



## **Configuring Microsoft Exchange Server 2010 Unified Messaging with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required to integrate Microsoft Exchange Server 2010 Unified Messaging (UM) with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Exchange UM is a voice mail system that combines voice messaging, fax, and e-mail into one inbox, which can be accessed from a telephone or computer. UM subscribers can have their calls cover to voicemail and can retrieve their messages from a telephone by calling into a voice mailbox, or from a PC via the Play-on-Phone feature available with Outlook Web Access (OWA). In addition, Exchange UM can control the Message Waiting Indicator (MWI) on a user's telephone to notify the user of new voicemail messages. The focus of these Application Notes is on the Exchange UM component of Microsoft Exchange Server 2010.

These tests were executed with the cooperation of Microsoft, based in part on test cases outlined in the Microsoft UC Open Interoperability Program (OIP) Test Plan, *Telephony Partner Product Interoperability Specification Interfaces for Connection to Mediation Server/OCS 2007 R2 and to Exchange Server 2010 Unified Messaging*, June 2009. Additional test cases specific to Avaya capabilities were also included. Not all test cases were executed successfully. Readers should note specific limitations and constraints as documented in **Section 2.2**, Test Results.

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

# 1. Introduction

These Application Notes describe the configuration steps required to integrate Microsoft Exchange Server 2010 Unified Messaging (UM) with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Exchange UM is a voice mail system that combines voice messaging, fax, and e-mail into one inbox, which can be accessed from a telephone or computer. UM subscribers can have their calls cover to voicemail and can retrieve their messages from a telephone by calling into a voice mailbox, or from a PC via the Play-on-Phone feature available with Outlook Web Access (OWA). In addition, Exchange UM can control the Message Waiting Indicator (MWI) on a user's telephone to notify the user of new voicemail messages. The focus of these Application Notes is on the Exchange UM component of Microsoft Exchange Server 2010.

## 2. General Test Approach and Test Results

The general test approach was to exercise the features of Exchange UM and verifying the appropriate behavior. All test cases were performed manually.

### 2.1. Interoperability Compliance Testing

The interoperability compliance test covered the following features:

- Calls to Exchange UM from subscribers and non-subscribers, including a VDN/vector scenario where final call treatment is to a subscriber's mailbox.
- Calls to UM subscribers covered to Exchange UM on no-answer and the appropriate greeting was played to the caller. Voicemail was left for the UM subscriber.
- Subscribers logging into Exchange UM.
- MWI lamp of a subscriber's phone was turned on when a new voicemail message existed.
- UM subscriber was able to retrieve voicemail messages from a phone, which would extinguish the MWI.
- UM subscriber was able to use Play-on-Phone via OWA to listen to voicemail messages.
- UM subscriber was able to navigate Exchange UM using the Voice User Interface or Telephony User Interface.
- Call transfer from Exchange UM to another subscriber.
- Calls to the UM Auto Attendant.
- G.711 and G.723 codec support.
- Calls to Exchange 2010 UM were performed with direct IP-IP media (i.e., shuffling) enabled.
- Configuration with Exchange 2007/2010 co-existence, Exchange 2010 UM redirected calls to Exchange 2007 UM for subscribers on Exchange 2007 UM.
- Configuration with primary and backup Exchange UM server, verified that the backup Exchange UM server would handle calls when the link to the primary server was down.
- Verified that calls can cover to Exchange UM for an extension specified in the "messaging" step of a vector.
- Various call transfer scenarios were verified with Exchange UM coverage.

- Call answering rules to do a “Find Me” or “Transfer” to another number.

## 2.2. Test Results

All test cases were successful, except for the following observations:

- Unlike Exchange 2007 UM, Exchange 2010 UM requires an external fax server, which wasn't available during testing. The T.38 negotiation would have been between Communication Manager and a 3<sup>rd</sup> party fax server. The scope of Fax T.38 testing was to verify that Exchange UM returns the correct URL of the external fax server in the REFER message when it detects a fax tone, which was verified successfully.
- In a configuration with Microsoft Exchange 2007/2010 co-existence, Shuffling (i.e., direct IP-IP calls) between H.323 stations and Exchange 2007 UM is not supported. If Exchange 2010 UM redirects a call to Exchange 2007 UM, the call is initially shuffled successfully. However, when the first DTMF digit is pressed on the H.323 station to log into Exchange UM or use the Telephony User Interface, Communication Manager un-shuffles the call, which is unsuccessful. Once no more DTMF tones are being sent, Communication Manager shuffles the call again successfully. When the H.323 station dials another DTMF digit, the call is un-shuffled again unsuccessfully. This occurs every time the H.323 station sends a DTMF tone. This causes the H.323 station to not hear all of the UM prompts.
- TLS is currently not supported between Exchange UM and Session Manager 5.2.1 due to certificate issues.

## 2.3. Support

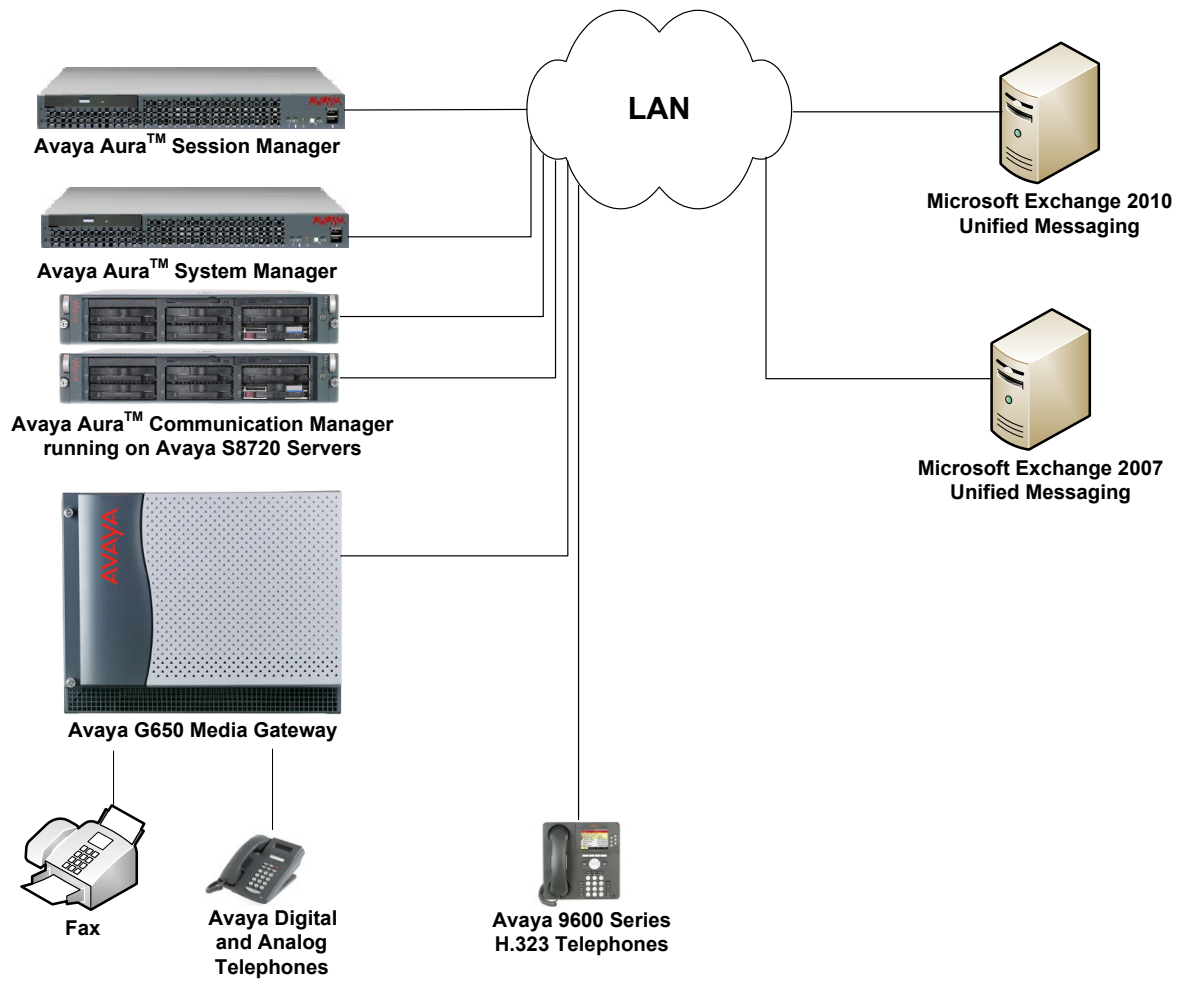
Technical support of Microsoft Exchange Server 2010 Unified Messaging is available at Microsoft Technet at <http://technet.microsoft.com/en-us/library/bb125141.aspx>. Additional support options are also covered on this webpage.

### 3. Reference Configuration

The following diagram illustrates a sample configuration consisting of Communication Manager running on a pair of S8720 Servers, Session Manager, and Exchange UM servers. Avaya 9600 Series H.323 IP Telephones, Avaya digital, and Avaya analog telephones were included in the configuration to serve as UM subscribers. A SIP trunk was established between Session Manager and the Exchange UM servers. The Avaya G650 Media Gateway connected to the PSTN via an ISDN-PRI trunk. Avaya Aura® System Manager was used to configure Session Manager.

**Note 1:** The configuration of Exchange 2007/2010 co-existence, while tested, is outside the scope of documenting configuration steps in these Application Notes and will not be covered. However, the configuration of a backup Exchange UM server to support UM failover scenarios is covered.

**Note 2:** Session Manager Release 5.2.1 was used as the basis for this set of testing. To support direct SIP endpoints, this release requires a Communication Manager Feature Server, which was not included in the configuration. Readers should take explicit note that Avaya SIP clients were not used in these tests.



**Figure 1: Test Bed Configuration**

## 4. Equipment and Software Validated

The following equipment and software were used in the configuration.

Equipment	Software
Avaya S8720 Servers with Avaya G650 Media Gateway	Avaya Aura® Communication Manager 5.2.1 (R015x.02.1.016.4) with SP 5 (Patch 18475)
Avaya G650 Media Gateway TN799DP C-LAN TN2602AP Media Processor TN2302AP Media Processor	HW01 FW031 HW02 FW047 HW20 FW120
Avaya Aura® Session Manager	5.2.1 (5.2.1.1.521012)
Avaya Aura® System Manager	5.2 (5.2.8.0)
Avaya 9630 IP Telephone	3.110b (H.323)
Avaya 6408D+ Digital Telephone	-
Analog Fax Machine	-
Microsoft Exchange Server 2007 SP 2 Unified Messaging with Microsoft Windows Server 2008 with SP 1 (64-bit)	Microsoft Exchange Server 2007 SP 2 Unified Messaging
Microsoft Exchange Server 2010 SP 1 Unified Messaging with Microsoft Windows Server 2008 with SP 2 (64-bit)	Microsoft Exchange Server 2010 SP 1 Unified Messaging

## 5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring a SIP trunk to Session Manager and a station with voicemail coverage to Exchange UM. Administration of Communication Manager was performed using the System Access Terminal (SAT). The SAT is accessed by establishing a telnet session to Communication Manager using a terminal emulation application.

This section covers the following configuration:

- **IP Node Names** to associate names with IP addresses.
- **IP Network Region** to specify the domain name and the IP codec set, to enable IP-IP direct audio (Shuffling), and to specify the UDP port range.
- **IP Codec Set** to specify the codec type used for calls to Exchange UM and to enable T.38 Fax support.
- **SIP trunks** for outgoing calls to Exchange UM and incoming calls from Exchange UM.
- **Private Numbering** to allow the caller's extension to be sent to Exchange UM.
- Voicemail **Hunt Group** for routing calls to Exchange UM.
- Voicemail **Coverage Path** to allow stations to cover to Exchange UM.
- **Stations** with voicemail coverage.
- **Locations** form to specify the route pattern used to send a re-INVITE when Exchange UM requests a different port number for receiving SIP signaling messages.
- **Call Routing** to route calls to Exchange UM using AAR.

