

Using Device Certificates on Htek IP Phones

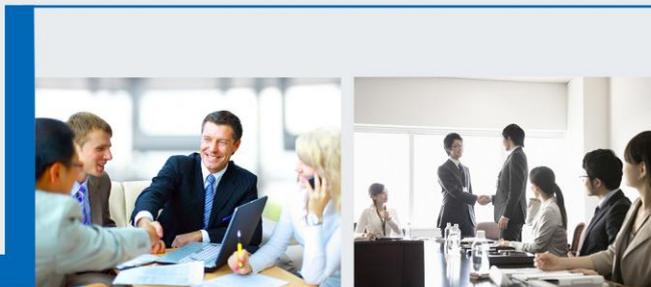


Table of Content

Introduction	3
Configuring Trusted CA	4
To upload a trusted CA via web user interface.....	4
To configure trusted CA via web user interface.....	5
Configuring Device Certificates.....	5
To upload a device certificate via web user interface	6
Configuring device certificates by web interface	6
Using Certificates OnHtek Phone	7
Check built-in device certificate	7
Using custom device certificates.....	8
Creating Custom Certificates.....	9
To create a self-signed CA	9
To issue a server certificate.....	10
To issue a client certificate	11

Introduction

Device Certificates are an important element in deploying a solution that ensures the integrity and privacy of communications involving UC8xx devices.

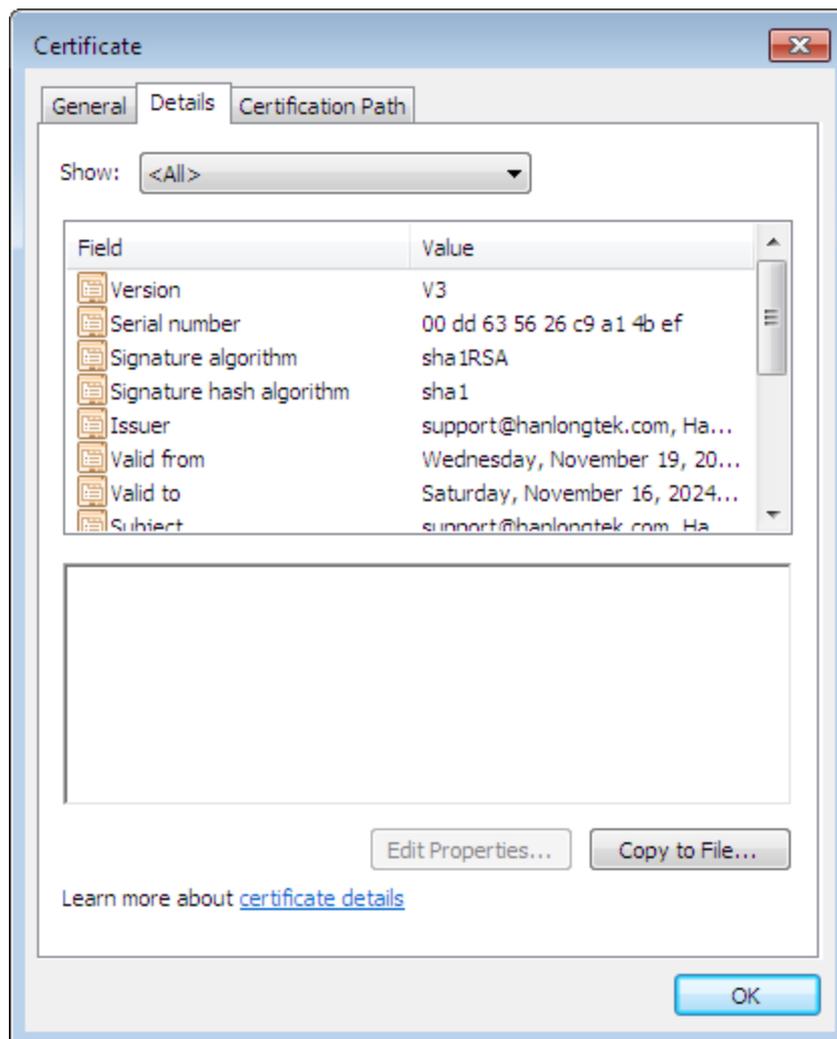
Mutual TLS Authentication allows a server to verify that a device is truly aHtek phone (and not a malicious endpoint or software masquerading as a Htek phone). This could be used for tasks like provisioning or SIP signaling using TLS signaling.

