Introduction to Reolink Open Platform v.1.0

Glossary

Term	Description	Note
ROP	Reolink Open Platform	“ROP” is an acronym for “Reolink Open Platform”
Partner	Customers using ROP.	-
Device	Cameras or other products produced by Reolink.	These products are integrated with Reolink Open Platform protocols.
Client	Servers, webpages, or mobile apps that use ROP interfaces.	Reolink is not responsible for the development and implementation of customers’ clients. Our customers will develop and maintain their clients.
UID	The unique ID of the device, consisting of uppercase letters and numbers.	The unique ID of the device produced by Reolink.
Core Server	Core service functional component of ROP.	Functions provided by ROP’s core modules.
Optional Component	Non-core service functional components of ROP.	Not required. Partners can choose to install or not.
Client Gateway	Gateways for clients. Non-core service functional components of ROP.	Nginx can be used for the gateway.
Authenticator	Gateways for authentication. Non-core service functional components of ROP.	Reolink provides a demo of authenticator. Partners can install it according to scenarios or install it after modification.

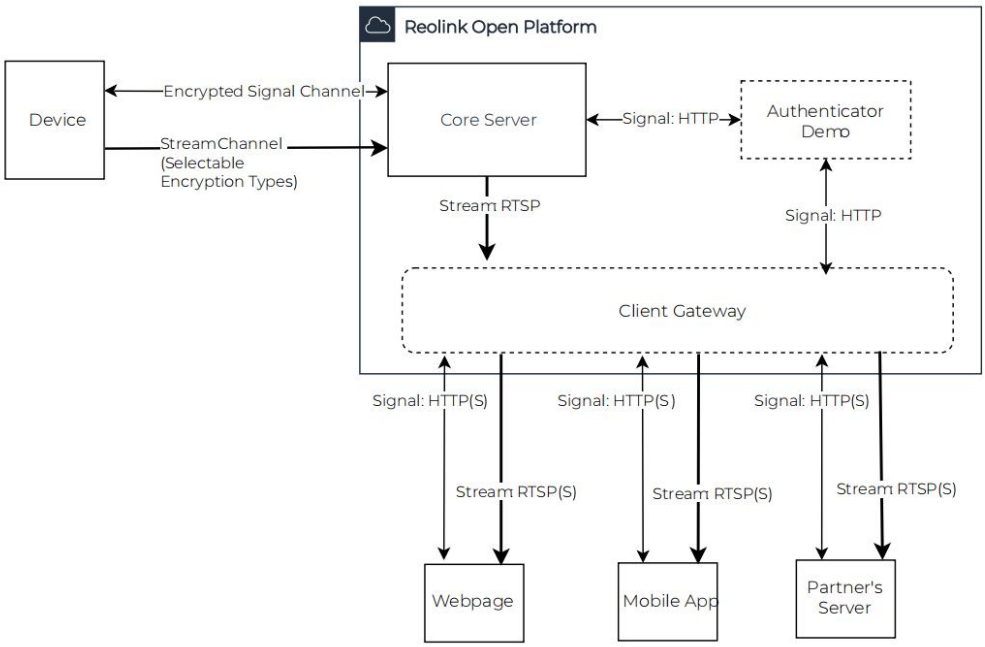
Objective

- The project aims at facilitating Reolink partners’ redesign of the devices.

Overview

- The document is provided to Reolink partners who intend to redesign Reolink devices. All server-side codes of ROP is completely open source. The source codes can be provided to our partners free of charge.

Block Diagram of the System



Device

> "Device" refers to products connected to ROP, including battery cameras, wired cameras, and NVRs.

Transmission Protocols Between Device and Core Server

- TLS is used to transmit signals.
- There are three types of encryption in transmitting streams. TLS is used for full encryption. TCP is used for non-encryption and selective encryption.

Why not use TLS for stream transmission all the time?

- Using TLS all the time requires high performance of Device. Most devices cannot support live view in clear mode and playback in clear mode at the same time.
- Using TLS all the time requires high performance of Core Server. If there are many devices viewing the streams at the same time, using TLS will lead to a significantly high server load.
- The selectively encrypted TCP designed by Reolink encrypts only a portion of the critical information. Even when the attacker eavesdrops the stream transmission, recovery of the data will be difficult. Using selective encryption will greatly reduce the stress of the device and the server.

