Avaya Aura® Contact Center and Avaya Aura® Unified Communications Platform Integration

Release 7.1
Issue 07.06
September 2021

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 as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

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 as indicated in the order, Documentation, or as authorized by Avaya in writing. 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.

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. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

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

The following applies only if the H.264 (AVC) codec is distributed with the product. 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 H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

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

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

Avaya is a registered trademark of Avaya Inc.

Contents

Chapter 1: Introduction

This document provides conceptual and procedural information to configure the Avaya Aura® Unified Communications platform for use with Avaya Aura® Contact Center.

Contact Center uses industry-standard SIP and CSTA (TR/87 over SIP) interfaces to communicate with SIP-enabled systems such as the Unified Communications platform. This integration gives Contact Center access to and control of the Avaya Aura® Unified Communications phones. The Avaya Aura® Unified Communications platform benefits from Contact Center skill-based routing, call treatments, reporting, and the graphical Orchestration Designer. Avaya Agent Desktop supports Avaya Aura® Unified Communications phones and continues to support voice, email, and Web chat contact types.

An Avaya Aura® Unified Communications (UC) platform supports up to three Avaya Aura® Contact Center (AACC) servers. The overall capacity of the combined AACC servers connected to a single UC platform must not exceed the maximum specified capacity of a single AACC instance connected to that UC platform. Where multiple AACC servers share a UC platform, AACC High Availability and or UC High Availability are not supported. Where multiple AACC instances share a single UC platform, the AACC instances use a single common SIP domain name.

Avaya Aura® Contact Center supports the following Avaya Aura® components:

Avaya Aura® component	Release
Avaya Aura® System Platform	7.0.x, 7.1.x, 8.0.x, 8.1.x
Avaya Aura® Communication Manager	7.0.x, 7.1.x, 8.0.x, 8.1.x
Avaya Aura® Application Enablement Services	7.0.x, 7.1.x, 8.0.x, 8.1.x
Avaya Aura® System Manager	7.0.x, 7.1.x, 8.0.x, 8.1.x
Avaya Aura® Session Manager	7.0.x, 7.1.x, 8.0.x, 8.1.x
Avaya Aura® Presence Services	7.0.0.1 or later, 8.0.x, 8.1.x

Important:

For more information about the supported Avaya Aura® Unified Communications Service Packs (SPs), Feature Packs (FPs), patches, and deployment types, refer to the Avaya Aura® Contact Center Release Notes.

You must configure the following Avaya Aura® Unified Communications components to work with Contact Center:

- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® Application Enablement Services

You use Avaya Aura® System Manager to configure Avaya Aura® Session Manager.

Note:

Avaya Aura® Contact Center does not support Avaya Aura® Communication Manager - Feature Server.

Prerequisites

- Read *Avaya Aura® Session Manager Overview.*
- Read *Administering Avaya Aura® Session Manager*.

Related resources

Avaya Aura® Contact Center Documentation

The following table lists the documents related to Avaya Aura® Contact Center. Download the documents from the Avaya Support website at https://support.avaya.com.

Title	Use this document to:	Audience
Overview		

Table continues…

Title	Use this document to:	Audience
Avaya Aura® Contact Center Overview and Specification	This document contains technical details you need to set up your Contact Center suite. The document contains the background information you need to plan and engineer your system (server preparation information, routing options, licensing configurations, and hardware configuration). The document also contains background information you require to install all software components that are part of and work with Contact Center. General information about considerations for upgrading your existing suite of Contact Center is also included. This document contains strategies and requirements to plan your network configuration and prepare your servers for Contact Center software installations.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center and Avaya Aura® Unified Communications Solution Description	This document describes the solution architecture, suggested topologies, and capacities for the Avaya Aura® Unified Communications platform. This document also describes the features and functional limitations of certain configurations.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center and Avaya Communication Server 1000 Solution Description	This document describes the solution architecture, suggested topologies, and capacities for the Avaya Communication Server 1000 platform. This document also describes the features and functional limitations of certain configurations.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center Documentation Catalog	This document describes available Avaya Aura® Contact Center documentation resources and indicates the type of information in each document.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center Terminology	This document contains definitions for the technical terms specific to Contact Center.	Customers and sales, services, and support personnel

Table continues…

Title	Use this document to:	Audience
Contact Center Performance Management Data Dictionary	This document contains reference tables that describe the statistics and data in the historical and real-time reports generated in Contact Center.	System administrators and contact center supervisors
Implementing		
Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration	This document contains information and procedures to integrate the Avaya Aura® Unified Communications platform with Contact Center.	Implementation personnel
Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration	This document contains information and procedures to integrate the Avaya Communication Server 1000 platform with Contact Center.	Implementation personnel
Deploying Avaya Aura® Contact Center DVD for Avaya Aura® Unified Communications	This document contains information about Contact Center DVD installation, initial configuration, and verification for the Avaya Aura® Unified Communications platform.	Implementation personnel
Deploying Avaya Aura® Contact Center DVD for Avaya Communication Server 1000	This document contains information about Contact Center DVD installation, initial configuration, and verification for the Avaya Communication Server 1000 platform.	Implementation personnel
Deploying Avaya Aura® Contact Center Software Appliance for Avaya Aura® Unified Communications	This document describes how to deploy the Avaya Aura® Contact Center Software Appliance for the Avaya Aura® Unified Communications platform.	Implementation personnel
Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications	This document contains information for Contact Center preparation, process, initial configuration, and verification of the installation on the Avaya Aura® Unified Communications platform.	Implementation personnel
Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000	This document contains information for Contact Center preparation, process, initial configuration, and verification of the installation on the Avaya Communication Server 1000 platform.	Implementation personnel
Avaya Aura® Contact Center and Proactive Outreach Manager Integration	This document provides conceptual and procedural information on the integration between Avaya Aura® Contact Center (AACC) and Avaya Proactive Outreach Manager (POM); it describes the tasks required for AACC and POM integration.	Implementation personnel

Table continues…

Title	Use this document to:	Audience
Upgrading and patching Avaya Aura® Contact Center	This document contains information and procedures to upgrade from previous releases to Contact Center, migrating the databases, and information and procedures to download and install service packs.	Implementation personnel and system administrators
Administering		
Avaya Aura® Contact Center Server Administration	This document contains information and procedures for day-today maintenance of all servers in the Contact Center suite, including server maintenance tasks, administrative tasks, managing data, configuring data routing, performing archives, and backing up data. It also describes the optional configuration procedures for server configuration.	System administrators
Avaya Aura® Contact Center Client Administration	This document contains information and procedures to configure the users and user access, skillsets, server management, and configuration data in the Contact Center database.	System administrators and contact center supervisors
Using Contact Center Orchestration Designer	This document contains information and procedures to configure script and flow applications in Contact Center Orchestration Designer.	System administrators
Maintaining		
Maintaining Avaya Aura® Contact Center	This document contains routine maintenance procedures such as installing service packs, and maintaining the databases for the Contact Center system.	System administrators and support personnel
Troubleshooting Avaya Aura® Contact Center	This document contains system-wide troubleshooting information and procedures for Contact Center hardware, software, and network.	System administrators and support personnel
Contact Center Event Codes	This document contains a list of errors in the Contact Center suite and recommendations to resolve them. This document is a Microsoft Excel spreadsheet.	System administrators and support personnel
Using		

Table continues…

Title	Use this document to:	Audience
Using Avaya Aura® Contact Center Reports and Displays	This document contains procedures to generate performance reports, and to monitor and analyze performance data and performance measurements.	System administrators and contact center supervisors
Using Agent Desktop for Avaya Aura® Contact Center	This document provides information and procedures for agents who use the Agent Desktop application to accept, manage, and close contacts of all media types in Contact Center.	Contact center agents and supervisors
Using the Contact Center Agent Browser application	This document provides information and procedures for agents who use the Agent Browser application to log on to Contact Center and perform basic tasks.	Contact center agents
Using Avaya Workspaces for AACC and ACCS	This document describes the tasks that Contact Center agents can perform using Avaya Workspaces.	Contact center agents and supervisors

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

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

Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

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

Note:

Videos are not available for all products.

Support

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

Chapter 2: Changes in this release

The following sections describe the changes in *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.

Features

New features in Release 7.1 base build

See the following sections for information about new features in the Release 7.1 base build:

Avaya Aura Contact Center interoperates with Avaya H175 Video Collaboration Station on page 17

Interoperability with the Avaya Workplace Client softphone on page 17

Support of Video contacts on page 17

New features in Release 7.1 Service Pack 1

There are no new features in Release 7.1 Service Pack 1.

New features in Release 7.1 Service Pack 2

There are no new features in Release 7.1 Service Pack 2.

New features in Release 7.1 Service Pack 3

There are no new features in Release 7.1 Service Pack 3.

New features in Release 7.1 Feature Pack 1

See the following sections for information about new features in the Release 7.1 Feature Pack 1:

Interoperability with Avaya Aura on page 17

Interoperability with the Avaya Workplace Client softphone on page 17

New features in Release 7.1 Feature Pack 2

See the following sections for information about new features in the Release 7.1 Feature Pack 2:

Interoperability with Avaya Aura on page 17

Interoperability with Avaya Workplace Client on page 18

Avaya Aura® Contact Center interoperates with Avaya H175 Video Collaboration Station

From Release 7.1 Contact Center supports Avaya H175 Video Collaboration Station. This phone is designed to work with SIP platforms only.

Interoperability with the Avaya Workplace Client softphone

From Release 7.1 Contact Center interoperates with Avaya Workplace Client version 3.5.x and 3.6 for Windows. You can now use the Avaya Workplace Client softphone as agent stations. Avaya Workplace Client version 3.6 supports video contacts.

Support of Video contacts

From Release 7.1 Avaya Aura® Contact Center supports routed video contacts. Video contacts are reported on in both real-time and historical reports. You can view video calls using Avaya Workplace Clientor Avaya Vantage™, however you must use Avaya Agent Desktop for call control actions.

To support video contacts, your solution must include Avaya Aura® Web Gateway.

You can enable Video for your Contact Center in Avaya Aura® Media Server and then configure Video using Avaya Aura® Communication Manager.

Interoperability with Avaya Aura®

From Release 7.1 Feature Pack 1, Avaya Aura® Contact Center supports interoperability with Avaya Aura® 8.1.2 and 8.1.3.

Interoperability with Avaya Aura®

From Release 7.1 Feature Pack 2, Avaya Aura® Contact Center supports interoperability with Avaya Aura® 7.1.3 and 8.1.3.2.

Interoperability with the Avaya Workplace Client softphone

From Release 7.1 Feature Pack 1, Contact Center interoperates with Avaya Workplace Client version 3.9 and 3.11 for Windows and Android.

Interoperability with Avaya Workplace Client

From Release 7.1 Feature Pack 2, Contact Center interoperates with Avaya Workplace Client 3.20 for Windows and Android. Agents and supervisors can use the latest Avaya Workplace Client with Agent Desktop and Avaya Workspaces.

Other changes

Other changes in the Release 7.1 base build

There are no other changes in the Release 7.1 base build.

Other changes in Release 7.1 Service Pack 1

There are no other changes in Release 7.1 Service Pack 1.

Other changes in Release 7.1 Service Pack 2

There are no other changes in Release 7.1 Service Pack 2.

Other changes in Release 7.1 Service Pack 3

There are no other changes in Release 7.1 Service Pack 3.

Other changes in Release 7.1 Feature Pack 1

There are no other changes in Release 7.1 Feature Pack 1.

Other changes in Release 7.1 Feature Pack 2

There are no other changes in Release 7.1 Feature Pack 2.

Chapter 3: Configuration Fundamentals

This section provides the conceptual information that you need to configure the Avaya Aura® Unified Communications platform to work with Avaya Aura® Contact Center.

Prerequisites

Read the *Avaya Aura® Unified Communications platform Release Notes*.

Third call appearance button functionality

In a SIP-enabled contact center with an Avaya Aura® Communication Manager, Avaya Aura® Contact Center supports a maximum of three call appearance buttons configured per agent station with Restrict Last Appearance (RLA) enabled. When Restrict Last Appearance is enabled, the last call appearance button of each agent station is always reserved for outbound calls or consults initiated by the agent. The first two call appearance buttons (lines) are for receiving incoming calls. If an agent is busy on one line, another line is free to accept another incoming call. The third line continues to be reserved for calls initiated by the agent. Only one call can be active at a time, the other calls must be on hold. If an agent is busy on a direct call or is handling a skillset call, no other skillset call is routed to them.

Third call appearance button matrix of call scenarios:

Agent Action Lines	Receive Skillset Call	Receive Personal Call	Make Personal Call (from desk phone)	Make Personal Call (from Agent Desktop)	Initiate Consult
3 lines available	Yes [1]	Yes [1]	Yes [1]	Yes [1]	—
1 line busy	No	Yes [2]	Yes [1]	Yes [1]	Yes [1]
2 lines busy	No	No	Yes [2]	Yes [2]	Yes [2]
3 lines busy	No	No	No	No	No

Table continues…

Agent Action Lines	Receive Skillset Call	Receive Personal Call	Make Personal Call (from desk phone)	Make Personal Call (from Agent Desktop)	Initiate Consult
1 busy and 1 consult	No	No	Yes [2]	Yes [2]	No
2 busy and 1 consult	No	No	No	No	No

- **Note 1**: Supported with two call appearance lines per agent station.
- **Note 2**: Supported with three call appearance lines per agent station.

Third call appearance button considerations:

- If an agent is on a DN call, the agent is not presented with a Contact Center (Route Point) call. When the agent is on a DN call, the agent is set busy and cannot take a Contact Center call.
- This feature is not multiplicity for voice. If an agent is busy on a Contact Center call, the agent is not presented with another Contact Center call.
- No more than three line appearances can be configured on an agent station. Contact Center does not support four or more lines.
- Avaya Agent Desktop does not list the parties in the joined/conference call. Therefore it does not provide the capability to drop other parties.
- Contact Center does not support configuring different coverage paths depending on whether the call is personal call or a Contact Center call.

Blocking multiple and nested consults when initiated using Agent Desktop

If an attempt is made to initiate a second consult using Agent Desktop, Contact Center checks if the call on which the consult is being initiated is already a part of a consult. If it is, then the consult request is rejected with a feature error. The checking for the consult is on the call hence it can block the following multi-consult scenario: Agent1 is presented with a call (DN / CDN). Agent1 initiates a consult (DN/CDN – transfer/conference). Agent2 answers the call. Agent2 initiates a consult (DN/CDN – transfer/conference).

Blocking multiple and nested consults when initiated using the desk phone

Communication Manager blocks multiple and nested consults when a second consult is initiated from the phone sets. If an agent initiating the consult, already has another consult call then the consult request is rejected. The checking for the consult is for the agent hence the following multi-consult scenario continues to work: Agent1 is presented with a call (DN/CDN). Agent1 initiates a consult (DN/CDN – transfer/conference). Agent2 answers the call. Agent2 initiates a consult (DN/CDN – transfer/conference).

Real time reporting

The real time reporting of the agent status for agents with two Call Appearance lines or three Call Appearance lines is the same. On the standard Agent Display, if an agent is on a skillset call their “In Contacts Status” is “Active”, if on a personal call it is “Busy”. If an agent is on an outgoing personal call the status in real time reporting of DN Out is “Active”. If the agent is on more than

one outgoing call the status remains “Active”. The DN Out Num” field stores the last dialed outgoing number.

If an agent is on an incoming personal call the status in real time reporting of “DN In” is “Active”. If the agent is on more than one incoming call the status remains “Active”. “Time in State” is not reset on the occurrence of a subsequent incoming or outgoing call. The timer is started on arrival of the first call and continues until all calls are ended.

High Availability

Contact Center supports High Availability when agents are using two Call Appearance lines or three Call Appearance lines. The agent experience during and after a switchover is the same for agent stations with two or three Call Appearance lines.

Enabling the third call appearance button

To use the third call appearance button functionality with Agent Desktop, you must perform the following:

- Using the Contact Center Server Configuration utility, enable “Third Line Enabled”. You must enable Third Line Appearance functionality in Contact Center, before configuring it on the Communication Manager.
- Configure Communication Manager to support Third Line Appearance functionality.
- Configure the Communication Manager stations used by Contact Center and Avaya Agent Desktop. After Contact Center and Communication Manager are configured to support three call appearance buttons, you can then configure the Communication Manager stations to support three call appearance buttons.
- Contact Center and Agent Desktop provide restricted support for solutions where some agent stations have two call appearance buttons and some agent stations have three call appearance buttons. This allows you to migrate your contact center solution from two call appearance buttons to three call appearance buttons. The following restrictions apply to Agent Desktop agents with two lines in mixed two line and three line solutions:
  - When an agent is on two calls, the agent cannot originate a new call because they do not have a third line.
  - When an agent is busy on two calls (for example, one inbound and one unrelated outbound call), the agent cannot initiate a transfer or a conference because they do not have a third line.

  If you are migrating from a two line solution to a three line solution, Avaya recommends that you expedite the migration to achieve a more consistent agent experience.

For more information about configuring the third call appearance button, see Communication Manager configuration on page 29.

Redirection considerations

How your contact center handles redirected calls depends on your solution and the available routing options. For more information about call redirection, see *Call Redirection with AACC Application Note*, available at http://support.avaya.com.

Avaya Aura® Unified Communications platform configuration

The basic procedure to configure the Avaya Aura® Unified Communications platform to work with Avaya Aura® Contact Center is as follows:

- Identify which calls to the Avaya Aura® Unified Communications platform are contact center calls to be handled by Contact Center. The Contact Center suite of applications then provides call treatments, skill-based routing, and reporting for these calls.
- Identify which Avaya Aura® Unified Communications phones are to become agent phones (controlled by Contact Center) and associated with Agent Desktop clients.
- Configure Avaya Aura® System Manager to enable Avaya Aura® Session Manager to forward calls, based on a dial pattern, to Contact Center.
  - Add Contact Center as a SIP Entity on the Avaya Aura® Session Manager. Add Contact Center as a SIP Entity on System Manager for Session Manager.
  - Add a dial pattern which resolves to Contact Center.
- Configure the Avaya Aura® Application Enablement Services (AES) to support CSTA (TR/87 over SIP) call control by the Contact Center using a certified Transport Layer Security (TLS) communication channel.
  - Enable the TR87 port.
  - Apply TLS certification
  - Add Contact Center as a trusted host.

Contact Center must then be configured to accept, control, and treat calls originating from the Avaya Aura® Unified Communications platform.

- Detail the voice and CTI proxy addresses and ports.
- Apply TLS certification
- Add the route point.

For more information about configuring Contact Center to accept incoming contacts from the Avaya Aura® Unified Communications platform, and to control phones, see *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications*.

Choosing a fallback option

Before implementing a fallback strategy you must first consider how voice contacts enter your Avaya Aura® Unified Communications solution and how these calls are routed to Avaya Aura® Contact Center. Individual enterprise solutions often use a combination of methods. Depending on the methods used, you can choose a fallback strategy suitable for your solution.

Customer calls typically enter an enterprise solution using the following methods:

- PSTN and traditional ISDN channels.
- PSTN and SIP networks through Session Border Controllers (SBCs).

If a customer dials a Vector Directory Number, the customer voice call can first be routed to Avaya Aura® Communication Manager and then through Avaya Aura® Session Manager to Avaya Aura® Contact Center. If the customer dials a Controlled Directory Number (CDN), the customer voice call can be routed directly through Avaya Aura® Session Manager to Avaya Aura® Contact Center.

For each inbound option the following routing options are supported:

Incoming voice contacts using PSTN and ISDN Gateways:

- Using the Avaya Aura® Communication Manager telephony dial plan, contacts are routed through Session Manager using SIP trunks to Avaya Aura® Contact Center.
- Using an Avaya Aura® Communication Manager dial plan, contacts are routed to a Communication Manager Vector Directory Number (VDN) and Vector “route-to” steps which perform the following:
  - The first option is to route to Avaya Aura® Session Manager using a SIP trunk to Avaya Aura® Contact Center.
  - If the first option fails, then fallback to either a hunt group, split, or skill (optional).

Incoming Voice contacts using SBC and SIP Gateways:

- Using Avaya Aura® Session Manager routing, contacts are routed to Avaya Aura® Contact Center using SIP trunks.
- Using Avaya Aura® Session Manager routing, contacts are routed to Avaya Aura® Communication Manager VDNs and Vector “route to” steps which performs the following:
  - The first option is to route back to Avaya Aura® Session Manager using SIP trunks and onwards to Avaya Aura® Contact Center.
  - If the first option fails, then vector fallback to either hunt group, split, or skill (optional).

Note:

Avaya Aura® Contact Center does not support using Avaya Communication Server 1000 as a SIP gateway.

If you are not implementing a High Availability solution, for both call entrance methods, Avaya recommends that you consider the possible failure points in your solution and how to protect against them. For an Avaya Aura® Contact Center solution all inbound voice contacts are routed through an Avaya Aura® Session Manager. In all non High Availability solutions, the single points of failure are therefore Avaya Aura® Session Manager and Avaya Aura® Contact Center. You must consider these possible failure points when choosing a fallback solution on Avaya Aura® Communication Manager.

For each possible failure point, the following methods can be deployed:

- In a solution with a single Avaya Aura® Session Manager deployment:
  - Use the vector fallback to a skill method. This method requires Avaya Aura® Call Center Elite licensing. After a fallback, Avaya Aura® Contact Center agents log on to an Avaya Aura® Call Center Elite fallback skill to handle routed voice contacts during the outage. For more information about this fallback option, see Fallback to Avaya Aura Call Center Elite skill configuration on page 163.
- In a solution with a single Avaya Aura® Contact Center deployment:
  - Use the Avaya Aura® Session Manager fallback to hunt group method. This method does not use Vector Variables or Elite. Avaya Aura® Contact Center agent stations are configured in a Communication Manager hunt group and voice contacts are handled by this hunt group in fallback mode. For more information about this fallback option, see Fallback to Avaya Aura Communication Manager Hunt Group configuration on page 128.
  - Use the vector fallback to a skill method. This requires Avaya Aura® Call Center Elite licensing. After a fallback, Avaya Aura® Contact Center agents log on to an Avaya Aura® Call Center Elite fallback skill to handle routed voice contacts during the outage. For more information about this fallback option, see Fallback to Avaya Aura Call Center Elite skill configuration on page 163.

These fallback methods are very similar and can be used in a variety of failure scenarios to provide a more resilient solution. Avaya recommends these methods in an Avaya Aura® Contact Center solution where High Availability is not deployed. If you are implementing a High Availability solution, these fallback methods are optional.

Contact Center agent desk phone supported features

This section specifies which desk phone feature buttons are supported on an Avaya Aura® Contact Center agent's desk phone. Avaya Aura® Communication Manager desk phones have programmable buttons. You can create feature buttons by assigning features or functionality to these programmable buttons.

Important:

If there are Contact Center agents using SIP desk phones, you must ensure that the SIP Network Transport communication protocol being used between Avaya Aura® Contact Center and Avaya Aura® Session Manager is TLS.

In solutions that support Avaya Aura® Contact Center fallback to Avaya Aura® Call Center Elite, agents use their desk phones to log on to either Contact Center or Elite.

Example: During normal operation support agents log on to Avaya Aura® Contact Center and handle customer calls routed to a Contact Center skillset. If Avaya Aura® Contact Center is offline or stopped for maintenance, the support agents can log on to an Elite support skill. During the Contact Center outage, customer calls intended for the Contact Center support skillset are rerouted to the Elite support skill, where the calls are answered by agents with support

experience. When Contact Center starts back up, the support agents must log out from Elite and log back on to Contact Center.

Note:

In solutions that support Contact Center fallback to Elite, agents log in to either Avaya Aura® Call Center Elite or Avaya Aura® Contact Center. During normal operation, Agents log in to Contact Center. During fallback operation, agents log in to an Elite skill. Agents are not permitted to log in to both Avaya Aura® Call Center Elite and Avaya Aura® Contact Center at the same time. Avaya recommends using remote/force logout to ensure agents are logged out from Elite before returning to Contact Center.

The feature buttons on the agent desk phones must be supported by Avaya Aura® Call Center Elite. Avaya Aura® Contact Center and Avaya Agent Desktop do not support these feature buttons, but the existence of these feature buttons on agent phones does not adversely impact call control or agent functionality during normal Contact Center operation.

When agents log on to an Elite skill, they can use the Communication Manager and Elite feature buttons as intended. When the agents log on to Contact Center, the following feature buttons have no adverse impact on contact center agent functionality or call control.

Avaya Aura® Call Center Elite feature buttons

Feature	Button Name or Label	Impact on Contact Center	Comment
Login / Logout	Feature Access Code and Agent ID and operation mode.	Logging on to Contact Center and Elite at the same time is not supported.	Permitted to configure login / logout on the phone-set to support fallback scenarios only. Supported, but only in fallback to Elite scenarios.
Select Operation Modes	manual-in / Manual In	None	No impact on Contact Center functionality, therefore supported on agent phones.
	auto-in / Auto in	None	No impact on Contact Center functionality, therefore supported on agent phones.
Change Agent State	aux-work / AuxWork	None	No impact on Contact Center functionality, therefore supported on agent phones.
	after-call / AfterCall	None	No impact on Contact Center functionality, therefore supported on agent phones.
Ability to render on phone-set display ASAI UUI associated with call	uui-info / UUI-Info	None	No impact on Contact Center functionality, therefore supported on agent phones.

Table continues…

Feature	Button Name or Label	Impact on Contact Center	Comment
Call Work Codes	work-code / Work Code	None	No impact on Contact Center functionality, therefore supported on agent phones.
VuStats	vu-display / VU Display	None	No impact on Contact Center functionality, therefore supported on agent phones.
Stroke Counts	stroke-cnt / Stroke Count	None	No impact on Contact Center functionality, therefore supported on agent phones.
Change Agent Skills (from phone-set)	alrt-agchg / Alert Agent	None	Button is configured on the agent set to notify the agent of the skill change. Supervisor uses FAC's to update the agents skillsets. No impact on Contact Center functionality, therefore supported on agent phones.
Forced Agent Logout	Configured using Feature Access Code.	None	Logout based on time in After Call Work (ACW) mode. No Impact on Contact Center functionality, therefore supported on agent phones.
Forced Agent Logout by Clock Time	Configured using Feature Access Code.	None	Logout based on specified time on Communication Manager. No impact on Contact Center functionality, therefore supported on agent phones.
Remote Logout of Agents	Feature Access Code and Agent ID.	None	Allows a Supervisor to logout an agent from any desk phone. No impact on Contact Center functionality, therefore supported on agent phones.

Avaya Aura® Communication Manager feature buttons

Feature	Button Name or Label	Impact on Contact Center	Comment
Autodial	SD	None	Must have an available line before using this button. Need to place any active calls on hold.

Table continues…

Feature	Button Name or Label	Impact on Contact Center	Comment
Direct Agent Calling (DAC)	Communication Manager feature – no extra keys configured.	None	Ability to call an agent directly by Agent ID. No impact on Contact Center functionality, therefore supported on agent phones.
MWI tracking for agent ID	Communication Manager feature setting – No extra keys configured.	None	No impact on Contact Center functionality, therefore supported on agent phones.

The supported feature buttons are supported only on the Avaya Aura® Contact Center agent desk phones used for Elite fallback support.

Caution:

Avaya Aura® Contact Center does not support any other feature buttons on agent desk phones.

Avaya Aura® Contact Center does not support buttons that can take CTI control.

The following feature buttons impact Avaya Aura® Contact Center and are therefore not supported on Contact Center agent desk phones.

Communication Manager feature buttons not compatible with Avaya Aura® Contact Center

Feature	Button Name or Label	Impact on Contact Center
Supervisor Assist	assist / Assist	Not supported
Supervisor Observe	serv-obsrv / Service Obsrv	Not supported
Supervisor Barge In	N/A	Not supported
Supervisor Whisper	whisp-act / WhisperAct	Not supported
	whisp-anbk / WhisperAnbk	Not supported
	whisp-off / WhisperOff	Not supported
Call Pickup	call-pkup / Call Pickup	Not supported
EC500	EC500	Not supported
Send All Calls	send-calls	Not supported
Call Forwarding	call-fwd	Not supported

High Availability Avaya Aura® Media Server

High Availability Avaya Aura® Media Server and G430/G450 configuration

If your G430 or G450 Media Gateway is installed on the same network subnet as your High Availability Linux-based Avaya Aura® Media Server cluster, then you must disable ARP Inspection

on the G430/G450. If an Avaya Aura® Media Server fails, the G430/G450 can then communicate with the other Avaya Aura® Media Server in that cluster.

On the G430 or G450, disable ARP spoofing protection by entering the CLI command: “no ip arp inspection”.

High Availability Avaya Aura® Media Server and G6xx configuration

In Avaya Aura® Contact Center High Availability solutions that contain High Availability Linux-based Avaya Aura® Media Servers and a G6xx Media Gateway, the Avaya Aura® Media Servers must be installed in a different network subnet to the G6xx Media Gateway.

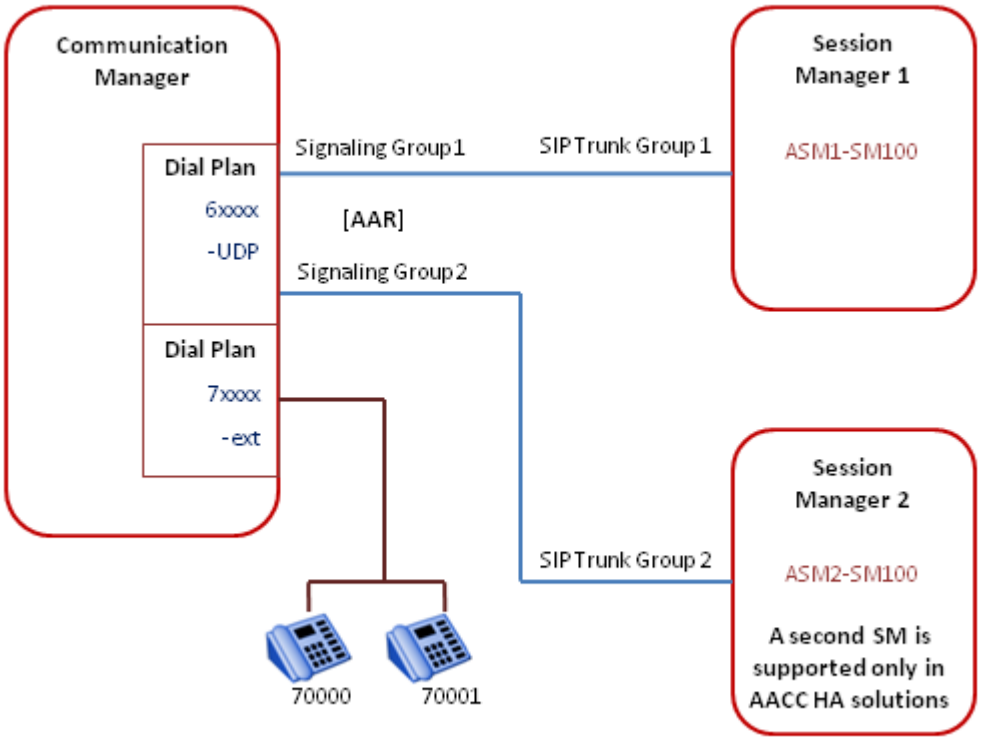
Chapter 4: Communication Manager configuration

This section describes how to configure Avaya Aura® Communication Manager for integration with Avaya Aura® Contact Center. Avaya Aura® Communication Manager delivers centralized call control for resilient and distributed networks. Communication Manager supports a wide range of servers, gateways, analog, digital, and IP-based communication devices.

The Avaya Aura® Contact Center Mission Critical High Availability feature requires two Avaya Aura® Session Managers in your solution.

The following diagram shows a typical Communication Manager deployment and configuration.

Figure 1: Example Communication Manager configuration

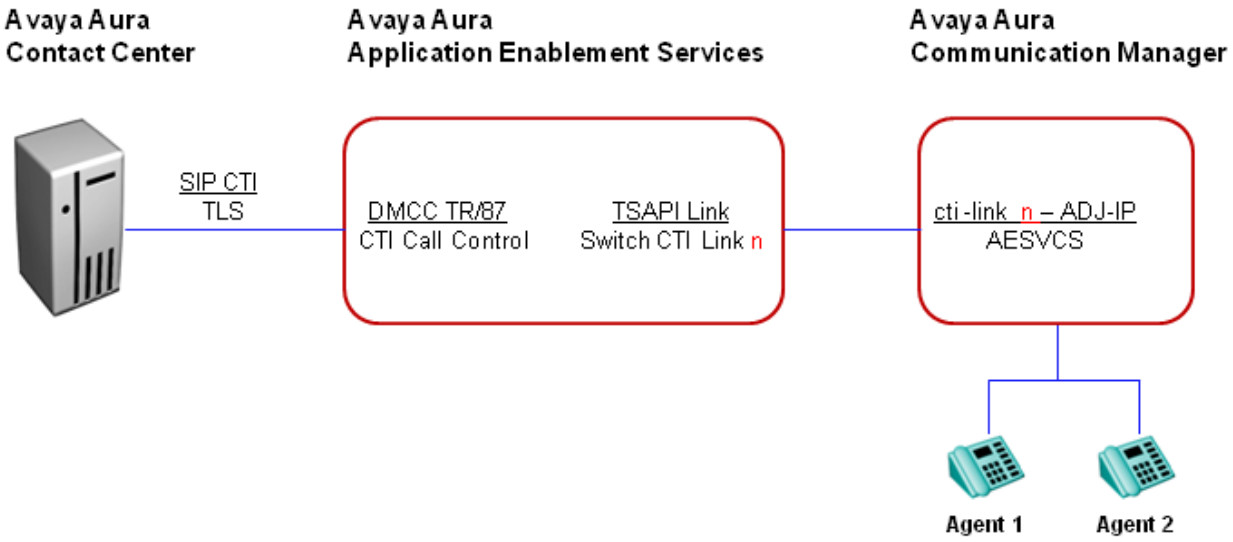


In addition to station configuration, the Communication Manager must be configured to route calls to and from Avaya Aura® Contact Center through SIP using one or more Avaya Aura® Session Managers.

Avaya Aura® Contact Center uses Avaya Aura® Application Enablement Services to monitor and control Communication Manager agent stations (phones).

Avaya Aura® Application Enablement Services (AES) provide a set of enhanced telephony APIs, protocols, and Web services. The Avaya Device, Media, and Call Control (DMCC) APIs provided by Application Enablement Services enable Avaya Aura® Contact Center to monitor and control Communication Manager phones.

Figure 2: Example Communication Manager call control



On the Communication Manager, configure IP services for Application Enablement Services (AESVCS) and then configure a cti-link of type ADJ-IP. The ADJ-IP link type is for Adjunct Switch Application Interface (ASAI) links administered by Avaya CTI applications, such as Application Enablement Services.

On the Application Enablement Services server, configure a secure TLS link with Avaya Aura® Contact Center. Enable DMCC TR/87 CTI call control, and add a TSAPI CTI link to the Communication Manager. The Application Enablement Services - TSAPI Switch CTI Link number must match the Communication Manager cti-link number.

Communication Manager System Access Terminal (SAT) navigation:

You configure Avaya Aura® Communication Manager using the System Access Terminal (SAT) interface.

Use the keyboard arrow keys to move around screen (when using a w2ktt Terminal Emulator).

- To save information, press Esc followed by e.
- To cancel, press Esc followed by x.
- To move onto next page, press Esc followed by n.
- To go to previous page, press Esc followed by p.
- To erase information, use the spacebar.
- To get help, press Esc followed by h, or type ‘help’.

Communication Manager configuration procedures

About this task

This task flow shows you the sequence of procedures you perform to configure Communication Manager.

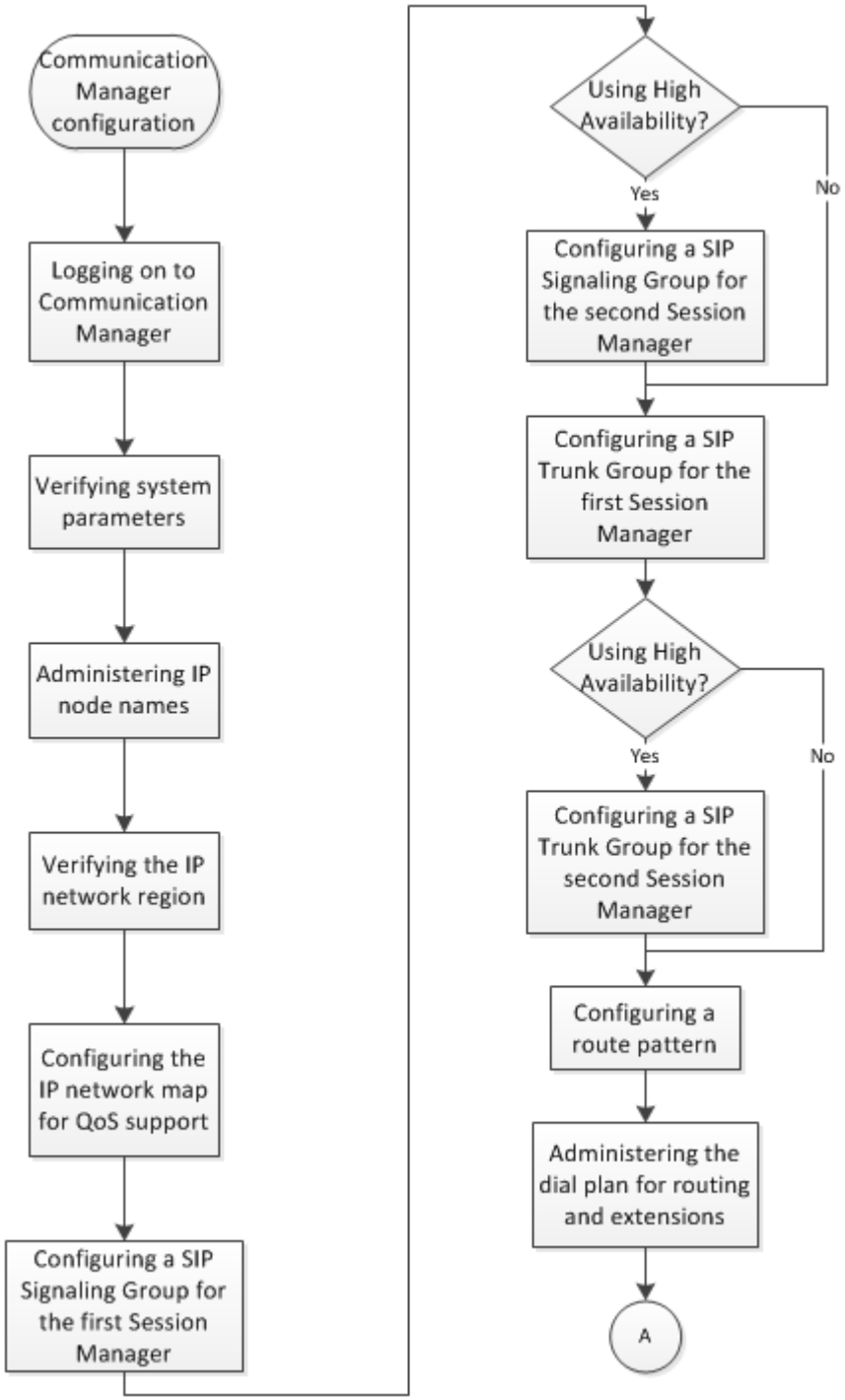


Figure 3: Communication Manager configuration procedures

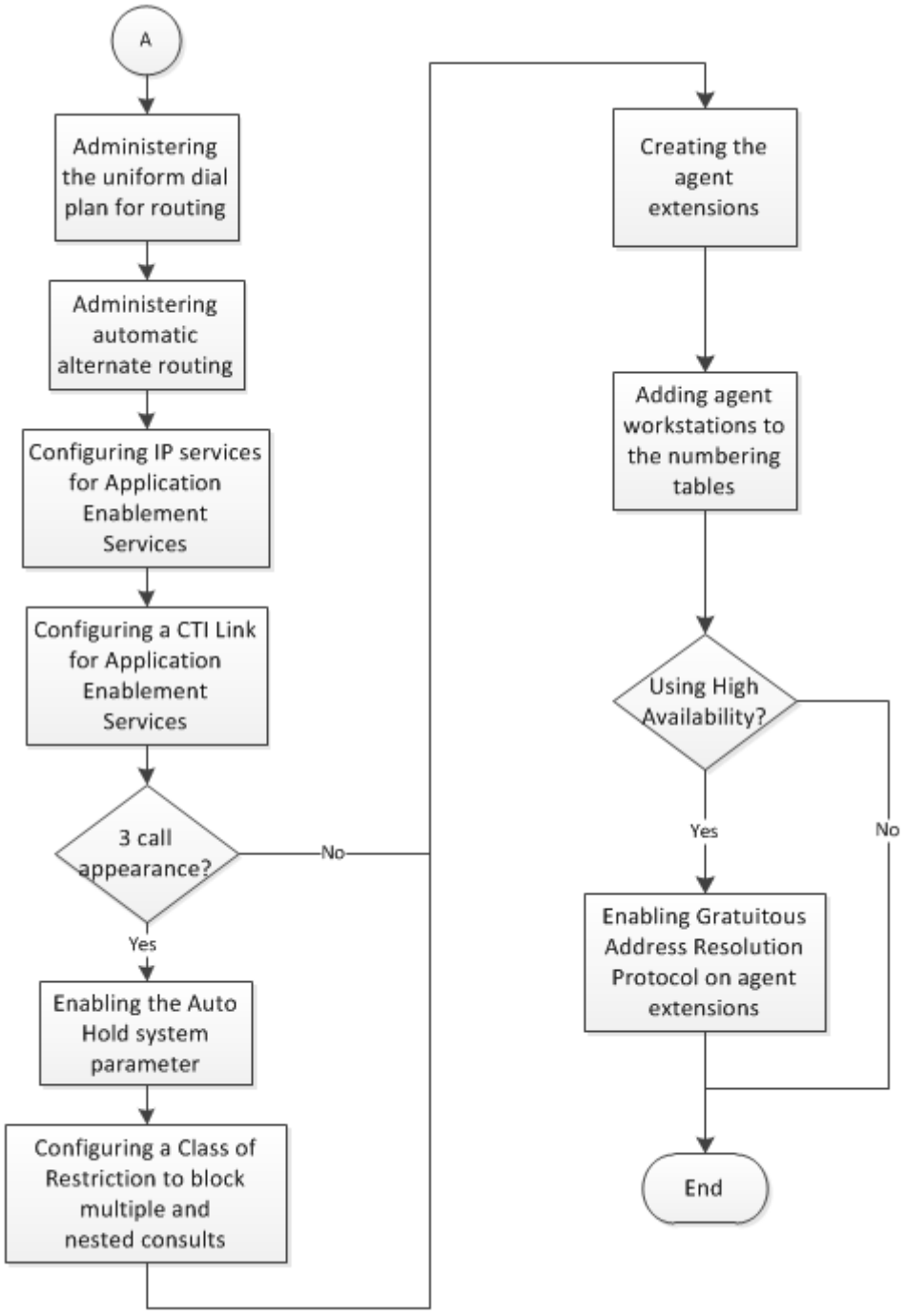


Figure 4: Communication Manager configuration procedures continued

Logging on to Communication Manager

About this task

Log on to Avaya Aura® Communication Manager to configure parameters and resources for integration with Avaya Aura® Contact Center.

Procedure

1. Using an SSH client such as PuTTY, begin an SSH session using the Communication Manager IP address.
2. Click **Open**.
3. When prompted enter the user name and password for the Communication Manager.
4. Press return to ignore terminal selection and when prompted for high priority session, enter `n`.
5. To access the System Access Terminal (SAT), type `sat` and enter the same password used above.
6. When prompted, enter a preferred terminal type. For example, select the w2ktt Terminal Emulator.

Verifying system parameters

About this task

On the Communication Manager System Parameters Features form, verify that Universal Call Identifier (UCID) is enabled. Universal Call Identifier is an Avaya proprietary call identifier used to help correlate call records between different systems. Universal Call Identifier must also be configured on the Trunk Group to Avaya Aura® Session Manager. For more information, see Configuring a SIP Trunk Group for the first Session Manager on page 43.

You must also ensure that SIP Endpoint Managed Transfer is disabled, as it is not supported.

Procedure

1. Verify that Universal Call Identifier is enabled and that the Network Node is a unique node identity. Use the **`display system-parameters features`** command.

```
display system-parameters features                              Page   5 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                     Switch Name:
           Emergency Extension Forwarding (min): 10
         Enable Inter-Gateway Alternate Routing? n
Enable Dial Plan Transparency in Survivable Mode? n
                            COR to Use for DPT: station

MALICIOUS CALL TRACE PARAMETERS
               Apply MCT Warning Tone? n   MCT Voice Recorder Trunk Group:
      Delay Sending RELease (seconds): 0
SEND ALL CALLS OPTIONS
     Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
              Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? y    UCID Network Node ID: 21
```

2. Verify that the Universal Call Identifier is forwarded to the Adjunct Switch Applications Interface (ASAI). Use the **`display system-parameters features`** command.

```
display system-parameters features                              Page  13 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
           Callr-info Display Timer (sec): 10
                       Clear Callr-info: next-call
        Allow Ringer-off with Auto-Answer? n

    Reporting for PC Non-Predictive Calls? n

           Agent/Caller Disconnect Tones? n

            Zip Tone Burst for Callmaster Endpoints: double

  ASAI
           Copy ASAI UUI During Conference/Transfer? n
      Call Classification After Answer Supervision? n
                                 Send UCID to ASAI? y
        For ASAI Send DTMF Tone to Call Originator? y
```

3. Verify that SIP Endpoint Managed Transfer is disabled. Use the **`display system-parameters features`** command.

```
display system-parameters features                          Page  19 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
IP PARAMETERS
                    Direct IP-IP Audio Connections? n
                              IP Audio Hairpinning? n
                            Synchronization over IP? n

                    SIP Endpoint Managed Transfer? n

CALL PICKUP
  Maximum Number of Digits for Directed Group Call Pickup: 2
                   Call Pickup on Intercom Calls? y     Call Pickup Alerting? n
      Temporary Bridged Appearance on Call Pickup? y     Directed Call Pickup? n
                      Extended Group Call Pickup: none
                   Enhanced Call Pickup Alerting? n


                        Display Information With Bridged Call? n
  Keep Bridged Information on Multiline Displays During Calls? n
                  PIN Checking for Private Calls? n
```

4. Verify that Direct IP-IP Audio Connections is disabled. Use the **`display system-parameters features`** command.

```
display system-parameters features                          Page  19 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
IP PARAMETERS
                    Direct IP-IP Audio Connections? n
                              IP Audio Hairpinning? n
                            Synchronization over IP? n

                    SIP Endpoint Managed Transfer? n

CALL PICKUP
  Maximum Number of Digits for Directed Group Call Pickup: 2
                   Call Pickup on Intercom Calls? y     Call Pickup Alerting? n
      Temporary Bridged Appearance on Call Pickup? y     Directed Call Pickup? n
                      Extended Group Call Pickup: none
                   Enhanced Call Pickup Alerting? n


                        Display Information With Bridged Call? n
  Keep Bridged Information on Multiline Displays During Calls? n
                  PIN Checking for Private Calls? n
```

Administering IP node names

About this task

The nodes defined in the Avaya Aura® Communication Manager IP Node Names form are used in other configuration screens to define the SIP signaling groups between Communication Manager and the Avaya Aura® Session Managers.

The Avaya Aura® Contact Center Mission Critical High Availability feature requires two Avaya Aura® Session Managers. Use the IP Node Names form to assign a node name and IP address for the two Avaya Aura® Session Managers.

Procedure

1. Use the System Access Terminal (SAT) interface to enter the node name and IP address for the first Avaya Aura® Session Manager. Use the **`change node-names ip`** command.
2. If your solution uses the Avaya Aura® Contact Center Mission Critical High Availability feature, enter the node name and IP address for the second Avaya Aura® Session Manager. Use the **`change node-names ip`** command.

Example

The following example of a Communication Manager IP Node Names display shows two Session Managers: ASM1-SM100 and ASM2-SM100.

```
display node-names ip
                                    IP NODE NAMES
    Name                  IP Address
ASM1-SM100              172.18.71.17
ASM2-SM100              172.18.71.18
ATFAES2                 172.18.70.243
ATFAES3                 172.18.70.246
ATFAES4                 172.18.70.249
ATFaes                  172.18.70.238
HCAP6AES                172.18.71.23
HCAPDC2AES              172.18.38.10
HCAPDC2CMSP             172.18.38.3
HCAPDC2SM100            172.18.38.7
default                 0.0.0.0
procr                   172.18.71.15
procr6                  ::



( 13 of 13   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

Note the procr name, as this is the Avaya Aura® Communication Manager processor interface. The Communication Manager processor (procr) IP address is 172.18.71.15.

In other Avaya configurations such as an Avaya G650 Media Gateway, the C-LAN interface address must be used as the SIP signaling interface to Session Manager, rather than the processor address (node name procr).

Note the Avaya Aura® Application Enablement Services node name and IP address from the image above is 172.18.71.23.

Verifying the IP network region

About this task

On the Communication Manager IP Network Region form, verify that the Authoritative Domain name matches the contact center SIP domain name.

Procedure

1. Use the System Access Terminal (SAT) interface to verify that the authoritative domain names matches the contact center SIP domain name. Use the **`display ip-network-region`** command.
2. If you require Quality of Service (QoS) support for Avaya Agent Desktop, ensure the DIFFSERV/TOS parameters are configured.

Example

The following example of a Communication Manager IP Network Region form, shows authoritative domain configured as siptraffic.com.

Note:

Ensure the DIFFSERV/TOS parameters are configured, if you require Quality of Service (QoS) support for Agent Desktop.

