

Microsoft Exchange Server 2007 Unified Messaging PBX Configuration Note: Avaya S8300 with AudioCodes Mediant 2000 using T1 CAS (In-band DTMF Tones)

By : AudioCodes

Updated Since : 2007-02-09

READ THIS BEFORE YOU PROCEED

This document is for informational purposes only and is provided "AS IS". Microsoft, its partners and vendors cannot verify the accuracy of this information and take no responsibility for the content of this document. **MICROSOFT, ITS PARTNERS AND VENDORS MAKE NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.**

Content

This document describes the configuration required to setup Avaya S8300 and AudioCodes Mediant 2000 using T1 CAS In-band DTMF Tones as the telephony signaling protocol. It also contains the results of the interoperability testing of Microsoft Exchange 2007 Unified Messaging based on this setup.

Intended Audience

This document is intended for Systems Integrators with significant telephony knowledge.

Technical Support

The information contained within this document has been provided by Microsoft, its partners or equipment manufacturers and is provided AS IS. This document contains information about how to modify the configuration of your PBX or VoIP gateway. Improper configuration may result in the loss of service of the PBX or gateway. Microsoft is unable to provide support or assistance with the configuration or troubleshooting of components described within. Microsoft recommends readers to engage the service of an Microsoft Exchange 2007 Unified Messaging Specialist or the manufacturers of the equipment(s) described within to assist with the planning and deployment of Exchange Unified Messaging.

Microsoft Exchange 2007 Unified Messaging (UM) Specialists

These are Systems Integrators who have attended technical training on Exchange 2007 Unified Messaging conducted by Microsoft Exchange Engineering Team. For contact information, visit [here](#).

Version Information

Date of Modification	Details of Modification
21 March 2007	Version 1

1. Components Information

1.1. PBX or IP-PBX

PBX Vendor	Avaya
Model	S8300
Software Version	R013x.01.2.632.1
Telephony Signaling	T1 CAS In-band DTMF Tones
Additional Notes	None

1.2. VoIP Gateway

Gateway Vendor	AudioCodes
Model	Mediant 2000
Software Version	5.00.017.003
VoIP Protocol	SIP

1.3. Microsoft Exchange Server 2007 Unified Messaging

Version	RTM
----------------	-----

2. Prerequisites

2.1. Gateway Prerequisites

The gateway also supports TLS (in addition to TCP). This provides security by enabling the encryption of SIP packets over the IP network. The gateway supports self-signed certificates as well as Microsoft Windows Certificates Authority (CA) capabilities.

2.2. PBX Prerequisites

- Enter the command “display system-parameters customer-options”, and then ensure that the “Mode Code for Centralized Voice Mail?” parameter (on screen 4 of the PBX configuration tool) is set to “y”.
- The PBX hardware must include an installed Trunk Card Module MM710.

2.3. Cabling Requirements

This integration uses standard RJ-48c cable to connect digital trunk (T1/E1) between MM710 and Mediant 2000 Trunk interface.

3. Summary and Limitations



A check in this box indicates the UM feature set is fully functional when using the PBX/gateway in question.

4. Gateway Setup Notes

Step 1: SIP Environment Setup

AudioCodes - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites

Address http://10.15.4.19/ Go Links >>

AudioCodes **TrunkPack 1610**
MG Module 1

Protocol Definition Advanced Parameters Manipulation Tables Routing Tables Profile Definitions Trunk Group Trunk Group Settings Digital Gateway Parameters VXML & RADIUS Parameters

Quick Setup
 Protocol Management
Advanced Configuration
Status & Diagnostics
Software Update
Maintenance
Log Off

Search
SIP

General

PRACK Mode	Supported
Channel Select Mode	Cyclic Ascending
Enable Early Media	Disable
183 Message Behavior	Progress
Session-Expires Time	0
Minimum Session-Expires	90
Session Expires Method	Re-Invite
Asserted Identity Mode	Disabled
Fax Signaling Method	T.38 Relay
I Detect Fax on Answer Tone	Initiate T.38 on Preamble
SIP Transport Type	TCP
SIP UDP Local Port	5060
SIP TCP Local Port	5060
SIP TLS Local Port	5061
Enable SIPS	Disable
Enable TCP Connection Reuse	Enable
SIP Destination Port	5060

Web Server Internet

Step 2: Routing Setup

AudioCodes - Microsoft Internet Explorer

Address: http://10.15.4.19/

AudioCodes TrunkPack 1610 MG Module 1

Protocol Definition Advanced Parameters Manipulation Tables Routing Tables Profile Definitions Trunk Group Trunk Group Settings Digital Gateway Parameters VXML & RADIUS Parameters

Quick Setup
Protocol Management
Advanced Configuration
Status & Diagnostics
Software Update
Maintenance
Log Off

SIP

Search

Web Server Internet

Proxy & Registration

Enable Proxy	Use Proxy
Proxy Name	
Proxy IP Address	10.15.3.207
First Redundant Proxy IP Address	0.0.0.0
Second Redundant Proxy IP Address	0.0.0.0
Third Redundant Proxy IP Address	0.0.0.0
Redundancy Mode	Parking
Proxy Load Balancing Method	Disable
Proxy IP List Refresh Time	60
Enable Proxy Keep Alive	Disable
Proxy Keep Alive Time	60
Enable Fallback to Routing Table	Disable
Prefer Routing Table	No
Use Routing Table for Host Names and Profiles	Disable
Always Use Proxy	Disable
Send All Invite to Proxy	No
Enable Proxy Hot-Swap	Disable

Note: The Proxy IP Address must be one that corresponds to the network environment in which the Microsoft Unified Messaging server is installed (For example, 10.15.3.207 or the FQDN of the Microsoft Unified Messaging host).

Step 3: Coder Setup

AudioCodes - Microsoft Internet Explorer

Address: <http://10.15.4.19/>

AudioCodes

TrunkPack 1610
MG Module 1

Protocol Definition | Advanced Parameters | Manipulation Tables | Routing Tables | Profile Definitions | Trunk Group | Trunk Group Settings | Digital Gateway Parameters | VXML & RADIUS Parameters

Quick Setup
Protocol Management
Advanced Configuration
Status & Diagnostics
Software Update
Maintenance
Log Off

Search

Coders

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711A-law	20	64	8	Disabled
G.711U-law	20	64	0	Disabled
G.723.1	30	5.3	4	Disabled

Submit

Web Server | Internet

Step 4: Digit Collection Setup

AudioCodes - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites RSS Print Mail New Tab

Links Interop Tasks Google G Go Bookmarks 155 blocked Check AutoLink AutoFill Send to Settings

Address http://10.15.4.13/ Go

AudioCodes **TrunkPack 1610**

Protocol Definition Advanced Parameters Manipulation Tables Routing Tables Profile Definitions Trunk Group Trunk Group Settings Digital Gateway Parameters VXML & RADIUS Parameters IPMedia Parameters

Quick Setup
Protocol Management
Advanced Configuration
Status & Diagnostics
Software Update
Save Configuration
Reset Device
Log Off

DTMF & Dialing

Max Digits In Phone Num for Overlap Dialing	15	←
Inter Digit Timeout for Overlap Dialing [sec]	2	←
Declare RFC 2833 in SDP	Yes	
1st Tx DTMF Option	Not Supported	
2st Tx DTMF Option	Not Supported	
3st Tx DTMF Option	Not Supported	
4st Tx DTMF Option	Not Supported	
5st Tx DTMF Option	Not Supported	
RFC 2833 Payload Type	101	←
Digit Mapping Rules	[x*#][x*#].t	←
Default Destination Number	1000	

Submit

Done Internet

Step 5: Manipulation Routing Setup

AudioCodes - Microsoft Internet Explorer

Address: http://172.20.22.201/

AudioCodes **TrunkPack 1610**

Protocol Definition | Advanced Parameters | **Manipulation Tables** | Routing Tables | Profile Definitions | Trunk Group | Trunk Group Settings | Digital Gateway Parameters | VXML & RADIUS Parameters

Destination Phone Number Manipulation Table for Tel -> IP Calls

Table Index: 1-10

	Destination Prefix	Source Prefix	Number of stripped Digits	Prefix (Suffix) to Add	Number of Digits to Leave
1	*	*	0		0
2					
3					
4					
5					
6					
7					
8					
9					
10					

Submit

Web Server Internet

Step 6: Trunk Group Setup

AudioCodes - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites RSS Print Mail

Address http://10.15.4.19/ Go Links

AudioCodes **TrunkPack 1610**
MG Module 1

Protocol Definition Advanced Parameters Manipulation Tables Routing Tables Profile Definitions **Trunk Group** Trunk Group Settings Digital Gateway Parameters VXML & RADIUS Parameters

Quick Setup
Protocol Management
Advanced Configuration
Status & Diagnostics
Software Update
Maintenance
Log Off

Search
SIP

Trunk Group Table

Trunk Group Index 1-12

Group Index	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Profile ID
1	1	1	1-24	1000		0
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						

Web Server Internet

Step 7: TDM BUS Setting

The screenshot shows the AudioCodes TrunkPack 1610 web interface. The browser is Microsoft Internet Explorer, displaying the URL <http://172.20.22.201/>. The page title is "AudioCodes - Microsoft Internet Explorer". The main navigation bar includes "Network Settings", "Media Settings", "Trunk Settings", "SS7 Configuration", "TDM Bus Settings" (highlighted), "Configuration File", "Regional Settings", "Security Settings", and "Management Settings". The left sidebar contains a "Quick Setup" menu with options: "Quick Setup", "Protocol Management", "Advanced Configuration" (highlighted), "Status & Diagnostics", "Software Update", "Maintenance", and "Log Off". The main content area is titled "TDM Bus Settings" and contains a table of configuration parameters:

TDM Bus Settings	
I PCM Law Select	MuLaw
TDM Bus Clock Source	Network
TDM Bus PSTN Auto Clock	Disable
I TDM Bus PSTN Auto Clock Reverting	Disable
I Idle PCM Pattern	255
I Idle ABCD Pattern	0x0F
TDM Bus Local Reference	1

Below the table is a "Submit" button. To the right of the table, two black arrows point to the "I PCM Law Select" and "TDM Bus Clock Source" rows. Below the table, a text box states: "To reboot and apply modified value(s) to the device, click 'Submit' then 'Reset' (with the 'Burn To FLASH' selected)."

