Avaya Aura® Application Enablement Services Overview and Specification

Release 10.2.x
Issue 2
April 2024

© 2015-2024, Avaya LLC
All Rights Reserved.

Notice

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

Documentation disclaimer

"Documentation" means information published in varying media which may include product information, subscription or service descriptions, 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

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

Licenses

The Global Software License Terms ("Software License Terms") are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

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

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

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, please contact your Avaya Sales Representative.

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 Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud 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 LLC.

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

Contents

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

Issue	Date	Summary of changes
2	April 2024	Updated the following sections: • AE Services resource requirements and the supported footprints. • Avaya Aura® applications deployment offers.
1	December 2023	Release 10.2 document.

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, web services, and REST APIs 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.

AE Services supports Antivirus and Malware installation on software-only deployment and the following Antivirus and Malware are tested in Avaya labs:

- McAfee
- Symantec
- ClamAV

Note:

ClamAV Antivirus is preinstalled on AE Services server for VMware deployment using OVA.

Supported browsers

The following are the minimum tested versions of the supported browsers:

- Microsoft Edge Release 119
- Google Chrome Release 119
- Mozilla Firefox Release 120

Note:

- From Avaya Aura® Release 10.1 and later, Microsoft Internet Explorer is no longer supported.
- Later versions of the browsers can be used. However, it is not explicitly tested.

Avaya Aura® applications deployment offers

Avaya Aura® supports the following deployment offers:

- Avaya Aura® Virtualized Environment (VE): Avaya Solutions Platform 130 (Dell PowerEdge R640, ESXi 7.0) and Customer-provided VMware infrastructure.
- Software-only and Infrastructure as a Service environment: Deployment on the Red Hat Enterprise Linux operating system.

  Note:

  The deployment of Avaya Aura® applications as software only is available but a restricted offer for net new deployments and requires Avaya Aura® BU approval before proceeding. If you have a business requirement to deploy Avaya Aura® as software only, please get in touch with your Avaya Sales team. Existing customers using software only deployments continue to be supported.

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 10.2.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 Software-Only and Infrastructure as a Service Environments*
- *Upgrading Avaya Aura® Application Enablement Services*

New in this release

New in Application Enablement Services Release 10.2

Avaya Aura® Application Enablement Services Release 10.2 supports the following new features and enhancements:

AE Services TSAPI Unencrypted Services port default changed

Earlier to Release 10.2, by default, both the Encrypted Services Port and Unencrypted Services Port were enabled.

With Release 10.2, by default, TSAPI Unencrypted Services Port is disabled and TSAPI Encrypted Services Port is enabled.

Support for VMware 8.0

With Release 10.2, Avaya Aura® applications support the VMware® vSphere ESXi 8.0 and VMware® vCenter Server 8.0 in a VMware virtualized environment.

Support of Root EULA for AE Services OVA deployment

With Release 10.2, AE Services displays the:

- A new **ROOT ACCESS ACCEPTANCE STATEMENT** tab is added next to the existing **End User License Agreement** tab added to accept the root EULA on the **License Agreements** page when deploying the AE Services OVA by using the ESXi directly.

- A new **Eula Acceptance page** > **ROOT ACCESS ACCEPTANCE STATEMENT** subpage is added to the existing **AVAYA GLOBAL SOFTWARE LICENSE TERMS** subpage when deploying the AE Services OVA by using Solution Deployment Manager.

AE Services REST APIs (Web Telephony interface)

The Web Telephony interface (WTI) service was introduced in AE Services Release 10.1.2. In AE Services Release 10.2, all the existing APIs are included as follows:

- The existing DMCC recovery design is extended to the WTI service.
- WTI service provides APIs corresponding to all the APIs provided by DMCC.
- The WTI service supports a WebSocket interface, enabling access to all AES APIs and Events.

Support for Trellix AV (formerly known as McAfee) in Virtualized Deployments

Avaya Aura® Release 10.2 supports deployment of Trellix AV software in a virtualized (OVA based) environment. This new feature effectively detects, prevents, and eliminates malware threats resulting in enhancing the security of your Avaya Aura® environment. The IT industry widely recognizes Trellix AV as a trusted cybersecurity solution. With the integration capabilities in Avaya Aura® Release 10.2, you can seamlessly integrate Avaya Aura® applications as managed devices as part of your existing Trellix deployment. For more information on support of Trellix for AV on Avaya Aura®, see *Application Note for Support of Trellix AV on Avaya Aura®* on the Avaya Support website at https://support.avaya.com.

Application Enablement Services feature matrix

The following table lists the feature matrix of Application Enablement Services from Release 7.x to Release 10.2.x. The features listed in the table cover the key features only.

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1 and Release 8.1.1	Release 8.1.2	Release 8.1.3	Release 10.1.x	Release 10.2.x
Third-party call control support for service observe					Y	Y	Y
VMware 7.0					Y	Y	Y
TSAPI 64-bit client for Windows and SDK					Y[c]	Y[c]	Y[c]
OVA signing	Y	Y	Y	Y[a]		Y[a]	Y[a]
IPv6 support	Y	Y	Y	Y	Y	Y	Y

Table continues…

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1 and Release 8.1.1	Release 8.1.2	Release 8.1.3	Release 10.1.x	Release 10.2.x
Enhanced Access Security Gateway (EASG)	Y	Y	Y	Y	Y	Y	Y
Compliance with DISA security STIGs	Y				Y		Y
Multi factor authentication	Y	Y	Y	Y	Y	Y	Y
Support for TLS 1.2	Y	Y	Y	Y	Y	Y	Y
Support for TLS 1.3						Y	Y
Red Hat Enterprise Linux (RHEL) 8.4						Y	Y
Customer Root Access		Y	Y	Y	Y	Y	Y
Preserve security hardening modes on upgrade		Y	Y	Y	Y	N[d]	N[d]
Support for 16-digit dial plan		Y	Y	Y	Y	Y	Y
Software-only support for KVM	Y	Y	Y			Y	Y
Support for Software-only deployment	Y	Y	Y		Y[b]	Y[b]	Y[b]
Support for Hyper-V in Software-Only environment		Y	Y		Y[b]	Y[b]	Y[b]
Support for third-party software in Software-Only environment		Y	Y	Y	Y[b]	Y[b]	Y[b]
Support of Held Call ID on auto dial request by Application Enablement Services		Y	Y	Y	Y	Y	Y

