# Securing Algo IP Endpoints:

# TLS and Mutual Authentication

Need Help?

(604) 454-3792 or support@algosolutions.com

# Table of Contents

## Introduction to TLS

TLS (Transport Layer Security) is a cryptographic protocol that provides authentication, privacy, and end-to-end security of data sent between applications or devices over the Internet. As hosted telephony platforms have become more common, the need for TLS to provide secure communication over the public internet has increased. Algo devices that support firmware 1.6.4 or later support Transport Layer Security (TLS) for both Provisioning and SIP Signaling.

*Note: the following endpoints do not support TLS: 8180 IP Audio Alerter (G1), 8028 IP Doorphone (G1), 8128 IP Visual Alerter (G1), 8061 IP Relay Controller.*

## Encryption vs Identity Verification

While TLS traffic is always encrypted and safe from third-party eavesdropping or modification, an additional layer of security can be provided by using Certificates to verify the identity of the other party. This allows the Server to verify the identity of the IP Endpoint device, and vice-versa. To perform the identity check, the Certificate file must be signed by a Certificate Authority (CA). The other device then checks this signature, using the Public (Trusted) Certificate from this CA.

## TLS Certificates

Algo IP Endpoints come pre-installed with a set of public certificates from trusted third-party Certificate Authorities (CAs), including Comodo, Verisign, Symantec, DigiCert, etc. The Certificate Authorities provide signed certificates to businesses to allow these businesses to prove that their servers or websites are in fact who they say they are. Algo devices can confirm that it is communicating with an authentic server by verifying the server's signed certificates against the public certificates from the CA that signed it. Additional public certificates can also be uploaded, to allow the Algo device to trust and verify additional servers that may not be included in the preinstalled certificates (for example, self-signed certificates).

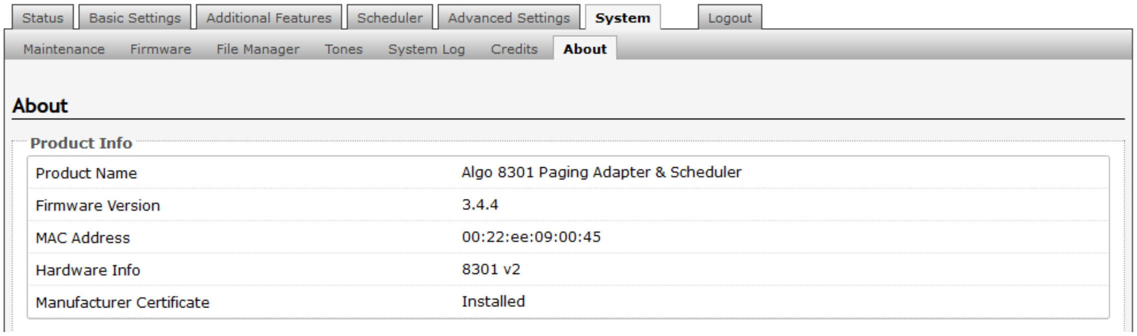
## Mutual Authentication

Mutual Authentication adds one additional layer of security by requiring the server to also validate and trust the endpoint device, in addition to the opposite direction of the endpoint validating the server. This is implemented using a unique Device Certificate, installed on each Algo SIP Endpoint at the time of manufacture. As the IP address of an Algo device is not fixed (it is determined by the customer's network), Algo cannot publish this information in advance with the trusted CAs, and instead these Device Certificates must be signed by Algo's own CA.

For the server to then trust the Algo device, the system administrator will need to install the public Algo CA certificate chain onto their server (for example the SIP Phone System or their provisioning server) so that this server can verify that the Device Certificate on the Algo device is in fact authentic.

Note: Algo IP endpoints manufactured in 2019 (starting with firmware 1.7.1) or later have the device certificate installed from factory.

To verify if the certificate is installed, navigate to System -> About tab. See the Manufacturer Certificate. If the certificate is not installed, please email support@algosolutions.com.



About

Product Info

| | |
|---|---|
| Product Name | Algo 8301 Paging Adapter & Scheduler |
| Firmware Version | 3.4.4 |
| MAC Address | 00:22:ee:09:00:45 |
| Hardware Info | 8301 v2 |
| Manufacturer Certificate | Installed |

## Cipher Suites

Cipher suites are sets of algorithms used during a TLS session. Each suite includes algorithms for authentication, encryption, and message authentication. Algo devices support many commonly used encryption algorithms such as AES256 and message authentication code algorithms such as SHA-2.

