Microsoft Exchange Server 2007 Unified Messaging Fundamentals
Avaya Communication Server 1000

7.5
NN43001-122, 05.03
August 2011

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Preventing Toll Fraud

“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: New in this release

The following sections detail what is new in *Microsoft Exchange Server 2007 Unified Messaging Fundamentals, NN43001-122* for Avaya Communication Server 1000 (Avaya CS 1000) Release 7.5.

Features

There are no updates to the feature descriptions in this document.

Other changes

This release contains no other changes.

Revision History

August 2011	Standard 05.03. This document is up-issued to support the removal of content for outdated features, hardware, and system types.
March 2011	Standard 05.02. This document is up-issued to reflect changes in the Operational Considerations section to support Communication Server 1000 Release 7.5.
November 2010	Standard 05.01. This document is up-issued to support Communication Server 1000 Release 7.5.
June 2010	Standard 04.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.0.
December 2009	Standard 03.03. This document is up-issued to add a note in the section TLS Configuration on UMS2007SP1.
June 2009	Standard 03.02. This document contains added section: "TLS Configuration on UMS2007SP1."
May 2009	Standard 03.01. This document is up-issued to support Communication Server 1000 Release 6.0.
May 2008	Standard 02.03. This document is issued to reflect changes in technical content.

March 2008	Standard 02.02. This document is issued to reflect changes due to CR#Q01808992.
December 2007	Standard 02.01. This document is issued to support Communication Server 1000 Release 5.5.
August 2007	Standard 01.01. This document is issued to support Communication Server 1000 Release 5.0 and Microsoft Exchange 2007 Unified Messaging.

Chapter 2: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, go to www.avaya.com/support. From this Web site, locate the Training link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Chapter 3: Avaya Communication Server 1000 with Microsoft Exchange Server 2007 Unified Messaging

Overview

Avaya Communication Server 1000 (Avaya CS 1000) support for Microsoft Exchange Server 2007 Unified Messaging (UM) enables interoperability between the voice service capabilities of Avaya CS 1000 and the Unified Messaging solution provided as a component of Microsoft Exchange Server 2007. This interoperability provides the following capabilities:

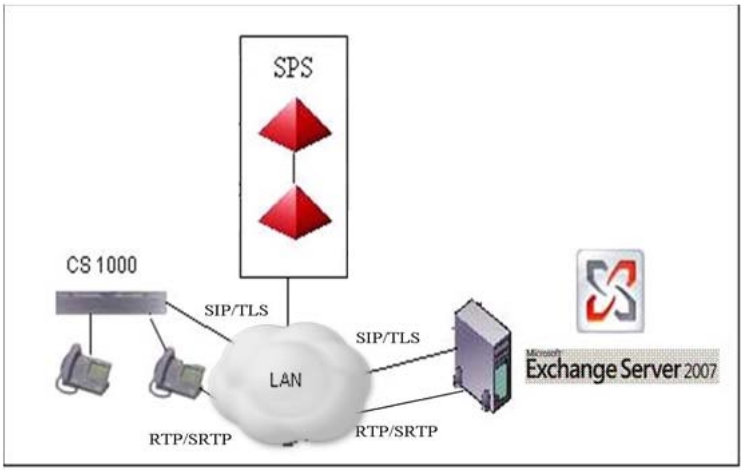
- Call Answering: With call answering, Avaya Communication Server 1000 with Microsoft Exchange Server 2007 Unified Messaging is configured to answer incoming calls on behalf of a user by playing their personal greeting, recording a voice message from the caller, and submitting it for delivery to the user inbox as an e-mail message.
- Subscriber Access: enables dial-in access for users. A subscriber dialing into the Microsoft Exchange Unified Messaging system accesses their mailbox using Outlook 2007 Voice Access, enabling access using either a telephone keypad or voice inputs. When dialed into the Unified Messaging system using a telephone, a subscriber or user can perform the following functions:
    - Listen to, forward, or reply to voice mail messages, and call the sender of the voice mail.
    - Listen to calendar information.
    - Access or dial contacts stored in the global address list or in a personal contact list.
    - Accept or cancel meeting requests.
    - Set a voice mail Out-of-Office message.
    - Set security preferences and personal options.
- Auto Attendant: Provides a set of voice prompts that provides access to the Microsoft Exchange Unified Messaging system by external users. Using the Auto Attendant, the external user navigates the menu structure, using either the telephone keypad or speech inputs, to place a call to a user or to locate a user for the purpose of placing a call to that user. In addition, the Auto Attendant gives system administrators the ability to perform the following functions:
    - Create a customizable set of menus for use by external users.

- Define informational greetings, business hours greetings, and non-business hours greetings, and greetings for holiday schedules.
- Add instructions for callers describing how to search the organizational directory, and how to connect to a specific user by means of their extension number.
- Enable access for external callers to the operator. For more information, see Configure the Operator Assistance feature on page 37.

- Play on Phone: Allows a Microsoft Exchange Unified Messaging-enabled user to access a voice mail message through Outlook 2007 or Outlook Web Access and listen to the message over a telephone.
- Message Waiting Indication (MWI): Designed by Geomant, the MWI application is an add-on to the Microsoft Exchange Unified Messaging Server 2007 which provides support for MWI notifications to users connected to the Microsoft Exchange Unified Messaging Server. For more information on the installation and configuration of the Geomant MWI application, see Geomant Message Waiting Indicator (MWI) application installation on page 39 and Configure Geomant Message Waiting Indicator (MWI) application on page 40.

Note:

The MWI 2007 software is a third-party software developed by Geomant. Information on Geomant and MWI 2007 is provided in this documentation for ease of reference only. Avaya does not sell, warrant or provide operational support for the Geomant MWI 2007 software product, nor warrant the accuracy of MWI 2007 descriptions contained in this document. Avaya recommends obtaining the most recent MWI 2007 documentation from Geomant.



Multiple Microsoft Exchange Unified Messaging servers on a single network

Multiple Servers can be configured for a single network to ensure the effective handling of potential issues caused by challenges of:

- Capacity: Each Microsoft Exchange Unified Messaging Server is capable of supporting a maximum of 200 total concurrent (combination of inbound and outbound) calls. In larger customer networks that need to support a higher volume of concurrent calls, additional Microsoft Exchange Unified Messaging Servers can be configured in the same network so that users can be load-balanced.
- Redundancy: An additional Microsoft Exchange Unified Messaging Server can be configured as a redundant server in a network by utilizing the Least Cost Routing Mechanism on the Network Routing Service (NRS) - configuring an additional Microsoft Exchange Unified Messaging Server provides a greater measure of fault tolerance for the services provided, allowing a continuation of those services in the event of system failure
- Geographical location: If network systems are located across multiple geographic locations, Microsoft Exchange Unified Messaging Servers can be implemented in such a way that they are both local and specific to each location. Configuring multiple servers in this way would automatically result in load sharing of access to Microsoft Exchange Unified Messaging services by users in the network.

Operational Considerations

Considerations specific to Microsoft Exchange Server 2007:

- Microsoft Exchange Server does not support Early media.
- The supported codecs are G.711 and G.723.
- RFC2833 is required for DTMF digit transmission to the Exchange Server.
- Exchange Server 2007 must always be configured as a static endpoint on the NRS as Registration is not supported.
- The Fax on UM capability is supported.
- Geomant Message Waiting Indicator (MWI) 2007 is a required add-on for MWI functionality.
- Microsoft Outlook 2007 is required.
- Exchange Server 2007 requires the use of x64 processors.

- For the Play on Phone option to function, the default Outlook data file used must be of type .ost. If the default Outlook data file is of type .pst, the Play on Phone option is not available.
- Calling a non-Exchange user using the Auto Attendant functionality is not supported by Microsoft Exchange Unified Messaging.
- Due to known issue concerning support of Payload 101 for RFC2833, intermittent DTMF issues will be experienced with PC-based clients.
- Interoperability with Avaya BCM/SRG and Avaya CS 2100 over H.323 causes speech path issues due to non-handling of RE-INVITE requests by Microsoft Exchange Unified Messaging Server.
- SRTP is not supported on Exchange for Avaya CS 1000 Release 5.5 and earlier.
- Exchange UM does not support Geographic Redundancy as the functionality is not available for performing a health check on the IP gateways and for any retry attempts on the next available gateway if the first choice fails to respond.

Considerations specific to the Geomant MWI Application:

- In a Main Office-Branch Office (MO-BO) environment, MWI functionality is provided in either Normal or Local mode, as MWI is not supported as multiple instances in the same domain.
- In a Geographic Redundant System environment, MWI functionality is provided in either a Primary Call Server (PCS) or a Secondary Call Server (SCS) system, as MWI is not supported as multiple instances in the same domain

Considerations specific to the Avaya Communication Server 1000:

- Only CDP dialing is supported between the home Avaya CS 1000 and the UM Server - users dial in to the home Avaya CS 1000 using any configured dialing plan to access services provided by Avaya Communications Server 1000 with Microsoft Exchange Server 2007 Unified Messaging.
- Configuration of the voice mail soft key cannot be changed if there is a combination of Avaya CallPilot™ and Microsoft Exchange Unified Messaging voice mail users on a single node. A recommended deployment solution would be to have Avaya CallPilot ™ users and Microsoft Exchange Unified Messaging users associated with separate Line TPS nodes.

  The voice mail soft key feature on the phone set assigns a unique key to each of the voice messaging functions.
- While operating with an MCS PC Client, Microsoft Exchange Unified Messaging calls cannot be placed on hold.
- The existing limitation on the NRS of multiple endpoints with the same static IP address is not supported. This affects network environments where two CDP domains are configured to use the same Microsoft Exchange Server 2007.

- The Avaya 2050 IP Softphone does not support RFC2833; therefore, it cannot be used with the Subscriber Access and Auto Attendant features of the Exchange Server 2007.
- If a call originates from an H.323 endpoint (Avaya CS 1000/Avaya BCM/SRG) and is tandem transferred by the Avaya CS 1000 to the Microsoft Exchange Unified Messaging Server using SIP, the Subscriber Access and Auto Attendant feature can only be accessed by voice command and not by keypad (DTMF), as there is no support for RFC2833 over an H.323 network.
- If the far end does not support RFC2833 (with a payload value of 101), the Play on Phone functionality is not supported.
- Calls forwarded by Integrated Call Director (ICD) to Microsoft Exchange Unified Messaging are not supported.
- If a call originates from CS 1000 Node A to Node B (TRO is enabled on both the nodes) which has call forward set to UM, same SA/AA DNs must be configured on both the nodes since the call is originated from Node A (and not Node B) in this case.

Microsoft Exchange Unified Messaging operational characteristics

- When a Microsoft Exchange Unified Messaging-enabled user plays back stored voice mail messages, the order of playback begins with the last message recorded. That is, when voice mail has been received (in order) from User 1, User 2, and User 3, the messages are replayed in the order of User 3, User 2, User 1.
- For a voice mail message that is a reply to an earlier voice mail message, the reply message is played before the playback of the original message.
- If there is only one voice mail message waiting for the user, it is not possible to undelete that voice mail message once it has been deleted.
- Voice mail messages that have been listened to will continue to register as a new message until the next option is used.
- When a user dials the Auto Attendant number (with speech enabled) and does not provide a name, Auto Attendant repeats the prompt for a name three times. After the third prompt, the call is forwarded to the operator automatically.
- Call answering does not work if the call is being redirected across CS 1000 nodes (or any SIP Gateways) with different dial plans.The Unified Messaging fails to answer calls from User A.

  For example, there are two users–User A on node_A, with DP_A and User B on node_B, with DP_B, User A's phone is set to forward all calls to B's DN.

  The UM is not able to resolve mailbox for User A between cross-dial plans.

Secure Real-Time Protocol support for Microsoft Exchange Server 2007 Unified Messaging

Avaya CS 1000 Microsoft Exchange Server 2007 Unified Messaging for supports Secure Real-Time Protocol (SRTP) in the following scenarios:

- Scenario 1—CS 1000 with SRTP using Exchange Server 2007 for voice mail.
- Scenario 2—CS 1000 interoperating through Multimedia Convergence Manager with Office Communication Server 2007 and Exchange Server 2007.
- Scenario 3—CS 1000 interoperating through Multimedia Convergence Manager with Integrated Office Communication Server 2007 and Exchange 2007.

Important:

TLS must be enabled between CS 1000, Exchange Server 2007, and Office Communication Server 2007 for SRTP to function. For more information about TLS, see *Avaya Security Management Fundamentals* (NN43001-604). For more information about Multimedia Convergence Manager with Integrated Office Communication Server 2007, see *Avaya Converged Office Fundamentals – Microsoft Office Communications Server 2007* (NN43001-121).

If CS 1000 and Unified Messaging are in different domains served by different DNS servers, each DNS server should have forwarders configured, which contain the domain name and IP of the other DNS server. So, if the first DNS server cannot resolve the FQDN, the DNS server itself would forward the request to the other DNS servers.

Scenario 1

This scenario describes the CS 1000 with SRTP using Microsoft Exchange Server 2007 for voicemail.

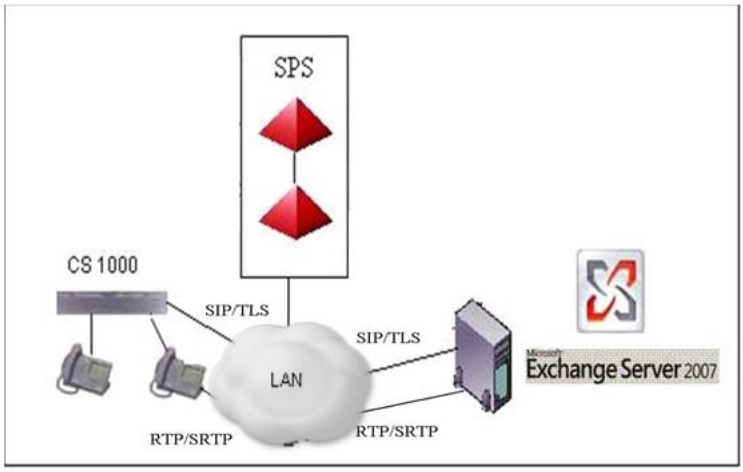


Figure 1: CS 1000 with SRTP using Microsoft Exchange Server 2007 for voicemail

Scenario 2

This scenario describes how the CS 1000 interoperates through Multimedia Convergence Manager with Office Communication Server 2007 and Exchange Server 2007

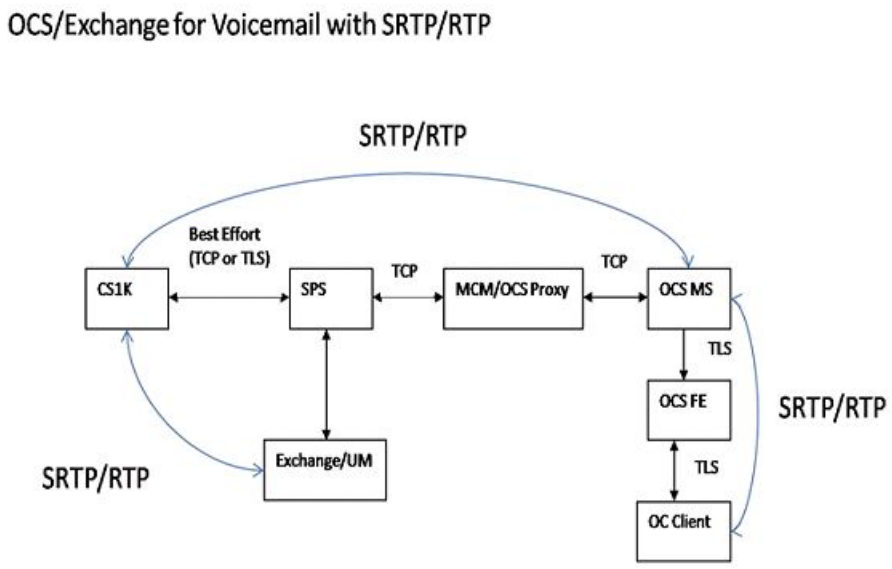


Figure 2: OCS/Exchange for Voicemail with SRTP/RTP

Scenario 3

This scenario describes how the CS 1000 interoperates through MCM with Integrated OCS 2007 and Exchange 2007

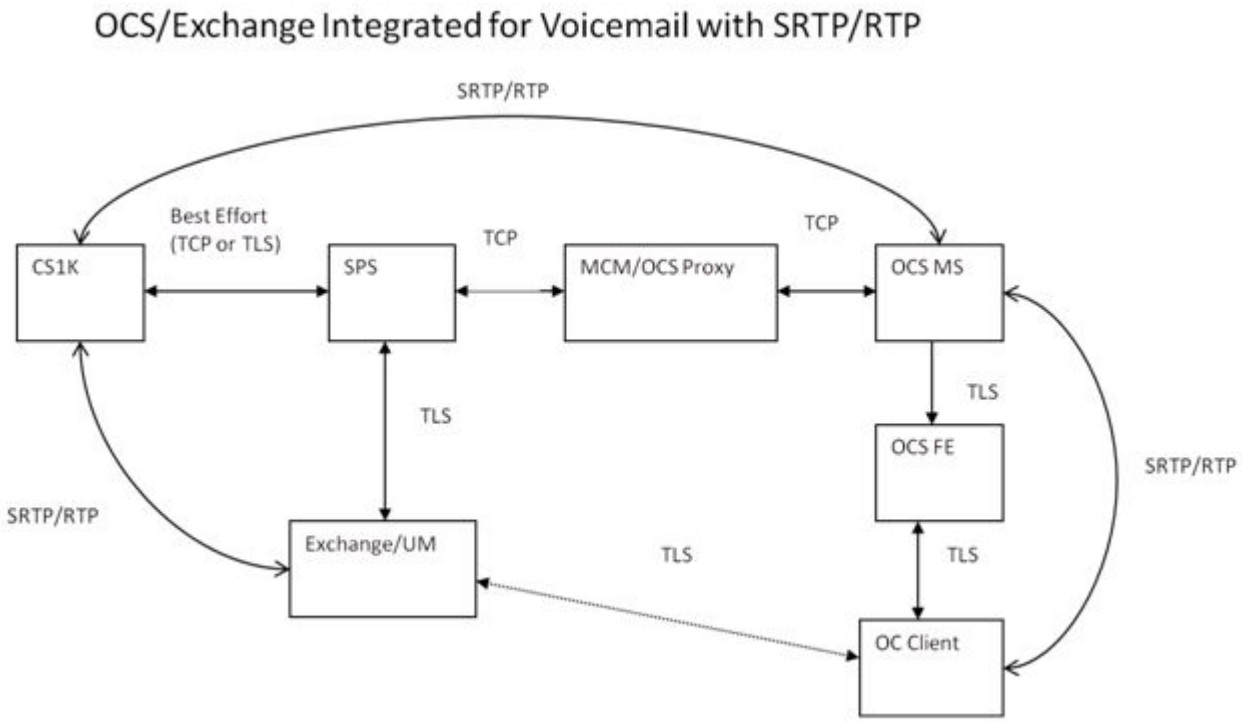


Figure 3: OCS/Exchange Integrated for Voicemail with SRTP/RTP

Feature Interactions

The following table provides feature interactions.

Table 1:

SRTP	Wave 13	RTP/SAVP, 200 OK, using RTP/AVP
best-effort SRTP	Microsoft Exchange 2007 Service Pack 1. VOIP Security: Secured	200 OK, using RTP/SAVP

best-effort SRTP	Microsoft Exchange 2007 Service Pack 1. VOIP Security: SIP Secured	503 Services Not Available
best-effort SRTP	Microsoft Exchange 2007 Service Pack 1. VOIP Security: Unsecured	503 Services Not Available

CS 1000 Interaction with Exchange 2007 Service Pack 1 and Exchange 2007 Wave 14

In order for CS 1000 and Exchange to communicate through SRTP, Element Manager must be configured to indicate if VOIP Security is configured as “Secured”. The following scenario is common between a Best Effort CS 1000 SIP INVITE to Exchange 2007 Service Pack 1 and Exchange 2007 Wave 14.

(1) A Best Effort offer to Exchange with VOIP Security: Secured

v=0 o=- 122 3 IN IP4 192.168.117.230 o=- 122 3 IN IP4 192.168.117.230 s=- t=0 0 c=IN IP4 0.0.0.0 m=audio 5200 RTP/AVP 0 8 101 111 a=tcap:1 RTP/SAVP a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:NatI39V92Sgt0WOOhzMIqBZJIb0lkZD7vykD 0uLJ|2^31|2776763240:4 a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:NatI39V92Sgt0WOOhzMIqBZJIb0lkZD7vykD 0uLJ|2^31 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 a= sendrecv a=pcfg:1 t=1

Below is a sample answer to Offer 1:v=0 o=- 128 2 IN IP4 192.168.116.230 s=- t=0 0 c=IN IP4 0.0.0.0 m=audio 5200 RTP/SAVP 0 8 101 111 a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:KY2o2u8S0tKrnai4YO0STMDvnquDOEPLWbczkHJZ|2^31|2776763240:4 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 a= sendrecv

From the sample above, the initial Best Effort offer: it supports the following Media Profiles: RTP/SAVP and defaults to RTP/AVP if RTP/SAVP cannot be used. Exchange responds with RTP/SAVP to indicate its usage of SRTP and does not include the media level attribute acfg.

Limitations

Secure Real-Time Protocol support for Microsoft Exchange Server 2007 Unified Messaging limitations

- CS 1000 has the capability to understand and process the acap attribute in an incoming offer but does not make use of it in the response or in a new offer as defined in Avaya’s SRD Section 16.6.2.[1]
- When CS 1000 is used with Exchange 2007 that has VoIP Security set as Secured, all mailboxes associated with that secured Dialling Plan are treated with a Media Security Class of Service of Always Secured. When VOIP Security is configured as Secured, it

requires the use of TLS for SIP Signalling between Exchange and CS 1000. Any IP or digital phones that do not support SRTP are not compatible with Exchange if VoIP Security is configured as Secured. The Exchange Unified Messaging 2007 Wave 14 limitations are unknown at this time.

- Exchange 2007 SRTP does not support MKI or <“from”, “to”> rekeying, however since the typical lifetime of RTP and RTCP packets is 2^31 this means supporting key update is unnecessary.

  Exchange 2007 does not renegotiate a new security context and uses the current security context for it to receive and send stream during a SIP REINVITE.

Table 2: Features not supported with Exchange 2007 SP 1 when SRTP and TLS are enabled

Action	Supported
Call on Hold	Not Supported
Call Transfer (blind)	Not Supported
Call Transfer (consultative)	Not Supported
Call Conference	Not Supported

Exchange 2007 Unified Messaging SP1 and Wave 14:

The patch to negotiate best effort SRTP does not impact previous limitations between CS 1000 5.x and Exchange 2007 Unified Messaging SP1 and Wave 14.

CS 1000 phone configuration

This section details phone configuration to provide operation for Avaya Communication Server 1000 with Microsoft Exchange Server 2007 Unified Messaging.

Required class of service configurations are as follows:

- CFXA (Call Forward External): Allowed
- FNA (Call Forward No Answer): Allowed
- HTA (Hunting): Allowed
- CLS (Trunk: Call Access Restriction): Unresricted
- MWA (Message Waiting Indicator): Allowed

Both FDN (Call Forward No Answer DN) and Hunt (Hunt DN) must be configured to the value for the configured Subscriber Access DN.

SIP provisioning guidelines

This section details the SIP provisioning requirements for operations on Avaya Communication Server 1000 with Microsoft Exchange Server 2007 Unified Messaging and/or via overlay.

For CS 1000 configuration information, see the following documents:

- *Avaya CS 1000 Input/Output: Administration* (NN43001-611)
- *Avaya CS 1000 Element Manager System Reference - Administration* (NN43001-632)

Configuring SIP/Virtual Trunks, Route, Dialplan, Route entries and Endpoints for CS 1000 to interoperate with Exchange/UM using Element Manager and/or through overlay

1. Create a new virtual D-Channel to the Node that registered in the Exchange Server - LD 17.
2. Create Virtual Route (RDB) using the D-Channel (LD 16) with following parameters: "PCID=SIP, INAC=Yes, CTYP-ukwn."
3. Create Virtual Trunks for the Route previously created - LD 14.
4. Create DMI(DGT), with no deletion or insertion - LD 86.
5. Create RLB using Route and DMI previously created in steps #2 and #4 - LD 86
6. Create CDP Distant Steering Code to route the call to the Exchange Server - LD 87.
7. Create ACD DNs with NCFW configured for both Subscriber Access and Auto Attendant numbers - LD 23.
8. For all subscriber phones, configure FDN/HUNT to Subscriber Access number and add the following features in CLS (LD 11): FNA, HTA, HFA, WTA, FBA, MWA, SFXA.

