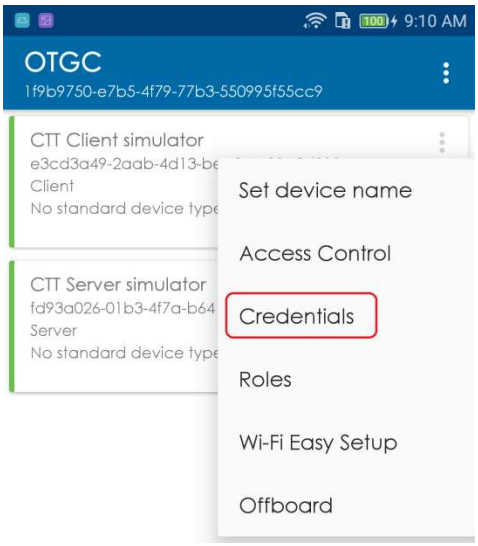

Figure 157: Provision credentials to the device, CT3.1.8

7. Click on the plus icon to provision a new credential, as Figure 158 shows.

Figure 158: Add a new credential, CT3.1.8

8. Select “Identity” and click on the “Save” button to provision an identity certificate, as Figure 159 shows.

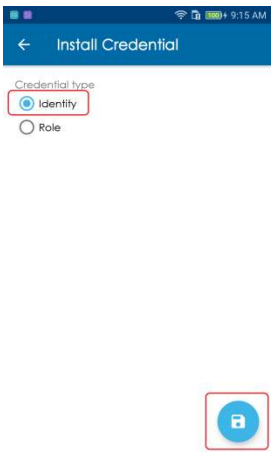

Figure 159: Provision an identity certificate to the device, CT3.1.8

9. Click on the three dots on the CTT server and select the “Credentials” option, as in the step 6.
10. Click on the plus icon to add a new credential, as in the step 7.
11. Select “Identity” and click on the “Save” button, as in the step 8.
12. Click on the three dots on the CTT server and select the “Access Control” option, as Figure 160 shows.

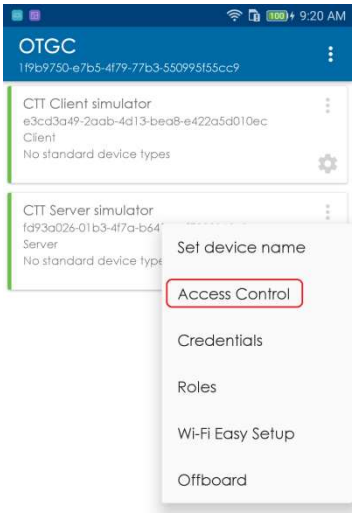

Figure 160: Provision ACEs to the CTT server, CT3.1.8

13. Click on the plus icon to add a new ACE, as Figure 161 shows.

Figure 161: Add a new ACE, CT3.1.8

14. Use the following configuration of the ACE and click on the “Save” button to provision a new ACE, as Figure 162 shows.
    a. Subject type: Connection type
    b. Connection type: Authenticated
    c. Permits: Retrieve (R)
    d. Wildcard -> All resources

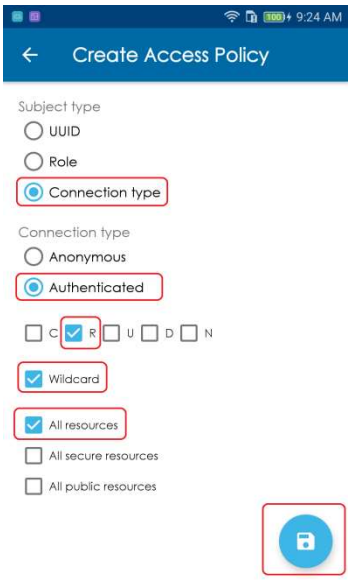

Figure 162: Provision an ACE for authenticated clients, CT3.1.8

15. Click on the “OK” button in the CTT to confirm the OTGC has provisioned to the CTT client and the CTT server.

5.1.10 CT3.1.10 OBT PROPERTLY PERFORMS CHAIN VALIDATION

The goal of this test case is to verify that the OTGC properly detects and rejects certificate profile and chaining violations during Manufacturer Certificate-based OTM.