## Algo Device Certificates

Device Certificates signed by the Algo Root CA have been factory installed on Algo devices since 2019, starting with firmware 1.7.1. The certificate is generated when the device is manufactured, with the common name field in the certificate containing the MAC address for each device.

The device certificate is valid for 30 years and resides in a separate partition, so it will not be erased even after factory resetting the Algo endpoint.

Algo devices also support uploading your own device certificate to use instead of the factory installed device certificate. This can be installed by uploading a PEM file containing both a device certificate and a private key it to the 'certs' directory (not the 'certs/trusted' directory!) in System -> File Manager tab. This file needs to be called 'sipclient.pem'.

## Uploading Public CA Certificates to Algo SIP Endpoints

If you are on a firmware lower than 3.1.X, please upgrade the device.

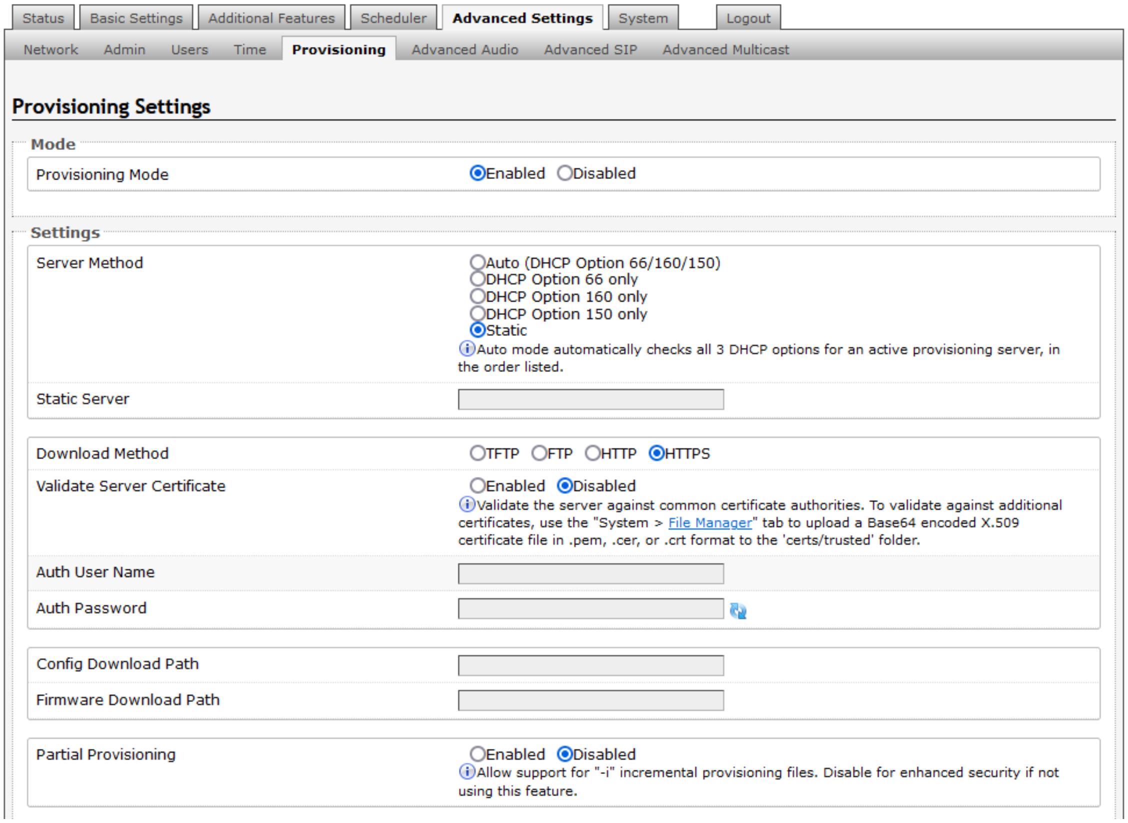
To install the certificate on an Algo device running firmware v3.1 & above, follow the steps below:

1. Obtain a public certificate from your Certificate Authority (any valid X.509 format certificate can be accepted). There is no specific format required for the filename.
2. In the web interface of the Algo device, navigate to the System -> File Manager tab.
3. Upload the certificate files into the 'certs/trusted' directory. Click the Upload button in the top left corner of the file manager and browse to the certificate.