Configuring SIP/Virtual Trunks, Route, Dialplan, Route entries and Endpoints for CS 1000 to interoperate with Exchange/UM using NRS

1. Add the Exchange Server and its IP address as a Static endpoint on NRS; and fill in the field "Static endpoint address" with the Exchange Server IP.
2. Add Routing Entries for Exchange Server gateway endpoint: DN type: Private Level 0 regional (CDP Steering Code) DN prefix: the Distant Steering Code

Assumptions

- Call model and traffic rate calculations are based on the assumptions provided by Microsoft for a typical heavy user, as described at the following URL: http://msexchangeteam.com/archive/2006/08/14/428677.aspx
- A single Microsoft Unified Messaging server can have up to 3 000 heavy users associated with it.
- All Microsoft Unified Messaging messages are received by telephone using an SIP Trunk, and not using Microsoft Exchange Client (which does not use an SIP Trunk).
- The use of Auto Attendant for Thru-Dial and other custom voice menu services makes the following assumptions:
  - Menu selection and call transfer time is 30 seconds, with a completed call duration of 180 seconds.
  - Busy Hour (BH) Auto Attendant usage is 0.35 calls per hour for each Microsoft Unified Messaging user.
- Auto Attendant operation requires the usage of two SIP trunks, which remain in use for the duration of the call.
- If Microsoft Unified Messaging system usage differs from the call model described for the purpose of SIP trunk table calculations, it is the responsibility of the customer to monitor the actual usage of the system and ensure that there are sufficient SIP trunks available for use.

Table 3: Assumptions

Number of UM Users	Typical BH Call Duration (seconds)	Typical BH CCS	Erlangs (ccs/36)	Number of SIP Trunks (Erlang B P05 Grade of Service)	Number of SIP Trunks (Erlang B P01 Grade of Service)	Number of SIP Trunks (Erlang B, Non-blocking)
50	15000	150	4.17	8	10	24
100	30000	300	8.33	13	16	33
200	60000	600	16.67	22	26	49
500	150000	1500	42	48	55	89
1000	300000	3000	83	88	99	147
2000	600000	6000	167	170	187	254
3000	900000	9000	250	250	273	355

Chapter 4: Configuration of Avaya Communication Server 1000 with Microsoft Exchange Server 2007 Unified Messaging

For the tasks and procedures associated with configuring Avaya Communication Server 1000 with Microsoft Exchange Server 2007 Unified Messaging, see the following:

Note:

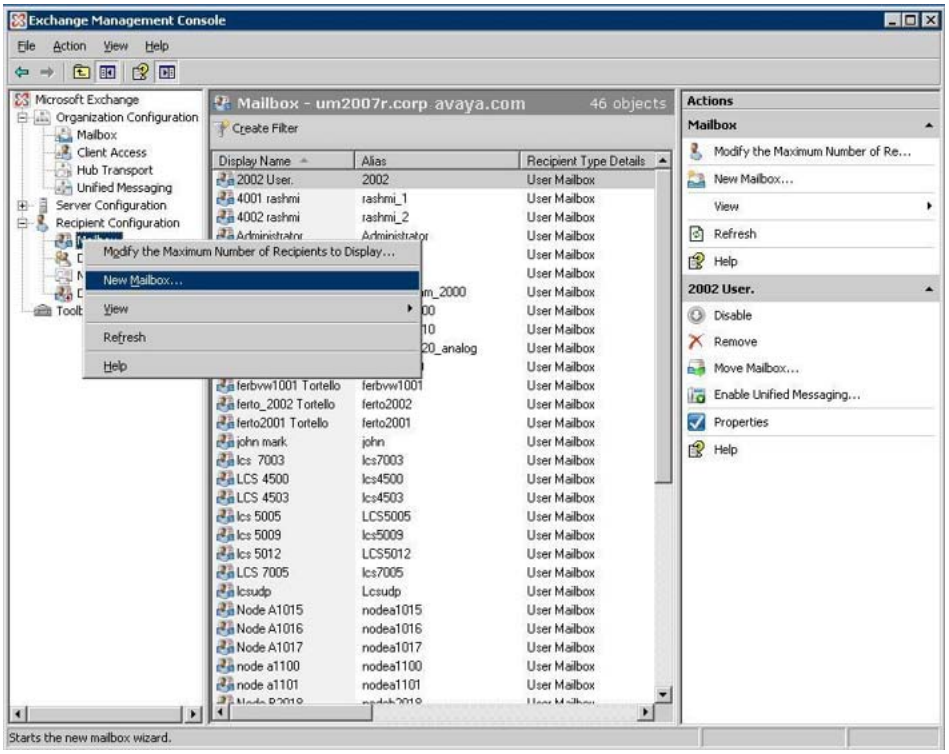
Throughout this document, screen captures of third-party software are included for the purposes of illustration only. While the screen captures in this document are believed to be accurate and reliable in their depiction of third-party software used in conjunction with this feature, the information is subject to change without notice. Therefore, Avaya presents all third-party screen captures in this document without express or implied warranty with regard to their complete accuracy.

Configure a new user mailbox for Microsoft Exchange Unified Messaging

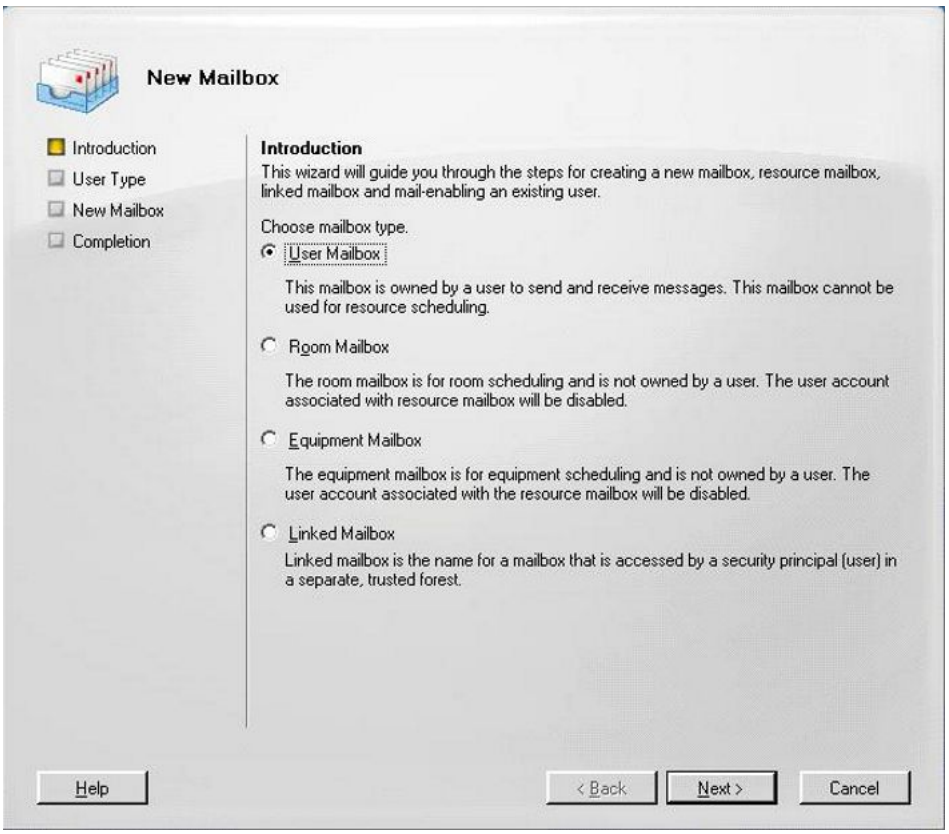
The following section details the required steps for the configuration of a Microsoft Exchange Unified Messaging mailbox.

Configuring a user mailbox for Microsoft Exchange Unified Messaging

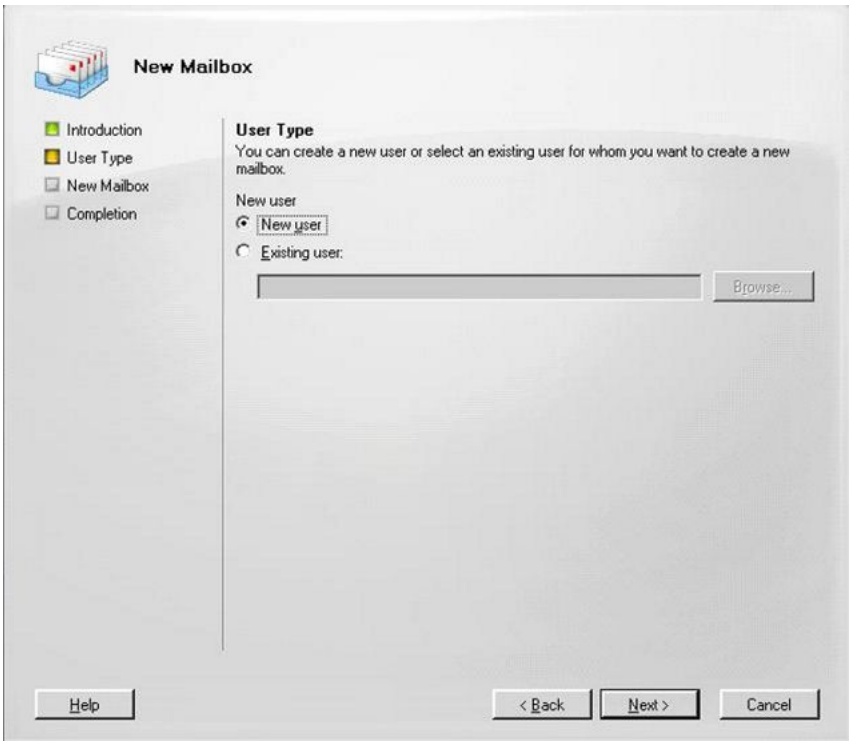
1. From the Exchange Management Console, select **Recipient Configuration** and right click on **Mailbox**. Select **New Mailbox**... to start the New Mailbox Wizard.



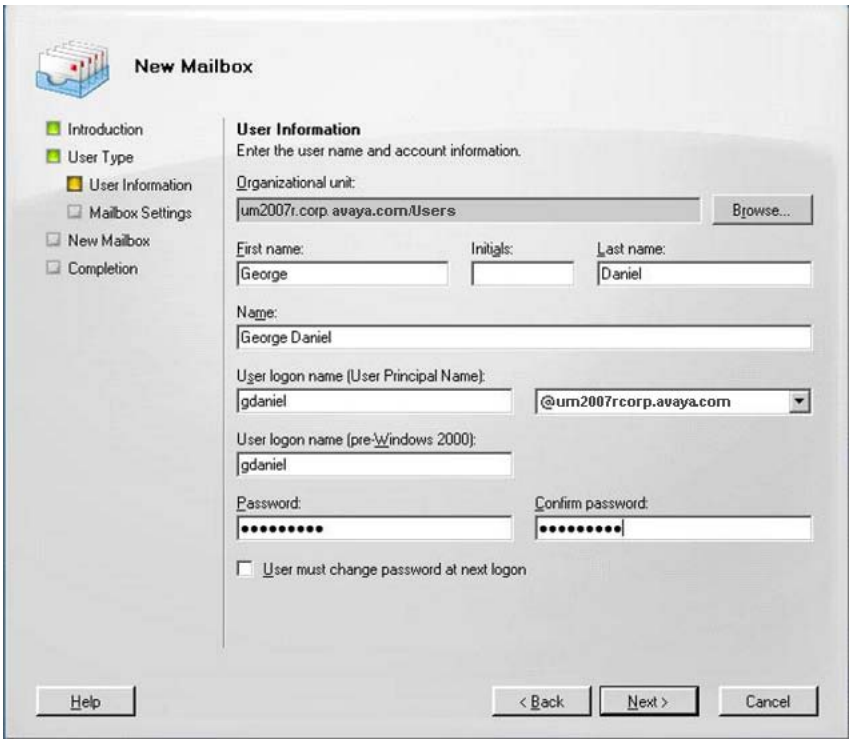
2. The opening screen for New Mailbox Wizard appears. Select **User Mailbox** and click **Next**, as shown in the following figure:



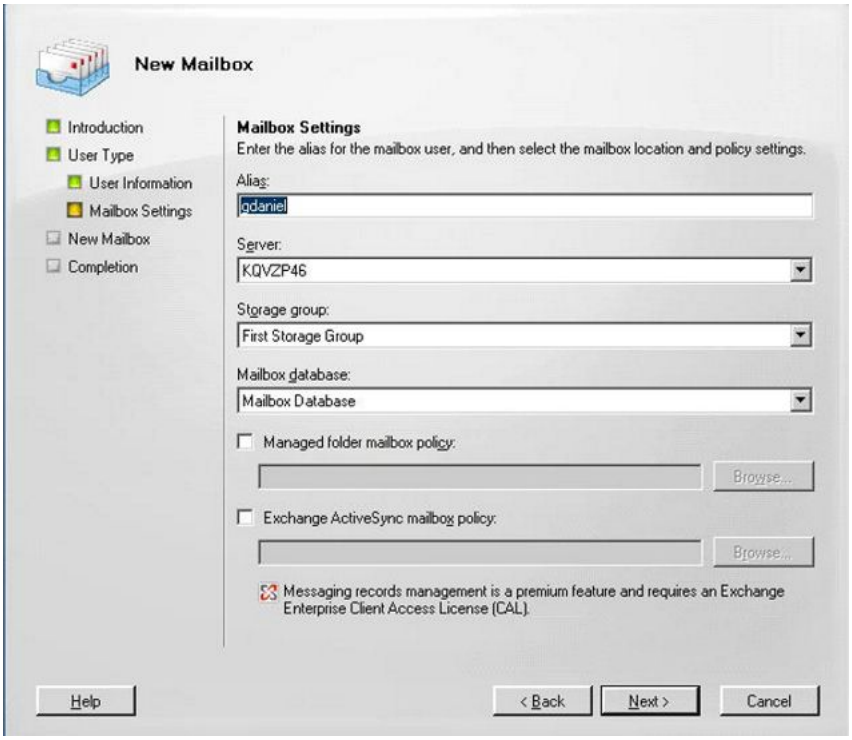
3. Select **New user** and click **Next**, as shown in the following figure:



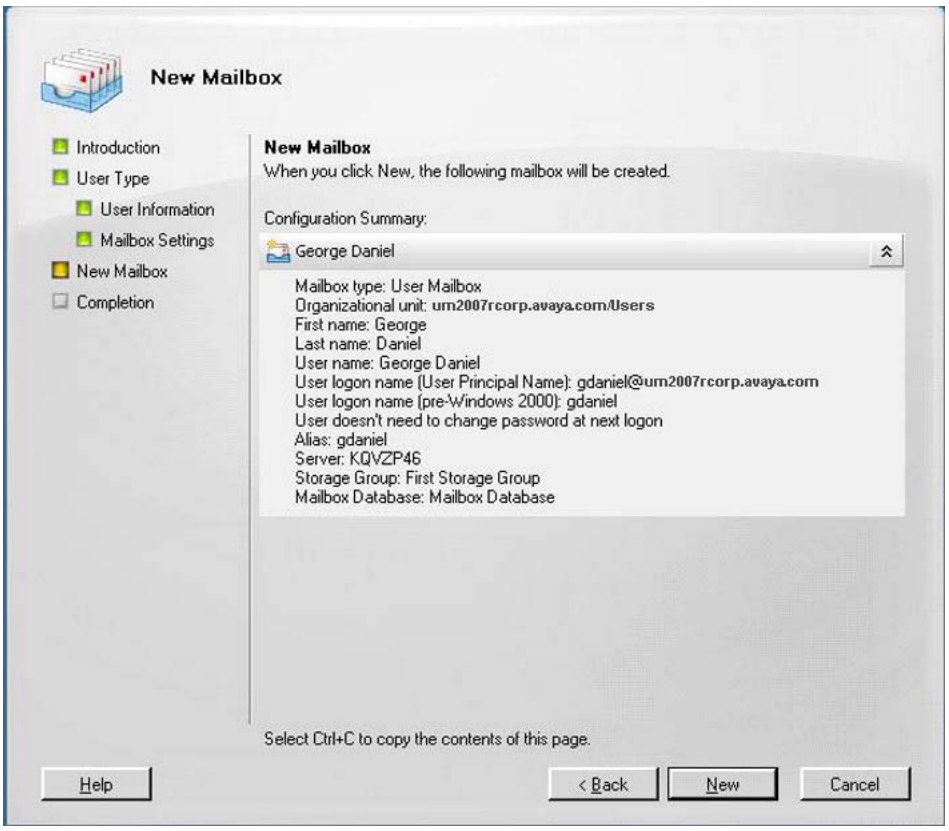
4. Enter account information for the mailbox user, as appropriate, as shown in the following figure:



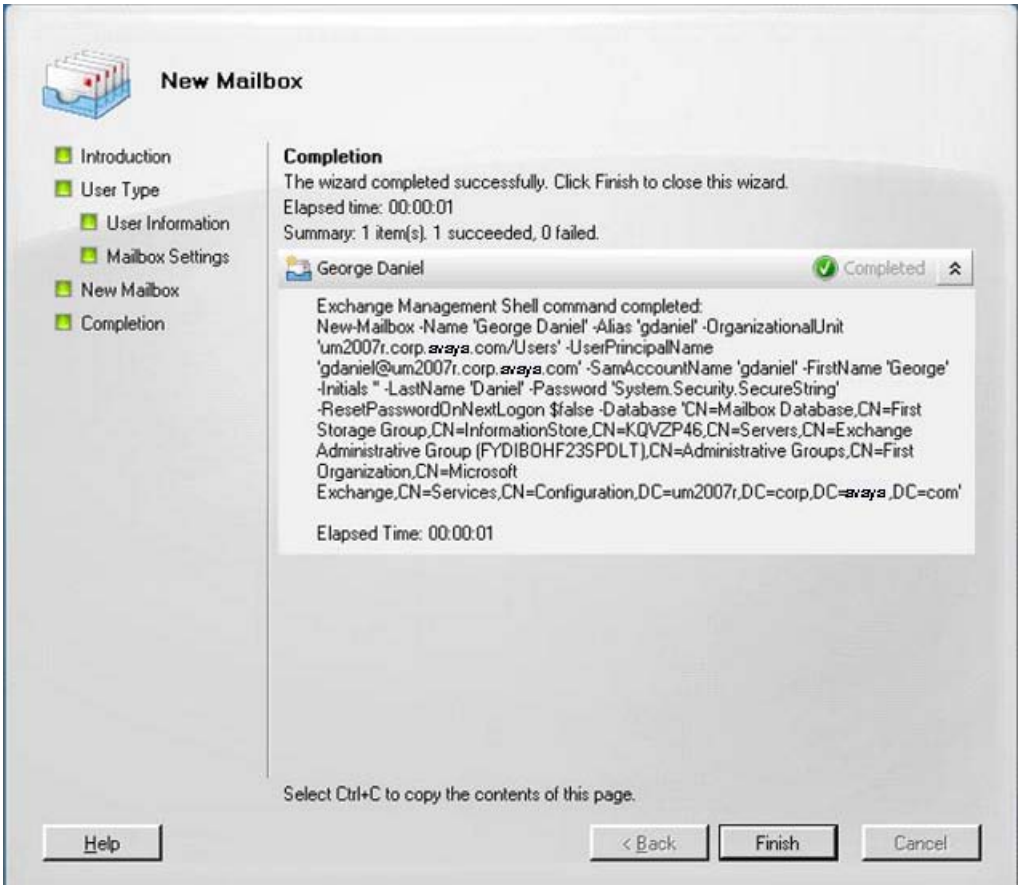
5. Click **Next** to continue
6. Enter the alias for the mailbox user, and select the mailbox location and policy settings, as shown in the following figure.



7. Click **Next** to continue.
8. The Configuration Summary for the current user mailbox is displayed, as shown in the following figure. Review for accuracy, and click **New** to create the user mailbox.



9. The completion screen of the New Mailbox Wizard appears. Click **Finish** to exit, as shown in the following figure:

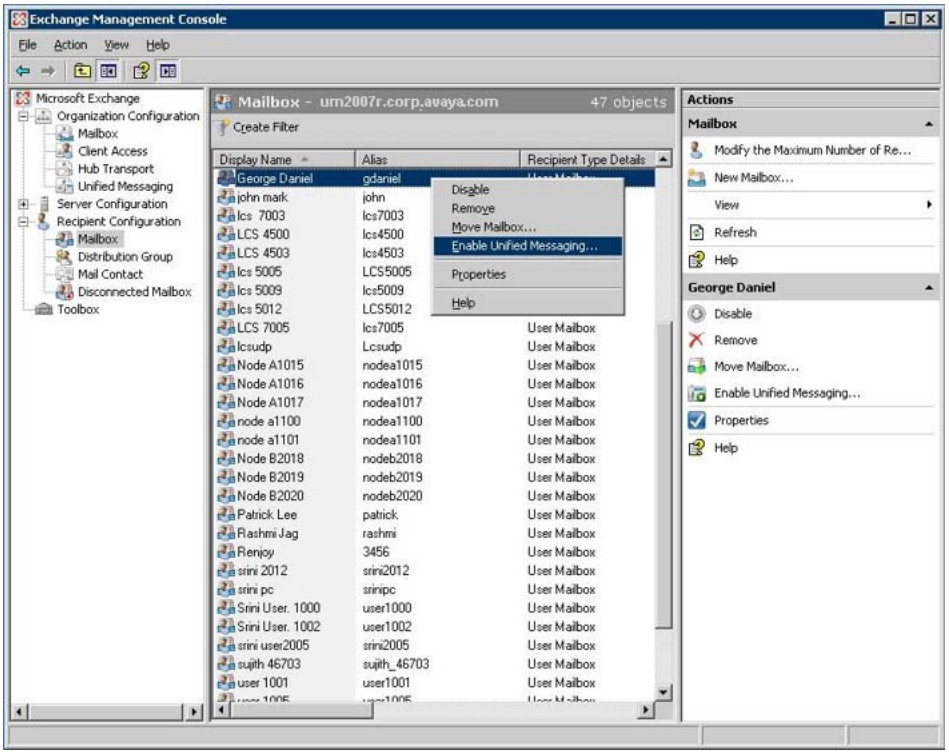


Enable a new user mailbox for use with Microsoft Exchange Unified Messaging

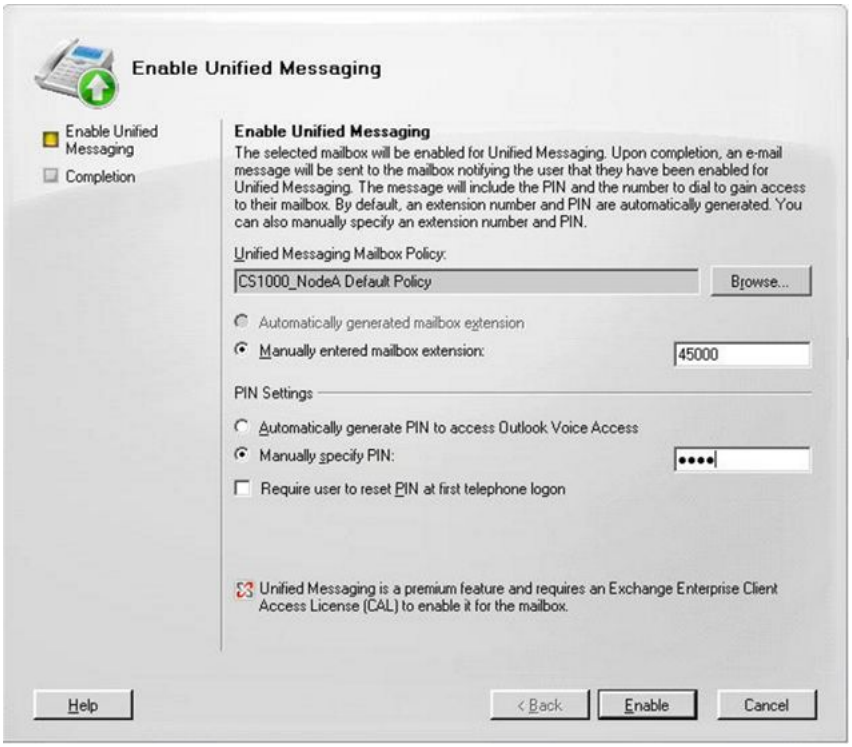
The following section details the required steps for the enabling an existing user mailbox for use with Microsoft Exchange Unified Messaging.

Enabling a user mailbox for use with Microsoft Exchange Unified Messaging

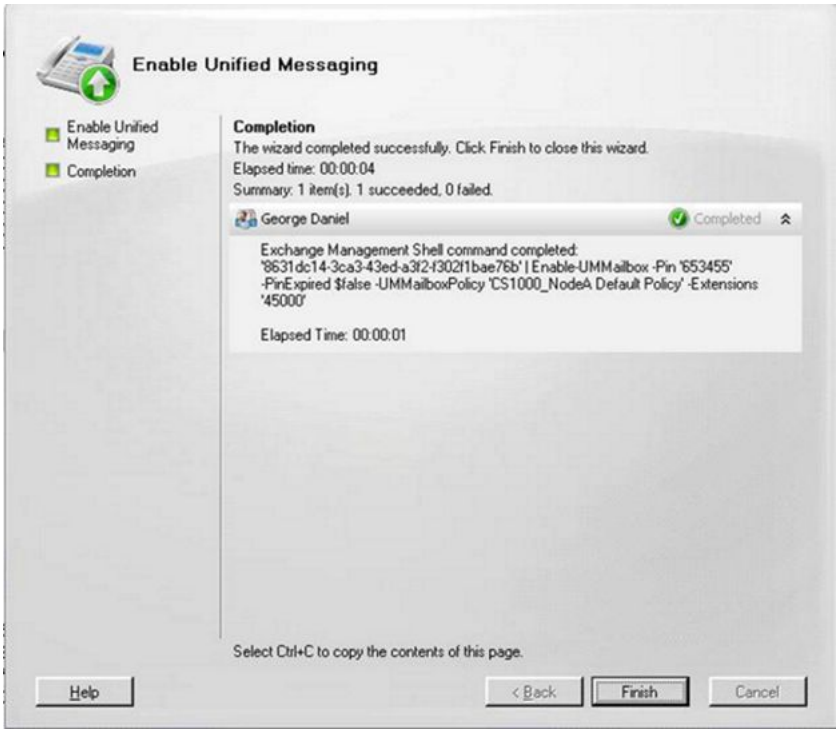
1. From the Exchange Management Console, select **Recipient Configuration > Mailbox**. Right click the specific user mailbox to be enabled and select **Enable Unified Messaging**, as shown in the following figure:



2. The Enable Unified Messaging Wizard appears, as shown in the following figure. Configure the Unified Messaging Mailbox Policy and PIN options, as appropriate for use on your network, and click **Enable**.



