



# **Avaya Converged Office Fundamentals Avaya Communication Server 1000**

7.5  
NN43001-525, 05.04  
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/](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](mailto: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

<b>Chapter 1: New in this release</b>	<b>9</b>
Navigation	9
Feature changes	9
Other changes	9
<b>Chapter 2: Customer service</b>	<b>13</b>
Navigation	13
Getting technical documentation	13
Getting product training	13
Getting help from a distributor or reseller	13
Getting technical support from the Avaya Web site	14
<b>Chapter 3: About this document</b>	<b>15</b>
Subject	15
Applicable systems	15
Intended audience	15
Conventions	16
Terminology	16
Related information	16
Technical documents	16
<b>Chapter 4: Overview</b>	<b>19</b>
Contents	19
Product Description	19
Technical Description	19
Release 5.0 enhancements	20
Remote Call Control with SIP CTI (TR/87)	20
Telephony Gateway and Services	22
Multimedia Convergence Manager	24
SIP CTI (TR/87) Protocol	24
<b>Chapter 5: Feature Operation</b>	<b>25</b>
Contents	25
Introduction	25
Sample configuration	25
Remote Call Control functionality	27
Microsoft® Office Communicator 2005 features	28
Contact Icons	40
Telephony Gateway and Services functionality	41
CS 1000 Services	41
PCA	41
MCM	42
Microsoft® Office Communicator 2005 features	42
Establishing Multimedia Sessions	48
Video calls	49
<b>Chapter 6: Planning and Engineering</b>	<b>53</b>
Contents	53
Introduction	53

Network Design.....	54
Small network.....	54
Medium network.....	55
Large network.....	56
General Recommendations.....	63
Operating System Required.....	64
Signaling Server.....	67
Trunking.....	67
Security Considerations.....	70
Dial Plan Considerations.....	73
Telephony Gateway and Services.....	77
Capacity.....	77
Redundancy.....	77
SIP routing.....	78
Feature Limitations.....	79
Remote Call Control with SIP CTI.....	86
Capacity.....	90
Redundancy.....	92
Feature limitations.....	94
<b>Chapter 7: Installation and Configuration.....</b>	<b>99</b>
Contents.....	99
Overview.....	99
Installing CS 1000 components.....	103
Installing the Call Server.....	103
Installing the Signaling Server.....	103
Installing Microsoft Live® Communications Server components.....	104
Installing Active Directory.....	104
Installing Live Communications Server 2005 Service Pack 1 (SP1).....	104
Installing and configuring MCM.....	106
Installing MCM software.....	106
Configuring MCM.....	109
Select component for configuration.....	123
Configuring Telephony Gateway and Services.....	124
Configuring Live Communications Server.....	124
Configuring Active Directory.....	141
Configuring the Call Server.....	144
Configuring Home LOC and Home NPA.....	152
Configuring the DNS Server.....	152
Configuring the SIP Trunk.....	153
Domain naming.....	154
URI Mapping.....	156
Configuring SIP Gateway CLID Parameters.....	157
Parameter: Country Code.....	159
Parameter: Area Code.....	159
Parameter: Subscriber / Number of Digits to strip.....	159
Parameter: Subscriber / Prefix to insert.....	159
Parameter: National / Number of Digits to strip.....	159

Parameter: International / Number of Digits to strip.....	160
Parameter: National / Prefix to insert.....	160
Parameter: International / Prefix to insert.....	160
Configuring SPS.....	160
Configuring NRS.....	160
Configuring Microsoft® Office Communicator 2005.....	162
Configuring CDR.....	166
Dialing E.164 International Format Numbers from Microsoft® Office Communicator - Computer Calls (SIP Gateway).....	166
Normalizing phone numbers.....	167
Configuring Remote Call Control.....	167
Configuring the CS 1000.....	167
Configuring the Signaling Server.....	170
Configuring SIP CTI Settings.....	173
Configuring SIP CTI CLID Parameters.....	177
Scenario 1 - SIP STI Dial Plan = CDP.....	178
Scenario 2 - SIP CTI Dial Plan = UDP.....	178
Parameter: Calling Device URI Format.....	178
Parameter: Country Code.....	179
Parameter: Area Code.....	180
Parameter: Subscriber/Number of Digits to strip.....	180
Parameter: Subscriber/Prefix to insert.....	180
Parameter: National/Number of Digits to strip.....	180
Parameter: National/Prefix to insert.....	180
Parameter: International/Number of Digits to strip.....	182
Parameter: International/Prefix to insert.....	183
Configuring Live Communications Server.....	183
Configuring Active Directory.....	183
Configuring the SIP URI Map.....	188
Configuring the Do Not Disturb feature.....	188
Configuring CDR.....	189
Configuring Microsoft® Office Communicator 2005.....	189
Configuring Phone Integration Settings.....	190
Configuring Account details.....	190
Dialing E.164 International Format Numbers from Microsoft® Office Communicator - Phone Calls (SIP CTI).....	191
Normalizing phone numbers.....	192
Normalizing Offline (Recommended).....	192
Normalizing using the Address Book Service.....	193
Creating Normalization rules.....	193
Configuring SIP Routing and Redundancy.....	197
Configuring Remote Call Control SIP Routing Using Phone Addressing.....	198
Configuring Remote Call Control SIP Routing Using a Gateway Endpoint Name.....	198
Configuring Redundancy.....	199
Deploying Live Communications Server Client PC application to end users.....	199
Installing Windows Messenger 5.1.....	199
Installing Microsoft® Office Communicator 2005 client software.....	199
Installing Microsoft® Office 2003 and Windows XP.....	200

Configuring Transport Layer Security (TLS).....	201
Limitations and requirements.....	201
Configuring TLS.....	202
<b>Chapter 8: Maintenance.....</b>	<b>213</b>
Contents.....	213
Introduction.....	213
Telephony Gateway and Services.....	213
Avaya Communication Server 1000.....	213
MCM.....	213
Remote Call Control.....	216
Signaling Server OAM Level CLI Commands.....	218
Operational Measurements.....	220
Signaling Server Expert Level CLI Commands.....	221
<b>Appendix A: Call Flow and Protocol Details.....</b>	<b>223</b>
Contents.....	223
Overview.....	223
Message sequence.....	224
Call flow.....	225
Remote Call Control Call Flow.....	225
Telephony Gateway and Services Call Flow.....	226
Supported features.....	228
<b>Appendix B: Configuration Examples.....</b>	<b>231</b>
Contents.....	231
Introduction.....	231
Standard Edition.....	231
Setting up the lab.....	232
Collecting required data.....	233
Configuring the Call Server.....	234
Configuring the Signaling Server.....	239
Configuring Active Directory.....	244
Configuring and installing MCM.....	247
Enterprise Edition.....	251
Overview of general lab set-up.....	251
LCS Management Console.....	254
Security/Certificates.....	259
Host Authorization.....	261
Routing.....	263
Configuring DNS.....	267
Active Directory configuration.....	269
Installing and configuring MCM.....	269
Configuring the Signaling Server.....	272
Configuring NRS.....	273
<b>Appendix C: Troubleshooting.....</b>	<b>275</b>
General Troubleshooting.....	275
Issues of concern.....	283
Issue 1.....	283
Issue 2.....	284

Issue 3.....	285
Issue 4.....	286
Issue 5.....	286
Issue 6.....	286
Issue 7.....	286
Issue 8.....	287
Case checklists.....	289
<b>Appendix D: Abbreviations.....</b>	<b>293</b>
<b>Appendix E: Glossary.....</b>	<b>295</b>
TR/87 Front End/ECMA Front End.....	295
<b>Index.....</b>	<b>297</b>



# Chapter 1: New in this release

The following sections details what's new in *Avaya Converged Office Fundamentals (NN43001-525)* for Avaya Communication Server 1000 Release 7.5.

---

## Navigation

- [Feature changes](#) on page 9
- [Other changes](#) on page 9

---

## Feature changes

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

---

## Other changes

### Revision history

August 2011	Standard 05.04. This document is up-issued to support the removal of content for outdated features, hardware, and system types.
March 2011	Standard 05.03. This document is up-issued to support Avaya Communication Server 1000 Release 7.5.
November 2010	Standard 05.02. This document is up-issued to support Avaya Communication Server 1000 Release 7.5.
November 2010	Standard 05.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.5.
March 2011	Standard 04.02. This document is up-issued to support Avaya Communication Server 1000 Release 7.0.
June 2010	Standard 04.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.0.

## New in this release

May 2009	Standard 03.02. This document is up-issued to support Communication Server Release 6.0.
May 2009	Standard 03.01. This document is up-issued to support Communication Server Release 6.0.
December 2008	Standard 02.03. This document is up-issued to include the DACP feature.
May 2008	Standard 02.02. This document is up-issued to support Transport Layer Security (TLS).
December 2007	Standard 02.01. This document is up-issued to support Release 5.5.
July 2007	Standard 01.04. This document is up-issued to address CR Q01461058.
June 2007	Standard 01.03. This document is up-issued to reflect changes in technical content and to address the following CRs: <ul style="list-style-type: none"><li>• Q01487669</li><li>• Q01539454</li><li>• Q01542198</li><li>• Q01544293</li><li>• Q01545631</li><li>• Q01565375</li><li>• Q01646965</li></ul>
June 2007	Standard 01.02. This document is up-issued to include new content and to address the following CRs: <ul style="list-style-type: none"><li>• Q01461313</li><li>• Q01461593</li></ul>
May 2007	Standard 01.01. This document is issued to support Communication Server 1000 Release 5.0. This document is renamed Converged Office Fundamentals (NN43001-525) and contains information previously contained in the legacy document, now retired: Converged Office Implementation Guide (553-3001-025).
December 2006	Standard 9.00. This document is up-issued to reflect changes in technical content and to address the following CRs: <ul style="list-style-type: none"><li>• Q01298206,</li><li>• Q01501375</li></ul>
October 2006	Standard 8.00. This document is up-issued to reflect changes in technical content.

July 2006	Standard 7.00. This document is up-issued to reflect changes in technical content and to address the following CRs: <ul style="list-style-type: none"><li>• Q01363480</li><li>• Q01377376</li></ul>
June 2006	Standard 6.00. This document is up-issued with corrections related to CS 1000 Release 4.5 content.
April 2006	Standard 5.00. This document is up-issued with corrections related to CS 1000 Release 4.5 content.
January 2006	Standard. 4.00. This document is up-issued with corrections related to CS 1000 Release 4.5 content.
January 2006	Standard 3.00. This document is up-issued with corrections related to CS 1000 Release 4.5 content.
January 2006	Standard 2.00. This document is up-issued with corrections related to CS 1000Release 4.5 content.
December 2005	Standard 1.00. This is a new document. It was created to support the new Microsoft® Office Live Communications Server Converged Office project.

New in this release

# 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](http://www.avaya.com) or go to one of the pages listed in the following sections.

---

## Navigation

- [Getting technical documentation](#) on page 13
- [Getting product training](#) on page 13
- [Getting help from a distributor or reseller](#) on page 13
- [Getting technical support from the Avaya Web site](#) on page 14

---

## Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to [www.avaya.com/support](http://www.avaya.com/support).

---

## Getting product training

Ongoing product training is available. For more information or to register, go to [www.avaya.com/support](http://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](http://www.avaya.com/support).

# Chapter 3: About this document

This is a global document. Contact your system supplier or your Avaya representative to verify that the hardware and software described are supported in your area.

---

## Subject

This document describes the various elements and processes involved in the Avaya - Microsoft® Office Live Communications Server 2005 Converged Office project to support the Avaya Communication Server 1000 platform.

For information relating to Office Communications Server (OCS) 2007, refer to Avaya Converged Office Fundamentals — Microsoft Office Communications Server 2007 (NN43001-121).

---

## Applicable systems

This document applies to the following systems:

- Avaya Communication Server 1000M Single Group (Avaya CS 1000M SG)
- Avaya Communication Server 1000M Multi Group (Avaya CS 1000M MG)
- Avaya Communication Server 1000E (Avaya CS 1000E)

---

## Intended audience

This document is intended for individuals who plan and configure the Avaya CS 1000 and Microsoft® Office Live Communications Server 2005 interworking.

---

## Conventions

---

## Terminology

In this document, the following systems are referred to generically as system:

- Communication Server 1000E (CS 1000E)
- Communication Server 1000M (CS 1000M)
- Meridian 1

---

## Related information

This section lists information sources that relate to this document.

---

## Technical documents

The following technical documents are referenced in this document:

- *Avaya New in This Release (NN43001-115)*
- *Avaya Transmission Parameters (NN43001-282)*
- *Avaya Signaling Server IP Line Applications Fundamentals (NN43001-125)*
- *Avaya IP Peer Networking: Installation and Commissioning (NN43001-313)*
- *Avaya Features and Services (NN43001-106)*
- *Avaya Software Input/Output: Maintenance (NN43001-711)*
- *Avaya Communication Server 1000M and Meridian 1: Small System Installation and Configuration (NN43011-310)*
- *Avaya Communication Server 1000M and Meridian 1: Large System Installation and Commissioning (NN43021-310)*
- *Avaya Communication Server 1000E: Installation and Configuration (NN43041-310)*

## Microsoft® Documentation

Before you read this document, Avaya strongly recommends that you refer to the companion document, *Microsoft® Office Communicator 2005 Telephony Planning and Deployment Guide*, available on the Microsoft® web site:

<http://www.microsoft.com/en/us/default.aspx>

On the Microsoft® web site, go to the Downloads page. On the Downloads page, search on Office Communicator 2005. On the results page, select the Office Communicator 2005 Planning and Deployment Guide link.

## Online

To access Avaya documentation online, go to:

[www.avaya.com/support](http://www.avaya.com/support)

About this document

# Chapter 4: Overview

---

## Contents

This section contains information about the following topics:

[Product Description](#) on page 19

[Technical Description](#) on page 19

[Remote Call Control with SIP CTI \(TR/87\)](#) on page 20

[Telephony Gateway and Services](#) on page 22

[Multimedia Convergence Manager](#) on page 24

[SIP CTI \(TR/87\) Protocol](#) on page 24

---

## Product Description

The multimedia strategy of many Avaya Communication Server 1000 customers is based on deploying the Microsoft® Office Communicator soft clients and Live Communications Server. This strategy enables the introduction of multimedia capabilities using popular instant messenger (IM) clients without the need to install and support additional desktop software.

The Avaya Converged Office feature combines the business-grade telephony of the Avaya CS 1000 with the real-time multimedia communication and the remote call control provided by Microsoft® Office Live Communications Server 2005 and Microsoft® Office Communicator 2005 products.

---

## Technical Description

Avaya Converged Office is defined by the following two components:

- Remote Call Control with Session Initiation Protocol (SIP) Computer Telephone Integration (CTI) TR/87 provides full Microsoft® Office integration of telephony to control

business grade telephony phones from within Microsoft® Office applications, as well as support for a standards-based CTI interface defined by the TR/87 protocol.

- Telephony Gateway and Services provides a basic SIP Telephony Gateway for connectivity between Private and Public Telephony networks and Live Communications Server 2005 clients.

Avaya offers a unique value with these two components by providing its telephony services to Office Communicator 2005 clients—in addition to providing connectivity between the Microsoft® Live Communications Server and the Avaya telephony network.

---

## Release 5.0 enhancements

---

### Remote Call Control with SIP CTI (TR/87)

---

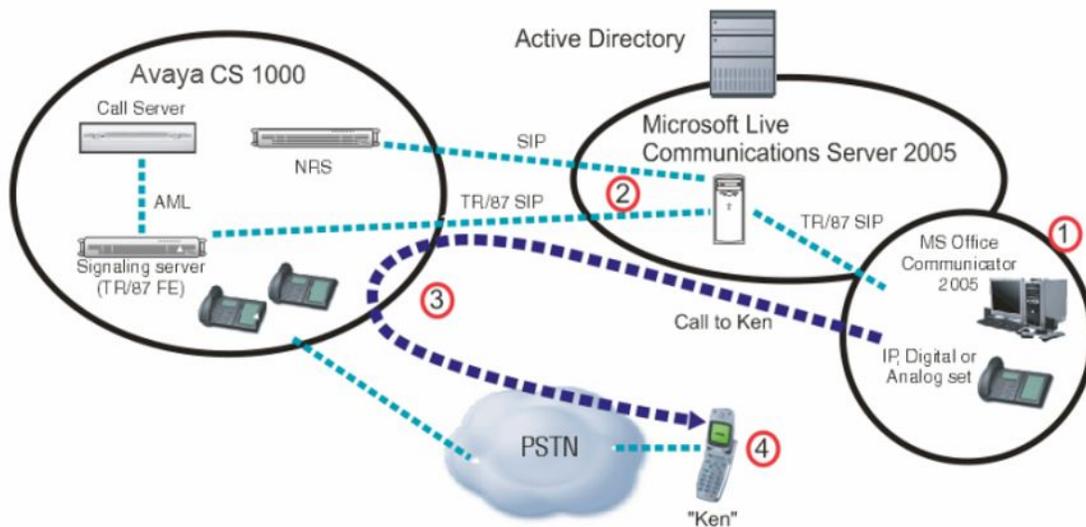
The Remote Call Control component (illustrated in [Figure 1: Remote Call Control with SIP CTI \(TR/87\)](#) on page 21) provides convergence beyond the Microsoft® desktop IM client by moving into the full suite of Microsoft® Office applications and documents. By using Remote Call Control, enabled by the Office Communicator 2005 client, users can invoke many telephony features of the CS 1000 telephones through the intuitive user interface of a PC client.

 **Important:**

A feature which is not supported by the phone cannot be invoked through Office Communicator.

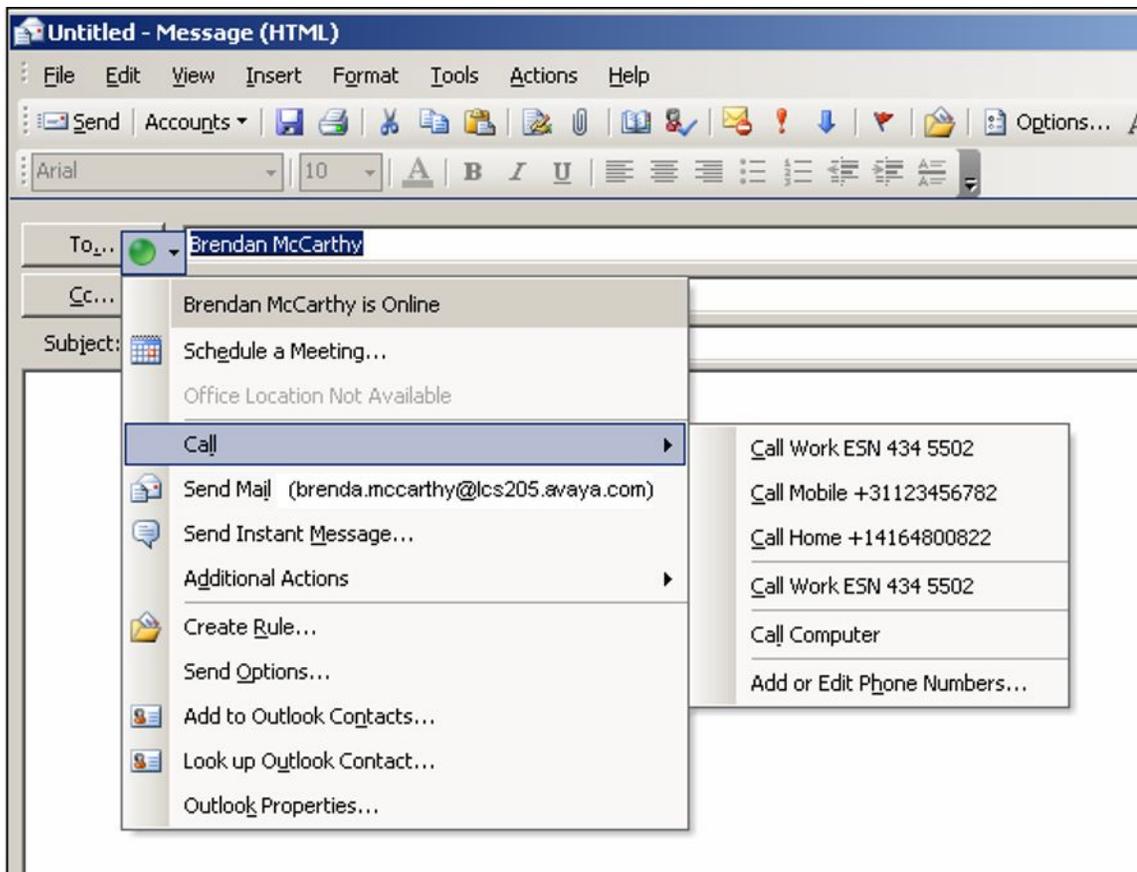
The example in Remote Call Control with SIP CTI (TR/87) shows the following:

1. A user selects "Call" to Ken's Mobile Phone number from his CS 1000 telephone
2. The Live Communications Server sends a call request to the CS 1000
3. The CS 1000 sets up a call from the user's phone to Ken's mobile phone number
4. Ken answers his mobile phone and a media path is established between the two phones



**Figure 1: Remote Call Control with SIP CTI (TR/87)**

Users can, for example, operate the “Call” function from any contact icon visible within an e-mail or document in the Microsoft® Office suite (see the example in [Figure 2: Contact menu](#) on page 22). This function is provided by support for the European Computer Manufacturer’s Association (ECMA) TR/87 protocol on the CS 1000 Signaling Server. TR/87 is the specification that Office Communicator 2005 uses to implement phone integration throughout the suite of Microsoft® Office applications.



**Figure 2: Contact menu**

The full set of business-grade telephony features available with CS 1000 telephones is integrated with the Microsoft® Office Communicator client and can also be operated from a CS 1000 IP Phone, even when the client is unavailable. This integration ensures that telephony service reliability is preserved during interruptions in soft client operation.

With the convergence of CS 1000 and Live Communications Server 2005 systems, the Office Communicator 2005 client compliments the voice communications between two users by offering the ability to add other media types, such as video, IM, file and application sharing to an existing voice call without the need to establish an independent session between users.

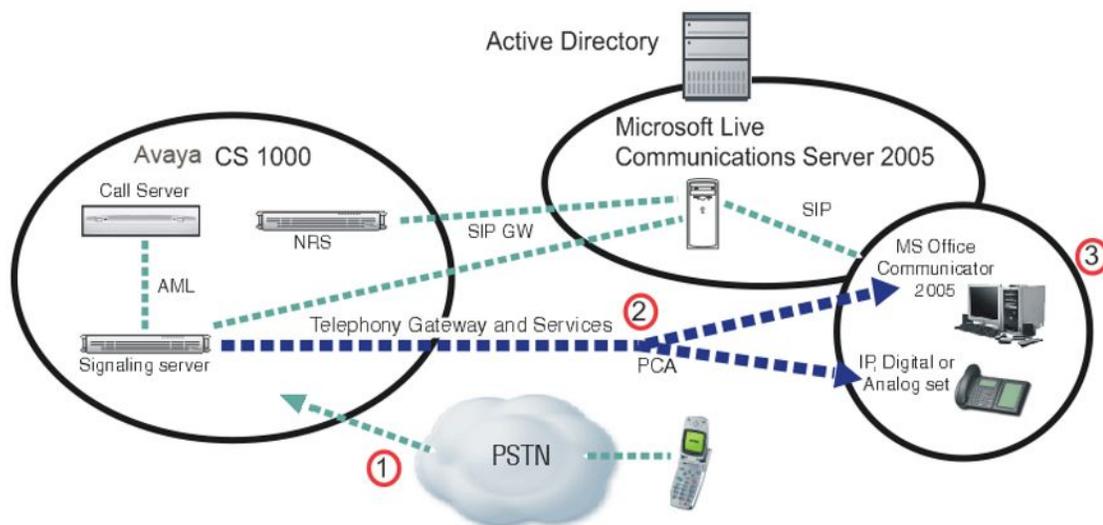
---

## Telephony Gateway and Services

Using the Telephony Gateway and Services component, users can select Microsoft® Office Communicator 2005 as one of the clients they use when handling telephony calls. This feature provides users with Computer to Phone and Phone to Computer connectivity, leveraging the Avaya provided dial plan, telephony infrastructure, and telephony features to make and receive calls using the Microsoft® Office Communicator Client as a soft client.

This solution requires that a Personal Call Assistant (PCA) is configured on the CS 1000 for each user configured with this functionality. A phone is not required for configuration if Office Communicator is available to the user. The CS 1000 configured with the PCA provides number plan translations, Call Detail Recording (CDR) for outgoing calls, and enables telephony features such as Call forward No Answer to Voice Mail, Attendant Recall, and participation as a client in a Group Call for incoming calls.

Using the Telephony Gateway and Services component, Office Communicator 2005 can be configured as a Multiple Appearance Directory Number (MADN) member for users with the Personal Call Assistant (PCA) feature provided by CS 1000. With the PCA feature, calls to a user's phone number can be presented to both the desktop phone and to the Office Communicator 2005 client simultaneously. The user can then choose to answer on the device that makes the most sense at the time.



**Figure 3: Telephony Gateway and Services**

For example, while at the office, a user may decide to use a desktop phone to answer calls. However, the user can still accept calls through Office Communicator while traveling to locations that have network connectivity (for example, at hotels). [Figure 3: Telephony Gateway and Services](#) on page 23 illustrates the following example:

1. The CS 1000 system receives a PSTN call to the user's phone number
2. The CS 1000 uses the Personal Call Assistant (PCA) feature to provide simultaneous ringing to both the user's phone and the Office Communicator voice client
3. The user has the option of answering the call through the CS 1000 phone or the Office Communicator voice client

Consequently, users can be reached no matter where they are on the network and significant cost savings are incurred by using IP telephony through VPN access to their private network.

As part of the user's telephony services, many features of incoming calls are available even when using Office Communicator as a telephony device. Features such as Call Forward No

Answer, Unified Messaging, Call Detail Recording, and Attendant Recall are maintained within the CS 1000 system for calls presented to the Office Communicator.

Another key feature of Telephony Gateway and Services is the ability to access all of the telephony network resources using the Office Communicator client. Calls can originate from the Office Communicator client to the PSTN, phones, or services within the telephony network. Users can therefore access all of their telephony network resources as long as they have the soft client and a high-quality connection to their private network. Telephony Gateway and Services is enabled by the interworking of the CS 1000 SIP Gateway with the Microsoft® Office Live Communications Server 2005 SIP gateway software.

---

## Multimedia Convergence Manager

Avaya also introduces a software component called the Multimedia Convergence Manager (MCM) to ensure the proper interoperability between the two systems with respect to protocols, users, and phone numbers managed within the Microsoft® Active Directory®.

---

## SIP CTI (TR/87) Protocol

The SIP CTI (TR/87) Front End (FE) application introduced with this package is not limited to Microsoft® applications. Through support of the ECMA TR/87 standard, Avaya partners can use this interface to develop SIP CTI capabilities for use with any specification-compliant application.

 **Important:**

Certain portions of the protocol are not supported at this time. Additional information about the SIP CTI (TR/87) protocol is available to Avaya partners upon request.

# Chapter 5: Feature Operation

---

## Contents

This section contains information about the following topics:

- [Remote Call Control functionality](#) on page 27
- [Telephony Gateway and Services functionality](#) on page 41
- [Establishing Multimedia Sessions](#) on page 48

---

## Introduction

This section describes the various features available to users of the Remote Call Control and Telephony Gateway and Services components.

 **Important:**

Customers must NOT use their Microsoft® Office Communicator client to call Emergency numbers (for example, 911). To ensure that emergency service organizations can accurately trace the source of the call, always use a desktop phone to place an emergency call.

---

## Sample configuration

To ensure consistency throughout this document, the following sample user information is used throughout. Unless otherwise indicated, the following SIP and IP information forms the basis of all examples in this document.

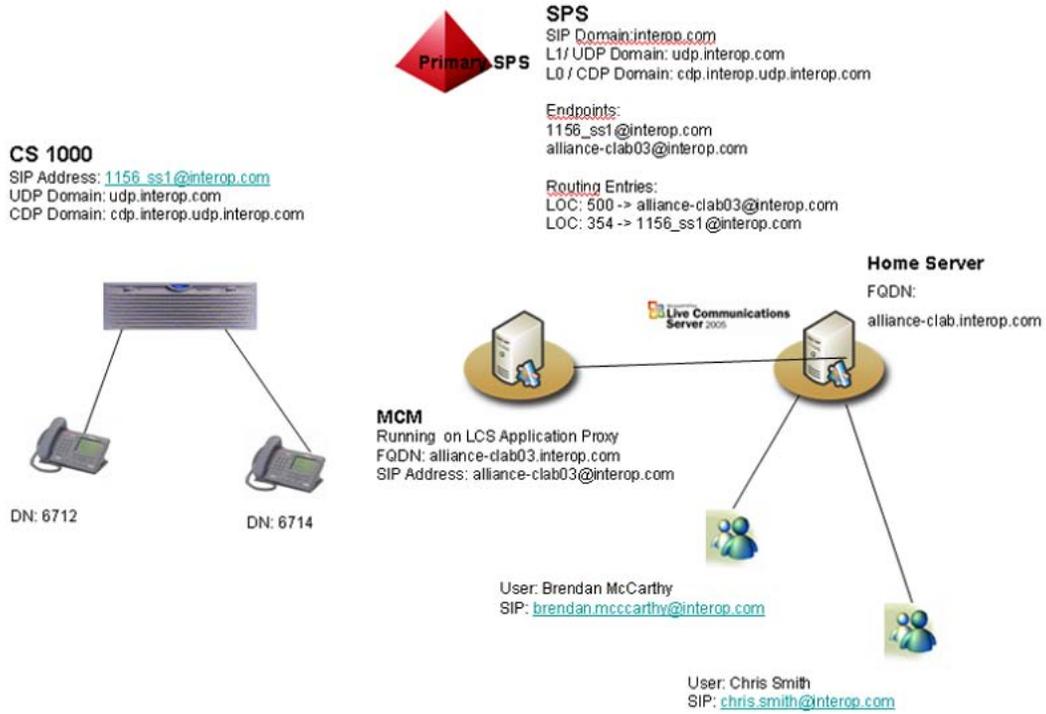


Figure 4: SIP diagram

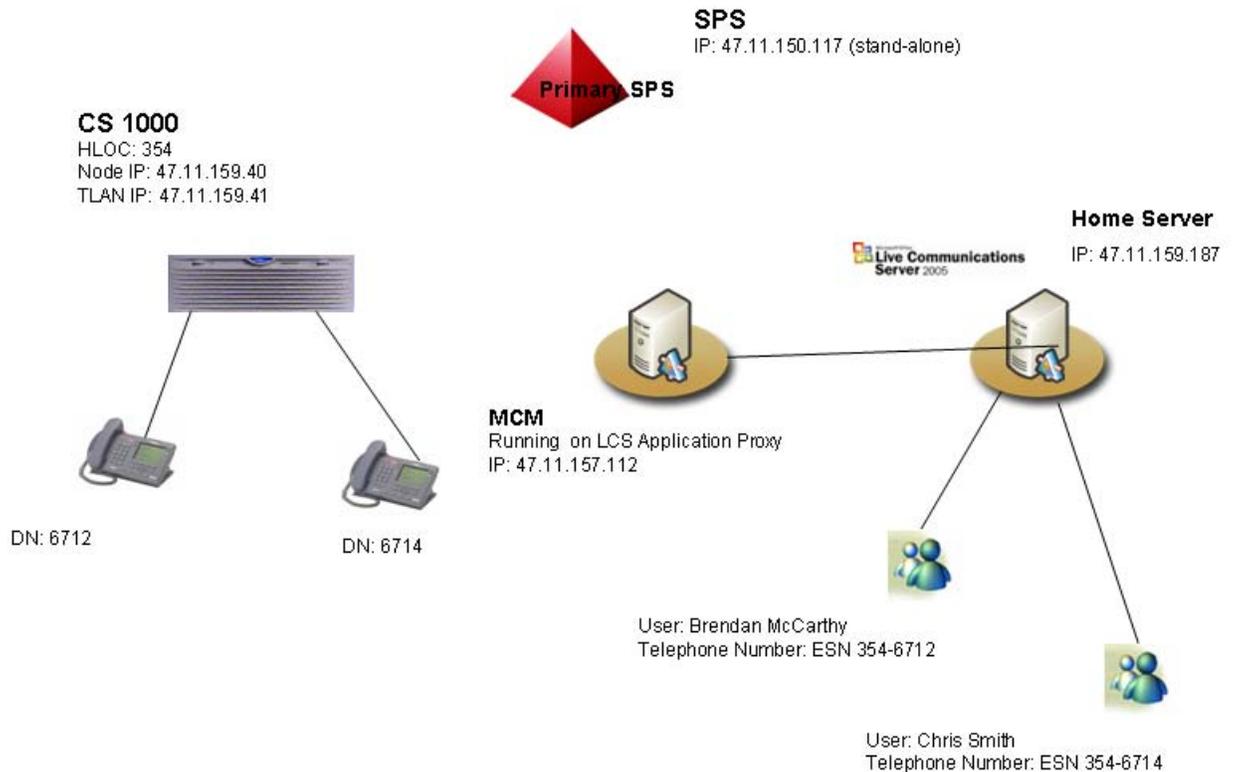


Figure 5: IP diagram

## Remote Call Control functionality

This section provides an overview of the Remote Call Control feature functionality. Microsoft® uses the term Remote Call Control to describe the ability of Microsoft® Office Communicator 2005 to remotely control the features of the phones of an IP PBX, such as the Avaya Communication Server 1000 from within the user interface of Office Communicator or other Microsoft® Office applications.

The Avaya Converged Office product supports Microsoft® Office Communicator Remote Call Control, which integrates Live Communication Server multimedia capabilities (for example, application sharing, instant messaging, and video) with Avaya business-grade telephony through the Avaya CS 1000 system.

The Avaya Converged Office Solution is implemented through an open interface to ensure that any CS 1000 feature supported through Microsoft® Office Communicator is also accessible to applications from other vendors and application developers that support these interfaces.

---

## Microsoft® Office Communicator 2005 features

This section provides an overview of the various Microsoft® Office Communicator 2005 features available through the Remote Call Control with SIP CTI component.

### Make Call

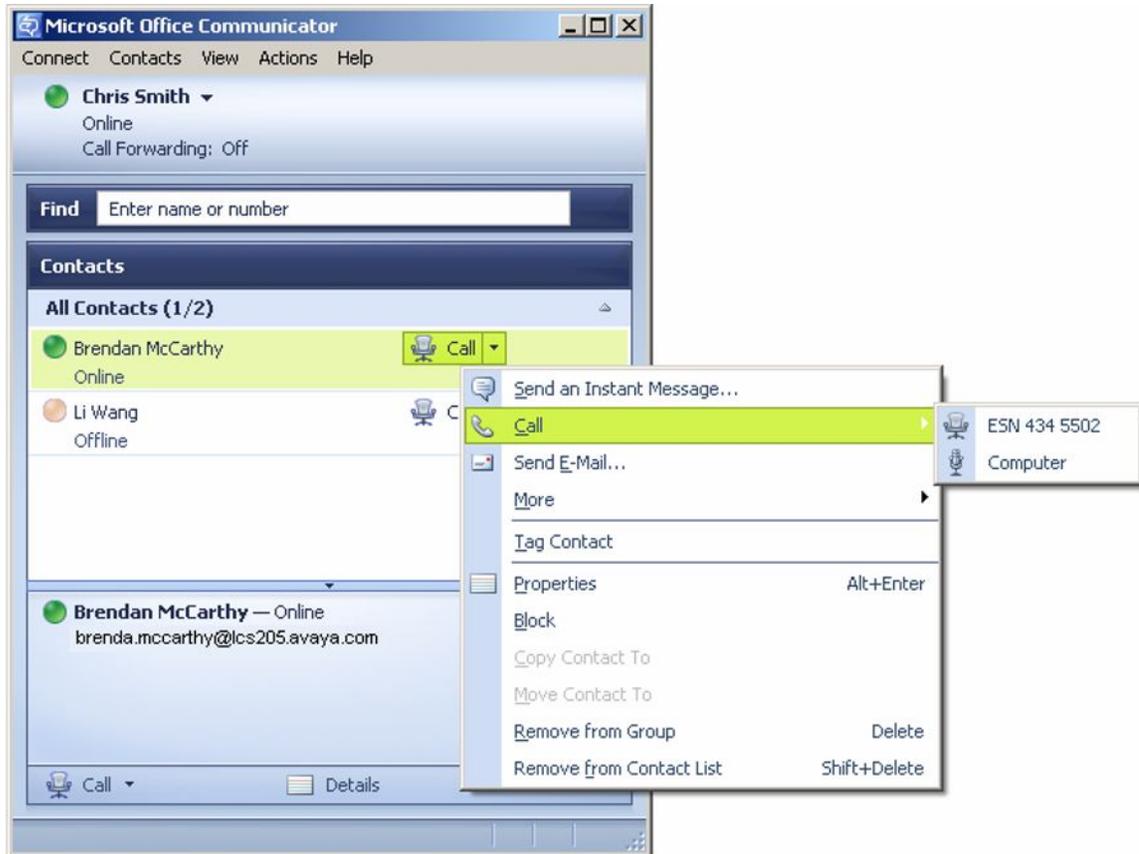
Using the Make Call feature, accessible through the user interface of Office Communicator (see [Figure 6: Make Call From Contact](#) on page 29), users can request that a call be made from their telephony device to a phone number. For example, a user can select the Call function associated with one of their contact icons to make a call from their CS 1000 phone to another user.

When a call is placed through Office Communicator, the default calling device can be either Phone or Computer (see [Figure 20: Default device option](#) on page 44). If you select Phone, Remote Call Control is used to originate the call from the CS 1000 phone. If you select Computer, a SIP (or VoIP) call is originated from the PC itself using a headset or your computer's microphone and speakers.



**Important:**

Remote Call Control is only used for making calls if your default device in the Phones tab is configured to Phone.



**Figure 6: Make Call From Contact**

The Make Call feature creates a new call and initiates a connection with the calling device. The Make Call feature assigns a ConnectionID to the calling device and returns it in positive acknowledgement. While establishing the connection with the calling device, the calling device may also be prompted to go off-hook (if necessary). When it does, either a call is placed to the called device, or the calling device is still in the process of dialing the called device.

The monitored device on-hook default path configuration setting defines whether the headset or hands-free operation is used. For phone types that do not support hands-free (M3905, i2001), it must be noted that in the absence of a headset, the speaker is used as the on-hook default path regardless of the on-hook default path configuration. Due to the absence of a microphone, only half-duplex is supported for the call.

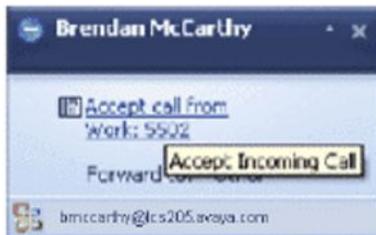
If no speaker is available, Make Call is supported when the phone is off-hook.

In the case of MADN, the Multiple Appearance Redirection Prime (MARP) TN is used as the originating device. The Make Call service request can originate from a number of different user interfaces, such as the Office Communicator 2005 buddy list.

## Answer Call

Using the Answer Call feature, a user can answer an incoming call to their CS 1000 phone by clicking an Accept call pop-up window (see [Figure 7: TR/87 Call Appearance pop-up window](#) on page 30). A user may also start an instant message (IM) session with that caller by clicking the name of the caller in the window rather than accept the call.

For example, a user may receive an Accept call pop-up window, and click on the Accept call link to answer the call. If that same user is too busy to answer the call, they can click the name of the caller in the pop-up window to send the caller an instant message (for example: "Call you back in 10 minutes").



**Figure 7: TR/87 Call Appearance pop-up window**

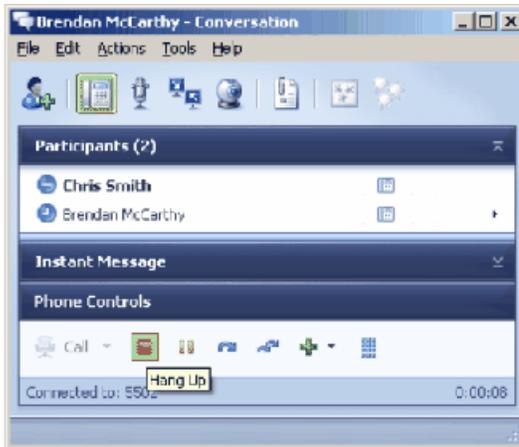
The Answer Call service connects an alerting or queued call. This service is typically associated with devices that have attached speakerphone units and headset telephones to connect to a call using hands-free operation.

The monitored device on-hook default path configuration setting defines whether headset or hands-free operation is used. For phone types that do not support hands-free (M3905, i2001), note that in the absence of a headset, the speaker is used as the on-hook default path regardless of the on-hook default path configuration. Due to the absence of a microphone, this provides only half-duplex support for the call. If no speaker is available, Answer Call is not supported.

Where MADN is used, the MARP TN is used as the receiving device.

## Clear Connection

Use Clear Connection (Release) to hang up from your soft client by clicking the Hang Up button on the user interface (see [Figure 8: Clear Connection UI window](#) on page 31). You can also press the release button on your phone.



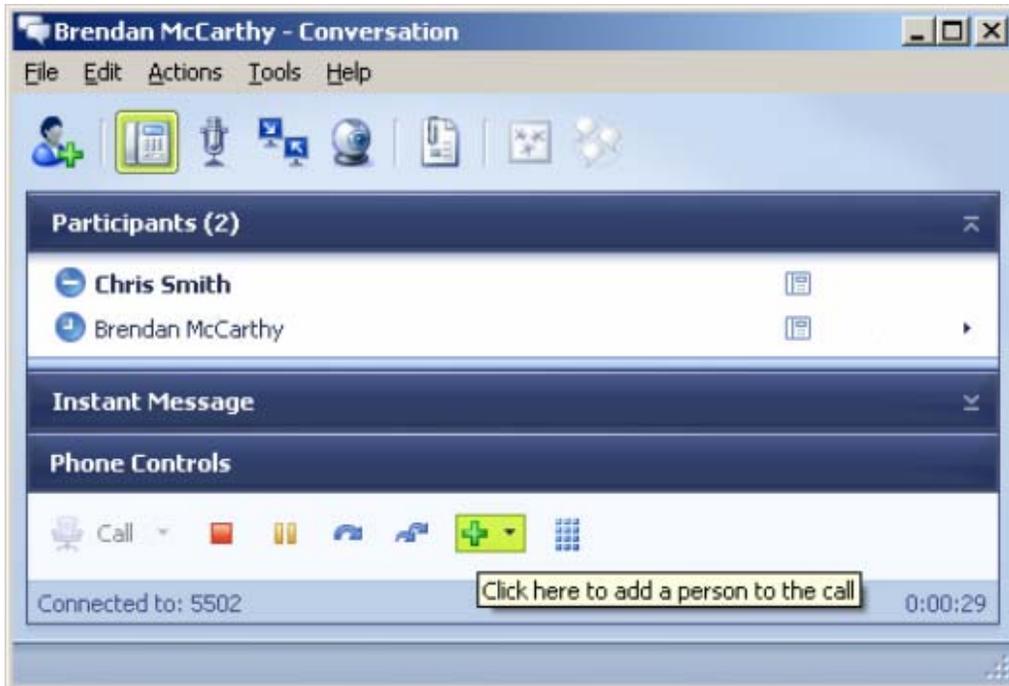
**Figure 8: Clear Connection UI window**

The Clear Connection service releases a specific device from a call. In the case of a two-party call, the call may be torn down. In the case of a conference call, a specific party may be removed from the conference.

The Clear Connection request is sent from the conversation dialog when a call is to be terminated from the client user interface. This is equivalent to pressing the release key on a phone keypad.

## Conference Call

Using the Conference Call service, users can control a conference on their phone through their on-screen interface using Office Communicator 2005 (see [Figure 9: Conference Call UI window](#) on page 32).



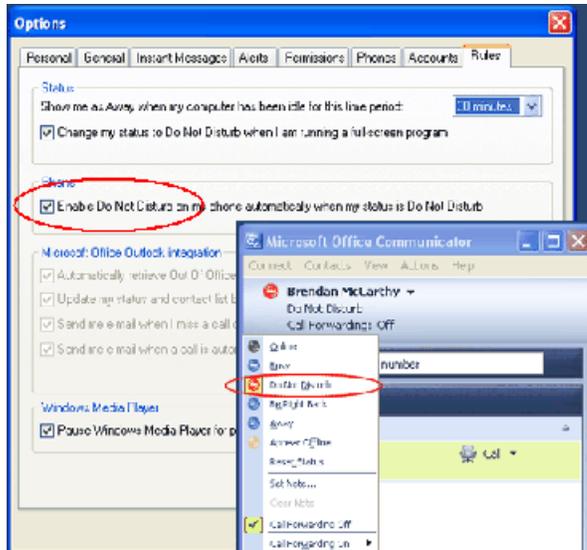
**Figure 9: Conference Call UI window**

This service provides a conference of an existing held call and another active call at a conferencing device. The two calls are merged into a single call, and the two connections at the conferencing device are resolved into a single connection. The Connection IDs formerly associated with the conferenced connections are released, and a new Connection ID for the resulting connection is created. The existing held call may consist of two or more devices.

The use of the Conference Call service requires that an A03 or A06 key be configured on the TN where the CLS T87A resides. The conference service request is sent from a conversation dialog to add a caller to the existing call. These keys may be part of the default configuration.

## Do Not Disturb

To enable the Do Not Disturb feature, the Make Set Busy key must be enabled on the phone and the “Enable Do Not Disturb” option must be selected in Office Communicator (see Do Not Disturb). The Do Not Disturb feature enables the Make Set Busy key on a call by call basis. As a result, incoming calls are directed to a user’s voicemail or receive a busy signal.



**Figure 10: Do Not Disturb**

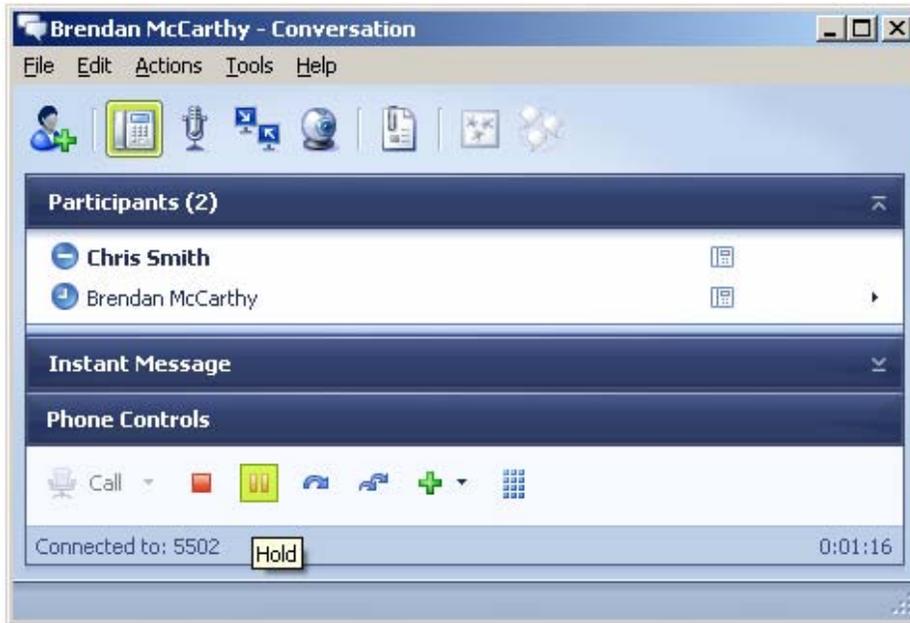
To completely avoid being disturbed by any incoming call to a user's phone and Office Communicator, including computer calls from other Microsoft Office Communicator clients and calls from other phones, the user must configure the status of Office Communicator to "Do Not Disturb." Also, the checkbox "Enable Do Not Disturb on my phone automatically when my status is Do Not Disturb" must be selected in the Rules tab of the Options window, as shown in [Figure 10: Do Not Disturb](#) on page 33.

If the status of Office Communicator is not configured to "Do Not Disturb," and the associated telephone has "Make Set Busy" enabled, the user will still receive a popup window from an incoming call in the following scenarios:

- Computer call from Office Communicator: in this scenario, one popup window for a computer call is shown.
- Telephony Gateway call where the associated DN is a MADN: in this case, two popup windows are shown and the user can choose to answer it either through Office Communicator or the phone. Actually, if the user is configured to support the Telephony Gateway call, the associated DN must be a MADN, as a PCA with the same DN is required.
- User is not configured to support the Telephony Gateway call: in this scenario, one popup window is shown when the associated DN is a MADN.

## Hold Call

The Hold Call service places a connected call on hold at the same device. This service interrupts communication for an existing call at the device. Essentially, this is equivalent to pressing the Hold key on a phone. In this case, however, the hold button is part of the Office Communicator 2005 interface (see [Figure 11: Call Hold UI window](#) on page 34).

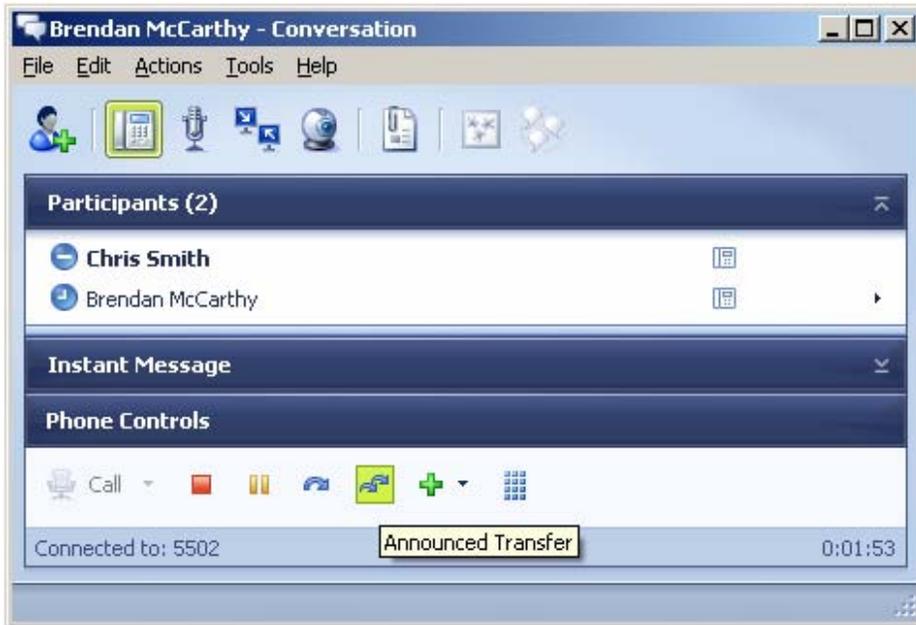


**Figure 11: Call Hold UI window**

Consistent with the behavior when initiated from a phone, a call on hold cannot be disconnected. The Hold Call service request is sent from the conversation dialog when a call is put on hold.

## Transfer Call

The Transfer Call service transfers a call held at a device to an active call at the same device. The held and active calls at the transferring device are merged into a new call. For example, you receive a call that might be better handled by a coworker. By clicking the Transfer Call button, the caller is placed on hold while you call the number of the coworker to whom you are transferring the call.



**Figure 12: Transfer Call UI window**

The connections of the held and active calls at the transferring device become Null and their ConnectionIDs are released (in other words, the transferring device is no longer involved with the call).

The use of the Transfer Call feature requires that a TRN key be configured on the TN where the CLS T87A resides. This key may be part of the default telephone configuration.

The Transfer Call service request is initiated from the conversation dialog when a call is to be transferred to another DN through the use of a consultation call.

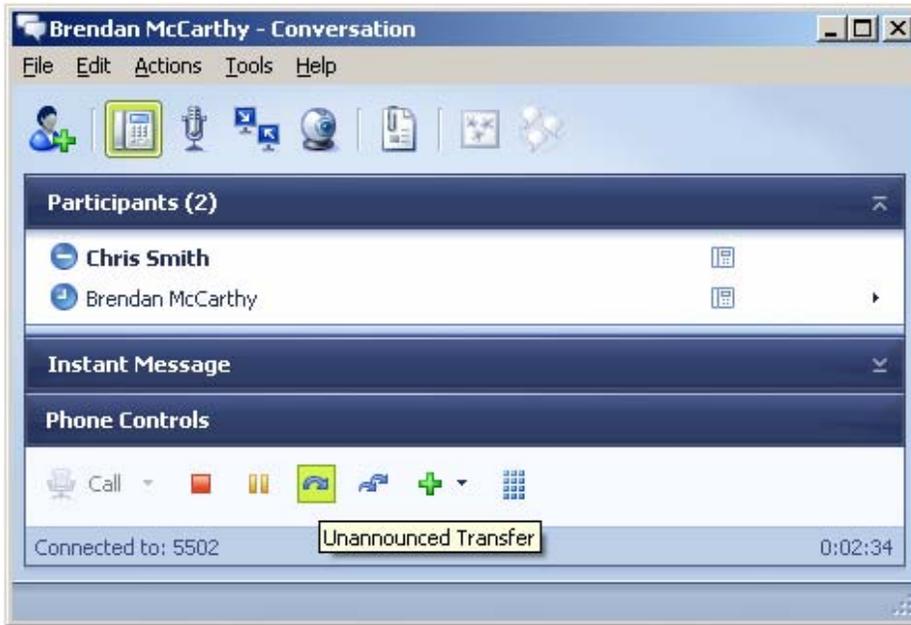
## Single Step Transfer Call

The Single Step (Blind) Transfer Call service (also known as Unannounced Transfer, see [Figure 13: Single Step Transfer UI window](#) on page 36) transfers an existing connection at one device to another device. This transfer is performed in a single step to prevent the device performing the transfer from placing the existing call on hold.

The transferring connection may be in the Alerting, Connected, Failed, Held, or Queued state.

### **Important:**

If a user has been configured with a phone number that has not been registered in the NRS, blind transfers to that user will fail if the user is in Computer mode. The user will only receive blind transfers if they are in Phone mode.



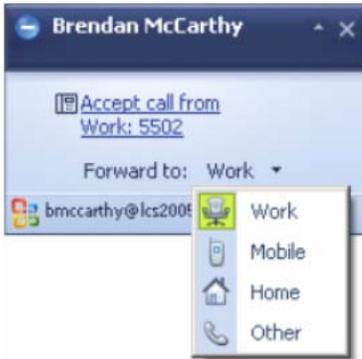
**Figure 13: Single Step Transfer UI window**

The use of this feature requires that a TRN key be configured on the TN where the CLS T87A resides.

The single step transfer call service request is initiated from the conversation dialog when a call is to be transferred directly to another DN. This is equivalent to the blind transfer function available from a phone.

## Deflect Call

Using the Deflect Call feature, users can forward an incoming call in its ringing state to a number of their choosing. For example, a user may have their work phone number programmed in Office Communicator so it is in the drop-down list in the pop-up window (see [Figure 14: Deflect Incoming Call](#) on page 37).



**Figure 14: Deflect Incoming Call**

Using the Deflect Call service, a user can divert a call to another destination that may be inside or outside the switching subdomain.

The Deflect Call service request is sent from the incoming call notification pop-up when an alternative destination is selected. This function is currently not available from the phone, and can be accessed only through the Office Communicator 2005 client. The deflect call service request is also used to implement the location-based forwarding service from Office Communicator 2005.

The deflect service request is supported for all call types. The deflect behaves as though the called device was configured with call forward to the target number. If a deflect fails, the call remains with the currently alerting device and the user is notified of the failure (see [Figure 15: Call Deflect Failure](#) on page 37).



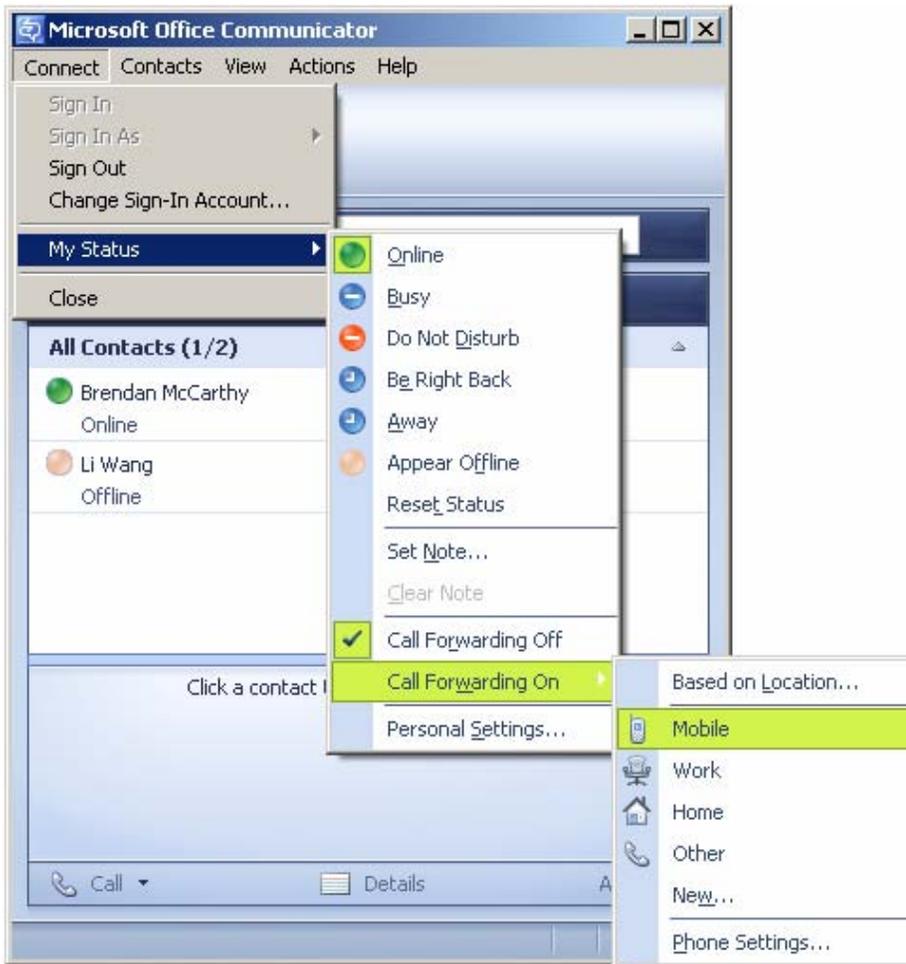
**Figure 15: Call Deflect Failure**

## Call Forwarding

There are two methods of call forwarding. Users can forward all calls by selecting Call Forwarding On (see [Figure 16: Call Forwarding](#) on page 38), and then select the number to which they want to forward calls.

The Call Forwarding service allows the computing function to control the forwarding feature at a specified device based on user-defined conditions. The forwarding feature is used to redirect calls that arrive at a specified device to an alternative destination.

Only one user-specified setting (the forwarding type and forward-destination combination) can be changed per service invocation.



**Figure 16: Call Forwarding**

The Call Forwarding service request is sent from Office Communicator 2005 when the call forwarding option is enabled. You can enable this option from a number of different locations within Office Communicator 2005. This function is equivalent to pressing the CFWD key on a phone.

This feature has a limitation. Refer to the section “Feature Limitations” for details.



**Warning:**

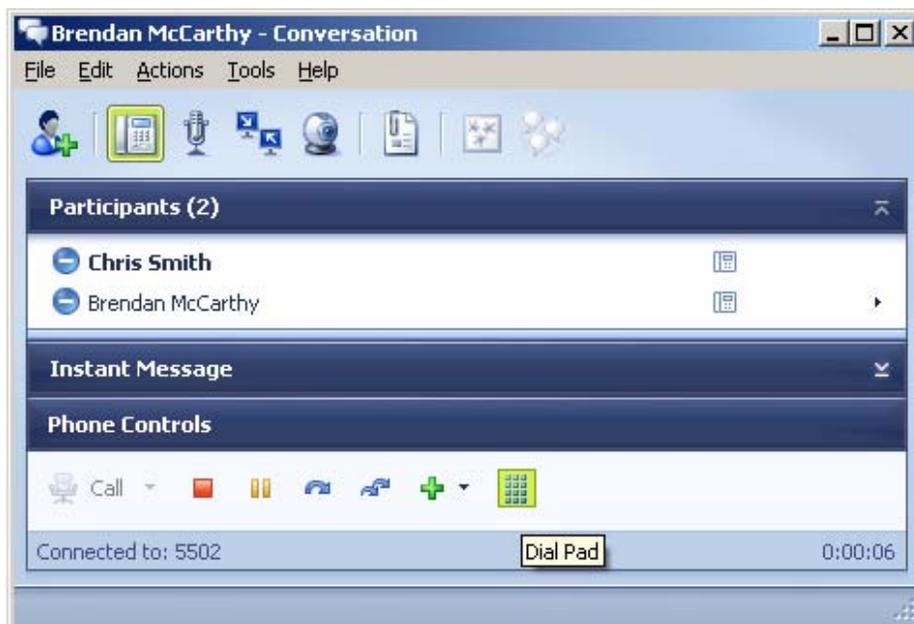
Microsoft® Office Communicator does not reflect call forward state changes made to the CS 1000 phone itself. When Office Communicator is active and controlling a DN, all Call Forward

changes must be made through Office Communicator to ensure that it is in the correct state.

When a user signs into Live Communications Server from their Office Communicator client, the forwarding status saved within Office Communicator overrides any forwarding status that may be configured from the phone. For example, if forwarding is off within Office Communicator, it is turned off following sign in, regardless of the phone forwarding status at the time.

## Generate Digits

The Generate Digits feature provides users with a keypad to enter phone numbers on their computer screen (see [Figure 17: Generate Digits](#) on page 39).



**Figure 17: Generate Digits**

The Generate Digits service causes a series of digits to be sent on behalf of a connection in a call. The digits may be sent in the form of Dual-tone Multifrequency (DTMF) tones. This service also:

- supports optional parameters to control digit generation
- generates end-to-end information that is to be sent to a device in a call (for example, not to address or select a device)
- does not affect the state or progress of a call
- supports analog, digital, and IP phone types and all trunk types

### **!** Important:

When both ends support RFC2833, the digits are sent out-of-band.

There is one scenario, however, that is not supported: when the originating and terminating endpoints are IP Phones. At this time, no known usage scenarios exist where this service is required between two IP Phones.

Within a service request, the characters 0 to 9, the pound sign (#), and the asterisk (\*) are supported. You can insert a pause into the dialstring by using a comma (,). Up to 31 characters to be dialed are supported within a single service request.

The Generate Digits service request is sent to Office Communicator 2005 from the toolbar on the conversation dialog. This function is equivalent to pressing digits on the dial pad of a phone during a call (for example, to access voice mail or a conference bridge).

---

## Contact Icons

The Remote Call Control component also provides, through the use of contact icons, the ability to call users directly from various Microsoft® Office applications (see [Figure 18: Contact icon](#) on page 40) such as Outlook, Excel, and Word.

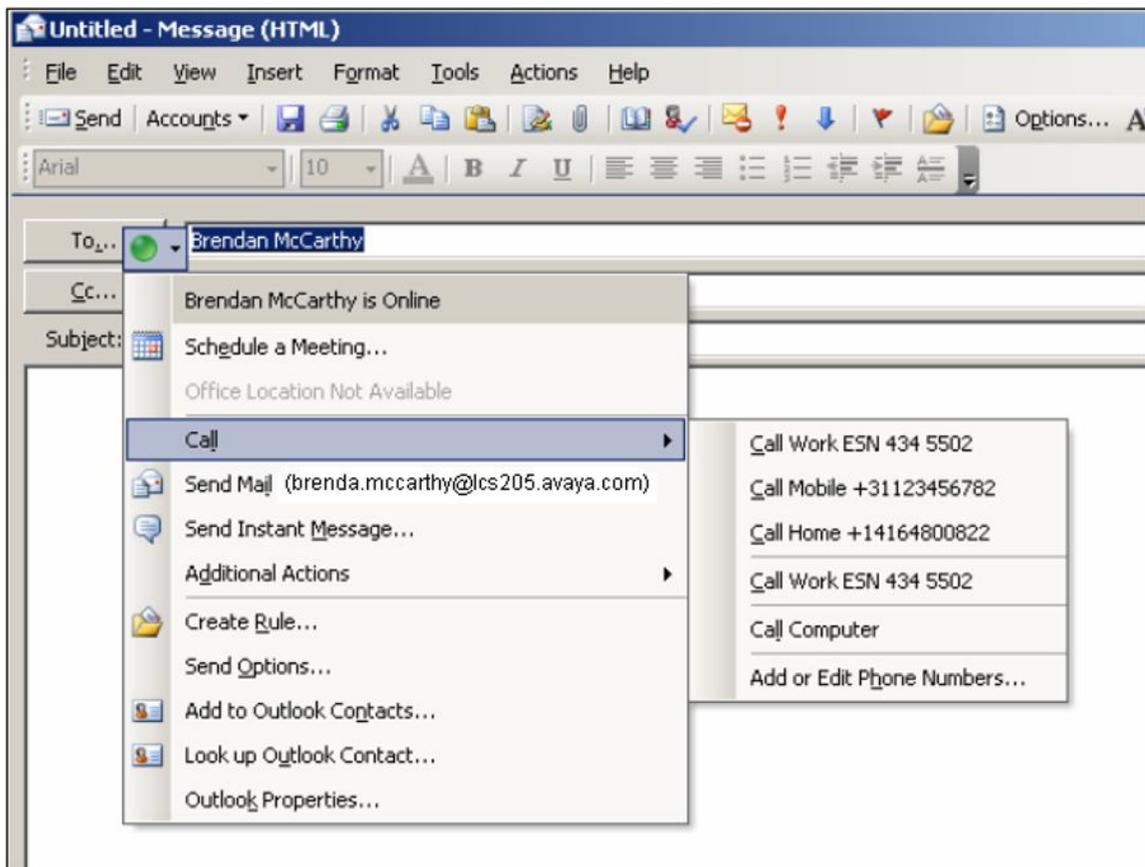


Figure 18: Contact icon

---

## Telephony Gateway and Services functionality

The ability to connect between computers and phones is not natively provided by Microsoft® Office Live Communications Server 2005; however, the Telephony Gateway and Services component enables this functionality using the SIP gateway and Multimedia Convergence Manager (MCM) application.

With Telephony Gateway, users can choose how calls are made and received. For outgoing calls, users can make a call from their Office Communicator soft client instead of their CS 1000 phone. Incoming calls can be handled in one of two ways: through the computer, with Office Communicator, or through a phone.

---

### CS 1000 Services

Many of the features provided by CS 1000 to traditional telephones are extended to Office Communicator clients configured with the Personal Call Assistant (PCA). For example, calls that remain unanswered may be forwarded using the "call forward - no answer" feature.

---

### PCA

If a user wants to use the Office Communicator soft client for some of their voice calls using the Telephony Gateway and Services, a PCA must be configured with the same DN as the user in a MADN arrangement. This offers incoming voice calls to the user's DN on their Office Communicator, as well as any phones that they have configured with the same DN.

For outgoing calls from the Office Communicator, the user must have at least one TN configured on a CS 1000 Call Server. The MCM locates the Call Server associated with a user by their numbering plan entry in the NRS. This generates calls from Office Communicator clients using Telephony Gateway and Services to always tandem through the user's active Call Server.

 **Important:**

With Geographic Redundancy features, a user's active Call Server may change during failure scenarios.

The Network Class of Service (NCOS) setting for outgoing calls from Office Communicator clients is determined by the configuration of the MARP TN when in a MADN group, or by the configuration of the PCA when it is the only TN for the user.

With PCA and Remote Call Control configured, users receive a pop-up window for the incoming call to their phone and a second pop-up for their computer. Users can then choose the most convenient way to answer an incoming call.

---

## MCM

Multimedia Convergence Manager (MCM) serves a number of functions, including:

- translation between telephony phone numbers and user IDs within Active Directory
- authentication of user phone numbers
- Numbering Plan normalization
- protocol interworking
- redundant connections to the CS 1000 network components (SRS, SPS, and redundant Signaling Servers)

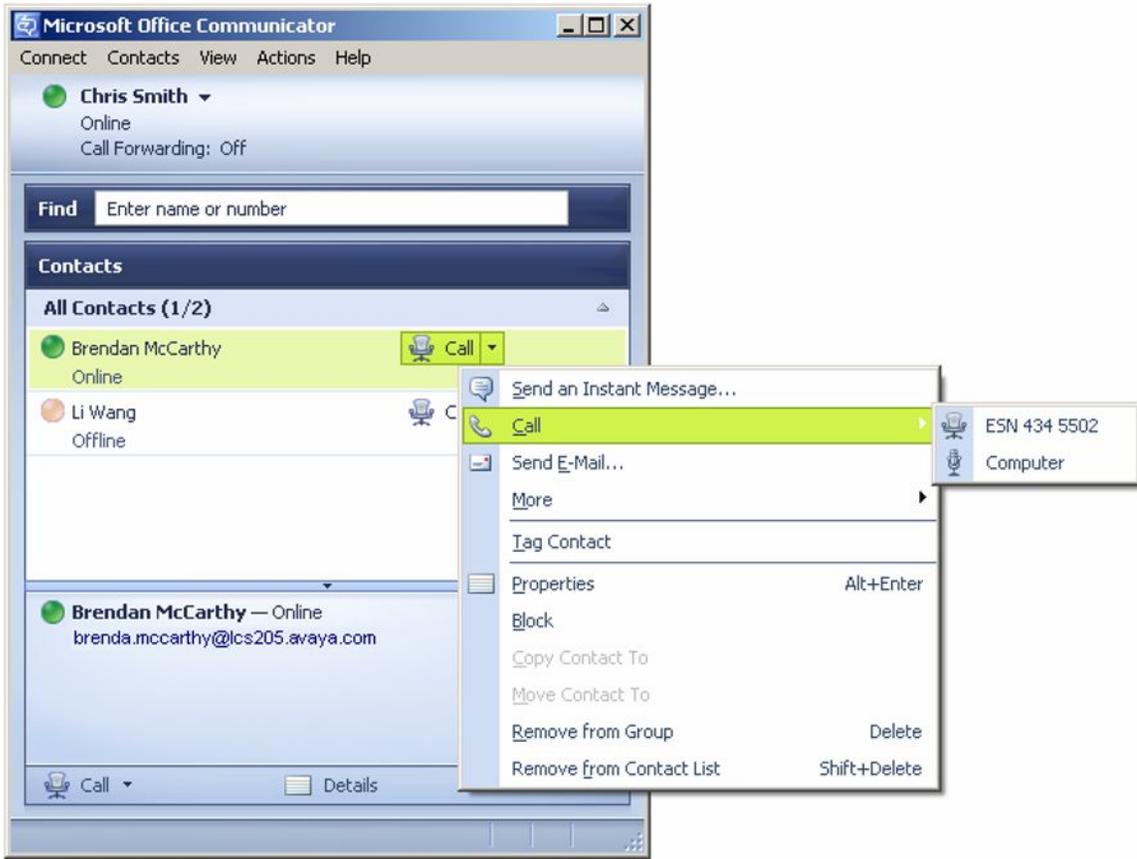
---

## Microsoft® Office Communicator 2005 features

This section provides an overview of the various Microsoft® Office Communicator 2005 features available through the Telephony Gateway and Services component.

### Make Call

Using the Make Call feature, available from the user interface of Office Communicator (see [Figure 19: Make Call From Contact](#) on page 43), users can request that a call be made from their telephony device to a phone number. For example, a user can select the Call function associated with one of their contact icons to make a call from their CS 1000 phone to another user.



**Figure 19: Make Call From Contact**

When a call is placed through Office Communicator, the default calling device can be either Phone or Computer. If you select Phone, Remote Call Control is used to originate the call from the CS 1000 phone. If you select Computer, a SIP (or VoIP) call is originated from the PC itself using a headset or your computer's microphone and speakers.

Configure this option by selecting the **Actions > Options > Phones** tab (see [Figure 20: Default device option](#) on page 44).

