# Manual of Reolink Open Platform v.1.0

## Overview

## Objective

To provide partners with an instruction to deploy Reolink Open Platform (ROP) and to configure and use the device.

## Applicability

The manual is suitable for people who have some experience in server development and deployment.

## Scope

The manual contains three parts: deployment of server, use of server, installation and use of device.

## Deployment of Server

## Hardware Requirements

- Minimum configuration for server host: dual-core CPU, 4GB RAM.

## Software Requirements

- Get the installation package rop.tgz provided by Reolink
- Use mainstream Linux distributions. The Debian distribution is recommended.
- Pre-install docker and docker-compose. You can refer to the content in this link.
- Prepare a domain name pointing to the server host IP. Or, configure a **permanent and unchanging** fixed IP address for the server.
- Ensure that the server's TCP ports 61008 and 61009 are open to clients
- Ensure that the server's TCP ports 61000-61007 are open to devices
- Ensure that the deployment is performed by a user with docker user group permissions.

# Assumptions

- We assume that our partners use the admin account to install ROP.
- We assume that the installation path of ROP is /home/admin/

# For First-Time Installation

## Installing Core Server (Required)

- Upload the installation package to the installation directory and unzip it.
  - Upload the rop.tgz package provided by Reolink to the installation directory /home/admin/.
  - Go to the installation path: cd /home/admin/.
  - Execute the command “tar -zxf rop.tgz” to extract the folder.
  - Enter the path of ROP: cd /home/admin/rop/.
- Set the ROP startup configuration environment variables, which are stored in the file “docker-compose.yml”.
  - The ROP_HOSTNAME should be the Core Server’s server domain name or unchanging fixed IP address. For example: www.rop.com.
  - RTSP_PLAY_URL_PREFIX is the prefix of the RTSP streaming URL. Because the RTSP streaming URL may be encrypted, a prefix is required when generating the address on the server side. The prefix includes three parts: protocol, server address, and port. For example, rtsp://www.rop.com:61008
  - ROP_ALARM_WEBHOOK is the address that ROP uses to request callback when a device generates an alarm, and the authentication is ensured by the address. For example, https://www.customer.server.com/alarm?key=Aa1zplGq4pySXEELHBSznbnwjqPbcHK4tl. If this feature is not needed, the field can be left blank.
- After modifying the ROP startup configuration, execute the command “docker-compose up -d” to start the container.

## Caution

- A self-signed root CA will be generated once the server is deployed. If the self-signed root CA is damaged, all devices will not be able to connect to the server. Therefore, it is recommended to back up the self-signed root CA. The path of the self-signed root CA is /home/admin/rop/data/certs/.
- There is important configuration information in the configuration file. It is recommended to back up the configuration file. The path of the configuration file is /home/admin/rop/data/config.json

# For ROP Code Update

For servers that have ROP and only need to update code.

## Overwriting the Code of Core Server

- Upload the installation package to the temporary directory (/home/admin/) and unzip it.
  - Upload rop.tgz package provided by Reolink to the installation directory: /home/admin/tmp/
  - Enter the temporary directory: cd/home/admin/tmp/
  - Execute the command “tar -zxf rop.tgz” to unzip the folder
  - Execute the command “rm -rf/home/admin/rop/app/” to delete the original code
  - Execute the command “cp -rf /home/admin/tmp/rop/app/ /home/admin/rop/app/” to copy new code to the running directory

## Restarting the Container

- Execute the command “docker restart rop-core-server” to restart it.

# Use of Server

# Functions of Core Server

| Function | Description | Prerequisites | Related Interfaces | Related Protocols | Note |
|---|---|---|---|---|---|
| Initializing the device | Initialize the device to ROP working mode. | 1. Device network is configured and connected. | **“Create the Device Initialization Session”** in “Interfaces” | HTTP/ HTTPS | |
| Getting/setting the device name | 1. Get the device name.<br>2. Set the device name. | 1. Device network is configured and connected.<br>2. Device is initialized. | 1. **“Get the Display Name of the Device”** in “Interfaces”<br>2. **“Set the Display Name of the Device”** in “Interfaces” | HTTP/ HTTPS | The acquired information has a validity period. The default validity period is 1 min, which can be changed in the configuration file. |

