



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Mitel InAttend using Mitel Attendant Connectivity Server from Mitel Sweden AB to interoperate with Avaya Aura® Communication Manager R7.0.1 and Avaya Aura® Session Manager R7.0.1 - 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 R7.0.1 via Avaya Aura® Session Manager R7.0.1.

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 from Mitel Sweden AB to interoperate with Avaya Aura® Communication Manager R7.0.1 via Avaya Aura® Session Manager R7.0.1.

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 Communication Server 1000 utilising a SIP connection to Avaya Aura® Session Manager using the Mitel Attendant Connectivity Server (ACS).

The Mitel Attendant Connectivity Server (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 (Mitel InAttend) 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 Attendant Connectivity Server consists of:

- NeTS 5.7.6.11
- MediaServer 1.7.34
- QueueManager 2.10.33.1

The Mitel InAttend Server includes:

- Collaboration Management CMG 8.3
- Virtual Reception 8.3
- Microsoft SQL 2012

Note: Virtual Reception consists of a Speech Attendant and Speech Office, these applications along with MS SQL and Collaboration Management gives the user a suite of attendant services.

Note: During Compliance Testing various applications such as Speech Attendant and Speech Office were tested alongside the InAttend console, all of these applications utilize the Attendant Connectivity Server (ACS) in order to connect to Session Manager. These Application Notes focus on that connection between the Attendant Connectivity Server (ACS) and Session Manager. However, the product that was tested was Mitel InAttend.

Note: 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 ACS is not necessarily required to be part of this Application Note, however **Section 7** 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 the ACS to communicate with the Communication Manager as implemented on a customer's premises using a SIP connection to Session Manager. Testing focused on verifying that ACS registered with Session Manager as a SIP Entity and 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 Mitel ACS is configured as a SIP Entity on Session Manager acting as a 3rd party PBX connecting to the Avaya solution over a SIP trunk. The connection was setup using UDP 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 Mitel ACS and the Avaya Aura® Session Manager.

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.

2.1. Interoperability Compliance Testing

The testing included:

- Verification of connectivity between Communication Manager and the ACS via Session Manager
- 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

2.2. Test Results

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

1. If the Operator calls to SIP phone and the SIP phone transfers the call to a H323 or Digital, upon completion the TAC of the SIP trunk is displayed on the H323 or Digital set.

2.3. Support

Technical support from Mitel can be obtained through the following:

Web: www.Mitel.com/service-and-support

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of a Communication Manager and a Session Manager. Mitel Attendant Connectivity Server 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, Digital and Analog phones were configured on Communication Manager to generate calls to Mitel InAttend and outbound calls to the PSTN. SIP and QSIG trunks were configured to connect Communication Manager to the PSTN.

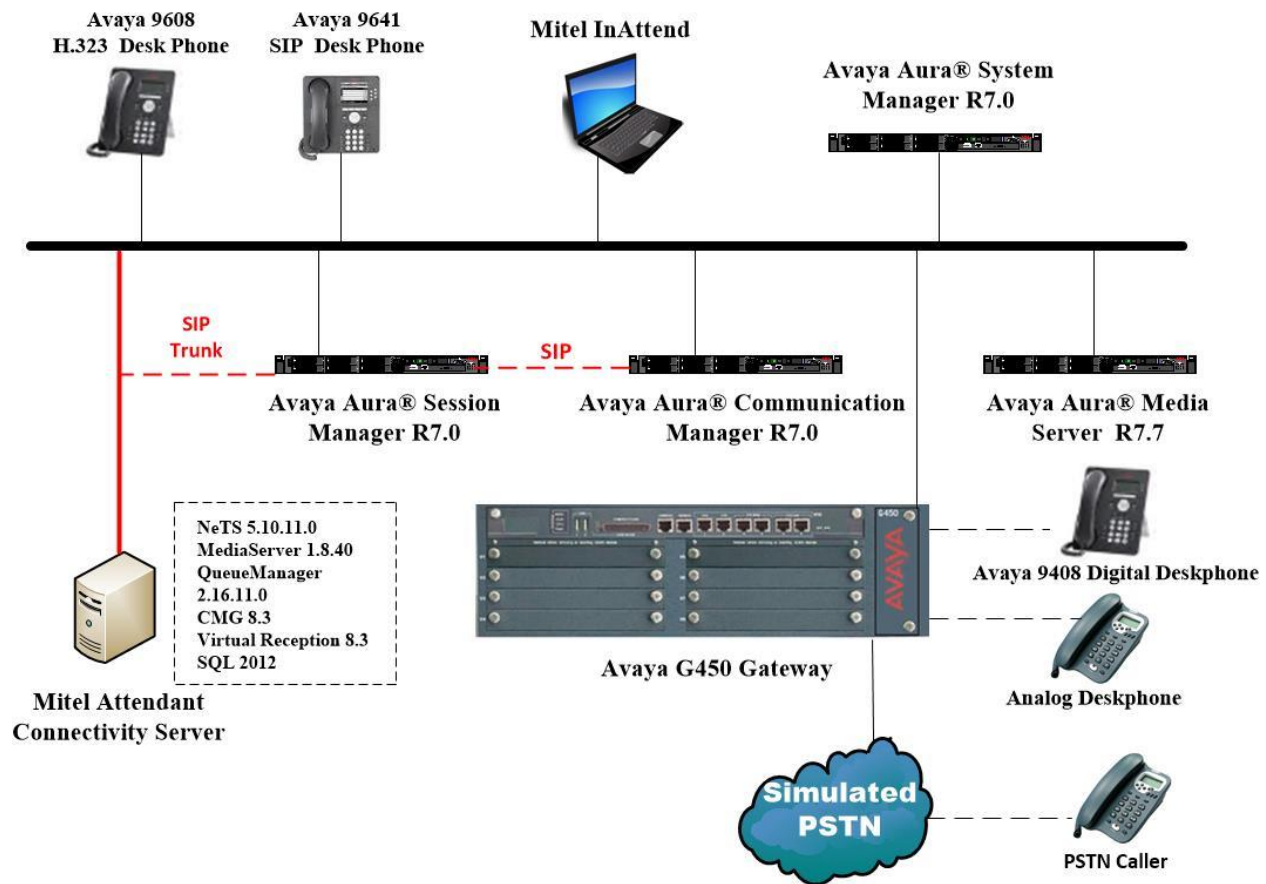


Figure 1: Avaya Communication Manager and Mitel Reference Configuration

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 running on a virtual server	System Manager 7.0.1.2 Build No. - 7.0.0.0.16266 Software Update Revision No: 7.0.1.2.086007 Service Pack 2
Avaya Aura® Session Manager running on a virtual server	Session Manager R7.0 SP2 Build No. – 7.0.1.2.701230
Avaya Aura® Communication Manager running on a virtual server	R7.0.1 R017x.00.0.441.0 00.0.441.0-23523
Avaya Media Server running on a virtual server	Media Server SYSTEM R7.7.0.8 Media Server R7.7.0.200
Avaya 9608 H323 Deskphone	96x1 H323 Release 6.6.028
Avaya 9641 SIP Deskphone	96x1 SIP Release 7.0.0.39
Avaya 9408 Digital Deskphone	V2.0
Analog Phone	N/A
Mitel Equipment	Software / Firmware Version
Mitel Attendant Connectivity Server running on Windows 2012 R2	Mitel Attendant Connectivity Server includes: NeTS 5.10.11.0 MediaServer 1.8.40 QueueManager 2.16.11.0
InAttend Server Running on Windows 2012 R2	Version 2.4 InAttend Server includes: CMG 8.3 Virtual Reception 8.3 SQL 2012
InAttend Attendant client running on Windows 7 Professional SP1	Version 2.4.17.0

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 10**.

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

- Verify System Parameters Customer Options.
- Configure System Features.
- Administer Dial Plan.
- Administer Route Selection for InAttend calls.
- Configure Network Region and IP Codec.
- Configure SIP Trunk.

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

5.1. 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.

display system-parameters customer-options		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
Maximum Administered SIP Trunks:		24000	319
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
ARS? y	Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? y	DCS (Basic)? y

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
Private Networking? y	Uniform Dialing Plan? y
	Usage Allocation Enhancements? y

5.2. 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 10** 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 Attnd-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	

5.3. 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 and therefore to InAttend. In order to achieve this, automatic alternate routing (aar) would be used to route the calls. The dial plan and aar routing analysis need to be changed to allow this.

Type **change dialplan analysis**, in order 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	
2	4	ext							
3	4	ext							
4	4	udp							
5	4	ext							
6	4	udp							
7	3	dac							
8	1	fac							
9	1	fac							
*	3	fac							
#	3	fac							

5.4. Administer Route Selection for InAttend Calls

As digits **4xxx** were defined in the dial plan as **udp** (Section 5.3), 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.

change aar analysis 4						Page 1 of 2	
AAR DIGIT ANALYSIS TABLE							
Location: all						Percent Full: 1	
Dialed	Total		Route	Call	Node	ANI	
String	Min	Max	Pattern	Type	Num	Reqd	
450	4	4	1	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 5.6**.