1. Execute the test case.
2. The test case requests to discover the CTT device, as Figure 163 shows.

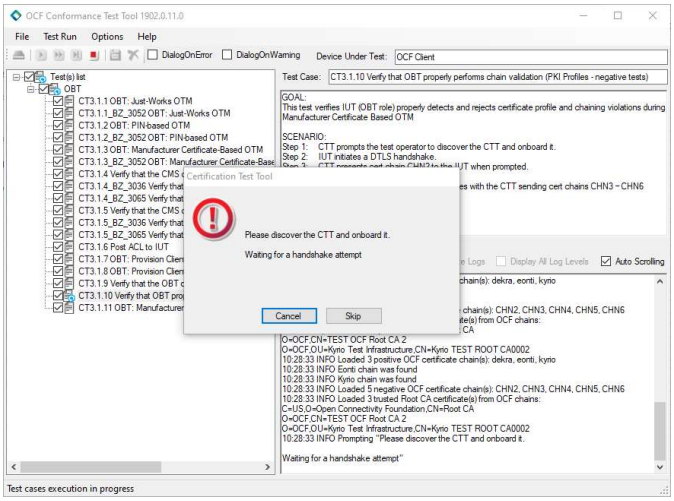

Figure 163: Discover the device and onboard it, CT3.1.10

3. Discover the devices clicking on the “Refresh” button at right-bottom, as Figure 164 shows.

Figure 164: Scan devices on the OTGC, CT3.1.10

4. Onboard the device clicking on the plus icon, as Figure 165 shows.

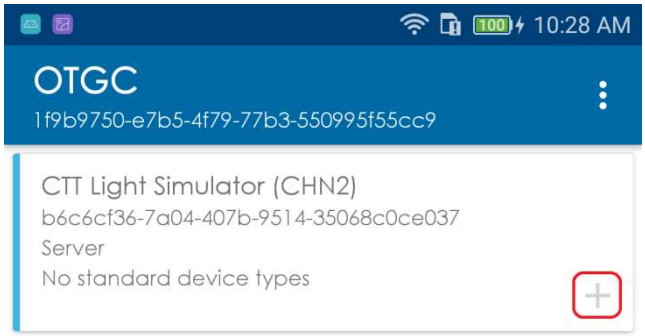

Figure 165: Onboard a device with a negative chain, CT3.1.10

5. The OTGC will show an error message to confirm that the ownership has failed.
6. Repeat the steps 2-5 for each negative certificate in the CTT installation folder.

5.1.11 CT3.1.11 MANUFACTURER CERTIFICATE-BASED OTM USING A CUSTOM TRUST ANCHOR

The goal of this test case is to verify that the OTGC is able to successfully onboard the CTT server using configured manufacturer certificate-based OTM.

1. Execute the test case.
2. The test case request to copy the manufacturer root certificate clicking on the “Copy” button, as Figure 166 shows.

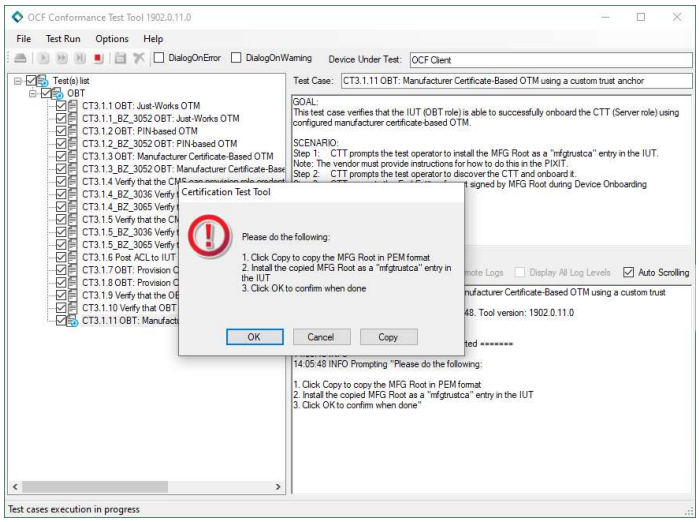

Figure 166: CTT requests to copy a new root certificate, 3.1.11

3. Copy it into a text file and copy the file to the OTGC.
4. Click on the three dots on the toolbar and select the “Trust Anchor Management” option to add new root certificates, as Figure 167 shows.

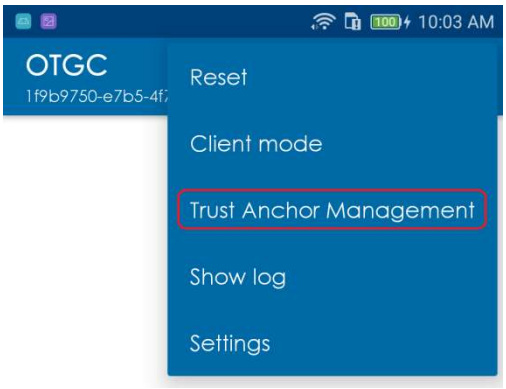

Figure 167: Trust anchor management, CT3.1.11

5. Click on the plus icon to add new root certificates, as Figure 168 shows.

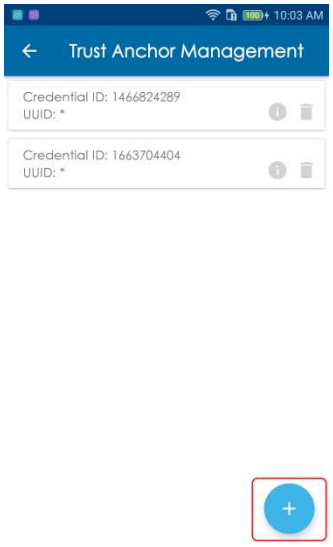

Figure 168: Add a new trust anchor, CT3.1.11

6. Select the file copied in the step 3, as Figure 169 shows.

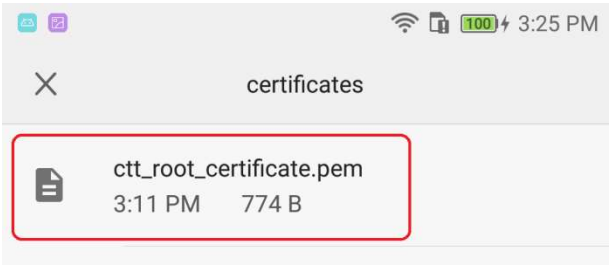

Figure 169: CTT root certificate, CT3.1.11

7. Click on the “OK” button in the CTT to confirm that the manufacturer certificate is copied into the OTGC.
8. The test case requests to discover the CTT and onboard it, as Figure 170 shows.

