



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Mitel InAttend using Mitel Attendant Connectivity Server V2.6 to interoperate with Avaya Aura® Communication Manager R8.1 - Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for Mitel InAttend using Mitel Attendant Connectivity Server from Mitel Sweden AB to interoperate with Avaya Aura® Communication Manager. The Mitel solution makes use of two separate connections to Avaya Aura® Session Manager and to Avaya Aura® Application Enablement Services.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe the configuration steps required for Mitel InAttend using Mitel Attendant Connectivity Server V2.6 from Mitel Sweden AB to interoperate with Avaya Aura® Communication Manager R8.1 utilizing a SIP trunk connection to Avaya Aura® Session Manager R8.1 and a TSAPI connection to Avaya Aura® Application Enablement Services (AES).

Mitel InAttend is the core application in their attendant offering and an essential part in the Mitel Collaboration Management (CMG). It is a multi-featured attendant solution that is built on open standards and offers advanced collaboration features. The InAttend attendant console provides all necessary information for efficient call handling yet is fully integrated with the Mitel CMG for a complete Unified Communications experience. The InAttend SIP-based platform opens a way for integration with Avaya Aura® Communication Manager utilising a SIP connection to Avaya Aura® Session Manager using the Mitel Attendant Connectivity Server (ACS).

The ACS is responsible for the SIP connection to Session Manager and is part of the Attendant Platform which provides Private Branch Exchanges (PBX) with extended functionality. The Attendant client communicates with the private branch exchange through ACS. Using an attendant client, attendants can initiate, answer, transfer and disconnect calls. The call queuing functionality with configurable call queues also supports camp on services. Other features include automatic call distribution, which distributes the call to the attendant with the longest idle time, and direct drop to voicemail, which lets the attendant transfer calls directly to subscriber's voicemail. ACS also provides a speech attendant that enables a caller to request a user by name, and if busy, enables the caller to be transferred to an attendant, to the user's voicemail, or added to a conference. ACS also incorporates its own voicemail system.

The Mitel InAttend solution makes use of two TSAPI connections to Avaya Aura® Application Enablement Services.

- TSAPI connection from the CMG – Used to set Call Forwarding and Message Waiting.
- TSAPI connection from the InAttend server – Used to monitor devices to provide Presence information.

Mitel InAttend is made up of the following all installed on the same sever.

- Mitel Attendant Connectivity Server.
  - NeTS 5.12.1010.0
  - MediaServer 1.9.30.0
  - QueueManager 2.18.604.0
- Mitel InAttend Server.
  - Collaboration Management CMG 8.5
  - Virtual Reception 8.5
  - Microsoft SQL 2012
  - Mitel InAttend Server 2.6

During compliance testing various applications such as Virtual Reception which consists of Speech Attendant and Speech Office and these were tested alongside the InAttend console, these applications utilize the ACS to connect to Session Manager and the Mitel InAttend Server to connect to TSAPI. Each of these applications add to the overall solution and this solution will be referenced as “InAttend” throughout the remainder of this document unless there is a specific reason to refer to a specific application.

Mitel supply, install and configure their solution for the end customer directly or through qualified partners. In line with Mitel’s request the configuration of InAttend is not necessarily required to be part of these Application Notes, however **Section 8** does include screen shots of the setup that was used during compliance testing.

## 2. General Test Approach and Test Results

The general test approach was to configure InAttend to communicate with the Communication Manager as implemented on a customer’s premises using a SIP connection to Session Manager and a TSAPI connection to AES. Testing focused on verifying that ACS registered with Session Manager as a SIP Entity and both TSAPI connections showing that all features behaved as expected. Various call scenarios were performed to simulate real call types as would be observed on a customer premises. See **Figure 1** for a network diagram. The interoperability compliance test included both feature functionality and serviceability tests.

The ACS is configured as a SIP Entity on Session Manager acting as a 3<sup>rd</sup> party PBX connecting to the Avaya solution over a SIP trunk. The connection was setup using TCP transport and port 5060. Calls were then made from Communication Manager to the Mitel Attendant using a Dialling Plan on Communication Manager. Calls can be made between the Mitel solution and Communication Manager extensions by a connection between the ACS and Session Manager.

The TSAPI client is installed on the InAttend server which also runs the CMG database. This client then connected to the AES using a user/password created on AES allowing the TSAPI events be passed to the InAttend server and be processed by the applications there.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Mitel InAttend did not include use of any specific encryption features as requested by Mitel.

## 2.1. Interoperability Compliance Testing

The testing included:

- Verification of connectivity between Communication Manager and InAttend via Session Manager and AES
- InAttend and Speech Attendant transfers calls
- Supervised and unsupervised transfer with answer
- Directing callers to conference calls via Speech Attendant
- Call queuing and retrieval
- Detection for busy and unanswered extensions
- End to end signalling
- Call re-queuing
- Direct drop to voice mail
- Setting Call Forward and Message Waiting
- Observing Presence Information
- Serviceability tests simulating a LAN failure

## 2.2. Test Results

Tests were performed to insure full interoperability of the Mitel solution with Communication Manager using the connection between the ACS and Session Manager and a TSAPI connection between the InAttend server and AES. The tests were all functional in nature and performance testing was not included. All test cases passed successfully with the following observations noted.

1. The DevConnect test environment consisted of two signalling/trunks groups one to the SIP phones and another to Session Manager for SIP trunk calls. Direct IP – IP Audio Connections was set to N on the Signalling Group used for SIP phones to allow DTMF work properly when connecting to the CMG Speech Office.
2. Mitel requires that a person's phone is forwarded to the conference application for a conference to take place. A Communication Manager user/extension will get a busy tone when attempting to call itself when the extension is forwarded. When the administrator of a conference needs to dial in to that conference, they will call their extension from another known source i.e., their mobile phone. This mobile number would be associated with this user/extension on the Mitel database and so this call would be recognised as the conference administrator dialling in. A Coverage Path can also be used instead of Call Forward and this will allow the user call in from the phone itself.
3. An issue was observed when carrying out "Direct Drop" i.e., a Communication Manager user calls into Mitel SA and then asks to leave a voicemail or speak to an Operator. Mitel SA is a service that redirects calls to a user's voicemail or to the Operator and when this

service is used that whole call is dropped. The issue was with REFER, where the “call leg did not exist” when the call was bounced back and forth from Communication Manager to Mitel. Mitel have a workaround in place where they can fall back to tromboning for these types of calls. This workaround is implemented in the registry on the Mitel ACS. This configuration is outlined in **Section 8.4**.

## 2.3. Support

Technical support from Mitel can be obtained through the following.

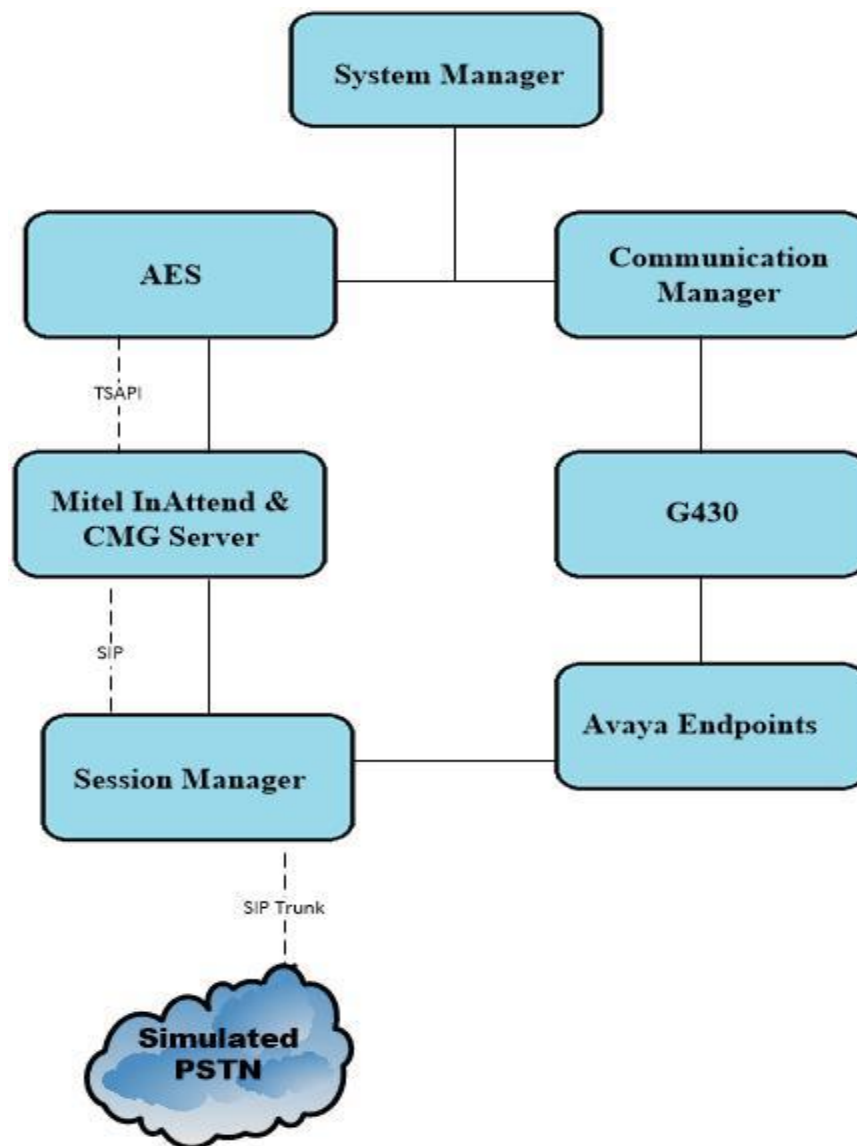
Web: [www.Mitel.com/service-and-support](http://www.Mitel.com/service-and-support)

Tel: +1 800-722-1301

Partners can log on to <https://miaccess.mitel.com/idp/index.xhtml> where access to TeamTrack is given for reporting issues.

### 3. Reference Configuration

**Figure 1** illustrates the network topology used during compliance testing. The Avaya solution consists of a Communication Manager, Session Manager and AES. Mitel InAttend is installed on a Windows Server 2012 OS. A network telephony server and SQL were also installed on the same server. (SQL may also be installed on a separate server). On Communication Manager the routing was configured to route 450x calls to Session Manager which in turn were routed to the ACS. Mitel InAttend was installed and configured on a client PC. H323, SIP and Digital phones were configured on Communication Manager to generate calls to Mitel InAttend and outbound calls to a simulated PSTN. A TSAPI connection was utilized between the Mitel InAttend server and AES.



**Figure 1: Avaya Aura® Communication Manager and Mitel InAttend configuration**

## 4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Avaya Equipment	Software / Firmware Version
Avaya Aura® System Manager	System Manager 8.1.0.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.0.079880
Avaya Aura® Session Manager	Session Manager R8.1 Build No. – 8.1.0.0.810007
Avaya Aura® Communication Manager	R8.1.0.1.0 – SP1 R018x.01.0.890.0 Update ID 01.0.890.0-25393
Avaya Aura® Application Enablement Services	R8.1 8.1.0.0.0.9-1
Avaya Aura® Media Server	8.0.0.169
Avaya Media Gateway G430	38.21.1/1
Avaya 96x1 H323 Deskphone	6.6604
Avaya 96x1 SIP Deskphone	7.1.2.0.14
Avaya J179 H323 Deskphone	6.7.002U
Avaya J129 SIP Deskphone	3.0.0.0.20
Avaya 9408 Digital Deskphone	V2.0
Mitel Equipment	Software / Firmware Version
Mitel Attendant Connectivity server running on Windows 2012 R2	Mitel Attendant Connectivity Server includes: NeTS 5.12.1010.0 MediaServer 1.9.30.0 QueueManager 2.18.604.0
Mitel InAttend server running on Windows 2012 R2	Version 2.6 Mitel InAttend Server includes: CMG 8.5 Virtual Reception 8.5 Microsoft SQL 2012
Mitel InAttend Attendant client running on Windows 10 Enterprise	Version 2.6.605.0

## 5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 11**.

The configuration operations described in this section can be summarized as follows:

- Verify System Parameters and Features
- Configure SIP Trunk
- Configure Call Routing for InAttend
- Configure Connection to AES
- Configure VDNs and Vectors for InAttend

**Note:** The configuration of PSTN trunks and routes are outside the scope of these Application Notes.

### 5.1. Verify System Parameters and Features

Each Communication Manager system will have its own setup with different System Parameters and Features configured depending on the requirement of the customer. Here is a snapshot of some of these values that were configured on the DevConnect lab for compliance testing.

#### 5.1.1. Verify System Parameters Customer Options

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 2**, verify that **Maximum Administered SIP Trunks** has sufficient capacity. Each call answered by InAttend uses a minimum of one SIP trunk. Calls that are routed back to stations on Communication Manager or calls that are routed back to Communication Manager to access the PSTN will use two SIP trunks.