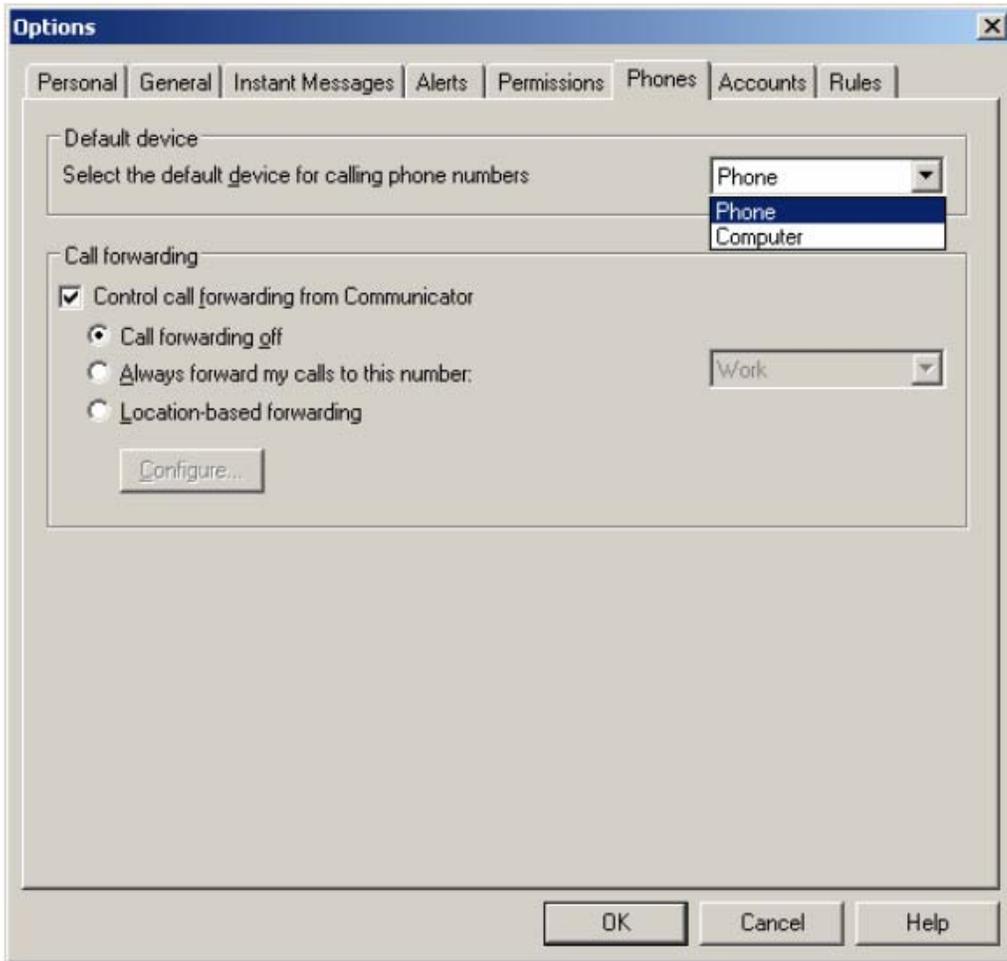


Figure 20: Default device option

## Answer Call

Using the Answer Call feature, the user can answer an incoming call in one of two ways: through Remote Call Control of the CS 1000 phone clicking an Accept call pop-up window (as shown in the second pop-up in [Figure 21: PCA Call Appearance pop-up window](#) on page 45), or through their computer.

With PCA enabled, users can accept calls to their computer. Selecting the Accept Computer call pop-up with the microphone icon allows users to answer the call as a computer, or VoIP, call on the PC itself.

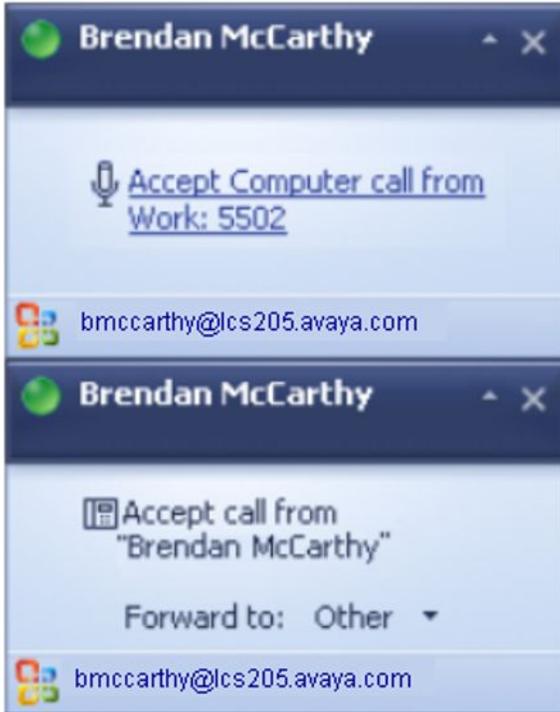


Figure 21: PCA Call Appearance pop-up window

## Clear Connection

Using the Clear Connection (Release) feature, users can hang up from their soft client by clicking the Hang Up button (see [Figure 22: Clear Connection window](#) on page 46).

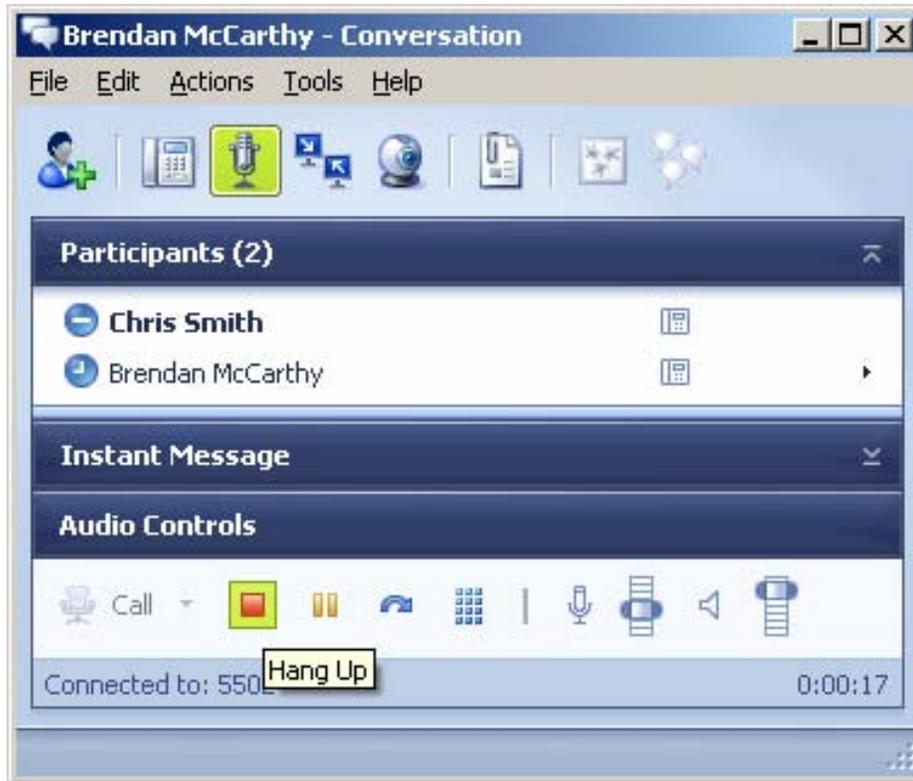


Figure 22: Clear Connection window

## Hold Call

The Hold Call feature places a connection on hold at the same device. Clicking the Hold button once (see [Figure 23: Call Hold window](#) on page 47) puts the call on hold and clicking the Hold button again restores the audio connection.

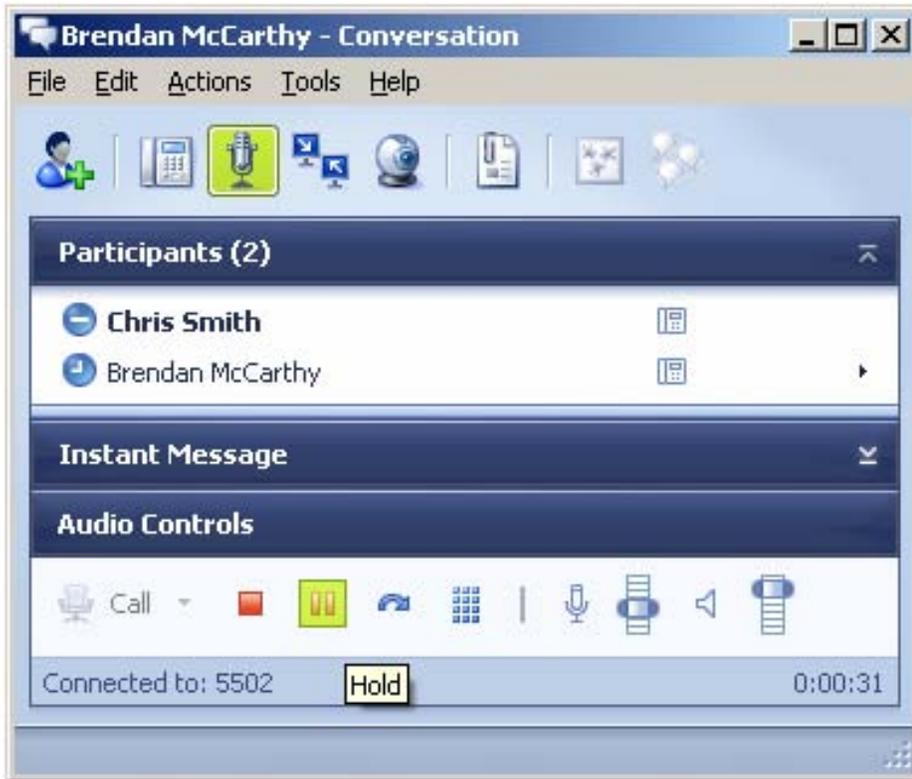


Figure 23: Call Hold window

## Single Step Transfer Call

The Single Step (Blind) Transfer Call feature transfers an existing connection at one device to another device in a single step. The device performing the transfer does not place the existing call on hold before transferring the connection.

### ! Important:

If a user has been configured with a phone number that has not been registered in the NRS, blind transfers to that user will fail if the user is in Computer mode. The user will only receive blind transfers if they are in Phone mode.



**Figure 24: Single Step Transfer window**

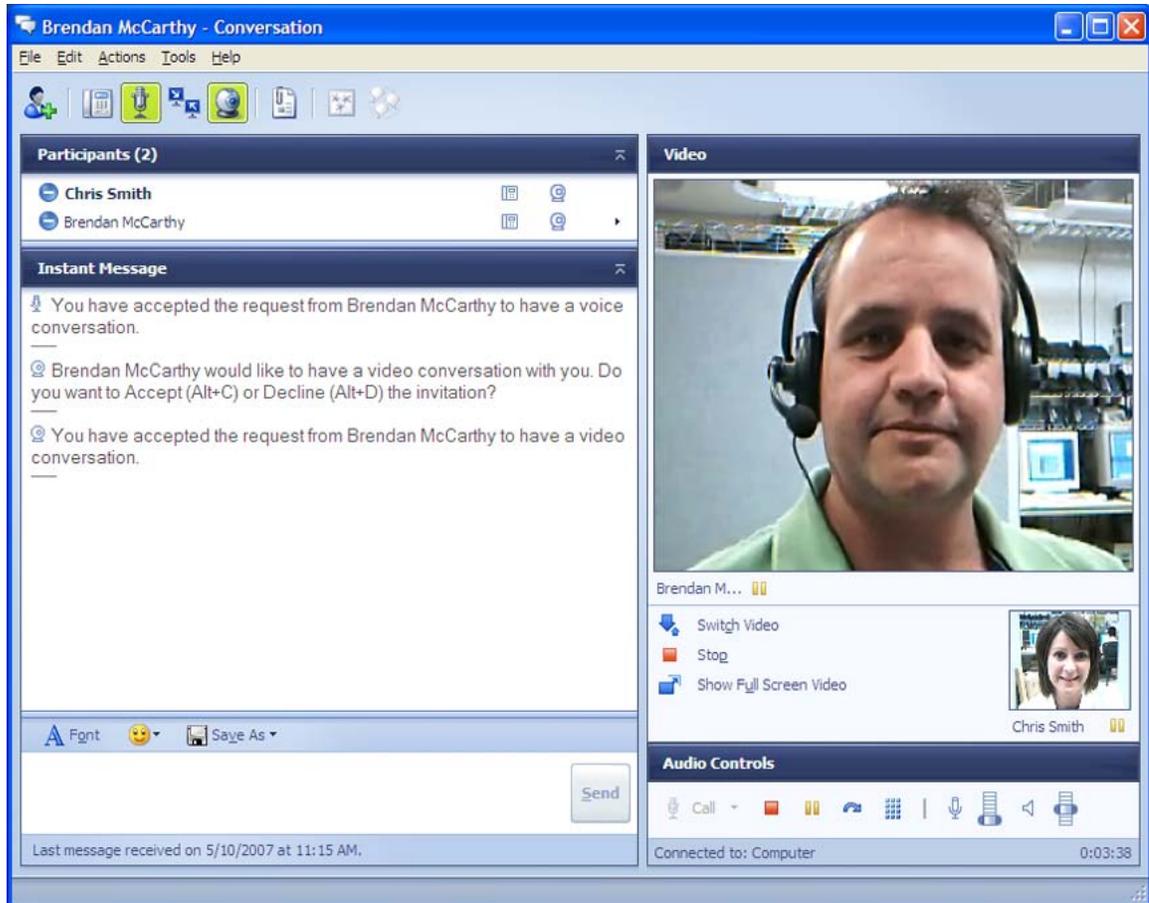
For Office Communicator SIP calls, Office Communicator 2005 supports "blind" no-hold transfers exclusively. For example, if computer A establishes a voice conversation with phone B, and computer A then transfers the call to phone C, the call is immediately presented to phone C.

Computer A cannot retrieve the call or talk to phone C, as the call releases from computer A when the call is presented to phone C. If phone C is busy or unavailable, the call terminates.

---

## Establishing Multimedia Sessions

All Live Communications Server multimedia features are immediately available for use on the corresponding call dialog when the phone number for an active call is resolved to a Live Communications Server user identity by Office Communicator. This applies to both Remote Call Control and Telephony Gateway and Services calls.



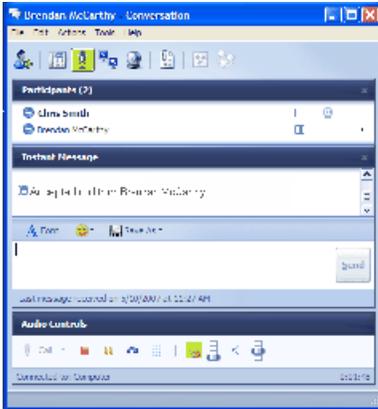
**Figure 25: Multimedia session**

For information on the process used to map phone numbers to Live Communications Server user identities from either SIP or TR/87 call events, refer to [Normalizing phone numbers](#) on page 167.

---

## Video calls

Video is supported for SIP CTI Office Communicator to SIP CTI Office Communicator calls or SIP Gateway Office Communicator to SIP Gateway Office Communicator calls.



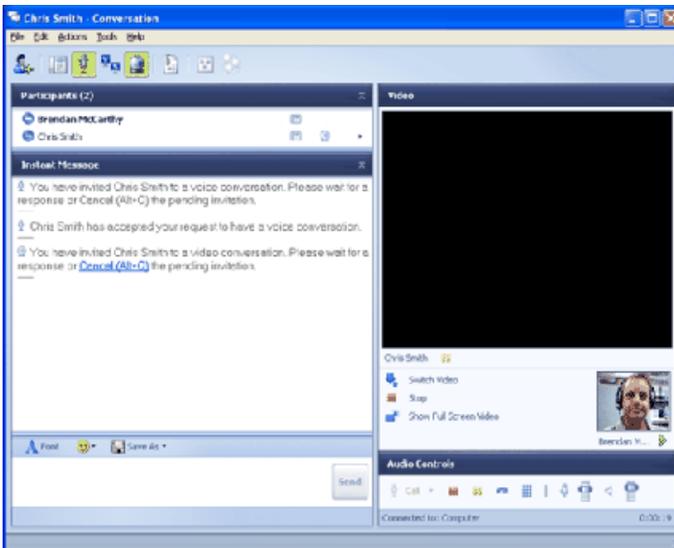
**Figure 26: Starting a video call**

By using Office Communicator as the actual phone instead of controlling the desktop phone, video calls are established by first establishing an active audio call between Office Communicator clients. Both endpoints must be using Office Communicator as a softphone (SIP Gateway). After the audio call is established, click the camera icon (see [Figure 26: Starting a video call](#) on page 50) to initiate a video call. The following screen appears ([Figure 27: Establishing video](#) on page 50):



**Important:**

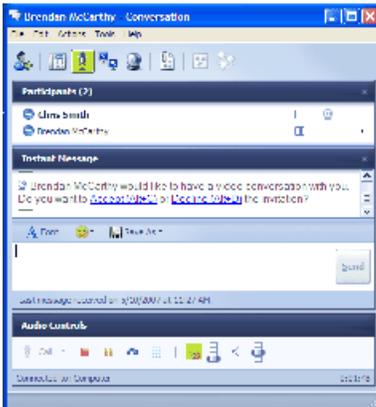
A SIP Gateway Office Communicator to SIP Gateway Office Communicator call must be established as an audio call only to a phone number before adding video.



**Figure 27: Establishing video**

In this example, Brendan invites Chris to join a video call, and is waiting for a reply. At this point, the main screen is blank, and Brendan's image appears in the lower right hand corner.

On the other end of the call, Chris receives a request to accept or decline the video call (see [Figure 28: Video call request](#) on page 51).



**Figure 28: Video call request**

When Chris accepts the request, a two-way video call is initiated (see [Figure 29: Video calls \(two-way video\)](#) on page 52). Chris sees you in the larger screen, while Chris appears in the smaller screen in the lower right section of the window. At this point, both audio and video are going to Office Communicator.

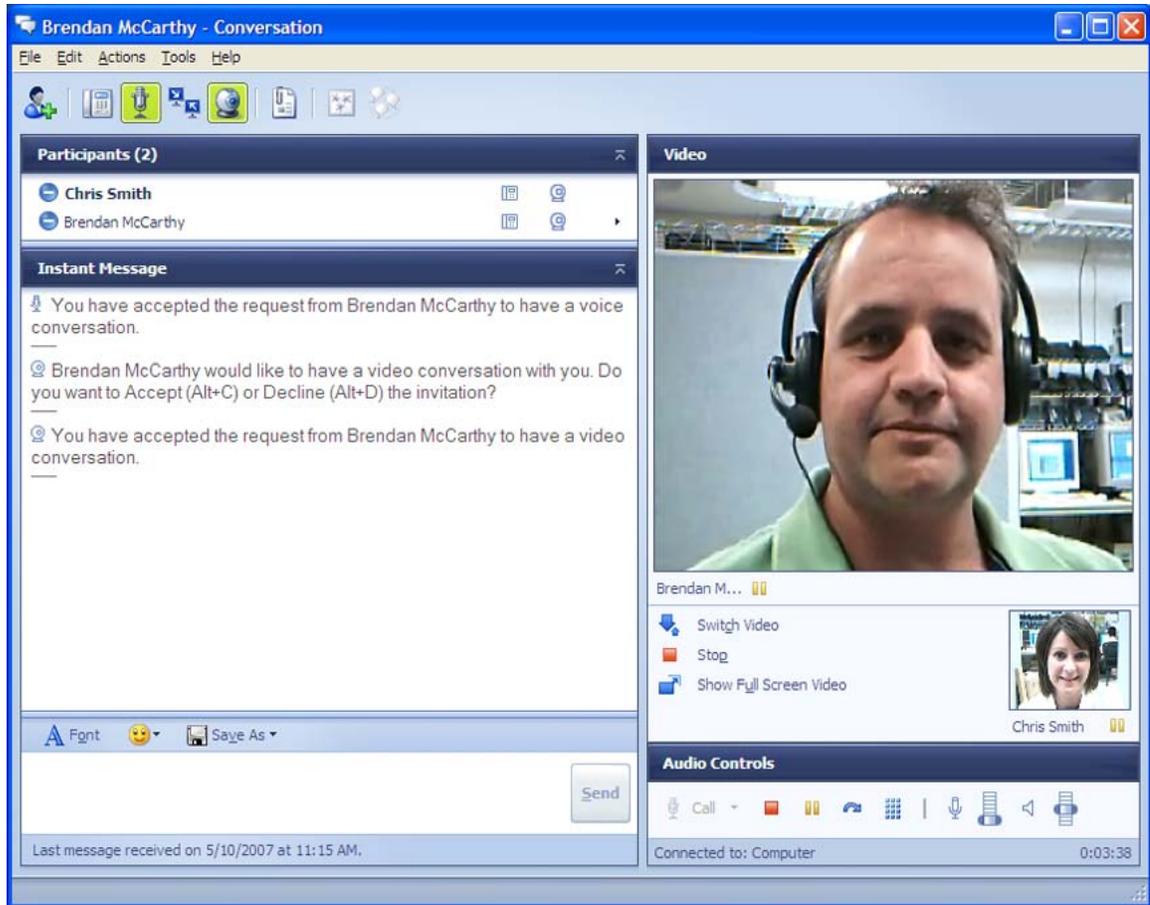


Figure 29: Video calls (two-way video)

# Chapter 6: Planning and Engineering

---

## Contents

This section contains information about the following topics:

- [Introduction](#) on page 53
- [Network Design](#) on page 54
  - [Small network](#) on page 54
  - [Medium network](#) on page 55
  - [Large network](#) on page 56
- [General Recommendations](#) on page 63
  - [Trunking](#) on page 67
  - [Security Considerations](#) on page 70
  - [Dial Plan Considerations](#) on page 73
- [Telephony Gateway and Services](#) on page 77
  - [Capacity](#) on page 77
  - [Redundancy](#) on page 77
  - [SIP routing](#) on page 78
  - [Feature Limitations](#) on page 79
- [Remote Call Control with SIP CTI](#) on page 86
  - [Capacity](#) on page 90
  - [Redundancy](#) on page 92
  - [Feature limitations](#) on page 94

---

## Introduction

Before you install and configure Avaya Converged Office, a number of issues must be addressed regarding network size and its impact on the type of software and hardware used.

Also, because each Converged Office component has its own unique set of installation and configuration considerations, issues exist that are related specifically to both Remote Call Control with SIP CTI and Telephony Gateway and Services.

 **Important:**

In this chapter, and the one that follows, Telephony Gateway and Services is presented first, followed by Remote Call Control. During the implementation phase, it is recommended that the Telephony Gateway and Services component be implemented first to provide basic connectivity, (which can be more readily debugged), followed by Remote Call Control for more complex feature operation. Configuring both Telephony Gateway and Remote Call Control is only necessary in situations where both components are required. The Telephony Gateway and Services component is not required in situations where Remote Call Control is the only required component.

---

## Network Design

The first consideration when you plan and engineer the Converged Desktop is the size of the network. Networks can be divided into three main categories: small, medium, and large, with each type requiring specific configurations.

The following sections describe typical network topologies you might consider depending upon your capacity and robustness requirements.

 **Note:**

The descriptions and graphical representations of the three network types are for illustration only, and are not intended to be actual configurations. The actual number of Avaya Communication Servers 1000 and Live Communications Servers will be based on the engineering guidelines found in this document and those provided by Microsoft®.

 **Note:**

Throughout this document, Live Communications Server 2005 Front End Enterprise Edition refers exclusively to Live Communications Server 2005 with Service Pack 1 (SP1).

---

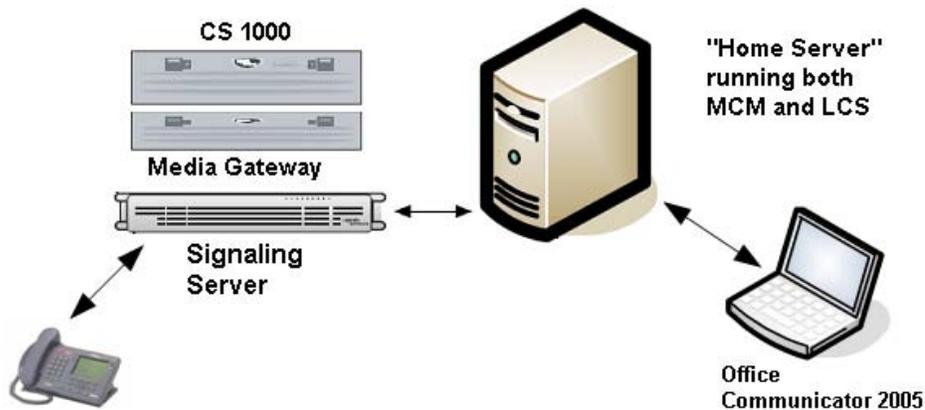
## Small network

Small networks require only a basic configuration, where MCM and Live Communications Server co-reside on the same Home Server. This configuration is recommended for small organizations that do not require redundancy.

 **Note:**

The recommended deployment requires that MCM reside on a separate Live Communications Server Application Proxy server; however, this is not required for small

networks. [Figure 30: Small network configuration](#) on page 55, shows a typical Home Server configuration.



**Figure 30: Small network configuration**

For small networks consisting of less than 500 users, you can install and operate Live Communications Server 2005 Standard Edition on a minimal hardware configuration. This configuration is not supported for large deployments or for the Enterprise Edition. The minimal hardware aligns with recommendations for hardware for Windows Server 2003 Standard Edition.

---

## Medium network

A medium network may require the following components:

- multiple Avaya CS 1000 systems with Media Gateway and Signaling Server
- a Primary NRS with an Alternate NRS (co-residing on one of the Signaling Servers)
- Live Communication Server 2005 Standard Edition
- a Live Communication Server Proxy running MCM (the recommended deployment requires that MCM reside on a separate Live Communications Server Proxy server)

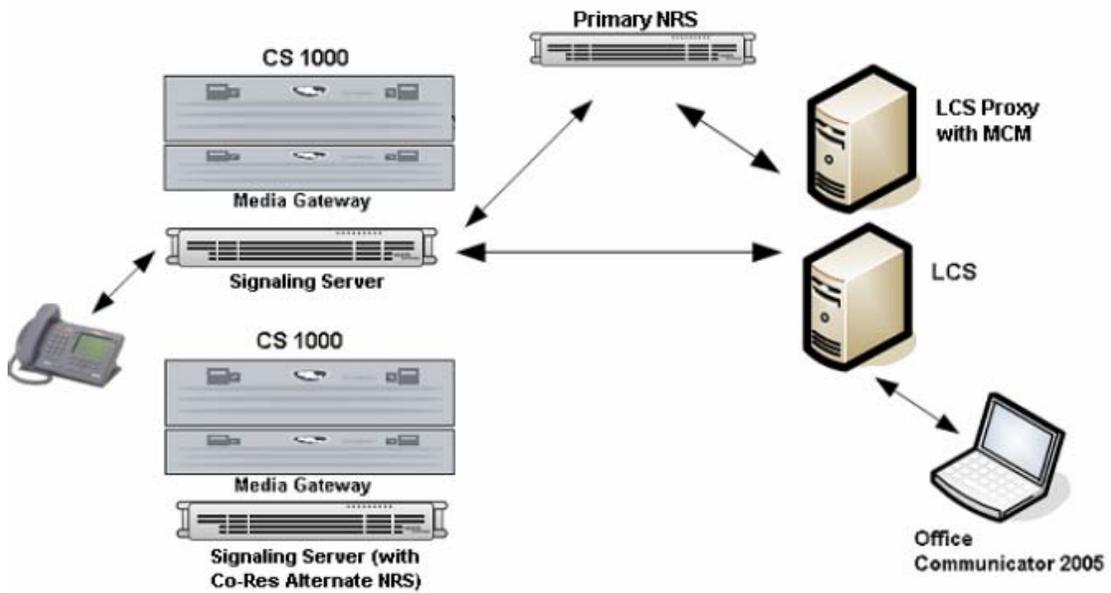


Figure 31: Medium network configuration

**! Important:**

SPS (Linux-based NRS) does not support co-residency.

---

## Large network

A large network may require the following components:

- multiple CS 1000 systems with Media Gateway and Signaling Server
- redundant Primary and Alternate NRS
- Live Communication Server 2005 Enterprise Edition (EE) with SP1 with a load balancer to front end the pool of Enterprise Edition Servers
- redundant Live Communication Server Proxies running MCM (the recommended deployment requires that MCM reside on a separate Live Communications Server Application Proxy server)
- multiple networks of CS 1000 systems can be configured using collaborative NRS

**! Important:**

If you are running the Enterprise Edition of Microsoft Live Communications Server 2005, you must use a load balancer even if only one server exists in the pool—per the Unified Communications Engineering Rules and Guidelines.

The load balancer ensures that the FQDN of the pool is not equal to the FQDN of any home server in the pool.

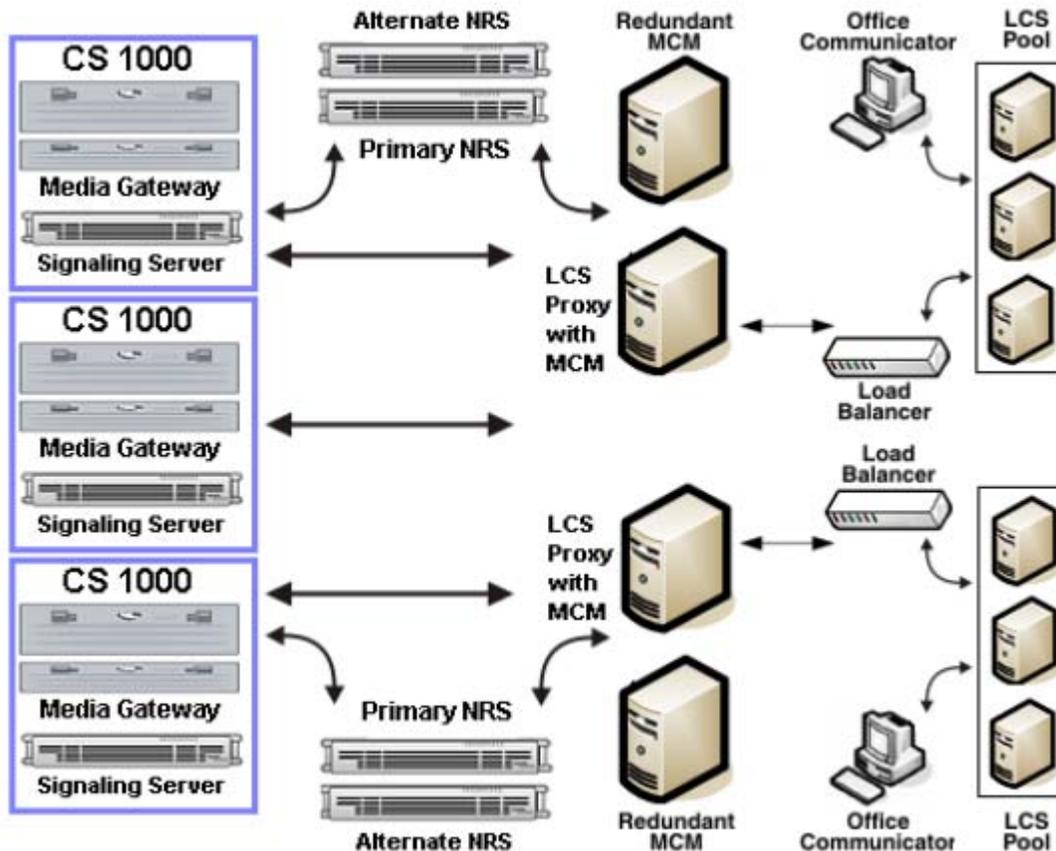


Figure 32: Large network configuration

**\* Note:**

The redundant, primary, and alternate NRS can be either the VxWorks NRS or the Linux-based NRS (SPS/SRS).

**\* Note:**

Microsoft requires, for Enterprise Edition, an SQL server as part of the network.

## Load Balancer

Hardware IP Load Balancers (for example, Avaya Application Switches) are required for Live Communications Server 2005 Enterprise Edition deployments. The Load Balancer exposes a single virtual IP (VIP) address to clients to prevent direct access to individual Live Communications Server Enterprise Edition Servers. The Load Balancer uses a metric (for example, round robin, or fewest connections) to route new client requests to the Live Communications Servers.

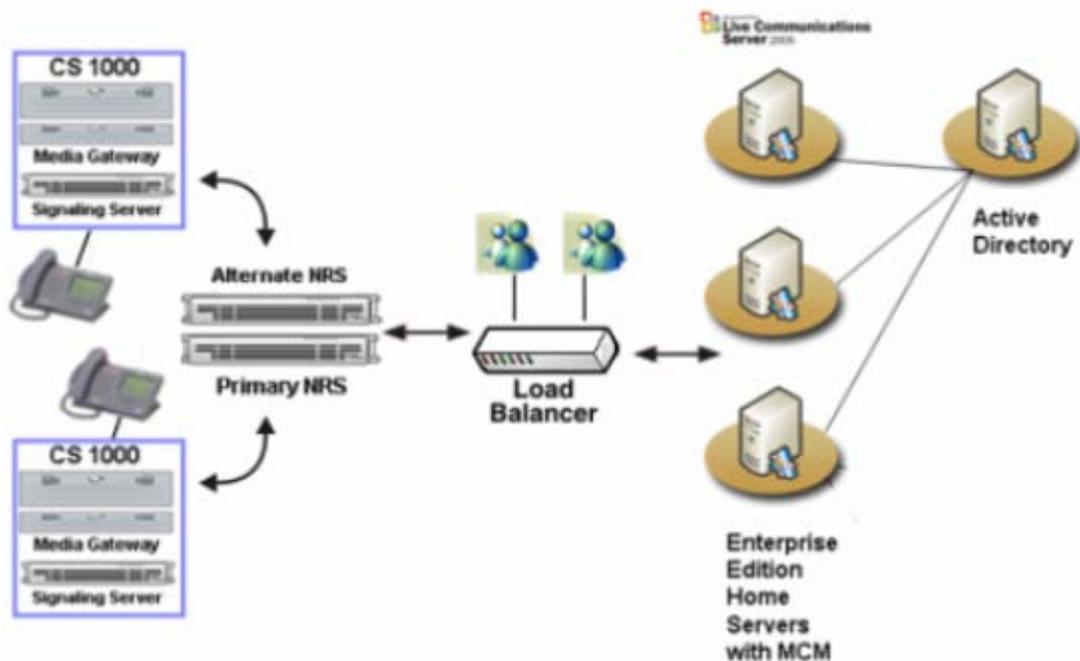
The Load Balancer can be configured in a number of ways depending on whether a Live Communications Server Application Proxy is deployed.

For more information about deployment of small, medium, and large networks, as well as Load Balancer requirements, refer to *Live Communications Server 2005 with SP1 Deployment Overview* from the Microsoft® site:

<http://office.microsoft.com/en-us/communicationsserver/default.aspx>

### Using a Load Balancer between a pool of Enterprise Edition LCS Home Servers pool running MCM and the CS 1000

It is possible to add redundancy to your network by placing a Load Balancer, such as an Avaya Application Switch, between a pool of Live Communications Server Home Servers and the CS 1000. The role of this Load Balancer is to balance SIP invites from the CS 1000 to the LCS Home Servers (which are part of Enterprise Edition pool). This load balancer is also used for the CS 1000. From the Home Servers, all SIP Invites are sent directly to the NRS and redirected to the appropriate CS 1000. This configuration is depicted in [Figure 33: Single Load Balancer](#) on page 58.



**Figure 33: Single Load Balancer**

In order for the Load Balancer to work correctly, the following conditions must be met:

1. The Load Balancer meets all the criteria for a Load Balancer specified by Microsoft®. For more information, refer to: <http://office.microsoft.com/en-us/communicationsserver/default.aspx>
2. The Load Balancer can handle the balancing of TCP IP traffic.
3. The Live Communications Server Home Servers adds the Virtual IP (VIP) address of the Load Balancer as well as all CS 1000 as Authorized Hosts.

4. The NRS has the Virtual IP (VIP) of the Load Balancer configured as a static entry. All dialing plan entries are redirected to the Virtual IP address of the Load Balancer.
5. The MCM application running on all Home Servers must use the NRS.

### **Using a Load Balancer between the LCS Home Server and Live Communications Server Application Proxy**

It is possible to add redundancy to your network by placing Load Balancers such as an Avaya Application Switch, between the Live Communications Server (LCS) Home Servers and Live Communications Server (LCS) Application Proxy.

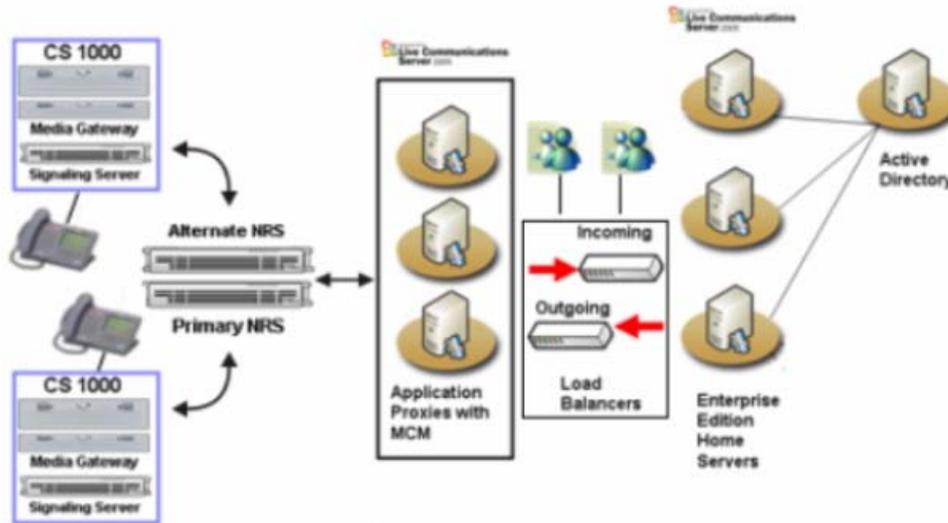
The configuration depicted in [Figure 34: Redundancy with Load Balancers](#) on page 60 shows two Load Balancers. An Outgoing Load Balancer and an Incoming Load Balancer.

The role of the Outgoing Load Balancer is to balance SIP invites from the Home Servers to the Application Proxy. From the Home Servers, all SIP Invites are sent to the Virtual IP (VIP) of the Outgoing Load Balancer. The Load Balancer then sends the SIP Invite to the least busy Live Communications Server Application Proxy.

The role of the Incoming Load Balancer is to balance SIP invites from the Application Proxy to the least busy Home Server. This is the same load balancer that is used when the office communicator addresses the pool for registration. The Application Proxy is configured to send all SIP invites to the Virtual IP (VIP) of the Incoming Load Balancer.

Redundancy is also ensured for calls to an Office Communicator user by having each LCS Application Proxy register to the MCM with a unique Registration ID and different cost factor. Therefore, if one of the LCS Application Proxy Servers is unavailable, the next one is selected.

It must be noted that the Outgoing and Incoming Load Balancers are viewed as two separate logical devices but can be one physical device configured to behave as two Load Balancers.



**Figure 34: Redundancy with Load Balancers**

In order for the Load Balancer to work correctly, the following conditions must be met:

Deployments with incoming Load Balancer only (TLS):

1. The Load Balancer meets all the criteria for a Load Balancer specified by Microsoft®. For more information, refer to: <http://www.microsoft.com/office/livecomm>
2. TLS transport is used, exclusively, for all connections between Live Communications Server Home Servers and the Live Communications Server Application Proxy.
3. The route added on the Live Communications Server Home Servers routes to the FQDN of the Live Communications Server Application Proxy using TLS.
4. The route added on the Live Communications Server Application Proxy routes to the FQDN of Live Communications Server pool.
5. The Live Communications Server Pool of Home Servers add the FQDN of the Live Communications Server Application Proxy Server as Authorized Hosts.
6. The Live Communications Server Application Proxy adds the FQDN of Live Communications Server pool as Authorized Hosts.

Deployments with incoming Load Balancer only (TCP):

1. The Load Balancer meets all the criteria for a Load Balancer specified by Microsoft®. For more information, refer to: <http://www.microsoft.com/office/livecomm>
2. TCP transport is used, exclusively, for all connections between Live Communications Server Home servers and the Live Communications Server Application Proxy.
3. The route added on the Live Communications Server Home Servers routes to the IP address of the Live Communications Server Application Proxy using TCP.

4. The route added on the Live Communications Server Application Proxy routes to the Virtual IP (VIP) address of incoming Load Balancer using TCP.
5. The Live Communications Server Pool of Home Servers add the IP address of the Live Communications Server Application Proxy Server and VIP address of incoming Load Balancer as Authorized Hosts.
6. The Live Communications Server Application Proxy adds the IP addresses of all Live Communications Server Home Servers as Authorized Hosts.

Deployments with incoming and outgoing Load Balancers (TCP):

1. The Load Balancer meets all the criteria for a Load Balancer specified by Microsoft®. For more information, refer to: [www.microsoft.com/office/livecomm](http://www.microsoft.com/office/livecomm)
2. TCP transport is used, exclusively, for all connections between Live Communications Server Home servers and the Live Communications Server Application Proxy
3. The route added on the Live Communications Server Home Servers routes to the VIP address of outgoing Load Balancer using TCP.
4. The route added on the Live Communications Server Application Proxy routes to the VIP address of incoming Load Balancer using TCP.
5. The Live Communications Server Pool of Home Servers add the IP address of the Live Communications Server Application Proxy Server as Authorized Hosts.
6. The Live Communications Server Application Proxy adds the IP addresses of all Live Communications Server Home Servers as Authorized Hosts.

Deployments with incoming and outgoing Load Balancers (TLS):

1. The Load Balancers meet all the criteria for a Load Balancer specified by Microsoft. For more information, see <http://www.microsoft.com/office/livecomm>.
2. The Live Communications Server Home Servers use certificates issued to the FQDN of the incoming Load Balancer. For more information, refer to the Microsoft Office Live Communications Server 2005 Certificate Configuration document at <http://office.microsoft.com/en-us/products/FX011526591033.aspx>.
3. The Live Communications Server Application Proxies use certificates issued to the server FQDN with the FQDN's of the server and the outgoing Load Balancer as the Subject Alternate Name. For more information, refer to the Microsoft Office Live Communications Server 2005 Certificate Configuration document at <http://office.microsoft.com/en-us/products/FX011526591033.aspx> and follow the steps as for a Director array.
4. TLS transport is used exclusively for all connections between Live Communications Server Home servers Pool and the Live Communications Server Application Proxies.
5. The route added on the Live Communications Server Home Servers' Pool routes to the FQDN of the outgoing Load Balancer using TLS.
6. The route added on each of the Live Communications Server Application Proxies routes to the FQDN of incoming Load Balancer using TLS.

7. The Live Communications Server Pool of Home Servers adds the FQDN of the outgoing Load Balancer as Authorized Host.
8. The Live Communications Server Application Proxies add the FQDN of the incoming Load Balancer as Authorized Host.

Deployments with mixed transport types (TCP in one direction and TLS in other):

Not supported

### **Microsoft Live Communications Server (LCS) Load balancing using Avaya Application Switch (NAS):**

Additional load balancer configuration information is available on the Avaya site. Use the following procedure to access this information.

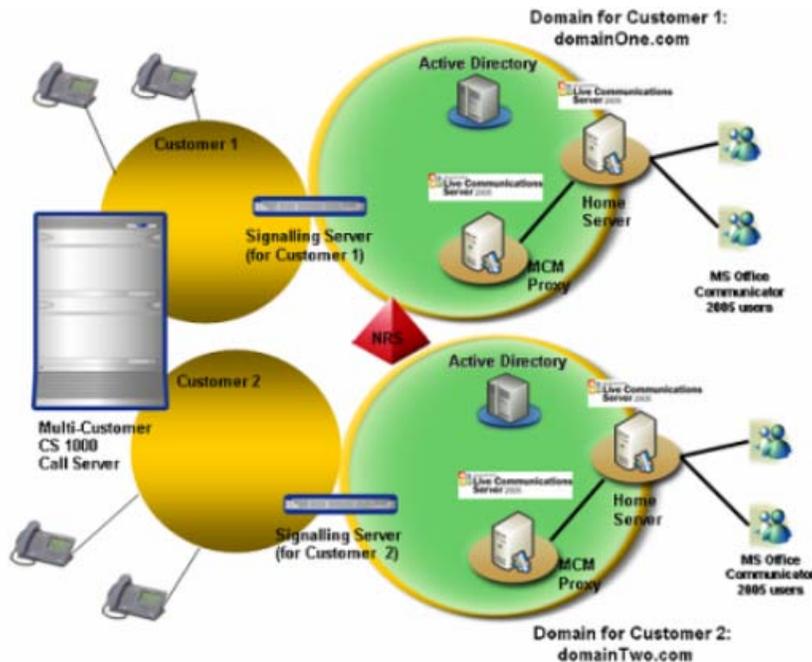
#### **Accessing Load Balancer information**

1. Open Internet Explorer.
2. Enter [www.avaya.com](http://www.avaya.com) as the URL.
3. Under Support, select Documentation.
4. Under Documentation, Software, and Bulletins, select Content Networking.
5. Under Application Switches, select Application Switch 2208.
6. Under Documentation, select Operations.
7. Select Microsoft Live Communications Server (LCS) Load Balancing Using Avaya Application Switch Installation/Configuration Guide from the list of available documents.

## **Multiple Customer Network**

A common feature in the Hosted Solution market, the CS 1000 can be configured with a number of customers. In this configuration, each of the customers on the CS 1000 have their own set of phones, trunks, features, restrictions, and numbering plans. In the Converged Office environment, as with the CS 1000 in general, each customer is treated as separate machine. Each customer has their own Node Number, Signalling Server, and SIP domain. For more information about the Multiple Customer environment, see Avaya Communication Server Features and Services (NN43001-106)

[Figure 35: SIP Gateway-only Network or SIP Gateway and SIP CTI Network](#) on page 63 provides an example of a Multiple Customer network. The figure shows two customers: Customer 1 and Customer 2, each with their own set of associated phones and Signalling Server(s). This type of configuration is required for any deployment that uses the Telephony Gateway and Services functionality, or in scenarios where both Telephony Gateway and Services and Remote Call Control functionality is deployed.



**Figure 35: SIP Gateway-only Network or SIP Gateway and SIP CTI Network**

The Signalling Server(s) for Customer 1 are in the domainOne.com domain. For each customer, a separate Live Communications Server domain must be configured. The Live Communications Server domain used by Customer 1 is in the same domain as the Signalling Server(s) domainOne.com. Each Live Communications Server domain requires its own Active Directory.

The only equipment shared by Customer 1 and 2 is the Call Server and the NRS. The NRS can only be shared by the two customers if it is configured with both domainOne.com and domainTwo.com.

The Signalling Server(s), Live Communications Server Application Proxy (which runs MCM), Live Communications Server Home Server, and Active Directory are completely separate. The number of Signalling Server(s), Live Communications Server Application Proxy, and Live Communications Server Home Servers required for each customer are the same as they would be if each customer were part of a single system. However, the total number of users allowed for the Call Server is the total number of users for all customers.

---

## General Recommendations

The following sections describe in detail the recommended platform for deploying Live Communications Server 2005.

---

## Operating System Required

Microsoft® Windows Server™ 2003 is the required operating system for Live Communications Server 2005 with SP1.

### Live Communications Server 2005 running MCM

MCM must be loaded on a Live Communications Server Application Proxy or the home server.



**Important:**

An Application Proxy is NOT an Access Proxy.

### Live Communications Server 2005 Standard Edition

- Dual Intel Xeon 3.06 GHz, 1-MB Cache, 533 MHz FSB (front side bus)
- 2-GB DDR (double data rate), 266 MHz RAM
- 2 × 18-GB hard disks (15,000 rpm SCSI)
- 100-megabit network adapter
- Windows Server 2003, Standard Edition
- MSDE 2000 Service Pack 3a
- At least two disk drives are required for optimal performance: one for the database and the other for the database transaction log.



**Important:**

Although Live Communications Server 2005 Standard Edition is compatible with Microsoft® Virtual Server 2005, it is not supported as part of the Avaya Converged Office feature. The Avaya software component Multimedia Convergence Manager (MCM) must not be installed on a Live Communications Server running Microsoft® Virtual Server 2005. For additional information about Virtual Server 2005, visit the Virtual Server Web site at: <http://www.microsoft.com/windowsserversystem/virtualsever/default.mspx>

### Live Communications Server 2005 Enterprise Edition Server

For each role of server that is part of the Live Communications Server 2005 Enterprise Edition, a low-end and a high-end hardware specification is provided.

A range is provided to accommodate the range of customer deployments that is supported:

- Low-end hardware supports between 0 to 50,000 clients.
- High-end hardware supports between 50,000 to 125,000 clients.

The low-end and high-end server platforms have different performance characteristics.

In general, a low-end computer does not mix with high-end computers in a deployment. An exception is components that are placed in the perimeter network (such as an Access Proxy) that provide service to a small percentage of the overall user base and, therefore, might make use of a lower-end computer while the remainder of the intranet deployment would contain higher-end computers.

## Configuration for an Enterprise Pool

The following shows the recommended hardware configuration for Live Communications Server 2005, Enterprise pool.

- Dual Intel Xeon 3.06 GHz, 1-MB Cache, 533 MHz FSB
- 2-GB DDR, 266 MHz RAM
- 2 × 18-GB hard disks
- 100-megabit network adapter
- Windows Server 2003, Standard Edition
- For deployments in excess of 50,000 users, a one gigabit network adapter is required for the Enterprise Edition Server.

## Live Communications Server 2005, Back-End Database

The following shows the low-end and high-end hardware configurations for Live Communications Server 2005, Back-End Database.

Low-end hardware configuration:

- Dual Intel Xeon 3.06 GHz, 1-MB Cache, 533 MHz FSB
- 2-GB DDR, 266 MHz RAM
- 2 SCSI Channels (split backplane)
- 5 × 18-GB hard disks, 15,000 rpm SCSI disk drives
- 1-gigabit network adapter
- Windows Server 2003 Standard Edition
- Windows SQL Server™ 2000 Service Pack 3a (SP3a)

High-end hardware configuration:

- Quad Intel Xeon 2.8 GHz, 2-MB Cache
- 8-GB DDR RAM
- 1-gigabit network adapter
- Windows Server 2003 Enterprise Edition
- SQL Server 2000 SP3a Enterprise Edition

SQL Server 2000 SP3a Enterprise Edition is required to take advantage of the 8 GB of RAM. SP3a is the minimum supported version of SQL for performance and security reasons. For more information about selecting the correct edition of SQL Server, refer to the following web site:

<http://www.microsoft.com/sql/techinfo/planning/ChoosEd.doc>

## Storage

Internal hard disks used for operating system and executable software, data, and transaction files are assumed to be on separate storage. The storage can be:

- DASD (Direct access storage device)
- SAN (Storage Area Network)
- External RAID (redundant array of independent disks)

Onboard storage:

- 2 SCSI Channels (split backplane)
- 5 x 18-GB hard disks, 15,000 rpm SCSI disk drives

Optional SAN:

- 1 Fibre Channel HBA (host bus adapter)
- SAN unit

## Application Proxy

For more information on Application Proxies, refer to [Application Proxy and MCM capacity](#) on page 91.



### Important:

To ensure you have the most current platform information, refer to *Microsoft® Office Live Communications Server 2005 with Service Pack 1 Planning Guide* from the Microsoft® web site:

<http://office.microsoft.com/en-us/communicationsserver/default.aspx>

---

## Signaling Server

To ensure that all features work correctly, all signaling servers must be running the latest software version.

---

## Trunking

To handle the traffic between the CS 1000 and the Live Communications Server 2005, you must configure sufficient SIP trunks and PCAs. The number of additional SIP trunks needed is determined by:

The number of Office Communicator Users using the SIP Gateway feature  
multiplied by:

The percentage expected to be on the phone at any given time

For example, 100 Office Communicator SIP Gateway users x 10% on the phone at any given time = 10 additional SIP trunks.

The percentage of users on a phone is decided by standard practice and the environment involved (Call Center, Normal Office, and so on).

PCA trunks are required for each Office Communicator user using the "Twinning" (for SIP Gateway) feature.

## Calculating SIP access port and PCA requirements

[Table 1: Inputs](#) on page 67 defines the inputs used to calculate SIP access ports and PCA requirements.

**Table 1: Inputs**

Input	Description
TN_MO_Users	Total Number of Office Communicator users that use the SIP Access Ports for voice services
PCA_MO_Users	Number of Office Communicator users that utilize Personal Call Assistant (PCA). The value entered is in addition to the number you indicate on the Software screen.
P_PCA_SIP	Percentage of PCA calls that use the soft client to answer

### Calculations

The following formulas are used to calculate traffic requirements:

Traffic for PCAs = (PCA\_MO\_Users) x (CCS per user) x (1 - P\_PCA\_SIP) x 10%

Traffic for SIP ports = (TN\_MO\_Users - PCA\_MO\_Users) x (CCS per user) + (PCA\_MO\_Users x P\_PCA\_SIP) x (CCS per user)

Total SIP Traffic = (Traffic for PCAs) + (Traffic for SIP ports)

Number of MO SIP ports = Poisson (Total SIP Traffic) at P.01 Grade of Service

\* - MO = Microsoft Office Communicator

[Table 2: Traffic figures](#) on page 68 shows traffic in CCS and number of ports calculated based on Poisson formula at P.01 Grade of Service.

**Table 2: Traffic figures**

Traffic (CCS)	Traffic (Erlang)	#Ports
5	0.14	2
10	0.28	3
15	0.42	3
20	0.56	4
25	0.69	4
30	0.83	4
35	0.97	5
40	1.11	5
45	1.25	5
50	1.39	6
55	1.53	6
60	1.67	6
65	1.81	6
70	1.94	7
75	2.08	7
80	2.22	7
85	2.36	7
90	2.5	8
95	2.64	8
100	2.78	8
125	3.47	9
150	4.17	10
175	4.86	12

Traffic (CCS)	Traffic (Erlang)	#Ports
200	5.56	13
225	6.25	14
250	6.94	15
275	7.64	16
300	8.33	17
325	9.03	18
350	9.72	19
375	10.42	19
400	11.11	20
425	11.81	21
450	12.5	22
475	13.19	23
500	13.89	24
550	15.28	26
600	16.67	28
650	18.06	29
700	19.44	31
750	20.83	33
800	22.22	35
850	23.61	36
900	25	38
950	26.39	40
1000	27.78	42
1500	41.67	58
2000	55.56	74
2500	69.44	90
3000	83.33	106
3500	97.22	121
4000	111.11	137
4500	125	152
5000	138.89	168

Traffic (CCS)	Traffic (Erlang)	#Ports
6000	166.67	198
7000	194.44	228
8000	222.22	258
9000	250	288
10000	277.78	318
20000	555.56	611
30000	833.33	908
40000	1111.11	1205
50000	1388.89	1502
60000	1666.67	1799
70000	1944.44	2096

## Port usage

The ports used between Live Communications Server and CS 1000 are the ports related to TCP and TLS. These are:

- 5060: TCP
- 5061: TLS

The dynamic port range used by Microsoft® Office Communicator for SIP/RTP is:

1024 - 65535

The port range can be controlled (restricted) to a smaller range using the group policy settings as described on the Microsoft® site:

<http://support.microsoft.com/default.aspx?scid=KB;EN-US;903056>

Note: Port ranges must not overlap.

---

## Security Considerations

When considering a Converged Office deployment, the following security concepts must be understood and integrated into deployment planning.

## Authentication of Live Communications Server Clients

Authentication of Microsoft® Office Communicator clients is provided by the Live Communications Server. For more information, refer to the *Microsoft® Office Communicator 2005 Planning and Deployment Guide* on the Microsoft® site:

<http://office.microsoft.com/en-us/communicationsserver/default.aspx>

## Authorization of TR/87 (Remote Call Control) Service Requests

Authorization of TR/87 (Remote Call Control) service requests within a Converged Office deployment is handled by the MCM. The main requirement for authorization of service requests arises from the ability for Office Communicator users to manually override the Phone Integration settings in Active Directory provisioned by an administrator. To ensure that each Live Communications Server user is restricted to the Active Directory configuration provisioned by an administrator for Remote Call Control, MCM provides an option to enable or disable authorization of TR/87 service requests. Refer to section [Configuring MCM for Remote Call Control](#) on page 121 for details on the authorization process and MCM configuration requirements.

## Signaling and Media Encryption

IP Connectivity between the Live Communications Server and the CS 1000 is provided by TCP and TLS. Similarly, Live Communications Server server-to-server traffic can also be TCP or TLS. TLS is the preferred option to provide signaling security between Live Communications Server and CS 1000.

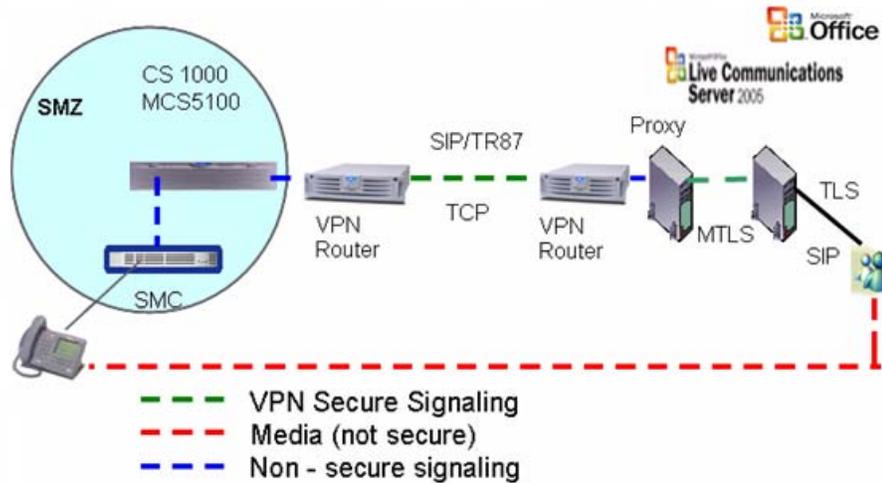
 **Note:**

A Linux-based NRS is required to ensure that TLS is supported. To ensure that TLS is configured correctly, see [Configuring Transport Layer Security \(TLS\)](#) on page 201.

 **Note:**

For more information on TLS, see [Installation and Configuration](#) on page 99.

To provide signaling security between the Live Communications Server and the CS 1000 (see [Figure 36: Signaling Security](#) on page 72), Contivity VPN routers can be used to tunnel SIP signaling between the Live Communications Server and the CS 1000. A single VPN router supporting Live Communications Server can service multiple individual VPN routers from multiple CS 1000 deployments.



**Figure 36: Signaling Security**

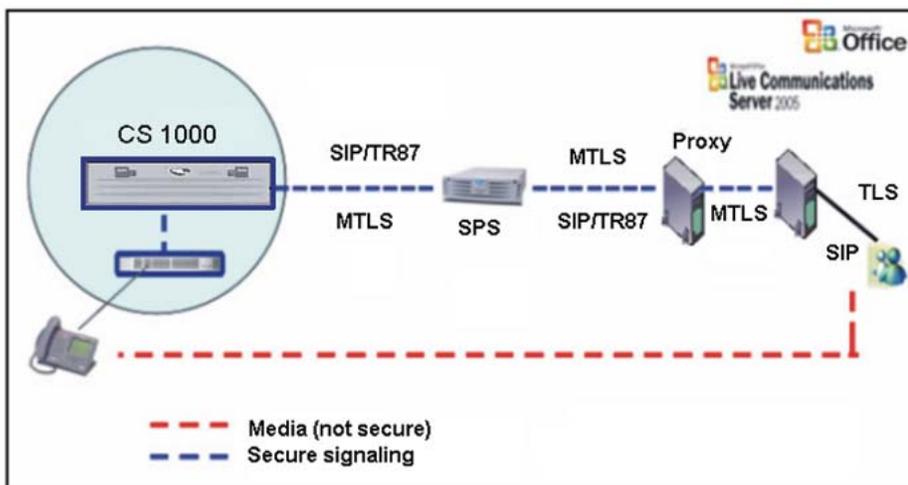
Secure Management Zone (SMZ) provides management access to local and remote devices over a secure connection. SMZ is a best practice that documents the LAN and WAN configurations required for secure management.

Virtual Private Network (VPN) enables secure communications through Secure Internet Protocol (IPSec) encryption.

Transport Layer Security (TLS) ensures that third parties cannot eavesdrop or tamper with messages when a server and client communicate.

**! Important:**

When configuring your security policies, note that policy secure end-to-end is not supported with this application.



**Figure 37: Signaling Security with TLS**

---

## Dial Plan Considerations

### Overview

As discussed in previous sections, Microsoft® Converged Office consists of two components:

1. SIP CTI Services, which provides CS 1000 native TR/87 support to enable the Remote Call Control functionality available with Microsoft® Office Communicator.
2. Telephony Gateway and Services, which provides the ability to originate and receive SIP calls (VoIP, Computer calls) from Microsoft® Office Communicator.

Whether a single or both components are chosen for deployment, an understanding of the existing dial plan and the mechanism through which it is exposed through Microsoft® Office Communicator is essential. This knowledge allows the existing dial plan (that users have become accustomed to with their existing telephony interfaces) to extend seamlessly to the Microsoft® Office Communicator client for either call type. This includes all existing CS 1000 dial plan features such as Coordinated Dial Plan (CDP), Uniform Dial Plan (UDP), and Group Dial Plan.

The following lists provide a summary of the features that contribute to the dial plan configuration for the Converged Office feature from the perspective of calls originated and received from Microsoft® Office Communicator.

Computer (SIP) Calls:

1. The format of the number itself entered in Active Directory or entered in Microsoft Office Communicator
2. Live Communications Server Address Book Service Normalization rules
3. The Network Redirect Service (NRS)
4. CS 1000 SIP Gateway Configuration
5. CS 1000 Call Server Configuration relating to the SIP Gateway

Phone (RCC or TR/87) Calls:

1. The format of the number itself entered in Active Directory or entered in Microsoft® Office Communicator
2. Live Communications Server Address Book Service Normalization rules
3. CS 1000 SIP CTI Services Configuration
4. CS 1000 Call Server Configuration relating to PBX phones

As highlighted by these lists, the number format and the normalization support provided by Live Communications Server is used to format numbers for both Remote Call Control and Computer calls. However, the interface from which they originate and receive calls from the CS 1000 is the TR/87 Front End and SIP Gateway respectively (as illustrated in [Figure 38: Signaling and media paths](#) on page 74).

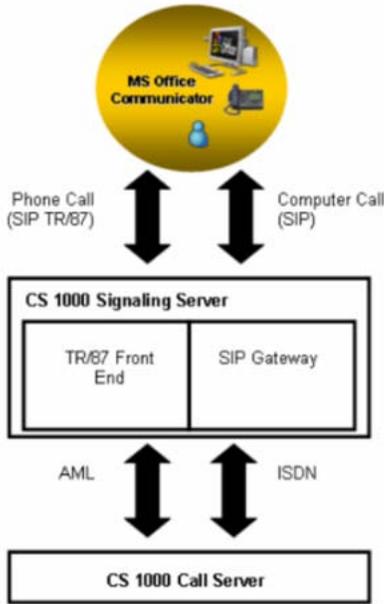


Figure 38: Signaling and media paths

## Number Formats Supported by Microsoft® Office Communicator

In general, there are two types of numbers used by Microsoft® Office Communicator: Dialstrings and E.164 International Format Numbers. Both number formats apply to Computer and Phone calls with Microsoft® Office Communicator.

By default, any digits dialed from Microsoft® Office Communicator that are not fully qualified are sent as dialstrings. The sequence of digits entered in Microsoft® Office Communicator are sent directly to the Call Server to be dialed. This allows a user to dial all numbers that you would typically expect to dial from a phone local to the CS 1000.

### Important:

If a user has been configured with a phone number that has not been registered in the NRS, blind transfers to that user will fail if the user is in Computer mode. The user will only receive blind transfers if they are in Phone mode.

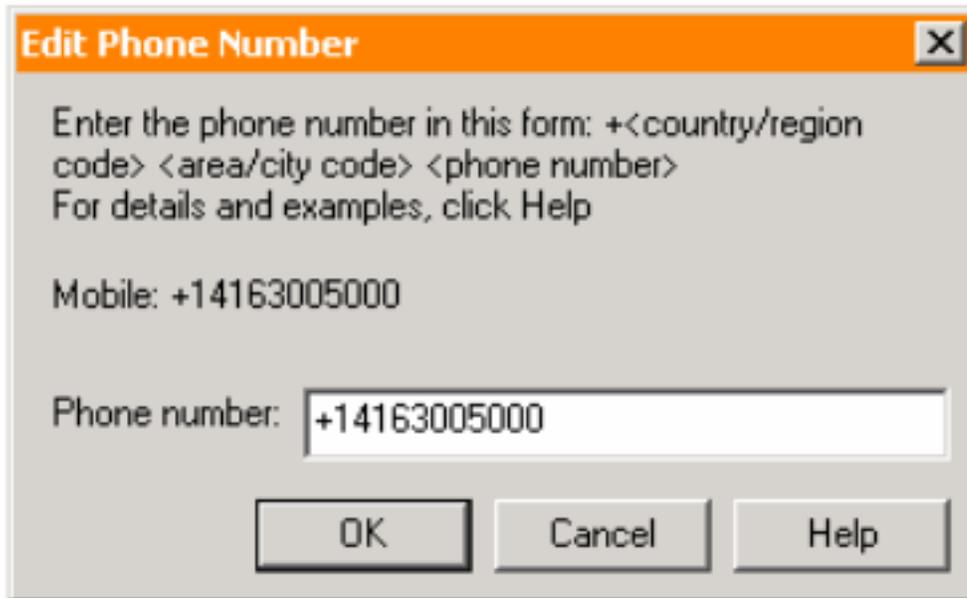
The recommended format of numbers stored in Microsoft® applications is the E.164 International format. This is a variable length number consisting of a '+' followed by a 1 to 3 digit country code and a national number that is 15-n digits long—where n is the length of the country code.

All E.164 numbers presented to the CS 1000, Computer, or Phone calls are expected to be in the following format:

+<country code><national number>

For example:

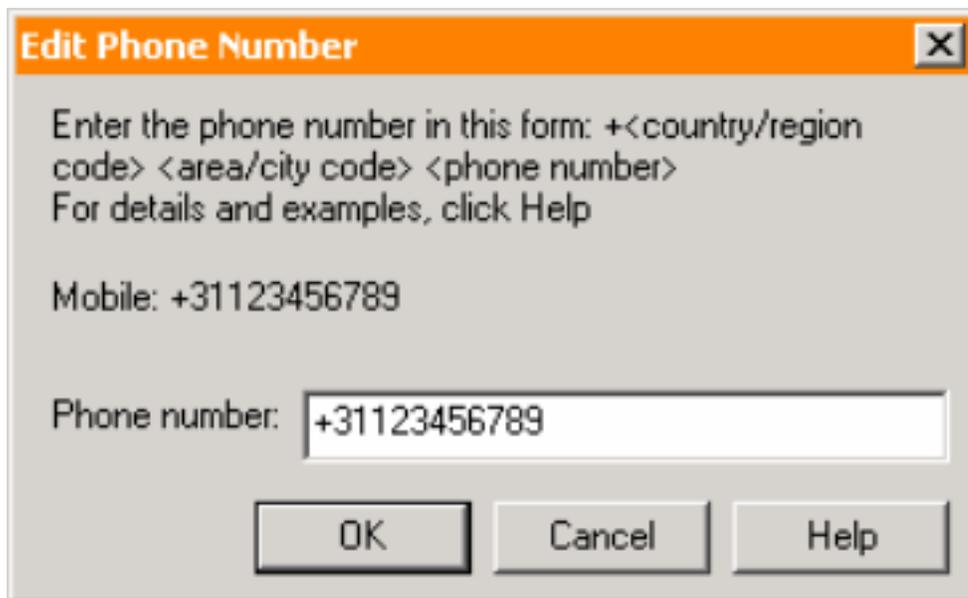
In North America, the Microsoft® Office Communicator Phone Number configuration input dialog would have the following entry (see [Figure 39: North American format](#) on page 75).



The screenshot shows a dialog box titled "Edit Phone Number" with a close button (X) in the top right corner. The text inside the dialog reads: "Enter the phone number in this form: +<country/region code> <area/city code> <phone number> For details and examples, click Help". Below this text, it says "Mobile: +14163005000". There is a text input field labeled "Phone number:" containing the value "+14163005000". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

**Figure 39: North American format**

Outside North America, the Microsoft® Office Communicator Phone Number configuration input dialog would have the following entry (see [Figure 40: Outside North America format](#) on page 75).



The screenshot shows a dialog box titled "Edit Phone Number" with a close button (X) in the top right corner. The text inside the dialog reads: "Enter the phone number in this form: +<country/region code> <area/city code> <phone number> For details and examples, click Help". Below this text, it says "Mobile: +31123456789". There is a text input field labeled "Phone number:" containing the value "+31123456789". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

**Figure 40: Outside North America format**

The Normalization feature, provided by the Microsoft® Live Communication Server Address Book Service, can be used to ensure that any formats used within a local deployment that do

not conform to this convention can be converted without changes to the existing numbers themselves.

For example, in the Netherlands, numbers in Active Directory may be entered in the following format:

+31(0)123456789

A normalization rule can be used to strip the digit in brackets to conform to the expected format for E.164 numbers when using the Converged Office feature:

+31123456789

For more information on Normalization rules, refer to [Creating Normalization rules](#) on page 193.

Handling numbers called from Microsoft® Office Communicator in E.164 format requires that the Call Server be configured to ensure that the number requested is within the defined dial plans:

1. Within North America, various types of numbers can be recognized, including international, national, local (NPA, NXX, Free Calling Area Screening, and so on), or private, using one or two access codes and number translators (AC1 and AC2). The E.164 number entering the Call Server for Converged Office calls must be recognizable by the Call Server so that the call can be routed appropriately. The number is interpreted based upon the access code used within the called number as it enters the Call Server (AC1 or AC2).

If calls entering the Call Server are identified as international and outside of North America (for example, the country code is not 1), the translator used must contain entries that recognize these international numbers and route the call to the appropriate route list. These entries are generally within the existing AC1/AC2 translator, since they are used to route international calls that are dialed directly from phones.

If calls entering the Call Server are national or local, the translation used must be able to recognize numbers with the national dialing prefix (for example, Converged Office calls) as well as numbers without the national prefix (for example, local calls dialed by users). To enable this without duplication of number plan entries, a Home NPA (HNPA) entry can be added to the AC1 translator to recognize calls within the local NPA that include the North American national dialing prefix (for example, 1613 within NPA 613). After matching this HNPA entry within AC1, the translation software automatically begins using the AC2 translator to recognize the rest of the digits received.

2. Outside North America, various types of numbers are recognized, including international, national, local, or private, using one of two access codes and number translators (AC1 and AC2) and SPN entries. The E.164 number entering the Call Server for Converged Office calls must be recognizable so that the call can be routed appropriately. The number is interpreted based upon the access code used within the called number as it enters the Call Server (AC1 or AC2). If calls entering the Call Server are identified as international and outside of the country of the caller, the translator used must contain entries that recognize these international numbers and route the call to the appropriate route list. These entries are generally within

the existing AC1/AC2 translator, since they are used to route international calls that are dialed directly from phones.

## Handling E.164 international format numbers for SIP Gateway and SIP CTI

The handling of E.164 international format numbers for SIP Gateway (Computer) calls is discussed in [Dialing E.164 International Format Numbers from Microsoft® Office Communicator - Computer Calls \(SIP Gateway\)](#) on page 166.

The handling of E.164 international format numbers for SIP CTI (Phone) calls is discussed in [Dialing E.164 International Format Numbers from Microsoft® Office Communicator - Phone Calls \(SIP CTI\)](#) on page 191.

---

## Telephony Gateway and Services

This section describes the various planning and engineering issues associated with the Telephony Gateway and Services component.

[Table 3: Systems, platforms, and applications](#) on page 77 identifies the systems, platforms, and applications supported by the Telephony Gateway and Services component.