### 5.1. Configure IP Node Names

In the **IP Node Names** form, assign a name and IP address for Session Manager and the C-LAN that will terminate the SIP trunk. The names will be used in the signaling group configuration configured later.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
03A_medpro	12.184.9.136	
<b>08A_CLAN</b>	<b>12.184.9.135</b>	
09A_Xfire	12.184.9.137	
default	0.0.0.0	
procr	0.0.0.0	
<b>sp-asm</b>	<b>12.184.9.144</b>	
( 6 of 6 administered node-names were displayed )		
Use 'list node-names' command to see all the administered node-names		
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name		

## 5.2. Configure IP Network Region

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *avaya.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints and Exchange UM 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 Exchange UM. This IP codec set is used when its corresponding network region (i.e., IP Network Region '1') is specified in the SIP signaling groups. Accept the default values for the other fields.

**Note:** The UDP port range should match the configured range on Exchange UM to avoid audio problems.

change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain: avaya.com	
Name: Avaya devices		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? y	
UDP Port Max: 65535		
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		



### 5.3. Configure IP Codec Set

In the **IP Codec Set** form, select the audio codec type supported for calls to Exchange UM. The form is accessed via the **change ip-codec-set 1** command. Note that IP codec set '1' was specified in IP Network Region '1'. The default settings of the **ip-codec-set** form are shown below. Exchange UM supports G.711mu-law, G.711a-law, and G.723.

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:	<b>G.711MU</b>	<b>n</b>	<b>2</b>	<b>20</b>		
2:						
3:						
4:						
5:						
6:						
7:						

To enable Fax T.38, set the Fax mode on **Page 2** of the IP codec set form to *t.38-standard*.

change ip-codec-set 1			Page	2 of	2
IP Codec Set					
Allow Direct-IP Multimedia? n					
	Mode	Redundancy			
<b>FAX</b>	<b>t.38-standard</b>	<b>0</b>			
Modem	off	0			
TDD/TTY	US	3			
Clear-channel	n	0			

## 5.4. Configure SIP Trunk for Outgoing Calls to Exchange UM

Add a signaling group for calls placed to Exchange UM. Incoming calls from Exchange UM (e.g., Play on Phone) will use a different signaling group configured in **Section 5.5**. Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form as shown below:

- Set the **Group Type** field to *sip*.
- Set the **Transport Method** field to *tcp*. TLS transport may also be used between Communication Manager and Session Manager.
- Specify the C-LAN in the Avaya G650 Media Gateway and the Session Manager as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values were configured in the **IP Node Names** form shown in **Section 5.1**.
- Set the **Near-end Listen Port** and the **Far-end Listen Port** fields to *5060*. If the **Far-end Network Region** field is configured, the codec for the call will be selected from the IP codec set assigned to that network region.
- Enter the domain name in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*.
- If calls to Exchange UM are to be shuffled, then the **Direct IP-IP Audio Connections** field must be set to 'y'.
- The **DTMF over IP** field is set to the default value of *rtp-payload*. Avaya Communication Manager supports DTMF transmission using RFC 2833.
- The default values for the other fields may be used.

add signaling-group 10		Page 1 of 1
SIGNALING GROUP		
Group Number: 10	Group Type: sip	
	Transport Method: tcp	
IMS Enabled? n		
Near-end Node Name: 08A_CLAN	Far-end Node Name: sp-asm	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
Far-end Domain: avaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? n	Direct IP-IP Early Media? n	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

Configure the **Trunk Group** form shown below for outgoing calls to Exchange UM. 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.

add trunk-group 10		Page 1 of 21	
TRUNK GROUP			
Group Number: 10	<b>Group Type: sip</b>	CDR Reports: y	
Group Name: To Sess Mgr	COR: 1	TN: 1	TAC: 1010
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
<b>Service Type: tie</b>	Auth Code? n		
		<b>Signaling Group: 10</b>	
		<b>Number of Members: 10</b>	

On **Page 3** of the trunk group form, set the **Numbering Format** field to *private*. This field specifies the format type of the calling party number sent to Exchange UM. The specific calling party number format is specified in the **Numbering- Private Format** form.

add trunk-group 10		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
<b>Numbering Format: private</b>			
		UUI Treatment: service-provider	
		Replace Restricted Numbers? n	
		Replace Unavailable Numbers? n	
Show ANSWERED BY on Display? y			

## 5.5. Configure SIP Trunk for Incoming Calls from Exchange UM

This signaling group is used for incoming calls from Exchange UM. A different signaling group is required because Exchange UM specifies a different domain in the SIP INVITE message than the one configured in the far-end domain name field of the Signaling Group form shown in **Section 5.4**. In the signaling group form, the **Far-end Domain** field may be left blank to match any domain in an incoming call request or set to the domain received in the SIP INVITE message from Exchange UM. In this configuration, Exchange UM specified `exch-a-919.cjcrvh-dom.extest.microsoft.com` as the domain. In this example, the field was set left blank. Follow the instructions described above for the other fields.

add signaling-group 11		Page 1 of 1
SIGNALING GROUP		
Group Number: 11	Group Type: sip	
	Transport Method: tcp	
IMS Enabled? n		
Near-end Node Name: 08A_CLAN	Far-end Node Name: sp-asm	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
<b>Far-end Domain:</b>		
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	
Enable Layer 3 Test? n	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 6	

Repeat the trunk group configuration in **Section 5.4** for the trunk group used for incoming calls from Exchange UM. The only difference would be to specify the signaling group configure above for this trunk group. All other fields may be entered as shown.

add trunk-group 11		Page 1 of 21
TRUNK GROUP		
Group Number: 11	Group Type: sip	CDR Reports: y
Group Name: From Sess Mgr	COR: 1	TN: 1 TAC: 1011
Direction: two-way	Outgoing Display? n	
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: tie	Auth Code? n	
<b>Signaling Group: 11</b>		
Number of Members: 10		

## 5.6. Configure Private Numbering

Configure the **Numbering – Private Format** form to send the calling party number to Exchange UM. Add an entry so that local stations with a 5-digit extension beginning with ‘2’ are sent to Exchange UM. This allows Exchange UM to provide the proper greeting on calls that cover to voicemail and to automatically recognize UM subscribers when retrieving messages. Since the **Trk Grp(s)** field is blank, this entry will apply for all outgoing trunk groups.

change private-numbering 0					Page 1 of 2	
NUMBERING - PRIVATE FORMAT						
Ext	Ext	Trk	Private	Total		
Len	Code	Grp(s)	Prefix	Len		
5	2			5	Total Administered: 1	
					Maximum Entries: 540	

## 5.7. Configure Voicemail Hunt Group

Configure a voicemail hunt group as shown below. Specify the voicemail pilot number in the **Group Extension** field. In this example, extension ‘29000’ is dialed by users to access Exchange UM.

add hunt-group 10		Page	1 of 60
HUNT GROUP			
Group Number: 10		ACD? n	
Group Name: Microsoft UM		Queue? n	
Group Extension: 29000		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:			

On **Page 2** of the hunt group, set the **Message Center** field to *sip-adjunct* since Exchange UM is accessed via SIP. Set the **Voice Mail Number** and the **Voice Mail Handle** fields to the digits used to route calls to Exchange UM (e.g., the same hunt group extension is used here) and set the **Routing Digits** field to the AAR access code. In this example, the AAR feature access code was used to route calls. The voice mail number is used by Communication Manager to route calls to Exchange UM.

add hunt-group 10			Page 2 of 60
HUNT GROUP			
Message Center: sip-adjunct			
Voice Mail Number	Voice Mail Handle	Routing Digits	
		(e.g., AAR/ARS Access Code)	
29000	29000	8	

## 5.8. Configure Coverage Path

Configure the coverage path for the voice mail hunt group, which is group *h10* in this sample configuration. The default values shown for **Busy**, **Don't Answer**, and **DND/SAC/Goto Cover** can be used for the *Coverage Criteria*.

add coverage path 10		Page 1 of 1	
COVERAGE PATH			
Coverage Path Number: 10			
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: h10	Rng:	Point2:	
Point3:		Point4:	
Point5:		Point6:	

## 5.9. Configure Station with Voicemail Coverage

When adding a station with voicemail coverage, configure the appropriate coverage path that points to the voicemail hunt group. The coverage path configured in **Section 5.8** was specified as shown below.

add station 20005		Page 1 of 5
STATION		
Extension: 20005	Lock Messages? n	BCC: 0
Type: 2420	Security Code:	TN: 1
Port: 01A0401	<b>Coverage Path 1: 10</b>	COR: 1
Name: DCP x20005	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 2	Time of Day Lock Table:	
Data Option: none	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 20005	
Display Language: english	Mute Button Enabled? y	
	Expansion Module? n	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Customizable Labels? y	

On **Page 2** of the station form, set the **MWI Served User Type** field to *sip-adjunct*.

add station 20005		Page 2 of 5
STATION		
FEATURE OPTIONS		
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?	
Service Link Mode: as-needed	EC500 State: enabled	
Multimedia Mode: enhanced	Display Client Redirection? n	
<b>MWI Served User Type: sip-adjunct</b>	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y		
Emergency Location Ext: 20005	Always Use? n IP Audio Hairpinning? n	

## 5.10. Configure the Locations Form

Use the command **change locations** command to configure the route pattern (**Proxy Sel Rte Pat**) used for outgoing calls to Exchange UM. In this configuration, route pattern '10' was used which routed calls over trunk group '10', the trunk group used for outgoing calls.

**Note:** When a call is made to Exchange UM, it initially responds with a "302 Temporarily Moved" SIP message, Communication Manager then uses the specified route pattern in the **Locations** form to place the call again using a different port requested by Exchange UM.

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

## 5.11. Configuring Call Routing

In this configuration, AAR was used to route calls to Exchange UM as specified on **Page 2** of the hunt group configured in **Section 5.7**. The UM pilot number is '29000' and those digits were used to route calls to Exchange UM whenever a call covers to voicemail or when a user dials Exchange UM directly. The UM auto attendant number is '29500' and is also routed to Exchange UM. For information in configuring AAR or ARS, refer to [2].



## 6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Locations that can be occupied by SIP Entities
- Adaptations to modify SIP messages as necessary
- SIP Entities corresponding to Session Manager, Communication Manager, and Exchange UM
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager, corresponding to the Avaya Aura™ Session Manager Server to be managed by Avaya Aura™ System Manager

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

### 6.1. Specify SIP Domain

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

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

Click **Commit**.

The screenshot displays the Avaya Aura™ System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the product name, and a user status message: "Welcome, admin Last Logged on at Oct. 13, 2010 2:42 PM". A "Help | Log off" link is also present. The main navigation menu on the left lists various management categories, with "Network Routing Policy" expanded to show "SIP Domains" as the selected option. The main content area is titled "Domain Management" and features a "Commit" and "Cancel" button. Below this, a table lists existing domains. One domain, "avaya.com", is shown with a "Type" of "sip" and a "Default" checkbox that is unchecked. A "Filter: Enable" link is visible to the right of the table. At the bottom of the form, a red asterisk indicates "Input Required", followed by another "Commit" and "Cancel" button.

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

## 6.2. Add Locations

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

Under *General*:

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

Under *Location Pattern*:

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

The screen below shows the addition of the *SP-BaskingRidge* location, where Communication Manager and Session Manager reside. Click **Commit** to save the Location definition.

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Oct. 13, 2010 2:42 PM [Help](#) | [Log off](#)

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](#)

1 Item | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 12.184.9.*	

Select : All, None ( 0 of 1 Selected )

\* **Input Required** [Commit](#) [Cancel](#)

**Shortcuts**

- [Change Password](#)
- [Help for Locations Details fields](#)
- [Help for Committing configuration changes](#)

The screen below shows the addition of the *Microsoft* location, where the Exchange UM servers reside. Click **Commit** to save the Location definition.

