Microsoft Exchange Server 2010 Unified Messaging

PBX Configuration Note:

Direct SIP Connection with Avaya Communication Server 2100 SE13

By : Avaya

Updated : 9/6/2011

IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

1. Document Overview

Content

This document describes the configuration required to setup Avaya Communication Server 2100, release SE13 with Exchange 2010 Unified Messaging using SIP connection through the Session Server Trunking (SST). It also contains the results of the interoperability testing 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 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 a Microsoft Exchange 2010 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 2010 Unified Messaging (UM) Specialists

These are Systems Integrators who have attended technical training on Exchange 2010 Unified Messaging conducted by Microsoft Exchange Engineering Team. For contact information, visit here.

Version Information

Date of Modification	**Details of Modification**
September 6, 2011	First Document

2. Component Information

PBX or IP-PBX

PBX Vendor	Avaya
Model	CS 2100
Software Version	CS2100 SE13
Telephony Signaling	Direct SIP connection through Avaya CS2100 Session Server Trunking (SST)
Additional Notes	-

VoIP Gateway

Gateway Vendor	N.A.
Model	N.A.
Software Version	N.A.
VoIP Protocol	N.A.

Microsoft Exchange Server 2010 Unified Messaging

Version	Exchange Server 2010 Version: 14.01.0218.013

3. Prerequisites

Gateway Requirements

- N/A

PBX Requirements

The information in this document applies to Communication Server 2100 (CS 2100).

1. The CS 2100 requires software release SE13.
2. The SST will use SIP (RFC3261) to communicate with Exchange 2010. SDP and RTP will be used for the call and carried over SIP to Exchange.
3. If Geographic Redundancy is required, a pair of Exchange 2010 SP servers and geographic redundant SST units will be required.

Cabling Requirements

- N/A

4. Summary and Limitations

☐ A check in this box indicates the UM feature set is fully functional (both, mandatory and additional, tests passed) when using the PBX/gateway in question.

1. Codec support
    a. G.711 is the only supported codec between CS 2100 and the Microsoft Exchange UM.
    b. The Centrex IP Client Manager (CICM) can accept calls having a packet time of 30ms if the CICM is configured to accept a packet time of 30 ms as a primary or secondary packet time in the audio profile.

2. RFC2833 is required for DTMF digit transmission to Microsoft Exchange UM. The effect of not supporting RFC2833 is that a user will not be able to login to Microsoft Exchange UM and navigate the UM menus, through the telephony client. The CS 2100 components listed below do not support RFC2833:

    a. Media Gateway 9000 (MG 9000)—all subtending nodes, ABI and Native lines (are supported through a workaround of provisioning loop around trunks which provides a conversion from RFC2833 to Inband DTMF digit transmission).
    b. MG 9000—Play on Phone is not supported from Exchange to an MG 9000 because the MG 9000 does not support RFC2833. Since DTMF is not supported by the MG 9000, the SDP sent from the MG 9000 to Exchange does not contain the necessary payload information.
    c. The Attendant Console is not supported.

       (Nortel's Meridian M2250 Digital Attendant Console delivers high-speed call processing and transforms the attendant position into a call answering and message center that manages and streamlines attendant services. The PC Console Interface Unit delivers the features and capabilities of the M2250 Attendant Console using a 3rd party PC-based console.)
    d. H.323 trunking between the CS 1000 and CS 2100 is not supported.
    e. H.323 trunking between the Business Communication Manager (BCM)/Survivable Remote Gateway (SRG) and CS 2100 is not supported.

3. Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) are not supported between the CS 2100 and the UM.
4. For Media Portal insertion to occur for calls to Microsoft Exchange UM, the SIP Trunk must be provisioned on the CS 2100 as an inter-domain trunk, along with the normal client media-insertion rules. With the SIP Trunk provisioned as inter-domain, all calls to Microsoft Exchange UM will attempt to insert the Media Portal and is independent of whether the Media Portal is required, i.e. Network Address Translation (NAT).

(Media Portal insertion is a function of the Real-time Transport Protocol (RTP) Media Portal, an optional media proxy device that provides a variety of functions that overcome obstacles to the general deployment of next-generation multimedia services. When an RTP Media Portal is required to facilitate a successful multimedia session, an available RTP Media Portal must be selected. The RTP Media Portal Insertion Rules are used to determine when an RTP Media Portal is required to facilitate successful multimedia communications.)

5. Microsoft Exchange UM does not support a value of c=0.0.0.0 in the SDP portion of a SIP Invite message. This corresponds to the SDP line "Connection Information (c): IN IP4 0.0.0.0" that is utilized to execute certain call processing features. This condition impacts multiple call scenarios not supported due to this limitation, as they interact with Microsoft UM. The current list of known features impacted by this issue follows:
    a. Hold/Retrieve
    b. Call Transfer
    c. Conference
    d. Attendant Console
    e. Release Link Trunk (RLT)
6. The E.164 dialing format is the recommended configuration for the Microsoft Exchange UM. The Microsoft Exchange UM and CS 2100 configuration has been validated using the E.164 format. An alternative dialing format that can be used with Exchange UM is a Private dialing format using a URI type of "Telephone Extension". Minimal validation has been done with the Microsoft Exchange UM and a CS 2100 configuration using a 7-digit Private dialing plan.
    a. In Order to make outbound calls from Microsoft Exchange UM using the E.164 format, translations on the CS 2100 must be configured for E.164
    b. The BCM50/SRG50 does not support E.164 to Microsoft Exchange UM, as it does not send a 10-digit OCN on a redirected call. The BCM/SRG has not been validated in a hosted CS 2100 UM environment.
7. CS 2100 interoperability with redundant Microsoft Exchange UM servers.
    a. In a redundant configuration, when one of the Microsoft Exchange UM servers is no longer available to the network and a call is directed to that UM, there is approximately a seven-second delay in redirecting the call to the second Microsoft Exchange UM.
    b. A redundant configuration is limited to the configuration of an optional Remote SIP Server address in the SST Remote SIP Server configuration. Redundancy cannot be accomplished with the use of multiple trunk groups. The expected behavior of the SST, configured with two Remote SIP Server addresses, is that calls will alternate between the two addresses.
8. Microsoft Exchange UM provides several out-dialing capabilities (such as Play on Phone, transfer, etc.). Due to limitations/restrictions with billing within the CS2100 and the SST that do not allow the correct billing for diverted calls involving non-local calls, Avaya recommends that only local dialing be allowed between Microsoft Exchange UM and the CS 2100.

5. Gateway Setup Notes

- N/A

Configuration Files

- N/A

TLS and Setup

- 'Did not perform TLS and SRTP setup'.

SRTP Setup

- 'Did not perform TLS and SRTP setup'.

Call Transfer(Basic Transfer/Blind Transfer/Supervised Transfer settings)

- N/A

MWI settings

- N/A

6. PBX Setup Notes

CS 2100 Configuration Summary

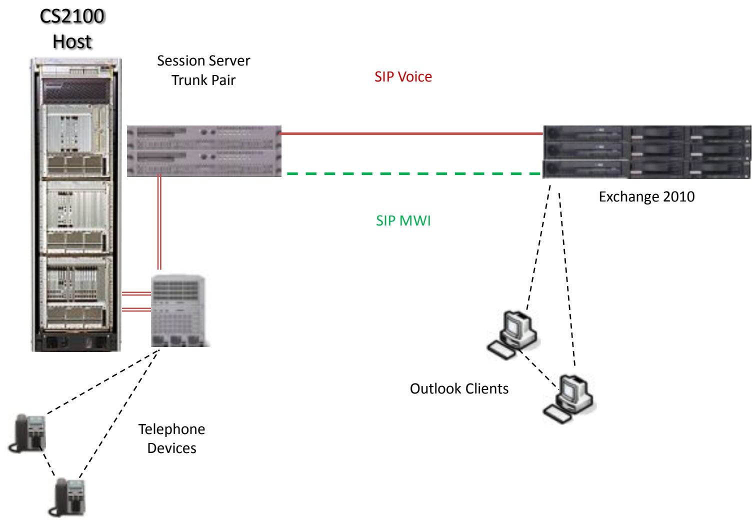


Figure 1 – Avaya CS 2100 and Microsoft Exchange 2010 UM Setup

Figure 1 summarizes the Unified Messaging setup used in this document. The following steps are required to enable Unified Messaging in a pre-configured CS 2100 SIP network:

- CS 2100 Configuration
- Gateway Controller Configuration
- SST Configuration
- Centrex IP Client Manager configuration
- Exchange 2010 Configuration

Configuration Assumptions

- CS 2100 is pre-configured to support IP Phones and Trunks.
- Exchange is configured with a UM Dial Plan and associated UMIPGateway object. The UMIPGateway object points to the IP address of the CS 2100 SIP Gateway.

CS 2100 Configuration

Prerequisites

CS 2100 switch load = SE13.

Table datafill

The following are examples of datafill used for configuring the CS 2100 in the Avaya test labs.

```
TABLE CLLI

ADD REGA2E2K7SST 202 0 EXCHANGE_UM
```

```
>TABLE CLLI


JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: CLLI


>ADD REGA2E2K7SST 202 0 EXCHANGE_UM


JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT


>Y


TUPLE TO BE ADDED:
   REGA2E2K7SST   202        0                 EXCHANGE_UM
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.


>Y


TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

```
TABLE TRKGRP


ADD REGA2E2K7SST IBNT2 0 ELO NCRT BNRRCH 0 MIDL 0 N +
ANSDISC 0 Y N N N N N N 0 1 N 0 0 0 0 N N N N N N N N N NATL $
```

```
CI:
```

```
>TABLE TRKGRP
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: TRKGRP
>ADD REGA2E2K7SST
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
GRPTYP:
>IBNT2
TRAFSNO:
>0
PADGRP:
>ELO
NCCLS:
>NCRT
CUSTNAME:
>BNRRCH
SUBGRPNO:
>0
SELSEQ:
>MIDL
NCOS:
>0
BILLDN:
>N
SUPV:
>ANSDISC
DISCTSEL:
>0
INTRAGRP:
>Y
DIGIT0:
>N
DIGIT1:
>N
DTI:
```

```
>N
TES:
>N
CDR:
>N
SMDR:
>N
TRC:
>0
ALTNCOS:
>1
TRKDSR:
>N
LSCFN:
>0
ALTLSCFN:
>0
LSCINCPT:
>0
ALSCINCP:
>0
IGA:
>N
FDN:
>N
FDV:
>N
FLASH:
>N
DPX:
>N
PREEMPT:
>N
AIOD:
>N
60REORIG:
```

```
>N
OFFNET:
>N
COFFTYP:
>NATL
OPTION:
>$
TUPLE TO BE ADDED:
   REGA2E2K7SST
      IBNT2 0 ELO NCRT BNRRCH 0 MIDL 0 N ANSDISC 0 Y N N N N N N
      0 1
             N 0 0 0 0 N N N N N N N N N NATL $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

TABLE TRKSGRP
ADD REGA2E2K7SST 0 DS1SIG C7UP 2W N N UNEQ NONE Q764 THRH 0 NIL $ NIL CIC

```
>TABLE TRKSGRP
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: TRKSGRP
>ADD REGA2E2K7SST 0 DS1SIG C7UP 2W N N UNEQ NONE Q764 THRH 0 NIL
$ NIL CIC
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
TUPLE TO BE ADDED:
   REGA2E2K7SST 0    DS1SIG    C7UP
2W N N UNEQ NONE Q764 THRH 0 NIL $ NIL CIC
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

TABLE TRKOPTS

ADD REGA2E2K7SST DPT DPT SIPT NET_IPY N

```
>TABLE DPTRKMEM
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: DPTRKMEM
>ADD REGA2E2K7SST SIPT 10
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
TUPLE TO BE ADDED:
   REGA2E2K7SST   SIPT   10
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

TABLE DPTRKMEM ADD REGA2E2K7SST SIPT 10

```
>TABLE IBNRTE
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: IBNRTE
>ADD  _ _2 N N N N N REGA2E2K7SST 751 $ $
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
TUPLE TO BE ADDED:
   2                                             (      N  N  N  N  N
REGA2E2K7SST   751)$

$
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

TABLE SIPLINK ADD REGATOE2K7LINK1 CS2CS ISUPTRK REGA2E2K7SST

```
>TABLE SIPLINK
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: SIPLINK
>ADD REGATOE2K7LINK1 CS2CS ISUPTRK REGA2E2K7SST
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
TUPLE TO BE ADDED:
 REGATOE2K7LINK1    CS2CS ISUPTRK    REGA2E2K7SST
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

TABLE IBNRTE ADD 2 N N N N N REGA2E2K7SST 751 $ $

```
>TABLE IBNRTE
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: IBNRTE
>ADD  _ _2 N N N N N REGA2E2K7SST 751 $ $
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
TUPLE TO BE ADDED:
   2                                           (      N N N N N
REGA2E2K7SST   751)$

$
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

TABLE IBNXLA ADD NRCH0 213 ROUTE N Y 0 N 5 12 NDGT Y T IBNRTE 2 $

```
>TABLE IBNXLA
```

```
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: IBNXLA
>ADD NRCH0 213 ROUTE N Y 0 N 5 12 NDGT Y T IBNRTE 2 $
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
TUPLE TO BE ADDED:
   NRCH0                 213
ROUTE N Y 0 N 5 12 NDGT Y T IBNRTE 2 $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

TABLE IBNRTE
ADD 3 N N N N N REGA2E2K7SST 0 $ $

```
>TABLE IBNRTE
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: IBNRTE
>ADD 3 N N N N N REGA2E2K7SST 0 $ $
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
TUPLE TO BE ADDED:
   3                                          (      N N N N N
REGA2E2K7SST     0)$

$
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

TABLE DNROUTE
ADD 214 997 9991 T IBNRTE 3
ADD 214 997 9992 T IBNRTE 3

```
>TABLE DNROUTE
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: DNROUTE
>ADD 214 997 9991 T IBNRTE 3
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
TUPLE TO BE ADDED:
     214      997        9991                                    T
IBNRTE    3
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
JOURNAL FILE INACTIVE
>ADD 214 997 9992 T IBNRTE 3
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
TUPLE TO BE ADDED:
     214      997        9992                                    T
IBNRTE    3
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

TABLE DIGMAN ADD 9 INC 214

```
>TABLE DIGMAN
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: DIGMAN
>ADD 9 INC 214
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
TUPLE TO BE ADDED:
```

```
      9
                                                  (            INC
214)$
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

Table MSGRTE

TABLE MSGRTE ADD PUBLIC 214997 214997 (SCTP 2 0 $ $) $

```
>TABLE MSGRTE
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: MSGRTE
>ADD PUBLIC 214997 214997 (sctp 2 0 $ $) $
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
TUPLE TO BE ADDED:
PUBLIC 214997 214997 (sctp 2 0 $ $) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

SOC MDC00078 NMS OVER IP (SCTP)

SELECT OPTION MDC00078 ASSIGN STATE ON TO MDC00078

```
>SOC
SOC:
>SOCDEBUG
SOCDEBUG:
>SELECT OPTION MDC00078 FULL

GROUP:MDC
```

```
OPTION    NAME                 RTU STATE   USAGE   LIMIT    UNITS
LAST_CHG
------    ----                 --- -----   -----   -----    -----
--------
MDC00078   NMS OVER IP(SCTP)        Y     OFF         -         -
-  07/11/08
          options needed:        NONE
          options not permitted: NONE
          replaces options:      NONE

          FEATURE   NAME                                    STATE
LAST_CHG
          -------   ----                                    -----
--------
          00007544  MDC NMS OVER IP(SCTP)                      ON
07/11/08
                features needed: NONE
                features not permitted:  NONE

>ASSIGN STATE ON TO MDC00078
Done.
>
```

1. Login to the CS 2100 CLI
2. Modify the datafill as indicated in the diagram above.

Gateway Controller Configuration

Prerequisites

- The Gateway controllers must be accessible on the network.

Supporting information

- The Gateway controllers must be in-service and on the network.
- Use the CS 2100 Management Tools to modify the gateway controller settings

Procedure outline

- Add/Modify the values as shown in the following procedure.