```
display ip-network-region 1                                   Page   1 of  20
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: siptraffic.com
    Name:
MEDIA PARAMETERS                 Intra-region IP-IP Direct Audio: yes
      Codec Set: 1               Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Configuring the IP network map for QoS support

About this task

Avaya Agent Desktop supports Quality of Service (QoS). This allows for the prioritization of voice traffic over data traffic by tagging voice packets with priority tags. You must configure the ip-network-map for your endpoints to support QoS.

Procedure

Use the System Access Terminal (SAT) interface to configure the ip-network-map for your endpoints. Use the **`change ip-network-map`** command.

Example

The following example of a Communication Manager IP Network Map form, shows an IP address range from 172.18.71.1 to 172.18.71.254. This is the IP address range for the Agent Desktop client computers. This IP address range maps to Network Region 1 and has been assigned to a VLAN ID.

```
change ip-network-map                                          Page   1 of  63
                                IP ADDRESS MAPPING

                                                    Subnet Network     Emergency
IP Address                                          Bits   Region VLAN Location Ext
------------------------------------------------- ------ ------ ---- -------------
FROM: 172.18.71.1                                 /___   1      0    _____________
  TO: 172.18.71.254
FROM:                                             /___   ___    n    _____________
  TO:
FROM:                                             /___   ___    n    _____________
  TO:
FROM:                                             /___   ___    n    _____________
  TO:
FROM:                                             /___   ___    n    _____________
  TO:
FROM:                                             /___   ___    n    _____________
  TO:
FROM:                                             /___   ___    n    _____________
  TO:
FROM:                                             /___   ___    n    _____________
  TO:
```

Configuring a SIP Signaling Group for the first Session Manager

About this task

On the Avaya Aura® Communication Manager, configure a Signaling Group for communication between Communication Manager and the first Avaya Aura® Session Manager.

Avaya Aura® Communication Manager uses a SIP Signaling Group and an associated SIP Trunk Group to route calls to an Avaya Aura® Session Manager.

Important:

If you use SIPS on Communication Manager signaling groups, you must configure SIPS as the default option on the SIP clients, which you use for media on the extension controlled by Avaya Aura® Contact Center. Ensure that the whole call flow is SIPS-enabled.

Procedure

1. Use the System Access Terminal (SAT) interface to add a signaling group for the first Session Manager. Use the **`add signaling-group <s1>`** command, where *s1* is an un-allocated signaling group.
2. You must disable the IP Multimedia Subsystem (IMS) on the Communication Manager Signaling Group. Ensure that your signaling group has the **IMS Enabled?** value set to `n`.

Example

The Communication Manager SIP Signaling Group for the first Avaya Aura® Session Manager, SIP Signaling Group number 1.

```
display signaling-group 1
                               SIGNALING GROUP

 Group Number: 1                Group Type: sip
  IMS Enabled? n          Transport Method: tls
       Q-SIP? n                                              SIP Enabled LSP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM


   Near-end Node Name: procr                  Far-end Node Name: ASM1-SM100
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                          Far-end Network Region: 2
                                       Far-end Secondary Node Name:
Far-end Domain: siptraffic.com
                                                  Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                       RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload                 Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                          IP Audio Hairpinning? n
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 2
```

Variable definitions

Variable	Value
Group Number	The number of the signaling group.
Group Type	The type of protocol used for this signaling group. For example, enter "sip".
Transport Method	Transport can be accomplished using either TCP or TLS. TLS is set by default.
Near-end Node Name	The node name of the near-end CLAN IP interface used for trunks that use this signaling group which must be already administered.
Far-end Node Name	The node name of the far-end CLAN IP interface used for trunks that use this signaling group which must be already administered. Use the Session Manager node name.
Far-end Domain	The name of the IP domain that is assigned to the far-end of the signaling group.

Configuring a SIP Signaling Group for the second Session Manager

About this task

On the Avaya Aura® Communication Manager, configure a Signaling Group for communication between Communication Manager and the second Avaya Aura® Session Manager.

Avaya Aura® Communication Manager uses a SIP Signaling Group and an associated SIP Trunk Group to route calls to an Avaya Aura® Session Manager.

Note:

A second Session Manager is supported only in an Avaya Aura® Contact Center Mission Critical High Availability solution.

Procedure

1. Use the System Access Terminal (SAT) interface to add a signaling group for the second Session Manager. Use the **`add signaling-group <s2>`** command, where *s2* is an un-allocated signaling group.
2. You must disable the IP Multimedia Subsystem (IMS) on the Communication Manager Signaling Group. Ensure that your signaling group has the **IMS Enabled?** value set to `n`.

Example

The Communication Manager SIP Signaling Group for the second Avaya Aura® Session Manager, SIP Signaling Group number 2.

```
display signaling-group 2
                                SIGNALING GROUP

 Group Number: 2                Group Type: sip
  IMS Enabled? n          Transport Method: tls
       Q-SIP? n                                          SIP Enabled LSP? n
    IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: ASM2-SM100
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 2
                                  Far-end Secondary Node Name:
Far-end Domain: siptraffic.com
                                              Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                 RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? y                 Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 2
```

Variable definitions

Variable	Value
Group Number	The number of the signaling group.
Group Type	The type of protocol used for this signaling group. For example, enter "sip".
Transport Method	Transport can be accomplished using either TCP or TLS. TLS is set by default.
Near-end Node Name	The node name of the near-end CLAN IP interface used for trunks that use this signaling group which must be already administered.
Far-end Node Name	The node name of the far-end CLAN IP interface used for trunks that use this signaling group which must be already administered. Use the Session Manager node name.
Far-end Domain	The name of the IP domain that is assigned to the far-end of the signaling group.

Configuring a SIP Trunk Group for the first Session Manager

About this task

On the Avaya Aura® Communication Manager, configure a SIP Trunk Group for communication between Communication Manager and the first Avaya Aura® Session Manager. Configure one SIP Trunk Group for each SIP Signaling Group associated with a Session Manager.

Avaya Aura® Communication Manager uses a SIP Signaling Group and an associated SIP Trunk Group to route calls to an Avaya Aura® Session Manager.

You must disable Network Call Redirection (NCR) on the SIP Trunk Group. If you disabled NCR at the system level, that setting applies to new trunk groups: you do not see the Network Call Redirection prompt on the Trunk Group form. There is one limitation to disabling NCR; for the following CDN conference scenarios, if one party goes on hold then Communication Manager streams music-on-hold into the 3-party conference (where Communication Manager has music-on-hold configured):

- CDN to CDN conference/join
- CDN call with supervisor Barge-In
- CDN call with agent Emergency

Procedure

1. Use the System Access Terminal (SAT) interface to add a SIP Trunk Group for the first Session Manager. Use the **`add trunk-group <t1>`** command, where *t1* is an un-allocated trunk group.

```
display trunk-group 1                                        Page   1 of  22
                              TRUNK GROUP

Group Number: 1                   Group Type: sip            CDR Reports: y
  Group Name: to ASM1                     COR: 1        TN: 1        TAC: #01
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                             Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 255
```

2. To support Universal Call Identifier (UCID), set **UUI Treatment** to shared, and then enable **Send UCID**.

```
display trunk-group 1                                          Page   3 of  22
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y


                    Numbering Format: private
                                                  UUI Treatment: shared
                                               Maximum Size of UUI Contents: 128
                                                  Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                    Modify Tandem Calling Number: no
                Send UCID? y


 Show ANSWERED BY on Display? y

 DSN Term? n
```

3. On the Trunk Group form of the Communication Manager to Session Manager SIP trunk, disable Network Call Redirection.

```
display trunk-group 1                                          Page   4 of  22
                              PROTOCOL VARIATIONS

                        Mark Users as Phone? n
              Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? n
                    Send Diversion Header? n
                  Support Request History? y
             Telephone Event Payload Type:


       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
       Identity for Calling Party Display: P-Asserted-Identity
                              Enable Q-SIP? n
```

Variable definitions

Variable	Value
Group Number	The number of the trunk group.
Group Type	The type of protocol used for this trunk group. For example, enter `sip`.
Group Name	A unique name that provides information about this trunk group. The name contains a maximum of 27 characters.
TAC	The TAC (Trunk Access Code) is the number that must be dialed to access the trunk group. A different TAC must be assigned to each trunk group. The characters asterisk (*) and number (#) can be used as the first character in a TAC and it accepts a one- to four-digit number.
Direction	The direction of traffic on this trunk group. Traffic on this trunk group is incoming and outgoing (two-way).
Service Type	The service for which the trunk group is dedicated.
Signaling Group	The signaling group to be used in accordance with this trunk group for communication between Communication Manager and the first Session Manager.

Configuring a SIP Trunk Group for the second Session Manager

About this task

On the Avaya Aura® Communication Manager, configure a SIP Trunk Group for communication between Communication Manager and the second Avaya Aura® Session Manager. Configure one SIP Trunk Group for each SIP Signaling Group associated with a Session Manager.

Avaya Aura® Communication Manager uses a SIP Signaling Group and an associated SIP Trunk Group to route calls to an Avaya Aura® Session Manager.

Note:

A second Session Manager is supported only in an Avaya Aura® Contact Center Mission Critical High Availability solution.

You must disable Network Call Redirection (NCR) on the SIP Trunk Group. If you disabled NCR at the system level, that setting applies to new trunk groups : you do not see the Network Call Redirection prompt on the Trunk Group form. There is one limitation to disabling NCR; for the

following CDN conference scenarios, if one party goes on hold then Communication Manager streams music-on-hold into the 3-party conference (where Communication Manager has music-on-hold configured):

- CDN to CDN conference/join
- CDN call with supervisor Barge-In
- CDN call with agent Emergency

Procedure

1. Use the System Access Terminal (SAT) interface to add a SIP Trunk Group for the second Session Manager. Use the **`add trunk-group <t2>`** command, where *t2* is an un-allocated trunk group.

```
display trunk-group 2                                        Page   1 of  22
                              TRUNK GROUP

Group Number: 2                   Group Type: sip            CDR Reports: y
  Group Name: to ASM2                     COR: 1        TN: 1        TAC: #02
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                             Member Assignment Method: auto
                                                       Signaling Group: 2
                                                     Number of Members: 255
```

2. To support Universal Call Identifier (UCID), set **UUI Treatment** to shared, and then enable **Send UCID**.

```
display trunk-group 2                                          Page   3 of  22
TRUNK FEATURES
          ACA Assignment? n              Measured: none
                                                        Maintenance Tests? y


                     Numbering Format: private
                                          UUI Treatment: shared
                                       Maximum Size of UUI Contents: 128
                                          Replace Restricted Numbers? n
                                        Replace Unavailable Numbers? n


                                  Modify Tandem Calling Number: no
                Send UCID? y


 Show ANSWERED BY on Display? y

 DSN Term? n
```

3. On the Trunk Group form of Communication Manager to the Session Manager SIP trunk, disable Network Call Redirection.

```
display trunk-group 2                                          Page   4 of  22
                              PROTOCOL VARIATIONS

                       Mark Users as Phone? n
             Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? n
                    Send Diversion Header? n
                  Support Request History? y
             Telephone Event Payload Type:


       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
       Identity for Calling Party Display: P-Asserted-Identity
                              Enable Q-SIP? n
```

Variable definitions

Variable	Value
Group Number	The number of the trunk group.
Group Type	The type of protocol used for this trunk group. For example, enter `sip`.
Group Name	A unique name that provides information about this trunk group. The name contains a maximum of 27 characters.
TAC	The TAC (Trunk Access Code) is the number that must be dialed to access the trunk group. A different TAC must be assigned to each trunk group. The characters asterisk (*) and number (#) can be used as the first character in a TAC and it accepts a one- to four-digit number.
Direction	The direction of traffic on this trunk group. Traffic on this trunk group is incoming and outgoing (two-way).
Service Type	The service for which the trunk group is dedicated.
Signaling Group	The signaling group to be used in accordance with this trunk group for communication between Communication Manager and the second Session Manager.

Configuring a route pattern

About this task

On the Avaya Aura® Communication Manager, configure a route pattern for the Avaya Aura® Session Manager SIP trunk groups.

Each Communication Manager route pattern contains a list of trunk groups that can be used to route calls. The maximum number of route patterns and trunk groups allowed depends on the configuration and memory available in your system.

Procedure

Use the System Access Terminal (SAT) interface to add a route pattern, where *n* is an available route pattern. Use the **`change route-pattern n`** command.

Example

This Communication Manager route pattern (number 1) shows the SIP Trunk Groups for the Session Managers, number 1 and number 2. Number 2 is required only for High Availability solutions.

```
display route-pattern 1                                          Page   1 of   3
                   Pattern Number: 1   Pattern Name: ASM
                                SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.   Inserted                              DCS/  IXC
    No          Mrk Lmt List Del   Digits                               QSIG
                                Dgts                                    Intw
 1: 1    0                                                               n    user
 2: 2    0                                                               n    user
 3: 7    0                                                               n    user
 4:                                                                      n    user
 5:                                                                      n    user
 6:                                                                      n    user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                  Dgts Format
                                                          Subaddress
 1: y y y y y n   n            rest                                     next
 2: y y y y y n   n            rest                                     next
 3: y y y y y n   n            rest                                     next
 4: y y y y y n   n            rest                                     none
 5: y y y y y n   n            rest                                     none
 6: y y y y y n   n            rest                                     none
```

Administering the dial plan for routing and extensions

About this task

On the Avaya Aura® Communication Manager, edit the dial plan to add your routing and the agent extensions (workstations).

The dial plan analysis table defines the dialing plan for your system. Communication Manager uses dial plans to define how dialed digits are interpreted, and how many digits to expect for each call.

Procedure

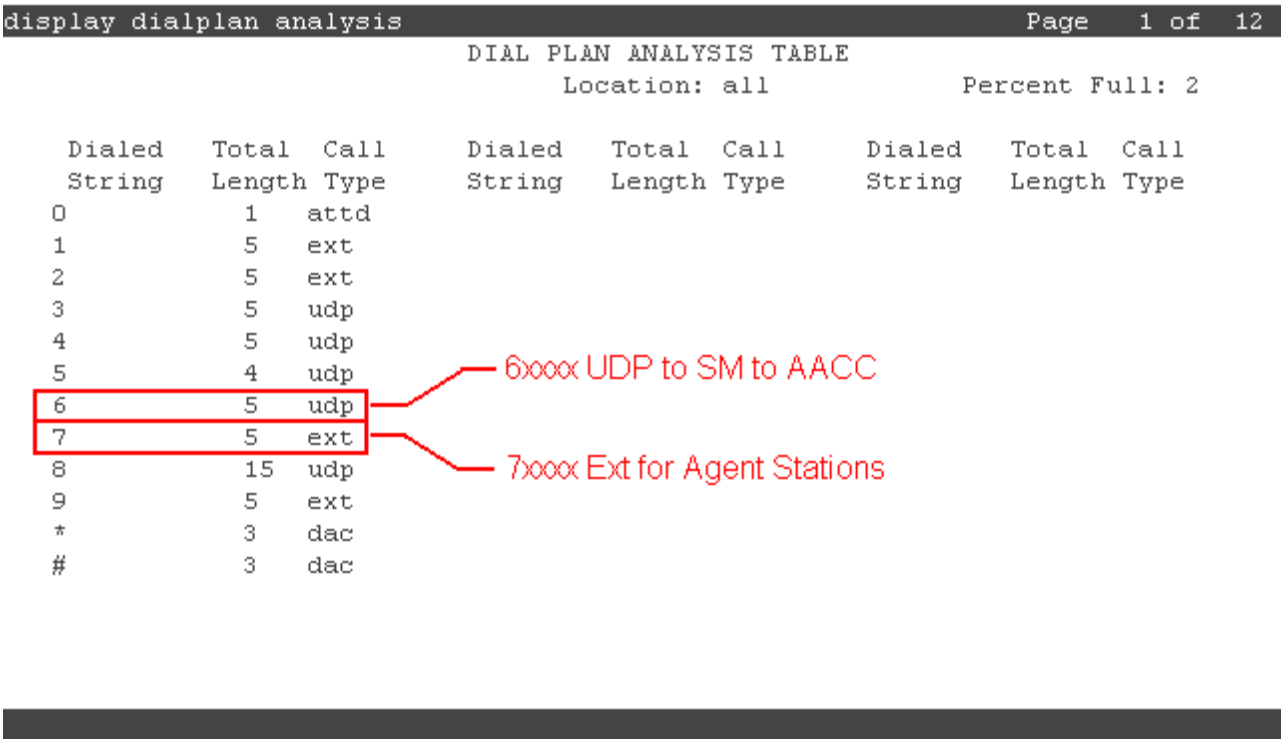
On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to create a dial plan for routing and the agent extensions. Use the **`change dialplan analysis`** command.

Example

This Communication Manager dial plan analysis table shows 5-digit extensions in the 7xxxx range (call type extension) and 5-digit routing in the 6xxxx range (call type uniform dial plan (UDP)).

The Call Type column in the dial plan analysis table indicates what the system does when a user dials the digit or digits indicated in the Dialed String column. The Total Length column indicates how long the dialed string is for each type of call.

For example, this dial plan shows that when users dial a 5-digit number that starts with the digit 7, they are dialing an extension or station.



Administering the uniform dial plan for routing

About this task

On the Avaya Aura® Communication Manager, create a uniform dial plan for routing.

Uniform dial plans (UDPs) are used to share a common dial plan among a group of Communication Manager servers. The UDP provides a common dial plan length, or a combination of extension lengths, that can be shared among a group of media servers or switches. Additionally, UDP can be used singly to provide uniform dialing between two or more private switching systems.

Procedure

Use the System Access Terminal (SAT) interface to update the uniform dial plan for routing. Use the **`change uniform-dialplan n`** command.

Example

The Communication Manager Uniform Dial Plan display shows the 5–digit 6xxxx route to Automatic Alternate Routing (AAR).

```
display uniform-dialplan 1                                    Page   1 of   2
                        UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching                    Insert                  Node
  Pattern        Len Del      Digits      Net Conv Num
3                  5   0                  aar  n
4                  5   0                  aar  n
5                  4   0                  aar  n
6                  5   0                  aar  n
8                  15  0                  aar  n
                                           n
                                           n
                                           n
                                           n
                                           n
                                           n
                                           n
                                           n
                                           n
                                           n
                                           n
```

Administering automatic alternate routing

About this task

On the Avaya Aura® Communication Manager, use automatic alternate routing (AAR) for routing configured calls to Avaya Aura® Contact Center.

Note:

You can use other routing methods.

For example, use AAR to route calls with dialed digits 6xxxx to Contact Center. Use the change dial plan analysis command, and add an entry to specify use of AAR for routing of digits 6xxxx.

AAR allows enterprise network calls to originate and terminate at one or many locations without accessing the public network. It routes calls over the private enterprise network.

Procedure

Use the System Access Terminal (SAT) interface to add an entry to specify the use of AAR for routing of digits 6xxxx. Use the **`change aar analysis n`** command.

Example

This Communication Manager AAR digit analysis table shows the use of AAR for the routing of digits matching 6xxxx to route pattern 1.

```
display aar analysis 1                                        Page   1 of   2
                           AAR DIGIT ANALYSIS TABLE
                                  Location: all            Percent Full: 1

      Dialed             Total      Route     Call    Node   ANI
      String           Min   Max   Pattern    Type    Num    Reqd
  2                    5     5     1          unku           n
  3                    5     5     1          aar            n
  4                    5     5     1          aar            n
  5                    4     4     1          aar            n
  6                    5     5     1          aar            n
  7                    5     5     1          aar            n
  8                    15    15    1          aar            n
                                                             n
                                                             n
                                                             n
                                                             n
                                                             n
                                                             n
                                                             n
                                                             n
```

Configuring IP services for Application Enablement Services

About this task

Configure IP Services for the Avaya Aura® Application Enablement Services (AES) transport link.

Procedure

1. Use the Communication Manager System Access Terminal (SAT) interface to configure IP services for the AES transport link. Use the **`change ip-services`** command.
2. On page 1, under **Type**, type `AESVCS`.
3. Under **Enabled**, type `y`.
4. For **Local Node**, type `procr`.
5. For **Local Port**, select the default port number 8765.
6. On page 3, under **AE Services Server**, type the name of the AES server.
7. For **Password**, type the AES administration password.

Note:

The name and password entered for the AE Services Server and Password fields are case sensitive, and must match the name and password on the AES server.

8. Set **Enabled** to `y`.

Example

The Communication Manager IP services page 1 displays the AESVCS (Application Enablement Services) IP Service type.

```
change ip-services                                             Page   1 of   3

                                   IP SERVICES
 Service       Enabled      Local          Local         Remote         Remote
  Type                      Node           Port          Node           Port
AESVCS          y        procr            8765
```

The Communication Manager IP services page 3 displays the Application Enablement Services (AES) server name. The name for the AES server is from the AES installation. You can determine the administered name from the AES server by typing **`uname -n`** at the Linux command prompt.

```
change ip-services                                          Page   3 of   3
                          AE Services Administration

 Server ID    AE Services      Password          Enabled    Status
                 Server
    1:        HCAP6AES                            y
    2:                                            y
    3:                                            y
    4:                                            y
    5:                                            y
    6:                                            y
    7:                                            y
    8:                                            _
    9:                                            _
   10:                                            _
   11:                                            _
   12:                                            _
   13:                                            _
   14:                                            _
   15:                                            _
   16:                                            _
```

Configuring a CTI Link for Application Enablement Services

About this task

Add a CTI link from the Communication Manager to the Avaya Aura® Application Enablement Services (AES) server. The other end of this CTI link is configured on the Avaya Aura® AES server. For more information, see Adding a CTI link to the Communication Manager on page 105.

Procedure

1. Use the Communication Manager System Access Terminal (SAT) interface to add a CTI link for the Avaya Aura® AES server. Use the **`add cti-link`** command.
2. Type `add cti-link n`, where *n* is an available CTI link number.
3. In the **Extension** field, type an available extension number.
4. For **Type**, type `ADJ-IP`.
5. For **Name**, type a descriptive name for this CTI link to the Avaya Aura® AES server. For example, type `CTI to AES`.

Example

The Communication Manager CTI link page displays an ADJ-IP link type. The ADJ-IP link type is for Adjunct Switch Application Interface (ASAI) links administered by Avaya CTI applications, such as Avaya Aura® Application Enablement Services.

```
display cti-link 1                                          Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 19999
     Type: ADJ-IP
                                                                  COR: 1
     Name: CTI to AES
```

Enabling the Auto Hold system parameter

About this task

On the Communication Manager System Parameters Features form, enable the Auto Hold system parameter. This ensures that the first call is not dropped if a second call is selected. You must enable this feature to support third call appearance button functionality with Avaya Aura® Contact Center and Avaya Agent Desktop.

Procedure

Use the System Access Terminal (SAT) interface to enable the **Auto Hold** feature. Use the **change system-parameters** command.

```
display system-parameters features                              Page   6 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
         Public Network Trunks on Conference Call: 5                Auto Start? n
    Conference Parties with Public Network Trunks: 6                Auto Hold? y
 Conference Parties without Public Network Trunks: 6             Attendant Tone? y
         Night Service Disconnect Timer (seconds): 180            Bridging Tone? n
                  Short Interdigit Timer (seconds): 3           Conference Tone? n
               Unanswered DID Call Timer (seconds):              Intrusion Tone? n
               Line Intercept Tone Timer (seconds): 30     Mode Code Interface? y
                  Long Hold Recall Timer (seconds): 0
                       Reset Shift Timer (seconds): 0
     Station Call Transfer Recall Timer (seconds): 0          Recall from VDN? n
           Trunk Alerting Tone Interval (seconds): 15
                                DID Busy Treatment: tone
               Allow AAR/ARS Access from DID/DIOD? n
                 Allow ANI Restriction on AAR/ARS? n
Use Trunk COR for Outgoing Trunk Disconnect/Alert? n
                  7405ND Numeric Terminal Display? n                   7434ND? n



    DTMF Tone Feedback Signal to VRU - Connection:          Disconnection:
```

Configuring a Class of Restriction to block multiple and nested consults

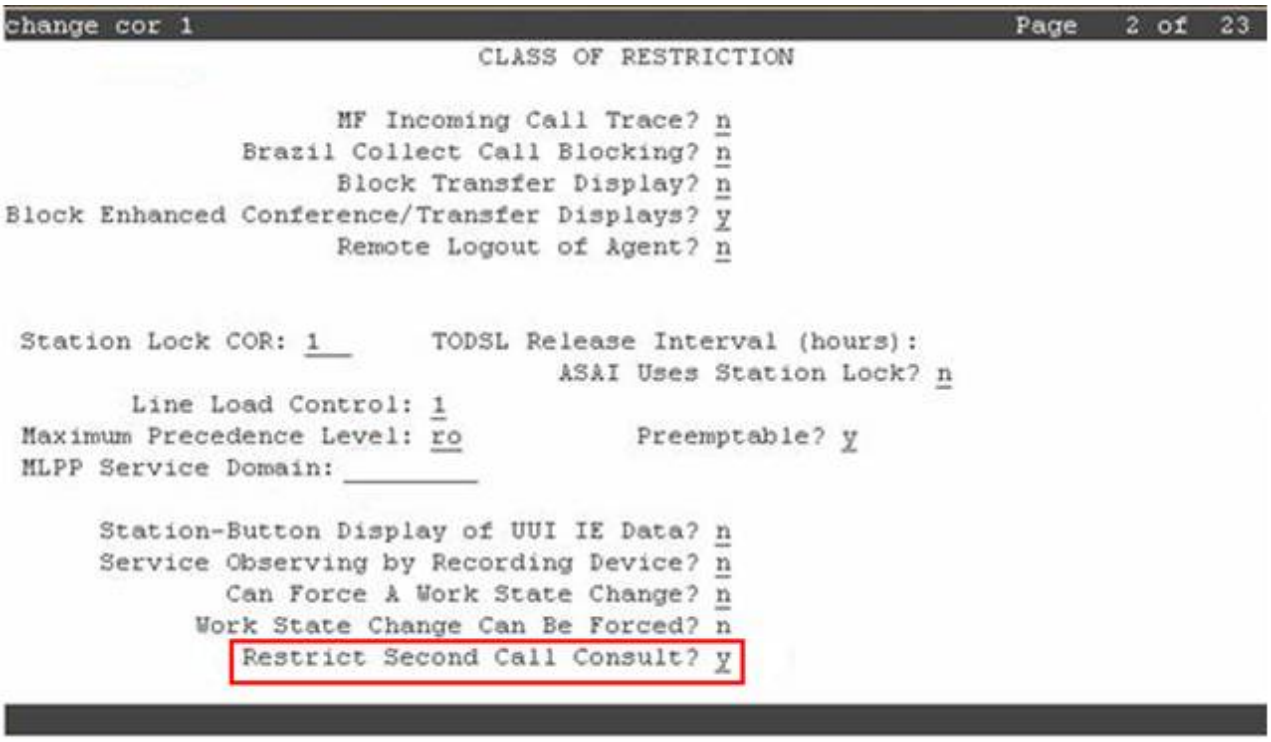
About this task

Configure a Class of Restriction (COR) that enables the Restrict Second Call Consult option. A Class of Restriction (COR) feature defines different levels of call origination and termination privileges, applies administration settings to all objects that share the same COR number, identifies the CORs that can be service observed, and the CORs that can be a service observer. CORs can be assigned to a variety of objects, including agent stations.

When the Restrict Second Call Consult option is enabled, Communication Manager blocks multiple and nested consults when a second consult is initiated from a station using this Class of Restriction (COR). Ensure that all Communication Manager agent stations controlled by Avaya Aura® Contact Center are using a COR with the Restrict Second Call Consult option enabled.

Procedure

Use the System Access Terminal (SAT) interface to enable the **Restrict Second Call Consult** option on a Class of Restriction. Use the **change cor** command.



Creating the agent extensions

About this task

On the Avaya Aura® Communication Manager, create the agent extensions. To ensure proper integration and Avaya Aura® Contact Center call control, Communication Manager stations (phones) must be configured as follows:

- A maximum of three call appearance buttons per agent station
- Restrict Last Appearance enabled
- Priority call feature disabled, as it is not supported
- IP Softphone enabled (IP Softphone is required to be enabled only when using a softphone. When enabled, agents can use a softphone or a desk phone. When disabled, agents can use only a desk phone.)
- Bridged Appearance is not supported.
- Per Station CPN - Send Calling Number enabled. If you want agents to see the calling party details, ensure this is enabled. If you want to hide the calling party details from agents, ensure this is disabled.

A limited configuration of Call Forwarding is supported, for more information see Coverage Path configuration on page 181.

With Communication Manager, Contact Center supports the following H.323 phones:

H.323 phones	Two call appearance buttons	Three call appearance buttons
Avaya 1600 Series IP deskphones	Yes	No
Avaya 4600 Series IP deskphones	Yes	Yes
Avaya 96x0 Series IP deskphones	Yes	Yes
Avaya 96x1 Series IP deskphones	Yes	Yes
Avaya J129 IP deskphone Avaya J139 IP deskphone Avaya J169 IP deskphone Avaya J179 IP deskphone	Yes	Yes
Avaya Agent Desktop embedded softphone. Provision an IP_Agent license on the Communication Manager for each softphone used by Contact Center.	Yes	Yes
Avaya one-X® Communicator softphone. You must disable the Agent Desktop embedded softphone to use Avaya one-X® Communicator.	Yes	Yes

Contact Center supports the following digital phones:

Digital phones	Two call appearance buttons	Three call appearance buttons
Avaya 24xx Series deskphones	Yes	No
Avaya 64xx Series deskphones	Yes	No

Contact Center supports the following SIP phones:

SIP phones	Two call appearance buttons	Three call appearance buttons
Avaya 96x0 Series IP deskphones	Yes	Yes
Avaya 96x1 Series IP deskphones	Yes	Yes
Avaya 9608 IP deskphone	Yes	Yes
Avaya 9611G IP deskphone	Yes	Yes
Avaya 9621G IP deskphone	Yes	Yes
Avaya 9641G IP deskphone	Yes	Yes

Table continues…

SIP phones	Two call appearance buttons	Three call appearance buttons
Avaya J129 IP deskphone Avaya J139 IP deskphone Avaya J169 IP deskphone Avaya J179 IP deskphone	Yes	Yes
Avaya one-X® Communicator softphone. You must disable the Agent Desktop embedded softphone to use Avaya one-X® Communicator.	Yes	Yes
Avaya Workplace Client for Windows softphone. You must disable the Agent Desktop embedded softphone to use Avaya Workplace Client for Windows.	Yes	Yes

Contact Center supports SIP phones for DTMF functionality. Contact Center supports SIP phones for High Availability functionality.

Avaya Agent Desktop supports three voice modes; Desk Phone, My Computer (softphone), Other Phone (Telecommuter mode).

- For each Agent Desktop agent, supervisor, or agent supervisor using My Computer (softphone) or Other Phone (Telecommuter mode), provision one IP_Agent license on the Communication Manager.
- For each Agent Desktop agent, supervisor, or agent supervisor using Desk Phone mode, the corresponding Communication Manager station consumes one IP_Phone license.
- Agent Desktop agents or agent supervisors that handle only multimedia contacts do not require Communication Manager licenses.

Shuffling (Direct IP to IP Audio Connections):

If you are using an Avaya Aura® Unified Communications platform PABX, Avaya recommends that you enable the shuffling feature to avoid unnecessary DSP usage. Avaya Aura® Shuffling (Direct IP-IP Audio Connections) attempts to renegotiate the media on an established SIP call, to update the anchor point of the media processor, thereby reducing the total number of Digital Signal Processor (DSP) channels required. On your Communication Manager, configure “Direct IP-IP Audio Connections? y” on every agent station, and on the SIP Signaling group configuration screens.

Note:

Communication Manager consumes DSPs if shuffling is turned off on either the SIP Signaling groups, or any of the agent IP stations. Avaya recommends that you enable shuffling on all agent stations (phones) and on the SIP signaling group.

Configure Communication Manager stations (phones) with a maximum of three call appearance buttons per agent station controlled by Contact Center.

Procedure

1. On the Communication Manager, use the System Access Terminal (SAT) interface to create an agent extension (workstation). Use the **`add station n`** command.

   For example, enter **`add station 70000`**.

2. If this station is to support three call appearance buttons, ensure that the station COR setting matches a Class of Restriction (COR) that enables the *Restrict Second Call Consult* option.
3. Enable **Restrict Last Appearance** on each station.
4. Repeat the SAT **`add station n`** command for each additional agent phone (extension) required.

Procedure job aid

The following Communication Manager station displays show one of the extensions (agent phones) configured to support Avaya Aura® Contact Center. The example extension number is 70000 and the phone type is an Avaya IP Deskphone 9640.

```
display station 70000                                    Page   1 of   5
                                    STATION

Extension: 70000                      Lock Messages? n                BCC: 0
     Type: 9640                       Security Code: 12345678          TN: 1
     Port: S09339                   Coverage Path 1:                  COR: 1
     Name: Agent one                Coverage Path 2:                  COS: 1
                                    Hunt-to Station:

STATION OPTIONS
                                         Time of Day Lock Table:
             Loss Group: 19          Personalized Ringing Pattern: 1
                                              Message Lamp Ext: 70000
           Speakerphone: 2-way             Mute Button Enabled? y
       Display Language: english                Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal            Media Complex Ext:
   Survivable Trunk Dest? y                        IP SoftPhone? y

                                        IP Video Softphone? n
                                  Short/Prefixed Registration Allowed: default

                                        Customizable Labels? y
```

Figure 5: Communication Manager station 70000

```
display station 70000                                    Page   2 of   5
                                    STATION
FEATURE OPTIONS
            LWC Reception: spe              Auto Select Any Idle Appearance? n
           LWC Activation? y                        Coverage Msg Retrieval? y
  LWC Log External Calls? n                                  Auto Answer: none
            CDR Privacy? n                             Data Restriction? n
   Redirect Notification? y                   Idle Appearance Preference? n
 Per Button Ring Control? n                 Bridged Idle Line Preference? n
   Bridged Call Alerting? n                     Restrict Last Appearance? Y
  Active Station Ringing: single
                                                        EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number? Y
       Service Link Mode: as-needed                    EC500 State: enabled
         Multimedia Mode: enhanced                 Audible Message Waiting? n
    MWI Served User Type:                        Display Client Redirection? n
            AUDIX Name:                        Select Last Used Appearance? n
                                                 Coverage After Forwarding? s
                                                   Multimedia Early Answer? n
 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
  Emergency Location Ext: 70000         Always Use? n IP Audio Hairpinning? n
     Precedence Call Waiting? y
```

Figure 6: Communication Manager station 70000 continued

```
display station 70000                                    Page   4 of   5
                                    STATION
 SITE DATA
       Room:                                              Headset? n
       Jack:                                              Speaker? n
      Cable:                                            Mounting: d
      Floor:                                         Cord Length: 0
   Building:                                           Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr    Configure 2 or 3                  5:
 2: call-appr    call appearance buttons           6:
 3: call-appr                                      7:
 4:                                                8:

    voice-mail
```

Figure 7: Communication Manager station 70000 continued

Adding agent workstations to the numbering tables

About this task

Avaya Aura® Contact Center (AACC) agents use Communication Manager workstations to handle customer calls. Add the Avaya Aura® Contact Center controlled workstations to the numbering tables to create caller identifications and calling numbers for locally originated Contact Center agent calls.

Adding agent workstations to the numbering tables ensures that the incoming SIP requests contain “From” headers that contain the agent's Uniform Resource Identifier (URI).

Note:

If a table entry applies to a SIP connection to Avaya Aura® Session Manager, the resulting number must be a complete E.164 number.

Procedure

1. Using the Communication Manager System Access Terminal, enter **change public-unknown-numbering**.
2. In the **Ext Len** field, type your extension length.
3. In the **Ext Code** field, type the starting digit(s) of the extension, such as the country code.
4. Leave the **Trk Grp(s)** field blank to apply to all trunks in the system.
5. In the **CPN Len** field, type the number of digits in your calling number.
6. Press **Enter** to save your changes.
7. Enter **`change private-numbering`**.
8. In the **Ext Len** field, type your extension length.
9. In the **Ext Code** field, type the starting digit(s) of the extension, such as the country code.
10. Leave the **Trk Grp(s)** field blank to apply to all trunks in the system.
11. In the **CPN Len** field, type the number of digits in your calling number.

    Note:

    The **CPN Len** parameter must have the same number of digits as the AACC agent station numbers. Otherwise, AACC does not recognize the incoming call as an AACC extension.
12. Press **Enter** to save your changes.

Enabling Gratuitous Address Resolution Protocol on agent extensions

About this task

If your Avaya Aura® Media Servers are installed on the Linux operating system, and if they are installed on the same network subnet as the H.323 phones, then you must configure your Avaya Aura® Communication Manager Utility Server to allow the phones and Avaya Aura® Media Server to support the High Availability feature. You must enable Gratuitous Address Resolution Protocol (GRATARP) for your agent extensions (stations/phones).

The Utility Admin IP Phone Settings Editor from Utility Server provides a Web-based tool for configuring the IP phone settings file. This significantly simplifies the process of making changes to the IP phone settings file and provides enhanced validation to help avoid misconfigurations. The Utility Admin IP Phone Settings Editor also provides IP Phone firmware management, enabling you to upload new phone firmware to the file server.

Procedure

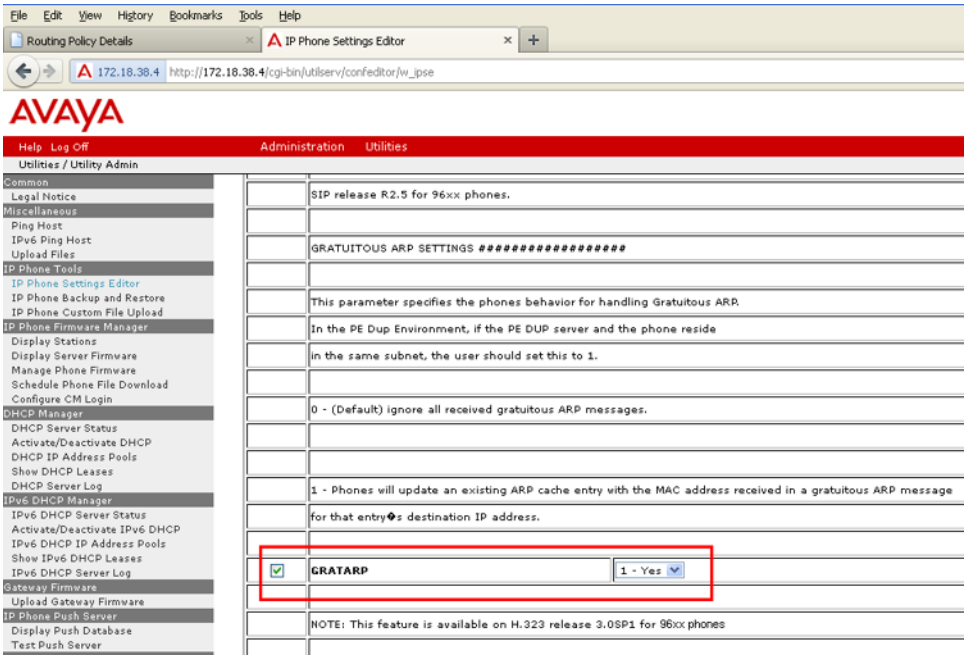
1. Start Internet Explorer.
2. In the Internet Explorer address box, type `http://<Utility Server IP address>`.

   For example, type `http://172.18.38.4`
3. On the Utility Server Web console, click **Utilities**.
4. Click **Utility Admin**.
5. Enter your Utility Server user name.
6. Click **Logon**.
7. Enter your Utility Server password.
8. Click **Logon**.

   The system displays the Utility Server Utility Admin menu.
9. From the left navigation menu, select **IP Phone Settings Editor**.
10. Click **Proceed with selected values**.
11. For your Contact Center phone types, set **GRATARP** to **Yes**. This configures the phones to process Gratuitous Address Resolution Protocol (ARP) requests and provides duplicate IP address detection. This enables the phones to work with Linux-based Avaya Aura® Media Server in a High Availability resilient solution.

Example

Enabling Gratuitous Address Resolution Protocol (ARP) on agent extensions with 9640 phones.


File Edit View History Bookmarks Tools Help
Routing Policy Details
IP Phone Settings Editor
172.18.38.4 http://172.18.38.4/cgi-bin/utilserv/confeditor/w_ipse
AVAYA
Help Log Off
Administration
Utilities
Utilities / Utility Admin
Common
Legal Notice
Miscellaneous
Ping Host
IPv6 Ping Host
Upload Files
IP Phone Tools
IP Phone Settings Editor
IP Phone Backup and Restore
IP Phone Custom File Upload
IP Phone Firmware Manager
Display Stations
Display Server Firmware
Manage Phone Firmware
Schedule Phone File Download
Configure CM Login
DHCP Manager
DHCP Server Status
Activate/Deactivate DHCP
DHCP IP Address Pools
Show DHCP Leases
DHCP Server Log
IPv6 DHCP Manager
IPv6 DHCP Server Status
Activate/Deactivate IPv6 DHCP
IPv6 DHCP IP Address Pools
Show IPv6 DHCP Leases
IPv6 DHCP Server Log
Gateway Firmware
Upload Gateway Firmware
IP Phone Push Server
Display Push Database
Test Push Server
SIP release R2.5 for 96xx phones.
GRATUITOUS ARP SETTINGS ##################
This parameter specifies the phones behavior for handling Gratuitous ARP.
In the PE Dup Environment, if the PE DUP server and the phone reside
in the same subnet, the user should set this to 1.
0 - (Default) ignore all received gratuitous ARP messages.
1 - Phones will update an existing ARP cache entry with the MAC address received in a gratuitous ARP message
for that entry's destination IP address.
GRATARP
1 - Yes
NOTE: This feature is available on H.323 release 3.0SP1 for 96xx phones

Chapter 5: System Manager configuration

Avaya Aura® System Manager delivers a set of shared, secure management services and a common console across multiple products. System Manager includes the following central management services:

- User Management: Allows for the administration of users and user groups.
- Communication System Management: Allows for the administration of individual and group stations and mailboxes.
- Routing: Allows for the administration of routing policies for all Session Manager instances within an enterprise.
- Alarm Management Service: Supports alarm monitoring, acknowledgement, configuration, clearing, and retiring.
- Logging Service: Receives log events formatted in the common log format.
- Enterprise Licensing Management Service.

You use Avaya Aura® System Manager to manage and configure Avaya Aura® Session Manager.

A central database that resides on the System Manager server stores all the System Manager central data, the Session Manager administration data, and the Central Data Distribution Service information. The Central Data Distribution Service detects changes to the System Manager central database and distributes these changes to the Session Manager instances. All communication between System Manager and Session Manager instances is done over secure links.

Prerequisites

Ensure that your Avaya Aura® platform meets the minimum template requirements for integration with Contact Center.

Logging on to the System Manager Web interface

Before you begin

- A user account to log on to the Avaya Aura® System Manager Web interface. If you do not have a user account, contact your system administrator to create your account.

About this task

The System Manager Web interface is the main interface of Avaya Aura® System Manager. You must log on to the System Manager Web console before you can perform any tasks.

Procedure

1. On the browser, type the Avaya Aura® System Manager URL (`https://<SERVER_NAME>/SMGR`) and press the `Enter` key.

   Where *SERVER_NAME* is the name or IP address of your System Manager server.
2. In the **User ID** box, type the user name.
3. In the **Password** box, type the password.
4. Click **Log On**.

Procedure job aid

The System Manager home page displays the main navigation menu. The tasks you can perform using System Manager depends on your user role.

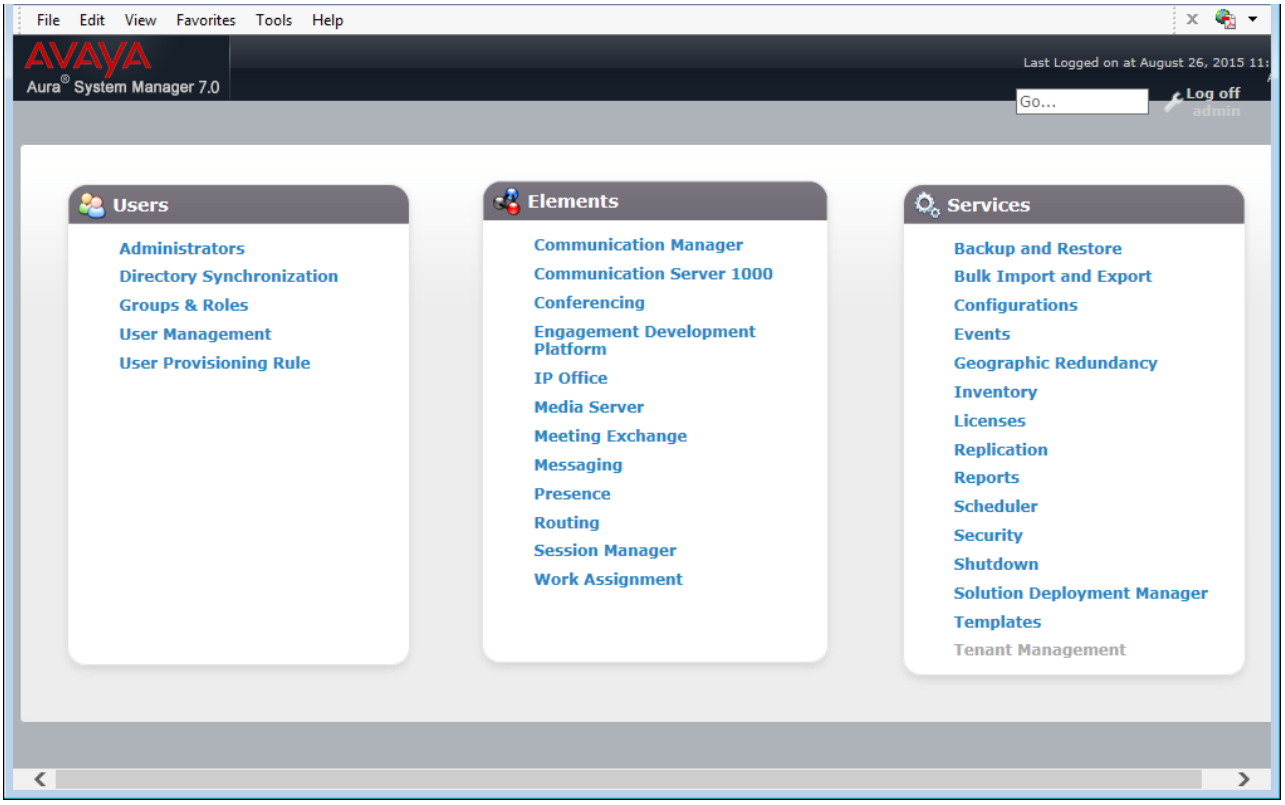


Figure 8: Example of the System Manager Web page

Chapter 6: Session Manager configuration

This section describes how to configure Avaya Aura® Session Manager for use with Avaya Aura® Contact Center.

Avaya Aura® Session Manager is a SIP routing and integration tool. It integrates all the SIP entities across the entire enterprise network within a company. Session Manager provides a core communication service that builds on existing equipment but adds a SIP-based architecture. Session Manager connects to and acts as a system-wide dial plan for call processing applications such as Avaya Aura® Communication Manager using direct SIP connections.

In an enterprise solution, the various SIP network components are represented as *SIP Entities* and the connections/trunks between Session Manager and those components are represented as *Entity Links*. Each SIP Entity connects to Session Manager and relies on Session Manager to route calls to the correct destination. This approach reduces the dial plan and trunking administration needed on each SIP Entity, and consolidates administration in a central place, namely Avaya Aura® System Manager.

Important:

If there are Contact Center agents using SIP desk phones, you must ensure that you configure Session Manager and the associated SIP entities to use TLS as the SIP Network Transport communication protocol. The default port number for TLS is 5061.

When calls arrive at Session Manager from a SIP Entity, Session Manager applies SIP protocol and numbering modifications to the calls. These modifications, referred to as *Adaptations*, are sometimes necessary to resolve SIP protocol differences between different SIP Entities, and also serve the purpose of normalizing the calls to a uniform numbering format. Session Manager then matches the calls against *Dial Patterns*, and determines the destination SIP Entities based on *Routing Policies* specified in the matching Dial Patterns. Lastly, before the calls are routed to the respective SIP Entity destinations, Session Manager again applies Adaptations in order to bring the calls into conformance with the SIP protocol interpretation and numbering formats expected by the destination SIP Entities.

Note:

A second Session Manager is supported only in an Avaya Aura® Contact Center Mission Critical SIP High Availability solution. All other SIP-enabled Contact Center configurations using a Unified Communications PABX support only a single active Session Manager.

