DevConnect Program

Application Notes for Mitel InAttend using Mitel Attendant Connectivity Server V2.7 to interoperate with Avaya Aura® Communication Manager R10.1 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Mitel InAttend v2.7 using Mitel Attendant Connectivity Server from Mitel Sweden AB to interoperate with Avaya Aura® Communication Manager R10.1. 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.

1. Introduction

These Application Notes describe the configuration steps required for Mitel InAttend using Mitel Attendant Connectivity Server V2.7 from Mitel Sweden AB to interoperate with Avaya Aura® Communication Manager R10.1 utilizing a SIP trunk connection to Avaya Aura® Session Manager R10.1 and a TSAPI connection to Avaya Aura® Application Enablement Services R10.1 (AES).

Mitel InAttend is the core application in the Mitel 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 5.13.25.0
  - MediaServer 1.9.145.0
  - QueueManager 2.19.25.0
- Mitel InAttend Server.
  - Collaboration Management CMG 8.6
  - Virtual Reception 8.6
  - Microsoft SQL 2019
  - Mitel InAttend Server 2.7

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 supplies, installs and configures their solution for the end customer 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 Communication Manager as implemented on a customer’s premises using a SIP connection to Session Manager and two TSAPI connections 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 third-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 ensure 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. When Call Forwarding Enhanced is used to forward an Avaya extension to InAttend, be that Call Forward No Answer or Call Forward Busy, InAttend is not aware of the reason that the call is being forwarded for Call Forward No Answer, it is aware for Call Forward Busy. Mitel are aware of this and are investigating the issue.
2. When Coverage Path is used to forward an Avaya extension to InAttend, be that Call Forward No Answer or Call Forward Busy, InAttend is not aware of the reason that the call is being forwarded for Call Forward No Answer, it is aware for Call Forward Busy. Mitel are aware of this and are investigating the issue.
3. 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.

4. The Transport Protocol for the SIP trunk connection between the Mitel Attendant Connectivity Server and Session Manager can be either TCP or UDP but does not currently support a TLS connection.

2.3. Support

Technical support from Mitel can be obtained through the following.

Web: 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 2019 OS. A network telephony server and SQL were also installed on the same 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.

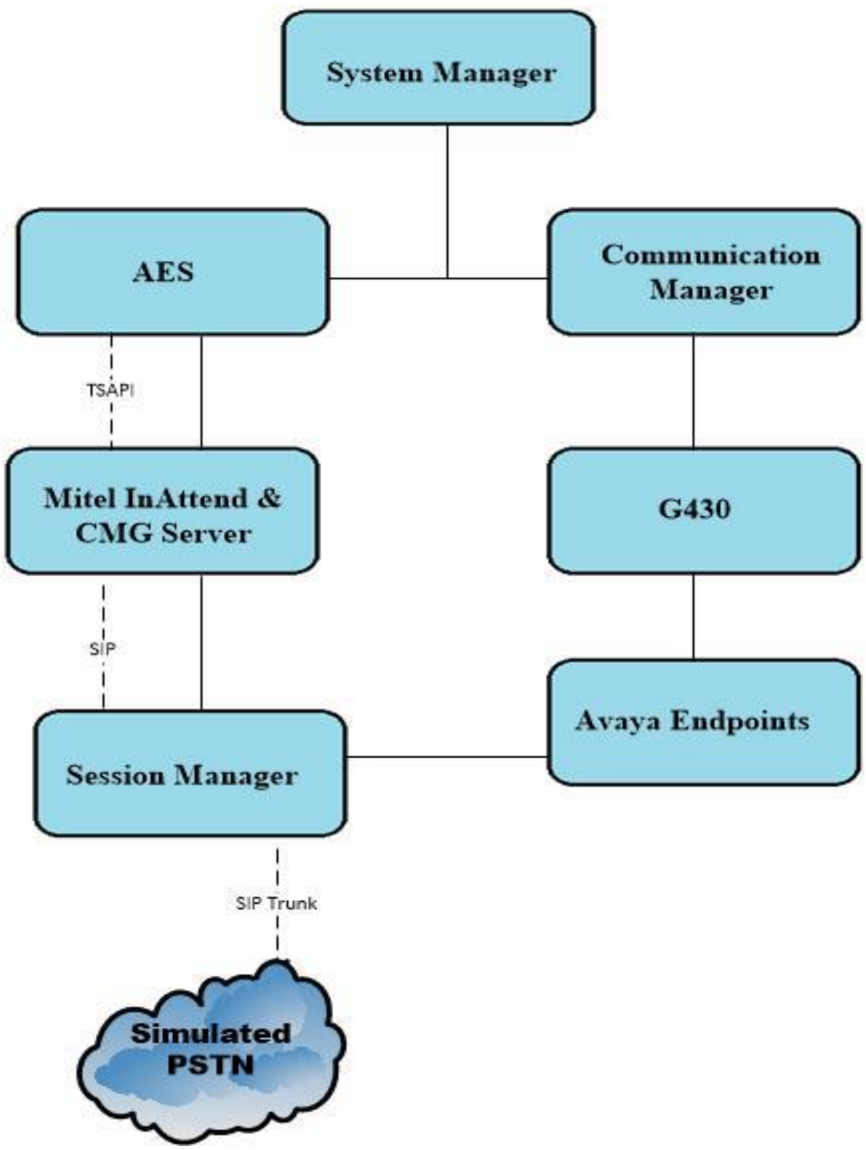


Figure 1: Avaya Aura® Communication Manager and Mitel InAttend configuration

4. Equipment and Software Validated

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

Avaya Equipment/Software	Release/ Version
Avaya Aura® System Manager	System Manager 10.1.3.0 Feature Pack 3 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.3.0.0715713
Avaya Aura® Session Manager	Session Manager R10.1 Build No. – 10.1.3.0.1013007
Avaya Aura® Communication Manager	R10.1.3.0 – FP3 R020x.01.0.974.0 Update ID 01.0.974.0-27893
Avaya Aura® Application Enablement Services	10.1.3 R10.1.3.0.0.11-0
Avaya Aura® Media Server	10.1.0.101
Avaya Media Gateway G450	42.7.0 /2
Avaya J100 Series (H323) Deskphone	6.8.5.3.2
Avaya J100 Series (SIP) Deskphone	4.0.14.0.7
Avaya 9404 Digital Deskphone	17.0
Avaya Session Border Controller (to facilitate simulated PSTN)	10.1
Mitel Equipment/Software	**Release/ Version**
Mitel Attendant Connectivity server running on Windows 2019 Mitel InAttend server running on Windows 2019 Mitel InAttend Attendant client running on Windows 10 Enterprise	Mitel Attendant Connectivity Server includes: NeTS 5.13.25.0 MediaServer 1.9.145.0 QueueManager 2.19.25.0 Version 2.7 Mitel InAttend Server includes: Collaboration Management 8.6 Virtual Reception 8.6 Microsoft SQL 2019 Version 2.7.28.0

Note: The Avaya Aura® platform as well as the Mitel equipment are all running on VMware.

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.

```
display system-parameters customer-options                    Page   2 of  12
                                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 4**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

```
display system-parameters customer-options                           Page   4 of  12
                                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   6 of  12
                                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
                                                       Uniform Dialing Plan? y
                    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 (**sm101x**). 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
sm101x              10.10.40.12
aespri101x          10.10.40.16
aessec101x          10.10.40.46
g450                10.10.40.15
procr               10.10.40.13
```

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 **greaneyp.sil6.avaya.com**. 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: greaneyp.sil6.avaya.com
    Name: Default region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              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 codecs 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; **G.722**, **G.711** and **G.729** were all tested. 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      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: OPUS-SWB24K                 1        20
 2: G.722-64K                   2        20
 3: G.711A           n          2        20
 4: G.711MU          n          2        20
 5: G.729A           n          2        20

     Media Encryption                   Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
```

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 **sm101x**).
- Ensure that the recommended TLS port value of **5062** 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: sm101x
 Near-end Listen Port: 5062                   Far-end Listen Port: 5062
                                        Far-end Network Region: 1

Far-end Domain: greaneyp.sil6.avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  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  4
                                TRUNK GROUP

Group Number: 1                   Group Type: sip           CDR Reports: y
  Group Name: SIP TRK                    COR: 1        TN: 1     TAC: *801
   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  4
      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  4
                                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

                                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
                                   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
```

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   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length 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 **4**xxx 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.

```
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        lev0         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 IP addresses by using the command **display node-names ip** and noting the IP address for the **procr** and the AES.

```
display node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
sm101x              10.10.40.12
aespri101x          10.10.40.16
aessec101x          10.10.40.46
g450                10.10.40.15
procr               10.10.40.13
```

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      Enabled      Local        Local       Remote       Remote
  Type                     Node         Port        Node         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 **aespri101x**.
- **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        Password          Enabled    Status
                   Server
      1:        aespri101x         ********          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
                                                                         COR: 1
     Name: aespri101x
```

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 A calls on Vector A which collects digits into VDN B 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 3082                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                         Extension: 3082                       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 3084** and this will use Vector **21**. This VDN is then referenced in **Section 8.5**.

```
add vdn 3084                                               Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                         Extension: 3084                       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 3084                     cov n if unconditionally
05
06
07
08
09
10
```

VDN 3084 uses the following Vector which simply provides **ringback** to the user while the VDN is being monitored.

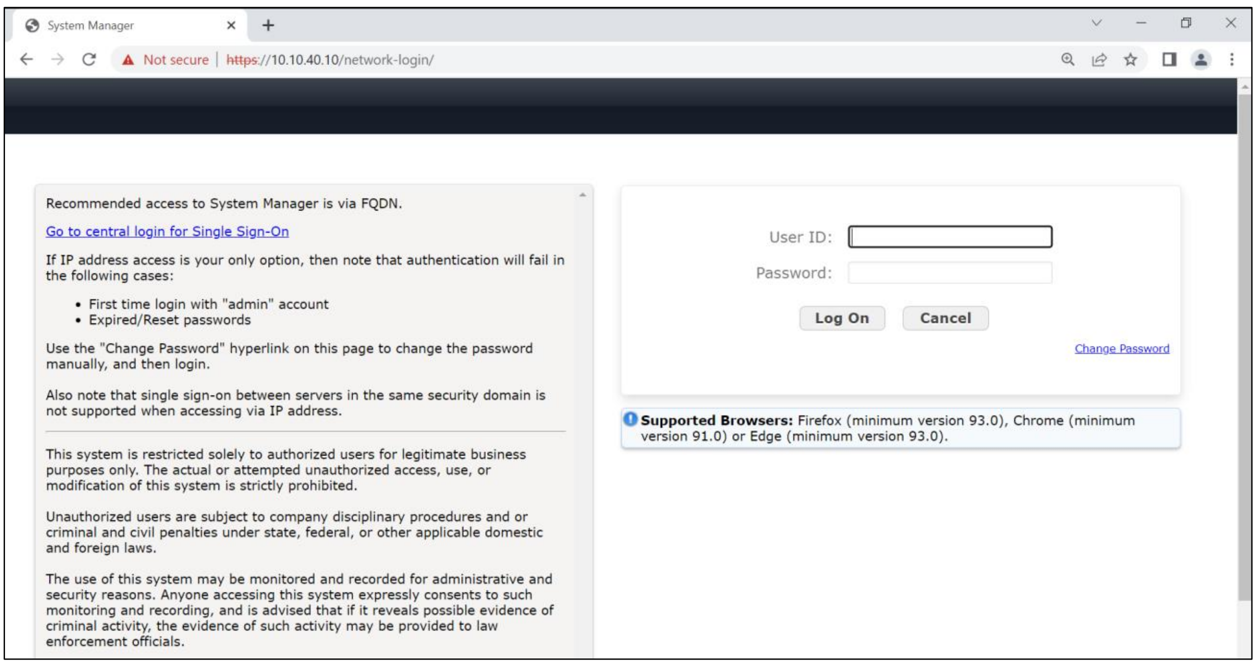
```
change vector 21                                             Page   1 of   6
                                  CALL VECTOR

    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

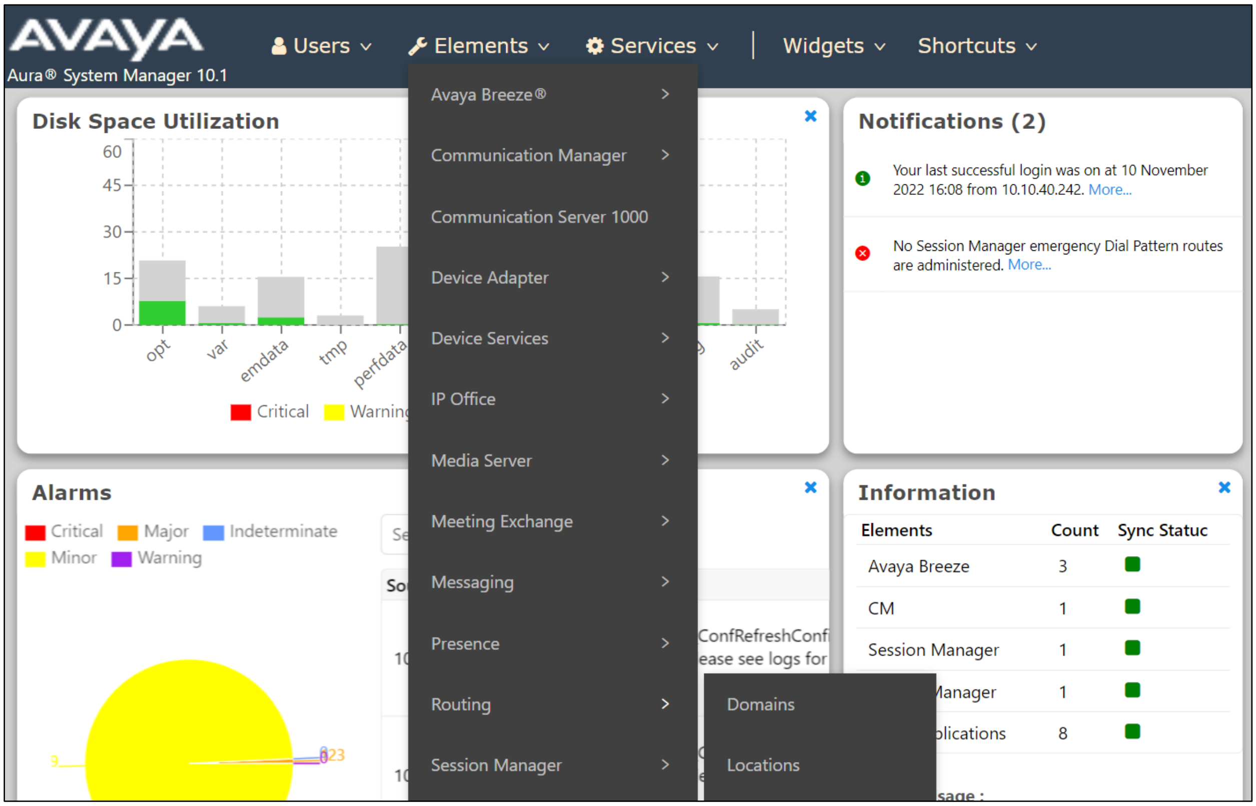
This section provides the procedures for configuring Session Manager to add the SIP Entity and routing to allow calls route to and from Mitel InAttend. Session Manager is configured via System Manager. The procedures include the following areas:

- 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**.



Once logged in navigate to **Elements** and click on **Routing**, as shown below.

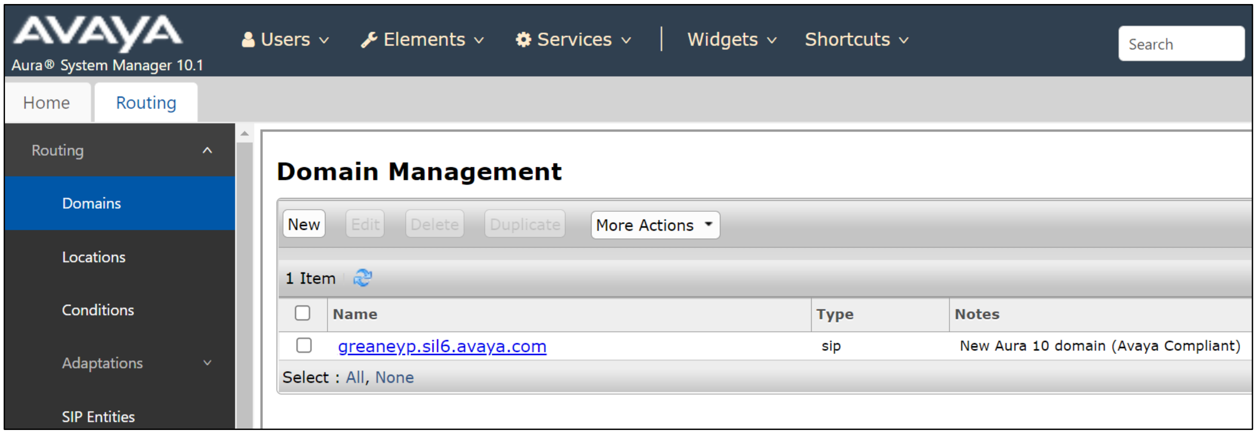


6.1. Domains and Locations

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.

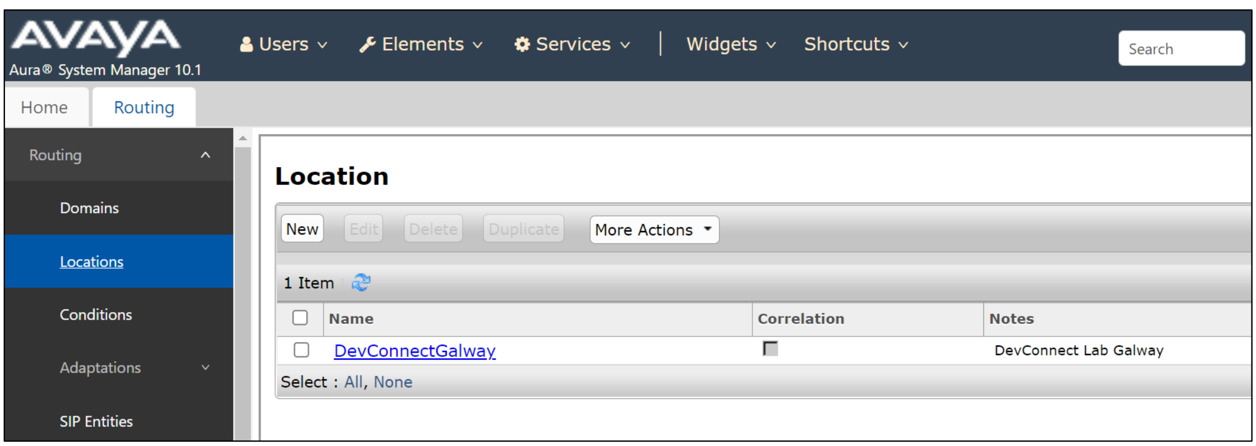
6.1.1. Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **greaneyp.sil6.avaya.com** 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.



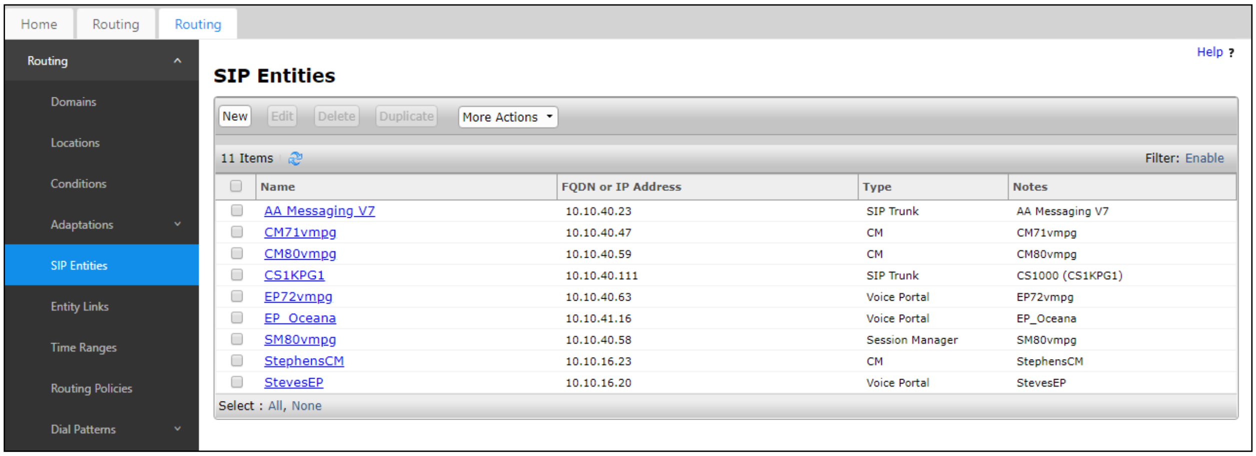
6.1.2. Display the Location

Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectGalway** 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.

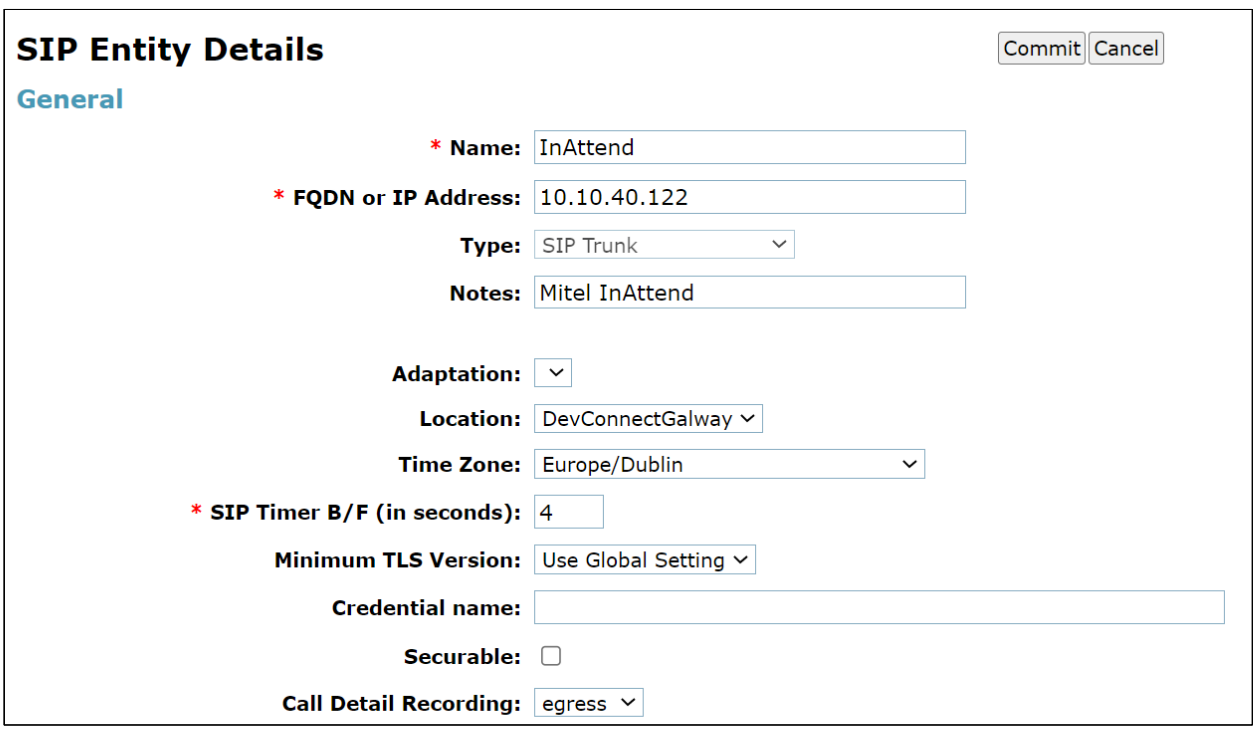


6.2. Configure Mitel InAttend SIP Entity

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.



