



Avaya Aura[®] Application Enablement
Services Implementation Guide for
Microsoft[®] Office Live Communications
Server 2005, Microsoft Office
Communications Server 2007, and
Microsoft Lync[®] Server 2010 and 2013

Release 6.3
June 2014
Issue 2

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the Avaya Support Web site: <http://www.avaya.com/support>

Licenses

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE <http://support.avaya.com/LicenseInfo/> ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). Customer may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicate with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated by Avaya provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). Customer may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User," means a user or device that has been expressly authorized by Avaya to access and

use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Product.

Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" for more information).

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and/or use 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 identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

<http://support.avaya.com/ThirdPartyLicense/>

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 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://www.avaya.com/support>

Trademarks

Avaya and Avaya Aura are registered trademarks of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: <http://www.avaya.com/support>

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 Support Web site:

<http://www.avaya.com/support>

Contents

Chapter 1: Introduction	11
Purpose.	11
Intended audience	11
Document changes since last issue	11
Resources	12
Documentation.	12
Training.	12
Avaya Mentor videos	13
Support.	14
Warranty	14
Chapter 2: Overview	15
Overview of the AE Services integration.	15
The AE Services provides seamless integration	15
Features of the AE Services implementation for Microsoft Office Communications Server	16
Features of the AE Services implementation for Microsoft Lync Server	17
What is TR/87?	18
What is SIP?	18
Features provided by AE Services	19
Integration with Microsoft Office Communicator	20
Microsoft Office Communicator 2007 feature-related changes.	21
A brief summary of Microsoft Office Communicator and Microsoft Live Communications Server	22
Making a simple phone call (LCS/OCS)	24
Setting up a dial plan	25
Integration with Microsoft Lync Server 2010 and Microsoft Lync Server 2013	27
A brief summary of Microsoft Lync Server	27
The Microsoft Lync Client.	27
Microsoft Lync Standard or Enterprise Server	27
Architectural Summary	27
Making a simple phone call (Lync)	28
Setting up a dial plan	29
Requirements for the AE Services integration	30
High Availability	34
AE Services System Platform High Availability Failover	34
The road map for integrating AE Services and Microsoft Office components	35
Phase 1: Setting up the Live Communications Server 2005 or the Office Communications Server 2007 environment	35
Phase 1 checklist: Live Communications Server	37

Phase 2: Setting up AE Services and Communication Manager	41
Phase 2 checklists: setting up AE Services and Communication Manager	42
Application Enablement Services on System Platform installation checklist	42
Bundled Server installation checklist	44
Software-Only server installation checklist	45
Phase 3: Integrating AE Services with Live Communications Server	46
Chapter 3: Integrating AE Services with Live Communications Server 2005	49
How to use the information in this chapter	49
Phase 3 Checklist --integrating AE Services with Live Communications Server .	49
About configuring AE Services for Live Communications Server	52
Enabling the TR/87 port	52
Administering Certificates -- certificate management.	53
Additional references	53
About the sample scenario	54
About obtaining certificates	54
Specifying key usage	54
Client and server authentication	55
Procedure 1 - Installing the trusted certificate on Live Communications Server	55
Installing the trusted certificate from another vendor.	55
Installing the trusted certificate generated by Microsoft Certificate Services	56
Importing the certificate into the Live Communications Server's trust store	57
Procedure 1a - Verifying the installation of the trusted certificate on Live Communications Server	58
Procedure 2 - Installing a server certificate for the Live Communications Server	59
Installing a server certificate from another vendor	59
Installing a Microsoft Certificate Services-based certificate on the Live Communications Server	60
Procedure 2a - Verifying the installation of the server certificate for Live Communications Server	62
Procedure 2b - Configuring the certificate for automatic routing	62
Procedure 3 - Installing the trusted certificate on the AE Server.	63
Generic procedure for installing the trusted certificate for AE Services .	64
Microsoft-based procedure for installing a trusted certificate chain. . . .	65
Importing the trusted certificate into the AE Services Management Console	66
Procedure 3a - Verifying the installation of the trusted certificate in AE Services	66
Converting Certificate files in other formats for AE Services	67

Procedure 4 - Creating a server certificate request for AE Services	67
Procedure 5 - Creating a server certificate for AE Services	69
Generic procedure for creating a server certificate for AE Services	69
Microsoft-based procedure for creating a server certificate for AE Services	70
Procedure 6 - Importing the server certificate into AE Services	71
Procedure 6a - Verifying the installation of the server certificate in AE Services	72
Replacing an expired server certificate	72
Dial Plan settings in AE Services	73
Before you begin.	73
About Tel URI formats and device IDs	74
About the From TelURI and To TelURI rules	75
TelURI settings - how incoming and outgoing numbers are processed	76
Pattern matching -- using Pattern and RegEx (regular expressions) . . .	76
Valid dial string characters and using the asterisk	77
The From Tel URI table	78
The To TelURI table	78
From TelURI settings for fixed-length extensions	79
To TelURI settings for fixed-length extensions	81
From TelURI settings for variable-length extensions	82
To TelURI settings for variable length extensions.	84
Pattern matching -- using Pattern and RegEx (regular expressions) . . .	85
Dial Plan tips	87
Administering dial plan settings on a per-switch basis.	87
Administering default dial plan settings	89
Administering AE Services access to Active Directory	90
DN entries and scope of search	92
Avoid making the Base Search DN too specific	92
Making changes on the Enterprise Directory Configuration page	93
Determining the DN for a user object.	93
Configuring Live Communications Server for AE Services	94
Enabling Remote Call Control in Active Directory	95
Setting up connections	96
Configuring a static route	97
Specifying the AE Server as an authorized host	98
Microsoft Office Communicator users - group policy settings	99
About authentication and authorization	99
Administering Live Communications Server 2005 for the agent login ID	100
Re-synchronizing states	100

Contents

Using the TR/87 Test features.	101
The Host AA setting and TR/87 test	101
Usage Tips for the Do Not Disturb feature	102
Recovering from a system outage	102
Known issues	103
Setting up forwarding off-switch	103
Using Call Forwarding and Send All Calls	104
Using the Do Not Disturb feature	104
Putting the active call on hold before starting a new call.	104
Clear Connection request on a held connection is not supported.	104
Bridging irregularities	105
Missed Call e-mail	105
Usage instructions for analog phones	106
Unidentified caller in Microsoft Office Communicator window.	107
Communicator displays numbers with trunk notation	108
Chapter 4: Integrating AE Services with Communications Server 2007.	109
How to use the information in this chapter	109
Phase 3 Checklist --integrating AE Services with Microsoft Office Communications Server 2007	109
About configuring AE Services for Microsoft Office Communications Server 2007	112
Enabling the TR/87 port	113
Administering Certificates -- certificate management.	114
Additional references	114
About the sample scenario	115
About obtaining certificates	115
Specifying key usage	115
Client and server authentication	116
Procedure 1 - Installing the trusted certificate on Office Communications Server 2007	116
Installing the trusted certificate from another vendor.	116
Installing the trusted certificate generated by Microsoft Certificate Services	117
Importing the certificate into the Microsoft Office Communications Server 2007 trust store	118
Procedure 1a - Verifying the installation of the trusted certificate on Office Communications Server	119
Procedure 2 - Installing a server certificate for the Office Communications Server	120
Installing a server certificate from another vendor	120
Installing a Microsoft Certificate Services-based certificate on the Microsoft Office	

Communications Server 2007	121
Procedure 2a - Verifying the installation of the server certificate for Microsoft Office Communications Server 2007	122
Procedure 2b - Configuring the certificate for automatic routing	123
Procedure 3 - Installing the trusted certificate on the AE Server.	124
Generic procedure for installing the trusted certificate for AE Services	124
Microsoft-based procedure for installing a trusted certificate chain.	125
Importing the trusted certificate into the AE Services Management Console	126
Procedure 3a - Verifying the installation of the trusted certificate in AE Services	127
Converting Certificate files in other formats for AE Services	127
Procedure 4 - Creating a server certificate request for AE Services	128
Procedure 5 - Creating a server certificate for AE Services	129
Generic procedure for creating a server certificate for AE Services	129
Microsoft-based procedure for creating a server certificate for AE Services	130
Procedure 6 - Importing the server certificate into AE Services	131
Procedure 6a - Verifying the installation of the server certificate in AE Services	132
Replacing an expired server certificate	132
Dial Plan settings in AE Services	133
Before you begin.	133
About Tel URI formats and device IDs	134
About the From TelURI and To TelURI rules	135
TelURI settings - how incoming and outgoing numbers are processed	136
Pattern matching -- using Pattern and RegEx (regular expressions)	136
Valid dial string characters and using the asterisk	137
The From Tel URI table	138
The To TelURI table	138
From TelURI settings for fixed-length extensions	139
To TelURI settings for fixed-length extensions	141
From TelURI settings for variable-length extensions	142
To TelURI settings for variable length extensions.	144
Pattern matching -- using Pattern and RegEx (regular expressions)	145
Dial Plan tips	146
Administering dial plan settings on a per-switch basis.	147
Administering default dial plan settings	148
Administering AE Services access to Active Directory.	150
DN entries and scope of search	152
Avoid making the Base Search DN too specific	152
Making changes on the Enterprise Directory Configuration page	153

Determining the DN for a user object.	153
Configuring Microsoft Office Communications Server 2007 for AE Services . . .	154
Enabling Remote Call Control in Active Directory	155
Setting up connections	157
Configuring a static route	157
Specifying the AE Server as an authorized host	158
Microsoft Office Communicator users - group policy settings.	159
About authentication and authorization	159
Using the TR/87 Test features.	160
The Host AA setting and TR/87 test	160
Administering Microsoft Office Communications Server 2007 for the agent login ID	161
Re-synchronizing states	161
Usage Tips for the Do Not Disturb feature	162
Recovering from a system outage	162
Known issues	163
Setting up forwarding off-switch	163
Using Call Forwarding and Send All Calls	163
Using the Do Not Disturb feature	164
Putting the active call on hold before starting a new call.	164
Clear Connection request on a held connection is not supported.	164
Bridging irregularities	165
Missed Call e-mail	165
Usage instructions for analog phones	165
Unidentified caller in Microsoft Office Communicator window.	166
Communicator displays numbers with trunk notation	167
Chapter 5: Integrating AE Services with Microsoft Lync Server 2010 and 2013. . . .	169
How to use the information in this chapter	169
Phase 1: Install and Configure Lync Server 2010 and Lync Server 2013	169
Documentation for Microsoft Lync Server 2010	170
Documentation for Microsoft Lync Server 2013	170
Phase 2: Setting up AE Services and Communication Manager	171
Phase 3: Integrating Application Enablement Services with Microsoft Lync Server	171
Installing the trusted certificate on Microsoft Lync Server	172
Creating a custom Certificate Template	172
Installing or re-installing certificates on the Microsoft Lync Server	173
Installing the trusted certificate on the AE Server.	174
Microsoft-based procedure for installing a trusted certificate chain.	174
Importing the trusted certificate into the AE Services Management Console. . . .	175

Verifying the installation of the trusted certificate in AE Services	175
Administering AE Services access to Active Directory.	176
Configuring Remote Call Control (RCC)	178
Enable users for RCC	181
Recommendations for Active Directory and Lync User related Administration. .	182
Using the TR/87 Test Features	184
The Host AA settings and TR/87 Test	184
Administering Lync Server for the Agent Login ID	185
Re-synchronizing States	185
Recovering from a system outage	186
Other AE Services Administration	186
Configuring Enterprise Directory Settings with Bridged Appearance Alert Blocking	186
Administering Auto Hold configuration	187
Known Issues - Lync 2013 Client	187
The cumulative update(CU) 2880474 package for Lync 2013.	188
Transferring a Call - Lync 2013 Client	188
Conferencing a call	188
Redirecting a Call from the Lync 2013 Client	188
Known Issues - Other	188
Setting up Forwarding Off-Switch	189
Using Call Forwarding and Send All Calls	189
Clear Connection request on a held connection is not supported.	189
Bridging irregularities	190
Unidentified Caller in Lync window	190
Communicator displays numbers with trunk notation	190
Appendix A: SIP requests and associated errors	193
Appendix B: AE Services Implementation for Microsoft LCS call flow	195
Message flow.	195
Appendix C: Capacities	199
Appendix D: Creating a certificate template for Server Certificates on the Microsoft CA Server	201
Creating a certificate template for Server Certificates on the Microsoft CA Server	202
Appendix E: Instructions for generating version 3 certificates	205
Creating Version 3 (Windows Server 2008) Certificate Templates for Server Certificates	205
Requesting and installing the server certificate.	212

Contents

Installing a Microsoft Certificate Services-based certificate on the Microsoft LCS 2005 or OCS 2007	218
Index	219

Chapter 1: Introduction

Purpose

This document describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.

Intended audience

This document is intended for people who want to gain a high-level understanding of the product features, functions, capacities, and limitations.

Document changes since last issue

The following changes have been made to this document since the last issue:

- Updated the values of host name, base search, and post number in [Administering AE Services access to Active Directory](#) on page 90.
- Updated the [License Consumption](#) on page 199.

Resources

Documentation

The following table lists the related documents for Avaya Aura® Application Enablement Services. Most of the documents listed are Release 6.3.3. Those listed that are for earlier releases have not required an update and remain compatible with AE Services 6.3.3 Obtain the related documents and documents about other Avaya products mentioned in this guide from the Avaya Support website: Avaya support site.

For information about setting up AE Services, Release 6.3.3, see the following documents.

- *Implementing Avaya AuraR Application Enablement Services for Avaya AuraR System Platform, 02-603468*
- *Implementing Avaya AuraR Application Enablement Services for a Bundled Server, 02-300356*
- *Implementing Avaya AuraR Application Enablement Services in a Software-Only Environment, 02-300355*
- *Avaya AuraR Application Enablement Services using VMwareR in the Avaya AuraR Virtualized Environment Deployment Guide*
- *Avaya AuraR Application Enablement Services Administration and Maintenance Guide, 02-300357*
- *Avaya AuraR Application Enablement Services Management Console online help (which is included with the AE Services server software)*
- *Administering Meeting Exchange. Applications, 04-603544*
- *White Paper on Avaya AuraR Application Enablement Services Integration for IBMR*
- *LotusR SametimeR Guidelines for a clustered environment*

AE Services documents are available from the Web in Portable Document Format (.pdf) at the Avaya Support Web Site (<http://www.avaya.com/support>).

Training

The following courses are available on <https://www.avaya-learning.com>. To search for the course, in the **Search** field, enter the course code and click **Go**.

Course code	Course title
ATI02595AEN	Application Enablement Services Implementation and Administration (Assessment)
AVA00962WEN	Application Enablement Services 4.0 Overview
1U00223O	Avaya Aura Application Enablement Services (AES) 6.2 - L2
1U00222O	Avaya Aura Application Enablement Services (AES) 6.2 - L1
3U00127O	Designing Avaya Aura Application Enablement Services (AES) - Technical Sales L1
10U00030E	Knowledge Access: AIPS - Avaya Aura Application Enablement Services Implementation
4100	Avaya Aura(R) Application Enablement Services Implementation Test
9Z04481V	Application Enablement Services

Avaya Mentor videos

Avaya Mentor videos are available to provide technical content on how to install, configure, and troubleshoot Avaya products.

Videos are available on the Avaya support site, listed under the video document type, and on the Avaya-run channel on YouTube.

To find videos on the Avaya support site, select the product name, and check the videos checkbox to see a list of available videos.

Note:

Videos are not available for all products.

To find the Avaya Mentor videos on YouTube, go to <http://www.youtube.com/AvayaMentor> and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Support

Visit the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at [http:// support.avaya.com/](http://support.avaya.com/) under **Help & Policies > Policies & Legal > Warranty & Product Lifecycle**. See also **Help & Policies > Policies & Legal > License Terms**.

Chapter 2: Overview

Overview of the AE Services integration

The AE Services integration with Microsoft Office Live Communications Server 2005, Microsoft Office Communications Server 2007, Microsoft Lync Server 2010, and Microsoft Lync Server 2013 provides a solution for controlling your Avaya telephone or IP softphone using Microsoft Office Communicator or Microsoft Lync. The AE Services integration enables users to operate more efficiently by launching and answering phone calls from the Microsoft Office Communicator or Microsoft Lync. As a result, people, teams, and organizations are able to communicate simply and effectively while working with Avaya and Microsoft applications.

Note:

Throughout this document the term Microsoft Office Communications Server 2007 is used in the inclusive sense. It refers to Microsoft Office Communications Server 2007 and Microsoft Office Communications Server 2007 R2.

Note the following information:

- Beginning with AE Services 4.2.2, AE Services supports Microsoft OCS 2007 R2.
- Beginning with AE Services 4.2.1 Patch 2 and 4.2.2, AE Services supports SIP UPDATE message with Microsoft OCS 2007 R2 integrations.
- Beginning with AE Services 5.2, Microsoft OCS 2007 R2 uses the SIP UPDATE message rather than REINVITE to refresh its sessions with AE Services. If the session is not refreshed in 30 minutes, the session will expire.

The AE Services provides seamless integration

AE Services integrates seamlessly with Microsoft Office Communicator to provide voice capabilities combined with presence awareness. As a result, you can take advantage of features such as:

- "Click to call" - make your instant message an instant call
- Forwarding calls - by forwarding your calls to another number you never have to miss a call
- Displaying an alert - when someone calls you can decide how to handle the call

For a more complete list of features, see [Features provided by AE Services](#) on page 19.

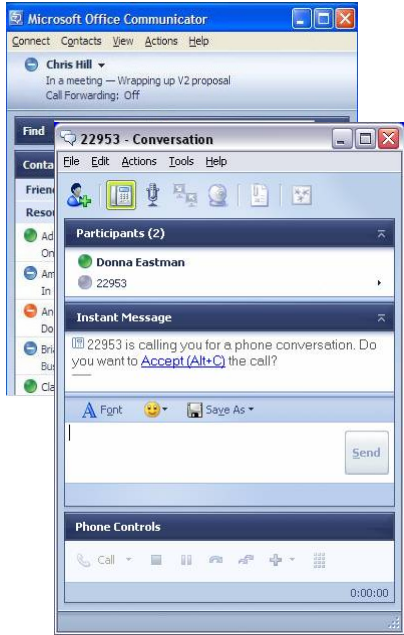
Features of the AE Services implementation for Microsoft Office Communications Server

With the AE Services and Microsoft Office Communications Server integration you have the simplicity and convenience of instant messaging (IM) combined with the power of the enterprise telephone network. The following features provide you with a rich set of communications capabilities:

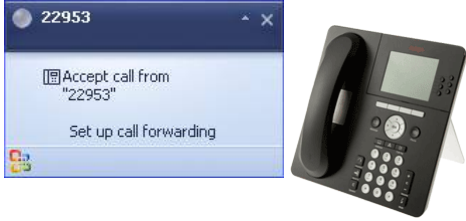
- Easily locate and contact people using corporate directories, Microsoft Outlook contacts, or your buddy list.
- Click-to-call - With click-to-call you can communicate seamlessly with others in different locations or time zones, using voice or instant messaging.
 - You can easily escalate an instant message to a call or a conference.
 - Your presence is shared.
 - Your phone and Microsoft Office Communicator stay in sync.
 - You have access to call control features such as Hold, Transfer, Call forwarding, and so on.
- View rich information about your contacts' availability - details about their schedule, or even their 'out of office' message - through integration with Microsoft Office Outlook and Microsoft Exchange Server.
- Tag key contacts so you can know when they become available for a phone call or IM session.

Figure 1: AE Services - as seen from Microsoft Office Communicator

Avaya brings enterprise telephony to Microsoft Office Communicator



- Communicator is on a PC
-- Corporate IM driven
- Avaya Provides the telephony connection
- You can use Click-to-Call in Microsoft Office Communicator
 - You can escalate an instant message to a call or a conference
 - Your phone and Microsoft Office Communicator stay in sync
 - Presence is shared
 - You have access to call control - Hold, Transfer, Call forwarding and so on
- The solution is endpoint-neutral
- No Avaya software is installed on the Microsoft Office Communicator client



Features of the AE Services implementation for Microsoft Lync Server

With the AE Services and Microsoft Lync Server integration you have the simplicity and convenience of instant messaging (IM) combined with the power of the enterprise telephone network. The following features provide you with a rich set of communications capabilities:

- Easily locate and contact people using corporate directories, Microsoft Outlook contacts, or your buddy list
- Click-to-call - With click-to-call, you can communicate seamlessly with others in different locations or time zones, using voice or instant messaging.
 - You can easily escalate an instant message to a call.
 - Your presence is shared.
 - Your phone and Microsoft Lync stay synchronized together.
 - You have access to call control features such as Hold, Transfer, Call forwarding, and so on.
- View rich information about your contacts' availability - details about their schedule, or even their 'out of office' message - through integration with Microsoft Office Outlook and Microsoft Exchange Server.

You can perform nearly all the same operations with Microsoft Lync that you could with OCS 2007 R2. However, the interface has changed.

Note:

When a Microsoft Lync 2013 user transfers a call to another device, the call is transferred. However, the transferred party has two conversation windows displayed. The transferred party cannot terminate the call by closing the conversation windows. The transferred party must terminate the call from the physical device.

What is TR/87?

TR/87 refers to the ECMA Technical Report, ECMA TR/87, which describes how CSTA can be used to provide CSTA call control functionality for SIP user agents. TR/87 is the means by which AE Services integrates with Microsoft Office products to provide the functionality described in [Features provided by AE Services](#).

What is SIP?

The Session Initiation Protocol (SIP) is a control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences. The current SIP specification only covers first party call control functionality.

In more familiar terms, SIP means real-time communication, presence, and collaboration in a variety of forms including voice, video, or instant text messaging.

Features provided by AE Services

The AE Services integration with Microsoft Office Communicator provides the following features:

- Call notification
- Call Control
 - Click to Dial - call someone by clicking name in the Contacts list or by entering their number in the Find box
 - Hold
 - Disconnect
 - Multiple Line Appearance
- Integrated call status (Microsoft Feature)
- Call Transfer
 - Unannounced (blind transfer)
 - Announced (consultative transfer)
- Conference (up to 6 parties)
- Call forwarding
- Do Not Disturb (send all calls)
- Integration with Microsoft Outlook (Contacts, Calendar, Out of Office, call handling notification email, and so forth -- all Microsoft-specific features).

About using analog phones

You must follow special usage instructions for analog phones. For more information, see [Usage instructions for analog phones](#) on page 106.

Integration with Microsoft Office Communicator

Avaya Aura® Application Enablement Services (AE Services) enables a wide variety of desktop telephony features for enterprise users through the Microsoft Office Communicator client. These features can improve the efficiency and productivity of the enterprise worker by eliminating the manual aspect of dialing numbers and by driving all their communication operations to a single desktop interface (such as Office Communicator client). The following list describes the telephony capabilities that were initially provided in AE Services R 4.0.

- Presence Status: On/Off Hook status integrated on Microsoft Office Communicator IM client
- Incoming Call Notification
- Incoming Call Answer
- Click-to-Call
- Call Hold
- Call Disconnect
- Call Transfer (blind transfer)
- Call Transfer (consultative transfer)
- Call Conference (up to 6 parties). See [Microsoft Office Communicator 2007 feature-related changes](#).
- Call Forwarding. See [Microsoft Office Communicator 2007 feature-related changes](#)
- Do Not Disturb (also referred to as Send All Calls or SAC). See [Microsoft Office Communicator 2007 feature-related changes](#)
- Integration with Microsoft Outlook (Contacts, Calendar, Out of Office, call handling notification email, and so forth -- all Microsoft-specific features).



Important:

You must follow special usage instructions for analog phones. For more information, see [Usage instructions for analog phones](#) on page 106.

Microsoft Office Communicator 2007 feature-related changes

With Microsoft Office Communicator 2007 the following features are no longer exposed to AE Services through the Remote Call Control (RCC) integration. As a result, they are not available in the AE Services Microsoft Office Communicator 2007 integration.

- Call Conferencing
- Do Not Disturb (also referred to as Send All Calls or SAC)

Additionally, with Microsoft Office Communicator 2007, aspects of the following feature are no longer exposed to AE Services via RCC (Remote Call Control) integration. Thus, the feature is not as rich in the AE Services-LCS 2005 integration:

- Call Forwarding – unconditional forwarding remains supported.
- Location-based forwarding, however, is not supported.

For example, the following scenario is no longer supported: for PC X (e.g. home PC) forward my calls to phone number A, but for PC Y (e.g. work PC) do not forward.

All other operations are fully supported as they were with Microsoft Office Communicator 2005.

A brief summary of Microsoft Office Communicator and Microsoft Live Communications Server

If the Microsoft Live Communications Server environment is new to you, use this section to familiarize yourself with a few terms and concepts.

Microsoft Office Communicator 2005 or Microsoft Office Communicator 2007 (Communicator)

Communicator is a presence-enabling communications client, that provides enterprise users with real-time communication in a variety of forms such as text, audio, and video. Communicator provides instant messaging, voice over IP, and the ability to control a physical phone set from your PC.

With Communicator, users can initiate a new conference from Microsoft Outlook®, create unplanned conferences with multiple modes depending on the capabilities of the CSP (conference service provider), escalate an audio call into a Live Meeting session, or escalate a multiparty IM conversation to a multiparty PSTN conference.

Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007

Both products, Microsoft Live Communications Server 2005 and Microsoft Office Communications Server 2007 enable instant messaging (IM), live collaboration, SIP telephony, and integration with telephony systems. Both products are offered in a standard and an enterprise edition:

Standard Edition: is geared toward smaller, simpler network configurations. It supports up to 20,000 users. Live Communications Server 2005 Standard Edition is a standalone server -- it operates without an external SQL Server.

Enterprise Edition: is designed for larger, more complex networks. It supports installations with up to 125,000 users. It requires an external database.

Active Directory

The Microsoft Live Communications Server 2005 and the Microsoft Office Communications Server 2007 rely on Active Directory Services for authenticating, authorizing, provisioning, and configuring Live Communications Server.

Microsoft Exchange Server

Communicator 2005 and Address Book Service are designed to integrate with the Exchange and Outlook environment to an even greater degree of presence. Communicator 2005 can work without Exchange. With Exchange, users can include scheduling and calendar information with their presence status.

Remote Call Control Gateway

AE Services performs the role Remote Call Control Gateway or RCC Gateway.

Communicator 2005 and Communicator 2007 use a standards based CTI protocol, and AE Services converts the protocol used by Communicator 2005 to the CTI protocol supported by Avaya Communication Manager.

Note:

The AE Services implementation for Microsoft Office Communication Server is not a SIP proxy (a server that processes and forwards SIP requests between calling and called parties). AE Services acts as a Remote Call Control Gateway.

Quick Search

The search facility in Communicator 2005 and Communicator 2007 saves time and improves efficiency. Communicator does this by storing a local address database on the client instead of retrieving it from a network server. As a result, search queries are much faster.

Address Book and Contacts in Communicator

The Address Book Service has a dual role:

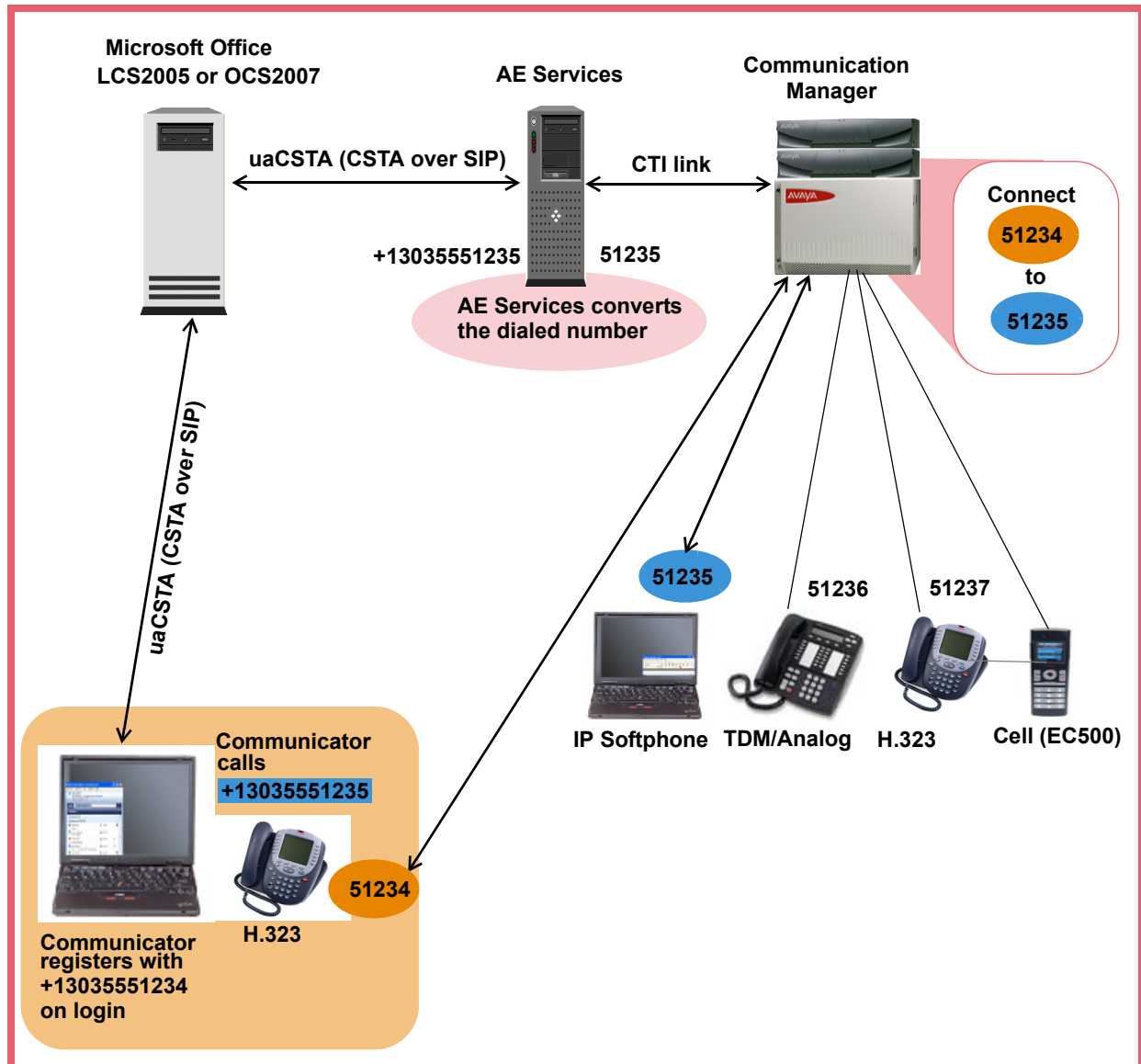
- Its primary role is to provide Global Address List updates to the Communicator 2005 or Communicator 2007 client. It performs this function daily.
- Additionally, it can be configured to normalize phone numbers for the Communicator 2005 or Communicator 2007. For more information, see [Set up Address Book Service](#) on page 40.

Making a simple phone call (LCS/OCS)

The following figure illustrates a simple call path (using MakeCall) from Communicator to an H.323 endpoint. While Communicator is shown in this diagram as controlling an H.323 telephone, it is also capable of controlling IP Softphone, a digital phone or an analog phone.

Note:

Analog phones require special usage instructions, see [Usage instructions for analog phones](#) on page 106.



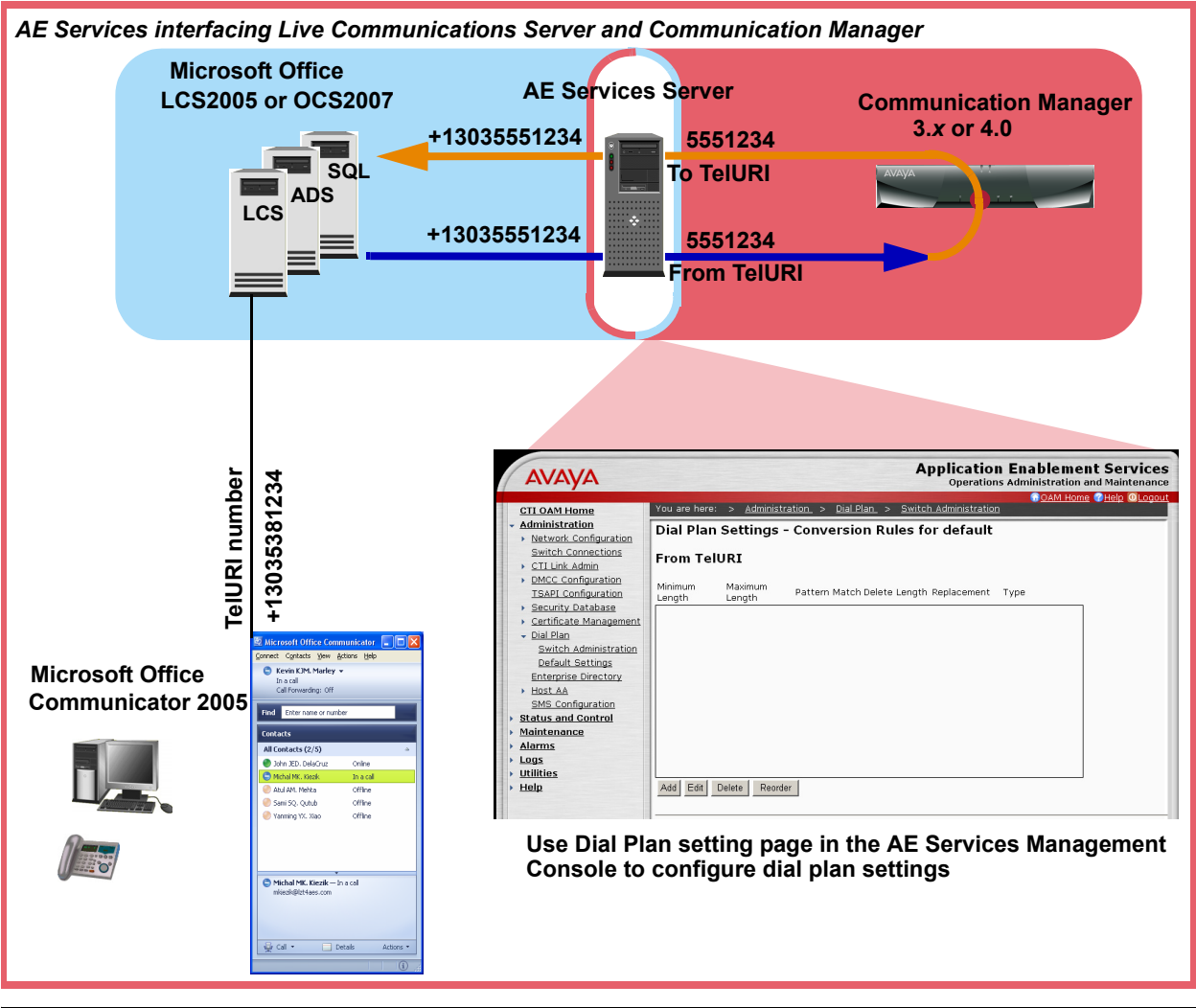
Setting up a dial plan

Refer to [Figure 2](#) as you read through this high level description of setting up a dial plan.

In terms of its basic functionality, the AE Services implementation for Microsoft Office Live Communications Server or Microsoft Office Communications Server 2007 acts as a SIP to CSTA III gateway. In simplest terms, the interactions between Communicator, AE Services and Communication Manager are as follows:

- Communicator passes phone numbers in TelURI format to AE Services.
- Based on Dial Plan settings, AE Services converts them **from TelURI** format (+13035551234) **to an extension** (such as 5381234), and passes them to Communication Manager.
- Communication Manager, in turn, passes the extension back to AE Services. Based on Dial Plan settings in the Application Enablement Services Management Console (AE Services Management Console) AE Services converts extensions **to TelURI** format and passes them back to Communicator.
- Specific Avaya SIP endpoints can be controlled if your configuration relies on AE Services 4.1 or later, and Communication Manager 5.0. AE Services 4.1, or later, supports SIP enabled endpoints (Avaya 16CC and 9620, 9630, 9630G, 9640, and 9640G SIP endpoints with firmware version 2). The requirements for SIP support are as follows:
 - Communication Manager 5.0, or later
 - SIP Enablement Services (SES) 5

Figure 2: AE Services implementation for Microsoft Office Communications server - dial plan



Integration with Microsoft Lync Server 2010 and Microsoft Lync Server 2013

A brief summary of Microsoft Lync Server

If the Microsoft Lync Server environment is new to you, use this section to familiarize yourself with a few terms and concepts.

The Microsoft Lync Client

The Lync client provides users with access to the features and capabilities of the Microsoft Lync environment. AE Services supports:

- Microsoft Lync Client 2010
- Microsoft Lync Client 2013 (version 15.0.4517.1504 or later). This is the full-featured client. (Lync 2013 Basic does not support Remote Call Control.)

Microsoft Lync Standard or Enterprise Server

Microsoft Lync is Microsoft's next generation feature rich Unified Communication Server. Microsoft Lync, like Microsoft Live Communications Server 2005 and Microsoft Office Communications Server 2007, enables instant messaging (IM), live collaboration, SIP telephony, and integration with telephony systems. Lync provides an enhanced topology builder feature, a central management store and many other changes, features and improvements over previous communications server offerings. Microsoft Lync 2010 and Microsoft Lync 2013 are offered in a standard and an enterprise edition that both run only on 64 bit Windows 2008 R2 Server.

Architectural Summary

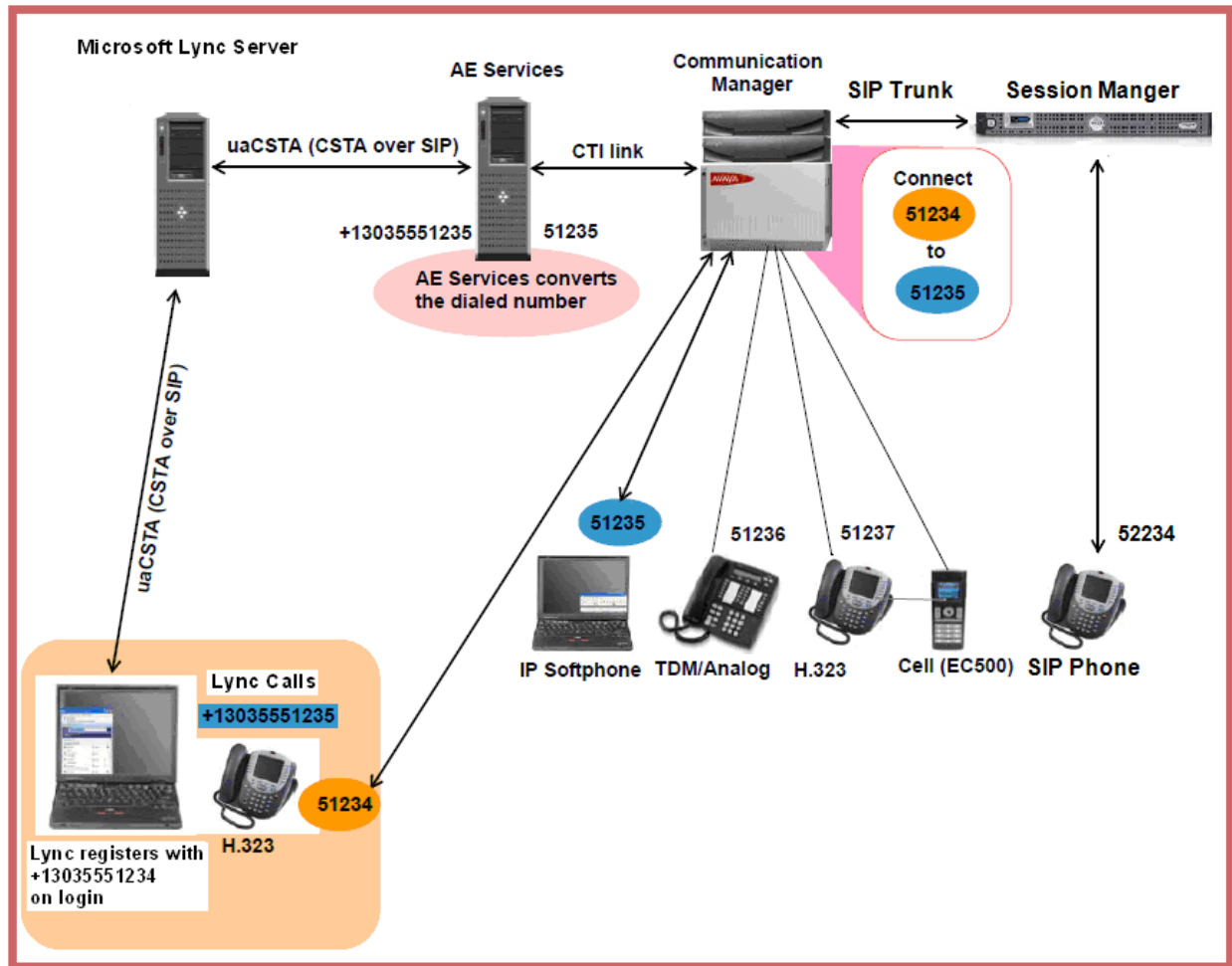
The AE Services Integration with Microsoft Lync makes use of AE Services DMCC over TR/87 Application support. TR/87 refers to the ECMA Technical Report, ECMA TR/87, which describes how Computer Supported Telecommunications Applications (CSTA) can be used to provide CSTA call control functionality for SIP user agents. TR/87 is the means by which AE Services Communicates with the Microsoft Lync Server for 3rd Party Call Control of Communication Manager PBX Stations. AE Services acts as a SIP to CSTA III Gateway. AE Services exchanges control and status messages with Avaya Aura Communication Manager over a Telephony Server Application Programming Interface (TSAPI) Link.

Making a simple phone call (Lync)

The following figure illustrates a simple call path (using MakeCall) from Lync to an H.323 endpoint. While Lync is shown in this diagram as controlling an H.323 telephone, it is also capable of controlling IP Softphone, a digital phone or an analog phone. Lync can also control specific Avaya SIP endpoints.

Note:

Analog phones require special usage instructions. See [Usage instructions for analog phones](#) on page 165.



Setting up a dial plan

Refer to the figure on the previous page as you read through this high-level description of setting up a dial plan. In terms of basic functionality, the AE Services implementation for Microsoft Lync Server 2010 and Microsoft Lync Server 2013 acts as a SIP to CSTA III gateway. In simplest terms, the interactions between Lync, AE Services, and Avaya Communication Manager are as follows:

- Lync passes phone numbers in TelURI format to AE Services.
- Based on Dial Plan settings, AE Services converts them **from TelURI** format (for example, +13035551234) **to an extension** (such as 5551234) and passes them to Avaya Communication Manager.
- Avaya Communication Manager, in turn, passes the extension back to AE Services. Based on the Dial Plan settings in the AE Services Management Console, AE Services converts extensions **to TelURI** format and passes them back to Lync.
- Specific Avaya SIP endpoints can be controlled if your configuration relies on AE Services 4.1 or later and Avaya Communication Manager 5.0. See the AE Services release notes for the list of supported SIP endpoints and firmware.

