



Avaya Solution & Interoperability Test Lab

Configuring SIP Trunks using Transport Layer Security and Secure Real-time Transport Protocol among Avaya Aura[®] Session Manager 6.2 FP2, AudioCodes Mediant 3000 Media Gateway 3.0 and Avaya Aura[®] Communication Manager 6.2 FP2 - Issue 1.0

Abstract

These Application Notes describe a network using SIP trunks among Avaya Aura[®] Session Manager Release 6.2 FP2, AudioCodes Mediant 3000 Media Gateway Release 3.0 and Avaya Aura[®] Communication Manager Evolution Server Release 6.2 FP2.

- Avaya Aura[®] Session Manager provides SIP proxy/routing functionality, routing SIP sessions across a TCP/IP network with centralized routing policies and registrations for SIP endpoints.
- AudioCodes Mediant 3000 Media Gateway consolidates PSTN facilities by concentrating and routing the calls over a SIP trunk to Avaya Aura[®] Session Manager.
- Avaya Aura[®] Communication Manager serves as an Evolution Server within the Avaya Aura[®] architecture and supports SIP endpoints registered to Avaya Aura[®] Session Manager.

To provide secure network connections, all SIP trunks use Transport Layer Security (TLS) protocol and Secure Real-time Transport Protocol (SRTP) is used for media.

These Application Notes provide information for the setup, configuration, and verification of the call flows tested in this solution.

Table of Contents

1.	Introduction.....	4
2.	Interoperability Testing.....	4
2.1.	Test Results and Observations	4
3.	Reference Configuration.....	5
4.	Equipment and Software Validated	7
5.	Configure Avaya Aura® Communication Manager.....	8
5.1.	Verify System Capacities and Licensing	8
5.1.1.	Verify Off-PBX Telephones Capacity.....	8
5.1.2.	Verify SIP Trunk Capacity	9
5.1.3.	Verify AAR/ARS Routing is Enabled	9
5.1.4.	Verify Media Encryption is Supported	10
5.1.5.	Verify Private Networking is Enabled.....	10
5.1.6.	Verify AAR Access Code.....	10
5.1.7.	Verify Initial INVITE with SDP for Secure Calls is Enabled	11
5.2.	Configure Trunk-to-Trunk Transfers	11
5.3.	Configure IP Codec Set.....	12
5.4.	Configure IP Network Region.....	12
5.5.	Add Node Names and IP Addresses	13
5.6.	Configure SIP Signaling Group	14
5.7.	Add SIP Trunk Group	15
5.8.	Configure Route Pattern.....	16
5.9.	Administer Private Numbering Plan	17
5.10.	Administer Uniform Dial Plan	18
5.11.	Administer AAR Analysis.....	18
5.12.	Configure Stations	19
5.13.	Verify Off-PBX-Telephone Station-Mapping.....	19
5.14.	Save Translations.....	19
6.	Configure Avaya Aura® Session Manager	20
6.1.	Define SIP Domains.....	21
6.2.	Define Locations	22
6.3.	Define SIP Entities	23
6.4.	Define Entity Links	25
6.5.	Define Routing Policy for SIP Users	26
6.6.	Define Routing Policies for AudioCodes Mediant 3000 Gateway	27
6.7.	Define Dial Patterns	28
7.	Configure AudioCodes Mediant 3000 Media Gateway.....	29
7.1.	Select Configurable Parameters	30
7.2.	Configure General Security Settings.....	31
7.3.	Configure HTTPS Security Settings	32
7.4.	Configure SIP Protocols and Ports.....	33
7.5.	Configure Codec Preferences.....	35
7.6.	Configure Trunk Group.....	36
7.7.	Configure Tel-to-IP Routing	37
7.8.	Configure Trunk Group Routing.....	38
7.9.	Configure SIP Proxy	39

7.10.	Configure Privacy Feature.....	40
7.11.	Generate TLS Certificate on AudioCodes Mediant 3000 Gateway	41
7.12.	Upload TLS Certificate to Avaya Aura® Session Manager	43
7.13.	Upload Avaya Aura® System Manager Root Certificate	45
7.14.	Configure Media Settings.....	50
8.	Verification Steps.....	51
8.1.	Verify Avaya Aura® Session Manager Configuration	51
8.2.	Verify AudioCodes Mediant 3000 Media Gateway Configuration	53
8.3.	Verify Avaya Aura® Communication Manager Operational Status	56
9.	Conclusion	58
10.	Additional References.....	59

1. Introduction

These Application Notes describe configuration of a network that uses SIP trunks among Avaya Aura® Session Manager Release 6.2 FP2, AudioCodes Mediant 3000 Media Gateway Release 3.0 and Avaya Aura® Communication Manager Release 6.2 FP2.

To provide secure network connections, all SIP trunks use Transport Layer Security (TLS) protocol and Secure Real-time Transport Protocol (SRTP) is used for media.

These Application Notes focus on the configuration of Avaya Aura® Session Manager, AudioCodes Mediant 3000 Media Gateway and Avaya Aura® Communication Manager Evolution Server using Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP). These instructions assume the following steps have already been completed.

- AudioCodes Mediant 3000 Media Gateway is installed, configured and operational and PSTN connectivity been established and is operational.
- Avaya Aura® Session Manager is installed, configured and operational.
- Avaya Aura® System Manager is installed, configured and operational.
- Avaya Aura® Communication Manager is installed, configured and operational.
- SIP Users are defined in System Manager and are registered to Session Manager.

Detailed administration of other aspects of AudioCodes Mediant 3000 Media Gateway, Communication Manager, System Manager or Session Manager will not be described. See the appropriate documentation listed in **Section 10** for more information.

2. Interoperability Testing

Test cases included bi-directional calls between PSTN users and Avaya IP Deskphones registered as SIP users to Session Manager using SRTP for media, as well as traditional telephony operations and features such as extension dialing, displays, hold/resume, block calling party ID, transfer, conferencing, and call forwarding.

2.1. Test Results and Observations

All test cases were successful.

3. Reference Configuration

These Application Notes describe configuration of a network that uses SIP trunks among Avaya Aura® Session Manager Release 6.2 FP2, AudioCodes Mediant 3000 Media Gateway R3.0 and Avaya Aura® Communication Manager Release 6.2 FP2.

In the sample configuration shown in **Figure 1**, a PSTN trunk delivers customer calls using a ISDN trunk interface to AudioCodes Mediant 3000 Media Gateway (M3K). The AudioCodes M3K Media Gateway converts the calls to SIP and routes them to Avaya Aura® Session Manager, using the SIP Signaling network interface on Session Manager.

Avaya 9600 Series IP Deskphones utilize the Avaya Aura® Session Manager User Registration feature and are supported by Avaya Aura® Communication Manager. For the sample configuration, SIP users are not IP Multimedia Subsystem (IMS) users and Communication Manager is configured as an Evolution Server in the Avaya Aura® architecture. When Communication Manager is configured as an Evolution Server, it applies both origination-side and termination-side features in a single step. For more information regarding configuring Communication Manager as an Evolution Server, see **References [4] through [7] in Section 10**.

Avaya Aura® Communication Manager is connected to Session Manager via a non-IMS SIP signaling group and associated SIP trunk group using Transport Layer Security (TLS) protocol.

Avaya Aura® Session Manager is managed by Avaya Aura® System Manager. For the sample configuration, Avaya Aura® Session Manager is running on a separate Avaya S8800 Server. Avaya Aura® Communication Manager Evolution Server runs on a pair of duplicated Avaya S8800 servers with an Avaya G650 Media Gateway.

AudioCodes Mediant 3000 Media Gateway provides consolidation of PSTN facilities into SIP. Audiocodes M3K Media Gateway is a carrier class product that offers channel scalability in a 19"-2U chassis. AudioCodes M3K Media Gateway provides a web-based user interface that is used for operations, administration, management, and provisioning functions.

Note: to simulate calls from PSTN network, a separate Avaya Aura® Communication Manager system is connected over ISDN trunk to Audiocodes Mediant 3000 Media Gateway.

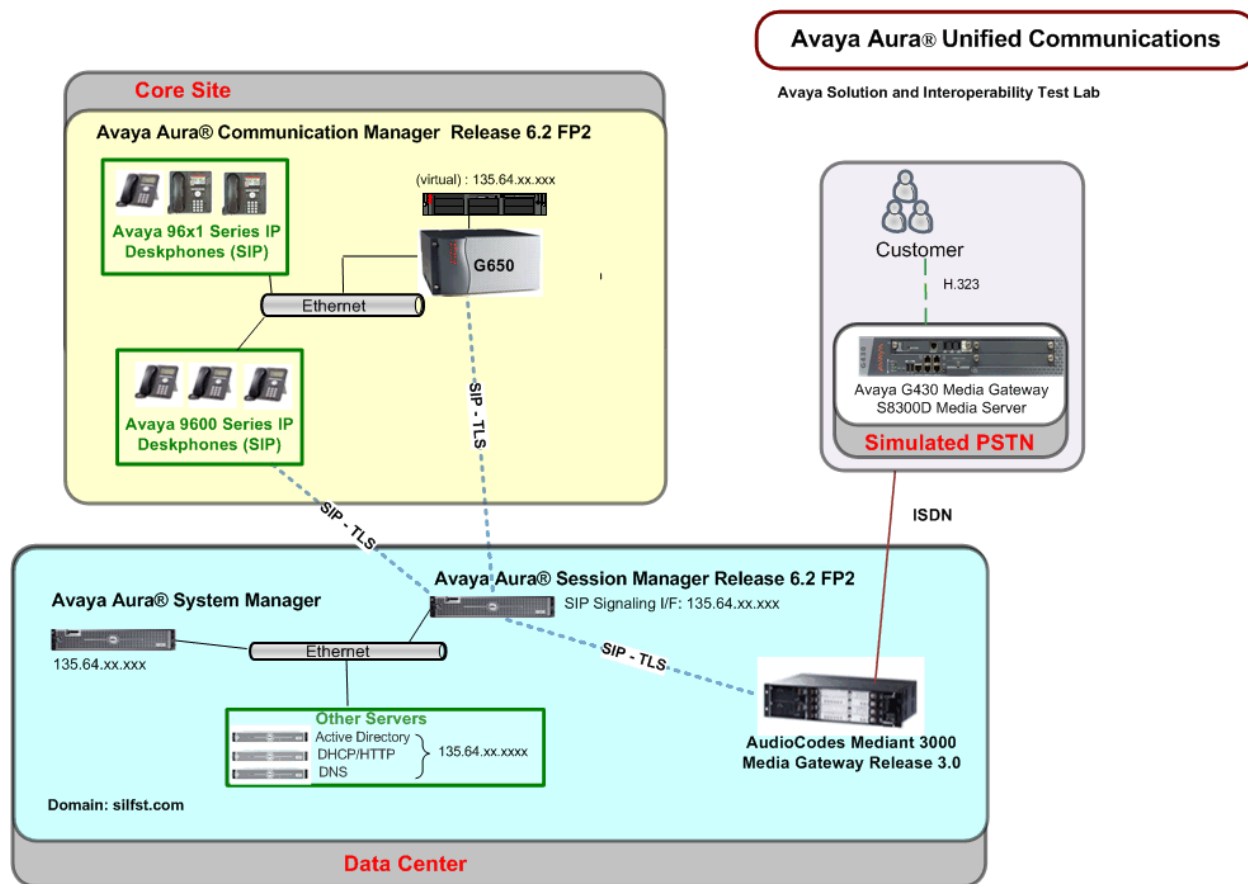


Figure 1: Network Topology used in Sample Configuration

Note: IP addresses have been partially hidden in **Figure 1** for security.

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration.

Component	Software Version
AudioCodes Mediant 3000 Media Gateway	R3.0 Firmware Version 6.60A.026.001
Avaya Aura [®] System Manager Avaya S8800 Media Server	Release 6.2, FP2 Version 6.3.2.4.1339
Avaya Aura [®] Session Manager Avaya S8800 Media Server	Release 6.2, FP2 Build 6.3.2.0.632023
Avaya Aura [®] Communication Manager Evolution Server • Duplicated Avaya S8800 Servers • Avaya G650 Media Gateway	Release 6.2, FP2 Version: R016.x.03.0.124.0-20553
Avaya 9600 Series IP Deskphones (with Avaya one-X [®] SIP firmware)	Release 2.6.10.1 Version 2-6-10-132005
Avaya 96x1 Series IP Deskphone (with Avaya one-X [®] SIP firmware)	Release 6.2.2.25 Build: 96x1_IPT-SIP-R6_2_2-060613

5. Configure Avaya Aura® Communication Manager

This section describes the steps needed to configure Communications Manager to use Secure Real-time Transport Protocol (SRTP) for media and to configure the SIP trunk using TLS between Communication Manager Evolution Server and Session Manager to support registration of SIP endpoints. These instructions assume the Avaya G650 Media Server is already configured on Communication Manager. For information on how to administer these other aspects of Communication Manager, see **References [6] through [10]** in **Section 10**.

This section describes the administration of Communication Manager using a System Access Terminal (SAT). Some administration screens have been abbreviated for clarity.

The following administration steps will be described:

- Verify System Capacities and Licensing
- Configure Trunk-to-Trunk Transfers
- Configure IP Codec Set
- Configure IP Network Region
- Configure IP Node Names and IP Addresses
- Configure SIP Signaling Group and Trunk Group
- Configure Route Pattern
- Administer Private Numbering Plan and Uniform Dialplan
- Administer AAR Analysis
- Verify Off-PBX-Telephone Station Mapping

After completing these steps, the **save translation** command should be performed.

5.1. Verify System Capacities and Licensing

This section describes the procedures to verify the correct system capacities and licensing have been configured. If there is insufficient capacity or a required features is not available, contact an authorized Avaya sales representative to make the appropriate changes.

5.1.1. Verify Off-PBX Telephones Capacity

On **Page 1** of the **system-parameters customer-options** command, verify an adequate number of Off-PBX Stations (OPS) Telephones are administered for the system as shown below.

```
display system-parameters customer-options                               Page 1 of 11
                                OPTIONAL FEATURES
G3 Version: V16                                     Software Package: Enterprise
  Location: 2                                       System ID (SID): 1
                                                USED
...
Maximum Off-PBX Telephones - EC500: 41000 0
Maximum Off-PBX Telephones - OPS: 41000 32
Maximum Off-PBX Telephones - PBFMC: 41000 0
...
```

5.1.2. Verify SIP Trunk Capacity

On **Page 2** of the **system-parameters customer-options** command, verify an adequate number of SIP Trunk Members are administered for the system as shown below.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks: 12000		0	
Maximum Concurrently Registered IP Stations: 18000		0	
Max Concur Registered Unauthenticated H.323 Stations: 414		0	
...			
Maximum Video Capable IP Softphones: 0		0	
Maximum Administered SIP Trunks: 24000		90	
...			

