Yealink

Entrust Video Conferencing Security

with Industry-leading Yealink Meeting Solution

Content

Company Brief Introduction

With nearly 20 years of experience in video and audio communication, Yealink aims to offer high quality conferencing services that the business demand today while meets the strong security requirements of our customers.

With many high-level compliances, for example, General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), Yealink is capable of providing customers with highly secured audio-video conferencing services.

Architecture

Yealink Meeting adopts the most advanced, stable, and secure global cloud architecture. It provides rich functions and broad compatibility under the premise of excellent audio-video conference quality. Yealink has a complete product solution, from room systems to PC or mobile clients, headsets, and other products, providing customers with complete and high-quality solutions based on Yealink Meeting.

Yealink Meeting services, room systems, and client software are designed and developed by Yealink. Our architecture contains the latest protocols, technologies, and application design concepts to provide the critical foundation of our cloud-based products and services. The data center and service node we deploy can cover over 99% of countries and areas in the world.

With the carefully crafted design, our solution can intelligently and strategically distribute different workloads to our resources across the globe, providing our customers with the optimal connecting experience and conference quality.

Moreover, the same conscious dispersal of geographical resources also improves resilience and reduces the potential impact of localized failures while keeping regulatory, legal, and privacy concerns of different countries in mind, meeting the need to keep data only within its country for some countries.

Benefits:

1. Secure and reliable global cloud architecture
2. Excellent audio-video quality
3. Powerful conference usability and collaboration capacity
4. Global intelligent routing connection, reducing network delay

Security

Yealink Meeting puts a lot of importance on security building and maintaining, from the architecture and the data security, to meet the security requirements of our customers. Nowadays, Yealink Meeting has acquired many compliances, including General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).

Secure Foundation

The cloud-based services of Yealink Meeting are hosted within highly secure Amazon Web Services (AWS) data centers. Yealink leverages AWS's independent third-party security and privacy certifications, for example, SOC and ISO27001, to provide customers with the most secure and reliable services.

Yealink chooses AWS for its most mature public cloud service. AWS is constantly innovating to provide new and improved cloud services. As we all know, video conferencing is the very elastic workload, so the capabilities of a public cloud partner like AWS allow Yealink to adjust quickly to customer needs.

Yealink has chosen AWS to optimize our operational efforts through single solution implementation, not a colocation or hybrid solution.

Secure Operation

The Yealink production service operates separately and independently from the Yealink corporate IT environment. Not only the system used for source control, build, and continuous integration (CI) but also the staging environment for quality assurance (QA) are each also maintained in separate and independent environments.

Secure Room Systems

Yealink designs and builds the room system hardware, the software, and the service that ties the hardware and software together. Yealink room systems, built upon decades of security knowledge, are rich in functionality, good quality, and highly secured.

- Yealink hardware and software are built from scratch with security as one of the vital architectural requirements.
- Yealink systems are custom-designed for video communications, which are different from component-based kits based on general-purpose operating systems. The closed-box design does not allow others to use and/or add their software applications.
- When the system is powered on, it is protected by secure boot, and the software in the system has secured with signed software images.
- Yealink secure software is encrypted when downloaded to the system.

- The only available interfaces of the system for third-party integrations and diagnostics are Yealink user interfaces and endpoint API.

Video Calling

Yealink Meeting services, room systems, and client software secure and encrypt the video, audio, content sharing (media) and, call setup (signaling) in every call end to end. Both the administrator and the user cannot disable the encryption. All calls are encrypted without influencing the call quality.

Encryption, the mandatory component of Yealink Meeting services, room systems, and client software, applies to both signaling (via TLS) and media (via SRTP).

Third-party H.323 systems will join video calls in a secure way when you set H.235 encryption. Third-party SIP systems will join in a secure way when you set SIP TLS.

Audio Calling

The Yealink Meeting cloud-based solution offers a dial-in audio conferencing feature, enabling PSTN-to-VoIP connectivity with direct routes to Yealink Meeting. Audio calls from the PSTN to the Yealink Meeting service will remain unencrypted, similar to other voice conferencing services.

Meeting Security

Yealink secures the conference with the following features:

- Passwords for securing conferences.
- Conferences can be locked. After that, participants will go to the lobby when they call into the conference. Only the conference moderators can allow them to join the conference.
- Users can use one-off conferences, but the one-off conferences will be deleted and hidden from the directory. After deleting the one-off conference, participants cannot call into the conference.
- Frequently used conferences can be hidden from the directory.
- Call escalation allows users to accept or reject new participants into a conference actively.
- During a conference, moderators can remove or mute individual participants.
- During a conference, moderators can remove or mute all participants.
- During a conference, moderators can disable their audio and/or video.

Authentication

Yealink Meeting supports local user authentication and management. Under this circumstance, the connection between Yealink Meeting cloud-based client software and services is authenticated through HTTPS, and the registrations are secured via TLS, providing robust security protection. Moreover, administrators can grant or revoke the permission of access to users or room systems at any time.