Procedure steps

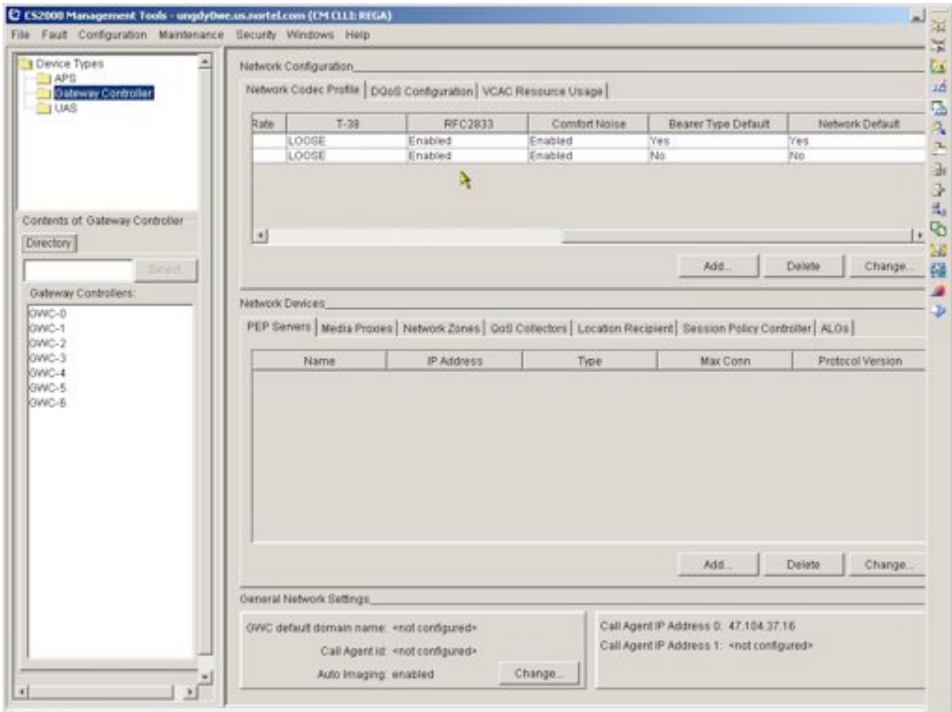


Figure 2 - CS 2100 Management Web Console

1. Login to the CS 2100 Management Web Console.
2. Select Gateway Controllers from the menu on the left.
3. Select the Network Codec Profile tab.
4. Change the SST's Gateway controller card to specify the following settings:
   a) T-38 – ON (Strict)
   b) RFC 2833 – Enabled
   c) Comfort Noise – Enabled
   d) Bearer Type Default – Yes
   e) Network Default - Yes

SST Configuration

- Prerequisites for Session Server Trunks (SST) configuration
  - Upgrade SST load to version 10.2_MB_Bld_43_b or higher
- Procedure outline
  - Login to SST element manager web application using IE 6.0 or above
  - Add a new SIP Server to communicate with Exchange 2010
  - Modify the following values as indicated below

Add Remote SIP Server for Exchange

1. Login to the SST Management console.

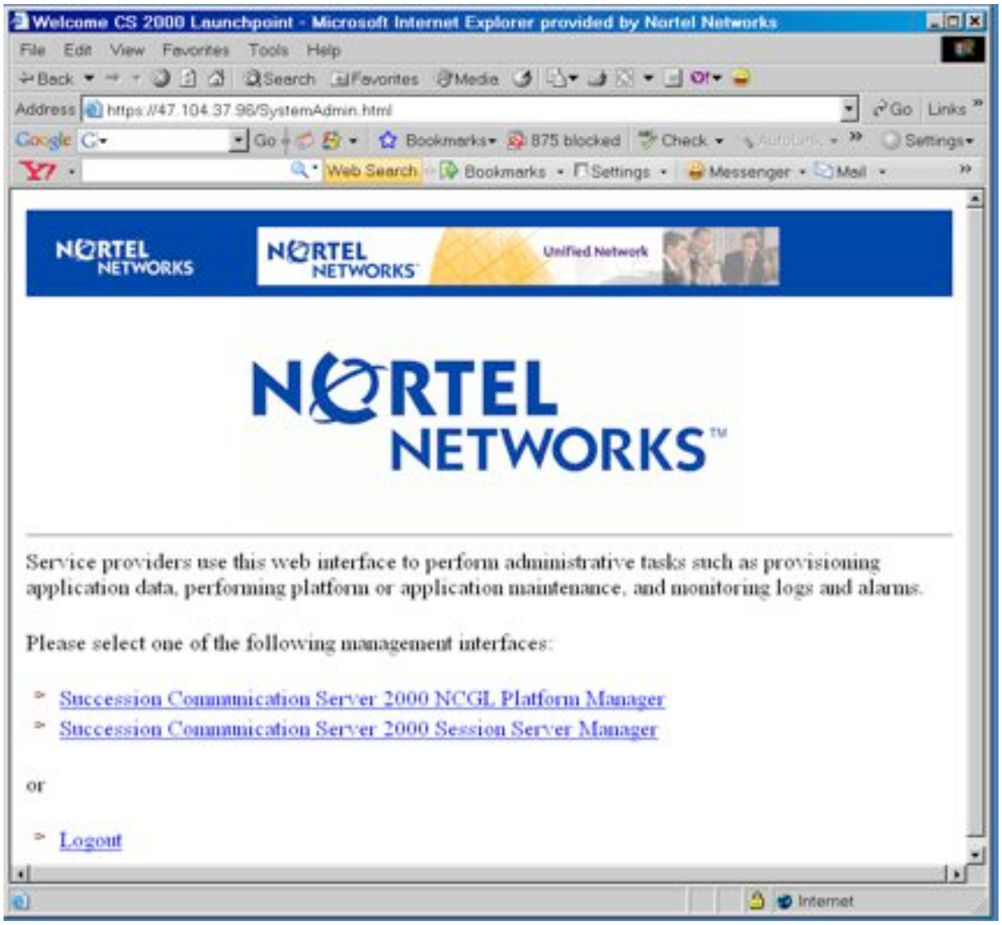


Figure 3 - SST Element Manager

2. Select the "Succession Communication Server 2000 Session Server Manager" management interface.

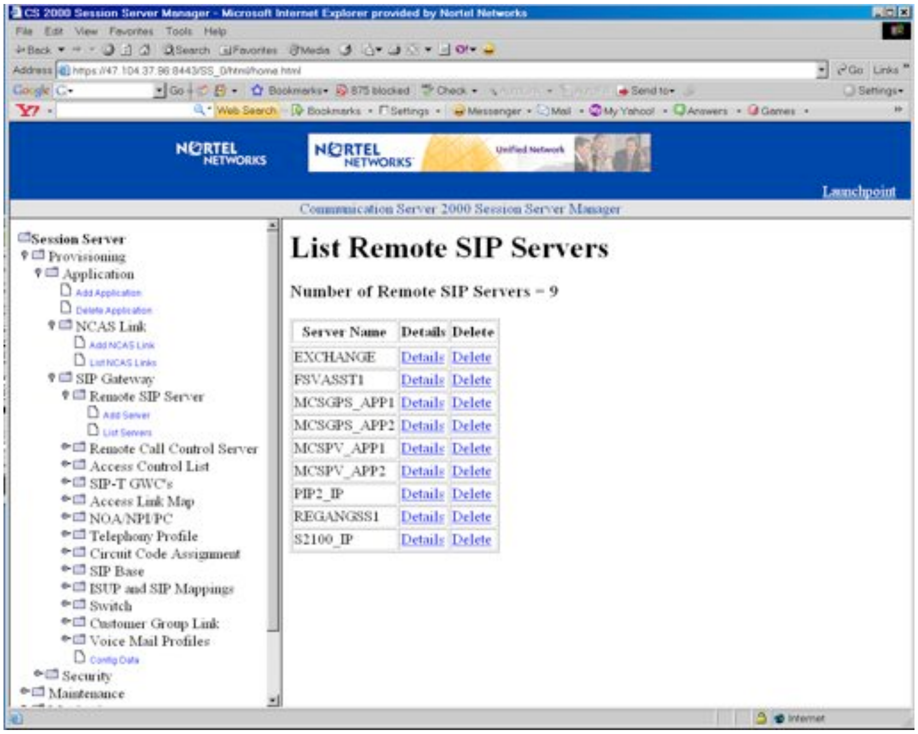


Figure 4 - List Remote SIP Servers

3. From the tree menu, open the SIP Gateway menu, then the Remote SIP Server menu.
4. Select the "Add Server" option if this is a new Exchange Server interface; or "List Servers" if the Exchange Server has already been added.

Figure 5 - SST - Modify a SIP Server (1)

5. Select "Session Server" as the Server Type.
6. Set the IP Address to the Exchange Server's IP Address.
7. Set the Port to 5060 and the Protocol to TCP.
8. Select Modify to save the settings.
9. Select the following Methods Supported: INVITE, CANCEL, BYE, OPTIONS, NOTIFY, REFER, PRACK.
10. SIP Header's supported should be set to: Content-Disposition, P-Asserted-ID, Privacy, Reason, Replace, and Referred-By, Diversion.

Figure 6 - SST Modify a SIP Server (2)

11. Select the following URI Parameters Supported: CIC, RN, NPDI, Phone-Context
12. Select "Long" SIP Header Format.
13. Select "Yes" for Use Options for Heartbeat.
14. Select "ReInvite" for Post-Answer Media Exchange.
15. Select "No" for Telephony Profile Support.
16. Select "Yes" for Accepts Early SDP.
17. Select "No" for Invite without SDP.
18. Select "No" for Enforce CODEC-Compatibility.
19. Select "No" for Accepts Encapsulated ISUP.
20. Select "Yes" for Conn Mode Allowed.
21. Select "No" for OCN and Header Interworking.
22. Select "No" for Default 183.
23. Select "No" for Re-Invite for Voice Band Data.
24. Select "Yes" for Enhanced Media Cut Through.
25. Select "No" for MBG Supported.
26. Select "Yes" for PRACK with SDP supported.

27. Select "Yes" for Auto-subscribe.
28. Select "Yes" for Retain Contact Info.
29. Select "No" for Validate Requested URI.
30. Select "No" for 2 CLI Supported.
31. Select "No" for Use Network Number.
32. Select "Yes" for E.164 Format Allowed.

    Note: If using a non-E.164 dialing plan as described in step 6 of the **Error! Reference source not found.Error! Reference source not found.**Summary and Limitations section, select "No" for E.164 format allowed.

33. Select "No" for Use DefaultLD for LD Calls.
34. Set Country Code to "1" for United States. (Use appropriate code if outside United States).

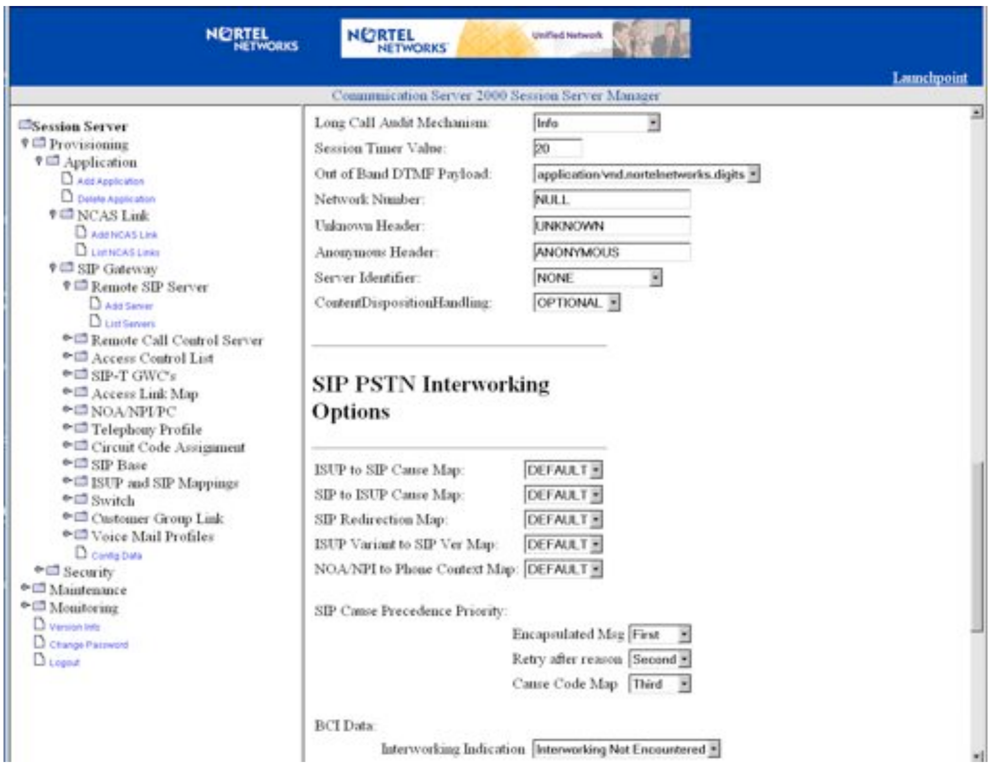


Figure 7 – SST - Modify a SIP Server (3)

35. Select "Info" for Long Call Audit Mechanism.
36. Set Session Timer Value to "20".
37. Set Out of Band DMTF Payload to "application/vnd.nortelnetworks.digits".
38. Set Network Number to NULL.
39. Set Unknown Header to UNKNOWN.

40. Set Anonymous Header to ANONYMOUS.
41. Set Server Identifier to NONE.
42. Set Content Disposition Handling to OPTIONAL.
43. Set all Options Maps to DEFAULT.
44. Set Encapsulated Msg to First.
45. Set Retry after Reason to Second.
46. Set Cause Code Map to Third.
47. Set Interworking Indication to Interworking Not Encountered.

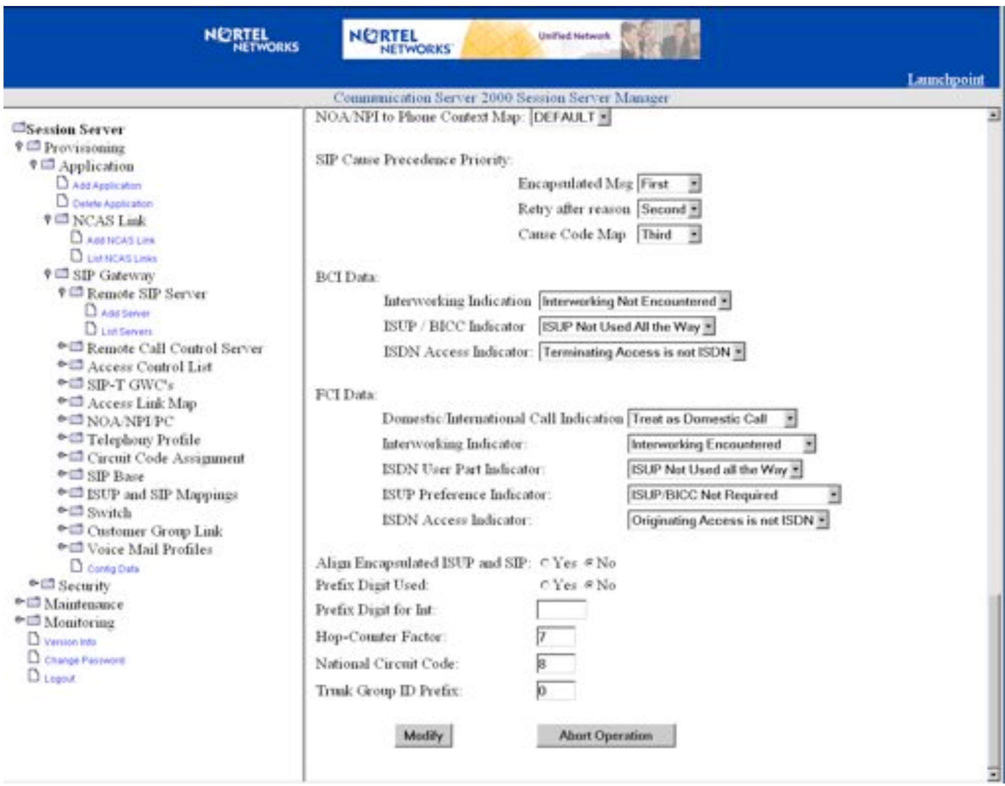


Figure 8 - SST Modify a SIP Server (4)

48. Set ISUP / BICC Indicator to Interworking Not Encountered.
49. Set ISDN Access Indicator to Terminating Access is not ISDN.
50. Set Domestic / International Call Indication to Treat as Domestic Call.
51. Set Interworking Indicator to Interworking Encountered.
52. Set ISDN User Part Indicator to ISUP Not Used all the Way.
53. Set ISDN Access Indicator to Originating Access is not ISDN.
54. Set Align Encapsulated ISUP and SIP to No.
55. Set Prefix Digit for Int to <Nothing>.

56. Set Hop-Counter Factor to 7.

57. Set National Circuit Code to 8.

58. Set Trunk Group ID Prefix to 0.

59. Select Modify to save the settings.

Add NGSS Loop-around Remote SIP Server

An NGSS loop-around server is required for Exchange to support out-dialing for scenarios such as transfers and Play-On-Phone.