**Table 3: Systems, platforms, and applications**

System, platform, and application	Supported
<b>M1/CS 1000 Systems</b>	
CS 1000M SG (CP PIV)	Yes
CS 1000M MG (CP PIV)	Yes
CS 1000E	Yes
MG 1000B	Yes

---

## Capacity

Refer to [Capacity](#) on page 90 for capacity information relating to the Telephony Gateway and Services and Remote Call Control components.

---

## Redundancy

Live Communications Server 2005 redundancy model is supported, with limitations, using Load Balancers.

## NRS redundancy

NRS redundancy is similar to Converged Office redundancy; a heartbeat mechanism between MCM 2.0 and NRS servers is implemented. When a heartbeat failure from the primary NRS server is detected, all messages are redirected to the secondary NRS server.

---

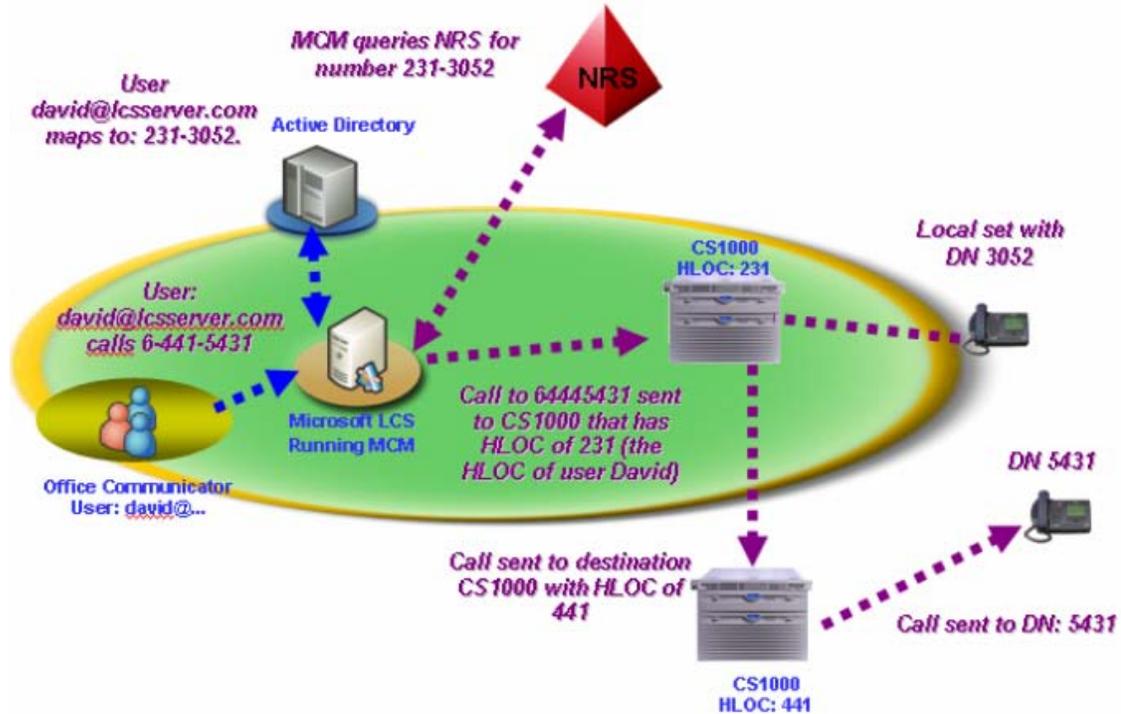
## SIP routing

MCM directs calls from an Office Communicator user to the CS 1000 connected to their "twinned" phone. A user may have a phone number in Active Directory associated with their account (in [Figure 41: SIP Routing](#) on page 79, the number used is 231-3052). Calls made from a user to any endpoint (Public number or Private) are directed to their CS 1000 first. The CS 1000 then tandems the call to the other CS 1000 , if necessary.

SIP routing ensures that:

- 1) All outgoing Office Communicator calls made by a "twinned" client can be tracked by Call Detailed Record (CDR)
- 2) Calls from Office Communicator to incompatible systems can be made

In [Figure 41: SIP Routing](#) on page 79 the user "david" calls 6-441-5431 (AC1-LOC-DN). The MCM application queries the Active Directory for the number associated with the originator "david", which comes back as 231-3052. MCM then uses the NRS to resolve the CS 1000 associated with the number 231-3052. MCM then directs the call to the CS 1000 that has the number of 231-3052. This CS 1000 then directs the call to the CS 1000 that has the destination number of 441-5431. This CS 1000 then directs the call to the CS 1000 that has the number 441-5431.



**Figure 41: SIP Routing**

It is important to understand the behavior of MCM when calculating the number of required SIP Trunks required by each CS 1000 . Calls made to a CS 1000 that the "twinned" phone is not based off of use two SIP trunks: one incoming and one outgoing.

If users commonly call between CS 1000 systems, additional SIP trunks may be needed.

The number of required SIP trunks is sufficiently covered through the use of the calculations described in [Trunking](#) on page 67 and the platform-specific Planning and Engineering document.

## Feature Limitations

The following sections describe the limitations of the Telephone Gateway feature.

### Call transfers for Office Communicator direct Computer to Computer calls

If a call is set up from an Office Communicator user in Computer mode to another Office Communicator user directly, the call is made to a "Computer" instead of a phone number (see [Figure 42: Computer call](#) on page 80). As a result, the CS 1000 is not involved in the call and this type of call cannot then be transferred to a phone number.



**Figure 42: Computer call**

## **Office Communicator-initiated Call Transfer in Computer/Telephony Gateway mode**

To handle a call transferred by Office Communicator, the SIP stack of the CS 1000 must handle the request to transfer the call. As such, the number a user is transferred to is not subject to the Class of Service associated with either user (the transferred party or the party performing the transfer). The Class of Service/Call Restriction controlling the transfer is only that of the SIP trunk itself.

## **Multi-Customer operation**

Multi-Customer operation is not supported within a single Signaling Server; a separate Signaling Server is required for each customer. Each customer configured on the Call Server requires a separate node number and domain. For more information about how to configure a Multi-Customer environment refer to [Multiple Customer Network](#) on page 62.

## **Deployment**

You can find all the required information to support Live Communications Server 2005 and Microsoft® Office Communicator deployment on Microsoft® Live Communications Server site:

<http://office.microsoft.com/en-us/communicationsserver/default.aspx>

MCM 2.0 uses LDAP queries to the Active Directory server for user-id/DN lookup. The Active Directory server must be engineered properly to provide the expected performance for the LDAP queries (less than 25 milliseconds). Live Communications Server and Active Directory APIs are used for queries and mapping.

## **Live Communications Server 2005 availability**

Live Communications Server 2005 availability is up to 99.99% as described on the Microsoft® web site. (This is a Microsoft® limitation.)

## Live Communications Server 2005 redundancy

The Live Communications Server 2005 redundancy model is supported, with limitations, using Load Balancers. For more information, refer to [Load Balancer](#) on page 57.

## Microsoft® Office Communicator Web Access

Converged Office requires that the client support SIP Gateway functionality. The web version of Office Communicator, Microsoft® Office Communicator Web Access, does not support SIP Gateway. Therefore, Microsoft® Office Communicator Web Access does not work with Converged Office.

## Microsoft® Office Communicator Mobile (COMO)

Converged Office requires that the client support Telephony Gateway. The Mobile version of Office Communicator, Microsoft® Office Communicator Mobile, has limited support for Telephony Gateway. Telephony Gateway is only supported when the device is running Windows Mobile 5.0. Also, VoIP calls work for incoming calls, but outgoing VoIP calls can only be placed to other Office Communicator users (Computer to Computer calls). Outgoing VoIP calls to phone numbers for Microsoft Office Communicator Mobile are not supported.

## Microsoft® Virtual Server 2005

Microsoft® Virtual Server 2005 is not supported as part of the Avaya Converged Office feature.

## DTMF

CS 1000 supports in-band DTMF digits and out-of-band DTMF digits for SIP calls through RFC2833. RFC2833 is an out-of-band mechanism for DTMF signaling. DTMF digit handling using RFC2833 enables Avaya CS 1000 products to work with other SIP products that support out-of-band DTMF signaling.

With RFC2833, a key press on a telephone is translated into a signaling packet (or packets) that flow with the VoIP stream to the far end. These signaling packets are in fact RFC packets which contain the DTMF key that was pressed. The same principle applies to TDM devices that are involved in a VoIP call. The Voice Gateway (VGW) TN that converts the TDM stream to VoIP also detects a tone on the TDM side and translates it to RFC2833 packets on the VoIP side. As well, the VGW TN can receive an RFC2833 packet on the VoIP side and generates a tone on the TDM side.

The correct Loss Values must be configured for in-band DTMF. For more information about correctly configuring the CS 1000 to support in-band DTMF tones, refer to [Configuring the Call Server](#) on page 144.

## Support of Multimedia Communicator Server (MCS) MeetMe Conference

There are no limitations for Office Communicator calls to the MCS MeetMe bridge provided that all tandem nodes are running the same software.

## Codecs

G.711 A/MU law and G.723.1 are codecs supported for Office Communicator 2005. CS 1000 configuration no longer restricts the use of G.723.1 (out-of-band DTMF digits are now supported).

 **Note:**

The G.711 codec must use a 20-ms payload at this time, due to the Microsoft® Office limitation.

 **Note:**

Office Communicator does not support G 729.

## IPDR/CDR capability

Live Communications Server 2005 does not support IPDR/CDR capability. CDR captures are supported on CS 1000 systems.

## Video Calls

Office Communicator calls made in "Computer" mode can only establish video when connected in a call to another Office Communicator that is also in "Computer" mode.

## Office Communicator 2005 video support

Office Communicator video is supported for both Remote Call Control and SIP Gateway. The video setup is exclusively Office Communicator client to Office Communicator client.

Note: For video calls to work, both users must be using the same form of Office Communicator (for example, both are using either SIP CTI Office Communicator or SIP Gateway Office Communicator).

## Video Call Transfer

Office Communicator calls made in "Computer" mode that have established video can be transferred to another Office Communicator user in "Computer" mode—although the new call is audio only. The transferred Office Communicator user will experience the call becoming audio only. After the transferred call is answered by the new endpoint, video can be established. As with all Call Transfers in "Computer" mode, it is a "Blind Call Transfer," meaning that the call is immediately transferred to the new party.

## Re-establishing Voice for Office Communicator Telephony Gateway to Office Communicator Telephony Gateway Video calls

Voice and Video calls that are established in Computer mode from one Office Communicator to another Office Communicator cannot drop the voice part of the call and then add back it again.

## Local Tones

Office Communicator 2005 does support the generation of local tones (for example, "Ringback"), but the tones generated by Office Communicator are unique tones that are not specific to any country. Also, ringback is only generated for a configured number of cycles — after which the other end continues to ring, but there is no audible ringback.

To change the ringback, or any tone, perform the following:

### Changing local tones

1. On the PC, select **Control Panel > Sounds and Multimedia**.
2. Select the **Sounds** tab.
3. Scroll down to the **Microsoft® Office Communicator 2005** section and select a tone (see [Figure 43: Sounds and Multimedia Properties](#) on page 84).

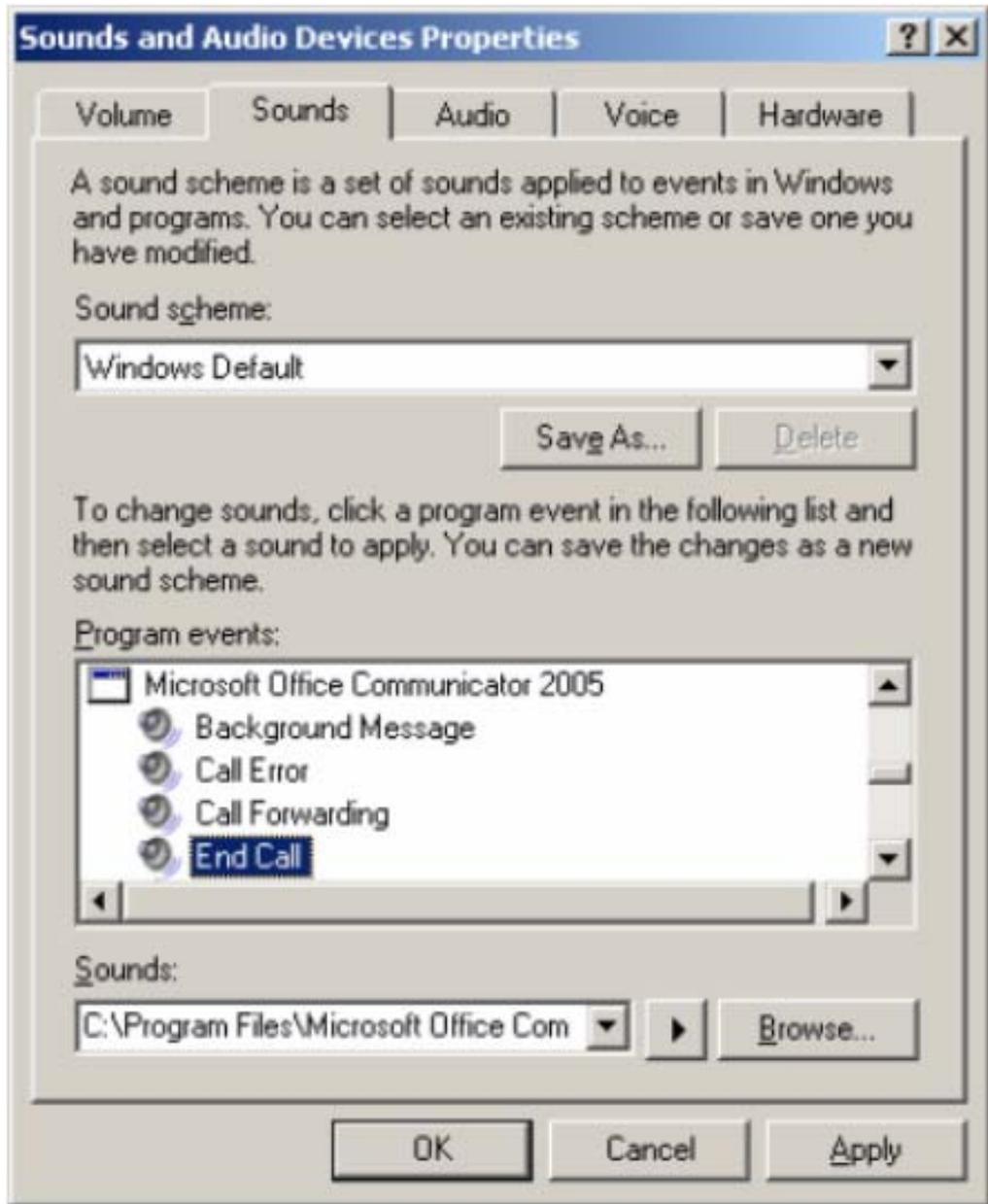


Figure 43: Sounds and Multimedia Properties

## Quality of Service (QoS)

Office Communicator 2005 does not support QoS (L2: 802.1p/q or L3: diffserv).

## Voice mail

Voice mail is not supported for direct Office Communicator calls. Voice mail is supported only with PCA/SimRing/CD1 Call Forward No Answer and Avaya Multimedia Communication Server 5100 (Avaya MCS 5100) Advanced Screening calls.

## Long distance/overseas control

Long distance or overseas calls from Office Communicator are allowed based on the Network Class of Service (NCOS) for the MARP TN of the number/ extension associated with the Office Communicator user. For example, if user david@lcsuser.com has a number/extension of 3052, david@lcsuser.com can call the same long distance and overseas numbers that the number/ extension 3052 can on the CS 1000.

For more information refer to [Configuring the Call Server](#) on page 144.

## Avaya MCS 5100

Avaya MCS 5100 interoperability and federation with Live Communications Server 2005 requires that a CS 1000 reside between the two, and is limited to voice in this feature.

## SIP Trunks

TCP or TLS-based SIP trunks are supported. SIP trunks and gateways must be enabled with enough trunks to handle the traffic between the CS 1000 and Live Communications Server 2005.

For more information, refer to [Trunking](#) on page 67.

## SIP CTI mode (phone mode)

Office Communicator 2005 supports SIP CTI mode (phone mode) where it controls the desktop phone to originate or answer calls and the non-CTI mode where voice calls can be originated or answered in the client.

## CDP

Local Steering Code must be part of the internal DN, if not OC clients fail to acquire the CS 1000 set. This is an unsupported configuration.

## Hold and Transfer

Office Communicator 2005 supports Hold and Transfer in stand-alone or non-CTI mode.

## ipDialog Ethernet Phone

Office Communicator 2005 clients can only work with the ipDialog Ethernet Phone if it is tandemed through a CS 1000.

## Country or region tone configuration

Country or region tone configuration is not supported by Live Communications Server 2005 and Office Communicator 2005.

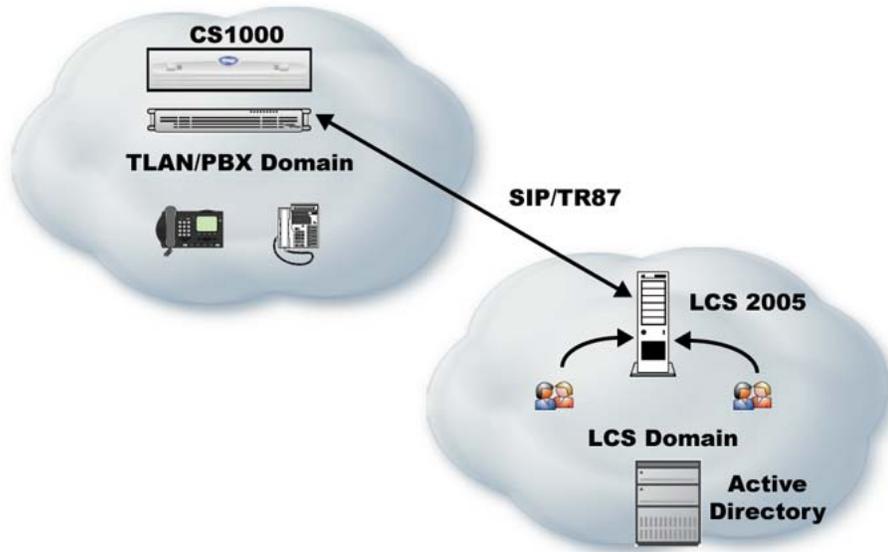
## DAPC

The Display of Access Prefix (DAPC) on Calling Line Identification (CLID) feature enhances the phone display by adding the Local, National, or International prefix to the CLID display. Prefix added by this feature to CLID display on CS 1000 phone is not carried to the twinned OCS Remote Call Control Phones display.

---

## Remote Call Control with SIP CTI

The Remote Call Control component works in all configurations that include a Signaling Server and is supported for IP, digital, and analog phone types.



**Figure 44: Simple network diagram**

Microsoft® Office Communicator 2005 is the first soft client to use the ECMA TR/87 specification. [Figure 44: Simple network diagram](#) on page 87 shows a sample customer network deploying Active Directory, Live Communications Server Home Server, and CS 1000. [Figure 44: Simple network diagram](#) on page 87 does not show a Live Communications Server Application Proxy that can be inserted between a Live Communications Server Home Server Pool and CS 1000 servers for easy network configuration.

The TR/87 FE is the application that resides on the CS 1000 Signaling Server to support the telephony control requests and responses received from Microsoft® Office Communicator 2005 within a Live Communications Server 2005 deployment.

You can configure the TR/87 FE as a static routing rule within each pool of Live Communications Server Home Servers, or you can use the NRS to route TR/87 association requests.

CS 1000 is supported in both the Live Communications Server 2005 Standard Edition and Enterprise Edition network configurations subject to the capacity restrictions defined in this document.

[Table 4: Supported systems, platforms, and applications](#) on page 87 identifies the various systems, platforms, or applications that are interoperable or supported by the Remote Call Control component.

**Table 4: Supported systems, platforms, and applications**

System, Platform or Application	Interoperable	Supported
<b>M1/CS 1000 Systems</b>		
Option 11C Cabinet	N	N
Option 11C Chassis	N	N
Option 51C	N	N

System, Platform or Application	Interoperable	Supported
<b>M1/CS 1000 Systems</b>		
Option 61C (CP3/4)	N	N
Option 61C (CP PIV)	N	N
Option 81C (CP3/4)	N	N
Option 81C (CP PIV)	N	N
CS 1000S	Y	Y
CS 1000M Cabinet	Y	Y
CS 1000M Chassis	Y	Y
CS 1000M Small	Y	Y
CS 1000M HG	Y	Y
CS 1000M SG (CP3/4)	Y	Y
CS 1000M SG (CP PIV)	Y	Y
CS 1000M MG (CP3/4)	Y	Y
CS 1000M MG (CP PIV)	Y	Y
CS 1000E	Y	Y
MG 1000B	Y	Y
Other Systems, Call Servers and Gateways		
CS 2000	N/A	N/A
CS 2100	N/A	N/A
Avaya MCS 5100	N/A	N/A
SRG 1.0	N/A	N/A
SRG 505	N/A	N/A
Avaya BCM 50	N/A	N/A
Avaya BCM 200/400	N/A	N/A
Avaya Applications		
IP Clients	N/A	N/A
CDR	N/A	N/A
Element Manager	N/A	N/A
IP Call Recording	N	N
(See 9.1.1) Avaya CallPilot	N/A	N/A
Avaya CallPilot Mini	N/A	N/A

<b>System, Platform or Application</b>	<b>Interoperable</b>	<b>Supported</b>
<b>M1/CS 1000 Systems</b>		
Meridian Mail	N/A	N/A
Meridian Mail Card Option	N/A	N/A
Meridian / Succession Companion DECT (DMC8 version)	N/A	N/A
VoIP - 802.11 Wireless IP Gateway	N/A	N/A
Remote Gateway 9150	N/A	N/A
Remote Office 9110/9115/ IP Adaptor	N/A	N/A
Mini Carrier Remote	N/A	N/A
Carrier Remote	N/A	N/A
Fiber I and Fiber II	N/A	N/A
Symposium Desktop TAPI Service Provider for MCA	N/A	N/A
Meridian Link Services [MLS]	Y	Y
Symposium TAPI Service Provider	N/A	N/A
Symposium Agent	N/A	N/A
Symposium Agent Greeting	N/A	N/A
Symposium Express Call Center (SECC)	N/A	N/A
Symposium Call Center Server [SCCS]	N/A	N/A
Symposium Web Centre Portal (SWCP)	N/A	N/A
Periphonics Open IVR (VPS/is)	N/A	N/A
Periphonics Integrated Package for Meridian Link (IPML) – VPS	N/A	N/A
Periphonics Multimedia Processing Server (MPS) 100	N/A	N/A
Periphonics Multimedia Processing Server (MPS) 500	N/A	N/A
Integrated Call Assistant (MICA)	N/A	N/A
Integrated Conference Bridge (MICB)	N/A	N/A
Integrated Recorded Announcer (MIRAN)	N/A	N/A
Integrated Call Director (MICPD)	N/A	N/A

System, Platform or Application	Interoperable	Supported
<b>M1/CS 1000 Systems</b>		
Hospitality Integrated Voice Services (HIVS)	N/A	N/A
Enterprise Data Networking	N/A	N/A
Third party applications		
AML based applications	Y	Y
Net6	N/A	N/A
Avaya H.323 GW	N/A	N/A
Avaya SIP GW	N/A	N/A
Competitors		
Cisco H.323 GW	N/A	N/A
Cisco SIP GW	N/A	N/A

---

## Capacity

When planning for capacity with SIP CTI services, there is a fundamental restriction that must be observed:

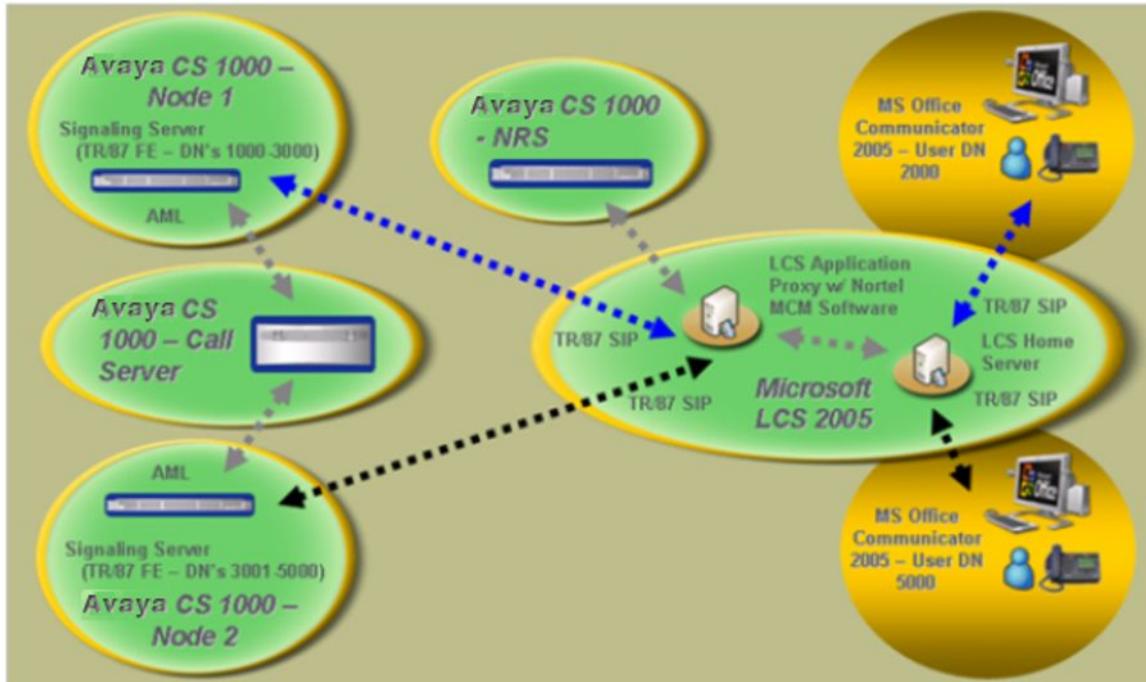
For a single Call Server that supports multiple nodes, each with SIP CTI services enabled, multiple SIP CTI(TR/87) sessions can be established for a given DN through the same node—but not through different nodes.

To illustrate this restriction, consider the following high level example:

Client A sends a TR/87 SIP INVITE to Node 1 to monitor DN 1000. The TR/87 association is established. Client B then sends a TR/87 SIP INVITE to Node 1 (the same node) to monitor DN 1000. Both sessions are established successfully. As a result of this sequence, two TR/87 sessions exist for DN 1000 through node 1.

However, if client B attempts to send a TR/87 SIP INVITE to Node 2 (which has an AML link to the same call server as Node 1), the attempt to establish the TR/87 session fails because the DN is already in use by client A's session through Node 1.

To solve this issue when planning for capacity, SIP routing must ensure that all TR/87 sessions for a given DN always terminate on the same node when there are multiple nodes for a single Call Server (see [Figure 45: Capacity example](#) on page 91).



**Figure 45: Capacity example**

This situation may arise in cases where there is an expectation that a single user has multiple clients logged in simultaneously (for example, a client at home, a client in the office, and a mobile client all with TR/87 capability).

## Impact on Signaling Server

The maximum number of SIP CTI/TR87 users on a single Signaling Server is 5000.

## Impact on Call Server

For different CPUs, the number of users supported is:

- CP PII 7000 users
- CP PIV 15000 users
- CP PM: 15000 users

## Application Proxy and MCM capacity

The Standard Performance Evaluation Corporation (SPEC) is a non-profit corporation formed to establish, maintain, and endorse a standardized set of relevant benchmarks that can be applied to the newest generation of high-performance computers.

MCM capacity numbers depend on the hardware platform this application runs on, and the unit used to identify the platform is SPECint.

A single MCM can support 20000 calls per hour (this is a projected value of 4000 users averaging 5 calls per hour - check this using Windows Performance Monitor), per box, with a SPECint of 18.6.

Since MCM co-resides with Microsoft® Live Communications Server on different platforms, the formula for different hardware platforms is:

Number of calls per hour supported = (20000 x SPECint for a box) / 18.6

Note: This formula is based on SPECint\_rate2000. The SPECint for each box can be found at <http://www.spec.org/>.

---

## Redundancy

SIP CTI services are supported (with limitations) in the following scenarios:

- Single node redundancy
- Campus redundancy
- Geographic redundancy

### Redundancy within a single node

The same master/follower mechanism used for VTRK and TPS applications is used to support redundancy within a node for Remote Call Control. After the master of the node goes down, one of the followers takes over the node IP and continues to deliver service. No SIP CTI session state is preserved when a new master is elected.

Redundancy across multiple nodes is possible using the least cost routing feature of NRS.



#### **Important:**

When considering a multi-node redundant configuration, refer to the restrictions on establishing TR/87 sessions from multiple nodes that have AML links to a single Call Server (see [Capacity](#) on page 90).

### Campus redundancy

Campus Redundancy increases the distance between the two CPU cores of Communication Server 1000E.

CS 1000E is the only large system that supports this feature.

## Geographic redundancy

Geographic Redundancy can be supported with the limitations that currently exist for SIP GW SIP traffic. The main impacts are:

1. During transition periods, situations may arise where IP Phones are registered to a Call Server different from the Call Server providing support for the TR/87 FE. In this case, TR/87 support is undefined. TR/87 clients are allowed to register successfully, however the status of the IP phone is impacted by any actions performed on the phone itself, or TR/87 client, since the FE and IP Phone are interfacing different Call Servers.

 **Important:**

NRS is required to support redundancy.

2. After an event occurs that causes the IP Phones to register to a server other than their home server (and then to return to their home server), the Office Communicator 2005 client does not automatically follow the IP Phone registration. In order for the TR/87 sessions to be directed back to the TR/87 FE corresponding to the home TPS, one of the following actions must be taken:
  - a. Users must log out and log back into the TR/87 client (for example, Office Communicator 2005) to force the previous SIP dialog to terminate so that a new dialog can be established, which NRS then redirects to the correct TR/87 FE.
  - b. An administrator issues the "SIPCTIStop all" command on the Signaling Server (see [Table 5: SIPCTIStop all Command](#) on page 93) to which the TR/87 sessions currently reside to terminate the SIP dialogs and force the clients to send another association request (for example, SIP INVITE) which the NRS then redirects to the correct TR/87 FE.

**Table 5: SIPCTIStop all Command**

Command	Description
SIPCTIStop all	De-acquire all AST DNs and terminate all TR/87 SIP sessions.

## Branch Office redundancy (MG 1000B/SRG)

Branch Office scenarios can be supported; however, SIP CTI support and Telephony Gateway and Services are available for Branch User IP Phones in Local mode (registered in the Branch Office) only when the following conditions are met:

- Branch Office has SIP CTI and Telephony Gateway and Services enabled and properly configured and has a Signaling Server (SS) dedicated to each branch.
- The network dialing plan is a Coordinated Dial Plan (CDP).
- The IP Phone (Branch User) has the same domain name (DN) configured in Main Office and Branch Office.
- The Branch Office has access the Network Redirect Service (NRS) and Live Communications Server (LCS). If access is disrupted, failure cases may not be supported if the NRS and LCS are located in close proximity to the Main Office, which is no longer available. For example, when the WAN link to the Main Office is down, the NRS and LCS are out of service.
- The SIP Gateway in the Main Office is out of service (in which case the SIP Gateway in the Branch Office is used).

The Microsoft Office Communicator client has no automated mechanism to register to the branch. Users must wait for the existing dialog to timeout (30 minutes) or manually log out and log in again after the IP Phones go to Local mode.

Digital and analog telephones in the Branch Office can have SIP CTI support and Telephony Gateway and Services when the Branch Office has access to the NRS and LCS.

---

## Feature limitations

The following sections describe the limitations of the Remote Call Control with SIP CTI component.

### Call Forwarding

Microsoft® Office Communicator does not reflect call forward state changes made to the CS 1000 phone itself.



#### **Warning:**

Microsoft® Office Communicator does not reflect call forward state changes made to the CS 1000 phone itself. When Office Communicator is active and controlling a DN, all Call Forward changes must be made through Office Communicator to ensure that it is in the correct state.

When a user signs into Live Communications Server from their Office Communicator client, the forwarding status saved within Office Communicator overrides any forwarding status

that may be configured from the phone. For example, if forwarding is off within Office Communicator, it is turned off following sign in, regardless of the phone forwarding status at the time.

## Analog phone usage

As a general rule, Office Communicator in SIP CTI mode can only control and invoke telephony features supported by the phone being controlled. If a feature is not supported or configured on a particular phone (whether it be Analog, IP, or Digital), that feature is not supported by Office Communicator. As such, Office Communicator in SIP CTI mode supervising an analog phone (2500) has the following limitations:

- Make Call: cannot be made through Office Communicator if the analog phone (2500) phone does not go off hook prior to placing the call
- Answer Call: cannot be performed through Office Communicator. Answer Call must be performed through the analog phone (2500)
- Call Conference: cannot be performed through Office Communicator
- Call Hold: can be performed through Office Communicator
- Call Transfer: Analog phones do not support the Conference and Transfer feature keys. As a result, Call Conference and Call Transfer (Announced and Blind) cannot be performed through Office Communicator.



### Important:

Flexible Feature Code (FFC) is not supported by AML and SIP CTI.

- Send DTMF digits: DTMF digits work with both Voicemail and Conferencing

## Multi-Customer operation

Multi-Customer operation is not supported within a single Signaling Server; a separate Signaling Server is required for each customer. For more information about how to configure a Multi-Customer environment refer to [Multiple Customer Network](#) on page 62.

## TR/87 front end application

The TR/87 FE application on a Signaling Server can support only a single Call Server.

## UDP Location Code

Only one UDP Location Code can be associated with each Signaling Server TR/87 interface.

## **Microsoft® Office Communicator Web Access**

Converged Office requires that the client support SIP CTI. The web version of Office Communicator, Microsoft® Office Communicator Web Access, does not support SIP CTI.

## **Microsoft® Office Communicator Mobile (COMO)**

While Converged Office requires that the client support Remote Call Control, the Mobile version of Office Communicator, Microsoft® Office Communicator Mobile, has limited support for Remote Call Control.

Outgoing VoIP calls to phone numbers for Microsoft® Office Communicator Mobile are not supported. Remote Call Control only permits the phone status to be updated (for example, on a call or not) when using Microsoft® Office Communicator Mobile. Remote Call Control supports Call Forward with COMO.

## **Microsoft® Virtual Server 2005**

Microsoft® Virtual Server 2005 is not supported as part of the Avaya Converged Office feature.

## **AML limitation**

CS 1000 has an AML limitation where only one application may acquire a DN/TN at any time. For example, the TR/87 FE application and IP Call Recording cannot co-exist on the same DN/TN. This also applies to the interaction between Symposium and Microsoft® Office Communicator Remote Call Control. Symposium uses the Application Module Link (AML) to acquire and control phones on CS 1000 Call Server.

## **Office Communicator 2005 Call Forward On feature**

When the CS 1000 Call Forward All Calls feature is enabled, only calls to the Prime DN or any single-appearance DN on the telephone are forwarded. Therefore, if an Office Communicator 2005 acquires a MADN which is not the Prime DN then the call is not forwarded, even if Call Forwarding On is enabled. For more information, refer to Avaya Communication Server Features and Services (NN43001-106).

## **Live Communications Server/MCS co-existence**

A user cannot have both Live Communications Server and MCS enabled for their extension (all TN's that have a particular number/extension). If any of the TN's have CLS CDMV or CLS

CDMO configured, then the extension is treated as having MCS enabled. When MCS (SIP CD) is enabled on an extension, Live Communications Server Converged Office is not supported for that extension.

**Important:**

All Converged Office users must have their extension configured as CLS CDMR.

## Avaya CallPilot configuration

In order for Telephony Gateway (Computer mode) calls to Avaya CallPilot to be able to access their mailbox by just pressing the "#" key, every mailbox needs to have the optional messaging network configured. In a normal CS 1000 - Avaya CallPilot, this configuration is optional and may not be configured. For Telephony Gateway (Computer Mode) calls to Avaya CallPilot to work properly, this extra configuration is required. For more information about the configuration of Avaya CallPilot see Avaya CallPilot network planning guide (NN44200-201).

## Conference Call and Do Not Disturb features

Conference Call and Do Not Disturb (DND) features in RCC mode are not supported by Microsoft.

## Flexible Feature Code

All Flexible Feature Codes (FFC) are not supported by RCC. In spite of FFC codes cannot be performed through Office Communicator in RCC mode, they can be used from converged phone.



# Chapter 7: Installation and Configuration

---

## Contents

This section contains information about the following topics:

[Overview](#) on page 99

[Installing CS 1000 components](#) on page 103

[Installing Microsoft Live® Communications Server components](#) on page 104

[Installing and configuring MCM](#) on page 106

[Configuring MCM](#) on page 109

[Configuring Telephony Gateway and Services](#) on page 124

[Configuring Remote Call Control](#) on page 167

[Normalizing phone numbers](#) on page 192

[Configuring SIP Routing and Redundancy](#) on page 197

---

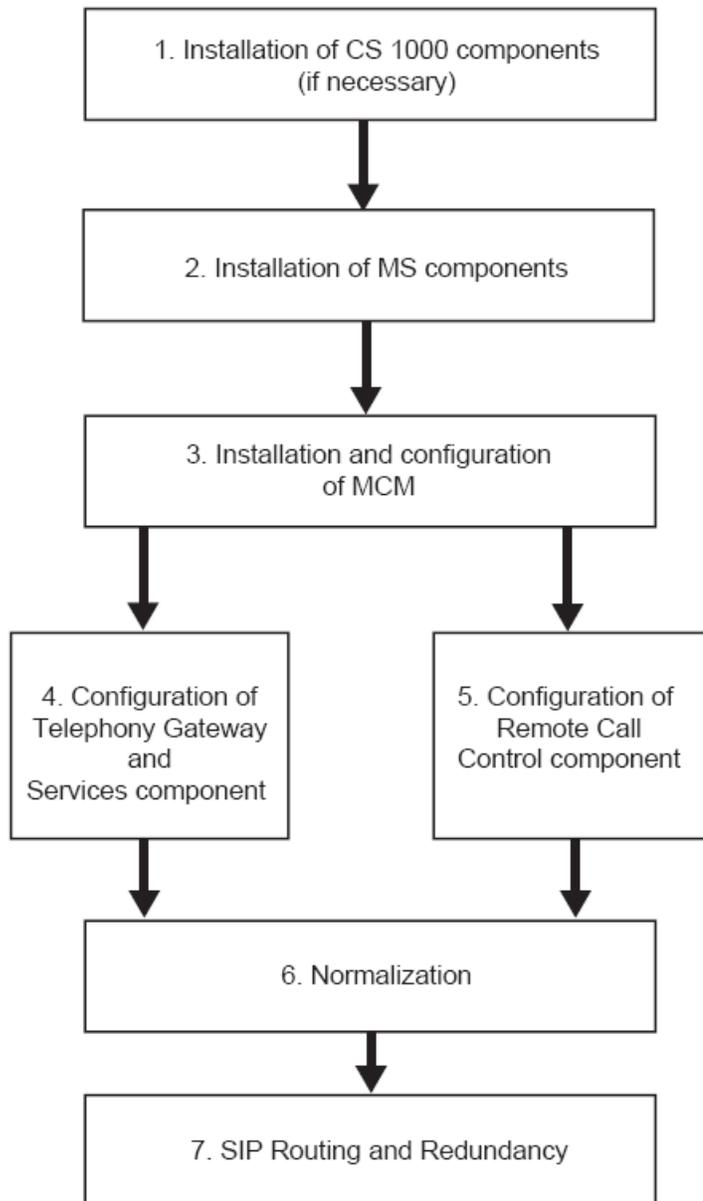
## Overview

This chapter contains the procedures necessary to install and configure Microsoft® Office Live Communications Server 2005 on an Avaya Communication Server 1000 system.

The first step is to install the necessary Avaya CS 1000 components (if you do not already have a working CS 1000 system in place). You then need to install the Microsoft server components. After all hardware and software is installed, you can configure the component you have selected: **Telephony Gateway and Services** or **Remote Call Control**.

After configuration is complete, normalization of phone numbers, SIP routing, and redundancy help you integrate the Avaya and Microsoft® Live Communications Server 2005 domains.

[Figure 46: Installation and configuration process](#) on page 100 illustrates this process.



**Figure 46: Installation and configuration process**

The following steps describe the installation and configuration process in greater detail.

1. [Installing CS 1000 components](#) on page 103
  - a. [Installing the Call Server](#) on page 103 (release 5.0 or later), including all DEP list PEPs and Converged Office PEPs.
  - b. [Installing the Signaling Server](#) on page 103 (release 5.0 or later), including all DEP list PEPs and Converged Office PEPs
2. [Installing Microsoft Live® Communications Server components](#) on page 104

- a. [Installing Active Directory](#) on page 104
  - b. [Installing Live Communications Server 2005 Service Pack 1 \(SP1\)](#) on page 104
  3. [Installing and configuring MCM](#) on page 106
    - a. [Installing MCM software](#) on page 106
    - b. [Configuring MCM](#) on page 109
  4. [Configuring Telephony Gateway and Services](#) on page 124
    - a. [Configuring Live Communications Server](#) on page 124
      - [Configuration of Static Routes on all intermediate Live Communications Servers](#) on page 130
      - [Configuring Host Authorization and Routing](#) on page 131
    - b. [Configuring Active Directory](#) on page 183
    - c. [Configuring the Call Server](#) on page 144
      - [Configuring the SIP Trunk](#) on page 145
      - [Configuring the Codec](#) on page 146
      - [Configuring the Loss Plan](#) on page 148
      - [Configuring the Dialing Plan to route to MCM](#) on page 148
      - [Configuring the Personal Call Assistant](#) on page 149
      - [Configuring the Call ID Table](#) on page 151
      - [Configuring Home LOC and Home NPA](#) on page 152 (if necessary)
    - d. [Configuring the Signaling Server](#) on page 170
      - [Configuring the DNS Server](#) on page 152
      - [Configuring the SIP Trunk](#) on page 153
    - e. [Configuring SIP Gateway CLID Parameters](#) on page 157
      - [Configuring NRS](#) on page 160
    - f. [Configuring Microsoft® Office Communicator 2005](#) on page 162
-  **Note:**  
Requires phone integration enabled (Microsoft® Knowledge Base article KB 910790)
- g. [Configuring CDR](#) on page 166
  - h. [Dialing E.164 International Format Numbers from Microsoft® Office Communicator - Computer Calls \(SIP Gateway\)](#) on page 166
  - i. [Normalizing phone numbers](#) on page 167

5. [Configuring Remote Call Control](#) on page 167
  - a. [Configuring the Call Server](#) on page 144
    - [Configuring the AML](#) on page 167
    - [Configuring the SIP CTI TR/87 ISM Limit](#) on page 168
    - [Configuring a station](#) on page 169
    - [Considering MADN \(Multiple Appearance DN\)](#) on page 170
    - [Configuring NRS](#) on page 170 (optional)
  - b. [Configuring the Signaling Server](#) on page 170
    - [Configuring Node Parameters](#) on page 171
    - [Configuring SIP Gateway Parameters](#) on page 172
    - [Configuring the DNS Server](#) on page 172
  - c. [Configuring SIP CTI Settings](#) on page 173
  - d. [Configuring SIP CTI Dial Plan Prefixes](#) on page 176
  - e. [Configuring SIP CTI CLID Parameters](#) on page 177
  - f. [Configuring Live Communications Server](#) on page 183
  - g. [Configuring Active Directory](#) on page 183
    - [Enabling the Remote Call Control Flag](#) on page 185
    - [Defining the Remote Call Control Controlled Line \(Device URI of the phone of the user\)](#) on page 187
    - [Defining the Remote Call Control SIP URI](#) on page 188
    - [Configuring the SIP URI Map](#) on page 188
  - h. [Configuring Microsoft® Office Communicator 2005](#) on page 189
    - [Configuring Phone Integration Settings](#) on page 190
    - [Configuring account details](#) on page 190
  - i. [Configuring CDR](#) on page 189
  - j. [Dialing E.164 International Format Numbers from Microsoft® Office Communicator - Phone Calls \(SIP CTI\)](#) on page 191
6. [Normalizing phone numbers](#) on page 192
  - a. [Normalizing Offline \(Recommended\)](#) on page 192
  - b. [Normalizing using the Address Book Service](#) on page 193
  - c. [Creating Normalization rules](#) on page 193
7. [Configuring SIP Routing and Redundancy](#) on page 197

- a. [Configuring Remote Call Control SIP Routing Using Phone Addressing](#) on page 198
  - b. [Configuring Remote Call Control SIP Routing Using a Gateway Endpoint Name](#) on page 198
  - c. [Configuring Redundancy](#) on page 199
8. [Deploying Live Communications Server Client PC application to end users](#) on page 199

---

## Installing CS 1000 components

The first step in the installation and configuration process is to install the CS 1000 and Signaling Server.

---

### Installing the Call Server

If you do not have a CS 1000 system installed and configured, refer to the following documents for detailed instructions:

- Avaya Communication Server 1000M and Meridian 1: Small System Installation and Commissioning (NN43011-310)
- Avaya Communication Server 1000M and Meridian 1: Large System Installation and Commissioning (NN43021-310)
- Avaya Communication Server 1000E: Installation and Configuration (NN43041-310)



**Important:**

PEPs, from the PEPs library, are required for both Call Server and Signaling Server installation for the Converged Office feature to operate.

Refer to the Avaya Converged Office Product Bulletin to ensure that you are using the most current versions of the Call Server and Signaling Server PEPs.

---

### Installing the Signaling Server

The Signaling Server must be installed. If it is not installed, refer to Avaya Signaling Server IP Line Applications Fundamentals (NN43001-125).

Configuring the Signaling Server is covered later in this chapter.

---

## Installing Microsoft Live® Communications Server components

After all CS 1000 components are installed, install the Microsoft® components, beginning with the Active Directory.

---

### Installing Active Directory

The Live Communications Server and Communicator 2005 environment have a strong dependency on Active Directory. Active Directory is used for authenticating, authorizing, provisioning, and configuring Live Communications Server 2005.

With Office Communicator 2005, Active Directory is also used to supply the enterprise address list to facilitate search-based lookups.

It is assumed at this stage that Active Directory is installed in accordance with Microsoft® documentation. For more information about Active Directory planning, refer to the *Live Communications Server 2005 Active Directory Preparation* document in the Deployment Resources area of the Microsoft® site:

<http://office.microsoft.com/en-us/communicationsserver/default.aspx>

---

### Installing Live Communications Server 2005 Service Pack 1 (SP1)

Following sections deals with Live Communication Server 2005 service pack 1 installation.

#### Microsoft® Office Live Communications Server 2005 Standard Edition

Live Communications Server 2005 Standard Edition provides a simple way to enable presence and IM services for small, simple networks. Standard Edition Server is completely self-contained and does not require Microsoft® SQL Server® 2000 to operate. It does; however, require Microsoft® Database Engine (MSDE).

## Microsoft® Office Live Communications Server Enterprise Edition

For deployments that require higher availability or a large degree of scalability, the concept of a Home Server is divided into two distinct parts:

- Live Communications Server 2005, Enterprise Edition (manages client connections, presence, and other real-time communication features like instant messaging)
- Live Communications Server 2005, Back-End Database (a back-end server, running Microsoft® SQL Server 2000 Service Pack 3a (SP3a), which can be clustered)

Together, the Enterprise Edition Server and the Back-End Database form a pool.

## Microsoft® Office Live Communications Server 2005 Enterprise Pool

Live Communications Server 2005, Enterprise pool is a collection of Enterprise Edition Servers that are connected to a central Live Communications Server 2005, Back-End Database.

Users (clients) register on an Enterprise pool. Users are directed to a specific server within the pool by a hardware load balancer that distributes the load to these servers. The load balancer exposes a single Virtual Internet Protocol (VIP) address that is used by the clients to access the pool. Each Enterprise Edition server within the pool is responsible for connection processing, security and authentication, protocol processing, and server applications. Static data, such as contact lists and access control lists (ACLs), are stored as persistent data on the Back-End Database Server.

A client can have multiple concurrent connection instances. A client can register on multiple servers at the same time. Each device to which the user is logged on (called an endpoint) can be connected through a different server at the same time.

The user data resides in the Back-End Database Server. The database contains records that hold static data and dynamic user data (such as endpoints and active descriptions for a user). The database runs a set of stored procedure calls that form the core of the operational software. Live Communications Servers within the pool are networked to the back-end server using a high-speed network. These Live Communications Servers also run User Replicator (UR) software to provide a connection to the Microsoft® Active Directory® directory service so that user account information can be synchronized between the Microsoft® Back-End Database Server and the Active Directory.

You can deploy Live Communications Server 2005 SP1 using one of the following methods:

- The deployment tool launched by Setup.exe. The deployment tool provides a set of wizards that guides you through each deployment task.
- Command-line tools provided on the Live Communications Server 2005 CD.

For more information about Live Communications Server 2005 SP1 installation, refer to the *Microsoft® Office Communicator 2005 Telephony Planning and Deployment Guide*, available at:

<http://office.microsoft.com/en-us/communicationsserver/default.aspx>

---

## Installing and configuring MCM

 **Important:**

If configuring for TLS, refer to [Configuring Transport Layer Security \(TLS\)](#) on page 201 for TLS-specific information.

---

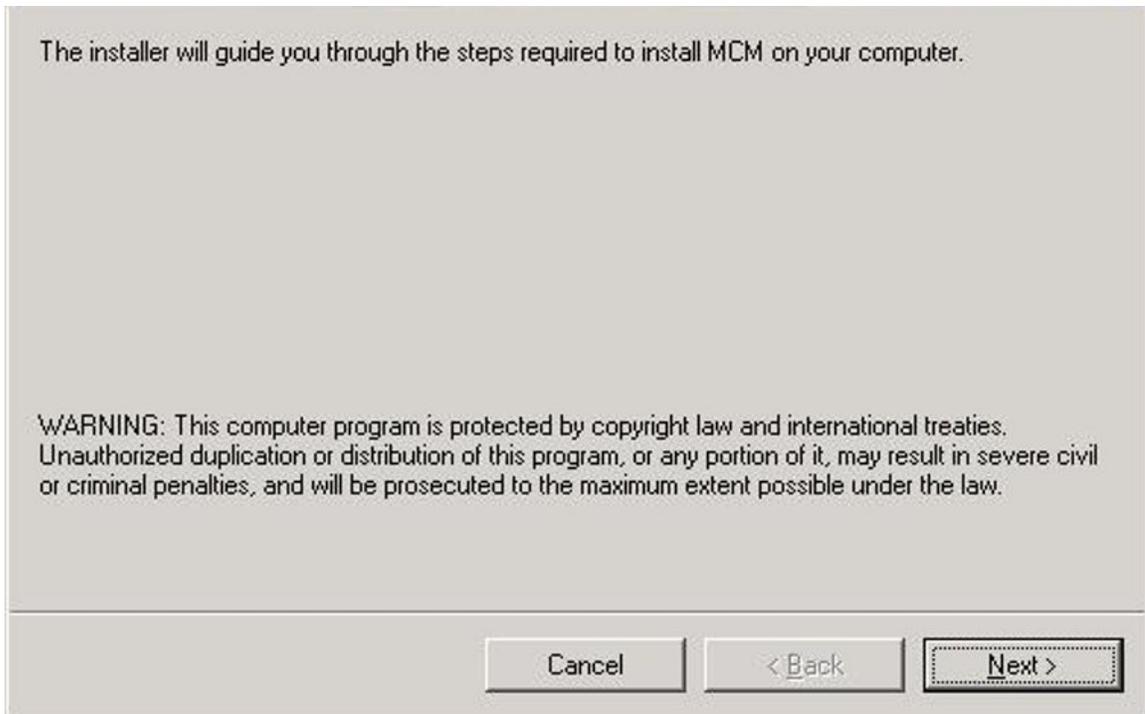
## Installing MCM software

 **Important:**

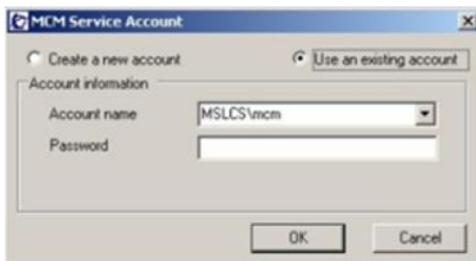
If upgrading to MCM 2.0, refer to [Upgrading MCM](#) on page 109.

MCM 2.0 software installation involves the use of a standard installation wizard. A domain user account is required for the installation (see [Figure 48: MCM Login](#) on page 107) of MCM. There are two options available to configure the domain account for MCM:

1. An Active Directory administrator can create the domain user account for MCM and provide the account name and password. After the account is created, run the MCM installation wizard and choose "use an existing account", and enter your user ID and password. The user account must be a member of the local "RTC Server Applications" and "RTC Local Administrators" groups. The user account must also have full control permissions on the MCM folder (c:\program files\Avaya\MCM by default).
2. Create the MCM domain user account from within the MCM installation wizard. To do this, the installer must be logged on to the server with a user ID, and granted the permissions to create users in the Active Directory. Run the MCM installation wizard and choose "create a new account".



**Figure 47: MCM Setup Wizard**

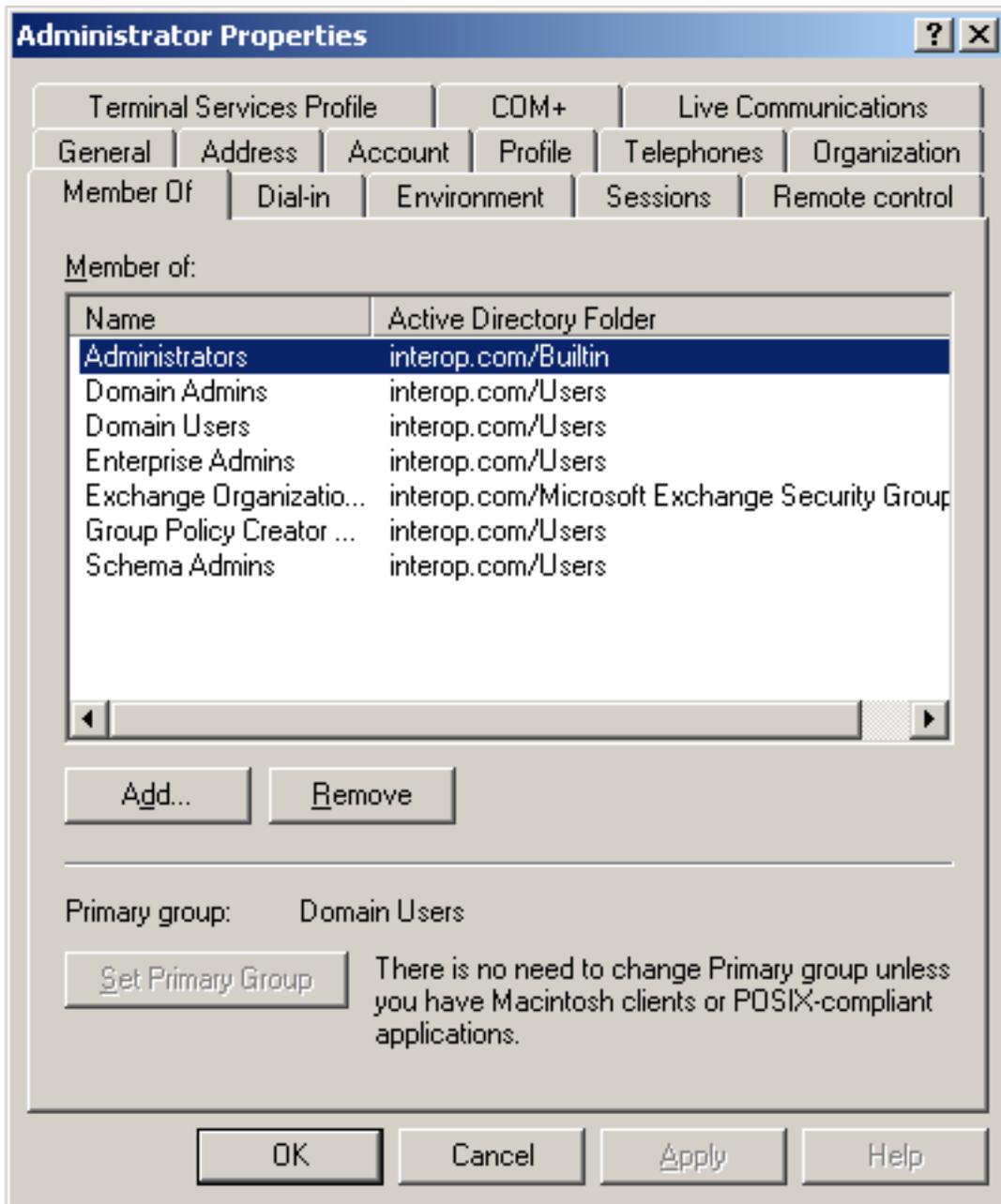


**Figure 48: MCM Login**

**! Important:**

[Figure 48: MCM Login](#) on page 107 shows the login screen for the MCM service account. The Account name is automatically entered by MCM.

[Figure 49: Member Of tab in Active Directory](#) on page 108 shows the "Member Of" tab in the Active Directory Administrator Properties window. This user is a member of the RTC Server Application



**Figure 49: Member Of tab in Active Directory**

MCM is installed on a Home Server for small deployments of 500 users or fewer with low traffic.

For large networks with multiple home servers or high traffic, MCM must run on top of a Live Communications Server Proxy to ensure Avaya support. This installation results in an easy deployment that can serve multiple Home Servers.

This installation also requires that you add a host authorization entry in the Application Proxy/ MCM Proxy for the Enterprise Edition pool fully qualified directory number (FQDN).

 **Important:**

A TLS connection is used between a Home Server pool and an Application Proxy.

MCM has two main components: **MCM Service**, which handles call processing, and **MCM Management Console**, which interfaces with the MCM Service component for configuration, administration, and maintenance.

 **Important:**

After the installation, open the MCM Console and start the MCM service.

## Uninstalling MCM

Use the Windows Add/Remove Programs utility to uninstall MCM. Be sure you stop MCM before you uninstall it.

## Upgrading MCM

Upgrading MCM involves uninstalling the old version of MCM and then installing the new version.

## Patching

Patching is supported by deploying an MCM up-issue. MCM uninstall/install is required for this up-issue.

---

## Configuring MCM

The Multimedia Convergence Manager (MCM) is one of the software components provided by Avaya to enable voice connectivity between CS 1000 clients and the Live Communications Server 2005 clients. MCM consists of the following modules:

- Call Processing Service
- Management Console

The MCM Call Processing Service handles the SIP telephony traffic between the CS 1000 and the Live Communications Server. The Management Console provides real-time status of the MCM, Live Communications Server, Primary NRS, and Secondary NRS. It also provides Administrative, Maintenance, and Configuration tools.

Microsoft® Live Communications Server 2005 SP1 provides multimedia and collaboration features such as Video, IM, Presence, White Board, Application Sharing, and VoIP capability. MCM enables the SIP VoIP connectivity between the CS 1000 and the Live Communications

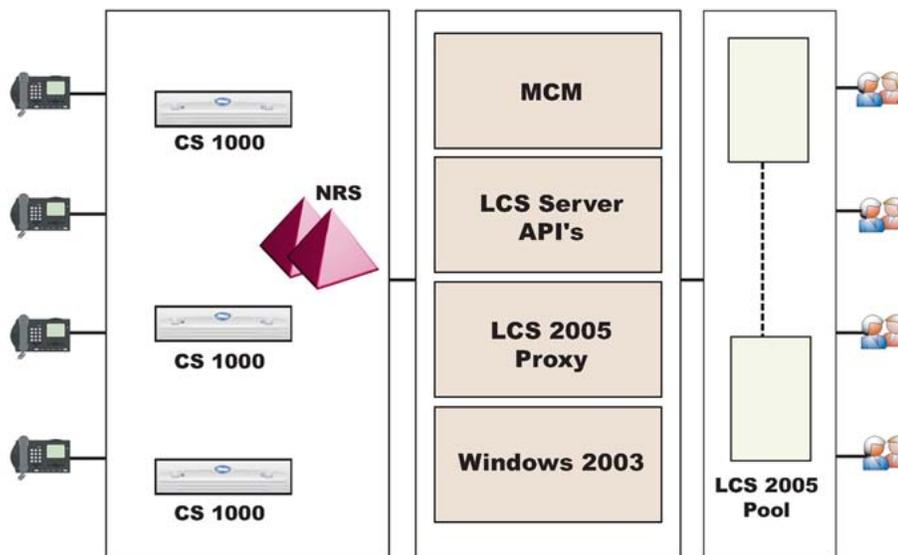
Server 2005 in addition to the TR/87 authorization functionality required for the Office Communicator 2005 Remote Call Control capability.

Telephones in a CS 1000 system can make direct SIP calls to Live Communications Server clients where the dialed number is mapped to the corresponding user ID using LDAP queries to the corporate Active Directory. MCM also allows the Live Communications Server clients to originate ESN and trunk calls to corporate and external users.

## MCM architecture

MCM resides between the Live Communications Server and the CS 1000. In the example, shown in [Figure 50: MCM architecture](#) on page 110, the MCM is running on top of a Live Communications Server 2005 Proxy which, in turn, is running on top of Windows 2003.

MCM can run on either an LCS Proxy or an LCS Home Server (in both Standard Edition or Enterprise Edition environments); however, the LCS Proxy is recommended in the case of Enterprise Edition for traffic/capacity purposes.



**Figure 50: MCM architecture**

The following examples illustrate how MCM handles call information. Understanding the role of MCM in the Telephony Gateway and Services component helps you determine how it must be configured.

### Example 1: Outgoing calls from Office Communicator

In this example, an invite travels from the client to the Live Communications Server Home Server and then on to the Live Communications Server MCM Proxy. MCM checks to see which NRS is active, and then sends an invite to that SRS. In this case, the invite is qualified. To return from the SRS, 302 is used.

The invite is now sent unqualified to the CS 1000 associated with the originator's location code and DN.

Example 2: incoming calls to Office Communicator with PCA

In this example, the user has a desktop telephone and a PCA pointing to a Live Communications Server 2005 server. The PCA sends a DN or Routing DN. The call was originally going to 6 231 3052, but the PCA hot key is configured with 6 344 5000. This is a "dummy" routing DN; it can be configured with all hot keys in the network.

In a CDP network, the dummy routing DN (for example, 6 231 3052) must also be configured by a DSC (for example, 82). The DSC is configured on the NRS as a routing entry for the MCM Gateway Endpoint.

The call is routed to the NRS. The invite is sent to the NRS, which returns a 302, and the CS 1000 sends an invite to the MCM Proxy. At this stage, look for a special header injected by the invite. That header, called x-nt-ocn, contains the actual number called. Use this header to compare against the Active Directory map for the user ID. This method is used to prevent you from having to program the hot key for each user to determine the correct DN upon which to terminate the call.

You need not configure each user. You need only configure the routing DN, and the header is automatically "injected" to identify the called party.

## MCM Direct configuration

For small CS 1000 deployments (without NRS), MCM supports Direct configuration. In this mode, MCM sends an invite from the client directly to the CS 1000 Node IP address specified in the MCM configuration.

### Note:

MCM does not check CS 1000 availability in Direct mode configuration.

### Note:

If you are using the MCM direct mode configuration, you must disable the G.729 codec on the media gateway controller if Office Communicator computer calls are deployed. Otherwise, if an originating computer mode user calls a phone mode user and the same phone mode user subsequently tries to conference a third computer mode user, the originating computer mode user's call drops (this scenario works for SPS and NRS).

For a complete description of the various MCM configuration screen fields, refer to [MCM Configuration screen](#) on page 114.

## The MCM management console

The following is a list of possible statuses for the various MCM components:

## MCM

- Running
- Pending
- Stopped

## LCS

- Running
- Pending
- Stopped

### Primary SRS/SPS (the IP address of the Primary SRS/SPS server)

- Active - Primary SRS/SPS is active. All messages are sent through the Primary NRS.
- Standby - Primary SRS/SPS is alive. The Secondary SRS/SPS is active.
- Not responding - Primary SRS/SPS is not responding. For normal processing, the Secondary SRS/SPS must be switched to Active state.
- Unknown - An unknown response is received by the SRS or SPS.

### Secondary SRS/SPS (the IP address of the Secondary SRS/SPS server)

- Active - Secondary SRS/SPS is active, which is possible only if the Primary SRS/SPS is down.
- Standby - Secondary SRS/SPS is alive, which is the normal state if the Primary SRS/SPS is active.
- Not responding - Secondary SRS/SPS is not responding. It is not possible to switch to it.
- Unknown - An unknown response is received by the Secondary SRS or SPS.

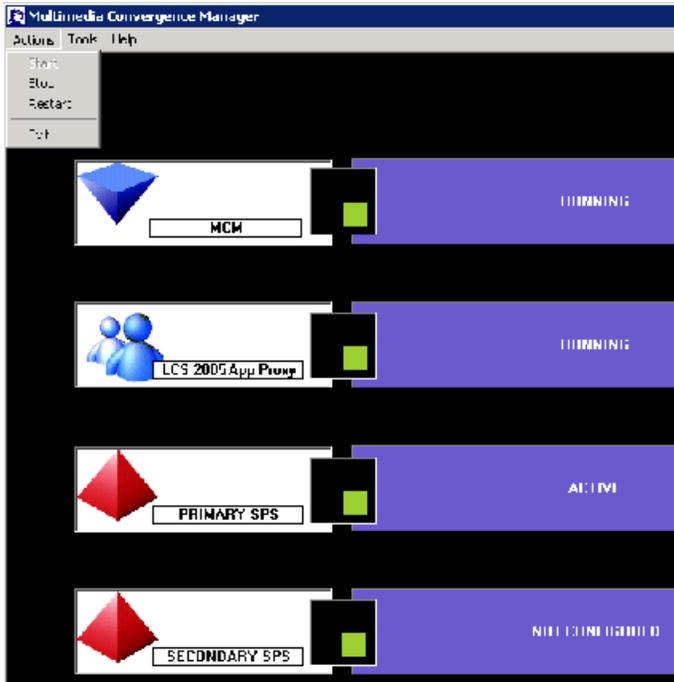


Figure 51: MCM Management Console

## MCM menu options

MCM has three menu options: Actions, Tools, and Help. The following describes the function of each menu item:

Actions menu:

- Start - start MCM service
- Stop - stop MCM service
- Restart - stop and start MCM service
- Exit - close current GUI for MCM service.

Tools menu:

- Configuration
- Active Calls Count
- Active Directory Query
- Backup
- Restore
- Set Log Level

Help menu:

Get Help information and general information about MCM.

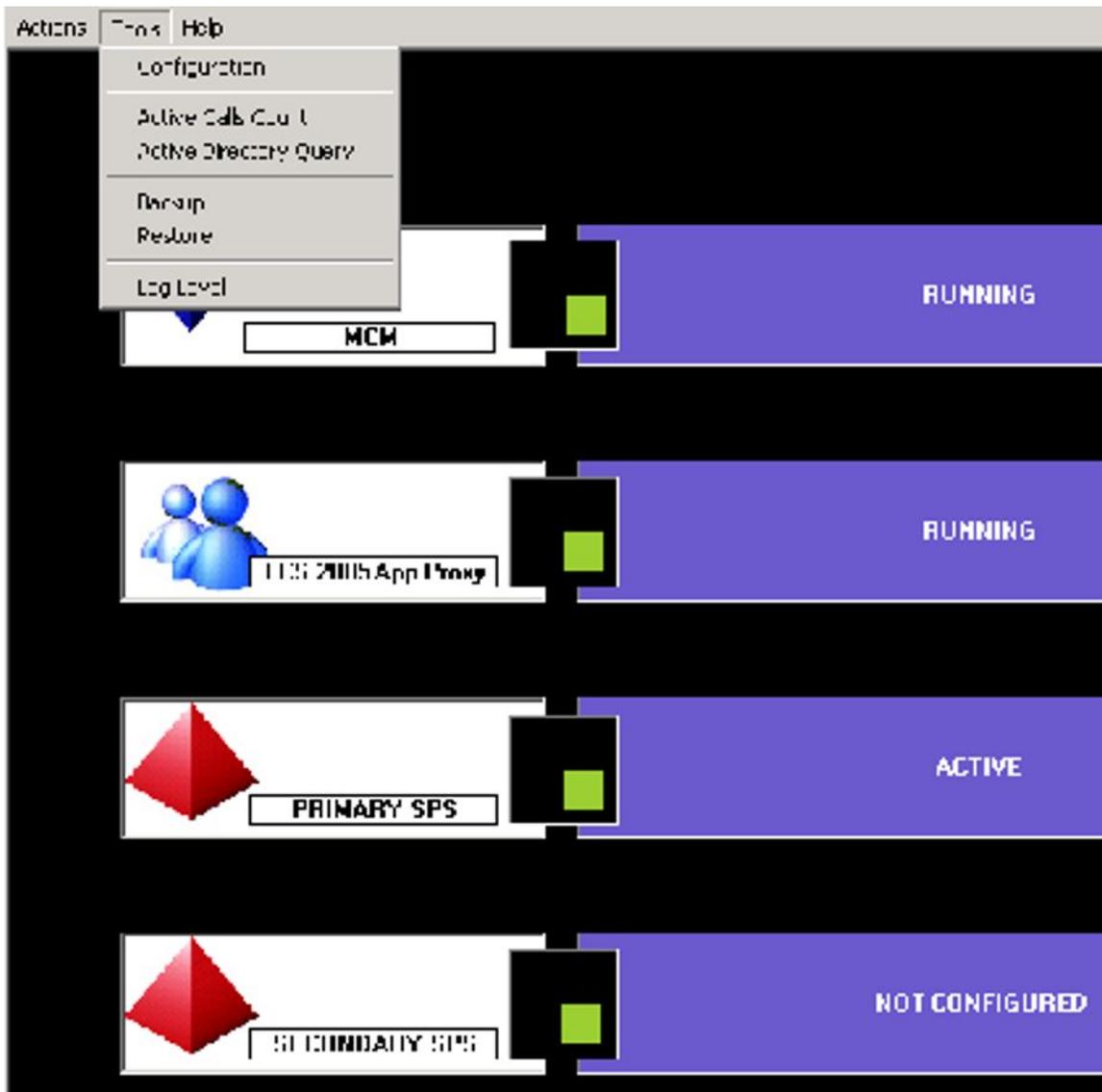


Figure 52: MCM menu options

## MCM Configuration screen

This section describes the various fields in the MCM Configuration screen ([Figure 53: MCM Configuration](#) on page 115).

The screenshot shows the MCM Configuration dialog box with the following settings:

- SIP Routing:**
  - SRS
  - SPS
  - Direct
  - Primary IP: 47.11.150.117
  - Secondary IP: 0.0.0.0
  - Mode: Proxy/All
  - CS1000 SS Node IP: 47.11.150.189
  - Transport: TCP, Port: 5060
- Registration:**
  - ID: elevance-clab03
  - IP: 47.11.157.112
- Active Directory Configuration:**
  - Query Server, Synchronize at: 03:00
  - Local Cache, Synchronize Now
  - Local Cache then Query Server
  - Non Default AD/LDAP Server
  - Server IP: 0.0.0.0, Port: 389
- Active Directory Mapping:**
  - Phone Field: telephoneNumber
  - Phone Format: ESN ???-????
- Incoming Call Processing Parameters:**
  - Called Phone Context: ucdp
  - Called Phone Prefix Delete: 0
  - Called Phone Prefix Inset:
  - Caller Phone Prefix Delete: 0
  - Caller Phone Prefix Inset: 6
- Outgoing CLID Number Parameters:**
  - Prefix Delete: 0
  - Prefix Inset:
- Outgoing CLID Name Parameters:**
  - Extract Last-First Data
  - Switch Last-First Order
  - Remove Last-First Comma Separator
- SIP-CTI Authorization:**
  - Enable Authorization

Figure 53: MCM Configuration

**! Important:**

MCM supports only SRS mode in a collaborative setup.

The SIP Routing options are SIP Redirect Service (SRS), SIP Proxy Server (SPS), and Direct. If you have only one system (as opposed to a network), select Direct and enter the CS 1000 IP address to point directly to the CS 1000 (the Node IP of the SIP CTI Signaling Server).

