

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 (<u>Yealink Management Cloud Service</u>): YMCS utilizes Microsoft Azure infrastructure to offer device management services. <u>Microsoft Azure</u> 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

<u>Microsoft Teams</u> 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 <u>Yealink End-User License Agreement</u> (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.



Control NormContegence of Data CollectedDestinese trappose pose for CollectionDestinese trappose the following Service ProvidersDeviceAccount Management: • Enterprise account and user• Autoenticate and authorize administrative access to the serviceMicrosoft AzureAdministrator• Enterprise D • Enterprise D • Password (hashed) • PisstLast Name • Phone number (optional)• Deliver the service • Deliver the service • Deliver the service • Password (hashed) • Pison number (optional)• Understand how devices are being used in a customer environmentMicrosoft AzureDeviceDevice Management: • Device ID • Device name • Servira address • Servira address • Servira address• Understand how devices are being used in a customer environmentMicrosoft AzureNetwork data• Device name • Device address • Servira address • Network identifiers • Device ID • NAC address • Log filesProvide details in support of room or devices issues that require supportDevice ID • Nac address • Device ID • Nac address • Device ID • Nac address • Log filesRemote Diagnosis: • Server ID • Site ID • Device geolocation dataDevice geolocation data• Device geolocation data	Source from	Categories of	Business Purpose	Disclosed to
Data Collected Account Management: Authenticate and authorize administrator Microsoft Administrator Enterprise account administrative access to the service Azure information Enterprise ID service Azure Password (hashed) Reporting Herosoft Password (hashed) Reporting Herosoft Prist/Last Name Usage/activity Herosoft Pevice Device Management: Understand how devices are being used in a customer Microsoft Network data Device name environment Help customer diagnose Service Service estatus Provide details in support of Device status Provide details in support of Device status Provide details in support of Provide details in support of Device offiguration records Network kidentifiers require support Network type PiPv4/v6 address PiPv4/v6 address Piedress PiPvadicess Piedress Piedress Piedress Network identifiers Piedress Piedress Piedress PiPvadicess Piedress Piedress Piedresis Piedre iD <td< th=""><th></th><th></th><th></th><th></th></td<>				
DeviceAccount Management:Authenticate and authorizeMicrosoftAdministratorEnterprise accountadministrative access to theAzureand userEnterprise IDserviceAzureinformationErnail addressDeliver the serviceAzurePassword (hashed)ReportingFirstLast NameUsage/activityPoviceDevice Management:Understand how devices areMicrosoftIdentifier andDevice IDbeing used in a customerAzureNetwork dataDevice nameenvironmentAzureServial numberServial numberServial susesServial numberServial numberServial numberSoftware versionthe technical susesServial numberProvide details in support ofDevice configuration recordsNetwork typeProvide detailsrequire supportNetwork typeProvide detailsSupport ofNetwork identifiersNetwork identifiersNetwork typeProvide detailsNAC addressProvide detailsProvide detailsSupport ofServer IDSter IDSter IDSter IDSter IDSter IDSter IDFirmware nameSter IDSter IDSter IDFirmware nameSter IDFi		Data Collecteu		_
DeviceAccount Management:Authenticate and authorize administratorMicrosoftAdministrator-Enterprise accountadministrative access to the serviceAzureinformation-Enterprise IDserviceAzureinformation-Enterprise ID-Reporting-Password (hashed)-ReportingPassword (hashed)-ReportingPhone number (optional)DeviceDevice Management:Identifier and-Device IDbeing used in a customerAzureNetwork data-Device nameNAC addressServer addressServer addressSoftware versionDevice configuration recordsDevice IDDevice Configuration recordsDevice Colfiguration recordsDevice IDNetwork identifiersDevice IDMAC addressDevice IDMAC addressDevice IDMAC addressDevice IDDevice ID <th>Data Collected</th> <th></th> <th></th> <th></th>	Data Collected			
AdministratorEnterprise accountadministrative access to the serviceAzureand userEnterprise IDserviceinformationEmail address-Deliver the servicePassword (hashed)-Reporting-Usage/activityPhone number (optional)-Device Management:-Understand how devices areMcrosoftIdentifier andDevice IDbeing used in a customerAzureNetwork data-Device nameenvironmentAzure-Server addresstechnical issuesSerial number-Collect analytics to improve-Server address-Collect analytics to improveSoftware versionthe technical performance of-Firmware versionthe customer's UC service-Device configuration recordsrequire support-Network identifiers-Device configuration recordsrequire supportservice-Network type-IPv4/v6 address-Device ID-MAC address-Device ID-MAC address-IPv4/v6 address-IPv4/v6 address-Device ID-MAC address-IPv4/v6 address-Device ID-Server ID-Server ID-Server ID-Site ID-Server ID-Server ID-Site ID-Server ID-Server ID-Server ID-Server ID-Server ID-Serv	Device	Account Management:	Authenticate and authorize	
