© 2015-2020, 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 modify 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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of 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

Warranty 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, https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" 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.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in the Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” 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 as set forth below in the Designated System(s) License (DS) section as applicable. 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 computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) 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: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. 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. 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 any other name or directory entry contained in a navigable 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.

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”).
Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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, information, 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.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

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 products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product, in whole or in part, including any code and software. Customer acknowledges and agrees that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: https://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: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.
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, its licensors, its suppliers, 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.

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.
Contents

Chapter 1: Introduction ........................................................................................................ 8
  Purpose......................................................................................................................... 8
  Change history ............................................................................................................ 8

Chapter 2: Overview........................................................................................................... 9
  Avaya Aura® Application Enablement Services overview ........................................... 9
  Avaya Aura® applications deployment offers ............................................................... 9

Chapter 3: What’s new in Application Enablement Services ............................................. 11
  New in this release ...................................................................................................... 11
    New in Application Enablement Services Release 8.1.2.1 ........................................ 11
    New in Application Enablement Services Release 8.1.2 .......................................... 11
    New in Application Enablement Services Release 8.1.1 .......................................... 12
    New in Application Enablement Services Release 8.1 ............................................. 12
  Application Enablement Services feature matrix ...................................................... 14

Chapter 4: AE Services Product Summary .................................................................... 16
  Introduction ............................................................................................................... 16
  DMCC service ............................................................................................................. 16
  TSAPI service ............................................................................................................. 17
  Web services ............................................................................................................... 17
  CVLAN service .......................................................................................................... 18
  DLG service ................................................................................................................ 18
  AE Services configuration at a glance ....................................................................... 19

Chapter 5: Network Security and Reliability ................................................................. 20
  AE Services security features ..................................................................................... 20
  Secure application links ............................................................................................. 21
  AE Services link resiliency and failover .................................................................... 22
  Support for an Enterprise Survivable Server configuration ..................................... 22

Chapter 6: Guidelines for configuring AES .................................................................. 24
  Guidelines and requirements for configuring AE Services ....................................... 24
  Configurations that use AEP connections .................................................................. 25
  AE Services deployment on Appliance Virtualization Platform on Dell™ PowerEdge™ R620 .................................................. 25
  Guideline for upgrading AE Services to Release 7.x or 8.x on Appliance Virtualization Platform .................................................. 26

Chapter 7: AE Services Architecture ............................................................................ 27
  AE Services integration with Microsoft Office Communication Servers and Microsoft Lync
  Servers ...................................................................................................................... 27
  AE Services architecture at a glance ........................................................................ 29

Chapter 8: Session Initiation Protocol (SIP) ................................................................. 30
  SIP support ............................................................................................................... 30
  SIP limitations .......................................................................................................... 31
## Chapter 9: AE Services Licensing
- AE Services licensing summary ........................................................................... 33
- Application Enablement Protocol connections licensing .................................... 35
- AE Services integration for Microsoft Lync Server licensing .......................... 36
- Device, Media, and Call Control (DMCC) licensing ......................................... 36
- Web services licensing ..................................................................................... 38
- System Management Service (SMS) licensing ................................................ 38
- TSAPI service (including JTAPI) licensing ...................................................... 38
  - TSAPI basic user license ............................................................................. 38
  - TSAPI advanced license .......................................................................... 39
- CVLAN licensing .......................................................................................... 40
- DLG licensing .............................................................................................. 40
- Enterprise-wide licensing ............................................................................ 41
- Comparison of standard licensing and enterprise-wide licensing ................. 41
- Licensing configuration examples ................................................................ 42
  - Standard licensing .................................................................................. 42
  - Enterprise-wide licensing — allocating licenses or features ................. 43
  - Enterprise-wide licensing — pointing to a master license on a remote server 44

## Chapter 10: Application Enablement Services Client and SDKs
- Application Enablement Services Client and SDKs ........................................ 45

## Chapter 11: Communication Manager features not supported with AE Services
- Communication Manager features not supported ............................................ 46

## Chapter 12: Capacities for AE Services
- Configuring hardware resources to support AE Services footprint flexibility .... 48
- Capacities for AE Services on Appliance Virtualization Platform .................. 49
- AE Services integration for Microsoft Office Communication Server .......... 49
- Capacities for calls in DMCC applications ..................................................... 50
  - Additional AE Services Restrictions ...................................................... 55
- Communication Manager capacities for DMCC ........................................... 56
  - Additional Communication Manager restrictions ................................... 56
- System capacities – Communication Manager ............................................. 57
- System capacities of the AE Services server ............................................... 57
- ASAI associations ...................................................................................... 58
- ASAI capacities ......................................................................................... 58
- CVLAN service capacities ......................................................................... 58
- DLG service capacities ............................................................................. 59
- TSAPI service capacities .......................................................................... 59
- System Management Services capacities .................................................. 59

## Chapter 13: AE Services Documentation
- Select documents based on products you use ............................................. 60
- Guidelines for selecting documents based on your role within an organization 60
  - Planners ............................................................................................... 60
  - Installers and administrators — VMware offer ....................................... 61
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installers and administrators — Software-Only offer</td>
<td>61</td>
</tr>
<tr>
<td>Application developers</td>
<td>62</td>
</tr>
<tr>
<td><strong>Chapter 14: Resources</strong></td>
<td>66</td>
</tr>
<tr>
<td>Application Enablement Services documentation</td>
<td>66</td>
</tr>
<tr>
<td>Finding documents on the Avaya Support website</td>
<td>67</td>
</tr>
<tr>
<td>Accessing the port matrix document</td>
<td>68</td>
</tr>
<tr>
<td>Avaya Documentation Portal navigation</td>
<td>68</td>
</tr>
<tr>
<td>Training</td>
<td>69</td>
</tr>
<tr>
<td>Viewing Avaya Mentor videos</td>
<td>69</td>
</tr>
<tr>
<td>Support</td>
<td>70</td>
</tr>
<tr>
<td>Using the Avaya InSite Knowledge Base</td>
<td>70</td>
</tr>
<tr>
<td><strong>Appendix A: AE Services compatibility</strong></td>
<td>72</td>
</tr>
<tr>
<td>API and client compatibility</td>
<td>72</td>
</tr>
<tr>
<td>Product compatibility</td>
<td>73</td>
</tr>
<tr>
<td>AE Services compatibility with Communication Manager Release 8.1.2 CTI interfaces</td>
<td>73</td>
</tr>
<tr>
<td>Communication Manager Release 8.1.2 — ASAI capabilities</td>
<td>73</td>
</tr>
<tr>
<td><strong>Glossary</strong></td>
<td>75</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

Purpose

This document describes tested characteristics and capabilities of Avaya Aura® Application Enablement Services, including feature descriptions, interoperability, performance specifications, security, and licensing requirements.