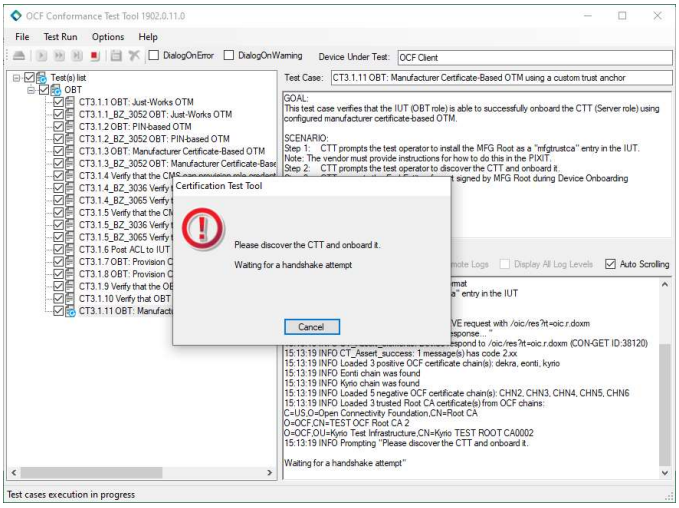

Figure 170: Discover the CTT device and onboard it, CT3.1.11

1. Discover the devices clicking on the “Refresh” button at right-bottom, as Figure 171 shows.

Figure 171: Scan devices on the OTGC, CT3.1.11

9. Onboard the CTT device clicking on the plus icon, as Figure 172 shows.

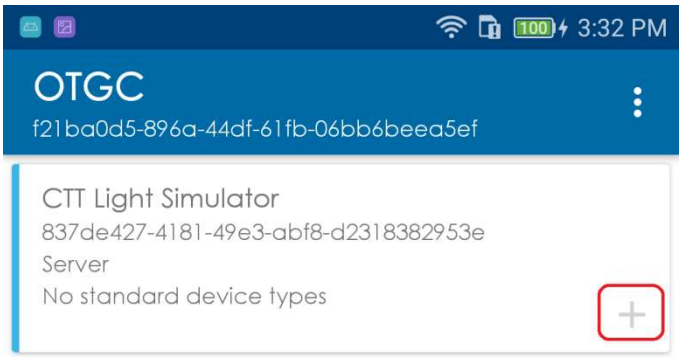

Figure 172: Onboard the CTT device, CT3.1.11

10. The OTGC will show an error message because the CTT turns off the CTT device before it responds to all requests.

5.2 CLIENT TEST CASES

5.2.1 PRE-EXECUTION CLIENT TEST CASES

The OTGC has to be in Client mode clicking on the three dots at right-top and selecting the “Client mode” option, as Figure 173 shows. If the “Client mode” option is not visible, the OTGC is already in Client mode.

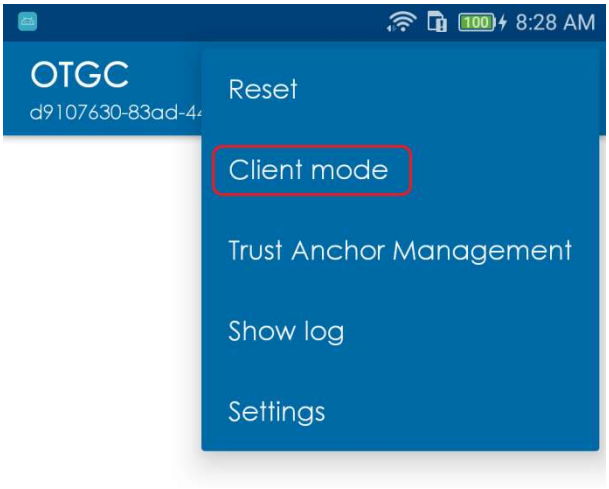

Figure 173: Set Client mode, Client test cases.

5.2.2 CT2.2.2 RETRIEVE MESSAGE BASED ON COAP

The goal of this test case is to verify that the OTGC sends proper RETRIEVE request messages to the CTT server for all resource types in the PICS.

1. Execute the test case.
2. CTT requests to discover the CTT server and to send a GET request to the resource, as Figure 174 shows.

