Avaya Aura® Application Enablement Services Overview and Specification

Release 6.3
Issue 3
May 2015

© 2015, Avaya Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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 you. “Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “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. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, 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 Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than an Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order 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). You 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 Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Copyright

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

written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

Avaya Aura is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 7
- Purpose 7
- Intended audience 7
- Document changes since last issue 7
- Related resources 7
  - Documentation 7
  - Training 9
  - Viewing Avaya Mentor videos 10
- Support 10
- Warranty 11

Chapter 2: Overview 12
- Avaya Aura® Application Enablement Services overview 12
- AE Services offers 12

Chapter 3: What's new in Application Enablement Services 14
- New in AE Services 6.3.3 14
  - VMware enhancement 14
  - Virtual IP Address for Geographic Redundancy High Availability 14
  - Improved support for contact center events 15
  - Improved consistency between station call logs and CTI applications 16
  - Support for Avaya Aura® Communication Manager 6.3.6 16
- New in AE Services 6.3.1 17
  - Geo Redundant High Availability 17
  - Virtualized Environment Footprint Flexibility 18
  - Endpoint registration enhancements 18
  - Support for the Avaya Common Server – Dell PowerEdge R620 server 19
  - Support for the Avaya Access Security Gateway (ASG) 19
  - Support for Avaya Aura® Communication Manager 6.3.2 20
  - Support for the Microsoft Lync Server 2013 20
- New in AE Services 6.3 20
  - ASAI enhancements 20
  - Enhancements for Agile Communication Environment™ and Avaya Aura® Contact Center 22
  - DMCC enhancements 23
  - Security enhancements 23
  - Support for Avaya Communication Manager 6.3.2 24
  - AE Services Management Console enhancements 24
  - Command enhancements for the AE Services on System Platform offer 25
  - Support for Microsoft Windows 8 26

Chapter 4: AE Services Product Summary 27
- Introduction 27

DMCC service ... 27
TSAPI service ... 28
Web services ... 28
CVLAN service ... 29
DLG service ... 29
AE Services configuration at a glance ... 30
Chapter 5: Network Security and Reliability ... 31
AE Services security features ... 31
Secure application links ... 32
AE Services link resiliency and failover ... 32
Support for an Enterprise Survivable Server configuration ... 33
Chapter 6: Guidelines and requirements for configuring AE Services ... 35
Configurations that use AEP connections ... 36
Chapter 7: AE Services Architecture ... 37
AE Services architecture at a glance ... 37
AE Services integration for IBM Lotus Sametime ... 38
AE Services integration with Microsoft Office Communication Servers and Microsoft Lync Servers ... 39
Chapter 8: Session Initiation Protocol (SIP) ... 41
SIP support ... 41
SIP limitations ... 41
Chapter 9: AE Services Licensing ... 43
AE Services licensing summary ... 43
Application Enablement Protocol connections licensing ... 45
AE Services integration for Microsoft Office Communications Server and Microsoft Lync Server licensing ... 46
AE Services integration for IBM Lotus Sametime licensing ... 46
Device, Media, and Call Control (DMCC) licensing ... 46
Web services licensing ... 47
System Management Service (SMS) licensing ... 47
TSAPI service (including JTAPI) licensing ... 48
TSAPI basic user license ... 48
TSAPI advanced license ... 49
CVLAN licensing ... 49
DLG licensing ... 50
Enterprise-wide licensing ... 50
Comparison of standard licensing and enterprise-wide licensing ... 50
Licensing configuration examples ... 51
Standard licensing ... 51
Enterprise-wide licensing — allocating licenses or features ... 52
Enterprise-wide licensing — pointing to a master license on a remote server ... 53
Additional documents ... 54
Chapter 10: Application Enablement Services Client and SDKs ... 55

Chapter 11: Communication Manager features not supported 56
Chapter 12: Capacities for AE Services 58
AE Services integration for Microsoft Office Communication Server 58
AE Services integration for IBM Sametime 59
Capacities for calls in DMCC applications 59
Additional AE Services Restrictions 63
Communication Manager capacities for DMCC 63
Additional Communication Manager restrictions 64
System Management Services capacities 65
System capacities – Communication Manager 65
System capacities – AE Services server 6.3.3 65
ASAI associations 66
CVLAN service capacities 66
DLG service capacities 67
TSAPI service capacities 67
Chapter 13: AE Services Documentation 68
Select documents based on products you use 68
Guidelines for selecting documents based on your role within an organization 68
Planners 68
Installers and administrators — Application Enablement Services on System Platform 70
Installers and administrators — Bundled Server offer 70
Installers and administrators — Software-Only offer 70
Application developers 71
Appendix A: AE Services Release 6.3.3 compatibility 75
API and client compatibility 75
AE Services compatibility with Communication Manager 76
AE Services compatibility with Communication Manager 6.3 CTI interfaces 77
Communication Manager 6.3 - ASAI capabilities 77

Chapter 1: Introduction

Purpose

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

Intended audience

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

Document changes since last issue

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

- Added new feature descriptions for the Avaya Aura® Application Enablement Services 6.3.3 release to the New in AE Services 6.3.3 section on page 17.
- Added additional restrictions for AE Services in Additional AE Services Restrictions on page 63.
- Added additional restrictions fir Communication Manager in Additional Communication Manager Restrictions on page 64.

Related resources

Documentation

The following table lists the related documents for Avaya Aura® Application Enablement Services. Most of the documents listed are Release 6.3.3. Those listed that are for earlier releases have not

required an update and remain compatible with AE Services 6.3.3. Obtain the related documents and documents about other Avaya products mentioned in this guide from the Avaya Support website: Avaya support site.

	Document title	Number	Release
1	*Avaya Application Enablement Services Overview and Specification*	02-300360	6.3.3
2	*Implementing Avaya Application Enablement Services on Avaya Aura® System Platform*	02–603468	6.3.3
3	*Implementing Avaya Application Enablement Services in a Software-Only Environment*	02-300355	6.3.3
4	*Implementing Avaya Application Enablement Services for a Bundled Server Upgrade*	02-300356	6.3.3
5	*Avaya Application Enablement Services using VMware® in the Avaya Aura® Virtualized Environment Deployment Guide*	Not applicable	6.3.3
6	*Avaya Application Enablement Services Administration and Maintenance Guide*	02-300357	6.3.3
7	*Avaya Application Enablement Services Implementation Guide for Microsoft® Live Communications Server 2005, Microsoft Office Communications Server 2007, and Microsoft Lync® Server 2010 and 2013*	02-601893	6.3.3
8	*Avaya Application Enablement Services Integration Guide for IBM Lotus Sametime*	02-602818	6.3
9	*Avaya Application Enablement Services Online Help* (packaged with Application Enablement Services software and not available on the Web)	Not applicable	6.3.3
10	*Avaya Application Enablement Services TSAPI Exerciser Help* (Online, packaged with the AE Services TSAPI Client SDK software and not available on the Web)	Not applicable	6.3.3
11	*Avaya Application Enablement Services Web Services Programmer's Guide*	02-300362	5.2
12	*Avaya Application Enablement Services Device, Media and Call Control API .NET Programmer's Guide*	02-602658	6.3.3
13	*Avaya Application Enablement Services Device, Media, and Call Control .NET Programmer's Reference* (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)	Not applicable	6.3.3
14	*Avaya Application Enablement Services Device, Media, and Call Control XML Programmer's Guide*	02-300358	6.3.3
15	*Avaya Application Enablement Services Device, Media, and Call Control XML Programmer 's Reference* (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)	Not applicable	6.3.3

Table continues…

	Document title	Number	Release
16	*Avaya Application Enablement Services Device, Media, and Call Control Java Programmer 's Guide*	02-300359	6.3.3
17	*Avaya Application Enablement Services Device, Media, and Call Control Java Programmer's Reference* (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)	Not applicable	6.3.3
18	*Avaya Application Enablement Services Device, Media, and Call Control Media Stack API Reference* (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)	Not applicable	6.3.3
19	*Avaya Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide*	02-300543	6.3.3
20	*Avaya Application Enablement Services TSAPI for Avaya Communication Manager Programmer's Reference*	02-300544	6.3.3
21	*Avaya Application Enablement Services TSAPI Programmer's Reference*	02-300545	4.1
22	*Avaya Application Enablement Services CVLAN Programmer's Reference*	02-300546	4.1
23	*Avaya Application Enablement Services JTAPI Programmer's Guide*	02–603488	5.2
24	*Avaya Application Enablement Services JTAPI Programmer's Reference* (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)	Not applicable	5.2
25	*Avaya Application Enablement Services ASAI Technical Reference*	03-300549	4.1
26	*Avaya Application Enablement Services ASAI Protocol Reference*	03-300550	3.1

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title
ATI02595AEN	Application Enablement Services Implementation and Administration (Assessment)
AVA00962WEN	Application Enablement Services 4.0 Overview
1U00223O	Avaya Aura Application Enablement Services (AES) 6.2 - L2
1U00222O	Avaya Aura Application Enablement Services (AES) 6.2 - L1
3U00127O	Designing Avaya Aura Application Enablement Services (AES) - Technical Sales L1

Table continues…

Course code	Course title
10U00030E	Knowledge Access: AIPS - Avaya Aura Application Enablement Services Implementation
4100	Avaya Aura(R) Application Enablement Services Implementation Test
9Z04481V	Application Enablement Services

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support site, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

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

Warranty

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

Chapter 2: Overview

Avaya Aura® Application Enablement Services overview

Avaya Aura® Application Enablement Services (AE Services) is a software platform that leverages the capabilities of Avaya Aura® Communication Manager. AE Services provides an enhanced set of Application Programming Interfaces (APIs), protocols, and web services that expose the functionality of Avaya Communication solutions to corporate application developers, third-party independent software vendors, and system integrators.

Note:

AE Services supports existing Communication Manager standalone implementations and Avaya Aura® Session Manager configurations with Communication Manager as an Access Server. AE Services does not support Communication Manager as a Feature Server.

AE Services runs on a Linux server and is tightly integrated with Communication Manager and Avaya Contact Center solutions. AE Services provides an open platform for supporting existing applications and serves as a catalyst for creating the next generation of applications and business solutions.

For information about new features for Release 6.3.3, see What's new in Application Enablement Services on page 14. AE Services 6.3.3 is backward compatible with previous releases of Communication Manager, going back to Release 6.0.x. For more information about feature compatibility, see AE Services Release 6.3.3 compatibility on page 75. To learn more about Avaya Aura® contact your Avaya client executive or authorized business partner. Also visit the Avaya Support Web site http://www.avaya.com/support.

AE Services offers

AE Services Release 6.3.3 provides the following product offers.

Avaya Application Enablement Services on Avaya Aura® System Platform

This offer was introduced in Release 5.2. Also referred to as Application Enablement Services on System Platform or AE Services on System Platform, this offer includes a hardware platform (Avaya Common Server – Dell™ R620, HP DL360 G7, or Dell™ R610), operating system (Red Hat Enterprise Linux 5), the Avaya Aura® System Platform software (System Platform Release 6.3.4), the AE Services Release 6.3.3 software, and a maintenance contract with Avaya. Customers who want to take advantage of the Application Enablement Services on System Platform High Availability

Failover feature must obtain this offer. For information about the High Availability Failover feature, see *Implementing Avaya Application Enablement Services on Avaya Aura® System Platform* Release 6.3.4.

Avaya Application Enablement Services Bundled Server

This offer does not include hardware. It is software for customers with an existing Bundled Server S8510 hardware platform who want to install or upgrade to AE Services Release 6.3.3. The High Availability Failover feature is not available with the Bundled Server offer.

Avaya Application Enablement Services Software-Only

This offer is available for customers who want to install AE Services on a computer that meets or exceeds the minimum server requirements for AE Services. The High Availability Failover feature is not available with the Software-Only offer.

Avaya Application Enablement Services using VMware® in the Avaya Aura® Virtualized Environment

This offer was introduced in Release 6.2 and deploys the Avaya Aura® Application Enablement Services virtual application in the Avaya Aura® Virtualized Environment. This offer consists of the AE Services template enabled for VMware, which includes the AE Services 6.3.3 software with the Red Hat Enterprise Linux 5.10 operating system running as a virtual machine on a system running the VMware vSphere version 5.5 virtualization platform.

Chapter 3: What's new in Application Enablement Services

This chapter presents an overview of the new features and enhancements for Avaya Application Enablement Services (AE Services).

New in AE Services 6.3.3

VMware enhancement

AE Services 6.3.3 adds the following for VMware:

- Support for the AE Services vApplication for VMware version 5.5.
- Support for the AE Services Geographic Redundancy High Availability (GRHA) feature on VMware.

For more information about GRHA, see *Avaya Aura® Application Enablement Services Administration and Maintenance*.

Related links

What's new in Application Enablement Services on page 14

Virtual IP Address for Geographic Redundancy High Availability

Earlier, AE Services 5.2 supported Fast Reboot High Availability (FRHA) and AE Services 6.2 supported Machine Preserving High Availability (MPHA).

AE Services 6.3.3 supports Geographic Redundancy High Availability (GRHA). With GRHA the limitations of cross over cables and dependence on System Platform is removed and the only prerequisite is the quality of the LAN or WAN between the data centres. AE Services 6.3.3 offers two options of GRHA:

- System Platform deployment with AES MPHA at one or both sites if preferred or otherwise a non HA AES
- VMware deployment

Earlier, the client application used two different IP addresses - one IP to connect to the primary AE Services GRHA server and another IP to connect to the secondary AE Services GRHA server. The client application was responsible to determine which AE Services GRHA server was active, and to connect to the active server using the appropriate IP address.

With AE Services 6.3.3, the client application uses one IP address to connect to either of the AE Services GRHA servers. If the primary AE Services GRHA server stops working, the virtual IP address is automatically assigned to the secondary AE Services GRHA server. You can configure the virtual IP address from the **High Availability Configuration** page in the **Eth0 Virtual IP Address** field.

The use of the virtual IP address has significant advantages:

- The client application can use the same IP address to connect to the active AE Services GRHA server. The client application does not have to maintain two different AE Services server IP addresses.
- If the virtual IP address is also used for the Switch Connectivity and Media Connectivity, any Device Media Call Control (DMCC) associations that are currently in place at the time of a GRHA fail-over will be automatically recovered by the new active AE Services server. The associations include: DMCC client sessions, DMCC devices and device monitors, DMCC station registrations, DMCC call associations, and DMCC system registrations.

Note:

For GRHA, the active and standby servers are synchronized every minute. Thus, if there is an unplanned fail-over, any new associations or other changes made within the last minute may not be synchronized. In that case, these last-minute changes will not be recovered by the new active server.

For more information about Virtual IP Address for Geographic Redundancy High Availability, see *Avaya Aura® Application Enablement Services Administration and Maintenance*.

Related links

What's new in Application Enablement Services on page 14

Improved support for contact center events

In AE Services 6.3.3 and ASAI Link release 7, the number of digits in the address of the Calling Party Number and the Connected Number is increased to 21. The number of digits for ASAI Link release 1 to 6 is still limited from 1 to 15 digits.

With this enhancement, the maximum limit the **Minimum Length** field, **Maximum Length** field, **Delete Length** field on Add Dial Plan-default page and Add Dial Plan – Switch Administration page is increased to 21 digits.

For more information about Add Dial Plan-default page and Add Dial Plan – Switch Administration page, see *Avaya Aura® Application Enablement Services Administration and Maintenance*.

Related links

What's new in Application Enablement Services on page 14

Improved consistency between station call logs and CTI applications

In AE Services 6.3.3 and later, with the combination of Avaya Aura® Feature Pack 4 and ASAI Link version 7, the ASAI Call Redirected event, the ASAI Busy/Unavailable event, and the Reorder/ Denial event now include the optional information elements mentioned in the table.

Element	Description
Calling Party Number IE	The extension number of the calling party
Redirecting Number IE	The extension number of the station from which the call is redirected
Redirection Number IE	The extension number to which the call is redirected
Cause IE	The reason why the call is redirected
Party ID IE	The party ID of the calling party

AE Services 6.3.3 with the support of ASAI Link Version 7 or later provides the following enhancements for CTI events.