The bottom status bar shows "Web Server" and "Internet".

Step 8: CAS Table Download

The screenshot shows the AudioCodes TrunkPack 1610 web interface. The browser is Microsoft Internet Explorer with the address bar showing <http://172.20.22.201/>. The page has a navigation menu on the left with options like Quick Setup, Protocol Management, Advanced Configuration (highlighted), Status & Diagnostics, Software Update, Maintenance, and Log Off. The main content area is titled 'Regional Settings' and contains three sections for uploading files to the device: 'Send "Call Progress Tones" file', 'Send "CAS" file', and 'Send "Voice Prompts" file'. Each section has a text input field, a 'Browse...' button, and a 'Send File' button. A black arrow points to the 'CAS' file upload section. Below these sections is a date and time selection table.

YYYY	MM	DD	Hour	Min	Sec
2000	1	11	21	52	48

Below the table is a 'Set Date & Time' button.

Note: The CAS file must be downloaded to the Mediant 2000. A suitable CAS file is attached to this document (refer to Section 4.1).

Step 9: Trunk Setting Setup

AudioCodes - Microsoft Internet Explorer

Address: http://172.20.22.201/

AudioCodes TrunkPack 1610

Network Settings Media Settings **Trunk Settings** SS7 Configuration TDM Bus Settings Configuration File Regional Settings Security Settings Management Settings

Trunk Number 1 2
Trunk Status

Trunk Settings

Trunk Configuration	
Trunk ID	1
Trunk Configuration State	Inactive
Protocol Type	T1 CAS
Clock Master	Recovered
Auto Clock Trunk Priority	0
Line Code	B8ZS
Line Build Out Loss	0 dB
Trace Level	No Trace
Line Build Out Overwrite	OFF
Framing Method	T1 FRAMING ESF CRC6
CAS Configuration	
CAS Table	loopstarttable_fxo_dtmf.dat (2006\10\12)
Play Ringback Tone to Trunk	Not Configured

Web Server Internet

Step 10: Voicemail In-Band DTMF Setup

http://172.20.22.201/WSVoiceMail - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites

Address http://172.20.22.201/WSVoiceMail Go Links

Voice Mail

General	
Voice Mail Interface	DTMF
Digit Patterns	
Forward on Busy Digit Pattern	#02#S.#R.#
Forward on No Answer Digit Pattern	#02#S.#R.#
Forward on Do Not Disturb Digit Pattern	#03##R.#
Forward on No Reason Digit Pattern	#02#S.#R.#
Internal Call Digit Pattern	#00#S.##
External Call Digit Pattern	#01#S.##
Disconnect Call Digit Pattern	
MWI	
MWI Off Digit Pattern	#2
MWI On Digit Pattern	*2
SMDI	
Enable SMDI	Disable
SMDI Timeout [msec]	2000

Submit

Done Internet

Step 11: FAX Setup

AudioCodes - Microsoft Internet Explorer

Address: http://10.15.4.19/

AudioCodes **TrunkPack 1610**
MG Module 1

Network Settings **Media Settings** Trunk Settings SS7 Configuration TDM Bus Settings Configuration File Regional Settings Security Settings Management Settings

Quick Setup
Protocol Management
Advanced Configuration
Status & Diagnostics
Software Update
Maintenance

Log Off

Search
SIP

Fax/Modem/CID Settings

Fax Transport Mode	T.38 Relay
Caller ID Transport Type	Mute
Caller ID Type	Bellcore
V.21 Modem Transport Type	Disable
V.22 Modem Transport Type	Enable Bypass
V.23 Modem Transport Type	Enable Bypass
V.32 Modem Transport Type	Enable Bypass
V.34 Modem Transport Type	Enable Bypass
Fax Relay Redundancy Depth	0
Fax Relay Enhanced Redundancy Depth	4
Fax Relay ECM Enable	Enable
Fax Relay Max Rate (bps)	14400
Fax/Modem Bypass Coder Type	G711Alaw
Fax/Modem Bypass Packing Factor	1
CNG Detector Mode	Events Only

Submit

Web Server Internet

Step 12: General Setup

AudioCodes - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites RSS Print Mail News Groups Feeds

Links Interop Tasks Google G Go Bookmarks 155 blocked Check AutoLink AutoFill Send to Settings

Address http://10.15.4.13/ Go

AudioCodes TrunkPack 1610

Protocol Definition **Advanced Parameters** Manipulation Tables Routing Tables Profile Definitions Trunk Group Trunk Group Settings Digital Gateway Parameters VXML & RADIUS Parameters IPMedia Parameters

- Quick Setup
- Protocol Management**
- Advanced Configuration
- Status & Diagnostics
- Software Update
- Save Configuration
- Reset Device
- Log Off

General Parameters

IP Security	Disable
Filter Calls to IP	Don't Filter
I Enable Digit Delivery to Tel	Disable
I Enable Digit Delivery to IP	Disable
Disconnect on Broken Connection	No
Broken Connection Timeout [100 msec]	100
Disconnect Call on Silence Detection	No
Silence Detection Period [sec]	120
Silence Detection Method	Packets Count
CDR and Debug	
CDR Server IP Address	
CDR Report Level	End Call
Debug Level	5
Misc. Parameters	
Progress Indicator to IP	Not Configured
Enable X-Channel Header	Disable

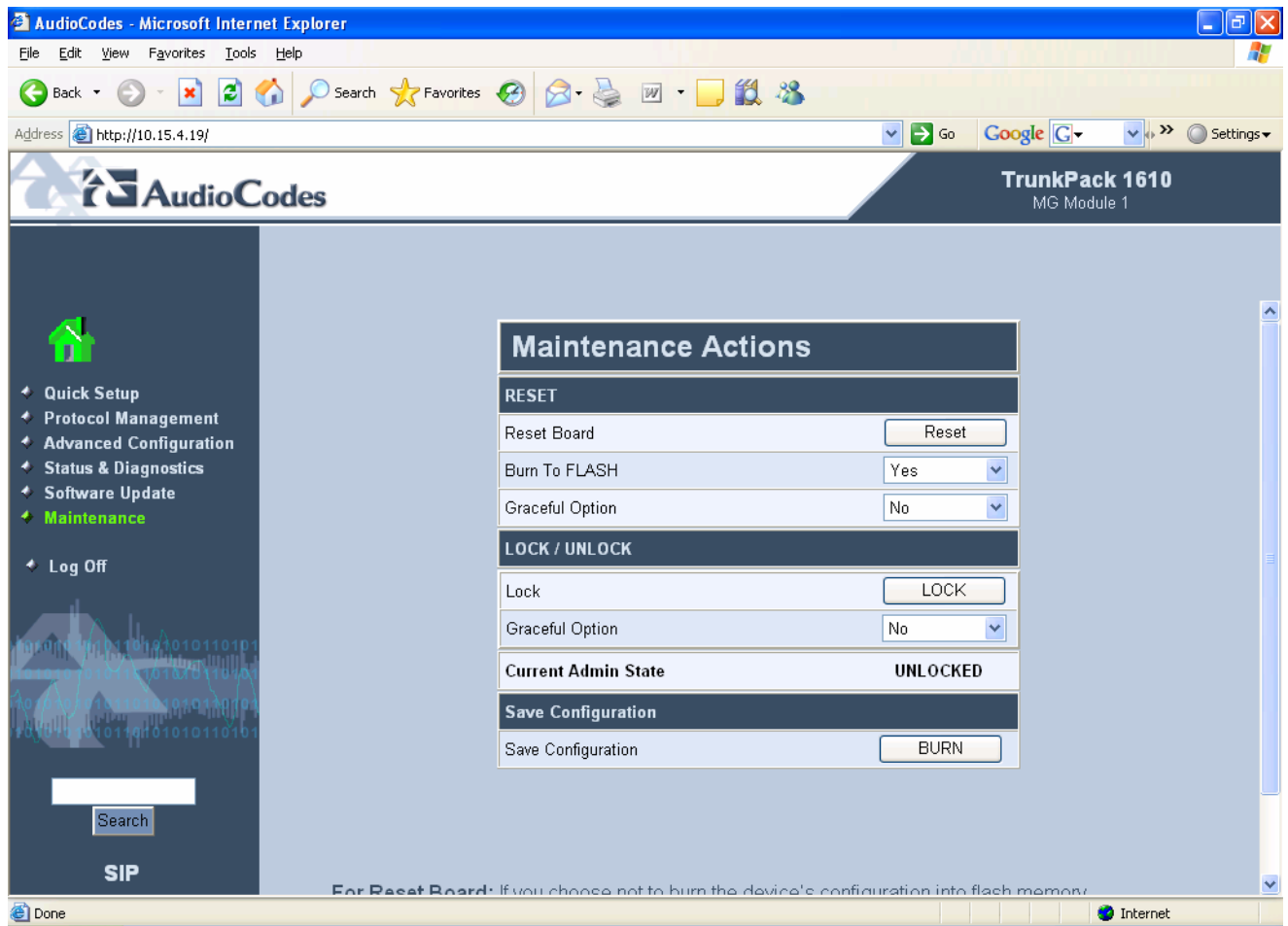
Done Internet

Step 13 : General Setup (Cont.)

