Yealink Management Cloud Service Security White Paper

Introduction

Yealink Management Cloud Service (YMCS) is a cloud-based solution that simplifies the management of Yealink devices by remotely controlling and managing devices to meet the specific needs of regions, user groups or device models. Devices will be automatically deployed upon a network connection, resulting in cost savings, improved efficiency, and simplified troubleshooting. YMCS is designed with security in mind, and security is always the most critical consideration for all of Yealink's products and services.

This white paper presents information about the security-related practices of Yealink Managed Cloud Services (YMCS), including how to apply these practices to design, development, testing, and improvement. It also describes YMCS's security features and access controls when processing personally identifiable information or personal data ("Personal Data") and customer data related to the operation of YMCS, as well as the location and transmission of Personal Data 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.

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

Security Team

Yealink has established an information management steering committee, a security leadership group, and a confidentiality group, with designated information security officers at various levels within each group, each responsible for specific roles and responsibilities. Please email to security@yealink.com.

Compliance and Certification

Yealink places great importance on the safety and compliance of its products and actively aligns with the compliance requirements of leading international

standards. Currently, YMCS has obtained several certifications, including SOC 2 TYPE 2, Rheinland GDPR COMPLIANCE, and ISO/IEC 27001:2013.

At the same time, Yealink invites independent third-party professional security testing organizations to conduct regular vulnerability scans and penetration tests on YMCS. In the process of continuous digging and repairing, the security protection system of the whole system is enhanced.

SOC 2 TYPE 2

The American Institute of Certified Public Accountants (AICPA) Service Organization Controls (SOC) 2 reports are an independent examination of the suitability of design and operating effectiveness of a service organization's controls relevant to security, availability, processing integrity, confidentiality, or privacy.

Yealink's SOC 2 report provides independent attestation on the suitability of design effectiveness of the controls relevant to the security, availability, and privacy of Yealink Management Cloud Service (YMCS) and Yealink Device Management Platform (YDMP).

GDPR COMPLIANCE

The General Data Protection Regulation (GDPR) has been known as the world's toughest privacy and security law. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU.

Yealink complies with current EU data protection regulations and has completed an independent GDPR compliance assessment, demonstrating our industry-leading level of data protection and privacy safeguards.

ISO/IEC 27001:2013

The International Organization for Standardization 27001 Standard (ISO 27001) is the world's best-known standard for implementing an Information Security Management System (ISMS) and specifies best practices to manage, monitor, review, and continuously improve an organization's ISMS. Certification is performed by an independent third-party auditor and provides assurance that certain security controls are in place and operating effectively.

Yealink's latest ISO 27001:2013 certification, which was issued on July 28, 2022, covers the following Yealink products: DECT phone, Video phone, SIP phone, conference phone, conference TV terminal system, headset and accessories. This accreditation certifies that Yealink has implemented best-practice information security processes.

PENETRATION TEST BY INDEPENDENT LEADING LABS

Static and dynamic vulnerability scans and penetration tests are performed by internal and external testing teams on production versions and on our internal corporate network on a regular basis. Yealink maintains a partnership with NetSPI Group, a leading international security penetration testing organization, to regularly conduct security penetration tests on our various products.

Secure Development Process

The development process of YMCS fully follows the Software Security Development Life Cycle (S-SDLC), which covers security activities in all phases of design, development, testing and maintenance. The core concept is to drive relevant personnel to bring security awareness/activities into the entire development life cycle, clarify the collaboration between various parties involved in the project development process, and continuously build enterprise-level software security development capabilities.

Requirement design: During the requirement design phase, we thoroughly assess the security aspects involved according to industry security certification standards, to avoid significant design risks. User privacy implications will be evaluated at each release so that the product design meets the product privacy policy and data processing security.

Development phase: Developers in the R&D center use IDE security plug-ins to integrate and develop code based on change requests, and detect security items in real time during development. Integrated into GitLab, SonarQube enables automatic code scanning to audit the quality of modified code. It helps reduce the risks associated with security vulnerabilities, quality defects, and code security flaws by performing SCA (Software Composition Analysis) open source component scanning and SAST (Static Application Security Testing) static source code scanning. If any exceptions are found when scanning codes, developers will immediately modify the code. Developers then upload the scanned code to GitLab and submit the code integration request in GitLab. Code can only be included in the program code after it has been approved by a designated reviewer. The code submitter and the code reviewer are not the same person. The developer packages and uploads the merged program code to the image repository. Once the code is uploaded to the image repository, it can no longer be modified.

