TLS for SIP Signalling and HTTPS Provisioning

Need Help?

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

Algo Communication Products Ltd
4500 Beedie St Burnaby BC Canada V5J 5L2
www.algosolutions.com

(604) 454-3792
support@algosolutions.com

Table of Contents

Algo Communication Products Ltd
4500 Beedie St Burnaby BC Canada V5J 5L2
www.algosolutions.com
(604) 454-3792
support@algosolutions.com

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**.

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 in order to verify the identity of the other party. This allows the Server to verify the identity of the SIP 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 SIP Endpoints come pre-installed with a set of public certificates from trusted third-party Certificate Authorities (CAs), including Comodo, Versign, Symantec, DigiCert, etc. These companies provide signed certificates to businesses, in order for these businesses to prove that their servers or websites are in fact who they say they are. The Algo device 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 Algo devices, in order to allow the Algo device to trust and verify additional servers that may not be included in the pre-installed certificates (for example, self-signed certificates).

Algo Communication Products Ltd
4500 Beedie St Burnaby BC Canada V5J 5L2
www.algosolutions.com
(604) 454-3792
support@algosolutions.com

Mutual Authentication

In order to go one step further and support Mutual Authentication, the *server* must 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 of course), Algo cannot publish this information in advance with the trusted CAs, and instead these Device Certificates must be signed by Algo's own CA.

In order 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.

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.

Any devices that were originally shipped with an older firmware version will not have the Device Certificate pre-loaded from the factory, although there is a procedure to load it in this case. *Please reach out to Algo support for more details.*

Once this certificate is installed, it will be valid for 30 years and reside in a separate partition, so it will not be erased even after factory resetting the Algo endpoint.

Algo Communication Products Ltd
4500 Beedie St Burnaby BC Canada V5J 5L2
www.algosolutions.com
(604) 454-3792
support@algosolutions.com

Uploading Public CA Certificates to Algo SIP Endpoints

Note that the capabilities and procedures for uploading public CA certificates has changed between firmware v1.7.6 and firmware v3.1. Please see the appropriate section below. Please contact Algo support if you require updated firmware.

Also note that pre-installed trusted certificates are not visible to users and are separate from the folders described below where additional certificates may be uploaded.

Details for Firmware v1.7.x

To install the public CA certificate on an Algo device running firmware v1.7.x, follow the steps below:

1. Obtain a public certificate from your Certificate Authority
2. Rename the public certificate 'siptrusted.pem' (only .pem format is supported)
3. In the web interface of the Algo device, navigate to the **Advanced Settings -> File Manager** tab.
4. Upload the certificate files into the '**certs**' directory. Click the Upload button in the top left corner of the file manager and browse to the certificate.

For **SIP** TLS, no default public CA certificates are used; only the above .pem file is supported, so this certificate file must be uploaded in order for SIP TLS authentication to occur (compare v3.1 firmware below, where both are supported).

For **Provisioning** TLS, only the default pre-installed public CA certificates are supported; no .pem file can be uploaded in this case (compare v3.1 firmware below, where both are supported).

Details for Firmware v3.1 and Above

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

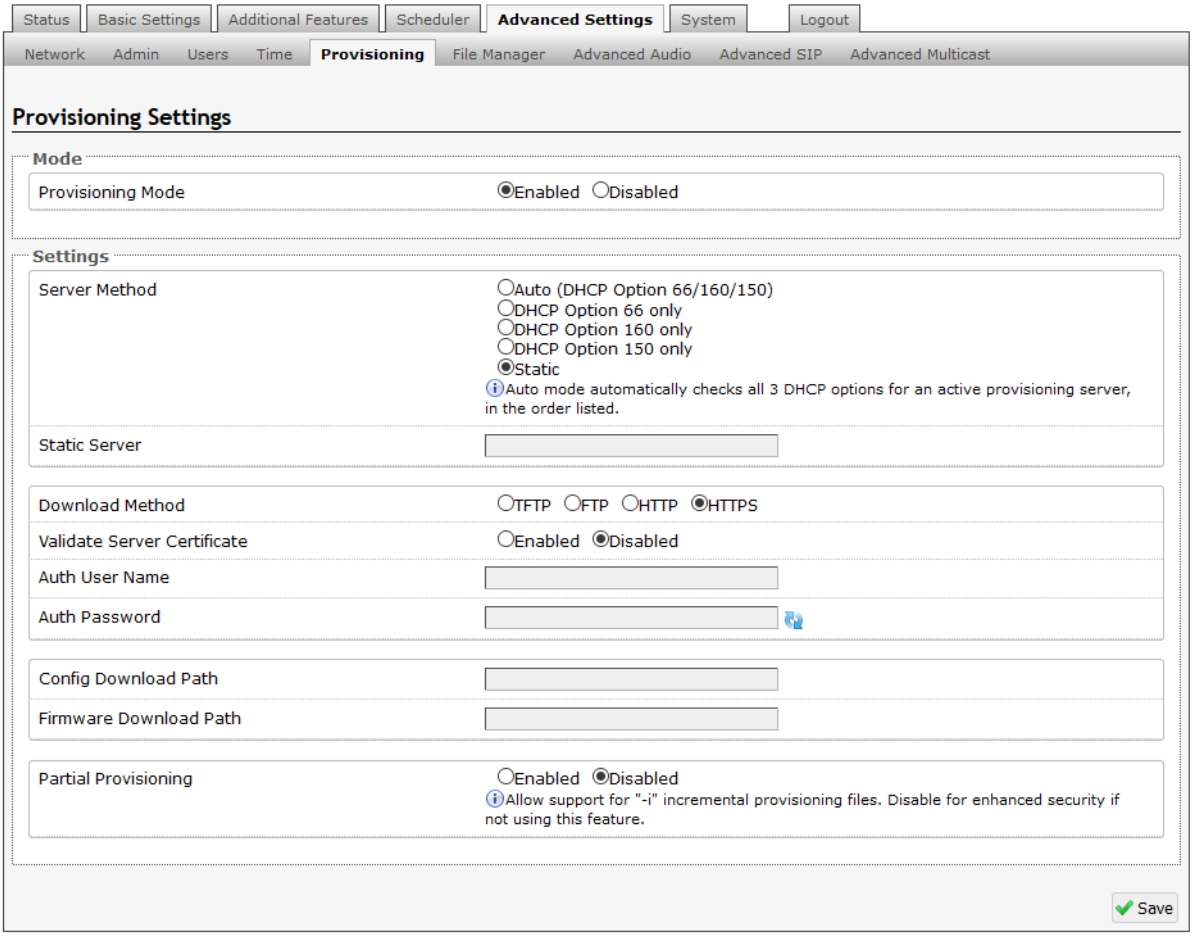
1. Obtain a public certificate from your Certificate Authority (any valid X.509 format certificate can be accepted).
2. In the web interface of the Algo device, navigate to the **System -> File Manager** tab.
3. Upload the certificate files into the '**certs/trusted**' directory (note this differs from the folder used in firmware v1.7.x). Click the Upload button in the top left corner of the file manager and browse to the certificate.