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

This guide applies to Htek UC8xx IP phones running firmware version 1.0.3.73 or later.

Please Note: The IP phone does not have the unique device certificate by upgrading firmware version to 1.0.3.73.

The following shows an example of aHtek generic certificate.



Please Note: In the feature profile, we use the terms CA and device certificates. These

are also known as server and client certificates.

Configuring Trusted CA

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 IP phone supports uploading 10 custom trusted certificates (CA certificates) at most.

To upload a trusted CA via web user interface

1. Click on Management->Trusted CA.

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.

2. Click Browse to locate the certificate (*.pem, *.crt) from your local system.

The screenshot shows the Htek web user interface. The top navigation bar includes links for Home, Account, Network, Function Keys, Setting, Directory, and Management. A sidebar on the left contains menu items: Password, Upgrade, Auto Provision, Configuration, Trusted CA (highlighted), Server CA, Tools, Restart, and Reboot. The main content area features a table with columns for Index, Issued TO, Issued By, and Expiration, containing 10 rows. Below the table is a 'Delete' button. A dialog box titled 'Import Trusted Certificates' is open, showing a text input field with the path 'D:\Apache2.2\conf\ca.crt' and a 'Browse...' button. Below the input field, there are radio buttons for 'Default Certificates' (selected), 'Custom Certificates', and 'All Certificates'. At the bottom of the dialog are 'SaveSet' and 'Cancel' buttons. A 'NOTE' section on the right provides instructions for password and trusted CA management.

3. Click “Import Trusted Certificates” to upload the certificate.

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

The screenshot shows the Htek web management interface. At the top, there is a navigation bar with the Htek logo and links for Home, Account, Network, Function Keys, Setting, Directory, and Management. A 'logout' link is also present. On the left, a vertical menu contains options: Password, Upgrade, Auto Provision, Configuration, Trusted CA (highlighted), Server CA, Tools, Restart, and Reboot. The main content area features a table of trusted certificates with columns for Index, Issued TO, Issued By, and Expiration. The first row is highlighted with a red border. Below the table is a 'Delete' button. Further down, there are fields for 'Import Trusted Certificate Files' with a 'Browse...' button, an 'Import Trusted Certificates' button, and radio buttons for 'Trusted Certificates' (Default Certificates, Custom Certificates, All Certificates). At the bottom, there are 'SaveSet' and 'Cancel' buttons. On the right side, a 'NOTE' section contains information about password modification and trusted CA file import.

Index	Issued TO	Issued By	Expiration	
1	Hanlongtek	Hanlong	Nov 18 02:38:24 2024 GMT	<input type="checkbox"/>
2				<input type="checkbox"/>
3				<input type="checkbox"/>
4				<input type="checkbox"/>
5				<input type="checkbox"/>
6				<input type="checkbox"/>
7				<input type="checkbox"/>
8				<input type="checkbox"/>
9				<input type="checkbox"/>
10				<input type="checkbox"/>

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

To configure trusted CA via web user interface

1. Click on Security->Trusted Certificates.
2. Select the desired value from list of Trusted Certificates.
 - If “Default Certificates” is checked, the IP phone will verify the server certificate based on built-in trusted certificates list.
 - If “Custom Certificates” is checked, the IP phone will verify the server certificate based on the custom trusted certificates list.
 - If “All Certificates” is checked, the IP phone will verify the server certificate based on the trusted certificates list, which contains built-in and custom trusted certificates.
3. Click “SaveSet” to accept the change.