- CVLAN enhancement: The CVLAN client library supports new optional IE values added to the ASAI Redirected event report event.
- TSAPI enhancement: The TSAPI Link supports the new optional IE values added in the ASAI Call Redirected event reports. The system uses the IE values to set CSTA Diverted event parameter values. The TSAPI service and TSAPI clients support a new private data version 12. The ATT Diverted Event now includes number of the calling party.
- JTAPI enhancement: The JTAPI Service negotiates private data version 4-12 when connecting to TSAPI Service Link administered with ASAI Link Version 7 or later. When the CSTA Diverted event from the TSAPI Service sends the confirmation, the JTAPI middleware converts the CSTA Diverted event into the equivalent JTAPI LucentV12DivertedEvent.
- DMCC enhancement: The DMCC Call Control Service negotiates private data version 12 while connecting to TSAPI or JTAPI administered with ASAI Link Version 7 or later. When the CSTA-1 Diverted event from the TSAPI Service sends the confirmation, the DMCC service converts the CSTA-1 Diverted event into the equivalent CSTA-3 Diverted event. The DMCC service forwards the CSTA-3 Diverted event to the appropriate DMCC clients.

For more information about TSAPI links, see *Avaya Aura® Application Enablement Services Administration and Maintenance*.

Related links

What's new in Application Enablement Services on page 14

Support for Avaya Aura® Communication Manager 6.3.6

For the latest and most accurate compatibility information, go to http://support.avaya.com/CompatibilityMatrix/Index.aspx..

Related links

What's new in Application Enablement Services on page 14

New in AE Services 6.3.1

Geo Redundant High Availability

AE Services 6.3.1 with Avaya Aura® Contact Center 6.4 introduces the Geo Redundant High Availability feature, which is a high availability solution that works across two data centers with a pair of servers connected over a routable network. When the standby AE Services server is activated, AE Services will start providing service approximately a minute after the connectivity failure to the active server was detected. Geo Redundant High Availability is not state preserving. As a result, only the configuration data is copied from the active AE Services server to the standby server.

Using the AE Services Management Console, you can

- administer the preferred node. If a preferred node is administered, that node will become active when connectivity between the two data centers is reestablished. If a preferred node is not administered, the current active AE Services server remains active.
- manually start and stop Geo Redundant High Availability
- synchronize the active and standby servers

  Note:

  Data synchronization occurs automatically every two minutes.
- manually switch to the standby server (interchange)
- suspend and unsuspend Geo Redundant High Availability
- ping targets to gauge the health of the network and determine which AE Services server should be active

Three levels of licensing are available for Geo Redundant High Availability:

- Small
- Medium
- Large

Note:

Geo Redundant High Availability is only supported on the AE Services 6.3.1 on System Platform 6.3.1 offer. The AE Services server in each data center must be protected against hardware failure using System Platform's Machine Preserving High Availability (MPHA) mode.

Related links

What's new in Application Enablement Services on page 14

Virtualized Environment Footprint Flexibility

In Release 6.3.1, the Avaya Application Enablement Services using VMware® in the Avaya Aura® Virtualized Environment offer allows you to configure the CPU and RAM of the virtual machine based on the number of available VMware licenses and the number of users to be supported. The AE Services 6.3.1 OVA template is built with a minimum resource consisting of 1 CPU and 2 GB of memory without CPU and memory reservation. CPU and memory reservation are required if you want to reach the advertised capacities (number of users and BHCC).

AE Services 6.3.1 supports the following footprint matrix.

Footprint	Microsoft Office Communicator/ Microsoft Lync/ Sametime	Avaya Aura Contact Center (Agent)	DMCC (non-server media)	TSAPI, DLG, CVLAN
1 CPU 2GB	10K/6K BHCC	1K/20K	1K/9K BHCC (concurrent 10)	1K msg/s
2 CPU 2GB	12K/12K BHCC	2.5K/50K	2.4K/18K BHCC (concurrent 20)	1K msg/s
4 CPU 4GB	20K/24K BHCC	5K/100K	4K/36K BHCC (concurrent 20)	2K msg/s

Related links

What's new in Application Enablement Services on page 14

Endpoint registration enhancements

In AE Services 6.3.1, DMCC, TSAPI, and JTAPI applications can receive endpoint registration state events that indicate when an H.323 and SIP endpoint has registered to and unregistered from a monitored station. These applications may also query for the H.323 and SIP endpoints registered at a station extension.

These new capabilities require Communication Manager 6.3 with Feature Pack 3 (that is, Communication Manager 6.3.2) or later.

AE Services 6.3.1 provides the following enhancements for endpoint registration events/query:

- **DMCC enhancements**

  DMCC can monitor the following updated events for each H.323 and SIP endpoint:

  - **EndpointRegisteredEvent**. There can be up to four events for a given station (three H.323 endpoints and one SIP endpoint).
  - **EndpointUnregisteredEvent**. There can be up to four events for a given station (three H. 323 endpoints and one SIP endpoint).

  Using the **EndpointRegistrationInforRequest**, DMCC can retrieve information on all endpoints registered to a given station on Communication Manager. The information for up to four endpoints for the station can be in the same response.

- **TSAPI enhancements**

  The following new CSTA Private Status events are available for monitored station extensions with TSAPI:

  - **ATTEndpointRegisteredEvent**
  - **ATTEndpointUnregisteredEvent**

  TSAPI can query a monitored station extension using the new **attQueryEndpointRegistrationInfo()** escape service.

  These new events and query require ASAI Link Version 6 and Private Data Version 11.

- **JTAPI enhancements**

  The following new events are available for LucentV11AddressListeners:

  - **LucentEndpointEvent.ENDPOINT_REGISTERED_EVENT**
  - **LucentEndpointEvent.ENDPOINT_UNREGISTERED_EVENT**

  The following new events are available for AddressObservers:

  - **LucentEndpointRegisteredEv**
  - **LucentEndpointUnregisteredEv**

  JTAPI can query a registered endpoint using the new **TsapiAddress.getRegisteredEndpoints()** command.

  These new events and query require ASAI Link Version 6.

Related links

What's new in Application Enablement Services on page 14

Support for the Avaya Common Server – Dell PowerEdge R620 server

AE Services 6.3.1 supports the Avaya Common Server – Dell™ PowerEdge R620 server.

Related links

What's new in Application Enablement Services on page 14

Support for the Avaya Access Security Gateway (ASG)

AE Services 6.3.1 supports the Avaya Access Security Gateway (ASG), which is a challenge and response authentication mechanism. When the ASG is configured, the craft and sroot accounts will receive a challenge when logging into the AE Services server using SSH and the AE Services Management Console.

Related links

What's new in Application Enablement Services on page 14

Support for Avaya Aura® Communication Manager 6.3.2

AE Services 6.3.1 is compatible with the following releases of Communication Manager:

- Communication Manager 5.2.1
- Communication Manager 6.0.x
- Communication Manager 6.2 Service Pack 2
- Communication Manager 6.3
- Communication Manager 6.3.2

Related links

What's new in Application Enablement Services on page 14

Support for the Microsoft Lync Server 2013

AE Services 6.3.1 supports Microsoft Lync Server 2013 and Microsoft Lync 2013 client (the full-featured client for Lync Server 2013). (Lync 2013 Basic client does not support Remote Call Control.)

Related links

What's new in Application Enablement Services on page 14

New in AE Services 6.3

ASAI enhancements

AE Services 6.3 provides the following ASAI capacity increases:

- Increased message rate limit on medium and large Communication Manager templates

  The AE Services 6.3 system message rate limit has increased from 1000 to 2000 messages per second (full duplex). Full bandwidth is available with a single session (that is, to one Communication Manager if only one Communication Manager is in use).

  The Communication Manager 6.3 system message rate limit has increased from 1000 to 2000 messages per second (full duplex) on medium and large templates. Full bandwidth is available with a single session (that is, to one Communication Manager if only one Communication Manager is in use). Full capacity is available over a single Processor Ethernet (PE) Application Enablement Protocol (AEP) connection and requires at least 10 CLANs. (There is no change per CLAN rates.)

Note:

There is no change in the message rate on small templates.

- Support for the multicast mechanism available in Communication Manager 6.3

  AE Services 6.3 supports the multicast mechanism available in Communication Manager 6.3. With the multicast mechanism, Communication Manager 6.3 can now pack the same ASAI message that is built for different associations/CTI links into a single AEP message. The multicast mechanism applies to events and route end messages destined for the same AE Services 6.3 server. AE Services 6.3 unpacks these messages and distributes them transparently to the appropriate upstream services.

  Note:

  - Communication Manager 6.3 applies this optimization automatically (where appropriate).
  - Optimization applies across all CTI services on the same AE Services server. (Multicast always benefits TSAPI since it uses additional monitors to implement CSTA.)
  - Multicast messages appear as normal, individual ASAI messages in Communication Manager MST tracing. The transport level message trace on AE Services shows the actual multicast messages.

- Increased Event Notifications limit on large Communication Manager templates

  AE Services 6.3 now supports a maximum of 30,000 Event Notifications up from 10,000 on large Communication Manager templates.

  Note:

  For small and medium Communication Manager templates, the maximum number of Event Notifications is still 10,000.

- Increased Adjunct Route Requests limit on large Communication Manager templates

  AE Services 6.3 now supports a maximum of 8,000 active Adjust Route Requests up from 4,000 on large Communication Manager templates.

  Note:

  - The increased maximum number of Adjunct Route Requests requires the purchase of the increased Adjunct Route license.
  - The maximum number of Adjunct Route Requests has not been increased on small and medium Communication Manager templates.
  - The increased maximum number of Adjunct Route Requests requires AE Services 6.3. Communication Manager will restrict the total Adjunct Route Requests to a maximum of 4,000 for all AE Services 6.2 and earlier systems.

- Increased ASAI associations

  AE Services 6.3 now supports a maximum of 128,000 ASAI associations across all CTI links. (This applies to TSAPI and CVLAN services.)

  AE Services 6.3 also supports a maximum of 32,000 Adjunct Routes per CTI link.

Related links

What's new in Application Enablement Services on page 14

Enhancements for Agile Communication Environment™ and Avaya Aura® Contact Center

AE Services 6.3 provides the following enhancements for Agile Communication Environment™ and Avaya Aura® Contact Center:

- GetTimeOfDay request

  The GetTimeOfDay request provides time information for a specified Communication Manager:

  - year
  - month
  - day
  - hour
  - minute
  - second

  The GetTimeOfDay request requires a switch name as a parameter to specify the switch that the application queries for the time information.

- Support for the Private Direct Number (DN) feature in Communication Manager 6.3

  The Private DN feature provides the following new feature access codes:

  - AACC No Conference Activation feature access code

    When the H.323 or DCP set is in this state, you cannot transfer or conference calls from the designated extension. To use this feature access code, you must administer the AACC No Conference Activation feature access code.

  - AACC One Conference Activation feature access code

    When the H.323 or DCP set is in this state, only one conference is allowed, and you can only transfer one call at a time. To use this feature access code, you must administer the AACC One Conference Activation feature access code.

  Note:

  - Only computer telephony integration (CTI) applications can activate the AACC No Conference and AACC One Conference feature access codes.
    - The extension used to invoke the AACC No Conference and AACC One Conference feature access codes must be a *monitored* extension. The feature access codes require a designated extension on which these features will be applied.

    - The ability to deactivate these features is available **to both** the application and the user (via a physical set).
  - You cannot activate the AACC No Conference Mode and AACC One Conference Mode features simultaneously.
  - The AACC No Conference Mode and AACC One Conference Mode features are not available currently for Avaya SIP endpoints.

Related links

What's new in Application Enablement Services on page 14

DMCC enhancements

AE Services 6.3 provides the following enhancements for the DMCC clients:

- Endpoint registration events

  The endpoint registration events enable you to:

  - Monitor H.323 endpoints registration activity on Communication Manager for up to three endpoints for a given extension.

    Note:

    The devices are not required to be registered via AE Services.

  - Retrieve information on H.323 endpoints registered to an extension on Communication Manager for up to three endpoints for a given extension.

  These events consume a basic TSAPI license for each extension and require Communication Manager Release 6.3 or later.

- Warning tone generation on a call for DMCC-registered endpoints

  A DMCC recording client can request AE Services to play a warning tone into a call using the following call recording methods:

  - Single Step Conference
  - Multiple Registration
  - Service Observing

Related links

What's new in Application Enablement Services on page 14

Security enhancements

AE Services 6.3 provides the following enhancements for FIPS 140-2 compliance:

- SHA512 encryption for password storage by default

The Linux passwords are hashed and stored on the server using SHA512 by default. However, you can configure the password encryption to SHA256 if needed.

- SSH client support of SSHv2 protocol only
  - AE Services supports the following ciphers: 3des, aes128, aes192, and aes256.

    SSH uses aes128, aes192, and aes256. AE Services processes use 3des and aes128 for signaling encryption.
  - AE Services supports the following Message Authentication Code (MAC): hmac-sha1.

Note:

SSH clients must be supported with the same ciphers and MAC as supported by AE Services. AE Services does not support CBC ciphers.

Related links

What's new in Application Enablement Services on page 14

Support for Avaya Communication Manager 6.3.2

AE Services 6.3.1 is compatible with the following releases of Avaya Communication Manager:

- Avaya Communication Manager 5.2.1
- Avaya Communication Manager 6.0.x
- Avaya Communication Manager 6.2 Service Pack 2
- Avaya Communication Manager 6.3
- Avaya Communication Manager 6.3.2

Related links

What's new in Application Enablement Services on page 14

AE Services Management Console enhancements

AE Services 6.3 provides the following enhancements to the AE Services Management Console:

- Log Manager

  Using the Log Manager feature, you can configure the trace/logging levels for the following services:
  - ASAI Link Manager
  - CVLAN Service
  - DLG Service
  - Management Console
  - Transport Layer Service

- TSAPI Service
- DMCC Service

Note:

Do not change the trace/logging levels without guidance from an Avaya engineer. Turning on the trace or increasing the logging levels may degrade system performance.

- DMCC Test

  Using the DMCC Test feature, you can make a first party call or third party call to test your DMCC configurations.

- Support for Microsoft Internet Explorer 9 and Microsoft Internet Explorer 10 running on Microsoft Windows 8 Pro and Microsoft Windows 8 Enterprise

Related links

What's new in Application Enablement Services on page 14

Command enhancements for the AE Services on System Platform offer

AE Services 6.3 provides the following command enhancements for the AE Services on System Platform offer:

- swversion command enhancement

  When you run the swversion command from the CDOM of the AE Services VM, the output now displays the AE Services version number with the System Platform version number.

  When you run the swversion command from the System Platform console domain, the output now displays the same information as when you run the swversion command from the AE Services VM with the swversion command from the console domain of VM.

- getlogs command enhancement

  Using the getlogs command from the System Platform console domain, you can now collect logs from both System Platform and the AE Services VM. When you run this command from the System Platform console domain, the output is stored in `/vspdata/getlogs/data` or `/vspdata/getlogs/archive` depending upon the arguments passed. The getlogs command options are:

  `-h` – shows all options for this command

  `-l` – shows the list of all VMs in System Platform

  `-r` – cleans out the logs

Related links

What's new in Application Enablement Services on page 14

Support for Microsoft Windows 8

The following AE Services 6.3 SDKs and clients support Microsoft Windows 8 Pro and Microsoft Windows 8 Enterprise:

- AE Services DMCC .NET SDK
- AE Services DMCC Java SDK
- AE Services DMCC XML SDK
- AE Services JTAPI SDK
- AE Services TSAPI SDK
- AE Services TSAPI client
- AE Services CVLAN client

Related links

What's new in Application Enablement Services on page 14

Chapter 4: AE Services Product Summary

Introduction

AE Services provides a platform that supports existing contact center application requirements, along with new, emerging APIs. Application Enablement Services provides programs that perform specific functions and provide application programming interfaces (APIs), protocols, and Web-based interfaces. A description of each service that is included in AE Services is provided in this chapter. For a high-level illustration of AE Services see configuration at a glance on page 30.

DMCC service

The Device, Media, and Call Control (DMCC) service provides third-party call control as well as first party call control (device control and media control). The DMCC SDK provides a Java API as well as XML and .NET interfaces. For more information about the DMCC SDKs, see SDKs on page 55.