**\* Note:**

The name configured on the SRS/SPS (Gateway endpoint) and the name entered inside the MCM configuration file must match. The name is case sensitive.

**\* Note:**

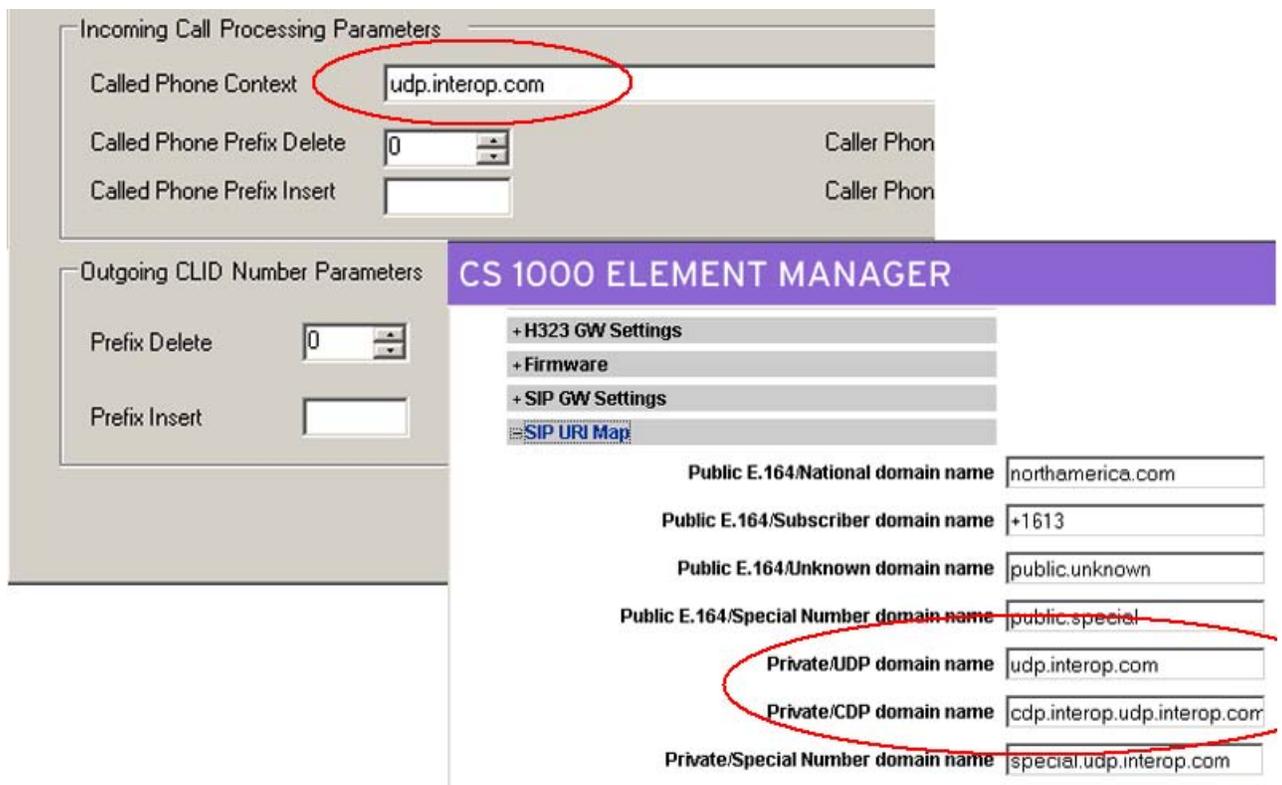
The MCM requires access rights to certain directories (for example: “Program Files/MCM...”). Ensure that the user has the Administrators rights to these directories.

**\* Note:**

When TCP is used, the Port must be configured to 5060. For TLS, the Port number is 5061. For additional information, see [Port usage](#) on page 70.

**! Important:**

The Called Phone Context entry in the MCM Configuration screen and the entries for UDP and CDP in the Signalling Server Element Manager must be the same, as shown in [Figure 54: Element Manager SIP URI MAP](#) on page 116. Entries are case sensitive.



**Figure 54: Element Manager SIP URI MAP**

Registration ID can be configured in two forms:

1. End\_Point\_Name@Service\_Domain\_Name, where End\_Point\_Name is the MCM End Point Name configured on the NRS and Service\_Domain\_Name is the service domain name configured on the NRS where the MCM End Point belongs.

**Note:**

@Service\_Domain\_Name is included if the SIP domain of the LCS does not match the SIP service domain of the NRS.

2. End\_Point\_Name, where End\_Point\_Name is the MCM End Point Name configured on the NRS. In this case, the first domain name served by Live Communications Server (configured in the properties of the domain forest of the Live Communications Server snap-in) is used by MCM.

If you choose the NRS, then this justifies the registration ID of the MCM. Imagine the MCM as another CS 1000 endpoint in the network. The MCM requires a registration IP ID and IP (if that the server runs as multiple IPs, you need to specify which IP).

**Important:**

Authentication is not supported for MCM configuration in the NRS.

**Active Directory Mapping :** The Active Directory Mapping field allows you to define which phone field you use for mapping. In the Active Directory, a user may have a business phone number, an IP phone number, and so on. This field defines which phone you are using. For the Phone Format field, the actual phone number stored in the Active Directory can be similar to the format in [Figure 53: MCM Configuration](#) on page 115. The format in this field must match the format in Active Directory exactly to correctly map the phone number for incoming calls.

Digits received by MCM from a CS 1000 are mapped into ??????? fields—for example, the number 3546714 maps into ESN 354-6714 for lookup in the Active Directory Phone Field. There are two main formats in Active Directory Mapping: UDP and CDP. For example:

- with UDP, if the Phone Field contains numbers like ESN 354-6714, the Phone Format field must be ESN ???-????.
- with CDP, if the Phone Field contains numbers like 6714, the Phone Format field must be ????

There are two modes for Active Directory Configuration: Realtime or Local Cache. Realtime mode is used for end-user ID mapping, which requires an LDAP query. Local Cache mode involves caching the Active Directory on the MCM server and using that cache information for queries.

This cache updates every day by default at the same time. You can force it to synchronize by clicking the Synchronize Now button.

**Important:**

Microsoft® recommends placing a GC Controller inside every network site. Avaya's GC LDAP server contains about 50 000 user records. The synchronization with local GC takes about 20-25 seconds. The GC LDAP server provides access to the Active Directory Global Catalog (GC) through the Lightweight Directory Access Protocol (LDAP). If the user is unfamiliar with GC, it is preferable to leave the default values in place.

The Local Cache is then used for mapping. The Non Default Active Directory/LDAP Server option is used for non-default active directories configured for Windows 2003 and Live Communications Server deployment.

By default, MCM uses the GC LDAP server, which contains partial information about all objects in the Active Directory domain forest. The GC LDAP server requires replication from all Domain controllers to the GC domain controller to be performed after changes made in the Active Directory User's configuration (the Active Directory Sites and Services snap-in).

The non-default LDAP server configuration may be used to:

1. specify GC LDAP server (the Port field is 3268 or blank) if there are multiple GC Domain Controllers in the Active Directory forest and only this server must be used.
2. specify non-GC LDAP server to reduce the search scope to only one domain.

### **Enabling propagation of any field to the Global Catalog**

MCM uses the Active Directory Global Catalog to search for necessary user information. However; by default, this Global Catalog contains few Active Directory fields that can be used for MCM, (for example, "otherTelephone").

To enable this field, so it can be propagated to the Global Catalog, the current schema used by Active Directory must be updated. There are a number of utilities that can perform this task, as described in the following link:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/24311c41-d2a1-4e72-a54f-150483fa885a.mspx>

The "isMemberOfPartialAttributeSet" field of the attribute is responsible for propagation. If configured to "TRUE", the attribute is propagated to Global Catalog during replication.

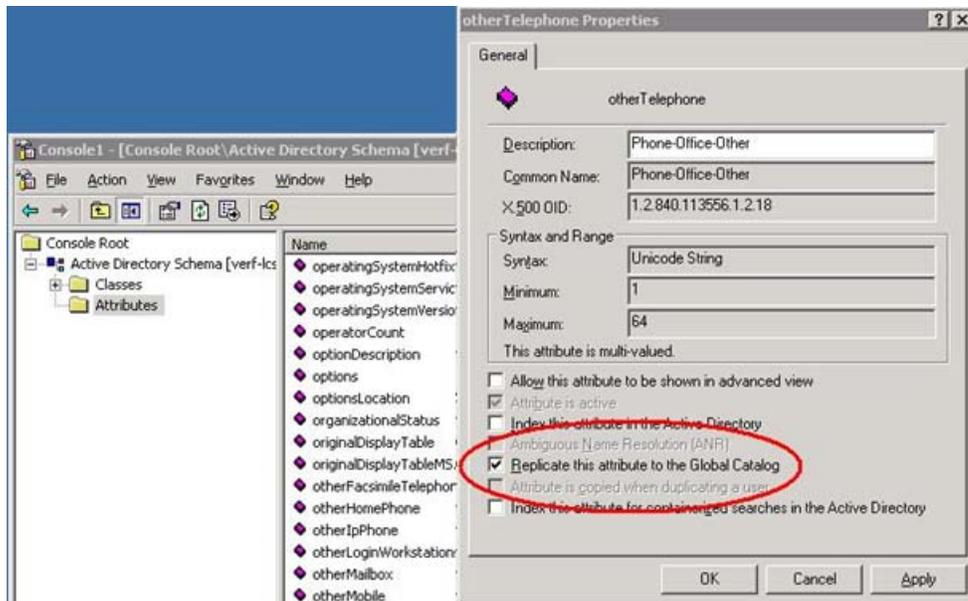
Active Directory Schema snap-in - The Active Directory Schema snap-in is not a default MMC (Microsoft Management Console) snap-in provided with Windows Server 2003. To make it appear in the list of available snap-ins, install the Windows Server 2003 Administration Tools Pack (Adminpak.msi). To register the Active Directory Schema snap-in, run Regsvr32 Schmmgmt.dll from the command prompt or from the Run command on the Start menu.

Another option is to execute the command mentioned above, "Regsvr32 Schmmgmt.dll", then run "mmc" and select the File > Add/Remove snap-in menu item. Click Add, then select Active Directory Schema. Click Add, then Close>OK.

To enable the replication of an attribute to the Global Catalog, use the following procedure:

### **Enabling replication to the Global Catalog**

1. Open the Active Directory Schema snap-in (see [Figure 55: Replicating attributes to the Global Catalog](#) on page 119)
2. Select Attributes on the left pane.
3. Right-click the necessary field ("otherTelephone" in this example)
4. Select Property menu item.
5. Enable Replicate this attribute to the Global Catalog .
6. Click OK.



**Figure 55: Replicating attributes to the Global Catalog**

Active Directory Query - The Active Directory Query tool allows users to check Active Directory mapping configuration. It searches for a user-id (SIP URI) by a given phone number, and vice versa. This tool is only used for maintenance, and emulates the same algorithm that is used by the MCM service in run-time.

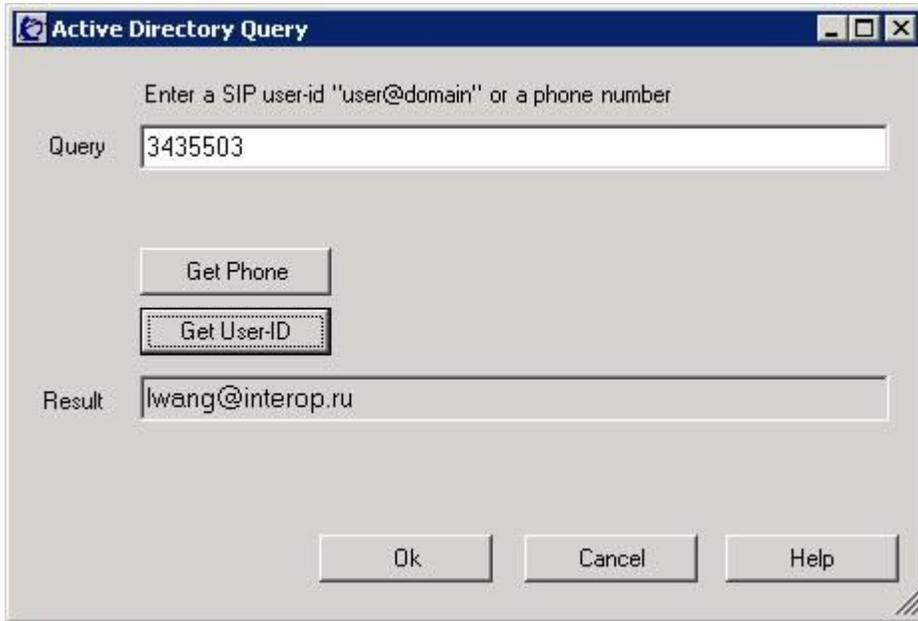
For example: user Chris Smith is defined in the Active Directory as:

SIP URI: sip:csmith@interop.com

Telephone number: ESN 354-6714

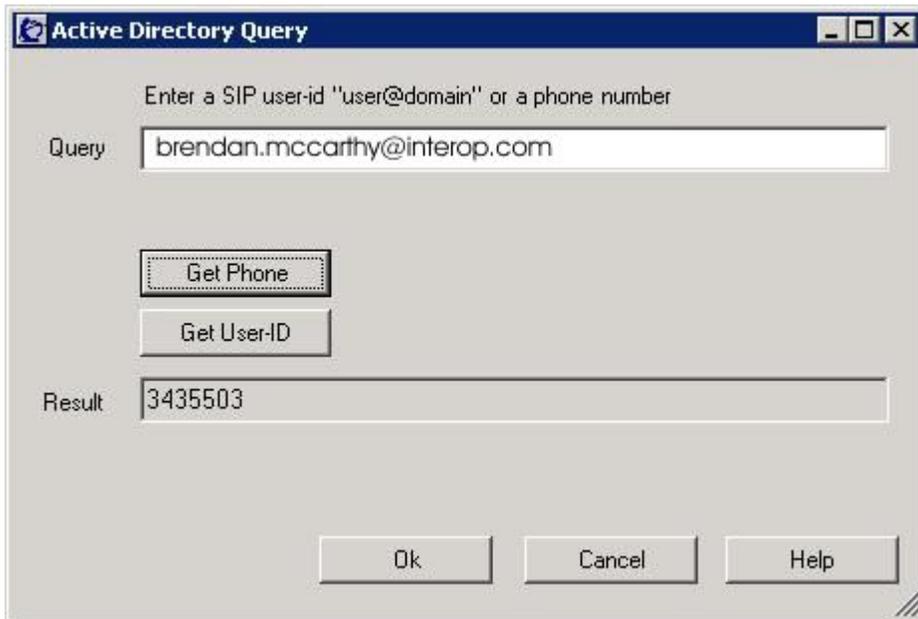
The phone format is defined as ESN ???-???? in MCM configuration.

If you type the phone number in the Query field and press Get SIP URI button, the SIP URI appears in the Result field (as shown in [Figure 56: Get SIP URI](#) on page 120).



**Figure 56: Get SIP URI**

If you type the SIP URI in the Query field and press the Get Phone button, the Telephone number appears in the Result field (see [Figure 57: Get phone](#) on page 120).



**Figure 57: Get phone**

Incoming Call Processing Parameters - This option refers to incoming CS 1000 calls to MCM that terminate on Office Communicator. You must specify the phone context. When the phone context is defined, mapping is performed (using CDP or UDP). In the case of a large network, the phone context used is UDP, while CDP is used for small networks. You can use Call Phone

Prefix Delete and Insert fields to manipulate digits received from the CS 1000 prior to mapping.

This manipulation is generally not necessary, but is available in case a scenario requires this type of manipulation. The Caller Phone Prefix Delete and Insert is used when Office Communicator maps to a user ID. When a CS 1000 telephone calls MCM and then Office Communicator, a pop-up window appears, and that pop-up displays the caller's user ID. This pop-up takes place on Office Communicator, and results from mapping the caller phone number to a user ID.

The origin of this mapping is the From header in the invite that comes to MCM and then to Office Communicator (for example, Office Communicator cannot map a number like 343 8888, because those numbers are normalized and stored in Office Communicator in the following format: X 343 8888 (a dialable number). In this scenario, insert 6 so that it matches a dialable number. Office Communicator can then map it to a user ID. So, when A calls B on a CS 1000 , and the call terminates on the Live Communications Server, Office Communicator can see who originated the call. B answers the call from A, and after the connection is established, B can also use IM, whiteboard, and other tools to communicate with A.

This information is configured on the Signaling Server and the NRS. For more information, refer to [URI Mapping](#) on page 156.

You can inject identity headers for calls going from Office Communicator to a CS 1000 . Then, when a call is made from Office Communicator to a CS 1000 IP Phone, you see the Calling Line ID (CLID) number and name. The first field, Prefix Delete, is not used often, but is available in case a CLID number needs to be manipulated.

Outgoing CLID Name Parameters manipulate the name string to display the name on a CS 1000 IP Phone in the desired format. The name must be defined in the Active Directory in the following format: Last, First [additional info].

This field extracts the Last and First names and removes the rest from the name string.

This field switches the order of the Last and First names in the name string.

Switch Last-First Order This field switches the order of the Last and First names in the name string.

Remove Last-First Comma Separator This field removes the comma separator between the Last and First names.

TR/87 Authorization TR/87 Authorization enables the authorization of the TR/87 (SIP-CTI) INVITEs from the Office Communicator to ensure that an Office Communicator user has control only over their own phone (as defined in Active Directory).

## Configuring MCM for Remote Call Control

For Remote Call Control, the Avaya MCM application that resides within the Live Communications Server domain provides support for authorizing TR/87 service requests and redundancy.

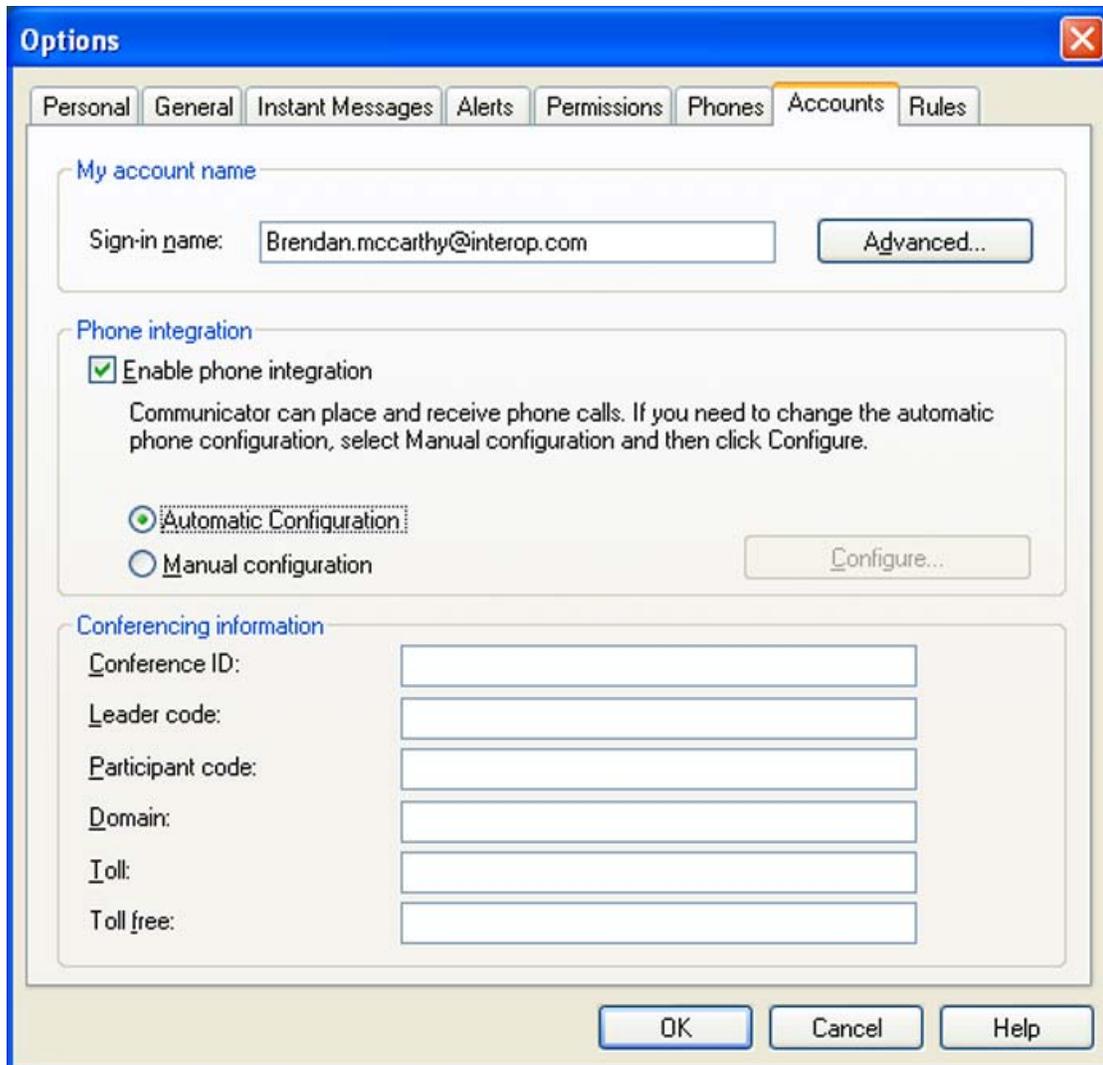
Authorization of TR/87 service - MCM supports authorization of Remote Call Control service requests from Microsoft® Communicator clients. The following is a summary of the authorization algorithm:

1. The SIP INVITE "from" header provides the Requestor Identity (for example, the Live Communications Server user identity).
2. The CSTA XML message provides the Controlled Device Identity (for example, the phone URI).
3. The Owner Identity is found by a reverse lookup using the Controlled Device Identity found in Step 2 as a query to Active Directory (Search Active Directory, Find the User whose msRTCSIP-Line equals "Controlled Device ID", then find the msRTCSIP-PrimaryUserAddress of that User).
4. If a result is found in Step 3, the Owner Identity is equal to the Requestor Identity, and msRTCSIP-OptionFlags (RCC bit - 5th bit) is configured to equal 1, then approve the request. Otherwise, reject the request.

The primary function of MCM (when authorization is enabled, see [Figure 58: Enable phone integration](#) on page 123) is to ensure that an Office Communicator user can use Remote Call Control only for the phone URI, and that Remote Call Control SIP URI is configured in Active Directory for that user by the system administrator. Placing control in the hands of the system administrator is necessary in environments where users must not override their phone integration configuration through the manual phone integration option in Office Communicator.

 **Note:**

Disabling TR/87 authorization on the MCM is strongly discouraged. When this functionality is disabled, users can override their active directory configuration and control any DN in the system that is provisioned to support SIP CTI.



**Figure 58: Enable phone integration**

Redundancy of the TR/87 interface is not provided natively with Live Communications Server 2005. Office Communicator does not support multiple Remote Call Control SIP URIs or SIP 300/302 redirection messages. To provide for redundancy of the TR/87 interface, the Avaya MCM application uses the redundancy of NRS and multiple FE endpoints.

## Select component for configuration

If you have elected to configure Telephony Gateway and Services, continue reading. If, however, you are configuring for Remote Call Control, proceed to [Configuring Remote Call Control](#) on page 167.

---

## Configuring Telephony Gateway and Services

This section describes the process you must follow to properly configure the Telephony Gateway and Services component.

---

## Configuring Live Communications Server

The starting point for Telephony Gateway and Services configuration is the Live Communications Server 2005 component.

### Group Policy

For Telephony Gateway and Services to operate properly, each Office Communicator 2005 user's group policy must have Computer-to-Phone calling enabled (see [Figure 59: Group policy settings](#) on page 125). Procedure 2 in [Enabling a group policy](#) on page 125 describes the process required to add/change a group policy.

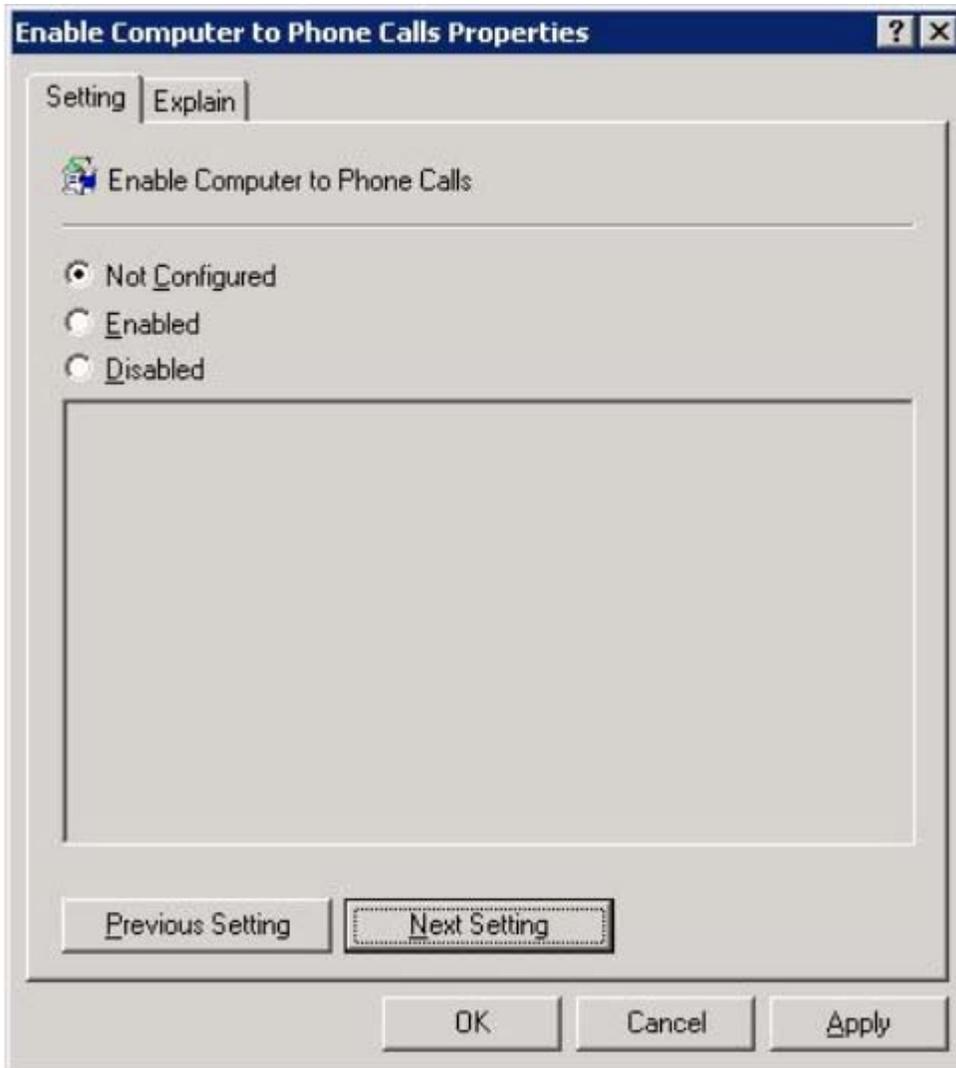
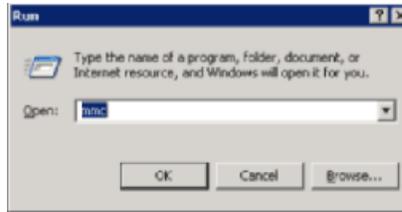


Figure 59: Group policy settings

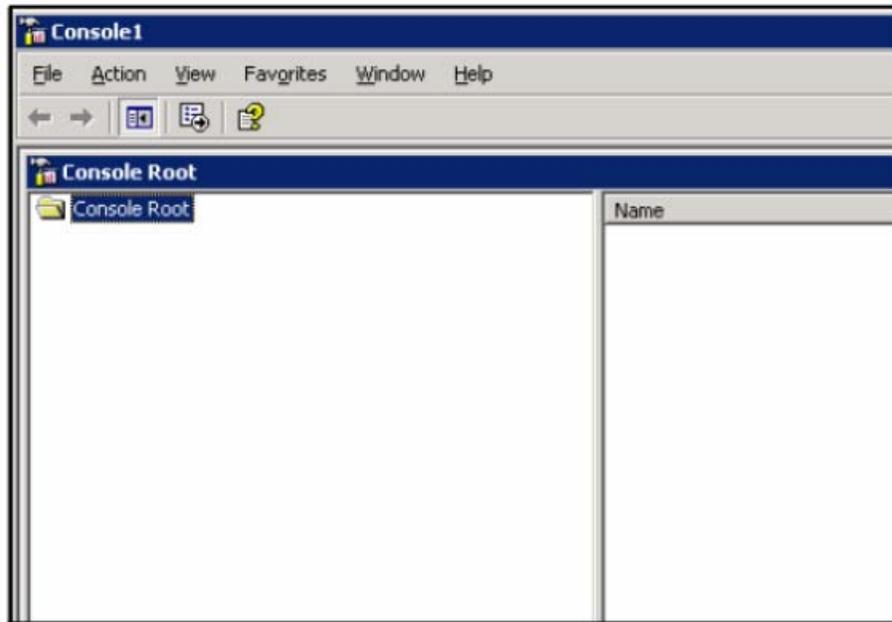
### Enabling a group policy

1. On the Communicator Installation CD (in the same directory as the Communicator.msi file or on the trial version), install Communicator.adm in the C:\Windows\inf directory. The Communicator.adm file must be stored where it is easy to find. In many cases, C:\Windows\inf is the first directory the group policy editor checks, but results may vary.
2. Choose Start/Run > MMC (see [Figure 60: Start/Run](#) on page 126)



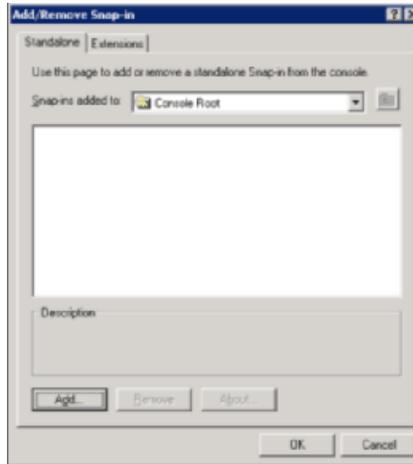
**Figure 60: Start/Run**

3. Choose File > Add-remove snap-in for Console1.



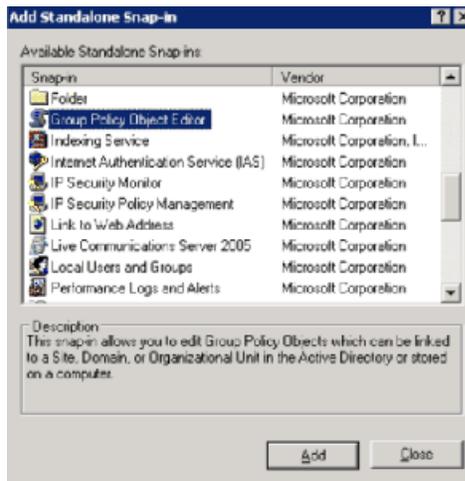
**Figure 61: Console 1**

4. Select Console Root from the "Snap-ins added to" menu (see [Figure 62: Add/Remove Snap-in](#) on page 127 ).
5. Click Add.



**Figure 62: Add/Remove Snap-in**

6. Select Group Policy Object Editor and click Add (see [Figure 63: Add Standalone Snap-in](#) on page 127).



**Figure 63: Add Standalone Snap-in**

7. The Group Policy object must be the local computer and handled on a per-computer basis. It is recommended that group policies also be handled on a per-domain basis (as shown in [Figure 64: Select Group Policy Object](#) on page 128). Click Finish and then Close.



Figure 64: Select Group Policy Object

8. Click OK, with the local computer policy showing as “added” (see [Figure 65: Add/Remove Snap-in](#) on page 128).

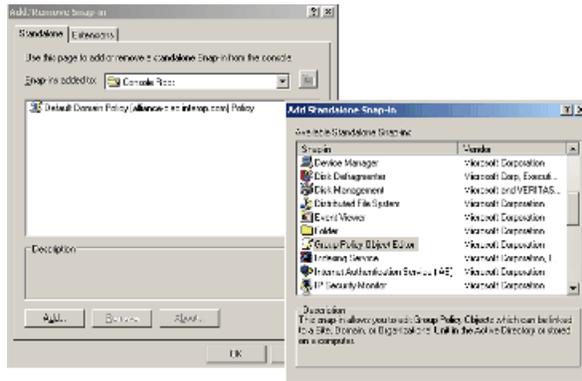


Figure 65: Add/Remove Snap-in

9. In the Console Root frame (see [Figure 66: Console Root](#) on page 128), expand the Local Computer Policy. Expand Computer Configuration and right-click Administrative Templates. Select Add/ Remove Templates.

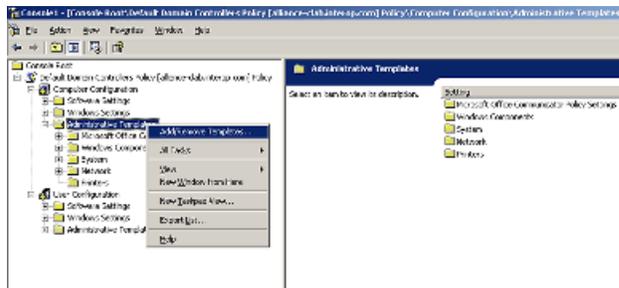
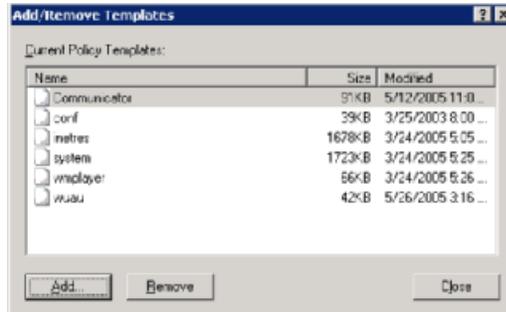


Figure 66: Console Root

10. Click Add.



**Figure 67: Add/Remove Templates**

11. Go to C:\Windows\inf (or the alternate location chosen to store the file), select Communicator.adm and click Open.



**Figure 68: Console Root**

12. In the Console Root frame, the Administrative Templates have a new subfield. To access this new subfield, expand Local Computer Policy > Computer Configuration > Administrative Templates > Microsoft Office Communicator Policy Settings (see [Figure 68: Console Root](#) on page 129).
13. Click Microsoft Office Communicator Feature Policies.
14. In the frame on the right, right-click Prevent Video Calls and select Properties. Click Disable > Ok.
15. Right-click Prevent Computer to Computer Audio Calls and select Properties. Click Disable > Ok.
16. Right-click Enable Computer to Phone Calls and select Properties. Click Enable > Ok.
17. Right-click Prevent Collaboration Features and select Properties. Click Disable > Ok.
18. Right-click Enable Phone Control and select Properties. Click Enable > Ok.
19. Right-click Disable Call Presence and select Properties. Click Disable > Ok.
20. All other features must be configured to “Not configured” at this time.
21. Close the Console Root window. When asked to save Console1 settings, click No. The settings are saved to the registry; there is no need to save them to an external file.

**! Important:**

In order for SIP Gateway Office Communicator-to-SIP Gateway Office Communicator video calls to work, the group policy for "Specify encryption for computer-to-computer audio and video calls" must be enabled and match for

Office Communicator clients. To enable these calls, select Enabled, in the Policy tab. In the How to handle encryption: menu, select Don't support Encryption (see [Figure 69: Specify encryption for computer-to-computer audio and video calls](#) on page 130).



Figure 69: Specify encryption for computer-to-computer audio and video calls

## Live Communications Server configuration procedures

For the specific Live Communications Server configuration procedures, refer to the Live Communications Server 2005 Deployment Resources page on the Microsoft® site:

<http://office.microsoft.com/en-us/communicationsserver/default.aspx>

On the Microsoft® Office web site, search on **Assistance > Live Communications Server 2005 Deployment Resources**. On the results page, select the **Live Communications Server 2005 Deployment Resources** link.

## Configuration of Static Routes on all intermediate Live Communications Servers

Configuration of the Live Communications Server involves the configuration of static routes on the Live Communications Server, and configuration of host authorization.

You must configure static routes between the client and server. For information about configuring static routes (Enterprise Edition pool behind a Load Balancer), see *Live Communications Server 2005 Planning Guide*, and the *Live Communications Server 2005 Enterprise Edition Deployment Guide* on the Microsoft® site:

<http://office.microsoft.com/en-us/communicationsserver/default.aspx>

Routing configuration on Live Communications Server 2005 servers - When a call is made using Office Communicator, the home server needs to know where to route the call (for example: is it routed to another Live Communications Server proxy?). The route must be defined using the Routing tab (see [Figure 70: Routing configuration on Live Communications Server 2005 servers](#) on page 131). When it terminates on the proxy, the MCM handles the routing by performing a check to determine which NRS is active (usually the primary NRS), and then sends an invite to the active NRS. At this point, it receives a 302 and redirects the call to the correct CS 1000 .

**\* Note:**

In small deployments where there is only one Live Communications Server, and it is running MCM, routing entries are not required.

**\* Note:**

Blind transfers from Office Communicator are possible only if the number dialed has previously been added to the NRS routing entries.

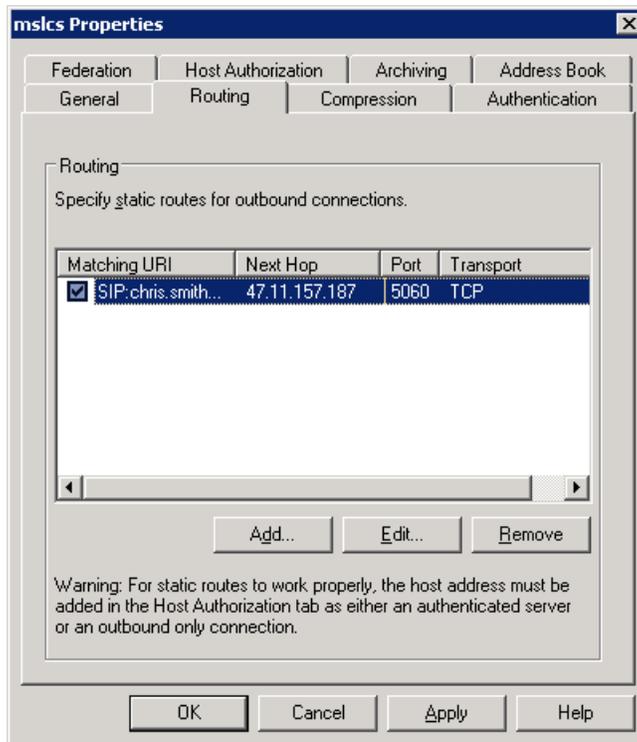


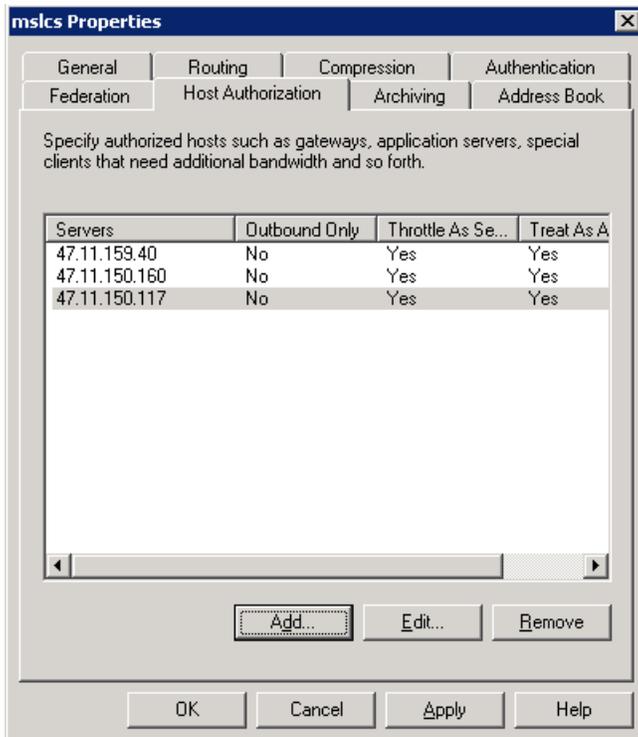
Figure 70: Routing configuration on Live Communications Server 2005 servers

## Configuring Host Authorization and Routing

For one Live Communications Server to communicate with another Live Communications Server, each Live Communications Server must have authorization to speak to the other. The Host Authorization page (see [Figure 71: Host Authorization: Live Communications Server-Live Communications Server, Live Communications Server-CS 1000](#) on page 132) is where you establish this authorization.

**! Important:**

Adding the FQDN of the CS 1000 to the Authorized Host list will only work when a TLS connection is used. Otherwise, the IP address of the CS 1000 must be added to the Authorized Host list.



**Figure 71: Host Authorization: Live Communications Server-Live Communications Server, Live Communications Server-CS 1000**

The Host Authorization page (found in a Live Communications Server running MCM), is where all CS 1000 endpoints are configured. These endpoints must be configured as authorized endpoints in the Live Communications Server MCM Proxy. Configure the CS 1000 IP addresses which, in turn, talk to the Live Communications Server. The same authorization must take place for both Live Communications Server to Live Communications Server authorization and Live Communications Server to CS 1000 authorization.

There are a number of rules that must be followed for Host Authorization.

For the Application Proxy:

1. Add the Home Server as an Authorized Host (and only if not using TLS). Add the Node IP of the CS 1000 (for example: 47.11.159.40). Add the SPS or SRS (for example: SPS IP: 47.11.150.160, SRS IP: 47.11.150.117). All must have "Treat as Authenticated" checked.

2. Add the following rule (for Standard Edition):

SIP:\*@\*;USER=PHONE Next Hop: Home Server

For example: SIP:\*@\*;USER=PHONE Next Hop: alliance-clab03.interop.com, Transport TLS, OR: alliance-clab03.interop.com, Transport TCP, OR: 47.11.159.112, Transport TCP.

This rule is for routing Telephony Gateway (SIP Gateway) calls.

For the Home Server:

1. Add the Application Proxy as an authorized host ONLY (and only if not using TLS) with "Treat as Authenticated" checked
2. Add the following two rules (for Standard Edition LCS):

- Rule 1: SIP:\*@\*;USER=PHONE Next Hop: The Application Proxy (for example: SIP:\*@\*;USER=PHONE Next Hop:alliance-clab04.interop.com, Transport TLS, OR: alliance-clab04.interop.com, Transport TCP, OR: 47.11.157.187, Transport TCP.

This rule is for routing Telephony Gateway calls (SIP Gateway).

- Rule 2: SIP: CS 1000 SIP Address Next Hop: The Application Proxy. For example: SIP: 1156\_SS1@interop.com Next Hop:alliance-clab04.interop.com, Transport TLS, OR: alliance-clab04.interop.com, Transport TCP, OR: 47.11.157.187, Transport TCP.

This rule is for routing Remote Call Control calls (SIP CTI).

For each Live Communications Server running MCM, Host Authorization is required for the Node IP address of all CS 1000 servers the Live Communications Server interacts with, as well as the TLAN IP address of the Primary, Secondary, and all possible collaborative NRS.

The following table contains a number of possible configurations of LCS and the required entries for each.



**Important:**

The transport to CS 1000 is TCP for all configuration types.

**Table 6: Routing rules**

Configuration Type	Component	Host-Authorization	Destination	User / Domain	Phone URI	Transport	Port
1. Single LCS Server	Single LCS Server	NRS and Node IP of CS 1000	NONE				
2. Home Server & Application Proxy, TLS Link	Home Server	Application Proxy FQDN	Application Proxy FQDN	* / *	YES	TLS	5061
			Application Proxy FQDN	CS 1000 SIP address	NO	TLS	5061
	Application Proxy	NRS and Node IP of CS 1000 ,	Home Server FQDN	* / *	NO	TLS	5061

Configuration Type	Component	Host-Authorization	Destination	User / Domain	Phone URI	Transport	Port
		Home Server FQDN					
3. Home Server & Application Proxy, TCP Link	Home Server	Application Proxy IP	Application Proxy IP	* / *	YES	TCP	5060
			Application Proxy IP	CS 1000 SIP address	NO	TCP	5060
	Application Proxy	Home Server IP, NRS and Node IP of CS 1000	Home Server IP	* / *	NO	TCP	5060
4. Pool of Home Servers & Single Application Proxy, TCP Link	Home Servers Pool	Application Proxy IP, Load Balancer IP	Application Proxy IP	* / *	YES	TCP	5060
			Application Proxy IP	CS 1000 SIP address	NO	TCP	5060
	Application Proxy	Home Servers IP, Load Balancer IP, NRS and Node IP of CS 1000	Load Balancer IP	* / *	NO	TCP	5060
5. Pool of Home Servers & Single Application	Home Servers Pool	Application Proxy FQDN	Application Proxy FQDN	* / *	YES	TLS	5061

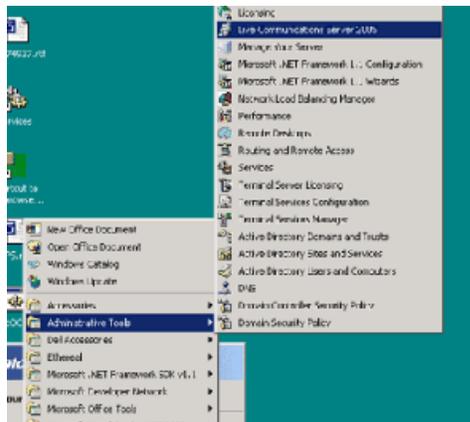
Configuration Type	Component	Host-Authorization	Destination	User / Domain	Phone URI	Transport	Port
Proxy, TLS Link							
			Application Proxy FQDN	CS 1000 SIP address	NO	TLS	5061
	Application Proxy	Load Balancer FQDN, NRS and Node IP of CS 1000	Load Balancer FQDN	* / *	NO	TLS	5061
6. Single Home Server & Pool of Application Proxy, TCP Link	Home Server	Application Proxies IP, Load Balancer IP	Load Balancer IP	* / *	YES	TCP	5060
			Load Balancer IP	CS 1000 SIP address	NO	TCP	5060
	Application Proxies Pool	Home Server IP, Load Balancer IP, NRS and Node IP of CS 1000	Home Server IP	* / *	NO	TCP	5060
7. Single Home Server & Pool of Application Proxy, TLS Link	Home Server	Application Proxies FQDN, Load Balancer FQDN	Load Balancer FQDN	* / *	YES	TLS	5061
			Load Balancer FQDN	CS 1000 SIP address	NO	TLS	5061

Configuration Type	Component	Host-Authorization	Destination	User / Domain	Phone URI	Transport	Port
	Application Proxies Pool	Home Server FQDN, Load Balancer FQDN, NRS and Node IP of CS 1000	Home Server FQDN	* / *	NO	TLS	5061
8. Pool of Home Servers & Pool of Application Proxy, TCP Link	Home Servers Pool	Application Proxies IP, Load Balancers IP (both home and proxy servers pools)	Load Balancer IP (Proxy Pool)	* / *	YES	TCP	5060
			Load Balancer IP (Proxy Pool)	CS 1000 SIP address	NO	TCP	5060
	Application Proxies	Home Servers IP, Load Balancers IP (both home and proxy servers pools), NRS and Node IP of CS 1000	Load Balancer IP (Home Pool)	* / *	NO	TCP	5060
9. Pool of Home Servers & Pool of Application Proxy, TLS Link	Home Servers Pool	Application Proxies FQDN, Load Balancers FQDN (both home and proxy servers pools)	Load Balancer FQDN (Proxy Pool)	* / *	YES	TLS	5061

Configuration Type	Component	Host-Authorization	Destination	User / Domain	Phone URI	Transport	Port
			Load Balancer FQDN (Proxy Pool)	CS 1000 SIP address	NO	TLS	5061
	Application Proxies	Load Balancers FQDN (both home and proxy servers pools), NRS and Node IP of CS 1000	Load Balancer FQDN (Home Pool)	* / *	NO	TLS	5061

### Configuring a static route and host authorization for the Application Proxy

1. Open the Live Communications Server Management Console. The console is accessed on the Windows server running Live Communications Server, as shown in [Figure 72: Opening the Live Communications Server Management Console](#) on page 137, by selecting **Start > Program > Administrative Tools > Live Communications Server 2005**.



**Figure 72: Opening the Live Communications Server Management Console**

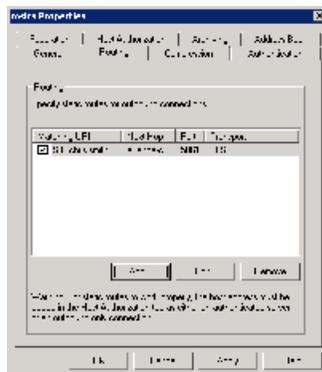
2. In the Live Communications Server Management Console, select the Live Communications Server (the server to which you are adding Host Authorization and changing the Routing) and right-click on that server. From the drop-down menu, select **Properties**. See [Figure 73: Live Communications Server Management Console](#) on page 138.



**Figure 73: Live Communications Server Management Console**

3. For the Application Proxy, route all incoming SIP requests to the Live Communication Server Home Server. This routes all incoming calls from CS 1000 to the Home Server, which then routes the call on to the appropriate Office Communicator user. Routing outgoing calls from the Live Communications Server Home Server on to the CS 1000 is not necessary as the MCM application is responsible for this task. Therefore, no routes from the Application Proxy to the CS 1000 need to be configured on the Application Proxy.

In [Figure 74: Routing configuration on Live Communications Server Application Proxy](#) on page 138, all incoming SIP requests are routed to the Home Server "bmcs5100-9.lcs2.." over TLS.



**Figure 74: Routing configuration on Live Communications Server Application Proxy**

4. On the Add Static Route dialog box (see the next figure), enter the user and route information.

**Important:**

Do not enable User equals phone on the static route configured on the application proxy.

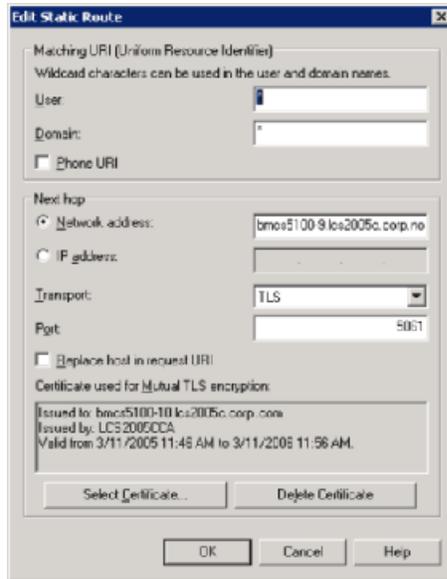


Figure 75: Add Static Route

5. On the Edit Authorized Host dialog box (see [Figure 76: Edit Authorized Host](#) on page 139), enter the IP address, click both the **Throttle As Server** and **Treat As Authenticated** check boxes, and then click **OK**. The IP addresses that require authorization on the Application Proxy are the Node IP addresses of all the CS 1000 in the network.

**Important:**

In Release 5.0, MCM adds a loopback address to the authorized host table automatically during startup. Therefore, users must not manually remove that entry.

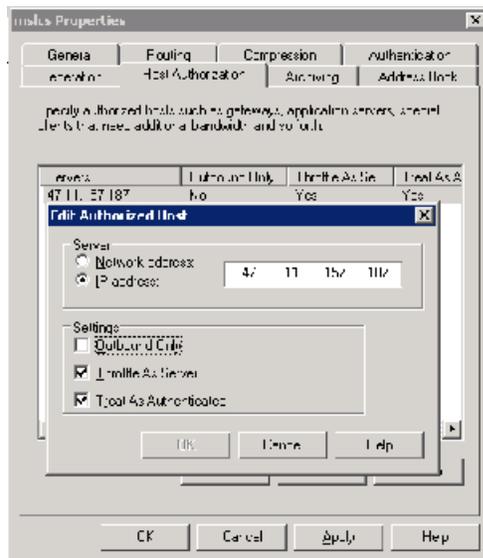
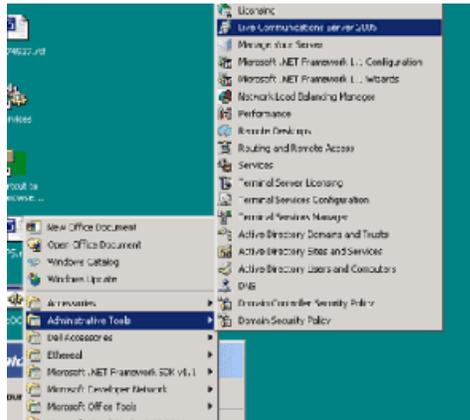


Figure 76: Edit Authorized Host

## Configuring a static route for the Home Server

1. Open the Live Communications Server Management Console. The console is accessed on the Windows server running Live Communications Server, as shown in [Figure 77: Opening the Live Communications Server Management Console](#) on page 140, by selecting **Start > Program > Administrative Tools > Live Communications Server 2005**.



**Figure 77: Opening the Live Communications Server Management Console**

2. In the Live Communications Server Management Console, select the Live Communications Server (the server to which you are adding Host Authorization and changing the Routing) and right-click on that server. From the drop-down menu, select **Properties**. See [Figure 78: Live Communications Server Management Console](#) on page 140.



**Figure 78: Live Communications Server Management Console**

3. On the Routing page of the Home Server, route all SIP messages to the appropriate Application Proxy. With MCM running on the Application Proxy, the SIP invite is sent to the correct CS 1000.

See [Figure 79: Routing tab](#) on page 141, all incoming SIP requests are routed to the Home Server "bmcs5100-9.lcs2..." over TLS.



**Figure 79: Routing tab**

4. On the Add Static Route dialog box, enter the user and route information.

## Configuring Active Directory

Active Directory configuration takes place in the Active Directory Users and the Computers (ADUC) window. Selecting the Users folder reveals the list of users (see [Figure 80: Active Directory \(Microsoft® LDAP server\)](#) on page 142). All users are defined in this folder.

### Important:

By default MCM uses GC LDAP server which contains partial information about all objects in the Active Directory domain forest. It requires replication from all Domain controllers to the GC domain controller to be performed after changes made in the Active Directory User's configuration ("Active Directory Sites and Services" snap-in).

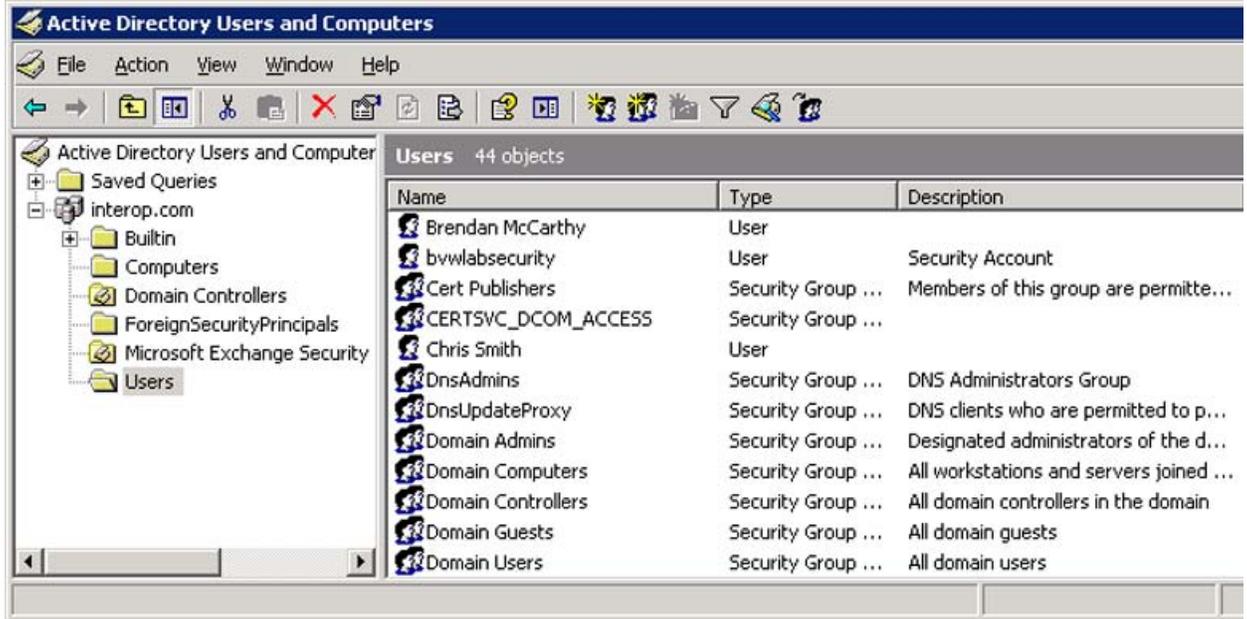


Figure 80: Active Directory (Microsoft® LDAP server)

### Defining users

1. Select a user from the list in the Users folder.
2. Right-click the user, and select **Properties**.
3. The Properties dialog box opens (see [Figure 81: User properties](#) on page 143).

The screenshot shows a Windows-style dialog box titled "Brendan McCarthy Properties". It has a tabbed interface with the following tabs: Member Of, Dial-in, Environment, Sessions, Remote control, Terminal Services Profile, COM+, Live Communications, General, Address, Account, Profile, Telephones, and Organization. The "General" tab is selected. Below the tabs, there is a profile picture of a man and the name "Brendan McCarthy". The form contains the following fields and buttons:

- First name:  Initials:
- Last name:
- Display name:
- Description:
- Office:
- Telephone number:
- E-mail:
- Web page:

At the bottom of the dialog are four buttons: OK, Cancel, Apply, and Help.

**Figure 81: User properties**

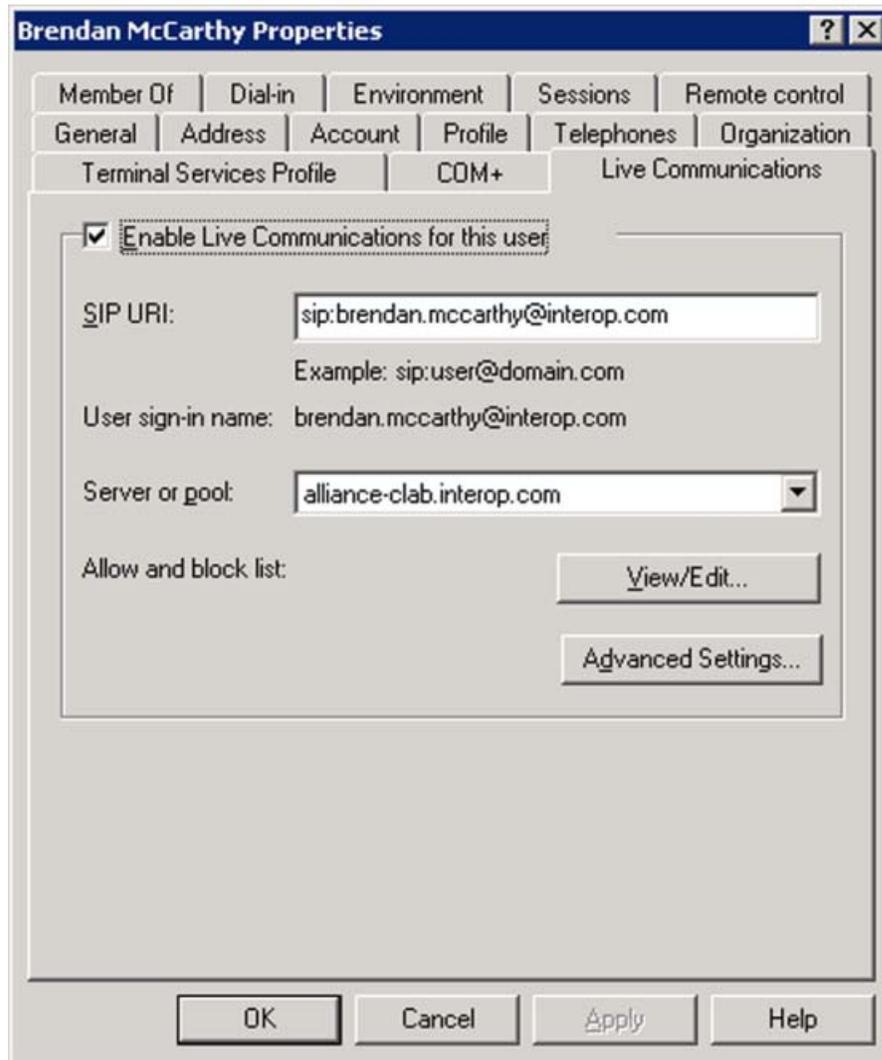
4. Enter the user's information (first name, last name, telephone number, and so on) in the appropriate fields in the General page.

**\* Note:**

The "Telephone number" field is the preferred field to enter the phone number used for the Twinning feature. It is extremely important that:

- The phone number is entered in the same field and in the exact same format for all users.
- The field and format used matches what is configured in MCM. Typical configuration involves using the Phone Number field, which maps to telephoneNumber in MCM and then puts the number in the format of "ESN 445-8888" which maps to "ESN ???-???" in MCM.

5. Select the Live Communications tab (see [Figure 82: Enable Live Communications Server connectivity for a user in Active Directory](#) on page 144).
6. Click the check box next to **Enable Live Communications for this user**.
7. In the fields provided, define the user **SIP URI** and the **Server or Pool** (see [Figure 82: Enable Live Communications Server connectivity for a user in Active Directory](#) on page 144). Office Communicator 2005 uses these addresses to place calls.



**Figure 82: Enable Live Communications Server connectivity for a user in Active Directory**

## Configuring the Call Server

CS 1000 configuration involves two separate functions: Signaling Server configuration (covered in the next section) and Call Server Configuration. All of the Signaling Server configuration is performed in Element Manager. Most of the Call Server configuration can also

be done in Element Manager, although some may need to be done at the Call Server prompt. This document assumes that you are already familiar with how to configure a CS 1000 .

It is important in ESN networks that the correct HLOC is configured in both Overlay 90 (required for ESN calls to work) and Overlay 15. If not, basic calling functionality does not work. Also, the Caller ID table (explained in this section), Home NPA, and LOC are required for outgoing calls to the Public network (PSTN) to correctly display the outgoing Caller Line ID (CLID) for North American networks.

Following ISDN interfaces are supported:

- 1TR6
- APAC
- AXEA, AXES
- D70, D100, D250
- EURO, E403
- EGF4, ESIG, ESGF, ESS4, ESS5
- ISGF, ISIG
- JTTC
- NUME,
- S100,
- SS12
- SWIS
- TCNZ

Package 408 is required for both Telephone Gateway and Services and Remote Call Control. Phones need not be configured as "AST," or have "T87A" enabled as a class of service; however, Package 408 must be added in order for Telephone Gateway and Services to work properly.

## Configuring the SIP Trunk

In order for a Live Communications Server 2005 Server to use a CS 1000 as a SIP Gateway, SIP Trunks must be configured on the CS 1000 . The configuration of the SIP Trunk requires that configuration be done on both the Call Server and the Signaling Server.

### **Note:**

Both can be done through Element Manager. For more information on how to create the required components on the Call Server, refer to *Avaya IP Peer Networking: Installation and Commissioning, NN43001-313*.

 **Important:**

The Route Data Block (RDB) must have the prompts NCNA and NCRD configured to Yes. Otherwise, calls that are "Twinned" to Office Communicator using PCA do not work.

 **Important:**

The Route Data Block (RDB) must have no value configured for the prompt "INST". Otherwise, incoming calls from Office Communicator to the CS 1000 do not work.

 **Important:**

When configuring the D Channel used by the SIP Trunk for Converged Office Telephony Gateway and Services, configure the NASA prompt to yes. Failure to do so may result in limited call transfers through Office Communicator.

Immediate (IMM) is recommended for both fields. If the trunk is intended for SIP DECT or Converged Office applications, use WNK/WNK instead. The Communication Server 1000 SIP trunk that receives Office Communicator calls must be configured to ESN5, and all associated Virtual trunks must be configured to WNK/WNK. These settings are required so that Office Communicator calls to the Public Network display the correct CLID and have the same Network Class of Service (NCOS) as a call from the associated Communication Server 1000 IP Phone.

The Virtual trunk is WNK/WNK if the output from Element Manager, or a terminal window, is:

```
DES IPTIE TN 081 0 00 02 VIRTUAL TYPE IPTI CDEN 8D CUST 0 XTRK VTRK
ZONE 000 TRK ANLG NCOS 0 RTMB 10 3 CHID 3 TGAR 0
STRI/STRO WNK WNK
SUPN YES AST NO IAPG 0 * CLS UNR DIP WTA LPR APN THFD XREP P10 NTC
MID TKID * AACR NO
```

 **Note:**

All of the SIP Virtual Trunks must be configured to WNK WNK.

The Route Data Block is ESN5 if the output from Element Manager, or a terminal window, is:

```
TYPE RDB CUST 00 DMOD ROUT 10 DES IPROUTE TKTP TIE VTRK YES ZONE 100
PCID SIP ... ANTK
SIGO ESN5
STYP SDAT
```

 **Note:**

If the Route Data Block (RDB) already has associated Virtual Trunks and is configured to SIGO STD, all Virtual Trunks must be removed before the RDB can be changed to ESN5.

## Configuring the Codec

Office Communicator 2005 supports the G.711 (20 milliseconds) codec. The G.723.1 is also supported and can be used. The G.711 codec must be enforced in the network by defining only the G.711 codec on the CS 1000 . As DTMF digits are sent in-band by Office

Communicator 2005, the G.711 codec must be the only codec used. If G.711 is not the only codec used, calls to voice mail (such as Avaya CallPilot) or call conferencing bridges (such as MCS MeetMe) do not work.

**\* Note:**

G.723.1 is supported in Release 5.0. However, it must only be enabled on the CS 1000 when the system is configured so that DTMF tones are not used for DTMF digit handling. Otherwise, calls from Office Communicator to voice mail (such as Avaya CallPilot) or call conferencing bridges (such as MCS MeetMe) do not work.

Other codecs cannot be configured on the CS 1000, as Office Communicator calls that tandem through the CS 1000 to other endpoints cannot be allowed to select a codec other than G.711.

The codec is configured as described in Avaya IP Peer Networking: Installation and Commissioning (NN43001-313). [Figure 83: Codec configuration](#) on page 147 demonstrates the correct location of Element Manager in which to configure the codec.

**- VGW and IP phone codec profile**

Enable Echo canceller

Echo canceller tail delay 128

Voice activity detection threshold -17

Idle noise level -65

DTMF Tone detection

Enable V.21 FAX tone detection

FAX maximum rate (bps) 14400

FAX playout nominal delay 100

FAX no activity timeout 20

FAX packet size 30

**- Codec G711**

Codec Name G711

Voice payload size (ms/frame) 20

Voice playout (jitter buffer) nominal delay 40

Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay 80

Modifications may cause changes to dependent settings

VAD

**Figure 83: Codec configuration**

## Configuring the Loss Plan

In order for DTMF digits to be transmitted at the correct volume, especially for Office Communicator 2005 to PSTN communications, the Loss Plan for the CS 1000 must be correctly configured. Calls from Office Communicator 2005 to a residential Voice Mail system (VoIP to PSTN) is an example of the necessity of Loss Plan configuration. For information on how to configure the Loss Plan refer to Avaya Transmission Parameters (NN43001-282).

It is important to not just configure the Loss Plan values, but also the DTI Data Block (DDB), in order that the Loss and Level Plans be configured correctly. For more information, refer to the "Loss values for Voice Gateway Media Card" section in Avaya Transmission Parameters (NN43001-282).

### Important:

When any kind of in-band signaling is to be used as payload audio packets (for example, DTMF tones) in the egress direction (IP to TDM), the Signal Limiter functionality must be disabled. If problems are encountered with DTMF tones from Office Communicator contact Avaya support to ensure the Signal Limiter functionality is disabled.

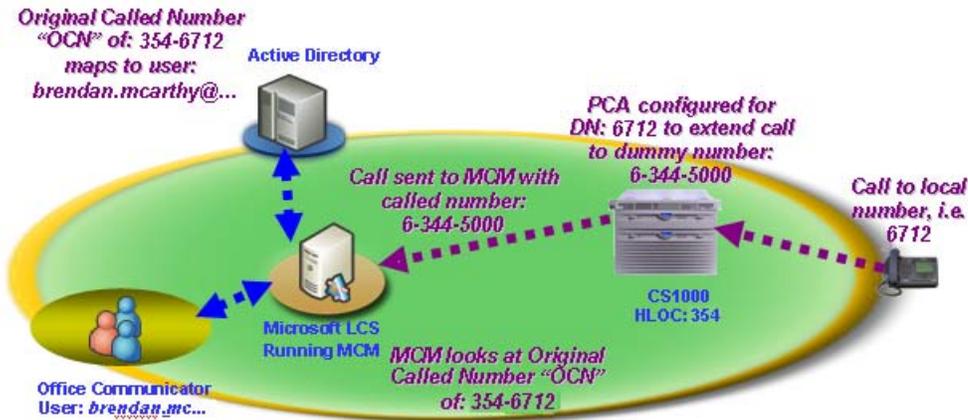
## Configuring the Dialing Plan to route to MCM

In order for calls to be extended using PCA to the Live Communications Server, a dialing plan entry must be entered on the Call Server to send the call to the SIP trunk. This dialing plan entry does not correspond with any number that is "dialable" within a network, but rather is used to route the call to the Live Communications Server. The MCM service running on the Live Communications Server handles the incoming call and directs the call to the correct Office Communicator client.

The reason for this is that the SIP Invite generated by PCA has two fields:

- **To:** this field is used for the sole purpose of routing the invite to MCM.
- **Original Called Number (OCN):** this field is used to determine the original number called. The OCN maps to stored information on the Active Directory and sends the call to the correct Office Communicator client.

For example, the CS 1000 network may be configured as shown in [Figure 84: Dialing plan to route to MCM](#) on page 149.



**Figure 84: Dialing plan to route to MCM**

In this figure, the CS 1000 has a HLOC of 231 and an LOC dialing plan entry of 344. The LOC dialing plan 344 is not "dialable", but calls to the DN: 3052 extends the call to the number 6-344-5000. By PCA extending the call to 6-344-5000, a SIP Invite is sent to the Live Communications Server.

The Live Communications Server runs MCM, which handles the Invite and reads the Original Called Number as 231-3052. The call is then sent to the user and is mapped to 231-3052. In this diagram the user is "david@...."

The purpose of configuring is to ensure that the Office Communicator has the same phone number for both incoming and outgoing calls.

For more information on Dialing Plans, refer to *Avaya IP Peer Networking: Installation and Commissioning (NN43001-313)*.

## Configuring the Personal Call Assistant

Personal Call Assistant (PCA) is used to "twin" incoming calls so users can answer the calls on either their desktop phone or Office Communicator 2005.

In order for the incoming calls to be extended to the "twinned" Office Communicator client, a PCA TN must be defined for that DN. PCA is configured as shown in *Avaya Communication Server Features and Services (NN43001-106)*.

The PCA TN is configured to send the call to another number. In the case of "twinning" to Office Communicator, the call is sent to a number that is not dialable but routes the invite to the Live Communication Server. For more information, refer to [Configuring the Dialing Plan to route to MCM](#) on page 148.

### **!** Important:

If SIP CTI control is also enabled for that telephone, the PCA TN cannot be MARP 0.

When you use a PCA, the MARP must be on the DN key of the phone itself, not the PCA. If the MARP is on the PCA, CTI clients (such as Office Communicator) do not receive Remote

Call Control call pop-ups for incoming calls (in addition to other problems). This is an unsupported configuration.

Note that MARP is assigned to the first DN key created, so if you create the PCA first and assign a DN key, it becomes the MARP by default. If you add a phone later with the same DN (to twin the phone with Office Communicator) the MARP stays on the PCA and you encounter this exact situation. The following is an example of an unsupported configuration:

```
REQ: prt
TYPE: dnb
CUST 0
DN a r l 6712
DATE
PAGE
DES

DN 6712
TYPE SL1
TN > t T 061 0 00 00 V t y KEY 00 MARP DES I2002 i F m > 28 AUG
2005
(I2002 )
TN 061 0 00 00 V KEY 00 DES I2002 28 AUG 2005
(PCA)
```

For more information about PCA, refer to the *Avaya Communication Server Features and Services (NN43001-106)* document.