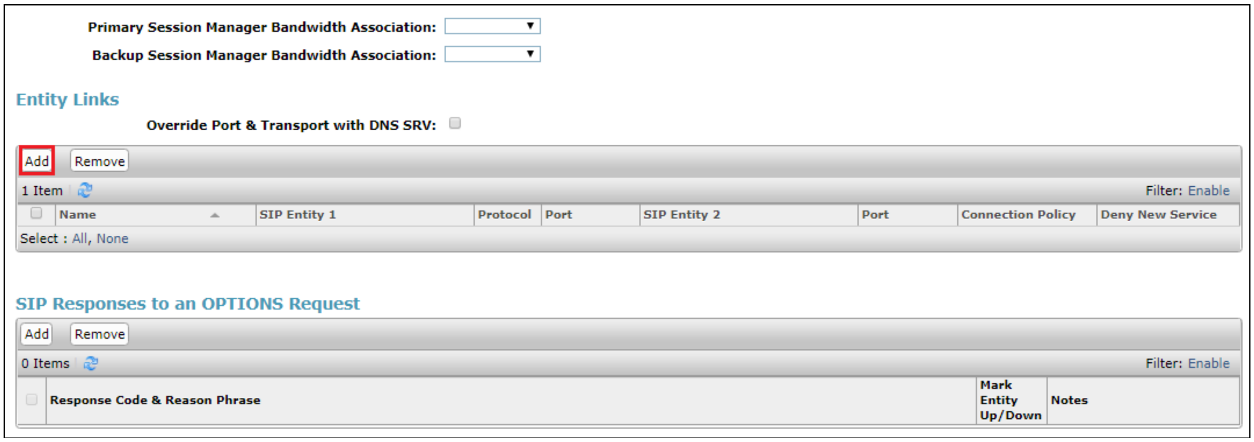
Enter a suitable **Name** for the new SIP Entity and the **IP Address** of the ACS. Enter the correct **Time Zone** and **Location** and scroll down to SIP Entity Links.



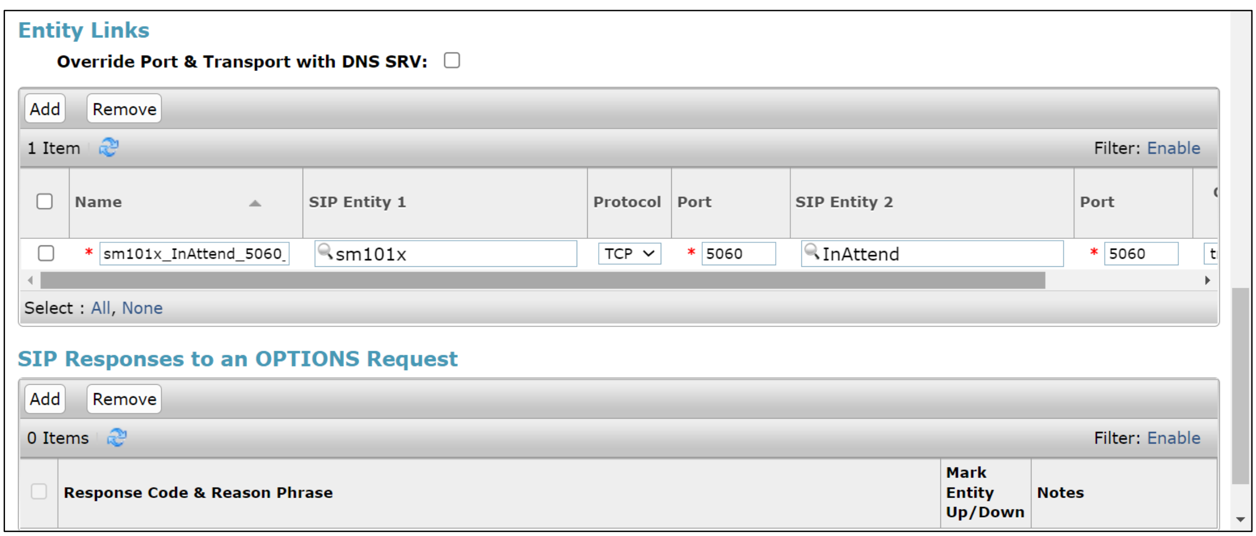
6.3. Configure Mitel InAttend SIP Entity Link

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**.

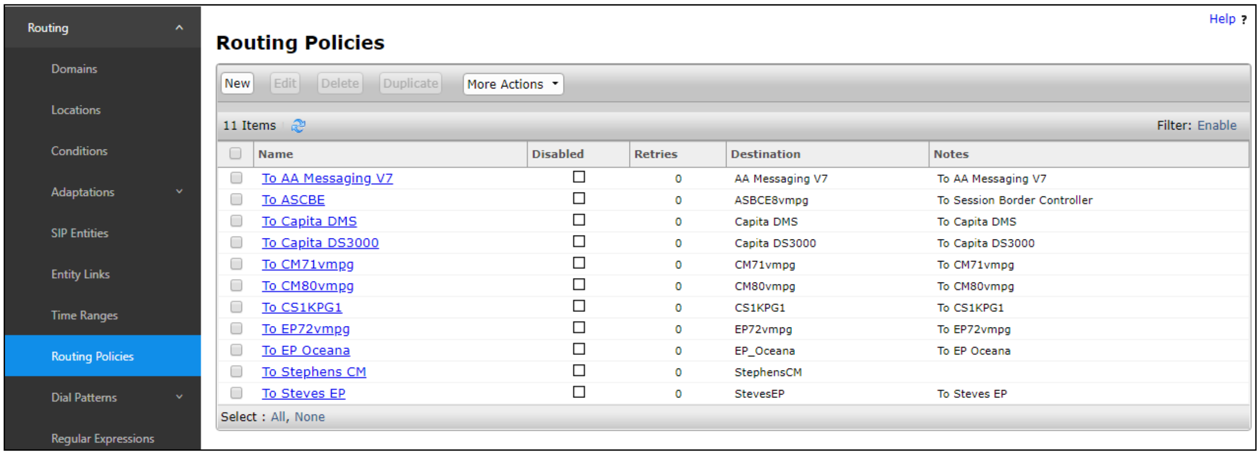


Enter a suitable **Name** for the Entity Link and select the **Session Manager** SIP Entity for **SIP Entity 1** and the newly created InAttend SIP Entity for **SIP Entity 2**. Ensure that **TCP** is selected for the **Protocol** and that **Port 5060** is used. Click on **Commit** once finished to save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

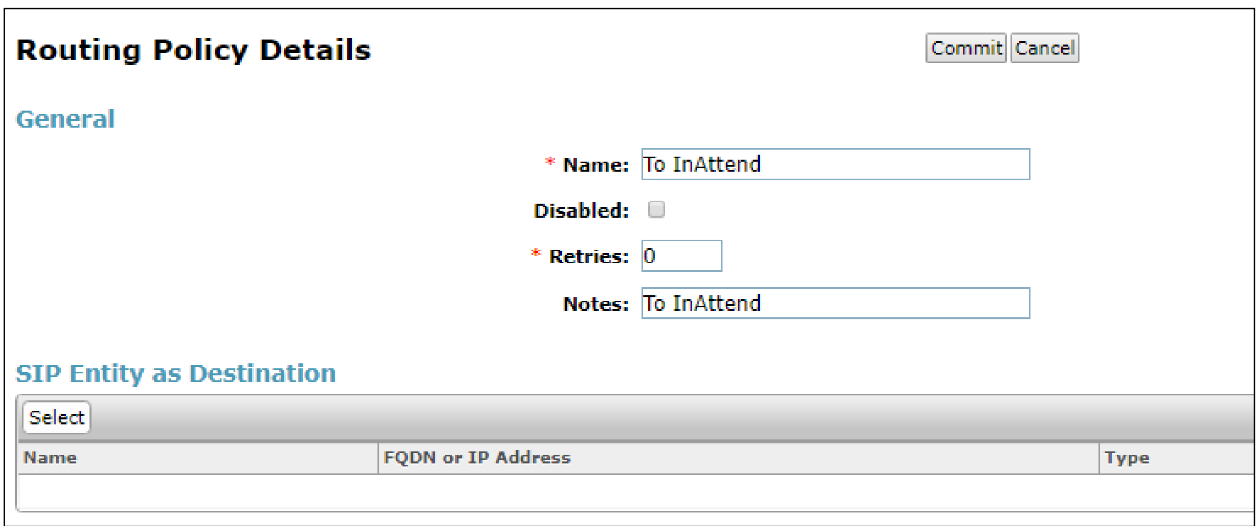


6.4. Configure Routing Policy for Mitel InAttend

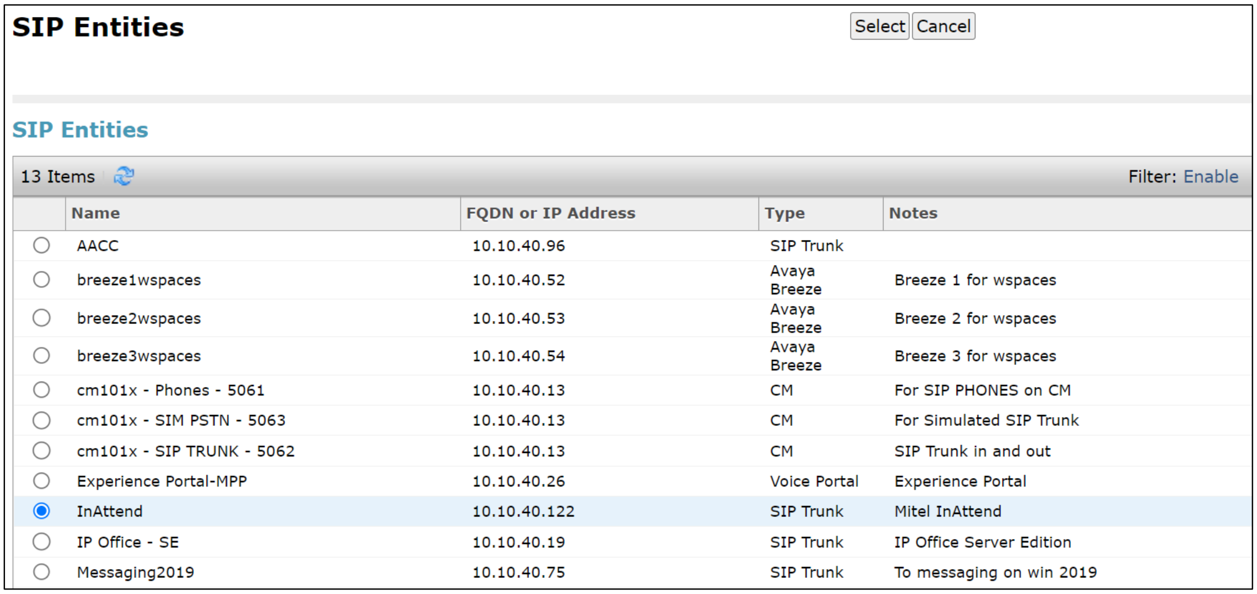
Click on **Routing Policies** in the left window and select **New** in the main window.



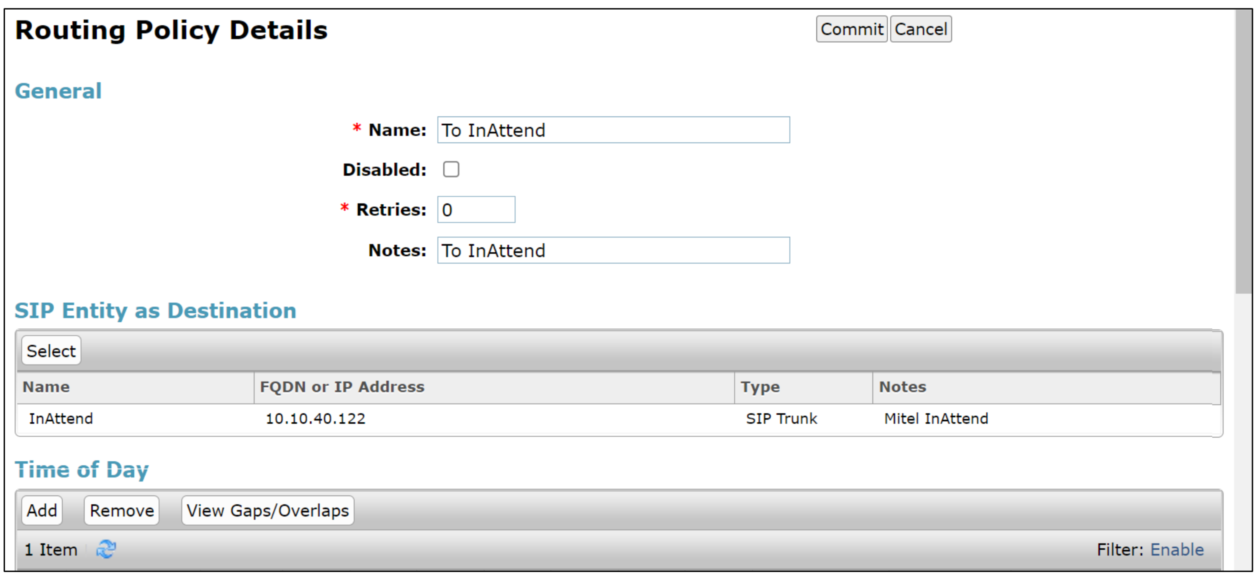
Enter a suitable **Name** for the Routing Policy and click on **Select** under **SIP Entity as Destination**, highlighted on next page.



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

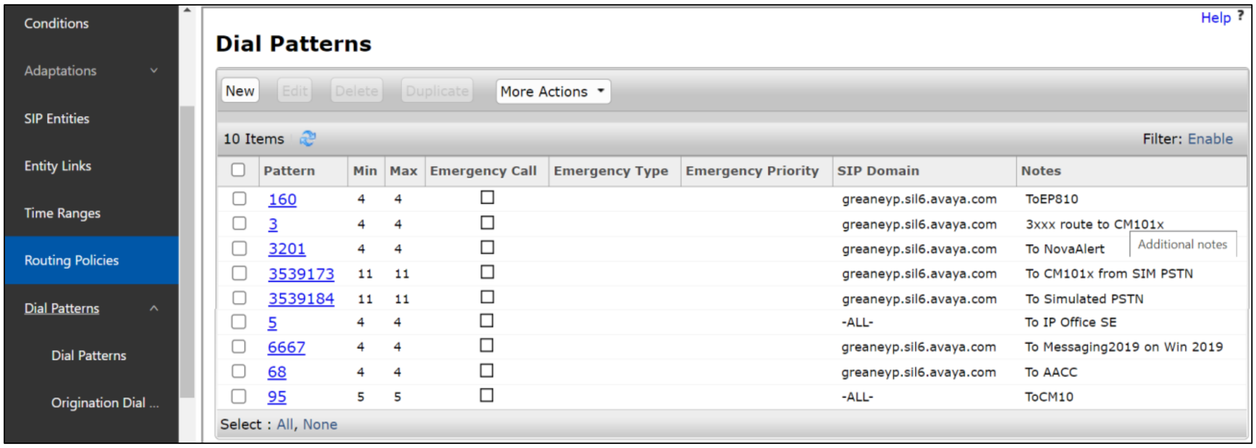


The selected destination is now shown, click on **Commit** to save this.

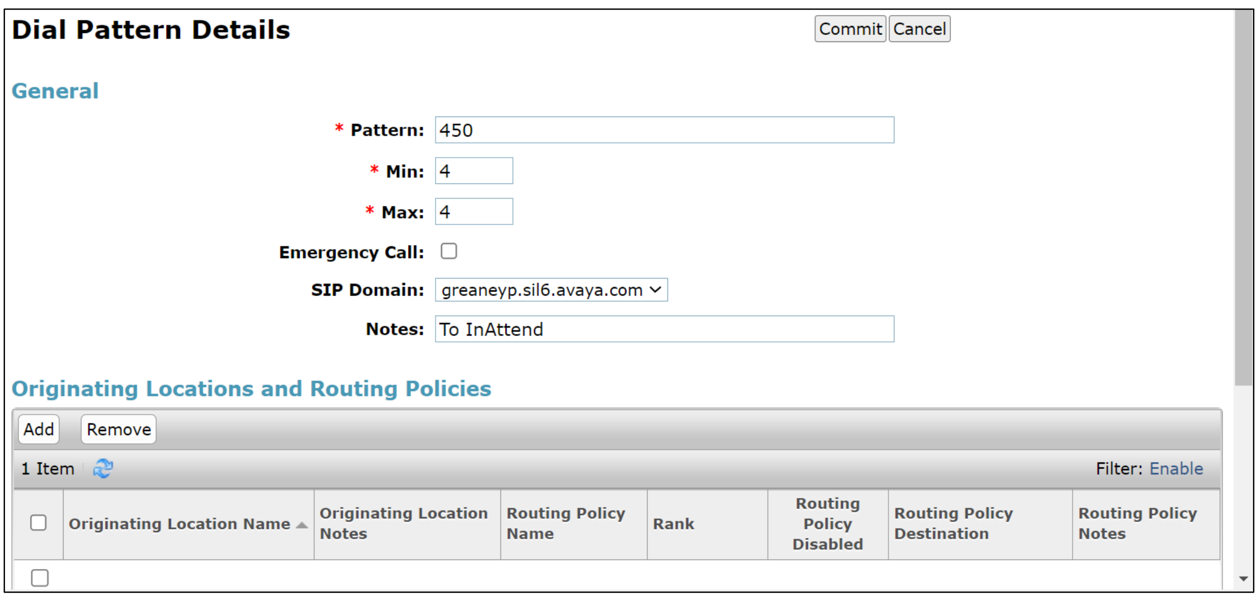


6.5. Configure Mitel InAttend Dial Pattern

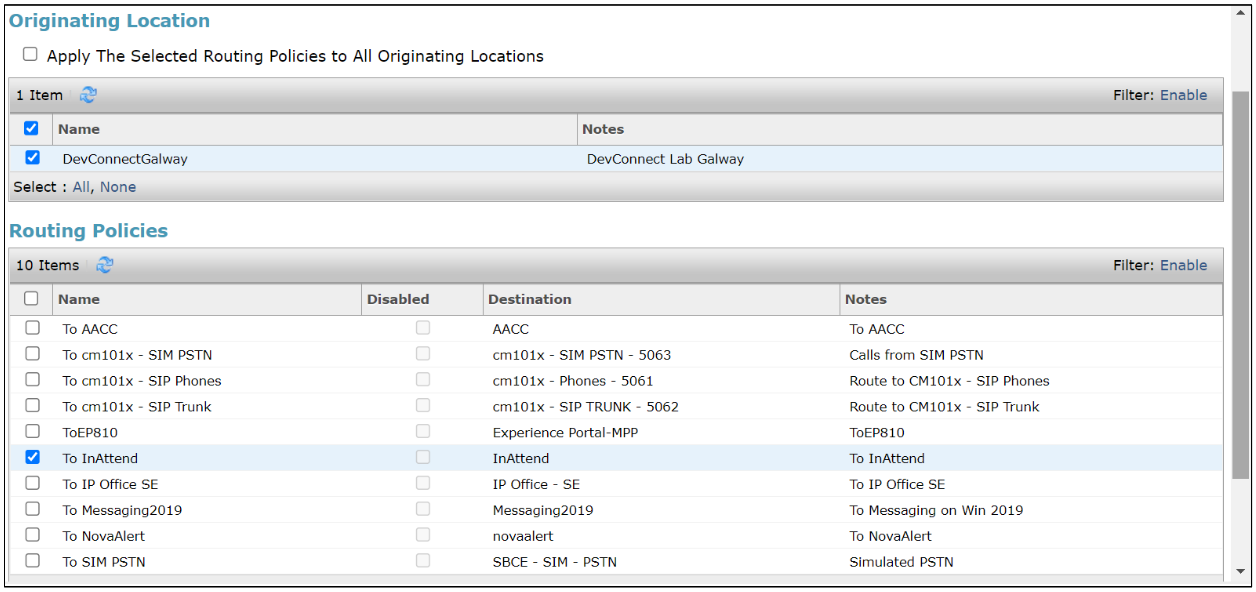
Select **Dial Patterns** in the left window and select **New** in the main window.