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

5.5. Configure Network Region and IP Codec

In the **Node Names IP** form, note the IP Address of the **procr** and the Session Manager (**sm70vmpg**). 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															Page 1 of 2	
IP NODE NAMES																
Name		IP Address														
AMS77vmpg		10.10.40.17														
CMS18vmpg		10.10.40.36														
IPO500V2		10.10.40.20														
IPOSE		10.10.40.25														
PGDECT		10.10.40.50														
aes70vmpg		10.10.40.26														
default		0.0.0.0														
procr		10.10.40.13														
procr6		::														
sm70vmpg		10.10.40.12														

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 6.2**. 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
                   Inter-region IP-IP Direct Audio: yes
                   UDP Port Min: 2048      IP Audio Hairpinning? n
                   UDP Port Max: 3329
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** has been set to **none**. This ensures that no media is encrypted.

```

change ip-codec-set 1                                     Page 1 of 2
                                IP CODEC SET

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt  Size(ms)
1: G.711A      n          2        20
2:
3:
4:
5:
6:
7:

Media Encryption      Encrypted SRTCP:
1: none
2:
3:
4:

```

5.6. Configure SIP Trunk

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 desired transport method, for compliance testing this 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 **sm70vmpg**), as per **Section 5.5**.
- 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 **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: sm70vmpg
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
DTMF over IP: rtp-payload		RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3		Direct IP-IP Audio Connections? n
Enable Layer 3 Test? y		IP Audio Hairpinning? 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                      Group Type: sip      CDR Reports: y
  Group Name: SIP TRK                COR: 1              TN: 1      TAC: *11
    Direction: two-way              Outgoing Display? y
    Dial Access? n                  Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 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
      Preferred Minimum Session Refresh Interval(sec): 600

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	Numbering Format: private
	UUI 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 **Send Diversion Header** and Support Request History are both 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? y
	Support Request History? y
	Telephone Event Payload Type: 101
	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

6. Configuring Avaya Aura® Session Manager

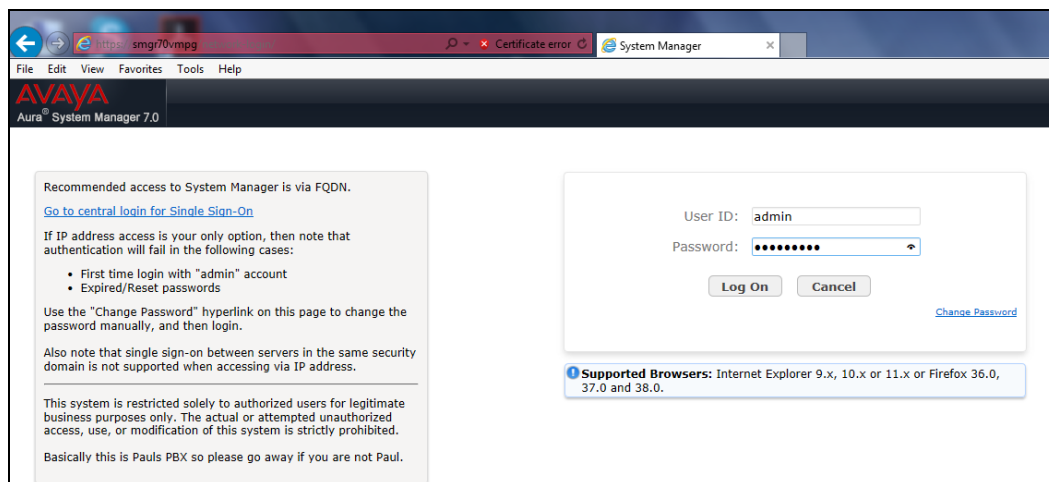
A number of configurations are required to enable Communication Manager to route call to the ACS and vice versa. All configurations of Session Manager are preformed using System Manager. The configuration operations described in this section can be summarized as follows:

- Logging on to System Manager
- Specify SIP Domain
- Add Location
- Create ACS as a SIP Entity
- Create an Entity Link for ACS
- Create a Routing Policy for ACS
- Create a Dial Pattern for ACS

Note: It is implied a working system is already in place. During compliance testing a SIP Entity and an Entity Link for Communication Manager were created. Also a Routing Policy and a Dial Pattern to route calls to Communication Manager were created and are outside the scope of these Application Notes.

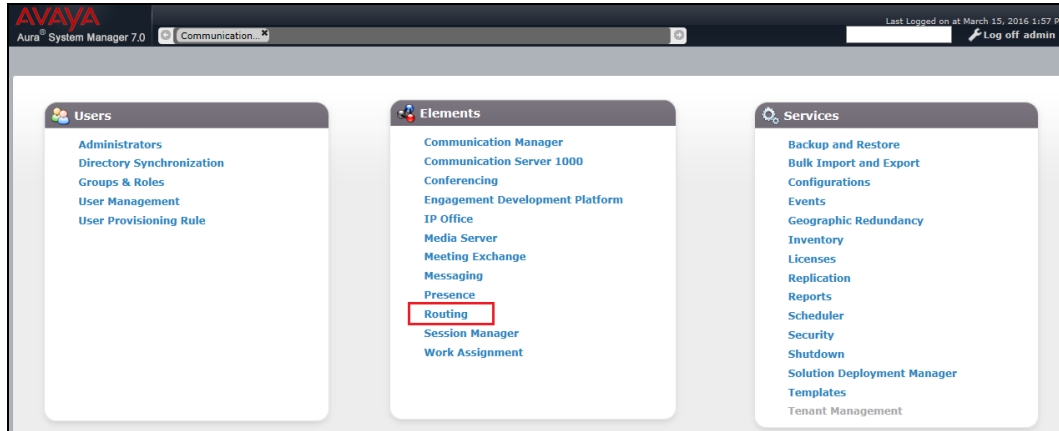
6.1. Logging on to Avaya Aura® System Manager

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



6.2. Specify SIP Domain

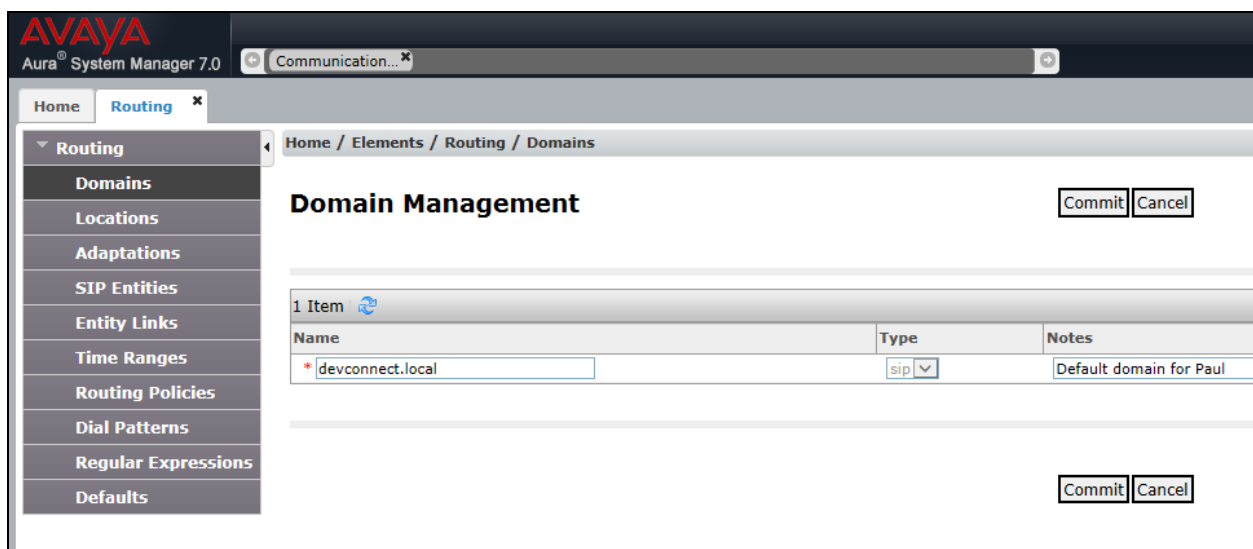
Add the SIP domain for which the communications infrastructure will be authoritative. From the home page of System Manager, navigate to **Elements** → **Routing**.



The Routing page will be displayed, select **Domains** on the left and click the **New** button on the right (not shown). The following screen will then be shown. Fill in the following:

- **Name:** The authoritative domain name (e.g., **devconnect.local**).
- **Type:** Select **sip** in the dropdown menu.
- **Notes:** Descriptive text (optional).
- Click **Commit**.

Since the sample configuration does not deal with any other domains, no additional domains need to be added.



6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management. To add a location, select **Locations** on the left and then click the **New** button on the right (not shown). The following screen will then be shown. Fill in the following:

- Under **General**:
 - **Name**: A descriptive name.
 - **Notes**: Descriptive text (optional).
- Under **Location Pattern**:
 - **IP Address Pattern**: A pattern used to logically identify the location.
 - **Notes**: Descriptive text (optional).