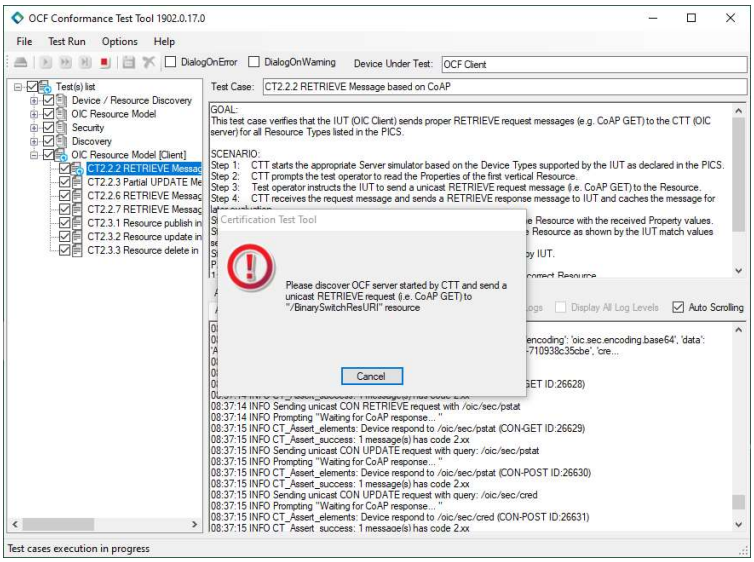

Figure 174: Send GET request to the resource, CT2.2.2

3. Discover the devices clicking on the “Refresh” button at right-bottom, as Figure 175 shows.

Figure 175: Scan devices on the CTT, CT2.2.2

4. Click on the “Gear” button to view the resources on the server, as Figure 176 shows.

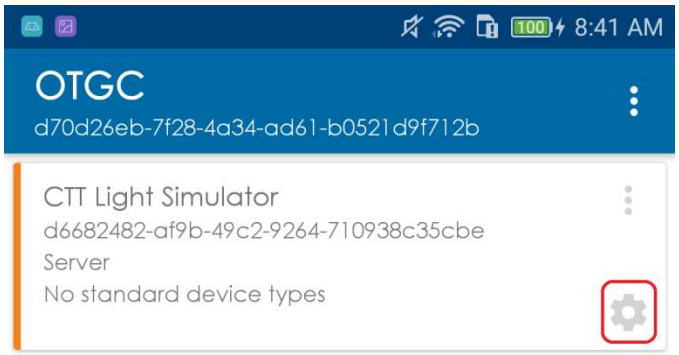

Figure 176: Click on the Gear button to view the resources, CT2.2.2

5. Click on the arrow of the resource to display its values, as Figure 177 and Figure 178 show.

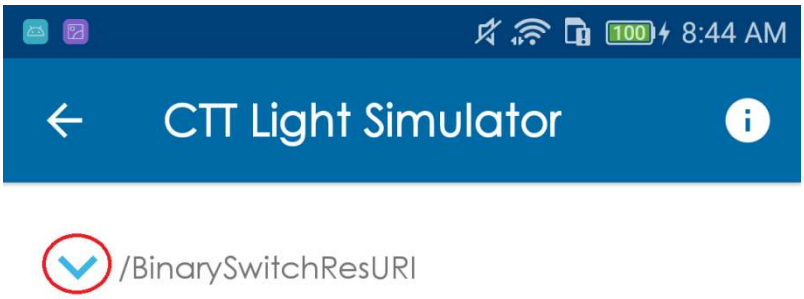

Figure 177: Click on the arrow to view the values of the resource, CT2.2.2

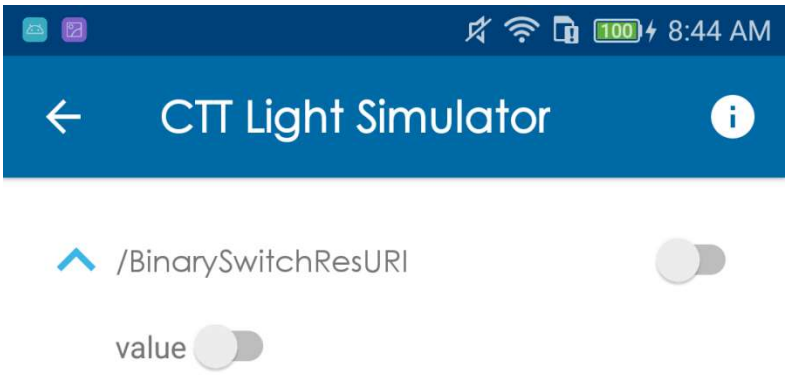

Figure 178: Values of the resource, CT2.2.2

6. The CTT requests to confirm that the OTGC has the possibility to display the received properties values and click on the “Yes” button, as Figure 179 shows.

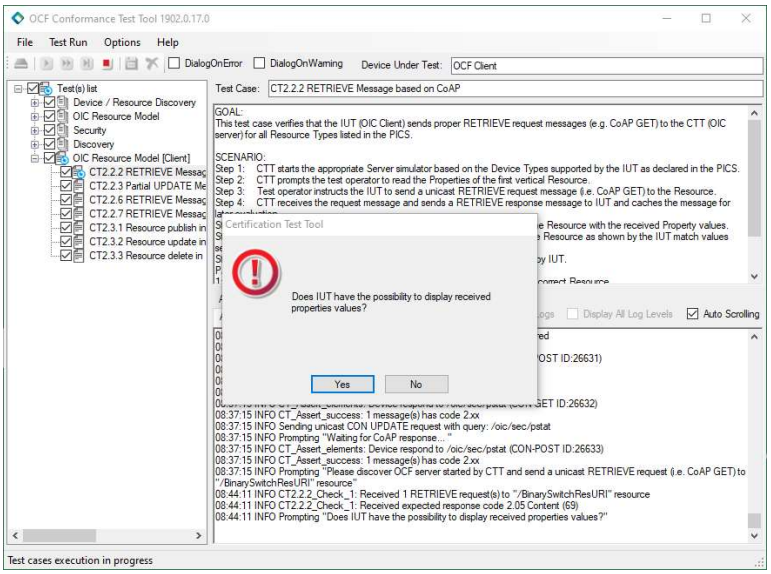

Figure 179: CTT requests to confirm that the OTGC displays the values, CT2.2.2

5.2.3 CT2.2.3 PARTIAL UPDATE MESSAGE BASED ON COAP

The goal of this test is to verify that the OTGC sends proper partial UPDATE request messages to the CTT server for all resource types with updateable properties listed in the PICS.

1. Execute the test case.
2. CTT requests to discover the CTT server and to send a POST request to the resource, as Figure 180 shows.