<b>display system-parameters customer-options</b>		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	250
Maximum Concurrently Registered IP Stations:		18000	2
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		414	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		18000	0
Maximum Video Capable IP Softphones:		18000	0
<b>Maximum Administered SIP Trunks:</b>		<b>24000</b>	<b>319</b>
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0



On **Page 3**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

display system-parameters customer-options		Page	3	of	11
OPTIONAL FEATURES					
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y		
Access Security Gateway (ASG)?	n	Authorization Codes?	y		
Analog Trunk Incoming Call ID?	y	CAS Branch?	n		
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n		
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n		
	<b>ARS? y</b>	Computer Telephony Adjunct Links?	y		
	<b>ARS/AAR Partitioning? y</b>	Cvg Of Calls Redirected Off-net?	y		
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y		

On **Page 5**, ensure that **Uniform Dialing Plan** is set to **y**.

display system-parameters customer-options		Page	5	of	11
OPTIONAL FEATURES					
Multinational Locations?	n	Station and Trunk MSP?	y		
Multiple Level Precedence & Preemption?	n	Station as Virtual Extension?	y		
Multiple Locations?	n				
		System Management Data Transfer?	n		
Personal Station Access (PSA)?	y	Tenant Partitioning?	y		
PNC Duplication?	n	Terminal Trans. Init. (TTI)?	y		
Port Network Support?	y	Time of Day Routing?	y		
Posted Messages?	y	TN2501 VAL Maximum Capacity?	y		
		<b>Uniform Dialing Plan?</b>	<b>y</b>		
Private Networking?	y	Usage Allocation Enhancements?	y		

### 5.1.2. Configure System Features

For the testing, **Trunk-to Trunk Transfer** was set to **all** on **Page 1** of the **system-parameters features** page. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction). See **Section 11** for supporting documentation.

```
display system-parameters features                                     Page 1 of 19
                                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
                                Call Park Timeout Interval (minutes): 10
                                Off-Premises Tone Detect Timeout Interval (seconds): 20
                                AAR/ARS Dial Tone Required? y

                                Music (or Silence) on Transferred Trunk Calls? no
                                DID/Tie/ISDN/SIP Intercept Treatment: attd
                                Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                                Automatic Circuit Assurance (ACA) Enabled? n

                                Abbreviated Dial Programming by Assigned Lists? n
                                Auto Abbreviated/Delayed Transition Interval (rings): 2
                                Protocol for Caller ID Analog Terminals: Bellcore
                                Display Calling Number for Room to Room Caller ID Calls? n
```

### 5.2. Configure SIP Trunk

In the **Node Names IP** form, note the IP Address of the processor interface of Communication Manager (**procr**) and the Session Manager (**sm81xvmpg**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

```
display node-names ip
                                IP NODE NAMES
                                Name          IP Address
                                IPOffice      10.10.40.25
                                aes81xvmpg    10.10.40.38
                                ams81vmpg     10.10.40.39
                                default        0.0.0.0
                                g430           10.10.40.15
                                procr          10.10.40.37
                                procr6         ::
                                sm81xvmpg      10.10.40.32
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 6.1.1**. In this configuration, the domain name is **devconnect.local**. The **IP Network Region** form also specifies the **IP Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session manager as **ip-network region 1** is specified in the SIP signaling group.

display ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain: devconnect.local	
Name: Default region		
MEDIA PARAMETERS		
Codec Set: 1	Intra-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	Inter-region IP-IP Direct Audio: yes	
UDP Port Max: 3329	IP Audio Hairpinning? n	
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

In the **IP Codec Set** form, select the audio codec's supported for calls routed over the SIP trunk to InAttend. The form is accessed via the **change ip-codec-set n** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), which is supported by InAttend. Note the **Media Encryption** includes a setting of **none** to allow for unencrypted media.

change ip-codec-set 1		Page 1 of 2
IP MEDIA PARAMETERS		
Codec Set: 1		
Audio	Silence	
Codec	Suppression	
1: G.711A	n	
2: G.711MU	n	
3: G.729A	n	
4:		
Media Encryption		
Encrypted SRTCP: enforce-unenc-srtcp		
1: 1-srtp-aescm128-hmac80		
2: none		
3:		

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form shown below as follows:

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the appropriate setting, in this case it was set to **tls**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Specify the node names for the procr and the Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These values are taken from the **IP Node Names** form shown above.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **sm81xvmpg**).
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured above. This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- **Far-end Domain** was set to the domain used during compliance testing.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- **Initial IP-IP Direct Media** is set to **n**.
- The default values for the other fields may be used.

change signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: sm81xvmpg	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: devconnect.local		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? Y	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from InAttend. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

change trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	<b>Group Type: sip</b>	CDR Reports: y	
<b>Group Name: SIP TRK</b>	COR: 1	TN: 1	<b>TAC: *11</b>
Direction: two-way	Outgoing Display? y	Night Service:	
Dial Access? n			
Queue Length: 0			
<b>Service Type: tie</b>	Auth Code? n		
Member Assignment Method: auto			
Signaling Group: 1			
Number of Members: 10			

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Mitel to prevent unnecessary SIP messages during call setup. Session refresh is used throughout the duration of the call, to check the other side has not gone away, for the compliance test a value of **600** was used.

change trunk-group 1		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 5000			
SCCAN? n	Digital Loss Group: 18		
<b>Preferred Minimum Session Refresh Interval(sec): 600</b>			
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto		Delay Call Setup When Accessed Via IGAR? n	

Settings on **Page 3** can be left as default. However, the **Numbering Format** in the example below is set to **private**.

change trunk-group 1	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n	<b>Numbering Format: private</b>
	UII Treatment: service-provider
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
	Hold/Unhold Notifications? y
	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y	

Settings on **Page 4** are as follows; ensure that the **Telephone Event Payload Type** is set to **101**. Ensure that **Support Request History** is set to **y**.

change trunk-group 1	Page 4 of 21
PROTOCOL VARIATIONS	
	Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
	Send Transferring Party Information? y
	Network Call Redirection? y
Build Refer-To URI of REFER From Contact For NCR? n	
	Send Diversion Header? n
	<b>Support Request History? y</b>
	<b>Telephone Event Payload Type: 101</b>
	Convert 180 to 183 for Early Media? n
	Always Use re-INVITE for Display Updates? n
	Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n	
	Accept Redirect to Blank User Destination? n
	Enable Q-SIP? n
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	

## 5.3. Configure Call Routing for InAttend

For compliance testing all calls beginning with 450 with a total length of 4 digits were to be sent across the SIP trunk to Session Manager and on to InAttend. To achieve this, automatic alternate routing (aar) would be used to route the calls.

### 5.3.1. Administer Dial Plan

It was decided for compliance testing that all calls beginning with 4 with a total length of 4 digits were to be sent across the SIP trunk to Session Manager. Type **change dialplan analysis**, to make changes to the dial plan. Ensure that **4** is added with a **Total Length** of **4** and a **Call Type** of **udp**.

change dialplan analysis						Page 1 of 12			
DIAL PLAN ANALYSIS TABLE									
Location: all						Percent Full: 2			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
1	4	ext							
2	4	ext							
3	4	udp							
4	4	udp							
8	1	fac							
9	1	fac							
*	3	fac							

### 5.3.2. Administer Route Selection for InAttend Calls

As digits **4xxx** were defined in the dial plan as udp (**Section 5.3.1**), use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to numbers beginning with **450** that are **4** digits in length will be matched. No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

change uniform-dialplan 4							Page 1 of 2		
UNIFORM DIAL PLAN TABLE									
							Percent Full: 0		
Matching				Insert					Node
Pattern	Len	Del		Digits	Net	Conv			Num
450	4	0			aar	n			
						n			

Use the **change aar analysis x** command to further configure the routing of the dialed digits. Calls to InAttend begin with **450** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 1**, which contains the outbound SIP Trunk Group.

<b>change aar analysis 4</b>							Page	1 of	2
AAR DIGIT ANALYSIS TABLE									
Location: all							Percent Full: 1		
Dialed	Total		<b>Route</b>	Call	Node	ANI			
String	Min	Max	<b>Pattern</b>	Type	Num	Reqd			
<b>450</b>	4	4	<b>1</b>	unku		n			

Use the **change route-pattern n** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, **Route Pattern Number 1** is used to route calls to trunk group (**Grp No**) **1**. This is the SIP Trunk configured in **Section 5.2**.

change route-pattern 1										Page	1 of	4
Pattern Number: 1    Pattern Name: SIPTRK												
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:	1	0								n	user	
2:								n	user			
3:								n	user			
4:								n	user			
5:								n	user			
	BCC	VALUE	TSC	CA-TSC	ITC BCIE			Service/Feature	PARM	No.	Numbering	LAR
	0	1	2	M	4	W	Request			Dgts	Format	
1:	y	y	y	y	y	n	n	unre			lev0-pvt	none
2:	y	y	y	y	y	n	n	rest				none
3:	y	y	y	y	y	n	n	rest				none
4:	y	y	y	y	y	n	n	rest				none
5:	y	y	y	y	y	n	n	rest				none
6:	y	y	y	y	y	n	n	rest				none



## 5.4. Configure Connection to Avaya Aura® Application Enablement Services

It is assumed that a connection to AES is already in place and that the TSAPI connection and switch connection between Communication Manager and AES is fully working. The following section outlines the connection that was setup for compliance testing.

### 5.4.1. Note procr IP Address for Avaya Aura® Application Enablement Services Connectivity

Display the procr IP address by using the command **display node-names ip** and noting the IP address for the **procr** and AES (**aes81xvmpg**).

<b>display node-names ip</b>		IP NODE NAMES
Name	IP Address	
IPOffice	10.10.40.25	
<b>aes81xvmpg</b>	<b>10.10.40.38</b>	
ams81vmpg	10.10.40.39	
default	0.0.0.0	
g430	10.10.40.15	
<b>procr</b>	<b>10.10.40.37</b>	
procr6	::	
sm81xvmpg	10.10.40.32	
( 8 of 8 administered node-names were displayed )		
Use 'list node-names' command to see all the administered node-names		
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name		

### 5.4.2. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES, use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** Should be set to **AESVCS**
- **Enabled:** Set to **y**
- **Local Node:** Set to the node name assigned for the procr in **Section 5.4.1**
- **Local Port:** Retain the default value of **8765**

change ip-services					Page	1 of 3
IP SERVICES						
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	
AESVCS	y	procr	8765			

Go to **Page 3** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aes81xvmpg**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

**Note:** The password entered for **Password** field must match the password on the AES server in **Section 7.2**. The **AE Services Server** must match the administered name for the AES server; this is created as part of the AES installation, and can be obtained from the AES server by typing **uname -n** at the Linux command prompt.

change ip-services					Page	3 of	3
AE Services Administration							
Server ID	AE Services Server	Password	Enabled	Status			
1:	aes81xvmpg	*****	y	idle			
2:							
3:							

### 5.4.3. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command, where n is the n is the cti-link number as shown in the example below this is **1**. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1					Page	1 of	3
CTI LINK							
CTI Link: 1							
Extension: 1990							
Type: ADJ-IP							
Name: aes81xvmpg					COR: 1		

## 5.5. Configure VDNs and Vectors for InAttend

There are two VDNs and two Vectors that need to be added to allow InAttend set the status of a user on Communication Manager using TSAPI. VDN one calls on Vector one which collects digits into VDN two which is monitored by InAttend as per **Section 8.5**.

### 5.5.1. Adding VDNs

There are two VDNs that are added one to collect digits and one to monitor the collected digits. Use the command **add vdn x**, where x is the vdn to be added. Each VDN uses a Vector which are outlined in **Section 5.5.2**.

```
add vdn 1082                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER
      Extension: 1082                               Unicode Name? n
      Name*: Diversion CMG
      Destination: Vector Number                22
      Attendant Vectoring? n
      Meet-me Conferencing? n
      Allow VDN Override? n
      COR: 1
      TN*: 1
      Measured: none      Report Adjunct Calls as ACD*? n

      VDN of Origin Annc. Extension*:
      1st Skill*:
      2nd Skill*:
      3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

Same command is used to **add VDN 1084** and this will use Vector **21**. This VDN is then referenced in **Section 8.5**.

```
add vdn 1084                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER
      Extension: 1084                               Unicode Name? n
      Name*: Hangup
      Destination: Vector Number                21
      Attendant Vectoring? n
      Meet-me Conferencing? n
      Allow VDN Override? n
      COR: 1
      TN*: 1
      Measured: none      Report Adjunct Calls as ACD*? n

      VDN of Origin Annc. Extension*:
      1st Skill*:
      2nd Skill*:
      3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

## 5.5.2. Adding Vectors

VDN 1082 on the previous page uses this **Vector 22** to collect up to **8 digits** and then routes the call to the other VDN 1084 configured again on the previous page in **Section 5.5.1**.

```
change vector 22                                     Page 1 of 6
                                                    CALL VECTOR

  Number: 22                      Name: Diversion CMG
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
  Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
  Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
  Variables? y      3.0 Enhanced? y
01 wait-time      0      secs hearing ringback
02 collect      8      digits after announcement none      for none
03 wait-time      2      secs hearing ringback
04 route-to      number 1084                        cov n if unconditionally
05
06
07
08
09
10
```

VDN 1084 uses the following Vector which simply provides **ringback** to the user while the VDN is being monitored.