# Web Interface Options

## HTTPS Provisioning

Provisioning can be secured by setting the ‘Download Method’ to ‘HTTPS’ (under the Advanced Settings > Provisioning tab). This prevents configuration files from being read by an unwanted third party. This resolves the potential risk of having sensitive data stolen, such as admin passwords and SIP credentials.



**Provisioning Settings**

**Mode**

Provisioning Mode ● Enabled ○ Disabled

**Settings**

Server Method
○ Auto (DHCP Option 66/160/150)
○ DHCP Option 66 only
○ DHCP Option 160 only
○ DHCP Option 150 only
● Static
ⓘ Auto mode automatically checks all 3 DHCP options for an active provisioning server, in the order listed.

Static Server

Download Method ○ TFTP ○ FTP ○ HTTP ● HTTPS

Validate Server Certificate ○ Enabled ● Disabled
ⓘ Validate the server against common certificate authorities. To validate against additional certificates, use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder.

Auth User Name

Auth Password

Config Download Path

Firmware Download Path

Partial Provisioning ○ Enabled ● Disabled
ⓘ Allow support for "-i" incremental provisioning files. Disable for enhanced security if not using this feature.

To perform identity verification on the Provisioning Server, also set ‘Validate Server Certificate’ to ‘Enabled’. If the provisioning server’s Certificate is signed by one of the common commercial CAs, then the Algo device should already have the public certificate for this CA and be able to perform the verification.

Upload additional certificates (Base64 encoded X.509 certificate file in .pem, .cer, or .crt format) by navigating to "System > File Manager" to the 'certs/trusted' folder.

**NOTE:** The ‘Validate Server Certificate’ parameter can also be enabled through provisioning: **prov.download.cert = 1**

## HTTPS Web Interface Protocol

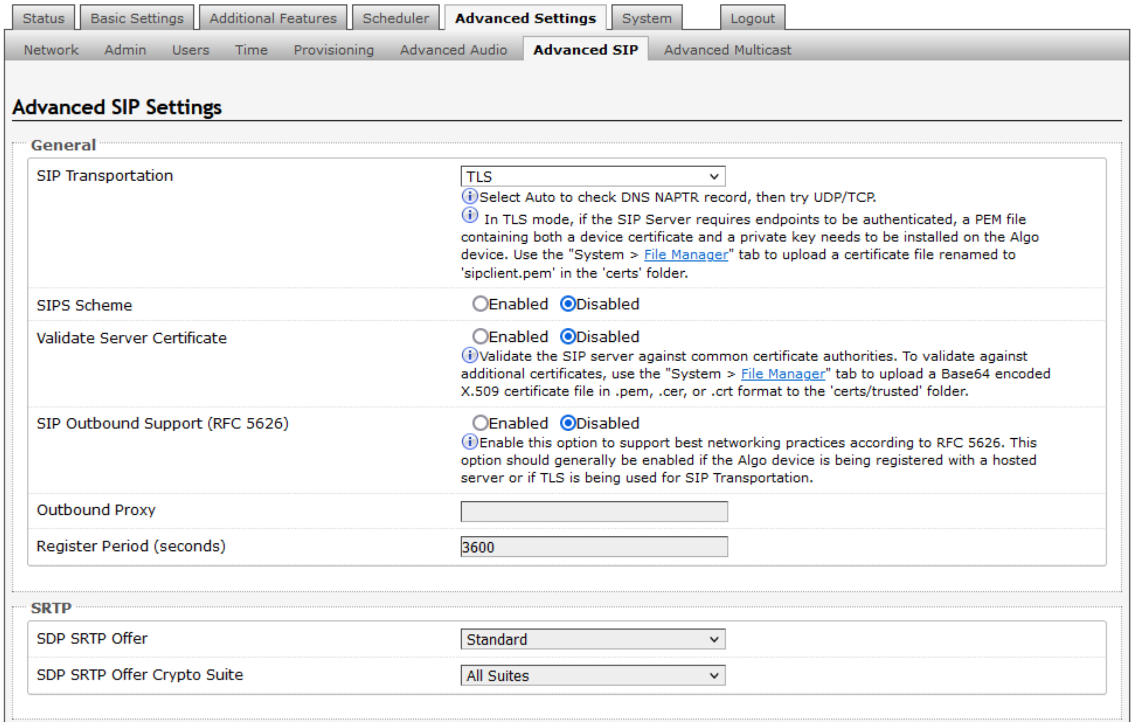
The procedure to upload a public certificate for HTTPS web browsing is similar as what's described in the section above. The httpd.pem file is a device certificate that is requested by your computer's browser when you navigate to the IP of the device. Uploading a custom one might let you get rid of the warning message if you access the WebUI using HTTPS. It's not a public CA certificate. The certificate must be uploaded to the ‘certs’.

```
-----BEGIN CERTIFICATE-----
<stuff goes here>
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
<more stuff here>
-----END PRIVATE KEY-----
```