Configuring Device Certificates

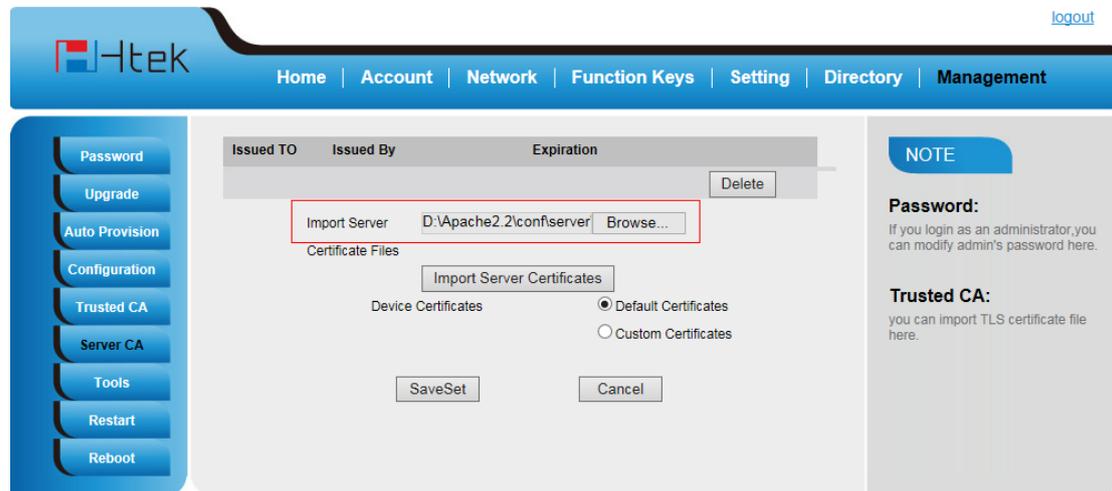
When a client requests an SSL connection with an IP phone, the IP phone sends a device certificate to the client for authentication. For new IP phones boxed with firmware version 1.0.3.73 or later, there is a unique device certificate. For IP phones running firmware version prior to 1.0.3.73, there isn't built-in 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.

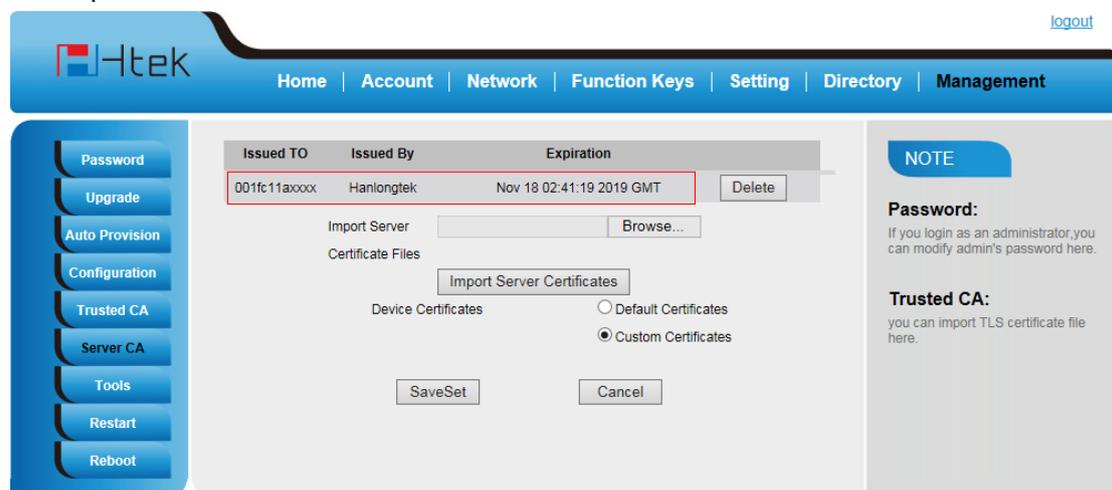
To upload a device certificate via web user interface

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



3. Click “Import Server Certificates” to upload the certificate.

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



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

Configuring device certificates by web interface

1. Click on Management->Server CA.
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.

Using Certificates OnHtek Phone

Certificates can be used in mutual TLS authentication. It allows the server and the phone to authenticate each other. This could be used for tasks like HTTPS provisioning or SIP. If you intend to use certificates on Htek IP phones, they must exist on the IP phones.

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

Certificates issued by Htek Certificate Authority (CA) are pre-loaded on Htek IP phones and a custom certificate can be uploaded to Htek IP phones. You can check whether a built-in device certificate is installed on your phone via phone user interface only. Server can verify that a device is truly aHtek device (not a malicious device or software masquerading as a Htek device).

Check built-in device certificate

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

1. Press OK or Menu->Status.
 2. Select Information.
 3. Press“DownKey” 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.