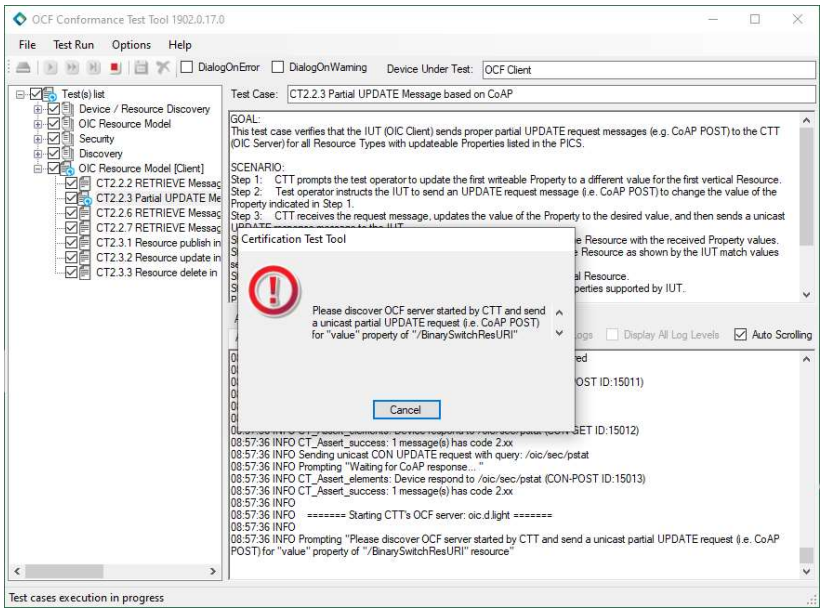

Figure 180: Send POST request to the resource, CT2.2.3

3. Discover the devices clicking on the “Refresh” button at right-bottom, as Figure 181 shows.

Figure 181: Scan devices on the CTT, CT2.2.3

4. Click on the “Gear” button to view the resources on the server, as Figure 182 shows.

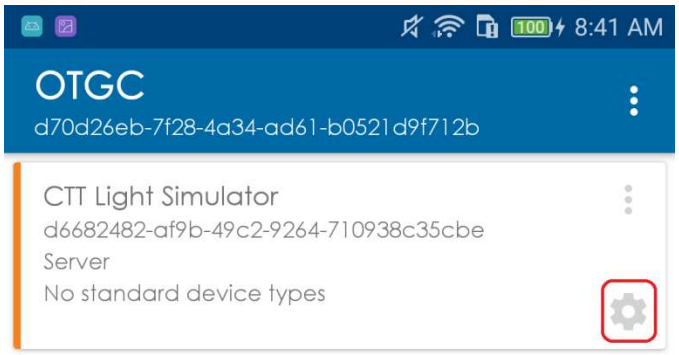

Figure 182: Click on the Gear button to view the resources, CT2.2.3

5. Click on the arrow of the resource to display its values, as Figure 183 and Figure 184 show.

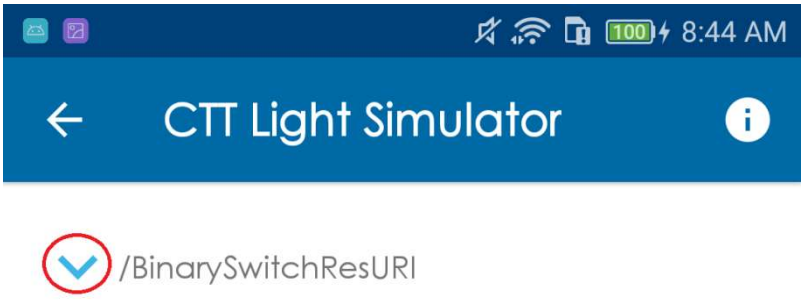

Figure 183: Click on the arrow to view the values of the resource, CT2.2.3

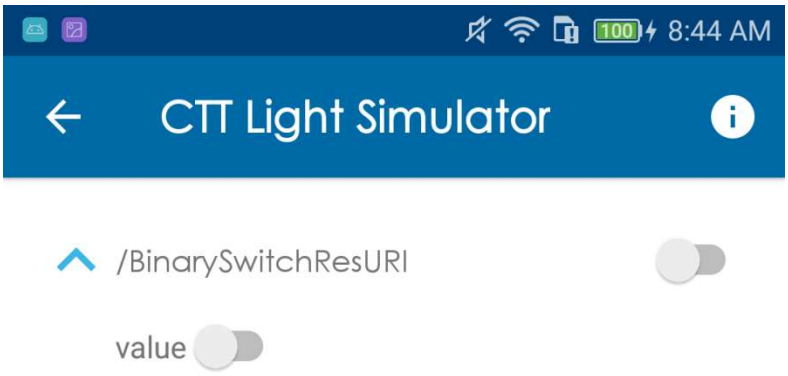

Figure 184: Values of the resource, CT2.2.3

6. Update the value of the resource, as Figure 185 shows.

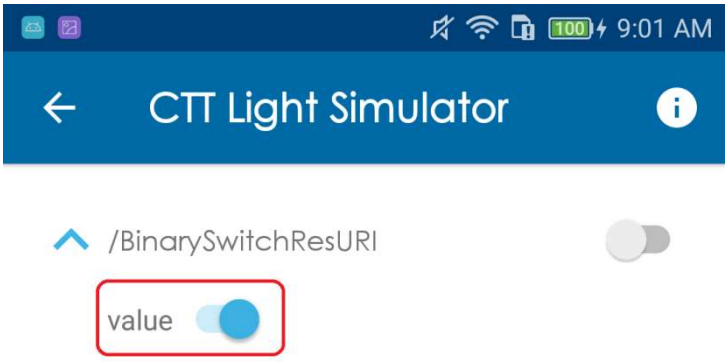

Figure 185: Update the value of the resource, CT2.2.3

7. The CTT requests to confirm that the OTGC has the possibility to display the received properties values and click on the “Yes” button, as Figure 186 shows.