This document is intended for anyone who wants to gain a high-level understanding of Avaya Aura® Application Enablement Services features, functions, capacities, and limitations within the context of solutions and verified reference configurations.

Change history

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>June 2020</td>
<td>• Added the New in Application Enablement Services Release 8.1.2 on page 11 section.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated the Communication Manager capacities for DMCC on page 56 section.</td>
</tr>
<tr>
<td>5</td>
<td>April 2020</td>
<td>Updated the Avaya Aura applications deployment offers on page 9 section.</td>
</tr>
<tr>
<td>4</td>
<td>March 2020</td>
<td>Added the New in Application Enablement Services Release 8.1.2 on page 11 section.</td>
</tr>
<tr>
<td>3</td>
<td>November 2019</td>
<td>Updated the SIP support on page 30 section.</td>
</tr>
<tr>
<td>2</td>
<td>October 2019</td>
<td>Updated the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Application Enablement Services feature matrix on page 14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• API and client compatibility on page 72</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web services programmers on page 62</td>
</tr>
<tr>
<td>1</td>
<td>June 2019</td>
<td>Release 8.1 document</td>
</tr>
</tbody>
</table>
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.

Avaya Aura® applications deployment offers

Avaya Aura® supports the following deployment offers:

• Avaya Aura® Virtualized Appliance (VA): Avaya-provided server, Avaya Aura® Appliance Virtualization Platform, based on the customized OEM version of VMware® ESXi 6.5.

• Avaya Aura® Virtualized Environment (VE): Customer-provided VMware infrastructure and Kernel-based Virtual Machine (KVM).

• Avaya Aura® on Infrastructure as a Service: Amazon Web Services, Microsoft Azure, Google Cloud Platform, and IBM Bluemix.

• Software-only environment: Deployment on the Red Hat Enterprise Linux operating system.
Note:

From Release 8.1.2 and later, Avaya Aura® does not provide ISO or OVA files for the following deployment offers:

- Avaya Aura® on Infrastructure as a Service: Amazon Web Services, Microsoft Azure, Google Cloud Platform, and IBM Bluemix.
- Software-only environment: Deployment on the Red Hat Enterprise Linux operating system.

You must install Application Enablement Services feature pack files to upgrade to Release 8.1.2 and later.

Application Enablement Services using Avaya Aura® Appliance Virtualization Platform

Avaya uses the VMware®-based Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications in Avaya Aura® Virtual Appliance offer.

Avaya Aura® Virtual Appliance offer includes:

- S8300E

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 6.0 and later. With Appliance Virtualization Platform, customers can run any combination of supported applications on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements.
Chapter 3: What’s new in Application Enablement Services

This chapter provides an overview of the new and enhanced features of Application Enablement Services Release 8.1.x.

For more information about these features and administration, see:

- Administering Avaya Aura® Application Enablement Services
- Deploying Avaya Aura® Application Enablement Services in Virtualized Environment
- Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment
- Deploying Avaya Aura® Application Enablement Services in Infrastructure as a Service Environment
- Deploying Avaya Aura® Application Enablement Services in Virtual Appliance
- Upgrading Avaya Aura® Application Enablement Services

New in this release

New in Application Enablement Services Release 8.1.2.1

From Release 8.1.2.1, Application Enablement Services is a part of Avaya IX™ Subscription offer.

For more information about Avaya IX™ Subscription offer, see Avaya Support website at http://support.avaya.com.

New in Application Enablement Services Release 8.1.2

Application Enablement Services Release 8.1.2 supports the following new features and enhancements:

Data Privacy

- **Data Encryption**: You can enable or disable data encryption for Avaya Aura® applications at the time of deployment. Data Encryption is supported only for Appliance Virtualization
Platform and VMware Virtualized environments. Once you deploy the application with data encryption, you cannot disable data encryption after deployment and vice-versa.

- **Support for Log and Trace Retention**: You can set the retention period for retaining logs and traces from 0 to 180 days. The saved log and trace files are deleted after the retention period is reached. You can set the retention period via OAM and CLI.

- **Support for Clearing Logs and Traces**: You can clear the logs and traces for a certain period or you can choose to clear all the logs and traces irrespective of the number of days. You can set the clearing period via OAM and CLI.

- **Support for Auto Log and Trace Delete**: When logs disk reaches 90% occupancy, AE Services will automatically delete the oldest logs and traces till the time when the occupancy reaches 75%.

**Support for 12–Party Conferencing**
With Release 8.1.2, AE Services supports 12 participants for ad-hoc and meet-me conferences.

---

**New in Application Enablement Services Release 8.1.1**

**Support for Location Parameter**
With Release 8.1.1, the Locations model in the System Management Service (SMS) supports setting and retrieving the Locations Parameter value. You can set the area code for each location and administer different location information for each location. With this feature, you can administer multiple location specifications. Otherwise, information for Location 1 applies to all locations.

The Location Parameter (Loc_Param) is supported with the SMS Software Development Kit (SDK). For more information, see the Model documentation on the SMS test page.

**VMware console for applications**
With Release 8.1.1, you can open the VM console in a new browser window or on a new browser tab for the application that reside on Appliance Virtualization Platform Release 7.1.2 and later.

Based on the role of the user, you can assign the permissions for accessing the console.

---

**New in Application Enablement Services Release 8.1**

Application Enablement Services Release 8.1 supports the following new features and enhancements:

**Appliance Virtualization Platform Hypervisor**
With Release 8.1, Appliance Virtualization Platform is based on the customized OEM version of VMware® ESXi 6.5.