SIP support requires:

- Avaya Communication Manager 5.0 or later
- SIP Enablement Services (SES) 5.

Requirements for the AE Services integration

The requirements for integration are as follows:

Live Communications Server 2005 or Office Communications Server 2007:

- All required servers must be joined to the domain and able to resolve each other's fully qualified domain names (FQDN). Microsoft Office Communicator clients must be able to communicate with each other.
- Microsoft Office Live Communications Server 2005 Address Book Service must be configured and deployed for an AE Services and Live Communications Server integration. The Address Book Service provides Microsoft Office Communicator users with a local cache of the global address list. This enables Communicator users to quickly search the global list using the Find feature. Optionally, you can set up Address Book to provide phone number normalization. For more information see, [Set up Address Book Service](#) on page 40.

Note:

AE Services supports a connection to only one Microsoft Office Communications Server (which can be any of the following: Live Communications Server 2005 Standard Edition Server, Live Communications Server 2005 Enterprise Pool, Office Communications Server 2007 Standard Edition Server, or Office Communications Server 2007 Enterprise Pool). For an illustration of sample configurations, see [Figure 4: Configuring AE Services with 20,000 or more concurrent users](#) on page 33).

A certificate authority (CA): The CA can be either Microsoft Certificate Services or a third party CA. The Live Communications Server must trust the certificate authority and have its own certificate installed.

Microsoft LCS and OCS integrations that use a server pool and load balancers require a Microsoft 2003 or 2008 Enterprise Edition CA or non-Microsoft CAs, for example, Verisign.

Note:

Windows 2003 or 2008 Server Standard Edition comes with a Standard Edition CA. However, Microsoft Standard Edition CAs are not supported. The Enterprise Edition CA is only included in Windows 2003 or 2008 Server Enterprise Edition and non-Microsoft CAs, for example, Verisign.

Avaya Communication Manager 3.0 or later: The Link Bounce Resiliency feature (available in Communication Manager 3.1 and later) is strongly recommended. Communication Manager 4.0 is required for any installation with more than 21,000 concurrent Microsoft Office Communicator 2005 (Communicator 2005) users or Office Communicator 2007 users



Important:

The latest Communication Manager patches are required.

Avaya Communication Manager 6.3 or later:**Important:**

ASAI requires the signaling groups between Communication Manager and Session Manager to use TLS.

AE Services Server 4.1 or later: AE Services supports an AE Server configured as an AE Services implementation for Microsoft Live Communications Server 2005 (or Office Communications Server 2007) and another application (such as a TSAPI-, JTAPI-, DLG-, CVLAN-, or DMCC-based application), subject to performance constraints.

A single AE Server can support up to 16 Communication Manager servers (switches) for an AE Services implementation for Microsoft LCS 2005 or OCS 2007 (see [Figure 3: Maximum number of Communication Manager servers supported by AE Services](#) on page 32).

An AE Services administrative workstation: The AE Services Bundled Server does not provide a Web browser, and the AE Services Software Only solution does not assume that you will install one. To administer AE Services, you need an administrative workstation -- a computer running a browser with network access to the AE Server.

Unified Desktop License: When you install AE Services and activate the "Unified CC API - Desktop Edition" license, the AE Server is TR/87-enabled. You do not have to install any special software. This is a per-user license. Every active Microsoft Office Communicator client consumes one Unified Desktop license for the duration of the period that it has an active dialog with Application Enablement Services.

Note:

The certificates distributed by the AE Services license file do not work in the Live Communications Server environment, and the AE Services administrator must configure certificates. For more information, see [Administering Certificates -- certificate management](#) on page 53.

SIP Requirements : Specific Avaya SIP endpoints can be controlled if your configuration relies on AE Services 4.1, or later, and Communication Manager 5.0. AE Services 4.1, or later, supports SIP enabled endpoints (Avaya 16CC and 9620, 9630, 9630G, 9640, and 9640G SIP endpoints with firmware version 2). The requirements for SIP support are as follows:

- Communication Manager 5.0, or later
- One of the following SIP servers:
 - SIP Enablement Services (SES) 5
 - Avaya Session Manager 6.0 or later

Figure 3: Maximum number of Communication Manager servers supported by AE Services

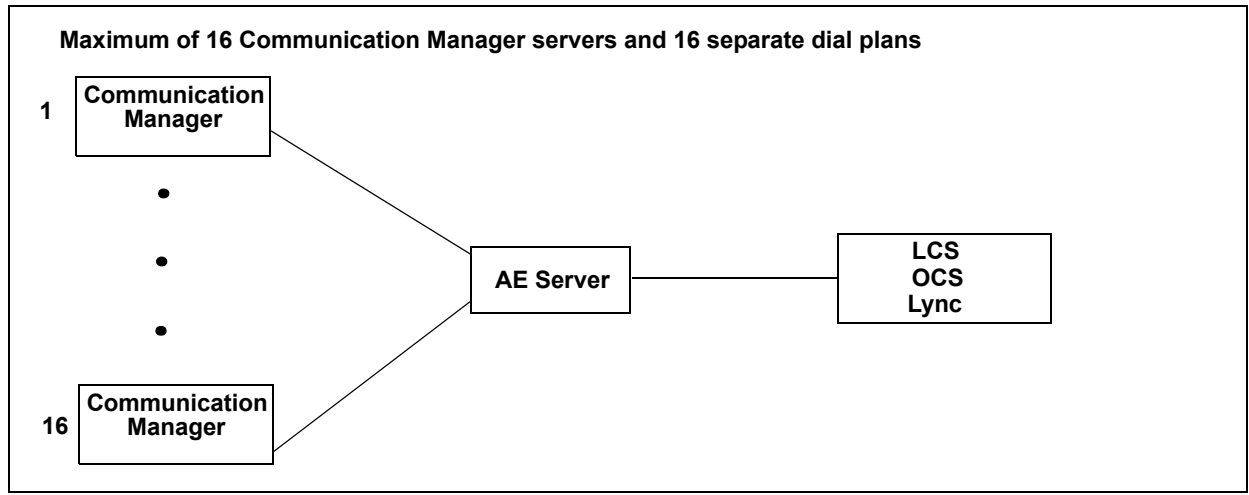
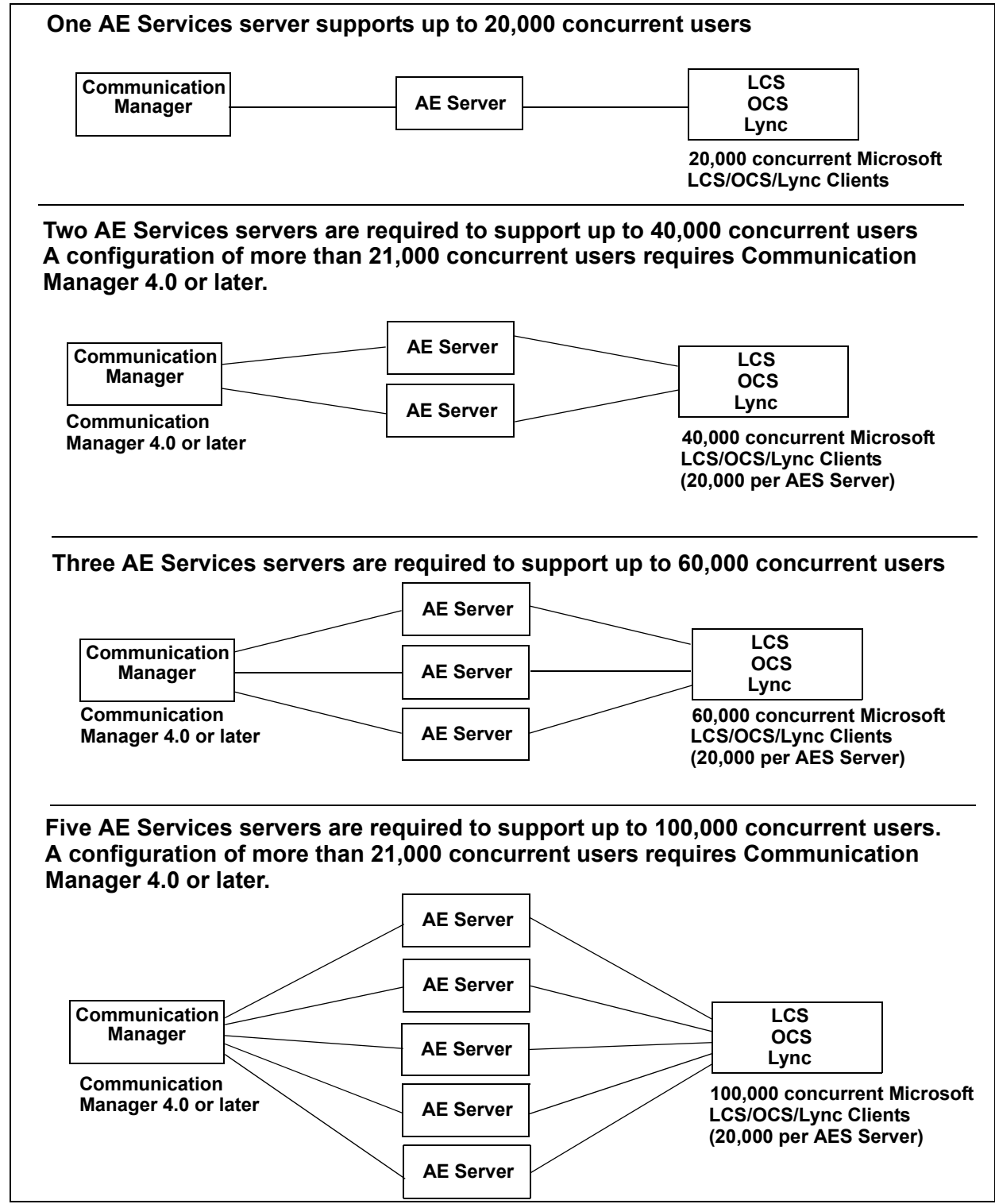


Figure 4: Configuring AE Services with 20,000 or more concurrent users

High Availability

While AE Services does not support an automatic failover to a backup server for the AE Services 6.3.3 Bundled Server and Software Only offers, it is possible to deploy AE Services in a high availability configuration with only a small amount of manual intervention to move to and from a backup server. It is possible to have active pairs, standby pairs, or an N+1 redundancy configuration.

For active, standby, or N+1 redundancy configurations, follow these guidelines:

- Configure the backup AE Server (or servers) with the same dial plan as the active AE Server (or servers).
- On the Microsoft Office Server (Live Communications Server 2005 Standard Edition Server, Live Communications Server 2005 Enterprise Pool, Office Communications Server 2007 Standard Edition Server, or Office Communications Server 2007 Enterprise Pool) administer static routes for all active AE Servers only.
- On Microsoft Office Live Communications Server, Office Communications Server, and Office Communications Server R2, specify each standby AE Server as an authorized host on the Host Authorization tab. Make sure to select **Throttle As Server** and **Treat As Authenticated** check boxes.
- In the event that an active AE server is not available, an administrator just needs to edit the static route entry for that server, and point it to the IP address or DNS address of the backup server.

All Microsoft Office Communicator clients will be periodically attempting to re-establish their sessions. As soon as this entry is updated, all INVITE messages will be routed to the new active server, and new sessions will be established with that server. If it is desired to move back to the primary server once it is back online, the administrator only needs to update the static route entry again, and all new sessions will be established with the restored server.

AE Services System Platform High Availability Failover

The Application Enablement Services on System Platform offer provides the high availability failover feature. With the System Platform high availability failover feature, you can install two identical AES servers that can be addressed and administered as a single entity. If one AES server fails, the second AES server quickly and automatically becomes available to client applications.

With the System Platform high availability failover feature, the dial plan and license file are automatically copied from the active AES server to the standby AES server. The static routes do not need to be updated in this case on the OCS/LCS/OCSSR2 because the same IP address is used by the standby. Communicator clients will automatically reconnect after the standby reboots.

The road map for integrating AE Services and Microsoft Office components

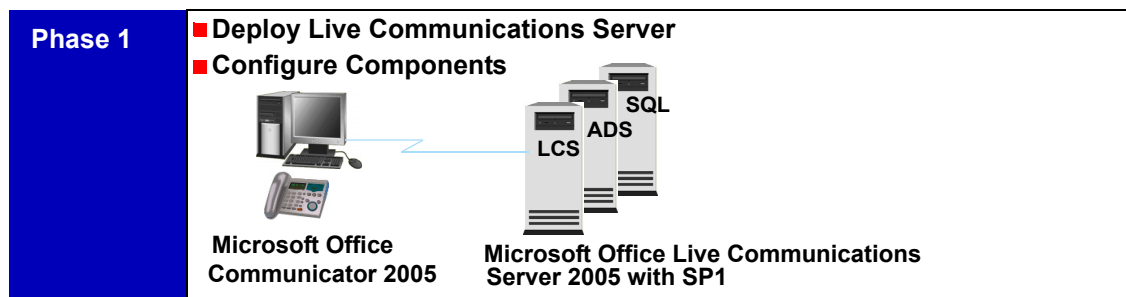
This section maps the integration activities to the documentation.

Phase 1: Setting up the Live Communications Server 2005 or the Office Communications Server 2007 environment

Note:

If OCS Enterprise edition is in use with an OCS server pool, the certificate should be issued in the name of the pool and must have both Server Authentication and Client Authentication. If a load balancer handles the pool, then the pool name should resolve to the load balancer's IP address. For example, if the OCS pool is called **ocspool.company.com**, and that is the pool that agents and OCS servers use, the DNS resolution of **ocspool.company.com** should be the IP address of the load balancer. Furthermore, the TLS certificate should be issued to **ocspool.company.com** from the correct authority with the correct company name, etc. Then, this certificate should be put on each of the OCS servers so that they pass this **ocspool.company.com** certificate when creating a secure socket to Application Enablement Services.

For a checklist of activities associated with Phase 1, see [Phase 1 checklist: Live Communications Server](#) on page 37. Note that Phase 1 and Phase 2 activities can be carried out concurrently.



Microsoft documents for Phase 1

This document assumes that you are implementing AE Services in one of the following configurations that is already in place:

- Microsoft Office Live Communications Server 2005 with SP1 configuration
- Microsoft Office Communications Server 2007

Documentation for Microsoft Office Live Communications Server 2005 with SP1 configuration

The following list is not the complete list of Microsoft Office Live Communications Server documents, but it includes documents that are strongly recommended for integrating AE Services with Live Communications Server. The Quick Start documents are particularly useful for integrating AE Services in a Live Communications Server environment.

- *Live Communications Server 2005 Enterprise Edition Lab Quick Start*
- *Live Communications Server 2005 with SP1 Standard Edition Lab Quick Start*
- *Microsoft Office Live Communications Server 2005 with SP1 Active Directory Preparation*
- *Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide*
- *Microsoft Office Live Communications Server 2005 Address Book Service Planning and Deployment Guide*
- *Microsoft Office Live Communications Server 2005 Certificate Configuration*
- *Microsoft Office Communicator Help*

You can download these documents from the Microsoft Download Center at the following Web address: <http://www.microsoft.com/downloads>

Documentation for Microsoft Office Communications Server 2007

The following list is not the complete list of Microsoft Office Communications Server 2007 documents, but it includes documents that are strongly recommended for integrating AE Services with Live Communications Server. The Quick Start documents are particularly useful for integrating AE Services in a Live Communications Server environment.

- *Microsoft Office Communications Server 2007 Enterprise Edition Deployment Guide*
- *Microsoft Office Communications Server 2007 Standard Edition Deployment Guide*
- *Microsoft Office Communications Server 2007 Document: Integrating Telephony with Office Communications Server 2007*
- *Microsoft Office Communications Server 2007 Active Directory Guide*
- *Microsoft Office Communications Server 2007 Document: Documentation Roadmap*
- *Microsoft Office Communicator 2007 Getting Started Guide*

You can download these documents from the Microsoft Download Center at the following Web address: <http://www.microsoft.com/downloads>

Documentation for Microsoft Office Communications Server 2007 R2

The following list is not the complete list of Microsoft Office Communications Server 2007 documents, but it includes documents that are strongly recommended for integrating AE Services with Live Communications Server. The Quick Start documents are particularly useful for integrating AE Services in a Live Communications Server environment.

- *Microsoft Office Communications Server 2007 R2 Enterprise Edition Deployment Guide*
- *Microsoft Office Communications Server 2007 R2 Standard Edition Deployment Guide*
- *Microsoft Office Communications Server 2007 R2 Deployment Guide*
- *Microsoft Office Communications Server 2007 R2 Walkthrough - Voice Deployment*
- *Microsoft Office Communications Server 2007 R2 Active Directory Guide*
- *Microsoft Office Communications Server 2007 R2 Documentation Roadmap*

You can download these documents from the Microsoft Download Center at the following Web address: <http://www.microsoft.com/downloads>

Phase 1 checklist: Live Communications Server

This checklist refers to activities described in [Phase 1: Setting up the Live Communications Server 2005 or the Office Communications Server 2007 environment](#) on page 35.

The information in [Table 1](#) is based on "Telephony Requirements" in the *Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide*. [Table 1](#) applies to either of the following configurations.

- Live Communications Server 2005 Standard Edition (up to 20,000 users)
- Live Communications Server 2005 Enterprise Edition (up to 125,000 users), sometimes referred to as an Enterprise Pool

These tasks can be performed at the same time as the tasks described [Phase 2: Setting up AE Services and Communication Manager](#) on page 41, but they must be completed before the tasks described in [Chapter 3: Integrating AE Services with Live Communications Server 2005](#).

Table 1: Checklist for Live Communications Server

	Task	Document
1	Active Directory is set up	
	<ul style="list-style-type: none"> Domain controllers with Microsoft Windows 2000 SP4 or Microsoft Windows 2003. Global catalog servers with Windows 2000 SP4 or Windows Server 2003. <p>For more information about Global catalog servers, see "Infrastructure Requirements," in <i>Live Communications Server 2005 with SP1 Active Directory Preparation</i>.</p> <p>Note: For your Active Directory user records, you must use a standard number format that can be normalized by Address Book. AE Services strongly recommends that you use E.164 format phone numbers.</p>	<ul style="list-style-type: none"> <i>Microsoft Office Live Communications Server 2005 with SP1 Standard Edition Deployment Guide</i> <i>Microsoft Office Live Communications Server 2005 with SP1 Enterprise Edition Deployment Guide</i>
2	Active Directory preparation is completed	
	<p>Carry out the Active Directory Preparation basic steps:</p> <ul style="list-style-type: none"> Prep Schema Prep Forest Prep Domain DomainAdd to the Forest Root 	<ul style="list-style-type: none"> <i>Microsoft Office Live Communications Server 2005 with SP1 Active Directory Preparation</i>. See "Running Active Directory Preparation Basic Steps: Prep Schema, Prep Forest, Prep Domain and DomainAdd to The Forest Root."
1 of 3		

Table 1: Checklist for Live Communications Server (continued)

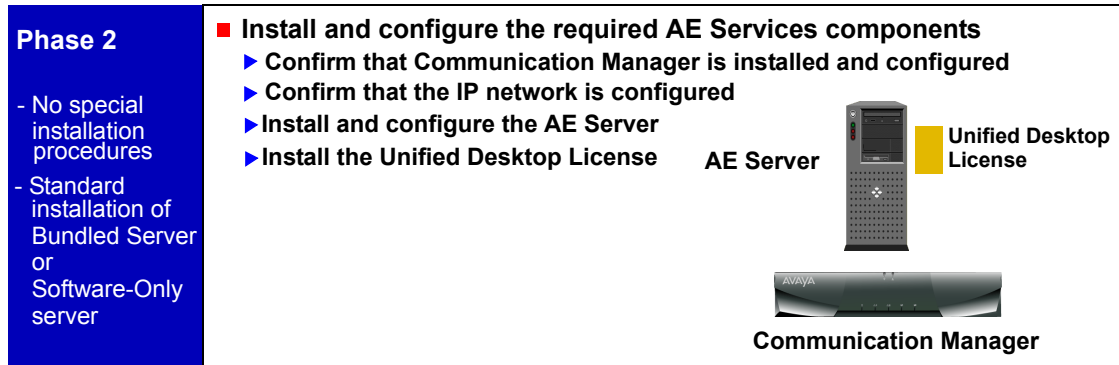
	Task	Document
3	Public Key Infrastructure (PKI) is set up	
	Set up a Public Key Infrastructure (PKI).	<ul style="list-style-type: none"> For more information, see <i>Microsoft Office Live Communications Server 2005 Certificate Configuration</i>. See also, <i>Live Communications Server 2005 with SP1 Security Guide</i>.
4	Certificates have been configured	
	For the AE Services Implementation for Microsoft Live Communications Server you must configure the Live Communications Server 2005 (Enterprise or Standard Edition) server to use Mutual TLS (Transport Layer Security) and then configure a certificate.	<ul style="list-style-type: none"> See <i>Microsoft Office Live Communications Server 2005 Certificate Configuration</i>, "Configuring Certificates on Live Communications Servers." See also, Administering Certificates -- certificate management on page 53.
5	Domain Name System (DNS) is set up and deployed	
	Set up the server.	<p>See "Configuring DNS, Client Access and User Settings" in either of these documents:</p> <ul style="list-style-type: none"> <i>Microsoft Office Live Communications Server 2005 with SP1 Standard Edition Deployment Guide</i> <i>Microsoft Office Live Communications Server 2005 with SP1 Enterprise Edition Deployment Guide</i>
6	Live Communications Server (either Standard or Enterprise) is deployed	
	<ul style="list-style-type: none"> Deploy Standard Edition. or Deploy Enterprise Edition. 	<ul style="list-style-type: none"> See "Deploying Live Communications Server 2005 Standard Edition" in the <i>Microsoft Office Live Communications Server 2005 with SP1 Standard Edition Deployment Guide</i>. See "Deploying Live Communications Server 2005 Enterprise Edition" in the <i>Microsoft Office Live Communications Server 2005 with SP1 Enterprise Edition Deployment Guide</i>.
2 of 3		

Table 1: Checklist for Live Communications Server (continued)

	Task	Document
7	Servers are configured	
	Configure either the Standard Edition Server or the Enterprise Edition Server.	<ul style="list-style-type: none"> See "Configuring the Standard Edition Server" in the <i>Microsoft Office Live Communications Server 2005 with SP1 Standard Edition Deployment Guide</i>. See "Configuring the Enterprise Edition Server" in the <i>Microsoft Office Live Communications Server 2005 with SP1 Enterprise Edition Deployment Guide</i>.
8	DNS is configured	
	Configure DNS.	<ul style="list-style-type: none"> See "Configuring DNS, Client Access and User Settings" in the <i>Microsoft Office Live Communications Server 2005 with SP1 Standard Edition Deployment Guide</i>. See "Configuring DNS, Client Access and User Settings" in the <i>Microsoft Office Live Communications Server 2005 with SP1 Enterprise Edition Deployment Guide</i>.
9	Set up Address Book Service <ul style="list-style-type: none"> Address Book Service is required for AE Services Live Communications Server integration. 	
	<p>The main function of the Address Book Service is to provide Microsoft Office Communicator with a local cache of the global address list. AE Services requires that you configure Live Communications Server with the Address Book service so that Communicator users can take advantage of this capability.</p> <p>Optionally, you can set up the Address Book Service to perform phone number normalization.</p> <p>Note: If you configure the Address Book Service to normalize phone numbers, bear in mind that it does not support multinational deployments of Live Communications Server. Only one set of normalization rules can be configured per Live Communications server. If that server is supporting multiple countries, you can do the normalization rules for only one of those countries.</p>	<ul style="list-style-type: none"> See <i>Microsoft Office Live Communications Server 2005 Address Book Service Planning and Deployment Guide</i>.
3 of 3		

Phase 2: Setting up AE Services and Communication Manager

For the checklist of activities associated with Phase 2, see [Phase 2 checklists: setting up AE Services and Communication Manager](#) on page 42.



AE Services documents for Phase 2

To install the AE Services software and bring the AE Server to an operational state, use either the Bundled Server or the Software Only installation guide, based on the offer you are using. Use the Administration Guide for administering Communication Manager.

- *Implementing Avaya Aura® Application Enablement Services for a Bundled Server*
- *Implementing Avaya Aura® Application Enablement Services in a Software-Only Environment*
- *Implementing Avaya Aura® Application Enablement Services on Avaya Aura® System Platform*
- *Avaya Aura® Application Enablement Services Administration and Maintenance Guide, 02-300357*
- Application Enablement Services Management Console online help (which is included with the AE Services server software)

AE Services documents are available from the Web in Portable Document Format (.pdf) at the Avaya Support Web Site (<http://www.avaya.com/support>).

Phase 2 checklists: setting up AE Services and Communication Manager

Use the checklists in this section for either a Bundled Server installation or a Software-Only server installation. The tasks in each of these checklists must be completed before you start the procedures described in [Chapter 3: Integrating AE Services with Live Communications Server 2005](#).

- [Table 2](#) summarizes the tasks that are required for carrying out an AE Services on System Platform installation.
- [Table 3](#) summarizes the tasks that are required for carrying out an AE Services Bundled Server installation.
- [Table 4](#) summarizes the tasks that are required for carrying out an AE Services Software-Only server installation.



Important:

For Communication Manager 6.3 and later, ASAI requires the signaling groups between Communication Manager and Session Manager to use TLS.

Application Enablement Services on System Platform installation checklist

Avaya Technical Services is responsible for installing and maintaining components in an Application Enablement Services on System Platform configuration. In [Table 2](#): FE refers to Field Engineer and PS refers to Professional Services.

Table 2: Application Enablement Services on System Platform installation checklist

	Task	Role	Document
1	Verify that the installation site meets the prerequisites.	FE	See <i>Implementing Avaya Aura® Application Enablement Services on Avaya Aura® System Platform</i> .
2	Install and configure the hardware.	FE	See <i>Implementing Avaya Aura® Application Enablement Services on Avaya Aura® System Platform</i> .
3	Install the software.	FE	See <i>Implementing Avaya Aura® Application Enablement Services on Avaya Aura® System Platform</i> .
1 of 2			

Table 2: Application Enablement Services on System Platform installation checklist (continued)

	Task	Role	Document
4	Install the AE Services license.	FE	See <i>Implementing Avaya Aura® Application Enablement Services on Avaya Aura® System Platform</i> . Note: For the AE Services implementation for Microsoft Live Communications Server 2005 or Office Communications Server 2007, install the "Unified CC API - Desktop Edition" license. This is a per-user license. Every active Microsoft Office Communicator client consumes one Unified Desktop license for the duration of the period that it has an active dialog with Application Enablement Services.
5	Verify Communication Manager requirements.	PS/FE	See the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> .
6	Verify TN799DP CLAN board installation and administration on Communication Manager. If you are using Processor Ethernet (PE) for AES to Communication Manager connectivity, then verify the relevant configuration.	PS/FE	See the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> .
7	Enable AE Services on Communication Manager.	PS	See the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> .
8	Administer a CTI link (ADJ-IP).	PS	See the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> .
9	Check the status of the switch connection (from Communication Manager to AE Services).	PS	See the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> .
2 of 2			

Bundled Server installation checklist

Avaya Technical Services is responsible for installing and maintaining components in a Bundled Server configuration. In [Table 3](#): FE refers to Field Engineer and PS refers to Professional Services.

Table 3: Bundled server installation checklist

	Task	Role	Document
1	Verify that the installation site meets the prerequisites.	FE	See <i>Implementing Avaya Aura® Application Enablement Services for a Bundled Server</i> .
2	Install and configure the hardware.	FE	See <i>Implementing Avaya® Application Enablement Services for a Bundled Server</i> .
3	Install the software.	FE	See <i>Implementing Avaya Aura® Application Enablement Services for a Bundled Server</i> .
4	Install the AE Services license.	FE	See <i>Implementing Avaya Aura® Application Enablement Services for a Bundled Server</i> . Note: For the AE Services implementation for Microsoft Live Communications Server 2005 or Office Communications Server 2007, install the "Unified CC API - Desktop Edition" license. This is a per-user license. Every active Microsoft Office Communicator client consumes one Unified Desktop license for the duration of the period that it has an active dialog with Application Enablement Services.
5	Verify Communication Manager requirements.	PS/FE	See the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> .
6	Verify TN799DP CLAN board installation and administration on Communication Manager. If you are using Processor Ethernet (PE) for AES to Communication Manager connectivity, then verify the relevant configuration.	PS/FE	See the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> .
7	Enable AE Services on Communication Manager.	PS	See the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> .
1 of 2			

Table 3: Bundled server installation checklist (continued)

	Task	Role	Document
8	Administer a CTI link (ADJ-IP).	PS	See the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> .
9	Check the status of the switch connection (from Communication Manager to AE Services).	PS	See the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> .
2 of 2			

Software-Only server installation checklist

The customer or an Information Technology (IT) Technician is responsible for installing and maintaining components in an AE Services Software-Only server configuration.

Table 4: Software-only server installation checklist

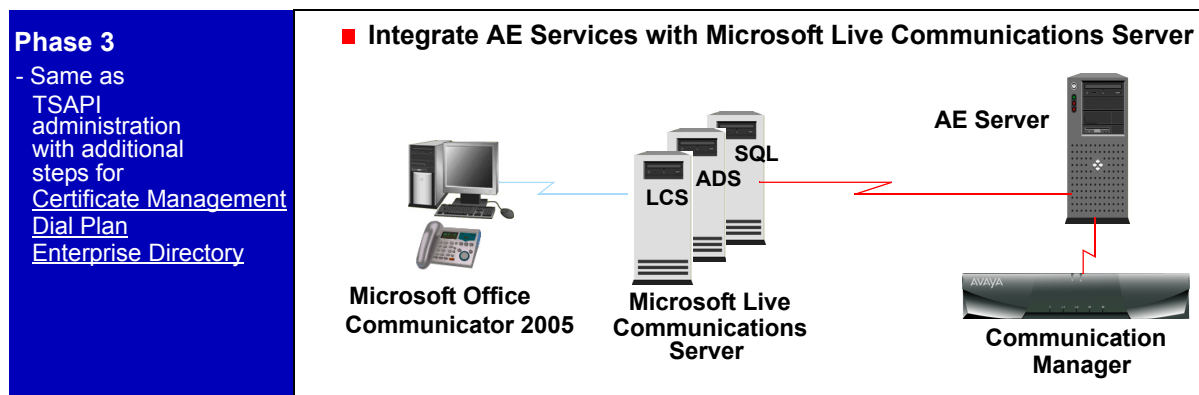
	Task	Admin domain	Document
1	Determine that you have met the prerequisites for AE Services.	AE Services	See <i>Implementing Avaya Aura® Application Enablement Services in a Software-Only Environment</i> .
2	Install the Linux platform software.	AE Services	See <i>Implementing Avaya Aura® Application Enablement Services in a Software-Only Environment</i> .
3	Install the software.	AE Services	See <i>Implementing Avaya Aura® Application Enablement Services in a Software-Only Environment</i> .
4	Install the AE Services license.	AE Services	See <i>Implementing Avaya Aura® Application Enablement Services in a Software-Only Environment</i> . Note: For the AE Services implementation for Microsoft Live Communications Server 2005 or Office Communications Server 2007, install the "Unified CC API - Desktop Edition" license. This is a per-user license. Every active Microsoft Office Communicator client consumes one Unified Desktop license for the duration of the period that it has an active dialog with Application Enablement Services.
5	Verify Communication Manager requirements.	Communication Manager	See the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> .
1 of 2			

Table 4: Software-only server installation checklist

	Task	Admin domain	Document
6	Verify TN799DP CLAN board installation and administration on Communication Manager. If you are using Processor Ethernet (PE) for AES to Communication Manager connectivity, then verify the relevant configuration.	Communication Manager	See the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> .
7	Enable AE Services on Communication Manager.	Communication Manager	See the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> .
8	Administer a CTI link (ADJ-IP).	Communication Manager	See the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> .
9	Check the status of the switch connection (from Communication Manager to AE Services).	Communication Manager	See the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> .
2 of 2			

Phase 3: Integrating AE Services with Live Communications Server

Phase 3 is presented separately in [Chapter 3: Integrating AE Services with Live Communications Server 2005](#). Chapter 2 describes the administrative procedures for AE Services and Live Communications Server that are necessary for a successful integration.



Microsoft Office Live Communications Server documents for Phase 3

- *Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide*
- *Microsoft Office Live Communications Server 2005 Certificate Configuration*

AE Services documents for Phase 3

- *Avaya Aura[®] Application Enablement Services Implementation Guide for Microsoft Live Communications Server, 02-601893*
- *Avaya Aura[®] Application Enablement Services Administration and Maintenance Guide, 02-300357*
- Application Enablement Services Management Console online help (included with the AE Services server software)

Chapter 3: Integrating AE Services with Live Communications Server 2005

How to use the information in this chapter

After you complete the tasks in Chapter 1, use the information in this chapter to integrate Application Enablement Services (AE Services) with Microsoft Live Communications Server.

Phase 3 Checklist --integrating AE Services with Live Communications Server

Use [Table 5](#) as a checklist for performing the tasks necessary for integrating AE Services in a Microsoft Live Communications Server environment.

Table 5: Checklist for integrating AE Services with Live Communications Server

Task		Admin domain	Notes
1	Administer a switch connection from AE Services to Communication Manager.	AE Services	See "AE Services integration for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007 - checklist," in Chapter 3 of the <i>Avaya Aura® Application Enablement Services Administration and Maintenance Guide</i> , 02-300357.
2	Check the status of the switch connection (from AE Services to Communication Manager).	AE Services	
3	Administer a TSAPI Link.	AE Services	
4	Enable the TR/87 Port in the AE Services Management Console.	AE Services	See Enabling the TR/87 port on page 52.
1 of 3			

Table 5: Checklist for integrating AE Services with Live Communications Server (continued)

Task		Admin domain	Notes
5	Administer certificates for AE Services and Microsoft Live Communications Server.	Microsoft Live Communications Server	See Procedure 1 - Installing the trusted certificate on Live Communications Server on page 55.
		Microsoft Live Communications Server	See Procedure 2 - Installing a server certificate for the Live Communications Server on page 59 of this document.
		AE Services	See Procedure 3 - Installing the trusted certificate on the AE Server on page 63 of this document.
		AE Services	See Procedure 4 - Creating a server certificate request for AE Services on page 67 of this document.
		AE Services	See Procedure 5 - Creating a server certificate for AE Services on page 69 of this document.
		AE Services	See Procedure 6 - Importing the server certificate into AE Services on page 71 of this document.
6	Administer settings for the dial plan.	AE Services	See Dial Plan settings in AE Services on page 73 of this document.
7	Administer settings for Active Directory.	AE Services	See Administering AE Services access to Active Directory on page 90 of this document.
8	Configure the Microsoft Office Communicator 2005 Client.	Microsoft -- either the client workstation or the Active Directory Server	See "Configuring the Client" in the <i>Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide</i> .
9	Set up a static route.	Microsoft Live Communications Server	See Configuring a static route on page 97.
			2 of 3

Table 5: Checklist for integrating AE Services with Live Communications Server (continued)

Task		Admin domain	Notes
10	Specify the AE Server as an authorized host.	Microsoft Live Communications Server	AE Services Implementation Guide for Microsoft Live Communications Server, see Specifying the AE Server as an authorized host on page 98.
11	Set up Remote Call Control for each user in Active Directory Services.	Microsoft Active Directory Server	AE Services Implementation Guide for Microsoft Live Communications Server, see Enabling Remote Call Control in Active Directory on page 95. Based on information from <i>Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide</i> .
			3 of 3

About configuring AE Services for Live Communications Server

In terms of the AE Services administration, configuring AE Services for Live Communications Server is an extension of TSAPI-based administration.

To configure AE Services for Live Communications Server, you must carry out the TSAPI-related administration tasks as well as the AE Services implementation for Microsoft LCS administration tasks.

- **TSAPI related administration tasks**, which are described in Chapter 3 of the *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, 02-300357:
 - administering a local IP
 - administering a switch connection
 - administering a TSAPI link
- **AE Services implementation for Microsoft LCS administration tasks**, which are described in this document:
 - enabling the TR/87 port - see [Enabling the TR/87 port](#) on page 52
 - administering certificates - see [Administering Certificates -- certificate management](#) on page 53
 - administering the dial plan settings - see [Dial Plan settings in AE Services](#) on page 73
 - administering settings for Active Directory - see [Administering AE Services access to Active Directory](#) on page 90

Enabling the TR/87 port

AE Services uses port 4723 for communications between AE Services and Microsoft Live Communications Server. Because this port is disabled by default in the AE Services Management Console, you must enable it.

1. From the browser on your AE Services administrative workstation, log in to the AE Services Management Console.
2. From the main menu of the AE Services Management Console, select **Networking > Ports**.
3. On the Ports page, under DMCC Server Ports, locate the TR/87 Port, and select the option button for **Enabled**.

Administering Certificates -- certificate management

AE Services and Microsoft Live Communication Server communicate using Transport Layer Security (TLS). For communication to take place, AE Services and Microsoft Live Communications Server must exchange signed server certificates each time a TLS session is opened. This section provides a sample certificate management scenario that includes the following procedures.

- [Procedure 1 - Installing the trusted certificate on Live Communications Server](#) on page 55
- [Procedure 2 - Installing a server certificate for the Live Communications Server](#) on page 59
- [Procedure 3 - Installing the trusted certificate on the AE Server](#) on page 63
- [Procedure 4 - Creating a server certificate request for AE Services](#) on page 67
- [Procedure 5 - Creating a server certificate for AE Services](#) on page 69
- [Procedure 6 - Importing the server certificate into AE Services](#) on page 71

Note:

If OCS Enterprise edition is in use with an OCS server pool, the certificate should be issued in the name of the pool and must have both Server Authentication and Client Authentication. If a load balancer handles the pool, then the pool name should resolve to the load balancer's IP address. For example, if the OCS pool is called **ocspool.company.com**, and that is the pool that agents and OCS servers use, the DNS resolution of **ocspool.company.com** should be the IP address of the load balancer. Furthermore, the TLS certificate should be issued to **ocspool.company.com** from the correct authority with the correct company name, etc. Then, this certificate should be put on each of the OCS servers so that they pass this **ocspool.company.com** certificate when creating a secure socket to Application Enablement Services.

Additional references

The following documents are useful for understanding the tasks that are required for a service integration.

- *Live Communications Server 2005 Enterprise Edition Lab Quick Start* or
- *Live Communications Server 2005 with SP1 Standard Edition Lab Quick Start*

About the sample scenario

Use the sample scenario to familiarize yourself with the basic tasks for integrating AE Services with Microsoft Live Communications Server. The procedures in the sample scenario are based on using:

- Microsoft Live Communications Server 2005 Enterprise Edition
- Microsoft Windows Server 2003 Standalone Certificate Authority.

Because it is likely that some users will rely on a certificate authority (CA) other than Microsoft Certificate Services, the CA-based procedures include generic instructions as well as Microsoft-based instructions.

Note:

If you are using a Microsoft Windows Server 2003 Enterprise Edition Certificate Authority, Appendix D provides a procedure for creating a server certificate template that supports both client authentication and server authentication. For more information see [Appendix D: Creating a certificate template for Server Certificates on the Microsoft CA Server](#) on page 201. Keep in mind that all of the procedures in Chapters 2 and 3 of this document are based on a Microsoft Windows Server 2003 Standalone Certificate Authority. If you use an Enterprise Edition CA, the procedures in Chapters 2 and 3 do not apply to your configuration.

About obtaining certificates

To obtain a certificate you must generate a certificate request and then submit the Certificate Request to a CA. Procedures for generating a certificate request and the data required for completing a certificate request can vary from one CA to another.

Specifying key usage

Based on the CA you use, you might be required to specify the key usage allowed for the certificate you are requesting. If your CA requires you to specify key usage, you must ensure that the `digitalSignature` and the `keyEncipherment` bits are enabled. For more information refer to RFC 2459.

Client and server authentication

The AE Services implementation for Live Communications Server requires a certificate that does both client authentication and server authentication.

In terms of the Microsoft Windows Server 2003 Standalone CA, this means that when you complete the Advanced Certificate Request, you will select Other... from the "Type of Certificate Needed" drop-down list. When you select **Other...**, the Advanced Certificate Request displays a text entry field for the OID (object identifier). For information about completing this field, see [Installing a Microsoft Certificate Services-based certificate on the Live Communications Server](#) on page 60.

If you use another CA (either a generic CA or the Microsoft Windows Server 2003 Enterprise CA), the certificate request will not contain the same drop-down menus and choices. For example with Microsoft Windows Server 2003 Enterprise CA, you might not see a field for the OIDs because the OIDs can be set by the CA administrator in a template.

Procedure 1 - Installing the trusted certificate on Live Communications Server

The trusted certificate is also referred to as the CA Certificate. From the Microsoft Live Communications Server, follow the appropriate procedure to obtain the trusted certificate and import it into the Microsoft Live Communications Server certificate store.

When installing the trusted certificate, note that Live Communications Server and AE Services must use either the same CA or an issuer in the same certificate chain.

- If you are using a third party certificate authority other than Microsoft Certificate Services, follow the procedure described in [Installing the trusted certificate from another vendor](#).
- If you are using Microsoft Certificate Services, follow the procedure described in [Installing the trusted certificate generated by Microsoft Certificate Services](#).

Installing the trusted certificate from another vendor

Steps 1 and 2 are provided as a general reference only -- follow the instructions on your CA's Web site.

1. From your browser, go your certificate authority's Web page for requesting a trusted certificate or a trusted certificate chain.
2. Import the trusted certificate. For information about importing certificates and using the certreq utility, see "Using a Public Certificate," in *Microsoft Office Live Communications Server 2005 Certificate Configuration*.
3. Continue with [Importing the certificate into the Live Communications Server's trust store](#) on page 57.

Installing the trusted certificate generated by Microsoft Certificate Services

Follow this procedure to download the trusted certificate generated by Microsoft Certificate Services.

1. From your browser, type the URL of the Microsoft Certificate Services Server. For example:
`http://<certificate_server.com>/certsrv`
2. From the Microsoft Certificate Services page, click **Download a CA certificate, certificate chain, or CRL**.
3. Complete the Download a CA Certificate, Certificate Chain, or CRL page as follows:
 - a. Under CA Certificate, in the list box, select the signing certificate.
 - b. Click **Base 64**.
 - c. Click **Download CA certificate chain**.
4. Save the CA certificate file (**lcscertnew.p7b**, for example) to a local directory on the Microsoft Live Communications Server (C:\temp, for example).
5. Continue with the steps described next in [Importing the certificate into the Live Communications Server's trust store](#).