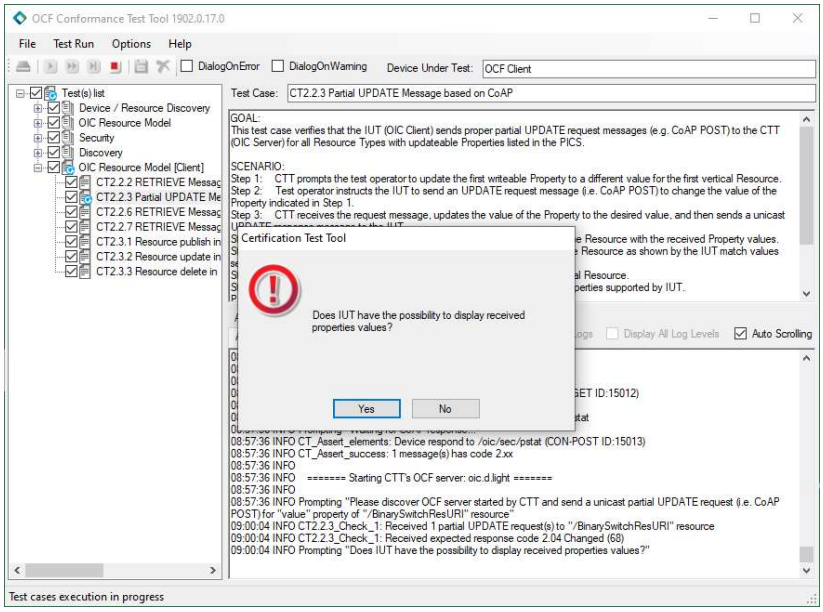

Figure 186: CTT requests to confirm that the OTGC displays the values, CT2.2.3

5.2.4 CT2.2.6 RETRIEVE MESSAGE WITH OBSERVE INDICATION BASED ON COAP

The goal of this test is to verify that the OTGC properly handles RETRIEVE request messages sent to the CTT server with an observe indication for all resource types listed in the PICS.

1. Execute the test case.
2. CTT requests to discover the CTT server and to send a GET request to the resource with the observe option = 0, as Figure 187 shows.

