Yealink

YMCS Security Solution

White Paper

Dec.2018

Introduction

Yealink Management Cloud Service (YMCS), as a real-time, online, unified and graphical management platform provided by Yealink for the enterprises to use Yealink devices, can help the enterprises to redirect, deploy, manage, analyze, monitor devices and so on. YMCS adopts multiple security plans, such as the protocol security, the data encryption, and the data disaster discovery, to guarantee the security.

Protocol Security

YMCS uses TLS security protocol, mutual TLS authentication and so on. After powered on, the phone will send RPS request which uses HTTPS protocol and need mutual authentication, and succeed in access only with the certificate authenticated by Yealink, so that it can avoid illegal access. With DM access permission, the phone can establish the persistent connection with the management platform. After the successful SSL handshake with the platform, the phone can be connected to the platform and the follow-up operations will be performed. As a private protocol designed by Yealink, the interactive protocol used by the persistent connection, can guarantee the data transmission security and prevent the malicious behavior such as intercepting and decoding.

Data Encryption

The data in the database, such as the user information and the password, is all encrypted. At the same time, the data is also encrypted during the transmission because we use the persistent connection.

Data Disaster Discovery

The database uses mongodb, and the two-cluster deployment plan, with one in China and the other one in America, can ensure disaster discovery effectively. The data of the cluster will be synced at regular time.

Permission Control

For the limited times of failing to logging into YMCS, we provide security limitation methods, for example, freezing the enterprise.

Distributed Deployment of the Server and the Database

The database and the server use two clusters, which are described as below:

- Shanghai, China: 3 database servers and 3 business servers
- Virginia, America: 3 database servers and 3 business servers

QOE

The call quality will be recorded in the platform, and you can view the quality of the current call. The recorded information includes: the user information (such as the account information and the site), the device information (such as the device name and the MAC address), the call-related information (such as the caller and the call type) and so on.
All these information is reported via the persistent connection and will not be intercepted.

Phone Configuration Information

The phone configuration information, such as the account information and the password, is all encrypted and pushed to the phone via the persistent connection, which can ensure the transmission

security.

The diagnostic Function

The diagnostic function can be used only with the user authentication. The diagnostic information, such as the screenshot, the recording files, the packets, and the device log, is reported via the persistent connection, which can ensure the transmission security. The data will be saved in the disk but they will be cleaned up at regular time, for example, the log is only available in 7 days, or the packets and the screenshot are deleted after viewing.