

Avaya Aura® Application Enablement Services Implementation Guide for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007

Release 6.1
February 2011
Issue 1

© 2011 Avaya Inc.
All Rights Reserved.

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

About this document 9

Chapter 1: Overview 11

Overview of the AE Services integration 11

What's new for this release 11

The AE Services provides seamless integration 11

Features of the AE Services implementation for Microsoft Office Communications Server 13

What is TR/87? 14

What is SIP? 14

Features provided by AE Services 15

Integration with Microsoft Office Communicator 16

Microsoft Office Communicator 2007 feature-related changes 16

A brief summary of Microsoft Office Communicator and Microsoft Live Communications Server 18

Making a simple phone call 20

Setting up a dial plan 21

Requirements for the AE Services integration 23

High Availability 27

AE Services System Platform High Availability Failover 27

The road map for integrating AE Services and Microsoft Office components . . 28

Phase 1: Setting up the Live Communications Server 2005 or the Office Communications Server 2007 environment 28

Phase 1 checklist: Live Communications Server 30

Phase 2: Setting up AE Services and Communication Manager 34

Phase 2 checklists: setting up AE Services and Communication Manager 34

Application Enablement Services on System Platform installation checklist 36

Bundled Server installation checklist 38

Software-Only server installation checklist 40

Phase 3: Integrating AE Services with Live Communications Server 41

Chapter 2: Integrating AE Services with Live Communications Server 2005 43

How to use the information in this chapter 43

Phase 3 Checklist --integrating AE Services with Live Communications Server . 43

About configuring AE Services for Live Communications Server 46

Enabling the TR/87 port 46

Administering Certificates -- certificate management 47

Additional references 47

About the sample scenario 48

About obtaining certificates 48

Specifying key usage 48
Client and server authentication 48
Procedure 1 - Installing the trusted certificate on Live Communications Server 49
Installing the trusted certificate from another vendor. 49
Installing the trusted certificate generated by Microsoft Certificate Services 50
Importing the certificate into the Live Communications Server's trust store 51
Procedure 1a - Verifying the installation of the trusted certificate on Live Communications Server 52
Procedure 2 - Installing a server certificate for the Live Communications Server 53
Installing a server certificate from another vendor 53
Installing a Microsoft Certificate Services-based certificate on the Live Communications Server 54
Procedure 2a - Verifying the installation of the server certificate for Live Communications Server 56
Procedure 2b - Configuring the certificate for automatic routing 56
Procedure 3 - Installing the trusted certificate on the AE Server. 58
Generic procedure for installing the trusted certificate for AE Services . 59
Microsoft-based procedure for installing a trusted certificate chain. . . . 61
Importing the trusted certificate into the AE Services Management Console 62
Procedure 3a - Verifying the installation of the trusted certificate in AE Services 63
Converting Certificate files in other formats for AE Services 64
Procedure 4 - Creating a server certificate request for AE Services. 65
Procedure 5 - Creating a server certificate for AE Services 67
Generic procedure for creating a server certificate for AE Services. . . . 67
Microsoft-based procedure for creating a server certificate for AE Services 68
Procedure 6 - Importing the server certificate into AE Services 69
Procedure 6a - Verifying the installation of the server certificate in AE Services 70
Replacing an expired server certificate 70
Dial Plan settings in AE Services. 71
Before you begin. 71
About Tel URI formats and device IDs 72
About the From TelURI and To TelURI rules. 73
TelURI settings - how incoming and outgoing numbers are processed. . . . 74
Pattern matching -- using Pattern and RegEx (regular expressions) . . . 74
Valid dial string characters and using the asterisk 75

The From Tel URI table 76
The To TelURI table 76
From TelURI settings for fixed-length extensions 78
To TelURI settings for fixed-length extensions 80
From TelURI settings for variable-length extensions 81
To TelURI settings for variable length extensions. 83
Pattern matching -- using Pattern and RegEx (regular expressions) . . . 84
Dial Plan tips 86
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
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 3: 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 115
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 . 125
Microsoft-based procedure for installing a trusted certificate chain. . . . 126
Importing the trusted certificate into the AE Services Management Console 127
Procedure 3a - Verifying the installation of the trusted certificate in AE Services 128
Converting Certificate files in other formats for AE Services 129
Procedure 4 - Creating a server certificate request for AE Services. 130
Procedure 5 - Creating a server certificate for AE Services 132
Generic procedure for creating a server certificate for AE Services. . . . 132
Microsoft-based procedure for creating a server certificate for AE Services 133

Procedure 6 - Importing the server certificate into AE Services 134
Procedure 6a - Verifying the installation of the server certificate in AE Services 135
Replacing an expired server certificate 135
Dial Plan settings in AE Services 136
Before you begin. 136
About Tel URI formats and device IDs 137
About the From TelURI and To TelURI rules 138
TelURI settings - how incoming and outgoing numbers are processed 139
Pattern matching -- using Pattern and RegEx (regular expressions) . . . 139
Valid dial string characters and using the asterisk 140
The From Tel URI table 141
The To TelURI table 141
From TelURI settings for fixed-length extensions 142
To TelURI settings for fixed-length extensions 144
From TelURI settings for variable-length extensions 145
To TelURI settings for variable length extensions. 147
Pattern matching -- using Pattern and RegEx (regular expressions) . . . 148
. 149
Dial Plan tips 150
Administering dial plan settings on a per-switch basis 151
Administering default dial plan settings 153
Administering AE Services access to Active Directory 154
DN entries and scope of search 156
Avoid making the Base Search DN too specific 156
Making changes on the Enterprise Directory Configuration page 157
Determining the DN for a user object. 157
Configuring Microsoft Office Communications Server 2007 for AE Services . . . 158
Enabling Remote Call Control in Active Directory 160
Setting up connections 161
Configuring a static route 162
Specifying the AE Server as an authorized host 163
Microsoft Office Communicator users - group policy settings 164
About authentication and authorization 164
Using the TR/87 Test features. 165
The Host AA setting and TR/87 test 165
Administering Microsoft Office Communications Server 2007 for the agent login ID 166
Re-synchronizing states 166
Usage Tips for the Do Not Disturb feature 167

Recovering from a system outage 167
Known issues 168
Setting up forwarding off-switch 168
Using Call Forwarding and Send All Calls 169
Using the Do Not Disturb feature 169
Putting the active call on hold before starting a new call 169
Clear Connection request on a held connection is not supported 169
Bridging irregularities 170
Missed Call e-mail 170
Usage instructions for analog phones 171
Unidentified caller in Microsoft Office Communicator window 172
Communicator displays numbers with trunk notation 173

Appendix A: SIP requests and associated errors 175

Appendix B: AE Services Implementation for Microsoft LCS call flow 177
Message flow 177

Appendix C: Capacities 181

Appendix D: Creating a certificate template for Server Certificates on the Microsoft CA Server 183
Creating a certificate template for Server Certificates on the Microsoft CA Server 184

Appendix E: Instructions for generating version 3 certificates 187
Creating Version 3 (Windows Server 2008) Certificate Templates for Server Certificates 188
Requesting and installing the server certificate 196
Installing a Microsoft Certificate Services-based certificate on the Microsoft LCS 2005 or OCS 2007 202

Index 203

About this document

As a high-level planning and implementation guide, this document serves as a roadmap for using the Microsoft Live Communications Server documents and the AE Services documents.

In terms of planning, this document is intended for anyone who is involved with integrating Application Enablement Services (AE Services) with either of the following Microsoft platforms:

- Microsoft Office Live Communications Server 2005 SP 1 (along with Microsoft Office Communicator 2005)
- Microsoft Office Communications Server 2007 (along with Microsoft Office Communicator 2007) and Microsoft Office Communications Server 2007 R2. 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.

In terms of implementation, it is directed toward administrators from the Microsoft and the AE Services administrative domains.

Note:

This document does not describe how to use the Microsoft Office Client. For information about using the Microsoft Office Client, see Microsoft Office Client Help or the *Microsoft Office Communicator 2007 Getting Started Guide*.

Chapter 1: Overview

Overview of the AE Services integration

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

What's new for this release

Release 6.1 includes the following updates.

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.

- 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

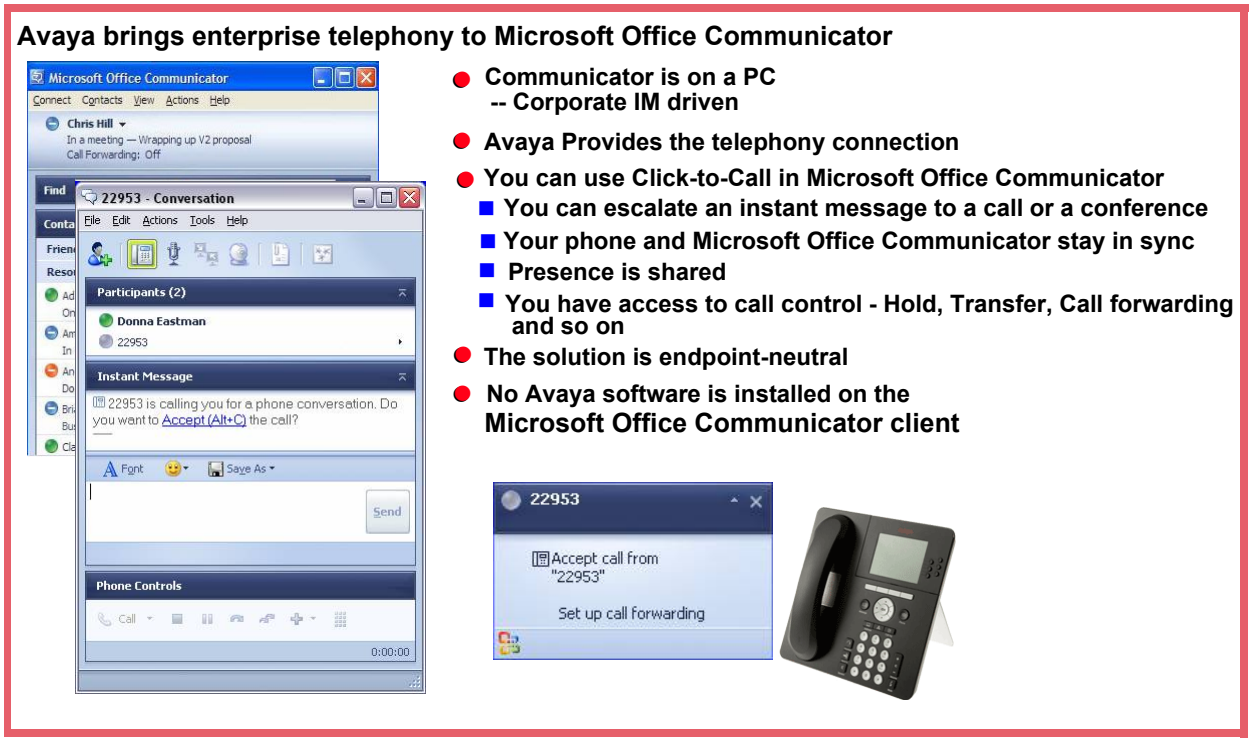
For a more complete list of features, see Features provided by AE Services on page 15.

