



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya one-X[®] Speech, Single Server Avaya Modular Messaging and Avaya Aura[™] Session Manager as part of Avaya Unified Communication Mobile Worker Solution – Issue 1.1

Abstract

These Application Notes describe the steps required to configure Avaya one-X[®] Speech and Single Server Avaya Modular Messaging to provide centralized functionality to multiple Avaya Aura[™] Communication Manager systems using Avaya Aura[™] Session Manager. Avaya one-X[®] Speech provides an interface that allows subscribers, regardless of their locations, to use speech commands to access and manage voice messages, place calls, and access to email through a telephone. Voice messages are managed using Avaya Modular Messaging and corporate email is managed on Microsoft Exchange using Avaya one-X[®] Speech.

1. Introduction

These Application Notes describe the steps required to configure Avaya One-X[®] Speech and Single Server Avaya Modular Messaging to provide centralized functionality to multiple Avaya Aura[™] Communication Manager systems using Avaya Aura[™] Session Manager. **Figure 1** shows the overall context in which the testing for these Application Notes took place. The scenario was designed to test the Avaya Unified Communication Mobile Worker Solution. This allows users in different locations to have full access to Avaya services. The configuration can be broken down into three types of user or location:

- Enterprise Office User
- Remote User
- Branch Office User

The Enterprise Office User has access to services via normal corporate network connections including wireless LAN. Services include access to centralized Avaya Modular Messaging (voicemail), Avaya one-X[®] Speech functionality, Avaya Web Conferencing, Avaya Meeting Exchange, Avaya Intelligent Presence Service and a wireless network or GSM connection for Avaya one-X[®] Mobile enabled handsets. The Avaya Aura[™] Communication Manager systems reside on both Enterprise and Remote Sites. End users are configured to use a variety of end points including one-X[®] Communicator, one-X[®] Portal, Avaya desk phones and a selection of third party mobile phones.

The Remote User has access to the same services on the Enterprise Site by using either an SSL or IPSEC VPN connection. The Remote User can be located in a home office, an airport, a hotel room or anywhere with access to either GSM or a network connection. In these cases the one-X[®] Mobile, one-X[®] Communicator and Avaya 9630 VPN desk phone can be used as end points.

The Branch Office User is situated in a separate office location. The Branch Office uses the centralized services located at the Enterprise Office. Connection of one-X[®] Mobile to either Avaya Aura[™] Communication Manager is again via GSM or a wireless network depending on the location.

An example Avaya Unified Communication Mobile Worker Solution is shown in **Figure 1**.

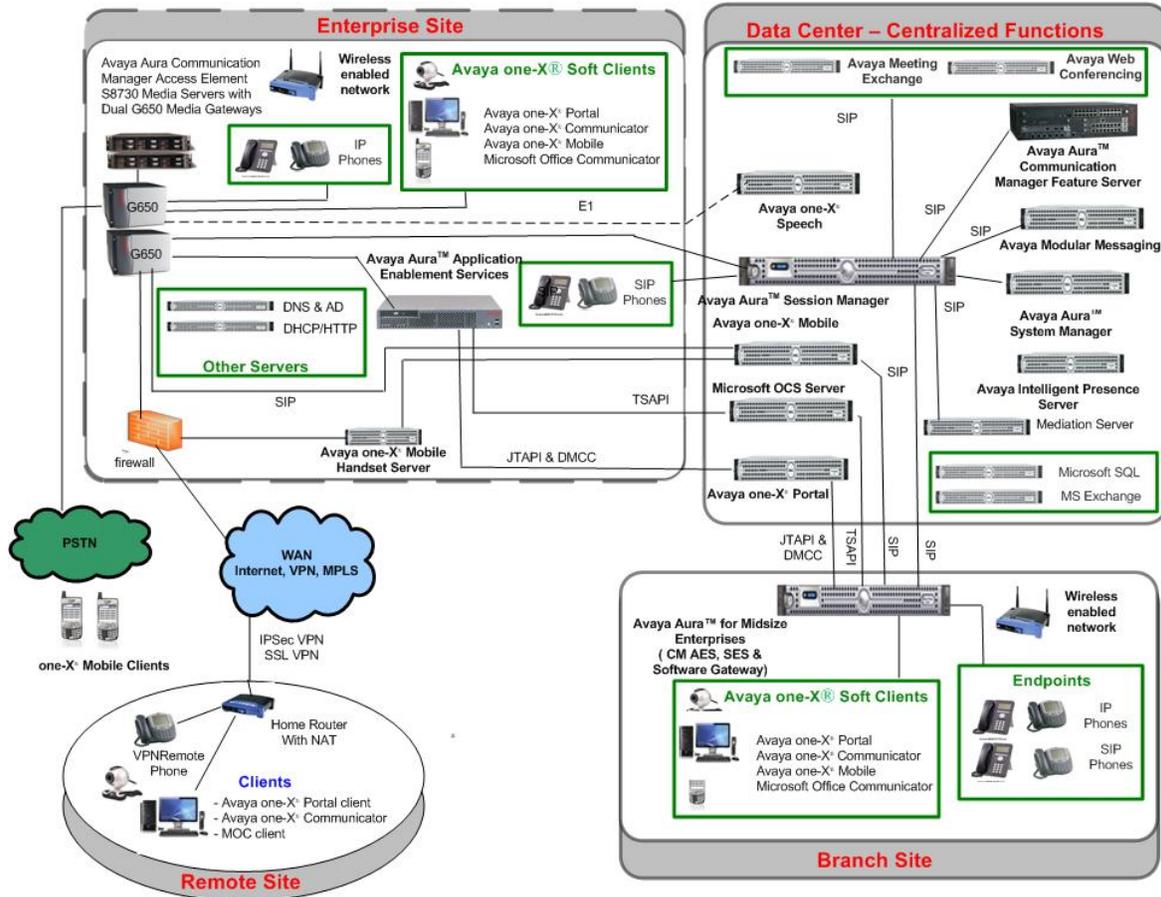


Figure 1: Sample Avaya Unified Communication Mobile Worker Solution

For the purposes of these Application Notes only the configuration relevant to Avaya Modular Messaging and Avaya one-X[®] Speech will be described in detail as shown in **Figure 2**. For details of other products not covered within please refer to **Section 10**.

Avaya one-X[®] Speech provides an interface that allows subscribers, regardless of their location, to use speech commands to access and manage voice messages, place calls, and access to email through a telephone. Voice messages are managed using Modular Messaging and corporate email is managed using Microsoft Exchange. Using a telephone, one-X[®] Speech subscribers communicate in spoken English. one-X[®] Speech employs Automatic Speech Recognition (ASR) technology to respond to speech commands and uses Text-to-Speech (TTS) technology to read text messages. The one-X[®] Speech Server provides speech access to voicemail and e-mail data stores through a telephony connection with Avaya Aura[™] Communication Manager. Using standards-based communication protocols, the one-X[®] Speech Server communicates with external systems through Local Area Networks (LANs), and with Avaya Aura[™] Communication Manager through an E1 connection. External systems include voice messaging servers, e-mail

servers, and corporate directories using the Lightweight Directory Access protocol (LDAP). **Figure 2** illustrates the network configuration used to verify these Application Notes.

Avaya Modular Messaging is connected using SIP to Avaya Aura™ Session Manager. In the sample configuration, Avaya Aura™ for Midsize Enterprises S8800 is connected to the Avaya Aura™ Session Manager. Also connected is Avaya S8730 acting as Avaya Aura™ Communication Manager Access Element. For simplicity these Application Notes concentrate on the configuration of these two Avaya Aura™ Communication Manager systems. However Avaya Aura™ Communication Manager Feature Server is also shown in **Figure 2** to allow for SIP endpoint registration on Avaya Aura™ Session Manager.

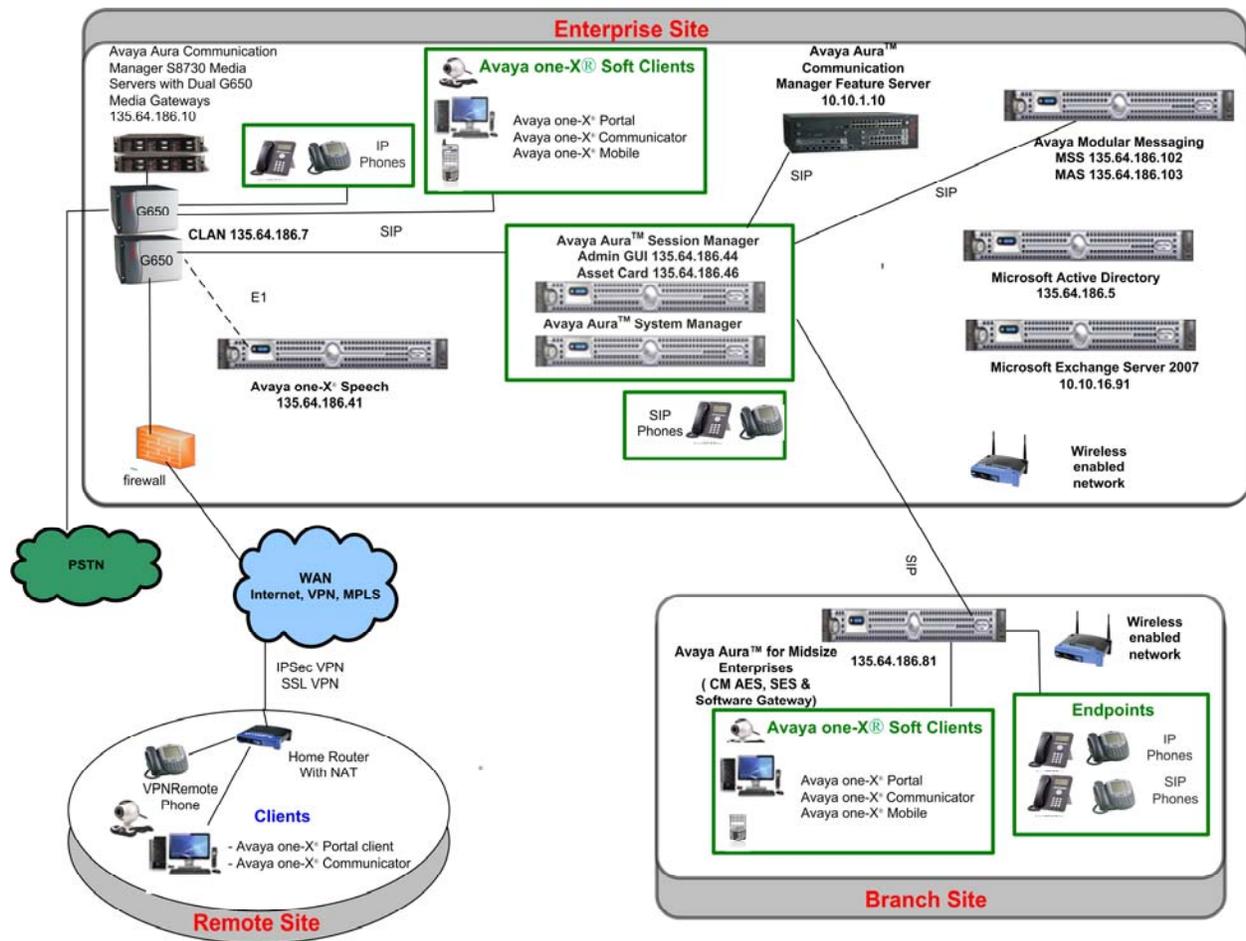


Figure 2: Avaya Modular Messaging and Avaya one-X® Speech Test Configuration

2. Equipment and Software Validated

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

Component	Version
Avaya S8800	Avaya Modular Messaging 5.2 (9.2.150.13)
Avaya 8730	Avaya one-X® Speech 5.2.0.0.38
Avaya S8720 Server (Access Element Server)	Avaya Aura™ Communication Manager 5.2 (S8720-015-02.1.016.4 with update 17774)
Avaya G650 Media Gateway TN2312BP IP Server Interface (IPSI) TN799DP Control-LAN (C-LAN) TN464GP DS1 Interface TN2224CP Digital Line TN2602AP IP Media Resource 320 (MedPro)	HW15 FW049 HW01 FW034 HW06 FW020 HW08 FW015 HW08 FW049
Avaya 9630 IP Telephone	Avaya one-X® Deskphone Edition H.323 Release S3.0
Avaya 9640 IP Telephone	Avaya one-X® Deskphone Edition H.323 Release S3.0
Avaya 4620SW IP Telephone	2.9
Avaya Aura™ System Manager Server S8510	5.2.0.1- SP0
Avaya Aura™ Session Manager Server S8510	5.2.0.1- SP0
Avaya Feature Server	Avaya Aura™ Communication Manager 5.2 (S8720-015-02.1.016.4 with update 17774)
Avaya Aura™ for Midsize Enterprises S8800	5.2.1.2.5
Microsoft Windows Server 2003 R2 x64 Edition Service Pack 2	Microsoft Exchange 2007 Version 08.01.0240.006
Microsoft Active Directory on Microsoft Windows Server 2003 R2 x64 Edition Service Pack 2	5.2.3790.3959

3. Configure Avaya Aura™ Communication Manager

This section discusses the configuration of both the various Communication Managers to allow integration with Modular Messaging via Session Manager. Full details of how to configure Communication Manager to connect to Modular Messaging via Session Manager are outlined in Reference [11]. The main difference between Reference [11] and the configuration shown in Figure 2 is that only a single Session Manager is used to connect to Modular Messaging.

3.1. Avaya Aura™ Communication Manager (Access Element)

This section discusses in detail the configuration of the Access Element Communication Manager to allow connection to Session Manager.

3.1.1. System Parameters Customer Options

Use the **display system-parameters customer-options** command. Navigate to **Page 2** and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections. Verify highlighted value, as shown below.

display system-parameters customer-options		Page	2 of	11
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
	Maximum Administered H.323 Trunks:	30	0	
	Maximum Concurrently Registered IP Stations:	18000	10	
	Maximum Administered Remote Office Trunks:	0	0	
Maximum Concurrently Registered Remote Office Stations:		0	0	
	Maximum Concurrently Registered IP eCons:	0	0	
Max Concur Registered Unauthenticated H.323 Stations:		0	0	
	Maximum Video Capable Stations:	10	1	
	Maximum Video Capable IP Softphones:	10	9	
	Maximum Administered SIP Trunks:	100	75	

3.1.2. Node Names IP

Use the **change node-names ip** command to configure the host **Name** and **IP Address** of the **clan1a3** interface server and the **SM100** (Session Manager Asset Card) that will terminate the SIP trunks. The host names will be used in the signalling group configuration discussed later.

```
change node-names ip                                     Page 1 of 2
```

Name	IP Address	IP NODE NAMES
Gateway001	135.64.186.1	
MBT	135.64.186.81	
MBTCM	135.64.186.68	
MX6200	135.64.186.15	
SM100	135.64.186.46	
StackFeature	10.10.1.11	
clan1a3	135.64.186.6	
clan1b3	135.64.186.7	
clanPSTN	10.10.16.115	
default	0.0.0.0	
mpro1a2	135.64.186.8	
mpro1b2	135.64.186.9	
onexmobile	135.64.186.30	
procr	135.64.186.10	
silstackaes	135.64.186.28	

3.1.3. IP Network Region

The **Authoritative Domain** field is configured to match the domain name configured on the Session Manager. This is configured by running the **change ip-network region n**, where n is an available ip-network region number. In this configuration, the domain name is **silstack.com**. By default, **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** (shuffling) are enabled (**yes**) to allow audio traffic to be sent directly between SIP endpoints without using media resources in the Avaya G650 Media Gateway. The IP Network Region form also specifies the **IP Codec Set** to be used for calls to Modular Messaging. This IP codec set is used when its corresponding network region (i.e., IP Network Region **1**) is specified in the SIP signaling groups shown in **Section 3.1.5**. Accept the default values for the other fields.

```
change ip-network-region 1                               Page 1 of 19
                                     IP NETWORK REGION
Region: 1
Location: 1      Authoritative Domain: silstack.com
Name: Stack
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
                      Inter-region IP-IP Direct Audio: yes
                      IP Audio Hairpinning? n
Codec Set: 1
  UDP Port Min: 2048
  UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS      RTCP Reporting Enabled? y
Call Control PHB Value: 46    RTCP MONITOR SERVER PARAMETERS
  Audio PHB Value: 46        Use Default Server Parameters? y
  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
```

3.1.4. IP Codec

Use the **change ip-codec-set n** command, where n is an available ip-codec-set number as shown below, to select the audio codec type supported for calls to Modular Messaging. Note that IP codec set **1** was specified in IP Network Region '1' shown in **Section 3.1.3**. The default settings of the ip-codec-set form are shown below.

```
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.722.1-32K          1          20
2: G.711MU              n          2          20
3:
4:
5:
6:
7:
```

3.1.5. Signaling Group

Add Signaling Group for Calls to the Session Manager using the command **add signaling-group n**, where n is an available signaling-group number as shown below. 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:

- **Group Number:** 120 in this example
- **Group Type:** sip
- **Transport Method:** tls for secure connection
- **Near-end Node Name:** clan1a3 as configured in **Section 3.1.2**
- **Far-end Node Name:** SM100 the asset card of the Session Manager
- **Near-end Listen Port:** 5061 in this example
- **Far-end Listen Port:** 5061 in this example
- **Far-end Domain:** Can be left blank
- **Far-end Network Region:** 1
- **Direct IP-IP Audio Connections:** y to enable audio shuffling
- **Enable Layer 3 Test :** y

```
change signaling-group 120                                     Page 1 of 1
                                                              SIGNALING GROUP
Group Number: 120                                           Group Type: sip
                                                              Transport Method: tls
IMS Enabled? n
IP Video? n
Near-end Node Name: clan1a3                                 Far-end Node Name: SM100
Near-end Listen Port: 5061                                  Far-end Listen Port: 5061
                                                              Far-end Network Region: 1
Far-end Domain:
Incoming Dialog Loopbacks: eliminate                       Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                                  RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3                        Direct IP-IP Audio Connections? y
                                                              IP Audio Hairpinning? n
Enable Layer 3 Test? y                                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? y                    Alternate Route Timer(sec): 6
```