**AVAYA**

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Oct. 13, 2010 2:42 PM

[Help](#) | [Log off](#)

Home / Network Routing Policy / Locations / Location Details

▶ 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

Shortcuts

[Change Password](#)

[Help for Locations Details fields](#)

[Help for Committing configuration changes](#)

Location Details

Commit

Cancel

General

\* Name:

Microsoft

Notes:

ExUM 2010

Managed Bandwidth:

\* Average Bandwidth per Call:

80

Kbit/sec

\* Time to Live (secs):

3600

Location Pattern

Add

Remove

1 Item | Refresh

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 131.107.5.*	

Select : All, None ( 0 of 1 Selected )

\* Input Required

Commit

Cancel

## 6.3. Add Adaptations

Adaptations are used to modify SIP messages that are leaving Session Manager (egress adaptation) and that are entering Session Manager (ingress adaptation). One reason to use an adaptation is to convert strings containing calling and called party numbers from the local dial plan of a SIP entity to the dial plan administered on the Session Manager, and vice versa. Another reason would be to convert the domain in a SIP INVITE URI to an IP address. The **DigitConversionAdapter** installed on Session Manager is used for this purpose.

To add an Adaptation, select **Adaptations** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **Module name:** Specify the appropriate adaptation module.

Defaults can be used for the remaining fields. Click **Commit** to save each Adaptation definition.

The following adaptation will be used for calls routed from Exchange UM to Communication Manager.

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Oct. 13, 2010 2:42 PM [Help](#) | [Log off](#)

Home / Network Routing Policy / Adaptations / **Adaptation Details**

**Adaptation Details** [Commit](#) [Cancel](#)

**General**

\* **Adaptation name:**

**Module name:**

**Module parameter:**

**Egress URI Parameters:**

**Notes:**

**Digit Conversion for Incoming Calls to SM**

[Add](#) [Remove](#)

0 Items [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
--------------------------	------------------	-----	-----	---------------	---------------	-------------------	-------

**Digit Conversion for Outgoing Calls from SM**

[Add](#) [Remove](#)

0 Items [Refresh](#) Filter: [Enable](#)


<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
--------------------------	------------------	-----	-----	---------------	---------------	-------------------	-------

\* **Input Required** [Commit](#) [Cancel](#)

**Shortcuts**

- [Change Password](#)
- [Help for Adaptation Details fields](#)
- [Help for Committing configuration changes](#)

The following adaptation will be used for calls routed from Communication Manager to Exchange UM. This adaptation will allow the domain in the SIP URI of the INVITE message received from Communication Manager to be converted to the UM IP address specified in the **Module parameter** field.



Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Oct. 13, 2010 2:42 PM
[Help](#) | [Log off](#)

Home / Network Routing Policy / Adaptations / **Adaptation Details**

▶ 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

Shortcuts
Change Password
Help for Adaptation Details fields
Help for Committing configuration changes

Adaptation Details

Commit

Cancel

General

\* Adaptation name:

MSUM2010 Adapter

New module name:

DigitConversionAdapter

Module parameter:

131.107.5.62

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add

Remove

0 Items | Refresh
Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes

Digit Conversion for Outgoing Calls from SM

Add

Remove

0 Items | Refresh
Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes

\* Input Required

Commit

Cancel

## 6.4. Add SIP Entities

In the sample configuration, a SIP Entity is added for Session Manager, the C-LAN in the G650 Media Gateway, and Exchange UM.

### 6.4.1. Avaya Aura® Session Manager

A SIP Entity must be added for Session Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface on Session Manager.
- **Type:** Select *Session Manager*.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

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

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Oct. 13, 2010 2:42 PM [Help](#) | [Log off](#)

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

**SIP Entity Details** [Commit](#) [Cancel](#)

**General**

\* **Name:** SP-ASM

\* **FQDN or IP Address:** 12.184.9.144

**Type:** Session Manager

**Notes:**

**Location:** SP-BaskingRidge

**Outbound Proxy:**

**Time Zone:** America/New\_York

**Credential name:**

**SIP Link Monitoring**

**SIP Link Monitoring:** Use Session Manager Configuration

**Entity Links**

Entity Links can be modified after SIP Entity is committed.

**Port**

[Add](#) [Remove](#)

0 Items | [Refresh](#) Filter: [Enable](#)

	Port	Protocol	Default Domain	Notes
--	------	----------	----------------	-------

\* Input Required [Commit](#) [Cancel](#)

### 6.4.2. Avaya Aura® Communication Manager

A SIP Entity must be added for Communication Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface (e.g., C-LAN board) on the telephony system.
- **Type:** Select *CM*.
- **Adaptation :** Select *CM Adapter* configured in **Section 6.3**. *This adaptation is required for Exchange UM transfers.*
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

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

The screenshot displays the Avaya Aura™ System Manager 5.2 web interface. The top header includes the Avaya logo, the product name, and a user status bar showing 'Welcome, admin' and 'Last Logged on at Oct. 13, 2010 2:42 PM'. A navigation menu on the left lists various system management categories, with 'Network Routing Policy' expanded to show 'SIP Entities'. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. The configuration fields are as follows:

- Name:** SP-CommMgr
- FQDN or IP Address:** 12.184.9.135
- Type:** CM
- Notes:** (empty text field)
- Adaptation:** CM Adapter
- Location:** SP-BaskingRidge
- Time Zone:** America/New\_York
- Override Port & Transport with DNS SRV:** (unchecked checkbox)
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none
- SIP Link Monitoring:** Use Session Manager Configuration

At the bottom, there is a red warning message: '\* Input Required'. The interface also includes 'Commit' and 'Cancel' buttons at the top right and bottom right of the configuration area.

### 6.4.3. Microsoft Unified Messaging

A SIP Entity must be added for Exchange UM. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** UM IP address.
- **Type:** Select *Other*.
- **Adaptation :** Select *MSUM2010 Adapter* configured in **Section 6.3**.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

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

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Oct. 13, 2010 2:42 PM [Help](#) | [Log off](#)

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

**SIP Entity Details** [Commit](#) [Cancel](#)

**General**

\* **Name:** MSUM2010

\* **FQDN or IP Address:** 131.107.5.62

**Type:** Other

**Notes:**

**Adaptation:** MSUM2010 Adapter

**Location:** Microsoft

**Time Zone:** America/New\_York

**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

**Entity Links**

**Entity Links can be modified after SIP Entity is committed.**

\* **Input Required** [Commit](#) [Cancel](#)

**Navigation Menu:**

- 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

**Shortcuts**

- Change Password
- Help for SIP Entity Details fields
- Help for Committing configuration changes

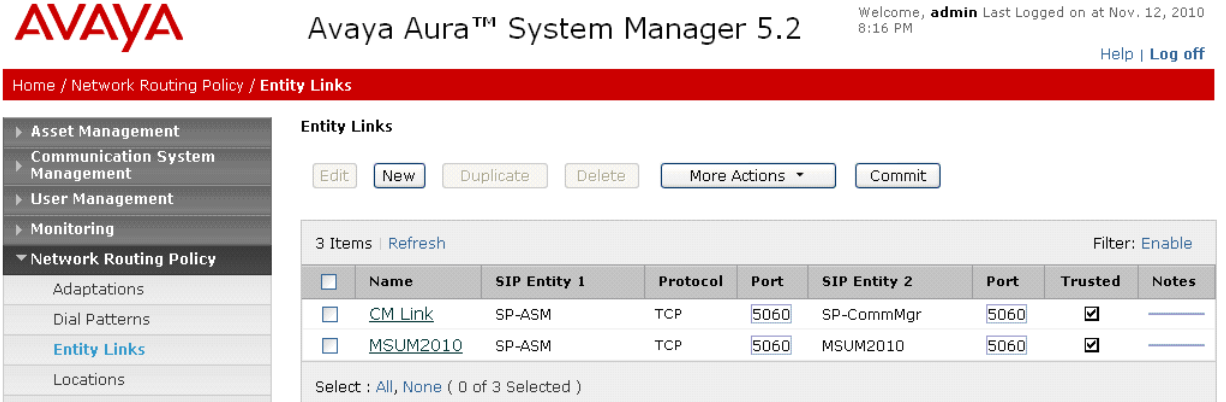


## 6.5. Add Entity Links

The SIP trunk from Session Manager to Communication Manager and Exchange UM are described by Entity Links. To add an Entity Link, select **Entity Links** on the left and click on the **New** button on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select *TCP* as the transport protocol.
- **Port:** Port number to which the other system sends SIP Requests (e.g., *5060* for TCP).
- **SIP Entity 2:** Select the name of Communication Manager or Exchange UM.
- **Port:** Port number on which the other system receives SIP requests (e.g., *5060* for TCP).
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.4** will be denied.*

The following screen displays two Entity Links after being configured per the instructions above. The first entity link is for Session Manager and Communication Manager and the second entity link is for Session Manager and Exchange UM.



The screenshot shows the Avaya Aura System Manager 5.2 interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura™ System Manager 5.2", and a user status bar indicating "Welcome, admin Last Logged on at Nov. 12, 2010 8:16 PM". The main content area is titled "Entity Links" and features a sidebar on the left with a tree view containing "Asset Management", "Communication System Management", "User Management", "Monitoring", and "Network Routing Policy". The "Entity Links" section is active, showing a table with 3 items. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. Two entity links are listed: "CM Link" and "MSUM2010". Both links are configured with SIP Entity 1 as "SP-ASM", Protocol as "TCP", and Port as "5060". The "CM Link" is associated with SIP Entity 2 "SP-CommMgr", and the "MSUM2010" is associated with SIP Entity 2 "MSUM2010". Both links are marked as "Trusted" (checked box). The "Notes" column contains a link icon for each entry. Below the table, there is a "Select" dropdown menu showing "All, None ( 0 of 3 Selected )".

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
<input type="checkbox"/>	<a href="#">CM Link</a>	SP-ASM	TCP	5060	SP-CommMgr	5060	<input checked="" type="checkbox"/>	<a href="#">Link</a>
<input type="checkbox"/>	<a href="#">MSUM2010</a>	SP-ASM	TCP	5060	MSUM2010	5060	<input checked="" type="checkbox"/>	<a href="#">Link</a>

Select : All, None ( 0 of 3 Selected )

## 6.6. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Three routing policies were added – one for Communication Manager, one for the UM Pilot Number, and one for the UM Auto Attendant. To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:

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

Under *Time of Day*:

Click **Add**, and select the time range configured in the previous section.

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

The screenshot displays the Avaya Aura System Manager 5.2 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura™ System Manager 5.2', and a user status message: 'Welcome, admin Last Logged on at Nov. 19, 2010 2:50 PM'. A red breadcrumb trail reads 'Home / Network Routing Policy / Routing Policies / Routing Policy Details'. On the left, a sidebar menu lists various management categories, with 'Network Routing Policy' expanded to show 'Routing Policies' as the selected option. The main content area is titled 'Routing Policy Details' and contains three sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. In the 'General' section, the 'Name' field is populated with 'ToCommMgr', and the 'Disabled' checkbox is unchecked. The 'SIP Entity as Destination' section features a 'Select' button and a table with one entry: 'SP-CommMgr' with FQDN '12.184.9.135' and Type 'CM'. The 'Time of Day' section includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. Below these is a table with one item, '24/7', which is selected. The table columns include 'Ranking', 'Name', days of the week (Mon-Sun), 'Start Time', 'End Time', and 'Notes'. The '24/7' entry shows all days selected and a time range from 00:00 to 23:59. At the bottom of the table, it states 'Select : All, None ( 0 of 1 Selected )'. 'Commit' and 'Cancel' buttons are located in the top right corner of the main content area.

Name	FQDN or IP Address	Type	Notes
SP-CommMgr	12.184.9.135	CM	

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

The following screen shows the Routing Policy for Exchange UM.