Importing the certificate into the Live Communications Server's trust store

Use this procedure to import the trusted certificate, from any CA, in to the Live Communications Server's trust store.

1. Start the Microsoft Management console -- Click **Start**, and then click **Run**. In the Run dialog box, type **mmc**, and click **OK**.
2. From the Console window, click **File > Add/Remove Snap-in...**
3. From the Add/Remove Snap-in dialog box, on the Standalone tab, which displays **Console Root** as the default, click **Add...**
4. From the Add Standalone Snap-in dialog box, select **Certificates**, and click **Add**.
5. From the Certificates snap-in dialog box, select **Computer account**, and click **Next**.
6. From the Select Computer dialog box, select **Local Computer: (the computer this console is running on)**, and click **Finish**.
7. Click **Close** from the Add Standalone Snap-in dialog box, and then click **OK** from the Add/Remove Snap-in dialog box.
8. From the left pane of the Console Root, under Certificates (Local Computer), expand **Trusted Root Certificates Authorities**.
9. Right-click **Certificates**, and then select **All Tasks** and click **Import**.
10. From the Certificate Import Wizard, Welcome screen, select **Next**.
11. Click **Browse**, and go to the directory where you stored the certificate file (**C:\temp\lscertnew.p7b**, for example). Select the certificate file (**lscertnew.p7b**, for example) and click **Open**. Click **Next** to advance to the Certificate Store screen.
12. In the Certificate Import Wizard, Certificate Store dialog box, make sure that **Place all certificates in the following store** is selected, and the Certificate Store is: **Trusted Root Certification Authorities**. Click **Next**.
13. When the Certificate Import Wizard dialog box displays the message "You have successfully completed the Certificate Import wizard," click **Finish**.

Procedure 1a - Verifying the installation of the trusted certificate on Live Communications Server

Follow this procedure to verify that the trusted certificate is installed correctly.

1. Start the Microsoft Management console -- Click **Start**, and then click **Run**. In the Run dialog box, type **mmc**, and click **OK**.
2. From the Console window, click **File > Add/Remove Snap-in...** .
3. From the Add/Remove Snap-in dialog box, on the Standalone tab, which displays **Console Root** as the default, click **Add...** .
4. From the Add Standalone Snap-in dialog box, select **Certificates**, and click **Add**.
5. From the Certificates snap-in dialog box, select **Computer account**, and click **Next**.
6. From the Select Computer dialog box, select **Local Computer: (the computer this console is running on)**, and click **Finish**.
7. Click **Close** from the Add Standalone Snap-in dialog box, and then click **OK** from the Add/Remove Snap-in dialog box.
8. Verify that the trusted certificate for the Live Communications Server is installed, as follows:
 - a. In the left pane of the console, Under Certificates (Local Computer) expand **Trusted Root Certificates Authorities** and click **Certificate**. The console displays a list of trusted certificates in the right pane.
 - b. In the right pane of the console, verify that the display includes the trusted certificate that you installed at the end of Procedure 1, as follows:
 - Make sure the Issued To field displays the fully-qualified domain name of the Live Communications Server.
 - Make sure the Issued By field displays the name of the certificate authority that issued the certificate.
 - Make sure the expiration date is correct.

Procedure 2 - Installing a server certificate for the Live Communications Server

Follow the appropriate procedure for installing a server certificate for the Live Communications Server.

- If you are using a third party certificate authority other than Microsoft Certificate Services, refer to [Installing a server certificate from another vendor](#) on page 59.
- If you are using Microsoft Certificate Services, refer to [Installing a Microsoft Certificate Services-based certificate on the Live Communications Server](#) on page 60.

Installing a server certificate from another vendor

Steps 1 through 3 are provided as a general reference only -- follow the instructions on your CA's Web site.

1. From your browser, go to your certificate authority's Web page for requesting a server certificate.
2. Complete the required fields for enrollment. Usually this includes contact information, such as your name, email address, your organizational unit (OU), and so on.

When you are providing the name and IP address for the server, use this rule of thumb. If you are using Enterprise Edition, use the fully qualified domain name and IP address of your pool; if you are using Standard Edition use the fully qualified domain name and IP of your server.

3. Import the server certificate. For information about importing certificates and using the certreq utility, see "Using a Public Certificate," in *Microsoft Office Live Communications Server 2005 Certificate Configuration*.
4. Continue with the steps for [Procedure 2b - Configuring the certificate for automatic routing](#) on page 62.

Installing a Microsoft Certificate Services-based certificate on the Live Communications Server

From the Microsoft Live Communications Server, follow this procedure to install a server certificate issued by Microsoft Certificate Services.

Note:

In terms of the Microsoft Live Communications Server 2005 Certificate Configuration Guide, the AE Services implementation for Microsoft LCS falls into the category of "interoperating with partner systems." This means that you must install a certificate that is configured for both client and server authorization, as depicted in Step 3c.

1. From your Web browser, type the URL of your certificate server. For example:
http://<certificate_server.com>/certsrv
2. From the Microsoft Certificate Services Welcome page, click **Request a Certificate**.
3. From the Advanced Certificate Request page, click **Create and submit a request to this CA**. Microsoft Certificate Services displays the next page of the of Advanced Certificate Request. Keep in mind that the fields presented on the Advanced Certificate Request pages depend on how the certification server is set up.

Follow Step [a](#) through Step [f](#) to complete the Advanced Certificate Request.

- a. Under Identifying Information, in the Name field, type the fully qualified domain name (FQDN) of your pool. For example: **mylcpool.example.com** . The pool entry in the Name field applies to the Enterprise Edition of Live Communications Server. If you are using Standard Edition of Live Communications Server, you would use the FQDN of the server.
- b. Under Type of Certificate Needed, in the selection box, select **Other...** . When you select **Other**, the Certificate Request displays the OID field.

Note:

If you do not see a selection for **Other...** , it means you are using a CA other than Microsoft Windows Server 2003 Standalone Certificate Authority. See [Client and server authentication](#) on page 55

- c. In the OID field, type the following OID for your certificate:
1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2 (be sure to use a comma between the two parts of the OID). The first part of the OID, which is provided by default, (1.3.6.1.5.5.7.3.1) is for server authentication. The second part (1.3.6.1.5.5.7.3.2), which you must add, is for client authentication.

- d. Under Key Options, make the following selections:
 - In the Key Usage Field, select the option button for **Both**.
 - In the CSP field, accept the default, which is **Microsoft Enhanced Cryptographic Provider v1.0**.
 - Select the check box for **Store Certificate in the local computer certificate store**.
 - e. Under additional options, In the Friendly Name field, type a name that will help you identify the certificate.
 - f. Click **Submit**. Microsoft Certificate Services displays the Certificate Issued page.
4. From the Certificate Issued page, click **Install this certificate**. Microsoft Certificate Services displays the Certificate Installed page.

Procedure 2a - Verifying the installation of the server certificate for Live Communications Server

Use this procedure to verify the installation of the server certificate, from any CA, for the Live Communications Server.

1. Start the Microsoft Management console -- Click **Start** and then click **Run**. In the Run dialog box, type **mmc**, and click **OK**.
2. From the Console window, click **File > Add/Remove Snap-in...**
3. From the Add/Remove Snap-in dialog box, on the Standalone tab, which displays **Console Root** as the default, click **Add...**
4. From the Add Standalone Snap-in dialog box, select **Certificates**, and click **Add**.
5. From the Certificates snap-in dialog box, select **Computer account**, and click **Next**.
6. From the Select Computer dialog box, select **Local Computer: (the computer this console is running on)**, and click **Finish**.
7. Click **Close** from the Add Standalone Snap-in dialog box, and then click **OK** from the Add/Remove Snap-in dialog box.
8. Verify that the server certificate for the Live Communications Server is installed, as follows:
 - a. In the left pane of the console, Under Certificates (Local Computer) expand **Personal** and click **Certificate**. The console displays a list of certificates in the right pane.
 - b. In the right pane of the console, verify that the display includes the server certificate that you installed at the end of Procedure 2, as follows:
 - Make sure the Issued To field displays the fully-qualified domain name of the Live Communications Server.
 - Make sure the Issued By field displays the name of the certificate authority that issued the certificate (referred to as the issuer on the certificate).
 - Make sure the expiration date is correct.

Procedure 2b - Configuring the certificate for automatic routing

Follow this procedure to configure the certificate for automatic routing among your pool and servers. For more information, see "Configuring Certificates for Automatic Routing Among Pools and Standard Edition Servers" in *Microsoft Office Live Communications Server Certificate Configuration*.

1. Open the Microsoft Office Live Communications Server 2005 management console.
2. In the left pane, expand the **Forest** node and the following subordinate nodes.
 - Live Communications servers and pools
 - **lcspool node** - the name of Live Communications Server pool node. If you are using Standard Edition, this refers to the Live Communications Server.

3. Under the lcs-pool node (**mylcpool**, for example), right-click the fully qualified domain name of your server (**mylcserver.example.com**, for example), and then click **Properties**.
4. From the **mylcserver.example.com Properties** dialog, follow these steps to add a TLS certificate and a security certificate.
 - a. Select the **General** tab. In the Connections box, select the listing for **Mutual TLS**.
Choose either 1 or 2, based on what is appropriate for your situation.
 1. In the Connections box, select the listed **Mutual TLS** connection, and click **Edit**. From the **Select Certificate** dialog box, select the certificate that was issued to the pool name, mylcpool.example.com, and click **OK**. Continue with Step 4b.
 2. Click **Add** to add a new connection so you can administer a certificate. From the Add Connection dialog box, select **TLS** for Transport Type and click **Select Certificate**. From the **Select Certificate** dialog box, select the certificate that was added to the pool name, mylcpool.example.com, and click **OK**. Continue with Step 4b.
 - b. Select the **Security** tab, and then click **Select Certificate**. From the Select Certificate dialog box, select the certificate you installed, and click **OK**.
 - From the Properties dialog, click **Apply**, and then click **OK** to close the Properties dialog.

Procedure 3 - Installing the trusted certificate on the AE Server

The trusted certificate is also referred to as the certificate authority (CA) certificate. It is issued by the certificate authority, which can be either Microsoft Certificate Services or another certificate authority.

- If you are using a certificate authority other than Microsoft Certificate Services, use the procedure described in [Generic procedure for installing the trusted certificate for AE Services](#) on page 64.
- If you are using Microsoft Certificate Services, use the procedure described in [Microsoft-based procedure for installing a trusted certificate chain](#) on page 65.

Generic procedure for installing the trusted certificate for AE Services

These steps are provided as a general reference only -- follow the instructions on your CA's Web site.

1. From your browser, go to your certificate authority's Web page and download the certificate chain.



Important:

You must import the entire certificate chain all the way back to the root certificate.

- The trusted certificate or certificate chain must be in text format (PEM or Base-64). If you are importing a certificate chain, it must be a text-based PKCS#7 file. Think of a PKCS#7 file as an envelope containing all trusted certificates.
 - It is acceptable to import certificates in the chain individually if they are not available in PKCS#7 format, but all certificates must be in the trusted certificates store.
2. The certificate authority processes your request and issues a trusted certificate (or certificate chain) for you to download.
 3. Download the entire certificate to the AE Services administrative workstation, and save it with a unique name (for example, **C:\templaetrucert.cer**).
 4. Using a text editor, open the trusted certificate file, and verify the header and trailer:
 - The header and trailer for a PEM or Base 64 file are as follows:


```
-----BEGIN CERTIFICATE----- (header)
-----END CERTIFICATE----- (trailer)
```
 - The header and trailer for a PKCS#7 file are as follows:


```
-----BEGIN PKCS7----- (header)
-----END PKCS7----- (trailer)
```

Note:

The header and trailer in your PKCS#7 file must read as follows before you import the contents of the file into OAM:

```
-----BEGIN PKCS7-----
-----END PKCS7-----
```

If the header and trailer read as:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

you must edit them to read as:

```
-----BEGIN PKCS7-----
-----END PKCS7-----.
```

5. Contact the Microsoft Live Communications Server administrator, and confirm that both the server certificate and the trusted certificate are installed and operating on Live Communications Server. The certificates must be installed and operating on Live Communications Server before you can carry out the procedures in the AE Services Management Console.

6. Continue with the steps described next in [Importing the trusted certificate into the AE Services Management Console](#) on page 66.

Microsoft-based procedure for installing a trusted certificate chain

If you use a Microsoft CA hierarchy, follow this procedure from the AE Server to import the trusted certificate chain in PKCS#7 format from Microsoft Certificate Services into the AE Services Management Console.

1. From Internet Explorer, type the URL of your certificate server. For example:
http://<microsoftcertificate_server.com>/certsrv
2. From the Microsoft Certificate Services page, click **Download a CA certificate, certificate chain, or CRL**.
3. On the Download a CA Certificate, Certificate Chain, or CRL page, select the option button for **Base 64**, and click **Download CA certificate chain**.
4. Save the CA certificate file (the trusted certificate) to a local directory on the Microsoft Live Communications Server (for example **C:\templaetrucert.p7b**).
5. Using a text editor, open the file and change the header and trailer as follows:

```
-----BEGIN PKCS7-----
-----END PKCS7-----
```



Important:

You must change the header and trailer in the PKCS#7 file as specified in Step 5. Otherwise, you will be unable to successfully import the trusted certificate chain from a Microsoft CA.

6. Contact the Microsoft Live Communications Server administrator, and confirm that both the server certificate and the trusted certificate are installed and operating on the Live Communications Server. The certificates must be installed and operating on Live Communications Server before you can carry out the procedures in the AE Services Management Console.
7. Continue with the steps described next in [Importing the trusted certificate into the AE Services Management Console](#) on page 66.

Importing the trusted certificate into the AE Services Management Console

1. From the main menu of the AE Services Management Console, select **Security > Certificate Management > CA Trusted Certificates**.
2. From the CA Trusted Certificates page, click **Import**.
3. Complete the Trusted Certificate Import page, as follows:
 - In the Certificate Alias field, type an alias for the trusted certificate (for example, **catrusted**). The trusted certificate alias can be arbitrary. It does not need to match any aliases for AE Services.
 - Click **Browse** to locate the trusted certificate file you want to import, and click **Apply**. If the import is successful, AE Services displays the following message: "Certificate Imported Successfully."

Note:

At this point it is recommended that you complete [Procedure 3a - Verifying the installation of the trusted certificate in AE Services](#) on page 66.

Procedure 3a - Verifying the installation of the trusted certificate in AE Services

Use this procedure to verify the installation of the entire certificate chain (all the way back to the root certificate) in AE Services.

1. In the AE Services Management Console, select **Security > Certificate Management > CA Trusted Certificates**.
2. From the CA Trusted Certificates page, select the alias of the trusted certificate (**catrusted**, based on this sample scenario), and click **View**.
3. From the Trusted Certificate Details page, verify that the information for the trusted certificate is correct.
 - a. Verify that the entire chain of certificates exists, all the way back to a self-signed certificate.
 - b. Verify that the Issued To field displays name of the organization that the trusted certificate is issued to.
 - c. Verify that the Issued By field Indicates the name of the certificate authority that issued the trusted certificate (referred to as the issuer on the certificate). This issuer should be either the same issuer, or an issuer in the same certificate chain, as described in Step 8b of Procedure 1a on page 58.
 - d. Verify that the Expiration Date Indicates the date that the trusted certificate expires.
 - e. Verify the information in the Details display. Make sure the Certificate Status is valid.
4. Click **Close** to exit the Trusted Certificate Details page.

Converting Certificate files in other formats for AE Services

If your CA provides you with a certificate in DER format, you must convert it to PEM before importing it into the AE Services Management Console. The following sections describe how to convert files using openssl tools, which are available on the Web at www.openssl.org.

Converting a DER file to PEM : If your certificate authority provides you with a DER-encoded certificate, you must convert it to PEM before you can import it into the AE Services Management Console. Use the following command to convert the DER file to PEM format.

```
openssl x509 -in <input>.cer -inform DER -out <output>.cer -outform PEM
```

Procedure 4 - Creating a server certificate request for AE Services

In the AE Services Management Console, use this procedure to create a server certificate request (also referred to as a certificate signing request, or CSR) for the AE Services server. This procedure generates a certificate signing request which includes a private key.

1. From the browser on your AE Services administrative workstation, log in to the AE Services Management Console.
2. Select **Security > Certificate Management > Server Certificates**.
3. On the Server Certificate pages, click **Add**.
4. Complete the Add Server Certificate page, as follows:
 - From the Certificate Alias list box, select the certificate alias:
 - **aeservices** refers to the AE Services: CVLAN, DLG, DMCC, and TSAPI.
 - **web** refers to Apache and Tomcat.
 - **ldap** refers to LDAP.
 - **server** refers to all (aeservice, web, and ldap).
 - Leave the Create Self-Signed Certificate check box unchecked (the default).
 - Leave the Enrollment Method set to **Manual** (the default).
 - In the Encryption Algorithm field, select **3DES**.
 - In the Password field, type the password of your choice.
 - In the Key Size field, accept the default **1024**.
 - In the Certificate Validity field, accept the default, **1825**.

- In the Distinguished Name field, type the LDAP entries required by your CA. These entries must be in LDAP format and they must match the values required by your CA. If you are not sure what the required entries are, contact your CA.

Among the required entries will be the FQDN of the AE Server in LDAP format. Additionally you might need to provide your company name, your organization name and so on. Separate each LDAP entry with a comma, and do not use blank spaces, for example:

cn=myaeserver.example.com,ou=myOrganizationalUnit,o=Examplecorp,L=Springfield,ST=Illinois,C=US

Note:

Currently the Add Server Certificate page in the AE Services Management Console does not support using commas within a DN attribute (for example: **o=Examplecorp, Inc**).

- In the Challenge password and Re-enter Challenge Password fields, type the challenge password of your choice.
- In the Key Usage field, accept the default; by default nothing is selected.
- In the Extended Key Usage field, accept the default; by default nothing is selected.
- In the SCEP Server URL field, accept the default; by default this field is blank.
- In the CA Certificate Alias field, accept the default; by default this field is blank.
- In the CA Identifier field, accept the default; by default this field is blank.
- Click **Apply**.

AE Services displays the Server Certificate Manual Enrollment Request page, which displays the certificate alias and the certificate request itself in PEM (Privacy Enhanced Mail) format. The certificate request consists of all the text in the box, including the header (-----BEGIN CERTIFICATE REQUEST -----) and the trailer (-----END CERTIFICATE REQUEST-----).

5. Copy the entire contents of the server certificate, including the header and the trailer. Keep the contents available in the clipboard for the next procedure.

Procedure 5 - Creating a server certificate for AE Services

Use the appropriate procedure for creating a server certificate for AE Services.

- If you are using a third party certificate authority other than Microsoft Certificate Services, refer to [Generic procedure for creating a server certificate for AE Services](#) on page 69.
- If you are using Microsoft Certificate Services, refer to [Microsoft-based procedure for creating a server certificate for AE Services](#) on page 70.

Generic procedure for creating a server certificate for AE Services

These steps are provided as a general reference only -- follow the instructions on your CA's Web site.

1. From your browser, go your CA's Web page for requesting a server certificate.
2. Complete the required fields for enrollment. Usually you provide information such as your such as your name, email address, the IP address of your server, your organizational unit (OU), and the type of server you have.
3. Paste the CSR into the appropriate field and submit or upload the request. (You paste the certificate request that you copied in Step 5 of Procedure 4 on page 68).
4. The certificate authority processes your request and issues a server certificate for you to download.
5. Download the certificate to your AE Services administrative workstation, and save it with a unique name (for example, C:\aescert.cer).

**Important:**

The certificate data you import into AE Services must be PEM-encoded (Base 64).

- If your CA issues certificates in DER format, you must convert it to PEM before importing it into the AE Services Management Console. See [Converting a DER file to PEM](#) on page 67.

Microsoft-based procedure for creating a server certificate for AE Services

If you use Microsoft Certificate Services as the certificate authority, use this procedure as a guide for creating a server certificate for AE Services.

1. From your Web browser, type the URL of your certificate server. For example:
http://<certificate_server.com>/certsrv
where: <certificate_server.com> is the domain name or IP address of your certificate server.
2. On the Welcome page of Microsoft Certificate Services, click **Request a certificate**.
3. On the Request a Certificate page, click **advanced certificate request**.
4. On the Advanced Certificate Request page, click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**. (AE Services uses a base-64-encoded CMC).
5. On the Submit a Request or Renewal Request page, paste the certificate request into the Saved Request input field, select a template with clientAuth and serverAuth in the Certificate Template field, and then click **Submit**. (You paste the certificate request that you copied in Step 5 of Procedure 4 on page 68).
6. From the Certificate Issued page, select **Base 64 encoded**, and click **Download certificate**.

Note:

Some CAs are not set up to automatically grant certificates. If this case, you might have to wait until your administrator issues the certificate. Once your administrator issues the certificate, return to the Welcome page of Microsoft Certificate Services, and click **View the status of a pending certificate request** to get to the "Issued Certificate" page.

7. From the File download dialog box, save the certificate to your computer.

Procedure 6 - Importing the server certificate into AE Services

From the AE Services Management Console follow this procedure to import the AE Services server certificate into the AE Services Management Console. This procedure assumes that your certificate is in PEM format. If your certificate is in another format, see [Converting Certificate files in other formats for AE Services](#) on page 67.

Note:

Always install just the server certificate (as opposed to a PKCS7 certificate chain), but be sure to select **Establish Chain of Trust** as indicated in Step 6.

1. From the main menu of the AE Services Management Console, select **Security > Certificate Management > Server Certificates > Pending Requests**.
2. From the Pending Server Certificate Requests page, select the certificate alias you specified when you created the CSR for AE Services (based on the example, the alias is aeservercert), and then click **Manual Enroll**.
3. From the Server Certificate Manual Enrollment Request page, click **Import**. When you click **Import**, your browser displays the Server Request Import page.
4. Complete the Server Certificate Import page, as follows:
 - From the Certificate Alias list box, select the alias you used to generate this certificate request.
 - Accept the default for **Establish Chain of Trust** (by default it is selected).
 - Click **Browse** to locate the signed server certificate file you want to import.
 - Click **Apply**.

If the import is successful, AE Services displays the message: "Certificate imported successfully."

Procedure 6a - Verifying the installation of the server certificate in AE Services

Follow this procedure to verify the installation of the server certificate in AE Services.

1. In the AE Services Management Console, select **Security > Certificate Management > Server Certificates**.
2. From the Server Certificates page, select the alias of the server certificate (**aeservercert**, based on this sample scenario), and click **View**.
3. From the Server Certificate Details page, verify that the information for the server certificate is correct.
 - a. Verify that the Issued To field displays the fully qualified domain name of the AE Server.
 - b. Verify that the Issued By field Indicates fully-qualified domain name of the certificate authority that issued the server certificate.
 - c. Verify that the Expiration Date Indicates the date that the server certificate expires.
 - d. Verify the information in the Details window. Make sure the Certificate Status is valid.
4. Click **Close** to exit the Server Certificate Details page.



CAUTION:

AE Services allows only one server certificate at a time. If you install more than one server certificate and restart AE Services, the TR/87 service will fail to initialize.

Replacing an expired server certificate

Once a server certificate has expired, links or security features that rely on the validity of the certificate may fail. Because AE Services allows only one server certificate at a time, you must carefully manage the process of replacing an expired certificate.

If you have a certificate that is about to expire, you can install a new certificate without impacting AE Services. Before the server certificate expires, select the server certificate on the Server Certificate page and delete it. Once you have deleted the expired server certificate, restart the AE Server. When AE Services restarts the newly-installed certificate will go into effect.

Dial Plan settings in AE Services

AE Services uses the information on the Dial Plan settings pages to process phone numbers used in your configuration of the AE Services implementation for Live Communications Server. In AE Services you can use either of the following methods to administer dial plan settings.

- You can administer the dial plan settings for one switch at a time. For more information, see [Administering dial plan settings on a per-switch basis](#) on page 87.
- You can administer default dial plan settings that are used for all switches. For more information, see [Administering default dial plan settings](#) on page 89.

**Important:**

In configurations with one AE Server supporting multiple switches, AE Services does not support Microsoft Office Communicator control of the same extension on more than one switch.

Before you begin

Before you start the procedures to administer dial plan settings, make sure you are familiar with Tel URI formats and the dial plan conversion pages in the AE Services Management Console. Tel URI is an abbreviation for Telephony Uniform Resource Identifier, sometimes it is expressed as "TelURI." the AE Services Management Console is an abbreviation for Operations, Administration and Maintenance.

- To familiarize yourself with Tel URI formats, see [About Tel URI formats and device IDs](#) on page 74.
- For information about using the AE Services Management Console pages to create dial plan conversion rules for converting E.164 phone numbers to switch extensions and switch extensions to E.164 phone numbers, see [About the From TelURI and To TelURI rules](#) on page 75.

To complete the dial plan settings in the AE Services Management Console, you need to know how the dial plan is administered for on Communication Manager. If you do not know what the dial plan settings are for a particular switch or set of switches, contact the Communication Manager administrator.

About Tel URI formats and device IDs

[Table 6](#) describes the supported Tel URI formats that AE Services supports. The preferred format is E.164, except in cases where the extension bears no resemblance to the E.164 number.

Calling device and monitored device ID: AE Services expects the calling device and monitored devices to be in either E.164PlusExt format or E.164 format. The extOnly format should be used only if there is no correlation between the E.164 number and the extension.

Called device ID: Called device IDs will not be in E.164PlusExt format, but they could be in any of the other formats listed in [Table 6](#).

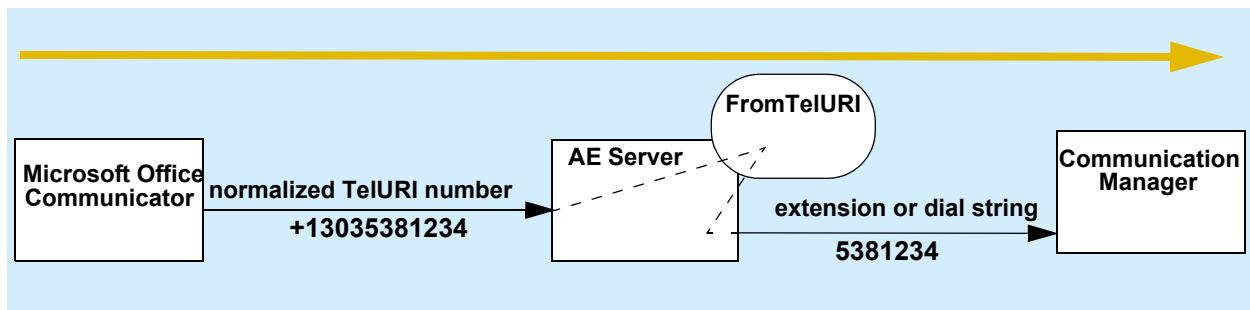
Table 6: Tel URI formats supported by AE Services

Format	Example
E.164	tel:+13035389000
E.164PlusExt	tel:+13035389000;ext=1234
extOnly	tel:5389000;phone-context=<domain> where <domain> can be any organization's domain name tel:5380112;phone-context=example.com

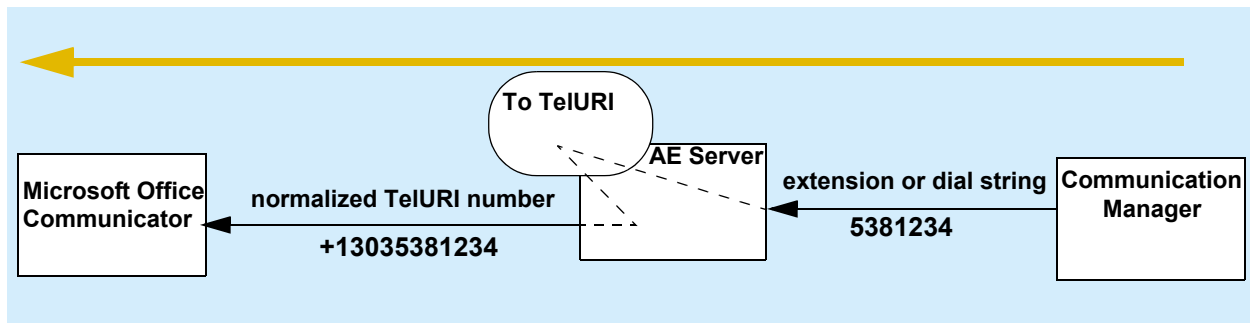
About the From TelURI and To TelURI rules

The dial plan conversion pages ("Dial Plan Settings - Conversion Rules for Default" and "Dial Plan Settings - Conversion Rules - switchname") in the AE Services Management Console are used for setting up conversion rules for a switch connection. The conversion rules are expressed as two tables in the AE Services Management Console, "From TelURI" and "To TelURI."

From TelURI: The term "From TelURI" is a shorthand way of saying "convert from a normalized TelURI number to an extension or dial string," which is handed off to the switch (Communication Manager).



To TelURI: The term "To TelURI" is a shorthand way of saying "convert from an extension or dial string to a normalized TelURI," which is handed off to Microsoft Office Communicator.



TelURI settings - how incoming and outgoing numbers are processed

Use the first two topics in this section ([The From Tel URI table](#) and [The To TelURI table](#)) to get a basic idea of how the From and To TelURI settings in AE Services work. Because the From TelURI settings and the To TelURI settings function as logic tables, this document often refers to them as the From TelURI table and the To TelURI table.

Before you administer the dial plan settings in the AE Services Management Console, review the topics that are appropriate for your switch.

If your switch uses a dial plan with fixed-length extensions, see the following topics:

- [From TelURI settings for fixed-length extensions](#) on page 79
- [To TelURI settings for fixed-length extensions](#) on page 81

If your switch uses a dial plan with variable-length extensions, see the following topics:

- [From TelURI settings for variable-length extensions](#) on page 82
 - [To TelURI settings for variable length extensions](#) on page 84
-

Pattern matching -- using Pattern and RegEx (regular expressions)

You can use one of the following two methods of "analyzing" or "matching" dial plan strings, as follows:

- **Pattern** - Select **Pattern** when you want to use a digit string as a way of detecting the presence of a specific sequence of digits in an incoming dial string. When you select Pattern you can create a matching string based on literal digits (0 through 9), one character literal (the #), and one special character, the asterisk (*) which will match any digit or sequence of digits. If you select **Pattern**, valid dial string characters are: all digits (0-9), the number sign (#), and the asterisk (*). The minimum length and maximum length fields important aspects to consider when writing a pattern match rule.
- **RegEx** - Select **RegEx** (regular expression) when you want to use a Java regular expression to analyze an incoming dial string. In certain cases (especially variable extension), RegEx rules will allow an administrator to minimize the number of rules that must be administered.

Regular expressions rely on symbolic notation - grouping of digits and special characters for analyzing incoming dial strings. For example, ([0-5]\\d{0,3}) is a regular expression which matches extensions that start with digits 0 - 5, and are 1 to 4 digits in length. Specifying a minimum, maximum, or delete length do not apply to regular expressions.

You can mix rule types

A From TelURI table in the AE Services Management Console can consist of rules based on the **Pattern** setting and rules based on the **RegEx** setting. That is, you can create a From TelURI table that uses rules based on Pattern and rules based on RegEx.

Valid dial string characters and using the asterisk

This information about using the asterisk applies only to pattern matching rules; it does not apply to regular expression (RegEx) rules.

For AE Services dial plan settings, valid dial string characters are: all digits (0-9), the number sign (#), and the asterisk (*).

The asterisk or number sign as literals

If your dial plan uses the asterisk or the number sign, and you need to configure a dial plan rule that detects the asterisk and the number sign, you must precede them with a backslash. For example to interpret the asterisk as a literal you would use * and to interpret the number sign as a literal you would use \# .

For example, if you need to have the asterisk interpreted as a literal asterisk in either the Matching Pattern field or the Replacement String Field of a From TelURI or a To TelURI table, you must precede the asterisk with a backslash. If you do not precede the asterisk with a backslash, it will be interpreted as a wildcard value for any valid character.

The asterisk as a wildcard

When you want to use the asterisk as a wildcard for any character, you must use it as a single character (by itself). That is, when used as a wildcard, the asterisk can not be preceded or followed by any other character.

The From Tel URI table

The **From TelURI** table in the AE Services Management Console determines the way that AE Services processes inbound E.164 numbers. Generally speaking, AE Services applies matching criteria to the incoming number. When the number satisfies the matching criteria, AE Services manipulates the digits and passes the number to Communication Manager (only one rule is applied for each number). When setting up the From TelURI settings, you can specify up to 200 rules. Each row in the table represents a rule. The rules are processed in order from top to bottom.

If you have a rule that contains a wildcard (* - asterisk) for the Minimum Length, Maximum Length, and Pattern match, it always must be the last rule in the list, and it must be a single asterisk (by itself). If you need to treat the asterisk as a literal in either the Pattern Match or the Replacement fields, you must precede it with a backslash, for example: *. Also, if your dial plan uses a number sign and you need to treat it as a literal in the Pattern Match field, you must precede it with a backslash.

Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
11	11	1303538	4	(field is empty)
11	11	1303	1	9
*	*	*	0	9011

The To TelURI table

The **To TelURI** table in the AE Services Management Console determines the way that the AE Services processes outbound E.164 numbers. Generally speaking, AE Services applies matching criteria to the outgoing number. When the number satisfies the matching criteria, AE Services manipulates the digits and passes the number to Microsoft Office Communicator (only one rule is applied for each number). When setting up the To TelURI settings, you can specify up to 200 rules. Each row in the table represents a rule. The rules are processed in order from top to bottom.

If you have a rule that contains a wildcard (* - asterisk) for the Minimum Length, Maximum Length, and Pattern match, it always must be the last rule in the list, and it must be a single asterisk (by itself). If you need to treat the asterisk as a literal in either the Pattern Match or the Replacement fields, you must precede it with a backslash, for example: *. Also, if your dial plan uses a number sign and you need to treat it as a literal in the Pattern Match field, you must precede it with a backslash.

Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
7	7	538	0	1303

Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
7	7	852	0	1732
10	10	*	0	1

From TelURI settings for fixed-length extensions

The following example demonstrates how to administer the **From TelURI** settings in the AE Services Management Console to support a dial plan for a switch using fixed-length-extensions. This switch supports three different extension prefixes: 538, 852, and 444. The 538 prefix is used for extensions hosted on that switch, and the other two prefixes are used for switches connected via QSIG.

Example - From TelURI rules for fixed-length extensions

	Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
A	11	11	1303538	4	(blank) ¹
B	11	11	1732852	4	(blank)
C	11	11	1720444	4	(blank)
D	11	11	1303	1	9
E	11	11	1720	1	9
F	11	11	1	0	9
G	*	*	*	0	9011

1. Blank means the replacement field is empty.

How the From TelURI rules process numbers for fixed-length extensions

- A** AE Services receives **+13035381234**, an 11-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 7 digits (**1303538**) are a pattern match, AE Services deletes the first 4 digits (**1303**) and does not prepend any digits. AE Services sends **5381234** to the switch.
- B** AE Services receives **+17328521234**, an 11-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 7 digits (**1732852**) are a pattern match, AE Services deletes the first 4 digits (**1732**) and does not prepend any digits. AE Services sends **8521234** to the switch.
- C** AE Services receives **+17204441234**, an 11-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 7 digits (**1720444**) are a pattern match, AE Services deletes the first 4 digits (**1720**) and does not prepend any digits. AE Services sends **4441234** to the switch.

- D** AE Services receives **+13036791234**, an 11-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 4 digits (**1303**) are a pattern match, AE Services deletes the first digit (**1**), and prepends **9** to the number. AE Services sends **93036791234** to the switch.
- E** AE Services receives **+17202891234**, an 11-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 4 digits (**1720**) are a pattern match, AE Services deletes the first digit (**1**), replaces it with a **9**. AE Services sends **97202891234** to the switch.
- F** AE Services receives **+18183891234**, an 11-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first digit (**1**) is a pattern match, AE Services deletes no digits, and prepends a **9** to the number. AE Services sends **918183891234** to the switch.
- G** AE Services receives **+4926892771234**, a 13-digit number, from Communication Manager. Because the minimum length, maximum length, and pattern match are set up with the wild card, any number is permitted. AE Services deletes no digits, prepends **9011** to the number and sends **90114926892771234** to the switch.

To TelURI settings for fixed-length extensions

The following example demonstrates how to administer the **To TelURI** settings in the AE Services Management Console to support a dial plan for a switch using fixed-length-extensions. This switch supports three different extension prefixes: 538, 852, and 444. The 538 prefix is used for extensions hosted on that switch, and the other two prefixes are used for switches connected via QSIG.

Example - To URI rules for fixed-length extensions

	Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
A	7	7	538	0	1303
B	7	7	852	0	1732
C	7	7	444	0	1720
D	5	5	2	0	173285
E	5	5	4	0	172044
F	10	10	*	0	1

How the To TelURI rules process numbers for fixed-length extensions

- A** AE Services receives **5381234**, a 7 digit number, from the switch. Because the number is within the minimum and maximum length requirements, and the first three digits (**538**) are a pattern match, AE Services deletes no digits, and prepends **1303** to the number. AE Services sends **+13035381234** to Communicator.
- B** AE Services receives **8521234**, a 7 digit number, from the switch. Because the number is within the minimum and maximum length requirements, and the first three digits (**852**) are a pattern match, AE Services deletes no digits, and prepends **1732** to the number. AE Services sends **+17328521234** to Communicator.
- C** AE Services receives **4441234**, a 7-digit number, from the switch. Because the number is within the minimum and maximum length requirements, and the first three digits (**444**) are a pattern match, AE Services deletes no digits, and prepends **1720** to the number. AE Services sends **+17204441234** to Communicator.
- D** AE Services will sometimes receive a 5 digit extension from a networked switch, even if the local dial plan is 7 digits (see [Dial Plan tips](#) on page 87). In this case, AE Services receives a 5 digit number **21234**. Based on the matching pattern of **2** at the beginning, AE Services prepends **173285** to the number and sends **+17328521234** to Communicator.
- E** AE Services will sometimes receive a 5 digit extension from a networked switch, even if the local dial plan is 7 digits (see [Dial Plan tips](#) on page 87). In this case, AE Services receives a 5 digit number **41234**. Based on the matching pattern of **4** at the beginning, AE Services prepends **172044** to the number and sends **+17204441234** to Communicator.
- F** AE Services receives a 10-digit number, **2126711234** from the switch. Based on the matching pattern of any 10-digit string, AE Services deletes no digits and prepends **1** to the number. AE Services sends **+12126711234** to Communicator.

From TelURI settings for variable-length extensions

The following example demonstrates how to administer the **From TelURI** settings in the AE Services Management Console to support a dial plan that uses variable-length extensions. This example assumes the following:

- The customer owns numbers +4969100 through +4969105 in the dial plan, but does not own +4969106 and higher.
- The dial plan accommodates 1- to 4-digit extensions
- The ARS code is 0, the inter-region code is 0, and the international dial code is 00. The ARS code, which in this case is 0, is always included before the inter-region code and international dial code.

Example - From TelURI rules for variable-length extensions

	Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
A	8	11	49697100	7	(blank) ¹
B	8	11	49697101	7	(blank)
C	8	11	49697102	7	(blank)
D	8	11	49697103	7	(blank)
E	8	11	49697104	7	(blank)
F	8	11	49697105	7	(blank)
G	*	*	4969	4	0
H	*	*	49	2	00
I	*	*	*	0	000

1. Blank means the replacement field is empty.

How the From TelURI rules process numbers for variable-length extensions

- A** AE Services receives **+49697100**, an 8-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the number is an exact pattern match, AE Services deletes the first 7 digits (**4969710**) and does not prepend any digits to the number. AE Services sends **0** to Communication Manager.
- B** AE Services receives **+49697101988**, an 11-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 8 digits (**49697101**) are a pattern match, AE Services deletes the first 7 digits and does not prepend any digits to the number. AE Services sends **1988** to Communication Manager.
- C** AE Services receives **+4969710211**, a 9-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 8 digits (**49697102**) are a pattern match, AE Services deletes 7 digits and does not prepend any digits to the number. AE Services sends **211** to Communication Manager.

- D** AE Services receives **+496971034**, a 9-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 8 digits (**49697103**) are a pattern match, AE Services deletes 7 digits and does not prepend any digits to the number. AE Services sends **34** to Communication Manager.
- E** AE Services receives **+4969710494**, a 10-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 8 digits (**49697104**) are a pattern match, AE Services deletes 7 digits and does not prepend any digits to the number. AE Services sends **494** to Communication Manager.
- F** AE Services receives **+4969710598**, a 10-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 8 digits (**49697105**) are a pattern match, AE Services deletes 7 digits and does not prepend any digits to the number. AE Services sends **598** to Communication Manager.
- G** AE Services receives **+496971060**, a 9-digit number, from Communicator. Because the wild card (*) permits a number of any length, and the first 4 digits (**4969**) are a pattern match, AE Services deletes the first 4 digits and prepends **0** to the number. AE Services sends **071060** to Communication Manager.
- H** AE Services receives **+49306441234**, an 11-digit number from Communicator. Because the wild card (*) permits a number of any length, and the first 2 digits (**49**) are a pattern match, AE Services deletes the first 2 digits and prepends **00** to the number. AE Services sends **00306441234** to Communication Manager.
- I** AE Services receives **+17328521234**, an 11 digit number, from Communicator. Because the minimum length, maximum length, and pattern match are set up with the wild card, any number is permitted. AE Services deletes no digits, prepends **000**, and sends **00017328521234** to Communication Manager.

To TelURI settings for variable length extensions

The following example demonstrates how to administer the **To TelURI** settings in the AE Services Management Console to support a dial plan that uses variable-length extensions. The set of rules in this example assumes the following:

- All numbers less than or equal to 4 digits are extensions. This assumption allows the table to have one rule, rather than 6, for all extension starts. In some cases, it might be necessary to be more specific.
- International numbers start with 00, and inter-region numbers start with 0. Any digits other than 0 or 00 are assumed to be local digits. AE Services prepends 4969, which represents country or city codes. Keep in mind that you must carefully analyze your dial plan before you attempt to apply a catch-all rule such as this.