```
change vector 21                                     Page 1 of 6
                                                    CALL VECTOR

  Number: 21                      Name: Diversion 2
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
  Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
  Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
  Variables? y      3.0 Enhanced? y
01 wait-time      60      secs hearing ringback
02 stop
03
04
05
06
07
08
09
10
```

## 6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager to add the SIP Entity and routing to allow calls route to and from Mitel InAttend. Session Manager is configured via System Manager. The procedures include the following areas:

- Domains and Locations
- Configure SIP Entity
- Configure Entity Link
- Configure Routing Policy
- Configure Dial Pattern

To make changes on Session Manager a web session is established to System Manager. Log into System Manager by opening a web browser and navigating to <https://<System Manager FQDN>/SMGR>. Enter the appropriate credentials for the **User ID** and **Password** and click on **Log On**.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:

**Supported Browsers:** Internet Explorer 11.x or Firefox 59.0, 60.0 or 61.0.

Once logged in navigate to **Elements** and click on **Routing** highlighted below.

**AVAYA** Aura® System Manager 8.0

Users | **Elements** | Services | Widgets | Shortcuts | Search | admin

**System Resource Utilization**

Avaya Breeze®

Communication Manager

Communication Server 1000

Conferencing

Device Adapter

Device Services

Media Server

Meeting Exchange

Messaging

Presence

Session Manager

Web Gateway

**Alarms**

Critical Major Indeterminate Minor Warning

**Application State**

License Status: Active

Deployment Type: VMware

Multi-Tenancy: DISABLED

OCBM State: DISABLED

Hardening Mode: Standard

**Information**

Elements	Count	Sync Status
CM	1	■
Session Manager	1	■
System Manager	1	■
UCM Applications	8	■

Current Usage:

11/250000 USERS

1/50 SIMULTANEOUS ADMINISTRATIVE LOGINS

**Notifications**

No data

**Shortcuts**

Drag shortcuts here

Administrative...

Management Instance check failed: [The following SM instance(s) failed the instance test: 10.10.40.57]

SM/BSM host name resolution failed: [The following SM/BSM failed the Host Name Resolution test: 10.10.40.57]

## 6.1. Domains and Locations

**Note:** It is assumed that a domain and a location have already been configured, therefore a quick overview of the domain and location that was used in compliance testing is provided here.

### 6.1.1. Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **devconnect.local** as shown below. If a domain is not already in place, click on **New**. This will open a new window (not shown) where the domain can be added.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar has a 'Routing' section with 'Domains' selected. The main panel is titled 'Domain Management' and shows a table with one item: 'devconnect.local' of type 'sip'. The table has columns for Name, Type, and Notes. The 'Name' column contains 'devconnect.local', the 'Type' column contains 'sip', and the 'Notes' column contains 'devconnect.local'. Above the table are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. Below the table is a 'Select : All, None' option.

Name	Type	Notes
devconnect.local	sip	devconnect.local

### 6.1.2. Display the Location

Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectLab\_PG** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click on **New** to add a new location.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar has a 'Routing' section with 'Locations' selected. The main panel is titled 'Location' and shows a table with one item: 'DevConnectLab\_PG'. The table has columns for Name, Correlation, and Notes. The 'Name' column contains 'DevConnectLab\_PG', the 'Correlation' column contains a small icon, and the 'Notes' column contains 'DevConnectLab\_PG'. Above the table are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. Below the table is a 'Select : All, None' option.

Name	Correlation	Notes
DevConnectLab_PG		DevConnectLab_PG

## 6.2. Configure Mitel InAttend SIP Entity

The ACS (also referred to as InAttend) is added on Session Manager as a SIP Entity with an Entity Link, every SIP endpoint that communicated over a SIP trunk would be added as such. Click on **SIP Entities** in the left column and select **New** in the right window.

Name	FQDN or IP Address	Type	Notes
AA Messaging V7	10.10.40.23	SIP Trunk	AA Messaging V7
CM71vmppg	10.10.40.47	CM	CM71vmppg
CM80vmppg	10.10.40.59	CM	CM80vmppg
CS1KPG1	10.10.40.111	SIP Trunk	CS1000 (CS1KPG1)
EP72vmppg	10.10.40.63	Voice Portal	EP72vmppg
EP_Oceana	10.10.41.16	Voice Portal	EP_Oceana
SM80vmppg	10.10.40.58	Session Manager	SM80vmppg
StephensCM	10.10.16.23	CM	StephensCM
StevesEP	10.10.16.20	Voice Portal	StevesEP

Enter a suitable **Name** for the new SIP Entity and the **IP Address** of the ACS. Enter the correct **Time Zone** and **Location** and scroll down to SIP Entity Links.

### SIP Entity Details

**General**

\* Name: InAttend

\* FQDN or IP Address: 10.10.40.122

Type: SIP Trunk

Notes: In Attend V2.6

Adaptation:

Location: DevConnectLab

Time Zone: Europe/Dublin

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable:

Call Detail Recording: egress

**Loop Detection**

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

### 6.3. Configure Mitel InAttend SIP Entity Link

An Entity link can be added from the SIP Entities page. Using the page from the previous page scroll down to Entity Links.

Upon scrolling down to **Entity Links** click on **Add**.

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

**Entity Links**

Override Port & Transport with DNS SRV: ☐

**Add** **Remove**

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
Select : All, None								

**SIP Responses to an OPTIONS Request**

**Add** **Remove**

0 Items Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

Enter a suitable **Name** for the Entity Link and select the **Session Manager** SIP Entity for **SIP Entity 1** and the newly created InAttend SIP Entity for **SIP Entity 2**. Ensure that **TCP** is selected for the **Protocol** and that **Port 5060** is used. Click on **Commit** once finished to save the new Entity Link.

**Entity Links**

Override Port & Transport with DNS SRV: ☐

**Add** **Remove**

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* SM81vmppg_InAttend_50	SM81vmppg	TCP	* 5060	InAttend	* 5060	trusted	<input type="checkbox"/>

Select : All, None

**SIP Responses to an OPTIONS Request**

**Add** **Remove**

0 Items Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

**Commit** **Cancel**



## 6.4. Configure Routing Policy for Mitel InAttend

Click on **Routing Policies** in the left window and select **New** in the main window.

<input type="checkbox"/>	Name	Disabled	Retries	Destination	Notes
<input type="checkbox"/>	<a href="#">To AA Messaging V7</a>	<input type="checkbox"/>	0	AA Messaging V7	To AA Messaging V7
<input type="checkbox"/>	<a href="#">To ASCBE</a>	<input type="checkbox"/>	0	ASBCE8vmppg	To Session Border Controller
<input type="checkbox"/>	<a href="#">To Capita DMS</a>	<input type="checkbox"/>	0	Capita DMS	To Capita DMS
<input type="checkbox"/>	<a href="#">To Capita DS3000</a>	<input type="checkbox"/>	0	Capita DS3000	To Capita DS3000
<input type="checkbox"/>	<a href="#">To CM71vmppg</a>	<input type="checkbox"/>	0	CM71vmppg	To CM71vmppg
<input type="checkbox"/>	<a href="#">To CM80vmppg</a>	<input type="checkbox"/>	0	CM80vmppg	To CM80vmppg
<input type="checkbox"/>	<a href="#">To CS1KPG1</a>	<input type="checkbox"/>	0	CS1KPG1	To CS1KPG1
<input type="checkbox"/>	<a href="#">To EP72vmppg</a>	<input type="checkbox"/>	0	EP72vmppg	To EP72vmppg
<input type="checkbox"/>	<a href="#">To EP_Oceana</a>	<input type="checkbox"/>	0	EP_Oceana	To EP Oceana
<input type="checkbox"/>	<a href="#">To Stephens CM</a>	<input type="checkbox"/>	0	StephensCM	To Stephens CM
<input type="checkbox"/>	<a href="#">To Steves EP</a>	<input type="checkbox"/>	0	StevesEP	To Steves EP

Select : All, None

Enter a suitable **Name** for the Routing Policy and click on **Select** under **SIP Entity as Destination**, highlighted on next page.

### Routing Policy Details

**General**

\* **Name:**

**Disabled:** ☐

\* **Retries:**

**Notes:**

**SIP Entity as Destination**

Name	FQDN or IP Address	Type

Select the **InAttend** SIP Entity as shown below and click on **Select**.

**SIP Entities** Select Cancel

**SIP Entities**

17 Items Filter: Enable

Name	FQDN or IP Address	Type	Notes
<input type="radio"/> AAMessaging	10.10.40.23	Messaging	
<input type="radio"/> applanx	10.10.40.121	SIP Trunk	applanx Gateway
<input type="radio"/> breeze1oc-sm100	10.10.40.161	Avaya Breeze	breeze1oc-sm100
<input type="radio"/> breeze2oc-sm100	10.10.40.162	Avaya Breeze	breeze2oc-sm100
<input type="radio"/> breeze3oc-sm100	10.10.40.163	Avaya Breeze	breeze3oc-sm100
<input type="radio"/> breeze4oc-sm100	10.10.40.164	Avaya Breeze	breeze4oc-sm100
<input type="radio"/> breeze5oc-sm100	10.10.40.165	Avaya Breeze	breeze5oc-sm100
<input type="radio"/> breeze6oc-sm100	10.10.40.166	Avaya Breeze	breeze6oc-sm100
<input type="radio"/> cm80vmpg	10.10.40.59	CM	cm80vmpg
<input type="radio"/> cm81Large	10.10.40.34	CM	
