Yealink

Yealink Management Cloud Service Security White Paper

Version 38.5.0.0 | May 2022

Contents

Introduction

Security is always the most critical consideration for all Yealink products and services.

To improve the security posture of our products, we invite third-party security organizations to do a thorough security vulnerability scanning and penetration testing on all devices on a regular basis. Our security team also focuses on security concerns and offers a hot patch or release a new version to address them.

This white paper describes security-related practices regarding Yealink Management Cloud Service ("YMCS") and includes information about how these practices are applied to the design, development, testing and improvement. It also describes the security features and access controls in Yealink's processing of personally identifiable information or personal data ("personal data") and customer data in connection with the running of YMCS, as well as the location and transfer of personal and other customer data.

This White Paper supplements the YMCS Privacy Policy and Yealink uses such data in a manner consistent with the YMCS Privacy Policy and this White Paper (as may be updated from time to time).

This white paper will be updated from time to time, and the latest version of this paper will be available on Yealink's website.

Product Design Security

Yealink follows Security by Design principles throughout our product creation and delivery lifecycle which includes considerations for confidentiality, integrity (data and systems) and availability. These extend to all systems that Yealink uses – both on-premises and in the cloud as well as to the development, delivery and support of Yealink products, cloud services and managed services.

The foundational principles which serve as the basis of Yealink's security practices include:

1. Security is required, necessary and foremost
2. Product full lifecycle design security
3. Data security, especially personal data security
4. Security testing and validation
5. Adherence to operational security and compliance audits

Product Basic Security

Physical Security

YMCS is hosted in the Amazon Cloud. For physical security, see AWS security documentation.

Application Security

Identity authentication

YMCS supports a strong password policy, which the password should include 6 to 32 characters with both numbers and letters (special characters are optional), to ensure account security. In addition, when users use the default password to log in, they must modify the default password. Otherwise, they cannot use YMCS.

Protection against malicious injections

YMCS has limits on the data format for all the input boxes, for example, the length and the characters, to avoid constructing SQL statements directly through the input boxes. Furthermore, executable commands are prohibited.

File and resource security

YMCS restricts the size and the format of the uploaded files, to avoid maliciously uploading large files and illegal executable files. Additionally, YMCS restricts the directory of the uploaded files to avoid modifying the storage directory of the server

from the front end. What's more, only the templates provided by YMCS are supported.

Protection against protocol attacks

A private protocol and TLS are used between the device and YMCS to encrypt transmission. Therefore, attackers are unable to obtain and forge protocol information to establish communication with the server.

Web Access Security

YMCS allows you to set the expiration time for the web session to prevent illegal operations by non-authenticated users. If the session timed out, the user needs to log in again. Besides, YMCS sets verification code for further verification if the user enters the wrong passwords for 5 times. What's more, YMCS transmits the login username and passwords with HTTPS.

Device Connection Security

The connection between phone and YMCS uses TLS 1.2 and a custom TCP. Only through TLS 1.2 mutual authentication can the phone be connected to YMCS.

When the phone and YMCS perform mutual authentication, YMCS verifies the legitimacy of the phone based on the phone's certificate (only a Yealink self-signed certificate can pass the verification) and MAC (the MAC of each phone is unique). At the same time, the phone verifies the certificate sent by YMCS to determine whether it is YMCS.

After the phone is connected to YMCS, the requests between them are authenticated by HTTPS and the data are transmitted by TLS 1.2.

API Security

Third-party applications need to apply for the AccessKey and the SecretKey if they want to access YMCS.

YMCS supports the anti-replay mechanism to avoid data packet spoofing, and it also uses the HTTPS to secure the access.