3.1.6. Trunk Group

Configure the Trunk Group for calls to the Session Manager using the **add trunk-group n** command, where n is an available trunk group number. Set the **Group Type** field to **sip**, 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.

```
change trunk-group 120                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 120                Group Type: sip                CDR Reports: y
  Group Name: Main Trunk To ASM    COR: 1                TN: 1                TAC: 120
  Direction: two-way              Outgoing Display? n
Dial Access? n                    Night Service:
Queue Length: 0
Service Type: tie                Auth Code? n

                                     Signaling Group: 120
                                     Number of Members: 10
```

On **Page 3** of the trunk group form, set the **Numbering Format** field to **public**. The specific calling party number format is specified in the Public Unknown Numbering form as described in **Section 3.1.8**.

```
change trunk-group 120                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                Measured: none
                                     Maintenance Tests? y

                                     Numbering Format: public
                                     UUI Treatment: service-provider
                                     Replace Restricted Numbers? n
                                     Replace Unavailable Numbers? n

Show ANSWERED BY on Display? y
```

3.1.7. Route Pattern

Configure a Route Pattern Trunk to correspond to the newly added SIP trunk group using the **change route-pattern n** command, where n is an available trunk group number as shown. Set the following values for the specified fields:

- **Pattern Name:** A descriptive name i.e. **To SMStack**
- **Grp No:** The trunk group number from **Section 3.1.6**
- **FLR:** Enter a level that allows access to this trunk, with **0** being least restrictive.
- **No Del Dgts:** **0**

```
change route-pattern 120                                     Page 1 of 3
                    Pattern Number: 120 Pattern Name: To SMStack
                    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: 120  0                                0          n  user
2:                                     n          n  user
3:                                     n          n  user
4:                                     n          n  user
5:                                     n          n  user
6:                                     n          n  user

  BCC VALUE TSC CA-TSC      ITC BCIE Service/Feature PARM No. Numbering LAR
  0 1 2 M 4 W      Request      Subaddress
1: y y y y y n  n          unre          none
2: y y y y y n  n          rest          none
3: y y y y y n  n          rest          none
4: y y y y y n  n          rest          none
5: y y y y y n  n          rest          none
6: y y y y y n  n          rest          none
```

3.1.8. Public Unknown Numbering

Configure the Public Unknown Numbering form to send the calling party number to Modular Messaging using the command **change public-unknown-numbering n**, where n is an available public unknown number as shown. Add an entry so that local stations with a 5-digit extension beginning with 2 are sent to Modular Messaging. This allows Modular Messaging to provide the proper greeting on calls that cover to voicemail and to automatically recognize subscribers when retrieving messages. Since the **Trk Grp(s)** field is blank, this entry will apply for all outgoing trunk groups.

```

change public-unknown-numbering 1                               Page 1 of 2
                NUMBERING - PUBLIC/UNKNOWN FORMAT
Ext Ext          Trk      CPN          Total
Len Code        Grp(s)   Prefix     Len
5  2
                Total Administered: 1
                Maximum Entries: 9999
  
```

3.1.9. Hunt Group

Configure a Hunt Group for Voice Messaging using the command **add hunt-group n**, where n is an available hunt group number as shown. Specify the voicemail pilot number in the **Group Extension** field. In this example, extension 20900 is dialed by users to access the Voice Mail box.

```

add hunt-group 1                                               Page 1 of 60
                HUNT GROUP
                Group Number: 1                                ACD? n
                Group Name: VoiceMail                         Queue? n
                Group Extension: 20900                       Vector? n
                Group Type: ucd-mia                          Coverage Path:
                TN: 1                                         Night Service Destination:
                COR: 1                                         MM Early Answer? n
                Security Code:                                Local Agent Preference? n
                ISDN/SIP Caller Display: mbr-name
  
```

On **Page 2** of the **Hunt Group**, set the **Message Center** field to **sip-adjunct** since Modular Messaging is accessed via SIP. Set the **Voice Mail Number** field to the digits used to route calls to Modular Messaging (e.g., the same hunt group extension is used here) and set the **Routing Digits** field to the AAR or ARS access code. In this example, the **AAR/ARS Access Code** was set to ***8** which is used to route calls. The voice mail number is used by the Communication Manager to route calls to Modular Messaging. The **Voice Mail Handle** is set to **VoiceMail**.

```

add hunt-group 2                                               Page 2 of 60
                HUNT GROUP
                Message Center: sip-adjunct
                Voice Mail Number      Voice Mail Handle      Routing Digits
                20900                 VoiceMail              (e.g., AAR/ARS Access Code)
                *8
  
```

3.1.10. Feature Access Code

Using the command **change feature-access-codes**, configure the feature access code to route calls using the AAR feature. **Auto Alternate Routing (AAR) Access Code** is set to ***8** as shown. This matches what was configured in **Section 3.1.9**.

```
change feature-access-codes                                     Page 1 of 6
                                FEATURE ACCESS CODE (FAC)
Abbreviated Dialing List1 Access Code:
Abbreviated Dialing List2 Access Code:
Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
Announcement Access Code:
Answer Back Access Code:
Attendant Access Code:
Auto Alternate Routing (AAR) Access Code: *8
Auto Route Selection (ARS) - Access Code 1:                Access Code 2:
Automatic Callback Activation:                            Deactivation:
Call Forwarding Activation Busy/DA:                       All:           Deactivation:
Call Forwarding Enhanced Status:                          Act:           Deactivation:
Call Park Access Code:
Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
CDR Account Code Access Code:
Change COR Access Code:
Change Coverage Access Code:
Contact Closure Open Code:                               Close Code:
```

3.1.11. Coverage Path

Configure the coverage path to be used for the voice messaging hunt group using the command **add coverage path n**, where n is an available coverage path number. In this sample the coverage path to be used for the voice messaging hunt group is group **h1** referring to the hunt group configured in **Section 3.1.10**. The default values shown for **Busy**, **Don't Answer**, and **DND/SAC/Goto Cover** can be used for the **Coverage Criteria**.

```
add coverage path 1
                                COVERAGE PATH
                                Coverage Path Number: 1
Cvg Enabled for VDN Route-To Party? n                    Hunt after Coverage? n
                                Next Path Number:      Linkage

COVERAGE CRITERIA
Station/Group Status   Inside Call   Outside Call
Active?                n             n
Busy?                  Y             Y
Don't Answer?         Y             Y           Number of Rings: 2
All?                   n             n
DND/SAC/Goto Cover?   Y             Y
Holiday Coverage?     n             n

COVERAGE POINTS
Terminate to Coverage Pts. with Bridged Appearances? n
Point1: h1             Rng:2 Point2:
Point3:                Point4:
Point5:                Point6:
```

3.1.12. Locations

Use the **change locations** command to assign the SIP route pattern for Avaya SIP endpoints to a location corresponding to the **Main** site. Add an entry for the **Main** site if one does not exist already, enter the following values for the specified fields, and retain default values for the remaining fields. Submit these changes.

- **Name:** A descriptive name to denote the Main site
- **Timezone Offset:** An appropriate time zone offset
- **Rule:** An appropriate daylight savings rule i.e. **0**
- **Proxy Sel. Rte. Pat.:** The route pattern number from i.e. **120**

```
change locations
                                LOCATIONS
                                ARS Prefix 1 Required For 10-Digit NANP Calls? y

Loc  Name           Timezone Rule  NPA           Proxy Sel
No           Offset
1:  Main           + 00:00    0             120
```

3.1.13. Station

Using the command **add station n**, where n is an available station number as shown with the appropriate **Station Type** and set the **Coverage Path** to the one used for voice messaging configured in **Section 3.1.11**. The Class of Restrictions (**COR**) and Class of Service (**COS**) assigned to the station should be configured with the appropriate call restrictions. The **Name** field is optional and may provide a descriptive name for the station. Use defaults for the other fields on **Page 1**.

```
add station 20002
                                Page 1 of 6
                                STATION
Extension: 24074                Lock Messages? n           BCC: 0
  Type: 9620                    Security Code: 12345678    TN: 1
  Port: S00023                  Coverage Path 1: 50       COR: 1
  Name: Luke Skywalker          Coverage Path 2:          COS: 1
                                Hunt-to Station:

STATION OPTIONS
                                Time of Day Lock Table:
  Loss Group: 19                Personalized Ringing Pattern: 1
                                Message Lamp Ext: 24074
  Speakerphone: 2-way           Mute Button Enabled? y
  Display Language: english
  Survivable GK Node Name:
  Survivable COR: internal       Media Complex Ext:
  Survivable Trunk Dest? y      IP SoftPhone? n
                                Customizable Labels? y
```

On **Page 2** of the station form, set the **MWI Served User Type** field to **sip-adjunct**. Also set the value **Per Station CPN – Send Calling Number?** to **y**.

add station 20002		Page 2 of 6
FEATURE OPTIONS		STATION
LWC Reception: spe		Auto Select Any Idle Appearance? n
LWC Activation? y		Coverage Msg Retrieval? y
LWC Log External Calls? n		Auto Answer: none
CDR Privacy? n		Data Restriction? n
Redirect Notification? y		Idle Appearance Preference? n
Per Button Ring Control? n		Bridged Idle Line Preference? n
Bridged Call Alerting? n		Restrict Last Appearance? n
Active Station Ringing: single		EMU Login Allowed? n
H.320 Conversion? n		Per Station CPN - Send Calling Number? y
Service Link Mode: as-needed		
Multimedia Mode: enhanced		
MWI Served User Type: sip-adjunct		Display Client Redirection? n
		Select Last Used Appearance? n
		Coverage After Forwarding? n
		Direct IP-IP Audio Connections? y
Emergency Location Ext: 24074		Always Use? n IP Audio Hairpinning? n

3.1.14. Save Translations

Configuration of Communication Manager is complete. Use the **save translations** command to save these changes.

3.2. Connection to Avaya one-X[®] Speech

This section describes the steps to configure an E1 trunk from the Access Element Communication Manager to one-X Speech.

3.2.1. Add DS1 Circuit Pack

Add the DS1 circuit pack. Enter the **add ds1 01b05** command where 01b05 represents the cabinet/carrier/slot/ of the DS1 circuit pack in the Avaya G650 Media Gateway. In this sample configuration, Communication Manager was configured with an **Interface** of **peer-master** and the one-X Speech platform was configured with an **Interface** of **peer-slave** (not shown). Set the **Side** option to **a** to match the **peer-master** setting. The **hdb3** setting for **Line Coding** is required by the E1-PRI card in the one-X Speech server as described in **Section 7.3.2**. The **pbx** option for **Connect** is used since the one-X Speech server is a peer switch. **Signaling Mode** of **isdn-pri** and **Peer Protocol** of **Q-SIG** are selected to enable the T1-PRI QSIG features on the trunk. A descriptive name of **Speech** was entered as the **Name**. Default values are used in the remaining fields.

```
add ds1 01b05                                     Page 1 of 1
                                                DS1 CIRCUIT PACK
Location: 01B05                                   Name: Speech
Bit Rate: 2.048                                  Line Coding: hdb3
Signaling Mode: isdn-pri
Connect: pbx                                     Interface: peer-master
TN-C7 Long Timers? n                             Peer Protocol: Q-SIG
Interworking Message: PROGRESS                   Side: a
Interface Companding: alaw                       CRC? y
Idle Code: 11111111                             Channel Numbering: timeslot
                                                DCP/Analog Bearer Capability: 3.1kHz
                                                T303 Timer(sec): 4
                                                Disable Restarts? n
Slip Detection? y                               Near-end CSU Type: other
```

3.2.2. Add Signaling Group

Enter the **add signaling group n** command where **n** is an available signaling group number. In this sample configuration, signaling group **105** was used. Set the **Group Type** to **isdn-pri**. Set the **Primary D-Channel** to the DS1 circuit pack created in **Section 3.2.1**. Set **TSC Supplementary Service Protocol** to **b** to enable QSIG supplementary services on this signaling group. Once the trunk group is created in the next section, return to this screen and set **Trunk Group for Channel Selection** to **105**. Default values are used in the remaining fields.

```
add signaling-group 105                                     Page 1 of 1
                                                           SIGNALING GROUP
Group Number: 105          Group Type: isdn-pri
Associated Signaling? y    Max number of NCA TSC: 0
Primary D-Channel: 01B0516 Max number of CA TSC: 0
Trunk Group for NCA TSC: 105
Trunk Group for Channel Selection: 105
TSC Supplementary Service Protocol: b    Network Call Transfer? n
```

3.2.3. Add Trunk Group

To create a trunk group enter the **add trunk n** command where **n** is an available trunk group number. In this sample configuration, trunk group **105** was used. On **Page 1**, set **Group Type** to **isdn** to allow QSIG features. Set the **TAC** to an available trunk access code. In this sample configuration, a **TAC** of **105** was used. Set the **Service Type** to **tie** as this is a general purpose trunk. A descriptive name is used as the **Group Name**. Default values are used in the remaining fields on this screen.

```
change trunk-group 105                                     Page 1 of 21
                                                           TRUNK GROUP
Group Number: 105          Group Type: isdn          CDR Reports: y
Group Name: One X Speech Server COR: 1          TN: 1          TAC: 105
Direction: two-way        Outgoing Display? y    Carrier Medium: PRI/BRI
Dial Access? y            Busy Threshold: 255 Night Service:
Queue Length: 0
Service Type: tie          Auth Code? n          TestCall ITC: rest
Far End Test Line No:
TestCall BCC: 4
```

On **Page 2**, set **Supplementary Services Protocol** to **b** which enables QSIG features. Default values are used in the remaining fields on this screen.

```
change trunk-group 105                                     Page 2 of 21
  Group Type: isdn

TRUNK PARAMETERS
  Codeset to Send Display: 6      Codeset to Send National IEs: 6
  Max Message Size to Send: 260  Charge Advice: none
  Supplementary Service Protocol: b  Digit Handling (in/out): enbloc/enbloc

  Trunk Hunt: cyclical

                                     Digital Loss Group: 13
Incoming Calling Number - Delete:  Insert:      Format:
  Bit Rate: 1200                  Synchronization: async  Duplex: full
Disconnect Supervision - In? y  Out? n
Answer Supervision Timeout: 0
  Administer Timers? n           CONNECT Reliable When Call Leaves ISDN? n
```

On **Page 3**, enable **Send Name**, **Send Calling Number**, and **Send Connected Number** options so that name and number information will be displayed. Default values are used in the remaining fields on this screen.

```
change trunk-group 105                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n           Measured: none           Wideband Support? n
                               Internal Alert? n         Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member:
                               Send Name: y             Send Calling Number: y
  Used for DCS? n           Hop Dgt? n              Send EMU Visitor CPN? n
  Suppress # Outpulsing? n  Format: public
Outgoing Channel ID Encoding: preferred  UUI IE Treatment: service-provider

                               Replace Restricted Numbers? n
                               Replace Unavailable Numbers? n
                               Send Connected Number: y
                               Hold/Unhold Notifications? y
                               Modify Tandem Calling Number? n

  Send UUI IE? y
  Send UCID? n
  Send Codeset 6/7 LAI IE? y           Dsl Echo Cancellation? n

  Apply Local Ringback? n
  Show ANSWERED BY on Display? y
                               Network (Japan) Needs Connect Before Disconnect? n
```

On **Page 5**, assign bearer channels to the trunk group. For this sample configuration, 30 channels are used to carry call traffic between Communication Manager and one-X Speech. For each channel (or Port), enter the **Sig Grp** associated with this trunk. For this sample configuration, signaling group **105**, created back in **Section 3.2.2**, will be used.

```
change trunk-group 105
```

Page 5 of 21

TRUNK GROUP

Administered Members (min/max): 1/30
Total Administered Members: 30

GROUP MEMBER ASSIGNMENTS

	Port	Code	Sfx	Name	Night	Sig Grp
1:	01B0501	TN464	F			105
2:	01B0502	TN464	F			105
3:	01B0503	TN464	F			105
4:	01B0504	TN464	F			105
5:	01B0505	TN464	F			105
6:	01B0506	TN464	F			105
7:	01B0507	TN464	F			105
8:	01B0508	TN464	F			105
9:	01B0509	TN464	F			105
10:	01B0510	TN464	F			105
11:	01B0511	TN464	F			105
12:	01B0512	TN464	F			105
13:	01B0513	TN464	F			105
14:	01B0514	TN464	F			105
15:	01B0515	TN464	F			105

3.2.4. Modify Dialplan Analysis

Enter the **display dialplan analysis** command. Verify dialed strings are configured for a 5-digit dial plan. Local Communication Manager extensions begin with **2**. Calls to one-X Speech pilot number **80900** are routed using automatic alternate routing (AAR).

```
change dialplan analysis
```

Page 1 of 12

DIAL PLAN ANALYSIS TABLE

Location: all Percent Full: 2

	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1		3	dac	*	2	fac			
2		5	ext	#	3	fac			
3		5	ext						
333		5	aar						
34		5	aar						
350		5	aar						
4		5	aar						
420		5	aar						
5		6	ext						
60		4	aar						
666		5	aar						
7		5	aar						
8		5	aar						
81		5	aar						
9		1	fac						

3.2.5. Modify AAR Analysis

Enter the **change aar analysis 8** command. In this sample configuration, 5 digit dial strings matching the number **80900** will be routed using a **Call Type** of **aar** and **Route Pattern** of **105**. Route pattern **105** will be created in the next section and will contain the E1/QSIG trunk group used for connectivity to one-X Speech.

```

change aar analysis 8                                     Page 1 of 2
                AAR DIGIT ANALYSIS TABLE
                Location: all                            Percent Full: 2

```

Dialed String	Total		Route Pattern	Call Type	Node Num	ANI Reqd
	Min	Max				
80900	5	5	105	aar		n
80950	5	5	120	aar		n
81950	5	5	199	aar		n
824076	6	6	120	aar		n
9	7	7	999	aar		n

3.2.6. Modify Route Pattern

Enter the **change route-pattern 105** command. In the route pattern screen, specify the E1/QSIG trunk group that connects to one-X Speech, by setting **Grp No** to **105**. A descriptive name of **Speech** was used as the **Pattern Name**. Default values are used in the remaining fields on this screen.

```

change route-pattern 105                               Page 1 of 3
                Pattern Number: 105 Pattern Name:Speech
                SCCAN? n      Secure SIP? n

```

Grp No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/	IXC
			Mrk	Lmt	List	Del	Digits	QSIG	
							Dgts	Intw	
1:	105	0						n	user
2:								n	user
3:								n	user
4:								n	user
5:								n	user
6:								n	user

BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR
0	1	2	M	4	W	Request		Dgts	Format	
							Subaddress			
1:	y	y	y	y	y	n	n	rest		none
2:	y	y	y	y	y	n	n	rest		none
3:	y	y	y	y	y	n	n	rest		none

3.2.7. Modify Public Unknown Numbering

Enter the **change public-unknown-numbering** command to allow Communication Manager to send the calling party number along with the call information across a particular trunk group. For this sample configuration, set the **Total CPN Len** to **5**. This setting allows Communication Manager to send a 5 digit calling number across trunk **105** for any 5 digit extension starting with the number **8**.

```

change public-unknown-numbering 0
NUMBERING - PUBLIC/UNKNOWN FORMAT
Total
Ext  Ext      Trk      CPN      Total
Len  Code      Grp(s)   Prefix   CPN
5    2          100      003531207 5
5    2          100      003531207 13
5    3          100      003531207 5
5    4          100      003531207 5
5    4          120      003531207 5
5    7          100      003531207 5
5    8          105      003531207 5
5    300        120      003531207 5
5    350        120      003531207 5
5    420        166      003531207 5
Total Administered: 11
Maximum Entries: 9999

```

3.3. Other Avaya Aura™ Communication Managers

The Feature Server shown in **Figure 2** is used in conjunction with Session Manager to provide SIP end point registration. The configuration for SIP registration is beyond the scope of these Application Notes. The Remote Site Communication Manager is used in conjunction with the SIP Enablement Services template to provide registration for both SIP and H.323 end points. The configuration of these Communication Manager is similar to that described in **Section 3.1** and is based on Reference [11].