**Support of Clear Alarm for License Normal mode**
With Release 8.1, AE Services sends a clear alarm notification that clears temporary license error alarms, when the license state returns to a Normal state from the license grace period state. This distinguishes license errors generated between transient state and network fluctuations.
Prior to Release 8.1, the license grace period alarms were generated but not cleared when the license state returned to normal mode. With this enhancement, AE Services sends the license clear alarm to notify the system administrator of the normal state of license mode.

**Support for a videoCall private data parameter**

With AE Services Release 8.1, a new private data parameter videoCall is added in CSTA Service Make call, Answer call, Consultation call and Single step transfer call requests, if CTI application requests endpoints to send and/or receive video stream.

Supported values for videoCall parameter are:

- **DISABLED**: No Video support required. This is the default value.
- **INCOMING**: Application requests endpoint to only receive video from far-end.
- **TWOWAY**: Application requests endpoint to send/receive video to/from far-end.

AE Services Release 8.1 also supports Channel Type in CSTA Originated event to identify an incoming SIP trunk calls as either Voice or Video via CTI.

**Support for G.722 codec**

With AE Services Release 8.1, call recording supports G.722 codec for DMCC applications in Client media mode. This enables DMCC applications to record end-to-end High Definition Media Stream.

**Support for command line utilities for configuring AE Services using CLI**

With Release 8.1, you can seamlessly configure AE Services in an automated manner through the command line interface. To facilitate this, the following command line utilities are provided:

- Switch Connection and CTI link
- Licensing
- Security Database
- Networking Configuration
- Certificate Management
- User Management
- SNMP configuration

**Enhancements to the 16-digit extension**

With Release 8.1, Avaya Aura® applications extend support for configuration of 16-digit extension to the following Communication Manager objects.

- hunt groups

  ✷ **Note:**

  Administration of hunt group with 16-digit group extension and group members.

- coverage answer groups
- ELIN
- abbr dial buttons
- Listed Directory Number
**Supported browsers**

- Internet Explorer 11
- Mozilla Firefox 65, 66, and 67

**Support for Red Hat Enterprise Linux operating system 7.6**

With Release 8.1, you can deploy and upgrade Avaya Aura® applications on the Red Hat Enterprise Linux operating system 7.6.

---

**Application Enablement Services feature matrix**

The following table lists the feature matrix of Application Enablement Services.

*Note:*

The features listed in the following table are not a comprehensive feature list. It only covers the new features.

<table>
<thead>
<tr>
<th>Feature name</th>
<th>Release 7.1.x</th>
<th>Release 8.0.x</th>
<th>Release 8.1 and Release 8.1.1</th>
<th>Release 8.1.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVA signing</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>IPv6 support</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Enhanced Access Security Gateway (EASG)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Compliance with DISA security STIGs</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Multi factor authentication</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Support for TLS 1.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Customer Root Access</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Preserve security hardening modes on upgrade</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Support for 16-digit dial plan</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Support for Software-only deployment</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Support for Hyper-V in Software-Only environment</td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Support for third-party software in Software-Only environment</td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Feature name</th>
<th>Release 7.1.x</th>
<th>Release 8.0.x</th>
<th>Release 8.1 and Release 8.1.1</th>
<th>Release 8.1.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support of Held Call ID on auto dial request by Application Enablement Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for Avaya Solutions Platform 120 Appliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for Avaya Solutions Platform 130 Appliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for G.722 codec</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for 12–Party Conferencing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* – OVA is available for VMware and not for KVM.
Chapter 4: AE Services Product Summary

Introduction

AE Services provides a platform that supports existing contact center application requirements, along with new, emerging Application Programming Interfaces (APIs). AE Services provides programs that perform specific functions and provide 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 19.

DMCC service

The Device, Media, and Call Control (DMCC) service provides third-party call control and first-party call control (device control and media control). The DMCC SDK provides a Java, XML and .NET API. For more information about the DMCC SDKs, see SDKs on page 45.

• DMCC first-party call control (1PCC)

  - DMCC with Device Control can 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.
• System Services

System Services allows applications to request and receive health status of a TSAPI TLink.

System Services also allows applications to request and receive events on the status of TSAPI CTI (Tlink) connections between the AE Services server and the Communications Manager(s). Once an application is registered, notification events are sent when the Tlink status changes for example linkUp/linkDown for the switches for which it has registered.

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.

The second phase 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 45.

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 45.
System Management Service
The System Management Service reveals the 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 Adjunct/Switch Application Interface (ASAI) messages with the AE ServicesServer. 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.

Note:
If 12–Party Conferencing is enabled on Communication Manager, the DLG CTI application will not work on AE Services.
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 “Chapter 5: Security Administration and Additional PAM Management” in the Avaya Application Enablement Services Administration and Maintenance Guide. This document and other related information is located on the Avaya Support Web site [http://www.avaya.com/support](http://www.avaya.com/support).
Secure application links

You can configure all the AE Services APIs to use secure application links. The AE Services server comes pre-installed with a set of default server certificates for lab use, that is out-of-the-box deployments. These default server certificates should not be used in a production environment. It is highly recommended to replace all default installed certificates using your own Public Key Infrastructure or a third party vendor.

Note:

The CA used to sign the server default certificate has changed. In order to allow your client to connect to the AE Services server using a TLS socket connection for lab testing, the new AE Services CA certificate will need to be exported from the server and imported into your client trust store.

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 Services 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
- Administering Avaya Aura® Application Enablement Services

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.

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.

Note:

Default server certificates should not be used in a production environment. It is highly recommended to replace all default installed certificates using your own Public Key Infrastructure or a third party vendor.
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.

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 for configuring AES

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 that is, first-party call control, 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 25.
- 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 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.
- The AE Services 7.0.x and later WebLM license will be preserved during a VMware offer type upgrade when Solution Deployment Manager 7.1 and later is used to perform the AE Services OVA upgrade.

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 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

AE Services deployment on Appliance Virtualization Platform on Dell™ PowerEdge™ R620

- You can deploy AE Services Profile 1 on Appliance Virtualization Platform on Dell R620 (4 NIC card) Server as Profile 1 does not require dedicated NIC.
- You can deploy AE Services Profile 2 or Profile 3 on Appliance Virtualization Platform without CM duplex or NIC bonding on Dell R620 (4 NIC card) Server.
- You cannot deploy AE Services Profile 2 or Profile 3 on Appliance Virtualization Platform with CM duplex or NIC bonding on Dell R620 (4 NIC card) Server as Profile 2 or Profile 3 requires dedicated NIC.
Guideline for upgrading AE Services to Release 7.x or 8.x on Appliance Virtualization Platform

In high traffic situations, use Profile 2 or 3 of AE Services with a dedicated Private IP and NIC.