<input type="radio"/> cm81vmpg - Oceana36TRUNK	10.10.40.37	CM	Used for Oceana 3.6
<input type="radio"/> cm81vmpg - SIP PHONES	10.10.40.37	CM	Used for SIP Phones on CM
<input type="radio"/> cm81vmpg - TRUNK	10.10.40.37	CM	For Trunk calls to CM
<input type="radio"/> EP722	10.10.40.31	Voice Portal	EP722 and POM
<input checked="" type="radio"/> InAttend	10.10.40.122	SIP Trunk	In Attend V2.6

Select : None Page 1 of 2

Select Cancel

The selected destination is now shown, click on **Commit** to save this.

**Routing Policy Details** Commit Cancel

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
InAttend	10.10.40.122	SIP Trunk	In Attend V2.6

## 6.5. Configure Mitel InAttend Dial Pattern

Select **Dial Patterns** in the left window and select **New** in the main window.

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
09173	9	9	<input type="checkbox"/>			-ALL-	To CM80vmpg from Syntec
2	4	4	<input type="checkbox"/>			devconnect.local	To CM80vmpg
280	4	4	<input type="checkbox"/>			devconnect.local	To EP72vmpg
290	4	4	<input type="checkbox"/>			devconnect.local	To EP Oceana
30	4	4	<input type="checkbox"/>			devconnect.local	To CS1KPG1
351212455779	12	12	<input type="checkbox"/>			-ALL-	To SBC8 for Syntec
380	4	4	<input type="checkbox"/>			devconnect.local	To Steves EP
4	4	4	<input type="checkbox"/>			devconnect.local	To CM71vmpg
52	4	4	<input type="checkbox"/>			devconnect.local	To CM80vmpg for simulated PSTN to IPO
6666	4	4	<input type="checkbox"/>			devconnect.local	To AA Messaging V7
7080	4	6	<input type="checkbox"/>			devconnect.local	To Capita DMS
8000	5	5	<input type="checkbox"/>			devconnect.local	To Capita DS3000
823	7	7	<input type="checkbox"/>			devconnect.local	To Stephens CM 823 000x

Enter the required digits for the Routing Pattern, in the example below **450** is used. This ensures that when 450x is dialled it will route to the InAttend server. Enter the appropriate domain for **SIP Domain** in this example the domain created in **Section 6.1.1** is added. Click on **Add** under **Originating Locations and Routing Policies** to select this Routing Policy.

**Dial Pattern Details** [Commit] [Cancel]

**General**

\* Pattern: 450

\* Min: 4

\* Max: 4

Emergency Call: ☐

SIP Domain: devconnect.local ▼

Notes: To InAttend

**Originating Locations and Routing Policies**

[Add] [Remove]

1 Item

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled

Select : All, None

Select the **Originating Location**, this will be the location added in **Section 6.1.2** select the newly created Routing Policy for InAttend.

Originating Location

Select Cancel

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

1 Item

<input checked="" type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	DevConnectLab	DevConnect Lab in Galway

Select : All, None

Routing Policies

8 Items

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To AA Messaging V7	<input type="checkbox"/>	AAMessaging	To AA Messaging V7
<input type="checkbox"/>	To Applianx	<input type="checkbox"/>	applianx	To Applianx Gateway
<input type="checkbox"/>	To CM80vmppg	<input type="checkbox"/>	cm80vmppg	To CM80vmppg
<input type="checkbox"/>	To cm81xvmppg	<input type="checkbox"/>	cm81vmppg - TRUNK	To cm81xvmppg
<input type="checkbox"/>	To EP722	<input type="checkbox"/>	EP722	To EP722
<input checked="" type="checkbox"/>	To InAttend	<input type="checkbox"/>	InAttend	To InAttend
<input type="checkbox"/>	To IP Office	<input type="checkbox"/>	IP Office	To IP Office
<input type="checkbox"/>	To Talkbase	<input type="checkbox"/>	TalkbaseServer	To Talkbase

Select : All, None

Select Cancel

With the Routing Policy selected click on **Commit** to finish adding the Dial Pattern.

Dial Pattern Details

Commit Cancel

General

\* Pattern: 450

\* Min: 4

\* Max: 4

Emergency Call: ☐

SIP Domain: devconnect.local

Notes: To InAttend

Originating Locations and Routing Policies

Add Remove

1 Item

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	DevConnectLab	DevConnect Lab in Galway	To InAttend	0	<input type="checkbox"/>	InAttend	To InAttend

Select : All, None

## 7. Configure Avaya Aura® Application Enablement Services

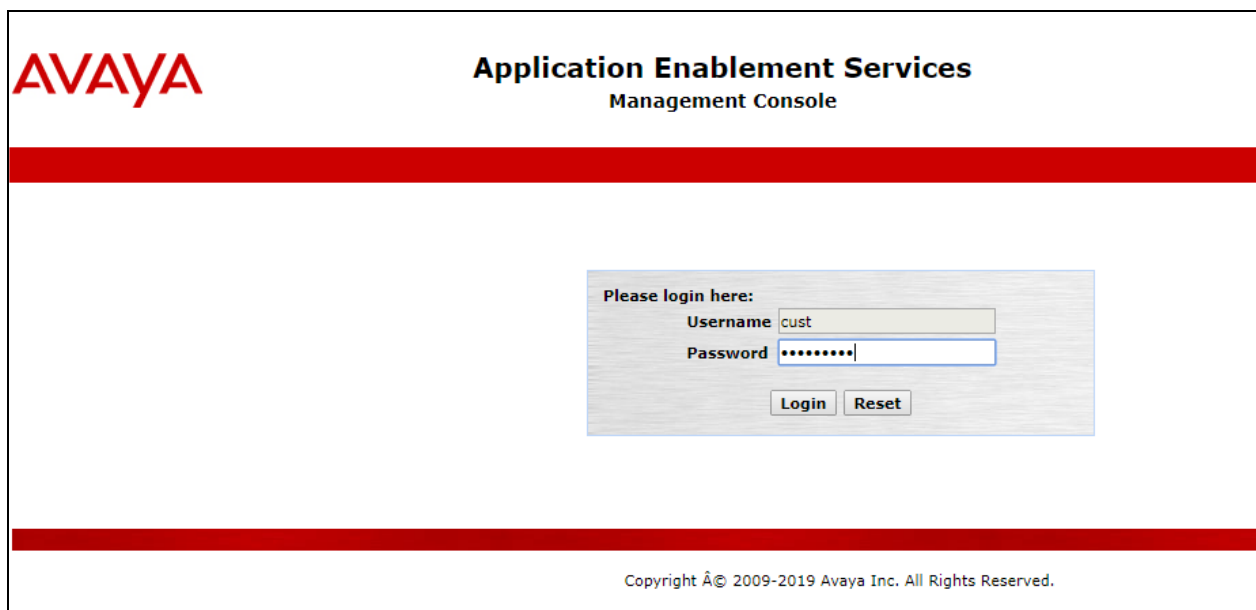
This section provides the procedures for configuring Application Enablement Services (AES).

The procedures fall into the following areas:

- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Identify Tlinks
- Enable TSAPI Ports
- Create CTI User
- Associate Devices with CTI User

### 7.1. Verify Licensing

To access the AES Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of the AES. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page below the header. In the center of the page is a login box with a light gray background. Inside this box, the text "Please login here:" is at the top. Below it are two input fields: "Username" with the value "cust" and "Password" with a masked value of "\*\*\*\*\*". At the bottom of the login box are two buttons: "Login" and "Reset". Another thick red horizontal bar is located below the login box. At the very bottom of the page, centered, is the copyright notice: "Copyright © 2009-2019 Avaya Inc. All Rights Reserved."

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license.

**AE Services** Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▶ TSAPI
- ▶ TWS
- ▶ **Communication Manager Interface**
  - ▶ High Availability
  - ▶ Licensing
  - ▶ Maintenance
  - ▶ Networking
  - ▶ Security
  - ▶ Status
  - ▶ User Management
  - ▶ Utilities
  - ▶ Help

**AE Services**

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
AE Services HA	Not Configured	N/A	N/A	N/A

For status on actual services, please use [Status and Control](#)

\* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

**License Information**  
You are licensed to run Application Enablement (CTI) release 8.x

## 7.2. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter a name for the Switch Connection to be added and click the **Add Connection** button.

**Communication Manager Interface | Switch Connections**

▶ AE Services

▼ **Communication Manager Interface**

- ▶ **Switch Connections**
- ▶ Dial Plan
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

**Switch Connections**

Connection Name	Processor Ethernet	Msg Period
<input type="button" value="Edit Connection"/>	<input type="button" value="Edit PE/CLAN IPs"/>	<input type="button" value="Edit H.323 Gatekeeper"/>
<input type="button" value="Delete Connection"/>	<input type="button" value="Survivability Hierarchy"/>	

In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.4.2**. The remaining fields should show as below. Click **Apply** to save changes.

**Connection Details - cm81xvmpg**

Switch Password

Confirm Switch Password

Msg Period  Minutes (1 - 72)

Provide AE Services certificate to switch ☐

Secure H323 Connection ☒

Processor Ethernet ☒

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button.

**Switch Connections**

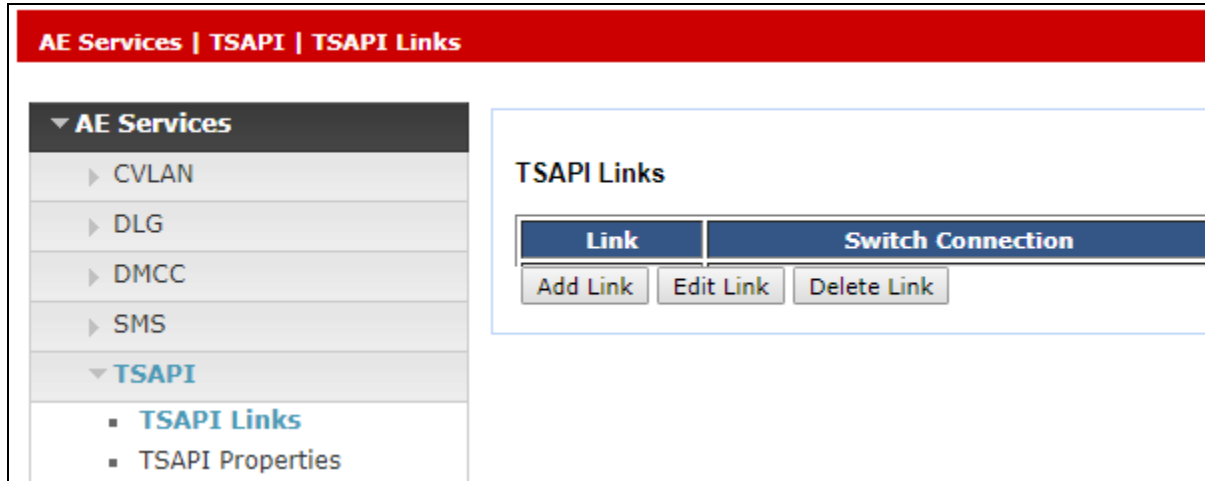
Connection Name	Processor Ethernet	Msg Period	
<input checked="" type="radio"/> cm81xvmpg	Yes	30	1

In the resulting screen, enter the IP address of the procr as shown in **Section 5.4.1** that will be used for the AES connection and select the **Add/Edit Name or IP** button.

**Edit Processor Ethernet IP - cm81xvmpg**

### 7.3. Administer TSAPI link

From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm81xvmpg**, which has already been configured in **Section 7.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4.3** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **8**.
- **Security:** This should be set to **Both** allowing both secure and nonsecure connections.

Once completed, select **Apply Changes**.


The screenshot shows the 'Edit TSAPI Links' configuration form. It contains the following fields and values:

Field	Value
Link	1
Switch Connection	cm81xvmpg
Switch CTI Link Number	1
ASAI Link Version	8
Security	Both

At the bottom of the form are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.




Another screen appears for confirmation of the changes made. Choose **Apply**.

**Apply Changes to Link**  
Warning! Are you sure you want to apply the changes?  
These changes can only take effect when the TSAPI server restarts.  
 **Please use the Maintenance -> Service Controller page to restart the TSAPI server.**

When the TSAPI Link is completed, it should resemble the screen below.

TSAPI Links				
Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	cm81xvmpg	1	8	Both
<input type="button" value="Add Link"/> <input type="button" value="Edit Link"/> <input type="button" value="Delete Link"/>				

The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance** → **Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.



**Application Enablement Services**  
Management Console

**Maintenance | Service Controller**

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

**Service Controller**

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

**Service Controller**

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