Note: The current name for NGSS is Session Server Trunking (SST)

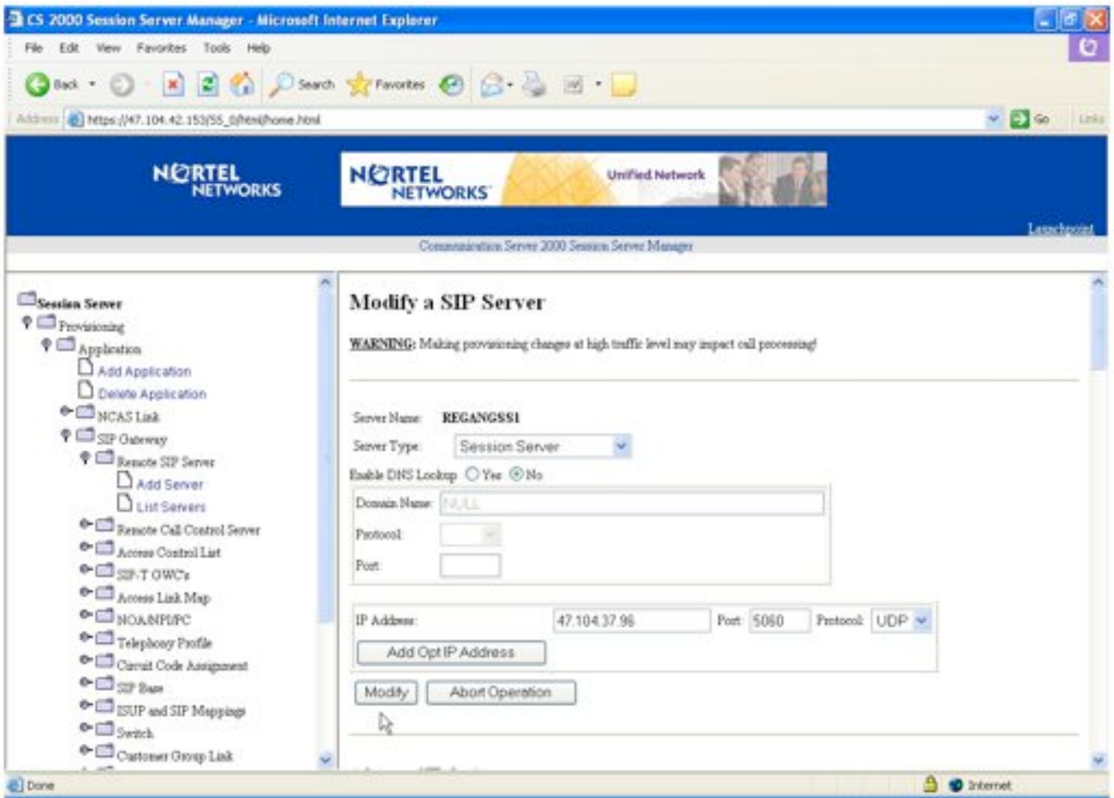


Figure 9 - Modify a SIP Server

1. Follow the previous steps to add a loop-around Remote SIP Server with the address of the NGSS server.

2. Select the options as indicated above

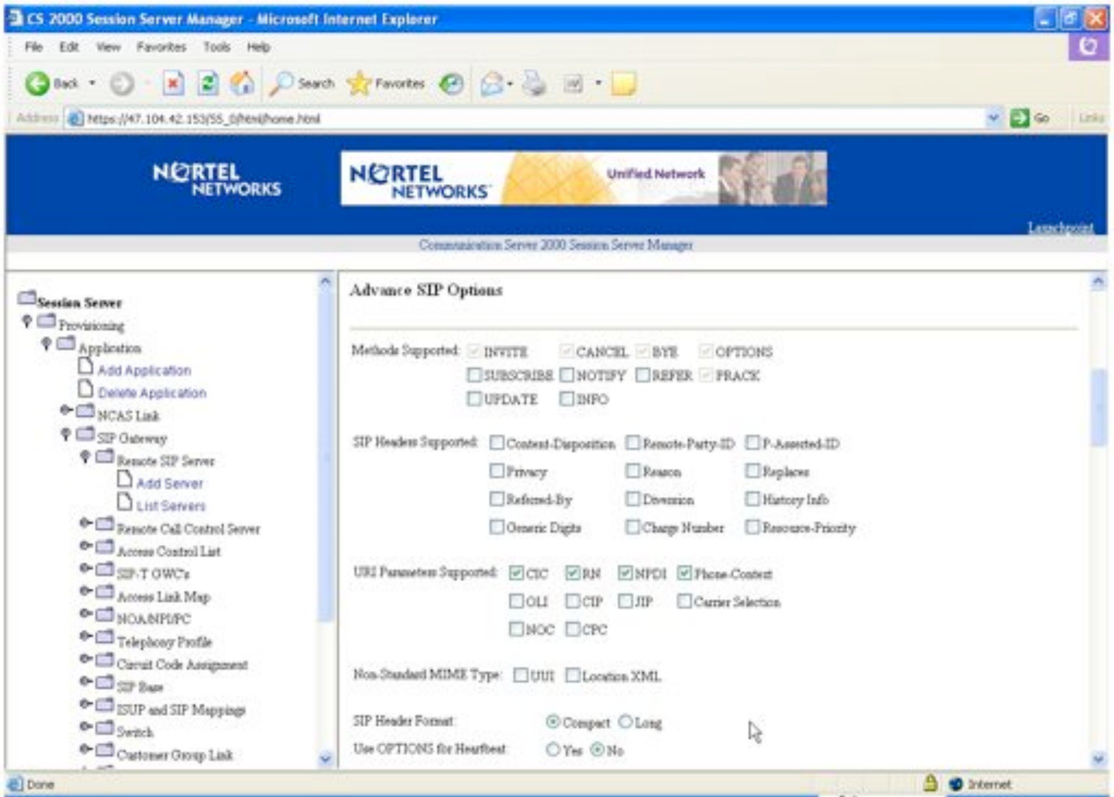


Figure 10 – Advance SIP options (1)

3. Select the Advance SIP options as indicated above.

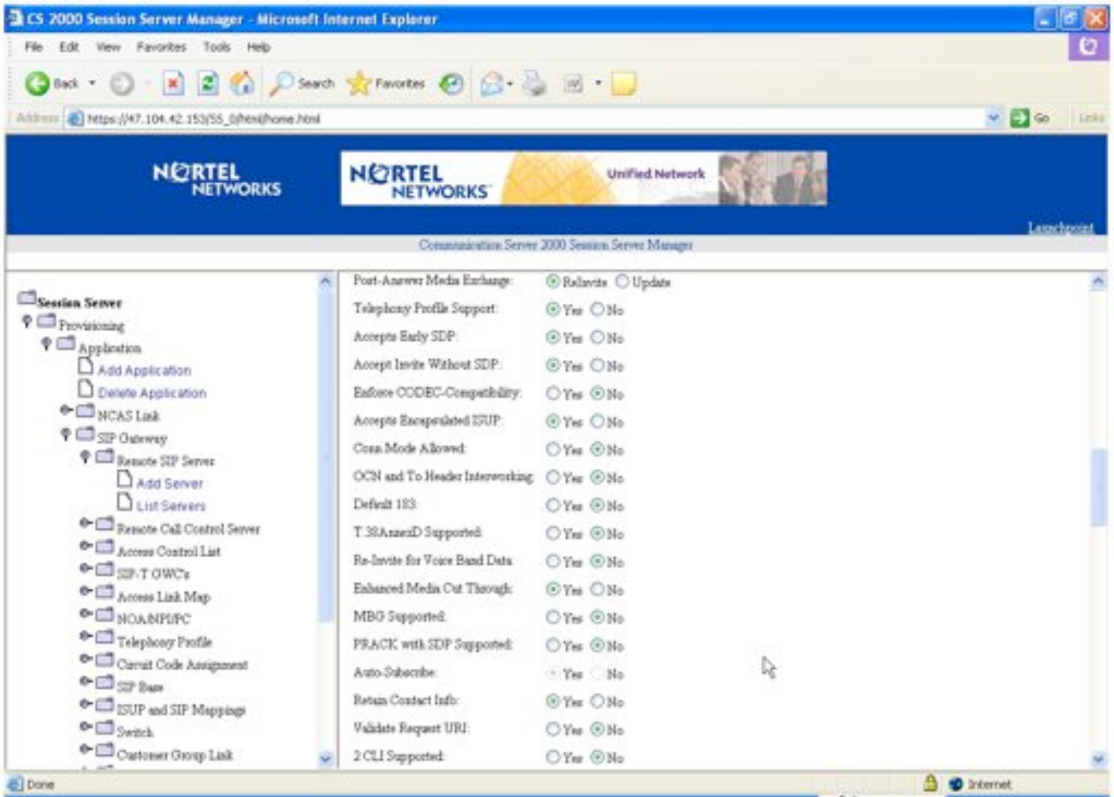


Figure 11 - Advance SIP options (2)

4. Select the next Advance SIP options as indicated above.

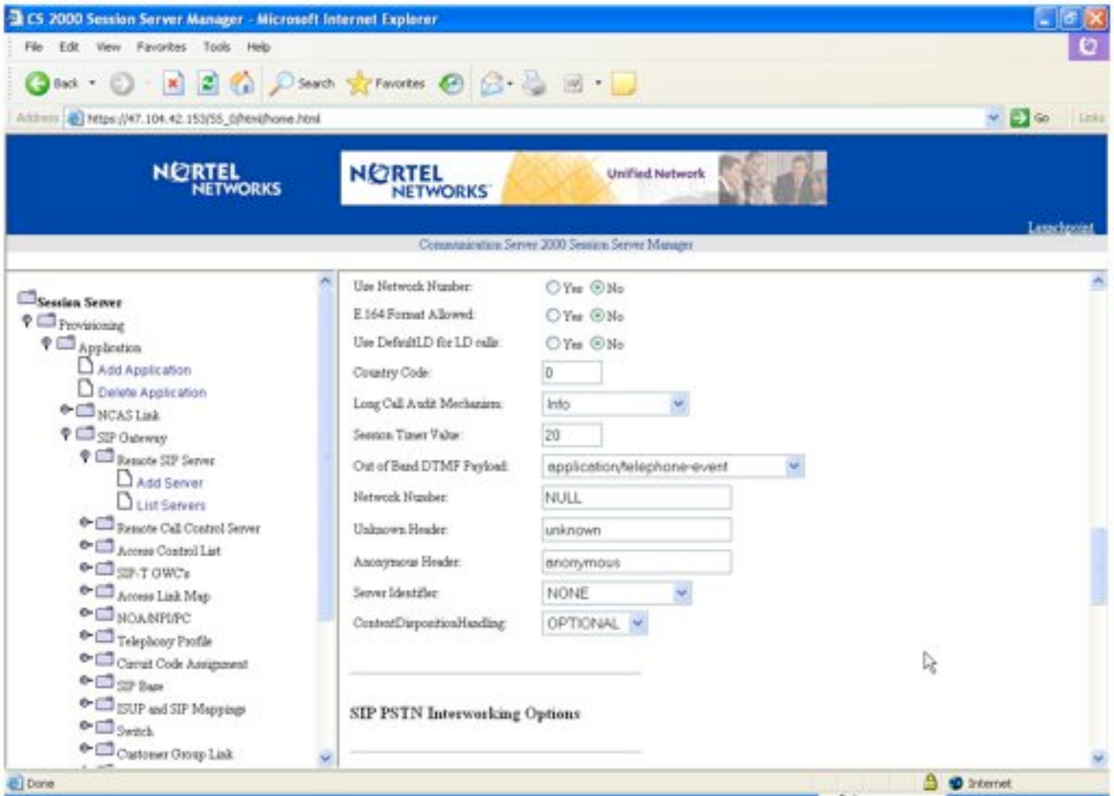


Figure 12 - Advance SIP options (3)

5. Select the next Advance SIP options as indicated above.

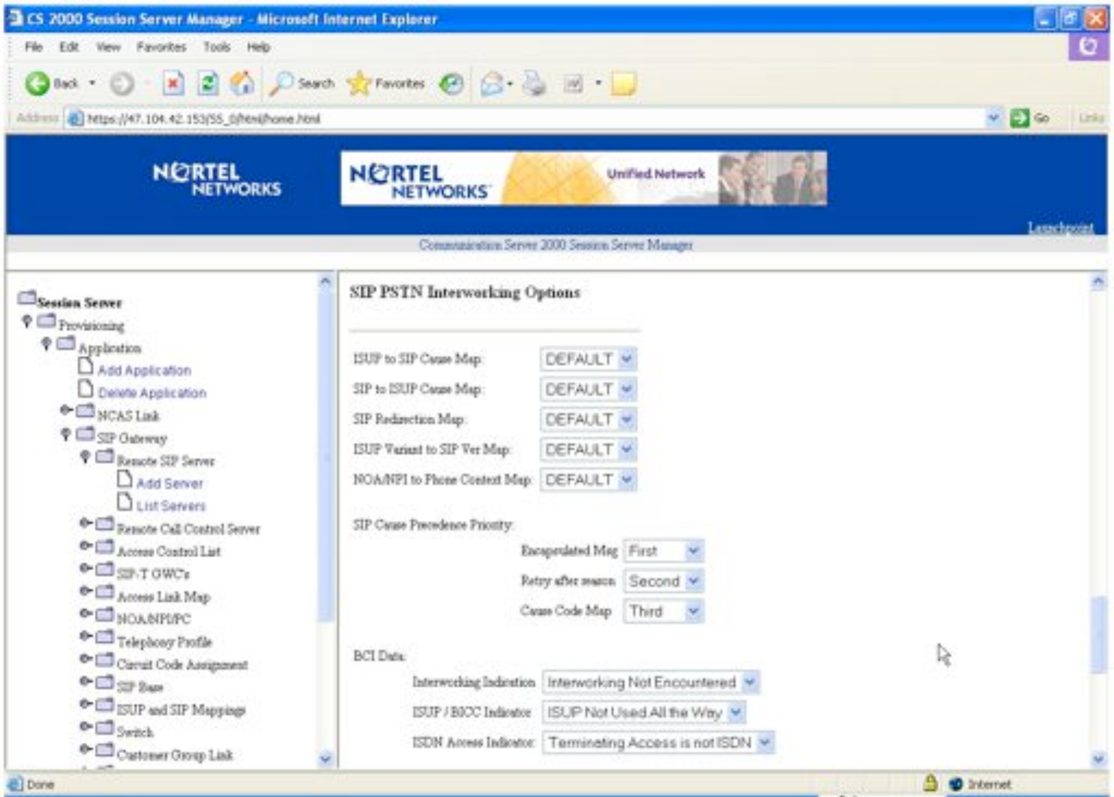


Figure 13 - SIP PSTN options (1)

6. Select the SIP PSTN options as indicated above.

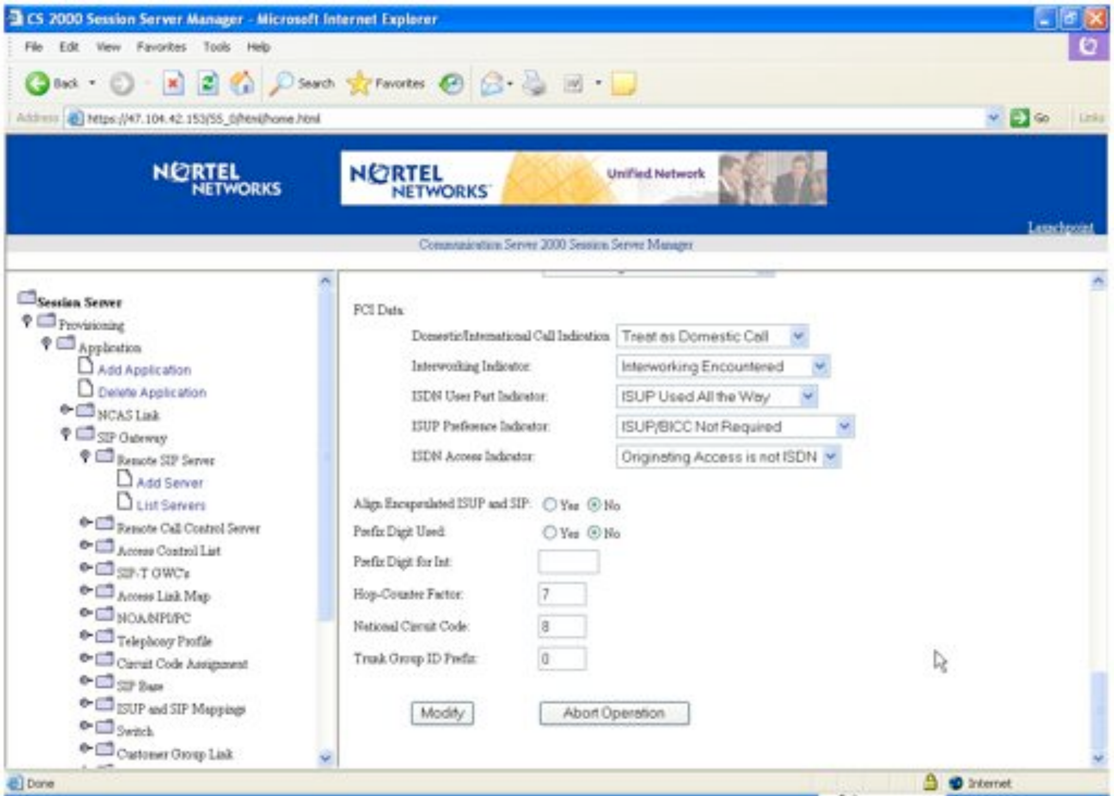


Figure 14 - PSTN SIP options (2)

7. Select the next PSTN SIP options as indicated above.
8. Select Modify to save the settings

Add NCAS link for MWI

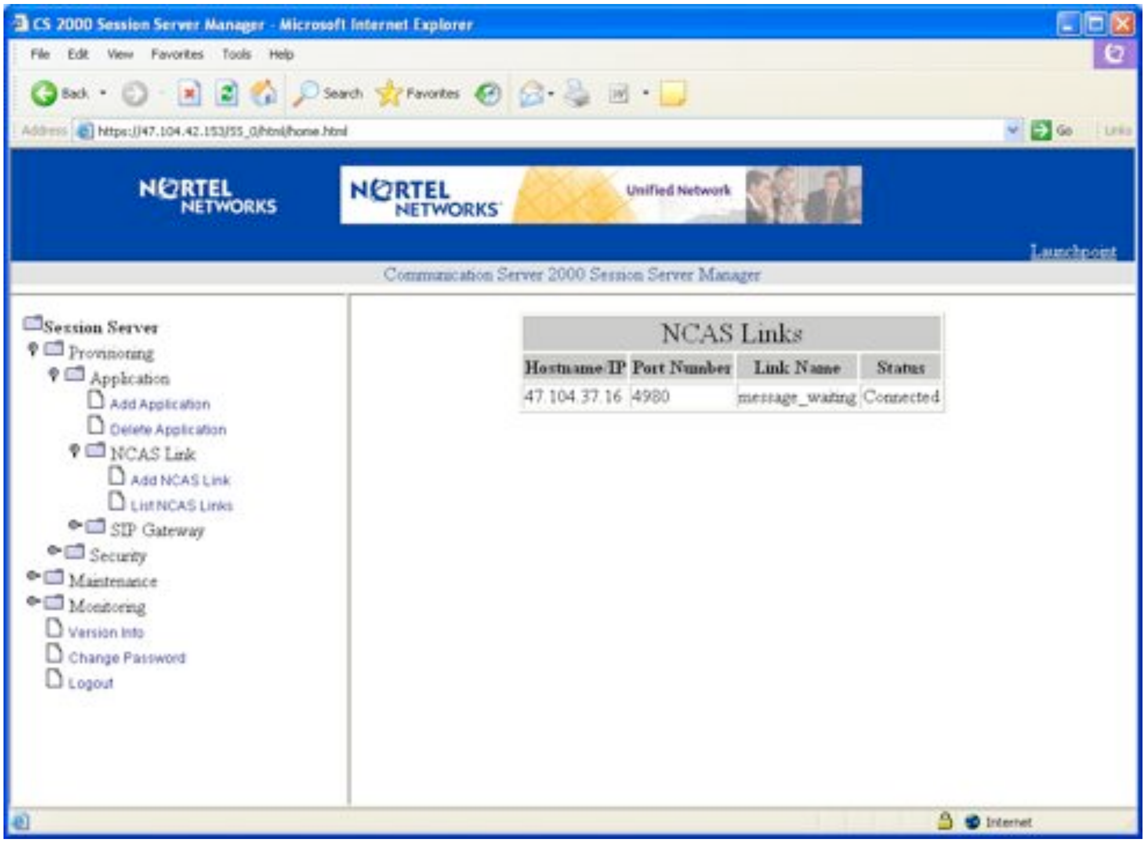


Figure 15 - NCAS CS 2100 Link

1. Select the NCAS Link menu item from the left side menu.
2. Select Add NCAS Link.
3. Specify the CS 2100 core IP address and port 4980.
4. Save the settings.
5. Select the List NCAS Links menu from the left side menu.
6. Verify the new NCAS Link has been added and is connected as shown above.

