

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. |

Disclaimer

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

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

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

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

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

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



TABLE OF CONTENTS

| | | |
|----------|--|-----------|
| 1 | SCOPE | 7 |
| 2 | REFERENCES | 8 |
| 3 | DEFINITIONS AND ABBREVIATIONS | 9 |
| 3.1 | DEFINITIONS | 9 |
| 3.2 | ABBREVIATIONS | 10 |
| 4 | USER INSTRUCTIONS..... | 11 |
| 4.1 | OVERVIEW | 11 |
| 4.2 | ANDROID..... | 12 |
| 4.2.1 | Wi-Fi scanning | 12 |
| 4.2.2 | Device scanning | 13 |
| 4.2.3 | Onboard a device | 14 |
| 4.2.4 | Manage a device | 14 |
| 4.2.5 | Credentials..... | 15 |
| 4.2.6 | Access control list..... | 17 |
| 4.2.7 | Offboard a device | 19 |
| 4.2.8 | Wi-Fi Easy Setup | 19 |
| 4.2.9 | Reset OTGC | 20 |
| 4.2.10 | Self-own the otgc..... | 21 |
| 4.3 | LINUX..... | 22 |
| 4.3.1 | Scanning devices..... | 22 |
| 4.3.2 | Onboard a device | 22 |
| 4.3.3 | Manage a device | 23 |
| 4.3.4 | Offboard a device | 25 |
| 4.3.5 | Reset OTGC | 26 |
| 4.3.6 | Owned OTGC by self..... | 26 |
| 4.4 | UWP | 27 |
| 4.4.1 | Scanning devices..... | 27 |
| 4.4.2 | Onboard a device | 27 |
| 4.4.3 | Manage a device | 28 |
| 4.4.4 | Credentials..... | 29 |
| 4.4.5 | Access control list..... | 30 |
| 4.4.6 | Offboard a device | 32 |
| 4.4.7 | Reset OTGC | 32 |
| 4.4.8 | Owned OTGC by self..... | 33 |
| 4.5 | IOS..... | 34 |
| 4.5.1 | Device scanning | 34 |
| 4.5.2 | Onboard a device | 34 |



| | | |
|-------|--------------------------|----|
| 4.5.3 | Manage a device | 35 |
| 4.5.4 | Credentials..... | 36 |
| 4.5.5 | Access control list..... | 38 |
| 4.5.6 | Offboard a device | 39 |
| 4.5.7 | Wi-Fi Easy Setup..... | 40 |
| 4.5.8 | Reset OTGC | 41 |
| 4.5.9 | Self-own the otgc..... | 42 |

TABLE OF FIGURES

| | |
|---|----|
| Figure 1: “Connect to Wi-Fi network” dialog, Android..... | 12 |
| Figure 2: Empty devices list screen, Android. | 13 |
| Figure 3: Devices list with an OCF device detected, Android. | 13 |
| Figure 4: Onboard button, Android..... | 14 |
| Figure 5: Owned-by-self device, Android. | 14 |
| Figure 6: Generic Client button. | 15 |
| Figure 7: Resources in an OCF server, Android..... | 15 |
| Figure 8: Device information panel, Android. | 15 |
| Figure 9: Credentials option, Android..... | 16 |
| Figure 10: Currently installed credentials list, Android..... | 16 |
| Figure 11: Provision a new credential, Android. | 17 |
| Figure 12: Access Control option, Android. | 17 |
| Figure 13: Access control list, Android. | 18 |
| Figure 14: Provision a new access control policy, Android..... | 19 |
| Figure 15: Offboard an owned device, Android. | 19 |
| Figure 16: “Wi-Fi Easy Setup” option, Android. | 20 |
| Figure 17: Input Wi-Fi credentials dialog, Android..... | 20 |
| Figure 18: Reset OTGC, Android. | 21 |
| Figure 19: Self-own the OTGC, Android..... | 21 |
| Figure 20: Scan devices, Linux. | 22 |
| Figure 21: Onboard a device, Linux. | 22 |
| Figure 22: Devices list with an owned device, Linux..... | 23 |
| Figure 23: Device information and Generic Client, Linux..... | 23 |
| Figure 24: Access control, Linux. | 24 |
| Figure 25: Credentials, Linux. | 25 |
| Figure 26: Offboard a device, Linux. | 26 |
| Figure 27: Reset OTGC, Linux..... | 26 |
| Figure 28: Self-own OTGC, Linux. | 26 |
| Figure 29: Scan devices, Windows 10. | 27 |
| Figure 30: Onboard a device, Windows 10. | 27 |
| Figure 31: Owned-by-self device, Windows 10. | 28 |
| Figure 32: Generic Client button, Windows 10. | 28 |
| Figure 33: Generic Client tab, Windows 10. | 28 |
| Figure 34: Generic Client screen, Windows 10. | 29 |
| Figure 35: Credential button, Windows 10. | 29 |



| | |
|---|----|
| Figure 36: Credentials tab, Windows 10..... | 29 |
| Figure 37: Credentials screen, Windows 10. | 30 |
| Figure 38: Add a new credential in Credentials screen, Windows 10. | 30 |
| Figure 39: Access control list button, Windows 10. | 31 |
| Figure 40: Access control tab, Windows 10. | 31 |
| Figure 41: Access control screen, Windows 10..... | 31 |
| Figure 42: Add a new access control policy in Access Control screen, Windows 10. .. | 32 |
| Figure 43: Offboard a device, Windows 10. | 32 |
| Figure 44: Reset OTGC, Windows 10..... | 33 |
| Figure 45: Self-own OTGC, Windows 10. | 33 |
| Figure 46: Empty devices list screen, iOS..... | 34 |
| Figure 47: List with OCF devices detected, iOS. | 34 |
| Figure 48: Onboard button, iOS. | 35 |
| Figure 49: Owned-by-self device, iOS..... | 35 |
| Figure 50: Generic Client button, iOS. | 35 |
| Figure 51: Resources in an OCF server, iOS..... | 36 |
| Figure 52: Device information panel, iOS..... | 36 |
| Figure 53: Credentials option, iOS. | 37 |
| Figure 54: Currently installed credentials list, iOS. | 37 |
| Figure 55: Provision a new credential, iOS. | 37 |
| Figure 56: Access Control option, iOS. | 38 |
| Figure 57: Access control list, iOS. | 38 |
| Figure 58: Provision a new access control policy, iOS. | 39 |
| Figure 59: Offboard an owned device, iOS. | 40 |
| Figure 60: “Wi-Fi Easy Setup” option, iOS. | 41 |
| Figure 61: Input Wi-Fi credentials dialog, iOS. | 41 |
| Figure 62: Reset OTGC, iOS. | 42 |
| Figure 63: Self-own the OTGC, iOS..... | 42 |

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.

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 the 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.

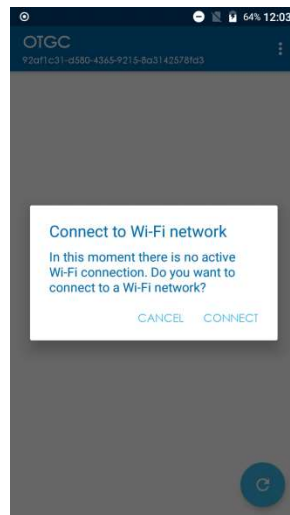


Figure 1: “Connect to Wi-Fi network” dialog, Android.

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.