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



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:

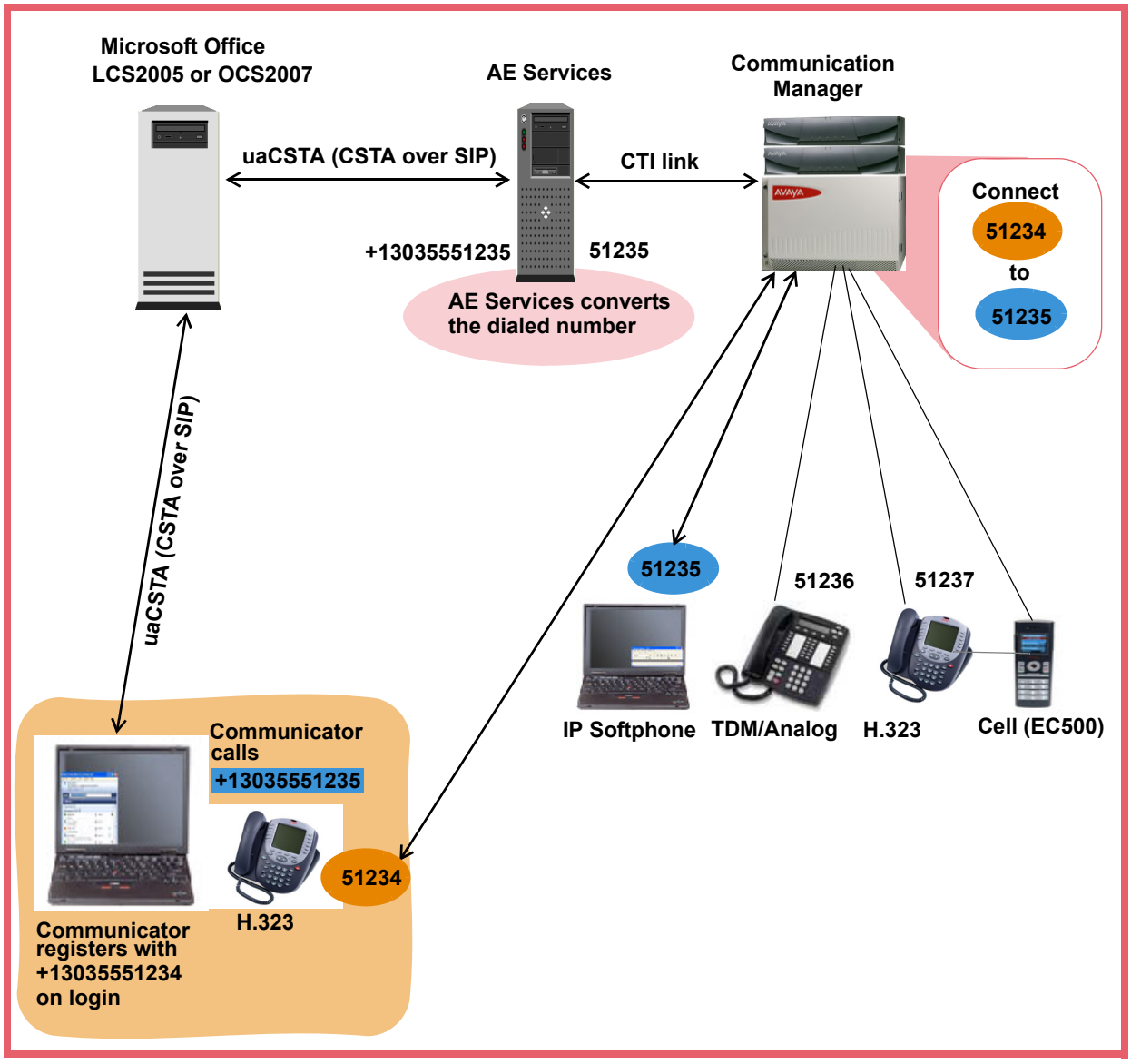
- Its primary role is to provide Global Address List updates to the Communicator 2005 or Communicator 2007 client. It performs this function daily.
- Additionally, it can be configured to normalize phone numbers for the Communicator 2005 or Communicator 2007. For more information, see Set up Address Book Service on page 33.

Making a simple phone call

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.



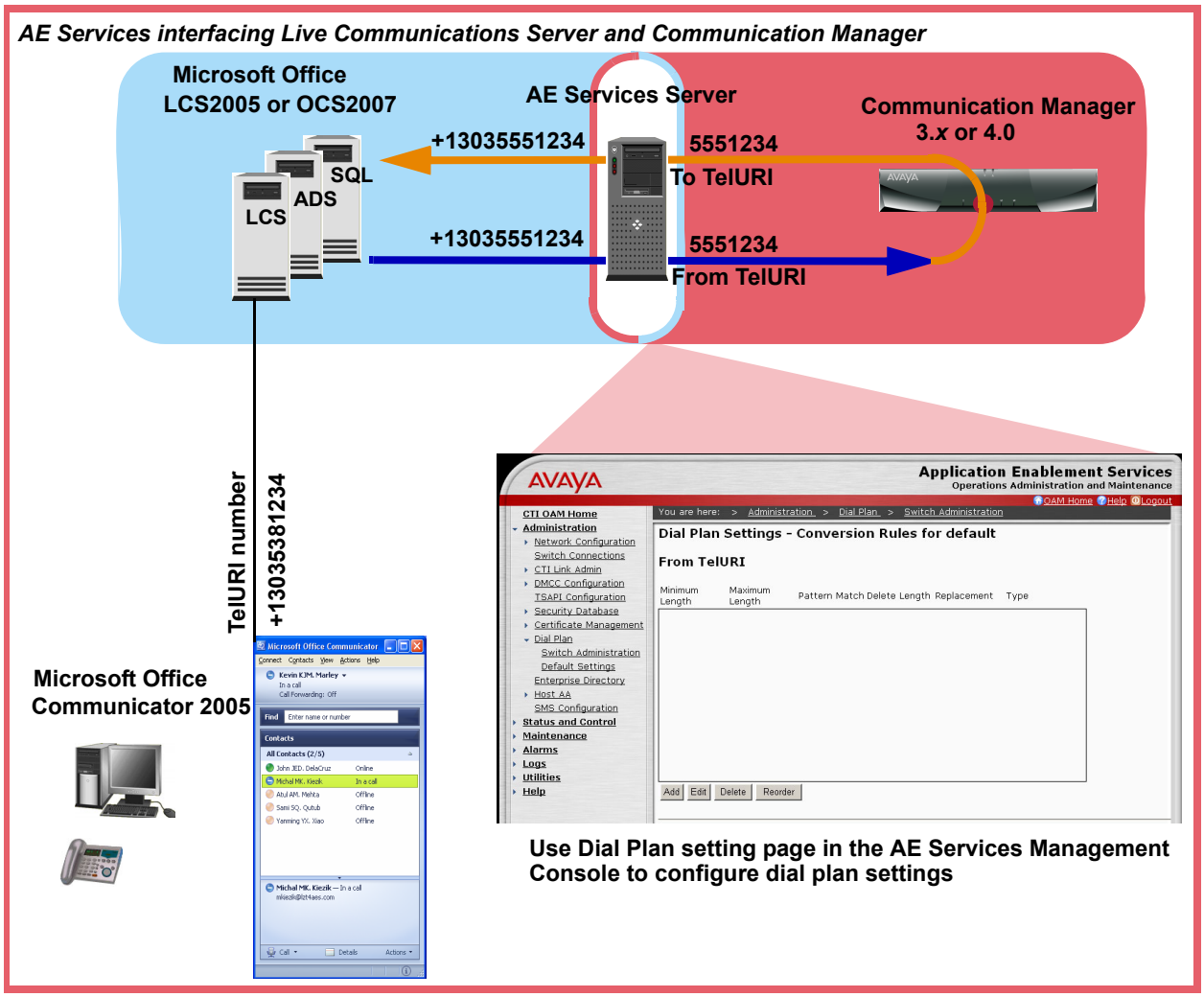
Setting up a dial plan

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



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 33.

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 26).

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.

Note:

Windows 2003 or 2008 Server Standard Edition comes with a Standard Edition CA, the Enterprise Edition CA is only included Windows 2003 or 2008 Server Enterprise Edition.

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.

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 25).

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 is 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 47.

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

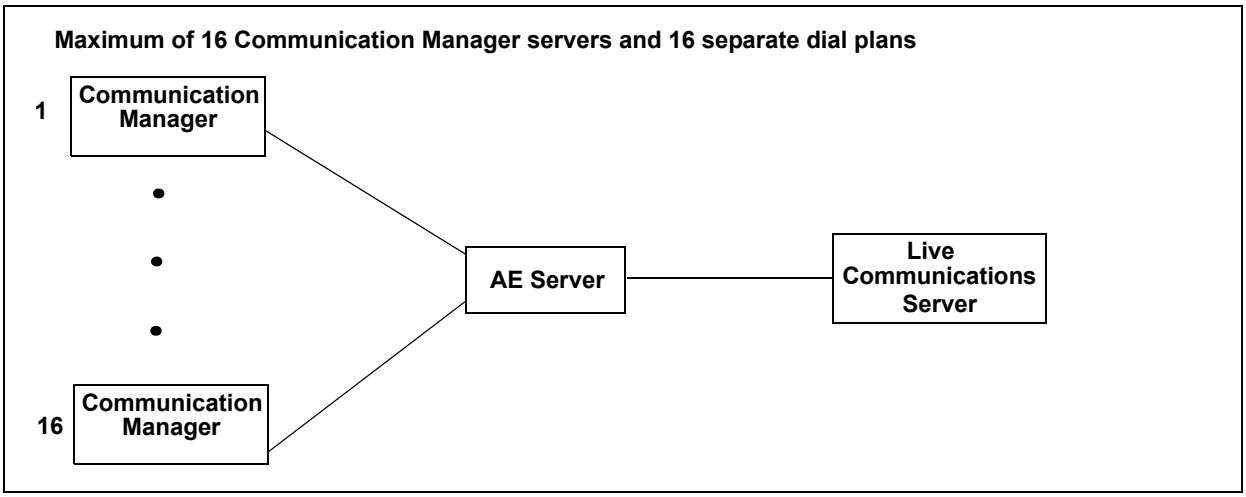
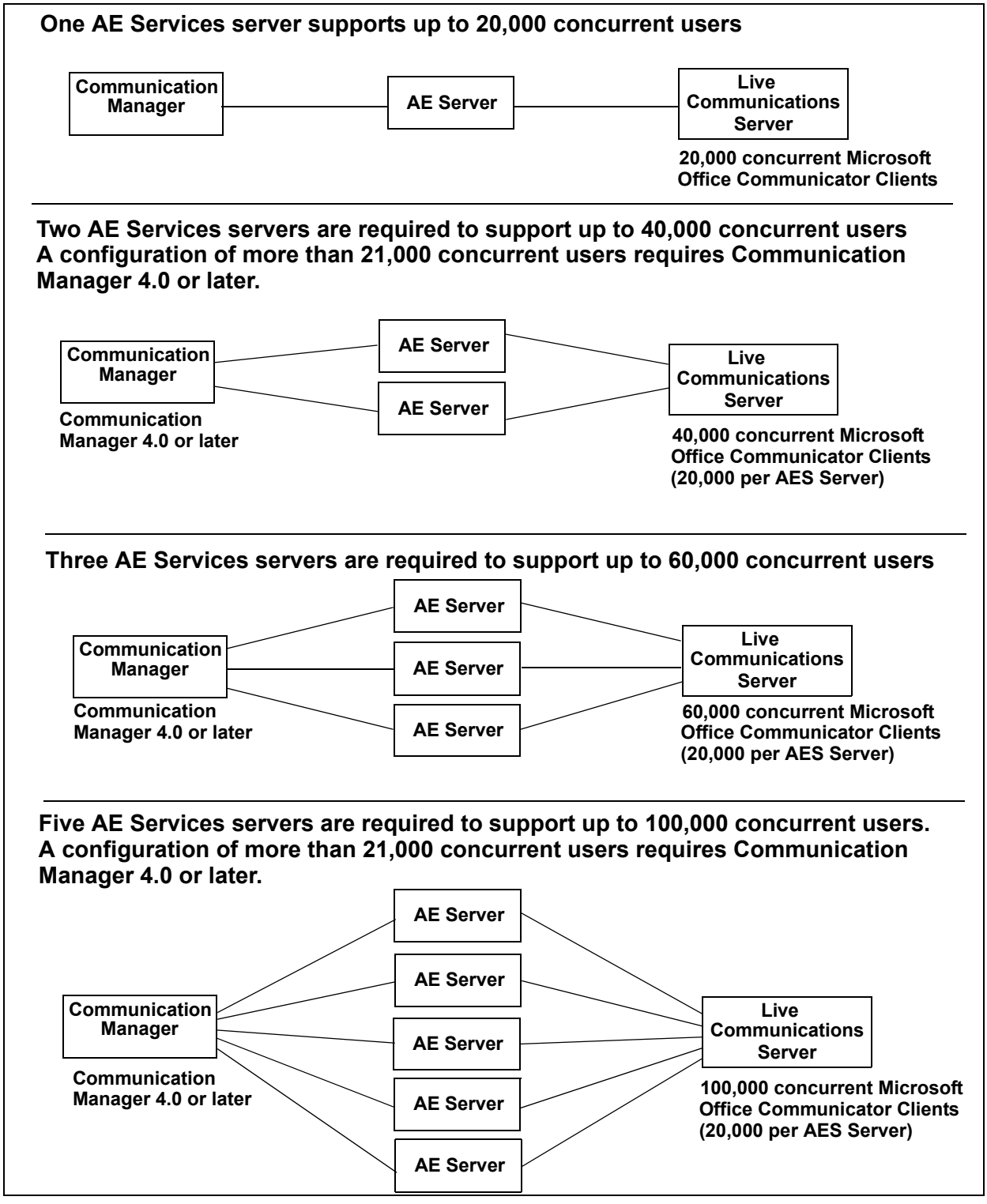


Figure 4: Configuring AE Services with 20,000 or more concurrent users



High Availability

While AE Services does not support an automatic failover to a backup server for the AE Services 6.1 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/OCSR2 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

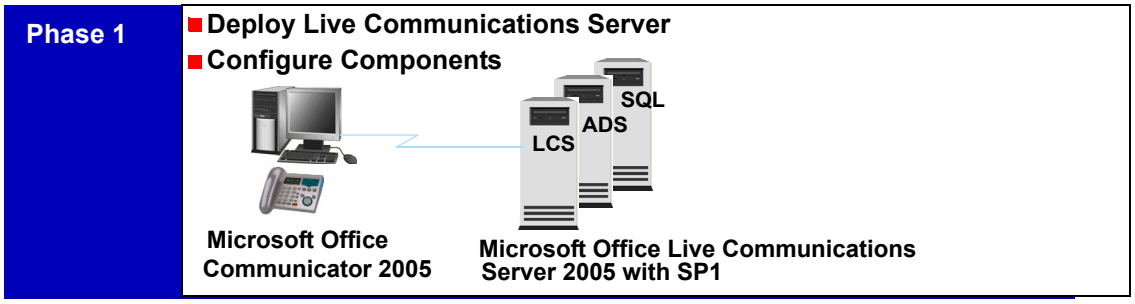
This section maps the integration activities to the documentation.