Cases of Stream Encryption

Encryption of Stream Transmission to ROP	**Description**	**Transport Protocol**	**Note**

Full Encryption	All streams transmitted to ROP are fully encrypted	TLS	-
Selective encryption	All streams sent to ROP are selectively encrypted	Selectively encrypted TCP designed by Reolink	An intermediate solution. Its demand on device performance is similar to non-encryption. Eavesdroppers are not able to recover the stream properly.
Non-Encryption	All streams transmitted to ROP are not encrypted	TCP	Not recommended, unless devices and ROP are deployed on a LAN and there is no risk of eavesdropping.

Core Server

Core Server is the core component of ROP. The Core Server is provided, developed, and maintained by Reolink.

Function List

For the specific information of interfaces and the full list of features, refer to “Interfaces of Reolink Open Platform v.1.0.”

Transport Protocols Provided by Core Server

Two cases:

- Using the RTSP plaintext protocol to transmit streams
- Using the HTTP plaintext protocol to transmit signals

Why doesn’t the Core Server provide client-side encryption?

- If the partner accesses ROP through a server or client on the same LAN as ROP, encryption will be optional. In this situation, Core Server provides only the basic functions.

Caution

- The Core Server must be deployed on a server with a fixed domain name or a fixed IP address.

The device can only be connected to the Core Server when the domain name or IP address is configured properly. Once the Core Server’s domain name or IP address is changed, all devices connected to it need to be reconfigured.

About Alarm Notifications

When the device generates an alarm notification, the notification will be pushed to Core Server, and the Core Server will push the alarm notification to the Client.

Prerequisites of using alarm notifications:

- The device’s alarm notification function is disabled by default. The function needs to be enabled manually.
- Partners need to provide a callback address used after the device generates an alarm notification. Refer to “Interfaces of Reolink Open Platform v.1.0” for details.

Authenticator

Authenticator is optional. It is not a required component of ROP. Partners can choose to install it or not according to their needs. Reolink will provide the simplest Authenticator Demo for reference. Our partners can modify the codes based on their needs. This referential demo provided by Reolink can only be used for the simplest authentication and cannot defend against high-level attacks.

- When to Use the Authenticator?

Core Server does not provide any authentication for accessing clients. If the Client and the Core Server are not on the same LAN, authentication for the clients is necessary. However, the authenticator provided by Reolink is very simple and can only defend against the simplest and the lowest-level attacks. To defend against high-level attacks,

our partners need to modify our Authenticator Demo or deploy other authenticators according to the scenarios.

- Transport Protocols Between Authenticator and Core Server

  HTTP is used to transmit data between the Authenticator and the Core Server. The streaming address is generated and authenticated by the Core Server.

Client Gateway

Client Gateway is optional. It is not a required component of ROP. Partners can choose to install it or not according to their needs. Nginx can be used as the client's encryption gateway. If the Client and the Core Server are not on the same LAN, encrypted data transmission between the Client and ROP is necessary.

- When to Use Client Gateway?

  The core server does not provide encryption. If the Client and the Core Server are not on the same LAN, using TLS for data transmission between the Client and ROP is necessary. The Client Gateway provided by Reolink is for reference only. The partners can use the cipher suites from their cloud service providers. For example, using ELB from AWS for HTTP encryption.

- Transport Protocols Between Client Gateway and Core Sever

  There are two cases: using the RTSP plaintext protocol to transmit streams, and using the HTTP plaintext protocol to transmit signals.

- Transport Protocols Between Client Gateway and Authenticator (If Any)

  Using the HTTP plaintext protocol to transmit data.

In general, if the Client and the Core Server are not on the same LAN, deployment of both Authenticator and Client Gateway is recommended to ensure security.

Client

Clients are able to access ROP. A Client can be the partner's own server, or a mobile app or webpage. Clients need to access ROP by interfaces. For specific information on interfaces, refer to "Interfaces of Reolink Open Platform v.1.0."

Types of Clients

Clients can be divided in two ways: clients with or without encrypted transmission, and clients requiring or not requiring authentication.