## 7.4. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure InAttend in **Section 8.5**.

The screenshot shows the 'Security | Security Database | Tlinks' page. On the left is a navigation menu with categories: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, and Security. The Security category is expanded, showing sub-items: Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database, and a list of items under Security Database: Control, CTI Users, Devices, Device Groups, Tlinks (highlighted in blue), Tlink Groups, and Worktops. The main content area on the right is titled 'Tlinks' and contains two radio button options for 'Tlink Name': 'AVAYA#CM81XVMGP#CSTA#AES81XVMGP' and 'AVAYA#CM81XVMGP#CSTA-S#AES81XVMGP'. Below these options is a 'Delete Tlink' button.

**Security | Security Database | Tlinks**

**Tlinks**

Tlink Name

☐ AVAYA#CM81XVMGP#CSTA#AES81XVMGP

☐ AVAYA#CM81XVMGP#CSTA-S#AES81XVMGP

Delete Tlink

## 7.5. Enable TSAPI Ports

To ensure that TSAPI ports are enabled, navigate to **Networking** → **Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below.

Networking   Ports				
<b>Ports</b>				
CVLAN Ports				Enabled Disabled
	Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
	Encrypted TCP Port	<input type="text" value="9998"/>	<input checked="" type="radio"/>	<input type="radio"/>
DLG Port	TCP Port	5678		
TSAPI Ports				Enabled Disabled
	TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	<input type="text" value="1050"/>		
	TCP Port Max	<input type="text" value="1065"/>		
	Encrypted TLINK Ports			
	TCP Port Min	<input type="text" value="1066"/>		
	TCP Port Max	<input type="text" value="1081"/>		
DMCC Server Ports				Enabled Disabled
	Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/>	<input type="radio"/>
	Encrypted Port	<input type="text" value="4722"/>	<input checked="" type="radio"/>	<input type="radio"/>
	TR/87 Port	<input type="text" value="4723"/>	<input checked="" type="radio"/>	<input type="radio"/>
H.323 Ports				
	TCP Port Min	<input type="text" value="20000"/>		
	TCP Port Max	<input type="text" value="29999"/>		
	Local UDP Port Min	<input type="text" value="20000"/>		
	Local UDP Port Max	<input type="text" value="29999"/>		
	Server Media		<input checked="" type="radio"/>	<input type="radio"/>

## 7.6. Create CTI User

A user ID and password needs to be configured for InAttend to communicate with the Application Enablement Services server. Navigate to the **User Management → User Admin** screen then choose the **Add User** option.

In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by InAttend setup in **Section 8.5**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with InAttend setup in **Section 8.5**.
- **CT User** - Select **Yes** from the drop-down menu.

Click on **Apply Changes** at the bottom of the screen (not shown).

Edit User	
* User Id	mitel
* Common Name	mitel
* Surname	mitel
User Password	••••••••
Confirm Password	••••••••
Admin Note	Mitel AES User
Avaya Role	None ▼
Business Category	
Car License	
CM Home	
Csx Home	
CT User	Yes ▼
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	

## 7.7. Associate Devices with CTI User

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the CTI user added in **Section 7.6** and click on **Edit**.

<div>AE Services</div> <div>Communication Manager Interface</div> <div>High Availability</div> <div>Licensing</div> <div>Maintenance</div> <div>Networking</div> <div>Security</div> <div>Account Management</div> <div>Audit</div> <div>Certificate Management</div> <div>Enterprise Directory</div> <div>Host AA</div> <div>PAM</div> <div>Security Database</div> <div>Control</div> <div>CTI Users</div> <div>List All Users</div>	CTI Users			
	User ID	Common Name	Worktop Name	Device ID
	<input type="radio"/> Enghouse	Enghouse	NONE	NONE
	<input type="radio"/> inisoft	inisoft	NONE	NONE
	<input checked="" type="radio"/> mitel	mitel	NONE	NONE
	<input type="radio"/> Oceana	Oceana	NONE	NONE
	<input type="radio"/> paul	Paul	NONE	NONE
	<input type="radio"/> paul1	paul1	NONE	NONE
	<div>Edit</div> <div>List All</div>			

In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.

Edit CTI User

User Profile:

User ID

Common Name

Worktop Name

Unrestricted Access

mitel

mitel

NONE ▼

☒

Call and Device Control:

Call Origination/Termination and Device Status

None ▼

Call and Device Monitoring:

Device Monitoring

Calls On A Device Monitoring

Call Monitoring

None ▼

None ▼

☐

Routing Control:

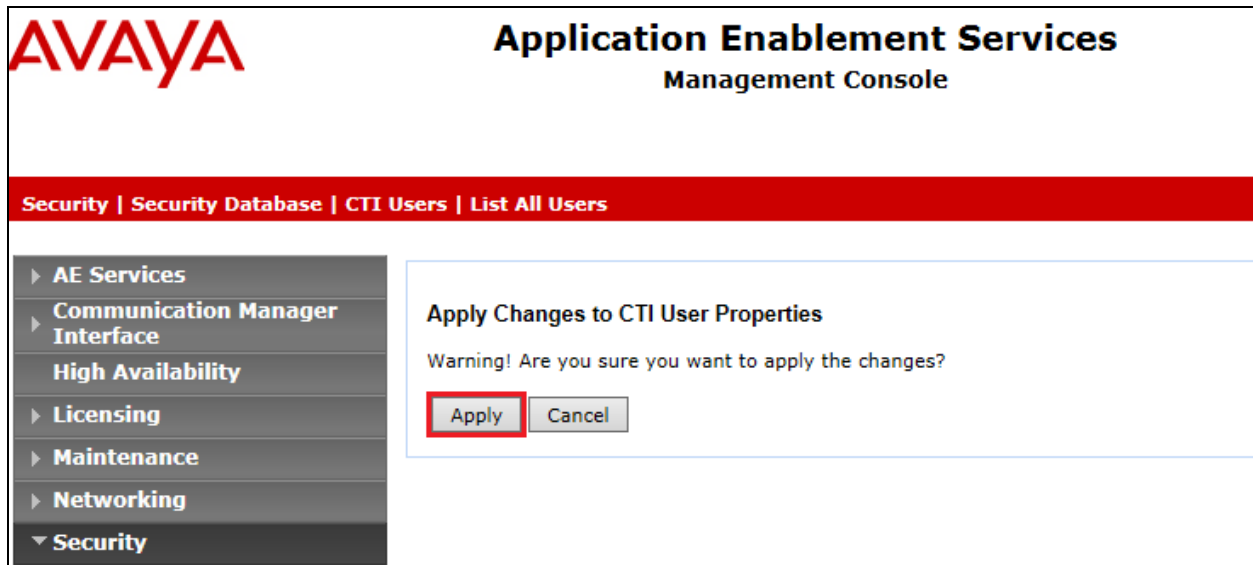
Allow Routing on Listed Devices

None ▼

Apply Changes

Cancel Changes

Click on **Apply** when asked again to apply changes.

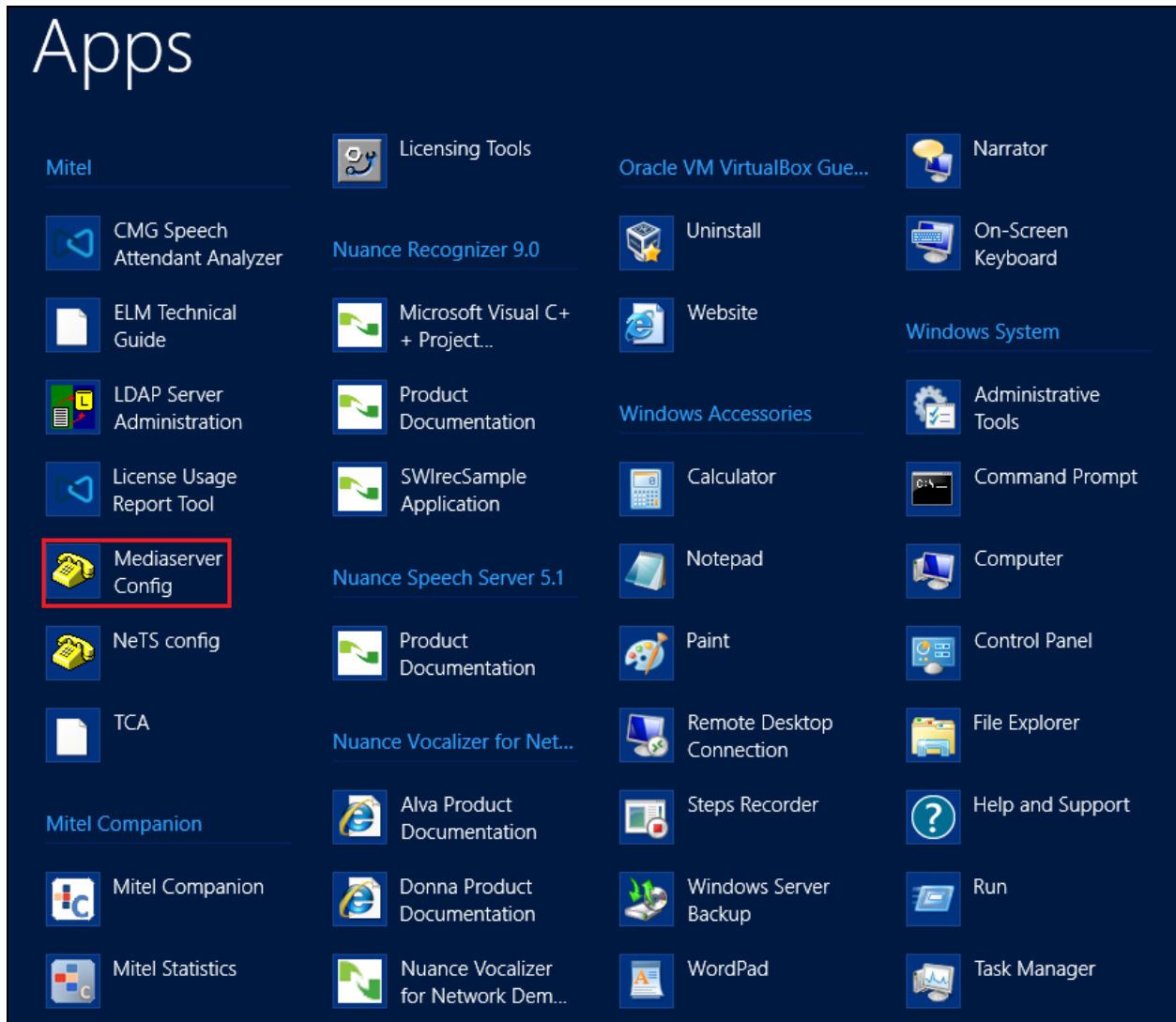


## 8. Configure Mitel Attendant Connectivity Server (ACS)

Although a Mitel engineer will setup the solution the following sections show information on the connection to Session Manager that was used for compliance testing, it may prove useful.

### 8.1. Mitel Media Server configuration

All Mitel applications are run from the Windows 2012 server, click on the **Mediaserver Config** as shown below.



These are the settings that were used for compliance testing. Take note of the **Codec Preference** as this is where they are set. Typically, these are the default settings.

**MediaServer Configuration v1.8.7.2**

**MediaServer Properties**

SIP port: 5065

Dialog TTL: 10 min

RTP port range: 40000-50000

☐ RTCP

MOH File: C:\Program Files (x86)\Mitel\MediaServer\ringing.wav

☒ Trim recordings

Codec Preference: pcmu,pcma,g722,g729,rfc2833,cn

☒ Forward DTMF to conference

Audio Files Prefix: C:\Program Files (x86)\Mitel\MediaServer\Prompts\

☐ SRTCP SDP Offer

☒ SRTCP Best Effort

Default Recording Rate: 16 kHz

**MediaServer Logs**

Log Path: C:\Program Files (x86)\Mitel\MediaServer\Logs

Log Level: Debug+3

Max size: 0 MB

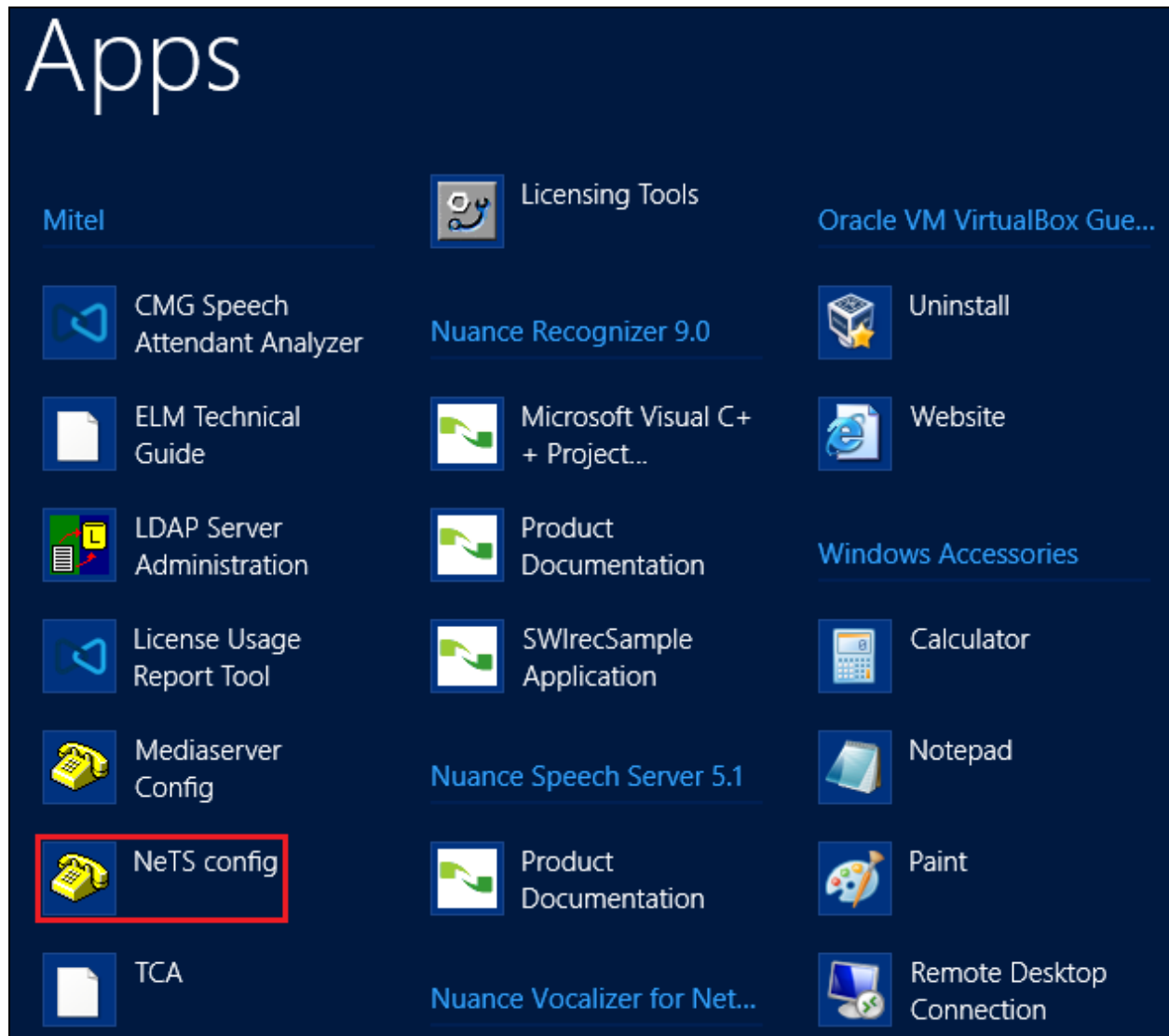
Discard after: 10 days

OK Apply Cancel



## 8.2. Mitel NeTS configuration

Click on the **NeTS config** as shown below.



These are the settings that were used for compliance testing. The only settings that are of interest to the connection to Session Manager are found under the **SIP** tab and **Local settings**. Typically, these are the default settings.

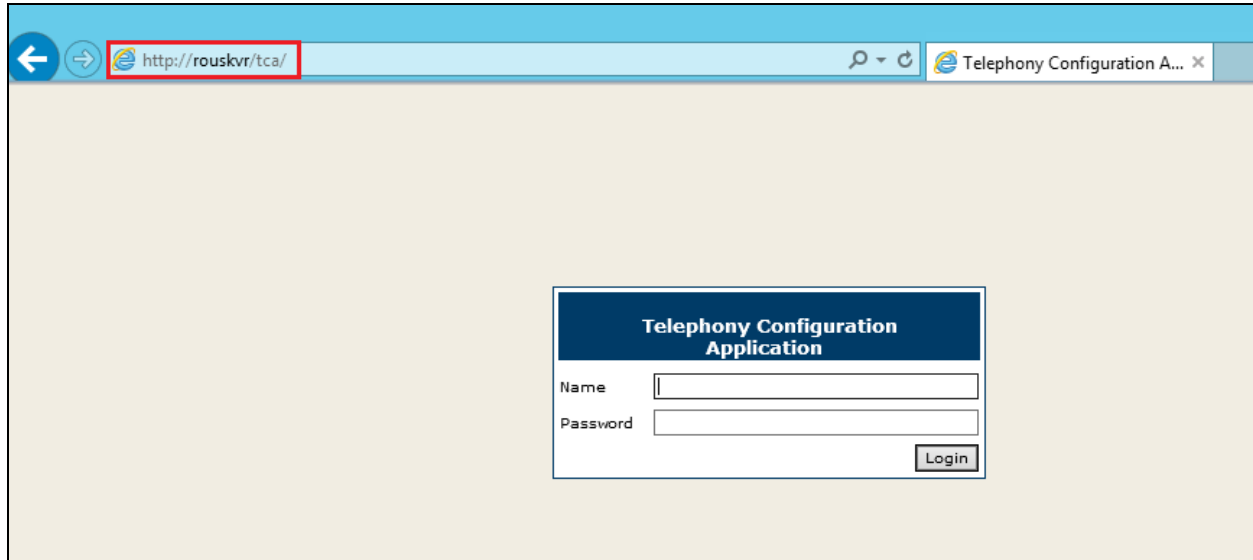
The screenshot shows the 'Network Telephony Services configuration' dialog box with the 'SIP' tab selected. The 'Local settings' section is highlighted in the left sidebar. The main area contains the following settings:

- ☒ Use SIP
- NeTS local SIP port for media control: ROUSKVR:5067
- Outbound proxy: (empty field)
- ☒ Use local IP in "From" header
- ☒ Use local IP in "Contact" header
- ☒ Follow redirects
- ☒ Use OPTIONS as to check if calls are valid
- ☒ Allow REGISTER requests
- ☐ Media-SDP in 180 Ringing
- ☒ Transfer A to B
- ☐ Hold before transfer
- ☐ Allow numbers with leading + (E.164)
- ☐ Load balance Media Servers
- PRACK support: Supported (dropdown)
- Option to check if SIP trunks are up. (s): 90 (spinner)
- Served-by-NeTS Header: P-Served-User (text field)
- Max wait for 100 Trying on Outbound calls. (ms): 1200 (spinner)

At the bottom are buttons for OK, Cancel, and Apply.

### 8.3. Mitel Telephony Configuration Application (TCA) configuration

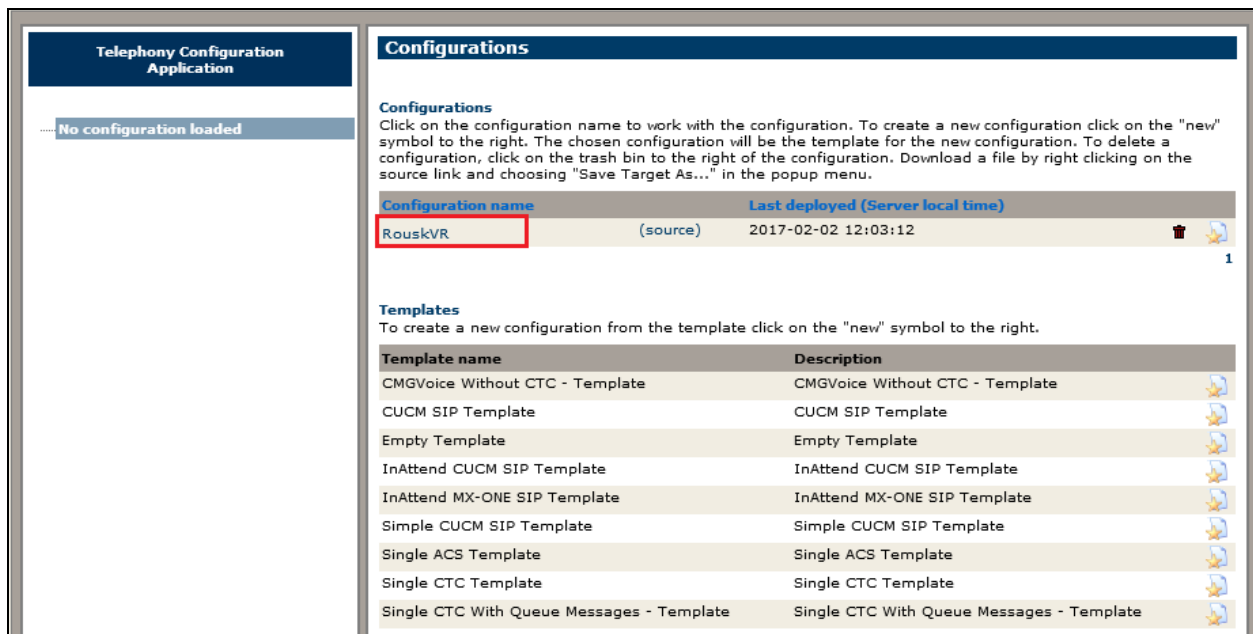
Open a web browser and browse to the ACS server name followed by TCA, for example `http://<servername>/tca`. Enter the appropriate credentials and click on **Login**.



The screenshot shows a web browser window with the address bar containing `http://rouskvr/tca/`. The page title is "Telephony Configuration Application". The main content area displays a login form with the following fields and buttons:

- Name**: A text input field.
- Password**: A text input field.
- Login**: A button to submit the credentials.

A configuration will be setup as part of the initial installation and configuration, click on that **Configuration name**.



The screenshot shows the main interface of the Telephony Configuration Application. The left sidebar indicates "No configuration loaded". The main area displays a list of configurations and templates.

**Configurations**

Click on the configuration name to work with the configuration. To create a new configuration click on the "new" symbol to the right. The chosen configuration will be the template for the new configuration. To delete a configuration, click on the trash bin to the right of the configuration. Download a file by right clicking on the source link and choosing "Save Target As..." in the popup menu.

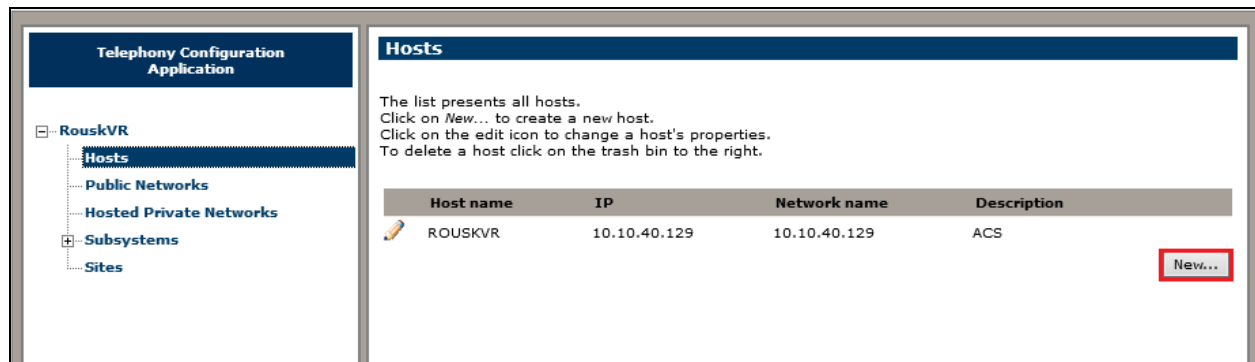
Configuration name	Last deployed (Server local time)
RouskVR (source)	2017-02-02 12:03:12

**Templates**

To create a new configuration from the template click on the "new" symbol to the right.

Template name	Description
CMGVoice Without CTC - Template	CMGVoice Without CTC - Template
CUCM SIP Template	CUCM SIP Template
Empty Template	Empty Template
InAttend CUCM SIP Template	InAttend CUCM SIP Template
InAttend MX-ONE SIP Template	InAttend MX-ONE SIP Template
Simple CUCM SIP Template	Simple CUCM SIP Template
Single ACS Template	Single ACS Template
Single CTC Template	Single CTC Template
Single CTC With Queue Messages - Template	Single CTC With Queue Messages - Template

Click into **Hosts** in the left window. A new host will need to be setup, and this can be done by clicking on **New** in the main window.



Enter a suitable **Host name** and **IP address**. This will be the Session Manager Security Module (SM100) IP address, as an example **10.10.40.12** was used below.