- DMCC first-party call control (1PCC)
  - DMCC with Device Control provides the ability to set up a DMCC softphone that gains exclusive or shared control of a softphone-enabled Communication Manager telephone or extension. A DMCC softphone is an instance of a phone or extension that is created by AE Services and then registered on Communication Manager.
  - DMCC with Media Control provides the ability to record media from a call into a WAV file or play a voice announcement or tone that is prerecorded in a WAV file. Media session control also provides a way for a client application to send and receive TTY characters over Real-time Transport Protocol (RTP) streams in the form of RFC2833 packets. Applications can use this capability to implement Voice Carry Over (VCO). The TTY capability is available in client-media mode only.
- DMCC third-party call control (3PCC)

  DMCC with Call Control Services uses the TSAPI service to provide an expanded set of third party call control capabilities, such as the ability to place calls, create conference calls, deflect calls, reconnect call, and monitor call control events, just to name a few.
- Routing Services

  Routing Services allows applications to request and receive routing instructions for a call. These instructions, issued by a client routing server application, are based on the incoming call information provided by Communication Manager.

DMCC call recording solutions - IP Migration Readiness and Optimization analysis

For DMCC call recording solutions, Avaya recommends that you use the Avaya IP Migration Readiness and Optimization services to help you safely implement IP-based solutions in a stable, optimized infrastructure.

These services include a two-phased, detailed analysis of the entire network to help assess whether you can deploy a converged IP solution such as AE Services without adversely affecting your existing network applications and services.

The first phase of this analysis is the Customer Infrastructure Readiness Survey (CIRS). Certified Avaya engineers conduct a high-level evaluation of the local and wide area network infrastructure to identify any significant network issues that must be resolved prior to deploying the proposed IP solution.

Phase 2 of this analysis, Network Analysis/Network Optimization (NANO), is required when the CIRS indicates that the network cannot support the proposed IP solution at the desired performance levels. Starting with the information and data gathered for the CIRS, Avaya engineers perform problem diagnosis to get at the root causes of network issues. They also provide functional requirements and recommendations for a network design that optimizes all of the resources needed to support the IP solution.

TSAPI service

Telephony Services API (TSAPI) is a C/C++ based API that provides a full complement of third-party call control capabilities such as controlling specific calls or stations, completing routing of incoming calls, receiving notifications of events, invoking Communication Manager features and querying Communication Manager for information. Java Telephony API (JTAPI) is a client-side interface to the TSAPI service, and, as such, it provides third party call control. For more information about the TSAPI SDK and the JTAPI SDK, see SDKs on page 55.

Web services

Web services provide a higher-level abstraction than the finer grained APIs. Web services provide convenient access to commonly used functionality through a published Web Services Definition Language (WSDL) and Simple Object Access Protocol (SOAP) connectivity.

For more information about the Web services SDKs, see SDKs on page 55.

System Management Service

The System Management Service exposes management features of Communication Manager. This service enables its clients to display, list, add, change and remove specific managed objects on Communication Manager.

Telephony Web Service

The Telephony Web Service is a Web services interface that enables high level call control functionality over standard Web services interfaces (SOAP/XML).The service hides the complicated concepts associated with traditional CSTA based call control such as connections, call identifiers and call states.

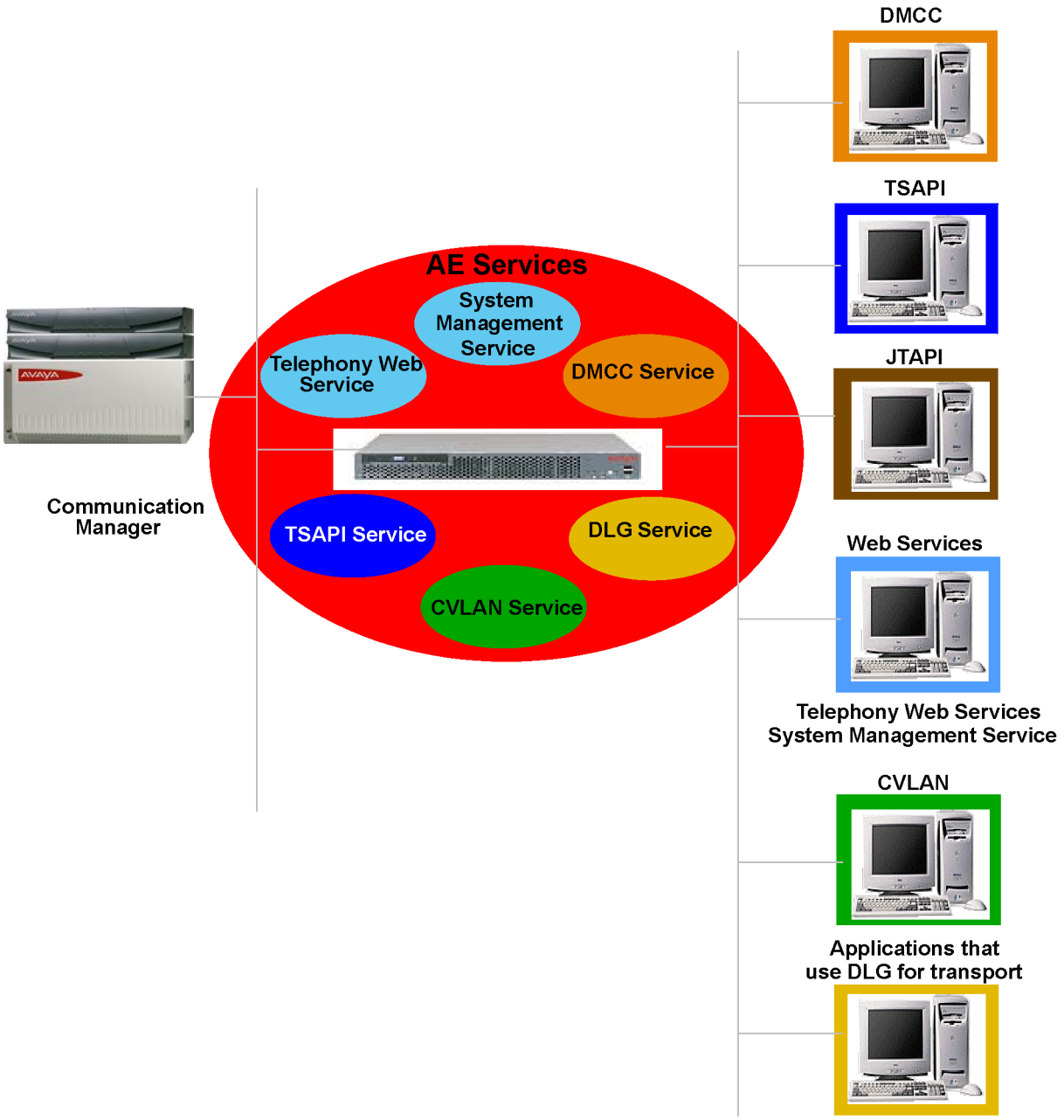
CVLAN service

The CallVisor LAN (CVLAN) service is a C/C++ based API that enables applications to exchange ASAI messages with the AE Server. CVLAN provides a full complement of third-party call control capabilities such as controlling specific calls or stations, completing routing of incoming calls, receiving notifications of events, invoking Communication Manager features and querying Communication Manager for information. CVLAN is an Avaya specific protocol and is not intended for new application development.

DLG service

The DEFINITY LAN Gateway (DLG) service tunnels messages over TCP/IP. That is, the DLG service supports a set of TCP/IP connections for the communications channel between Communication Manager and AE Services. The DLG service is also used for transporting ASAI/Q.931 messages. DLG is an Avaya specific protocol and is not intended for new application development.

AE Services configuration at a glance



Chapter 5: Network Security and Reliability

AE Services security features

The following list highlights the AE Services security features.

Linux shell access control

The Modify Login page in the AE Services Management Console (**Security** > **Account Management** > **Modify Login**) provides the AE Services administrator with the ability to control Linux shell access for a Linux account.

Login Audit

The Unused Login Audit page in AE Services Management Console (**Security** > **Audit** > **Login Audit**) lets the AE Services administrator enable an audit process for disabling any unused Linux account.

Lock or unlock a Linux account

The Lock/Unlock Login feature in AE Services Management Console (**Security** > **Account Management** > **Lock/Unlock Login**) lets the AE Services administrator lock or unlock a Linux account.

Login Reports

The Login Reports feature in AE Services Management Console (**Security** > **Audit** > **Login Reports**) lets the AE Services administrator generate reports based on a login ID.

Role Based Access Control (RBAC)

Access to AE Services Management Console Web pages can be restricted by user authorization level. The operations that users are allowed to perform such as read, edit and delete can also be restricted.

Additional AE Services security features information

For more information about AE Services security features, see *White Paper on Security in Application Enablement Services for the Bundled, AES on System Platform and Software Only Solutions*. Also see “Chapter 5: Security Administration and Additional PAM Management” in the *Avaya Application Enablement Services Administration and Maintenance Guide*. These documents are located on the Avaya Support Web site http://www.avaya.com/support.

Secure application links

You can configure all AE Services APIs to use secure application links. The AE Services client installation programs install certificates by default. You can use the default certificates for secure communications, or, if you have your own Public Key Infrastructure system already set up, you can install your own certificates.

DMCC API

The DMCC API provides:

- Validation of the AE Services server certificate on the DMCC client application
- Optional validation of the client certificate on the AE Server

  For more information see the following documents:

  - *Avaya Application Enablement Services Device, Media and Call Control API Java Programmers Guide*, 02-300359
  - *Avaya Application Enablement Services Device, Media and Call Control API XML Programmers Guide*, 02-300358
  - *Avaya Application Enablement Services Device, Media and Call Control API .NET Programmers Guide*, 02-602658
  - *Avaya Application Enablement Services Administration and Maintenance Guide*, 02-300357

TSAPI, JTAPI, and CVLAN

TSAPI, JTAPI, and CVLAN provide validation of the server certificate. For more information, see the following documents:

- *Avaya Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide*, 02-300543.
- *Avaya Application Enablement Services JTAPI Programmers Guide*, 02-603488.

Web Services

For Web Services, AE Services provides a Tomcat RPM that includes a default certificate and a default keystore of encryption keys for use in connecting to the AE Services server via Secure Sockets Layer (SSL). For more information, see the *Application Enablement Services Web Services Programmer Guide*, 02-300362.

AE Services link resiliency and failover

AE Services provides an AEP connection that establishes and maintains a secure communication channel between AE Services and Communication Manager. This transport service, implemented on the AE Services server and on Communication Manager, tunnels ASAI and call information services messages over TCP/IP, using a proprietary Avaya protocol called Application Enablement Protocol (AEP). The AEP connection is secured via Transport Layer Security (TLS).

An AEP transport connection is a secure TCP/IP connection between the AE Services server and a CLAN or Processor Ethernet connection on Communication Manager. When the transport service

starts up, it establishes the Communication Manager/AEP transport connection sessions based on the switch connections administered in the AE Services Management Console.

The Link Bounce Resiliency feature provides increased link reliability to the AEP transport connection. This feature ensures that no messages are lost during an interchange or a short network outage of up to 30 seconds.

One AE Services server can support up to 16 AEP transport connections. The 16 AEP connections provide a redundancy failover capability for configurations that use CLAN or Processor Ethernet connections.

- If a CLAN goes down or is not accessible over the network, the traffic is redistributed to the remaining CLANs. This failure should be transparent to the application, provided that the failed CLAN was not necessary to support the message bandwidth required by the application.
- If a Processor Ethernet connection goes down or is not accessible over the network, the session is still preserved. As long as it is reestablished within 30 seconds, no data will be lost.

Support for an Enterprise Survivable Server configuration

Prior to AE Services 6.1, only switch connections on CLANs were supported for Enterprise Survivable Server (ESS) configurations. Beginning with AE Services 6.1, switch connections on both CLANs and Processor Ethernet (PE) connections are supported for ESS configurations. Additionally, any DMCC endpoints registered to the main switch (using the Time-to-Service feature) will automatically re-register to the ESS or LSP.

Note:

A combination of CLANs and PEs for ESS configurations are supported if the main switch connection is configured as a CLAN. If the main switch connection is configured as a PE connection, then all ESS configurations should be configured as PE connections.

Note:

Partial PE support can be achieved between AE Services 6.1 or later and Communication Manager 5.2.x or later. However, for full support of PEs, Communication Manager 6.0 or later is required.

Uninterrupted telephony is important for many enterprises, especially for mission-critical applications. Avaya Communication Manager provides Enterprise Survivable Server (ESS) and Local Survivable Processor (LSP) for failover from the main media server. This feature provides the ability for media gateways, endpoints, application servers like AE Services and its applications to continue their operations without major interruption.

AE Services recommends that all applications in an ESS configuration connect to a local AE Services server which, in turn, is connected to either the media server at the main site or a media gateway with an ESS or LSP at the remote site. In this configuration, the applications and associated AE Services server at the remote sites are always active and are supplying functionality

for the local resources at the remote site. This type of configuration ensures the most seamless survivability in an ESS configuration.

For more information, see *White paper on Avaya Application Enablement Services High Availability (HA) Configurations,* located on the Avaya Support Web site http://www.avaya.com/support.

Chapter 6: Guidelines and requirements for configuring AE Services

This topic provides some requirements and guidelines for configuring AE Services. For more information about configuring AE Services, see *White paper on Avaya Application Enablement Services High Availability (HA) Configurations,* located on the Avaya Support Web site http://www.avaya.com/support.

- Only one instance of the AE Services server software can reside on an AE Services server machine (requirement).
- More than one AE Services server can connect to the same Communication Manager server.
  - If your applications do not use an AEP connection, there is no limit to the number of connections to Communication Manager servers. For example, if you are using the DMCC service for Device and Media control only and you are using Communication Manager licenses for DMCC endpoints , you would not use the transport link. If you want to use WebLM's DMCC-DMC licenses, you need a transport link.
  - If your applications use an AEP connection, AE Services can support up to 16 connections to Communication Manager servers. For more information, see Configurations that use AEP connections on page 36.
- AE Services recommends that you use the Processor Ethernet interface for all configurations.
- Applications must run on a separate client application machine (several applications can run on one machine if the machine has the resources to run these applications).
- It is recommended that Communication Manager be configured for H.323 registration using the Time-to-Service feature. For High Availability Failover and ESS, it is required that Communication Manager be configured for H.323 registration using the Time-to-Service feature in order to do silent recovery of DMCC registrations. For AE Services 6.1 and later, DMCC Device Control depends on the Call Information Link and the AEP connection to determine if the Communication Manager server supports the H.323 Time to Service registration feature for AE Services.
- An application should use a local HA cluster of Application Enablement Services on System Platform.
- An application that uses the Device, Media and Call Control (DMCC) service should keep trying to reestablish the DMCC session when it loses its socket communication link to the DMCC service. Because the runtime state is preserved, once the session is reestablished, all of the DeviceIDs, device or call monitors, and device registrations will still be intact.
- An application that uses the CVLAN, DLG or TSAPI service should reestablish its sessions when it loses the socket connection to the service on the AE Services server. Because no

runtime state is preserved for these services, the application should also reestablish any monitors/associations.

- The AE Services server can support a mixed environment that includes TSAPI, DMCC, Web Services, CVLAN, and DLG based applications.

Configurations that use AEP connections

AE Services can support up to 16 AEP connections to Communication Manager. AE Services recommends that you use the Processor Ethernet interface for all configurations. If, however, you use CLANs, AE Services strongly recommends that you use at least 2 CLANs for each switch connection to Communication Manager.

