ADTRAN Operating System

SIP Signaling and Media Security

Configuration Guide

6AOSCG0069-29F

July 2020

To the Holder of this Document

This document is intended for the use of ADTRAN customers only for the purposes of the agreement under which the document is submitted, and no part of it may be used, reproduced, modified or transmitted in any form or means without the prior written permission of ADTRAN.

The contents of this document are current as of the date of publication and are subject to change without notice.

Trademark Information

“ADTRAN” and the ADTRAN logo are registered trademarks of ADTRAN, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by ADTRAN’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with ADTRAN that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall ADTRAN be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.

Table of Contents

1. Overview of TLS and SRTP

TLS is a cryptographic protocol, intended to replace Secure Sockets Layer, that provides communication security over the Internet. TLS is used to authenticate communication peers through the exchange of symmetric keys and authentication certificates. The protocol certifies the relation between a certificate and its owner as well as administers the validity of certificates used between communication peers. TLS operates on top of an underlying transport protocol, such as Transport Control Protocol (TCP), which carries the encrypted data. Privacy and security is provided by TLS between media endpoints, particularly in SIP signaling in Voice over IP (VoIP) networks. The certificate authority (CA) profile is responsible for certificate storage and management. Each TLS profile is associated with exactly one CA profile. TLS is configurable on a per-SIP trunk (or SIP proxy server) basis by applying a TLS profile. The profile is used by each SIP/TLS entity, and contains the configuration necessary to control TLS usage, such as identity validation, negotiable cipher suites, CA profiles, and server or mutual authentication settings.

SRTP is a protocol used to provide confidentiality, message authentication, and replay protection to Realtime Transfer Protocol (RTP) traffic. This protocol provides a framework for encryption and message authentication of RTP streams between media endpoints. Typically, SRTP uses TLS for signaling authentication and encryption. Although SRTP protects the media shared between endpoints, it relies on the exchange of Session Description Protocol Security Descriptions (SDES) keys that appear in clear text within the SIP message. TLS is used with SRTP to encrypt the signaling and protect against snooping of the SDES keys. TLS is not required for successful SRTP negotiation, but it is strongly recommended. In AOS, SRTP is used for calls when SRTP is enabled and the capabilities of the communication peer allow it. Similar to TLS configuration, SRTP configuration in AOS depends on the configuration of a SRTP profile. This profile controls SRTP usage for the AOS device and is applied on a per-trunk basis for the back-to-back user agent (B2BUA) or to the SIP proxy in the AOS device.

This configuration guide explains how to update your ADTRAN Operating System (AOS) firmware using the AOS Web-based graphical user interface (GUI) with Trivial File Transfer Protocol (TFTP) TFTP, Hypertext Transfer Protocol (HTTP), HTTP Secure (HTTPS), File Transfer Protocol (FTP), XMODEM, and a Universal Serial Bus (USB) flash drive. Also included in this guide are instructions for creating a random access memory (RAM) disk for uploading firmware updates in safe mode and upgrading a unit using AOS bootstrap mode.

2. Hardware and Software Requirements and Limitations

SIP TLS and SRTP were introduced in AOS in firmware release R11.5.0. Platforms that support SIP TLS and SRTP are outlined in the *AOS Product Feature Matrix*, available online at https://supportforums.adtran.com.

In AOS firmware release R13.1.0, support for TLS and SRTP to secure SIP signaling and media, respectively, between the AOS SIP proxy and the softswitch was added to the SIP proxy. Configuration for the new application of these security features is detailed in *Enabling TLS and SRTP on the AOS SIP Proxy on page 17*. For more information about configuring the SIP proxy, refer to the *SIP Proxy in AOS* configuration guide, available online at https://supportforums.adtran.com.

In AOS firmware release R13.4.0, the **reduced-rekeying** parameter was added to the **srtp** command on voice trunks to aid with interoperability.

In AOS firmware release R13.7.0, the **roc-reset-on-reinvite** parameter was added to the **srtp** command on voice trunks to aid with interoperability with non-RFC compliant devices.

In AOS firmware release R13.8.0, the **fallback [1.0 | 1.1 | 1.2]** parameter was added to the **tls-version** command when configuring a SIP TLS profile to allow manual configuration of the lowest fallback version allowed. By default, the fallback is set to version 1.2.

TLS Specifics

TLS versions 1.0, 1.1, and 1.2 are supported. The TLS cipher suites supported by AOS are outlined in *Table 1*. The supported suites with a high strength are enabled by default.

Table 1. Supported TLS Cipher Suites

Suite
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_GMC_SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_NULL_MD5
TLS_RSA_WITH_NULL_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

NOTE

In AOS firmware release 13.1.0, support for the TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WITH_AES_256_GMC_SHA384 cipher suites was added. In addition, support for the SSL_DES_192_EDE3_CBC_WITH_MDS, SSL_RC4_128_WITH_MD5, TLS_DHE_RSA_WITH_DES_CBC_SHA, and TLS_RSA_WITH_DES_CBC_SHA cipher suites was removed.

SIP TLS is compatible with Session Initiation Protocol Security (SIPS) Uniform Resource Identifiers (URIs). When TLS is configured, inbound or outbound SIPS operations are not rejected if the inbound or outbound link is configured and able to support TLS.

The maximum number of certificates stored in the AOS device include the following:

- 10 trusted certificates
- 10 self certificates

TLS server authentication and mutual authentication modes are both supported. When AOS is acting as the TLS server, and server authentication mode is enabled while mutual authentication mode is disabled, AOS does not request or authenticate the validity of the client certificate. When mutual authentication is enabled, AOS requests and authenticates the client certificate. When AOS is acting as a TLS client and the server requests the local certificate, AOS complies and sends the local certificate (if it is available) regardless of the mutual authentication setting.

SRTP Specifics

Enforcing the constraints provided in the SRTP profile configuration requires AOS to be in the media path.

SRTP in AOS does not support the optional encryption mode AES-f8 specified in RFC 3711. The supported SRTP crypto suites are outlined in *Table 2*. By default, only the AES_CM_128_HMAC_SHA1_80 suite is enabled.

Table 2. Supported SRTP Crypto Suites

SRTP Crypto Suites	Associated RFC
AES_256_CM_HMAC_SHA1_32	RFC 6188
AES_256_CM_HMAC_SHA1_80	RFC 6188
AES_CM_128_HMAC_SHA1_32	RFC 4568
AES_CM_128_HMAC_SHA1_80	RFC 4568
SRTP_NULL_HMAC_SHA1_32	RFC 3711
SRTP_NULL_HMAC_SHA1_80	RFC 3711

As of AOS firmware release R13.1.0, SRTP can be configured to allow non-RTP media to be forwarded along the media path without SRTP security. This feature can be beneficial for traffic like T.38 over UDP Transport Layer (UDPTL). By default, when the AOS device is configured to use SRTP, any non-RTP media is disallowed. By allowing non-RTP media, SRTP secures all RTP media but forwards any non-RTP media unsecured.

Additional Features Impacted by TLS or SRTP

The Voice Quality Monitoring (VQM) feature in AOS can analyze an SRTP stream by viewing the RTP headers. In order to analyze Realtime Transfer Control Protocol (RTCP) streams, VQM must participate in SRTP so the media can be decrypted for analysis.

Loopback accounts can be used with SRTP. When a call is made from a loopback account, external signaling takes place only when the call is routed to an account requiring external signaling. The loopback account has no SIP properties of its own, therefore it has no TLS properties; however, the account does send and receive media and therefore does have RTP properties. Loopback accounts can signal SRTP properties, which allow it to emulate an SRTP-capable endpoint. This feature is beneficial for controlling SRTP operation when loopback calls are delivered to a trunk whose setting is SRTP optional and when testing a SIP trunk's SDP and SDES processing and translation. Loopback accounts are configured for SRTP when an SRTP profile is applied to the loopback account.

As of AOS firmware release R13.1.0, the server side of the AOS SIP proxy can optionally be configured to use both TLS and SRTP to secure SIP signaling and media.

3. Configuring SIP Signaling and Media Security Using the CLI

To configure TLS and SRTP security services using the CLI, you will need to complete the following tasks:

1. Accessing the AOS Product Using the CLI
2. Configuring CA profiles for use with TLS and SRTP
3. Configuring the TLS Profile
4. Configuring the SRTP Profile
5. Enabling SIP TLS globally
6. Configuring TLS and SRTP on the SIP trunk
7. Enabling TLS and SRTP for additional AOS features (optional)

Accessing the AOS Product Using the CLI

To begin configuring the TLS and SRTP services on the AOS product, access the CLI following these steps:

1. Boot up the unit.
2. Telnet to the unit (**telnet** <*ip address*>), for example: **telnet 10.10.10.1**.

> **NOTE**
>
> *If during the unit's setup process you have changed the default IP address (**10.10.10.1**), use the configured IP address.*

3. Enter your username and password at the prompt.

> **NOTE**
>
> *The AOS default user name is admin and the default password is password. If your product no longer has the default user name and password, contact your system administrator for the appropriate user name and password.*

4. Enter Enable mode on your unit by entering **enable** at the prompt as follows:

```
>enable
```

5. Enter your Enable mode password at the prompt.
6. Enter the unit's Global Configuration mode as follows:

```
#configure terminal
(config)#
```

You can now begin configuring the TLS and SRTP features.