The following is an example of a correctly configured PCA:

```
DES PCA
TN 097 0 00 01 VIRTUAL
TYPE PCA
CDEN 8D
CUST 0
ZONE 000
FDN
TGAR 1
LDN NO
NCOS 0
SGRP 0
RNP 0
SCI 0
SSU
XLST
SFLT NO
CAC_CIS 3
CAC_MFC 0
CLS CTD FBD WTA LPR MTD FND HTD TDD HFA CRPD
MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE
DRG1
POD DSX VMD CMSD SLKD CCSD SWD LND CNDD
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCB
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXD ARHD CLTD ASCD
CPFA CPTA HSPD ABDD CFHD FICD NAID DNAA RDLA BUZZ
AGRD MOAD
UDI RCC HBT D AHA IPND DDGA NAMA MIND PRSD NRW
NRCD NROD DRDD EXR0
USMD USRD ULAD CCB D RTDD RBDD RBHD PGND OCB
FLXD FTTC DNDY DNO3 MCBN
FDS NOVD VOLA VOUD CDMR ICRD MCDD T87D
CPND_LANG ENG Note: All TNs for a DN used for Converged Office must
have CLS CDMR
HUNT
PLEV 02
```

```

CSDN
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
DNDR 0
KEY 00 SCR 6712 0 [Note: "Twinned" DN of 6712, CLID Table 0 (that is
covered later)]
ANIE 0
01 HOT P 8 63445000 [Note: HOT P key points to a "FAKE" number that just
directs the call to the MCM/LCS server. In this example the call is directed to:
AC1 ("6")+ LOC ("344") of MCM + Dummy DN of 5000]

```

## Configuring the Call ID Table

The Caller ID table is used to correctly build the Caller ID (CLID) for both Private network and Public network calls from a number/extension. The Caller ID table is used by all CS 1000 telephones and is required for Office Communicator calls to work.

In Private network calls where the Uniform Dialing Plan (UDP) is used, the Location Code (LOC) is normally prefixed to the Called and Calling number. Therefore, the Active Directory for all users must include the LOC for their number. A telephone number of ESN 354-6712, has an LOC of 354 and an extension of 6712.

For PCA Twinning to work correctly in a UDP environment, the full Original Called Number (OCN) must be sent by the CS 1000 to the Live Communications Server. To have the full OCN sent, the CLID table must be configured with the Home Location (HLOC) of the CS 1000.

Outgoing Office Communicator calls to the Public network must have the Call ID table used by the associated MARP TN (a TN with the same extension used by Office Communicator marked as MARP) correctly configured. The associated MARP TN must point to a Call ID table that has the International Country Code configured. The International Country Code is the prompt INTL (in North America the value is 1). The associated MARP TN must point to a Call ID table that also has the Home Exchange configured. The Home Exchange is the prompt HLCL and is the '967' in 1-800-967-3052.

For example, a phone with an extension of 3052, an ESN number of 231-3052, and a Public Number of 967-3052 in North America is configured in the following manner:

```

>ld 11
REQ: prt
TYPE: i2004
TN 61 00
DATE
PAGE
...
DNDR 0
KEY 00 SCR 3052 0 MARP
CPND
CPND_LANG ROMAN
NAME Chris Smith

```

This user is configured to use the default CLID table entry of 0 (the CLID table number is always next to the extension). The CLID table entry 0 must have the correct HLOC of 231, HLCL of 967, and INTL of 1.

The CLID table entry of 0 with an HLOC of 231 is configured in the following manner:

```
>ld 15
REQ: chg
TYPE: net
TYPE NET_DATA
CUST 0
OPT
AC2
FNP
CLID yes
SIZE 5
INTL 1
ENTRY 0
HNTN
...
HLCL 967
...
HLOC 231
...
```

The response to SIZE must be a number greater than 0. The response to ENTRY must match the CLID table entry for the target telephones. Generally the default is 0.

---

## Configuring Home LOC and Home NPA

In order for the correct Caller Line ID (CLID) to be correctly displayed for Office Communicator calls to the Public network, both the HLOC and HNPA may require configuration. All Office Communicators that are part of an ESN network require HLOC configuration. All Office Communicators that make calls to the Public network in North America require that the Area Code be configured.

For more information on the HLOC and HNPA, refer to Avaya IP Peer Networking: Installation and Commissioning (NN43001-313).

---

## Configuring the DNS Server

In Element Manager, under LAN configuration (see [Figure 85: DNS configuration](#) on page 153), you have the option of entering up to three DNS server IP addresses. The DNS server must be correctly configured with the Fully Qualified Domain Name (FQDN) of all LCS Servers and Enterprise Edition Pools. Also, the FQDN must resolve to the IP address of the LCS server for all types of DNS queries (not just for the SIP service type).

DNS server must respond with the correct IP for a generic DNS query. There are a number of different types of DNS queries that can be performed.

**! Important:**

The Signaling Server must be rebooted to ensure that all DNS server configurations take effect.

**\* Note:**

Users upgrading from Release 4.5 to Release 5.0 or later still see Host Table configuration in Element Manager, but that information is no longer used.

<b>- LAN configuration</b>	
<b>Embedded LAN (ELAN) configuration</b>	
Call server IP address	<input type="text" value="47.11.159.10"/>
Unistern Signaling port	<input type="text" value="15000"/>
Broadcast port	<input type="text" value="15001"/> ( 1024 - 65535 )
<b>Telephony LAN (TLAN) configuration</b>	
Unistern Signaling port	<input type="text" value="5000"/>
RTP/RTCP Starting port	<input type="text" value="5200"/> ( 1024 - 65535 )
<b>Embedded LAN (ELAN) Routes</b>	<input type="button" value="Add"/>
<b>Host Table</b>	<input type="button" value="Add"/>
<b>Host Name</b>	<b>IP Address</b>
<b>DNS Servers</b>	
Primary DNS Server IP address	<input type="text" value="47.11.159.187"/>
Alternate DNS Server1 IP address	<input type="text" value="0.0.0.0"/>
Alternate DNS Server2 IP address	<input type="text" value="0.0.0.0"/>

Figure 85: DNS configuration

## Configuring the SIP Trunk

In order for calls to be made between the CS 1000 and Office Communicator 2005, you must configure the SIP trunks. For more information on how to configure SIP trunks, refer to Avaya IP Peer Networking: Installation and Commissioning (NN43001-313).

A CS 1000 with existing SIP trunks requires a configuration change to be compatible with Microsoft® Live Communications Server 2005. In order for a SIP Trunk to communicate with Live Communications Server 2005, the SIP Transport Protocol must be configured as TCP, not UDP (see [Figure 86: SIP Gateway configuration](#) on page 154). However, this is not valid when SPS in Proxy All mode is used, since everything goes through SPS.

**! Important:**

The default Local SIP Port of 5060 is required.

- Signaling Server 47.11.159.11 Properties
Remove

**Role** Leader

**Type** ISP1100

**Embedded LAN (ELAN) IP address**  \*

**Embedded LAN (ELAN) MAC address**  \*

**Telephony LAN (TLAN) IP address**  \*

**Telephony LAN (TLAN) gateway IP address**

**Hostname**  \*

**H323 ID**

**Enable Line TPS**

**Enable IP Peer Gateway (Virtual Trunk TPS)** 

If Telephony LAN(TLAN) IP address and Telephony LAN(TLAN) gateway IP address are not in the same subnet as Telephony LAN(TLAN) Node IP address when Line TPS or IP Peer Gateway is enabled, then the TPS and/or VTRK applications will not run.

**Enable SIP Proxy / Redirect Server**

**Local SIP TCP/UDP Port to Listen to**

**SIP Domain name**

**SIP Gateway Endpoint Name**

**SIP Gateway Authentication Password**

**Enable Gatekeeper**

**Network Routing Service Role**

**Figure 86: SIP Gateway configuration**

## Domain naming

In most configurations where the CS 1000 acts as a SIP Gateway for a Microsoft® Live Communications Server, it is recommended that the SIP Trunk Domain name and the Live Communications Server Domain name be an exact match.

In situations where both the LCS and the CS 1000 have already both been assigned a domain name, and the domain names do not match, there is an alternative. MCM can be configured to register to the NRS using an End\_Point\_Name@Service\_Domain\_Name. For more information, refer to [MCM Configuration screen](#) on page 114.

The domain is listed under the Domains folder in the Management console for Live Communications Server. For example, in the next figure, the Live Communications Server Domain is lcs2005s.corp.avaya.com.



**Figure 87: SIP Trunk Domain name**

[Configuring the SIP Trunk Domain name](#) on page 155 describes how to configure the SIP Trunk domain name to match the Live Communications Server domain name.

### Configuring the SIP Trunk Domain name

1. Log into the Element Manager page for the Signaling Server.
2. Go to **IP Telephony**.
3. Click **Nodes > Servers, Media Cards**.
4. Select **Configuration**.
5. Click **Edit** next to the correct node.
6. Open the **Signaling Server Properties** (see [Figure 88: Element Manager Signaling Server Properties](#) on page 156).

**- Signaling Server 47.11.159.11 Properties**
Remove

**Role** Leader

**Type** ISP1100

**Embedded LAN (ELAN) IP address**  \*

**Embedded LAN (ELAN) MAC address**  \*

**Telephony LAN (TLAN) IP address**  \*

**Telephony LAN (TLAN) gateway IP address**

**Hostname**  \*

**H323 ID**

**Enable Line TPS**

**Enable IP Peer Gateway (Virtual Trunk TPS)**  ▼

If Telephony LAN(TLAN) IP address and Telephony LAN(TLAN) gateway IP address are not in the same subnet as Telephony LAN(TLAN) Node IP address when Line TPS or IP Peer Gateway is enabled, then the TPS and/or VTRK applications will not run.

**Enable SIP Proxy / Redirect Server**

**Local SIP TCP/UDP Port to Listen to**

**SIP Domain name**

**SIP Gateway Endpoint Name**

**SIP Gateway Authentication Password**

**Enable Gatekeeper**

**Network Routing Service Role**

**Figure 88: Element Manager Signaling Server Properties**

7. In most cases, the value for the field SIP Domain Name must match the domain of the Live Communications Server. In [Figure 88: Element Manager Signaling Server Properties](#) on page 156 the SIP Domain name is interop.com. Only in situations where the MCM is configured to register to the NRS using End\_Point\_Name@Service\_Domain\_Name can the two SIP Domain Names not match. For more information, refer to [MCM Configuration screen](#) on page 114.

## URI Mapping

The SIP URI Map must be configured in order to correctly register with the NRS. Also, the SIP URI map information is required for configuration of the MCM Service running on the Live Communications Server. The Private/UDP domain name or Private/CDP domain name is used by MCM to obtain the correct context of the Calling Number.

The SIP URI Map (see [Figure 89: SIP URI Map](#) on page 157) is also configured in Element Manager under Node Configuration.

<ul style="list-style-type: none"> <li>- Feature Code Restriction</li> <li>- Incoming Digit Translation</li> <li>- Tools <ul style="list-style-type: none"> <li>+ Backup and Restore</li> <li>- Call Server Initialization</li> <li>- Date and Time</li> <li>+ Logs and reports</li> </ul> </li> <li>- Security <ul style="list-style-type: none"> <li>+ Passwords</li> <li>+ Policies</li> <li>+ Login Options</li> </ul> </li> </ul>	<table border="1"> <thead> <tr> <th colspan="2" style="background-color: #cccccc;">- SIP URI Map</th> </tr> </thead> <tbody> <tr> <td>Public E.164/National domain name</td> <td>northamerica.com *</td> </tr> <tr> <td>Public E.164/Subscriber domain name</td> <td>+1613 *</td> </tr> <tr> <td>Public E.164/Unknown domain name</td> <td>public.unknown</td> </tr> <tr> <td>Public E.164/Special Number domain name</td> <td>public.special</td> </tr> <tr> <td>Private/UDP domain name</td> <td>udp.interop.com</td> </tr> <tr> <td>Private/CDP domain name</td> <td>cdp.interop.udp.interop.</td> </tr> <tr> <td>Private/Special Number domain name</td> <td>special.udp.interop.com</td> </tr> <tr> <td>Private/Unknown (vacant number routing) domain name</td> <td>private.unknown</td> </tr> <tr> <td>Unknown/Unknown domain name</td> <td>unknown.unknown</td> </tr> </tbody> </table>	- SIP URI Map		Public E.164/National domain name	northamerica.com *	Public E.164/Subscriber domain name	+1613 *	Public E.164/Unknown domain name	public.unknown	Public E.164/Special Number domain name	public.special	Private/UDP domain name	udp.interop.com	Private/CDP domain name	cdp.interop.udp.interop.	Private/Special Number domain name	special.udp.interop.com	Private/Unknown (vacant number routing) domain name	private.unknown	Unknown/Unknown domain name	unknown.unknown
- SIP URI Map																					
Public E.164/National domain name	northamerica.com *																				
Public E.164/Subscriber domain name	+1613 *																				
Public E.164/Unknown domain name	public.unknown																				
Public E.164/Special Number domain name	public.special																				
Private/UDP domain name	udp.interop.com																				
Private/CDP domain name	cdp.interop.udp.interop.																				
Private/Special Number domain name	special.udp.interop.com																				
Private/Unknown (vacant number routing) domain name	private.unknown																				
Unknown/Unknown domain name	unknown.unknown																				

**Figure 89: SIP URI Map**

The SIP URI Map must match the NRS server configuration in the following manner:

- The Private/UDP domain name maps to the L0 Domain on the NRS
- The Private/CDP domain name maps to the L1 Domain on the NRS

MCM must be configured to match one of the domain names. For example, in a UDP network, the configured domain name is LCS2005\_UDP in MCM.

---

## Configuring SIP Gateway CLID Parameters

The SIP Gateway CLID parameters are used to adjust the format of telephone numbers for incoming call appearances. For Microsoft® Office Communicator these settings impact the format of numbers that appear on the incoming call popup for Telephony Gateway and Services (the SIP call leg for Microsoft® Office Communicator clients that are twinned with a CS 1000 DN through a PCA).

- SIP GW Settings	
Primary Proxy / Re-direct IP address	<input type="text" value="47.11.108.100"/>
Primary Proxy / Re-direct IP Port	<input type="text" value="5060"/>
Primary Proxy Supports Registration	<input checked="" type="checkbox"/>
Primary CDS Proxy or Re-direct server flag	<input type="checkbox"/>
Secondary Proxy / Re-direct IP address	<input type="text" value="47.11.108.105"/>
Secondary Proxy / Re-direct IP Port	<input type="text" value="5060"/>
Secondary Proxy Supports Registration	<input checked="" type="checkbox"/>
Secondary CDS Proxy or Re-direct server flag	<input type="checkbox"/>
CLID Parameters	
Country Code	<input type="text" value="31"/>
Area Code	<input type="text" value="123"/>
Subscriber / Number of digits to strip	<input type="text" value="0"/> ▼
Subscriber / Prefix to insert	<input type="text"/>
National / Number of digits to strip	<input type="text" value="0"/> ▼
National / Prefix to insert	<input type="text"/>

Figure 90: SIP GW CLID Parameters

**\* Note:**

These settings are independent of the similar SIP CTI CLID parameters to allow independent control of the format of numbers on the incoming call popup for telephony gateway and services.

For all public calls (subscriber (for example, NXX in North America), national (for example, NPA in North America), or international) E.164 fully qualified numbers are used to represent the caller. This is made possible through the use of the following parameters:

- Country Code
- Area Code
- Subscriber/Number of Digits to strip

- Subscriber/Prefix to insert
- National/Number of Digits to strip
- National/Prefix to insert

The E.164 format of subscriber calls (for example, NXX in North America) is:

+<countrycode><area code><subscriber number>.

The parameters Subscriber/Number of digits to strip and prefix to insert are used to modify the format of subscriber numbers presented from the PSTN due to region specific requirements.

The E.164 format of national calls (for example, NPA in North America) is:

+<countrycode><national number>.

The parameters National / Number of digits to strip and prefix to insert are used to modify the format of national numbers presented from the PSTN due to region specific requirements.

---

## Parameter: Country Code

This parameter defines the country code to be used in CLID generation.

---

## Parameter: Area Code

This parameter defines the area code to be used in CLID generation.

---

## Parameter: Subscriber / Number of Digits to strip

For incoming subscriber (NXX) calls this parameter defines the number of digits to strip from the incoming phone number prior to conversion to E.164 format.

---

## Parameter: Subscriber / Prefix to insert

For incoming subscriber (NXX) calls this parameter defines the prefix to insert after stripping any digits necessary from the incoming phone number prior to conversion to E.164 format.

---

## Parameter: National / Number of Digits to strip

For incoming national (NPA) calls this parameter defines the number of digits to strip from the incoming phone number prior to conversion to E.164 format.

---

## Parameter: International / Number of Digits to strip

For incoming international calls this parameter defines the number of digits to strip from the incoming phone number prior to conversion to E.164 format.

---

## Parameter: National / Prefix to insert

For incoming national (NPA) calls this parameter defines the prefix to insert after stripping any digits necessary from the incoming phone number prior to conversion to E.164 format.

---

## Parameter: International / Prefix to insert

For incoming international calls this parameter defines the prefix to insert after stripping any digits necessary from the incoming phone number prior to conversion to E.164 format.

---

## Configuring SPS

SIP Proxy Server (SPS) is configured through MCM (see [Figure 53: MCM Configuration](#) on page 115).

SPS options include:

- Primary and Secondary IP addresses
- Three different modes: Proxy All, Redirect, and Proxy SIP Gateway Calls
- Transport: TLS (5061) and TCP (5060)

---

## Configuring NRS

As stated earlier in this document, the use of the term Network Routing Service (NRS) implies both SPS and SRS. In the event that SPS is used in the deployment, the IP address of a valid DNS server must be configured on the SIP Proxy Server (during a Linux-based installation).

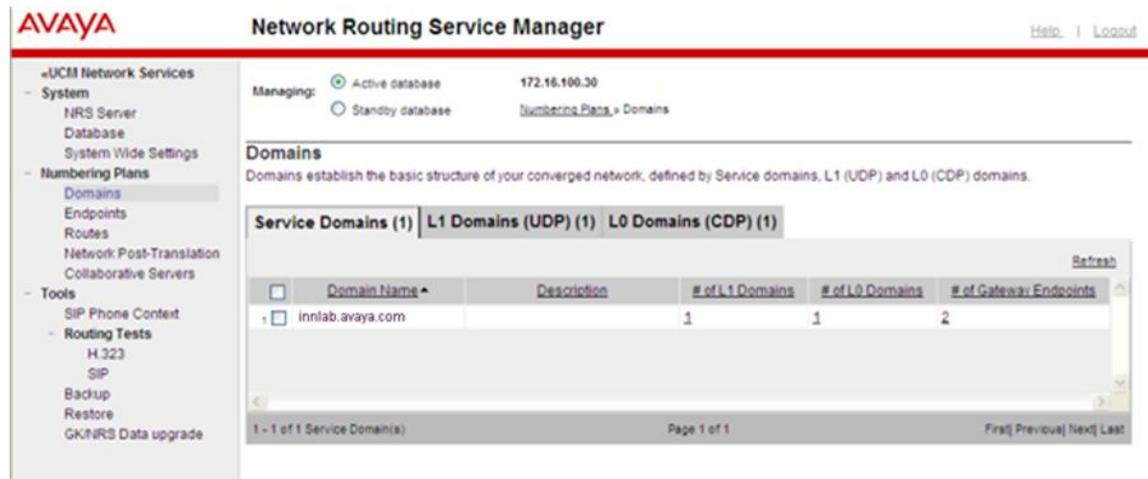
The Server IP running the MCM application (generally a Live Communications Server 2005 Proxy) must be configured on the NRS as a dynamic SIP endpoint, or gateway, and not as a collaboration server.

 **Note:**

NRS configuration is the legacy method.

A Live Communications Server Service Domain must be created for the Signaling Server and MCM. The Signaling Server and MCM register to the Live Communications Server Service Domain on the NRS. This Live Communications Server Service Domain must also match the domain name of the Live Communications Server.

The Service Domain between the NRS and the Live Communication Server must also match—or MCM is configured to register with `End_Point_Name@Service_Domain_Name`, where the 'Service Domain Name' matches the Service Domain configured on the NRS.



**Figure 91: Live Communications Server Service Domain**

In [Figure 91: Live Communications Server Service Domain](#) on page 161, the NRS is configured with the matching Service Domain of `lcs2005c.avaya.com`.

The L1 and L0 Domains must also be configured and match what the CS 1000 is configured under SIP URI Map. Dynamic Gateway endpoints must be configured for the CS 1000 and the MCM with appropriate dialing plan entries.

The NRS must have the same UDP or CDP dialing plan prefix to route calls to the MCM endpoint. This UDP or CDP dialing plan prefix is the same one configured for the PCA calls.

For example, the Location Code (LOC) 344 from the PCA example appears as:

01 HOT P 8 63445000

The NRS must be configured to analyze and qualify numbers dialed from the Live Communications Server (for example, if you configure prefixes to identify the call type, then you might use 6011 for International, 61 for National, and 6 for UDP).

For more information on how to configure the NRS, refer to *Avaya IP Peer Networking: Installation and Commissioning (NN43001-313)*.

---

## Configuring Microsoft® Office Communicator 2005

The following figures demonstrate how to configure a SIP account in Office Communicator 2005.

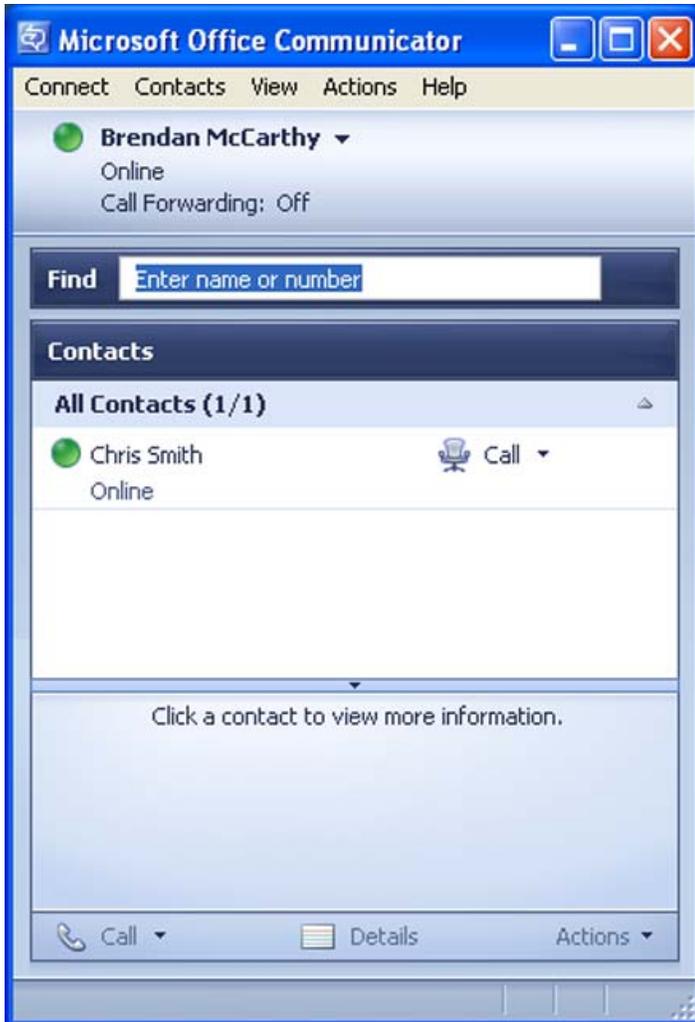


Figure 92: Office Communicator 2005 Main Window

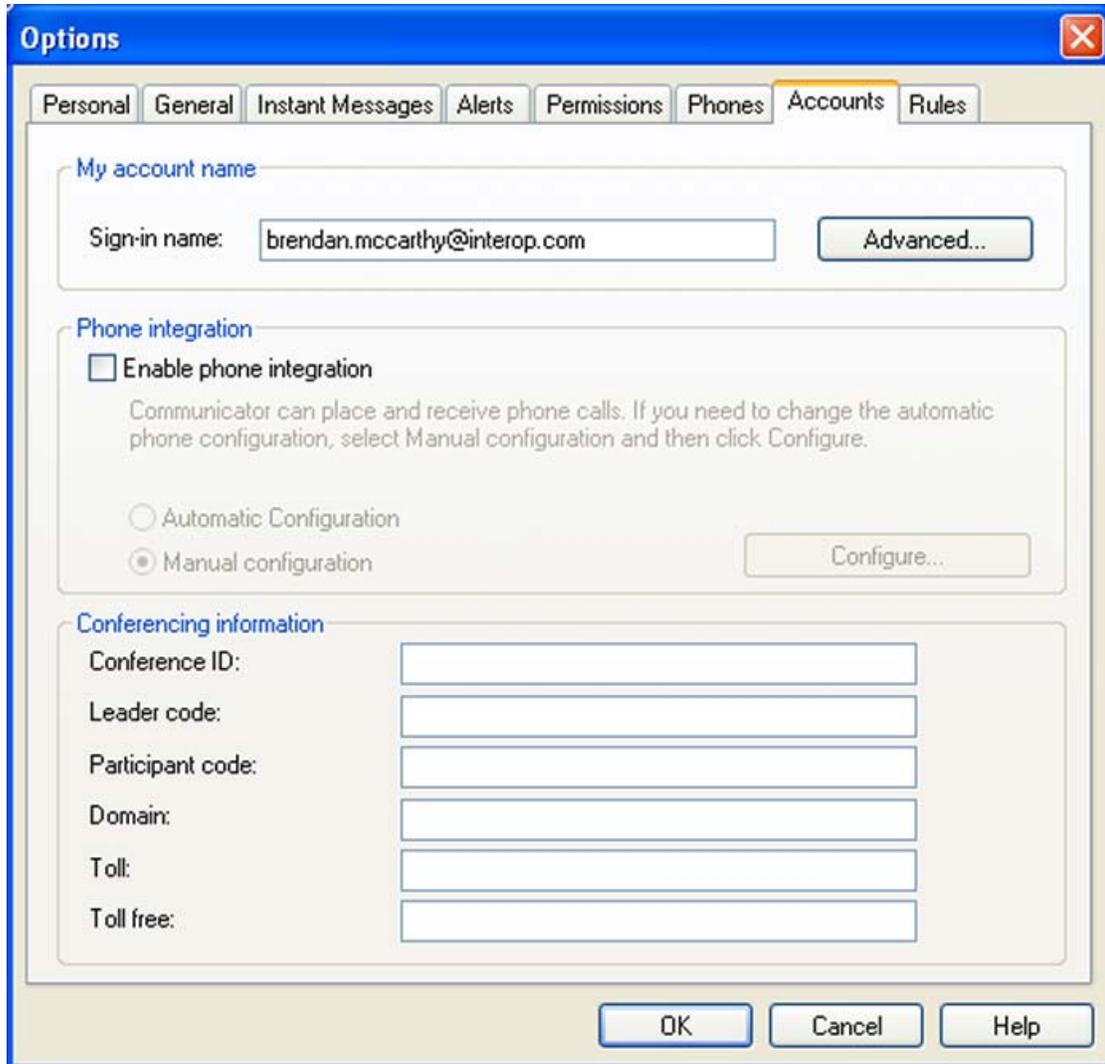
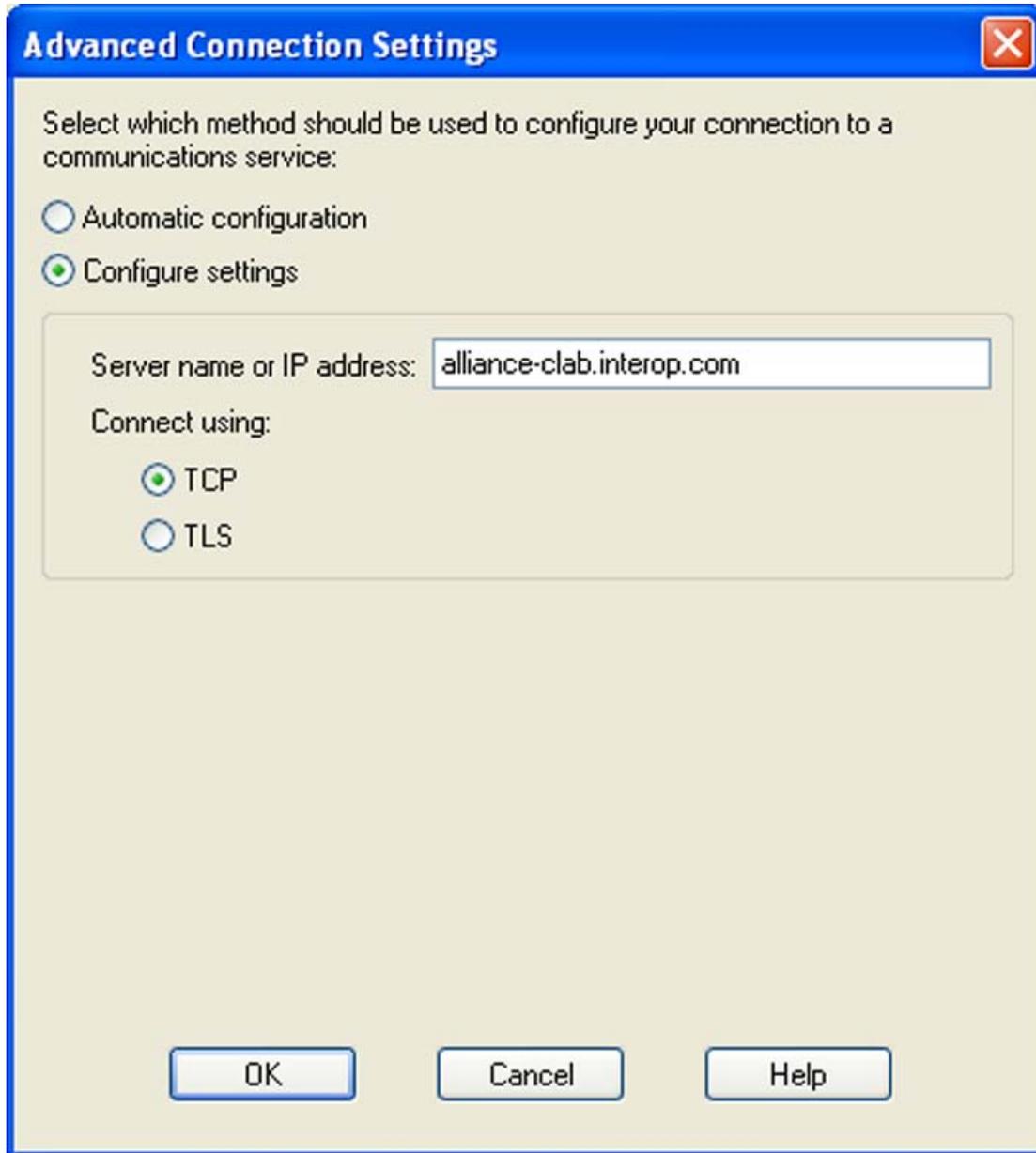


Figure 93: Account Configuration Window in Office Communicator 2005

**! Important:**

The Enable phone integration box must be checked for the Office Communicator "blind" transfer feature to work. For more information, refer to the following Microsoft® Knowledge Base Article:

<http://support.microsoft.com/kb/910790>



**Figure 94: Server Connection Configuration Window**

Although you can select UDP as a transport protocol in Office Communicator 2005, Live Communications Server 2005 does not support UDP.

Client-to-server and server-to-client communication can be achieved only through TCP or TLS in the following manner:

- within the internal network perimeter
- outside the internal network perimeter, or
- across the internal network perimeter.

The use of TLS is recommended for communicating outside or across the network perimeter, as this protocol provides high security levels. TLS requires PKI and certificates, whereas TCP does not.

---

## Configuring CDR

Call Detail Recording (CDR) is supported for outgoing calls from Office Communicator. Office Communicator CLID is included in the CDR record. From Office Communicator, when a call is made, the Office Communicator CLID (extracted from the Active Directory) is identified.

The following is an example of an outgoing call:

```
N 024 00 A030 001 T012 023 09/12 10:48:23 00:00:02.0
614165558888&2452336XXXXXXXXXX
```

The dialed number appears at the end (XXXXXXXXXX) and the Office Communicator CLID and the CDR records appear after the ampersand (&); a location code of 245 is followed by 2336 (a location code of 245 followed by 2336). Again, MCM supports redundant NRS configurations.

---

## Dialing E.164 International Format Numbers from Microsoft® Office Communicator - Computer Calls (SIP Gateway)

It is important to note that the dialed number sent from Microsoft® Office Communicator to the CS 1000 for SIPGW calls follows the same format as those dialed on the station. As such, there is no distinction within or outside North America for the handling of computer (SIP Gateway) calls.

Calls to International format numbers are handled by the SIP Gateway and arrive with a request URI in the SIP INVITE for the following call:

```
sip: +CCCXXXXXXXXX@domain; user=phone
```

In order to support these calls, placed through the SIP Gateway, you must configure the parameters CNTC, NATC, and INTC in LD 15. These parameters ensure that fully qualified numbers within the same country are dialed as national numbers by stripping the country code and adding the national dial prefix.

### Example 1 (Outside of North America)

```
AC1=0, CNTC=31, NATC=0, INTC=00
```

The URI incoming for the SIP INVITE for the call is:

```
sip:+31123456789@domain.com;user=phone
```

The digits sent on the outgoing trunk are: 0123456789

## Example 2 (North America)

AC1=8, CNTC=1, NATC=1, INTC=011

The URI incoming for the SIP INVITE for the call is:

sip: +12125551212@domain.com;user=phone

The digits sent on the outgoing trunk are: 812125551212

---

## Normalizing phone numbers

Now that you have completed the installation and configuration of Telephony Gateway and Services, you may proceed directly to the next step in the process: [Normalizing phone numbers](#) on page 192.

---

## Configuring Remote Call Control

This section describes the process to configure the Remote Call Control with SIP CTI component.

---

## Configuring the CS 1000

Application Module Link (AML) is the main interface used to support call control requests from SIP CTI clients between the SS TR/87 FE application and the CS 1000 .

Incremental Software Management (ISM) defines the number of TNs that can be accessed through SIP CTI by the CLS T87A.

Per-TN configuration is required to define which TNs are used for SIP CTI and to define the specific DN keys on each TN that are available for control by SIP CTI applications.

## Configuring the AML

The following tables ([Table 7: LD 17: Configure AML Link](#) on page 168 and [Table 8: LD 17: Configure VAS \(Value Added Server\)](#) on page 168) display the prompts used for AML link configuration:

**Table 7: LD 17: Configure AML Link**

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	ADAN	
ADAN	<new ELAN #>	A new AML link; the link is an ELAN type. The link number can be from 32 to 47 on a small system and from 32 and 127 on a large system. An AML link number within the above range implies that the transport is over a TCP link.
CTYP	ELAN	Card Type: ELAN

To verify that the AML link is up and running, use the STAT ELAN command from LD 48:

```
>LD 48
STAT ELAN
ELAN #: 032 DES: CDLCS
APPL_IP_ID: 47 .164 .116 .43 : 0000F600 LYN7: ACTIVE EMPTY
APPL ACTIVE
```

Refer to *Avaya Communication Server Software Input/Output: Maintenance (NN43001-711)* for more information on the STAT ELAN command.

 **Important:**

For redundancy, one AML link is required for each Front End within the node, regardless of whether the Front End is a leader or a follower.

**Table 8: LD 17: Configure VAS (Value Added Server)**

Prompt	Response	Description
REQ	CHG	Change existing data
TYPE	VAS	Value Added Server
VAS	NEW	
VSID	<VAS#>	VAS ID, ranges from 32 to 47 on a small system and from 32 to 127 on a large system
ELAN	<LINK #>	AML ELAN link number provisioned when the AML link was created

## Configuring the SIP CTI TR/87 ISM Limit

A new ISM (SIP CTI TR/87) is introduced to define the number of TNs that may be configured with the T87A class of service. The TR/87 configuration for a given TN requires that in addition to the existence of the CLS T87A, the controlled line itself must also be identified as an AST DN. This implies that AST ISMs are also required.

As part of the ordering process, a corresponding AST license is provided for each SIP CTI TR/87 license. This ISM limit is prompted only if package 408 (MS\_CONV) is unrestricted (requires level 2 packages).

The SIP CTI TR87 ISM is an instant ISM and does not require a cold start of the Call Server to take effect (see [Figure 95: LD 22: ISM Limit printout](#) on page 169).

TYPE	slt	Print System Limits			
<...>					
PCA	32767	LEFT	32767	USED	0
ITG ISDN TRUNKS	32767	LEFT	32767	USED	0
H.323 ACCESS PORTS	32767	LEFT	32767	USED	0
<b>AST</b>	<b>32767</b>	<b>LEFT</b>	<b>32767</b>	<b>USED</b>	<b>0</b>
SIP CONVERGED DESKTOPS	32767	LEFT	32767	USED	0
<b>SIP CTI TR_87</b>	<b>32767</b>	<b>LEFT</b>	<b>32767</b>	<b>USED</b>	<b>11</b>
RAN CON	32767	LEFT	32767	USED	0
MUS CON	32767	LEFT	32767	USED	0
SURVIVABILITY	0	LEFT	0	USED	0
<...>					

**Figure 95: LD 22: ISM Limit printout**

## Configuring a station

SIP CTI control of a DN key can be supported on IP, digital, and analog stations.



### Important:

Features such as Make Call and Answer Call depend on the hands-free capability of the station and the on-hook default path configuration on the station. Therefore the use of certain features on stations without hands-free support is limited.

A new CLS (T87A) is introduced to allow a TN to support the SIP CTI application.

The AST prompt is used to configure which DN key on the TN is controlled or monitored by the SIP CTI application. A maximum of two keys per TN can be configured as AST keys.

CLID information is sent, or suppressed, to Office Communicator based on the CLS CNDA/CNDD consistent with the presentation of the CLID information on the station display itself.

This affects whether CLID information (that may be available for calls that do not map to Active Directory users) appears on the Microsoft® Office Communicator call toast (for example, PSTN calls).

## Considering MADN (Multiple Appearance DN)

When you configure a station, you must consider certain issues if Office Communicator is used in a MADN environment:

- When multiple TNs exist in a MADN group, the T87A CLS and AST configuration are configured only on the MARP TN
- When "twinning" a station with Office Communicator using a PCA, the MARP TN within the MADN group must be on a station and not on the PCA. From LD 11 prt dnb:

```
DN 6712
TYPE SL1
TN 061 0 00 00 V KEY 00 MARP DES I2002 28 AUG 2005
(I2002 )
TN 061 0 00 21 V KEY 00 DES PCA 28 AUG 2005
(PCA )
```

- Any Remote Call Control service request sent by Microsoft® Office Communicator 2005, such as Make Call or Answer Call, always apply to the device defined as the MARP TN.
- For SCR keys telephony, presence updates (for example, on the phone) are supported for all TNs within a MADN group. Example: Answering a call on a wireless station SCR key on a non-MARP TN shows the Live Communications Server user as "On the Phone".
- For MCR keys telephony, presence is supported only for the MARP TN within a MADN group. Example: Answering a call on a wireless station MCR key on a non-MARP TN does not show the Live Communications Server user as "On the Phone". Only calls answered on the MARP TN affect the presence status of that user.

## Configuring NRS

Use of the NRS is optional. However, if you use the NRS, MCM and TR/87 FE must be configured on the NRS as the Gateway Endpoints.

The corresponding Routing Entries must be defined to support SIP gateway calls.

---

## Configuring the Signaling Server

The TR/87 FE application shares the TPS master/follower mechanism to provide redundancy within a node. The TR/87 FE application shares one instance of the SIP stack with the SIP GW and correspondingly uses some of the existing SIP GW configuration parameters:

- SIP Transport Protocol, Local SIP Port, SIP Domain Name
- The SIP URI map

The IP address and domain name of any Live Communications Server proxy responsible for forwarding TR/87 traffic to the Signaling Server must be added to the Signaling Server Host

Table in Element Manager. A new section is introduced to Element Manager to configure SIP CTI-specific parameters.

**! Important:**

When the SIP CTI service is enabled and any dependent configuration parameter is modified in Element Manager, all active SIP CTI sessions are terminated so the configuration data can be updated.

## Configuring Node Parameters

The node IP is the IP address of the TR/87 FE:

- You can configure multiple nodes to support TR/87 applications for additional capacity. The Remote Call Control SIP URI of users determines which node they use.
- An AML restriction dictates that only one application can acquire a given DN on a Call Server.

**! Important:**

When you add additional nodes to balance TR/87 load, SIP routing must be configured so that all clients that attempt to control a DN terminate on the same node.

The TR/87 FE application can run within a TPS node as well as a non-TPS node (see [Figure 96: TR/87 Node configuration](#) on page 171).

- Signaling Server 47.11.159.11 Properties Remove

Role	Leader
Type	ISP1100
Embedded LAN (ELAN) IP address	47.11.159.11
Embedded LAN (ELAN) MAC address	00:02:b3:bb:40:e6
Telephony LAN (TLAN) IP address	47.11.159.41
Telephony LAN (TLAN) gateway IP address	47.11.159.33
Hostname	1156_ss1
H323 ID	1156_ss1
Enable Line TPS	<input checked="" type="checkbox"/>

**Figure 96: TR/87 Node configuration**

## Configuring SIP Gateway Parameters

The SIP Gateway application must be enabled. To enable the SIP Gateway, TR/87 FE uses the following SIP Gateway configuration parameters (see [Figure 97: SIP Gateway configuration](#) on page 172):

- SIP Transport Protocol (must be TCP for Live Communications Server 2005 deployments)
- Local SIP Port (default 5060)
- SIP Domain Name

**- Signaling Server 47.11.159.11 Properties** Remove

**Role** Leader

**Type** ISP1100

**Embedded LAN (ELAN) IP address** 47.11.159.11 \*

**Embedded LAN (ELAN) MAC address** 00:02:b3:bb:40:e6 \*

**Telephony LAN (TLAN) IP address** 47.11.159.41 \*

**Telephony LAN (TLAN) gateway IP address** 47.11.159.33

**Hostname** 1156\_ss1 \*

**H323 ID** 1156\_ss1

**Enable Line TPS**

**Enable IP Peer Gateway (Virtual Trunk TPS)** SIP only ▼

If Telephony LAN(TLAN) IP address and Telephony LAN(TLAN) gateway IP address are not in the same subnet as Telephony LAN(TLAN) Node IP address when Line TPS or IP Peer Gateway is enabled, then the TPS and/or VTRK applications will not run.

**Enable SIP Proxy / Redirect Server**

**Local SIP TCP/UDP Port to Listen to** 5060

**SIP Domain name** interop.com

**SIP Gateway Endpoint Name** 1156\_ss1

**SIP Gateway Authentication Password** ●●

**Enable Gatekeeper**

**Network Routing Service Role** ▼

Figure 97: SIP Gateway configuration

## Configuring the DNS Server

Host Table configuration is replaced in Release 5.0 with DNS configuration. In Element Manager, under LAN configuration (see [Figure 98: DNS configuration](#) on page 173), you have the option of entering up to three DNS server IP addresses. The DNS server must be correctly configured with the Fully Qualified Domain Name (FQDN) of all LCS Servers and Enterprise

Edition Pools. Also, the FQDN must resolve to the IP address of the LCS server for all types of DNS queries (not just for the SIP service type).

DNS server must respond with the correct IP for a generic DNS query. There are a number of different types of DNS queries that can be performed.

**\* Note:**

Users upgrading from Release 4.5 to Release 5.0 and later still see Host Table configuration in Element Manager, but that information is no longer used.

<b>- LAN configuration</b>	
<b>Embedded LAN (ELAN) configuration</b>	
Call server IP address	<input type="text" value="47.11.159.10"/>
Unistern Signaling port	15000
Broadcast port	<input type="text" value="15001"/> ( 1024 - 65535 )
<b>Telephony LAN (TLAN) configuration</b>	
Unistern Signaling port	5000
RTP/RTCP Starting port	<input type="text" value="5200"/> ( 1024 - 65535 )
<b>Embedded LAN (ELAN) Routes</b>	<input type="button" value="Add"/>
<b>Host Table</b>	<input type="button" value="Add"/>
<b>Host Name</b>	<b>IP Address</b>
<b>DNS Servers</b>	
Primary DNS Server IP address	<input type="text" value="47.11.159.187"/>
Alternate DNS Server1 IP address	<input type="text" value="0.0.0.0"/>
Alternate DNS Server2 IP address	<input type="text" value="0.0.0.0"/>

Figure 98: DNS configuration

## Configuring SIP CTI Settings

All SIP CTI configuration parameters can be configured in Element Manager. See [Figure 99: SIP CTI configuration](#) on page 174.

<b>- SIP CTI Services</b>	
Service Enabled	<input checked="" type="checkbox"/>
<b>CTI Settings</b>	
Customer Number	0 <small>Range: 0 to 99</small>
Maximum Associations per DN	3
International Calls As National	<input checked="" type="checkbox"/>
<b>Dial Plan Prefix</b>	
National Prefix	<input type="text"/>
International Prefix	<input type="text"/>
Location Code Call Prefix	<input type="text"/>
Special Number Prefix	<input type="text"/>
Subscriber Prefix	<input type="text"/>
<b>CLID Parameters</b>	
Dialing Plan	UDP
Calling Device URI Format	phone-context=dialstring
Home Location Code	<input type="text"/>
Country Code	<input type="text"/>
Area Code	<input type="text"/>
Subscriber / Number of digits to strip	0
Subscriber / Prefix to insert	<input type="text"/>
National / Number of digits to strip	0
National / Prefix to insert	<input type="text"/>

**Figure 99: SIP CTI configuration**

**\* Note:**

For each of the SIP CTI settings, if a configuration change is made and a save and transfer is performed, all active SIP CTI sessions are terminated to apply the change. Microsoft® Office Communicator automatically reestablishes the session without user intervention.

### Parameter: Service Enabled

The default state of the SIP CTI service is disabled. To enforce the change of state for this parameter, you must reboot. The SIP CTI service consumes approximately 140 MB of RAM on the Signaling Server when enabled.

**\* Note:**

The configuration change to enable or disable the SIP CTI service is propagated to all Signaling Servers within the node. Ensure that engineering guidelines are considered for all Signaling Servers within the node before you enable this feature.

### Parameter: Customer Number

The customer number parameter defines the customer on the Call Server to which SIP CTI service requests apply. Each TR/87 FE can support one customer number. Additional customers may be supported by adding additional Signaling Servers.

## Parameter: Maximum Associations Per DN

This parameter defines the maximum number of simultaneous TR/87 SIP dialogs that can be active for a single DN. This parameter relates to the Office Communicator 2005 location-based forwarding feature that is based on the assumption that multiple instances of Office Communicator are active, each with their own active TR/87 session (for example, home, office, laptop). This parameter limits the number of simultaneous client sessions for a single DN.

## Parameter: International Calls As National

This parameter is used in combination with the following parameters:

- SIP CTI Dial Plan Prefix - National Prefix
- SIP CTI Dial Plan Prefix - International Prefix
- SIP CTI CLID Parameters - Country Code

When enabled this feature monitors all SIP CTI calls made using the E.164 international number format. For E.164 called numbers that are within the local country the SIP CTI national dial prefix is used to originate the call from the Call Server. For E.164 called numbers that are outside the local country the international dial prefix is used to originate the call from the Call Server.

When this feature is disabled all SIP CTI calls made using the E.164 number format uses the international dial prefix when originating the call from the Call Server.

Two scenarios are provided using the following example parameters:

- SIP CTI Settings - International Calls As National = Enabled
- SIP CTI Dial Plan Prefix - National Prefix = 61
- SIP CTI Dial Plan Prefix - International Prefix = 6011
- SIP CTI CLID Parameters - Country Code - 1
- AC1 = 6

### Scenario 1

A call is placed from Microsoft® Office Communicator to +14167008000. The TR/87 Front End application on the Signaling Server uses the above SIP CTI settings to determine that the E.164 destination is within the local country. The call originates through AML from the Call Server using the national dial string 614167008000.

### Scenario 2

A call is placed from Microsoft® Office Communicator to +31123456789. The TR/87 Front End application on the Signaling Server uses the preceding SIP CTI settings to determine that the E.164 destination is not within the local country. The call originates through AML from the Call Server using the international dial string 601131123456789.

## Configuring SIP CTI Dial Plan Prefixes

The SIP CTI dial plan prefixes configuration settings are used to prefix phone numbers sent to the Call Server as a result of SIP CTI call attempts.

### **Parameter: National Prefix**

When calls are made to E.164 fully qualified numbers this parameter is used in combination with the “International Calls as National” setting in the CTI IP settings section. When a call to an E.164 destination contains the same country code as the local country the call is placed from the Call Server as a national call using this prefix rather than the international call prefix.

This parameter is also used to prefix calls that are made with a URI that contains a phone-context equal to the Public E.164/National domain in the SIP URI map.

Refer to [Parameter: International Calls As National](#) on page 175 for an example of the use of this parameter.

### **Parameter: International Prefix**

When calls are made to E.164 fully qualified numbers this parameter is used in combination with the “International Calls as National” setting in the CTI settings section. If the “International Calls as National” feature is disabled, all calls to any E.164 number are prefixed with this prefix. If the “International Calls as National” feature is enabled, only calls to E.164 destinations outside of the local country are dialed with this prefix.

Refer to the section [Parameter: International Calls As National](#) on page 175 for an example of the use of this parameter.

### **Parameter: Location Code Call Prefix**

This parameter is used to prefix calls that are made with IRAs with a phone-context equal to the Private/UDP domain in the SIP URI map.

This parameter is also used in conjunction with the Calling Device URI Format setting. Refer to the section [Parameter: Calling Device URI Format](#) on page 178 for an example of the use of this parameter.

### **Parameter: Special Number Prefix**

This parameter is used to prefix calls that are made with a URI that contains a phone-context equal to the Public/E.164 Special Number domain in the SIP URI map.

### **Parameter: Subscriber Prefix**

This parameter is used to prefix calls that are made with a URI that contains a phone-context equal to the Public E.164/Subscriber domain in the SIP URI map.

---

## Configuring SIP CTI CLID Parameters

The SIP CTI CLID parameters are used to adjust the format of phone numbers for incoming call appearances. For Microsoft® Office Communicator these settings impact the format of numbers that appear on the incoming call popup for Remote Call Control.

 **Note:**

These settings are independent of the similar SIP GW CLID parameters to allow independent control of the format of numbers on the incoming call popup for Remote Call Control.

For all public calls (subscriber (for example, NXX in North America), national (for example, NPA in North America), or international) E.164 fully qualified numbers are used to represent the caller. This is made possible through the use of the following parameters:

- Country Code
- Area Code
- Subscriber/Number of Digits to strip
- Subscriber/Prefix to insert
- National/Number of Digits to strip
- National/Prefix to insert

The E.164 format of subscriber calls (NXX) is:

+<countrycode><area code><subscriber number>.

The parameters Subscriber/Number of digits to strip and prefix to insert are used to modify the format of subscriber numbers presented from the PSTN due to region specific requirements.

The E.164 format of national calls (NPA) is:

+<countrycode><national number>.

The parameters National/Number of digits to strip and prefix to insert are used to modify the format of national numbers presented from the PSTN due to region specific requirements.

The parameters International/Number of digits to strip and prefix to insert are used to modify the format of international numbers presented from the PSTN due to region specific requirements.

### Parameter: Dialing Plan

When configured to CDP, no changes are made to CDP numbers from the Call Server. However, when configured to UDP, the location code prefix and location code are added as a prefix to CDP numbers to aid in normalization. When this setting is enabled all user phone numbers in the active directory can be entered using the home location code to ensure a

consistent unique format throughout the enterprise. Two scenarios are provided using the following example parameters:

- SIP CTI Dial Plan Prefix - Location Code Call Prefix = 6
- SIP CTI CLID Parameters - Home Location Code = 343

---

## Scenario 1 - SIP STI Dial Plan = CDP

A call is placed to the DN controlled by Microsoft® Office Communicator for RCC from DN 5000 on the same Call Server. The call popup that appears on the users desktop shows call from 5000.

---

## Scenario 2 - SIP CTI Dial Plan = UDP

A call is placed to the DN controlled by Microsoft® Office Communicator for RCC from DN 5000 on the same Call Server. The call popup that appears on the users desktop shows call from 63435000.

---

## Parameter: Calling Device URI Format

This configuration setting defines whether phone-context=dialstrings or the SIP Gateway URI map is used to qualify the TEL URIs used for TR/87.

 **Note:**

For Live Communications Server installations, phone-context=dialstring must be used to ensure compatibility with Microsoft® Office Communicator.

It may be desirable to use the SIP GW URI map to qualify TEL URIs for non-Converged Office implementations as this removes the need to interpret dial plan digits outside of the Call Server.

The combination of the URIs generated by the TR/87 FE and the normalization rules available to Office Communicator 2005 define the ability for Office Communicator to match incoming phone numbers to Live Communications Server user identities (for example, on the incoming call pop-up window).

The CSTA-delivered event contains a parameter called callingDevice that notifies the Office Communicator when a call is presented to the Remote Call Control controlled line. This field contains a TEL URI that is generated based on the combination of the SIP CTI dialing plan and Calling Device URI format parameters. Four scenarios are provided where a call is placed

to the DN controlled by Microsoft® Office Communicator for RCC from DN 5000 using the following example parameters:

- SIP CTI Dial Plan Prefix - Location Code Call Prefix = 6
- SIP CTI CLID Parameters - Home Location Code = 343

### **Scenario 1 - Dial Plan = UDP, Calling Device URI Format = phone-context=dialstring:**

The TEL URI generated for the caller is: "tel:63435000;phone-context=dialstring"

### **Scenario 2, Dial Plan = UDP, Calling Device URI Format = phone-context= SIP GW URI map entries:**

The TEL URI generated for the caller is: "tel:3435000;phone-context=udp.avaya.com"

### **Scenario 3, Dial Plan = CDP, Calling Device URI Format = phone-context= phone-context=dialstring:**

The TEL URI generated for the caller is: "tel:5000;phone-context=dialstring"

### **Scenario 4, Dial Plan = CDP, Calling Device URI Format = phone-context= SIP GW URI map entries:**

The TEL URI generated for the caller is: "tel:5000;phone-context=cdp.avaya.com"

When Office Communicator receives notification of an incoming call, this TEL URI is matched against all known phone numbers (after normalization) to determine if the caller is a known Live Communications Server user.

## **Parameter: Home Location Code**

This parameter defines the home location code to be used in CLID generation in combination with the SIP CTI dial plan setting.

Refer to section [Parameter: Dialing Plan](#) on page 177 for an example of the use of this parameter.

---

## **Parameter: Country Code**

This parameter defines the country code to be used in CLID generation.

---

## Parameter: Area Code

This parameter defines the area code to be used in CLID generation.

---

## Parameter: Subscriber/Number of Digits to strip

For incoming subscriber (for example, NXX in North America) calls this parameter defines the number of digits to strip from the incoming phone number prior to conversion to E.164 format.

---

## Parameter: Subscriber/Prefix to insert

For incoming subscriber (for example, NXX in North America) calls this parameter defines the prefix to insert after stripping any digits necessary from the incoming phone number prior to conversion to E.164 format.

---

## Parameter: National/Number of Digits to strip

For incoming national (for example, NPA in North America) calls this parameter defines the number of digits to strip from the incoming phone number prior to conversion to E.164 format.

---

## Parameter: National/Prefix to insert

For incoming national (for example, NPA in North America) calls this parameter defines the prefix to insert after stripping any digits necessary from the incoming phone number prior to conversion to E.164 format.

## North American SIP CTI Configuration Example

With the configuration defined as in [Figure 100: North American CLID Manipulation](#) on page 181, the following occurs:

- An incoming Subscriber Call with phone number 4005000 produces tel:+16134005000 on the Microsoft® Office Communicator incoming call popup.
- An incoming National Call with phone number 4169008000 produces tel:+14169008000 on the Microsoft® Office Communicator incoming call popup.
- An RCC call from Microsoft® Office Communicator to the E.164 number +16135006000 produces a call from the controlled DN to 616135006000.

An RCC call from Microsoft® Office Communicator to the E.164 number +33123456789 produces a call from the controlled DN to 601133123456789.

<b>- SIP CTI Services</b>	
Service Enabled	<input checked="" type="checkbox"/>
<b>CTI Settings</b>	
Customer Number	0 <small>Range: 0 to 99</small>
Maximum Associations per DN	3
International Calls As National	<input checked="" type="checkbox"/>
<b>Dial Plan Prefix</b>	
National Prefix	61
International Prefix	6011
Location Code Call Prefix	6
Special Number Prefix	6
Subscriber Prefix	9
<b>CLID Parameters</b>	
Dialing Plan	UDP
Calling Device URI Format	phone-context=dialstring
Home Location Code	343
Country Code	1
Area Code	613
Subscriber / Number of digits to strip	0
Subscriber / Prefix to insert	
National / Number of digits to strip	0
National / Prefix to insert	

**Figure 100: North American CLID Manipulation**

## Non-North American SIP CTI Configuration Example

With the configuration defined as in [Figure 101: Non-North American CLID Manipulation](#) on page 182 the following occurs:

- An incoming Subscriber Call with phone number 4005000 produces +311234005000 on the Microsoft® Office Communicator incoming call popup.
- An incoming National Call with phone number 00123456789 produces +31123456789 on the Microsoft® Office Communicator incoming call popup.
- An RCC call from Microsoft® Office Communicator to the E.164 number +31123456789 produces a call from the controlled DN to 00123456789.
- An RCC call from Microsoft® Office Communicator to the E.164 number +33123456789 produces a call from the controlled DN to 00033123456789.

- SIP CTI Services	
Service Enabled	<input checked="" type="checkbox"/>
CTI Settings	
Customer Number	<input type="text" value="0"/> Range: 0 to 99
Maximum Associations per DN	<input type="text" value="3"/>
International Calls As National	<input checked="" type="checkbox"/>
Dial Plan Prefix	
National Prefix	<input type="text" value="00"/>
International Prefix	<input type="text" value="000"/>
Location Code Call Prefix	<input type="text"/>
Special Number Prefix	<input type="text"/>
Subscriber Prefix	<input type="text"/>
CLID Parameters	
Dialing Plan	<input type="text" value="CDP"/>
Calling Device URI Format	<input type="text" value="phone-context=dialstring"/>
Home Location Code	<input type="text"/>
Country Code	<input type="text" value="31"/>
Area Code	<input type="text" value="123"/>
Subscriber / Number of digits to strip	<input type="text" value="0"/>
Subscriber / Prefix to insert	<input type="text"/>
National / Number of digits to strip	<input type="text" value="2"/>
National / Prefix to insert	<input type="text"/>

Figure 101: Non-North American CLID Manipulation

### Parameter: International/Number of Digits to strip

For incoming international calls this parameter defines the number of digits to strip from the incoming phone number prior to conversion to E.164 format.

---

## Parameter: International/Prefix to insert

For incoming international calls this parameter defines the prefix to insert after stripping any digits necessary from the incoming phone number prior to conversion to E.164 format.

---

## Configuring Live Communications Server

Configuration of Live Communications Server for Remote Call Control has the same requirements and procedures as those documented for Telephony Gateway and Services. See [Configuring Live Communications Server](#) on page 124.

When configuring static routing on any Live Communications Server, the request-URI used by Microsoft Office Communicator to establish a TR/87 dialog with CS 1000 is the Remote Call Control SIP URI configured on a per-user basis in Active Directory. Information on the configuration of the Remote Call Control SIP URI can be found in [Defining the Remote Call Control SIP URI](#) on page 188.

There must be a static routing rule on each Live Communications Server to define the SIP routing path between the Microsoft Office Communicator client and the MCM application.

Also note that Authorization of TR/87 service requests is provided by the MCM application based on the per-user Active Directory configuration. Refer to [Configuring MCM for Remote Call Control](#) on page 121 for a description of this feature. If the manual configuration option is used in Microsoft Office Communicator to define the Remote Call Control SIP URI and Phone URI, ensure that TR/87 authorization is disabled on the MCM. Without the corresponding Active Directory configuration to allow the authorization to succeed, the TR/87 SIP messages generated by Microsoft Office Communicator is rejected by the MCM.

---

## Configuring Active Directory

This section is based on the assumption that a Live Communications Server 2005 user account is created, and that all SIP CTI configuration on the CS 1000 is complete.

 **Note:**

By default MCM uses GC LDAP server which contains partial information about all objects in the Active Directory domain forest. It requires replication from all Domain controllers to the GC domain controller to be performed after changes made in the Active Directory User's configuration (Active Directory Sites and Services snap-in).

## Active Directory configuration

1. In the Active Directory Users and Computers (ADUC) window, expand **Users**, right-click the user, and select **Properties**.
2. Select the **Live Communications** tab (see [Figure 102: Active Directory configuration](#) on page 185).
3. On the Live Communications page, click **Advanced Settings**.
4. On the User Advanced Settings dialog box, click **Enable Remote Call Control** to enable remote control of a PBX line (see [Enabling the Remote Call Control Flag](#) on page 185).
5. Specify the user's **SIP URI** or **TEL URI**, and the **Destination URI** in their respective text boxes.
6. If you specified a SIP URI for the user, specify the SIP URI for the telephony gateway to which the user's calls are routed.
7. Click **OK**.

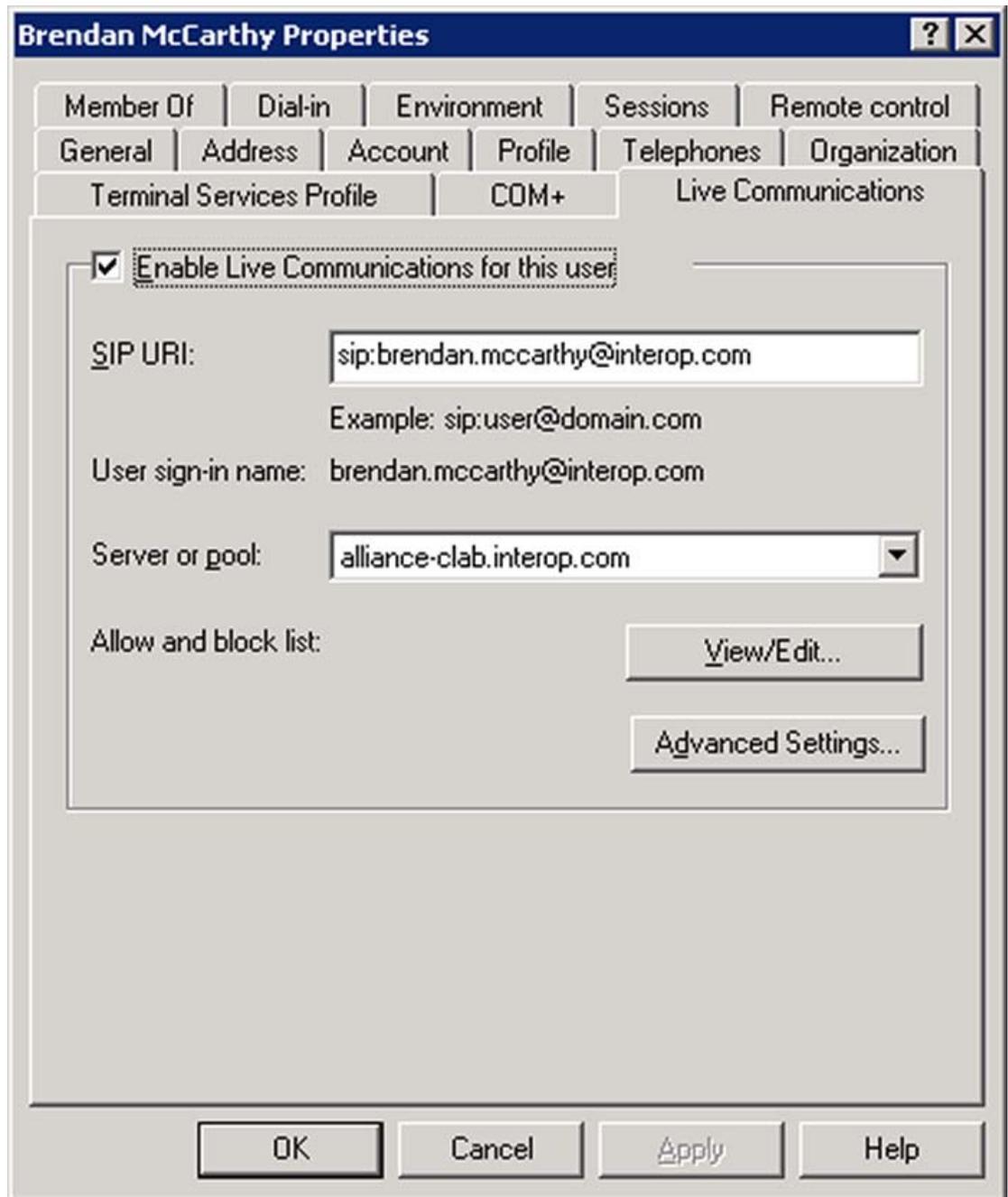


Figure 102: Active Directory configuration

## Enabling the Remote Call Control Flag

The status of the Enable Remote Call Control flag (see the following figure), either enabled or disabled, is enforced by MCM as a part of the authorization process.

If this flag is disabled, all attempts to use Remote Call Control through automatic or manual configuration in Microsoft® Office Communicator when authorization is enabled on MCM fail due to the status of this flag.

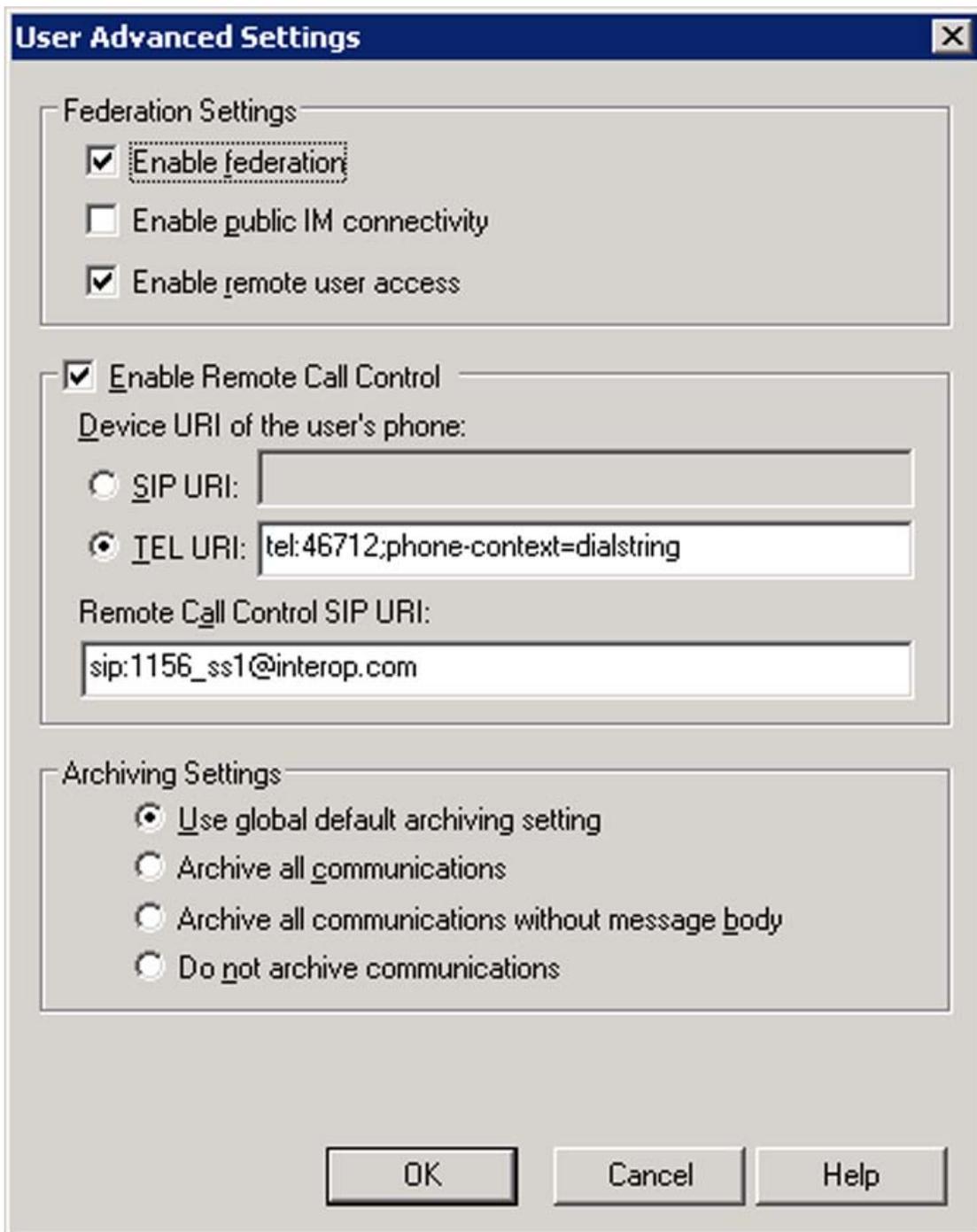


Figure 103: User Advanced Settings

## Defining the Remote Call Control Controlled Line (Device URI of the phone of the user)

This configuration defines the DN to be controlled, which depends on the LD 11 configuration for the TN on which the DN key resides.

CS 1000 SIP CTI services support the following URI formats to define the controlled line (DN) for Remote Call Control:

### TEL URI with a phone-context attribute

If the phone-context descriptor matches the UDP domain as configured in the SIP GW URI map, the HLOC is stripped from the telephone subscriber portion of the URI prior to issuing the AML IACR request.

In all other cases, the phone-context descriptor is ignored. Examples of this are:

- tel:3432330;phone-context=LCS2005S\_UDP
- tel:2330;phone-context=LCS2005S\_CDP.LCS2005S\_UDP
- tel:2330;phone-context=logicalDevice

### TEL URI without a phone-context attribute

For a TEL URI without a phone-context attribute, the number is assumed to be an E.164 number. For controlled lines, an ext attribute must be present for this to be considered a valid URI representing a controlled line.

The ext attribute value is used as the DN to acquire in the AML IACR request. For example:

```
tel:+16139712330;ext=2330
```

### SIP URI

A SIP URI derived from a TEL URI has the entire telephone-subscriber portion of the TEL URL, including any parameters, placed into the userinfo part of the SIP or SIPS URI.

If the SIP URI is derived from a TEL URI, then the equivalent TEL URI is handled according to the first two cases above.

### Examples

- sip:3432330;phone-context=LCS2005S\_UDP@cs1kdomain.corp.avaya.com:5060;user=phone
- sip:2330;phone-context=LCS2005S\_CDP.LCS2005S\_UDP@cs1kdomain.corp.avaya.com:5060;user=phone
- sip:2330;phone-context=logicalDevice@cs1kdomain.corp.avaya.com:5060;user=phone
- sip:+16139712330;ext=2330@cs1kdomain.corp.avaya.com:5060;user=phone

If the no user=phone attribute exists within the URI, the URI is not derived from a Tel URI. Therefore, the user portion must represent a user on the local PBX.

- The only users that are recognized on the CS 1000 are DNs.
- The user portion of the SIP URI is used as the DN in the AML IACR request. For example:  
sip:2330@cs1kdomain.corp.avaya.com

## Defining the Remote Call Control SIP URI

The Remote Call Control SIP URI is the per-client configuration parameter that defines the content of the request URI header field in the SIP INVITE sent from Microsoft® Office Communicator to the Live Communications Server home server to establish a TR/87 SIP dialog for Remote Call Control. For example:

sip:sw18\_FE@lcs2005.avaya.com

The routing configuration on the Live Communications Server Home Server defines how the TR/87 INVITE is routed based on the request URI:

- For example, the next hop for a Live Communications Server Home Server can be the proxy upon which the MCM resides.
- The MCM can be configured to route the request to an NRS or directly to a specific node with TR/87 support.

---

## Configuring the SIP URI Map

The existing SIP URI map (see [Figure 104: SIP URI Map](#) on page 188) configured for SIP GW application is also used by the TR/87 FE application to parse incoming URIs within SIP CTI service requests.