In order for Find Me functionality to work correctly in these Application Notes, the **locations** form set the **Proxy Sel Rte Pat** to point to the Session Manager route pattern as described in **Section 3.1.12**. In this case the route pattern is **120**.

```

change locations
LOCATIONS
ARS Prefix 1 Required For 10-Digit NANP Calls? y
Loc  Name      Timezone Rule  NPA      Proxy Sel
No   Offset
1:   Main       + 00:00  0        120

```

4. Configure Avaya Modular Messaging

This section deals with the configuration of the single server Avaya Modular Messaging. It is assumed that Modular Messaging server has the correct software installed and are appropriately licensed as described in Reference [7].

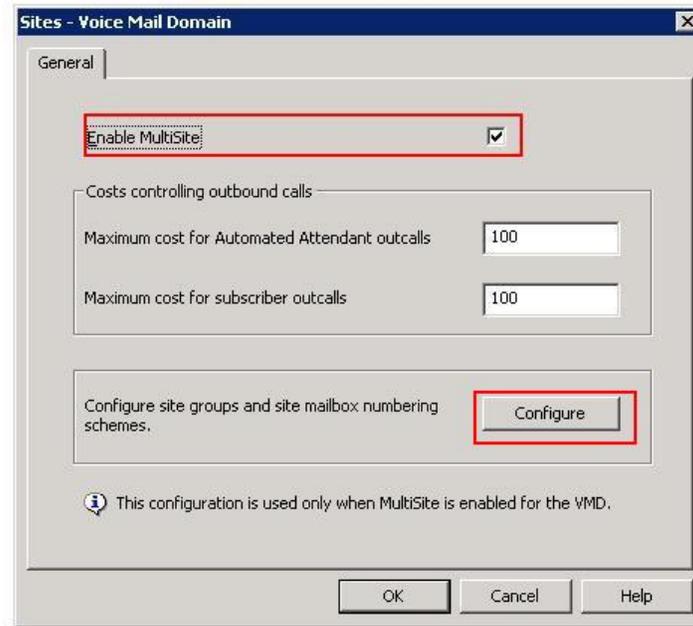
Note: A private Windows domain is being used in these Application Notes for communication between Avaya Message Storage Server (MSS) and Avaya Message Application Server (MAS). This is not a requirement.

4.1. MultiSite Configuration

In order to enable MultiSite functionality on Modular Messaging, the MAS must be configured as exemplified in this section. Reference [8] contains more information on MultiSite configuration. The configuration can be verified by following the instructions in this section. Log in to the Avaya MAS server using the appropriate credentials. Select **Start** → **Programs** → **Avaya Modular Messaging** → **Voice Mail System Configuration** to start the Voice Mail System Configuration tool.



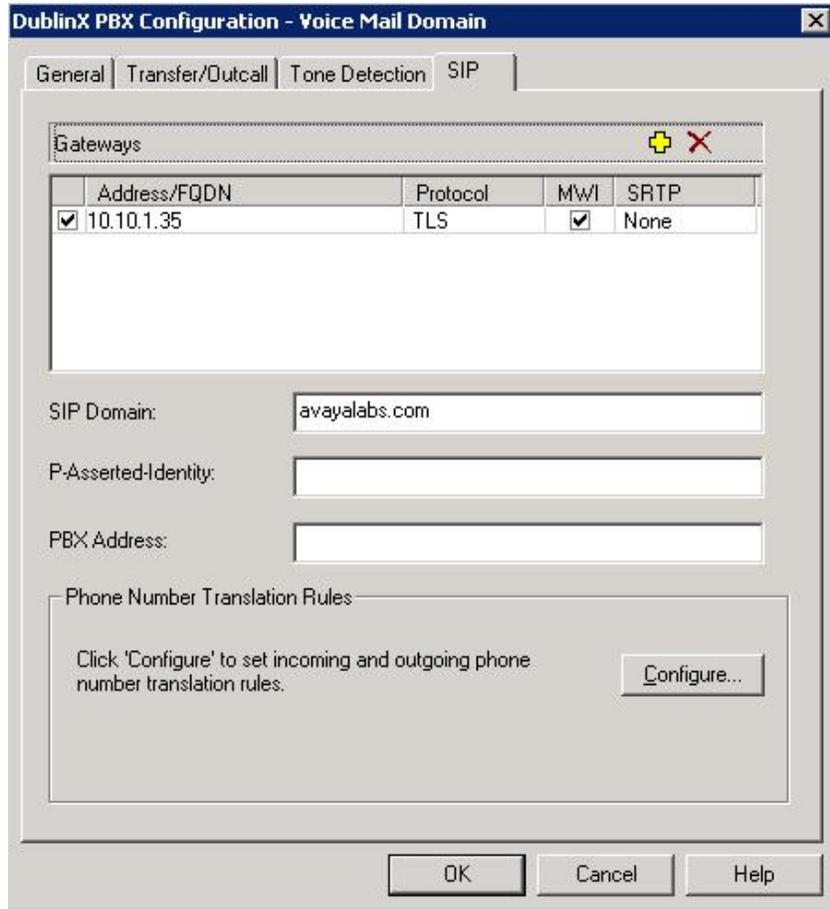
From that window go to **Voice Mail Domains** → **SPMMVMD** → **Sites** and confirm that the **Enable MultiSite** checkbox is selected in the screen as shown. Click **Configure** to open the **Site Configuration** window.



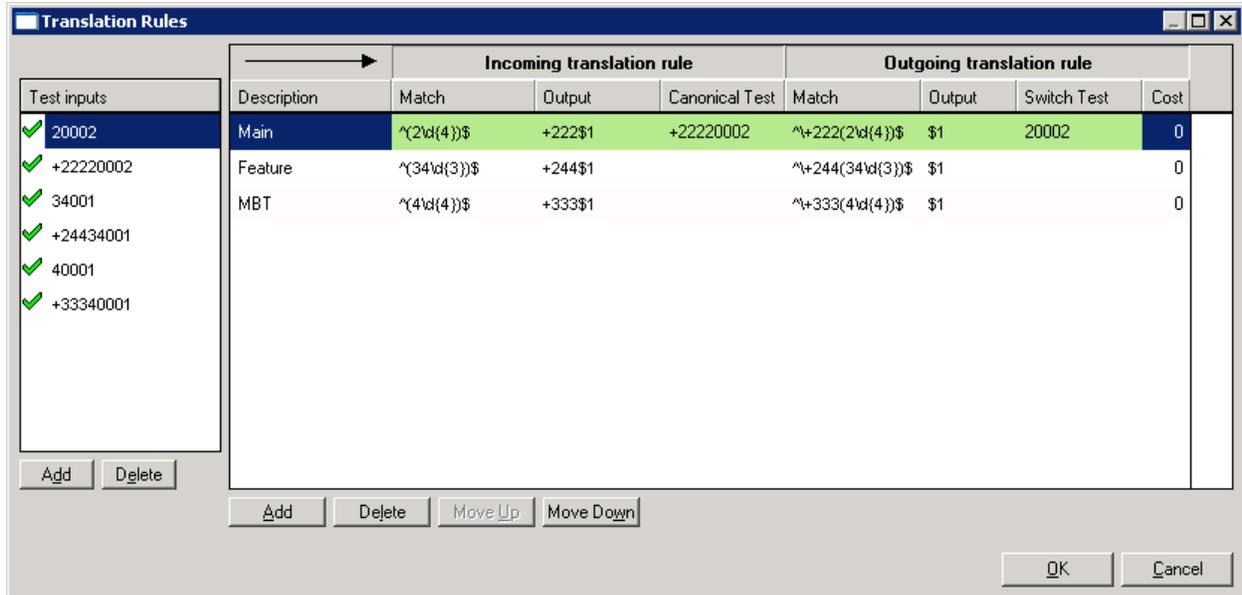
In this example the **Enterprise Access Element** site has an **ID** of **222**, a **Full Mailbox** length of **8** and a **Short Mailbox** length of **5**. The **PBX Name** is the name of the PBX as shown in **Voice Mail Domains** → **PBXs** described later in this section. Two other sites have been added to represent the Feature Server Communication Manager on the Enterprise Site and the Communication Manager on the Remote Site.

Site/group	ID	Mailbox number			Name	PBX
		Full	Short	Preview		
Enterprise Access Element	222	8	5	222 xxxxxx	stackhq	
Enterprise Feature	244	8	5	244 xxxxxx	stackhq	
Remote MBT	333	8	5	333 xxxxxx	stackhq	

To check the SIP integration of Avaya MAS, from the **Voice Mail System Configuration** window, go to **Voice Mail Domains → SPMMVMD → PBXs** and click on the **SIP** tab. Ensure that the IP address or fully qualified domain name (FQDN) of the Asset Card in the Session Manager is entered in the **Address/FQDN** field. Configure **Protocol** and **SRTP** settings to match the Session Manager and Communications Manager settings discussed in **Section 3**. Note in this example, **SRTP** was not enabled and the chosen **Protocol** was **TLS**. Click the **Configure** button located near the bottom of the screen to configure the incoming and outgoing phone number translation rules.

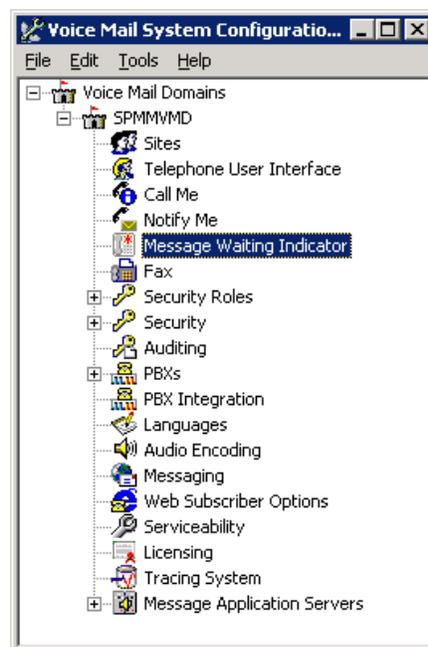


The **Translation Rules** screen opens as shown below. The example translation rules shown below will map an incoming number of **20002** to its canonical form of **+22220002**. For more details in creating incoming and outgoing translation rules please refer to Reference [8]. There are example translation rules for each of the sites created earlier in this section.

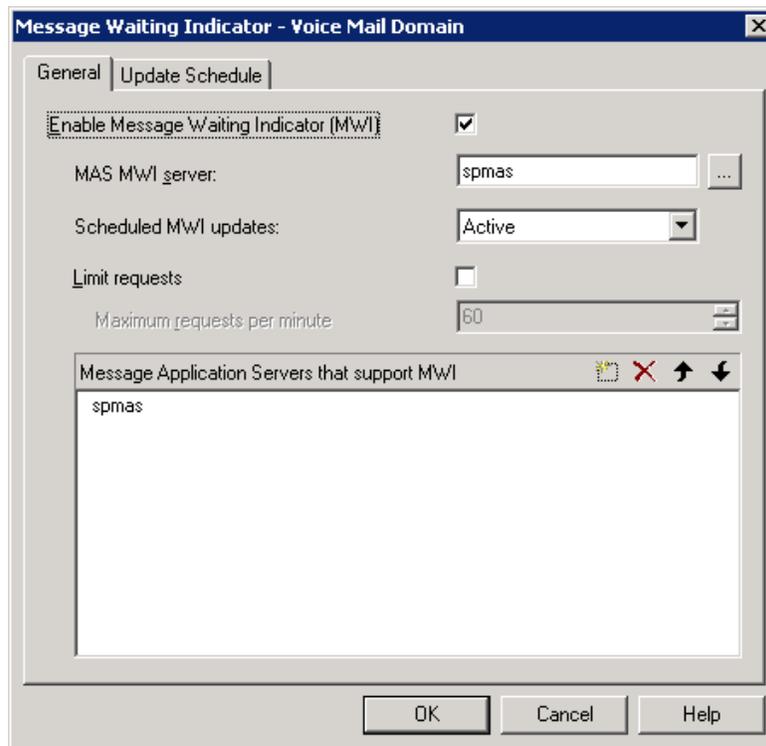


4.2. Configuration of Services

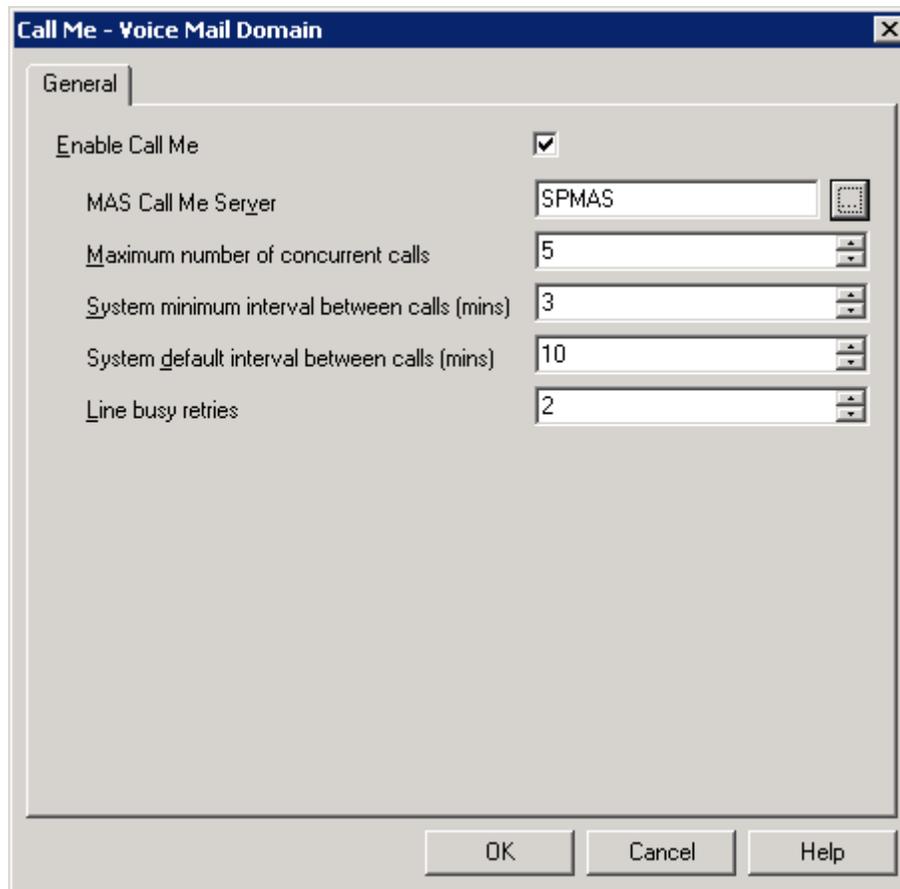
From the **Voice Mail System Configuration** Application Window, go to **Voice Mail Domains** → **SPMMVMD** and double click **Message Waiting Indicator**.



In the **Message Waiting Indicator** screen that opens, check **Enable Message Waiting Indicator (MWI)**. Then set **Message Application Servers that support MWI** to the name of the Primary Site MAS as shown. Click **OK**.



From the **Voice Mail System Configuration** Application Window, go to **Voice Mail Domains** → **SPMMVMD** and double click **Call Me**. In the **Call Me** popup that appears, check **Enable Call Me** and set **MAS Call Me Server** as shown.