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 30. 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 28.

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 34, but they must be completed before the tasks described in Chapter 2: Integrating AE Services with Live Communications Server 2005.

Table 1: Checklist for Live Communications Server

	Task	Document
1	**Active Directory is set up**	
	• Domain controllers with Microsoft Windows 2000 SP4 or Microsoft Windows 2003. • Global catalog servers with Windows 2000 SP4 or Windows Server 2003. For more information about Global catalog servers, see "Infrastructure Requirements," in *Live Communications Server 2005 with SP1 Active Directory Preparation*. **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.	• *Microsoft Office Live Communications Server 2005 with SP1 Standard Edition Deployment Guide* • *Microsoft Office Live Communications Server 2005 with SP1 Enterprise Edition Deployment Guide*
2	**Active Directory preparation is completed**	
	Carry out the Active Directory Preparation basic steps: • Prep Schema • Prep Forest • Prep Domain • DomainAdd to the Forest Root	• *Microsoft Office Live Communications Server 2005 with SP1 Active Directory Preparation*. 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)

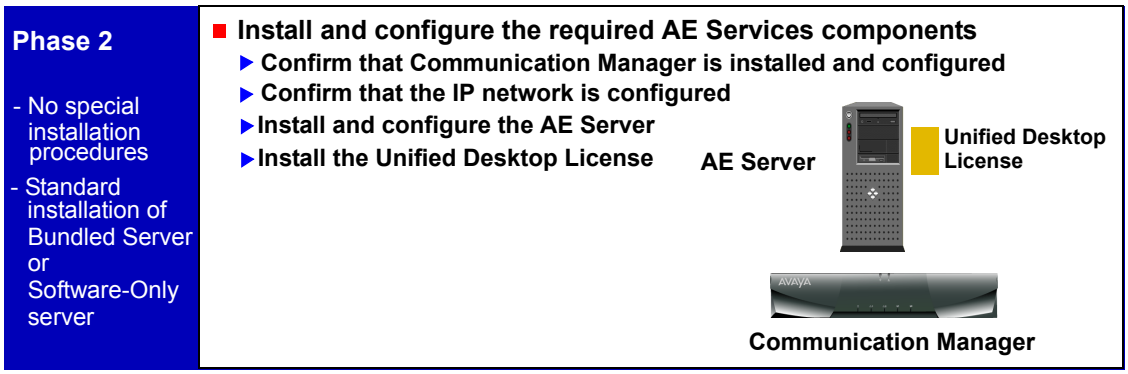
	Task	Document
3	**Public Key Infrastructure (PKI) is set up**	
	Set up a Public Key Infrastructure (PKI).	• For more information, see *Microsoft Office Live Communications Server 2005 Certificate Configuration.* • See also, *Live Communications Server 2005 with SP1 Security Guide*.
4	**Certificates have 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.	• See *Microsoft Office Live Communications Server 2005 Certificate Configuration*, "Configuring Certificates on Live Communications Servers." • See also, Administering Certificates -- certificate management on page 47.
5	**Domain Name System (DNS) is set up and deployed**	
	Set up the server.	See "Configuring DNS, Client Access and User Settings" in either of these documents: • *Microsoft Office Live Communications Server 2005 with SP1 Standard Edition Deployment Guide* • *Microsoft Office Live Communications Server 2005 with SP1 Enterprise Edition Deployment Guide*
6	**Live Communications Server (either Standard or Enterprise) is deployed**	
	• Deploy Standard Edition. or • Deploy Enterprise Edition.	• See "Deploying Live Communications Server 2005 Standard Edition" in the *Microsoft Office Live Communications Server 2005 with SP1 Standard Edition Deployment Guide.* • See "Deploying Live Communications Server 2005 Enterprise Edition" in the *Microsoft Office Live Communications Server 2005 with SP1 Enterprise Edition Deployment Guide.*
		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.	• See "Configuring the Standard Edition Server" in the *Microsoft Office Live Communications Server 2005 with SP1 Standard Edition Deployment Guide.* • See "Configuring the Enterprise Edition Server" in the *Microsoft Office Live Communications Server 2005 with SP1 Enterprise Edition Deployment Guide.*
8	**DNS is configured**	
	Configure DNS.	• See "Configuring DNS, Client Access and User Settings" in the *Microsoft Office Live Communications Server 2005 with SP1 Standard Edition Deployment Guide.* • See "Configuring DNS, Client Access and User Settings" in the *Microsoft Office Live Communications Server 2005 with SP1 Enterprise Edition Deployment Guide.*
9	**Set up Address Book Service** • **Address Book Service is required for AE Services Live Communications Server integration.**	
	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. Optionally, you can set up the Address Book Service to perform phone number normalization. **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.	• See *Microsoft Office Live Communications Server 2005 Address Book Service Planning and Deployment Guide.*
		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 34.



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 2: Integrating AE Services with Live Communications Server 2005.

- Table 2 summarizes the tasks that are required for carrying out an AE Services on Syste 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.

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 *Implementing Avaya Aura™ Application Enablement Services on Avaya Aura™ System Platform*.
2	Install and configure the hardware.	FE	See *Implementing Avaya Aura™ Application Enablement Services on Avaya Aura™ System Platform*.
3	Install the software.	FE	See *Implementing Avaya Aura™ Application Enablement Services on Avaya Aura™ System Platform*.
4	Install the AE Services license.	FE	See *Implementing Avaya Aura™ Application Enablement Services on Avaya Aura™ System Platform*. **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 is has an active dialog with Application Enablement Services.
5	Verify Communication Manager requirements.	PS/FE	See the *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*.
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 *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*.
7	Enable AE Services on Communication Manager.	PS	See the *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*.
			1 of 2

Table 2: Application Enablement Services on System Platform installation checklist

	Task	Role	Document
8	Administer a CTI link (ADJ-IP).	PS	See the *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*.
9	Check the status of the switch connection (from Communication Manger to AE Services).	PS	See the *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*.
			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 *Implementing Avaya Aura™ Application Enablement Services for a Bundled Server*.
2	Install and configure the hardware.	FE	See *Implementing Avaya Aura™ Application Enablement Services for a Bundled Server*.
3	Install the software.	FE	See *Implementing Avaya Aura™ Application Enablement Services for a Bundled Server*.
4	Install the AE Services license.	FE	See *Implementing Avaya Aura™ Application Enablement Services for a Bundled Server*. **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 is has an active dialog with Application Enablement Services.
5	Verify Communication Manager requirements.	PS/FE	See the *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*.
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 *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*.
7	Enable AE Services on Communication Manager.	PS	See the *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*.
			1 of 2

Table 3: Bundled server installation checklist (continued)

	Task	Role	Document
8	Administer a CTI link (ADJ-IP).	PS	See the *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*.
9	Check the status of the switch connection (from Communication Manger to AE Services).	PS	See the *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*.
			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

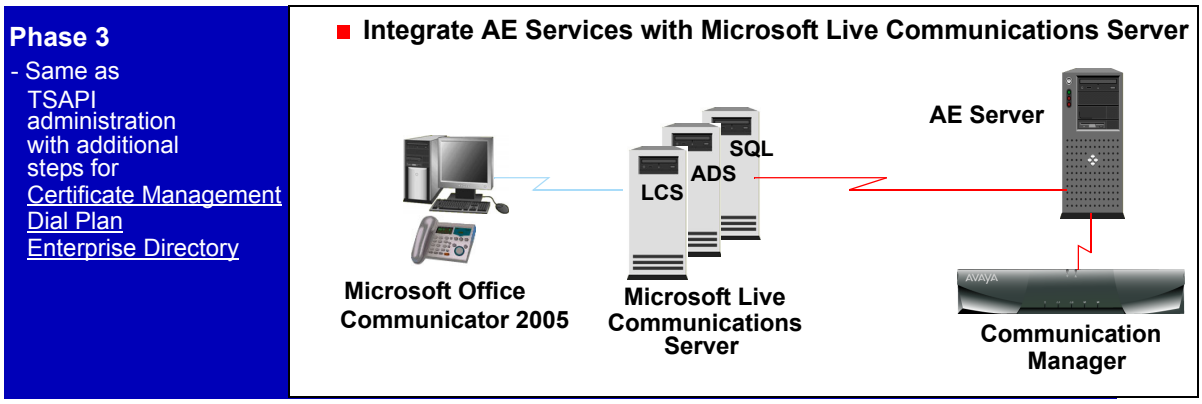
	Task	Admin domain	Document
1	Determine that you have met the prerequisites for AE Services.	AE Services	See *Implementing Avaya Aura™ Application Enablement Services in a Software-Only Environment*.
2	Install the Linux platform software.	AE Services	See *Implementing Avaya Aura™ Application Enablement Services in a Software-Only Environment*.
3	Install the software.	AE Services	See *Implementing Avaya Aura™ Application Enablement Services in a Software-Only Environment*.
4	Install the AE Services license.	AE Services	See *Implementing Avaya Aura™ Application Enablement Services in a Software-Only Environment*. **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 is has an active dialog with Application Enablement Services.
5	Verify Communication Manager requirements.	Communication Manager	See the *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*.
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 *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*.
7	Enable AE Services on Communication Manager.	Communication Manager	See the *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*.
			1 of 2

Table 4: Software-only server installation checklist

	Task	Admin domain	Document
8	Administer a CTI link (ADJ-IP).	Communication Manager	See the *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*.
9	Check the status of the switch connection (from Communication Manger to AE Services).	Communication Manager	See the *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*.
			2 of 2

Phase 3: Integrating AE Services with Live Communications Server

Phase 3 is presented separately in Chapter 2: 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 2: 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 *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*, 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 46.
			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 49.
		Microsoft Live Communications Server	See Procedure 2 - Installing a server certificate for the Live Communications Server on page 53 of this document.
		AE Services	See Procedure 3 - Installing the trusted certificate on the AE Server on page 58 of this document.
		AE Services	See Procedure 4 - Creating a server certificate request for AE Services on page 65 of this document.
		AE Services	See Procedure 5 - Creating a server certificate for AE Services on page 67 of this document.
		AE Services	See Procedure 6 - Importing the server certificate into AE Services on page 69 of this document.
6	Administer settings for the dial plan.	AE Services	See Dial Plan settings in AE Services on page 71 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 *Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide*.
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 *Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide.*
			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 46
  - administering certificates - see Administering Certificates -- certificate management on page 47
  - administering the dial plan settings - see Dial Plan settings in AE Services on page 71
  - 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 49
- Procedure 2 - Installing a server certificate for the Live Communications Server on page 53
- Procedure 3 - Installing the trusted certificate on the AE Server on page 58
- Procedure 4 - Creating a server certificate request for AE Services on page 65
- Procedure 5 - Creating a server certificate for AE Services on page 67
- Procedure 6 - Importing the server certificate into AE Services on page 69

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 183. 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 54.