5.1.3. Verify AAR/ARS Routing is Enabled

To simplify the dialing plan for calls between SIP endpoints, verify the following AAR/ARS features are enabled on the system.

On **Page 3** of **system-parameters customer-options** command, verify the following features are enabled.

- **ARS?** Verify “y” is displayed.
- **ARS/AAR Partitioning?** Verify “y” is displayed.
- **ARS/AAR Dialing without FAC?** Verify “y” is displayed.

display system-parameters customer-options		Page	3 of 11
OPTIONAL FEATURES			
A/D Grp/Sys List Dialing Start at 01? n		CAS Main? n	
Answer Supervision by Call Classifier? n		Change COR by FAC? n	
ARS? y		Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y		Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? y		DCS (Basic)? y	
ASAI Link Core Capabilities? y		DCS Call Coverage? n	
...			

5.1.4. Verify Media Encryption is Supported

On **Page 4** of **system-parameters customer-options** command, verify the **Media Encryption Over IP** feature is set to “y”.

```
display system-parameters customer-options                               Page 4 of 11
                                OPTIONAL FEATURES
...
Enterprise Survivable Server? n                                         ISDN-BRI Trunks? y
Enterprise Wide Licensing? n                                           ISDN-PRI? y
ESS Administration? y                                                  Local Survivable Processor? n
Extended Cvg/Fwd Admin? y                                             Malicious Call Trace? y
External Device Alarm Admin? y                                         Media Encryption Over IP? y
...
```

5.1.5. Verify Private Networking is Enabled

On **Page 5** of **system-parameters customer-options** command, verify the **Private Networking** feature is set to “y”.

```
display system-parameters customer-options                               Page 5 of 11
                                OPTIONAL FEATURES
Port Network Support? y                                               Time of Day Routing? n
Posted Messages? n                                                   TN2501 VAL Maximum Capacity? y
                                                                    Uniform Dialing Plan? y
Private Networking? y                                             Usage Allocation Enhancements? y
Processor and System MSP? y
Processor Ethernet? y                                                Wideband Switching? n
```

5.1.6. Verify AAR Access Code

To enable Communication Manager to route calls to SIP endpoints, verify an Automatic Alternative Routing (AAR) access code has been defined for the system.

On **Page 1** of **feature-access-codes** command, verify a value has been defined in the **Auto Alternate Routing (AAR) Access Code** field. In the sample configuration, “8” was used.

```
change feature-access-codes                                             Page 1 of 10
                                FEATURE ACCESS CODE (FAC)
...
Attendant Access Code:
Auto Alternate Routing (AAR) Access Code: 8
Auto Route Selection (ARS) - Access Code 1: 9                       Access Code 2:
Automatic Callback Activation: *08                                   Deactivation: *09
...
```

5.1.7. Verify Initial INVITE with SDP for Secure Calls is Enabled

On **Page 19** of **system-parameters features** command, verify the **Initial INVITE with SDP for secure calls** feature is set to “y”.

```
display system-parameters features                                     Page 19 of 20
                                FEATURE-RELATED SYSTEM PARAMETERS
IP PARAMETERS
    Direct IP-IP Audio Connections? y
    IP Audio Hairpinning? n
    Synchronization over IP? n
    Initial INVITE with SDP for secure calls? y
    SIP Endpoint Managed Transfer? n
...
```

5.2. Configure Trunk-to-Trunk Transfers

Use the **change system-parameters features** command to enable trunk-to-trunk transfers. This feature is needed when an incoming call to a SIP station is transferred to another SIP station. For simplicity, the **Trunk-to-Trunk Transfer** field on **Page 1** was set to “all” to enable all trunk-to-trunk transfers on a system wide basis.

Note: Enabling this feature poses significant security risk by increasing the risk of toll fraud, and must be used with caution. To minimize the risk, a COS could be defined to allow trunk-to-trunk transfers for specific trunk group(s). For more information regarding how to configure Communication Manager to minimize toll fraud, see **Reference [10]** in **Section 10**.

```
change system-parameters features                                     Page 1 of 20
                                FEATURE-RELATED SYSTEM PARAMETERS
    Self Station Display Enabled? n
    Trunk-to-Trunk Transfer: all
    Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
...
```

5.3. Configure IP Codec Set

Use the **change ip-codec-set n** command where **n** is the number used to identify the codec set.

Enter the following values:

- **Audio Codec** Enter “**G.711MU**” and “**G.729**” as supported types.
- **Silence Suppression** Retain the default value “**n**”.
- **Frames Per Pkt** Enter “**2**”.
- **Packet Size (ms)** Enter “**20**”.
- **Media Encryption** Enter “**1-srtp-aescm128-hmac80**” on first line.

```
change ip-codec-set 3                                     Page 1 of 2
                                     IP Codec Set
Codec Set: 3

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size (ms)
1: G.711MU          n           2          20
2: G.729           n           2          20
3:

Media Encryption
1: 1-srtp-aescm128-hmac80
2:
...
```

5.4. Configure IP Network Region

Use the **change ip-network-region n** command where **n** is an available network region.

Enter the following values and use default values for remaining fields.

- **Authoritative Domain:** Enter the correct SIP domain for the configuration.
For the sample configuration, “**silstack.com**” was used.
- **Name:** Enter descriptive name.
- **Codec Set:** Enter the number of the IP codec set configured in **Section 5.3**.
- **Intra-region IP-IP Direct Audio:** Enter “**yes**”.
- **Inter-region IP-IP Direct Audio:** Enter “**yes**”.

```
change ip-network-region 1                               Page 1 of 20
                                     IP NETWORK REGION
Region: 1
Location: 1      Authoritative Domain: silstack.com
Name: SIP calls for ASM
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 3          Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048    IP Audio Hairpinning? n
UDP Port Max: 16585
```

On **Page 3**, verify **Allow SIP URI Conversion** field is set to “**n**”.

Note: When this field is set to “**n**”, calls from SIP endpoints supporting SRTP to other endpoints that do not support SRTP will not be allowed.

change ip-network-region 1		Page 3 of 20
IP NETWORK REGION		
INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY		
Incoming LDN Extension:		
Conversion To Full Public Number - Delete:		Insert:
Maximum Number of Trunks to Use for IGAR:		
Dial Plan Transparency in Survivable Mode? n		
BACKUP SERVERS (IN PRIORITY ORDER)		H.323 SECURITY PROFILES
1		1 challenge
2		2
3		3
4		4
5		
6		Allow SIP URI Conversion? n
...		

5.5. Add Node Names and IP Addresses

Use the **change node-names ip** command to add the node-name and IP Addresses for the “**procr**” interface on Communication Manager and the SIP signaling interface of Session Manager, if not previously added.

In the sample configuration, the node-name of the SIP signaling interface for Session Manager is “**ASM1**” with an IP address of “**135.64.xx.xxx**”.

Note: IP addresses have been partially hidden for security.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
ASM1	135.64.xxx.xx	
ASM2	135.64.xxx.xx	
ASM3	135.9.xxx.xx	
S8300	135.64.xxx.xx	
...		
default	0.0.0.0	
procr	135.64.xx.xxx	
...		

5.6. Configure SIP Signaling Group

Use the **add signaling-group n** command, where **n** is an available signaling group number to create SIP signaling group. In the sample configuration, trunk group “2” and signaling group “2” were used for connecting to Session Manager.

On **Page 1**, enter the following values and use default values for remaining fields.

- **Group Type:** Enter “**sip**”.
- **IMS Enabled?** Enter “**n**”.
- **Transport Method:** Enter “**tls**”.
- **Peer Detection Enabled?** Enter “**y**”.
- **Peer Server:** Use default value.
Note: default value is replaced with “**SM**” after SIP trunk to Session Manager is established.
- **Enforce SIPS URI for SRTP?** Enter “**y**”.
- **Near-end Node Name:** Enter “**procr**” node name from **Section 5.5**.
- **Far-end Node Name:** Enter node name for Session Manager defined in **Section 5.5**.
- **Near-end Listen Port:** Verify “**5061**” is used.
- **Far-end Listen Port:** Verify “**5061**” is used.
- **Far-end Network Region:** Enter network region defined in **Section 5.4**.
- **Far-end Domain:** Leave blank.

add signaling-group 2		Page 1 of 2
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? y	Priority Video? y	Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr		Far-end Node Name: ASM1
Near-end Listen Port: 5061		Far-end Listen Port: 5061
		Far-end Network Region: 1
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate		Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload		RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3		Direct IP-IP Audio Connections? y
Enable Layer 3 Test? y		IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n		Initial IP-IP Direct Media? n
		Alternate Route Timer(sec): 6

5.7. Add SIP Trunk Group

Add the corresponding trunk group controlled by the signaling group defined **Section 5.6** using the **add trunk-group n** command where **n** is an available trunk group number.

Fill in the indicated fields as shown below. Default values can be used for the remaining fields.

- **Group Type:** Enter “**sip**”.
- **Group Name:** Enter a descriptive name.
- **TAC:** Enter an available trunk access code.
- **Direction:** Enter “**two-way**”.
- **Outgoing Display?** Enter “**y**”.
- **Service Type:** Enter “**tie**”.
- **Signaling Group:** Enter the number of the signaling group from **Section 5.6**.
- **Number of Members:** Enter the number of members in the SIP trunk (must be within limits configured in **Section 5.1.2**).

Note: once the **add trunk-group** command is completed, trunk members will be automatically generated based on the value in the **Number of Members** field.

add trunk-group 2		Page 1 of 22
TRUNK GROUP		
Group Number: 2	Group Type: sip	CDR Reports: y
Group Name: SIP Trunk to ASM1	COR: 1	TN: 1
TAC: *02	Direction: two-way	Outgoing Display? y
Dial Access? n		Night Service:
Queue Length: 0		
Service Type: tie	Auth Code? N	
	Member Assignment Method: auto	
	Signaling Group: 2	
	Number of Members: 50	

On **Page 3**, fill in the indicated fields as shown below. Default values can be used for the remaining fields.

- **Numbering Format:** Enter “**private**”.
- **Show ANSWERED BY on Display?** Enter “**y**”.

add trunk-group 2		Page 3 of 22
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: private		
	UI Treatment: service-provider	
	Replace Restricted Numbers? n	
	Replace Unavailable Numbers? n	
Show ANSWERED BY on Display? y		

On **Page 5**, verify **Support Request History?** is set to “y”. Use Default values for remaining fields.

```

add trunk-group 2                                     Page 5 of 21
                                                    PROTOCOL VARIATIONS

                Mark Users as Phone? y
            Prepend '+' to Calling Number? n
        Send Transferring Party Information? n
            Network Call Redirection? n
                Send Diversion Header? n
            Support Request History? y
        Telephone Event Payload Type: 120
  
```

5.8. Configure Route Pattern

This section provides the configuration of the route pattern used in the sample configuration for routing calls between SIP endpoints and PSTN users.

Use **change route-pattern n** command where **n** is an available route pattern.

Fill in the indicated fields as shown below and use default values for remaining fields.

- **Pattern Name** Enter descriptive name.
- **Secure SIP?** Verify “n” is displayed.
Note: this parameter should never be enabled for SIP trunk to Session Manager.
- **Grp No** Enter number of trunk group defined in **Section 5.7**
- **FRL** Enter “0”.
- **Numbering Format** Enter “lev0-pvt”.

In the sample configuration, route pattern “2” was created as shown below.

```

change route-pattern 2                               Page 1 of 3
                Pattern Number: 2  Pattern Name: ASM1 SIP Trunk
                SCCAN? n          Secure SIP? n

Grp FRL NPA Pfx Hop Toll No.  Inserted          DCS/ IXC
No           Mrk Lmt List Del  Digits          QSIG
                Dgts                      Intw
1: 2      0
2:
3:
...
    BCC VALUE  TSC CA-TSC      ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W      Request          Dgts Format
                                Subaddress
1: y y y y y n  n          rest          lev0-pvt  none
2: y y y y y n  n          rest          none
3: y y y y y n  n          rest          none
...
  
```

5.9. Administer Private Numbering Plan

Extension numbers used for SIP Users registered to Session Manager must be added to either the private or public numbering table on Communication Manager. For the sample configuration, private numbering was used and all extension numbers were unique within the private network. However, in many customer networks, it may not be possible to define unique extension numbers for all users within the private network. For these types of networks, additional administration may be required as described in **Reference [7]** in **Section 10**.

Use the **change private-numbering n** command, where **n** is the length of the private number.

Fill in the indicated fields as shown below.

- **Ext Len:** Enter length of extension numbers.
In the sample configuration, 5 digit extension numbers were used.
- **Ext Code:** Enter leading digit (s) from extension number.
In the sample configuration, “12xxx” and “31xxx” were used.
- **Trk Grp(s):** Leave field blank.
- **Private Prefix:** Leave field blank unless an enterprise canonical numbering scheme is defined in Session Manager.
If so, enter the appropriate prefix.
- **Total Length:** Enter “5” since a private prefix was not defined.

change private-numbering 5					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	12			5	Total Administered: 7
5	31				5
Maximum Entries: 540					
...					

5.10. Administer Uniform Dial Plan

Use the **change uniform-dialplan n** command, where **n** is the first digit of the extension numbers used for SIP stations in the system.

In the sample configuration, 5-digit extension numbers starting with “**12xxx**” and “**31xxx**” were used for extensions associated with SIP stations.

Fill in the indicated fields as shown below and use default values for remaining fields.

- **Matching Pattern** Enter digit pattern of extensions assigned to SIP endpoints.
- **Len** Enter extension length.
- **Net** Enter “**aar**”.

change uniform-dialplan 2						Page	1 of	2
UNIFORM DIAL PLAN TABLE								
						Percent Full:	0	
Matching			Insert		Node			
Pattern	Len	Del	Digits	Net	Conv	Num		
12	5	0		aar	n			
31	5	0		aar	n			

5.11. Administer AAR Analysis

This section provides the configuration of the AAR pattern used in the sample configuration for routing calls between SIP endpoints and other stations. In the sample configuration, extension numbers starting with digits “**12xxx**” and “**31xxx**” were used.

Note: Other methods of routing may be used.

Use the **change aar analysis n** command where **n** is the first digit of the extension numbers.

Fill in the indicated fields as shown below and use default values for remaining fields.

- **Dialed String** Enter leading digit (s) of extension numbers.
- **Min** Enter minimum number of digits that must be dialed.
- **Max** Enter maximum number of digits that may be dialed.
- **Route Pattern** Enter Route Pattern defined in **Section 5.8**.
- **Call Type** Enter “**unku**”.

change aar analysis 1							Page
1 of 2							
AAR DIGIT ANALYSIS TABLE							
Location: all				Percent Full:		1	
	Dialed	Total	Route	Call	Node	ANI	
	String	Min Max	Pattern	Type	Num	Reqd	
12		5 5	2	unku		n	
31		5 5	2	unku		n	

5.12. Configure Stations

These instructions assume SIP users have been defined using System Manager and the administrator selected the option is to automatically generate a SIP station when adding a new SIP user. For information on how to add SIP users, see **References [17] and [18] in Section 10.**

5.13. Verify Off-PBX-Telephone Station-Mapping

Use the **change off-pbx-telephone station-mapping xxx** command where **xxx** is an extension assigned to SIP endpoints to verify an Off-PBX station mapping was automatically created for the SIP station.