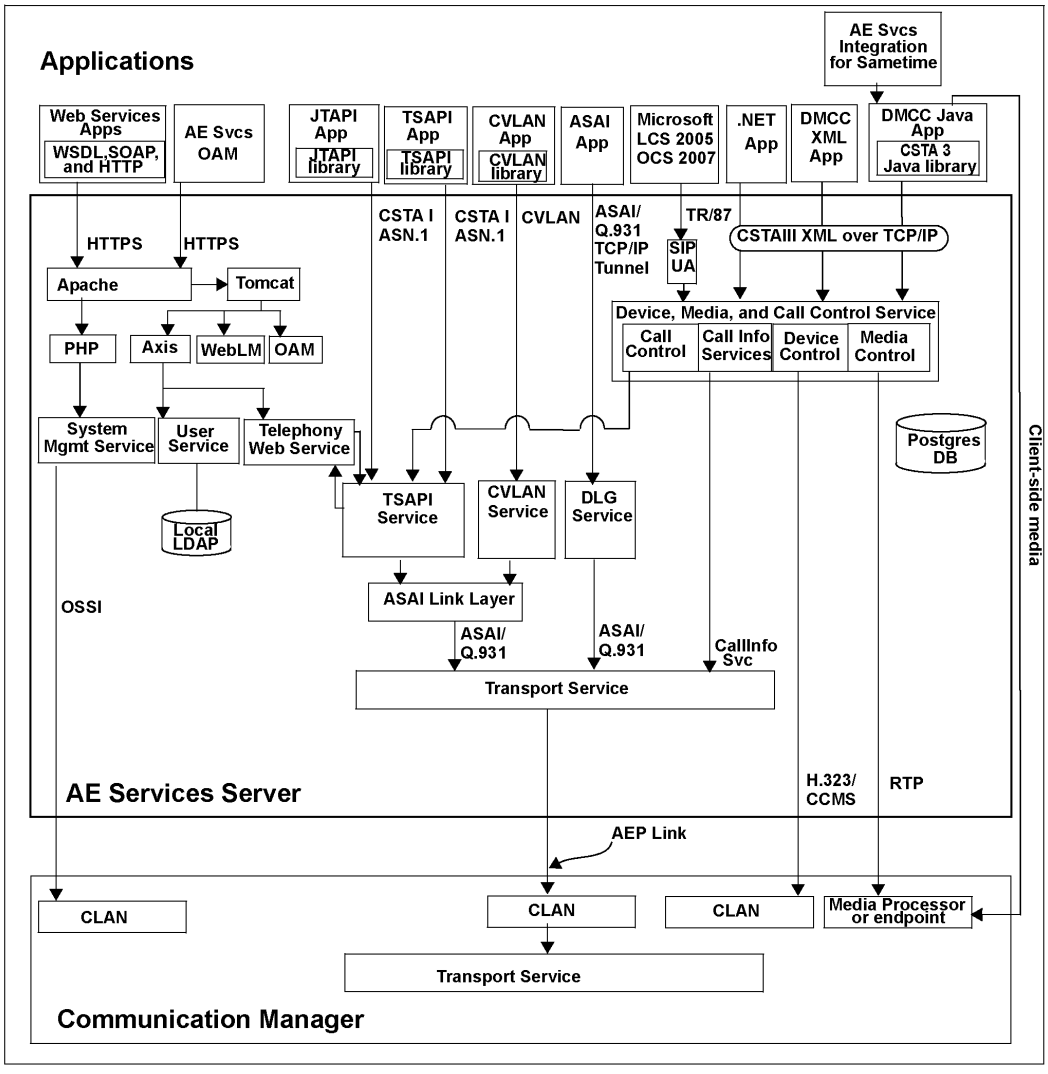
- TSAPI

  The following APIs, services, and integrations also use the TSAPI service:

  - JTAPI
  - AE Services integration for IBM Lotus Sametime
  - AE Services integration for Microsoft Live Communications Server 2005
  - AE Services integration for Microsoft Office Communications Server 2007
  - AE Services integration for Microsoft Lync Server 2010
  - AE Services integration for Microsoft Lync Server 2013
  - DMCC with Call Control
  - Telephony Web Services
- DMCC endpoint registration using WebLM's DMCC-DMC licenses
- DMCC with Call Information Services
- CVLAN
- DLG

Chapter 7: AE Services Architecture

AE Services architecture at a glance

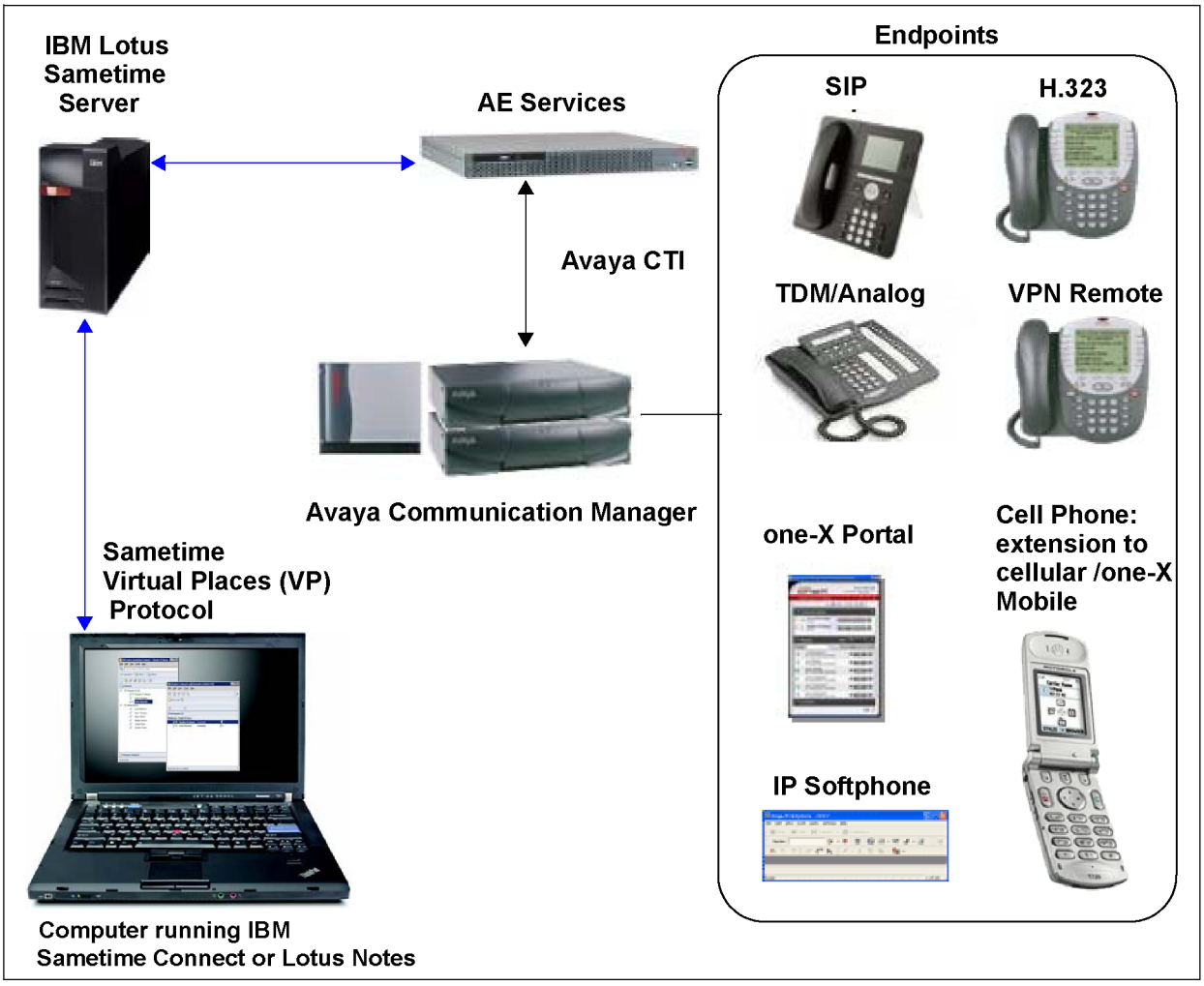


AE Services integration for IBM Lotus Sametime

The AE Services integration for IBM Lotus Sametime is a special packaging of the AE Services DMCC service that is positioned as an offer. The AE Services integration for IBM Lotus Sametime provides a solution for controlling your Avaya telephone or IP softphone using IBM Lotus Sametime. AE Services integration for IBM Lotus Sametime was introduced in AE Services 4.2. For Release 6.3.1, AE Services supports IBM Sametime 8.5.2 in addition to IBM Sametime 8.5.1, 8.5.0, 8.0.2, and 7.5.

The AE Services integration for IBM Lotus Sametime requires a Telephony Conferencing Provider Interface (TCSPI) plug-in which is provided by the DMCC client.

For more information, see the *Avaya Application Enablement Services Integration Guide for IBM Lotus Sametime*, 02-602818.



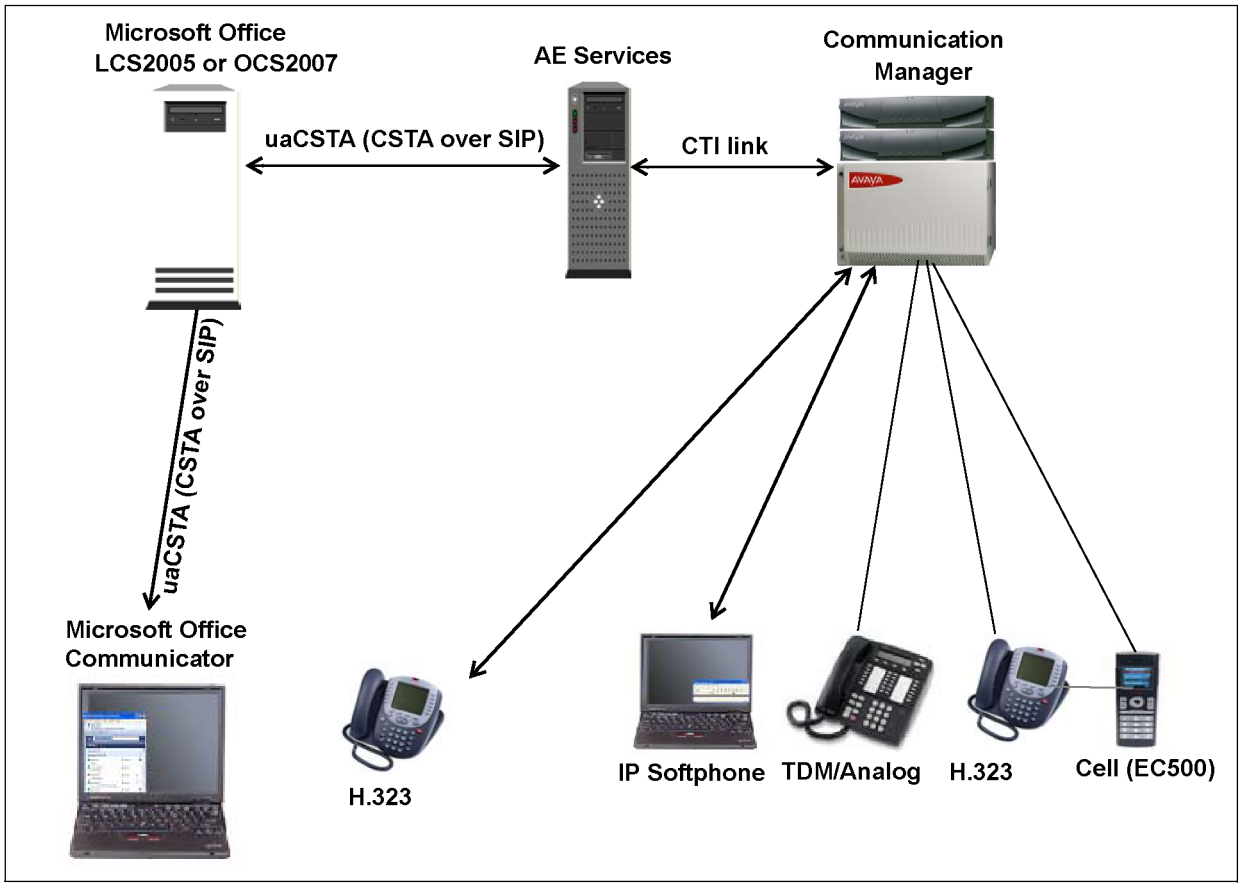
AE Services integration with Microsoft Office Communication Servers and Microsoft Lync Servers

AE Services provides an integration solution that is compatible with either of the following Microsoft Office platforms:

- Microsoft Office Live Communications Server 2005
- Microsoft Office Communications Server 2007 R1 and R2
- Microsoft Lync Server 2010
- Microsoft Lync Server 2013

The AE Services integration with Microsoft Office and Lync products is a special packaging of the AE Services DMCC service that is positioned as an offer. The AE Services integration with Microsoft Office and Lync provides a solution for controlling your Avaya telephone or IP softphone using Microsoft Office Communicator or Microsoft Lync client. You do not have to install any Avaya software on the Microsoft Office client or Lync client, and the AE Server can support a mixed environment that includes either of the AE Services Microsoft Office and Lync platforms as well as TSAPI, DMCC, Web Services, CVLAN and DLG based applications. The AE Services integration with Microsoft Office Live Communications Server was initially released in AE Services 4.0. The AE Services integration with Microsoft Office Communications Server 2007 was initially released in AE Services 4.1.

For more information, see the *Avaya Aura® Application Enablement Services Implementation Guide for Microsoft® Live Communications Server 2005, Microsoft Office Communications Server 2007, and Microsoft Lync® Server 2010 and 2013*, 02-601893.


Microsoft Office
LCS2005 or OCS2007
AE Services
Communication
Manager
uaCSTA (CSTA over SIP)
CTI link
uaCSTA (CSTA over SIP)
Microsoft Office
Communicator
H.323
IP Softphone
TDM/Analog
H.323
Cell (EC500)

Chapter 8: Session Initiation Protocol (SIP)

SIP support

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

Specific Avaya SIP endpoints can be controlled with AE Services 4.1 or later and Communication Manager 5.0 or later. AE Services 5.2 or later supports SIP enabled endpoints Avaya 96XX (including 9620, 9630, 9630G, 9640 and 9640 G) with firmware version 2 or greater and Avaya 16CC with all firmware versions.

The requirements for SIP support are as follows:

- Communication Manager 5.0 or later
- SIP Enablement Services (SES) 5.0 or later, or Avaya Session Manager (ASM)

AE Services 4.1 with Communication Manager 5.0 and SIP Enablement Services (SES) 5.0 introduced the ability to control Avaya SIP endpoints via TSAPI/JTAPI. This capability is not available through DLG.

SIP limitations

The following topics list the SIP limitations for AE Services. For more information about SIP limitations, see the Application Enablement Services Release Notes.

DMCC

All third-party call control capabilities are supported for the endpoints listed in SIP support on page 41. The following scenarios are not supported for SIP endpoints:

- The media forking implementation approach to call recording introduced in AE Services 4.2 is not supported. That is, an application registering a DMCC softphone in dependent mode with the same extension as the user's SIP phone or softphone is not supported. If the DMCC endpoint is registered as dependent to the SIP extension, it will not receive media.
- With respect to device control, DMCC cannot register an application controlled softphone in dependent mode with the same extension as the user's SIP phone or softphone for purposes such as pressing buttons, monitoring LEDs, and monitoring display.

TSAPI/JTAPI

All third-party call control capabilities are supported for the endpoints listed in SIP support on page 41, except the following capabilities:

- Third-Party Selective Listening Hold
- Third-Party Selective Listening Retrieve

IBM Lotus Sametime integration

All third-party call control capabilities are supported for the endpoints listed in SIP support on page 41, except the following capabilities:

- Send DTMF (Dual Tone Multi-Frequency) digits
- Third-Party Selective Listening Disconnect
- Third-Party Selective Listening Reconnect
- The automatic setting and unsetting of the Send All Calls feature based on a user's Do Not Disturb status does not work for SIP endpoints.