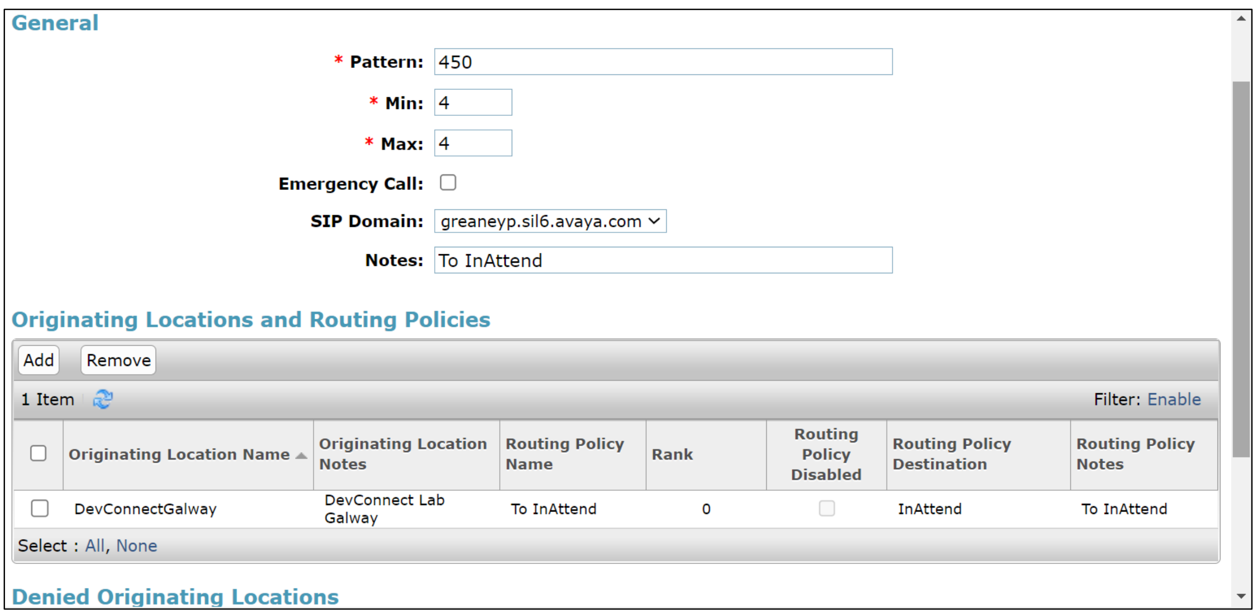
Enter the required digits for the Routing Pattern, in the example below **450** is used. This ensures that when 450x is dialled it will route to the ACS. Enter the appropriate domain for **SIP Domain** in this example the domain created in **Section 6.1.1** is added. Click on **Add** under **Originating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



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



With the Routing Policy selected, click on **Commit** (not shown) to finish adding the Dial Pattern.



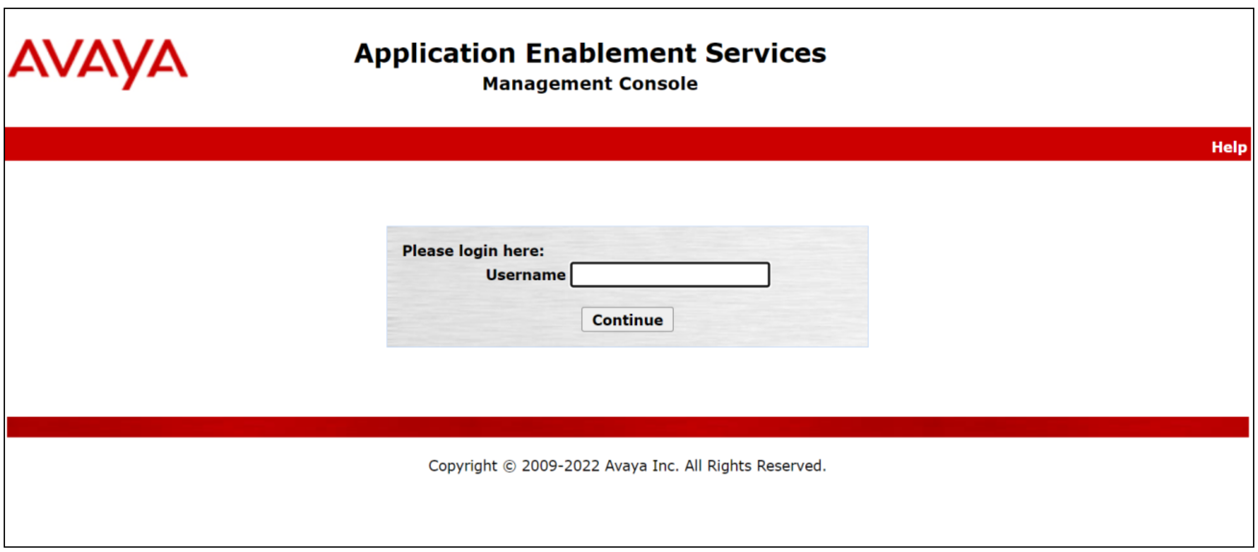
7. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services (AES). The procedures fall into the following areas:

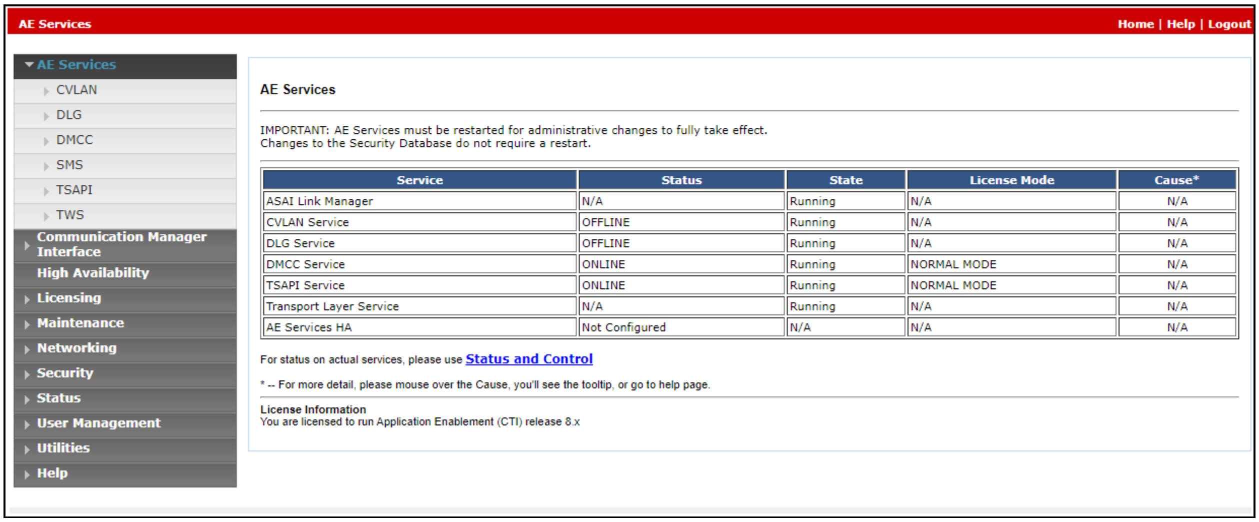
- Verify Licensing
- Switch Connection
- Administer TSAPI Link
- Identify Tlinks
- Enable TSAPI Ports
- Create CTI User
- Configure Security
- Restart AE Server

7.1. Verify Licensing

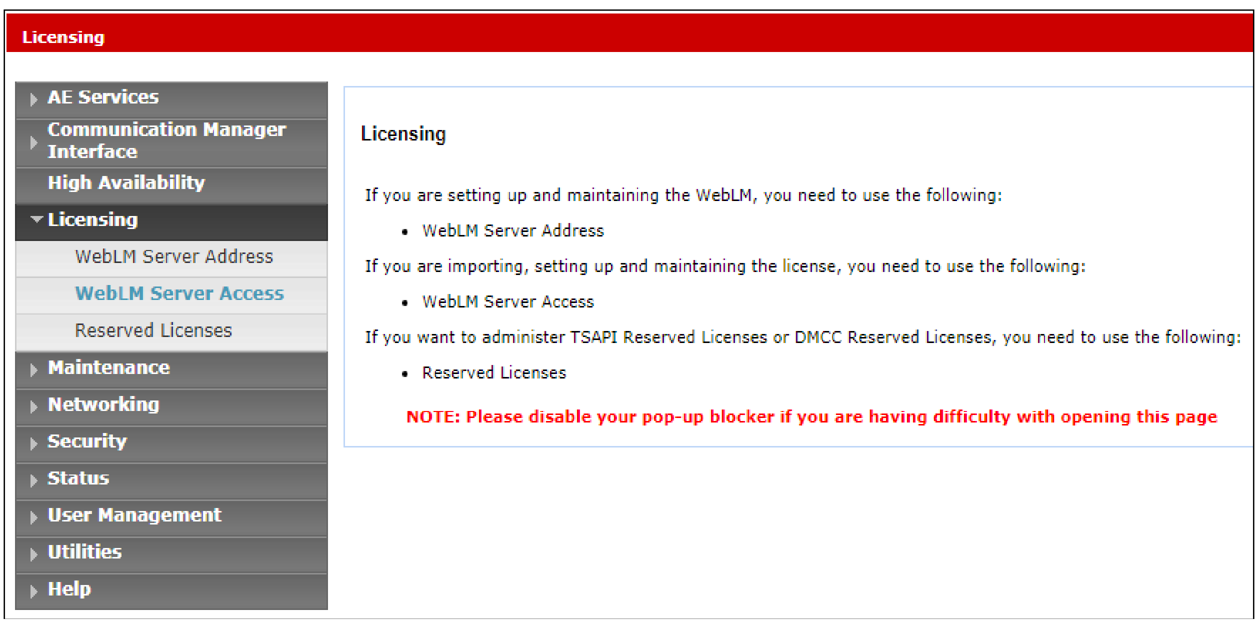
To access the AES Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of the AES. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.



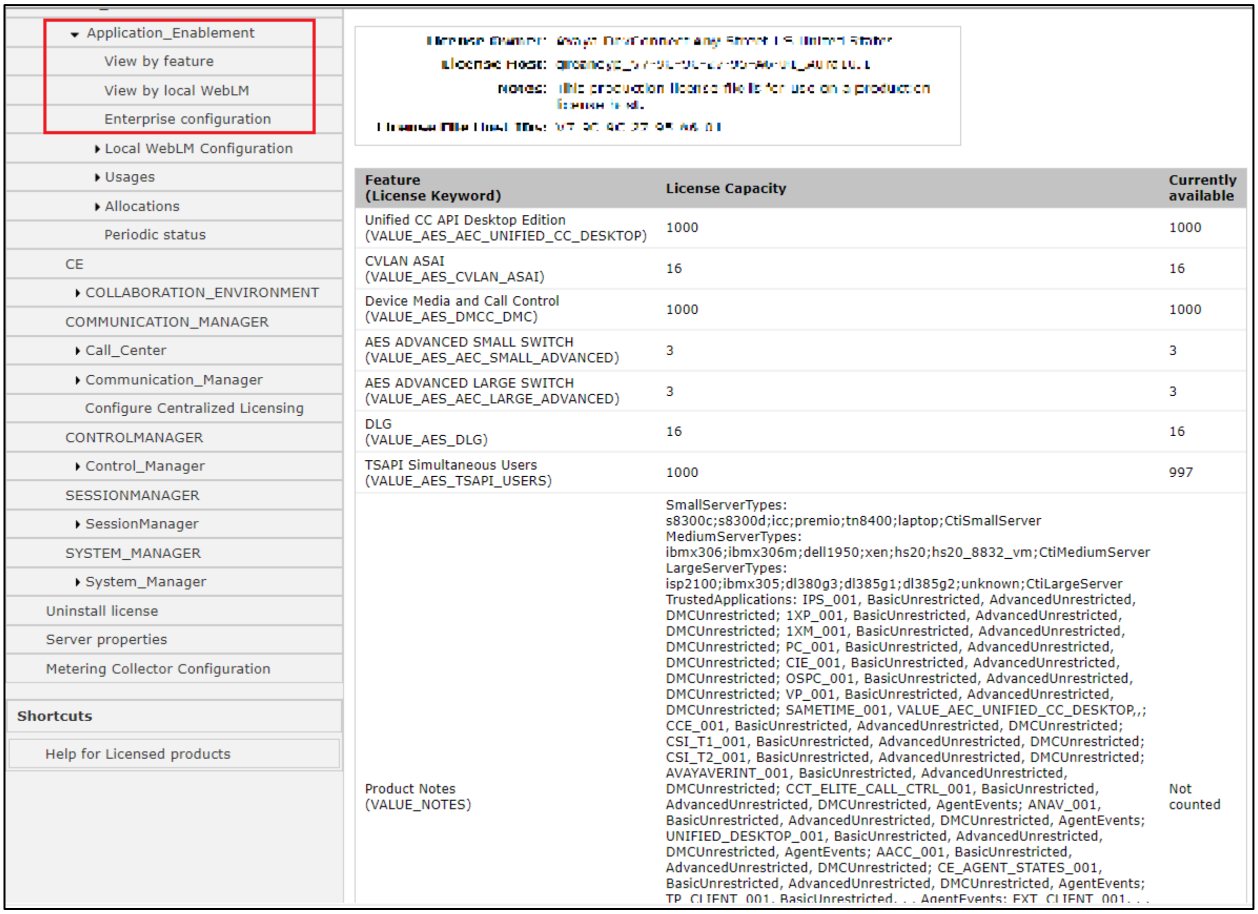
The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL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



The TSAPI licenses are user licenses issued by the Web License Manager to which the Application Enablement Services server is pointed to. From the left window open **Licensing** and click on **WebLM Server Access** as shown below.

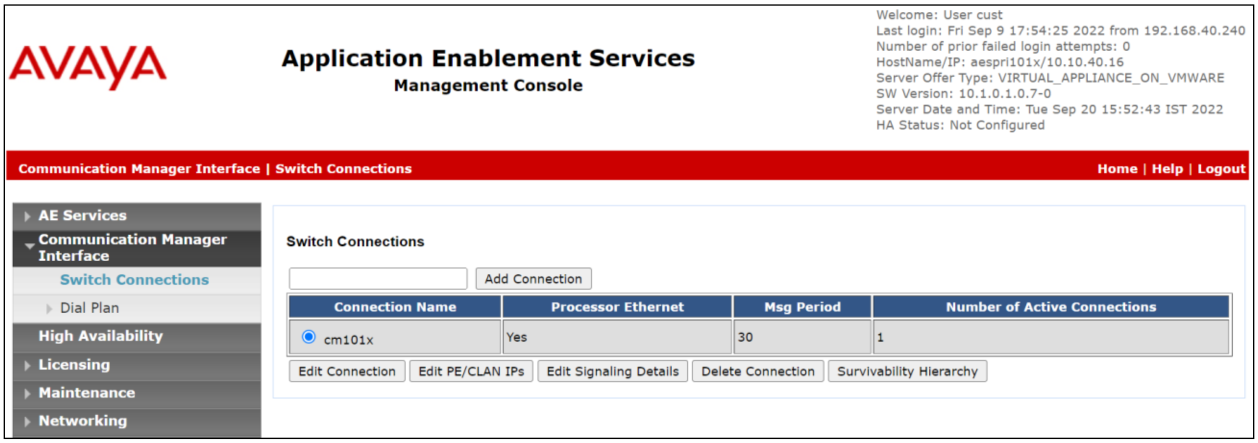


The following screen shows the available licenses for **TSAPI** users.

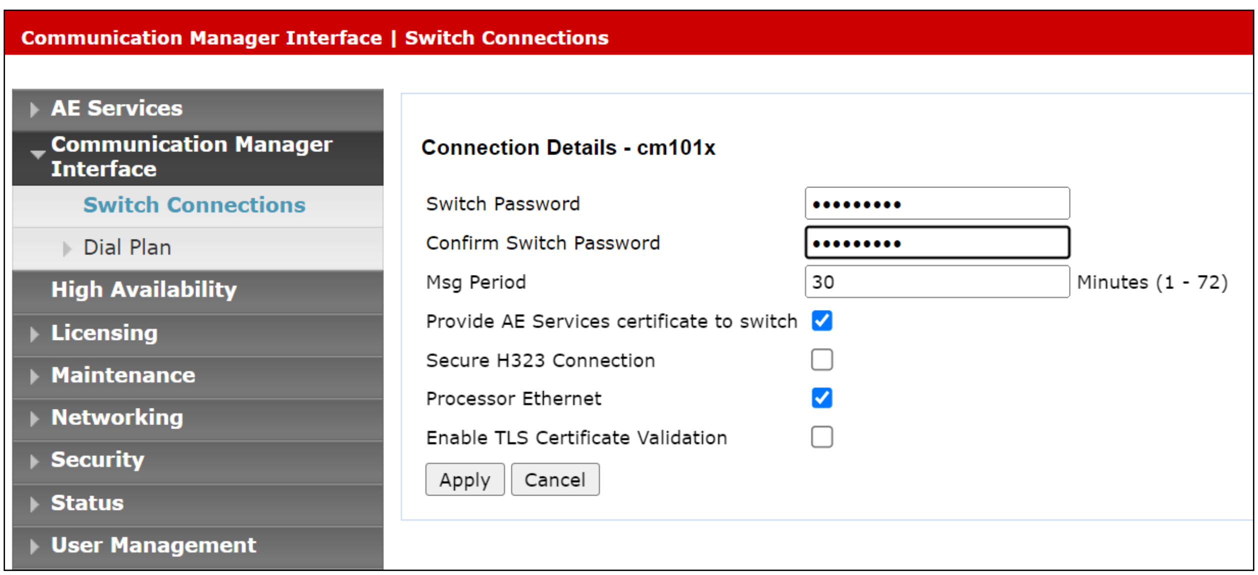


7.2. Create Switch Connection

Typically, the connection between the Application Enablement Services and Communication Manager is setup as part of the initial installation and would not usually be outlined in these Application Notes. From the AES Management Console navigate to **Communication Manager Interface → Switch Connections**, the connection to Communication Manager should be present as shown below but if one is not present one can be added by clicking on **Add Connection**.

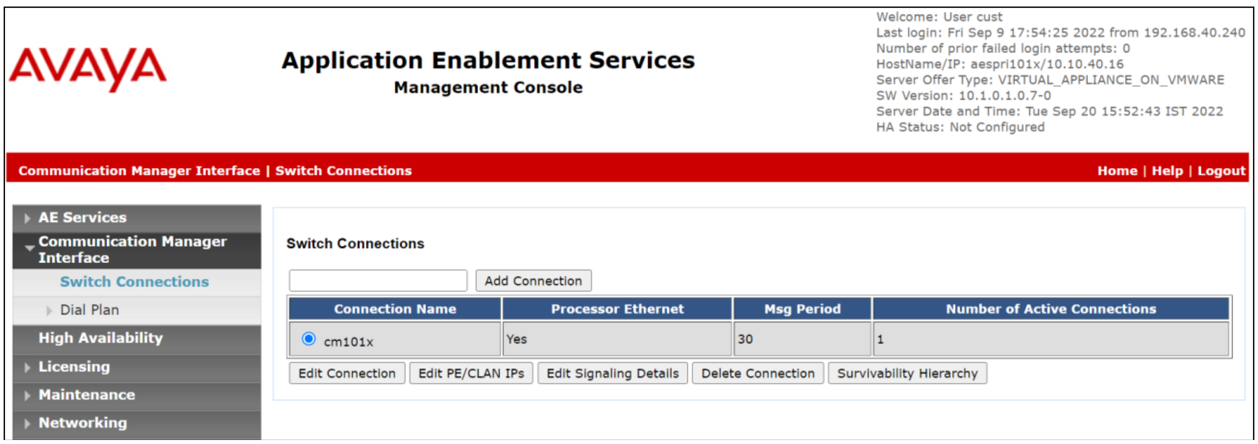


In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.4.2**. **Secure H323 Connection** was left unticked, as shown below. Click **Apply** to save changes.

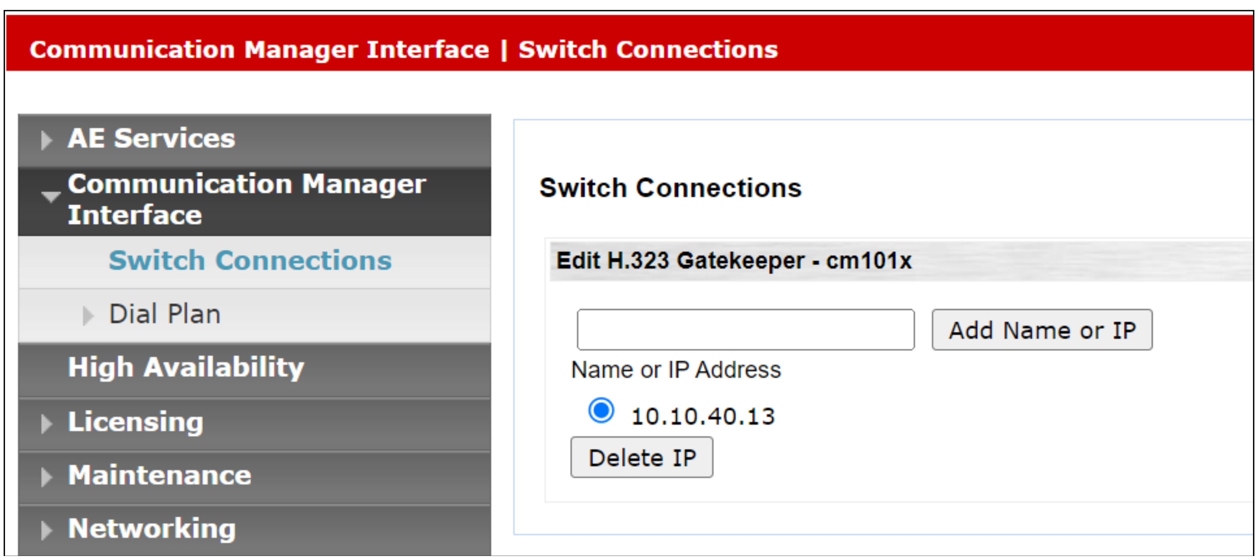


From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button (not shown), see screen at the bottom of the previous page. In the resulting screen, enter the IP address of the procr, as shown in **Section 5.4.1**, that will be used for the AES connection and select the **Add/Edit Name or IP** button.

Clicking on **Edit Signaling Details** below brings up the H.323 Gatekeeper page.

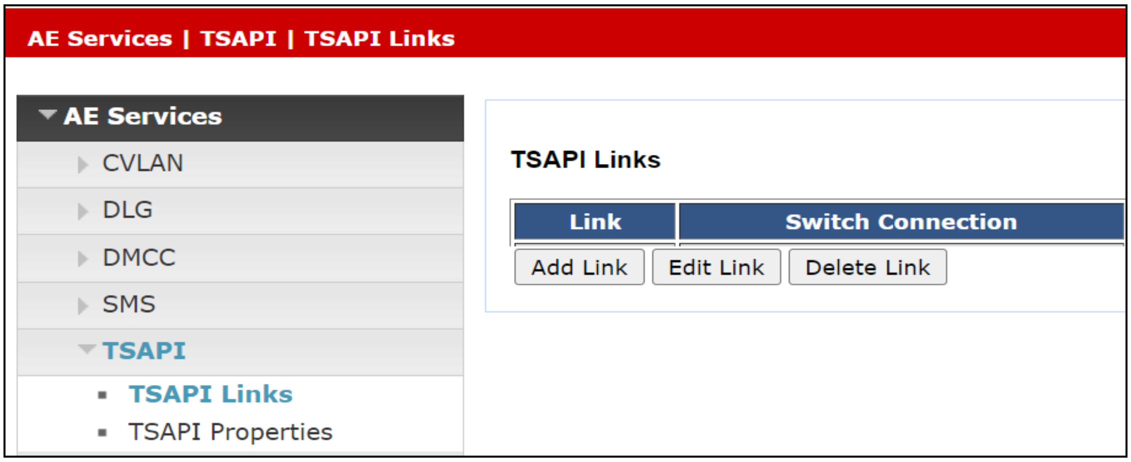


The IP address of Communication Manager is set for the **H.323 Gatekeeper**, as shown below.



