Using Security Certificates on Yealink IP Phones

This guide provides the detailed instructions on how to configure and use certificates on Yealink IP phones. In addition, this guide provides step-by-step instructions on how to create custom certificates for Yealink IP phones.

This guide applies to the following Yealink IP phones:

- CP860, SIP-T46G, SIP-T42G and SIP-T41P IP phones running firmware version 71 or later
- SIP-T48G IP phones running firmware version 72 or later
- SIP-T58A, SIP VP-T49G, SIP-T40P, SIP-T29G, SIP-T23P/G, SIP-T21(P) E2, SIP-T19(P) E2, CP960 and W56P IP phones running firmware version 80 or later
- SIP-T48S, SIP-T46S, SIP-T42S, SIP-T41S, SIP-T40G, SIP-T27G, W52P, W60P and CP920 IP phones running firmware version 81 or later
- VP59, W53P and CP930W-Base IP phones running firmware version 83 or later
- SIP-T57W, SIP-T54W, SIP-T53W and SIP-T53 IP phones running firmware version 84 or later

Introduction

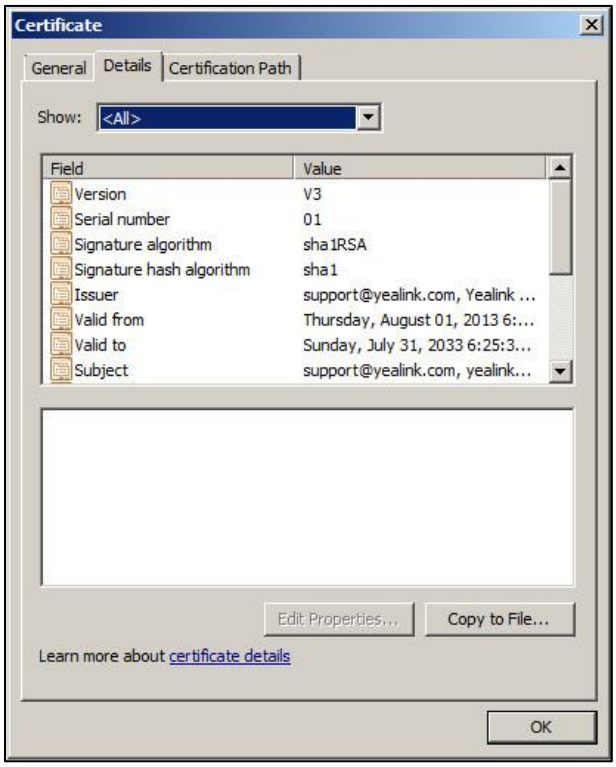
Certificate is an important element in deploying a solution that ensures the integrity and privacy of communications involving Yealink IP phones.

Three types of certificates are pre-loaded on Yealink IP phones and comply with X.509 standard.

- **A unique device certificate**: It is installed at the time of manufacture and is unique to an IP phone (based on the MAC address) and issued by the Yealink Certificate Authority (CA). This certificate is available on Yealink IP phones running firmware version 72 or later.
- **A generic device certificate**: It is installed by default and is issued by the Yealink Certificate Authority (CA). If no unique certificate exists, the IP phone may send a generic certificate for authentication.
- **Trusted certificates** (**Certificate Authority certificates**): For SIP VP-T49G IP phones, there are 30 trusted certificates installed by default. For VP59/SIP-T58A/CP960 IP phones there are 186 trusted certificates installed by default. For SIP-T57W/T54W/T53W/T53/T48G/T48S/T46G/T46S/T42G/T42S/T41P/T41S/T40P/T40G/T29G/T27G/T23P/T23G/T21(P) E2/T19(P) E2 and CP920 IP phones, there are 77 trusted certificates installed by default. For CP860, W52P, W53P, W56P, W60P and CP930W-Base IP phones, there are 76 trusted certificates installed by default. Refer to Appendix B Trusted Certificate Authority List for more information.

Note The IP phone does not have the unique device certificate by upgrading firmware version to 72.

The following shows an example of a Yealink generic certificate. For the information on fields of X.509 certificate, refer to Appendix A X.509 Certificate Structure.



Configuring Trusted Certificates on Yealink IP Phones

When an IP phone requests an SSL connection with a server, the IP phone should verify that whether the server can be trusted. The server sends its certificate to the IP phone and the IP phone verifies this certificate based on its trusted certificates list. The SIP VP-T49G IP phones have 30 built-in trusted certificates. The VP59/SIP-T58A/CP960 IP phones have 186 built-in trusted certificates. The SIP-T57W/T54W/T53W/T53/T48G/T48S/T46G/T46S/T42G/T42S/T41P/T41S/T40P/T40G/T29G/T27G/T23P/T23G/T21(P) E2/T19(P) E2 and CP920 IP phones have 77 built-in trusted certificates. The CP860, W52P, W53P, W56P, W60P and CP930W-Base IP phones have 76 built-in trusted certificates. For more information, refer to Appendix B Trusted Certificate Authority List. The IP phone supports uploading 10 custom trusted certificates (CA certificates) at most. For more information on customizing a trusted certificate, refer to Appendix C Creating Custom Certificates.