The screenshot shows a dialog box titled 'Edit host -- Webpage Dialog'. It has a tab labeled 'Edit host'. The dialog contains four input fields: 'Host name' (with a clear 'X' button), 'IP address', 'Network name', and 'Description'. The values entered are '10.10.40.12', '10.10.40.12', '10.10.40.12', and 'SessionManager' respectively. Below the fields is a note: 'Note! Host name, Ip address and Network name must exist on the LAN in order for the configuration to work properly.' At the bottom right are 'Update' and 'Cancel' buttons.

Host name: 10.10.40.12 X

IP address: 10.10.40.12

Network name: 10.10.40.12

Description: SessionManager

Note! Host name, Ip address and Network name must exist on the LAN in order for the configuration to work properly.

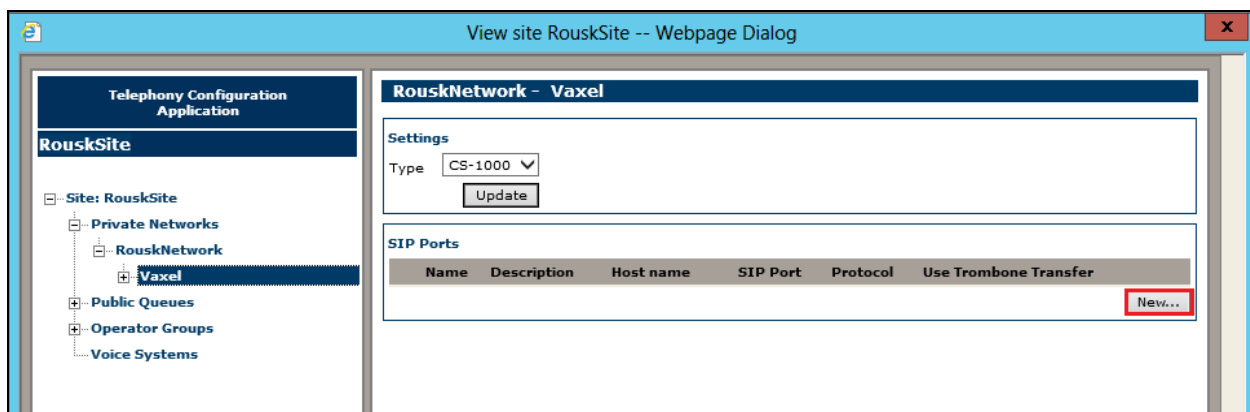
Update Cancel

Click on **Sites** in the left window and once again a site will have been already configured during the initial setup, click on that site.



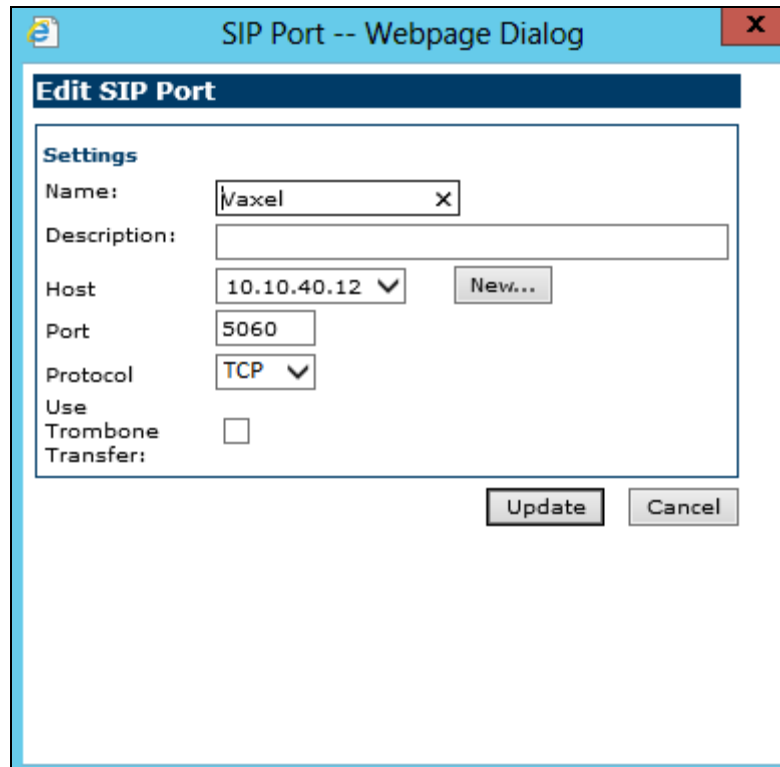
Navigate to **Vaxel** in the left window and click on **New** in the main window. This will create a new PBX connection. Note that the **Type** can be set to **CS-1000** before clicking on **New**.

**Note:** The Type being set to CS-1000 does not matter for Communication Manager, this is correct as there is no specific setting for Communication Manger and the closest is CS-1000.



Enter a suitable name and select the **Host** that was created above from the drop-down menu. The **Port** should be set to **5060** and the **Protocol** should be set to **TCP**, this will match the **Entity Link** setup in **Section 6.3**.

**Note:** The Protocol used can be either TCP or UDP, but it must match that setup on the Entity Link in **Section 6.3**.



The screenshot shows a web-based dialog box titled "SIP Port -- Webpage Dialog". Inside, there is a section titled "Edit SIP Port" with a "Settings" sub-header. The settings include:

- Name:** A text input field containing "Vaxel" with a small 'x' icon to its right.
- Description:** An empty text input field.
- Host:** A dropdown menu showing "10.10.40.12" with a downward arrow, and a "New..." button to its right.
- Port:** A text input field containing "5060".
- Protocol:** A dropdown menu showing "TCP" with a downward arrow.
- Use Trombone Transfer:** An unchecked checkbox.

At the bottom right of the dialog, there are two buttons: "Update" and "Cancel".

Navigate to **Domains** in the left window and note the **SIP Domain** is entered here as per **Section 6.1.1**. Devices can be entered by clicking on the **New** button at the bottom right of the screen. This will add Communication Manager extensions that can be used for other functions that are not covered in these Application Notes.

**View site RouskSite -- Webpage Dialog**

**RouskNetwork - Vaxel - Domains - Rousk**

**Settings**

PBX Id: 1

Default internal prefix: 1

CMG View: [ ]

**SIP Domain**: devconnect.local

SIP Domain Description: [ ]

Phone context: [ ]

Create \*23-numbers [ ]

[ Update ]

**Ports**

Name	Type	Host name	Port	Protocol	Description
Vaxel	sip	10.10.40.12	5060	UDP	

[ Add ]

**Media servers**

Name	Order
MS	1

[ Add ]

**Device ranges**

Description	Range	Type
Ext	4500	Application number
Int	4507	Application number
CMGSpeech	4502	Application number
SpeechAttendant	4503	Application number
SAAR	7990	Application number
DirectDrop	4504	Application number
Office	3000 - 3030	Phone

[ New... ]

These extensions are entered as shown below, for example extensions from **3000** to **3030** were entered as shown.

**Device range -- Webpage Dialog**

**Edit device range**

Type: Phone

Description: Office

Internal prefix: [ ]

Range: 3000 To 3030

[ Update ] [ Cancel ]

## 8.4. Update the Registry on the Mitel Attendant Connectivity Server

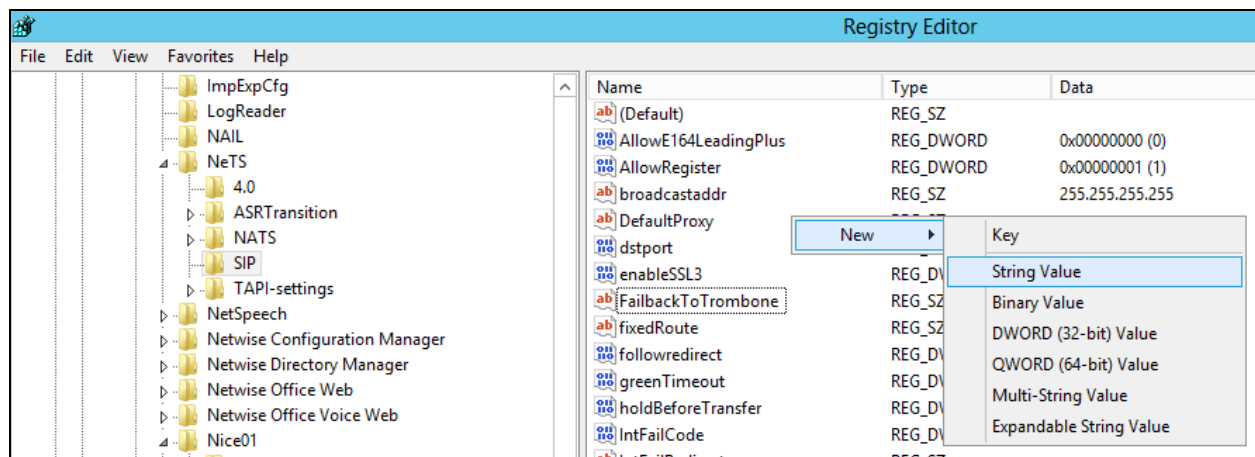
A registry setting was added to the NeTS process on the ACS server to allow a re-invite to be sent to overcome an issue found during the following scenarios:

1. Caller from Communication Manager calls to the Mitel InAttend operator.
2. The operator transfers the caller to a voicemail box, 'Direct Drop' to the mailbox.

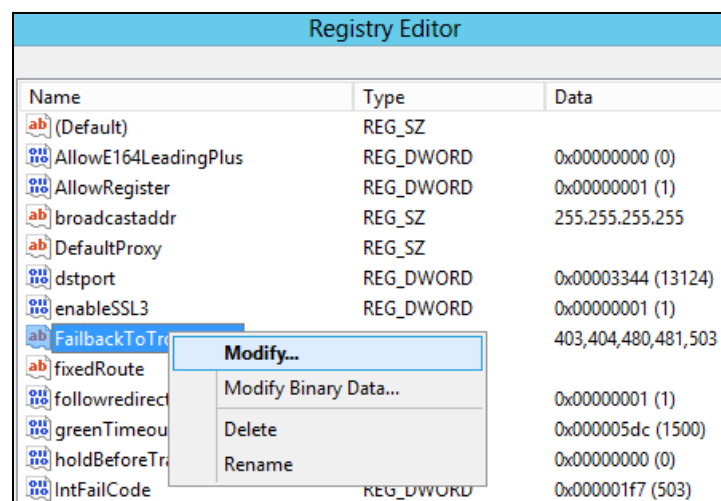
Without the update in the registry the call could not be transferred correctly. The ACS will initiate a transfer using REFER and Communication Manager sends an ACCEPT but then immediately after sends a NOTIFY message containing "481 Call Transaction does not exist". The NETS then creates a new invite with the trombone transfer and this overcomes the issue.

The registry is updated as follows. Navigate to

**Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow4332Node\Netwise\NeTS\SIP.**  
In the main window, right-click anywhere on the screen and select **New → String Value**.

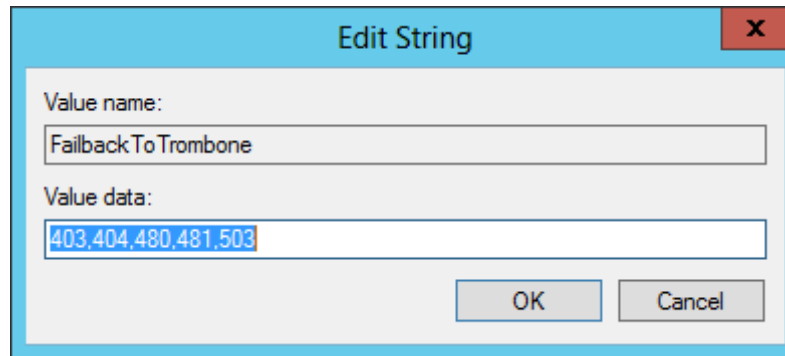


Enter the name **FailbackToTrombone** as the name for the new **REG\_DWORD** (not shown) and right-click on the REG\_DWORD and select **Modify** as shown.



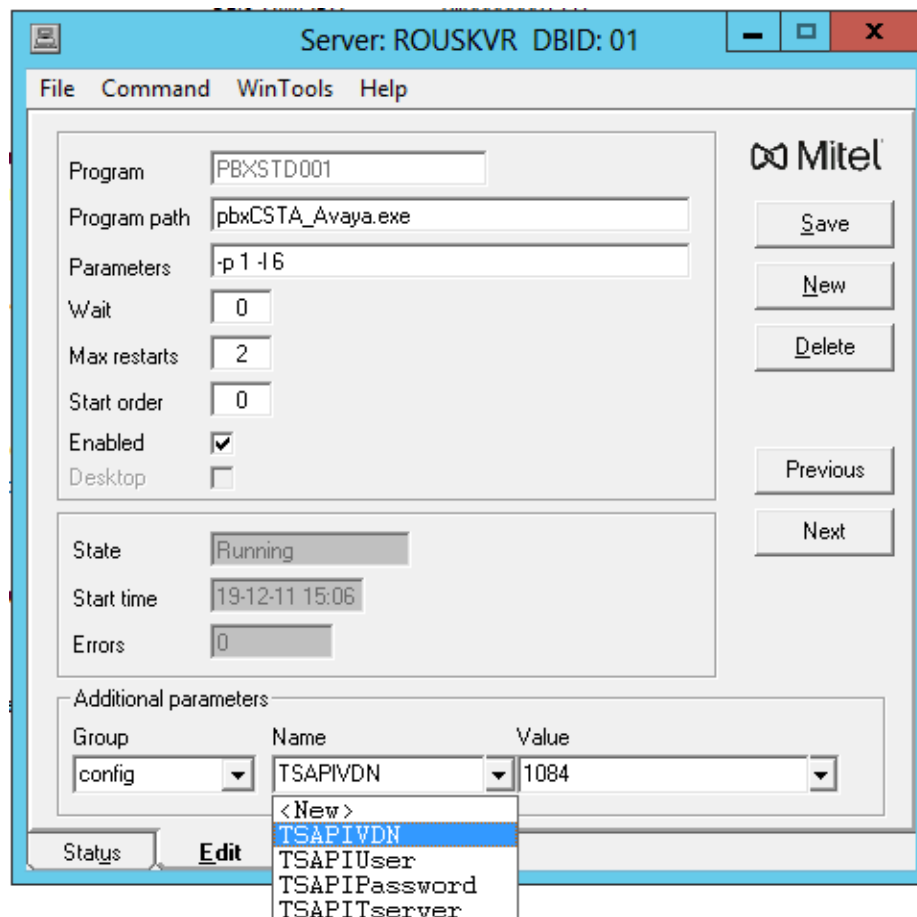


Enter the **Value data 403,404,480,481,503** and click on **OK**.



## 8.5. Configure TSAPI connection from Collaboration Management (CMG) module

Open SPMAN (not shown), this is a Mitel application that reads the registry. The following screen is displayed. Changes are made to the **Additional parameters** at the bottom of the screen below. The **TSAPIVDN** is the VDN added in **Section 5.5.1**. This will be the second VDN added, the VDN that the collect digits Vector routes to. The **TSAPIUser** and **TSAPIPassword** is that of the CTI user added in **Section 7.6**.



The **TSAPITserver** information is filled in from the TLINK as shown in **Section 7.4**.

**Note:** The unsecure link was used for the compliance testing.

Server: ROUSKVR DBID: 01

File Command WinTools Help

Program: PBXSTD001

Program path: pbxCSTA\_Avaya.exe

Parameters: -p 1 -l 6

Wait: 0

Max restarts: 2

Start order: 0

Enabled: ☒

Desktop: ☐

State: Running

Start time: 19-12-11 15:06

Errors: 0

Additional parameters:

Group	Name	Value
config	TSAPITserver	AVAYA#CM81XVMGP#CSTA#

Save New Delete Previous Next

Status Edit

## 8.6. Configure TSAPI connection from the InAttend Server module

Open a web browser to the InAttend server, as shown. The following screen will appear, and the **PBX link configuration** can be set. **Avaya Communication Manager** is chosen for the **Telephone system**. The **PBX connection** is set to **TSAPI** and the **Save** button can be pressed.


The screenshot shows the 'PBX link configuration' page in the Mitel administration interface. The page has a header with the Mitel logo and navigation links: 'User Configuration', 'CTI Server', 'Presence Server', 'Tools', and 'Help'. Below the header is a banner image with the text 'PBX link configuration'. The main content area is divided into two sections: 'Properties' on the left and 'Telephone system' on the right. The 'Properties' section includes a sidebar with links: 'Telephone system', 'Telephony', 'Direct connection', 'Server settings', and 'Number alignment'. The 'Telephone system' section contains the following fields: 'PBX link name' (Avaya), 'PBX link number' (1), 'Server' (ROUSKVR), 'Telephone system' (Avaya Communication Manager), 'PBX connection' (TSAPI), 'Recognition of external / internal phone numbers' (Prefix), 'Value' (0), 'Handling of outgoing numbers' (Add line prefix), and 'Handling of incoming numbers' (Add line prefix). There are 'Save' and 'Back to the link list' buttons at the top right of the form.

Pressing **Save** on the previous screen brings up the following window where the **TSAPI-Interface** details are added, which include the TLINK, TSAPI user and password. Click on **Save** again once the information is filled in.

The screenshot shows the 'PBX link configuration' page in the Mitel administration interface, now displaying the 'TSAPI - Interface' section. The page has the same header and banner as the previous screenshot. The 'Properties' section on the left is the same. The 'TSAPI - Interface' section contains the following fields: 'Telephony server' (AVAYA#CM81XVMPG#CSTA#A), 'Username' (mitel), 'Password' (\*\*\*\*\*), and 'Path of Csta32.dll' (C:\Windows\SysWOW64\csta32.dll). There are 'Save' and 'Back to the link list' buttons at the top right of the form. A message box in the top right corner reads: '(11/12/2019 18:08:54.599) For the processing further data is necessary. Please supplement the marked fields.'

The following screen is then shown containing the new connection. This connection must be started by pressing the start icon, highlighted below.

The screenshot shows the Mitel PBX links configuration page. The header includes the Mitel logo and navigation links: User Configuration, CTI Server, Presence Server, Tools, and Help. The main heading is "PBX links". Below this, there is a "Server" section with a dropdown menu showing "ROUSKVR" and "All Servers". To the right of the dropdown are "Refresh" and "Add PBX Link" buttons. A table displays the PBX link configuration:

	PBX link	PBX link No.	Server	
	Avaya	1	ROUSKVR	

A successful connection will appear as green, as it is shown below.

The screenshot shows the Mitel PBX links configuration page with the connection status updated. The table now shows a successful connection:

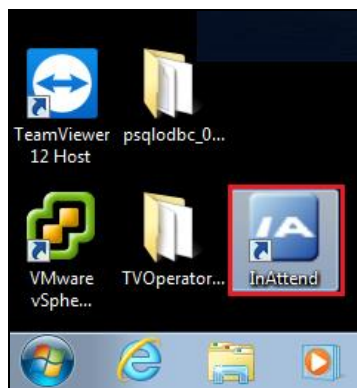
	PBX link	PBX link No.	Server	
	Avaya	1	ROUSKVR	