- EnableMWI = 1
- SubscriptionMode = 1
- LineTransferMode = 1
- IsSpecialDigits = 1
- EnableDetectRemoteMACChange = 2
- ECNLPMODE = 1
- TrunkTransferMode_X = 3

Note: "X" refers to the Trunk number, for example: for the first trunk
TrunkTransferMode_0 = 3

Step 14: Reset Mediant 2000



Click **Reset** to reset the gateway.

4.1. Configuration Files

The ZIP file includes the following files:

- Audiocodes configuration ini file (.ini file extension).
- Audiocodes T1 CAS file (.dat file extension).



AudioCodes Files -Avaya S8300.zip

4.2. TLS Setup

The specific gateway software version used in this PBX Configuration Guide was not tested for TLS. However, TLS was tested successfully for other gateway software versions operating with Microsoft Exchange 2007 TLS capabilities.

Refer to the procedure below for TLS setup.

Step 1: PBX to IP Routing Setup

Proxy & Registration	
Enable Proxy	Use Proxy
Proxy Name	exchange2007.server2003.c
Proxy IP Address	10.15.3.207
First Redundant Proxy IP Address	0.0.0.0
Second Redundant Proxy IP Address	0.0.0.0
Third Redundant Proxy IP Address	0.0.0.0
Redundancy Mode	Parking
Proxy Load Balancing Method	Disable
Proxy IP List Refresh Time	60
Enable Proxy Keep Alive	Disable
Proxy Keep Alive Time	60
Enable Fallback to Routing Table	Disable
Prefer Routing Table	No
Use Routing Table for Host Names and Profiles	Disable
Always Use Proxy	Disable
Send All Invite to Proxy	No
Enable Proxy Host Supp	Disable

Note: The Proxy IP Address and Name must be one that corresponds to the network environment in which the Microsoft Unified Messaging server is installed (For example, 10.15.3.207 for IP Address and exchaneg2007.server2003.com for the FQDN of the Microsoft Unified Messaging host).

Step 2: SIP Environment and Gateway Name Setup

AudioCodes - Microsoft Internet Explorer

Address: http://10.15.4.13/

AudioCodes TrunkPack 1610

Protocol Management

Quick Setup
Protocol Management
Advanced Configuration
Status & Diagnostics
Software Update
Maintenance
Log Off

Search

SIP

Parameter	Value
Enable Failback to Routing Table	Disable
Prefer Routing Table	No
Use Routing Table for Host Names and Profiles	Disable
Always Use Proxy	Disable
Send All Invite to Proxy	No
Enable Proxy Hot-Swap	Disable
Enable Registration	Disable
Gateway Name	gw1.m2k.audiocodes.com
Gateway Registration Name	
DNS Query Type	A-Record
Proxy DNS Query Type	A-Record
Use Gateway Name for OPTIONS	No
Number of RTX Before Hot-Swap	3
User Name	
Password
Cnonce	Default_Cnonce

Register Un-Register Submit

Web Server Internet

Note: Assign an FQDN name to the gateway (for example, gw1.m2k.audiocodes.com). Any gateway name that corresponds to your network environment is applicable; the only limitation is not to include underscores in the name (Windows Certification server limitation).

Step 3: SIP Environment Setup (Cont.)

AudioCodes - Microsoft Internet Explorer

Address: http://10.15.4.13/

AudioCodes **TrunkPack 1610**

Protocol Definition | Advanced Parameters | Manipulation Tables | Routing Tables | Profile Definitions | Trunk Group | Trunk Group Settings | Digital Gateway Parameters | Advanced Applications

General

PRACK Mode	Supported	
Channel Select Mode	Cyclic Ascending	←
Enable Early Media	Disable	
183 Message Behavior	Progress	
Session-Expires Time	0	
Minimum Session-Expires	90	
Session Expires Method	Re-Invite	
Asserted Identity Mode	Disabled	
Fax Signaling Method	T.38 Relay	←
I Detect Fax on Answer Tone	Initiate T.38 on Preamble	
SIP Transport Type	TLS	←
SIP UDP Local Port	5000	←
SIP TCP Local Port	5040	←
SIP TLS Local Port	5060	←
Enable SIPs	Disable	
Enable TCP Connection Reuse	Enable	
SIP Destination Port	5061	←
Use "user-agent" in SIP URI	Yes	

Web Server | Internet

Step 4: DNS Servers Setup

AudioCodes - Microsoft Internet Explorer

Address: http://10.15.4.13/

AudioCodes TrunkPack 1610

Network Settings | Media Settings | Trunk Settings | SS7 Configuration | TDM Bus Settings | Configuration File | Regional Settings | Security Settings | Management Settings

Quick Setup
Protocol Management
Advanced Configuration
Status & Diagnostics
Software Update
Maintenance
Log Off

SIP

IP Settings

IP Networking Mode	Single IP Network
IP Address	10.15.4.13
Subnet Mask	255.255.0.0
Default Gateway Address	10.15.0.1

DNS Settings

DNS Primary Server IP	10.1.1.11
DNS Secondary Server IP	10.1.1.10

DHCP Settings

Enable DHCP	Disable
-------------	---------

NAT Settings

NAT IP Address	0.0.0.0
----------------	---------

Differential Services

Network QoS	48
Media Premium QoS	46
Control Premium QoS	40
Gold QoS	26

Note: Define the primary and secondary DNS servers' IP addresses so that they correspond to your network environment (for example, 10.1.1.11 and 10.1.1.10). If no DNS server is available in the network, then skip this step.

Step 5: Internal DNS Setup

The screenshot shows the AudioCodes TrunkPack 1610 web interface in a Microsoft Internet Explorer browser. The address bar shows <http://10.15.4.13/>. The interface has a top navigation bar with the AudioCodes logo and the title "TrunkPack 1610". Below this is a menu bar with the following items: Protocol Definition, Advanced Parameters, Manipulation Tables, **Routing Tables** (highlighted in green), Profile Definitions, Trunk Group, Trunk Group Settings, Digital Gateway Parameters, and Advanced Applications. On the left side, there is a sidebar with a green house icon and a list of links: Quick Setup, **Protocol Management** (highlighted in green), Advanced Configuration, Status & Diagnostics, Software Update, Maintenance, and Log Off. Below these links is a search bar with the text "SIP" and a "Search" button. The main content area is titled "Internal DNS Table" and contains a table with 10 rows. The first row is pre-filled with "exchange2007.server20" in the Domain Name column and "10.15.3.207" in the First IP Address column. The other columns are empty. A black arrow points to the right side of the table. Below the table is a "Submit" button.

	Domain Name	First IP Address	Second IP Address
1	exchange2007.server20	10.15.3.207	
2			
3			
4			
5			
6			
7			
8			
9			
10			

Submit

Note: If no DNS server is available in the network, define the internal DNS table where the domain name is the FQDN of the Microsoft Unified Messaging server and the First IP Address corresponds to its IP address (for example, exchange2007.com and 10.15.3.207).

Step 6: NTP Server Setup

The screenshot shows the AudioCodes TrunkPack 1610 configuration interface. The browser window is titled 'AudioCodes - Microsoft Internet Explorer' and the address bar shows 'http://10.15.4.13/'. The interface has a navigation menu on the left with options like 'Quick Setup', 'Protocol Management', 'Advanced Configuration', 'Status & Diagnostics', 'Software Update', 'Maintenance', and 'Log Off'. The main content area is titled 'Application Settings' and contains several sections: 'NTP Settings', 'Telnet Settings', 'STUN Settings', and 'NFS Settings'. The 'NTP Settings' section is highlighted, and a black arrow points to the 'NTP Server IP Address' field, which contains the value '10.15.6.50'. Other fields in the 'NTP Settings' section include 'NTP UTC Offset' (Hours: 0, Minutes: 0) and 'NTP Update Interval' (Hours: 24, Minutes: 0). The 'Telnet Settings' section includes 'Embedded Telnet Server' (Disable), 'Telnet Server TCP Port' (23), and 'Telnet Server Idle Timeout' (0). The 'STUN Settings' section includes 'Enable STUN' (Disable), 'STUN Server Primary IP' (0.0.0.0), and 'STUN Server Secondary IP' (0.0.0.0). The 'NFS Settings' section includes an 'NFS Table' field with a '-->' button. A 'Submit' button is located at the bottom right of the 'Application Settings' window.

NTP Settings	
NTP Server IP Address	10.15.6.50
NTP UTC Offset	Hours: 0 Minutes: 0
NTP Update Interval	Hours: 24 Minutes: 0

Telnet Settings	
Embedded Telnet Server	Disable
Telnet Server TCP Port	23
Telnet Server Idle Timeout	0

STUN Settings	
Enable STUN	Disable
STUN Server Primary IP	0.0.0.0
STUN Server Secondary IP	0.0.0.0

NFS Settings	
NFS Table	-->

Note: Define the NTP server's IP address so that it corresponds to your network environment (for example, 10.15.3.50). If no NTP server is available in the network, then skip this step (as the gateway uses its internal clock).

