Yealink Security Configuration Guide

Release time: July 2023

1. General

The Security Configuration Guide provides users with an illustrative document for adopting security policies in deploying Yealink's products. It contains the best safety practices in the industry. It is important to note that implementing security control measures may have certain impacts on availability, performance, or other operational tasks. Recommendations and implications need to be carefully checked when adopting security configurations.

This guide is not an exhaustive list of all possible security configurations. We recommend that customers use this configuration guide and the Yealink Product User Guide as reference points and deploy security configurations according to the actual situation.

1.1 Target Audience

This document applies to IT administrators, application administrators, platform deployers, security specialists, auditors, etc., who plan to develop, deploy, evaluate, or use Yealink’s products.

1.2 Definition of Levels

The recommended level definition for security configuration in this document is as follows:

Level 1: This type of configuration is the most fundamental requirement for organizational security. Failure to configure it properly may result in potential security risks.

Level 2: This type of configuration expands on the Level 1 configuration and is suitable for security-critical environments. However, implementing this configuration may impact the business and require configuration by IT administrators.

2. Yealink Device Security Configuration Recommendations

2.1 Web Access Control

2.1.1 Changing User Names and Passwords

Level: Level 1

Configuration Recommendations:

By default, Yealink's devices are shipped with fixed passwords, and the admin has higher operating privileges. To better control the personnel's use of the device's resources, it is necessary for you to change the default password to avoid remote control of the device due to unchanged default passwords.

The factory default password is fixed, which should be changed to keep one password per machine for all devices.

Check steps:

1. Log in to the device with the default account and password of the admin.
2. To detect which user accounts are open using this method: successfully log in to the web interface, navigate to the "Password" tab under "Security", and verify the "User Type" category.
3. Pass all user passwords under the “User Type” type: password complexity: recommended eight or more combinations of letters, numbers, and special characters (at least two or more combinations).

Remarks:

Administrators familiar with Yealink's Configuration Management Appliance can configure passwords via auto-deployment with the statement: security.user_password=admin:xxxxxx

Applicable models: All Series

* All series include Yealink Phone products (VoIP Phone Series, Android Phone Series, Dect Phone Series, Teams Phone Series, Zoom Phone Series) and Yealink Video products (Intelligent Room Device Series, Meeting Bar Series, Meeting Eye Series, Meeting Board Series, DeskVision Series).

2.1.2 Configuring Users to Force a Password Change

Level: Level 1

Configuration Recommendations:

Yealink's devices are shipped with fixed passwords by default. If the administrator has not configured to change the password, you can configure it to force the user to change the password before use.

By default, a fixed password is set, and users are required to change it. We recommend modifying the password for all devices to maintain a one-to-one correspondence or enable the mandatory password change feature.

Check steps:

1. Place the security.password_use_default.enable=1 configuration through Yealink's auto-deploy feature.
2. When using the advanced features, the device needs to change the password before it can be used commonly.

Applicable models: All Series

2.1.3 Restriction of same-origin access

Level: Level 2

Configuration Recommendations:

Yealink devices can access the web interface through DNS rebinding. Malicious websites may utilize DNS rebinding to gain same-origin access to the web interface. By default, there are no restrictions on domain name access permissions. Domain name restrictions can be set to mitigate this risk.

For users with high-security requirements who have not turned off web functionality, they can configure it according to their specific needs.

Check Steps:

1. Configure the environment with a domain name that redirects to the IP address of the phone, for example, test.yealink.com
2. Autop update wui.secure_domain_list =test.yealink.com
3. Log in to the webpage with the IP of the phone or the domain name test.yealink.com, and you can log in successfully. Note: autop configures multiple domain names, which should be separated by a semicolon, such as wui.secure_domain_list = test.yealink.com; product.yealink.com

Applicable models: All Series

2.1.4 Restricting IP Access

Level: Level 2

Configuration Recommendations:

Yealink's devices are shipped from the factory without restriction on PC address access, and any IP address not restricted by the network will be able to access Yealink's devices. If users need to implement network isolation within the internal network, they can restrict access by configuring an allowed IP list for accessing web pages.

For users with high-security requirements who have not turned off web functionality, they can configure it according to their specific needs.