Configuring CA Profiles for Use with TLS and SRTP

The CA profile configuration options have been updated to include TLS and SRTP support. The CA profiles are configured to be used by the TLS profile or the SRTP profile, in the same way that CA profiles are configured for Virtual Private Network (VPN) use. In fact, the AOS device provides a single certificate store for managing individual certificates, thus allowing the flexibility to use the same certificates for VPN and TLS, or to use different certificates for the two services. The updated CA profile configuration options allow the certificate request to be written directly to local file storage.

The CLI provides an enrollment dialog when creating CA profiles. This dialog prompts you to enter information about the profile's configuration, including the type of certificate and specific certificate configuration settings. This configuration can also be completed using CLI commands from the CA Profile Configuration mode prompt. The CA profile enrollment dialog has been updated to include prompts for the commands used to complete the tasks outlined in the following section: *Using Trusted Certificates in the CA Profile on page 8*.

Using Trusted Certificates in the CA Profile

There are two modes for configuring trusted certificates in the CA profile: client authentication and server authentication. The commands used for these authentication types are described in the following sections.

Client-Only Authentication

To configure the CA profile with trusted certificates when performing client-only authentication, use the following commands:

1. Create the CA profile using the **crypto ca profile** <*profile name*> from the Global Configuration mode. The <*profile name*> parameter is the name of the CA profile you are creating. Use the **no** form of this command to remove the profile from the device's configuration. The CA profile must be created before configuring certificate parameters. Enter the command as follows:

```
(config)#crypto ca profile MYPROFILE
Configuring New CA Profile MYPROFILE
(config-profile)#
```

2. Use the **crypto ca authenticate** <*profile name*> **[**<*drive*> <*name*>**]** command to import the CA certificate. The <*profile name*> parameter specifies the name of the CA profile you are authenticating. The optional <*drive*> <*name*> parameters specify that the certificate to be authenticated is loaded from a file identified by it's location (<*drive*>), such as **nonvol, cflash, usbdrive0**, etc., and the name of the file (<*name*>). This bypasses the terminal loading process. To initiate CA authentication for a specific file, enter the command from the Global Configuration mode as follows:

```
(config)#crypto ca authenticate MYPROFILE nonvol CA.pem
```

Server Authentication

To configure the CA profile with trusted certificates when performing server authentication, use the following commands:

1. Create the CA profile using the **crypto ca profile** <*profile name*> from the Global Configuration mode. The <*profile name*> parameter is the name of the CA profile you are creating. Use the **no** form of this command to remove the profile from the device's configuration. The CA profile must be created before configuring certificate parameters. Enter the command as follows:

```
(config)#crypto ca profile MYPROFILE
Configuring New CA Profile MYPROFILE
(config-profile)#
```

2. Use the **crypto ca authenticate** <*profile name*> **[**<*drive*> <*name*>**]** command to import the CA certificate. The <*profile name*> parameter specifies the name of the CA profile you are authenticating. The optional <*drive*> <*name*> parameters specify that the certificate to be authenticated is loaded from a file identified by it's location (<*drive*>), such as **nonvol, cflash, usbdrive0**, etc., and the name of the file (<*name*>). This bypasses the terminal loading process. To initiate CA authentication for a specific file, enter the command from the Global Configuration mode as follows:

```
(config)#crypto ca authenticate MYPROFILE nonvol CA.pem
```

3. Use the **crypto ca enroll** <*profile name*> **[**<*drive*> <*name*>**] [force-overwrite]** command to create the certificate request and begin the enrollment process. When the command is issued, a copy of the

certificate request is written in binary (.der) and BASE64 (.pem) formats. The <*profile name*> parameter specifies the name of the CA profile you are creating. The optional <*drive*> <*name*> parameter is the file storage location available on the platform (<*drive*>), such as **nonvol, cflash, usbdrive0**, etc., and the name of the file (<*name*>). The optional **force-overwrite** parameter instructs the AOS device to overwrite any existing file with the same name. If the <*drive*> <*name*> parameters are not specified, the enrollment dialog will prompt you to indicate if the certificate request should be written to a file, and if yes, the drive and filename to use. If the certificate request is not saved to file, the keys remain and the request is discarded. If the enrollment is repeated the keys are overwritten and a new request is generated to match the keys. To create the certificate and begin the enrollment process, enter the command from the Global Configuration mode as follows:

```
(config)#crypto ca enroll MYPROFILE nonvol SELF.csr force-overwrite
(config-ca-profile-MYPROFILE)#
```

4. Use the **crypto ca import** <*profile name*> <**certificate | crl**> **[**<*drive*> <*name*>**]** command to import your signed self certificate (**certificate**) or a certificate revocation list (CRL) (**crl**) for a specific CA profile (<*profile name*>). The certificate or CRL can be imported from a specific file using the optional **[**<*drive*> <*name*>**]** parameters. If the file is specified, terminal loading is bypassed.

   Enter the command from the Global Configuration mode as follows:

```
(config)#crypto ca import MYPROFILE certificate nonvol SELF.pem
```

Configuring the TLS Profile

Each entity that uses TLS uses a TLS profile. Multiple TLS profiles can exist and the same TLS profile can be used by as many entities using TLS as required. The TLS profile essentially operates as a template for TLS operation and is applied on a per-trunk basis (refer to *Configuring TLS and SRTP on the SIP Trunk on page 13*).

The TLS profile is configured by entering the **tls-profile** <*profile name*>command from the Global Configuration mode. This command enters the TLS Profile Configuration mode, from which the operation of TLS is configured. The <*profile name*> parameter is the name of the TLS profile. If a profile name is specified that already exists, this command reenters that TLS profile's configuration mode. The **no** form of this command removes the TLS profile from the AOS device and removes all other commands that reference this TLS profile from the configuration. By default, no TLS profiles are configured. To create a new TLS profile, and enter the profile's configuration mode, enter the command from the Global Configuration mode as follows:

```
(config)#tls-profile TLSPROFILE1
(config-tls-profile-TLSPROFILE1)#
```

Once the TLS profile has been created, you can use the following commands to specify the TLS operation for the profile.

1. To specify the TLS version used by this profile, enter the **tls-version [1.2 | 1.1 | 1.0] fallback [1.2 | 1.1 | 1.0]** command from the profile's configuration mode. This command sets the TLS version as a fixed value, or allows fallback from the highest supported version to the lowest specified version. By default, fallback 1.2 is enabled. Use the **no** form of this command to return to the default value. To specify that the TLS profile uses TLS version **1.2**, enter the command as follows:

```
(config)#tls-profile TLSPROFILE1
(config-tls-profile-TLSPROFILE1)#tls-version 1.2
```

2. To enable mutual TLS authentication in the TLS profile, enter the **authentication mutual** command from the profile's configuration mode. If mutual authentication is configured, when the entity using the TLS profile is responding to a TLS negotiation (server role), the server requests the client's certificate, and then authenticates the client. If the client does not provide a certificate, or the certificate fails validation, the TLS connection is rejected by the server. If mutual authentication is not configured, the responder (server) does not request or require a certificate from the client. When the entity using the TLS profile is

initiating a SIP/TLS negotiation (client role), the client always requests the server's certificate and then authenticates the server. If the server does not provide a certificate or the certificate fails validation, the TLS connection is rejected by the client. The **no** form of this command disables mutual authentication and reverts to server authentication (default). To enable mutual authentication, enter the command as follows:

```
(config)#tls-profile TLSPROFILE1
(config-tls-profile-TLSPROFILE1)#authentication mutual
```

3. To specify a TLS cipher suite for the TLS profile, enter the **secure-ciphersuite** <*name*> **[**<*number*>**]** command from the profile's configuration mode. The <*name*> parameter is the name of a supported TLS cipher suite to use in the TLS negotiation. Supported TLS cipher suites are outlined in Table 1 on page 5. The optional <*number*> parameter is an integer that describes the cipher suite's desired relative position among all enabled cipher suites within the profile when used in the TLS negotiation. Valid range is **1** to **65535**. If multiple cipher suites have the same value specified, they are placed at that number position and then subsorted in the order they appear in the configuration. One instance of this command exists for each supported TLS cipher suite. Use the **no** form of this command to remove the cipher suite from the TLS profile. By default, all high strength cipher suites are individually enabled and all other cipher suites are individually disabled. To enable a specific TLS cipher suite on the profile, enter the command as follows:

```
(config)#tls-profile TLSPROFILE1
(config-tls-profile-TLSPROFILE1)#secure-ciphersuite
  TLS_RSA_WITH_RC4_128_SHA 150
```