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 51.

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 (**Icscertnew.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\lcscertnew.p7b**, for example). Select the certificate file (**lcscertnew.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 53.
- If you are using Microsoft Certificate Services, refer to Installing a Microsoft Certificate Services-based certificate on the Live Communications Server on page 54.

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 56.

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: **mylcspool.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 48

   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 in 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 (**mylcspool**, for example), right-click the fully qualified domain name of your server (**mylcserver.example.com**, for example), and then click **Properties**.
4. From the ***mylcsserver.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, mylcspool.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, mylcspool.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 59.
- If you are using Microsoft Certificate Services, use the procedure described in Microsoft-based procedure for installing a trusted certificate chain on page 61.

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:\temp\aetrucert.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 62.

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:\temp\aetrucert.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 62.

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 63.

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 52.
   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 certicificate alias:
     - **aeservices** refers to tthe 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 67.
- If you are using Microsoft Certificate Services, refer to Microsoft-based procedure for creating a server certificate for AE Services on page 68.

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 66).
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 64.

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, and click **Submit**. (You paste the certificate request that you copied in Step 5 of Procedure 4 on page 66).
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 64.

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 72.
- 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 73.

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.

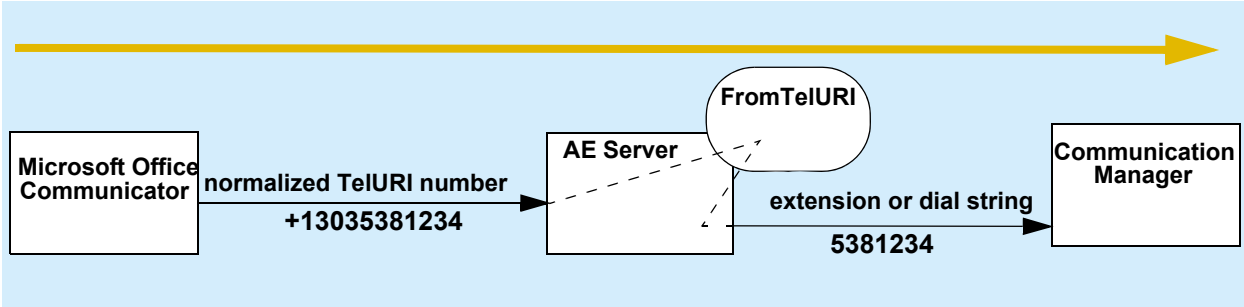
Table 6: Tel URI formats supported by AE Services

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

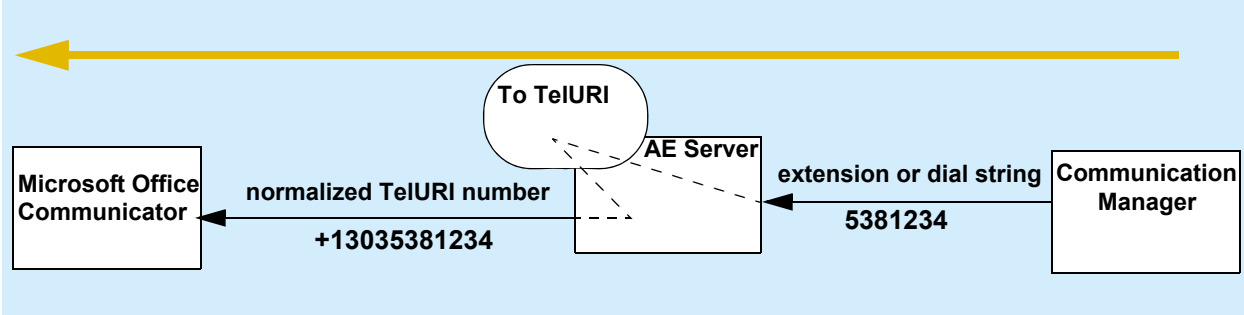
About the From TelURI and To TelURI rules

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 78
- To TelURI settings for fixed-length extensions on page 80

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

- From TelURI settings for variable-length extensions on page 81
- To TelURI settings for variable length extensions on page 83

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 86). 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 86). 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 73.

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 **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 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\,Al,cn=sertech,cn=services,cn=users,dn=example,dc=com

     cn=RTCAdmin,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:

     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 90:

- User DN for Query Authentication

  cn=Pat Brown,cn=sertech,cn=services,cn=users,dc=example,dc=com

- Base Search DN

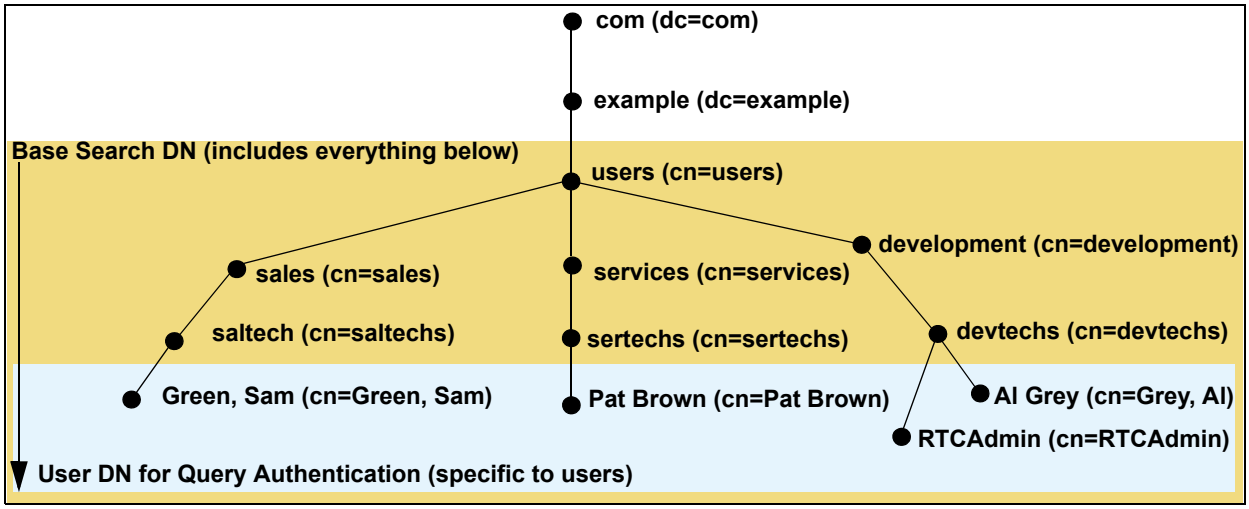
  cn=users,dc=example,dc=com

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 redisplays 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 31).
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 31).
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.

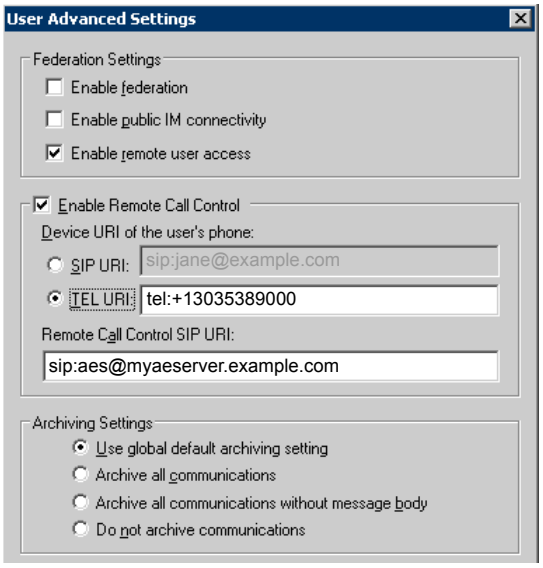
Tip:

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.



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@myaeserver.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: **mylcserver.example.com**
3. From the "mylcserver.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 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 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 3: 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 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 130 of this document.
		AE Services	See Procedure 5 - Creating a server certificate for AE Services on page 132 of this document.
		AE Services	See Procedure 6 - Importing the server certificate into AE Services on page 134 of this document.
6	Administer settings for the dial plan.	AE Services	See Dial Plan settings in AE Services on page 136 of this document.
7	Administer settings for Active Directory.	AE Services	See Administering AE Services access to Active Directory on page 154 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 *Microsoft Office Communicator 2007 Telephony Planning and Deployment Guide*.
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 162.
			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 163.
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 160. Based on information from *Microsoft Office Communicator 2005 Telephony Planning and Deployment Guide.*
			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 136
  - administering settings for Active Directory - see Administering AE Services access to Active Directory on page 154

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 130
- Procedure 5 - Creating a server certificate for AE Services on page 132
- Procedure 6 - Importing the server certificate into AE Services on page 134

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 183. 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 (**Icscertnew.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 in 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 125.
- If you are using Microsoft Certificate Services, use the procedure described in Microsoft-based procedure for installing a trusted certificate chain on page 126.

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:\temp\aetrucert.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 127.

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:\temp\aetrucert.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 127.

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 128.

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 132.
- If you are using Microsoft Certificate Services, refer to Microsoft-based procedure for creating a server certificate for AE Services on page 133.

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 131).
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 129.

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, and click **Submit**. (You paste the certificate request that you copied in Step 5 of Procedure 4 on page 131).
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 129.

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 151.
- You can administer default dial plan settings that are used for all switches. For more information, see Administering default dial plan settings on page 153.

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 137.
- 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 138.

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.

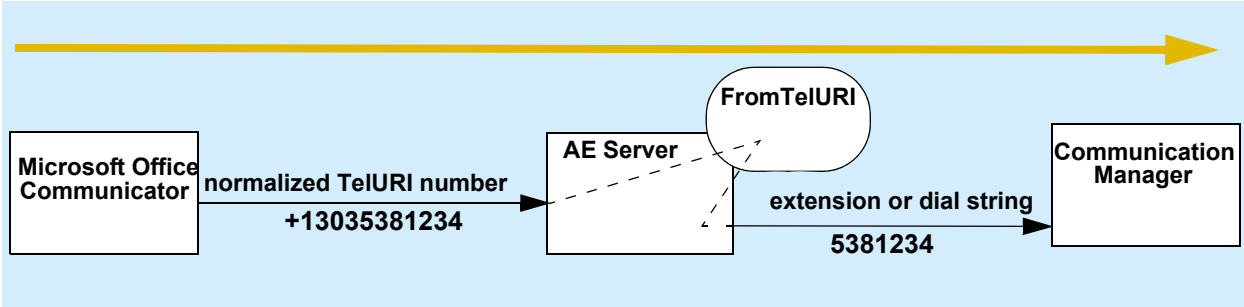
Table 9: Tel URI formats supported by AE Services

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

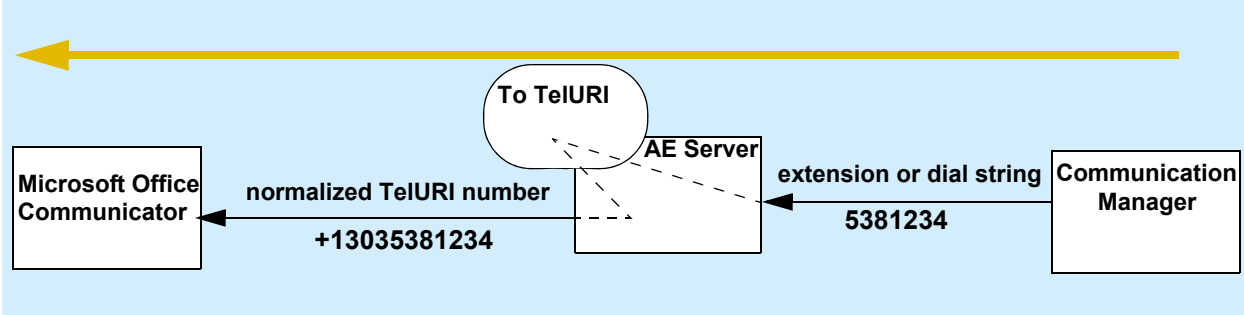
About the From TelURI and To TelURI rules

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 142
- To TelURI settings for fixed-length extensions on page 144

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

- From TelURI settings for variable-length extensions on page 145
- To TelURI settings for variable length extensions on page 147

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 150). 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 150). 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 138.