Microsoft Office Communications Server (OCS) integration

All third-party call control capabilities are supported for the endpoints listed in SIP support on page 41, except the following capabilities:

- Send DTMF (Dual Tone Multi-Frequency) digits
- Third-Party Selective Listening Disconnect
- Third-Party Selective Listening Reconnect

Chapter 9: AE Services Licensing

AE Services licensing summary

The table in this topic summarizes how features are licensed on Communication Manager and AE Services. For further information about licensing for a specific product, see the following topics:

Application Enablement Protocol connections licensing on page 45

AE Services integration for Microsoft Office Communications Server and Microsoft Lync Server licensing on page 46

AE Services integration for IBM Lotus Sametime licensing on page 46

Device, Media, and Call Control (DMCC) licensing on page 46

Web services licensing on page 47

System Management Service (SMS) licensing on page 47

TSAPI service (including JTAPI) licensing on page 48

CVLAN licensing on page 49

DLG licensing on page 50

Enterprise-wide licensing on page 50

Comparison of standard licensing and enterprise-wide licensing on page 50

Licensing configuration examples on page 51

AE Services product or service	Required feature licensed on Communication Manager	Optional feature licensed on Communication Manager	AE Services feature
	Use display system-parameters customer-options command to see if the feature is provided by the Communication Manager License.		**Use WebLM to see if this feature is provided by the Application Enablement license.**
AE Services Integration with Office Communications Server	Not applicable	Not applicable	Unified Desktop

Table continues…

AE Services product or service	Required feature licensed on Communication Manager	Optional feature licensed on Communication Manager	AE Services feature
	Use display system-parameters customer-options command to see if the feature is provided by the Communication Manager License.		**Use WebLM to see if this feature is provided by the Application Enablement license.**
AE Services Integration IBM Lotus Sametime	Not applicable	Not applicable	Unified Desktop
DMCC - Device and Media Control	• STA • IP_STA	IP-API_A - all pre-existing IP_API_A licenses in Communication Manager license remain there and may be used once the AE Services feature licenses are exhausted.	Device, Media, and Call Control
DMCC - Call Control	• Computer Telephony Adjunct Links • If using Call Control along with Device and Media Control, see Device Media and Call Control DMCC licensing on page 46.	None	• TSAPI Basic license (denoted as TSAPI Simultaneous Users in license file)
TSAPI Service (which includes JTAPI) for applications that use a Basic TSAPI license	Computer Telephony Adjunct Links	None	TSAPI Basic license (denoted as TSAPI Simultaneous users in license file)
TSAPI Service (which includes JTAPI) for applications that use an Advanced TSAPI license	Computer Telephony Adjunct Links	Increased Adjunct Routes	• AES Advanced Small Switch • AES Advanced Medium Switch • AES Advanced Large Switch
Web Services - Telephony Web Service	Computer Telephony Adjunct Links	None	• TSAPI Basic license (denoted as TSAPI Simultaneous Users in license file)
Web Services-System Management Service	None	None	None

Table continues…

AE Services product or service	Required feature licensed on Communication Manager	Optional feature licensed on Communication Manager	AE Services feature
	Use display system-parameters customer-options command to see if the feature is provided by the Communication Manager License.		**Use WebLM to see if this feature is provided by the Application Enablement license.**
CVLAN Service (Avaya Interaction Center)	Computer Telephony Adjunct Links	Increased Adjunct Route Capacity (for adjunct routing applications)	CVLAN Proprietary Links
CVLAN Service (Non-Avaya applications) **Note:** ASAI Core and ASAI Plus are included for one Communication Manager server when purchasing the CVLAN service.	ASAI Core	• CTI Stations • Phantom Calls • Adjunct Routing (Communication Manager 5.1 or later) • Increased Adjunct Route Capacity	CVLAN ASAI
DLG Service **Note:** ASAI Core and ASAI Plus are included for one Communication Manager server when purchasing the DLG service.	ASAI Core	• CTI Stations • Phantom Calls • Adjunct Routing (Communication Manager 5.1 or later) • Increased Adjunct Routes	DLG

Application Enablement Protocol connections licensing

Beginning in AE Services 5.2, an Application Enablement Protocol (AEP) is no longer discretely licensed in AE Services. This capability is provided to all licensed systems.

You can administer a total of 16 AEP connections but AE Services strongly recommends that you use 2 AEP connections to Communication Manager when the CLAN is used for connectivity. When all AEP connections are in use, no additional AEP connections are brought online. For more information, see Configurations that use AEP connections on page 36. Only a single AEP connection is required when connecting to Communication Manager using the Processor Ethernet interface.

You can use WebLM to determine the number of licensed AEP connections. You can check for the number of AEP connections on the **AE Services License** page.

AE Services integration for Microsoft Office Communications Server and Microsoft Lync Server licensing

The AE Services integration with either Microsoft Office Live Communications Server 2005, Microsoft Office Communications Server 2007, and Microsoft Lync Server 2010 and 2013 requires the Unified Desktop Edition RTU (Right To Use) license.

Every active Microsoft Office Communicator/Lync client consumes one Unified Desktop license for the duration of the period that it has an active dialog with AE Services (every registered Microsoft Office Communicator/Lync client, not only those in the call).

For more information, see *Avaya Aura® Application Enablement Services Implementation Guide for Microsoft® Live Communications Server 2005, Microsoft Office Communications Server 2007, and Microsoft Lync® Server 2010 and 2013*, 02-601893.

AE Services integration for IBM Lotus Sametime licensing

The AE Services integration for IBM Lotus Sametime integration requires the AE Services Unified Desktop Edition RTU (Right To Use) license.

Every active Sametime Connect/Lotus Notes client will consume one Unified Desktop Edition RTU license for the duration of the dialog with AE Services.

For more information, see *Avaya Aura® Application Enablement Services Integration Guide for IBM Lotus Sametime*, 02-602818.

Device, Media, and Call Control (DMCC) licensing

The DMCC Service provides control of devices and media streams and a subset of third-party call control services.

DMCC Device and Media Control Service

Historically, licensing for registering a DMCC (formerly CMAPI) station was in the Communication Manager license file, via the IP_API_A field. For customers who had previously purchased those licenses, the IP_API_A licenses will continue to remain accessible by AE Services applications, regardless of which AE Services release the server is running.

Factoring in release levels: In certain circumstances, purchases of new or add-on DMCC licenses are reflected in the AE Services license file as well as in the IP_API_A on Communication Manager. The release levels of both AE Services and Communication Manager determine where any new DMCC licenses will be placed.

- If AE Services is Release 4.2 or higher and Communication Manager is Release 5.1 or higher, any new or add-on DMCC licenses will be added to the AE Services license file in addition to the IP_API_A in the Communication Manager license. Note that this double licensing will be reconciled in the future, and a switch connection must be administered in addition.
- If one or both of these cases does not apply (in other words, if AE Services is Release 4.1 or lower or Communication Manager is Release 5.0 or lower), new or add-on DMCC licenses will continue to be added to the IP_API_A in the Communication Manager license file only.

For customers who have existing licenses in IP_API_A and then purchase additional DMCC licenses, the information provided above about factoring in release levels continues to apply. Effective with Communication Manager Release 6.0, all new DMCC licenses will be added only to the AE Services license file VALUE_DMCC_DMC field.

Upon a registration request, AE Services will first attempt to consume a DMCC license from the AE Services license file. If these are exhausted, AE Services will look to IP_API_A for additional licenses to consume.

Note:

Regardless of whether DMCC registrations are licensed on Communication Manager or on AE Services, the addition of a DMCC station on Communication Manager also consumes an IP_STA license and an STA license.

DMCC Call Information Service

Licenses are not required to use the DMCC Call Information Service.

DMCC Call Control Service

To use the DMCC Call Control Service, you must license and enable Computer Telephony Adjunct Links on Communication Manager. Because the DMCC Call Control Service uses third-party call control, the AE Services TSAPI Basic Users license is also required.

Web services licensing

For the Telephony Web Service, Communication Manager requires Computer Telephony Adjunct Links to be licensed for Web services. Because the Telephony Web Service uses third-party call control, the AE Services TSAPI Basic Users license is also required.

System Management Service (SMS) licensing

Beginning in AE Services 5.2, System Management Service (SMS) is no longer discretely licensed in AE Services. This capability is provided to all licensed systems.

TSAPI service (including JTAPI) licensing

The TSAPI Service provides third-party call control services. AE Services JTAPI is a client-side interface to the TSAPI service, and, as such it provides third-party call control as well.

For TSAPI (and JTAPI), AE Services provides two types of licenses: the TSAPI Basic Users license, and the TSAPI Advanced license. The TSAPI Advanced license provides access to a different set of features than the TSAPI Basic User license. That is, the Advanced license does not include the capabilities provided by the TSAPI Basic Users license.

TSAPI basic user license

The TSAPI basic user license is often referred to as either an “agent-based license” or a “station based license.” It is intended for applications that want to monitor or control a station or monitor an ACD split. In the license file it is referred to as a “Simultaneous User” license. It is scaled in terms of the number of agents, stations, or ACD splits that you want to monitor and control.

The TSAPI basic user license requires that you license and enable Computer Telephony Adjunct Links on Communication Manager. The following table shows the TSAPI basic user license capabilities in terms of TSAPI service requests.

Call Control Service Group	Monitor Service Group
Alternate Call	Monitor Device
Answer Call	Change Monitor Filter
Clear Connection	
Conference Call	
Consultation Call	
Deflect Call	
Hold Call	
Make Call	
Pickup Call	
Reconnect Call	
Retrieve Call	
Single Step Conference Call	
Single Step Transfer Call	
Transfer Call	

Once a TSAPI basic user license has been allocated on behalf of a station, that license will remain in use as long as one of the following conditions exists:

- The station is being monitored.
- There are any calls present at the station.

Once a TSAPI basic user license has been allocated on behalf of an ACD split, that license will remain in use as long as the ACD split is being monitored.

Note:

The TSAPI basic user licenses may be reserved or pre-allocated through OAM. The reserved TSAPI basic user licenses are acquired when the TSAPI Service is started and remain in use until the TSAPI Service is stopped.

TSAPI advanced license

The TSAPI advanced license is intended for applications that launch calls (predictive dialing applications) or route calls. The TSAPI advanced license is based on the number of Communication Manager servers you want to license and the size of the Communication Manager platform: Small (S84xx), Medium (S85xx), and Large (S87xx and S8800).

Note:

When used as a replacement for the S85xx, the S8800 platform is a Medium platform.

The following table shows the capabilities provided with the TSAPI advanced license.

Call Control Service Group	Routing Service Group
Make Predictive Call	Route Select
Selective Listening Hold	Route Select Inv
Selective Listening Retrieve	

The TSAPI Advanced License requires that you license and enable the Communication Manager feature for Computer Telephony Adjunct Links.

If you have a routing application that requires additional capacity, you have the option of licensing the Increased Adjunct Route Capacity feature on Communication Manager.

Once a TSAPI advanced license is acquired on behalf of a Communication Manager server, that license remains in use till the TSAPI Service is stopped or restarted.

CVLAN licensing

The CVLAN Service provides third-party call control. The CVLAN Service is integrated with Avaya applications, and it is used by customer applications.

- When the CVLAN Service is used for customer applications, it requires a Communication Manager license for ASAI Core. CVLAN bundles ASAI Core and ASAI Plus for a single Communication Manager. Optionally, you can license the following features on Communication Manager: ASAI Plus, CTI Stations, Phantom Calls, Adjunct Route, and Increased Adjunct

Route Capacity. Customer applications must use an ASAI-IP link type on Communication Manager. This link type requires ASAI Core and ASAI Plus.

- Avaya Interaction Center (IC) requires an ADJ-IP link type.

  Note:

  Avaya IC is the only CVLAN application that can use an ADJ-IP link on Communication Manager.

DLG licensing

The DLG Service requires a Communication Manager license for ASAI Core. DLG bundles ASAI Core and ASAI Plus for a single Communication Manager. Optionally, you can license the following features on Communication Manager: ASAI Plus, CTI Stations, Phantom Calls, Adjunct Route, and Increased Adjunct Route Capacity. Customer applications must use an ASAI-IP link type on Communication Manager. This link type requires ASAI Core and ASAI Plus.

Enterprise-wide licensing

Beginning with Release 4.2, AE Services supports enterprise-wide licensing. With enterprise-wide licensing, AE Services customers are able to purchase any number of licenses and then allocate those licenses to various AE Servers at their own discretion. This means that AE Services customers are able to pool or share all AE Services features, and Rights To Use (RTU) among AE Servers. This applies only to AE Services features licensed in the AE Services license file and not those licensed in the Communication Manager license file.

- To compare standard licensing with enterprise-wide licensing, see Comparison of standard licensing and enterprise-wide licensing on page 50.
- For examples of licensing configurations, see Licensing configuration examples on page 51.

Comparison of standard licensing and enterprise-wide licensing

Standard licensing	Enterprise-wide licensing
AE Services has used the standard license file since the introduction of the platform (Release 3.0). The	AE Services introduced support for enterprise-wide licensing with Release 4.2.

Table continues…

Standard licensing	Enterprise-wide licensing
standard license file continues to be used for standalone AE Services server licensing.	
A standard license is generated by the Product Licensing and Delivery System (PLDS) from the system record for an AE Services server.	Enterprise-wide licensing includes a master enterprise license file (ELF) and an allocation license file (ALF). • The master enterprise license file (ELF) is generated by the PLDS from the system record from the enterprise. The master license file can reside on an AE Services server or a dedicated WebLM server. • The allocation license file (ALF) is generated by WebLM based on features in the master license file and user allocations on the AE Services server. The ALF or ALFs can reside on one or more AE Services servers.
The standard license file is installed on the AE Services server. In a standard licensing arrangement, AE Services and the WebLM server are normally co-resident.	With enterprise wide licensing, the WebLM server does not have to be co-resident with AE Services, but each local WebLM server is normally co-resident with the AE Services server that it licenses.
With standard licensing, a license can not be moved from one server to another, and capacities can not be reallocated.	With enterprise-wide licensing, you can reallocate enterprise capacities and features as desired.

Licensing configuration examples

To understand how licensing configurations work, this section provides a description of standard licensing and enterprise-wide licensing.

Standard licensing

In a standard licensing configuration for Bundled and Software-only offers, the standard license file (SLF) is installed on the AE Services server and is controlled by the WebLM server running on the AE Services server. For System Platform installations, the standard license file is normally installed on, and controlled by, the WebLM server running in the Console Domain (c-dom).

Note:

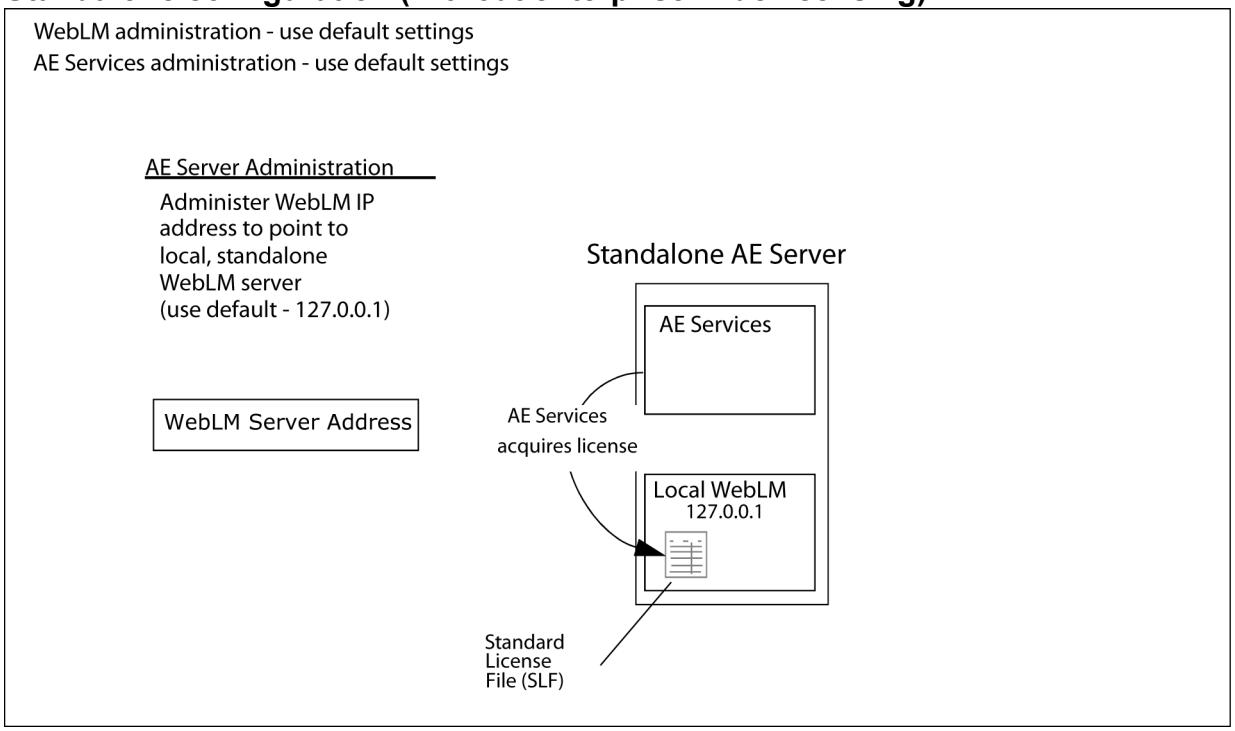
For System Platform installations, when using the WebLM server in c-dom, port 52233 should be used for licensing.