If you are upgrading AE Services to Release 7.x or 8.x on Appliance Virtualization Platform and you only have 4 NIC ports, you can enable only limited services. Dell™ PowerEdge™ R620 Server has only 4 NIC cards. For more information, see PSN020394u.

If you will configure NIC Teaming (alias Bonding) on a 4 NIC Port Server (Dell™ PowerEdge™ R620), you cannot use a private NIC port associated with AE Services. The private NIC port requires additional NIC Port 5. If you are not configuring NIC Teaming, you can use the one port out of four for a dedicated Private IP on the 4th NIC.
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 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 Services 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 Deploying Avaya Aura® Application Enablement Services for Microsoft® Lync Server Products, 02-601893.
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), and 9601 (SIP Only) with firmware version 2 or greater and Avaya 16CC with all firmware versions.

AE Services 8.0.1 and later support J169 and J179 series phones with SIP 2.0 firmware. The station type should be set to 96x1SIP or 96x1SIPCC in case of 1PCC operation for Communication Manager 8.0. From Communication Manager Release 8.0.1, you can use J169 or J179 template.

The requirements for SIP support are as follows:

- Communication Manager 5.0 or later
- Session Manager

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

The following table lists the SIP endpoints that have been tested to date.

In general, all AE Services third-party call control functions are supported for these SIP endpoints, except for the limitations outlined in the next section.

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>Administered as</th>
<th>Endpoint Firmware</th>
<th>AE Services Release</th>
<th>Communication Manager/Session Manager Pair</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Communication Manager- ES Release</td>
</tr>
<tr>
<td>9620</td>
<td>9620SIP</td>
<td>2.6 SP12</td>
<td>8.1.x</td>
<td>8.1.x</td>
</tr>
<tr>
<td>9640</td>
<td>9640SIP</td>
<td>2.6 SP12</td>
<td>8.1.x</td>
<td>8.1.x</td>
</tr>
</tbody>
</table>

Table continues…
### 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 30. 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 30, except the following capabilities:

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

Microsoft Office Communications Server (OCS) integration

All third-party call control capabilities are supported for the endpoints listed in SIP support on page 30, 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 35
- AE Services integration for Microsoft Lync Server licensing on page 36
- Device, Media, and Call Control (DMCC) licensing on page 36
- Web services licensing on page 38
- System Management Service (SMS) licensing on page 38
- TSAPI service (including JTAPI) licensing on page 38
- CVLAN licensing on page 40
- DLG licensing on page 40
- Enterprise-wide licensing on page 41
- Comparison of standard licensing and enterprise-wide licensing on page 41
- Licensing configuration examples on page 42

<table>
<thead>
<tr>
<th>AE Services product or service</th>
<th>Required feature licensed on Communication Manager</th>
<th>Optional feature licensed on Communication Manager</th>
<th>AE Services feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>AE Services Integration with Office Communications Server</td>
<td>Use display system-parameters customer-options command to see if the feature is provided by the Communication Manager License.</td>
<td>Use WebLM to see if this feature is provided by the Application Enablement License.</td>
<td>Unified Desktop</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>AE Services product or service</th>
<th>Required feature licensed on Communication Manager</th>
<th>Optional feature licensed on Communication Manager</th>
<th>AE Services feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMCC - Device and Media Control</td>
<td>Use display system-parameters customer-options command to see if the feature is provided by the Communication Manager License.</td>
<td>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.</td>
<td>Use WebLM to see if this feature is provided by the Application Enablement license.</td>
</tr>
</tbody>
</table>
| 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 36. | None | Device, Media, and Call Control |
| 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…
<table>
<thead>
<tr>
<th>AE Services product or service</th>
<th>Required feature licensed on Communication Manager</th>
<th>Optional feature licensed on Communication Manager</th>
<th>AE Services feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVLAN Service (Avaya Interaction Center)</td>
<td>Use display system-parameters customer-options command to see if the feature is provided by the Communication Manager License.</td>
<td>Use WebLM to see if this feature is provided by the Application Enablement license.</td>
<td>CVLAN Proprietary Links</td>
</tr>
<tr>
<td>CVLAN Service (Non-Avaya applications)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note: ASAI Core and ASAI Plus are included for one Communication Manager server when purchasing the CVLAN service.</td>
<td>ASAI Core</td>
<td>Increased Adjunct Route Capacity (for adjunct routing applications)</td>
<td>CVLAN ASAI</td>
</tr>
<tr>
<td>DLG Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note: ASAI Core and ASAI Plus are included for one Communication Manager server when purchasing the DLG service.</td>
<td>ASAI Core</td>
<td>Increased Adjunct Routes</td>
<td>DLG</td>
</tr>
</tbody>
</table>

**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 25. 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 Lync Server licensing**

The AE Services integration with Microsoft Lync Server 2010 and 2013 requires the Unified Desktop Edition RTU (Right To Use) license.

Every active Microsoft 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 Lync client, not only those in the call).

For more information, see *Deploying Avaya Aura® Application Enablement Services for Microsoft® Lync Server Products*, 02-601893.

---

**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, literally doubling the quantity of DMCC Basic licenses with every order.

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:**

Contact your Account Team to reconcile any DMCC double licensing.
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.

DMCC/CMAPI Double Licensing Reconciliation Process
When Application Enablement Services (AES) was deployed on Communication Manager (CM) releases prior to 6.x, DMCC Basic (formerly known as CMAPI Basic) licenses were also included in the CM license file as IP_API_A licenses as well as in the AE Services license file for compatibility reasons. This meant Avaya literally doubled the quantity of DMCC Basic licenses with every order which still continues today (for example AE Services 6.3.3 deployed on a CM 5.2.x). This is creating a discrepancy between the customer’s quantities purchased and the actual licenses in place and should be reconciled when the customer’s CM release is upgraded to 6.x or newer, and or an AE Services upgrade or SA/UA recast (with existing CM 6+) or a license move is requested in a CM 6.x (or later) environment.