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 153. 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 156 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\,Al,cn=sertech,cn=services,cn=users,dn=example,dc=com

     cn=RTCAdmin,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 157. If you are not sure what the DN is for a user object, see Determining the DN for a user object on page 157.

   - 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 154:

- User DN for Query Authentication

  cn=Pat Brown,cn=sertech,cn=services,cn=users,dc=example,dc=com

- Base Search DN

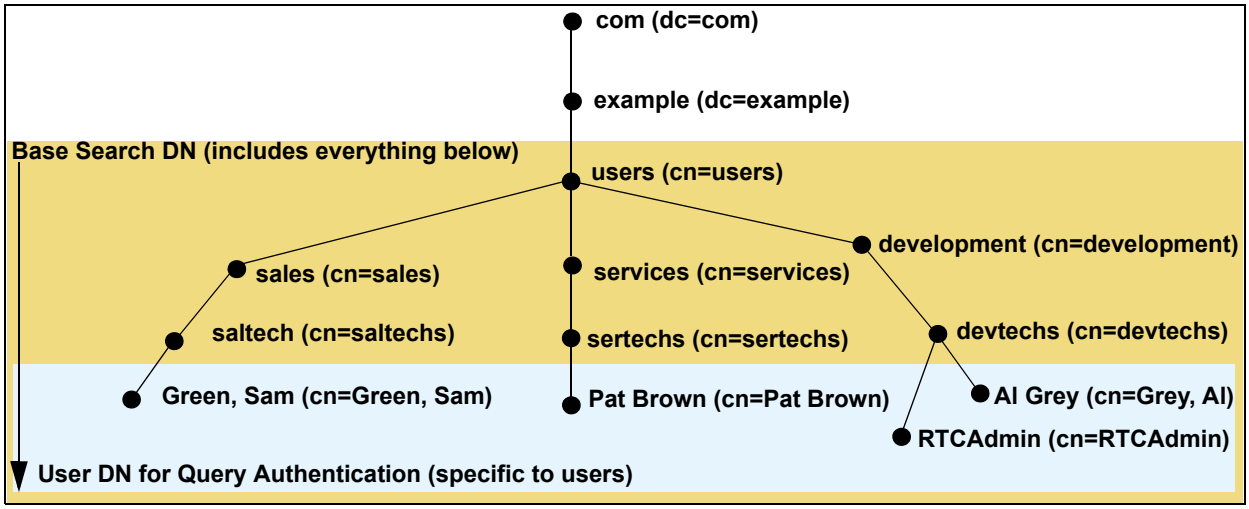
  cn=users,dc=example,dc=com

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 redisplays 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 31).
3	Enable RCC Extensions.	Follow the procedure for Enabling Remote Call Control in Active Directory on page 160 of this document. Also, see the **Tip** following this table.
4	Set up connections.	Follow the procedure for Setting up connections on page 161 of this document.
5	Set up static routes.	Follow the procedures for Configuring a static route on page 162 and Specifying the AE Server as an authorized host on page 163.
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.



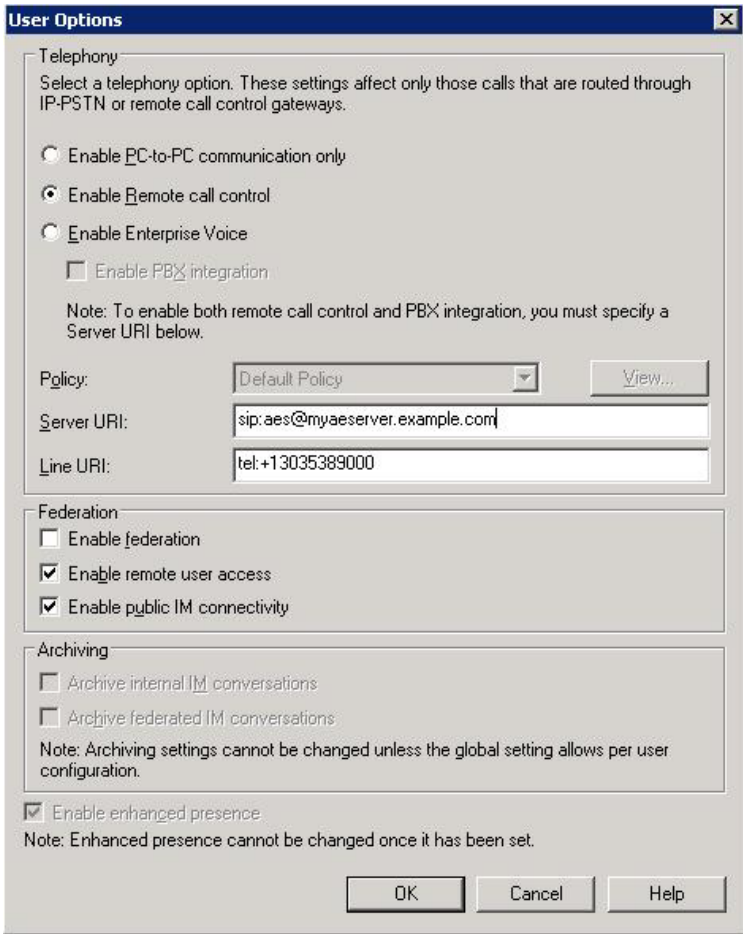
Tip:

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.



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@myaeserver.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: **mylcserver.example.com**
3. From the "mylcserver.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, **myaeserver.example.com**).
    b. In the FQDN field, type the fully qualified domain name of the AE Server (for example, **myaeserver.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 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 160) 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 or 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 168
- Using Call Forwarding and Send All Calls on page 169
- Using the Do Not Disturb feature on page 169
- Putting the active call on hold before starting a new call on page 169
- Clear Connection request on a held connection is not supported on page 169
- Bridging irregularities on page 170
- Missed Call e-mail on page 170
- Usage instructions for analog phones on page 171.

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 172
- Communicator displays numbers with trunk notation on page 173

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."

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.

- 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

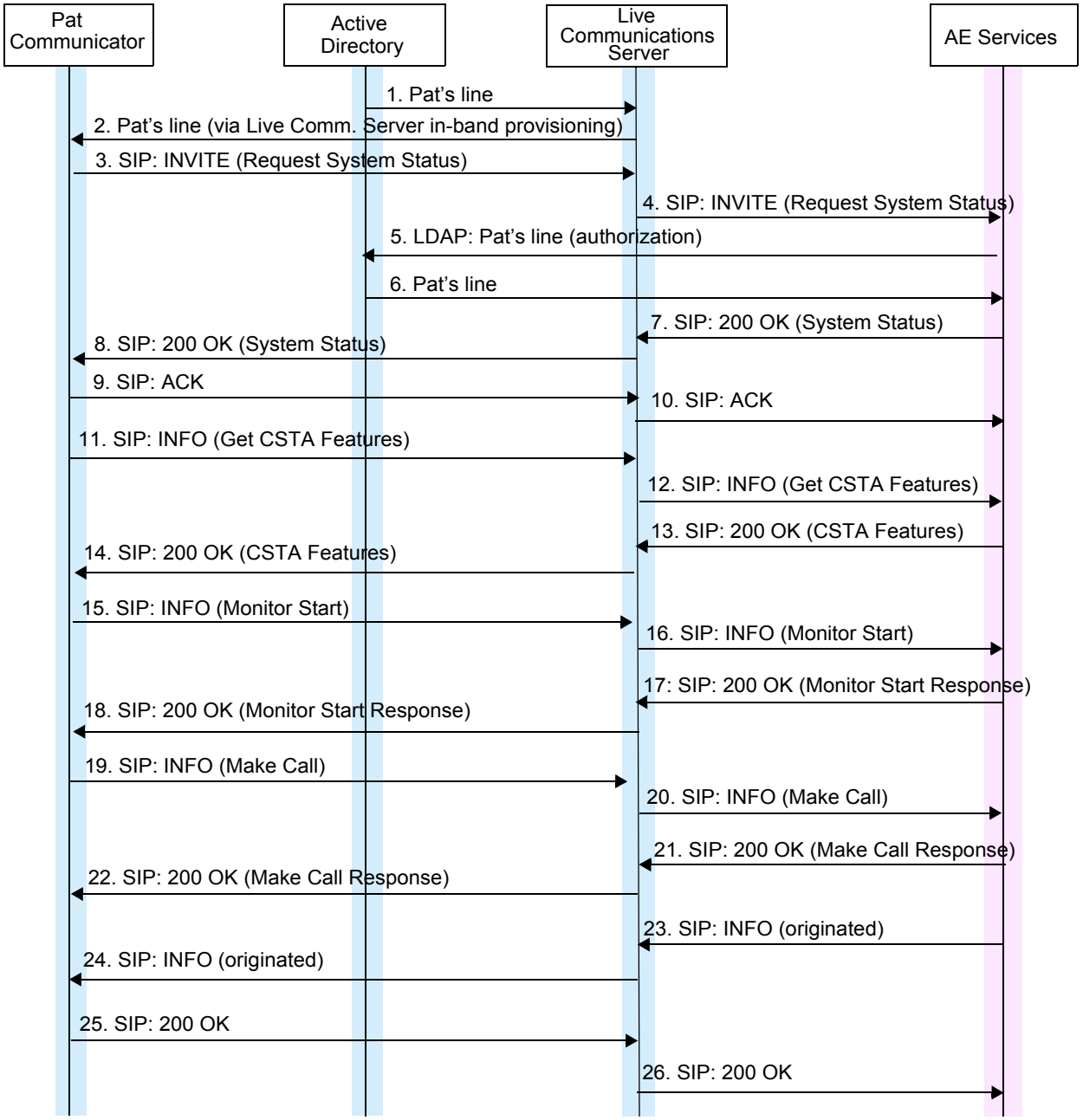
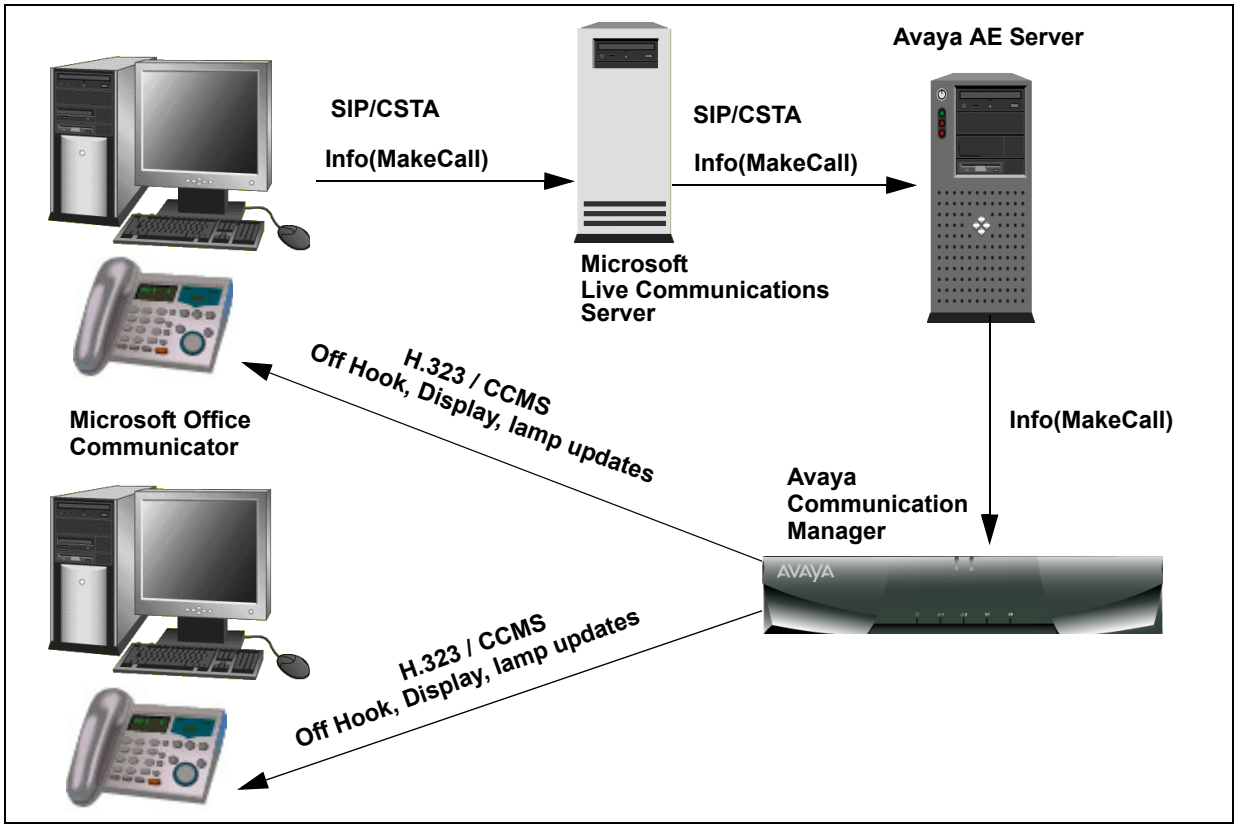


Figure 8 illustrates the Message flow for the Make Call operation in terms of a basic connectivity diagram. Other requests would follow a similar pattern.