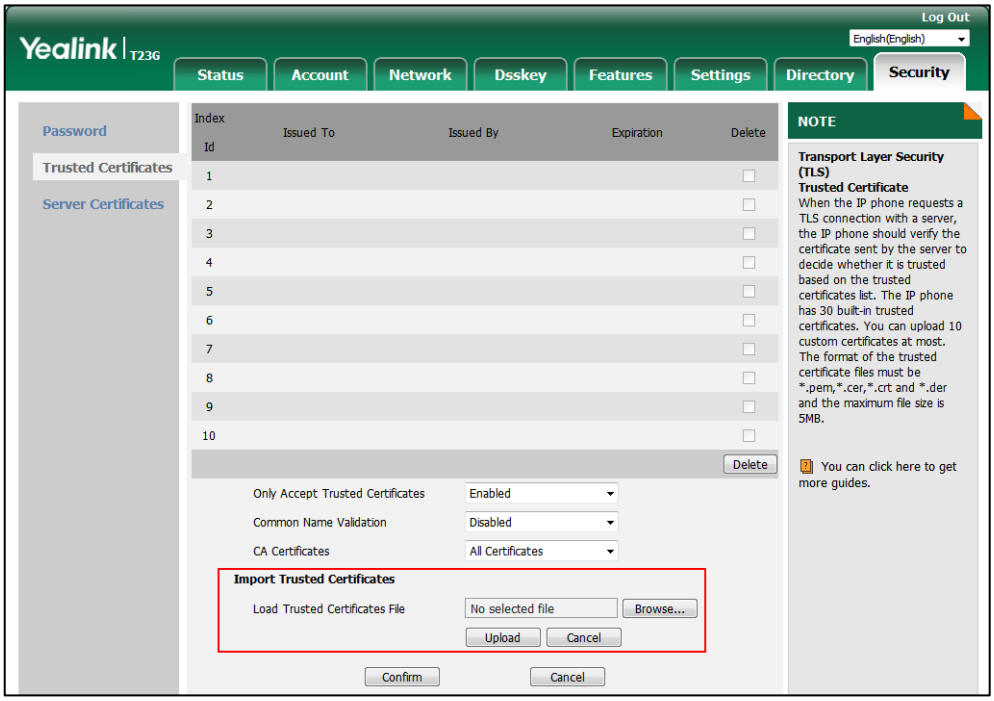
Note For the IP phone to determine whether a certificate is within its valid time range, check that the time and date on the phone are configured properly.

Configuring Trusted Certificate via Web User Interface

The followings take the SIP-T23G IP phone as examples.

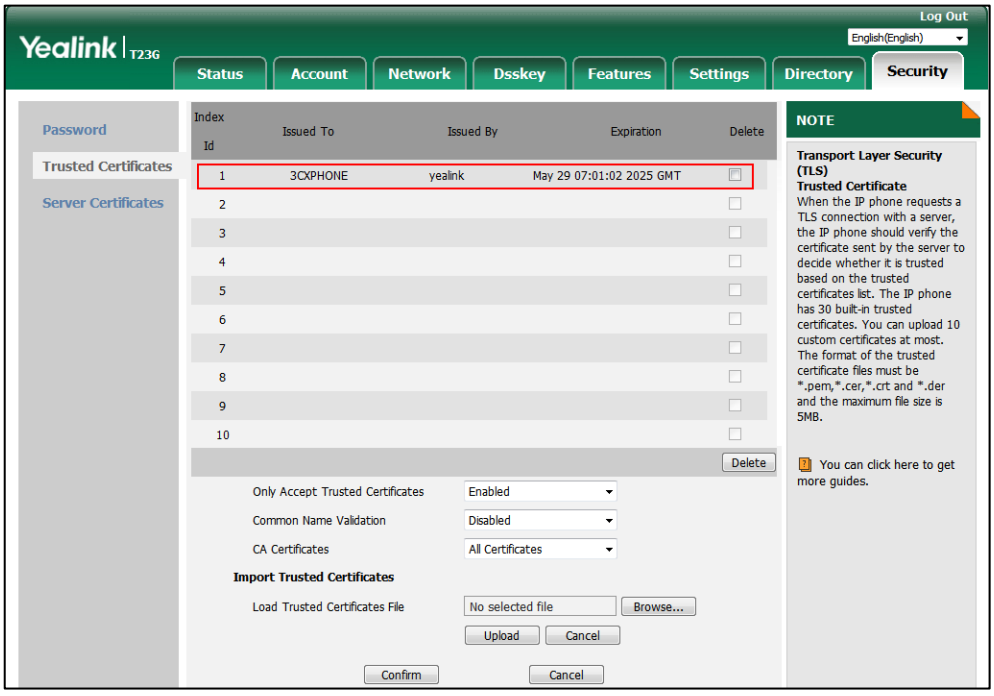
To upload a trusted certificate via web user interface:

1. Click on **Security**->**Trusted Certificates**.
2. Click **Browse** to locate the certificate (*.pem, *.crt, *.cer or *.der) from your local system.



3. Click **Upload** to upload the certificate.

   The information of the custom trusted certificate is displayed on the web user interface of the IP phone.



Note The information of built-in trusted certificates is not displayed on the web user interface of the IP phone.

To configure trusted certificates via web user interface:

1. Click on **Security**->**Trusted Certificates**.
2. Select the desired value from the pull-down list of **Only Accept Trusted Certificates**.
   - If **Enabled** is selected, the IP phone will verify the server certificate based on the trusted certificates list. Only when the authentication succeeds, the IP phone will trust the server.
   - If **Disabled** is selected, the IP phone will trust the server no matter whether the certificate received from the server is valid or not.
3. Select the desired value from the pull-down list of **Common Name Validation**.
   - If **Enabled** is selected, the IP phone will verify the CommonName or subjectAltName of the server certificate.
   - If **Disabled** is selected, the IP phone will not verify the CommonName or subjectAltName of the server certificate.
4. Select the desired value from the pull-down list of **CA Certificates**.
   - If **Default Certificates** is selected, the IP phone will verify the server certificate based on the built-in trusted certificates list.
   - If **Custom Certificates** is selected, the IP phone will verify the server certificate based on the custom trusted certificates list.
   - If **All Certificates** is selected, the IP phone will verify the server certificate based on the trusted certificates list, which contains built-in and custom trusted certificates.
5. Click **Confirm** to accept the change.