CICM (Centrex IP Client Manager) Configuration

Prerequisites

- CICM must be visible on the network.
- Must be logged into sets to modify configuration.

Supporting information

- CICM is configured through the web interface.
- Login to web interface to modify settings.

Procedure outline

- Add / modify the following values as indicated below.

Procedure steps

The CICM is configured through a Web interface.

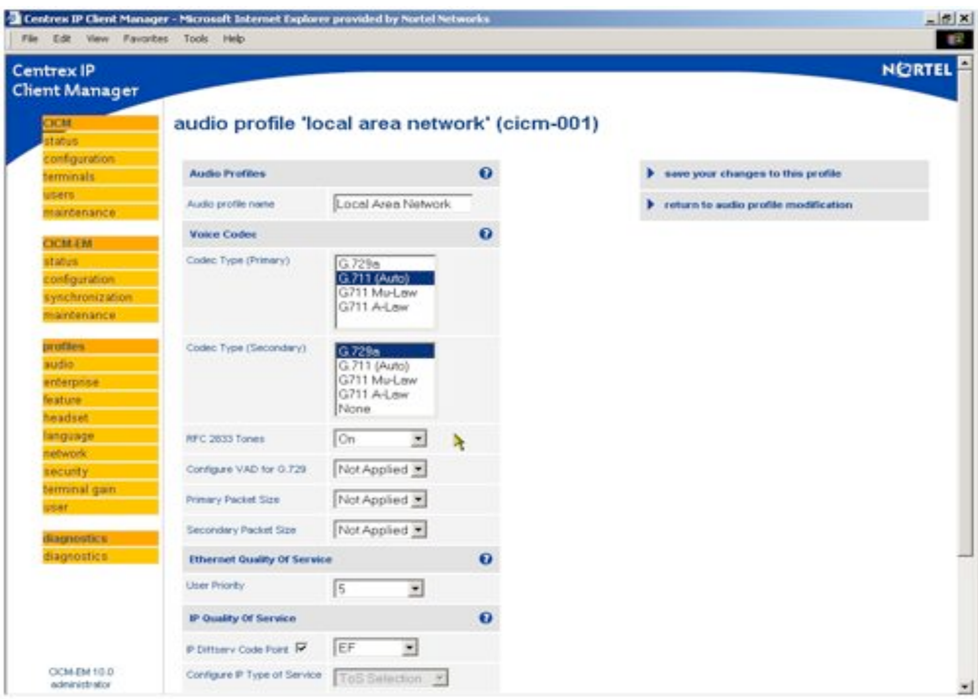


Figure 16 - CICM Audio Profile Configuration

1. Login to CICM
2. Select Audio Profiles from the menu.
3. Select the audio profile for the Local Area Network.

4. Set the Primary Voice Codec Type to G.711 (Auto).
5. Set the Secondary Voice Codec Type to G.729e.
6. Set the RFC 2633 Tones to On.
7. Set Configure VAD for G.729 to Not Applied.
8. Set Primary Packet Size to Not Applied.
9. Set Secondary Packet Size to Not Applied.
10. Set User Priority to 5.
11. Set IP Diffserve Code Point to "checked" and EF.
12. The Configure IP Type or Service will be grayed out.
13. Save the changes to the profile.

Exchange 2010 Server Configuration

Prerequisites

- Domain Controller must be installed and available.
- DNS must be installed and available.
- UM, Client Access, Hub Transport and mailbox roles have been installed per Exchange 2010 installation guide.
- Exchange 2010 server must be visible on the network.

Supporting information

- Configuration for Exchange 2010 is done through the Exchange 2010 Console.
- Exchange 2010 requires Windows 2003 or higher (64 bit).
- Login to the Domain when making configuration changes in Exchange 2010.
- Calls from inside Exchange 2010 must be configured to be local to the switch due to a limitation in the way billing is handled by the SST. (See the CS 2100 and SST sections for details on configuration.)

Procedure outline

- Login to the domain on the Exchange 2010 server.
- Add/modify the following values as indicated below.

Procedure steps

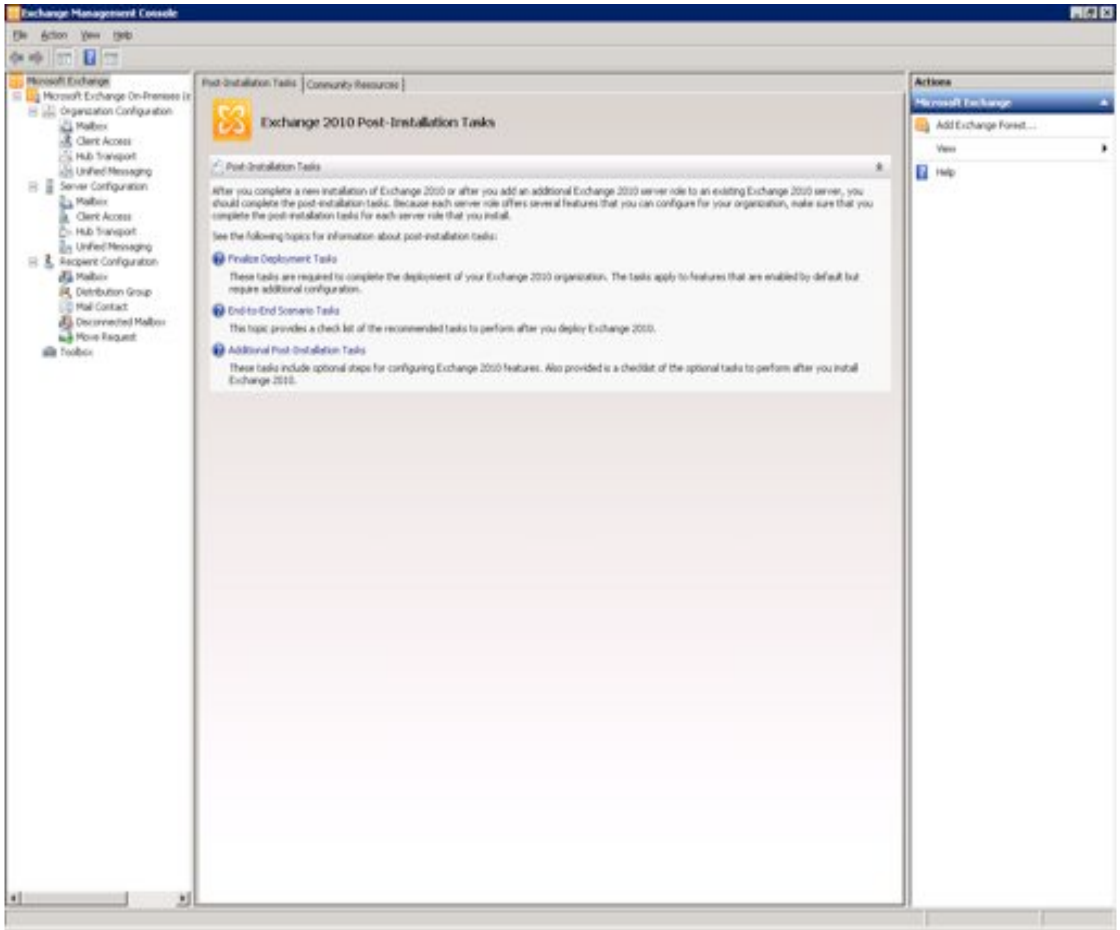


Figure 17 - Exchange 2010 Console

1. Open the Exchange 2010 Console from the Start menu.
2. Select Unified Messaging from under the Organization Configuration tree.
3. Select the Dialing Plan tab and add a dialing plan from the menu on the right.

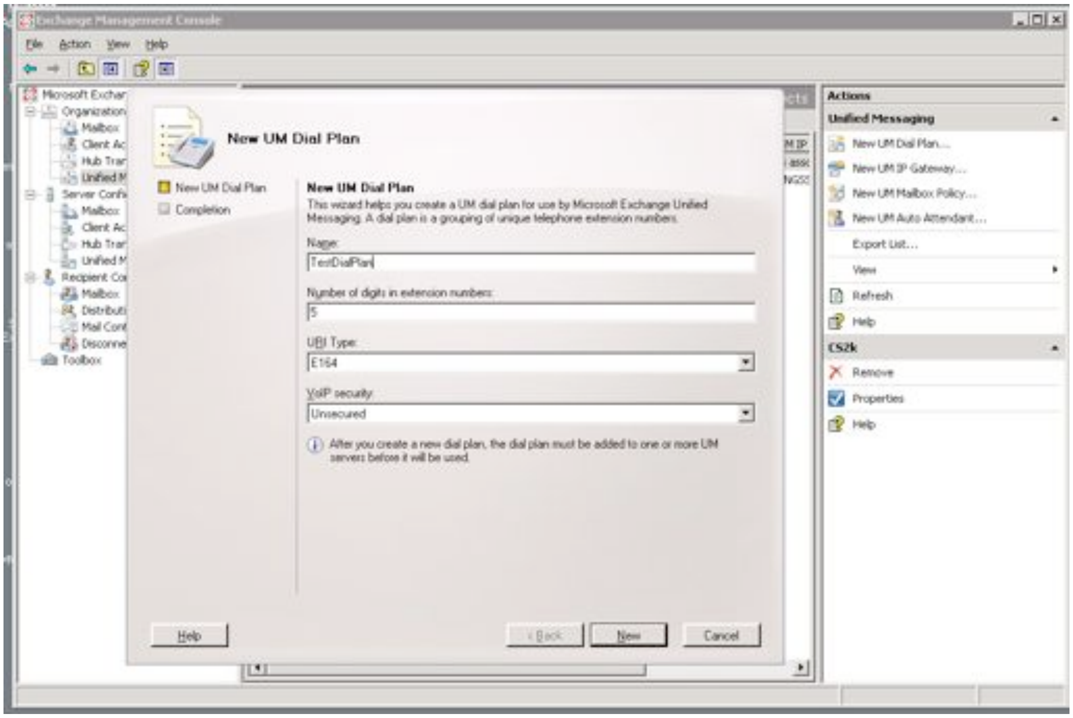


Figure 18 - Add Dialing Plan

4. Select the URI Type at E.164 and VoIP Security as "Unsecured".

   Note: If using a non-E.164 dialing plan as described in step 7 of the **Error! Reference source not found.Error! Reference source not found.**Summary and Limitations section of this document, select URI Type as "Telephone Extension", and VoIP Security as "Unsecured".

5. Configure the dialing plan by selecting it and selecting "Properties" from the menu.

6. Click on the "New" button to continue configuring the dial plan.

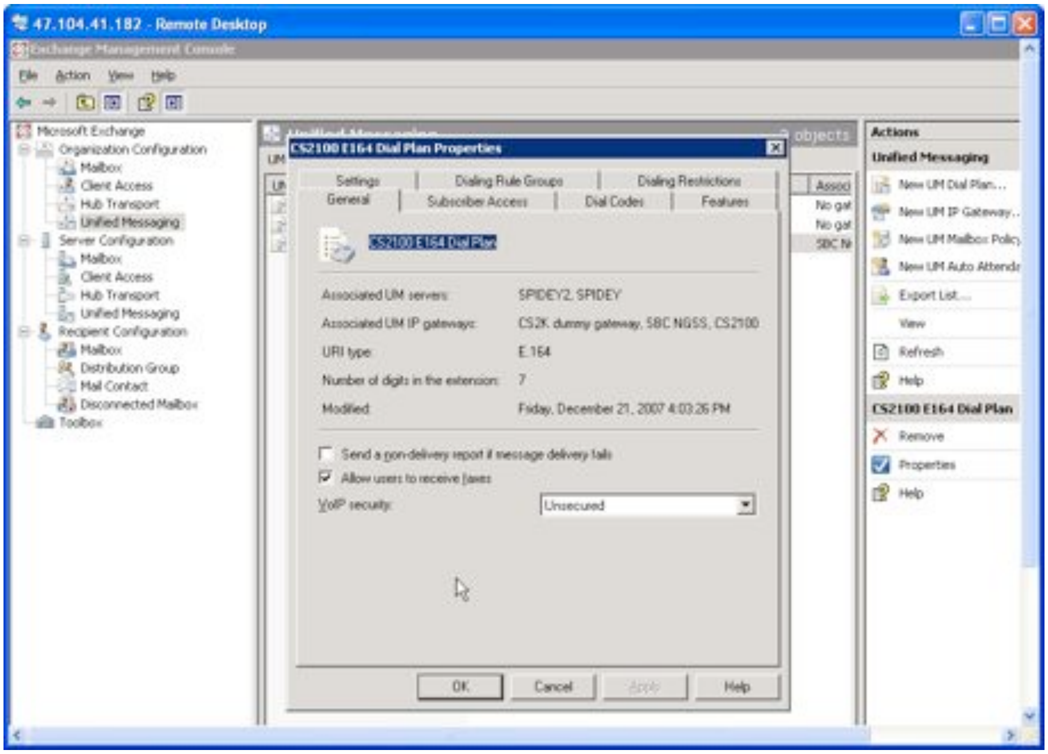


Figure 19 - Server General Properties

7. Go to the properties page of the dial plan you have just created

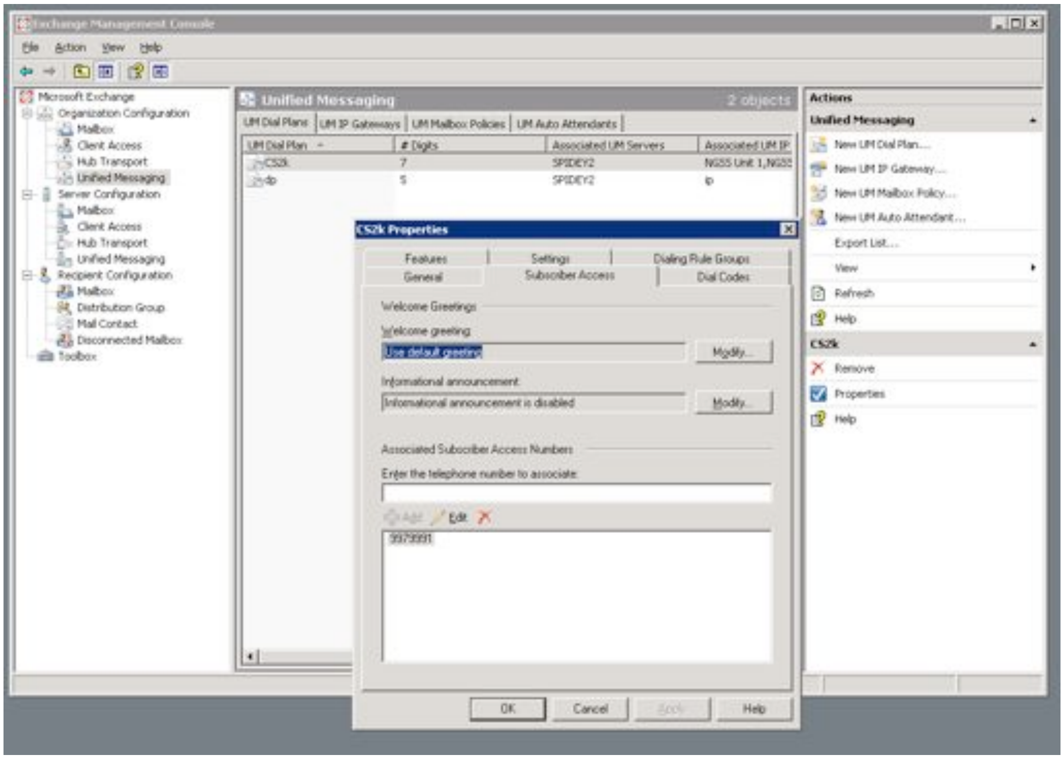


Figure 20 - UM Dial Plan Subscriber Access

8. Select the “Subscriber Access” tab.
9. Specify the telephone number to associate. This is the number configured in the SST that a user calls to access voice mail.

