Avaya Solution & Interoperability Test Lab

Application Notes for iNEMSOFT CLASSONE® iCAS with Avaya Meeting Exchange – Issue 1.0

Abstract

These Application Notes contain instructions for iNEMSOFT CLASSONE® iCAS to successfully interoperate with Avaya Meeting Exchange.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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 contain instructions for iNEMSOFT CLASSONE® iCAS to successfully interoperate with Avaya Meeting Exchange.

The CLASSONE® iCAS is a system-of-systems, enabling operators to take control of their communications network and manage multiple transactions from many types of devices.

CLASSONE® iCAS (iCAS) solution enables operators to handle inbound calls, connect with radio dispatch, bridge various radio talk groups and frequencies with each other and with back office voice systems, collaborate and manage field operations regardless of the type of voice-enabled device, while maintaining the highest level of business continuity and interoperability. iCAS as a solution, integrates with several interfaces provided by Avaya products. However, this document only contains instructions for Avaya Meeting Exchange. iCAS uses the Avaya Conferencing Provider Interface (ACPI) to open conferences that allow inbound calls to automatically join open conferences. Application notes related to other interfaces may be obtained via Avaya Support site.

- Application Notes for iNEMSOFT CLASSONE® iCAS IP Radio Gateway with Avaya Aura® Session Manager
- Application Notes for iNEMSOFT CLASSONE® iCAS Dispatch Console with Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services
- Application Notes for iNEMSOFT CLASSONE® Endpoint Manager with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services

2. General Test Approach and Test Results

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 this DevConnect Application Note 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 iNEMSOFT did not utilize encryption capabilities.

2.1. Interoperability Compliance Testing

During Interoperability Compliance testing, functional call routing scenarios were tested:

- Heartbeats from iCAS to Meeting Exchange
- Opening and closing conferences
- Participants joining conferences
- Participant property control. i.e. name, allow listen only or talk
- DTMF tone generation and detection
- Direct SIP access from one conference to anther on Meeting Exchange

Additionally, survivability tests such as network connectivity loss and restart of iCAS were also performed. Please note that performance testing or load testing were not part of this test effort.

2.2. Test Results

All planned test cases were passed.

2.3. Support

iNEMSOFT CLASSONE® iCAS support can be obtained via following means:

Phone: 214-423-2815
Web: www.inmentsoft.com
Email: rtisupport@inemsoft.com

3. Reference Configuration

Figure 1 illustrates a sample configuration that consists of Avaya Products and iNEMSOFT CLASSONE® iCAS. Though this document only contains instructions for and iNEMSOFT CLASSONE® iCAS Application Server with Avaya Meeting Exchange, the following diagram shows the entire solution that was tested during compliance testing.

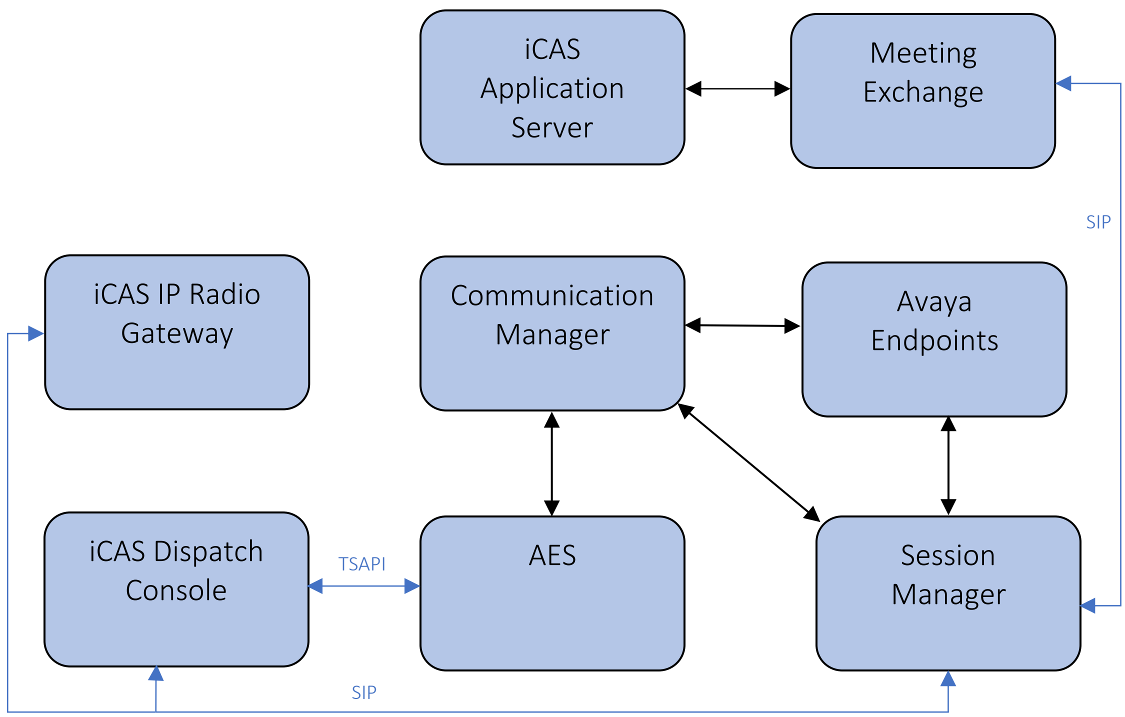


Figure 1: Test Configuration of CLASSONE® iCAS and Avaya Products

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided: With the exception of Avaya G450 Gateway, all other Avaya products were deployed on a Virtualization Environment.

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	8.1.0.1.1.890.25517
Avaya G450 Media Gateway	FW 40.19.1
Avaya Aura® Media Server	8.0.1.121
Avaya Aura® Session Manager	8.1.0.0.810007
Avaya Aura® System Manager	8.1.0.0.733078
Avaya Meeting Exchange	6.2 SP7
Avaya 9600 Series IP Deskphones	6.8.2 (H.323) 7.1.6.1 (SIP)
Avaya J100 Series IP Phones	6.8.2 (H.323) 4.0.2.1 (SIP)
iNEMSOFT CLASSONE® iCAS Application Server	4.19

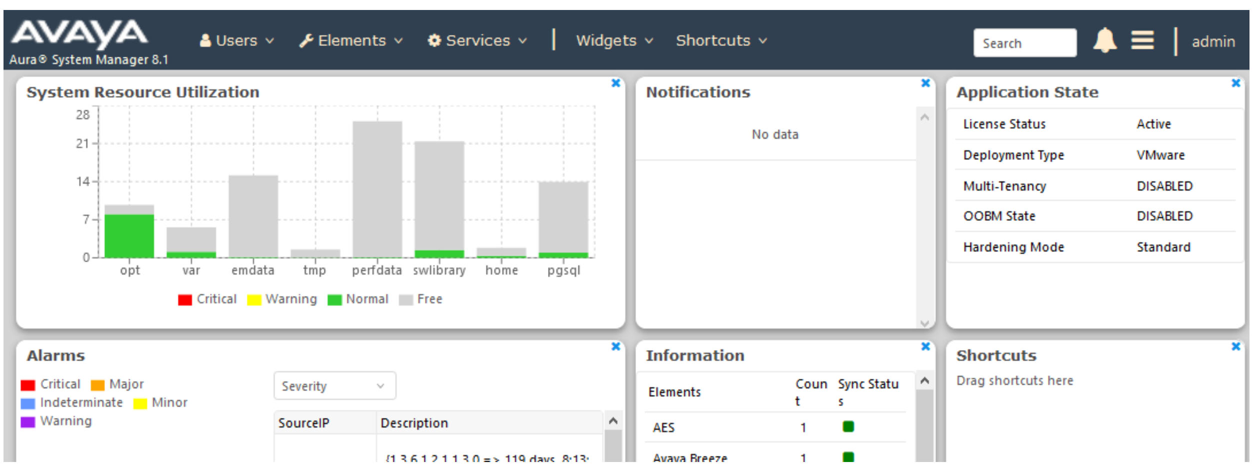
5. Configure Avaya Aura® Session Manager

Though iCAS doesn't directly integrate with Session Manager, a SIP Trunk to Meeting Exchange is required for participants to join conferences. Alternatively, SIP Trunks from Communication Manager can also be used. During Compliance test, following configuration was performed.

