# Engagement Call Control Snap-in Reference



Release 3.2
Issue 1
October 2016

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

**Link disclaimer**

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

**Warranty**

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

**Hosted Service**

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

**Licenses**

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

**License types**

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

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

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

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number

indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

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

**Heritage Nortel Software**

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

**Copyright**

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

**Virtualization**

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

**Third Party Components**

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. 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**

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. 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.

**Compliance with Laws**

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

**Preventing Toll Fraud**

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

**Avaya Toll Fraud intervention**

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see

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

**Security Vulnerabilities**

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

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

**Downloading Documentation**

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

**Contact Avaya Support**

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

**Trademarks**

# Contents

**Chapter 1: Introduction** ..... 8
Purpose ..... 8
Change history ..... 8
**Chapter 2: ECC overview** ..... 9
Engagement Call Control overview ..... 9
Architecture ..... 10
Functionalities supported by Engagement Call Control features ..... 11
**Chapter 3: Interoperability** ..... 14
Product interoperability ..... 14
**Chapter 4: Application Enablement Services and Communication Manager configuration** ..... 16
Application Enablement Services and Communication Manager configuration ..... 16
Configuring Communication Manager for Engagement Call Control snap-in deployment ..... 17
Configuring multiple Communication Manager ..... 17
Configuring Application Enablement Services ..... 18
Adding an Application Enablement Services user ..... 18
Adding CLANs to the network ..... 19
Enabling Processor Ethernet ..... 20
Enabling AE Services ..... 21
Administering a CTI Link for TSAPI, JTAPI, DMCC with Call Control, Telephony Web Service, or an AE Services integration ..... 22
Adding a switch connection ..... 23
Checking the status of a switch connection -- from Communication Manager to the AE Services server ..... 24
Checking the status of a switch connection -- from the AE Services Server to Communication Manager ..... 24
Editing a Processor Ethernet name or IP address ..... 25
Adding TSAPI Links ..... 25
Configuring Application Enablement Services for Engagement Call Control snap-in deployment ..... 26
Adding the Avaya Breeze™ CA certificate to the Application Enablement Services trust store ..... 27
Configuring Application Enablement Services Dial Plan rules ..... 28
System Manager Trust Management ..... 29
Checklist for using System Manager as a Certificate Authority to generate signed certificates ..... 29
Creating an end entity for the AE Services server ..... 30
Creating the AE Services server certificate ..... 30
Downloading the System Manager CA certificate that signed the AE Services server certificate ..... 31

Importing the System Manager CA certificate into the AE Services server ..... 31
Importing the new AE Services server certificate into the AE Services server ..... 32
**Chapter 5: Deployment** ..... 33
Deploying Engagement Call Control Solution ..... 33
Modifying the disk allocation for Engagement Call Control deployment profiles ..... 33
Resources and memory configuration ..... 33
Configuring Avaya Breeze™ for Engagement Call Control solution ..... 34
Engagement Call Control solution deployment checklist ..... 35
Loading the snap-in ..... 36
Installing the snap-in ..... 37
Configuring the Unified Collaboration Model snap-in attributes ..... 38
Configuring the Unified Collaboration Administration snap-in attributes ..... 39
Configuring the Call Server Connector snap-in attributes ..... 40
Configuring Avaya Aura® Messaging for voice mail operations ..... 42
Using the sample snap-in to test Engagement Call Control Engagement Call Control capabilities ..... 43
Installing trust certificate of HTTPS server ..... 44
Installing the Avaya Aura® Messaging certificate on the Avaya Breeze™ cluster ..... 44
**Chapter 6: Upgrading Engagement Call Control solution** ..... 46
Upgrading Engagement Call Control solution ..... 46
**Chapter 7: Performance** ..... 47
Configuring cluster attributes for production deployment ..... 47
**Chapter 8: Troubleshooting** ..... 48
Log files ..... 48
Searching for log files ..... 48
Events ..... 49
Troubleshooting ..... 50
Calls for newly added users or extensions do not work ..... 50
Duplicate snap-in attribute seen after loading Web Call Controller Snap-in in the upgrade scenario ..... 50
SIP Endpoints registered over TCP do not work ..... 50
Inter-Provider Call sharing UCID across providers ..... 51
Multi device access errors ..... 51
Privilege violation error ..... 51
Redirect operation fails ..... 52
Checking the status of a switch connection from Communication Manager to Application Enablement Services server ..... 52
TSAPI Test ..... 52
**Chapter 9: Maintenance** ..... 53
Editing the Engagement Call Control snap-in attributes ..... 53
Changing the number of servers in an Engagement Call Control cluster ..... 53
**Chapter 10: Resources** ..... 54
Documentation ..... 54

Finding documents on the Avaya Support website..... 55
Developer resources..... 55
Viewing Avaya Mentor videos..... 56
Support..... 56

# Chapter 1: Introduction

## Purpose

This document describes Engagement Call Control characteristics and capabilities, including overview and feature descriptions, interoperability, and performance specifications. The document also provides instructions on how to deploy, configure, and troubleshoot the Engagement Call Control solution.

This document is intended for people who need to install, configure, and use Engagement Call Control. Engagement Call Control is a snap-in solution that runs on Avaya Breeze™.

This document contains specific information about Engagement Call Control. For an overview of Avaya Breeze™, see *Avaya Breeze™ Overview and Specification*. For general information about Avaya Breeze™ snap-in deployment, see *Quick Start to Deploying Avaya Breeze™ Snap-ins*.

## Change history

| Issue | Date | Summary of changes |
|---|---|---|
| 1 | October 2016 | Initial issue |

# Chapter 2: ECC overview

## Engagement Call Control overview

The Engagement Call Control solution Release 3.1 supports:

- Representational State Transfer (REST) APIs for call control operations and voice messaging.
- Functional equivalency to some of the Agile Communication Environment™ Simple Object Access Protocol (SOAP) web services.
- REST interfaces to allow an application to initiate and manage a call between two communication endpoints.
- Call operations, such as making a call, answering a call, dropping a call, holding a call, transferring a call, conferencing a call, forwarding a call, and redirecting a call.
- Messaging operations.

Engagement Call Control solution Release 3.1.1 supports:

- Sharing of CCC snap-ins with Work Assignment. For more information, see *Whitepaper for co-deployment of Engagement Call Control and Work Assignment solution*.
- An optional parameter to input the Context ID data.

  When there are more than two participants in the call, the Context ID of the call can be updated as part of drop participant if one of them wants to drop. In this situation, the Context ID may not be updated in the following events received by the participants.

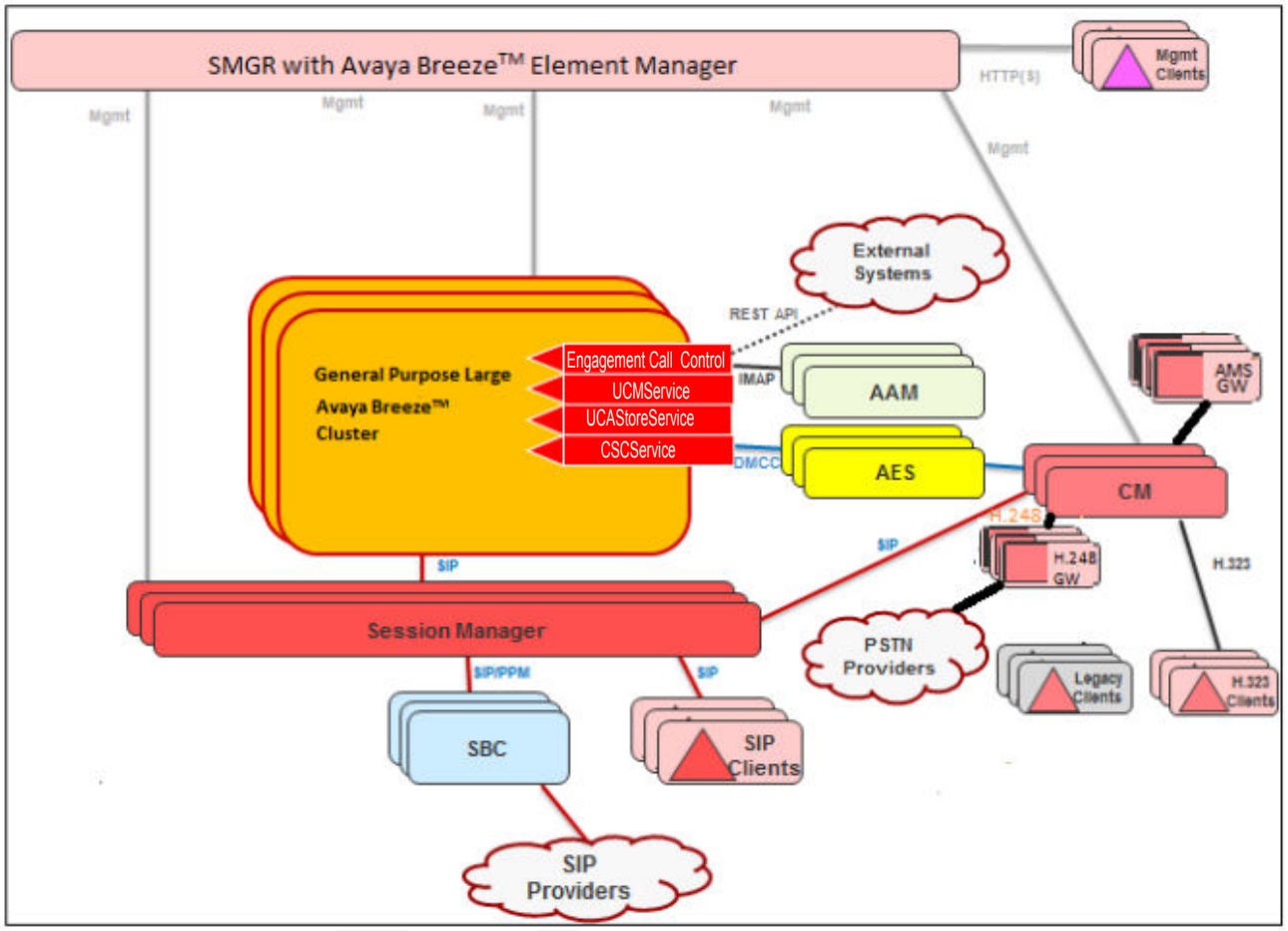
### REST API

Engagement Call Control REST Call Control services and events are different from the Avaya Breeze™ Call Manipulation Java APIs. The REST services are independent and do not invoke the Call Manipulation Java APIs.

Call operations that are possible using the REST API services:

- Monitoring and controlling all calls, including endpoint-to-endpoint calls
- Holding and retrieving calls
- Transferring calls
- Enabling an endpoint to answer a call
- Receiving event notifications for hold, retrieve, transfer, drop, conference, forward, and redirect call operations.