and user information:Enterprise ID :Email addressserviceiserviceinformation:Email address:Deliver the serviceiservice:Password (hashed):Reporting:Usage/activityiservice:Phone number (optional):Usage/activityiserviceMicrosoftDeviceDevice Management::Understand how devices are environmentMicrosoftNetwork data:Device IDbeing used in a customerAzure:MAC address:Help customer diagnose:Server address:Collect analytics to improve:Software versionthe technical performance of the customer's UC service:Povice status:Povice details in support of require support:Network identifiers:Network identifiers:Network identifiers:Povice details in support of require support:Network type:IPv4/v6 address:Povice ID :MAC address:Server aldress:Device ID:MaC address:Leg files:Povice ID:MaC address:Leg files:Povice ID:MaC address:Leg files:Povice ID :MAC address:Leg files:Povice ID :MaC address:Leg files:Povice ID :MaC address:Leg files:Powice ID :Site ID :Site ID :Site ID :Site ID :Site ID 		-		
information• Email address• Deliver the service• Reporting• Password (hashed)• Reporting• Usage/activity• Phone number (optional)• Usage/activityDeviceDevice Management:• Understand how devices areIdentifier and• Device nameenvironment• NAC address• Help customer diagnose• Server address• Collect analytics to improve• Software versionthe technical performance of• Firmware version• Provide details in support of• Device configuration records• Network type• Network type• Povide address• Network type• Device ID• Network type• Provide details in support of• Device configuration records• require support• Network type• Povide address• Device ID• MAC address• Device ID• MAC address• Device ID• MAC address• Device ID• Server ID• Server ID• Server ID• Site ID• Server ID• Site ID• Server ID• Site ID• Firmware name				Azure
Password (hashed) • First/Last Name • Phone number (optional)• Reporting • Usage/activity• Identifies • Usage/activityDeviceDevice Management: • Device name• Understand how devices are being used in a customerMicrosoft AzureNetwork data• Device name • Device name• Help customer diagnose • Server address• Help customer diagnose • Software version• Collect analytics to improve • Software version• Collect analytics to improve • Software version• Device environment • Collect analytics to improve • Software version• Device diagnose • Provide details in support of • Device status• Provide details in support of • Device status• Provide details in support of • Device status• Provide details in support of • Device daties in support• Device in the customer's UC service • Provide details in support of • Device offiguration records • Network type • IPv4/v6 address• Remote Diagnosis: • Device ID • MAC address • Log files• Resource Management: • Server ID • Site ID • Site ID • Site ID • Site ID• Reporting • Firmware name• Active • Remote Diagnosis: • Server ID • Site ID • Firmware name• Reporting • Remote Diagnosis: • Server ID • Site ID • Firmware name• Reporting • Remote Diagnosis: • Server ID • Site ID • Firmware name• Reporting • Remote Diagnosis • Remote Diagnosis • Server ID • Site ID • Firmware name• Reporting • Remote Diagnosis • Remote Diagnosis • Server ID • Site ID • Firmware name• Remote Diagnosis • Remote Diagnosis • Remote Diagnosis • Server ID • Site ID • Firmware name• Remote Diagnosis • Remot				
+ First/Last Name • Phone number (optional)• Usage/activity• Image/activityDevice Identifier and Network dataDevice Management: • Device name• Understand how devices are being used in a customer environmentMacrosoft AzureNetwork data• Device nameenvironmentAzure• MAC address• Help customer diagnose technical issues• Server address• Server address• Collect analytics to improve • Software version• Collect analytics to improve the technical performance of • Device status• Device onfiguration records • Device status• Provide details in support of room or devices issues that require support• Network type • IPV4/v6 address• Device status• Device ID • MAC address• Device ID • MAC address• Device ID • MAC address• Log files• Device ID • MAC address• Log files• Device ID • MAC address• Server ID • Site ID • Site ID • Site ID • Firmware name	momaton			
Phone number (optional)Indication of the series is set at the series of the		. ,		
Device Device Management: • Understand how devices are being used in a customer Microsoft Identifier and • Device ID being used in a customer Azure Network data • Device name environment Azure • MAC address • Help customer diagnose technical issues • Collect analytics to improve • Server address • Collect analytics to improve technical performance of the customer's UC service • Device status • Provide details in support of room or devices issues that require support • Network type • IPv4/v6 address • Device ID • MAC address • IP address • Log files • Mac address • Log files • Server ID • Server ID • Server ID • Server ID • Site ID • Firmware name • Server ID • Server ID			- Usage/activity	