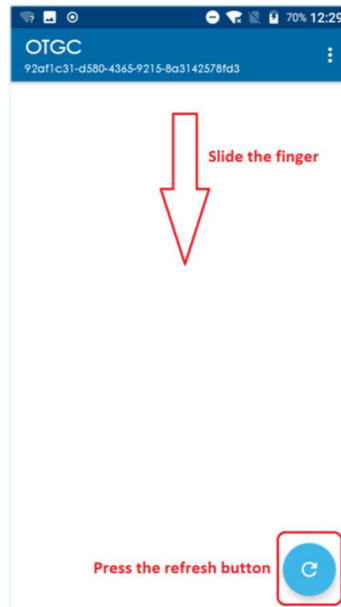


Figure 2: Empty devices list screen, Android.

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.

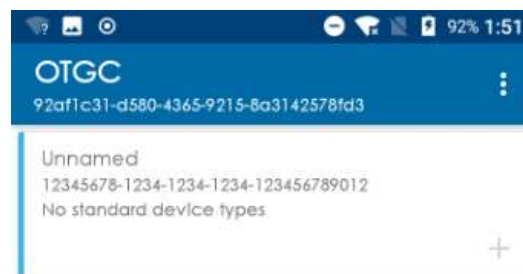


Figure 3: Devices list with an OCF device detected, Android.

4.2.3 ONBOARD A DEVICE

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



Figure 4: 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.

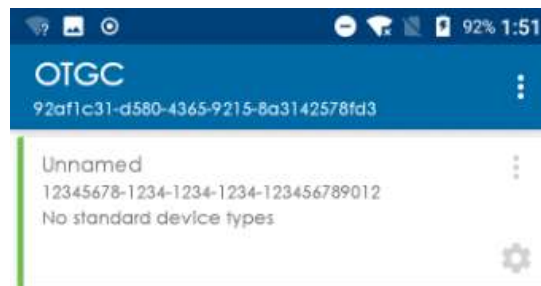


Figure 5: Owned-by-self device, Android.

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 6: Generic Client button.

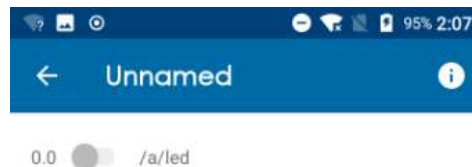


Figure 7: Resources in an OCF server, Android.

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

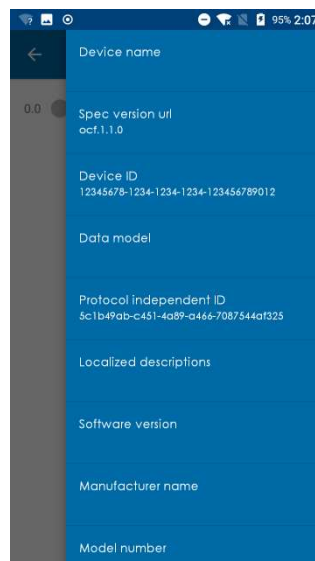


Figure 8: Device information panel, Android.

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

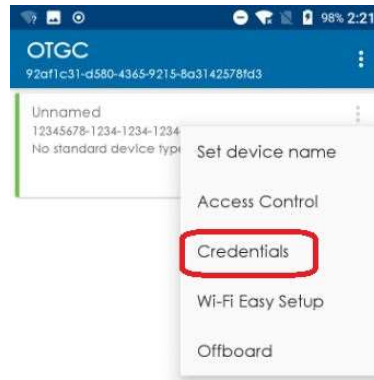


Figure 9: Credentials option, Android.

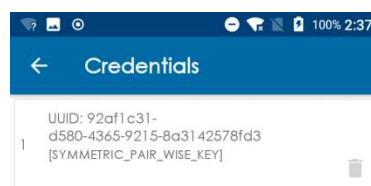


Figure 10: Currently installed credentials list, Android.

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

- Identity certificates.
- Role certificates.

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

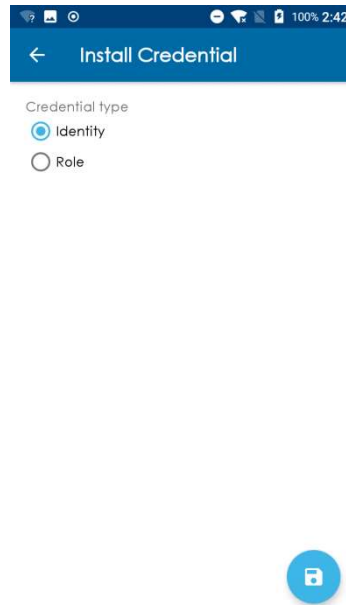


Figure 11: Provision a new credential, Android.

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 13.

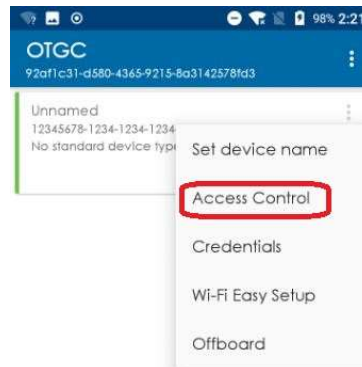


Figure 12: Access Control option, Android.



Figure 13: 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 13 and a new screen appears with a form to fill (Figure 14). The following fields can be configured:

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

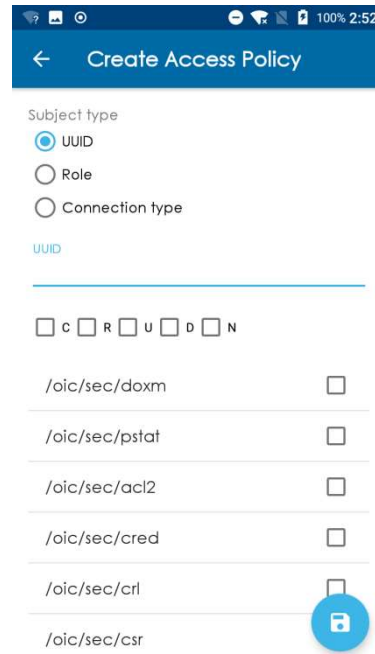


Figure 14: Provision a new access control policy, Android.

4.2.7 OFFBOARD A DEVICE

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

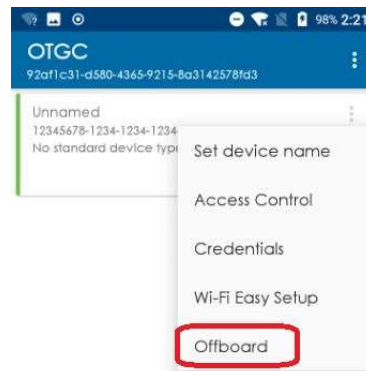


Figure 15: Offboard an owned device, Android.

4.2.8 WI-FI EASY SETUP

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

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

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

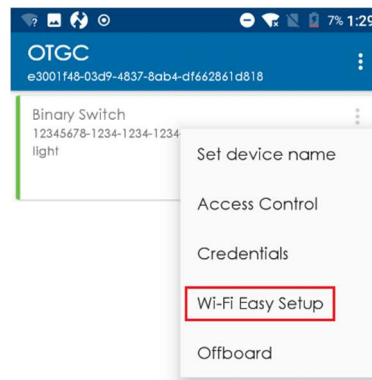


Figure 16: “Wi-Fi Easy Setup” option, Android.