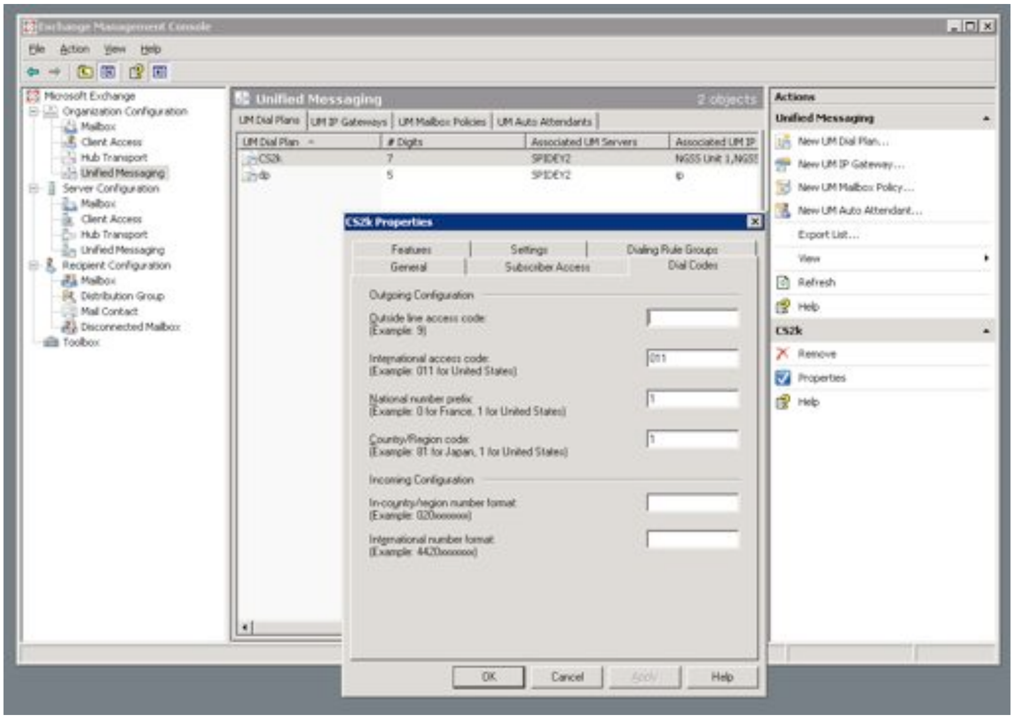


Figure 21 - Dial Codes

10. Select the “Dial Codes” tab. Specify the International, national, and country codes.

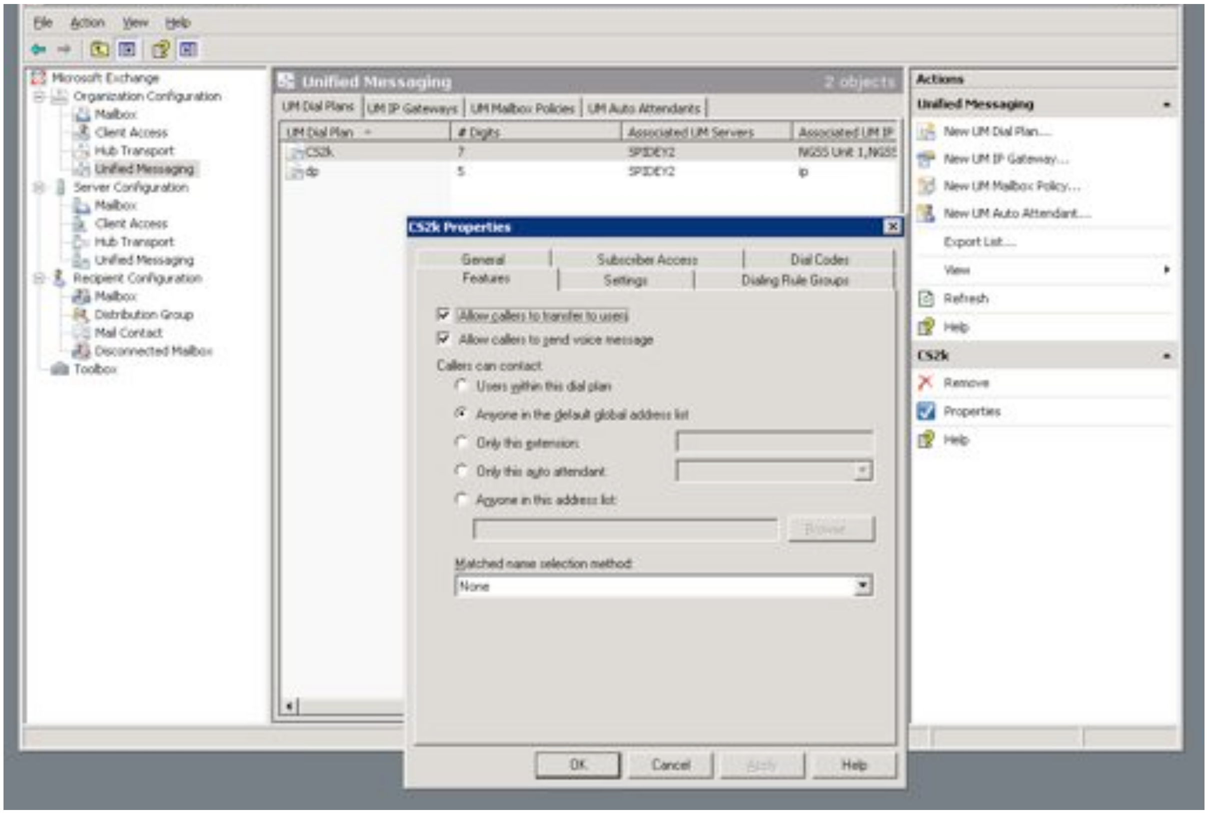


Figure 22 - UM Dial Plan features

11. Select the “Features” tab.
12. Check the “Allow callers to transfer to users” and “Allow callers to send voice message” options.
13. Select the radio button specifying that callers can contact anyone in the global address list.

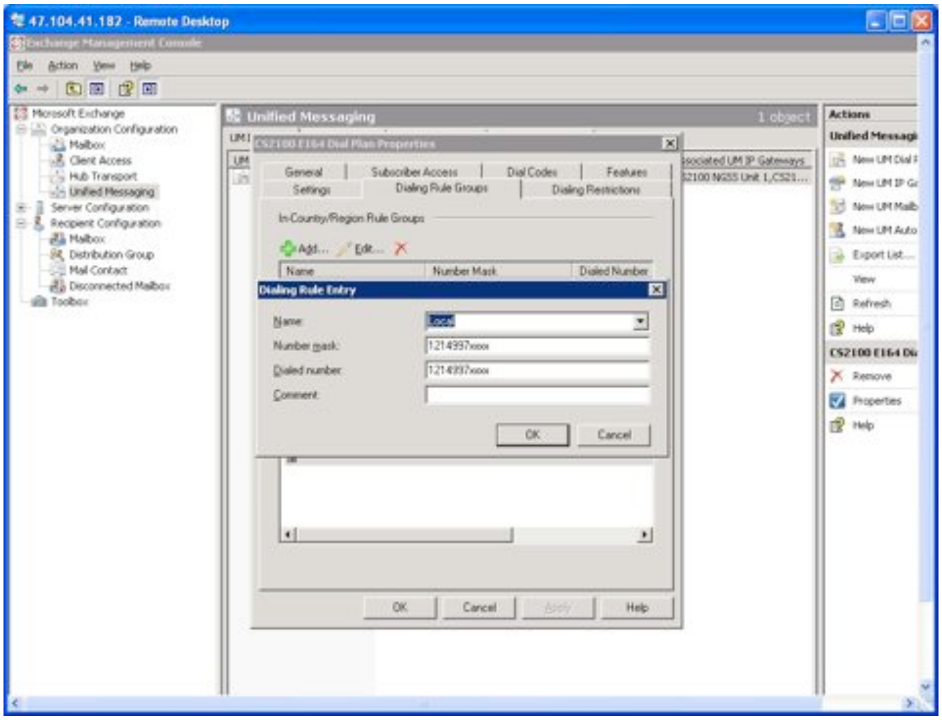


Figure 23 – Dialing Rule Entry

14. Select the "Dialing Rule Groups" tab
15. Select "Add"
16. Configure the dialing rule entries for local dialing.
    a) Set the Name.
    b) Set the Number mask.
    c) Set Dialing number.
    d) Click on OK.

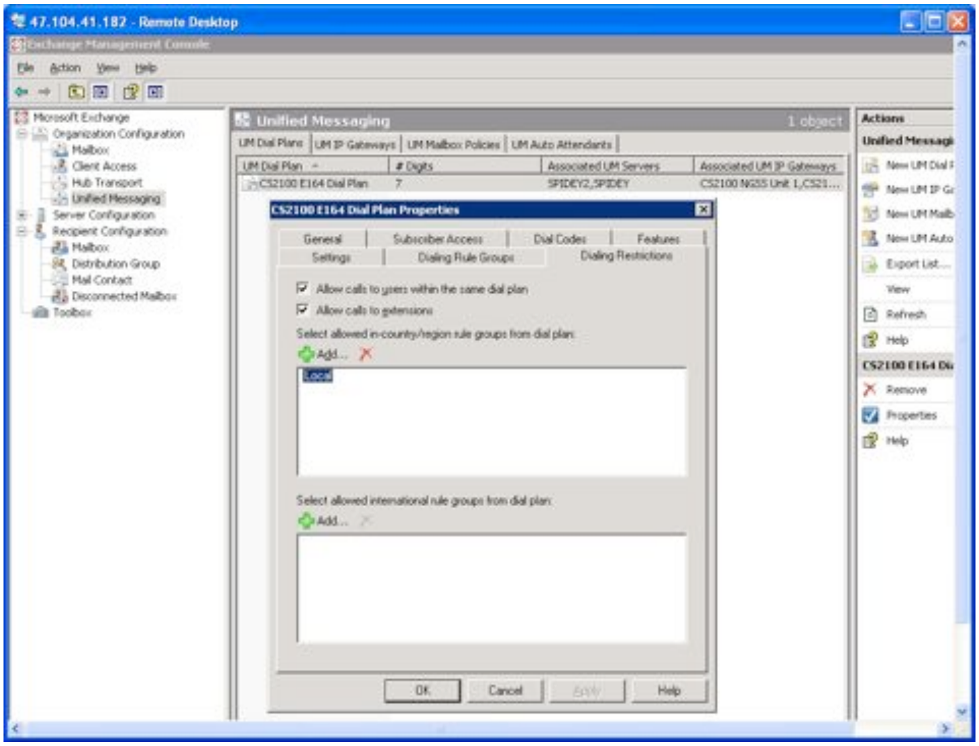


Figure 24 - Dialing Restrictions

17. Select the "Dialing Restrictions" tab
18. Check the "Allow calls to users in the same dial plan", and "Allow calls to extensions" options
19. Apply the dialing rules to the Dialing Restrictions tab
    a) Select the "Add" button
    b) Click on the Dialing Rules entry you created in the previous steps
    c) Select OK
20. Add a new UM Gateway for each IP address that will be communicating with Exchange 2010. SST (NGSS) has two units that should be added in addition to the main IP address. A total of three gateways should be added for the SST.

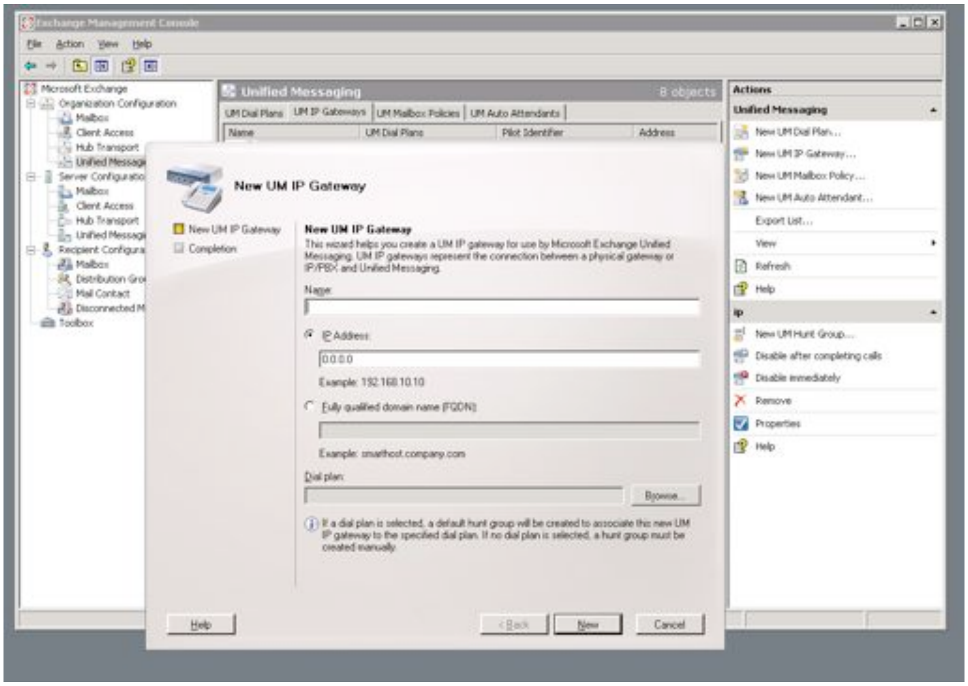


Figure 25 - Add Gateway

21. Specify the IP address and name of the gateway in Exchange 2010.
22. Click on “Browse” and select the dial plan you have just created.

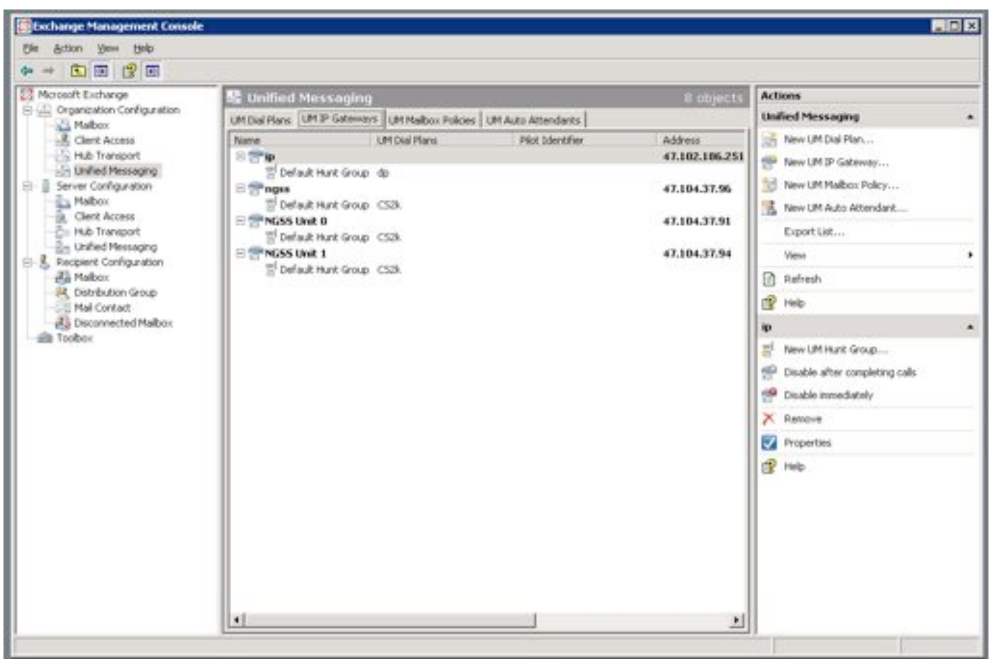


Figure 26 - SST Gateways

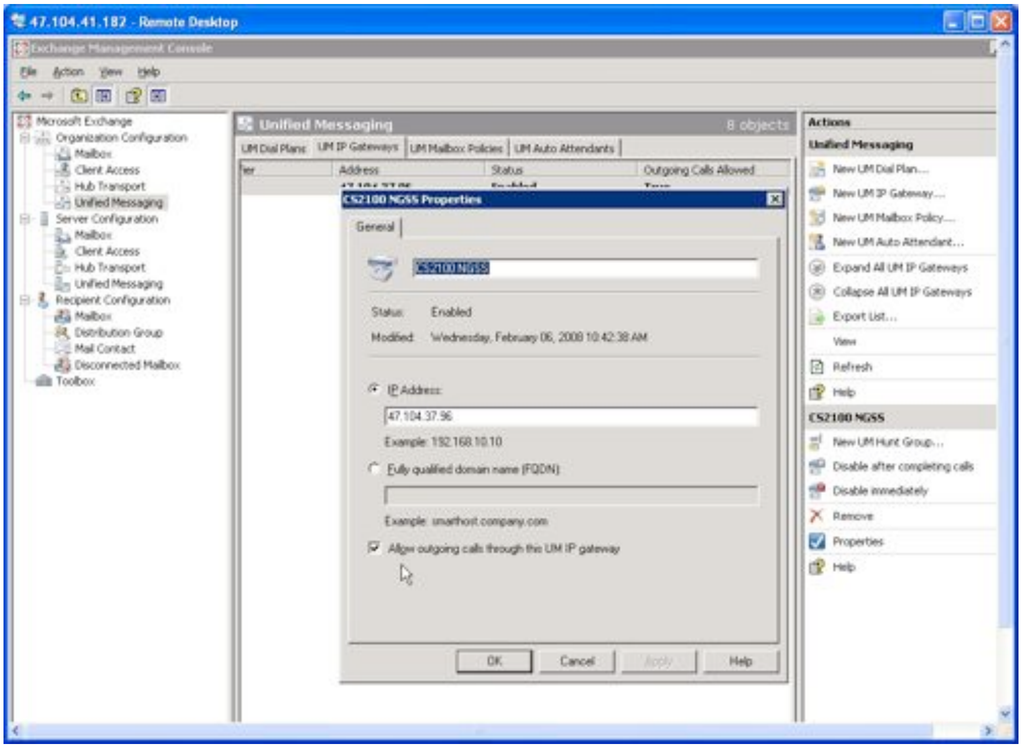


Figure 27 - SST Gateways

23. Optional – While Gateways are designated as outbound by default, the option "Allow outgoing calls through this UM IP gateway" provides the option to enable or disable each gateway as outbound. This is option should be checked for Exchange to have the ability to make outbound calls for features such as Play on Phone.