Note: the example below shows the Avaya Subnet **10.10.40.x** and another subnet **172.29.187.x** added. Click on **Commit** to complete.

AVAYA
Aura® System Manager 7.0

Home / Elements / Routing / Locations

Location Details

General

* Name: PGLAB

Notes: Pauls Lab

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

2 Items

	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.40.*	Pauls subnet
<input type="checkbox"/>	* 172.29.187.*	Etrails subnet

Select : All, None

Commit Cancel

6.4. Add SIP Entity for ACS

A SIP Entity must be added for Mitel ACS. To add a SIP Entity select SIP Entities on the left and click on the **New** button on the right (not shown). On the screen displayed, fill in the following under the **General** section of the main screen:

- **Name:** A descriptive name.
- **FQDN or IP Address:** Enter Mitel ACS IP address.
- **Type:** Select **SIP Trunk**.
- **Adaptation:** There is no Adaptation required for Mitel ACS.
- **Location:** Select the location defined previously.
- **Time Zone:** Time zone for this location.

Defaults may be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The left sidebar shows a navigation menu with 'Routing' expanded, containing options like Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' with a 'Commit' button. The 'General' section contains the following fields: Name (Mitel ACS), FQDN or IP Address (10.10.40.129), Type (SIP Trunk), Notes, Adaptation, Location (PGLAB), Time Zone (Europe/Dublin), SIP Timer B/F (in seconds) (4), Credential name, Securable (checkbox), and Call Detail Recording (egress). The 'Loop Detection' section includes Loop Detection Mode (On), Loop Count Threshold (5), and Loop Detection Interval (in msec) (200).

AVAYA
Aura® System Manager 7.0

Home Routing

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* Name: Mitel ACS

* FQDN or IP Address: 10.10.40.129

Type: SIP Trunk

Notes:

Adaptation:

Location: PGLAB

Time Zone: Europe/Dublin

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

Credential name:

Securable: ☐

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

6.5. Add Entity Link for ACS

The SIP trunk from Session Manager to ACS is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button on the right (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the appropriate protocol.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the Mitel ACS.

Click on **Commit** when completed.

AVAYA
Aura® System Manager 7.0

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
<input type="checkbox"/>	MitelACS_UDP	sm70vmpg	UDP	5060	Etrali_OT	<input type="checkbox"/>	5060	trusted

Select : All, None

Commit Cancel

6.6. Add Routing Policy for ACS

Routing policies describe the conditions under which calls will be routed to the SIP Entities. A routing policy must be added for ACS. To add a routing policy, select **Routing Policies** on the left and click on the New button on the right (not shown). The following screen is displayed. Fill in the following:

- Under **General**: Enter a descriptive name in Name.
- Under **SIP Entity as Destination**: Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

Routing Policy Details

General

* Name: To Mitel ACS

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
------	--------------------	------	-------

Time of Day

Add Remove View Gaps/Overlaps

1 Item

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Select the **Mitel ACS** SIP Entity for the Routing Policy and click on **Select** as highlighted below.

SIP Entities

Select Cancel

SIP Entities

17 Items

Name	FQDN or IP Address	Type	Notes
aacc64SIPvmppg	10.10.40.55	SIP Trunk	
AACC70vmppg	10.10.40.80	SIP Trunk	AACC70vmppg
ASBCE_PG	10.10.40.151	SIP Trunk	Session Boarder Controller
cm63vmppg	10.10.40.31	CM	R6.3 CM
cm70vmppg	10.10.40.13	CM	
CPE	10.10.40.251	SIP Trunk	For Stephen Wilson
CS1000E	10.10.40.111	Other	CS1KPG1
EnghouseCP	10.10.40.106	SIP Trunk	EnghouseCP
EP-POM	10.10.40.135	Voice Portal	EP POM Server
Etrali_OT	172.29.187.244	SIP Trunk	
IPOS00V2	10.10.40.20	SIP Trunk	
messaging63vmppg	10.10.40.22	SIP Trunk	AA Messaging R6.3
Mitel ACS	10.10.40.129	SIP Trunk	
NECDAP011	10.10.40.208	Endpoint Concentrator	DAP 1
NovaLink	10.10.40.44	SIP Trunk	

Select : None

Click on **Commit** when finished.

AVAYA
Aura® System Manager 7.0

Home / Elements / Routing / Routing Policies

Routing Policy Details Commit Cancel Help ?

General

* Name: To Mitel ACS

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Mitel ACS	10.10.40.129	SIP Trunk	

6.7. Add Dial Pattern for routing to ACS

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the sample configuration, 4-digit extensions beginning with 450x route to the Mitel ACS. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button on the right (not shown). Fill in the following under the **General** section in the main window.

- **Pattern:** Dialed number or prefix.
- **Min:** Minimum length of dialed number.
- **Max:** Maximum length of dialed number.
- **SIP Domain:** Select the SIP domain as defined in **Section 6.2** or **ALL** as is shown below.
- Under **Originating Locations and Routing Policies:** Click **Add**, and then select the appropriate location and routing policy from the list.

AVAYA
Aura® System Manager 7.0

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 450

* Min: 4

* Max: 4

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: To Mitel ACS

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Select : All, None						

The following screen shows the Routing Policy created in **Section 6.6** being added for the dial pattern. Click **Select** to save this dial pattern.

Home / Elements / Routing / Dial Patterns

Originating Location

Select Cancel

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

1 Item Filter: Enable

Name	Notes
PGLAB	Pauls Lab

Select : All, None

Routing Policies

13 Items Filter: Enable

Name	Disabled	Destination	Notes
<input type="checkbox"/> To_aacc64SIPvmpp	<input type="checkbox"/>	aacc64SIPvmpp	aacc64SIPvmpp
<input type="checkbox"/> To_AACC70vmpp	<input type="checkbox"/>	AACC70vmpp	To_AACC70vmpp
<input type="checkbox"/> To ASBCE	<input type="checkbox"/>	ASBCE_PG	Calls to ASBCE
<input type="checkbox"/> To_cm63vmpp	<input type="checkbox"/>	cm63vmpp	Routing to CM63
<input type="checkbox"/> To_cm70vmpp	<input type="checkbox"/>	cm70vmpp	
<input type="checkbox"/> To_CPE	<input type="checkbox"/>	CPE	For Stephen
<input type="checkbox"/> To CS1000E	<input type="checkbox"/>	CS1000E	Routing to CS1KPG1
<input type="checkbox"/> To_EnghouseCP	<input type="checkbox"/>	EnghouseCP	
<input type="checkbox"/> To Etrali	<input type="checkbox"/>	Etrali_OT	Etrali
<input type="checkbox"/> To IPO500V2	<input type="checkbox"/>	IPO500V2	To IPO500V2
<input type="checkbox"/> To_Messaging	<input type="checkbox"/>	messaging63vmpp	AA Messaging R63
<input checked="" type="checkbox"/> To Mitel ACS	<input type="checkbox"/>	Mitel ACS	
<input type="checkbox"/> To_NovaLink	<input type="checkbox"/>	NovaLink	

Select : All, None

Click on **Commit** to finish.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern: 450

* Min: 4

* Max: 4

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: To Mitel ACS

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
PGLAB	Pauls Lab	To Mitel ACS	0	<input type="checkbox"/>	Mitel ACS	