Data Security

Data Processing

When you are the Enterprise User, the Yealink Management Cloud Service collects and processes YMCS registration information and data related to the provisioning, configuration, and management of the devices supported by your enterprise including:

- **Account information** (includes the email address, company name, country or region, contact name, and contact email address that you provided when you registered with YMCS)
- **Data related to the provisioning, configuration, and management of the devices supported by your enterprise including:**

• Site names, descriptions, and locations
• Site device counts
• Device information, logs
• Device configuration files, resource files
• Device software updates
• Call quality statistics (not including call content)

When you are a Channel, the Yealink Management Cloud Service collects and processes data including:

- **Account information** (includes the email address, company name, country or region, contact name, and contact email address that you provided when you registered with YMCS)
- **Device data** (includes information such as type of device, device name and installed software version)
- **Configuration data**
- **Order data**

If someone is an individual user and the decision to use YMCS has been made by their employer as the customer, all the privacy information relating to personal data in this white paper is subject to their employer's privacy policies as controller of such personal data.

Purpose of Processing

The primary purposes of processing information by the Yealink Management Cloud Service for Enterprise User are to:

- Authenticate and authorize administrative access to services
- Provide device management cloud services
- Performing analysis to improve technical performance of the service
- Responding to customer support requests

The primary purposes of processing information by the Yealink Management Cloud Service for Channel are to:

- Service for customers
- Diagnose technical problems
- Performing analysis to improve the technical performance of the service
- Respond to customer support requests

Storage Security

The Yealink Management Cloud Service is hosted in Amazon Web Services (AWS) with data centres located in Virginia, USA and Frankfurt, Germany. YMCS operations will store data separately in accordance with local legal and regulatory requirements. In addition, Yealink has implemented technical and physical controls, such as "data fencing", to prevent unauthorized access or disclosure of customer content and to ensure data security and user privacy.

When YMCS receives the user data, the user data is verified and stored in the data center mentioned above, which uses mongodb with secure access control and data encryption policies. Yealink database is behind a fully-patched firewall, and the access to any service not requires by YMCS is blocked.

Besides, the data is regularly backed up and stored. Backups are also stored with encryption. We have systems, procedures, and policies in place to prevent unauthorized access to customer data and content by Yealink employees.

Data Access Security

Data access among enterprises, channels, and the enterprise administrator accounts is isolated from each other.

Data isolation between enterprises

Data between enterprises is isolated and inaccessible mutually.

YMCS gives the data of every enterprise a unique marker, which is used for identifying the owner of the data. This unique marker is in the token, which the enterprise can get by successfully logging in to YMCS. When an enterprise sends a request for accessing the data to YMCS, this token should be brought, so YMCS can verify whether the token is legal and read the unique marker in the token, and then return the corresponding enterprise data.

Data isolation between enterprises and channels

Data between channels and enterprises is also isolated and inaccessible mutually.

The channel creates the enterprise account. However, without enterprise permission, the channel has no access to the enterprise platform and the enterprise data. Only when the enterprise authorizes the channel to manage the devices for him, can the channel log in to the enterprise platform and have full permissions.

Data isolation between the enterprise administrator accounts

The enterprise accounts are divided into the administrator and the sub-administrator accounts.

The administrator creates the sub-administrator accounts. He can divide the sub-administrator accounts according to the site and assign the function and data permissions to the sub-administrator accounts. Besides, the administrator can delete the sub-administrator accounts and modify the assigned function and data permissions.

The sub-administrator account can only add, delete, and modify the device under the site he can manage. The sub-administrator can only use the assigned function and data permissions.

Transmission Security

The access to YMCS uses HTTPS and is encrypted by ECDHE-RSA-AES256-GCM-SHA512.

All communication in YMCS web portal is over a standard secure SSL connection, which encrypts all requests and responses. Besides, all connections to YMCS are encrypted with TLS 1.2 to secure the data transmission.

Yealink ensures that the data between the device and YMCS is encrypted through long connection protocols based on SSL and TLS, which can prevent malicious attacks and data tampering to ensure data security. The keys of the certificates used in Long Connection Protocol is also stored with encryption, which can effectively prevent the key from being used illegally if it is stolen. Moreover, sensitive data is transferred with TLS_RSA_WITH_AES_128_CBC_SHA encryption.