7.3. Administer TSAPI link

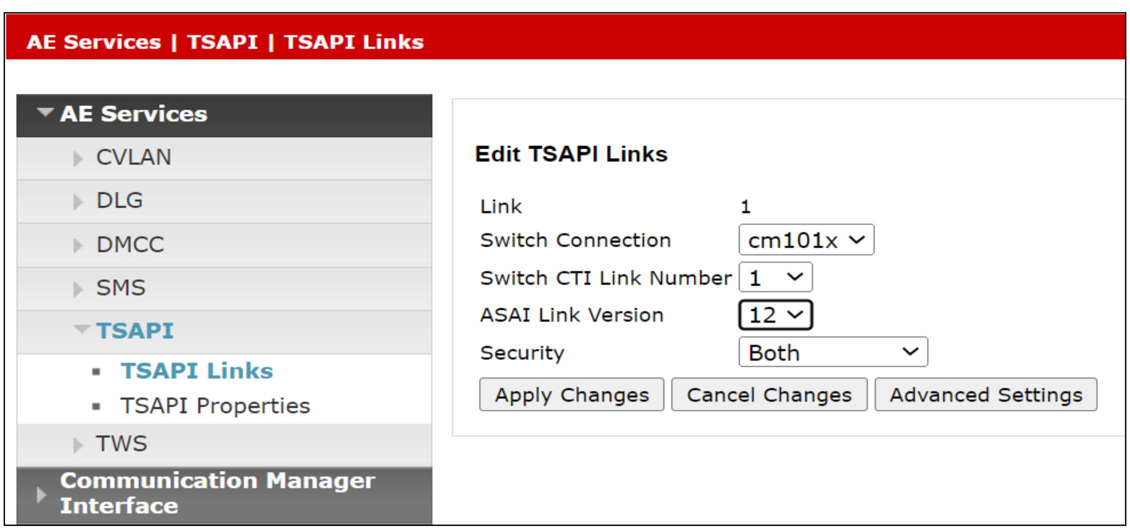
From the Application Enablement Services Management Console, select **AE Services → TSAPI → TSAPI Links**. Select **Add Link** button as shown in the screen below.



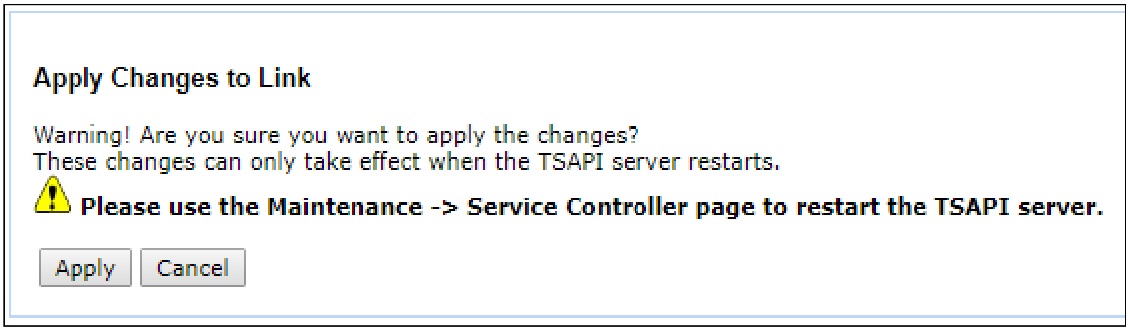
On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm101x**, 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: 12** was used for compliance testing but the latest version available can be chosen).
- **Security:** This can be left at the default value of **Both**.

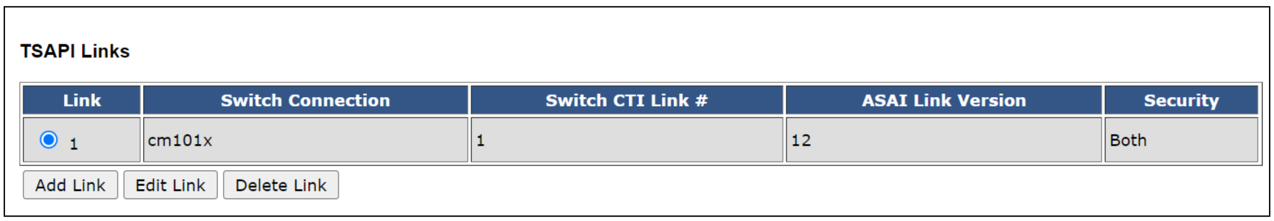
Once completed, select **Apply Changes**.



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

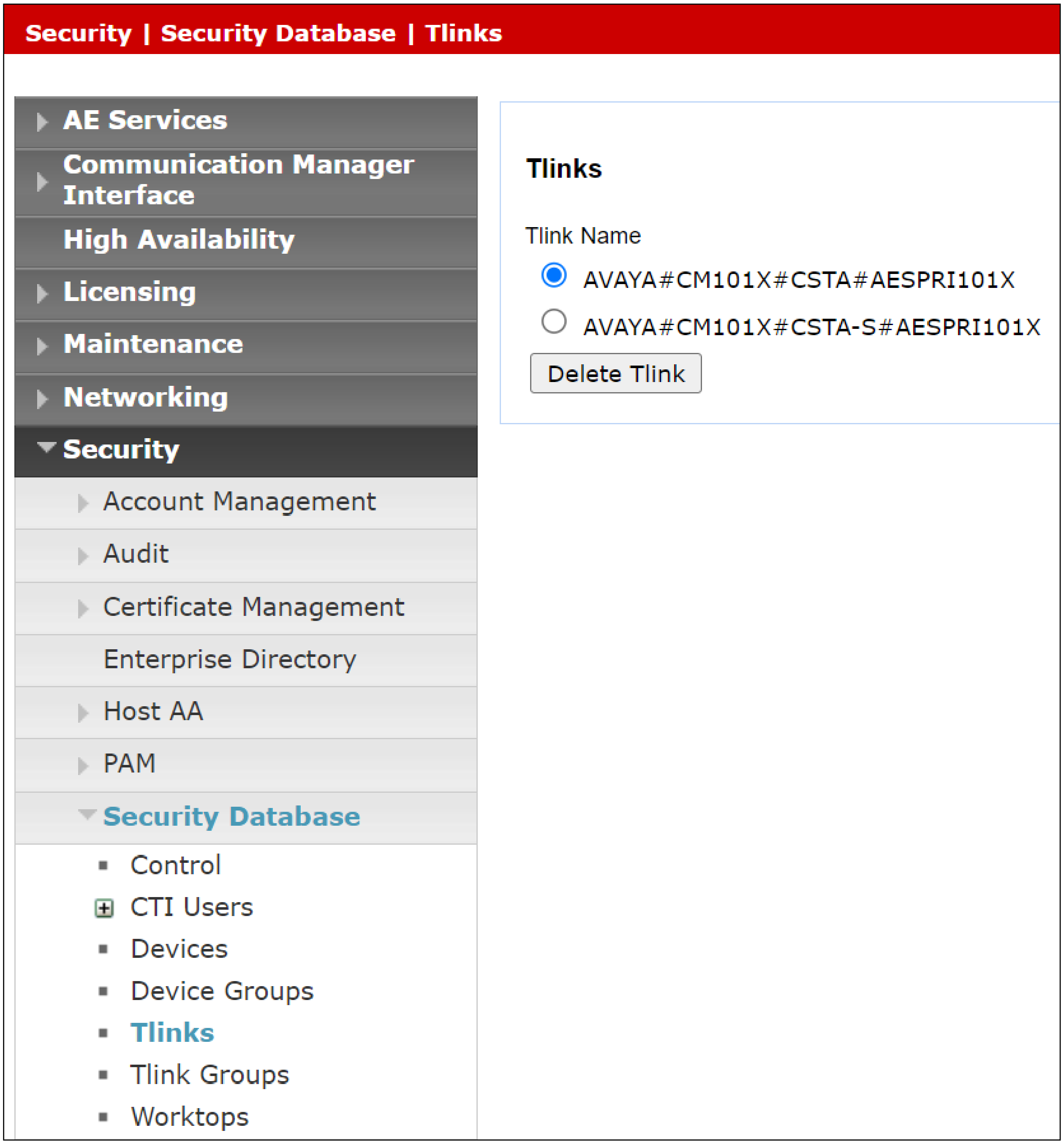


When the TSAPI Link is completed, it should resemble the screen below.



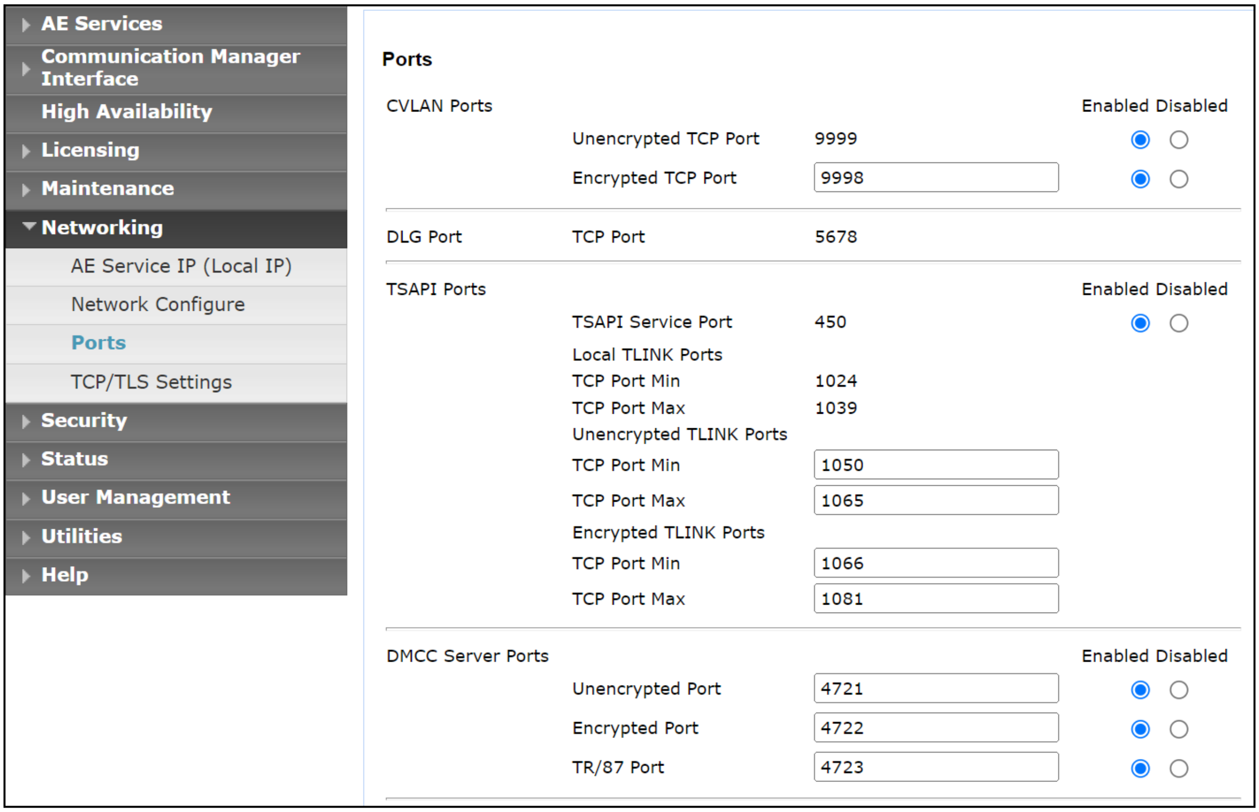
7.4. Identify Tlinks

Navigate to **Security → Security Database → Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure Mitel Collaboration Management (CMG) module in **Section 8.5**.



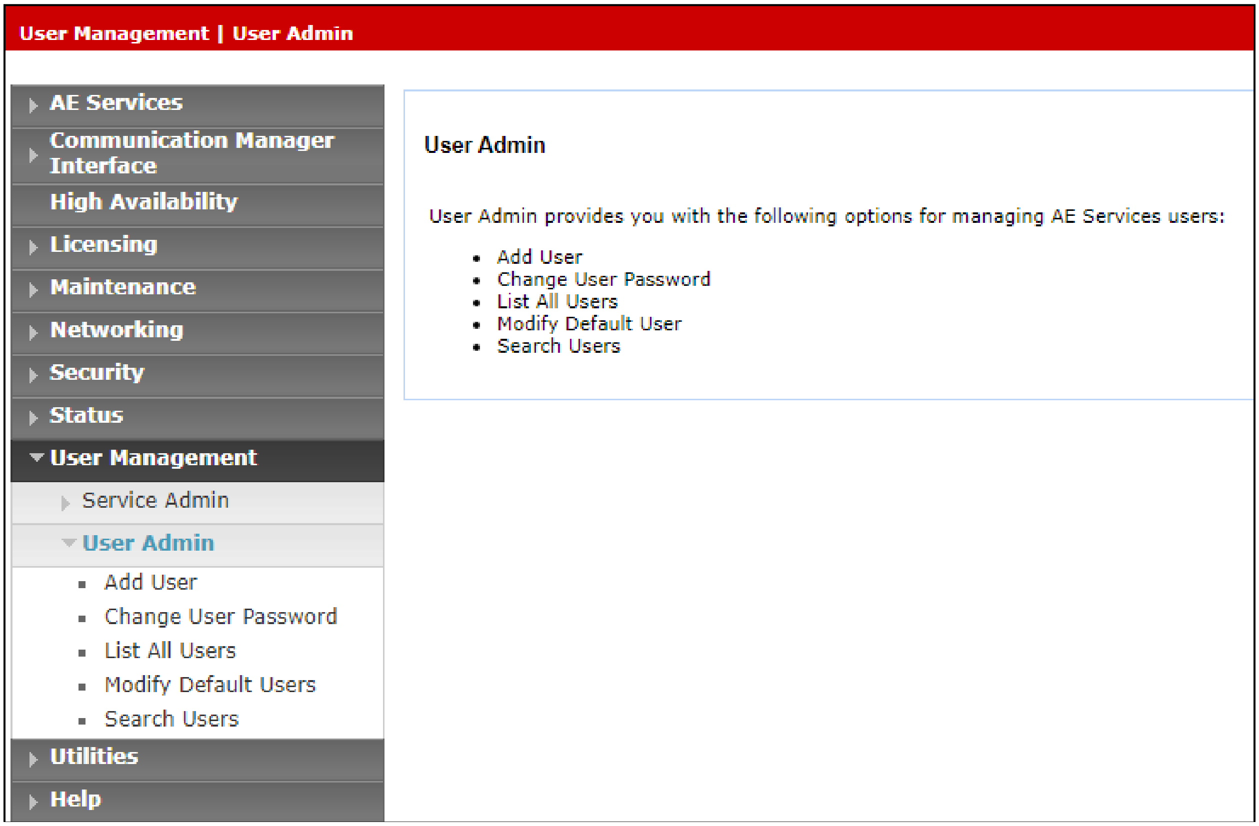
7.5. Enable TSAPI Ports

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



7.6. Create CTI User

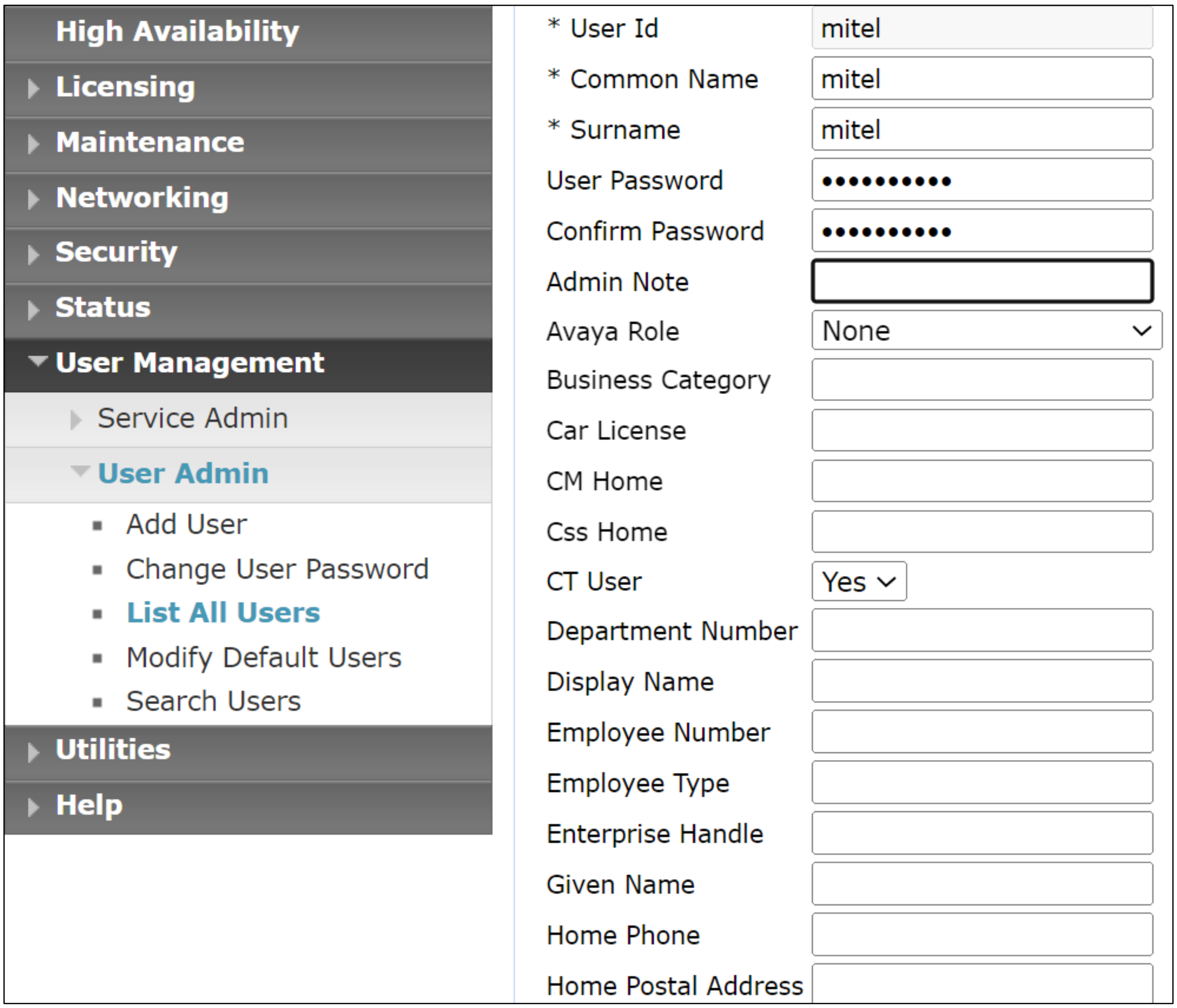
A User ID and password needs to be configured for InAttend Server module to communicate with the Application Enablement Services server. Navigate to the **User Management → User Admin** screen then choose the **Add User** option.



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

- **User Id -** This will be used by InAttend Server module in **Section 8.6**.
- **Common Name** and **Surname -** Descriptive names need to be entered.
- **User Password** and **Confirm Password -** This will be used with the InAttend Server module in **Section 8.6**.
- **CT User -** Select **Yes** from the drop-down menu.

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



7.7. Configure Security

The CTI user permissions and the database security are set under **Security Database**.

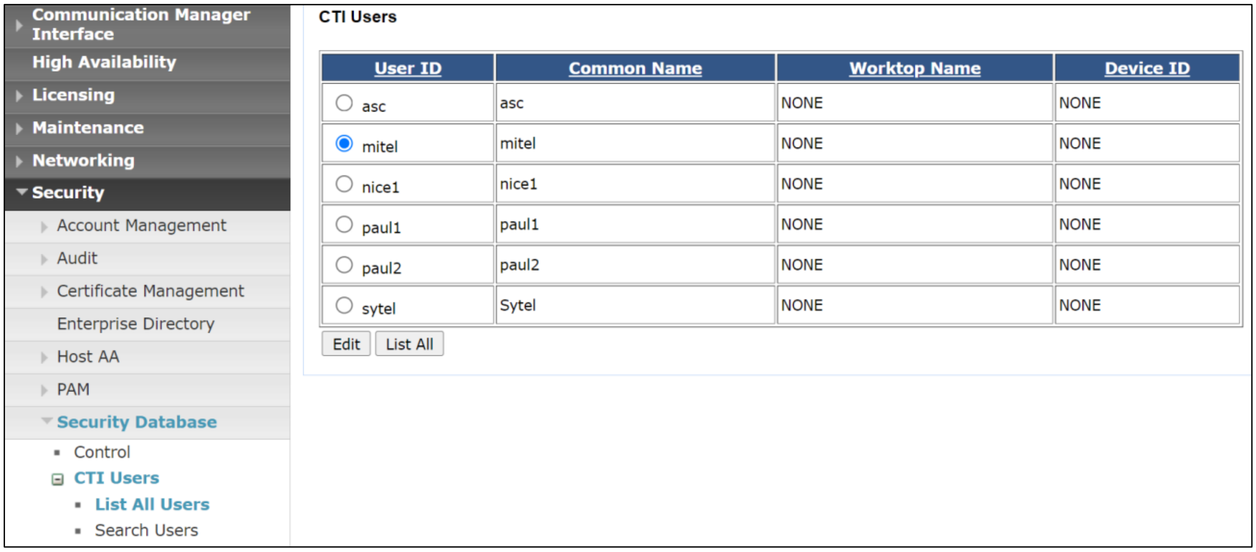
7.7.1. Configure Database Control

The security database can be set differently depending on the requirements of the customer in question. For compliance testing, the DevConnect lab was setup as shown below, however this may be changed by opening **Control** and ticking the boxes shown.