On **Page 1**, verify the following fields were correctly populated.

- **Application** Verify “**OPS**” is assigned.
- **Trunk Selection** Verify “**aar**” is assigned.

change off-pbx-telephone station-mapping 12004							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
12004	OPS	—		21001	aar	1	
		—					
		—					

On **Page 2**, verify the following fields were correctly populated.

- **Call Limit:** Verify “**3**” is assigned.
- **Mapping Mode:** Verify “**both**” is assigned.
- **Calls Allowed:** Verify “**all**” is assigned.

change off-pbx-telephone station-mapping 12004							Page 2 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Appl Name	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	Location	
12004	OPS	3	both	all	none		
			—				

5.14. Save Translations

Configuration of Communication Manager Evolution Server is complete. Use the **save translation** command to save these changes.

Note: After making a change on Communication Manager which alters the numbering plan, synchronization between Communication Manager and System Manager must be completed. See **References [17] in Section 10** for more information.

6. Configure Avaya Aura® Session Manager

This section describes the procedures for configuring Avaya Aura® Session Manager to support SIP connectivity to Communication Manager and AudioCodes Mediant 3000 Media Gateway using TLS.

These instructions assume other administration activities have already been completed such as defining SIP entity for Session Manager, defining the network connection between System Manager and Session Manager, defining Communication Manager as a Managed Element and adding SIP users. For more information on these additional actions, see **References [2], [5] and [18] in Section 10.**

The following administration activities will be described:

- Define SIP Domain and Locations
- Define SIP Entities for Communication Manager and AudioCodes Mediant 3000 Media Gateway
- Define Entity Links, which describe the SIP trunk parameters used by Session Manager when routing calls between SIP Entities
- Define Routing Policy and Dial Plan to route outgoing calls to PSTN users via AudioCodes Mediant 3000 Media Gateway.

Note: Some administration screens have been abbreviated for clarity.

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager, using the URL “**http://<ip-address>/SMGR**”, where “**<ip-address>**” is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials.

6.1. Define SIP Domains

Expand **Elements** → **Routing** and select **Domains** from the left navigation menu.

Click **New**. Enter the following values and use default values for remaining fields.

- **Name** Enter the Authoritative Domain Name specified in **Section 5.4**.
For the sample configuration, “**silstack.com**” was used.
- **Type** Select “**sip**” from drop-down menu.
- **Notes** Add a brief description. [Optional].

Click **Commit** (not shown) to save.

The screen below shows the SIP Domain defined for the sample configuration.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top header includes the Avaya logo, the product name "Avaya Aura® System Manager 6.3", and user information: "Last Logged on at March 25, 2013 9:07 AM" and "Help | About | Change Password | Log off admin". The navigation menu on the left shows "Routing" expanded, with "Domains" highlighted. The main content area is titled "Domain Management" and shows a table with one domain: "silstack.com" of type "sip". The table has columns for "Name", "Type", and "Notes". A red box highlights the "Domains" menu item and the table row. Another red box highlights the "New" button. The table also includes a "Filter: Enable" link and a "Select : All, None" option.

	Name	Type	Notes
☐	silstack.com	sip	

6.2. Define Locations

Locations are used to identify logical and/or physical locations where SIP Entities or SIP endpoints reside, for purposes of bandwidth management or location-based routing.

Expand **Elements** → **Routing** and select **Locations** from the left navigation menu.

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name such as “**Galway**”.
- **Notes:** Add a brief description. [Optional].

Scroll down to the **Location Pattern** section and click **Add**. Enter the following values.

- **IP Address Pattern** Enter the logical pattern used to identify the location.
For the sample configuration, “**135.64.xxx.***” was used.
- **Notes** Add a brief description. [Optional]

Click **Commit** to save.

The screen below shows a Location used in the sample configuration.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura® System Manager 6.3', and a user status bar indicating 'Last Logged on at March 25, 2013 9:07 AM' with links for 'Help | About | Change Password | Log off admin'. The left sidebar shows a navigation tree with 'Routing' expanded and 'Locations' selected. The main content area is titled 'Home / Elements / Routing / Locations' and contains a 'Location Details' section with a 'General' tab. In this tab, the 'Name' field is set to 'Galway' and the 'Notes' field is empty. Below this is the 'Location Pattern' section, which includes an 'Add' button and a table with one item. The table has columns for 'IP Address Pattern' and 'Notes'. The 'IP Address Pattern' field contains '135.64.██.*' and the 'Notes' field contains 'AACC IP Pattern'. At the bottom of the interface, there are 'Commit' and 'Cancel' buttons.

Avaya Avaya Aura® System Manager 6.3 Last Logged on at March 25, 2013 9:07 AM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Locations Help ?

Location Details

Commit Cancel

General

* Name: Galway

Notes:

Location Pattern

Add Remove

1 Item Refresh Filter: Enable

IP Address Pattern	Notes
* 135.64.██.*	AACC IP Pattern

Select : All, None

Commit Cancel

Note: IP address has been partially hidden for security.

6.3. Define SIP Entities

Step 1: Define a SIP Entity for Communication Manager.

To add a SIP Entity, expand **Elements** → **Routing** and select **SIP Entities** from the left menu.

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter an identifier for new SIP Entity.
In the sample configuration, “**CM-Main**” was used.
- **FQDN or IP Address:** Enter IP address of “**procr**” interface defined in **Section 5.5**
- **Type:** Select “**CM**” for Communication Manager.
- **Notes:** Enter a brief description. [Optional].
- **Location:** Select Location defined in **Section 6.2**.
- **Time Zone:** Select previously defined Time Zone.

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select “**Use Session Manager Configuration**”.

Click **Commit** to save SIP Entity definition.

The following screen shows the SIP Entity defined for Communication Manager.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.3', and a user status bar indicating 'Last Logged on at March 25, 2013 9:07 AM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left sidebar shows a tree view with 'Routing' expanded and 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains two sections: 'General' and 'SIP Link Monitoring'. The 'General' section includes fields for 'Name' (CM-Main), 'FQDN or IP Address' (135.64. [redacted]), 'Type' (CM), 'Notes' (empty), 'Adaptation' (dropdown), 'Location' (Galway), and 'Time Zone' (Europe/Dublin). Below these are checkboxes for 'Override Port & Transport with DNS SRV' and 'SIP Timer B/F (in seconds)' (4), a 'Credential name' field, and a 'Call Detail Recording' dropdown (none). The 'SIP Link Monitoring' section has a dropdown for 'SIP Link Monitoring' set to 'Use Session Manager Configuration'. A red box highlights the 'General' section fields, and another red box highlights the 'SIP Link Monitoring' dropdown.

Note: IP address of the “**procr**” interface has been partially hidden for security.

Step 2: Configure a SIP Entity for AudioCodes Mediant 3000 Media Gateway.

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter an identifier for new SIP Entity.
In the sample configuration, “**AudioCodes M3K**” was used.
- **FQDN or IP Address:** Enter IP address of AudioCodes M3K Media Gateway.
- **Type:** Select “**Gateway**”.
- **Notes:** Enter a brief description. [Optional].
- **Location:** Select Location defined in **Section 6.2**.
- **Time Zone:** Select previously defined Time Zone.

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select “**Use Session Manager Configuration**”.

Click **Commit** to save SIP Entity definition.

The following screen shows the SIP Entity defined for AudioCodes M3K Media Gateway.

The screenshot displays the 'SIP Entity Details' configuration page. The left sidebar shows a navigation menu with 'SIP Entities' highlighted. The main content area has a breadcrumb trail 'Home / Elements / Routing / SIP Entities' and buttons for 'Commit' and 'Cancel'. The 'General' section is active, showing fields for Name (Audiocodes M3K), FQDN or IP Address (135.64...), Type (Gateway), Notes (Audiocodes M3K Gateway), Adaptation, Location (Galway), and Time Zone (Europe/Dublin). Below this is the 'Override Port & Transport with DNS SRV' checkbox and 'SIP Timer B/F (in seconds): 4'. The 'Credential name' and 'Call Detail Recording' (none) fields are also present. The 'Loop Detection' section shows 'Loop Detection Mode' set to 'Off'. The 'SIP Link Monitoring' section at the bottom shows 'SIP Link Monitoring' set to 'Use Session Manager Configuration'.

Routing

- Domains
- Locations
- Adaptations
- SIP Entities**
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: Audiocodes M3K

* FQDN or IP Address: 135.64...

Type: Gateway

Notes: Audiocodes M3K Gateway

Adaptation:

Location: Galway

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Note: IP address has been partially hidden for security.

6.4. Define Entity Links

A SIP trunk between Session Manager and each telephony system is described by an Entity Link.

Step 1: To add an Entity Link, expand **Elements** → **Routing** and select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values.

- **Name** Enter an identifier for the link to Communication Manager.
- **SIP Entity 1** Select entity for Session Manager previously defined.
- **SIP Entity 2** Select the SIP Entity added for Communication Manager defined in **Section 6.3** from drop-down menu.
- **Protocol** After selecting both SIP Entities, verify “**TLS**” is selected as the required Protocol.
- **Port** Verify **Port** for both SIP entities is “**5061**”.
- **Connection Policy** Select “**trusted**”.
- **Notes:** Enter a brief description. [Optional].

Click **Commit** to save Entity Link definition.

The following screen shows the Entity Link defined in the sample configuration for the SIP trunk between Communication Manager Evolution Server and Session Manager.

Avaya Aura® System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Refresh Filter:

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
☐	* ASM1_CM-Main	* ASM1	TLS	* 5061	* CM-Main	* 5061	trusted	☐	

Select : All, None

Step 2: Define Entity Link between Session Manager and AudioCodes M3K Media Gateway.

Click **New** (not shown). Enter the following values.

- **Name** Enter an identifier for the link to AudioCodes M3K Media Gateway.
- **SIP Entity 1** Select entity for Session Manager previously defined.
- **SIP Entity 2** Select the SIP Entity added for M3K Media Gateway defined in **Section 6.3** from drop-down menu.
- **Protocol** After selecting both SIP Entities, verify “**TLS**” is selected as the required Protocol.
- **Port** Verify **Port** for both SIP entities is “**5061**”.
- **Connection Policy** Select “**trusted**”.
- **Notes:** Enter a brief description. [Optional].

Click **Commit** to save Entity Link definition.

The following screen shows the Entity Link defined in the sample configuration for the SIP trunk between Session Manager and AudioCodes M3K Media Gateway.

Avaya Aura® System Manager 6.3

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Refresh Filter: Enable

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
☐	*ASM1_Audiocodes M	*ASM1	TLS	*5061	*Audiocodes M3K	*5061	trusted	☐	

Select: All, None

6.5. Define Routing Policy for SIP Users

Since the SIP users are registered to Session Manager, a routing policy does not need to be defined for calls to SIP endpoints supported by Communication Manager Evolution Server.

For more information on defining a routing policy to route calls to non-SIP stations on Communication Manager Evolution Server, see **References [7] and [17] in Section 10.**

6.6. Define Routing Policies for AudioCodes Mediant 3000 Gateway

To route calls to PSTN users, configure a routing policy for AudioCodes M3K Media Gateway.

To define a routing policy, expand **Elements** → **Routing** and select **Routing Policies**.

Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier to define the routing policy
- **Disabled:** Leave unchecked.
- **Notes:** Enter a brief description. [Optional]

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown).

- Select the SIP Entity associated with AudioCodes M3K Media Gateway defined in **Section 6.3** and click **Select**.
- The selected SIP Entity displays on the **Routing Policy Details** page.

Use default values for remaining fields. Click **Commit** to save Routing Policy definition.

Note: The routing policy defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks.

The following screen shows the Routing Policy for routing calls to PSTN users.

AVAYA Avaya Aura® System Manager 6.3

Last Logged on at July 22, 201
[Help](#) | [About](#) | [Change Password](#) | [Log](#)

Routing x

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

* Name: ASM-Audiocode M3K

Disabled: ☐

* Retries: 0

Notes: Routing to PSTN via M3K

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Audiocodes M3K	135.64. [redacted]	Gateway	Audiocodes M3K Gateway

Note: IP address has been hidden for security.

6.7. Define Dial Patterns

Define the Dial Pattern(s) corresponding to PSTN destinations. In the sample configuration, stations associated with PSTN users were assigned 5-digit numbers starting with “110”.

To define a dial pattern, expand **Elements** → **Routing** and select **Dial Patterns** (not shown).

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern
- **Min:** Enter the minimum number of digits that must be dialed.
- **Max:** Enter the maximum number of digits that may be dialed.
- **SIP Domain:** Select SIP Domain defined in **Section 6.1**.
- **Notes:** Enter a brief description. [Optional].

In the **Originating Locations and Routing Policies** section, click **Add**.

The **Originating Locations and Routing Policy List** page opens (not shown).

- In **Originating Locations** table, select Location defined in **Section 6.2**.
- In **Routing Policies** table, select the Routing Policy defined in **Section 6.6** for AudioCodes M3K Media Gateway.
- Click **Select** to save these changes and return to **Dial Pattern Details** page.

Click **Commit** to save. The following screen shows Dial Pattern defined for calls to PSTN users in sample configuration.

The screenshot displays the 'Dial Pattern Details' configuration page. The left sidebar shows the navigation menu with 'Dial Patterns' selected. The main content area is divided into two sections. The 'General' section, highlighted with a red box, contains the following fields: 'Pattern' (110), 'Min' (5), 'Max' (7), 'Emergency Call' (unchecked), 'Emergency Priority' (1), 'Emergency Type' (empty), 'SIP Domain' (silstack.com), and 'Notes' (PSTN phones). The 'Originating Locations and Routing Policies' section, also highlighted with a red box, includes an 'Add' button and a table with 3 items. The table has columns: 'Originating Location Name', 'Originating Location Notes', 'Routing Policy Name', 'Rank', 'Routing Policy Disabled', 'Routing Policy Destination', and 'Routing Policy Notes'. The first item in the table is 'Galway', with 'Originating Location Notes' as 'ASM-Audiocode M3K', 'Rank' as '0', 'Routing Policy Disabled' as unchecked, 'Routing Policy Destination' as 'Audiocodes M3K', and 'Routing Policy Notes' as 'Routing to PSTN via M3K'.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐ Galway	ASM-Audiocode M3K		0	☐	Audiocodes M3K	Routing to PSTN via M3K

Repeat this step as necessary to define Dial Patterns for other PSTN destinations.