The following diagram shows a typical Session Manager deployment and configuration. The procedures and SIP Entity names in this section are based on this example routing configuration.

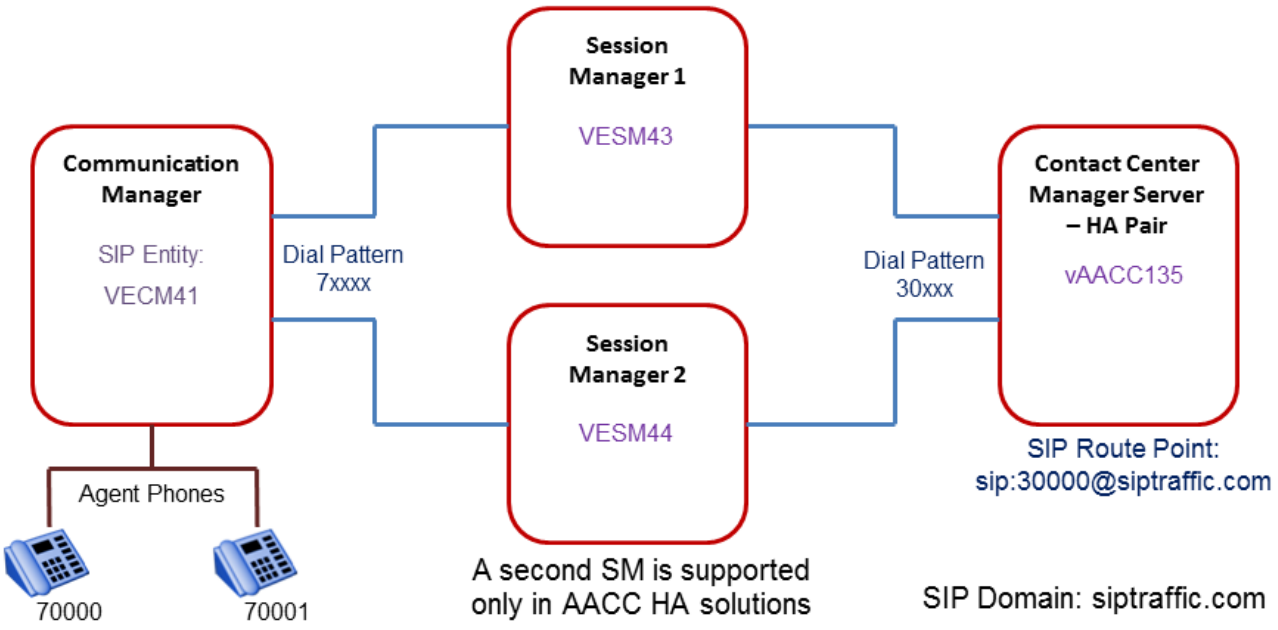


Figure 9: Example of a typical Session Manager routing solution

Session Manager offers a core communication service that builds on existing equipment but adds a SIP-based architecture. Session Manager connects to and acts as a system-wide dial plan for call processing applications such as Avaya Aura® Communication Manager using direct SIP connections.

You use Avaya Aura® System Manager to configure Avaya Aura® Session Manager.

Prerequisites

Log on to the System Manager Web interface. For more information, see Logging on to the System Manager Web interface on page 66.

Session Manager configuration procedures

About this task

This task flow shows you the sequence of procedures you perform to configure the Session Manager.

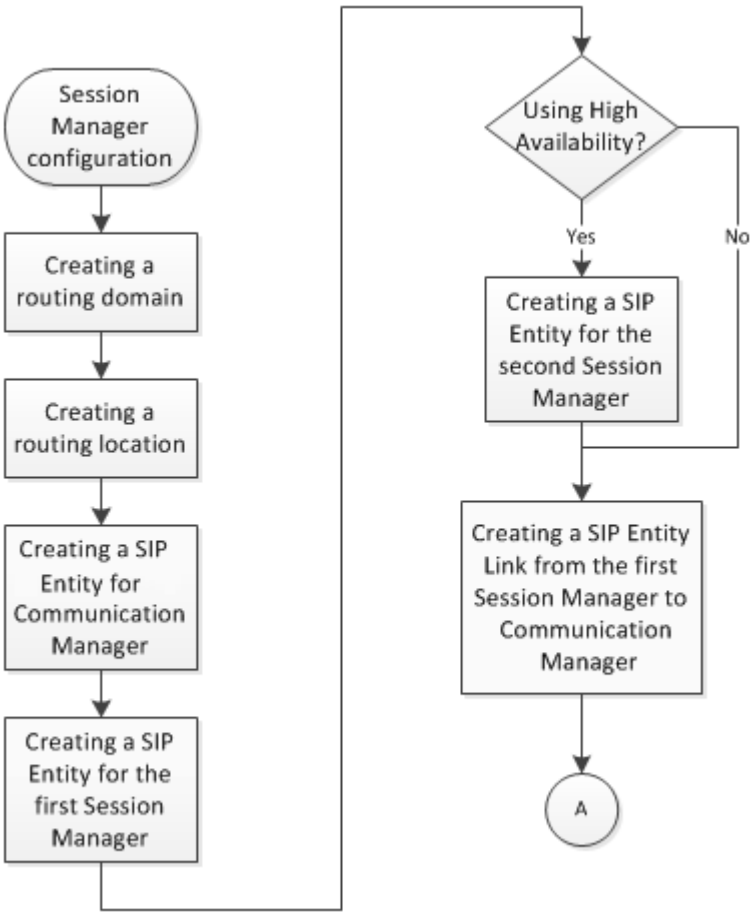


Figure 10: Session Manager configuration procedures

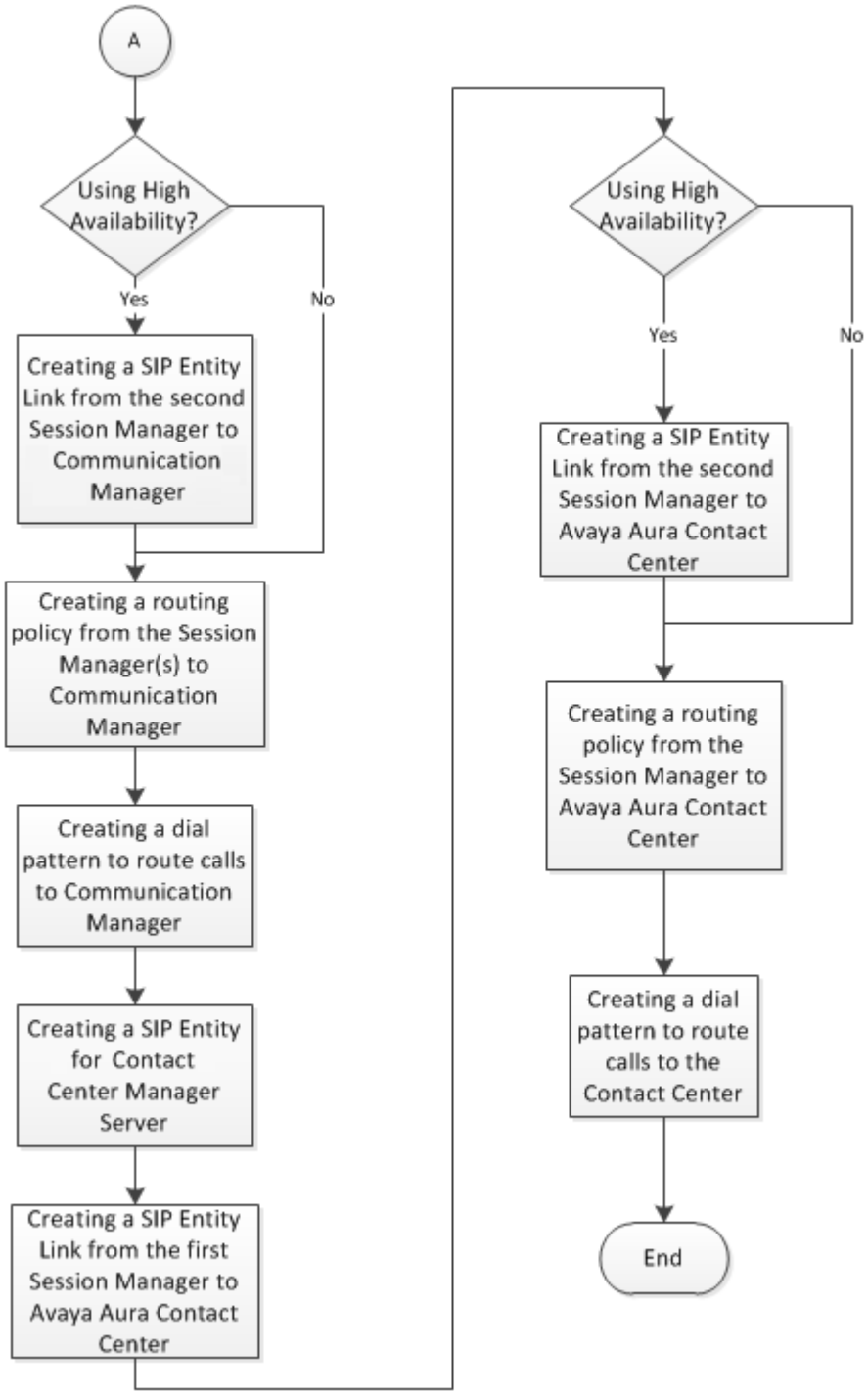


Figure 11: Session Manager configuration procedures continued

Creating a routing domain

About this task

Routing domains determine whether the Session Manager dial plan routes a particular call. Typically, in a contact center, the routing domain name matches the Windows Active Directory domain name.

Routing domains determine whether the Session Manager dial plan routes a particular call. SIP Domains are the domains for which Session Manager routes SIP calls. Session Manager applies Network Routing Policies to route calls in this domain to SIP Entities. For calls to other domains, Session Manager routes those calls to another SIP proxy (either a pre-defined default SIP proxy or one discovered through DNS).

The Session Manager SIP Routing Domain name configured for contact center solution must match the Avaya Aura® Contact Center "Local SIP Subscriber Domain Name".

Typically, in a contact center, the routing domain name also matches the Windows Active Directory domain name.

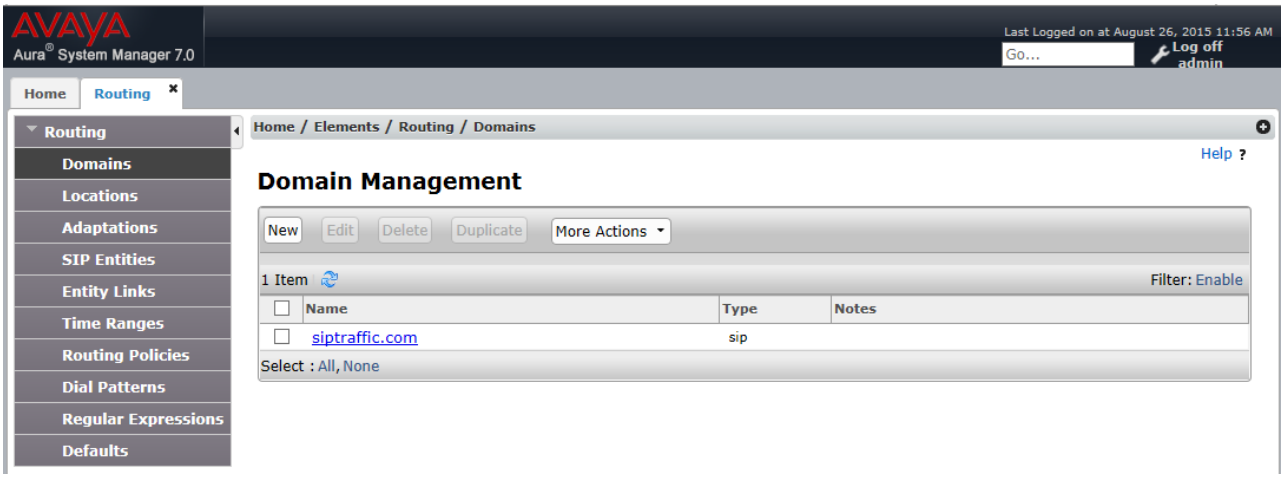
Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **Domains**.
2. Click **New**.
3. On the Domain Management page, in the **Name** box, type the new contact center solution domain name.

   Avaya recommends that you type a descriptive name for your domain.
4. From the **Type** list, select **sip**.
5. In the **Notes** box, type your notes about this domain.
6. Click **Commit**.

Example

Example of a Session Manager domain.



Creating a routing location

About this task

Configure the location of your Session Manager. Session Manager uses the origination location to determine which dial pattern to use when routing calls. Locations are also used to limit the number of calls coming out of or going to a physical location.

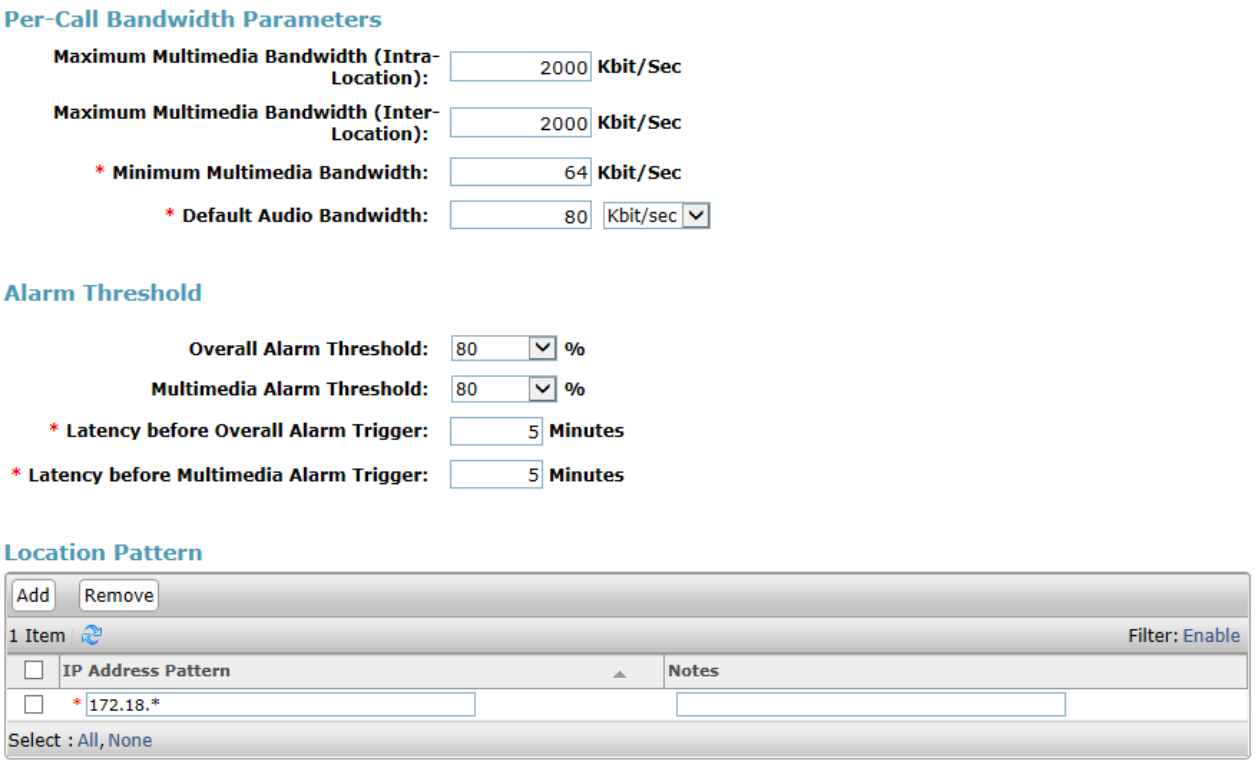
Procedure

1. On the System Manager console, select **Routing** > **Domains**
2. Click **New**.
3. In the **Name** box, type the location name.

   Avaya recommends that you type a descriptive name for your location.
4. In the **Notes** box, type your notes about this location.
5. From the **Managed Bandwidth Units** list, select **kbit/sec**.
6. In the **Total Bandwidth** box, type your required bandwidth.
7. To add a location pattern, click **Add** under **Location Pattern**.
8. In the **IP Address Pattern** box, type the pattern string to match your system.
9. Under **Location Pattern**, in the **Notes** box, type your notes about this pattern.
10. Click **Commit**.

Example

Example of a Session Manager routing location. If your Communication Manager has an IP address of 172.18.71.41 and if your Session Manager has an IP address of 172.18.71.47, then a suitable IP Address Pattern is 172.18.*. This pattern must cover the addresses that you deem part of this routing location.



Creating a SIP Entity for Communication Manager

About this task

A SIP Entity represents a SIP network element. Create a SIP Entity for Communication Manager. To administer minimal routing using Session Manager, you need to configure a SIP Entity of type Communication Manager and Session Manager.

Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** box, type the name of the Communication Manager SIP Entity.

   Avaya recommends that you type a descriptive name for your Communication Manager SIP Entity.
4. In the **FQDN or IP address** box, type the IP address of the Communication Manager.
5. From the **Type** list, select **CM**.
6. If you need to specify an Adaptation Module for the Communication Manager SIP entity, from the **Adaptation** list, select an adaptation value.

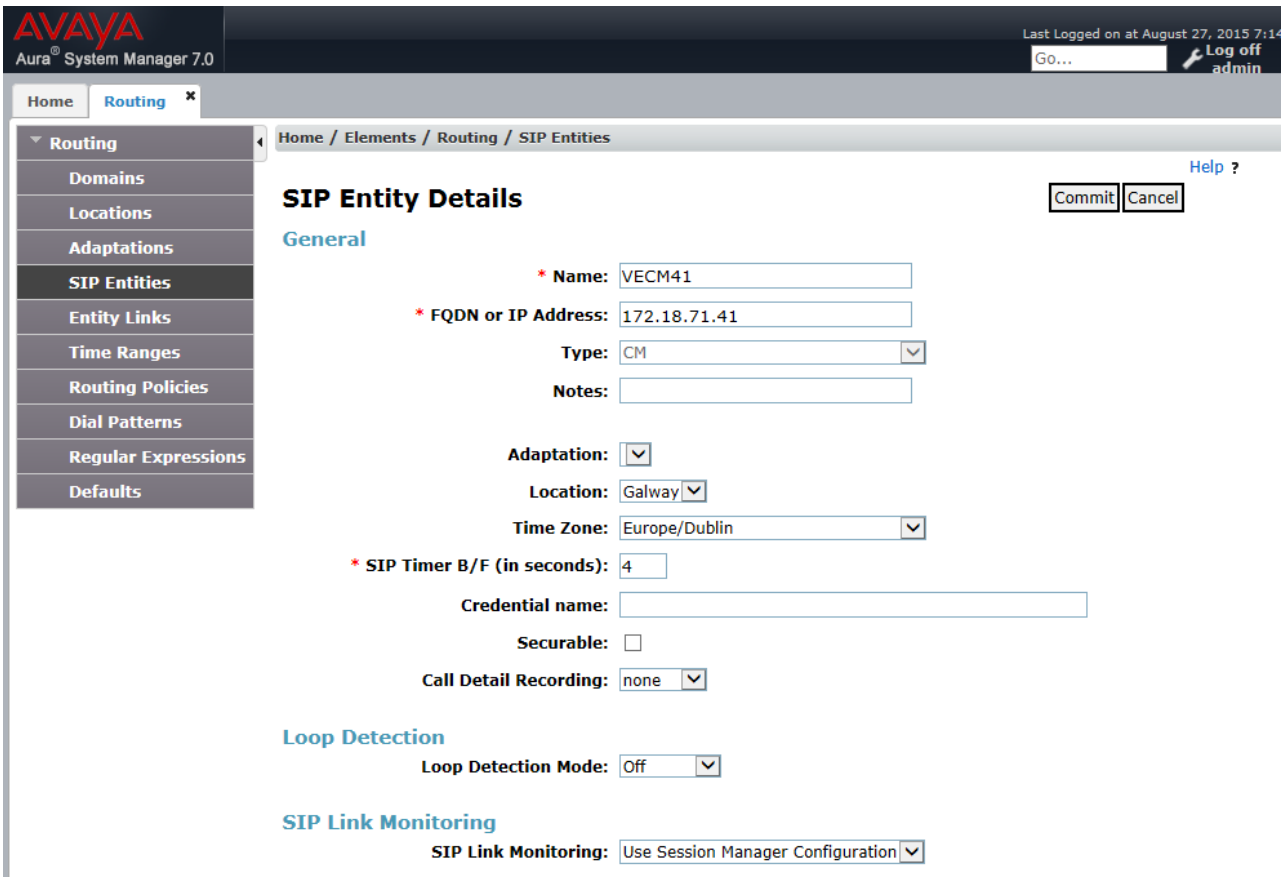
7. In the **Location** box, select the location for this Communication Manager.
8. In the **Credential name** box, enter a regular expression string.

   The Credential name is used for TLS connection validation by searching for this string in the SIP entity identity certificate.
9. From the **SIP Link Monitoring** list, select one of the following:
   - Use Session Manager Configuration - Use the settings under **Session Manager–Session Manager Administration**.
   - Link Monitoring Enabled - Enables link monitoring on this SIP entity.
   - Link Monitoring Disabled - Link monitoring is turned off for this SIP entity.
10. If you need to specify the port parameters, under **Port** click **Add**.

    When Session Manager receives a request where the host-part of the request-URI is the IP address of the Session Manager, it associates one of the administered domains with the port on which the request was received.
11. Enter the necessary **Port** and **Protocol** parameters.
12. Click **Commit**.

Example

Example of a Communication Manager SIP Entity.



Variable definitions

Variable	Value
Name	SIP entity name. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the Communication Manager.
Type	SIP entity type, such as a Communication Manager.
Notes	Additional notes about the SIP entity.
Adaptation	Adaptation to be used for the SIP entity. Select from already defined adaptations.
Location	Communication Manager SIP entity location. Select from previously defined locations.
Time Zone	Time zone for the SIP entity.

Table continues…

Variable	Value
Override Port & Transport with DNS SRV	Specify if you wish to use DNS routing. SIP uses DNS procedures to allow a client to resolve a SIP URI into the IP address, port, and transport protocol of the next hop to contact. It also uses DNS routing to allow a server to send a response to a backup client if the primary client fails.
SIP Timer B/F (in seconds)	Amount of time the Session Manager waits for a response from the SIP entity.
Credential name	Enter a regular expression string in the Credential name. Credential name is used for TLS connection validation by searching this string in the SIP entity identity certificate.
Call Detail Recording	Select or clear the check box to turn SIP monitoring on or off.
Proactive cycle time (Seconds)	Enter a value between 120 and 9000 seconds. The default is 900. This specifies how often the entity is monitored when the link to the entity is up or active.
Reactive cycle time (Seconds)	Enter a value between 30 and 900 seconds. The default is 120. This specifies how often the entity is monitored when a link to the entity is down or inactive.
Number of retries	Enter a value between 0 and 15. The default is 1. This specifies the number of times Session Manager tries to ping or reach the SIP entity before marking it as down or unavailable.
Port	Add a listening port for the SIP entity.
Protocol	Protocol that the SIP entity uses.
SIP Domain	The domain of the SIP entity.
Notes	Additional notes about the port and port parameters.

Creating a SIP Entity for the first Session Manager

About this task

A SIP Entity represents a SIP network element. Create a SIP Entity for the Session Manager. To administer minimal routing using Session Manager, you need to configure two SIP Entities, a SIP Entity of type Communication Manager and a SIP Entity of type Session Manager.

Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **SIP Entries**.
2. Click **New**.

3. In the **Name** box, type the name of the Session Manager SIP Entity.

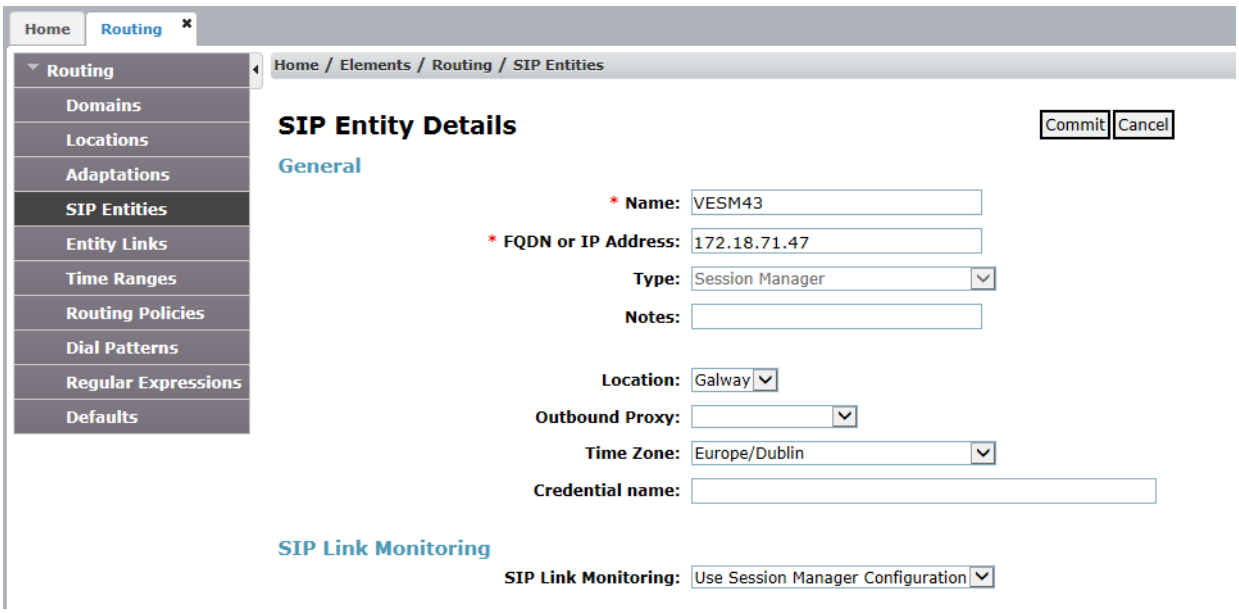
   Avaya recommends that you type a descriptive name for your Session Manager SIP entity.
4. In the **FQDN or IP address** box, type the IP address of the Session Manager.
5. From the **Type** list, select **Session Manager**.
6. If you need to specify an Adaptation Module for the Session Manager SIP entity, from the **Adaptation** list, select an adaptation value.
7. In the **Location** box, select the location for this Session Manager.
8. If the SIP entity type is **Session Manager** and you need to specify an Outbound Proxy for the SIP entity, click the drop-down selector for the **Outbound Proxy** box.
9. In the **Credential name** box, enter a regular expression string.

   The Credential name is used for TLS connection validation by searching for this string in the SIP entity identity certificate.
10. From the **SIP Link Monitoring** list, select one of the following:
    - Use Session Manager Configuration - Use the settings under **Session Manager–Session Manager Administration**.
    - Link Monitoring Enabled - Enables link monitoring on this SIP entity.
    - Link Monitoring Disabled - Link monitoring is turned off for this SIP entity.
11. If you need to specify the port parameters, under **Port** click **Add**.

    When Session Manager receives a request where the host-part of the request-URI is the IP address of the Session Manager, it associates one of the administered domains with the port on which the request was received.
12. Enter the necessary **Port** and **Protocol** parameters.
13. Click **Commit**.

Example

Example of a Session Manager SIP Entity.



Variable definitions

Variable	Value
Name	SIP entity name. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the Session Manager SIP Entity.
Type	SIP entity type, such as a Session Manager.
Notes	Additional notes about the SIP entity.
Adaptation	Adaptation to be used for the SIP entity. Select from already defined adaptations.
Location	SIP entity location. Select from previously defined locations.
Outbound Proxy	Outbound proxy if the entity type is Session Manager, and you wish to specify a proxy.
Time Zone	Time zone for the SIP entity.
Override Port & Transport with DNS SRV	Specify if you wish to use DNS routing. SIP uses DNS procedures to allow a client to resolve a SIP URI into the IP address, port, and transport protocol of the next hop to contact. It also uses DNS routing to allow a server to send a response to a backup client if the primary client fails.
SIP Timer B/F (in seconds)	Amount of time the Session Manager waits for a response from the SIP entity.

Table continues…

Variable	Value
Credential name	Enter a regular expression string in the Credential name. Credential name is used for TLS connection validation by searching this string in the SIP entity identity certificate.
Call Detail Recording	Select or clear the check box to turn SIP monitoring on or off.
Proactive cycle time (Seconds)	Enter a value between 120 and 9000 seconds. The default is 900. This specifies how often the entity is monitored when the link to the entity is up or active.
Reactive cycle time (Seconds)	Enter a value between 30 and 900 seconds. The default is 120. This specifies how often the entity is monitored when a link to the entity is down or inactive.
Number of retries	Enter a value between 0 and 15. The default is 1. This specifies the number of times Session Manager tries to ping or reach the SIP entity before marking it as down or unavailable.
Port	Add a listening port for the SIP entity.
Protocol	Protocol that the SIP entity uses.
SIP Domain	The domain of the SIP entity.
Notes	Additional notes about the port and port parameters.

Creating a SIP Entity for the second Session Manager

About this task

Create a SIP Entity for the second Session Manager. To administer minimal routing using Session Manager, you must configure two SIP Entities, a SIP Entity of type Communication Manager and a SIP Entity of type Session Manager.

Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** box, type the name of the Session Manager SIP Entity.

   Avaya recommends that you type a descriptive name for your Session Manager SIP entity.
4. In the **FQDN or IP address** box, type the IP address of the Session Manager.
5. From the **Type** list, select **Session Manager**.
6. If you need to specify an Adaptation Module for the Session Manager SIP entity, from the **Adaptation** list, select an adaptation value.

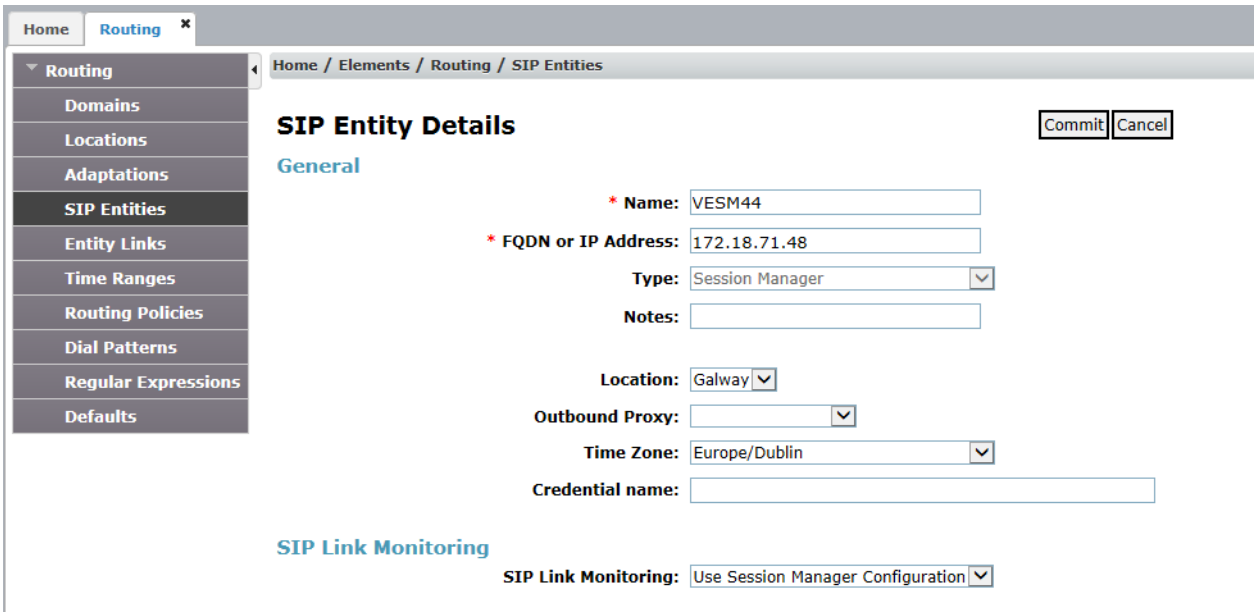
7. In the **Location** box, select the location for this Session Manager.
8. If the SIP entity type is **Session Manager** and you need to specify an Outbound Proxy for the SIP entity, click the drop-down selector for the **Outbound Proxy** box.
9. In the **Credential name** box, enter a regular expression string.

   The **Credential name** is used for TLS connection validation by searching for this string in the SIP entity identity certificate.
10. From the **SIP Link Monitoring** list, select one of the following:
    - Use Session Manager Configuration - Use the settings under **Session Manager – Session Manager Administration**.
    - Link Monitoring Enabled - Enables link monitoring on this SIP entity.
    - Link Monitoring Disabled - Link monitoring is turned off for this SIP entity.
11. If you need to specify the port parameters, under **Port**, click **Add**.

    When Session Manager receives a request where the host-part of the request-URI is the IP address of the Session Manager, it associates one of the administered domains with the port on which the request was received.
12. Enter the necessary **Port** and **Protocol** parameters.
13. Click **Commit**.

Example

Example of the SIP Entity for the second Session Manager.



Variable definitions

Variable	Value
Name	SIP entity name. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the Session Manager SIP Entity.
Type	SIP entity type, such as a Session Manager.
Notes	Additional notes about the SIP entity.
Adaptation	Adaptation to be used for the SIP entity. Select from already defined adaptations.
Location	SIP entity location. Select from previously defined locations.
Outbound Proxy	Outbound proxy if the entity type is Session Manager, and you wish to specify a proxy.
Time Zone	Time zone for the SIP entity.
Override Port & Transport with DNS SRV	Specify if you wish to use DNS routing. SIP uses DNS procedures to allow a client to resolve a SIP URI into the IP address, port, and transport protocol of the next hop to contact. It also uses DNS routing to allow a server to send a response to a backup client if the primary client fails.
SIP Timer B/F (in seconds)	Amount of time the Session Manager waits for a response from the SIP entity.
Credential name	Enter a regular expression string in the Credential name. Credential name is used for TLS connection validation by searching this string in the SIP entity identity certificate.
Call Detail Recording	Select or clear the check box to turn SIP monitoring on or off.
Proactive cycle time (Seconds)	Enter a value between 120 and 9000 seconds. The default is 900. This specifies how often the entity is monitored when the link to the entity is up or active.
Reactive cycle time (Seconds)	Enter a value between 30 and 900 seconds. The default is 120. This specifies how often the entity is monitored when a link to the entity is down or inactive.
Number of retries	Enter a value between 0 and 15. The default is 1. This specifies the number of times Session Manager tries to ping or reach the SIP entity before marking it as down or unavailable.

Table continues…

Variable	Value
Port	Add a listening port for the SIP entity.
Protocol	Protocol that the SIP entity uses.
SIP Domain	The domain of the SIP entity.
Notes	Additional notes about the port and port parameters.

Creating a SIP Entity Link from the first Session Manager to the Communication Manager

About this task

Create a SIP entity link to the Communication Manager. Session Manager enables you to create an entity link between the Session Manager and any other administered SIP entity. You must configure an entity link between a Session Manager and any entity that you have administered if you want Session Manager to be able to send or receive messages from that entity directly. To be able to communicate with other SIP entities, each Session Manager instance must know the port and the transport protocol of its entity link to these SIP entities in the network.

Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **Entity Links**.
2. Click **New**.
3. In the **Name** box, type the name for this SIP Entity Link.

   Avaya recommends that you type a descriptive name for your SIP Entity Link.
4. Under **SIP Entity 1**, select the required Session Manager SIP entity from the drop-down list and provide the required port number.

   SIP entity 1 must always be a Session Manager instance.

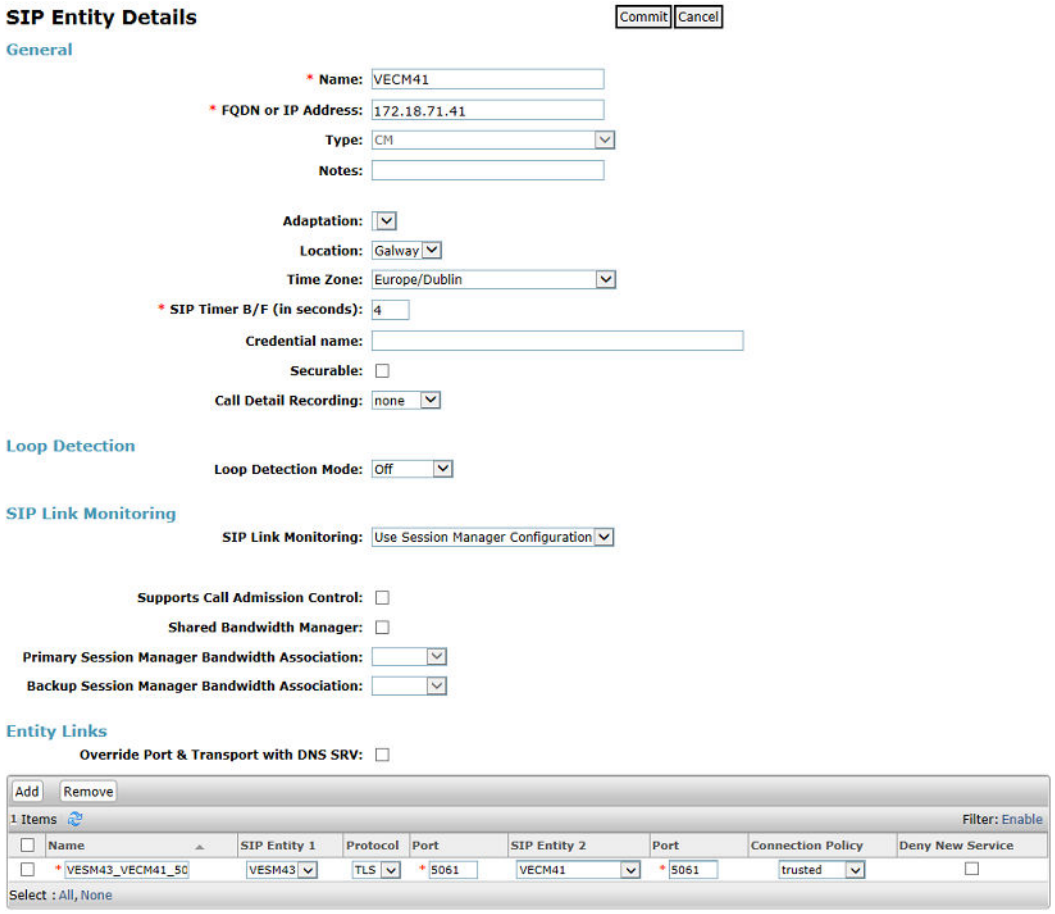
   The default port for TCP and UDP is 5060. The default port for TLS is 5061.
5. Under **SIP Entity 2**, select the required Communication Manager SIP entity from the drop-down list and provide the required port number.

   The port number is the port on which you have configured the remote entity to receive requests for the specified transport protocol.
6. From the Connection Policy list, select the **Trusted**.

   Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
7. Click **Commit**.

Example

The Communication Manager SIP Entity details show one link to the first Session Manager SIP Entity.



Creating a SIP Entity Link from the second Session Manager to the Communication Manager

About this task

Create a SIP entity link from the second Session Manager to the Communication Manager. You must configure an entity link to allow Session Manager to be able to send messages to, or receive messages from, that entity directly. To be able to communicate with other SIP entities, each Session Manager instance must know the port and the transport protocol of its entity link to these SIP entities in the network.

Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **Entity Links**.

2. Click **New**.
3. In the **Name** box, type the name for this SIP Entity Link.

   Avaya recommends that you type a descriptive name for your SIP Entity Link.
4. Under **SIP Entity 1**, select the required Session Manager SIP entity from the drop-down list and provide the required port number.

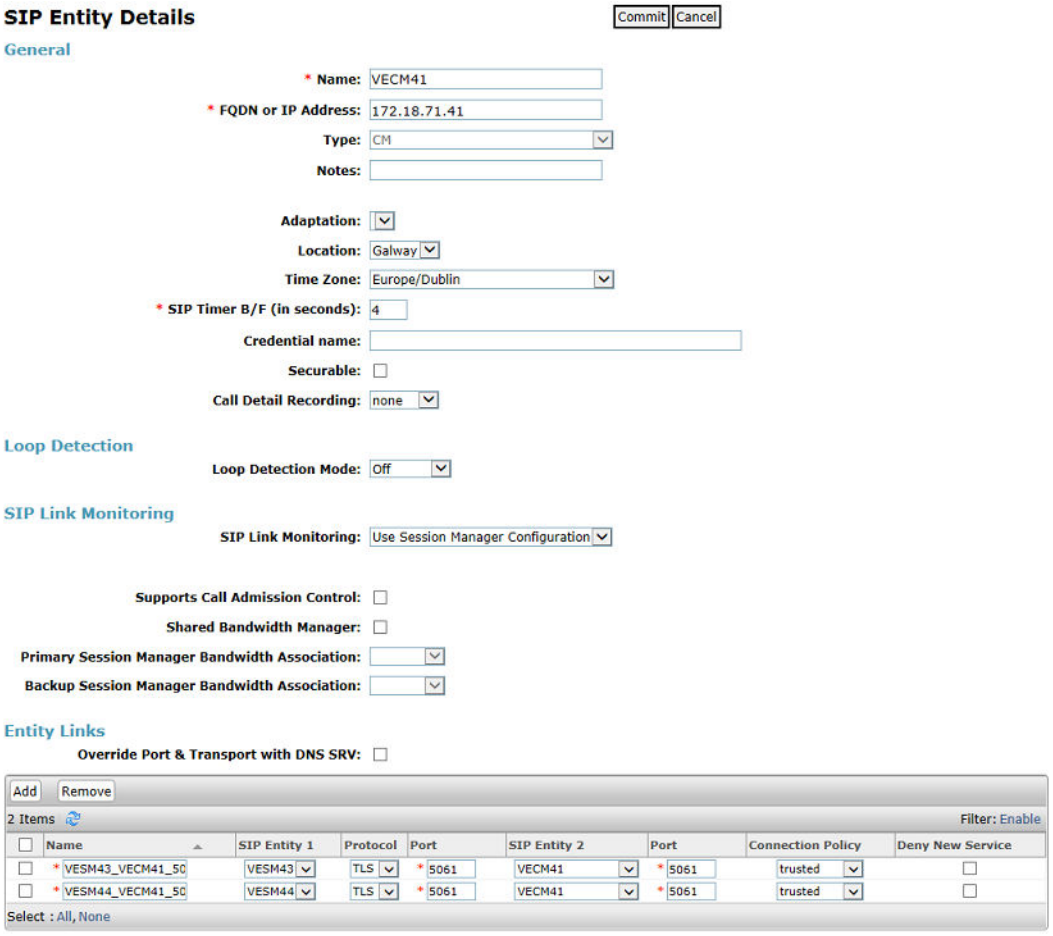
   SIP entity 1 must always be a Session Manager instance.

   The default port for TCP and UDP is 5060. The default port for TLS is 5061.
5. Under **SIP Entity 2**, select the required Communication Manager SIP entity from the drop-down list and provide the required port number.
6. From the Connection Policy list, select **Trusted**.

   Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
7. Click **Commit**.

Example

The Communication Manager SIP Entity details showing two SIP Entity links.



Creating a routing policy from the Session Manager to Communication Manager

About this task

Create a routing policy from Session Manager to Communication Manager. Routing Policies define how Session Manager routes calls between SIP network elements.

Session Manager uses the data configured in the Routing Policy to find the best match against the number (or address) of the called party.

Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **Routing Policies**.
2. Click **New**.

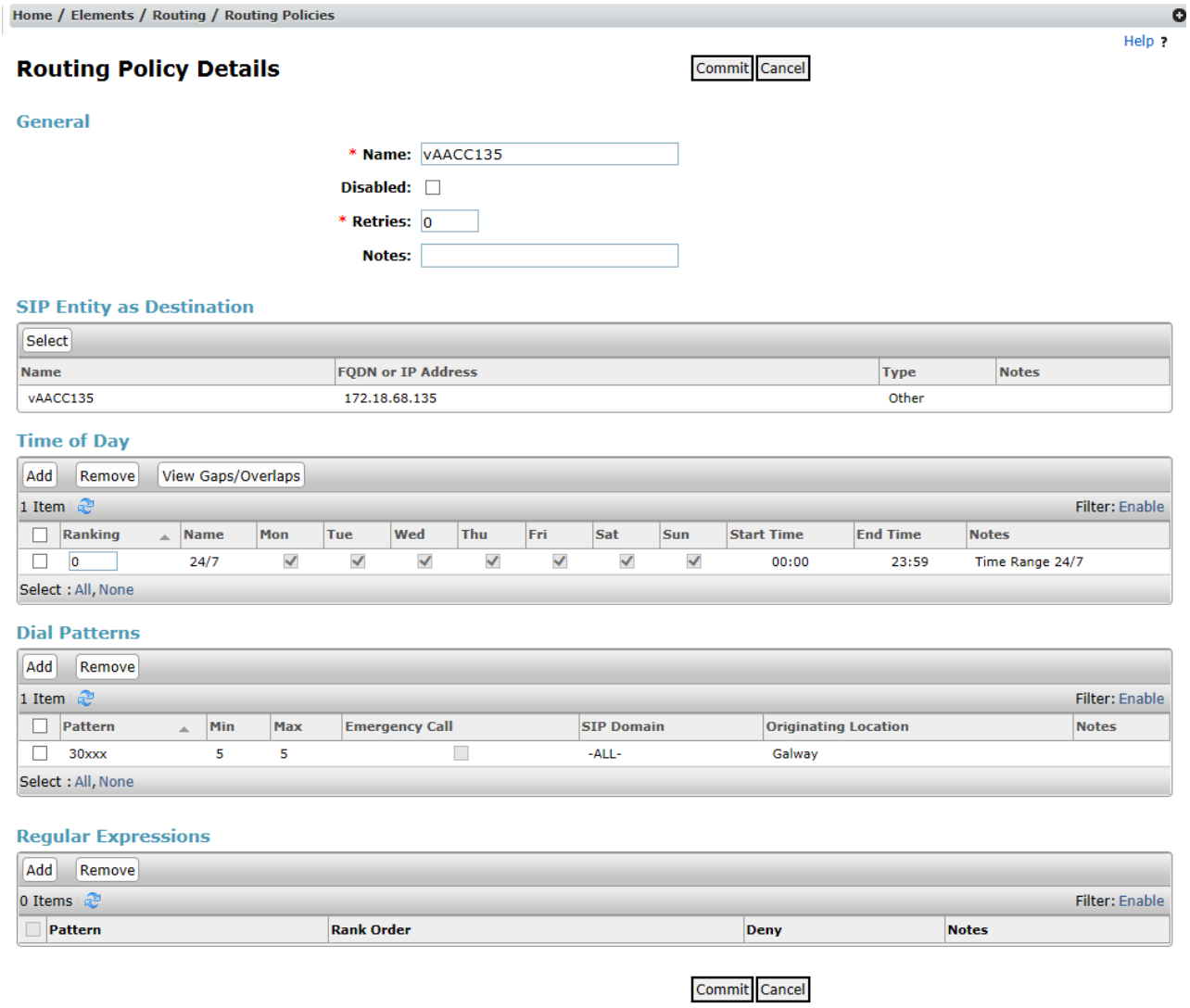
   The Routing Policy Details screen is displayed.

3. In the **General** section, in the **Name** box, type the name for the Routing Policy.

   Avaya recommends that you type a descriptive name for your Routing Policy.
4. In the **Notes** box, type your notes about this Routing Policy.
5. In the **SIP Entities as Destination** section, click **Select**.
6. From the list of SIP Entities, select the SIP Entity for your Communication Manager, click **Select**.
7. If you need to associate the Time of Day routing parameters with this Routing Policy, click **Add** from the **Time of Day** section.
8. Select the Time of Day patterns that you want to associate with this routing pattern and click **Select**.
9. Click **Commit**.

Example

The routing policy from the Session Managers to Communication Manager.



Creating a dial pattern to route calls to Communication Manager

About this task

Create a dial pattern using the Session Manager to Communication Manager Routing Policy. Session Manager uses this dial pattern to route calls to Communication Manager.

A dial pattern specifies which routing policy or routing policies are used to route a call based on the digits dialed by a user which match that pattern. The originating location of the call and the domain in the request-URI also determine how the call gets routed.

A Dial Pattern specifies a set of criteria and a set of Routing Policies for routing calls that match the criteria. The criteria include the called party number and SIP domain in the Request-URI, and the Location from which the call originated. For example, if a call arrives at Session Manager and matches a certain Dial Pattern, then Session Manager selects one of the Routing Policies specified in the Dial Pattern. The selected Routing Policy in turn specifies the SIP Entity to which the call is to be routed.

