Safeguarding Data Privacy:

Yealink Android-based Room Devices and DM Service

Secure device connectivity with device management platforms is essential for protecting data in workplace. This article delves into how these two work together to secure customer experience in Yealink ecosystem.

Certified by Microsoft Teams, Yealink Android devices (MeetingBar A10/A20/A30; MeetingBoard 65/86; DeskVision A24) seamlessly integrate all the necessary features for efficient collaboration. As an **optional and value-added service,** Yealink Device Management platform enables customers to efficiently manage multiple devices in bulk, providing core benefits as bellow:

- Device Healthy Status Alert
- Bulk device upgrades and management
- Remote diagnosis

Yealink provides two device management platform options:

- YDMP (Yealink Device Management Platform): Customers can install Yealink's Device Management (DM) software in their own data center. This allows them to have full control over managing and securing Yealink devices.
- YMCS (Yealink Management Cloud Service): YMCS utilizes Microsoft Azure infrastructure to offer device management services. Microsoft Azure is a trusted cloud computing platform used by enterprises worldwide. YMCS is SOC2 Type 2 and GDPR certified, ensuring adherence to strict security and privacy standards. It operates independent data centers in the United States, Europe, and Australia, enhancing data security, redundancy, and compliance with regional regulations.

Device Connection with YMCS

Yealink follows best practices employed to establish secure device connections with device management platforms. By implementing robust authentication mechanisms, secure communication protocols, firewalls, and secure device enrollment and onboarding processes, organizations can ensure that only authorized devices can connect to the management platform. This helps protect sensitive data, prevent unauthorized access, and build trust in the IoT infrastructure.

To ensure a device is connected to the Yealink Management Cloud Service (YMCS), it is necessary for the enterprise administrator to actively deploy the device. Without this deployment, the device will not actively report telemetry data to YMCS. Users have the option to manually configure the device's connection with YMCS through the device's user interface or device manager interface. This allows users to control whether the device can connect to YMCS or not.

Data Interaction between Device and YMCS

Microsoft Teams ensures that "no end-user data is transferred to, or accessible by, the Microsoft Teams Rooms device." This commitment to data privacy means that the data interaction between Yealink devices and YMCS centers on device-related data, such as configurations, firmware updates, alerting, and diagnostics. Under privacy policy and Yealink End-User License Agreement (EULA), YMCS acts as a centralized management platform, enabling administrators to remotely configure and manage various device settings without accessing or transferring end-user data. This approach ensures that personal information, conversations, and files shared through Microsoft Teams remain secure and inaccessible to the device management platform.

Source from Where Data Collected	Categories of Data Collected	Business Purpose for Collection	Disclosed to the following Service Providers
Device Administrator and user information	**Account Management:** • Enterprise account • Enterprise ID • Email address • Password (hashed) • First/Last Name • Phone number **(optional)**	• Authenticate and authorize administrative access to the service • Deliver the service • Reporting • Usage/activity	Microsoft Azure
Device Identifier and Network data	**Device Management:** • Device ID • Device name • MAC address • Server address • Serial number • Software version • Firmware version • Device status • Device configuration records • Network identifiers • Network type • IPv4/v6 address **Remote Diagnosis:** • Device ID • MAC address • IP address • Log files **Resource Management:** • Server ID • Site ID • Firmware name • Device geolocation data including time zone • etc.	• Understand how devices are being used in a customer environment • Help customer diagnose technical issues • Collect analytics to improve the technical performance of the customer's UC service • Provide details in support of room or devices issues that require support	Microsoft Azure

Data Transmission and Encryption between Device and YMCS

Data transmission between the Yealink device and YMCS is highly secure and protected. YMCS employs TLS 1.2 or higher with a strong cipher suite to encrypt all information during transmission. This ensures that all communication channels are encrypted once a session is established over TLS.

The data exchanged between the device and YMCS is encrypted, providing robust protection against potential malicious attacks and data tampering. This encryption ensures the confidentiality and integrity of the data, enhancing overall data security.

Preconfigured Domain

When the Yealink device is rebooted or when executing a service, it will access the preset server addresses. The following server addresses are preconfigured:

Domain Name	Business Function	Request Method
www.msftncsi.com/ncsi.txt www.google.com/generate_204	Network connectivity check, trigger request on reboot or network change.	Enabled by default
time.windows.com pool.ntp.org	NTP's sever address, power-up and periodic queries.	
dm.yealink.com	Server address for device detection upgrade	Disabled by default, customers need to enable it manually
www.google.com	Proxy Tested Access Sites	
www.yealink.com	Web page hyperlink address that provides quick access to the official Yealink website.	
support.yealink.com	Web page hyperlink addresses that provide quick access to Yealink support center.	

Resources:

1. Yealink Security Whitepaper for Android devices and YMCS:

   https://www.yealink.com/en/trust-center/resources

2. Microsoft Teams Rooms security on Android:

   https://learn.microsoft.com/en-us/microsoftteams/rooms/security