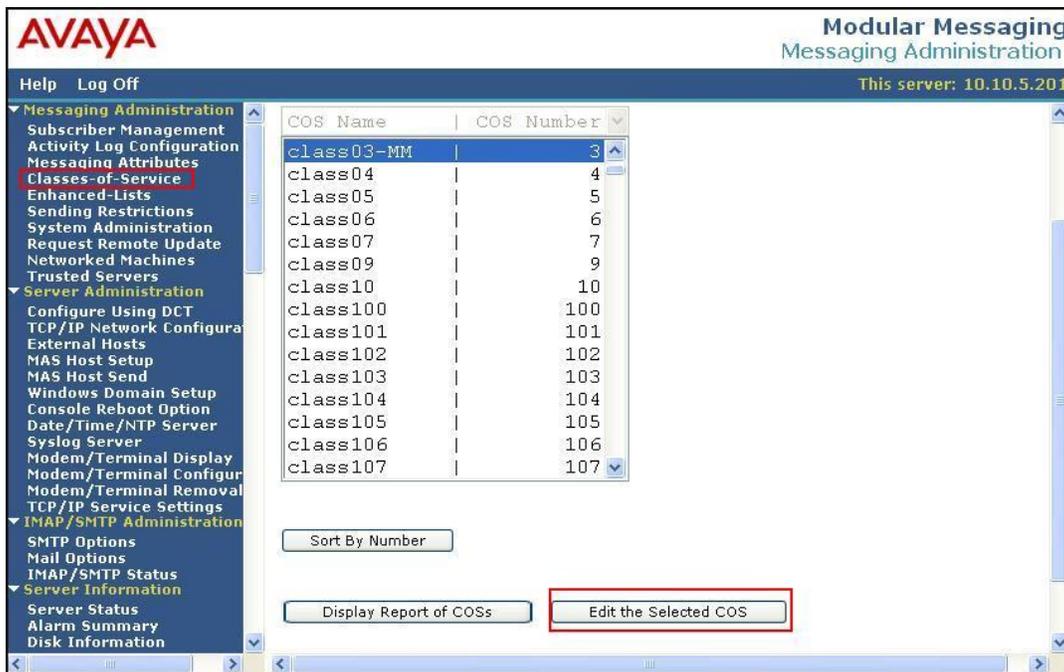


4.3. Class of Services

This section describes how to configure an example Class of Service that can be used in creating Modular Messaging subscribers. Configuration is performed through the Modular Messaging Message Administration application. To launch the application, enter Avaya MSS hostname or IP address in the URL field of a web browser. Log in with the appropriate credentials. The following webpage is displayed.



Select the **Classes-of-Service** menu option from the Messaging Administration Menu on the left of the screen. The **Manage Classes-of-Service** screen opens up. Select a class of service from the displayed list and click **Edit the Selected COS** as shown.



The **Edit a Class-of-Service** screen opens. Scroll down the screen to the **Subscriber Feature and Services** section and set the options as appropriate for the configuration. In this case **Call Me Allowed**, **Find Me Allowed** and **Message Waiting Indication Allowed** are all set to **yes**.

The screenshot shows the Avaya Modular Messaging Messaging Administration web interface. The left sidebar contains a navigation menu with categories like Messaging Administration, Server Administration, and IMAP/SMTP Administration. The main content area displays a grid of configuration options for a Class-of-Service, each with a dropdown menu. The 'Time Zone' is set to 'Use System Timezone'. The 'Message Waiting Indication Allowed' is set to 'yes'. The 'Find Me Allowed' is set to 'yes'. The 'Call Me Allowed' is set to 'yes'. Other options include 'Call Handling' (yes), 'Outbound Fax Calls' (no), 'Inbound Fax' (yes), 'Page via PBX' (no), 'Caller Application Announcement Recording' (no), 'Telephone User Interface' (MM Aria), and 'Personal Operator Configuration' (no). The 'Restrict Client Access' is set to 'yes' and 'Unsent Message Allowed' is set to 'no'. The top right corner indicates 'This server: 10.10.5.201'.

Option	Value
Time Zone	Use System Timezone
Message Waiting Indication Allowed	yes
Call Me Allowed	yes
Find Me Allowed	yes
Notify Me Allowed	yes
Call Handling	yes
Call Screening	yes
Outbound Fax Calls	no
Extended Absence Greeting Allowed	yes
Inbound Fax	yes
Aria TUI Date & Time Playback	Never
Page via PBX	no
Record Mailbox Greetings	yes
Caller Application Announcement Recording	no
Caller Application	(none)
Telephone User Interface	MM Aria
Restrict Client Access	yes
Personal Operator Configuration	no
Unsent Message Allowed	no

Save any changes made by clicking **Save** which is located at the bottom of the screen (not shown).

4.4. Subscriber Creation

Click on the **Subscriber Management** option in the Messaging Administration Menu. Enter the **Local Subscriber Mailbox Number** and click **Add or Edit**. In this case the Mailbox Number is 22220001.

Manage Subscribers

• Local Subscriber Mailbox Number

	Machine Name	Subscriber Licenses Used	Total Subscribers	Filtered Subscribers
• Local Subscribers	spmss	7	11	<input type="button" value="Filter"/> 11 <input type="button" value="Manage"/>
• Remote Subscribers	oneXPortal3	0	0	<input type="button" value="Filter"/> 0 <input type="button" value="Manage"/>
	internet	0	0	<input type="button" value="Filter"/> 0 <input type="button" value="Manage"/>

In this example, the **Canonical** form of the **PBX Extension** is used. This refers to the combination of the **Site ID**, in this case 222 as configured in **Section 4.1**, and the **Switch Native** extension, in this case 20001. Enter in the appropriate details for the subscriber and ensure that the **Class-of-Service** is set to the one described in **Section 4.3**. The default **Community ID** is selected.

Edit Local Subscriber

BASIC INFORMATION
* (Required Fields)

*Last Name	User	First Name	Speech
*Password		*Mailbox Number	22220001
*Numeric Address	22220001	PBX Extension	+22220001 <input checked="" type="radio"/> Canonical <input type="radio"/> Switch Native
*Class Of Service	3 - Class03-MM	*Community ID	1

SUBSCRIBER DIRECTORY

Email Handle	22220001@spmss.silstack.com	Telephone Number	22220001
Common Name	Speech User	ASCII Version of Name	Speech User

Save any changes by clicking the **Save** button (not shown) and repeat the process for all required subscribers.

4.5. Enable IMAP4 Connection

In order to allow one-X Speech to interoperate with Modular Messaging successfully, the IMAP4 ports must be enabled on Modular Messaging. Configuration is performed through the Modular Messaging Message Administration application. To launch the application refer to **Section 4.3**. Click **System Administration** under **Messaging Administration**. Scroll down to **SYSTEM TCP/IP PORTS** and ensure that the **IMAP4 Port** is **Enabled** as shown and set to **143**. Click **Save** to keep any changes.

The screenshot shows the Avaya Modular Messaging Administration web interface. The main content area displays the 'SYSTEM TCP/IP PORTS' configuration table. The 'IMAP4 Port' is set to 143 and is 'Enabled'. Other ports like LDAP, SMTP, and POP3 are also visible with their respective settings.

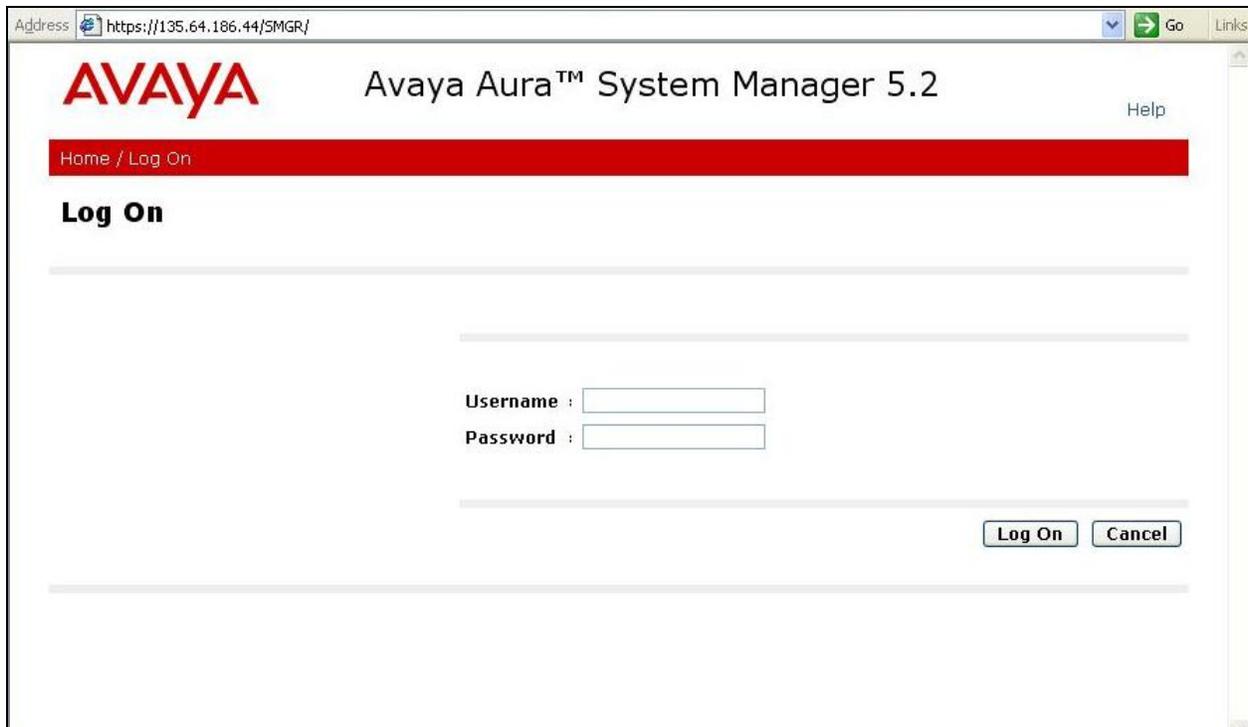
SYSTEM TCP/IP PORTS				
LDAP Port	389	Authenticated or Anonymous	LDAP SSL Port	636 Enabled
LDAP Internal Server Port	55389	Enabled	LDAP Directory Update Port	56389 Enabled
LDAP Front End Alternate Port		Disabled	IMAP4 TUI Port	55143 Enabled
IMAP4 Port	143	Enabled	IMAP4 SSL Port	993 Enabled
POP3 Port	110	Disabled	POP3 SSL Port	995 Disabled
SMTP Port	25	Enabled	SMTP Alternate Port	Disabled
SMTP SSL Port	465	Disabled	Allow TLS for Outgoing SMTP	25 Enabled
MCAPI Port	55000	Enabled		

5. Configure Avaya Aura™ Session Manager

The following steps describe the administrative procedures for configuring the Session Manager.

5.1. Access the Web Interface

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **https://<ip-address>/SMGR**, where **<ip-address>** is the IP address of the System Manager. Click **Log on** after entering the appropriate credentials.



The screenshot shows a web browser window with the address bar containing `https://135.64.186.44/SMGR/`. The page title is "Avaya Aura™ System Manager 5.2". The Avaya logo is displayed in the top left corner. A red navigation bar contains the text "Home / Log On". Below this, the heading "Log On" is displayed. The login form consists of two input fields: "Username :" and "Password :". At the bottom right of the form, there are two buttons: "Log On" and "Cancel". A "Help" link is visible in the top right corner of the page content.

5.2. Network Routing Policy

Begin configuration by selecting **Network Routing Policy** from the left panel menu. A short procedure for configuring Network Routing Policy is shown on the right panel.

The screenshot shows the Avaya Aura System Manager 5.2 web interface. The browser address bar displays the URL: <https://135.64.186.44/NRP/faces/pages/nrpWelcome.xhtml?clientTZ=0&clientTZName=Europe/London&cid=75>. The page header includes the Avaya logo, the title "Avaya Aura™ System Manager 5.2", and a welcome message for user "admin" last logged on at Jan. 26, 2010 4:20 PM. There are links for "Help" and "Log off".

A red navigation bar shows the current path: Home / Network Routing Policy. On the left, a sidebar menu lists various management categories: Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy (selected), Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies, SIP Domains, SIP Entities, Time Ranges, Personal Settings, Security, and Applications.

The main content area is titled "Introduction to Network Routing Policy (NRP)". It explains that Network Routing Policy consists of several NRP applications like "Domains", "Locations", "SIP Entities", etc. It provides a recommended order for using these applications to configure the network configuration:

- Step 1: Create "Domains" of type SIP (other NRP applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

5.3. SIP Domains

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting **SIP Domains** on the left and clicking the **New** button (not shown) on the right. Fill in the following fields:

- **Name:** The authoritative domain name (e.g., **silstack.com**)
- **Notes:** Descriptive text (e.g., **Test Lab**)

Click **Commit** to save changes.

The screenshot shows the Avaya Aura System Manager 5.2 interface. The browser address bar shows <https://135.64.186.44/NRP/faces/pages/sipDomains.xhtml>. The page header includes the Avaya logo, the title "Avaya Aura™ System Manager 5.2", and a welcome message for user "admin" last logged on at Jan. 26, 2010 4:20 PM. There are "Help" and "Log off" links.

A red breadcrumb trail reads: Home / Network Routing Policy / SIP Domains.

The left sidebar contains a navigation menu with the following items: Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy (expanded), Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies, SIP Domains (highlighted), SIP Entities, Time Ranges, and Personal Settings.

The main content area is titled "Domain Management" and includes "Commit" and "Cancel" buttons. Below this is a table with one item:

Name	Type	Default	Notes
* silstack.com	sip	<input type="checkbox"/>	Test Lab

Below the table, there is a "* Input Required" message and another set of "Commit" and "Cancel" buttons.

5.4. Adaptations

No adaptations were needed for this test configuration.

5.5. Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management. Location is added to the configuration for both Communication Manager and Modular Messaging. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. Fill in the following details for the **Avaya** location:

Under **General**:

- **Name:** A descriptive name (e.g. **Avaya**)
- **Notes:** Descriptive text (optional)

Under **Location Pattern**:

- **IP Address Pattern:** A pattern used to logically identify the location
- **Notes:** Descriptive text (optional)

Click **Commit** to save.

Home / Network Routing Policy / Locations / Location Details

Location Details Commit Cancel

General

* **Name:**

Notes:

Managed Bandwidth:

* **Average Bandwidth per Call:**

* **Time to Live (secs):**

Location Pattern

Add Remove

2 Items | Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.1.x	
<input type="checkbox"/>	* 135.64.186.*	

Select : All, None (0 of 2 Selected)

* **Input Required** Commit Cancel

5.6. SIP Entities

A SIP Entity must be added for the Session Manager for each SIP-based telephony system supported by a SIP Trunk. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown) on the right. SIP Entities were created for Communication Manager, Modular Messaging, and Session Manager. Enter the following for each SIP Entity.

Under **General**:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface for each SIP Entity.
- **Type** Select **CM** for Communication Manager Entities, **Modular Messaging** for Modular Messaging Entities, and **Session Manager** for Session Manager Entities.
- **Location:** Select one of the locations defined previously.

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition. The following screen shows the SIP Entity for the Access Element Communication Manager. Repeat for the Communication Manager at the branch site.

The screenshot shows a web-based configuration interface for SIP Entities. The breadcrumb trail at the top reads: Home / Network Routing Policy / SIP Entities / SIP Entity Details. On the right side of the breadcrumb, there are links for 'Help' and 'Log off'. A left-hand navigation menu is visible, with 'SIP Entities' highlighted under the 'Network Routing Policy' section. The main content area is titled 'SIP Entity Details' and contains a 'General' section with the following fields: 'Name' (text input with value 'AvayaCM'), 'FQDN or IP Address' (text input with value '135.64.186.6'), 'Type' (dropdown menu with value 'CM'), 'Notes' (text area), 'Adaptation' (dropdown menu), 'Location' (dropdown menu with value 'Avaya'), and 'Time Zone' (dropdown menu with value 'Europe/Dublin'). Below these is an 'Override Port & Transport with DNS SRV' checkbox (unchecked). The 'SIP Timer B/F (in seconds)' field has a value of '4'. There is a 'Credential name' text input field. The 'Call Detail Recording' dropdown menu is set to 'none'. At the bottom, the 'SIP Link Monitoring' section has a dropdown menu set to 'Use Session Manager Configuration'. 'Commit' and 'Cancel' buttons are located at the top right of the configuration area.

The following screen shows the SIP Entity for Modular Messaging.

The screenshot displays a web-based configuration interface for SIP Entity Details. The breadcrumb trail at the top reads: Home / Network Routing Policy / SIP Entities / SIP Entity Details. A navigation sidebar on the left lists various management categories, with 'Network Routing Policy' expanded to show 'SIP Entities' as the active section. The main content area is titled 'SIP Entity Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' section, the following fields are visible: 'Name' (VoiceMail), 'FQDN or IP Address' (135.64.186.103), 'Type' (Modular Messaging), and 'Notes' (VoiceMail). The 'Adaptation' field is empty, 'Location' is set to Avaya, and 'Time Zone' is set to Etc/GMT+1. An 'Override Port & Transport with DNS SRV' checkbox is unchecked. The 'SIP Timer B/F (in seconds)' is set to 4, and the 'Credential name' field is empty. The 'Call Detail Recording' dropdown is set to 'none'. Under the 'SIP Link Monitoring' section, the 'SIP Link Monitoring' dropdown is set to 'Use Session Manager Configuration'.

Home / Network Routing Policy / SIP Entities / SIP Entity Details

SIP Entity Details

Commit Cancel

General

* Name: VoiceMail

* FQDN or IP Address: 135.64.186.103

Type: Modular Messaging

Notes: VoiceMail

Adaptation:

Location: Avaya

Time Zone: Etc/GMT+1

Override Port & Transport with DNS SRV:

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

A Session Manager SIP Entity must be created as shown.

The screenshot displays the Avaya Aura™ System Manager 5.2 web interface. At the top left is the Avaya logo. The main header reads "Avaya Aura™ System Manager 5.2". On the top right, a user status bar shows "Welcome, admin Last Logged on at Jan. 26, 2010 5:05 PM" and links for "Help | Log off". A red breadcrumb trail indicates the path: "Home / Network Routing Policy / SIP Entities / SIP Entity Details".