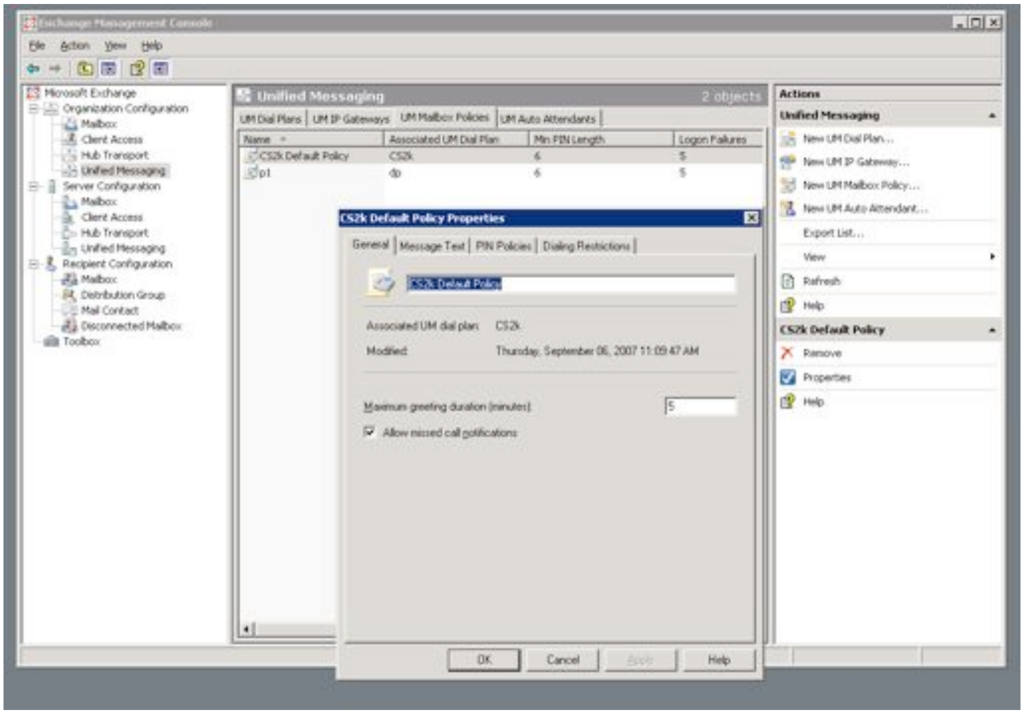


Figure 28 - General Policy Properties

24. Select the “UM Mailbox Policies” tab and click on create a new UM Mailbox from the right side menu. After creating a new mailbox policy changes can be made to the policy by opening the properties for the policy.

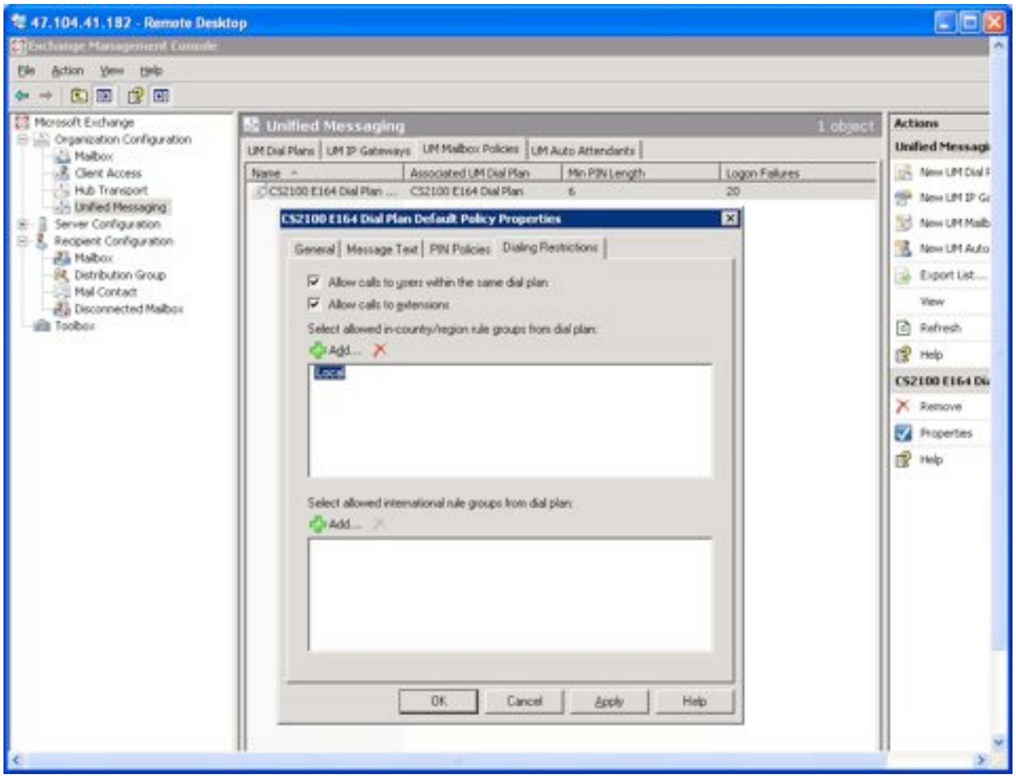


Figure 29 - CS2100 E.164 Dial Plan Default Policy Properties

25. Select the "Dialing Restrictions" tab, and change the dialing restrictions to allow calls to users in the same dialing plan and to extensions.
26. Apply the dialing rules to the Dialing Restrictions tab
    a. Select the Add button.
    b. Click on the Dialing Rules entry you created in the previous steps.
    c. Select OK.

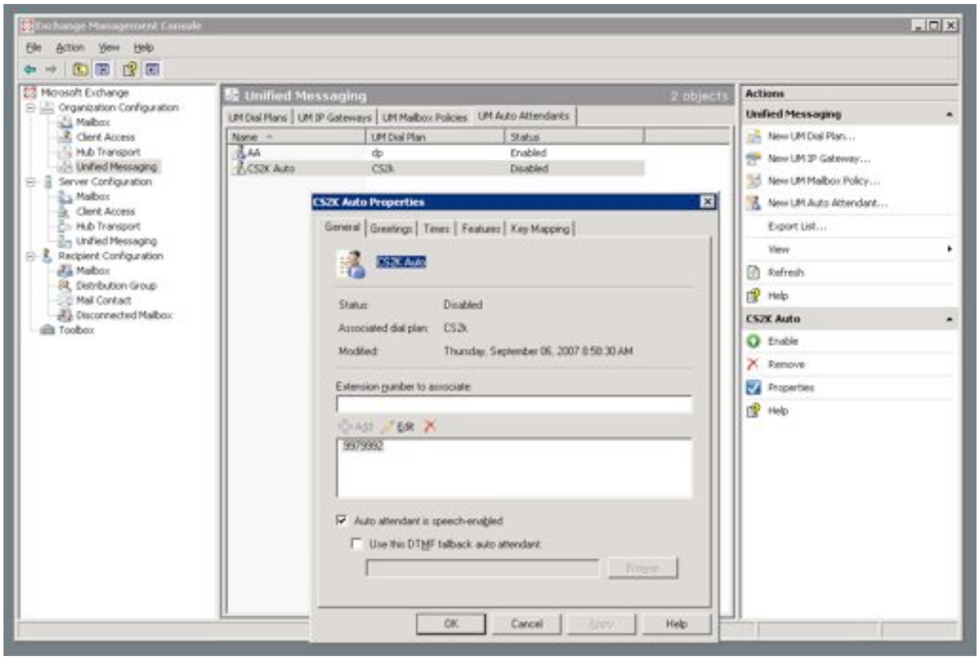


Figure 30 - Auto Attendant

27. Select the “UM Auto Attendants” tab.
28. Select “New UM Auto Attendant” from the right side menu. After an auto attendant is created the properties can be displayed by selecting properties from the right side menu when the auto attendant is selected in the list.
29. Add the number which is configured in the SST to call for voice mail in the box for “Extension number to associate”.

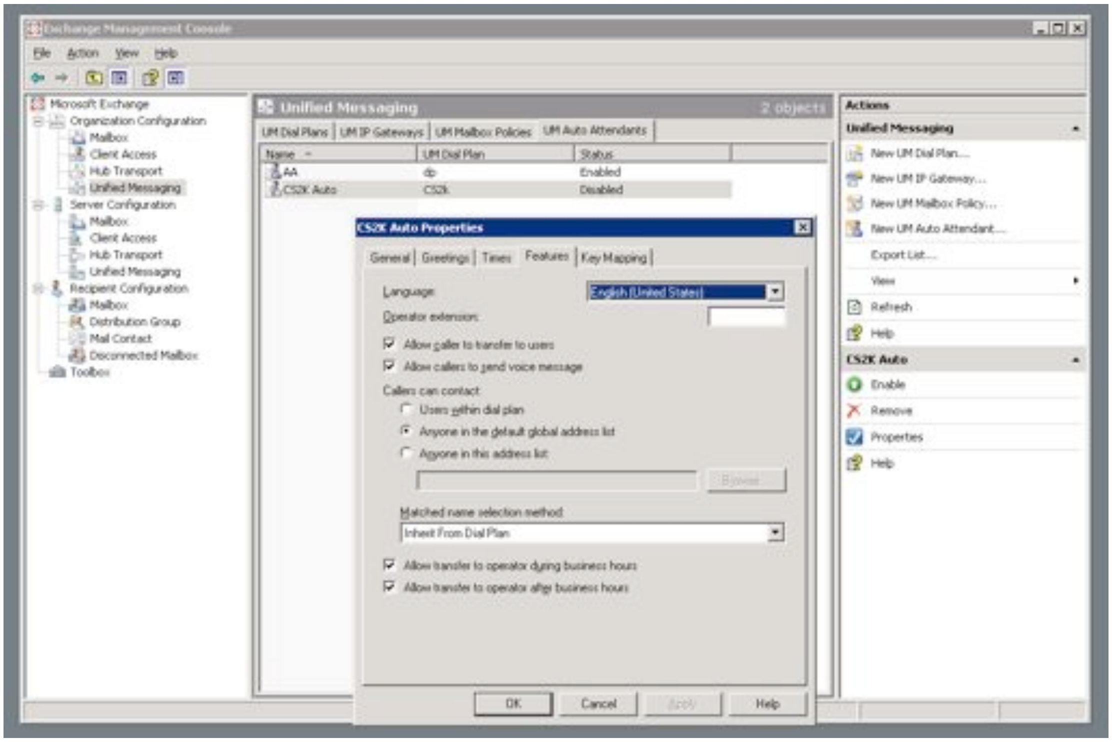


Figure 31 - Auto Attendant Features

30. Select the “Features” tab and specify the Auto Attendant features as follows:
    a) Allow calls to transfer to users
    b) Allow callers to send voice mail
    c) Callers can contact anyone in the default global address list
    d) Matched name selection method should be Inherent From Dial Plan
    e) Allow transfer to operator during business hours
    f) Allow transfer to operator after business hours

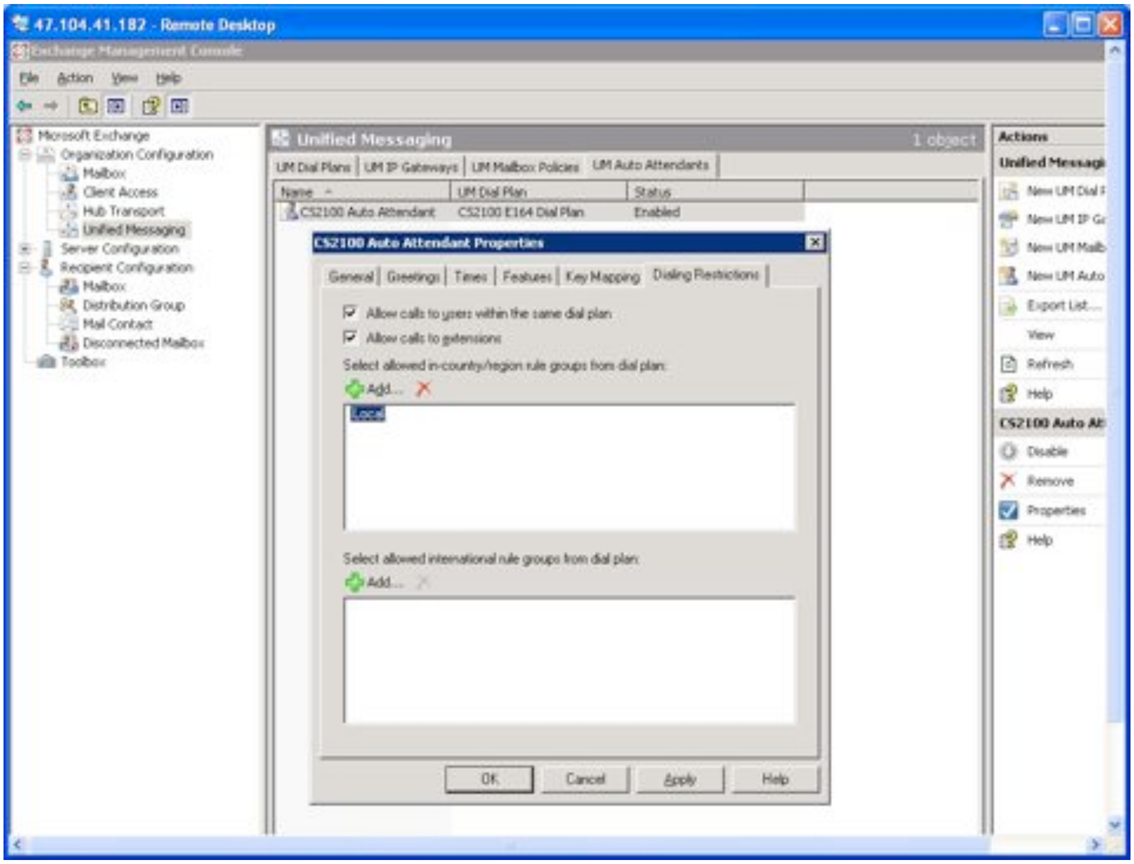


Figure 32 - Auto Attendant Properties

31. Select the "UM Auto Attendants" tab from the Unified Messaging menu.
32. Select the "Dialing Restrictions" tab.
33. Configure the Auto Attendant properties by checking the "Allow calls to users within the same dial plan" and "Allow calls to extensions" options.
34. Apply the dialing rules to the "Dialing Restrictions" tab.
    a) Select the Add button.
    b) Click on the Dialing Rules entry you created in the previous steps.
    c) Select OK.
35. Open the Server Configuration tree on the left menu

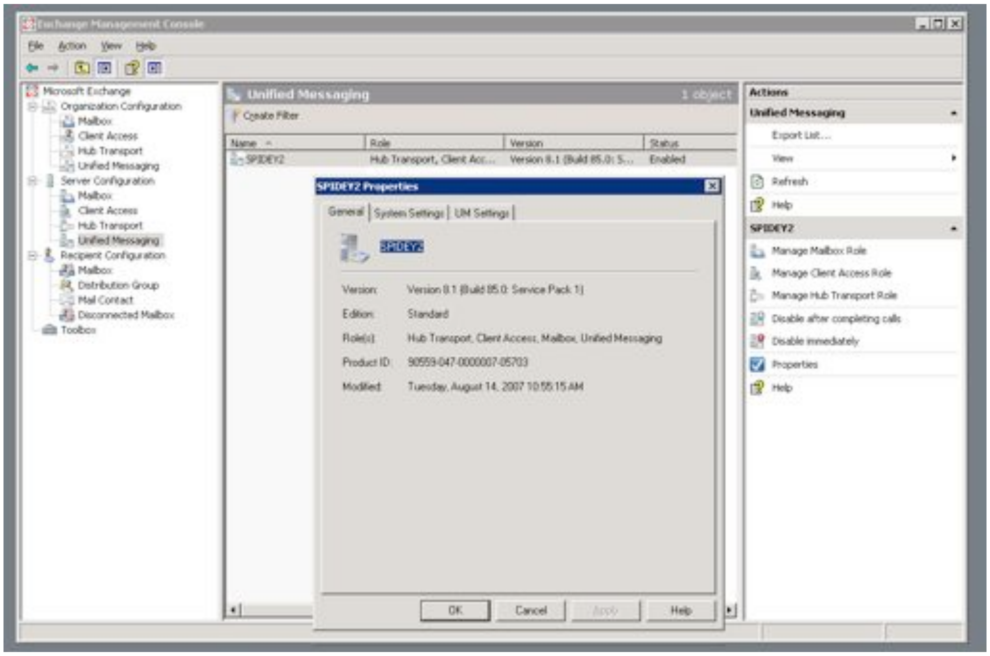


Figure 33 - Server Properties

36. Add a server using the New Server action menu on the right side menu. (This step is only performed if you intend to add a new UM server to your domain.)
37. After a server is added the properties can be changed using the properties menu on the right side menu.