Table continues…

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1 and Release 8.1.1	Release 8.1.2	Release 8.1.3	Release 10.1.x	Release 10.2.x
Support for Avaya Solutions Platform 120 Appliance		Y	Y	Y	Y		
Support for Avaya Solutions Platform 130 Appliance		Y	Y	Y	Y	Y	Y
Support for G.722 codec			Y	Y	Y	Y	Y
Support for 12–Party Conferencing			Y	Y	Y	Y	Y
Real Time Agent Events						Y	Y
REST APIs (Web Telephony Interface)						Y	Y
Support for VMware ESXi 8.0							Y

[a] - OVA is available for VMware and not for KVM.

[b]- To install Application Enablement Services Release 8.1.3 FP in software-only environment, you must follow the following steps:

1. Install Release 8.1 or Release 8.1.1 ISO
2. Upgrade to Release 8.1.2.x FP
3. Upgrade to Release 8.1.3 FP

[c] - TSAPI client and SDK supports 64-bit architecture for Windows and Linux platforms which is backward compatible with AE Services Release 8.1.x server.

[d]- AE Services does not take any status backup of SELinux and Kernel FIPS mode during database backup. If the status of SELinux and Kernel FIPS mode is enabled on the current version, after upgrading to Release 10.1 and later, you must enable the status manually.

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 16.

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 38.

- 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 38.

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 38.

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 Services Server. CVLAN provides a full complement of third-party call control capabilities such as controlling specific calls or stations, completing routing of incoming calls, receiving notifications of events, invoking Communication Manager features and querying Communication Manager for information. CVLAN is an Avaya specific protocol and is not intended for new application development.

DLG service

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

Note:

If 12–Party Conferencing is enabled on Communication Manager, the DLG CTI application will not work on AE Services.

Web Telephony Interface (WTI) Service

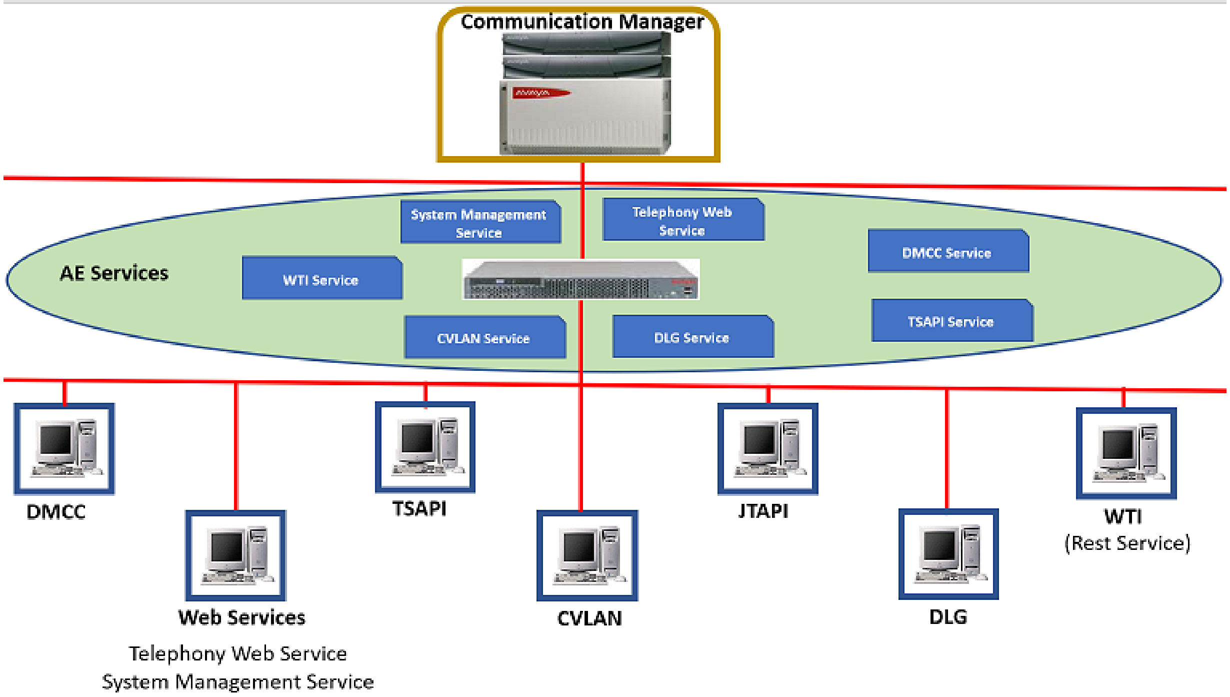
AE Services supports WTI (Web Telephony Interface) Service which provides integration with enterprise applications through REST services. These services expose core telephone functionality and provide access to third party call control features on Communication Manager. The Telephony REST Service provides a high-level interface for basic call control services, simplifying traditional CSTA based call control. Applications need to maintain a bearer token to manage their session on the server and do not need to track call state or information.

The Telephony REST Service also supports third-party call control events corresponding to the API. It enables users to originate outbound calls and receive updates on the call progression. This service uses a session-based model where sessions can be explicitly created by sending a create session request using session APIs with credentials. The service uses the DMCC TSAPI Service to perform most of its requests, which requires Computer Telephony Adjunct Links to be licensed on Communication Manager and a TSAPI Basic license (denoted as TSAPI Simultaneous Users in the license file) for each device in use concurrently by the Telephony REST Services.

From AE Services Release 10.2, WTI service provides APIs corresponding to all the APIs provided by DMCC.

For more information, see the Avaya DevConnect Web site http://www.avaya.com/devconnect.

AE Services configuration at a glance



Chapter 5: Network Security and Reliability

AE Services security features

The following list highlights the AE Services security features.