Example - To TelURI rules for an installation with variable length extensions

	Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
A	1	4	*	0	4969710
B	*	*	00	2	
C	*	*	0	1	49
D	*	*	*	0	4969

How the To TelURI rules process numbers for variable length extensions

- A** AE Services receives **1234**, a 4-digit number from the switch. Because the number is within the minimum and maximum length requirements, and the wild card (*) permits a match of any 1- to 4-digit number, AE Services deletes no digits and prepends **4969710** to the number. AE Services sends **49697101234** to Microsoft Office Communicator.
- B** AE Services receives **0017328524321**, a 13-digit number, from the switch. Because the number is not within the range specified by the 1- to 4-digit rule (A) it satisfies this rule, which permits a number of any length where first two digits (**00**) are a pattern match. AE Services deletes the first 2 digits, prepends nothing to the number, and sends **17328524321** to Microsoft Office Communicator.
- C** AE Services receives **0306441234**, a 10-digit number, from the switch. Because the number is not within the range specified by the 1- to 4-digit rule (A) it satisfies this rule, which permits a number of any length where first digit (**0**) is a pattern match. AE Services deletes the first digit, prepends **49** to the number, and sends **49306441234** to Microsoft Office Communicator.
- D** AE Services receives **45427**, a 5-digit number, from the switch. Because the number is not within the range specified by the 1- to 4-digit rule (A) it satisfies this "catch-all" rule that permits a number of any length and any pattern of digits. AE Services deletes no digits, prepends **4969** to the number, and sends **496945427** to Microsoft Office Communicator.

Pattern matching -- using Pattern and RegEx (regular expressions)

You can use one of the following two methods of "analyzing" or "matching" dial plan strings, as follows:

- **Pattern** - Use Pattern when you want to use a digit string as a way of detecting the presence of a specific sequence of digits in an incoming dial string. When you select Pattern you can create a matching string based on literal digits (0 through 9), one character literal (the #), and one special character, the asterisk (*) which will match any digit or sequence of digits. If you select **Pattern**, valid dial string characters are: all digits (0-9), the number sign (#), and the asterisk (*).
- **RegEx** - Use RegEx (regular expression) when you want to use a Java regular expression to analyze an incoming dial string. Regular expressions rely on symbolic notation - grouping of digits and special characters for analyzing incoming dial strings. For example, ([0-5]\\d{0,3}) is a regular expression which matches extensions that start with digits 0 - 5, and are 1 to 4 digits in length. If you are using regular expressions, you have the option of specifying a minimum, maximum or delete length. Specifying a minimum, maximum, or delete length fields do not apply to regular expressions. These field apply to pattern matching only.

You can mix rule types : A From the TelURI table in the AE Services Management Console can consist of rules based on the **Pattern** setting and rules based on the **RegEx** setting. That is, you can create a From TelURI table that uses rules based on Pattern and rules based on RegEx.

Using the asterisk : If you have a rule that contains an asterisk (*) for the Minimum Length, Maximum Length, and Pattern match it must be the last rule in the list.

[Table 7](#) is an example that depicts a mix of regular expression rules and simple pattern match rules.

Table 7: Example of Incoming rules for RegEx

	Min length	Max length	Pattern	Delete Length	Replacement
A			4969710([0-5]\\d{0,3})		\$1
B			4969(\\d{1,})		0\$1
C	*	*	49	2	00
D	*	*	*	1	000

- A** This rule uses a RegEx pattern to specify that Call Control Services is to look for a string starting with **4969710**, matching an extension that starts with **0** through **5** and is **1** to **4** digits in length.
- The parentheses around the extension indicate a group, which is correlated with the **\$1** in the replacement string. The **\$1** says to replace the matching string (the entire E.164 number) with the group designated by the parentheses (the extension). For example, the incoming string **496971001234** would be converted to **01234**. As another example, the incoming string **49697102123** would be converted to **2123**.
- B** This rule uses a RegEx pattern to specify that Call Control Services is to look for a string starting with **4969**, followed by 1 or more digits.
- The parentheses again correlate with the **\$1** in the replacement string, which says to take the group (the E.164 number without country code or city code) and to add a **0** in front of it (the ARS code). For example, the incoming string **49695671234** would be converted to **05671234**.
- C** This rule uses a simple pattern match. The asterisk in the Min and Max length permits a number of any length. The pattern indicates that Call Control Services is to look for a string starting with **49**. When it detects 49, it deletes the first 2 digits, and replaces them with **00**. For example, the incoming string **49891234567** would be converted to **00891234567**.
- D** This rule uses a wildcard pattern match. The asterisk in the Min and Max length permits a number of any length, and the asterisk in the pattern permits pattern of digits. When any number that does not satisfy the first 3 rules (A,B, and C) is detected, Call Control Services deletes the first digit and replaces it with **000**. For example, the incoming string **13035391234** would be converted to **0003035391234**.

Dial Plan tips

When switches are networked together using ISDN QSIG tie trunks or ISDN tie trunks, in some call scenarios Communication Manager sends extension numbers from the networked switch to the AE Server. The format of these extension numbers may be different than the format of local extension numbers.

To optimize the experience of Microsoft Office Communicator users, be sure to administer "To TelURI" rules for the networked switch, or switches, as well as the local switch. Additionally, if the networked switch has a different extension length than the local switch, extensions might be reported with both the local extension length and the networked extension length. Be sure to administer "To TelURI" rules that can successfully convert both extension lengths for the networked switch.

Also, you might need multiple entries in the "To TelURI" rules for the networked switch if that switch has a different extension length than the local switch.

Administering dial plan settings on a per-switch basis

Follow this procedure to administer the dial plan settings for a switch connection you have already administered the AE Services Management Console. AE Services uses the dial plan information to convert E.164 phone numbers to switch extensions (From TelURI) and switch extensions to E.164 phone numbers (To TelURI). For more information, see [About the From TelURI and To TelURI rules](#) on page 75.

Note:

If your configuration of the AE Services implementation for Live Communications Server uses a number of switches that all have the same dial plan, use the procedure described in [Administering default dial plan settings](#) on page 89. By using the default settings, you enter the dial plan settings only once.

1. From the browser on your AE Services administrative workstation, log in to the AE Services Management Console.
2. Select **Communication Manager Interface > Dial Plan > Switch Administration**.
3. From the Switch Dial Plan Administration page, select the connection name for the switch you want to administer, for example **aeslcs switch**, and click **Details**.

AE Services displays the Dial Plan Settings - Conversion Rules for **aeslcs switch** page. This page provides you with a way to Add, Edit, Delete and Reorder "From TelURI" conversion rules and "To TelURI" conversion rules. The Edit, Delete, and Reorder functions apply to existing rules. This example assumes the initial state of the page -- no conversion rules exist -- and focuses on adding two conversion rules, one for From TelURI and one for To TelURI.

4. Follow Step a to add a From TelURI conversion rule, and follow Step b to add a To TelURI conversion rule.
 - a. In the From TelURI section of the page, under the blank display area, click **Add**.
 1. From the Add Dial Plan to aeslcs switch page, complete the fields for the **From TelURI** settings, based on your dial plan.
 2. Click **Apply Changes**. Your browser displays the Add Dial Plan page, which asks you to confirm your dial plan changes. From the Add Dial Plan page, click **Apply**.

At this point you have added one From TelURI conversion rule. If you want to add another From TelURI conversion rule, you must repeat Steps a, 1, and 2.
 - b. In the To TelURI section of the page, under the blank display area, click **Add**.
 1. From the Add Dial Plan to aeslcs switch page, complete the fields for the **To TelURI** settings, based on your dial plan.
 2. Click **Apply Changes**. Your browser displays the Add Dial Plan page, which asks you to confirm your dial plan changes. From the Add Dial Plan page, click **Apply**.

At this point you have added one To TelURI conversion rule. If you want to add another To TelURI conversion rule, you must repeat Steps b, 1, and 2.

At this point the changes you made to your dial plan settings are in effect, and you do not have to restart the AE Server.

Administering default dial plan settings

If you use more than one switch in your configuration of the AE Services implementation for Live Communications Server, and all the switches have common dial plan settings, you can use the Default Dial Settings page as a template. When you add a switch connection for AE Services implementation for Microsoft LCS, the dial plan settings that you have administered on the Default Dial Plan settings page are applied to that switch connection. Use this procedure to set up the Default Dial Settings page.

1. From the browser on your AE Services administrative workstation, log in to the AE Services Management Console.

2. Select **Communication Manager Interface > Dial Plan > Default Settings**.

AE Services displays the Dial Plan Settings - Conversion Rules for default page. This page provides you with a way to Add, Edit, Delete and Reorder "From TelURI" conversion rules and "To TelURI" conversion rules. The Edit, Delete, and Reorder functions apply to existing rules. This example assumes the initial state of the page -- no conversion rules exist -- and focuses on adding two conversion rules, one for From TelURI and one for To TelURI.

3. Follow Step a to add a From TelURI conversion rule, and follow Step b to add a To TelURI conversion rule.

- a. In the From TelURI section of the page, under the blank display area, click **Add**.

1. From the Add Dial Plan to default page, complete the fields for the From TelURI settings, based on your dial plan.
2. Click **Apply Changes**. Your browser displays the Add Dial Plan page, which asks you to confirm your dial plan changes." From the Add Dial Plan page, click **Apply**.

At this point you have added one From TelURI conversion rule. If you want to add another From TelURI conversion rule, you must repeat Steps a, 1, and 2.

- b. In the To TelURI section of the page, under the blank display area, click **Add**.

1. From the Add Dial Plan to default page, complete the fields for the To TelURI settings, based on your dial plan.
2. Click **Apply Changes**. Your browser displays the Add Dial Plan page, which asks you to confirm your dial plan changes. From the Add Dial Plan page, click **Apply**.

At this point you have added one To TelURI conversion rule. If you want to add another To TelURI conversion rule, you must repeat Steps b, 1, and 2.

At this point the changes you made to your dial plan settings are in effect, you do not have to restart the AE Server.

Administering AE Services access to Active Directory

Follow this procedure to set up the connection to Active Directory for AE Services.

- The examples in this procedure use the "example.com" domain name.
- See also, [DN entries and scope of search](#) on page 92 for a diagram depicting Distinguished Names.
- 1. From the browser on your AE Services administrative workstation, log in to the AE Services Management Console.
- 2. Select **Security > Enterprise Directory**.
- 3. Complete the Enterprise Directory page, as follows.
 - User DN for Query Authentication - Type the DN for the user object that AE Services uses for accessing the Active directory. Based on how users are set up in Active Directory, the user object could correspond to a Full Name, a Display Name, or a User logon name. Here are two examples:

`cn=Grey\,AI,cn=sertech,cn=services,cn=users,dn=example,dc=com`

`cn=RTCAAdmin,cn=devtech,cn=services,cn=development,dc=example,dc=com`

Note:

If a DN attribute has a comma within it, you must precede it with a backslash. For more information, see [Making changes on the Enterprise Directory Configuration page](#) on page 93. If you are not sure what the DN is for a user object, see [Determining the DN for a user object](#) on page 93.

- Password - Type a password to be used for Active Directory access; retype the same password in the Confirm Password field. This Active Directory password is stored in an encrypted format on the AE Server.
- Base Search DN - The Base Search DN is less specific than the User DN. Type the DN of the node that includes all user accounts that need access to the AE Services and Live Communications Server integration in the following format:

dc=avaya,dc=com
- HostName/IP Address - Type the IP address or Host Name of the Domain Controller that has the Global Catalog. Typically the host name would be the main domain controller i.e. avaya.com.
- Port - (used for Active Directory access) - Change the default port number to an appropriate value for your configuration. The default is 3268 (the default Global Catalog port).
- Secondary HostName/IP Address - Accept the default (leave the field blank). This field does not apply to the AE Services implementation for Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007.

- Secondary Port - Accept the default (leave the field blank). This field does not apply to the AE Services implementation for Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007.
 - User ID Attribute Name - This setting defaults to **uid**, which is the default for AE Services User Management. For Microsoft Active Directory you must change this setting. The default setting for Microsoft Active Directory is **samaccountname**. If your implementation does not use the default for Microsoft Active Directory, enter the name of the attribute that is appropriate for your implementation.
 - User Role Attribute Name - Enter the name of the attribute for the user role that your Enterprise Directory Server uses, for example roles.L
 - Change Password URL - Accept the default (leave the field blank). This field does not apply to the AE Services implementation for Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007.
 - LDAP-S - Select LDAP-S if your configuration uses a TLS connection from AE Services to your Enterprise Directory Server.
4. Select **Apply Changes** to put your changes into effect.

DN entries and scope of search

The DN entries you specify in the User DN for Query Authentication and the Base Search DN field are, in effect, search paths in an LDAP structure.

Consider the DN examples used in [Administering AE Services access to Active Directory](#) on page 90:

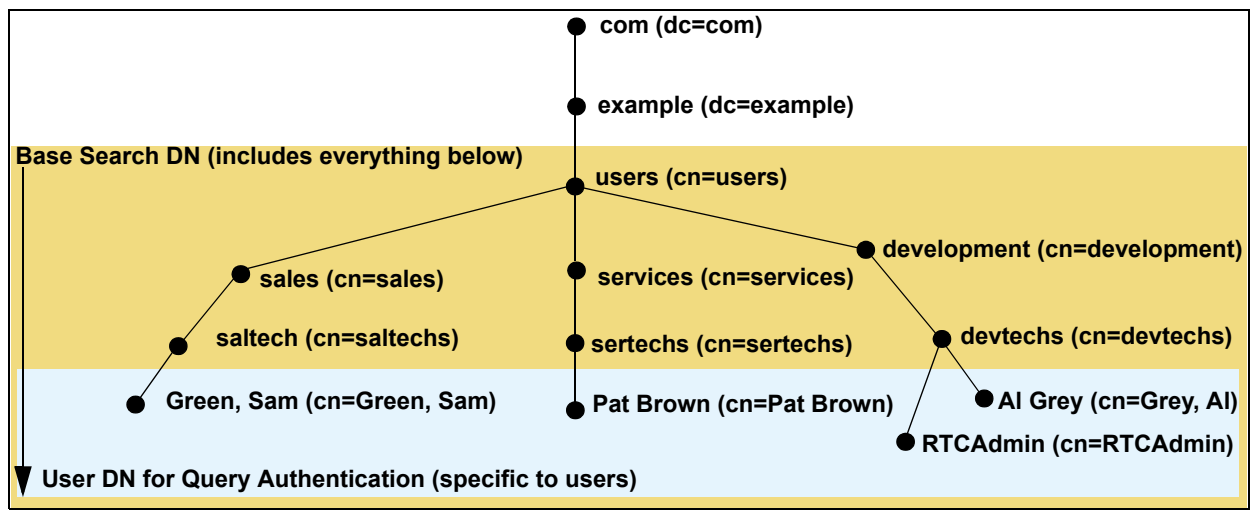
- User DN for Query Authentication
cn=Pat Brown,cn=sertech,cn=services,cn=users,dc=example,dc=com
- Base Search DN
cn=users,dc=example,dc=com

Both DNs are unique, but the User DN for Query Authentication is more specific than the Base Search DN.

Avoid making the Base Search DN too specific

If you were to specify a Base Search DN of **cn=development,cn=users,dc=example,dc=com** the users in services and sales would not be able to establish a session. Instead, you should specify a Base Search DN that is less specific, such as **cn=users,dc=example,dc=com**.

Figure 5: DN entries and scope of search



Making changes on the Enterprise Directory Configuration page

Follow these guidelines for completing the "User DN for Query Authentication" and the "Base Search DN" fields on the Enterprise Directory Configuration page in the AE Services Management Console.

If you are entering a DN attribute that has an internal comma, you must precede it with a backslash, for example: `cn=Green\,Sam,cn=saltech,cn=sales,cn=users,dc=example,dc=com` . This is necessary because the comma is a delimiter that is used for separating DN attribute-value pairs. When you click **Apply Changes**, AE Services processes the data you submit.

As a result of this processing, the backslash gets removed from any DN attributes that are in the "User DN for Query Authentication" and the "Base Search DN" fields. When the AE Services Management Console redisplay the Enterprise Directory Configuration Web page, these attributes will be displayed with a single backslash.

Note:

Whenever you are making changes to any of the fields on the Enterprise Directory Configuration page in the AE Services Management Console, make sure that each DN attribute with an internal comma is preceded by a backslash before you click **Apply Changes**.

Determining the DN for a user object

If you are not sure what the DN for the user object is, follow this procedure from the Active Directory Services domain controller.

1. At the command prompt, run the `csvde -f` command against the Users domain and save the output to a file (`csvde -f file.csv`).
2. Open the file with a text editor or a spreadsheet program and locate the appropriate user object (which can be the Full Name, Display Name, or User logon name on the Active Directory User Properties dialog).
3. Copy the DN for the user object, and paste it into User DN for Query Authentication field in the AE Services Management Console.

Configuring Live Communications Server for AE Services

When you set up the Microsoft Live Communications Server, you will need to make sure that you have followed the necessary steps for configuring the server. These steps are listed in "Configuring the Server" (a subsection of "Deploying Telephony") in the *Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide*. Use this table as a guideline as you read through "Configuring the Server" in the *Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide*.

Steps listed in Microsoft Telephony Planning and Deployment Guide		Notes
1	Update Live Communications Server schema.	Completed when you carried out the Active Directory Preparation Basic Steps (see Task 2 in Table 1: Checklist for Live Communications Server on page 38).
2	Normalize the phone numbers.	Completed when you set up the Address Book Service (see Task 9 in Table 1: Checklist for Live Communications Server on page 38).
3	Enable RCC Extensions.	Follow the procedure for Enabling Remote Call Control in Active Directory on page 95 of this document. Also, see the Tip following this table.
4	Set up connections.	Follow the procedure for Setting up connections on page 96 of this document.
5	Set up static routes.	Follow the procedures for Configuring a static route on page 97 and Specifying the AE Server as an authorized host on page 98.
6	Set controlled line configuration.	This is accomplished when you complete the three previous tasks: 3) Enable RCC Extensions, 4) Set up connections, and 5) Set up Static Routes.
7	Configure a CTI link.	Completed when you administered a CTI link on Communication Manager, and you administered a TSAPI link in the AE Services Management Console.
8	Configure PBX SIP Proxy.	Not applicable. In terms of the Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide, the AE Server performs the role of the RCC Gateway only. The SIP/PSTN Gateway and the PBX-SIP Proxy do not apply to the AE Services implementation for Microsoft LCS.



Tip:

Microsoft provides a utility called **Office Communicator 2005 Phone Normalization Script** that enables you to make bulk changes to Active Directory. If you run this utility, you do not have to do per-user manual administration. To get this phone normalization script, go to www.microsoft.com, and locate **Live Communications Server 2005 with SP1 Resource Kit**. The resource kit includes this phone normalization script.

Enabling Remote Call Control in Active Directory

Enabling Remote Call Control in Active Directory refers to setting up users so they can control their phones from the Microsoft Office Communicator client. Follow this procedure to enable a specific user to control a specific phone from Microsoft Office Communicator.

1. From the Live Communications Server, start the management console for **Active Directory Users and Computers**.
2. From the left pane of the console, select **Active Directory Users and Computers**.
3. Expand the tree for your pool node (or server node), and click **Users**.
4. From the list of users in the right pane, right click a user name, and select **Properties**.
5. From the Properties dialog box, select the **Live Communications** tab.
6. From the Live Communications tab, click **Advanced Settings**. Live Communications Server displays the User Advanced Settings dialog box.

The image shows the 'User Advanced Settings' dialog box. It has three main sections: Federation Settings, Remote Call Control, and Archiving Settings. In Federation Settings, 'Enable remote user access' is checked. In Remote Call Control, 'Enable Remote Call Control' is checked, and the 'TEL URI' radio button is selected with the value 'tel:+13035389000'. The 'SIP URI' is 'sip:jane@example.com' and the 'Remote Call Control SIP URI' is 'sip:aes@myaesserver.example.com'. In Archiving Settings, 'Use global default archiving setting' is selected.

7. Click the option button for TEL URI, and type the appropriate telephone number in Tel URI format. For example: **tel:+13035389000**.

Note:

If necessary, you can use the following format: **tel:E.164 phone number;ext=extension** (for example, **tel:+13035389000;ext=9000**).

In most cases, the extension (ext=extension) is not required. It is required only under these circumstances:

- If the user's extension does not match the last digits of their E.164 Direct Inward Dial (DID) number.
- If the dial plan information has not been configured for the user's switch.

8. In the Remote Call Control SIP URI field, type the destination URI in the following format:
`sip:aes@AE_server_FQDN`.

where: **aes** is the identifier for the AE Server and **AE_server_FQDN** is a term you substitute with the fully qualified domain name of your AE Server. For example:

`sip:aes@myaesserver.example.com` .

Setting up connections

From the management console of the Live Communications Server, follow these steps to set up the connection that Live Communications Server uses for sending and receiving SIP messages.

1. Start the management console from the Live Communications Server
2. Expand the tree to display the FQDN of the server node, and right-click on the fully qualified domain name the Live Communications Server, for example:
mylcsserver.example.com
3. From the "mylcsserver.example.com" Properties dialog box, click **Add**.
4. From the Add Connection dialog box, under Transport Type, select **TLS** from the pull-down, and in the "Listen on this port" field, type **5061**. Click **Select Certificate...** .
5. From the Select Certificate dialog box, select the certificate for the fully qualified domain name of the Live Communications Server, and click **OK**.

Configuring a static route

Handling SIP traffic from the Live Communications Server to AE Services requires creating a static route between the Live Communications Server (or servers) and the AE Services server. This procedure is based on a configuration using Live Communications Server 2005 Enterprise Edition.

Follow this procedure to configure a static route between the Live Communications Server and the AE Services Server.

1. Open the Live Communications Server 2005 administrative snap-in: Click **Start**, point to **All Programs > Administrative Tools**, and click **Live Communications Server 2005**.
2. In the left pane of the administrative snap-in, expand the **Forest** node, and then expand **Live Communications servers and pools**. (For Standard Edition, **Live Communications servers and pools** represents the server node; for Enterprise Edition, it represents the pool node.)
3. Depending on whether you use Server Standard Edition or Enterprise Edition, right-click the **<server name>** (for Standard Edition) or the **<pool name>** (for Enterprise Edition) and select **Properties**.
4. From the Properties dialog box, select the **Routing** tab, and click **Add**.
5. Complete the fields on the Add Static Route dialog box as follows:
 - a. In the User field, type **aes**.
 - b. In the Domain field, type the fully qualified domain name of the AE Server (for example, **myaeserver.example.com**).
 - c. In the Network address field, type the fully qualified domain name of the AE Server (for example, **myaeserver.example.com**).
 - d. In the Transport field, select **TLS**.
 - e. In the Port field, type the port that was administered as the **TR87 Port** in the AE Services Management Console. The default is **4723**.
 - f. (The next two steps apply to Live Communications Server Standard Edition only.)
 1. Click **Select Certificate**.
 2. From the Select Certificate dialog box, select the **<Live Communications Server certificate>**, and click **OK** to close the Select Certificate dialog box. Continue with Step g.
 - g. Click **OK** to close the Add Static Route dialog box.

Specifying the AE Server as an authorized host

Follow this procedure to set up AE Services as an authorized host. This procedure is based on a configuration using Live Communications Server 2005 Enterprise Edition.

1. Open the Microsoft Office Live Communications Server 2005 management console, and in the left pane, expand the **Forest** node.
2. Right-click **Live Communications servers and pools** (the pool node), and select **Properties**.
3. From the Properties dialog box, select the **Host Authorization** tab, and click **Add**.
4. Complete the fields on the Add Authorized Host dialog box as follows:
 - a. In Network address field, type the fully qualified domain name of the AE Server (for example, **myaeserver.example.com**).
 - b. Select the check boxes (enable) for the following settings: **Throttle as server** and **Treat As Authenticated**. Make sure that **Outbound only** is not checked (disabled).
 - c. Click **OK**.

For more information about setting up host authorization, refer to the figure called "Edit Authorized Host" in the *Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide*.

Microsoft Office Communicator users - group policy settings

Microsoft Office Communicator users must have the following features configured as policy settings:

- Enable Computer to Phone Calls
- Enable Phone Control

For information about group policy settings, see "Group Policy Configuration (.adm)," in *Microsoft Office Communicator 2005 Planning and Deployment*.

About authentication and authorization

For the AE Services implementation for Microsoft LCS, authentication and authorization are handed as follows.

- AE Services authenticates Live Communications Server by using TLS to verify the Live Communications Server certificate.
- The Live Communications Server authenticates (confirms the identity) of the Microsoft Office Communicator user.
- The AE Server, in turn, authorizes (grants permission to) the user for device control.
- To carry out authorization, AE Services verifies that the requested Tel URI matches the Tel URI in the user record before granting access to a device.

Note:

When you complete the procedure to enable the Communicator client for RCC, ([Enabling Remote Call Control in Active Directory](#) on page 95) you are provisioning Active Directory with the user information that AE Services queries for.

Administering Live Communications Server 2005 for the agent login ID

Perform the following steps before signing in to Microsoft Office Communicator as an agent.

1. Log in to the Microsoft Office Live Communications Server 2005 server and open the Microsoft Office Live Communications Server 2005 console.
2. Click on **Live Communications servers and pools**, and select **Users**.
3. Right-click on the agent's **Display Name** and select **Properties**.
4. Click on **Advanced Settings...**
5. Enter the Tel URI parameter using the following format:

tel:agentID;phone-context=agent-login-id.domain

For example **tel:1234;phone-context=agent-login-id.example.com**

where:

- **agentID** is the agent's login ID, for example **1234**.
 - **example.com** is the domain name.
6. Next, have the agent log in to the Telephone / Softphone / Agent software that is to be used.
 7. Finally, have the agent sign in to Microsoft Office Communicator and verify that calls can be answered and made successfully.



Important:

Always sign out of Microsoft Office Communicator before logging off the physical device to ensure that the Microsoft Office Communicator sign in and the agent login states are always synchronized.

Re-synchronizing states

If the agent logs off the physical device first, Microsoft Office Communicator will be re-synchronized only after the next call is received or attempted. The yellow icon in the Microsoft Office Communicator status bar will provide a visual confirmation.

Using the TR/87 Test features

Follow these steps to use TR/87 test features in the AE Services Management Console.

1. From the browser on your AE Services administrative workstation, log in to the AE Services Management Console.
2. Select **Utilities > Diagnostics > AE Services > TR/87 Test**.
3. From the TR/87 Self Test page, select from the following tests:
 - **TR/87 Transport** -- use TR/87 Transport to verify that the installed certificate can be used to establish a SIP session on the loopback interface. This does not verify the far-end server certificate.
 - **TR/87 Service** -- use TR/87 Service to verify the following:
 - the caller is administered in Active Directory
 - the dial plan is administered for the caller's number
 - the user's telephone device can be monitored
 - **TR/87 Makecall** -- use TR/87 Makecall to verify that phone control is active for the user.

Note:

The TR/87 Makecall test depends on receiving confirmation of a call being established. In certain scenarios involving trunks this may not be available. The TR/87 Makecall test should be considered a valid test only when using two stations on the same switch to perform the test.

The Host AA setting and TR/87 test

The Host AA settings in the AE Services Management Console have an effect on the TR/87 Test utility. If you enable host authorization, the authorized hosts list must include the Peer Certificate CN (which is the Server Certificate Subject Name). Because the TR/87 Test utility depends on the Host AA settings and uses the same certificate that is used by Tomcat, you must restart the Web Server after adding a server certificate.

Usage Tips for the Do Not Disturb feature

For integration with Microsoft Office Live Communications Server 2005

AE Services recommends that you activate and deactivate Do Not Disturb feature using the Microsoft Office Communicator client (as opposed to your physical phone).

For Do Not Disturb (DND) to function properly, you must administer a coverage path on the station, in Communication Manager. When you complete the Coverage path screen in Communication Manager, make sure that you enable **DND/SAC/Go to Cover** for inside calls and outside calls -- the settings for **Inside Call** and **Outside Call** should be **y**.

For information about administering a coverage path in Communication Manager, see "Creating coverage paths" in *Administrator Guide for Avaya Communication Manager*, 03-300509.

For integration with Microsoft Office Communications Server 2005

The Microsoft Office Communicator 2007 does not provide the Do Not Disturb feature.

Recovering from a system outage

When AE Services returns to an operational state after an outage, you will be able to use Microsoft Office Communicator (Communicator) to place and control new calls. If you experience an outage, bear the following in mind:

- If you were on a call when an AE Services outage occurred, complete the call and manually hang up the phone so that your phone and Communicator are synchronized. When you are ready to start a new call in Communicator, your phone and Communicator will be synchronized.
- If Communicator signs you out as result of a network outage, you must sign in to Communicator again before you can control new calls. If you attempt to sign in during an AE Services outage, Communicator displays the warning icon along with the pop-up indicating that Communicator can not make phone calls.

Known issues

This section describes a few feature-related issues, as follows:

- [Setting up forwarding off-switch](#) on page 103
- [Using Call Forwarding and Send All Calls](#) on page 104
- [Using the Do Not Disturb feature](#) on page 104
- [Putting the active call on hold before starting a new call](#) on page 104
- [Clear Connection request on a held connection is not supported](#) on page 104
- [Bridging irregularities](#) on page 105
- [Missed Call e-mail](#) on page 105
- [Usage instructions for analog phones](#) on page 106.

Additionally, this section addresses the general issue that under certain conditions a party's telephone number will not be available to Microsoft Office Communicator. When this is the case, Microsoft Office Communicator can not display a telephone number or party identifier.

- [Unidentified caller in Microsoft Office Communicator window](#) on page 107
- [Communicator displays numbers with trunk notation](#) on page 108

Setting up forwarding off-switch

If you experience problems setting up forwarding off-switch (to your home or cell phone, for example) you should contact the Communication Manager administrator. There are certain settings in Communication Manager that could prevent your ability to set up forwarding off-switch.

Using Call Forwarding and Send All Calls

From the Microsoft Office Communicator, you can use Call Forwarding and Send All Calls as follows:

- You can set your phone to forward calls.
- You can set the Microsoft Office Communicator to forward calls relative to the client you are signed in to. (This does not apply to Microsoft Office Communicator 2007).
- You can set your phone to "Do Not Disturb" mode, which refers to Send All Calls (SAC) in AE Services. (This does not apply to Microsoft Office Communicator 2007).



CAUTION:

Keep in mind, however, that you should not press the Forwarding or the Send All Calls (SAC) buttons on a physical phone set. Pressing these buttons can cause the Microsoft Office Communicator to lose synchronization with the phone.

Using the Do Not Disturb feature

For Do Not Disturb (DND) to function properly, you must administer a coverage path on the station, in Communication Manager. When you complete the Coverage path screen in Communication Manager, make sure that you enable **DND/SAC/Go to Cover** for inside calls and outside calls -- the settings for **Inside Call** and **Outside Call** should be **y**.

For information about administering a coverage path in Communication Manager, see "Creating coverage paths" in *Administrator Guide for Avaya Communication Manager*, 03-300509.

Putting the active call on hold before starting a new call

It is not possible to start a new call through Microsoft Office Communicator while there is already an active call. You must put the active call on hold before starting a new call.

Clear Connection request on a held connection is not supported

Communication Manager does not support a Clear Connection request on a held connection. For the Microsoft Office Communicator user, this means that if you have a held call and you press the red, "stop" button on the call windows, you will get an error message and the call will remain in the held state.

Bridging irregularities

In an AE Services and Live Communications Server environment, the Microsoft Office Communicator might not behave as expected if you use bridged call appearances. Here are some examples of irregularities associated with bridged calls.

- If a user answers on a bridged extension, Microsoft Office Communicator continues to alert on the primary extension and eventually times out.
 - This bridging irregularity occurs when you administer EC500 phones with XMOBILE. If you administer EC500 phones with OPTIM, the bridging irregularities do not occur. For more information see, “Considerations for Extension to Cellular” in *Feature Description and Implementation for Avaya Communication Manager*, 555-245-205. OPTIM refers to Off-PBX Telephone Integration and Mobility.
- If you call someone whom has a bridged extension, the Microsoft Office Communicator conversation window might display either of the following:
 - an additional party on the call representing that bridged extension.
 - "Unidentified Caller"

Missed Call e-mail

Missed Call e-mail is sent only if the caller hangs up before the call goes to call coverage (voice mail).

Usage instructions for analog phones

If you use an analog phone, follow these special usage instructions.

Placing a call: method 1 - pick up the handset, then start the call in Communicator

1. With the Communicator window open, physically pick up the handset on your phone.

Note:

Upon hearing the dial tone, you have 10 seconds to place the call. After 10 seconds you will hear the intercept tone (alternating high and low tone). Once you receive the intercept tone, a Microsoft Office Communicator call will fail. If you attempt to place a call, you will receive an error notification in the Microsoft Office Communicator window.

2. From the Contacts list in the Microsoft Office Communicator window, right-click the **<name of the person you want to call>**, select **Call**, then click the **<phone number>**. Wait for the person you are calling to answer the phone. You will hear a ringback tone.

Microsoft Office Communicator displays the Conversation window. The status of your call is displayed in the Instant Message section of the window.

3. When the person you are calling answers the phone, start your voice conversation.
4. Once the voice conversation is over, physically hang up the handset and then close the Microsoft Office Conversation Window.

Placing a call: method 2 - start the call in Communicator, then pickup the handset

1. From the Contacts list in the Microsoft Office Communicator window, right-click the **<name of the person you want to call>**, select **Call**, then click the **<phone number>**.

Note:

You must pick up the handset within 5 seconds after clicking the phone number. If you do not pick up the handset within 5 seconds, the call will fail and Communicator will display an error message in the Instant Message section. Also note that your analog phone does not ring when the call is placed from Communicator.

Microsoft Office Communicator displays the Conversation window. The status of your call is displayed in the Instant Message section of the window.

2. Pick up the handset on your phone, and wait for the person you are calling to answer the phone. You will hear a ringback tone.
3. When the person you are calling answers the phone, start your voice conversation.
4. Once the voice conversation is over, physically hang up the handset and then close the Microsoft Office Conversation Window.

Answering a call with an analog phone

If you have an analog phone, you must pick up the handset to answer a call when your phone rings. Just pick up the handset as you normally would, and do nothing in Communicator.

Unidentified caller in Microsoft Office Communicator window

For the following reasons you might see "Unidentified Caller" in the Microsoft Office Communicator conversation window:

- The user you have called has a bridged extension.
- Your call went to a voice mail system. If your call is answered by a voice mail system, the voice mail system itself appears as an "Unidentified Caller."
- Your call went to Music-on Hold by way of a Voice Announcement with LAN (VAL) board on Communication Manager, causing you to lose phone control on your Microsoft Office Communicator. You can resolve this issue by upgrading Communication Manager with Service Pack 12866.
- You manually entered a number in the FIND box that was not in the proper format.

If you are manually typing the number in the FIND box, be sure to enter the full phone number, including the country code and either the area code or the region code, whichever is appropriate. Depending on how the system has been administered, it might be acceptable to not include the country code in the entered number. In all cases, the Automatic Route Selection (ARS) code for the outside line (9, for example) should not be included.

Communicator displays numbers with trunk notation

Microsoft Office Communicator displays telephone numbers as trunk identifiers instead of telephone numbers in both transfer and conference scenarios. Trunk identifiers are numbers that are displayed in the following form: **T5237#2**.

- In some transfer scenarios, Microsoft Office Communicator displays a trunk identifier instead of a calling or called party.
- In some conference scenarios, Microsoft Office Communicator displays a trunk identifier as an extra party on the call.

Contact the Communication Manager administrator

In either type of scenario, the presence of trunk group identifiers might be the result of improperly administered trunk groups in Communication Manager. If Microsoft Office Communicator displays a trunk identifier, contact the Communication Manager administrator.

The Communication Manager administrator should verify that ISDN trunks are properly administered (Trunk Group screen). The settings for "Send Calling Number" and "Send Connected Number" should be set to **y**. Administering ISDN trunks also requires administration of the "Numbering - Public/Unknown Format" screens. For more information, see *Administrator Guide for Avaya Communication Manager*, 03-300509. ISDN is the acronym for Integrated Services Digital Network.

Note:

When "QSIG Value-Added" is enabled for QSIG trunks, the label for "Send Connected Number" changes to "Send Called/Busy/Connected Number."

Chapter 4: Integrating AE Services with Communications Server 2007

How to use the information in this chapter

After you complete the tasks in Chapter 1, use the information in this chapter to integrate Application Enablement Services (AE Services) with Microsoft Office Communications Server 2007.

AE Services support Microsoft Office Communications Server 2007 and Microsoft Office Communications Server 2007 R2.

Phase 3 Checklist --integrating AE Services with Microsoft Office Communications Server 2007

Use [Table 8](#) as a checklist for performing the tasks necessary for integrating AE Services in a Microsoft Office Communications Server 2007 environment.

Table 8: Checklist for integrating AE Services with Microsoft Office Communications Server 2007

Task		Admin domain	Document
1	Administer a switch connection from AE Services to Communication Manager.	AE Services	See the AE Services Administration and Maintenance Guide.
2	Check the status of the switch connection (from AE Services to Communication Manager).	AE Services	See the AE Services Administration and Maintenance Guide.
3	Administer a TSAPI Link.	AE Services	See the AE Services Administration and Maintenance Guide.
4	Enable the TR/87 Port in the AE Services Management Console.	AE Services	See Enabling the TR/87 port on page 113.
1 of 3			

Table 8: Checklist for integrating AE Services with Microsoft Office Communications Server 2007 (continued)

Task		Admin domain	Document
5	Administer certificates for AE Services and Microsoft Office Communications Server 2007.	Microsoft Office Communications Server 2007	See Procedure 1 - Installing the trusted certificate on Office Communications Server 2007 on page 116.
		Microsoft Office Communications Server 2007	See Procedure 2 - Installing a server certificate for the Office Communications Server on page 120 of this document.
		AE Services	See Procedure 3 - Installing the trusted certificate on the AE Server on page 124 of this document.
		AE Services	See Procedure 4 - Creating a server certificate request for AE Services on page 128 of this document.
		AE Services	See Procedure 5 - Creating a server certificate for AE Services on page 129 of this document.
		AE Services	See Procedure 6 - Importing the server certificate into AE Services on page 131 of this document.
6	Administer settings for the dial plan.	AE Services	See Dial Plan settings in AE Services on page 133 of this document.
7	Administer settings for Active Directory.	AE Services	See Administering AE Services access to Active Directory on page 150 of this document.
8	Configure the Microsoft Office Communicator 2007 Client.	Microsoft -- either the client workstation or the Active Directory Server	See "Configuring the Client" in the <i>Microsoft Office Communicator 2007 Telephony Planning and Deployment Guide</i> .
9	Set up a static route.	Microsoft Office Communications Server 2007	AE Services Implementation Guide for Microsoft Office Communications Server 2007, see Configuring a static route on page 157.
			2 of 3

Table 8: Checklist for integrating AE Services with Microsoft Office Communications Server 2007 (continued)

Task		Admin domain	Document
10	Specify the AE Server as an authorized host.	Microsoft Office Communications Server 2007	AE Services Implementation Guide for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007, see Specifying the AE Server as an authorized host on page 158.
11	Set up Remote Call Control for each user in Active Directory Services.	Microsoft Active Directory Server	AE Services Implementation Guide for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007, see Enabling Remote Call Control in Active Directory on page 155. Based on information from <i>Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide</i> .
3 of 3			

About configuring AE Services for Microsoft Office Communications Server 2007

Configuring AE Services for Microsoft Office Communications Server 2007 is an extension of TSAPI-based administration.

To configure AE Services for Microsoft Office Communications Server 2007, you must carry out the TSAPI-related administration tasks as well as the AE Services implementation for Microsoft LCS administration tasks.

- **TSAPI related administration tasks**, which are described in Chapter 3 of the *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, 02-300357:
 - administering a local IP
 - administering a switch connection
 - administering a TSAPI link
- **AE Services implementation for Microsoft LCS administration tasks**, which are described in this document:
 - enabling the TR/87 port - see [Enabling the TR/87 port](#) on page 113
 - administering certificates - see [Administering Certificates -- certificate management](#) on page 114
 - administering the dial plan settings - see [Dial Plan settings in AE Services](#) on page 133
 - administering settings for Active Directory - see [Administering AE Services access to Active Directory](#) on page 150

Enabling the TR/87 port

AE Services uses port 4723 for communications between AE Services and Microsoft Office Communications Server 2007. Because this port is disabled by default in the AE Services Management Console, you must enable it.

1. From the browser on your AE Services administrative workstation, log in to the AE Services Management Console.
2. From the main menu of the AE Services Management Console select **Networking > Ports**.
3. On the Ports page, under DMCC Server Ports, locate the TR/87 Port, and select the option button for Enabled.

Administering Certificates -- certificate management

AE Services and Microsoft Office Communication Server communicate using Transport Layer Security (TLS). For communication to take place, AE Services and Microsoft Office Communications Server 2007 must exchange signed server certificates each time a TLS session is opened. This section provides a sample certificate management scenario that includes the following procedures.

- [Procedure 1 - Installing the trusted certificate on Office Communications Server 2007](#) on page 116
- [Procedure 2 - Installing a server certificate for the Office Communications Server](#) on page 120
- [Procedure 3 - Installing the trusted certificate on the AE Server](#) on page 124
- [Procedure 4 - Creating a server certificate request for AE Services](#) on page 128
- [Procedure 5 - Creating a server certificate for AE Services](#) on page 129
- [Procedure 6 - Importing the server certificate into AE Services](#) on page 131

Note:

If OCS Enterprise edition is in use with an OCS server pool, the certificate should be issued in the name of the pool and must have both Server Authentication and Client Authentication. If a load balancer handles the pool, then the pool name should resolve to the load balancer's IP address. For example, if the OCS pool is called **ocspool.company.com**, and that is the pool that agents and OCS servers use, the DNS resolution of **ocspool.company.com** should be the IP address of the load balancer. Furthermore, the TLS certificate should be issued to **ocspool.company.com** from the correct authority with the correct company name, etc. Then, this certificate should be put on each of the OCS servers so that they pass this **ocspool.company.com** certificate when creating a secure socket to Application Enablement Services.

Additional references

The following documents are useful for understanding the tasks that are required for a service integration.

- *Office Communications Server 2007 Document: Standard Edition Deployment Guide*
- *Office Communications Server 2007 Document: Integrating Telephony with Office Communications Server 2007*
- *Office Communications Server 2007 Document: Enterprise Edition Deployment Guide*
- *Office Communications Server 2007 Document: Active Directory Guide*

About the sample scenario

Use the sample scenario to familiarize yourself with the basic tasks for integrating AE Services with Microsoft Office Communications Server 2007. The procedures in the sample scenario are based on using:

- **Microsoft Office Communications Server 2007 Enterprise Edition**
- Microsoft Windows Server 2003 Standalone Certificate Authority.

Because it is likely that some users will rely on a certificate authority (CA) other than Microsoft Certificate Services, the CA-based procedures include generic instructions as well as Microsoft-based instructions.