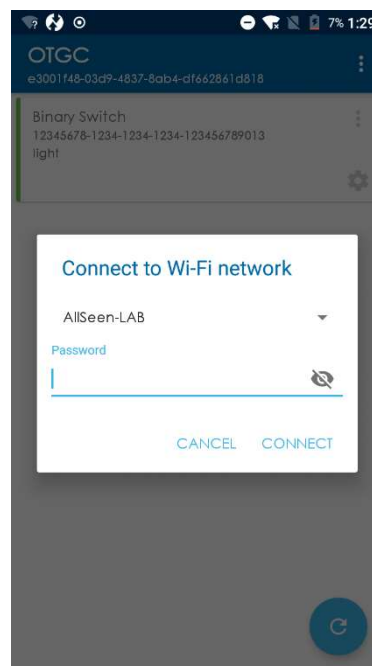


Figure 17: Input Wi-Fi credentials dialog, Android.

4.2.9 RESET OTGC

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

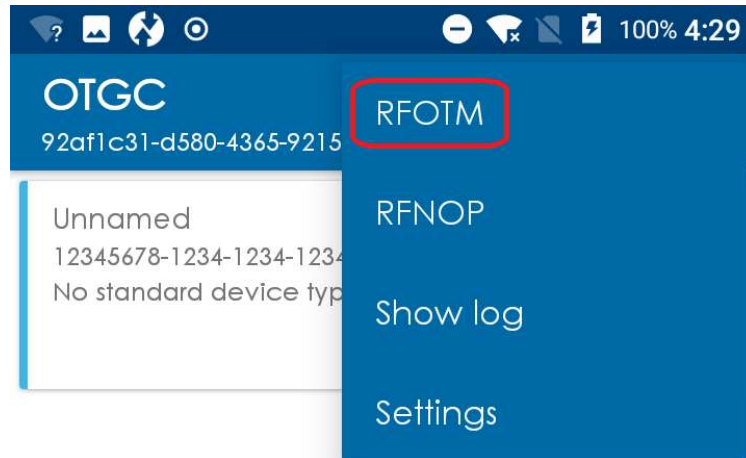


Figure 18: Reset OTGC, Android.

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

4.2.10 SELF-OWN THE OTGC

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

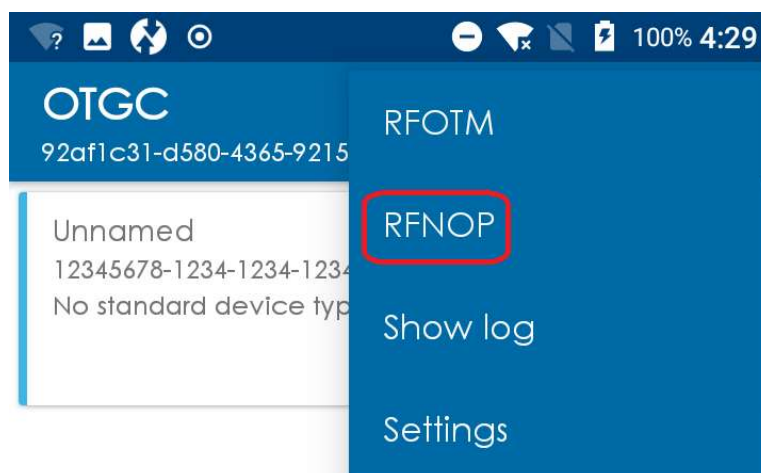


Figure 19: Self-own the OTGC, Android.

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 20 shows.



Figure 20: Scan devices, Linux.

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

4.3.2 ONBOARD A DEVICE

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



Figure 21: Onboard a device, 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 22: Devices list with an owned device, Linux.

4.3.3 MANAGE A DEVICE

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

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

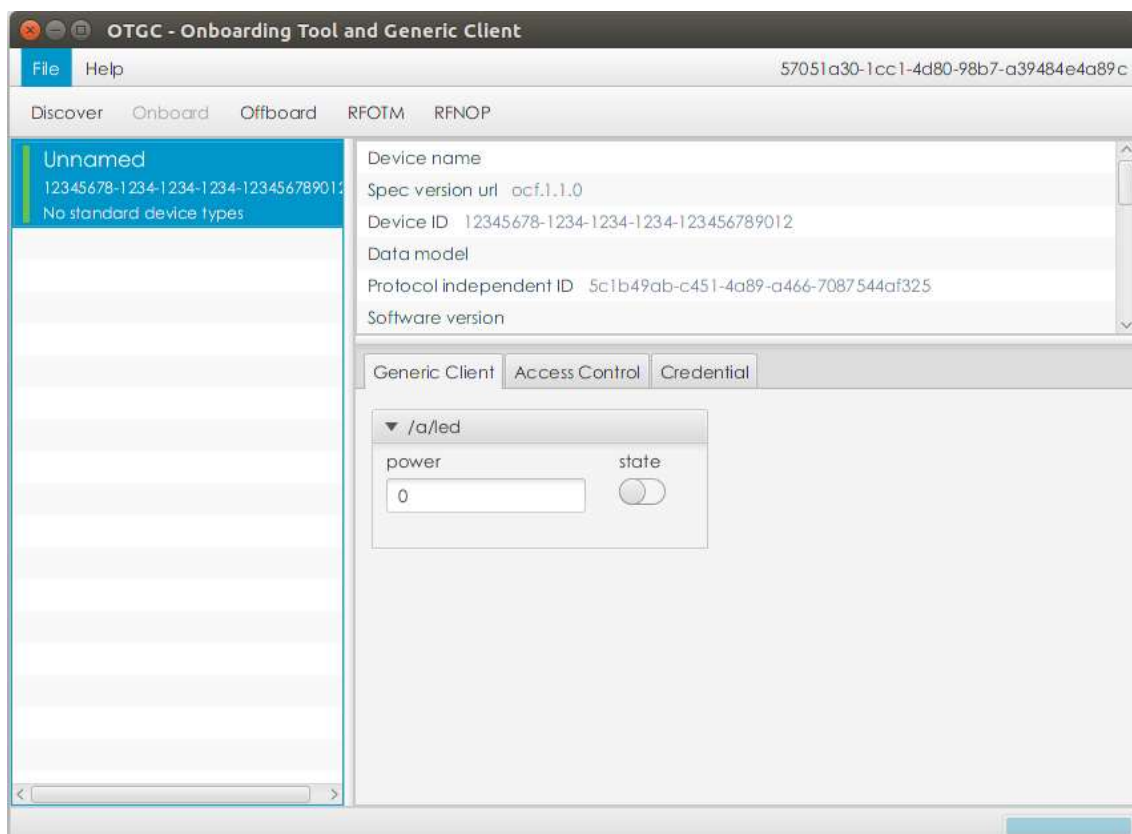


Figure 23: Device information and Generic Client, Linux.