Configuring Trusted Certificate Using Configuration Files

The following IP phones use the new auto provisioning mechanism:

- SIP-T58A/CP960 IP phones running firmware version 80 or later
- SIP-T48G/T48S/T46G/T46S/T42G/T42S/T41P/T41S/T40P/T40G/T29G/T27G/T23P/T23G/T21(P) E2/T19(P) E2, CP860, CP920, W60P, W52P and W56P IP phones running firmware version 81 or later
- VP59, W53P and CP930W-Base IP phones running firmware version 83 or later
- SIP-T57W, SIP-T54W, SIP-T53W and SIP-T53 IP phones running firmware version 84 or later

Other IP phones or the IP phones listed above running old firmware version use the old auto provisioning mechanism.

For Old Auto Provisioning Mechanism

To configure trusted certificates using configuration files:

1. Add/Edit trusted certificates parameters in the configuration file (e.g., y000000000044.cfg).

   The following table lists the information of parameters:

Parameters	Permitted Values	Default
trusted_certificates.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom trusted certificate used to authenticate the connecting server. **Note:** The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format. **Web User Interface:** Security->Trusted Certificates->Load trusted certificates file **Phone User Interface:** None		
security.trust_certificates	**0 or 1**	**1**
Description: Enables or disables the IP phone to only trust the server certificates in the Trusted Certificates list. **0**-Disabled **1**-Enabled **Web User Interface:** Security->Trusted Certificates->Only Accept Trusted Certificates **Phone User Interface:** None		
security.cn_validation	**0 or 1**	**0**
Description: Enables or disables the IP phone to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server. **0-**Disabled **1-**Enabled **Web User Interface:** Security->Trusted Certificates->Common Name Validation **Phone User Interface:** None		

Parameters	Permitted Values	Default
security.ca_cert	**0, 1 or 2**	**2**
Description: Configures the type of certificates in the Trusted Certificates list for the IP phone to authenticate for TLS connection. **0**-Default Certificates **1**-Custom Certificates **2**-All Certificates **Web User Interface:** Security->Trusted Certificates->CA Certificates **Phone User Interface:** None		

The following shows an example of failover configurations for account 1 in the <y0000000000xx.cfg> configuration file:

trusted_certificates.url = http://192.168.1.20/tc.crt

security.trust_certificates = 1

security.cn_validation = 0

security.ca_cert = 2

2. Upload configuration files to the root directory of the provisioning server and trigger IP phones to perform an auto provisioning for configuration update.

   For more information on auto provisioning, refer to the latest Auto Provisioning Guide on Yealink Technical Support.

For New Auto Provisioning Mechanism

To configure trusted certificates using configuration files:

1. Add/Edit trusted certificates parameters in the configuration file (e.g., static.cfg).

   The following table lists the information of parameters:

Parameters	Permitted Values	Default
static.trusted_certificates.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom trusted certificate used to authenticate the connecting server. **Note:** The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format. **Web User Interface:**		

Parameters	Permitted Values	Default
Security->Trusted Certificates->Load Trusted Certificates File **Phone User Interface:** None		
static.security.trust_certificates	**0 or 1**	**1**
Description: Enables or disables the IP phone to only trust the server certificates in the Trusted Certificates list. **0**-Disabled **1**-Enabled **Web User Interface:** Security->Trusted Certificates->Only Accept Trusted Certificates **Phone User Interface:** None		
static.security.cn_validation	**0 or 1**	**0**
Description: Enables or disables the IP phone to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server. **0-**Disabled **1-**Enabled **Web User Interface:** Security->Trusted Certificates->Common Name Validation **Phone User Interface:** None		
static.security.ca_cert	**0, 1 or 2**	**2**
Description: Configures the type of certificates in the Trusted Certificates list for the IP phone to authenticate for TLS connection. **0**-Default Certificates **1**-Custom Certificates **2**-All Certificates **Web User Interface:** Security->Trusted Certificates->CA Certificates **Phone User Interface:** None		

The following shows an example of failover configurations for account 1 in the configuration file:

static.trusted_certificates.url = http://192.168.1.20/tc.crt

static.security.trust_certificates = 1

static.security.cn_validation = 0

static.security.ca_cert = 2

2. Reference the configuration file in the boot file (e.g., y000000000000.boot).

   Example:

   include:config "http://10.2.1.158/static.cfg"

3. Upload the boot file and configuration file to the root directory of the provisioning server.
4. Trigger IP phones to perform an auto provisioning for configuration update.

   For more information on auto provisioning, refer to the latest Auto Provisioning Guide on Yealink Technical Support.

Configuring Device Certificates on Yealink IP Phones

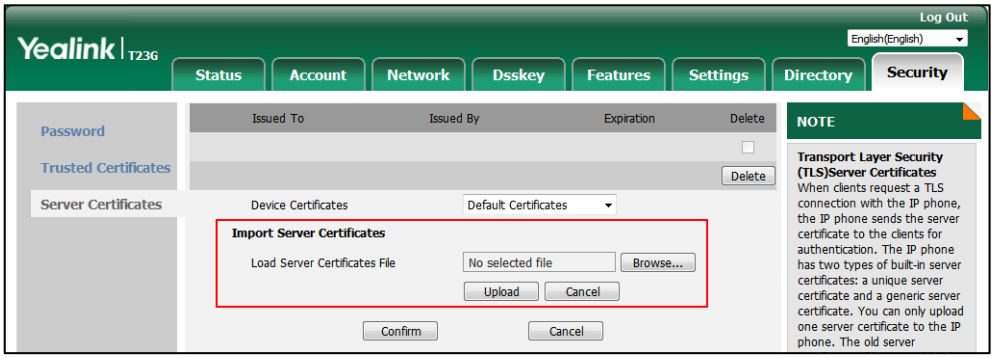
When a client requests an SSL connection with an IP phone, the IP phone sends a device certificate to the client for authentication. For new IP phones boxed with firmware version 72 or later, there are two built-in device certificates: a unique and a generic device certificate. For IP phones running firmware version prior to 72, there is only one built-in device certificate: a generic device certificate. The IP phone supports uploading one custom device certificate at most. The old custom device certificate will be overridden by the new one. For more information on customizing a device certificate, refer to Appendix C Creating Custom Certificates.