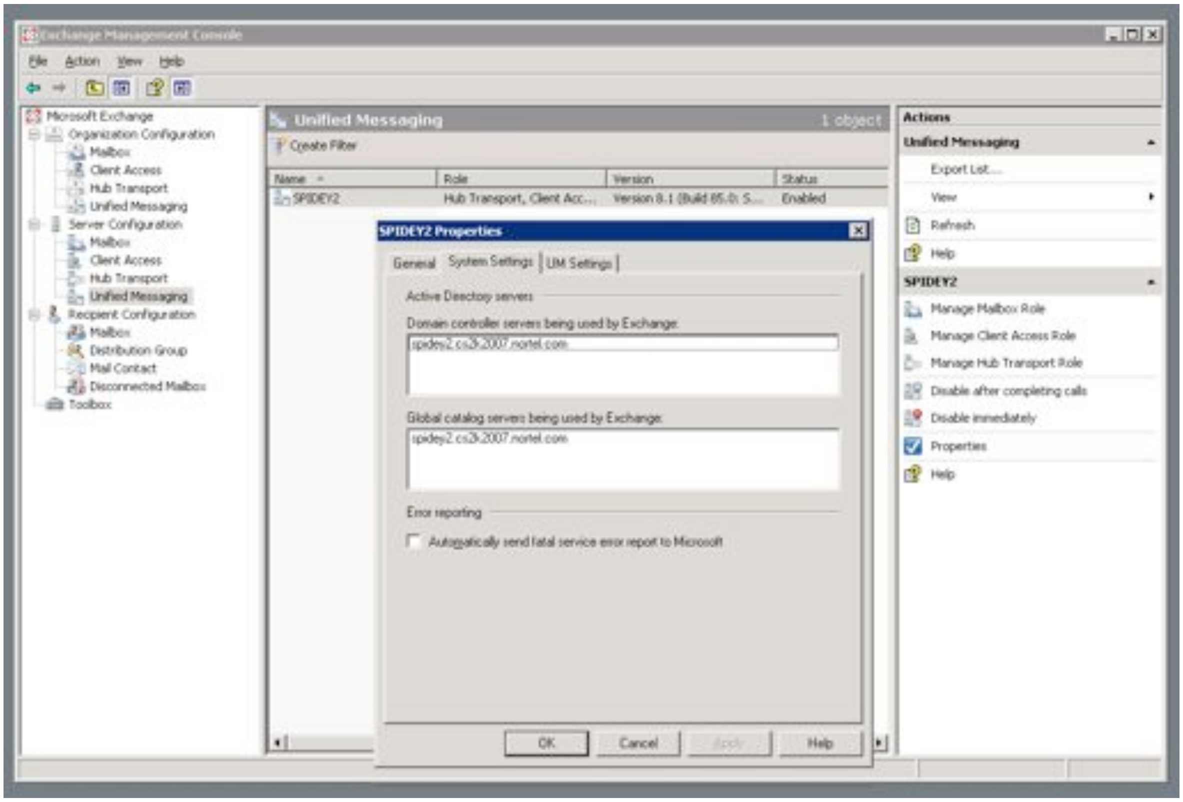


Figure 34– Server Properties System Settings

38. Select the "System Settings" tab.
39. Specify the domain controller and global catalog to be used by this Exchange 2007 server.

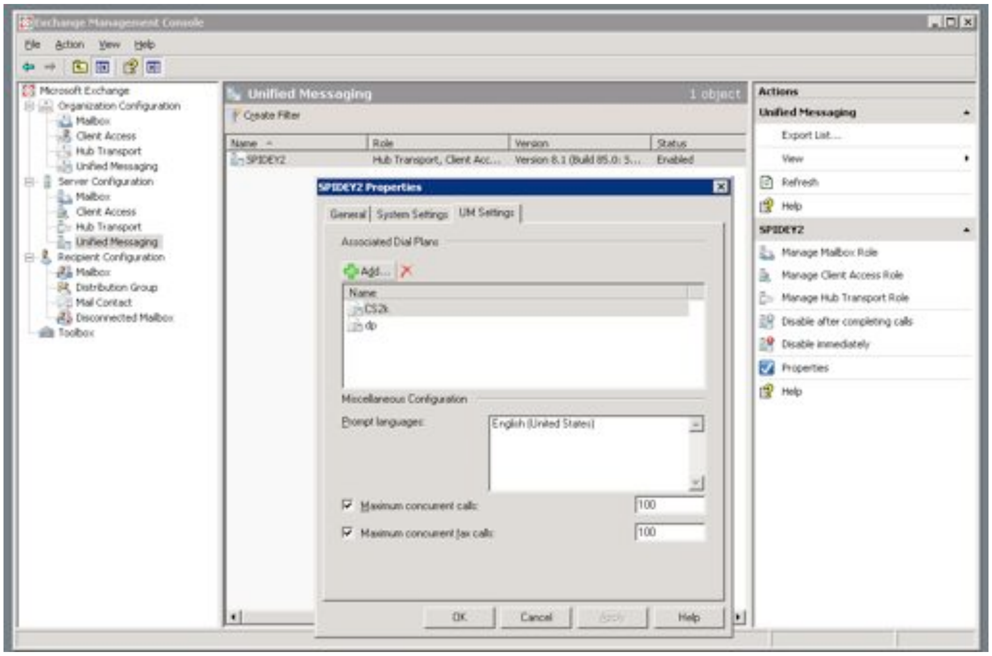


Figure 35 - Server Properties Settings

40. Select the “UM Settings” tab.
41. Select the dialing plan to associate with the server. This should be the one created in the steps above.

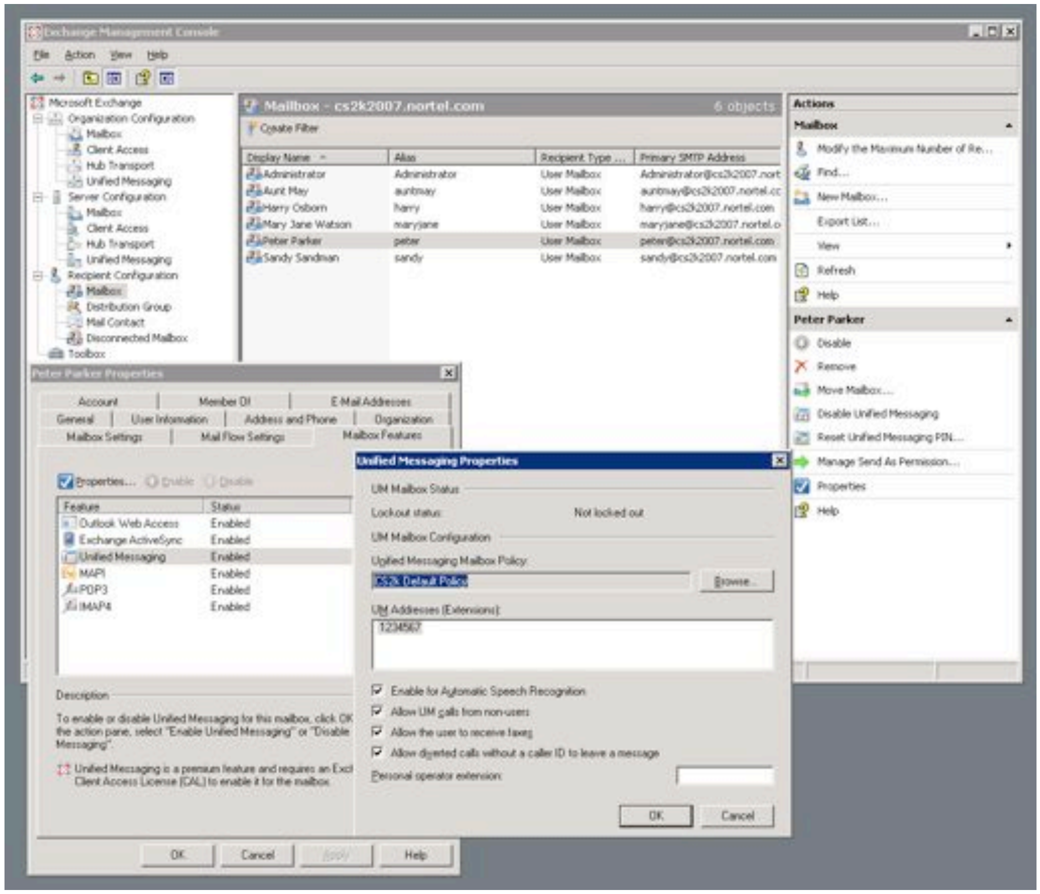


Figure 36 - User Properties

42. Select “Mailbox” under the Recipient Configuration tree on the left side menu.
43. Under the Actions menu select “New User”. Specify the user name and extension.
44. After a user has been added, the “Properties” menu on the right side menu will allow you to view the user settings.
45. Under the “Mailbox Features” tab, enable the Unified Messaging by selecting “Unified Messaging” and selecting “Properties”.
46. Select the Mailbox Policy that was created in the steps above by clicking on the Browse button next to the field for Unified Messaging Mailbox Policy.
47. Select the following options:
    a) “Enable for Automatic Speech Recognition”
    b) “Allow UM calls for non-users”
    c) “Allow directed calls without a caller ID to leave a message”

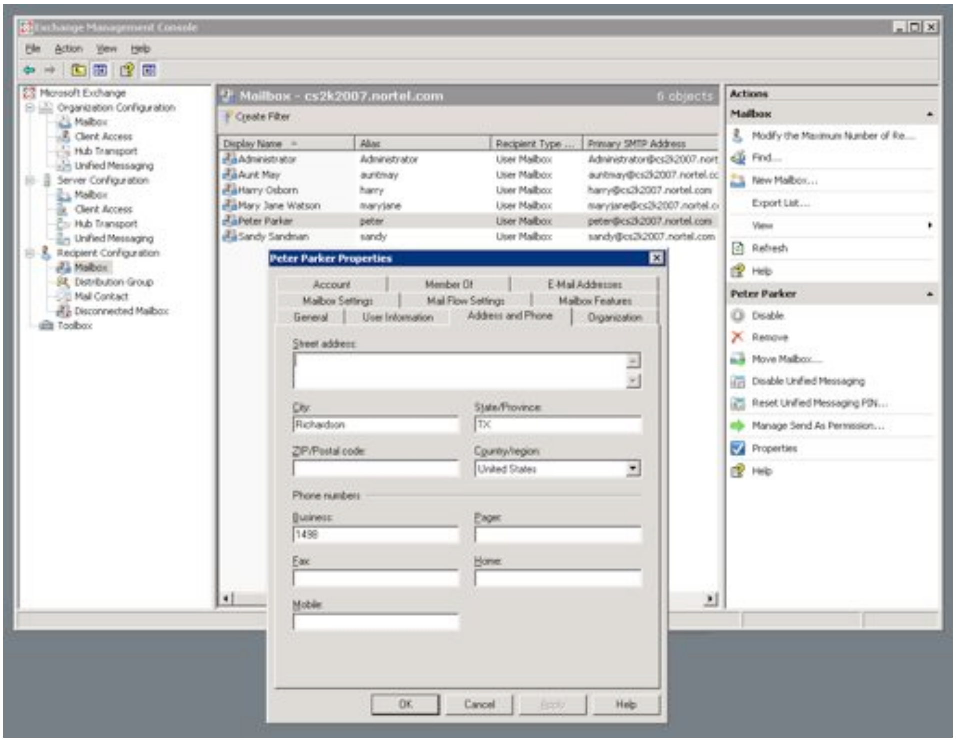


Figure 37 - User Properties - Phone Number

48. Specify the Business Phone number in the user properties dialog under the "Address and Phone" tab.

TLS Setup

- 'Did not perform TLS setup'.

SRTP Setup

- 'Did not perform TLS and SRTP setup'.

Call Transfer(Basic Transfer/Blind Transfer/Supervised Transfer settings)

- N/A

MWI settings

- See configuration guidelines above

Fail-Over Configuration

- N/A

Tested Phones

All CS 2100 supported telephones.

Other Comments

- N/A

7. Exchange 2010 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**)
- Fail (**F**)
- Not Tested (**NT**)
- Not Applicable (**NA**)

The test scenarios are divided into (1) Core mandatory scenarios and (2) Additional scenarios:

1. Mandatory scenarios: These test scenarios MUST pass (**P**) to declare that Exchange UM is functional when using the PBX/gateway in question.
2. Additional scenarios: These additional test scenarios MUST also pass (**P**) to declare that Exchange UM feature set is *fully* functional when using the PBX/gateway in question (See Summary and Limitations).

Refer to:

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

Part I Mandatory Scenarios

No.	**Call Scenarios (see appendix for more detailed instructions)**	(**P**/**F**/**NT**)	**Reason for Failure (see detailed description of limitations)**
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: "<Microsoft Exchange Earcon>. To access your mailbox, enter your extension…"		
2	Navigate mailbox using the Voice User Interface (VUI).		
3	Navigate mailbox using the Telephony User Interface (TUI).		
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.		
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.		
5	Dial Auto Attendant (AA). 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.		
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.		
6c	Call Transfer by Directory Search when the called party does not answer. Confirm the call is routed to the called party's voicemail.		
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.		
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.		
7b	Listen to voicemail using OWA’s Play-On-Phone feature to an external number.		
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: “<Microsoft Exchange UM Earcon>. <User>. Please enter your pin and press the pound key.”		
9	MWI Ensure that a UM-enabled user’s mailbox does not have any new voice mails.		
9a	Dial the user’s extension and leave a voicemail. Confirm the MWI lamp on the phone lights up.		
9b	Mark the voice mail email as read in OWA. Confirm the MWI lamp on the phone turns off.		
10	Execute Test-UMConnectivity.		

Part II Additional Scenarios

No.	Call Scenarios (see appendix for more detailed instructions)	(P/F/NT/NA)	Reason for Failure (see 6.1 for more detailed descriptions)
11	Ensure that a Partner fax Solution is appropriately setup and UM is appropriately configured. Send a test fax message to an user extension.		

	Confirm that the fax is received in the user's inbox.		
12	Setup TLS between gateway/IP-PBX and Exchange UM. *Replace this italicized text with your TLS configuration: self-signed certificates or Windows Certificate Authority (CA).*		
12a	Dial the pilot number and logon to a user's mailbox. Confirm UM answers the call and confirm UM responds to DTMF input.		
12b	Dial a user extension and leave a voicemail. Confirm the user receives the voicemail.		
12c	Send a test fax message to user extension. Confirm the fax is received in the user's inbox.		
13	Setup TLS and SRTP between gateway/IP-PBX and Exchange UM. *Replace this italicized text with your TLS configuration: self-signed certificates or Windows Certificate Authority (CA).*		
13a	Dial the pilot number and logon to a user's mailbox. Confirm UM answers the call and confirm UM responds to DTMF input.		
13b	Dial a user extension and leave a voicemail. Confirm the user receives the voicemail.		
13c	Send a test fax message to user extension.		

	Confirm the fax is received in the user's inbox.		
14	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). Dial the pilot number and confirm the UM system answers the call.		
15	Setup and test fail-over configuration on the Gateway or IP-PBX to work with two UM servers.		
16	Setup and test Exchange Server 2007 and Exchange Server 2010 co-existence scenario.		
16a	Dial a user's extension whose mailbox is still on Exchange Server 2007 and leave a voicemail. Confirm the user receives the voicemail.		
16b	Dial the pilot number from the user's extension and logon to a user's mailbox. Confirm hearing the prompt: "<Microsoft Exchange UM Earcon>. To access your mailbox, enter your extension…"		
16c	Navigate mailbox using the Voice User Interface (VUI).		
17	*Applicable only to IP-PBXs:* Setup and test configuration involving transfer between multiple phone endpoints connected to IP-PBX wherein the transfer target is unconditionally forwarded to UM and the IP-PBX acts as a Back-to-Back User Agent.		
18	*Set up Call answering rules to do a "find-me" for 2 numbers and try to call the users extension.* *Confirm that the system plays the Call*		

	answering rules prompt and allows the caller to try reach the number specified		
19	*Setup Call answering rules to do a "Transfer to another rextension or phone number* *Confirm that the system plays the Call answering rules prompt and transfer the caller to the extension configured.*		

Detailed Description of Limitations

Failure Point	
Phone type (if phone-specific)	
Call scenarios(s) associated with failure point	
List of UM features affected by failure point	
Additional Comments	

Failure Point	
Phone type (if phone-specific)	
Call scenarios(s) associated with failure point	
List of UM features affected by failure point	
Additional Comments	

8. Troubleshooting

[DELETE THIS] Provide Troubleshooting information if applicable.

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 prompt: "<Exchange UM Earcon>. 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

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

b. From an External Phone

- From an external phone, dial the extension for a UM-enabled user and leave a voicemail message.
- Confirm the voicemail message arrives in the called user's inbox.
- 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:
  - Under the Exchange Management Console, expand "Organizational Configuration" and then click on "Unified Messaging".
  - Go to the Auto Attendant tab under the results pane.
  - Click on the "New Auto Attendant…" under the action pane to invoke the AA wizard.
  - Associate the AA with the appropriate dial plan and assign an extension for the AA.
  - Create PBX dialing rules to always forward calls for the AA extension to the UM server.
  - 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.
    - UM Enable a user by invoking the “Enable-UMMailbox” wizard.
    - Assign an unused extension to the user.
    - Do not map the extension on the PBX to any user or device.
    - Call Transfer by Directory Search to this user.
    - Confirm the call fails and the caller is prompted with appropriate messages.