# Architecture




Engagement Call Control exposes REST Call Control APIs for external applications to use. REST is an architectural style for network hypermedia applications. REST is used to build web services that are lightweight, maintainable, and scalable. A service based on REST is called a RESTful service. REST is not dependent on any protocol, but almost every RESTful service uses HTTP as the underlying protocol.

Call Control feature provides REST interfaces to allow an application to initiate and manage a call between two communication endpoints. Voice messaging feature provides a REST interface that allows clients to manage their voice mails stored on an Avaya Aura® Messaging server. Avaya Breeze™ communicates to the messaging servers by using IMAP (Internet Message Access Protocol), based on RFC 3501 for retrieving, deleting and purging voice mails.

### REST Versioning

Ensure that the REST request's ACCEPT header contains the supported version. For information on supported versions, see the REST API documentation.

### Engagement Call Control and Communication Manager

Engagement Call Control has visibility and control over all the Communication Manager calls, be they station to station, station to trunk, or trunk to station. Engagement Call Control uses Application Enablement Services (Application Enablement Services) to communicate to Communication Manager.

### Engagement Call Control snap-ins

The Engagement Call Control comprises the following snap-ins:

- **Unified Collaboration Administration (UCA)**: UCA reads the configuration data from System Manager and provides it as hierarchical data to Avaya Breeze™ for provider provisioning.
- **Unified Collaboration Model (UCM)**: Engagement Call Control uses the call model provided by UCM. Engagement Call Control depends on UCM for call events and uses the UCM APIs to send third party call operations to the Call Server Connector snap-in.
- **Call Server Connector (CSC)**: This is the connector snap-in that communicates to Communication Manager through the Device, Media and Call Control (DMCC) interface in Application Enablement Services. CSC integrates with UCM to provide real time view of the call activities to the UCM clients.
- **Engagement Call Control (ECC)**: This snap-in provides REST APIs for all the call control and messaging operations. This snap-in publishes call events and voice mail events to external clients.

Publication of call progress events and the APIs for the notification subscription are provided through the Eventing Connector.

**Note:**

Endpoints supported in Engagement Call Control are the same as those supported by Application Enablement Services. See the latest Application Enablement Services release notes to view the list of the supported endpoints.

# Functionalities supported by Engagement Call Control features

### Call control operations

Engagement Call Control supports the following call control operations:

- Make Call
- Get Call
- Drop Call
- Drop Connection
- Answer Call
- Hold Call
- Retrieve Call
- Get Call Forward

- Set Call Forward
- Cancel Call Forward
- Get Connections By Address
- Get Call Connections
- Get Connections Details
- Redirect Call
- Single Step Transfer
- Consult Initiate
- Complete Transfer
- Complete Conference
- Cancel Consult

## Messaging operations

Engagement Call Control supports the following messaging operations:

- Get Messagebox by Id: Gets message box information for the given id, which includes metadata of all messages in the message box and the count.
- Get Message by Id: Gets the metadata for a particular message.
- Get All Messages: Gets the metadata for all messages in the message box.
- Get Message Flags: Gets all message flags for a particular message.
- Set Message Flags: Sets the message flag for a particular message.
- Get Message Parts: Gets the metadata of all parts in a message.
- Get Message Part by Id: Gets the metadata of a part in the message.
- Get Message Part Content: Gets the media or the audio file for the voice mail.
- Purge All Messages in Trash: Removes all messages that has the **taggedForDeletion** flag set to **true**.

**Tip:**

Use the Web Call Controller sample snap-in to try the call and messaging operations.

## Events

Engagement Call Control supports the following events:

- ALERTING
- ANSWERED
- PARTICIPANT_DROPPED
- CONFERENCED
- TRANSFERRED
- HELD
- UNHELD

- ACTIVE
- FAILED
- TRANSFER_COMPLETE
- CONFERENCE_COMPLETE
- CALL FORWARD
- REDIRECT EVENTS

# Chapter 3: Interoperability

## Product interoperability

The following are minimal requirements:

- System Manager 7.0.0.1
- Avaya Breeze™ 3.2
- Application Enablement Services 6.3.3 with Super patch 5 onwards with latest service packs available.
- Communication Manager Release 6.3.x onwards.
- Avaya Aura® Messaging Release 6.3.2

| Call Server Connector / Avaya Breeze™ version | Application Enablement Services version | Compatibility |
|---|---|---|
| 3.1 | 6.3 | Yes |
| | 7.0 | Yes |
| | 7.0.1 | Change the TLS setting on Application Enablement Services. Navigate to **Networking** > **TCP / TLS Settings**, and select the **Support TLSv1.0 Protocol** check box. Restart Application Enablement Services. |
| 3.1.1 | 6.3 | Yes |
| | 7.0 | Yes |
| | 7.0.1 | Change the TLS setting on Application Enablement Services. Navigate to **Networking** > **TCP / TLS Settings**, and select the **Support TLSv1.0 Protocol** check box. Restart Application Enablement Services. |
| 3.1.1.1 | 6.3 | Yes |
| | 7.0 | Yes |
| | 7.0.1 | No change in TLS setting required on Application Enablement Services |

*Table continues…*

| Call Server Connector / Avaya Breeze™ version | Application Enablement Services version | Compatibility |
|---|---|---|
| 3.1.1.1 | 6.3 | Yes |
| | 7.0 | Yes |
| | 7.0.1 | No change in TLS setting required on Application Enablement Services |
| 3.2 | 6.3 | Yes |
| | 7.0 | Yes |
| | 7.0.1 | No change in TLS setting required on Application Enablement Services |

# Chapter 4: Application Enablement Services and Communication Manager configuration

## Application Enablement Services and Communication Manager configuration

Before you deploy the Engagement Call Control solution, you must:

- Install System Manager Release 7.0.0.1
- Install Avaya Breeze™ Release 3.1.
- Add the Avaya Breeze™ servers and assign the servers to a General Purpose Large cluster.
- Complete the replication of the Avaya Breeze™ servers in the cluster.
- Install Application Enablement Services Release 6.3.3 or later. For more information, see *Deploying Avaya Aura® Application Enablement Services in Virtualized Environment*.
- Add the Application Enablement Services license file in System Manager Element Manager.
- Install and configure Communication Manager Release 6.3.x onwards. For more information, see *Deploying Avaya Aura® Communication Manager*.
- Add Communication Manager to System Manager inventory, and perform the Communication Manager synchronization.
- Configure Application Enablement Services for Engagement Call Control. For more information, see Configuring Application Enablement Services on page 18.
- Configure Application Enablement Services Dial Plan rules. For more information, see Configuring dial plan rules on page 28.

Engagement Call Control solution Release 3.1.1 onwards supports the following:

- Communication Manager High Availability configuration.
- Application Enablement Services Geo-Redundant High Availability configuration.

For more information, see *Administering and Maintaining Avaya Aura® Application Enablement Services*.

# Configuring Communication Manager for Engagement Call Control snap-in deployment

## About this task

Perform the following configurations in Communication Manager to administer and send the Communication Manager UCID over ASAI.

## Procedure

1. Log in to the Communication Manager SAT terminal.
2. Type `change system-parameters features`.
3. On System Parameters Features page 5, set **Create Universal Call ID (UCID)** to **Y**.
4. Enter `x` for **UCID Network Node ID**, where x is unique within the network.
5. On page 13, set the **Send UCID to ASAI?** field to `y`.
6. Type **`list signaling-group`** to view the list of signaling group
7. Type **`change signaling-group <signaling-group id>`**.
8. Remove the Communication Manager configuration as a feature server. On page 1 of the relevant Signaling Group, ensure that **IMS** is set to **n**.
9. If a SIP station needs to work with Engagement Call Control, type **`change station extension`**. On Stations Administration page 6, ensure that the value for **Type of 3PCC Enabled** is **Avaya**.
10. If you use TCP entity links between Communication Manager and Session Manager, and if the endpoint is registered over TCP, you must set **ENABLE_OOD_MSG_TLS_ONLY** and **SET CONFIG_SERVER_SECURE_MODE** parameters to **0** in the Endpoints Settings file.

# Configuring multiple Communication Manager

## About this task

This configuration is required only when more than one Communication Manager is being configured as provider.

## Procedure

1. On Communication Manager SAT terminal, `type trunk group n`, where *n* is a trunk group configured between Communication Manager and Session Manager.
2. On page 3, set the **UUI Treatment** field to **shared**.
3. Set the **UCID Send** field to **y**.
4. Save the changes.

5. On Communication Manager SAT terminal, run the `save translation all` command to save the changes permanently.

# Configuring Application Enablement Services

## Before you begin

Install Application Enablement Services.

## Procedure

1. Install the Application Enablement Services license on System Manager.

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

   **Note:**

   From the Application Enablement Services management console > Status, ensure that the DMCC and TSAPI license status displays **Online**. The DMCC and TSAPI licsense status must be in the **Normal Mode**.

2. Add a switch connection for the TSAPI link. See Adding a switch connection on page 23.
3. Add a Communication Manager IP. See Editing a Processor Ethernet name or IP address on page 25.
4. Configure Application Enablement Services for Engagement Call Control solution. See Administering TSAPI links on page 25 and Configuring AE Services for Engagement Call Control Solution on page 26.
5. To check whether the Tlink you have chosen is secure. On the Application Enablement Services web interface, click **Status** > **Status and Control** > **TSAPI Service Summary**. Select the **Tlink** status button and ensure that the **Tlink** name contains **-S**.
6. Test the TSAPI link status. On the Application Enablement Services web interface, click **Status** > **Status and Control** > **TSAPI Service Summary**. For your Switch Name, ensure that the **Status** field displays **Talking**, and the **State** field displays **Online**.

# Adding an Application Enablement Services user

## Procedure

1. Log in to Application Enablement Services management console.
2. Click **User management** > **User Admin** > **Add User**
3. On the Add User screen, enter the following:
   - **UserID**: Any user ID.

- **Common Name**: Any name.
- **Surname**: Any surname.
- **User Password**: Password.
- **Confirm Password**: Reenter the password.

4. On the Add User screen, in the **CT User** field, select **Yes**.
5. Click **Apply**.
6. Click **Security** > **Security Database** > **CTI users** > **List All Users**.
7. On the CTI Users screen, select the user that you created.
8. Click **Edit**.
9. On the Edit CTI user screen, select **Unrestricted Access**.
10. Click **Apply Changes**.

# Adding CLANs to the network

## About this task

If you are using a media server that uses CLANs, you must add the CLANs to the Communication Manager network.

**Important:**

All CLANs dedicated to AE Services should be in a separate network region from those CLANs servicing endpoints. CLANs that provide connectivity for other endpoints should be in another network region.