Test verification: The test engineers retrieve the code package of the to-be-released version from the image repository and perform functional testing in the testing environment using test cases. Additionally, they utilize DAST scanners such as AWVS and Nessus for dynamic application security testing and manual penetration testing to uncover vulnerabilities within the application. Furthermore, they conduct periodic reviews and training sessions on product vulnerabilities to establish a security knowledge base. Test engineers will send test results back to

the R&D center and product department via email. If they find defects during testing, they will report them to developers to fix the defects. If they don't, the product manager will conduct user acceptance testing and submit the results and deployment comments to the testing and the product departments. After the test passes, the test engineer initiates the deployment request, which specifies the change rollback plan, and the project director makes the final approval.

Online evaluation: Each version release undergoes a rigorous evaluation process to ensure compliance with environment, application, and online security requirements. The criteria for formal online deployment are determined based on system-level security conditions. Once deployment approval is granted, the implementation engineer in charge of operations and maintenance submits the deployment application and carries out the change deployment upon approval from the operations and maintenance project leader.

Maintenance phase: Once deployed, the image undergoes regular scanning and timely patching. In the formal environment, operations and maintenance personnel continuously monitor product security using security devices like WAF, XDR, and others. They respond promptly to any detected attacks and establish a vulnerability management system to address and fix external vulnerabilities reported in a timely manner.

Yealink has established a standardized change management process to ensure that all changes to YMCS are documented, tested, security assessed, change impact analyzed, and approved prior to implementation into the production environment. The change process is divided into eight steps: change request, change requirement survey, change proposal, change review, change proposal preparation, change proposal confirmation, change proposal implementation, and change delivery. Each version change requires a personal information impact assessment, and if applicable, affected customers are notified of the change.

Privacy Data Processing

Privacy Policy

Yealink has established the Information Security System Compilation, which outlines the company's commitment to legally collecting and handling personal information and providing clear information to the data subjects. The handling of personal information is conducted in accordance with the data subject's consent and the agreements in place. The privacy team oversees and reviews the handling of personal information, and the privacy policy is regularly updated and published.

Yealink has established a privacy protection plan, which regulates the processes of privacy risk identification, data compliance management, system measure

assessment, system security assessment, information governance, and supervision and investigation.

Yealink has established a privacy policy, which specifies the information collection scenarios, collection methods, categories of information, purposes of use, as well as access, update, storage, disposal, transmission and disclosure of personal information. And in order to ensure the authenticity, accuracy and completeness of the user information obtained by Yealink, Yealink expressly states that customers must guarantee the accuracy of the user information they submit.

In the privacy policy, Yealink specifies the feedback channels for customers' complaints about personal information or privacy. Yealink's privacy team will promptly investigate to determine if unfair or illegal practices have been committed.

Yealink has implemented a privacy team consisting of legal, audit and product-related personnel to oversee compliance with Yealink's privacy policies and procedures. The privacy team is responsible for assessing customer privacy concerns and complaints, determining if urgent reporting or remedial action is necessary, and directly communicating with customers by providing solutions for their concerns and complaints.

The privacy officer reviews relevant privacy laws and regulations semi-annually, updates policies for compliance, and ensures that the definition of "sensitive" personal information is correctly delineated and communicated to personnel. In turn, legal counsel reviews the privacy policy issued by Yealink at least once a year to ensure its consistency with internal policies and applicable laws and regulations. When the privacy policy changes, Yealink will notify the customer by email, and the customer can continue to use the service only after confirming the updated privacy policy. Customers can check and read the latest Privacy Policy and trace its historical version on the website.

To ensure that user information is collected with the express consent of the relevant customer, the customer must agree to and confirm acceptance of the Yealink Service Agreement and Privacy Policy when logging in to the Yealink platform for the first time.

Privacy Compliance Assessment

In terms of business compliance, Yealink has established a regular assessment mechanism for privacy data compliance and provides personnel with up-to-date training, including defining what personal information is and what personal information is considered sensitive.

Yealink has created a manual customer data inventory to maintain customer data, including classifications based on confidentiality and sensitivity. The privacy team reviews the customer data inventory semi-annually to ensure the legality

and compliance of the data collected. Semi-annually, the person responsible for privacy reviews the information collection process and examines internal and external notification procedures. For any new personal information collected, the privacy team shall meet and discuss the effectiveness of the Privacy Policy. Through these control activities, Yealink verifies that the collection procedures, storage and use of personal information comply with the privacy protection requirements.