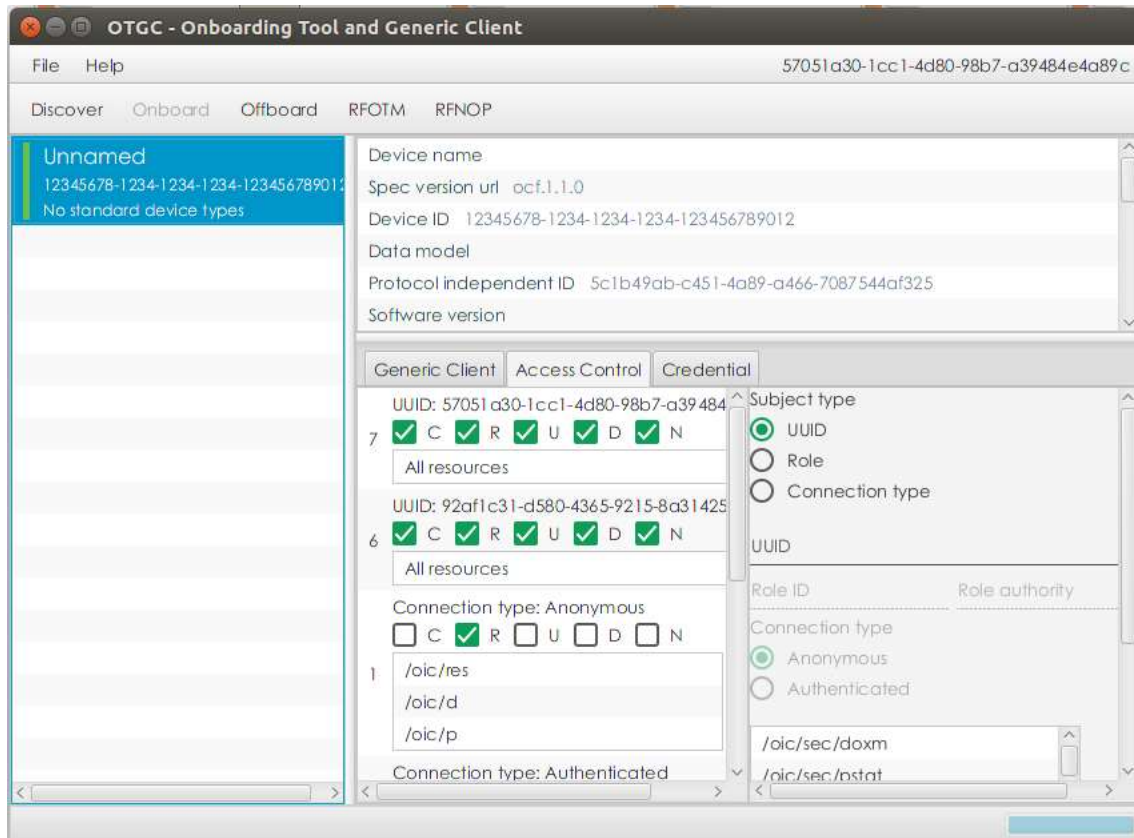


Figure 24: Access control, Linux.

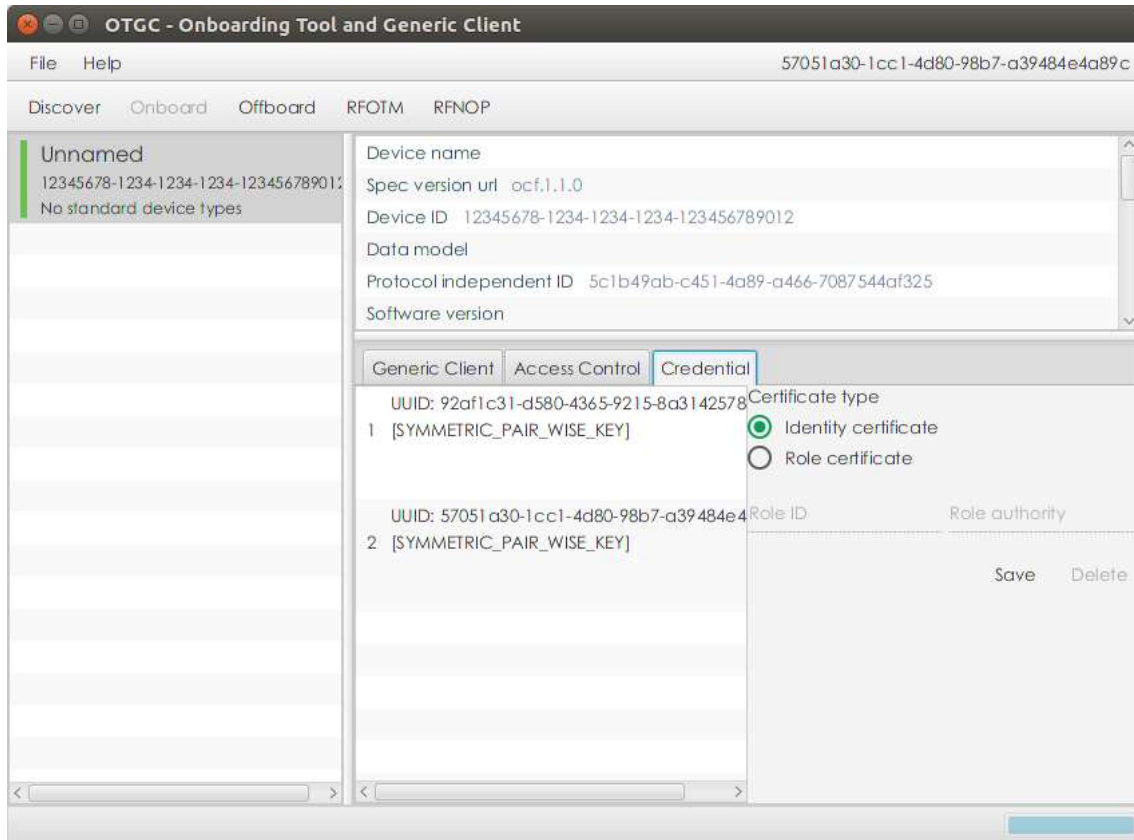


Figure 25: Credentials, Linux.

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

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

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

4.3.4 OFFBOARD A DEVICE

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

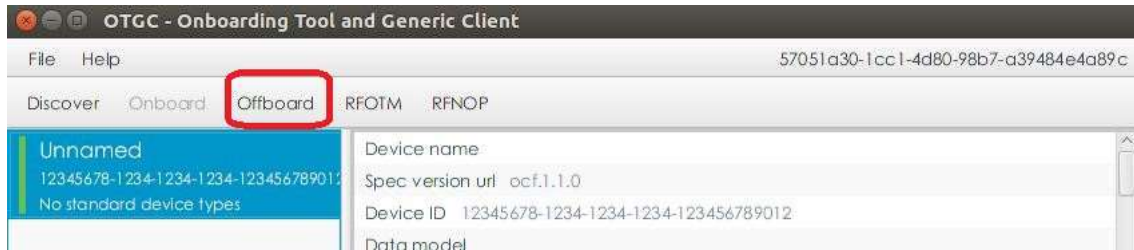


Figure 26: Offboard a device, Linux.

4.3.5 RESET OTGC

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

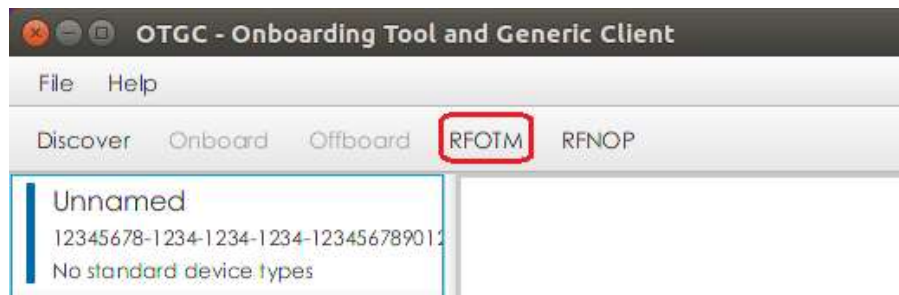


Figure 27: Reset OTGC, Linux.