This section provides the procedures for configuring Session Manager, assuming it has been installed and licensed. The procedures include the following items:

- Specify SIP Domain
- Add Locations
- Add SIP Entities
- Add Entity Links
- Add Routing Policies
- Add Dial Patterns

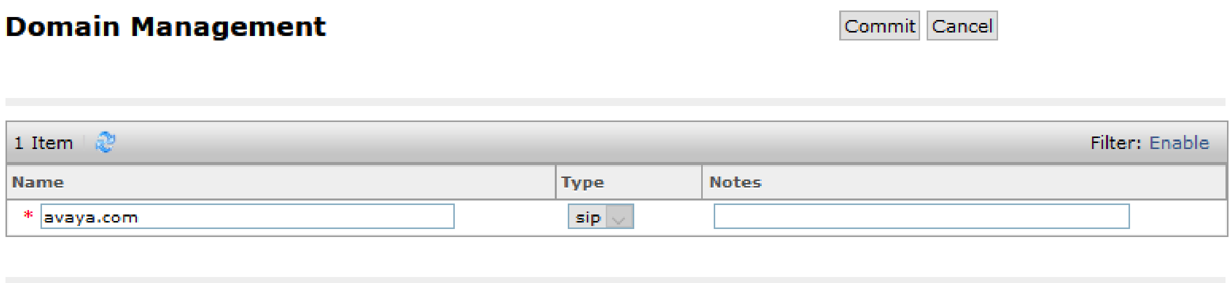
Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>**, where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials. The menu shown below is displayed. Select **Elements → Routing**.



5.1. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Select **Domains** on the left and click the **New** button on the right. The following screen will be shown. Fill in the following fields and click **Commit**.

- **Name:** The authoritative domain name (e.g. **avaya.com**)
- **Type** Select **sip**
- **Notes:** Descriptive text (optional)



5.2. Add Locations

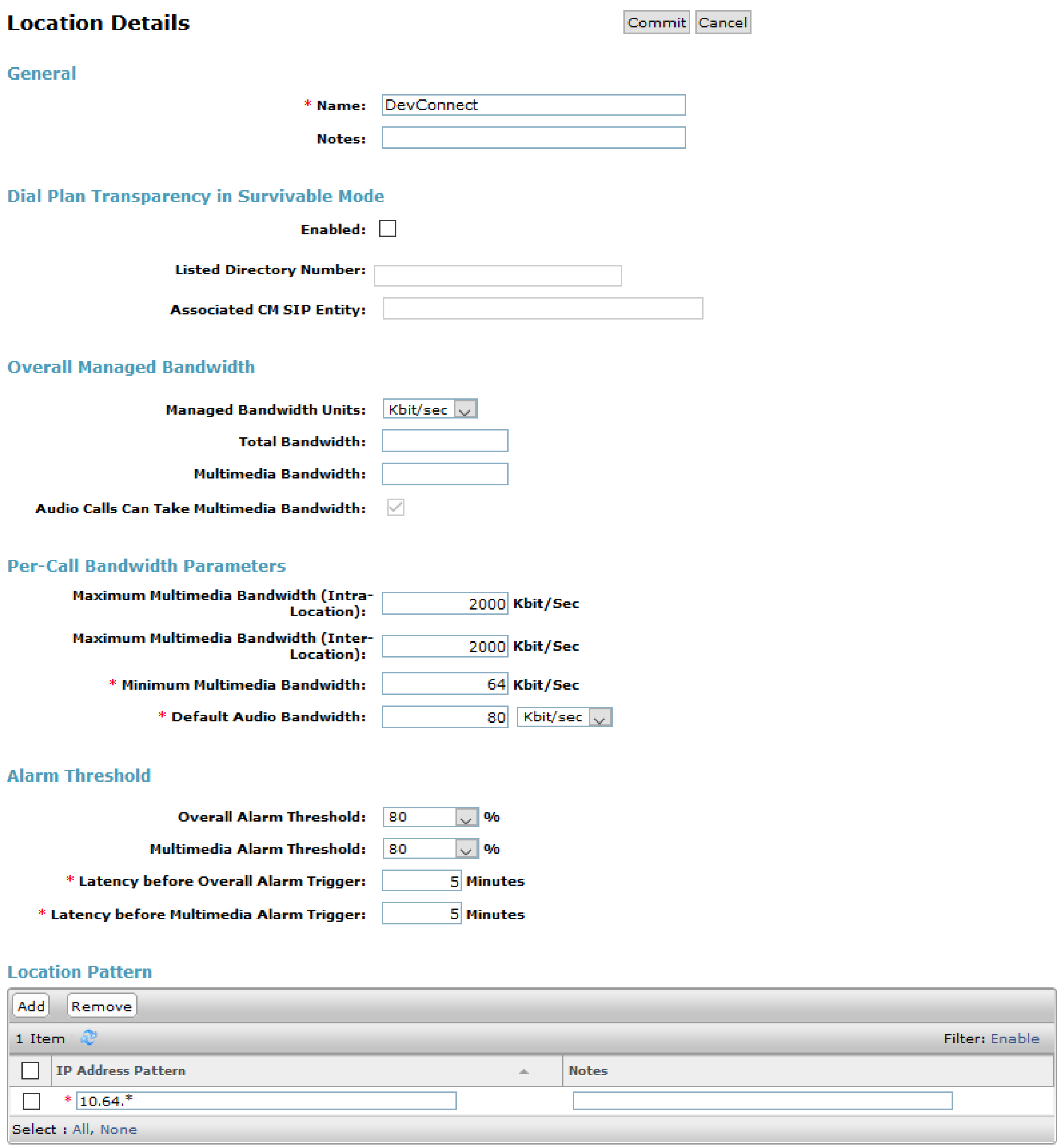
Locations can be used to identify logical and/or physical locations where SIP Entities reside, for the purpose of bandwidth management. To add a location, select **Locations** on the left and click on the **New** button on the right. The following screen will be shown. Fill in the following fields:

Under **General**:

- **Name:** A descriptive name
- **Notes:** Descriptive text (optional)

Under **Location Pattern**:

- **IP Address Pattern:** A pattern used to logically identify the location. In these Application Notes, the pattern represented the networks involved, i.e. **10.64.***"
- **Notes:** Descriptive text (optional)


Location Details
Commit
Cancel
General
* Name:
DevConnect
Notes:
Dial Plan Transparency in Survivable Mode
Enabled:
Listed Directory Number:
Associated CM SIP Entity:
Overall Managed Bandwidth
Managed Bandwidth Units:
Kbit/sec
Total Bandwidth:
Multimedia Bandwidth:
Audio Calls Can Take Multimedia Bandwidth:
Per-Call Bandwidth Parameters
Maximum Multimedia Bandwidth (Intra-Location):
2000
Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location):
2000
Kbit/Sec
* Minimum Multimedia Bandwidth:
64
Kbit/Sec
* Default Audio Bandwidth:
80
Kbit/sec
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
1 Item
Filter: Enable
IP Address Pattern
Notes
* 10.64.*
Select : All, None