The actual controller of YMCS user data is the customer, not Yealink. Yealink processes user data in compliance with the law, and only uses it as an actual customer to provide relevant functions and data display, and does not obtain any personally sensitive information.

The telemetry data transmitted by endpoints comprises essential equipment information required for equipment operation and maintenance management, and it does not contain any personal or sensitive information. The decision to connect to the YMCS and transmit this data is entirely up to the endpoint users themselves.

Web Portal Security

Web Access Security

1. Web transmission security

YMCS services are transmitted via HTTPS and use TLS V1.2 to encrypt the entire transmission channel to ensure channel security;

2. Web authentication anti-brute force

When users access the YMCS, they need to enter valid account and password information. The web requires graphical verification when some failed attempts occur. The account will be locked if the number of failed attempts exceed the limit;

3. Anti-SQL injection, XSS scripting attacks

YMCS's web service employs regular monitoring and multiple layers of validation to counter SQL injection and XSS script attacks. Also, YMCS has strict format restrictions for file uploads to avoid importing executable programs;

4. Network session timeout mechanism

YMCS supports the use of session expiration time to prevent unauthorized actions by non-authenticated users. If the session times out, the user needs to log in again;

Identification

1. Password policy

To ensure account security, YMCS supports a strong password policy, which requires a password length of 8 to 32 characters and must include at least three of the following: digits, uppercase letters, lowercase letters, and symbols (excluding spaces). In addition, when users use the default password to log in, they must modify the default password. Otherwise, they cannot use YMCS.

2. Multi-factor authentication

YMCS provides multi-factor authentication, which requires two-step authentication (email verification code or Google Authenticator) to ensure login security.

3. SSO

Users can also log in to YMCS using Microsoft credentials (Azure Active Directory), providing OAuth 2.0-based single sign-on technology (SSO), multi-factor authentication, and conditional access. This helps prevent cybersecurity attacks and offers users a convenient and compliant solution.

Device and Cloud Connectivity Security

Device Connection Security

The premise that the device is connected to the YMCS is that the enterprise administrator has carried out active deployment behavior for the device; otherwise the device will not actively report telemetry data to the YMCS;

Users have the option to manually configure the device to allow or prohibit connection with YMCS through the device user interface or device manager interface. Additionally, the features provided by YMCS can be individually set to allowed or prompt, giving end users full control over security settings.

- Authorization features of the phone device to the YMCS include allowing/disallowing: platform connection, screenshot, packet capture, and QoE reporting;
- Authorization features for the room devices to YMCS include allowing/disallowing: platform connection, screenshot, and remote desktop.

The connection between the phone and YMCS is encrypted using HTTPS authentication and TLS 1.2 transport. Only with mutual authentication using TLS 1.2, the phone can establish a connection with YMCS. During the mutual

authentication between the phone and YMCS, YMCS verifies the device's identity through device certificates and device identity authentication policies, ensuring a secure device connection.

Transmission and Encryption

All information transmission on YMCS is encrypted. YMCS utilizes TLS 1.2 or higher with a robust cipher suite to transmit signals, ensuring that all transport links are encrypted once a session is established over TLS.