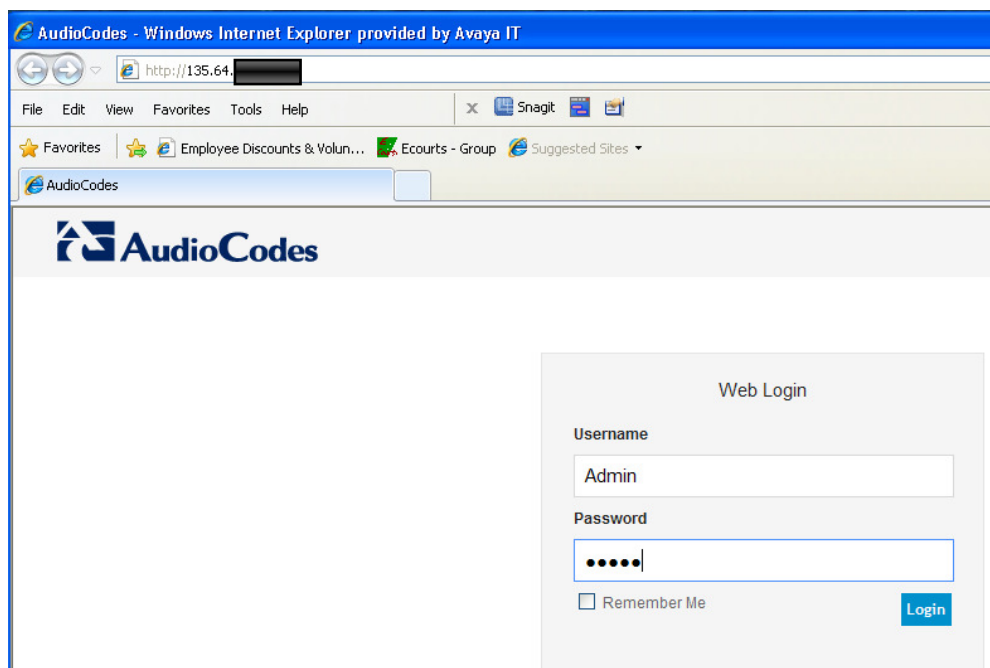
7. Configure AudioCodes Mediant 3000 Media Gateway

This section provides the procedures for configuring AudioCodes Mediant 3000 Media Gateway using the web based graphical user interface. The procedures include the following areas:

- Select all configurable parameters
- Configure General Security Settings
- Configure SIP Protocols and Ports
- Configure Codec Preferences
- Configure Trunk Group
- Configure Tel-to-IP routing
- Configure Trunk Group Routing
- Generate TLS Certificate and upload to Session Manager
- Upload Root Certificate from System Manager to AudioCodes M3K Media Gateway
- Configure Media Settings

These Application Notes assume the AudioCodes Mediant 3000 Gateway is already installed and is functioning properly and PSTN Connectivity to the Mediant 3000 Gateway has been established and is operational. See the documentation listed in **Section 10** for more information.

Configuration is accomplished by accessing the browser-based GUI of AudioCodes M3K Gateway, using the URL “<http://<ip-address>/>”, where “<ip-address>” is the IP address of AudioCodes M3K Gateway server. Log in with the appropriate credentials.



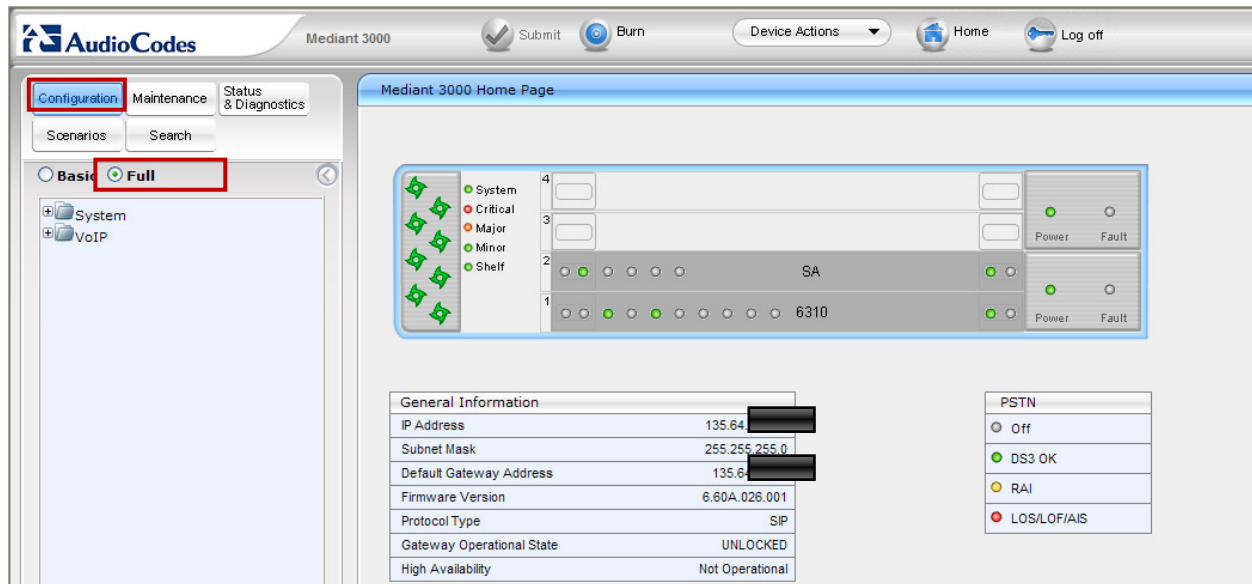
Note: IP address has been partially hidden for security.

7.1. Select Configurable Parameters

The **Mediant 3000 Home Page** will be displayed. Select **Configuration** tab in left pane.

Verify all configurable parameters are displayed by selecting **Full** in the left pane.

In the screenshot below, both TP6310 and SA boards are shown.



Note: IP addresses have been hidden for security.

7.2. Configure General Security Settings

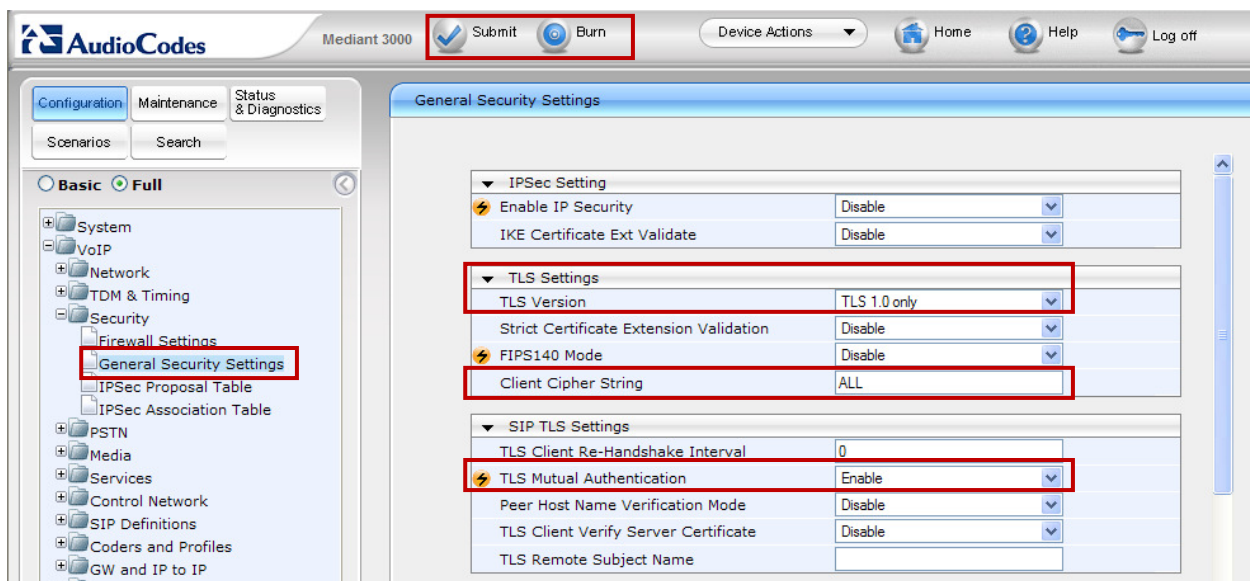
Step 1: On **Configuration** tab, expand **VoIP** → **Security** → **General Security Settings**.

Under **TLS Settings** section, enter the following values and use default values for remaining fields.

- **TLS Version** Select “**TLS 1.0 only**”.
- **Client Cipher String** Enter “**ALL**”.

Under **SIP TLS Settings** section, enter the following values and use default values for remaining fields.

- **TLS Mutual Authentication** Select “**Enable**”.



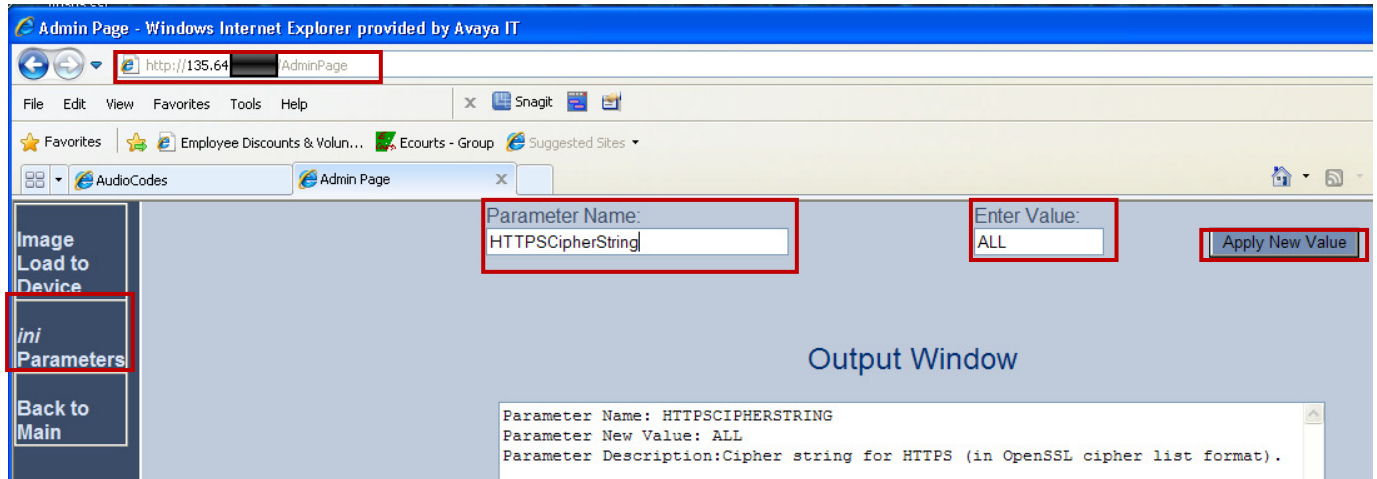
Click **Submit** and then **Burn** to save the changes.

7.3. Configure HTTPS Security Settings

To edit HTTPS settings, open **Admin Page** using URL “<http://<ip-address>/AdminPage>”, where “<ip-address>” is the IP address of AudioCodes M3K Gateway server.

Click **ini Parameters** link on left side and enter following values.

- **Parameter Name** Enter “**HTTPSCipherString**”.
- **Enter Value** Enter “**ALL**”.



Click **Apply New Value** to save the changes.

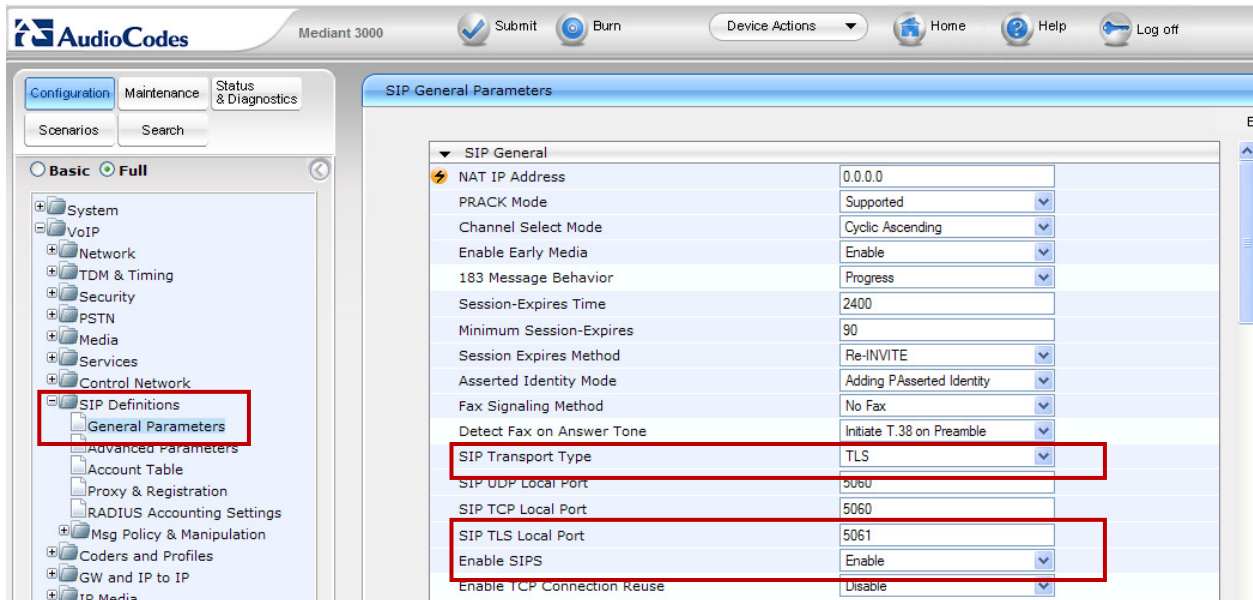
Note: Value entered in **Parameter Name** field will be replaced with all capital letters after changes are saved as shown in **Output Window**.

7.4. Configure SIP Protocols and Ports

On Configuration tab, expand VoIP → SIP Definitions → General Parameters.

Enter the following values and use default values for remaining fields.

- **SIP Transport Type** Select “**TLS**”.
- **SIP TLS Local Port** Enter “**5061**”.
- **Enable SIPS** Select “**Enabled**”.



SIP General	
NAT IP Address	0.0.0.0
PRACK Mode	Supported
Channel Select Mode	Cyclic Ascending
Enable Early Media	Enable
183 Message Behavior	Progress
Session-Expires Time	2400
Minimum Session-Expires	90
Session Expires Method	Re-INVITE
Asserted Identity Mode	Adding PAsserted Identity
Fax Signaling Method	No Fax
Detect Fax on Answer Tone	Initiate T.38 on Preamble
SIP Transport Type	TLS
SIP UDP Local Port	5060
SIP TCP Local Port	5060
SIP TLS Local Port	5061
Enable SIPS	Enable
Enable TCP Connection Reuse	Disable

Scroll down further and enter the following values.