Identifier and Network dataDevice IDbeing used in a customerAzureNetwork data-Device nameenvironmentHelp customer diagnose·MAC address-Help customer diagnose-Server addresstechnical issues·Server address-Collect analytics to improve-Software versionthe technical performance of·Firmware versionthe customer's UC service-Device configuration recordsroom or devices issues that·Device configuration records·Network identifiersrequire support·Network type-Device ID-Network type·Device ID·MAC address-IP val/v6 address·Device ID·MAC address-IP val/ress·Log files-Device ID-Server ID·Server ID·Server ID-Server ID·Site ID·Site ID-Server ID·Site ID·Site ID·Firmware name-Server ID	Dovico	,	• Understand how devices are	Microsoft
Network data Device name environment Help customer diagnose Server address technical issues Serial number Collect analytics to improve Software version the technical performance of Firmware version the customer's UC service Device status Provide details in support of Device configuration records Network type IPv4/v6 address Network type IPv4/v6 address Lo evice ID MAC address Log files Server ID Server ID				
• MAC address• Help customer diagnose• Server addresstechnical issues• Serial number• Collect analytics to improve• Software versionthe technical performance of• Firmware versionthe customer's UC service• Device status• Provide details in support of• Device configuration recordsroom or devices issues that• Network identifiersrequire support• Network type• IPv4/v6 address• Device ID• MAC address• Log files• Log files• Log files• Server ID• Site ID• Site ID• Firmware name• Log files				Azure
 Server address Software version Firmware version Device status Provide details in support of room or devices issues that require support Remote Diagnosis: Device ID MAC address IP address Log files Resource Management: Server ID Site ID Firmware name 	Network data			
 Serial number Software version Firmware version Device status Device configuration records Device configuration records Network identifiers Network type IPv4/v6 address Device ID MAC address IP address Server ID Site ID Firmware name Collect analytics to improve Provide details in support of Com or devices issues that require support Remote Diagnosis: IP address IP addres IP address IP address <l< td=""><td></td><td></td><td></td><td></td></l<>				
 Software version Firmware version Device status Device configuration records Network identifiers Network identifiers IPv4/v6 address Pevice ID MAC address IP address Log files Resource Management: Server ID Site ID Firmware name 				
 Firmware version Device status Provide details in support of room or devices issues that Network identifiers Network type IPv4/v6 address Remote Diagnosis: Device ID MAC address IP address Log files Resource Management: Server ID Site ID Site ID Firmware name 				
 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 Site ID Firmware name 				
 Device configuration records Network identifiers Network type IPv4/v6 address Device ID MAC address IP address Log files Resource Management: Server ID Site ID Site ID Firmware name 				
 Network identifiers Network type IPv4/v6 address Remote Diagnosis: Device ID MAC address IP address Log files Resource Management: Server ID Site ID Site ID Firmware name 				
 Network type IPv4/v6 address Remote Diagnosis: Device ID MAC address IP address I P address Log files Resource Management: Server ID Site ID Site ID Firmware name 				
 IPv4/v6 address Remote Diagnosis: Device ID MAC address IP address Log files Resource Management: Server ID Site ID Firmware name 				
Remote Diagnosis: • Device ID • MAC address • IP address • Log files Resource Management: • Server ID • Site ID • Site ID • Firmware name				
 Device ID MAC address IP address Log files Resource Management: Server ID Site ID Firmware name 				
 Device ID MAC address IP address Log files Resource Management: Server ID Site ID Firmware name 		Remote Diagnosis:		
 MAC address IP address Log files Resource Management: Server ID Site ID Firmware name 		-		
 IP address Log files Resource Management: Server ID Site ID Firmware name 				
Resource Management: • Server ID • Site ID • Firmware name				
Resource Management: • Server ID • Site ID • Firmware name		• Log files		
Server ID Site ID Firmware name				
Server ID Site ID Firmware name		Resource Management:		
Site ID Firmware name		_		
Firmware name		• Site ID		
Device geolocation data				
		Device geolocation data		
including time zone		-		
• etc.		-		

Yealink

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



Resources:

- 1. Yealink Security Whitepaper for Android devices and YMCS: <u>https://www.yealink.com/en/trust-center/resources</u>
- 2. Microsoft Teams Rooms security on Android: <u>https://learn.microsoft.com/en-us/microsoftteams/rooms/security</u>