Data Deletion and Retention

All information collected from the customer is stored in the database and configured with access control mechanisms. Nothing is transferred outside of the Yealink Management Cloud Service servers. All data is self-contained in a database in the data center.

Yealink may retain customer data for as long as needed to provide the customer with any Yealink cloud services for which they have subscribed and for product improvement purposes. When a customer makes a request for deletion to privacy@yealink.com, Yealink will review and delete the requested data within seven (7) days, unless the data is required to be retained to provide the service to customer.

When deleting the enterprise or the channel accounts, all data information under the account including the connected devices, the account information, the sub-account information, and others are simultaneously destroyed. No data of the enterprise and channel accounts will be retained.

For audit requirements, YMCS may retain log records regarding user activity, but such data and log records will be retained for no longer than the maximum period

necessary for the user to authorize us to process them or to comply with applicable data protection regulations.

Privacy Data Processing Authorization

In compliance with applicable laws and regulations, YMCS provides users with a comprehensive privacy policy that explains what information we collect, how we store and protect the information, and how users can exercise his or her data rights. The Privacy Policy requires authorization from the user and can be easily found and accessed when the user logs in and uses YMCS. YMCS cannot and will not collect user information without authorization.

Operation Security

Operation Norms

Yealink has a professional team to provide remote server monitoring 24 hours a day, 7 days a week.

Inspecting the online business regularly, automatically, and manually, YMCS can find the abnormal issues, and then promptly inform technicians to solve it.

Beside, Yealink also organizes project review, code inspection, vulnerability detection, and virus cleaning regularly.

Access and Audit

YMCS is hosted in the Amazon Cloud. To access the production server of YMCS, Yealink has the following limitations. First, only authorized staff members with proper access permissions can access the production server. Second, only the IP address within the Yealink domain can be used to access the production server. Third, only when you pass the authentication of the fortress machine can you log in to the production server via SSH finally.

Besides, the system records operation and maintenance logs for later audits if required.

Security Incident Response

Yealink classifies security incidents and adopts different solutions. From the stage of occurrence, processing, analysis, and review, Yealink conducts closed-loop management and continuous improvements for enhancing the ability to respond to the security incidents and keeping the system stable.

When a security event occurs, the related log and information are collected, and an expert group is established.

In the stage of processing, the expert group makes temporary solutions and assists the later improvements.

In the stage of analysis, Yealink reviews the process of how the security incident occurs, analyzes the problem from all aspects, and improves it in the later version.

In the stage of review, we will summary the root cause and improve the mechanism of controlling beforehand and detecting in the process.

Security Test

Both static and dynamic vulnerability scanning as well as penetration testing are regularly performed for production releases and against our internal corporate network by both internal and external test teams. Yealink maintains a partnership with NetSPI Group, a leading international security penetration testing organization, to regularly perform security penetration tests on a wide range of our products.

Security Certification

YMCS strictly complies with the requirements of the EU General Data Protection Regulation ("GDPR") and has received certification from TÜV Rheinland, a leading international third-party inspection, testing and certification organization.

YMCS-GDPR Certificate.pdf

About Yealink

Yealink (Stock Code: 300628) is a global brand that specializes in video conferencing, voice communications and collaboration solutions with best-in-class quality, innovative technology and user-friendly experience. As one of the best providers in more than 140 countries and regions, Yealink ranks No.1 in the global market share of SIP phone shipments (Global IP Desktop Phone Growth Excellence Leadership Award Report, Frost & Sullivan, 2019).

Copyright

Technical Support

Visit Yealink WIKI (http://support.yealink.com/) for firmware downloads, product documents, FAQ, and more. For better service, we sincerely recommend you to use Yealink Ticketing system (https://ticket.yealink.com) to submit all your technical issues.

YEALINK(XIAMEN) NETWORK TECHNOLOGY CO.,LTD.
Web: www.yealink.com
Addr: No.1 Ling-Xia North Road, High Tech Park,
Huli District, Xiamen, Fujian, P.R.C