Configuring Device Certificates via Web User Interface

The followings take the SIP-T23G IP phone as examples.

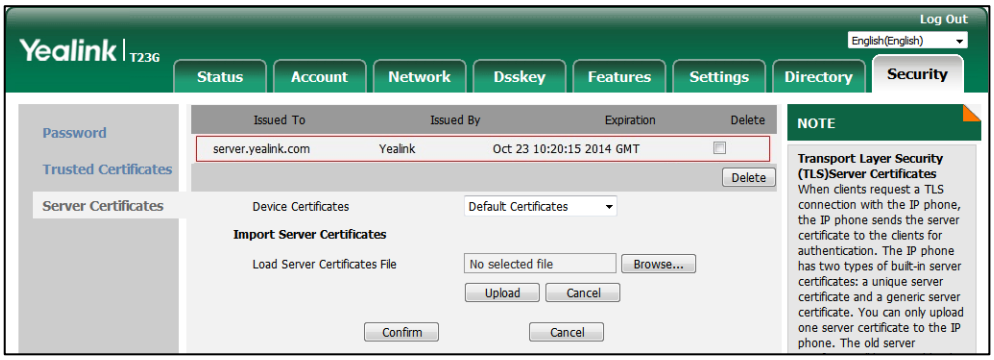
To upload a device certificate via web user interface:

1. Click on **Security**->**Server Certificates**.
2. Click **Browse** to locate the certificate (*.pem and *.cer) from your local system.



3. Click **Upload** to upload the certificate.

   The information of the custom device certificate is displayed on the web user interface of the IP phone.



Note The information of built-in device certificates is not displayed on the web user interface of the IP phone.

To configure device certificates via web user interface:

1. Click on **Security**->**Server Certificates**.
2. Select the desired value from the pull-down list of **Device Certificates**.
   - If **Default Certificates** is selected, the IP phone will send the unique or the generic device certificate to clients for authentication.
   - If **Custom Certificates** is selected, the IP phone will send custom certificates to clients for authentication.
3. Click **Confirm** to accept the change.

Configuring Device Certificates Using Configuration Files

The following IP phones use the new auto provisioning mechanism:

- SIP-T58A/CP960 IP phones running firmware version 80 or later
- SIP-T48G/T48S/T46G/T46S/T42G/T42S/T41P/T41S/T40P/T40G/T29G/T27G/T23P/T23G/T21(P) E2/T19(P) E2, CP860, CP920, W60P, W52P and W56P IP phones running firmware version 81 or later
- VP59, W53P and CP930W-Base IP phones running firmware version 83 or later
- SIP-T57W, SIP-T54W, SIP-T53W and SIP-T53 IP phones running firmware version 84 or later

Other IP phones or the IP phones listed above running old firmware version use the old auto provisioning mechanism.

For Old Auto Provisioning Mechanism

To configure device certificates using configuration files:

1. Add/Edit device certificates parameters in the configuration file (e.g., y000000000044.cfg).

   The following table lists the information of parameters:

Parameters	Permitted Values	Default
server_certificates.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the certificate the IP phone sends for authentication. **Note:** The certificate you want to upload must be in *.pem or *.cer format. **Web User Interface:** Security->Server Certificates->Load server cer file **Phone User Interface:** None		
security.dev_cert	**0 or 1**	**0**
Description: Configures the type of the device certificates for the IP phone to send for TLS authentication. **0**-Default Certificates **1**-Custom Certificates **Web User Interface:** Security->Server Certificates->Device Certificates **Phone User Interface:** None		

   The following shows an example of failover configurations for account 1 in the <y0000000000xx.cfg> configuration file:

   server_certificates.url = http://192.168.1.20/ca.pem

   security.dev_cert = 0

2. Upload configuration files to the root directory of the provisioning server and trigger IP phones to perform an auto provisioning for configuration update.

   For more information on auto provisioning, refer to the latest Auto Provisioning Guide on Yealink Technical Support.

For New Auto Provisioning Mechanism

To configure device certificates using configuration files:

1. Add/Edit device certificates parameters in configuration files.

The following table lists the information of parameters:

Parameters	Permitted Values	Default
static.server_certificates.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the certificate the IP phone sends for authentication. **Note:** The certificate you want to upload must be in *.pem or *.cer format. **Web User Interface:** Security->Server Certificates->Load Server Certificates File **Phone User Interface:** None		
static.security.dev_cert	**0 or 1**	**0**
Description: Configures the type of the device certificates for the IP phone to send for TLS authentication. **0**-Default Certificates **1**-Custom Certificates **Web User Interface:** Security->Server Certificates->Device Certificates **Phone User Interface:** None		

The following shows an example of failover configurations for account 1 in the <y0000000000xx.cfg> configuration file:

static.server_certificates.url = http://192.168.1.20/ca.pem

static.security.dev_cert = 0

2. Reference the configuration file in the boot file (e.g., y000000000000.boot).

   Example:

   include:config "http://10.2.1.158/static.cfg"

3. Upload the boot file and configuration file to the root directory of the provisioning server.
4. Trigger IP phones to perform an auto provisioning for configuration update.