A left-hand navigation menu is visible, with "SIP Entities" highlighted in blue. The main content area is titled "SIP Entity Details" and includes "Commit" and "Cancel" buttons. Under the "General" section, the following fields are populated:

- Name:** SessionManager
- * FQDN or IP Address:** 135.64.186.46
- Type:** Session Manager (dropdown)
- Notes:** (empty text box)
- Location:** Avaya (dropdown)
- Outbound Proxy:** (empty dropdown)
- Time Zone:** Europe/Dublin (dropdown)
- Credential name:** (empty text box)

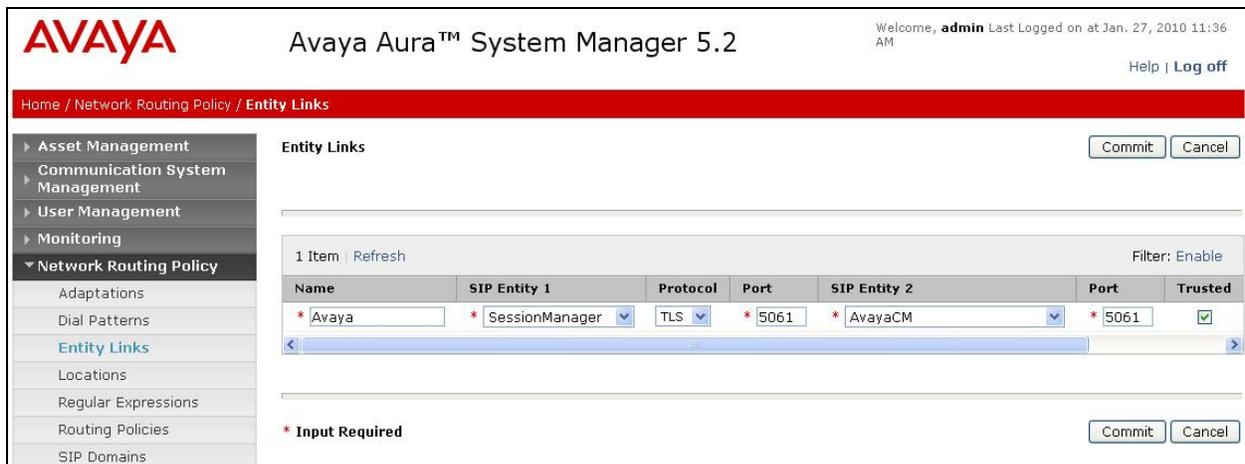
Under the "SIP Link Monitoring" section, the "SIP Link Monitoring" field is set to "Use Session Manager Configuration" (dropdown).

5.7. Entity Links

A SIP trunk between the Session Manager and a telephony system is described by an Entity link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown) on the right. Entity Links were created for all Communication Manager systems and Modular Messaging. Enter the following for each Entity link.

- **Name:** An informative name
- **SIP Entity 1:** Select **SessionManager** as created in **Section 5.6**
- **Port:** Port number to which the other system sends its SIP requests
- **SIP Entity 2:** The other SIP Entity for this link, created in **Section 5.6**
- **Port:** Port number to which the other system expects to receive SIP requests
- **Trusted:** Whether to trust the other system
- **Protocol:** Transport protocol to be used to send SIP requests

Click **Commit** to save each Entity Link definition. The following screen illustrates adding the Entity Links for the Access Element Communication Manager. Similar Entity Links need to be added for other Communication Manager systems (not shown).



The screenshot shows the Avaya Aura System Manager 5.2 interface. The top navigation bar includes the Avaya logo, the system name, and user information. The left sidebar shows a menu with 'Entity Links' selected. The main content area displays the 'Entity Links' configuration page with a table containing one entry.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
* Avaya	* SessionManager	TLS	* 5061	* AvayaCM	* 5061	<input checked="" type="checkbox"/>

* Input Required

The following screen illustrates adding the Entity Links for Modular Messaging.

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Jan. 27, 2010 11:36 AM

Help | Log off

Home / Network Routing Policy / Entity Links

Entity Links

Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
* SessionManager_V	* SessionManager	TLS	* 5061	* VoiceMail	* 5061	<input checked="" type="checkbox"/>

* Input Required

Commit Cancel

5.8. Time Range

Time Range defines time range for any time. To add time ranges, select **Time Ranges** on the left panel menu and click on the **New** button on the right. For this test the time range was set to always to allow routing always and was given the name **24/7**. Click **Commit** to save changes to time range.

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Jan. 27, 2010 11:36 AM

Help | Log off

Home / Network Routing Policy / Time Ranges

Time Ranges

Edit New Duplicate Delete More Actions Commit

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	24/7	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7						

Select : All, None (0 of 1 Selected)

5.9. Routing Policies

Create routing policies to direct how calls will be routed to a system. Several routing policies must be added; one for each Communication Manager and one for Modular Messaging. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown) on the right. Fill in the following fields for the new Routing Policies:

Under **General**:

- **Name:** Enter an informative name
- **SIP Entity as Destination:** Click **Select**, and then select the appropriate SIP entity to which this routing policy applies
- **Time of Day:** Click **Add**, and then select the time range
- **Dial Pattern:** Pattern for the routing call

Click **Commit** to save each. The following screen shows the Routing Policy of the Access Element Communication Manager where extensions start with **200xx**.

- Asset Management
- Communication System Management
- User Management
- Monitoring
- Network Routing Policy
 - Adaptations
 - Dial Patterns
 - Entity Links
 - Locations
 - Regular Expressions
 - Routing Policies
 - SIP Domains
 - SIP Entities
 - Time Ranges
 - Personal Settings
- Security
- Applications
- Settings
- Session Manager

Routing Policy Details

General

* Name:

Disabled:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
AvayaCM	135.64.186.6	CM	

Time of Day

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0		<input checked="" type="checkbox"/>	00:00	23:59							

Select : All, None (0 of 1 Selected)

Dial Patterns

5 Items Refresh Filter: Enable

<input type="checkbox"/>	Pattern ▲	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	0	8	15	<input type="checkbox"/>	-ALL-	-ALL-	Mobile out
<input type="checkbox"/>	200xx	5	5	<input type="checkbox"/>	-ALL-	-ALL-	Enterprise CM
<input type="checkbox"/>	300	5	5	<input type="checkbox"/>	-ALL-	-ALL-	
<input type="checkbox"/>	80900	5	5	<input type="checkbox"/>	-ALL-	-ALL-	
<input type="checkbox"/>	9	7	15	<input type="checkbox"/>	-ALL-	-ALL-	External Line

Select : All, None (0 of 5 Selected)

Regular Expressions

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------

* Input Required

The Remote Site Communication Manager uses extensions in the **400xx** range. A similar route pattern must be added for that Communication Manager (not shown). The following screen shows the Routing Policy of Modular Messaging where the pilot number is **20900**.

Home / Network Routing Policy / Routing Policies / Routing Policy Details

Routing Policy Details Commit Cancel

General

* Name:

Disabled:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
VoiceMail	135.64.186.103	Modular Messaging	VoiceMail

Time of Day

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7						

Select : All, None (0 of 1 Selected)

Dial Patterns

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Pattern ▲	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	20900	5	5	<input type="checkbox"/>	-ALL-	-ALL-	

Select : All, None (0 of 1 Selected)

Regular Expressions

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Pattern	Rank Order ▲	Deny	Notes
<input type="checkbox"/>	VoiceMail@silstack.com	0	<input type="checkbox"/>	

Select : All, None (0 of 1 Selected)

5.10. Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity as shown in the Routing Policies described in **Section 5.9**. In the sample configuration, 5-digit extensions beginning with **200** reside on the Access Element Communication Manager. The five digit extension **20900** resides on Modular Messaging. The Remote Site Communication Manager uses extensions in the **400xx** range. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following details:

Under **General**:

- **Pattern:** Dialed number or prefix
- **Min:** Minimum length of dialed number
- **Max:** Maximum length of dialed number
- **Notes:** Comment on purpose of dial pattern

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 this dial pattern. As an example the following screen shows the dial pattern definitions for the Access Element Communication Manager.

The screenshot shows the Avaya Aura System Manager 5.2 interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura™ System Manager 5.2', and user information: 'Welcome, admin Last Logged on at Jan. 27, 2010 1:33 PM'. There are links for 'Help' and 'Log off'.

The breadcrumb trail is: Home / Network Routing Policy / Dial Patterns / Dial Pattern Details.

The left sidebar shows a navigation menu with categories: Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy (expanded), Security, Applications, and Settings. Under Network Routing Policy, 'Dial Patterns' is selected.

The main content area is titled 'Dial Pattern Details' and has 'Commit' and 'Cancel' buttons. It is divided into two sections:

- General:**
 - * **Pattern:** 200xx
 - * **Min:** 5
 - * **Max:** 5
 - Emergency Call:**
 - SIP Domain:** -ALL-
 - Notes:** Enterprise CM
- Originating Locations and Routing Policies:**
 - Buttons: Add, Remove
 - 1 Item | Refresh | Filter: Enable
 - Table with columns: Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, Routing Policy Notes.

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	AvayaCM	0	<input type="checkbox"/>	AvayaCM	

A dial pattern is required for all Communication Manager systems in the configuration (Not Shown)

The following screenshot shows the dial pattern for Modular Messaging.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Jan. 27, 2010 1:33 PM [Help](#) | [Log off](#)

Home / Network Routing Policy / Dial Patterns / Dial Pattern Details

Dial Pattern Details

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	VoiceMail	0	<input type="checkbox"/>	VoiceMail	

Select : All, None (0 of 1 Selected)

5.11. Regular Expression

Create Regular Expressions so the Session Manager knows how to route the voice mail handle out to the Communication Manager hunt group as configured in **Section 3.1.9**. To add a regular expression, select **Regular Expression** on the left and click on the **New** button (not shown) on the right. Fill in the following details:

Under **General**:

- **Pattern:** Configure the pattern as to match the setting in **Section 3.1.9**
- **Routing Policy:** Add the VoiceMail routing policy configured in **Section 5.9**

Click **Commit** to save changes to the regular expression.

The screenshot displays the Avaya Aura System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the system name "Avaya Aura™ System Manager 5.2", and a user status message: "Welcome, admin Last Logged on at Jan. 27, 2010 1:33 PM". A "Help | Log off" link is also present. The breadcrumb trail reads: "Home / Network Routing Policy / Regular Expressions / Regular Expression Details".

The left sidebar contains a navigation menu with the following items: Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy (expanded), Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions (highlighted), Routing Policies, SIP Domains, SIP Entities, Time Ranges, Personal Settings, Security, Applications, Settings, and Session Manager.

The main content area is titled "Regular Expression Details" and includes "Commit" and "Cancel" buttons. It is divided into two sections:

- General:** Contains fields for:
 - * **Pattern:** A text input field containing "VoiceMail@silstack.com".
 - * **Rank Order:** A text input field containing "0".
 - Deny:** A checkbox that is currently unchecked.
 - Notes:** An empty text input field.
- Routing Policy:** Contains "Add" and "Remove" buttons. Below them is a table with one item:

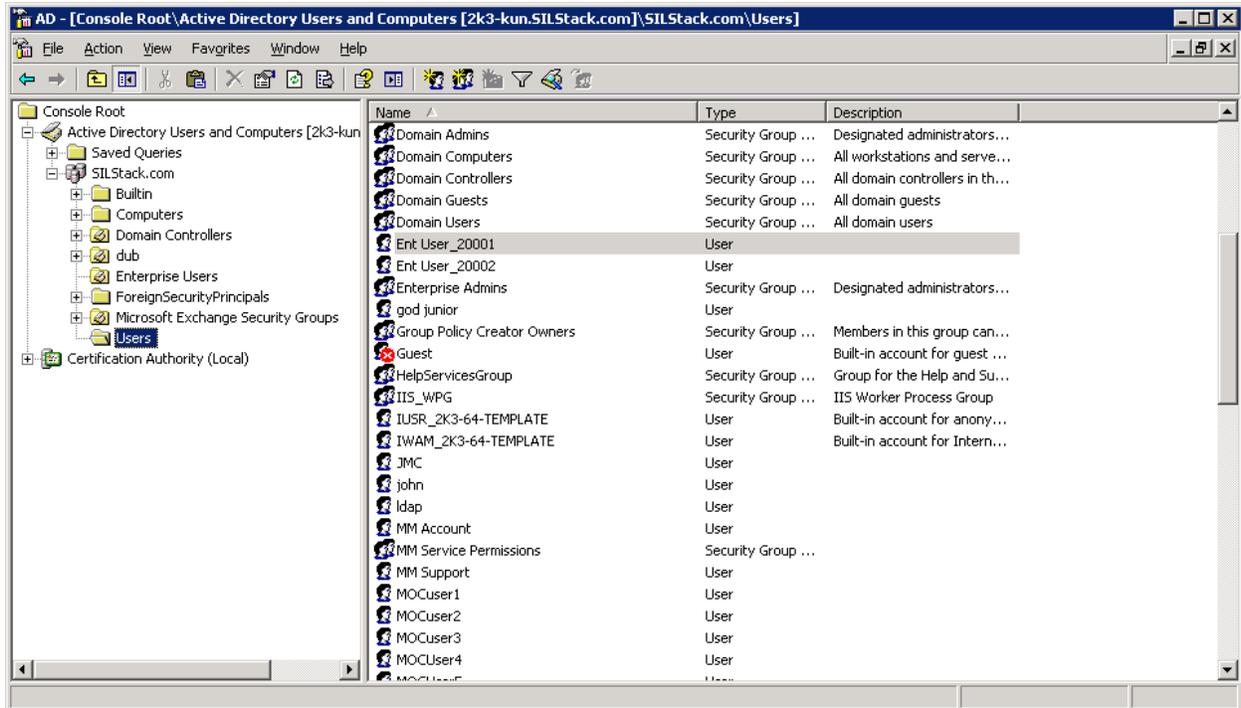
<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	VoiceMail	<input type="checkbox"/>	VoiceMail	

Below the table, it says "Select : All, None (0 of 1 Selected)".

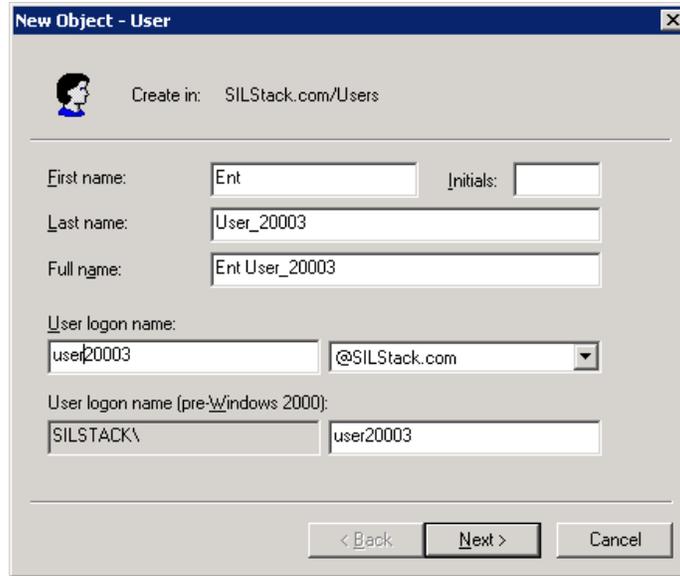
At the bottom of the form, there is a red asterisk and the text "* Input Required", along with "Commit" and "Cancel" buttons.

6. Configure Microsoft Exchange 2007 Subscriber Accounts

This section details the administrative steps for adding a new subscriber in Microsoft Exchange. This is accomplished by creating a new user account in the Active Directory server of the sample Avaya configuration. It is assumed that Microsoft Exchange has been installed and configured properly. From the desktop of the Active Directory server, select **Start**→**Programs**→**Active Directory Users and Computers**. This action will launch the **Active Directory Users and Computers** window as seen below.

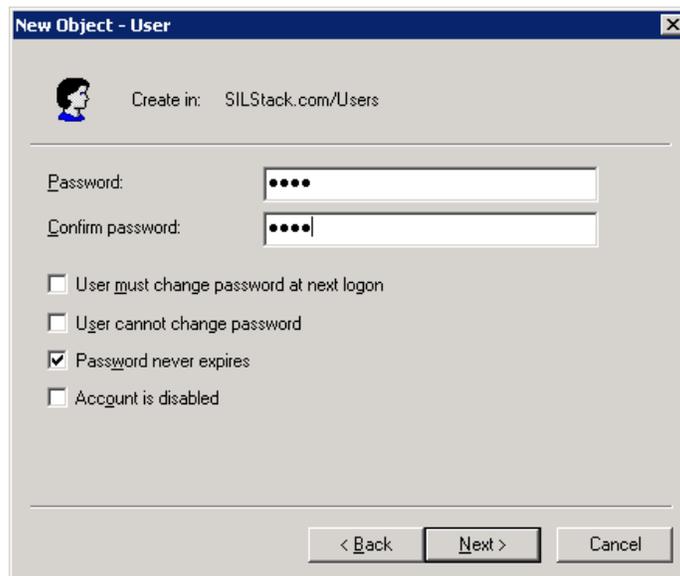


Select **Action**→**New**→**User** to create a new account (not shown). This action will launch the **New Object - User** window. In the **New Object – User** window, enter **First name**, **Initials** (if required), **Last name**, and **User logon name**. The **Full name** and **User logon name** are populated automatically based on the entries from the other fields. Click on **Next** to continue.



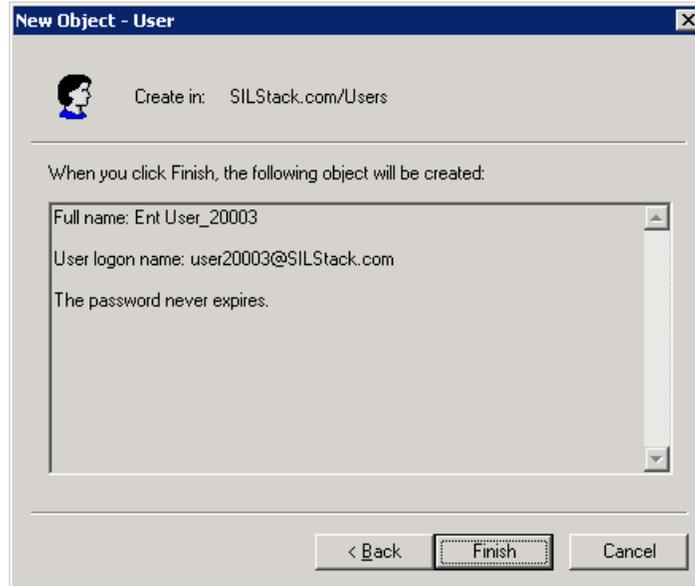
The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: SILStack.com/Users'. Below this, there are several input fields: 'First name' with the value 'Ent', 'Initials' (empty), 'Last name' with the value 'User_20003', and 'Full name' with the value 'Ent User_20003'. There are also fields for 'User logon name' (value 'user20003') and a dropdown menu (value '@SILStack.com'). Below these is a field for 'User logon name (pre-Windows 2000)' with the value 'SILSTACK\user20003'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Enter the **Password** and **Confirm password** entries. For these Application Notes, there is no need to change the password, so the **Password never expires** checkbox is enabled. Click **Next** to continue.