4.3.6 OWNED OTGC BY SELF

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

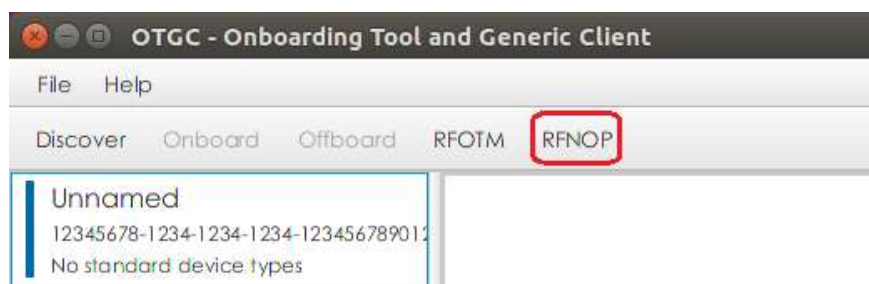


Figure 28: Self-own OTGC, Linux.

4.4 UWP

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 29 shows:

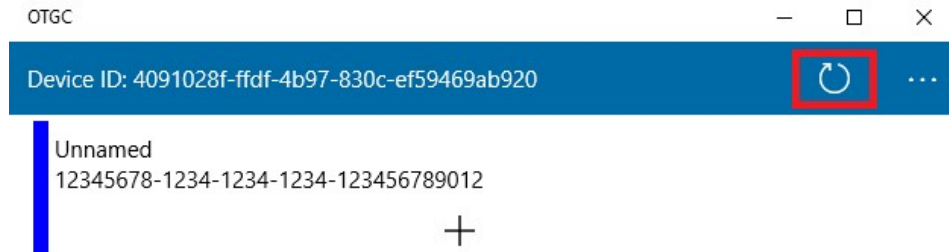


Figure 29: Scan devices, Windows 10.

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 30.

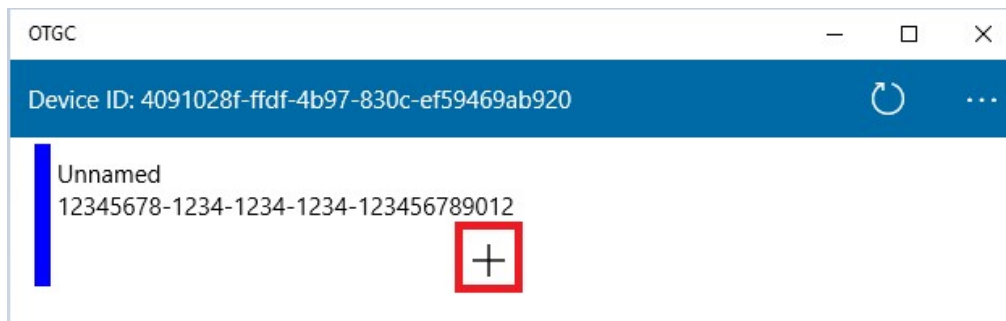


Figure 30: Onboard a device, Windows 10.

When a device is successfully onboarded, its state changes to owned-by-self(green) as shown in Figure 31.

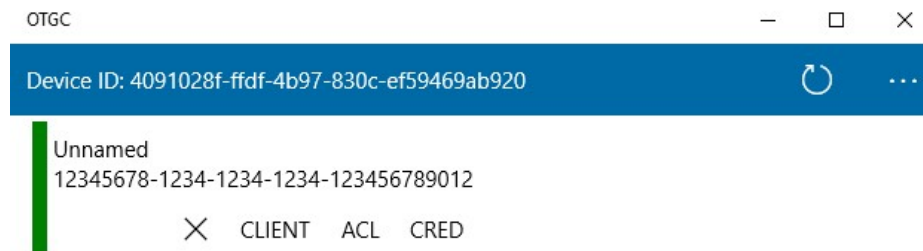


Figure 31: Owned-by-self device, Windows 10.

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 32 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 33 and Figure 34.

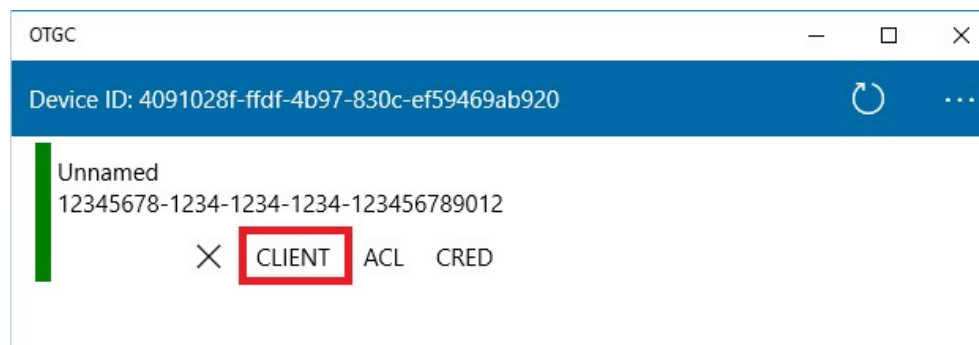


Figure 32: Generic Client button, Windows 10.

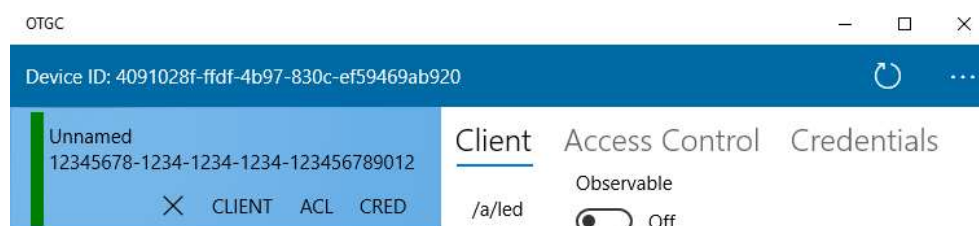


Figure 33: Generic Client tab, Windows 10.

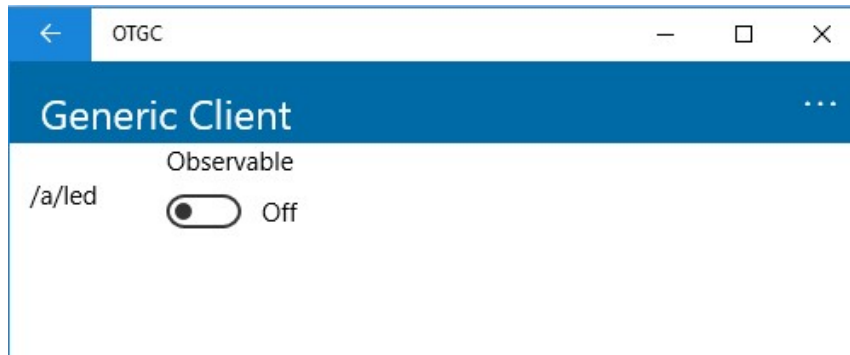


Figure 34: Generic Client screen, Windows 10.