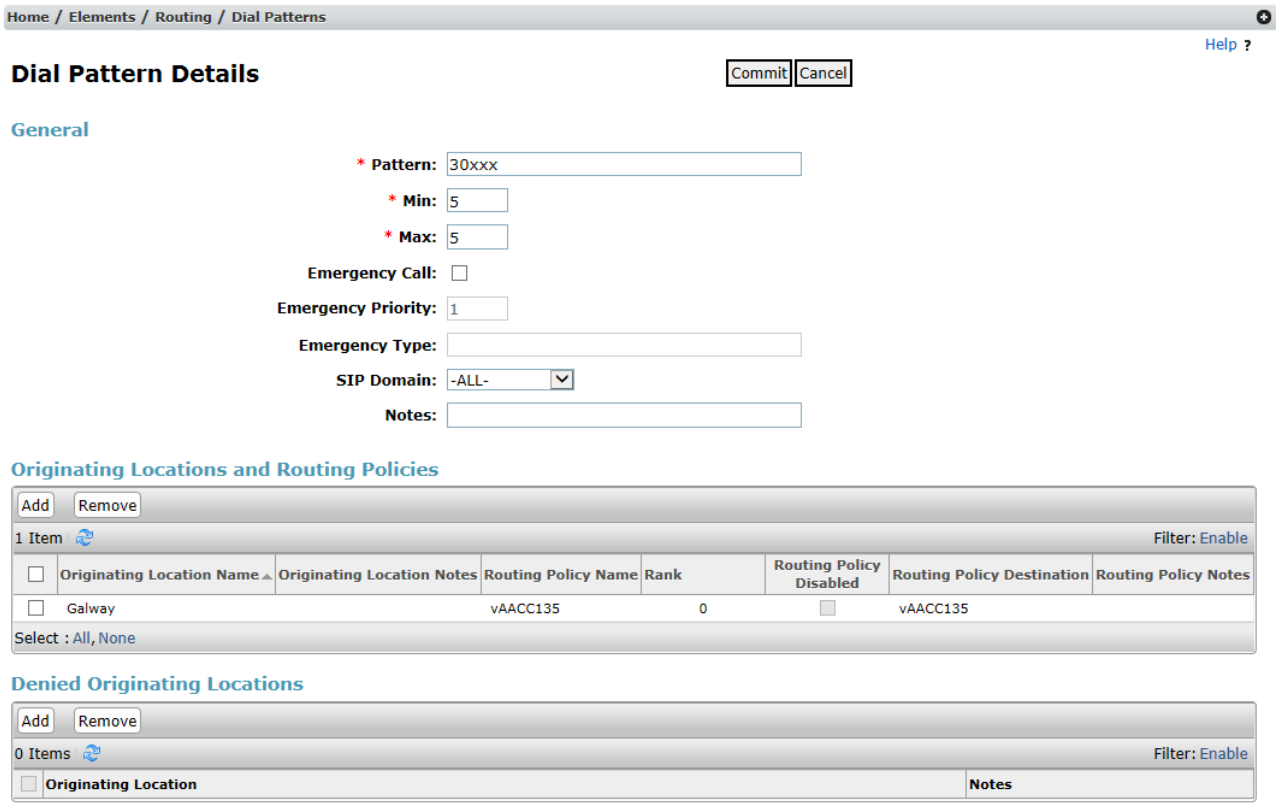
Dial Patterns are matched after ingress Adaptations have already been applied.

Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **Dial Patterns**.
2. Click **New**.
3. In the **Pattern** box, type the dial pattern for voice calls to Communication Manager.
4. In the **Min** box, type the minimum number of digits from the dial pattern to match.
5. In the **Max** box, type the maximum number of digits from the dial pattern to match.
6. From **SIP Domain**, select the SIP domain for this dial pattern. You can select a specific domain, or all domains.
7. Under the **Originating Locations and Routing Policies** section, click **Add**.
8. Select the check box for the location.
9. From **Routing Policy Name**, select the Session Manager to Communication Manager Routing Policy.
10. From the **Routing Policy Destination**, select the Communication Manager SIP Entity.
11. Click **Select** to indicate that you have completed your selections.
12. Click **Commit**.

Example

Example of a dial pattern to route calls to Communication Manager.



Variable definitions

Variable	Value
Pattern	Dial pattern to match. The pattern can have between 1 and 36 characters.
Min	Minimum number of digits to be matched.
Max	Maximum number of digits to be matched.
Emergency Call	Indicate if it is an emergency call. **Note:** Some of the important constraints on the use of this feature are as follows: — Each location must be assigned to only one emergency dial number. — This emergency dial number must match the emergency dial number in the 96xx Deskphone settings file for all SIP phones in the identified location.

Table continues…

Variable	Value
SIP Domain	Domain for which you want to restrict the dial pattern.
Notes	Other details that you wish to add.
Select check box	Use this check box to select and use the digit conversion for the incoming calls.
Location Name	Name of the location to be associated to the dial pattern.
Location Notes	Notes about the selected location.
Routing Policy Name	Name of the routing policy to be associated to the dial pattern.
Routing Policy Disabled	Name of the disabled routing policy.
Routing Policy Destination	Destination of the routing policy.
Routing Policy Notes	Any other notes about the routing policy that you wish to add.

Creating a SIP Entity for the Contact Center Manager Server

About this task

Create a SIP Entity for the Contact Center Manager Server. A SIP Entity represents a SIP network element.

Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** box, type the name of the Contact Center Manager Server SIP Entity.

   Avaya recommends that you type a descriptive name for your Contact Center Manager Server SIP entity.
4. In the **FQDN or IP address** box, type the IP address of the Contact Center Manager Server.
5. From the **Type** list, select **Other**.
6. If you need to specify an Adaptation Module for the Contact Center Manager Server SIP entity, from the **Adaptation** list, select an adaptation value.
7. In the **Location** box, select the location for this Session Manager.
8. In the **Credential name** box, enter a regular expression string.

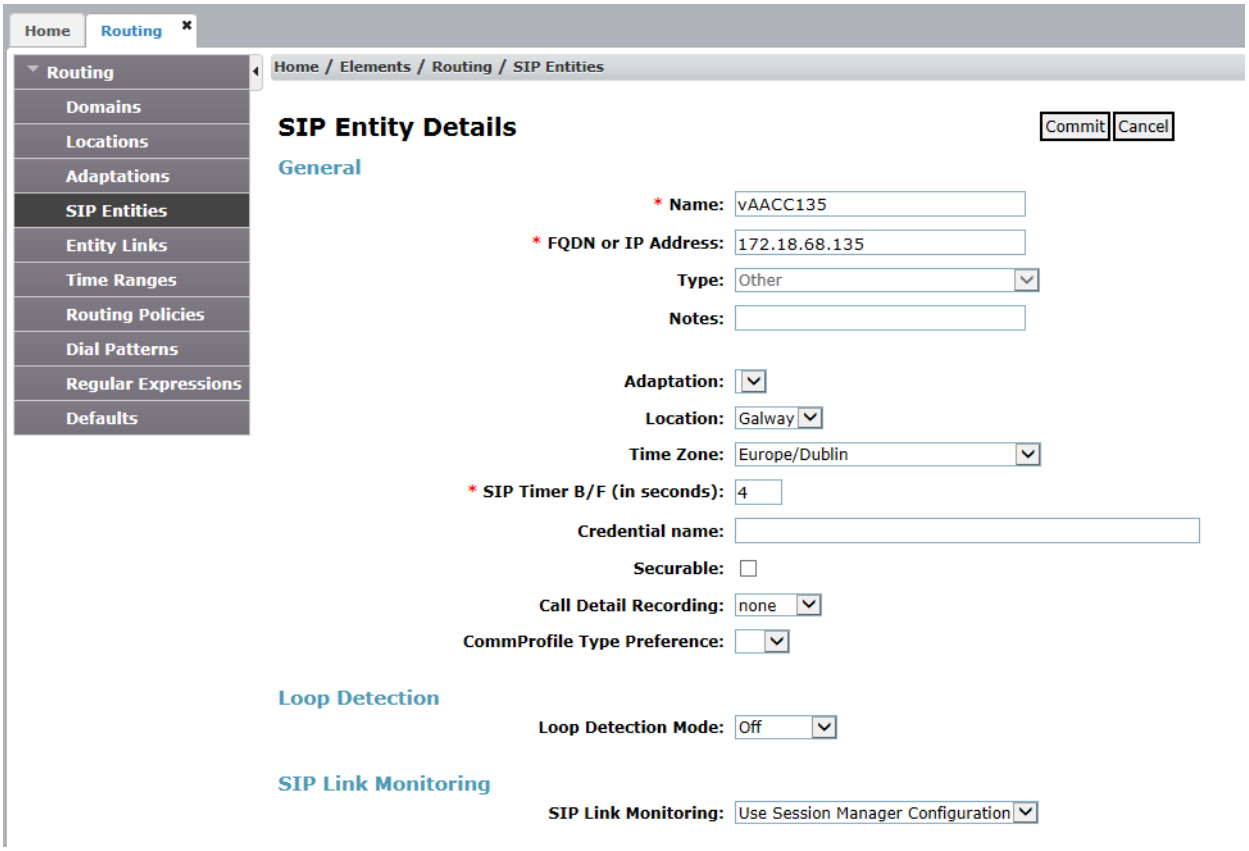
The **Credential name** is used for TLS connection validation by searching for this string in the SIP entity identity certificate.

9. From the **SIP Link Monitoring** list, select one of the following:
   - Use Session Manager Configuration - Use the settings under **Session Manager – Session Manager Administration**.
   - Link Monitoring Enabled - Enables link monitoring on this SIP entity.
   - Link Monitoring Disabled - Link monitoring is turned off for this SIP entity.
10. If you need to specify the port parameters, under **Port**, click **Add**.

    When Session Manager receives a request where the host-part of the request-URI is the IP address of the Session Manager, it associates one of the administered domains with the port on which the request was received.
11. Enter the necessary **Port** and **Protocol** parameters.
12. Click **Commit**.

Example

Example of a SIP Entity for a Contact Center Manager Server.



Variable definitions

Variable	Value
Name	SIP entity name. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the Avaya Aura® Contact Center SIP entity. If your Avaya Aura® Contact Center supports High Availability (HA) then the IP address for the Avaya Aura® Contact Center SIP Entity is the Contact Center Manager Server HA cluster IP address. If your Avaya Aura® Contact Center does not support High Availability (HA) then the IP address for the Avaya Aura® Contact Center SIP Entity is the Contact Center Manager Server IP Address.
Type	SIP entity type, such as a Other.
Notes	Additional notes about the SIP entity.
Adaptation	Adaptation to be used for the SIP entity. Select from already defined adaptations.
Location	SIP entity location. Select from previously defined locations.
Outbound Proxy	Outbound proxy if the entity type is Session Manager, and you wish to specify a proxy.
Time Zone	Time zone for the SIP entity.
Override Port & Transport with DNS SRV	Specify if you wish to use DNS routing. SIP uses DNS procedures to allow a client to resolve a SIP URI into the IP address, port, and transport protocol of the next hop to contact. It also uses DNS routing to allow a server to send a response to a backup client if the primary client fails.
SIP Timer B/F (in seconds)	Amount of time the Session Manager waits for a response from the SIP entity.
Credential name	Enter a regular expression string in the Credential name. Credential name is used for TLS connection validation by searching this string in the SIP entity identity certificate.
Call Detail Recording	Select or clear the check box to turn SIP monitoring on or off.
Proactive cycle time (Seconds)	Enter a value between 120 and 9000 seconds. The default is 900. This specifies how often the entity is monitored when the link to the entity is up or active.

Table continues…

Variable	Value
Reactive cycle time (Seconds)	Enter a value between 30 and 900 seconds. The default is 120. This specifies how often the entity is monitored when a link to the entity is down or inactive.
Number of retries	Enter a value between 0 and 15. The default is 1. This specifies the number of times Session Manager tries to ping or reach the SIP entity before marking it as down or unavailable.
Port	Add a listening port for the SIP entity.
Protocol	Protocol that the SIP entity uses.
SIP Domain	The domain of the SIP entity.
Notes	Additional notes about the port and port parameters.

Creating a SIP Entity Link from the first Session Manager to the Avaya Aura® Contact Center

About this task

Entity Links define the SIP trunk parameters and trust relationship between Session Manager instances and other SIP Entities in the solution.

Create a SIP entity link from the first Session Manager to the Avaya Aura® Contact Center. Session Manager enables you to create an entity link between the Session Manager and any other administered SIP entity. You must configure an entity link between a Session Manager and any entity that you have administered if you want Session Manager to be able to send or receive messages from that entity directly. To be able to communicate with other SIP entities, each Session Manager instance must know the port and the transport protocol of its entity link to these SIP entities in the network.

Procedure

1. On the System Manager console, select **Routing** > **Entity Links**.
2. Click **New**.
3. In the **Name** box, type the name for this SIP Entity Link.
4. Under **SIP Entity 1**, select the required Session Manager SIP entity from the drop-down list and provide the required port number.

   SIP entity 1 must always be a Session Manager instance.

   The default port for TCP is 5060.
5. Under **SIP Entity 2**, select the required Contact Center Manager Server SIP entity from the drop-down list and provide the required port number.

The port number is the port on which you have configured Contact Center Manager Server to receive requests for the specified transport protocol. By default this is port 5060.

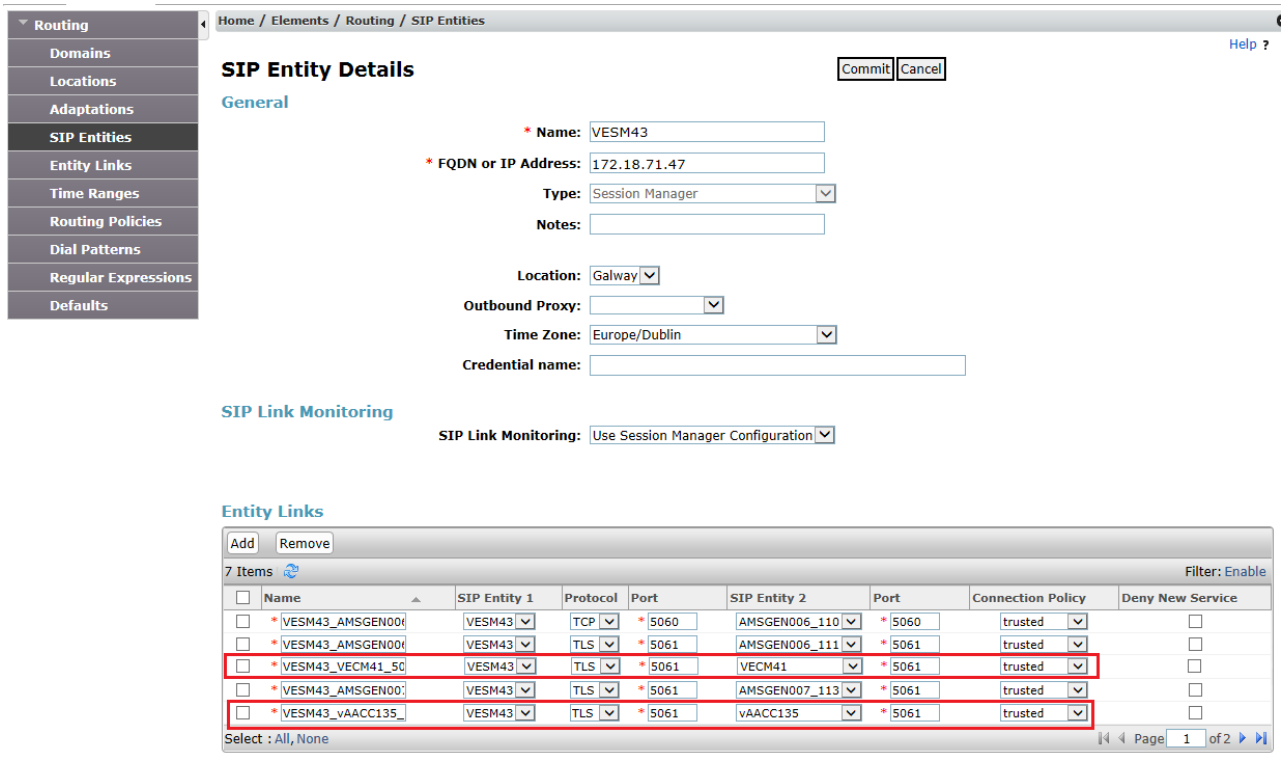
6. From the **Connection Policy** list, select **Trusted HA**.

   Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.

7. Click **Commit**.

Example

Avaya Aura® Session Manager SIP entity showing SIP Entity links to Avaya Aura® Contact Center and Avaya Aura® Communication Manager.



Creating a SIP Entity Link from the second Session Manager to the Avaya Aura® Contact Center

About this task

Create a SIP entity link from the second Session Manager to the Avaya Aura® Contact Center. Session Manager enables you to create an entity link between the Session Manager and any other administered SIP entity. You must configure an entity link between a Session Manager and any entity that you have administered if you want Session Manager to be able to send or receive messages from that entity directly. To be able to communicate with other SIP entities, each

Session Manager instance must know the port and the transport protocol of its entity link to these SIP entities in the network.

Procedure

1. On the System Manager console, select **Routing** > **Entity Links**.
2. Click **New**.
3. In the **Name** box, type the name for this SIP Entity Link.
4. Under **SIP Entity 1**, select the required Session Manager SIP entity from the drop-down list and provide the required port number.

   SIP entity 1 must always be a Session Manager instance.

   The default port for TCP is 5060.
5. Under **SIP Entity 2**, select the required Contact Center Manager Server SIP entity from the drop-down list and provide the required port number.

   The port number is the port on which you have configured Contact Center Manager Server to receive requests for the specified transport protocol. By default this is port 5060.
6. From the **Connection Policy** list, select **Trusted HA**.

   Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
7. Click **Commit**.

Creating a routing policy from the Session Manager to Avaya Aura® Contact Center

About this task

Create a routing policy from Session Manager to Avaya Aura® Contact Center. Routing policies can include the “Origination of the caller”, the “dialed digits” of the called party, the “domain” of the called party, and the actual time the call occurs. Optionally, instead of “dialed digits” of the called party and the “domain” of the called party a “regular expression” can be defined.

Depending on one or multiple of the inputs mentioned above a destination is where the call is routed to. Optionally, the destination can be qualified by “deny” which means that the call is not routed.

Session Manager uses the data configured in the Routing Policy to find the best match against the number (or address) of the called party.

Procedure

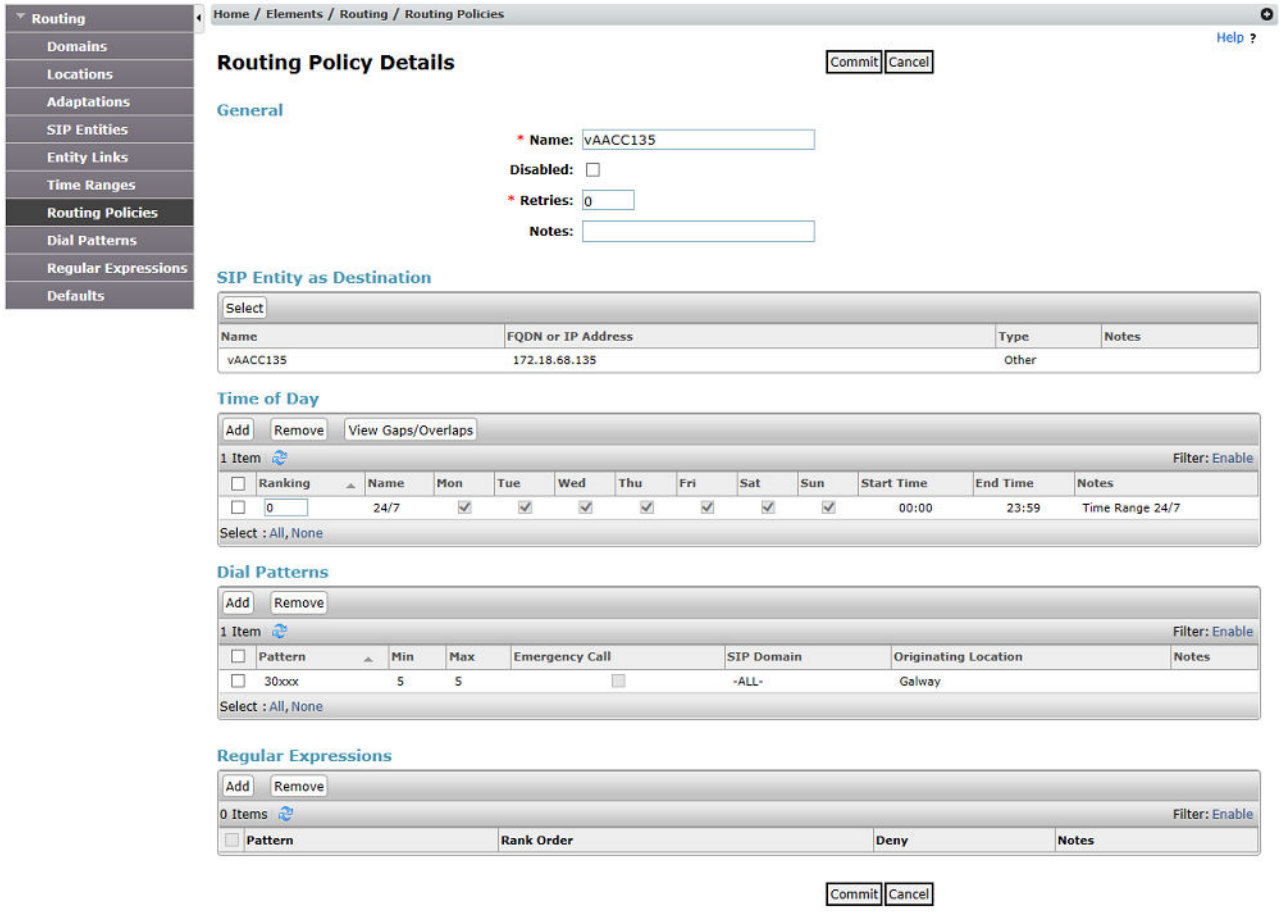
1. On the Avaya Aura® System Manager console, select **Routing** > **Routing Policies**.
2. Click **New**.

3. In the **General** section, in the **Name** box, type the name for the Routing Policy.

   Avaya recommends that you type a descriptive name for your Routing Policy.
4. In the **Notes** box, type your notes about this Routing Policy.
5. In the **SIP Entities as Destination** section, click **Select**.
6. From the list of SIP Entities, choose the SIP Entity for your Contact Center Manager Server, click **Select**.
7. If you need to associate the Time of Day routing parameters with this Routing Policy, click **Add** from the **Time of Day** section.
8. Select the Time of Day patterns that you want to associate with this routing pattern and click **Select**.
9. Click **Commit**.

Example

Example of creating a routing policy from Session Manager to Contact Center Manager Server.



Creating a dial pattern to route calls to the Contact Center

About this task

Create a dial pattern using the Session Manager to Avaya Aura® Contact Center Routing Policy. Session Manager uses this dial pattern to route calls to the contact center for processing.

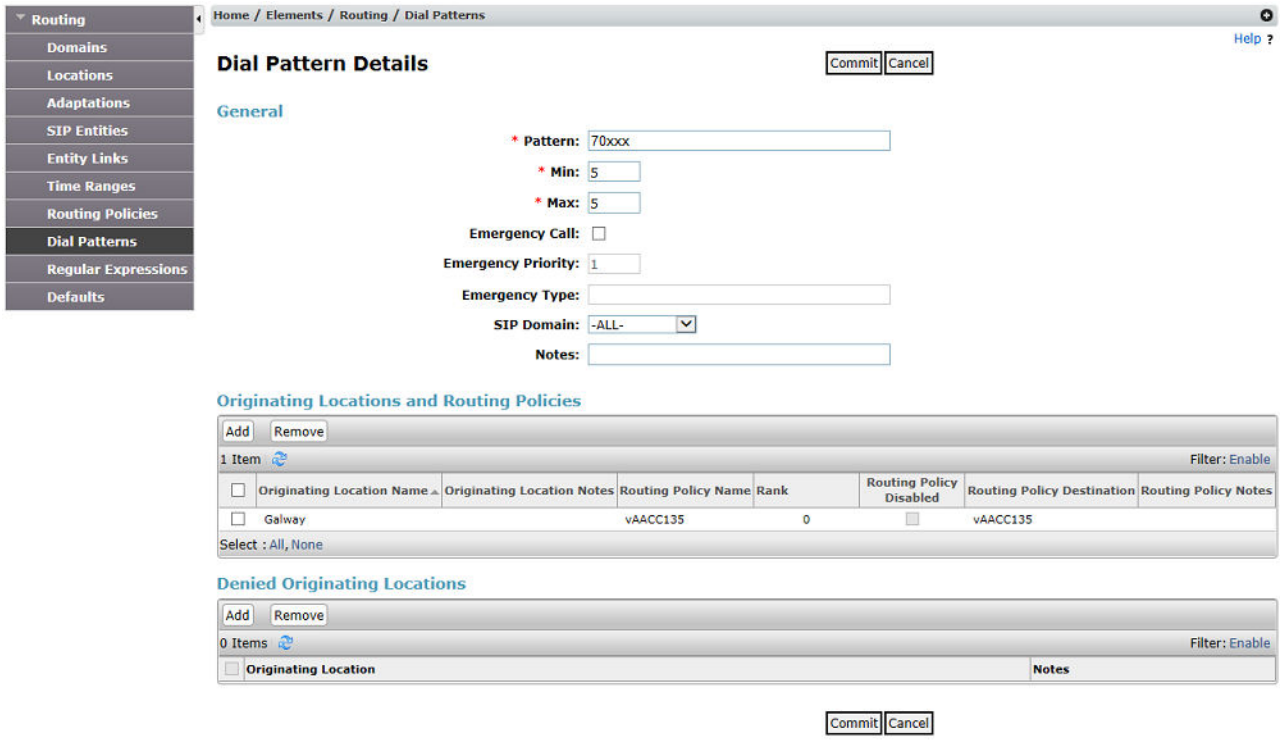
A dial pattern specifies which routing policy or routing policies are used to route a call based on the digits dialed by a user which match that pattern. The originating location of the call and the domain in the request-URI also determine how the call gets routed.

Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **Dial Patterns**.
2. Click **New**.
3. In the **Pattern** box, type the dial pattern for voice calls to the contact center.
4. In the **Min** box, type the minimum number of digits from the dial pattern to match.
5. In the **Max** box, type the maximum number of digits from the dial pattern to match.
6. From **SIP Domain**, select the SIP domain for this dial pattern. You can select a specific domain, or all domains.
7. Under the **Originating Locations and Routing Policies** section, click **Add**.
8. Select the check box for the location.
9. From **Routing Policy Name**, select the Session Manager to Contact Center Manager Server Routing Policy.
10. From the **Routing Policy Destination**, select the Contact Center Manager Server SIP Entity.
11. Click **Select** to indicate that you have completed your selections.
12. Click **Commit**.

Example

Example of creating a dial pattern using the Session Manager to Contact Center Manager Server routing policy.



Variable definitions

Variable	Value
Pattern	Dial pattern to match. The pattern can have between 1 and 36 characters.
Min	Minimum number of digits to be matched.
Max	Maximum number of digits to be matched.
Emergency Call	Indicate if it is an emergency call. **Note:** Some of the important constraints on the use of this feature are as follows: — Each location must be assigned to only one emergency dial number. — This emergency dial number must match the emergency dial number in the 96xx Deskphone settings file for all SIP phones in the identified location.
SIP Domain	Domain for which you want to restrict the dial pattern.

Table continues…

Variable	Value
Notes	Other details that you wish to add.
Select check box	Use this check box to select and use the digit conversion for the incoming calls.
Location Name	Name of the location to be associated to the dial pattern.
Location Notes	Notes about the selected location.
Routing Policy Name	Name of the routing policy to be associated to the dial pattern.
Routing Policy Disabled	Name of the disabled routing policy.
Routing Policy Destination	Destination of the routing policy.
Routing Policy Notes	Any other notes about the routing policy that you wish to add.

Chapter 7: Application Enablement Services configuration

Avaya Aura® Application Enablement Services (AES) is a set of enhanced telephony APIs, protocols, and Web services. These applications support access to the call processing, media, and administrative features available in Communication Manager. AES enables off-the-shelf and custom integration with communications applications such as Avaya Aura® Contact Center.

The Avaya Device, Media, and Call Control (DMCC) APIs provided by Application Enablement Services enable applications such as Contact Center to access the physical device, media, and basic third-party call control capabilities of Communication Manager.

The AES server uses Transport Layer Security (TLS) communication channels for the SIP CTI connection with Avaya Aura® Contact Center. TLS is a public key encryption protocol that helps secure a communications channel from danger or loss, and thus helps provide privacy and safety. TLS uses certificates to manage the public and private encryption keys.

You must use server and root certificates for the secure TLS link between Contact Center and the Application Enablement Services server. To use certificates signed by a CA, create a new Security Store on Contact Center.

This section describes how to configure Avaya Aura® Application Enablement Services for use with Contact Center.

Prerequisites

- Read the *Avaya Aura® Unified Communications platform Release Notes*.
- Ensure that your Avaya Aura® Unified Communications platform meets the minimum template requirements for integration with Contact Center.
- Ensure Avaya Aura® Application Enablement Services and Contact Center servers can communicate with each other by name. Ensure that they can ping each other.

Accessing the AES server management console

About this task

You can log on to AES directly or you can log on using the System Platform.

Procedure

1. Start a Web browser.
2. In the **Address** box, type the following URL: `https://<AES_IPaddress>`, where *<AES_IPaddress>* is the IP address for the Application Enablement Services server. Skip to step 3.

   OR

   On the System Platform Virtual Machine Management, in the virtual machine list, click the wrench or spanner icon to the left of the AES server.

   A welcome page appears.
3. Click **Continue To Login**.

   A Logon dialog box appears.
4. In the **Username** box, type your user name.

   The default user name is craft.
5. In the **Password** box, type your password.

   The default password is craft01. Avaya recommends that you change the default password after your first login. Passwords must be at least six characters. Avaya recommends using only alphanumeric characters.
6. Click **Login**.

   An Application Enablement Services Management Console appears.

Procedure job aid

The Avaya Application Services Management Console is a set of applications designed to simplify system administration, provisioning, and network management, including fault and performance management.

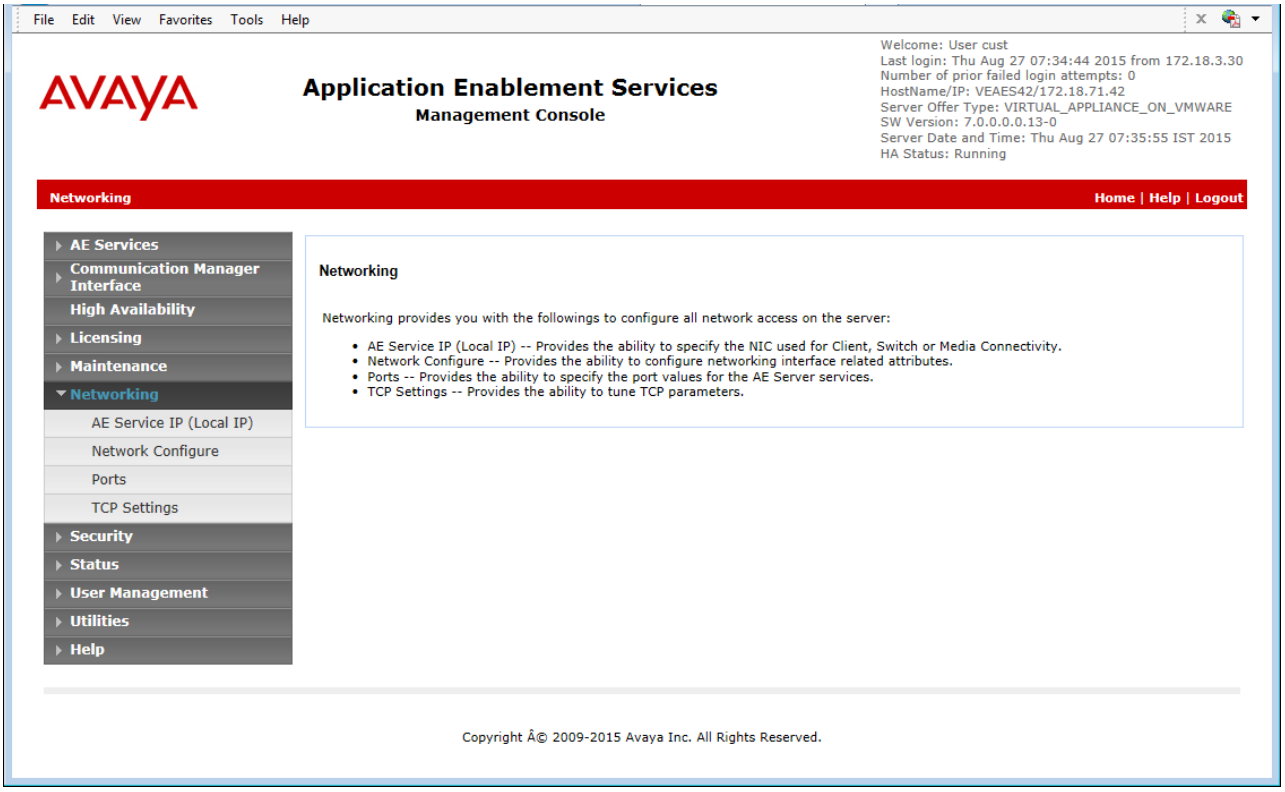


Figure 12: Example of the Application Enablement Services Management console

Adding Communication Manager switch connection

About this task

Add the Communication Manager switch connection to the Application Enablement Services (AES) to enable communication between them.

Procedure

1. In the left pane of the AES management console, click **Communication Manager Interface**.
2. Select **Switch Connections**.
3. Under **Switch Connections**, type the host name of your Communication Manager.

   The Communication Manager host name is case-sensitive.
4. Click **Add Connection**.
5. In the **Switch Password** box, type the Communication Manager switch password.

The default password is AESPASSWORD1. This password must match the password entered when configuring IP Services. For more information, see Configuring IP services for Application Enablement Services on page 53.

6. In the **Confirm Switch Password** box, type the Communication Manager switch password again.
7. In the **Msg Period** box, accept the default (30 minutes).
8. Select **Processor Ethernet**.

   Select **Processor Ethernet** if the AE Services connects to the Processor Ethernet of the Communication Manager.
9. Click **Apply**.

   The new Communication Manager switch connection is added to the list of switch connections.

Adding Communication Manager switch connection CLAN IP

Before you begin

- Add the Communication Manager switch connection, see Adding Communication Manager switch connection on page 103.

About this task

Add the switch connection CLAN IP so Application Enablement Services (AES) can communicate with the Communication Manager. After you add a switch connection, you must associate the switch connection name with a CLAN host name or IP address. Use this procedure when you are setting up a switch connection with a Communication Manager media server that uses a CLAN connection to AES.

Procedure

1. In the left pane of the AES management console, click **Communication Manager Interface**.
2. Select **Switch Connections**.
3. From the list of **Switch Connections**, identify the switch connection to your Communication Manager.
4. Under your switch connection, click **Edit PE/CLAN IPs**.
5. In the **Edit CLAN IPs** box, type the IP address of your Communication Manager server.
6. Click **Add Name or IP**.

Adding a CTI link to the Communication Manager

Before you begin

- Add the Communication Manager switch connection, see Adding Communication Manager switch connection on page 103.
- Associate the Communication Manager switch connection with a host IP address, see Adding Communication Manager switch connection CLAN IP on page 104.

About this task

Add a CTI (TSAPI) link between Application Enablement Services (AES) and the Communication Manager.

Procedure

1. In the left pane of the AES management console, click **AE Services**.
2. Select **TSAPI** > **TSAPI Links**.
3. Under **TSAPI Links**, click **Add Link**.
4. From the **Link** list, select the link number.
5. From the **Switch Connection** list, select the Communication Manager.
6. From the **Switch CTI Link Number** list, select the link number.

   The switch CTI link number must match that of the IP Services Server ID for AES as configured in Communication Manager.
7. From the **ASAI Link Version** list, select **5** or later.

   When using ASAI link version 7 or higher, enable the following Special Application on the Communication Manager: SA9124 - AACC Connected Information Enhancement. Before enabling the application, read *Avaya Aura™ Communication Manager Special Application Features* available at http://support.avaya.com.
8. From the **Security** list, select the default.
9. Click **Apply Changes**.

Procedure job aid

When adding a CTI (TSAPI) link between Application Enablement Services (AES) and the Communication Manager, the switch CTI link number on the AES must match that of the IP Services Server ID for AES as configured in Communication Manager.

Restarting the AES to Communication Manager connection

Before you begin

- Add the Communication Manager switch connection, see Adding Communication Manager switch connection on page 103.
- Associate the Communication Manager switch connection with a host IP address, see Adding Communication Manager switch connection CLAN IP on page 104.

About this task

Restart the TSAPI connection between Application Enablement Services (AES) and the Communication Manager. You must restart the TSAPI Service for changes to the CTI link between the AES and the Communication Manager to take effect.

Procedure

1. In the left pane of the AES management console, click **Maintenance**.
2. Select **Service Controller**.
3. Under the Service Controller list of services, select **TSAPI Service**.
4. Ensure none of the other services are selected.
5. Click **Restart Services**.

Enabling TR87 on the AES

About this task

Enable TR87 SIP CTI call control on the Avaya Aura® Application Enablement Services (AES) server. TR87 can be used over a SIP session to control and observe SIP user agents.

The TR87 interface on the AES is used by Avaya Aura® Contact Center to control and monitor agent stations on Avaya Aura® Communication Manager.

Procedure

1. In the left pane of the AES management console, click **Networking**.
2. Click **Ports**.
3. Scroll down to the DMCC Server section.
4. In the **DMCC** section, select the **Enabled** check box to the right of **TR/87 Port**.
5. Confirm that the **TR/87 Port** number is 4723.
6. Click **Apply Changes**.
7. Click **Apply**.

Procedure job aid

The AES Server uses port 4723 for TR/87. By default this port is disabled.

You must enable this port if you use the AES implementation for Contact Center. You can change the default port number of the TR/87 Port, if necessary.

For Avaya Aura® Contact Center to successfully use AES for TR/87 call control, the AES TR/87 port number must match the Contact Center Manager Server SIP CTI Proxy Server port number.

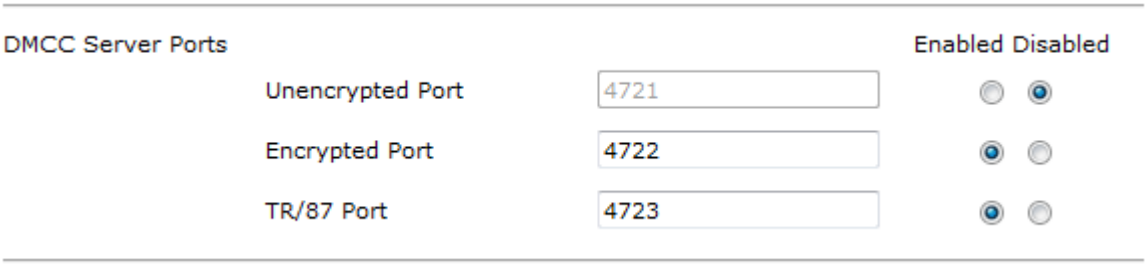


Figure 13: Example of AES TR/87 configuration

Configuring security on the AES

About this task

Configure AES security to require authorized host connections with the required client certification.

Procedure

1. In the left pane of the AES management console, click **Security**.
2. Click **Service Settings**.
3. Select the **TR/87** > **Require Trusted Host Entry** check box.
4. Click **Apply Changes**.

Importing a Certificate Authority root certificate into AES

Before you begin

- Export the CA root certificate from the Contact Center security store, and copy it to the Application Enablement Services (AES) server.

About this task

To communicate securely with the Contact Center, the AES sever must import the CA root certificate from the Contact Center security store. AES uses the root certificate to validate the Contact Center server certificate to initiate secure communications.

Procedure

1. In the left pane of the AES management console, click **Security**.
2. Click **Certificate Management** > **CA Trusted Certificates**.
3. Click **Import**.

   A Trusted Certificate Import page appears.
4. In the **Certificate Alias** box, type the certificate alias.
5. Click **Browse**, and select the root certificate you copied from the Contact Center server.
6. Click **Apply**.

   Contact Center displays a Certificate imported successfully message when the certificate is imported.
7. Click **Close**.

   The CA root certificate is added to the list of CA trusted certificates.
8. On the list of **CA Trusted Certificates**, locate your root certificate and confirm that the **Status** for it is **valid**.

Procedure job aid

The following screen shows an example of importing a Certificate Authority root certificate into AES as a Trusted Certificate.

AES must have the CA root certificate from the Contact Center security store to communicate securely with it using TLS. For more information about configuring Contact Center certificates, see *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications*.

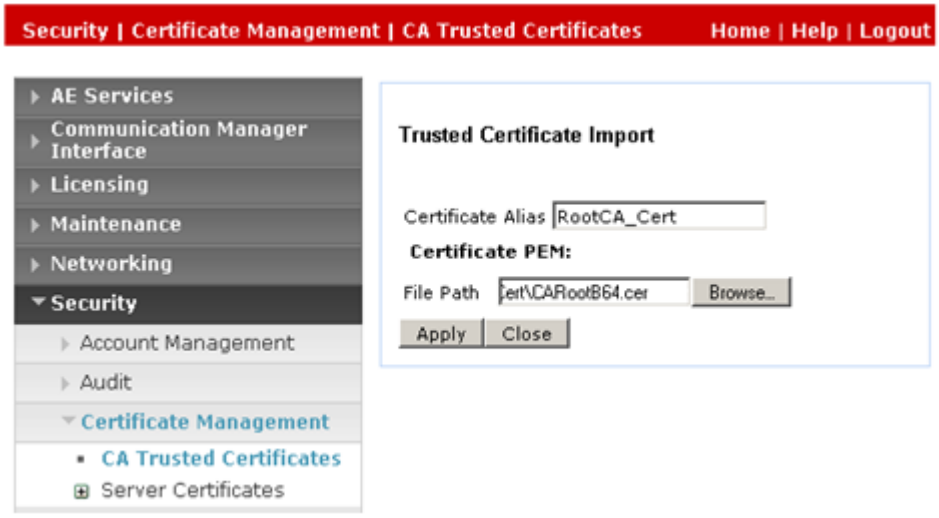


Figure 14: Example of importing a CA root certificate into AES

Generating an AES Certificate Signing Request

Before you begin

- Import the Contact Center root certificate into AES.

About this task

Create an AES Certificate Signing Request (CSR) to request a signed server certificate from your Certificate Authority.

Procedure

1. In the left pane of the AES management console, click **Security**.
2. Click **Certificate Management** > **Server Certificates**.
3. Click **Add**.

   AES displays the Add Server Certificate page.
4. From the **Certificate Alias** list, select **aesservices**.
5. In the **Password** box, type a certificate key password.
6. In the **Re-enter Password** box, re-type the certificate key password.
7. In the **Distinguished Name (DN)** box, type the FQDN of the AES server.
8. You must enter the Distinguished Name using X.509 attribute format.

Note:

The Common Name (CN) attribute must be the name of the AES server. Common Name is case-sensitive. For example, if the FQDN of your AES server is AESserver.DevLab3.com, then type “CN=AESserver,DN=DevLab3,DN=com”.

9. In the **Challenge Password** box, type a certificate request password.
10. In the **Re-enter Challenge Password** box, type the certificate request password again.
11. Click **Apply**.

    A Server Certificate Manual Enrollment Request page appears.
12. Copy all the text in the **Certificate Request PEM** box into a text file.

    This text is the Certificate Signing Request (CSR) text.

Next steps

After you perform this procedure, use the certificate signing request to get a certificate signed by a Certificate Authority. Contact your System Administrator for the preferred method of processing the certificate signing request file to obtain a signed certificate. Send the Certificate Signing Request file to a Certificate Authority and receive a signed server certificate and root certificate to import to the security store.

Procedure job aid

Copy the Certificate Signing Request (CSR) text and save it to a text file to request a certificate from your Certificate Authority. The CSR request is generated on the AES server using the Common Name (CN) of the AES server, so the signed server certificate that the CA provides is valid only on the AES server.

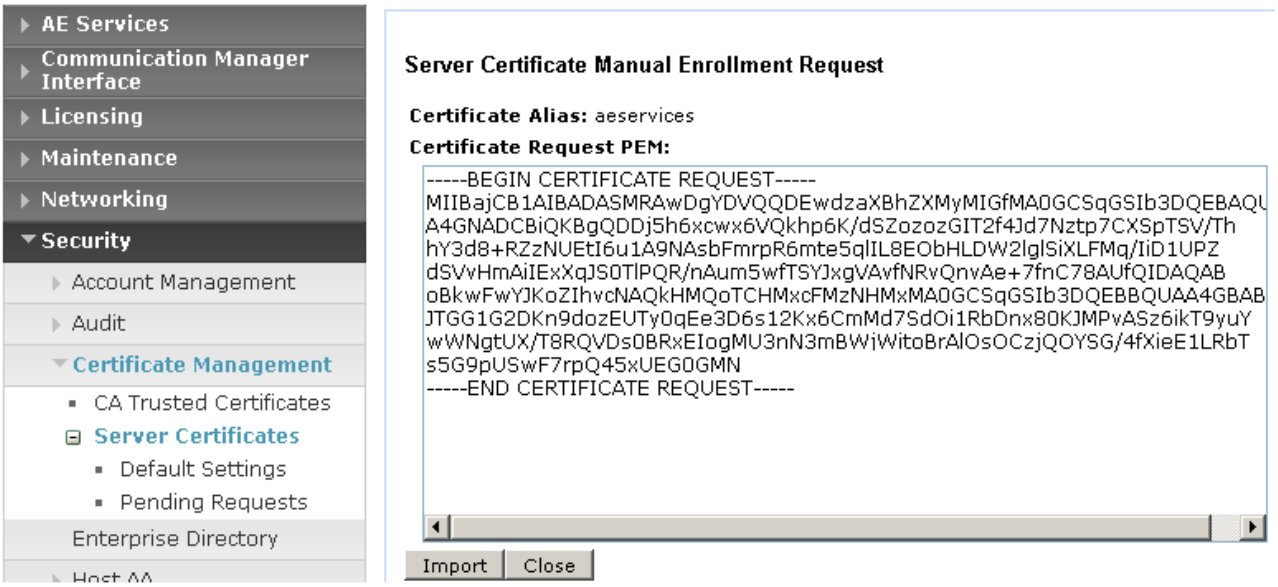


Figure 15: Example of Certificate Signing Request (CSR) text

Importing a signed certificate into AES

Before you begin

- Use the CSR file to obtain a Certificate Authority signed server certificate and root certificate.
- Copy the certificates to the Application Enablement Services server.

About this task

Import the signed server certificate into AES, so that AES can communicate securely with Contact Center using TLS for the SIP CTI connection.

Procedure

1. Log on to the AES Management Console.
2. Select **Security** > **Certificate Management** > **Server Certificates** > **Pending Requests**.
3. From the Pending Server Certificate Requests page, select the signed certificate you want to import and click **Manual Enroll**.
4. On the Server Certificate Manual Enrollment Request page, click **Import**.

   AES displays the Server Certificate Import page.
5. From the **Certificate Alias** list, select **aesservices**.
6. Select **Establish Chain of Trust**.
7. Click **Browse**, and select the signed certificate you downloaded from your Certificate Authority.

8. Click **Apply**.

   AES displays a Server Certificate Import - Certificate imported successfully message.

9. Click **Close**.

   The certificate is added to the Server certificates list.

10. On the list of **Server Certificates**, locate your server certificate and confirm that the **Status** for it is **valid**.

Procedure job aid

Import a signed certificate so AES can communicate securely.

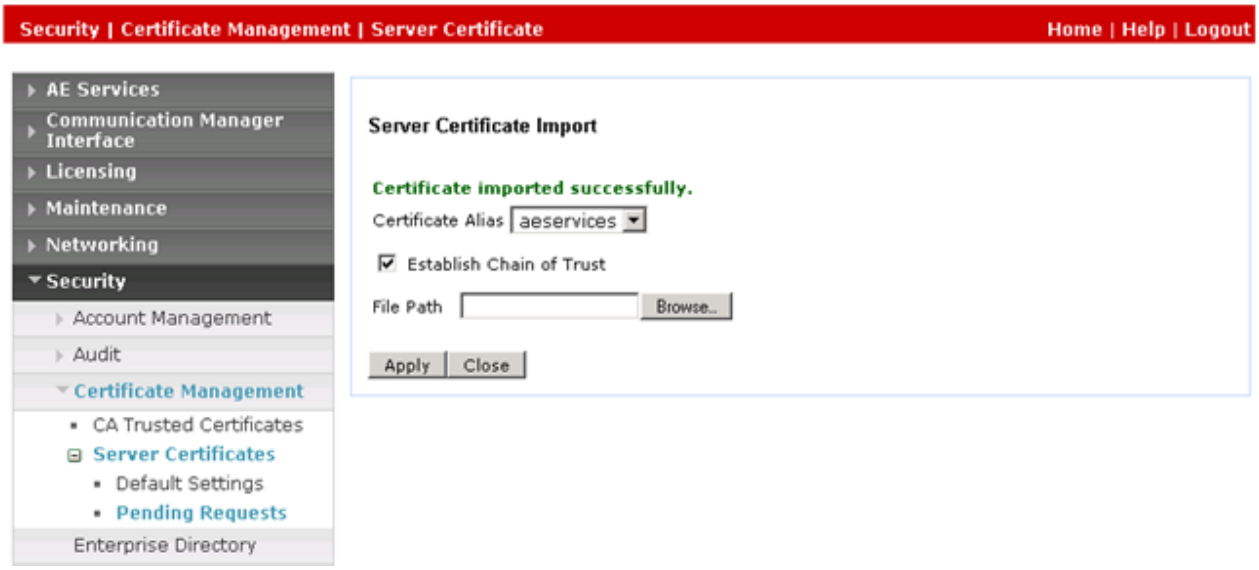


Figure 16: Example of importing a signed certificate into AES

After you import the signed server certificate, the AES can communicate securely using TLS for the SIP CTI connection.