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Nov. 19, 2010 2:50 PM

Help | Log off

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

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

Shortcuts

Change Password

Routing Policy Details

CommitCancel

General

\* Name:

ToMSUM2010

Disabled:

☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
MSUM2010	131.107.5.62	Other	

Time of Day

AddRemoveView Gaps/Overlaps

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"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None ( 0 of 1 Selected )

## 6.7. Add Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the sample configuration, 5-digit extensions beginning with “2” reside on Communication Manager, extension “29000” is the UM pilot number and extension “29500” is the UM auto attendant. 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:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **SIP Domain** SIP domain of dial pattern.
- **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. The following screen shows the dial pattern definitions for local extensions on Communication Manager.

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Nov. 19, 2010 2:50 PM Help | Log off

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

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

**General**

\* Pattern: 2

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: avaya.com

Notes:

**Originating Locations and Routing Policies** [Add] [Remove]

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	ToCommMgr	0	<input type="checkbox"/>	SP-CommMgr	

Select : All, None ( 0 of 1 Selected )

The following screen shows the dial pattern definition for the UM pilot number.

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Nov. 19, 2010 2:50 PM [Help](#) | [Log off](#)

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

**Dial Pattern Details** Commit Cancel

**General**

\* Pattern: 29000

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: avaya.com

Notes: UM Pilot Number

**Originating Locations and Routing Policies**

Add Remove

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	ToMSUM2010	0	<input type="checkbox"/>	MSUM2010	

Select : All, None ( 0 of 1 Selected )

The following screen shows the dial pattern definition for the UM auto attendant.

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Nov. 19, 2010 2:50 PM [Help](#) | [Log off](#)

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

**Dial Pattern Details** Commit Cancel

**General**

\* Pattern: 29500

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: avaya.com

Notes: UM Auto Attendant

**Originating Locations and Routing Policies**

Add Remove

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	ToMSUM2010	0	<input type="checkbox"/>	MSUM2010	

Select : All, None ( 0 of 1 Selected )

## 6.8. Add Session Manager

To complete the configuration, add the Session Manager to provide the linkage between Avaya Aura™ System Manager and Avaya Aura™ Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Click **Add** (not shown), and fill in the fields as described below and shown in the following screen:

Under *Identity*:

- **SIP Entity Name:** Select the name of the SIP Entity added for Session Manager.
- **Description:** Descriptive comment (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

Under *Security Module*:

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager.

Accept default values for the remaining fields. Click **Commit** to add this Session Manager.

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Oct. 13, 2010 2:42 PM [Help Log off](#)

Home / Session Manager / Session Manager Administration / New Session Manager

**Add Session Manager** [Commit](#) [Cancel](#)

[General](#) | [Security Module](#) | [Monitoring](#) | [CDR](#) | [Personal Profile Manager \(PPM\)](#) - [Connection Settings](#) | [Event Server](#) | [Expand All](#) | [Collapse All](#)

**General**

\*SIP Entity Name

Description

\*Management Access Point Host Name/IP

\*Direct Routing to Endpoints

**Security Module**

SIP Entity IP Address

\*Network Mask

\*Default Gateway

\*Call Control PHB

\*QOS Priority

\*Speed & Duplex

VLAN ID

## 6.9. Configuring a Backup Exchange UM Server

This section covers the additional configuration in Session Manager required to support a backup Exchange UM server. The configuration steps are similar to adding the primary Exchange UM server configured in **Section 6**.

1. Add another **Adaptation** that specifies the IP address of the backup Exchange UM server in the **Module parameter** field. See the **MSUM2010 Adapter** in **Section 6.3**.
2. Add a **SIP Entity** for the backup Exchange UM server. Follow the instructions for configuring the **MSUM2010** SIP Entity in **Section 6.4.3**, except that the IP address would be different and the **Adaptation** configured in the step above would be assigned.
3. Configure an **Entity Link** between Session Manager and the backup Exchange UM server.
4. Configure **Routing Policy** for the backup Exchange UM server.
5. For the **Dial Pattern** associated with the UM pilot number (e.g., 29000), configured in **Section 6.7**, specify two SIP entities, the primary Exchange UM server and the backup Exchange UM server. The backup Exchange UM server should have a lower rank (i.e., higher number) than the primary Exchange UM server so that calls are only routed to the backup server if the primary Exchange UM server fails. If the rank were the same, the Exchange UM calls would be equally distributed between both servers. Below is a sample **Dial Pattern** configuration.

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Nov. 19, 2010 2:50 PM [Help](#) | [Log off](#)

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

**Dial Pattern Details** [Commit](#) [Cancel](#)

**General**

\* **Pattern:**

\* **Min:**

\* **Max:**

**Emergency Call:** ☐

**SIP Domain:**

**Notes:**

**Originating Locations and Routing Policies**

[Add](#) [Remove](#)

2 Items | [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	<a href="#">ToMSUM2010</a>	0	<input type="checkbox"/>	MSUM2010	
<input type="checkbox"/>	-ALL-	Any Locations	<a href="#">ToMSUMBackup</a>	1	<input type="checkbox"/>	MSUM-Backup	

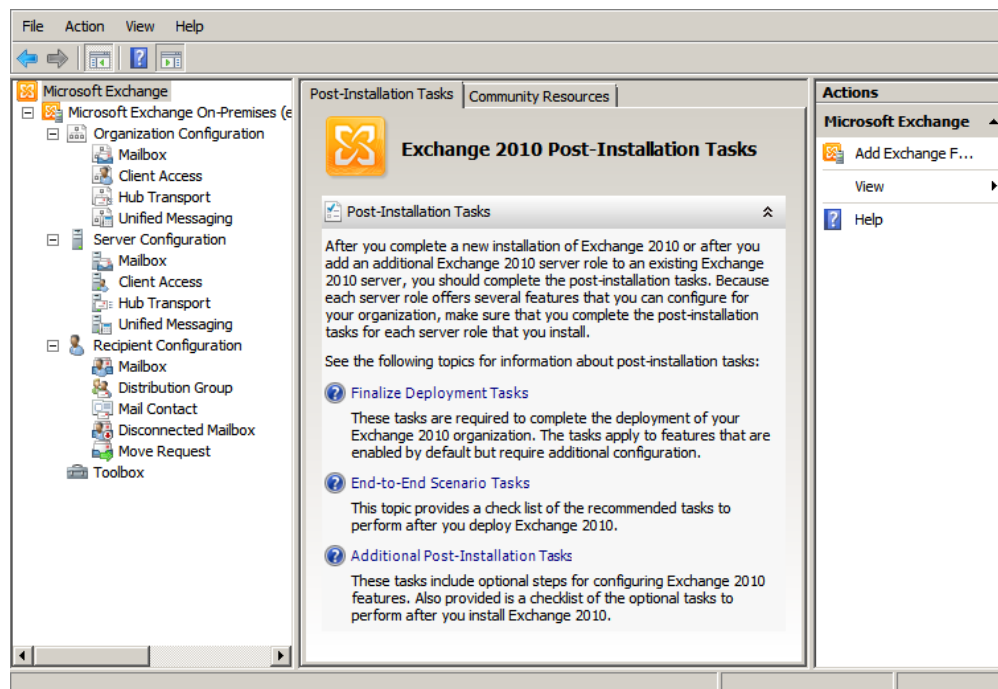
Select : All, None ( 0 of 2 Selected )

[Shortcuts](#)

## 7. Configure Microsoft Exchange Server 2010 Unified Messaging

This section covers the configuration of Exchange UM using the Exchange Management Console. The following screen illustrates the main page of the Exchange Management Console. The steps required include:

- Creating a UM Dial Plan
- Creating a UM IP Gateway
- Creating a UM Hunt Group
- Assign the UM Dial Plan to a Exchange UM Server and a UM IP Gateway
- Creating a User Mailbox
- Enabling a User for Exchange UM





## 7.1. Create a UM Dial Plan

A UM dial plan establishes a link from the telephone extension number of an Exchange 2010 recipient in Active Directory to a UM-enabled mailbox. In the console tree of Exchange Management Console, expand the Organization Configuration node and click on **Unified Messaging**. In the action pane, select **New UM Dial Plan...** to display the following window and create a dial plan. Enter a descriptive name and specify the **Number of digits in extension numbers**. In this configuration, a 5-digit dial plan was used. Configure the other fields as shown below. Click **Next** to display the **Completion** screen.

**New UM Dial Plan**

☒ Introduction  
☐ Set UM Servers  
☐ New UM Dial Plan  
☐ Completion

**Introduction**  
This wizard helps you create a UM dial plan for use by Microsoft Exchange Unified Messaging. A dial plan is a grouping of unique telephone extension numbers.