Account teams are responsible to initiate reconciliations and should perform an analysis of current license quantities. Once this analysis has been completed, Avaya Product Operations should be engaged to make the actual corrections within Avaya’s licensing tools. The following tasks should be performed by the account team with the customer:

- Verify the license quantities in AES, CM, and PLDS.
- Verify the license quantities purchased.
- If the customer has licenses that were not purchased, determine the total license quantities along with the quantities that are in use.
  - Determine the quantities to be purchased and/or removed.
  - If licenses will be removed, determine what platform (CM, AES, PLDS) they will be removed from and the associated quantities.

The following additional information will assist in determining an accurate inventory count of the DMCC / CMAPI Basic licenses:

Note:
Some CM releases included a licensing quantity of 4-IP_API_As so the total license count may need to reflect this quantity.

Note:
Avaya Self-Service Offers add some additional complexity to determining the total license count because they use the IP_API_A with Voice Portal and Experience Portal H.323 connections and our Self-Service Offers support CM 6.x and 7.x (along with pre-PLDS CMs: CM 5.2.x with RFA). This needs to be taken into account in any reconciliation.
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.
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.
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

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 server 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 41.
- For examples of licensing configurations, see [Licensing configuration examples](#) on page 42.

## Comparison of standard licensing and enterprise-wide licensing

<table>
<thead>
<tr>
<th>Standard licensing</th>
<th>Enterprise-wide licensing</th>
</tr>
</thead>
<tbody>
<tr>
<td>The 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.</td>
<td>Enterprise-wide licensing includes a master enterprise license file (ELF) and an allocation license file (ALF).</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>With standard licensing, a license can not be moved from one server to another, and capacities can not be reallocated.</td>
<td>With enterprise-wide licensing, you can reallocate enterprise capacities and features as desired.</td>
</tr>
</tbody>
</table>
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 Software-only offer, 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.

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)

| WebLM administration - use default settings |
| AE Services administration - use default settings |

AE Server Administration
Administer WebLM IP address to point to local, standalone WebLM server (use default - 127.0.0.1)

AE Services

WebLM Server Address

 Local WebLM 127.0.0.1

AE Services acquires license

Standard License File (SLF)

Note:
The default IP address, 127.0.0.1, shown in the illustration above is for both, the AE Services Software-only offer and VMware offer.
Enterprise-wide licensing — allocating licenses or features

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. 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:

System Platform Administration
Administrator WebLM IP address to point to Local WebLM Server
(use default -127.0.0.1)

WebLM Administration
Administrator Web LM on Master WebLM Server
- Add Local WebLM
- Allocate Licenses

Application Enablement Services on System Platform
(Local WebLM Server)
135.8.17.123

AE Services
AE Services acquires license

Local WebLM
127.0.0.1

Allocate license

Master WebLM Server
135.8.17.122

Master WebLM
Enterprise License File (ELF)

Allocation License file
ALF

Note: The IP addresses in this example are not valid IP address. They are used as examples only.
**Note:**
Beginning with AE Services 7.0, System Platform is not supported.

---

**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.

**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.

---

**Note:**
Beginning with AE Services 7.0, System Platform is not supported.
Chapter 10: Application Enablement Services Client and SDKs

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Distribution</th>
<th>Material code/URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Enablement Services TSAPI SDK</td>
<td>Contact your account executive</td>
<td>700500048</td>
</tr>
<tr>
<td>Application Enablement Services TSAPI client</td>
<td></td>
<td>700510417</td>
</tr>
<tr>
<td>Application Enablement Services CVLAN client</td>
<td>Avaya DevConnect Developer Program</td>
<td><a href="http://www.avaya.com/devconnect">www.avaya.com/devconnect</a></td>
</tr>
<tr>
<td>Application Enablement Services DMCC Java SDK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Enablement Services DMCC XML SDK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Enablement Services DMCC .NET SDK supporting .NET Framework 4.5.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Enablement Services Web Service — Telephony Web Svc SDK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Enablement Services JTAPI SDK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Enablement Services SMS SDK</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 11: Communication Manager
features not supported with AE Services

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.

Communication Manager Attendant Console monitoring by ASAI (CTI)
The Communication Manager Attendant Console cannot be monitored by ASAI (CTI), and recording functions are not possible.

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.

Device, Media, and Call Control (DMCC) does not support the extensions of digits in length.

• 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:
For a given call appearance, ASAI can only administer configurations with up to 16 bridged appearances and other Communication Manager group features in total.
• **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.

**Meet-me Conference feature**

The Meet-me Conference feature is not supported in AE Services.
Chapter 12: Capacities for AE Services

This chapter provides the capacities for AE Services.

Configuring hardware resources to support AE Services footprint flexibility

About this task
Use this procedure to reconfigure hardware resources to support AE Services footprint flexibility.

Procedure
1. Connect to the host or cluster using the VMware vSphere client.
2. Log in using the admin login and password.
3. Power off the virtual machine:
   a. Right-click on the virtual machine name.
   b. Select Power > Shut Down Guest.
   c. Click Yes in the Shutdown Confirmation dialog box.
4. Right-click on the virtual machine name and select Edit Settings.
5. Change the Memory Configuration:
   a. Click on the Hardware tab.
   b. Click Memory.
   c. Change the Memory Size to the appropriate limit.
   d. (Optional) Click on the Resources tab.
   e. (Optional) Select Memory,
   f. (Optional) Verify the Reservation is set correctly.
   g. (Optional) clear the Unlimited checkbox.
   h. (Optional) Verify the Limit slide is set to the same value as the Reservation.
6. Change the CPU configuration:
   a. Click the Hardware tab.
   b. Select CPUs.
   c. Change the Number of virtual sockets according to the limit requirement.
   d. (Optional) Click on the Resources tab.
   e. (Optional) Select CPU.
   f. (Recommended) Verify the Reservation is set correctly.
      Avaya recommends the Reservation be set to the value of multiplying the number of CPUs by 2190. For example, if the number of CPUs is 4, the Reservation should be set to 8760. One CPU should be equal to 2190.
   g. (Optional) Uncheck the Unlimited checkbox.
   h. (Optional) Verify the Limit slide is set to the same value as the Reservation.