Adding the Contact Center server as a trusted host on AES

About this task

Add the Avaya Aura® Contact Center (AACC) server as a trusted host on the Application Enablement Services (AES) server.

Note:

If you are using the Contact Center High Availability feature, you must add both the active AACC and the standby AACC servers as trusted hosts on AES.

Procedure

1. In the left pane of the AES management console, click **Security**.
2. Click **Host AA**.
3. Click **Trusted Hosts**.
4. Click **Add**.

   An Add Trusted host page appears.
5. In the **Certificate CN or SubAltName** box, type the FQDN name of the Contact Center server.

   Note:

   Certificate CN and SubAltName are case sensitive.
6. From the **Service Type** list, select **TR/87**.
7. From the **Authentication Policy** list, select **Not Required**.
8. From the **Authorization Policy** list, select **Unrestricted Host**.
9. Click **Apply Changes**.

   A confirmation page appears.
10. Click **Apply**.
11. If you are using the Contact Center High Availability feature, repeat this procedure to add the standby AACC server as a trusted host on AES.

Procedure job aid

When adding Contact Center Manager Server (CCMS) as a trusted host on the AES, the trusted Host DN setting on AES must match the CCMS full computer FQDN, as set in the CCMS Security Manager.

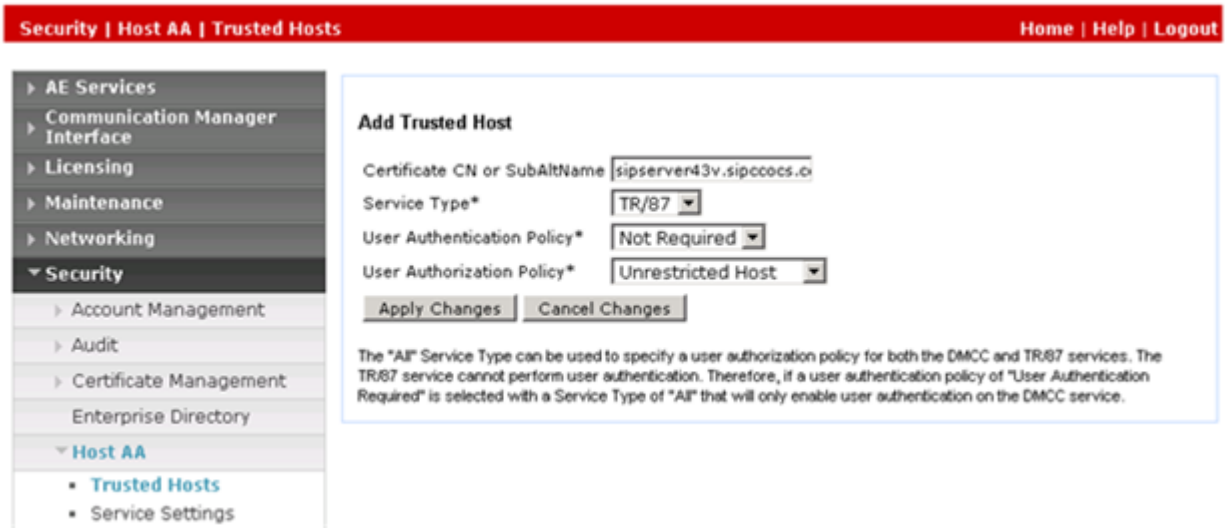


Figure 17: Example of adding the Contact Center Manager Server as a trusted host

Restarting the AES Linux server

About this task

Restart the Application Enablement Services (AES) Linux server. AES services are not available while the AES server is restarting.

Procedure

1. In the left pane of the AES management console, click **Maintenance**.
2. Click **Service Controller**.
3. Click **Restart Linux**, to restart the AES Linux server.
4. Click **Restart**.

Procedure job aid

Some configuration changes to the AES server take effect only when the AES server starts; therefore, you must restart the AES to apply configuration changes.

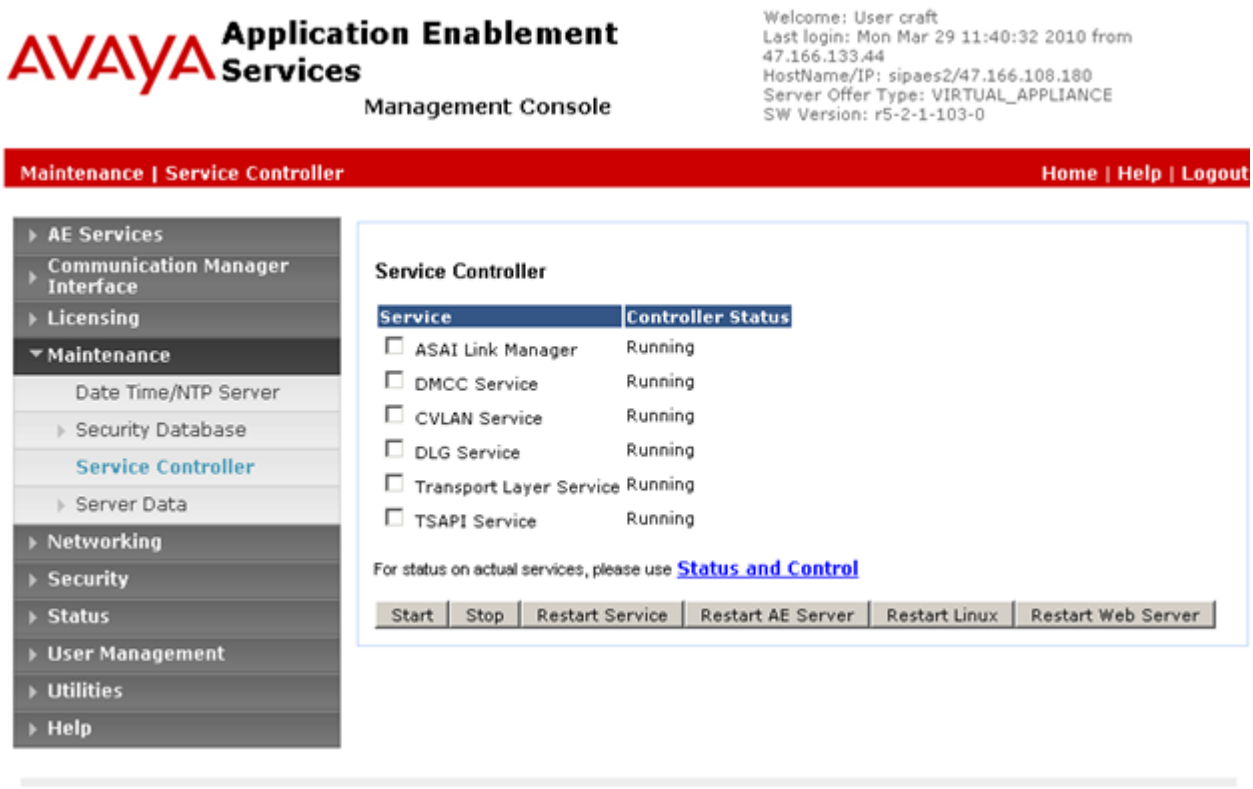


Figure 18: Example of restarting the AES Linux server

Verifying the AES services are running

About this task

Some configuration changes made to the AES server only take effect when the AES server starts, so it is sometimes necessary to restart the AES to apply configuration changes. If you make configuration changes that require the AES server to be restarted, then check that those changes are applied when the AES server starts up after the restart.

Procedure

1. In the left pane of the AES management console, click **AE Services**.
2. Ensure the **DMCC Service** has an **ONLINE** status and a **Running** State.
3. Ensure the **TSAPI Service** has an **ONLINE** status and a **Running** State.

Procedure job aid

To ensure that you have made valid configuration changes and that they are applied, verify that the core Application Enablement Services started after you restart the system.

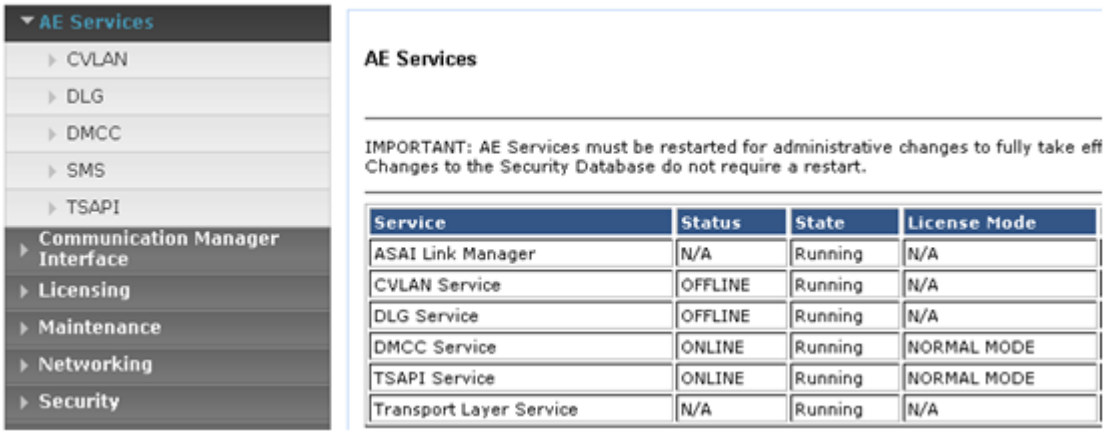


Figure 19: Example of verifying the AES services after a restart

Verifying the AES connection to Communication Manager switch

About this task

After starting the Application Enablement Services (AES) server, confirm that it is still communicating with the Communication Manager.

Procedure

1. In the left pane of the AES management console, click **Status**.
2. Click **Status and Control**.
3. Click **Switch Conn Summary**.
4. Ensure the **Switch Connections Summary** has a **Conn State** of **Talking**.

Procedure job aid

To ensure that you made valid configuration changes and that they are applied, verify that the Application Enablement Services are still communicating with the Communication Manager after a restart.

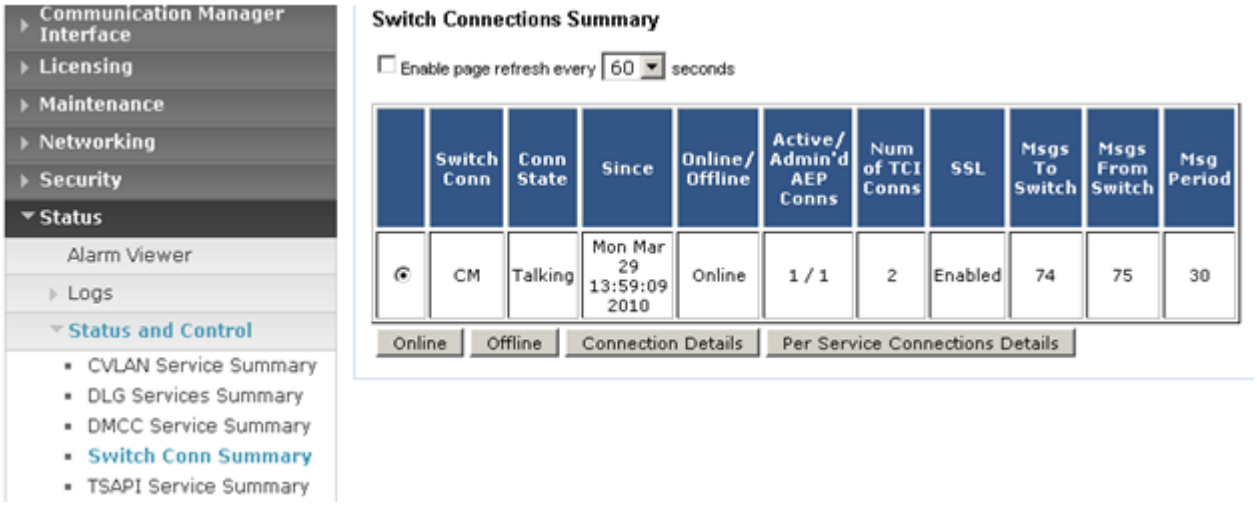


Figure 20: Example of verifying the AES connectivity with the Communication Manager after a restart

Verifying the AES TSAPI connection

About this task

After starting the AES server, confirm that it is still communicating with the Telephony Service API (TSAPI).

Procedure

1. In the left pane of the AES management console, click **Status**.
2. Click **Status and Control**.
3. Click **Switch Conn Summary**.
4. Ensure the **TSAPI Service Summary** has a **Conn State** of **Talking**.

Procedure job aid

To ensure that you made valid configuration changes and that they are applied, verify that the Application Enablement Services are still communicating with the Communication Manager after a restart.

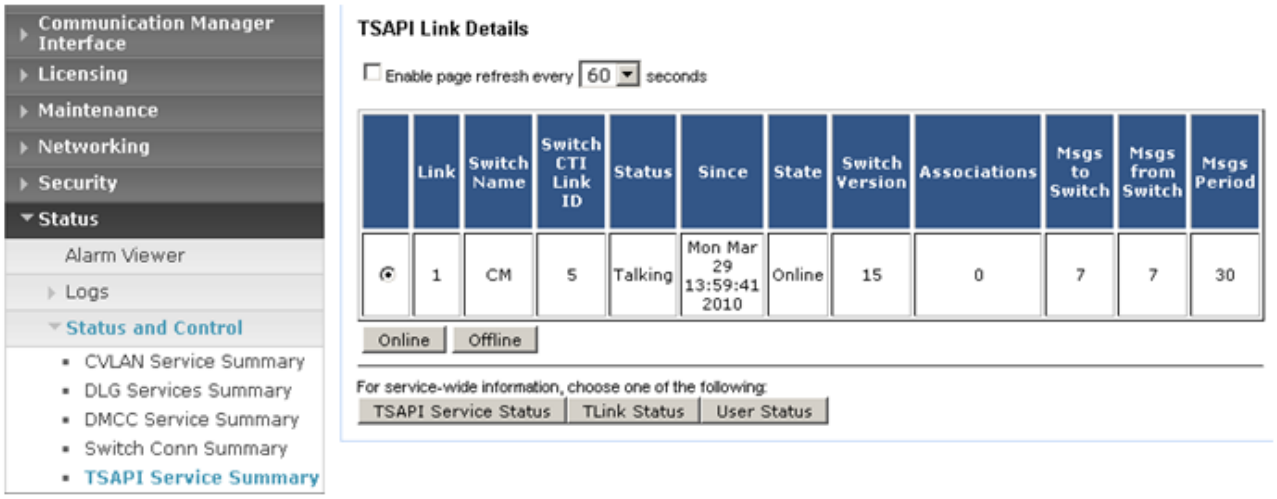


Figure 21: Example of verifying the AES connectivity with the Communication Manager after a restart

Debugging the AES server

About this task

After starting the AES server confirm that it is still communicating with the Telephony Service API (TSAPI).

Procedure

1. In the left pane of the AES management console, click **Status**.
2. Click **Logs** > **Error Logs**.

   The list of error logs appears on the right pane.
3. Select the file to view, scroll down, and click **view**.

   Copy all text and paste it into a text editor to view.

Procedure job aid

Use the AES error logs to debug AES issues.

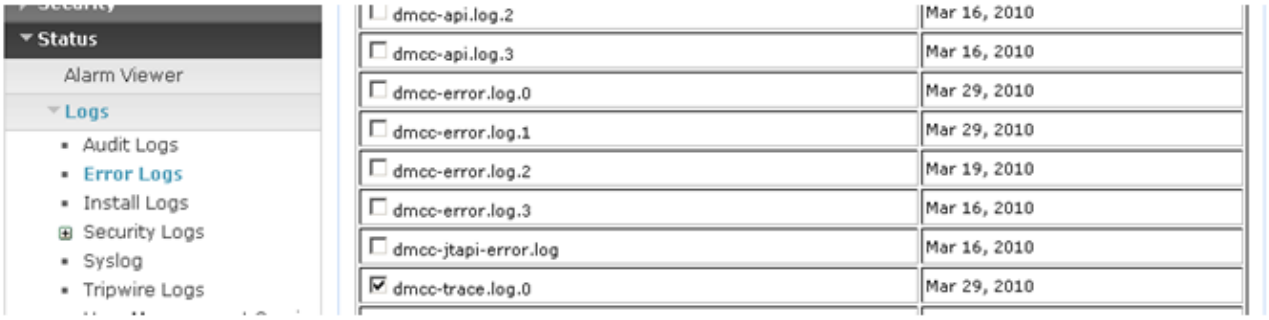


Figure 22: Example of AES Error Logs list

Confirming the AES and CCMS are communicating

Before you begin

- Enable TR87 SIP CTI, see Enabling TR87 on the AES on page 106.
- Configure security, see Configuring security on the AES on page 107.
- Import server and root certificates.
- Add CCMS as a trusted host, see Adding Contact Center Manager Server as a trusted host on AES on page 112.
- The Contact Center Manager Server (CCMS) is commissioned. For more information about commissioning CCMS for SIP, see *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications*.

About this task

Log on to the Application Enablement Services (AES) server using Secure Shell (SSH) and confirm that AES is communicating with the Contact Center Manager Server (CCMS) on port 4723. Also confirm that there is an established connection between the AES and CCMS. The AES server uses port 4723 to listen to the TR87 SIP CTI link between it and the CCMS.

Procedure

1. On the AES SSH console, enter `netstat -an | grep 4723`.

   The AES server console displays the network status of the AES.

2. Confirm that the link to your Contact Center Manager Server is established.
3. Confirm that the Application Enablement Services server is listening on port 4723.

Procedure job aid

The following is an example of using the Application Enablement Services Secure Shell to check the connection to the Contact Center Manager Server.

```
[craft@aes521svr01 ~]$ netstat -an | grep 4723
tcp 0 0 ::ffff:127.0.0.1:4723 :::* LISTEN
```

```
tcp 0 0 ::ffff:47.165.84.45: 4723 :::* LISTEN
tcp 0 0 ::ffff:47.165.84.45:4723 :ffff:47.165.84.163:65235  ESTABLISHED
```

In this example the AES IP address is 47.165.84.45 and the CCMS IP address 47.165.84.163. The AES server (47.165.84.45) is listening on port 4723. There is an ESTABLISHED link between the AES server (47.165.84.45) and CCMS (47.165.84.163).

Chapter 8: DNIS support using Session Manager configuration

Avaya Aura® Contact Center uses Dialed Number Identification Service (DNIS) to identify the phone number dialed by the incoming caller. Contact Center agents can receive calls from customers calling in on different DNISs and customize their response according to the DNIS number. Based on the DNIS, the contact center solution can direct contacts to a Route Point (CDN) and supply different treatments.

DNIS information is transported between SIP entities using the TO header information within each SIP INVITE message. Each SIP INVITE message is routed using the REQUEST URI header information. Initially, when a customer initiates a call, the REQUEST URI and the TO header are normally the same. If the incoming SIP INVITE message to Contact Center contains a REQUEST URI that differs to the TO header information, Contact Center deems the TO header address to contain the DNIS information for that call.

Avaya Aura® Session Manager serves as a central point for supporting SIP-based communication services in an enterprise. Session Manager applies any configured SIP header adaptations and digit conversions, and based on configured network Routing Policies, determines to where a call is routed next. Session Manager Adaptations are used to modify SIP headers and apply configured digit conversions for the purpose of inter-working with specific SIP Entities. You can use Digit Conversion Adaptations to change the digit strings in the destination REQUEST URI header of SIP messages sent to and received from SIP Entities.

To support DNIS in a solution with Avaya Aura® Contact Center, Avaya Aura® Communication Manager (CM), and Avaya Aura® Session Manager (SM):

- Route all DNIS numbers to the Session Manager.
- Typically, a call enters Session Manager with the REQUEST URI and TO header both containing the DNIS number.
- In the Session Manager Dial Plan, configure the DNIS numbers to route to one or more Avaya Aura® Contact Center Route Point.
- Before the call is routed to a Contact Center Route Point, use a Session Manager adaptation to change the destination REQUEST URI to the Route Point number.
- The call arrives at the Avaya Aura® Contact Center Route Point with REQUEST URI = Route Point, and the TO header = DNIS.
- Using Avaya Aura® Contact Center Orchestration Designer applications, treat the call using the DNIS number.

Example of DNIS support using Session Manager configuration

A customer dials phone number 2320740 to access a contact center solution. A second customer dials phone number 2320741 to access the same contact center solution.

A Session Manager Dial Pattern and Routing Policy combination routes all calls matching this (DNIS) number range “232074x” to Contact Center. As these calls leave Session Manager, a digit conversion Adaptation converts the 232074x number range into a Contact Center Route Point number, for example 2450740. Both customer phone calls are routed to the same Contact Center Route Point, even though the customers dialed different phone numbers.

Each customer call arrives at Avaya Aura® Contact Center with SIP REQUEST URI configured with the Route Point number, and the SIP TO header still containing the original customer DNIS number. A Contact Center Orchestration Designer application, associated with the 2450740 Route Point, can access the DNIS number used by each customer and distinguish between the numbers dialed. A single Contact Center Orchestration Designer application can process or treat each customer phone call based on the phone number the customer dialed.

The procedures, Route Point, and Dial Pattern in this section are based on this example DNIS configuration. You must complete all the procedures in this section in sequential order.

Creating a DNIS to Route Point Adaptation

About this task

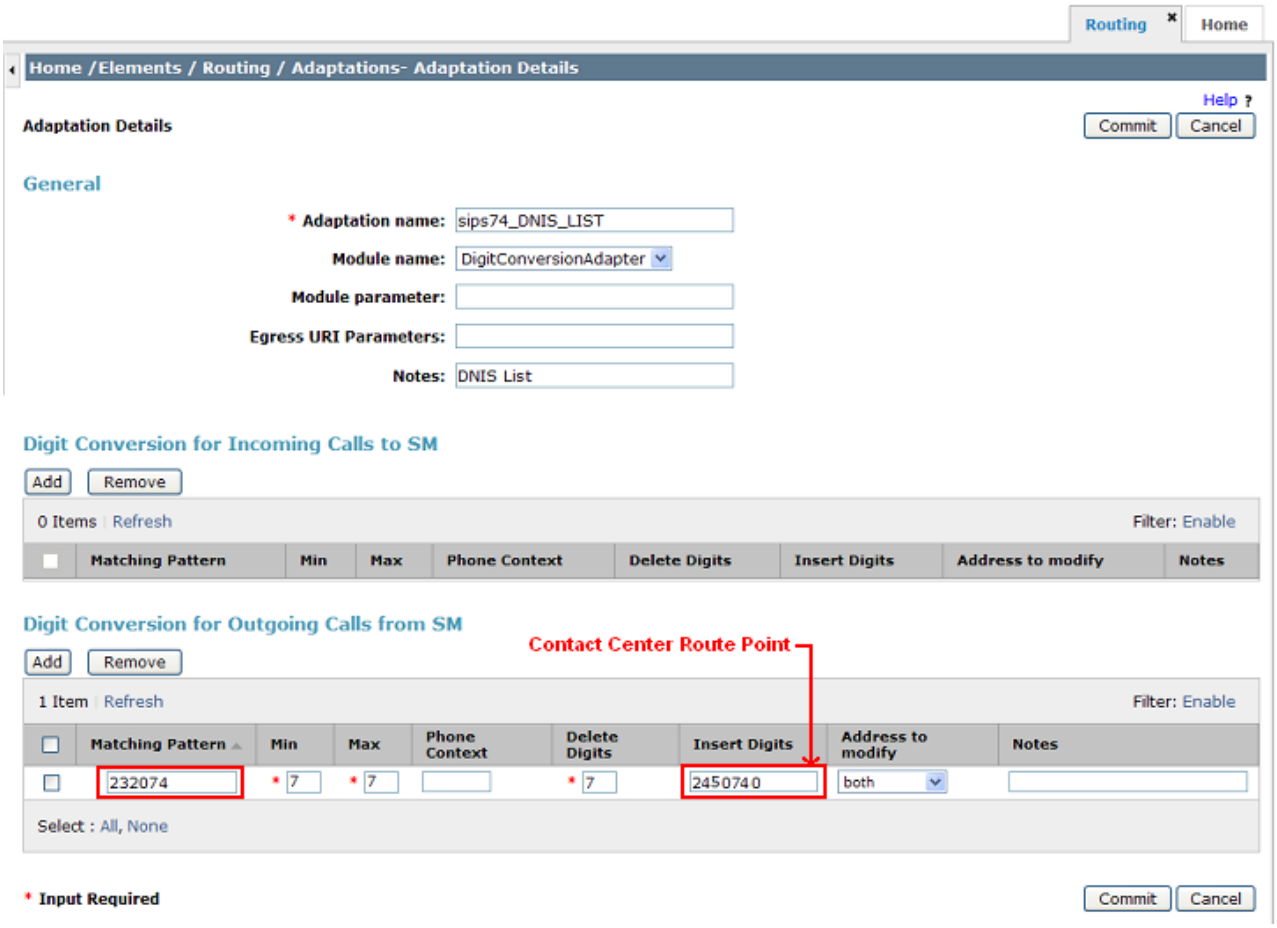
Create a Digit Conversion Adapter adaptation to convert a Dialed Number Identification Service (DNIS) number to an Avaya Aura® Contact Center Route Point number.

Procedure

1. On the System Manager console, select **Routing** > **Adaptation**.
2. In the **Adaptation Name** box, enter a descriptive name for the Adaptation.
3. In the **Module name** list, select or type **DigitConversionAdapter**.
4. Under **Digit Conversion for Outgoing Calls from SM**, click **Add**.
5. In the **Matching Pattern** box, type a DNIS number, or a number pattern for a range of DNIS numbers.
6. In the **Min** box, type the minimum number of digits.
7. In the **Max** box, type the maximum number of digits.
8. In the **Delete Digits** box, type the number of digits to replace.
9. In the **Insert Digits** box, type the Avaya Aura® Contact Center Route Point number.
10. In the **Notes** box, type a descriptive note about this adaptation.
11. Click **Commit**.

Example

Example of an adaptation to convert a Dialed Number Identification Service (DNIS) number to an Avaya Aura® Contact Center Route Point number. This sips74_DNIS_LIST example adaptation converts the DNIS number range 2320740 to 2320749 into the Avaya Aura® Contact Center Route Point number 2450740.



Configuring the Contact Center SIP Entity Adaptation

About this task

Configure the Contact Center Manager Server SIP Entity to use the Dialed Number Identification Service (DNIS) to Route Point adaptation.

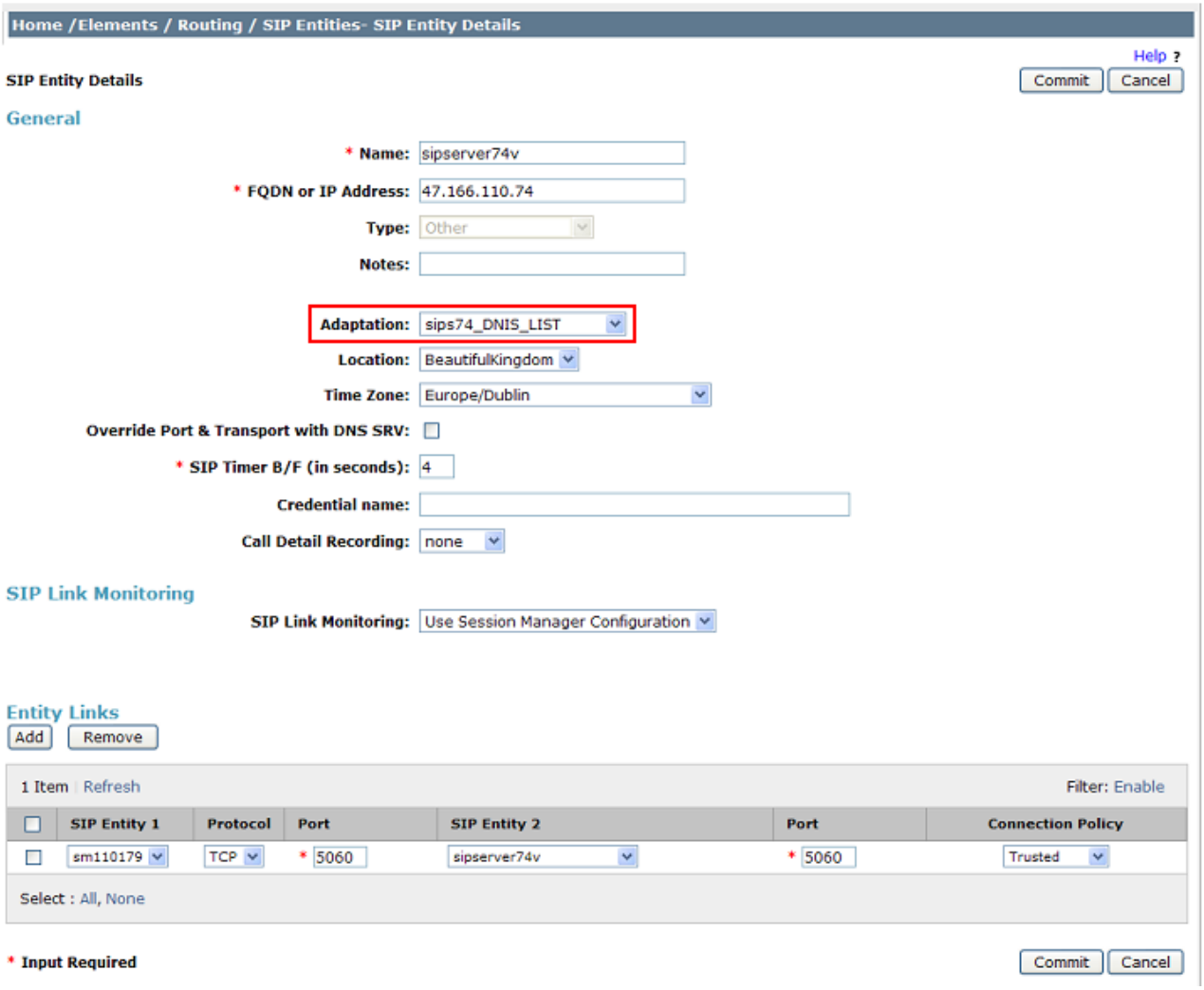
Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **SIP Entities**.
2. Select the Contact Center Manager Server SIP Entity.

3. For the Contact Center Manager Server SIP entity, from the **Adaptation** list, select the DNIS to Route Point adaptation.
4. Click **Commit**.

Example

Example of a Contact Center Manager Server SIP Entity using an Dialed Number Identification Service (DNIS) to Route Point adaptation.



Creating a routing policy from Session Manager to Contact Center

About this task

Create a routing policy from Session Manager to Avaya Aura® Contact Center. Routing policies can include the “Origination of the caller”, the “dialed digits” of the called party, the “domain” of the called party, and the actual time the call occurs. Optionally, instead of “dialed digits” of the called party and the “domain” of the called party a “regular expression” can be defined.

Depending on one or multiple of the inputs mentioned above a destination is where the call is routed to. Optionally, the destination can be qualified by “deny” which means that the call is not routed.

Session Manager uses the data configured in the Routing Policy to find the best match against the number (or address) of the called party.

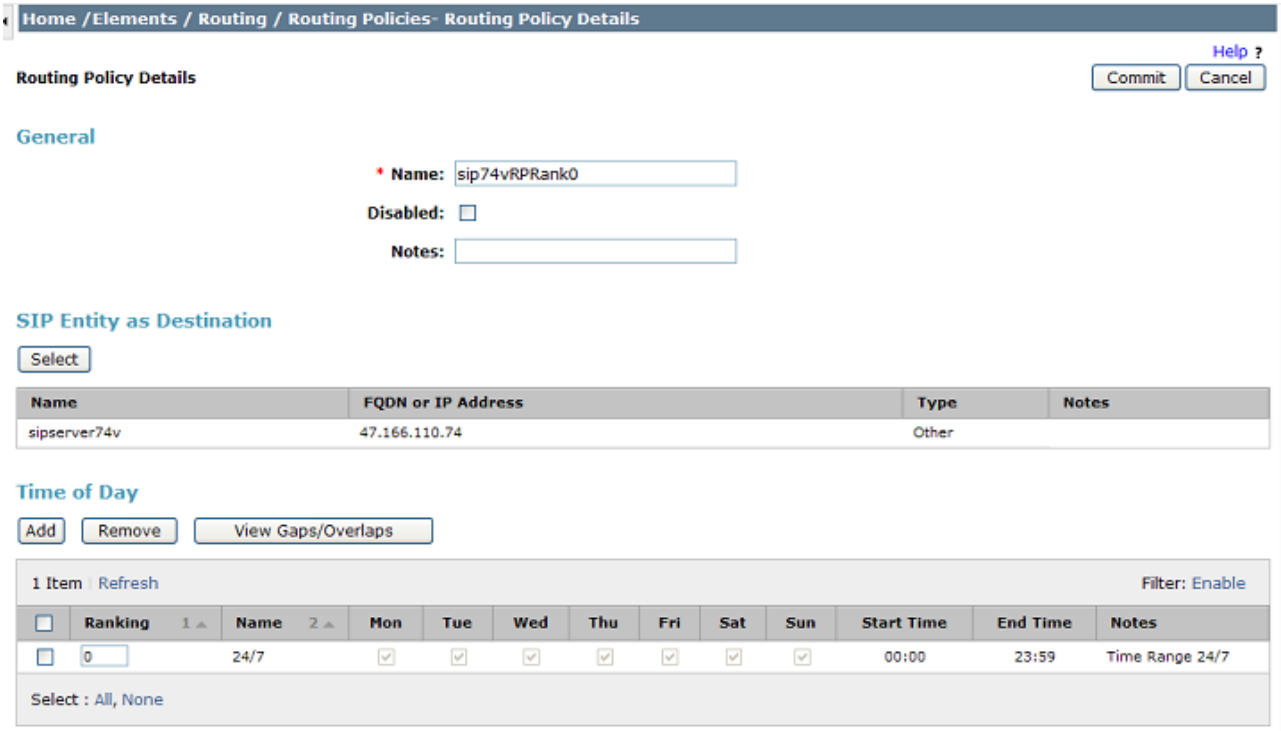
Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **Routing Policies**.
2. Click **New**.
3. In the **General** section, in the **Name** box, type the name for the Routing Policy.

   Avaya recommends that you type a descriptive name for your Routing Policy.
4. In the **Notes** box, type your notes about this Routing Policy.
5. In the **SIP Entities as Destination** section, click **Select**.
6. From the list of SIP Entities, choose the SIP Entity for your Contact Center Manager Server, click **Select**.
7. If you need to associate the Time of Day routing parameters with this Routing Policy, click **Add** from the **Time of Day** section.
8. Select the Time of Day patterns that you want to associate with this routing pattern and click **Select**.
9. Click **Commit**.

Example

Example of creating a routing policy from Session Manager to Contact Center Manager Server.



Creating a dial pattern to the Contact Center

About this task

Create a dial pattern to route matching calls to Avaya Aura® Contact Center. Session Manager uses this dial pattern to route calls to the contact center for processing.

A dial pattern specifies which routing policy or routing policies are used to route a call based on the digits dialed by a user which match that pattern. The originating location of the call and the domain in the request-URI also determine how the call gets routed.

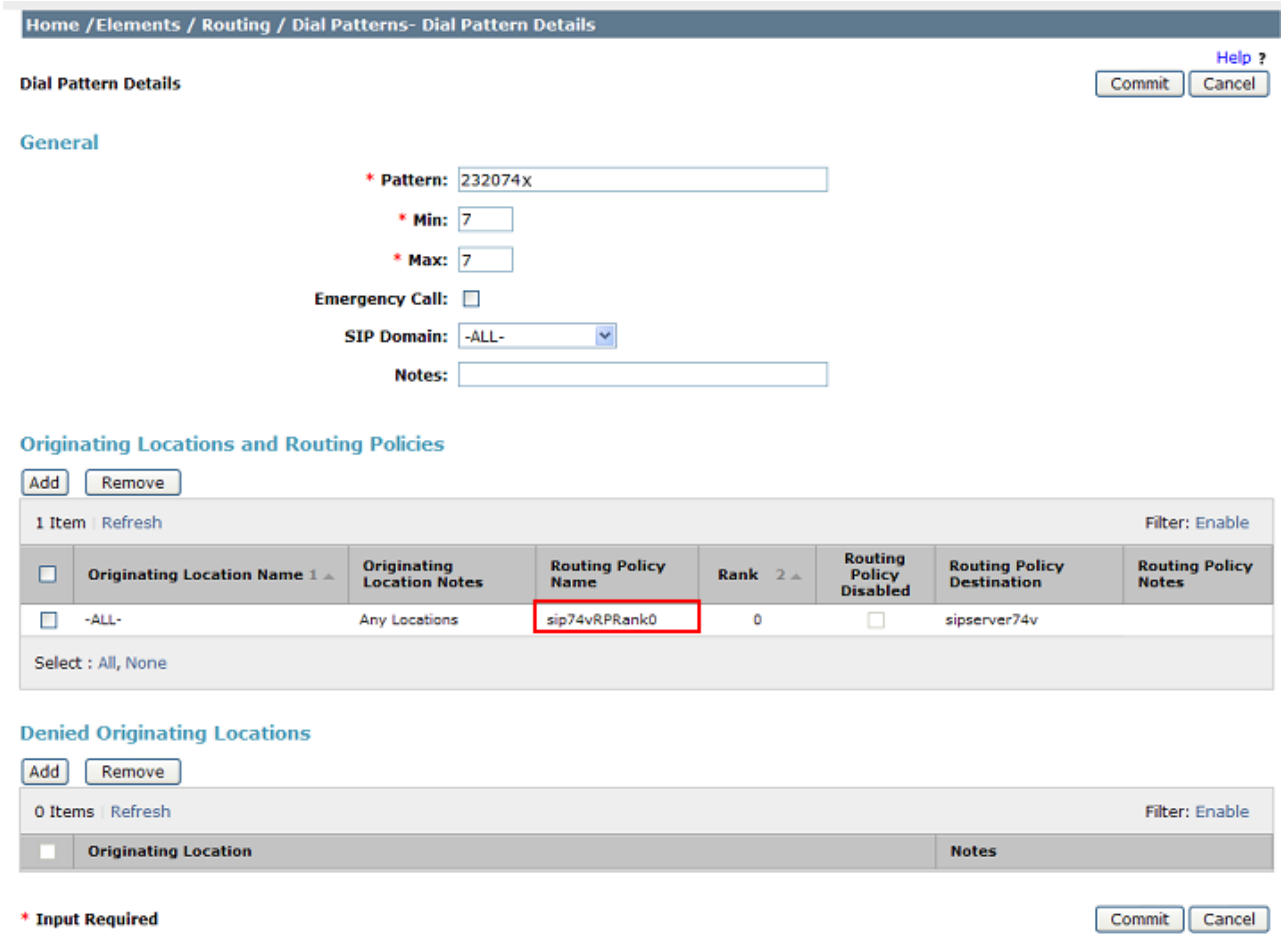
Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **Dial Patterns**.
2. Click **New**.
3. In the **Pattern** box, type the dial pattern for voice calls to the contact center.
4. In the **Min** box, type the minimum number of digits from the dial pattern to match.
5. In the **Max** box, type the maximum number of digits from the dial pattern to match.
6. From **SIP Domain**, select the SIP domain for this dial pattern. You can select a specific domain, or all domains.
7. Under the **Originating Locations and Routing Policies** section, click **Add**.

8. Select the check box for the location.
9. From **Routing Policy Name**, select the Session Manager to Contact Center Manager Server Routing Policy.
10. From the **Routing Policy Destination**, select the Contact Center Manager Server SIP Entity.
11. Click **Select** to indicate that you have completed your selections.
12. Click **Commit**.

Example

Example of creating a dial pattern using the Session Manager to Contact Center Manager Server routing policy. This example dial pattern and routing policy combination routes all phones calls in the number range 2320740 to 2320749 to Contact Center Manager Server.



Chapter 9: Fallback to Avaya Aura® Communication Manager Hunt Group configuration

If Avaya Aura® Contact Center is unable to process voice contacts, Avaya Aura® Session Manager can reroute customer voice contacts intended for Contact Center to an Avaya Aura® Communication Manager Hunt Group.

This section describes how to use Avaya Aura® Session Manager to reroute customer voice contacts intended for Contact Center to a Communication Manager Hunt Group if Avaya Aura® Contact Center is unable to process voice contacts. You must complete all the procedures in this section in sequential order.

A Communication Manager Hunt Group is a group of agent stations that can handle multiple calls to a single phone number. For each call to the Hunt Group number, Communication Manager hunts for an available agent station in the Hunt Group, and it then connects the customer call to that station. There are many types of Hunt Group, each using a different method to select an available agent station. Use the Communication Manager Hunt Group screen to create a Hunt Group, identified by a Hunt Group number, and to assign Hunt Group member agents by their station extension numbers.

Session Manager routing policies indicate the rank order of a particular SIP entity. Multiple routing policies can be associated with a dial pattern to specify alternate routing. The lowest ranking policy has priority. Configure a low routing policy to route calls to Avaya Aura® Contact Center.

In normal operation Session Manager routes customer calls to Avaya Aura® Contact Center (AACC) for treatment and routing to Contact Center agents.

On the Communication Manager, add the contact center agent phone numbers to a Hunt Group. On the Session Manager, configure the first (lowest) routing policy to route calls to Avaya Aura® Contact Center, as normal. Configure a second (higher) routing policy to route calls to the Communication Manager.

In fallback operation, Session Manager routes customer calls intended for Contact Center to a Communication Manager Hunt Group for treatment. The Contact Center agent phones are members of the Communication Manager fallback Hunt Group, therefore the Contact Center agents can use their desk phones to continue answering customer calls during the Contact Center outage.

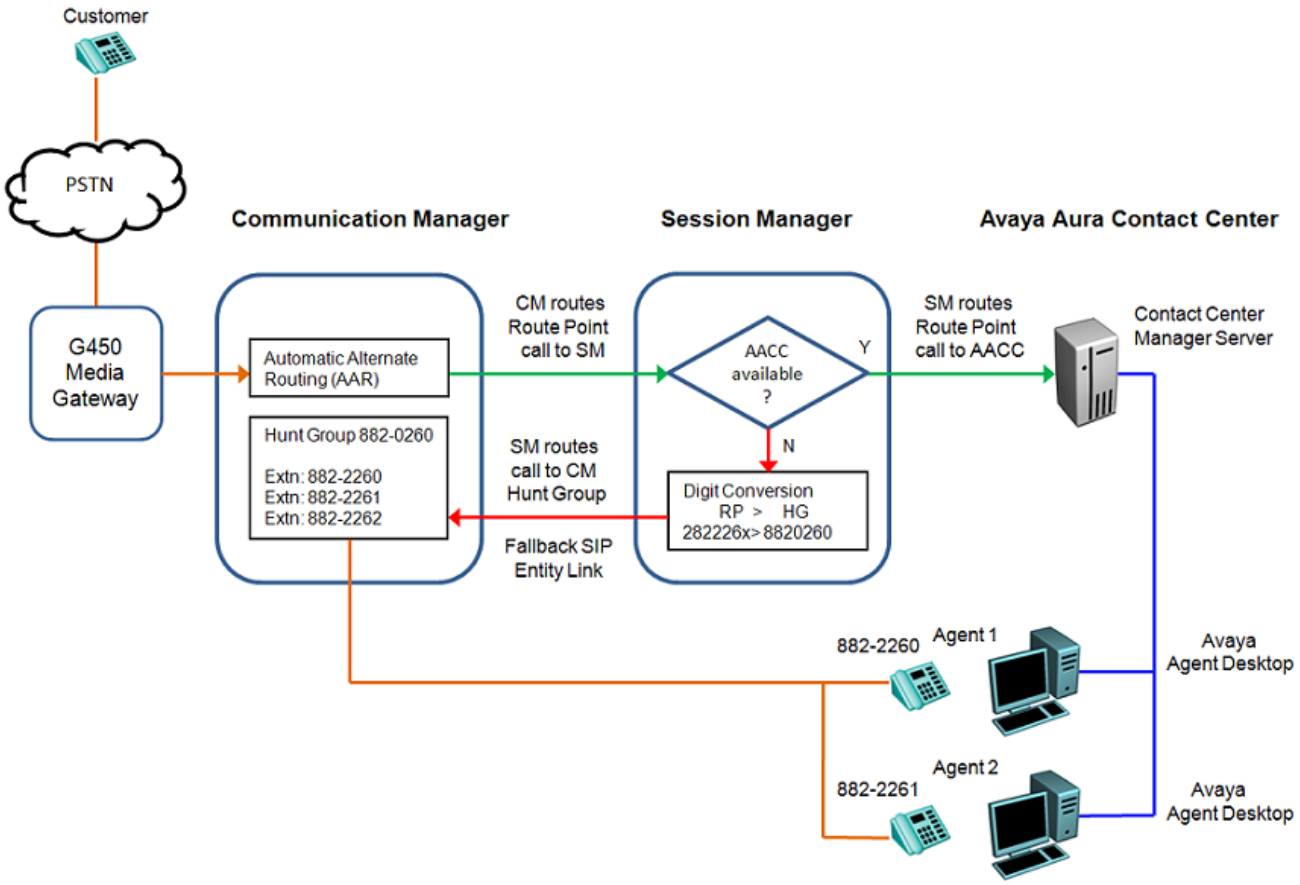


Figure 23: Example of a Communication Manager Hunt Group configuration

If Session Manager detects an Avaya Aura® Contact Center failure, Session Manager chooses the second routing policy to route calls to the Communication Manager. Before routing the call to Communication Manager, a Digit Conversion Adaptation on Session Manager reforms the call number so it resolves onto the Hunt Group. For efficiency and an improved customer experience, un-staffed agent stations must be set to the Hunt Group busy status.

Session Manager alternative routing is applied on a call-by-call basis. When Avaya Aura® Contact Center recovers, Session Manager reverts to the first routing policy and Contact Center call treatments continue as normal.

Session Manager can detect the following Avaya Aura® Contact Center issues:

- Contact Center Manager Server SIP Gateway Manager (SGM) application is offline
- Contact Center Manager Server SGM response indicating routing failure
  - No contact center Route Point acquired
  - No Media Server available to anchor calls
- Contact Center Manager Server power outage
- Contact Center Manager Server network failure

Adding a Hunt Group

About this task

Add a Communication Manager Hunt Group. Use the Hunt Group screen to create a Hunt Group, identified by a hunt group number, and to assign hunt group member agents by their station extension numbers.

Procedure

1. Use the Communication Manager — System Access Terminal (SAT) interface **add hunt-group** command to add a new Hunt Group. Choose an Group Type appropriate to your requirements.

```
display hunt-group 226                                        Page   1 of  60
                                   HUNT GROUP

           Group Number: 226
             Group Name: sips226HG
        Group Extension: 882-0260
             Group Type:                          Coverage Path:
                     TN: 1              Night Service Destination:
                    COR: 1                        MM Early Answer? n
          Security Code:                    Local Agent Preference? n
ISDN/SIP Caller Display:
```

2. Add the Avaya Aura® Contact Center agent extensions to the Hunt Group.

```
display hunt-group 226                                        Page   3 of  60
                                  HUNT GROUP
          Group Number: 226  Group Extension: 882-0260      Group Type: circ
  Member Range Allowed: 1 - 1500       Administered Members (min/max): 1   /3
                                           Total Administered Members: 3
GROUP MEMBER ASSIGNMENTS
      Ext            Name(19 characters)        Ext            Name(19 characters)
   1: 882-2260       Agent226                14:
   2: 882-2261       Agent2261               15:
   3: 882-2262       BC8822262               16:
   4:                                        17:
   5:                                        18:
   6:                                        19:
   7:                                        20:
   8:                                        21:
   9:                                        22:
  10:                                        23:
  11:                                        24:
  12:                                        25:
  13:                                        26:

  At End of Member List
```

Creating an Adaptation

About this task

Create a Digit Conversion Adapter adaptation to convert an Avaya Aura® Contact Center Route Point number into a Communication Manager Hunt Group number.