Note:

If you are using a Microsoft Windows Server 2003 Enterprise Edition Certificate Authority, Appendix D provides a procedure for creating a server certificate template that supports both client authentication and server authentication. For more information see [Appendix D: Creating a certificate template for Server Certificates on the Microsoft CA Server](#) on page 201. Keep in mind that all of the procedures in Chapters 2 and 3 of this document are based on a Microsoft Windows Server 2003 Standalone Certificate Authority. If you use an Enterprise Edition CA, the procedures in Chapters 2 and 3 do not apply to your configuration.

About obtaining certificates

To obtain a certificate you must generate a certificate request and then submit the Certificate Request to a CA. Procedures for generating a certificate request and the data required for completing a certificate request can vary from one CA to another.

Specifying key usage

Based on the CA you use, you might be required to specify the key usage allowed for the certificate you are requesting. If your CA requires you to specify key usage, you must ensure that the `digitalSignature` and the `keyEncipherment` bits are enabled. For more information refer to RFC 2459.

Client and server authentication

The AE Services implementation for Microsoft Office Communications Server 2007 requires a certificate that does both client authentication and server authentication.

In terms of the Microsoft Windows Server 2003 Standalone CA, this means that when you complete the Advanced Certificate Request, you will select Other... from the "Type of Certificate Needed" drop-down list. When you select Other... , the Advanced Certificate Request displays a text entry field for the OID (object identifier). For information about completing this field, see [Installing a Microsoft Certificate Services-based certificate on the Microsoft Office Communications Server 2007](#) on page 121.

If you use another CA (either a generic CA or the Microsoft Windows Server 2003 Enterprise CA), the certificate request will not contain the same drop-down menus and choices. For example with Microsoft Windows Server 2003 Enterprise CA, you might not see a field for the OIDs because the OIDs can be set by the CA administrator in a template.

Procedure 1 - Installing the trusted certificate on Office Communications Server 2007

The trusted certificate is also referred to as the CA Certificate. From the Microsoft Office Communications Server 2007, follow the appropriate procedure to obtain the trusted certificate and import it into the Microsoft Office Communications Server 2007 certificate store.

When installing the trusted certificate, note that Microsoft Office Communications Server 2007 and AE Services must use either the same CA or an issuer in the same certificate chain.

- If you are using a third party certificate authority other than Microsoft Certificate Services, follow the procedure described in [Installing the trusted certificate from another vendor](#).
- If you are using Microsoft Certificate Services, follow the procedure described in [Installing the trusted certificate generated by Microsoft Certificate Services](#).

Installing the trusted certificate from another vendor

Steps 1 and 2 are provided as a general reference only -- follow the instructions on your CA's Web site.

1. From your browser, go your certificate authority's Web page for requesting a trusted certificate or a trusted certificate chain.
2. Import the trusted certificate. For information about configuring certificates, see the *Microsoft Office Communications Server 2007 Standard Edition Deployment Guide* or the *Microsoft Office Communications Server 2007 Enterprise Edition Deployment Guide*.
3. Continue with [Importing the certificate into the Microsoft Office Communications Server 2007 trust store](#) on page 118.

Installing the trusted certificate generated by Microsoft Certificate Services

Follow this procedure to download the trusted certificate generated by Microsoft Certificate Services.

1. From your browser, type the URL of the Microsoft Certificate Services Server. For example:
`http://<certificate_server.com>/certsrv`
2. From the Microsoft Certificate Services page, click **Download a CA certificate, certificate chain, or CRL**.
3. Complete the Download a CA Certificate, Certificate Chain, or CRL page as follows:
 - a. Under CA Certificate, in the list box, select the signing certificate.
 - b. Click **Base 64**.
 - c. Click **Download CA certificate chain**.
4. Save the CA certificate file (**lcscertnew.p7b**, for example) to a local directory on the Microsoft Office Communications Server 2007 (C:\temp, for example).
5. Continue with the steps described next in [Importing the certificate into the Microsoft Office Communications Server 2007 trust store](#).

Importing the certificate into the Microsoft Office Communications Server 2007 trust store

Use this procedure to import the trusted certificate, from any CA, in to the Microsoft Office Communications Server 2007's trust store.

1. Start the Microsoft Management console -- Click **Start**, and then click **Run**. In the Run dialog box, type **mmc**, and click **OK**.
2. From the Console window, click **File > Add/Remove Snap-in...** .
3. From the Add/Remove Snap-in dialog box, on the Standalone tab, which displays **Console Root** as the default, click **Add...** .
4. From the Add Standalone Snap-in dialog box, select **Certificates**, and click **Add**.
5. From the Certificates snap-in dialog box, select **Computer account**, and click **Next**.
6. From the Select Computer dialog box, select **Local Computer: (the computer this console is running on)**, and click **Finish**.
7. Click **Close** from the Add Standalone Snap-in dialog box, and then click **OK** from the Add/Remove Snap-in dialog box.
8. From the left pane of the Console Root, under Certificates (Local Computer), expand **Trusted Root Certificates Authorities**.
9. Right-click **Certificates**, and then select **All Tasks** and click **Import**.
10. From the Certificate Import Wizard, Welcome screen, select **Next**.
11. Click **Browse**, and go to the directory where you stored the certificate file (**C:\temp\lcscertnew.p7b**, for example). Select the certificate file (**lcscertnew.p7b**, for example) and click **Open**.
12. In the Certificate Import Wizard, Certificate Store dialog box, make sure that **Place all certificates in the following store** is selected, and the Certificate Store is: **Trusted Root Certification Authorities**. Click **Next**.
13. When the Certificate Import Wizard dialog box displays the message "You have successfully completed the Certificate Import wizard," click **Finish**.

Procedure 1a - Verifying the installation of the trusted certificate on Office Communications Server

Follow this procedure to verify that the trusted certificate is installed correctly.

1. Start the Microsoft Management console -- Click **Start**, and then click **Run**. In the Run dialog box, type **mmc**, and click **OK**.
2. From the Console window, click **File > Add/Remove Snap-in...** .
3. From the Add/Remove Snap-in dialog box, on the Standalone tab, which displays **Console Root** as the default, click **Add...** .
4. From the Add Standalone Snap-in dialog box, select **Certificates**, and click **Add**.
5. From the Certificates snap-in dialog box, select **Computer account**, and click **Next**.
6. From the Select Computer dialog box, select **Local Computer: (the computer this console is running on)**, and click **Finish**.
7. Click **Close** from the Add Standalone Snap-in dialog box, and then click **OK** from the Add/Remove Snap-in dialog box.
8. Verify that the trusted certificate for the Microsoft Office Communications Server 2007 is installed, as follows:
 - a. In the left pane of the console, Under Certificates (Local Computer) expand **Trusted Root Certificates Authorities** and click **Certificate**. The console displays a list of trusted certificates in the right pane.
 - b. In the right pane of the console, verify that the display includes the trusted certificate that you installed at the end of Procedure 1, as follows:
 - Make sure the Issued To field displays the name of the certificate authority.
 - Make sure the Issued By field displays the name of the certificate authority that issued the certificate. This issuer should be either the same issuer, or an issuer in the same certificate chain.
 - Make sure the expiration date is correct.

Procedure 2 - Installing a server certificate for the Office Communications Server

Follow the appropriate procedure for installing a server certificate for the Microsoft Office Communications Server 2007.

- If you are using a third party certificate authority other than Microsoft Certificate Services, refer to [Installing a server certificate from another vendor](#) on page 120.
- If you are using Microsoft Certificate Services, refer to [Installing a Microsoft Certificate Services-based certificate on the Microsoft Office Communications Server 2007](#) on page 121.

Installing a server certificate from another vendor

Steps 1 through 3 are provided as a general reference only -- follow the instructions on your CA's Web site.

1. From your browser, go to your certificate authority's Web page for requesting a server certificate.
2. Complete the required fields for enrollment. Usually this includes contact information, such as your name, email address, your organizational unit (OU), and so on.

When you are providing the name and IP address for the server, use this rule of thumb. If you are using Enterprise Edition, use the fully qualified domain name and IP address of your pool; if you are using Standard Edition use the fully qualified domain name and IP of your server.

3. Import the server certificate. For information about configuring certificates, see the *Microsoft Office Communications Server 2007 Standard Edition Deployment Guide* or the *Microsoft Office Communications Server 2007 Enterprise Edition Deployment Guide*.
4. Continue with the steps for [Procedure 2b - Configuring the certificate for automatic routing](#) on page 123.

Installing a Microsoft Certificate Services-based certificate on the Microsoft Office Communications Server 2007

From the Microsoft Office Communications Server 2007, follow this procedure to install a server certificate issued by Microsoft Certificate Services.

Note:

In terms of the Microsoft Office Communications Server 2007 Certificate Configuration Guide, the AE Services implementation for Microsoft Office Communications Server 2007 falls into the category of "interoperating with partner systems." This means that you must install a certificate that is configured for both client and server authorization. You do this by selecting **Include client EKU** as depicted in Step 8d.

1. Log on to the Microsoft Office Communications Server that needs to be configured with a certificate.
2. From the Start Menu of the Microsoft Office Communications Server 2007 management console, select **Administrative Tools > Office Communications Server 2007**.
3. From the left pane of the Microsoft Office Communications Server control panel, expand the **Forest** node (Forest - example.com) then **Enterprise pools** and **Front Ends**.
4. Right click the name of your server node, and click **Certificates**.
5. From the Welcome screen of the Certificate Wizard, click **Next**.
6. From the Available Certificate Tasks screen, accept the default selection, **Create a new certificate**, and click **Next**.
7. From the Delayed or Immediate Request screen, accept the default selection, **Send the request immediately to an online certification authority**, and click **Next**.
8. Complete the Name and Security Settings screen as follows:
 - a. In the Name field, type the name of the certificate. Create a name that is meaningful and unique for your server.
 - b. In the Bit length field, accept the default, 1024.
 - c. Accept the default for Mark cert as exportable (by default a check mark appears in the check box).
 - d. Select **Include client EKU** in the certificate request. Make sure a check mark appears in this box. By selecting this option, you are installing a certificate that is configured for both client and server authorization.
 - e. Click **Next**.
9. From the Organizational Information screen, accept the default Organization name and Organizational Unit, and click **Next**.
10. From the screen labeled Your Server's Subject Name, accept the default Subject Name and the Subject Alternate Name, and click **Next**.

11. From the Choose a Certification Authority screen, in the **Select a certificate authority from the list detected in your environment** field, select your CA from the drop-down list or specify your external CA, and click **Next**.
12. From the Request Summary screen, review the information in the text display area, and click **Next**.

The Office Communications Server Wizard displays the Certificate Wizard completed successfully screen, with an Assign button and a View button. Click **View** to inspect the certificate you just obtained, then click **Assign** to assign the certificate to the server. Click **Finish** to Exit the Wizard.

13. To put the certificate into effect, restart the Microsoft Office Communications Server 2007.

Note:

When you use the Certificate Wizard to install a certificate, the Wizard configures the certificate for automatic routing among your pool and servers.

Procedure 2a - Verifying the installation of the server certificate for Microsoft Office Communications Server 2007

Use this procedure to verify the installation of the server certificate, from any CA, for the Microsoft Office Communications Server 2007.

1. Start the Microsoft Management console -- Click **Start** and then click **Run**. In the Run dialog box, type **mmc**, and click **OK**.
2. From the Console window, click **File > Add/Remove Snap-in...**
3. From the Add/Remove Snap-in dialog box, on the Standalone tab, which displays **Console Root** as the default, click **Add...**
4. From the Add Standalone Snap-in dialog box, select **Certificates**, and click **Add**.
5. From the Certificates snap-in dialog box, select **Computer account**, and click **Next**.
6. From the Select Computer dialog box, select **Local Computer: (the computer this console is running on)**, and click **Finish**.
7. Click **Close** from the Add Standalone Snap-in dialog box, and then click **OK** from the Add/Remove Snap-in dialog box.
8. Verify that the server certificate for the Microsoft Office Communications Server 2007 is installed, as follows:
 - a. In the left pane of the console, Under Certificates (Local Computer) expand **Personal** and click **Certificate**. The console displays a list of certificates in the right pane.
 - b. In the right pane of the console, verify that the display includes the server certificate that you installed at the end of Procedure 2, as follows:

- Make sure the Issued To field displays the fully-qualified domain name of the Microsoft Office Communications Server 2007 for Standard Edition OCS 2007 or the fully-qualified domain name of the Enterprise Pool name for Enterprise Edition OCS 2007.
- Make sure the Issued By field displays the name of the certificate authority that issued the certificate (referred to as the issuer on the certificate).
- Make sure the expiration date is correct.

Procedure 2b - Configuring the certificate for automatic routing

Follow this procedure to configure the certificate for automatic routing among your pool and servers.

1. Log on to the Microsoft Office Communications Server that needs to be configured with a certificate.
2. From the Start Menu of the Microsoft Office Communications Server 2007 management console, select **Administrative Tools > Office Communications Server 2007**.
3. From the left pane of the Microsoft Office Communications Server control panel, expand the **Forest** node (Forest - example.com) then **Enterprise pools** and **Front Ends**.
4. Right click the name of your server node, and click **Certificates**.
5. From the Welcome screen of the Certificate Wizard, click **Next**.
6. From the Available Certificate Tasks screen, click option button for **Assign an existing certificate**, and click **Next**.
7. From the Available Certificates screen, select the appropriate certificate, and click **Next**.
8. From the Configure the Certificate(s) of your Server screen, click **Next**.
9. From the Certificate Wizard completed successfully screen click **Finish**.
10. To put the certificate into effect, restart the Microsoft Office Communications Server 2007.

Procedure 3 - Installing the trusted certificate on the AE Server

The trusted certificate is also referred to as the certificate authority (CA) certificate. It is issued by the certificate authority, which can be either Microsoft Certificate Services or another certificate authority.

- If you are using a certificate authority other than Microsoft Certificate Services, use the procedure described in [Generic procedure for installing the trusted certificate for AE Services](#) on page 124.
- If you are using Microsoft Certificate Services, use the procedure described in [Microsoft-based procedure for installing a trusted certificate chain](#) on page 125.

Generic procedure for installing the trusted certificate for AE Services

These steps are provided as a general reference only -- follow the instructions on your CA's Web site.

1. From your browser, go to your certificate authority's Web page and download the certificate chain.



Important:

You must import the entire certificate chain all the way back to the root certificate.

- The trusted certificate or certificate chain must be in text format (PEM or Base-64). If you are importing a certificate chain, it must be a text-based PKCS#7 file. Think of a PKCS#7 file as an envelope containing all trusted certificates.
 - It is acceptable to import certificates in the chain individually if they are not available in PKCS#7 format, but all certificates must be in the trusted certificates store.
2. The certificate authority processes your request and issues a trusted certificate (or certificate chain) for you to download.
 3. Download the entire certificate to the AE Services administrative workstation, and save it with a unique name (for example, **C:\templaetrucert.cer**).
 4. Using a text editor, open the trusted certificate file, and verify the header and trailer:
 - The header and trailer for a PEM or Base 64 file are as follows:
-----BEGIN CERTIFICATE----- (header)
-----END CERTIFICATE----- (trailer)
 - The header and trailer for a PKCS#7 file are as follows:
-----BEGIN PKCS7----- (header)
-----END PKCS7----- (trailer)

Note:

The header and trailer in your PKCS#7 file must read as follows before you import the contents of the file into OAM:

```
-----BEGIN PKCS7-----
```

```
-----END PKCS7-----
```

If the header and trailer read as:

```
-----BEGIN CERTIFICATE-----
```

```
-----END CERTIFICATE-----
```

you must edit them to read as:

```
-----BEGIN PKCS7-----
```

```
-----END PKCS7-----.
```

5. Contact the Microsoft Office Communications Server 2007 administrator, and confirm that both the server certificate and the trusted certificate are installed and operating on Microsoft Office Communications Server 2007. The certificates must be installed and operating on Microsoft Office Communications Server 2007 before you can carry out the procedures in the AE Services Management Console.
6. Continue with the steps described next in [Importing the trusted certificate into the AE Services Management Console](#) on page 126.

Microsoft-based procedure for installing a trusted certificate chain

If you use a Microsoft CA hierarchy, follow this procedure from the AE Server to import the trusted certificate chain in PKCS#7 format from Microsoft Certificate Services into the AE Services Management Console.

1. From Internet Explorer, type the URL of your certificate server. For example:
http://<microsoftcertificate_server.com>/certsrv
2. From the Microsoft Certificate Services page, click **Download a CA certificate, certificate chain, or CRL**.
3. On the Download a CA Certificate, Certificate Chain, or CRL page, select the option button for **Base 64**, and click **Download CA certificate chain**.
4. Save the CA certificate file (the trusted certificate) to a local directory on the Microsoft Office Communications Server 2007 (for example **C:\templaetrucert.cer**).
5. Using a text editor, open the file and change the header and trailer as follows:

```
-----BEGIN PKCS7-----
```

```
-----END PKCS7-----
```

**Important:**

You must change the header and trailer in the PKCS#7 file as specified in Step 5. Otherwise, you will be unable to successfully import the trusted certificate chain from a Microsoft CA.

6. Copy the entire contents of the CA certificate file, including the updated header and trailer.

7. Contact the Microsoft Office Communications Server 2007 administrator, and confirm that both the server certificate and the trusted certificate are installed and operating on the Microsoft Office Communications Server 2007. The certificates must be installed and operating on Microsoft Office Communications Server 2007 before you can carry out the procedures in the AE Services Management Console.
8. Continue with the steps described next in [Importing the trusted certificate into the AE Services Management Console](#) on page 126.

Importing the trusted certificate into the AE Services Management Console

1. From the main menu of the AE Services Management Console, select **Security > Certificate Management > CA Trusted Certificates**.
2. From the CA Trusted Certificates page, click **Import**.
3. Complete the Trusted Certificate Import page, as follows:
 - In the Certificate Alias field, type an alias for the trusted certificate (for example, **catrusted**). The trusted certificate alias can be arbitrary. It does not need to match any aliases for AE Services.
 - Click **Browse** to locate the trusted certificate file you want to import, and click **Apply**. If the import is successful, your browser displays the following message: "Certificate Imported Successfully."

Note:

At this point it is recommended that you complete [Procedure 3a - Verifying the installation of the trusted certificate in AE Services](#) on page 127.

Procedure 3a - Verifying the installation of the trusted certificate in AE Services

Use this procedure to verify the installation of the entire certificate chain (all the way back to the root certificate) in AE Services.

1. From the main menu of the AE Services Management Console, select **Security > Certificate Management > CA Trusted Certificates**.
2. From the CA Trusted Certificates page, select the alias of the trusted certificate (**catrusted**, based on this sample scenario), and click **View**.
3. From the Trusted Certificate Details page, verify that the information for the trusted certificate is correct.
 - a. Verify that the entire chain of certificates exists, all the way back to a self-signed certificate.
 - b. Verify that the Issued To field displays name of the organization that the trusted certificate is issued to.
 - c. Verify that the Issued By field Indicates the name of the certificate authority that issued the trusted certificate (referred to as the issuer on the certificate). This issuer should be either the same issuer, or an issuer in the same certificate chain, as described in Step 8b of Procedure 1a on page 119.
 - d. Verify that the Expiration Date Indicates the date that the trusted certificate expires.
 - e. Verify the information in the Details display. Make sure the Certificate Status is valid.
4. Click **Close** to exit the Trusted Certificate Details page.

Converting Certificate files in other formats for AE Services

If your CA provides you with a certificate in DER format, you must convert it to PEM before importing it into the AE Services Management Console. The following sections describe how to convert files using openssl tools, which are available on the Web at www.openssl.org.

Converting a DER file to PEM : If your Certificate Authority provides you with a DER-encoded certificate, you must convert it to PEM before you can import it into AE Services. Use the following command to convert the DER file to PEM format.

```
openssl x509 -in <input>.cer -inform DER -out <output>.cer -outform PEM
```

Procedure 4 - Creating a server certificate request for AE Services

In the AE Services Management Console, use this procedure to create a server certificate request (also referred to as a certificate signing request, or CSR) for the AE Services server. This procedure generates a certificate signing request which includes a private key.

1. From the browser on your AE Services administrative workstation, log in to the AE Services Management Console.
2. Select **Security > Certificate Management > Server Certificate.s**
3. On the Server Certificate page, click **Add**.
4. Complete the Add Server Certificate page, as follows:
 - From the Certificate Alias list box, select the appropriate alias.
 - Leave the Create Self-Signed Certificate check box unchecked (the default).
 - In the Encryption Algorithm field, select **3DES**.
 - In the Password field, type the password of your choice.
 - In the Key Size field, accept the default **1024**.
 - In the Certificate Validity field, accept the default, **1825**.
 - In the Distinguished Name field, type the LDAP entries required by your CA. These entries must be in LDAP format and they must match the values required by your CA. If you are not sure what the required entries are, contact your CA.

Among the required entries will be the FQDN of the AE Server in LDAP format. Additionally you might need to provide your company name, your organization name and so on. Separate each LDAP entry with a comma, and do not use blank spaces, for example:

cn=myaeserver.example.com,ou=myOrganizationalUnit,o=Examplecorp,L=Springfield,ST=Illinois,C=US

Note:

Currently the Add Server Certificate page in the AE Services Management Console does not support using commas within a DN attribute (for example: **o=Examplecorp, Inc**).

- In the Challenge password and Re-enter Challenge Password fields, type the challenge password of your choice.
- In the Key Usage field, accept the default; by default nothing is selected.
- In the Extended Key Usage field, accept the default; by default nothing is selected.
- In the SCEP Server URL field, accept the default; by default this field is blank.
- In the CA Certificate Alias field, accept the default; by default this field is blank.

- In the CA Identifier field, accept the default; by default this field is blank.
- Click **Apply**.

AE Services displays the Server Certificate Manual Enrollment Request page, which displays the certificate alias and the certificate request itself in PEM (Privacy Enhanced Mail) format. The certificate request consists of all the text in the box, including the header (-----BEGIN CERTIFICATE REQUEST -----) and the trailer (-----END CERTIFICATE REQUEST-----).

5. Copy the entire contents of the server certificate, including the header and the trailer. Keep the contents available in the clipboard for the next procedure.

Procedure 5 - Creating a server certificate for AE Services

Use the appropriate procedure for creating a server certificate for AE Services.

- If you are using a third party certificate authority other than Microsoft Certificate Services, refer to [Generic procedure for creating a server certificate for AE Services](#) on page 129.
- If you are using Microsoft Certificate Services, refer to [Microsoft-based procedure for creating a server certificate for AE Services](#) on page 130.

Generic procedure for creating a server certificate for AE Services

These steps are provided as a general reference only -- follow the instructions on your CA's Web site.

1. From your browser, go your CA's Web page for requesting a server certificate.
2. Complete the required fields for enrollment. Usually you provide information such as your name, email address, the IP address of your server, your organizational unit (OU), and the type of server you have.
3. Paste the CSR into the appropriate field and submit or upload the request. (You paste the certificate request that you copied in Step 5 of Procedure 4 on page 129).
4. The certificate authority processes your request and issues a server certificate for you to download.
5. Download the certificate to your AE Services administrative workstation, and save it with a unique name (for example, C:\aescert.cer).

Important:

The certificate data you import into the AE Services Management Console system must be PEM-encoded (Base 64).

- If your CA issues certificates in DER format, you must convert it to PEM before importing it into AE Services. See [Converting a DER file to PEM](#) on page 127.

Microsoft-based procedure for creating a server certificate for AE Services

If you use Microsoft Certificate Services as the certificate authority, use this procedure as a guide for creating a server certificate for AE Services.

1. From your Web browser, type the URL of your certificate server. For example:
http://<certificate_server.com>/certsrv
where: <certificate_server.com> is the domain name or IP address of your certificate server.
2. On the Welcome page of Microsoft Certificate Services, click **Request a certificate**.
3. On the Request a Certificate page, click **advanced certificate request**.
4. On the Advanced Certificate Request page, click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**. (AE Services uses a base-64-encoded CMC).
5. On the Submit a Request or Renewal Request page, paste the certificate request into the Saved Request input field, select a template with clientAuth and serverAuth in the Certificate Template field, and then click **Submit**. (You paste the certificate request that you copied in Step 5 of Procedure 4 on page 129).
6. From the Certificate Issued page, select **Base 64 encoded**, and click **Download certificate**.

Note:

Some CAs are not set up to automatically grant certificates. If this case, you might have to wait until your administrator issues the certificate. Once your administrator issues the certificate, return to the Welcome page of Microsoft Certificate Services, and click **View the status of a pending certificate request** to get to the "Issued Certificate" page.

7. From the File download dialog box, save the certificate to your computer.

Procedure 6 - Importing the server certificate into AE Services

From the AE Services Management Console follow this procedure to import the AE Services server certificate into the AE Services Management Console. This procedure assumes that your certificate is in PEM format. If your certificate is in another format, see [Converting Certificate files in other formats for AE Services](#) on page 127.

Note:

Always install just the server certificate (as opposed to a PKCS7 certificate chain), but be sure to select **Establish Chain of Trust** as indicated in Step 6.

1. UFrom the main menu of the AE Services Management Console, select **Security > Certificate Management > Server Certificates > Pending Requests**.
2. From the Pending Server Certificate Requests page, select the certificate alias you specified when you created the CSR for AE Services (based on the example, the alias is `aeservercert`), and then click **Manual Enroll**.
3. From the Server Certificate Manual Enrollment Request page, click **Import**. When you click **Import**, your browser displays the Server Request Import page.
4. Complete the Server Certificate Import page, as follows:
 - From the Certificate Alias list box, select the alias you used to generate this certificate request (based on the example, it is `aeservercert`).
 - Accept the default for **Establish Chain of Trust** (by default it is selected).
 - Click Browse to locate the signed server certificate file you want to import.
 - Click **Apply**.

If the import is successful, AE Services displays the message: "Certificate imported successfully."

Procedure 6a - Verifying the installation of the server certificate in AE Services

Follow this procedure to verify the installation of the server certificate in AE Services.

1. From the main menu of the AE Services Management Console, select **Security > Certificate Management > Server Certificates**.
2. From the Server Certificates page, select the alias of the server certificate (**aeservercert**, based on this sample scenario), and click **View**.
3. From the Server Certificate Details page, verify that the information for the server certificate is correct.
 - a. Verify that the Issued To field displays the fully qualified domain name of the AE Server.
 - b. Verify that the Issued By field Indicates fully-qualified domain name of the certificate authority that issued the server certificate.
 - c. Verify that the Expiration Date Indicates the date that the server certificate expires.
 - d. Verify the information in the Details window. Make sure the Certificate Status is valid.
4. Click **Close** to exit the Server Certificate Details page.



CAUTION:

AE Services allows only one server certificate at a time. If you install more than one server certificate and restart AE Services, the TR/87 service will fail to initialize.

Replacing an expired server certificate

Once a server certificate has expired, links or security features that rely on the validity of the certificate may fail. Because AE Services allows only one server certificate at a time, you must carefully manage the process of replacing an expired certificate.

If you have a certificate that is about to expire, you can install a new certificate without impacting AE Services. Before the server certificate expires, select the server certificate on the Server Certificate page and delete it. Once you have deleted the expired server certificate, restart the AE Server. When AE Services restarts the newly-installed certificate will go into effect.

Dial Plan settings in AE Services

AE Services uses the information on the Dial Plan settings pages to process phone numbers used in your configuration of the AE Services implementation for Microsoft Office Communications Server 2007. In AE Services you can use either of the following methods to administer dial plan settings.

- You can administer the dial plan settings for one switch at a time. For more information, see [Administering dial plan settings on a per-switch basis](#) on page 147.
- You can administer default dial plan settings that are used for all switches. For more information, see [Administering default dial plan settings](#) on page 148.

**Important:**

In configurations with one AE Server supporting multiple switches, AE Services does not support Microsoft Office Communicator control of the same extension on more than one switch.

Before you begin

Before you start the procedures to administer dial plan settings, make sure you are familiar with Tel URI formats and the dial plan conversion pages in the AE Services Management Console. Tel URI is an abbreviation for Telephony Uniform Resource Identifier, sometimes it is expressed as "TelURI."

- To familiarize yourself with Tel URI formats, see [About Tel URI formats and device IDs](#) on page 134.
- For information about using the AE Services Management Console pages to create dial plan conversion rules for converting E.164 phone numbers to switch extensions and switch extensions to E.164 phone numbers, see [About the From TelURI and To TelURI rules](#) on page 135.

To complete the dial plan settings in the AE Services Management Console, you need to know how the dial plan is administered for on Communication Manager. If you do not know what the dial plan settings are for a particular switch or set of switches, contact the Communication Manager administrator.

About Tel URI formats and device IDs

[Table 9](#) describes the supported Tel URI formats that AE Services supports. The preferred format is E.164, except in cases where the extension bears no resemblance to the E.164 number.

Calling device and monitored device ID: AE Services expects the calling device and monitored devices to be in either E.164PlusExt format or E.164 format. The extOnly format should be used only if there is no correlation between the E.164 number and the extension.

Called device ID: Called device IDs will not be in E.164PlusExt format, but they could be in any of the other formats listed in [Table 9](#).

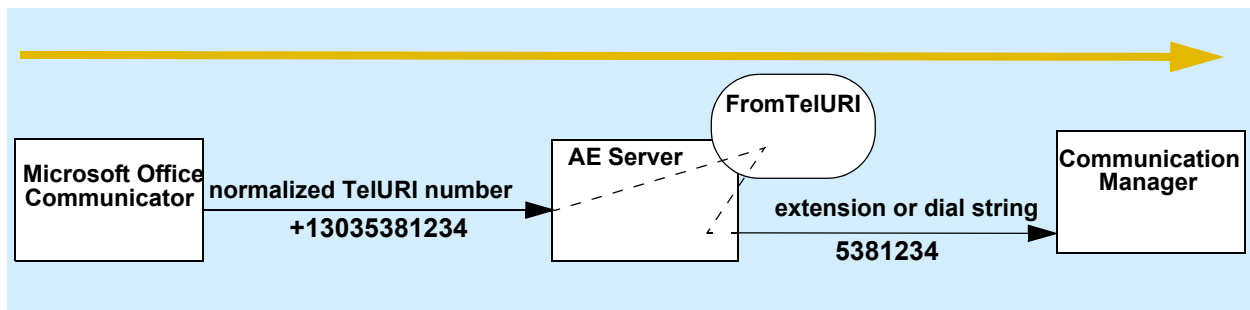
Table 9: Tel URI formats supported by AE Services

Format	Example
E.164	tel:+13035389000
E.164PlusExt	tel:+13035389000;ext=1234
extOnly	tel:5389000;phone-context=<domain> where <domain> can be any organization's domain name tel:5380112;phone-context=example.com

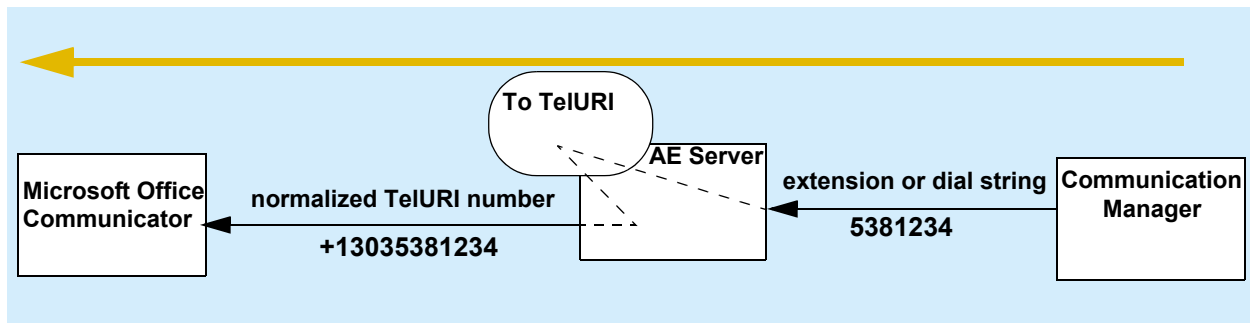
About the From TelURI and To TelURI rules

The dial plan conversion pages ("Dial Plan Settings - Conversion Rules for Default" and "Dial Plan Settings - Conversion Rules - switchname") in the AE Services Management Console are used for setting up conversion rules for a switch connection. The conversion rules are expressed as two tables in the AE Services Management Console, "From TelURI" and "To TelURI."

From TelURI: The term "From TelURI" is a shorthand way of saying "convert from a normalized TelURI number to an extension or dial string," which is handed off to the switch (Communication Manager).



To TelURI: The term "To TelURI" is a shorthand way of saying "convert from an extension or dial string to a normalized TelURI," which is handed off to Microsoft Office Communicator.



TelURI settings - how incoming and outgoing numbers are processed

Use the first two topics in this section ([The From Tel URI table](#) and [The To TelURI table](#)) to get a basic idea of how the From and To TelURI settings in AE Services work. Because the From TelURI settings and the To TelURI settings function as logic tables, this document often refers to them as the From TelURI table and the To TelURI table.

Before you administer the dial plan settings in AE Services, review the topics that are appropriate for your switch.

If your switch uses a dial plan with fixed-length extensions, see the following topics:

- [From TelURI settings for fixed-length extensions](#) on page 139
- [To TelURI settings for fixed-length extensions](#) on page 141

If your switch uses a dial plan with variable-length extensions, see the following topics:

- [From TelURI settings for variable-length extensions](#) on page 142
 - [To TelURI settings for variable length extensions](#) on page 144
-

Pattern matching -- using Pattern and RegEx (regular expressions)

You can use one of the following two methods of "analyzing" or "matching" dial plan strings, as follows:

- **Pattern** - Select **Pattern** when you want to use a digit string as a way of detecting the presence of a specific sequence of digits in an incoming dial string. When you select Pattern you can create a matching string based on literal digits (0 through 9), one character literal (the #), and one special character, the asterisk (*) which will match any digit or sequence of digits. If you select **Pattern**, valid dial string characters are: all digits (0-9), the number sign (#), and the asterisk (*). For more information about using pattern matching, see the following help topics:
- **RegEx** - Select **RegEx** (regular expression) when you want to use a Java regular expression to analyze an incoming dial string. In certain cases (especially variable extension), RegEx rules will allow an administrator to minimize the number of rules that must be administered.

Regular expressions rely on symbolic notation - grouping of digits and special characters for analyzing incoming dial strings. For example, ([0-5]\\d{0,3}) is a regular expression which matches extensions that start with digits 0 - 5, and are 1 to 4 digits in length. If you are using regular expressions, you have the option of specifying a minimum, maximum or delete length. Specifying a minimum, maximum, or delete length fields do not apply to regular expressions. These field apply to pattern matching only.

You can mix rule types

A From TelURI table in the AE Services Management Console can consist of rules based on the **Pattern** setting and rules based on the **RegEx** setting. That is, you can create a From TelURI table that uses rules based on Pattern and rules based on RegEx.

Valid dial string characters and using the asterisk

For AE Services dial plan settings, valid dial string characters are: all digits (0-9), the number sign (#), and the asterisk (*).

The asterisk or number sign as literals

If your dial plan uses the asterisk or the number sign, and you need to configure a dial plan rule that detects the asterisk and the number sign, you must precede them with a backslash. For example to interpret the asterisk as a literal you would use * and to interpret the number sign as a literal you would use \#.

For example, if you need to have the asterisk interpreted as a literal asterisk in either the Matching Pattern field or the Replacement String Field of a From TelURI or a To TelURI table, you must precede the asterisk with a backslash. If you do not precede the asterisk with a backslash, it will be interpreted as a wildcard value for any valid character.

The asterisk as a wildcard

When you want to use the asterisk as a wildcard for any character, you must use it as a single character (by itself). That is, when used as a wildcard, the asterisk can not be preceded or followed by any other character.

The From Tel URI table

The **From TelURI** table determines the way that AE Services processes inbound E.164 numbers. Generally speaking, AE Services applies matching criteria to the incoming number. When the number satisfies the matching criteria, AE Services manipulates the digits and passes the number to Communication Manager (only one rule is applied for each number). When setting up the From TelURI settings, you can specify up to 200 rules. Each row in the table represents a rule. The rules are processed in order from top to bottom.

If you have a rule that contains a wildcard (* - asterisk) for the Minimum Length, Maximum Length, and Pattern match, it always must be the last rule in the list, and it must be a single asterisk (by itself). If you need to treat the asterisk as a literal in either the Pattern Match or the Replacement fields, you must precede it with a backslash, for example: *. Also, if your dial plan uses a number sign and you need to treat it as a literal in the Pattern Match field, you must precede it with a backslash.

Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
11	11	1303538	4	(field is empty)
11	11	1303	1	9
*	*	*	0	9011

The To TelURI table

The **To TelURI** table determines the way that the AE Services processes outbound E.164 numbers. Generally speaking, AE Services applies matching criteria to the outgoing number. When the number satisfies the matching criteria, AE Services manipulates the digits and passes the number to Microsoft Office Communicator (only one rule is applied for each number). When setting up the To TelURI settings, you can specify up to 200 rules. Each row in the table represents a rule. The rules are processed in order from top to bottom.

If you have a rule that contains a wildcard (* - asterisk) for the Minimum Length, Maximum Length, and Pattern match, it always must be the last rule in the list, and it must be a single asterisk (by itself). If you need to treat the asterisk as a literal in either the Pattern Match or the Replacement fields, you must precede it with a backslash, for example: *. Also, if your dial plan uses a number sign and you need to treat it as a literal in the Pattern Match field, you must precede it with a backslash.

Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
7	7	538	0	1303
7	7	852	0	1732
10	10	*	0	1

From TelURI settings for fixed-length extensions

The following example demonstrates how to administer the **From TelURI** settings in the AE Services Management Console to support a dial plan for a switch using fixed-length-extensions. This switch supports three different extension prefixes: 538, 852, and 444. The 538 prefix is used for extensions hosted on that switch, and the other two prefixes are used for switches connected via QSIG.

Example - From TelURI rules for fixed-length extensions

	Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
A	11	11	1303538	4	(blank) ¹
B	11	11	1732852	4	(blank)
C	11	11	1720444	4	(blank)
D	11	11	1303	1	9
E	11	11	1720	1	9
F	11	11	1	0	9
G	*	*	*	0	9011

1. Blank means the replacement field is empty.

How the From TelURI rules process numbers for fixed-length extensions

- A** AE Services receives **+13035381234**, an 11-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 7 digits (**1303538**) are a pattern match, AE Services deletes the first 4 digits (**1303**) and does not prepend any digits. AE Services sends **5381234** to the switch.
- B** AE Services receives **+17328521234**, an 11-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 7 digits (**1732852**) are a pattern match, AE Services deletes the first 4 digits (**1732**) and does not prepend any digits. AE Services sends **8521234** to the switch.
- C** AE Services receives **+17204441234**, an 11-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 7 digits (**1720444**) are a pattern match, AE Services deletes the first 4 digits (**1720**) and does not prepend any digits. AE Services sends **4441234** to the switch.
- D** AE Services receives **+13036791234**, an 11-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 4 digits (**1303**) are a pattern match, AE Services deletes the first digit (**1**), and prepends **9** to the number. AE Services sends **93036791234** to the switch.

- E** AE Services receives **+17202891234**, an 11-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 4 digits (**1720**) are a pattern match, AE Services deletes the first digit (**1**), replaces it with a **9**. AE Services sends **97202891234** to the switch.
- F** AE Services receives **+18183891234**, an 11-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first digit (**1**) is a pattern match, AE Services deletes no digits, and prepends a **9** to the number. AE Services sends **918183891234** to the switch.
- G** AE Services receives **+4926892771234**, a 13-digit number, from Communication Manager. Because the minimum length, maximum length, and pattern match are set up with the wild card, any number is permitted. AE Services deletes no digits, prepends **9011** to the number and sends **90114926892771234** to the switch.

To TelURI settings for fixed-length extensions

The following example demonstrates how to administer the **To TelURI** settings in the AE Services Management Console to support a dial plan for a switch using fixed-length-extensions. This switch supports three different extension prefixes: 538, 852, and 444. The 538 prefix is used for extensions hosted on that switch, and the other two prefixes are used for switches connected via QSIG.

Example - To URI rules for fixed-length extensions

	Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
A	7	7	538	0	1303
B	7	7	852	0	1732
C	7	7	444	0	1720
D	5	5	2	0	173285
E	5	5	4	0	172044
F	10	10	*	0	1

How the To TelURI rules process numbers for fixed-length extensions

- A** AE Services receives **5381234**, a 7 digit number, from the switch. Because the number is within the minimum and maximum length requirements, and the first three digits (**538**) are a pattern match, AE Services deletes no digits, and prepends **1303** to the number. AE Services sends **+13035381234** to Communicator.
- B** AE Services receives **8521234**, a 7 digit number, from the switch. Because the number is within the minimum and maximum length requirements, and the first three digits (**852**) are a pattern match, AE Services deletes no digits, and prepends **1732** to the number. AE Services sends **+17328521234** to Communicator.
- C** AE Services receives **4441234**, a 7-digit number, from the switch. Because the number is within the minimum and maximum length requirements, and the first three digits (**444**) are a pattern match, AE Services deletes no digits, and prepends **1720** to the number. AE Services sends **+17204441234** to Communicator.
- D** AE Services will sometimes receive a 5 digit extension from a networked switch, even if the local dial plan is 7 digits (see [Dial Plan tips](#) on page 146). In this case, AE Services receives a 5 digit number **21234**. Based on the matching pattern of **2** at the beginning. AE Services prepends **173285** to the number and sends **+17328521234** to Communicator.
- E** AE Services will sometimes receive a 5 digit extension from a networked switch, even if the local dial plan is 7 digits (see [Dial Plan tips](#) on page 146). In this case, AE Services receives a 5 digit number **41234**. Based on the matching pattern of **4** at the beginning, AE Services prepends **172044** to the number and sends **+17204441234** to Communicator.
- F** AE Services receives a 10-digit number, **2126711234** from the switch. Based on the matching pattern of any 10-digit string, AE Services deletes no digits and prepends **1** to the number. AE Services sends **+12126711234** to Communicator.

From TelURI settings for variable-length extensions

The following example demonstrates how to administer the **From TelURI** settings in the AE Services Management Console to support a dial plan that uses variable-length extensions. This example assumes the following:

- The customer owns numbers +4969100 through +4969105 in the dial plan, but does not own +4969106 and higher.
- The dial plan accommodates 1- to 4-digit extensions
- The ARS code is 0, the inter-region code is 0, and the international dial code is 00. The ARS code, which in this case is 0, is always included before the inter-region code and international dial code.