3. The completion screen of the Enable Unified Messaging Wizard appears. Click **Finish** to exit, as shown in the following figure:



Configure a new Dial Plan for Microsoft Exchange Unified Messaging

The following section details the required steps for the configuration of the Microsoft Exchange Unified Messaging Dial Plan.

Configure the Microsoft Exchange Unified Messaging Dial Plan

1. From the Exchange Management Console, select **Organization Configuration > Unified Messaging > New UM Dial Plan**. The New UM Dial Plan screen appears, as shown in the following figure:

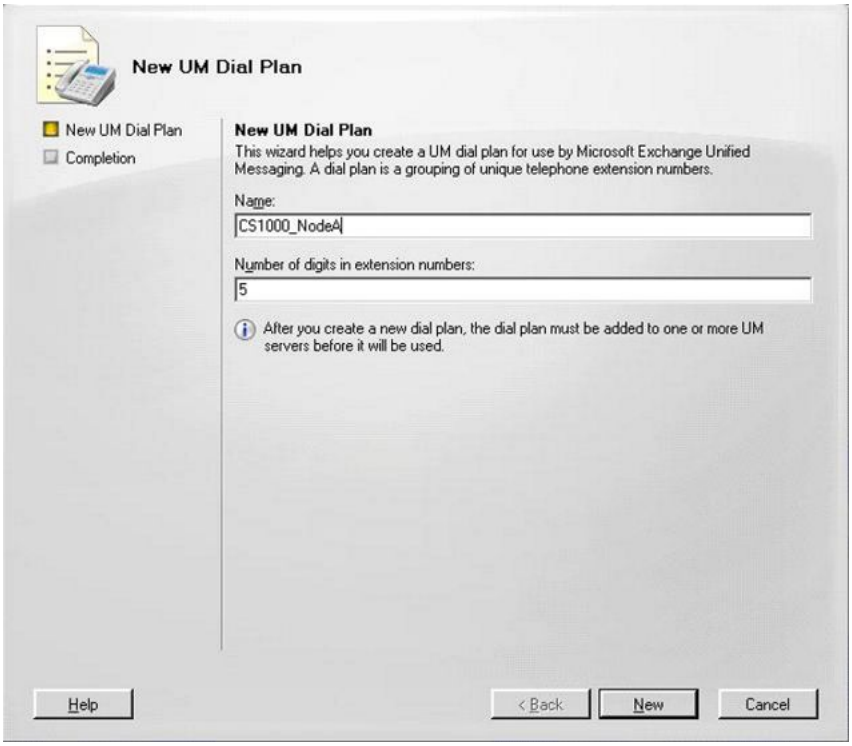


Figure 4: New UM Dial Plan screen

2. Enter the Dial Plan name and the number of digits used for the user extension expected. Click **New**. Right-click the newly-created Dial Plan and select **Properties**. The Dial Plan Properties screen appears.
3. Click the **General** tab. From the **VoIP security** drop-down list, select **Unsecured**, as shown in the following figure:

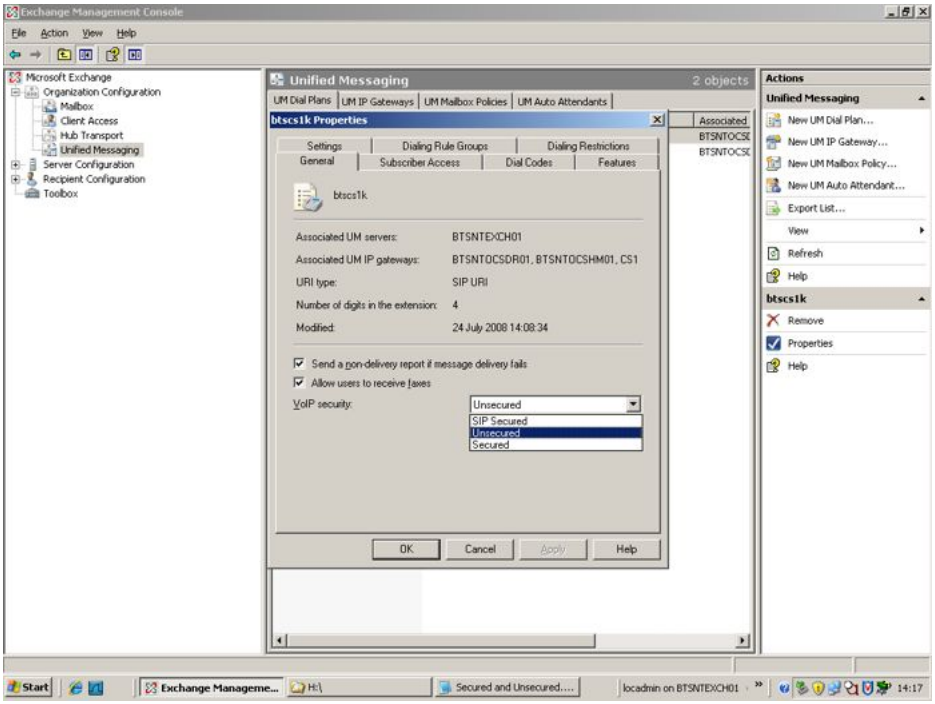


Figure 5: Dial Plan General Tab

4. Click the **Subscriber Access** tab. Specify the Welcome Greeting, Informational announcement value, and the Subscriber Access and Call Answer number to be associated with the new Dial Plan. Click **Apply** and then **OK** to accept, as shown in the following figure:

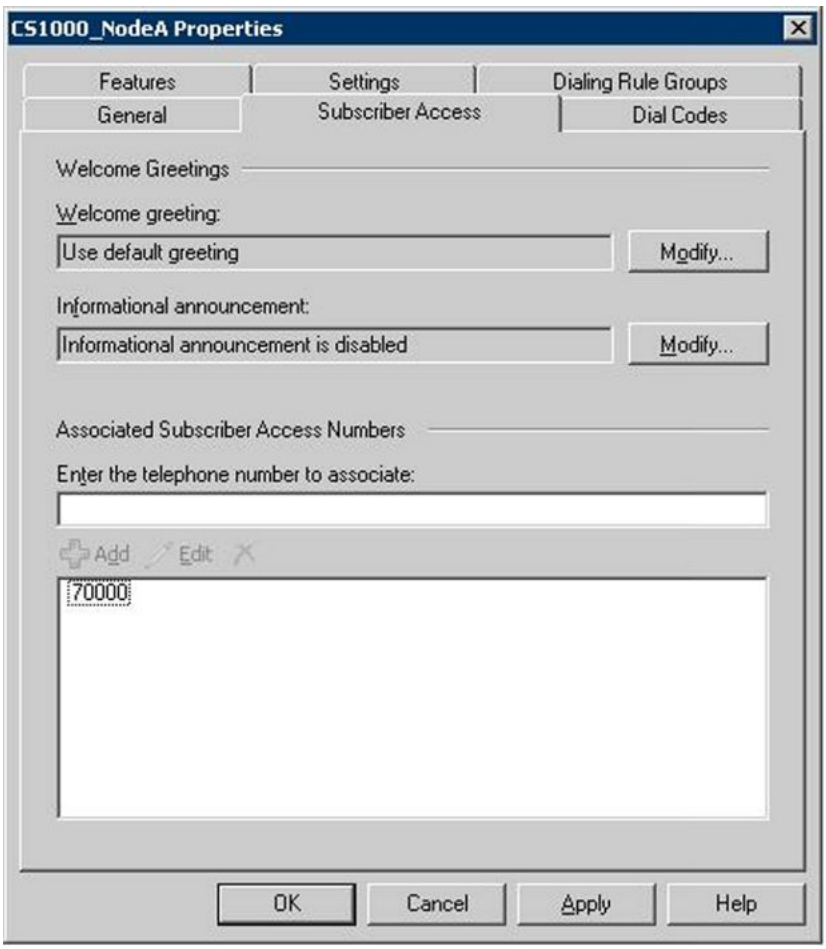
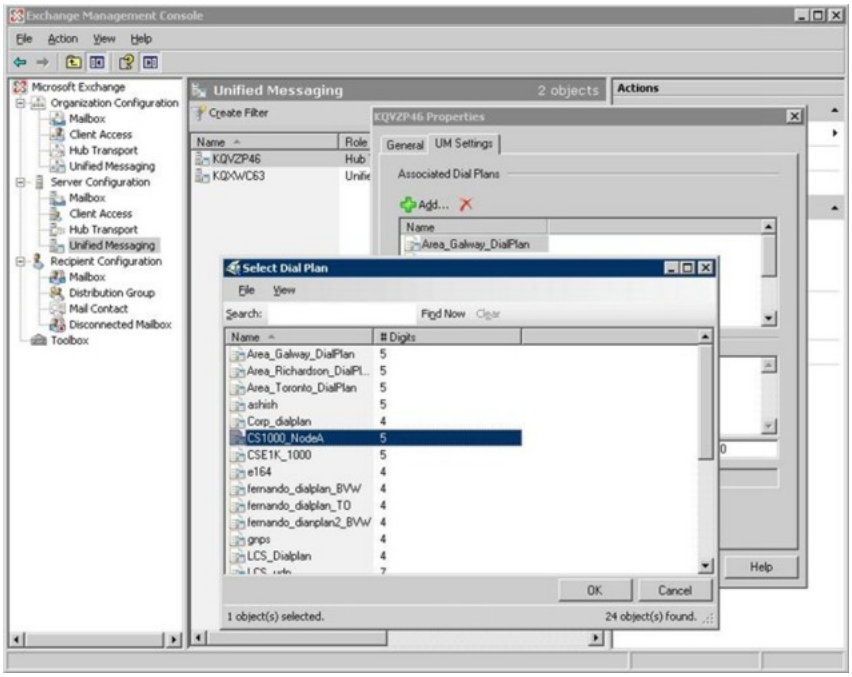
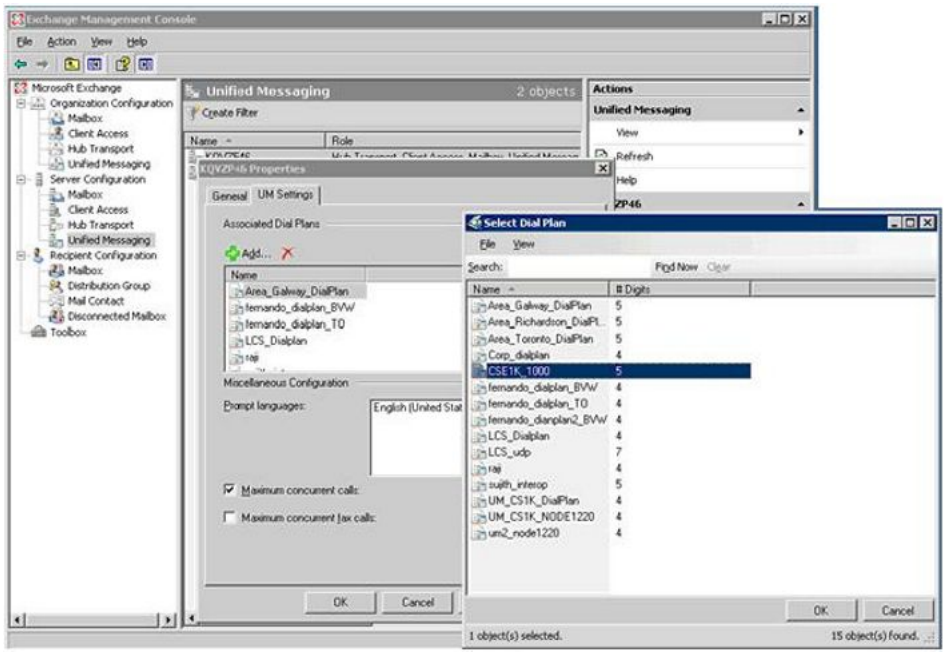


Figure 6: Dial Plan Properties screen

5. Select **Server Configuration > Unified Messaging**, and right-click the server name for which your newly-created Dial Plan is intended. Select **Properties**, as shown in the following figure:



6. Add the configured Dial Plan under the **UM Settings** tab, as shown in the following figure:



7. Click **OK**.
8. Specify the SIP Gateway name and IP address (Signaling Server node address) for the current Dial plan, as shown in the following figure:

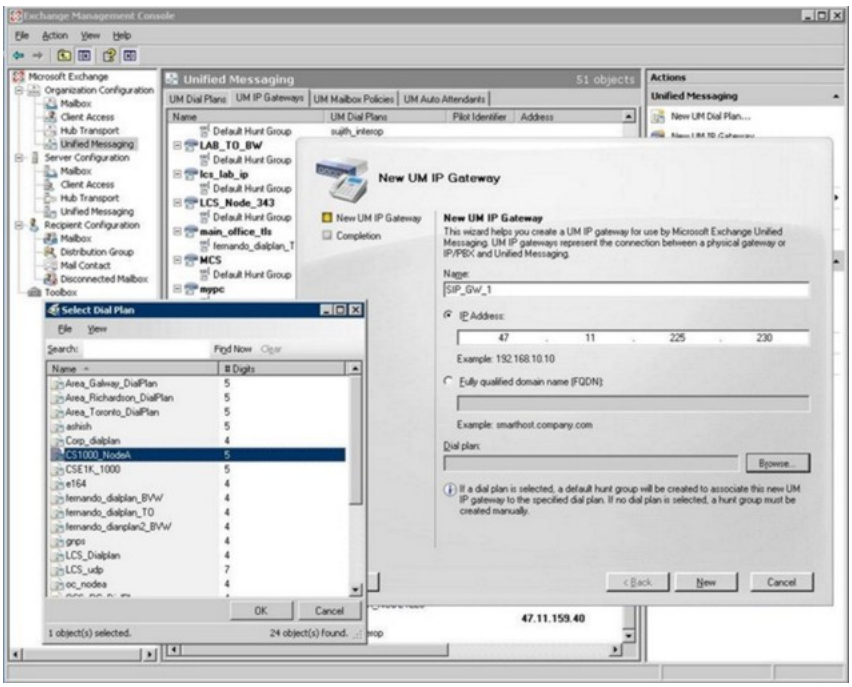
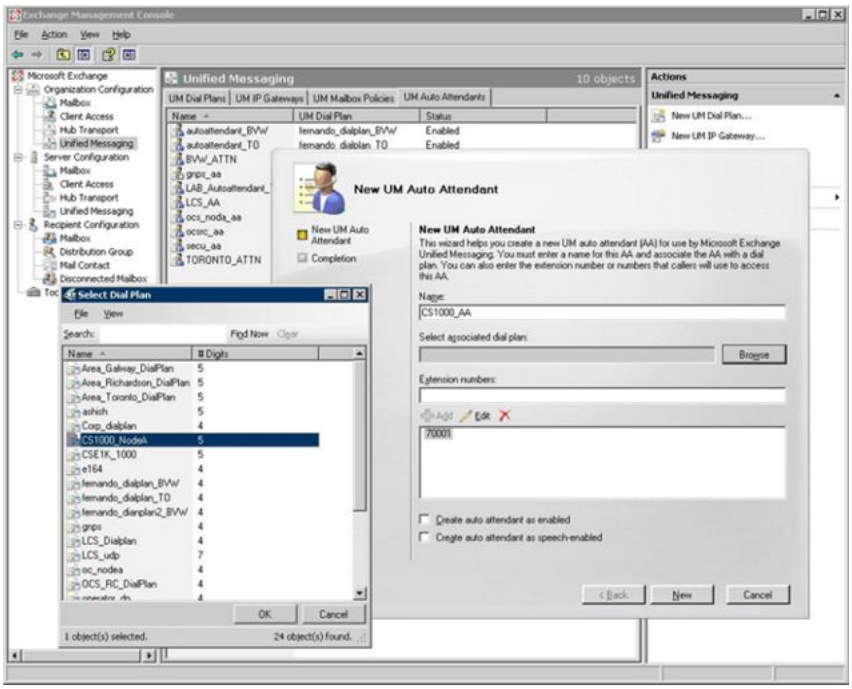


Figure 7: Configuration screen for new UM IP Gateway

9. Specify Auto Attendant name and number for the new UM Dial plan. The Auto Attendant Configuration number is provided for the UM Dial Plan configured, as shown in the following figure:



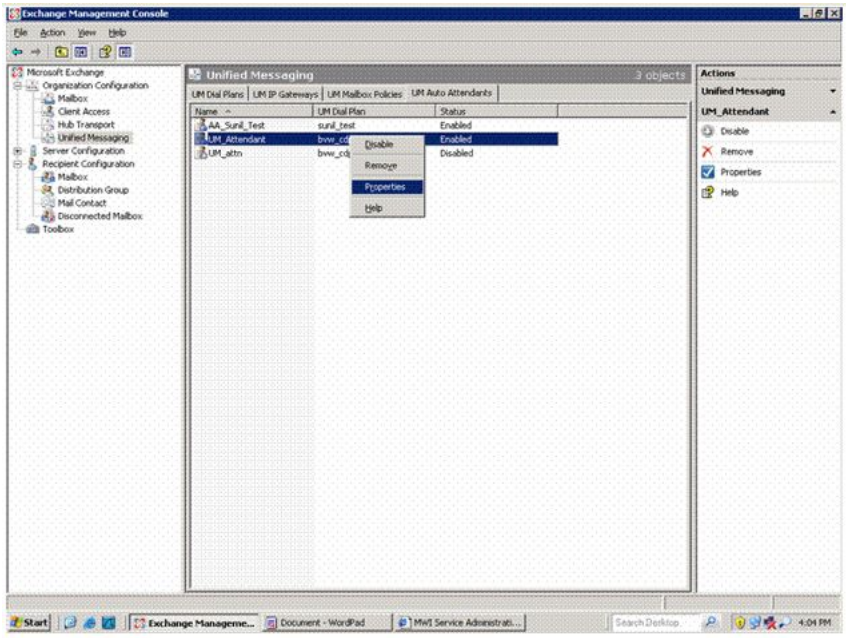
10. Allow users to receive fax under the dialing plan:
    - In the Exchange Management Console, expand the Organization Configuration node, and then click the **Unified Messaging** node.
    - On the **UM Dial Plans** tab, select the UM dial plan for which you want to allow users associated with the dial plan to receive fax messages, and then click Properties in the action pane.
    - On the dial plan Properties page, on the General tab, select the check box next to **Allow users to receive faxes**.
    - Click **OK** to save your changes.
11. Allow the user to receive fax under user profile:
    - In the Exchange Management Console, expand the Recipient Configuration node, and then click the **Mailbox** node.
    - In the result pane, select the user mailbox that you want to modify.
    - In the action pane, click **Properties**.
    - On the **Mailbox Features** tab, click **Unified Messaging**, and then click **Properties**.
    - On the Unified Messaging Properties page, select the check box next to **Allow the user to receive faxes**.
    - Click **OK** to save your changes.
12. On the Exchange Server, enable inband fax detection:
    - Go to C:\Program Files\Microsoft\Exchange Server\Bin
    - Open file globcfg.xml: <EnableInbandFaxDetection>false</EnableInbandFaxDetection>
    - Change to: <EnableInbandFaxDetection>true</EnableInbandFaxDetection>
13. Restart the Exchange UM service.

Configure the Operator Assistance feature

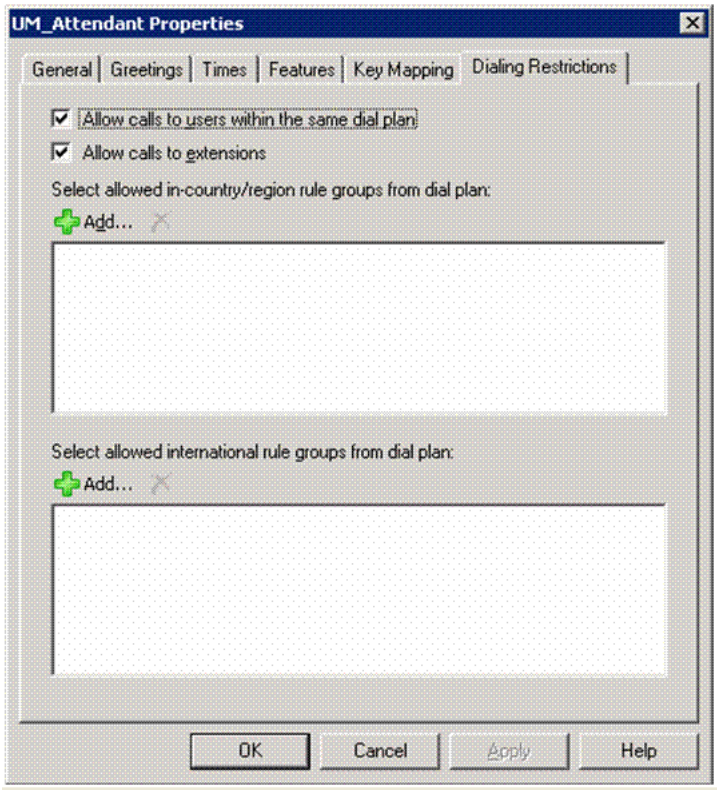
To configure the Operator Assistance feature to be used with a configured UM Dial Plan, perform the tasks in the following procedure:

Configure the Operator Assistance feature

1. After providing the operator assistance number in Dial Plan and Mailbox users, open the Exchange Management Shell.
2. Right-click on the **dial plan**, and select **Properties** from the list of the available options. Optionally, you can click on the properties menu in the action pane as shown in the following figure:

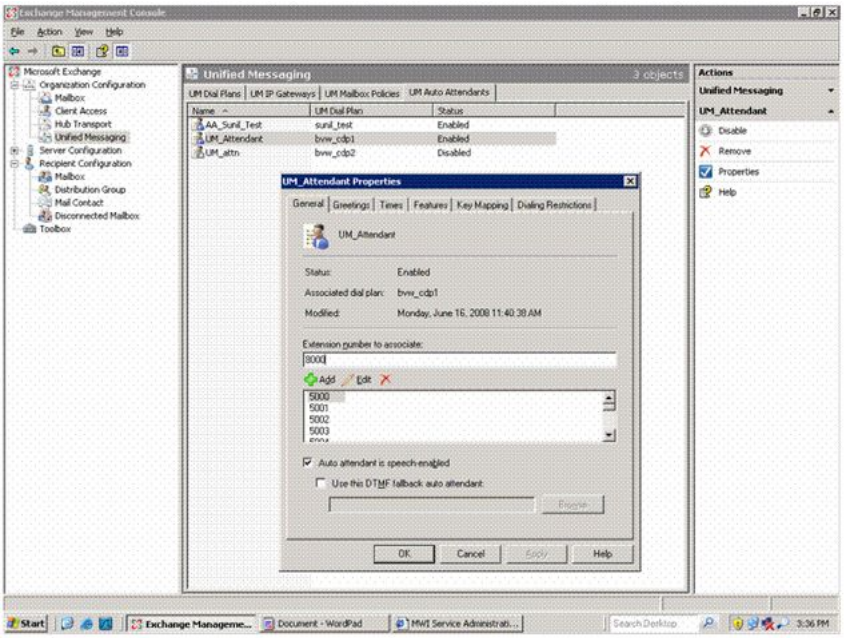


The Attendant properties window appears:



Select **Allow calls to extensions** under **Dialing Restrictions** and click **OK**.

3. Add an attendant number on the properties window, under the **General** tab, enter the DN number for the auto attendant, click **Add** and then **OK** to add:



After dialling the number, the prompts for Auto Attendant service are heard by the user.

Geomant Message Waiting Indicator (MWI) application installation

Prerequisites:

- Download the detailed procedures to be used in the installation of the Geomant MWI application at http://www.geomant.com/index.php?mainpage=true > Downloads > Product documentation.
- Exchange Auto Discovery Feature must be configured on the domain. See the *Setting up E12 Autodiscover* document that can be found in the downloaded documentation package.
- As part of Exchange Auto Discovery configuration, a Certificate Authority Server must be configured in the domain. For installation instructions, see http://www.tacteam.net/isaserverorg/vpnkitbeta2/installenterpriseca.htm
- On the Active Directory used to start the MWI service, the user must be configured with Administrator permissions.