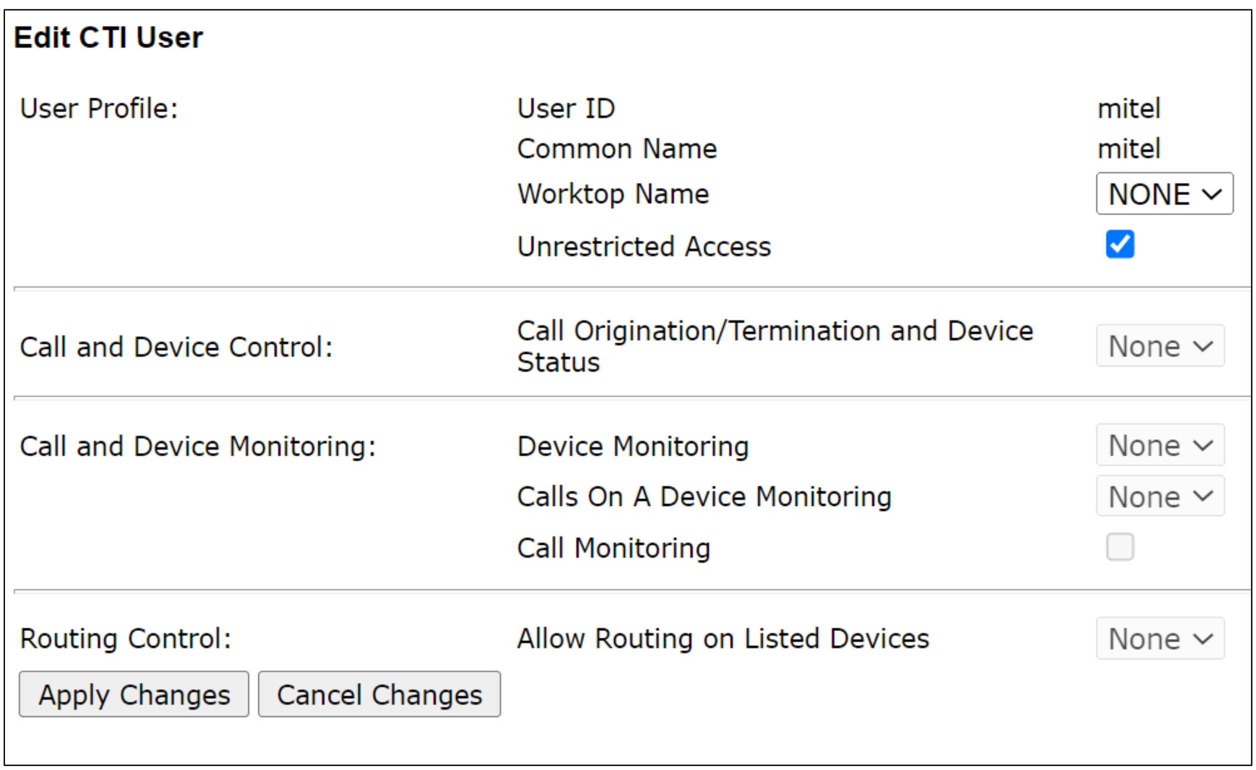
Note: The AES Security Database (SDB) provides the ability to control a user's access privileges. The SDB stores information about Computer Telephony (CT) users and the devices they control. The DMCC service, the TSAPI service, and Telephony Web Services use this information for permission checking. Please look to **Section 11** for more information on this.

7.7.2. 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**.

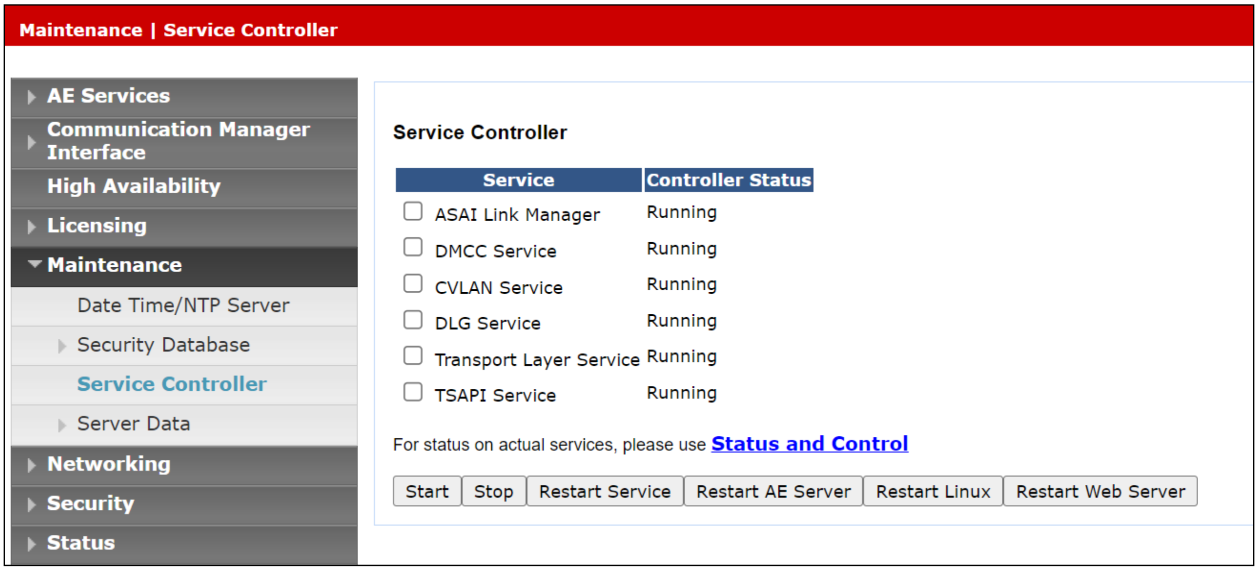


In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.

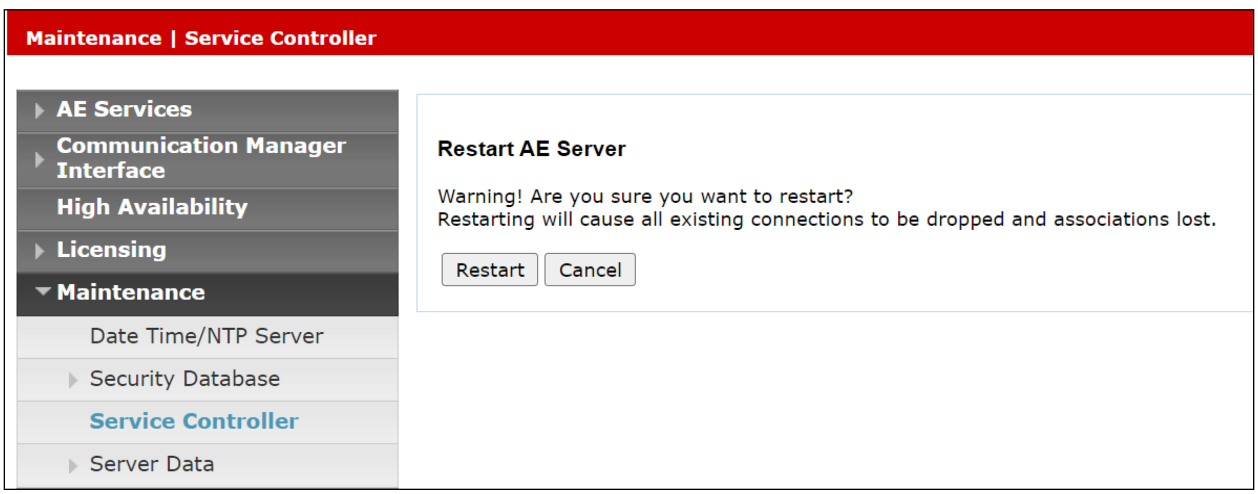


7.8. Restart AE Server

Once everything is configured correctly, it is best practice to restart AE Server (if possible), this will ensure that the new connections are brought up correctly. Click on the **Restart AE Server** button at the bottom of the screen.



A message confirming the restart will appear, click on **Restart** to proceed.

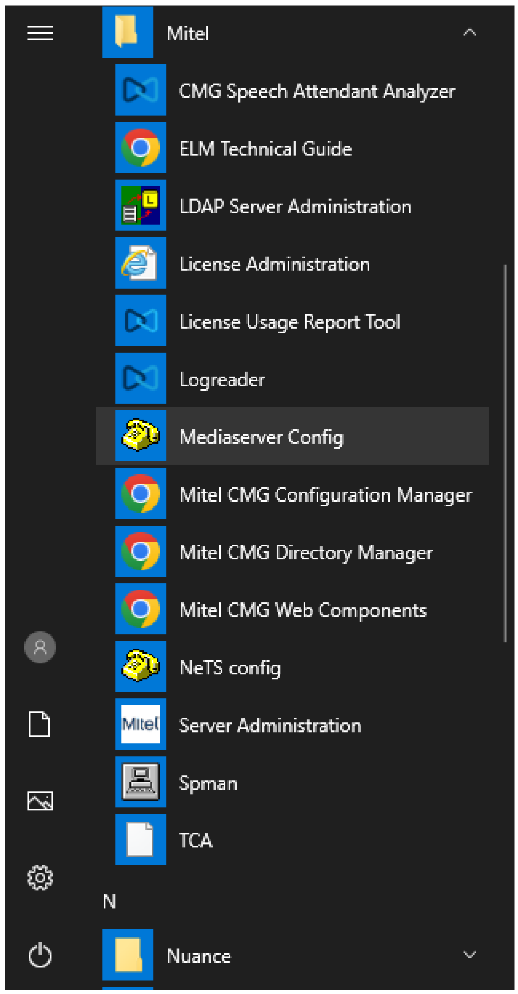


8. Configure Mitel Attendant Connectivity Server (ACS)

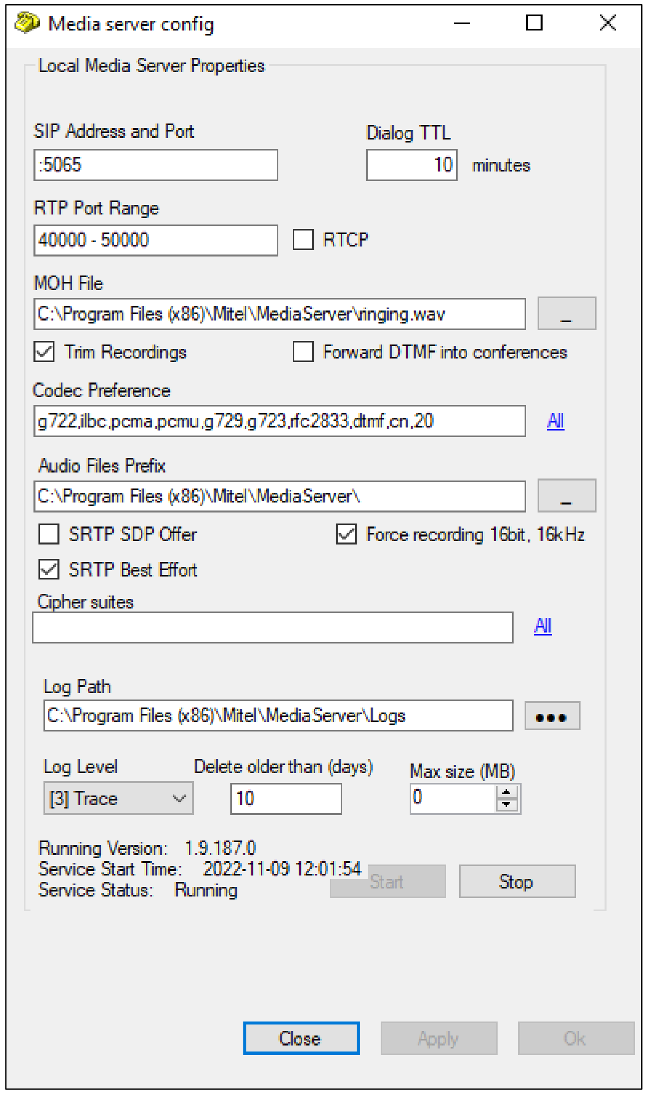
Although a Mitel engineer will setup the solution the following sections show information on the connection to Session Manager that was used for compliance testing, it may prove useful.

8.1. Mitel Media Server configuration

All Mitel applications are run from the Windows 2019 server, click on the **Mediaserver Config**, as shown below.

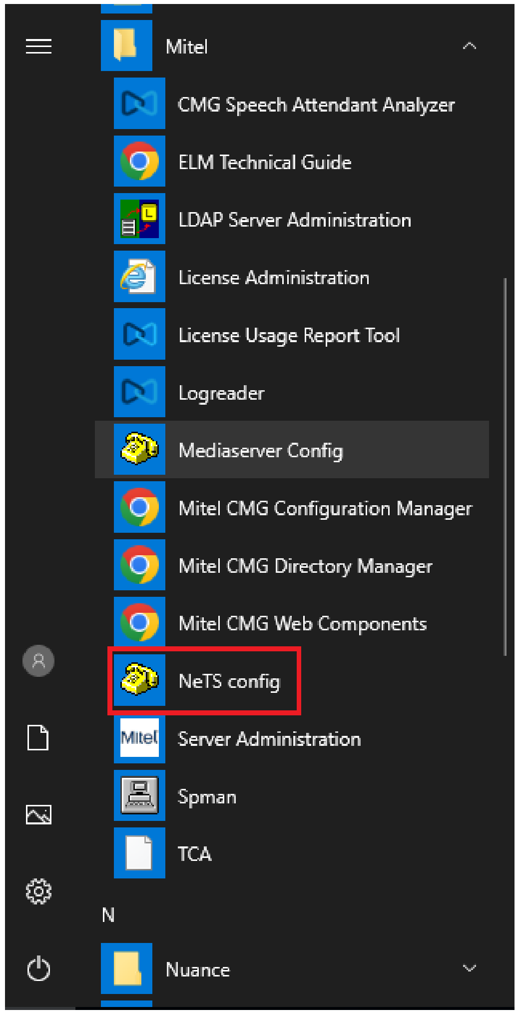


These are the settings that were used for compliance testing. Take note of the **Codec Preference** as this is where they are set. Typically, these are the default settings.

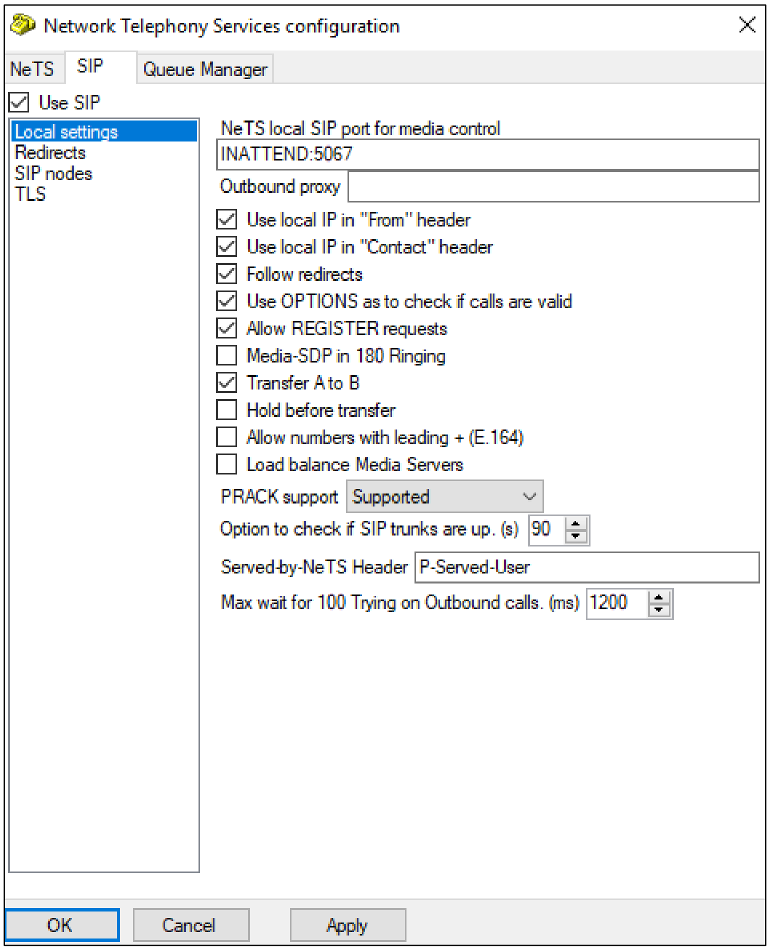


8.2. Mitel NeTS configuration

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

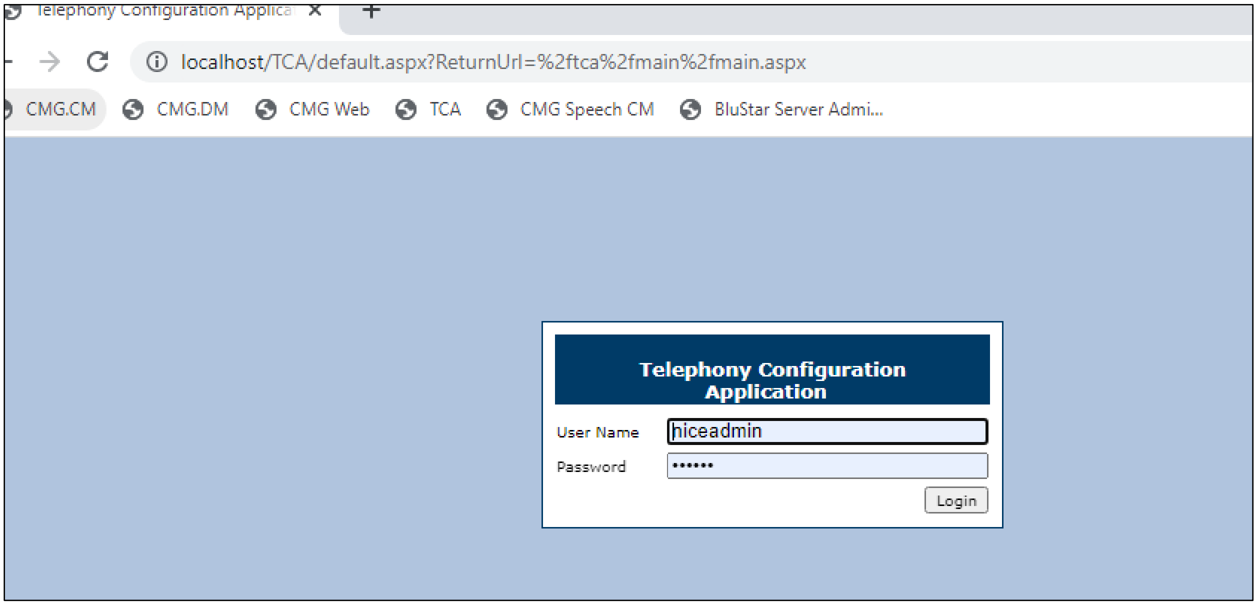


These are the settings that were used for compliance testing. The only settings that are of interest to the connection to Session Manager are found under the **SIP** tab and **Local settings**. Typically, these are the default settings.

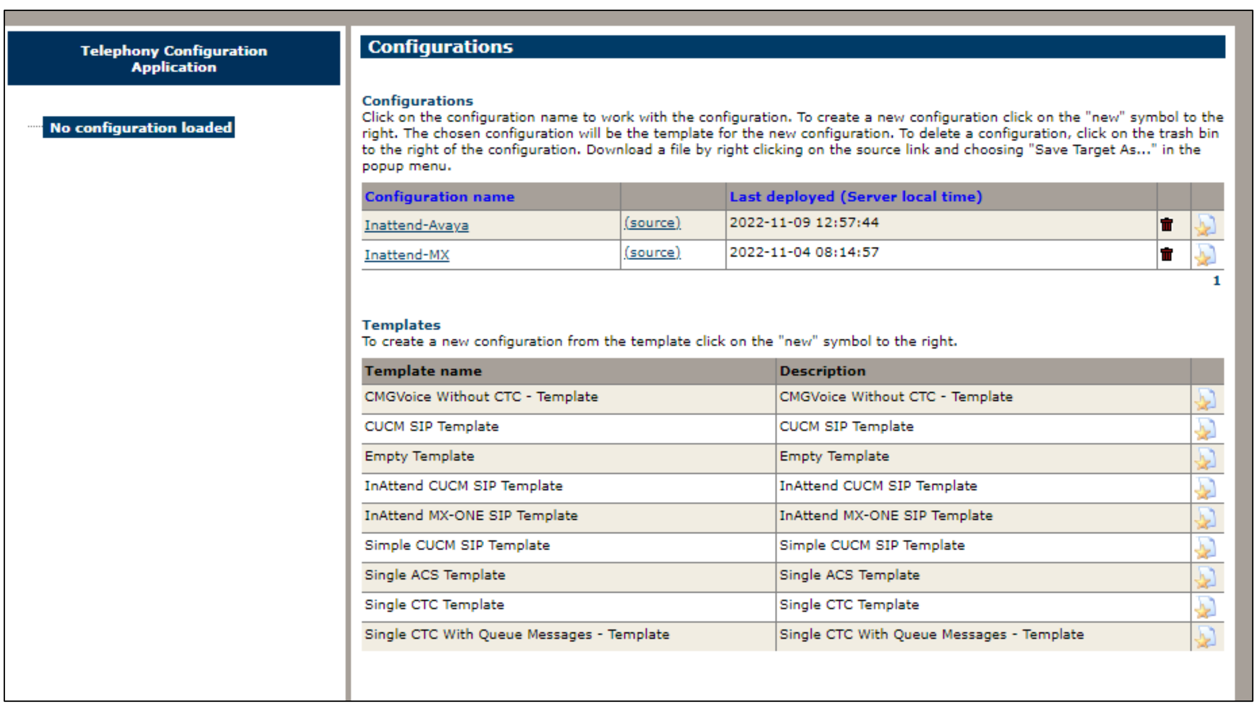


8.3. Mitel Telephony Configuration Application (TCA) configuration

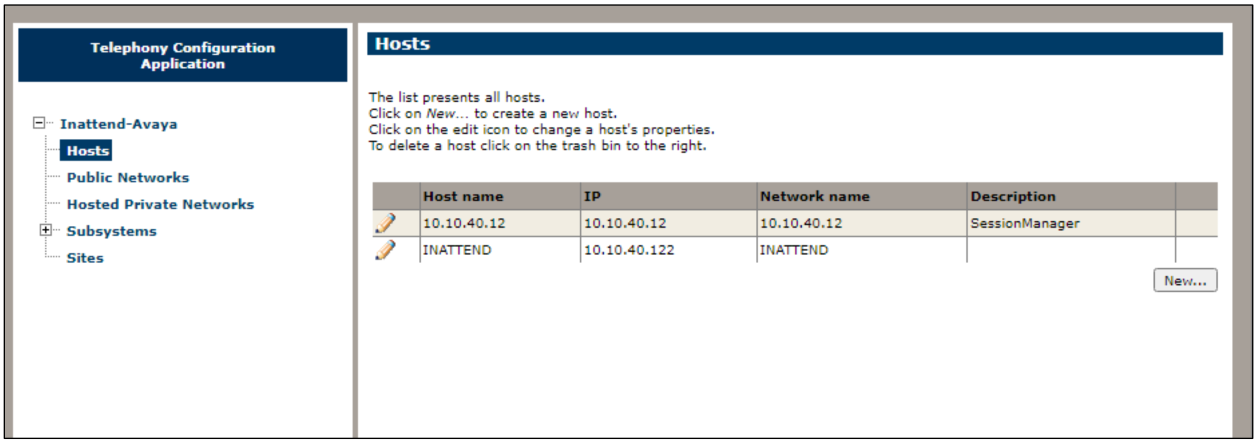
Open a web browser and browse to the ACS server name followed by TCA, for example http://<servername>/tca. Enter the appropriate credentials and click on **Login**.