Example - From TelURI rules for variable-length extensions

	Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
A	8	11	49697100	7	(blank) ¹
B	8	11	49697101	7	(blank)
C	8	11	49697102	7	(blank)
D	8	11	49697103	7	(blank)
E	8	11	49697104	7	(blank)
F	8	11	49697105	7	(blank)
G	*	*	4969	4	0
H	*	*	49	2	00
I	*	*	*	0	000

1. Blank means the replacement field is empty.

How the From TelURI rules process numbers for variable-length extensions

- A** AE Services receives **+49697100**, an 8-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the number is an exact pattern match, AE Services deletes the first 7 digits (**4969710**) and does not prepend any digits to the number. AE Services sends **0** to Communication Manager.
- B** AE Services receives **+49697101988**, an 11-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 8 digits (**49697101**) are a pattern match, AE Services deletes the first 7 digits and does not prepend any digits to the number. AE Services sends **1988** to Communication Manager.
- C** AE Services receives **+4969710211**, a 9-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 8 digits (**49697102**) are a pattern match, AE Services deletes 7 digits and does not prepend any digits to the number. AE Services sends **211** to Communication Manager.

- D** AE Services receives **+496971034**, a 9-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 8 digits (**49697103**) are a pattern match, AE Services deletes 7 digits and does not prepend any digits to the number. AE Services sends **34** to Communication Manager.
- E** AE Services receives **+4969710494**, a 10-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 8 digits (**49697104**) are a pattern match, AE Services deletes 7 digits and does not prepend any digits to the number. AE Services sends **494** to Communication Manager.
- F** AE Services receives **+4969710598**, a 10-digit number, from Communicator. Because the number is within the minimum and maximum length requirements, and the first 8 digits (**49697105**) are a pattern match, AE Services deletes 7 digits and does not prepend any digits to the number. AE Services sends **598** to Communication Manager.
- G** AE Services receives **+496971060**, a 9-digit number, from Communicator. Because the wild card (*) permits a number of any length, and the first 4 digits (**4969**) are a pattern match, AE Services deletes the first 4 digits and prepends **0** to the number. AE Services sends **071060** to Communication Manager.
- H** AE Services receives **+49306441234**, an 11-digit number from Communicator. Because the wild card (*) permits a number of any length, and the first 2 digits (**49**) are a pattern match, AE Services deletes the first 2 digits and prepends **00** to the number. AE Services sends **00306441234** to Communication Manager.
- I** AE Services receives **+17328521234**, an 11 digit number, from Communicator. Because the minimum length, maximum length, and pattern match are set up with the wild card, any number is permitted. AE Services deletes no digits, prepends **000**, and sends **00017328521234** to Communication Manager.

To TelURI settings for variable length extensions

The following example demonstrates how to administer the **To TelURI** settings to support a dial plan that uses variable-length extensions. The set of rules in this example assumes the following:

- All numbers less than or equal to 4 digits are extensions. This assumption allows the table to have one rule, rather than 6, for all extension starts. In some cases, it might be necessary to be more specific.
- International numbers start with 00, and inter-region numbers start with 0. Any digits other than 0 or 00 are assumed to be local digits. AE Services prepends 4969, which represents country or city codes. Keep in mind that you must carefully analyze your dial plan before you attempt to apply a catch-all rule such as this.

Example - To TelURI rules for an installation with variable length extensions

	Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
A	1	4	*	0	4969710
B	*	*	00	2	
C	*	*	0	1	49
D	*	*	*	0	4969

How the To TelURI rules process numbers for variable length extensions

- A** AE Services receives **1234**, a 4-digit number from the switch. Because the number is within the minimum and maximum length requirements, and the wild card (*) permits a match of any 1- to 4-digit number, AE Services deletes no digits and prepends **4969710** to the number. AE Services sends **49697101234** to Microsoft Office Communicator.
- B** AE Services receives **0017328524321**, a 13-digit number, from the switch. Because the number is not within the range specified by the 1- to 4-digit rule (A) it satisfies this rule, which permits a number of any length where first two digits (**00**) are a pattern match. AE Services deletes the first 2 digits, prepends nothing to the number, and sends **17328524321** to Microsoft Office Communicator.
- C** AE Services receives **0306441234**, a 10-digit number, from the switch. Because the number is not within the range specified by the 1- to 4-digit rule (A) it satisfies this rule, which permits a number of any length where first digit (**0**) is a pattern match. AE Services deletes the first digit, prepends **49** to the number, and sends **49306441234** to Microsoft Office Communicator.
- D** AE Services receives **45427**, a 5-digit number, from the switch. Because the number is not within the range specified by the 1- to 4-digit rule (A) it satisfies this "catch-all" rule that permits a number of any length and any pattern of digits. AE Services deletes no digits, prepends **4969** to the number, and sends **496945427** to Microsoft Office Communicator.

Pattern matching -- using Pattern and RegEx (regular expressions)

You can use one of the following two methods of "analyzing" or "matching" dial plan strings, as follows:

- **Pattern** - Use Pattern when you want to use a digit string as a way of detecting the presence of a specific sequence of digits in an incoming dial string. When you select Pattern you can create a matching string based on literal digits (0 through 9), one character literal (the #), and one special character, the asterisk (*) which will match any digit or sequence of digits. If you select **Pattern**, valid dial string characters are: all digits (0-9), the number sign (#), and the asterisk (*).
- **RegEx** - Use RegEx (regular expression) when you want to use a Java regular expression to analyze an incoming dial string. Regular expressions rely on symbolic notation - grouping of digits and special characters for analyzing incoming dial strings. For example, ([0-5]\d{0,3}) is a regular expression which matches extensions that start with digits 0 - 5, and are 1 to 4 digits in length. If you are using regular expressions, you have the option of specifying a minimum, maximum or delete length. Specifying a minimum, maximum, or delete length fields do not apply to regular expressions. These field apply to pattern matching only.

You can mix rule types : A From the TelURI table in the AE Services Management Console can consist of rules based on the **Pattern** setting and rules based on the **RegEx** setting. That is, you can create a From TelURI table that uses rules based on Pattern and rules based on RegEx.

Using the asterisk : If you have a rule that contains an asterisk (*) for the Minimum Length, Maximum Length, and Pattern match it must be the last rule in the list.

[Table 10](#) is an example that depicts a mix of regular expression rules and simple pattern match rules.

Table 10: Example of Incoming rules for RegEx

	Min length	Max length	Pattern	Delete Length	Replacement
A			4969710([0-5]\d{0,3})		\$1
B			4969(\d{1,})		0\$1
C	*	*	49	2	00
D	*	*	*	1	000

- A** This rule uses a RegEx pattern to specify that Call Control Services is to look for a string starting with **4969710**, matching an extension that starts with **0** through **5** and is **1** to **4** digits in length.

The parentheses around the extension indicate a group, which is correlated with the **\$1** in the replacement string. The **\$1** says to replace the matching string (the entire E.164 number) with the group designated by the parentheses (the extension).
- B** This rule uses a RegEx pattern to specify that Call Control Services is to look for a string starting with **4969**, followed by 1 or more digits.

The parentheses again correlate with the **\$1** in the replacement string, which says to take the group (the E.164 number without country code or city code) and to add a **0** in front of it (the ARS code).
- C** This rule uses a simple pattern match. The asterisk in the Min and Max length permits a number of any length. The pattern indicates that Call Control Services is to look for a string starting with **49**. When it detects 49, it deletes the first 2 digits, and replaces them with **00**.
- D** This rule uses a wildcard pattern match. The asterisk in the Min and Max length permits a number of any length, and the asterisk in the pattern permits pattern of digits. When any number that does not satisfy the first 3 rules (A,B, and C) is detected, Call Control Services deletes the first digit and replaces it with **000**.

Dial Plan tips

When switches are networked together using ISDN QSIG tie trunks or ISDN tie trunks, in some call scenarios Communication Manager sends extension numbers from the networked switch to the AE Server. The format of these extension numbers may be different than the format of local extension numbers.

To optimize the experience of Microsoft Office Communicator users, be sure to administer "To TelURI" rules for the networked switch, or switches, as well as the local switch. Additionally, if the networked switch has a different extension length than the local switch, extensions might be reported with both the local extension length and the networked extension length. Be sure to administer "To TelURI" rules that can successfully convert both extension lengths for the networked switch.

Also, you might need multiple entries in the "To TelURI" rules for the networked switch if that switch has a different extension length than the local switch.

Administering dial plan settings on a per-switch basis

Follow this procedure to administer the dial plan settings for a switch connection you have already administered. AE Services uses the dial plan information to convert E.164 phone numbers to switch extensions (From TelURI) and switch extensions to E.164 phone numbers (To TelURI). For more information, see [About the From TelURI and To TelURI rules](#) on page 135.

Note:

If your configuration of the AE Services implementation for Microsoft Office Communications Server 2007 uses a number of switches that all have the same dial plan, use the procedure described in [Administering default dial plan settings](#) on page 148. By using the default settings, you enter the dial plan settings only once.

1. From the browser on your AE Services administrative workstation, log in to the AE Services Management Console.
2. From the main menu of the AE Services Management Console, select **Communication Manager Interface > Dial Plan > Switch Administration**.
3. From the Switch Dial Plan Administration page, select the connection name for the switch you want to administer, for example **aeslcswitch**, and click **Details**.

AE Services displays the Dial Plan Settings - Conversion Rules for aeslcswitch page. This page provides you with a way to Add, Edit, Delete and Reorder "From TelURI" conversion rules and "To TelURI" conversion rules. The Edit, Delete, and Reorder functions apply to existing rules. This example assumes the initial state of the page -- no conversion rules exist -- and focuses on adding two conversion rules, one for From TelURI and one for To TelURI.

4. Follow Step a to add a From TelURI conversion rule, and follow Step b to add a To TelURI conversion rule.
 - a. In the From TelURI section of the page, under the blank display area, click **Add**.
 1. From the Add Dial Plan to aeslcswitch page, complete the fields for the **From TelURI** settings, based on your dial plan.
 2. Click **Apply Changes**. Your browser displays the Add Dial Plan page, which asks you to confirm your dial plan changes. From the Add Dial Plan page, click **Apply**.
At this point you have added one From TelURI conversion rule. If you want to add another From TelURI conversion rule, you must repeat Steps a, 1, and 2.
 - b. In the To TelURI section of the page, under the blank display area, click **Add**.
 1. From the Add Dial Plan to aeslcswitch page, complete the fields for the **To TelURI** settings, based on your dial plan.

2. Click **Apply Changes**. Your browser displays the Add Dial Plan page, which asks you to confirm your dial plan changes. From the Add Dial Plan page, click **Apply**.

At this point you have added one To TelURI conversion rule. If you want to add another To TelURI conversion rule, you must repeat Steps b, 1, and 2.

At this point the changes you made to your dial plan settings are in effect, and you do not have to restart the AE Server.

Administering default dial plan settings

If you use more than one switch in your configuration of the AE Services implementation for Microsoft Office Communications Server 2007, and all the switches have common dial plan settings, you can use the Default Dial Settings page as a template. When you add a switch connection for AE Services implementation for Microsoft LCS, the dial plan settings that you have administered on the Default Dial Plan settings page are applied to that switch connection. Use this procedure to set up the Default Dial Settings page.

1. From the browser on your AE Services administrative workstation, log in to the AE Services Management Console.
2. Select **Communication Manager Interface > Dial Plan > Default Settings**.

AE Services displays the Dial Plan Settings - Conversion Rules for default page. This page provides you with a way to Add, Edit, Delete and Reorder "From TelURI" conversion rules and "To TelURI" conversion rules. The Edit, Delete, and Reorder functions apply to existing rules. This example assumes the initial state of the page -- no conversion rules exist -- and focuses on adding two conversion rules, one for From TelURI and one for To TelURI.
3. Follow Step a to add a From TelURI conversion rule, and follow Step b to add a To TelURI conversion rule.
 - a. In the From TelURI section of the page, under the blank display area, click **Add**.
 1. From the Add Dial Plan to default page, complete the fields for the From TelURI settings, based on your dial plan.
 2. Click **Apply Changes**. Your browser displays the Add Dial Plan page, which asks you to confirm your dial plan changes." From the Add Dial Plan page, click **Apply**.

At this point you have added one From TelURI conversion rule. If you want to add another From TelURI conversion rule, you must repeat Steps a, 1, and 2.
 - b. In the To TelURI section of the page, under the blank display area, click **Add**.
 1. From the Add Dial Plan to default page, complete the fields for the To TelURI settings, based on your dial plan.

2. Click **Apply Changes**. Your browser displays the Add Dial Plan page, which asks you to confirm your dial plan changes. From the Add Dial Plan page, click **Apply**.

At this point you have added one To TelURI conversion rule. If you want to add another To TelURI conversion rule, you must repeat Steps b, 1, and 2.

At this point the changes you made to your dial plan settings are in effect, you do not have to restart the AE Server.

Administering AE Services access to Active Directory

Follow this procedure to set up the connection to Active Directory for AE Services.

- The examples in this procedure use the "example.com" domain name.
 - See also, [DN entries and scope of search](#) on page 152 for a diagram depicting Distinguished Names.
1. From the browser on your AE Services administrative workstation, log in to the AE Services Management Console.
 2. From the main menu of the AE Services Management Console, select **Security > Enterprise Directory**.
 3. Complete the Enterprise Directory page, as follows.
 - User DN for Query Authentication - Type the DN for the user object that AE Services uses for accessing the Active directory. Based on how users are set up in Active Directory, the user object could correspond to a Full Name, a Display Name, or a User logon name. Here are two examples:
`cn=Grey\,AI,cn=sertech,cn=services,cn=users,dn=example,dc=com`
`cn=RTCAAdmin,cn=devtech,cn=services,cn=development,dc=example,dc=com`

Note:

If a DN attribute has a comma within it, you must precede it with a backslash. For more information, see [Making changes on the Enterprise Directory Configuration page](#) on page 153. If you are not sure what the DN is for a user object, see [Determining the DN for a user object](#) on page 153.

- Password - Type a password to be used for Active Directory access; retype the same password in the Confirm Password field. This Active Directory password is stored in an encrypted format on the AE Server.
- Base Search DN - The Base Search DN is less specific than the User DN. Type the DN of the node that includes all user accounts that need access to the AE Services and Microsoft Office Communications Server 2007 integration in the following format:
`cn=users,dc=example,dc=com`
- HostName/IP Address - Type the IP address or Host Name of the Domain Controller that runs Active Directory.
- Port - (used for Active Directory access) - Change the default port number to an appropriate value for your configuration. The default is 389 (the port assignment for LDAP).
- Secondary HostName/IP Address - Accept the default (leave the field blank). This field does not apply to the AE Services implementation for Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007.

- Secondary Port - Accept the default (leave the field blank). This field does not apply to the AE Services implementation for Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007.
 - User ID Attribute Name - This setting defaults to **uid**, which is the default for AE Services User Management. For Microsoft Active Directory you must change this setting. The default setting for Microsoft Active Directory is **samaccountname**. If your implementation does not use the default for Microsoft Active Directory, enter the name of the attribute that is appropriate for your implementation.
 - User Role Attribute Name - Enter the name of the attribute for the user role that your Enterprise Directory Server uses, for example roles.L
 - Change Password URL - Accept the default (leave the field blank). This field does not apply to the AE Services implementation for Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007.
 - LDAP-S - Select LDAP-S if your configuration uses a TLS connection from AE Services to your Enterprise Directory Server.
4. Select **Apply Changes** to put your changes into effect.

DN entries and scope of search

The DN entries you specify in the User DN for Query Authentication and the Base Search DN field are, in effect, search paths in an LDAP structure.

Consider the DN examples used in [Administering AE Services access to Active Directory](#) on page 150:

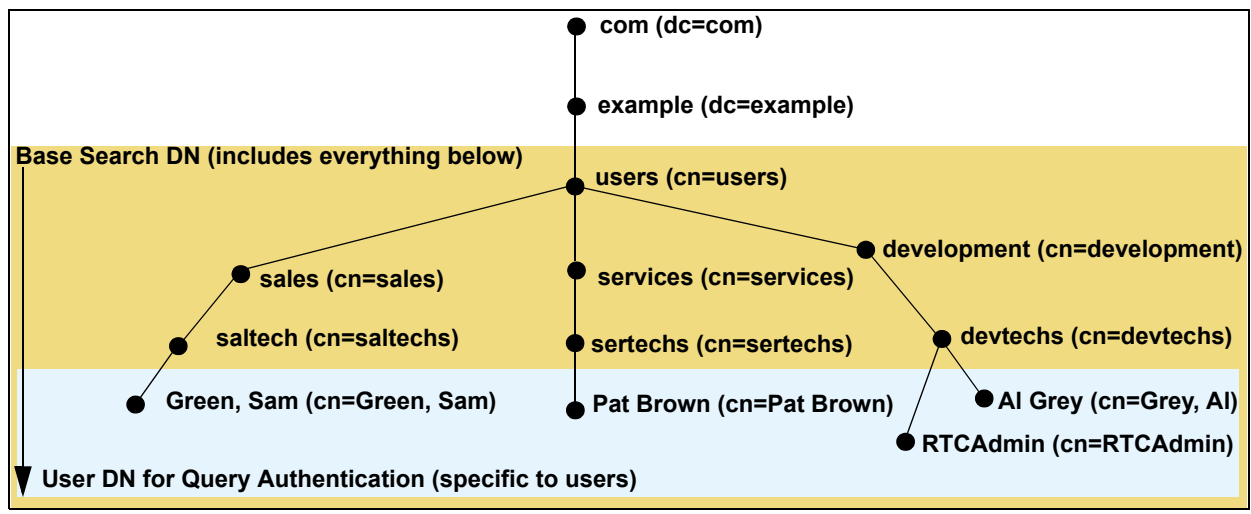
- User DN for Query Authentication
cn=Pat Brown,cn=sertech,cn=services,cn=users,dc=example,dc=com
- Base Search DN
cn=users,dc=example,dc=com

Both DNs are unique, but the User DN for Query Authentication is more specific than the Base Search DN.

Avoid making the Base Search DN too specific

If you were to specify a Base Search DN of **cn=development,cn=users,dc=example,dc=com** the users in services and sales would not be able to establish a session. Instead, you should specify a Base Search DN that is less specific, such as **cn=users,dc=example,dc=com**.

Figure 6: DN entries and scope of search



Making changes on the Enterprise Directory Configuration page

Follow these guidelines for completing the "User DN for Query Authentication" and the "Base Search DN" fields on the Enterprise Directory Configuration Web page in the AE Services Management Console.

If you are entering a DN attribute that has an internal comma, you must precede it with a backslash, for example: `cn=Green\,Sam,cn=saltech,cn=sales,cn=users,dc=example,dc=com` . This is necessary because the comma is a delimiter that is used for separating DN attribute-value pairs. When you click **Apply Changes**, AE Services processes the data you submit.

As a result of this processing, the backslash gets removed from any DN attributes that are in the "User DN for Query Authentication" and the "Base Search DN" fields. When the AE Services Management Console redisplay the Enterprise Directory Configuration Web page, these attributes will be displayed with a single backslash.

Note:

Whenever you are making changes to any of the fields on the Enterprise Directory Configuration page in the AE Services Management Console, make sure that each DN attribute with an internal comma is preceded by a backslash before you click **Apply Changes**.

Determining the DN for a user object

If you are not sure what the DN for the user object is, follow this procedure from the Active Directory Services domain controller.

1. At the command prompt, run the `csvde -f` command against the Users domain and save the output to a file (`csvde -f file.csv`).
2. Open the file with a text editor or a spreadsheet program and locate the appropriate user object (which can be the Full Name, Display Name, or User logon name on the Active Directory User Properties dialog).
3. Copy the DN for the user object, and paste it into User DN for Query Authentication field.

Configuring Microsoft Office Communications Server 2007 for AE Services

When you set up the Microsoft Office Communications Server 2007, you will need to make sure that you have followed the necessary steps for configuring the server. These steps are listed in "Configuring the Server" (a subsection of "Deploying Telephony") in the *Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide*. Use this table as a guideline as you read through "Configuring the Server" in the *Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide*.

Steps listed in Microsoft Telephony Planning and Deployment Guide		Notes
1	Update Microsoft Office Communications Server 2007 schema.	Completed when you carried out the Active Directory Preparation Basic Steps (see Task 2 in Table 8: Checklist for integrating AE Services with Microsoft Office Communications Server 2007 on page 109).
2	Normalize the phone numbers.	Completed when you set up the Address Book Service (see Task 9 in Table 1: Checklist for Live Communications Server on page 38).
3	Enable RCC Extensions.	Follow the procedure for Enabling Remote Call Control in Active Directory on page 155 of this document. Also, see the Tip following this table.
4	Set up connections.	Follow the procedure for Setting up connections on page 157 of this document.
5	Set up static routes.	Follow the procedures for Configuring a static route on page 157 and Specifying the AE Server as an authorized host on page 158.
6	Set controlled line configuration.	This is accomplished when you complete the three previous tasks: 3) Enable RCC Extensions, 4) Set up connections, and 5) Set up Static Routes.
7	Configure a CTI link.	Completed when you administered a CTI link on Communication Manager, and you administered a TSAPI link in the AE Services Management Console.
8	Configure PBX SIP Proxy.	Not applicable.

**Tip:**

Microsoft provides a utility called **Office Communicator 2005 Phone Normalization Script** that enables you to make bulk changes to Active Directory. If you run this utility, you do not have to do per-user manual administration. To get this phone normalization script, go to www.microsoft.com, and locate **Microsoft Office Communications Server 2007 with SP1 Resource Kit**. The resource kit includes this phone normalization script.

Enabling Remote Call Control in Active Directory

Enabling Remote Call Control in Active Directory refers to setting up users so they can control their phones from the Microsoft Office Communicator client. Follow this procedure to enable a specific user to control a specific phone from Microsoft Office Communicator.

1. From the Microsoft Office Communications Server 2007, start the management console for **Active Directory Users and Computers**.
2. From the left pane of the console, select **Active Directory Users and Computers**.
3. Expand the tree for your pool node (or server node), and click **Users**.
4. From the list of users in the right pane, right click a user name, and select **Properties**.
5. From the Properties dialog box, select the **Communications** tab.
6. From the Communications tab, click **Configure...**. Microsoft Office Communications Server 2007 displays the User Options dialog box.

User Options

Telephony
Select a telephony option. These settings affect only those calls that are routed through IP-PSTN or remote call control gateways.

☐ Enable PC-to-PC communication only

☒ Enable Remote call control

☐ Enable Enterprise Voice

☐ Enable PBX integration

Note: To enable both remote call control and PBX integration, you must specify a Server URI below.

Policy:

Server URI:

Line URI:

Federation

☐ Enable federation

☒ Enable remote user access

☒ Enable public IM connectivity

Archiving

☐ Archive internal IM conversations

☐ Archive federated IM conversations

Note: Archiving settings cannot be changed unless the global setting allows per user configuration.

☒ Enable enhanced presence

Note: Enhanced presence cannot be changed once it has been set.

7. Click the option button for Enable Remote call control and then in the LINE URI text box, type the appropriate telephone number in Tel URI format. For example:
tel:+13035389000.

Note:

If necessary, you can use the following format: **tel:E.164 phone number;ext=extension** (for example, **tel:+13035389000;ext=9000**).

In most cases, the extension (ext=extension) is not required. It is required only under these circumstances:

- If the user's extension does not match the last digits of their E.164 Direct Inward Dial (DID) number.
 - If the dial plan information has not been configured for the user's switch.
8. In the Remote Call Control SERVER URI field, type the destination URI in the following format: **sip:aes@AE_server_FQDN.**

where: **aes** is the identifier for the AE Server and **AE_server_FQDN** is a term you substitute with the fully qualified domain name of your AE Server. For example:
sip:aes@myaesserver.example.com .

Setting up connections

From the management console of the Microsoft Office Communications Server 2007, follow these steps to set up the connection that Microsoft Office Communications Server 2007 uses for sending and receiving SIP messages.

1. Start the management console from the Microsoft Office Communications Server 2007
2. Expand the tree to display the FQDN of the server node, and right-click on the fully qualified domain name the Microsoft Office Communications Server 2007, for example: **mylcserv.example.com**
3. From the "mylcserv.example.com" Properties dialog box, verify that there is a MTLS port at 5061, unless you have assigned it to another port (5061 is the default) .
4. Select the Certificate tab. Verify that the server certificate is correct, and click **OK**.

Configuring a static route

Handling SIP traffic from the Microsoft Office Communications Server 2007 to AE Services requires creating a static route between the Microsoft Office Communications Server 2007 (or servers) and the AE Services server. This procedure is based on a configuration using Microsoft Office Communications Server 2007 Enterprise Edition.

Follow this procedure to configure a static route between the Microsoft Office Communications Server 2007 and the AE Services Server.

1. Open the Microsoft Office Communications Server 2007 administrative snap-in: Click **Start**, point to **All Programs > Administrative Tools**, and click **Microsoft Office Communications Server 2007**.
2. In the left pane of the administrative snap-in, expand the **Forest** node, and then expand **Communications servers and pools**. (For Standard Edition, **Communications servers and pools** represents the server node; for Enterprise Edition, it represents the pool node.)
3. Expand the pool node (for Standard Edition) or server node (Enterprise Edition), then right-click the **Front Ends** node and select **Properties**.
4. From the Properties dialog box, select the **Routing** tab, and click **Add**.
5. Complete the fields on the Add Static Route dialog box as follows:
 - a. in the Domain field, type the fully qualified domain name of the AE Server (for example, **myaeserv.example.com**).
 - b. In the FQDN field, type the fully qualified domain name of the AE Server (for example, **myaeserv.example.com**).
 - c. In the Transport field, select **TLS**.

- d. In the Port field, type the port that was administered as the **TR87 Port** in the AE Services Management Console. The default is **4723**.
- e. (The next two steps apply to Microsoft Office Communications Server 2007 Standard Edition only.)
 1. Click **Select Certificate**.
 2. From the Select Certificate dialog box, select the **<Microsoft Office Communications Server 2007 certificate>**, and click **OK** to close the Select Certificate dialog box. Continue with Step g.
- f. Click **OK** to close the Add Static Route dialog box.

Specifying the AE Server as an authorized host

Follow this procedure to set up AE Services as an authorized host. This procedure is based on a configuration using Microsoft Office Communications Server 2007.

1. Open the Microsoft Office Communications Server 2007 management console, and in the left pane, expand the **Forest** node.
2. Expand the pool node (for Standard Edition) or server node (Enterprise Edition), then right-click the **Front Ends** node and select **Properties**.
3. From the Properties dialog box, select the **Host Authorization** tab, and click **Add**.
4. Complete the fields on the Add Authorized Host dialog box as follows:
 - a. In the FQDN field, type the fully qualified domain name of the AE Server (for example, **myaeserver.example.com**).
 - b. Select the check boxes (enable) for the following settings: **Throttle as server** and **Treat As Authenticated**. Make sure that **Outbound only** is not checked (disabled).
 - c. Click **OK**.

For more information about setting up host authorization, refer to the figure called "Edit Authorized Host" in the *Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide*.

Microsoft Office Communicator users - group policy settings

Microsoft Office Communicator users must have the following feature configured as a policy settings:

- Enable Phone Control - The option to Enable Phone Control is called **Telephony Mode**. You must enable the Telephony Mode option must be **Enabled** and set Telephony Mode to **2 = RCC Enabled**.

For information about group policy settings, see "Group Policy Configuration (.adm)," in *Microsoft Office Communicator 2005 Planning and Deployment*.

About authentication and authorization

For the AE Services implementation for Microsoft LCS, authentication and authorization are handed as follows.

- AE Services authenticates Microsoft Office Communications Server 2007 by using TLS to verify the Microsoft Office Communications Server 2007 certificate.
- The Microsoft Office Communications Server 2007 authenticates (confirms the identify) of the Microsoft Office Communicator user.
- The AE Server, in turn, authorizes (grants permission to) the user for device control.
- To carry out authorization, AE Services verifies that the requested Tel URI matches the Tel URI in the user record before granting access to a device.

Note:

When you complete the procedure to enable the Communicator client for RCC, ([Enabling Remote Call Control in Active Directory](#) on page 155) you are provisioning Active Directory with the user information that AE Services queries for.

Using the TR/87 Test features

Follow these steps to use TR/87 test features in the AE Services Management Console.

1. From the browser on your AE Services administrative workstation, log in to the AE Services Management Console.
2. From the main menu of the AE Services Management Console, select **Utilities > Diagnostics > AE Services > TR/87 Test**.
3. From the TR/87 Self Test page, select from the following tests:
 - **TR/87 Transport** -- use TR/87 Transport to verify that the installed certificate can be used to establish a SIP session on the loopback interface. This does not verify the far-end server certificate.
 - **TR/87 Service** -- use TR/87 Service to verify the following:
 - the caller is administered in Active Directory
 - the dial plan is administered for the caller's number
 - the user's telephone device can be monitored
 - **TR/87 Makecall** -- use TR/87 Makecall to verify that phone control is active for the user.

Note:

The TR/87 Makecall test depends on receiving confirmation of a call being established. In certain scenarios involving trunks this may not be available. The TR/87 Makecall test should be considered a valid test only when using two stations on the same switch to perform the test.

The Host AA setting and TR/87 test

The Host AA settings in the AE Services Management Console have an effect on the TR/87 Test utility. If you enable host authorization, the authorized hosts list must include the Peer Certificate CN (which is the Server Certificate Subject Name). Because the TR/87 Test utility depends on the Host AA settings and uses the same certificate that is used by Tomcat, you must restart the Web Server after adding a server certificate.

Administering Microsoft Office Communications Server 2007 for the agent login ID

Perform the following steps before signing in to Microsoft Office Communicator as an agent.

1. Log in to the Microsoft Office Communications Server 2007 server and open the Microsoft Office Communications Server 2007 console.
2. Click on **Communications servers and pools**, and select **Users**.
3. Right-click on the agent's **Display Name** and select **Properties**.
4. Click on **Advanced Settings...**
5. Enter the Tel URI parameter using the following format:

tel:agentID;phone-context=agent-login-id.domain

For example **tel:1234;phone-context=agent-login-id.example.com**

where:

- **agentID** is the agent's login ID, for example **1234**.
 - **example.com** is the domain name.
6. Next, have the agent log in to the Telephone / Softphone / Agent software that is to be used.
 7. Finally, have the agent sign in to Microsoft Office Communicator and verify that calls can be answered and made successfully.



Important:

Always sign out of Microsoft Office Communicator before logging off the physical device to ensure that the Microsoft Office Communicator sign in and the agent login states are always synchronized.

Re-synchronizing states

If the agent logs off the physical device first, Microsoft Office Communicator will be re-synchronized only after the next call is received or attempted. The yellow icon in the Microsoft Office Communicator status bar will provide a visual confirmation.

Usage Tips for the Do Not Disturb feature

The Do Not Disturb feature is fully functional for AE Services, Release 4.1, or later. You can activate or deactivate Do Not Disturb using either the Microsoft Office Communicator client or a physical phone.

For Do Not Disturb (DND) to function properly, you must administer a coverage path on the station, in Communication Manager. When you complete the Coverage path screen in Communication Manager, make sure that you enable **DND/SAC/Go to Cover** for inside calls and outside calls -- the settings for **Inside Call** and **Outside Call** should be **y**.

For information about administering a coverage path in Communication Manager, see "Creating coverage paths" in *Administrator Guide for Avaya Communication Manager*, 03-300509.

Recovering from a system outage

When AE Services returns to an operational state after an outage, you will be able to use Microsoft Office Communicator (Communicator) to place and control new calls. If you experience an outage, bear the following in mind:

- If you were on a call when an AE Services outage occurred, complete the call and manually hang up the phone so that your phone and Communicator are synchronized. When you are ready to start a new call in Communicator, your phone and Communicator will be synchronized.
- If Communicator signs you out as result of a network outage, you must sign in to Communicator again before you can control new calls. If you attempt to sign in during an AE Services outage, Communicator displays the warning icon along with the pop-up indicating that Communicator can not make phone calls.

Known issues

This section describes a few feature-related issues, as follows:

- [Setting up forwarding off-switch](#) on page 163
- [Using Call Forwarding and Send All Calls](#) on page 163
- [Using the Do Not Disturb feature](#) on page 164
- [Putting the active call on hold before starting a new call](#) on page 164
- [Clear Connection request on a held connection is not supported](#) on page 164
- [Bridging irregularities](#) on page 165
- [Missed Call e-mail](#) on page 165
- [Usage instructions for analog phones](#) on page 165.

Additionally, this section addresses the general issue that under certain conditions a party's telephone number will not be available to Microsoft Office Communicator. When this is the case, Microsoft Office Communicator can not display a telephone number or party identifier.

- [Unidentified caller in Microsoft Office Communicator window](#) on page 166
- [Communicator displays numbers with trunk notation](#) on page 167

Setting up forwarding off-switch

If you experience problems setting up forwarding off-switch (to your home or cell phone, for example) you should contact the Communication Manager administrator. There are certain settings in Communication Manager that could prevent your ability to set up forwarding off-switch.

Using Call Forwarding and Send All Calls

From the Microsoft Office Communicator, you can use Call Forwarding and Send All Calls as follows:

- You can set your phone to forward calls.
- You can set the Microsoft Office Communicator to forward calls relative to the client you are signed in to.
- You can set your phone to "Do Not Disturb" mode, which refers to Send All Calls (SAC) in AE Services.



CAUTION:

Keep in mind, however, that you should not press the Forwarding or the Send All Calls (SAC) buttons on a physical phone set. Pressing these buttons can cause the Microsoft Office Communicator to lose synchronization with the phone.

Using the Do Not Disturb feature

For Do Not Disturb (DND) to function properly, you must administer a coverage path on the station, in Communication Manager. When you complete the Coverage path screen in Communication Manager, make sure that you enable **DND/SAC/Go to Cover** for inside calls and outside calls -- the settings for **Inside Call** and **Outside Call** should be **y**.

For information about administering a coverage path in Communication Manager, see "Creating coverage paths" in *Administrator Guide for Avaya Communication Manager*, 03-300509.

Putting the active call on hold before starting a new call

Although this is listed as a known issue for the AE Services integration with Microsoft Office Live Communications Server 2005 and Microsoft Office Communicator 2005, this is not an issue for integration with Microsoft Office Live Communications Server 2007 and Microsoft Office Communicator 2007. Microsoft Office Communicator 2007 places a consultation call on your behalf.

Clear Connection request on a held connection is not supported

Communication Manager does not support a Clear Connection request on a held connection. For the Microsoft Office Communicator user, this means that if you have a held call and you press the red, "stop" button on the call windows, you will get an error message and the call will remain in the held state.

Bridging irregularities

In an AE Services and Live Communications Server 2005 or Office 2007 environment, the Microsoft Office Communicator might not behave as expected if you use bridged call appearances. Here are some examples of irregularities associated with bridged calls.

- If a user answers on a bridged extension, Microsoft Office Communicator continues to alert on the primary extension and eventually times out.
 - This bridging irregularity occurs when you administer EC500 phones with XMOBILE. If you administer EC500 phones with OPTIM, the bridging irregularities do not occur. For more information see, “Considerations for Extension to Cellular” in *Feature Description and Implementation for Avaya Communication Manager*, 555-245-205. OPTIM refers to Off-PBX Telephone Integration and Mobility.
- If you call someone whom has a bridged extension, the Microsoft Office Communicator conversation window might display either of the following:
 - an additional party on the call representing that bridged extension.
 - "Unidentified Caller"

Missed Call e-mail

Missed Call e-mail is sent only if the caller hangs up before the call goes to call coverage (voice mail).

Usage instructions for analog phones

If you use an analog phone, follow these special usage instructions.

Placing a call: method 1 - pick up the handset, then start the call in Communicator

1. With the Communicator window open, physically pick up the handset on your phone.

Note:

Upon hearing the dial tone, you have 10 seconds to place the call. After 10 seconds you will hear the intercept tone (alternating high and low tone). Once you receive the intercept tone, a Microsoft Office Communicator call will fail. If you attempt to place a call, you will receive an error notification in the Microsoft Office Communicator window.

2. From the Contacts list in the Microsoft Office Communicator window, right-click the **<name of the person you want to call>**, select **Call**, then click the **<phone number>**. Wait for the person you are calling to answer the phone. You will hear a ringback tone.

Microsoft Office Communicator displays the Conversation window. The status of your call is displayed in the Instant Message section of the window.

3. When the person you are calling answers the phone, start your voice conversation.
4. Once the voice conversation is over, physically hang up the handset and then close the Microsoft Office Conversation Window.

Placing a call: method 2 - start the call in Communicator, then pickup the handset

1. From the Contacts list in the Microsoft Office Communicator window, right-click the **<name of the person you want to call>**, select **Call**, then click the **<phone number>**.

Note:

You must pick up the handset within 5 seconds after clicking the phone number. If you do not pick up the handset within 5 seconds, the call will fail and Communicator will display an error message in the Instant Message section. Also note that your analog phone does not ring when the call is placed from Communicator.

Microsoft Office Communicator displays the Conversation window. The status of your call is displayed in the Instant Message section of the window.

2. Pick up the handset on your phone, and wait for the person you are calling to answer the phone. You will hear a ringback tone.
3. When the person you are calling answers the phone, start your voice conversation.
4. Once the voice conversation is over, physically hang up the handset and then close the Microsoft Office Conversation Window.

Answering a call with an analog phone

If you have an analog phone, you must pick up the handset to answer a call when your phone rings. Just pick up the handset as you normally would, and do nothing in Communicator.

Unidentified caller in Microsoft Office Communicator window

For the following reasons you might see "Unidentified Caller" in the Microsoft Office Communicator conversation window:

- The user you have called has a bridged extension.
- Your call went to a voice mail system. If your call is answered by a voice mail system, the voice mail system itself appears as an "Unidentified Caller."
- Your call went to Music-on Hold by way of a Voice Announcement with LAN (VAL) board on Communication Manager, causing you to lose phone control on your Microsoft Office Communicator. You can resolve this issue by upgrading Communication Manager with Service Pack 12866.
- You manually entered a number in the FIND box that was not in the proper format.

If you are manually typing the number in the FIND box, be sure to enter the full phone number, including the country code and either the area code or the region code, whichever is appropriate. Depending on how the system has been administered, it might be acceptable to not include the country code in the entered number. In all cases, the Automatic Route Selection (ARS) code for the outside line (9, for example) should not be included.

Communicator displays numbers with trunk notation

Microsoft Office Communicator displays telephone numbers as trunk identifiers instead of telephone numbers in both transfer and conference scenarios. Trunk identifiers are numbers that are displayed in the following form: **T5237#2**.

- In some transfer scenarios, Microsoft Office Communicator displays a trunk identifier instead of a calling or called party.
- In some conference scenarios, Microsoft Office Communicator displays a trunk identifier as an extra party on the call.

Contact the Communication Manager administrator

In either type of scenario, the presence of trunk group identifiers might be the result of improperly administered trunk groups in Communication Manager. If Microsoft Office Communicator displays a trunk identifier, contact the Communication Manager administrator.

The Communication Manager administrator should verify that ISDN trunks are properly administered (Trunk Group screen). The settings for "Send Calling Number" and "Send Connected Number" should be set to **y**. Administering ISDN trunks also requires administration of the "Numbering - Public/Unknown Format" screens. For more information, see *Administrator Guide for Avaya Communication Manager*, 03-300509. ISDN is the acronym for Integrated Services Digital Network.

Note:

When "QSIG Value-Added" is enabled for QSIG trunks, the label for "Send Connected Number" changes to "Send Called/Busy/Connected Number."

Chapter 5: Integrating AE Services with Microsoft Lync Server 2010 and 2013

How to use the information in this chapter

This chapter provides the configuration tasks you must perform to integrate AE Services into an existing Microsoft Lync infrastructure. This document is not intended to be a comprehensive configuration guide. This chapter focuses only on the steps required to integrate AE Services with the Microsoft Lync Server.

The Avaya Aura Application Enablement Services Integration for Microsoft Lync Server 2010 and Microsoft Lync Server 2013 is an application that provides click-to-call, and telephony presence. It enables users to operate more efficiently by launching phone calls from the Microsoft Lync client. As a result, people, teams, and organizations are able to communicate simply and effectively while working with Avaya and Microsoft applications. The AE Services Integration for Microsoft Lync is for customers who want a click-to-call solution that takes advantage of their existing Avaya Aura Communication Manager.

Phase 1: Install and Configure Lync Server 2010 and Lync Server 2013

The documentation for installing and configuring Lync Server 2010 and Lync Server 2013 is available online at the Microsoft TechNet Library (technet.microsoft.com). Recommended documents are specified in the following sections:

- Set up and Prepare Active Directory
- Set up, Deploy, and Configure Domain Name System (DNS)
- Install Lync Server

Documentation for Microsoft Lync Server 2010

The following list includes documents that are strongly recommended for integrating AE Services with Microsoft Lync Server 2010. The documents *Deploying Remote Call Control* and *Microsoft Lync Server 2010 (Release Candidate) Lab Deployment Guide* are particularly useful for integrating AE Services in a Microsoft Lync Server environment.

- *Planning for Microsoft Lync Server 2010*
- *Preparing Active Directory Domain Services for Lync Server 2010*
- *Microsoft Lync Server 2010 Active Directory Guide*
- *Deploying Lync Server 2010 Standard Edition*
- *Deploying Lync Server 2010 Enterprise Edition*
- *Deploying Edge Servers*
- *Deploying Remote Call Control*
- *Microsoft Lync Server 2010 (Release Candidate) Lab Deployment Guide*
- *Microsoft Lync Server 2010 Client and Device Deployment Guide*
- *Microsoft Lync Server 2010 Active Directory Guide*
- *Microsoft Lync Server 2010 Capacity Calculator*

You can download these documents from the Microsoft Download Center at the following Web address: <http://www.microsoft.com/downloads>.

Documentation for Microsoft Lync Server 2013

The following list includes documents that are strongly recommended for integrating AE Services with Microsoft Lync Server 2013. The documents *Deploying Remote Call Control* and *Deploying Microsoft Lync Server 2013* are particularly useful for integrating AE Services in a Microsoft Lync Server environment.

The following documentation is available online at technet.microsoft.com under Lync 2013 Server:

- *Planning Primer: Planning for Your Organization for Lync Server 2013*
- *Deploying Lync Server 2013*
- *Preparing Active Directory Domain Services for Lync Server 2013*
- *Setting Up Edge Servers for Lync Server 2013*
- *Deploying Remote Call Control for Lync Server 2013*

- *Deploying Clients and Devices for Lync Server 2013*
- *Using the Lync Server 2013 Capacity Planning Calculator*

Phase 2: Setting up AE Services and Communication Manager

Refer to [Phase 2: Setting up AE Services and Communication Manager](#) on page 41. This information is the same for Lync 2010 and Lync 2013.



Important:

For Communication Manager 6.3 and later, ASAI requires the signaling groups between Communication Manager and Session Manager to use TLS.