Note:

The MWI 2007 software is a third-party software developed by Geomant. Information on Geomant and MWI 2007 is provided in this documentation for ease of reference only. Avaya does not sell, warrant or provide operational support for Geomant's MWI 2007 software product, nor warrant the accuracy of MWI 2007 descriptions contained in this document.

Customers using this document are strongly recommended to obtain the most recent MWI 2007 documentation from Geomant.

The Message Waiting Indicator (MWI) functionality of Microsoft Exchange Unified Messaging is not provided through Exchange Server 2007. Geomant MWI, a third-party vendor application, is an add-on application for use with Exchange 2007 Server, and is used to provide all notifications of new incoming messages to user telephones associated with a voice mail account on the Exchange Server 2007.

Each implemented instance of Geomant MWI is capable of providing message waiting indications for 2500 users, and has a 10 minute built-in timer for user notification timeout purposes.

Installation of Multiple MWI applications

It is possible to install and configure multiple instances of the MWI application on the same network, to accommodate a larger number of users. Users configured on the Exchange Server are distributed between the available instances of the MWI application to provide effective MWI notification.

Note:

Due to a limitation of the Geomant MWI application, a user cannot be configured to receive MWI notifications from more than one MWI application. A document describing the steps for a manual installation of the MWI application software can be found in the documentation package downloaded at http://mwi2007.com . Go to **downloads > documentation package**.

Configure Geomant Message Waiting Indicator (MWI) application

Following the successful installation of the MWI application, you are able to configure the MWI application by means of the Geomant MWI Service Web page.

The Geomant MWI Service Web page can be opened on the local server using the link https://localhost/MWISrvAdmin/.

Note:

The Geomant MWI Service Web page can also be accessed from a different (non-local) system by replacing **localhost** with the IP Address of the server on which the MWI application has been installed.

The Geomant MWI Service Web page appears, as shown in the following figure:

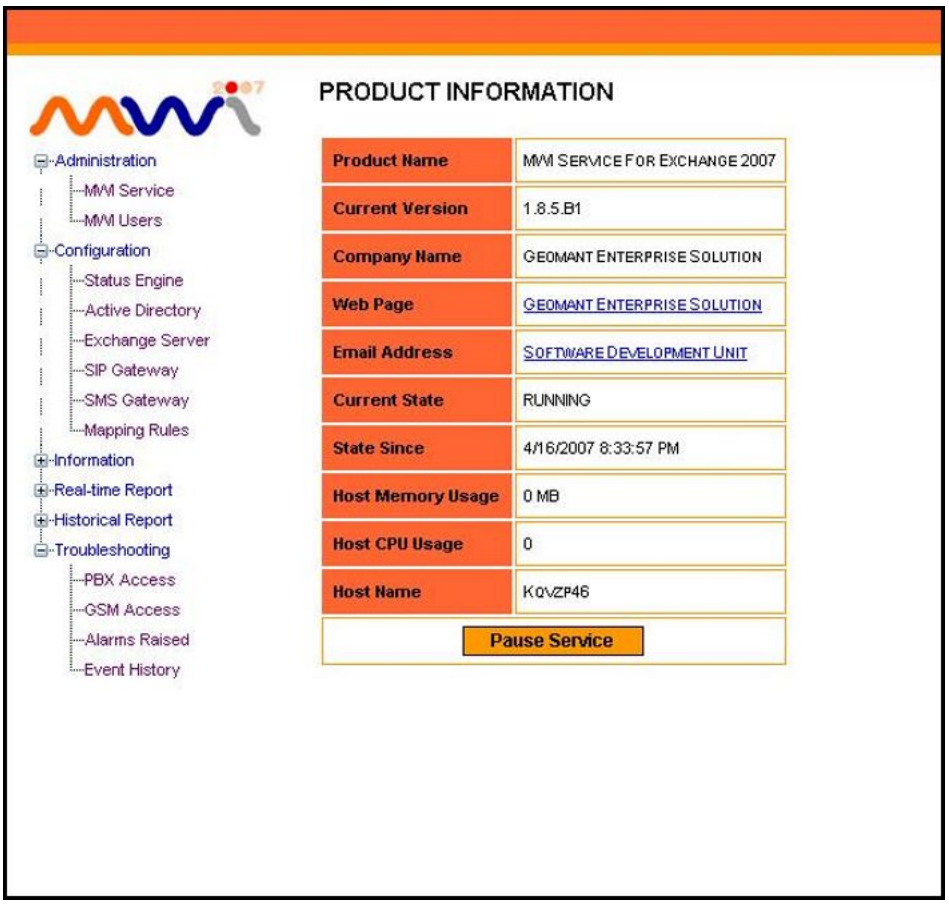


Figure 8: Geomant MWI Service Web page

To configure MWI licenses for each SIP gateway through which MWI notifications will be sent, click the **SIP Gateway** option of the Geomant MWI Service Web page (as shown in the preceding figure). Enter the appropriate values for each SIP gateway to be used.

The SIP Gateway configuration screen appears, as shown by the following:

Display Name	Transport	Gateway Port	MWI Ports	Subscription	Local Port
AREA_TORONTO_IP_GW	TCP	5060	0	☐	5060
AREA_RICHARDSON_IP_GW	TCP	5060	0	☐	5060
AREA_GALWAY_IP_GW	TCP	5060	0	☐	5060

Figure 9: SIP Gateway configuration screen

The installed MWI service can be enabled and configured on a per-user basis with the SIP gateway to which the associated MWI notifications are to be sent. To configure MWI for each user, click the **MWI Users** option on the Geomant MWI Service Web page. This prompts the Unified Messaging User Properties screen to appear, as shown in the following figure.

Figure 10: Unified Messaging User Properties screen

Additional notes on configuring Avaya CS 1000 for MWI

- The SIP DCH should be configured with MWI for the RCAP value (LD 17).
- User telephones should be configured with MWA (Message Waiting Allowed) Class of Service to receive MWI Lamp notification.
- The Node configuration page (in Element Manager) needs to be configured with information for both the **MWI Application DN** and the **MWI Dialing Plan**. The configured MWI DN and MWI Dialing plan should be administered as a valid DN on the Call Server to ensure routing back to the SIP gateway; this is required if the ISDN Facility Response is to be sent back to the SIP gateway. For more information on configuring the MWI DN and MWI Dial Plan, see Configure information for the MWI Application DN on page 48 and Configure the Microsoft Exchange Unified Messaging Dial Plan on page 32.

SRTP configuration using Element Manager

Use the following procedure to configure SRTP negotiation between CS 1000 and Exchange 2007 in Element Manager

Enabling SRTP/TLS for Exchange 2007

1. Navigate to **Element Manager**.
2. Click **Nodes: Server, Media Cards**.
3. Click the node you want to view.
4. Click the **Microsoft Unified Messaging** tab.
5. Select the **Enable Secure Media** check box.
6. Click **Save and Transfer**.

Configure Microsoft Exchange Unified Messaging in CS 1000 Element Manager

The following sections detail the use of Element Manager in configuring Microsoft Exchange Unified Messaging services on the CS 1000.

The Edit page of the Element Manager Nodes: Servers, Media Cards configuration page has a new configuration tab – Microsoft Unified Messaging. The Microsoft Unified Messaging tab is used to add Microsoft Exchange Unified Messaging numbers that have been defined for use with Subscriber Access and Auto Attendant and also to configure MWI DNs and Dialing Plans.

Up to five Subscriber numbers and five Auto Attendant numbers can be configured. These numbers can be added, modified or deleted using the functions of the Microsoft Unified Messaging tab.

Configure a Node in Element Manager for use with Microsoft Exchange Unified Messaging

Access to all parameters for configuration of a node for interaction with Microsoft Exchange Unified Messaging are found under IP Telephony Node section of Edit page for Nodes: Servers, Media Cards, as shown in the following figure:

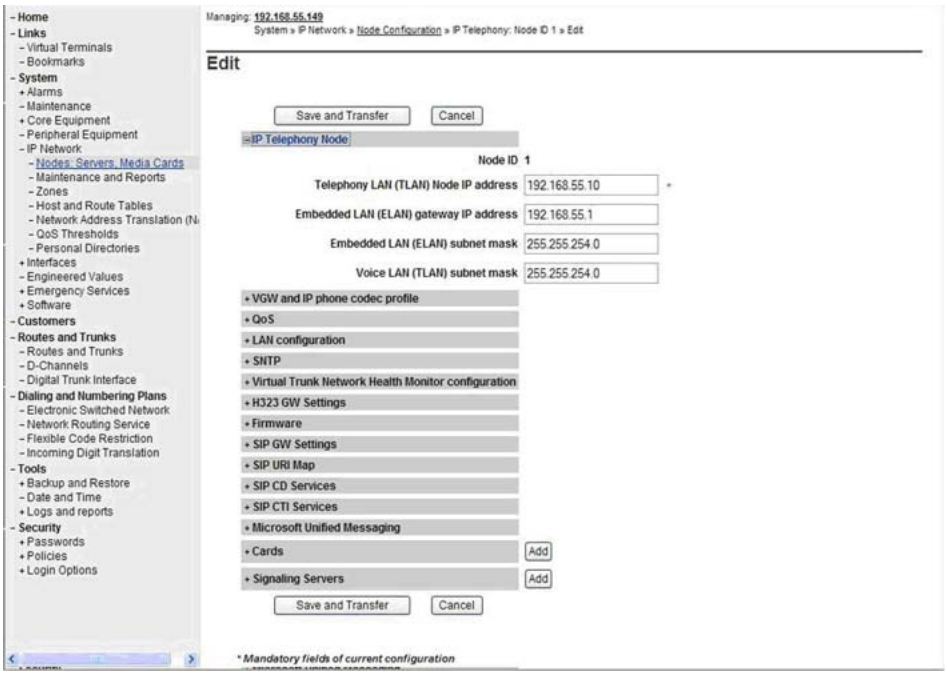


Figure 11: Configuring a Node for use with Microsoft Exchange Unified Messaging: IP Telephony Node

A Node can be imported and its parameters edited to interact specifically with Microsoft Exchange Unified Messaging.

Import and edit a Node for Microsoft Exchange Unified Messaging interaction

1. Log on to Element Manager with a valid User Account.
2. Navigate to the **Nodes: Servers, Media Cards** page.

3. Launch the **Import Node Files** page and import the node to be configured for use with Microsoft Exchange Unified Messaging and edit the imported node by navigating to the **Edit** page of that node.
4. Configure the Unified Messaging parameters for the node by expanding the **Microsoft Unified Messaging** section and saving the changes. For more information, see Configure Subscriber Access, Auto Attendant, and MWI DN information on page 45.

Configure Subscriber Access, Auto Attendant, and MWI DN information

Opening the Microsoft Unified Messaging tab of the Edit page for Nodes: Servers, Media Cards allows the Subscriber Access, Auto Attendant, and MWI DN information to be configured. These configuration parameters, once expanded, appear as shown in the following image:

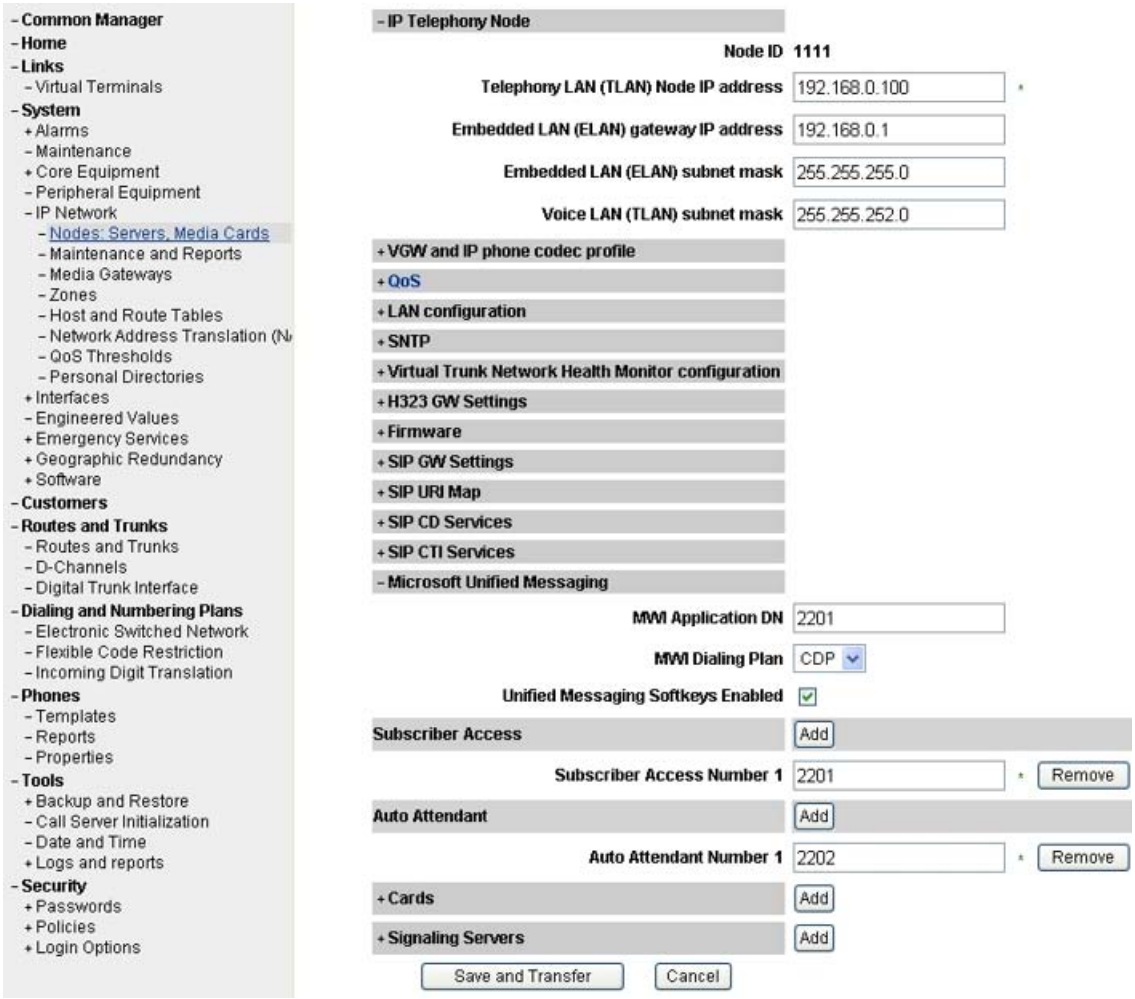


Figure 12: Subscriber Access, Auto Attendant, MWI DN and Voice mail softkeys configuration parameters

The acceptable data entries for the Subscriber Access, Auto Attendant, and MWI DN information fields are as follows:

- Subscriber Access Number: This is a numeric field for up to 32 digits.
- Auto Attendant Number: This is a numeric field for up to 32 digits.
- MWI Application DN: This is a numeric field for up to 32 digits.

Adding, modifying, or deleting Subscriber Access Numbers for a Microsoft Exchange Unified Messaging Node

The following procedures detail the steps to add, modify, or delete the Subscriber Access Number information for a Node interacting with Microsoft Exchange Unified Messaging.

Add new Subscriber Access Number information

1. Log on to Element Manager with a valid User Account.
2. Navigate to the **Edit** page of the **Nodes: Servers, Media Cards** configuration page.
3. Expand the **Microsoft Unified Messaging**.
4. In the space provided, add information for up to five Subscriber Access Numbers by clicking **Add** and saving the configuration. The **Add** button becomes inactive after the fifth entry.

Modify Subscriber Access Number information

1. Log on to Element Manager with a valid User Account.
2. Navigate to the **Edit** page of the **Nodes: Servers, Media Cards** configuration page.
3. Expand the **Microsoft Unified Messaging**.
4. In the space provided, modify the configuration information as required for up to five Subscriber Access Numbers and save the configuration.

Delete Subscriber Access Numbers

1. Log on to Element Manager with a valid User Account.
2. Navigate to the **Edit** page of the **Nodes: Servers, Media Cards** configuration page.
3. Expand the **Microsoft Unified Messaging**.
4. Delete the required Subscriber Access Number(s) by clicking the **Remove** button and saving the configuration.

Adding, modifying, or deleting Auto Attendant numbers for a Microsoft Exchange Unified Messaging Node

The following procedures detail the steps to add, modify, or delete the Auto Attendant Number information for a Node interacting with Microsoft Exchange Unified Messaging.

Add new Auto Attendant number information

1. Log on to Element Manager with a valid User Account.
2. Navigate to the **Edit** page of the **Nodes: Servers, Media Cards** configuration page.

3. Expand **Microsoft Unified Messaging**.
4. In the space provided, add information for up to five Auto Attendant Numbers by clicking **Add** and save the configuration. The **Add** button becomes inactive after the fifth entry.

Modify Auto Attendant Number information

1. Log on to Element Manager with a valid User Account.
2. Navigate to the **Edit** page of the **Nodes: Servers, Media Cards** configuration page.
3. Expand **Microsoft Unified Messaging**.
4. In the space provided, modify the configuration information as required for up to five Auto Attendant Numbers and save the configuration.

Delete Auto Attendant Numbers

1. Log on to Element Manager with a valid User Account.
2. Navigate to the **Edit** page of the **Nodes: Servers, Media Cards** configuration page.
3. Expand **Microsoft Unified Messaging**.
4. Delete the required Auto Attendant Number(s) by clicking the **Remove** button and saving the configuration.

Configure information for the MWI Application DN

The following procedure details the steps to configure the MWI Application DN information for a Node interacting with Microsoft Exchange Unified Messaging.

Configure MWI Application DN information

1. Log on to Element Manager with a valid User Account.
2. Navigate to the **Edit** page of the **Nodes: Servers, Media Cards** configuration page.
3. Expand **Microsoft Unified Messaging**.
4. Configure the proxy DN for the MWI application and save the configuration.

Select MWI Dial Plan type

The following procedure details the steps for selecting the desired MWI Dial Plan type for a Node interacting with Microsoft Exchange Unified Messaging.

Note:
Currently, the available dial plan types are restricted to CDP and UDP only.

Select the desired MWI Dial Plan type

1. Log on to Element Manager with a valid User Account.
2. Navigate to the **Edit** page of the **Nodes: Servers, Media Cards** configuration page.
3. Expand the **Microsoft Unified Messaging**.
4. Select either **CDP** or **UDP** for the MWI Dial Plan type and save the configuration.

Voice mail softkeys configuration

The use of Exchange UM softkeys on IP phones (11XX, 12XX, 2007, 2004, 2002) is enabled through Element Manager by selecting the Unified Messaging Softkeys Enabled checkbox under Microsoft Unified Messaging. In addition, the Inbox key of each of the phones can be configured to access the Subscriber Access DN and MWK directly.

The key mapping for the softkeys is static and consists of the following options:

- Play
- Delete
- Call
- Stop
- Unread
- Reply
- Compose
- Forward
- Info

Allowing calling party numbers to update while leaving message

If a call is modified after reaching the Exchange 2007 UM Server, the calling party number is modified as well. To ensure that voice messages left will have the correct calling party information, calling party number information must be updated to the Exchange 2007 UM Server by generating a SIP INFO message with new content type header text/source-party.

This SIP INFO message is then delivered to the Exchange 2007 UM Server, allowing any voice messages left there to reflect the correct calling party caller information.

To enable this functionality of the SIP INFO message, the following changes must be made on the Exchange 2007 UM Server:

- In the GlobCfg.XML file, set the SourcePartyInfoEnabled flag to true.
- Both the Microsoft Exchange Speech Engine and the Microsoft Unified Messaging Services must be restarted.

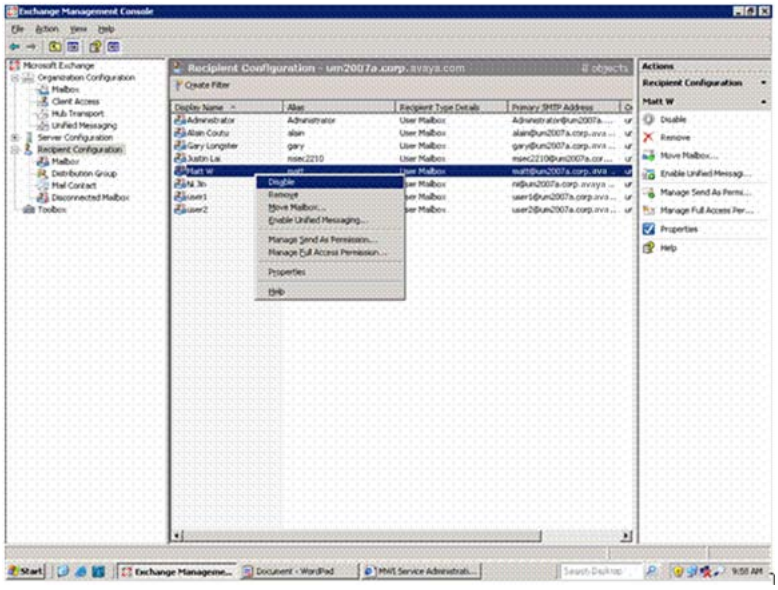
Note:
The CS 1000 FAX user set must be configured with MPTD class of service in LD 11.

Disable a user mailbox

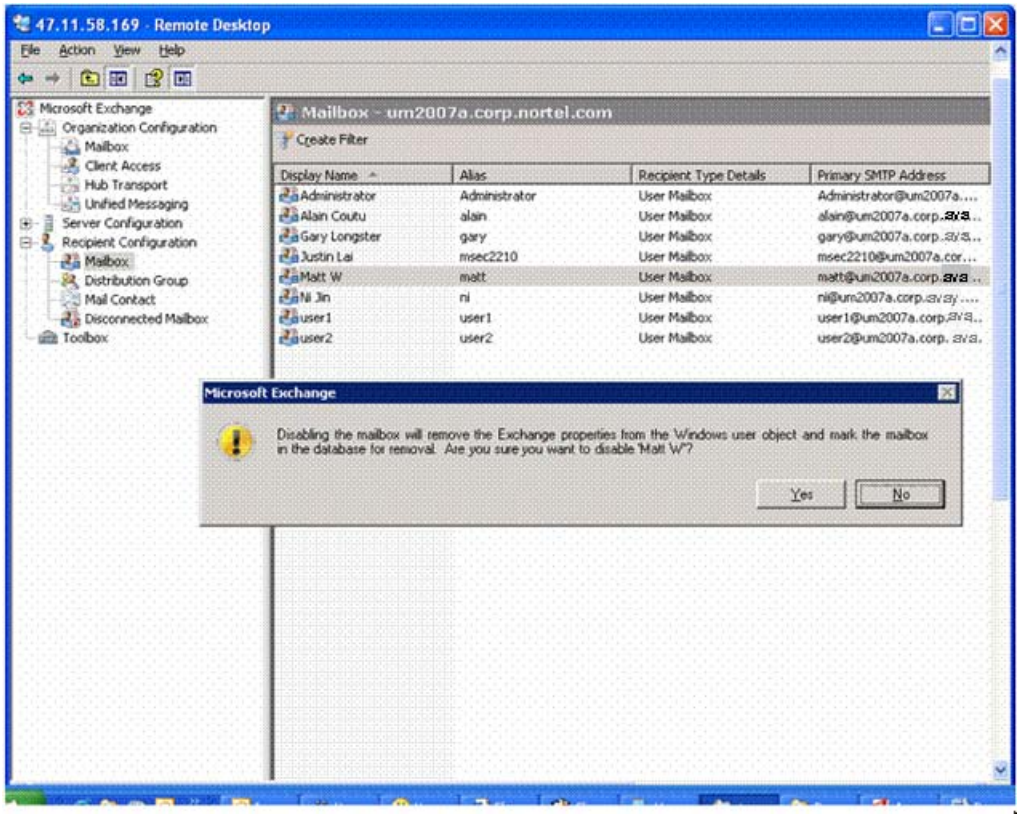
The following section details the required steps for removing all Exchange mailbox attributes from a user object in Active Directory without deleting the user object in Active Directory.