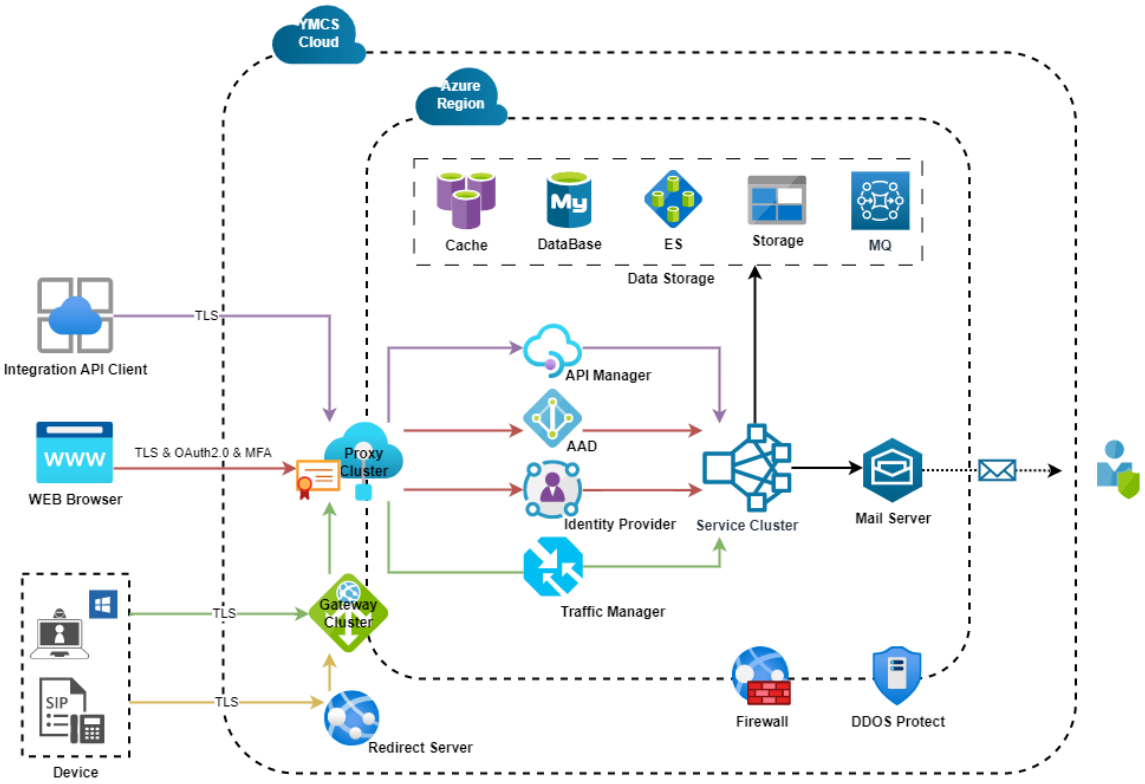
Data exchanged between the device and YMCS is encrypted to safeguard against malicious attacks and data tampering, thus ensuring data security. The default configuration between the device and server enables TLS certificate mutual authentication, as well as dual-factor security authentication for device identity.

The server's certificate private key is securely stored in encrypted form to prevent theft and unauthorized use of the key.

List of encryption protocols supported by the platform:

- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Data Transmission between the Device and the Cloud



Data Security

Yealink has established the following system requirements to ensure data security:

- Information classification and classification management procedures: These procedures establish standardized criteria for classifying information assets and provide guidelines for identifying, protecting, and handling information at different stages of the information asset lifecycle.
- Information Security and Confidentiality System: This system defines the scope of confidential data and outlines requirements for classifying, identifying, and implementing confidentiality controls for data. It also specifies measures to address illegal disposal of data.
- Compilation of information security system: This system outlines management requirements for cryptographic keys throughout their lifecycle, including key generation, usage, storage, updates, destruction, and auditing.

Data Storage Security

YMCS is hosted in Azure Blob Storage, with data centers in Virginia, USA and Paris, France, where 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.

You can select the region where your enterprise is located:

- US Region: All YMCS data is hosted at Microsoft Azure's East US datacenter in Virginia, USA.
- EU Region: All YMCS data is hosted at Microsoft Azure's France Central datacenter in Paris, France.
- AU Region: All YMCS data is hosted at Microsoft Azure's East datacenter in New South Wales, Australia.

Data Isolation

Data access among different tenant accounts is isolated from each other.

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 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. The channel can log in to the YMCS for the enterprise and gain full permissions to manage the enterprise's devices only when the enterprise grants the channel the permission to manage the devices.

Data Deletion

Customer data is kept on the server for a long time by default without deletion; if some paid users cannot renew their subscriptions in time for some reasons, we will downgrade these paid users to free users to prevent their important data from being deleted.

When a customer makes a request for deletion to privacy@yealink.com, Yealink will review and delete the relevant data within 30 days.

Data Access and Audit

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, access to the production server is limited to IP addresses within the Yealink domain.

Third, users can only log in to the production server via SSH after passing authentication on the fortress machine.

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

High Availability and Disaster Tolerance

Yealink has established the Business Continuity Management Procedures, which regulate the purpose, scope, roles, responsibilities and work procedures related to business continuity.

To identify and mitigate potential threats that may disrupt Yealink's critical business operations, we conduct annual business impact analysis and risk assessments. This process involves identifying various types of failures, determining the time required for recovery from each failure, developing risk response strategies, and documenting all relevant information in the business continuity management plan.