**Note:**

Some configurations will require more network regions. See the AE Services documentation for details.

## Procedure

1. Type `change node-names ip`.

   Communication Manager displays the IP NODE NAMES form.
2. Complete the following fields on the IP NODE NAMES form.
   a. In the **Name** field, type the name you want to assign to this CLAN, for example `CLAN1`.
   b. In the **IP Address** field, type the IP address you want to assign to this CLAN.
3. Type `add ip-interface` <*board location*> (where <*board location*> is the board location for the CLAN, for example `1A06`).

   Communication Manager displays the IP INTERFACES form.

4. Complete the following fields on the IP INTERFACES form.
   a. In the **Node Name** field, type <*CLAN name*>, for example `CLAN1`.
   b. In the **IP Address** field, accept the default.
   c. In the **Subnet Mask** field, type the appropriate subnet mask for your network configuration.
   d. In the **Gateway Node Name** field, type the name of the gateway node for your network configuration.
   e. In the **Enable Interface** field, type `y`.
   f. In the **Network Region** field, type `1`.
   g. In the **VLAN** field, accept the default.
   h. In the **Target socket load and Warning level** field, accept the default.
   i. In the **Auto** field, type `y` .
5. Type `add data-module next`.

   Communication Manager displays the DATA MODULE form.
6. Complete the following fields on the DATA MODULE form.
   a. In the **Data Extension** field, accept the default value.
   b. (Required) In the **Type** field, type `ethernet`.
   c. (Required) In the **Port** field, type the board location and port 17, for example `1D07017 .`
   d. In the **Name** field, type the name you want to assign to the data module, for example `CLAN1DATA`. This name is not used for further administration. It is a name you use to help you identify the data module.
   e. In the **Network uses 1's for Broadcast Addresses** field, type `y`.

# Enabling Processor Ethernet

## About this task

Processor Ethernet support on the S85xx, S87xx, and S88xx Communication Manager media servers requires Communication Manager 3.1 or later. Follow this procedure to enable Processor Ethernet on S85xx, S87xx, and S88xx Communication Manager media servers.

**Note:**

On the S8300 and S8400 Communication Manager media servers, Processor Ethernet support is enabled by default.

## Procedure

1. Type `display system-parameters customer-options`.

2. Verify that Processor Ethernet is enabled. You must perform this verification step before proceeding with the next step.
3. Type `add ip-interface procr`.

**Note:**

Beginning with AE Services 6.1, the Processor Ethernet interface provides a message rate of 1000 messages per second, full duplex, for S8510, S87xx, and S88xx media servers. For the S8500 media server, the Processor Ethernet provides a message rate of 720 messages per second, full duplex. For S83xx and S84xx media servers, the Processor Ethernet interface provides a message rate of 240 messages per second, full duplex.

# Enabling AE Services

## About this task

Enabling AE Services refers to administering the transport link between Communication Manager and AE Services. You need to enable AE Services if any of the following AE Services features are to be employed.

- Device, Media, and Call Control (DMCC) applications that use Registration Services or Call Information Services (1st party call control)
- DMCC applications that use Call Control Services (3rd party call control)
- Telephony Web Service
- JTAPI
- TSAPI
- CVLAN
- DLG (ASAI applications)

## Procedure

1. Type `change ip-services`.

   Communication Manager displays the IP SERVICES form.
2. Complete Page 1 of the IP SERVICES form as follows:
   a. In the **Service Type** field, type `AESVCS`.
   b. In the **Local Node** field, type the appropriate entry based on whether you are using a Processor Ethernet interface or a CLAN interface:
      - For Communication Manager S8300, S8400, S85xx, S87xx, and S88xx systems that use a processor ethernet interface, type `procr`.

**Note:**

On the S8300 and S8400 Communication Manager media servers, Processor Ethernet support is enabled by default. On S85xx S87xx, and S88xx Communication Manager media servers, Processor Ethernet support is not enabled by default. To enable AE Services Processor Ethernet support, see Enabling Processor Ethernet.

- For DEFINITY Server Csi systems and Communication Manager S8400, S85xx, S87xx, and S88xx systems that use a CLAN interface, type <*nodename*> (where <*nodename*> is the name of the CLAN).

  You can locate node names by typing `display node-names ip` and checking the **Local Node** field on the IP NODE NAMES form.

c. In the **Local Port** field, accept the default (**8765**).

   If you are adding more than one CLAN for AE Services, repeat Step 2 for each CLAN you add.

3. Complete Page 3 of the IP SERVICES form as follows.

   a. In the **AE Services Server** field, type the name of the AE Services server, for example `aeserver1`.

   **Note:**

   On the AE Services server you can obtain this name by typing uname -n at the command prompt. The name you use on Communication Manager must match the AE Services server name exactly.

   b. In the **Password** field, create a password that consists of 12 to 16 alphanumeric characters, for example `aespassword1`.

   **Important:**

   This is the password that the AE Services administrator must set on the AE Services Server (**Communication Manager Interface > Switch Connections > Edit Connection > Switch Password**). The passwords must exactly match on both Communication Manager and the AE Services server.

   c. Set the **Enabled** field to `y`.

# Administering a CTI Link for TSAPI, JTAPI, DMCC with Call Control, Telephony Web Service, or an AE Services integration

## About this task

Follow these steps from a Communication Manager SAT to administer a CTI link type ADJ-IP.

### Procedure

1. Type `add cti-link` <*link number*>, for example `add cti-link 5`.
2. Complete the CTI LINK form as follows:
   a. In the **Extension** field, type an unassigned station extension.
   b. In the **Type** field, type `ADJ-IP`.
   c. In the **Name** field, type <*name of AE Server*>, for example `aeserver1`.

# Adding a switch connection

### About this task

You must administer a switch connection for all applications except DMCC applications that use device and media control only.

If you have a DMCC application that uses device and media control only, and you want to administer a switch connection to use the gatekeeper feature, see the AE Services documentation.

### Procedure

1. From the AE Services Management Console main menu, select **Communication Manager Interface > Switch Connections**.
2. On the **Switch Connections** page, in the **Add Connection** field, type a switch connection name (for example `Switch1`) .

   The switch connection name can be any name you want to use, but it must consist of alphanumeric characters only.
3. Click **Add Connection**.
4. On the **Connections Details** page, do the following:
   a. In the **Switch Password** field, type the password that the Communication Manager administrator assigned when the node name of the AE Services Server on the IP-Services form was administered, see Enabling AE Services.
   b. In the **Confirm Switch Password** field, retype the password.
   c. In the **Msg Period** field, accept the default (30 minutes).
   d. For the **Provide AE Services certificate to switch** check box, do one of the following:
      - For Communication Manager Release 6.3.6 or later, accept the default (check box is checked).

        Ensure that the Communication Manager recognizes the Certificate Authority used by the AE Services certificate.
      - For any previous release of Communication Manager, clear the **Provide AE Services certificate to switch** check box.

e. For the **Secure H323 Connection** check box, do one of the following:

- For Communication Manager Release 6.3.6 or later and TLS for the H.323 Signaling Channel (normally associated with FIPS Mode), select the **Secure H323 Connection** check box.
- For any previous release of Communication Manager without TLS for the H.323 Signaling Channel, clear the **Secure H323 Connection** check box.

  For information about Communication Manager media servers that support a Processor Ethernet connection, see Enabling AE Services.

f. Click **Apply**.

AE Services adds the switch connection and returns you to the **Switch Connections** page. The new switch connection name appears in the **Connection Name** column.

# Checking the status of a switch connection -- from Communication Manager to the AE Services server

### About this task

Once you have added a switch connection on the AE Services server, you validate the switch connection by checking its status on both the AE Services server and on Communication Manager.

### Procedure

To check the status of a switch connection on Communication Manager, type `status aesvcs link`.

# Checking the status of a switch connection -- from the AE Services Server to Communication Manager

### Procedure

1. From the AE Services Management Console main menu, select **Status > Status and Control > Switch Connections Summary**.
2. From the **Switch Connections Summary** page, select the switch connection you just added, for example, **Switch1**.
3. Click **Connection Details**.
4. Review the information on the **Connection Details** page. Verify that the connection state is **Talking** and the Online/Offline status is **Online**.

**Important:**

After you complete this procedure, check the status of the switch connection from Communication Manager to the AE Services server.

# Editing a Processor Ethernet name or IP address

## About this task

After you add a switch connection, you must associate the switch connection name with Processor Ethernet host name or IP address.

## Procedure

1. From the AE Services Management Console main menu, select **Communication Manager Interface > Switch Connections** .
2. From the **Switch Connections** page, select the connection name you just added (for example, **Switch2**).
3. Click **Edit PE/CLAN IPs**.
4. Choose a Processor Ethernet.
5. On the **Add/Edit Processor Ethernet IP** page, in the **Add/Edit Name or IP** field, type the host name or the IP address of the Processor Ethernet.

   **Note:**

   You must use either an explicit IPv4 address or an IPv6 address. Do not use an IPv4-mapped/compatible IPv6 address that combines the IPv4 and IPv6 formats.
6. Click **Add/Edit Name or IP**.

# Adding TSAPI Links

## About this task

TSAPI links are used by TSAPI applications, JTAPI applications, Telephony Web Service applications, DMCC applications that use Call Control, and DMCC applications that use Logical Device Feature Services. TSAPI links are also used for the AE Services integration for Microsoft Live Communications Server and the AE Services integration for IBM Lotus Sametime.

You can administer one TSAPI link for each switch connection.

## Procedure

1. On Application Enablement Services Management Console, go to **AE Services** > **TSAPI** > **TSAPI Links**.

2. Click **Add Link**.
3. On the Add TSAPI Links page, do the following:
   a. In the **Link** field, select the link number.
   b. In the **Switch Connection** field, click a switch connection value.
   c. In the **Switch CTI Link Number** field, select the switch CTI link number administered on Communication Manager for this TSAPI link.
   d. In the **ASAI Link Version** field, select **7**.

      Link version 7 is only supported for Communication Manager 6.3.6 and later and AE Services 6.3.3 and later.
   e. In the **Security** field, select one of the following:

      - **Unencrypted**: To use unencrypted client connections.
      - **Encrypted**: To encrypt client connections for this TSAPI link.
      - **Both**: To use both encrypted and unencrypted client connections.

      If you select **Both**, all TSAPI clients using the Encrypted Advertised TLINK require AES 4.1 or later TSAPI client. Any TSAPI clients using the Unencrypted Advertised TLINK can be earlier versions.
   f. Click **Apply Changes**.
4. On the Apply Changes to Link page, click **Apply**.
5. Restart the TSAPI Service for the changes to take effect. To restart the TSAPI Service do the following:
   a. On Application Enablement Services Management Console, go to **Maintenance** > **Service Controller**.
   b. On the Service Controller page, select **TSAPI Service**.
   c. Click **Restart Service**.