7. Play-On-Phone

- To access play-on-phone:
    - Logon to Outlook Web Access (OWA) by going to URL https://<server name>/owa.
    - After receiving a voicemail in the OWA inbox, open this voicemail message.
    - At the top of this message, look for the Play-On-Phone field (Play on Phone...).
    - 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:
    - 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:
    - $dp = get-umdialplan -id <dial plan ID>
    - $dp.ConfiguredInCountryOrRegionGroups.Clear()
    - $dp.ConfiguredInCountryOrRegionGroups.Add("anywhere,*,*,")
    - $dp.AllowedInCountryOrRegionGroups.Clear()
    - $dp.AllowedInCountryOrRegionGroups.Add(“anywhere")
    - $dp|set-umdialplan
    - $mp = get-ummailboxpolicy -id <mailbox policy ID>
    - $mp.AllowedInCountryGroups.Clear()
    - $mp.AllowedInCountryGroups.Add("anywhere")
    - $mp|set-ummailboxpolicy
    - The user must be enabled for external dialing on the PBX.
    - 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: “<Exchange UM Earcon>. <User>. 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. Message Waiting Indicator (MWI)

- MWI is enabled by default on the UM Mailbox.
- Ensure that a UM-enabled user's mailbox does not have any new (or marked unread) voice mail notifications

a. MWI lamp on phone lights up

- Dial the extension for that UM-enabled user and leave a voicemail message.
- Confirm the MWI lamp on the phone lights up.

b. MWI lamp on phone turns off

- Logon to Outlook Web Access (OWA) by going to URL https://<server name>/owa.
- Mark the voice mail notification email as read in OWA.
- Confirm the MWI lamp on the phone turns off.

10.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.

11. Fbax

- Fax is enabled by default on UM Dial Plan and UM Mailbox.
- Use the Management Console or the Management Shell to enable fax on UM Mailbox Policy.
    - Management Console:

    - Go to “Unified Messaging” under “Organization Configuration” and then to the “UM Mailbox Policies” tab.
    - Double click on the relevant UM Mailbox Policy and go to”General” tab.
    - Check the box “Allow inbound faxes” and enter the Partner Fax Server URI
  - Management Shell - execute the following command:
    - Set-UMMailboxPolicy –identity <UMMailboxPolicy> –AllowFax:$true –FaxServerURI:”sip:<URI>:<port>;transport=<udp|tcp|tls>”
    - For example: Set-UMMailboxPolicy -Identity "dp Default Policy" -AllowFax $true -FaxServerURI "sip:faxserver.default.com:1234;transport=tcp”
- To test fax functionality:
  - Dial the extension for a UM user from a fax machine.
  - Confirm the fax message is received in the user’s inbox.
  - 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.

12.MUTUAL TRANSPORT SECURITY LAYER (MTLS)

- Setup TLS on the gateway/IP-PBX and Exchange 2010 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 11 (above) with TLS turned on.

13. MUTUAL TRANSPORT SECURITY LAYER (MTLS) AND SECURE RTP (SRTP)

- Setup TLS and SRTP on the gateway/IP-PBX and Exchange 2010 UM.
- Import/Export all the appropriate certificates.

a. Dial Pilot Number and Mailbox Login

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

b. Dial User Extension and Leave a Voicemail

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

c. Fax

- Execute the steps in scenario 11 (above) with TLS turned on.

14.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.

15.Test Fail-Over Configuration on gateway or IP-PBX with Two UM Servers

- If the gateway or IP-PBX supports fail-over configuration (e.g., round-robin calls between two or more UM servers):
    - Provide the configuration steps in Section 5.
    - Configure the Gateway or IP-PBX to work with two UM servers.
    - Simulate a failure in one UM server.
    - Confirm the Gateway or IP-PBX transfers new calls to the other UM server successfully.

16. Exchange Server 2007 and Exchange Server 2010 co-existence scenario.

- Setup an Exchange Server 2007 deployment. In particular,
    - UM-enable a user
    - Ensure that voice mail left for the user's extension is delivered to their mailbox
    - Ensure that you can dial the pilot number from the user's extension and log on to the user's mailbox and navigate using Voice User Interface (VUI).
- Setup an Exchange Server 2010 server to coexist with an Exchange Server 2007 deployment as directed here.
- Add the Exchange Server 2010 server to the existing dial plan created in the context of the Exchange Server 2007 deployment
- Configure the gateway or IP-PBX to send all calls to the Exchange Server 2010 UM server.

a. Dial User Extension and Leave a Voicemail

- Dial the extension for a UM-enabled user whose mailbox is still on Exchange Server 2007 and leave a voicemail message.

- Confirm the voicemail message arrives in the called user's mailbox.

b. Dial Pilot Number and Mailbox Login

- Dial the pilot number of the UM server from the UM-enabled user's extension.
- Confirm hearing the prompt: "<Exchange UM Earcon>. <User>. Please enter your pin and press the pound key."
- Enter the PIN of an UM-enabled user.
- Confirm successful logon to the user's mailbox.

c. Navigate Mailbox using Voice User Interface (VUI)

- Logon to a user's UM mailbox.
- Navigate through the mailbox and try out various voice commands to confirm that the VUI is working properly.

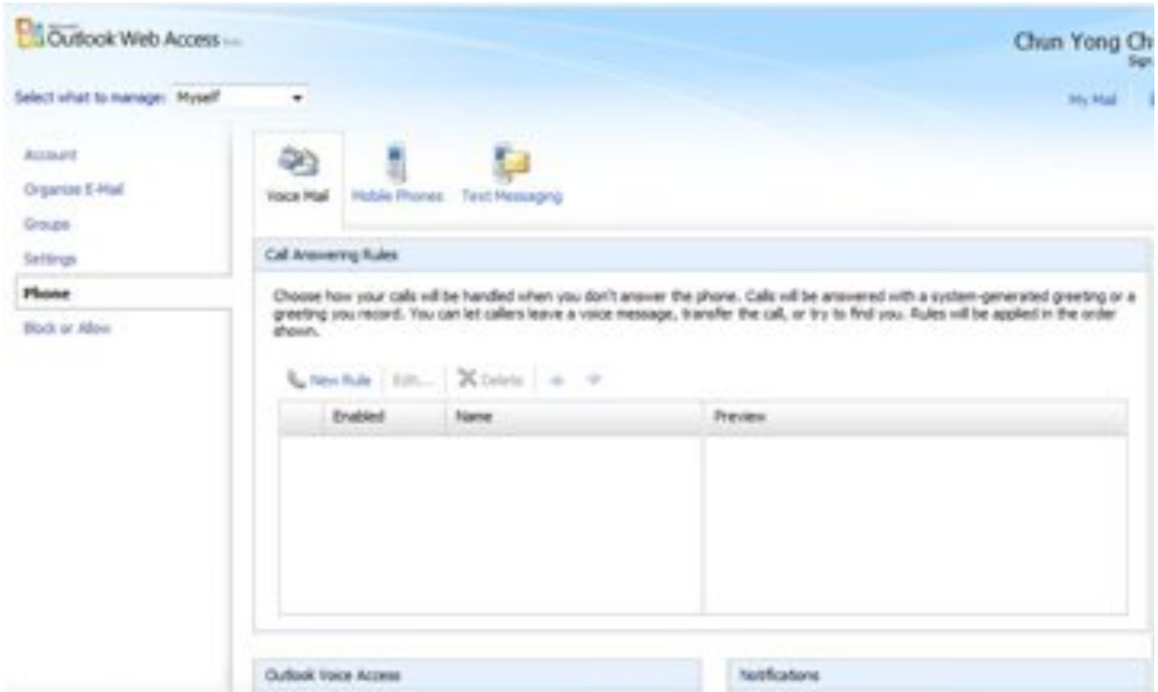
17. Transfer between multiple phone endpoints connected to IP-PBX

- This is only required for direct SIP integration with IP-PBXs. If there are scenarios wherein multiple phone endpoints are connected to IP-PBX and the IP-PBX acts as a Back-to-Back User Agent (B2BUA) between these endpoints and Exchange UM then:
    - Set up three phone endpoints (A, B and C)
    - Create a UM-enabled mailbox associated with C
    - Configure C to forward all calls to UM unconditionally
    - Call from A to B and then transfer the call to C
    - Confirm that A is able to leave a message for C

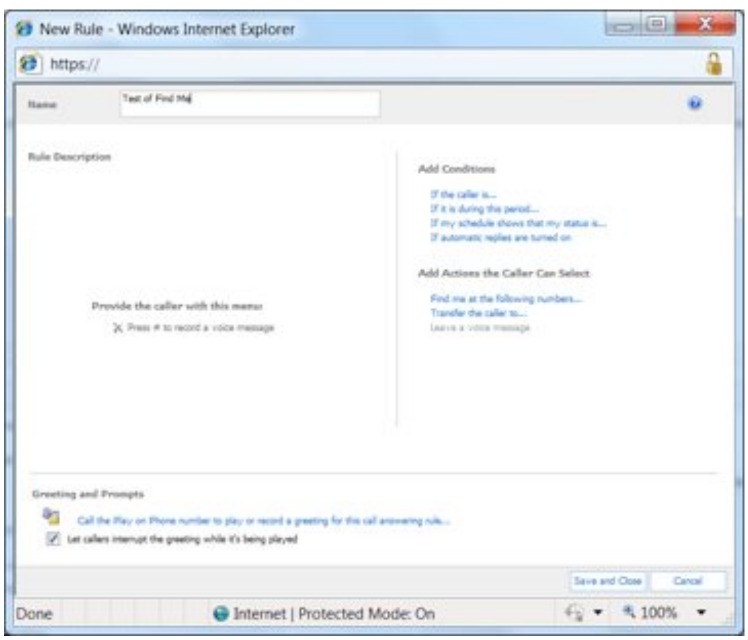
18. Call Answering rules

a. Set up a Call Answering Rules to do *Find Me* and Transfer

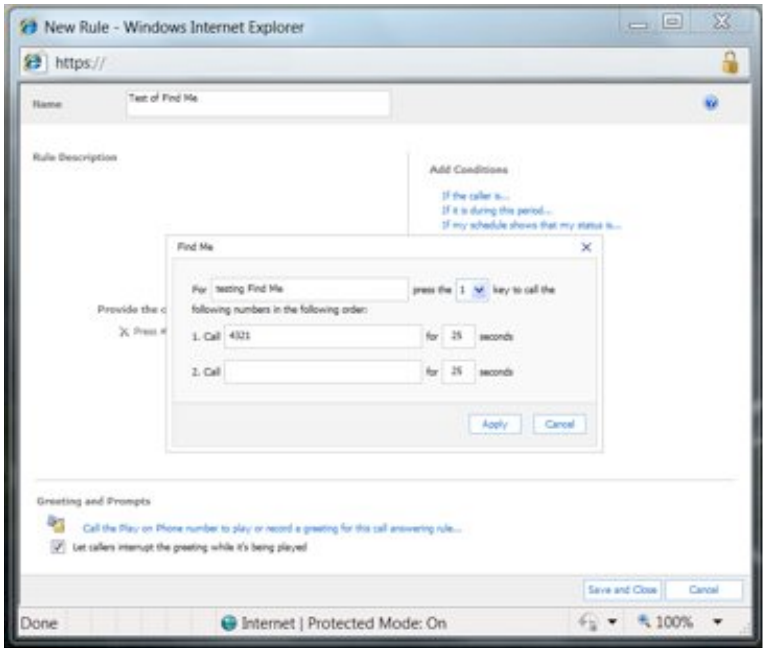
- Call answering rules are managed as part of voice mail personal configuration. Log in to a UM-enabled mailbox with Outlook Web Access and navigate to the *Options* page. Then choose *Phone* settings and the *Voice Mail* tab:



- Click on *New Rule* to create a new Call Answering rule. Give the rule a name (e.g. *Test of Find Me)*

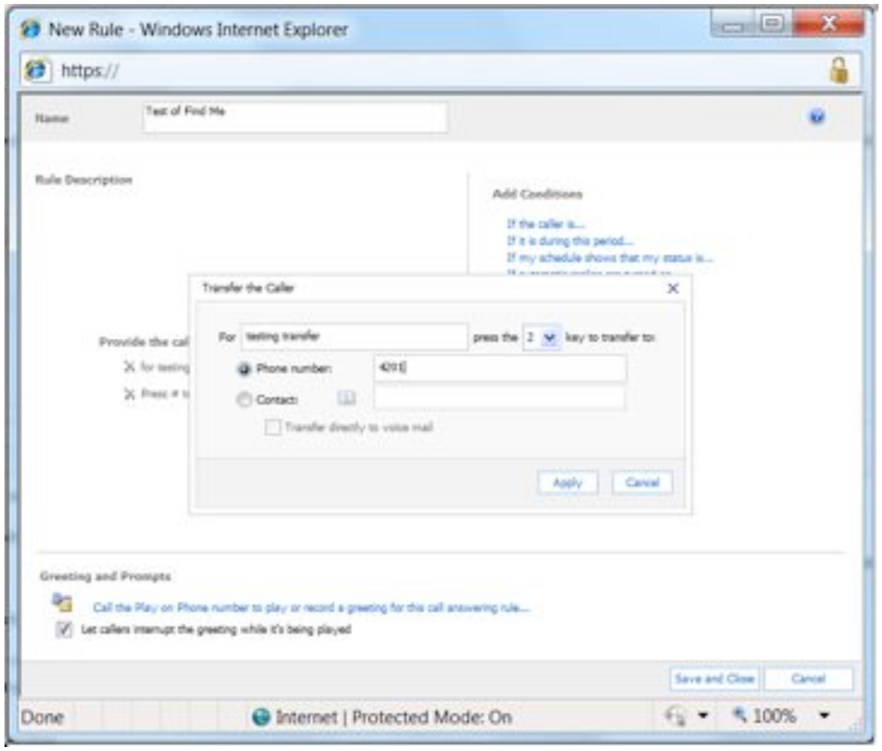


- Under *Add Actions the Caller Can Select*, choose the *Find me at the following numbers…* link.

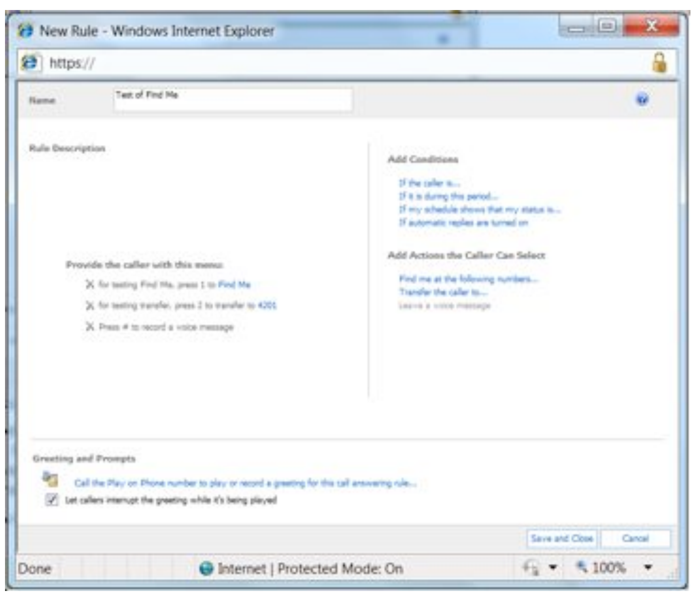


- Enter some text in the *For* edit control (e.g. *testing Find Me*). In the first *Call* control, enter the number of an extension or other phone that can be reached from the gateway to which UM is connected. UM will place a call to this number as part of the Find Me feature.
- In the second *Call* control, enter the number of a different extension or phone that UM can call. Click on *Apply.*

- In the main dialog, add another action to the Call Answering Rule by clicking on *Transfer the caller to…*



- Enter some text in the *For* edit control (e.g. *testing transfer*). In the control beside *Phone number*, enter the number of an extension or other phone that can be reached from the gateway to which UM is connected. (This can be the same as one or other of the numbers used for the Find Me test). Click on the *Apply* button.
- You should now have a Call Answering Rule with three choices for the caller: 1 for Find Me, 2 for transfer and # to leave a message:



- Click on *Save and Close* to finish the creation of the Call Answering Rule. There are no conditions in the rule, so it should run for every call that UM answers for the associated mailbox.

b. Test Transfer by the Call Answering Rule

- Place a call to the extension that corresponds to the UM-enabled mailbox with the Call Answering Rule. Allow the call to forward to UM.
- UM will play a synthetic greeting, announcing the options (1 for Find Me, 2 for transfer, # to leave a message).
- Press 2.
- UM should transfer the call to the configured endpoint. Answer the call and verify end-to-end connectivity.
- Hang up.

c. Test *Find Me* by the Call Answering Rule: Reject Call to First Number

- Place a call to the extension that corresponds to the UM-enabled mailbox with the Call Answering Rule. Allow the call to forward to UM.
- UM will play a synthetic greeting, announcing the options (1 for Find Me, 2 for transfer, # to leave a message).
- Press 1.
- UM will prompt for a spoken name (to announce to the user). Speak a name.
- UM will place an outbound call to the first number configured. Answer this call.
- On the answered call, UM will announce the name of the caller and request that you press 1 to accept the call, 2 to reject.
- Press 2 to reject the call.
- Wait. Verify that UM hangs up the call.
- Wait. Verify that UM calls the second number.
- Hang up the original call.
- Verify that UM stops calling the second number.

d. Test *Find Me* by the Call Answering Rule: Answer Second Number

- Place a call to the extension that corresponds to the UM-enabled mailbox with the Call Answering Rule. Allow the call to forward to UM.

- UM will play a synthetic greeting, announcing the options (1 for Find Me, 2 for transfer, # to leave a message).
- Press 1.
- UM will prompt for a spoken name (to announce to the user). Speak a name.
- UM will place an outbound call to the first number configured. <u>Do not answer this call.</u>
- After 20 – 30s, UM will stop calling the first number and will start calling the second number. Answer this call.
- On the answered call, UM will announce the name of the caller and request that you press 1 to accept the call.
- Press 1 to accept the call.
- Verify end-to-end connectivity with the calling party.
- Hang up.