Name:  
CM-SM-5-Digit

Number of digits in extension numbers:  
5

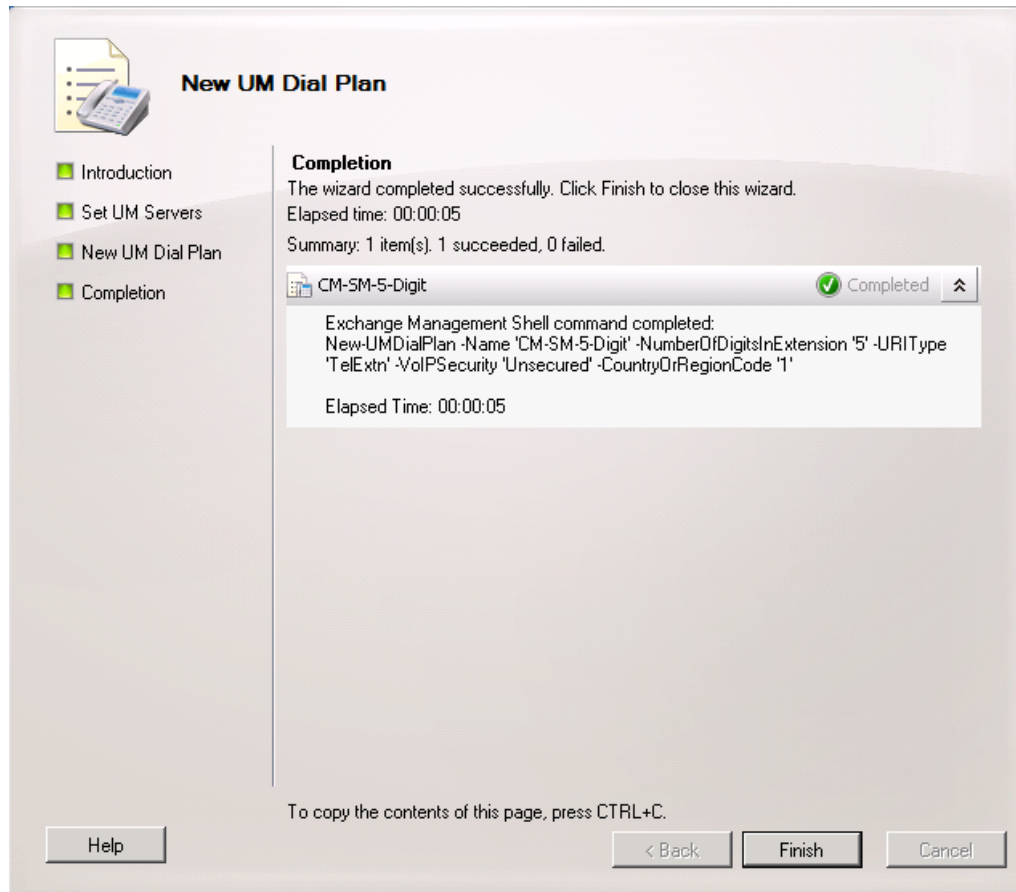
URI type:  
Telephone Extension

VoIP security:  
Unsecured

Country/Region code:  
1

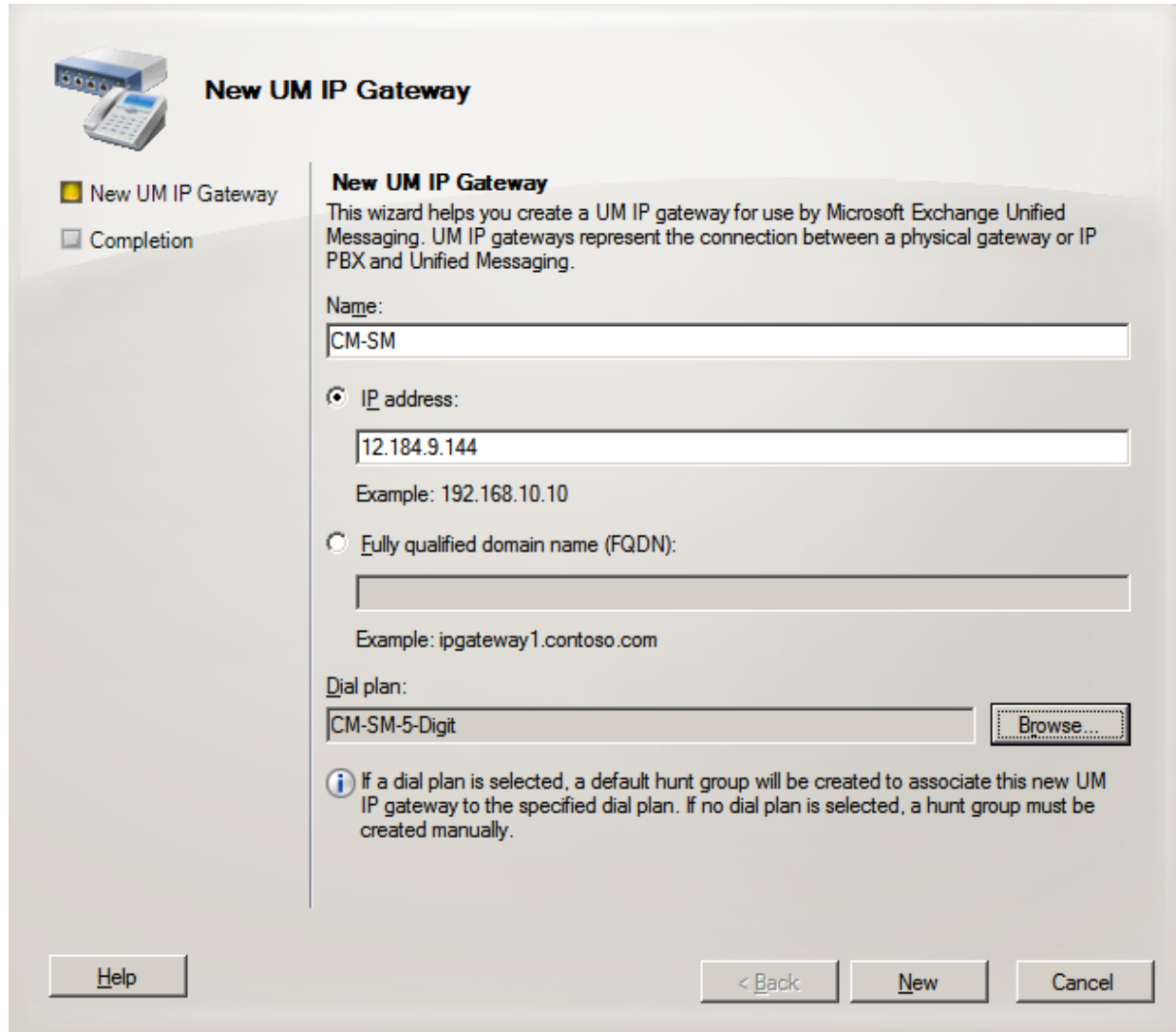
Help      < Back      Next >      Cancel

On the **Completion** screen, click the **Finish** button to submit the new UM dial plan.



## 7.2. Create a UM IP Gateway

Session Manager will serve as the IP gateway used by Exchange UM to connect to the telephony network through SIP. In the console tree of Exchange Management Console, expand the Organization Configuration node and click on **Unified Messaging**. In the action pane, select **New UM IP Gateway...** to display the following window and create an IP gateway. Enter a descriptive name and specify the **IP Address** or **Fully qualified domain name (FQDN)** of Session Manager. Click **New** to submit the IP gateway.



The screenshot shows the 'New UM IP Gateway' wizard. On the left, there is a navigation pane with two steps: 'New UM IP Gateway' (selected) and 'Completion'. The main area is titled 'New UM IP Gateway' and contains the following fields and options:

- Name:** A text box containing 'CM-SM'.
- IP address:** A radio button is selected, with a text box containing '12.184.9.144'. Below it is an example: 'Example: 192.168.10.10'.
- Fully qualified domain name (FQDN):** A radio button is unselected, with an empty text box below it. Below that is an example: 'Example: ipgateway1.contoso.com'.
- Dial plan:** A text box containing 'CM-SM-5-Digit' and a 'Browse...' button.
- Information:** A blue 'i' icon followed by the text: 'If a dial plan is selected, a default hunt group will be created to associate this new UM IP gateway to the specified dial plan. If no dial plan is selected, a hunt group must be created manually.'

At the bottom, there are three buttons: 'Help', '< Back', and 'New' (highlighted), and a 'Cancel' button.

### 7.3. Create the UM Hunt Group

After creating the UM IP Gateway, create a new UM hunt group and then associate the UM hunt group with the UM IP gateway. A UM hunt group provides the communication link between the UM IP gateway and the UM dial plan. In the console tree of Exchange Management Console, expand the Organization Configuration node and click on **Unified Messaging** and then click on the UM IP Gateways tab. Select the UM IP gateway created in **Section 7.2** and then click on **New UM hunt Group...** in the action pane. The window below is displayed. The UM hunt group will already be associated with the UM IP gateway. Next, specify a descriptive **Name** and associate the UM dial plan configured in **Section 7.1** by clicking the **Browse** button. Lastly, assign the **Pilot identifier** for this UM hunt group and then click **New** to submit the configuration. Extension 29000 was assigned to this UM hunt group.

**New UM Hunt Group**

☒ New UM Hunt Group  
☐ Completion

**New UM Hunt Group**  
This wizard helps you create a UM hunt group for use by Microsoft Exchange Unified Messaging. A hunt group represents a connection between a UM IP gateway and a UM dial plan, and associates the dial plan with the pilot identifier specified below.

Associated UM IP gateway:  
CM-SM

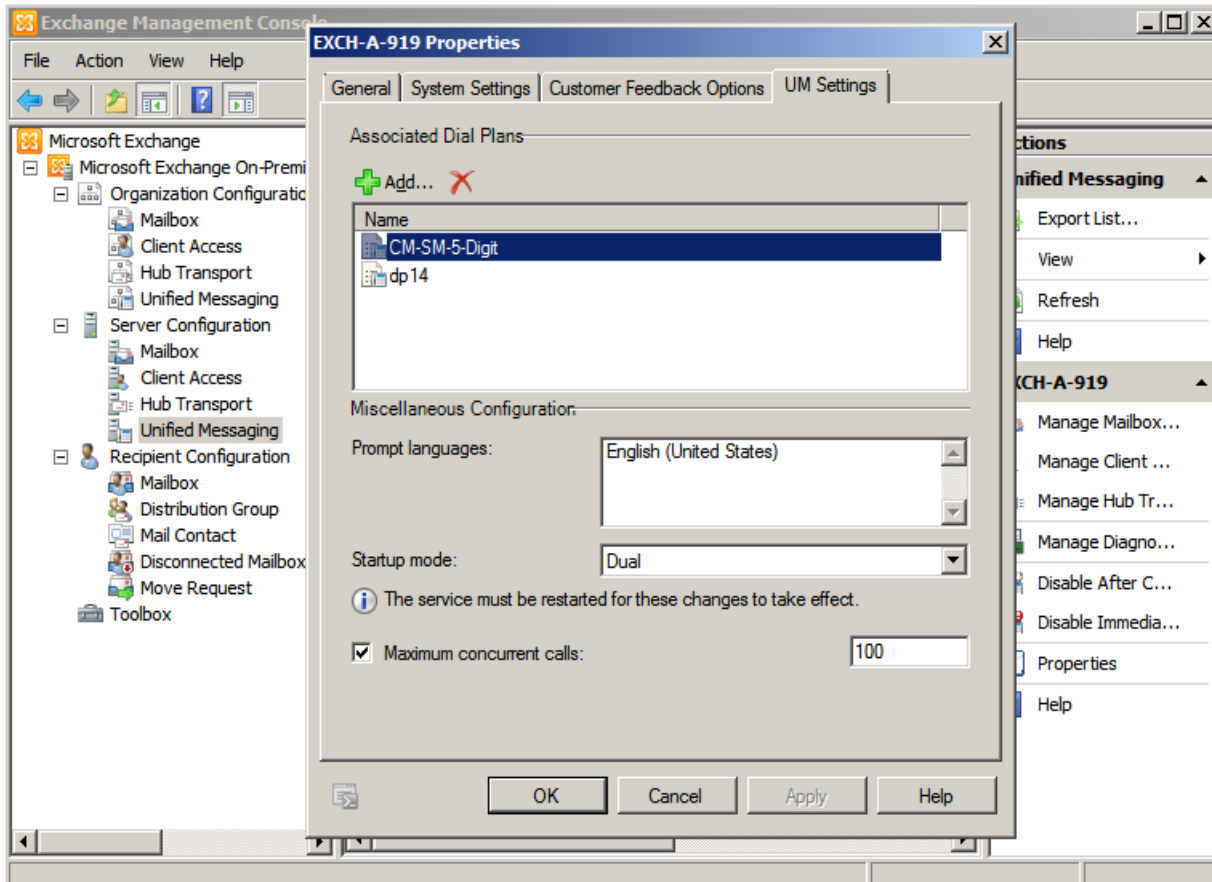
Name:  
UM Hunt Group

Dial plan:  
CM-SM-5-Digit

Pilot identifier:  
29000

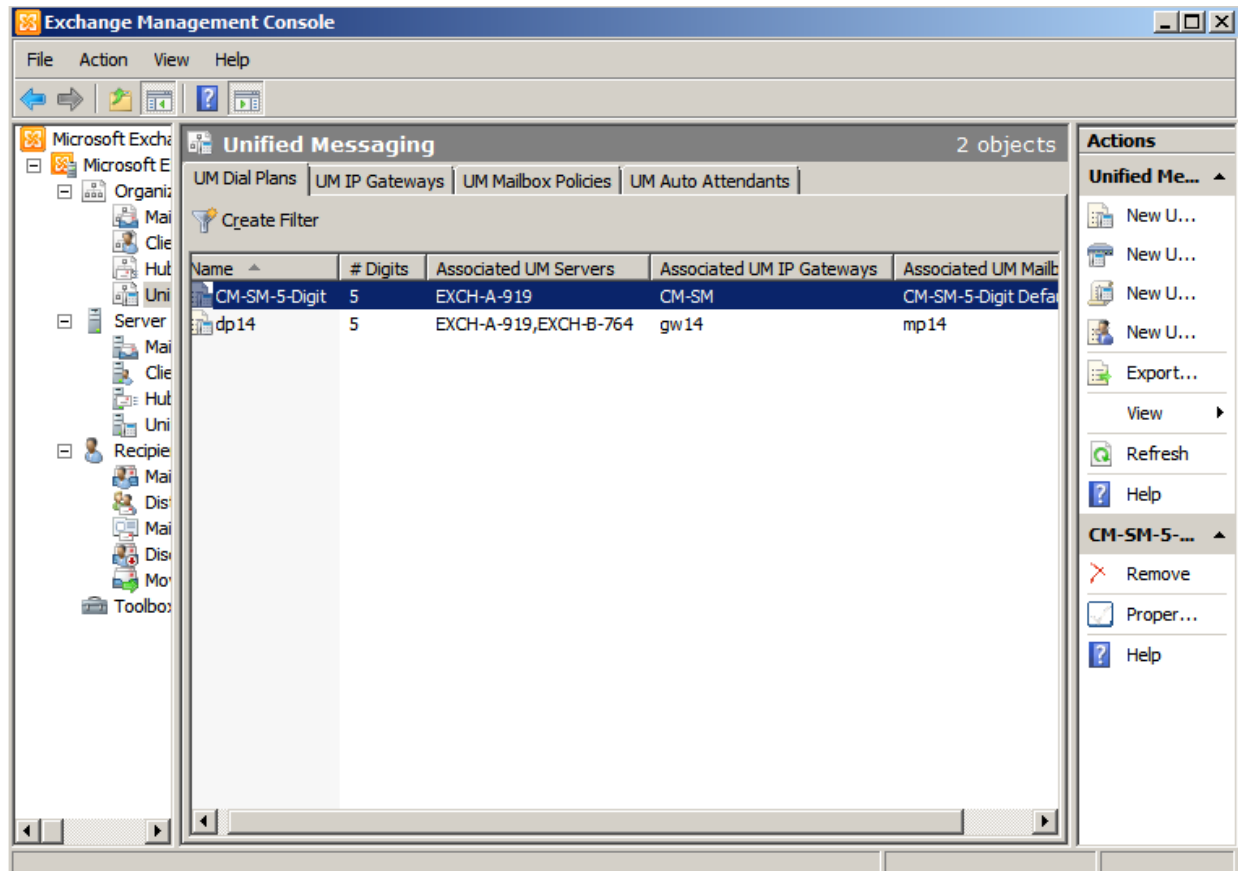
## 7.4. Assign UM Dial Plan to Exchange UM Server

In the console tree of Exchange Management Console, expand the Server Configuration node and click on **Unified Messaging**. In the work pane, double-click on the Exchange UM Server and select the **UM Settings** tab in the window below. Assign the UM dial plan configured in **Section 7.1** with the Exchange UM server, and then click **OK**.