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 35 shows, the OTGC shows the currently installed credentials, depending on the window size, in a new screen as shown in Figure 37 or in the “Credentials” tab at right of the device list as shown in Figure 36. A credential can be deleted pressing on the trash icon.

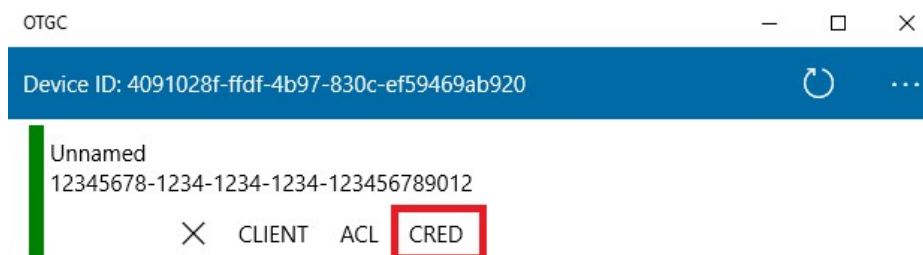


Figure 35: Credential button, Windows 10.

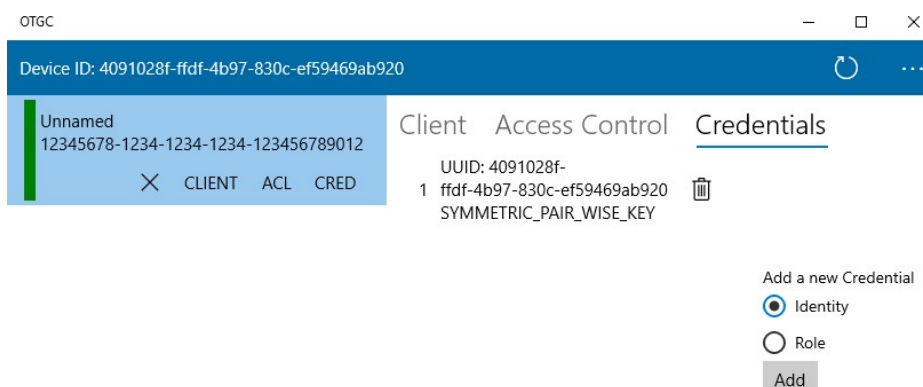


Figure 36: Credentials tab, Windows 10.

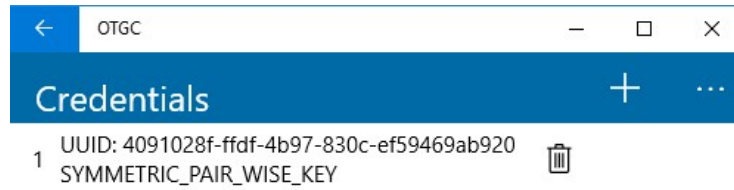


Figure 37: Credentials screen, Windows 10.

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 36. 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 38.

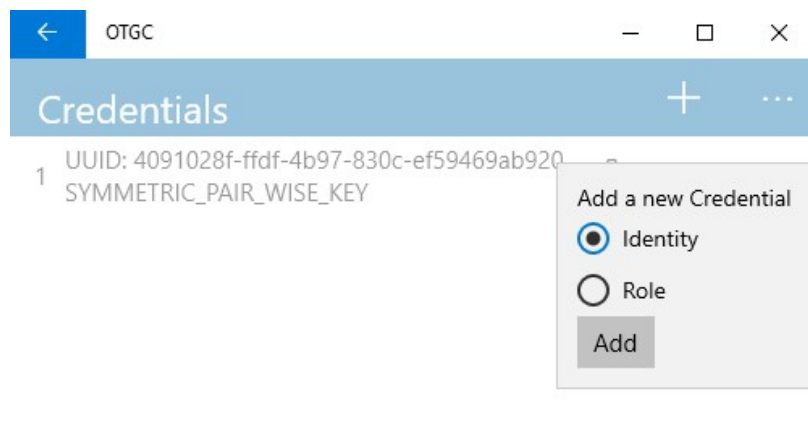


Figure 38: Add a new credential in Credentials screen, Windows 10.

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 39 shows, the OTGC will show the currently installed access control policies, depending on the window size, in a new screen (Figure 37) or in the “Access Control” tab at right of the device list (Figure 40). An access control policy can be deleted, pressing on the trash icon.



Figure 39: Access control list button, Windows 10.

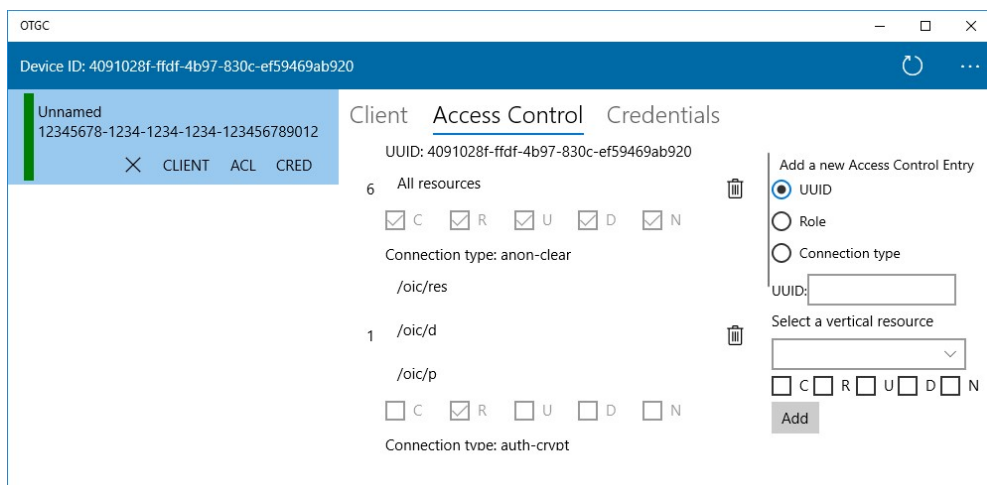


Figure 40: Access control tab, Windows 10.

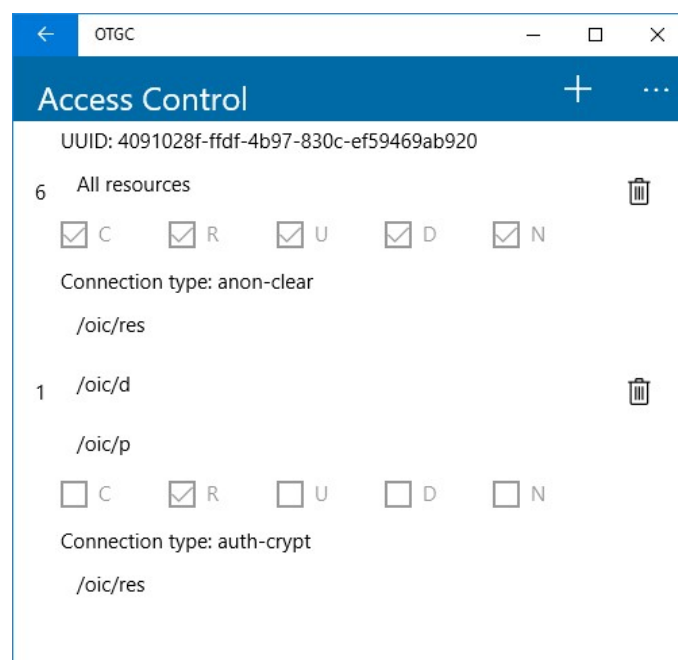


Figure 41: Access control screen, Windows 10.