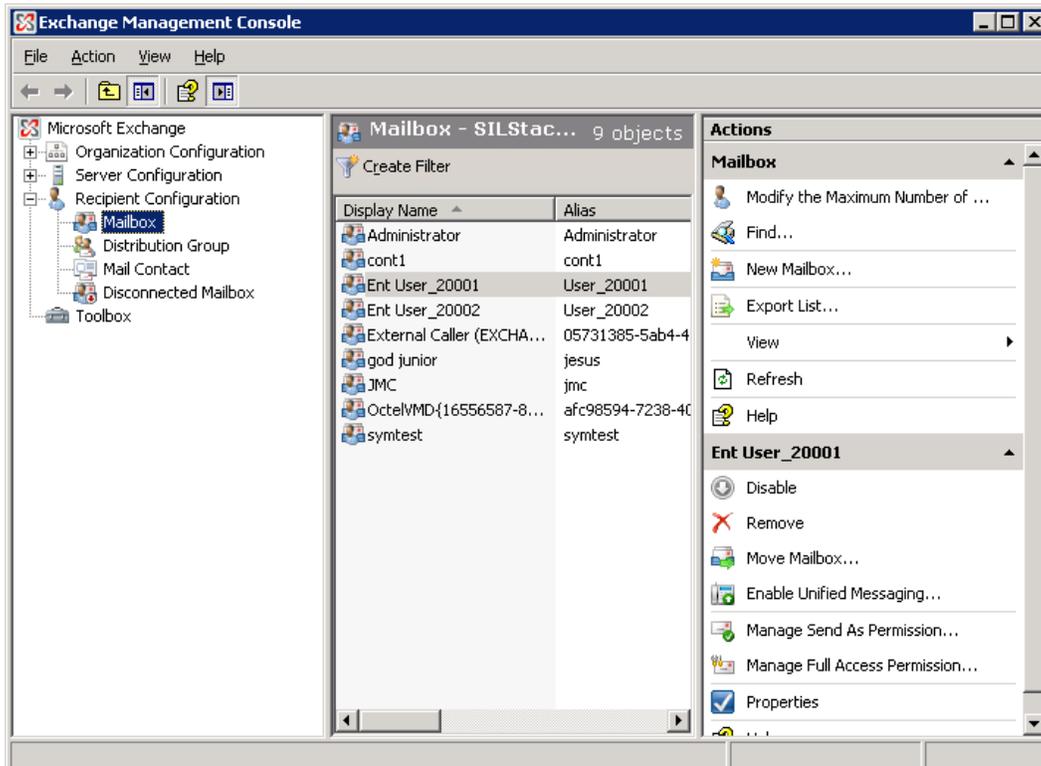


The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: SILStack.com/Users'. Below this, there are two password input fields: 'Password' and 'Confirm password', both containing four dots. Below these are four checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (unchecked), 'Password never expires' (checked), and 'Account is disabled' (unchecked). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

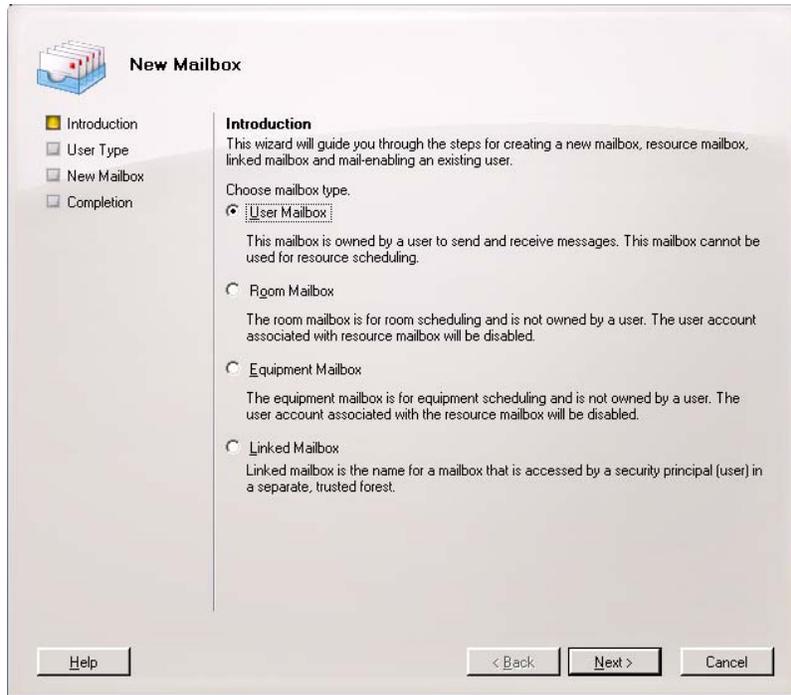
Click Finish to confirm the creation of the new subscriber



From the desktop of the Microsoft Exchange 2007 server, select **Start→Programs→Microsoft Exchange Server 2007→Exchange Management Console**.



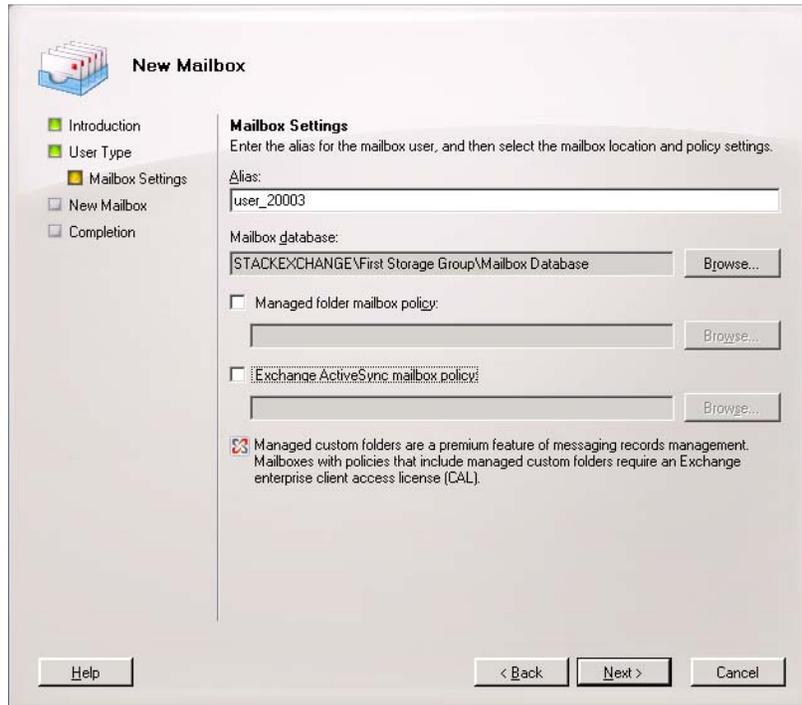
Right click **Recipient Configuration**→**Mailbox** and select **New Mailbox**. The New Mailbox wizard opens up. Select **User Mailbox** and click **Next**.



Select **Existing user** and click the **Add** button to display a list of users already created in the active directory earlier in this section (not shown). Once the user is added, click **Next**.



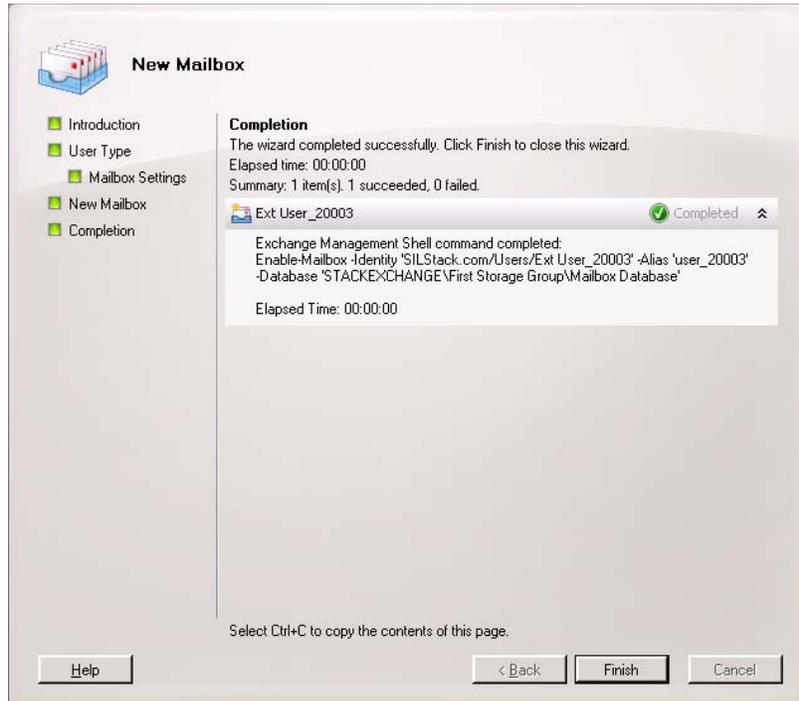
Select the required **Mailbox database**. For the purposes of these Application Notes the remaining settings remained unchanged. Click **Next**.



Click **New** on the next screen to create the Mailbox.



A confirmation screen is displayed after successful completion. Click **Finish**.



At this point please refer to References [9] and [10] to configure the active directory permissions for this subscriber to allow one-X Speech interact with subscriber emails.

7. Configure Avaya one-X[®] Speech

This section details the administrative steps for configuring a new one-X Speech server.

7.1. Pre-Installation Requirements of an Avaya one-X[®] Speech Server

References [9] and [10] discuss in detail the hardware and software requirements of a new one-X Speech Server. This section is intended to be used as a quick overview of those requirements.

- 1) The one-X Speech system requires NMS Communication T1/E1 telephony adapter cards to interface with Communication Manager. See Reference [10] for more detail. During software installation, the proper NMS drivers are installed. Some manual configuration is required once installation is complete. This will be discussed further in **Section 7.3.2**.
- 2) A valid license file is required during installation of one-X Speech software. Contact an authorized Avaya account representative to obtain a license file.
- 3) Ensure that the proper CDO and Hotfix is installed. See the Reference [10] for details.
- 4) For one-X Speech to communicate with Microsoft Exchange e-mail servers, a dedicated service account for a domain user with local administrative login privileges on the standalone one-X Speech server must be created as documented in reference [9]. This service account must be visible in the global address list (GAL) to ensure that one-X Speech operates properly. These Application Notes use a service account of cont1@silstack.com.
- 5) Each subscriber must be configured with the correct permission in Active Directory as documented in reference [9].

7.2. Avaya one-X[®] Speech Software Installation Guidelines

Follow the instructions for one-X Speech installation as described in Reference [4]. A successful one-X Speech installation is dependent on meeting all pre-installation requirements in **Section 7.1**. This section is intended to be used in conjunction with the system installation instructions referenced above for one-X Speech. Listed below are some suggestions to ensure a smooth installation.

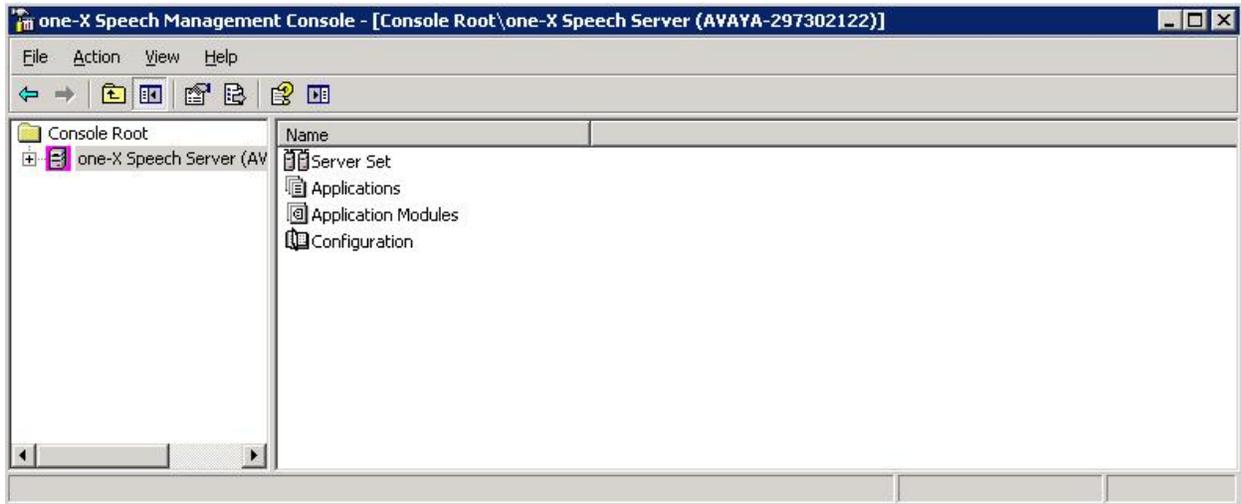
1. Turn off all installed virus protection software for the duration of the install.
2. Do not select **Use Secure Sockets Layer (SSL) for web interfaces** on the **Speech Server Configuration** window if the proper certificates for SSL are not installed. Access to WebLM as well as one-X Speech Access User Preferences and one-X Speech Access Users Management will not be accessible if not configured properly.
3. The **one-X Speech – Installation Wizard** is the ‘master’ configuration wizard for one-X Speech system installation. This ‘master’ wizard initiates each software install process, and then once the software has successfully been installed, the ‘master’ wizard regains

control and either prompts for a reboot, or continues on to the next software package to install.

4. From the **one-X Speech – Installation Wizard** window, select either **en-US** for US English or **en-UK** for UK English when selecting languages to install for **Avaya one-X Speech Access**. Do not select both languages as one-X Speech supports only one installed language.
5. When prompted for **Installation Reminders**, select **Configure Windows to automatically login on reboots**. The system will reboot several times after certain software installations. Enabling this feature will allow Windows to store the service account password for use when needed to log back in Windows after a reboot.
6. There will be times when a software package requires a reboot after installation (i.e. after Nuance is installed). When prompted by the software installer to restart the system, select **“No, I will restart my computer later”**. The **one-X Speech – Installation Wizard** will then display a **Reboot Required** dialog box. Click **Reboot Now** to reboot the server. Once the server is rebooted, the **one-X Speech – Installation Wizard** will continue the install from the previous spot before the reboot was executed.
7. A valid WebLM license file is required for installation of the one-X Speech Server. Do not continue without installing this license file. Initial configuration of the one-X Speech Server reads the license file before creating the default engines (i.e. Speech Engines) for the Server Set. Without a proper license file, the complete set of default engines will not be created.
8. A Public folder needs to be added from Exchange Management Console on the Microsoft Exchange 2007 server for a storage group. While adding users, one-X Speech assumes that a Public Folder has been added for a storage group.

7.3. Avaya one-X[®] Speech Software Configuration

This section details the administrative steps for configuring one-X Speech. This section will also cover adding user accounts to the one-X Speech database. Launch **Server Management Console** from the one-X Speech server desktop, select **Start→Programs→Avaya one-X Speech Server →Avaya one-X Speech Server Management Console**. This action will launch the **one-X Speech Server Management Console** window as seen below. The **one-X Speech Server** name of **AVAYA-29730212** is derived from the machine name created when Windows 2003 Server was installed.



7.3.1. Number Translation Parameters

Expand the **one-X Speech Server (AVAYA-29730212)** node in the Component Tree. Select **OK** to set up telephony properties when the **Important** dialog box is displayed on initial startup (not shown). The **Number Translation Parameters** window is displayed. At a minimum, the **Dialing Parameters for System** section in the upper left hand corner should be completed. More detailed information on completing this form can be found by navigating to **Start→Programs→Avaya one-X Speech Server→Administrator Guide**. The dial plan configured here should match the dial plan configured in Communication Manager. When changes to the dial plan are required in one-X Speech, they can be made at any time by navigating in the **one-X Speech Server Management Console** to **Configuration→Telephony Setup**, then clicking the **Number Translation Parameters** button. For these Application Notes, the Local Numbers were configured for a 5 digit extension dial plan. No additional entries were needed beyond setting up the **Dialing Parameters for System** section. Click **Accept** when complete. Click **OK** when the **Continue?** Dialog box is displayed (not shown). This action launches a hidden auto initialization process that takes a few seconds to complete. At this time, all default engines are created. Keystrokes and button clicks will not be accepted during this initialization process. After the process is complete, The **one-X Speech Server Management Console** is displayed.