Step 7: Generate Certificate Setup

Use the screen below to generate CSR. Copy the certificate signing request and send it to your Certification Authority for signing.

The screenshot shows the AudioCodes TrunkPack 1610 web interface in Microsoft Internet Explorer. The browser address bar shows `http://10.15.4.13/`. The page title is "AudioCodes" and the version is "TrunkPack 1610". The navigation menu includes: Network Settings, Media Settings, Trunk Settings, SS7 Configuration, TDM Bus Settings, Configuration File, Regional Settings, Security Settings (highlighted), and Management Settings. The left sidebar contains: Quick Setup, Protocol Management, Advanced Configuration (highlighted), Status & Diagnostics, Software Update, Maintenance, and Log Off. The main content area is titled "Certificate Signing Request". It features a form with a "Subject Name" field containing "gw1.m2k.audiocodes.com" and a "Generate CSR" button. Below the form, it instructs the user to "Copy the certificate signing request and send it to your Certification Authority for signing." and displays the following text:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBYDCBygIBADAhMR8wHQYDVQOExZndzEubTJrLmF1ZGlvY29kZXMuY29tMIGf
MAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBQC2AZdeiLwVBBni+bI638fpEWIn4nuh
cc6U1LhAMPuhtjoaqlYeNeFMfT6i92wEX0gehQbxAZyAOP0jqT0bbmrROMugs8pt
hghJTbajgg1INFppccm181pW7FDz4rZyMZtm5pC4PgYT6W2QF4MyxhE3h2qmLkZf
UEH5XCaOMFI8CQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAkwv9R2XqUEqCRUXb
wV8LVp+7OzkzCMQkc3FUKqL6uqs9IW5B2h+MyO/nxBcWV355sT/zksb0d6hW13E9
rCa+ar0OM1yOmUDcTh1TqobakBN53PKLMDElkG1QcFRfTfs9UggsBDCg9nHYPrBP
1Mow1QrUvnp711Fhuedt/h2xUUo=
-----END CERTIFICATE REQUEST-----
```

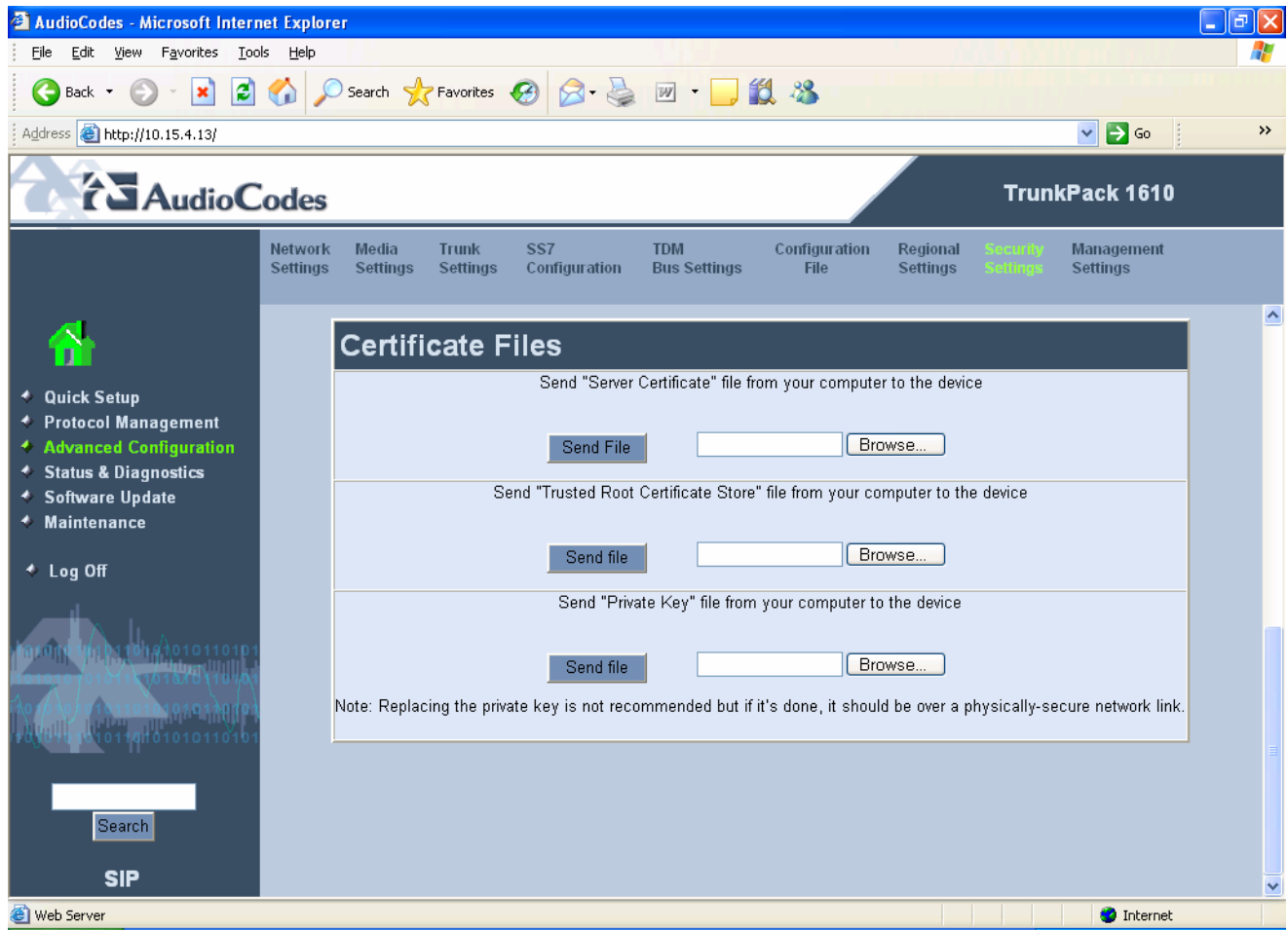
Below the text, there is a small note: "Press the button 'Generate self-signed' to create a self-signed certificate using the subject name provided above." At the bottom of the page, there are two tabs: "Web Server" and "Internet".

Step 8: Uploading Certificates Setup

The screen below is used to upload the sign certificates.

In the "Server Certificate" area, upload the gateway certificate signed by the CA.

In the "Trusted Root Certificate Store" area, upload the CA certificate.



5. PBX Setup Notes

Information used for this test case:

- Digital VoiceMail ports: ext. 5061 – 5084 ,24 T1 Channel
- VoiceMail Hunt Group Pilot: ext. 5060
- VoiceMail User Phone: ext. 5006 and ext. 5096
- Coverage Path for ext. 5006 and 5096 is 2
- User Test Phone Avaya 2420

Step 1: Add Station with Coverage Path

Add a station using **the Add Station** command, and then configure the station using the below settings (in this example, it's a digital station, but it can also be an analog station). Define the Coverage Path for this station, for example, as 2.

The screenshot shows the Avaya Site Administration interface for station configuration. The window title is "Avaya Site Administration - [S8300 GEDII]". The menu bar includes File, Edit, View, System, Action, Tools, Window, and Help. The toolbar contains various icons for file operations and navigation. Below the toolbar is a status bar with the text "change station 5006" and buttons for "send (return)", "help (f5)", "cancel (esc)", "enter (f3)", "schedule (f9)", "next (f7)", and "previous (f8)".

The main configuration area is titled "STATION" and contains the following fields:

- Extension: 5006
- Type: 2420
- Port: 0010401
- Name: 2420
- Lock Messages?: n
- Security Code: [empty]
- Coverage Path 1: 2
- Coverage Path 2: [empty]
- Hunt-to Station: [empty]
- BCC: 0
- TN: 1
- COR: 1
- COS: 1

Below the "STATION" section is the "STATION OPTIONS" section, which includes:

- Loss Group: 2
- Data Option: none
- Speakerphone: 2-way
- Display Language: english
- Personalized Ringing Pattern: 2
- Message Lamp Ext: 5006
- Mute Button Enabled?: y
- Expansion Module?: n
- Media Complex Ext: [empty]
- IP SoftPhone?: n
- Remote Office Phone?: n

At the bottom of the window, there is a status bar with the text "Right-click in a field to see a list of valid entries or help text" and "Ready". The taskbar at the very bottom shows the Start button, several application icons, and the system clock displaying "12:01 PM".

Step 2: Define the Coverage Path Properties

Add a coverage path using the **Add Coverage Path** command. Configure the coverage path properties using the below settings. Note: Ensure that you define the coverage destination point.

The screenshot shows the Avaya Site Administration - [S8300 GEDI] window. The main menu includes File, Edit, View, System, Action, Tools, Window, and Help. The toolbar contains icons for various functions and a dropdown menu showing S8300. Below the toolbar are buttons for send (return), help (F5), cancel (esc), enter (F3), schedule (F9), next (F7), and previous (F8).

The main window displays the following configuration details:

COVERAGE PATH

Coverage Path Number: 2

Next Path Number: Hunt after Coverage? n
Linkage

COVERAGE CRITERIA

Station/Group Status	Inside Call	Outside Call	
Active?	n	n	
Busy?	y	y	
Don't Answer?	y	y	Number of Rings: 3
All?	n	n	
DND/SAC/Goto Cover?	y	y	

COVERAGE POINTS

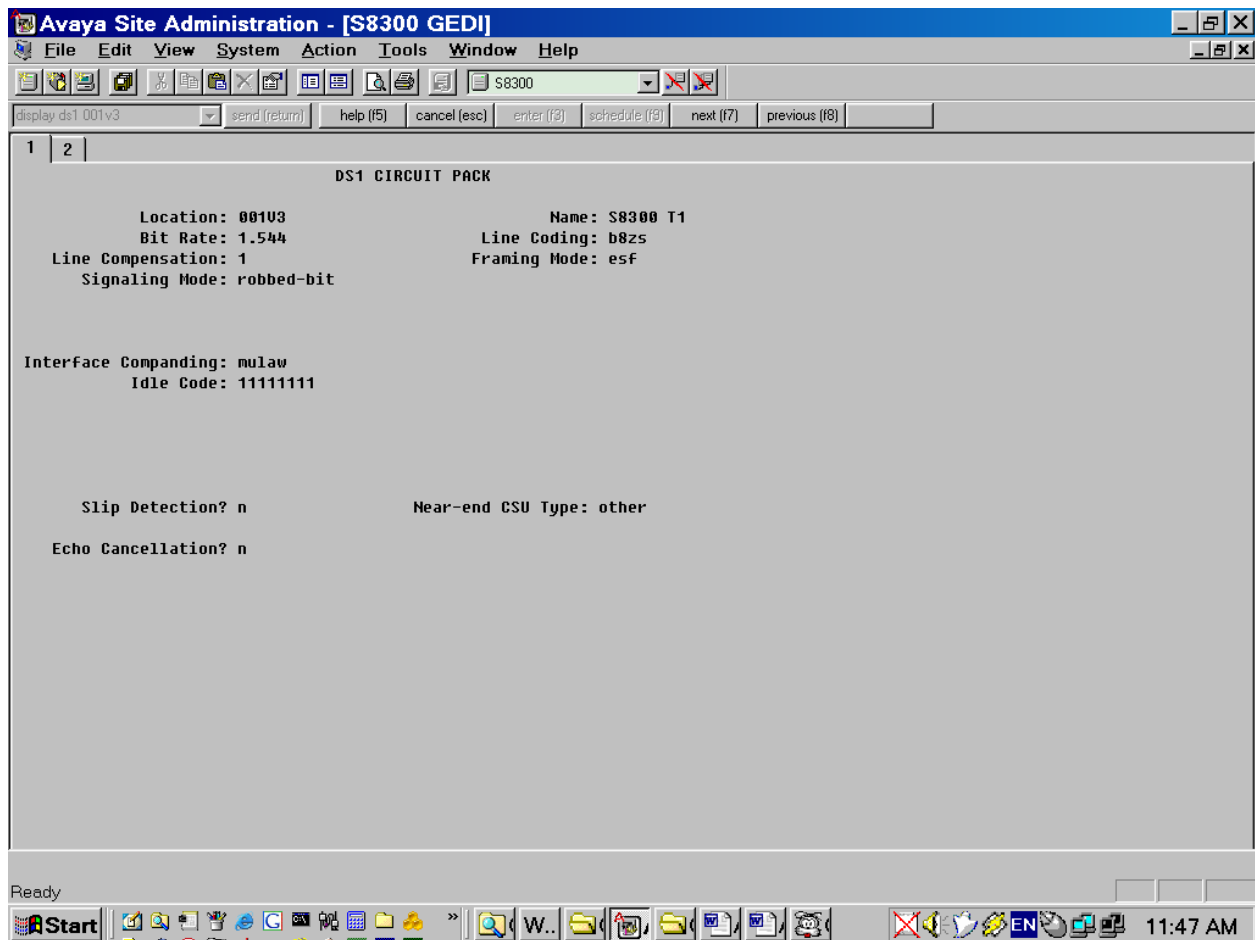
Terminate to Coverage Pts. with Bridged Appearances? n

Point1: h2 Rng: Point2: Point3:
Point4: Point5: Point6:

The coverage path example configured in the figure above, means that when the station does not answer the call or the call is busy, the call is forwarded to hunt group 2 (Point1: h2).

Step 3: T1 Setting using E1/T1 Card

Define T1 using the E1/T1 card that is connected to the Mediant 2000, using the **Add DS1** command.



Step 4: Configuring T1 Ports