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 40). 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 42).

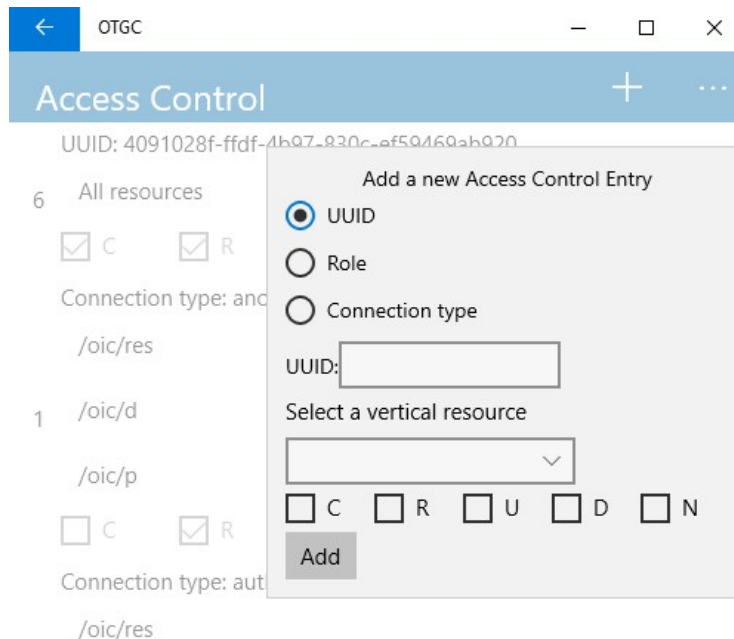


Figure 42: Add a new access control policy in Access Control screen, Windows 10.

4.4.6 OFFBOARD A DEVICE

An OCF device owned by the OTGC can be unowned by clicking on the “Cancel” icon, as shown in Figure 43. If the action succeeds, the device changes its state to unowned.



Figure 43: Offboard a device, Windows 10.

4.4.7 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 44.

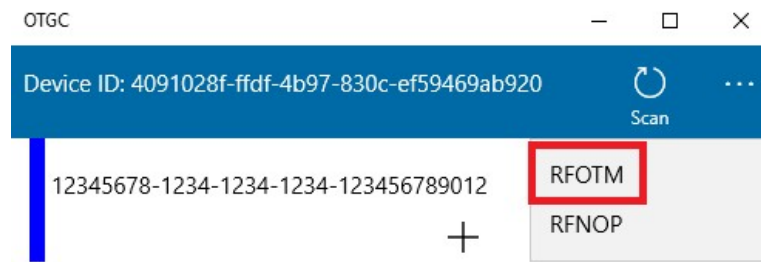


Figure 44: Reset OTGC, Windows 10.

4.4.8 OWNED OTGC BY SELF

To self-own the OTGC, click on the “RFNOP” button on the secondary options of the command bar as Figure 45 shows.

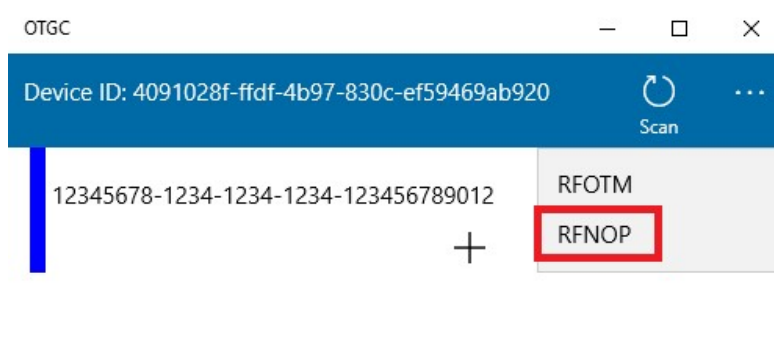


Figure 45: Self-own OTGC, Windows 10.

4.5 IOS

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.

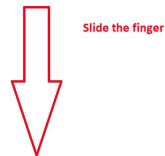


Figure 46: Empty devices list screen, iOS.

When scan finishes, OTGC will show a list with OCF devices similar to the Figure 47.

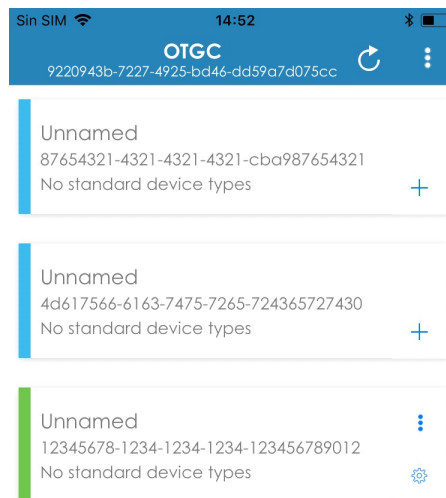


Figure 47: List with OCF devices detected, iOS.

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 48.

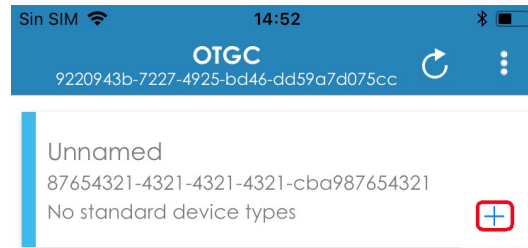


Figure 48: Onboard button, iOS.

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.

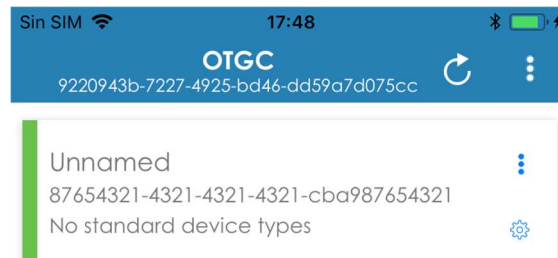


Figure 49: Owned-by-self device, iOS.

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.

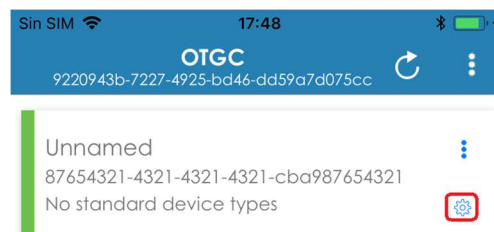


Figure 50: Generic Client button, iOS.

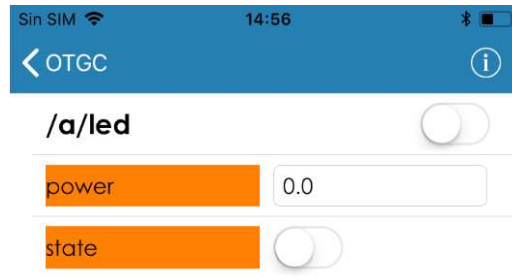


Figure 51: Resources in an OCF server, iOS.

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.

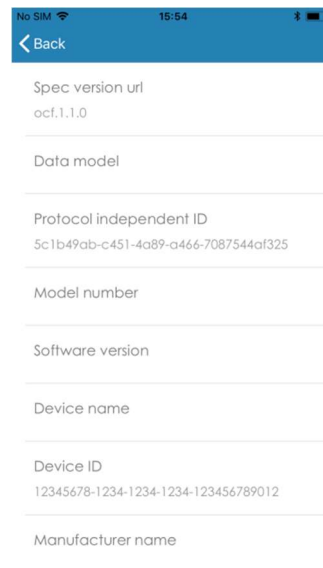


Figure 52: Device information panel, iOS.