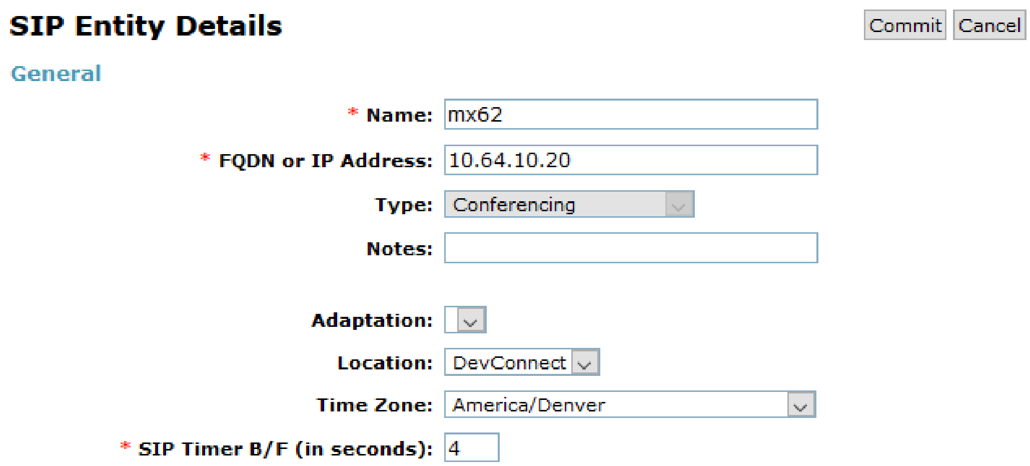
5.3. SIP Entity

Select SIP Entities on the left and click on the **New** button on the right.

Under **General**:

- **Name:** A descriptive name
- **FQDN or IP Address:** IP address of the signaling interface of Meeting Exchange, i.e. **10.64.10.22**
- **Type:** Select **Conferencing**
- **Location:** Select a pre-defined location
- **Time Zone:** Time zone for this entity

Defaults can be used for the remaining fields. The screen below shows the configuration of the Meeting Exchange SIP Entity.

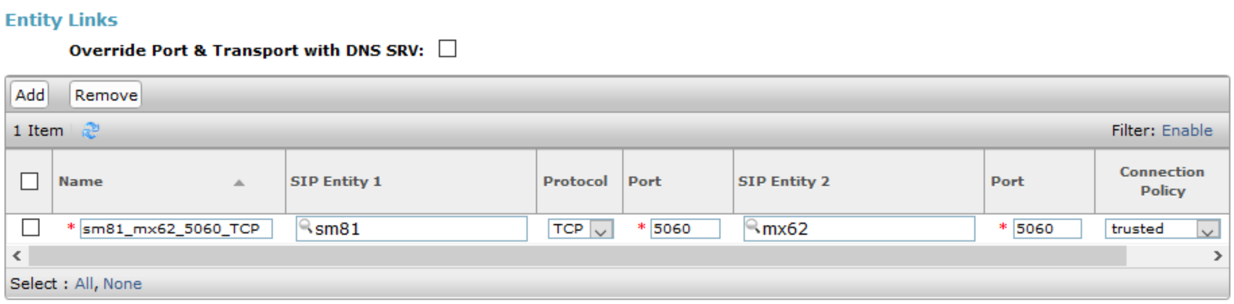


5.4. SIP Entity Link

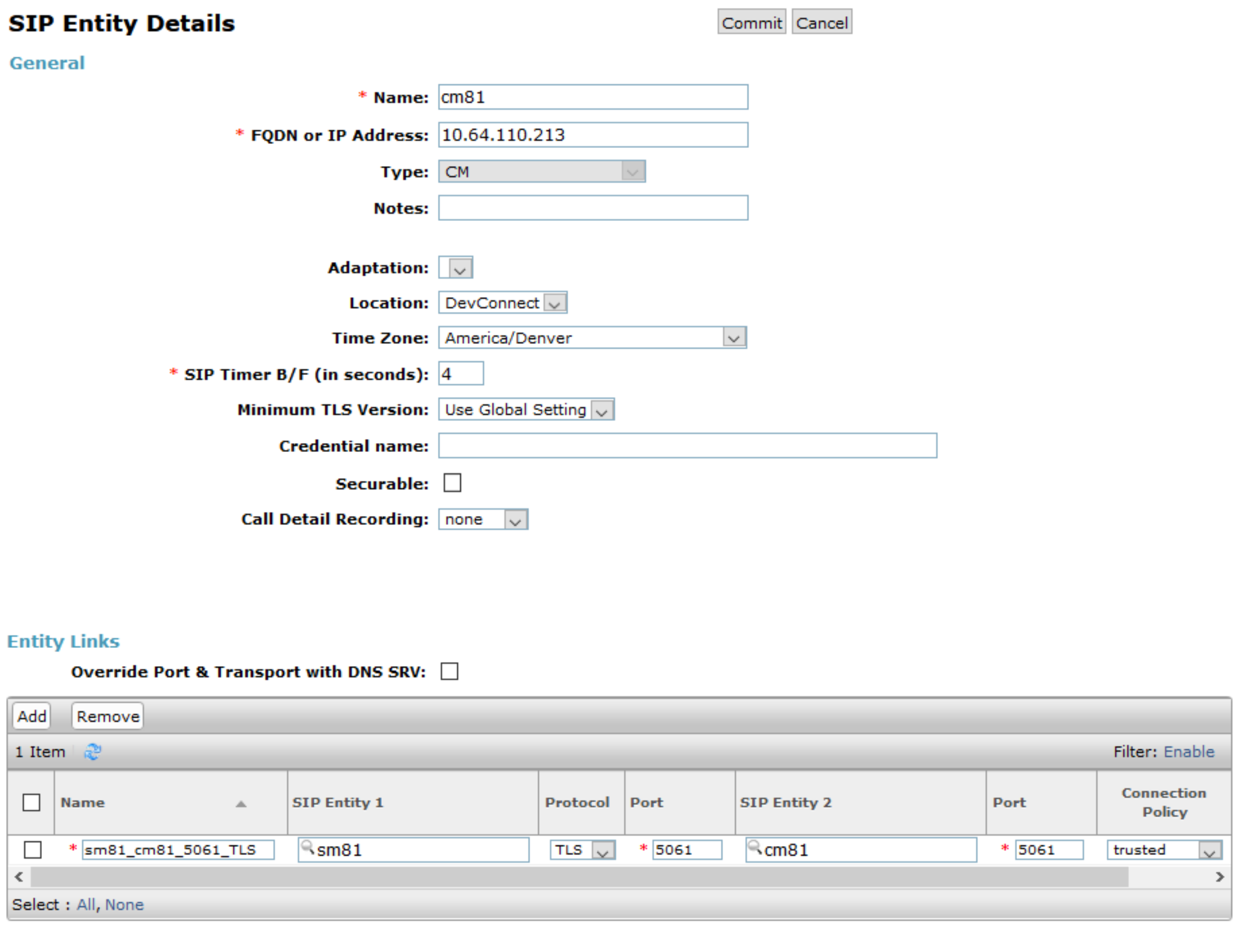
Continuing from above, scroll down to the **Entity Links** section. Select **Add** to add an entity link.

- Type in a **Name**
- Select Session Manager SIP Entity for **SIP Entity 1**
- Select **TCP** for **Protocol**
- Select **mx62** for **SIP Entity 2**

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



Similarly, add a SIP Entity and an Entity Links for Communication Manager. The screen capture below shows the Communication SIP Entity and Entity Links.