   For more information on auto provisioning, refer to the latest Auto Provisioning Guide on Yealink Technical Support.

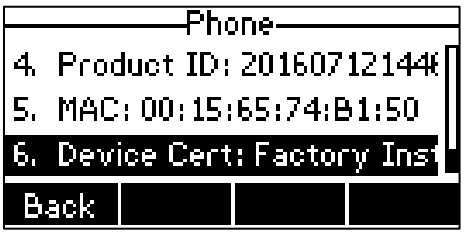
Using Certificates on Yealink IP Phones

Certificates are used in mutual TLS authentication. It allows the server and the IP phone to authenticate each other. This could be used for tasks like HTTPS provisioning or SIPs signaling.

If you intend to use certificates on Yealink IP phones, they must exist on the IP phones. Certificates issued by Yealink Certificate Authority (CA) are pre-loaded on Yealink IP phones and a custom certificate can be uploaded to Yealink IP phones. You can check whether a built-in device certificate is installed on your phone via web/phone user interface. A built-in device certificate can be either a unique certificate (based on the MAC address) or a generic certificate. Each certificate is issued by the Yealink Certificate Authority (CA), so a server can verify that a device is truly a Yealink device (not a malicious device or software masquerading as a Yealink device).

To check whether a built-in device certificate is installed on your phone via phone user interface:

1. Press **OK** or **Menu**->**Status**.
2. Press (▾) to scroll to **More** and then press the **Enter** soft key.
3. Select **Phone**.
4. Press (▾) to scroll to **Device Cert** and read status.



- If the status is **Factory Installed**, it means there is a valid device certificate installed on your phone. If your IP phone is running firmware version 71, the valid certificate is a generic certificate. If your IP phone is running firmware version 72 or later, the valid certificate is a unique certificate.

- If the status is **Not Installed**, it means there is no valid device certificate installed on your phone.

Note

The followings you need to know:

- It is not possible to modify or delete the built-in device certificates.
- Resetting the IP phone to factory defaults will not affect the built-in device certificates at all. The built-in device certificates and associated private keys are stored on the IP phone in its non-volatile memory as part of the manufacturing process.
- Resetting the IP phone to factory defaults will delete custom certificates by default. But this feature is determined by the value of the parameter "phone_setting.reserve_certs_enable" or "static.phone_setting.reserve_certs_enable". It is only applicable to SIP-T48G/T46G/T42G/T41P IP phones running firmware version 73 or later and SIP VP-T49G/T40P/T29G/T23P/T23G/T21(P) E2/T19(P) E2/CP860 IP phones running firmware version 80 or later. The parameter "static.phone_setting.reserve_certs_enable" is only applicable to CP960/SIP-T58A and SIP-T57W/T54W/T53W/T53/T48G/T48S/T46G/T46S/T42G/T42S/T41P/T41S/T40P/T40G/T29G/T27G/T23P/T23G/T21(P) E2/T19(P) E2, CP860, CP920, W60P, W52P and W56P IP phones running firmware version 81 or later, VP59, W53P and CP930W-Base IP phones running firmware version 83 or later.
- Resetting the IP phone to factory defaults will reset trusted and server certificates settings by default. But this feature is determined by the value of the parameter "phone_setting.reserve_certs_config.enable". It is only applicable to IP phones running firmware version 83 or later.
- Firmware upgrade from version 71 to 72 will result in update of the generic device certificate.

When the IP phone initiates an SSL connection, we consider it as a client. The server will send its certificate to the IP phone and the IP phone verifies this certificate. If "Mutual TLS Authentication Required" is enabled on your server, the IP phone should send its certificate to the server as well. The client certificate is the same as the server certificate.

The following shows a scenario of a mutual TLS authentication. In this scenario, the IP phone acts as a client and connects to the HTTPS server for provisioning.

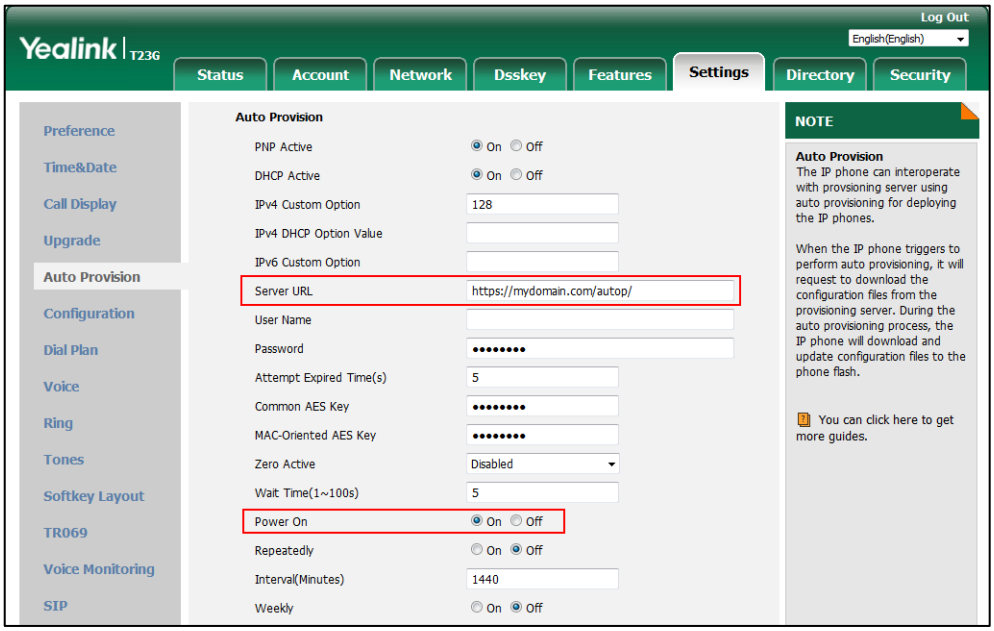
To use custom device certificates for mutual TLS authentication:

1. Create CA, server and client certificates. For more information, refer to Appendix C Creating Custom Certificates.
2. Install CA and server certificates on your server. For more information, refer to the online resource.
3. Upload a CA certificate (trusted certificate) and a client certificate (device certificate) on your IP phone. For more information, refer to Configuring Trusted Certificates on Yealink IP Phones and Configuring Device Certificates on Yealink IP Phones.
4. Check if **Only Accept Trusted Certificates** option has been enabled on the IP phone.
   - If Yes, go to step 5.
   - If No, please enable **Only Accept Trusted Certificates** option. For more information, refer to Configuring Trusted Certificates on Yealink IP Phones.
5. Check if **CA Certificates** option has been configured as **Custom Certificates** or **All Certificates** on the IP phone.

- If Yes, go to step 6.
- If No, please configure **CA Certificates** option. For more information, refer to Configuring Trusted Certificates on Yealink IP Phones.

6. Check if **Device Certificates** option has been configured as **Custom Certificates** on the IP phone.
   - If Yes, go to step 7.
   - If No, please configure **Device Certificates** option. For more information, refer to Configuring Device Certificates on Yealink IP Phones.
7. Make sure that "Mutual TLS Authentication Required" is enabled on your server.
8. Make sure that auto provisioning URL on the IP phone begins with https, e.g., "https://mydomain.com/autop/".
9. Configure auto provisioning settings. For example, mark the **On** radio box in the **Power On** field, and then reboot the IP phone. The IP phone will perform auto provisioning with mutual TLS authentication.

For more information on auto provisioning, refer to the latest Auto Provisioning Guide on Yealink Technical Support.



Appendix A X.509 Certificate Structure

An X.509 digital certificate is a digitally signed statement. The X.509 standard defines what information can go into a certificate.

The following table describes fields of a X.509 certificate:

Field	Description
Version	Identifies the version of the certificate. It must be version 3 if extensions are present. Most currently valid X.509 certificates follow version 3.
Serial number	Identifies a unique serial number per certificate.
Signature	Identifies the algorithm used by the Certificate Authority (CA) to sign the certificate.
Issuer	Identifies the entity that has issued the certificate.
Validity	Identifies a period during which the CA warrants that it will maintain information about the status of the certificate.
Subject	Identifies the entity associated with the public key stored in the subject public key information field.
Subject Public Key Information	Carries the public key and identifies the algorithm with which the key is used.
Extensions	Define a sequence of one or more certificate extensions that cover information about keys and procedures, attributes of owners and issuers, and constraints of the certificate path. They appear only if the version is 3.

Appendix B Trusted Certificate Authority List

Yealink IP phones trust the following CAs by default:

1. DigiCert High Assurance EV Root CA
2. Deutsche Telekom Root CA 2
3. Equifax Secure Certificate Authority
4. Equifax Secure eBusiness CA-1
5. Equifax Secure Global eBusiness CA-1
6. GeoTrust Global CA
7. GeoTrust Global CA2
8. GeoTrust Primary Certification Authority
9. GeoTrust Primary Certification Authority G2
10. GeoTrust Universal CA
11. GeoTrust Universal CA2
12. Thawte Personal Freemail CA
13. Thawte Premium Server CA

14. Thawte Primary Root CA
15. Thawte Primary Root CA - G2
16. Thawte Primary Root CA - G3
17. Thawte Server CA
18. VeriSign Class 1 Public Primary Certification Authority
19. VeriSign Class 1 Public Primary Certification Authority - G2
20. VeriSign Class 1 Public Primary Certification Authority - G3
21. VeriSign Class 2 Public Primary Certification Authority - G2
22. VeriSign Class 2 Public Primary Certification Authority - G3
23. VeriSign Class 3 Public Primary Certification Authority
24. VeriSign Class 3 Public Primary Certification Authority - G2
25. VeriSign Class 3 Public Primary Certification Authority - G3
26. VeriSign Class 3 Public Primary Certification Authority - G4
27. VeriSign Class 3 Public Primary Certification Authority - G5
28. VeriSign Class 4 Public Primary Certification Authority - G2
29. VeriSign Class 4 Public Primary Certification Authority - G3
30. VeriSign Universal Root Certification Authority
31. ISRG Root X1 (Let's Encrypt Authority X1 and Let's Encrypt Authority X2 certificates are signed by the root certificate ISRG Root X1.)

Note SIP-T48G/T46G/T42G/T41P/T40P/T29G/T23P/T23G/T21(P) E2/T19(P) E2 IP phones running firmware version earlier than X.80.0.95 do not support ISRG Root X1, Let's Encrypt Authority X1 and Let's Encrypt Authority X2 certificates.

32. Baltimore CyberTrust Root
33. DST Root CA X3
34. Verizon Public SureServer CA G14-SHA2

Note SIP-T48G/T46G/T42G/T41P/T40P/T29G/T23P/T23G/T21(P) E2/T19(P) E2 IP phones running firmware version earlier than X.80.0.130 do not support Baltimore CyberTrust Root, DST Root CA X3 and Version Public SureServer CA G14-SHA2 certificates.