      The TSAPI service has successfully restarted when the Controller Status displays **Running**.

# Configuring Application Enablement Services for Engagement Call Control snap-in deployment

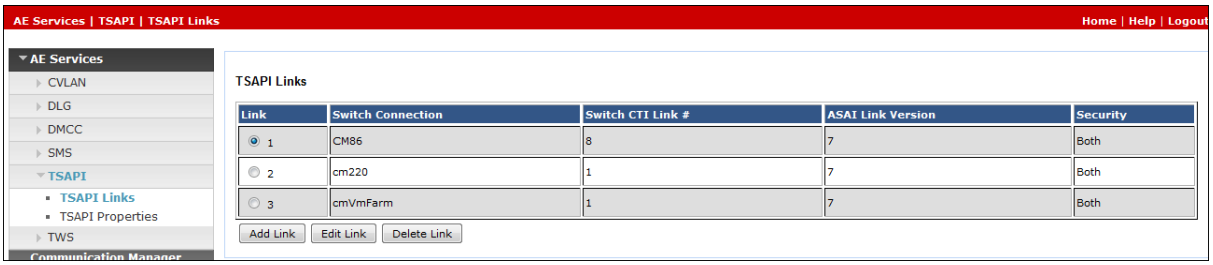
## About this task

Perform the following procedure to configure a secure link between Application Enablement Services and Communication Manager.

## Procedure

1. Log in to the Application Enablement Services console.

2. Click **AE Services** > **TSAPI** > **TSAPI Links**.




3. Select the link that you want to configure, and click **Edit Link**.
4. Modify the **Security** field to **Both**.
5. Modify the **ASAI Link Version** to the latest version that is available.

   For example, use version 7 for **ASAI Link Version**.
6. Click **Apply changes**.
7. Click **Security** > **Host AA** > **Service Settings**.
8. Select the appropriate check boxes, and click **Apply changes**.

**Note:**

For Mutual TLS (MTLS) to work, you must use **non-default certificate** on Application Enablement Services. MTLS will not work if Application Enablement Services is using the default certificate.

When MTLS is enabled on TSAPI service, two different clients with different certificates cannot connect to Application Enablement Services at the same time.

9. Restart the TSAPI services. To restart the TSAPI services, go to **Maintenance** > **Service Controller**, select the TSAPI service, and click **Restart Service** button.

# Adding the Avaya Breeze™ CA certificate to the Application Enablement Services trust store

## Procedure

1. Login to the Application Enablement Services web console.
2. Click **Security** > **Certificate Management** > **CA Trusted Certificates**.
3. Click **Import**.
4. Browse to the location where you have stored the System Manager CA certificate.
5. Click **OK** to import the certificate.

**Note:**

If you use a third party certificate, import that certificate to Application Enablement Services.

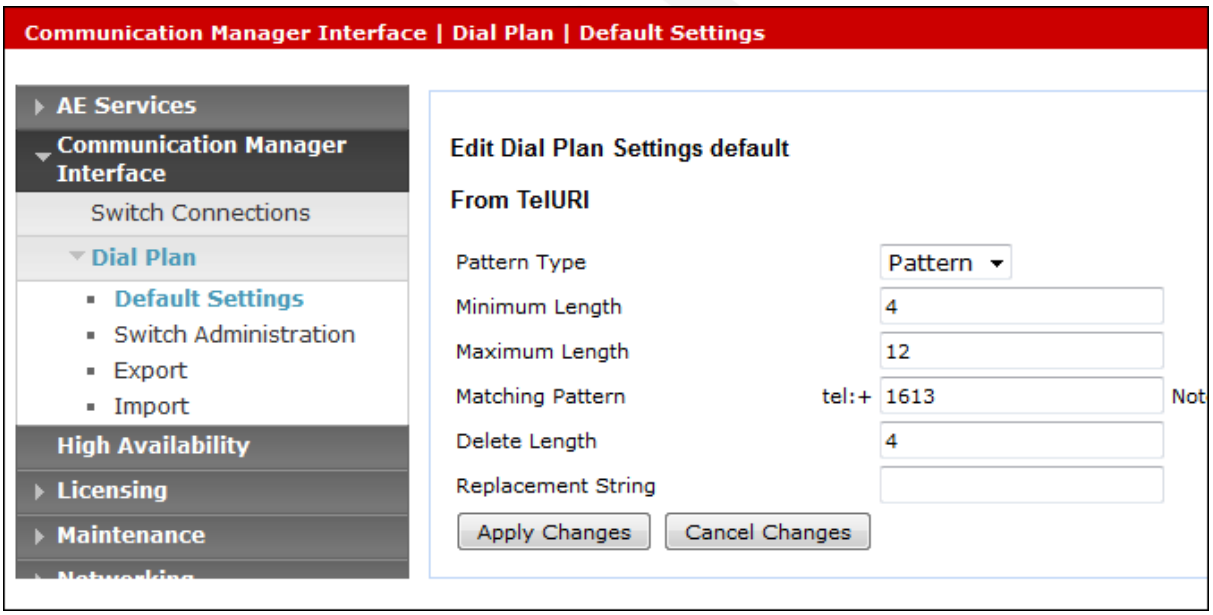
# Configuring Application Enablement Services Dial Plan rules

## About this task

Perform the following procedure to configure the dial plan rules for the E164 format.

## Procedure

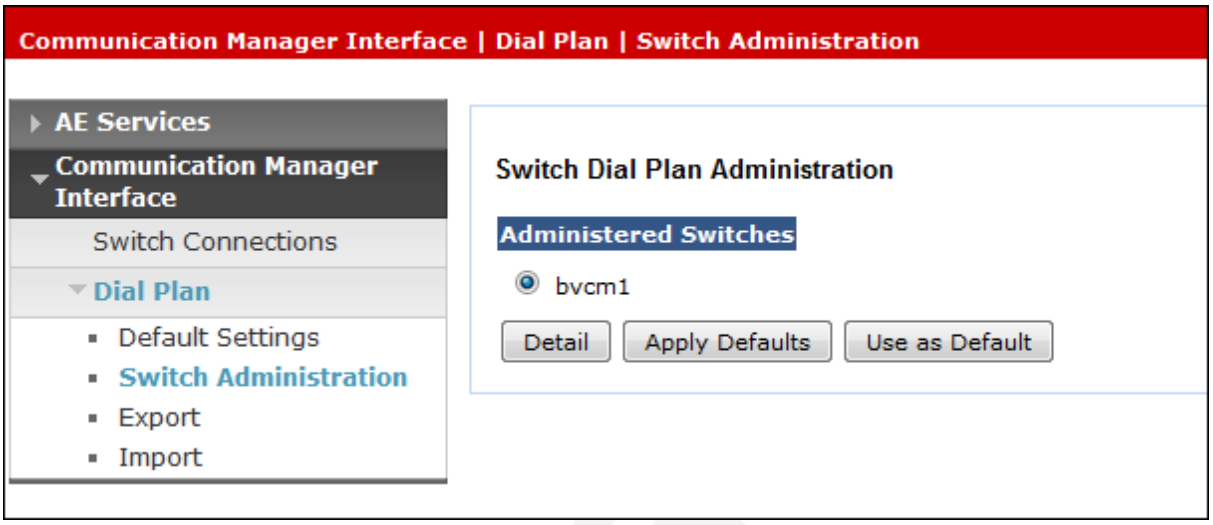
1. Log in to the Application Enablement Services web interface.
2. Click **Communication Manager Interface** > **Dial Plan** > **Default Settings**.
3. Click **Add**.




4. Add the default dial plan settings. Specify the settings like pattern, minimum length, maximum length.
5. For Engagement Call Control to work with E.164 numbers, configure dialplan rules to convert the E.164 format to a dialable number.

   For more information, see *Administering and Maintaining Avaya Aura® Application Enablement Services*.
6. Click **Apply Changes** to add the dial plan settings.

7. To apply the dial plan to your switch:




   a. Click **Dial Plan** > **Switch Administration**.
   b. From the Administered Switches section, select your switch and click **Apply Defaults**.

      Your default dial plan settings will be applied to your administered switch. This configuration is mandatory for E.164 format.

# System Manager Trust Management

## Checklist for using System Manager as a Certificate Authority to generate signed certificates

| No. | Task | Reference | ✔ |
|---|---|---|---|
| 1 | Create an end entity for the AE Services server. | Creating an end entity for the AE Services server on page 30 | |
| 2 | Create the AE Services server certificate. | Creating the AE Services server certificate on page 30 | |
| 3 | Download the System Manager CA certificate that signed the AE Services server certificate. | Downloading the System Manager CA certificate that signed the AE Services server certificate on page 31 | |
| 4 | Import the System Manager CA certificate into the AE Services server. | Importing the System Manager CA certificate into the AE Services server on page 31 | |

*Table continues…*

| No. | Task | Reference | ✔ |
|---|---|---|---|
| 5 | Import the new AE Services server certificate into the AE Services server. | Importing the new AE Services server certificate into the AE Services server on page 32 | |

# Creating an end entity for the AE Services server

## Procedure

1. On the System Manager web console, navigate to **Services** > **Security** > **Certificates** > **Authority**.
2. Click **Add End Entity**.
3. In the **End Entity Profile** field, click `INBOUND_OUTBOUND_TLS`.
4. Type a username and password.

   This password is used to encrypt the P12 trust store file.
5. Complete the fields that you want in your certificate:
   - **E-mail address**: *labmanager@yourcompany.com*
   - **CN, Common name**: *aeshostname.yourcompany.com*
   - **OU, Organizational Unit**: `IT`
   - **O, Organization**: *your Company Name*
   - **L, Locality**: `Denver`
   - **ST, State or Province**: `CO`
   - **C, Country**: `US`
6. In the **Certificate Profile** field, select **ID_CLIENT_SERVER**.
7. In the **CA** field, select **tmdefaultca**.
8. In the **Token** field, select **P12 file**.
9. Click **Add**.

   The system displays the `End Entity username added successfully` message.

# Creating the AE Services server certificate

## Procedure

1. On the System Manager web console, navigate to **Services** > **Security** > **Certificates** > **Authority**.
2. In the navigation pane, click **Public Web**.

3. On the Public Web page , click **create key store**.
   a. Enter the user name and password of the end entity, and click **OK**.
   b. Select the certificate key length.

      2048 is recommended.
   c. Click **Enroll**.
   d. Save the server certificate to a known location.

   This certificate is the signed server certificate that you have to import into the AE Services server.