## SIP Signalling (and RTP Audio)

SIP signaling is secured by setting ‘SIP Transportation’ to ‘TLS’ (under the Advanced Settings > Advanced SIP tab).

- It ensures that the SIP traffic will be encrypted.
- The SIP signaling is responsible for establishing the call (the control signals to start and end the call with the other party), but it does not contain the audio.
- For the audio (voice) path, use the setting ‘SDP SRTP Offer’.
- Setting this to ‘Optional’ means the SIP call’s RTP audio data will be encrypted (using SRTP) if the other party also supports audio encryption.
- If the other party does not support SRTP, then the call will still proceed, but with unencrypted audio. To make audio encryption mandatory for all calls, set ‘SDP SRTP Offer’ to ‘Standard’. In this case, if the other party does not support audio encryption, then the call attempt will be rejected.
- To perform identity verification on the SIP Server, also set ‘Validate Server Certificate’ to ‘Enabled’.
- If the SIP server’s Certificate is signed by one of the common commercial CAs, then the Algo device should already have the public certificate for this CA and be able to perform the verification. If not (for example with self-signed certificates), then the appropriate public certificate can be uploaded to the Algo device as described earlier in this document.



**Advanced SIP Settings**

General

| | |
|---|---|
| SIP Transportation | TLS<br>ⓘSelect Auto to check DNS NAPTR record, then try UDP/TCP.<br>ⓘ In TLS mode, if the SIP Server requires endpoints to be authenticated, a PEM file containing both a device certificate and a private key needs to be installed on the Algo device. Use the "System > File Manager" tab to upload a certificate file renamed to 'sipclient.pem' in the 'certs' folder. |
| SIPS Scheme | ○Enabled ●Disabled |
| Validate Server Certificate | ○Enabled ●Disabled<br>ⓘValidate the SIP server against common certificate authorities. To validate against additional certificates, use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder. |
| SIP Outbound Support (RFC 5626) | ○Enabled ●Disabled<br>ⓘEnable this option to support best networking practices according to RFC 5626. This option should generally be enabled if the Algo device is being registered with a hosted server or if TLS is being used for SIP Transportation. |
| Outbound Proxy | |
| Register Period (seconds) | 3600 |

SRTP

| | |
|---|---|
| SDP SRTP Offer | Standard |
| SDP SRTP Offer Crypto Suite | All Suites |

## TLS Version 1.2

Algo devices running firmware v3.1 & above support TLS v1.1 and v1.2. 'Force Secure TLS Version' option may be used to require TLS connections to use TLSv1.2. To enable this feature:

- Go to Advanced settings > Advanced SIP
- Set the 'Force secure TLS Version' as enabled and save.

**NOTE: This option has been removed in v4.0+ since TLS v1.2 is used by default**

## Algo Certificates Download

Below are a set of links to download the Algo CA certificate chain. The files can be installed on the SIP Server or Provisioning Server in order for these servers to authenticate the Device Certificates on Algo SIP Endpoints, and thus allow Mutual Authentication:

Algo Root CA: http://firmware.algosolutions.com/pub/certs/algo_issuing.crt

Algo Intermediate CA: http://firmware.algosolutions.com/pub/certs/algo_intermediate.crt

Algo Public Certificate: http://firmware.algosolutions.com/pub/certs/algo_ca.crt

## Troubleshooting

If the TLS handshake is not getting completed, please send a packet capture to Algo support for analysis. To do that you’ll have to mirror the traffic, from the port the Algo endpoint is connected to on the network switch, back to a computer.