| Function | Description | Prerequisites | Related Interfaces | Related Protocols | Note |
|---|---|---|---|---|---|
| Getting (the status of)/ enabling/ disabling the device's alarm notification | 1. Get the status of the device's alarm notification.<br>2. Enable/ disable the device's alarm notification. | 1. Device network is configured and connected.<br>2. Device is initialized. | 1. **"Get the Status of the Device's Alarm Notification"** in "Interfaces"<br>2. **"Enable/Disable the Device's Alarm Notification"** in "Interfaces" | HTTP/ HTTPS | With the alarm notification on the device enabled, the ROP server will send a POST request to the set address once the device generates an alarm notification. For more details, see the "Interfaces" document. |
| Watching the live view of the device | Get the live view stream of the device and watch it via the player. | 1. Device network is configured and connected.<br>2. Device is initialized. | 1. **"Request the Live View Address"** in "Interfaces" | 1. Use HTTP/ HTTPS for signals<br><br>1. Use RTSP/ RTSPS for streams | 1. It is recommended to use TCP as the transmission protocol of RTSP. |
| Watching the playback of the device | 1. Get the device's list of recordings.<br>2. Get the stream of the device playback and watch it via the player. | 1. Device network is configured and connected.<br>2. Device is initialized. | 1. **"Get the Dates with Recordings in a Calendar Month"** in "Interfaces"<br>2. **"Get the List of Recordings of the Device in a Calendar Day"** in "Interfaces"<br>3. **"Request the Recording Playback Address"** in "Interfaces" | 1. Use HTTP/ HTTPS for signals<br><br>2. Use RTSP/ RTSPS for streams | 1. It is recommended to use TCP as the transmission protocol of RTSP. |

| Function | Description | Prerequisites | Related Interfaces | Related Protocols | Note |
|---|---|---|---|---|---|
| Device firmware update | Update the firmware version of the device. | 1. Upload the firmware file (suffix must be pak or paks) to /home/admin /rop/data/firmware<br>2. Device network is configured and connected.<br>3. Device is initialized. | 1. **"Create the Firmware Update Session"** in "Interfaces"<br>2. **"Get the Status of Firmware Update"** in "Interfaces" | HTTP/ HTTPS | |
| Get the real-time snapshot taken by the device | Get the real-time snapshot taken by the device | 1. Device network is configured and connected.<br>2. Device is initialized. | 1. **"Get the Real-Time Snapshot Taken by the Device"** in "Interfaces" | HTTP/ HTTPS | Cannot operate the offline devices |
| Get the real-time battery status of the device | Get the real-time battery status of the device | 1. Device network is configured and connected.<br>2. Device is initialized. | 1, **"Get the Real-Time Battery Status of the Device**" in "Interfaces" | HTTP/ HTTPS | Cannot operate the offline devices |
| Get/Set the PIR alarm notification configuration of the device | 1. Get the PIR alarm notification configuration of the device<br>2. Set the PIR alarm notification configuration of the device | 1. Device network is configured and connected.<br>2. Device is initialized. | 1. **"Get the PIR Alarm Notification Configuration of the Device**" in "Interfaces"<br>2. "**Set the PIR Alarm Notification Configuration of the Device**" in "Interfaces" | HTTP/ HTTPS | Cannot operate the offline devices |

| Function | Description | Prerequisites | Related Interfaces | Related Protocols | Note |
|---|---|---|---|---|---|
| Control the PTZ function of the device | 1. Set the magnification times for optical zoom of the device<br>2. Set the PTZ focal length of the device<br>3. Control the PTZ rotation function of the device | 1. Device network is configured and connected.<br>2. Device is initialized. | 1. "**Set the Magnification Times for Optical Zoom of the Device**" in "Interfaces"<br>2. "**Set the PTZ Focal Length of the Device**" in "Interfaces"<br>3. "**Control the PTZ Rotation Function of the Device**" in "Interfaces" | HTTP/ HTTPS | Cannot operate the offline devices |
| Get the list of online devices | Get the list of devices currently online | - | 1. **"Get the List of Online Devices"** in "Interfaces" | HTTP/ HTTPS | Cannot operate the offline devices |
| Get/set the WiFi configuration of the device | 1. Get the WiFi configuration of the device<br>2. Set the WiFi configuration of the device | 1. Device network is configured and connected.<br>2. Device is initialized.<br>3. Device supports WiFi. | 1. "**Get the WiFi configuration of the device**" in "Interfaces"<br>2. "**Set the WiFi configuration of the device**" in "Interfaces" | HTTP/ HTTPS | Cannot operate the offline devices |
| Start scanning the WiFi list on the device | Start scanning the WiFi list of the device | 1. Device network is configured and connected.<br>2. Device is initialized.<br>3. Device supports WiFi. | 1. "**Start scanning the WiFi list of the device**" in "Interfaces" | HTTP/ HTTPS | Cannot operate the offline devices |
| Get the WiFi list scanned on the device | Get the WiFi list scanned on the device | 1. Device network is configured and connected.<br>2. Device is initialized.<br>3. Device supports WiFi. | 1. "**Get the WiFi list scanned on the device**" in "Interfaces" | HTTP/ HTTPS | Cannot operate the offline devices |