- **SIP Destination Port** Enter “**5061**”.
- **Use user=phone in SIP URL** Select “**Yes**”.

The screenshot shows the AudioCodes Mediant 3000 configuration interface. The left sidebar shows a tree view with 'SIP Definitions' expanded, and 'General Parameters' selected. The main panel displays the 'SIP General Parameters' configuration table. The following table represents the data visible in the screenshot:

Parameter	Value
Enable TCP Connection Reuse	Disable
TCP Timeout	0
SIP Destination Port	5061
Use user=phone in SIP URL	Yes
Use user=phone in From Header	No
Use Tel URI for Asserted Identity	Disable
Tel to IP No Answer Timeout	180
Enable Remote Party ID	Disable
Add Number Plan and Type to RPI Header	Yes
Enable History-Info Header	Enable
Use Source Number as Display Name	No
Use Display Name as Source Number	No
Enable Contact Restriction	Disable
Play Ringback Tone to IP	Don't Play
Play Ringback Tone to Tel	Prefer IP
Use Tgrp information	Disable
Enable GRUU	Disable
User-Agent Information	
SDP Session Owner	AudiocodesGW
Play Busy Tone to Tel	Don't Play

Optionally, scroll down further and set the **SDP Session Owner** field. The default value is “**AudiocodesGW**” which defines the creator or owner of the SIP session.

The screenshot shows the same AudioCodes Mediant 3000 configuration interface, but scrolled down to show more parameters. The 'SDP Session Owner' field is highlighted with a red rectangle. The following table represents the data visible in this section of the screenshot:

Parameter	Value
Enable GRUU	Disable
User-Agent Information	
SDP Session Owner	AudiocodesGW
Play Busy Tone to Tel	Don't Play
Subject	
Multiple Packetization Time Format	None
Enable Semi-Attended Transfer	Disable
3xx Behavior	Forward
Enable P-Charging Vector	Disable
Enable VoiceMail URI	Disable
Retry-After Time	0
Enable P-Associated-URI Header	Disable
Source Number Preference	

Click **Submit** and then **Burn** to save the changes.

7.5. Configure Codec Preferences

On **Configuration** tab, expand **VoIP → Coders And Profiles → Coders** in the left pane.

In the **Coders Table** in the right pane, select the same set of codecs specified in **Section 5.3**.

In the sample configuration, “**G.711U-law**” and “**G.729**” codecs were used.

The **Coders Table** for the sample configuration is shown below.

The screenshot shows the AudioCodes Mediant 3000 configuration interface. The left pane shows the navigation tree with 'Coders' selected under 'Coders And Profiles'. The right pane displays the 'Coders Table' with the following data:

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711U-law	20	64	0	Disabled
G.729	20	8	18	Disabled

Click **Submit**.

7.6. Configure Trunk Group

On **Configuration** tab, expand **VoIP → GW and IP to IP → Trunk Group** in the left pane.

Select **Trunk Group**. The **Trunk Group Table** is displayed in the right pane.

Select the **Group Index** to configure.

Enter the following values and use default values for remaining fields.

- **From Trunk and To Trunk** Select available Trunk numbers.
In sample configuration, “1” and “5” were used.
- **Channels** Enter number of Channels.
In sample configuration, “1-24” was used.
- **Trunk Group ID** Enter available Trunk Group ID.
In sample configuration, “1” was used.

The **Trunk Group Table** for the sample configuration is shown below.

The screenshot shows the AudioCodes Mediant 3000 configuration interface. The left pane shows the navigation tree with 'Trunk Group' selected under 'VoIP → GW and IP to IP'. The right pane displays the 'Trunk Group Table' configuration. At the top, there are dropdowns for 'Add Phone Context As Prefix' (set to 'Disable') and 'Trunk Group Index' (set to '1-10'). Below these is a table with 10 rows. The first row is highlighted with a red border and contains the following values: Group Index: 1, From Trunk: 1, To Trunk: 5, Channels: 1-24, Phone Number: (empty), Trunk Group ID: 1, and Tel Profile ID: 0. The bottom right corner of the interface has a 'Submit' button with a checkmark icon.

Group Index	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	1	5	1-24		1	0
2						
3						
4						
5						
6						
7						
8						
9						
10						

Click **Submit** and then **Burn** to save the changes.

7.7. Configure Tel-to-IP Routing

On **Configuration** tab, expand **VoIP → GW and IP to IP → Routing** in the left pane.

Select **Tel to IP Routing**. The **Tel to IP Routing** table is displayed in the right pane.

Enter the following values and use default values for remaining fields.

- **Src. Trunk Group ID** Enter Trunk Group ID defined in **Section 7.6**.
- **Dest. Phone Prefix** Enter dial pattern(s) for extension numbers used in network. In sample configuration, “12*” and “31*” were assigned to SIP stations
- **Source Phone Prefix** Enter dial pattern(s) for PSTN numbers. In sample configuration, “1*” was assigned to PSTN users.
- **Dest. IP Address** Enter IP Address of Session Manager.
- **Port** Enter “5061”.
- **Transport Type** Select “TLS”.

The **Tel to IP Routing** table for the sample configuration is shown below.

The screenshot shows the AudioCodes Mediant 3000 configuration interface. The left pane shows the navigation tree with 'Routing' and 'Tel to IP Routing' highlighted. The right pane displays the 'Tel to IP Routing' table. The table has columns: Src. Trunk Group ID, Dest. Phone Prefix, Source Phone Prefix, Dest. IP Address, Port, Transport Type, Dest. IP Group ID, Dest. SRD, IP Profile ID, and Status. The table contains 7 rows of data, with the first three rows highlighted by a red box. The Dest. IP Address column is masked with a black box.

Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	Dest. IP Address	Port	Transport Type	Dest. IP Group ID	Dest. SRD	IP Profile ID	Status
1	12*	1*	135.64.	5061	TLS	-1	-1	0	OK
2	2*	1*	135.64.	5061	TLS	-1	-1	0	OK
3	31*	1*	135.64.	5061	TLS	-1	-1	0	OK
4	3*	1*	135.64.	5061	TLS	-1	-1	0	OK
5	4*	1*	135.64.	5061	TLS	-1	-1	0	OK
6	4*	1*	135.64.	5061	TLS	-1	-1	0	OK
7	5*	1*	135.64.	5061	TLS	-1	-1	0	OK

Note: IP Addresses have been hidden for security.

Click **Submit** and then **Burn** to save changes.

7.8. Configure Trunk Group Routing

In the sample configuration, **IP to Trunk Group Routing** is used to route SIP calls received from Session Manager to PSTN users. These calls are routed by AudioCodes M3K Media Gateway over the previously defined PSTN trunk using configuration defined in this section.

On **Configuration** tab, expand **VoIP → GW and IP to IP → Routing** in the left pane.

Select **IP to Trunk Group Routing**. The **IP to Trunk Group Routing Table** is displayed.

Enter the following values and use default values for remaining fields.

- **Dest. Phone Prefix** Enter “*”.
- **Source Phone Prefix** Enter “*”.
- **Trunk Group ID** Enter Trunk Group ID defined in **Section 7.6**.

Note: a value of “*” for **Dest. Phone Prefix** and **Source Phone Prefix** indicates all possible values.

The **IP to Trunk Group Routing Table** for the sample configuration is shown below.

The screenshot shows the AudioCodes Mediant 3000 configuration interface. The left pane shows the navigation tree with 'IP to Trunk Group Routing' selected. The main pane displays the 'IP To Trunk Group Routing Table' with a table containing 8 columns: Source Host Prefix, Dest. Phone Prefix, Source Phone Prefix, Source IP Address, Source SRD ID, Trunk Group ID, IP Profile ID, and Source IP Group ID. The first row is highlighted with a red box, showing asterisks for the first three columns and specific values for the last three.

Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Source SRD ID	Trunk Group ID	IP Profile ID	Source IP Group ID
	*	*		-1	1	0	-1
				-1			
				-1			
				-1			
				-1			
				-1			
				-1			

Click **Submit** and then **Burn** to save changes.

7.9. Configure SIP Proxy

On **Configuration** tab, expand **VoIP → SIP Definitions** in the left pane.

Select **Proxy & Registration**. Select the arrow associated with **Proxy Set Table** field as highlighted below to open the **Default Proxy Sets Table**.

The screenshot shows the AudioCodes Mediant 3000 configuration interface. The left pane displays the navigation tree with 'SIP Definitions' and 'Proxy & Registration' highlighted. The main pane shows the 'Proxy & Registration' settings. A red arrow points to the 'Proxy Set Table' field, which is currently set to 'sipunetlab.com'.

Select **“TLS”** for the **Transport Type** field as shown below.

The screenshot shows the 'Default Proxy Sets Table' configuration interface. The table has columns for Proxy Set ID, Proxy Address, and Transport Type. The first row is highlighted with a red box, showing Proxy Set ID 1, Proxy Address 135.64, and Transport Type TLS.

Proxy Set ID	Proxy Address	Transport Type
1	135.64	TLS
2	135.64	TLS
3		
4		
5		

Click **Submit** and then **Burn** (not shown).

7.10. Configure Privacy Feature

To enable SIP users to activate the feature to block sending Calling Party ID, verify AudioCodes M3K Media Gateway is configured to remove Calling Party ID when the SIP INVITE from Session Manager indicates the information is restricted.

On **Configuration** tab, expand **VoIP → GW and IP to IP → Digital Gateway** in the left pane.

Select **Digital Gateway Parameters** and verify **Remove CLI when Restricted** field is set to **“Yes”** as shown below.

The screenshot shows the AudioCodes Mediant 3000 configuration interface. The left pane shows the navigation tree with 'VoIP' expanded, and 'GW and IP to IP' selected. Under 'GW and IP to IP', 'Digital Gateway' is expanded, and 'Digital Gateway Parameters' is selected. The main pane displays the 'Digital Gateway Parameters' configuration table. The 'Remove CLI when Restricted' field is highlighted with a red box and set to 'Yes'.

Parameter	Value
Send Screening Indicator to IP	Not Configured
Send Screening Indicator to ISDN	Not Configured
Add IE in SETUP	
Trunk Groups to Send IE	
User-to-User IE for Tel to IP	Disable
User-to-User IE for IP to Tel	Disable
Enable ISDN Tunneling Tel to IP	Disable
Enable QSIG Tunneling	Disable
Enable ISDN Tunneling IP to Tel	Disable
ISDN Transfer on Connect	Alert
Remove CLI when Restricted	Yes
Remove Calling Name	Disable
TDM Over IP Min Calls	0
ISDN Facility Trace	Disable
Use EndPoint Number As Calling Number Tel2IP	Disable
Use EndPoint Number As Calling Number IP2Tel	Disable
Default Cause Mapping From ISDN to SIP	0
Add Prefix to Redirect Number	
Copy Destination Number to Redirect Number	Don't copy

Click **Submit** and then **Burn** (not shown).

7.11. Generate TLS Certificate on AudioCodes Mediant 3000 Gateway

To establish secure communication between the AudioCodes Mediant 3000 Media Gateway and Session Manager using TLS, the server certificate for the AudioCodes M3K Media Gateway must be saved in PEM format and uploaded to Session Manager.

The certificate is saved in PEM format using the CLI interface.

Step 1: Enable SSH or Telnet access using Mediant 3000 Administration web interface.

On **Configurations** tab, expand **System** → **Management** and select **Telnet/SSH Settings** in the left pane.

On the **Telnet/SSH Settings** page, -under **SSH Settings**, set **Enable SSH Server** field to “**Enable**” as shown below:

The screenshot shows the AudioCodes Mediant 3000 Administration web interface. The left sidebar contains a tree view with the following structure:

- Configuration
- Maintenance
- Status & Diagnostics
- Scenarios
- Search
- Basic
- Full
- System
 - Application Settings
 - Syslog Settings
 - Regional Settings
 - Certificates
 - Management
 - WEB User Accounts
 - WEB Security Settings
 - Telnet/SSH Settings
 - WEB & Telnet Access List
 - RADIUS Settings
 - SNMP
 - VoIP

The main content area displays the 'Telnet/SSH Settings' page. It contains two sections:

- Telnet Settings**
 - Embedded Telnet Server: Disable
 - Telnet Server TCP Port: 23
 - Telnet Server Idle Timeout: 0
- SSH Settings**
 - Enable SSH Server: Enable
 - Server Port: 22
 - SSH Admin Key:
 - Require Public Key: Disable
 - Max Payload Size: 32768
 - Max Binary Packet Size: 35000
 - Enable Last Login Message: Enable
 - Max Login Attempts: 3

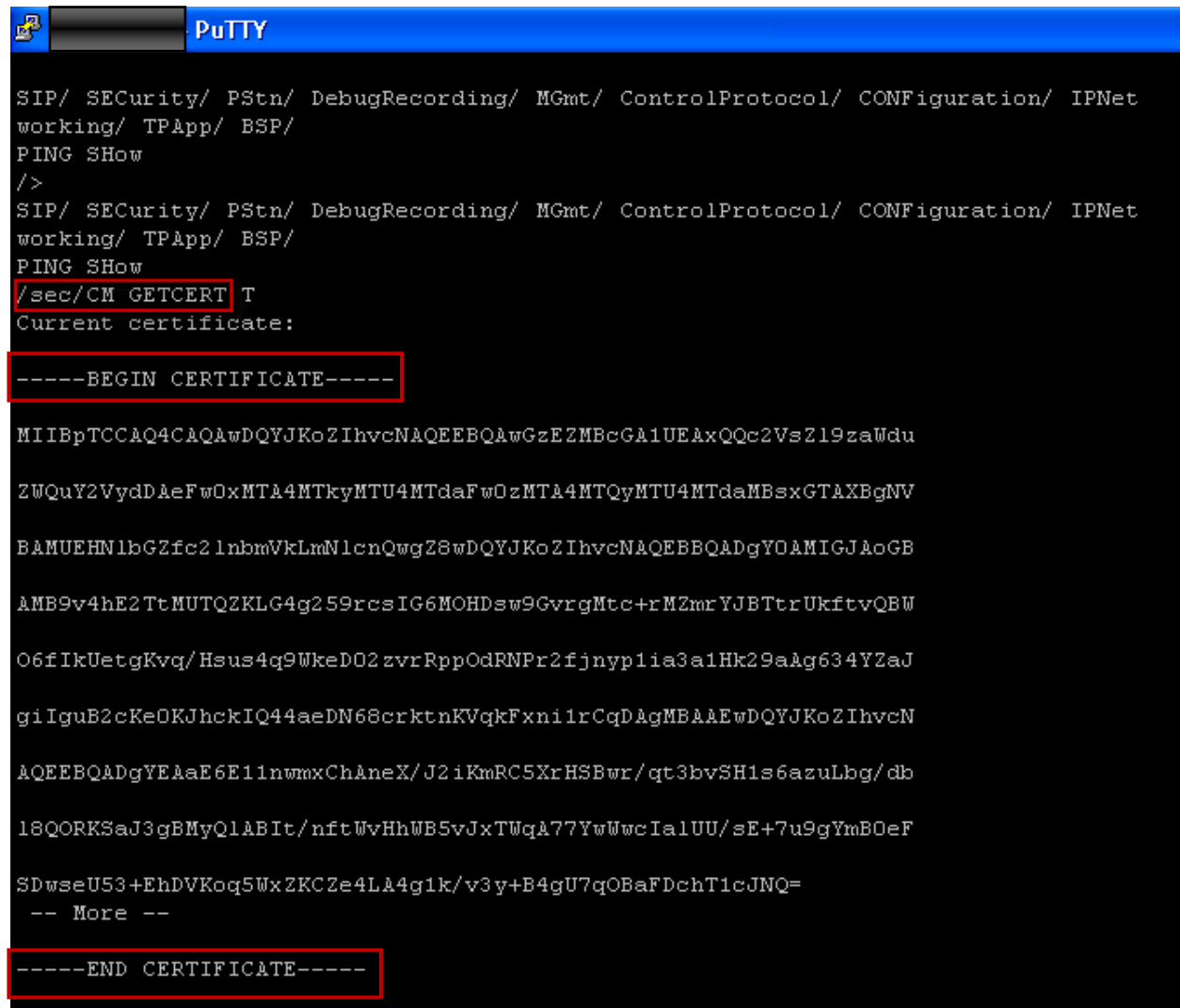
A 'Submit' button is located at the bottom right of the page.