Algo Communication Products Ltd
4500 Beedie St Burnaby BC Canada V5J 5L2
www.algosolutions.com
(604) 454-3792
support@algosolutions.com

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.



In order to perform identify 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. 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. Note that for firmware versions prior to v3.1, only the *built-in certificates* may be used for provisioning.

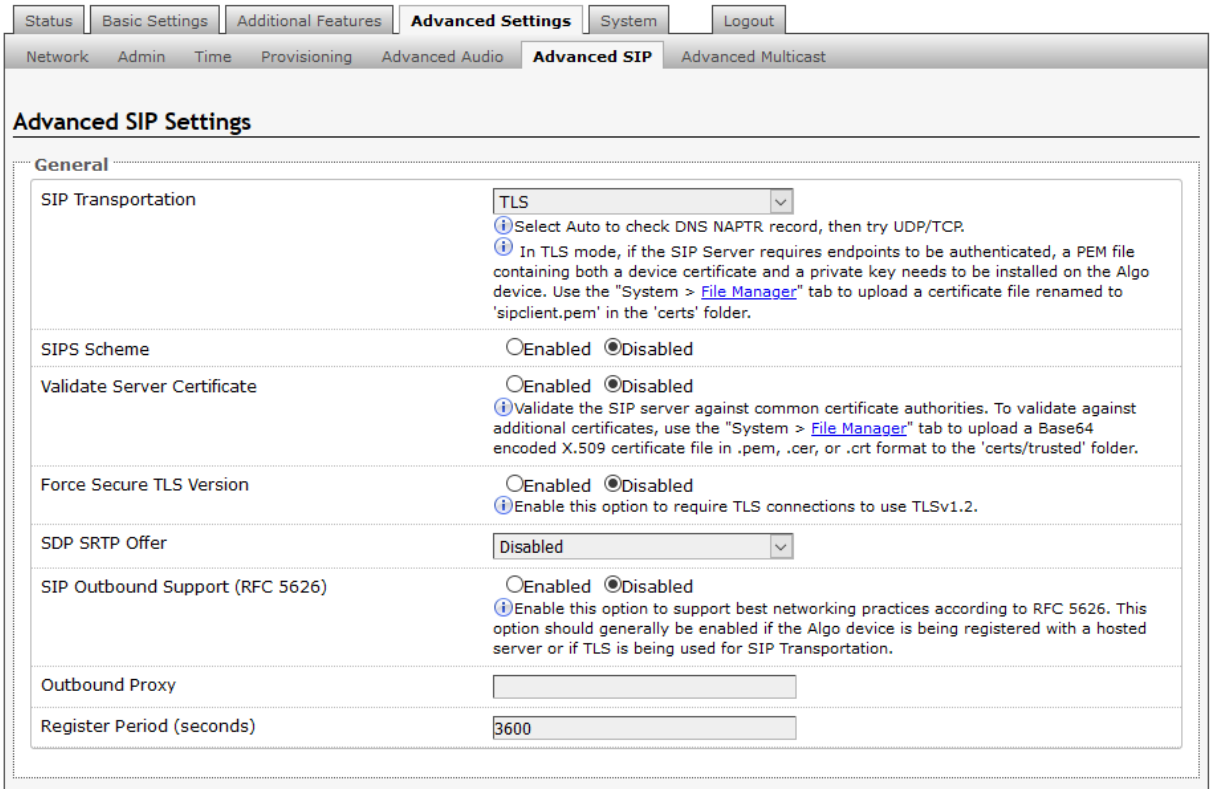
The 'Validate Server Certificate' parameter can also be enabled through provisioning:

- prov.download.cert = 1

SIP Signalling (and RTP Audio)

SIP signalling is secured by setting 'SIP Transportation' to 'TLS' (under the **Advanced Settings > Advanced SIP** tab). Setting it to 'TLS' ensures that the SIP traffic will be encrypted. The SIP signalling 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. In order 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.



In order to perform identify 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. Note that for firmware versions prior to v3.1, only the uploaded '*siptrusted.pem*' certificate may be used for SIP.

On Algo devices running firmware v3.1 & above, Force Secure TLS Version option may be used to to require TLS connections to use TLSv1.2.

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

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

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