Number Translation Parameters

Dialing Parameters for System

Country Code (U)

Area Code (G)

Off PBX Prefix (P)

National Prefix (N)

International Prefix (I)

Calling Number (ANI) Substitutions for None

ANI Template	ANI Substitution

Add Delete Edit

Dialing Parameters for **Default** Group

Country Code

Area Code

Off PBX Prefix

National Prefix

International Prefix

Group Members

Group Template

All Accounts

Dialing Rules

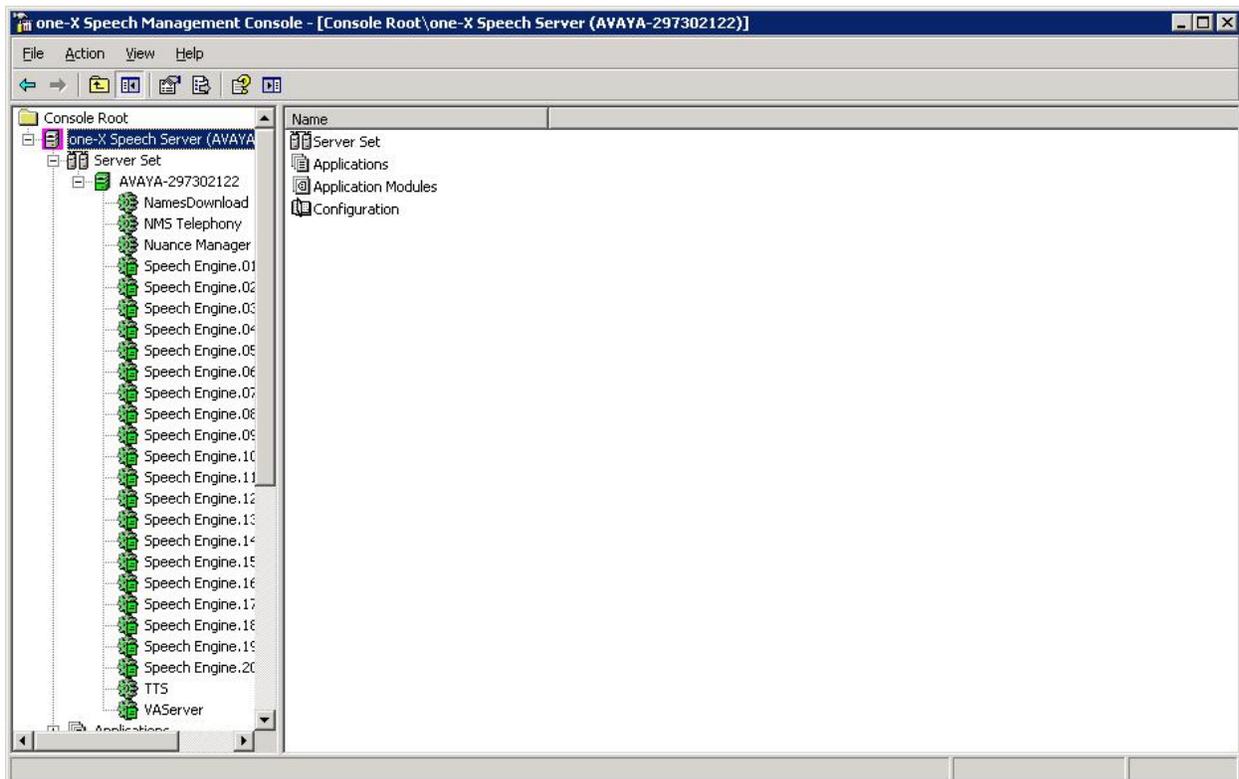
CC	AC	Prefix	Number	Dial	ANI Sub Tbl
Forbidden Numbers					
Private Numbers					
Local Numbers					
			RRRRR	XXXXX	
Long Distance Numbers					
1			RRRRRRRRR	PNXXXXXXXXXX	
International Numbers					
V			0000000000RRRRR	PIUXXXXXXXXXXXXXX	

Add Delete Edit

Accept Cancel

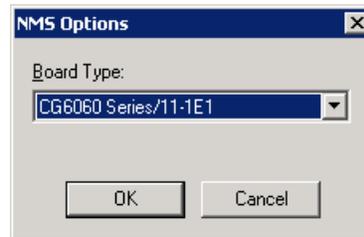
Expand the **Server Set** node in the Component Tree to view the engines created. Ensure that the following engines are created by the auto-initialization process:

- **NamesDownload** – Engine for retrieving and downloading corporate information such as directory names and telephone numbers using LDAP.
- **NMS Telephony** – Engine used for providing adapters required for interoperability with Communication Manager.
- **Nuance Manager** – Engine that provides isolated speech recognition functions.
- **Telephony Engines** [named **Speech Engine.1** to **Speech Engine.20**] - Engine that hosts the virtual machine that executes the one-X Speech application. A Telephony Engine process can support one user at a time but multiple engines can run simultaneously on an one-X Speech server. For these Application Notes, 20 Telephony Engines were defined.
- **TTS** - Engine that is responsible for applying dictionary rules to text strings and translates the text strings into an audio stream.
- **VAServer** – Engine for one-X Speech Server Set level management functions.

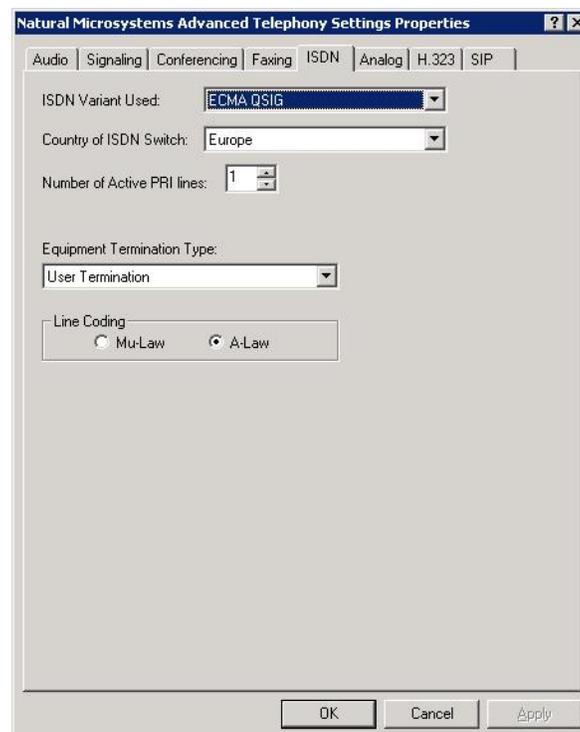


7.3.2. Configuring E1 Connection

Click on **NMS Telephony** in the Component Tree. The properties for this engine are displayed on the right side of the screen. From the **Properties** screen, select the **Options** button (not shown). The **NMS Options** window is displayed. Select the **Board Type** installed in the server. For the one-X Speech server used in these Application Notes, a **CG6060 Series** card was installed. Click **OK** when complete.

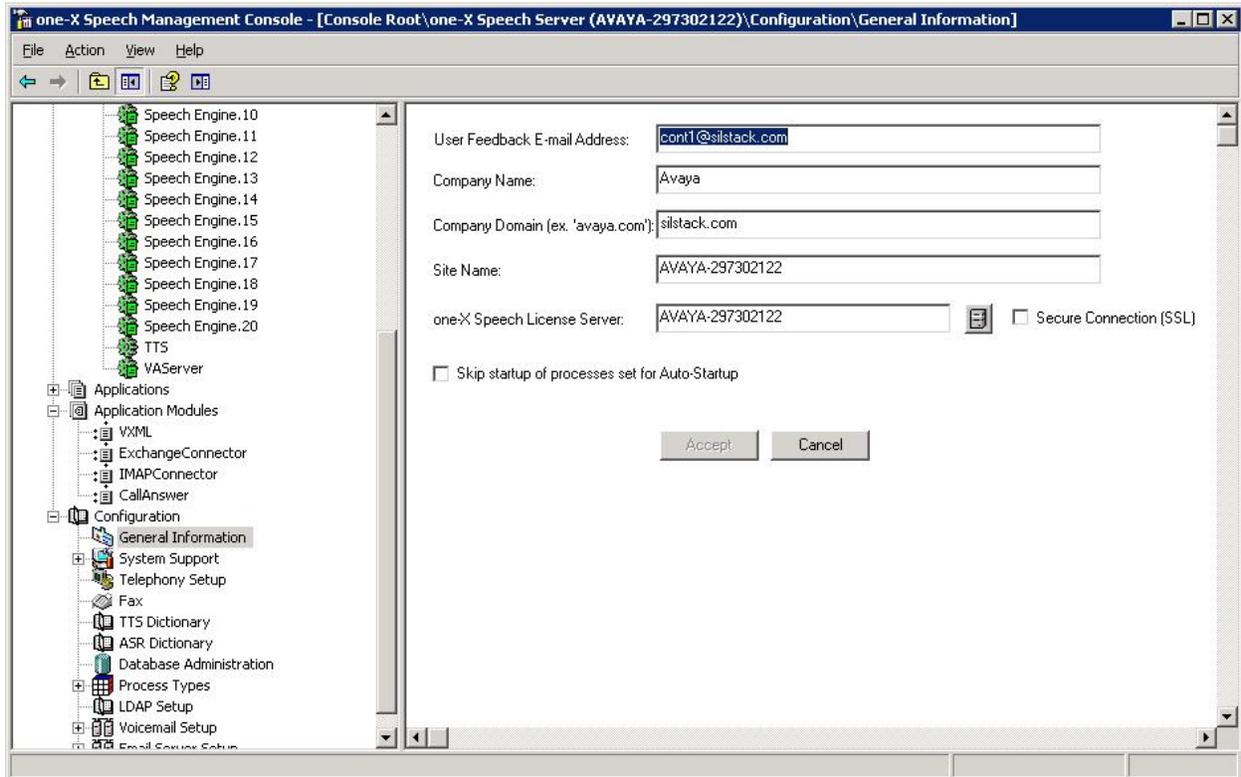


From the **Properties** screen, select the **Advanced** button. The **Natural Microsystems Advanced Telephony Settings Properties** window is displayed. Select the **ISDN** tab. Select the correct value for **Number of Active PRI lines**. These Application Notes utilize only one ISDN-PRI trunk. Click **OK** when complete. When the NMS Telephony engine is set up correctly and connected to an active E1 trunk from Communication Manager, the engine indicator light will change from red to green. This will be seen throughout the remainder of the Application Note in subsequent screen shots of the **one-X Speech Server Management Console**. Please refer to Reference [12] for more information on configuring an E1 trunk on Communication Manager.



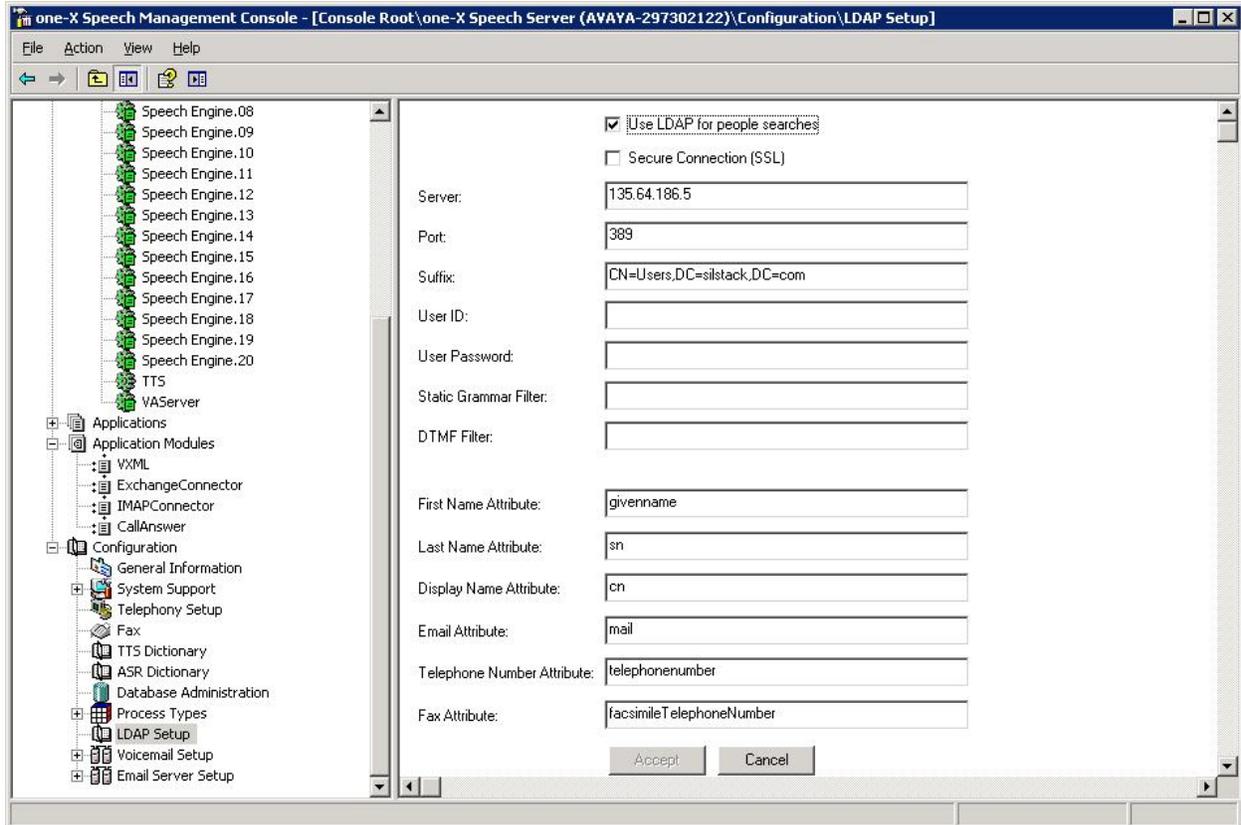
7.3.3. Configuring General Information

From the **one-X Speech Management Console**, expand the **Configuration** node. Click on **General Information** and complete all fields. The service account of cont1@silstack.com that is mentioned in **Section 7.1** is used as the **User Feedback E-mail Address**. A **Company Domain** of **silstack.com** is used. The **Site Name** and **one-X Speech License Server** are set to the one-X Speech server name of **AVAYA-29730212**. Click **Accept** when complete.



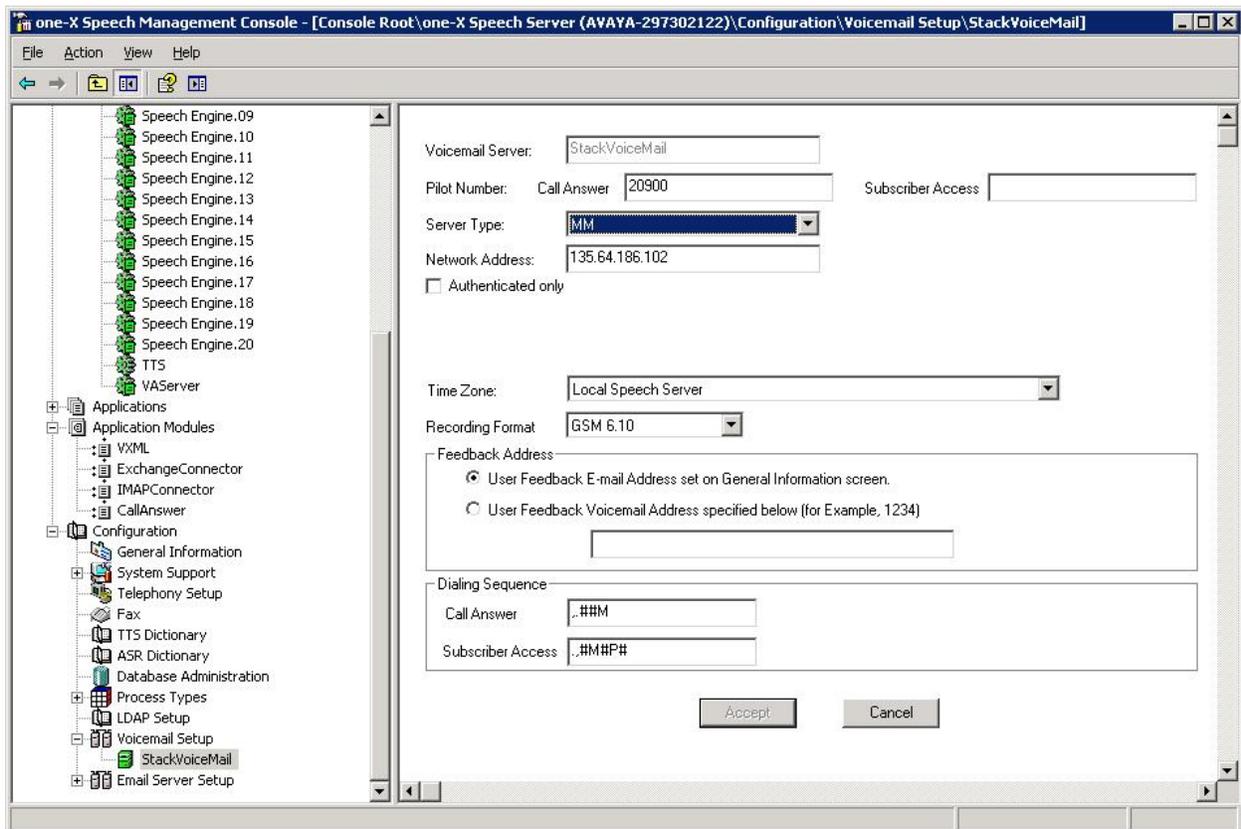
7.3.4. Configuring LDAP Integration

From the **one-X Speech Management Console**, expand the **Configuration** node. Click on **LDAP Setup**. Select **Use LDAP for people searches** to enable LDAP searches in Active Directory. The server is set to **135.64.186.5**, which is the Active Directory server IP address. The **Port** is **389**, which is the default LDAP port. A **Suffix** of **CN=Users,DC=silstack,DC=com** was used where CN is a container name, and DC is the DNS and DNS qualifier. Default values may be used in the remaining fields. Click **Accept** when complete.