35. AddTrust External CA Root
36. Go Daddy Class 2 Certification Authority
37. Class 2 Primary CA
38. Cybertrust Public SureServer SV CA
39. DigiCert Assured ID Root G2
40. DigiCert Assured ID Root G3

41. DigiCert Assured ID Root CA

42. DigiCert Global Root G2

43. DigiCert Global Root G3

44. DigiCert Global Root CA

45. DigiCert Trusted Root G4

46. Entrust Root Certification Authority

47. Entrust Root Certification Authority - G2

48. Entrust.net Certification Authority (2048)

49. GeoTrust Primary Certification Authority - G3

50. GlobalSign Root CA

51. GlobalSign Root CA - R2

52. Starfield Root Certificate Authority - G2

53. TC TrustCenter Class 2 CA II

54. TC TrustCenter Class 3 CA II

55. TC TrustCenter Class 4 CA II

56. TC TrustCenter Universal CA I

57. TC TrustCenter Universal CA III

58. Thawte Universal CA Root

59. VeriSign Class 3 Secure Server CA - G2

60. VeriSign Class 3 Secure Server CA – G3

61. Thawte SSL CA

62. StartCom Certification Authority

63. StartCom Certification Authority G2

64. Starfield Services Root Certificate Authority - G2

65. RapidSSL CA

66. Go Daddy Root Certificate Authority - G2

67. Cybertrust Global Root

68. COMODOSSLCA

69. COMODO RSA Domain Validation Secure Server CA

70. COMODO RSA Certification Authority

71. AmazonRootCA4

72. AmazonRootCA3

73. AmazonRootCA2

74. AmazonRootCA1

75. Yealink Root CA

76. Yealink Equipment Issuing CA

Note SIP-T48G/T48S/T46G/T46S/T42G/T42S/T41P/T41S/T40P/T40G/T29G/T27G/T23P/T23G/T21(P) E2/T19(P) E2 IP phones running firmware version earlier than X.81.0.15, and CP860/W52P/W56P IP phones running firmware version earlier than X.81.0.10 do not support the certificates from 35 to 76.

77. SIP Core

Note SIP-T48G/T48S/T46G/T46S/T42G/T42S/T41P/T41S/T40P/T40G/T29G/T27G/T23P/T23G/T21(P) E2/T19(P) E2 IP phones running firmware version earlier than X.82.0.10, do not support the certificates 77.

78. (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.