Phase 3: Integrating Application Enablement Services with Microsoft Lync Server

You must complete the following steps prior to configuring certificates and other tasks directly related to integrating AE Services with Microsoft Lync Server 2010 and Microsoft Lync Server 2013.

1. Administer a switch connection from AE Services to Communication Manager. (See the *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*.)
2. Check the status of the switch connection (from AE Services to Communication Manager). (See the *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*.)
3. Administer a TSAPI Link. (See the *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*.)
4. Enable the TR/87 Port in the AE Services Management Console. (See [Enabling the TR/87 port](#) on page 113.)
5. Administer the Dial Plan. (See [Dial Plan settings in AE Services](#) on page 133.)

Installing the trusted certificate on Microsoft Lync Server

If you have not already installed certificates on the Microsoft Lync Server 2010 or Microsoft Lync Server 2013 as part of the Microsoft Lync deployment you can use the following procedure to create a custom template that includes the attributes required by AE Services and then specify this template during the Certificate Assignment phase of the Lync Server deployment.

If the Microsoft Lync Server deployment has been previously completed, use this procedure to re-run Step 3 of the Microsoft Lync Deployment Wizard so the Lync Server will have a certificate that includes the Application Policies required by AE Services. Care must be taken to insure the template used and the issuing server satisfies all trust management needs of the Microsoft Lync Environment.

When installing the trusted certificate, note that Microsoft Lync Server and AE Services must use either the same CA or an issuer in the same certificate chain.

Creating a custom Certificate Template

Use this procedure to create a template that can be used when assigning certificates to the Microsoft Lync Server. The template you create will contain the Client and Server Authentication Policies required by AE Services. This procedure assumes the use of a Microsoft 2008 or Microsoft Server 2012 Certificate Authority (CA) Server. If you are using another vendors CA, use this as a general guide and consult the documentation for the CA Server.

Perform the following step:

1. Access the Windows 2008 or Windows Server 2012 CA Server Console, and run the CA MMC snap-in or access **Start > Administrative Tools > Certificate Authority**.
2. Expand the CA Server in the left pane, and then right-click on the **Certificate Templates** folder in the left pane.
3. Select **Manage**.
4. Right-click **RAS and IAS Server**, and select **duplicate template**.

Note:

RAS and IAS template was chosen for this example because it includes Client and Server Authentication Application Policies required by Avaya AE Services. You should select a template that meets the needs of your environment which also satisfies Avaya AE Services requirements.

5. On the General tab in the Properties of New Template dialog box, give the template a unique name like *AES* and then click **Apply** and **OK**.

Installing or re-installing certificates on the Microsoft Lync Server

Step 3 of the Lync Server Deployment Wizard requests installs and assigns certificates required by the Microsoft Lync Server. For integration with AE Services you will need to specify the template you created in the previous step which contains the client and server authentication application policy required by AE Services. During this process the Certificate Wizard allows for specifying the template you created.

Perform the following steps:

1. From the Lync Server system Console, select **Start > All Programs > Microsoft Lync Server > Lync Server Deployment Wizard** to start the Lync Server Deployment Wizard.
2. Click **Install or Update Lync Server System**.
The Lync Server Deployment Wizard launches.
3. For step 3 of the wizard, **Request, Install or Assign Certificates**, click **Run** or **Run Again**.
The Certificate Wizard launches.
4. Click **Request**.
5. On the Certificate Request screen, click **Next**.
6. On the Delayed or Immediate Requests screen, click **Send the request immediately to the certificate authority**, and then click **Next**.
7. On the Choose a certificate Authority (CA) screen, click **Select a CA from the list detected in your environment**.
8. From the dropdown list box, select **CA Server**, and then click **Next**.
9. On the Certificate Authority Account screen, click **Next**.
10. On the Specify Alternate Certificate Template screen, click the **Use alternate certificate template for the selected certification authority** check box.
11. In the text box, enter the name of the template you created earlier, and then click **Next**.
12. On the Name and Security Settings screen, enter a friendly name.
13. From the Bit Length box, select **1024**, and then click **Next**.
14. On the Organization Information screen, enter your organizational information as prompted, and then click **Next**.
15. On the Geographical Information screen, enter your geographical information, and then click **Next**.
16. On the Subject Name / Subject Alternate Names screen, click **Next**.

17. On the SIP Domain setting on Subject Alternate Names (SANs) screen, select the SIP domain(s) that were configured as part of the Lync deployment, and then click **Next**.
18. On the Configured Additional Subject Alternate Names screen, click **Next**.
19. On the Certificate Request Summary screen, click **Next**.
The Executing Commands screen display summary of commands executed.
20. Click **Next**.
21. On the Online Certificate Request Status screen, make sure the **Assign this certificate to Lync Server certificate usages** check box is checked, and click **Finish**.
The Certificate Assignment wizard launches.
22. Click **Next**.
23. On the Certificate Assignment Summary screen, click **Next**.
The summary screen displays the executed commands and "Task status: Completed."
24. Click **Finish**.
The Certificate Assignment Wizard closes. Selecting the dropdown next to **Default certificate** in the Certificate Wizard now shows the certificates and status.
25. Click **Close**.

Installing the trusted certificate on the AE Server

The trusted certificate is also referred to as the "certificate authority (CA) certificate." It is issued by the certificate authority, which can be either Microsoft Certificate Services or another certificate authority.

Microsoft-based procedure for installing a trusted certificate chain

If you use a Microsoft CA hierarchy, perform the following steps from the AE Server to import the trusted certificate chain in PKCS#7 format from Microsoft Certificate Services into the AE Services Management Console:

1. From Internet Explorer, type the URL of your certificate server (for example, ***http://<microsoftcertificate_server.com>/certsrv***)
2. From the Microsoft Certificate Services page, click **Download a CA certificate, certificate chain, or CRL**.

3. On the Download a CA Certificate, Certificate Chain, or CRL page, click **Base 64**, and then click **Download CA certificate**.
4. Save the CA certificate file (the trusted certificate) to a local directory on the Microsoft Lync Server (for example, **C:\temp\certnew.cer**).
5. Contact the Microsoft Lync Server administrator, and confirm that the certificate with the client and server authentication policies is installed and operating on the Microsoft Lync Server. The certificate must be installed and operating on Microsoft Lync Server before you can perform the procedures in the AE Services Management Console.

Importing the trusted certificate into the AE Services Management Console

Perform the following steps to import the trusted certificate into the AE Services Management Console:

1. From the main menu of the AE Services Management Console, select **Security > Certificate Management > CA Trusted Certificates**.
2. On the CA Trusted Certificates page, click **Import**.
3. Complete the Trusted Certificate Import page, as follows:
 - a. In the Certificate Alias field, type an alias for the trusted certificate (for example, **lynccert**). The trusted certificate alias can be arbitrary. It does not need to match any aliases for AE Services.
 - b. Click **Browse** to locate the trusted certificate file you want to import, and then click **Apply**.

If the import is successful, AE Services displays the following message: "Certificate imported successfully."

Verifying the installation of the trusted certificate in AE Services

Perform the following steps to verify the installation of the entire certificate chain (all the way back to the root certificate) in AE Services:

1. In the AE Services Management Console, select **Security > Certificate Management > CA Trusted Certificates**.

2. From the CA Trusted Certificates page, select the alias of the trusted certificate (**lynccert**, based on this sample scenario), and click **View**.
3. From the Trusted Certificate Details page, verify that the information for the trusted certificate is correct.
 - a. Verify that the entire chain of certificates exists, all the way back to a self-signed certificate.
 - b. Verify that the Issued To and Issued By fields display the name of the organization that the trusted certificate is issued to.
 - c. Verify that the Expiration Date Indicates the date that the trusted certificate expires.
 - d. Verify the information in the Details display. Make sure the Certificate Status is valid.
4. Click **Close** to exit the Trusted Certificate Details page.

Administering AE Services access to Active Directory

Perform the following steps to set up the connection to Active Directory for AE Services:

1. From a browser, log in to the AE Services Management Console.
2. In the AE Services Management Console, select **Security > Enterprise Directory**.
3. Complete the Enterprise Directory page, as follows:
 - User DN for Query Authentication - Type the DN for the user object that AE Services uses for accessing the Active directory. Based on how users are set up in Active Directory, the user object could correspond to a Full Name, a Display Name, or a User logon name.
 - Password - Type a password to be used for Active Directory access. Retype the same password in the Confirm Password field. This Active Directory password is stored in an encrypted format on the AE Server.
 - Base Search DN -The Base Search DN is less specific than the User DN. Type the DN of the node that includes all user accounts that need access to the AE Services and Live Communications Server integration in the following format:
cn=users,dc=example,dc=com
 - HostName/IP Address - Type the IP address or Host Name of the Domain Controller that runs Active Directory.
 - Port - (used for Active Directory access) - Change the default port number to an appropriate value for your configuration. The default is 389 (the port assignment for LDAP).
 - Secondary Host Name / IP Address - Accept the default (leave the field blank). This field does not apply to the AE Services implementation for Microsoft Lync Server.

- Secondary Port - Accept the default (leave the field blank). This field does not apply to the AE Services implementation for Microsoft Lync Server.
- User ID Attribute Name - This setting defaults to uid, which is the default for AE Services User Management. For Microsoft Active Directory, you must change this setting. The default setting for Microsoft Active Directory is samaccountname. If your implementation does not use the default for Microsoft Active Directory, enter the name of the attribute that is appropriate for your implementation.
- User Role Attribute Name - Enter the name of the attribute for the user role that your Enterprise Directory Server uses or leave blank if appropriate.
- Change Password URL - Accept the default (leave the field blank). This field does not apply to the AE Services implementation for Microsoft Lync Server.
- LDAP-S - Select LDAP-S if your configuration uses a TLS connection from AE Services to your Enterprise Directory Server.

For example:

- | | |
|-------------------------------------|---|
| ● User DN for Query Authentication: | cn=Administrator,cn=Users,dc=lync2010,dc=local |
| ● Password: | ***** |
| ● Confirm Password: | ***** |
| ● Base Search DN: | cn=Users,dc=lync2010,dc=local |
| ● HostName/IP Address: | 135.9.107.90 |
| ● Port: | 389 |
| ● Secondary Host Name/IP Address: | - |
| ● User ID Attribute Name: | samaccountname |
| ● User Role Attribute Name: | - |
| ● Change Password URL: | - |
| ● Device ID Attribute: | msRTCSIP-Line |
| ● Search Filter Attribute Name: | msRTCSIP-PrimaryUserAddress |
| ● LDAPS | Select if used |

4. Click **Apply Changes** to put your changes into effect.

For more information, see [Making changes on the Enterprise Directory Configuration page](#) on page 93.

Configuring Remote Call Control (RCC)

The Lync Server Management Shell is used to add an RCC gateway. It is recommended that RCC configuration be performed by or in coordination with the Lync Server System Administrator.

In the following example, RCC is set up using the Microsoft Lync Management Shell for Lync Server 2010. The same steps apply to setting up RCC for Lync Server 2013.

In step 5, `avaessrv` is a unique name chosen for the new application ID. It does not map to any previous configuration.

Example:

1. Select **Start > All Programs > Microsoft Lync Server > Lync Server Management Shell** to start the Lync Server Management Shell using the appropriate credentials. From the command prompt, enter the command specified at each step.

2. Run the following commands to capture any pre-existing configuration data if any for reference and copy to Notepad:

```
PS C:\Users> Get-CsStaticRoutingConfiguration (should return null results unless a static route has previously been configured)
```

```
Identity : Global
```

```
Route    : {}
```

```
PS C:\Users> Get-CsSipDomain (To view configured SIP domain(s). This will not be modified during RCC configuration in this example.)
```

```
PS C:\Users> Get-CsTrustedApplicationPool (Retrieves settings for one or more pools that contain the computers that host trusted applications).
```

```
PS C:\Users> Get-CsSite (Retrieves site related configuration information.)
```

For help with the Lync Server management Shell:

```
PS C:\Users> Get-Help
```

3. To create a static route, first set the variable `$TLSRoute`:
 - a. PS C:\Users> **\$TLSRoute = New-CsStaticRoute-TLSRoute -Destination `avaessrv.aes.lync2010.local` -Port 4723 -UseDefaultCertificate \$true -MatchUri `aes.lync2010.local`**

Note:

In step 3a, `avaessrv.aes.lync2010.local` is the Fully Qualified Domain Name (FQDN) for the AE Services server; `aes.lync2010.local` is a sub-domain of your SIP domain.

- b. PS C:\Users> **Set-CsStaticRoutingConfiguration -Route @{Add=\$TLSRoute}**

4. Create a new trusted application entry. Type the following at the command prompt:

```
PS C:\Users> New-CsTrustedApplicationPool -Identity avaessrv.aes.lync2010.local  
-Registrar lyncss.lync2010.local -Site 1 -TreatAsAuthenticated $true  
-ThrottleAsServer $true -RequiresReplication $false
```

Note:

In step 4, **lyncss.lync2010.local** is the FQDN of the Microsoft Lync Standard Server; **1** is a SiteID that was configured during Lync Server Deployment. See output of **Get-CsSite** for the SiteID field value.

5. Add the trusted application to the pool. Type the following at the command prompt:

```
PS C:\Users> New-CsTrustedApplication -ApplicationID avaessrv  
-TrustedApplicationPoolFqdn avaessrv.aes.lync2010.local -Port 4723
```

6. Use `Get-CsStaticRoutingConfiguration` and `Get-CsTrustedApplicationPool` to view the changes:

```
PS C:\Users> Get-CsStaticRoutingConfiguration
```

Identity : Global

Route : {MatchUri=*aes.lync2010.local;MatchOnlyPhoneUri=False;Enabled=True;
ReplaceHostInRequestUri=False}

```
PS C:\Users> Get-CsTrustedApplicationPool
```

Identity : TrustedApplicationPool:avaessrv.aes.lync2010.local

Registrar : Registrar:lyncss.lync2010.local

FileStore :

ThrottleAsServer : True

TreatAsAuthenticated : True

OutboundOnly : False

RequiresReplication : False

AudioPortStart :

AudioPortCount : 0

AppSharingPortStart :

AppSharingPortCount : 0

VideoPortStart :

VideoPortCount : 0

Applications : {urn:application:avaessrv}

DependentServiceList : {}

ServiceId : 1-ExternalServer-1

SiteId : Site:westy

PoolFqdn : avaessrv.aes.lync2010.local

Version : 5

Role : TrustedApplicationPool

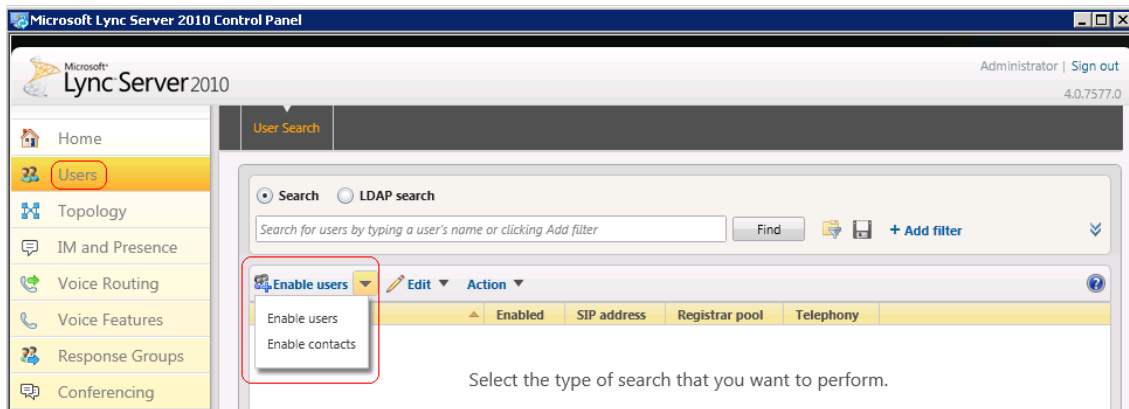
7. To implement the published changes you have made to the topology, type the command:

```
PS C:\Users> Enable-CsTopology
```

Enable users for RCC

AD users must be enabled in the Lync Server Control Panel before using the Microsoft Lync Client.

1. Select **Start > All Programs > Microsoft Lync Server > Lync Server Control Panel** to access the Lync Server Console using the appropriate credentials.
2. To enable users, click **Users** in the left pane.
3. In the right pane, select **Enable Users** from the dropdown list box.



4. In the Enable users dialog box, click **Add**.

There are different types of Active Directory searches you can perform to find various groups of users. To enable an AD user, enter the AD user's name and click **Find**. Select the user from the list, and then click **OK**.

The New Lync Server User screen appears.

5. From the Assign users to a pool dropdown box, select the pool which is typically the FQDN of the Lync Server.
6. In the Generate a User's SIP URI area, select an appropriate option.
7. From the Telephony box, select **Remote call control** or **Remote call control only**. **Remote call control only** will not allow users to place calls using their computer.
8. In Line URI text box, specify a line URI in the format: tel:+13033731018. Lync also supports dial plan conversion to extensions on the user form using the format: tel:+13033731018;ext=731018. However, this prevents name resolution in the call window received at the called party when the client places a call. Using the E.164 number format without the extension and doing any necessary dial plan conversion in AE Services is recommended.

9. In the Line Server URI box, assign the line server URI. The format for this is sip:aes@avaessrv.aes.lync2010.local where avaessrv.aes.lync2010.local is the FQDN of the Avaya AE Services Server.

Recommendations for Active Directory and Lync User related Administration

You can configure name resolution independently from the Active Directory user administration, but the simplest way to accomplish this is to start by setting up the AD User record > General Tab > Telephone Number field with the e.164 phone number: "+13033731018". Access Active Directory Users and Groups on the appropriate Domain Controller or system running Remote Server Administration Tools (RSAT).

From the console, select **Start > Administrative Tools > Active Directory Users and Computers**. Expand the appropriate domain in the left pane, and then select the **Users** folder. You can right click on the Users folder and select **New > User** to create a new AD user account or, after selecting the user folder, select a user to modify in the right pane.

By populating the E.164 number in the Telephone number box on the General tab in the Properties dialog box, the default behavior for RCC calls originated from this client will be to resolve the Active Directory name and display as follows in the call window that appears at the called client:

"John Smith"

"Work +1 (303) 373-1018 X731018 is calling you"

In cases where it is not easy to configure AD users with a +E.164 format phone number on the AD User record General tab, you can implement translations rules on the Microsoft Lync Server to normalize non +E.164 formatted numbers to +E.164 format. The Lync Client will not display the number for any contact that does not normalize to +E.164 format. Name resolution will fail for calls placed from any client whose number fails to normalize to +E.164 format. Setting up translation rules will also normalize numbers entered in the Lync Client search box, allowing the user to complete calls that might otherwise not complete.

To implement E.164 Normalization, perform the following steps:

1. Create a file called Company_Phone_Number_Normalization_Rules.txt and save it on the Microsoft Lync Server 2010 in the root directory of <Share Name>\1-WebServices-1\ABfiles\ . On Lync Server 2013, save in the directory of <Install directory for Microsoft Lync Server 2013>\Web Components\Address Book Files\Files.

2. Enter values to handle conversions in the following format:

##

Normalize AD Phone Number Patterns From AD to +E.164

##

(\d{10})

+1\$1

– Matches string 303-555-1212 and converts this to +1-303-555-1212

(\d{7})

+1303\$1

– Matches the string 555-1212 and converts this to +1-303-555-1212

Note:

The default behavior of Lync is to ignore and remove the characters "(", ")" and "-" automatically so these characters do not pose a concern when entered in AD and other fields a user may populate.

You will need to create a conversion entry for every string you wish to handle in this file.

To insure clients use the translation rules, avoid using the following client setting in the Lync Server client policy configuration:

"AddressBookAvailability:WebSearchOnly"

The recommended settings are:

"AddressBookAvailability::FileDownloadOnly"

"AddressBookAvailability::WebSearchAndFileDownload" (this is the default setting)

To view the current configuration for this setting, run this command from the Lync Server Management Shell:

PS C:\Users> get-CsClientPolicy

Identity : Global

PolicyEntry : {}

Description :

AddressBookAvailability : **WebSearchAndFileDownload** (default)

AttendantSafeTransfer :

AutoDiscoveryRetryInterval :

BlockConversationFromFederatedContacts :

Using the TR/87 Test Features

Follow these steps to use TR/87 test features in the AE Services Management Console.

1. From the browser on your AE Services administrative workstation, log into the AE Services Management Console.
2. From the main menu of the AE Services Management Console, select **Utilities > Diagnostics > AE Services > TR/87 Test**.
3. From the TR/87 Self Test page, select from the following tests:
 - **TR/87 Transport** - use **TR/87 Transport** to verify that the installed certificate can be used to establish a SIP session on the loopback interface. This does not verify the far-end server certificate.
 - **TR/87 Transport Service** - use **TR/87 Service** to verify the following:
 - the caller is administered in Active Directory
 - the dial plan is administered for the caller's number
 - the user's telephone device can be monitored
 - **TR/87 Makecall** - use **TR/87 Makecall** to verify that phone control is active for the user.

Note:

The TR/87 Makecall test depends on receiving confirmation of a call being established. In certain scenarios involving trunks, this may be unavailable. The TR/87 Makecall test should be considered a valid test only when using two stations of the same switch to perform the test.

The Host AA settings and TR/87 Test

The Host AA settings in the AE Services Management Console have an effect on the TR/87 Test utility. If you enable host authorization, the authorized hosts list must include the Peer Certificate CN (which is the Server Certificate Subject Name). Because the TR/87 Test utility depends on the Host AA settings and uses the same certificate that is used by Tomcat, you must restart the Web Server after adding a server certificate.

Administering Lync Server for the Agent Login ID

Perform the following steps before signing in Lync as an agent.

1. Log into Lync 2010 or 2013 Server and open the Lync Server 2010 or 2013 Control Panel.
2. Select **Users** and search or display the users you wish to administer.
3. Enter the Tel URI parameter using the following format:

tel:agent/D;phone-context=agent-login-id.domain

where:

- **agent/ID** is the agent's login ID (for example, 1234).
- **domain** is the domain name (for example, example.com)

An example Tel URI parameter is:

tel:1234;phone-context=agent-login-id.example.com

where:

- **1234** is the agent's login ID.
 - **example.com** is the domain name.
4. Have the agent log into the Telephone/Softphone/Agent software that is to be used.
 5. Have the agent sign into Lync and verify that the agent can answer and make calls successfully.



Important:

Always sign out of Lync before logging off the physical device to ensure that the Lync sign-in and the agent login states are always synchronized.

Re-synchronizing States

If the agent logs off the physical device first, Lync will be re-synchronized only after the next call is received or attempted.

Recovering from a system outage

When AE Services returns to an operational state after an outage, you will be able to use Lync to place and control new calls. If you experience an outage, keep in mind the following information:

- If you were on a call when an AE Services outage occurred, complete the call and manually hang up the phone so that your phone and Lync are synchronized. When you are ready to start a new call in Lync, your phone and Lync will be synchronized.
- If Lync signs you out as a result of a network outage, you must sign into Lync again before you can control new calls. If you attempt to sign in during an AE Services outage, Lync displays the warning icon along with the pop-up indicating that Lync cannot make phone calls.

Other AE Services Administration

Configure the following settings in AE Services:

- Enterprise directory configuration settings with bridged appearance alert blocking. See [Configuring Enterprise Directory Settings with Bridged Appearance Alert Blocking](#) on page 186.
- Auto Hold settings. See [Administering Auto Hold configuration](#) on page 187.

Configuring Enterprise Directory Settings with Bridged Appearance Alert Blocking

The enterprise directory is used in conjunction with the bridged appearance alert blocking feature. This feature applies to DMCC applications as well as the AE Services integrations with Microsoft Office LCS, OCS, Lync Server 2010, and Lync Server 2013. DMCC applications that have requested the desktop call control filtering mode can take advantage of the bridged appearance alert blocking feature. For more information about setting up a DMCC application to use the call filtering mode, see the following documents:

- *Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer's Guide*, 02-300359
- *Avaya Aura® Application Enablement Services Device, Media, and Call Control XML Programmer's Guide*, 02-300358

Administering Auto Hold configuration

Use this procedure to enable/disable the Auto Hold feature for Microsoft Office Communicator clients and Microsoft Lync clients. When the Auto Hold feature is enabled, a Microsoft Office Communicator client or Microsoft Lync client that is on an active call will receive a notification (a "toaster pop-up") of a new incoming call arrives. When the Auto Hold feature is disabled, a Microsoft Office Communicator client or Microsoft Lync client that is on an active call will be not notified if a new incoming call arrives.

Perform the following steps:

1. Log into the AE Services Management Console.
2. From the AE Services Management Console main menu, select **AE Services > DMCC > Auto Hold Configuration**.
3. Perform one of the following steps:
 - If you want to enable the Auto Hold feature, make sure the **Auto Hold** check box is checked.
 - If you want to disable the Auto Hold feature, make sure the **Auto Hold** check box is unchecked.
4. Perform one of the following steps:
 - If you want AE Services to refuse holdCall requests from Microsoft Lync and Microsoft Office Communicator clients, make sure the **Prevent Lync and Office Communicator clients from holding calls** check box is checked. When this feature is enabled, users can only place calls on hold via the device.
 - If you want AE Services to accept holdCall requests from Microsoft Lync and Microsoft Office Communicator clients, make sure the **Prevent Lync and Office Communicator clients from holding calls** check box is unchecked.
5. Click **Apply Changes**.
6. On the Apply Changes to Auto Hold Configuration page, click **Apply** to confirm your action.

Known Issues - Lync 2013 Client

There are known issues with Lync 2013 client during following actions:

- transferring call
- redirecting a call

The cumulative update(CU) 2880474 package for Lync 2013

The Conference and Transfer issues are resolved. For more information, see KB 2941643. However, redirecting a call remains an issue after this CU is applied.

Transferring a Call - Lync 2013 Client

When a Lync 2013 client is transferred to another party, the Lync 2013 client being transferred (the transferred party) will have two conversation windows displayed after the transfer is completed. The transferred party will be unable to end the call using the Lync 2013 user interface. The call must be ended from the device.

There are also issues when a Lync 2013 client is transferred to an "existing conversation" and the Lync 2013 transferred party is unable to end the call from the user interface.

Conferencing a call

When a Lync 2013 client is a participant in a conference call, an orphan conversation window (the call before the conference was established) will remain open after the call ends. The conversation window must be manually closed. Note that when an orphan conversation window remains displayed after a call ends, new calls that are answered by the Lync 2013 client will automatically be placed on hold until the orphan window is closed.

Redirecting a Call from the Lync 2013 Client

The Lync clients allow the user to administer mobile, home, and "other" phone numbers. When a Lync 2013 client receives a call, the user may redirect the call to one of the administered numbers (in the Options drop-down box in the alerting window). When a call is redirected to a destination that is a Lync client, the Lync client to which the call was redirected will be unable to answer the call from the user interface. The call must be answered from the device.

Known Issues - Other

This section addresses the following feature-related issues:

- setting up forwarding off switch
- using Call Forwarding and Send All Calls

- putting the active call on hold before starting a new call
- Clear Connection request on a held connection is not supported
- bridging irregularities
- Missed Call email
- usage instructions for analog phones

This section also addresses the general issue that under certain conditions a party's telephone number will be unavailable to Lync. In this situation, Lync cannot display a telephone number or party identifier. For more information, see:

- unidentified caller in Microsoft Office Communicator window
- Communicator displays numbers with trunk notation.

Setting up Forwarding Off-Switch

If you experience problems setting up forwarding off-switch (for example, to your home or cell phone), contact the Avaya Communication Manager administrator. There are certain settings in Communication Manager that could prevent your ability to set up forwarding off-switch

Using Call Forwarding and Send All Calls

From the Lync client, you can use Call Forwarding as follows:

- You can set your telephone to forward calls.
- You can set Lync to forward calls relative to the client you are signed into.



Important:

You should not press the Forwarding button on a physical telephone set. Pressing these buttons can cause Lync to lose synchronization with the telephone.

Clear Connection request on a held connection is not supported

Avaya Communication Manager does not support a Clear Connection request on a held connection. If you are a Lync user and you have a held call and try to end the call, you will receive an error message, and the call will remain in the held state.

Bridging irregularities

In an AE Services and Lync Server environment, the Lync client may not behave as expected if you use bridged call appearances. Here are some examples of irregularities associated with bridged calls:

- If a user answers on a bridged extension, Lync continues to alert on the primary extension and eventually times out. This bridging irregularity occurs when you administer EC500 telephones with XMOBILE. If you administer EC500 telephones with OPTIM (Off-PBX Telephone Integration and Mobility), the bridging irregularities do not occur. For more information, see "Considerations for Extension to Cellular" in *Feature Description and Implementation for Avaya Communication Manager*, 555-245-205.
- If you call someone who has a bridged extension, the Lync conversation window may display either of the following:
 - an additional party on the call representing that bridged extension
 - "Unidentified Caller"

Unidentified Caller in Lync window

For the following reasons, you may see "Unidentified Caller" in the Lync conversation window:

- The user you have called has a bridged extension.
- Your call went to a voice mail system. If your call is answered by a voice mail system, the voice mail system appears as an "Unidentified Caller."
- Your call went to Music-On-Hold by way of a Voice Announcement with LAN (VAL) board on Communication Manager, causing you to lose telephone control on your Lync. You can resolve this issue by upgrading Communication Manager with Service Pack 12866.
- You manually entered a number in the FIND box that was not in the proper format. If you are manually typing the number in the FIND box, be sure to enter the full telephone number, including the country code and either the area code or the region code, whichever is appropriate. Depending on how the system has been administered, it may be acceptable to not include the country code in the entered number. In all cases, you should not include the Automatic Route Selection (ARS) code for the outside line (for example, 9).

Communicator displays numbers with trunk notation

Lync displays telephone numbers as trunk identifiers instead of telephone numbers in transfer scenarios. Trunk identifiers are numbers that are displayed in the following form: **T5237#2**. In some transfer scenarios, Lync displays a trunk identifier instead of a calling or called party.

In either type of scenario, the presence of trunk group identifiers might be the result of improperly administered trunk groups in Communication Manager. If Lync displays a trunk identifier, contact the Communication Manager administrator.

The Communication Manager administrator should verify that the ISDN trunks are properly administered (the Trunk Group screen). The settings for "Send Calling Number" and "Send Connected Number" should be set to **y**. Administering ISDN trunks also requires administration of the "Numbering - Public/Unknown Format" screens. For more information, see *Administrator Guide for Avaya Communication Manager*, 03-300509.

Note:

When "QSIG Value-Added" is enabled for QSIG trunks, the label for "Send Connected Number" changes to "Send Called/Busy/Connected Number."

Appendix A: SIP requests and associated errors

SIP INVITE request (start application session)	
Code	Description
200	OK
401	Unauthorized: Session could not be established - invalid AD search parameters
404	Not found: Session could not be established - no AD record for this user
408	Request timeout: Session could not be established - AD request timed out
480	Temporarily unavailable: Session could not be established - unable to connect to AD Server
486	Busy Here: AE Services is temporarily overloaded.
500	Internal server error: Session could not be established.

Appendix B: AE Services Implementation for Microsoft LCS call flow

This appendix provides a basic message flow description and two illustrations that show the interaction between Microsoft components and Avaya components in an Application Enablement Services (AE Services) Implementation for Microsoft Live Communications Server (LCS).

Message flow

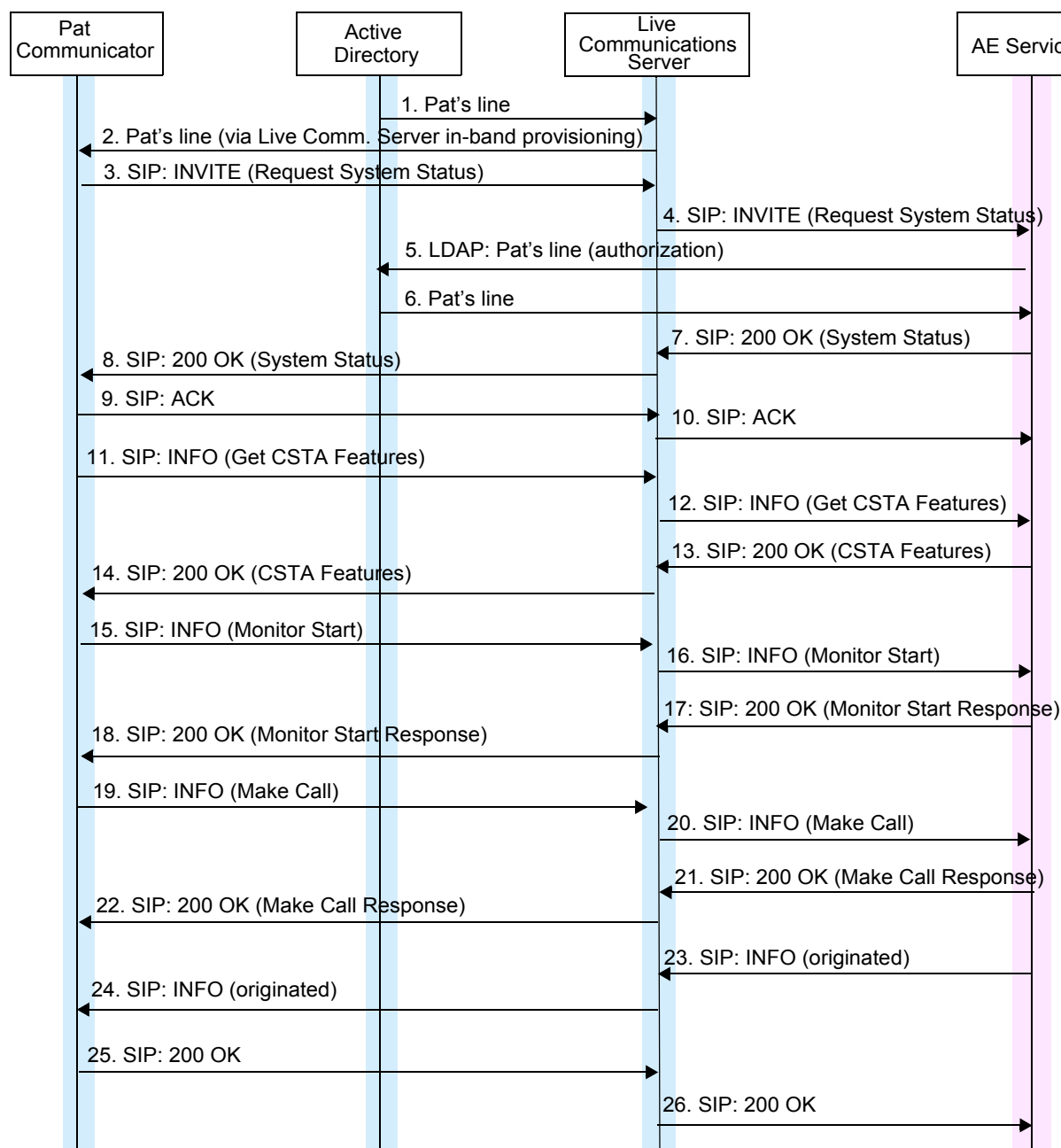
The message flow diagram in [Figure 7](#) shows the flow of messages from application startup (Microsoft Office Communicator) to a successful MakeCall operation and associated Originated event (AE Services and Communication Manager).

- Steps 1 and 2 show some initial provisioning between the application, Microsoft Active Directory Services, and Live Communications Server.
- Steps 3 through 10 show the establishment of the SIP dialog.
 - The Communicator client sends a SIP INVITE containing a Request System Status message.
 - When Live Communications Server receives this message, it opens a TLS connection to AE Services. AE Services will be provisioned with the certificate of the Live Communications Server server so that Live Communications Server will be a trusted server on the TR/87 port.
 - After the TLS connection has been established, Live Communications Server forwards the INVITE message on to AE Services. At this point, the AE Services Device, Media, and Call Control service will extract the user identity from the SIP message and query Microsoft Active Directory Services to find the extension(s) that the given user can control. This will be used for authorization of all subsequent requests.
 - It will then send a SIP OK message with a System Status message indicating everything is operational.
- Steps 11 through 14 show the Communicator client requesting the set of supported CSTA features. This is because not all telephony systems support all of the services that Communicator uses.
- Steps 15 through 18 show the Communicator client establishing a monitor for Pat's station.

Appendix B: AE Services Implementation for Microsoft LCS call flow

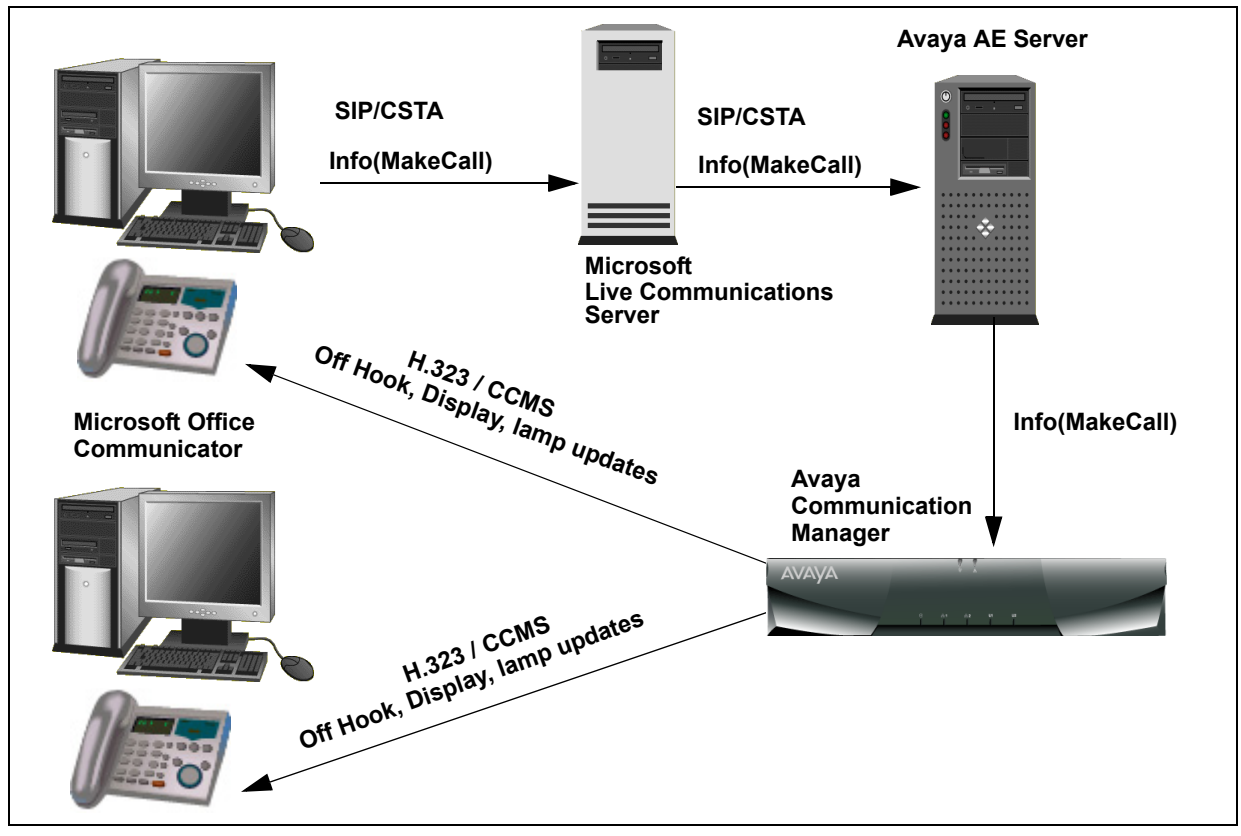
- Steps 19 through 22 show a Make Call request from Communicator being sent through to AE Services. For more details on what happens when this request is received, refer to [Figure 7](#).
- Steps 23 through 26 show an Originated event coming from AE Services and being delivered to the Communicator client. This would have started with a CSTA 1 event from TSAPI to Call Control Services. CCS would then map this to the appropriate Call Control Listener, convert the event to CSTA 3, and invoke the proper method on the listener. This would result in the event being sent to the SIP UA and out to the Live Communications Server and eventually to the Communicator Client.

Figure 7: Call flow scenario -- MakeCall and an associated Originated Event



[Figure 8](#) illustrates the Message flow for the Make Call operation in terms of a basic connectivity diagram. Other requests would follow a similar pattern.

Figure 8: AE Services Implementation for Microsoft LCS Call flow



Appendix C: Capacities

Communication Manager Domain Control Capacity Increase

The number of supported domain controls on Communication Manager 4.0 is 32,000. This increase applies only to the S87-series servers and the S8500 server. If Communication Manager is used for call center or other call control functionality, care must be taken to not exceed the total number of domain controls.

AE Services Associations

The number of supported generic associations on the AE Services Server (AE Server) is 32,768.

Busy Hour Call Completion (BHCC)

For the AE Services implementation for Live Communications Server and Lync Server, the BHCC rate, in terms of Live Communications Server traffic, is 36,000 calls per hour. This rate is based on counting a Make Call request and an Answer Call request as separate calls on the AE Server. One Microsoft Office Communicator/Lync client user calling another Microsoft Office Communicator/Lync client user would therefore count as two calls in the BHCC measurements.

Maximum Users

The AE Services server supports a maximum of 20,000 concurrent users. If you plan to support more than 20,000 concurrent Microsoft Office Communicator/Lync clients you must use more than one AE Services server. For more information, see [Figure 4: Configuring AE Services with 20,000 or more concurrent users](#) on page 33.

Throughput

The AE Server supports six TR/87 (CSTA 3) messages per second, per 1000 users.

License Consumption

One Unified CC API-Desktop Edition license, also known as Unified Desktop license, is consumed for each Microsoft Office Communicator client, for the duration of the period that it has an active dialog with Application Enablement Services via the LCS or OCS

Appendix D: Creating a certificate template for Server Certificates on the Microsoft CA Server

Note:

If you are using a Microsoft Windows Server 2003 Enterprise Edition Certificate Authority, you can use the procedure in this appendix to create a server certificate template that supports both client authentication and server authentication.

The server certificates exchanged between AE Services and Microsoft configurations (either Live Communications Server 2005 or Microsoft Office Communications Server 2007) must support both client authentication and server authentication.

Note:

This appendix applies to exclusively configurations that use a Certification Authority on Microsoft Windows Server 2003 R2 Enterprise Edition Service Pack 2. That is, it is not applicable to the procedures for administering certificates in Chapter 2 or Chapter 3 of this document.