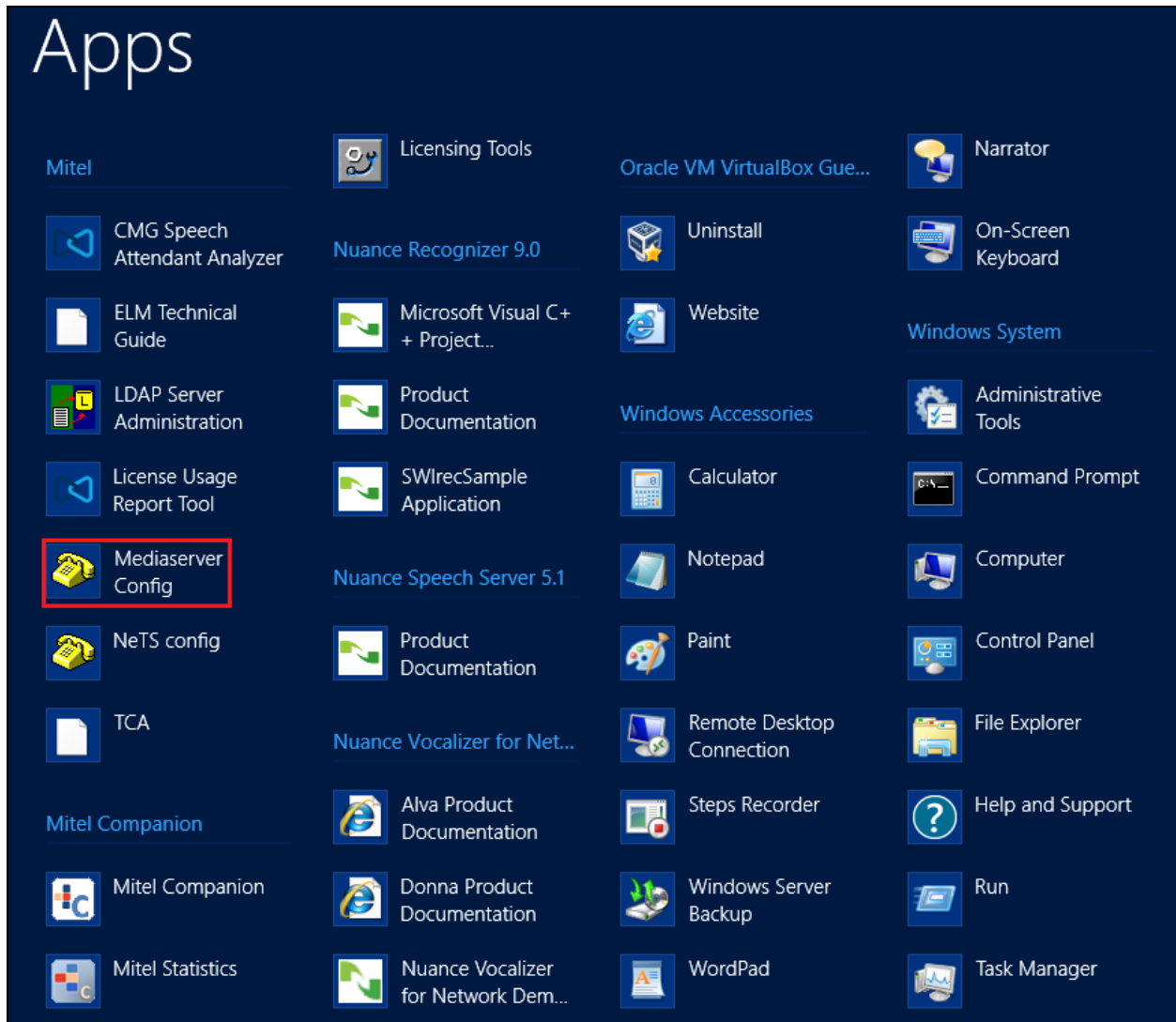
Select : All, None

7. Configure Mitel Attendant Connectivity Server (ACS)

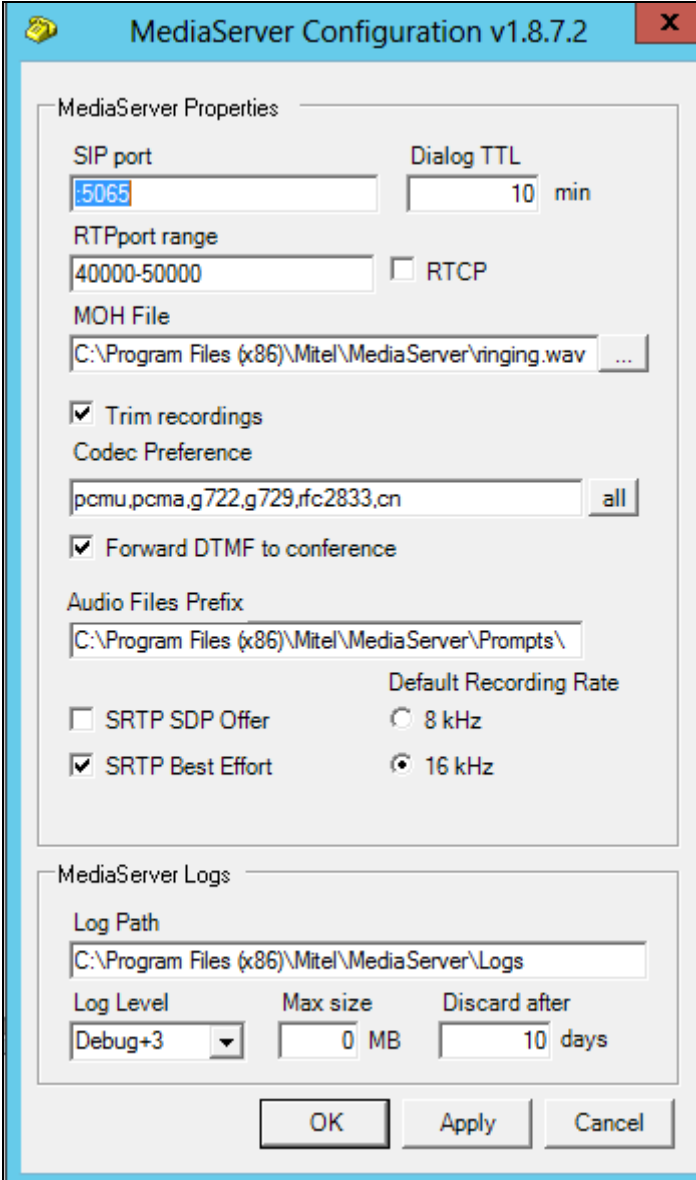
Although a Mitel engineer will setup the solution the following sections show information on the connection to Session Manager that was used for compliance testing, it may prove useful.

7.1. 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.



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\vinging.wav

☒ Trim recordings

Codec Preference: pcmu,pcma,g722,g729,fc2833,cn

☒ Forward DTMF to conference

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

☐ SRTP SDP Offer

☒ SRTP Best Effort

Default Recording Rate: 16 kHz

MediaServer Logs

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

Log Level: Debug+3

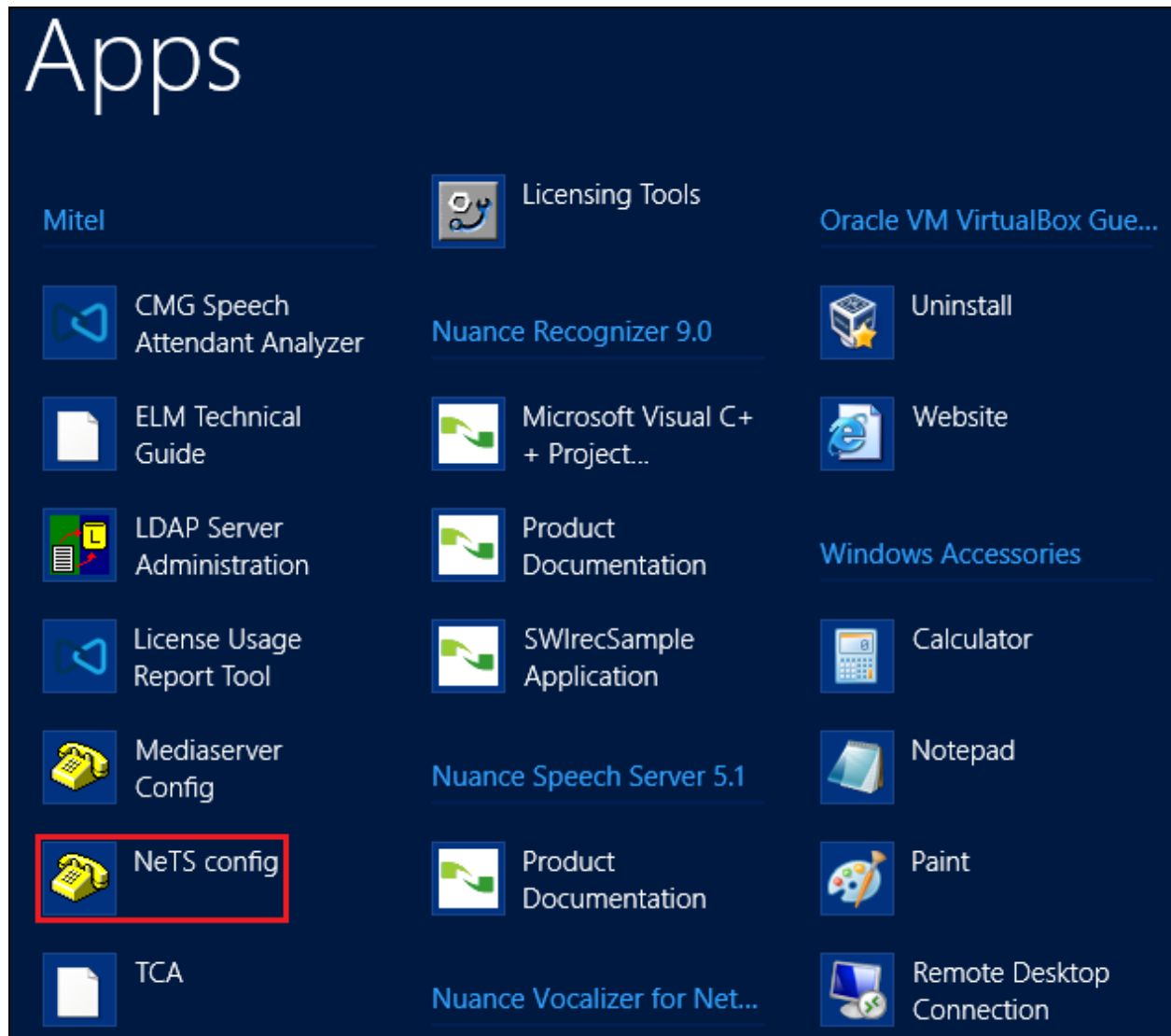
Max size: 0 MB

Discard after: 10 days

OK Apply Cancel

7.2. 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**.