Click **Submit**.

Step 2: Open a SSH or Telnet session to the AudioCodes Mediant 3000 Media Gateway with administrator credentials and run the command “/sec/CM GETCERT”.

Copy the certificate information, including the “**BEGIN CERTIFICATE**” and “**END CERTIFICATE**” lines (and all dashes) to a text file.

Edit text file using basic text editor application such as Microsoft WordPad to remove any extra lines and “—More—”.



```
PuTTY

SIP/ SEcUritY/ PStn/ DebugRecording/ MGmt/ ControlProtocol/ CONFIguration/ IPNet
working/ TPApp/ BSP/
PING SHow
/>
SIP/ SEcUritY/ PStn/ DebugRecording/ MGmt/ ControlProtocol/ CONFIguration/ IPNet
working/ TPApp/ BSP/
PING SHow
/sec/CM GETCERT T
Current certificate:
-----BEGIN CERTIFICATE-----
MIIBpTCCAQ4CAQAwDQYJKoZIhvcNAQEEBQAwGzEZMBcGA1UEAxQQc2VsZ19zaWdu
ZWQuY2VydAeFw0xMTA4MTkyMTU4MTdaFw0xMTA4MTQyMTU4MTdaMBsxGTAXBgNV
BAMUEHNlbGZfc2lnbmVklmNlcnQwgZ8wDQYJKoZIhvcNAQEEBQADgYOAAMIGJAoGB
AMB9v4hE2TtMUTQZKLg4g259rcsIG6MOHDsw9GvrgMtc+rMZmrYJBTtrUkftvQBW
O6fIkUetgKvq/Hsus4q9WkeD02zvrRppOdRNP2fjnyplia3a1Hk29aAg634YZaJ
giIguB2cKeOKJhckIQ44aEDN68crktnKVqkFxn1rCqDAgMBAEEwDQYJKoZIhvcN
AQEEBQADgYEAaE6E11nwmXChAneX/J2iKmRC5XrHSBwr/qt3bvSH1s6azuLbg/db
l8QORKSaJ3gBMyQlABIt/nftWvHhWB5vJxTWqA77YwUwcIalUU/sE+7u9gYmBOeF
SDwseU53+EhDVkoq5WxZKCZe4LA4g1k/v3y+B4gU7qOBaFDchT1cJNQ=
-- More --
-----END CERTIFICATE-----
```

Note: An alternative method to access command line interface using the URL “**http://<ip-address>/FAE**”, where “<ip-address>” is the IP address of AudioCodes M3K Gateway server. Login with administrator credentials and select “**Cmd Shell**” link (not shown) on left hand side.

7.12. Upload TLS Certificate to Avaya Aura® Session Manager

Step 1: Expand Services → Inventory and select **Manage Elements**.

Select the entry for Session Manager and select **Configure Trusted Certificates** (not shown) from the **More Actions** menu.

Avaya Aura® System Manager 6.3

Home / Services / Inventory / Manage Elements

Manage Elements

Elements

View Edit New Delete Get Current Status More Actions

Name	Node	Type
192.168.2.11	192.168.2.11	UCMAApp
192.168.2.20	192.168.2.20	UCMAApp
192.168.2.21	192.168.2.21	UCMAApp
192.168.2.24	192.168.2.24	UCMAApp
192.168.2.25	192.168.2.25	UCMAApp
ASM1	135.64	Session Manager
ASM2	135.64	Session Manager

Click the **Add** button (not shown) and select the **Import as PEM certificate** radio button.

Home / Services / Inventory / Manage Elements

Add Trusted Certificate

Select Store Type to add trusted certificate All

☐ Import from file

☒ Import as PEM certificate

☐ Import from existing certificates

☐ Import using TLS

Please paste the PEM certificate contents into this space.

You may include the start and end tags: "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----".

```
-----BEGIN CERTIFICATE-----
MIIDdjCCA6gAwIBAgIQejSWyOic8axBOSrDY3xFFzANBgkqhkiG9w0BAQUFADBD
MRMwEQYKCZImiZPyLQGByRyDy29tMRgwFgYKZCImiZPyLQGByRyIU0IMU3RhY2sx
EjAQBGNVBAmtCVRSSUdHRVJDQTAeFw0xMzAzMjIxMDAzMjVafW0yMzAzMjIxMDEz
MTNaMEMxEzARBgoJkiaJk/IsZAEZFgNjb20xGDAWBgoJkiaJk/IsZAEZFghTSUxT
dGFjazESMBAGA1UEAxMJVFJJR0dFUKNBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEApMvd1SNQ2wRh9OCaUSbSYHgr/CJoJf8L3u11nwIIZq8bzLUENULN
sy8LbKhyP6tMGRRX4212Crc1Qn+F7wIIfh/0j18IRUooEgEF1qYCeAEXA5iic+p+
zhKo1YrtPw0vA2Koz6im79ZqymzGdJrWuHUKW0//SaJLVSGhd7oTIDEMLEjLecE
ao+Vc8ZB6MVWigoRWFHHSKV/DHF30Ru+w3wxwLgbE2mnymcbro0NLG8/piHoiDTm
1WqxTTdzyniBUFWdrYE9bjMXKFAnXvNp+loJ35XjHiKJiceZxZWuf9JWSkjQDj3
5ofw7hbnOhmecKwJQsjxEVF357FowbTE6wIDAQABo2YwZDATBgkrBgEEAYI3FAIE
Bh4EAEMAQTALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQ
J
```

Paste the trusted certificate from AudioCodes M3K Media Gateway as described in **Section 7.11** and click **Commit** (not shown). Click **Done** (not shown) to save the changes.

Step 2: Expand **Elements** → **Session Manager** → **System Status** and select **Security Module Status**.

Select the entry for Session Manager and select **Update Installed Certificates** (not shown) from the **Certificate Management** menu.

AVAYA Avaya Aura® System Manager 6.3 Last Logged on at July 23, 2013 11:42 AM
Help | About | Change Password | Log off admin

Session Manager x Inventory x Home

Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Managed Bandwidth Usage
Security Module Status

Home / Elements / Session Manager / System Status / Security Module Status Help ?

Security Module Status

This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.

3 Items Refresh Show ALL Filter: Enable

	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)	Certificate Used
☒	► Show	ASM1	SM	Up	33	135.64.1.1	4	135.64.1.1	Disabled	10/10	Customer CA
☐	► Show	ASM2	SM	Up	31	135.64.1.2	4	135.64.1.2	Disabled	10/10	Customer CA
☐	► Show	ASM3	SM	Up	22	135.9.2.1	4	135.9.2.1	Disabled	5/5	Customer CA

Select : None

Click **Confirm** on **Confirm Security Module Update Installed Certificates** window as shown below.

Home / Elements / Session Manager / System Status / Security Module Status

Confirm Security Module Update Installed Certificates

Session Manager	Type	Status
ASM1	SM	Up

7.13. Upload Avaya Aura® System Manager Root Certificate

AudioCodes M3K Media Gateway uses a Private Key and a Server Certificate to perform the TLS handshake with Session Manager. Both the Private Key and Server Certificate are signed by System Manager which functions as the Trusted CA root authority in the sample configuration.

The following procedure outlines the required steps.

Step 1: Create End Entity for AudioCodes M3K Media Gateway.

From the System Manager **Home** page (not shown), navigate to **Security → Certificates → Authority → RA Functions** and select **Add End Entity**.

Enter the following values and use default values for remaining fields.

- **End Entity Profile** Select “**INBOUND_OUTBOUND_TLS**”.
- **Username** Enter username.
In the sample configuration, “**AudioCodes**” was used.
- **Password** Enter password.
- **Confirm Password** Enter the same password as previous entry.
- **CN, Common Name** Enter the IP Address of AudioCodes M3K Media Gateway.
- **Token** Select “**PEM file**”.

Click **Add End Entity** to submit.

CA Functions

- Basic Functions
- Edit Certificate Profiles
- Edit Publishers
- Edit Certificate Authorities
- RA Functions**
- Edit User Data Sources
- Edit End Entity Profiles
- Add End Entity**
- List/Edit End Entities
- Supervision Functions**
- Approve Actions
- View Log
- System Functions**
- System Configuration
- Edit Services
- Public Web

Certificate Authority

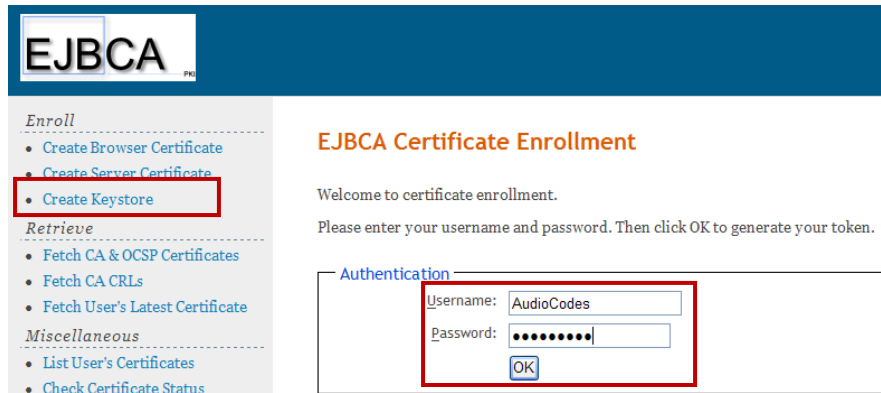
Add End Entity

End Entity Profile	INBOUND_OUTBOUND_TLS	Required
Username	AudioCodes	☒
Password		☒
Confirm Password		
Email		☐
Subject DN Fields		
CN, Common Name	135.64	☒
CN, Common Name		☐
OU, Organization Unit	SDP	☐
O, Organization	AVAYA	☐
C, Country (ISO 3166)	US	☐
Certificate Profile	ID_CLIENT_SERVER	☒
CA	tmdefaultca	☒
Token	PEM file	☒
Add End Entity Reset		

Step 2: Navigate to **Security → Certificates → Authority → Public Web** (not shown).

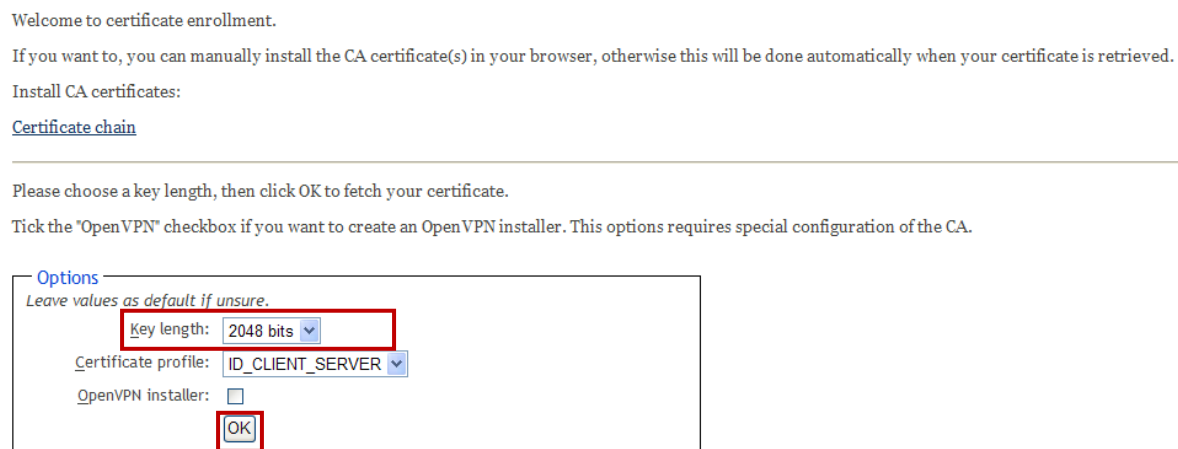
The **EJBCA** window is displayed, as shown below. Click on **Create Keystore**.

Under **Authentication** section, enter **Username** and **Password** defined in **Step 1** and click **OK**.



In the **Options** section on **EJBCA Token Certificate Enrollment** page, select “**2048 bits**” for **Key length** field and click **OK** to continue.

EJBCA Token Certificate Enrollment



In the next window, click **Save** (not shown) to save file to local PC.

Step 3: Open the PEM file containing the System Manager certificate created in **Step 2** using a basic text editor application such as Microsoft WordPad. The file generated and saved in PEM format contains the Private Key, Server certificate and Trusted Root certificate.

In the example shown below:

- The top section is the **Private Key** and is highlighted in **bold**.
- The middle section is the **Server Certificate** and is highlighted in **bold and red**.
- The third section is the **Trusted Root Certificate** and is highlighted in **bold and blue**.

Note: IP address has been partially hidden for security.