Procedure

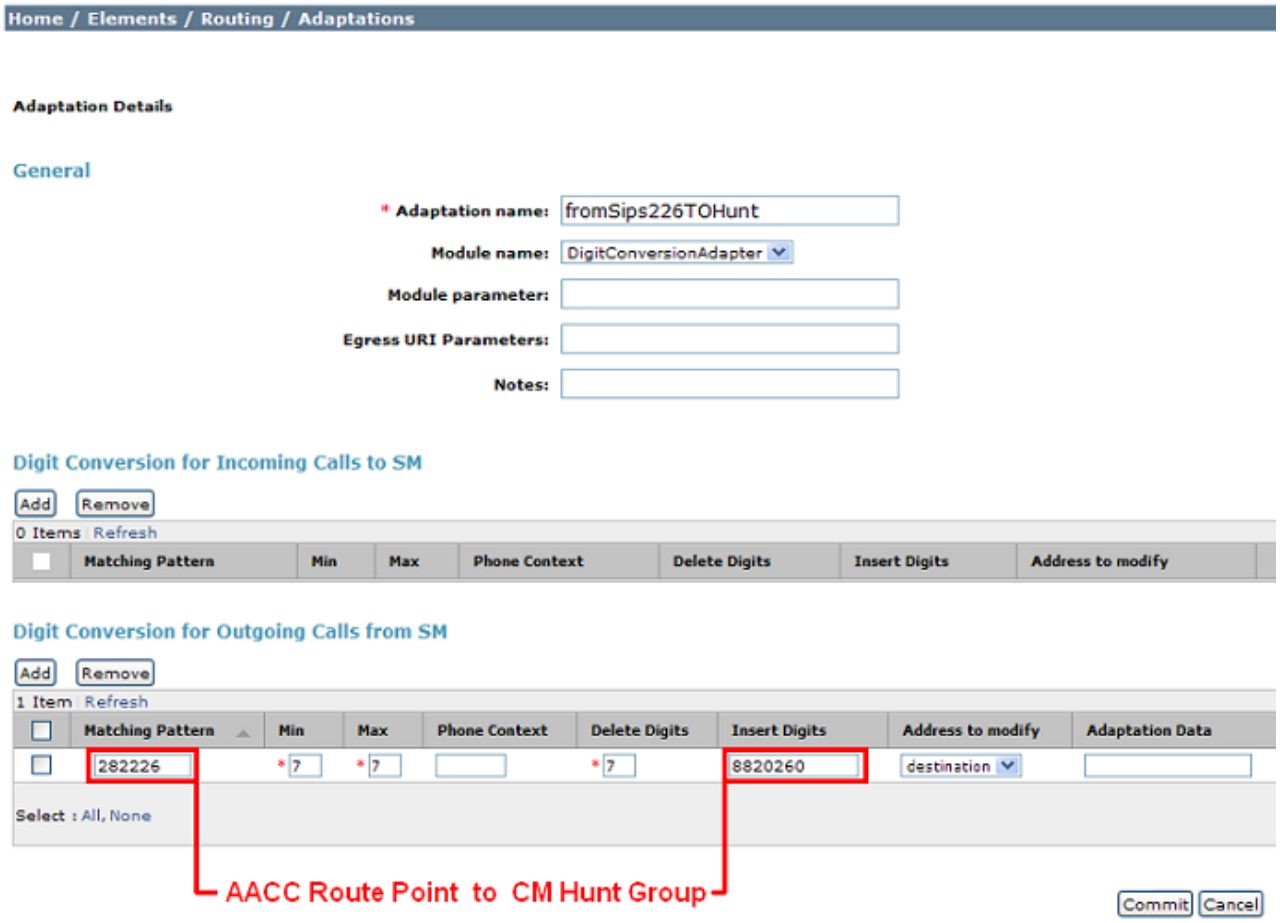
1. On the System Manager console, select **Routing** > **Adaptation**.
2. In the **Adaptation Name** box, enter a descriptive name for the Adaptation.
3. In the **Module name** list, select or type **DigitConversionAdapter**.
4. Under **Digit Conversion for Outgoing Calls from SM**, click **Add**.

   Do not edit Digit Conversion for Incoming Calls to SM.
5. In the **Matching Pattern** box, type the Avaya Aura® Contact Center Route Point number.
6. In the **Min** box, type the minimum number of digits.
7. In the **Max** box, type the maximum number of digits.
8. In the **Delete Digits** box, type the number of digits to replace.
9. In the **Insert Digits** box, type the Communication Manager Hunt Group number.
10. In the **Notes** box, type a descriptive note about this adaptation.

11. Click **Commit**.

Example

Example of an adaptation to convert an Avaya Aura® Contact Center (AACC) Route Point number into a Communication Manager (CM) Hunt Group number:



Adding an additional Signaling Group

About this task

Add an additional Signaling Group to support fallback. If Avaya Aura® Contact Center is unable to process voice contacts, Session Manager can reroute customer voice contacts intended for Contact Center to this Communication Manager Signaling Group.

The additional Signaling Group, SIP Trunk Group, and the associated Session Manager SIP Entity Link are required so that adaptations are not applied to normal calls from SIP stations to Communication Manager.

On the Communication Manager, configure a Signaling Group for communication between Communication Manager and the Avaya Aura® Session Manager.

Communication Manager uses a SIP Signaling Group and an associated SIP Trunk Group to route calls to an Avaya Aura® Session Manager.

Procedure

1. Use the System Access Terminal (SAT) interface to add a signaling group for the Session Manager. Use the **`add signaling-group <s1>`** command, where *s1* is an un-allocated signaling group.
2. You must disable the IP Multimedia Subsystem (IMS) on the Communication Manager Signaling Group. Ensure that your signaling group has the **IMS Enabled?** value set to `n`.
3. In the **Near-end Listen Port** field, type the port number. This port number must avoid a port conflict with the standard Session Manager to Communication Manager Signaling Group. For more information about the standard Signaling Group, see Configuring a SIP Signaling Group for the first on page 40.
4. In the **Far-end Listen Port** field, type the port number. This port number must match the port number used by the additional SIP Entity Link from Session Manager. For more information about the additional SIP Entity Link required to support fallback, see Creating an additional SIP Entity Link for Communication Manager on page 137.
5. Create an additional Communication Manager SIP Trunk Group and associate it with this SIP Signaling Group.

Example

If Avaya Aura® Contact Center is unable to process voice contacts, Session Manager can reroute customer voice contacts intended for Contact Center to this Communication Manager Signaling Group and the associated SIP Trunk Group.

```
display signaling-group 4                                    Page   1 of   2
                                SIGNALING GROUP

 Group Number: 4                Group Type: sip
  IMS Enabled? n          Transport Method: tcp
       Q-SIP? n
    IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: SM
 Near-end Listen Port: 5070                Far-end Listen Port: 5070
                                        Far-end Network Region: 1
                                  Far-end Secondary Node Name:
Far-end Domain: sipccocs.com
                                              Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: allow                       RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? y                  Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```

Creating an additional SIP Entity for Communication Manager

Before you begin

- Create the standard SIP Entity for Communication Manager. For more information, see Creating a SIP Entity for the Communication Manager on page 74.

About this task

Create an additional SIP Entity for Communication Manager. This additional SIP Entity is used to provide Avaya Aura® Contact Center fallback to a Communication Manager Hunt Group.

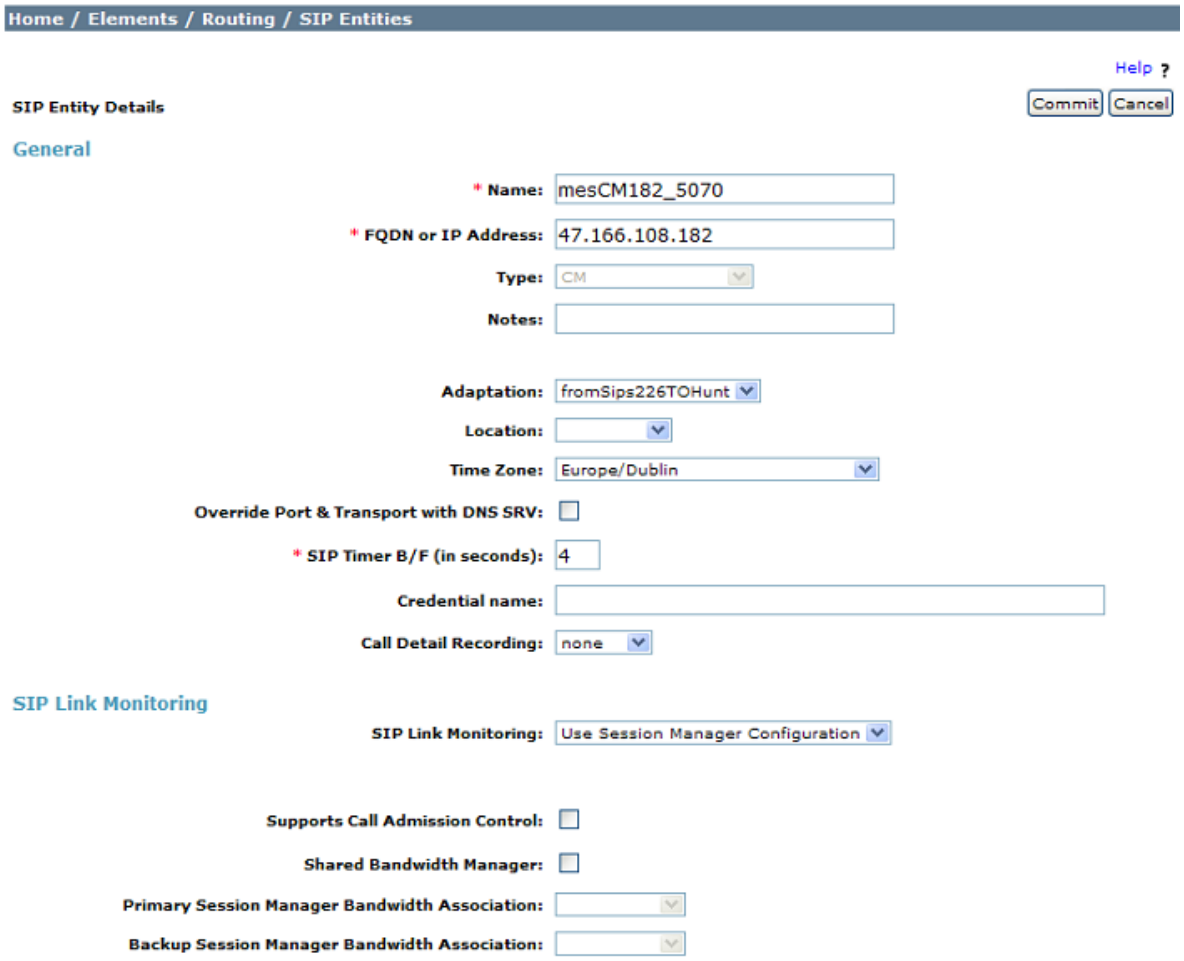
Assign an adaptation to the Communication Manager SIP Entity. The Digit Conversion Adaptation converts an Avaya Aura® Contact Center Route Point number into a Communication Manager Hunt Group number. If Avaya Aura® Contact Center is not available to process a call, the dialed Route Point number is replaced by a Hunt Group number, before the call is re-directed to Communication Manager.

Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **SIP Entities**.
2. Click **New**.

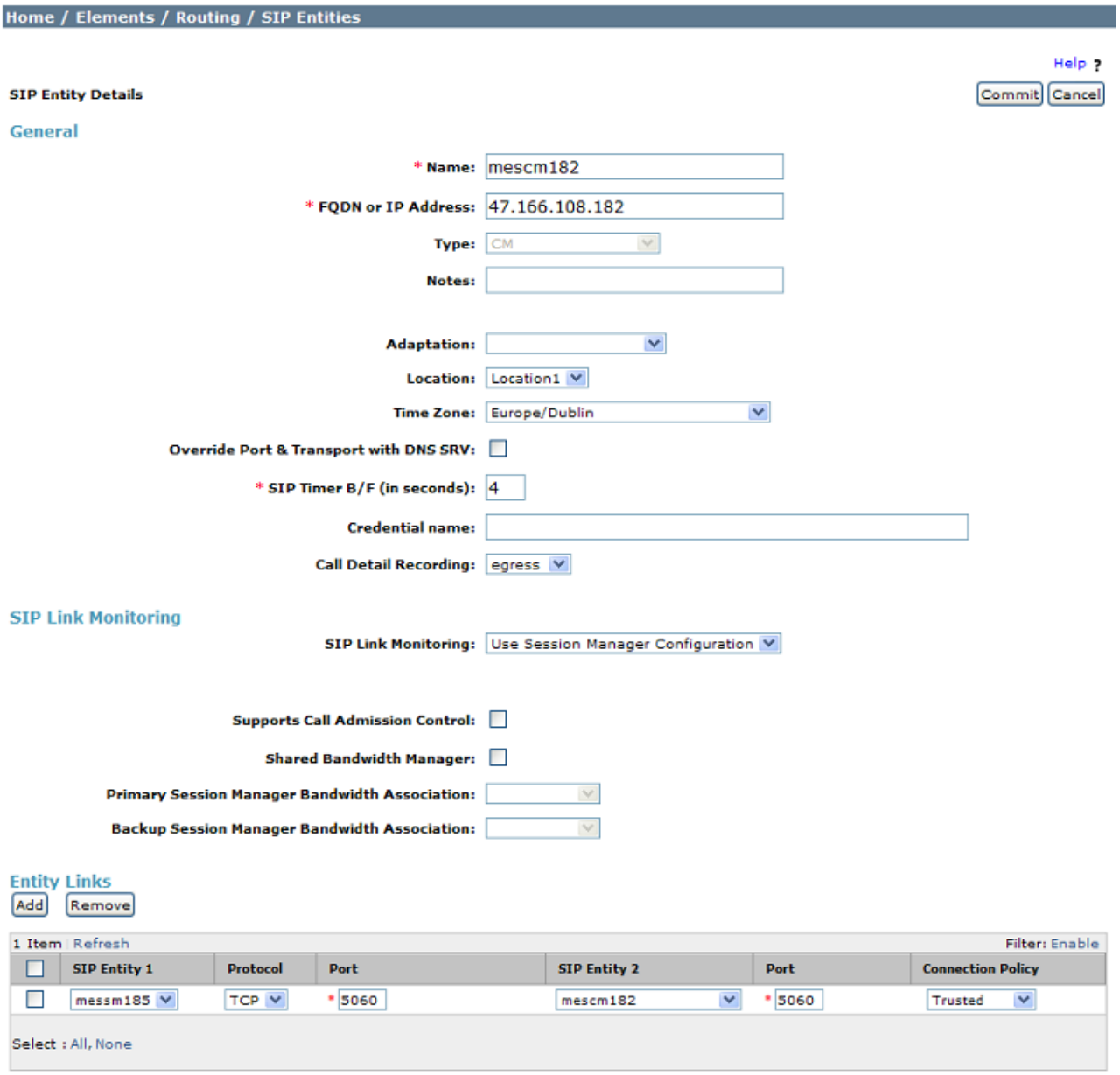
3. In the **Name** box, type the name of the Communication Manager SIP Entity.

   Avaya recommends that you type a descriptive name for your Communication Manager SIP Entity.
4. In the **FQDN or IP address** box, type the IP address of the Communication Manager.
5. From the **Type** list, select **CM**.
6. If you need to specify an Adaptation Module for the Communication Manager SIP entity, from the **Adaptation** list, select an adaptation value. For example, select the fromSips226TOHunt Adaptation.
7. In the **Location** box, select the location for this Communication Manager.
8. In the **Credential name** box, enter a regular expression string.
9. From the **SIP Link Monitoring** list, select one of the following:
   - Use Session Manager Configuration - Use the settings under **Session Manager–Session Manager Administration**.
   - Link Monitoring Enabled - Enables link monitoring on this SIP entity.
   - Link Monitoring Disabled - Link monitoring is turned off for this SIP entity.
10. Click **Commit**.



Example

The following is an example of the standard Communication Manager SIP Entity. Note that this standard SIP Entity and the associated SIP Entity Link use TCP port 5060. The fallback to Communication Manager SIP Entity Link must therefore use a different port number.



Creating an additional SIP Entity Link for Communication Manager

Before you begin

- Configure an additional SIP Entity for Communication Manager. For more information see, Creating an additional SIP Entity for Communication Manager on page 134.

About this task

Create a SIP Entity Link to the additional Communication Manager SIP Entity. If Avaya Aura® Contact Center is unable to process voice contacts, Session Manager uses this SIP Entity Link to reroute customer voice contacts intended for Contact Center to Communication Manager. This additional SIP Entity Link is required so that adaptations are not applied to normal calls from SIP stations to Communication Manager.

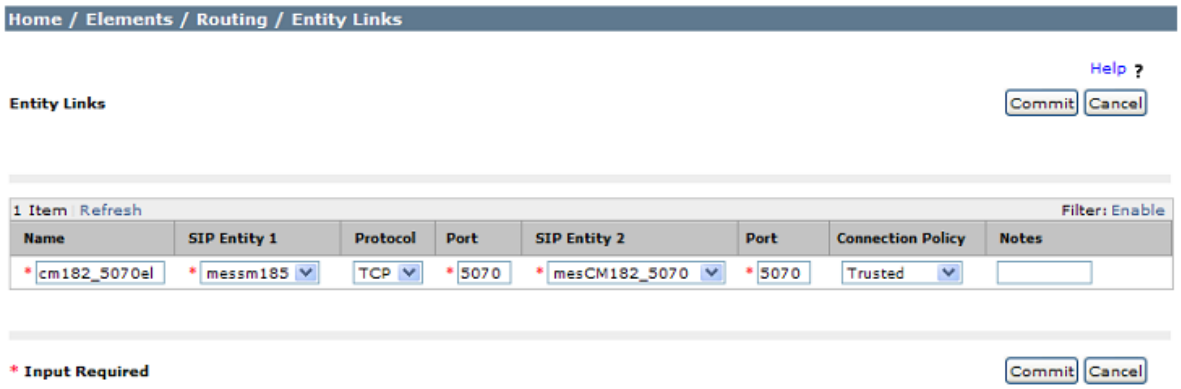
Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **Entity Links**.
2. Click **New**.
3. In the **Name** box, type the name for this SIP Entity Link.

   Avaya recommends that you type a descriptive name for your SIP Entity Link.
4. Under **SIP Entity 1**, select the required Session Manager SIP entity from the drop-down list.

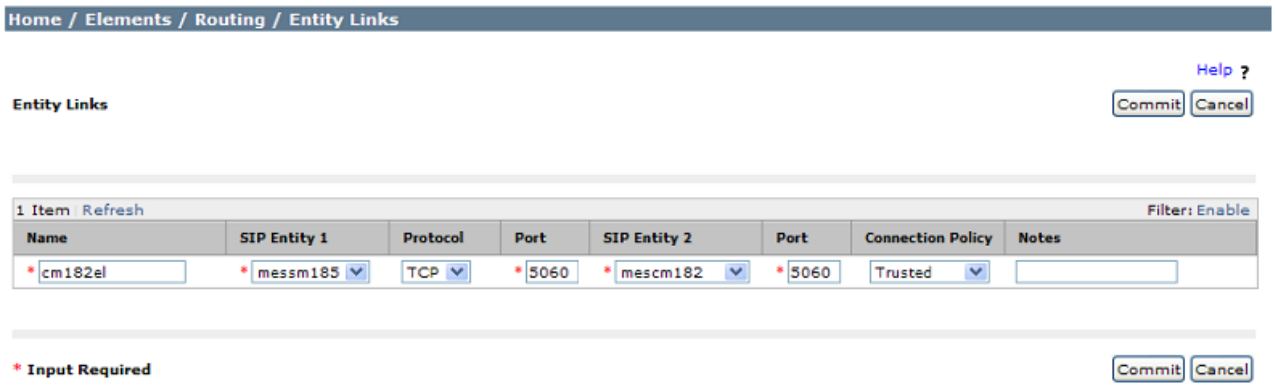
   SIP entity 1 must always be a Session Manager instance.
5. In the **Port** box, type the SIP entity 1 port number.
6. Under **SIP Entity 2**, select the required Communication Manager SIP entity from the drop-down list. For example, select the additional Communication Manager SIP Entity mesCM182_5070.
7. In the **Port** box, type the SIP entity 2 port number.
8. From the Connection Policy list, select the **Trusted**.

   Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
9. Click **Commit**.



Example

The following is an example of the SIP Entity Link to the standard Communication Manager SIP Entity. Note that this SIP Entity Link uses port 5060.



Creating a routing policy to Avaya Aura® Contact Center

About this task

Create a routing policy from Session Manager to Avaya Aura® Contact Center. Session Manager uses the data configured in the Routing Policy to find the best match against the number (or address) of the called party.

Procedure

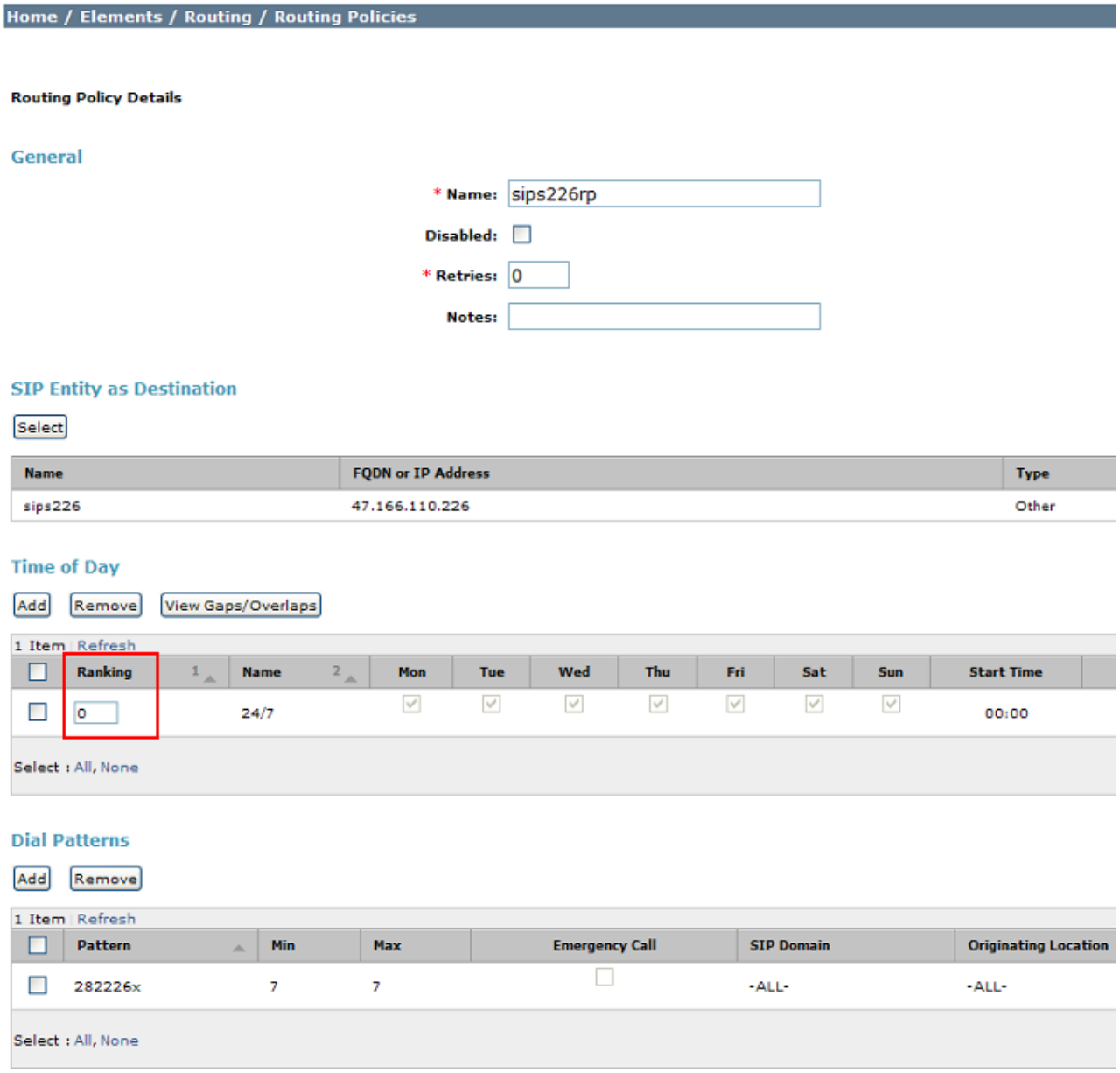
1. On the Avaya Aura® System Manager console, select **Routing** > **Routing Policies**.
2. Click **New**.

   The Routing Policy Details screen is displayed.
3. In the **General** section, in the **Name** box, type the name for the Routing Policy.

   Avaya recommends that you type a descriptive name for your Routing Policy.
4. In the **Notes** box, type your notes about this Routing Policy.
5. In the **SIP Entities as Destination** section, click **Select**.
6. From the list of SIP Entities, choose the SIP Entity for your Avaya Aura® Contact Center, click **Select**.
7. If you need to associate the Time of Day routing parameters with this Routing Policy, click **Add** from the **Time of Day** section.
8. Select the **Time of Day** patterns that you want to associate with this routing pattern.
9. Click **Select**.
10. In the **Ranking** box, type 0. This ranking number must be lower than the ranking number assigned to the Communication Manager routing policy.
11. Click **Commit**.

Example

The following diagram shows an example of the routing policy from Session Manager to Avaya Aura® Contact Center. Note that Ranking is set to 0, and the associated Dial Pattern covers the Avaya Aura® Contact Center Route Point (CDN) range:



Creating a routing policy to Avaya Aura® Communication Manager

About this task

Create a routing policy from Session Manager to Avaya Aura® Communication Manager. Session Manager uses the data configured in the Routing Policy to find the best match against the number (or address) of the called party.

Procedure

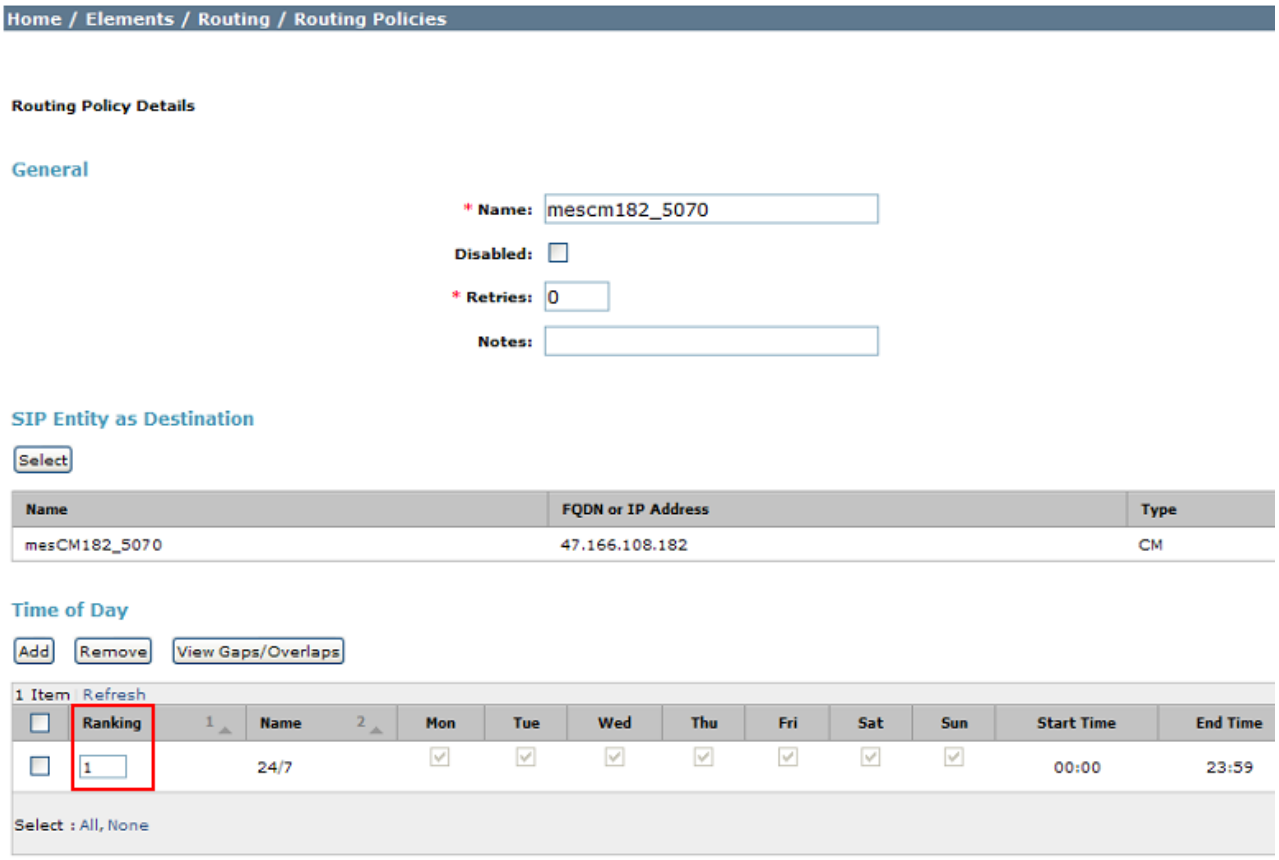
1. On the Avaya Aura® System Manager console, select **Routing** > **Routing Policies**.
2. Click **New**.

   The Routing Policy Details screen is displayed.
3. In the **General** section, in the **Name** box, type the name for the Routing Policy.

   Avaya recommends that you type a descriptive name for your Routing Policy.
4. In the **Notes** box, type your notes about this Routing Policy.
5. In the **SIP Entities as Destination** section, click **Select**.
6. From the list of SIP Entities, choose the SIP Entity for your Communication Manager, click **Select**.
7. If you need to associate the **Time of Day** routing parameters with this Routing Policy, click **Add** from the **Time of Day** section.
8. Select the **Time of Day** patterns that you want to associate with this routing pattern.
9. Click **Select**.
10. In the **Ranking** box, type 1. This ranking number must be higher than the ranking number assigned to the Avaya Aura® Contact Center routing policy.
11. Click **Commit**.

Example

Example of a routing policy from Session Manager to Avaya Aura® Communication Manager:



Creating a dial pattern

About this task

Create a dial pattern using the Avaya Aura® Contact Center and Communication Manager Routing Policies. Session Manager uses these dial patterns to route calls. A dial pattern specifies which routing policy or routing policies are used to route a call based on a number of parameters including ranking. Routing Policies with a higher ranking (lower rank number) are selected first. If the first Routing Policy is not available, the second Routing Policy is used instead.

Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **Dial Patterns**.
2. Click **New**.

   The Dial Pattern Details screen is displayed.
3. In the **General** section, type the Dial Pattern General information.

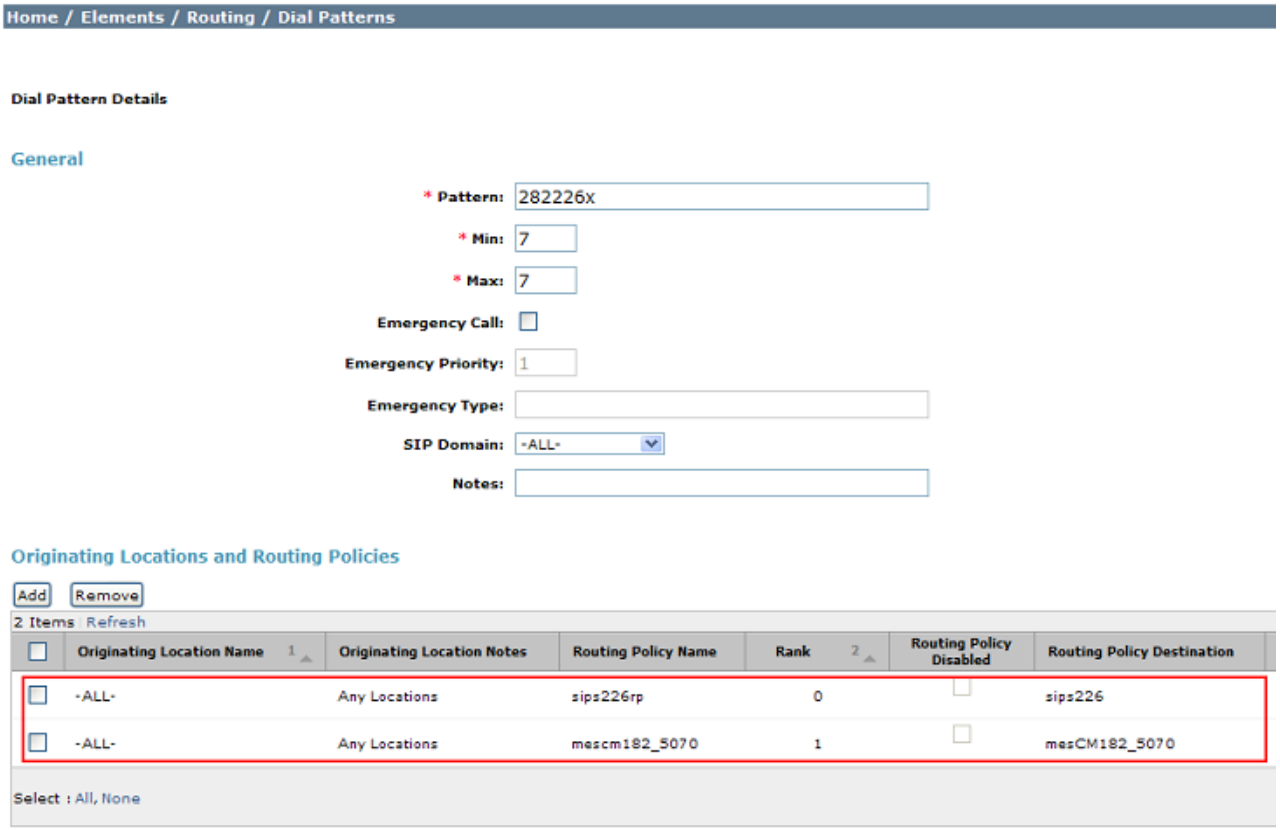
Note:

A **Domain** can be provided to restrict the Dial Pattern to the specified Domain.

4. Under the **Originating Locations and Routing Policies** section, click **Add**.
5. Select all the required Locations and Routing Policies that you want associated with the Dial Pattern by selecting the check box in front of each item.
6. From **Routing Policy Name**, select the Session Manager to Avaya Aura® Contact Center Routing Policy.
7. From the **Routing Policy Destination**, select the Avaya Aura® Contact Center SIP Entity.
8. Click **Select** to indicate that you have completed your selections.
9. Under the **Originating Locations and Routing Policies** section, click **Add**.
10. Select all the required Locations and Routing Policies that you want associated with the Dial Pattern by selecting the check box in front of each item.
11. From **Routing Policy Name**, select the new Session Manager to Communication Manager Routing Policy with Ranking set to 1.
12. From the **Routing Policy Destination**, select the Communication Manager SIP Entity.
13. Click **Select** to indicate that you have completed your selections.
14. If you need to specify that calls from the specified locations are denied, under the **Denied Originating Locations** section, click **Add**.
15. Select all the **Locations** that are to be denied and click **Select** to indicate that you have completed your selections.
16. Click **Commit**.

Example

Example of dial pattern using the Avaya Aura® Contact Center and Communication Manager Routing Policies. Routing Policies with a higher ranking (lower rank number) are selected first. If the first Routing Policy is not available, the second Routing Policy is used instead. In this example, the Avaya Aura® Contact Center Routing Policy has a ranking of zero. Under normal operation, this dial pattern resolves to Avaya Aura® Contact Center. If Avaya Aura® Contact Center is not available, this dial pattern resolves to the Communication Manager Routing Policy. Calls intended for Avaya Aura® Contact Center fallback to the Communication Manager Hunt Group until Avaya Aura® Contact Center regains call control.



Variable definitions

Variable	Value
Pattern	Dial pattern to match. The pattern can have between 1 and 36 characters.
Min	Minimum number of digits to be matched.
Max	Maximum number of digits to be matched.

Table continues…

Variable	Value
Emergency Call	Indicate if it is an emergency call. **Note:** Some of the important constraints on the use of this feature are as follows: — Each location must be assigned to only one emergency dial number. — This emergency dial number must match the emergency dial number in the 96xx Deskphone settings file for all SIP phones in the identified location.
SIP Domain	Domain for which you want to restrict the dial pattern.
Notes	Other details that you wish to add.
Select check box	Use this check box to select and use the digit conversion for the incoming calls.
Location Name	Name of the location to be associated to the dial pattern.
Location Notes	Notes about the selected location.
Routing Policy Name	Name of the routing policy to be associated to the dial pattern.
Routing Policy Disabled	Name of the disabled routing policy.
Routing Policy Destination	Destination of the routing policy.
Routing Policy Notes	Any other notes about the routing policy that you wish to add.

Chapter 10: Avaya Aura® Call Center Elite and Avaya Aura® Contact Center configuration

This section describes how to add an Avaya Aura® Contact Center voice and multimedia contact center to an existing Avaya Aura® Communication Manager and Avaya Aura® Call Center Elite solution. You must complete all the procedures in this section in sequential order.

Avaya Aura® Communication Manager supports concurrent interoperability with Avaya Aura® Call Center Elite and Avaya Aura® Contact Center. Customers with an existing Avaya Aura® Call Center Elite deployment can add Avaya Aura® Contact Center voice contact support to the same Communication Manager. The existing Avaya Aura® Call Center Elite system remains unchanged from the agent point of view. You must configure the Communication Manager platform to add support for the Avaya Aura® Contact Center voice agents.

To support Avaya Aura® Contact Center voice agents and Avaya Aura® Call Center Elite voice agents on the same Communication Manager, there must be no interaction between the two sets of agents. Elite agent extension ranges must be unique and not overlap with Avaya Aura® Contact Center agent extension ranges. Both applications must use separate inbound and outbound PSTN numbers – the numbers for each application must not overlap. Avaya Aura® Call Center Elite supervisors, agents, and customers must not interact with Avaya Aura® Contact Center supervisors, agents, and customers.

Avaya Aura® Call Center Elite contacts must be handled by Elite agents and supervisors. Avaya Aura® Contact Center contacts must be handled by the Contact Center agents and supervisors. Contacts cannot be transferred, conferenced, or forwarded from Avaya Aura® Call Center Elite to Avaya Aura® Contact Center and vice versa. Avaya Aura® Call Center Elite and Avaya Aura® Contact Center must be logically separated on the Communication Manager.

The following Communication Manager features support the logical separation of Avaya Aura® Call Center Elite and Avaya Aura® Contact Center:

- Class of Restriction (COR)
- Facility Restriction Levels (FRL)
- Class of Service (COS) optional

The **Class of Restriction** (COR) feature defines different levels of call origination and termination privileges, applies administration settings to all objects that share the same COR number, identifies the CORs that can be service observed, and the CORs that can be a service observer. CORs can be assigned to a variety of objects, such as: telephones, trunks, and agent login IDs. CORs also

apply to Elite agent telephones, Elite agent IDs, Trunk Groups and Hunt Groups. Communication Manager supports many levels of COR.

The **Facility Restriction Levels** (FRL) feature determines the calling privileges of a user. The Facility Restriction Levels control the privileges of the call originator. For example, you can use FRL to allow some users to place international calls, and restrict other users to place only local calls. Facility Restriction Levels are ranked from 0 to 7, where 7 has the highest level of privileges.

The **Class of Service** (COS) feature allows or denies user access to some system features. Use the COS feature to allow or deny user access to some system features, such as Automatic Callback, Call Forwarding, Data Privacy, Contact Closure Activation, and Console Permission. Use the Class of Restriction (COR) feature, instead of COS, to define the restrictions that apply when a user places or receives a call.

You can use the COR and FRL features to support Avaya Aura® Contact Center and Avaya Aura® Call Center Elite on the same Avaya Aura® Communication Manager. Use the COR and FRL features to restrict the following actions:

- Elite agents restricted from calling, forwarding, conferencing, or transferring Elite calls to/from Avaya Aura® Contact Center agents and Controlled Directory Numbers (CDNs).
- Avaya Aura® Contact Center agents are restricted from calling, forwarding, conferencing, or transferring calls to/from Elite agents, Elite Vector Directory Number (VDN) and optional Hunt Groups.

There are many methods to achieve this logical separation but the example method used here is one of the simplest and easiest to implement.

The example solution used in this section has two separate contact centers operating independently of each other but using the same Communication Manager infrastructure. Agents either work exclusively as Elite based agents or as Avaya Aura® Contact Center based agents. Agents must not swap on a daily basis between each contact center. The Avaya Aura® Contact Center components add voice and optional multimedia contact support for Avaya Aura® Contact Center agents. Elite agents continue to be serviced by the Avaya Aura® Call Center Elite application.

Note:

To support an Avaya Aura® Call Center Elite voice contact center and a separate Avaya Aura® Contact Center contact center on the same Communication Manager, Communication Manager must be Release 6.0.1 or later.

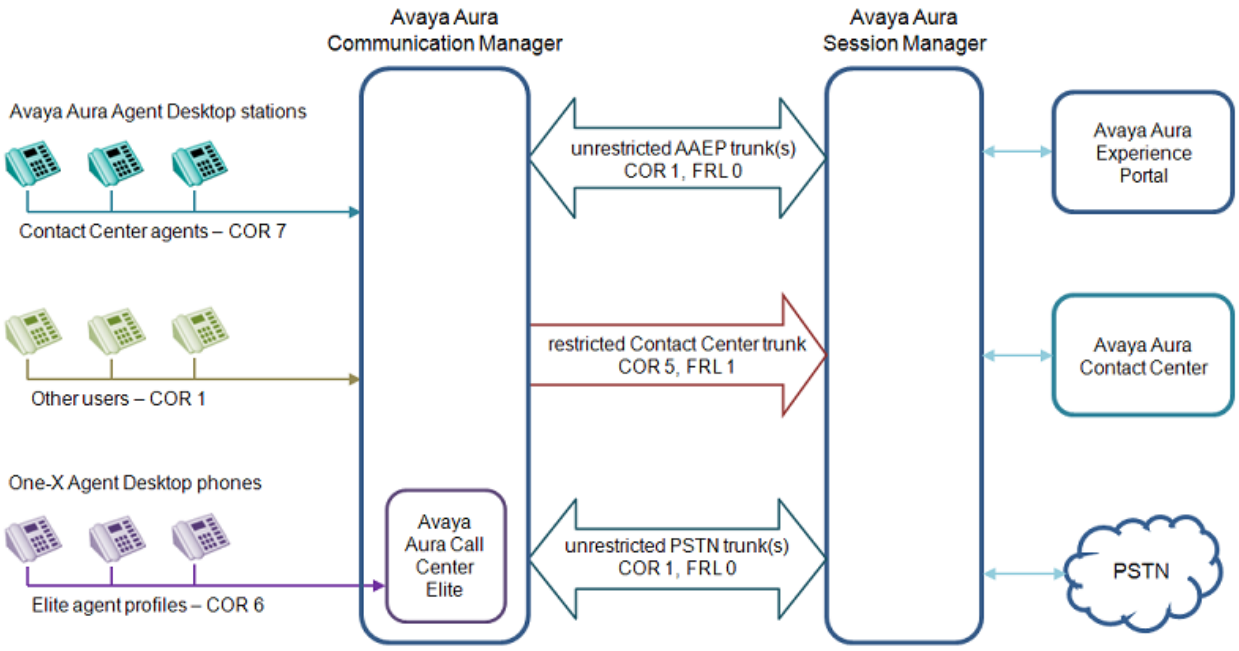


Figure 24: Example of a typical solution with Avaya Aura® Contact Center and Avaya Aura® Call Center Elite supported on the same Avaya Aura® Communication Manager

In this typical example there are three groups of users:

- Avaya Aura® Call Center Elite agents and associated desk phones
- Avaya Aura® Contact Center agents and associated desk phones
- Other users within the enterprise and their associated desk phones

The example solution uses the following configuration settings:

- Users with COR 1 are unrestricted, they have full dialing access to all other users and trunks with any COR. In the example, all “other” users in the enterprise are unrestricted.
- Avaya Aura® Contact Center agents and resources are configured with COR 7 and a FRL of 1.
- Avaya Aura® Call Center Elite agents and resources are configured with COR 6 and a FRL of 0.
- Avaya Aura® Contact Center agents and Avaya Aura® Call Center Elite agents cannot interact with each other.
- A dedicated outgoing trunk group from Communication Manager to Avaya Aura® Session Manager. This trunk is used to access Contact Center CDNs. This must be an outgoing trunk group to prevent Session Manager from using these trunks for inbound voice contacts to the restricted users.
- The Contact Center CDN trunk in the example is configured with COR 5. This means you do not have to modify all the other trunks (Session Manager to Avaya Aura® Experience Portal trunks) already configured on the Communication Manager platform.

- Communication Manager SIP signaling trunks used for Avaya Aura® Contact Center have a FRL level of 1 defined in COR 5 for these trunks. This means that users with COR settings must have a FRL level equal to or higher than 1 to access any resources through these signaling trunks.
- Elite users with COR 6 and FRL 0 therefore cannot access Avaya Aura® Contact Center resources in COR 7.
- Elite users also cannot access the SIP signaling trunks to Avaya Aura® Contact Center CDNs.
- Elite resources with COR 6 are restricted from the Contact Center trunk group unless they access it using the PSTN. All other COR's can internally access this trunk group.

The choice of COR numbers is arbitrary, you can use any COR numbers compatible with your existing enterprise dial plan. Avaya Aura® Contact Center agents and all the other enterprise users can access Avaya Aura® Contact Center (CDNs) using multiple methods; direct dial, transfer, conference, or PSTN dialing. Elite agents cannot access Avaya Aura® Contact Center CDNs either using internal direct dial, conference, transfer, forward capabilities due to their COR settings. Users with either COR value can access resources on Elite or Avaya Aura® Contact Center by dialing the external PSTN. The worked example does not prevent this as external dialing is required in most enterprises.

Agent Desktop solutions

In solutions where Avaya Aura® Contact Center shares the same Avaya Aura® Communication Manager as an Avaya Aura® Call Center Elite deployment, you must logically separate the Elite agents from the Contact Center agents. The transferring, conferencing, or forwarding of contacts between the two groups of agents is not supported.

Avaya Aura® Call Center Elite agents use one of the following:

- Physical desk phone
- One X- Agent

After deploying Avaya Aura® Contact Center on the same Communication Manager, Elite agents continue to use any of these options. Avaya Aura® Contact Center agents use the voice capabilities of the Communication Manager platform with the added benefit of full multimedia contact support. Avaya Aura® Contact Center agents use Avaya Agent Desktop in one of the supported modes:

- CTI control of a physical Communication Manager phone
- Softphone mode with embedded H.323
- Telecommuter mode

In solutions that support Avaya Aura® Contact Center fallback to Avaya Aura® Call Center Elite, Avaya Agent Desktop does not support Avaya Aura® Call Center Elite agents. Elite agents must use One-X Agent or a physical phone. In fallback mode, Contact Center agents use their desk phones to access the fallback Elite skill and handle customer voice contacts.

Avaya Aura® Call Center Elite agents and Avaya Aura® Contact Center agents both support presence capabilities. Peer to Peer Instant Message (IM) interactions are supported between Avaya Aura® Call Center Elite agents and Avaya Aura® Contact Center agents. This solution also supports interactions between all other presence-enabled enterprise users and Avaya Aura® Call Center Elite or Avaya Aura® Contact Center users. These Instant Message interactions are "client to client" or "peer to peer" messages, they are not routed IM contacts.

Prerequisites

Configure Avaya Aura® Communication Manager for integration with Avaya Aura® Contact Center as normal. For more information see, Communication Manager configuration on page 29.

Changing the Class of Restriction value for Contact Center agent stations

Before you begin

- Create the Avaya Aura® Contact Center agent stations as normal. For more information about creating Avaya Aura® Contact Center agent stations, see Creating the agent extensions on page 58.

About this task

Change the Avaya Aura® Contact Center agent station Class of Restriction (COR) value to separate the Contact Center agents from the Avaya Aura® Call Center Elite agents.

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to change the Avaya Aura® Contact Center agent station COR value. Use the **`change station n`** command.

   For example, enter **`change station 3171503`**.

2. Change the COR value to separate the Contact Center agents from the Avaya Aura® Call Center Elite agents.
3. Repeat the SAT **`change station n`** command for each additional Contact Center agent station you need to separate from Avaya Aura® Call Center Elite.

Example

The following Communication Manager station display shows one of the Contact Center agent phones configured with a Class of Restriction value of 7.

```
display station 3171503                                      Page   1 of   5
                                    STATION

Extension: 317-1503                    Lock Messages? n                BCC: 0
     Type: 9620                        Security Code: 12345678          TN: 1
     Port: S00294                    Coverage Path 1:                  COR: 7
     Name: agent1 aacc4              Coverage Path 2:                  COS: 1
                                     Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
             Loss Group: 19          Personalized Ringing Pattern: 1
                                               Message Lamp Ext: 317-1503
          Speakerphone: 2-way               Mute Button Enabled? y
       Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y

                                           IP Video Softphone? n
                                Short/Prefixed Registration Allowed: default

                                          Customizable Labels? y
```

Changing the Contact Center agent station Class of Restriction details

Before you begin

- Create the Avaya Aura® Contact Center agents stations as normal. For more information about creating Avaya Aura® Contact Center agent stations, see Creating the agent extensions on page 58.

About this task

Edit the Class of Restriction (COR) value used by the Contact Center agent stations to separate them from Avaya Aura® Call Center Elite agents. Change the Facility Restriction Levels (FRL) of this COR and edit the Calling Permission details to block Avaya Aura® Call Center Elite agents.

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to change the Contact Center agent COR permission details. Use the **`change cor n`** command.

   For example, enter **`change cor 7`**.

2. Change the COR permission details to separate the Contact Center agents from Avaya Aura® Call Center Elite agents.

Example

The following Communication Manager Class of Restriction display shows COR 7 (page 1). This COR has a Facility Restriction Levels (FRL) value of 1. Facility Restriction Levels are ranked from 0 to 7, where 7 has the highest level of privileges. Only Communication Manager users (agents) with a FRL of 1 or higher can access resources controlled by this COR value. This separates Avaya Aura® Call Center Elite agents with a COR value of 6 and a FRL value of 0 from Contact Center agents.