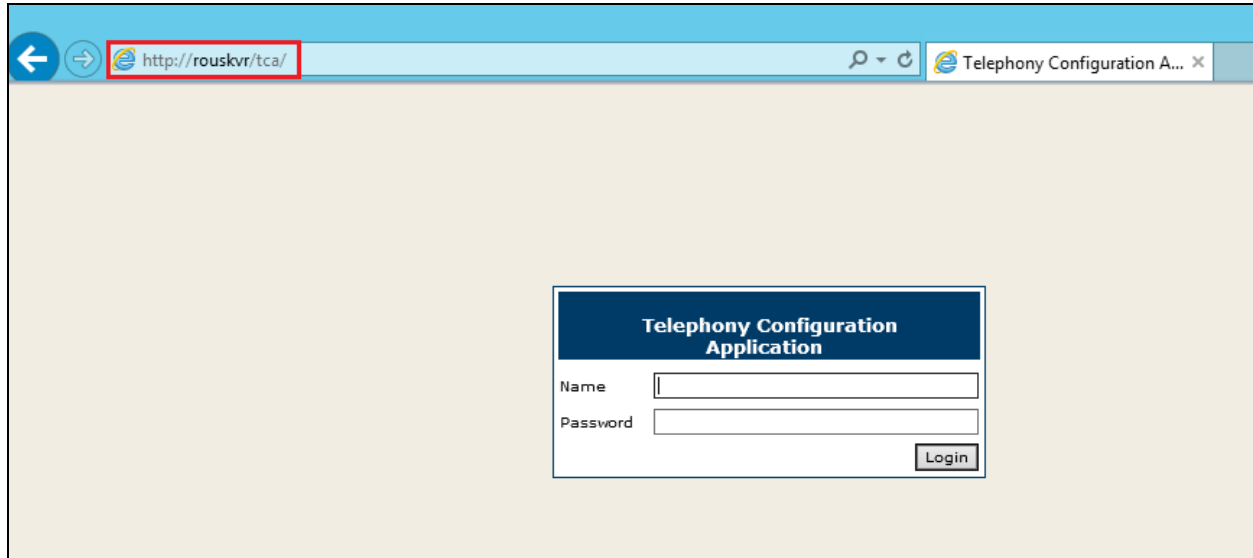
The screenshot shows the 'Network Telephony Services configuration' dialog box with the 'SIP' tab selected. The 'Local settings' section is highlighted in the left sidebar. The main area contains the following settings:

- ☒ 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 (dropdown)
- Max wait for 100 Trying on Outbound calls. (ms): 1200 (spinner)

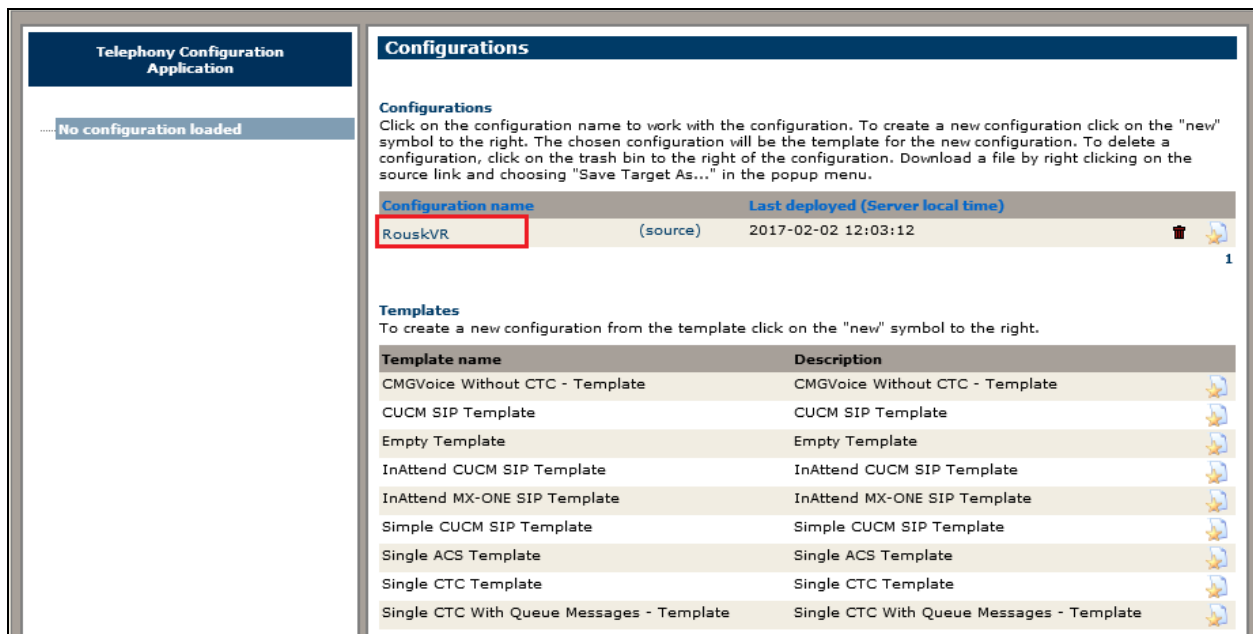
At the bottom are buttons for OK, Cancel, and Apply.

7.3. Mitel Telephony Configuration Application (TCA) configuration

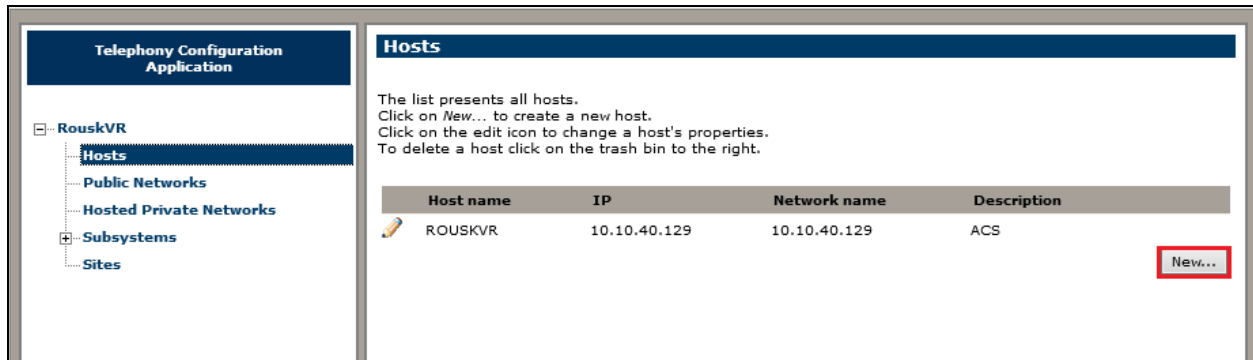
Open a web browser and browse to the ACS server name followed by TCA, for example `http://<servername>/tca`. Enter the appropriate credentials and click on **Login**.



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



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.

The screenshot shows a dialog box titled 'Edit host -- Webpage Dialog'. Inside, the 'Edit host' section has four input fields: 'Host name' (containing '10.10.40.12'), 'IP address' (containing '10.10.40.12'), 'Network name' (containing '10.10.40.12'), and 'Description' (containing 'SessionManager'). Below these 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