4. To associate a CA profile with the TLS profile enter the **ca-profile** <*name*> command from the profile's configuration mode. A CA profile must be specified for TLS operation and the TLS profile is not valid until it is associated with a valid CA profile. The <*name*> parameter is the CA profile's name. Only one CA profile can be associated with a TLS profile. If the command is entered more than once, the previous instance of the command is overwritten. Use the **no** form of this command to remove the CA profile from the TLS profile. By default, no CA profile is associated with the TLS profile. To associate a CA profile with the TLS profile, enter the command as follows:

```
(config)#tls-profile TLSPROFILE1
(config-tls-profile-TLSPROFILE1)#ca-profile MYPROFILE
```

5. Use the **validate identity [fqdn configured | fqdn resolved | ip-address | string]** command to control how the identity of the TLS communication peer's certificate, received during the TLS handshake, is validated. The **fqdn configured** parameter specifies that the peer's subject alternative name (SAN) IP domain naming service (DNS) name is used to validate the peer. The name must match the FQDN configured for the peer at the trunk. The **fqdn resolved** parameter specifies that the peer's SAN IP domain DNS name is used to validate the peer. The name must match the FQDN as resolved by DNS SRVs from the FQDN as configured for the peer at the trunk. The **ip-address** parameter specifies that the peer's SAN IP address is used to validate the peer. The address must match the IP address configured or resolved by DNS for the peer at the trunk. The **string** parameter specifies that the peer's SAN fields or Subject components are used to identify the peer. The string must match the string configured on the trunk (using the **peer-certificate-identity** command from the trunk's configuration mode). By default, identity validations are disabled and only proper signing is verified. Use the **no** form of this command to remove the identity validation method from the TLS profile. Up to one instance of each validation method can be specified in the profile, and each method specified must be matched in order for successful validation. These identity validation methods do not specify the value that must be matched, but rather specify an attribute whose value is related to the current session. To enable identity validation for the TLS profile based on IP address, enter the command as follows:

```
(config)#tls-profile TLSPROFILE1
(config-tls-profile-TLSPROFILE1)#validate identity ip-address
```

Configuring the SRTP Profile

Each entity that uses SRTP uses an SRTP profile. Multiple SRTP profiles can exist and the same SRTP profile can be used by as many entities using SRTP as required. The SRTP profile essentially operates as a template for SRTP operation and is applied on a per-trunk basis (refer to *Configuring TLS and SRTP on the SIP Trunk on page 13*).

The SRTP profile is configured by entering the **srtp-profile** <*profile name*> command from the Global Configuration mode. This command enters the SRTP Profile Configuration mode, from which the operation of SRTP is configured. The <*profile name*> parameter is the name of the SRTP profile. If a profile name is specified that already exists, this command reenters the named SRTP profile's configuration mode. The **no** form of this command removes the SRTP profile from the AOS device and removes all other commands that reference this SRTP profile from the configuration. By default, no SRTP profile is configured. To create a new SRTP profile, and enter the profile's configuration mode, enter the command from the Global Configuration mode as follows:

```
(config)#srtp-profile SRTPPROFILE1
(config-srtp-profile-SRTPPROFILE1)#
```

Once the SRTP profile has been created, you can use the following commands to specify the SRTP operation for the profile.

1. To specify an STRP cryptography suite for the SRTP profile, enter the **crypto-suite** <*name*> command from the profile's configuration mode. The <*name*> parameter is the name of a supported SRTP crypto suite to use in the SRTP cryptography. Supported SRTP crypto suites are outlined in Table 2 on page 6. Use the **no** form of this command to remove the crypto suite from the SRTP profile. By default, only the AES_CM_128_HMAC_SHA1_80 crypto suite is enabled. To specify a different SRTP crypto suite on the profile, enter the command as follows:

   ```
   (config)#srtp-profile SRTPPROFILE1
   (config-srtp-profile-SRTPPROFILE1)#crypto-suite AES_256_CM_HMAC_SHA1_80
   ```

2. To specify the SRTP authentication method for the SRTP profile, enter the **srtp [auth | offer-no-auth | strict-no-auth]** command from the profile's configuration mode. The **auth** setting, used by default, specifies that the session must authenticate SRTP. When enabled as an offerer, the crypto attributes offered do not contain the UNAUTHENTICATED_SRTP session parameter, and any answers containing that parameter are not accepted. When enabled as an answerer, the crypto attribute containing the UNAUTHENTICATED_SRTP session parameter is not accepted. The **offer-no-auth** setting specifies that the session can authenticate, but it is not required. When enabled as an offerer, crypto attributes offered contain the UNAUTHENTICATED_SRTP parameter, and valid answers with or without that parameter are accepted. When enabled as an answerer, the crypto attribute with or without this parameter will be selected in an offer. The **strict-no-auth** setting specifies that the session must not authenticate. When enabled, as an offerer, crypto attributes offered contain the session parameter UNAUTHENTICATED_SRTP and answers that do NOT contain this parameter are rejected. When enabled as an answerer, the crypto attribute containing the parameter is not accepted in an offer. To specify that the SRTP profile accepts sessions with or without the UNAUTHENTICATED_SRTP parameter, enter the command as follows:

   ```
   (config)#srtp-profile SRTPPROFILE1
   (config-srtp-profile-SRTPPROFILE1)#srtp offer-no-auth
   ```

> **NOTE**
>
> *This command is not available for Secure Realtime Transfer Control Protocol (SRTCP) because SRTCP must always be authenticated.*

3. To specify the SRTP encryption method for the SRTP profile, enter the **srtp [encrypt | offer-no-encrypt | strict-no-encrypt]** command from the profile's configuration mode. The **encrypt** setting, used by default, specifies that the session must encrypt SRTP. When enabled as an offerer, the crypto attributes offered do not contain the UNENCRYPTED_SRTP parameter, and answers that contain this parameter are not accepted. The **offer-no-encrypt** setting specifies that encryption can be used, but is not required. When enabled as an offerer, the crypto attributes offered contain the UNENCRYPTED_SRTP session parameter, and valid answers with or without the parameter are accepted. When enabled as an answerer, a crypto attribute with or without the UNENCRYPTED_SRTP parameter will be accepted. The **strict-no-encrypt** setting specifies that the session must not encrypt SRTP. When enabled as an offerer, the crypto attributes offered contain the UNENCRYPTED_SRTP session parameter, and answers not containing the same parameter are not accepted. When enabled as an answerer, a crypto attribute that does not contain the UNENCRYPTED_SRTP parameter is rejected. To specify that the SRTP profile does not allow encryption, enter the command as follows:

```
(config)#srtp-profile SRTPPROFILE1
(config-srtp-profile-SRTPPROFILE1)srtp strict-no-encrypt
```

4. To specify the SRTCP encryption method for the SRTP profile, enter the **srtcp [encrypt | offer-no-encrypt | strict-no-encrypt]** command from the profile's configuration mode. The **encrypt** setting, used by default, specifies that the session must encrypt SRTCP. When enabled as an offerer, the crypto attributes offered do not contain the UNENCRYPTED_SRTCP parameter, and answers that contain this parameter are not accepted. The **offer-no-encrypt** setting specifies that encryption can be used, but is not required. When enabled as an offerer, the crypto attributes offered contain the UNENCRYPTED_SRTCP session parameter, and valid answers with or without the parameter are accepted. When enabled as an answerer, a crypto attribute with or without the UNENCRYPTED_SRTCP parameter will be accepted. The **strict-no-encrypt** setting specifies that the session must not encrypt SRTCP. When enabled as an offerer, the crypto attributes offered contain the UNENCRYPTED_SRTCP session parameter and answers not containing the same parameter are not accepted. When enabled as an answerer, a crypto attribute that does not contain the UNENCRYPTED_SRTCP parameter is rejected. To specify that the SRTP profile does not encrypt SRTCP, enter the command as follows:

```
(config)#srtp-profile SRTPPROFILE1
(config-srtp-profile-SRTPPROFILE1)srtcp strict-no-encrypt
```

NOTE

The SRTP authentication and encryption commands, as well as the SRTCP encryption command, are set once at the SRTP profile but they affect each crypto attribute associated with a media session.

Enabling SIP TLS Globally

The TLS transport for SIP must be enabled globally for the TLS negotiation to function. To specify that the TLS transport is allowed for SIP on the AOS device, enter the **sip tls [**<*port*>**]** command from the Global Configuration mode.The optional <*port*> parameter specifies the TCP port on which the SIP stack listens for TLS packets. By default, the port is set to **5061**. The **no** form of this command disables TLS. Enter the command as follows:

```
(config)#sip tls
(config)#
```

Configuring TLS and SRTP on the SIP Trunk

Both the TLS and SRTP profiles are applied on a per-trunk basis. The following sections outline the TLS and SRTP configurations available on SIP trunks.