Type of Client	Prerequisite	Transmission Protocols	Application Scenario	Comment	Note

With encrypted transmission; Requiring authentication.	1. Client Gateway deployed; 2. Authenticator deployed.	Transmission protocols between Client and Client Gateway: 1. RTSPS for streams; 2.HTTPS for signals	Client and Core Server are not deployed on the same LAN.	Recommended	This type of Clients are usually mobile apps or webpages.
Without encrypted transmission; Not requiring authentication.	1. Client Gateway not deployed; 2. Authenticator not deployed.	Client and Core Server are connected directly without using Client Gateway. Transmission protocols between Client and Core Server: 1.RTSP for streams; 2.HTTP for signals	Client and Core Server are deployed on the same LAN.	Recommended	This type of Clients are usually servers built by partners.
With encrypted transmission; Not requiring authentication.	1.Client Gateway deployed; 2. Authenticator not deployed.	Transmission protocols between Client and Client Gateway: 1. RTSPS for streams; 2.HTTPS for signals	-	Not recommended	-
Without encrypted transmission; Requiring authentication.	1.Client Gateway not deployed; 2. Authenticator deployed.	1.Client and Authenticator are connected directly. Use HTTP to transmit signals between Client and Authenticator; 2. Client and Core Server are directly connected. Use RTSP to transmit streams between Client and Core Server.	-	Not recommended	-

Constraints

Development/runtime environment

- Runtime environment: Linux 64-bit machine. Dual-core CPU 4GB RAM. The Debian distribution is recommended.
- Programming Language: typescript, Node.js

Performance

- A single server supports 10,000 devices staying online at the same time and watching 30 video streams in clear mode at the same time. The statistics are for reference only, the actual performance may vary according to the server's hardware.

Features of the Future Versions

Features that are not available in the v.1.0 version but may be added in future versions.

- Load balancing of ROP.

Security Design

Security design involves transmission security and authentication.

Transmission Security

Transmission security is mainly ensured by TLS.

Transmission Security Between Device and Core Server

- Transmission between the Device and the Core Server is mainly encrypted by TLS. The server certificate needs to be configured for the Core Server. If our partners do not have applicable certificates, they can refer to the "Manual of Reolink Open Platform v.1.0" and find the method of generating server certificates by self-signed certificate authority (CA).

Transmission Security Between Client and ROP

- If the Client and ROP are deployed on the same LAN, the level of transmission security can be lowered depending on the scenario. Plaintext transmission can be used in this situation.
- If the Client and ROP are not deployed on the same LAN, TLS encryption is recommended for transmission. If our partners do not have applicable certificates, they can refer to the "Manual of Reolink Open Platform v.1.0" and find the method of generating server certificates by self-signed certificate authority (CA).

Alarm Notification Pushed from Core Server to Client

- HTTPS is recommended for the callback address of push notifications.

Authentication

Authentication is based on the security in transmission. Without guaranteed transmission security, authentication will not have much meaning.

Core Server's Authentication of Device

In its initialization, the device will load the device certificate issued by the server and use it to establish a secure mutually authenticated TLS connection with the server.

ROP's Authentication of Client

Use the optional component Authenticator to authenticate the Client. Referring to the simple Authenticator Demo provided by Reolink, our partners can make Authenticator by themselves.

Alarm Notification Pushed from Core Server to Client

Authentication is not required in the process because the callback address is configured by partners. The address does not need to be published.

Authentication of Streaming Address

The streaming address is generated and authenticated by the Core Server.