Public E.164 National domain name	Public E.164 Subscriber domain name	Public E.164 Unknown domain name	Public E.164 Special Number domain name	Private309 domain name	Private309 domain name	PrivateSpecial Number domain name	Private Unknown (occasional number routing) domain name	Unknown Unknown domain name
ip*homeoffice.com	*RIS	public unknown	public special	uds.inetop.com	cds.inetop.uds.inetop.com	special.udp.inetop.com	private.unknown	unknown.unknown

Figure 104: SIP URI Map

---

## Configuring the Do Not Disturb feature

To enable the Do Not Disturb feature (see [Figure 105: Enable Do Not Disturb](#) on page 189), perform the following:

## Configuring Do Not Disturb

1. Open Office Communicator 2005.
2. On the **Actions** menu, select **Options**.
3. In the **Options** dialog box, click the **Rules** tab.
4. Select **Enable Do Not Disturb on my phone automatically when my status is Do Not Disturb**.
5. Click **OK**.



### Note:

Enabling the Do Not Disturb feature also requires configuration of the “Make Set Busy” key on the phone.

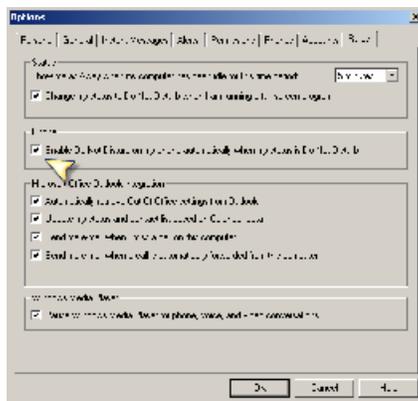


Figure 105: Enable Do Not Disturb

For more information about configuring Office Communicator, refer to the *Microsoft® Office Communicator 2005 Telephony Planning and Deployment Guide*, available on the Microsoft® Live Communications Server site:

<http://office.microsoft.com/en-us/communicationsserver/default.aspx>

---

## Configuring CDR

Call Detail Recording (CDR) records are produced for calls controlled using the Remote Call Control feature. The format of these CDR records is the same as those of calls dialed directly from a telephone's keypad.

---

# Configuring Microsoft® Office Communicator 2005

## Configuring Phone Integration Settings

Phone integration must be enabled on the Office Communicator 2005 client to enable the client to establish a Remote Call Control session at start-up.

Automatic configuration uses the Remote Call Control Settings defined for this Live Communications Server user in Active Directory.

Using manual configuration, the settings in Active Directory can be defined locally on a per-client basis (see [Figure 106: Phone Integration Settings](#) on page 190).

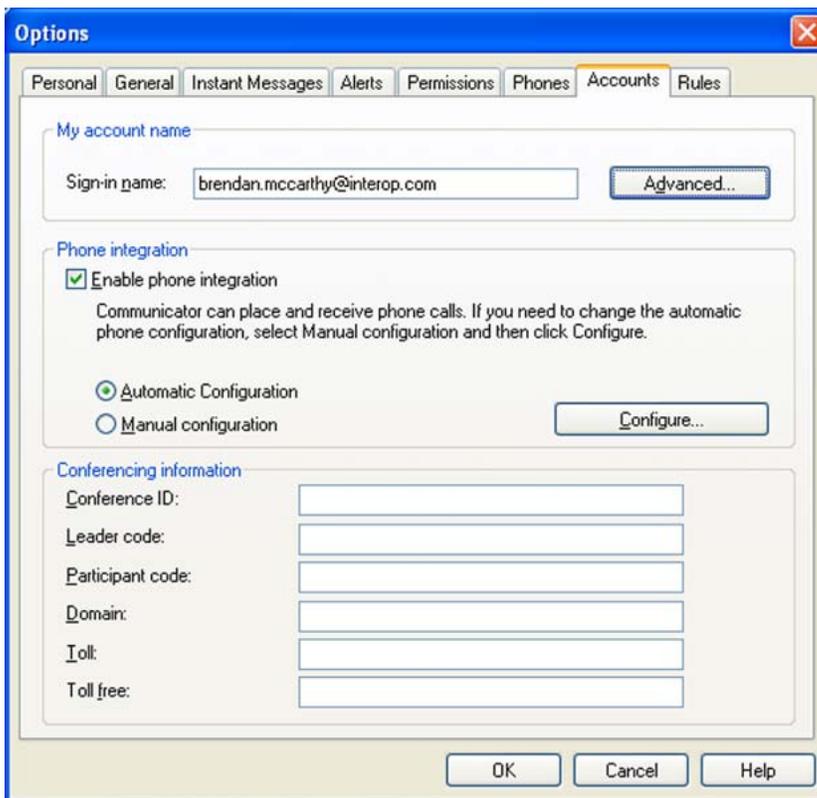


Figure 106: Phone Integration Settings

## Configuring Account details

To configure your account details, perform the following:

### Configuring account details

1. Open **Office Communicator 2005**.
2. On the Actions menu, select **Options**.

3. In the Options dialog box, click the **Accounts** tab.
4. Click **Advanced**.
5. Click **Configure Settings**.
6. In Server Name or IP address, type the fully qualified domain name (FQDN) of the SIP server.
7. Select **TCP** or **TLS**.
8. Click **OK**.

---

## Dialing E.164 International Format Numbers from Microsoft® Office Communicator - Phone Calls (SIP CTI)

When a call is originated from Microsoft® Office Communicator to an E.164 number (such as +14163005000) through Remote Call Control, the make call service request arrives at the TR/87 FE within a SIP INFO message as per the TR/87 specification. See [Figure 107: SIP INFO message](#) on page 191.

```
<?xml version="1.0"?>
<MakeCall xmlns="http://www.ecma-international.org/standards/ecma-323/csta/ed3">
  <callingDevice>
    tel:3432356;phone-context=nortel
  </callingDevice>
  <calledDirectoryNumber>
    tel:+14163005000
  </calledDirectoryNumber>
  <autoOriginate>
    doNotPrompt
  </autoOriginate>
</MakeCall>
```

**Figure 107: SIP INFO message**

The TR/87 FE that resides on the Signaling Server contains a feature to insert the appropriate dial plan prefix, either national or international, depending on the location of the Call Server and destination of the call. This ensures calls within the country use the national dial format and calls outside the country use the international dial format. This feature is enabled or disabled in Element Manager in the SIP CTI Settings section. When “All International Calls As National” is enabled, any calls within the local country have the country code stripped from the E.164 number and the national dial prefix applied. The format of the number presented by the TR/87 FE to the Call Server through AML in this scenario is:

<SIP CTI national prefix><national subscriber number>.

Any calls outside the country have only the international dial prefix applied to the E.164 phone number. The format of the number presented by the TR/87 FE to the Call Server through AML in this scenario is:

<SIP CTI international prefix><international number>.

When “All International Calls As National” is disabled, all calls to any E.164 destination use the international dial format. Refer to the section [Parameter: International Calls As National](#) on page 175 for additional detail on the configuration of this feature and an illustrative example.

---

## Normalizing phone numbers

Office Communicator 2005 requires that all phone numbers be in standard TEL URI format as defined in RFC 3966 for dialing and for reverse number lookup.

Office Communicator 2005 uses phone numbers that are provisioned (Active Directory and Outlook) and that are adhoc from the user through the user interface. All sources can be free format—a convention that is not in compliance with TEL URI.

For example:

(425) 7712345 x 12345

425-7712345

Phone numbers are normalized in Active Directory. Each user may have multiple phone numbers such as Office, Mobile, and Home. Two options are available to normalize these numbers: **Offline** and **Address Book Service**.



**Note:**

All normalization rules must be in Company script.

---

## Normalizing Offline (Recommended)

The user's phone number is read from the Active Directory user object, original fields. These numbers are normalized offline to TEL URI format and stored in Active Directory in a different field named proxy address (multi value). Microsoft® provides a reference on how to build a tool for this task.

If you use this option, then Address Book Service must not normalize the phone numbers and must instead publish only normalized phone numbers in the proxy address.

Each number in the proxy address is attached with an attribute that describes the phone number (for example: Office, Home, and so on).

For example:

tel:+14255551212;ad-rdn=telephoneNumber;displayName=(425)555-1212

The ad-rdn = telephoneNumber is a proprietary parameter describes the type of the phone number and displayName, which is a proprietary parameter that holds the display format of this phone number (by default, the original phone number before normalization).

By default, the msRTCSIP-RCC Line is copied from the proxy address (attribute ad-rdn=telephoneNumber). The phone number is copied without ad-rdn and display name parameters.

For example:

```
tel:+14257771234;ext=1234;ad-rdn=telephoneNumber;display-name="(425) 7771234 *  
1234"
```

is shown as:

```
tel:+14257771234;ext=1234
```

---

## Normalizing using the Address Book Service

The Run time: Address Book service normalizes the original phone numbers in Active Directory. In this case, the normalized phone numbers are not stored in Active Directory and the output cannot be analyzed before it is used by Office Communicator.

---

## Creating Normalization rules

Matching incoming calling numbers to the phone numbers for a Live Communications Server user, and transforming free-form dialstrings to URIs that can be called through TR/87, is performed by Live Communications Server 2005 and Office Communicator 2005 through a process called Normalization.

Normalization rules, according to Microsoft® guidelines, must be defined to make use of the integration of Office Communicator 2005 Remote Call Control and Live Communications Server 2005 Multimedia functionality.

Each Live Communications Server user that uses Office Communicator Remote Call Control capability must have appropriate Live Communications configuration (in addition to the per-TN configuration discussed previously).

You must consider and define SIP routing for TR/87 sessions for each Live Communications Server user.

MCM provides authorization of Remote Call Control service requests based on the configuration defined in Active Directory for each Live Communications Server user.

Microsoft® Office Communicator requires that all phone numbers be in the standardized TEL URI format (RFC 3966) for reverse number lookup (matching the phone number of an incoming call to a known Live Communications Server user) and for dialing (either through an adhoc interface or through a menu from a user object).

Matching an incoming phone number to a Live Communications Server user identity is used to establish multimedia sessions. If the Live Communications Server user identity cannot be determined from a phone number, then Live Communications Server multimedia sessions cannot be established with the calling or called party.

Most Microsoft® interfaces and applications accept phone numbers as free-form strings. For example:

- Entering 3000 from Microsoft® Office Communicator
- Using an existing number in active directory such as ESN 343-2356
- Using an Outlook contact wizard that creates +1(613)971-2356

Normalization is the process by which a free-form string is mapped to a TEL URI. Some sample mappings for the numbers above to TEL URIs (with appropriate rules) might be:

- tel:3000;phone-context=dialstring
- tel:63432356;phone-context=dialstring
- tel:+16139712356

Refer to the *Microsoft® Office Communicator Planning and Deployment Guide* on the Microsoft® support site for further details:

<http://office.microsoft.com/en-us/communicationsserver/default.aspx>

For more in-depth information about deploying the Address Book Service, refer to the *Address Book Service Planning and Deployment Guide*, also available on the Microsoft® support site.

## Example

A Live Communications Server user accesses an Active Directory phone number for Jim (in Outlook, for example) to make a Remote Call Control phone call. Office Communicator uses normalization to map the free-form phone number to a TEL URI prior to sending the TR/87 Make Call service request. You can assume the following points for normalizing phone numbers:

- The normalization method chosen is Address Book Service – "Run time" as opposed to using the offline method
- An Active Directory entry exists for Jim with business phone number ESN 343-2356
- A normalization rule exists that defines a regular expression (as defined in [Figure 108: Normalization rule example](#) on page 194) to map ESN 343-2356 to tel:63432356;phone-context=dialstring

```
#
# ESN ddd-dddd
#

.*ESN\s* (\d\d\d) [\s () \-\. /] * (\d\d\d\d)
6$1$2;phone-context=dialstring
```

**Figure 108: Normalization rule example**

## Result

The normalized version (tel:63432356;phone-context=dialstring) of the business number in Active Directory entries is stored in the Global Address List (GAL) and downloaded at login by the Office Communicator 2005 client from the Address Book Service.

When you use a contact in a buddy list for Jim, or any other Microsoft® Office Application that makes use of Active Directory phone numbers, the URI sent to the TR/87 FE for a TR/87 Make Call service request is:

tel:63432356;phone-context=dialstring

## Adding a new Normalization rule

The procedure, Adding a new Normalization rule describes the process of adding a new normalization rule.

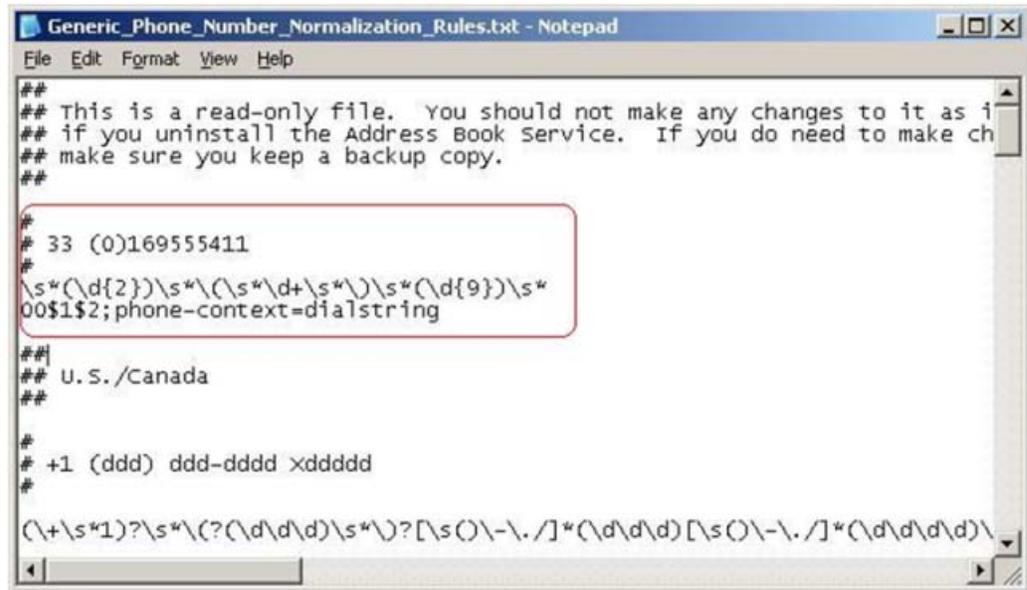
### Adding a new normalization rule

1. Add an appropriate rule to the beginning of the “%ProgramFiles%\Microsoft LC 2005\Address Book Service\Generic\_Phone\_Number\_Normalization\_Rules.txt” file (see [Figure 109: Generic phone number normalization rules](#) on page 196). A description of the language used in the Address Book Normalization rules can be found in:

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/cpgenref/html/cpconregularexpressionslanguageelements.asp>

The rules file uses a format of: 1) Regular expression; 2) Replacement pattern.

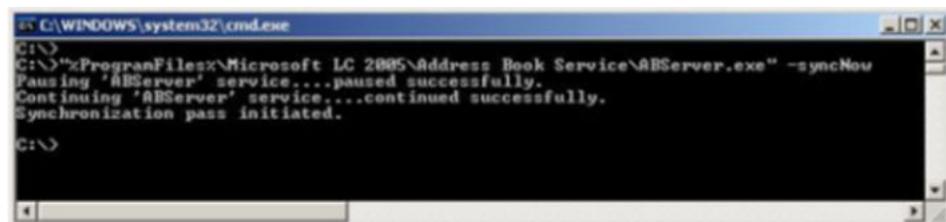
2. As in Step 1, add an appropriate rule to the beginning of the “%ProgramFiles%\Microsoft LC 2005\Address Book Service\Company\_Phone\_Number\_Normalization\_Rules.txt” file. This ensures that the email notification provides the correct link.



**Figure 109: Generic phone number normalization rules**

3. Refresh the Address Book on the server (as shown in [Figure 110: Refresh Address Book on the server](#) on page 196) by issuing the following command on the server running ABService:

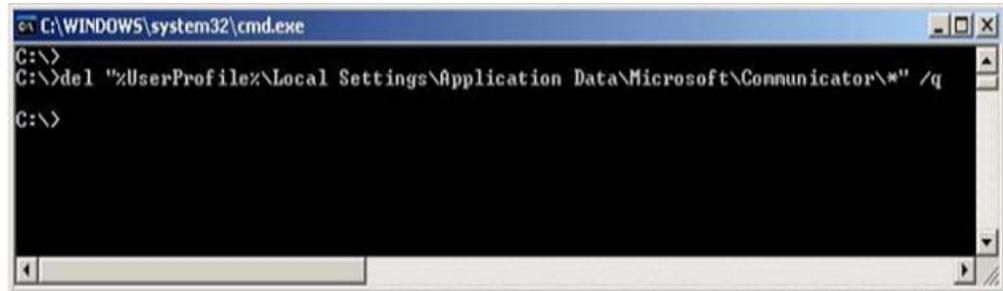
“%ProgramFiles%\Microsoft LC 2005\Address Book Service\ABServer.exe - syncNow”



**Figure 110: Refresh Address Book on the server**

4. Exit from Office Communicator 2005.
5. Refresh Address Book on the client (as shown in [Figure 111: Refresh Address Book on the client](#) on page 197). Issue the following command on the PC running Office Communicator 2005:

Del “%UserProfile%\Local Settings\Application Data\Microsoft\ Communicator\\*” / q



**Figure 111: Refresh Address Book on the client**

6. Launch Office Communicator 2005.

---

## Configuring SIP Routing and Redundancy

Microsoft® Office Communicator 2005 is a soft phone application as well as a SIP User Agent (UA). Live Communications Server Home Server (Standard Edition Server or Enterprise Edition Server) hosts Office Communicator 2005.

The TR/87 FE within the CS 1000 is also a SIP UA. Office Communicator 2005 establishes a SIP dialog in one direction only: from the application to the TR/87 FE. The Live Communications Server home server, which functions as a SIP Proxy, is a required component. The Multimedia Communications Manager (MCM) is also required to provide support for authorization and the use of an NRS.

**\* Note:**

Due to the inability of the Office Communicator 2005 client to support the SIP 302 redirect message (a fundamental requirement for the basic operation of the NRS), the MCM application installed on the Live Communications Server to support Telephony Gateway and Services functionality is also a required component for Remote Call Control support when using Microsoft® Office Communicator 2005. The MCM application handles the 302 redirect message on behalf of Office Communicator 2005 clients.

When Office Communicator 2005 establishes a dialog with the TR/87 FE, it also retrieves the SIP address for the TR/87 FE from the Active Directory (Automatic) or from a specific server using the specified protocol (Manual). The SIP address for the Remote Call Control Gateway can be in phone address format. [Table 9: SIP Examples](#) on page 197 shows examples of these addresses:

**Table 9: SIP Examples**

Item	Example
SIP From header	sip:alice@avaya.com
SIP To header (using a gateway endpoint name)	sip:tr87fe1@avaya.com

Item	Example
SIP To header (using a phone address)	sip:2356;phone-context=cdp.domain@avaya.com;user=phone
Device ID (Phone URI)	tel:2356; phone-context=cdp.domain

---

## Configuring Remote Call Control SIP Routing Using Phone Addressing

When an NRS is used with SIP addressing, based on the phone address format, the CS 1000 TR/87 FE used to support a Remote Call Control session for a user must be co-resident with the SIP GW. This is essential, as the URI that is present in the INVITE to establish a TR/87 session is identical to the URI used to place a SIP call to the user. Thus, the NRS redirects the INVITE based on the request URI only (and not the mime content type within the INVITE).

The TR/87 FE recognizes the TR/87 mime type within an INVITE and intercepts the TR/87 INVITE if it is co-resident with the SIP Gateway. This ensures that both TR/87 sessions and phone calls with the same request URI are handled appropriately — either by the TR/87 FE or SIP Gateway, on the same Signaling Server.

---

## Configuring Remote Call Control SIP Routing Using a Gateway Endpoint Name

If NRS is used, you must configure MCM and the TR/87 FE on the NRS as Gateway Endpoints. You can use the gateway endpoint name as the Remote Call Control URI to define the TR/87 FE that is used to service a group of users. Given that the gateway endpoint name is independent of the URI used to address a user to place a SIP call, no dependency exists on the choice of a gateway endpoint name and URIs that may be used to place SIP calls to the user. If this addressing method is used, the TR/87 FE may or may not be co-resident on the SIP gateway.

The SIP Request URI and the To: headers are populated with msRTCSIP-LineServer, provisioned in Active Directory. Office Communicator sends an INVITE message to the Live Communications Server 2005 Home Server, which hosts Office Communicator. The Home Server is identified by settings entered on the Advanced Connection Setting dialog, which is accessible from the Accounts page of the Options dialog in Office Communicator 2005.

The Live Communications Server 2005 SP1 home server forwards the INVITE message to the Next Hop FQDN, based on a static routing rule for the URI in the INVITE Request URI addressTo. The Next Hop FQDN defines a path for the INVITE that eventually leads to the proxy on which the MCM resides, or to the Signaling Server, which defines the TR/87 FE that supports the Remote Call Control session for this user.

If the Next Hop is not a Live Communications Server 2005 server, the Next Hop device must be provisioned as a secure link. When the SIP dialog is initially established, the same dialog

path is used in both directions to route subsequent SIP messages. For information about configuring static routes, refer to the next section: "Configuring Static Routes on Live Communications Server 2005".

 **Note:**

Geographic Redundancy is supported only with the Phone Addressing format, as the alternate routing logic used to provide Geographic Redundancy for virtual trunk calls is also used for TR/87. For more information on alternate routing logic, refer to Avaya IP Peer Networking: Installation and Commissioning (NN43001-313).

---

## Configuring Redundancy

For information on Redundancy, refer to [Redundancy](#) on page 77.

---

# Deploying Live Communications Server Client PC application to end users

The following installations are performed after all other components are configured and tested.

---

## Installing Windows Messenger 5.1

Windows Messenger 5.1 must be installed on the user's desktop before you install Office Communicator. Installing Messenger is required for "presence" in Microsoft® Office applications.

 **Note:**

Although Windows Messenger 5.1 is not supported for the Avaya Converged Office feature, it is required to support Office Communicator 2005.

For information about Windows Messenger 5.1 installation, refer to the *Microsoft® Office Communicator 2005 Telephony Planning and Deployment Guide*, available at:

<http://office.microsoft.com/en-us/communicationsserver/default.aspx>

---

## Installing Microsoft® Office Communicator 2005 client software

This section guides you through the steps to install the client component of Microsoft® Office Communicator 2005 (version 1.0) on a user's desktop.

To ensure that Office Communicator 2005 operates properly, a number of group policies must be created, and they must be configured in the correct order. There are a number of deployment methods available. For a full description of the deployment options, refer to the *Microsoft® Office Communicator 2005 Telephony Planning and Deployment Guide*, available at:

<http://office.microsoft.com/en-us/communicationsserver/default.aspx>

## Installing the Client

Use the following procedures to install the client component of Office Communicator 2005.

### Installing Office Communicator 2005

1. Double-click **Communicator.msi**.
2. Follow the instructions in the Office Communicator 2005 Setup wizard.

### Silent installation of Office Communicator 2005

1. Use the following script to silently install Office Communicator 2005:

```
%SERVERPATH%\Communicator.msi /q
```

2. After it is installed, launch Office Communicator 2005 using the following script:

```
%Program Files%\ Microsoft Office Communicator\  
communicator.exe
```



#### **Important:**

The following hotfixes are required when using Office Communicator 2005 with CS 1000 , and can be found under **C:\Program Files\Microsoft Office Communicator**:

- Communicator.exe
- Lcmedia.dll

At the time of publication, version 1.0.559.212 is the most current for each of these files. Refer to <http://support.microsoft.com/> and search for hotfixes for Office Communicator 2005 (search "1.0.559").

For more hotfix information, refer to the following MS Knowledge Base Article:

<http://support.microsoft.com/kb/928606>

For a full description of the Office Communicator installation process, refer to the *Microsoft® Office Communicator 2005 Telephony Planning and Deployment Guide*, available at:

<http://office.microsoft.com/en-us/communicationsserver/default.aspx>

---

## Installing Microsoft® Office 2003 and Windows XP

For full Live Communications Server integration, you must install Microsoft® Office 2003 (or later) and Windows XP (full integration). For information about how full integration may be

achieved with earlier versions of Microsoft® Office, refer to the Live Communications Server site:

<http://office.microsoft.com/en-us/communicationsserver/default.aspx>

---

## Configuring Transport Layer Security (TLS)

---

### Limitations and requirements

#### End to End security

“End To End Security” is not supported for Converged Office solution/CS 1000 Node configuration.

#### Issued To (subject) parameter

The Issued To (Subject) parameter must be FQDN for all certificates used by Converged Office solutions (for example: Live Communications Server, SPS, SIP Gateway).

#### Security Options

The Security Option “System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing” must be enabled on the Live Communications Server that talks to the CS 1000 using TLS. This option is automatically enabled by MCM if TLS transport is configured.

Enabling this option affects other system components (Terminal Services, Encrypting File System Service). For example, Remote Desktop Client cannot connect to the server from a Windows 2000 PC because it does not support FIPS. New Remote Desktop Client must be installed on the Windows XP PC (Windows 2003 Server %SystemRoot%\System32\Clients\tsclient).

#### Local host IP Address

Local host IP Address 127.0.0.1 must be authorized on the Live Communications Server that talks to the CS 1000 using TLS. Authorization is performed by MCM automatically if TLS transport is configured.

## DNS server

The DNS server used by Live Communications Server must resolve SPS FQDN to its IP address—and vice versa.

## Private Certificate Authority (Avaya ECM)

Certificates signed by the Private CA (Avaya ECM) cannot be used on the Live Communications Server. For example, certificates for LCS servers must be issued by either Microsoft CA or another external CA (refer to Microsoft's Live Communications Server 2005 Configuring Certificates:

<http://office.microsoft.com/en-us/FX011450741033.aspx> <http://office.microsoft.com/en-us/FX011450741033.aspx>

---

## Configuring TLS

The next procedure describes how to configure TLS for Converged Office. For this procedure, the following is assumed:

A Live Communications Server SE Home Server running MCM with:

- IP Address – 192.168.60.9
- FQDN – mslcsserver.mslcs.mera.ru

A SIP Proxy Server (SPS):

- IP Address – 192.168.29.100
- FQDN – aknv-4221.mera.ru

Live Communications Server uses certificates issued by the Microsoft Certification Authority. CS 1000 components use the Private CA (Avaya ECM) signed certificates.

### Configuring TLS

1. Configure the DNS server (see [Figure 112: Configure the DNS server](#) on page 203) used by Live Communications Server to resolve SPS FQDN to its IP Address and vice versa.

 **Note:**

If SPS is used by MCM in a Redirect mode (Redirect All, Proxy SIP and Redirect SIP-CTI) then FQDNs of all SIP Gateways with TLS enabled must be resolved to IP Addresses by DNS and vice versa.

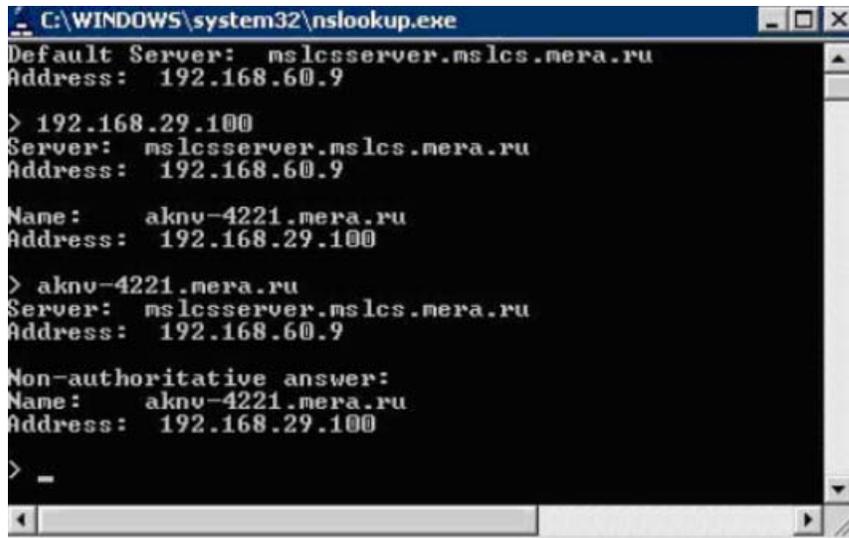


Figure 112: Configure the DNS server

2. Add Private CA certificate to the Trusted Root Certification Authorities

Copy and Save Private CA certificate to a file on the LCS server (see [Figure 113: Private Certificate Authority](#) on page 203).

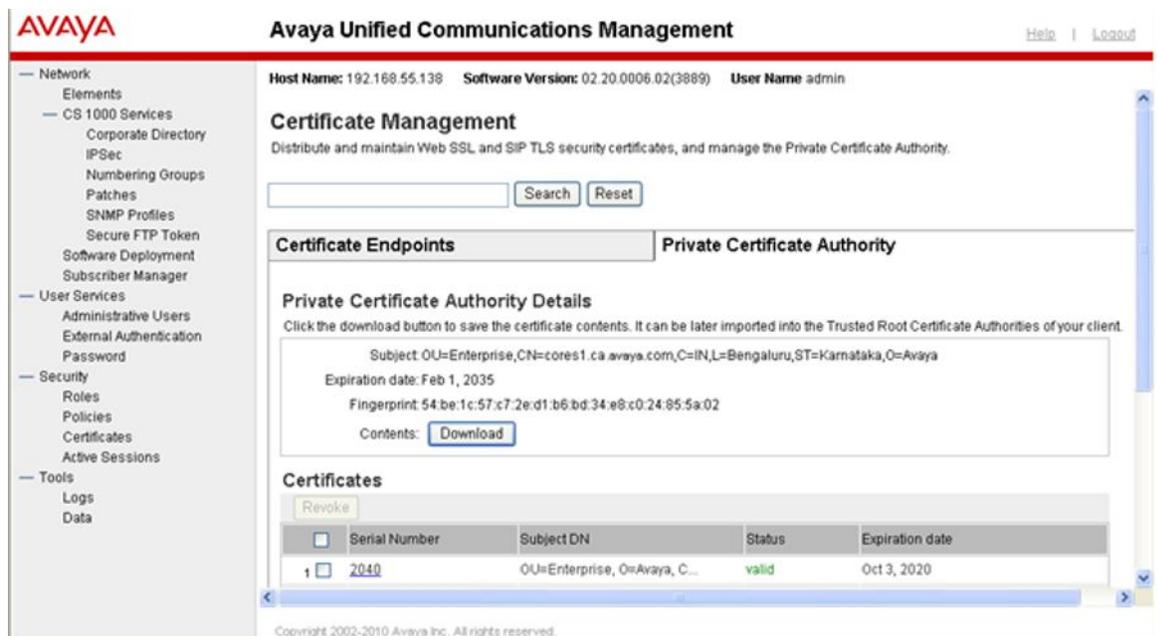


Figure 113: Private Certificate Authority

3. Open MMC on the Live Communication Server and add the Certificates (Local Computer) snap-in (see [Figure 114: Certificates snap-in](#) on page 204).

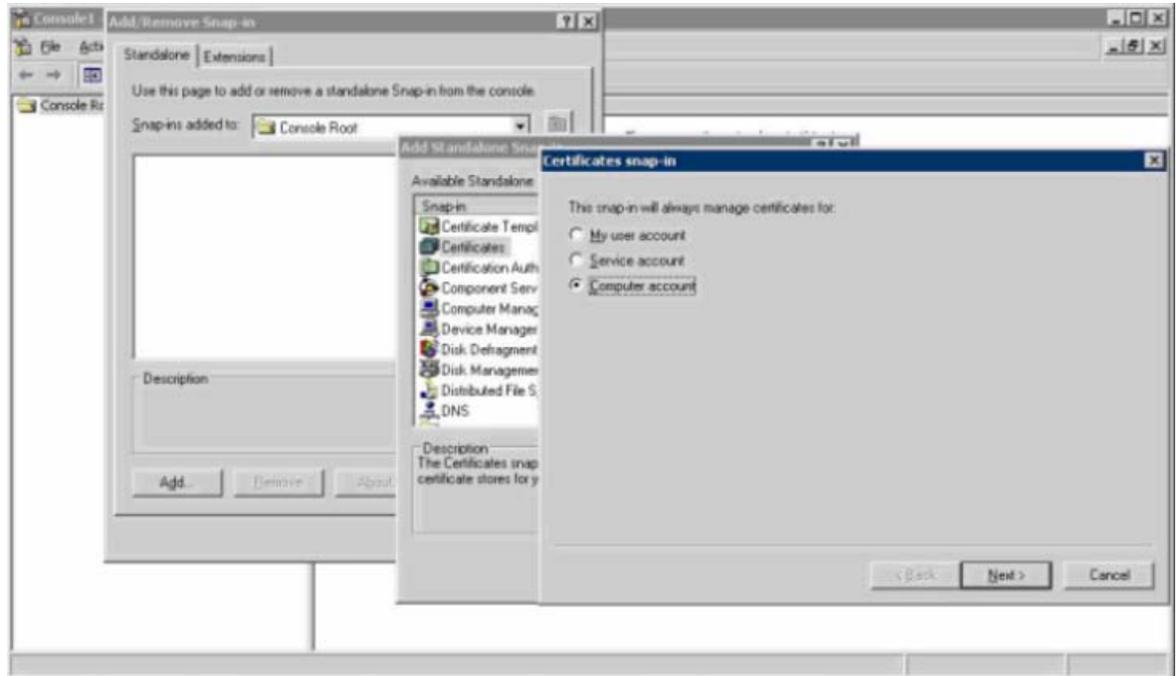


Figure 114: Certificates snap-in

4. Import the saved file to the Trusted Root Certification Authorities (see [Figure 115: Import to Trusted Root Certificate Authorities](#) on page 204).

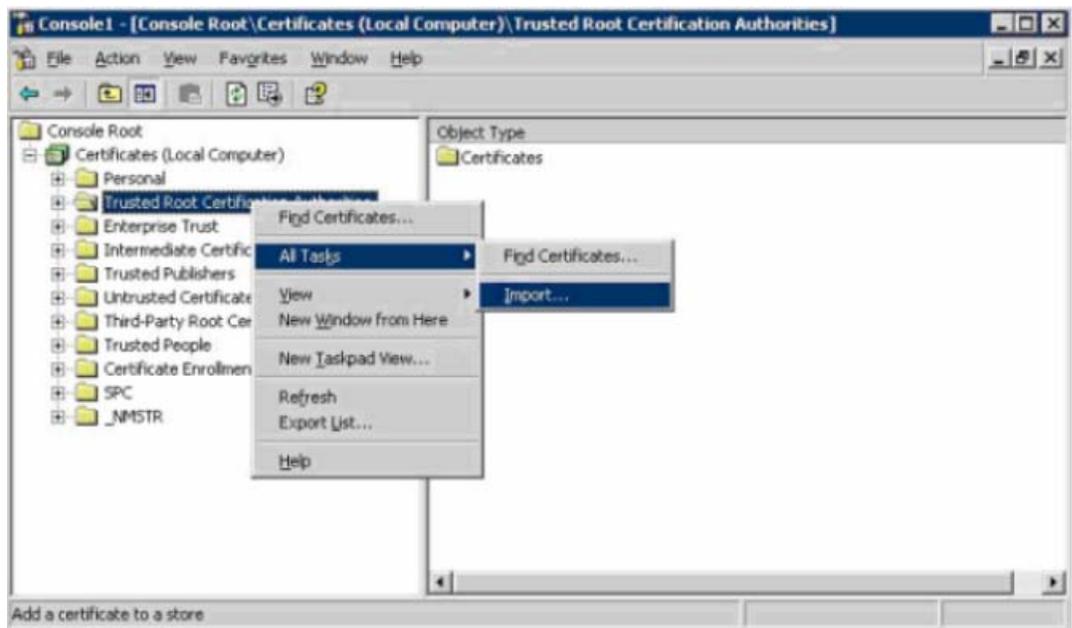
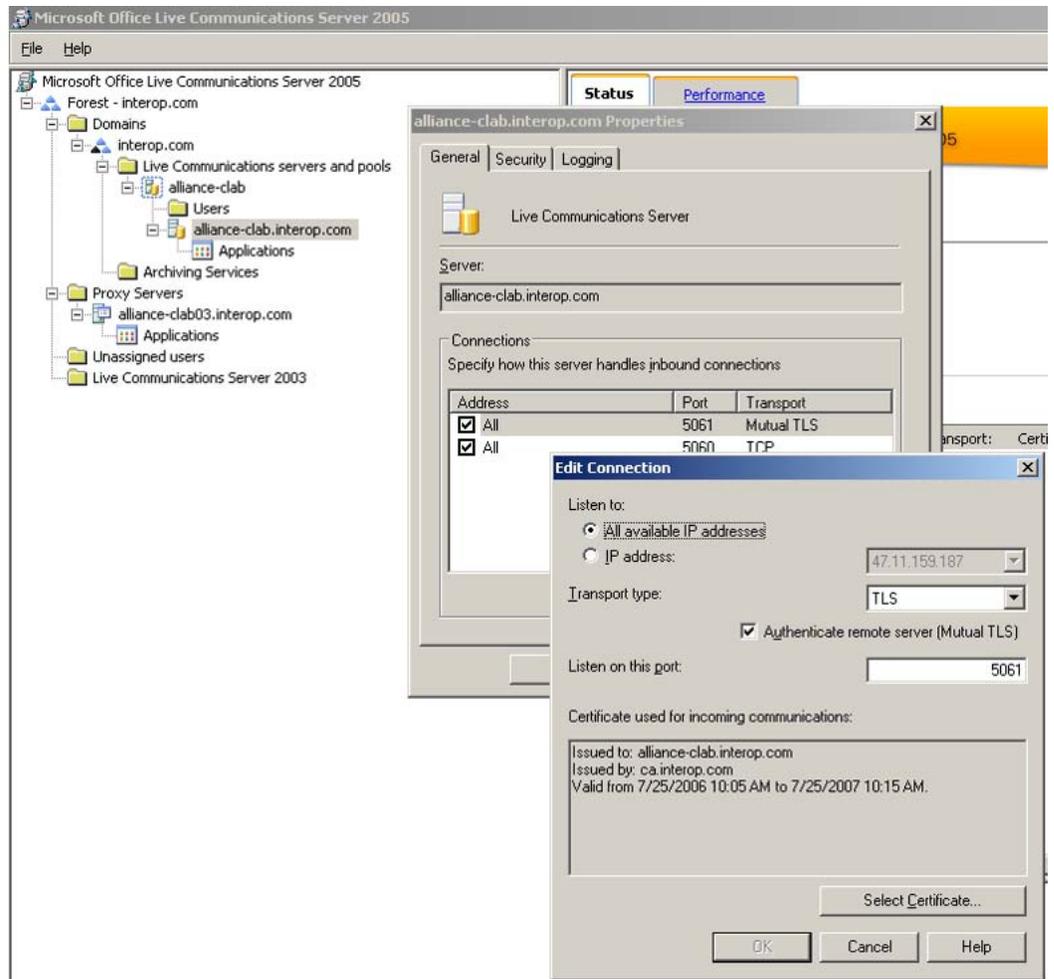


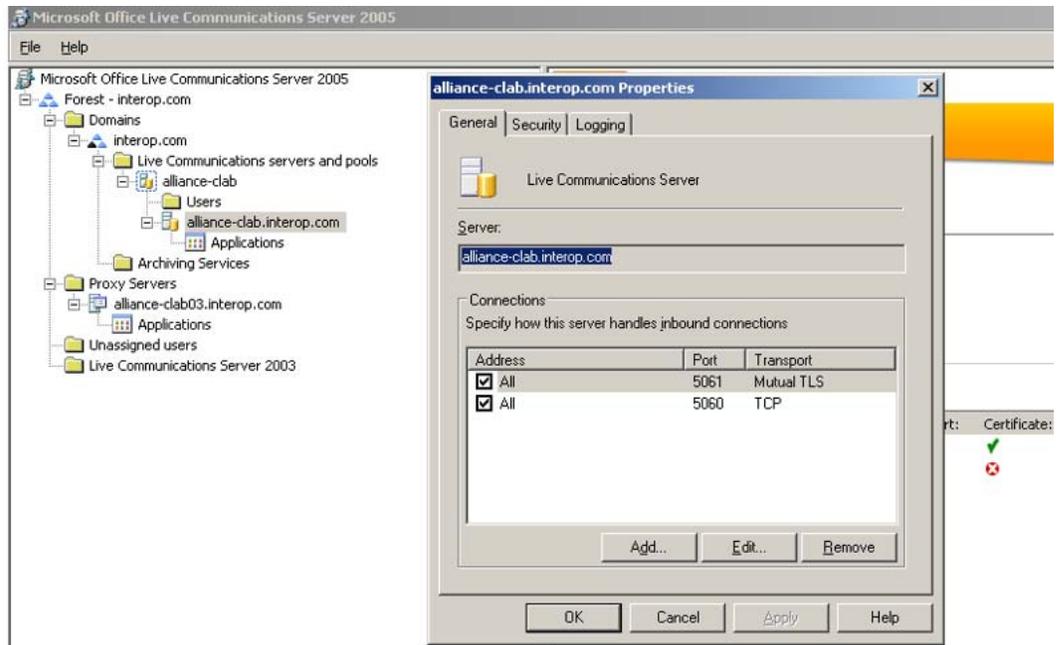
Figure 115: Import to Trusted Root Certificate Authorities

5. Enable incoming TLS connections on the Live Communication Server (see [Figure 116: Enable Incoming TLS connections](#) on page 205).



**Figure 116: Enable Incoming TLS connections**

6. Configure the default certificate used for outgoing TLS connections by the Live Communications Server (see [Figure 117: Configure default certificate](#) on page 206).



**Figure 117: Configure default certificate**

7. Add **SPS FQDN** to the Host Authorization table on the Live Communication Server (see [Figure 118: Add SPS FQDN](#) on page 207).

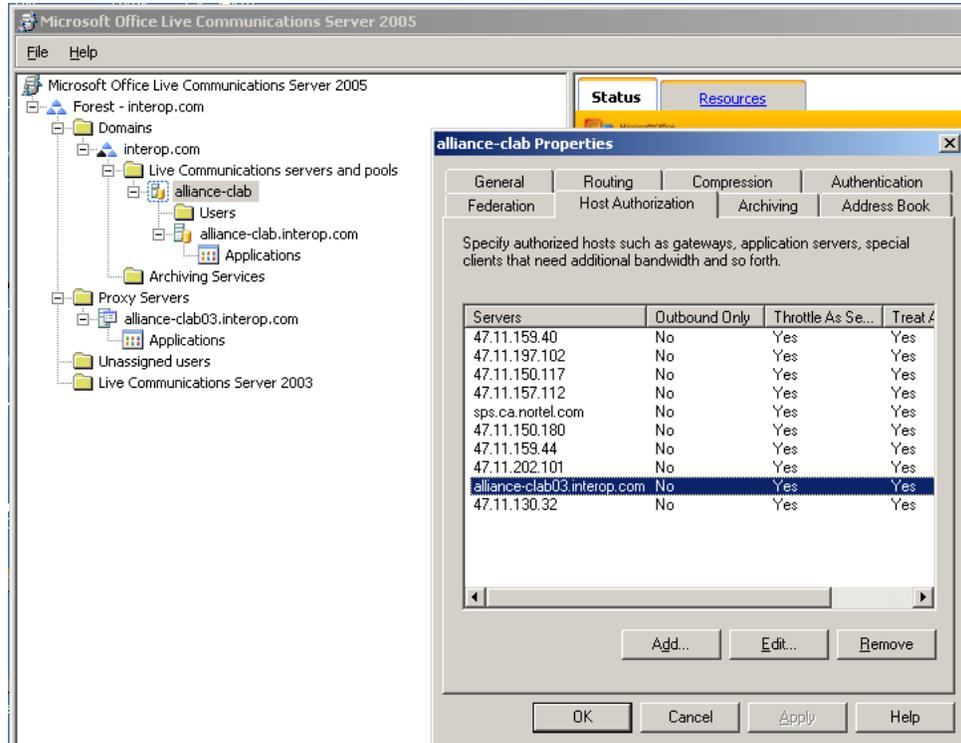
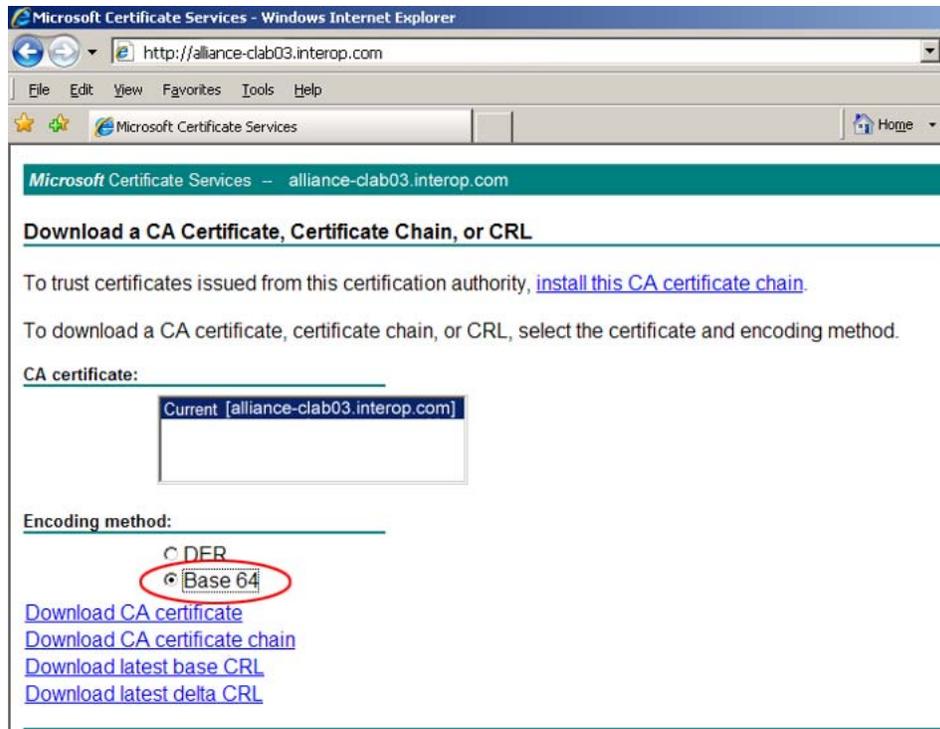


Figure 118: Add SPS FQDN

**Note:**

If SPS is used by MCM in a Redirect mode (Redirect All, Proxy SIP and Redirect SIP-CTI) the FQDNs of all SIP Gateways with TLS enabled have to be added to the table.

8. Add Microsoft CA certificate to the Trusted Certificate Authorities on SPS (see [Figure 119: Add Microsoft CA Certificate](#) on page 208). Download Microsoft CA certificate and save it to file on the Live Communication Server in Base-64 encoding



**Figure 119: Add Microsoft CA Certificate**

9. Open the saved file in Notepad and copy its content to clipboard. Add the copied content to the Trusted Certificate Authorities (see [Figure 120: Add a CA to the Service](#) on page 209).

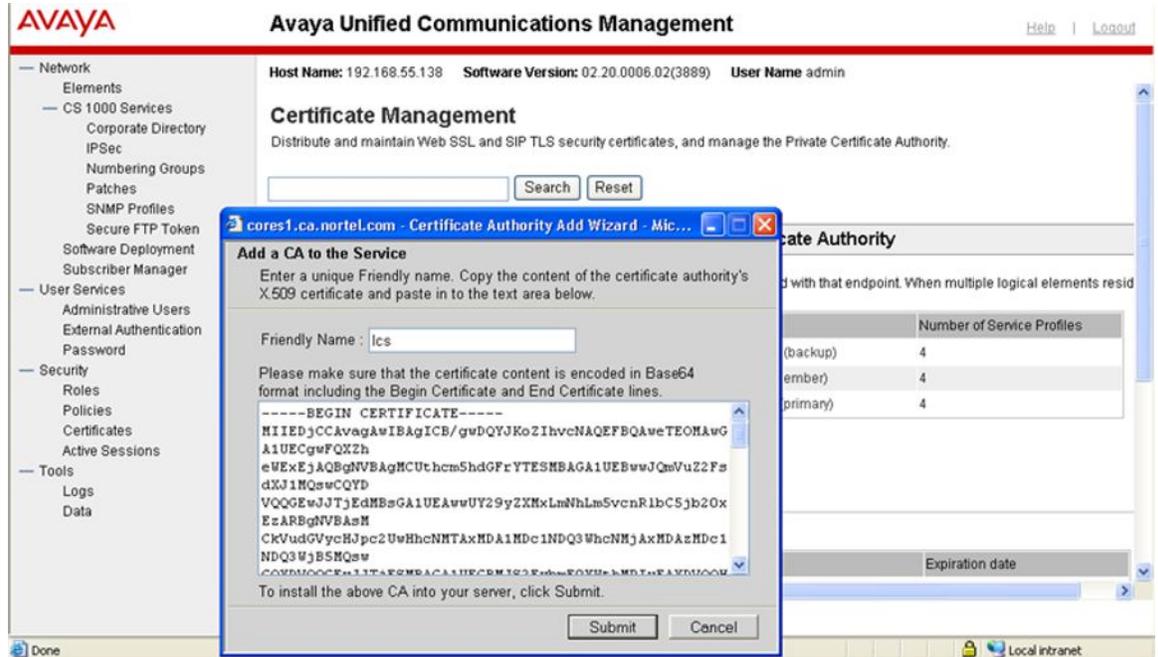


Figure 120: Add a CA to the Service

The following figure shows the newly added Certificate Authority:

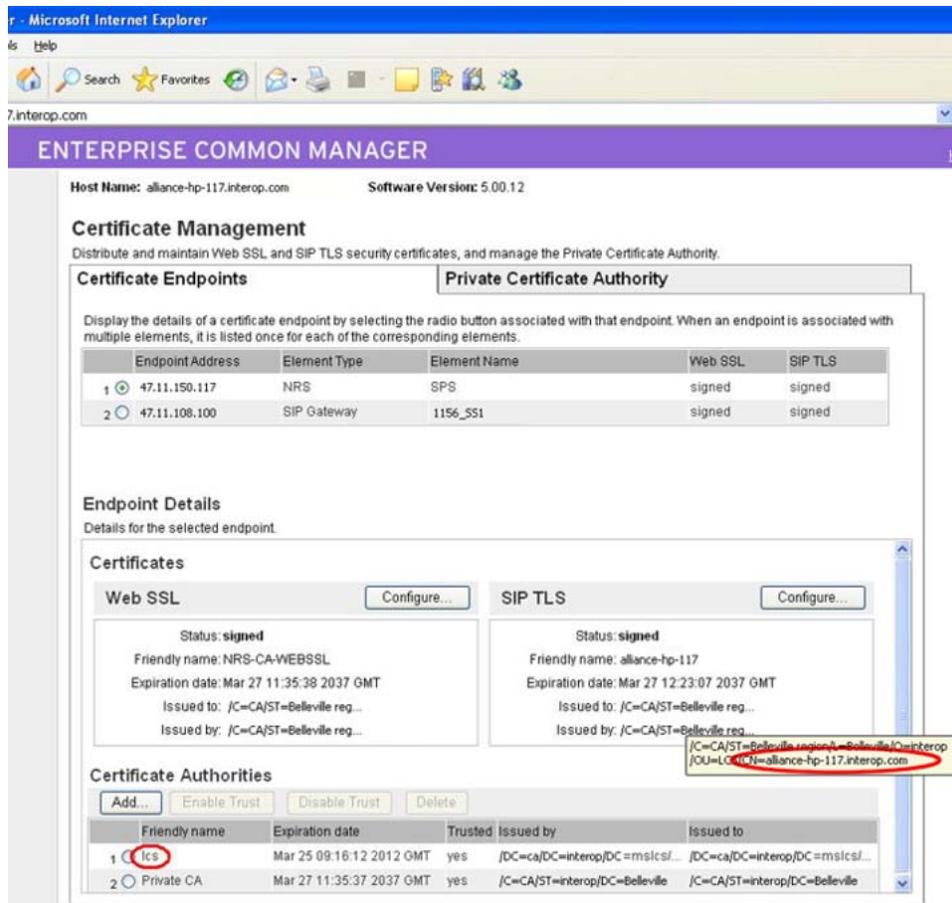
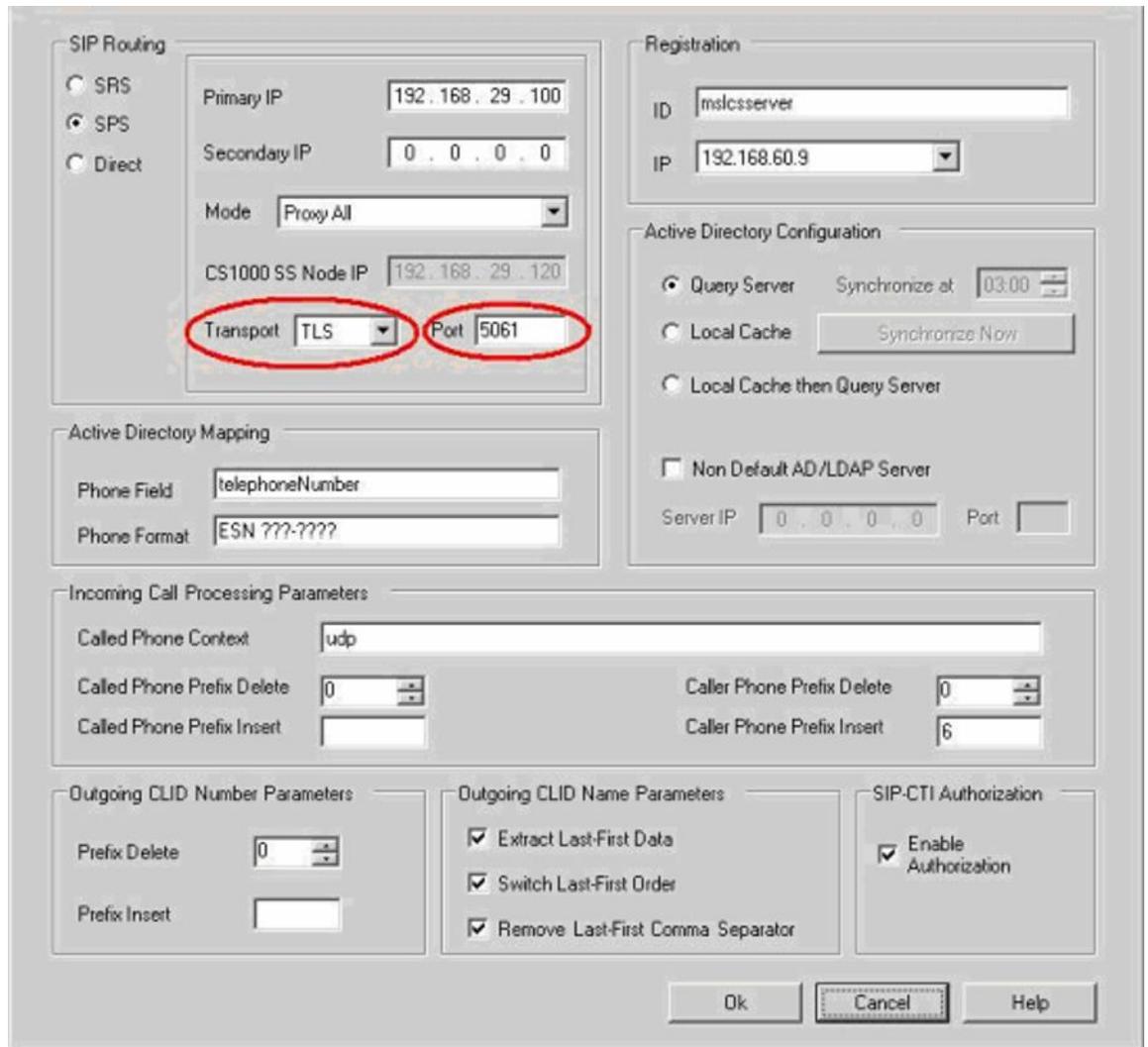


Figure 121: Certificate Endpoints

**Note:**

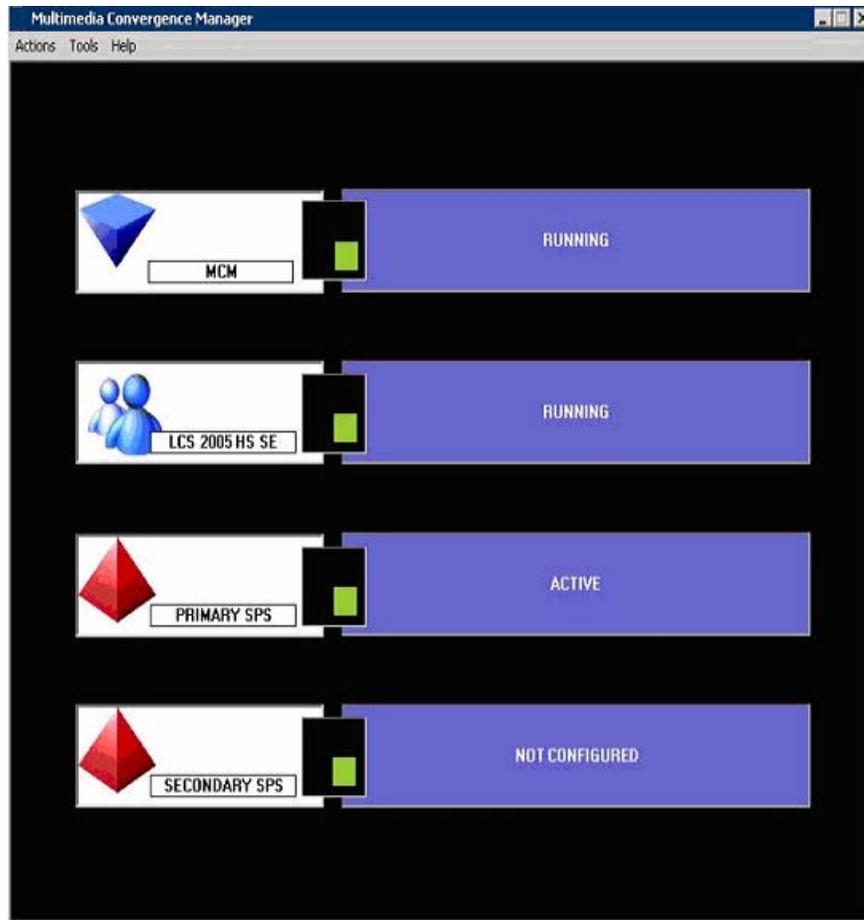
The Certificate used by SPS is issued to its FQDN. If SPS is used by MCM in a Redirect mode (Redirect All, Proxy SIP and Redirect SIP-CTI) then the same actions have to be done for each SIP GW/SIP CTI FE.

10. Configure TLS transport on MCM as shown in [Figure 122: Configure TLS transport](#) on page 211.



**Figure 122: Configure TLS transport**

11. Check that MCM is registered with SPS (see [Figure 123: MCM Status](#) on page 212).



**Figure 123: MCM Status**

If the SPS status is NOT RESPONDING, it may take up to five minutes until all the Live Communication Server changes are applied.

For more information on TLS, refer to:

- *Avaya Security Management (NN43001-604)*
- Microsoft's Live Communications Server 2005 Configuring Certificates: <http://office.microsoft.com/en-us/FX011450741033.aspx>

# Chapter 8: Maintenance

---

## Contents

This section contains information about the following topics:

[Introduction](#) on page 213

[Telephony Gateway and Services](#) on page 213

[Remote Call Control](#) on page 216

---

## Introduction

The following are maintenance and troubleshooting tips for the Telephony Gateway and Services and Remote Call Control components.

---

## Telephony Gateway and Services

---

### Avaya Communication Server 1000

No new SIP tracing capabilities are available on the Avaya Communication Server 1000 (Avaya CS 1000). Existing SIP Trunk and Gateway tracing capabilities are used.

---

## MCM

MCM 2.0 provides the following maintenance features:

## Tools

MCM provides the following commands on the Tools menu:

- Active Directory Query: Check phone to user-id mapping. DNs can be entered, and found user-ids are displayed
- Backup Data: Back up a configuration file to the user specified location.
- Restore Data: Restore configuration files from user specified location.
- Set Log Level: Determine (configure) which information is logged in the MCM log file. For more information about logging, refer to [Logging](#) on page 214.
- Get Active Calls Count: Show how many calls are connected through Live Communications Server.
  - The Multimedia Convergence Manager 1.0 service provides a test capability to retrieve user-id by phone number.
  - The Primary and Secondary NRS status utility is available from the application main window.
  - You can deploy Ethereal software on the Live Communications Server 2005 Application Proxy to provide call traces. MCM also provides full SIP-tracing capability. MCM SIP tracing is important particularly when MTLS (Mutual Transport Layer Security) is enabled in future CS 1000 releases- where SIP traces cannot be captured by a tool like Ethereal. MCM SIP tracing can be filtered by DN number. MCM SIP tracing is implemented as part of the application logging functionality. Special commands are not required.
  - You can remotely access the Live Communications Server application using the Windows 2003 server remote access capability.
  - Task Manager is supported in Windows 2003 Server for MCM.

## Logging

MCM 2.0 logging has the following levels:

- None: No messages or alarms are logged to the file. (Alarms are still logged to Windows Event Viewer).
- SIP: SIP messages (filtered by distinct DN) are logged further to alarms. Only one DN can be specified at the same time in MCM 2.0.
- Debug: Debug information is logged to the MCM log file.
- SIP and Debug

The MCM 2.0 creates a daily log file with no maximum size restrictions and no cleanup procedures are implemented. The contents of the existing log file remain in all cases.

SNMP is not supported on MCM 2.0 application. Alarms are logged to an MCM log file in addition to the Windows 2003 Event Viewer.

Generally, when a problem is encountered, it is recommended that you check the logs as follows:

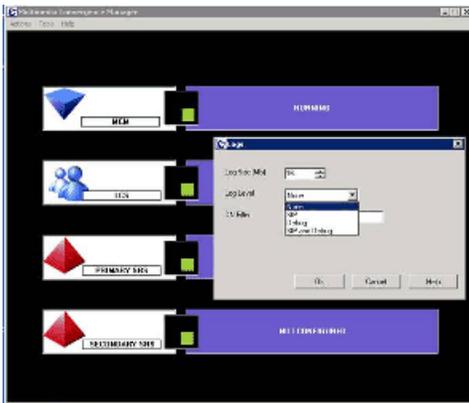
1. CS 1000 Signaling Server logs
2. MCM logs
3. Live Communications Server logs.

The following section details how to turn on MCM logging and what to expect.

### MCM.log file

The MCM log is captured through the MCM utility OAM.

Select **Tools > Set Log Level**. Configure the Log Level to Debug (see [Figure 124: MCM Logs](#) on page 215). This is the highest level of debug. The MCM.log file is located in the following directory: Program Files/Avaya/MCM/MCM.log.



**Figure 124: MCM Logs**

The following is an example of an MCM log:

```
-----
-----
05.04.2006 12:44:07: 1.0.19.14: Debug: ServerEventHandler: got Event
#0
05.04.2006 12:44:07: 1.0.19.14: Debug: ServerEventHandler: got Event
#0
05.04.2006 12:44:08: 1.0.19.14: Debug: ServerEventHandler: got Event
#0
05.04.2006 12:44:08: 1.0.19.14: SIP:
-----
-----

Request: INVITE sip:svg-cs 1000@domain.local
contact: <sip:werner@domain.local:1668;maddr=192.168.77.100;transport=
tcp;ms-received-cid=B00>
via: SIP/2.0/TCP192.168.77.100:13224;ms-received-port=
1668;ms-received-cid=b00
max-forwards: 70
from: "Werner Myrvang"<sip:werner@domain.local>;tag=a8d52f94b8;epid
=a64eccfac2

to: <sip:sip:svg-cs 1000@domain.local>
call-id: 3b55793fa6da4109bbb73f580d7002ae
```

```
cseq: 1 INVITE
user-agent: LCC/1.3
supported: timer
Session-Expires: 1800;refresher=uac
Min-SE: 1800
content-disposition: signal;handling=required
content-type: application/csta+xml
content-length: 350

<?xml version="1.0"?> <RequestSystemStatus xmlns="http://www.ecma-
international.org/standar
ds/ecma-323/csta/ed3"><extensions><privateData><private><lcs:line
xmlns:lcs="http://schemas.microsoft.com/Lcs/2005/04/ RCCExtension'>tel:67381:phones-
context=cdpsvg-cs 1000.livecommmlab.com/
</lcs:line></private></privateData></extensions></RequestSystemStatus>
```

## Patches and upgrades

Patching is not supported in MCM 2.0. Fixes are provided in up-issues and maintenance releases.

Software upgrades install the new application and use or upgrade the existing configuration file. MCM 2.0 is delivered on a CD and available for download from the Avaya web site.

All customer configured MCM application data is retained in case of the MCM application upgrade.

---

## Remote Call Control

One of the first questions raised when Office Communicator 2005 is not working correctly is "Is Phone Integration enabled and active?"

If Phone Integration is enabled in Office Communicator and a SIP dialog for TR/87 was established successfully, the Call Forward menu item is visible in the Office Communicator user interface (see [Figure 125: Phone Integration enabled](#) on page 217).

If Phone Integration is enabled in Office Communicator and a SIP dialog for TR/87 was attempted and not established successfully, a small icon is visible in the lower right corner of the Office Communicator user interface (see [Figure 126: SIP dialog not established](#) on page 218).



Figure 125: Phone Integration enabled



Figure 126: SIP dialog not established

## Signaling Server OAM Level CLI Commands

The Signaling Server OAM Level CLI commands are used to query active TR/87 sessions to turn on tracing at the SIP level. You can use these commands to terminate either a session for a specific DN or to terminate all TR/87 sessions that are currently active on the server.

**Table 10: Signaling Server OAM Level CLI commands**

Command	Description
SIPCTISessionShow	Show the total number of TR87 SIP sessions.
SIPCTITraceShow	Display the trace settings for SIP CTI application, including the trace filter setting and output setting.
SIPCTIShow	Show SIP CTI application status and configuration.
SIPCTIClientShow	Show information about the all the soft clients associated.
SIPCTITraceLevel <level>	Configure the TR87 SIP message Trace Level. The level can be one of the following: 0 –TR87 SIP message body (ECMA 323) only 1 – TR87 SIP message body (ECMA 323) and message headers
SIPCTITrace on	Turn on SIP CTI trace for all soft clients in both incoming and outgoing directions.
SIPCTITrace off	Turn off SIP CTI trace for all soft clients in both incoming and outgoing directions.
SIPCTITrace <MsgRcv> <MsgSend>	Turn on SIP CTI trace for all soft clients in incoming and/or outgoing. The parameter is either on or off.
SIPCTITrace sc <soft client SIP/Tel URI/DN> <MsgRcv><MsgSend>	Turn on SIP CTI trace for a specific soft client in incoming and/or outgoing direction(s). This may result in a number of sessions as a single URI could be used for multiple active sessions.
SIPCTIOutput <Dest> <"fileName">	Redirecting the SIP CTI trace to a specific output destination. The destination can be one of the following: 1. TTY 2. RPTLOG 3. File If File is selected as the output destination, the filename must be given.
SIPCTIStop all	De-acquire all AST DNs and terminate all the TR87 SIP sessions.
SIPCTIStop <dn>	De-acquire one specific AST DN and terminate all the TR87 SIP sessions associated with this AST DN.

---

## Operational Measurements

The following Operational Measurements (OM) details are collected for SIP CTI:

- SIPCTITotalSoftClientLoginAttempts
- SIPCTITotalSoftClientLoginSuccesses
- SIPCTITotalAnswerCallRequests
- SIPCTITotalAnswerCallSuccesses
- SIPCTITotalClearConnectionRequests
- SIPCTITotalClearConnectionSuccesses
- SIPCTITotalConsultationCallRequests
- SIPCTITotalConsultationCallSuccesses
- SIPCTITotalDeflectCallRequests
- SIPCTITotalDeflectCallSuccesses
- SIPCTITotalHoldCallRequests
- SIPCTITotalHoldCallSuccesses
- SIPCTITotalMakeCallRequests
- SIPCTITotalMakeCallSuccesses
- SIPCTITotalRetrieveCallRequests
- SIPCTITotalRetrieveCallSuccesses
- SIPCTITotalSingleStepTransferRequests
- SIPCTITotalSingleStepTransferSuccesses
- SIPCTITotalTransferCallRequests
- SIPCTITotalTransferCallSuccesses
- SIPCTITotalMonitorStartRequests
- SIPCTITotalMonitorStartSuccesses
- SIPCTITotalMonitorStopRequests
- SIPCTITotalMonitorStopSuccesses
- SIPCTITotalConferenceCallRequests
- SIPCTITotalConferenceCallSuccesses
- SIPCTITotalSetForwardingRequests
- SIPCTITotalSetForwardingSuccesses

- SIPCTITotalGetForwardingRequests
- SIPCTITotalGetForwardingSuccesses
- SIPCTITotalSessionTerminated

For information on how to access these OM's through Element Manager, refer to Avaya Element Manager: System Administration (NN43001-632).

## Signaling Server Expert Level CLI Commands

Using Signaling Server Expert Level CLI commands (see [Table 11: Signaling Server Expert Level CLI commands](#) on page 221), you can trace AML commands that are sent by the TR/87 FE to the Call Server on behalf of the Office Communicator clients that may be active.

**Table 11: Signaling Server Expert Level CLI commands**

Command	Description
SIPCTIAmlTrace level	<p>Configure AML Trace level for SIP CTI application. The level can be one of the following:</p> <ul style="list-style-type: none"> <li>0—Turn off trace.</li> <li>1—Print all input and output AML data buffer.</li> <li>2—Print all input and output AML data buffer except POLLING message.</li> <li>3—Print all input and output AML data buffer except POLLING message, with IE type decoding.</li> <li>4—Print all input and output AML data buffer except POLLING message with IE type and data decoding.</li> </ul> <p> <b>Note:</b></p> <p>This trace prints out AML messages to and from CS at the transport layer. Because sending and receiving AML messages are per AML link instead of per DN or TN, no good solution exists to filter on this AML trace tool. Avaya recommends that you do not turn on the trace in a busy system.</p>



# Appendix A: Call Flow and Protocol Details

---

## Contents

This section contains information about the following topics:

[Overview](#) on page 223

[Message sequence](#) on page 224

[Call flow](#) on page 225

---

## Overview

The Converged Office feature provides interworking between Avaya and Microsoft® products to address the market in which customers require that their user community use Microsoft® client software for their multimedia needs, but want to use the Business Grade Telephony of Avaya IP PBX.

The software component introduced to implement this functionality is the TR/87 Front End application that resides on the Signaling Server.

The same TR/87 FE that supports the Microsoft® Office Communicator 2005 client also serves as a core component of the SIP Contact Center architecture.

From the perspective of the TR/87 FE, all client types are transparent, whether Microsoft® Office Communicator 2005, a TR/87 session initiated by the Contact Center Manager Server (CCMS), or some other SIP UA.