## Downloading the System Manager CA certificate that signed the AE Services server certificate

### Procedure

1. On the System Manager web console, navigate to **ServicesSecurityCertificatesAuthority**.
2. In the navigation pane, click **Public Web**.
3. Click **Fetch CA certificates**.
4. Click **Download PEM chain**.
5. Save the CA certificate to a known location.

   This certificate is the CA certificate that needs to be imported into the AE Services server.

## Importing the System Manager CA certificate into the AE Services server

### Procedure

1. On the AE Services Management console, navigate to **Security** > **Certificate Management** > **Trusted Certificates**.
2. Click **Import**, and upload the System Manager CA certificate you downloaded earlier.
3. Click **Apply**.

   You must import this CA before you can import the server certificate.

# Importing the new AE Services server certificate into the AE Services server

## Procedure

1. On the AE Services Management console, navigate to **Security** > **Certificate Management** > **Server Certificates**.
2. Click **Import**, and upload the new AE Services server certificate you created earlier.
3. Click **Apply**.
4. Enter the password you used while creating the end entity.
5. Click **Apply**.
6. Click **Apply**.

   You must import the CA before you can import the server certificate

# Chapter 5: Deployment

## Deploying Engagement Call Control Solution

### Modifying the disk allocation for Engagement Call Control deployment profiles

#### About this task

Perform this procedure to modify the disk allocation according to the deployment profile you choose. This is a prerequisite before you load and install the Engagement Call Control snap-ins. When you deploy the Avaya Breeze™ ova, select the appropriate deployment profile and modify the memory accordingly.

#### Procedure

1. Ensure that the Avaya Breeze™ VM is Powered down.
2. Right-click the Avaya Breeze™ VM, and select **Edit Settings**.
3. Edit the **Provisioned Size** of **Hard Disk 1** from **50GB** to **150GB**.
4. Click **OK**.
5. Power up the VM.

### Resources and memory configuration

The following table specifies the resource and memory configuration for Engagement Call Control deployments. This snap-in provides both call control functionality and programmatic access to voicemail.

The number of Avaya Breeze™ servers required for each deployment profile varies based on whether voicemail access is in use, and on the number of Avaya Aura® Messaging Servers used. If the deployment is using only the call control functionality, use the value indicated in the **Avaya Breeze Servers required without Voicemail**. If voicemail access is in use, use the value indicated in the **No. of Messaging Servers : Avaya Breeze Servers required with Voicemail** column. The first number in this column indicates the number of Avaya Aura® Messaging Servers and the second number indicates the required number of Avaya Breeze™ servers.

For more information about the deployment profiles, see *Avaya Engagement Call Control Snap-in Reference*.

| Deployment Profile | Avaya Breeze Footprint | Max Call Rates | Max. no. of Communication Managers | Max no. of endpoints | Maximum simultaneous calls | Avaya Breeze Servers required without Voicemail | No. of Messaging Servers : Avaya Breeze Servers required with Voicemail |
|---|---|---|---|---|---|---|---|
| Small | Profile 2 - 4 vCPU, 8 GB | 2 CPS | 2 | 15000 | 360 | 1 | 1:1<br>2:1<br>3:2 |
| Medium | Profile 4 - 8 vCPU, 16 GB | 15 CPS | 3 | 30000 | 2700 | 2 | 1:2<br>2:2<br>3:2 |
| Large | Profile 4 - 8 vCPU, 16 GB | 24 CPS | 3 | 41000 | 4320 | 2 | 1:2<br>2:3<br>3:3 |

**Note:**

Choose Profile 2 for Voicemail when you have 1 to 3 Avaya Aura® Media Server servers.

Media fetches /Avaya Aura® Media Server = 4

For information about Application Enablement Services and Communication Manager deployment profiles, see the respective product deployment guides.

# Configuring Avaya Breeze™ for Engagement Call Control solution

## About this task

Perform this configuration before you install and configure the Engagement Call Control snap-ins.

## Procedure

1. Create a **General Purpose Large** cluster.
2. Add the Avaya Breeze™ servers to the cluster.

   Wait for replication to complete before you proceed with the snap-in installation.
3. Ensure that the Avaya Breeze™ server is not sequenced for the extensions on the same Communication Manager that are expected to call each other.

4. For Avaya Breeze™ to validate the certificate presented by Application Enablement Services, provision one of the following trusted certificates for Avaya Breeze™:
   - The CA certificate that was used to sign the Application Enablement Services certificate.
   - The Application Enablement Services certificate.

# Engagement Call Control solution deployment checklist

This table specifies the deployment steps for the Engagement Call Control solution.

See Resources and memory configuration on page 33 to determine your deployment profile and the resources for the deployment. Use the same deployment type, that is, SMALL, MEDIUM, or LARGE, when you install UCM, UCA, and CSC.

| No. | Task | Description | ✔ |
|---|---|---|---|
| 1 | Check the prerequisites for the Engagement Call Control (ECC) snap-in deployment. | See the topic Prerequisites before installing the Engagement Call Control solution on page 16. | |
| 2 | Applying the license. | Apply TSAPI Basic User License for Engagement Call Control. The number of licenses should match the number of devices that you want to access by using Engagement Call Control. | |
| 3 | Load the Unified Collaboration Model (UCM) snap-in. | Download the .svar from PLDS. For information on loading the snap-in, see the topic Loading the snap-in on page 36. | |
| 4 | Load the Unified Collaboration Administration (UCA) snap-in. | Download the .svar from PLDS. For information on loading the snap-in, see the topic Loading the snap-in on page 36. | |
| 5 | Load the Call Server Connector (CSC) snap-in. | Download the .svar from PLDS. For information on loading the snap-in, see the topic Loading the snap-in on page 36. | |
| 6 | Load the Engagement Call Control (ECC) snap-in. | Download the .svar from PLDS. For information on loading the snap-in, see the topic Loading the snap-in on page 36. | |
| 7 | Install the Unified Collaboration Model snap-in. | See the topic Installing the snap-in on page 37. | |
| 8 | Configure the Unified Collaboration Model snap-in attributes | See the topic Configuring the Unified Collaboration Model snap-in attributes on page 38. | |
| 9 | Install the Unified Collaboration Administration snap-in. | See the topic Installing the snap-in on page 37. | |

*Table continues…*

| No. | Task | Description | ✔ |
|---|---|---|---|
| 10 | Configure the Unified Collaboration Administration snap-in. | See the topic Configuring Unified Collaboration Administration Snap-in Attributes on page 39. | |
| 11 | Install the Call Server Connector snap-in. | See the topic Installing the snap-in on page 37. | |
| 12 | Configure the Call Server Connector snap-in attributes. | See the topic Configuring the Call Server Connector snap-in attributes on page 40. | |
| 13 | Install the Engagement Call Control snap-in. | | |
| 14 | Reboot all the servers in the cluster. | See the topic Installing the snap-in on page 37. | |
| 15 | Configure Avaya Aura® Messaging for Voicemail operations.<br>**Note:**<br>This is an optional step. | See the topic Configuring Avaya Aura Messaging for Voicemail operations on page 42. | |
| 16 | Configure Engagement Call Control snap-in. | See the topic Configuring Avaya Aura Messaging for Voicemail operations on page 42. | |

**Note:**

Do not install Engagement Call Control and Work Assignment solution snap-ins on the same cluster. We do however support sharing of common components of these solutions. For more information, see White paper for co-deployment of Engagement Call Control and Work Assignment solution.

After you deploy the solution, if you modify the snap-ins or the snap-in attributes, you must reboot the servers in the cluster for the changes to take effect.

# Loading the snap-in

## About this task

This task describes how to load a snap-in to System Manager from your development environment or alternate location. You can skip this step when installing a pre-loaded snap-in. Pre-loaded snap-ins are provided with the Avaya Breeze™ Element Manager in System Manager.

## Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.
2. In the left navigation pane, click **Service Management**.
3. Click **LOAD**.

   You can load multiple snap-ins at a time.

4. On the Load Service page, depending on the browser used, click **Browse** or **Choose File**, and browse to your snap-in file location.

   You can select up to 50 files or a maximum of 3 GB files whichever limit is reached first.

5. Click **Browse** again repeat until all the files are selected.
6. Click **LOAD**.

   **Note:**

   If there are licensed snap-ins you will be presented with a separate EULA for each of those snap-ins.

7. Click **Open**.

   Your snap-in file should end with `.svar`. The Service Archive (svar) file is provided by service developers.

8. On the Load Service page, click **LOAD**.

   For Avaya snap-ins only, you will be prompted to accept the Avaya End User License Agreement (EULA).

9. If you agree to the Avaya EULA, click **Accept**.

   Your snap-in displays on the Service Management page with a **State of Loaded**.

   If you clicked **Cancel** to reject the agreement, the load action stops.

# Installing the snap-in

## About this task

For .svar files larger than 50 MB, schedule snap-in installation during a maintenance window.

## Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze**.
2. In the left navigation pane, click **Service Management**.
3. Select the snap-in that you want to install.
4. Click **Install**.
5. Select the cluster(s) where you want the snap-in to reside, and click **Commit**.
6. To see the status of the snap-in installation, click the Refresh Table icon located in the upper-left corner of the **All Services** list.

   **Installed** with a green check mark indicates that the snap-in has completed installation on all the Avaya Breeze™ servers in the cluster. **Installing** with a yellow exclamation mark enclosed in a triangle indicates that the snap-in has not completed installation on all the servers.

**Note:**

Most of the snap-ins automatically start but a snap-in developer has provision to control starting/stopping snap-in.

7. To track the progress of a snap-in installation, on the Server Administration page, click the **Service Install Status** for an Avaya Breeze™ server.

   The system displays the Service Status page with the installation status of all the snap-ins installed on that server.