Bag Attributes

friendlyName: 135.64.xxx.xxx

-----BEGIN PRIVATE KEY-----

MIICdWIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBALbm5+3HShDK0h06
EmMz3m39vzGBW2vQbAOmX3cLR+h7a90UdoFfJba8nDcxcu8oATTdYPg+FRzQWRCD
RwpAcXzjxYyOGImmdbnJ4MCleBTlQk1AZ/KX7wNjSurXFoGgOGKd0i+Jk2rFu5C
XOW2RwJ5HBFVykIXfMcjvpurooUNAgMBAAECgYAv36yhXmKS1qP8pnCdqrVzyle7
IgLN65X6NpgSTs+ZmISZL3v9TOxQMnopMDZHRw9Zwk1ePNHF4vsNCW+UzV1mwnfW
fqmghid9BXS5pQ//ZJbVfJU2QafL3dGxmt45sOKcqzuxThGn44FTRMxNsLWvezA+
awe4q4k/cqJc3N1/QQJBAP3Bp1cyvUvXHkkyhev5g7+yquWLAzD5T1PDpes+Dfj
FXVlerPJAhtC6E0z71BjZjTu/dmP9r91bNKbkAUL8oUCQQC4hOKBg5VCsp871Yzs
8wGhpbQ7t4UwOLGR3k/86gYKPyh940PSRGEyb8jbxDHaiqIDh+/jaFpl8QtIe+iI
MsLpAkEA7SVPzggGL1lQ2X1U/ObpaLQnNeo3Korcrso2SfuFUb1wLXF0FZbQU2F4
9cWffY0VtHxxUiSfpcKKxUJKetzqfQJAJ37qLobJcD1jtBFS1PU/CCa76Xxi2euI
trxrSqudF1xlgmy++6b/VxhuWfwo36qE+1SBmJ+hmeH6jc1X/K9A4QJBAM+bYQaG
JIsZgVEMPEKqXKS8uboktSm2p9vk4zyw/IMJhT/C3Ng8gRLAeCuPCLeGrAnVmXBV
OFIirgZPkB2GX6I=

-----END PRIVATE KEY-----

Bag Attributes

friendlyName: 135.64.xxx.xxx

subject=/CN=135.64.xxx.xxx/OU=SDP/O=AVAYA/C=US

issuer=/CN=default/OU=MGMT/O=AVAYA

-----BEGIN CERTIFICATE-----

MIICbDCCAdWgAwIBAgIIa+eX5sN3Bg0wDQYJKoZIhvcNAQEFBQAwMTEQMA4GA1UE
AwWHZGVmYXVsdDENMAsGA1UECwwETUdnVDEOMAwGA1UECgwFQVZBWUEwHhcNMTIx
MTI2MTM0MjE5WmcNMjEwNzE1MTEeMDQzWjA/MRIwEAYDVQQDDAlhdmF5YS5jb20x
DDAKBgNVBAsMA1NEUDEMawGA1UECgwFQVZBWUEwEzA1JBgNVBAYTA1VTMIGfMA0G
CSqGSIb3DQEBBQUAA4GNADCBiQKBgQC25uftx0oQytIdOhJjM95t/b8xgVtr0GwD
p193C0foe2vdFHaBXyW2vJw3MXLvKAE0w8j4PhUc0FkQg0cKQHF848WMjhiJps3W
5yeDapXgU5UJNQGfYl+8DY0rq1xaBoDhindIviZNqxbuQlzltkcCeRwRVcpCF3zh
I76bq6KFDQIDAQAB038wftAdBgNVHQ4EFgQUtlyKVDFdYA//0FNqfOnQG0Js6z8w
DAYDVR0TAQH/BAIwADafBgNVHSMEGDAWgBQFRuH9J1bDcmt/HwFWqmrJFtAVBDAO
BgNVHQ8BAf8EBAMCA/gwHQYDVR01BBYwFAYIKwYBBQUHAWEGCCsGAQUFBwMCMA0G
CSqGSIb3DQEBBQUAA4GBAF0wla7jpPoutiFEz07D3zdFurigZ8tFC9amA61pp3d4y
7UXW0Q2Q3+tmYXY9qm5u09YxzzPrigv8fUG4XoSla6myIkWZbbwNsFrkX9GSF/x7
MDZ3Zd8ZM32TGyE4NnNHiqScSQylqhO3mmzwXIS4eava8lamCysV1Au547+iInuA

-----END CERTIFICATE-----

Bag Attributes

friendlyName: default

subject=/CN=default/OU=MGMT/O=AVAYA

issuer=/CN=default/OU=MGMT/O=AVAYA

-----BEGIN CERTIFICATE-----

```
MIICQjCCAaugAwIBAgIIJPi5aPzXr+owDQYJKoZIhvcNAQEFBQAwMTEQMA4GA1UE
AwWHZGVmYXVsdDENMAsgA1UECwwETUdNVDEOMAwGA1UECgwFQVZBWUEwHhcNMTIw
NzE3MTExMDQzWhcNMjIwNzE1MTExMDQzWjAxMRAwDgYDVQQDDAdkZWZhdWx0MQ0w
CwYDVQQQLDARNR01UMQ4wDAYDVQQKDAVBVkfZQTCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEAhDS0j+ZPhN0S0FKuGnH73CVE+WtZEpKmG5kKjYWD/PzHJqqTgzO1
jo9epyKAbiNgQ9venpS4d6eOtanKcW/b8DpeUwU/B00SCdKmpCiOFEjOdiWGiRhN
F5YdYuREwchJjj017o9GRjm4ossbrUvTHy0Z7VaVxa/9zK4JXYM40U0CAwEAAAnj
MGEwHQYDVR0OBByEFaVG4f0nVsNya38fAVaqaskW0BUEMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBgwFoAUBUBh/SdWw3Jrfx8BVqpqyRbQFQwDgYDVDR0PAQH/BAQD
AgGGMAM0GCSqGSIb3DQEBBQUAA4GBAEuK6AUKU5u2/EV/GfgjG8TskWKPIUE0hOzQ
n+0Vzs09Q1DPQAT9jt7eG1AZ2XamYA0oOiMat1pfgrHhUy7YXj2a9Y3bcqPPbxPU
GMCbmHd6Qsc/WROMi5vzaKhQVn5efFKLwKAr+3Awz91R96XPtGAY3Aqss9bYFnZc
XL7X143e
```

-----END CERTIFICATE-----

Copy the Private Key, Server certificate, and the Trusted Root certificate into three separate text files. Include the “**BEGIN PRIVATE KEY**” and “**END PRIVATE KEY**” lines (and all dashes) in the first file and the “**BEGIN CERTIFICATE**” and “**END CERTIFICATE**” lines (and all dashes) in the two certificate files.

Step 4: Upload Avaya Aura® System Manager certificates to AudioCodes M3K Media Gateway.

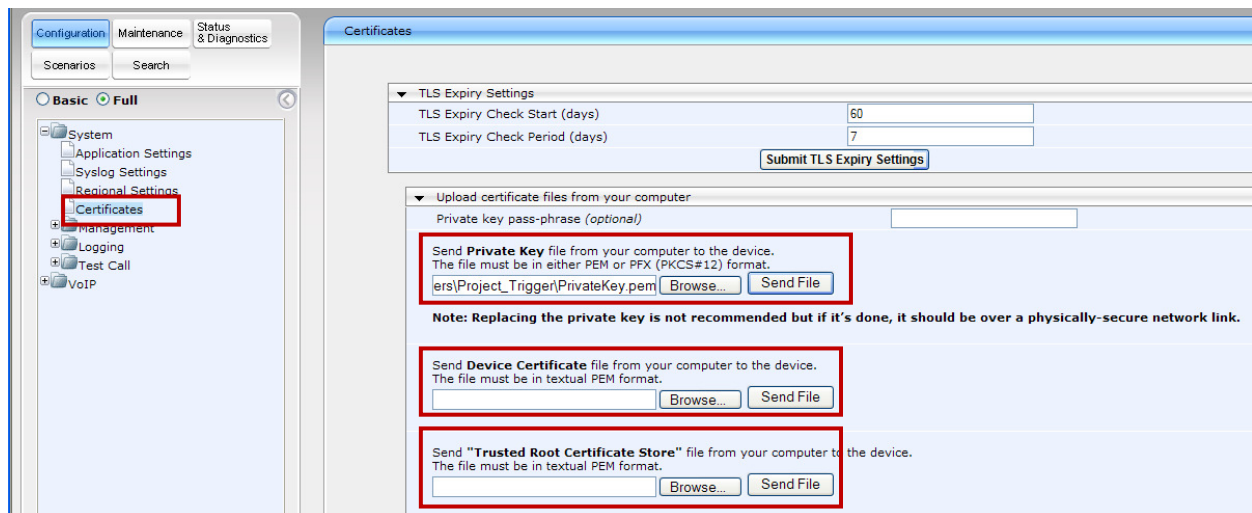
Log into browser-based GUI of AudioCodes M3K Gateway as described in **Section 7.1**.

On **Configuration** tab, expand **System** → **Certificates** and scroll down to “**Upload certificates files from your computer**” section.

In **Private Key** section, click **Browse** to upload the first of the three files created in **Step 3** and click **Send File**.

Repeat this step to upload the two files containing certificates as described below.

- **Private Key:** Select the file containing the Private Key created in **Step 3** and highlighted in **bold**.
- **Device Certificate:** Select the file containing the Server certificate created in **Step 3** and highlighted in **bold and red**.
- **Trusted Root Certificate:** Select the file containing the Trusted CA certificate created in **Step 3** and highlighted in **bold and blue**.



Click **Submit** (not shown) to save changes.

7.14. Configure Media Settings

Step 1: On **Configuration** tab, expand **VoIP** → **Media** and select **Media Security**.

Under the **General Media Security Settings** section, enter the following values.

- **Media Security** Select “**Enable**”.
- **Media Security Behavior** Select “**Mandatory**”.

Expand **SRTP offered Suites** section and select **CIPHER AES CM 128 HMAC SHA1 80**.

The screenshot shows the AudioCodes Mediant 3000 configuration interface. On the left, the 'Configuration' tab is active, and the 'Media' folder under 'VoIP' is expanded. The 'Media Security' option is selected. The main panel displays the 'Media Security' configuration page. The 'General Media Security Settings' section is expanded, showing the following settings:

Setting	Value
Media Security	Enable
Aria Protocol Support	Disable
Media Security Behavior	Mandatory
Authentication On Transmitted RTP Packets	Active
Encryption On Transmitted RTP Packets	Active
Encryption On Transmitted RTCP Packets	Inactive
SRTP Tunneling Authentication for RTP	Disable
SRTP Tunneling Authentication for RTCP	Disable

The 'SRTP Setting' section is also expanded, showing:

Setting	Value
Master Key Identifier (MKI) Size	0
Symmetric MKI Negotiation	Disable

The 'SRTP offered Suites' section is expanded, showing the following settings:

Suite	Value
CIPHER SUITES AES CM 128 HMAC SHA1 80	☒
CIPHER SUITES AES CM 128 HMAC SHA1 32	☐
CIPHER SUITES ARIA CM 128 HMAC SHA1 80	☐
CIPHER SUITES ARIA CM 192 HMAC SHA1 80	☐

Step 2: On **Configuration** tab, expand **VoIP** → **SIP Definitions** and select **General Parameters**. Verify **Enable SIPs** field is set to “**Enable**”.

The screenshot shows the AudioCodes Mediant 3000 configuration interface. On the left, the 'Configuration' tab is active, and the 'SIP Definitions' folder under 'VoIP' is expanded. The 'General Parameters' option is selected. The main panel displays the 'SIP General Parameters' configuration page. The 'SIP General' section is expanded, showing the following settings:

Setting	Value
NAT IP Address	0.0.0.0
PRACK Mode	Supported
Channel Select Mode	Cyclic Ascending
Enable Early Media	Enable
183 Message Behavior	Progress
Session-Expires Time	2400
Minimum Session-Expires	90
Session Expires Method	Re-INVITE
Asserted Identity Mode	Adding P-Asserted Identity
Fax Signaling Method	No Fax
Detect Fax on Answer Tone	Initiate T.38 on Preamble
SIP Transport Type	TLS
SIP UDP Local Port	5060
SIP TCP Local Port	5060
SIP-TLS Local Port	5061
Enable SIPs	Enable
Enable TCP Connection Reuse	Disable
TCP Timeout	In

Click **Submit** and then **Burn**.

8. Verification Steps

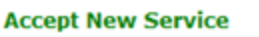
The following sections demonstrate some of the methods available to verify network connectivity and trace calls between PSTN users and SIP users registered to Session Manager.

8.1. Verify Avaya Aura® Session Manager Configuration

Step 1: Verify Avaya Aura® Session Manager is Operational

Expand **Elements** → **Session Manager** and select **Dashboard** to verify the overall system status of Session Manager.

Specifically, verify the status of the following fields as shown below:

- **Tests Pass** 
- **Security Module** 
- **Service State** 
- **Data Replication** 



Avaya Aura® System Manager 6.3

Last Logged on at March 28, 2013 11:35 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Session Manager x Inventory x Home

Home / Elements / Session Manager

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State Shutdown System As of 6:06 PM

2 Items Refresh Show ALL Filter: Enable

☐	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	Version
☐	ASM1	Core	✓	0/0/0	Up	Accept New Service	0/8	0	15/15	✓	6.3.1.0.631004

Step 2: Verify SIP Entity Link Status

Navigate to **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring** to view more detailed status information for the specific SIP Entity Link used for calls between SIP endpoints and non-SIP stations on Communication Manager Evolution Server.

Select the SIP Entity for Communication Manager Evolution Server from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page.

In the **All Entity Links to SIP Entity: CM-ManagedIP** table, verify the **Conn. Status** of SIP Entity link is “Up” as shown below:

Click  to view more information associated with the selected Entity Link.

Note: IP address has been partially hidden for security.

AVAYA Avaya Aura® System Manager 6.3

Last Logged on at March 28, 2013 11:35 A
Help | About | Change Password | Log off adm

Session Manager x Inventory x Home

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: CM-ManagedIP

Summary View

Status Details for the selected Session Manager:
Time Last Down: 03/28/13 12:08:51 Last Message Sent: 03/28/13 12:08:51
Time Last Up: 03/28/13 10:03:47 Last Response Latency (ms): 6

2 Items (1 Selected) | Refresh Filter: Enable

Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
☒ ASM1	135.64. [REDACTED]	5061	TLS	FALSE	UP	200 OK	UP
☐ ASM2	135.64. [REDACTED]	5061	TLS	FALSE	DOWN	408 Request Timeout	DOWN

Repeat the above step and select SIP Entity for AudioCodes M3K Media Gateway Server to verify the **Conn. Status** of SIP Entity link is “Up” as shown below:

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

Help ?