TLS Trunk Configuration

TLS is used by a trunk when the call processing logic selects a server entry that specifies TLS transport. TLS is specified at the server level within a trunk using the following commands. You can specify the trunk registrar, server, and outbound proxy TLS trunk settings.

> **NOTE**
>
> *When an outbound proxy is not specified, the protocol specified for the SIP server and registrar is used between the AOS device and the SIP server and registrar. When an outbound proxy is specified, the protocol specified for the outbound proxy is used between the AOS device and the proxy. The protocol specified for the SIP server and the registrar takes place between the proxy and the SIP server and registrar.*

1. To specify the TLS trunk SIP server settings, enter the **sip-server [primary | secondary]** <*value*> **tls** <*profile name*> **[**<*port*>**] [srv** <*service-name-prefix*> **[**<*transport-name-prefix*>**]]** command from the trunk's configuration mode. The **primary** and **secondary** parameters specify whether this is a primary or secondary SIP server. The <*value*> parameter is the IP address or domain name of the device that is the peer for this SIP trunk. Either an address or domain name must be specified. The **tls** <*profile name*> parameter associates the TLS profile with the SIP server, thus specifying the TLS operation. A TLS profile must be specified. The optional <*port*> parameter specifies the target port to use when initiating the TLS session. Port **5061** is used by default. The optional **srv** parameters are used when the <*value*> parameter is specified as a domain name. The literal text specified in the <*service-name-prefix*>, and optional <*transport-name-prefix*> parameters are used to format the DNS SRV request used to resolve the domain name. Underscores are added automatically for prefixes. By default, the service name prefix is set to **sips** and the transport name prefix is set to **tcp**. Use the **no** form of this command to remove the SIP server from the trunk. To specify **10.10.10.1** as the primary SIP server using TLS profile **TLSPROFILE1** on the default port, enter the command as follows:

```
(config)#voice trunk T01 type sip
(config-T01)#sip-server primary 10.10.10.1 tls TLSPROFILE1
(config-T01)#
```

2. To optionally specify the TLS trunk registrar settings, enter the **registrar [primary | secondary]** <*value*> **tls** <*profile name*> **[**<*port*>**] [srv** <*service-name-prefix*> **[**<*transport-name-prefix*>**]]** command from the trunk's configuration mode. The **primary** and **secondary** parameters specify whether this is a primary or secondary SIP registrar server. The <*value*> parameter is the IP address or domain name of the device that is the peer for this SIP trunk. Either an address or domain name must be specified. The **tls** <*profile name*> parameter associates the TLS profile with the registrar, thus specifying the TLS operation. A TLS profile must be specified. The optional <*port*> parameter specifies the target port to use when initiating the TLS session. Port **5061** is used by default. The optional **srv** parameters are used when the <*value*> parameter is specified as a domain name. The literal text specified in the <*service-name-prefix*>, and optional <*transport-name-prefix*> parameters are used to format the DNS SRV request used to resolve the domain name. Underscores are added automatically for prefixes. By default, the service name prefix is set to **sips** and the transport name prefix is set to **tcp**. Use the **no** form of this command to remove the registrar from the trunk. To specify **10.10.10.2** as the primary registrar server using TLS profile **TLSPROFILE1** on the default port, enter the command as follows:

```
(config)#voice trunk T01 type sip
(config-T01)#registrar primary 10.10.10.2 tls TLSPROFILE1
(config-T01)#
```

3. To optionally specify the TLS trunk outbound proxy settings, enter the **outbound-proxy [primary | secondary]** <*value*> **tls** <*profile name*> **[**<*port*>**] [srv** <*service-name-prefix*> **[**<*transport-name-prefix*>**]]** command from the trunk's configuration mode. The **primary** and **secondary** parameters specify whether this is a primary or secondary outbound proxy. The <*value*> parameter is the IP address or domain name of the device that is the peer for this SIP trunk. Either an address or domain name must be specified. The **tls** <*profile name*> parameter associates the TLS profile with the outbound proxy, thus specifying the TLS operation. A TLS profile must be specified. The optional <*port*> parameter specifies the target port to use when initiating the TLS session. Port **5061** is used by default. The optional **srv** parameters are used when the <*value*> parameter is specified as a domain name. The literal text specified in the <*service-name-prefix*>, and optional <*transport-name-prefix*> parameters are used to format the DNS SRV request used to resolve the domain name. Underscores are added automatically for prefixes. By default, the service name prefix is set to **sips** and the transport name prefix is set to **tcp**. Use the **no** form of this command to remove the outbound proxy from the trunk. To specify **10.10.10.3** as the primary outbound proxy using TLS profile **TLSPROFILE1** on the default port, enter the command as follows:

```
(config)#voice trunk T01 type sip
(config-T01)#outbound-proxy primary 10.10.10.3 tls TLSPROFILE1
(config-T01)#
```

4. To optionally configure a static string used in peer validation for TLS, enter the **peer-certificate-identity** <*string*> from the trunk's configuration mode. The <*string*> value is the literal text specified at the trunk and used by the TLS profile to match for validation. Use the **no** form of this command to remove the string from the trunk's configuration. To define a static string on the trunk to be used for TLS validation, enter the command as follows:

```
(config)#voice trunk T01 type sip
(config-T01)#peer-certificate-identity PEER1VALID
(config-T01)#
```

5. To optionally configure validated SIP trunk failover, enter the **sip-server validation register** command from the trunk's configuration mode. This configuration is useful when using client-only authentication. With this type of authentication, a persistent connection is established to the SIP server. In this scenario, it is ideal to enable validated SIP trunk failover so that the unit only contacts the server with which it is registered. Use the **no** form of this command to disable the feature. Enter the command from the trunk's configuration mode as follows:

```
(config)#voice trunk T01 type sip
(config-T01)#sip-server validation register
(config-T01)#
```

NOTE

For more information about SIP trunk failover, refer to the configuration guide Configuring SIP Trunk Failover in AOS, available online at https://supportforums.adtran.com.

6. To optionally configure the AOS device to use the TCP port from which AOS initiated a TLS connection in the Contact URI, enter the **grammar contact host port persistent** command from the trunk's configuration mode. This configuration is useful when using client-only authentication. With this type of authentication, a persistent connection is established to the SIP server. Many SIP servers and session

border controllers (SBCs) need to see the TCP port from which AOS initiated the TLS connection in the Contact URI sent by AOS. Use the **no** form of this command to disable this feature. Enter the command from the trunk's configuration mode as follows:

```
(config)#voice trunk T01 type sip
(config-T01)#grammar contact host port persistent
(config-T01)#
```

SRTP Trunk Configuration

To enable SRTP functionality on the SIP trunk, enter the **srtp [allow-non-rtp-media] [optional avp] [optional avp-savp] [reduced-rekeying] [roc-reset-on-invite] [tls-optional]** *<profile name>* command from the trunk's configuration mode. The optional **allow-non-rtp-media** parameter configures SRTP to allow non-RTP media, such as T.38 over UDP Transport Layer (UDPL), that cannot be protected by SRTP. When this option is specified, RTP media is secured by SRTP, but any non-RTP media is forwarded unsecured. By default, SRTP is configured and non-RTP media is rejected to prevent unsecured media from transversing the device. The optional **optional avp** parameter specifies the RTP audio video profile (AVP) is used for both offers and RTP/AVP answers containing crypto attributes. The optional **optional avp-savp** parameter specifies the RTP AVP is used for offers and the secure AVP (SAVP) is used for RTP/AVP answers containing crypto attributes. If neither **optional** option is set, SRTP must be used or the call fails. The optional **reduced-rekeying** parameter specifies that SRTP rekeying on reINVITES will be disabled if the received SDP offer is unchanged. The optional **roc-reset-on-reinvite** parameter specifies that AOS will reset the outbound rollover counter (ROC) when it sends a reINVITE. The optional **tls-optional** parameter specifies that SDES negotiation of SRTP is permitted over an unsecure control channel (NOT RECOMMENDED). If this option is not set, the control channel must be secured by TLS in order to perform SDES negotiation. The *<profile name>* specifies the name of the SRTP profile to associate with the trunk. This profile sets the rules for SRTP use on the trunk. An SRTP profile must be specified. To configure the trunk to use SRTP and TLS control channel security with SRTP profile SRTPPROFILE1, enter the command as follows:

```
(config)#voice trunk T01 type sip
(config-T01)#srtp SRTPPROFILE1
(config-T01)#
```

Many combinations of this command can be used to configure SRTP on the trunk. *Table 3* outlines the result of each combination of SRTP command settings and conditions.