Linux shell access control

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

Login Audit

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

Lock or unlock a Linux account

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

Login Reports

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

Role Based Access Control (RBAC)

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

Additional AE Services security features information

For more information about AE Services security features, see “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.

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 third-party certificates for lab use, that is out-of-the-box deployments. These default third-party certificates must 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*.
  - *Avaya Application Enablement Services Device, Media and Call Control API XML Programmers Guide*.
  - *Avaya Application Enablement Services Device, Media and Call Control API .NET Programmers Guide*.
  - *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*.
- *Avaya Application Enablement Services JTAPI Programmers Guide*.

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 through Secure Sockets Layer (SSL). For more information, refer the *Application Enablement Services Web Services Programmer Guide*.

Note:

Default server certificates must 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.

WTI Services

AE Services provides a default certificate and keystore for encryption keys for Secure Sockets Layer (SSL) connections to the AE Services. Certificates, either as a web alias or server alias, can be used to secure the connection to AE Services, overwriting the default certificates.

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 22.
- 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 Device IDs, 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.

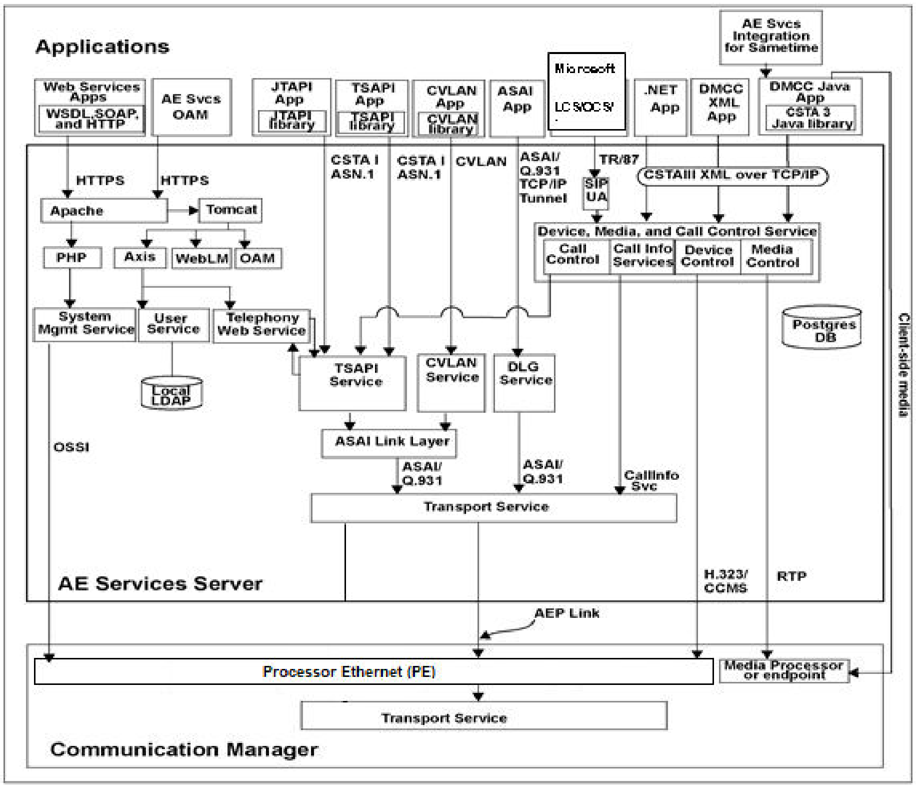
- TSAPI

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

  - JTAPI
  - DMCC with Call Control
  - Telephony Web Services
- DMCC endpoint registration using WebLM's DMCC-DMC licenses
- DMCC with Call Information Services
- CVLAN
- DLG
- WTI

Chapter 7: AE Services Architecture

AE Services architecture at a glance



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.

AE Services 8.0.1 and later support J169 and J179 series phones with SIP 2.0 firmware. The station type must be set to 96x1SIP or 96x1SIPCC for 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
- Session Manager

AE Services with Communication Manager and Session Manager introduced the ability to control Avaya SIP endpoints through 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.

Endpoint	Administered as	Endpoint Firmware	AE Services Release	Communication Manager/Session Manager Pair	
				Communication Manager- ES Release	Session Manager Release
9620	9620SIP	2.6 SP12	10.2.x	10.2	10.2
9640	9640SIP	2.6 SP12	10.2.x	10.2	10.2
9640G	9640SIP	2.6 SP12	10.2.x	10.2	10.2
9630G	9630SIP	2.6 SP12	10.2.x	10.2	10.2
9650	9600SIP	2.6 SP12	10.2.x	10.2	10.2
9601	9608SIP	6.4	10.2.x	10.2	10.2

Table continues…

Endpoint	Administered as	Endpoint Firmware	AE Services Release	Communication Manager/Session Manager Pair	
				Communication Manager- ES Release	Session Manager Release
9608	9608SIP/9608SIPCC*	6.4	10.2.x	10.2	10.2
9611	9611SIP/9611SIPCC*	6.4	10.2.x	10.2	10.2
9621	9621SIP/9621SIPCC*	6.4	10.2.x	10.2	10.2
9641	9641SIP/9641SIPCC*	6.4	10.2.x	10.2	10.2
Avaya Workplace Client	9641SIP	3.24	10.2.x	10.2	10.2
J129	J129	4.0.1	10.2.x	10.2	10.2
J139	J129	4.0.1	10.2.x	10.2	10.2
J169	J169/J169CC*	4.0.1	10.2.x	10.2	10.2
J179	J179/J179CC*	4.0.1	10.2.x	10.2	10.2

*: If you want to use the endpoints for Avaya Aura® Call Center Elite operations, you must administer the endpoint with type or endpoint profile as CC.