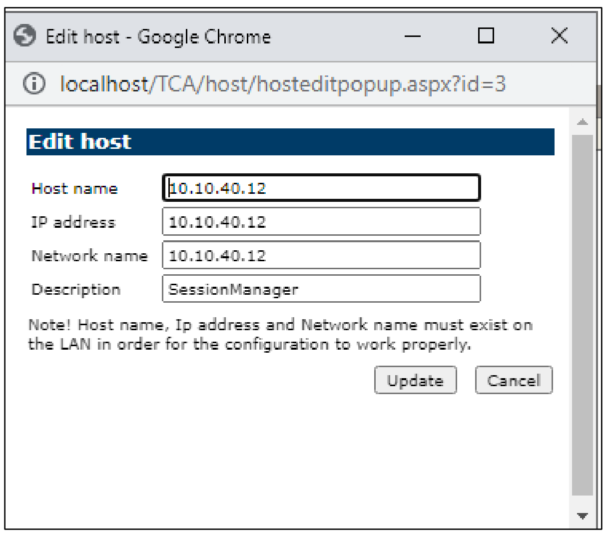
A configuration will be setup as part of the initial installation and configuration, click on that **Configuration name**, for compliance testing this was **Inattend-Avaya**.



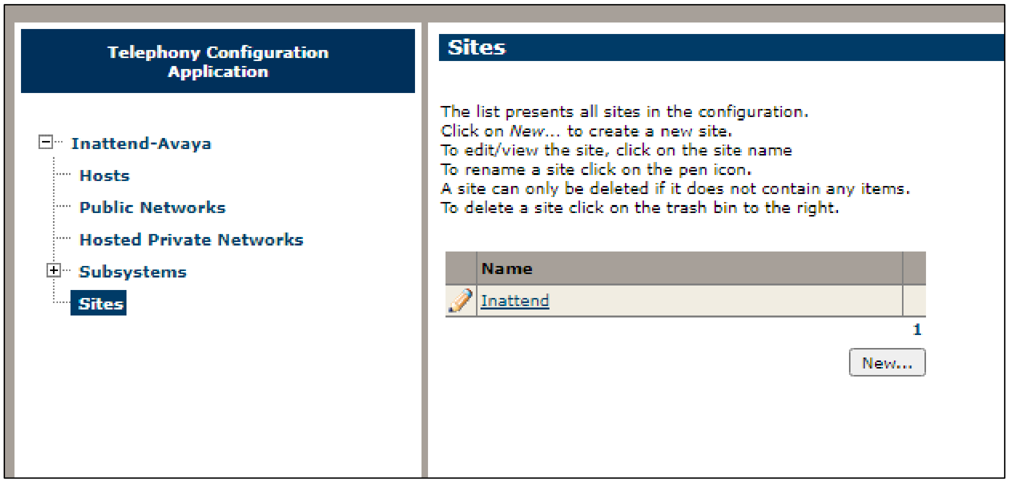
Click into **Hosts** in the left window. The hosts below were already configured by Mitel for compliance testing and clicking on the edit icon will show more information on these hosts. A new host can be added by clicking on **New** in the main window.



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.

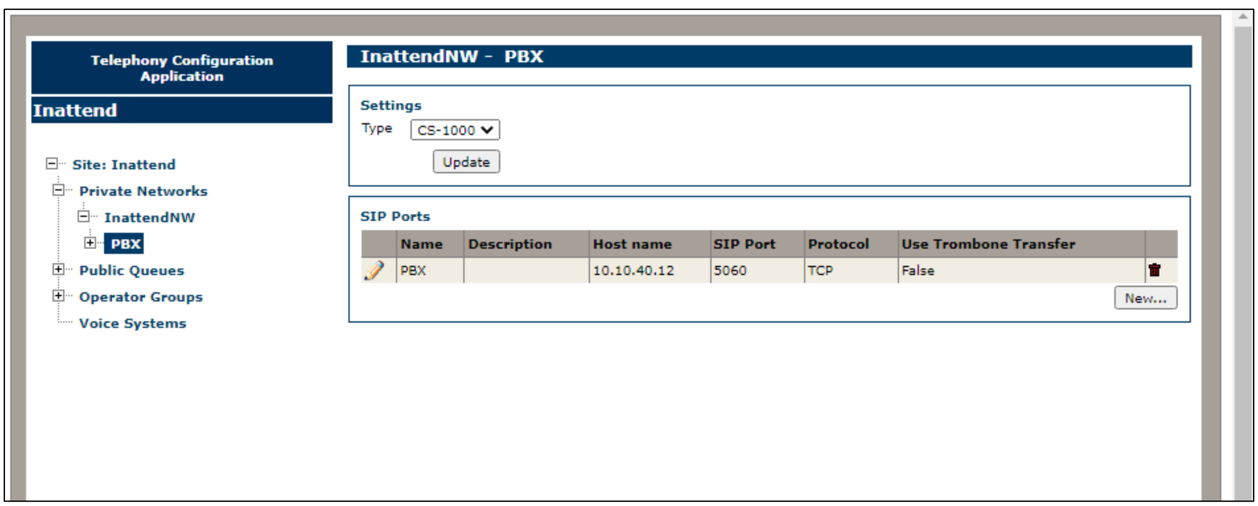


Click on **Sites** in the left window and once again a site will have been already configured during the initial setup, click on that site.



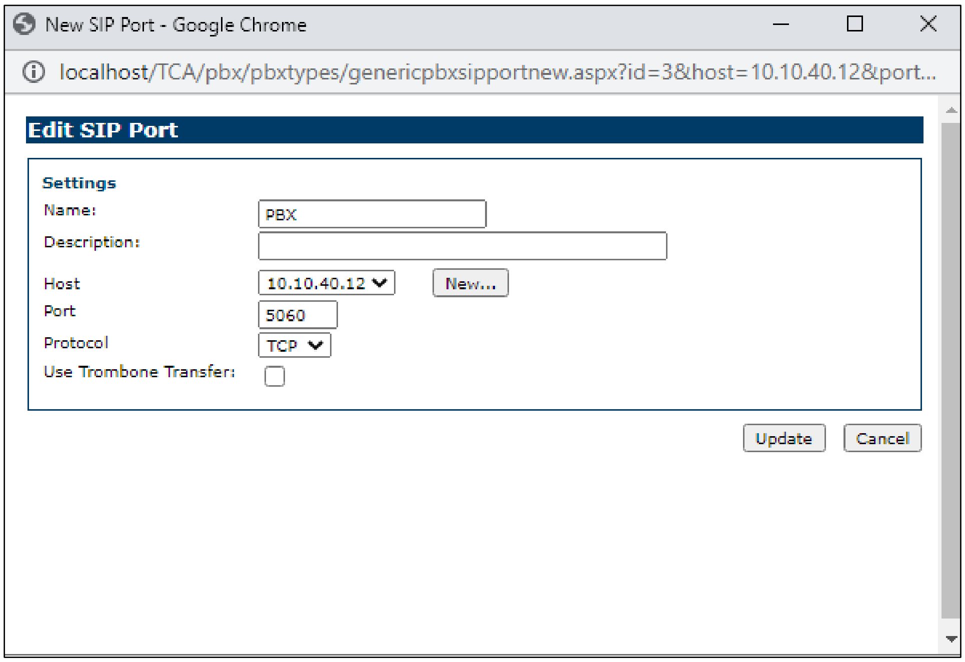
Navigate to **PBX** in the left window and click on **New** in the main window. This will create a new PBX connection. Note that the **Type** can be set to **CS-1000** before clicking on **New**.

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.

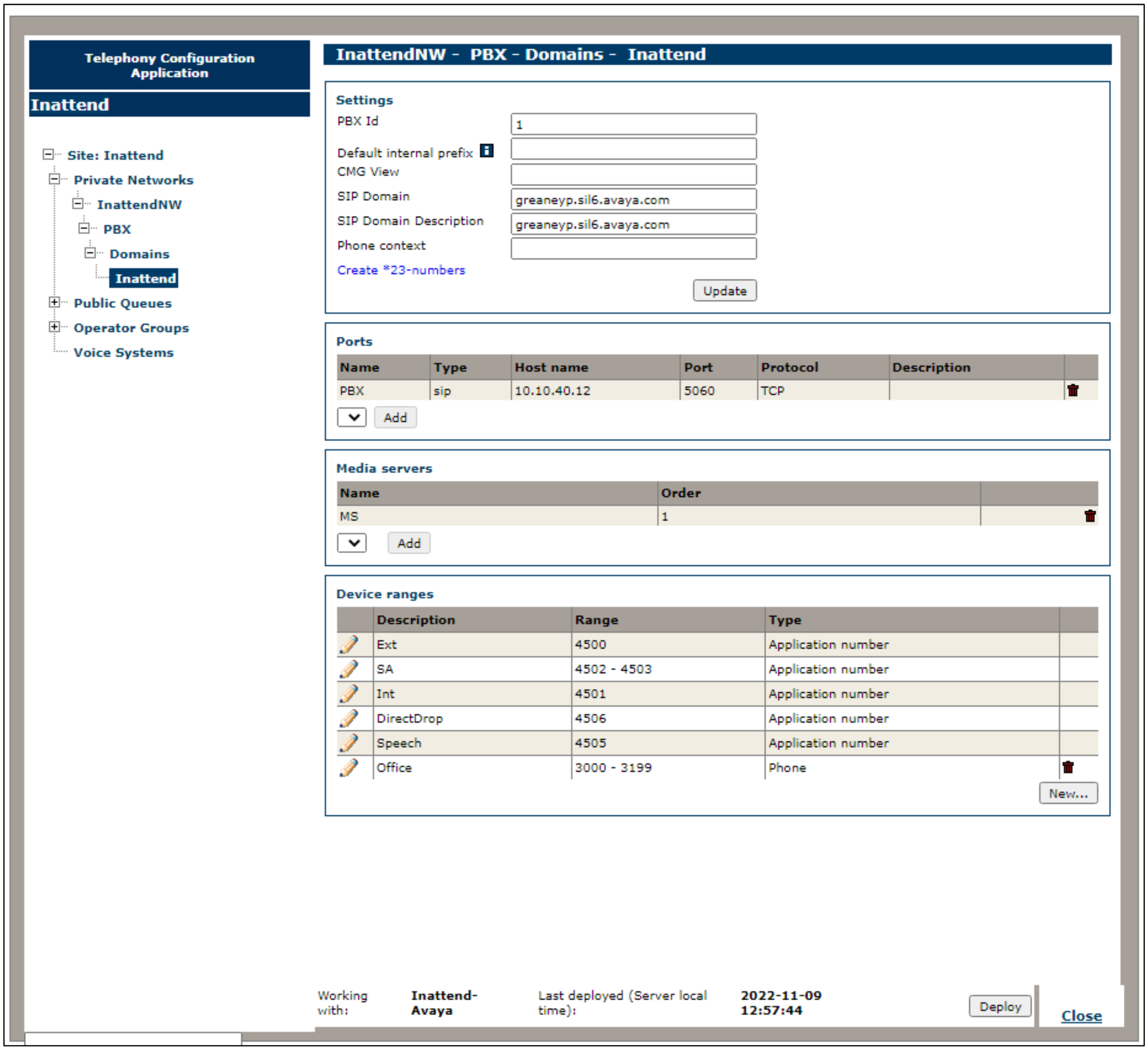


Enter a suitable name and select the **Host** that was created above from the drop-down menu. The **Port** should be set to **5060** and the **Protocol** should be set to **TCP**, this will match the **Entity Link** setup in **Section 6.3**.

Note: The Protocol used can be either TCP or UDP, but it must match that setup on the Entity Link in **Section 6.3**. A connection using TLS is currently not supported.



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.



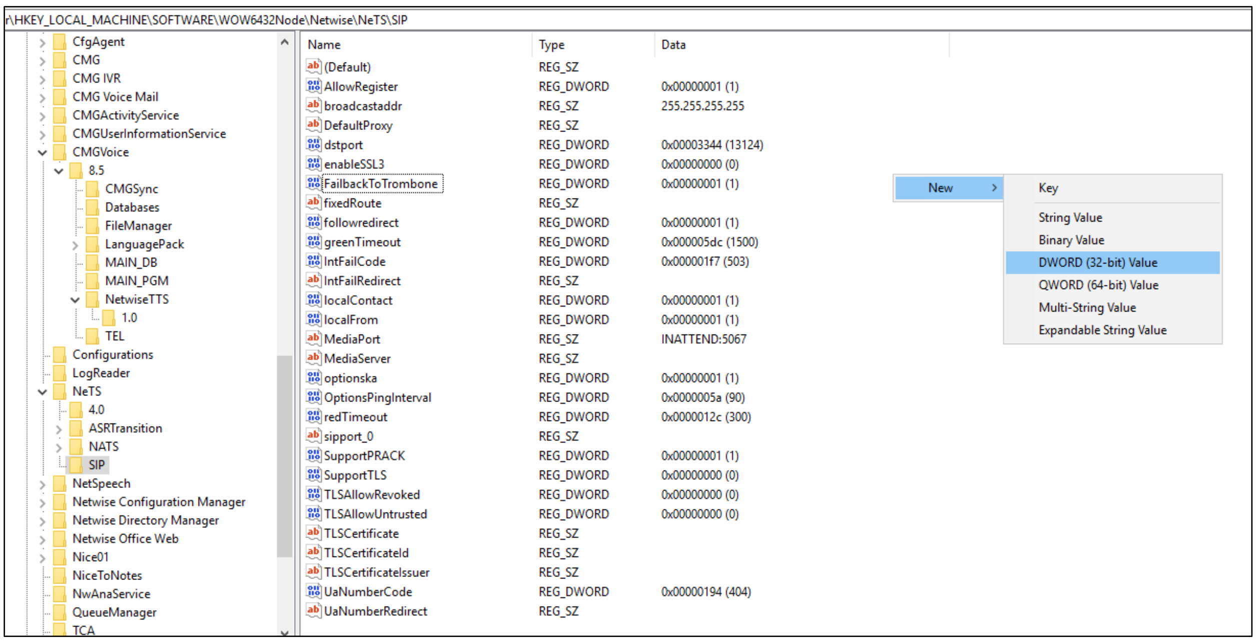
8.4. Update the Registry on the Mitel Attendant Connectivity Server

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:

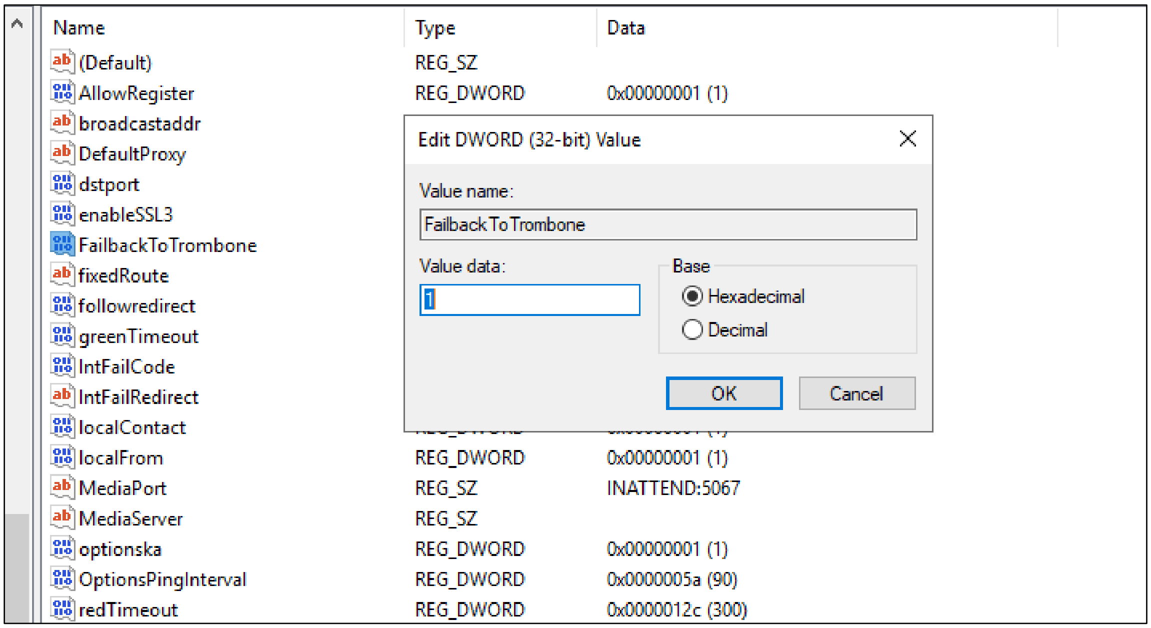
1. Caller from Communication Manager calls to the Mitel InAttend operator.
2. The operator transfers the caller to a voicemail box, 'Direct Drop' to the mailbox.

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

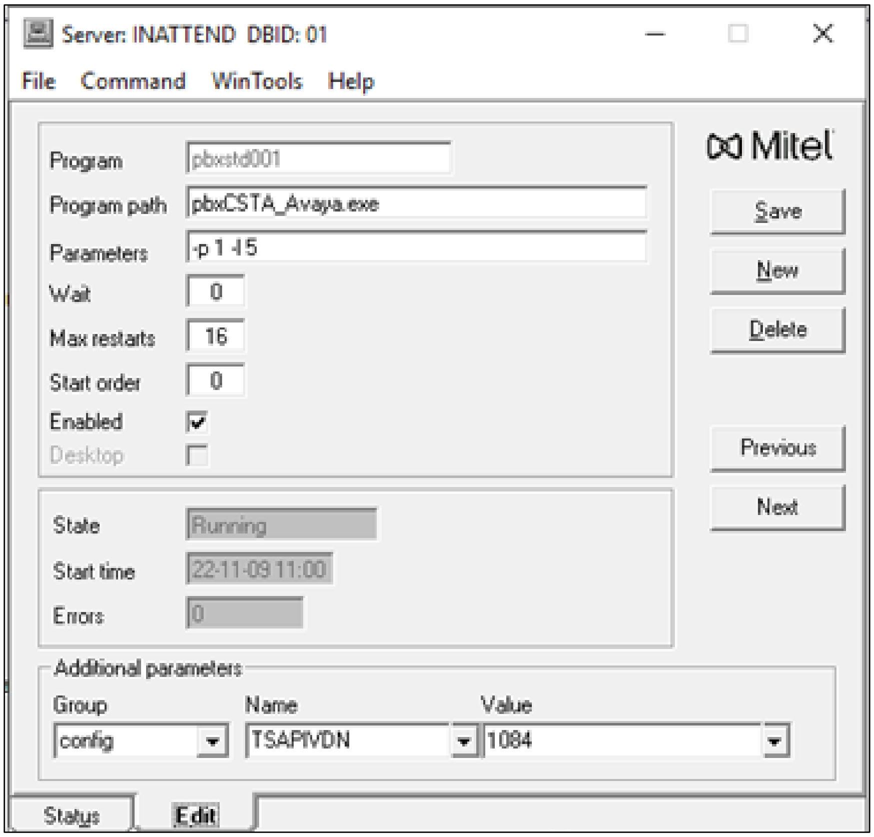


Enter the name **FailbackToTrombone** as the name for the new **REG_DWORD** (not shown) and right-click on the REG_DWORD and select **Modify** as shown. Ensure that the **Value data** is set to **1** and the **Base** to **Hexadecimal**, as shown below. Click in **OK** once finished.



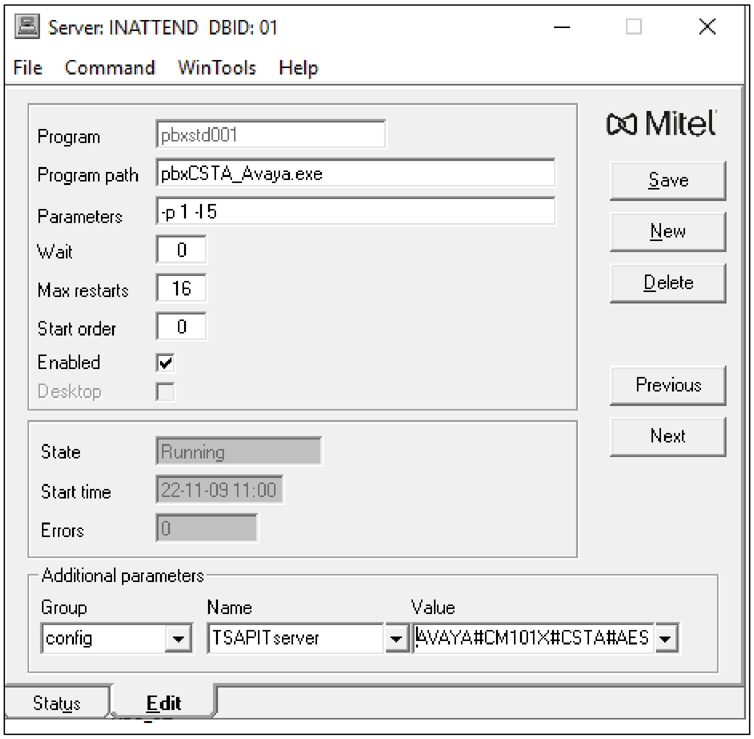
8.5. Configure TSAPI connection from Collaboration Management (CMG) module

Open SPMAN (show that screen shot that was taken of the Mitel folder), 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**.