Table 3. SRTP Command Settings and Conditions

TLS Optional Setting	SRTP Optional Setting	Was TLS Negotiated?	Is the Peer Able to Negotiate SRTP?	Local Action and Call Result
Required	Required	Yes	Yes	SRTP offered and negotiated
Optional	Required	Yes	Yes	SRTP offered and negotiated
Required	Required	Yes	No	SRTP offered, call fails
Optional	Required	Yes	No	SRTP offered, call fails
Required	Optional	Yes	No	SRTP offered, RTP negotiated
Optional	Optional	Yes	No	SRTP offered, RTP negotiated

Table 3. SRTP Command Settings and Conditions

TLS Optional Setting	SRTP Optional Setting	Was TLS Negotiated?	Is the Peer Able to Negotiate SRTP?	Local Action and Call Result
Required	Required	No	Yes	Call fails, no TLS
Optional	Required	No	Yes	SRTP offered and negotiated, SDES not TLS secured
Required	Optional	No	Yes	Call fails, no TLS
Optional	Optional	No	Yes	SRTP is offered and negotiated, SDES not TLS secured
Required	Required	No	No	Call fails, no TLS
Optional	Required	No	No	SRTP offered, call fails
Required	Optional	No	No	Call fails, no TLS
Optional	Optional	No	No	SRTP offered, RTP negotiated

Enabling TLS and SRTP for Additional AOS Features (Optional)

You can optionally enable TLS on the AOS VoIP name service (VNS), VQM features, and TLS and SRTP on the AOS SIP proxy using the commands detailed in the following sections.

Enabling TLS on the AOS VoIP VNS and VQM Features

Enable TLS on the AOS VoIP VNS and VQM features using the following commands:

1. The **voip name-service host** <*hostname*> **sip tls [srv** <*service-name-prefix*> **[**<*transport-name-prefix*>**]]** command adds the ability to specify TLS as the transport protocol when statically adding a name to the VNS cache. The <*hostname*> parameter is the fully qualified domain name (FQDN) of the added host. The optional **srv** parameters allows the modification of the SRV service and transport prefixes to the name. The literal text specified in the <*service-name-prefix*> and optional <*transport-name-prefix*> parameters are used to format the DNS SRV request used to resolve the domain name. Underscores are added automatically for prefixes. By default, the service name prefix is set to **sips** and the transport name prefix is set to **tcp**. To configure TLS as the transport protocol for a statically added host, enter the command from the Global Configuration mode as follows:

   ```
   (config)#voip name-service host voip.example.com sip tls
   ```

2. The **collector [primary | secondary]** <*value*> **tls** <*profile name*> **[**<*port*>**] [srv** <*service-name-prefix*> **[**<*transport-name-prefix*>**]]** command is used to configure a TLS connection between the AOS device's VQM reporter and the VQM collector in the network. TLS secures the content of the information collected by the device when it is being transferred to a VQM collector. The **primary** and **secondary** parameters specify whether this is a primary or secondary VQM collector. The <*value*> parameter is the IP address or FQDN of the collector. Either an address or domain name must be specified. The **tls** <*profile name*> parameter associates the TLS profile with the collector. A TLS profile must be specified. The optional <*port*> parameter specifies the target port to use when initiating the TLS session. Port **5061** is used by default. The optional **srv** parameters are used when the <*value*> parameter is specified as a domain

name. The literal text specified in the <*service-name-prefix*> and optional <*transport-name-prefix*> parameters are used to format the DNS SRV request used to resolve the domain name. Underscores are added automatically for prefixes. By default, the service name prefix is set to **sips** and the transport name prefix is set to **tcp**. Use the **no** form of this command to remove the collector from the VQM reporter. To specify **10.10.10.1** as the primary collection server using TLS profile **TLSPROFILE1** on the default port, enter the command as follows:

```
(config)#ip rtp quality-monitoring reporter REPORTER1
(config-rtp-reporter-REPORTER1)#collector primary 10.10.10.1 tls
  TLSPROFILE1
```

3. The **outbound-proxy [primary | secondary]** <*value*> **tls** <*profile name*> **[**<*port*>**] [srv** <*service-name-prefix*> **[**<*transport-name-prefix*>**]]** command to configure the IP address or host name of the outbound proxy used by the VQM reporter. TLS secures the content of the information collected by the device when it is being sent to the outbound proxy. The <*value*> parameter is the IP address or fully qualified domain name of the proxy server. Either an address or domain name must be specified. The **tls** <*profile name*> parameter associates the TLS profile with the proxy server. A TLS profile must be specified. The optional <*port*> parameter specifies the target port to use when initiating the TLS session. Port **5061** is used by default. The optional **srv** parameters are used when the <*value*> parameter is specified as a domain name. The literal text specified in the <*service-name-prefix*> and optional <*transport-name-prefix*> parameters are used to format the DNS SRV request used to resolve the domain name. Underscores are added automatically for prefixes. By default, the service name prefix is set to **sips** and the transport name prefix is set to **tcp**.

   Use the **no** form of this command to remove the outbound proxy from the VQM reporter. To specify **10.10.10.2** as the outbound proxy server using TLS profile **TLSPROFILE1** on the default port, enter the command as follows:

```
(config)#ip rtp quality-monitoring reporter REPORTER1
(config-rtp-reporter-REPORTER1)#outbound-proxy primary 10.10.10.2 tls
  TLSPROFILE1
```

Enabling TLS and SRTP on the AOS SIP Proxy

Enable TLS and SRTP on the AOS SIP Proxy using the following commands:

1. The **sip proxy sip-server [primary | secondary]** <*hostname* | *ip address*> **tls** <*profile name*> **[**<*TLS port*>**] [srv** <*service-name-prefix*> **[**<*transport-name-prefix*>**]]** command specifies that the SIP server uses TLS for SIP traffic between the AOS SIP proxy and the softswitch. The **primary** and **secondary** keywords specify whether you are configuring the primary or secondary SIP server. The <*hostname* | *ip address*> parameter is the fully qualified domain name (FQDN) or IP address of the outbound SIP proxy server. IPv4 address should be expressed in dotted decimal notation (for example, **208.61.209.1**). If a host name is used to specify the outbound SIP proxy server, a DNS server must be configured on the AOS unit manually, or learned via a dynamic IP interface.

   The **tls** <*profile name*> parameter associates the TLS profile with the SIP proxy server. A TLS profile must be specified. The optional <*tls port*> parameter specifies the target port to use when initiating the TLS session. Port **5061** is used by default. To configure the softswitch with a TLS profile, the TLS profile must have been created prior to adding it to the proxy server. If a specified TLS profile is ever deleted, both the primary and all secondary softswitches are automatically removed from the AOS device's configuration.

   The optional **srv** parameters allows the modification of the SRV service and transport prefixes to the name. The literal text specified in the <*service-name-prefix*> and optional <*transport-name-prefix*> parameters are used to format the DNS SRV request used to resolve the domain name. Underscores are added automatically for prefixes. By default, the service name prefix is set to **sips** and the transport name prefix is set to **tcp**.

To apply a TLS profile to a server used by the AOS SIP proxy, enter the command from the Global Configuration mode as follows:

```
(config)#sip proxy sip-server primary 198.51.100.1 tls profile TLSPROFILE1
```

2. The **sip proxy srtp server** *<profile name>* **[allow-non-rtp-media] [tls-optional]** command configures SRTP on the server side of the SIP proxy. The *<profile name>* parameter specifies a name for the SRTP profile to apply to the server side of the SIP proxy. By default, no SRTP profile is configured for the SIP proxy; however, when one is configured, any non-RTP media is rejected by default. The **no** version of this command disables the SRTP feature on the AOS SIP proxy.

   The optional **allow-non-rtp-media** parameter configures SRTP to allow non-RTP traffic media, such as T.38 over UDPTL, that cannot be protected by SRTP. When this option is specified, RTP media is secured by SRTP, but any non-RTP media is forwarded unsecured. By default, when SRTP is configured, the proxy rejects any non-RTP media to prevent unsecured media from transversing the device. In AOS, when an SDP offer arrives at the proxy that has SRTP enabled, the proxy removes any non-RTP media before forwarding the SDP offer. The proxy indicates to the offerer that the non-RTP media has been rejected. If no media is left after the non-RTP media is removed, the call is terminated with either a SIP error response or SIP BYE message. When non-RTP media is allowed to pass through the SRTP enabled SIP proxy, all RTP media is secured by SRTP, but any non-RTP media is forwarded unsecured.

   The optional **tls-optional** parameter removes the requirement that SRTP key negotiation is protected by TLS. This setting is NOT RECOMMENDED. When this feature is disabled, the system does not send SRTP in outbound offers or accept SRTP in inbound offers unless the SIP messaging is protected by TLS, thus keeping SRTP keys from transversing an unsecured channel.

   To configure and apply an SRTP profile to the server side of the SIP proxy, enter the command from the Global Configuration mode as follows:

```
(config)#sip proxy srtp server PROFILE1
```

4. TLS and SRTP Configuration Examples

The following section describes a typical TLS and SRTP configuration on an AOS device, in which SIP signaling and media are protected on the SIP trunk between the AOS device and a service provider. The customer PBX is connected to the AOS device via a PRI. The AOS device is operating in client-only mode with a persistent connection to the SIP server. The persistent connection is established after the unit boots up and attempts to register with the SIP server. *Figure 1* describes the network configuration for this example.