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 24. 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 24, except the following capabilities:

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

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 more information about licensing for a specific product, see the following topics:

Application Enablement Protocol connections licensing on page 28

Device, Media, and Call Control licensing on page 29

WTI services licensing on page 30

Web services licensing on page 31

System Management Service (SMS) licensing on page 31

TSAPI service (including JTAPI) licensing on page 31

CVLAN licensing on page 33

DLG licensing on page 33

Enterprise-wide licensing on page 34

Comparison of standard licensing and enterprise-wide licensing on page 34

Licensing configuration examples on page 35

AE Services product or service	**Required feature licensed on Communication Manager**	**Optional feature licensed on Communication Manager**	**AE Services feature**
	Use display system-parameters customer-options command to see if the feature is provided by the Communication Manager License.		**Use WebLM to see if this feature is provided by the Application Enablement license.**
DMCC - Device and Media Control	• STA • IP_STA	IP-API_A - all pre-existing IP_API_A licenses in Communication Manager license remain there and may be used once the AE Services feature licenses are exhausted.	Device, Media, and Call Control
DMCC and WTI - 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 29.	None	• TSAPI Basic license (denoted as TSAPI Simultaneous Users in license file)
TSAPI Service (which includes JTAPI) for applications that use a Basic TSAPI license	Computer Telephony Adjunct Links	None	TSAPI Basic license (denoted as TSAPI Simultaneous users in license file)
TSAPI Service (which includes JTAPI) for applications that use an Advanced TSAPI license	Computer Telephony Adjunct Links	Increased Adjunct Routes	• AES Advanced Small Switch • AES Advanced Medium Switch • AES Advanced Large Switch
Web Services - Telephony Web Service	Computer Telephony Adjunct Links	None	• TSAPI Basic license (denoted as TSAPI Simultaneous Users in license file)
Web Services-System Management Service	None	None	None

Table continues…

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

Application Enablement Protocol connections licensing

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

You can administer a total of 16 AEP connections but AE Services strongly recommends that you use 2 AEP connections to Communication Manager when the CLAN is used for connectivity. When all AEP connections are in use, no additional AEP connections are brought online. For more information, see Configurations that use AEP connections on page 22. 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.

Device, Media, and Call Control licensing

The Device, Media, and Call Control (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.

WTI services licensing

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

Note:

A separate license is not required to use WTI. The WTI service consumes TSAPI and DMCC licenses in AE Services 10.1.2 and later.

Web services licensing

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

System Management Service (SMS) licensing

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

TSAPI service (including JTAPI) licensing

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

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

TSAPI basic user license

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

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

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

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

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

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

Note:

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

TSAPI advanced license

The TSAPI advanced license is intended for applications that launch calls such as predictive dialing applications or to route calls. The TSAPI advanced license is based on the following Communication Manager servers for which you need license and the size of the Communication Manager platform:

- SMALL CM 8.x and later: CM Main Max Users 1000, CM survivable Max Users 1000
- Medium CM 8.x and later: CM Main Max Users 2400
- Large CM 8.x and later: CM Hi Duplex Max Users 36000, CM Duplex Max Users 30000, CM Main/survivable Max Users 36000

Note:

You need a Large CM 8.x TSAPI advanced license for deploying CM 8.x in the virtualized environment.

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

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

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 34.
- For examples of licensing configurations, see Licensing configuration examples on page 35.

Comparison of standard licensing and enterprise-wide licensing

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

Licensing configuration examples

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

Standard licensing

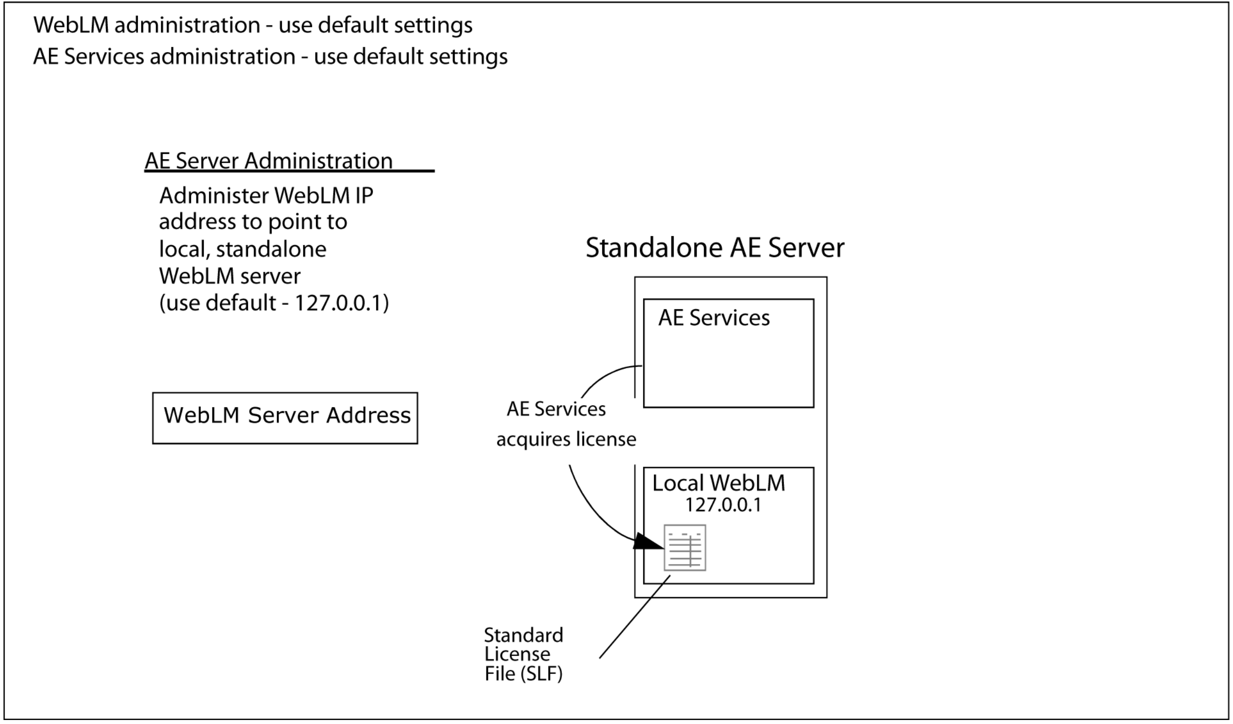
In a standard licensing configuration for Software-only offer, the standard license file (SLF) is installed on the AE Services server and is controlled by the WebLM server running on the AE Services server.