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, 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 client user calling another Microsoft Office Communicator client user would therefore count as two calls in the BHCC measurements.

Maximum Users

The AE Services server supports a maximum of 15,000 concurrent users. If you plan to support more than 15,000 concurrent Microsoft Office Communicator clients you must use more that one AE Services server. For more information, see Figure 4: Configuring AE Services with 20,000 or more concurrent users on page 26.

Throughput

The AE Server supports six TR/87 (CSTA 3) messages per second, per 1000 users.

License Consumption

A TSAPI license is consumed for the entire duration of time that Microsoft Office Communicator is signed in with Live Communications Server.

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:

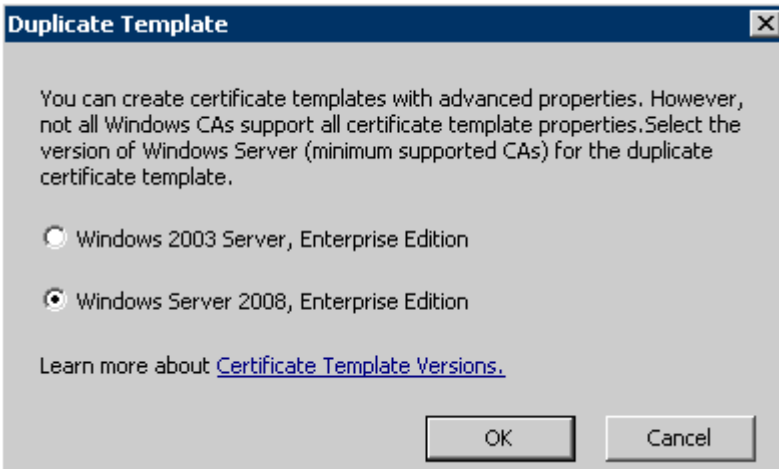
If OCS Enterprise edition is in use with an OCS server pool, the certificate should be issued in the name of the pool and must have both Server Authentication and Client Authentication. If a load balancer handles the pool, then the pool name should resolve to the load balancer's IP address. For example, 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.

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 C**ertification Authority** node, right-click on **Certificate Templates**, and select **Manage** to launch the Certificate Templates MMC snap-in.

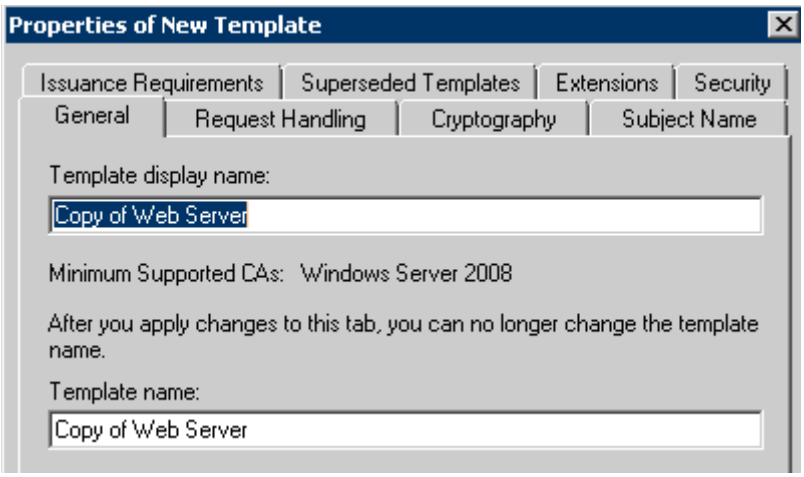
3. In the right pane of the Certificate Templates MMC snap-in, right-click on the Web Server template, and select **Duplicate Template**.

   The system displays the Duplicate Template dialog box.

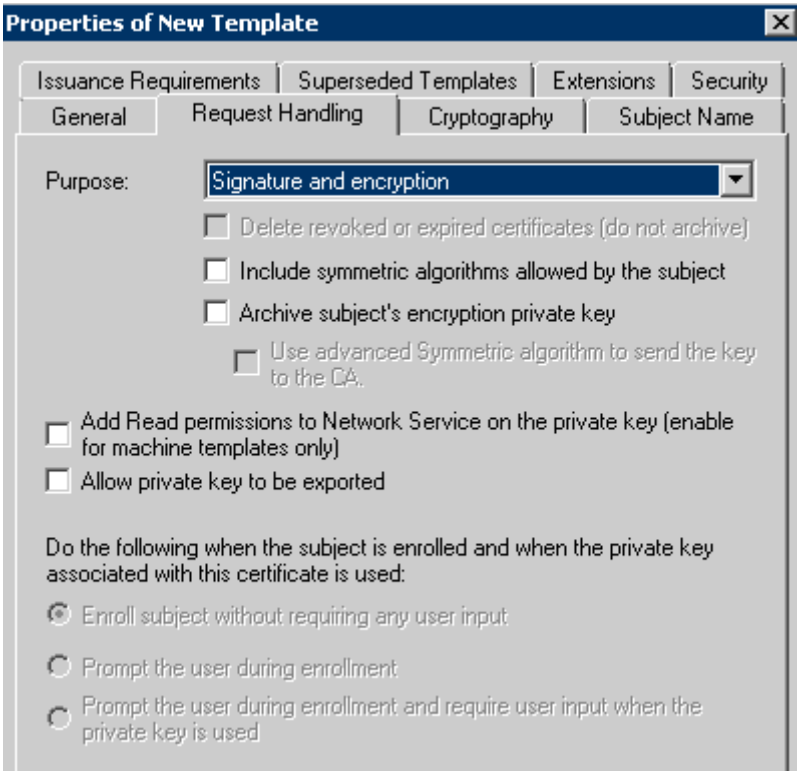


4. In the Duplicate Template dialog box, select **Windows Server 2008, Enterprise Edition**.

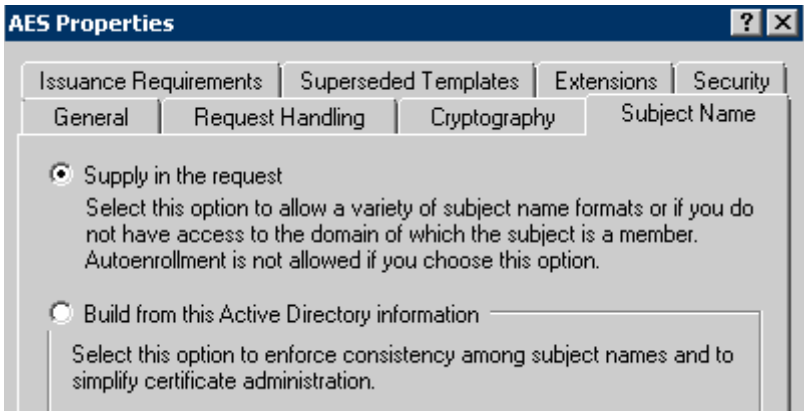
The system displays the Properties of New Template window.



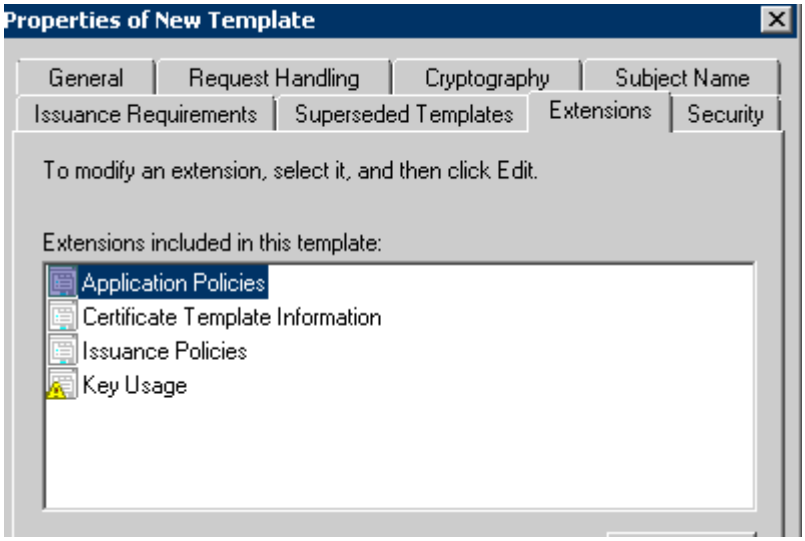
5. From the **General** tab of the Properties of New Template dialog box, in the **Template display name** field, type a descriptive name for the template.
6. In the **Properties of New Template** dialog box, select the **Request Handling** tab, and ensure that the **Purpose** selection is set to **Signature and encryption**.



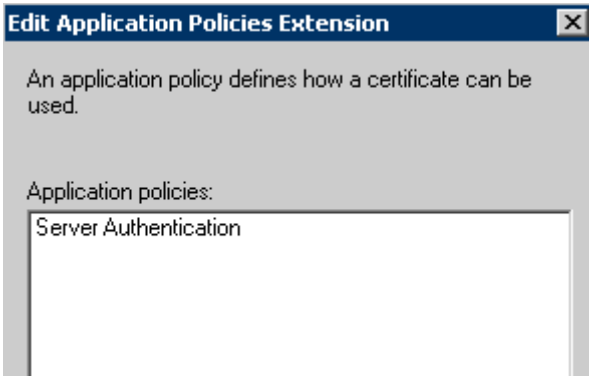
7. In the **AES Properties** dialog box, select the **Subject Name** tab, and ensure that the **Supply in the request** option is selected.



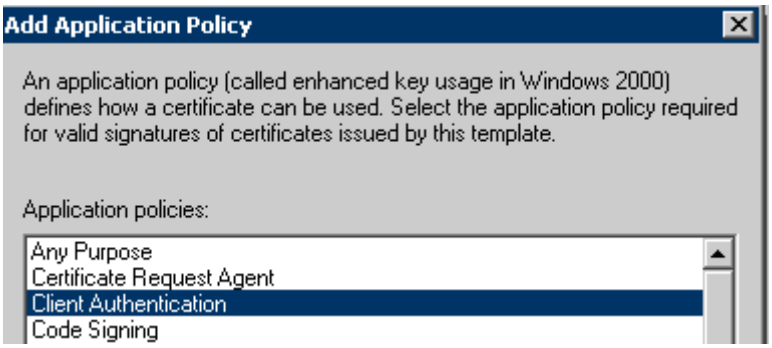
8. In the **Properties of New Template** dialog box, select the **Extensions** tab. In the **Extensions included in this template** section, select **Application Policies** and click **Edit**.



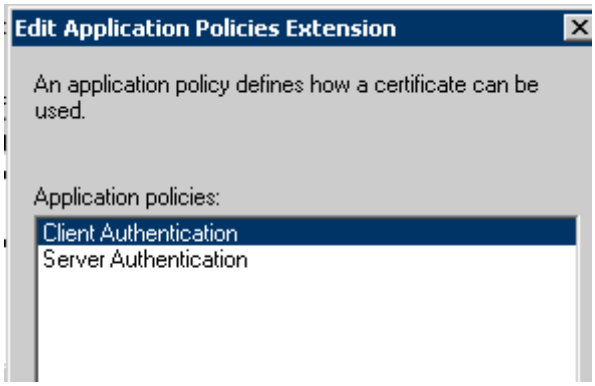
9. In the **Edit Application Policies Extension** dialog box, click **Add**.