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

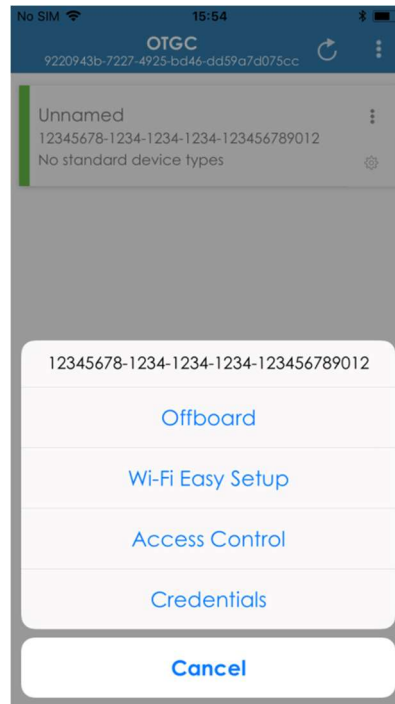


Figure 53: Credentials option, iOS.



Figure 54: 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 54 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 55 shows.



Figure 55: 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 57.

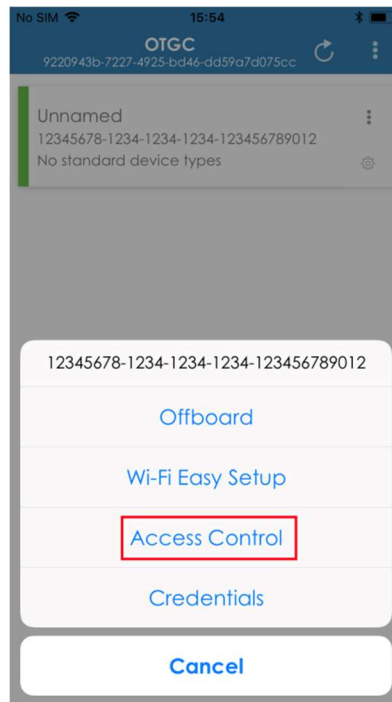


Figure 56: Access Control option, iOS.

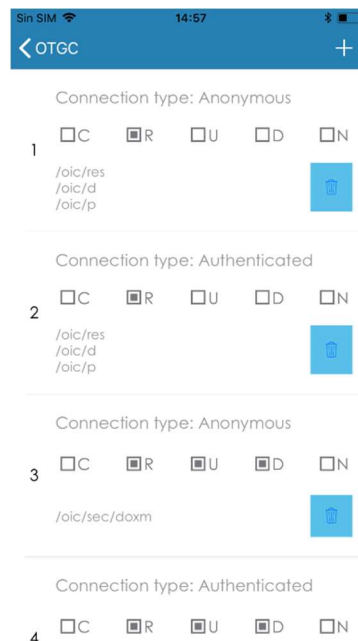


Figure 57: Access control list, iOS.

There are three types of access control policies that the OTGC 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 57 and a new screen appears with a form to fill (Figure 58). 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 58: 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 59. If the action succeeds, the device changes its state to unowned.

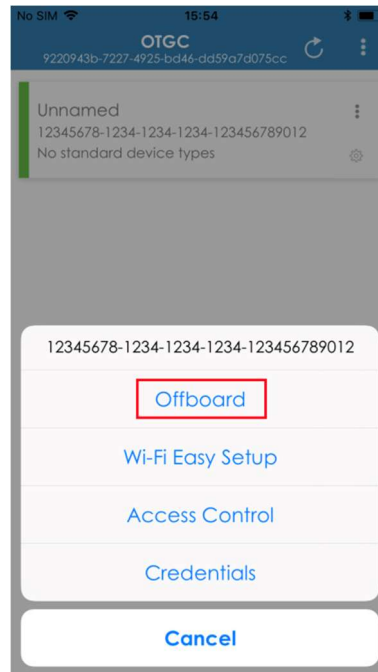


Figure 59: Offboard an owned device, iOS.

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 60).
4. Connect to the new network manually on your iPhone.
5. Introduce the configuration of the network the new connected (see Figure 61).
6. Scan the network to verify that the device has connected properly.

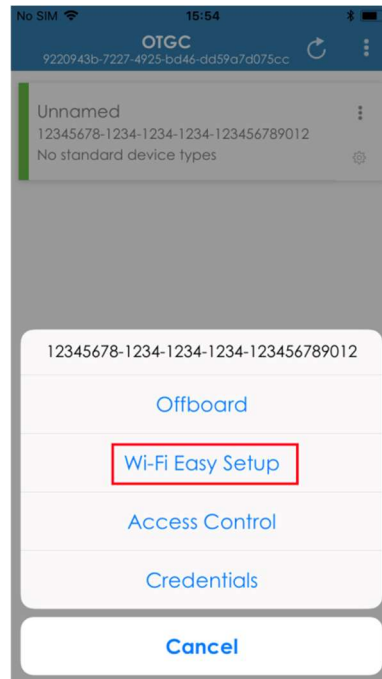
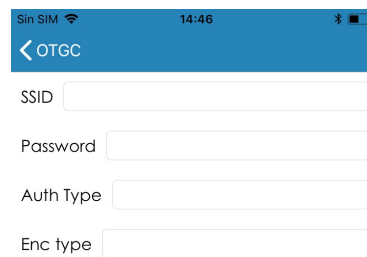


Figure 60: “Wi-Fi Easy Setup” option, iOS.



ok

Figure 61: 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 62 shows.

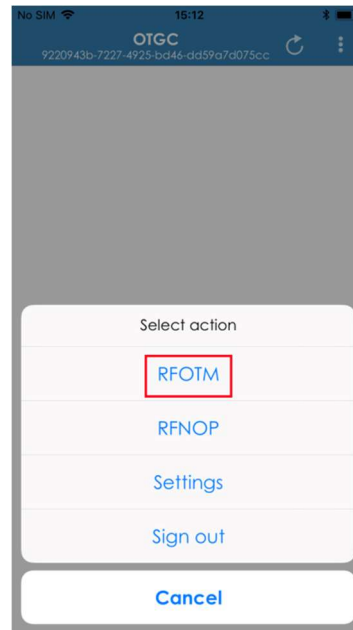


Figure 62: Reset OTGC, iOS.

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 63 shows.

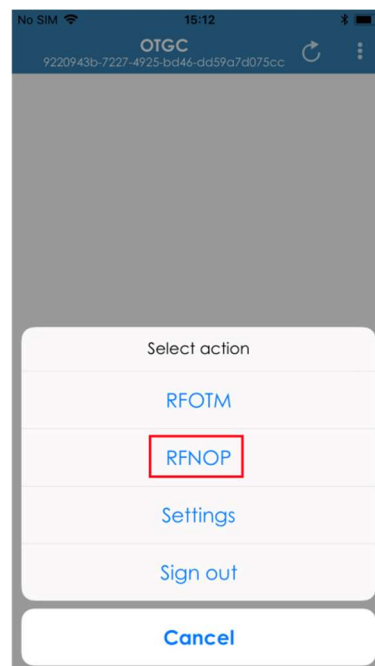


Figure 63: Self-own the OTGC, iOS.