In addition, Yealink has developed an Emergency Response Plan to address various emergencies that may arise within YMCS, and established a regular review mechanism for the emergency plan. The Emergency Response Plan is reviewed annually by the head of the testing department. Moreover, Yealink conducts emergency drills for key products at least once a year and prepares corresponding emergency drill reports.

Yealink has developed a Capacity Management Policy to standardize the capacity management process. Every year, the Operations and Maintenance (O&M) department performs stress tests on the production environment, evaluates capacity requirements, and develops capacity plans. These plans are then reviewed by the O&M department's team leader to ensure their reasonableness. Additionally, Yealink has defined the process for capacity adjustment, which includes both capacity expansion and reduction. When developers propose capacity adjustment plans based on the overall planning and

daily needs, these plans undergo thorough validation by test engineers, developers, and operations and maintenance engineers. Only after the adjustment plans have been fully validated can the operations and maintenance engineers proceed with the necessary adjustments.

In terms of capacity management, Yealink implements systematic monitoring of server resource capacity based on its monitoring platform. The O&M team configures monitoring and alerting policies in Prometheus and uses Grafana to visually display monitoring to ensure that the platform automatically alerts relevant O&M staff to follow up on any abnormalities.

Yealink has established a backup mechanism for the YMCS to improve availability. Node data is backed up and stored locally on a daily basis. The system monitors the backup status, and in the event of any error or failure, automatic email notifications are sent to the O&M staff for further action and follow-up.

Yealink mandates the implementation of a redundancy mechanism in the YMCS, leveraging multiple regions and availability zones to ensure the uninterrupted operation of the cloud service. Additionally, Yealink utilizes an nginx proxy for the YMCS front-end, enabling request distribution and load balancing across instances, thereby guaranteeing high service availability.

Vulnerability Management and Security Incident Response

Security has always been a top priority for Yealink. As security technologies continue to evolve, Yealink dedicates significant resources each year to enhance its security measures. Additionally, Yealink collaborates with multiple reputable third-party organizations for annual security audits to ensure that its security standards align with the latest industry advancements. Yealink proactively identifies issues to ensure product security through multiple channels, including internal incident checking, vulnerability scanning, and penetration testing. If you find a possible security issue while using Yealink products, you can contact us in Yealink's security center or submit a ticket through the ticket system, and we will respond promptly and deal with relevant issues.

Security emergency response is mainly divided into four stages: problem collection, vulnerability analysis, vulnerability fix, tracking and resolution, and information disclosure.

- **Problem collection:** Yealink has a dedicated security team responsible for tracking, handling, and verifying responses to security incidents and related feedback. This team diligently collects and addresses security

issues reported by customers and takes appropriate actions to resolve them effectively.

- **Vulnerability analysis:** Priority is given to determining vulnerability risks and affected range based on the issue. In the processing stage, temporary solutions will be provided first to avoid the problem from expanding further. This approach ensures that immediate measures are taken to mitigate the impact of the issue and minimize potential risks.
- **Vulnerability fix**: Analyze the root cause of the problem based on its occurrence, trace the reasons for the defects in the design and solve the vulnerability problem promptly from the root cause.
- **Tracking and resolution**: Troubleshooting similar problems for problem fixing; internal security engineers validate the fixes; after undergoing a strict change process, security patch updates are released to address the problems effectively.
- **Information disclosure:** Yealink provides timely information disclosure on vulnerability fixes and security incident handling through official channels. This proactive approach keeps users informed about security updates and enhances transparency in addressing potential vulnerabilities.

Yealink has established the following system requirements related to security event management.

- **Information security incident management procedures**: Specify the classification, escalation, notification and resolution process for security failures.
- **Information system access and use monitoring management procedures**: Specify the requirements for system monitoring configuration and log review.
- **Closed-loop management and continuous operation encompass the entire lifecycle of security events**, including their occurrence, processing, tracing, and recovery. This comprehensive approach aims to enhance the emergency management of security events and ensure the safe and stable operation of business systems.

We recommend that you can email security@yealink.com to provide feedback on security issues through the official Yealink channels. Yealink has a dedicated security team for tracking and handling.

Disclaimer

This white paper is for reference only and does not authorize any legal rights to any intellectual property in any Yealink product. This white paper is for informational purposes only. Yealink makes no express, implied, or statutory warranties regarding the information in this white paper. This white paper is provided "as is" and may be updated from time to time by Yealink. To view the latest version of this white paper, please visit our website.

Yealink Network Technology CO., LTD.

White Paper (Version 2)

June 2023