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: Audiocodes M3K

Summary View

Status Details for the selected Session Manager:
Time Last Down: 07/24/13 13:03:02 Last Message Sent: 07/24/13 13:03:02
Time Last Up: 05/22/13 11:37:56 Last Response Latency (ms): 37

3 Items (1 Selected) | Refresh Filter: Enable

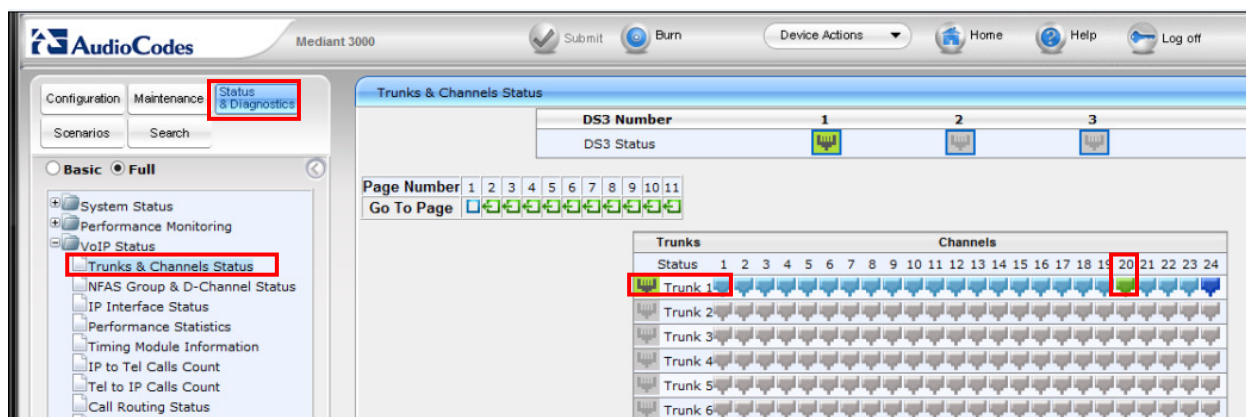
Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
☒ ASM1	135.64. [REDACTED]	5061	TLS	FALSE	UP	200 OK	UP

8.2. Verify AudioCodes Mediant 3000 Media Gateway Configuration

Verify the status of the SIP trunk group on AudioCodes M3K Media Gateway by accessing the web interface described in **Section 7.1**.

Step 1: On **Status & Diagnostics** tab, expand **VoIP Status** → **Trunks & Channel Status**.

Make a test call from a SIP user to a PSTN user and verify there is an active channel for the Trunk Group configured in **Section 7.6** as shown below.



Step 2: Verify AudioCodes M3K Media Gateway is correctly processing SIP messages from Session Manager using Syslog. Enable external logging from AudioCodes M3K Gateway to a client PC which will be used capture Syslog traces. It is assumed that a Syslog application such as **ACSysLog** is installed on the client PC.

On **Configurations** tab, expand **System** in the left pane and select **Syslog Settings**.

Under **Syslog Settings** on the right side, enter the following values.

- **Enable Syslog** Select “**Enable**”.
- **Syslog Server IP Address** Enter the IP address of the client PC.
- **Syslog Server Port** Enter port number.
In the sample configuration, “**515**” was used.
- **Debug Level** Select debug level.
Note: “**7**” is highest level.

The screenshot displays the AudioCodes Mediant 3000 configuration web interface. On the left, the 'Configuration' tab is active, and the 'System' menu item is expanded, showing 'Syslog Settings' as the selected option. The main panel on the right is titled 'Syslog Settings' and contains two sections. The first section, 'Syslog Settings', includes fields for 'Enable Syslog' (set to 'Enable'), 'Syslog Server IP Address' (172.16.14.10), 'Syslog Server Port' (515), 'Debug Level' (5), and 'Trunks Filter' (-1). The second section, 'Activity Types to Report via 'Activity Log' Messages', lists various events with checkboxes: Parameters Value Change, Auxiliary Files Loading, Device Reset (checked), Flash Memory Burning, Device Software Update, Access to Restricted Domains, Non-Authorized Access, Sensitive Parameters Value Change, and Login and Logout. A 'Submit' button is located in the bottom right corner of the interface.

Click **Submit**. Start the Syslog application on the client PC and begin tracing.

Place test call from PSTN user and verify proper routing through AudioCodes M3K Media Gateway by inspecting the SIP messages as shown in a subset of a syslog trace below.

Note: Trace has been edited to partially hide IP addresses for security purposes.

```
---- Incoming SIP Message from 135.64.xxx.xxx:23887 to SIPInterface #0
TlsTransportObject[#2598] ----
21:03:14.294 : 135.64.xxx.xxx : NOTICE : [S=114413] [SID:625214308] PRACK
sips:1021@135.64.xxx.xxx:5061;transport=tls SIP/2.0 User-Agent: Avaya
CM/R016x.03.0.124.0 AVAYA-SM-6.3.2.0.632023 AVAYA-SM-6.3.2.0.632023 Av-
Global-Session-ID: 2f6b1a80-f49c-11e2-9cd9-14feb5dc43ea Via: SIP/2.0/TLS
135.64.xxx.xxx;branch=z9hG4bK25310833789059-AP;ft=9 Via: SIP/2.0/TLS
135.64.xxx.xxx:15061;rport=34955;ibmsid=local.1369244184436_7617393_7642989;b
ranch=z9hG4bK25310833789059 Via: SIP/2.0/TLS
135.64.xxx.xxx;branch=z9hG4bK19656693540523-AP-
AP;ft=591611;received=135.64.xxx.xxx;rport=19434 Via: SIP/2.0/TLS
135.9.xxx.xxx;branch=z9hG4bK19656693540523-AP;ft=3 Via: SIP/2.0/TLS
135.9.xxx.xxx:15061;rport=45257;ibmsid=local.1373992360694_410174_416505;bran
ch=z9hG4bK19656693540523 Via: SIP/2.0/TLS
135.9.228.103;branch=z9hG4bK80608439c9f7e2165cd51f85e2e00-
AP;ft=56035;received=135.9.xxx.xxx;rport=54125 Via: SIP/2.0/TLS
135.64.187.75;branch=z9hG4bK80608439c9f7e2165cd51f85e2e00 Via: SIP/2.0/TLS
135.9.88.118:5061;branch=z9hG4bK10_b6681996ae8634f5d56c7e6_I31003 RACK: 1 1
INVITE Endpoint-View:
<sips:31003@silstack.com;gr=ff0838317ca22ecc6e0408409f76fc25>;local-tag=-
79a0792b51f041415d56c390_F31003135.9.88.118;call-id=f_b668146-
474aa5aa5d56c298_I@135.9.xxx.xxx;remote-tag=80608439c9f7e2161cd51f85e2e00
From: "westminster, uc_user_3"
<sips:31003@silstack.com;user=phone>;tag=80608439c9f7e2162cd
21:03:14.328 : 135.64.xxx.xxx : NOTICE : [S=114414] [SID:625214308] (
sip_stack)(423105 ) New SIPMessage created - #279 (
lgr_flow)(423106 ) | (SIPTU#2602)PRACK
State:Invited(80608439c9f7e2163cd51f85e2e00)
...
```

8.3. Verify Avaya Aura® Communication Manager Operational Status

Verify the status of the SIP trunk group on Communication Manager by using the **status trunk n** command, where **n** is the trunk group number administered in **Section 5.7**.

Verify that all trunks in the trunk group are in the “**in-service/idle**” state as shown below:

```
status trunk 2
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0002/001	T00006	in-service/idle	no
0002/002	T00007	in-service/idle	no
0002/003	T00008	in-service/idle	no
0002/004	T00009	in-service/idle	no
0002/005	T00014	in-service/idle	no
0002/006	T00015	in-service/idle	no
0002/007	T00043	in-service/idle	no
...			

Verify the status of the SIP signaling group by using the **status signaling-group** command, where **n** is the signaling group numbers administered in **Section 5.6**.

Verify the signaling group is “**in-service**” as indicated in the **Group State:** field shown below:

```
status signaling-group 2
```

STATUS SIGNALING GROUP	
Group ID: 2	Active NCA-TSC Count: 0
Group Type: sip	Active CA-TSC Count: 0
Signaling Type: facility associated signaling	
Group State: in-service	

Use **Page 3** of the **status trunk 000x/0xx** command where **000x** is trunk group defined in **Section 5.7** and **0xx** is trunk member to verify SRTP is being used in active call as shown below:

```
status trunk 0002/032
```

Page 3 of 3	
SRC PORT TO DEST PORT TALKPATH	
src port: T00038	
T00038:TX:135.9.228.230:35018/g711u/20ms/1-srtp-aescm128-hmac80	
T00041:RX:135.9.228.230:35020/g711u/20ms/1-srtp-aescm128-hmac80	

Use the SAT command, **list trace tac #**, where **tac #** is the trunk access code for the trunk group defined in **Section 5.7** to trace trunk group activity for the SIP trunk between Session Manager and Communication Manager. For example, the trace below illustrates a call from a SIP endpoint using extension “**31003**” to a PSTN user using extension “**11022**”.

Note: Trace has been edited to partially hide IP addresses for security purposes.

```
list trace tac *02                                     Page 1
LIST TRACE
time      data
20:51:31 TRACE STARTED 07/24/2013 CM Release String cold-03.0.124.0-999999
20:51:37 SIP<INVITE sips:31003@silstack.com;avaya-cm-fnu=off-hook SI
20:51:37 SIP<P/2.0
20:51:37      Call-ID: 8_b655e44-474ae2c75d559c9e_I@135.9.xxx.xxx
20:51:37 SIP>SIP/2.0 183 Session Progress
20:51:37      Call-ID: 8_b655e44-474ae2c75d559c9e_I@135.9.xxx.xxx
20:51:42 SIP>SIP/2.0 484 Address Incomplete
20:51:42      Call-ID: 8_b655e44-474ae2c75d559c9e_I@135.9.xxx.xxx
20:51:42 SIP<INVITE sips:11022@silstack.com SIP/2.0
20:51:42      Call-ID: 8_b655e44-474ae2c75d559c9e_I@135.9.xxx.xxx
20:51:42 SIP>SIP/2.0 100 Trying
20:51:42      Call-ID: 8_b655e44-474ae2c75d559c9e_I@135.9.xxx.xxx
20:51:42 SIP>INVITE sips:11022@135.64.xxx.xxx;user=phone SIP/2.0
20:51:42      Call-ID: 0567180c7f7e2126cd51f85e2e00
20:51:42      dial 11022 route:UDP|AAR
20:51:42      term trunk-group 2      cid 0x44e
20:51:42      dial 11022 route:UDP|AAR
20:51:42      route-pattern 2 preference 1 location 1/ALL cid 0x44e
20:51:42      seize trunk-group 2 member 2      cid 0x44e
20:51:42      Calling Number & Name NO-CPNumber NO-CPName
20:51:42 SIP<ACK sips:31003@silstack.com;avaya-cm-fnu=off-hook SIP/2
20:51:42 SIP<.0
20:51:42      Call-ID: 8_b655e44-474ae2c75d559c9e_I@135.9.xxx.xxx
20:51:42      Proceed trunk-group 2 member 2      cid 0x44e
20:51:42 SIP>SIP/2.0 180 Ringing
20:51:42      Call-ID: 8_b655e44-474ae2c75d559c9e_I@135.9.xxx.xxx
20:51:42      Alert trunk-group 2 member 2      cid 0x44e
20:51:43 SIP<PRACK sips:1019@135.64.xxx.xxx;transport=tls SIP/2.0
20:51:43      Call-ID: 8_b655e44-474ae2c75d559c9e_I@135.9.xxx.xxx
20:51:43 SIP>PRACK sips:1019@135.64.xxx.xxx:5061;transport=tls;gsid=7
20:51:43 SIP>3719260-f49a-11e2-9cd9-14feb5dc43ea SIP/2.0 20:51:43      Call-
ID: 0567180c7f7e2126cd51f85e2e00
20:51:43 SIP>SIP/2.0 200 OK
20:51:43      Call-ID: 8_b655e44-474ae2c75d559c9e_I@135.9.xxx.xxx
20:51:44 SIP>SIP/2.0 200 OK
20:51:44      Call-ID: 8_b655e44-474ae2c75d559c9e_I@135.9.xxx.xxx
20:51:44      active trunk-group 2 member 2      cid 0x44e
20:51:44 SIP<SIP/2.0 200 OK
20:51:44      Call-ID: 0b0d382c7f7e212acd51f85e2e00
...
```

9. Conclusion

These Application Notes describe how to configure a network with SIP trunks among Avaya Aura® Session Manager Release 6.2 FP2, AudioCodes Mediant 3000 Media Gateway Release 3.0 and Avaya Aura® Communication Manager Release 6.2 FP2. To provide secure network connections, all SIP trunks use Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) is used for media.

Test cases included bi-directional calls between PSTN users and Avaya IP Deskphones registered as SIP users to Session Manager, as well as traditional telephony operations and features such as extension dialing, displays, hold/resume, calling display block, transfer, conferencing, and call forwarding.

10. Additional References

Product documentation relevant to these Application Notes is available at <http://support.avaya.com>.

Avaya Aura® Session Manager

- 1) Avaya Aura® Session Manager Overview, Doc ID 100068105.
- 2) Installing and Configuring Avaya Aura® Session Manager, Doc ID 03-603473.
- 3) Avaya Aura® Session Manager Case Studies, Doc ID 03-603478.
- 4) Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325.
- 5) Administering Avaya Aura® Session Manager, Doc ID 03-603324.

Avaya Aura® Communication Manager

- 6) SIP Support in Avaya Aura® Communication Manager Running on Avaya S8xxx Servers, Doc ID 555-245-206.
- 7) Administering Avaya Aura® Communication Manager, Doc ID 03-300509.
- 8) Administering Avaya Aura® Communication Manager Server Options, Doc ID 03-603479.
- 9) Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide, Doc ID 210-100-500.
- 10) Avaya Toll Fraud Security Guide, Doc ID 555-025-600.

Avaya IP Deskphones (SIP)

- 11) Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide, Release 2.6. June 7, 2010.
- 12) Avaya one-X® Deskphone SIP Installation and Maintenance Guide Release 2.6, June 7, 2010.

Audio Codes Mediant 3000 Media Gateway

- 13) AudioCodes Mediant™ 3000 Setup Guide .
- 14) Installing and Operating the AudioCodes Mediant 3000 Media Gateway.

Avaya Application Notes

- 15) Create Certificate Signing Requests and apply Third-Party Certificates for Project Trigger
- 16) Configuring Avaya 96X1 SIP Deskphones with TLS as a Remote User with and without NAT Traversal with Avaya Session Border Controller Advanced for Enterprise 6.2 and Avaya Aura® Infrastructure
- 17) Configuring Avaya 9620L-PDB IP Deskphones using Secure Real-Time Transport Protocol (SRTP) with Avaya Aura® Session Manager Release 6.2 FP1 and Avaya Aura® Communication Manager Evolution Server Release 6.2 FP1
- 18) Configuring SIP Trunks among Avaya Communication Server 1000E 7.5, Avaya Aura® Session Manager 6.2, and AudioCodes Mediant 3000 Media Gateway 2.0

©2013 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabinotes@list.avaya.com