```
display cor 7                                                Page   1 of  23
                              CLASS OF RESTRICTION

                 COR Number: 7
            COR Description: Restricted AACC COR for AACC Agents

                        FRL: 1                                  APLT? y
  Can Be Service Observed? n                Calling Party Restriction: outward
Can Be A Service Observer? n                 Called Party Restriction: none
        Time of Day Chart: 1              Forced Entry of Account Codes? n
         Priority Queuing? n                      Direct Agent Calling? n
     Restriction Override: none             Facility Access Trunk Test? n
     Restricted Call List? n                        Can Change Coverage? n

            Access to MCT? y                   Fully Restricted Service? n
Group II Category For MFC: 7                   Hear VDN of Origin Annc.? n
         Send ANI for MFE? n                    Add/Remove Agent Skills? n
            MF ANI Prefix:                      Automatic Charge Display? n
Hear System Music on Hold? y          PASTE (Display PBX Data on Phone)? n
                          Can Be Picked Up By Directed Call Pickup? n
                                        Can Use Directed Call Pickup? n
                                        Group Controlled Restriction: inactive
```

The following Communication Manager Class of Restriction display shows COR 7 (page 4). This display shows that Contact Center agent stations with COR 7 are restricted from accessing system resources with a COR value of 6. Contact Center agents do not have permission to access Avaya Aura® Call Center Elite agents with a COR value of 6.

```
display cor 7                                                Page   4 of  23
                                CLASS OF RESTRICTION

CALLING PERMISSION (Enter "y" to grant permission to call specified COR)

  0? y      15? y      30? y      44? y      58? y      72? y      86? y
  1? y      16? y      31? y      45? y      59? y      73? y      87? y
  2? y      17? y      32? y      46? y      60? y      74? y      88? y
  3? y      18? y      33? y      47? y      61? y      75? y      89? y
  4? y      19? y      34? y      48? y      62? y      76? y      90? y
  5? y      20? y      35? y      49? y      63? y      77? y      91? y
  6? n      21? y      36? y      50? y      64? y      78? y      92? y
  7? y      22? y      37? y      51? y      65? y      79? y      93? y
  8? y      23? y      38? y      52? y      66? y      80? y      94? y
  9? y      24? y      39? y      53? y      67? y      81? y      95? y
 10? y      25? y      40? y      54? y      68? y      82? y      96? y
 11? y      26? y      41? y      55? y      69? y      83? y      97? y
 12? y      27? y      42? y      56? y      70? y      84? y      98? y
 13? y      28? y      43? y      57? y      71? y      85? y      99? y
 14? y      29? y
```

The following Communication Manager Class of Restriction display shows COR 1. In this example, COR 1 is used by other users in the solution. These users are not Avaya Aura® Call Center Elite agents or Avaya Aura® Contact Center agents. These users have permission to access all Class of Restriction controlled resources. These users can communicate with Avaya Aura® Call Center Elite agents and Avaya Aura® Contact Center agents. Typically these users are experts or back-office support staff.

```
display cor 1                                                Page   4 of  23
                              CLASS OF RESTRICTION

CALLING PERMISSION (Enter "y" to grant permission to call specified COR)

  0? y      15? y      30? y      44? y      58? y      72? y      86? y
  1? y      16? y      31? y      45? y      59? y      73? y      87? y
  2? y      17? y      32? y      46? y      60? y      74? y      88? y
  3? y      18? y      33? y      47? y      61? y      75? y      89? y
  4? y      19? y      34? y      48? y      62? y      76? y      90? y
  5? y      20? y      35? y      49? y      63? y      77? y      91? y
  6? y      21? y      36? y      50? y      64? y      78? y      92? y
  7? y      22? y      37? y      51? y      65? y      79? y      93? y
  8? y      23? y      38? y      52? y      66? y      80? y      94? y
  9? y      24? y      39? y      53? y      67? y      81? y      95? y
 10? y      25? y      40? y      54? y      68? y      82? y      96? y
 11? y      26? y      41? y      55? y      69? y      83? y      97? y
 12? y      27? y      42? y      56? y      70? y      84? y      98? y
 13? y      28? y      43? y      57? y      71? y      85? y      99? y
 14? y      29? y
```

Changing the Class of Restriction value for Elite agent profiles

Before you begin

- Create the Avaya Aura® Call Center Elite agent profiles as normal.

About this task

Change the Avaya Aura® Call Center Elite agent profile Class of Restriction (COR) value to separate the Elite agents from the Avaya Aura® Contact Center agents.

When an Elite agent logs on to a telephone, the Elite agent profile COR setting overrides the COR setting for the physical desk phone. Do not set a COR setting on desk phones used by Elite agents, instead configure the COR setting on the Elite agent profile. This simplifies the work required to support the solution described here.

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to change the Avaya Aura® Call Center Elite agent profile COR value. Use the **`change agent-loginID n`** command.

   For example, enter **`change agent-loginID 3171600`**.

2. Change the COR value to separate the Elite agents from the Avaya Aura® Contact Center agents.
3. Repeat the SAT **`change agent-loginID n`** command for each additional Avaya Aura® Call Center Elite agent profile that you need to separate from Avaya Aura® Contact Center.

Example

The following Communication Manager display shows one of the Elite agent profiles configured with a Class of Restriction value of 6.

```
display agent-loginID 3171600                                  Page   1 of   3
                                AGENT LOGINID

               Login ID: 317-1600                                AAS? n
                   Name: Agent3171600Elite                     AUDIX? n
                     TN: 1                               LWC Reception: spe
                    COR: 6                      LWC Log External Calls? n
              Coverage Path:                   AUDIX Name for Messaging:
              Security Code:
                                         LoginID for ISDN/SIP Display? n
                                                              Password:
                                             Password (enter again):
                                                         Auto Answer: station
                                                 MIA Across Skills: system
                                          ACW Agent Considered Idle: system
                                          Aux Work Reason Code Type: system
                                            Logout Reason Code Type: system
                        Maximum time agent in ACW before logout (sec): system
                                             Forced Agent Logout Time:   :

     WARNING:  Agent must log in again before changes take effect
```

Changing the Elite agent profile Class of Restriction details

Before you begin

- Create the Avaya Aura® Call Center Elite agent profile as normal.

About this task

Edit the Class of Restriction (COR) value of the Avaya Aura® Call Center Elite agent profiles to separate them from Avaya Aura® Contact Center (agent and trunk) resources.

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to change the Avaya Aura® Call Center Elite agent profile COR permissions. Use the **change cor n** command.

   For example, enter **change cor 6**.

2. Change the COR permissions to separate the Avaya Aura® Call Center Elite agents from Contact Center resources.

Example

The following Communication Manager Class of Restriction display shows COR 6 (page 1). This COR has a Facility Restriction Levels (FRL) value of 0. Facility Restriction Levels are ranked from 0 to 7, where 7 has the highest level of privileges. FRL 0 is the default lowest level for resources that use FRLs. This separates Avaya Aura® Call Center Elite agents with a COR value of 6 and a FRL value of 0 from Contact Center resources with a FRL value of 1. Avaya Aura® Call Center Elite agents cannot communicate with Contact Center agents or use Contact Center trunks.

```
display cor 6                                                Page   1 of  23
                              CLASS OF RESTRICTION

                 COR Number: 6
           COR Description: Restricted COR Elite Agents

                       FRL: 0                                     APLT? y
  Can Be Service Observed? n                Calling Party Restriction: outward
Can Be A Service Observer? n                 Called Party Restriction: none
        Time of Day Chart: 1              Forced Entry of Account Codes? n
         Priority Queuing? n                        Direct Agent Calling? n
     Restriction Override: none            Facility Access Trunk Test? n
     Restricted Call List? n                      Can Change Coverage? n

            Access to MCT? y                  Fully Restricted Service? n
Group II Category For MFC: 7                  Hear VDN of Origin Annc.? n
         Send ANI for MFE? n                   Add/Remove Agent Skills? n
            MF ANI Prefix:                     Automatic Charge Display? n
Hear System Music on Hold? y    PASTE (Display PBX Data on Phone)? n
                          Can Be Picked Up By Directed Call Pickup? n
                                       Can Use Directed Call Pickup? n
                                       Group Controlled Restriction: inactive
```

The following Communication Manager Class of Restriction display shows COR 6 (page 4). This display shows that Elite agent profiles with a COR value of 6 are restricted from accessing system resources with a COR value of 5 or 7. Avaya Aura® Contact Center agent station have a COR value of 7. The Session Manager to Communication Manager trunk used for Avaya Aura® Contact Center CDN calls has a COR value of 5. Therefore Elite agents cannot access or communicate with these Avaya Aura® Contact Center resources.

```
display cor 6                                                Page   4 of  23
                                CLASS OF RESTRICTION

CALLING PERMISSION (Enter "y" to grant permission to call specified COR)

  0? y      15? y      30? y      44? y      58? y      72? y      86? y
  1? y      16? y      31? y      45? y      59? y      73? y      87? y
  2? y      17? y      32? y      46? y      60? y      74? y      88? y
  3? y      18? y      33? y      47? y      61? y      75? y      89? y
  4? y      19? y      34? y      48? y      62? y      76? y      90? y
  5? n      20? y      35? y      49? y      63? y      77? y      91? y
  6? y      21? y      36? y      50? y      64? y      78? y      92? y
  7? n      22? y      37? y      51? y      65? y      79? y      93? y
  8? y      23? y      38? y      52? y      66? y      80? y      94? y
  9? y      24? y      39? y      53? y      67? y      81? y      95? y
 10? y      25? y      40? y      54? y      68? y      82? y      96? y
 11? y      26? y      41? y      55? y      69? y      83? y      97? y
 12? y      27? y      42? y      56? y      70? y      84? y      98? y
 13? y      28? y      43? y      57? y      71? y      85? y      99? y
 14? y      29? y
```

Changing the Contact Center trunk group Class of Restriction details

Before you begin

- Create the Communication Manager to Session Manager trunk group used for Avaya Aura® Contact Center calls.

About this task

Edit the Class of Restriction (COR) value used by the Contact Center trunk to separate the trunk from Avaya Aura® Call Center Elite agents.

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to change the Contact Center trunk COR permissions. Use the **`change cor n`** command.

   For example, enter **`change cor 5`**.

2. Change the COR permissions to separate the Contact Center trunk group from Avaya Aura® Call Center Elite agents.

Example

The following Communication Manager Class of Restriction display shows COR 5 (page 1). This COR has a Facility Restriction Levels (FRL) value of 1. Facility Restriction Levels are ranked from 0 to 7, where 7 has the highest level of privileges. Only Communication Manager users (agents) with a FRL of 1 or higher can access resources controlled by this COR value. This separates Avaya Aura® Call Center Elite agents with a COR value of 6 and a FRL value of 0 from the Contact Center trunk group.

```
display cor 5                                                Page   1 of  23
                              CLASS OF RESTRICTION

                   COR Number: 5
            COR Description: Restricted trunk Elite to AACC ret

                        FRL: 1                                  APLT? y
  Can Be Service Observed? n                Calling Party Restriction: outward
Can Be A Service Observer? n                 Called Party Restriction: none
        Time of Day Chart: 1              Forced Entry of Account Codes? n
         Priority Queuing? n                        Direct Agent Calling? n
     Restriction Override: none             Facility Access Trunk Test? n
     Restricted Call List? n                        Can Change Coverage? n

            Access to MCT? y                    Fully Restricted Service? n
Group II Category For MFC: 7                    Hear VDN of Origin Annc.? n
         Send ANI for MFE? n                     Add/Remove Agent Skills? n
            MF ANI Prefix:                      Automatic Charge Display? n
Hear System Music on Hold? y          PASTE (Display PBX Data on Phone)? n
                                Can Be Picked Up By Directed Call Pickup? n
                                           Can Use Directed Call Pickup? n
                                           Group Controlled Restriction: inactive
```

Changing the Class of Restriction value of the Contact Center trunk group

Before you begin

- Create the Communication Manager to Session Manager trunk group used for Avaya Aura® Contact Center calls.

About this task

Change the Avaya Aura® Contact Center trunk group Class of Restriction (COR) value to separate the Contact Center trunk from the Avaya Aura® Call Center Elite agents.

This example trunk group 5 directs all voice traffic intended for the Avaya Aura® Contact Center CDNs. Avaya recommends that you give Avaya Aura® Contact Center trunk groups their own COR settings so that there is minimal disruption on all other trunk groups on the existing

Communication Manager. The trunk group used by Avaya Aura® Contact Center must be “outgoing” from Communication Manager.

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to change the Avaya Aura® Contact Center trunk group COR value. Use the **`change trunk-group n`** command.

   For example, enter **`change trunk-group 5`**.

2. Change the COR value to separate the Contact Center trunk group from Avaya Aura® Call Center Elite agents.

Example

The following Communication Manager trunk group display shows the Contact Center trunk group configured with a Class of Restriction value of 5. This COR value separates this Contact Center trunk group from Avaya Aura® Call Center Elite agents with a COR value of 6. This trunk group is configured with an “outgoing” direction.

```
display trunk-group 5                                        Page   1 of  21
                              TRUNK GROUP

Group Number: 5                    Group Type: sip           CDR Reports: y
  Group Name: TG to SM for CDN Restricted COR: 5        TN: 1        TAC: *05
   Direction: outgoing       Outgoing Display? n
 Dial Access? n
Queue Length: 0
Service Type: tie
                                          Member Assignment Method: auto
                                                   Signaling Group: 5
                                                 Number of Members: 255
```

Changing the Contact Center route pattern Facility Restriction Levels

Before you begin

- Create the Avaya Aura® Contact Center route pattern as normal. For more information about configuring route patterns, see Configuring a route pattern on page 49.

About this task

Change the Avaya Aura® Contact Center route pattern to use a Facility Restriction Levels (FRL) value that separates Contact Center from Avaya Aura® Call Center Elite agents.

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to change the Contact Center route pattern Facility Restriction Levels (FRL) value. Use the **`change route-pattern n`** command.

   For example, enter **`change route-pattern 5`**.

2. Change the Facility Restriction Levels (FRL) value to separate the Contact Center route pattern from Avaya Aura® Call Center Elite agents.

Example

The following Communication Manager route pattern display shows route pattern 5 (page 1). This route pattern has a Facility Restriction Levels (FRL) value of 1. Facility Restriction Levels are ranked from 0 to 7, where 7 has the highest level of privileges. Only Communication Manager users (agents) with a FRL of 1 or higher can access resources controlled by this FRL value. This separates Avaya Aura® Call Center Elite agents with a COR value of 6 and a FRL value of 0 from the Contact Center trunk.

```
display route-pattern 5                                          Page   1 of   3
                     Pattern Number: 5   Pattern Name: Restricted CDN
                                SCCAN? n     Secure SIP? n
    Grp  FRL NPA Pfx Hop Toll No.   Inserted                              DCS/  IXC
    No       Mrk Lmt List Del   Digits                                  QSIG
                            Dgts                                        Intw
1:  5    1                                                               n    user
2:                                                                       n    user
3:                                                                       n    user
4:                                                                       n    user
5:                                                                       n    user
6:                                                                       n    user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
1:  y y y y y n  n            rest                                      none
2:  y y y y y n  n            rest                                      none
3:  y y y y y n  n            rest                                      none
4:  y y y y y n  n            rest                                      none
5:  y y y y y n  n            rest                                      none
6:  y y y y y n  n            rest                                      none
```

To use the FRL features you must ensure that the Automatic Alternate Routing (AAR) settings are correct. In our example the Avaya Aura® Contact Center CDNs are defined as 3174XXX and when they are dialed on the Avaya Aura® Communication Manager, it uses route pattern 5. Route pattern 5 is covered by FRL level 1, so calls to the Avaya Aura® Contact Center CDNs are separated from Avaya Aura® Call Center Elite agents with a FRL level of 0.

```
display aar analysis 0                                       Page   1 of   2
                         AAR DIGIT ANALYSIS TABLE
                                 Location: all            Percent Full: 1

      Dialed             Total      Route    Call    Node   ANI
      String           Min   Max   Pattern   Type    Num    Reqd
  3172                 7     7     1         aar            n
  3173                 7     7     1         aar            n
  3174                 7     7     5         aar            n
  3175                 7     7     1         aar            n
  5                    7     7     999       aar            n
  6                    7     7     999       aar            n
  7                    7     7     999       aar            n
  8                    7     7     999       aar            n
  9                    7     7     999       aar            n
                                                            n
                                                            n
                                                            n
                                                            n
                                                            n
                                                            n
```

Chapter 11: Fallback to Avaya Aura® Call Center Elite skill configuration

In solutions where Avaya Aura® Contact Center shares the same Avaya Aura® Communication Manager as an Avaya Aura® Call Center Elite deployment, you can configure the solution to manually reroute customer voice contacts to Elite if Avaya Aura® Contact Center is offline or stopped for maintenance.

The Avaya Aura® Contact Center fallback to Avaya Aura® Call Center Elite method described in this example solution uses Communication Manager vectors, Vector Directory Numbers, and a vector variable. You must complete all the procedures in this section in sequential order.

Vectors: A Communication Manager vector is a series of commands that program the system to handle incoming calls. A vector contains a number of steps and allows customized call routing and treatments. For example, you can use a vector to play multiple announcements, route calls to internal and external destinations, and collect and respond to dialed information. The vector follows the commands in each vector step in order. The vector interprets each step and follows the commands in that step if the conditions are correct. If the command cannot be followed, the vector skips the step and reads the next step. Communication Manager handles calls based on a number of conditions, including the number of calls in a queue, how long a call has been waiting, the time of day, the day of the week, and changes in call traffic or staffing conditions.

Vector Directory Numbers: A Vector Directory Number (VDN) is an extension that directs an incoming call to a specific vector. This number is a logical or virtual extension number not assigned to a physical location. VDNs must follow your dial plan. For example, you can create a VDN 2233 for your sales department. A call into 2233 routes to vector 11. This vector plays an announcement and queues calls to the sales department.

Vectors variables: Vectors can use vector variables to provide increased manager and application control over call treatments. The vector variables are defined in a central variable administration table. Values assigned to some types of variables can also be quickly changed by means of special vectors, Vector Directory Numbers (VDNs), or Feature Access Codes (FACs) that you administer specifically for that purpose. Depending on the variable type, variables can use either call-specific data or fixed values that are identical for all calls. In either case, an administered variable can be reused in many vectors.

You can configure your solution to manually reroute customer calls to Avaya Aura® Call Center Elite if Avaya Aura® Contact Center is offline or stopped for maintenance. This vector variable fallback technique is manually controlled by a contact center supervisor or administrator with the correct level of access to the solution components. The supervisor can manually reroute Contact Center

calls to a fallback VDN. This VDN then routes calls to a hunt group, split extensions or Elite skill extensions. Avaya recommends using a single fallback VDN.

To implement Contact Center fallback to Elite you must configure the following Communication Manager resources:

- VDN and associated vector which allows a supervisor to dial in and set value of a fallback vector variable. This vector is used to *configure* whether Communication Manager reroutes calls intended for Contact Center to Elite or not.
- VDN and associated vector which routes calls either to Avaya Aura® Contact Center or Avaya Aura® Call Center Elite depending on the value of the fallback vector variable. This vector is used to *control* whether Communication Manager reroutes voice contacts intended for Contact Center to Elite or not.

If Avaya Aura® Contact Center is operational and processing voice contacts as normal, the value of the vector variable is set to one (1). If Avaya Aura® Contact Center is offline or stopped for maintenance. the value of the vector variable is set to zero (0). The vector variable is manually set by the supervisor or administrator according to the operational state of the Avaya Aura® Contact Center.

To redirect Avaya Aura® Contact Center calls to Avaya Aura® Call Center Elite, a supervisor dials a Vector Directory Number (VDN). The vector associated with this VDN is programmed with a number of vector commands. In this worked example the *configuration* vector uses a series of announcements to allow the supervisor to change the value of a global vector variable. To reroute Contact Center calls to Elite, the supervisor changes the value of the vector variable to zero.

All incoming voice contacts destined for Avaya Aura® Contact Center flow through another dedicated Communication Manager VDN and associated vector. This *control* vector checks the state of the global vector variable. If the value of the variable is one, then the vector routes the call onto Avaya Aura® Contact Center as normal. If the value of the variable is zero, then the call is routed to either a hunt group, a split extension or an Elite skill. Split extensions and Elite skills require Avaya Aura® Communication Manager and Avaya Aura® Call Center Elite licenses.

The following diagram illustrates how a supervisor manually reroutes Avaya Aura® Contact Center voice contacts to an Avaya Aura® Call Center Elite skill.

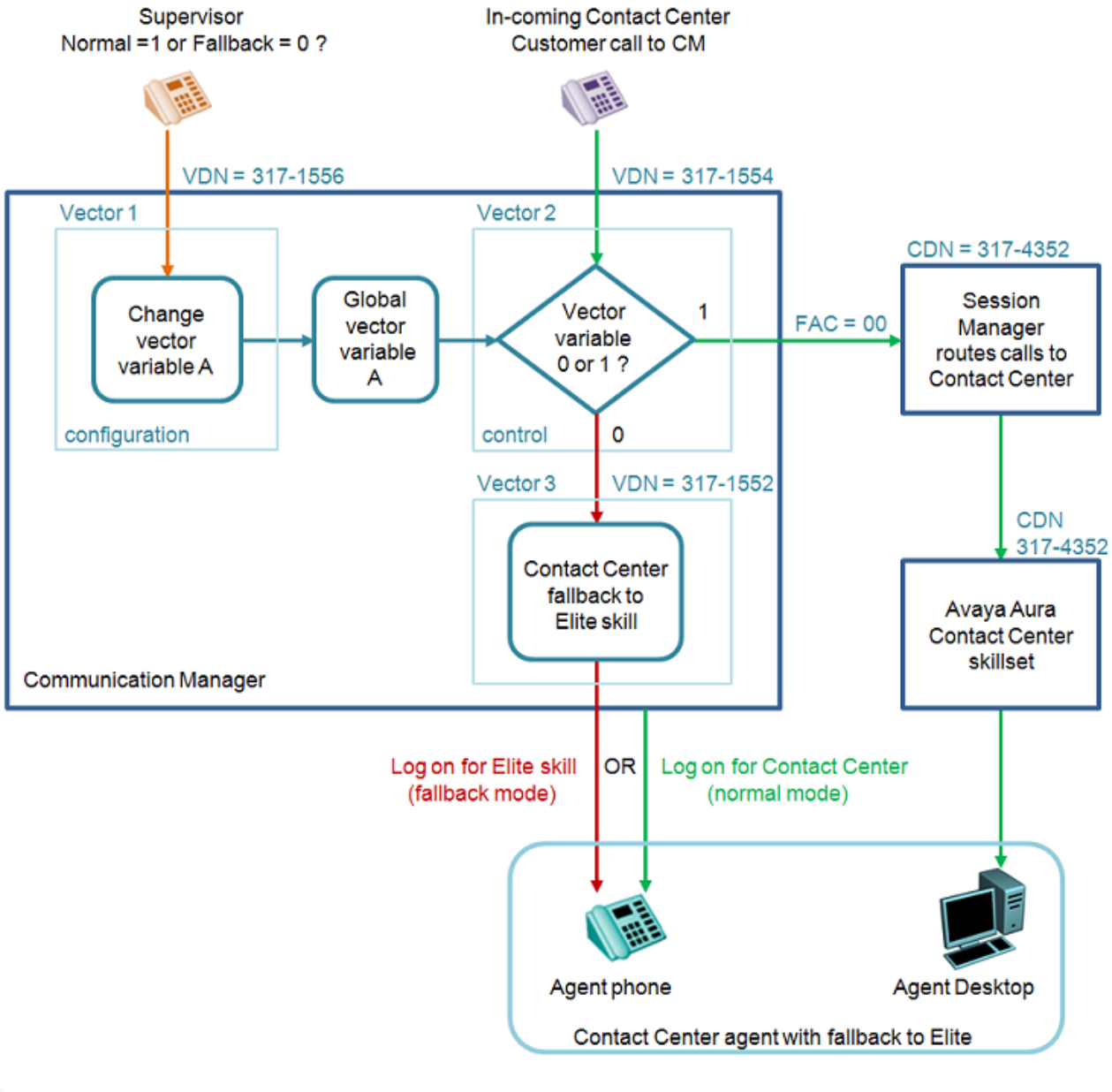


Figure 25: Example of a how a supervisor manually reroutes Avaya Aura® Contact Center voice contacts to an Avaya Aura® Call Center Elite skill

In the event of an Avaya Aura® Contact Center outage, the supervisor can choose to reroute Avaya Aura® Contact Center voice contacts to an Avaya Aura® Call Center Elite skill.

Adding support for Elite functionality on Avaya Aura® Contact Center stations

To support this fallback to an Avaya Aura® Call Center Elite skill method you must configure Contact Center agent stations with the ability to log on to a fallback Avaya Aura® Call Center Elite skill. You must therefore program Avaya Aura® Contact Center agent stations with the Avaya Aura® Call Center Elite login, logout, and aux feature buttons.

Fallback to Avaya Aura® Contact Center agent stations

You can use the same agent phones for both Avaya Aura® Contact Center and Avaya Aura® Call Center Elite, but not at the same time. Agents can log on to a phone to handle either Avaya Aura® Contact Center voice contacts or Elite voice contacts. Typically, Avaya Aura® Contact Center agents log on to Avaya Agent Desktop and their desk phone while Avaya Aura® Call Center Elite agents log on to One-X Agent and their desk phone.

If the supervisor changes the solution to route Avaya Aura® Contact Center voice contacts to a fallback Elite skill, Avaya Aura® Contact Center agents must log off from Avaya Agent Desktop, and then log on to the fallback Elite skill. The Avaya Aura® Contact Center voice contacts are then routed to a fallback Elite skill, the Avaya Aura® Contact Center agents are now logged on to their phones in an Elite skill and they can continue to use their domain knowledge to handle customers calls intended for Avaya Aura® Contact Center.

You must program the telephone stations that are used for normal Avaya Aura® Contact Center operation with the feature buttons required to log on to the Avaya Aura® Call Center Elite fallback skill. The additional Avaya Aura® Call Center Elite station buttons are supported only during fallback mode. They are not supported during normal Avaya Aura® Contact Center operation.

In order to handle fallback calls, Contact Center agents must login to an Elite fallback skill. Avaya Aura® Contact Center agents stations must therefore be programmed with the following feature buttons:

- auto-in
- manual-in
- aux-work
- release
- after-call

These feature buttons are supported only when the agent stations are used to handle Elite voice contacts. Agents who normally handle voice contacts from Avaya Aura® Call Center Elite already have these programmed as standard. Agents who normally handle voice contacts from Avaya Aura® Contact Center must have these programmed to support fallback to Elite. A standard station template suitable for fallback operation can be rolled out across the contact center for pre and post fallback modes.

For more information about the supported feature buttons, see Contact Center agent desk phone supported features on page 24.

In the event of failure of the Avaya Aura® Contact Center application, supervisors must direct all Avaya Aura® Contact Center agents to first log out of Avaya Aura® Contact Center and then log on to the Avaya Aura® Call Center Elite fallback skill using the additional buttons on their physical station.

Three important steps that must be followed for support of the vector variable fallback solution:

- Avaya Aura® Contact Center agents that wish to handle fallback voice contacts from the Avaya Aura® Call Center Elite application must first logout of Avaya Agent Desktop as logging on to both applications simultaneously is not supported.
- Only Avaya Aura® Contact Center agents that use a physical station can handle voice contacts in a fallback mode. Agents that use the embedded H.323 Softphone might not have full functionality depending on the nature of the failure in the contact center.

- The above two requirements do not apply to Avaya Aura® Call Center Elite agents that handle fallback voice contacts.

Prerequisites

Separate Avaya Aura® Contact Center and Avaya Aura® Call Center Elite on the same Avaya Aura® Communication Manager. For more information about separating Avaya Aura® Contact Center and Avaya Aura® Call Center Elite, see Avaya Aura Call Center Elite and Avaya Aura Contact Center configuration on page 146.

Configuring the announcements

About this task

Record and configure announcements to inform the contact center supervisor about the current Avaya Aura® Contact Center routing state (fallback or normal). Record and configure the following announcements types:

- An announcement to inform the supervisor that Avaya Aura® Contact Center calls are routing as normal.
- An announcement to inform the supervisor that Avaya Aura® Contact Center calls are being rerouted to Avaya Aura® Call Center Elite.
- An announcement to ask the supervisor if they wish to change the fallback state.

A minimum of three announcements are required, but you can add additional announcements to improve the supervisor's experience. You must record announcements before you use them in a vector. For more information about recording announcements, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to configure a gateway for announcements. Use the **`change media-gateway n`** command.
2. Use the **`add announcement x`** command to configure announcements.

Example

The following Communication Manager display shows an example of configuring a gateway for announcements.

```
display media-gateway 1                                    Page   2 of   2
                            MEDIA GATEWAY 1

                                Type: g450

Slot    Module Type             Name                    DSP Type  FW/HW version
 V1:                                                    MP80      44    6
 V2:
 V3:
 V4:
 V5:
 V6:
 V7:
 V8:                                                Max Survivable IP Ext: 8
 V9:    gateway-announcements   ANN VMM
```

The following Communication Manager display shows an example of configuring three announcements.

```
list announcement

                          ANNOUNCEMENTS/AUDIO SOURCES
Announcement                                                 Source      Num of
Extension             Type       Name                    Pt/Bd/Grp     Files
317-1900              integrated Failback1                 001V9         1
317-1901              integrated Second                    001V9         1
317-1902              integrated Variablechangeto0         001V9         1
```

```
Command successfully completed
Command:
```

Configuring a fallback global vector variable

About this task

This example solution uses two vectors to configure and control the fallback state of Avaya Aura® Contact Center. The first vector allows a supervisor to dial a Communication Manager phone number and change the value of a global vector variable. This first vector is used to *configure* the value of a global vector variable. The second vector uses the value of this global vector variable to *control* the fallback state of Avaya Aura® Contact Center.

If the value of this global vector variable is one, voice contacts intended for Avaya Aura® Contact Center are routed to Avaya Aura® Contact Center. If the value of this vector variable is zero, voice contacts intended for Avaya Aura® Contact Center are routed to Avaya Aura® Call Center Elite.

Assign any unused vector variable for use by the two fallback (*configure* and *control*) vectors. This example uses vector variable A. This vector variable is initialized with a value of 1 indicating that voice contacts intended for Avaya Aura® Contact Center are routed to Avaya Aura® Contact Center.

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to configure a global vector variable. Use the **`change variables`** command.
2. Change the **Scope** value of variable A to be global and assign it an initial value of 1.

Example

The following Communication Manager display shows vector variable A configured with a global scope and an initial value of 1.

```
display variables                                          Page   1 of  39
                              VARIABLES FOR VECTORS

Var Description                 Type    Scope Length Start Assignment       VAC
A   Used for AACC failover      collect G     1      1     1
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
```

Configuring the fallback configuration vector

Before you begin

- Configure and assign a global vector variable. For more information about configuring a global vector variable, see Configuring a fallback global vector variable on page 169.
- Configure three announcements. For more information about configuring announcements, see Configuring the announcements on page 167.

About this task

This example solution uses two vectors to configure and control the fallback state of Avaya Aura® Contact Center. This first vector is used to *configure* the value of the global vector variable. The first vector allows a supervisor to dial a Communication Manager phone number and change the value of a global vector variable.

If the value of this global vector variable is one, voice contacts intended for Avaya Aura® Contact Center are routed to Avaya Aura® Contact Center. If the value of this vector variable is zero, voice contacts intended for Avaya Aura® Contact Center are routed to Avaya Aura® Call Center Elite.

The following table illustrates the vector commands used by the fallback configuration vector. The comment column is not part of the vector code, it is shown here to explain each vector step.

Step	Command			Comment
01	wait-time	2	secs hearing ringback	Give ringback.
02	goto step	13	if A = 1	If the global vector variable A is initially set to one, use an announcement to inform the supervisor that vector variable A has a value of one and Avaya Aura® Contact Center CDN calls are routing normally.
03	goto step	16	if A = 0	If the global vector variable A is initially set to zero, use an announcement to inform the supervisor that vector variable A has a value of zero and Avaya Aura® Contact Center CDN calls are routing to Elite.
04	collect	1	digits after announcement 3171902 for none	Use an announcement to ask the supervisor to enter a digit value to change the vector variable. The collected digit is stored in “digits”.
05	goto step	9	if A = 1	If the global vector variable A changes value to one, use an announcement to inform the supervisor that vector variable A has a value of one and Avaya Aura® Contact Center CDN calls are routing normally.
06	goto step	11	if A = 0	If the global vector variable A changes value to zero, use an announcement to inform the supervisor that vector variable A has a value of zero and Avaya Aura® Contact Center CDN calls are routing to Elite.
07	goto step	4	if unconditionally	Main loop, wait for supervisor to enter digit.
08	stop			
09	set		A = digits CATL 1	Concatenate on the left, set A equal the value of the above collected digit + 1.
10	disconnect		after announcement 3171901	Use an announcement to inform the supervisor that vector variable A has a value of one and Avaya Aura® Contact Center CDN calls are routing normally.
11	set		A = digits CATL 0	Concatenate on the left, set A equal the value of the above collected digit + 0.
12	disconnect		after announcement 3171900	Use an announcement to inform the supervisor that vector variable A has a value of zero and Avaya Aura® Contact Center CDN calls are routing to Elite.
13	announcem ent		3171901	Tell the supervisor that A is set to one, normal operation.
14	goto step	4	if unconditionally	Return to ask if the supervisor wants to change this.
15	stop			

Table continues…

Step	Command			Comment
16	announcement		3171900	Tell the supervisor that A is set to zero, fallback operation.
17	goto step	4	if unconditionally	Return to ask if the supervisor wants to change this.
18	stop			

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to change Vector 1 to be a fallback configuration vector. Use the **`change vector n`** command.

   For example, enter **`change vector 1`**.

2. Modify the vector steps and commands to use announcements and a supervisor digit input to configure the value of a global vector variable A. This global vector variable A is used to control the fallback state of Avaya Aura® Contact Center.

Example

The following Communication Manager display shows some of the commands for the example fallback configuration vector, vector 1.

```
display vector 1                                          Page   1 of   6
                                CALL VECTOR

    Number: 1                Name: flv dialin
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y    Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 goto step    13            if A                =      1
03 goto step    16            if A                =      0
04 collect      1    digits after announcement 3171902  for none
05 goto step    9             if digits           =      1
06 goto step    11            if digits           =      0
07 goto step    4             if unconditionally
08 stop
09 set          A      = digits CATL  1
10 disconnect   after announcement 3171901
11 set          A      = digits CATL  0
12 disconnect   after announcement 3171900

                      Press 'Esc f 6' for Vector Editing
```

The following Communication Manager display shows the remaining commands for the example fallback configuration vector, vector 1.

```
display vector 1                                          Page   2 of   6
                                  CALL VECTOR
13 announcement 3171901
14 goto step    4             if unconditionally
15 stop
16 announcement 3171900
17 goto step    4             if unconditionally
18 stop
19
20
21
22
23
24
25
26
27
28
29
30
31
32
```

Configuring the fallback configuration Vector Directory Number

Before you begin

- Configure the fallback configuration vector. For more information, see Configuring the fallback configuration vector on page 170.

About this task

Configure a Vector Directory Number (VDN) to access the fallback configuration vector. The contact center supervisor dials this VDN to access the fallback configuration vector and change the Avaya Aura® Contact Center fallback state.

This example solution uses a vector to configure the value of a global vector variable. This fallback configuration vector allows a supervisor to dial a Communication Manager phone number and change the value of a global vector variable. The value of this global vector variable is later used to control the Avaya Aura® Contact Center fallback state, and reroute CDN calls if necessary.

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to change Vector 1 to be a fallback configuration vector. Use the **`change vdn n`** command.

For example, enter **change vector 3171556**.

2. Modify the **Destination** to be Vector Number 1.

Example

The following Communication Manager display shows Vector Directory Number 3171556. Calls to this VDN 3171556 are routed to vector 1 for treatment and/or processing. In this example vector 1 is used to configure the Avaya Aura® Contact Center fallback state.

```
display vdn 3171556                                          Page   1 of   3
                          VECTOR DIRECTORY NUMBER

                            Extension: 317-1556
                                Name*: VVariableAssignment
                          Destination: Vector Number        1
                  Attendant Vectoring? n
                Meet-me Conferencing? n
                  Allow VDN Override? n
                                COR: 1
                                TN*: 1
                           Measured: none


        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:



* Follows VDN Override Rules
```

Configuring Feature Access Codes for Auto Alternate Routing

About this task

Configure Feature Access Codes (FACs) to enable the Auto Alternate Routing (AAR) access code “00” which is used by the fallback control vector. This FAC code is used with Auto Alternate Routing to route customer calls to Avaya Aura® Contact Center. This example uses “00” , but you can use any unused access code that meets your dial plan.

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to change the Feature Access Codes for AAR access. Use the **change feature-access-codes** command.

2. Modify the **Auto Alternate Routing (AAR) Access Code** to be 00.

Example

The following Communication Manager display shows the Feature Access Codes with Auto Alternate Routing (AAR) Access Code configured.

```
display feature-access-codes                                  Page   1 of  10
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *89
         Abbreviated Dialing List2 Access Code: *88
         Abbreviated Dialing List3 Access Code: *87
Abbreviated Dial - Prgm Group List Access Code: *86
                      Announcement Access Code: *19
                       Answer Back Access Code:

      Auto Alternate Routing (AAR) Access Code: *00
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                  Automatic Callback Activation:       Deactivation:
Call Forwarding Activation Busy/DA:        All:       Deactivation:
   Call Forwarding Enhanced Status:        Act:       Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
             Conditional Call Extend Activation:       Deactivation:
                   Contact Closure   Open Code:         Close Code:
```

Configuring the fallback control vector

Before you begin

- Configure and assign a global vector variable.

About this task

This example solution uses two vectors to configure and control the fallback state of Avaya Aura® Contact Center. This second vector is used to *control* the Avaya Aura® Contact Center fallback state.

If the value of the global vector variable A is one, this fallback control vector routes voice contacts intended for Avaya Aura® Contact Center to an Avaya Aura® Contact Center CDN.

If the value of the global vector variable A is zero, this fallback control vector routes voice contacts intended for Avaya Aura® Contact Center to an Avaya Aura® Call Center Elite VDN.

The following table illustrates the vector commands used by the fallback control vector. The comment column is not part of the vector code, it is shown here to explain each vector step.

Step	Command			Comment
01	wait-time	2	secs hearing ringback	Give ringback.
02	goto step	6	if A = 0	
03	route-to		number *003174352 with cov y if unconditionally	If the value of the global vector variable A is one, route calls intended for Avaya Aura® Contact Center to this Avaya Aura® Contact Center CDN. The Avaya Aura® Contact Center CDN 3174352 is accessed using FAC 00.
04	goto step	2	if unconditionally	
05	stop			
06	route-to		number 3171552 with cov y if unconditionally	If the value of the global vector variable A is zero, route calls intended for Avaya Aura® Contact Center to this Avaya Aura® Call Center Elite VDN.
07	wait-time	2	secs hearing silence	
08	goto step	6	if unconditionally	

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to change Vector 2 to be a fallback control vector. Use the **`change vector n`** command.

   For example, enter **`change vector 2`**.

2. Modify the vector steps and commands to use the value of the global vector variable A to control the routing of Avaya Aura® Contact Center voice contacts.

Example

The following Communication Manager display shows the commands for the example fallback control vector.

```
display vector 2                                          Page   1 of   6
                                CALL VECTOR

    Number: 2                Name: Flvr 2 Elite Sk
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n            Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 goto step    6             if A                =      0
03 route-to     number *003174352       with cov y if unconditionally
04 goto step    2             if unconditionally
05 stop
06 route-to     number 3171552          with cov y if unconditionally
07 wait-time    2   secs hearing silence
08 goto step    6             if unconditionally
09
10
11
12

                        Press 'Esc f 6' for Vector Editing
```

Configuring the fallback control Vector Directory Number

Before you begin

- Configure the fallback control vector. For more information, see Configuring the fallback control vector on page 175.

About this task

Configure a Vector Directory Number (VDN) to access the fallback control vector. All calls intended for Avaya Aura® Contact Center are routed through this VDN and onto the associated control vector, Vector 2.

This second vector is used to *control* the Avaya Aura® Contact Center fallback state. If the value of the global vector variable A is one, this fallback control vector routes voice contacts intended for Avaya Aura® Contact Center to an Avaya Aura® Contact Center CDN. If the value of the global vector variable A is zero, this fallback control vector routes voice contacts intended for Avaya Aura® Contact Center to an Avaya Aura® Call Center Elite VDN.

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to change Vector 2 to be a fallback control vector. Use the **`change vdn n`** command.

For example, enter **change vdn 3171554**.

2. Modify the **Destination** to be Vector Number 2.

Example

The following Communication Manager display shows Vector Directory Number 3171554. Calls to this VDN 3171554 are routed to Vector 2 for treatment and/or processing.

```
display vdn 3171554                                          Page   1 of   3
                          VECTOR DIRECTORY NUMBER

                            Extension: 317-1554
                                 Name*: Failover
                          Destination: Vector Number        2
                  Attendant Vectoring? n
                Meet-me Conferencing? n
                  Allow VDN Override? n
                                 COR: 1
                                 TN*: 1
                            Measured: none


      VDN of Origin Annc. Extension*:
                          1st Skill*:
                          2nd Skill*:
                          3rd Skill*:



* Follows VDN Override Rules
```

Configuring an Elite fallback vector

About this task

Configure a vector to route calls to an Elite skill. The vector in this example routes all incoming calls to skill 1.

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to change Vector 3 to be a fallback configuration vector. Use the **change vector n** command.

   For example, enter **change vector 3**.

2. Modify the vector steps and commands to route all incoming calls to skill 1.

Example

The following Communication Manager display shows the commands for the example Elite fallback vector.

```
display vector 3                                                Page   1 of   6
                                  CALL VECTOR

    Number: 3                Name: cecvector1
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n            Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y    Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    5   secs hearing ringback
02 queue-to     skill 1    pri m
03 goto step    2              if unconditionally
04
05
06
07
08
09
10
11
12

                          Press 'Esc f 6' for Vector Editing
```

Configuring an Elite fallback Vector Directory Number

Before you begin

- Configure the Elite fallback vector. For more information, see Configuring an Elite fallback vector on page 178.

About this task

Configure a Vector Directory Number (VDN) to access the Elite fallback vector. If the value of the global vector variable A is zero, Vector 2 routes voice contacts intended for Avaya Aura® Contact Center to this Avaya Aura® Call Center Elite VDN. This VDN then routes the calls to Vector 3.

Procedure

1. On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to change Vector 3 to be a fallback control vector. Use the **`change vdn n`** command.

   For example, enter **`change vdn 3171552`**.

2. Modify the **Destination** to be Vector Number 3.

Example

The following Communication Manager display shows Vector Directory Number 3171552. Calls to this VDN 3171552 are routed to Vector 3 for treatment and/or processing.

```
display vdn 3171552                                          Page   1 of   3
                          VECTOR DIRECTORY NUMBER

                            Extension: 317-1552
                                 Name*: cec3171552vdn
                          Destination: Vector Number        3
                  Attendant Vectoring? n
                Meet-me Conferencing? n
                  Allow VDN Override? n
                                COR: 6
                                TN*: 1
                           Measured: none


        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:



* Follows VDN Override Rules
```

Chapter 12: Coverage Path configuration

Avaya Aura® Contact Center supports a limited configuration of Coverage Path to allow agent stations to have voice message boxes on a Communication Manager PABX. This configuration applies only to Avaya voice messaging systems connected to Communication Manager using the SIP protocol. Avaya Aura® Contact Center does not support Avaya voice messaging systems using other protocols, such as QSIG, or third-party voice mail systems.

Functionality Supported

This solution supports the following voice messaging platforms and configurations (only with SIP integration to Communication Manager using Session Manager):

- Modular Messaging 5.2
- Avaya Aura® Messaging
- Communication Manager Messaging
- Avaya IX Messaging

This solution supports only:

- a single coverage path configured on the agent's station
- a Coverage Path Group configured with a single coverage point to a voice mail Hunt Group (i.e., the Hunt Group has only one entry, the entry for the voice messaging system)
- coverage for Busy & Don't Answer for calls directly to the agent's DN

Functionality Not Supported

This solution does not support:

- third party voice mail messaging platforms
- QSIG integrations between Communication Manager and the voice messaging system
- Coverage Path for calls routed with the "QUEUE TO SKILLSET" and "QUEUE TO AGENT" commands – Avaya Aura® Contact Center must always maintain control of these calls and reroute to the next available agent
- the following Coverage Path functionality:
  - DND / SAC (Send All Calls)/Go to Cover keys
  - multiple coverage points
  - coverage points other than voice messaging Hunt Group

Note:

Agent stations must not cover back to Avaya Aura® Contact Center. This configuration is not supported and if configured, it adversely impacts the operation of the contact center. This scenario is handled by Avaya Aura® Contact Center without the need for Communication Manager configuration.

Avaya Aura® Contact Center Call Presentation Class configuration

When you configure the Coverage Path Group on the Communication Manager, the **Number of Rings** setting for **Don't Answer?** must be greater than the agent's Avaya Aura® Contact Center Call Presentation Class Return to Queue or Call Force Delay timer. This ensures that Avaya Aura® Contact Center maintains control of a customer call which it has queued to an agent who does not answer the call for any reason. If there are other agents available in the skillset who can handle the customer call, it is better for Avaya Aura® Contact Center to re-queue the call to a different agent than for that call to go to the first agent's voice mail. This also ensures that the customer call does not go to an agent's voice mail before the call has been force answered.

The following table illustrates each **Number of Rings** setting for **Don't Answer?**, and the corresponding value you must configure for your Call Presentation Class Return to Queue or Call Force Delay timer.

Number of Rings setting for Don't answer?	AACC Call Presentation Class Return to Queue/Call Force Delay timer (in seconds)
1	RTQ or CFD timer equal to or less than 5
2	RTQ or CFD timer equal to or less than 10
3	RTQ or CFD timer equal to or less than 15
4	RTQ or CFD timer equal to or less than 20
5	RTQ or CFD timer equal to or less than 25

Note:

The Number of Rings setting is country specific and can vary depending on your location. The example values included in the table above were calculated using the default Communication Manager values.

Configuring the Hunt Group

Before you begin

Add a Communication Manager Hunt Group. For more information, see Adding a Hunt Group on page 130.

About this task

Configure a Hunt Group to use the voice mail number.

Procedure

1. Use the Communication Manager — System Access Terminal (SAT) interface **change hunt-group** command to configure the Hunt Group.

```
display hunt-group 4                                    Page   1 of   60
                                   HUNT GROUP

               Group Number: 4                                   ACD? n
                 Group Name: msgserver                         Queue? n
            Group Extension: 19998                            Vector? n
                 Group Type: ucd-mia                    Coverage Path:
                         TN: 1              Night Service Destination:
                        COR: 1                        MM Early Answer? n
              Security Code:                    Local Agent Preference? n
    ISDN/SIP Caller Display:
```

2. Configure the Hunt Group to use the voice mail number, for example 32000.

```
display hunt-group 4                                    Page   2 of   60
                                   HUNT GROUP



                        Message Center: sip-adjunct

Voice Mail Number         Voice Mail Handle          Routing Digits
                                                  (e.g., AAR/ARS Access Code)
32000                     cmm
```

In this example of Hunt Group 4, 32000 is a number that the Communication Manager dial plan routes to Session Manager, which routes it to Communication Manager Messaging (CMM).

Configuring the Coverage Path Group

Before you begin

Configure the Hunt Group. See Configuring the Hunt Group on page 182.

About this task

Configure a Coverage Path Group with a single coverage point.

Procedure

1. Use the Communication Manager — System Access Terminal (SAT) interface **add coverage path** command to add a new Coverage Path Group.
2. Set the value of Point1 to h4, the Hunt Group that routes calls to the voice mail system. See Configuring the Hunt Group on page 182.
3. Set the value of the **Number of Rings** setting for **Don't Answer?**.

Important:

The **Number of Rings** setting for **Don't Answer?** must be greater than the agent's Avaya Aura® Contact Center Call Presentation Class Return to Queue or Call Force Delay timer.

Example

Example of configuring the Coverage Path Group.

```
display coverage path 1
                                COVERAGE PATH

                  Coverage Path Number: 1
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                       Next Path Number:          Linkage

COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
              Active?             n               n
                Busy?             y               y
       Don't Answer?              y               y         Number of Rings: 2
                 All?             n               n
 DND/SAC/Goto Cover?              y               y
   Holiday Coverage?              n               n


COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h4              Rng:    Point2:
  Point3:                         Point4:
  Point5:                         Point6:
```

Configuring the agent station

Before you begin

- Create an agent extension. See Creating the agent extensions on page 58.
- Configure the Coverage Path Group. See Configuring the Coverage Path Group on page 183.

About this task

Configure the agent station with a single coverage path.

Procedure

1. Use the Communication Manager — System Access Terminal (SAT) interface **change station** command to configure the agent station.
2. Set the coverage path to the Coverage Path group configured previously.
3. Ensure the **Message Lamp ext** setting equals the agent's station number.

Example

Example of configuring the agent station.