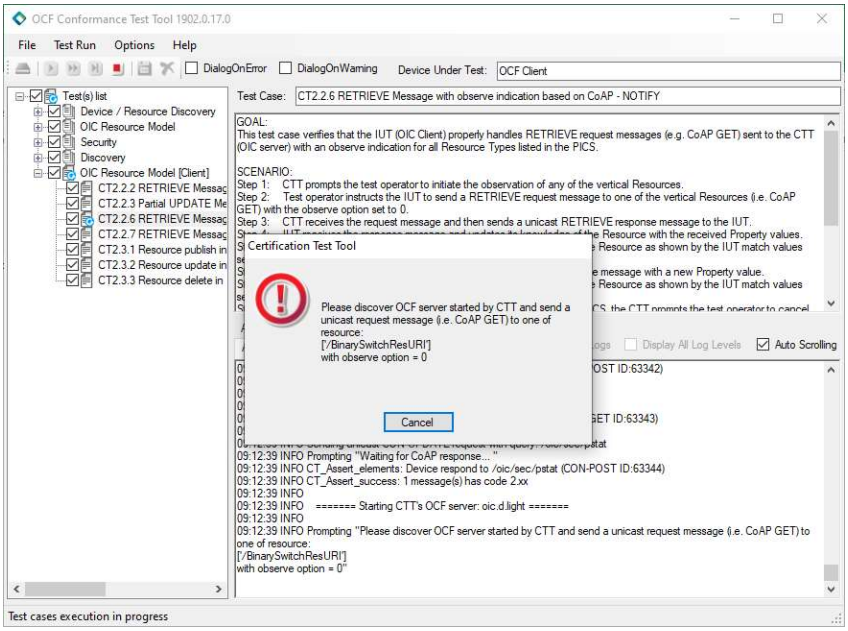

Figure 187: Send GET request with observe option to the resource, CT2.2.6

3. Discover the devices clicking on the “Refresh” button at right-bottom, as Figure 188 shows.

Figure 188: Scan devices on the CTT, CT2.2.6

4. Click on the “Gear” button to view the resources on the server, as Figure 189 shows.

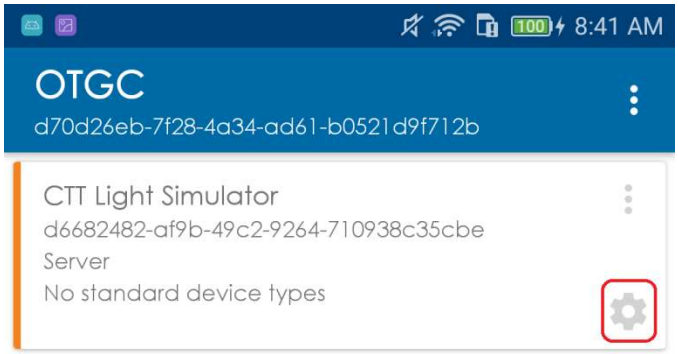

Figure 189: Click on the Gear button to view the resources, CT2.2.6

5. Click on the arrow of the resource to display its values, as Figure 190 and Figure 191 show.

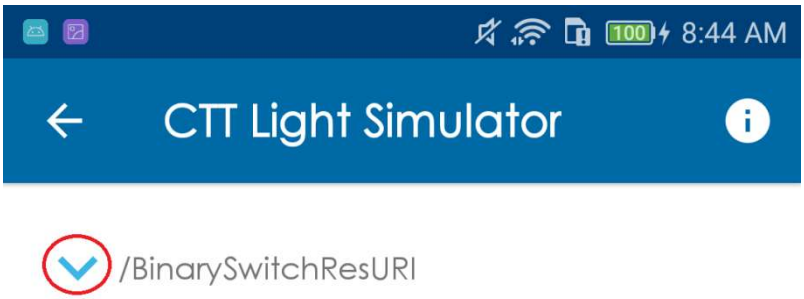

Figure 190: Click on the arrow to view the values of the resource, CT2.2.3

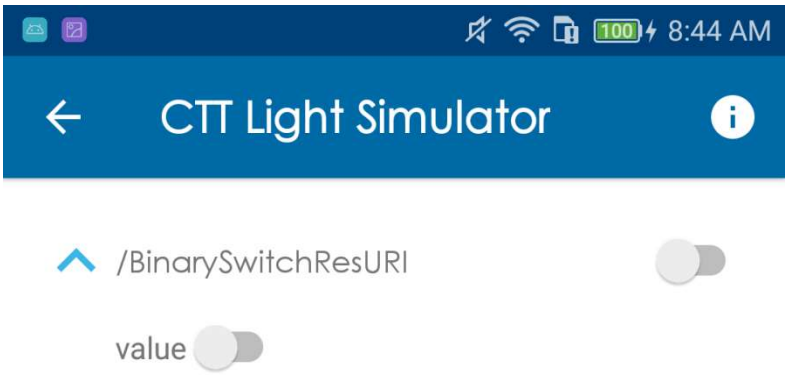

Figure 191: Values of the resource, CT2.2.3

6. Click on the observe switch to enable the observation, as Figure 192 shows.

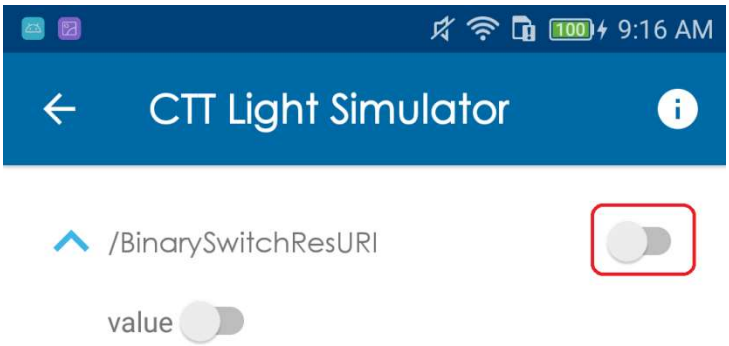

Figure 192: Click on the observe switch to enable the observation, CT2.2.6

7. The CTT requests to confirm that the OTGC has the possibility to display the received properties values and click on the “Yes” button, as Figure 193 shows.