IP address: 10.10.40.12

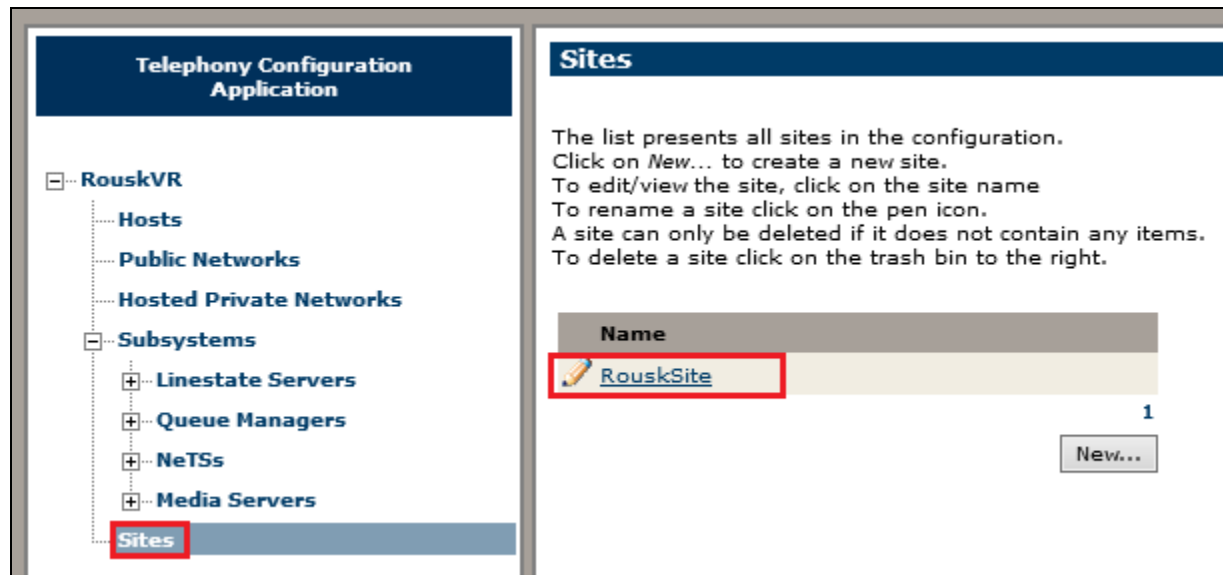
Network name: 10.10.40.12

Description: SessionManager

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

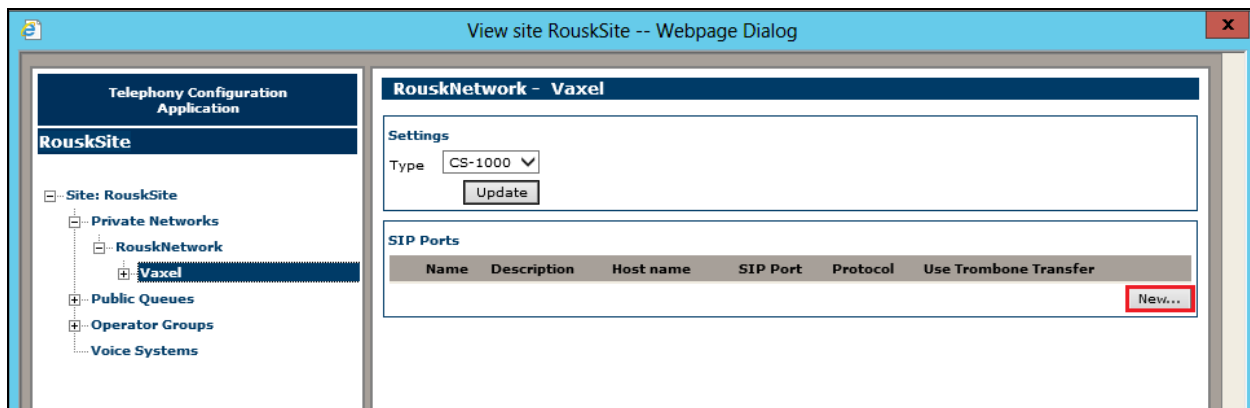
Update Cancel

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.

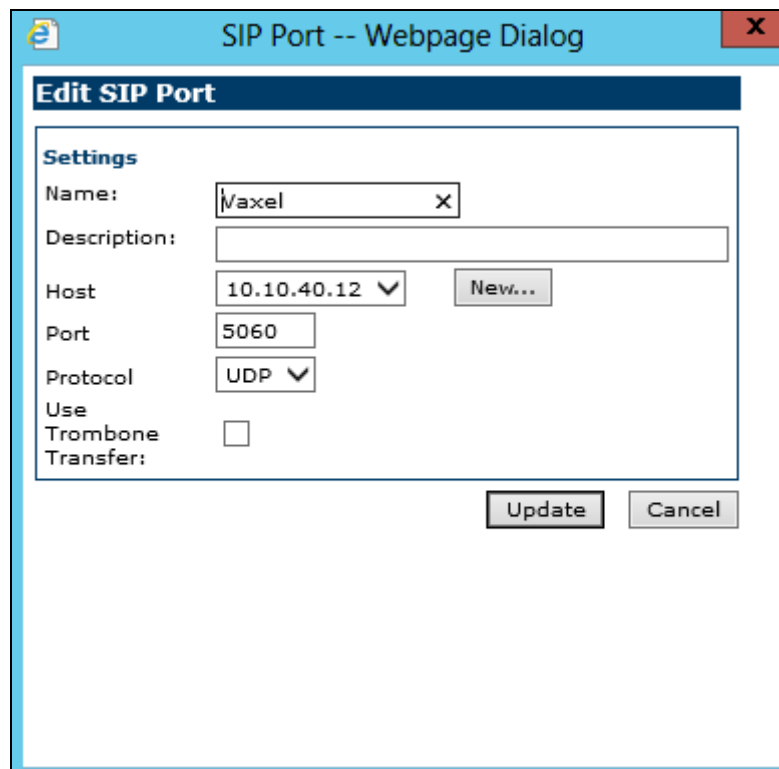


Navigate to **Vaxel** in the left window and click on **New** in the main window. This will create a new PBX connection. Note that the **Type** can be set to **CS-1000** before clicking on **New**.

Note: The Type being set to CS-1000 does not matter for Avaya Aura® 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 **UDP**, this will match the **Entity Link** setup in **Section 6.5**.



The screenshot shows a web browser window titled "SIP Port -- Webpage Dialog". Inside the window is a form titled "Edit SIP Port". The form contains the following fields and controls:

- Name:** A text input field containing "Maxel" 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 "UDP" with a downward arrow.
- Use Trombone Transfer:** A checkbox that is currently unchecked.

At the bottom right of the form are two buttons: "Update" and "Cancel".

Navigate to **Domains** in the left window and note the **SIP Domain** is entered here as per **Section 6.2**. 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: [i]

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]

7.4. Update the Registry on the Mitel Attendant Connectivity Server

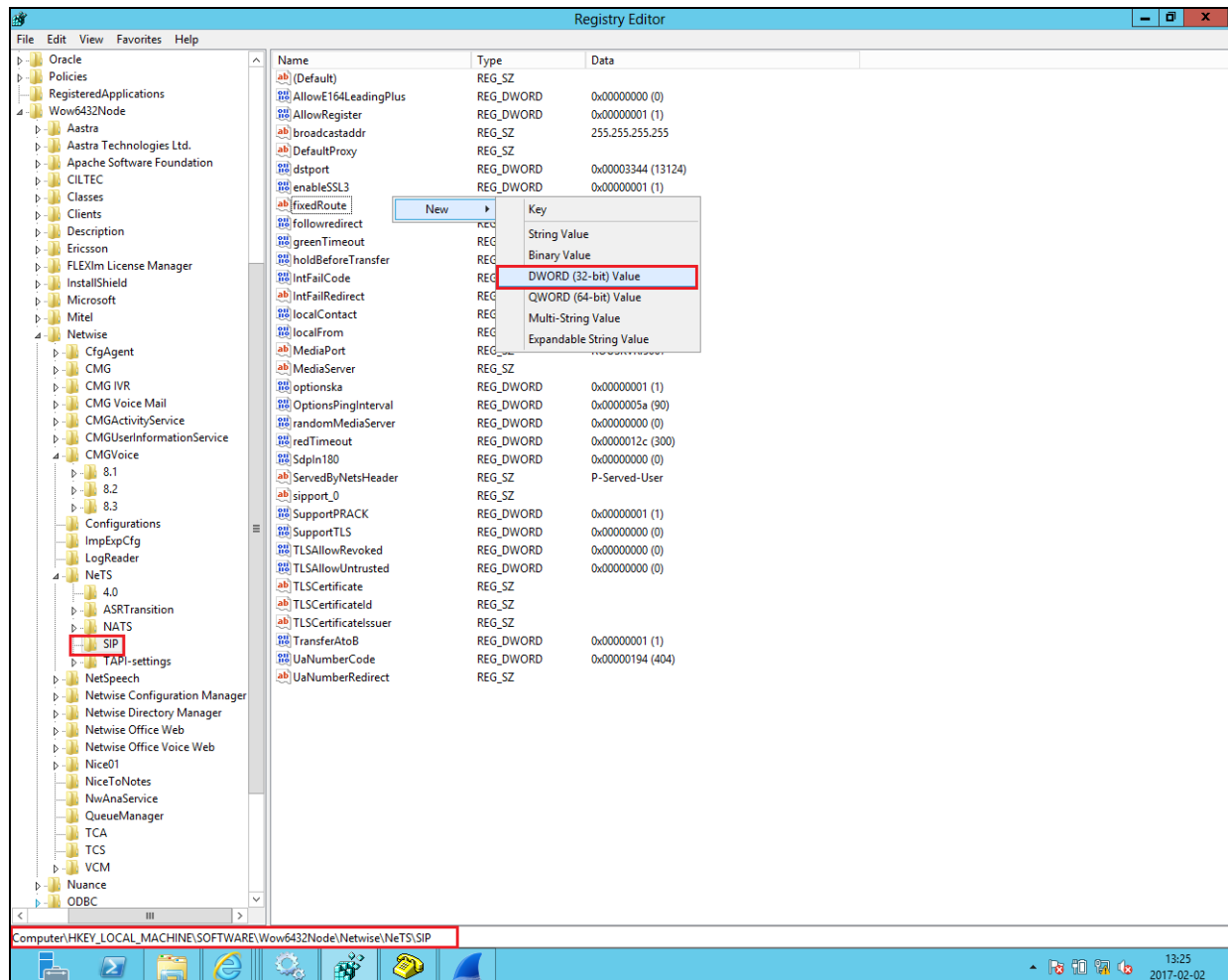
A registry setting was added to the NeTS process on the ACS server to allow a re-invite be sent to overcome an issue found during the following scenario:

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.