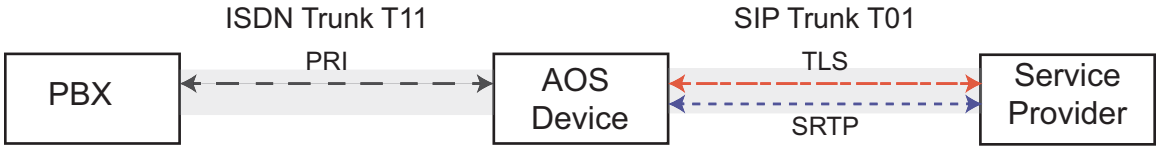

Figure 1. SIP Signaling and Media Protected Between a SIP PBX and Service Provider

NOTE

The configuration parameters entered in these examples are sample configurations only. You should configure these applications in a manner consistent with the needs of your particular network. You should make the necessary adjustments to these configurations before adding them to your configuration to ensure they will function properly in your network.

The following is the pertinent configuration on the AOS device:

```
crypto ca profile "PROVIDER_CA"
!
crypto ca certificate chain "PROVIDER_CA"
  certificate ca 99a9506fe22878b9
-----BEGIN CERTIFICATE-----
MIID3zCCAsegAwIBAgIJAJmpUG/iKHi5MA0GCSqGSIb3DQEBCwUAMIGFMQswCQYD
VQQGEwJVUzEQMA4GA1UECAwHQWxhYmFtYTETMBEGA1UEBwwKSHVudHN2aWxsZTEV
MBMGA1UECgwMQURUUkFOLCBJbmMuMRYwFAYDVQQLDA1Eb2N1bWVudGF0aW9uMSAw
HgYDVQQDDBdBRFRSQU4gRG9jdW1lbnRhdGlvbiBDQTAeFw0xNDExMTgyMzM0NDha
Fw0xNzExMTcyMzM0NDhaMIGFMQswCQYDVQQGEwJVUzEQMA4GA1UECAwHQWxhYmFt
YTETMBEGA1UEBwwKSHVudHN2aWxsZTEVMBMGA1UECgwMQURUUkFOLCBJbmMuMRYw
FAYDVQQLDA1Eb2N1bWVudGF0aW9uMSAwHgYDVQQDDBdBRFRSQU4gRG9jdW1lbnRh
dGlvbiBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKWkIh9MycuR
F1p6KsH6nQXQw/Fmbnl7RFOFTFKl5HzETFIHQnkZQR8QvgZ7CZAC4o0A1QwuXbTq
OdroS/3hC7rhGIP8RrEmxEkI+deM57pmYXTG63puL9pgWGHyr2PVBnvLMFule8kn
n3fmDZLTvpSfZOR1vnBXdWWcgiFbSvLZDuMNL2uTyTQtbwg26GThs19SwUpTZv4L
kP7Ddr23EAcK5uYszhrD3ZKUQxrL3/6zeM0IudUQgW8tMu1fonXWF2Yff8VedfmP
G5/X78EjHLT2uKYlEWJSRl0YBje6SUAm8SVqaR1FBBhNMAXn8ClAIxreNfBf2lJS
Bp4KFc6fAG0CAwEAAaNQME4wHQYDVR0OBBYEFElQUMpZl5VWgl8thOyKXZUIsLct
MB8GA1UdIwQYMBaAFElQUMpZl5VWgl8thOyKXZUIsLctMAwGA1UdEwQFMAMBAf8w
DQYJKoZIhvcNAQELBQADggEBAF/JCpfmF5Uf06rTEHqsaPZel/HNVIzPn4w8Rbgo
5qxy/SsygLa0KNJHDD+lENO6zSFpDYHSuom4mUr1BerUlW+PIytbob8njmASlb43
WepxhIoWWYa/OK0MPt9ck/N6Y6zI3Ioxw/iARe4b+7wJqXtGJ/DIJO54oGvSf3pg
uwZIEn7fO9PIcIPWLHeg1S/tbVeUWIELgr/f2a6i9PwdaKBBnYMS9qS1f6FvQtUM
DcfrMqzZF1wKfr+1q9Gb0XAtApkIH45sN6sN0DkzzKtECCexuNJcqacNCZY1tWEJ
KGmkJ4RTzBsi8me3ze40/RjLwgZNhsIFnC3Z+vzcDH+fskc=
-----END CERTIFICATE-----
quit
!
!
tls-profile PROVIDER_TLS
  tls-version 1.2
  ca-profile PROVIDER_CA
  validate identity ip-address
  validate identity fqdn configured
  secure-ciphersuite TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  secure-ciphersuite TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  secure-ciphersuite TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
  secure-ciphersuite TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
  no secure-ciphersuite TLS_RSA_WITH_AES_256_CBC_SHA
  no secure-ciphersuite TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
  no secure-ciphersuite TLS_RSA_WITH_3DES_EDE_CBC_SHA
  secure-ciphersuite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  secure-ciphersuite TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  no secure-ciphersuite TLS_RSA_WITH_AES_128_CBC_SHA
  no secure-ciphersuite SSL_DES_192_EDE3_CBC_WITH_MD5
!
!
```

```
interface t1 0/3
  tdm-group 1 timeslots 1-24
  no shutdown
!
!
interface pri 1
  connect t1 0/3 tdm-group 1
  no shutdown
!
!
timing-source t1 0/3
!

isdn-group 1
  connect pri 1
!
sip tls
!
srtp-profile PROVIDER_SRTP
  crypto-suite AES_CM_128_HMAC_SHA1_80
!
voice trunk T01 type sip
description PROVIDER SIP TRUNK
sip-server primary voip.example.com tls PROVIDER_TLS
sip-server validation register
  srtp PROVIDER_SRTP
  register 2565550100 auth-name 2565550100 password 7164bd8f04bef2cf
  grammar contact host port persistent
!
voice trunk T11 type isdn
description PBX
connect isdn-group 1
!
voice grouped-trunk PROVIDER
trunk T01
accept NXX-NXX-XXXX cost 0
  accept 1-NXX-NXX-XXXX cost 0
 accept 011-$ cost 0
  accept 411 cost 0
  accept 611 cost 0
  accept 911 cost 0
!
voice grouped-trunk PBX
trunk T11
accept <DIDs/DID patterns>
accept <PBX extension patterns>
!
```

5. TLS and SRTP Configuration Command Summary

The following tables summarize the configuration commands used for TLS and SRTP configuration.

Table 4. CA Profile Configuration Commands for TLS/SRTP

Prompt	Command	Description
(config)#	**[no] crypto ca profile** <*profile name*>	Creates a CA profile and enters the profile's configuration mode. A profile must be created before authenticating, importing, or enrolling CA certificates. Use the **no** form of this command to remove the profile from the AOS device's configuration.
(config)#	**crypto ca authenticate** <*profile name*> **[**<*drive*> <*name*>**]**	Imports and authentications a CA certificate for the named profile. The optional <*drive*> and <*name*> parameters specify that the certificate to be authenticated is located by the file's location and name. This bypasses the terminal loading process. The command is used for authenticating manually configured trusted certificates.
(config)#	**crypto ca enroll** <*profile name*> **[**<*drive*> <*name*>**] [force-overwrite]**	Creates the certificate request and begins the enrollment process. The file is saved locally to the specified drive with the specified file name. The <*profile name*> parameter is the name of the CA profile. The optional **force-overwrite** option specifies the AOS device will overwrite any existing file with the same name. The command is used for configuring a trusted certificate manually.
(config)#	**crypto ca import** <*profile name*> <**certificate	crl**> **[**<*drive*> <*name*>**]**	Imports a self certificate (**certificate**) or a CRL (**crl**) for the specified CA profile. The certificate or CRL can be imported from a specific file using the optional <*drive*> and <*name*> parameters. If the file is specified, terminal loading is bypassed. The command is used to import manually configured trusted certificates.