Check steps:

1. Autop updates wui.limit_ip to limit visitors; e.g. wui.limit_ip = 10.3.21.45,10.10.21. *,192.168.*.6*
2. Web access with non-permitted PCs, the device does not respond to illegal network requests
3. This configuration allows for specifying individual IP addresses and certain network segments. Null and any mean that access rights for visitors are not restricted.

Applicable models: All Series

2.1.5 Banned User Access Type: User user access

Level: Level 2

Configuration Recommendations:

Yealink's devices will be open to admin and user by default when shipped (see the product manual for details), and the management can restrict the users without access needs through configuration, preventing the users without access needs from being attacked.

For users with high-security requirements who have not turned off web functionality, they can configure it according to their specific needs.

Check steps:

1. Autop updates security.web_limited_access_level for user open type, e.g., security.web_limited_access_level=user
2. By default, the device only allows login via the admin user and does not permit login via the User user.

Model: All Series

2.1.6 Turning off Web Page Functions

Level: Level 1

Configuration Recommendations:

Yealink's devices are shipped with default open access to the HTTPS web page. It is up to the user administrator to determine whether granting web page access to end users is necessary. If web page access is not essential, it can be directly turned off. Reduce the risk of attacks on web pages.

Users with a standard security level may choose not to update, while users with strict security requirements can configure it as 0

Check steps:

1. Autop update wui.http_enable=0, wui.https_enable=0
2. Unable access to the device's web page using HTTP and HTTPS.

Remarks:

We recommend turning all devices off if deployed on the public network.

Applicable models: All Series

2.2 SIP Protocol Security

2.2.1 Enabling Trusted IP

Level: Level 1

Configuration Recommendations:

You can configure the SIP-related signaling processing only to accept messages from the server IP address and ignore any notifications from IP addresses outside the server IP range. This helps prevent SIP attacks and ensures that only authorized server IP addresses are allowed to send SIP messages.

Factory default is 0, and we recommend that all users configure it as 1

Check steps:

1. Autop update sip.trust_ctrl=1
2. SIP network attacks via sipvicious fail to acquire SIP devices on the Internal network. Avoiding Ghost Phone Attacks

Remarks:

Enabling this feature will cause IP broadcasting to be unavailable

Applicable models: VoIP Phone Series, Android Phone Series, Dect Phone Series

2.2.2 Turning off Live IP Streaming

Level: Level 2

Configuration Recommendations:

Turn off IP peer-to-peer communication to avoid the need for the device to process SIP messages from untrusted IPs, resulting in the receipt of ghost calls.

Check steps:

1. Autop update features.direct_ip_call_enable=0
2. The cooperating machine initiates a live IP call, and the DUT does not respond to the associated call request

Remarks:

Configuring sip.trust_ctrl=1 is sufficient, and there is no need to configure features.direct_ip_call_enable=0.

Applicable models: VoIP Phone Series, Android Phone Series, Dect Phone Series

2.3 TLS Authentication Related

2.3.1 Mandatory CN Verification

Level: Level 2

Configuration Recommendations:

Yealink's devices are shipped without turning on the CN of the mandatory verification server. In enterprises with strict security and standardized processes, you can turn on the CommonName service of the mandatory verification server certificate.

Normal security level users can be left un-updated; severe security users are configured as 1

Check steps:

1. Autop update security.cn_validation=1 All applications that use TLS have CommonName or SubjectAltName turned on to force validation of server-side certificates.

Remarks:

After enabling certificate CN verification, it is necessary to ensure that the certificate issued by the server matches the server's domain name. Otherwise, the TLS handshake will fail because the CN verification fails.

Applicable models and function range:

(Support configuration function: Auto Provision, Devices Management) Intelligent Room Device Series, Meeting Bar Series, Meeting Eye Series, Meeting Board Series, DeskVision Series, Teams Phone Series, Zoom Phone Series

(List of supported features: Auto Provision, Devices Management, LDAPS, XML Browser, Remote PhoneBook, TR069, BroadSoft XSI) VoIP Phone Series, Android Phone Series, Dect Phone Series

2.3.2 TLS Default Protocol Versions

Level: Level 1

Configuration Recommendations:

Yealink's devices are not factory-enabled to force the use of TLS protocol versions, negotiate from a higher version to a lower version and by default. At this stage, TLS1.0 and TLS1.1 are classified as insecure algorithms, and users can limit the TLS protocol version of the device by configuring different values.