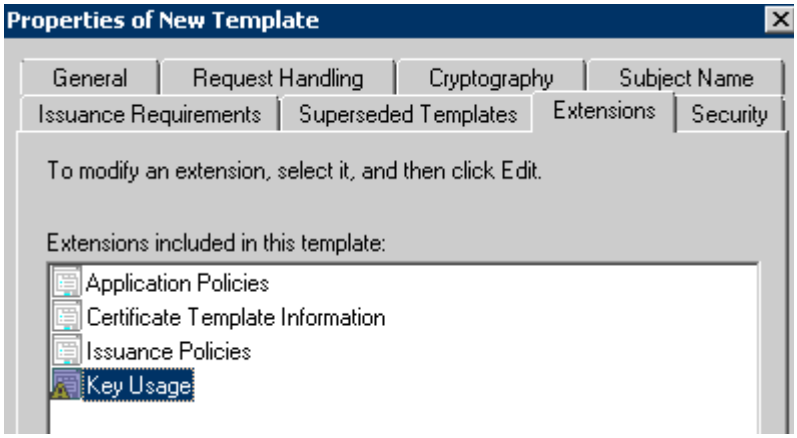
10. In the Add Application Policy dialog box, select **Client Authentication** and click **OK**.



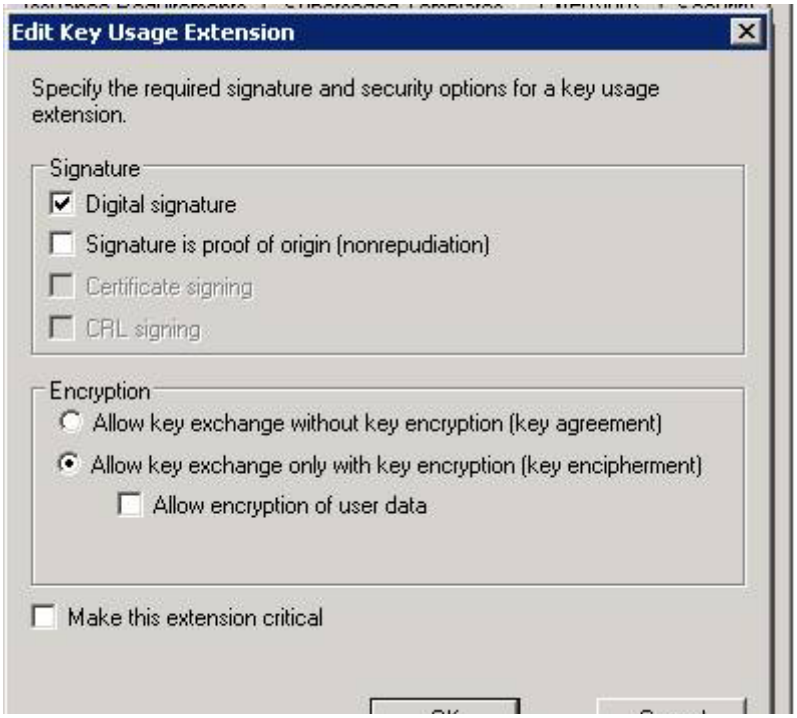
11. In the **Edit Application Policies Extension** dialog box, ensure that both **Server Authentication** and **Client Authentication** are included in the Application Policies list. Click **OK**.



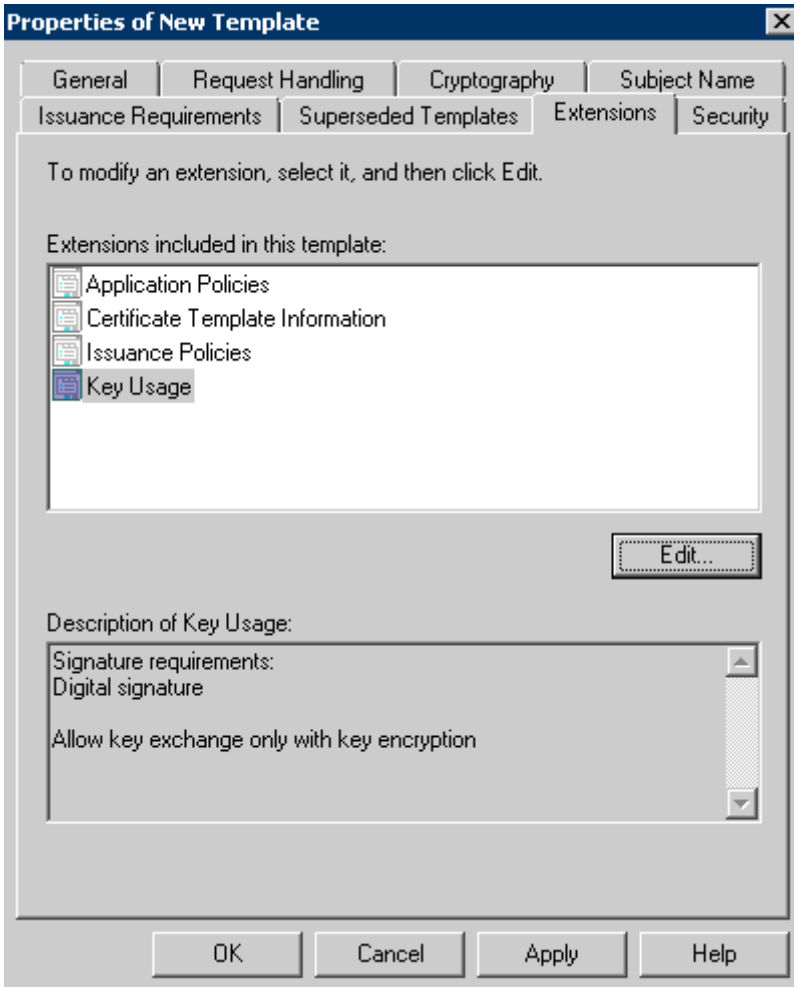
12. In the **Properties of New Template** dialog box, select the **Extensions** tab. In the **Extensions included in this template** section, select **Key Usage** and click **Edit**.



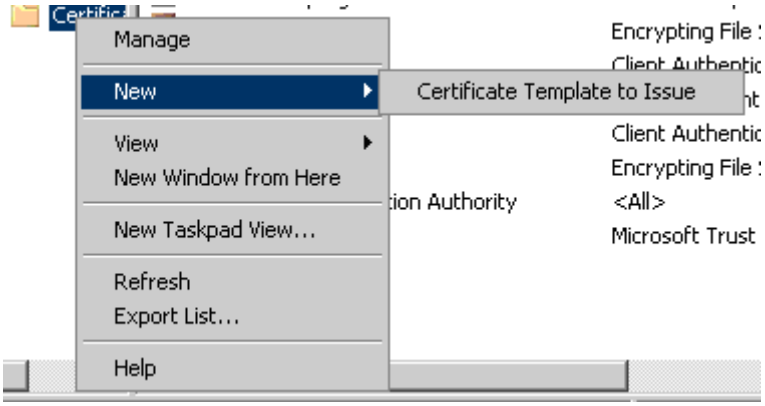
13. In the Edit Key Usage Extension dialog box, uncheck **Make this extension critical** and click on **OK**.



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 188)

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

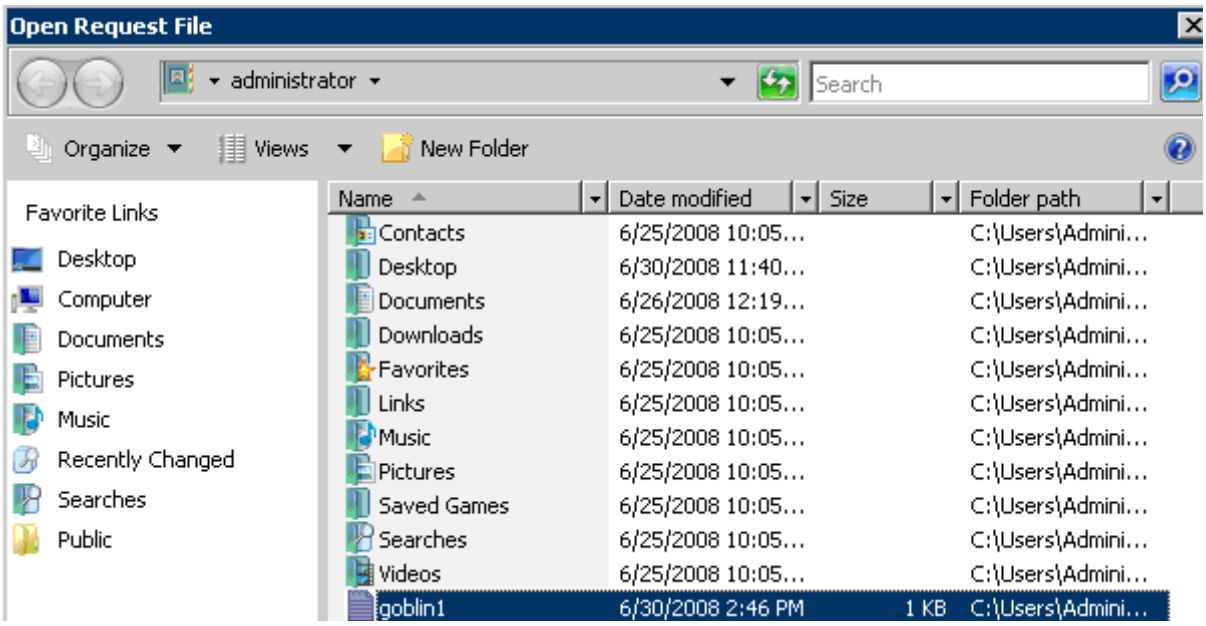
      For example:

      CN=msavaes1.sitlms.net,OU=SITL,O=Avaya,L=Lincroft,S=New Jersey,C=US

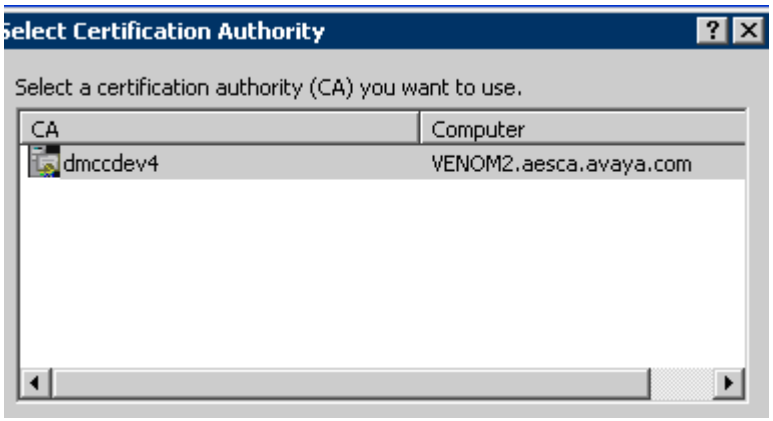
   e. Leave the other fields at the defaults, and click **Apply.**
5. From the main menu of the AE Services management console, select **Security** > **Certificate Management** > **Server Certificates** > **Pending Requests**.
6. From the Pending Server Certificates Request page, select the certificate, 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**.

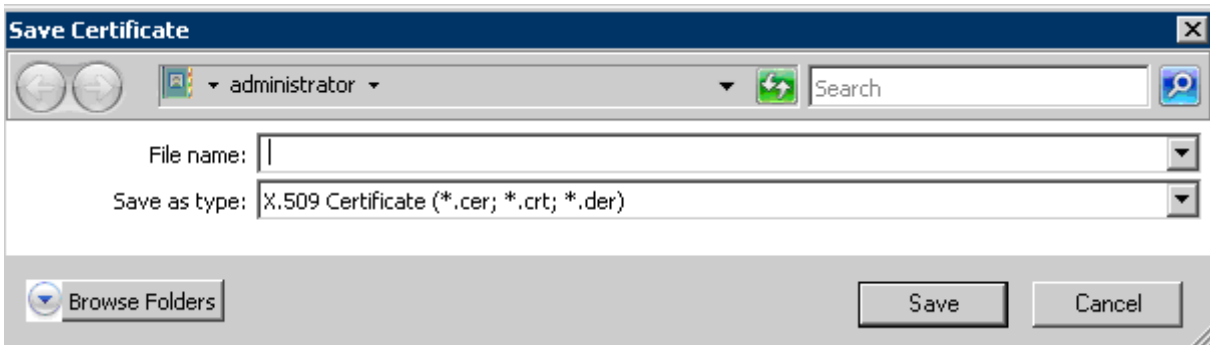
12. From the Open Request File window, select the file you created previously, for example, **goblin1**.



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.