The following figure illustrates the standard licensing configuration.

Note:

If you use the standalone configuration, use the default settings on the WebLM Server Address page in the AE Services Management Console.

Standalone configuration (without enterprise-wide licensing)



Note:

The default IP address, 127.0.0.1, shown in the illustration above is only for the AE Services Bundled and AE Services Software-only offers. The default IP address for the AE Services on System Platform offer is the IP address of the c-dom on System Platform. For the AE Services on VMware offer, there is no default WebLM address. The user must enter an appropriate IP address for the WebLM server.

Enterprise-wide licensing — allocating licenses or features

Starting with Release 4.2, AE Services expanded its licensing capabilities to include enterprise-wide licensing. Enterprise-wide licensing provides the flexibility to move capacities and features from one AE Services server to another. For example, prior to AE Services 4.2, if you had purchased 3 AE Services servers with different licensing capacities, you could not move capacity purchased for one AE Services server to another AE Services server. With enterprise-wide licensing, you can move capacities or features from one server to another by using a master WebLM server to allocate license features to different AE Services servers.

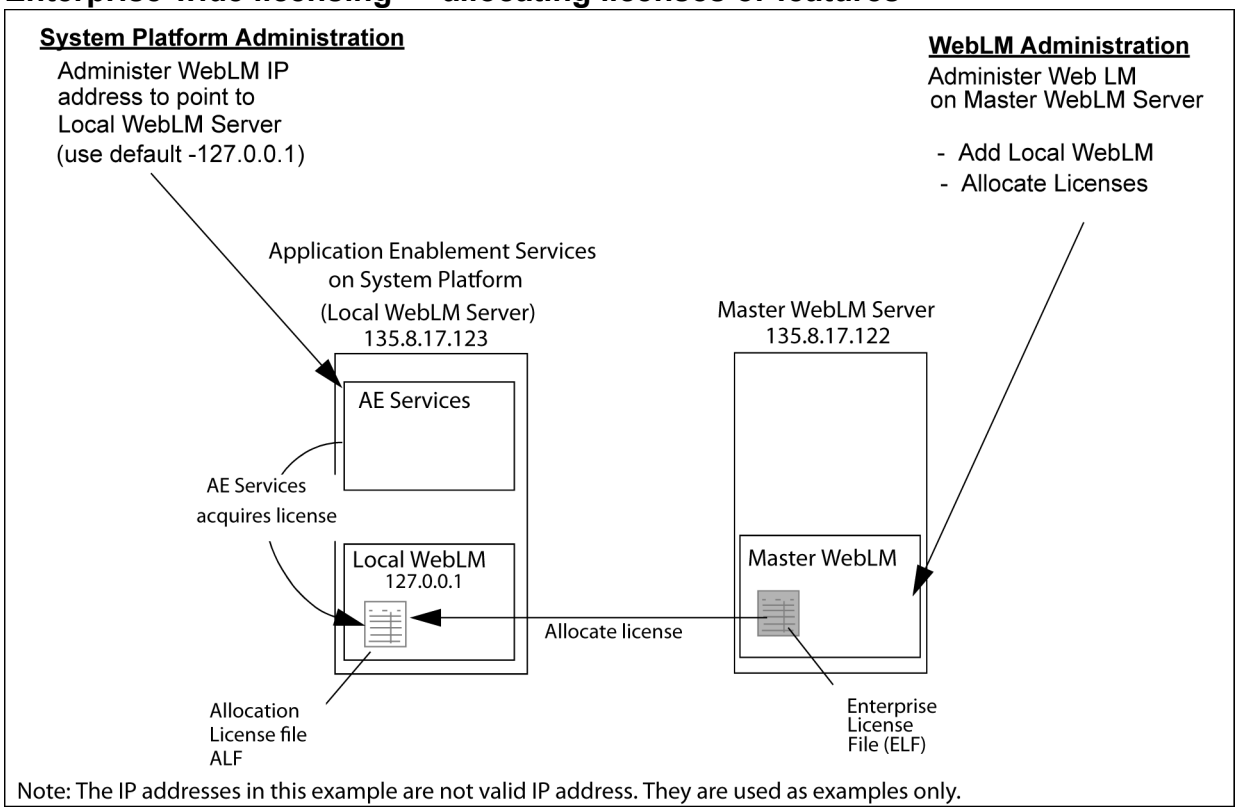
Because this configuration relies on a master enterprise license file (ELF), which generates allocation license files (ALF), it is referred to as an ELF/ALF configuration. Each ALF will reside on

an AE Services server with a Local WebLM Server. This is the recommended model for AE Services enterprise configurations. If you use the ELF/ALF model, you do not need to change the default settings on the WebLM Server Address page.

For this configuration you must use WebLM Administration to configure the master WebLM server so that it can allocate licenses to each local WebLM server on the AE Services servers. (In the WebLM Administration, select **Licensed Products** > **Application Enablement (CTI)** > **Configure Local WebLMs** > **Add Local WebLM**.)

The following figure illustrates an ELF/ALF configuration.

Enterprise-wide licensing — allocating licenses or features



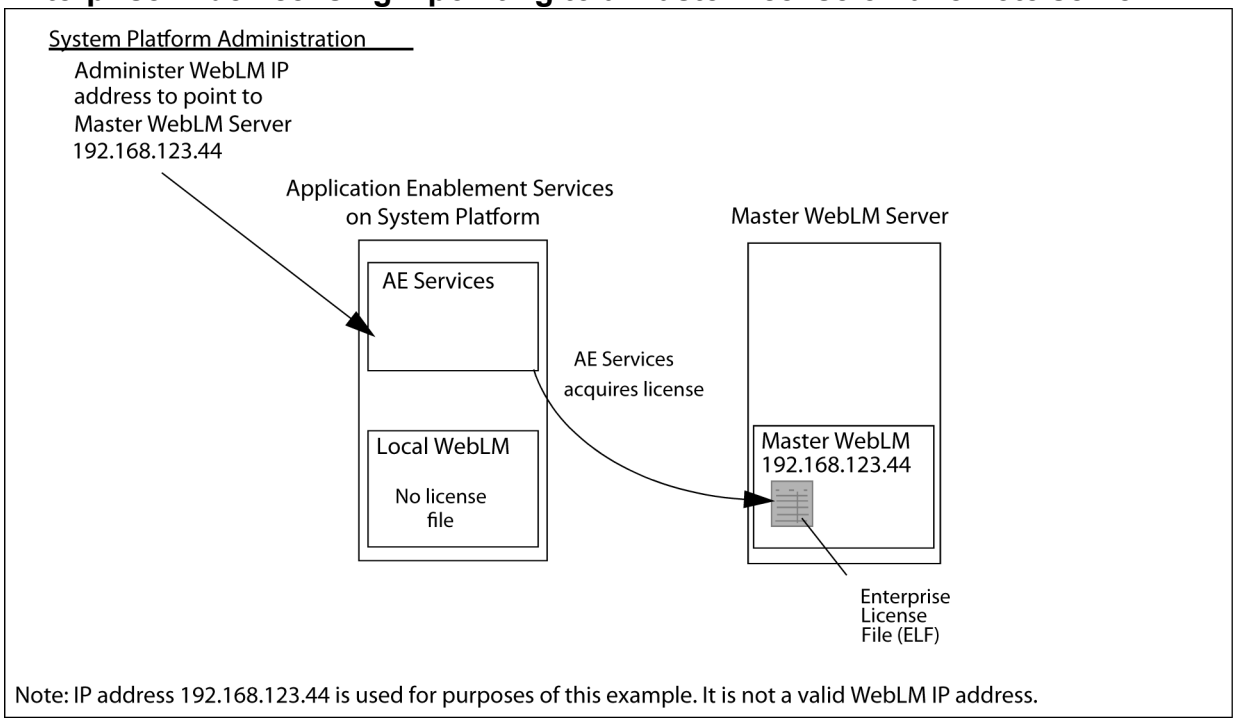
Enterprise-wide licensing — pointing to a master license on a remote server

Another type of enterprise licensing configuration is an enterprise license file (ELF)-only configuration. In an ELF-only configuration, the enterprise license file resides on a master WebLM server, and one or more AE Services servers point to the IP address of the master WebLM server. No allocation license files (ALFs) reside on AE Services servers.

If you use the ELF-only configuration, you must administer the WebLM Server Address page in the AE Services Management Console with the WebLM IP address and WebLM port number for the master WebLM server that hosts the ELF.

The following figure illustrates an ELF-only configuration.

Enterprise-wide licensing – pointing to a master license on a remote server



Caution:

Using the ELF-only configuration is not recommended because network latency and outages can affect the ability of the AE Services server to acquire licenses, and it creates a single point of failure for licensing.

Additional documents

See the following documents for more information about AE Services licensing.

- *Implementing Avaya Application Enablement Services on Avaya Aura® System Platform*, Release 6.3
- *Implementing Avaya Application Enablement Services for a Bundled Server*, Release 6.3
- *Implementing Avaya Application Enablement Services in a Software-Only Environment*, Release 6.3
- *Avaya Application Enablement Services Administration and Maintenance Guide*, Release 6.3
- *Avaya white paper on Application Enablement Services Enterprise-Wide Licensing*

Chapter 10: Application Enablement Services Client and SDKs

All Application Enablement Services Software Development Kits (SDKs), with the exception of the TSAPI SDK, are available on the Avaya Support Web site http://www.avaya.com/support and the Avaya DevConnect Web site www.avaya.com/devconnect where you can download them at no charge. If you prefer a DVD-ROM copy of an SDK, contact your account executive. The following table lists the SDKs provided with Application Enablement Services.

Name	Distribution	Material code/URL
Application Enablement Services TSAPI SDK	Contact your account executive	700500048
Application Enablement Services TSAPI client	Avaya DevConnect Developer Program	http://www.avaya.com/support www.avaya.com/devconnect
Application Enablement Services CVLAN client	Avaya DevConnect Developer Program	http://www.avaya.com/support www.avaya.com/devconnect
Application Enablement Services DMCC Java SDK	Avaya DevConnect Developer Program	http://www.avaya.com/support www.avaya.com/devconnect
Application Enablement Services DMCC XML SDK	Avaya DevConnect Developer Program	http://www.avaya.com/support www.avaya.com/devconnect
Application Enablement Services DMCC .NET SDK	Avaya DevConnect Developer Program	http://www.avaya.com/support www.avaya.com/devconnect
Application Enablement Services Web Service — Telephony Web Svc SDK	Avaya DevConnect Developer Program	http://www.avaya.com/support www.avaya.com/devconnect
Application Enablement Services JTAPI SDK	Avaya DevConnect Developer Program	http://www.avaya.com/support www.avaya.com/devconnect
Application Enablement Services SMS SDK	Avaya DevConnect Developer Program	http://www.avaya.com/support www.avaya.com/devconnect

Chapter 11: Communication Manager features not supported

Maintenance state of Communication Manager endpoints

ASAI is not informed of and does not report the maintenance state (in service/out of service) of any Communication Manager endpoints via a domain control.

QSIG Interactions

- **ASAI:** For ISDN trunks administered with Supplementary Service Protocol “b” (also referred to as QSIG-enabled), ASAI is not able to track calls with supplementary UUI information. ASAI does not support QSIG path replacement. If any of the QSIG optional parameters are enabled on the Communication Manager QSIG Optional Features form, ASAI can not keep track of the call.
- **CVLAN:** Because the CVLAN service is implemented using ASAI, CVLAN support for this feature is also incomplete.
- **TSAPI:** The TSAPI service does not properly handle certain call scenarios involving QSIG trunks.
- **JTAPI:** Because JTAPI is an interface to TSAPI, JTAPI does not properly handle certain call scenarios involving QSIG trunks.

Bridging

- **ASAI:** A bridged call appearance is selected for a single-step conference by Communication Manager only if there are no regular call appearances available at the added station. Other than that, bridging is not supported with either single-step conference or phantom calls.

  Note:

  ASAI does not support configurations where there are more than 16 bridged appearances administered for a given call appearance.
- **CVLAN:** Because the CVLAN service is implemented using ASAI, CVLAN support for this feature is also incomplete.
- **TSAPI:** Because the TSAPI service is implemented using ASAI, TSAPI support for this feature is also incomplete.
- **JTAPI:** Because JTAPI is an interface to TSAPI, JTAPI support for this feature is also incomplete.

Call Park

- **ASAI:** A call may be parked manually at a station by using the call park button (with or without the conference and transfer buttons), or by using the feature access code and the conference or transfer buttons. When a call is parked using the call park button (without either the

conference or the transfer buttons) no event reports are generated. When the call is unparked, a Connected Event Report is generated with the calling and called numbers indicating the station on which the call had been parked, and the connected number is that of the station unparking the call. If the call remains active at the parking station (via conference), no changes occur to the listening disconnected paths as a result of parking. If the call drops from the parking station (via transfer), its paths are disconnected from everyone on the call. A single-step conference request will be denied if the call is parked.

- **CVLAN:** Because the CVLAN service is implemented using ASAI, CVLAN support for this feature is also incomplete.
- **TSAPI:** Because the TSAPI service is implemented using ASAI, TSAPI support for this feature is also incomplete.
- **JTAPI:** Because JTAPI is an interface to TSAPI, JTAPI support for this feature is also incomplete.

Chapter 12: Capacities for AE Services

This chapter provides the capacities for AE Services.

Note:

If the Machine Preserving High Availability (MPHA) feature is enabled, the overall capacities of AE Services are reduced by 50 percent.

Related links

AE Services integration for Microsoft Office Communication Server on page 58
AE Services integration for IBM Sametime on page 59
Capacities for calls in DMCC applications on page 59
Communication Manager capacities for DMCC on page 63
System Management Services capacities on page 65
System capacities – Communication Manager on page 65
System capacities – AE Services server 6.3.3 on page 65
ASAI associations on page 66
CVLAN service capacities on page 66
DLG service capacities on page 67
TSAPI service capacities on page 67

AE Services integration for Microsoft Office Communication Server

Requires 2 G memory and hardware platform equivalent to the Avaya S8510/Dell 1950.

Microsoft Office Communicator Clients per AE Server	
AE Server dedicated to Microsoft Office Communicator integration	Support for up to 20,000 concurrent clients at 24,000 BHCC
Microsoft Office Communicator and other API traffic	Support for up to 5,000 concurrent OC clients at 6000 BHCC and 2000 DMCC clients in client media mode at 36,000 BHCC **or**

Table continues…

Microsoft Office Communicator Clients per AE Server	
	Support for up to 10,000 concurrent OC clients at 12,000 BHCC and 1000 DMCC clients in client media mode at 18,000 BHCC

Related links

Capacities for AE Services on page 58

AE Services integration for IBM Sametime

Requires 2 G memory and hardware platform equivalent to the Dell 1950 Quad Core.

IBM Sametime Connect Clients per AE Server	
AE Server dedicated to IBM Sametime integration	10,000 concurrent clients at 12,000 BHCC
IBM Sametime and other API traffic	Support for up to 5,000 concurrent Sametime clients at 6000 BHCC and 2000 DMCC clients in client media mode at 36,000 BHCC **or** Support for up to 10,000 concurrent Sametime clients at 12,000 BHCC and 1000 DMCC clients in client media mode at 18,000 BHCC

Related links

Capacities for AE Services on page 58

Capacities for calls in DMCC applications

The number of simultaneous active calls that Device, Media, and Call Control (DMCC) applications can expect to handle depends on many factors.