5.5. Add Routing Policies

Routing policies describe the condition under which calls will be routed to the SIP Entities specified in **Section 5.3**. Two routing policies were added: one for Communication Manager and another for Meeting Exchange. To add a routing policy, select **Routing Policies** on the left and click on the **New** button on the right. The following screen is displayed. Fill in the following fields:

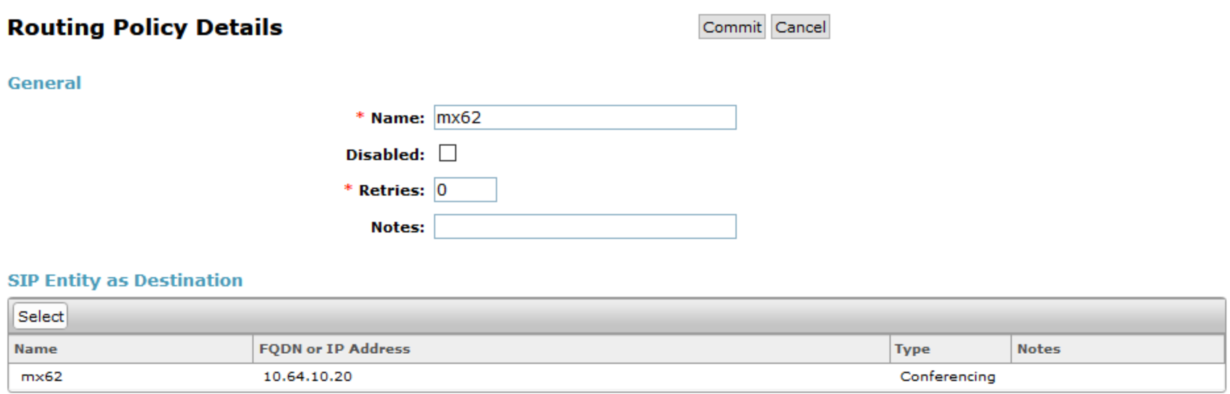
Under **General:**

- Enter a descriptive name in **Name**

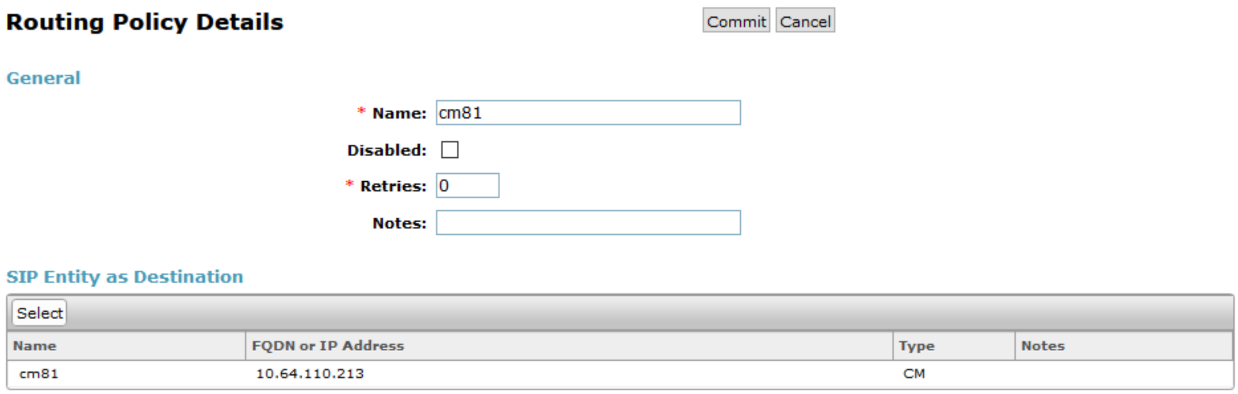
Under **SIP Entity as Destination:**

- Click **Select**, and then select the appropriate SIP entity to which this routing policy applies

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following screen captures shows the Routing Policy for Meeting Exchange.



The following screen shows the Routing Policy for Communication Manager.



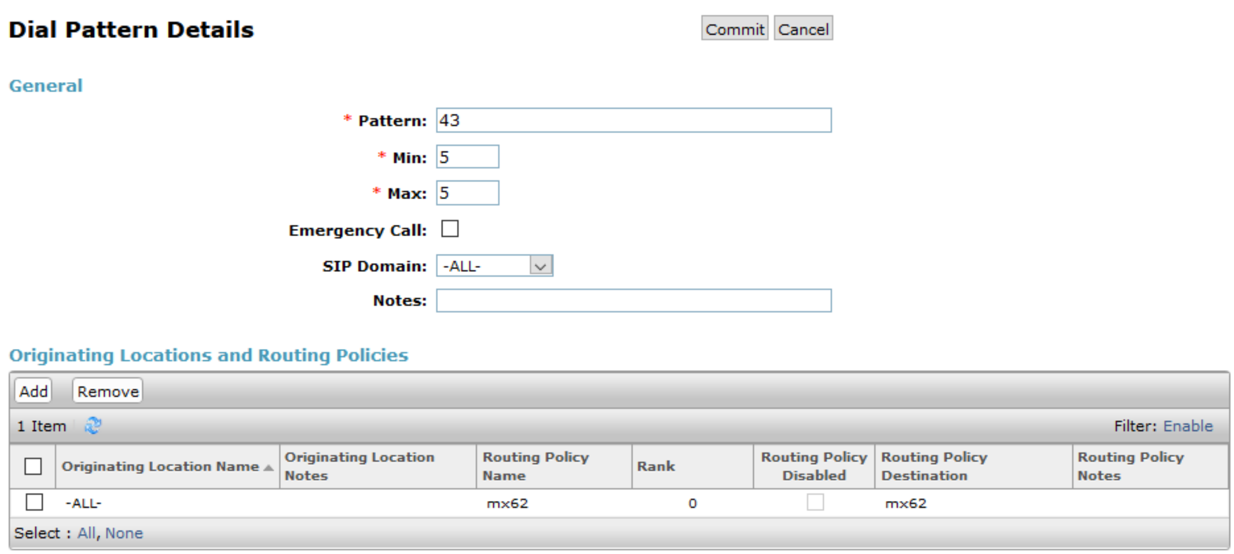
5.6. Add Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button on the right. Following Dial Pattern was added for Meeting Exchange:

Under **General**:

- **Pattern:** Dialed number or prefix, **43**
- **Min:** Minimum length of dialed number, **5**
- **Max:** Maximum length of dialed number, **5**
- **SIP Domain:** Select **-ALL-**

Under **Originating Locations and Routing Policies**, click **Add**, and then select the appropriate location and routing policy from the list. Default values can be used for the remaining fields. Click **Commit** to save the dial pattern. Numbers dialed with a prefix of 43 and were 5 digits long, were routed to Meeting Exchange.