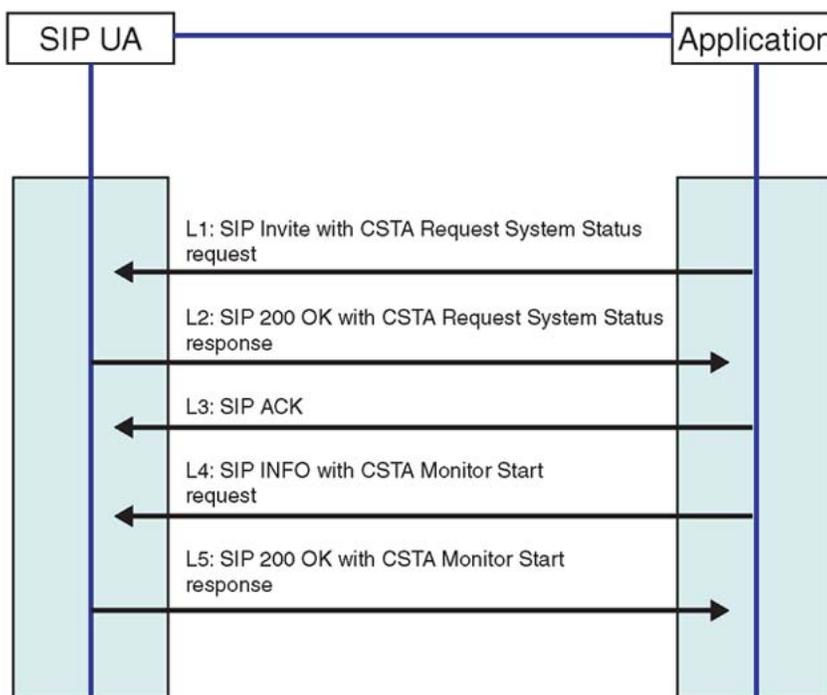
Within the scope of Avaya Communication Server 1000 TR/87 supported services and events noted in this document, all operations performed on the telephone are directly reflected in the client and vice versa. Similarly, all phone restrictions applicable to a physical TN also apply to the soft client that is issuing commands on behalf of a controlled DN.

## Message sequence

TR/87(4) is an ECMA Technical Report that describes the use of SIP as a transport of service requests and events defined by the ECMA-269(5) specification as XML bodies within SIP messages. The ECMA-323(6) specification defines the XML format of ECMA-269 services and events.

The Front End (FE) application conforms to the minimum subset of the TR/87 specification defined for Microsoft® Live Communications Server 2005 interworking and those components necessary to support the next generation SIP Contact Center requirements.

[Figure 127: Message sequence diagram - CSTA Session Establishment and Monitor Start](#) on page 224 shows the expected message flow for establishing and monitoring a CSTA session as defined by TR/87.



**Figure 127: Message sequence diagram - CSTA Session Establishment and Monitor Start**

[Figure 128: SIP INFO message with ECMA-323 content](#) on page 225 is an example of a SIP INFO message with ECMA-323 content.

```

INFO fe1_cs1000@lcs2005s.corp.nortel.com
Via: SIP/2.0/TCP 157.56.66.156:16714
Max-Forwards: 70
From:<sip:alice@microsoft.com>;tag=0d9280080ada4a1ea504f7d78d434336;epid=5fc880096d
To:<sip:fe1_cs1000@lcs2005s.corp.nortel.com>;tag=3f181801fc9d4fab27ef7d89bd28f9f
Call-ID: fdbcb6a6184a4e92a5f001865f84a2c6@157.56.66.156
CSeq: 2 INFO
Contact: <sip:alice@microsoft.com:16714
Contact:<sip:alice@microsoft.com:9609;maddr=47.130.16.136;transport=tcp>;proxy=replace
User-Agent: RTC/1.2
Content-Type: application/csta+xml
Content-Disposition: signal; handling=required
Content-Length: 189
<?xml version="1.0" encoding="UTF-8">
<MakeCall
xmlns="http://www.ecma-international.org/standards/ecma-323/csta/ed3.">
<callingDevice>tel:+14257777777</callingDevice>
<calledDirectoryNumber>tel:65000;phone
context=microsoft.com</calledDirectoryNumber>
</MakeCall>

```

Figure 128: SIP INFO message with ECMA-323 content

## Call flow

This section illustrates the call flow sequence for both Remote Call Control and Telephony Gateway and Services.

## Remote Call Control Call Flow

[Figure 129: Remote Call Control Session Establishment through SRS](#) on page 225 illustrates the Remote Call Control Session Establishment through SRS.

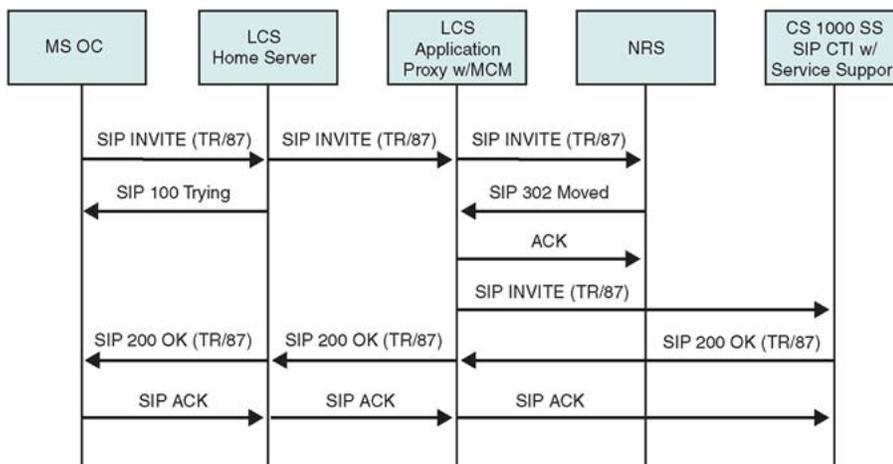


Figure 129: Remote Call Control Session Establishment through SRS

## Telephony Gateway and Services Call Flow

### Microsoft® Office Communicator Incoming Call Flow

Incoming calls to Office Communicator can originate directly from a phone behind Avaya CS 1000 where the Request URI represents the destination.

Incoming calls can also come from a PCA, where the Request URI is a service DN used to route the call to the Live Communications Server, and the actual destination is determined by a special header (x-nt-ocn) that contains the destination DN. MCM checks for the x-nt-ocn and routes the call accordingly.

Personal Call Assistant (PCA) configuration provides additional Office Communicator features such as forwarding to voice mail, and so on. Configuration of PCA is performed through station administration tools.

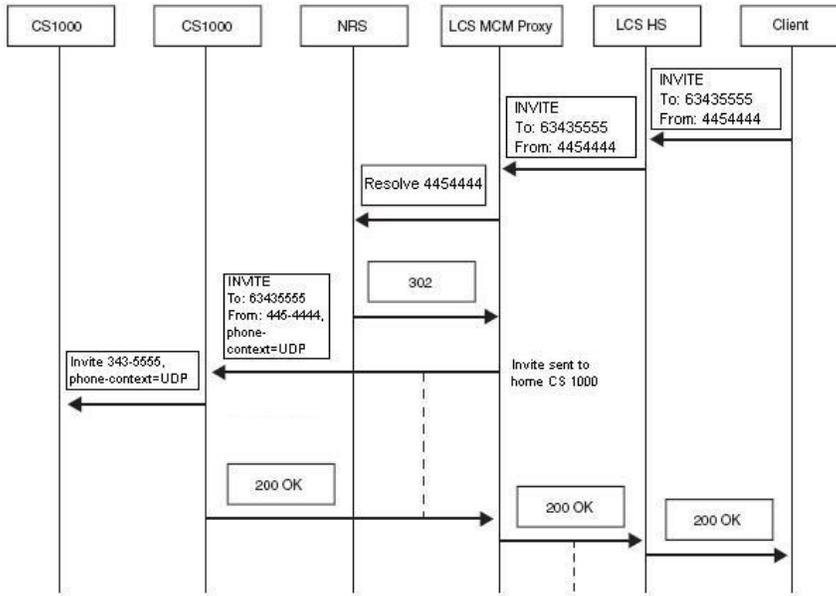


Figure 130: Microsoft® Office Communicator Outgoing Call Flow



Figure 131: Microsoft Office Communicator Outgoing Call Flow with SPS

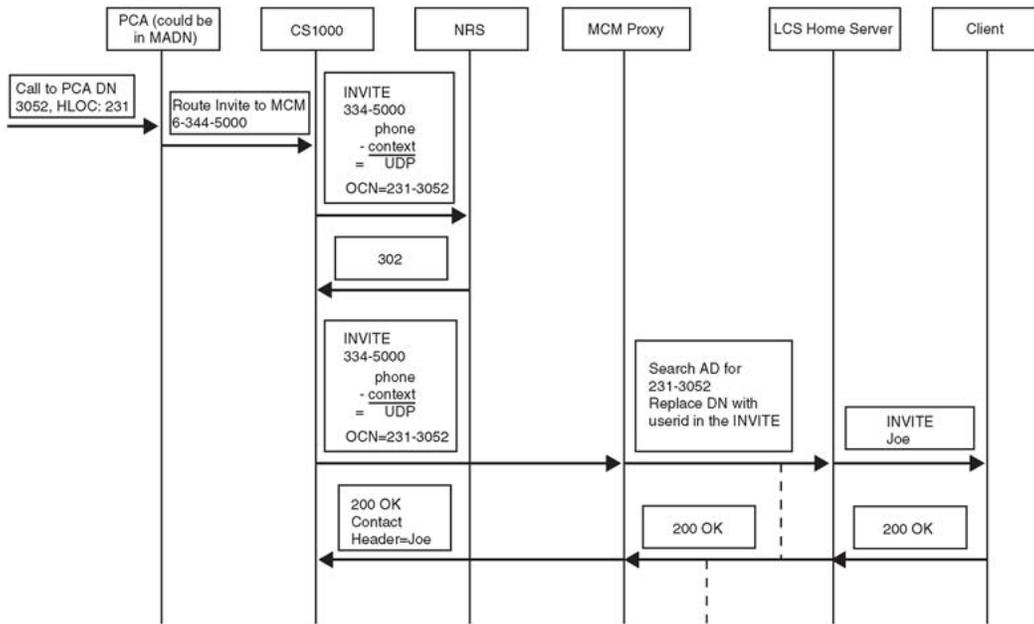


Figure 132: Microsoft® Office Communicator Incoming Call Flow using PCA

## Supported features

Table 12: SIP CTI supported features

Feature	Supported by CS 1000 TR/87 FE	Supported by Microsoft® Office Communicator 2005
<i>Call Control Events</i>		
17.2.3 - Conferenced	X	X
17.2.4 - Connection Cleared	X	X
17.2.5 - Delivered	X	X
17.2.7 - Diverted	X	X
17.2.8 - Established	X	X
17.2.9 - Failed	X	X
17.2.10 - Held	X	X
17.2.14 - Originated	X	X
17.2.16 - Retrieved	X	X

<b>Feature</b>	<b>Supported by CS 1000 TR/87 FE</b>	<b>Supported by Microsoft® Office Communicator 2005</b>
17.2.18 - Transferred	X	X
<i>Call Associated Services</i>		
18.1.4 - Generate Digits	X	X
<i>Call Associated Events</i>		
18.2.5 - Service Completion Failure	X	X
<i>Logical Device Features</i>		
22.1.9 - Get Do Not Disturb	X (Release 5.0)	X
22.1.10 - Get Forwarding	X	X
22.1.17 - Set Do Not Disturb		X
22.1.18 - Set Forwarding	X	X
<i>Logical Device Feature Event</i>		
22.2.12 - Do Not Disturb	X (Release 5.0)	X
22.2.13 - Forwarding	X	X
<i>Capability Exchange Services</i>		
13.1.1 - Get CSTA Features	X	X
<i>System Services</i>		
14.2.1 - Request System Status	X	X
<i>Monitoring Services</i>		
15.1.2 - Monitor Start	X	X
15.1.3 - Monitor Stop	X	X
<i>Call Control Services</i>		
17.1.2 - Alternate Call		X
17.1.3 - Answer Call	X	X
17.1.8 - Clear Connection	X	X
17.1.9 - Conference Call	X	X
17.1.10 - Consultation Call	X	X
17.1.11 - Deflect Call	X	X
17.1.15 - Hold Call	X	X
17.1.18 - Make Call	X	X
17.1.21 - Reconnect Call		X

## Call Flow and Protocol Details

<b>Feature</b>	<b>Supported by CS 1000 TR/87 FE</b>	<b>Supported by Microsoft® Office Communicator 2005</b>
17.1.22 - Retrieve Call	X	X
17.1.25 - Single Step Transfer Call	X	X
17.1.26 - Transfer Call	X	X

# Appendix B: Configuration Examples

---

## Contents

- [Introduction](#) on page 231
- [Standard Edition](#) on page 231
- [Enterprise Edition](#) on page 251
- [Host Authorization](#) on page 261
- [Routing](#) on page 263
- [Configuring DNS](#) on page 267
- [Active Directory configuration](#) on page 269
- [Installing and configuring MCM](#) on page 269
- [Configuring the Signaling Server](#) on page 272
- [Configuring NRS](#) on page 273

---

## Introduction

As described in the Planning and Engineering chapter, small, medium, and large networks require different editions of Live Communications Server (LCS) 2005. This appendix contains configuration examples for both Standard Edition and Enterprise Editions of LCS 2005.

---

## Standard Edition

This section provides information on how to configure and troubleshoot the Converged Office solution running the Standard Edition LCS 2005. This sample configuration is for a small network deployment, with only one LCS server acting as the home server with a co-resident MCM.

## Setting up the lab

Follow these steps to ensure the lab is set up correctly:

### Setting up the lab

1. Confirm that the Communication Server 1000 server is version (6.0) or later with all patches as required in the Product Bulletin.
2. Confirm that the Signaling Server is version (6.0) or later with all patches as required in the Product Bulletin
3. Confirm that the LCS Standard Edition server is SP1 with patches as detailed in the Product Bulletin.
4. Confirm that MCM is version is the latest GA version. Find the latest GA version of MCM on the Avaya Website at Undefined Resource.

[Figure 133: Overview of lab set-up](#) on page 232 illustrates how to set up a lab for Converged Office.



Figure 133: Overview of lab set-up

## Collecting required data

Collect the required data listed in the following three tables before you begin to configure the Converged Office solution. The information entered here can be used to verify configuration settings later on.

**Table 13: Microsoft Active Directory**

Required information	Record your information	For example
User SIP URI		brendan.mccarthy@interop.com
Remote Call Control URI		sip:1156_ss1@interop.com
Telephone URI		tel:6712;phone-context=dialstring

**Table 14: NRS**

Required information	Record your information	For example
IP-address Primary SPS		47.11.159.187
IP-address Secondary SPS		Not used
Node IP-address		47.164.115.234
LCS endpoint name		alliance-clab03
Avaya CS 1000 SIP gateway endpoint name		1156_ss1
Routing Entry for PCA		8214
Service domain		interop.com
Level 1 domain		udp.interop.com
Level 0 domain		cdp.interop

**Table 15: Element Manager**

Required information	Record your information	For example
Avaya CS 1000 SIP gateway endpoint name		1156_ss1
SIP Domain name		interop.com
SIP Gateway Endpoint name		1156_ss1
SIP URI map, Private/UDP domain name		udp.interop.com

Required information	Record your information	For example
SIP URI map, Private/CDP domain name		cdp.interop.udp.interop.com
SIP CTI Service, Service enabled		Yes
SIP CTI Service, Customer Number		0
SIP CTI Service, International Calls As National		Yes
SIP CTI Service, National Prefix		0
SIP CTI Service, International Prefix		00
SIP CTI Service, Dialing Plan		cdo
SIP CTI Service, Calling Device URI Format		Phone-context=dialstring
SIP CTI Service, Country Code		33
SIP CTI Service, National/ Number of digits to strip		1
SIP CTI Service, National Prefix		1

---

## Configuring the Call Server

Use the following procedure to check the configuration of the Call Server.

### Checking the Call Server configuration

1. Check the version of the CS 1000 Call Server. The CS 1000 Call Server version must be at least release 5.0.
2. Check the Product Bulletin and download the required patches for Converged Office.
3. In LD 22, confirm that AST, PCA, and SIP CTI TR87 licenses are available. For example:

```
>ld 22
REQ slt
PCA 32767 LEFT 32762 USED 5
AST 32767 LEFT 32756 USED 11
SIP CTI TR87 32767 LEFT 32753 USED 14
SIP ACCESS PORTS 32767 LEFT 32757 USED 10
```

4. Also in LD 22, confirm that the MS\_CONV package is present (this package is required). For example:

```
>ld 22
REQ prt
TYPE pkg
MS_CONV 408
```

5. Ensure that the VSID and the ELAN ID are greater than or equal to 32 and that the SECU parameter is configured to YES for ELAN and for VAS configuration. For example:

```
>ld 22
PT2000
REQ prt
TYPE vas
VSID 032
DLOP
ELAN 032
SECU YES
INTL 0001
MCNT 9999
```

6. Immediate (IMM) is recommended for both fields. If the trunk is intended for SIPDECT or Converged Office applications, use WNK/WNK instead. .In LD 20, confirm that STRI/STRO is WNK for SIP Trunk configuration. For example:



**Note:**

The screen output shown here may differ, depending on the setup used.

```
>ld 20
PT0000
REQ: prt
TYPE: tnb
TN 156 0 0 0
DATE
PAGE
DES
```

```
DES SIP
TN 156 0 00 00 VIRTUAL
TYPE IPTI
CDEN 8D
CUST 0
XTRK VTRK
ZONE 000
TRK ANLG
NCOS 0
RTMB 62 1
CHID 1
TGAR 0
STRI/STRO WNK WNK
SUPN YES
AST NO
IAPG 0
CLS UNR DTN WTA LPR APN THFD XREP
P10 NTC
TKID
AACR NO
DATE 5 DEC 2006
```

7. In LD 21, check that NCNA and NCRD are configured to YES and that SIGO is ESN5 in the SIP Route Configuration. For example:

```
>ld 21
REQ: prt
TYPE: rdb
CUST 0
ROUT 62
TYPE RDB
CUST 00
ROUT 62
DES SIP
TKTP TIE
NPID_TBL_NUM 0
ESN NO
RPA NO
CNVT NO
SAT NO
RCLS EXT
VTRK YES
ZONE 000
PCID SIP
CRID YES
NODE 81
DTRK NO
ISDN YES
MODE ISLD
DCH 63
IFC SL1
PNI 00001
NCNA YES
NCRD YES
TRO YES
FALT NO
```

```
CTYP UKWN
INAC YES
ISAR NO
DAPC NO
PTYP ATT
...
DEXT NO
ANTK
SIGO ESN5
MFC NO
...
```

8. For TN configuration in LD 11, configure AST, TR87A and CDMR Class of Service. Configure MARP for the telephone. For example:



**Note:**

The screen output shown here may differ depending on the setup used.

```
>ld 11
SL1000
MEM AVAIL: (U/P): 3665391 USED U P: 981685 104283 TOT:
4751359
DISK SPACE NEEDED: 116 KBYTES
2MB BACKUP DISKETTE(S) NEEDED: 1 (PROJECTED LD43 -
BKO)
TNS AVAIL: 32539 USED: 228 TOT: 32767
REQ: prt
TYPE: dnb
```

CUST 0  
 DN 6712  
 DATE  
 PAGE  
 DES

DN 6712  
 CPND  
 CPND\_LANG ROMAN  
 NAME CD LCS1 Fabulite  
 XPLN 16  
 DISPLAY\_FMT FIRST, LAST  
 TYPE SL1  
 TN 152 0 00 14 V KEY 00 MARP DES CDLCS 14 AUG 2006  
 (I2004 )  
 TN 152 0 00 30 V KEY 00 DES PCA 12 JUL 2006

REQ: prt  
 TYPE: tnb  
 TN 152 0 0 14  
 DATE  
 PAGE  
 DES

DES CDLCS  
 TN 152 0 00 14 VIRTUAL  
 TYPE I2004  
 CDEN 8D  
 CTYP XDLC  
 CUST 0  
 ZONE 000  
 FDN  
 TGAR 0  
 LDN NO  
 NCOS 0  
 SGRP 0  
 RNPG 0  
 SCI 0  
 SSU  
 LNRS 16  
 XLST 0  
 SCPW 6712  
 SFLT NO  
 CAC\_MFC 0  
 CLS CTD FBD WTA LPR MTD FND HTD TDD HFD CRPD  
 MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE  
 DRG1  
 POD SLKD CCSA-CSI SWD LNA CNDA  
 CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCB  
 ICDD CDMD LLCN MCTD CLBD AUTU  
 GPUD DPUD DNDA CFXD ARHD FITD CLTD ASCD  
 CPFA CPTA HSPD ABDD CFHD FICD NAID BUZZ  
 UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD  
 NRCD  
 NROD  
 DRDD EXR0  
 USRD ULAD CCBD RTDD RBDD RBHD PGND OCB  
 FLXD  
 FTTC  
 DNDY DNO3 MCBN  
 FDSD NOVD VOLA VOUD CDMR ICRD MCDD T87A KEM2  
 CPND\_LANG ENG  
 BFTN 152 0 01 00  
 HUNT  
 PLEV 02  
 CSDN

```
AST 00  
IAPG 0
```

9. Configure PCA for SIP Gateway (PC-only configuration).
  - a. Confirm that AST is not configured.
  - b. Configure TR87D and CDMR Class Of Service
  - c. Confirm that this PCA is not configured as MARP.
  - d. Configure Hot P for SIP Gateway calls. For example:

 **Note:**

The screen output shown here may differ depending on the setup used.

```
REQ: prt  
TYPE: pca  
TN 152 0 00 30  
DATE  
PAGE  
DES  
DES PCA  
TN 152 0 00 30 VIRTUAL  
TYPE PCA  
CDEN 8D  
CTYP XDLC  
CUST 0  
ZONE 000  
FDN  
TGAR 1  
LDN NO  
NCOS 0  
SGRP 0  
RNPG 0  
SCI 0  
SSU  
XLST 0  
SCPW 6712  
SFLT NO  
CAC_MFC 0  
CLS CTD FBD WTA LPR MTD FND HTD TDD HFA CRPD  
MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE  
DRG1  
POD SLKD CCSA-CSI SWD LND CNDD  
CFTD SFD MRD ADV CNID CDCA MSID DAPA BFED RCB  
ICDD CDMD LLCN MCTD CLBD AUTU  
GPUD DPUD DNDD CFXD ARHD FITD CLTD ASCD  
CPFA CPTA HSPD ABDD CFHD FICD NAID BUZZ  
UDI RCC HBT  
AHBTD AHA IPND DDGA NAMA MIND PRSD NRWD  
NRCD NROD  
DRDD EXR0  
USRD ULAD CCBD RTDD RBDD RBHD PGND OCB  
D FLXD  
FTTC  
DNDY DNO3 MCBN  
FDSD NOVD VOLA VOUD CDMR ICRD MCDD T87D  
CPND_LANG ENG  
HUNT  
PLEV 02  
CSDN  
AST  
IAPG 0  
AACS NO  
ITNA NO  
DGRP  
MLWU_LANG 0  
DNDR 0
```

```

KEY 00 SCR 6712 0
CPND
CPND_LANG ROMAN
NAME CD LCS1 Fabulite
XPLN 16
DISPLAY_FMT FIRST, LAST
01 HOT P 4 8214
02

```

10. Configure DSC for PCA. Create a DSC to route the call to the SIP route using the RL1. For example:

**Note:**

The screen output shown here may differ depending on the setup used.

```

MEM AVAIL: (U/P): 3665391 USED U P: 981685 104283 TOT:
4751359
DISK SPACE NEEDED: 116 KBYTES
2MB BACKUP DISKETTE(S) NEEDED: 1 (PROJECTED LD43 -
BKO)
REQ prt
CUST 0
FEAT cdp
TYPE dsc
DSC 8214
DSC 8214
FLEN 4
DSP LSC
RRPA NO
RLI 1
CCBA NO
NPA
NXX

```

11. Check that PCA is activated. In LD 21, configure the PCA to ON to allow the incoming to twin to the PCA and make the SIP Gateway call work.

For example:

```

ld 21
REQ: prt
TYPE: ftr
TYPE FTR_DATA
CUST 0
...
PCA ON
...

```

---

## Configuring the Signaling Server

Use the following procedure to confirm the correct configuration of the Signaling Server.

### Checking the configuration of the Signaling Server

1. Confirm that the Signaling Server is version 6.0 or later. Refer to the Product Bulletin for any required patches for Converged Office.
2. Confirm that your installation meets the memory requirements.

The maximum number of SIP CTI/TR87 users on a single Signaling Server is 5000. The Standard Signaling Server memory is 1GB (minimum requirement) and is required in the following scenarios:

- a. if SIP CTI/TR87 is co-resident with PD/RL/CL application
  - b. if SIP CTI/TR87 is co-resident with H.323/SIP GW serving more than 200 ports, or co-resident with Terminal Proxy Server serving more than 1000 IP users
3. Confirm the configuration of the Home server or Application Proxy server. Right click on My Computer and choose the **Computer Name** tab.

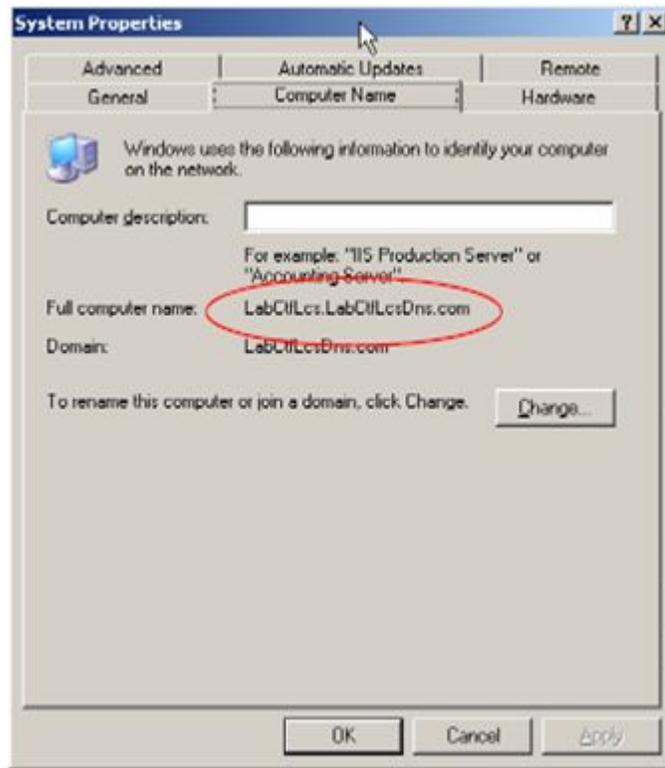


Figure 134: FQDN of the LCS Home Server

4. Define the IP address of the server acting as DNS. For example, in [Figure 135: DNS configuration on the Signaling Server](#) on page 241, the IP address is 47.11.159.187.

Host Name	IP Address
alliance-clab03.interop.c	47.11.157.112
alliance-clab.interop.co	47.11.159.187

DNS Servers

Primary DNS Server IP address: 47.11.159.187

Alternate DNS Server1 IP address: 0.0.0.0

Alternate DNS Server2 IP address: 0.0.0.0

**Figure 135: DNS configuration on the Signaling Server**



**Note:**

Users upgrading from Release 4.5 to Release 5.0 and later still see Host Table configuration in Element Manager, but that information is no longer used.

5. Ensure that the SIP GW settings match the settings as shown in [Figure 136: SIP GW Settings](#) on page 241.

General | SIP Gateway Settings | SIP Gateway Services

**Proxy Or Redirect Server:**

Primary TLAN IP Address: 47.11.150.17      Secondary TLAN IP Address: 0.0.0.0

Port: 5060 (1 - 65535)      Port: 5060 (1 - 65535)

Transport protocol: TCP      Transport protocol: TCP

Options:  Support registration      Options:  Support registration

Primary CDS Proxy       Secondary CDS Proxy

**CLID Presentation:**

Country code (CCC): 8

Area code:      NPA in North America

Number Translation: Strip:      Prefix:      CLID Display Format:

Subscriber (SN): 0      <CCC><Area code><SN>

National (NN): 0      <CCC><NN>

International: 0      0      <International number>

\* Required Value.      Note: Changes made on this page will NOT be transmitted until the Node is also saved.      Save      Cancel

**Figure 136: SIP GW Settings**

6. Confirm that the SIP URI Map settings match the settings as shown in [Figure 137: SIP URI Map](#) on page 242.

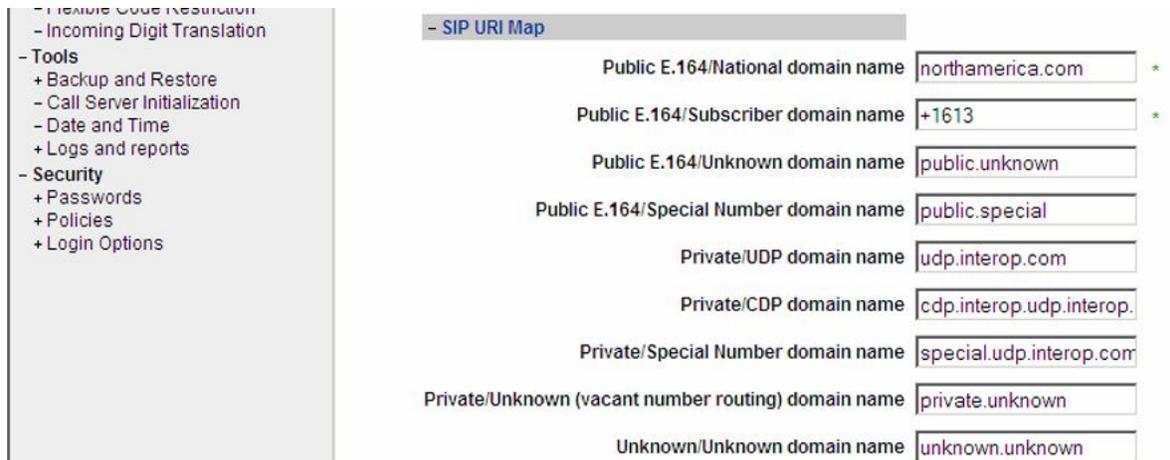


Figure 137: SIP URI Map

7. Confirm that the SIP CTI Services settings match the settings, as shown in [Figure 138: SIP CTI Services](#) on page 242.

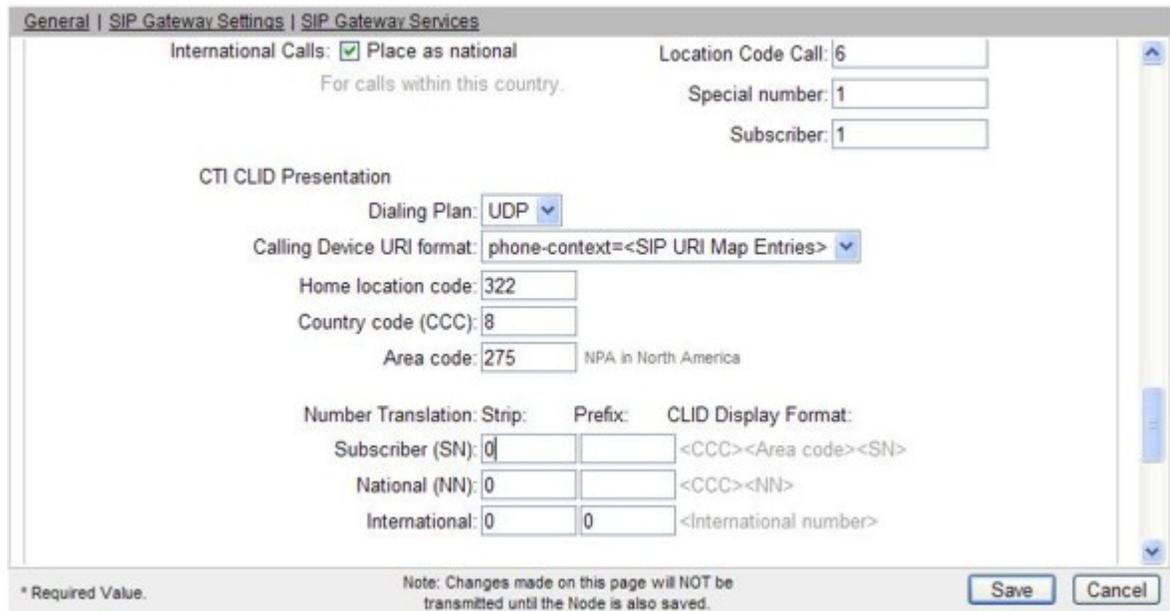


Figure 138: SIP CTI Services

## Configuring NRS

Use the following procedure to check the configuration of NRS.

### Checking NRS configuration

1. Check the Signaling Server and MCS Endpoints Status as shown in [Figure 139: Signaling Server and MCM Endpoints status on NRS](#) on page 243.

Figure 139: Signaling Server and MCM Endpoints status on NRS



**Note:**

Ensure that all the endpoints are registered (the endpoints must be listed as "Dynamic Sip" under the Supported Protocols column and have an IP address under the Call Signalling IP column in [Figure 139: Signaling Server and MCM Endpoints status on NRS](#) on page 243.

2. Check the PCA Routing Entry as shown in [Figure 140: Routing Entry for PCA](#) on page 243 (refer to the information you recorded in [Table 14: NRS](#) on page 233). To configure PCA for SIP Gateway, see step 9 in [Checking the Call Server configuration](#) on page 234.

Figure 140: Routing Entry for PCA

3. Check the LCS Standard Edition Configuration.

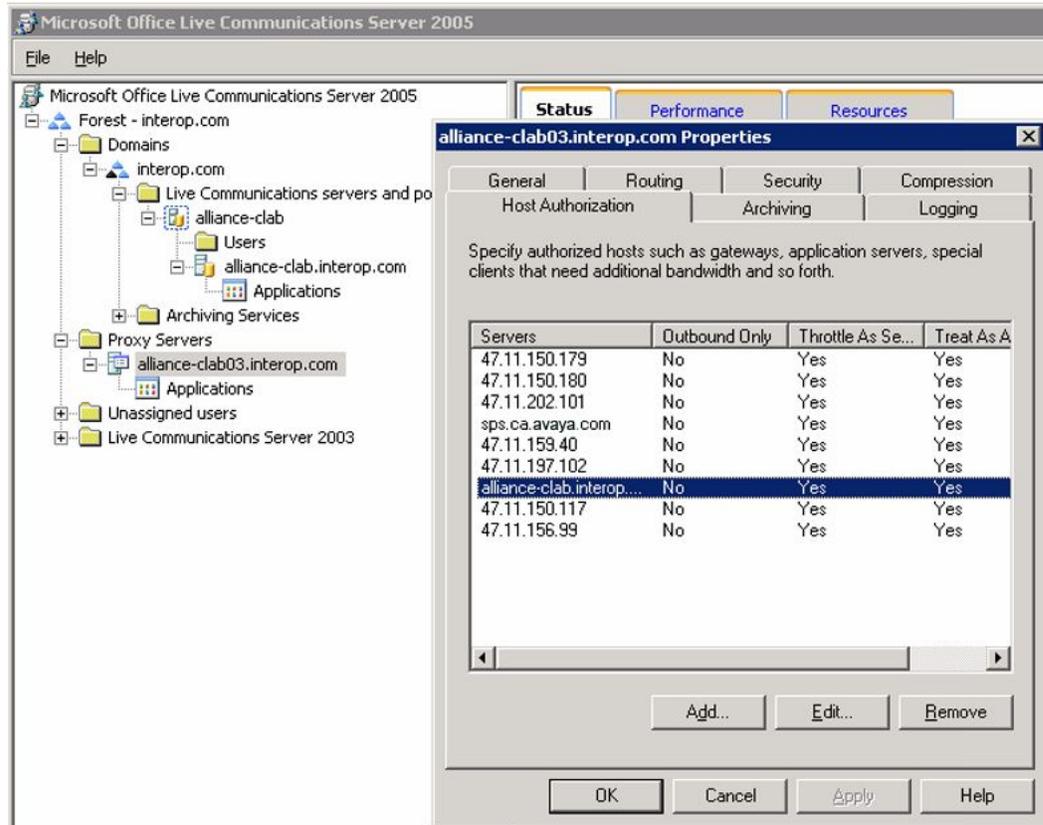
In Host Authorization for a LCS Standard Edition, configure the IP Address of the SPS IP and the Node IP (see [Figure 141: Host Authorization](#) on page 244. As

shown in [Table 14: NRS](#) on page 233, the SPS IP is 47.11.150.147, and the Node IP is 47.11.159.187.



**Note:**

Communication between MCM and the CS 1000 is based on TCP. When using TCP, enter the IP address instead of FQDN.



**Figure 141: Host Authorization**

No routing is required for LCS Standard Edition if MCM is co-resident with the Home Server.

## Configuring Active Directory

Use the following procedure to check the Active Directory user configuration.

### Checking the settings of Active Directory user configuration

Check the Active Directory user configuration, complete the following actions:

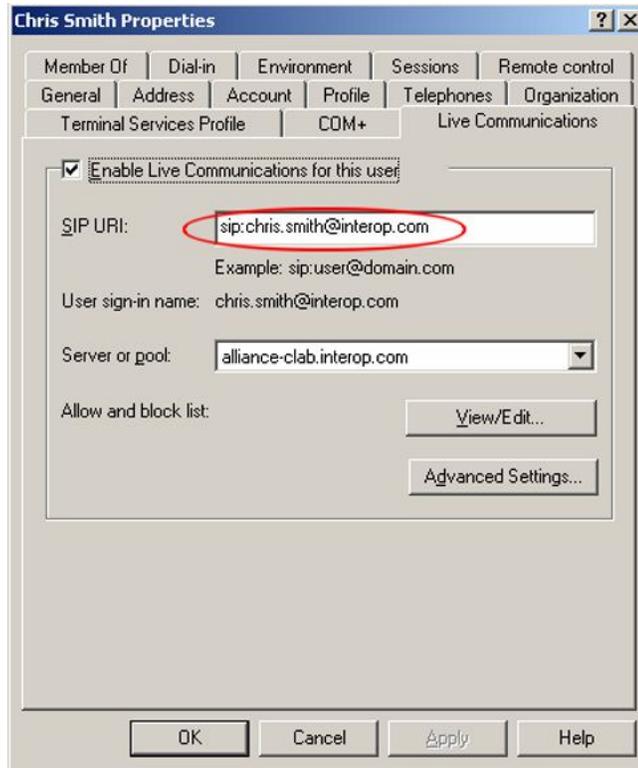
- a. Compare and match your LCS User General properties settings with those in Undefined Resource . In particular, note the telephone number in the

Telephone Number field (this must be the same as the information recorded in [Table 13: Microsoft Active Directory](#) on page 233).

The screenshot shows a Windows-style dialog box titled "Chris Smith Properties". It has several tabs at the top: "Member Of", "Dial-in", "Environment", "Sessions", "Remote control", "Terminal Services Profile", "CDM+", "Live Communications", "General", "Address", "Account", "Profile", "Telephones", and "Organization". The "General" tab is selected. Below the tabs, there is a small icon of a person and the name "Chris Smith". The form contains several text input fields: "First name:" with "Chris", "Last name:" with "Smith", "Display name:" with "Chris Smith", "Description:" (empty), "Office:" (empty), "Telephone number:" with "ESN 354-6714" (circled in red), "E-mail:" with "chris.smith@interop.com", and "Web page:" (empty). There are also "Other..." buttons next to the "Telephone number" and "Web page" fields. At the bottom, there are "OK", "Cancel", "Apply", and "Help" buttons.

**Figure 142: LCS User General properties**

- b. Compare and match your settings in LCS user Live Communications properties with those in Undefined Resource. In particular, note the SIP URI (this must be the same as the information recorded in [Table 13: Microsoft Active Directory](#) on page 233).



**Figure 143: LCS user Live Communications properties**

- c. Compare and match your LCS user Advanced settings with those in Undefined Resource. In particular, note the TEL URI and the Remote Call Control SIP URI (these must be the same as the information recorded in [Table 13: Microsoft Active Directory](#) on page 233).

Figure 144: LCS user Advanced Settings

**\* Note:**

The Remote Call Control SIP URI field is the SIP endpoint URI of the Signaling Server with TR87 FE (Front End) installed.

## Configuring and installing MCM

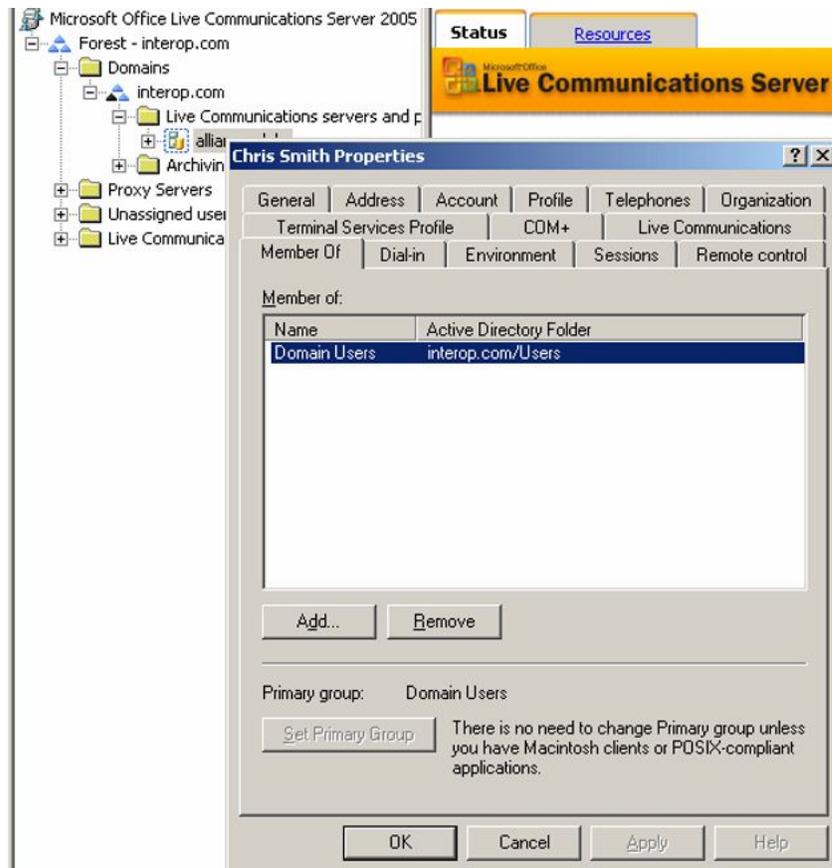
Use the following procedure to check that MCM is properly installed and configured.

### Configuring and installing MCM

1. In MCM Installation and Configuration, compare and match the configuration of MCM Groups with the configuration settings in [Figure 145: MCM User Groups](#) on page 248.

**\* Note:**

Check that MCM user Member of tab lists Administrators and RTC Server Applications.



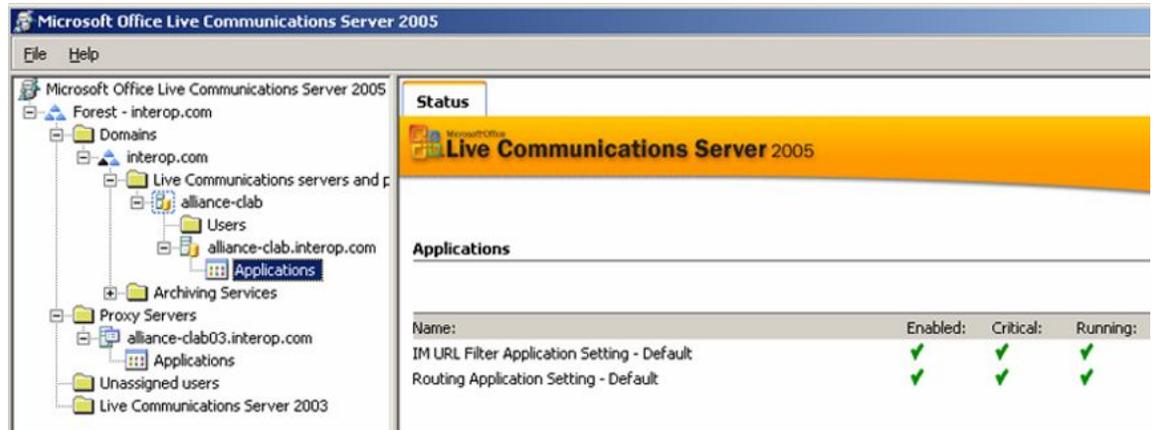
**Figure 145: MCM User Groups**

2. For MCM Application, confirm that MCM is running. Confirm that the two other Default LCS applications, IM URL Filter and Routing Application are running (see [Figure 146: MCM Application](#) on page 249).

If the MCM application is not running:

Confirm that MCM is configured with the MCM user groups Administrators and RTC Server Applications.

- i. Confirm that the MCM user password is correct.
- ii. Check the Event logs to find out why MCM is not running.



**Figure 146: MCM Application**

- See [Figure 147: MCM Gateway Endpoint Configuration](#) on page 250 and [Figure 148: MCM 2.0 Configuration screen](#) on page 251 to check for proper MCM configuration on NRS.

View Gateway Endpoint Property (lab.com / labfrance.com / cdpfabulite)

Endpoint name: mcmendpoint

Endpoint description: LCS site CTF

Tandem gateway endpoint name:  [Look up](#)

Endpoint authentication enabled: OFF

Authentication password:

E.164 country code: 1

E.164 area code:

E.164 international dialing access code: 00

E.164 national dialing access code: 0

E.164 local (subscriber) dialing access code:

Private L1 domain (JDP location) dialing access code: 6

Private special number 1:

Private special number 2:

Static endpoint address type: IP version 4

Static endpoint address:

H.323 Support: H.323 not supported

SIP support: Dynamic SIP endpoint

SIP transport: TCP

SIP port: 5060

Network Connection Server enabled:

Figure 147: MCM Gateway Endpoint Configuration

The screenshot displays the MCM 2.0 Configuration screen with the following sections and settings:

- SIP Routing:**
  - Radio buttons:  SRS,  SPS,  Direct
  - Primary IP: 47 . 11 . 150 . 117
  - Secondary IP: 0 . 0 . 0 . 0
  - Mode: Redirect All
  - CS1000 SS Node IP: 47 . 11 . 150 . 189
  - Transport: TCP, Port: 5060
- Registration:**
  - ID: mcm, registration ID mcm-endpoint
  - IP: 47.11.157.112
- Active Directory Configuration:**
  - Radio buttons:  Query Server,  Local Cache,  Local Cache then Query Server
  - Synchronize at: 03:00
  - Synchronize Now button
  - Non Default AD/LDAP Server
  - Server IP: 0 . 0 . 0 . 0, Port: 389
- Active Directory Mapping:**
  - Phone Field: telephoneNumber
  - Phone Format: ????
- Incoming Call Processing Parameters:**
  - Called Phone Context: cdp.interop.udp.interop.com
  - Called Phone Prefix Delete: 0
  - Called Phone Prefix Insert:
  - Caller Phone Prefix Delete: 0
  - Caller Phone Prefix Insert:
- Outgoing CLID Number Parameters:**
  - Prefix Delete: 0
  - Prefix Insert:
- Outgoing CLID Name Parameters:**
  - Extract Last-First Data
  - Switch Last-First Order
  - Remove Last-First Comma Separator
- SIP-CTI Authorization:**
  - Enable Authorization

Figure 148: MCM 2.0 Configuration screen

## Enterprise Edition

This section describes the configuration of the LCS Enterprise Edition.

### Overview of general lab set-up

[Figure 149: LCS Enterprise Edition General Overview](#) on page 252, illustrates the lab set-up, which includes:

- Call Server version 6.0
- Signaling Server version 6.0

- MCM version 2.0
- 1 DNS/Active Directory Server
- LCS Home Server with a Pool and a Microsoft Software Load Balancer (NLB)
- 1 LCS Application Proxy Server

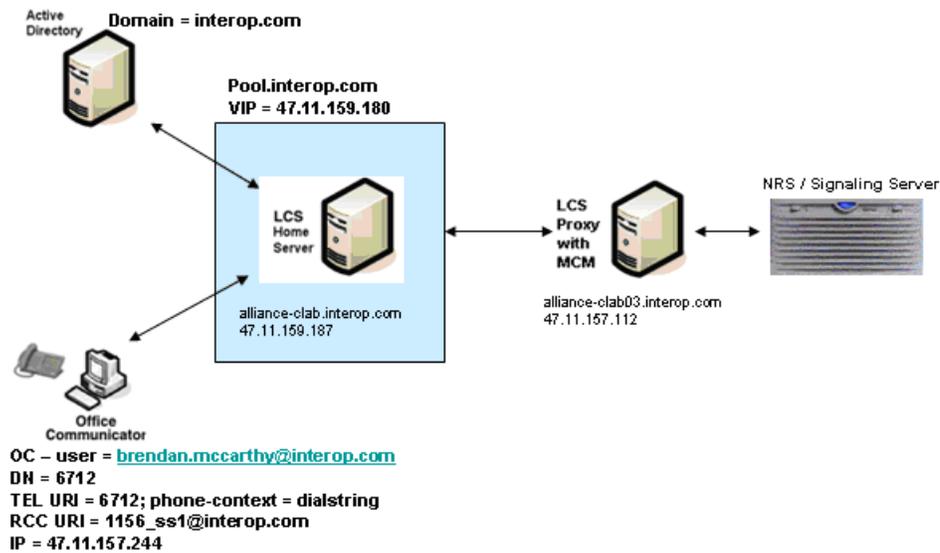


Figure 149: LCS Enterprise Edition General Overview

## Collecting Data for Enterprise Edition

Collect the required data listed in the following four tables before you begin to configure the Converged Office solution.



**Note:**

The FQDN field is case sensitive. Enter the exact FQDN.



**Note:**

The Certificate is complex and its correct configuration is not described in this section. Confirm that you have configured the Certificate correctly.

Table 16: Microsoft Active Directory

Required information	Record your information	For example
User SIP URI		brendan.mccarthy@interop.com
Remote Call Control URI		1156_ss1@interop.com

Required information	Record your information	For example
Telephone URI		tel:6712;phone-context=dialstring

**Table 17: LCS**

Required information	Record your information	For example
LCS Application Proxy Server		alliance-clab03.interop.com 47.11.157.112
LCS Enterprise Edition Pool		Pool.interop.com 47.11.159.180
LCS Enterprise Edition Home Server		alliance-clab.interop.com 47.11.159.187

**Table 18: NRS**

Required information	Record your information	For example
IP-address Primary SPS		47.11.150.117 (standalone)
IP-address Secondary SPS		Not used
Node IP-address		47.11.159.187
LCS endpoint name		alliance-clab03
CS 1000 SIP gateway endpoint name		1156_ss1
Routing Entry for PCA		8214
Service domain		interop.com
Level 1 domain		udp.interop.com
Level 0 domain		cdp.interop

**Table 19: Element Manager**

Required information	Record your information	For example
LAN configuration, FQDN (LCS Application Proxy and LCS Pool)		ctflabcsproxy.ctflab.net Pool.ctflab.net
LAN configuration, IP Address (LCS Application Proxy and LCS Pool)		47.11.159.187
CS 1000 SIP gateway endpoint name		1156_ss1
SIP Domain name		interop.com

Required information	Record your information	For example
SIP Gateway Endpoint name		1156_ss1
SIP URI map, Private/UDP domain name		udp.interop.com
SIP URI map, Private/CDP domain name		cdp.interop.udp.interop.com
SIP CTI Service, Service enabled		Yes
SIP CTI Service, Customer Number		0
SIP CTI Service, International Calls As National		Yes
SIP CTI Service, National Prefix		0
SIP CTI Service, International Prefix		00
SIP CTI Service, Dialing Plan		CDP
SIP CTI Service, Calling Device URI Format		Phone-context=dialstring
SIP CTI Service, Country Code		33
SIP CTI Service, National/Number of digits to strip		1
SIP CTI Service, National Prefix		1

---

## LCS Management Console

The LCS Management Console, shown in [Figure 150: LCS Management Console](#) on page 255, provides an overview of LCS configuration:

- The LCS Enterprise Edition Pool: Pool.interop.com
- The LCS Enterprise Edition Home Server(s): alliance-clab.interop.com



**Note:**

The Enterprise edition can have multiple Home Servers.

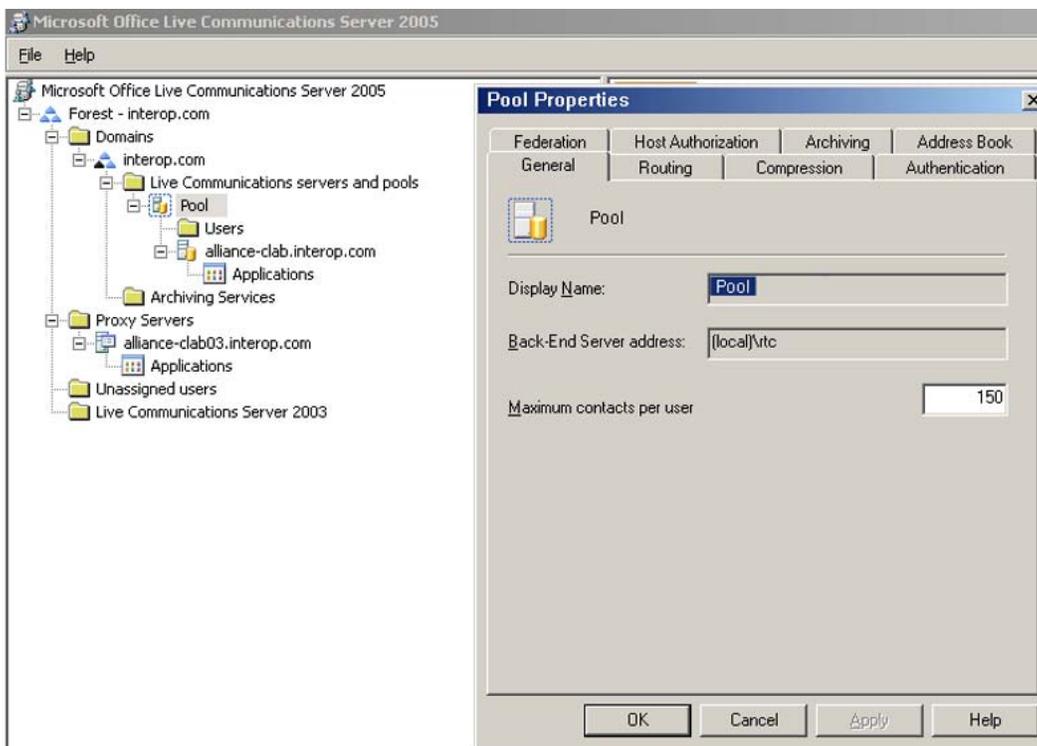
- The LCS Enterprise Edition Proxy Server: alliance-clab03.interop.com

**Note:**

The LCS GUI is always displayed in lower case. To determine the correct FQDN, right click on **pool**, and the correct FQDN displays under **Display Name** (see [Figure 151: Determining the exact FQDN of the pool](#) on page 255).



**Figure 150: LCS Management Console**



**Figure 151: Determining the exact FQDN of the pool**

## LCS Default Applications Running

Use the following procedure to determine which default applications are running.

### Identifying the active default applications

1. To determine the exact FQDN of Pool, confirm that the two default applications, IM URL Filter Application Setting and Routing Application Setting are running (see [Figure 152: Default applications](#) on page 256).

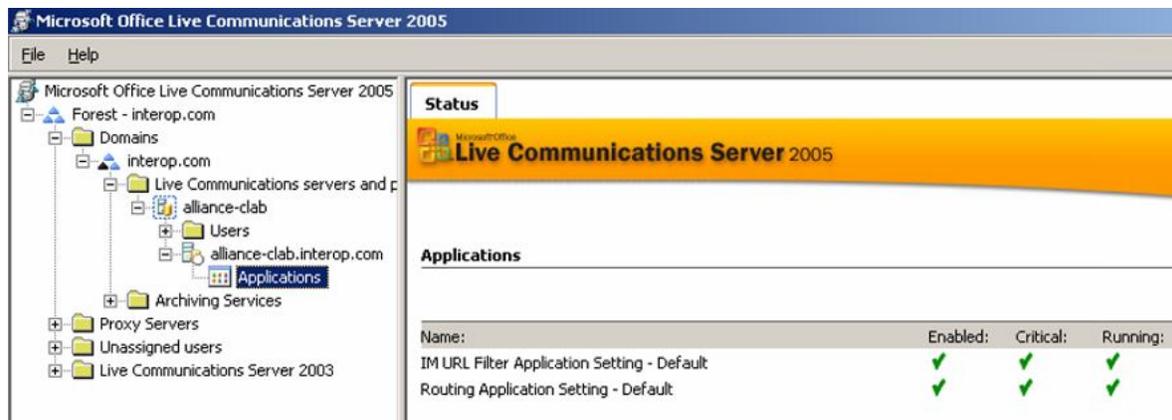


Figure 152: Default applications

2. Under the Application Proxy Server, confirm that the MCM is running correctly, as shown in [Figure 153: MCM Application](#) on page 256.

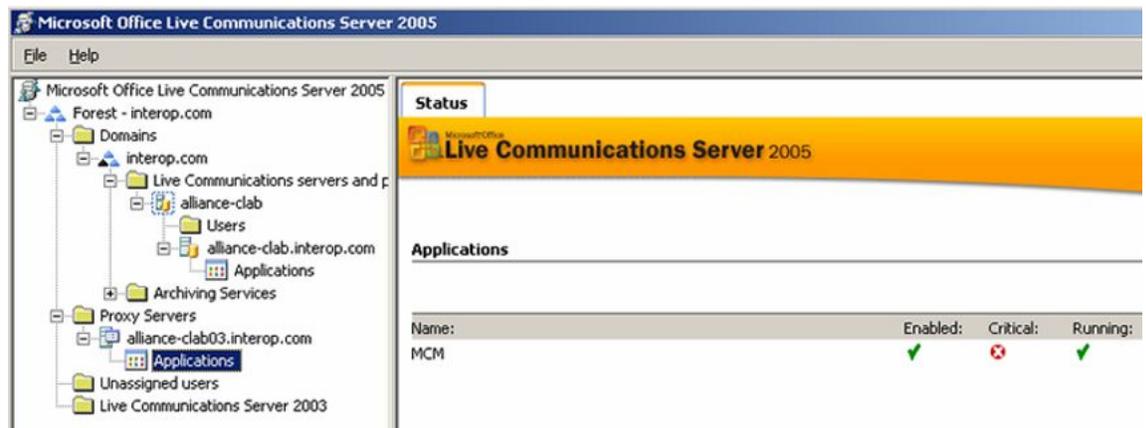


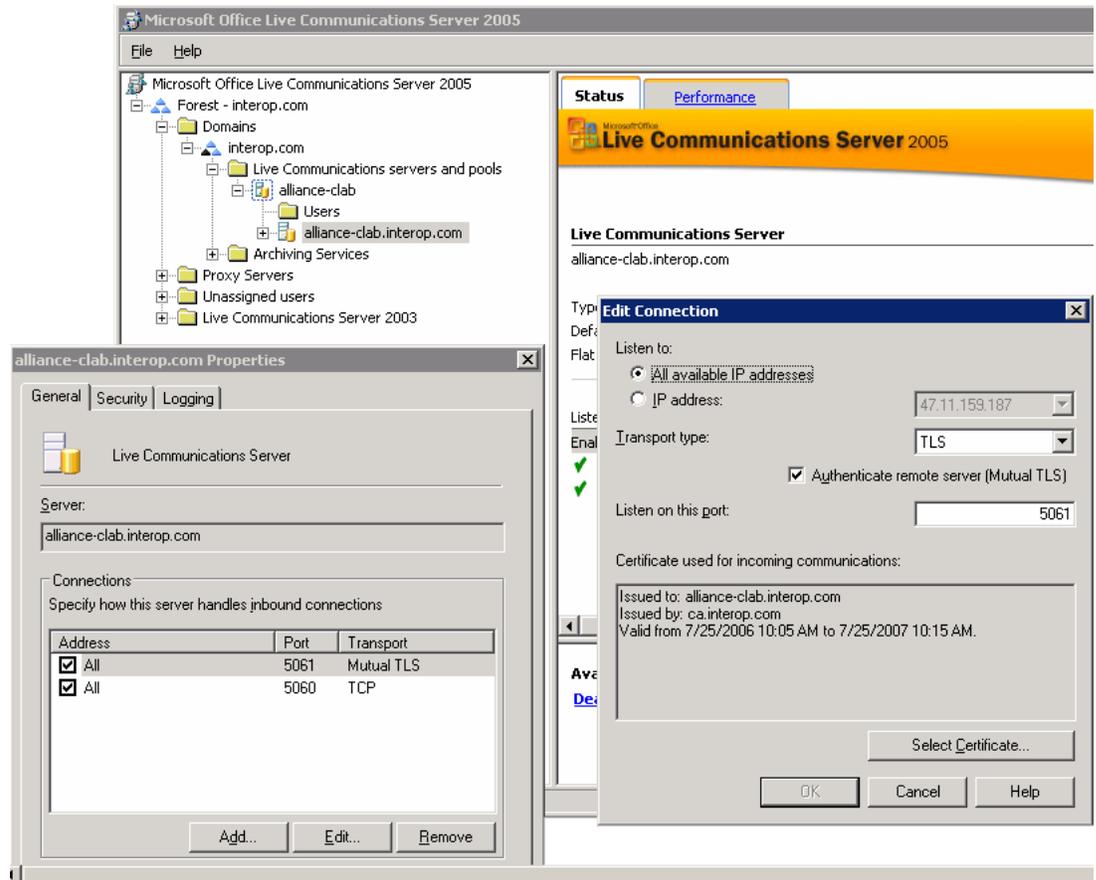
Figure 153: MCM Application

## General tab settings

Use the following procedure to confirm the correct settings in the General tab.

## Checking the settings in the General and Edit Connection for the Home Server

1. Confirm the correct settings for the General tab and Edit Connection for TLS (see [Figure 154: Home Server Edit Connection - TLS](#) on page 257).
  - a. Confirm that the **Authenticate remote server (Mutual TLS)** box is checked.
  - b. Under Certificate, the **Issue to** field must be equal to the FQDN of the Pool.



**Figure 154: Home Server Edit Connection - TLS**

2. Confirm you have the correct settings for the Home Server General tab and Edit Connection for TCP (see [Figure 155: Home Server Edit Connection - TCP](#) on page 258).

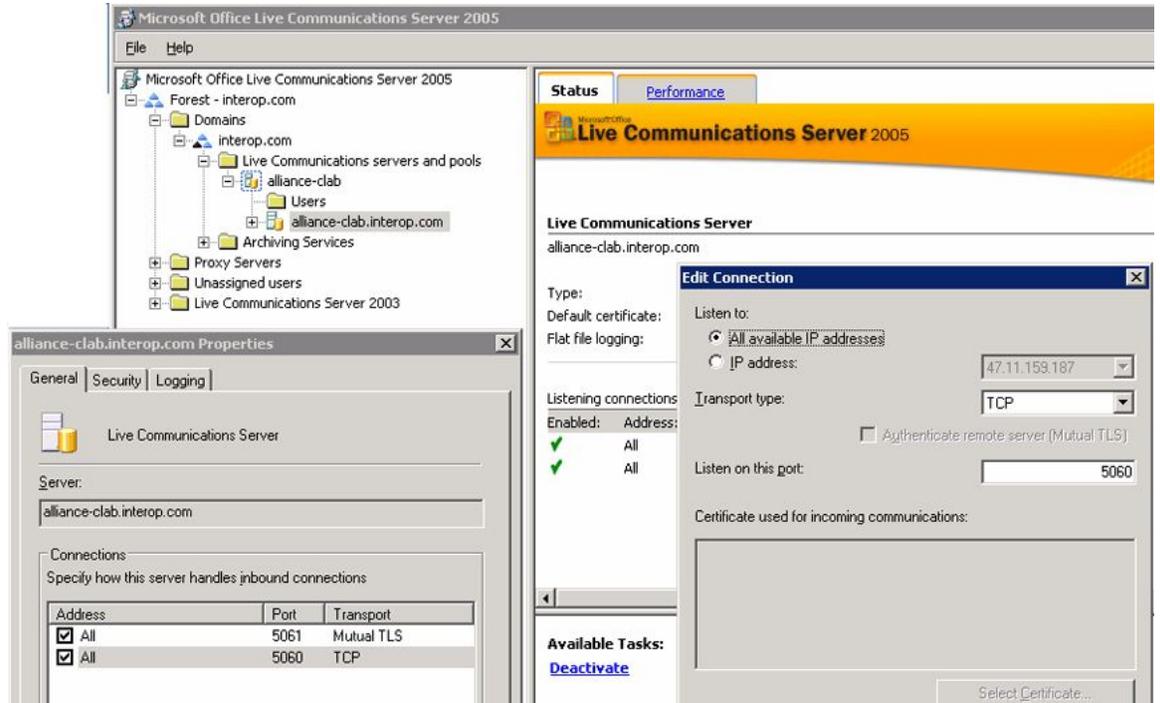


Figure 155: Home Server Edit Connection - TCP

3. To confirm the TLS settings for the Proxy Server, check the settings on the **General** tab and Edit Connection for TLS (see [Figure 156: Proxy Server Edit Connection - TLS](#) on page 259).
  - a. Confirm that the **Authenticate remote server (Mutual TLS)** box is checked.
  - b. Confirm that the **Issue to** field in the Certificate used for incoming communications box is the FQDN of the Proxy Server.

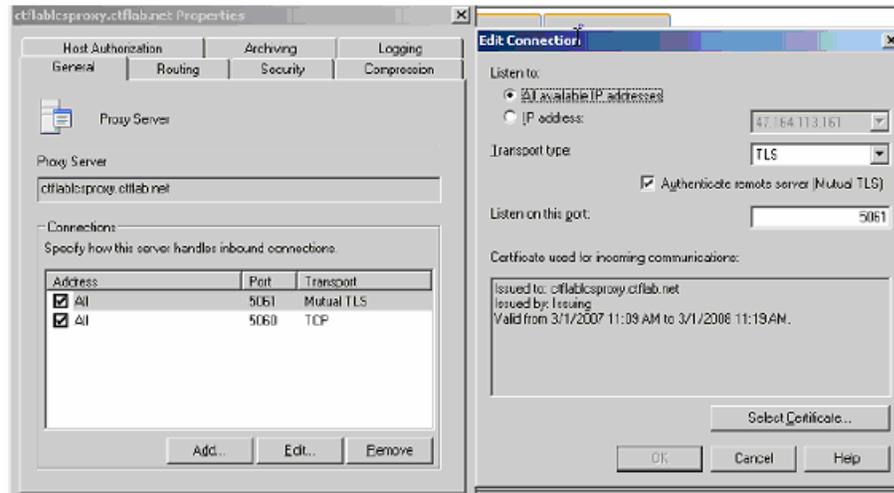


Figure 156: Proxy Server Edit Connection - TLS

- To confirm the TCP settings for the Proxy Server, check the settings on the **General** tab and Edit Connection for TCP (see [Figure 157: Server Edit Connection - TCP](#) on page 259).

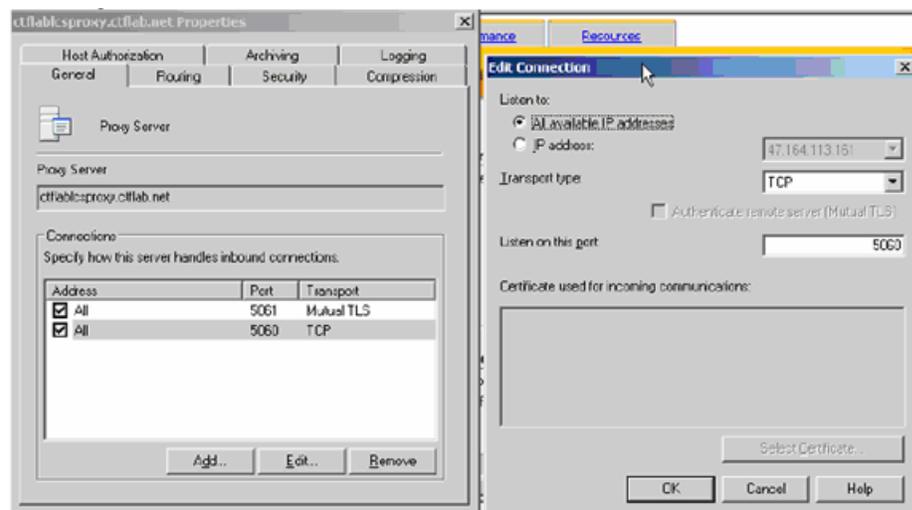


Figure 157: Server Edit Connection - TCP

## Security/Certificates

Prior to the setup of Converged Office, configure certificates.

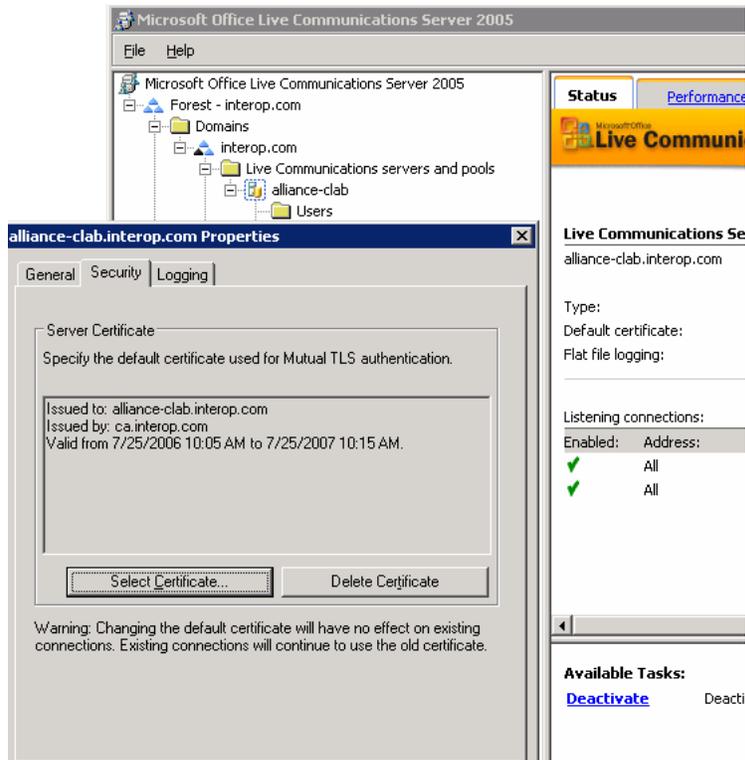
**\* Note:**

Certificate configuration is not covered in this section.

Use the following procedure to check your configuration settings of Security/Certificates.

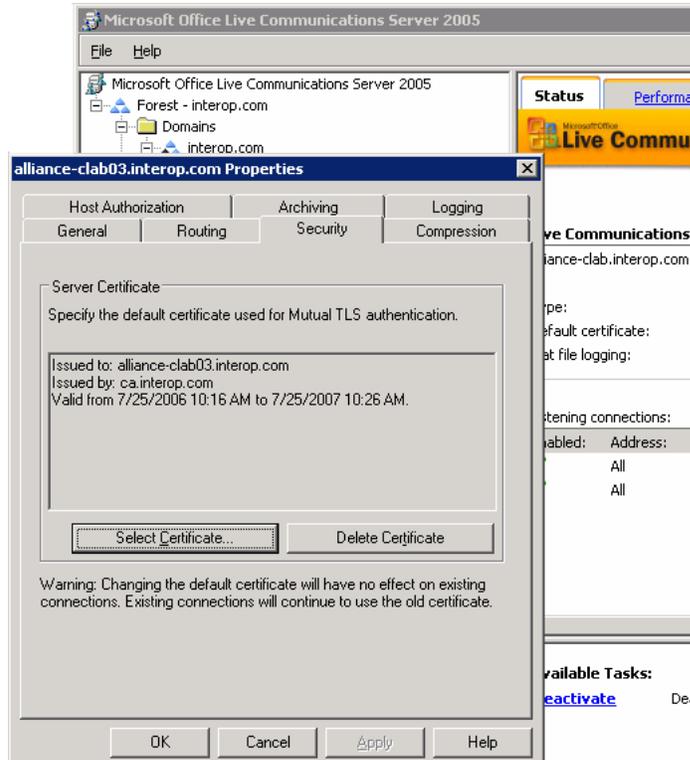
## Checking the configuration of Security/Certificates

1. Confirm the settings of the Home Server Certificate. The Certificate must be issued to the FDQN of the Pool, not to FQDN of the Home Server (see [Figure 158: Home Server Certificate](#) on page 260).