Configure the ports on the T1 circuit. Note that the parameter 'Type' must be set to VMIFD to enable DTMFs. For T1 define 24 stations.

The screenshot shows the Avaya Site Administration - [S8300 GEDI] window. The title bar includes standard window controls and a menu bar with File, Edit, View, System, Action, Tools, Window, and Help. Below the menu bar is a toolbar with various icons. A status bar at the top shows 'change station 5080' and several function keys: send (return), help (F5), cancel (esc), enter (F3), schedule (F9), next (F7), and previous (F8).

The main area is titled 'STATION' and contains the following configuration fields:

Extension: 5080	Lock Messages? <input type="checkbox"/>	BCC: 0
Type: VMIFD	Security Code: <input type="text"/>	TN: 1
Port: 001U301		COR: 1
Name: UMI T1-1		COS: 1
		Tests? <input type="checkbox"/>

Below the station configuration, there is a section titled 'STATION OPTIONS' with the following fields:

Loss Group: 4
Off Premises Station? y
R Balance Network? <input type="checkbox"/>

At the bottom of the window, there is a status bar with the text 'Right-click in a field to see a list of valid entries or help text' and 'Ready'. The Windows taskbar at the very bottom shows the Start button, several open applications, and the system clock displaying 4:42 PM.

Step 5: Add a Hunt Group

Add a hunt group using the **Add Hunt Group** command. Define the hunt group number (for example, 3) and properties using the below settings.

The screenshot shows the Avaya Site Administration - [S8300 GEDI] window. The title bar is blue with the text "Avaya Site Administration - [S8300 GEDI]". Below the title bar is a menu bar with "File", "Edit", "View", "System", "Action", "Tools", "Window", and "Help". Below the menu bar is a toolbar with various icons. Below the toolbar is a status bar with "change hunt-group 2", "send (return)", "help (f5)", "cancel (esc)", "enter (f3)", "schedule (f9)", "next (f7)", and "previous (f8)". Below the status bar is a grid of numbers 1 through 32, with a "3:" label and a right arrow. Below the grid is the "HUNT GROUP" configuration screen. The screen has a light gray background and contains the following fields:

Group Number:	2	ACD?	<input type="checkbox"/>
Group Name:	T1 CAS to UK	Queue?	<input type="checkbox"/>
Group Extension:	5060	Vector?	<input type="checkbox"/>
Group Type:	ucd-mia	Coverage Path:	<input type="checkbox"/>
TN:	1	Night Service Destination:	<input type="checkbox"/>
COR:	1	MM Early Answer?	<input type="checkbox"/>
Security Code:		Local Agent Preference?	<input type="checkbox"/>
ISDN/SIP Caller Display:			

Right-click in a field to see a list of valid entries or help text

Ready

Step 6: Assign T1 Ports to Hunt Group

Assign the T1 ports that you defined in Step 4 to the hunt group.

The screenshot shows the 'Avaya Site Administration - [S8300 GEDI]' window. The title bar includes standard window controls and a menu bar with File, Edit, View, System, Action, Tools, Window, and Help. Below the menu bar is a toolbar with various icons. The main window area displays the configuration for 'HUNT GROUP'. At the top, there are fields for 'change hunt-group 2', 'send (return)', 'help (f5)', 'cancel (esc)', 'enter (f3)', 'schedule (f9)', 'next (f7)', and 'previous (f8)'. Below these are tabs numbered 1 through 32. The main content area shows the following information:

HUNT GROUP
Group Number: 2 Group Extension: 5060 Group Type: ucd-mia
Member Range Allowed: 1 - 1500 Administered Members (min/max): 1 /24
Total Administered Members: 24

GROUP MEMBER ASSIGNMENTS

Ext	Name (24 characters)	Ext	Name (24 characters)
1: 5061	T1 UMI	14: 5074	T1 UMI
2: 5062	T1 UMI	15: 5075	T1 UMI
3: 5063	T1 UMI	16: 5076	T1 UMI
4: 5064	T1 UMI	17: 5077	T1 UMI
5: 5065	T1 UMI	18: 5078	T1 UMI
6: 5066	T1 UMI	19: 5079	T1 UMI
7: 5067	T1 UMI	20: 5080	T1 UMI
8: 5068	T1 UMI	21: 5081	T1 UMI
9: 5069	T1 UMI	22: 5082	T1 UMI
10: 5070	T1 UMI	23: 5083	T1 UMI
11: 5071	T1 UMI	24: 5084	T1 UMI
12: 5072	T1 UMI	25:	
13: 5073	T1 UMI	26:	

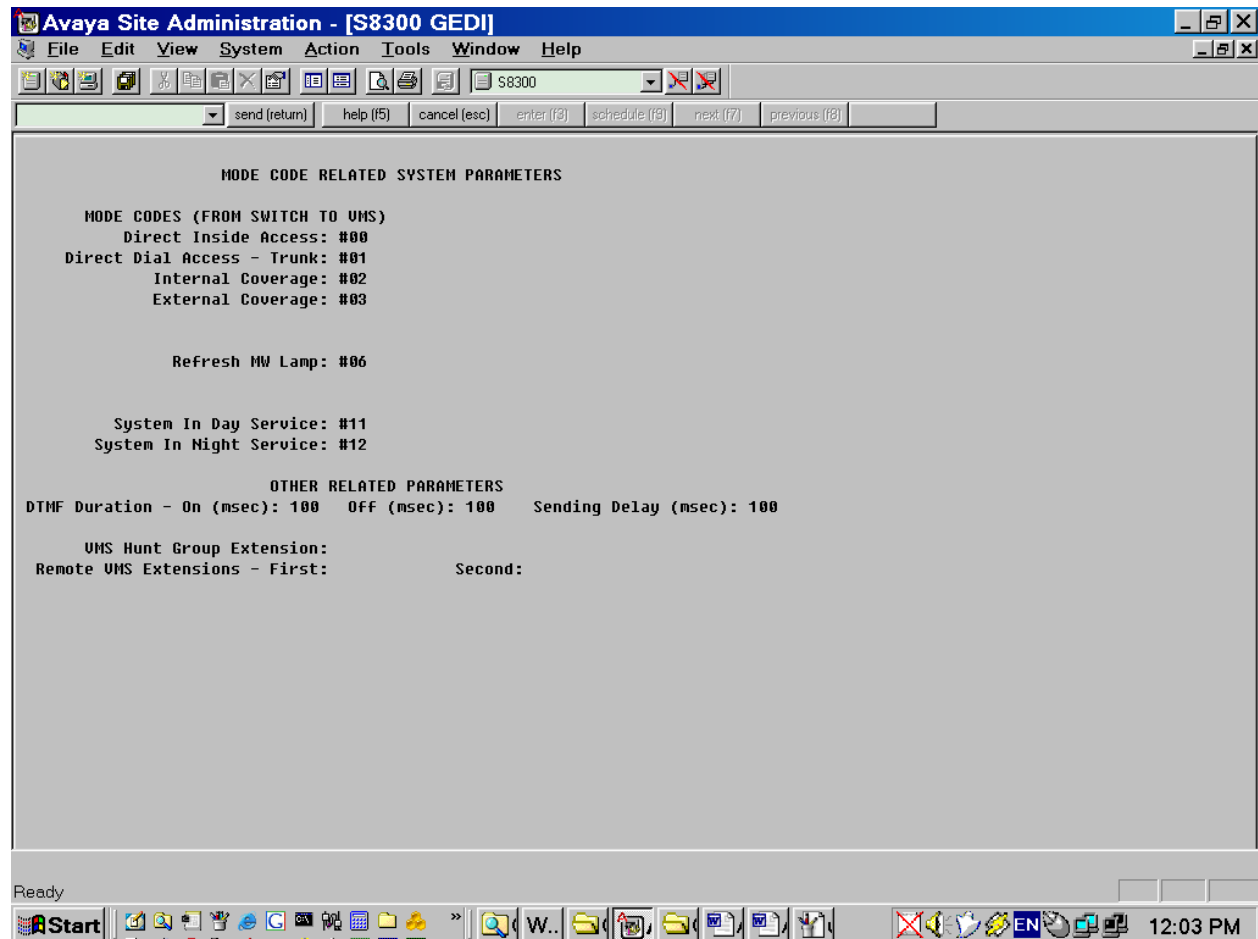
At End of Member List

Right-click in a field to see a list of valid entries or help text
Ready

Step 7: Viewing Mode-code Related System Parameters and Feature Access Codes

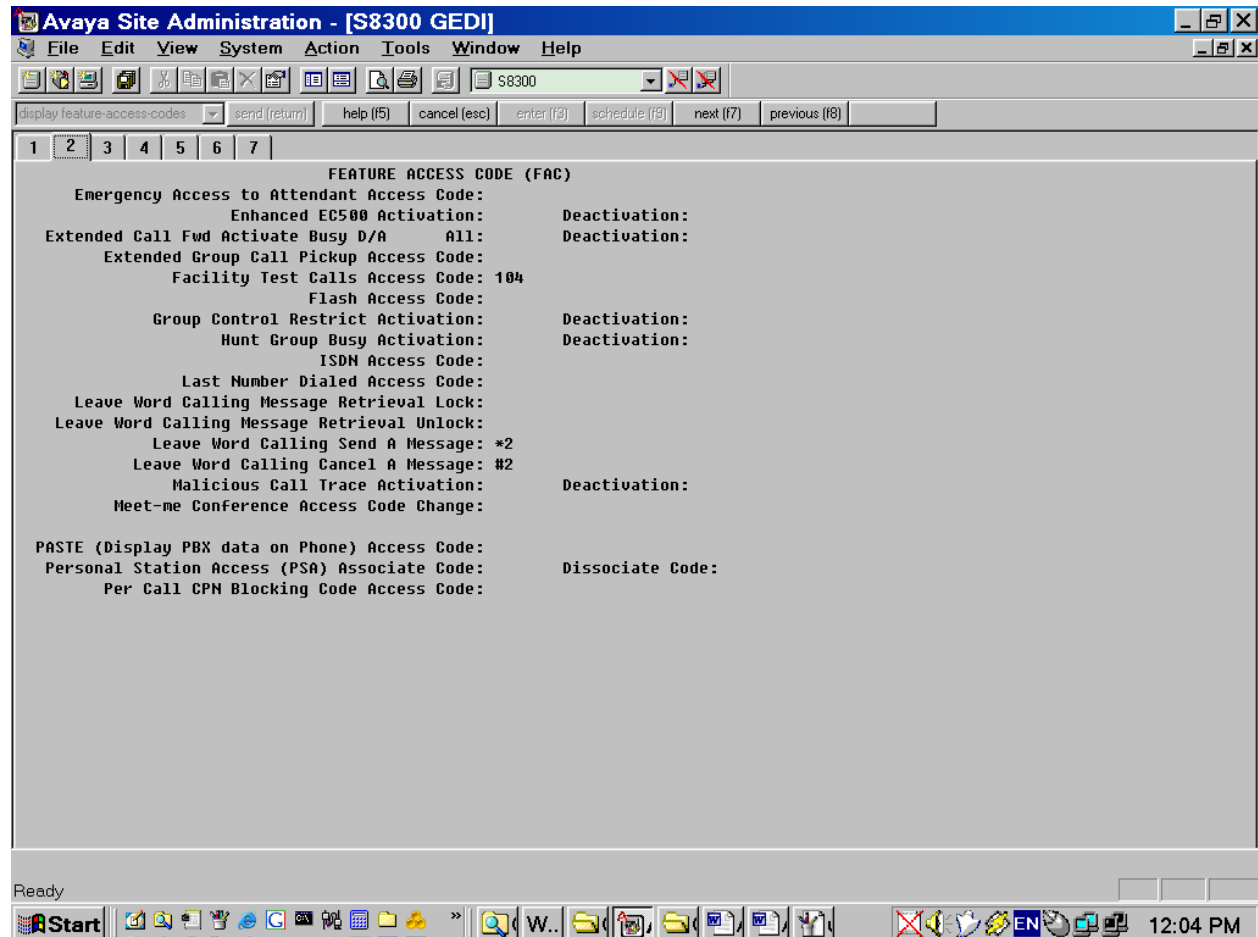
The DTMF signals sent from the PBX to the voice mail system providing the forwarding information (calling party, called party, etc.,) are called Mode Code.

The figure below displays the mode-code related system parameters for the Avaya S8300 PBX.



Feature Access Code:

Below is the feature access code that defines the code sent from the gateway to the PBX for activating / deactivating Message Waiting Indication (MWI), for example, *16 and #16.



5.1. TLS Setup

- N/A.

5.2. Fail-Over Configuration

- N/A.

5.3. Tested Phones

Avaya 2420 Model Telephone.

5.4. Other Comments

None.

6. Exchange 2007 UM Validation Test Matrix

The following table contains a set of tests for assessing the functionality of the UM core feature set. The results are recorded as either:

- Pass (**P**)
- Conditional Pass (**CP**)
- Fail (**F**)
- Not Tested (**NT**)
- Not Applicable (**NA**)

Refer to:

- Appendix for a more detailed description of how to perform each call scenario.
- Section 6.1 for detailed descriptions of call scenario failures, if any.

No.	Call Scenarios (see appendix for more detailed instructions)	(P/CP/F/NT)	Reason for Failure (see 6.1 for more detailed descriptions)
1	Dial the pilot number from a phone extension that is NOT enabled for Unified Messaging and logon to a user's mailbox. Confirm hearing the prompt: "Welcome, you are connected to Microsoft Exchange. To access your mailbox, enter your extension..."	P	
2	Navigate mailbox using the Voice User Interface (VUI).	P	