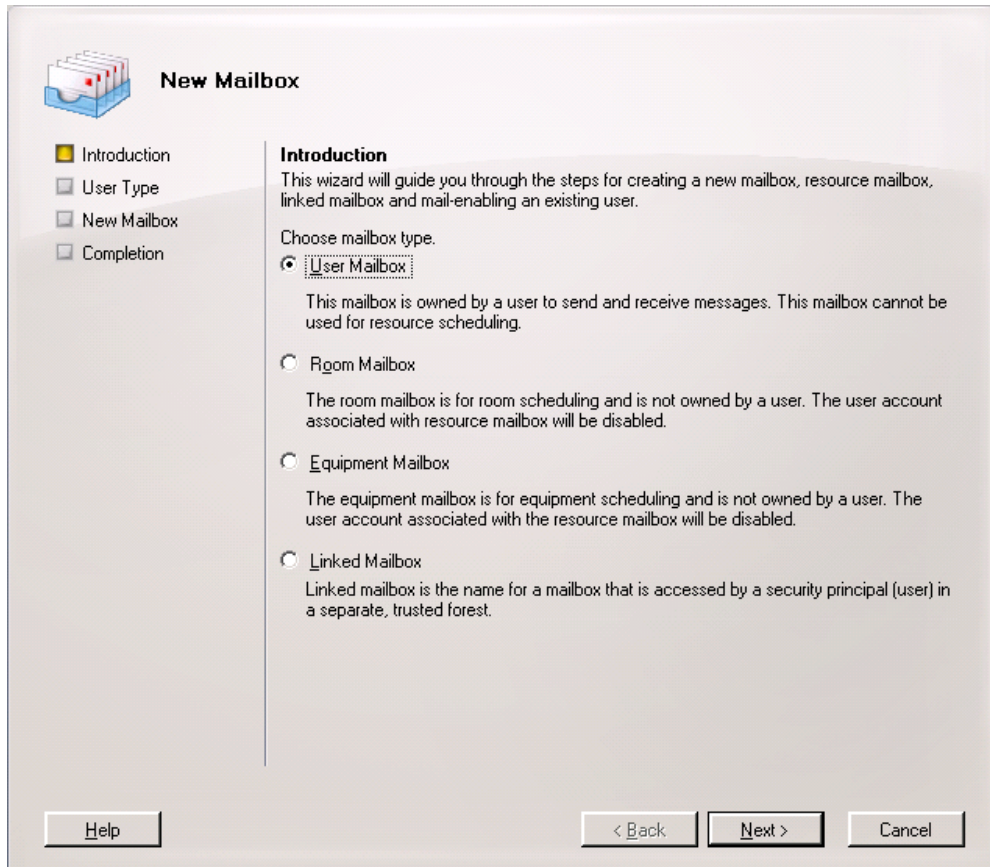
Next, verify the associated UM dial plan and UM IP gateway. Click on **Unified Messaging** under the Organization Configuration node. The window shown below is displayed. Verify that the UM dial plan is associated with the appropriate Exchange UM server and UM IP gateway configured in the steps above.

**Note:** Click on **Refresh** in the action pane to update the window if necessary.



## 7.5. Create New Mailbox

In the Exchange Management Console, click **Recipient Configuration**. In the action pane, click **New Mailbox** to display the New Mailbox wizard. On the **Introduction** page shown below, select **User Mailbox**, and then click **Next**.



The image shows the 'New Mailbox' wizard in the Exchange Management Console. The title bar says 'New Mailbox'. On the left, there is a list of steps: 'Introduction' (selected with a yellow square), 'User Type' (disabled with a grey square), 'New Mailbox' (disabled with a grey square), and 'Completion' (disabled with a grey square). The main area is titled 'Introduction' and contains the following text: 'This wizard will guide you through the steps for creating a new mailbox, resource mailbox, linked mailbox and mail-enabling an existing user.' Below this, it says 'Choose mailbox type.' and lists four options with radio buttons: 'User Mailbox' (selected), 'Room Mailbox', 'Equipment Mailbox', and 'Linked Mailbox'. Each option has a brief description. At the bottom, there are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button.

**New Mailbox**

☒ Introduction  
☐ User Type  
☐ New Mailbox  
☐ Completion

**Introduction**  
This wizard will guide you through the steps for creating a new mailbox, resource mailbox, linked mailbox and mail-enabling an existing user.

Choose mailbox type.

☒ **User Mailbox**  
This mailbox is owned by a user to send and receive messages. This mailbox cannot be used for resource scheduling.

☐ **Room Mailbox**  
The room mailbox is for room scheduling and is not owned by a user. The user account associated with resource mailbox will be disabled.

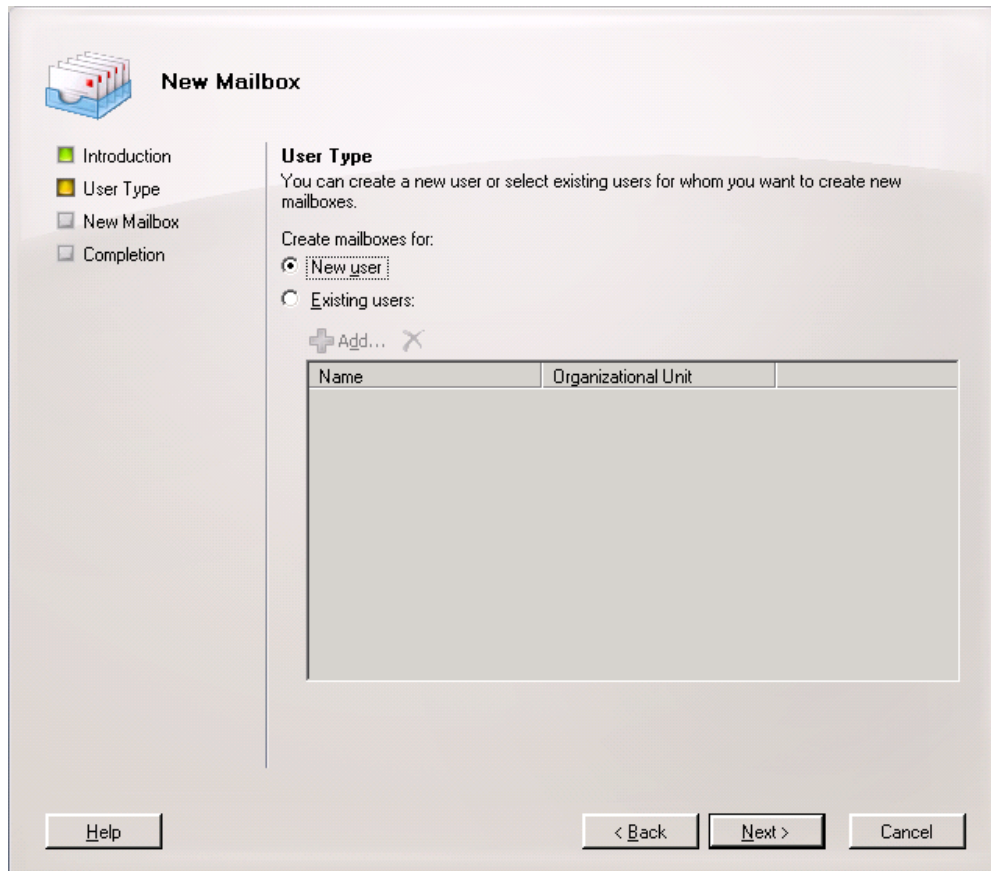
☐ **Equipment Mailbox**  
The equipment mailbox is for equipment scheduling and is not owned by a user. The user account associated with the resource mailbox will be disabled.

☐ **Linked Mailbox**  
Linked mailbox is the name for a mailbox that is accessed by a security principal (user) in a separate, trusted forest.

[Help](#) [< Back](#) [Next >](#) [Cancel](#)



On the **New Mailbox** page, select **New User**, and then click **Next**.



The screenshot shows a 'New Mailbox' wizard window. On the left is a navigation pane with four steps: 'Introduction' (green square), 'User Type' (yellow square), 'New Mailbox' (grey square), and 'Completion' (grey square). The 'New Mailbox' step is currently selected. The main area is titled 'User Type' and contains the text: 'You can create a new user or select existing users for whom you want to create new mailboxes.' Below this, it says 'Create mailboxes for:' followed by two radio buttons. The first radio button, labeled 'New user', is selected. The second radio button is labeled 'Existing users:'. Below the radio buttons is a button with a plus icon and the text 'Add...'. At the bottom of the main area is a table with two columns: 'Name' and 'Organizational Unit'. The table is currently empty. At the bottom of the window are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button to the right of 'Next >'.

**New Mailbox**

Introduction  
User Type  
New Mailbox  
Completion

**User Type**  
You can create a new user or select existing users for whom you want to create new mailboxes.  
Create mailboxes for:  
☒ New user  
☐ Existing users:  
+ Add... X

Name	Organizational Unit
------	---------------------

Help < Back Next > Cancel



On the **User Information** page, enter the user name and account information as shown below, and then click **Next**.