**Figure 158: Home Server Certificate**

2. Confirm the settings of the Proxy Server Certificate (see [Figure 159: Proxy Server Certificate](#) on page 261).



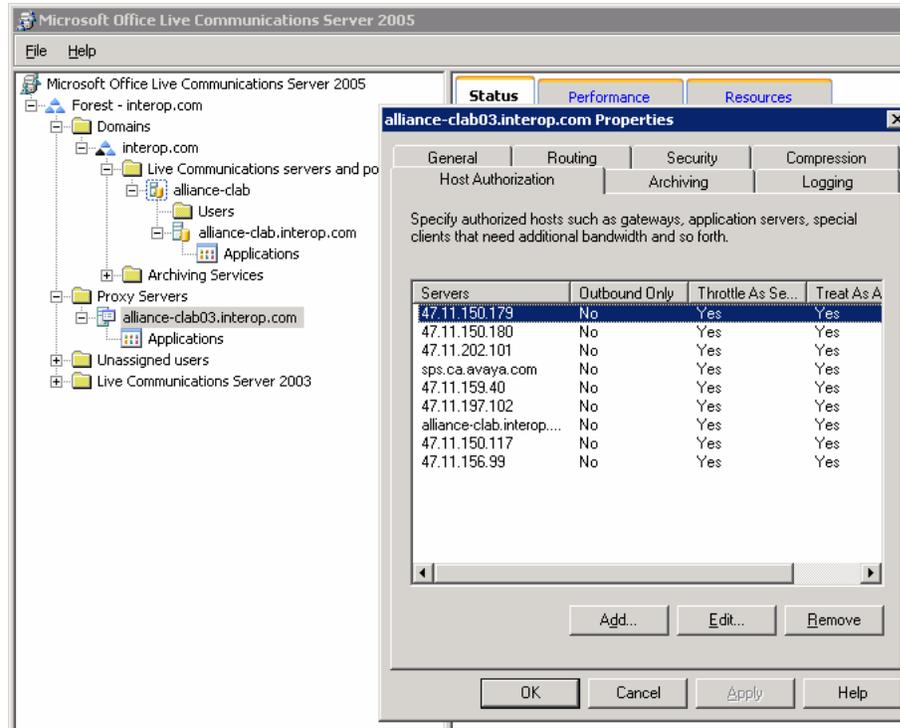
**Figure 159: Proxy Server Certificate**

## Host Authorization

Use the following procedure to check your configuration settings of Host Authorization.

### Checking the configuration of Host Authorization

1. Confirm the settings of the Host Authorization for the Home Server (see [Figure 160: Host Authorization for Home Server](#) on page 262).



**Figure 160: Host Authorization for Home Server**

2. Confirm the settings of the Host Authorization for Application Proxy Server (see [Figure 161: Host Authorization for Proxy Server](#) on page 263).

Use the IP address to configure TCP. Use FQDN to configure TLS. In the example in [Figure 161: Host Authorization for Proxy Server](#) on page 263, the Proxy server exchanges messages with Communication Server 1000 using TCP and with the Pool/Home Server using TLS.

**\* Note:**

As illustrated in [Figure 161: Host Authorization for Proxy Server](#) on page 263, the Node IP is 47.164.115.234 and the NRS IP is 47.164.115.235.

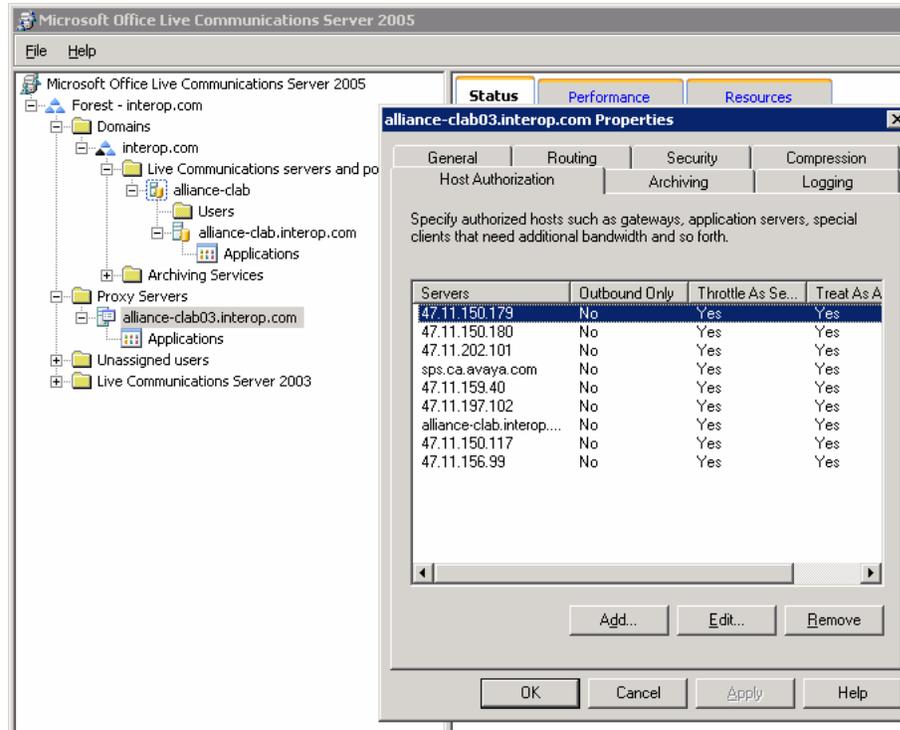


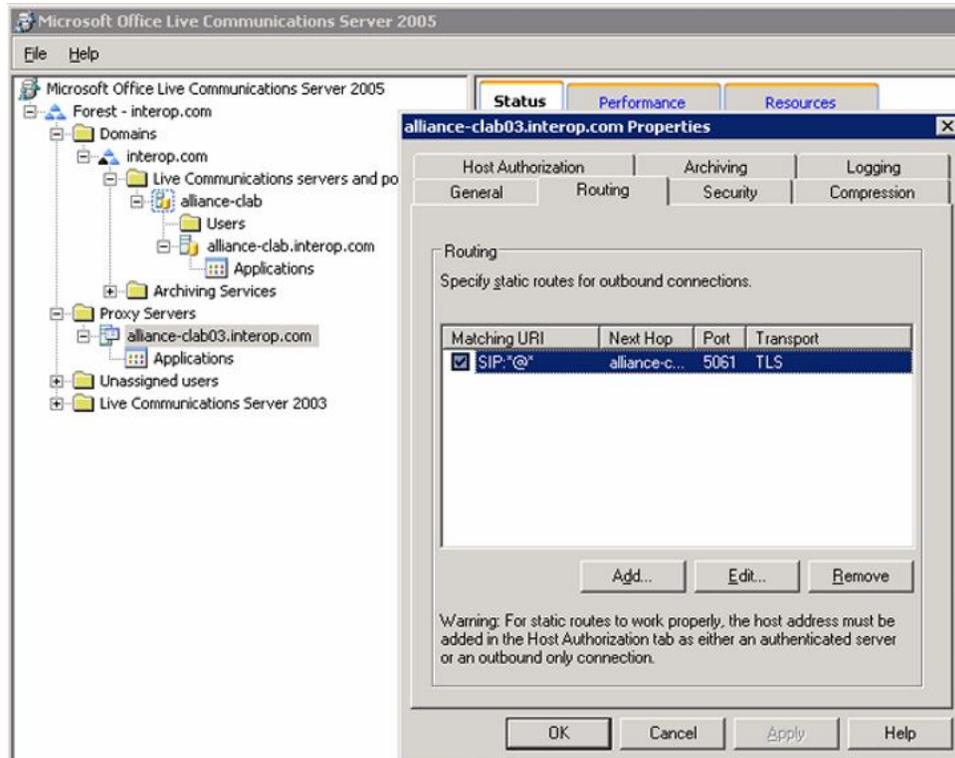
Figure 161: Host Authorization for Proxy Server

## Routing

Use the following procedure to check that Routing is correctly configured.

### Checking that Routing is correctly configured

1. Compare the Routing settings of the Home Server Enterprise Pool with the Routing settings in [Figure 162: Routing for Enterprise Pool](#) on page 264.



**Figure 162: Routing for Enterprise Pool**

2. Confirm the Phone URI rule settings in the Edit Static Route menu (see [Figure 163: Edit Static Route - Phone URI rule](#) on page 265). Forward all requests with Phone URI to the Proxy Server.

**\* Note:**

Use TLS protocol and FQDN of the Proxy server.

**Edit Static Route**

Matching URI (Uniform Resource Identifier)  
Wildcard characters can be used in the user and domain names.

User: \*

Domain: \*

Phone URI

Next hop

Network address: alliance-clab.interop.com

IP address:

Transport: TLS

Port: 5061

Replace host in request URI

Certificate used for Mutual TLS encryption:

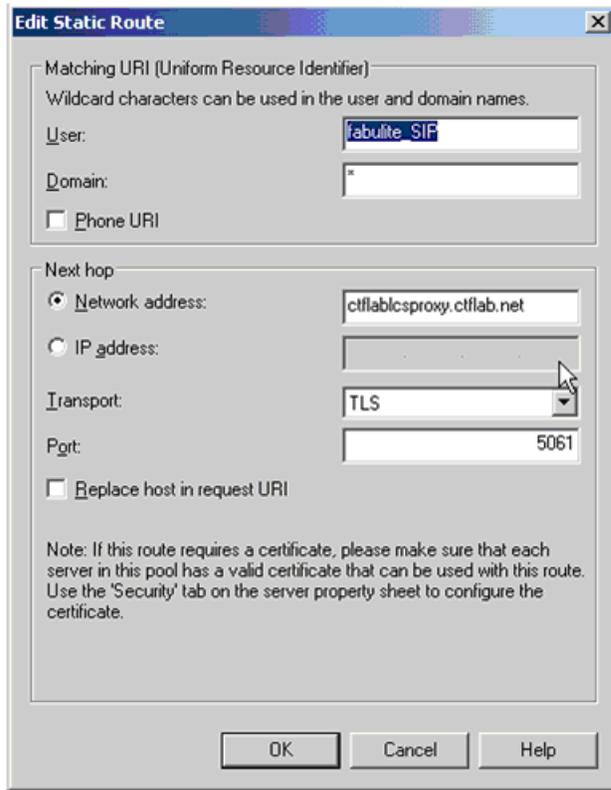
Issued to: alliance-clab03.interop.com  
Issued by: ca.interop.com  
Valid from 7/25/2006 10:16 AM to 7/25/2007 10:26 AM.

Select Certificate... Delete Certificate

OK Cancel Help

**Figure 163: Edit Static Route - Phone URI rule**

3. Confirm the TR87 FE rule settings in the Edit Static Route menu (see [Figure 164: Edit Static Route - TR87 FE rule](#) on page 266). Forward all requests related to the TR87 FE (Signaling Server Endpoint) to the Proxy Server.



**Figure 164: Edit Static Route - TR87 FE rule**

4. Confirm the Routing and Edit Connection in the Edit Static Route menu (see [Figure 165: Edit Static Route](#) on page 267).

Forward all messages back to the Pool.

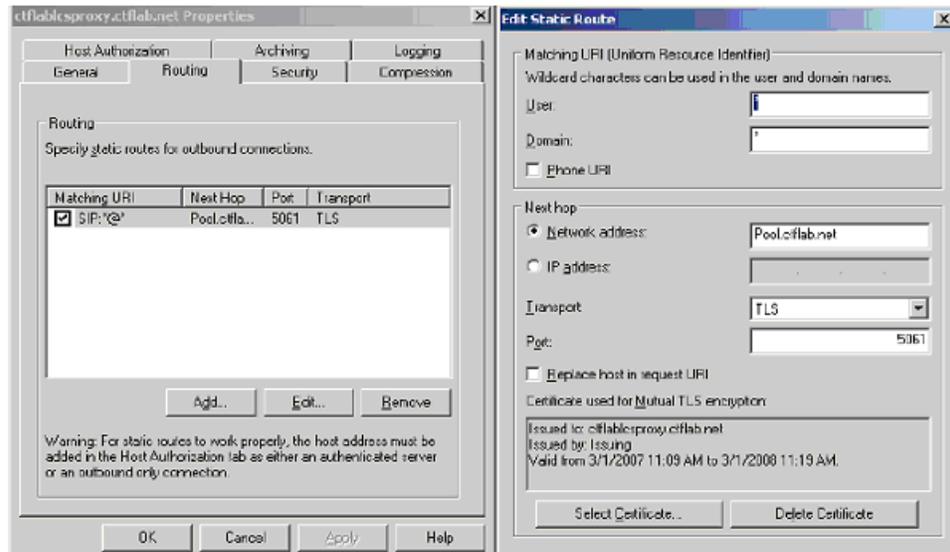


Figure 165: Edit Static Route

## Configuring DNS

Use the following procedure to check the settings for DNS Configuration. Checking these settings assumes that the DNS service is enabled on the Windows 2003 server. The LCS servers are also using this DNS server.

### Checking that DNS is correctly configured

1. Check that `_sipinternaltls` and `_sipinternal` SRV records are configured properly. Refer to the Microsoft LCS Enterprise Edition Deployment Guide for more information regarding these configurations. [Figure 166: `\_sipinternal` and `\_sipinternaltls` SRV records](#) on page 268 shows the settings for `_sipinternal` and `_sipinternaltls` SRV records.

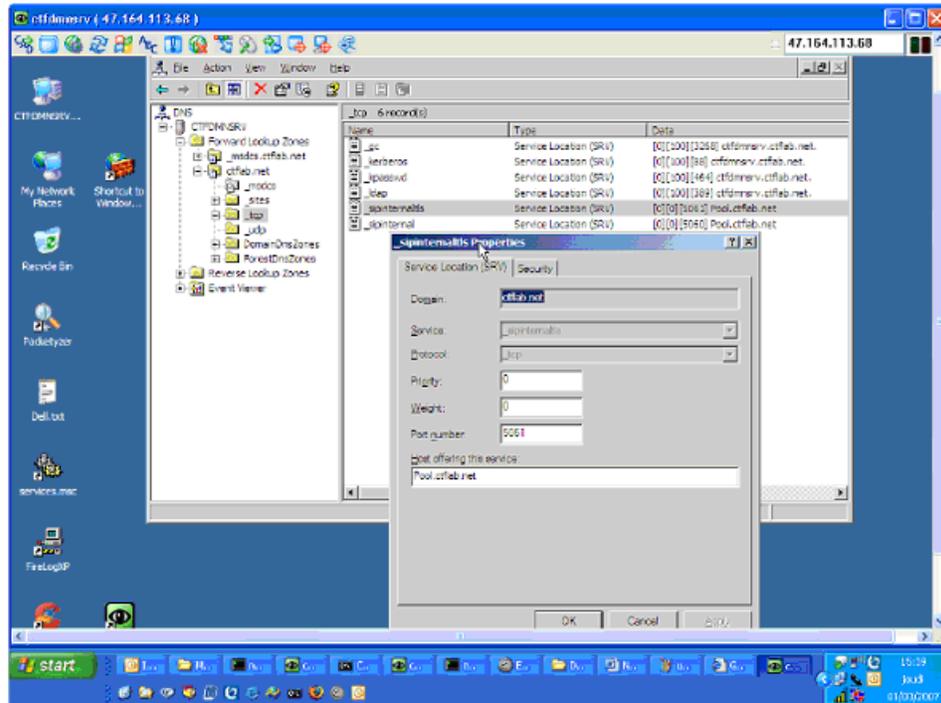


Figure 166: \_sipinternal and \_sipinternaltls SRV records

2. Check the settings of the Host (A) record for the Pool (see [Figure 167: Host \(A\) record for the Pool](#) on page 268).

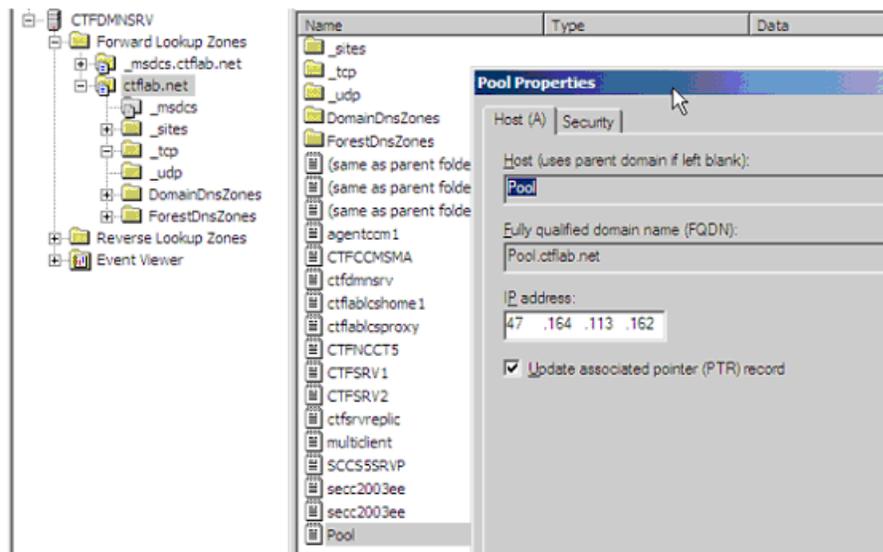
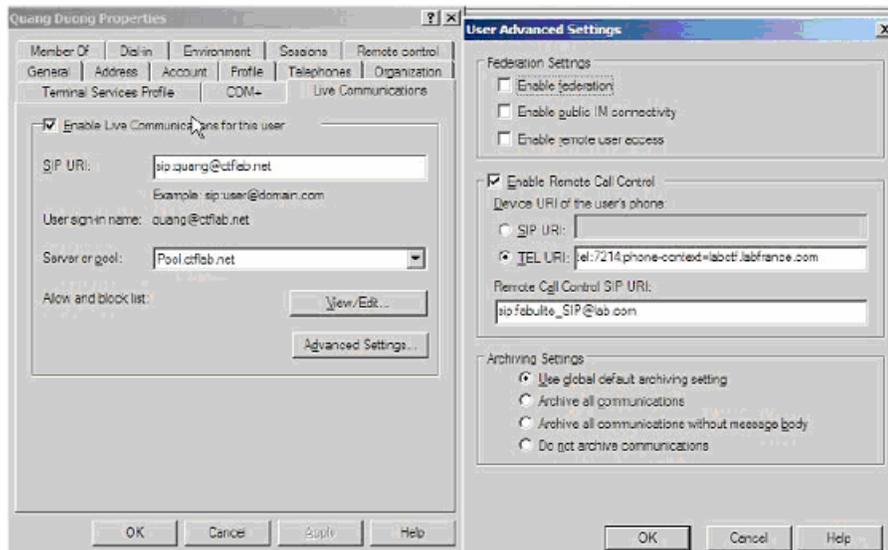


Figure 167: Host (A) record for the Pool

## Active Directory configuration

See [Figure 168: User Advanced Settings](#) on page 269 to check the settings TEL URI and Remote Call Control SIP URI.



**Figure 168: User Advanced Settings**

**Note:**

Refer to the Standard Edition section at the beginning of this Appendix for more detail on the user configuration of Active Directory.

## Installing and configuring MCM

Use the following procedure to check that MCM is correctly installed and configured.

### Checking that MCM is correctly installed and configured.

1. Assign the required Local group to the MCM user.

Prior to installation of MCM, an MCM user inside the Active Directory is created and the Administrators and RTC Server Application local group is assigned to this user.

2. On the Proxy Server, right-click on My Computer and choose Manage (as shown in [Figure 169: Manage MCM Local Group](#) on page 270). This assigns the MCM user to the local administrator and RTC Server Application.

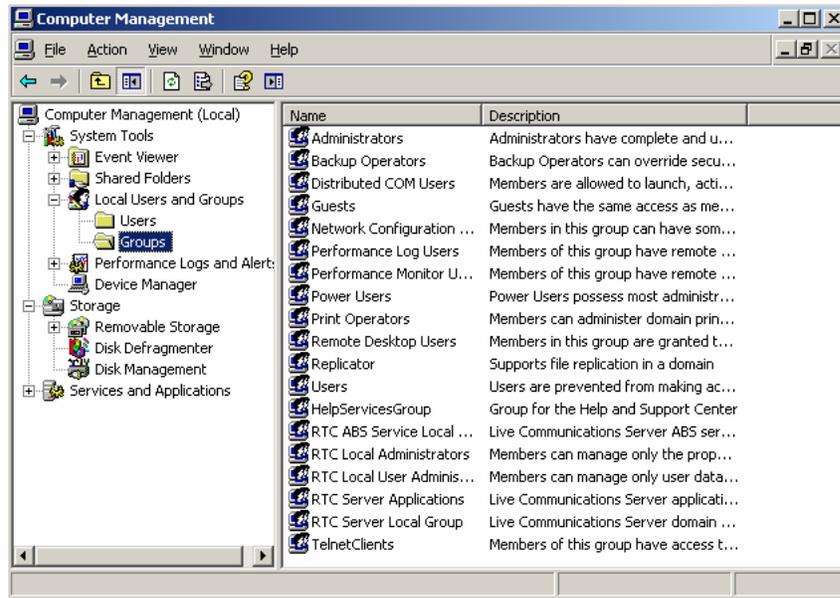


Figure 169: Manage MCM Local Group

3. Confirm that the settings of the Local Administrators Group are correct (See [Figure 170: Local Administrators group](#) on page 270).

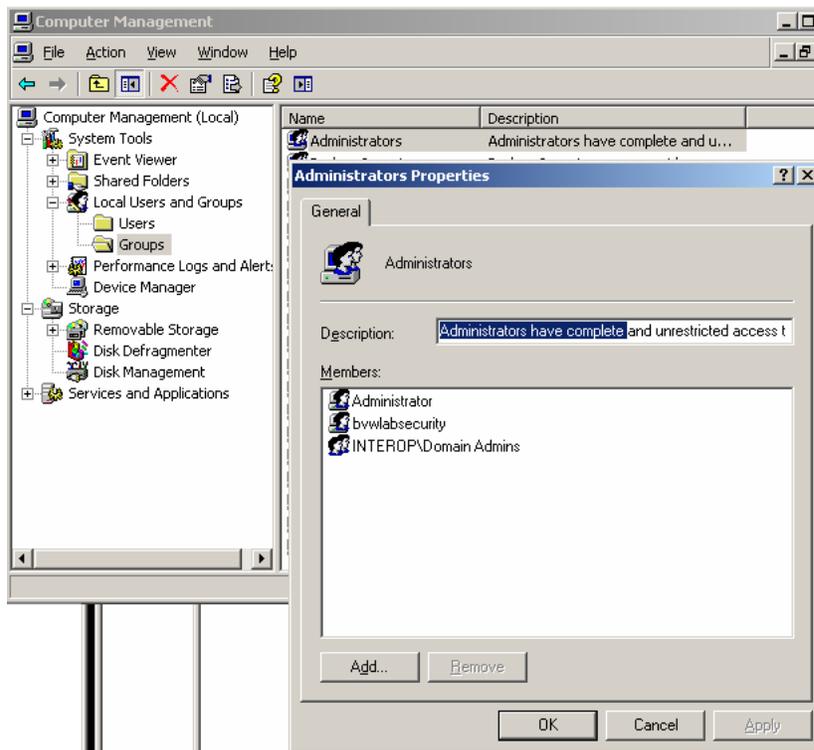
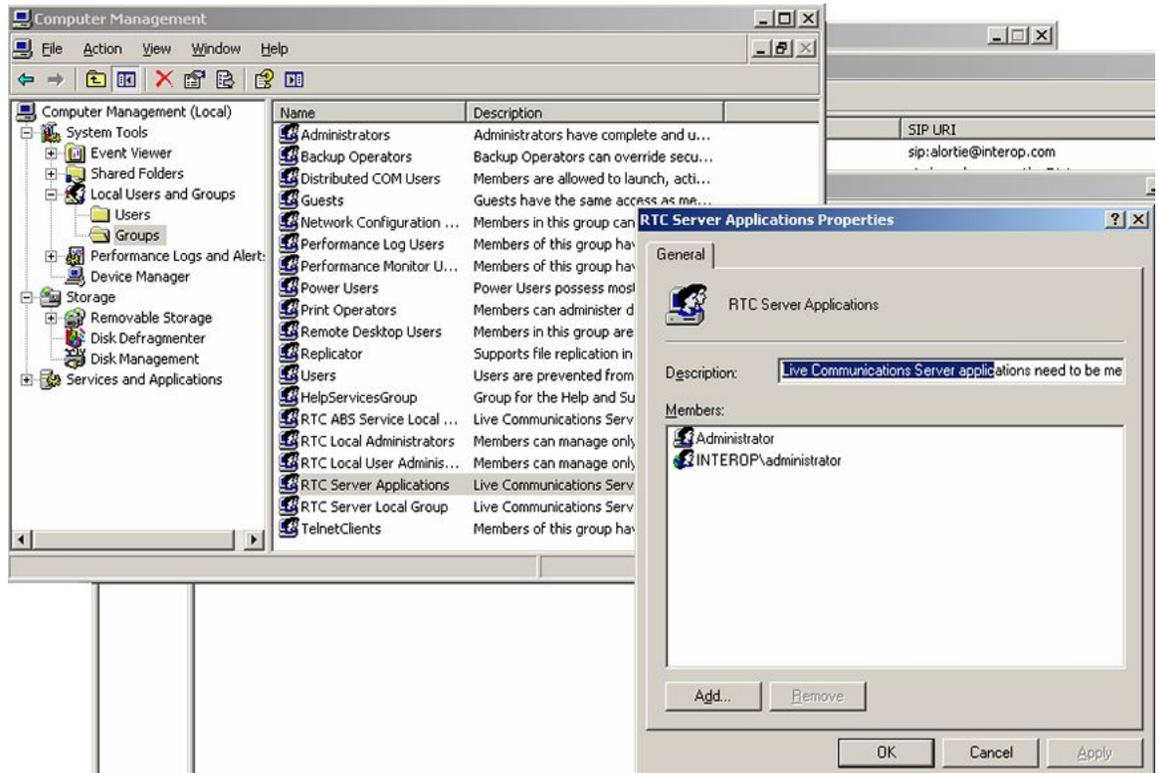


Figure 170: Local Administrators group

4. Confirm that the settings of the RTC Server Application group are correct (see [Figure 171: RTC Server Application group](#) on page 271).

**! Important:**

- MCM may not run if the MCM user is not configured to belong to the required groups.
- MCM may not run if an incorrect password is entered during the MCM installation.



**Figure 171: RTC Server Application group**

5. For MCM configuration, ensure that the correct Called Phone Context is entered. The Called Phone Context must correspond to what is configured for the user inside Active Directory and the SIP URI map, Private/CDP domain name configured in Element Manager (see [Figure 172: MCM configuration](#) on page 272).

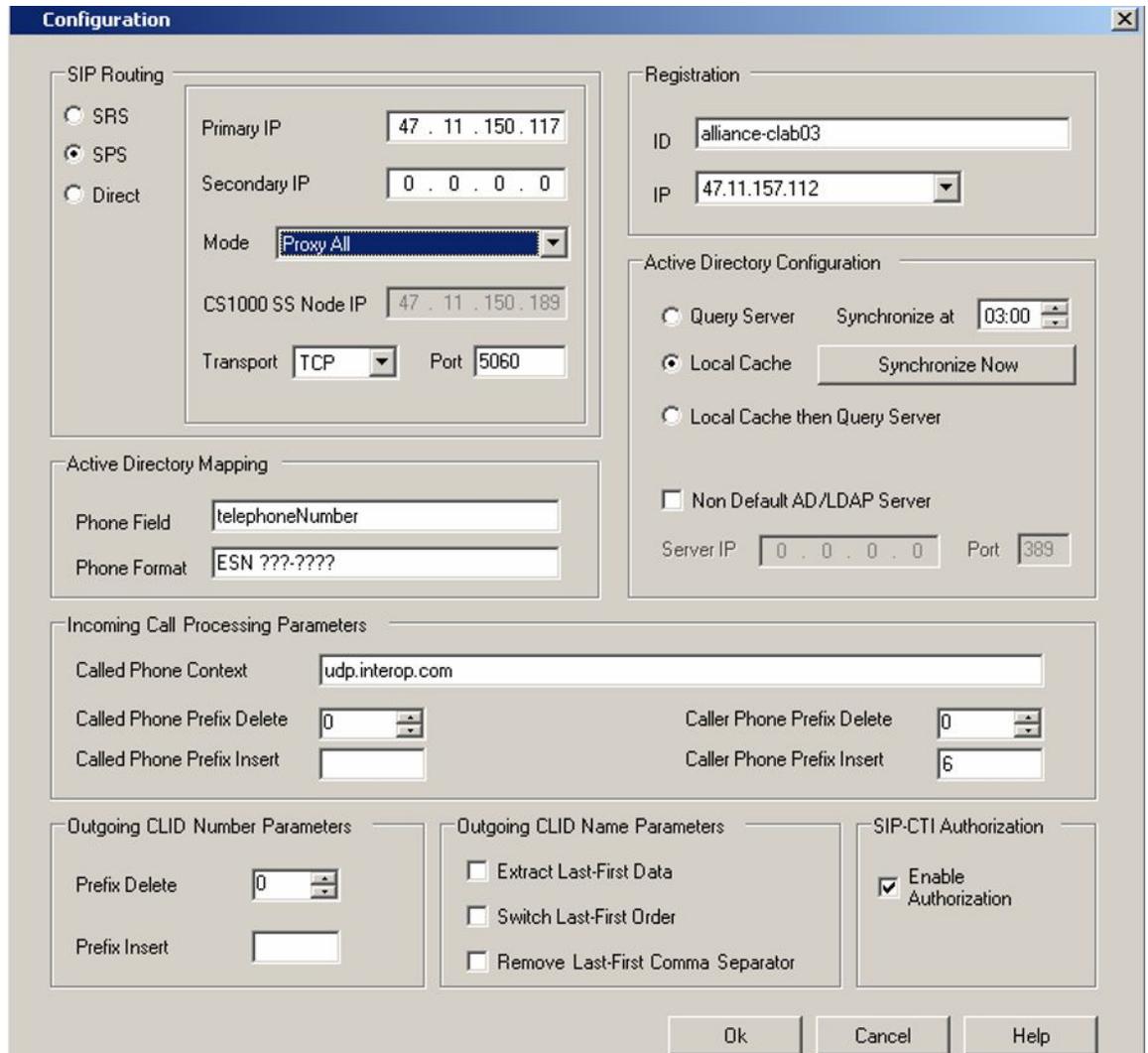


Figure 172: MCM configuration

## Configuring the Signaling Server

Use the following procedure to check that the Signaling Server is correctly configured.

### Checking that the Signaling Server is correctly configured

1. In the Host table, confirm that the correct FQDN for the Pool and the Proxy Server were entered (see [Figure 173: Host Table](#) on page 273).
2. Assign the required Local group to the MCM user in the Host table.

Host Table		Add
Host Name	IP Address	
alliance-clab03.interop.c	47.11.157.112	Remove
alliance-clab.interop.co	47.11.159.187	Remove

Figure 173: Host Table

3. Check the settings of SIP URI (see [Figure 174: SIP URI](#) on page 273).

- SIP URI Map	
Public E.164/National domain name	northamerica.com
Public E.164/Subscriber domain name	+1613
Public E.164/Unknown domain name	public.unknown
Public E.164/Special Number domain name	public.special
Private/UDP domain name	udp.interop.com
Private/CDP domain name	cdp.interop.udp.interop.
Private/Special Number domain name	special.udp.interop.com
Private/Unknown (vacant number routing) domain name	private.unknown
Unknown/Unknown domain name	unknown.unknown

Figure 174: SIP URI

## Configuring NRS

Use the following procedure to check that the NRS is correctly configured.

### Checking that NRS is correctly configured

1. In Gateway Endpoints, confirm that the settings are correct (see [Figure 175: TR87A FE and MCM endpoints](#) on page 273).



#### Note:

TR87A FE = Fabulite\_SIP and MCM = mcmendpoint

11	unstable.ac	Dynamic SIP	Not registered	SDO 804E 19 SIP	5
12	route 1023	RAS 11320	47.114.115.234	450W11320	5
13	route SIP	Dynamic SIP	47.114.115.234	RIC 45375 SIP	2
14	sdm sip	Dynamic SIP	Not registered	09 j065 SIP	2
15	sdm sip	RES 14125	Not registered	sdm	2
15	mcmendpoint	Dynamic SIP / NCC	47.114.113.151	Not available	1

Figure 175: TR87A FE and MCM endpoints

2. In Routing Entries for PCA > Endpoints, confirm that the settings are correct (see [Figure 176: Routing Entries for PCA Endpoints](#) on page 274).

User Endpoints  
=> Routing Entries  
Default Routes  
Collaborative Servers

lab.com / latfrance.com / labctf /

Gateway Endpoint: mcmendpoint [Look up](#)

With DN Type: < All DN Types > [Show](#)

Showing 1 - 1 of 1 < Previous

#	DN Prefix	DN Type	Route Cost	SIP URI Phone Context
1	8214	Private level 0 regional (CDP steering code)	1	labctf@latfrance.com

**Figure 176: Routing Entries for PCA Endpoints**

# Appendix C: Troubleshooting

---

## General Troubleshooting

Use the following procedures to troubleshoot general Converged Office problems.

### Checking Telephony Gateway (SIP Gateway) configuration to troubleshoot Converged Office problems

1. Check all required Avaya Communication Server 1000 resources (packages, license, and Avaya CS 1000 patches).
2. Check the DN, telephone TN and PCA configuration.
3. Check the DNS on the Signaling Server.
4. Verify the Signaling Server SIP and the MCM endpoint registration on the NRS.
5. Ensure that MCM is registered to the NRS.
6. Verify the Host Authorization and Certificates inside LCS Servers and Pool.



**Note:**

Improper configuration of Host Authorization and Certificates in LCS Servers and Pool is the primary reason Converged Office does not function properly in the Enterprise Edition configuration.

### Checking Remote Call Control (SIP CTI) configuration to troubleshoot Converged Office problems

1. Check all required CS 1000 resources (packages, license, and CS 1000 patches).
2. Check the DN, telephone TN and PCA configuration.
3. Verify that AST, IAPG, and CLS (CDMR/TR87A) are configured correctly (SIP CTI only).
4. Verify that the AML Link status is up. Make sure that the ELAN ID is greater or equal to 32 (SIP CTI only).
5. Check the SIP CTI status (on the Signaling Server, under PDT, issue the command SIPCTIShow). Make sure the SIP CTI status reads Application status: Active (SIP CTI only).
6. Check the DNS on the Signaling Server.
7. Verify the Signaling Server SIP and the MCM endpoint registration on the NRS.

8. Ensure that MCM is registered to the NRS.
9. Verify the MCM configuration for the Called Phone Context and check it against:
  - a. the user TEL URI inside Active Directory; and
  - b. the Signaling Server configuration for the SIP URI map and Private/CDP domain name parameter (SIP CTI only).
10. Verify the Routing, Host Authorization, and Certificates inside LCS Servers and Pool.



**Note:**

Improper configuration of Routing, Host Authorization, and Certificates in LCS Servers and Pool is the primary reason Converged Office does not function properly in the Enterprise Edition configuration.

If a problem still exists after following the steps in Undefined Resource and [Checking Remote Call Control \(SIP CTI\) configuration to troubleshoot Converged Office problems](#) on page 275, capture traces to further investigate the cause of the problem.

[Capturing traces and logs to troubleshoot Converged Office problems](#) on page 276 guides you through capturing traces.

### Capturing traces and logs to troubleshoot Converged Office problems

1. In LD 48, activate AML traces on the Call Server (SIP CTI only):
  - enl msgi 32 (Enable incoming AML traces for ELAN 32)
  - enl msgi 32 (Enable incoming AML traces for ELAN 32)
  - enl msgi 32 (Enable incoming AML traces for ELAN 32)

The following are examples of AML traces when logging a user:

```
ELAN32 I MTYP=3B IACR TN=0 TIME=18:07:34
ELAN32 IN B1B1BE7A OUT B1B1BE7C QSIZE 00000000
ELAN32 03 20 00 00 00 00 1E 3B 00 0B 00 00 95 01 05 36 02
72 14 E6
ELAN32 0C BF EE 01 FF FF FF 00 00 0F FF 00 00
```

```
ELAN32 O MTYP=3C IACS TN=0 TIME=18:07:34
ELAN32 IN B1B1BE8B OUT 00000000 QSIZE 00000000
ELAN32 03 27 00 00 00 00 1E 3C 00 0B 00 00 95 01 05 36 02
72 14 E6
ELAN32 0C BF EE 01 FF FF FF 00 00 0F FF 00 00 37 02 98
C2 AA 01 00
```

```
ELAN32 I MTYP=1D SETFTR TN=0 TIME=18:07:34
ELAN32 IN B1B1C6E8 OUT B1B1C6EA QSIZE 00000000
ELAN32 03 16 00 00 00 00 16 1D 00 0B 00 00 46 01 08 36 02
72 14 3F
ELAN32 02 00 00
```

```
ELAN32 O MTYP=1D SETFTR TN=0 TIME=18:07:34
ELAN32 IN B1B1C6EE OUT 00000000 QSIZE 00000000
ELAN32 03 1D 00 00 00 00 16 1D 00 0B 00 00 3F 02 98 C2 46
```

```
01 08 36  
ELAN32 02 72 14 71 01 01 78 02 20 0E
```

2. Under PDT, to activate SIP CTI Traces on the Signaling Server (SIP CTI only):

- pdt>SIPCTITrace on
- pdt>SIPCTITraceLevel 1

The following figure shows an example of SIP CTI Traces on the Signaling Server:

```

pdt> SIPCTITrace: (13/04/06 15:34:39) <?xml version=1.0?>
SIPCTITrace: (13/04/06 15:34:39) <RequestSystemStatus xmlns=http://www.ecma-international.org/standards
SIPCTITrace: (13/04/06 15:34:39) /ecma-323/csta/ed3><extensions><privateData><private><cs:line xmlns:l
SIPCTITrace: (13/04/06 15:34:39) cs=http://schemas.microsoft.com/Lcs/2005/04/RCCExtension>tel:7214;pho
SIPCTITrace: (13/04/06 15:34:39) ne-context=odpfabulita.labfrance.com.labfrance.com</cs:line></private>
SIPCTITrace: (13/04/06 15:34:39) </privateData></extensions></RequestSystemStatus>
SIPCTITrace: (13/04/06 15:34:39) <?xml version=1.0 encoding=UTF-8?>
SIPCTITrace: (13/04/06 15:34:39) <RequestSystemStatusResponse xmlns=http://www.ecma-international.org/s
SIPCTITrace: (13/04/06 15:34:39) tandards/ecma-323/csta/ed3>
SIPCTITrace: (13/04/06 15:34:39) <systemStatus>normal</systemStatus></RequestSystemStatusResponse>
SIPCTITrace: (13/04/06 15:34:39) <?xml version=1.0?>
SIPCTITrace: (13/04/06 15:34:39) <GetCSTAFeatures xmlns=http://www.ecma-international.org/standards/ecm
SIPCTITrace: (13/04/06 15:34:39) a-323/csta/ed3><extensions><privateData><private><cs:line xmlns:lcs=
SIPCTITrace: (13/04/06 15:34:39) http://schemas.microsoft.com/Lcs/2005/04/RCCExtension>tel:7214;phone-c
SIPCTITrace: (13/04/06 15:34:39) ontext=odpfabulita.labfrance.com.labfrance.com</cs:line></private></pr
SIPCTITrace: (13/04/06 15:34:39) ivateData></extensions></GetCSTAFeatures>
SIPCTITrace: (13/04/06 15:34:39) <?xml version=1.0 encoding=UTF-8?>
SIPCTITrace: (13/04/06 15:34:39) <GetCSTAFeaturesResponse xmlns=http://www.ecma-international.org/stand
SIPCTITrace: (13/04/06 15:34:39) ards/ecma-323/csta/ed3 xmlns:xsi=http://www.w3.org/2001/XMLSchema-ins
SIPCTITrace: (13/04/06 15:34:39) tances><supportedServices><systemStatServList><requestSystemStatus/></s
SIPCTITrace: (13/04/06 15:34:39) ystemStatServList><monitoringServList><monitorStart><monitorStop/></mo
SIPCTITrace: (13/04/06 15:34:39) nitoringServList><callControlServList><answerCall/><clearConnection/><c
SIPCTITrace: (13/04/06 15:34:39) onferenceCall/><consultationCall/><deflectCall/>
SIPCTITrace: (13/04/06 15:34:39) <holdCall/><makeCall/><retrieveCall/><singleStepTransfer/><transferCall
SIPCTITrace: (13/04/06 15:34:39) /></callControlServList><callAssociatedServList><generateDigits/></call
SIPCTITrace: (13/04/06 15:34:39) AssociatedServList><logicalServList><getForwarding/><setForwarding/></l
SIPCTITrace: (13/04/06 15:34:39) ogicalServList></supportedServices><supportedEvents><allControlEvtsList
SIPCTITrace: (13/04/06 15:34:39) t><conferenced/><connectionCleared/><delivered/><diverted/><established
SIPCTITrace: (13/04/06 15:34:39) /><failed/><held/><originated/><retrieved/><transferred/></callControlE
SIPCTITrace: (13/04/06 15:34:39) vtsList><logicalEvtsList><forwarding/></logicalEvtsList></supportedEven
SIPCTITrace: (13/04/06 15:34:39) ts></GetCSTAFeaturesResponse>
SIPCTITrace: (13/04/06 15:34:39) <?xml version=1.0?>
SIPCTITrace: (13/04/06 15:34:39) <MonitorStart xmlns=http://www.ecma-international.org/standards/ecma-3
SIPCTITrace: (13/04/06 15:34:39) 23/csta/ed3><monitorObject><deviceObject>tel:7214;phone-context=odpfab
SIPCTITrace: (13/04/06 15:34:39) ulita.labfrance.com.labfrance.com</deviceObject><monitorObject></Monit
SIPCTITrace: (13/04/06 15:34:39) orStart>
SIPCTITrace: (13/04/06 15:34:39) <?xml version=1.0 encoding=UTF-8?>
SIPCTITrace: (13/04/06 15:34:39) <MonitorStartResponse xmlns=http://www.ecma-international.org/standard
SIPCTITrace: (13/04/06 15:34:39) s/ecma-323/csta/ed3>
SIPCTITrace: (13/04/06 15:34:39) <monitorCrossRefID>23</monitorCrossRefID></MonitorStartResponse>
SIPCTITrace: (13/04/06 15:34:39) <?xml version=1.0?>
SIPCTITrace: (13/04/06 15:34:39) <SetForwarding xmlns=http://www.ecma-international.org/standards/ecma-
SIPCTITrace: (13/04/06 15:34:39) 323/csta/ed3><device>tel:7214;phone-context=odpfabulita.labfrance.com.
SIPCTITrace: (13/04/06 15:34:39) labfrance.com</device><forwardingType>forwardImmediate</forwardingType>
SIPCTITrace: (13/04/06 15:34:39) <activateForward>false</activateForward></SetForwarding>
SIPCTITrace: (13/04/06 15:34:39) <?xml version=1.0 encoding=UTF-8?>
SIPCTITrace: (13/04/06 15:34:39) <SetForwardingResponse xmlns=http://www.ecma-international.org/standar
SIPCTITrace: (13/04/06 15:34:39) ds/ecma-323/csta/ed3>

```

**Figure 177: SIP CTI Traces on the Signaling Server**

3. Under PDT, to activate (only) SIP Gateway traces on the Signaling Server:

- pdt>SIPCallTrace on
- pdt>SIPTraceLevel 1

[Figure 178: SIP Gateway Trace](#) on page 279 is an example of a SIP Gateway Trace:

```

pdr> 13/04/2006 15:41:46 LOG0006 SIPNPM: SIPCallTrace: 13/4/6 15:41:46 Recv chid:10
ip:47.164.132.159:2236 SIP INVITE
13/04/2006 15:41:46 LOG0006 SIPNPM: -> INVITE
sip:7210@47.164.113.161:5060;maddr=47.164.115.234;transport=tcp;user=phone;x-nt-
redirect=redi
13/04/2006 15:41:46 LOG0006 SIPNPM: ->> reat-server SIP/2.0
13/04/2006 15:41:46 LOG0006 SIPNPM: -> From: Duong Quang
[CTF:4782:EXCH]<sis:quang@lab.com>;tag=957bf4be67;spid=70e54056f7
13/04/2006 15:41:46 LOG0006 SIPNPM: -> To: <sip:7210@47.164.113.161;user=phone>
13/04/2006 15:41:46 LOG0006 SIPNPM: -> Call-ID: 49559ca04a8e423090363406b988a778
13/04/2006 15:41:46 LOG0006 SIPNPM: -> CSa: 1 INVITE
13/04/2006 15:41:46 LOG0006 SIPNPM: -> ms-user-data: ms-publiccloud=false;ms-
federation=false
13/04/2006 15:41:46 LOG0006 SIPNPM: -> Max-Forwards: 69
13/04/2006 15:41:46 LOG0006 SIPNPM: -> User-Agent: LCC/1.3
13/04/2006 15:41:46 LOG0006 SIPNPM: -> Ms-Conversation-ID: 928DAC21-3665-4C6E-
99AA-
62D5C3A09C03
13/04/2006 15:41:46 LOG0006 SIPNPM: -> P-Asserted-Identity: Quang, Duong.
<sis:7214:phonecontext=
cdofabulite.labfrance.com@lab.com;user=
13/04/2006 15:41:46 LOG0006 SIPNPM: ->> phone>
13/04/2006 15:41:46 LOG0006 SIPNPM: -> Record-Route: <sis:ctfca.lab.com;transport=tcp;lr>
:tag=EEB5EDD0354B38457A2C2C47BAD08E08
13/04/2006 15:41:46 LOG0006 SIPNPM: -> Via: SIP/2.0/TCP
47.164.113.161:4848;branch=z9hG4bK221144EE.ED9C6784;branched=TRUE
13/04/2006 15:41:46 LOG0006 SIPNPM: -> Via: SIP/2.0/TCP 47.164.132.159:14047;ms-
receivedport=
2236;ms-received-cid=47900
13/04/2006 15:41:46 LOG0006 SIPNPM: -> Contact:
<sip:quang@lab.com:2236;maddr=47.164.132.159;transport=tcp;ms-received-cid=47900>
13/04/2006 15:41:46 LOG0006 SIPNPM: -> Content-Type: application/SDP
13/04/2006 15:41:46 LOG0006 SIPNPM: -> Content-Length: 450
13/04/2006 15:41:46 LOG0006 SIPNPM: ->
13/04/2006 15:41:46 LOG0006 SIPNPM: -> v=0
13/04/2006 15:41:46 LOG0006 SIPNPM: -> o=- 0 0 IN IP4 47.164.132.159
13/04/2006 15:41:46 LOG0006 SIPNPM: -> s=session
13/04/2006 15:41:46 LOG0006 SIPNPM: -> c=IN IP4 47.164.132.159
13/04/2006 15:41:46 LOG0006 SIPNPM: -> b=CT:1000
13/04/2006 15:41:46 LOG0006 SIPNPM: -> t=0 0
13/04/2006 15:41:46 LOG0006 SIPNPM: -> m=audio 24914 RTP/AVP 97 111 112 60 8 4 5 3
101
13/04/2006 15:41:46 LOG0006 SIPNPM: -> a=rtpmap:97 red/8000
13/04/2006 15:41:46 LOG0006 SIPNPM: -> a=rtpmap:111 SIREN/16000
13/04/2006 15:41:46 LOG0006 SIPNPM: -> a=fmtp:111 bitrate=16000
13/04/2006 15:41:46 LOG0006 SIPNPM: -> a=rtpmap:112 G7221/16000
13/04/2006 15:41:46 LOG0006 SIPNPM: -> a=fmtp:112 bitrate=24000
13/04/2006 15:41:46 LOG0006 SIPNPM: -> a=rtpmap:6 DVT4/16000
13/04/2006 15:41:46 LOG0006 SIPNPM: -> a=rtpmap:0 PCMU/8000
13/04/2006 15:41:46 LOG0006 SIPNPM: -> a=rtpmap:8 PCMA/8000
13/04/2006 15:41:46 LOG0006 SIPNPM: -> a=rtpmap:4 G723/8000
13/04/2006 15:41:46 LOG0006 SIPNPM: -> a=rtpmap:5 DVT4/8000
13/04/2006 15:41:46 LOG0006 SIPNPM: -> a=rtpmap:3 GSM/8000
13/04/2006 15:41:46 LOG0006 SIPNPM: -> a=rtpmap:101 telephone-event/8000
13/04/2006 15:41:46 LOG0006 SIPNPM: -> a=fmtp:101 0-16
13/04/2006 15:41:46 LOG0006 SIPNPM: ->

```

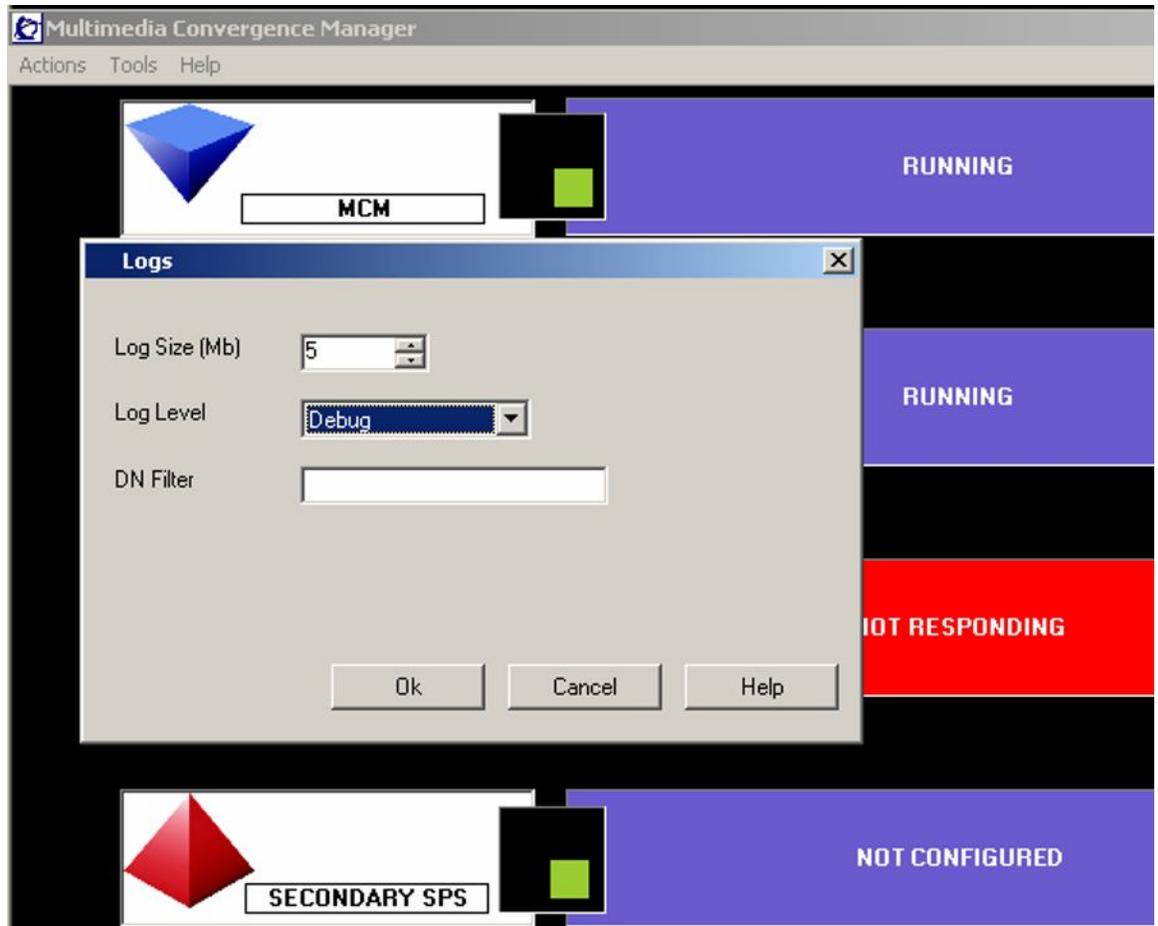
**Figure 178: SIP Gateway Trace**

4. On the MCM interface, to activate MCM logs, select **Tools** → **Log Level** and then select **Log Level = Debug** (applies to both SIP CTI and SIP Gateway).

The logs are copied into the file MCM.log in the directory where MCM is installed.

**\* Note:**

To reset the trace, configure the Log Level to None and then delete the MCM.log file and reset the Log Level to Debug, as shown in the following figure.



**Figure 179: MCM logs**

The following figure shows an example of MCM logs:

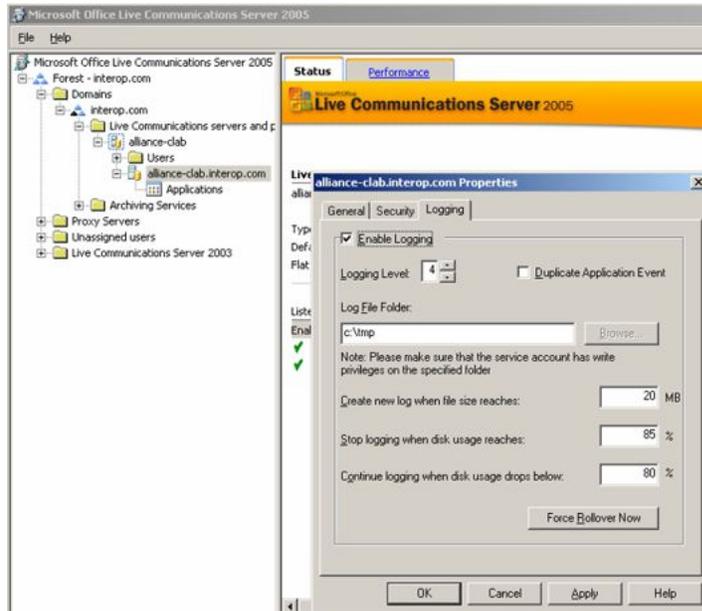
```

11/14/2006 6:35:15 PM: 1.0.20.7: Debug: ServerEventHandler: got Event #0
11/14/2006 6:35:15 PM: 1.0.20.7: SIP:
-----
Request: INVITE sip:brahim@LabCtfLcsDns.com
contact: <sip:nico@LabCtfLcsDns.com:1463;ma addr=47.165.248.245;transport=tcp;ms-received-
cid=4400>
via: SIP/2.0/TCP 47.165.248.245:11746;ms-received-port=1463;ms-received-cid=4400
max-forwards: 70
from: Nico Nguyen <sip:nico@LabCtfLcsDns.com>;tag=dc038094fe;epid=1e24064768
to: <sip:brahim@LabCtfLcsDns.com>
call-id: 731a4e0dbba0437ea1ce2899eaa11a1b
cseq: 1 INVITE
user-agent: LCC/1.3
Ms-Conversation-ID: BC26228E-E2B6-4D94-97A3-D06F2880DDCD
ms-text-format: text/plain; charset=UTF-
8;msg=WAAAtAE0ATQBTAC0ASQBNAC0ARgBvAHIAbQBhAHQA0gAgAEYATgA9AE0A
UwAlADIAMABTAGgAZQBsAG
wAJQAYADAARABsAGcAOwAgAEUARgA9ADsAlABDAE8APQAwADsAlABDAFMAPQ
AwADsAlABQAEYAPQAwAA0A
CgANAAoA;ms-
body=VHUgcGV1eCBtJ2FwcGVsZXIgc3VyIGxIIIG51bWVYbyA3MjEwIFNUUA==
supported: ms-delayed-accept
supported: ms-renders-gif
Roster-Manager: sip:nico@LabCtfLcsDns.com
EndPoints: Nico Nguyen <sip:nico@LabCtfLcsDns.com>, <sip:brahim@LabCtfLcsDns.com>
supported: commicrosoft.rtc-multiparty
content-type: application/sdp
content-length: 125
v=0
o=- 0 0 IN IP4 47.165.248.245
s=session
c=IN IP4 47.165.248.245
t=0 0
m=message 5060 sip sip:nico@LabCtfLcsDns.com
-----
11/14/2006 6:35:15 PM: 1.0.20.7: Debug: ServerEventHandler: got Event #0
11/14/2006 6:35:15 PM: 1.0.20.7: SIP:
-----
Response: 100 Trying
via: SIP/2.0/TCP 47.165.248.245:11746;ms-received-port=1463;ms-received-cid=4400
from: Nico Nguyen <sip:nico@LabCtfLcsDns.com>;tag=dc038094fe;epid=1e24064768
to: <sip:brahim@LabCtfLcsDns.com>;epid=72fa56eb1c;tag=3fbf31efe2
call-id: 731a4e0dbba0437ea1ce2899eaa11a1b
cseq: 1 INVITE
user-agent: LCC/1.3
content-length: 0

```

**Figure 180: Example of MCM logs**

- To activate LCS logs, right click **LCS Home Server** and click the **Logging** tab. Configure Logging Level to **4** and configure **Force Rollover Now** to a new LCS file, as shown in the following figure.



**Figure 181: Activate LCS logs**

If you are using an LCS Enterprise Edition, repeat Step 5 on both the Home Server and the Application Proxy Server. The following figure shows an example of LCS logs:

```

$$end_record
$$begin_record
LogType: protocol
Date: 2006/11/13 11:57:29
Direction: Incoming
Peer: 47.164.133.191:2084
Message-Type: Request
Start-Line: SERVICE sip:tel:7210;phone-context=dialstring SIP/2.0
To: <sip:tel:phone-context=dialstring>
From: Quang Duong <sip:Quang@LabCtfLcsDns.com>;tag=58115997ed;epid=eaab4184c6
Call-ID: 0a8ce19bbb714de087df7580b0a76788
CSeq: 1 SERVICE
Contact:
<sip:Quang@LabCtfLcsDns.com:11526;maddr=47.164.133.191;transport=tcp>;proxy=replace
Via: SIP/2.0/TCP 47.164.133.191:11526
Max-Forwards: 70
Content-Length: 277
Content-Type: application/SOAP+xml
Other-headers: User-Agent: LCC/1.3.5371 (Microsoft Office Communicator 2005 1.0.559.121)
Other-headers: Proxy-Authorization: Kerberos qop=auth, realm=SIP Communications Service,
opaque=0F2BD4CF,
crand=a3722d1f, cnum=345, targetname=sip/LabCtfLcs.LabCtfLcsDns.com,
response=602306092a864886f71201020201011100ffffffffffe53dcf1cc59e1dd6d1ae09be4528e59a
Message-Body: <SOAP-ENV:Envelope xmlns:SOAP-
ENV=http://schemas.xmlsoap.org/soap/envelope/><SOAPENV:
Body><m:getPresence xmlns:m=http://schemas.microsoft.com/winrtc/2002/11/sip><presentity
uri=sip:tel:7210;phonecontext=
dialstring/></m:getPresence></SOAP-ENV:Body></SOAP-ENV:Envelope>
$$end_record

```

**Figure 182: Example of LCS logs**

---

## Issues of concern

The following are some common issues users may encounter, and suggested solutions to resolve those issues.

---

### Issue 1

**Problem:** Lack of Memory for Signaling Server.

**Symptom:** After SIP CTI services are activated, inability to log in to the Signaling Server through Element Manager. When rebooting, some HTTP tasks are not up.

**Possible cause:** Insufficient memory.

Solution: Check the memory and upgrade the memory to 1Gb, if required.

Only 512 MB of Signaling Server memory is required for Release 4.5, but 4.50.75 or above (running Converged Office) requires 1 GB of memory.

---

## Issue 2

Problem: SIP CTI service down.

Symptom: After SIP CTI services are activated, SIPT CTI services do not come up.

Possible cause: VSID or ELAN ID is lower than 32.

Solution: Follow the steps in [Solving a problem where SIP CTI service does not come up](#) on page 284 to solve this issue.

### Solving a problem where SIP CTI service does not come up

1. Reconfigure the VSID and ELAN IDs so that each is greater than 32. Confirm that the SIP CTI service is up.
2. Check the SIPCTI status on the Signaling Server (see [Figure 183: Check the SIP CTI status](#) on page 284.

```
pdt> SIPCTIShow
SIP CTI Status and Settings:
-----
Application status: Active
Customer number: 0
Dialing plan: CDP
SIP URI format: dialstring
Maximum number of associations per DN: 5
-----
CTI Dial Plan Information
-----
Home Location Code: Not Configured
Country Code: 33
NPA Prefix: 00
INTL Prefix: 000
LOC Prefix: Not Configured
SPN Prefix: Not Configured
NXX Prefix: Not Configured
```

**Figure 183: Check the SIP CTI status**

3. Check the ELAN status on the Call Server

```
Id 48
.stat elan
SERVER TASK: ENABLED
```

```

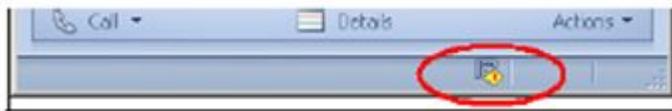
ELAN #: 032 DES: CDLCS
APPL_IP_ID: 47.11.157.112 : 0000F600 LXR7: ACTIVE EMPTY
APPL ACTIVE

```

## Issue 3

Problem: Telephone not controlled by MOC.

Symptom: When logged into the MOC, the telephone is not controlled. The icon in [Figure 184: Telephone not controlled icon](#) on page 285 is observed:



**Figure 184: Telephone not controlled icon**

Possible cause 1: The Tel URI or the Remote Call Control SIP URI is incorrect.

Solution 1: Check the parameters configured in AD for this user. Activate the SIPCTITrace on the Signaling Server and the MCM logs to check the problem.

Possible cause 2: Use Microsoft's nslookup tool to verify the DNS configuration of the Signaling Server and the Host Name resolution into each IP address. For more information on the nslookup tool see [Figure 185: nslookup tool](#) on page 285, or visit <http://support.microsoft.com/kb/200525>.

 A screenshot of a Windows command prompt window titled 'C:\WINDOWS\system32\cmd.exe'. The window shows the following text:
 

```

C:\>nslookup
Default Server: teddi.mslcs2.mera.ru
Address: 192.168.60.158

> 192.168.60.9
Server: teddi.mslcs2.mera.ru
Address: 192.168.60.158

Name: mslcsserver.mslcs.mera.ru
Address: 192.168.60.9

> exit

```

**Figure 185: nslookup tool**

Solution 2: Confirm that the FQDN (case sensitive) and the IP address are correct.

For causes (not mentioned), the actions below may help identify the problem:

- Activate AML traces on the Call Server to check if the IACR/IACS (TN acquire) are correct
- Activate SIPCTITrace

- Activate LCS home server and Proxy server traces
- Activate MCM logs
- Capture Ethereal traces

---

## Issue 4

Problem: SIP CTI popup not displayed.

Symptom: When a MOC user receives a call, the telephone called rings, but no pop-up appears for the user to click on to answer the call.

Possible cause: The Phone Context may be not correct.

Solution: Ensure that the user (inside AD), the MCM (TEL URI) and the Signaling Server (L1 parameter) have the correct Phone Context.

---

## Issue 5

Problem: Delay for SIP Gateway call.

Symptom: MOC users observe a delay at the beginning of a call.

Possible cause: Missing MOC patch.

Solution: Ensure that the MOC patch is up-to-date (especially Microsoft patch KB909087).

---

## Issue 6

Problem: MOC cancels the Call Forward configured on the telephone.

Symptom: The telephone is on Call Forward to another number. When MOC user who is associated to this telephone logs in (this telephone is controlled by the MOC user through SIP CTI), the MOC cancels the Call Forward.

Possible cause: This is a Microsoft issue that escalated to Microsoft.

Solution: No solution yet.

---

## Issue 7

Problem: MOC user cannot control the telephone after having been disconnected several times.

Symptom: Customers using smart telephones or Mobile Communicators cannot take control of the telephone after having been disconnected abruptly three or more times. This disconnection could be due to the customer's network (for example, GPRS or WLAN).

Possible cause: This problem occurs because the SIP CTI link is disconnected abnormally and the Association is out of service for 30 minutes (1800 seconds). This timer is hard-coded by MOC and cannot be changed.

Solution: Increase the Maximum Associations per DN on the Signaling Server through Element Manager. This field is configured to 3 by default. Increase this parameter to allow more network disconnections.

---

## Issue 8

Problem: MCM cannot synchronize new users in AD Cache Mode.

Symptom: Several new users are configured in AD, but MCM did not download them to its AD Cache during synchronization and cannot find them.

Possible cause 1: The changes made to those users in AD is not replicated to the Global Catalog (GC) server used by MCM.

Solution 1: One solution is to consult with Network Administrators about the schedule of replications between Domain Controllers (DCs).

Another alternative is to manually check the GC content. Follow the steps in [How to manually check the GC content](#) on page 287 to manually check the GC content.

### How to manually check the GC content

1. Install the OS Support Tools on the server (usually the Tools setup is on the MS Windows 2003 Server setup disk).
2. Run the LDP tool (%ProgramFiles%\Support Tools\ldap.exe).
3. Connect to the GC server IP address at the port 3268 (Connection -> Connect ...).
4. Bind with the MCM service account credentials (Connection -> Bind ...).
5. Download the AD structure tree (View -> Tree).
6. Navigate to the object of one of those just configured users.
7. Confirm that the object contains the properties:
  - msRTCSIP-UserEnabled and it is configured to TRUE
  - msRTCSIP-PrimaryUserAddress and it is configured with correct User
  - SIP URI
  - telephoneNumber or thefield configured on MCM and it is configured
  - with correct phone number

- msRTCSIP-OptionFlags
- msRTCSIP-Line
- msRTCSIP-LineServer

If some of those properties are not presented, or configured with old values, then the GC server is not replicated. The user must wait for the next automatic replication or run the replication manually.

If unsure that the replication is complete, or that the properties msRTCSIPUserEnabled and/or msRTCSIP-OptionFlags are not presented, go on to the next possible cause.

Possible cause 2: MCM Service credentials are not sufficient to view the msRTCSIP properties.

Solution 2: Check the access permissions for the AD object properties. Follow [How to manually check the access permissions to the AD object properties](#) on page 288 to check the access permission to the AD object properties.

### How to manually check the access permissions to the AD object properties

1. Install the OS Support Tools on the server (usually the Tools setup is on the MS Windows 2003 Server setup disk).
2. Run the ADSIEdit tool (%ProgramFiles%\Support Tools\adsiedit.msc).
3. Navigate to the users object container or the specific user's object.
4. Right-Click the item and open **Properties**.
5. Go to the **Security** tab and click the **Advanced** button.
6. Search for the permission entry specific for the msRTCSIP properties group or RTCTPropetySet. If there is a specific user group that has access rights to that property group, then the best solution is to add the MCM service account to this user group. Otherwise, you have to allow MCM Service account to read the properties msRTCSIP-UserEnabled, msRTCSIP-PrimaryUserAddress, msRTCSIPOptionFlags, msRTCSIP-Line, and msRTCSIP-LineServer.
7. Click **Add**.
8. Choose the MCM service account and click **OK**.
9. Go to the **Properties** tab.
10. Select **User objects** in the field **Apply onto**.
11. In the **Permissions** list box select the **Allow** check boxes across the Read permission of necessary properties and RTCTPropetySet.
12. Click **OK**.

Possible cause 3: The Active Directory field is not enabled for propagation to the Global Catalog.

Solution: Enable propagation of the Active Directory field to the Global Catalog. Be sure to specify a Domain Controller LDAP server (port 389) to reduce the search scope to only one domain.

## How to enable propagation of the Active Directory field to the Global Catalog

1. Open the Active Directory Schema snap-in.
2. Select the Attributes folder on the left pane.
3. Find and the right-click the necessary field (“otherTelephone”).
4. Click the **Property** menu item.
5. Enable “Replicate this attribute to the Global Catalog”.
6. Click **OK**.

---

## Case checklists

Use the following checklists prior to opening a case to ensure that all relevant information is collected:

**Table 20: Signaling Server information**

	Check
The patches list installed on the Signaling Server: pdt>mdp issp	
The configuration on the Signaling Server: <ul style="list-style-type: none"> <li>• pdt&gt;cd /u/config</li> <li>• pdt&gt;copy config.ini</li> </ul>	
Are you connected to the Signaling Server with Telnet and under pdt?  pdt>SIPCTIShow	

**Table 21: Call Server information**

	Check
Provide the patches list installed on the Call Server <ul style="list-style-type: none"> <li>• ld 22</li> <li>• issp</li> </ul>	
Capture the print out for the user DN in LD 11	
Capture the print out for the TN configured for this DN (do both for all TNs, including the PCA)	
Capture the DSC configuration for the PCA (configured for the Hot P 1)	

In LD 48, perform the command stat elan	
Provide the print out for the SIP Route and all related RLI/DMI	

**Table 22: NRS Configuration information**

	Check
NRS Configuration	
Print Capture of the Signaling Server endpoint Configuration	
Print Capture of the MCM endpoint configuration	
Print capture of the Routing Entries for the MCM endpoint	

**Table 23: MCM Configuration information**

	Check
Send the MCM.ini file	

**Table 24: LCS Configuration information**

	Check
The FQDN name of the Proxy server and the IP address	
The FQDN name of the Pool and his IP name	
The VIP of the Load Balancer	
On the Proxy Server capture Routing and for each route, Edit it and capture the screen	
On the Pool, capture Routing and for each route, Edit it and capture the screen	
On the Proxy Server, capture the screen Host Authorization	
On the Pool, capture the screen Host Authorization	
Home Server Properties -> General tab -> Mutual TLS/TLS row -> Edit	
Home Server Properties -> Security tab	
App Proxy Properties -> General tab -> Mutual TLS/TLS row -> Edit	
App Proxy Properties -> Security tab	

**Table 25: Active Directory Configuration information**

	Check
Print Capture of the LCS user for the General Tab	

Print Capture of the LCS user for the Live Communications	
Print Capture of the LCS user for the Live Communication--> Advanced Settings	

**Table 26: Tracing information**

	Check
An example AML trace on the Call Server (if it is a problem regarding the RCC feature not able to control the telephone)	
An example Signaling Server trace: SIPCallTrace (For problem related to SIP Gateway)	
An example Signaling Server trace: SIPCallTrace (For problem related to SIP Gateway)	
An example Signaling Server trace: SIPCTITrace (For problem related to SIP CTI)	
An example MCM.log with the log level = SIP + Debug for the failed call scenario (to reset the trace: put the trace level to none, delete the MCM.log file and put back the level to Debug)	
An example LCS trace on the LCS Proxy server. Configure the level to 4 and execute the Force Rollover Now to have a new trace file	
An example LCS trace on the LCS Home Server. Configure the level to 4 and execute the Force Rollover Now to have a new trace file	



# Appendix D: Abbreviations

<b>ACD</b>	Automatic Call Distribution
<b>AML</b>	Applications Module Link
<b>ATS</b>	Activity Tracking System
<b>AUX</b>	Auxiliary
<b>BRSC</b>	Basic Rate Signaling Concentrator
<b>CAST</b>	Customer Assurance and Serviceability Test
<b>CCMS</b>	Contact Center Manager Server
<b>CCR</b>	Customer Controlled Routing
<b>CDR</b>	Call Detail Recording
<b>CSTA</b>	Computer Supported Telecommunications Applications
<b>DRAM</b>	Dynamic Random Access Memory
<b>DN</b>	Directory Number
<b>DNIS</b>	Dialed Number Identification Services
<b>EMS</b>	Enterprise Multimedia Systems
<b>EPROM</b>	Erasable Programmable Read-Only Memory
<b>FS</b>	Feature Specification
<b>GNTS</b>	Global Network Technical Support
<b>MISP</b>	Multipurpose ISDN Signaling Processor
<b>MNM</b>	Meridian Network Management
<b>MSDL</b>	Multi-purpose Serial Data Link
<b>NCR</b>	Number of Call Registers
<b>P</b>	Pentium
<b>PRD</b>	Product Requirements Document

## Abbreviations

<b>SA</b>	StrongARM
<b>SISP</b>	Small System ISDN Signaling Processor
<b>TN</b>	Terminal Number
<b>VGMC</b>	Voice Gateway Media Card
<b>XPEC</b>	Expanded Peripheral Equipment Controller Pack

# Appendix E: Glossary

---

## TR/87 Front End/ECMA Front End

The front end application (FE) is the application that resides on the Signaling Server to provide TR/87 session support. The FE interfaces with the SIP GW to manage TR/87 sessions. The FE also issues and receives AML messages from the CS to service the TR/87 sessions.



## Index

---

### Special Characters

(PCA) .....[234](#)