Access Control

One of the six roles can be assigned to authorized users in Yealink Meeting client. The roles and what they can do are as below:

User:

As a user, you can:

- Place and receive calls
- Disable your audio or video
- Create and own a conference
- Set or change the password for the conference you create
- Hide your meetings from the directory
- Add or remove individual or all participants in the conference you create
- Mute individual or all participants in the conference you create
- Chat with users or groups (if the administrator has enabled chat)
- Live stream the conference you create (if the administrator has enabled the live streaming)
- Record the conference (if the administrator has enabled recording)

Operation manager

As an operation manager, you can:

- Dashboard
- Member Management (users, room systems, external contacts)
- Collaboration Files (recordings, shared record and recycle bin)
- Statistics (reports, CDR, billing)
- Enterprise Settings (enterprise profile, meeting settings, recording settings, operation log)

- Teams Access

Meeting operator

As a meeting operator, you can:

- Dashboard
- Meeting Management
- VMR Management

Meeting manager

As a meeting manager, you can:

- Dashboard
- Meeting Management
- VMR Management
- Collaboration Files (recordings, shared record and recycle bin)
- Statistics (reports, CDR, billing)

Customize

The enterprise administrator can customize the role to be assigned to sub-administrator:

- Dashboard
- Member Management (users, room systems, external contacts)
- Meeting Management
- VMR Management
- Collaboration Files (recordings, shared record and recycle bin)
- Statistics (reports, CDR, billing)
- Enterprise Settings (enterprise profile, meeting settings, recording settings, operation log)
- Segment Resources
- Teams Access

Administrator

The enterprise administrator is the role with the highest permission and can assign roles for sub-administrators:

- Role assignment
- Dashboard
- Member Management (users, room systems, external contacts)
- Meeting Management
- VMR Management
- Collaboration Files (recordings, shared record and recycle bin)
- Statistics (reports, CDR, billing)
- Enterprise Settings (enterprise profile, meeting settings, recording settings, operation log)
- Segment Resources
- Teams Access

Firewall/NAT Traversal

The Yealink Meeting architecture can keep your Yealink room systems and client software safely behind your firewall and manage firewall traversal through our global service. Besides, any firewall ports to be opened inbound from the internet are not required by Yealink room systems and client software.

Also, there is no need for static public IP addressing or complicated static NAT and port-forwarding firewall configurations. This can maintain your existing perimeter posture and protect your users and devices from SIP and H.323 nuisance calls, which are common on the open internet.

Yealink only uses outbound TCP/UDP connections to realize call signaling and media. These TCP/UDP connections are always initiated by the Yealink room system or client software to establish specific channels and dynamic port address translations. These connections are directed only to our global service resources on the specific list of published FQDNs, allowing for specially designed firewall rules. Yealink manages these FQDNs and controls their Time to Live (TTL), so they are always current.

Firewall Configuration

For more information about opening ports and configuring the network, visit our website.

Privacy

Call Data Retention

Video communication data is transient but encrypted in flight. Yealink does not view, record, or store any audio, video, or presentation, except for the video conference data recorded by users on Yealink Meeting.

Call Information

Yealink only stores basic metadata of each call so that client administrators can access usage reports and information. This data does not include any media. If you choose not to use Yealink Meeting, the data will be permanently deleted 180 days after the end of your contract.

Similarly, the server log is retained for technical support engagements and troubleshooting for 180 days. This data does not include any media.

User Information

Yealink only stores the basic information of user accounts for each of our customers. If you choose not to use Yealink Meeting, the data will be permanently deleted 180 days after the end of your contract.

Administrator:

- Email address/phone number (which is also the username)
- Password (for non-SSO accounts only)
- First name, last name
- Display name
- Address
- Company

User/operation manager/meeting operator/meeting manager/customize:

- Display name
- Email address (which is also the username)
- Password (for non-SSO accounts only)

Yealink Stream, Record and Share

Yealink offers streaming and recording services for our customers. Recorded calls are stored in secure AWS facilities. Access to view recordings may be globally restricted to users within your organization only by the administrator.

- Yealink Meeting Recording and Sharing is available to subscribers of the Yealink Meeting services.
- You can only share content within your organization.
- Yealink Meeting Live Stream and Recording are encrypted using SRTP for the streaming, recording, or playback.
- Yealink Meeting Recording and Sharing is hosted on AWS, which is designed for security across all geographies and verticals.
- All the conference participants will receive the on-screen notifications, which notify users that the call is being recorded and by whom.

Chat

Yealink Meeting chat is encrypted in-flight with HTTPS and TLS and is hosted on AWS. The chat is valid only in the current conference. Once the conference ends, the chat becomes invalid. Moreover, the chat is not stored in Yealink Meeting or the local.

Service Optimization & Availability

The Yealink Meeting services are operated in secure AWS data centers in North America, South America, Europe, and Asia. Yealink Meeting calling capacity is hosted in AWS. Yealink room systems and client software will automatically create conferences in the optimal AWS data center based on the location of the initial participants of the conference. Conference recordings are stored in the AWS data center where the conference was hosted. They are not replicated outside of that AWS data center.

In some cases, your Yealink room systems and client software users will be routed to another available part of the service without disconnecting a live call if a server failure occurs. Failed services are automatically replaced and returned to full capacity within minutes, without any manual intervention by Yealink staff. Our systems are backed up, ensuring that your configurations are protected and up to date.

Yealink

YMinfo@yealink.com | www.yealinkmeeting.com