Disabling a user mailbox

1. In the Exchange Management Console, select **Recipient Configuration > Mailbox** . In the action pane, click **Disable** to disable the mailbox. Optionally, you can right-click the selected mailbox, and choose **Disable** on the pop up menu as shown in the following figure:



2. Click **Yes** to confirm the disabling of the user mailbox, as shown in the following figure:



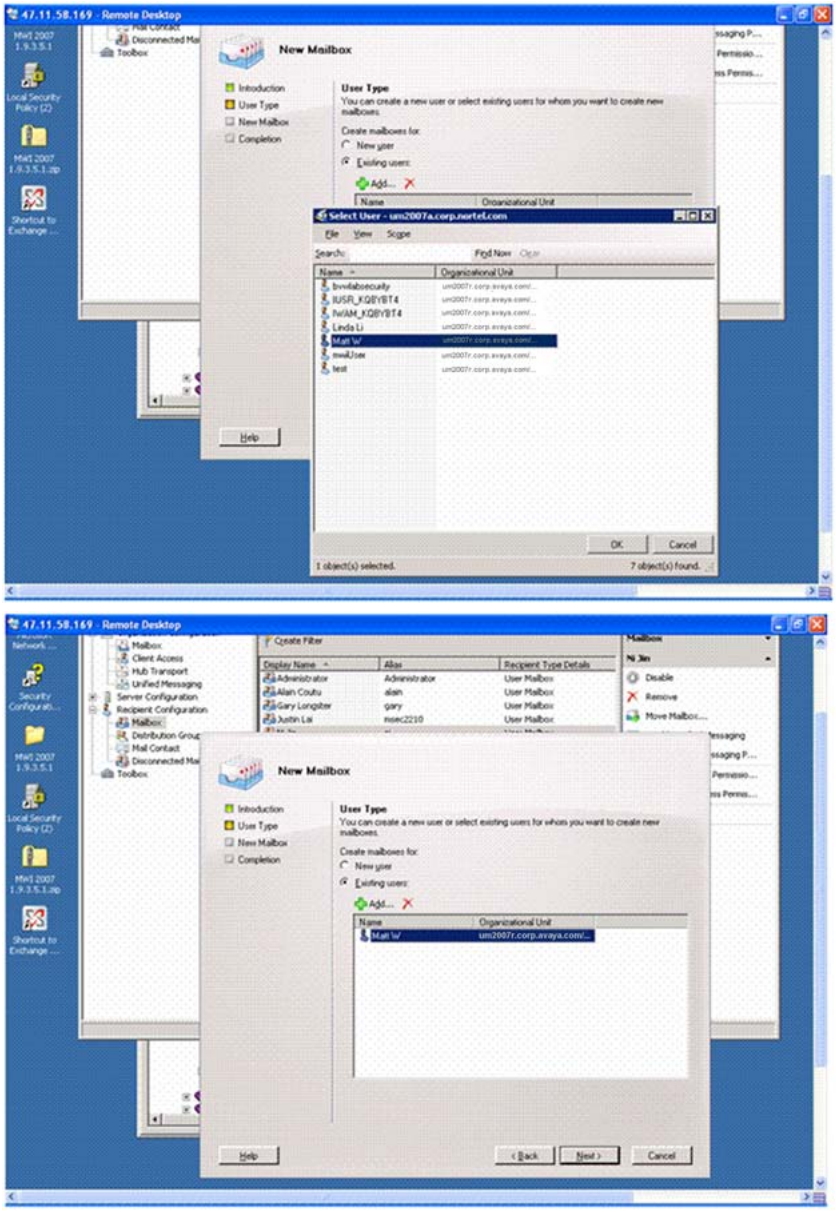
Enable the user mailbox after disabling

The user mailbox can be enabled after disabling it. The following section details the required steps to enable a disabled user mailbox.

Enabling the user mailbox after disabling

1. Add a new mailbox using the **New Mailbox Wizard**, but select **Existing users** instead of **New users** when prompted for **User Type**.

   For more information about using the New Mailbox Wizard, see Configure a new user mailbox for Microsoft Exchange Unified Messaging on page 23.
2. Click **Add**. A window appears displaying all existing users in the active directory.
3. Select the disabled user mailbox as appropriate and click **OK**, as shown by the following:



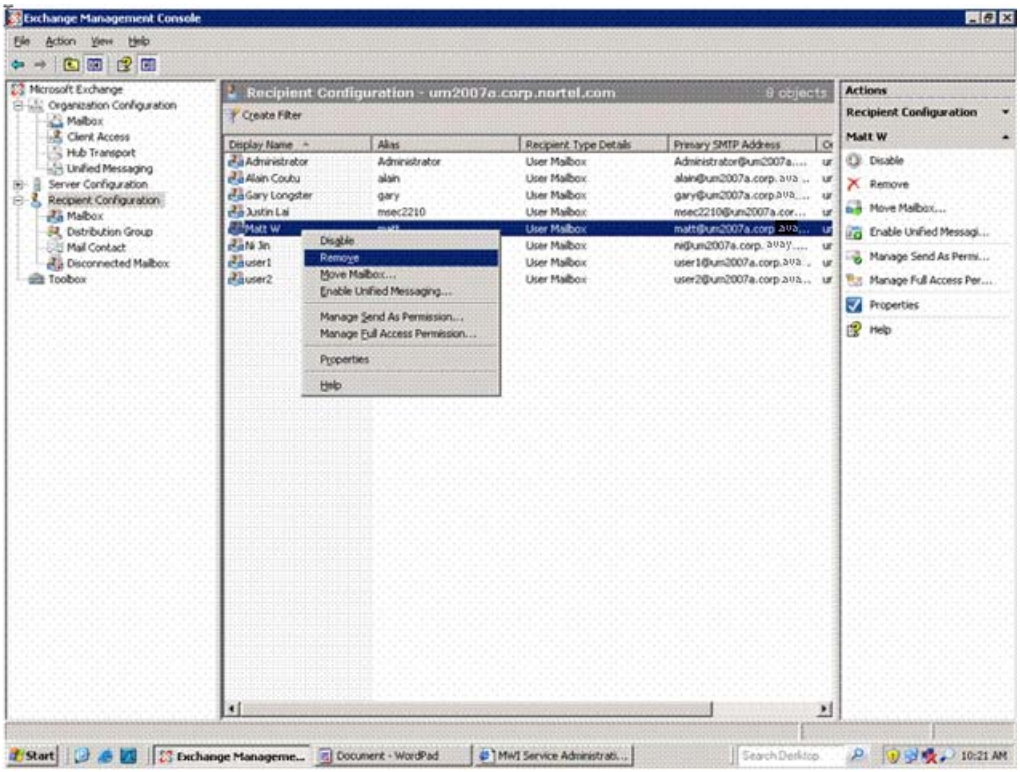
4. Click **Next** and follow the steps to add a new mailbox, without changing current user account information.

Remove a user mailbox

This procedure details the required steps for removing a user mailbox.

Removing a user mailbox

1. In the Exchange Management Console, select **Recipient Configuration** > **Mailbox** .
2. In the action pane, click **Remove** to remove the mailbox, as shown by the following:



Optionally, you can right-click the selected user mailbox, and choose **Remove** from the list of menu options.

Note:

When you remove a user mailbox, all associated user Exchange data is marked for deletion and the associated user account entry in the Active Directory is deleted.

Remove a dial plan

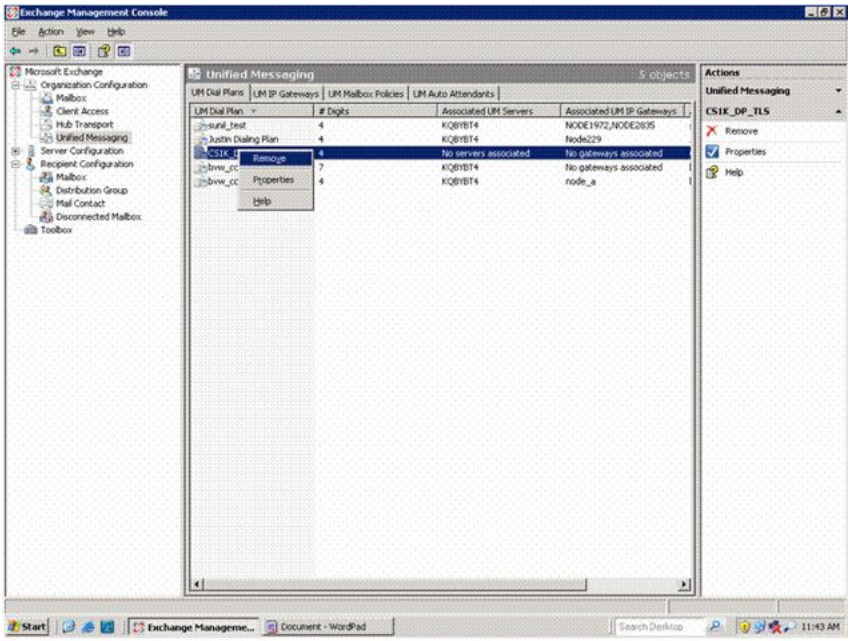
This procedure details the required steps for removing a UM dial plan.

Note:

Before you can remove a UM dial plan, you must remove any existing associations with other UM components such as UM mailbox policies, Unified Messaging servers, or UM IP gateways.

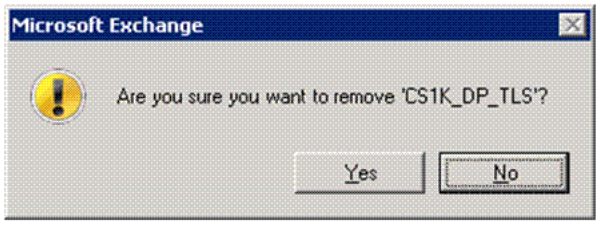
Removing a dial plan

1. In the Exchange Management Console, select **Organization Configuration>Unified Messaging**
2. Select the appropriate UM dial plan and click **Remove** on the action pane to remove the dial plan, as shown by the following:



Optionally, you can right-click the UM dial plan and select **Remove** from the list of available options.

3. Click **Yes** to confirm the removal of the selected UM dial plan.



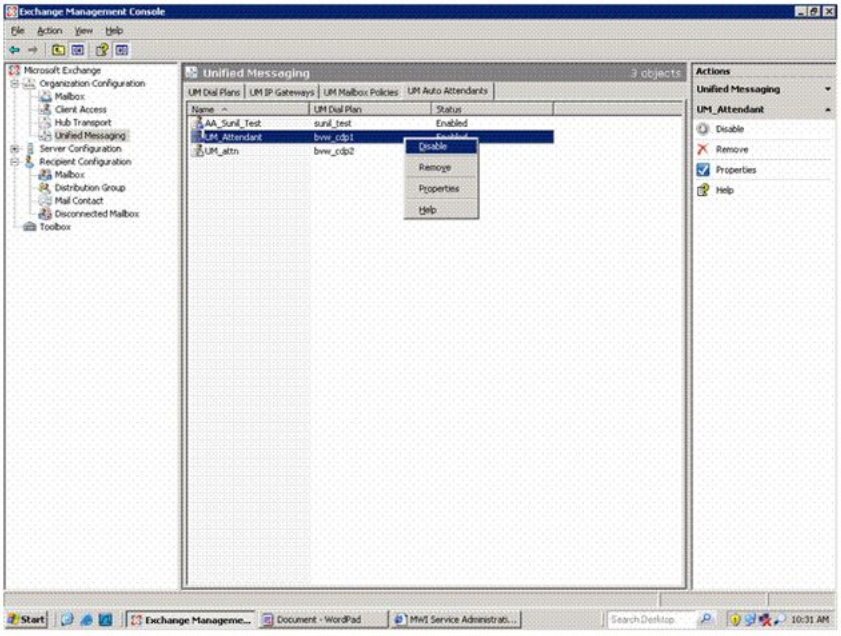
Disable Operator Assistance feature

This module details the required steps for disabling Operator Assistance feature functionality, provided by the UM Auto Attendant.

The UM Auto Attendant can be disabled: if an auto attendant is disabled, no incoming calls will be answered.

Disabling the UM Auto Attendant

1. In the Exchange Management Console, select **Organization Configuration > Unified Messaging** .
2. Select the appropriate UM Auto Attendant and click **Disable** on the action pane to remove the dial plan, as shown by the following:



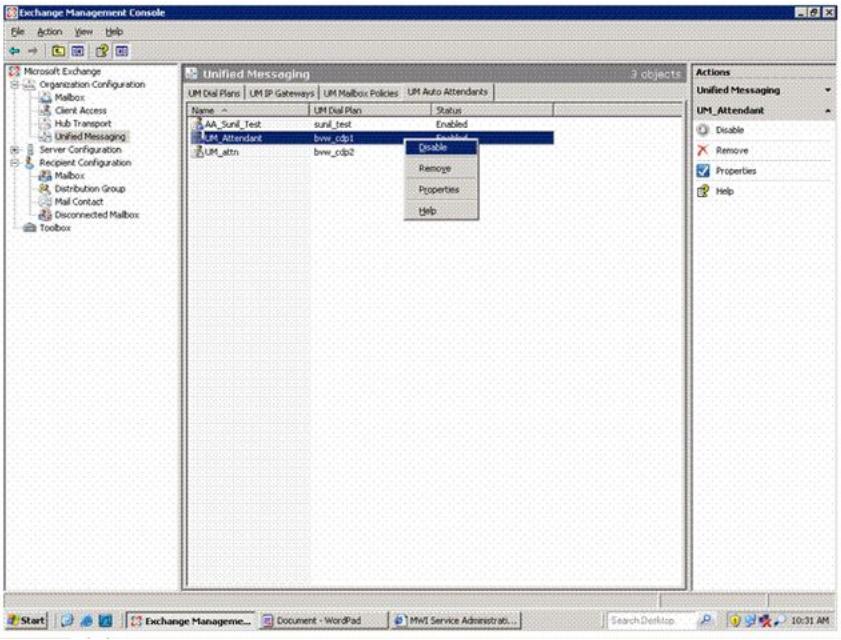
Optionally, you can right-click the UM Auto Attendant and select **Disable** from the list of available options.

Remove Operator Assistance feature

This module details the required steps to follow for removing a configured UM Auto Attendant.

Removing the UM Auto Attendant

1. In the Exchange Management Console, select **Organization Configuration > Unified Messaging** .
2. Select the appropriate UM Auto Attendant and click **Remove** on the action pane to remove the dial plan, as shown by the following:



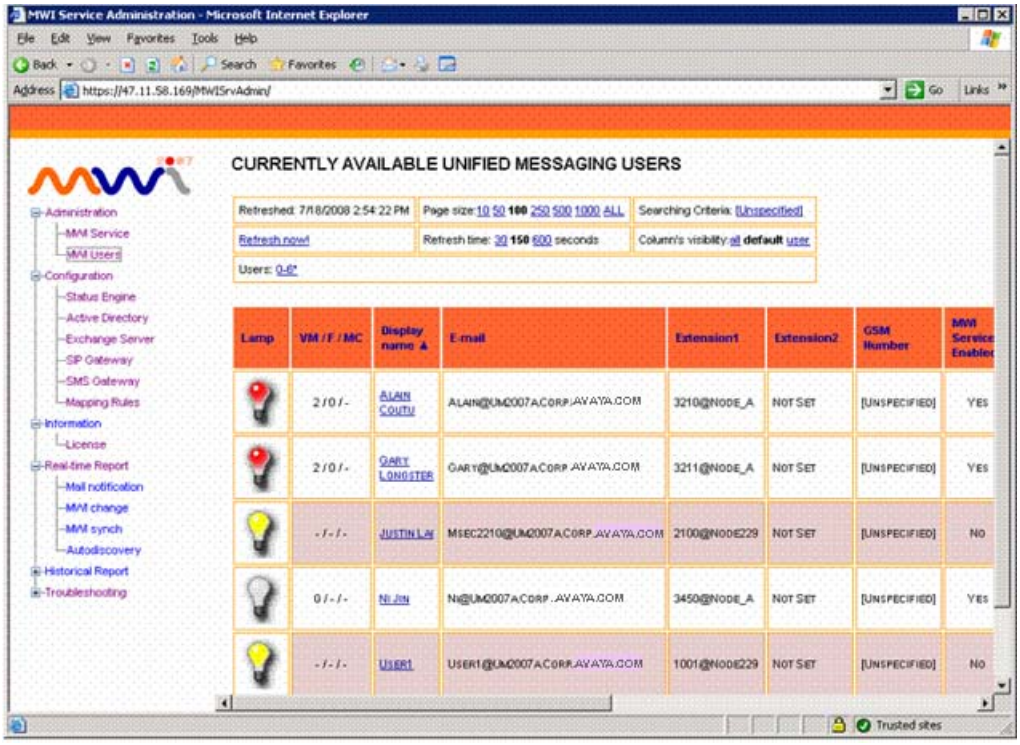
Optionally, you can right-click the UM Auto Attendant and select **Remove** from the list of available options.

Disable MWI service for a user phone set

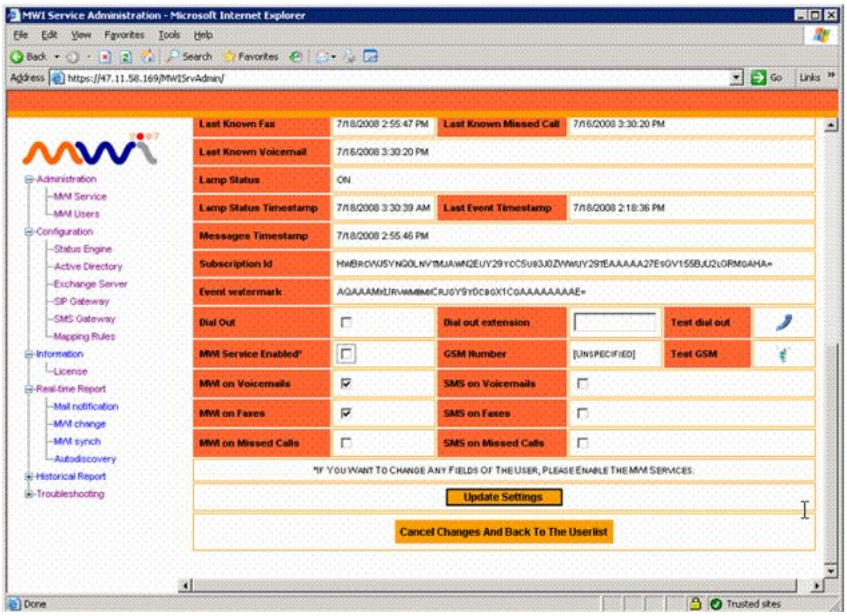
This module details the procedure for disabling MWI service access on a user phone set.

Disabling MWI service for a user phone set

1. Access the Geomant MWI Service Web page. For more information about accessing the Geomant MWI Service Web page, see Configure Geomant Message Waiting Indicator (MWI) application on page 40
2. Select **Administration > MWI Users** .



3. Select a user from the list. The Unified Messaging User Properties page appears.



4. On the Unified Messaging User Properties screen, uncheck **MWI Service Enabled** to disable MWI service for the user.

End user experience scenarios

This section describes the end user scenarios for Unified Messaging features.

Navigation

Answering the call

This is an end user scenario for answering the call on behalf of a user.

1. User A calls User B, who is a subscriber to UM services.
2. The call is redirected to UM, if the User B does not answer or his phone is busy.

   Important:
   The caller hears the default greeting or personal greeting (if recorded).
3. The caller can leave a voicemail for User B after the beep tone.
4. After the message is recorded, the caller has to press the pound (#) key for more options or wait to send the recorded message to User B mailbox.

Subscriber Access

This sections describes the end user scenario for subscriber dialing into the Microsoft Exchange Unified Messaging.

1. Call the UM Subscriber Access number.

The caller receives the greeting prompting to enter the pin number.

2. Press the star (*) key, if the mailbox does not belong to the caller. Enter the pin number to open the mailbox.
3. The caller has various options to select from voicemail, email and so on after opening the mailbox.

Important:
Both voice commands and DTMF options are available

Auto Attendant

The auto attendant service allows call transfer to any number or persion in the corporate directory. This section describes the end user scenario for auto attendant service into the Microsoft Exchange Unified Messaging.

1. Call the UM Auto Attendant number.
2. The caller receives the greeting prompting to enter the name of the person or press the pound key (#) two times.

   Enter the email or press the pound key if you know the extension.

   Important:
   If the auto attendant is speech enabled, then the UM will prompt for the name of the person.
3. After the user name, number, and email is entered the auto attendant prompts the callers to press the pound key. You can leave a message to the user or wait to contact the user.

Message waiting indication

This section describes the end user scenario fir the message waiting indication in the Microsoft Exchange Unified Messaging.

1. User A calls User B.

   Important:
   User B must have the mailbox configured in Exchange UM.
2. If User B does not answer the call, then the call is redirected to UM to record the voice message.

3. User A leaves a voice mail for user B.
4. The MWI indicator on User B is illuminated. This indicates that there is a message waiting for User B in the mailbox.

Important:

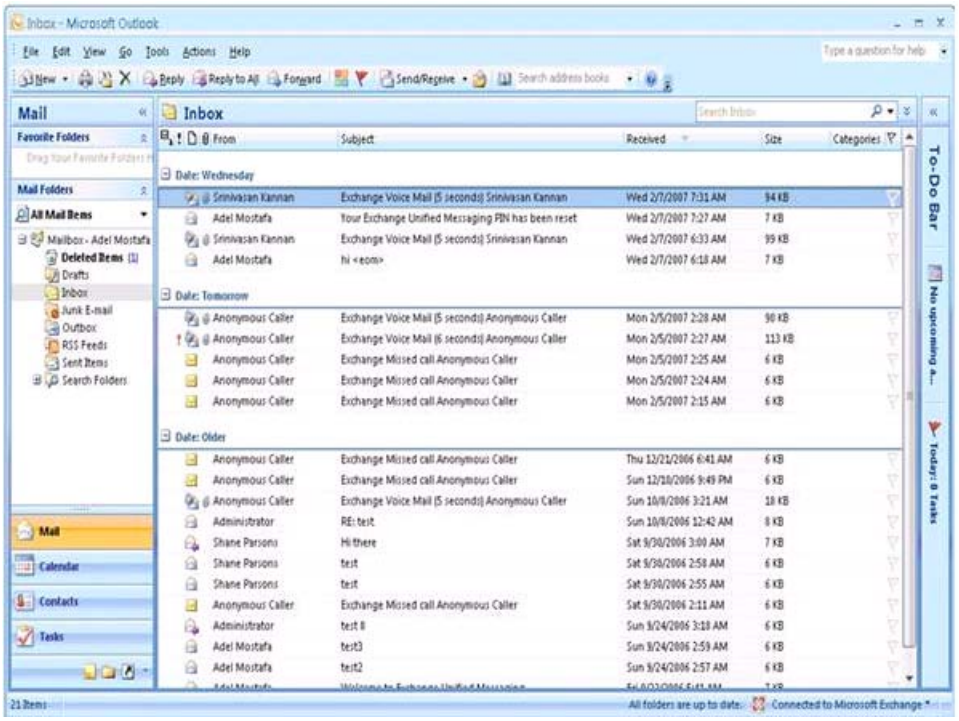
The message waiting features assumes that there are no voice mail in the mailbox if the User B indicator is not illuminated.

Play on phone features

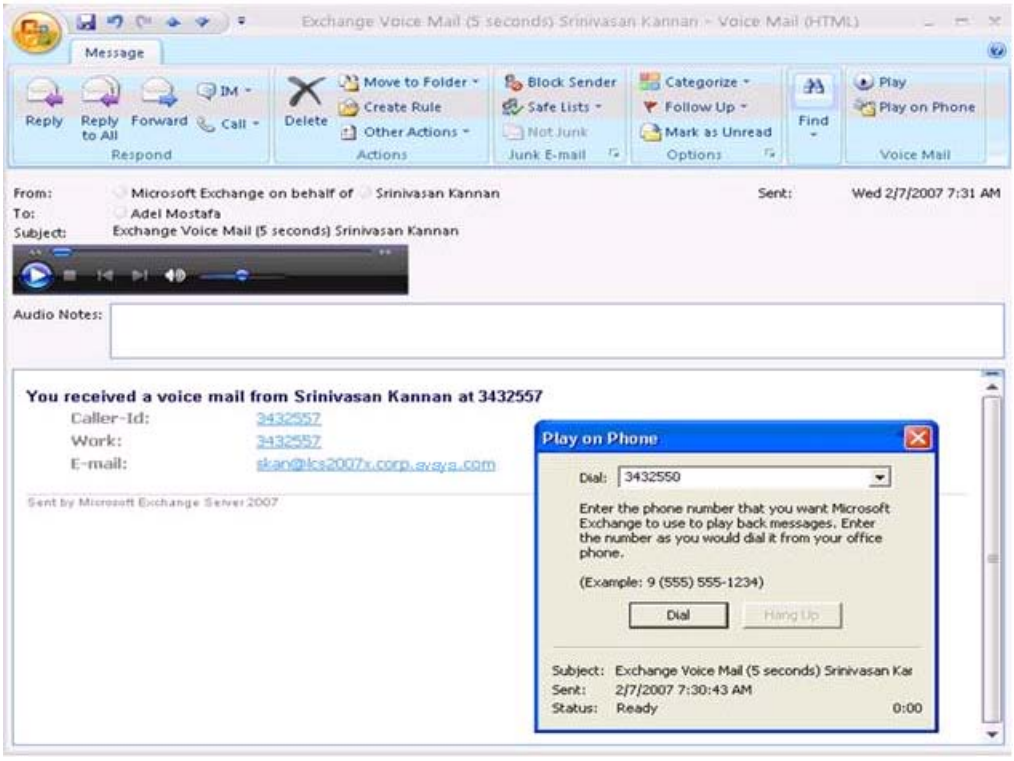
This section describes the end user scenario for the play on phone feature in the Microsoft Exchange Unified Messaging.

Users can invoke play on phone feature to call a phone and hear the voicemail.

1. Select voicemail in the Outlook or use Outlook web access (OWA) default feature provided by Exchange UM.



2. Play the message on the system or over the phone by using play on phone option.
3. To play using the play on phone, select the option available with the voice mail.
4. Enter the phone number where the message needs to be played.
5. Press dial.



6. The destination phone number can also be set using the option tab so that it need not be entered again the next time a message is played.

RE-INVITE issue with Exchange 2007

- Exchange 2007 do not support RE-INVITE with a modified codec list or a reordered codec list.
- Only G711 and G723 codecs are supported, with preference given to G711 as this will ensure that any RE-INVITE with a modified codec is handled by the RE-INVITE workaround solution provided below.