## 9. Verification Steps

This section provides the tests that can be performed to verify correct configuration of the Avaya and Mitel solutions.

1. Make a call to the InAttend attendant and request to be transferred to a known extension. Ensure the call is connected.
2. Make a call to the InAttend attendant and request to be transferred to a known extension which is busy and request to leave a voice message. Ensure the call is transferred to voicemail and a message can be left.
3. Make a call to the Attendant queue. Ensure the attendant receives and answers the call.

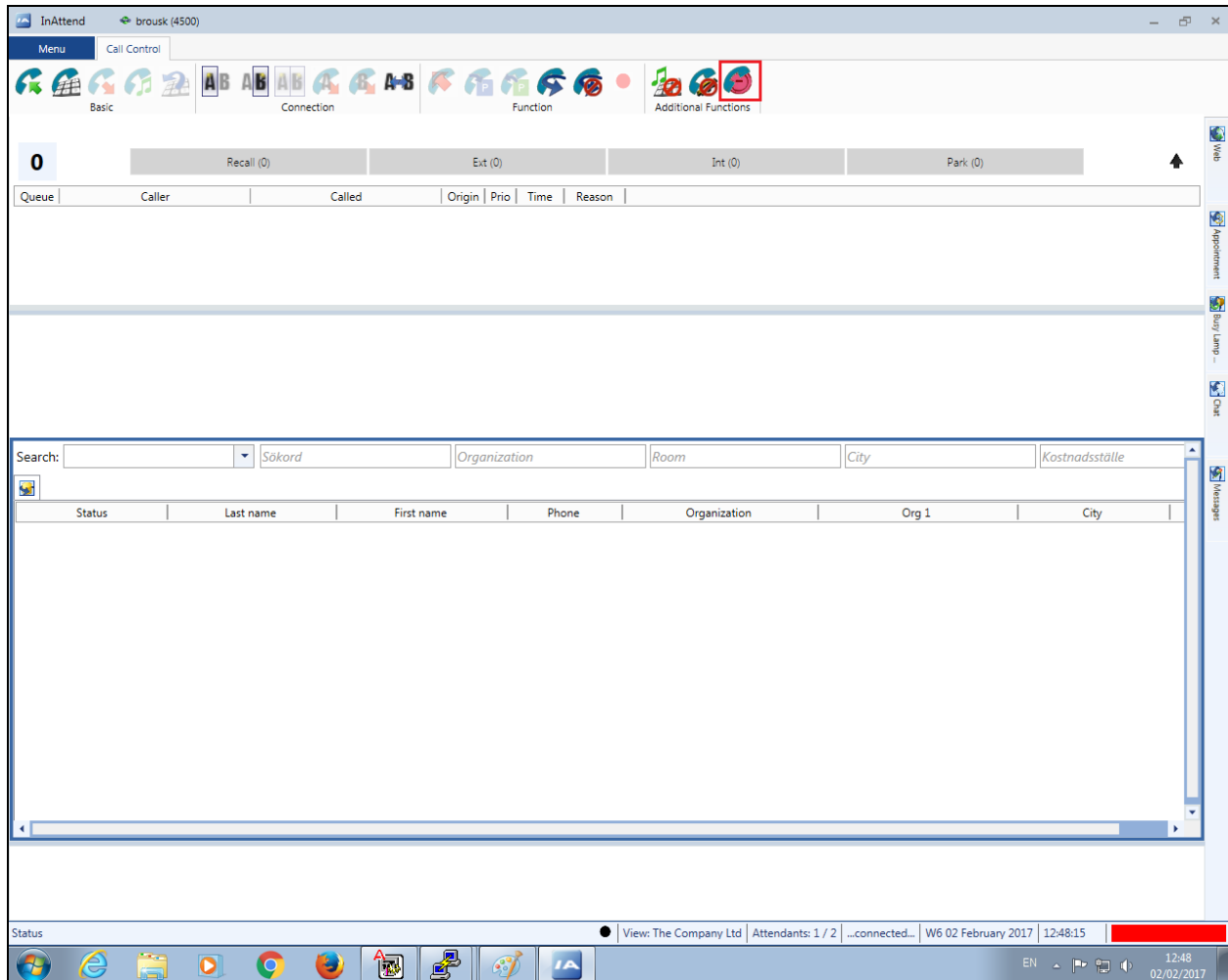
**InAttend** can be started from the shortcut or by navigating to the program on the client PC.



Enter the appropriate credentials and click on **Log On**.

A screenshot of the Mitel InAttend login screen. The background is dark blue. At the top left is the Mitel logo, followed by a vertical line and the text 'InAttend'. Below this, there are two input fields: 'Username' with the text 'brousk' and 'Password' with a masked password of ten dots. Below the password field is a checkbox labeled 'Remember password'. At the bottom right are two buttons: 'Log On' and 'Cancel'.

Once logged in the operator will be in night mode as shown below with the red bar. Click on the icon highlighted to change this to normal operation.



Once a call is presented to the attendant the caller is shown on the attendant screen and the attendant can answer the call using the mouse or keyboard. Presence information on users beginning with 100 are shown at the bottom of the screen.

The screenshot displays the InAttend software interface for user 'brousk (4500)'. The interface includes a top menu bar with 'Menu' and 'Call Control'. Below this is a toolbar with icons for Basic, Connection, Function, and Additional Functions. A central control area shows 'Recall (0)', 'Ext (1)' (highlighted in green), 'Int (0)', and 'Park (0)'. A call log table is visible, showing a call from PSTN (091732000) to Avaya Night (4500). Below the call log, a large panel displays call details for PSTN 091732000 and INT Avaya Night 4500. At the bottom, a search bar is set to '100', and a table lists users with status 'In a call', including Rousk Björn and Andersson Mikael. The status bar at the very bottom indicates 'View: The Company Ltd', 'Attendants: 1 / 3', and the date/time 'W50 Wednesday 11 December 2019 17:20:08'.

Queue	Caller	Called	Origin	Prio	Time	Reason	Call Identifier
Ext	PSTN (091732000)	Avaya Night (4500)	int	10	00:04	New call	1156

Status	Phone	Last name	First name	Organization	Org 1	City
In a call	1000	Rousk	Björn	Market Access	0008-008.1	
In a call	1001	Andersson	Mikael			

With the call answered the caller's information is displayed and this information can be augmented with information from the InAttend database.

The screenshot displays the Avaya InAttend software interface. At the top, there are tabs for 'Basic', 'Connection', 'Function', and 'Additional Functions'. Below these are fields for 'Recall (0)', 'Ext (0)', 'Int (0)', and 'Park (0)'. A table with columns 'Queue', 'Caller', 'Called', 'Origin', 'Prio', 'Time', and 'Reason' is visible. The main section shows caller information for Louise Finnigan, including her name, phone number 7001, and extension 4500. Below this is a search bar with fields for 'Sökord', 'Organization', 'Room', 'City', and 'Kostnadsställe'. The bottom section displays a detailed view of Louise Finnigan, including her phone number 7001 and a list of activities. The status bar at the bottom shows 'Status', 'New: The Company Ltd', 'Attendants: 1 / 2', '...connected...', 'W6 02 February 2017', and '12:47:17'.

Detail	Value
Title	Shop Manager
E-Mail	louise.finnigan@thecompany.com
	Manager
	Shop Manager
	Cashier
Sökord	Receipts
	Shop Inventory
	Salesman
	Mail
Phone	7001



## 9.1. Verify the connection to Avaya Aura® Application Enablement Services

The following can be checked to ensure that the connections to the AES are in operation correctly.

### 9.1.1. Verify the link to Application Enablement Services from Communication Manager

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Check the TSAPI link status with Application Enablement Services by using the command **status aesvcs cti-link**. Verify the **Service State** of the TSAPI link is **established**.

status aesvcs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	8	no	aes81xvmpg	established	87	61

Use the command **status aesvcs interface** to verify that the status **Local Node** of Application Enablement Services interface is connected and **listening**.

status aesvcs interface			
AE SERVICES INTERFACE STATUS			
Local Node	Enabled?	Number of Connections	Status
procr	yes	1	listening

Verify that there is a link with the Application Enablement Services and that messages are being sent and received by using the command **status aesvcs link**.

status aesvcs link						
AE SERVICES LINK STATUS						
Srvr/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
01/01	aes81xvmpg	10.10.40.38	57650	procr	683	665

### 9.1.2. Verify the link to Communication Manager Link from Application Enablement Services

On the AES Management Console verify the status of the link to Communication Manager by selecting **Status → Status and Control → Switch Conn Summary** to display the **Switch Connections Summary** screen. Verify the status of the link by checking that the **Conn State** is **Talking** and the **Online/Offline** is **Online**.

Switch Connections Summary

☐ Enable page refresh every 60 seconds

	Switch Conn	Conn State	Processor Ethernet	Since	Online/Offline	Active/Standby/Admin'd AEP Conns	Num of TCI Conns	SSL	Msgs To Switch	Msgs From Switch	Msg Period
<input type="radio"/>	cm81large	Talking	Yes	Wed Dec 11 07:56:25 2019	Online	1 / 0 / 1	2	Enabled	616	631	30
<input checked="" type="radio"/>	cm81xvmpg	Talking	Yes	Wed Dec 11 07:56:26 2019	Online	1 / 0 / 1	2	Enabled	717	709	30

By clicking **Connection Details** on the screen above, the **Switch Connection Details** should resemble that what is shown below.

Switch Connection Details - cm81xvmpg

☐ Enable page refresh every 60 seconds

	Hostname or IP Address	Connection State	Cluster ID/MID	Online/Offline	Since	Msgs To Switch	Msgs From Switch	Msg Period
<input checked="" type="radio"/>	10.10.40.37	Talking	1	Online	Wed Dec 11 07:56:26 2019	717	709	30

### 9.1.3. Verify the TSAPI Link from Application Enablement Services

Select **Status** → **Status and Control** → **TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.

The screenshot shows the 'TSAPI Link Details' screen. On the left is a navigation menu with categories like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, and Status. Under 'Status', 'Status and Control' is expanded, showing options like CVLAN Service Summary, DLG Services Summary, DMCC Service Summary, Switch Conn Summary, and TSAPI Service Summary. The main content area is titled 'TSAPI Link Details' and includes a refresh toggle set to 60 seconds. Below this is a table with columns: Link, Switch Name, Switch CTI Link ID, Status, Since, State, Switch Version, Associations, Msgs to Switch, Msgs from Switch, and Msgs Period. Two links are listed, both with status 'Talking' and state 'Online'. Below the table are 'Online' and 'Offline' buttons. At the bottom, a section for 'For service-wide information' offers tabs for 'TSAPI Service Status', 'TLink Status', and 'User Status'.

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
1	cm81xvmpg	1	Talking	Wed Dec 11 07:57:01 2019	Online	18	3	115	118	30
2	cm81large	1	Talking	Wed Dec 11 07:57:01 2019	Online	18	0	15	15	30

Click in **User Status** on the screen above. A new window is displayed below showing the CTI user **mitel** connected to receive the TSAPI events.

The screenshot shows the 'CTI User Status' screen. It has a refresh toggle set to 60 seconds. Below this, there's a 'CTI Users' section with a dropdown menu set to 'All Users' and a 'Submit' button. It displays 'Open Streams 6' and 'Closed Streams 31'. The 'Open Streams' section contains a table with columns: Name, Time Opened, Time Closed, and Tlink Name. Five streams are listed, all with names starting with 'DMCCLCSUserDoNotModify'. Below the table are buttons for 'Show Closed Streams', 'Close All Opened Streams', and 'Back'.

Name	Time Opened	Time Closed	Tlink Name
mitel	Wed 11 Dec 2019 02:45:34 PM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 11 Dec 2019 07:58:17 AM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 11 Dec 2019 07:58:17 AM GMT		AVAYA#CM81LARGE#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 11 Dec 2019 07:58:17 AM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 11 Dec 2019 07:58:17 AM GMT		AVAYA#CM81LARGE#CSTA#AES81XVMPG

## 9.2. Verify the SIP Trunk connection

The SIP trunk from Communication Manager to Session Manager can be checked using the following steps.

### 9.2.1. Verify Avaya Aura® Communication Manager

The following steps can be taken if there are any issues with calls being made. This should help verify the links between the products. From the SAT interface, verify the status of the SIP trunk groups by using the **status trunk n** command, where “n” is the trunk group number administered in **Section 5.2**. Verify that all trunks are in the **in-service/idle** state as shown below (just a sample of the trunks configured).