Table 5. TLS Profile Configuration Commands

Prompt	Command	Description
(config)#	**[no] tls-profile** <*profile name*>	Creates the TLS profile and enters the profile's configuration mode. The **no** form of this command removes the TLS profile from the AOS device's configuration.
(config-tls-profile-TLSPROFILE1)#	**[no] tls-version [1.2 | 1.1 | 1.0] fallback [1.2 | 1.1 | 1.0]**	Sets the TLS version as a fixed value, or allows fallback from the highest supported version to the lowest specified version. By default, **fallback 1.2** is enabled. The **no** form of this command returns the version to the default value.
(config-tls-profile-TLSPROFILE1)#	**[no] authentication mutual**	Enables mutual authentication in the TLS profile. The **no** form of this command disables mutual authentication and reverts to server authentication (default authentication method).
(config-tls-profile-TLSPROFILE1)#	**[no] secure-ciphersuite** <*name*> **[**<*number*>**]**	Specifies a TLS cipher suite to be used by the TLS profile. The <*name*> parameter is the cipher suite's name, and the optional <*number*> parameter is the position of the suite among all enabled cipher suites in the profile. Valid number range is **1** to **65535**. The **no** form of this command removes the suite from the profile's configuration.
(config-tls-profile-TLSPROFILE1)#	**[no] ca-profile** <*name*>	Applies a CA profile to the TLS profile. A CA profile must be specified for TLS operation. The **no** form of this command removes the CA profile from the TLS profile's configuration.
(config-tls-profile TLSPROFILE1)#	**[no] validate identity [fqdn configured | fqdn resolved | ip-address | string]**	Controls how the identity of the TLS communication peer's certificate, received during the TLS handshake, is validated. The **fqdn configured** parameter specifies that the peer's subject alternative name (SAN) IP domain naming service (DNS) name is used to validate the peer. The name must match the FQDN configured for the peer at the trunk. The **fqdn resolved** parameter specifies that the peer's SAN IP domain DNS name is used to validate the peer. The name must match the FQDN as resolved by DNS SRVs from the FQDN as configured for the peer at the trunk. The **ip-address** parameter specifies that the peer's SAN IP address is used to validate the peer. The address must match the IP address configured or resolved by DNS for the peer at the trunk. The **string** parameter specifies that the peer's SAN fields or Subject components are used to identify the peer. The string must match the string configured at the trunk (using the **peer-certificate-identity** command from the trunk's configuration mode). By default, identity validations are disabled and only proper signing is verified. The **no** form of this command removes the identity validation method from the TLS profile.

Table 6. SRTP Profile Configuration Commands

Prompt	Command	Description
(config)#	**[no] srtp-profile** <*profile name*>	Creates an SRTP profile and enters the profile's configuration mode. The **no** form of this command removes the SRTP profile from the AOS device's configuration.
(config-srtp-profile-SRTPPROFILE1)#	**crypto-suite** <*name*>	Specifies the SRTP crypto suite to be used by the SRTP profile. By default, only the **AES_CM_128_HMAC_SHA1_80** crypto suite is enabled.
(config-srtp-profile-SRTPPROFILE1)#	**srtp [auth | offer-no-auth | strict-no-auth]**	Specifies the SRTP authentication method used by the profile. The **auth** parameter indicates that SRTP must be authenticated (default setting), the **offer-no-auth** parameter indicates authentication may or may not be used, and the **strict-no-auth** parameter indicates authentication is not used.
(config-srtp-profile-SRTPPROFILE1)#	**srtp [encrypt | offer-no-encrypt | strict-no-encrypt]**	Specifies the SRTP encryption method used by the profile. The **encrypt** parameter indicates SRTP must be encrypted (default setting), the **offer-no-encrypt** parameter indicates encryption may or may not be used, and the **strict-no-encrypt** parameter indicates encryption is not used.
(config-srtp-profile-SRTPPROFILE1)#	**srtcp [encrypt | offer-no-encrypt | strict-no-encrypt]**	Specifies the SRTCP encryption method used by the profile. The **encrypt** parameter indicates SRTCP must be encrypted (default setting), the **offer-no-encrypt** parameter indicates encryption may or may not be used, and the **strict-no-encrypt** parameter indicates encryption is not used.

Table 7. Global TLS Configuration Command

Prompt	Command	Description
(config)#	**[no] sip tls [**<*port*>**]**	Enables TLS transports globally for TLS negotiation. The optional <*port*> parameter specifies the TCP port on which the SIP stack listens for TLS packets. The port is set to **5061** by default. The **no** form of this command disables TLS.

Table 8. Trunk TLS and SRTP Configuration Commands

Prompt	Command	Description
(config-T01)#	**[no] sip-server [primary | secondary]** <*value*> **tls** <*profile name*> **[**<*port*>**]** **[srv** <*service-name-prefix*> **[**<*transport-name-prefix*>**]]**	Specifies the TLS trunk's SIP server settings for a primary or secondary SIP server. The <*value*> parameter is the IP address or FQDN of the device that is the peer for this trunk. The **tls** <*profile name*> parameter associates the TLS profile with the SIP server. The optional <*port*> parameter specifies the port to use for TLS sessions (**5061** by default). The optional **srv** <*service-name-prefix*> and <*transport-name-prefix*> are used when an FQDN is specified. The **no** form of this command removes the SIP server from the trunk
(config-T01)#	**[no] registrar [primary | secondary]** <*value*> **tls** <*profile name*> **[**<*port*>**]** **[srv** <*service-name-prefix*> **[**<*transport-name-prefix*>**]]**	Specifies the TLS trunk's registrar settings for a primary or secondary SIP registrar server. The <*value*> parameter is the IP address or FQDN of the device that is the peer for this trunk. The **tls** <*profile name*> parameter associates the TLS profile with the registrar. The optional <*port*> parameter specifies the port to use for TLS sessions (**5061** by default). The optional **srv** <*service-name-prefix*> and <*transport-name-prefix*> are used when an FQDN is specified. The **no** form of this command removes the registrar from the trunk.
(config-T01)#	**[no] outbound-proxy [primary | secondary]** <*value*> **tls** <*profile name*> **[**<*port*>**]** **[srv** <*service-name-prefix*> **[**<*transport-name-prefix*>**]]**	Specifies the TLS trunk's outbound proxy settings for a primary or secondary outbound proxy. The <*value*> parameter is the IP address or FQDN of the device that is the peer for this trunk. The **tls** <*profile name*> parameter associates the TLS profile with the outbound proxy. The optional <*port*> parameter specifies the port to use for TLS sessions (**5061** by default). The optional **srv** <*service-name-prefix*> and <*transport-name-prefix*> are used when an FQDN is specified. The **no** form of this command removes the outbound proxy from the trunk
(config-T01)#	**[no] peer-certificate-identity** <*string*>	Configures a static string used in peer validation for TLS. The <*string*> value is the literal text specified at the trunk and used by the TLS profile to match for validation. The **no** form of this command removes the string from the trunk's configuration.
(config-T01)#	**[no] sip-server validation register**	Enables validated SIP trunk failover. Use the **no** form of this command to disable the feature.
(config-T01)#	**[no] grammar contact host port persistent**	Specifies that the TCP port from which AOS initiated the TLS connection is visible in the Contact URI sent by AOS. Use the **no** form of this command to disable the feature.

Table 8. Trunk TLS and SRTP Configuration Commands *(Continued)*

Prompt	Command	Description
(config-T01)#	**[no] srtp [allow-non-rtp-media] [optional avp] [optional avp-savp] [reduced-rekeying] [roc-reset-on-reinvite] [tls-optional]** <*srtp profile*>	Enables SRTP functionality on the trunk. The optional **allow-non-rtp-media** parameter specifies that SRTP allows non-RTP media, such as T.38 over UDPTL, that cannot be protected by SRTP. The optional **optional avp** parameter specifies that RTP AVP is used for both offers and RTP/AVP answers containing crypto attributes. The optional **optional avp-savp** parameter specifies that RTP AVP is used for offers and the SAVP is used for RTP/AVP answers containing crypto attributes. The optional **reduced-rekeying** parameter specifies that rekeying on reINVITES will be disabled if the received SDP offer is unchanged. The optional **roc-reset-on-reinvite** parameter specifies that AOS will reset the outbound rollover counter (ROC) when it sends a reINVITE. The optional **tls-optional** parameter allows SDES negotiation of SRTP is permitted over an unsecure control channel (NOT RECOMMENDED). The <*srtp profile*> is the SRTP profile to associate with the trunk. The **no** form of this command removes the profile from the trunk.

Table 9. TLS for Additional AOS Features Configuration Commands

Prompt	Command	Description
(config)#	**voip name-service host** <*hostname*> **sip tls [srv** <*service-name-prefix*> **[**<*transport-name-prefix*>**]]**	Adds the ability to specify TLS as the transport protocol when statically adding a name to the VNS cache. The <*hostname*> parameter is the FQDN of the added host. The optional **srv** <*service-name-prefix*> and <*transport-name-prefix*> are used when an FQDN is specified.
(config-rtp-reporter-REPORTER1)#	**collector [primary | secondary]** <*value*> **tls** <*profile name*> **[**<*port*>**]** **[srv** <*service-name-prefix*> **[**<*transport-name-prefix*>**]]**	Configures TLS connection between the AOS device's VQM reporter and the VQM collector in the network. The **tls** <*profile name*> associates a TLS profile with the VQM collector. The optional <*port*> parameter specifies the port used for the TLS session (**5061** by default). The optional **srv** <*service-name-prefix*> and <*transport-name-prefix*> are used when an FQDN is specified for the <*value*> parameter.