RE-INVITE work-around

There are many applications and features in CS 1000 which trigger RE-INVITE to UM. The codec offered can be a subset of the initial offered codec or it can be a new set of codecs based on the feature.

Any modification to the media stream should be offered using RE-INVITE for an established session and the update method for a future session.

Exchange has a major limitation with respect to codec re-negotiation using RE-INVITES. UM does not accept RE-INVITES with a modified or re-ordered codec list.

The work-around is as follows:

- If the initial INVITE to UM features the G711 codec (and RFC 2833 is supported) then solution Modified the INITIAL SDP to UM with only G711 and RFC 2833 DTMF payload as the offered codec list to UM, with order of law (A Law / Mu Law for G711) maintained as offered from the far end (in case of tandem call scenario) /near-end.
- If the offered SDP does not have G711 and/or RFC 2833 Payload then the offered SDP is sent as is and the RE-INVITE solution does not modify the call scenario, leaving Exchange to handle the call for all subsequent RE-INVITE.
- If the SDP offered in the initial Invite is modified using the RE-INVITE solution, the solution will trigger every time there is a RE-INVITE to UM. It will attempt to modify the offered codec list in the same order, using the same list as long as negotiated voice codes are available in the RE-INVITE. If the negotiated codec is not present in RE-INVITE then the SDP is forwarded as is UM must handle the call
- RE-INVITE solution will not trigger if the RE-INVITE has a pTime (SDP attribute) value greater than the pTime (SDP attribute) value in Initial Invite.
- If a Video SDP is received in the offered coded list, it will not be sent to Exchange as part of RE-INVITE solution.

Note:

This is only if the RE-INVITE solution is triggered based on the conditions described above, in which case the offer SDP to UM will not contain the Video codecs. Port 0 is then added by CS 1000 to ensure that the video offer is rejected. Only audio is accepted as part of UM calls.

- For SRTP calls the RE-INVITE solution will trigger based on the criterion suggested above.
- For audio. if one mline offer stands for RTP, and a second one for SRTP, with CS 1000 in tandem node, then the RE-INVITE solution will ensure that there is only one mline sent to Exchange with SRTP attributes added in the terminal capability audio attribute “a=tcap”. The answer generated will still have multiple mline with port 0 for the audio capability, which is not accepted by Exchange.

Note:

- SRTP is supported with limitations on RE-INVITE work-around.
- The CS 1000 gateway and Exchange UM 2007 should be configured with same Law (A-Law or Mu-Law).

Secured Dial Plan Creation

There are 3 types of VOIP security provided by Exchange UM:

- Unsecured (default)
- SIP secured
- Secured

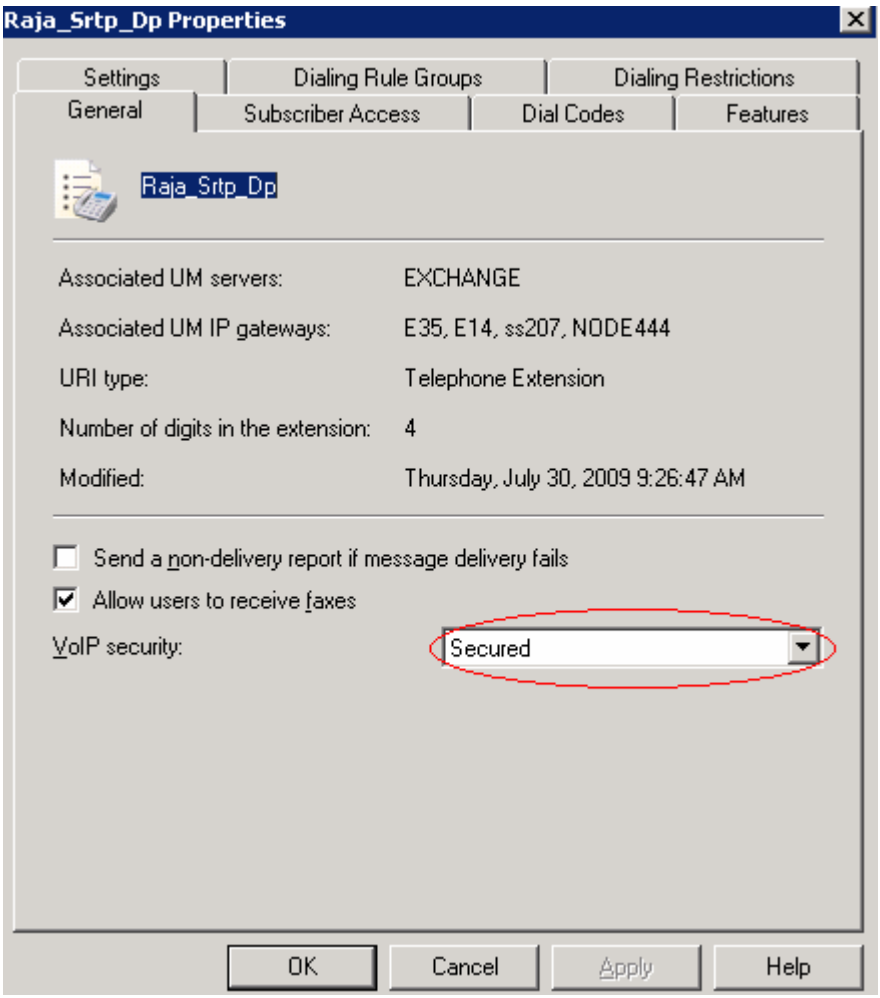


Figure 13: Secured

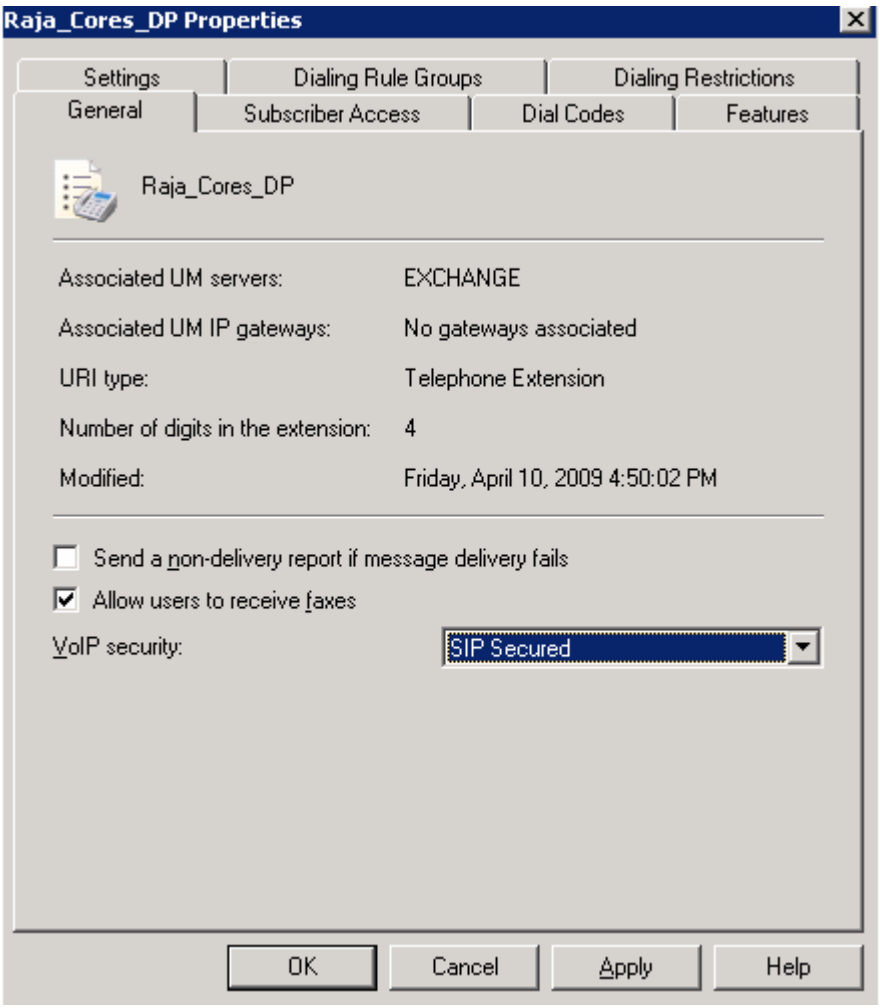
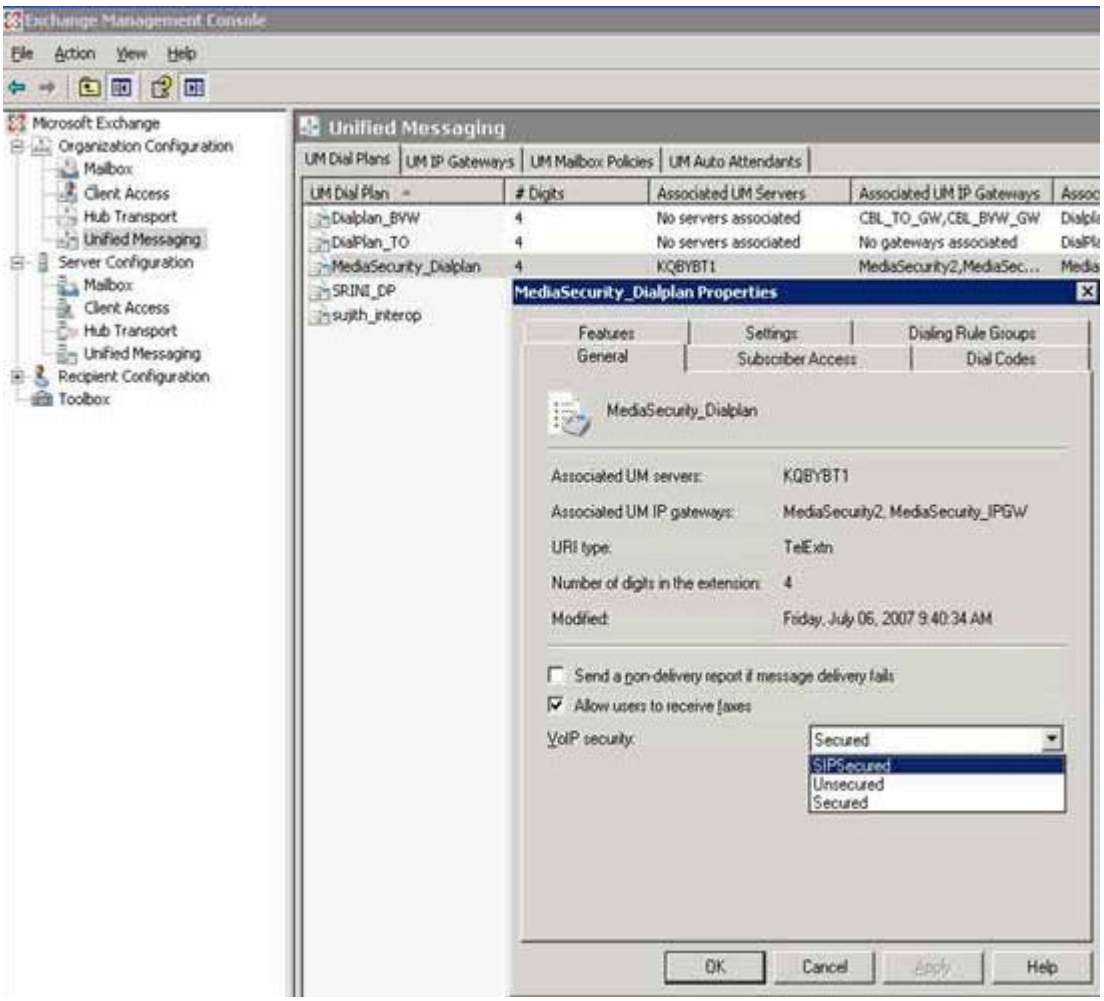


Figure 14: SIP Secured

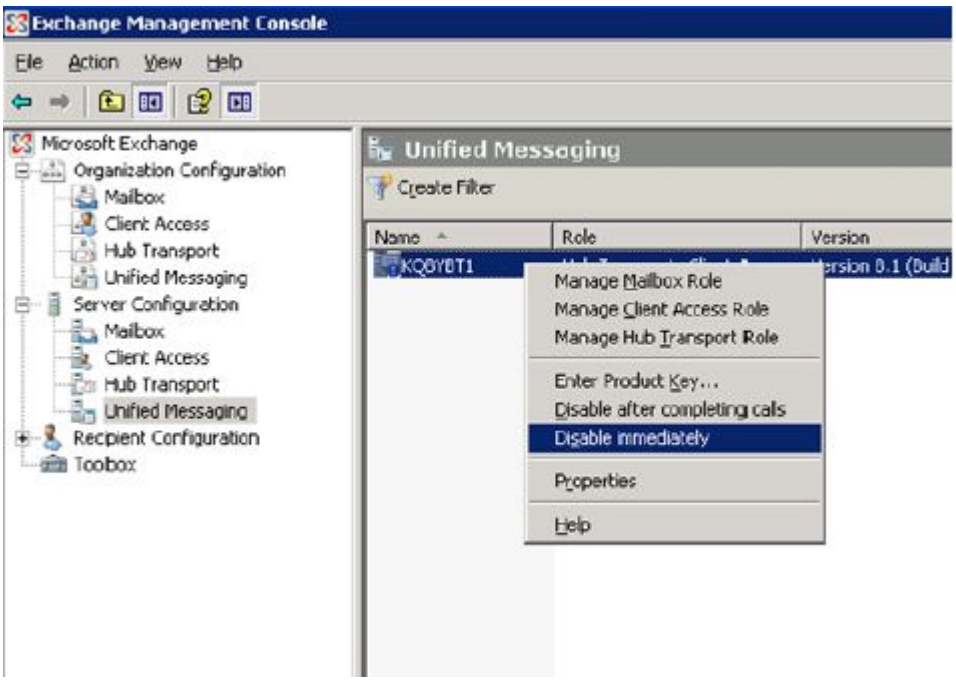
Configuring TLS on UMS 2007 SP1

Configure TLS on the Unified Message Service (UMS) 2007 SP1.

1. Set up the UM Dial Plan to SIPSecured.

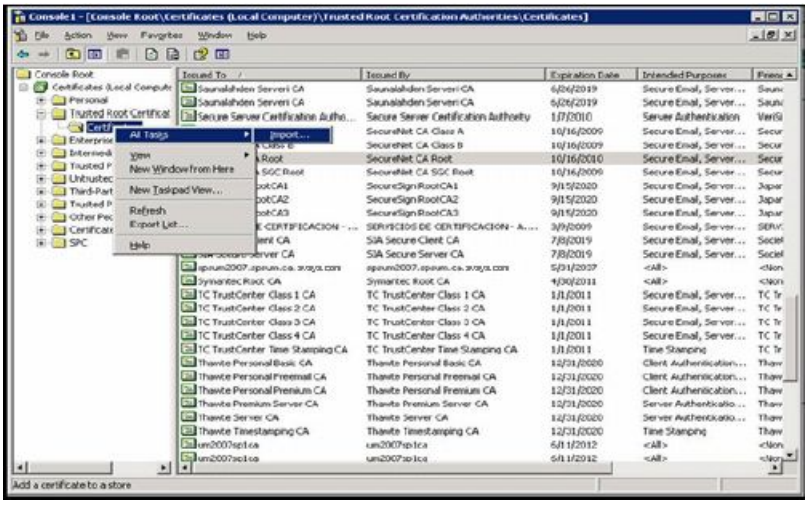


2. Restart the Unified Messaging Service.



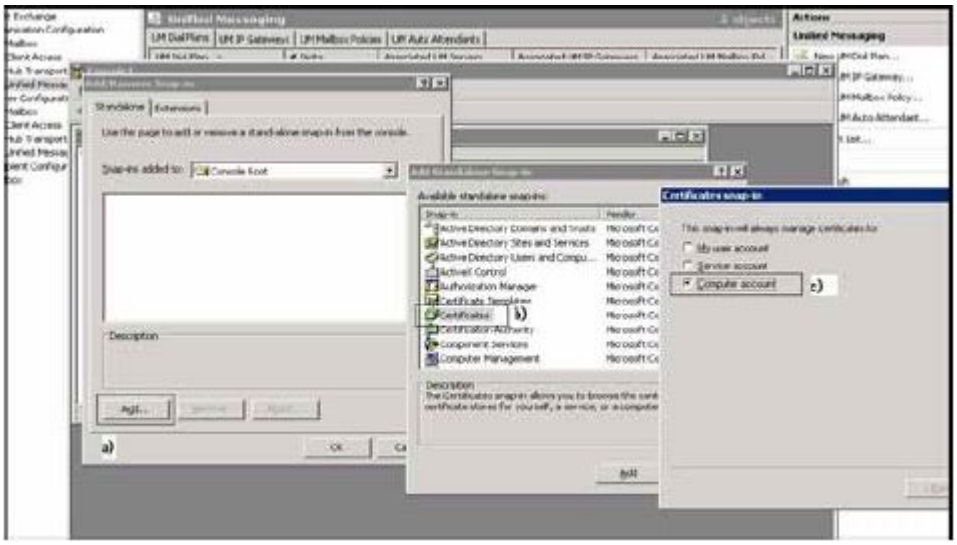
3. Generate a certificate signed by a private local Certificate Authority (CA) on the SPS with the FQDN of your Signaling Server as the subject.

4. Copy the Private Certificate Authority Certificate into a text file with .cer extension.

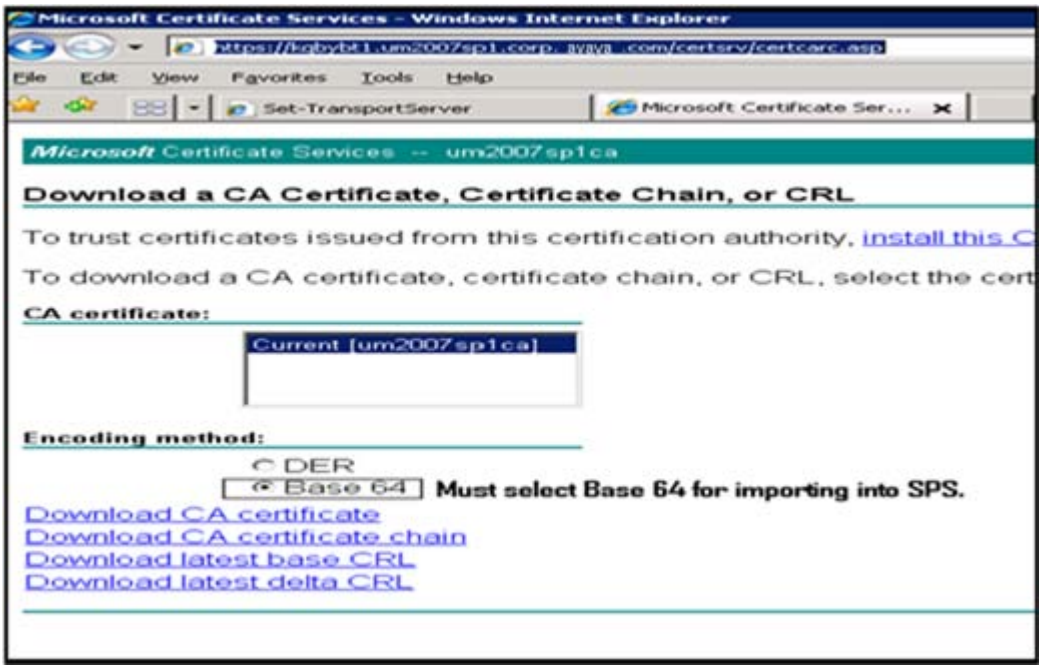


5. Go to the **Start** menu, and type **run > mmc**.
6. Add (Certificate) snap-in.

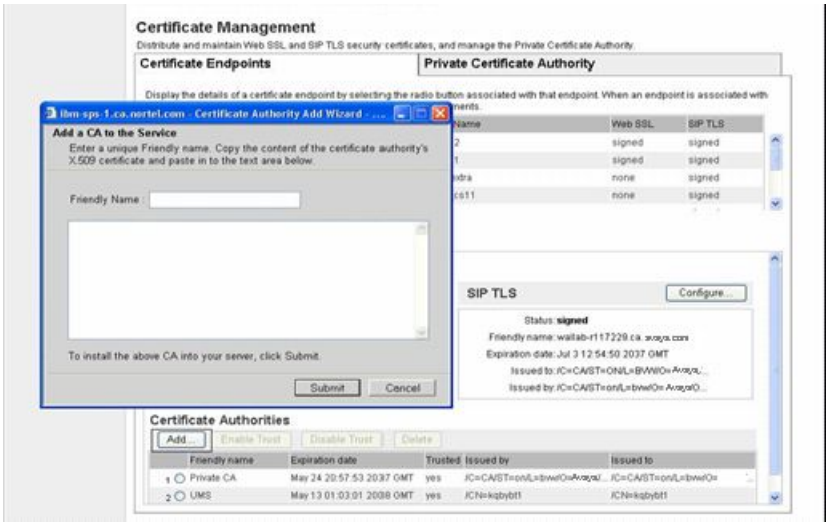
7. Select **Computer Account** certificate store to import the PCA Certificate to the UMS2007 server.



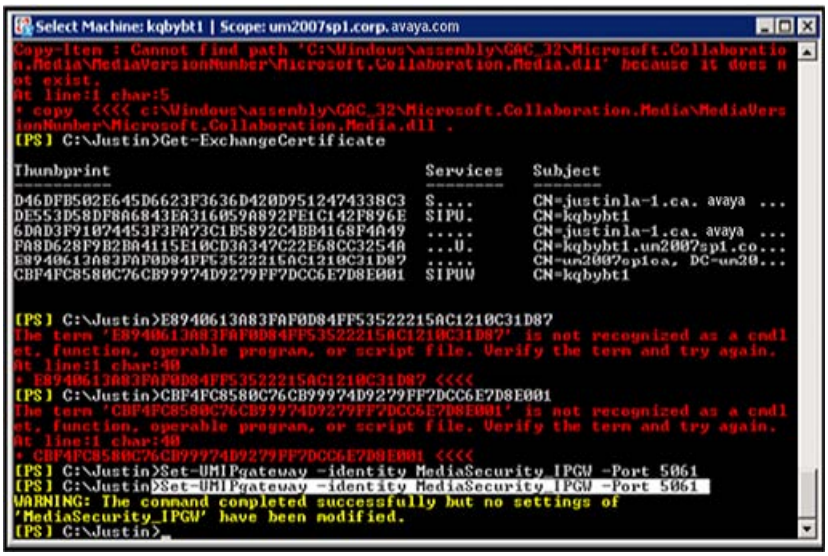
8. Export the Microsoft Certificate Authority certificate from the following Web site: https://<UMS FQDN>/certsrv/certcarc.asp.



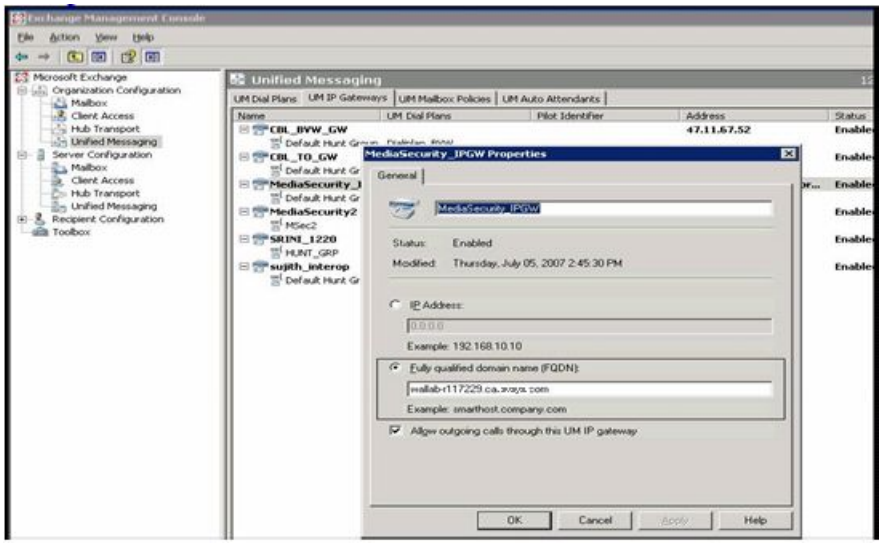
9. Open the Microsoft CA certificate in a text editor and copy the content into SPS Certificate Authorities->Add pop-up window.