3	Navigate mailbox using the Telephony User Interface (TUI).	P	
4	Dial user extension and leave a voicemail.		
4a	Dial user extension and leave a voicemail from an internal extension. Confirm the Active Directory name of the calling party is displayed in the sender field of the voicemail message.	P	
4b	Dial user extension and leave a voicemail from an external phone. Confirm the correct phone number of the calling party is displayed in the sender field of the voicemail message.	P	
5	Dial Auto Attendant (AA).	P	

	Dial the extension for the AA and confirm the AA answers the call.		
6	Call Transfer by Directory Search.		
6a	Call Transfer by Directory Search and have the called party answer. Confirm the correct called party answers the phone.	P	
6b	Call Transfer by Directory Search when the called party's phone is busy. Confirm the call is routed to the called party's voicemail.	P	
6c	Call Transfer by Directory Search when the called party does not answer. Confirm the call is routed to the called party's voicemail.	P	
6d	Setup an invalid extension number for a particular user. Call Transfer by Directory Search to this user. Confirm the number is reported as invalid.	P	The PBX indicates an invalid number by playing the user error tone.
7	Outlook Web Access (OWA) Play-On-Phone Feature.		
7a	Listen to voicemail using OWA's Play-On-Phone feature to a user's extension.	P	
7b	Listen to voicemail using OWA's Play-On-Phone feature to an external number.	P	
8	Configure a button on the phone of a UM-enabled user to forward the user to the pilot number. Press the voicemail button. Confirm you are sent to the prompt: "Welcome, you are connected to Microsoft Exchange. <User>. Please enter your pin and press the pound key."	P	
9	Send a test FAX message to user extension.	P	

	Confirm the FAX is received in the user's inbox.		
10	<p>Setup TLS between gateway/IP-PBX and Exchange UM.</p> <p>Replace this italicized text with your TLS configuration: self-signed certificates or Windows Certificate Authority (CA).</p>		
10a	<p>Dial the pilot number and logon to a user's mailbox.</p> <p>Confirm UM answers the call and confirm UM responds to DTMF input.</p>		The gateway supports TLS. However, TLS implementation is currently being tested.
10b	<p>Dial a user extension and leave a voicemail.</p> <p>Confirm the user receives the voicemail.</p>		The gateway supports TLS. However, TLS implementation is currently being tested.
10c	<p>Send a test FAX message to user extension.</p> <p>Confirm the FAX is received in the user's inbox.</p>		The gateway supports TLS. However, TLS implementation is currently being tested.
11	<p>Setup G.723.1 on the gateway. (If already using G.723.1, setup G.711 A Law or G.711 Mu Law for this step).</p> <p>Dial the pilot number and confirm the UM system answers the call.</p>	P	
12	<p>Setup Message Waiting Indicator (MWI).</p> <p>Geomant offers a third party solution: MWI 2007. Installation files and product documentation can be found on Geomant's MWI 2007 website.</p>	P	
13	Execute Test-UMConnectivity.	NT	
14	Setup and test fail-over configuration on the IP-PBX to work with two UM servers.	NA	

6.1. Detailed Description of Limitations

Failure Point	None
Phone type (if phone-specific)	
Call scenarios(s) associated with failure point	
List of UM features affected by failure point	
Additional Comments	

7. Troubleshooting

The tools used for debugging include network sniffer applications (such as Ethereal) and AudioCodes' Syslog protocol.

The Syslog client, embedded in the AudioCodes gateways (MP-11x, Mediant 1000, and Mediant 2000), sends error reports/events generated by the gateway application to a Syslog server, using IP/UDP protocol.

To activate the Syslog client on the AudioCodes gateways:

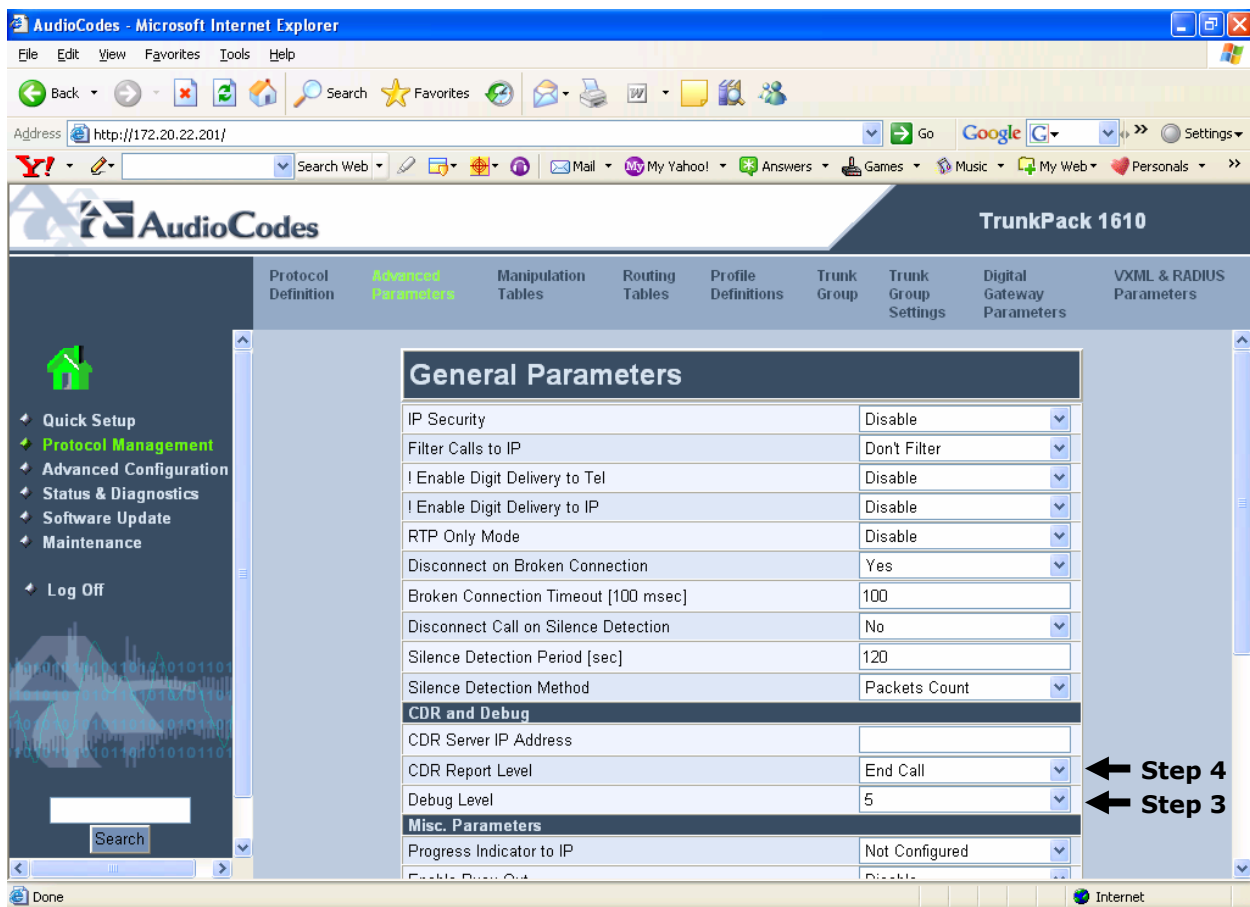
1. Set the parameter **Enable Syslog** to 'Enable'.
2. Use the parameter **Syslog Server IP Address** to define the IP address of the Syslog server you use.

The screenshot shows the AudioCodes TrunkPack 1610 MG Module 1 web interface. The left sidebar contains a navigation menu with options: Quick Setup, Protocol Management, Advanced Configuration (highlighted), Status & Diagnostics, Software Update, Maintenance, and Log Off. The main content area is titled 'Management Settings' and contains several sections: Syslog Settings, SNMP Settings, and Activity Types to Report via 'Activity Log' Messages. The Syslog Settings section includes the following fields: Syslog Server IP Address (10.15.2.5), Syslog Server Port (514), and Enable Syslog (a dropdown menu set to 'Enable'). The SNMP Settings section includes: SNMP Managers Table, SNMP Community String, SNMP V3 Table, Enable SNMP (a dropdown menu set to 'Enable'), and Trap Manager Host Name. The Activity Types to Report via 'Activity Log' Messages section includes: Parameters Value Change, Auxiliary Files Loading, Device Reset, Flash Memory Burning, and Device Software Update. Arrows point to the 'Enable Syslog' dropdown (labeled 'Step 1') and the 'Syslog Server IP Address' field (labeled 'Step 2').

Management Settings	
Syslog Settings	
Syslog Server IP Address	10.15.2.5
Syslog Server Port	514
Enable Syslog	Enable
SNMP Settings	
SNMP Managers Table	-->
SNMP Community String	-->
SNMP V3 Table	-->
Enable SNMP	Enable
Trap Manager Host Name	
Activity Types to Report via 'Activity Log' Messages	
Parameters Value Change	<input type="checkbox"/>
Auxiliary Files Loading	<input type="checkbox"/>
Device Reset	<input type="checkbox"/>
Flash Memory Burning	<input type="checkbox"/>
Device Software Update	<input type="checkbox"/>

Note: The Syslog Server IP address must be one that corresponds to your network environment in which the Syslog server is installed (for example, 10.15.2.5).