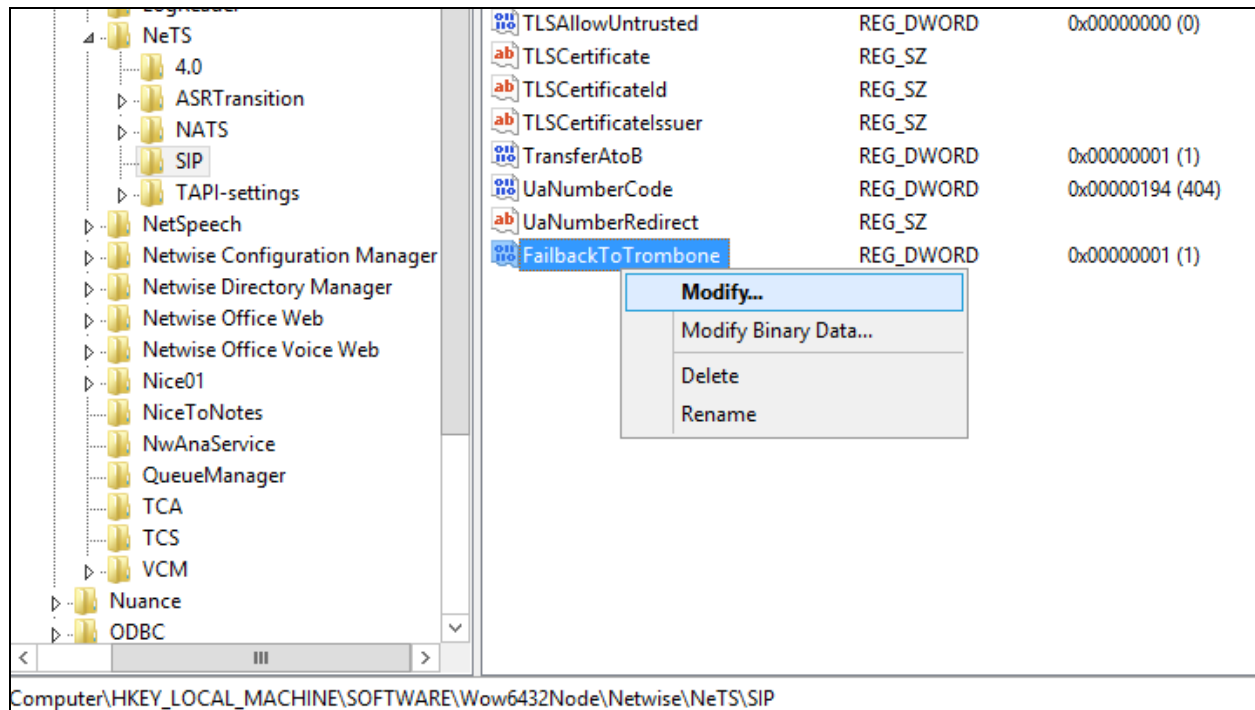
Without the update in the registry the call could not be transferred correctly. The ACS will initiate a transfer using REFER and Communication Manager sends an ACCEPT but then immediately after sends a NOTIFY message containing "481 Call Transaction does not exist". The NETS then creates a new invite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

The registry is updated as follows. Navigate to

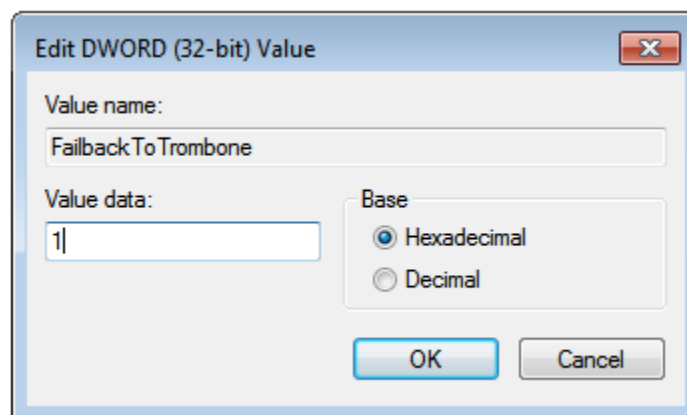
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netwise\NeTS\SIP. In the main window, right-click anywhere on the screen and select **New → DWORD (32-bit) Value**.



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 1** for **Hexadecimal** and click on **OK**.

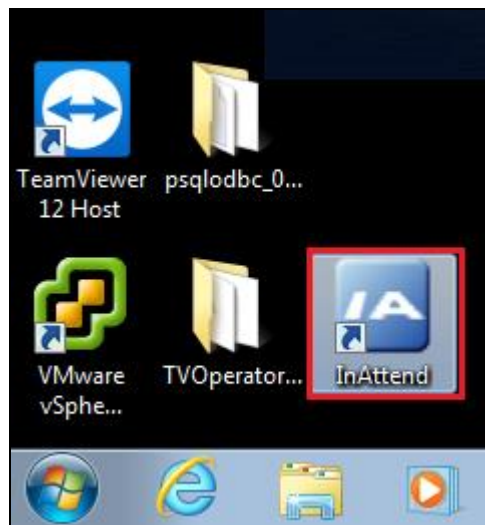


8. Verification Steps

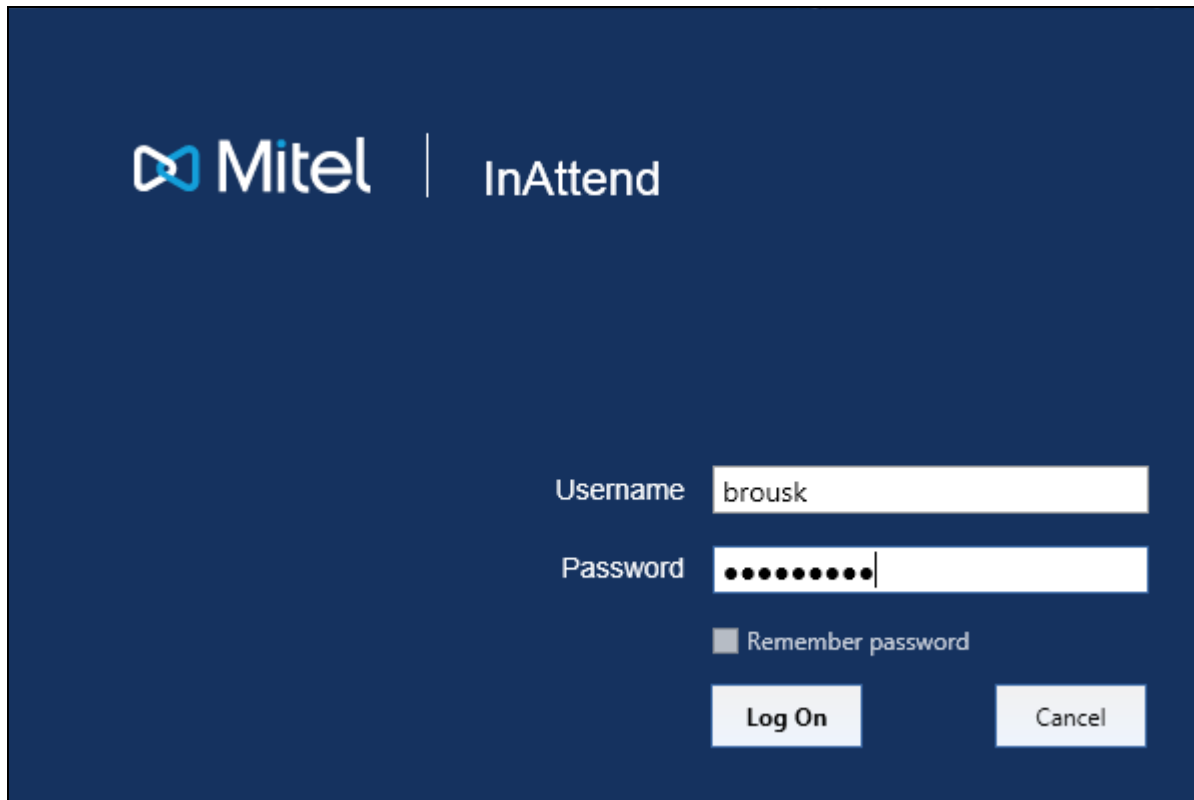
This section provides the tests that can be performed to verify correct configuration of Avaya and Mitel solution.