10. On the UMS command console: **Set-UMIPgateway -identity <IP_GATEWAY> -Port 5061**.



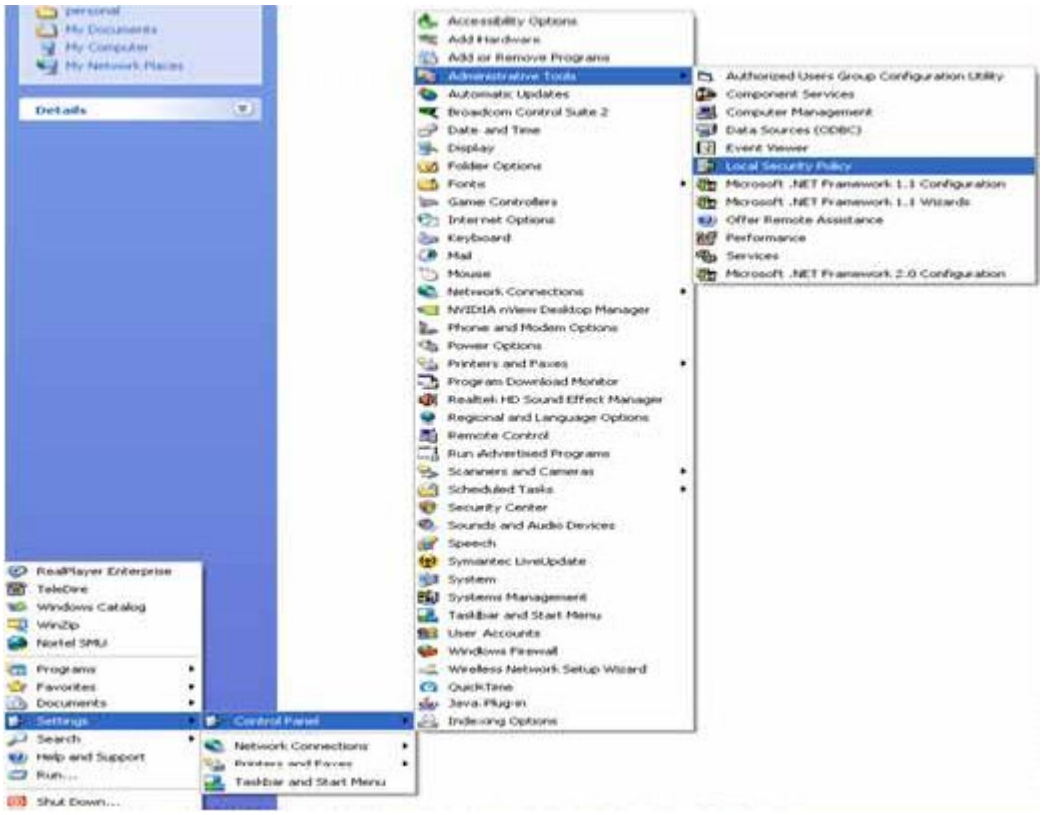
Make sure your IP_GATEWAY is identified by its FQDN in the Exchange Management Console.



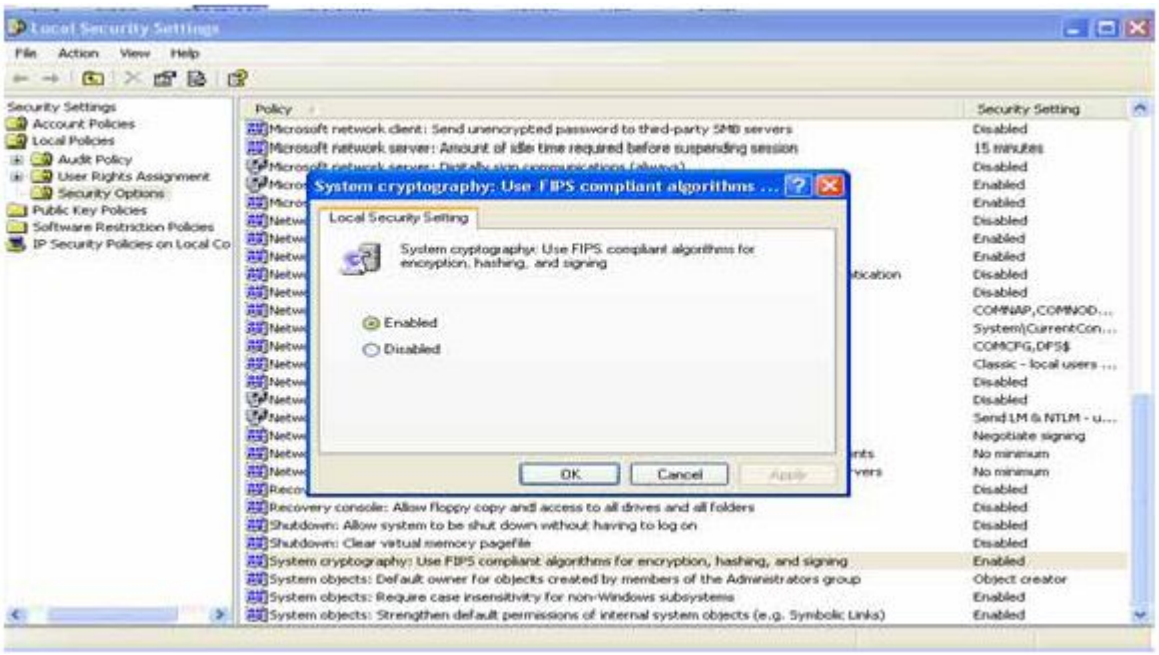
11. Select **Control Panel > Administrative Tools > Local Security Policy** to apply the configuration on the Exchange front end that interacts with SPS.

Note:

If UM is installed on the AD server, then it is under Domain Security Policy.



12. Right click **Security Options > System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**, and click **Enabled**.



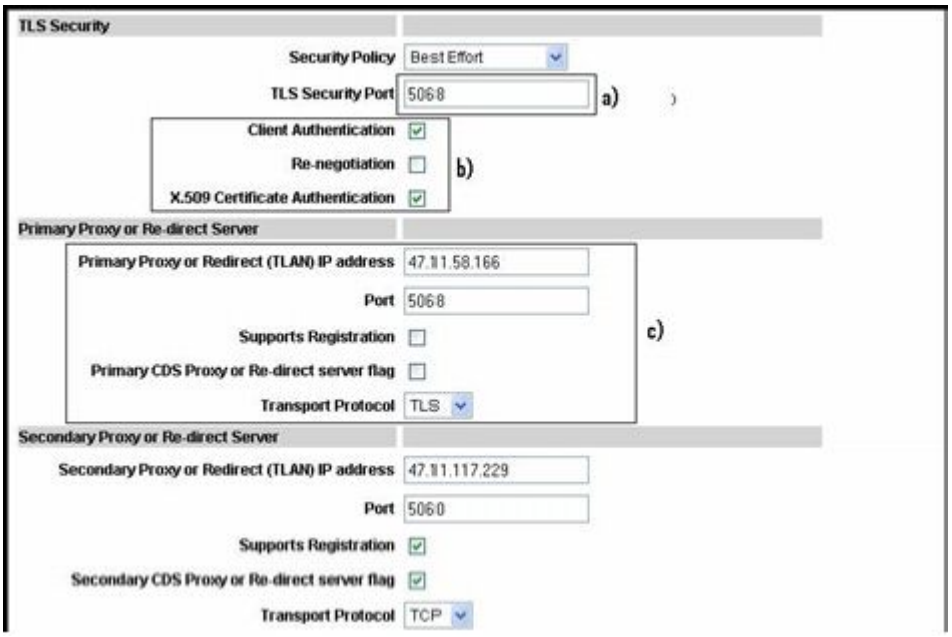
13. Navigate through SPS in the Network Routing Service Manager. Select SIP Proxy Server, Gatekeeper, and Network Connection Server.

14. Click **Restart**.
15. Select the Element Manager and configure the TLS port to 5061.

Note:

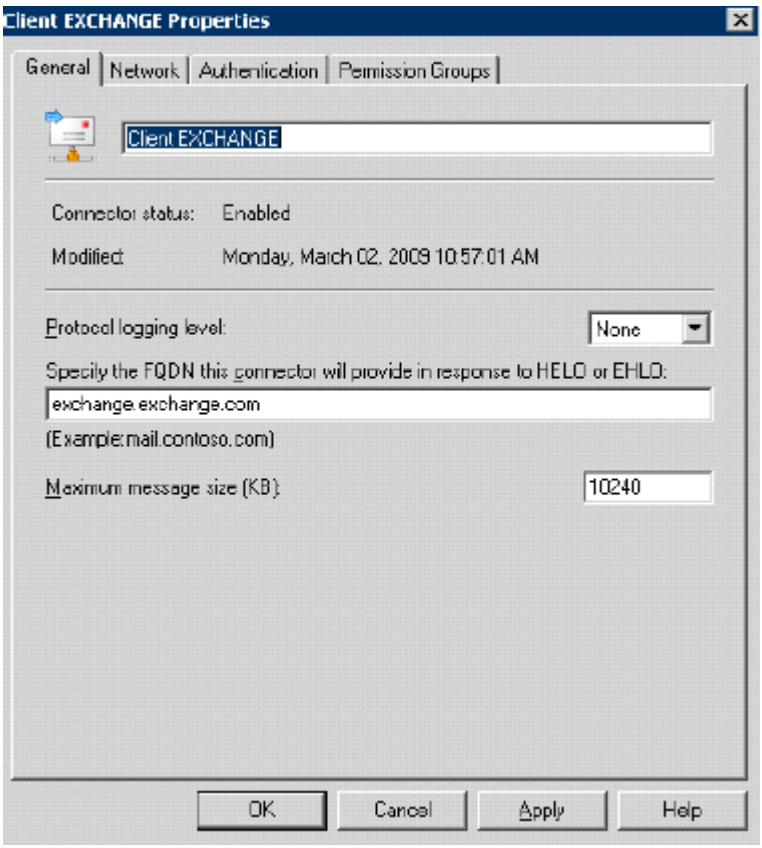
If you encounter continuous redirection when trying to make a SIP call, use the port number provided by the UM in the SIP/2.0 302 Moved Temporarily CONTACT header.05/07/2007 17:26:38 LOG0006 SIPNPM:->SIP/2.0 302 Moved Temporarily05/07/2007 17:26:38 LOG0006 SIPNPM: ->CONTACT: <sip: 5510;phone-context= fittest.swlab@bvw.com: 5068;transport=TLS;user=phone>.

16. Turn on Client Authentication and X.509 Certificate Authentication.
17. Special case for setup without SPS involvement. You can set the Primary Proxy to your UMS.
18. The DNS IP address should be updated in Element Manager (config.ini) for UM calls to complete when using TLS.

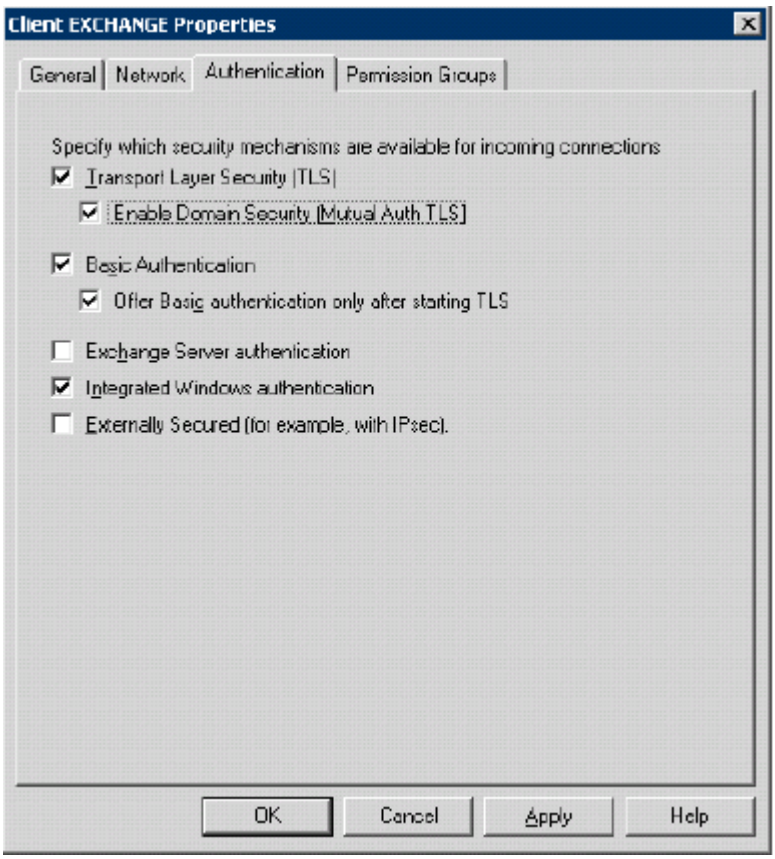


19. Verify that SPS is using the correct DNS Server with the correct class A FQDN entries for SPS and UM.
20. Restart Exchange UM service in Exchange server, as shown in the following steps.

    a. In the Client EXCHANGE Properties window, click the **Authentication** tab.



b. Select the **Enable Domain Security (Mutual Auth TLS)** check box.



c. Click **OK**.

CS 1000 CA certificate is loaded correctly into the trusted list on Exchange Server.

TLS Limitations:

- Only TLS capable Web Browsers are supported.
- Remote desktop version must be RDP client version 5.2 or greater.

For more information, see the following Web site: http://support.microsoft.com/kb/811833.

Chapter 5: Appendix UM Dialing Plan configuration examples

This chapter provides configuration examples of various customer deployment scenarios.

Navigation

Coordinated Dialing Plan network in the same cost area

The following diagram depicts multiple Avaya Communication Server 1000 (Avaya CS 1000) nodes within the same location using the Coordinated Dialing Plan (CDP).

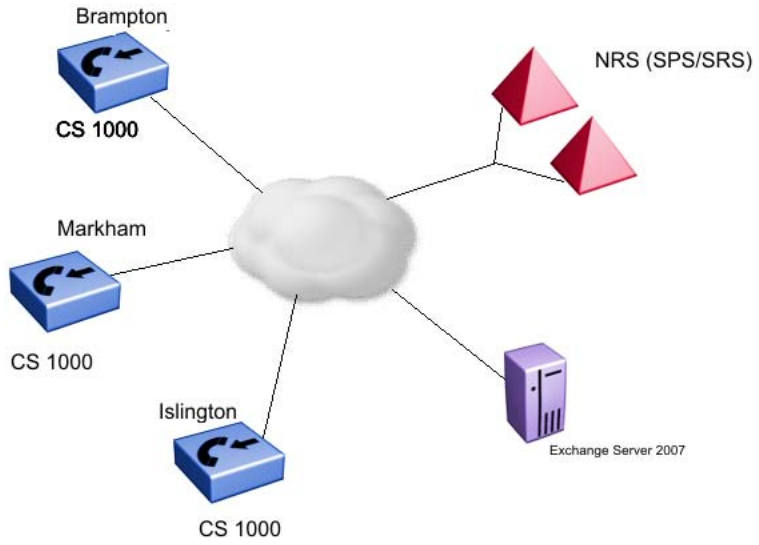


Figure 15: CDP Network in the same cost area

UM Gateway dialing plan configuration

The Gateways at each are individually configured on Unified Messaging 2007 using the same dialing plan.

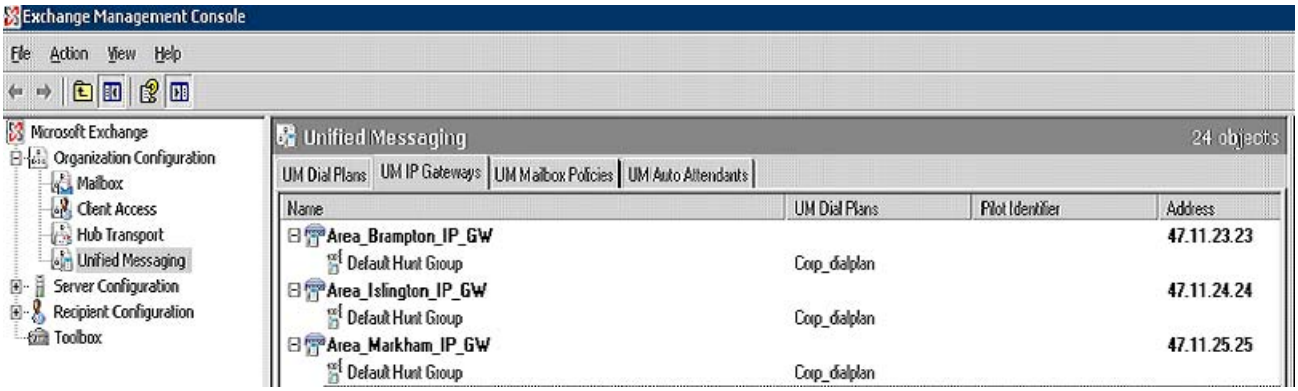


Figure 16: Unified Messaging Window—same cost area

Subscriber Access and Auto Attendant Configuration

The Subscriber Access (SA) or Auto Attendant (AA) numbers are configured using the same dialing plan. The following examples show two configurations for when these numbers are the same and when the numbers are different.

Same SA/AA numbers

All nodes in the network are configured with the same SA and AA numbers as shown in the following example.

- Markham
  - — Auto Attendant: 5000
  - — Subscriber Access: 5001
- Islington
  - — Auto Attendant: 5000
  - — Subscriber Access: 5001
- Brampton
  - — Auto Attendant: 5000
  - — Subscriber Access: 5001

Different SA/AA numbers

All nodes in the network are configured with different SA and AA numbers.

For example, a user in Brampton can access voice mail from any location using the site specific Subscriber Access number of 3001.

- Markham
  - — Auto Attendant: 5000
  - — Subscriber Access: 5001
- Islington
  - — Auto Attendant: 4000

— Subscriber Access: 4001

- Brampton

— Auto Attendant: 3000

— Subscriber Access: 3001

Outbound calling

Using the example diagram in Figure 15: CDP Network in the same cost area on page 78, the assumption is that Islington, Brampton, and Markham locations are within a local calling area. Outbound calls are enabled for all nodes by checking the Allow outgoing calls through this UM IP gateway check box as depicted in the following figure.

When a user selects the Play on the phone option from Outlook 2007, UM sends a request to one of the SIP Gateways in the same dialing plan. If one of these IP Gateways is down, UM selects another IP Gateway in the same dialing plan using a round-robin selection.

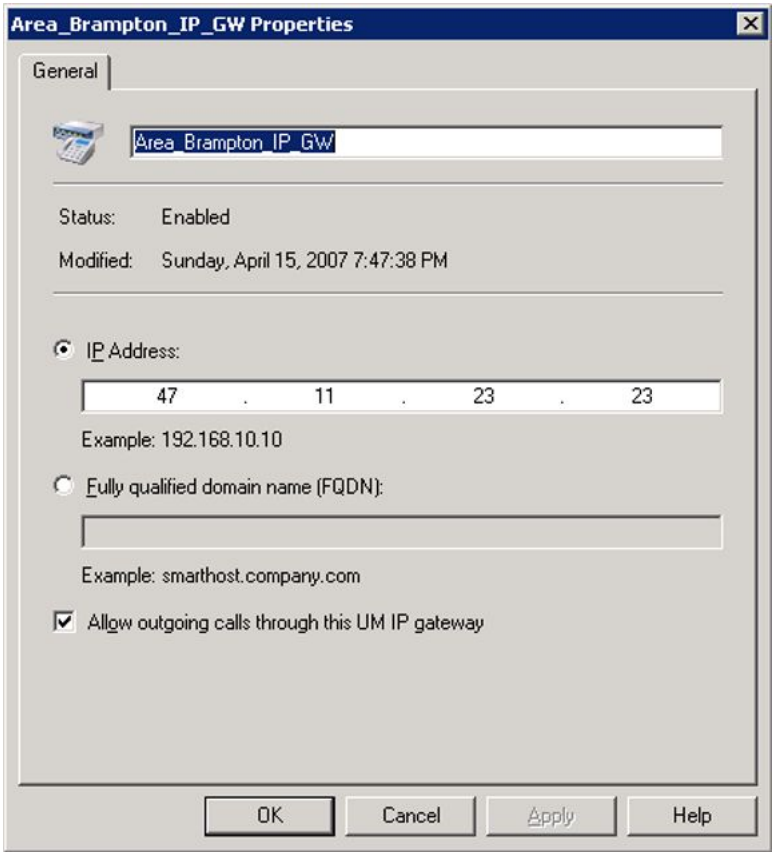


Figure 17: IP Gateway Properties window

Message Waiting Indicator configuration

For each other, the gateway is selected on the same node where the user is located. The Message Waiting Indicator (MWI) notification is sent to the selected gateway when a new voice mail message is received by the UM server. In the following figure, the Gateway is selected for the users at the Brampton node.

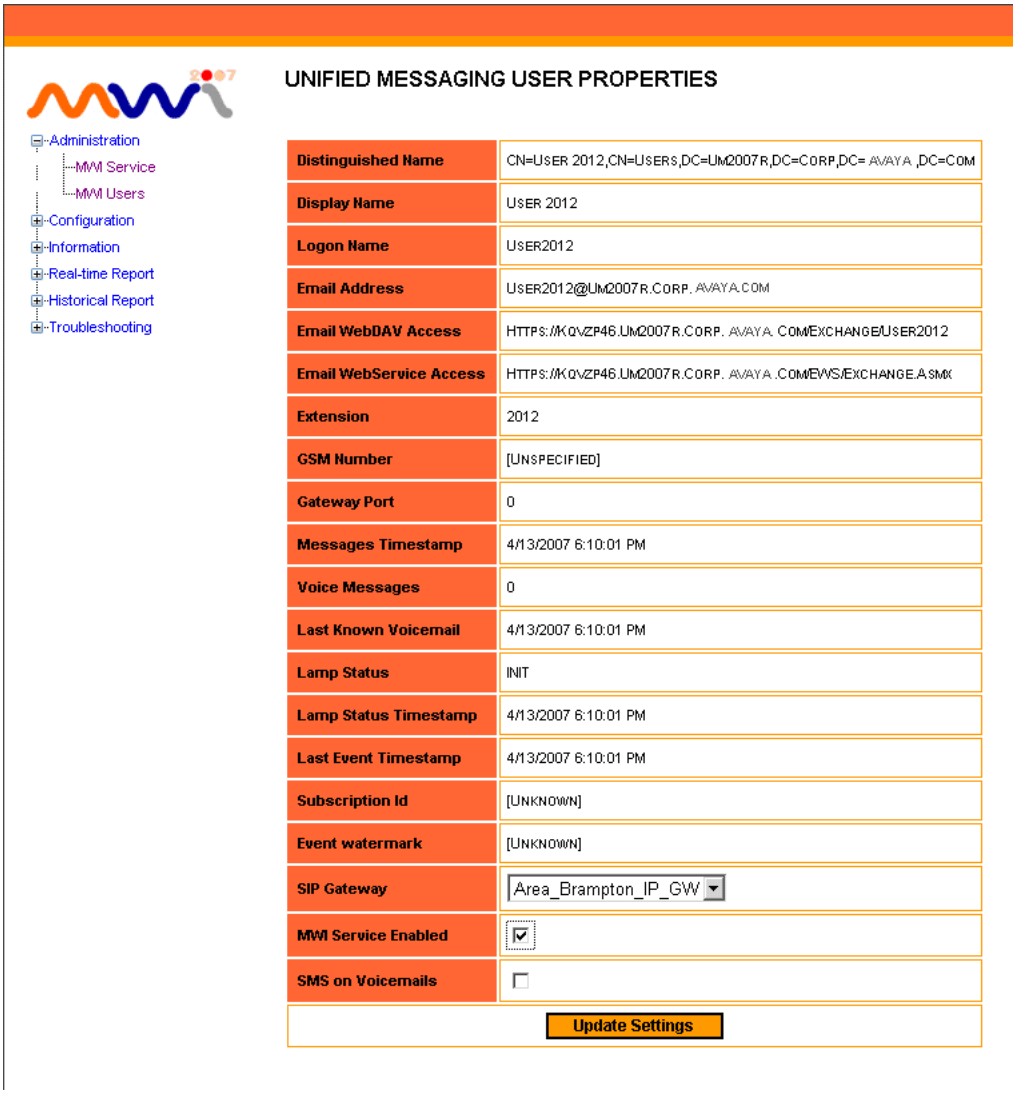


Figure 18: MWI UM User Properties

Coordinated Dialing Plan network in different cost areas

The following diagram depicts multiple Avaya CS 1000 nodes in different locations using Coordinated Dialing Plan (CDP).

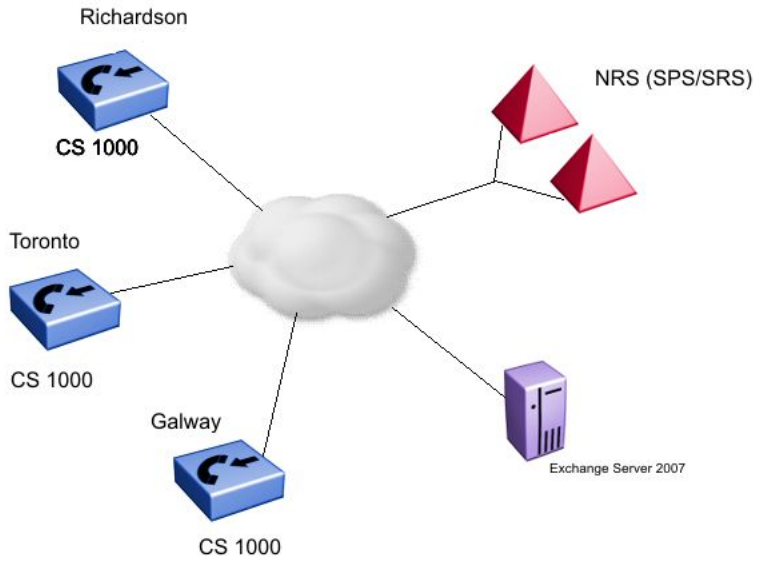


Figure 19: CDP network in different cost areas

UM Gateway dialing plan configuration

Each location must have a unique dialing plan associated with the Gateway as shown in the following figure.