**New Mailbox**

☒ Introduction  
☒ User Type  
☒ **User Information**  
☐ Mailbox Settings  
☐ Archive Settings  
☐ New Mailbox  
☐ Completion

**User Information**  
Enter the user name and account information.

☐ Specify the organizational unit rather than using a default one:

First name:  Initials:  Last name:

Name:

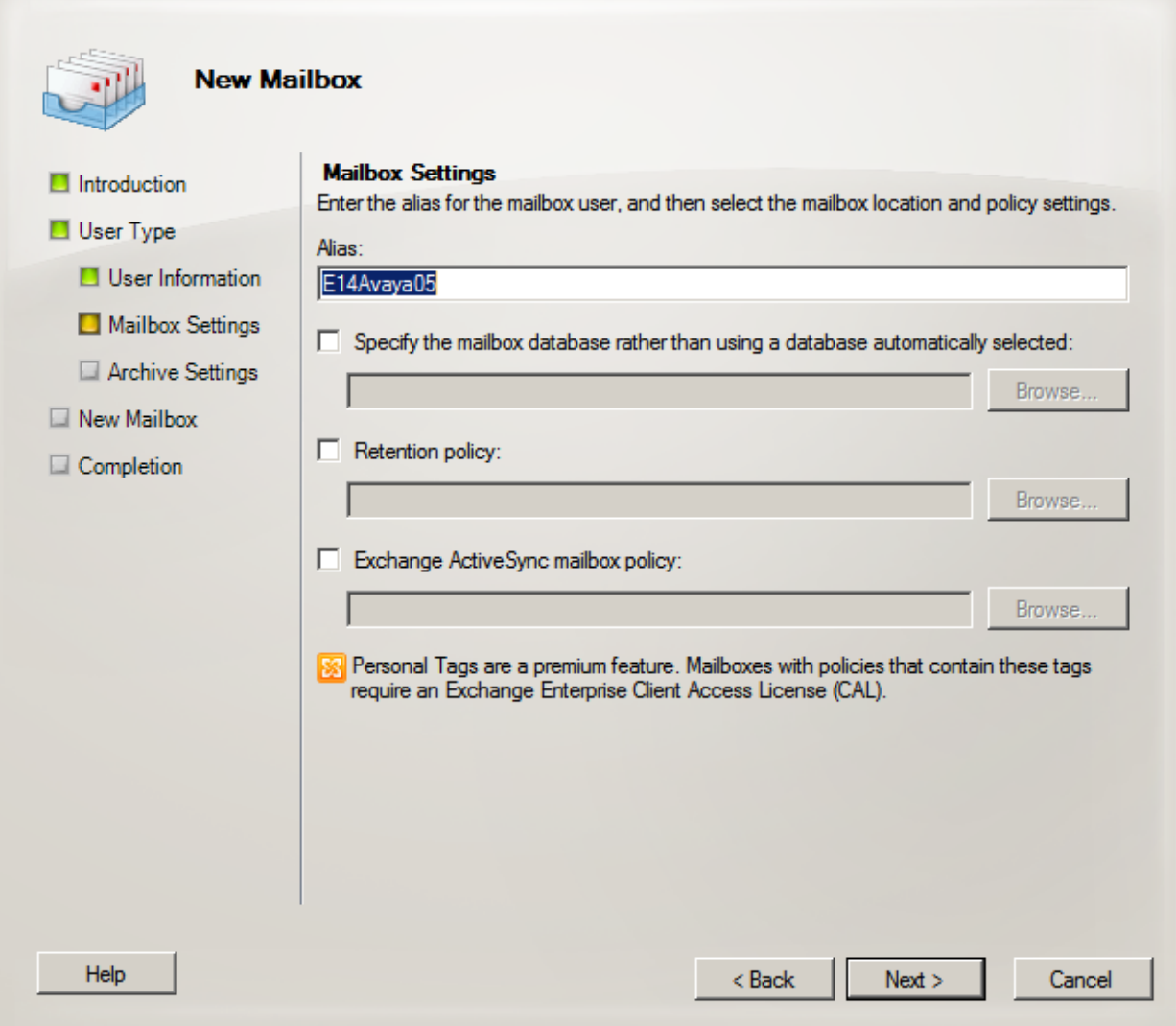
User logon name (User Principal Name):

User logon name (pre-Windows 2000):

Password:  Confirm password:

☐ User must change password at next logon

On the **Mailbox Settings** page, complete the **Alias** field, and then click **Next**. Review the **Configuration Summary**, and then click **New** to create the new mailbox. On the **Completion** page, click **Finish**.



The screenshot shows the 'New Mailbox' wizard in a web-based interface. On the left is a navigation pane with a tree view containing the following items: 'Introduction' (green square), 'User Type' (green square), 'User Information' (green square), 'Mailbox Settings' (yellow square), 'Archive Settings' (grey square), 'New Mailbox' (grey square), and 'Completion' (grey square). The main content area is titled 'New Mailbox' and 'Mailbox Settings'. Below the title, it says 'Enter the alias for the mailbox user, and then select the mailbox location and policy settings.' The 'Alias:' label is followed by a text input field containing 'E14Avaya05'. Below this are three optional settings, each with a checkbox and a 'Browse...' button: 'Specify the mailbox database rather than using a database automatically selected:', 'Retention policy:', and 'Exchange ActiveSync mailbox policy:'. At the bottom of the main area is a note with an orange icon: 'Personal Tags are a premium feature. Mailboxes with policies that contain these tags require an Exchange Enterprise Client Access License (CAL)'. At the bottom of the wizard are four buttons: 'Help', '< Back', 'Next >', and 'Cancel'.

**New Mailbox**


**Mailbox Settings**  
Enter the alias for the mailbox user, and then select the mailbox location and policy settings.

Alias:


☐ Specify the mailbox database rather than using a database automatically selected:

☐ Retention policy:

☐ Exchange ActiveSync mailbox policy:

 Personal Tags are a premium feature. Mailboxes with policies that contain these tags require an Exchange Enterprise Client Access License (CAL).

Enable Unified Messaging for the user. In the console tree of the Exchange Management Console, expand Recipient Configuration. In the result pane, select the user mailbox that will be enabled for Exchange UM. In the action pane, click **Enable Unified Messaging**. The **Enable Unified Messaging** wizard is displayed as shown below. Click the **Browse** button to select the **Unified Messaging Mailbox Policy** and specify a PIN for the user. Click **Next**.

 **Enable Unified Messaging**


☒ Introduction  
☐ Extension Configuration  
☐ Enable Unified Messaging  
☐ Completion

**Introduction**  
The selected mailbox will be enabled for Unified Messaging. Upon completion, an e-mail message will be sent to the mailbox notifying the user that they have been enabled for Unified Messaging. The message will include the PIN and the number to dial to gain access to their mailbox. By default, an extension number and PIN are automatically generated. You can also manually specify an extension number and PIN.

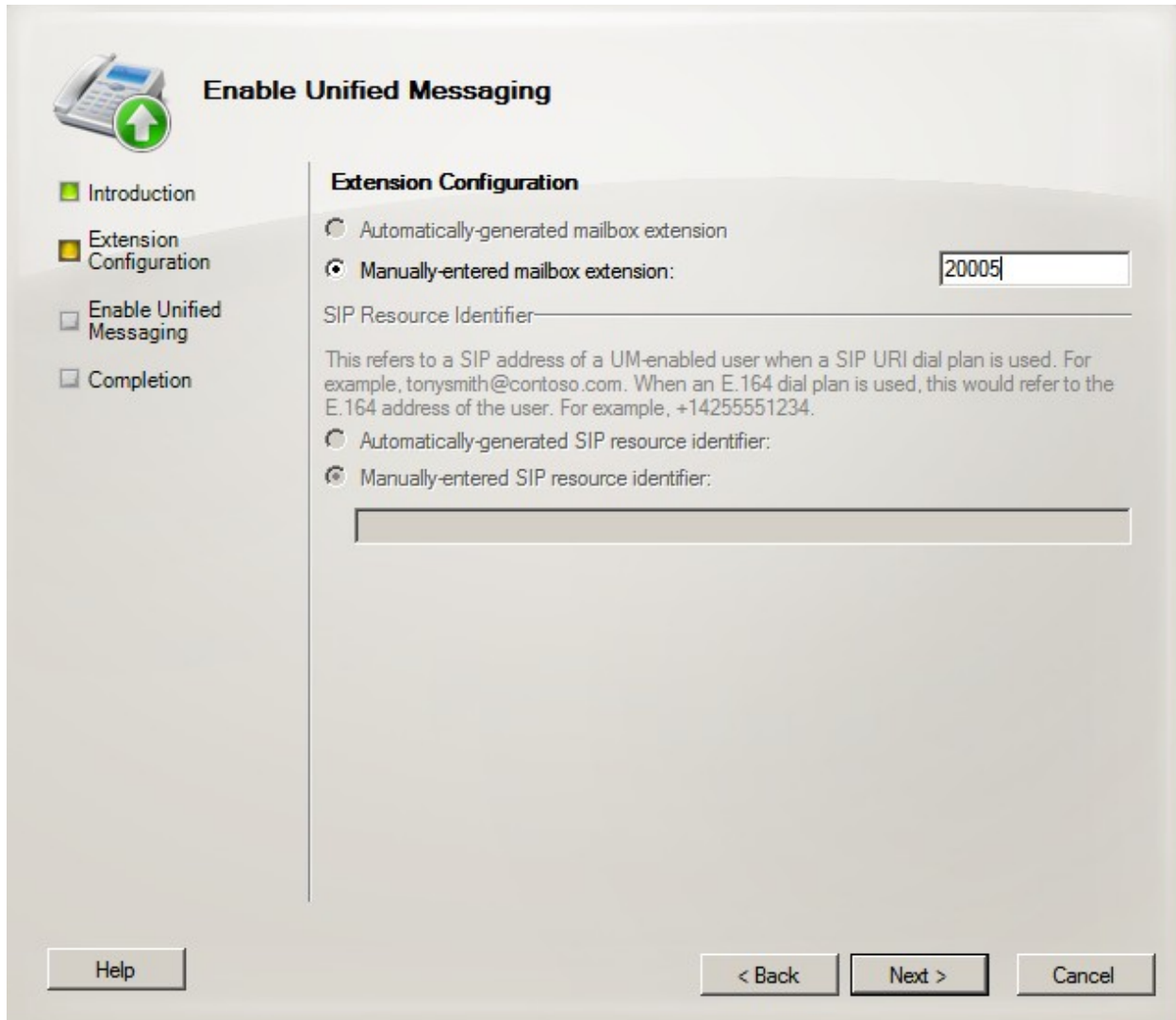
Unified Messaging Mailbox Policy:

PIN Settings

☐ Automatically generate PIN to access Outlook Voice Access  
☒ Manually specify PIN:   
☐ Require user to reset PIN at first telephone logon

 Unified Messaging is a premium feature and requires an Exchange Enterprise Client Access License (CAL) to enable it for the mailbox.

On the **Extension Configuration** page, specify the mailbox extension and then click **Next**. On the next page, click **Enable**. And finally, on the **Completion** page, click **Finish**.



The image shows a screenshot of the 'Enable Unified Messaging' wizard, specifically the 'Extension Configuration' step. The wizard has a sidebar on the left with four steps: 'Introduction' (green square), 'Extension Configuration' (yellow square), 'Enable Unified Messaging' (grey square), and 'Completion' (grey square). The main area is titled 'Extension Configuration' and contains two radio button options. The first option, 'Automatically-generated mailbox extension', is unselected. The second option, 'Manually-entered mailbox extension:', is selected, and a text box next to it contains the value '20005'. Below this, there is a section for 'SIP Resource Identifier' with a descriptive paragraph and two more radio button options. The first option, 'Automatically-generated SIP resource identifier:', is unselected. The second option, 'Manually-entered SIP resource identifier:', is selected, and a text box next to it is empty. At the bottom of the wizard, there are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button on the far right.

**Enable Unified Messaging**

Introduction  
Extension Configuration  
Enable Unified Messaging  
Completion

**Extension Configuration**

☐ Automatically-generated mailbox extension

☒ Manually-entered mailbox extension:

SIP Resource Identifier

This refers to a SIP address of a UM-enabled user when a SIP URI dial plan is used. For example, tonysmith@contoso.com. When an E.164 dial plan is used, this would refer to the E.164 address of the user. For example, +14255551234.