| Function | Description | Prerequisites | Related Interfaces | Related Protocols | Note |
| --- | --- | --- | --- | --- | --- |
| Test the availability of WiFi | Test the availability of WiFi | 1. Device network is configured and connected.<br>2. Device is initialized.<br>3. Device supports WiFi. | 1. “**Test the availability of WiFi**” in “ Interfaces” | HTTP/ HTTPS | Cannot operate the offline devices |

# Important Configuration Items of Core Server

Configuration files are in JSON format and located in /home/admin/rop/data/config.json.

| Field | Path | Description | Type | Value Range | Note |
| --- | --- | --- | --- | --- | --- |
| serverHost | Under the root path | IP address or domain name of the server | String | Less than 255 bytes | If deployed to an IP address, it must be **a permanent and unchanging** fixed one. A domain name, instead of a fixed IP address, is strongly recommended. |
| playURLPrefix | Under the RTSP path | Prefix of the RTSP streaming address, containing protocol, domain name, and port number. Default: rtsp://${serverHost}:61008 | String | Less than 255 bytes | When using an encrypted connection, the prefix should be rtsps://${serverHost}: 61010 |

| Field | Path | Description | Type | Value Range | Note |
| --- | --- | --- | --- | --- | --- |
| encryptMode | Under the deviceStream path | Method of encrypting stream transmission between device and ROP. The available types are full encryption, selective encryption, and non-encryption. | String | “TLS”, “TCP”, or “encryptTCP” | |
| notificationURL | Under the alarm path | Alarm notification callback address | String | Less than 255 bytes | |
| deviceKeys | Under the deviceAuth path | Key pairs the device has used. | Map. Mapping from accessKey to secretAccessKey . | accessKey is a string of 16 bytes. SecretAccessKey is a string of 32 bytes. | Very important. Once lost, the battery-powered devices are not able to connect to the server. |
| currentKeyIndex | Under the deviceAuth path | The accessKey that all devices should currently use | String | A string of 16 bytes. | |
| signKey | Under the authCode path | Signature used to issue the initialization authorization code to the device | String | A string of 32 bytes. | Very important. Once lost, it will affect the device certificate refresh. |

# Server Ports

The default ports of ROP. Partners can modify the ports by themselves.

- Default Ports of Core Server

| Port | Use | Note |
| --- | --- | --- |
| 61000 | Used by the device to download the server’s self-signed root CA certificate | Used in device initialization |
| 61001 | Used by the device to get device certificate and certificate chain | Device certificate is used for device authentication |

| Port | Use | Note |
| --- | --- | --- |
| 61002 | Used by the device to register with the server and get the TCP encryption negotiation key | The obtained key is used to negotiate the encryption of the TCP connection |
| 61003 | To keep the connection with battery-powered devices alive | Used to keep the connection between battery-powered devices and server |
| 61005 | For TLS connection of signals | Used to transmit signals between server and device |
| 61006 | For TLS connection of streams | Used to send streams from device to client with full encryption. |
| 61007 | For TCP connection of streams | Used to send streams from device to client with selective encryption or non-encryption. |
| 61008 | For client's RTSP request | Used by client to obtain RTSP streams |
| 61009 | For client's HTTP request | Used for client's signal requests |

- Default Ports of Optional Components

| Port | Use | Note |
| --- | --- | --- |
| 61004 | For client's RTSPS request | Used to transmit RTSPS streams between client and server |
| 61010 | For client's HTTPS request | Used to transmit HTTPS signals between client and server |

# Optional Component Instructions - Client Gateway

The Client Gateway is implemented with Nginx.

- If Nginx is used for Client Gateway to secure the transmission between the Client and Core Server, the partners need to configure certificates and rotate them periodically.
- The partners can also use cipher suites from cloud service providers to secure the transmission between Client and Core Server. For example, using ELB from AWS for HTTP encryption.
- Example of using Nginx to configure HTTPS encryption.

```
server {
    listen       61010 ssl http2;
    server_name  amazon-us-east-1a.stream.reolink.com;

    ssl_certificate      /data/certs/fullchain.pem;
    ssl_certificate_key  /data/certs/key.pem;

    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_ciphers ECDHE-RSA-AES256-SHA384:AES256-
SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM;
    ssl_prefer_server_ciphers on;
    ssl_session_timeout 10m;
    sendfile on;

    location / {

        proxy_pass http://127.0.0.1:61009;
    }

}
```