Important:

If OCS Enterprise edition is in use with an OCS server pool, the certificate should be issued in the name of the pool and must have both Server Authentication and Client Authentication. If a load balancer handles the pool, then the pool name should resolve to the load balancer's IP address. For example, if the OCS pool is called **ocspool.company.com**, and that is the pool that agents and OCS servers use, the DNS resolution of **ocspool.company.com** should be the IP address of the load balancer. Furthermore, the TLS certificate should be issued to **ocspool.company.com** from the correct authority with the correct company name, etc. Then, this certificate should be put on each of the OCS servers so that they pass this **ocspool.company.com** certificate when creating a secure socket to Application Enablement Services.

Creating a certificate template for Server Certificates on the Microsoft CA Server

Use the following procedure to create a server certificate template, for the Microsoft CA Server, that provides client authentication and server authentication. After you create the CA certificate template, each server certificate you request will provide client authentication and server authentication.

1. On the Microsoft Enterprise CA server, start the **Certification Authority** Microsoft Management Console (MMC) snap-in.
2. In the left pane of the Certification Authority MMC snap-in, expand the Certification Authority node, right-click on **Certificate Templates**, and select **Manage** to start the Certificate Templates MMC snap-in.
3. In the right pane of the Certificate Templates MMC snap-in, right-click on the Web Server template, and select **Duplicate Template**.
4. In the Properties of New Template dialog box, select the **General** tab, and complete the following fields:
 - Template display name -- to complete this field enter a descriptive name for the template display; for example: **Web Server Cert with Client and Server Authentication**.
 - Template name -- to complete this field enter a descriptive name for the template; for example: **WebServerCertClientServerAuthen**
5. In the Properties of New Template dialog box, select the **Request Handling** tab. Verify that Purpose is set to **Signature and encryption**, and then click **CSPs....**
6. In the CSP Selection dialog box, select the option button for **Requests must use one of the following CSPs:**. In the CSPs: list, select the checkbox for **Microsoft Enhanced Cryptographic Provider v1.0**, and click **OK**.
7. In the Properties of New Template dialog box select the **Subject Name** tab and verify that **Supply in the request** is selected.
8. In the Properties of New Template dialog box, select the **Extensions** tab. In the Extensions included in this template section, select **Application Policies** and click **Edit**.
9. In the Edit Application Policies Extension dialog box, click **Add**.
10. In the Add Application Policy dialog box, select **Client Authentication** and click **OK**.
11. In the Edit Application Policies Extension dialog box check the Application policies list, and verify that both Server Authentication and Client Authentication are included. Click on **OK**.
12. In the Properties of New Template dialog box, click **OK**.

13. In the Certification Authority MMC snap-in, expand the Certification Authority node.
Right-click on **Certificate Templates**, and select **New > Certificate Template to Issue**.

In the Enable Certificate Templates dialog box, select the Certificate Template created in Steps 3 -12 (based on the example, select **WebServerCertClientServerAuthen**) and click **OK**.

Appendix E: Instructions for generating version 3 certificates

Microsoft Windows 2008 Enterprise CA Server does not support web enrollment for version 3 certificate templates. If you would like to use version 3 templates with your AES server use the following recommended instructions to generate your certificate.

For version2 certificate templates use the web enrollment procedure.

Creating Version 3 (Windows Server 2008) Certificate Templates for Server Certificates

The server certificates exchanged between Avaya Application Enablement Services (AES) and Microsoft Office Communications Server (OCS) must support both Server Authentication and Client Authentication key usage.

This section describes the steps for creating a certificate template on the Windows Server 2008 Enterprise Certification Authority (CA). The certificate template is used to create server certificates for both AES and OCS.

Note:

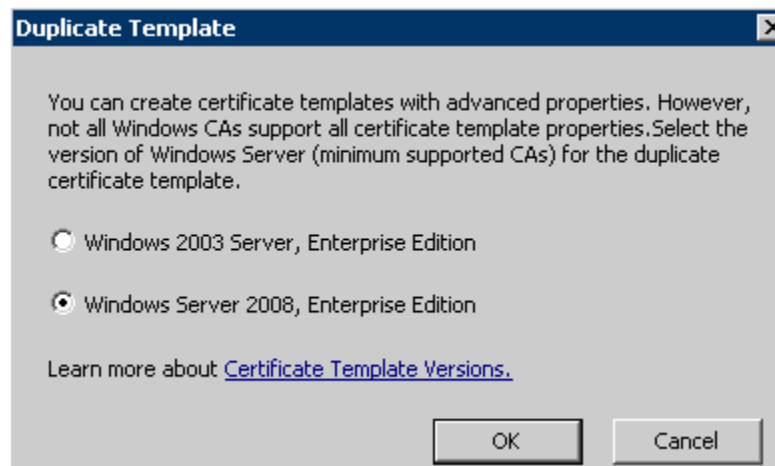
If OCS Enterprise edition is in use with an OCS server pool, the certificate should be issued in the name of the pool and must have both Server Authentication and Client Authentication. If a load balancer handles the pool, then the pool name should resolve to the load balancer's IP address. For example, if the OCS pool is called **ocspool.company.com**, and that is the pool that agents and OCS servers use, the DNS resolution of **ocspool.company.com** should be the IP address of the load balancer. Furthermore, the TLS certificate should be issued to **ocspool.company.com** from the correct authority with the correct company name, etc. Then, this certificate should be put on each of the OCS servers so that they pass this **ocspool.company.com** certificate when creating a secure socket to Application Enablement Services. See [Figure 9: Certificates in a load-balancing scenario](#).

Appendix E: Instructions for generating version 3 certificates

Follow this procedure to create a certificate template on the Windows Server 2008 Enterprise Certification Authority (CA).

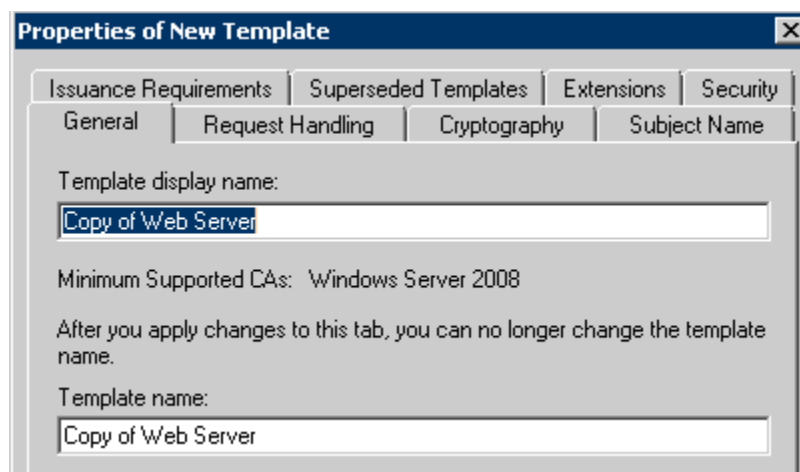
1. On the windows 2008 Enterprise CA server, start the **Certification Authority** Microsoft Management Console (MMC) snap-in.
2. In the left pane of the Certification Authority MMC snap-in, expand the **Certification Authority** node, right-click on **Certificate Templates**, and select **Manage** to launch the Certificate Templates MMC snap-in.
3. In the right pane of the Certificate Templates MMC snap-in, right-click on the Web Server template, and select **Duplicate Template**.

The system displays the Duplicate Template dialog box.

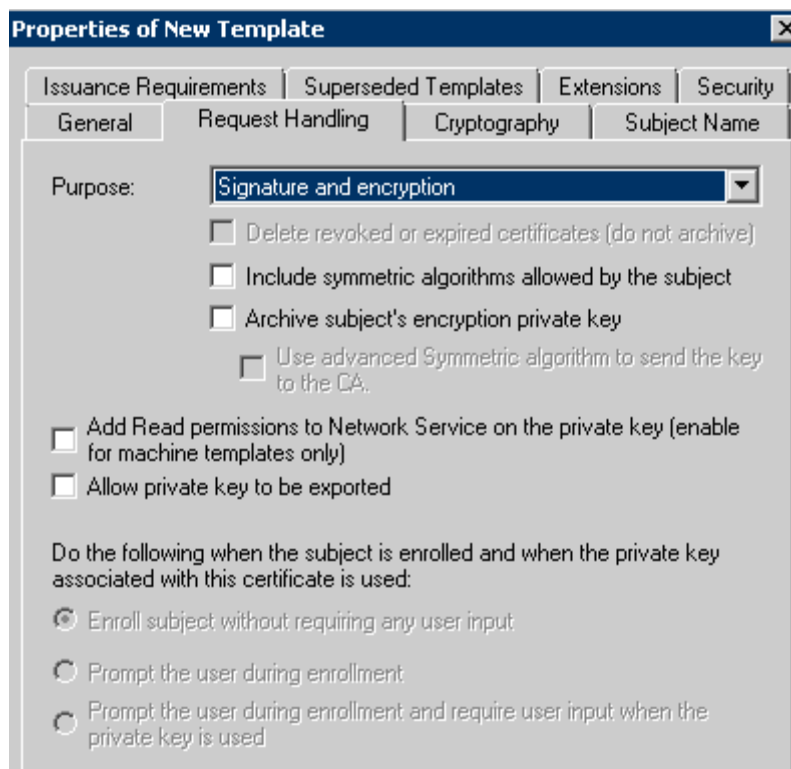


4. In the Duplicate Template dialog box, select **Windows Server 2008, Enterprise Edition**.

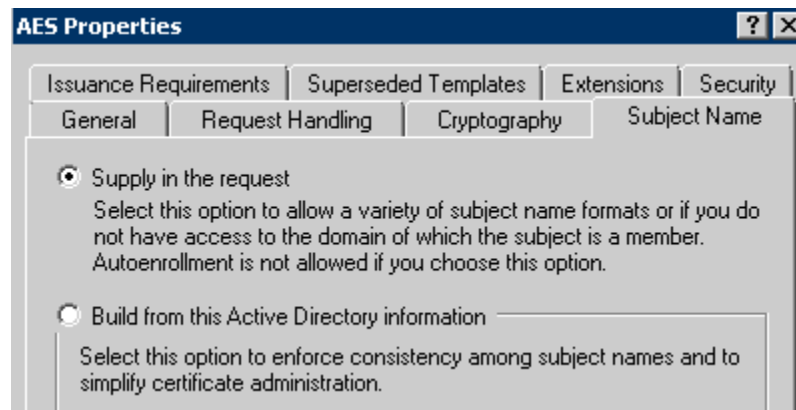
The system displays the Properties of New Template window.



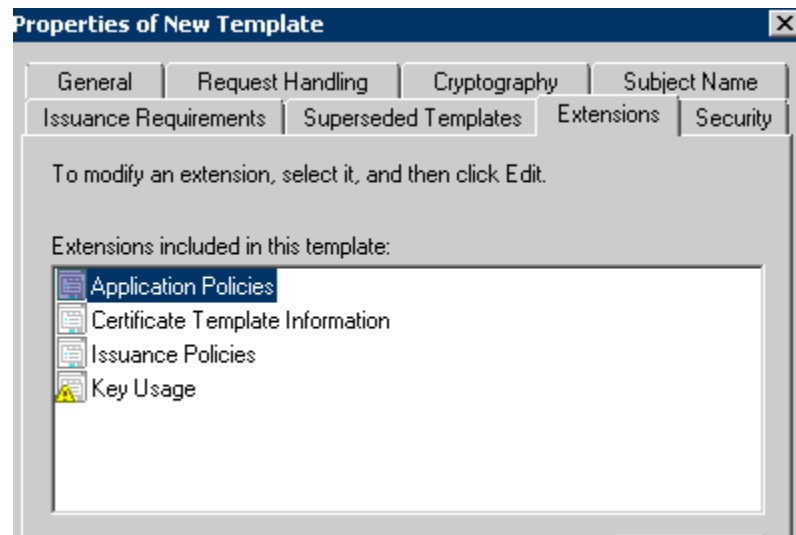
5. From the **General** tab of the Properties of New Template dialog box, in the **Template display name** field, type a descriptive name for the template.
6. In the **Properties of New Template** dialog box, select the **Request Handling** tab, and ensure that the **Purpose** selection is set to **Signature and encryption**.



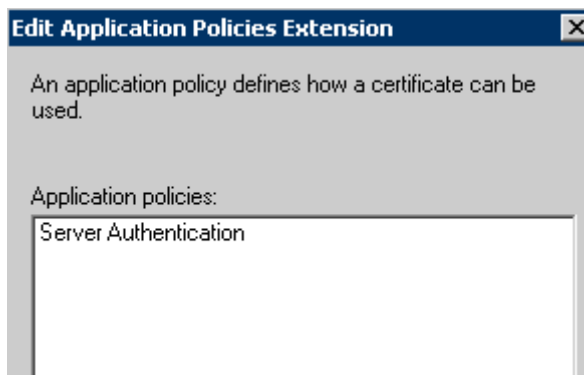
7. In the **AES Properties** dialog box, select the **Subject Name** tab, and ensure that the **Supply in the request** option is selected.



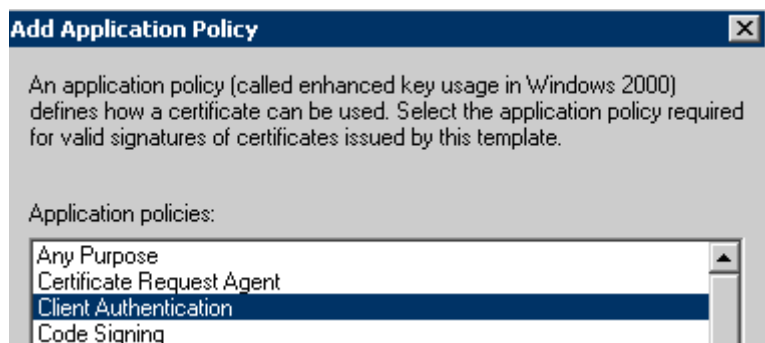
8. In the **Properties of New Template** dialog box, select the **Extensions** tab. In the **Extensions included in this template** section, select **Application Policies** and click **Edit**.



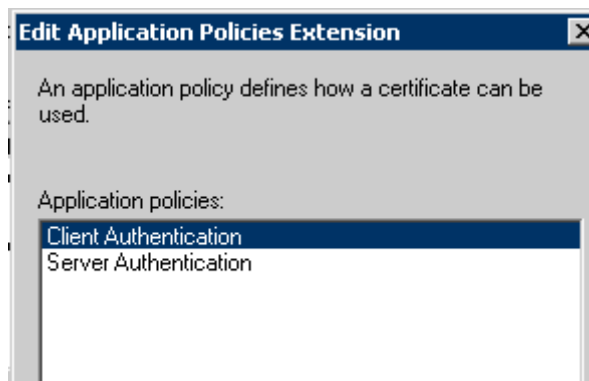
9. In the **Edit Application Policies Extension** dialog box, click **Add**.



10. In the Add Application Policy dialog box, select **Client Authentication** and click **OK**.

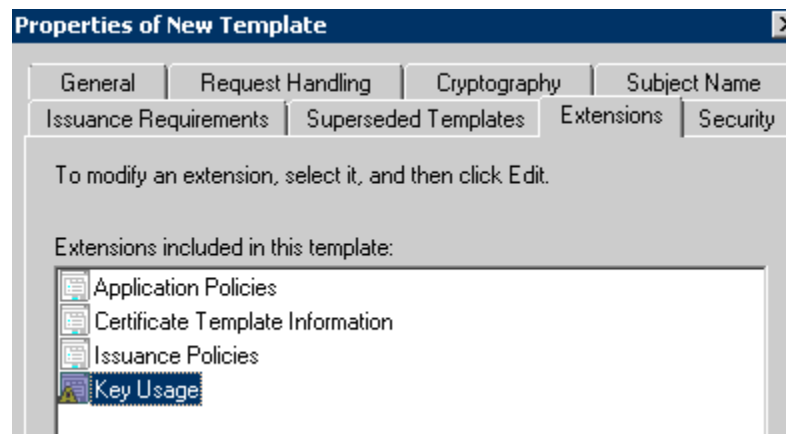


11. In the **Edit Application Policies Extension** dialog box, ensure that both **Server Authentication** and **Client Authentication** are included in the Application Policies list. Click **OK**.

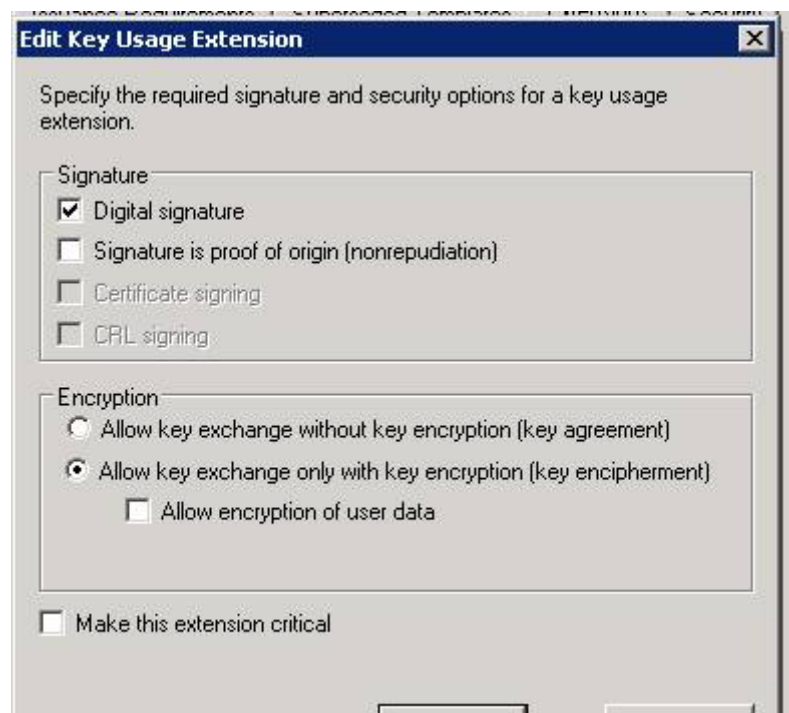


Appendix E: Instructions for generating version 3 certificates

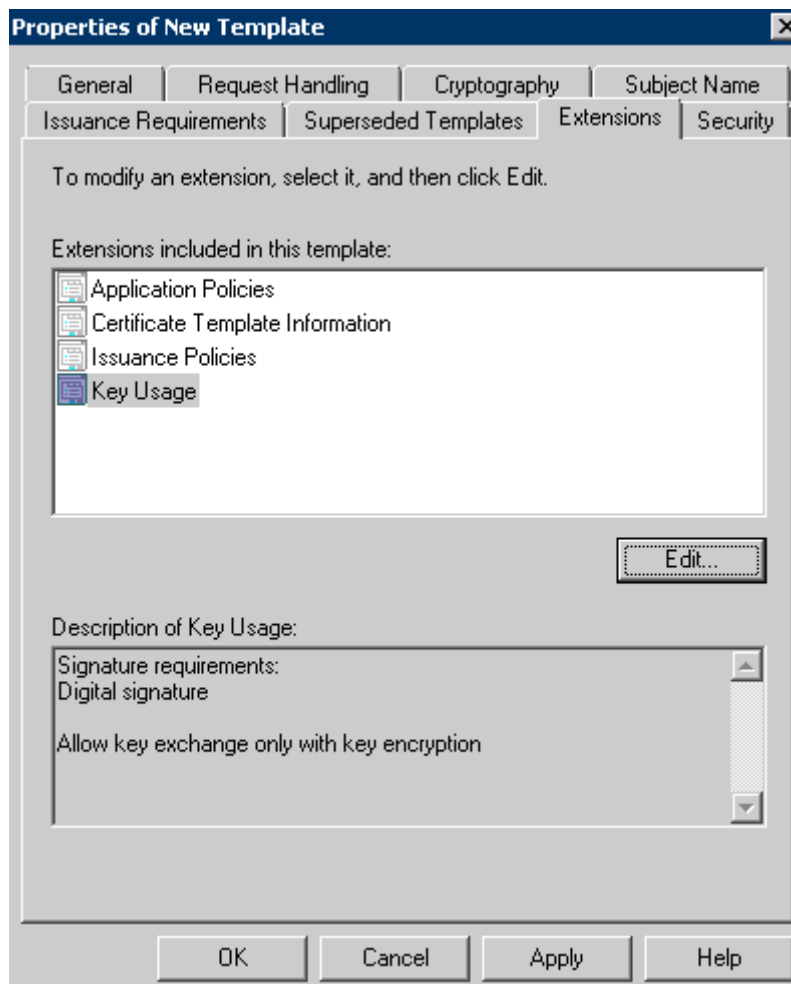
12. In the **Properties of New Template** dialog box, select the **Extensions** tab. In the **Extensions included in this template** section, select **Key Usage** and click **Edit**.



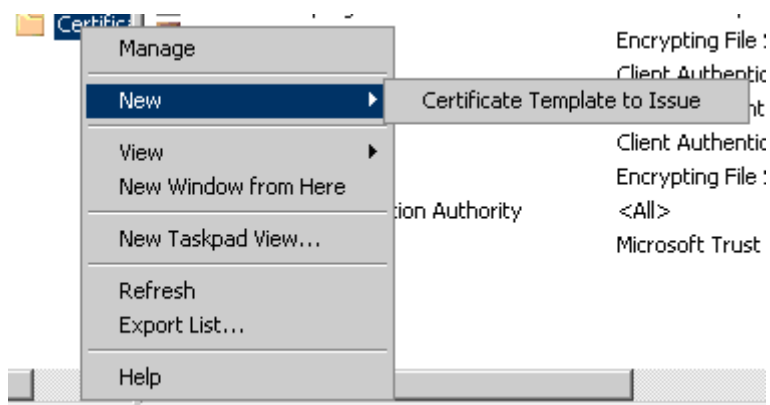
13. In the Edit Key Usage Extension dialog box, uncheck **Make this extension critical** and click on **OK**.



14. From the **Properties of New Template** dialog box, click **OK**.



15. In the **Certification Authority MMC snap-in**, expand the **Certification Authority** node. Right-click on **Certificate Templates**. Select **New Certificate Template to Issue**.



16. In the **Enable Certificate Templates** dialog box, select the Certificate Template you created in Steps 3 -14 and click **OK**.

Requesting and installing the server certificate

The server certificate you are installing is based on the Windows 2008 Enterprise CA server certificate template you created when you completed the procedure [Creating Version 3 \(Windows Server 2008\) Certificate Templates for Server Certificates](#) on page 205)

Follow these steps to request and install the server certificate on the Avaya Application Enablement Services Server.

1. On the Microsoft OCS server, start your Web browser, and log in to the Avaya Application Enablement Services Management Console.
2. From the main menu of the AE Services management console, select **Security > Certificate Management > Server Certificates**.
3. From the In the Server Certificates page, click **Add**.
4. Follow these steps to complete the **Add Server Certificate** page.
 - a. In the **Certificate Alias** field, select a certificate alias (for example **aeservices**).
 - b. In the **Password** field enter an arbitrary password.
 - c. In the **Re-enter Password** field, type the password again.
 - d. In the **Distinguished Name** field, type the distinguished name attributes for your AE Server, as follows:

`CN=AE_Server_FQDN,OU=Department,O=Company,L=City,S=State,C=Country/Region`
For example:

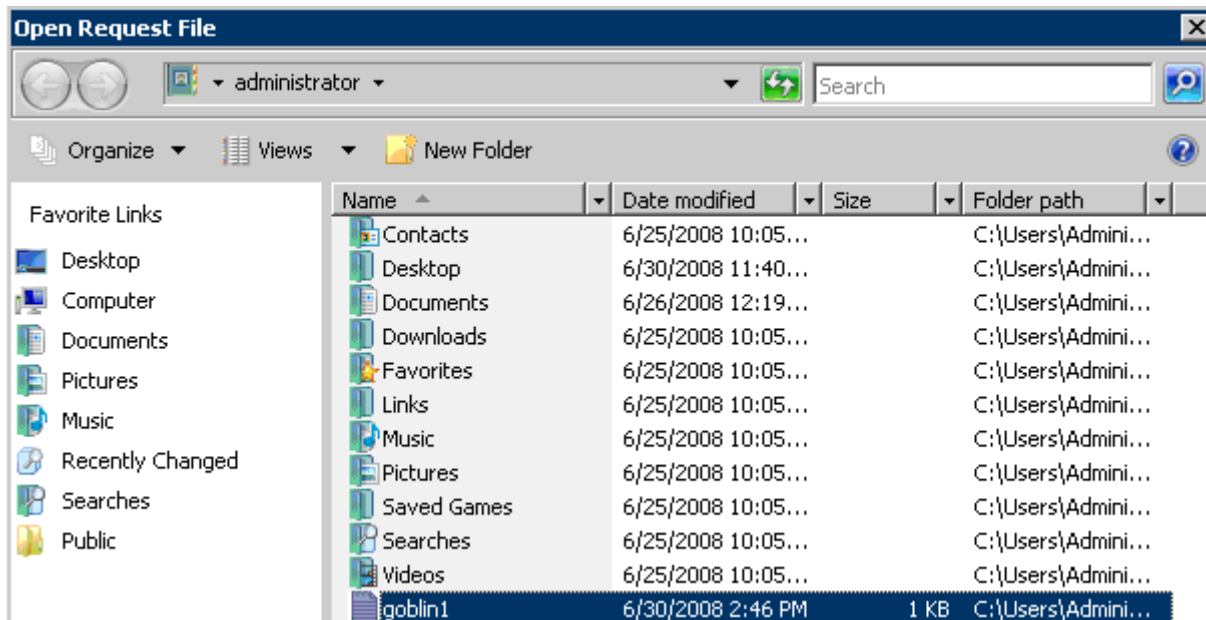
`CN=msavaes1.sitlms.net,OU=SITL,O=Avaya,L=Lincroft,S=New Jersey,C=US`
 - e. Leave the other fields at the defaults, and click **Apply**.
5. From the main menu of the AE Services management console, select **Security > Certificate Management > Server Certificates > Pending Requests**.
6. From the Pending Server Certificates Request page, select the certificate, and click **Manual Enroll**.
7. On the Server Certificate Manual Enrollment Request page, copy the entire contents of the Certificate Request PEM text box, and paste it into a text file, for example **goblin1.txt**
8. On Windows 2008 Enterprise CA server, click **Start > Run**.
9. In the Run dialog box, type `cmd` and click **OK**

10. At the command prompt, type the following command:

```
certreq -attrib "CertificateTemplate:<template name>"
```

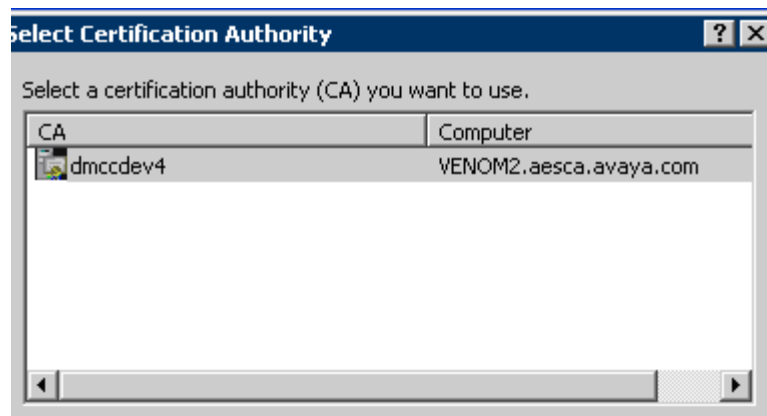
11. Press **Enter**.

12. From the Open Request File window, select the file you created previously, for example, **goblin1**.

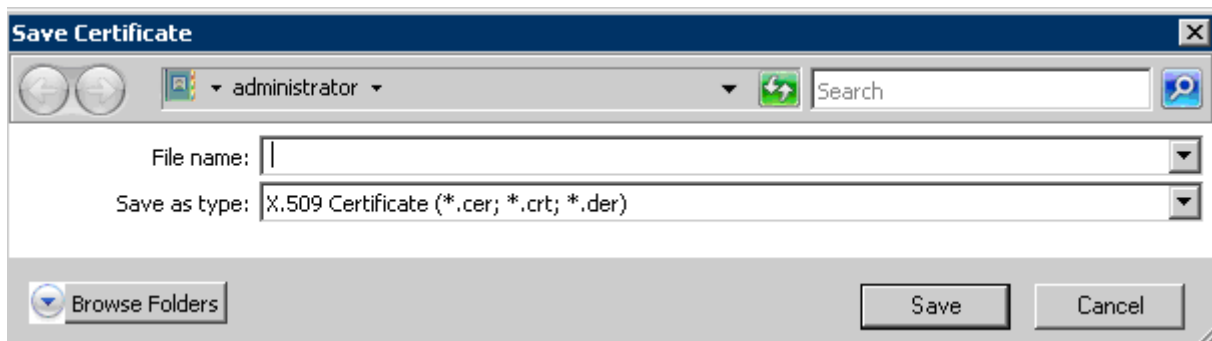


Appendix E: Instructions for generating version 3 certificates

The system displays the Select Certification Authority window that lets you select the CA that will issue the certificate.



13. Select the issuing CA, for example **dmccdev4**, and click **OK**.
14. The system displays the Save Certificate window.



15. In the Save Certificate window, type the file name, for example **goblin1.cer**, and click **Save** to save the file to your local machine.

16. From the main menu of the Avaya AE Services Management Console, click **Security > Certificate Management > Server Certificate > Pending Requests**.

Pending Server Certificate Requests

Manual Enroll		Auto Enroll		Delete
Alias	Creation Date			
<input type="checkbox"/> server	Mon Jun 30 2008 20:44:52			
<input checked="" type="checkbox"/> certname	Tue Jul 01 2008 02:18:36			

17. From the Pending Requests Certificate Requests page, select the alias for the certificate request created in [4a](#) (aeservices) and click **Manual Enroll**.

Server Certificate Manual Enrollment Request

NOTE:

Please make a note of "Certificate Alias" as this value will be required for manual import of signed c

Host localhost

Certificate Alias: certname

Certificate Request PEM:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBBzCB2QIBADAXMRUwEwYDVQQDEwxtZXN1cnZlc15jb20wgZ8wDQYJKoZIhvcN
AQEBBQADgYOAMIGJAoGBAM9hNY0YqtIqC5cdjyMVcCdwDefIQU+t6I1ITSJHOcID
WZ9qEvF+z4MG98aDExCSZ50Mkq570cN3gzTJne94OKEMjeIsw9e9EeI+Xyg8v0wY
xd/BzAmTVN+BgNbZjvPfe59EGBKMMgl81qTInv9CjzIuOyZmKDO/ropkcMh5zwU7
AgMBAAAGGTAXBgkqhkiG9w0BCQcxChMIIcGFzc3dvcmQwDQYJKoZIhvcNAQEEBQAD
gYEAUhVbhFj7kao9sk97NyTOT/2Y/XyrfPYrR9pRDT2wftpbazj2KOi6tW9wUNuk
kO1bHxFt6BKXyaT1W+SsTKXW49MJLygEbQ3KhZ/cowupftBX79wHEydcqeBgTCj1
Qn+I/NERvWurQAsqtW7vjy3pwgn2It10JqMaCYaCHGMO6Og=
-----END CERTIFICATE REQUEST-----
```

Import Close

18. From the Server Certificate Manual Enrollment Request page, click on **Import**.
Your browser displays the Server Certificate Import page.

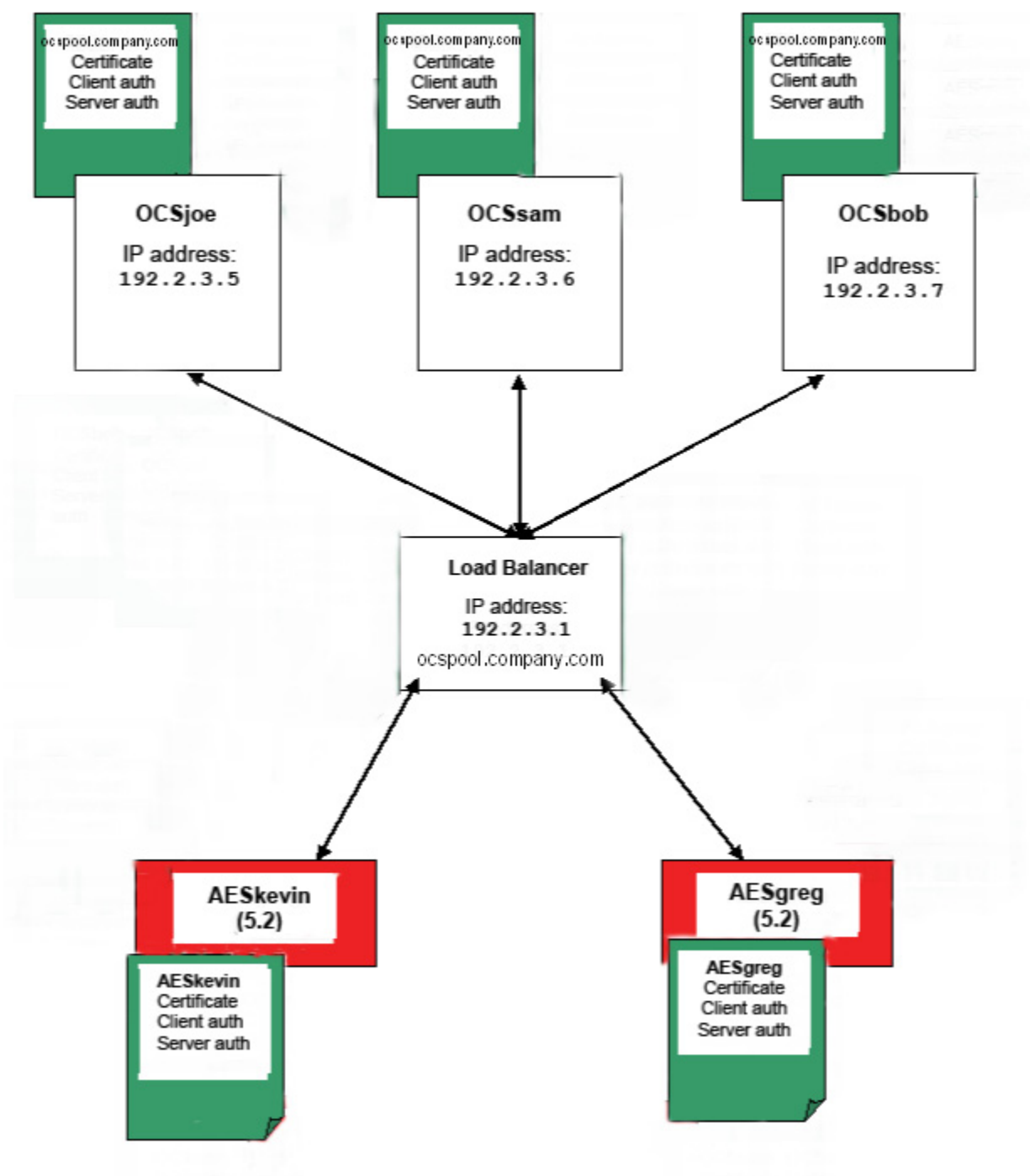


The screenshot shows a dialog box titled "Server Certificate Import". It contains a "Certificate Alias" dropdown menu with "aeservices" selected. Below this is a checked checkbox labeled "Establish Chain of Trust". Underneath is a "File Path" text box followed by a "Browse..." button. At the bottom are "Apply" and "Close" buttons.

19. Complete the Server Certificate Import page as follows:
 - a. In the Certificate Alias field select the same Certificate Alias, aeservices, for example. (For default this step can be skipped).
 - b. Ensure that the Establish Chain of Trust checkbox is checked.
 - c. Load the file saved in Step [15](#); for example, **goblin1.cer**.
 - d. Click **Apply**.

If the import is successful, your browser redisplay the Server Certificate Import with following message: "Certificate imported successfully"

Figure 9: Certificates in a load-balancing scenario



Installing a Microsoft Certificate Services-based certificate on the Microsoft LCS 2005 or OCS 2007

See [Chapter 4: Integrating AE Services with Communications Server 2007](#). Alternatively you can use other tools, for example the LCSCertUtil.exe tool.

Index

A

- Address Book Service
 - local cache of address list [40](#)
 - requirement for AE Services - Live Communications Server integration [30](#)
 - setting up [40](#)
- AE Services administrative workstation, requirement . [31](#)
- AE Services associations capacity [199](#)
- AE Services Server 4.0, integration requirement . . . [31](#)
- Asterisk
 - when interpreted as a literal [77](#), [137](#)
- Asterisk, when treated as a wildcard [78](#), [138](#)
- Authentication of client and server [55](#), [116](#)
- Automatic routing, configuring certificate for [62](#), [123](#)

B

- Bundled Server installation checklist [42](#), [44](#)

C

- Call flow (message flow) diagram [196](#)
- Call flow, TR/87 [195](#)
- capacities
 - AE Services associations [199](#)
 - busy hour call completion (BHCC) [199](#)
 - license consumption [199](#)
 - maximum concurrent users [199](#)
 - throughput [199](#)
- Certificate administration
 - configuring certificate for automatic routing (Live Communications Server). [62](#), [123](#)
 - importing the trusted certificate into AE Services [66](#), [126](#)
 - installing Microsoft-based certificate on Live Communications Server [60](#), [121](#)
 - installing the trusted certificate on AE Server . [63](#), [124](#)
 - summary of sample scenario [53](#), [114](#)
 - verifying installation of entire certificate chain in AE Services [66](#), [127](#)
 - verifying installation of server certificate for Live Communications Server [62](#), [122](#)
- Certificate authority, integration requirement [30](#)
- Certificate management
 - converting certificates from other formats. . . [67](#), [127](#)
 - importing the server certificate into AE Services [71](#), [131](#)
 - installing a trusted certificate chain on AE Server [65](#), [125](#)
- Certificate management scenario, explanation of. [54](#), [115](#)

- Certificate management, Microsoft-based procedure for creating a server certificate for AE Services. . . [70](#), [130](#)
- Checklist
 - Bundled Server installation. [42](#), [44](#)
 - Software-Only server installation [45](#)
- Checklist for Live Communications Server, phase 1. . [37](#)
- Communication Manager, integration requirement . . [30](#)
- Configuring AE Services with 5,000 or more concurrent users, diagram [33](#)
- Configuring AE Services, summary [52](#), [112](#)
- Converting a DER file to PEM [67](#), [127](#)

D

- Dial plan administration in AE Services
 - per-switch settings. [87](#), [147](#)
 - summary [73](#), [133](#)
 - using defaults [89](#), [148](#)
- Dial string characters [77](#), [137](#)
- Distinguished Name (DN) entries and scope of search [92](#), [152](#)

E

- EC500 with XMOBILE, and bridging irregularities [105](#), [165](#)
- Error codes and SIP requests [193](#)

F

- FQDN (fully qualified domain name) of pool [60](#)
- From TelURI and To TelURI rules [75](#), [135](#)
- From TelURI settings [76](#), [82](#), [136](#), [142](#)

H

- High availability configuration [34](#)

I

- Information Technology (IT) technician, bundled server installation [45](#)
- Integration checklist for AE Services and Live Communications Server (Phase 3) [49](#), [109](#)
- ISDN trunk administration in Communication Manager [108](#), [167](#)

K

Known Issues

- Microsoft Office Communicator displays numbers with trunk notation [108](#), [167](#)
- unidentified caller in Microsoft Office Communicator window [107](#), [166](#)

Known issues

- Clear Connection request on a held connection not supported. [104](#), [164](#)
- missed call e-mail. [105](#), [165](#)
- putting active call on hold before starting new call. [104](#)
- setting up forwarding off-switch [103](#), [163](#)
- using the Call Forwarding or Send All Calls features [104](#), [163](#)
- using the Do Not Disturb feature . [102](#), [104](#), [162](#), [164](#)

L

- license consumption [199](#)
- License, Unified CC API Desktop Edition [31](#)
- Live Communications Server
 - installing server certificate [59](#), [120](#)
 - installing trusted certificate [55](#), [116](#)
 - specifying AE Server as authorized host . . . [98](#), [158](#)

M

- Make call, call flow diagram. [198](#)
- maximum concurrent users supported by AE Services [199](#)
- Maximum number of Communication Manager Servers supported, diagram. [32](#)
- Microsoft Lync Server, integrating with AE Services . [169](#)
- Microsoft Office Communicator
 - configuring a static route [97](#), [157](#)
 - group policy settings [99](#), [159](#)

N

- Normalizing phone numbers, Address Book [40](#)

O

- OID (Object Identifier Field), how to complete [60](#)

P

- Phase 1 -- Setting up the Live Communications Server environment [35](#)
- Phase 1 checklist -- Live Communications Server . . [37](#)
- Phase 2 -- Setting up AE Services and Communication Manager. [41](#)
- Phase 3 -- Integrating AE Services with Live Communications Server [46](#)

- Phase 3 Checklist -- integrating AE Services and Live Communications Server [49](#), [109](#)
- Phone Normalization Script [94](#), [155](#)

Procedure 1 - certificate management

- if installing trusted certificate from another vendor [55](#), [116](#)
- importing certificate into trust store [57](#), [118](#)
- installing trusted certificate from Microsoft Certificate Services. [56](#), [117](#)
- installing trusted certificate on Live Communications Server. [55](#), [116](#)

Procedure 1a - verifying installation of trusted certificate on Live Communications Server. [58](#), [119](#)Procedure 2 - installing server certificate for Live Communications Server [59](#), [120](#)Procedure 2a - Verifying the installation of the server certificate for Live Communications Server . . . [62](#), [122](#)Procedure 3 - Installing the trusted certificate on the AE Server [63](#), [124](#)Procedure 3a - Verifying the installation of the trusted certificate in AE Services [66](#), [127](#)Procedure 4 - Creating a server certificate request for AE Services [67](#), [128](#)Procedure 5 - Creating a server certificate for AE Services [69](#), [129](#)Procedure 6 - Importing the server certificate into AE Services OAM [71](#), [131](#)Procedure 6a - Verifying the installation of the server certificate in AE Services [72](#), [132](#)**R**

- Recovering from a system outage [102](#), [162](#)
- Remote Call Control (RCC) extensions, enabling. [94](#), [154](#)
- Remote Call Control SIP URI field [96](#), [156](#)
- Replacing an expired server certificate. [72](#), [132](#)
- Requirements for AE Services - Live Communications Server integration [30](#)

S

- Service Pack 12866, Communication Manager . [107](#), [166](#)
- SIP requests and error codes [193](#)
- SIP requirements [25](#), [31](#)
- SIP URI field [96](#), [156](#)
- Software-Only server, installation checklist [45](#)
- static route [97](#), [157](#)

T

- Tel URI format, example [95](#), [156](#)
- Tel URI formats and device IDs [74](#), [134](#)
- To TelURI settings [78](#), [81](#), [84](#), [138](#), [141](#), [144](#)
- TR/87 port in OAM, enabling [52](#), [113](#)
- TR/87, defined [18](#)
- Trust store, Live Communications Server [57](#), [118](#)