Table 9. TLS for Additional AOS Features Configuration Commands *(Continued)*

Prompt	Command	Description
(config-rtp-reporter-REPORTER1)#	**outbound-proxy [primary | secondary]** <*value*> **tls** <*profile name*> **[**<*port*>**] [srv** <*service-name-prefix*> **[**<*transport-name-prefix*>**]]**	Configures the IP address or host name of the outbound proxy used by the VQM reporter. TLS secures the content of the information collected by the device when it is being sent to the outbound proxy. The **tls** <*profile name*> associates a TLS profile with the VQM collector. The optional <*port*> parameter specifies the port used for the TLS session (**5061** by default). The optional **srv** <*service-name-prefix*> and <*transport-name-prefix*> are used when an FQDN is specified for the <*value*> parameter.
(config)#	**sip proxy sip-server [primary | secondary]** <*hostname* | *ip address*> **tls** <*profile name*> **[**<*tls port*>**] [srv** <*service-name-prefix*> **[**<*transport-name-prefix*>**]]**	Specifies that the SIP server uses TLS for SIP traffic between the AOS SIP proxy and the softswitch. The **primary** and **secondary** keywords specify whether you are configuring the primary or secondary SIP server. The <*hostname* | *ip address*> parameter is the fully qualified domain name (FQDN) or IP address of the outbound SIP proxy server. IPv4 address should be expressed in dotted decimal notation (for example, **208.61.209.1**). The **tls** <*profile name*> parameter associates the TLS profile with the SIP proxy server. The optional <*tls port*> parameter specifies the target port to use when initiating the TLS session. Port **5061** is used by default.The optional **srv** parameters allows the modification of the SRV service and transport prefixes to the name. By default, the service name prefix is set to **sips** and the transport name prefix is set to **tcp**.
(config)#	**sip proxy srtp server** <*profile name*> **[allow-non-rtp-media] [tls-optional]**	Configures SRTP on the server side of the SIP proxy. The <*profile name*> parameter specifies a name for the SRTP profile to create and apply to the SIP proxy server. The optional **allow-non-rtp-media** parameter configures SRTP to allow non-RTP traffic media, such as T.38 over UDPTL, that cannot be protected by SRTP. The optional **tls-optional** parameter removes the requirement that SRTP key negotiation is protected by TLS. This setting is NOT RECOMMENDED.

6. Troubleshooting TLS and SRTP

Troubleshooting the configuration of TLS and SRTP services can be done by using various **show**, **clear**, and **debug** commands from the CLI.

Show Commands

The **show** commands are used to display current configurations and states of the various TLS and SRTP components, including configured CA profiles, CA certificates, TLS profiles, TLS sessions, TLS statistics, SRTP sessions, and SRTP statistics. Reviewing the configuration of these items allows you to verify item configurations as a first step in troubleshooting functionality issues. The **show** commands available for CA, TLS, and SRTP configurations, entered from the Enable mode prompt, include the following:

1. Use the **show crypto ca certificates** command to display configured CA certificates. Displayed information includes key usage, extended key usage, associated URIs, whether the certificate is self-signed, and other certificate information. Enter the command from the Enable mode prompt as follows:

   ```
   #show crypto ca certificates
   ```

2. Use the **show crypto ca profiles** command to display the settings configured for CA profiles. Displayed information includes the profile enrollment mode, the drive and file name (if specified), extended key usage, configured URI, and other profile information. Enter the command from the Enable mode prompt as follows:

   ```
   #show crypto ca profiles
   ```

3. Use the **show tls profile [**<*profile name*>**]** command to display the content of configured TLS profiles on the AOS device. The optional <*profile name*> parameter limits the output to the named TLS profile. By default, all TLS profiles are displayed. Enter the command from the Enable mode prompt as follows:

   ```
   #show tls profile TLS_PROFILE1
   Name: TLS_PROFILE1
   tls-version: 1.2
   authentication: server
   ca-profile:PROFILE1
   allow-self-signed-cert: no
   Identities Validated:
     ip-address
     fqdn configured
   Ciphersuite list:
     TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
     TLS_DHE_RSA_WITH_AES_256_CBC_SHA
     TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
     TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
     TLS_RSA_WITH_AES_256_CBC_SHA
     TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
     TLS_RSA_WITH_3DES_EDE_CBC_SHA
     TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
     TLS_DHE_RSA_WITH_AES_128_CBC_SHA
     TLS_RSA_WITH_AES_128_CBC_SHA
     SSL_DES_192_EDE3_CBC_WITH_MD5
   ```

4. Use the **show tls sessions** command to display information about each active TLS sessions. Enter the command from the Enable mode prompt as follows:

   ```
   #show tls sessions
   Application: SIP
   ```

```
Version: TLS v1.2
Ciphersuite: AES256-SHA
Session ID: kKnKqvAM70IkGRBxzVHdVb8F8vkHpsL28A3D89xDGjA=
Role: Client-only
Local: 192.0.2.243:10459
Peer: 198.51.100.4:5061
Peer Certificate:
  Subject: CN = voip.example.com
  SAN IP Address:  2001:DB8:64FE::4 198.51.100.4  (Validated)
  SAN FQDN: ipv6.voip.example.com ipv4.ents.adtran.com voip.example.com
  (Validated)

There are 1 active TLS sessions
```

5. Use the **show tls statistics** command to display a summary of statistics for TLS on the AOS device. Enter the command from the Enable mode prompt as follows:

```
#show tls statistics
TLS Connection Requests
  Total:2
  Passed:2
  Failed:0
TLS Handshake
  Passed:2
  Failed:0
TLS Connections
  Dropped:0
  Closed:1
```

6. Use the **show rtp media sessions** command to display whether the media session is using SRTP. Enter the command from the Enable mode prompt as follows:

```
#show rtp media sessions
----------- --- ------- ---- ------- -------
  ------------------------------------------------------------------------
    Call ID TTL Packets Ovrd Type    Session   SRTP
----------- --- ------- ---- ------- -------
  ------------------------------------------------------------------------
          1  45 160     No   Audio   DspSrtp   Yes
    Anchored: 10.19.247.5:10000
    Remote:   10.100.254.4:19888

          1  45 168     No   Audio   IntSrtp   Yes
    Anchored: [::]:10002
    Remote:   127.0.0.1:10002

          1  41 0       No   Audio   DspSrtp   Yes
    Anchored: 10.19.247.5:10001
    Remote:   10.100.254.4:19889

          1  41 0       No   Audio   IntSrtp   Yes
    Anchored: [::]:10003
```

```
        Remote:   127.0.0.1:10003

    There are 4 active media sessions.
```

Clear Commands

The **clear** commands associated with TLS and SRTP are used to clear statistics associated with TLS or SRTP sessions. Use the **clear sip tls session** <***** | *session ID*> command to clear the specified active TLS session. The ***** parameter clears all the TLS sessions used for SIP. The <*session ID*> parameter specifies the session ID of the individual TLS session to clear. To clear the TLS sessions, enter the command from the Enable mode prompt as follows:

```
#clear sip tls session *
```

Debug Commands

The **debug** commands associated with TLS and SRTP can be used to aid in troubleshooting TLS and SRTP configurations. The available TLS and SRTP **debug** commands include the following:

1. Use the **debug crypto pki** command to activate all public key infrastructure (PKI) debug messages. These messages include the interactions within certificate and CRL storage parameters and between applications using certificates (such as IKE or TLS) and certificate and CRL storage. Enter the command from the Enable mode prompt as follows:

   ```
   #debug crypto pki
   ```

2. Use the **debug tls sip** <**events | negotiation**> command to enable debug messages for SIP TLS. The command can be entered multiple times, once for each parameter. The **events** parameter displays TLS events (such as errors and state changes), and the **negotiation** parameter displays information about each step of all TLS handshakes. If no additional parameters are specified, by default TLS events for any port are displayed. Enter the command from the Enable mode prompt as follows:

   ```
   #debug tls sip
   ```

3. Use the **debug voice srtp sdes [events | negotiation | parse]** command to enable debug messages for the SDES method of key management for SRTP. The command can be entered multiple times, once for each parameter. The optional **events** parameter displays SDES events, such as errors an state changes. The optional **negotiation** parameter displays information about each step of all SDES negotiations. The optional **parse** parameter displays information about the parsing of the SDES content. If no optional parameters are specified, by default SDES events are displayed. Enter the command from the Enable mode prompt as follows:

   ```
   #debug voice srtp sdes
   ```

7. Warranty and Contact Information

Warranty and contact information for all ADTRAN products can be obtained using the information in the following sections.

Warranty

Warranty information can be found online by visiting www.adtran.com/warranty.

Contact Information

To contact ADTRAN, choose one of the following methods:

Department	Contact Information	
Customer Care	From within the U.S.: From outside the U.S.:	(888) 4ADTRAN ((888)-423-8726)+ +1 (256) 963-8716
Technical Support	Support Community Product Support:	www.supportforums.adtran.com www.adtran.com/support
Training	Email: ADTRAN University:	training@adtran.com www.adtran.com/training
Sales	For pricing and availability:	1 (800) 827-0807