- Example of using Nginx to configure RTSPS encryption

```
upstream rtsp_server {
    server 127.0.0.1:61008;
}

server{
    listen 61010 ssl;
    ssl_certificate      /data/certs/fullchain.pem;
    ssl_certificate_key   /data/certs/key.pem;
    tcp_nodelay on;
    ssl_session_cache off;
    ssl_session_timeout  10m;
    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_ciphers  HIGH:!aNULL:!MD5;
    ssl_prefer_server_ciphers  on;
    proxy_pass rtsp_server;
}
```

# Optional Component Instructions - Authenticator

Use Nginx to enable HTTP basic authentication.

- Example of using Nginx to configure Authentication.

```
  {
     location / {
          auth_basic             "ROP";
          auth_basic_user_file  conf/htpasswd;
     }
}
```

- Refer to the content in this link for details about how to generate htpasswd files.
- Header Authorization needs to be added in the client request when using the Authenticator provided by Reolink. Refer to content in this link for details

# Cross-Domain Configuration Instructions

If the partner uses a webpage to connect to the ROP server, it is necessary to solve the cross-domain problem. The Core Server does not provide cross-domain support.

- It is recommended to set up cross-domain configuration in the Client Gateway. Reolink provides an example of using Nginx for Cross-Domain Configuration.

```
{
    location / {
            add_header 'Access-Control-Allow-Origin' $http_origin always;
            add_header 'Access-Control-Allow-Headers'
'Authorization,Accept,Origin,Keep-Alive,User-Agent,X-Requested-With,
If-Modified-Since,Cache-Control,Content-Type,Content-Range,Range' always;
            add_header 'Access-Control-Allow-Methods'
'GET,POST,OPTIONS,PUT,DELETE,PATCH' always;
            if ($request_method = 'OPTIONS') {
                add_header 'Access-Control-Allow-Origin' $http_origin always;
                add_header 'Access-Control-Allow-Headers'
'Authorization,Accept,Origin,Keep-Alive,User-Agent,X-Requested-With,
If-Modified-Since,Cache-Control,Content-Type,Content-Range,Range' always;
                add_header 'Access-Control-Allow-Methods'
'GET,POST,OPTIONS,PUT,DELETE,PATCH' always;
                add_header 'Access-Control-Max-Age' 172800;
                add_header 'Content-Type' 'text/plain charset=UTF-8';
                add_header 'Content-Length' 0;
                return 204;
            }
            proxy_pass http://127.0.0.1:61009;
        }
}
```

## Caution

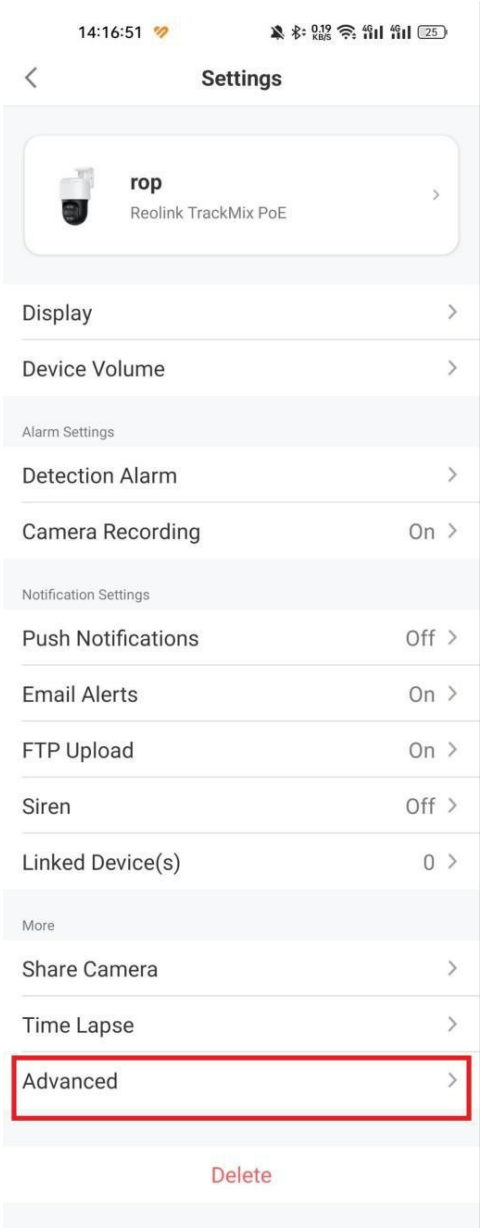
- The certificates for optional components (/data/certs/fullchain.pem and /data/certs/key.pem) need to be downloaded and maintained by partners themselves.