- If either Client or Server Media mode is used, the following should be taken into consideration:
  - Your application's demand for VoIP resources relative to the VoIP resources available on Communication Manager
  - The codec used and packet size chosen for media
  - Media encryption
- Whether encryption is used for the application link or the signaling link

Compare the DMCC capacities listed in Table 1: Non-server media (client media, telecommuter, and no-media) on page 60 and Table 2: Server media on page 60 with the Communication Manager resources and capacities described in capacities for DMCC on page 63 to make sure that you have adequate Communication Manager resources for a given DMCC implementation.

Table 1: Non-server media (client media, telecommuter, and no-media)

Session and H323 Signaling Encryption Profile	AE Server Capacity	Traffic Rate for Applications
None	4,000 endpoints and a 36,000 BHCC (Avaya Common Server – Dell R620, HP DL360 G7, or Dell R610, S8800, Dell 1950, or equivalent customer-provided server)	AE Services and Communication Manager can support up to 20 outstanding registration requests by an application at any time If multiple CLANs are used, the client must distribute 20 outstanding registration requests evenly among allocated CLANs. If signaling encryption is used, the number of outstanding registration requests must not exceed 10.
PIN-EKE	3,200 endpoints and a 28,800 BHCC (Avaya Common Server – Dell R620, HP DL360 G7, or Dell R610, S8800, Dell 1950, or equivalent customer-provided server)	AE Services and Communication Manager can support up to 20 maximum registration requests by an application in a 10-second interval. Based on a recommendation of 5 registrations per CLAN, this can be reached by having 4 CLANs, which are able to process 5 encrypted registrations each. Note that the same limit of 20 registrations in a 10-second limit applies for Processor Ethernet also. Developers need to consider this limit when designing applications (that is, a gap of 10 seconds is required between each set of 20 registrations if 4 CLANs are being utilized; a gap of 10 seconds is required between each set of 15 registrations if 3 CLANs are being utilized; a gap of 10 seconds is required between each set of 20 registrations if 10 CLANs are being utilitzed with 4 registrations per CLAN; and so forth).
H323TLS	2,000 endpoints and a 18,000 BHCC (Avaya Common Server – Dell R620, HP DL360 G7, or Dell R610, S8800, Dell 1950, or equivalent customer-provided server) For more information see, Additional AE Services Restrictions on page 63.	AE Servicesand Communication Manager can support up to 20 registration, when sent by an application, in a 10-second interval. Avaya recommendations 5 registrations per CLAN. 4 CLANs can fulfill the capacity for 20 registrations.Note that the same limit of 20 registrations in a 10-second limit applies for Processor Ethernet also..

Table 2: Server media

	Code Type	AE Server Capacity	Traffic Rate for Applications
No signaling and media encryption	G729	120 endpoints	AE Services and Communication Manager can support up to 100

Table continues…

	Code Type	AE Server Capacity	Traffic Rate for Applications
			maximum simultaneous registration requests by an application in a 10-second interval. Based on a recommendation of 20 registrations per CLAN, this can be reached by having 10 CLANs, which are able to process 20 unencrypted registrations each per 10-second interval. Note that the same limit of 100 registrations in a 10-second interval applies for Processor Ethernet also. Developers need to consider this limit when designing applications (that is, a gap of 10 seconds is required between each set of 100 registrations if 10 CLANs are being utilized; a gap of 10 seconds is required between each set of 80 registrations if 4 CLANs are being utilized; and so forth).
	G711	75 endpoints	AE Services and Communication Manager can support up to 75 maximum simultaneous registration requests by an application in a 10-second interval. Based on a recommendation of 20 registrations per CLAN, this can be reached by having 4 CLANs, which are able to process 20 unencrypted registrations each per 10-second interval. Note that the same limit of 75 registrations in a 10-second interval applies for Processor Ethernet also. Developers need to consider this limit when designing applications (that is, a gap of 10 seconds is required between each set of 75 registrations if 4 CLANs are being utilized; a gap of 10 seconds is required between each set of 60 registrations if 3 CLANs are being utilized; and so forth).
Signaling and media encryption	G729	96 endpoints	AE Services and Communication Manager can support up to 96 maximum registration requests by an application in a 10-second interval.

Table continues…

	Code Type	AE Server Capacity	Traffic Rate for Applications
			Based on a recommendation of 5 registrations per CLAN, this can be reached by having 20 CLANs, which are able to process 5 encrypted registrations each. Note that the same limit of 96 registrations in a 10-second limit applies for Processor Ethernet also. Developers need to consider this limit when designing applications (that is, a gap of 10 seconds is required between each set of 20 registrations if 4 CLANs are being utilized; a gap of 10 seconds is required between each set of 15 registrations if 3 CLANs are being utilized; a gap of 10 seconds is required between each set of 20 registrations if 10 CLANs are being utilitzed with 4 registrations per CLAN; and so forth).
	G711	60 endpoints	AE Services and Communication Manager can support up to 60 maximum registration requests by an application in a 10-second interval. Based on a recommendation of 5 registrations per CLAN, this can be reached by having 12 CLANs, which are able to process 5 encrypted registrations each. Note that the same limit of 60 registrations in a 10-second limit applies for Processor Ethernet also. Developers need to consider this limit when designing applications (that is, a gap of 10 seconds is required between each set of 20 registrations if 4 CLANs are being utilized; a gap of 10 seconds is required between each set of 15 registrations if 3 CLANs are being utilized; a gap of 10 seconds is required between each set of 20 registrations if 10 CLANs are being utilitzed with 4 registrations per CLAN; and so forth).

Note:

Traffic rate for applications is a gap of 10 seconds between each set of 100 registrations.

Related links

Capacities for AE Services on page 58
Additional AE Services Restrictions on page 63

Additional AE Services Restrictions

Following are some additional AE Services Restrictions:

- Using the PIN-EKE Security Profile can reduce the capacity of each AE Services server by 20%.
- Using the H323TLS Security Profile can reduce the capacity of each AE Services server by 50% .
- Supporting Communication Manager versions for FIPS and the H323TLS Security Profile:
  - The H323TLS Security Profile when used with Processor Ethernet is supported with the Communication Manager FIPS template for Communication Manager 6.3.6 and later.
  - The H323TLS Security Profile when used with CLAN is supported with the Communication Manager FIPS template for Communication Manager 6.3.7 and later.

Related links

Capacities for calls in DMCC applications on page 59

Communication Manager capacities for DMCC

Component	Capacity
For each IP endpoint in a call, including AE Services endpoints	• 1 VoIP channel is used (with a G.711 codec) • 2 VoIP channels are used (with a G.729 codec)
TN2302 media processor card	64 channels
TN2602 Crossfire media processor card	320 channels
MM760 VoIP card	64 channels
G700 media gateway motherboard VoIP	64 channels
G350 media gateway motherboard VoIP	32 channels
TN799DP CLAN card	400 DMCC station registrations For more information, see Additional Communication Manager Restrictions on page 64
Processor Ethernet	• 400 DMCC station registrations for Communication Manager running on S83xx or S84xx series servers

Table continues…

Component	Capacity
	• 4000 DMCC station registrations for Communication Manager running on S8510, S87xx, and S8800 series servers For more information, see Additional Communication Manager Restrictions on page 64

Related links

Capacities for AE Services on page 58
Additional Communication Manager restrictions on page 64

Additional Communication Manager restrictions

Following are the additional restrictions for Communication Manager:

- Using the PIN-EKE Security Profile can reduce the capacity of the Communication Manager platform by 15%.
- Using the H323TLS Security Profile can reduce the Communication Manager platform capacity by 50%. Communication Manager limits the number of H323TLS registration based on its size.
  - 160 DMCC station registrations for a Small Communication Manager platform (S83xx or S84xx)
  - 1000 DMCC station registrations for a Medium Communication Manager platform
  - 2000 DMCC station registrations for a Large Communication Manager platform

    When Secure Mode with FIPS option is enabled, the H323TLS Security Profile is used by default. The actual number of H323TLS connections for an AE Services server across multiple Communication Managers may be limited by the capacity of each individual Communication Manager. If a mix of FIPS enabled Communication Managers and non FIPS Communication Mangers are used, you can calculate the number of registrations DMCC can support by considering that a H323TLS signaling channel consumes double the resources as that of a non-H323TLS DMCC registration.
- Supported Communication Manager versions for FIPS and the H323TLS Security Profile.
  - The H323TLS Security Profile when used with Processor Ethernet is supported with the Communication Manager FIPS template for Communication Manager 6.3.6 and later.
  - The H323TLS Security Profile when used with CLAN is supported with the Communication Manager FIPS template for Communication Manager 6.3.7 and later.

Related links

Communication Manager capacities for DMCC on page 63

System Management Services capacities

Component	Capacity
Simultaneous Communication Manager Servers	16
Simultaneous sessions/logins per Communication Manager	5
Single session – average number of Web requests serviced for station model	~6 requests/second
Multiplexed sessions – average number of Web requests serviced for station model	~10 requests/second

Related links

Capacities for AE Services on page 58

System capacities – Communication Manager

For information about Communication Manager system capacities, see Avaya Aura® Communication Manager System Capacities Table on http://support.avaya.com/

Note:

The overall system limit is not restricted by the type of underlying transport that is used. For example, either a single Processor Ethernet connection or 10 CLANs plus 1 redundant CLAN will be able to reach 1000 msgs/sec.

Related links

Capacities for AE Services on page 58

System capacities – AE Services server 6.3.3

Component	Capacity
Communication Manager servers supported by one AE Services Server	16
Connections to a Communication Manager server with one AE Services Server	16
Messages per second per AE Services Server connection to Communication Manager (1 CLAN)	200
Messages per second per AE Services Server connection to Communication Manager (processor ethernet)	2000
Messages per second per AE Services Server connection from Communication Manager (1 CLAN)	240

Table continues…

Component	Capacity
Messages per second per AE Services Server connection from Communication Manager (processor ethernet)	1000
Messages per second (per system)	2000 (see Note below)

Note:

The overall system limit is not restricted by the type of underlying transport that is used. For example, either a single Processor Ethernet connection or 10 CLANs plus 1 redundant CLAN will be able to reach 2000 msgs/sec.

Related links

Capacities for AE Services on page 58

ASAI associations

The number of supported domain controls on Communication Manager 4.0 is 32,000. This increase applies only to S85xx, S87xx, and S8800 servers. 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.

The number of supported generic associations on the AE Services 6.3.1 server is 128,000.

Related links

Capacities for AE Services on page 58

CVLAN service capacities

Component	Capacity
Clients supported	60
ASAI associations	128,000, shared over 16 links
Links	16

Related links

Capacities for AE Services on page 58

DLG service capacities

Component	Capacity
Clients supported	16
Links	16

Related links

Capacities for AE Services on page 58

TSAPI service capacities

Component	Capacity
Users (client connections) **Note:** A client connection refers to a unique AE Services session established by a TSAPI application. A single client connection may be used to monitor and control multiple stations or agents.	2500 TLinks
Links	16 (each to a different Communication Manager)

Note:

For any AE Server, there may be only one TSAPI link to any given Communication Manager.

Related links

Capacities for AE Services on page 58

Chapter 13: AE Services Documentation

Select documents based on products you use

One way of identifying the appropriate documents to use is to select a group of related AE Services documents for a specific product. For example, if you use the Device, Media, and Call Control (DMCC) API in a Java environment, the following documents would be applicable.

- *Avaya Aura® Avaya Application Enablement Services Device, Media and Call Control API Java Programmers Guide*, 02-300359

  This guide describes how to use the Device, Media and Call Control API, and it provides tips for writing an application.

- *Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer Reference* (HTML document)

  This guide provides the implementation details that you need when you are designing or implementing an application, such as which features and interfaces are supported by AE Services.

- *Avaya Aura® Application Enablement Services Device, Media, and Call Control Media Stack API Reference* (HTML document)

  This document is optional. You will need this document if your DMCC application is handling its own media, and you are using the media stack provided by Avaya.

- *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, 02-300357.

Guidelines for selecting documents based on your role within an organization

Planners

If you are involved with planning an Application Enablement Services server installation use this document, the *Avaya Aura® Application Enablement Services Overview and Specification*, 02-300360. Depending on the scope of your planning, you might want to consult additional

documents for more information. The following sections provide information about using additional documents for implementing Application Enablement Services.

AE Services with IBM Lotus Sametime integration

If you plan to integrate AE Services with IBM Lotus Sametime, see the following documents.

- *Avaya Aura® Application Enablement Services Integration Guide for IBM Lotus Sametime*, 02–602818. This guide is a high-level planning and implementation guide for integrating AE Services and IBM Lotus Sametime. It is directed toward an AE Services and a IBM Lotus Sametime administrative audience.
- *Implementing Avaya Aura® Application Enablement Services on Avaya Aura® System Platform*, 02–603468. If your integration uses the Application Enablement Services on System Platform offer, consult this document for information about installing AE Services.
- *Implementing Avaya Aura® Application Enablement Services for a Bundled Server* , 02–300356. If your integration uses the AE Services Bundled Server, consult this document for information about installing AE Services.
- *Implementing Avaya Aura® Application Enablement Services in a Software-Only Environment*, 02–300355. If your integration uses the AE Services Software-Only server consult this document for information about installing AE Services.
- *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, 02–300357. Use this document for information about administering Avaya Communication Manager and the AE Services server.
- *Avaya Aura® Application Enablement Services Management Console online help*. Use this online help for information about administering the AE Services server.

AE Services integration with Microsoft Office Communications Server and Microsoft Lync Server 2010 and 2013

If you plan to integrate AE Services with Microsoft Office Live Communications Server 2005, Microsoft Office Communications Server 2007, or Microsoft Lync Server 2010 or 2013, see the following documents.

- *Avaya Aura® Application Enablement Services Implementation Guide for Microsoft® Live Communications Server 2005, Microsoft Office Communications Server 2007, and Microsoft Lync® Server 2010 and 2013*, 02–601893
- *Implementing Avaya Aura® Application Enablement Services on Avaya Aura® System Platform*, 02–603468. If your integration uses the Application Enablement Services on System Platform offer, consult this document for information about installing AE Services.
- *Implementing Avaya Aura®Application Enablement Services for a Bundled Server* , 02–300356. If your integration uses the AE Services Bundled server, consult this document for information about installing AE Services.
- *Implementing Avaya Aura® Application Enablement Services in a Software-Only Environment*, 02–300355. If your integration uses the AE Services Software-Only server, consult this document for information about installing AE Services.
- *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, 02–300357. Use this document for information about administering Avaya Communication Manager and the AE Services server.
- *Avaya Aura® Application Enablement Services Management Console online help*. Use this online help for information about administering the AE Services server.

Installers and administrators — Application Enablement Services on System Platform

To install the AE Services software and to configure Communication Manager and AE Services, use the following documents.

- *Implementing Avaya Aura® Application Enablement Services on Avaya Aura® System Platform*, 02–603468.
- *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, 02–300357.
- *Avaya Aura® Application Enablement Services Management Console online help*.

Note:

AE Services does not assume that you will install a browser on the AE Server. To access WebLM (Avaya Web-based license management software) and to administer AE Services, you need a computer running a browser with network access to the AE Server.

Installers and administrators — Bundled Server offer

To install the AE Services software and to configure Communication Manager and AE Services, use the following documents.

- *Implementing Avaya Aura® Application Enablement Services for a Bundled Server* , 02–300356.
- *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, 02–300357.
- *Avaya Aura® Application Enablement Services Management Console online help*.

Note:

AE Services does not assume that you will install a browser on the AE Server. To access WebLM (Avaya Web-based license management software) and to administer AE Services, you need a computer running a browser with network access to the AE Server.

Installers and administrators — Software-Only offer

To install the AE Services software and to configure Communication Manager and AE Services, use the following documents.

- *Implementing Avaya Aura® Application Enablement Services in a Software-Only Environment*, 02–3003565.
- *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, 02–300357.

- *Avaya Aura® Application Enablement Services Management Console online help*.

Note:

AE Services does not assume that you will install a browser on the AE Server. To access WebLM (Avaya Web-based license management software) and to administer AE Services, you need a computer running a browser with network access to the AE Server.

If you are installing TSAPI and CVLAN clients and SDKs, refer to *Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide*, 02–300543.