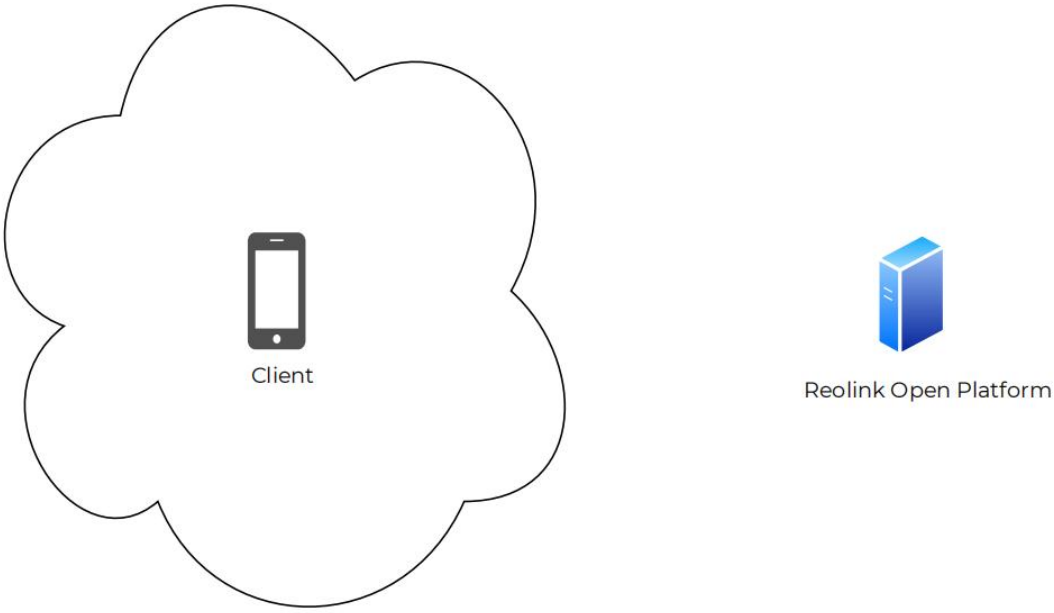
Deployment

ROP, Device, and Client can be deployed on the same LAN or on different networks.

Caution

- All deployment methods require a domain name or a fixed IP address of the server where ROP is deployed.
- If our partners do not have server certificates, they can refer to the **"Manual of Reolink Open Platform v.1.0"** and find the method of generating server certificates by self-signed certificate authority (CA).

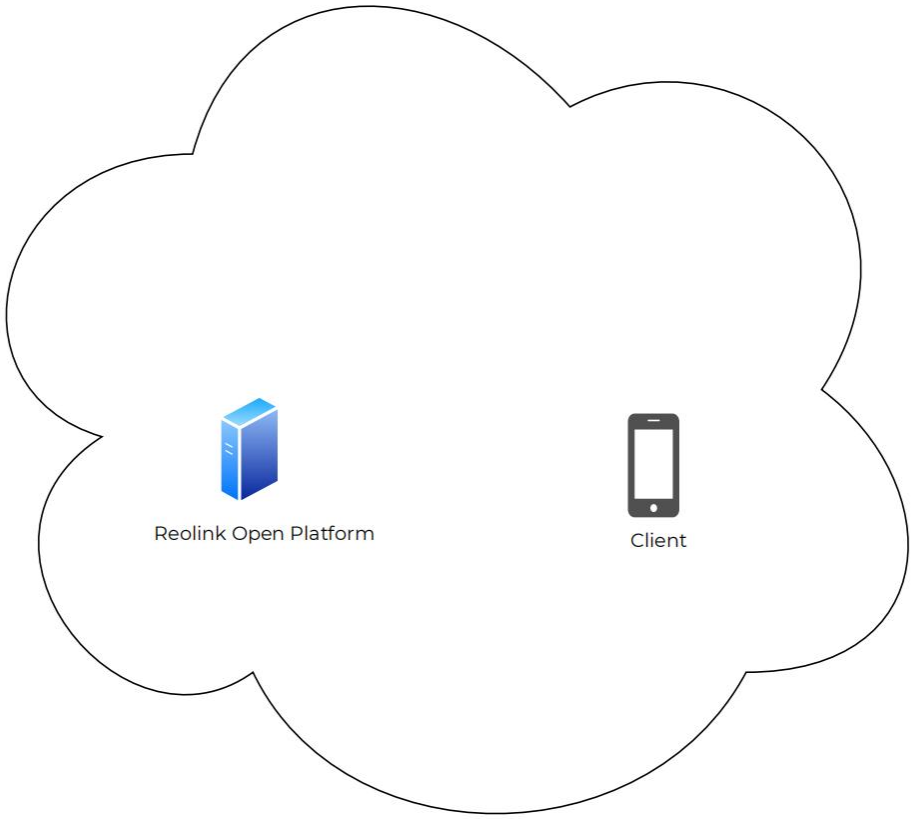
Deployment by Scenarios



- Application Scenarios

  Client and ROP are on different networks.

- Caution
  - It is recommended not to expose the Client request ports of the Core Server to the public network directly. Deployment of Client Gateway is recommended for forwarding the Client's requests for signals and streams and encrypting data transmission. Deployment of the authenticator is also recommended.



- Application Scenario
  - Clients and ROP are on the same network.

- Caution
  - Do not expose the Client request ports for signals and streams of the Core Server to the public network. They should only be used on LAN.