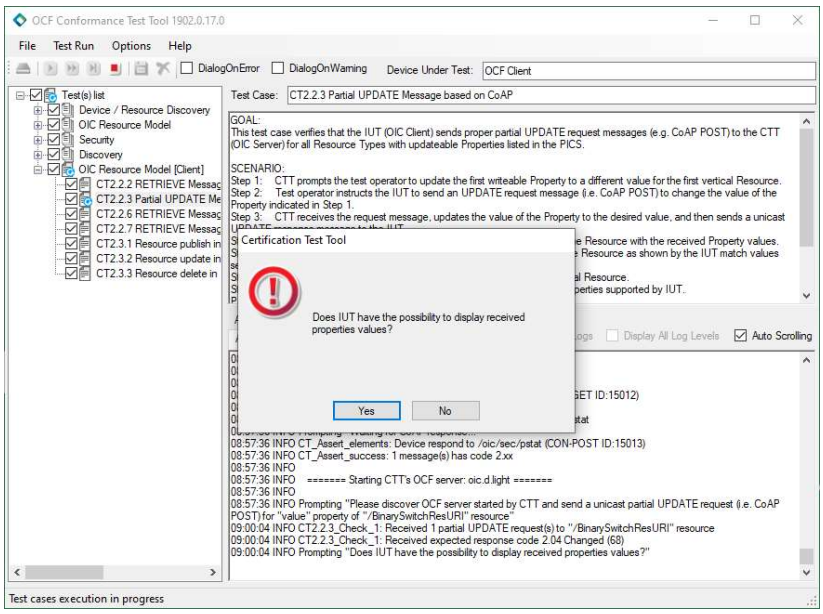

Figure 193: CTT requests to confirm that the OTGC displays the values, CT2.2.6

8. Wait 5 seconds.
9. The CTT sends a NOTIFY request with a new value, as Figure 194 shows.

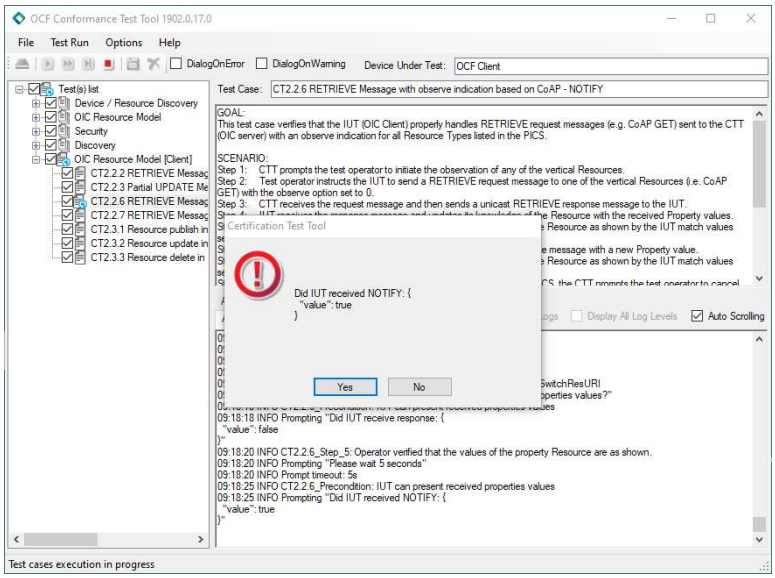

Figure 194: CTT sends a NOTIFY request, CT2.2.6

10. The OTGC should update the value on the UI, as Figure 195 shows.

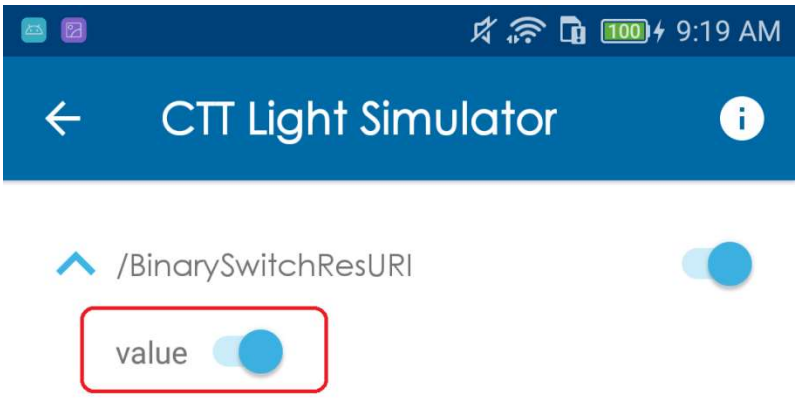

Figure 195: The OTGC updates the value of the resource, CT2.2.6

11. Click on the “Yes” button to confirm that the OTGC has updated the value of the resource.
12. The CTT requests to send a GET request to the resource with the observe option = 1, as Figure 196 shows.

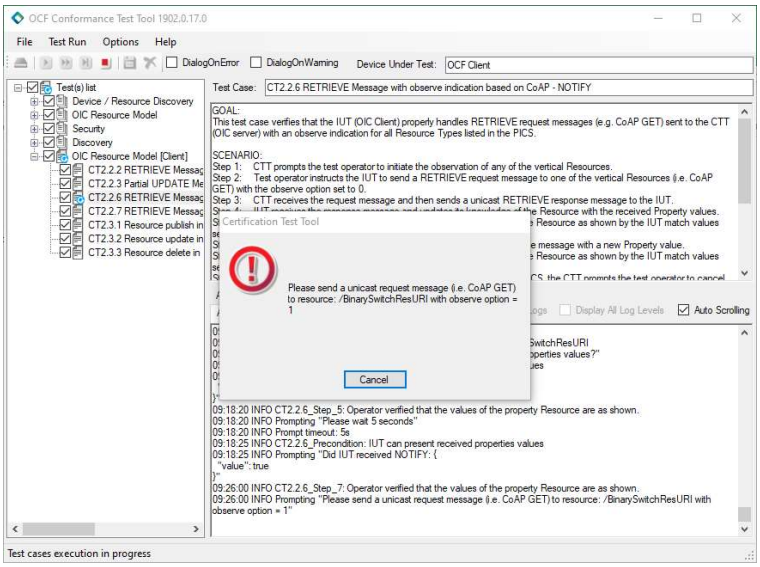

Figure 196: CTT requests to send a GET request with observe option = 1, CT2.2.6

13. Click on the observe switch to disable the observation, as Figure 197 shows.

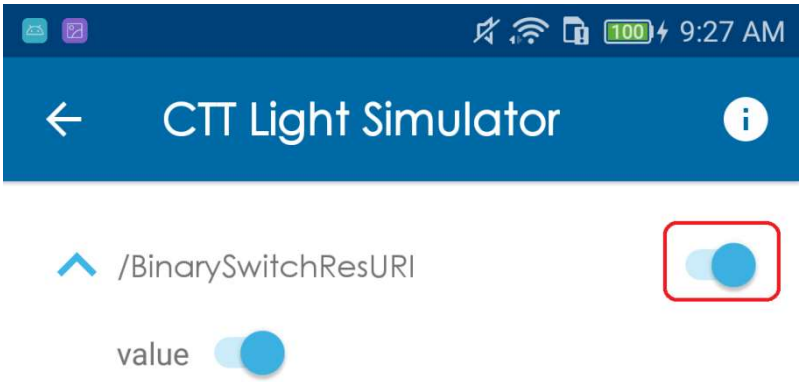

Figure 197: Click on the observe switch to disable the observation, CT2.2.6