7. Click OK.

8. Wait until the virtual machine finishes the reconfiguration procedure.


---

**Capacities for AE Services on Appliance Virtualization Platform**

You can deploy multiple AE Services instances on Appliance Virtualization Platform.

For example, HP DL 360 G9 Profile 3 with the hardware specifications (32 GB RAM, 12 vCPUs with 2.4 GHz, and 300 GB HDD) can have up to 6 AE Services instances of Profile 1 (1 CPU, 4 GB).

---

**AE Services integration for Microsoft Office Communication Server**

<table>
<thead>
<tr>
<th>Microsoft Office Communicator Clients per AE Server</th>
<th>Support for up to 20,000 concurrent clients at 24,000 BHCC.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AE Server dedicated to Microsoft Office Communicator integration.</td>
<td>Support for up to 5,000 concurrent OC clients at 6000 BHCC and 2000 DMCC clients in client media mode at 36,000 BHCC.</td>
</tr>
<tr>
<td>Microsoft Office Communicator and other API traffic.</td>
<td></td>
</tr>
</tbody>
</table>
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 50 and Table 2: Server media on page 52 with the Communication Manager resources and capacities described in capacities for DMCC on page 56 to ensure that you have adequate Communication Manager resources for a given DMCC implementation.

*Note:*

Registration per call for recorders in the high traffic call centers are not supported.

These capacities are based on the AE Services Profile 3.

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

<table>
<thead>
<tr>
<th>Session and H323 Signaling Encryption Profile</th>
<th>AE Server Capacity</th>
<th>Traffic Rate for Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>8,000 endpoints and a 36,000 BHCC on the Avaya Common Servers.</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Session and H323 Signaling Encryption Profile</th>
<th>AE Server Capacity</th>
<th>Traffic Rate for Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN-EKE</td>
<td>3,200 endpoints and a 28,800 BHCC on the Avaya Common Servers.</td>
<td>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 utilized with 4 registrations per CLAN; and so forth).</td>
</tr>
<tr>
<td>H323TLS</td>
<td>2,000 endpoints and a 18,000 BHCC on the Avaya Common Servers. For more information see, Additional AE Services Restrictions on page 55.</td>
<td>AE Services and Communication Manager can support up to 20 registration, when sent by an application, in a 10-second interval. Avaya recommends 5 registrations per CLAN. 4 CLANs can fulfill the capacity for 20 registrations. Note: The 20 registrations in a 10-second limit applies for Processor Ethernet as well.</td>
</tr>
</tbody>
</table>

Note:
- The 20 registrations in a 10-second limit applies for Processor Ethernet as well.
### Table 2: Server media

<table>
<thead>
<tr>
<th>Code type</th>
<th>AE Server capacity</th>
<th>Traffic rate for applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>No signaling and media encryption</td>
<td>G729</td>
<td>120 endpoints</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AE Services and Communication Manager can support up to 100 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).</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Code type</th>
<th>AE Server capacity</th>
<th>Traffic rate for applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>G711</td>
<td>75 endpoints</td>
<td>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).</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Code type</th>
<th>AE Server capacity</th>
<th>Traffic rate for applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signaling and media encryption</td>
<td>G729</td>
<td>96 endpoints</td>
</tr>
</tbody>
</table>

AE Services and Communication Manager can support up to 96 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 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 utilized with 4 registrations per CLAN; and so forth).

Table continues…
### Capacities for calls in DMCC applications

<table>
<thead>
<tr>
<th>Code type</th>
<th>AE Server capacity</th>
<th>Traffic rate for applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>G711</td>
<td>60 endpoints</td>
<td>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 utilized with 4 registrations per CLAN; and so forth).</td>
</tr>
</tbody>
</table>

**Note:**

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

---

### 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.
# Communication Manager capacities for DMCC

These capacities are based on the AE Services Profile 3.

<table>
<thead>
<tr>
<th>Component</th>
<th>Capacity</th>
</tr>
</thead>
</table>
| 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 56 |
| Processor Ethernet | • 400 DMCC station registrations for Communication Manager running on S83xx series servers  
• 8000 DMCC station registrations for Communication Manager common servers  
**Note:** This capacity is per AE Services server.  
For more information, see Additional Communication Manager Restrictions on page 56 |

## 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 Manager and non FIPS Communication Manager 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.

---

**System capacities – Communication Manager**

For information about Communication Manager system capacities, see Avaya Aura® Communication Manager System Capacities Table on [http://support.avaya.com/](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 2000 msgs/sec.

For more information about Spectre and Meltdown fixes included in Avaya Aura® Release 7.1.3 and 8.0, see PSN020346u on the Avaya Support site at: [https://downloads.avaya.com/css/P8/documents/101048606](https://downloads.avaya.com/css/P8/documents/101048606).

---

**System capacities of the AE Services server**

<table>
<thead>
<tr>
<th>Component</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication Manager servers supported by one AE Services Server</td>
<td>16</td>
</tr>
<tr>
<td>Connections to a Communication Manager server with one AE Services server</td>
<td>16</td>
</tr>
<tr>
<td>Messages per second per AE Services Server connection:</td>
<td></td>
</tr>
<tr>
<td>To Communication Manager (1 CLAN)</td>
<td>200</td>
</tr>
<tr>
<td>From Communication Manager (1 CLAN)</td>
<td>240</td>
</tr>
</tbody>
</table>

*Table continues…*
### Component Capacities

<table>
<thead>
<tr>
<th>Component</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages per second per AE Services Server connection to and from Communication Manager (processor ethernet)</td>
<td>2000</td>
</tr>
<tr>
<td>Messages per second (per system)</td>
<td>2000</td>
</tr>
<tr>
<td>See Note below.</td>
<td></td>
</tr>
</tbody>
</table>

**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.

---

### ASAI associations

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

### ASAI capacities

If you are using ASAI, you can administer up to 16 bridged appearances and other Communication Manager group features, such as Answer Coverage Group, in total.