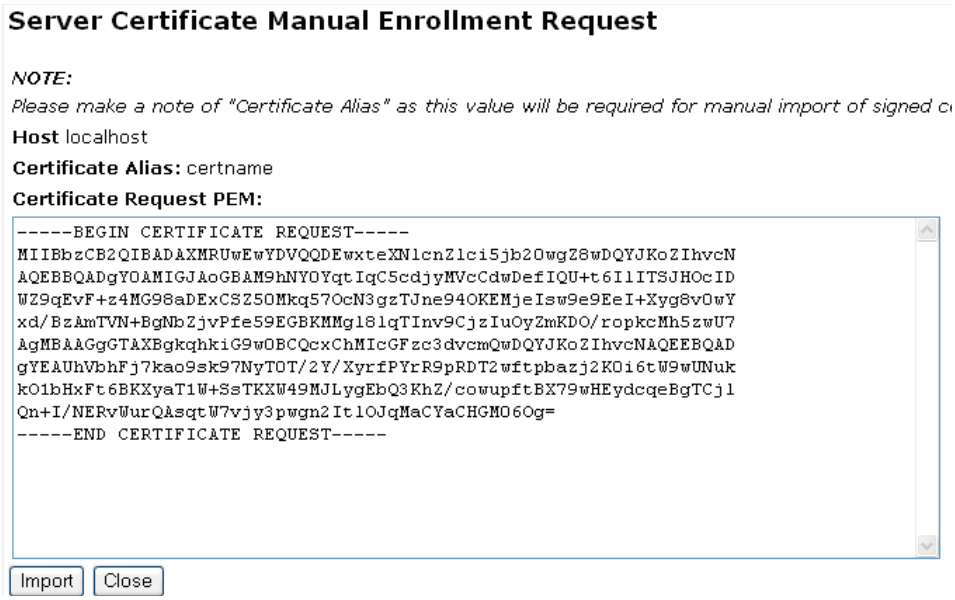


15. In the Save Certificate window, type the file name, for example **goblin1.cer**, and click **Save** to save the file to your local machine.

16. From the main menu of the Avaya AE Services Management Console, click **Security** > **Certificate Management** > **Server Certificate** > **Pending Requests**.



17. From the Pending Requests Certificate Requests page, select the alias for the certificate request created in 4a (**aeservices**) and click **Manual Enroll**.



18. From the Server Certificate Manual Enrollment Request page, click on **Import**.

    Your browser displays the Server Certificate Import page.



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).

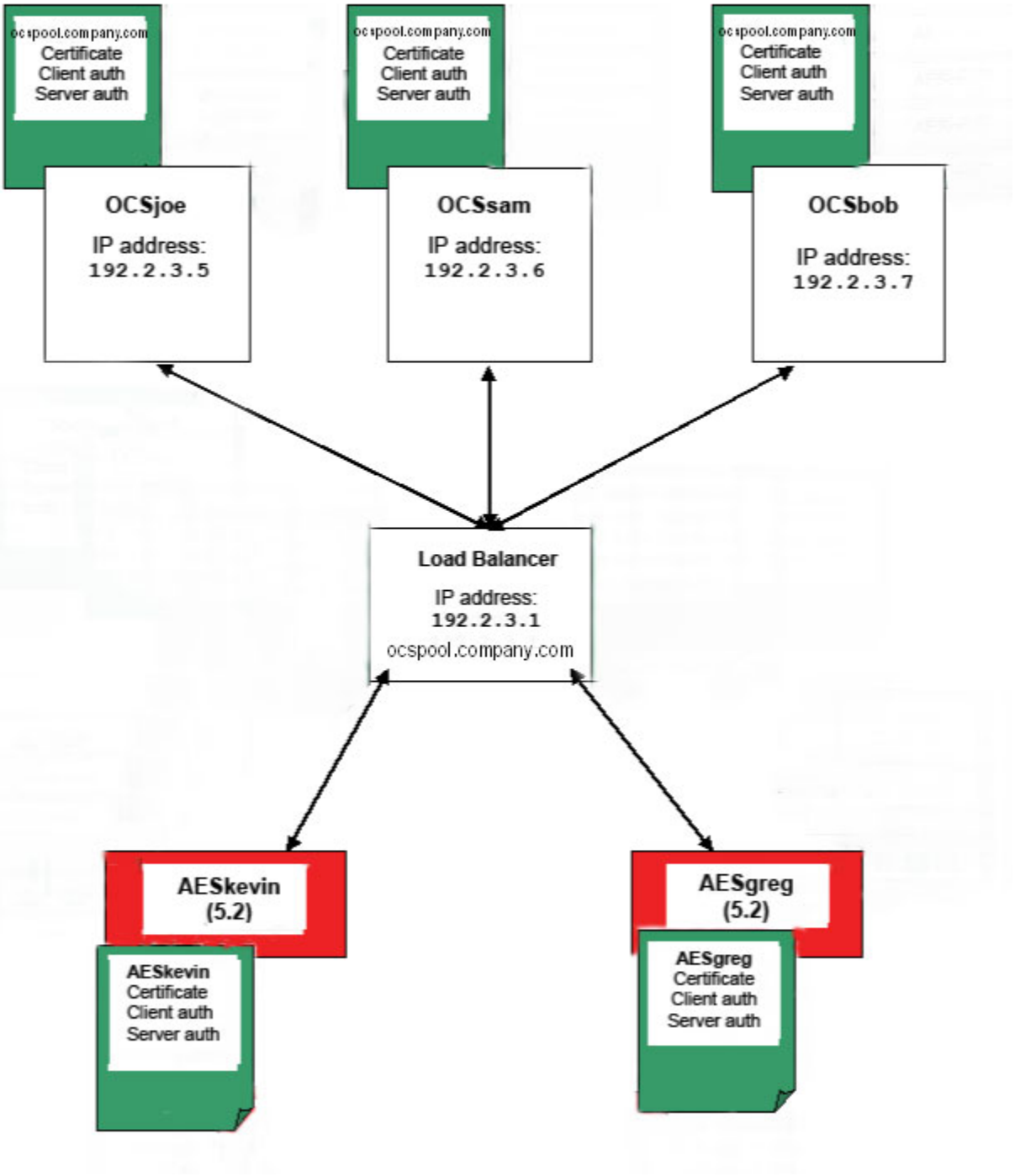
    b. Ensure that the Establish Chain of Trust checkbox is checked.

    c. Load the file saved in Step 15; for example, **goblin1.cer**.

    d. Click **Apply**.

    If the import is successful, your browser redisplays 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 3: 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 . . . 33
- requirement for AE Services - Live Communications Server integration . . . 23
- setting up . . . 33

AE Services administrative workstation, requirement . 24
AE Services associations capacity . . . 181
AE Services Server 4.0, integration requirement . . . 24
Asterisk
- when interpreted as a literal . . . 75, 140

Asterisk, when treated as a wildcard . . . 76, 141
Authentication of client and server . . . 48, 115
Automatic routing, configuring certificate for . . . 56, 123

B

Bundled Server installation checklist . . . 36, 38

C

Call flow (message flow) diagram . . . 178
Call flow, TR/87 . . . 177
capacities
- AE Services associations . . . 181
- busy hour call completion (BHCC) . . . 181
- license consumption . . . 181
- maximum concurrent users . . . 181
- throughput . . . 181

Certificate administration
- configuring certificate for automatic routing (Live Communications Server) . . . 56, 123
- importing the trusted certificate into AE Services 62, 127
- installing Microsoft-based certificate on Live Communications Server . . . 54, 121
- installing the trusted certificate on AE Server . 58, 124
- summary of sample scenario . . . 47, 114
- verifying installation of entire certificate chain in AE Services . . . 63, 128
- verifying installation of server certificate for Live Communications Server . . . 56, 122

Certificate authority, integration requirement . . . 23
Certificate management
- converting certificates from other formats . . . 64, 129
- importing the server certificate into AE Services 69, 134
- installing a trusted certificate chain on AE Server 61, 126

Certificate management scenario, explanation of . 48, 115
Certificate management, Microsoft-based procedure for creating a server certificate for AE Services . . . 68, 133
Checklist
- Bundled Server installation . . . 36, 38
- Software-Only server installation . . . 40

Checklist for Live Communications Server, phase 1 . . 30
Communication Manager, integration requirement . . 23
Configuring AE Services with 5,000 or more concurrent users, diagram . . . 26
Configuring AE Services, summary . . . 46, 112
Converting a DER file to PEM . . . 64, 129

D

Dial plan administration in AE Services
- per-switch settings . . . 87, 151
- summary . . . 71, 136
- using defaults . . . 89, 153

Dial string characters . . . 75, 140
Distinguished Name (DN) entries and scope of search 92, 156

E

EC500 with XMOBILE, and bridging irregularities 105, 170
Error codes and SIP requests . . . 175

F

FQDN (fully qualified domain name) of pool . . . 54
From TelURI and To TelURI rules . . . 73, 138
From TelURI settings . . . 74, 81, 139, 145

H

High availability configuration . . . 27

I

Information Technology (IT) technician, bundled server installation . . . 40
Integration checklist for AE Services and Live Communications Server (Phase 3) . . . 43, 109
ISDN trunk administration in Communication Manager 108, 173

K

Known Issues
Microsoft Office Communicator displays numbers with trunk notation . . . 108, 173
unidentified caller in Microsoft Office Communicator window . . . 107, 172
Known issues
Clear Connection request on a held connection not supported . . . 104, 169
missed call e-mail . . . 105, 170
putting active call on hold before starting new call . 104
setting up forwarding off-switch . . . 103, 168
using the Call Forwarding or Send All Calls features 104, 169
using the Do Not Disturb feature . 102, 104, 167, 169

L

license consumption . . . 181
License, Unified CC API Desktop Edition . . . 24
Live Communications Server
installing server certificate . . . 53, 120
installing trusted certificate . . . 49, 116
specifying AE Server as authorized host . . . 98, 163

M

Make call, call flow diagram . . . 180
maximum concurrent users supported by AE Services 181
Maximum number of Communication Manager Servers supported, diagram . . . 25
Microsoft Office Communicator
configuring a static route . . . 97, 162
group policy settings . . . 99, 164

N

Normalizing phone numbers, Address Book . . . 33

O

OID (Object Identifier Field), how to complete . . . 54

P

Phase 1 -- Setting up the Live Communications Server environment . . . 28
Phase 1 checklist -- Live Communications Server . . 30
Phase 2 -- Setting up AE Services and Communication Manager . . . 34
Phase 3 -- Integrating AE Services with Live Communications Server . . . 41
Phase 3 Checklist -- integrating AE Services and Live Communications Server . . . 43, 109
Phone Normalization Script . . . 94, 159
Procedure 1 - certificate management
if installing trusted certificate from another vendor 49, 116
importing certificate into trust store . . . 51, 118
installing trusted certificate from Microsoft Certificate Services . . . 50, 117
installing trusted certificate on Live Communications Server . . . 49, 116
Procedure 1a - verifying installation of trusted certificate on Live Communications Server . . . 52, 119
Procedure 2 - installing server certificate for Live Communications Server . . . 53, 120
Procedure 2a - Verifying the installation of the server certificate for . . . 56, 122
Procedure 3 - Installing the trusted certificate on the AE Server . . . 58, 124
Procedure 3a - Verifying the installation of the trusted certificate . . . 63, 128
Procedure 4 - Creating a server certificate request for AE Services . . . 65, 130
Procedure 5 - Creating a server certificate for AE Services 67, 132
Procedure 6 - Importing the server certificate into AE Services OAM . . . 69, 134
Procedure 6a - Verifying the installation of the server certificate in AE Services . . . 70, 135

R

Recovering from a system outage . . . 102, 167
Remote Call Control (RCC) extensions, enabling . 94, 158
Remote Call Control SIP URI field . . . 96, 161
Replacing an expired server certificate . . . 70, 135
Requirements for AE Services - Live Communications Server integration . . . 23

S

Service Pack 12866, Communication Manager . 107, 172
SIP requests and error codes . . . 175
SIP requirements . . . 21, 24
SIP URI field . . . 96, 161
Software-Only server, installation checklist . . . 40
static route . . . 97, 162

T

Tel URI format, example . . . 95, 161
Tel URI formats and device IDs . . . 72, 137
To TelURI settings . . . 76, 80, 83, 141, 144, 147
TR/87 port in OAM, enabling . . . 46, 113
TR/87, defined . . . 14
Trust store, Live Communications Server . . . 51, 118