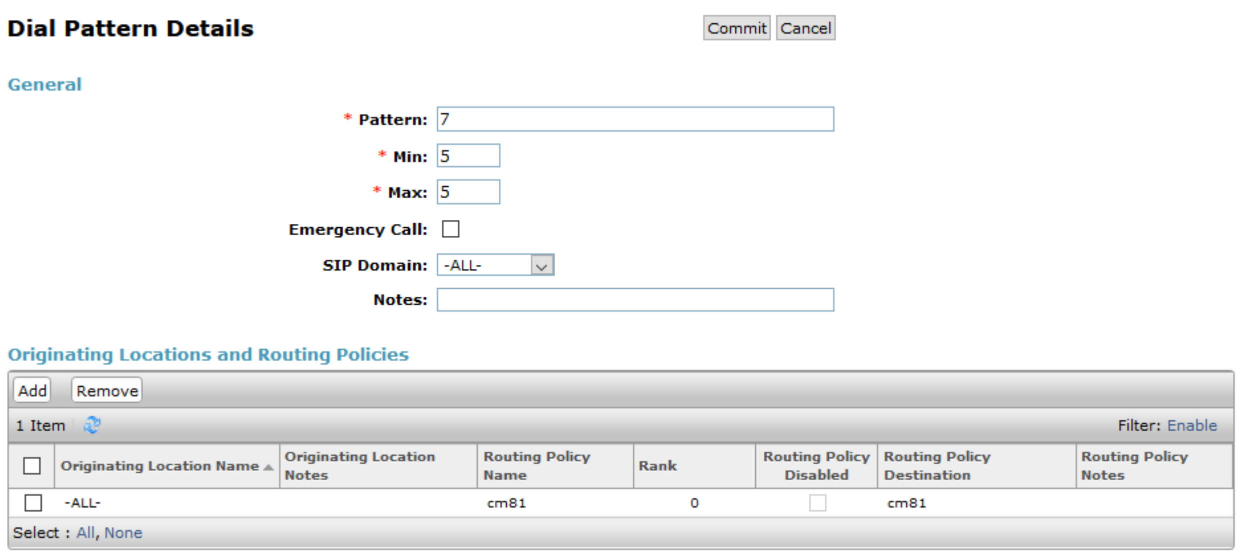


Repeat the process to add one or more dial patterns for routing calls to Communication Manager

Under **General**:

- **Pattern:** Dialed number or prefix, **7**
- **Min:** Minimum length of dialed number, **5**
- **Max:** Maximum length of dialed number, **5**
- **SIP Domain:** Select **-ALL-**

Under **Originating Locations and Routing Policies**, click **Add**, and then select the appropriate location and routing policy from the list. Default values can be used for the remaining fields. Click **Commit** to save the dial pattern. Numbers dialed with a prefix of 7 and were 5 digits long, were routed to Communication Manager.



6. Configure Avaya Aura® Communication Manager

This section contains steps necessary to configure iNETMSOFT CLASSONE® ICAS successfully with Avaya Aura® Communication Manager.

All configurations in Communication Manager were performed via SAT terminal.

6.1. Administer IP Network Region

Use the **change ip-network-region *n*** command to configure a network region, where ***n*** is an existing network region.

Configure this network region as follows:

- Set **Location** to **1**
- Set **Codec Set** to **1**
- Set **Intra-region IP-IP Direct Audio** to **yes**
- Set **Inter-region IP-IP Direct Audio** to **yes**
- Enter an **Authoritative Domain**, e.g. avaya.com

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1       NR Group: 1
Location: 1       Authoritative Domain: avaya.com
    Name:                       Stub Network Region: n
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
```

6.2. Administer IP Codec Set

Use the **change ip-codec-set** ***n*** command to configure IP codec set, where ***n*** is an existing codec set number.

Configure this codec set as follows, on **Page 1**:

- Set **Audio Codec 1** to **G.711MU**

```
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.711MU           n         2        20
 2:
 3:
 4:
 5:
 6:
 7:


     Media Encryption
 1:
 2:
 3:
```

6.3. Administer IP Node Names

Use the **change node-names ip** command to add an entry for Session Manager. For compliance testing, **sm81** and **10.64.110.212** entry was added.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
aes81               10.64.110.215
ams81               10.64.110.214
cms19               10.64.110.225
default             0.0.0.0
procr               10.64.110.213
procr6              ::
sm81                10.64.110.212
```

6.4. Administer SIP Signaling Group

Use the **add signaling-group *n*** command to add a new signaling group, where ***n*** is an available signaling group number.

Configure this signaling group as follows:

- Set **Group Type** to **sip**
- Set **Transport Method** to **tls**
- Set **Near-end Node Name** to **procr**
- Set **Far-end Node Name** to the configured Session Manager in **Section 6.3**, i.e. sm81
- Set **Far-end Network region** to the configured region in **Section 6.1**, i.e. 1

```
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? y
  Peer Detection Enabled? y  Peer Server: SM                       Clustered? n
 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: sm81
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain:
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: out-of-band            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
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

Note: Signaling Group, Trunk Group and Route Pattern for simulated PSTN calls for inter-site calls over ISDN/PRI and SIP were pre-configured and are not shown in this document.

6.5. Administer SIP Trunk Group

Use the **add trunk-group *n*** command to add a trunk group, where ***n*** is an available trunk group number.

Configure this trunk group as follows, on **Page 1**:

- Set **Group Type** to **sip**
- Enter a **Group Name**, e.g. SM Trunk
- Enter a valid **TAC**, e.g. 101
- Set **Service Type** to **tie**
- Enter **Signaling Group** value to the signaling group configured in **Section 6.4**, i.e. 1
- Enter a desired number in **Number of Member** field

```
change trunk-group 1                                            Page   1 of   5
                                TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: SM Trunk                    COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? n
 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 3**:

- Set **Number Format** to private

```
change trunk-group 1                                            Page   3 of   5
TRUNK FEATURES
          ACA Assignment? n            Measured: both
                                                      Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                                UUI Treatment: shared
                                              Maximum Size of UUI Contents: 128
                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
```

6.6. Administer Route Pattern

Use the **change route-pattern *n*** command to configure a route pattern, where ***n*** is an available route pattern.

Configure this route pattern as follows:

- Type a name in **Pattern Name** field
- For line 1, set **Grp No** to the trunk group configured in **Section 6.5**, i.e. 1
- For line 1, set **FRL** to **0**

```
change route-pattern 1                                          Page   1 of   4
                    Pattern Number: 1      Pattern Name: SM
    SCCAN? n    Secure SIP? n     Used for SIP stations? 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
```

6.7. Administer Private Numbering

Use the **change private-numbering 0** command to define the calling party number to send to Session Manager.

Configure private numbering as follows:

- Add entries for trunk group configured in **Section 6.5**

Note: For compliance testing, 5-digit extensions beginning with 7 routed over trunk groups 1 resulted in a 5-digit calling party number.

```
change private-numbering 0                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext                  Trk        Private          Total
Len Code                 Grp(s)     Prefix           Len
 5  7                    1                           5  Total Administered: 1
                                                          Maximum Entries: 540
```

6.8. Configure AAR Analysis

Use **change aar analysis *n*** command to add an entry in aar table, where ***n*** is an extension number that will be used to route calls to Meeting Exchange.

```
change aar analysis 43                                             Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 0

          Dialed           Total      Route    Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    43                    5    5     1         aar          n
```

6.9. Configure Vectors

Use **change vector *n*** to configure a Vector, where ***n*** is an available Vector number.

```
change vector 101                                                 Page   1 of   6
                                  CALL VECTOR

    Number: 101              Name: ClassOne
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    2   secs hearing ringback
02 route-to     number 43001                   cov n if unconditionally
03 wait-time    30  secs hearing ringback
```

6.10. Configure VDN

Use **add vdn *n*** to add a vdn, where ***n*** is an available vdn extension**.** On Page 1:

- In the **Name** field, enter a descriptive name
- In the **Destination** field, set **Vector Number** to the vector configured earlier in this document (**Section 6.9**). i.e., Vector Number 101.

```
change vdn 73999                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 73999                    Unicode Name? n
                                 Name*: ClassOne VDN
                           Destination: Vector Number        101
                   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:
```

7. Configure Avaya Meeting Exchange

This section contains steps necessary to configure iNEMSOFT CLASSONE® iCAS successfully with Meeting Exchange.