3. To determine the Syslog logging level, use the parameter **Debug Level** and set this parameter to '5'.
4. Change the **CDR Report Level** to 'End Call' to enable additional call information.



AudioCodes has also developed advanced diagnostic tools that may be used for high-level troubleshooting. These tools include the following:

- PSTN Trace: PSTN Trace is a procedure used to monitor and trace the PSTN elements (E1/T1) in AudioCodes digital gateways (Mediant 1000 & Mediant 2000). These utilities are designed to convert PSTN trace binary files to textual form.
- DSP Recording: DSP recording is a procedure used to monitor the DSP operation (e.g., rtp packets and events).

Appendix

1. Dial Pilot Number and Mailbox Login

- Dial the pilot number of the UM server from an extension that is NOT enabled for UM.
- Confirm hearing the greeting prompt: "Welcome, you are connected to Microsoft Exchange. To access your mailbox, enter your extension..."
- Enter the extension, followed by the mailbox PIN of an UM-enabled user.
- Confirm successful logon to the user's mailbox.

2. Navigate Mailbox using Voice User Interface (VUI)

- Logon to a user's UM mailbox.
- If the user preference has been set to DTMF tones, activate the Voice User Interface (VUI) under personal options.
- Navigate through the mailbox and try out various voice commands to confirm that the VUI is working properly.
- This test confirms that the RTP is flowing in both directions and speech recognition is working properly.

3. Navigate Mailbox using Telephony User Interface (TUI)

- Logon to a user's UM mailbox.
- If the user preference has been set to voice, press "#0" to activate the Telephony User Interface (TUI).
- Navigate through the mailbox and try out the various key commands to confirm that the TUI is working properly.
- This test confirms that both the voice RTP and DTMF RTP (RFC 2833) are flowing in both directions.

4. Dial User Extension and Leave Voicemail

- Note: If you are having difficulty reaching the user's UM voicemail, verify that the coverage path for the UM-enabled user's phone is set to the pilot number of the UM server.

a. From an Internal Extension

- a. From an internal extension, dial the extension for a UM-enabled user and leave a voicemail message.
- b. Confirm the voicemail message arrives in the called user's inbox.
- c. Confirm this message displays a valid Active Directory name as the sender of this voicemail.

b. From an External Phone

- a. From an external phone, dial the extension for a UM-enabled user and leave a voicemail message.
- b. Confirm the voicemail message arrives in the called user's inbox.
- c. Confirm this message displays the phone number as the sender of this voicemail.

5. Dial Auto Attendant(AA)

- Create an Auto Attendant using the Exchange Management Console:
 - a. Under the Exchange Management Console, expand "Organizational Configuration" and then click on "Unified Messaging".
 - b. Go to the Auto Attendant tab under the results pane.
 - c. Click on the "New Auto Attendant..." under the action pane to invoke the AA wizard.
 - d. Associate the AA with the appropriate dial plan and assign an extension for the AA.
 - e. Create PBX dialing rules to always forward calls for the AA extension to the UM server.
 - f. Confirm the AA extension is displayed in the diversion information of the SIP Invite.
- Dial the extension of Auto Attendant.
- Confirm the AA answers the call.

6. Call Transfer by Directory Search

- Method one: Pilot Number Access
 - Dial the pilot number for the UM server from a phone that is NOT enabled for UM.
 - To search for a user by name:
 - Press # to be transferred to name Directory Search.
 - Call Transfer by Directory Search by entering the name of a user in the same Dial Plan using the telephone keypad, last name first.
 - To search for a user by email alias:
 - Press "# " to be transferred to name Directory Search
 - Press "# #" to be transferred to email alias Directory Search
 - Call Transfer by Directory Search by entering the email alias of a user in the same Dial Plan using the telephone keypad, last name first.
- Method two: Auto Attendant
 - Follow the instructions in appendix section 5 to setup the AA.
 - Call Transfer by Directory Search by speaking the name of a user in the same Dial Plan. If the AA is not speech enabled, type in the name using the telephone keypad.

- Note: Even though some keys are associated with three or four numbers, for each letter, each key only needs to be pressed once regardless of the letter you want. Ignore spaces and symbols when spelling the name or email alias.

a. Called Party Answers

- Call Transfer by Directory Search to a user in the same dial plan and have the called party answer.
- Confirm the call is transferred successfully.

b. Called Party is Busy

- Call Transfer by Directory Search to a user in the same dial plan when the called party is busy.
- Confirm the calling user is routed to the correct voicemail.

c. Called Party does not Answer

- Call Transfer by Directory Search to a user in the same dial plan and have the called party not answer the call.
- Confirm the calling user is routed to the correct voicemail.

d. The Extension is Invalid

- Assign an invalid extension to a user in the same dial plan. An invalid extension has the same number of digits as the user's dial plan and has not been mapped on the PBX to any user or device.
 - a. UM Enable a user by invoking the "Enable-UMMailbox" wizard.
 - b. Assign an unused extension to the user.
 - c. Do not map the extension on the PBX to any user or device.
 - d. Call Transfer by Directory Search to this user.
 - e. Confirm the call fails and the caller is prompted with appropriate messages.