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)
WebLM Server Address
Standalone AE Server
AE Services
AE Services acquires license
Local WebLM 127.0.0.1
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

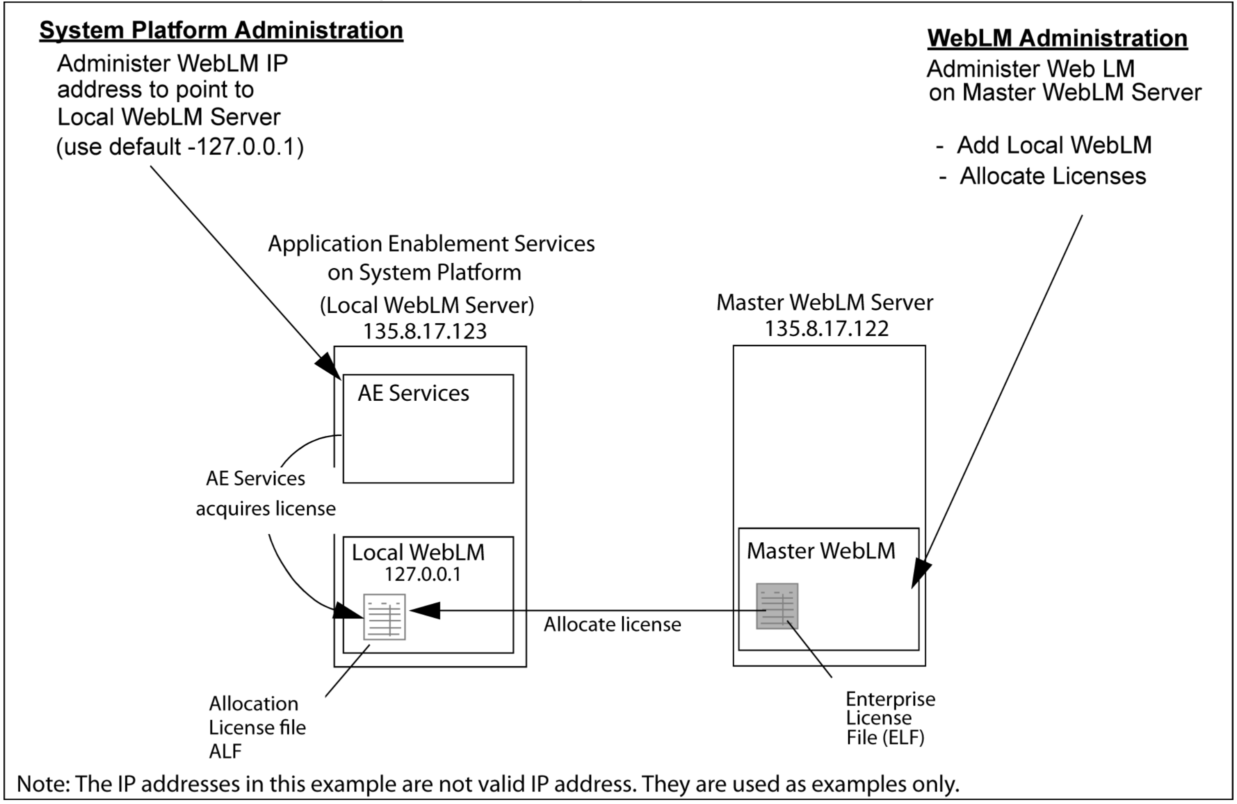
AE Services expanded its licensing capabilities to include enterprise-wide licensing. Enterprise-wide licensing provides the flexibility to move capacities and features from one AE Services server to another. With enterprise-wide licensing, you can move capacities or features from one server to another 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:

Enterprise-wide licensing — allocating licenses or features


System Platform Administration
Administer WebLM IP address to point to Local WebLM Server (use default -127.0.0.1)
WebLM Administration
Administer Web LM on Master WebLM Server
- Add Local WebLM
- Allocate Licenses
Application Enablement Services on System Platform
(Local WebLM Server)
135.8.17.123
Master WebLM Server
135.8.17.122
AE Services
AE Services acquires license
Local WebLM
127.0.0.1
Master WebLM
Allocate license
Allocation License file ALF
Enterprise License File (ELF)
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.

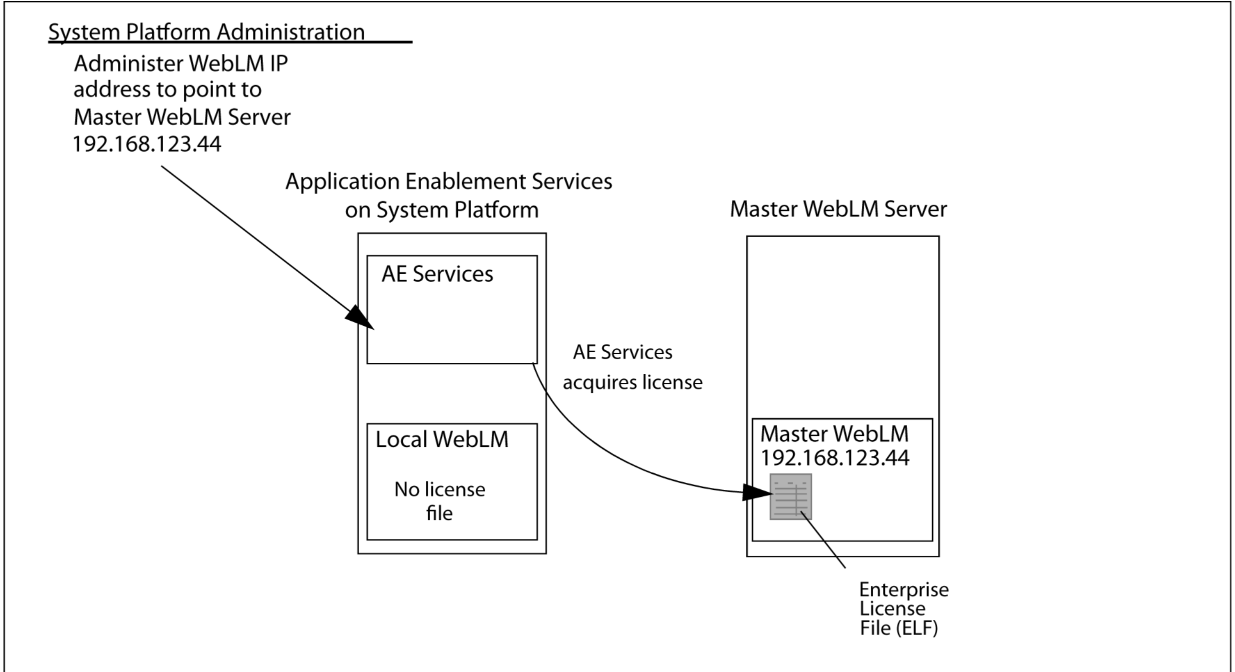
Enterprise-wide licensing — pointing to a master license on a remote server