The default is three. Negotiation to TLS 1.0 is supported, and we recommended that all users configure to five; only TLS 1.2 or higher can be used.

Check steps:

1. Autop updates security.default_ssl_method=5, where the different values represent the following

   0-TLS 1.0

   3-SSLV23 (default)

   4-TLS 1.1

   5-TLS 1.2

   6-TLS 1.3

2. After setting it up by grabbing the packet ssl and seeing what the TLS version of the grabbed packet is

3. The device is not supporting TLS versions below TLS 1.2.

Applicable models and function range:

(List of supported features: Auto Provision, Devices Management) Intelligent Room Device Series, Meeting Bar Series, Meeting Eye Series, Meeting Board Series, DeskVision Series, Teams Phone Series, Zoom Phone Series

(List of supported features: Auto Provision, Devices Management, LDAPS, XML Browser, Remote PhoneBook, TR069, BroadSoft XSI) VoIP Phone Series, Android Phone Series, Dect Phone Series

2.3.3 Configuring the Suite of Algorithms Supported by the Client

Level: Level 2

Configuration Recommendations:

Yealink's devices have been configured with high encryption level encryption algorithms at the factory. If users have higher requirements for encryption algorithms, the administrator can modify the algorithm suite through the following configuration.

The default algorithm basically meets the conditions. After enabling web functionality, users with higher security requirements can configure it based on their specific needs.

Check steps:

1. Autop update security.tls_cipher_list=

Reference to the high-level suite of encryption algorithms

ECDHE + DHE Elliptic curve:
kEDH:kEECDH:!LOW:!SHA1!CAMELLIA:!ADH:@STRENGTH

ECDH + DH Elliptic curve:
DH:ECDH:!LOW:!SHA1:!ADH:!aNULL:!eNULL:@STRENGTH

highly compatible algorithmic suites are used by default:
AES:!ADH:!LOW:!EXPORT:!aNULL:!eNULL:!MEDIUM (security level that meets the needs of the majority of customers)

2. Grab a packet to see the list of algorithm suites carried by the Client Hello sent from the device.

Remarks:

This configuration needs to be configured carefully and requires a specialized security engineer to configure it, which may result in the risk of the device TLS being unavailable.

Applicable models and function range:

(List of supported features: Auto Provision, Devices Management) Intelligent Room Device Series, Meeting Bar Series, Meeting Eye Series, Meeting Board Series, DeskVision Series, Teams Phone Series, Zoom Phone Series

(List of supported features: Auto Provision, Devices Management, LDAPS, XML Browser, Remote PhoneBook, TR069, BroadSoft XSI) VoIP Phone Series, Android Phone Series, Dect Phone Series

3. Introduction of Key Terms

- VoIP Phone Series: T3 Series, T4 Series, T5 Series, CP925, CP935
- Android Phone Series: VP59, SIP-T58W (Pro), CP965, T64, T67
- Dect Phone Series: W90, W80, W70B
- Intelligent Room Device Series: RoomPanel, RoomPanelPlus, Roomcast
- Meeting Bar Series: MeetingBar A10, MeetingBar A20, MeetingBar A30
- Meeting Eye Series: MeetingEye 500
- Meeting Board Series: MeetingBoard 65, MeetingBoard 86
- DeskVision Series: DeskVision A24
- Teams Phone Series : MP58-Teams, MP56-Teams,MP54-Teams, MP52-Teams, VP59-Teams, CP965-Teams.
- Zoom Phone Series: MP58-Zoom, MP56-Zoom, MP54-Zoom, VP59-Zoom, CP965-Zoom.

4. Introductory Remarks

This article guides for customers to check and deploy the security configuration of Yealink's network devices, helping them improve their security defenses and adapt to the company's security policies.

This document is provided for reference purposes only and has no legal effect or constitutes legal advice. It should not be considered as a guarantee or a sole

basis for ensuring the security of deploying Yealink's products for any customer. Customers should assess the enterprise security level appropriately and add to or tailor this baseline configuration guide as needed.

Detailed Configuration Guide for each device, please refer to https://support.yealink.com/.

If you have any security-related queries or requests, feel free to contact the Yealink data security team at security@yealink.com.