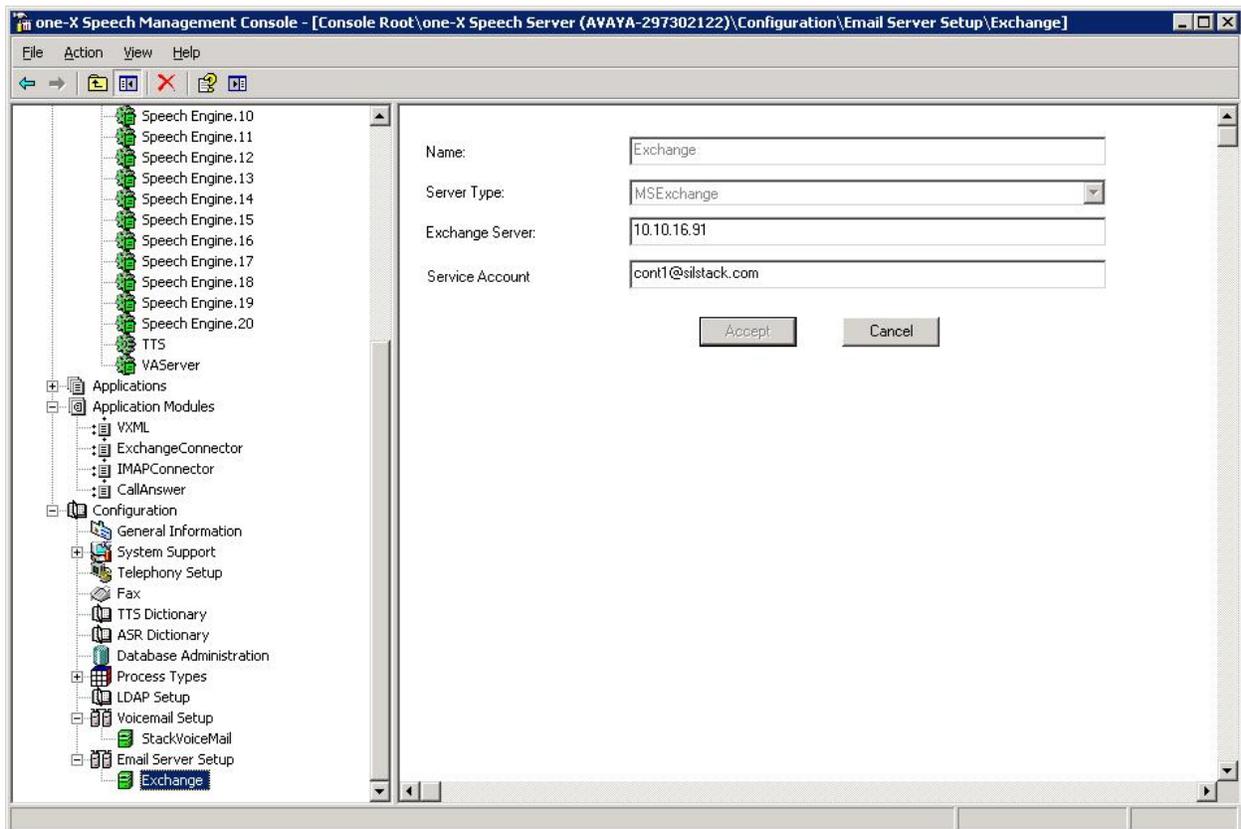
7.3.5. Configuring Voicemail Integration

From the **one-X Speech Management Console**, expand the **Configuration** node. Right click on **Voicemail Setup**, and then select **new**→**Voicemail Server** from the dropdown menu to add a voicemail server to the one-X Speech server. Enter a descriptive name for **Voicemail Server**. The **Server Type** field is **MM**, which equates to the MSS at **Network Address 185.64.186.102**. **Subscriber Access** is set to **20900** which is the pilot number for Avaya Modular Messaging. Default values are used in the remaining fields. Click **Accept** when complete. The screen shot below displays a voice mail server already configured for one-X Speech, which is used to describe field entries for this step.



7.3.6. Configuring Email Integration

From the **one-X Speech Management Console**, expand the **Configuration** node. Right click on **Email Server Setup**, and then select **new**→**Email Server** from the dropdown menu to add an email server to the server. Select **MSEExchange** as the **Server Type** to designate this as a Microsoft Exchange email server. The **Name** will default to **Exchange** as a result of setting the **Server Type** field to **MSEExchange**. The **Exchange Server IP address** is **10.10.16.91**. The **Service Account** value entered should match the service account mentioned in **Section 7.1**. Click **Accept** when complete. The screen shot below displays an email server already configured for one-X Speech, which is used to describe field entries for this step.



7.3.7. Configuring VAOutlook

From the **one-X Speech Management Console**, expand the **Applications** node. Click on **VAOutlook** to display the properties. Click on the **Advanced** button in the **Properties** window (not shown). This action launches the **Advanced** window as seen below. Set the **Account Number length** appropriately. This sample server uses a **5** digit account number. Default values are used in the remaining fields. Click **Done** when complete.

The screenshot shows the 'Advanced' configuration window for VAOutlook. The window is titled 'Advanced' and contains three sections:

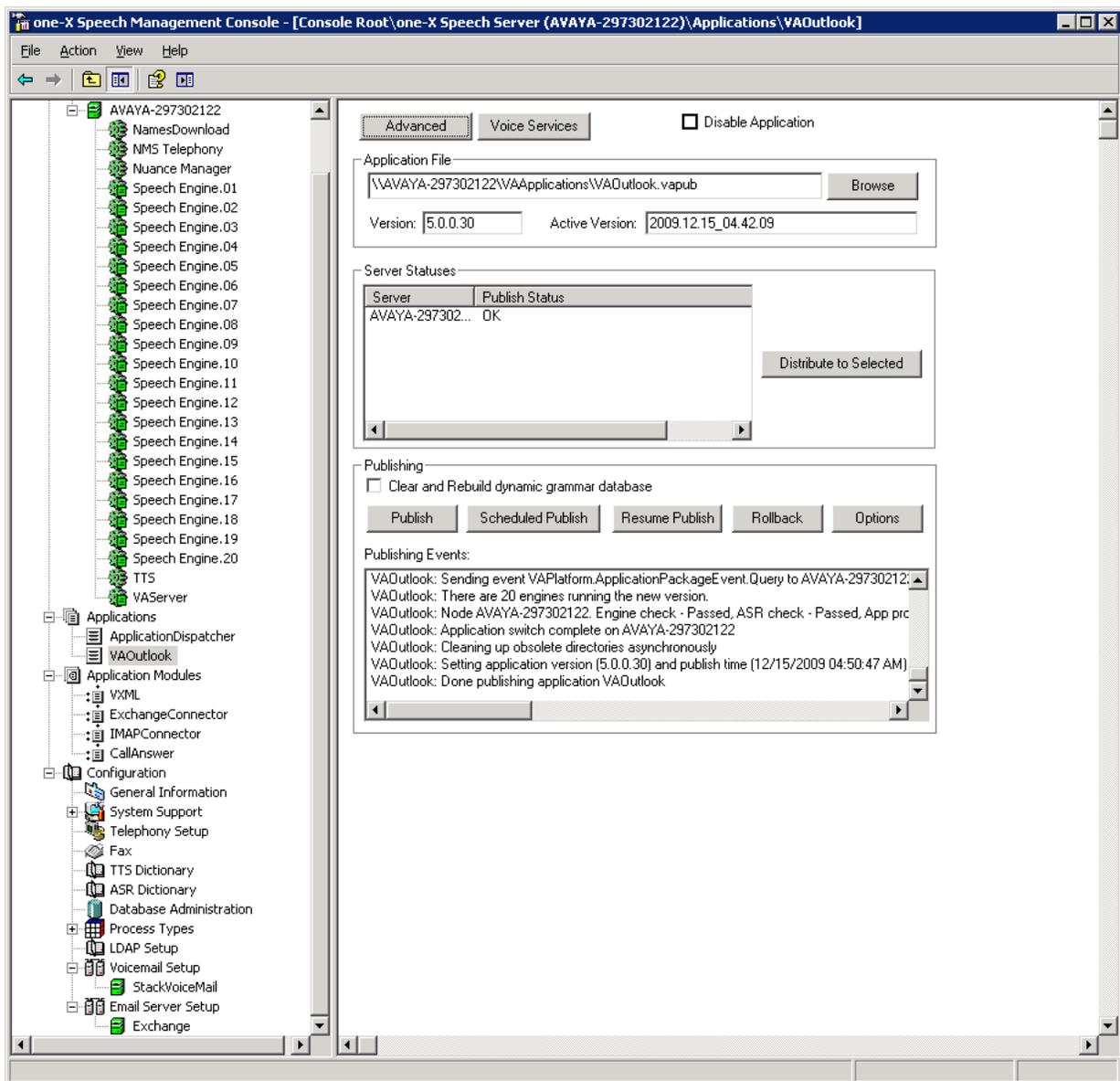
- Application Settings:**
 - Allow SA to access Microsoft Exchange
 - Account Number length:
 - Use Voice Server directory
 - Always require password for Express Logon
 - Allow SA to access Lotus calendar
 - Lotus calendar delegate account password:
- Music On Hold:**
 - Path to wave file:
 -
- Speech Recognition Parameters:**
 - Return N Best Recognition Results
 - Max Number of Recognition Results:

At the bottom of the window are two buttons: and .

7.3.8. Publishing Application Modules

From the **one-X Speech Management Console**, expand the **Application Modules** node. From here, the following Application Modules require publishing: **ExchangeConnector**, **IMAPConnector**, and **CallAnswer**. This is accomplished by clicking on each module, and in the **Properties** window, clicking on the **Publish** button. Only publish one application module at a time. It will take up to 5 minutes for an application module to publish. A confirmation message will be displayed when publishing is complete for a particular application module.

After these 3 application modules are published, from the **one-X Speech Management Console**, expand the **Application** node and publish the **VAOutlook** Application. An example of the **VAOutlook** module after a successful publish is displayed below. The last line of the **Publishing Events** dialog box should contain the text **Done publishing**.



7.3.9. User Creation

To create a one-X Speech user, go to **Start**→ **Programs**→**Avaya one-X Speech Access**→**one-X Speech Access Users Management**. This action launches the **one-X Speech Access Users Management** web screen. Enter the proper Administrator login name and password to access the web screen. To create a user, enter the following information

- **Account Number:** A unique 5 digit number. This 5 digit account number length was defined in **Section 7.3.7**. For this example, the account number will match the user **Phone Number** of **20001**.
- **Authorization Code:** A value is required in this field if the PBX requires an authorization code. This code is also used for advanced features of one-X Speech such as Reach- Me and Wake-up.
- **Outcall Restriction:** This restricts the type of phone numbers the subscriber can dial for advanced features such as Reach-me and Wake-up.
- **Display name:** A descriptive name of the user.
- **Voicemail Server Setup:** Select the appropriate **Voicemail Server** in the drop down list. The server list was created back in **Section 7.3.5**.
- **Exchange Setup:** Enter the email **Alias**. The alias was this user was created in **Section 7.3.6**. Click **Add User** when complete.

The screenshot shows the 'one-X Speech User Management' web application in a Windows Internet Explorer browser. The page title is 'User Management' and it features the Avaya logo. The main content area is titled 'Add User' and contains several sections:

- Navigation Links:** Add User, Modify User, List Users, Bulk Provisioning, Product Information.
- Form Fields:**
 - Account Number: 20001
 - Phone Number: 20001
 - Authorization Code: (empty)
 - Outcall Restriction: International
 - Display Name: Ent User 20001
 - Reach-Me:
- Voicemail Server Setup:**
 - Voicemail
 - Voicemail Server: StackVoiceMail
 - Voice Mailbox: 20001
 - No voicemail
- Exchange Setup:**
 - Exchange
 - Alias: EntUser_20001
 - No E-mail
- one-X Speech Password:** (password field)

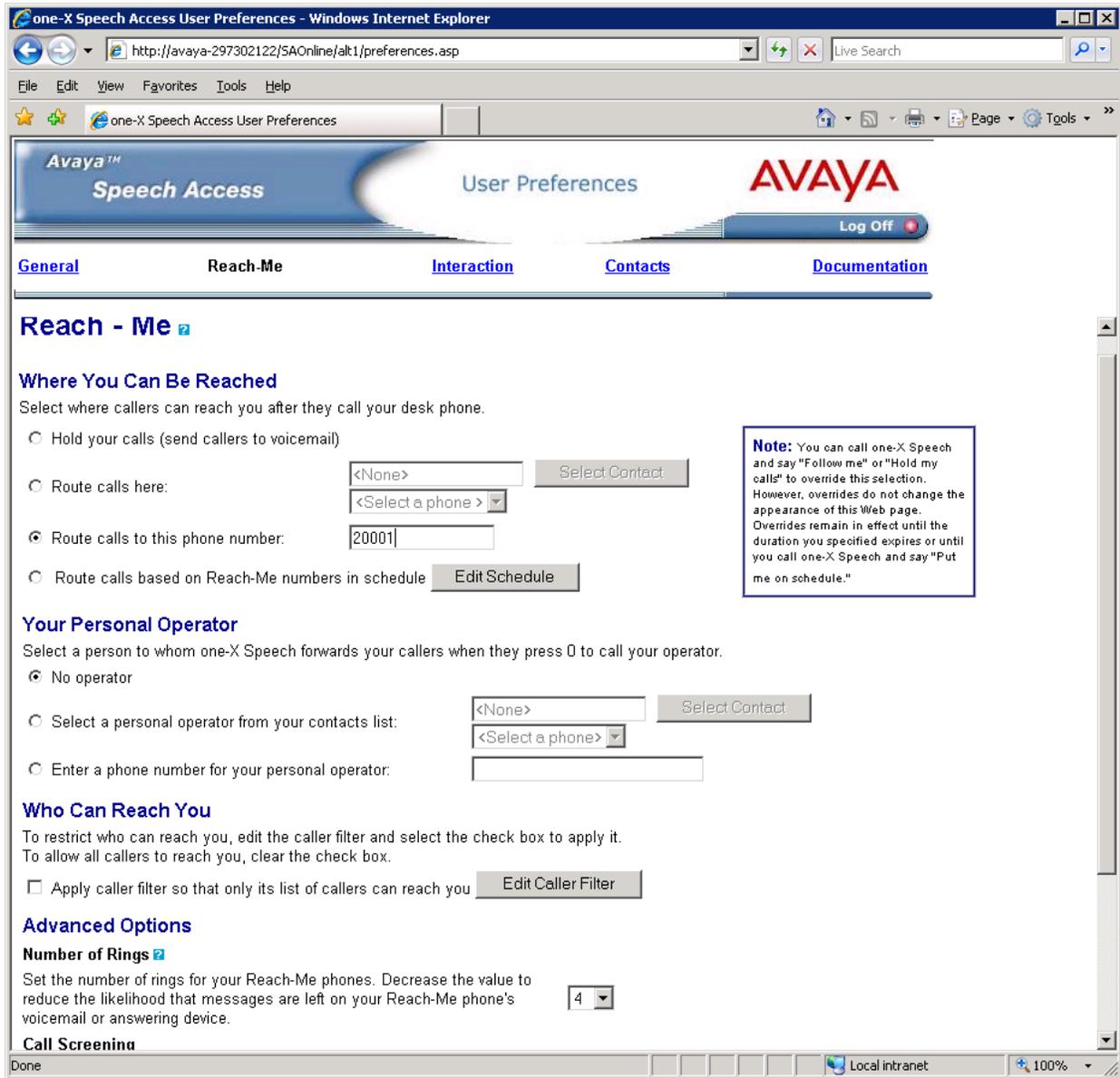
A yellow tooltip box on the right side of the form contains the text: "Enter the subscriber's Exchange alias. This alias must be valid."

At the bottom of the form are two buttons: "Add User" and "Clear".

On the left side of the page, there is a sidebar with the following information:
Total Users: 0
Available Licenses: 1000

7.3.10. User Configuration

Users can be configured by running **Start**→ **Programs**→**Avaya one-X Speech Access**→**one-X Speech Access Users Management**. The appropriate credentials for the user are entered in the log in screen (not shown). Select **Reach Me** in the top menu of the subsequent screen to display the screen shown below. Ensure that **Route calls to this phone number** is configured to the extension of the user. This will allow speech users to receive calls while logged into one-X Speech.



8. Verification Steps

The following steps can be used to verify correct operation of the configuration as described in these Application Notes.

- Place a call to a configured user for example 20001. Leave a message on that subscribers voicemail. Ensure the MWI is illuminated on the handset.
- Dial one-X Speech using the pilot number 80900 from a different handset. Enter the account number via DTMF or voice. In this case it is 20001. Enter the Modular Messaging subscriber password. A greeting tone should be played by one-X Speech followed by the message “**What can I do for you?**”
- Say “**Dial a Number**” and follow the instructions to dial a number. Ensure that the correct number is dialed. Answer and hang up the call.
- Say “**List my voice messages**”. one-X Speech should play the voice mail left earlier. This will verify correct integration with Modular Messaging.
- Say “**List my e-mails**”. one-X Speech should play any emails associated with this account. This will verify correct integration with Microsoft Exchange.

9. Conclusion

These Application Notes show that Avaya one-X[®] Speech and Single Server Avaya Modular Messaging can provide centralized functionality to multiple Avaya Aura[™] Communication Manager systems using a single Avaya Aura[™] Session Manager.

10. Additional References

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

Avaya Aura™ Session Manager:

- [1] Avaya Aura™ Session Manager Overview, Doc ID 03-603473, available at <http://support.avaya.com>.
- [2] Installing and Upgrading Avaya Aura™ Session Manager, Doc ID 03-603324, available at <http://support.avaya.com>.
- [3] Maintaining and Troubleshooting Avaya Aura™ Session Manager, Doc ID 03-603325, available at <http://support.avaya.com>.
- [4] Administering Avaya Aura™ Session Communication Manager as a Feature Server, Doc ID 03-603479, available at <http://support.avaya.com>.

Avaya Aura™ Communication Manager 5.2.1:

- [5] SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers, Doc ID 555-245-206, May, 2009, available at <http://support.avaya.com>.
- [6] Administering Avaya Aura™ Communication Manager, Doc ID 03-300509, May 2009, available at <http://support.avaya.com>.

Avaya Modular Messaging 5.2:

- [7] Installing Avaya Modular Messaging on a Single Server Configuration, available at <http://www.avaya.com>.
- [8] Modular Messaging Multisite Guide Release 5.2, available at <http://www.avaya.com>.

Avaya one-X® Speech 5.2:

- [9] Avaya™ one-X™ Speech Release 5.2 Installation Guide, available at <http://www.avaya.com>.
- [10] Avaya™ one-X™ Speech Release 5.2 Site Preparation Guide, available at <http://www.avaya.com>.

Avaya Configuration Notes:

- [11] Configuration Note 88011 – Version B (1/10) Avaya S8300/S85x0/S84x0/S87x0 SIP Integration using Avaya Session Manager, available at <http://www.avaya.com>.
- [12] Configuration Note 3603 – Rev. K (2/09) UCC / Avaya one-X Speech Avaya IP 600/G3/S8700/S8300 –E1 QSIG, available at <http://www.avaya.com>.

Avaya Application Notes:

- [13] Application Notes for Configuring Remote User Access for Avaya Telephony Products over VPN IPSEC and VPN SSL, available at <http://www.avaya.com>.
- [14] Application Notes for Configuring Avaya one-X® Mobile as part of Avaya Unified Communication Mobile Worker Solution, available at <http://www.avaya.com>.

[15] Application Notes for Configuring Avaya one-X® Portal as part of Avaya Unified Communication Mobile Worker Solution, available at <http://www.avaya.com>.

©2010 Avaya Inc. All Rights Reserved.

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

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