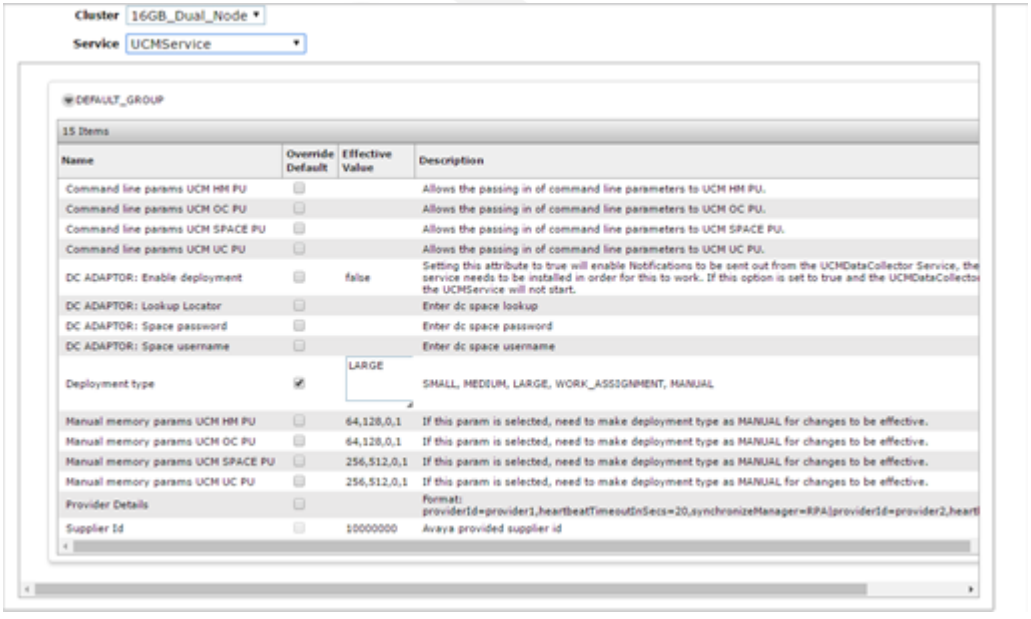
# Configuring the Unified Collaboration Model snap-in attributes

## Before you begin

Load and install the Unified Collaboration Model snap-in.

## Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.
2. In the left navigation pane, click **Configuration** > **Attributes**.
3. From the **Cluster** field, select the cluster on which you have installed the Unified Collaboration Model snap-in.
4. From the **Service** field, select **UCMService**.
5. Configure the Unified Collaboration Model snap-in attributes at the cluster level:




   a. For the **Deployment Type** field, select the **Override Default** checkbox and specify the Effective value according to your deployment.

b. Do not change the values for the **Command line params UCM UC PU**, **Manual memory params UCM SPACE PU**, and **Manual memory params UCM UC PU** fields.

6. Click **Commit**.
7. On the dialog prompt, click **OK** to save the snap-in attribute configuration.

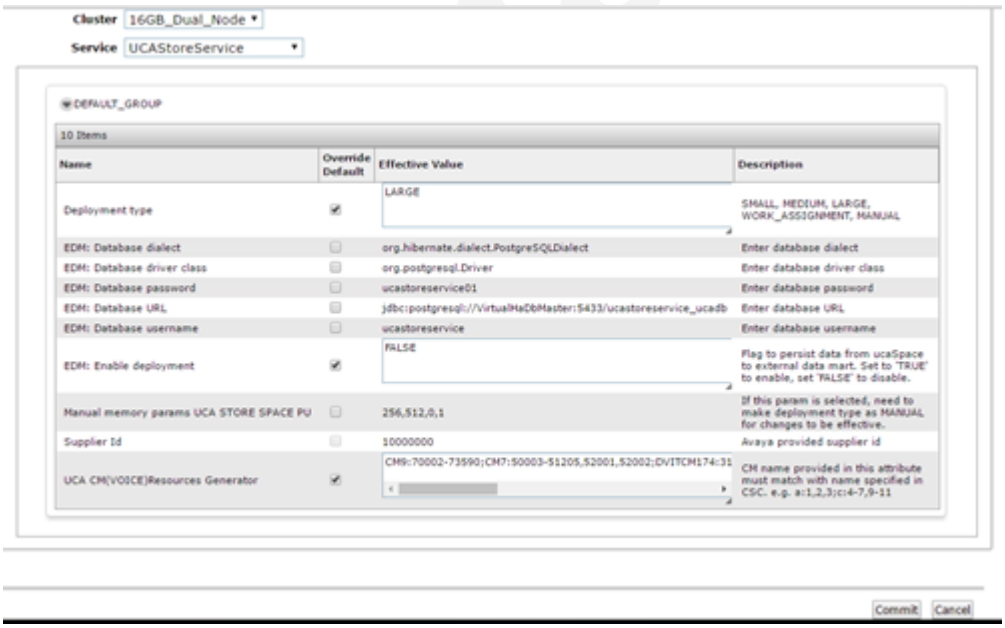
# Configuring the Unified Collaboration Administration snap-in attributes

## Before you begin

Load and install the Unified Collaboration Administration snap-in.

## Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.
2. In the left navigation pane, click **Configuration** > **Attributes**.
3. From the **Cluster** field, select the cluster on which you have installed the Unified Collaboration Administration snap-in.
4. From the **Service** field, select **UCAService**.
5. Configure the UCA snap-in attributes at the cluster level.




6. Select the **Override Default** checkbox for the **Deployment type** field.
7. Determine the value according to your deployment and specify the **Deployment type** value as SMALL, MEDIUM or LARGE.

8. For the **UCA CM filter list** field, select the **Override Default** checkbox and enter the value in one of the following formats:
   - For new, enter a list of providers separated by semi-colons with a colon after the provider if a range of resource extension needs to be declares.

     A blank or empty filter is considered invalid and will not replicate anything.

     The range must be a single number or two numbers separated by a dash. Multiple ranges can be declared for each provider separated by commas and must in ascending order and must not overlap.

     For example, `a:1,2,3;b;c:4-7,9-11`
   - For backwards compatibility, a list of providers separated by commas with no spaces and at least one character before and after every comma.

     For example, `a,b,c`

     A blank or empty filter is considered invalid and will not replicate anything.
   - `ALL` for all Communication Managers and extensions synced and available on System Manager.

**Note:**

For a multi-node cluster, the minimum number of Communication Manager instances is 1 and the maximum number of Communication Manager instances is 3.

For a single node cluster, the minimum number of Communication Manager instances is 1 and the maximum number of Communication Manager instances is 2.

9. Set the **UCA polling interval in minutes** field to **5**.
10. Click **Commit**.
11. On the dialog prompt, click **OK** to save the snap-in attributes.

# Configuring the Call Server Connector snap-in attributes

## Before you begin

Add an AES user.

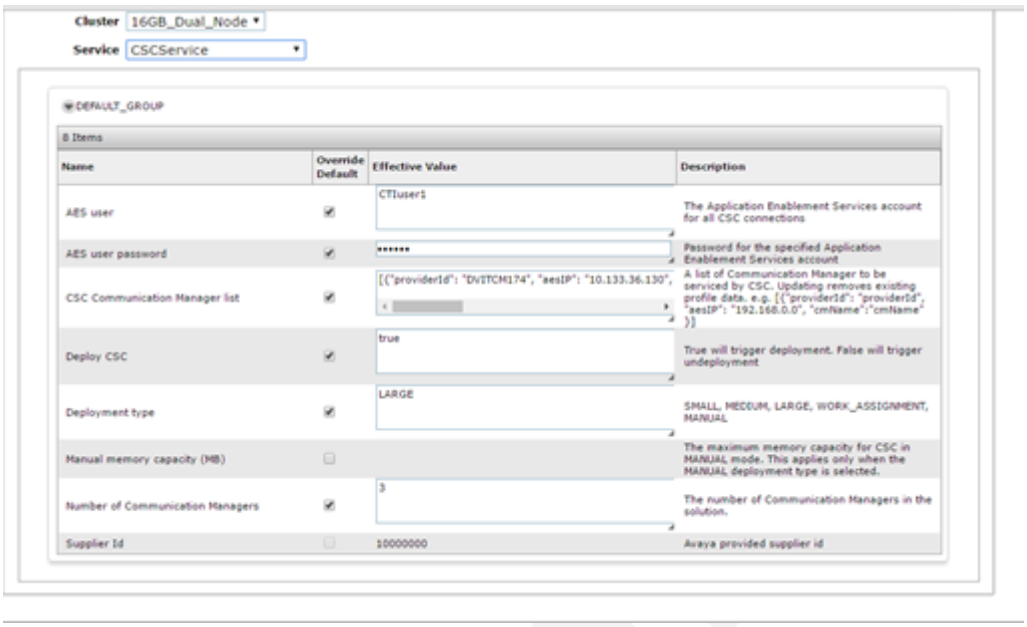
**Important:**

Configure the Call Server Connector snap-in attributes at the cluster level only. Do not configure the attributes at the global level.

## Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.
2. In the left navigation pane, click **Configuration** > **Attributes**.
3. From the **Cluster** field, select the cluster on which you have installed the Call Server Connector snap-in.

4. From the **Service** field, select **CSCService**.
5. Configure the following Call Server Connector snap-in attributes at the cluster level:




   a. For the **AES User** field, specify the user name for the Application Enablement Services account used by CSC.
   b. For the **AES user password** field, specify the associated password as configured in Application Enablement Services.
   c. For the **CSC Communication Manager list** field, select the **Override Default** checkbox and the specify the Effective Value as **[{"providerId": "providerId", "aesIP": "192.168.0.0", "cmName":"cmName" }]**.

      In this step, the providerId is the name of the Communication Manager as specified in **System Manager** > **Inventory** > **Manage Elements**.

      `aesIP` is the IP address of the Application Enablement Services that has the TSAPI link with the Communication Manager.

      `cmName` is the Communication Manager name as configured in **AES** > **TSAPI** > **TSAPI Links** > **Communication Manager Interface** page in **Switch Connection**

      Example value for the multiprovider configuration in CSC: `[{"providerId": "DVITCM174", "aesIP": "10.133.36.130", "cmName":"CM174"}, {"providerId": "CM7", "aesIP": "10.133.36.130", "cmName":"CM7"}]`.
   d. Set the **Deploy CSC** value to **True**.
   e. For the **Deployment Type** field, select the **Override Default** checkbox and specify the Effective Value according to your deployment size.

      For the **Number of CMs** field, select the **Override Default** checkbox and specify the Effective Value as `<# of CMs>`.

**Note:**

1. For a multi-node cluster, the minimum value is 1 and maximum value is 3.
2. For a single node cluster the minimum value is 1 and maximum value is 2.

6. Click **Commit** to save the snap-in attribute configuration.

# Configuring Avaya Aura® Messaging for voice mail operations

## About this task

This configuration procedure is optional. Perform this procedure if you want to configure the Engagement Call Control solution for voicemail operations.

## Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.
2. In the left navigation pane, click **Server Administration**.
3. Click the Avaya Breeze™ servers.

   The system displays the Avaya Breeze Instance Editor page.
4. Make a note of the **UCID Network Node ID** and the **Security Module IP** of all the servers that are a part of the Engagement Call Control cluster.
5. Click **Configuration** > **Attributes**.
6. Select the appropriate **Cluster** and **EngagementCallControl** for the **Service** field.
7. Set the **AAM Password** at the global or cluster level.

   **Note:**

   This is the password with which Avaya Aura® Messaging and Engagement Call Control establish trust. This password must be the same irrespective of the number of servers in the cluster.
8. Login to the Avaya Aura® Messaging console.
9. Click **Administration** > **Messaging** > **Server Settings (Storage)** > **Trusted Servers**.
10. Add the Avaya Breeze™ servers as a trusted server in Avaya Aura® Messaging.