Information	
2.IP:	192.168.0.127
3.MAC:	00:1f:c1:1a:b5:80
4.Firmware(IMG):	 1.0.3.73(2014-11-25 10..
5.Firmware(BOOT):	 1.0.3.35(2014-10-16 13..
6.Firmware(ROM):	 1.0.3.73(2014-11-25 10..
7.Device Cert:	Factory Installed
Back	

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

Information	
2.IP:	192.168.0.127
3.MAC:	00:1f:c1:1a:b5:80
4.Firmware(IMG):	 1.0.3.73(2014-11-25 10..
5.Firmware(BOOT):	 1.0.3.35(2014-10-16 13..
6.Firmware(ROM):	 1.0.3.73(2014-11-25 10..
7.Device Cert:	Not Installed
Back	

Please Note:

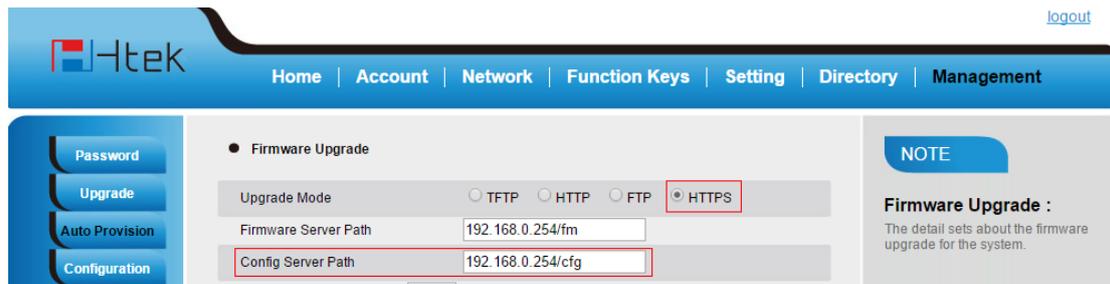
- It is not possible to modify or delete the built-in device certificates.
- Resetting the IP phone to factory defaults will not affect the built-in device certificates at all. The built-in device certificates and associated private keys are stored on the IP phone in its non-volatile memory as part of the manufacturing process.
- Resetting the IP phone to factory defaults will delete custom certificates by default.

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

Using custom device certificates

Using custom device certificates for mutual TLS authentication:

1. Create CA, server and client certificates. For more information, refer to “5. Creating Custom Certificates”.
2. Install CA and server certificates on your server.
3. Upload a CA certificate (trusted certificate) and a client certificate (device certificate) on your phone.
5. CA Certificates option has been configured as Custom Certificates or All Certificates on the IP phone.
6. Device Certificates option has been configured as Custom Certificates on the IP phone.
7. Make sure that “Mutual TLS Authentication Required” is enabled on your server.
8. Make sure that auto provisioning on the IP phone work with https:



9. Reboot the IP phone. The IP phone will perform auto provisioning with mutual TLS authentication.

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.

Here 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:

The command will generate a ca.key file.

```
[root@localhost openssl-1.0.1i]#opensslgenrsa -out ca.key 1024
```

```
Generating RSA private key, 1024 bit long modulus
```

```
.....++++++
```

```
.....++++++
```

```
e is 65537 (0x10001)
```

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

```
[root@localhost openssl-1.0.1i]#opensslreq -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]: **JS**
Locality Name (eg, city) [Madison]: **NJ**
Organization Name (eg, company) [My Company Ltd]: **Hanlong**
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []: **Hanlong CA**
Email Address []: **support@Hanlongtek.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-1.0.1i]#opensslx509 -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-1.0.1i]#opensslgenrsa -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-1.0.1i]# opensslreq -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]: **JS**
Locality Name (eg, city) [Madison]: **NJ**
Organization Name (eg, company) [My Company Ltd]: **Hanlong**
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []: **server.hanlongtek.com**
Email Address []: **support@hanlongtek.com**
Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:8616123456

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.

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-1.0.1i]#openssl x509 -req -days 365 -CA ca.crt -CAkeyca.key -CAcreateserial -CAserialca.srl -in server.csr -out server.crt
```

Signature ok

```
subject=/C=CN/ST=JS/L=NJ/O=Hanlong/CN=server.hanlongtek.com/emailAddress=support@hanlongtek.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-1.0.1i]#openssl x509 -text -in server.crt
```

To issue a client certificate

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-1.0.1i]#openssl genrsa -out client.key 1024
```

```
[root@localhost openssl-1.0.1i]#openssl req -new -key client.key -out client.csr
```

```
[root@localhost openssl-1.0.1i]#openssl x509 -req -days 365 -CA ca.crt -CAkeyca.key -CAcreateserial -CAserialca.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-1.0.1i]#cat client.crt client.key>client.pem
```