Application developers

Application Enablement Services provides Software Development Kits (SDKs) and programming documents for developing applications. For a list of the Application Enablement Services SDKs, see SDKs on page 55.

Avaya DevConnect Program

Application developers who want to take advantage of the AE Services APIs or protocols are encouraged to participate in the Avaya DevConnect Program. The Avaya DevConnect Program gives you access to a comprehensive set of support and marketing programs that help you create the new generation of intelligent communications solutions. For more information, go to the Avaya DevConnect Web site www.avaya.com/devconnect.

Web services programmers

Application Enablement Services provides the following Web services.

- System Management Service

  The System Management Service is used to enable SOAP-based access to Communication Manager administration functions. AE Services 5.2 introduced the following SMS enhancements:

  - XML formatted input and output
  - Template look and feel
  - Unicode support
  - ISV model schema enhancements

- Telephony Web Service

  The Telephony Web Service allows users SOAP-based access to simple third-party call control features such as:

  - make call
  - answer call
  - drop call
  - conference call
  - transfer call

Note:

As of AE Services 4.1, the AE Services User Service SDK is discontinued. AE Services will not support applications written to the User Service. Applications developed for the User Service prior to AE Services 4.1 will continue to work on AE Services 4.1.

For more information about Web services, see the *Avaya Aura® Application Enablement Services Web Services Programmer's Guide*, 02–300362.

DMCC API programmers

Application Enablement Services provides DMCC programmers with tools that help them learn how to use the APIs and with SDKs for implementing the APIs.

Note:

DMCC API was formerly known as Communication Manager API.

- To see the capabilities of an AE Services DMCC application, see “Sample Device, Media, and Call Control applications” in the *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, 02–300357.
- If you are ready to program, see the following documents.
  - *Avaya Aura® Application Enablement Services Device, Media, and Call Control XML Programmer's Guide*, 02–300358
  - *Avaya Aura® Application Enablement Services Device, Media, and Call Control XML Programmer 's Reference* (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)
  - *Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer 's Guide*, 02–300359
  - *Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer's Reference* (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)
  - *Avaya Aura® Application Enablement Services Device, Media and Call Control API .NET Programmer's Guide*, 02–602658
  - *Avaya Aura® Application Enablement Services Device, Media, and Call Control .NET Programmer's Reference* (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)

TSAPI programmers

If you program to TSAPI, use the following documents to develop or maintain your applications.

- *Avaya Aura® Application Enablement Services TSAPI for Avaya Communication Manager Programmer’s Reference*, 02-300544. Use this document as your primary reference for TSAPI applications. It documents all third-party call control services, including Private Data Services, provided by Avaya Communication Manager. Private Data Services allow you to take advantage of the extended functionality of Communication Manager services.

- For information about installing the TSAPI clients and SDKs, see the *Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide*, 02-300543.
- *Application Enablement Services TSAPI Programmer's Reference*, 02-300545. This document describes the Telephony Services API, which is based on ECMA CSTA Standards 179 and 180. This document is required only if you need to learn the fundamental principles of TSAPI. If you are developing or maintaining TSAPI applications, and you are familiar with TSAPI, use the *Application Enablement Services TSAPI for Avaya Communication Manager Programmer's Reference*, 02-300544, as your primary reference.

JTAPI programmers

If you program to JTAPI, use the following documents to develop or maintain your applications.

- *Avaya Aura® Application Enablement Services JTAPI Programmers Guide*, 02-603488. This document describes how to use the AE Services JTAPI implementation to develop, debug, and deploy telephony applications.
- *Avaya Aura® Application Enablement Services JTAPI Programmer's Reference* (an HTML document available on the Web only at the Avaya Support Site and the Avaya DevConnect Site). This document provides you with a reference to API calls in the Avaya implementation of the Java Telephony API. This document describes all call control services, including Private Data Services, provided by Avaya Communication Manager. Private Data Services allow you to take advantage of the extended functionality of Communication Manager services.

CVLAN programmers

If you program to the CVLAN API (which is an implementation of the ASAI protocol), use the following documents.

Note:

AE Services does not support newly-developed CVLAN applications.

- *Avaya Aura® Application Enablement Services CVLAN Programmer's Reference*, 02-300546. Use this document as your primary reference for CVLAN applications. It documents all call control services provided by Avaya Communication Manager.
- For information about installing the CVLAN clients and SDKs, see the *Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide*, 02-300543.
- *Application Enablement Services ASAI Technical Reference*, 03–300549. The CVLAN call control capabilities are based on the capabilities described in this document. Consult this document when a high level of detail is required.
- *Application Enablement Services ASAI Protocol Reference*, 03–300550. CVLAN uses the ASAI protocol. Consult this document when a high level of detail regarding information elements and the layout of ASAI messages is required.

ASAI programmers

If you program directly to the Adjunct Switch Application Interface (ASAI) protocol, use the following documents as your primary reference.

Note:

AE Services does not support newly-developed ASAI applications.

- *Application Enablement Services ASAI Technical Reference*, 03–300549. This document provides technical descriptions of ASAI third-party call control capabilities.
- *Application Enablement Services ASAI Protocol Reference*, 03–300550. This document provides byte-level descriptions of ASAI messages.

Appendix A: AE Services Release 6.3.3 compatibility

This appendix describes the clients, API, and versions of Communication Manager that AE Services 6.3.3 supports. Additionally, this appendix describes the Communication Manager platforms that support AE Services 6.3.3.

API and client compatibility

AE Services 6.3.3 supports the API and clients described in this topic.

DMCC compatibility

Note:

- DMCC 5.x refers to any of the following releases: 5.2, 5.2.1, 5.2.2, 5.2.3
- DMCC API refers to any of the following releases: XML API, .NET SDK and Java SDK on JDK 5.0.
- DMCC 6.2.x Java API applications
- DMCC 6.2.x XML applications
- DMCC 6.3.x Java API applications
- DMCC 6.3.x XML applications

AE Services 6.3.3 is compatible with the following DMCC API-based applications.

- XML developers should be aware that AE Services changed to ECMA 323 edition 3 and the schemas have therefore changed. DMCC 3.1.x XML applications should continue to request 3.0 protocol version (ECMA 323 edition 2).
- The DMCC 4.2.x Java API applications:

  The DMCC 4.2.x client library and Java SDK 5.0 will work with the AE Services 6.3.3 DMCC Service.
- DMCC 4.2.x XML applications:

  The DMCC 4.2.x XML applications will work with the AE Services 6.3.3 DMCC Service.
- The DMCC 5.2.x Java API applications:

The DMCC 5.2.x client library and Java SDK 5.0 will work with the AE Services 6.3.3 DMCC Service.

- DMCC 5.2.x XML applications:

  The DMCC 5.2.x XML applications will work with the AE Services 6.3.3 DMCC Service.

- The DMCC 6.1.x Java API applications:

  The DMCC 6.1.x client library and Java SDK 5.0 will work with the AE Services 6.3.3 DMCC Service.

- DMCC 6.1.x XML applications:

  The DMCC 6.1.x XML applications will work with the AE Services 6.3.3 DMCC Service.

Web Services compatibility

For AE Services 6.3.3, the Telephony Web Service does not introduce any new features.

System Management Service compatibility

For AE Services 6.3.3, the System Management Service does not introduce any new features.

TSAPI compatibility

AE Services 6.3.3 TSAPI Service includes all of the functionality provided by AE Services 5.2, 6.1, 6.2, 6.3, and Avaya CT 1.x. AE Services 6.3.3 TSAPI Service is backward compatible with the following TSAPI/JTAPI clients and libraries: AE Services 5.2, 6.1, 6.2, and 6.3.

CVLAN compatibility

The AE Services 6.3.3 CVLAN Service includes all of the functionality provided by AE Services 6.3 CVLAN Service, CVLAN on MAPD, and the CVLAN R9 Server for Linux. The AE Services 6.3.3 CVLAN Service is backward compatible with the following CVLAN clients and libraries: AE Services 5.2, 6.1, 6.2, and 6.3.

DLG compatibility

AE Services 6.3.3 and Communication Manager 6.3.2 releases do not introduce any new DLG Service features.

- The AE Services 6.3.3 DLG Service includes all of the functionality provided by previous releases of the AE Services DLG Service (3.x through 6.3), the “DLG on the MAPD”, and the “Co-Res (co-resident) DLG.”
- The AE Services 6.3.3 DLG Service is compatible with existing applications that rely on the DLG Service.

AE Services compatibility with Communication Manager

AE Services 6.3.1 is compatible with the following Communication Manager releases:

- Communication Manager 5.2.1
- Communication Manager 6.0.x
- Communication Manager 6.2

- Communication Manager 6.3
- Communication Manager 6.3.2

Communication Manager 6.3.2 is compatible with the following AE Services releases:

- AE Services 6.2
- AE Services 6.3
- AE Services 6.3.1

AE Services compatibility with Communication Manager 6.3 CTI interfaces

AE Services relies on the CLAN and the Processor Ethernet for communications with Communication Manager. (The CLAN and the Processor Ethernet reside on Communication Manager.) The following table describes the Communication Manager platforms that use either CLANs or the Processor Ethernet (or in some cases, both).

Communication Manager platform	Communications interface
S8300	Processor Ethernet only
S8400	Processor Ethernet and CLAN
S85xx	Processor Ethernet and CLAN
S87xx MultiConnect (MC)	Processor Ethernet and CLAN
S87xx IP (see note below)	Processor Ethernet and CLAN
S88xx IP (see note below)	Processor Ethernet and CLAN
Avaya Common Server – Dell R620, HP DL360 G7, or Dell R610 (see note below)	Processor Ethernet and CLAN

Note:

With AE Services 5.2 or later and Communication Manager 5.2.1 or later, switch connections, H.323 links, and SMS connections can now be established directly to the Processor Ethernet on Communication Manager S87xx, S8800, and Avaya Common Server – Dell R620, HP DL360 G7, or Dell R610.

Communication Manager 6.3 - ASAI capabilities

For customer-developed CVLAN and ASAI-based applications, Communication Manager must be provisioned with ASAI features.

ASAI Core features

- Adjunct Call Control Group (for example, third-party call control)

- Domain Control Group (for example, domain control of a station)
- Event Notification Group (for example, event stream for VDN)
- Request Feature Group (for example, login agent and send all calls)
- Set Value Group (for example, set message waiting indicator)
- Single Step Conference
- II Digits

ASAI Plus features

- Switch classified call (Predictive Dialing)
- Answering Machine Detection (from within classified call)
- Selective Listening Hold/Retrieve

ASAI Optional Features

- CTI Stations
- Phantom Calls
- Adjunct Routing
- Increased Adjunct Route Capacity

Application Enablement Protocol (AEP) connection

Refers to the secure TCP connection between the AE Server and Communication Manager. It tunnels ASAI messages and Call Information Services messages between AE Services and Communication Manager.

Application Enablement Protocol (AEP)

The protocol used by an AEP connection.

ASAI

Adjunct Switch Application Interface. ASAI is a protocol that enables software applications to access call processing capabilities provided by Communication Manager.

Authentication

The process of validating the identity of a user by means of user profile attributes.

Authorization

The process of granting a user the ability to carry out certain activities based on permissions.

CLAN

Control LAN. CLAN refers to the Avaya TN799 Control LAN circuit pack, which resides on Communication Manager. AE Services relies on the CLAN for communicating with Communication Manager.

Call Information Service

The Call Information Service allows applications to get detailed call information and to determine the status of the call information link.

Computer Telephony Integration

Abbreviated as CTI. The integration of services provided by a computer and a telephone. In simplest terms, it means connecting a computer to a communications server (or switch) and having the computer issue commands that control calls.

CTI Link

The term CTI link refers to a generic link type that is used in the context of Communication Manager administration. As a generic link type, it can refer to any of the following AE Services links: CVLAN links, DLG links, and TSAPI links (JTAPI and the Telephony Web Service use TSAPI links). When an OAM Web page, such as TSAPI Service Summary, displays a column heading for a CTI link type, it is referring to TSAPI link as it is administered on Communication Manager. Up to 64 links can be administered on Communication Manager.

DMCC Service

Device, Media, and Call Control. The DMCC Service encompasses Device Control, Media Control, and Call Control capabilities. Device Control enables applications to monitor and control station lamps and displays. Media Control allows applications to direct media connections, play sounds, and interpret voice/tones on a media stream. Call Control allows applications to monitor and control calls.

JTAPI

Java Telephony Application Programming Interface. JTAPI is an API that provides access to the complete set of Third Party call control features provided by the TSAPI Service. JTAPI uses the TSAPI Service for communication with Communication Manager.

First Party Call Control

First party call control refers to the application acting as the user would operate their telephone. The application invokes operations such as “Go off-hook”, “Press button," and so forth, until the switch collects enough digits to initiate the call.

LDAP

Lightweight Directory Access Protocol. LDAP defines a standard protocol for organizing directory hierarchies and a standard interface for clients to access directory servers.

Link

A communications channel between system components.

Monitor

A monitor refers to a capability that watches for activity on a call or a device. A monitor placed on a device or a call causes reports of changes in the status of the device or call to be sent to the client requesting the monitor. If your application places a device monitor on your phone, your application is notified of changes in your phone's status (for example, an incoming call has been received, a call ended, and so forth). Many applications rely on monitors to provide this type of information.

Operations, Administration, and Maintenance

Abbreviated as OAM. The administrative interface for the Application Enablement Services platform. Now referred to as the AE Services Management Console.

PKI

Public Key Infrastructure. PKI is a system or framework that provides users of a non-secure public network to securely and privately exchange data through the use of a cryptographic key pair that is provided by a trusted authority, typically a Certificate Authority. A public key infrastructure includes of a certificate authority (CA), a registration authority (RA) and a means of managing certificates.

Private Data

Private data is a switch-specific software implementation that provides value added services.

PLDS

Product Licensing and Delivery System. AE Services 6.2 uses the PLDS for license management and software distribution.

Registration, Administration, and Status

Abbreviated as RAS. RAS is an International Telecommunications Union specification for terminal registration and authentication. RAS is part of the H.323 protocol suite.

Routing

Selecting an appropriate path for a call. When a routing application is started, it sends route registration requests, which contain a device ID, to Communication Manager. Routing requests instruct Communication Manager to send all incoming calls to these device IDs. The TSAPI or CVLAN Service sends the call to the application for routing. Communication Manager does not route these calls. Also referred to as adjunct routing.

RTP

Real-time Transport Protocol. RTP is an Internet standard for transmission of time-critical data, and for control of the transmission.

SIP

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.

SDK

Software Development Kit. An SDK is a package that enables a programmer to develop applications for a specific platform. Typically, an SDK includes one or more APIs, documentation, and perhaps programming tools.

Switch Connection Name

Switch Connection Name is a term that refers to either of the following: (1) A collection of Host Names or IP addresses associated with one (and only one) switch. This definition applies to the TSAPI Service, the Web Telephony Service, the CVLAN Service, and the DLG Service. (2) A collection of H.323 Gatekeepers that are associated with one (and only one) switch. AE Services supports up to 16 switch connections to Communication Manager. Switch Connection names, also referred to as switch connections can consist of multiple CLAN connections (up to 16).

Telephony Web Service

An interface that enables high level call control functionality over standard web services interfaces (SOAP/XML).The service hides the complicated concepts associated with traditional CSTA based call control such as connections, call identifiers and call states.

Third Party Call Control

Third party call control means that, rather than acting as the user, the application is making requests on the behalf of the user. A third-party make call says “Make a call from extension X to extension Y”.

Tlink

A Tlink is a service identifier that is created when the administrator adds a TSAPI Link in AE Services OAM. A Tlink refers to a switch connection between a specific switch and a specific AE Server.

Transport link

A transport link is a secure TCP/IP connection between the AE Services server and a CLAN on Communication Manager. When the AE Services Transport Service starts up, it establishes the transport link between the AE Services server and the Communication Manager server, based on administering a switch connection in AE Services Management Console.

The CLAN IP addresses that you administer from the Edit CLAN IPs page in AE Services Management Console are used to set up TLS connections between AE Services and Communication Manager. These TLS connections are called transport links.

TSAPI Service

The CSTA-based third party call control services provided by AE Services.

Web Services

A set of standards that allow a service to be described and consumed in a platform-neutral way.