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.

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


System Platform Administration
Administer WebLM IP address to point to Master WebLM Server 192.168.123.44
Application Enablement Services on System Platform
Master WebLM Server
AE Services
AE Services acquires license
Local WebLM
No license file
Master WebLM 192.168.123.44
Enterprise License File (ELF)

Note: IP address 192.168.123.44 is used for purposes of this example. It is not a valid WebLM IP address.

Note:

Beginning with AE Services 7.0, System Platform is not supported.

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.

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.

Name	Distribution	Material code/URL
Application Enablement Services TSAPI SDK	Contact your account executive	700500048
Application Enablement Services TSAPI client		700510417
Application Enablement Services CVLAN client	Avaya DevConnect Developer Program	www.avaya.com/devconnect
Application Enablement Services DMCC Java SDK		
Application Enablement Services DMCC XML SDK		
Application Enablement Services DMCC .NET SDK supporting .NET Framework 4.5.2		
Application Enablement Services Web Service — Telephony Web Svc SDK		
Application Enablement Services JTAPI SDK		
Application Enablement Services SMS SDK		

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.

Answering a call from an extension that is already present in an outgoing call

- **ASAI:** If a user tries to answer a call from an extension that is already present in an ongoing call through a different line appearance, it will fail with the following error:

  ```
  RESOURCE_BUSY
  ```

  To resolve this issue, the user first needs to put the current call on hold and then the other call can be answered on another line appearance.
- **CVLAN:** Because the CVLAN service is implemented using ASAI, CVLAN support for this feature is also incomplete but it works with HOLD API.
- **TSAPI:** Because the TSAPI service is implemented using ASAI, TSAPI support for this feature is also incomplete but it works with HOLD API.
- **JTAPI:** Because JTAPI is an interface to TSAPI, JTAPI support for this feature is also incomplete but it works with HOLD API.
- **TWS:** This cannot be achieved with TWS as TWS does not support HOLD API.

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.

Warning:

Special application features on Communication Manager are intended to serve the specific needs and are not recommended for general use. Special application features on Communication Manager have limited testing and are applicable only to some specific configurations. Activating one or more of these features on Communication Manager may result in an unpredictable system behavior or malfunction with all AE Services messages (TSAPI/DMCC/JTAPI/TWS). Before activating any special application feature on Communication Manager, please read the associated Communication Manager documentation for special application at http://support.avaya.com.

Limitation of Event Notification for Bridge parties

Event Notification for bridge parties is supported up to 20 bridges per principal station in AE Services.

Note:

When processing a snapshot response, AES marks devices as inactive if they are present in the call record as kludged party with partyIDs that exceed 300 (for ASAI link version up to 10) and 1344 (for ASAI link version 11 onwards). Therefore, all the subsequent ASAI events related to these devices do not get propagated to application. So, you must configure not more than 20 bridges per principal station to avoid such cases.

Chapter 12: Capacities for AE Services

This chapter provides the capacities for AE Services.

AE Services resource requirements and the supported footprints

The following tables show the resource requirements and the supported footprints for deploying AE Services using the following platforms:

Note:

Avaya Aura® Application Enablement Services supports VMware hosts with Hyperthreading enabled at the BIOS level.

To improve the performance of the GRHA, use profiles 2 and 3.

- ISO:
  - On-premise - VMware, KVM, Hyper-V
  - On cloud - Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud for VMware Solutions
- OVA: VMware or Avaya Solutions Platform

Footprints	Profile 1	Profile 2	Profile 3
vCPUs	1	2	4
CPU MHz Reservation **Note:** Reservations are applicable to VMware only.	2190 MHz	4380 MHz	8760 MHz
RAM	4 GB	4 GB	6 GB
HDD	55 GB	55 GB	55 GB
NICs	1 to 3*	1 to 3*	1 to 3*
IOPS	6	6	6

Note:

* Depending on the network topology, you can configure the following types of networks:

1. Public network (Mandatory)
2. Private network (Optional)
3. Out of Band Management (Optional)

		DMCC, WTI — Third party call control: Avaya Aura® Contact Center		DMCC — First Party call control		TSAPI, DLG, CVLAN
Profile	**Footprint**	**Maximum number of users or agents**	**Maximum BHCC**	**Maximum number of users or agents**	**Maximum BHCC**	**Maximum Messages per second (MPS) Rate**
Profile 1	**1 CPU and 4 GB RAM**	1K 10K	20K BHCC 6K BHCC	1K	9K BHCC	1K MPS
Profile 2	**2 CPU and 4 GB RAM**	2.5K 12K	50K BHCC 12K BHCC	2.4K	18K BHCC	1K MPS
Profile 3	**4 CPU and 6 GB RAM**	5K 20K	100K BHCC 24K BHCC	8K	36K BHCC	2K MPS