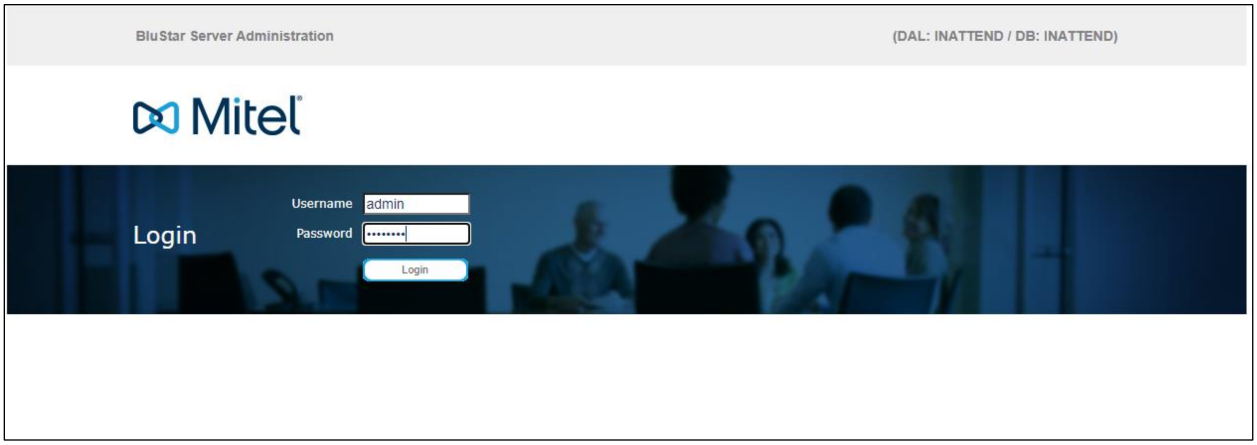
The **TSAPITserver** information is filled in from the TLINK as shown in **Section 7.4**.

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

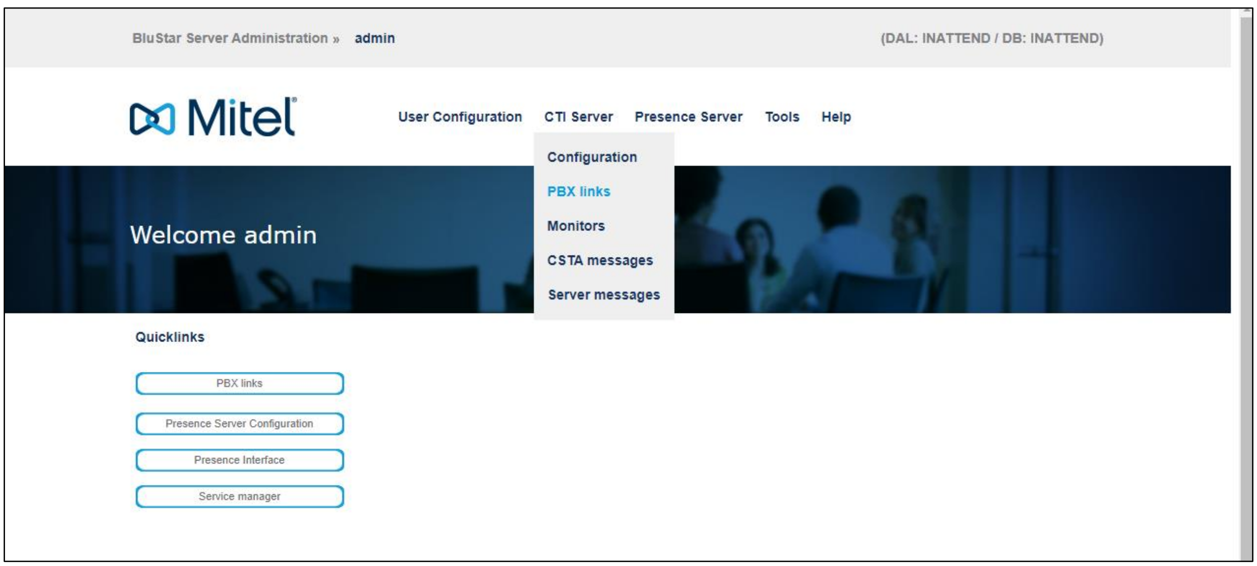


8.6. Configure TSAPI connection from the InAttend Server module

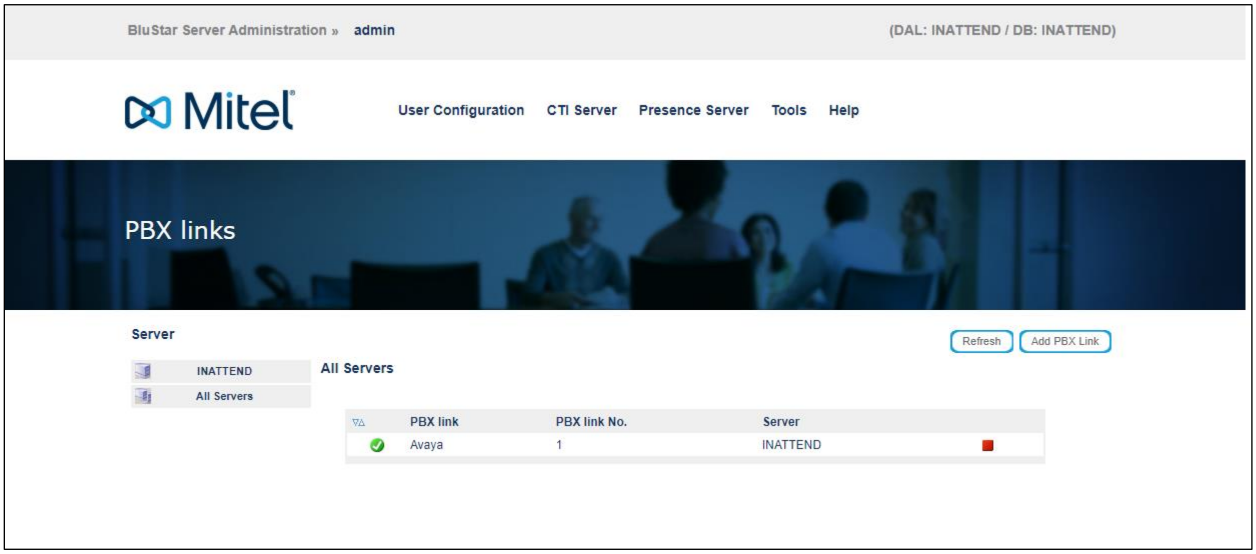
Open a web browser to the InAttend server as shown. Enter the appropriate credentials and click on **Login**.



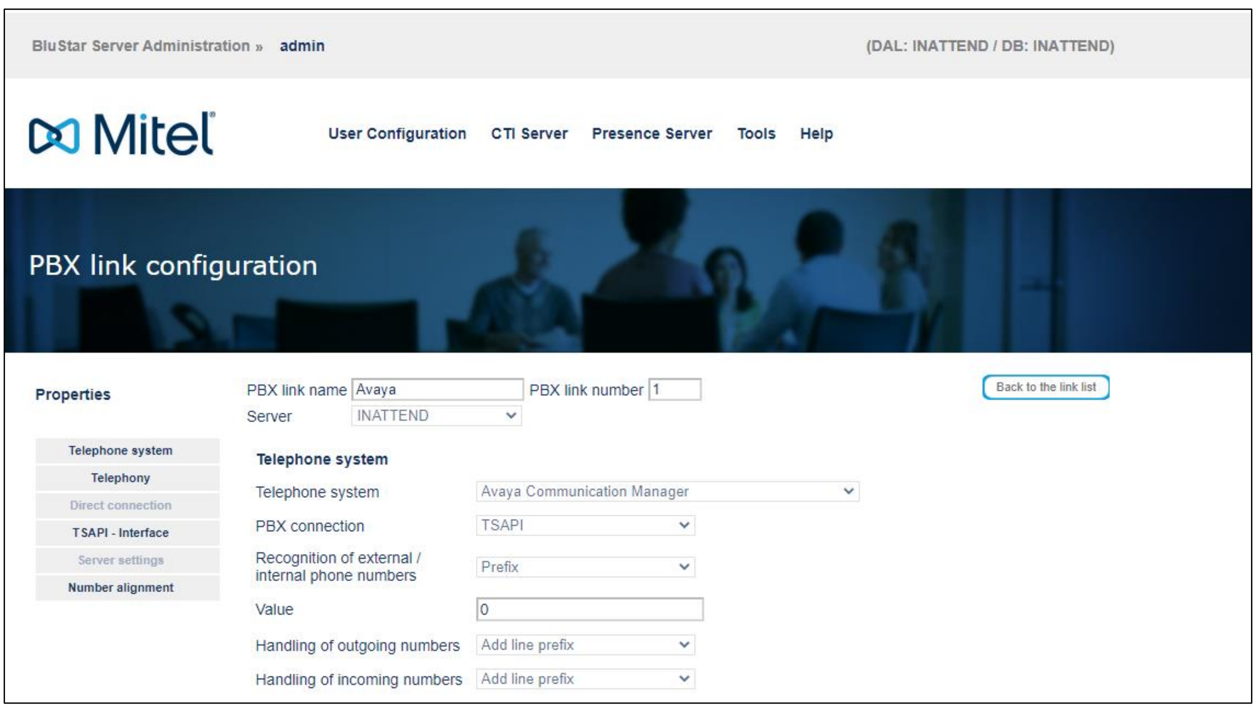
Click on **CTI Server → PBX links**.



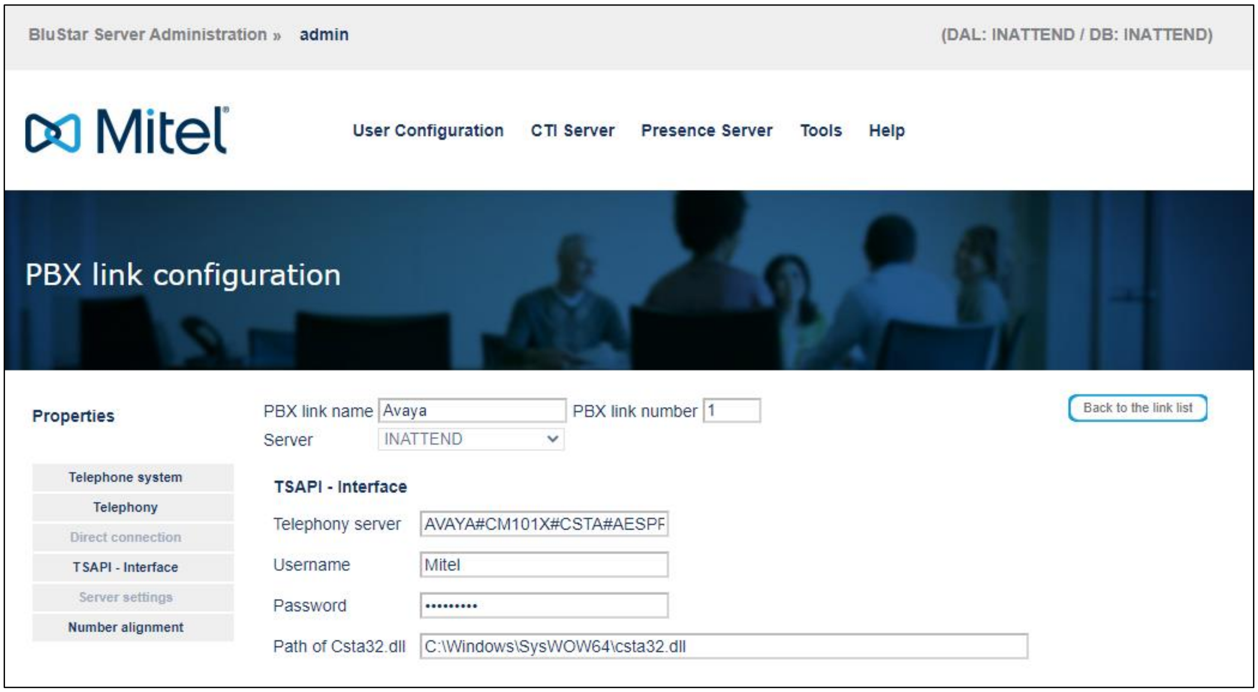
The following PBX link was already configured, but a new one can be added by clicking on **Add PBX Link**.



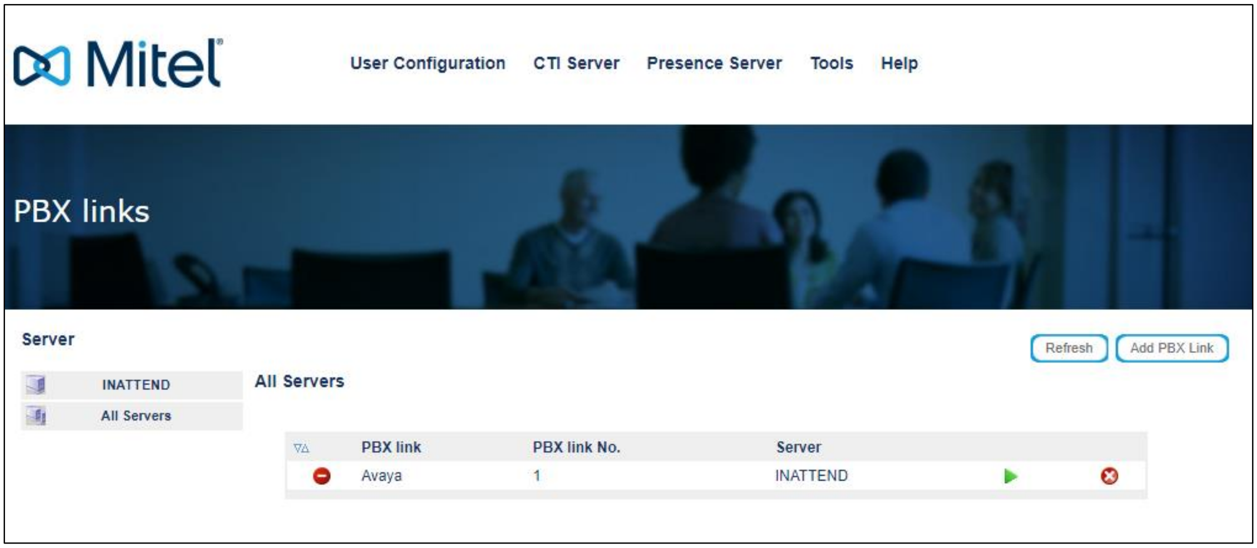
The following screen appears, and the **PBX link configuration** can be set. **Avaya Communication Manager** is chosen for the **Telephone system**. The **PBX connection** is set to **TSAPI** and the **Save** button can be pressed (not shown).



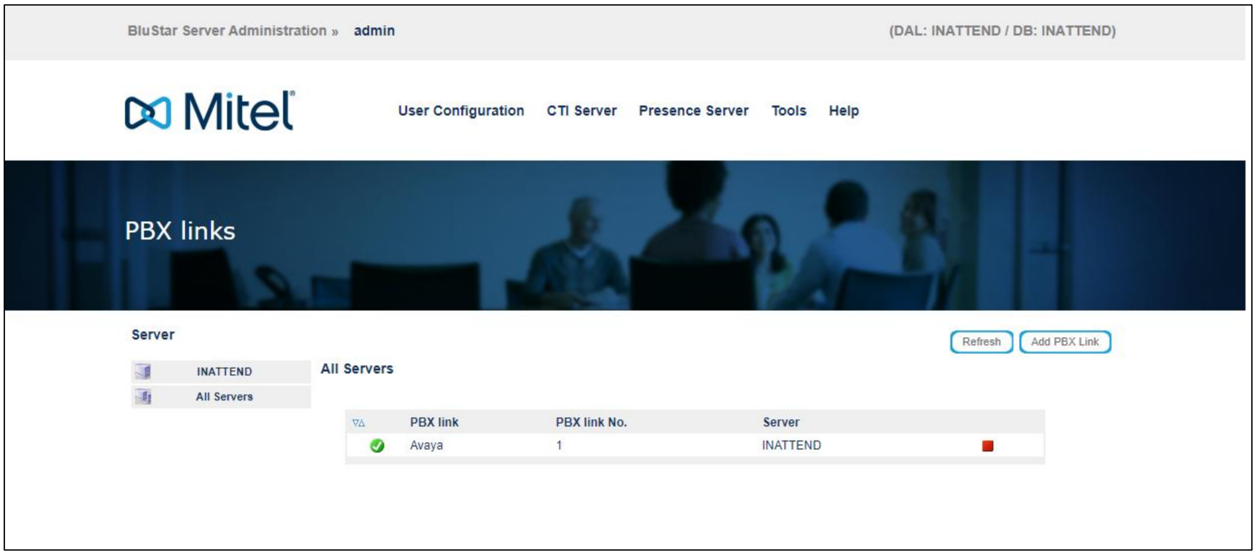
Pressing **Save** on the previous screen brings up the following window where the **TSAPI-Interface** details are added, which include the TLINK, TSAPI user and password. Click on **Save** again once the information is filled in.



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



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

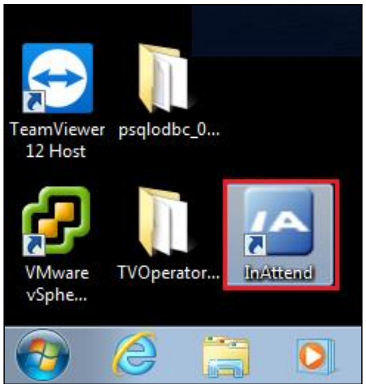


9. Verification Steps

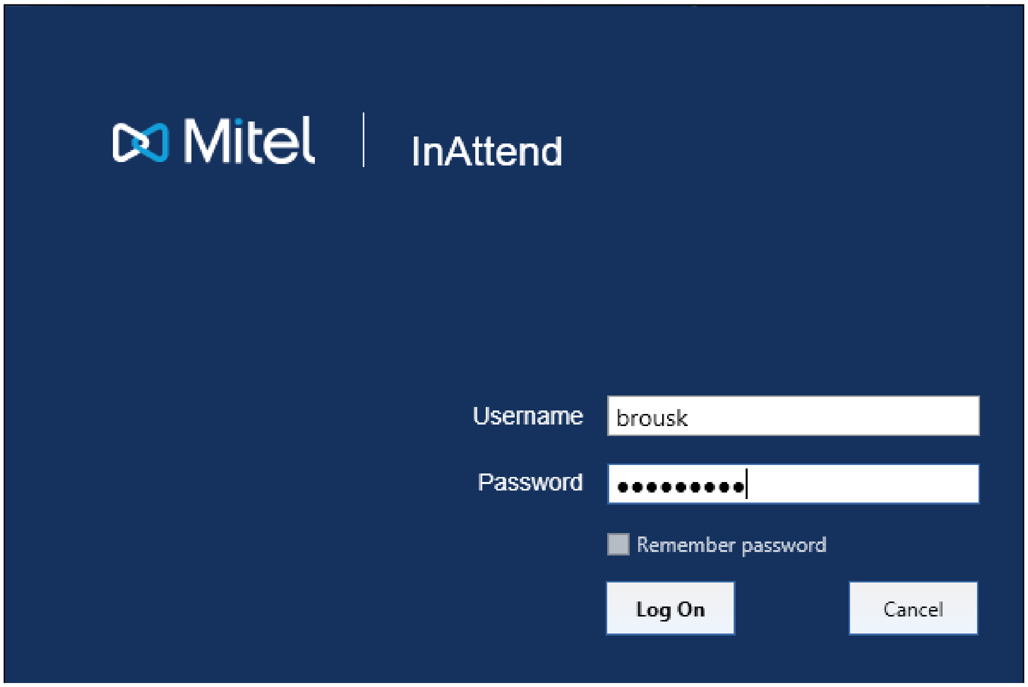
This section provides the tests that can be performed to verify correct configuration of the Avaya and Mitel solutions.

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.

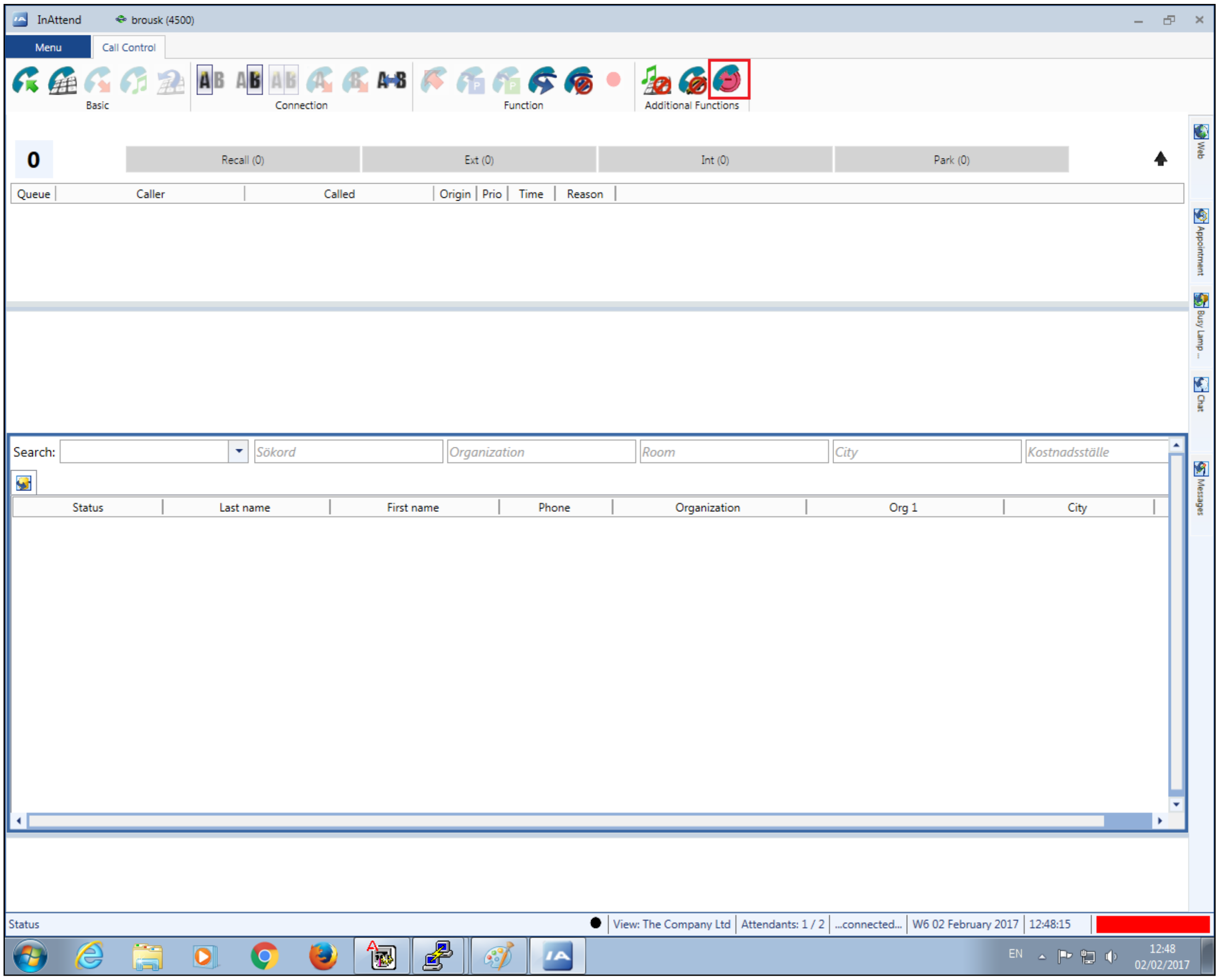
InAttend can be started from the shortcut or by navigating to the program on the client PC.