    **Important:**

    The **Trusted Server Name** must be in the format `EDPServer-[UCID]`. For example, if the UCID Network ID is 7, then the trusted server name must read **EDPServer-7**.
11. On the Trusted Server page, ensure that the:
    a. **Machine Name/IP Address** is the Security Module IP of the Avaya Breeze™ cluster.
    b. **Service Name** matches the TrustedServer Name.
    c. **IMAP4 Super User Access Allowed** is set to Yes.

d. **Password** matches the password set in Step 7.

12. Click **Messaging System (Storage)** > **System Administration**.
13. Select the **IMAP4 Port** and **IMAP4 SSL Port** fields.
14. To deploy Avaya Aura® Messaging using RAID configuration, set the **Avaya Aura® Messaging RAID configuration** to **ESXi is 'RAID + 0'**.
15. Click **Save**.
16. Perform steps 10 to 14 for each Avaya Breeze™ server.
17. On the Avaya Breeze™ CLI, type **`ce dlogw EngagementCallControl`**

    The system displays a heartbeatService on Engagement Call Control, indicating an active connection with Avaya Aura® Messaging.

# Using the sample snap-in to test Engagement Call Control Engagement Call Control capabilities

## About this task

Web Call Controller (WCC) is a sample snap-in that is available along with the Avaya Breeze™ SDK. Use Web Call Controller to try the capabilities of the Engagement Call Control solution.

## Procedure

1. Download the Web Call Controller .svar and load the snap-in.
2. Install the Web Call Controller snap-in.
3. On the **Configuration** > **Attributes** page, click the **Service Clusters** tab.
4. From the **Cluster** field, select the cluster on which you are installing the snap-in.
5. From the **Service** field, select the **WebCallController** snap-in.
6. Configure the following sample snap-in attributes:
   a. **IP/FQDN of Avaya Breeze Asset or Cluster IP**: Select the **Override Default** checkbox and specify the Effective Value. For a two-node cluster, enter the cluster IP address. For a single node cluster, enter the asset IP of the Avaya Breeze™ server.
   b. **Use https as transport**: Set this value to **true** if you want the sample snap-in to send only the HTTPS requests only.
7. Click **Commit** to save the configuration.
8. Access the sample snap-in through `http(s)://<assetip>/services/WebCallController/main.jsp`.

   For single node clusters, use the asset IP instead of the cluster IP while accessing the sample snap-in.

9. Try the Engagement Call Control capabilities like Make Call, Get Call, Get Connections and so on.

**Note:**

For more information, see the *Web Call Controller sample snap-in documentation*. The sample snap-in documentation is available with the Engagement Call Control SDK.

# Installing trust certificate of HTTPS server

## Before you begin

Certificates that you intend to add as trusted certificates must be accessible to System Manager.

## About this task

If the callback URL specified in the REST CALL events subscription is HTTPS, CA certificate of the event listener server must be added to the trust store of Avaya Breeze™. Use the following procedure to add CA certificate of the event listener server to the trust store of Avaya Breeze™.

## Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze**.
2. In the navigation pane, click **Cluster Administration**.
3. Select the cluster on which Engagement Call Control snap-in is installed.
4. Click **Certificate Management** > **Install Trust Certificate (All Avaya Breeze Instances)**.
5. From the **Select Store Type to install trusted certificate** menu, select **WebSphere** or **ALL**.
6. Click **Browse** to the location of your Trust Certificate, and select the certificate.
7. Click **Retrieve Certificate**, and review the details of the Trusted Certificate.
8. Click **Commit**.

# Installing the Avaya Aura® Messaging certificate on the Avaya Breeze™ cluster

## Procedure

1. Navigate to **System Manager** > **Inventory** > **Manage Elements**.
2. Select **Avaya Breeze node** from the **Manage Elements** table, and click **More Actions** > **Configure Trusted Certificates**.

   **Manage Elements** opens Trusted Certificate page.
3. Click the **ADD** button, and select **WEBSPHERE** from the drop-down list.

4. Select **Import using TLS**, and configure the following fields:
    a. Enter the Avaya Aura® Messaging IP address.
    b. Enter the Avaya Aura® Messaging port number as 993.
5. Click **Retrieve Certificate**, and complete the certificate installation on the node.
6. Repeat the process for all **Avaya Breeze node**s in the cluster.
7. Reinstall the Engagement Call Control snap-in to apply the changes.

# Chapter 6: Upgrading Engagement Call Control solution

## Upgrading Engagement Call Control solution

### Before you begin

Upgrade System Manager to Release 7.0.1. For more information, see *Upgrading Avaya Aura® System Manager*.

### Procedure

1. Upgrade Avaya Breeze™ to Release 3.1.1.

   For more information, see *Upgrading Avaya Breeze™*.
2. Uninstall the older versions of Engagement Call Controlsolution snap-ins.

   For more information, see “Uninstalling a snap-in”.
3. Uninstall older versions of Engagement Call Control eventing connector and CECS.
4. Install new versions of eventing connector and CECS.
5. Delete all the older version of Engagement Call Controlsolution snap-ins.
6. Reboot all nodes in the Avaya Breeze™ cluster.
7. Enable the Avaya Breeze™ cluster Database.
8. Load and install new versions of 3.2 Engagement Call ControlSnap-in in the order UCA,UCM and CSC from Service Management.

   For more information, see *Snap-in Install guide*.
9. Configure the attributes of Engagement Call Control solution snap-ins.
10. Load and install the new WCC version.
11. Reboot all nodes in the Avaya Breeze™ cluster simultaneously.

# Chapter 7: Performance

## Configuring cluster attributes for production deployment

### About this task

Set the following voice mail cluster attributes for performance and scalability.

### Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.
2. In the left navigation pane, click **Cluster Administration**.
3. Select the cluster on which you have deployed the **EngagementCallControl** snap-in, and click **Edit**.
4. Set the **HTTP or HTTPS limit on connections** to **6000**.
5. Set the **HTTP or HTTPS traffic rate limit in bytes/second** to **0**.

# Chapter 8: Troubleshooting

## Log files

See the following table to view the Engagement Call Control solution log files:

| Snap-in | Log file location |
|---|---|
| UCA | Snap-in logs: `/var/log/Avaya/services/UCAService/` |
| UCM | Snap-in logs: `/var/log/Avaya/services/UCMService/`<br>PU logs: `/var/log/Avaya/dcm/pu/UCMService` |
| CSC | Snap-in logs: `/var/log/Avaya/services/CSCService/CSCService.log`<br>PU logs: `/var/log/Avaya/dcm/pu/CSCService` |
| ECC | Snap-in logs: `/var/log/Avaya/services/EngagementCallControl/` |

Logs are also printed in asm.log, TextLog* at `/var/log/Avaya/sm/`.

## Searching for log files

**Procedure**

1. On the System Manager web console, click **Services** > **Events**
2. In the navigation pane, click **Logs** > **Log Viewer**.
3. Click **Advanced Search**.
4. In the **Criteria** field, select one of the following :
   - **Log ID**
   - **Host Name**
   - **Product Type**
   - **Severity**
   - **Message**
   - **Event ID**
   - **Process name**

- **Facility**
- **Time Stamp**

5. Enter the search value.
6. If you want to add another search condition:
   a. Click the + sign and repeat the steps 3 and 4.
   b. Click the – sign to delete a search condition.
   c. Select the **AND** or **OR** operator from the drop-down field.
7. Click **Search** .

# Events

The following are the events raised by the UCA, UCM, and CSC snap-ins:

| Event ID/ Event | Component | Severity | Description |
|---|---|---|---|
| PU_STATUS | UCA | Normal | Status of a PU is updated by the datagrid. |
| PU_STATUS | UCA | Warning | Status of a PU changes from INTACT to SCHEDULED. |
| PU_FAILED | UCA | Warning | Unknown error from datagrid during deployment. |
| MASTER_NODE | UCA | Normal | Host machine xxxx changes to master node. Seen during start and fail over scenarios. |
| PROP_UPDATE | UCA | Normal | Svar properties updated and persisted in manager space. Commonly seen during deployment. |
| Link Down | CSC | | Link between CSC and Application Enablement Services is down. |
| Alarm | UCA | | Failure to write DRS data as UCA space is not available. |
| Replication failed | UCA | Infrequent | UCA space is available, yet DRS change cannot be written. |
| Deploy war context completed | UCA | | Deployment is successful. |
| Svar attribute update | UCM | Infrequent | Svar attribute is updated. |
| Deployment error | UCM | Infrequent | Data grid throws an exception on deployment. |

# Troubleshooting

## Calls for newly added users or extensions do not work

### Condition

Calls for newly added users or synchronized extensions on System Manager do not work.

### Cause

When you add a new Communication Manager extension in System Manager, it is reflected in UCA after 5 minutes, which is the UCA polling time. The extension is then populated in UCASpace by CSC. Thus after you add a new extension, it takes around 5 minutes for Engagement Call Control to use it.

### Solution

After you add a user or a new Communication Manager extension in System Manager, wait for 5 minutes before using the extension for Engagement Call Control call operations.

## Duplicate snap-in attribute seen after loading Web Call Controller Snap-in in the upgrade scenario

### Condition

After loading new Web Call Control snap-in, the **IP/FQDN of security module or cluster IP** attribute is duplicated.

### Solution

1. Configure the same value for the **IP/FQDN of security module or cluster IP** attribute as configured earlier, and click **Commit**.
2. You could delete the older version of Web Call Control Snap-in to view only one copy of the attribute.

## SIP Endpoints registered over TCP do not work

### Condition

CTI operations on addresses that are registered by SIP endpoints over TCP do not work.

### Solution

On the Endpoints Settings file, ensure that **ENABLE_OOD_MSG_TLS_ONLY** and **SET CONFIG_SERVER_SECURE_MODE** are set to **0**.

Ensure that you use TLS as this is more secure.

# Inter-Provider Call sharing UCID across providers

### Condition

In an inter-provider call where a UCID is shared across providers, you cannot use the UCID for Engagement Call Control REST call control services.

### Cause

When a UCID is shared across different service providers, the Engagement Call Control solution cannot decide which provider to use. Thus you cannot use the UCID for call control services.

### Solution

Ensure that you use the specific call Id for call control operations.

# Multi device access errors

### Condition

With multi-device access, a user cannot specify which device is to be used for Engagement Call Control call control operations.

### Cause

When a user logs in with multiple devices from multiple endpoints, Session Manager forks the call to all the devices. The user can use any of the device to attend the call. However, with Engagement Call Control, users cannot specify which device is to be used for call control operations. Engagement Call Control does not support the EC500 feature or forking enablement.