---

### CVLAN service capacities

<table>
<thead>
<tr>
<th>Component</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clients supported</td>
<td>60</td>
</tr>
<tr>
<td>ASAI associations</td>
<td>128,000, shared over 16 links</td>
</tr>
<tr>
<td>Links</td>
<td>16</td>
</tr>
</tbody>
</table>
### DLG service capacities

<table>
<thead>
<tr>
<th>Component</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clients supported</td>
<td>16</td>
</tr>
<tr>
<td>Links</td>
<td>16</td>
</tr>
</tbody>
</table>

### TSAPI service capacities

<table>
<thead>
<tr>
<th>Component</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users (client connections)</td>
<td>2500 TLinks</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Links</td>
<td>16 (each to a different Communication Manager)</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
</tr>
<tr>
<td>For any AE Server, there may be only one TSAPI link to any given Communication Manager.</td>
<td></td>
</tr>
</tbody>
</table>

### System Management Services capacities

<table>
<thead>
<tr>
<th>Component</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simultaneous Communication Manager Servers</td>
<td>16</td>
</tr>
<tr>
<td>Simultaneous sessions/logins per Communication Manager</td>
<td>5</td>
</tr>
<tr>
<td>Single session – average number of Web requests serviced for station model</td>
<td>~6 requests/second</td>
</tr>
<tr>
<td>Multiplexed sessions – average number of Web requests serviced for station model</td>
<td>~10 requests/second</td>
</tr>
</tbody>
</table>
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.

• **Administering Avaya Aura® Application Enablement Services, Maintaining Avaya Aura® Application Enablement Services.**

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

Comments on this document? infodev@avaya.com
documents for more information. The following sections provide information about using additional
documents for implementing Application Enablement Services.

**AE Services integration with Microsoft Lync Server 2010 and 2013**

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

- *Deploying Avaya Aura® Application Enablement Services for Microsoft® Lync Server Products*, 02–601893
- *Deploying Avaya Aura® Application Enablement Services in Software-Only Environment*, 02–300355. If your integration uses the AE Services Software-Only server, consult this document for information about installing AE Services.
- *Administering Avaya Aura® Application Enablement Services*. 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 — VMware offer**

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

- *Deploying Avaya Aura® Application Enablement Services in Virtualized Environment*
- *Administering Avaya Aura® Application Enablement Services*

**Note:**

AE Services does not assume that you will install a browser on the AE Services. 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 Services.

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

---

**Installers and administrators — Software-Only offer**

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

- *Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment.*
- *Administering Avaya Aura® Application Enablement Services.*
**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, see *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 45.

**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](http://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 introduced the following SMS features:
  
  - XML formatted input and output
  - Template look and feel
  - Unicode support
  - ISV model schema enhancements
  - Location parameter field in the PHP output

- **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
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 *Administering Avaya Aura® Application Enablement Services*.
- 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.
# Chapter 14: Resources

## Application Enablement Services documentation

The following table lists the documents related to Application Enablement Services. Download the documents from the Avaya Support website at [http://support.avaya.com](http://support.avaya.com).

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Design</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Aura® Application Enablement Services Overview and Specification</td>
<td>Understand high-level product features and functionality.</td>
<td>Customers and sales, services, and support personnel</td>
</tr>
<tr>
<td>Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide</td>
<td>Installing TSAPI and CVLAN Client and SDK</td>
<td>Customers and sales, services, and support personnel</td>
</tr>
<tr>
<td><strong>Using</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upgrading Avaya Aura® Application Enablement Services</td>
<td>Upgrading Application Enablement Services applications.</td>
<td>System administrators and IT personnel</td>
</tr>
<tr>
<td>Administering Avaya Aura® Application Enablement Services</td>
<td>Administering Application Enablement Services applications and install patches on Application Enablement Services applications.</td>
<td>System administrators and IT personnel</td>
</tr>
<tr>
<td><strong>Implementation</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deploying Avaya Aura® Application Enablement Services for Microsoft® Lync Server Products</td>
<td>Deploy Application Enablement Services applications in Microsoft Lync Server Products</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Deploying Avaya Aura® Application Enablement Services in Virtual Appliance</td>
<td>Deploy Application Enablement Services applications in Virtual Appliance</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Deploying Avaya Aura® Application Enablement Services in Virtualized Environment</td>
<td>Deploy Application Enablement Services applications in Virtualized Environment</td>
<td>Implementation personnel</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploying Avaya Aura® Application Enablement Services in Infrastructure as a Service Environment</td>
<td>Deploy Application Enablement Services applications in Infrastructure as a Service Environment</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment</td>
<td>Deploy Application Enablement Services applications in Software-Only Environment</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Maintenance and Troubleshooting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintaining Avaya Aura® Application Enablement Services</td>
<td>Maintaining Application Enablement Services applications and install patches on Application Enablement Services applications.</td>
<td>System administrators and IT personnel</td>
</tr>
</tbody>
</table>

Related links
- Finding documents on the Avaya Support website on page 67
- Accessing the port matrix document on page 68
- Avaya Documentation Portal navigation on page 68

---

Finding documents on the Avaya Support website

Procedure

1. Go to [https://support.avaya.com](https://support.avaya.com).
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product > Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.
   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.
   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

Related links
- [Application Enablement Services documentation](#) on page 66
Accessing the port matrix document

Procedure

2. Log on to the Avaya website with a valid Avaya user ID and password.
4. In Enter Your Product Here, type the product name, and then select the product from the list of suggested product names.
5. In Choose Release, select the required release number.
6. In the Content Type filter, select one or more of the following categories:
   • Application & Technical Notes
   • Design, Development & System Mgt
   The list displays the product-specific Port Matrix document.
7. Click Enter.

Related links
Application Enablement Services documentation on page 66

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com.

Important:
For documents that are not available on the Avaya Documentation Portal, click Support on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Portal, you can:

• Search for content in one of the following ways:
  - Type a keyword in the Search field.
  - Type a keyword in Search, and click Filters to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
• Find a document from the Publications menu.
• Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
• Add content to your collection by using My Docs (⭐).
Navigate to the **My Content > My Docs** menu, and do any of the following:
- Create, rename, and delete a collection.
- Add content from various documents to a collection.
- Save a PDF of selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive content that others have shared with you.

* Add yourself as a watcher by using the **Watch** icon (🔍).

Navigate to the **My Content > Watch list** menu, and do the following:
- Set how frequently you want to be notified, starting from every day to every 60 days.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

**Note:**
Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

**Related links**
- [Application Enablement Services documentation](#) on page 66

---

**Training**

The following courses are available on the Avaya Learning website at [http://www.avaya-learning.com](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.