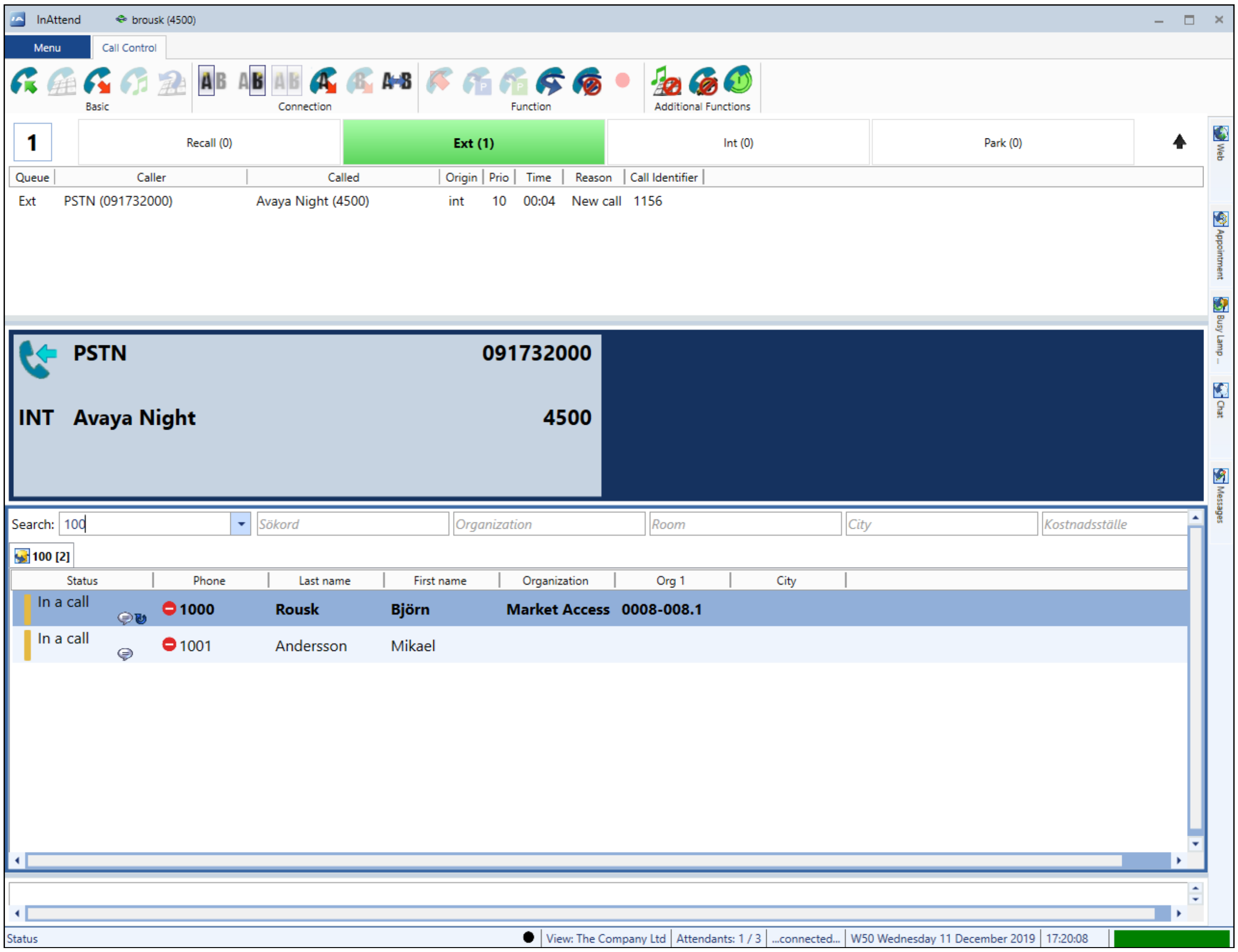
Enter the appropriate credentials and click on **Log On**.



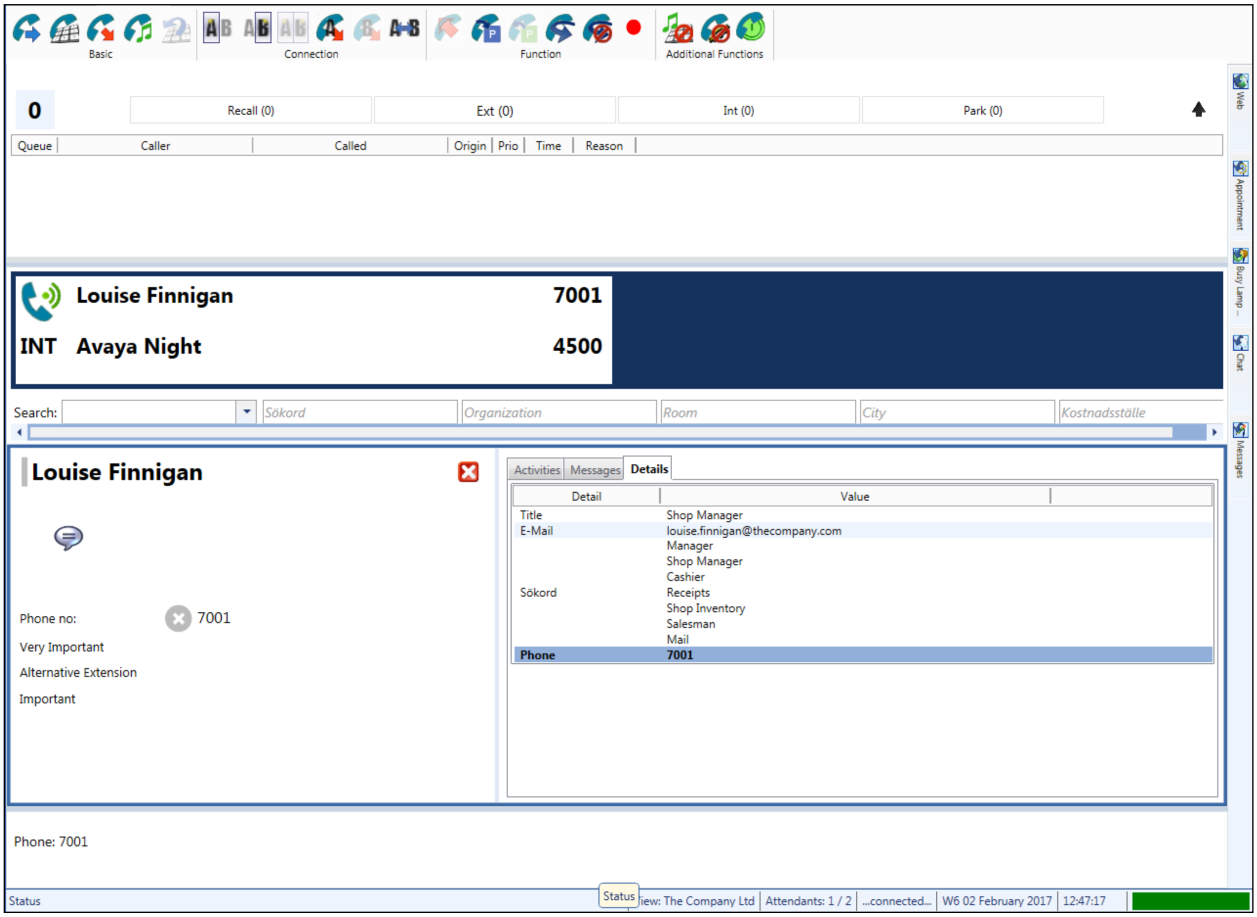
Once logged in the operator will be in night mode as shown below with the red bar. Click on the icon highlighted to change this to normal operation.



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.



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



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   Version     Mnt   AE Services          Service       Msgs
Link              Busy     Server            State         Sent      Rcvd

1         12      no      aespri101x         established   865       865
```

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

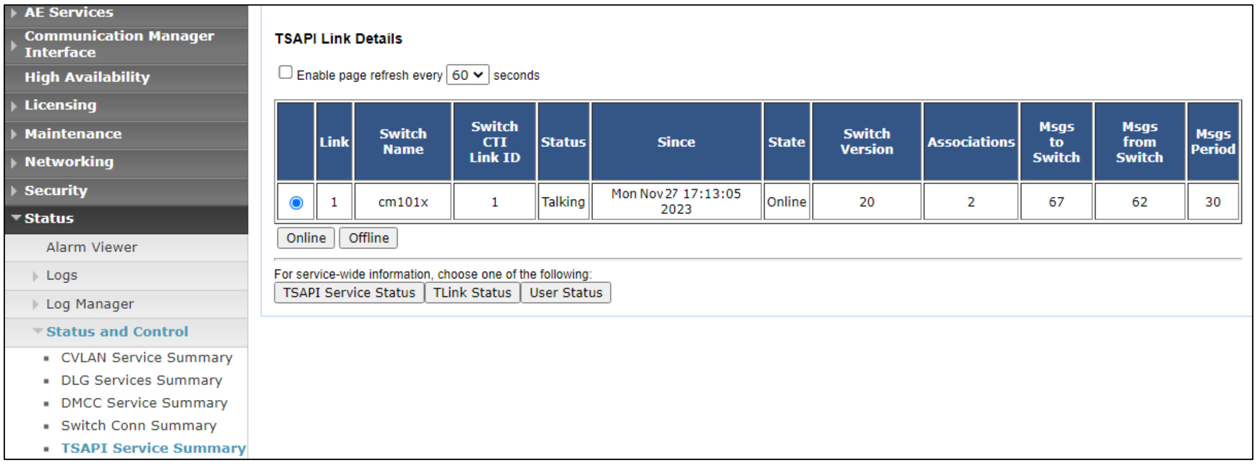
```
status aesvcs interface

                          AE SERVICES INTERFACE STATUS

Local Node         Enabled?  Number of     Status
                             Connections

procr              yes       1             listening
```

Verify that the 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/  AE Services     Remote IP         Remote  Local Node      Msgs
Link   Server                            Port                    Sent    Rcvd

01/01  aespri101x      10.10.40.16       56722   procr            683     665
```

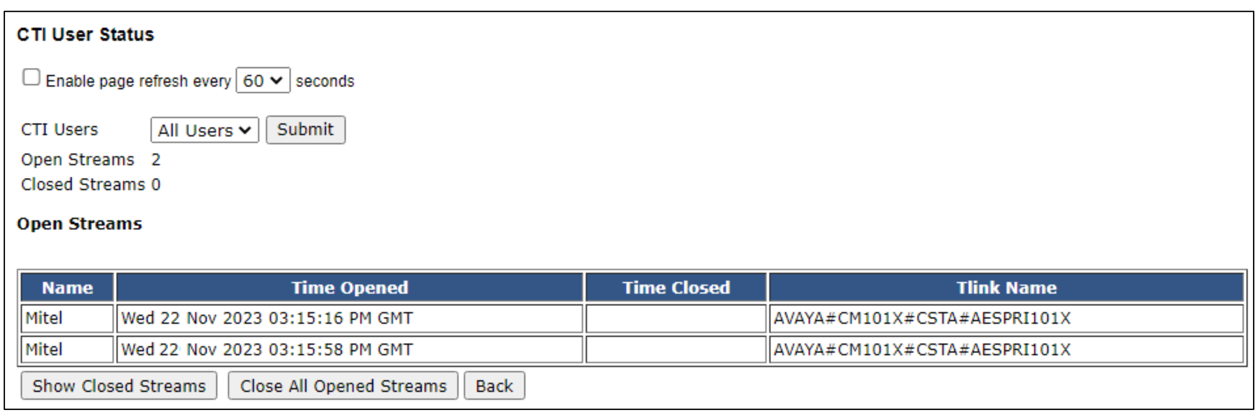
9.1.2. Verify the TSAPI Link from Application Enablement Services

On the AES Management Console, verify the status of the TSAPI link by selecting **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**. There were two devices monitored during compliance testing and so **Associations** is showing **2** below.



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. As per **Section 1**, the Mitel InAttend solution makes use of two TSAPI connections to 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.



9.2. Verify the SIP Trunk connection

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

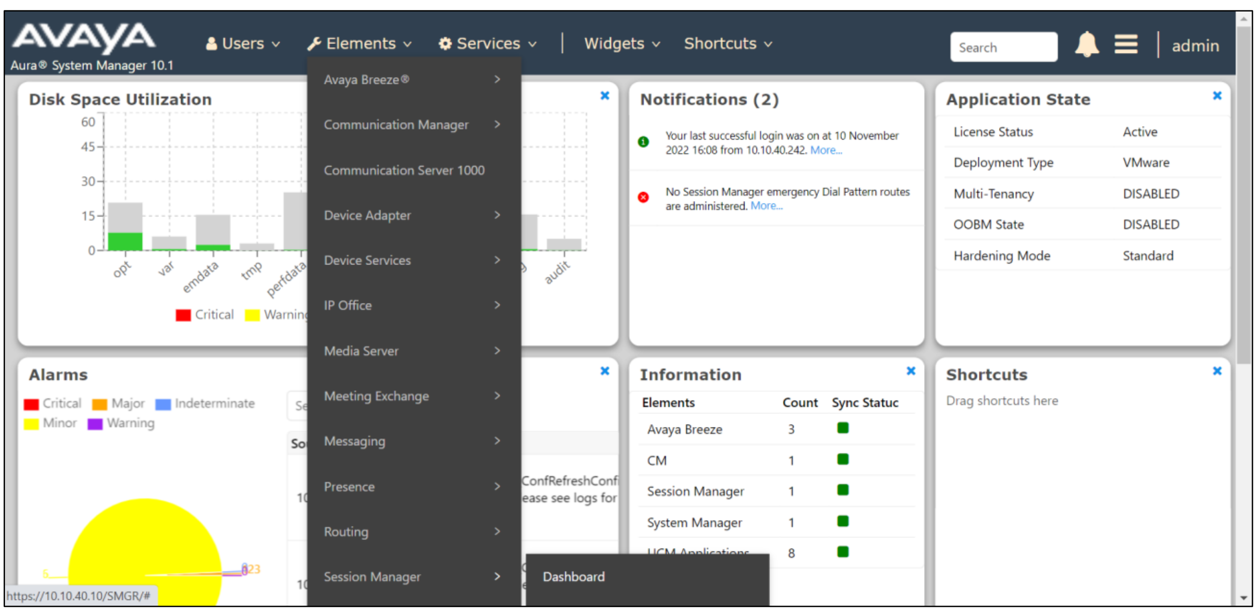
9.2.1. Verify Avaya Aura® Communication Manager

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).

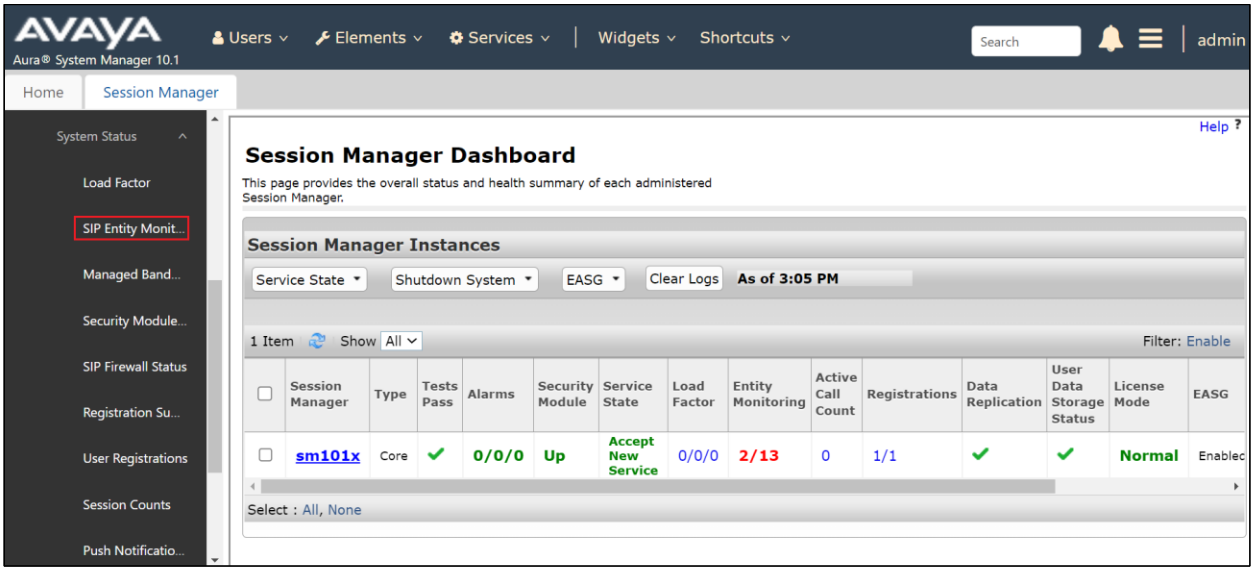
```
status trunk 1

                              TRUNK GROUP STATUS

Member     Port     Service State      Mtce Connected Ports
                                       Busy

0001/0001 T00001  in-service/idle    no
0001/0002 T00002  in-service/idle    no
0001/0003 T00003  in-service/idle    no
```

9.2.2. Verify InAttend SIP Entity is up

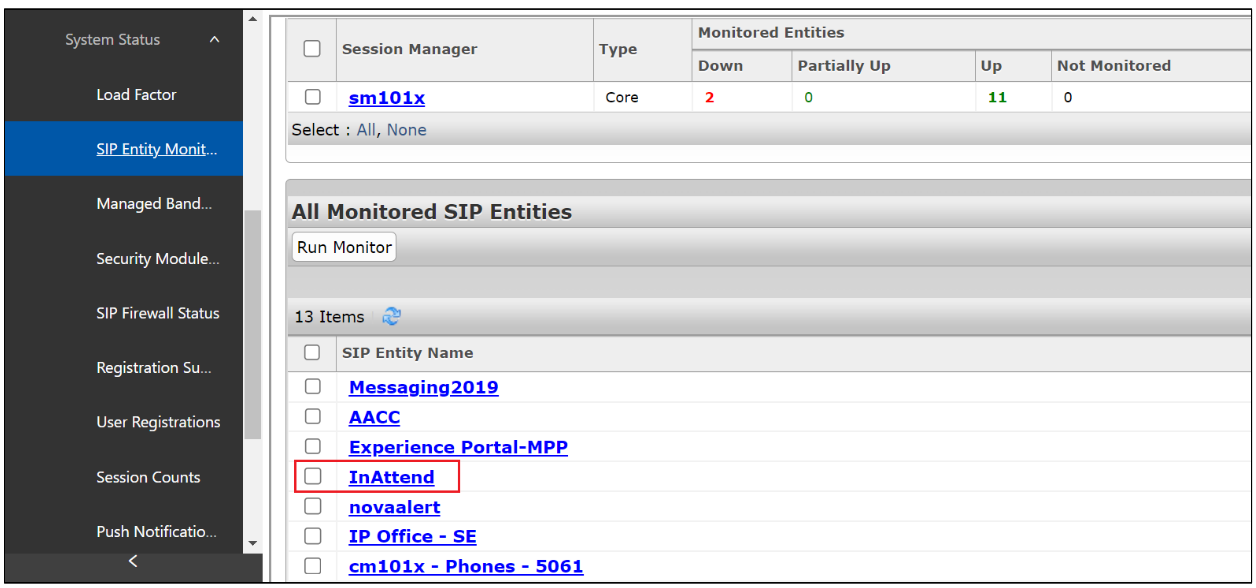
Log into System Manager as per **Section 6**. Navigate to **Elements** and click on **Session Manager**.



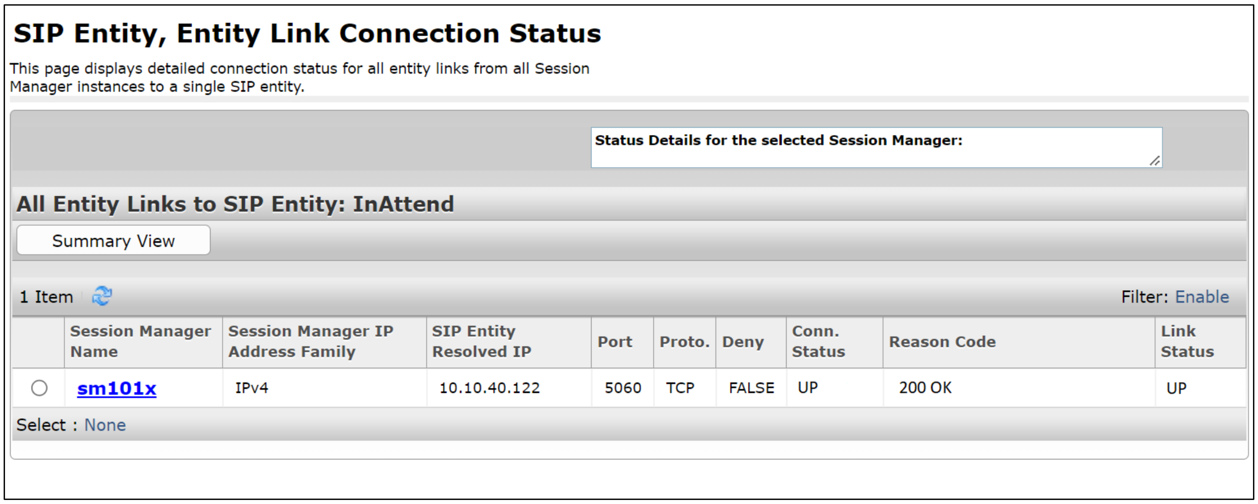
Selected **SIP Entity Monitoring** in the left window.



Select the **InAttend** SIP Entity.



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



10. Conclusion

The interoperability of Mitel InAttend using Mitel Attendant Connectivity Server V2.7 from Mitel Sweden AB to interoperate with Avaya Aura® Communication Manager R10.1 utilizing a SIP trunk connection to Avaya Aura® Session Manager R10.1 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 10.1

[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Release 10.1

[3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide* Release 10.1

[4] *Administering Avaya Aura® Session Manager* – Release 10.1

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

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.