7.1. Create login users for Avaya Meeting Exchange

Log in to Meeting Exchange via SSH client using appropriate credentials as a super user. Type in **dm** to launch the **System Maintenance Main Menu** window

```
                   mx62.avaya.com -- station 257
             Avaya, Inc.                      Audio Conferencing System
     P/N: S0700500  Revision: 01             Copyright 2007 Avaya, Inc.




                      lqq System Maintenance Main Menu qqk
                      x                                  x
                      x      Network Configuration       x
                      x       FDAPI Configuration        x
                      x        LAN Configuration         x
                      x        Administrator Menu        x
                      x        Re-Initialization         x
                      x         System Shutdown          x
                      x        Transmission Level        x
                      x               EXIT               x
                      mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

Navigate to **Administrator Menu → Sign-In Management → Create Operator Sign-In.** Create login user by typing in **Sign-In Name** and **Password**, followed by ‘ESC’, then **Y** to save. e.g, userID=rtisvr1 and password=rti **(** the user type can be either ‘administrator’ or ‘operator’ type)

```
mx-bridge -- station 257
              Avaya, Inc.                      Audio Conferencing System
      P/N: S0700500  Revision: 01             Copyright 2007 Avaya, Inc.

         lqqqqqqqqqqqqqqqqqqqCreate Operator Sign-Inqqqqqqqqqqqqqqqqqqqqqk
         x                                                              x
         x Sign-In Name    : rtisrv1                                    x
         x Password        : rti                                        x
         x Telephone Number:                                            x
         mqqqqqqqqqqqqqqqqqqqqqqqq ESC to Exit qqqqqqqqqqqqqqqqqqqqqqqqqj
```

Continue from above, **Administrator Menu → Configure Conference Scheduler**. Configure the scheduler as shown in the screen capture below.

```
                              mx-bridge -- station 257
              Avaya, Inc.                      Audio Conferencing System
      P/N: S0700500  Revision: 01             Copyright 2007 Avaya, Inc.

                 lqqqqqqqConfigure Conference Schedulerqqqqqqqqk
                 x                                             x
                 x Group Name                      : schedule   x
                 x Status                          : ENABLED    x
                 x Invalid Code                    : HANG-UP    x
                 x Timeout                         : HANG-UP    x
                 x Conference Secured              : HANG-UP    x
                 x Max. Lines Reached              : HANG-UP    x
                 x Invalid Time of Day             : HANG-UP    x
                 x Scan Time (5-20)                : 10         x
                 x Scan Attempts (1-3)             : 3          x
                 x Auto Hang-up                    : DISABLED   x
                 mqqqqqqq More-Next/Prev Page ESC to Exit qqqqqqj
```

7.2. DTMF Tone Configuration

Continue from above, naviagate to **Administrator Menu → Configuration → System Config,** configure Page 1 and Page 2 as shown in the screen captures below.

```
       mx-bridge -- station 257
              Avaya, Inc.                      Audio Conferencing System
      P/N: S0700500  Revision: 01             Copyright 2007 Avaya, Inc.

 lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqSystem Configurationqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
 x                                                                              x
 x System Name          : mxdev62o    Operator Assistance  : INDVL              x
 x Entry Tone           : 1-Beep      Automatic Conf. ID   : OFF                x
 x Exit Tone            : 1-Beep      Starting  Conf. ID   : 000000000001       x
 x DTMF Acknowledge     : OFF         Conference Gain      : OFF                x
 x Bridge ID Num (0-255): 0           Moderator Lecture    : ON                 x
 x Playback Roll Call   : OFF         Playback Mute        : OFF                x
 x Transaction Logs     : OFF         Self Mute            : Anyone             x
 x Automatic CDR Print  : OFF         Secure Blocks Record : ON                 x
 x Automatic Record All : OFF         Sub Conferencing Mode: OFF                x
 x Automatic Conf. Clear: OFF         On-Hold Msg Frequency: OFF                x
 x Attended ODO         : OFF         Startup Notify Time  : OFF                x
 x First Person Message : OFF         Date Format          : mm/dd/yyyy         x
 x Auto-Extend-Duration : OFF         Time Format          : 12-hour clock      x
 x Auto-Extend-Ports    : OFF                                                   x
 x Early Start Minutes  : OFF                                                   x
 x Ignore DTMF Commands : ON          Conference Passcode  : OFF                x
 x                                                                              x
 mqqqqqqqqqqqqqqqqqqqqqqq More-Next/Prev Page ESC to Exit qqqqqqqqqqqqqqqqqqqqqqqj
```

```
mx-bridge -- station 257
              Avaya, Inc.                       Audio Conferencing System
      P/N: S0700500  Revision: 01             Copyright 2007 Avaya, Inc.

 lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqSystem Configurationqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
 x                                                                              x
 x Bridge Record        : On-bridge                                             x
 x Phone Number         :                                                       x
 x Dial String          :                                                       x
 x PreDial Delay Period : 2           NRP Seconds         : 0                   x
 x Log User Transaction : ON          Web ID Length       : 0                   x
 x DRP: Auto-gen fname  : OFF         DTMF Conf. Hangup   : DISABLED            x
 x Single Person (SP) 1st Period : 0  DTMF Regeneration   : ON                  x
 x   # of SP Subsequent Prompts  : 0  DTMF Passthrough    : OFF                 x
 x   SP Prompt Waiting Period    : 5  Billing Code Length : 0                   x
 x   Participant Threshold       : 0  System Alert        : OFF                 x
 x Recite wrong passcode: OFF         System Message      : 0                   x
 x Country Code         :             Small Jump          : 60                  x
 x International Prefix :             Medium Jump         : 300                 x
 x Local Prefix         :             Long Jump           : 1200                x
 x                                                                              x
 x MoHang Msg Dest      : INDVL                                                 x
 x Conf Sec Msg Dest    : INDVL                                                 x
 mqqqqqqqqqqqqqqqqqqqqqqq More-Next/Prev Page ESC to Exit qqqqqqqqqqqqqqqqqqqqqqqj
```

Exit the **dm** menu and type in **config**. Edit softMediaServer.cfg file. Set the highlighted fields to the values shown in the screen capture below.

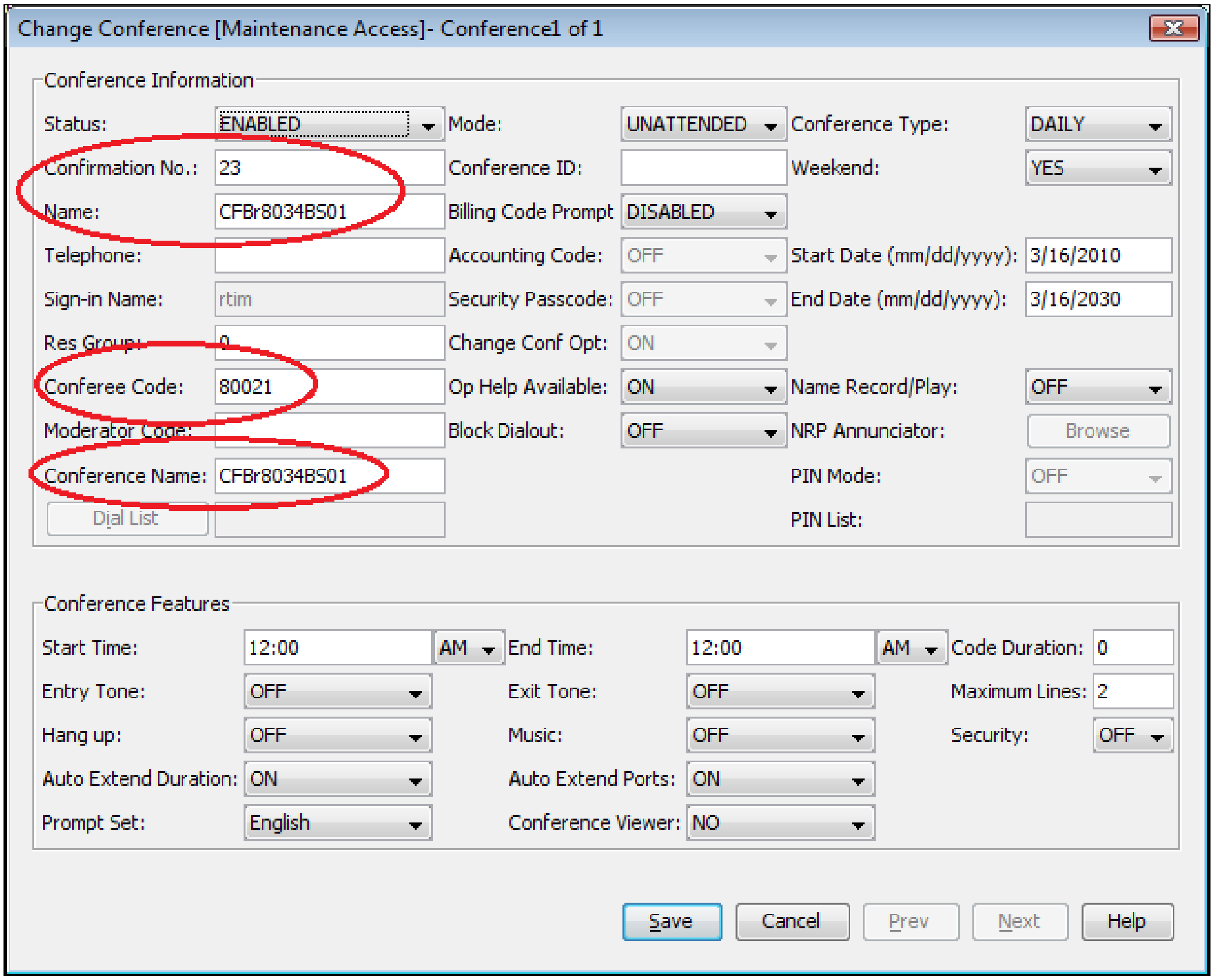
```
# [description: Decision factors for inband DTMF: reverse twist, forward twist and
threshold minimum.
# [type: int]
# [runtime: false]
dtmfReverseTwistDifference=-12
dtmfForwardTwistDifference=-11
dtmfTMinLevel=-36
```

Meeting Exchange needs to be restarted for the changes made above become effective. Type **service mx-bridge restart** to restart Meeting Exchange.

7.3. Schedule a heartbeat conference for each CLASSONE® CFBrSrv instance via Avaya Bridge Talk

Configuration for Meeting Exchange conferences is performed via Avaya Bridge Talk, which is installed on a Windows PC.

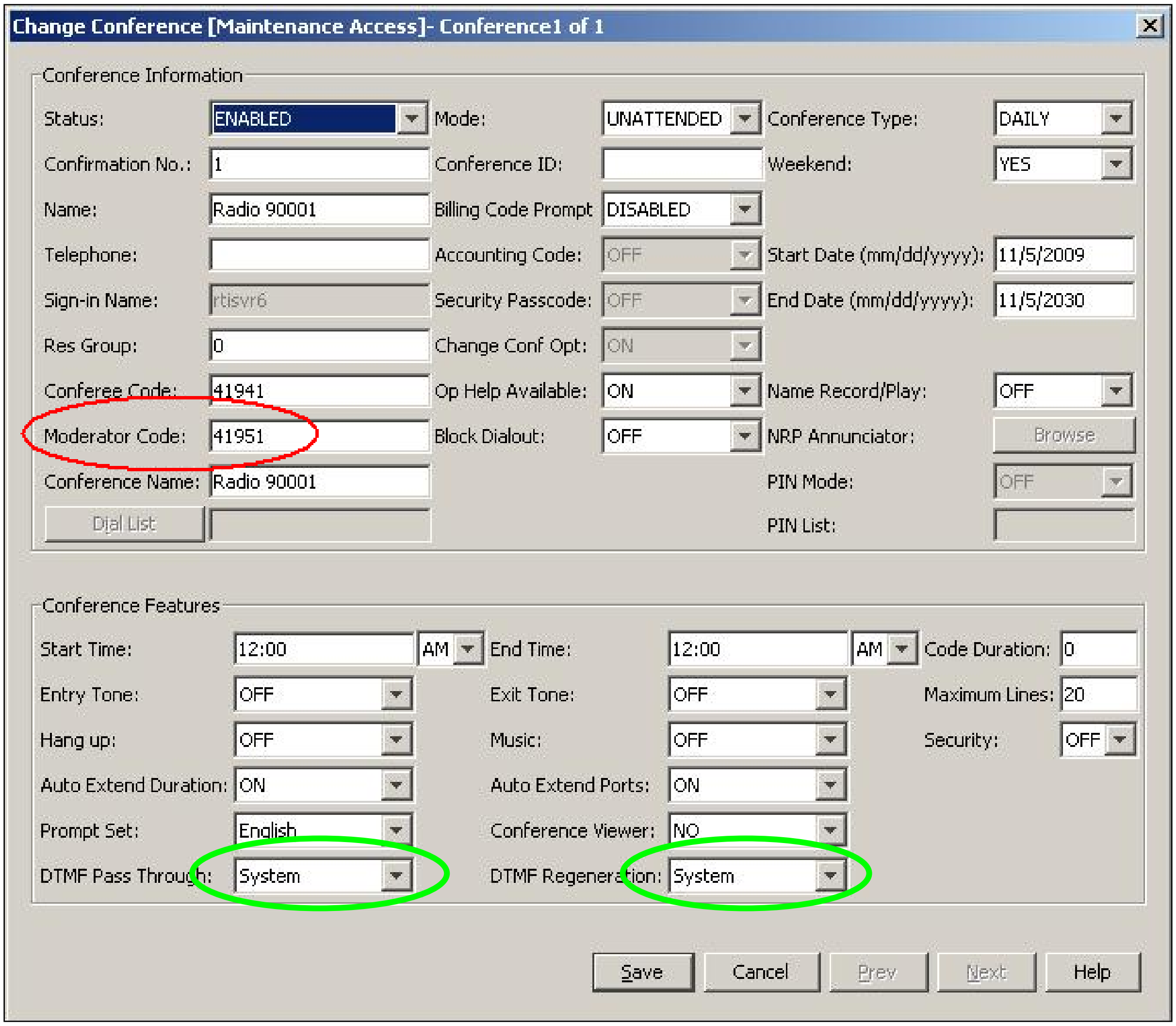
1. Start Avaya Bridge Talk
2. Open 'Conference Scheduler' window by:
   View menu → Conference Scheduler
3. Open Schedule Conference window by:
   Conference Scheduler's **File** menu → **Schedule Conference...**
4. Fill in data in 'Schedule Conference', refer following screen shot as an example
   NOTE:
   - *'Conferee Code' field uses the following naming rule*
     - Prefix 800
     - (The digit immediate before the last digit) 1 for group A and 2 for group B
     - (The last digit) 2 represent the server# ('2' represents server 2 or server 12)
   - *'Name' and 'Conference Name' fields may be the same. It should indicate the corresponding Meeting Exchange, the failover group and the embedding server. An example is CFBr8034BS01*
   - *'Confirmation No' field must be unique. If error pups up, increase this number*


Change Conference [Maintenance Access]- Conference1 of 1
Conference Information
Status: ENABLED
Mode: UNATTENDED