79. AAA Certificate Services

80. AC Raíz Certicámara S.A.

81. ACCVRAIZ1

82. ACEDICOM Root

83. Actalis Authentication Root CA

84. AddTrust Class 1 CA Root

85. AddTrust Public CA Root

86. AddTrust Qualified CA Root

87. AffirmTrust Commercial

88. AffirmTrust Networking

89. AffirmTrust Premium

90. AffirmTrust Premium ECC

91. America Online Root Certification Authority 1

92. America Online Root Certification Authority 2

93. ApplicationCA

94. Atos TrustedRoot 2011

95. A-Trust-nQual-03

96. Autoridad de Certificacion Firmaprofesional CIF A62634068

97. Buypass Class 2 CA 1

98. Buypass Class 2 Root CA

99. Buypass Class 3 CA 1

100. Buypass Class 3 Root CA

101. CA Disig

102. CA Disig Root R1

103. CA Disig Root R2

104. Certigna

105. Certinomis - Autorité Racine

106. certSIGN ROOT CA

107. Certum CA

108. Certum Trusted Network CA

109. Chambers of Commerce Root

110. Chambers of Commerce Root - 2008

111. China Internet Network Information Center EV Certificates Root

112. CNNIC ROOT

113. COMODO Certification Authority

114. COMODO ECC Certification Authority

115. ComSign Secured CA

116. DST ACES CA X6

117. D-TRUST Root Class 3 CA 2 2009

118. D-TRUST Root Class 3 CA 2 EV 2009

119. EBG Elektronik Sertifika Hizmet Sağlayıcısı

120. EC-ACC

121. EE Certification Centre Root CA

122. e-Guven Kok Elektronik Sertifika Hizmet Saglayicisi

123. Entrust Root Certification Authority - EC1

124. Entrust.net Secure Server Certification Authority

125. ePKI Root Certification Authority

126. E-Tugra Certification Authority

127. FNMT Clase 2 CA

128. Global Chambersign Root

129. Global Chambersign Root – 2008

130. GlobalSign Root CA - R3

131. Government Root Certification Authority

132. GTE CyberTrust Global Root

133. Hellenic Academic and Research Institutions RootCA 2011

134. Hongkong Post Root CA 1

135. IGC/A

136. Izenpe.com

137. Juur-SK

138. KISA RootCA 1

139. KISA RootCA 3

140. Microsec e-Szigno Root CA

141. Microsec e-Szigno Root CA 2009

142. NetLock Arany (Class Gold) Főtanúsítvány

143. NetLock Expressz (Class C) Tanusitvanykiado

144. NetLock Kozjegyzoi (Class A) Tanusitvanykiado

145. NetLock Uzleti (Class B) Tanusitvanykiado

146. Network Solutions Certificate Authority

147. OISTE WISeKey Global Root GA CA

148. QuoVadis Root CA 2

149. QuoVadis Root CA 3

150. QuoVadis Root Certification Authority

151. Root CA Generalitat Valenciana

152. RSA Security 2048 V3

153. Secure Certificate Services

154. Secure Global CA

155. SecureSign RootCA11

156. SecureTrust CA

157. Security Communication EV RootCA1

158. Security Communication RootCA1

159. Security Communication RootCA2

160. Sonera Class2 CA

161. Staat der Nederlanden Root CA

162. Staat der Nederlanden Root CA - G2

163. Starfield Class 2 Certification Authority

164. Swisscom Root CA 1

165. Swisscom Root CA 2

166. Swisscom Root EV CA 2

167. SwissSign Gold CA - G2

168. SwissSign Silver CA - G2

169. TDC Internet Root CA

170. TeliaSonera Root CA v1

171. Trusted Certificate Services

172. Trustis FPS Root CA

173. T-TeleSec GlobalRoot Class 3

174. TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3

175. TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. (c) Aralık 2007

176. TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. (c) Kasım 2005

177. TWCA Global Root CA

178. TWCA Root Certification Authority

179. UTN - DATACorp SGC

180. UTN-USERFirst-Hardware

181. ValiCert Class 1 Policy Validation Authority

182. ValiCert Class 2 Policy Validation Authority

183. ValiCert Class 3 Policy Validation Authority

184. Visa eCommerce Root

185. Wells Fargo Root Certificate Authority

186. WellsSecure Public Root Certificate Authority

187. XRamp Global Certification Authority

Note Yealink endeavors to maintain a built-in list of the most commonly used CA Certificates. Due to memory constraints, we cannot ensure a complete set of certificates. If you are using a certificate from a commercial Certificate Authority not in the list above, you can send a request to your local distributor. At this point, you can upload your particular CA certificate into your phone. For more information on uploading a custom CA certificate, refer to Configuring Trusted Certificates on Yealink IP Phones.

The certificates from 78 to 187 are only applicable to VP59/SIP-T58A/CP960 IP phones.

Appendix C Creating Custom Certificates

You can create and use your own CA to issue certificates. This requires a tool that supports SSL and TLS protocols. We recommend you to use OpenSSL on Linux. The OpenSSL software is available for free online: http://www.openssl.org/source/. If Windows is required, we recommend you to use the apache server with OpenSSL. The software is available for free online: http://httpd.apache.org/download.cgi. Be sure to install OpenSSL before you read the following instructions. For more information, refer to the network resource.

This appendix includes information on:

- Creating a self-signed CA
- Issuing certificates

To create a self-signed CA:

1. Open a terminal window.
2. Execute the following command to create a RSA private key for your CA:

   [root@localhost openssl-0.9.8k]#openssl genrsa -out ca.key 1024

   Generating RSA private key, 1024 bit long modulus

   .....++++++

   .....++++++

e is 65537 (0x10001)

The command will generate a **ca.key** file.

3. Execute the following command to create a self-signed CA certificate with the RSA private key:

[root@localhost openssl-0.9.8k]#openssl req -new -x509 -days 3650 -key ca.key -out ca.crt

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank. For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [US]:CN

State or Province Name (full name) [Wisconsin]:FJ

Locality Name (eg, city) [Madison]:XM

Organization Name (eg, company) [My Company Ltd]: Yealink

Organizational Unit Name (eg, section) []:

Common Name (eg, your name or your server's hostname) []:Yealink CA

Email Address []:support@yealink.com

You will be prompted to enter a few attributes (e.g., State, organization or Common Name (CN)). The command will generate a self-signed X.509 certificate valid for ten years (3650 days).

You can execute the following command to see the details of this certificate.

[root@localhost openssl-0.9.8k]#openssl x509 -noout -text -in ca.crt

A server certificate is a digital certificate issued to a server by a CA. It verifies the server's identity for the client so that the client can securely browse the server. After the server certificate is issued, you need to install the certificate on the server.

To issue a server certificate:

1. Open a terminal window.
2. Execute the following command to create a RSA private key for your server:

[root@localhost openssl-0.9.8k]#openssl genrsa -out server.key 1024

Generating RSA private key, 1024 bit long modulus

.....++++++

.....++++++

e is 65537 (0x10001)

The command will generate a **server.key** file.

3. Execute the following command to create a server Certificate Signing Request (CSR) with the server RSA private key:

[root@localhost openssl-0.9.8k]# openssl req -new -key server.key -out server.csr

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank. For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [US]:CN

State or Province Name (full name) [Wisconsin]:FJ

Locality Name (eg, city) [Madison]:XM

Organization Name (eg, company) [My Company Ltd]:Yealink

Organizational Unit Name (eg, section) []:

Common Name (eg, your name or your server's hostname) []:server.yealink.com

Email Address []:support@yealink.com

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:1234567890

An optional company name []:

You will be prompted to enter a few attributes (e.g., State, organization or Common Name (CN)). The command will generate a **server.csr** file.

Note The Common Name (CN) in the server certificate must match the name supplied as the server. This is because the IP phone does not perform a DNS lookup, but only performs a simple string comparison. The use of an IP address is also valid.

4. Execute the following command to issue your server certificate with ca.crt and ca.key generated above:

   [root@localhost openssl-0.9.8k]#openssl x509 -days 365 -CA ca.crt -CAkey ca.key -req -CAcreateserial -CAserial ca.srl -in server.csr -out server.crt

   Signature ok

   subject=/C=CN/ST=FJ/L=XM/O=Yealink/CN=server.yealink.com/emailAddress=support@yealink.com

   Getting CA Private Key

   The command will generate a X.509 server certificate valid for one year (365 days).

You can execute the following command to view the details of this certificate.

[root@localhost openssl-0.9.8k]#openssl x509 -text -in server.crt

A client certificate is a digital certificate issued to a client by a CA. Client certificate issue steps are very similar to server certificate. Remember to specify a unique CN.

Execute the following commands to issue a client certificate:

[root@localhost openssl-0.9.8k]#openssl genrsa -out client.key 1024

[root@localhost openssl-0.9.8k]#openssl req -new -key client.key -out client.csr

[root@localhost openssl-0.9.8k]#openssl x509 -days 365 -CA ca.crt -CAkey ca.key -req -CAcreateserial -CAserial ca.srl -in client.csr -out client.crt

These commands will generate a client.key file, a client.csr file and a client.crt file.

If the mutual TLS authentication is required, you need to generate a *.pem certificate and upload it to the IP phone.

Execute the following command to generate a client.pem file with client.crt and client.key files generated above:

[root@localhost openssl-0.9.8k]#cat client.crt client.key > client.pem

Customer Feedback

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocsFeedback@yealink.com.