### Solution

Engagement Call Control does not support multiple device access. The last device logged in receives all the calls. Other devices do not receive the calls. Ensure that you logout of all the devices and login only through one device at a time.

# Privilege violation error

### Condition

Engagement Call Control Rest operation fails and the system displays a Privilege violation error.

### Cause

The system displays this error message when SIP stations do not subscribe to Communication Manager features.

### Solution

1. Ensure that you provision endpoints with **SET ENABLE_AVAYA_ENVIRONMENT 1** in the Endpoints Settings file. Alternatively, set the **SET ENABLE_AVAYA_ENVIRONMENT** value to **Yes** from the craft menu.

2. If you have provisioned the endpoints, check for configuration issues related to dial plan. For more information on configuring dial plan, see Configuring dial plan rules on page 28.
3. Ensure that you have set the **DigitConversionAdapter** adaption module property in the **Session Manager** > **Adaptations** page. Configure this property to insert and delete appropriate digits for incoming and outgoing calls to Session Manager.
4. Check whether you are receiving a 403 response when you run the SM trace tool.

# Redirect operation fails

## Condition

Assume A calls B, and B redirects the call to C. If C sets call forwarding to D, the redirect operation fails.

## Cause

Redirect operation fails if call forwarding is enabled on an extension.

## Solution

Ensure that call forwarding is not set during the call operation. Chained forwarding is not supported in Engagement Call Control.

# Checking the status of a switch connection from Communication Manager to Application Enablement Services server

## Procedure

On the Communication Manager SAT terminal, type status `aesvcs` link.

# TSAPI Test

## About this task

To verify that client is set up correctly and the TSAPI Service has been administered correctly. TSAPI Test applies to TSAPI, JTAPI, and Telephony Web Service applications. To run TSAPI Test, on the AES web console, navigate to **Utilities** > **Diagnostic** > **AE Service** > **TSAPI Test**

For more information about TSAPI Test, see *Administering and Maintaining Avaya Aura® Application Enablement Services* .

# Chapter 9: Maintenance

## Editing the Engagement Call Control snap-in attributes

### About this task

Perform the following procedure if you want to edit the snap-in attributes for any of the snap-ins in the Engagement Call Control solution.

### Procedure

1. Go to the **Avaya Breeze** > **Configuration** > **Attributes** page.
2. Select the appropriate snap-in and cluster from the drop-down list.
3. Edit the snap-in attributes at the cluster level and click **Commit**.
4. Restart all the Avaya Breeze™ servers in the cluster.

## Changing the number of servers in an Engagement Call Control cluster

### About this task

Perform the following steps when you add or remove a server to the Engagement Call Control cluster. You must follow this procedure when you change from a single to a multi-node cluster or vice versa.

### Procedure

1. Add or remove a server to the Engagement Call Control cluster.
2. If you have changed a snap-in attribute after adding or removing a server, **Reboot** all the servers in the cluster.

# Chapter 10: Resources

## Documentation

### Developer Documentation

For more details on Engagement Call Control, see the following sections in the Engagement Call Control SDK:

- Web Call Controller (WCC) documentation to use WCC. WCC is a sample snap-in that is available with the Engagement Call Control Software Development Kit (SDK).
- A complete list of the REST APIs.
- Engagement Call Control events.
- Reference to video using Web Call Controller.

### User Documentation

| Title | Purpose | Audience |
|---|---|---|
| *Avaya Aura® Application Enablement Services Administration and Maintenance Guide* | This document provides information on configuring and administering Application Enablement Services. | Implementation engineers<br>System administrators |
| *Avaya Breeze™ Release 3.1 documentation* | The documentation provide information about architecture, administration, implementation, and configuration of Avaya Breeze™ 3.1. | Implementation engineers<br>System administrators |
| *Administering Avaya Aura® System Manager* | This document provides the procedures to administer and configure System Manager. | System administrators |
| *Deploying Avaya Aura® Communication Manager* | This document provides information on deploying Avaya Aura® Communication Manager. | Implementation engineers<br>System administrators |

**Related links**

Finding documents on the Avaya Support website on page 55

## Finding documents on the Avaya Support website

### About this task

Use this procedure to find product documentation on the Avaya Support website.

### Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

### Related links

Documentation on page 54

# Developer resources

Avaya DevConnect provides resources for Avaya Breeze™ developers.

You must register to access the DevConnect.

Basic DevConnect membership is free and gives you access to the following information and resources:

- Programming and product documentation
- Sample applications
- Videos
- Webinar recordings
- Forums

Upgraded membership options offer developer-oriented technical support and other program services.

Use a browser to navigate to the Avaya Breeze™ DevConnect website at http://www.avaya.com/breezedeveloper.

# Viewing Avaya Mentor videos

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

## About this task

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

## Procedure

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

**Note:**

Videos are not available for all products.

# Support

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

# Index


## A

add data-module command ..... 19
adding
TSAPI Links ..... 25
Adding a CLANs ..... 19
adding servers to the Engagement Call Control cluster ..... 53
Adding the Avaya Breeze CA certificate
AES trust store
to AES trust store
trust store ..... 27
add nodes
ECC cluster ..... 53
administering
TSAPI Links ..... 25
Administering a switch connection. ..... 23
Administering Switch Connections ..... 23
AE Services end entiry ..... 30
AE Services server certificate ..... 30, 32
AES trust store
add CA certificate
Avaya Breeze CA certificate ..... 27
Application Enablement Services
configure
ECC .....
Engagement Call Control solution ..... 18
ECC deployment ..... 26
Architecture
ECC snap-in solution ..... 10

## C

Call forwarding enabled
redirect fails ..... 52
Calls do not work
Engagement Call Control
ECC ..... 50
Calls for new users do not work ..... 50
Certificate Authority
certificate authority ..... 29
change history ..... 8
change node-names ip command ..... 19
changing disk allocation
150GB ..... 33
CLAN, adding ..... 19
configure Communication Manager
ECC solution
ECC deployment ..... 17
configure dial plan rules
ECC .....
Engagement Call Control solution ..... 28
Configure snap-in attributes
UCM
ECC ..... 38
Configuring AES ..... 18
configuring Application Enablement Services
Engagement Call Control
ECC deployment ..... 26
Configuring Application Enablement Services ..... 18
Configuring Avaya Aura Messaging for voice mail operations ..... 42
Configuring Avaya Breeze for ECC ..... 34
Configuring Call Server Connector snap-in attributes ..... 40
configuring Communication Manager
Engagement Call Control deployment
ECC deployment ..... 17
configuring Communication Manager for Engagement Call Control snap-in deployment ..... 17
configuring CSC snap-in attributes ..... 40
configuring dial plan rules
E 164 format ..... 28
Configuring Engagement Call Control ..... 34
Configuring IP services ..... 21
configuring performance related attributes ..... 47
Configuring the ..... 39
configuring UCA snap-in attributes ..... 39
Configuring UCM snap-in attributes ..... 38
configuring voice mail attributes for performance ..... 47
CTI link for TSAPI, JTAPI, Telephony Web Service, DMCC with Call Control, or an AE Services integration (Microsoft or IBM Sametime) ..... 22

## D

Deployment checklist
Engagement Call Control solution ..... 35
DevConnect ..... 55
duplicate attribute error ..... 50

## E

ECC ..... 9
configure dial plan rules ..... 28
events ..... 49
ECC deployment
prerequisites ..... 16
ECC troubleshooting ..... 51
Editing ECC solution snap-in attributes ..... 53
Editing snap-in attributes ..... 53
Enabling Processor Ethernet ..... 20
Engagement Call Control
architecture ..... 10
overview ..... 9
resources
memory configuration
deployment configuration

multi device access error *(continued)*
deployment configuration *(continued)*
sizing tool ..... 33
supported functionalities
call operations ..... 11
messaging operations ..... 11
test capabilities
sample snap-in to test
WCC ..... 43
troubleshooting
call sharing across providers ..... 51
multi device access error
MDA error ..... 51
Engagement Call Control configuration
Avaya Breeze ..... 34
Engagement Call Control events ..... 49
Engagement Call Control functionalities ..... 11
Engagement Call Control installation
checklist
license ..... 35
Engagement Call Control log files ..... 48
engagement call control solution ..... 46
Engagement Call Control solution ..... 9, 18, 48, 52
configuring
configure
snap-in attributes ..... 38
prerequisites ..... 16
Engagement Call Control solution installation
requirements
interoperability ..... 14
Engagement Call Control troubleshooting ..... 50, 51
CTI operations do not work
SIP endpoints over TCP do not work ..... 50
redirect call fails ..... 52
EULA ..... 36
Events
UCA ..... 49

## G

Gateway list (as opposed to H.323 Gatekeeper list), creating a switch connection name for a named list of CLAN IP addresses (for APIs that use the transport layer - DMCC, TSAPI, JTAPI, CVLAN, and DLG) ..... 23

## H

HTTPS ..... 44

## I

installing; Avaya Aura Messaging certificate ..... 44
installing; Avaya Aura Messaging certificate on Avaya Breeze cluster ..... 44
installing; Avaya Breeze cluster ..... 44
IP FQDN of security module or cluster IP ..... 50
IP services, configuring ..... 21

## L

loading snap-ins
service ..... 36
load snap-ins ..... 36
Logs
Engagement Call Control ..... 48

## M

Modifying disk allocation
Engagement Call Control
deployment profiles ..... 33

## P

preferred version
setting ..... 37
Privilege violation error ..... 51
Processor Ethernet, enabling ..... 20
Processor Ethernet name or IP address, editing ..... 25
product interoperability ..... 14

## R

Redirect call operation not supported ..... 52
remove nodes
ECC cluster ..... 53
removing servers from the Engagement Call Control cluster ..... 53

## S

Sizing tool
Engagement Call Control ..... 33
snap-in
installation ..... 37
loading ..... 36
snap-in attributes
configure
Engagement Call Control solution ..... 40
Snap-in attributes
UCA
UCM
CSC
ECC ..... 53
snap-in install status ..... 37
support ..... 56
Switch connection, administering ..... 23
Switch Connections, administering ..... 23
Switch connection status ..... 24
Switch Connection status (AE Services) ..... 24
System Manager CA certificate ..... 31

## T

Topology
Engagement Call Control ..... 10
Troubleshooting
Engagement Call Control ..... 50
privilege violation error ..... 51
trust certificate ..... 44
TSAPI Links
adding ..... 25
administering ..... 25

## U

UCA
snap-in attributes
configuring snap-in ..... 39
using sample snap-in to test Engagement Call Control ..... 43

## V

videos ..... 56
voice mail operations
Avaya Aura Messaging ..... 42
configure ..... 42

## W

Web Call Controller ..... 43