Conference Type: DAILY
Confirmation No.: 23
Conference ID:
Weekend: YES
Name: CFBr8034BS01
Billing Code Prompt DISABLED
Telephone:
Accounting Code: OFF
Start Date (mm/dd/yyyy): 3/16/2010
Sign-in Name: rtim
Security Passcode: OFF
End Date (mm/dd/yyyy): 3/16/2030
Res Group: 0
Change Conf Opt: ON
Conferee Code: 80021
Op Help Available: ON
Name Record/Play: OFF
Moderator Code:
Block Dialout: OFF
NRP Annunciator: Browse
Conference Name: CFBr8034BS01
PIN Mode: OFF
Dial List
PIN List:
Conference Features
Start Time: 12:00 AM
End Time: 12:00 AM
Code Duration: 0
Entry Tone: OFF
Exit Tone: OFF
Maximum Lines: 2
Hang up: OFF
Music: OFF
Security: OFF
Auto Extend Duration: ON
Auto Extend Ports: ON
Prompt Set: English
Conference Viewer: NO
Save
Cancel
Prev
Next
Help

7.4. Schedule a conference on Avaya Bridge Talk for each radio VDN that is registered in CM

CLASSONE® iCAS requires every radio VDN defined in Communication Manager and its Conference Code defined on every Bridge to be identical.

1. Start Avaya Bridge Talk
2. Open **Conference Scheduler** window by:
   View menu → **Conference Scheduler**
3. Open **Schedule Conference** window by:
   Conference Scheduler's **File** menu → **Schedule Conference...**
4. Fill in data in **Schedule Conference**, refer following screen shot as an example
   NOTE:
   - *'Name', 'Conference Name' and 'Conferee Code' fields may all use radio's VDN.*
   - *'Maximum Line' field is set up according to business requirement. In iNETMSOFT lab, we set it to 20. (The maximum line should be set to auto-expandable normally on the MX)*
   - *'Confirmation No' field must be unique. If error pups up, increase this number.*
   - *Moderator Code must be unique*
   - *set 'DTMF Pass Through' and 'DTMF Regeneration' to 'System' (if not visible, set as following, for Bridge Talk 5.2 or later)*



Right click **Avaya Bridge Talk** shortcut, select **Properties** then select **Find Target** to get into the directory where **Avaya Bridge Talk.ext** installed, edit the template.xml file, change:

<Property value="**false**" type="Boolean" name="EnableDTMFPassThrough" hidden="false" />

to

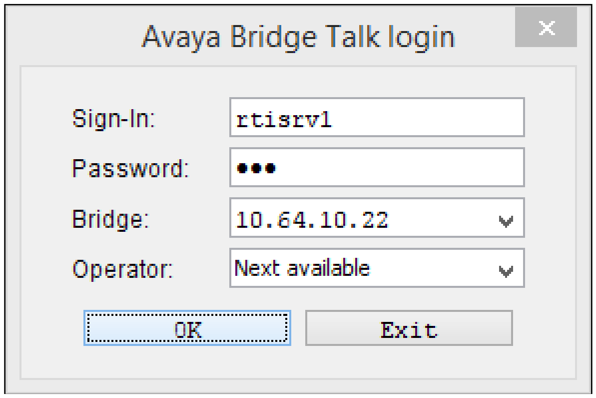
<Property value="**true**" type="Boolean" name="EnableDTMFPassThrough" hidden="false" />

8. Configure iNEMSOFT CLASSONE® iCAS

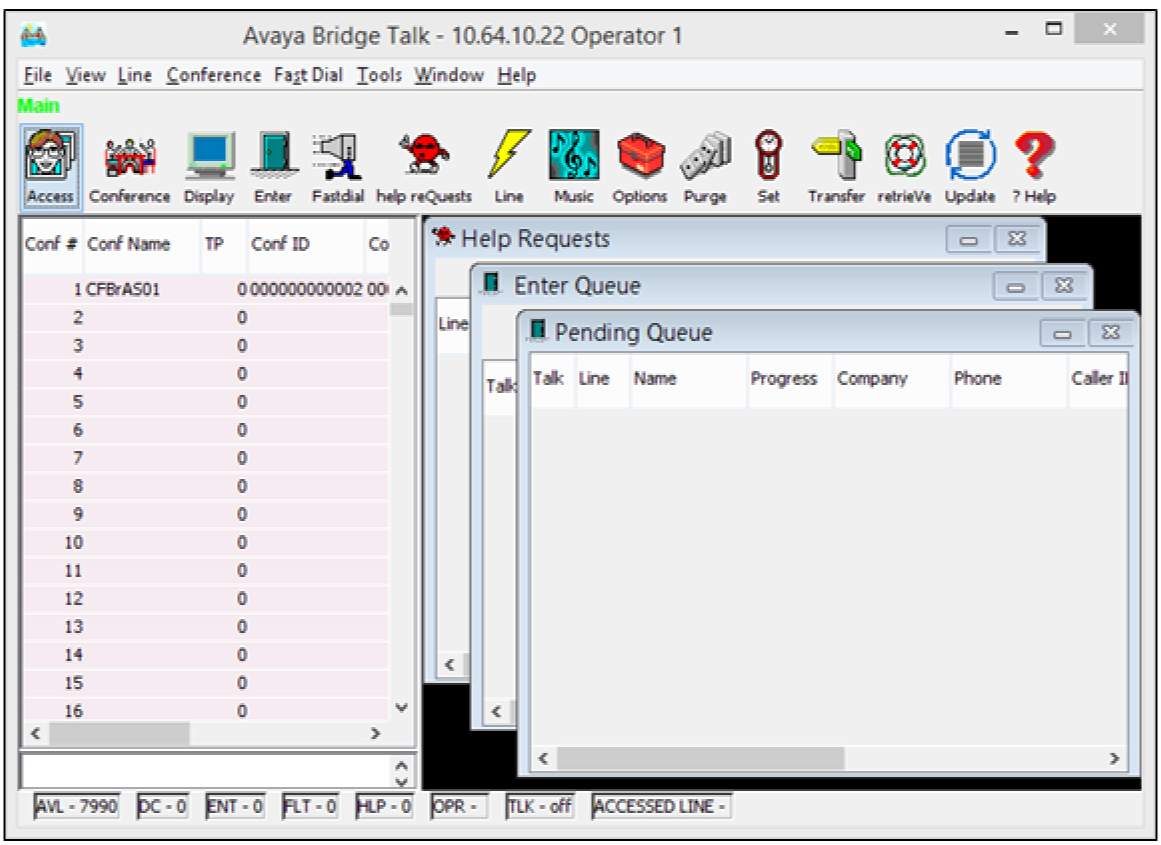
Configuration of iNEMSOFT CLASSONE® iCAS is done by designated iNEMSOFT engineers. Hence, no configuration is provided in this document.

9. Verification Steps

Verify the newly created user from **Section 7.1** by login them via Avaya Bridge Talk.



If login was created successfully, user will be able to log in successfully.



10. Conclusion

iNEMSOFT CLASSONE® iCAS was able to successfully interoperate with Avaya Meeting Exchange. All executed test cases were passed.

11. Additional References

This section references the product documentation relevant for these Application Notes.

[1] Administering Avaya Aura® Communication Manager, Release 8.1.x, Issue 4, November 2019.

[2] Administering Avaya Aura® Application Enablement Services, Release 8.1.x, Issue 3, October 2019

[3] Administering Avaya Aura® Session Manager, Release 8.1.1, Issue 2, October 2019

[4] Implementing Avaya™ Meeting Exchange, Release 6.2, 04-604003, Issue 1, November 2012

Documentation related to iNEMSOFT CLASSONE® iCAS can be directly obtained from iNEMSOFT.

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.