```
status trunk 1
```

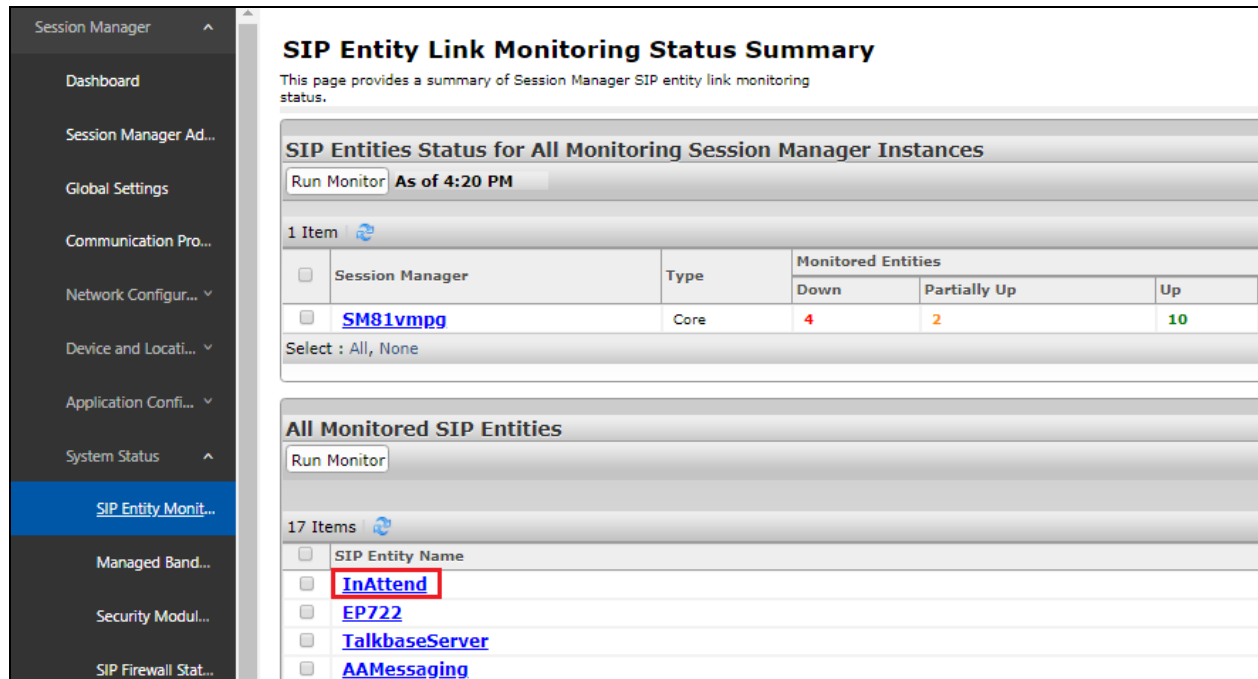
TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports	Busy
0001/0001	T00001	<b>in-service/idle</b>	no	
0001/0002	T00002	<b>in-service/idle</b>	no	
0001/0003	T00003	<b>in-service/idle</b>	no	

### 9.2.2. Verify InAttend SIP Entity is up

Log into System Manager as per **Section 6**. Navigate to **Elements** and click on **Session Manager**.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The 'Elements' menu is open, showing a list of system components including Communication Manager, Communication Server 1000, Conferencing, Device Adapter, Device Services, Media Server, Meeting Exchange, Messaging, Presence, Routing, **Session Manager** (highlighted), and Web Gateway. The main dashboard area contains several panels: 'System Resource Utilization' with a bar chart showing usage for 'opt', 'var', and 'emdata'; 'Alarms' with a circular gauge showing 'Critical', 'Major', 'Minor', and 'Warning' levels; 'Application State' with a table showing License Status (Active), Deployment Type (VMware), Multi-Tenancy (DISABLED), OOBM State (DISABLED), and Hardening Mode (Standard); 'Notifications' with a 'No data' message; 'Information' with a table showing Elements (CM, Session Manager, System Manager, UCM Applications) and their Count and Sync Status; and 'Shortcuts' with a 'Drag shortcuts here' area and a button for 'Administrative...'. The bottom of the dashboard shows 'Current Usage' with '11/250000 USERS' and '1/50 SIMULTANEOUS ADMINISTRATIVE LOGINS'.

Select the **InAttend** SIP Entity.



**SIP Entity Link Monitoring Status Summary**

This page provides a summary of Session Manager SIP entity link monitoring status.

**SIP Entities Status for All Monitoring Session Manager Instances**

Run Monitor As of 4:20 PM

1 Item

Session Manager	Type	Monitored Entities		
		Down	Partially Up	Up
<a href="#">SM81vmpg</a>	Core	4	2	10

Select : All, None

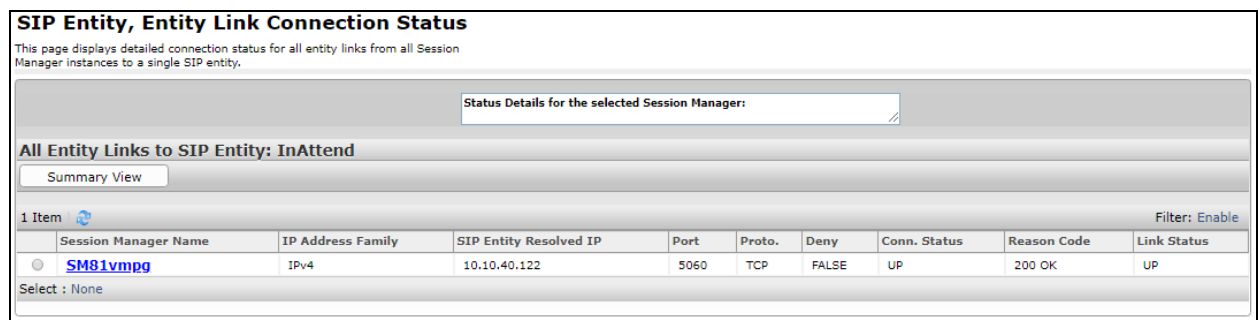
**All Monitored SIP Entities**

Run Monitor

17 Items

SIP Entity Name
<a href="#">InAttend</a>
<a href="#">EP722</a>
<a href="#">TalkbaseServer</a>
<a href="#">AAMessaging</a>

The SIP Entity should show as **UP** as it is shown below.



**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.

Status Details for the selected Session Manager:

**All Entity Links to SIP Entity: InAttend**

Summary View

1 Item Filter: Enable

Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<a href="#">SM81vmpg</a>	IPv4	10.10.40.122	5060	TCP	FALSE	UP	200 OK	UP

Select : None

## 10. Conclusion

The interoperability of Mitel InAttend using Mitel Attendant Connectivity Server V2.6 from Mitel Sweden AB to interoperate with Avaya Aura® Communication Manager R8.1 utilizing a SIP trunk connection to Avaya Aura® Session Manager R8.1 and a TSAPI connection to Avaya Aura® Application Enablement Services was successful for this specific setup to place calls to and from InAttend. All issues and observations are outlined in **Section 2.2**.

## 11. Additional References

These documents form part of the Avaya official technical reference documentation suite. Further information can be obtained from <http://support.avaya.com> or from your Avaya representative.

- [1] *Administering Avaya Aura® Communication Manager* – Release 8.1
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.1
- [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide* Release 8.1
- [4] *Administering Avaya Aura® Session Manager* – Release 8.1

Product Documentation for Mitel InAttend can be obtained from Mitel at:  
<http://www.Mitel.com/support>

---

**©2019 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 DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).