## Instructions on device initialization and configuration

Upgrade device to ROP version
Unzip Firmware.tgz provided by Reolink and find the .pak or .paks file, which is the firmware used for ROP.
For a power camera, please see the guide on the Reolink website for upgrade via Reolink Client on your PC:
https://support.reolink.com/hc/en-s/Articles/900004550323-how-to-Upgrade-FIRMWARE-VIA-Reolink-Client-New-Client-//
For a battery-powered camera, please see the guide on the Reolink website for upgrade with an SD card:
https://support.reolink.com/hc/en-us/articles/15038092365465-Howto-Manually-Upgrade-Firmware-for-Reolink-WiFi-Battery-Powered-Cameras-/

Device initialization and ROP configuration

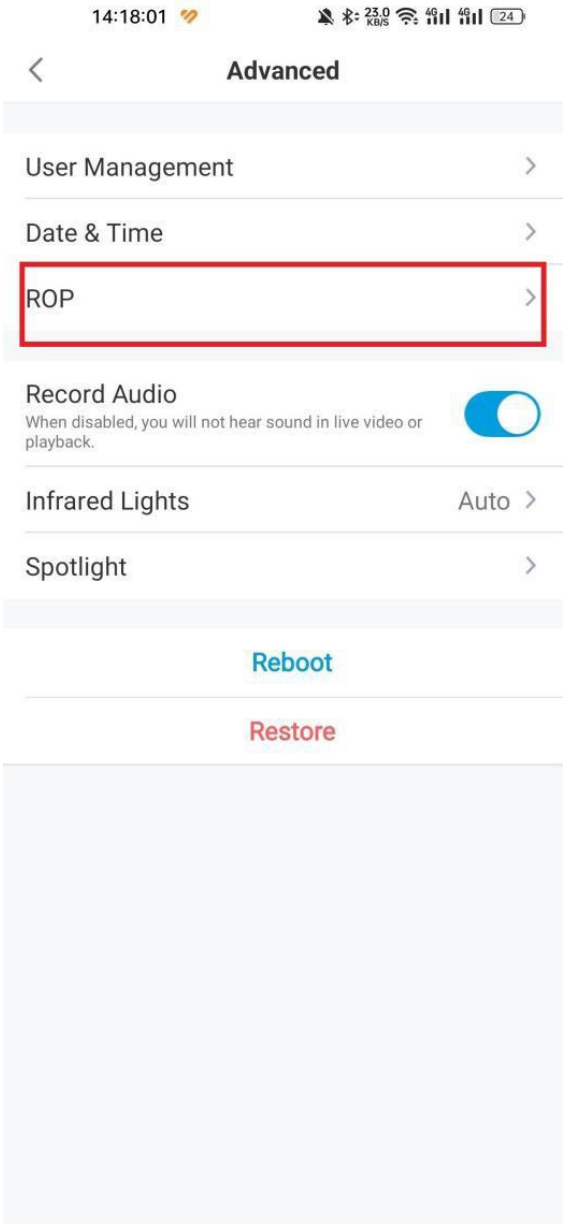
- Camera supports network cable
  For details, see **Manual of Reolink Open Platform v.1.0 - ROP Configuration via LAN**
- Camera supports WiFi only
  STEP 1: Configure WiFi (to be updated)
  STEP 2: Configure ROP via LAN. For details, see **Manual of Reolink Open Platform v.1.0 - ROP Configuration via LAN**
- Camera supports 4G only
  Install the app provided by Reolink for configuring ROP, **app-Reolink-4.36.0.4.20230331.apk**
  Set up the camera using the Reolink app. For details, see https://support.reolink.com/hc/en-us/articles/360012300954/
  After the device is added and connected, go to the Remote Configuration page and select **Advanced**, as shown below.



Generate QR code for ROP configuration

Obtain the device initialization information using the **Create device initialization session** interface included in Reolink Open Platform v1.0. Generate a QR code with the device initialization information for ROP configuration. Note: The QR code is valid for 1 minute. If an expired QR code is used, the app will return “failure”.

Select ROP on the app and scan the QR code.



Caution:

The camera firmware and Reolink app are ROP-specific. ROP configuration is not supported for other versions.

After ROP is configured for the camera, change to the ROP mode. Reolink app cannot be connected to the device.

The camera must be connected to the server, which requires that the server use a public IP or be in the same LAN as the camera. For 4G devices, the ROP server must be deployed on a public network.