1. Make a call to the ACS Speech attendant and request to be transferred to a known extension. Ensure the call is connected.
2. Make a call to the ACS Speech 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 voice mail and a message can be left.
3. Make a call to the ACS 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**.



The image shows a login interface for Mitel InAttend. The background is dark blue. In the top left, the Mitel logo (a blue square with a white 'M') is followed by the word 'Mitel' in white, and then 'InAttend' in a smaller white font. Below the logo, there are two input fields. The first is labeled 'Username' and contains the text 'brousk'. The second is labeled 'Password' and contains ten black dots. Below the password field is a checkbox labeled 'Remember password'. At the bottom right, there are two buttons: 'Log On' and 'Cancel'.

Mitel | InAttend

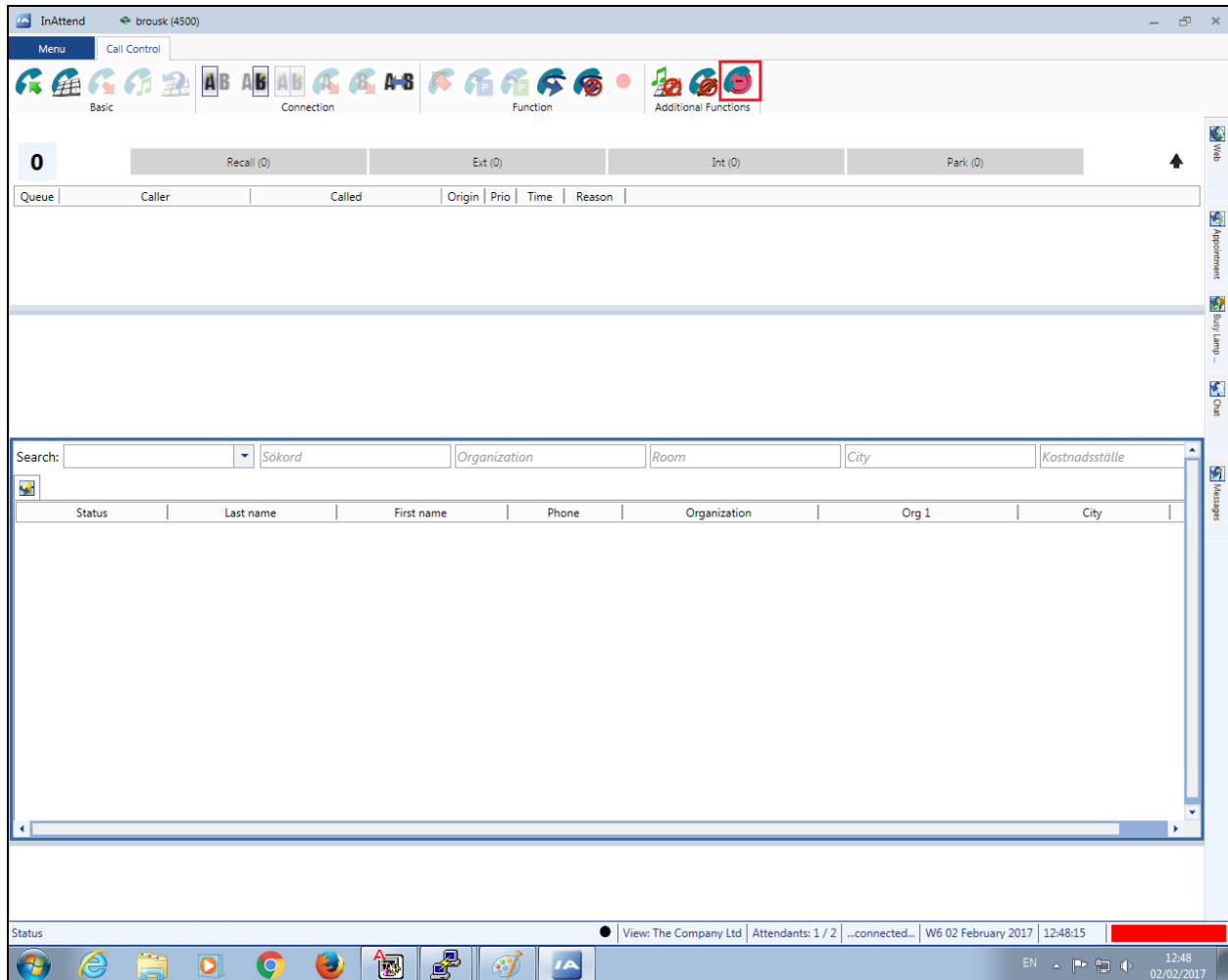
Username brousk

Password ••••••••••

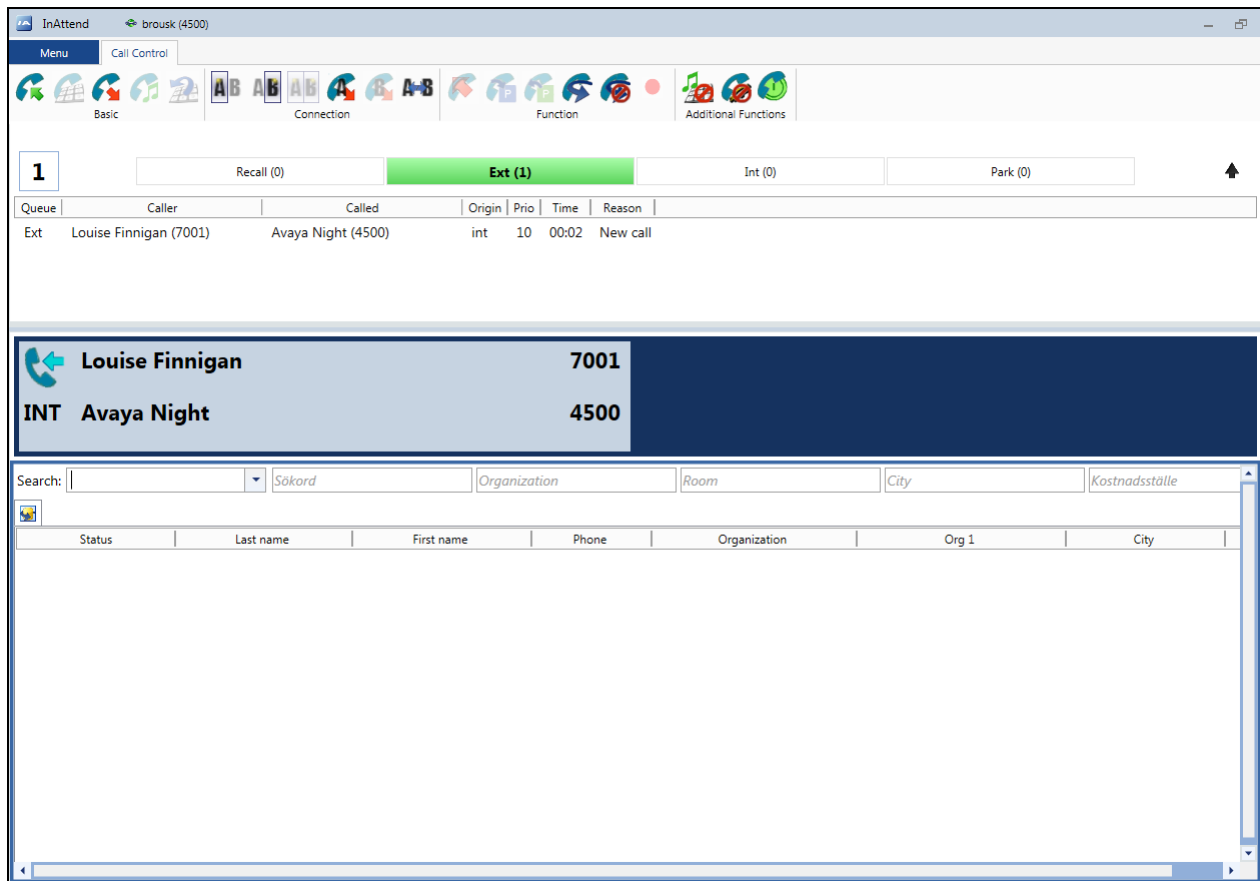
☐ Remember password

Log On 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.



With the call answered the caller's information is displayed and this information can be boosted with information found from the Mitel database.

The screenshot displays the Mitel Avaya IP Office web 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, importance level (Very Important), and a list of activities. The status bar at the bottom shows the system is connected and displays the date and time.

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

9. Conclusion

The interoperability of Mitel InAttend using Mitel Attendant Connectivity Server from Mitel Sweden AB with Avaya Aura® Communication Manager R7.0.1 via Avaya Aura® Session Manager R7.0.1 was successful for this specific setup in order to place calls to and from InAttend. All issues and observations are outlined in **Section 2.2**.

10. 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*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Administering Avaya Aura® Session Manager*, Release 7.0, 03-603324

Product Documentation for Mitel InAttend and Mitel ACS can be obtained from Mitel at: www.Mitel.com/support

©2017 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.