☐ Automatically-generated SIP resource identifier:

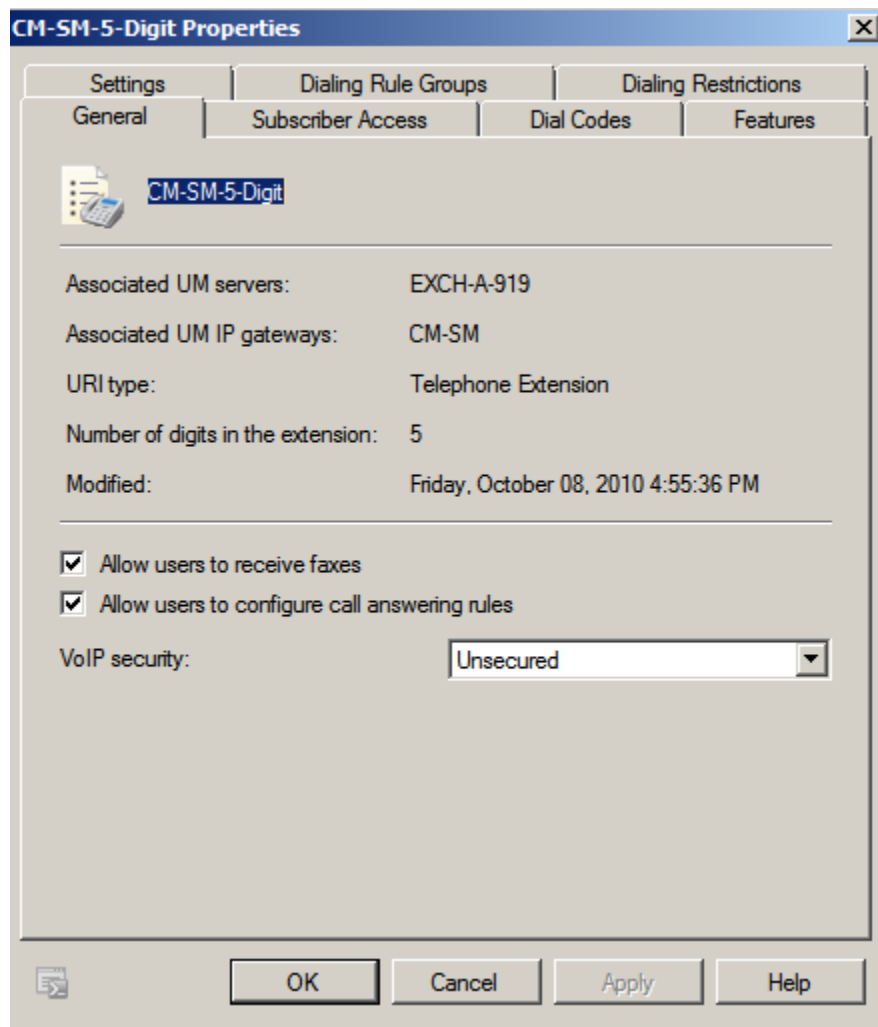
☒ Manually-entered SIP resource identifier:

Help < Back Next > Cancel

## 7.6. Enable Fax T.38 Support

This section covers the steps to enable Fax support on Exchange UM.

First, verify that the UM dial plan allows users to receive faxes. The **Allow users to receive faxes** checkbox must be enabled in the **General** tab of the UM dial plan properties window. By default, this field is enabled.



Next, enable Fax T.38 Support for the UM subscriber. In the console tree of Exchange Management Console, expand the Organization Configuration node and click on **Unified Messaging** and select the **UM Mailbox Policies** tab. Open the UM mailbox default policy object for the corresponding dial plan. The screen below is displayed. Verify that the UM mailbox allows receiving faxes. The **Allow users to receive faxes** checkbox must be enabled in the UM properties of the UM mailbox. By default, this field is enabled. Also, specify the partner fax server URI in the appropriate field.

**Note:** Unlike Exchange 2007 UM, Exchange 2010 UM requires an external fax server, which wasn't available during testing. The T.38 negotiation would have been between Communication Manager and a 3<sup>rd</sup> party fax server. The scope of Fax T.38 testing was to verify that Exchange UM returns the correct URL of the external fax server in the REFER message when it detects a fax tone.

**CM-SM-5-Digit Default Policy Properties**

General | Message Text | PIN Policies | Dialing Restrictions | Protected Voice Mail

CM-SM-5-Digit Default Policy

Associated UM dial plan: CM-SM-5-Digit

Modified: Friday, October 08, 2010 4:55:37 PM

Maximum greeting duration (minutes): 5

☒ Allow missed call notifications

☒ Allow Message Waiting Indicator

☒ Allow inbound faxes

Partner fax server URI:

(Examples: sip.fax3.eng.contoso.com:5060;transport=tcp, sip.rfx.it.litware.com:5061;transport=tls)

☒ Allow Voice Mail Preview

☒ Allow Outlook Voice Access

☒ Allow Play on Phone

☒ Allow users to configure call answering rules

OK Cancel Apply Help

## 7.7. Enable MWI for UM Subscriber

In the screen displayed above for the UM mailbox policy object for the dial plan, verify that MWI is enabled for the UM mailbox. The **Allow Message Waiting Indicator** checkbox must be enabled.

**CM-SM-5-Digit Default Policy Properties**

General | Message Text | PIN Policies | Dialing Restrictions | Protected Voice Mail

CM-SM-5-Digit Default Policy

Associated UM dial plan: CM-SM-5-Digit

Modified: Friday, October 08, 2010 4:55:37 PM

Maximum greeting duration (minutes): 5

☒ Allow missed call notifications

☒ Allow Message Waiting Indicator

☒ Allow inbound faxes

Partner fax server URI:

(Examples: sip.fax3.eng.contoso.com:5060;transport=tcp,  
sip.rfx.it.litware.com:5061;transport=tls)

☒ Allow Voice Mail Preview

☒ Allow Outlook Voice Access

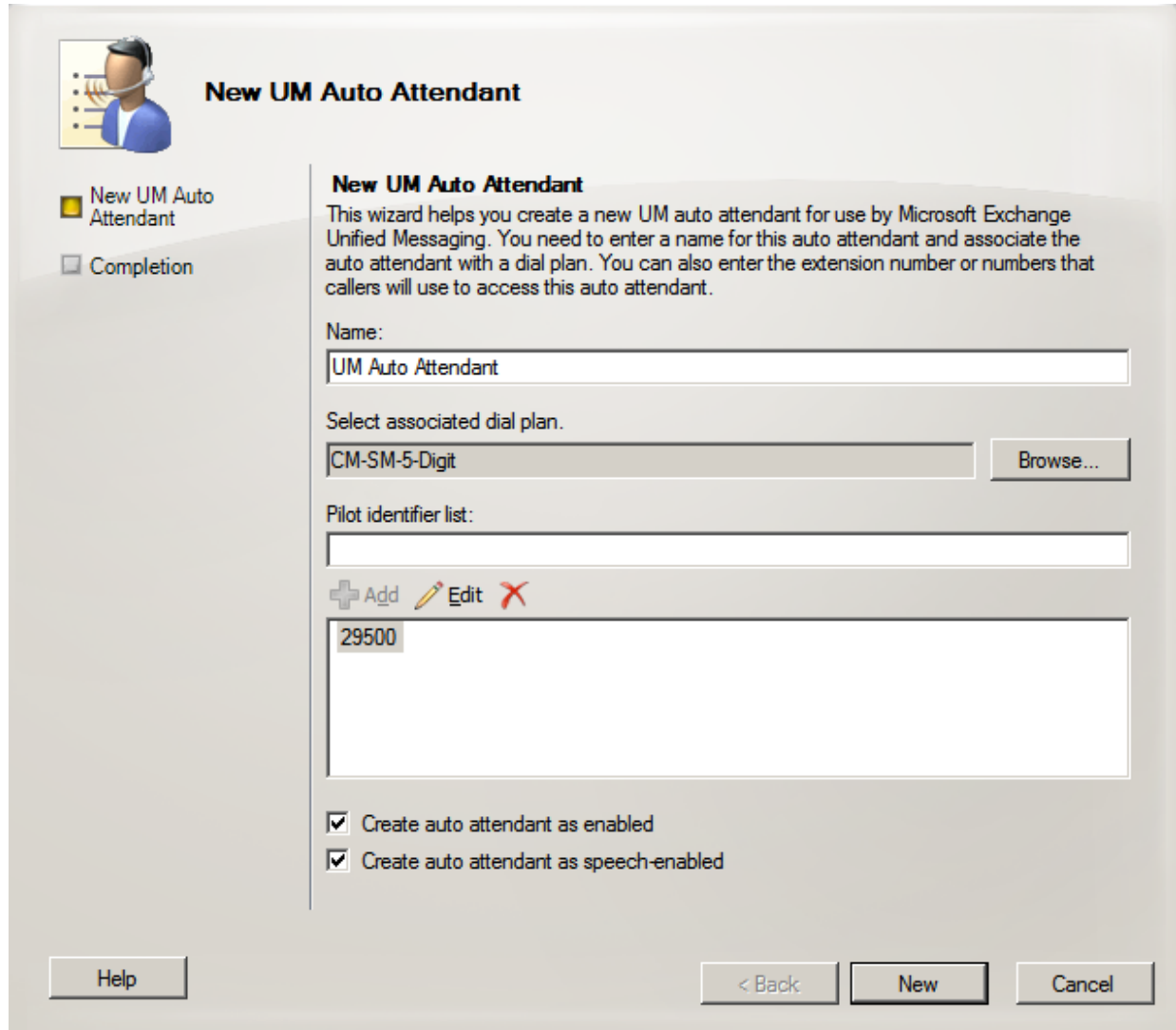
☒ Allow Play on Phone

☒ Allow users to configure call answering rules

OK Cancel Apply Help

## 7.8. Add Auto Attendant

In the console tree of Exchange Management Console, expand the Organization Configuration node and click on **Unified Messaging**. In the action pane, select **New Auto Attendant...** to display the following window and create an auto attendant. Enter a descriptive name and set the dial plan. In the **Pilot identifier list** field, specify the extension of the auto attendant. Click **New** to submit the auto attendant.



The screenshot shows the 'New UM Auto Attendant' wizard. On the left, there is a navigation pane with two steps: 'New UM Auto Attendant' (selected) and 'Completion'. The main area has a title 'New UM Auto Attendant' and a description: 'This wizard helps you create a new UM auto attendant for use by Microsoft Exchange Unified Messaging. You need to enter a name for this auto attendant and associate the auto attendant with a dial plan. You can also enter the extension number or numbers that callers will use to access this auto attendant.'

The 'Name:' field contains 'UM Auto Attendant'. The 'Select associated dial plan.' dropdown shows 'CM-SM-5-Digit' with a 'Browse...' button next to it. The 'Pilot identifier list:' field is empty. Below it, there are icons for '+ Add', 'Edit', and 'X'. The list itself contains the number '29500'. At the bottom, there are two checked checkboxes: 'Create auto attendant as enabled' and 'Create auto attendant as speech-enabled'. Navigation buttons at the bottom include 'Help', '< Back', 'New', and 'Cancel'.



## 8. Verification Steps

The following steps can be used to verify installations in the field.

1. Verify that the SIP trunk is in-service using the **status trunk** command on Communication Manager.
2. Verify that the UM Entity Link is up on Session Manager.
3. Verify that users can dial the UM pilot number and that the proper greeting is played. If Exchange UM is called by a UM subscriber, the user should not be prompted for the extension, only the password.
4. Place a call to a UM subscriber and let the call cover to voicemail. Verify that the proper greeting is played.
5. Leave a voice message for a UM subscriber and verify that the MWI of the user's telephone is illuminated.
6. Log on to Exchange UM to retrieve voice messages from a telephone. Use the telephone or voice interface to navigate through the menu. Verify that the voice message is heard by the user.
7. Retrieve voice messages from Outlook Web Access (OWA). Enter `https://<ip-addr>/owa`, where `<ip-addr>` is the IP address of the Exchange 2010 server, as the URL in an Internet browser and log on. Use the Play-on-Phone feature to play the messages on a telephone.
8. Delete the voice messages and verify that the MWI lamp is extinguished.

## 9. Conclusion

These Application Notes have described the configuration steps required to integrate Microsoft Exchange Server 2010 Unified Messaging with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Observations are noted in **Section 2.2**.

## 10. Additional References

- [1] *Administering Avaya Aura® Session Manager*, August 2010, Issue 3, Release 6.0, Document Number 03-603324, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura® Communication Manager*, June 2010, Release 6.0, Issue 6.0, Document Number 03-300509, available at <http://support.avaya.com>.
- [3] *Telephony Partner Product Interoperability Specification Interfaces for Connection to Mediation Server/OCS 2007 R2 and to Exchange Server 2010 Unified Messaging*, June 2009.

---

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