7. Play-On-Phone

- To access play-on-phone:
 - a. Logon to Outlook Web Access (OWA) by going to URL <https://<server name>/owa>.
 - b. After receiving a voicemail in the OWA inbox, open this voicemail message.
 - c. At the top of this message, look for the Play-On-Phone field (Play on Phone...).
 - d. Click this field to access the Play-On-Phone feature.

a. To an Internal Extension

- Dial the extension for a UM-enabled user and leave a voicemail message.
- Logon to this called user's mailbox in OWA.

- Once it is received in the user's inbox, use OWA's Play-On-Phone to dial an internal extension.
- Confirm the voicemail is delivered to the correct internal extension.

b. To an External Phone number

- Dial the extension for a UM-enabled user and leave a voicemail message.
- Logon to the UM-enabled user's mailbox in OWA.
- Confirm the voicemail is received in the user's mailbox.
- Use OWA's Play-On-Phone to dial an external phone number.
- Confirm the voicemail is delivered to the correct external phone number.
- Troubleshooting:
 - a. Make sure the appropriate UMMailboxPolicy dialing rule is configured to make this call. As an example, open an Exchange Management Shell and type in the following commands:
 - b. `$dp = get-umdialplan -id <dial plan ID>`
 - c. `$dp.ConfiguredInCountryOrRegionGroups.Clear()`
 - d. `$dp.ConfiguredInCountryOrRegionGroups.Add("anywhere,*,*,")`
 - e. `$dp.AllowedInCountryOrRegionGroups.Clear()`
 - f. `$dp.AllowedInCountryOrRegionGroups.Add("anywhere")`
 - g. `$dp|set-umdialplan`
 - h. `$mp = get-ummailboxpolicy -id <mailbox policy ID>`
 - i. `$mp.AllowedInCountryGroups.Clear()`
 - j. `$mp.AllowedInCountryGroups.Add("anywhere")`
 - k. `$mp|set-ummailboxpolicy`
 - l. The user must be enabled for external dialing on the PBX.
 - m. Depending on how the PBX is configured, you may need to prepend the trunk access code (e.g. 9) to the external phone number.

8. Voicemail Button

- Configure a button on the phone of a UM-enabled user to route the user to the pilot number of the UM server.
- Press this voicemail button on the phone of an UM-enabled user.
- Confirm you are sent to the prompt: "Welcome, you are connected to Microsoft Exchange. <User Name>. Please enter your pin and press the pound key."
- Note: If you are not hearing this prompt, verify that the button configured on the phone passes the user's extension as the redirect number. This means that the user extension should appear in the diversion information of the SIP invite.

9. FAX

- Use the Management Console or the Management Shell to FAX-enable a user.
- Management Console:
 - a. Double click on a user's mailbox and go to Mailbox Features tab.
 - b. Click Unified Messaging and then click the properties button.
 - c. Check the box "Allow faxes to be received".
- Management Shell - execute the following command:
 - a. Set-UMMailbox -identity UMUser -FaxEnabled:\$true
- To test fax functionality:
 - a. Dial the extension for this fax-enabled UM user from a fax machine.
 - b. Confirm the fax message is received in the user's inbox.
 - c. Note: You may notice that the UM server answers the call as though it is a voice call (i.e. you will hear: "Please leave a message for..."). When the UM server detects the fax CNG tones, it switches into fax receiving mode, and the voice prompts terminate.
 - d. Note: UM only support T.38 for sending fax.

10.TRANSPORT SECURITY LAYER (TLS)

- Setup TLS on the gateway/IP-PBX and Exchange 2007 UM.
- Import/Export all the appropriate certificates.

a. Dial Pilot Number and Mailbox Login

- Execute the steps in scenario 1 (above) with TLS turned on.

b. Dial User Extension and Leave a Voicemail

- Execute the steps in scenario 4 (above) with TLS turned on.

c. FAX

- Execute the steps in scenario 9 (above) with TLS turned on.

11.G.723.1

- Configure the gateway to use the G.723.1 codec for sending audio to the UM server.
- If already using G.723.1 for the previous set of tests, use this step to test G.711 A Law or G.711 Mu Law instead.
- Call the pilot number and verify the UM server answers the call.
- Note: If the gateway is configured to use multiple codecs, the UM server, by default, will use the G.723.1 codec if it is available.

12.Message Waiting Indicator (MWI)

- Although Exchange 2007 UM does not natively support MWI, Geomant has created a 3rd party solution - MWI2007. This product also supports SMS message notification.
- Installation files and product documentation can be found on Geomant's [MWI 2007 website](#).

13.Test-UMConnectivity

- Run the Test-UMConnectivity diagnostic cmdlet by executing the following command in Exchange Management Shell:
- Test-UMConnectivity -UMIPGateway:<Gateway> -Phone:<Phone> |fl
- <Gateway> is the name (or IP address) of the gateway which is connected to UM, and through which you want to check the connectivity to the UM server. Make sure the gateway is configured to route calls to UM.
- <Phone> is a valid UM extension. First, try using the UM pilot number for the hunt-group linked to the gateway. Next, try using a CFNA number configured for the gateway. Please ensure that a user or an AA is present on the UM server with that number.
- The output shows the latency and reports if it was successful or there were any errors.

14.Test Fail-Over Configuration on IP-PBX with Two UM Servers

- This is only required for direct SIP integration with IP-PBX. If the IP-PBX supports fail-over configuration (e.g., round-robin calls between two or more UM servers):
 - a. Provide the configuration steps in Section 5.
 - b. Configure the IP-PBX to work with two UM servers.
 - c. Simulate a failure in one UM server.
 - d. Confirm the IP-PBX transfers new calls to the other UM server successfully.