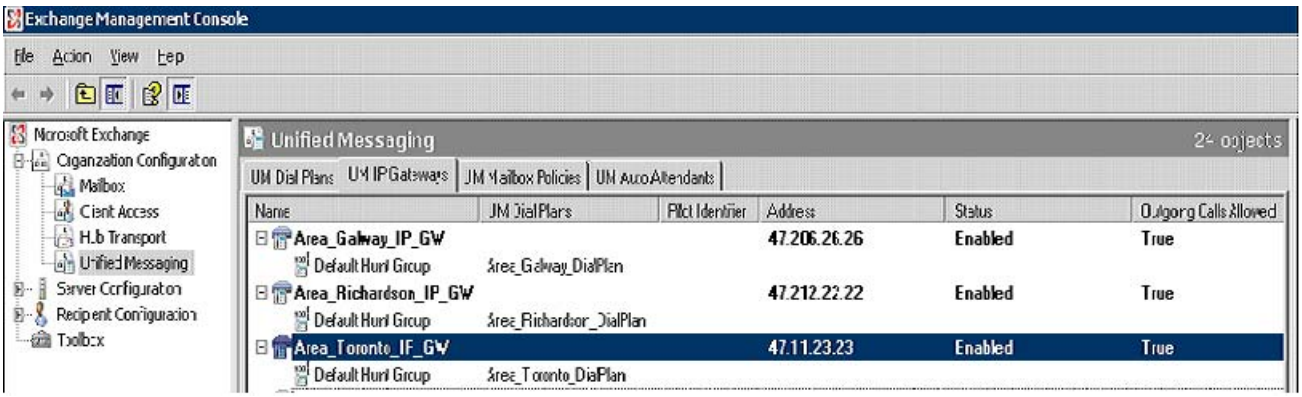


Figure 20: CDP in different locations

Subscriber Access and Auto Attendant configuration

All nodes in the network are configured with unique SA and AA numbers to access UM.

When a Toronto user accesses the UM service from Richardson, the user dials the local number 4000, the NRS routes the call to the UM server if a routing entry to UM exists. If no routing entry exists, the user cannot access the service because Richardson has a different dialing plan.

- Richardson
  - — Auto Attendant: 5000
  - — Subscriber Access: 5001
- Toronto
  - — Auto Attendant: 4000
  - — Subscriber Access: 4001
- Galway
  - — Auto Attendant: 3000
  - — Subscriber Access: 3001

The administrator must provision the network to allow the UM services to be accessed from different locations. The following example shows how the Desktop Management Interface (DMI) can be used. This example allows users from other locations to use the SA/AA number without incurring long distance charges or restrictions.

- In Richardson, insert prefix 4 for DN 4001, for example 44001.
- Configure 44 as a routing entry for Toronto on the NRS.
- In Toronto, delete prefix 4 and route the call to the NRS to terminate on UM.

Outbound calling

Each locations maps to a separate dialing plan. When a user from Richardson selects Play on phone option to dial a number, the call is routed through the Richardson Gateway. Outbound calls for each location are enabled by checking the Allow outgoing calls through this UM IP gateway check box as depicted in the following figure. Long distance charges and restrictions for the user in the Exchange Server console apply.

UDP/CDP network in different cost area

The following diagram depicts the three locations in relation to each other as defined in the UDP dialing plan.

For one location to reach another location, the user must dial the location code followed by the user DN.

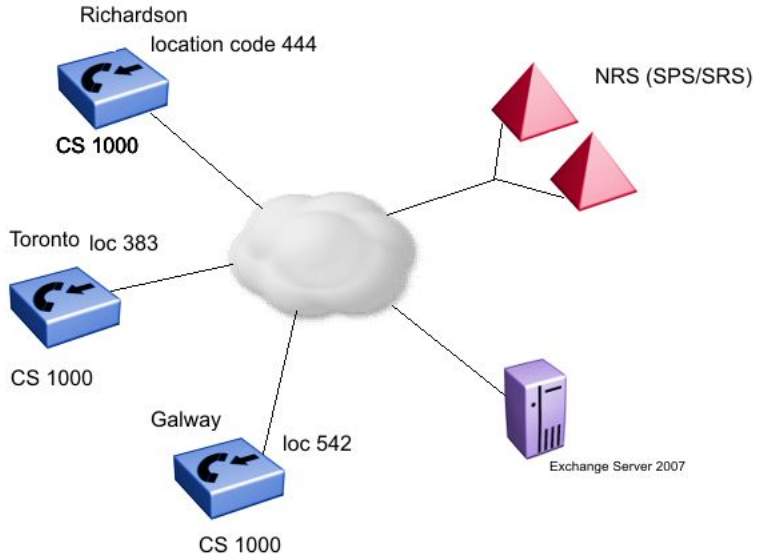


Figure 21: UDP/CDP in different cost areas

UM gateway dialing plan configuration

Each location must have a dialing plan associated with the gateway.

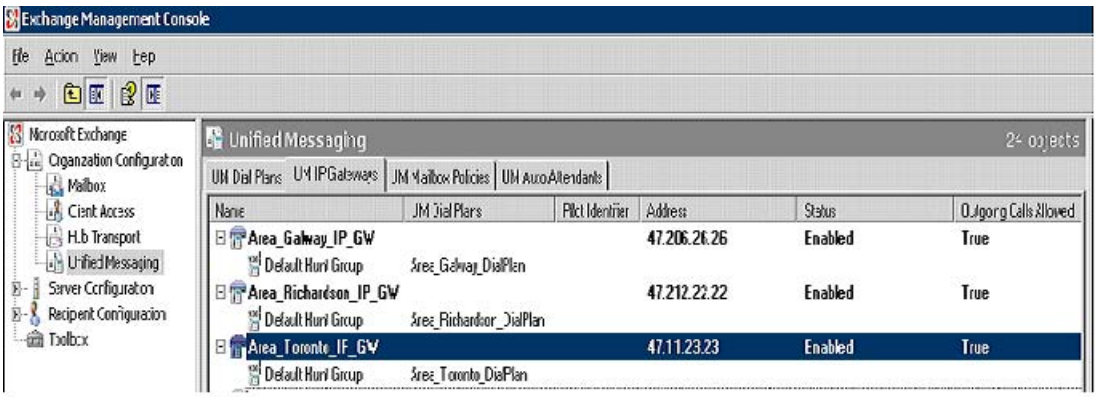


Figure 22: UDP/CDP network in different cost areas

Subscriber Access and Auto Attendant configuration

Users can directly access the local SA/AA number. When access is required from a remote location, the location code must be prefixed to the SA/AA number.

When a Toronto user accesses UM service from Richardson, the location code of Toronto (383) must be included with the number. For example, 383-5000. The user can then make the call from the home CS 1000. UM permits the Subscriber Access to use the services.

Each node can have the same or different SA/AA numbers. All sites have the same SA/AA number as follows:

- Auto Attendant: 5000
- Subscriber Access: 5001

Outbound calling

Each location maps to a separate dialing plan. When a user from Richardson selects the Play on phone option to dial a number, the Richardson Gateway is used. The restriction rules apply for the user as defined on the Exchange console.

Branch Office in the same long distance cost area

The following diagram depicts a Branch office scenario where the Main Office (MO) and two Branch Offices are in the same long distance cost area. One BO is in local mode (IP connection to the MO was lost).

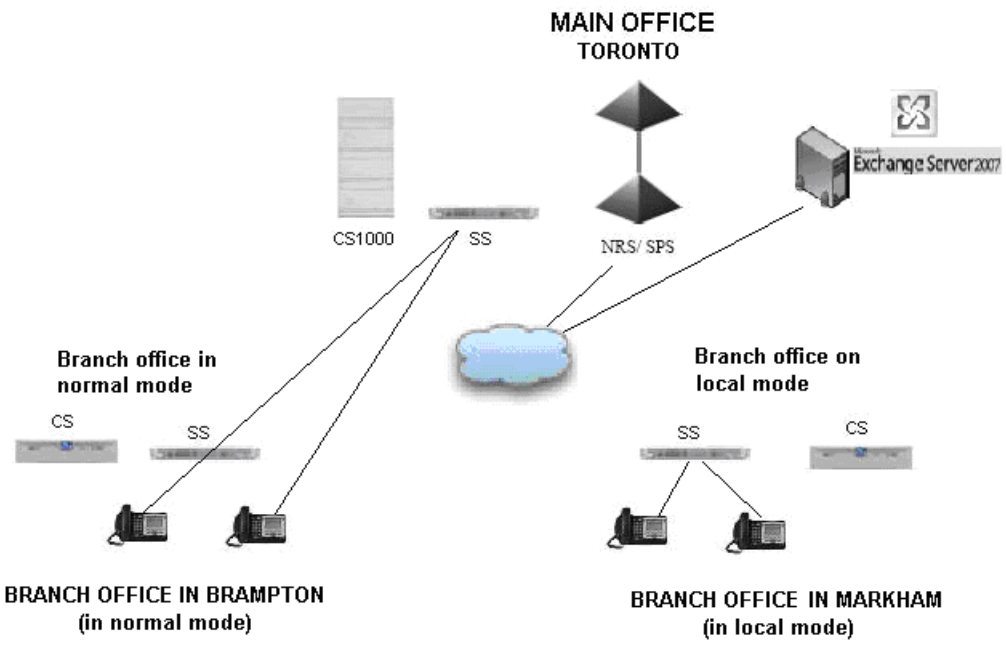


Figure 23: Branch Office in the same long distance cost area

UM Gateway dialing plan configuration

The gateways at each Main Office and Branch Office site are configured individually on UM 2007 with the same dialing plan,

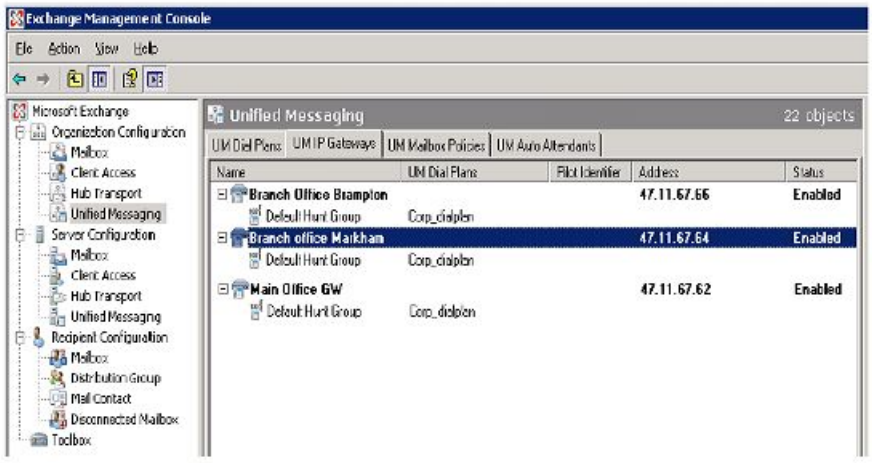


Figure 24: BO in the same long distance cost area

Subscriber Access and Auto Attendant configuration

The following list describes the Subscriber Access modes available for Branch Office:

- Branch Office in normal mode: In normal mode, telephones are registered to the MO Signaling Server. When a user dials the SA number, the MO SIP Gateway sends a request to UM 2007. When the MO Gateway is configured with the corporate dialing plan, UM grants access to the user mailbox.
- Branch Office in Local mode: in local mode, telephones are registered to the BO Gateway. When the user dials the SA number, the BO SIP Gateway sends a request to UM 2007. When BO Gateway is configured with the same dialing plan as the MO, UM grants access to the user mailbox.

Outbound calling

When the Branch Office locations are in the same long distance cost area (Toronto, Brampton, and Markham), all three gateways are enabled for outbound calling by selecting the Allow outgoing calls through this UM IP gateway check box as shown in the following figure. When a user selects the Play on phone feature of Outlook 2007, UM sends a request to one of the SIP Gateways in the same dialing plan. When the selected Gateway is down, UM selects another IP Gateway in the same dialing plan using a round-robin selection.

MWI configuration

Each user in the MO/BO is configured for either normal or local Mode. MWI support can be provided to the user either in the normal or local mode, but not both. This is a limitation of the Geomant MWI application. The application does not support multiple IP Gateway configurations for an individual user or multiple instances of the MWI application. The following figure describes the configuration for MWI support for normal mode.

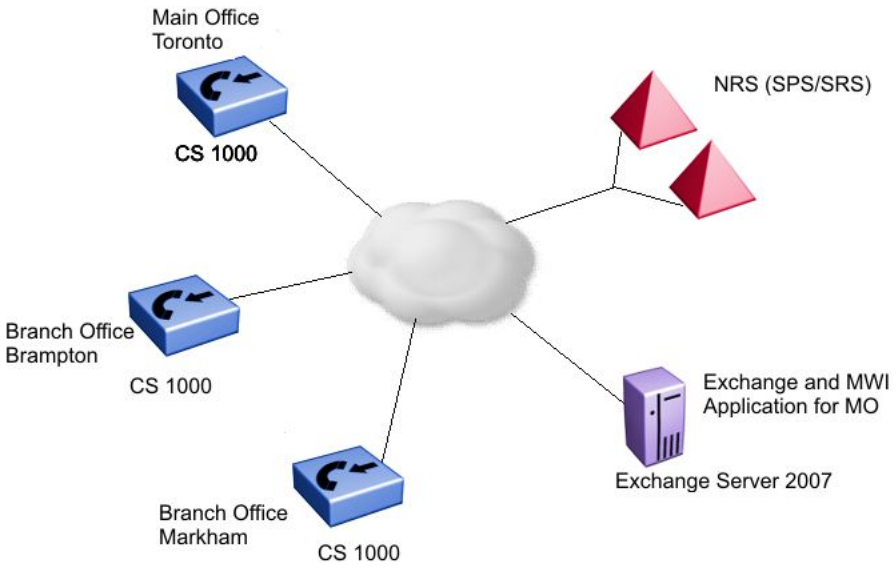


Figure 25: MWI support for normal mode

The following describes the required configuration for MWI for Unified Messaging User Properties for normal and local mode for a user on the Brampton BO.

- MWI support for normal mode: The SIP Gateway parameter points to the MO Gateway
- MWI support for local mode: The SIP Gateway parameter points to the Brampton BO Gateway

Branch Office in a different long distance cost area

For outbound calling, the configuration for the Gateway is disabled by clearing the box Allow outgoing calls through this UM IP gateway. This is necessary as one or more BOs are in different long distance cost areas.

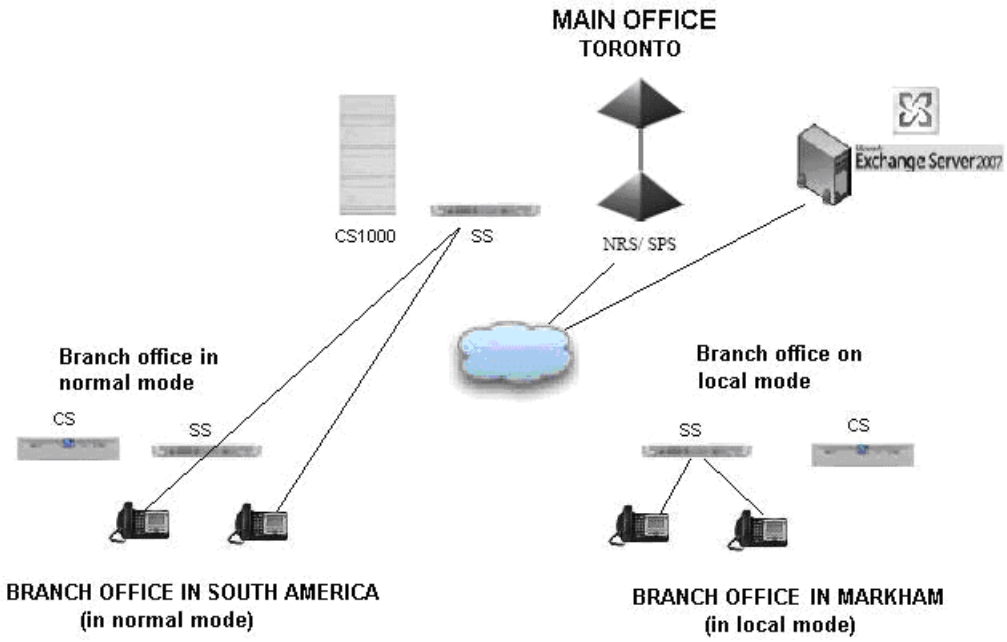


Figure 26: Branch Office in a different long distance cost area

Virtual Office

The following diagram depicts a virtual office scenario

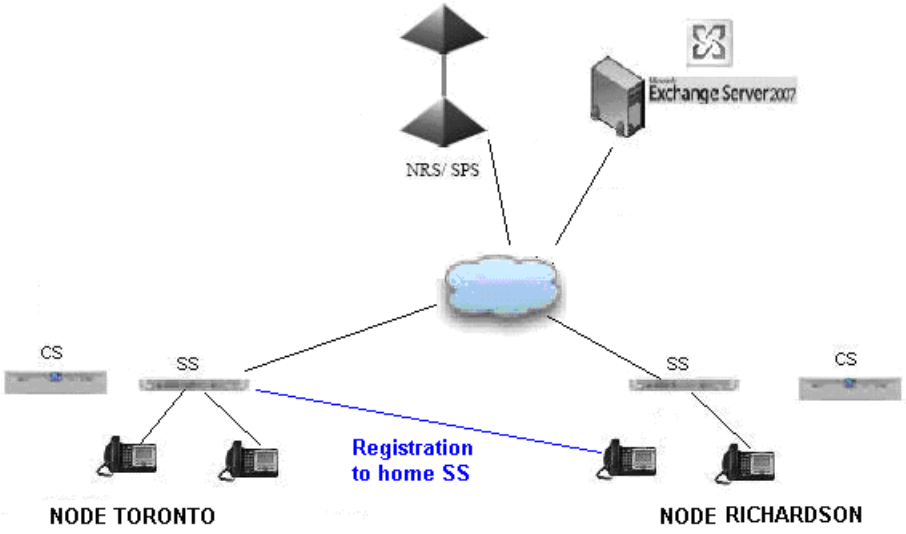


Figure 27: Virtual Office

UM Gateway dialing plan configuration

You can individually configure the gateway on each site using the same or a different dialing plan.

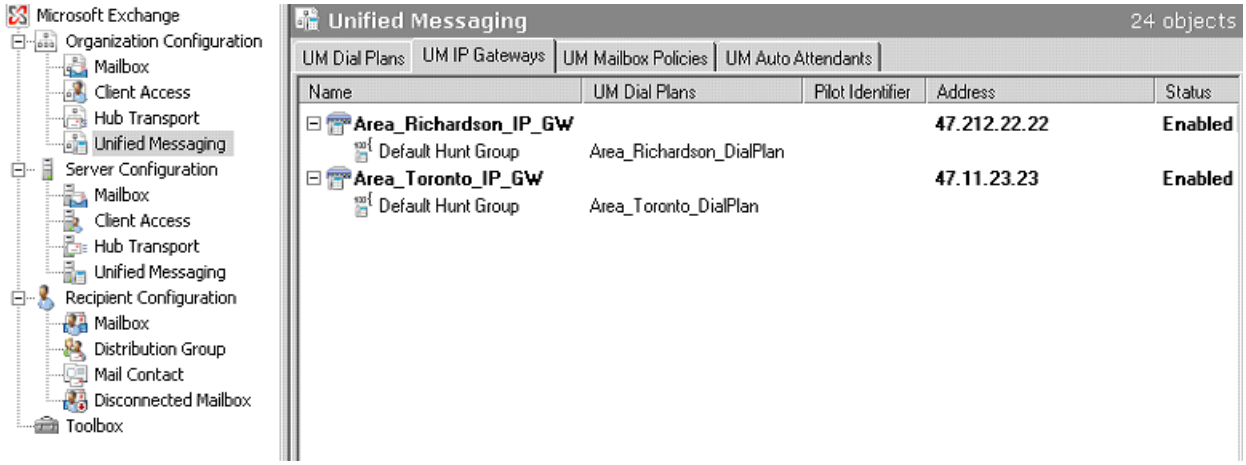


Figure 28: Unified Messaging Window—Virtual Office dialing plan

Subscriber Access and Auto Attendant number configuration

When a user in Toronto travels temporarily to the Richardson location, the user performs a Virtual Office logon and the telephone registers to the Toronto Gateway. The local Toronto access number is dialed and the Toronto Gateway sends a request to UM allowing access to the user mailbox.

Outbound calling

When logged on with the Virtual Office feature, outbound calling is operational.

Geographic Redundancy

The following diagram depicts an example of Geographic Redundancy.

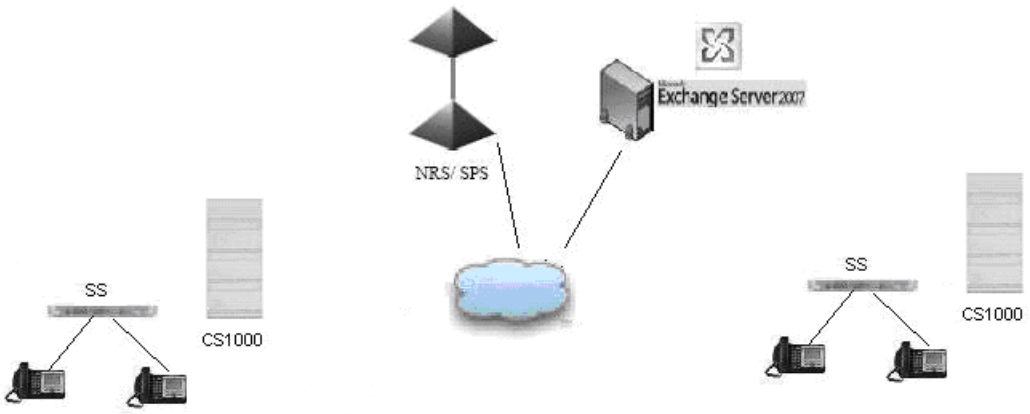


Figure 29: Geographic Redundancy

With Geographic Redundancy, telephones are redirected to the secondary Call Server if the Primary Call Server goes down. The Gateway for both Call Servers is configured in UM 2007 using the same dialing plan.

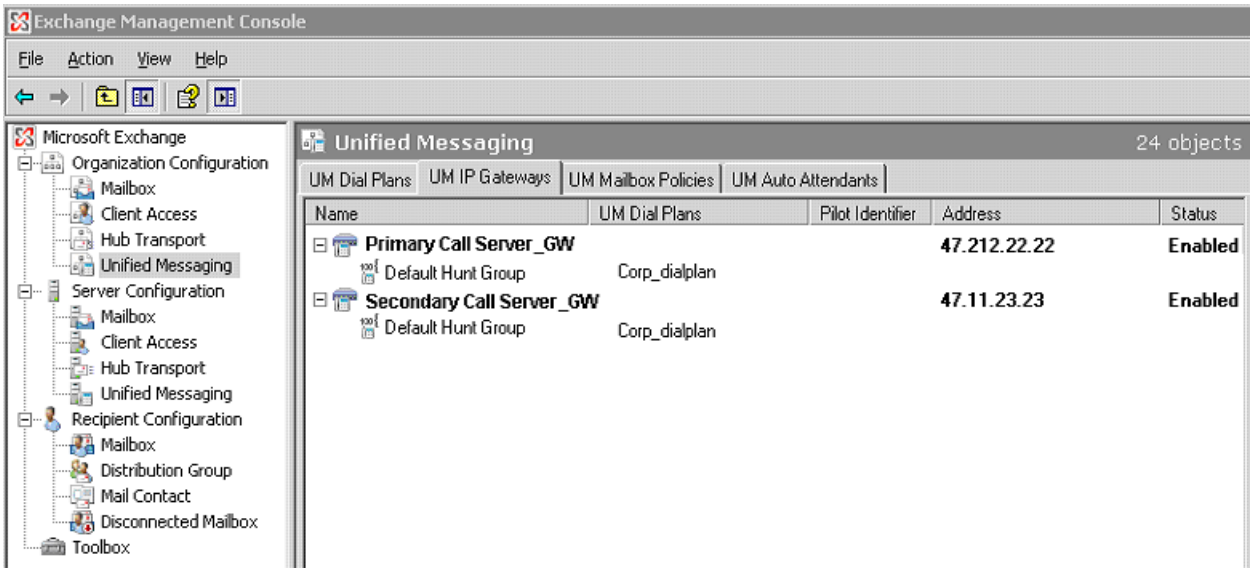


Figure 30: Geographic Redundancy Dialing plan

Subscriber Access and Auto Attendant configuration

The primary and secondary Call Server are both configured as part of the same dialing plan. The users can connect to UM in primary Call Server or secondary Call Server mode.

Outbound calling

Outbound callings works the same as in Main Office and Branch Office configurations.

Message Waiting Indicator

The Message Waiting Indicator setup is similar to the Main Office, Branch Office, and Geographic Redundancy configurations.

Other scenarios

Many combinations of scenarios identified in this chapter are also possible.