<table>
<thead>
<tr>
<th>Course code</th>
<th>Course title</th>
</tr>
</thead>
<tbody>
<tr>
<td>20980W</td>
<td>What's New with Avaya Aura® Release 8.1</td>
</tr>
</tbody>
</table>

---

**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.

• To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In Search, type Avaya Mentor Videos, click Clear All and select Video in the Content Type.
  - In Search, type the product name. On the Search Results page, click Clear All and select Video in the Content Type.
  
    The Video content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.

• To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic.
    For example, Contact Centers.

  Note:
  Videos are not available for all products.

Support
Go to the Avaya Support website at https://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.

Related links
Using the Avaya InSite Knowledge Base on page 70

Using the Avaya InSite Knowledge Base
The Avaya InSite Knowledge Base is a web-based search engine that provides:

• Up-to-date troubleshooting procedures and technical tips
• Information about service packs
• Access to customer and technical documentation
Information about training and certification programs

Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

2. Log on to the Avaya website with a valid Avaya user ID and password. The system displays the Avaya Support page.
3. Click **Support by Product > Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press **Enter**.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

[Support](#) on page 70
Appendix A: AE Services compatibility

This appendix describes the supported:

- Clients, API, and, versions of Communication Manager with AE Services.
- Communication Manager platforms with AE Services.

API and client compatibility

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

DMCC compatibility

The DMCC 7.0 and earlier applications will work with the AE Services Release 8.1.2 DMCC Service. DMCC provides a Java, XML and .NET API.

Web Services compatibility

For AE Services Release 8.1.2, the Telephony Web Service does not introduce any new features.

System Management Service compatibility

For AE Services Release 8.1.2, the System Management Service does not introduce any new features.

TSAPI compatibility

AE Services Release 8.1.2 TSAPI Service includes all of the functionality provided by AE Services 6.3.x, 7.0 and Avaya CT 1.x. AE Services Release 8.1.2 TSAPI Service is backward compatible with the following TSAPI/JTAPI clients and libraries: AE Services 6.3.x, 7.0.x, 7.1.x, 8.0.x, and 8.1.x.

CVLAN compatibility

The AE Services Release 8.1.2 CVLAN Service includes all of the functionality provided by AE Services 7.0 CVLAN Service, CVLAN on MAPD, and the CVLAN R9 Server for Linux. The AE Services Release 8.1.2 CVLAN Service is backward compatible with the following CVLAN clients and libraries: AE Services 6.3.x., 7.0.x, 7.1.x, 8.0.x, and 8.1.x.
Product compatibility

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

AE Services compatibility with Communication Manager
Release 8.1.2 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.

Note:

Switch connections, H.323 links, and SMS connections can be established directly to the Processor Ethernet on Communication Manager on supported hardware. For more details, see Avaya Aura® Communication Manager Overview and Specification.

Communication Manager Release 8.1.2 — ASAI capabilities

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

Important:

If you are using ASAI, you can only administer up to 16 bridged appearances and other Communication Manager group features, such as Answer Coverage Group, in total.

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)
AE Services compatibility

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

**ASAI Optional Features**
- CTI Stations
- Phantom Calls
- Adjunct Routing
- Increased Adjunct Route Capacity
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Enablement Protocol (AEP)</td>
<td>The protocol used by an AEP connection.</td>
</tr>
<tr>
<td>Application Enablement Protocol (AEP) connection</td>
<td>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.</td>
</tr>
<tr>
<td>ASAI</td>
<td>Adjunct Switch Application Interface. ASAI is a protocol that enables software applications to access call processing capabilities provided by Communication Manager.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The process of validating the identity of a user by means of user profile attributes.</td>
</tr>
<tr>
<td>Authorization</td>
<td>The process of granting a user the ability to carry out certain activities based on permissions.</td>
</tr>
<tr>
<td>Call Information Service</td>
<td>The Call Information Service allows applications to get detailed call information and to determine the status of the call information link.</td>
</tr>
<tr>
<td>CLAN</td>
<td>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.</td>
</tr>
<tr>
<td>Computer Telephony Integration</td>
<td>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.</td>
</tr>
<tr>
<td>CTI Link</td>
<td>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.</td>
</tr>
<tr>
<td><strong>DMCC Service</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>First-Party Call Control</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>JTAPI</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>LDAP</strong></td>
<td>Lightweight Directory Access Protocol. LDAP defines a standard protocol for organizing directory hierarchies and a standard interface for clients to access directory servers.</td>
</tr>
<tr>
<td><strong>Link</strong></td>
<td>A communications channel between system components.</td>
</tr>
<tr>
<td><strong>Monitor</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Operations, Administration, and Maintenance</strong></td>
<td>Abbreviated as OAM. The administrative interface for the Application Enablement Services platform. Now referred to as the AE Services Management Console.</td>
</tr>
<tr>
<td><strong>PKI</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>PLDS</strong></td>
<td>Product Licensing and Delivery System. AE Services uses the PLDS for license management and software distribution.</td>
</tr>
<tr>
<td><strong>Private Data</strong></td>
<td>Private data is a switch-specific software implementation that provides value added services.</td>
</tr>
<tr>
<td><strong>Registration, Administration, and Status</strong></td>
<td>Abbreviated as RAS. RAS is an International Telecommunications Union specification for terminal registration and authentication. RAS is part of the H.323 protocol suite.</td>
</tr>
<tr>
<td><strong>Routing</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>RTP</strong></td>
<td>Real-time Transport Protocol. RTP is an Internet standard for transmission of time-critical data, and for control of the transmission.</td>
</tr>
<tr>
<td><strong>SDK</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>SIP</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Switch Connection Name</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Telephony Web Service</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Third-Party Call Control</strong></td>
<td>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”.</td>
</tr>
<tr>
<td><strong>Tlink</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Glossary</strong></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td></td>
</tr>
<tr>
<td><strong>Transport link</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>TSAPI Service</strong></td>
<td>The CSTA-based third-party call control services provided by AE Services.</td>
</tr>
<tr>
<td><strong>Web Services</strong></td>
<td>A set of standards that allow a service to be described and consumed in a platform-neutral way.</td>
</tr>
</tbody>
</table>