Supported footprints for AE Services on Amazon Web Services

AES Deployment Type	Footprint	AWS ISO instance type	HDD (GB)	NICs
AES (Software only)	Profile 1	m3.medium or higher	55 GB	2
AES (Software only)	Profile 2	c4.large or higher, c5a.large, or c5.large	55 GB	2
AES (Software only)	Profile 3	c3.xlarge or higher, c5a.xlarge, or c5.xlarge	55 GB	2

Supported footprints for AE Services on Microsoft Azure

AES Deployment Type	Footprint	Azure instance type	HDD (GB)	NICs
AES (Software only)	Profile 1	Standard B2s (2 vcpus, 4 GiB memory)	55 GB	2
AES (Software only)	Profile 2	Standard B2s (2 vcpus, 4 GiB memory)	55 GB	2
AES (Software only)	Profile 3	Standard F4s v2 (4 vcpus, 8 GiB memory)	55 GB	2

Supported footprints for AE Services on Google Cloud Platform

AES Deployment Type	Footprint	GCP instance type	HDD (GB)	NICs
AES (Software only)	Profile 1	n1-custom-1-4096 (1 vcpus, 4 GiB memory)	55 GB	2
AES (Software only)	Profile 2	n2-custom-2-4096 (2 vcpus, 4 GiB memory)	55 GB	2
AES (Software only)	Profile 3	n2-custom-4-6144 (4 vcpus, 6 GiB memory)	55 GB	2

Capacities for AE Services in Virtualized Environment

You can deploy multiple AE Services instances in Virtualized Environment.

For example, Dell PowerEdge R640 Profile 3 with the hardware specifications (48 GB RAM, 20 vCPUs with 2.20 GHz, and 1 TB HDD) can have up to 10 AE Services instances of Profile 1 (1 CPU, 4 GB).

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 different factors.

- If either Client or Server Media mode is used, the following must 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 45 and Table 2: Server media on page 46 with the Communication Manager resources and capacities described in capacities for DMCC on page 47 to ensure that you have adequate Communication Manager resources for a given DMCC implementation.

Note:

Registration for each 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)

Session and H323 Signaling Encryption Profile	AE Server Capacity	Traffic Rate for Applications
None	8,000 endpoints and a 36,000 BHCC on the Avaya Common Servers.	For Processor Ethernet, AE Services and Communication Manager can support up to 20 outstanding registration requests by an application at any time.
PIN-EKE	3,200 endpoints and a 28,800 BHCC on the Avaya Common Servers.	For Processor Ethernet, AE Services and Communication Manager can support up to 20 outstanding registration requests by an application at any time.
H323TLS	4,000 endpoints and a 18,000 BHCC on the Avaya Common Servers. For more information see, Additional AE Services Restrictions on page 46.	For Processor Ethernet, AE Services and Communication Manager can support up to 20 outstanding registration requests by an application at any time.

Note:

For Non-ASL application network, if remote Avaya WebLM is used without reserved licensing, delay or latency between AE Services and Remote Avaya WebLM must be in the permissible value.

When AES is configured with reserved licensing, the time it takes for registering the stations is lesser compared to AES Configured without reserved licensing.

Table 2: Server media

	Code type	AE Server capacity	Traffic rate for applications
No signaling and media encryption	G729	120 endpoints	For Processor Ethernet, AE Services and Communication Manager can support up to 20 outstanding registration requests by an application at any time.
	G711	75 endpoints	For Processor Ethernet, AE Services and Communication Manager can support up to 20 outstanding registration requests by an application at any time.
Signaling and media encryption	G729	96 endpoints	For Processor Ethernet, AE Services and Communication Manager can support up to 20 outstanding registration requests by an application at any time.
	G711	60 endpoints	For Processor Ethernet, AE Services and Communication Manager can support up to 20 outstanding registration requests by an application at any time.

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.

Component	Capacity
For each IP endpoint in a call, including AE Services endpoints	• 1 VoIP channel is used (with a G.711 codec) • 2 VoIP channels are used (with a G.729 codec)
TN2302 media processor card	64 channels
TN2602 Crossfire media processor card	320 channels
MM760 VoIP card	64 channels
G700 media gateway motherboard VoIP	64 channels
G350 media gateway motherboard VoIP	32 channels
TN799DP CLAN card	400 DMCC station registrations For more information, see Additional Communication Manager Restrictions on page 48
Processor Ethernet	• 1000 DMCC station registrations are supported on following Communication Manager profiles: - CM Main Max users 1000 - CM Survivable Max users 1000 - CM_SurvRemoteEmbed - CM_onlyEmbed • 2400 DMCC station registrations are supported on following Communication Manager profiles: - CM Main Max users 2400 • 8000 DMCC station registrations are supported on following Communication Manager profiles: - Main/Survivable Core Duplex (CM_Duplex) Large - CM Main/Survivable max users 41000 **Note:** This capacity is per AE Services server. For more information, see Additional Communication Manager Restrictions on page 48.

Additional Communication Manager restrictions

Following are the additional restrictions for Communication Manager per AE Services server:

- 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.
    - 500 DMCC station registrations for a Small Communication Manager platform (CM Main Max users 1000 or CM Survivable Max users 1000)
    - 1200 DMCC station registrations for a Medium Communication Manager platform
    - 4000 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/

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.

System capacities of the AE Services server

Component	Capacity
Communication Manager servers supported by one AE Services Server	16
Connections to a Communication Manager server with one AE Services server	16
Messages per second per AE Services Server connection: To Communication Manager (1 CLAN) From Communication Manager (1 CLAN)	200 240
Messages per second per AE Services Server connection to and from Communication Manager (processor ethernet)	2000
Messages per second (per system)	2000 See Note below.

Note:

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

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

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

DLG service capacities

Component	Capacity
Clients supported	16
Links	16

TSAPI service capacities

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

Note:

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

System Management Services capacities

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

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*.

  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*. Depending on the scope of your planning, you can refer additional documents for more information. The following sections provide information about using additional documents for implementing Application Enablement Services.

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*.

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 Software-Only and Infrastructure as a Service Environments*.
- *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*.

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 38.

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 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*.

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*.
  - *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*.
- *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*.
- *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)

WTI programmers

If you program to WTI, use the following documents.

- *Avaya Aura® Application Enablement Services Web Telephony Interface Service API Reference*. This document describes the REST Telephony Services which exposes core telephone functionality and enables access to basic third party call control features on Avaya Communication Manager.

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*. 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 enables 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*.
- The *Application Enablement Services TSAPI Programmer’s Reference* document describes the Telephony Services API, which is based on ECMA CSTA Standards 179 and 180. This document is required, when 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*, 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*. 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*.
- *Application Enablement Services ASAI Technical Reference*. 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*. 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*. This document provides technical descriptions of ASAI third-party call control capabilities.
- *Application Enablement Services ASAI Protocol Reference*. 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.

Title	Description	Audience
Design		
Avaya Aura® Application Enablement Services Overview and Specification	Understand high-level product features and functionality.	Customers and sales, services, and support personnel
Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide	Installing TSAPI and CVLAN Client and SDK	Customers and sales, services, and support personnel
Using		
Upgrading Avaya Aura® Application Enablement Services	Upgrading Application Enablement Services applications.	System administrators and IT personnel
Administering Avaya Aura® Application Enablement Services	Administering Application Enablement Services applications and install patches on Application Enablement Services applications.	System administrators and IT personnel
Avaya Aura® Application Enablement Services Data Privacy Guidelines	Describes how to administer Application Enablement Services to fulfill Data Privacy requirements.	Sales Engineers, Implementation Engineers, Support Personnel
Implementation		
Deploying Avaya Aura® Application Enablement Services in Virtualized Environment	Deploy Application Enablement Services applications in Virtualized Environment	Implementation personnel
Deploying Avaya Aura® Application Enablement Services in Software-Only and Infrastructure as a Service Environments	Deploy Application Enablement Services applications in Software-Only and Infrastructure as a Service Environments	Implementation personnel
Maintenance and Troubleshooting		

Table continues…

Title	Description	Audience
Maintaining Avaya Aura® Application Enablement Services	Maintaining Application Enablement Services applications and install patches on Application Enablement Services applications.	System administrators and IT personnel

Related links

Finding documents on the Avaya Support website on page 57
Accessing the port matrix document on page 57
Avaya Documentation Center navigation on page 58

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list
8. In **Select Release**, select the appropriate release number.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
9. Press **Enter**.

Related links

Application Enablement Services documentation on page 56

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list

8. In **Choose Release**, select the required release number.
9. In the **Content Type** filter, select one or both the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
10. Press **Enter**.

Related links

Application Enablement Services documentation on page 56

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.
- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** (🌐) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** (☆).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.
- Add yourself as a watcher using the **Watch** icon (👁).

Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - 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 website.

- 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 website. The available functionality depends on your role.

Related links

Application Enablement Services documentation on page 56

Training

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

Course code	Course title
20980W	What's New with Avaya Aura®

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 keyword or keywords 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 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 60

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.

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.

   The system displays the Avaya Support page.

5. Click **Support by Product** > **Product-specific Support**.
6. In **Enter Product Name**, enter the product, and press `Enter`.
7. Select the product from the list, and select a release.
8. Click the **Technical Solutions** tab to see articles.
9. Select **Related Information**.

Related links

Support on page 60

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

AE Services Release 10.2.x DMCC Service .Net/Java/XML SDKs are backward compatible with the following AE Services releases:

- AE Services 8.1.x
- AE Services 10.1.x

Web Services compatibility

For AE Services Release 10.2.x, the Telephony Web Service clients and libraries does not introduce any new features.

System Management Service compatibility

For AE Services Release 10.2.x, the System Management Service clients and libraries does not introduce any new features.

TSAPI compatibility

The AE Services Release 10.2.x TSAPI Service clients and libraries are backward compatible with the following AE Services releases:

- AE Services 8.1.x
- AE Services 10.1.x

JTAPI compatibility

The AE Services Release 10.2.x JTAPI Service SDKs are backward compatible with the following AE Services releases:

- AE Services 8.1.x

- AE Services 10.1.x

CVLAN compatibility

The AE Services Release 10.2.x CVLAN Service clients and libraries are backward compatible with the following AE Services releases:

- AE Services 8.1.x
- AE Services 10.1.x

Product compatibility

For the latest and most accurate compatibility information, go to **TOOLS** > **Product Compatibility Matrix** on the Avaya Support website.

AE Services compatibility with Communication Manager Release 10.2.x 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 10.2.x — 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.

⚠ **Warning:**

Special application features on Communication Manager are intended to serve the specific needs and are not recommended for general use. Special application features on Communication Manager have limited testing and are applicable only to some specific configurations. Activating one or more of these features on Communication Manager may result in an unpredictable system behavior or malfunction with all AE Services messages (TSAPI/DMCC/JTAPI/TWS). Before activating any special application feature on Communication Manager, please read the associated Communication Manager documentation for special application at http://support.avaya.com.

ASAI Core features

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

ASAI Plus features

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

ASAI Optional Features

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

Glossary

Application Enablement Protocol (AEP)
The protocol used by an AEP connection.

Application Enablement Protocol (AEP) connection
Refers to the secure TCP connection between the AE Server and Communication Manager. It tunnels ASAI messages and Call Information Services messages between AE Services and Communication Manager.

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

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

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

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

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

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

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

DMCC Service

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

First-Party Call Control

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

JTAPI

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

LDAP

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

Link

A communications channel between system components.

Monitor

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

Operations, Administration, and Maintenance

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

PKI

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

PLDS

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

Private Data

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

Registration, Administration, and Status

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

Routing

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

RTP

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

SDK

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

SIP

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

Switch Connection Name

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

Telephony Web Service

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

Third-Party Call Control

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

Tlink

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

Transport link

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

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

TSAPI Service

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

Web Services

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

WTI

Web Telephony Interface. The Telephony REST Service provides a high-level interface for basic call control services, simplifying traditional CSTA based call control.