```
display station 15050                                        Page   1 of   5
                                    STATION

Extension: 15050                      Lock Messages? n                BCC: 0
     Type: 9640                       Security Code: 12345678          TN: 1
     Port: S01095                    Coverage Path 1: 1               COR: 1
     Name: SM_Super                   Coverage Path 2:                COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                         Time of Day Lock Table:
             Loss Group: 19           Personalized Ringing Pattern: 1
                                             Message Lamp Ext: 15050
           Speakerphone: 2-way             Mute Button Enabled? y
       Display Language: english                Button Modules: 0
 Survivable GK Node Name:
         Survivable COR: internal            Media Complex Ext:
   Survivable Trunk Dest? y                        IP SoftPhone? y

                                          IP Video Softphone? n
                                 Short/Prefixed Registration Allowed: default

                                          Customizable Labels? y
```

Configuring the agent mailbox

About this task

Configure the agent's mailbox for voice messaging.

Procedure

Configure the agent’s mailbox in the normal way, referencing the relevant voice messaging system documentation.

Chapter 13: SIP Endpoints configuration

This section describes how to configure SIP users and how to automatically generate the corresponding SIP stations on the Avaya Aura® Communication Manager.

Session Manager is managed using Avaya Aura® System Manager. Communication Manager is administered using System Access Terminal (SAT).

Avaya Aura® Contact Center supports Communication Manager stations (phones) with a maximum of three Call Appearance lines per agent station.

Creating a new SIP User

About this task

Create a new SIP User, register it with one or more Session Manager, and automatically generate the corresponding SIP station on the primary Communication Manager.

Procedure

1. On the System Manager console, under **Users**, click **User Management**.
2. Click **Manage Users** in the left navigation pane.
3. On the User Management page, click **New**.
4. On the **Identity** tab, in the **Last Name** box, type the last name of the user.
5. In the **First Name** box, type the first name of the user.
6. In the **Description** box, type a short description of the user.
7. In the **Login Name** box, type a unique system login name for user.

   For SIP sets type a unique `name@domain.com` using the appropriate SIP domain in Session Manager. This name is used to create the user's primary handle.
8. From the **Authentication Type** list, select **Basic**.
9. In the **Password** box, type the password.

   The password must start with a letter character. Type the password to be used to log into the System Manager application.
10. In the **Confirm Password** box, retype the password.

11. In the **Localized Display Name** box, type the localized display name of the user.
12. In the **Endpoint Display Name** box, type the full text name of the user represented in ASCII.

    This supports displays that cannot handle localized text.
13. On the **Communication Profile** tab, in the **Communication Profile Password** box, type the Communication profile password.

    The password must be all numeric characters. This user uses this password to log on to the phone. Remember this password, it is used later for the Endpoint Profile Security code.
14. In the **Confirm Password** box, retype the password.
15. On the **Communication Profile** tab, in the **Communication Address** section, click **New**.
16. From the **Type** list, select **Avaya SIP**.
17. In the **Fully Qualified Address** box, type the full extension number of the SIP phone.
18. From the list following the **@** sign, select the appropriate domain.
19. Click **Add**.
20. Select the check box to the left of the entry you just added.
21. Click **New**.
22. From the **Type** list, select **Avaya E.164**.
23. In the **Fully Qualified Address** box, type the private handle.
24. From the list following the **@** sign, select the appropriate domain.
25. Click **Add**.
26. Select the check the box to the left of **Session Manager Profile**.

    The Session Manager Profile section is displayed.
27. From the **Primary Session Manager** list, Select the Session Manager instance to be used as the home server for the currently displayed Communication Profile.

    As a home server, the selected primary Session Manager instance is used as the default access point for connecting devices associated with the Communication Profile to the Aura® network.
28. From the **Secondary Session Manager** list, select the appropriate Session Manager instance to be used as the backup server.

    If a secondary Session Manager instance is selected, this Session Manager provides continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available.
29. From the **Origination Application Sequence** list, select the appropriate application sequence name that is used when calls are routed from this user. A selection is optional.

Note:

If both an origination and a termination application sequence are specified and each contains a Communication Manager application, the Communication Manager must be the same in both sequences.

30. From the **Termination Application Sequence** list, select the appropriate application sequence name used when calls are routed to this user from the drop-down menu.
31. From the **Survivability Server** list, select the entity to be used for survivability.

    For a Survivable Remote Session Manager, select the **Survivable Remote Session Manager SIP Entity**.
32. From the **Home Location** list, select the Communication Manager server SIP Entity to be used as the home location for call routing for this user.
33. Select the check the box to the left of **Endpoint Profile**.

    The Endpoint Profile section is displayed.
34. From the **System** list, select the Communication Manager server on which you need to add the endpoint.
35. From the **Profile Type** list, select **Endpoint**.
36. Clear the **Use Existing Endpoints** check box.
37. In the **Extension** box, type the extension for the endpoint on the Communication Manager.
38. From the **Template** list, select the template (system defined or user defined) you want to associate with the endpoint.

    Select the template based on the set type you want to add. For a Session Manager server, use the SIP version of the template (for example, DEFAULT_9640SIP_CM_6_0).
39. In the **Port** box, type the relevant port number for the set type you select.
40. Select the **Delete Endpoint on Unassign of Endpoint from User or Delete User** check box.
41. Click **Commit**.

Procedure job aid

Use Avaya Aura® System Manager to create a new user. System Manager registers this user with one or more Session Managers and automatically generates the User's station on the Avaya Aura® Communication Manager.

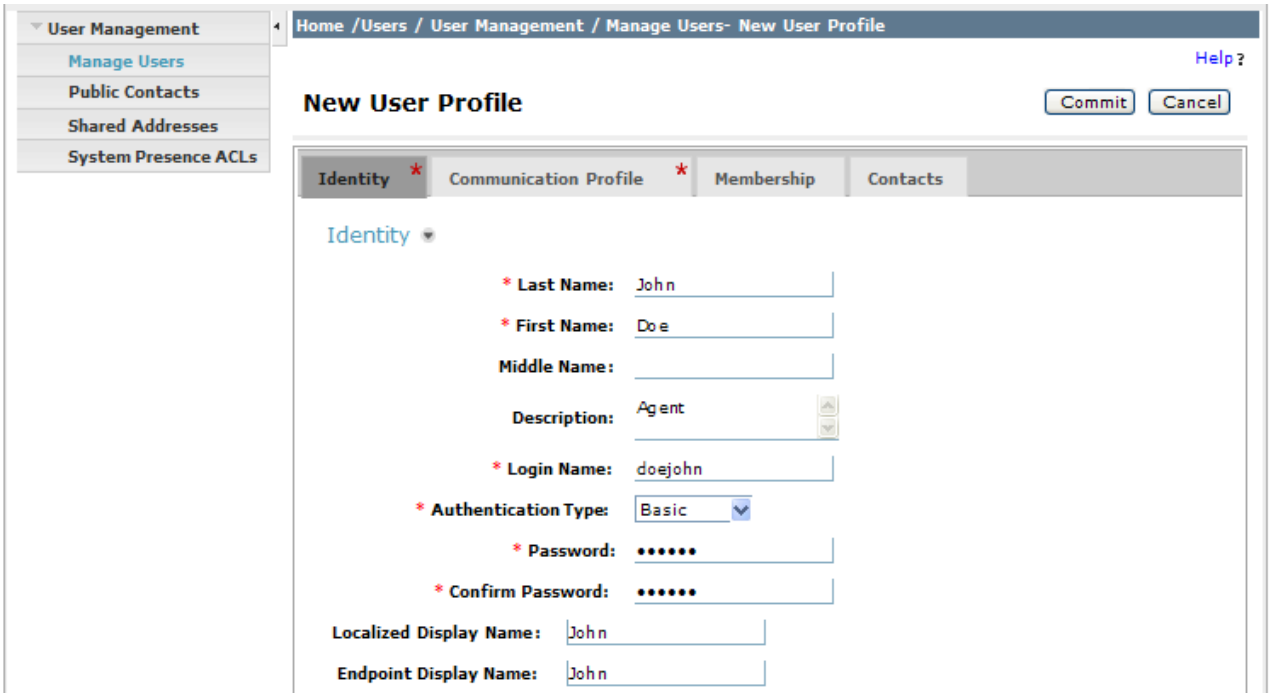


Figure 26: Example of adding a new User in System Manager

Verifying a SIP User using System Manager

About this task

Verify a SIP User is registered with one or more Session Managers using Avaya Aura® System Manager.

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager** > **System Status** > **User Registrations**.
2. In the table, click on **Show** in the row containing the Address or Login Name of the user.
3. Verify that the information in the **Registration Detail** record is correct.

Procedure job aid

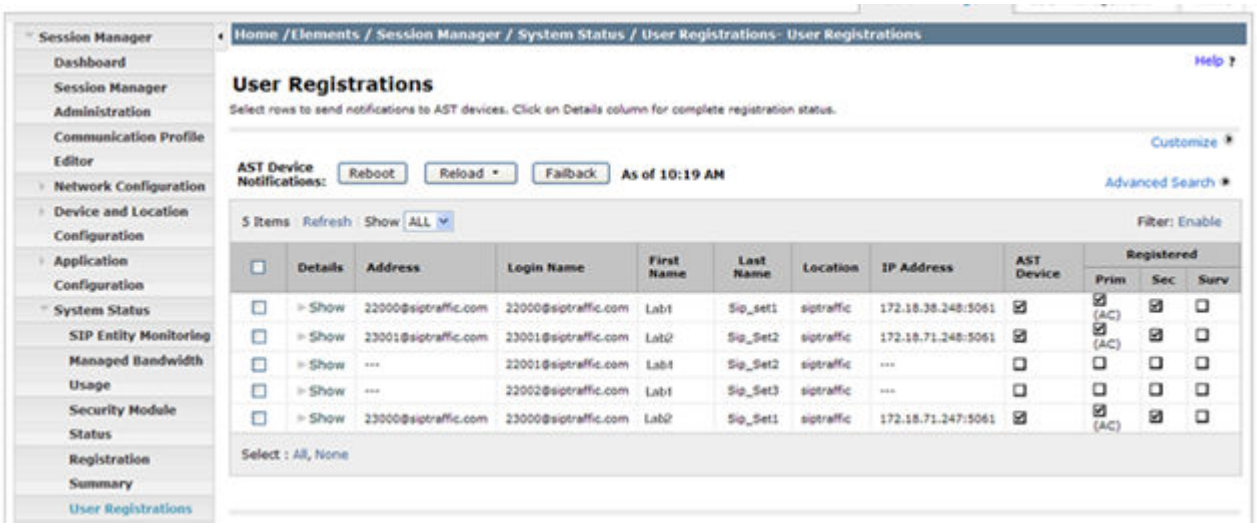


Figure 27: Example of verifying the user is registered with a Session Manager

Verifying a SIP User station on Communication Manager

About this task

Verify a SIP User station is configured on the Communication Manager using the System Access Terminal (SAT). Use the SAT utility to verify the station information entered using System Manager was correctly added to the Communication Manager. Use the SAT utility to verify the third-party call control (3PCC) and off-pbx-telephone station mapping details.

Procedure

1. Using SAT, enter **display station xxxxx**, where xxxxx is the phone extension of the user.
2. Verify that the station **Type** is set to **SIP**, for example **9640SIP**.
3. Go to page 6 of the station form.
4. Verify that **SIP Trunk** is set to **aar**.
5. Enter **display off-pbx-telephone stationmapping xxxxx**, where xxxxx is the phone extension of the user.
6. Verify that **Type of 3PCC Enabled** is set to **Avaya**.
7. Verify that **Trunk Selection** for the phone extension is **aar**.
8. Verify that the station has a maximum of three Call Appearance lines.

Procedure job aid

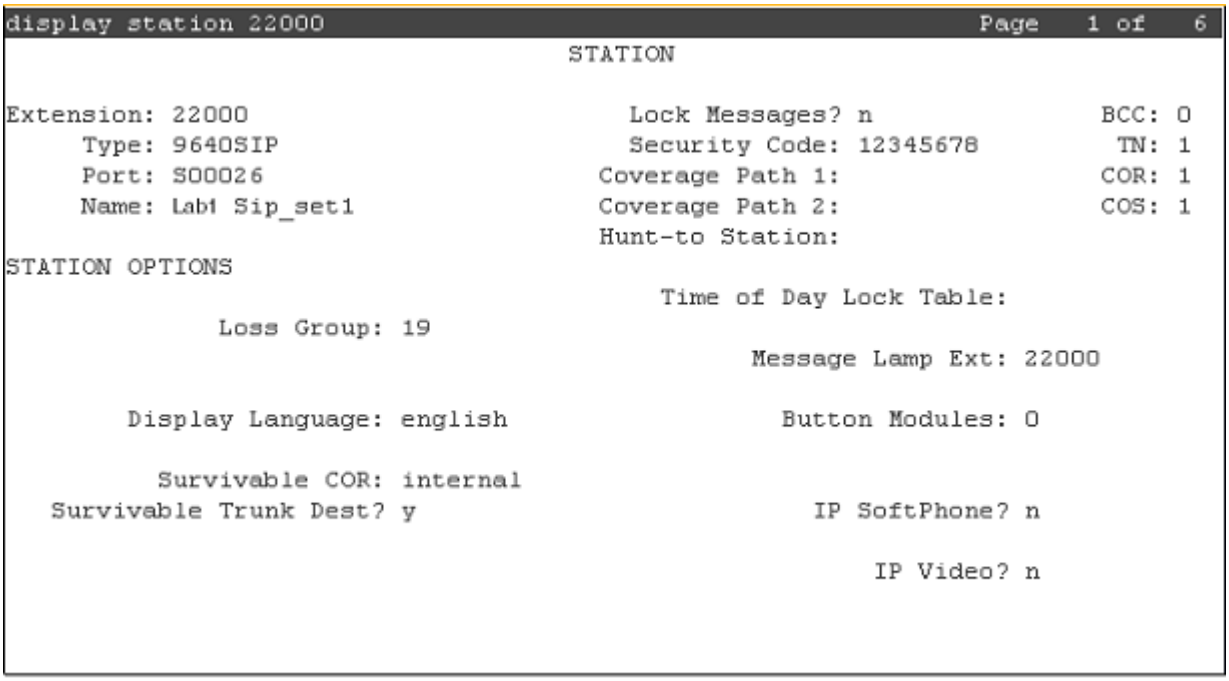


Figure 28: Example of verifying the user station on Communication Manager

Chapter 14: Video feature configuration

AACC can handle video contact types. If you want video contacts routed to Contact Center agents, you must create a video route point, add video skillsets, and assign the video contact type and video skillsets to agents. Contact Center treats and routes video contacts using the same methods as it uses to route voice contacts. Video contacts are reported on in both real-time and historical reports.

The Avaya Aura® Web Gateway WebRTC client is used to route video contacts, through the SM, in the Avaya Aura® Contact Center solution. Contact Center routes the contacts to a video agent using a supported SIP video endpoint. See SIP Endpoints configuration on page 187.

Note:

To support video feature, it is required that you use Avaya Aura® Web Gateway version 3.3 or later.

Contact Center supports using Avaya Workplace Client or Avaya Vantage™ as a video endpoint. You can view video calls using Avaya Workplace Client or Avaya Vantage™, however you must use Avaya Agent Desktop for call control actions.

You can record the audio part of video call using DMCC call recording.

Use the CM portal to check if the video feature licensing is enabled.

Configuring Video Media Processor in AAMS

About this task

Use this procedure to configure Video Media Processor in Avaya Aura® Media Server Element Manager and enable video contacts for your Contact Center.

Procedure

1. In Avaya Aura® Media Server Element Manager, on the left panel, click **System Configuration**.
2. Click **Server Profile**.
3. Click **General Settings**.
4. Under **Server Functions**, select the **Video Media Processor** checkbox.
5. Click **Save**.

   Restart the server for changes to take effect.

Configuring codec settings for Video

About this task

Use the Communication Manager System Access Terminal (SAT) interface to configure the ip-codec-set for video.

Procedure

1. Log on to Communication Manager to gain access to the Communication Manager administration interface. See Logging on to Communication Manager on page 34.
2. In SAT, use the `change ip-codec-set` command.
3. On the **IP Media Parameters** screen, page 1, add the `G.722.1-32K` codec.

```
display ip-codec-set 1                                    Page   1 of   2

                        IP MEDIA PARAMETERS
   Codec Set: 1

   Audio          Silence       Frames   Packet
   Codec          Suppression   Per Pkt  Size(ms)
1: G.711MU             n           6        60
2: G.729A              n           6        60
3: G.722.1-32K                     1        20
4:
5:
6:
7:
```

4. Move to the page 2 of the **IP Media Parameters** screen.
5. In the **Maximum Call Rate for Direct-IP Multimedia** field, set the value to 1920 Kbits.

6. In the **Maximum Call Rate for Priority Direct IP-Multimedia**, set the value to 1920 Kbits.

```
display ip-codec-set 1                                        Page   2 of   2

                        IP MEDIA PARAMETERS

                             Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:  1920:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:  1920:Kbits

                                          Redun-                      Packet
                        Mode              dancy                       Size(ms)
    FAX                 relay             0
    Modem               off               0
    TDD/TTY             US                3
    H.323 Clear-channel n                 0
    SIP 64K Data        n                 0                           20


Media Connection IP Address Type Preferences
 1: IPv4
 2:
```

Changing IP network region for Video

About this task

Use the Communication Manager System Access Terminal (SAT) interface to configure the ip-network-region for video.

Procedure

1. Log on to Communication Manager to gain access to the Communication Manager administration interface. See Logging on to Communication Manager on page 34.
2. In SAT, use the `change ip-network-region` command.
3. In the **Location** field, type `1`.
4. In the **Authoritative Domain** field, type your SIP domain name.

5. In the **Name To** field, type `Customer`.

```
display ip-network-region 1                                   Page   1 of  20
                              IP NETWORK REGION
  Region: 1       NR Group: 1
Location: 1       Authoritative Domain: sipccgal.com
    Name: To Customer           Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
       Audio PHB Value: 46
       Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
       Audio 802.1p Priority: 6
       Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

6. In the **Intra-region IP-IP Direct Audio** field, type `yes`.
7. In the **Inter-region IP-IP Direct Audio** field, type `yes`.
8. On the page 3, set the value of **H.323 SECURITY PROFILES** to `any-auth`.

```
display ip-network-region 1                                   Page   3 of  20
                              IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY
 Incoming LDN Extension:
 Conversion To Full Public Number - Delete:    Insert:
 Maximum Number of Trunks to Use for IGAR:
 Dial Plan Transparency in Survivable Mode? n

BACKUP SERVERS(IN PRIORITY ORDER)    H.323 SECURITY PROFILES
 1                                   1   any-auth
 2                                   2
 3                                   3
 4                                   4
 5
 6                                   Allow SIP URI Conversion? y

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS
   Near End Establishes TCP Signaling Socket? y
                        Near End TCP Port Min: 61440
                        Near End TCP Port Max: 61444
```

Updating signaling group for Video

About this task

Use the Communication Manager System Access Terminal (SAT) interface to configure the signaling-group for video. The signaling group is already preset for the SM67.

Procedure

1. Log on to Communication Manager to gain access to the Communication Manager administration interface. See Logging on to Communication Manager on page 34.
2. In SAT, use the `change signaling-group` command.
3. On the **Signaling group** screen, page 1, in the **Priority Video** field, type `y`.
4. In the **IP Video** field, type `y`.
5. In the **Initial IP-IP Direct Media?** field, type `y`.

```
display signaling-group 67                                    Page   1 of   3
                              SIGNALING GROUP

 Group Number: 67              Group Type: sip
  IMS Enabled? n         Transport Method: tls
       Q-SIP? n
    IP Video? y           Priority Video? y        Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM                       Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: sm67
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain: sipccgal.com
                                              Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                 RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? y                 Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```

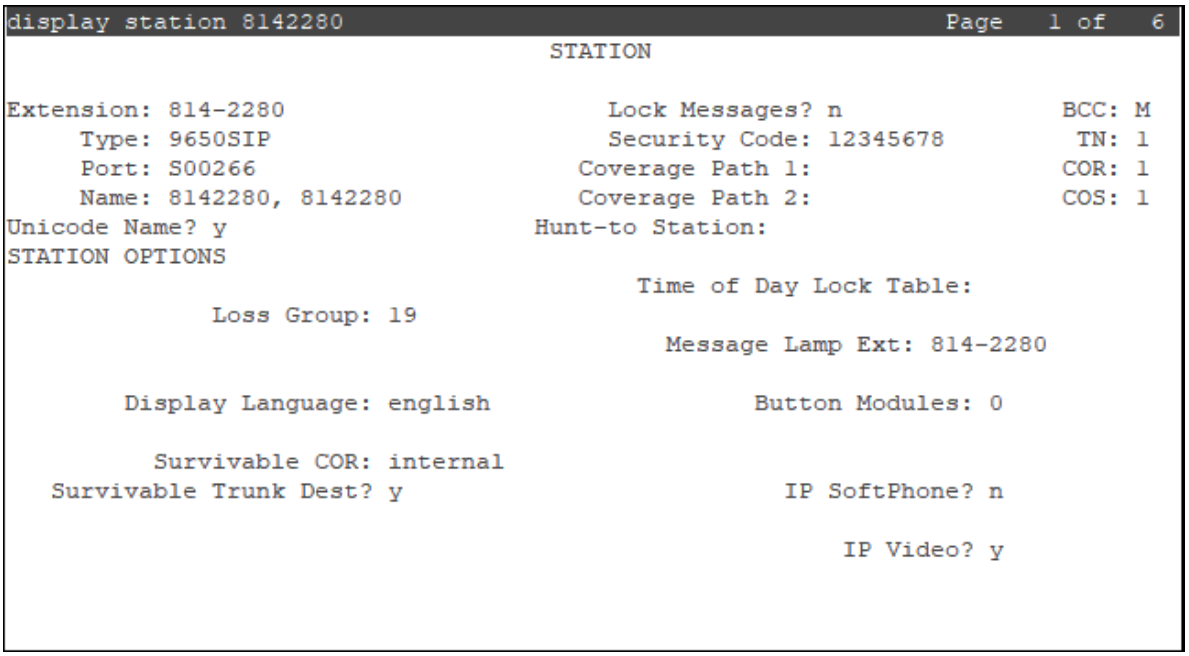
Updating station configuration for Video

About this task

Use the Communication Manager System Access Terminal (SAT) interface to update the station configuration for video.

Procedure

1. Log on to Communication Manager to gain access to the Communication Manager administration interface. See Logging on to Communication Manager on page 34.
2. In SAT, use the `change station` command.
3. On the **Station** screen, page 1, in the **IP Video** field, type `y`.



Verifying the video feature licensing

About this task

Use this procedure to verify licensing of the video feature.

Procedure

1. Log on to Communication Manager to gain access to the Communication Manager administration interface. See Logging on to Communication Manager on page 34.
2. Click **Licensing**.
3. Click **Feature Administration**.
4. Check if the following features are enabled:
   - ARS/AAR Dialing without FAC
   - Multimedia IP SIP Trunking
   - Media Encryption Over IP

When enabled, the value is set to `Y`.

Configuring AE Services

About this task

Use this procedure to configure AE Services.

Procedure

1. Log on to the AES management console.
2. In the left pane, click **AE Services**.
3. Select **TSAPI** > **TSAPI Links**.
4. Perform one of the following actions:
   - Click **Add Link** to add the ASAI Link version 10.
   - Click **Edit Link** to updated the existing ASAI Link to the version 10,

Chapter 15: SRTP configuration

Avaya Aura® Contact Center (AACC) supports implementing Secure Real-Time Transport Protocol (SRTP) for voice contacts within the contact center.

Secure Real-Time Transport Protocol (SRTP) is an extension to the Real-time Transport Protocl (RTP) to support secure real-time communications. The primary use of SRTP is to encrypt and authenticate voice over IP (VOIP) on the network.

Before implementing SRTP in Contact Center, you must have TLS on the following links:

- Communication Manager to Session Manager
- Agent telephones to Communication Manager
- Session Manager to Contact Center
- Contact Center to Application Enablement Services
- Contact Center to Avaya Aura® Media Server

To provide SRTP for routed Contact Center voice calls, you must configure SRTP on the following links:

- Agent telephones to Communication Manager
- Agent telephones to Avaya Aura® Media Server
- DMCC interface from Communication Manager to Avaya Contact Recorder (if used)

This chapter describes how to configure SRTP on the necessary Unified Communications platform and Contact Center components. You must also configure SRTP on Avaya Aura® Media Server. For more information on how to configure SRTP on Avaya Aura® Media Server, see *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications*.

If your Contact Center agents use the Agent Desktop embedded softphone, you must configure the Media Encryption settings on the Group Policy administrative template. For more information, see *Deploying Avaya Aura® Contact Center DVD for Avaya Aura® Unified Communications*.

Prerequisites

- Ensure your Avaya Aura® Contact Center is licensed for TLS SRTP Signaling and Media Encryption.
- TLS is a licensed feature on Communication Manager. Check that you have a Communication Manager license for TLS.

Enabling TLS between agent stations and Communication Manager

Before you begin

- If you are not using AACC default certificates to set up SRTP, apply the signed certificates to Communication Manager. For more information on generating and applying signed certificates, see the Communication Manager documentation at http://support.avaya.com.

About this task

Follow this procedure to enable TLS on the Communication Manager agent stations.

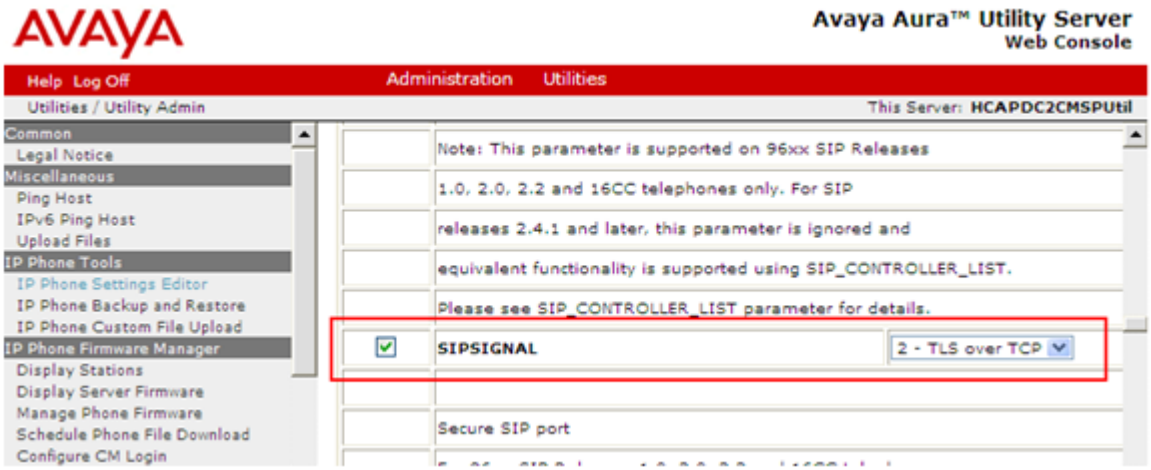
Procedure

1. Start Internet Explorer.
2. In the Internet Explorer address box, type http://<Utility Server IP address>.
3. On the Utility Server Web console, click **Utilities**.
4. Click **Utility Admin**.
5. Enter your Utility Server user name.
6. Click **Logon**.
7. Enter your Utility Server password.
8. Click **Logon**.

   The system displays the Utility Server Utility Admin menu.
9. From the left navigation menu, select **IP Phone Settings Editor**.
10. Click **Proceed with selected values**.
11. For your Contact Center phone types, set **SIPSIGNAL** to **2 – TLS over TCP**.

Example

Enabling Transport Layer Security (TLS) on agent extensions with 9640 phones.



Next steps

These changes do not take effect until the telephones reboot. During a scheduled maintenance or out of hours window, use the force reboot command to ensure the phones reboot.

Enabling SRTP on SIP endpoints

About this task

Follow this procedure to enable SIP deskphones for SRTP. You can select up to two of the following supported media encryption settings:

- 1 aescm128-hmac80
- 2 aescm128-hmac32
- 9 none

If you want to allow for best-effort connections, ensure you select 9 (none). If you select 9 (none), then agent sets can communicate with other components that do not support SRTP, by implementing RTP for the session.

If you want to enforce security, do not select 9 (none). In this case agent sets can communicate only with other components that support SRTP.

Procedure

1. Start Internet Explorer.
2. In the Internet Explorer address box, type http://<Utility Server IP address>.
3. On the Utility Server Web console, click **Utilities**.
4. Click **Utility Admin**.
5. Enter your Utility Server user name.
6. Click **Logon**.
7. Enter your Utility Server password.
8. Click **Logon**.

   The system displays the Utility Server Utility Admin menu.
9. From the left navigation menu, select **IP Phone Settings Editor**.
10. Click **Proceed with selected values**.
11. For your Contact Center phone types, select **MEDIAENCRYPTION**.
12. Set up to two of the following:
    - 1 aescm128-hmac80
    - 2 aescm128-hmac32
    - 9 none

Communication Manager supports only the values 1, 2, and 9.

Next steps

These changes do not take effect until the telephones reboot. During a scheduled maintenance or out of hours window, use the force reboot command to ensure the phones reboot.

Enabling SRTP on Communication Manager

About this task

Follow this procedure to configure Communication Manager to support SRTP requests. You must configure encryption on each of the codecs on the Communication Manager to match the configuration you applied for the SIP endpoints in Utility Server. The encryption settings in SAT use the descriptions, rather than the equivalent Utility Server IP Phone Settings Editor numerical values, for the SRTP settings, as follows:

- “1-srtp-aescm128-hmac80” in SAT equates to “1” in the IP Phone Settings Editor.
- “2-srtp-aescm128-hmac32” in SAT equates to “2” in the IP Phone Settings Editor.
- “none” in SAT equates to “9” in the IP Phone Settings Editor.

Communication Manager supports a maximum of two settings, and must match the settings for SIP endpoints in the Server Utility IP Phone Settings Editor.

You must also configure system parameters settings on the Communication Manager.

Procedure

1. Open a SAT terminal to Communication Manager.
2. In SAT, change the **ip-codec-set**.
3. For each IP Codec, under **Media Encryption**, set the same encryption values you configured for the SIP endpoints:
   - 1-srtp-aescm128-hmac80 (1)
   - 2-srtp-aescm128-hmac32 (2)
   - none (9)
4. Use the **change system-parameters features** command to ensure the following parameter is set to **y**.
   - Initial INVITE with SDP for secure calls?

Example

```
display ip-codec-set 1                                          Page   1 of   2

                        IP Codec Set

    Codec Set: 1

    Audio          Silence      Frames   Packet
    Codec          Suppression  Per Pkt  Size(ms)
 1: G.711MU             n          2        20
 2: G.711A              n          2        20
 3: G.729               n          2        20
 4:
 5:
 6:
 7:
```

```
     Media Encryption
 1: 1-srtp-aescm128-hmac80
 2: none
 3:
```

```
display system-parameters features                              Page  19 of  20
                      FEATURE-RELATED SYSTEM PARAMETERS
IP PARAMETERS
                   Direct IP-IP Audio Connections? y
                             IP Audio Hairpinning? n
                          Synchronization over IP? y
        Initial INVITE with SDP for secure calls? y
                  SIP Endpoint Managed Transfer? n

   Expand ISDN Numbers to International for 1XCES? n
CALL PICKUP
  Maximum Number of Digits for Directed Group Call Pickup: 2
                  Call Pickup on Intercom Calls? y     Call Pickup Alerting? n
    Temporary Bridged Appearance on Call Pickup? y     Directed Call Pickup? n
                     Extended Group Call Pickup: none
                  Enhanced Call Pickup Alerting? n


                       Display Information With Bridged Call? n
  Keep Bridged Information on Multiline Displays During Calls? n
                 PIN Checking for Private Calls? n
```

Enabling TLS on Communication Manager

Before you begin

- TLS is a licensed feature on Communication Manager. Check that you have a Communication Manager license for TLS.

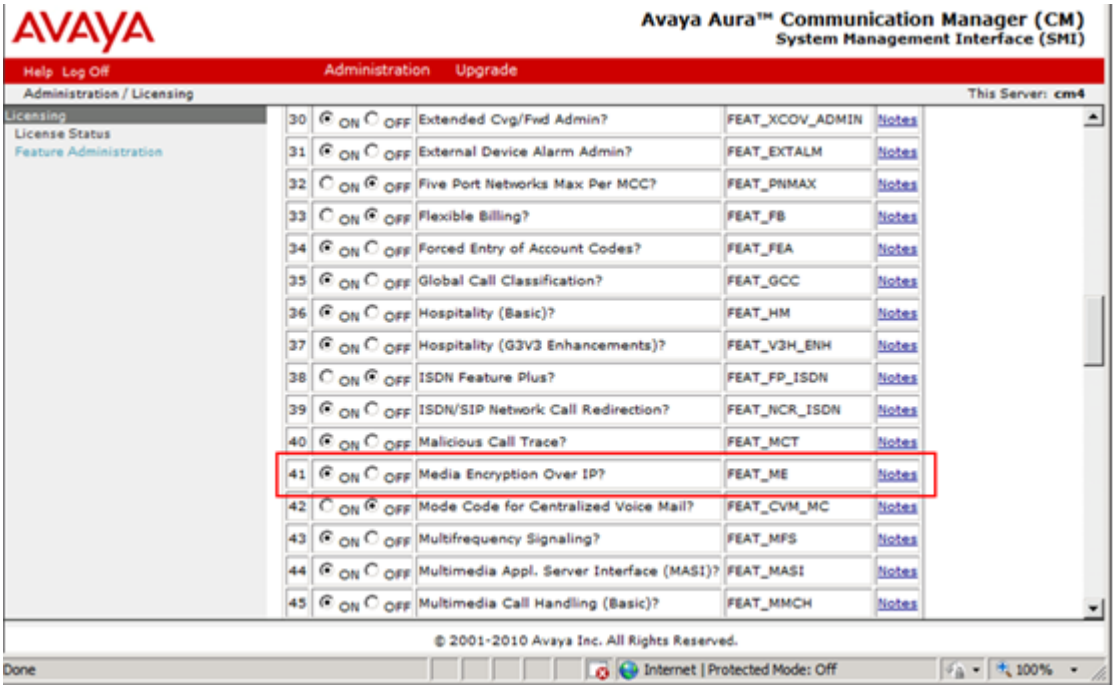
About this task

Follow this procedure to enable TLS on Communication Manager.

Procedure

1. Start Internet Explorer.
2. In the Internet Explorer address box, type http://<Communication Manager Server IP address>.
3. Enter your Communication Manager user name.
4. Click **Logon**.
5. Enter your Communication Manager password.
6. Click **Logon**.

   The System Management Interface appears.
7. Click **Administration** > **Licensing**.
8. Click **Feature Administration**.
9. Select **Current Settings** and click **Display**.
10. Set **Media Encryption over IP?** to **On**.



11. Click **Submit**.
12. Open a SAT terminal on Communication Manager.
13. In SAT, on the **system-parameters customer options** screen, verify that **Media Encryption over IP?** is **Y**.

    Do not set the value here, only verify that it is correctly set.
14. For each signaling group:
    a. Busy out the signaling group.
    b. Set the **Transport Method** to **tls**.
    c. Set **Enforce SIP URI for SRTP** to **Y**.
    d. Set **Near-end Listen Port** to 5061.
    e. Set **Far-end Listen Port** to 5061.
15. Save your changes.

Example

```
display signaling-group 9
                               SIGNALING GROUP

 Group Number: 9                Group Type: sip
  IMS Enabled? n          Transport Method: tls
       Q-SIP? n                                          SIP Enabled LSP? n
    IP Video? y            Priority Video? n       Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: sipsm1
Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                       Far-end Network Region: 1
                                  Far-end Secondary Node Name:
Far-end Domain: sipccocs.com
                                                  Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                      RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload                Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                         IP Audio Hairpinning? n
         Enable Layer 3 Test? y                       Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n               Alternate Route Timer(sec): 6
```

Enabling TLS between Communication Manager and Session Manager

Before you begin

- If you are not using AACC default certificates to set up TLS, the Session Manager must have the signed certificates uploaded. For more information, see the Session Manager documentation at http://support.avaya.com.

About this task

Follow this procedure to enable TLS on the link between Communication Manager and Session Manager.

Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **SIP Entities**.
2. Ensure that the Entity Link for all Communication Manager SIP Entities has **Protocol** set to **TLS** and **Port** set to **5061**.
3. Click **Commit**.
4. On the Avaya Aura® System Manager console, under **Services**, click **Replication**.
5. For your Session Manager, ensure the **Synchronization Status** is showing as **Synchronized**.

Enabling TLS between Session Manager and AACC

Before you begin

- If you are not using AACC default certificates to configure SRTP, apply the signed certificates to AACC. For more information on applying signed certificates to AACC, see *Deploying Avaya Aura® Contact Center DVD for Avaya Aura® Unified Communications*.
- **Important:**

  This procedure requires you to reboot the Contact Center server. If your contact center implements High Availability, you must disable HA before performing this procedure.

About this task

Follow this procedure to enable TLS on the link between the Session Manager and AACC.

In a SIP-enabled Contact Center, incoming calls use a SIP URI scheme. For secure transmission, calls must use the SIPS URI scheme. You must enforce SIPS on your AACC server. When enabled, all SIP-initiated legs of Contact Center calls use SIPS. This includes call legs between AACC and Session Manager, Avaya Aura® Media Server or agent stations. For example, if Session Manager routes a call to AACC and the URI scheme is SIP (unsecured SIP), all subsequent SIP-initiated legs of that Contact Center call is SIPS.

If SIPS is not enabled, the URI scheme matches the incoming call. For example, if SIP arrives on an inbound call, then unsecured SIP is used on all subsequent call legs.

Procedure

1. On the Avaya Aura® System Manager console, select **Routing** > **SIP Entities**.
2. Ensure that the Entity Link for all AACC SIP Entities has **Protocol** set to **TLS** and **Port** set to **5061**.
3. Click **Commit**.
4. On the Avaya Aura® System Manager console, under **Services**, click **Replication**.
5. For your Session Manager, ensure the **Synchronization Status** is showing as **Synchronized**.
6. Log on to the Contact Center server using an account with administrative privileges.
7. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
8. In the left pane, expand **SIP** > **Network Settings**.
9. Under **Voice Proxy Server**, check that the port is **5061**.
10. From **Transport** list select **TLS**.
11. Select **Enforce SIPS**.
12. Click **Save**.
13. Click **Exit**.
14. Reboot the Contact Center server.

15. If your contact center implements High Availability:
    a. Repeat 6 on page 208 to 14 on page 208 on the standby server.
    b. Re-enable High Availability.

Verifying the existing TLS link between AES and Contact Center

About this task

The basic operation of Contact Center requires Avaya Aura® Application Enablement Services (AES) TLS certification. If you are adding SRTP to an existing Contact Center, check that the AES certificates already in use match those you use for SRTP. For example, if the AES currently uses the default AACC certificates, you can change these to a signed server and root certificate from a Certificate Authority.

For more information on AES certificates, see Application Enablement Services configuration on page 101.

Procedure

If you are not using the default AACC signed certificates for your overall SRTP implementation, check that the AES and Contact Center have the correct signed server and root certificates from the Certificate Authority you are using.

Chapter 16: Avaya Aura® Hotdesking configuration

This section outlines hotdesking in an Avaya Aura® Communication Manager platform based contact center.

The Avaya Aura® Communication Manager allows any agent to use their own credentials (extension number and password) to log on to any designated station. The Avaya Aura® Communication Manager then registers that station using the agent's extension number and the agent can receive their calls on that station's phone.

Logging on to a Communication Manager station

Before you begin

- Using the Avaya Aura® Communication Manager System Parameters Customer-Options screen, configure Personal Station Access (PSA).

About this task

Log on to an Avaya Aura® Communication Manager station using your extension number to receive your phone calls.

Procedure

1. On the Avaya Aura® Communication Manager desk phone, press the **Menu** button.
2. Scroll down to the **Login** option.
3. Enter your extension number and password credentials.

Chapter 17: UUI data display configuration

SIP-enabled contact centers using a Communication Manager PABX can pass User-to-User Information (UUI) data to agents' station displays. For example, an agent's station can display the Contact Center skillset of a voice contact routed to them by Contact Center. The size of the UUI data forwarded by Contact Center is limited to 96 characters. However, stations truncate the data to the number of characters that their display supports. UUI data is hexadecimal-encoded, and as a result of this it supports only the ASCII character set for agent names.

If the agent uses Agent Desktop, they can access UUI data on a voice contact by clicking the **Work Item Details** button. Agent Desktop displays the data in the **User to User Info** field. The **User to User Info** field displays up to 41 characters, and provides a tooltip showing all 96 characters.

In advanced solutions, for example contact centers that use Integrated Voice Response (IVR), it is possible to program the UUI data attached to the call. Where the solution does not program the UUI data (that is, the UUI field is not already in use), the station can display default data. For example, when an agent uses the Call Supervisor feature, the UUI data for the supervisor contains "CALL SUPER" followed by the agent's first name and last name. This occurs only if the station is configured to display UUI data.

Configuring the Communication Manager for UUI data display

On the Communication Manager (CM), you make three configuration changes. You enable UUI sharing on the trunk group between the Communication Manager and the Session Manager to which Contact Center connects. On the Class of Restriction (COR) for the agent stations, you verify or change the property for the Station Button display of UUI data. Finally you configure a button on each agent's station to display the data.

Depending on the station the agent uses, and the button that you set to display UUI data, the agent might need to page their station display to see the data. For example, if you configure Button Assignment 3 for UUI data, and the agent station has a two-button display, the agent needs to page the display to see the data. If the agent station has a three-button display, then the agent sees the UUI data without paging.

Modifying the SIP Trunk Group for UUI Data

About this task

On the Avaya Aura® Communication Manager, modify the SIP Trunk Group for communication between Communication Manager and the Avaya Aura® Session Manager.

Procedure

1. Use the System Access Terminal (SAT) interface to modify the SIP Trunk Group for the Session Manager.
2. Change the **UUI Treatment** setting to **Shared**.

```
change trunk-group 9                                          Page   3 of  22
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                    Maintenance Tests? y


                    Numbering Format: private
                                          UUI Treatment: shared
                                       Maximum Size of UUI Contents: 128
                                          Replace Restricted Numbers? n
                                         Replace Unavailable Numbers? n


                                  Modify Tandem Calling Number: no
               Send UCID? n


 Show ANSWERED BY on Display? y

 DSN Term? n
```

Changing Class Of Restriction Properties for UUI Data Display

About this task

On the Avaya Aura® Communication Manager, change the Class of Restriction (COR) that the agent stations use, so that it supports the display of UUI data.

Procedure

1. Use the System Access Terminal (SAT) interface to change the Class of Restriction properties for the agents' stations.
2. In the Class of Restriction, change the **Station-Button Display of UUI IE Data** setting to **Y**.

```
change cor 1                                                  Page   2 of  23
                              CLASS OF RESTRICTION

                      MF Incoming Call Trace? n
                 Brazil Collect Call Blocking? n
                      Block Transfer Display? n
Block Enhanced Conference/Transfer Displays? n
                      Remote Logout of Agent? n


 Station Lock COR: 1___      TODSL Release Interval (hours):
                                    ASAI Uses Station Lock? n
        Line Load Control: 1
 Maximum Precedence Level: ro           Preemptable? y
 MLPP Service Domain: ________

      Station-Button Display of UUI IE Data? y
      Service Observing by Recording Device? n
              Can Force A Work State Change? n
            Work State Change Can Be Forced? n
```

Creating a Button Assignment for UUI Data

About this task

On the Avaya Aura® Communication Manager, create a button assignment on each agent station on which you want Contact Center to display UUI data.

Procedure

1. Use the System Access Terminal (SAT) interface to modify each agent's station record.
2. Create a button assignment with the value **uui-info**. This can be on any button except button 1 or button 2.

```
change station 8320510                                    Page   4 of   5
                                    STATION
 SITE DATA
       Room: ___________                          Headset? n
       Jack: ______                               Speaker? n
      Cable: ______                              Mounting: d
      Floor: ___________                    Cord Length: 0
   Building: ___________                       Set Color: _______

ABBREVIATED DIALING
     List1: _________          List2: _________          List3: _________



BUTTON ASSIGNMENTS
 1: call-appr                              4: ___________
 2: call-appr                              5: ___________
 3: uui-info                               6: ___________

    voice-mail _____________________________
```

Chapter 18: Toll Free Queuing Configuration

Regulations introduced in Germany in 2012 require that callers to special service numbers for contact centers must not be charged for their call while their reason for calling is not being attended to. A transitional arrangement allowed for a two-minute free period during queuing, but as of June 2013 call queues must either be a fixed price or free of charge. The Avaya Aura® Contact Center Toll Free Queuing feature supports free queuing of calls within certain technical constraints.

The legislation requires that all queues must also be free of charge, including secondary queues, such as when an agent puts the caller on hold or transfers the caller. Currently there is no technical solution in the industry to support secondary queues: once call charging commences it cannot be suspended or resumed.

Important:

Contact Center supports this feature only in integrations with Avaya Aura® Communication Manager (CM) where the customer call arrives on the CM through an ISDN trunk. In a mixed environment, calls to the contact center CM from other PABXs or other types of trunk do not support Toll Free Queuing.

Operation

When you enable Toll Free Queuing, Contact Center does not send a SIP 200 OK final response to the caller SIP INVITE when it queues the call. Instead, Contact Center sends a 183 Session Progress message. The 183 Session Progress message is a reliable provisional response, that Contact Center resends periodically. This delays the PABX from sending the carrier an ISDN CONNECT thus delaying the carrier from establishing the call. The Contact Center Orchestration Designer application flows can give ringback, recorded announcements (RAN), silence, IVR Play Prompt, and music without affecting call completion. During this time, the carrier cannot start charging the caller. During this period the carrier bears the cost of the call. Some carriers place a time limit on this period, after which they drop the call if Contact Center has not answered it.

Contact Center sends the SIP 200 OK response to the CM when the application flow gives an IVR Play and Collect Treatment to the caller, when an agent answers the call, after a fixed period of time configured by the contact center administrator, or when the Orchestration Designer application flow implements a Free Form IVR block with the **Toll_Free_Queuing_Connect** parameter. The CM then sends an ISDN CONNECT message to the carrier, which starts charging the caller.

The best solution results where the external carrier, connected to the CM by ISDN trunks, supports Annex K (Procedure for establishment of bearer connection prior to call acceptance) of the ISDN specification. In this case you set PROGRESS with Progress Indicator 8 indicating in band information. The caller can hear ringback, RAN, IVR Play Prompt, and music that Contact Center provides, without incurring a charge from the carrier.

If a carrier does not support Annex K of the IDSN specification, you must set the ALERTING interworking message on Communication Manager. The caller can hear only ringback provided by the network and cannot hear Contact Center treatments.

In Contact Center, you enable this feature using a checkbox on the Contact Center Manager Administration Global Settings page. You also set the time after which the Contact Center enables billing to start.

Calls disconnected by the carrier before Contact Center answers them appear as standard abandoned calls in Real Time Displays and Historical Reports. Contact Center does not provide additional reporting for this feature.

Toll Free Queueing is not a licensed feature.

Limitations

While the German regulations relate to all queues, Toll Free Queuing affects only the caller's first queue; that is, the queue in which the caller waits for their initial contact with the contact center. Toll Free Queuing does not support secondary queues. For example, if an agent answers a caller, and then transfers the caller to another agent, places the call on hold, or transfers the caller to a Route Point where they queue for another agent, the second queue is not toll free.

When Contact Center enables both Toll Free Queuing and High Availability, there is no call protection for calls that Contact Center has not answered with a 200 OK SIP message. If a switchover occurs, Contact Center loses every call that is not being charged; that is, every call for which it has not sent a 200 OK message.

If a Contact Center flow application redirects a call out of Contact Center by using the ROUTE CALL command, the **Maximum time to delay call establish** setting has no effect. In this case the carrier drops the call if the endpoint to which Contact Center redirected it does not answer within the carrier's charge-free time limit.

You must not implement Contact Center Toll Free Queueing if the Session Manager implements the Session Manager Sequence Application. Avaya recommends that you decommission the Sequence Application and implement the Toll Free Queuing feature. For more information about the Session Manager Sequence Application, see the Session Manager documentation at http://support.avaya.com.

When you implement Toll Free Queuing, any call that does not come directly from the Communication Manager (CM) or a Session Border Controller (SBC) to AACC is not supported, and AACC rejects the call. For example, consider the following call flow:

1. A call for a non-agent extension number comes in to the CM through an ISDN trunk.
2. The CM re-routes the call with Cover No answer to Avaya Aura® Messaging voicemail.
3. The caller presses 0 to use the zero out feature of Avaya Aura® Messaging, routing the call to an AACC CDN.

AACC rejects the call, because the call to the CDN comes from Avaya Aura® Messaging, not from the CM or SBC.

Configuring Communication Manager for Toll Free Queuing

Before you begin

Understand whether the external carrier ISDN trunk supports Annex K of the ISDN specification.

About this task

The Toll Free Queuing feature requires specific settings on the Communication Manager external ISDN Trunks. Follow this procedure to enable the correct messaging for each incoming ISDN trunk.

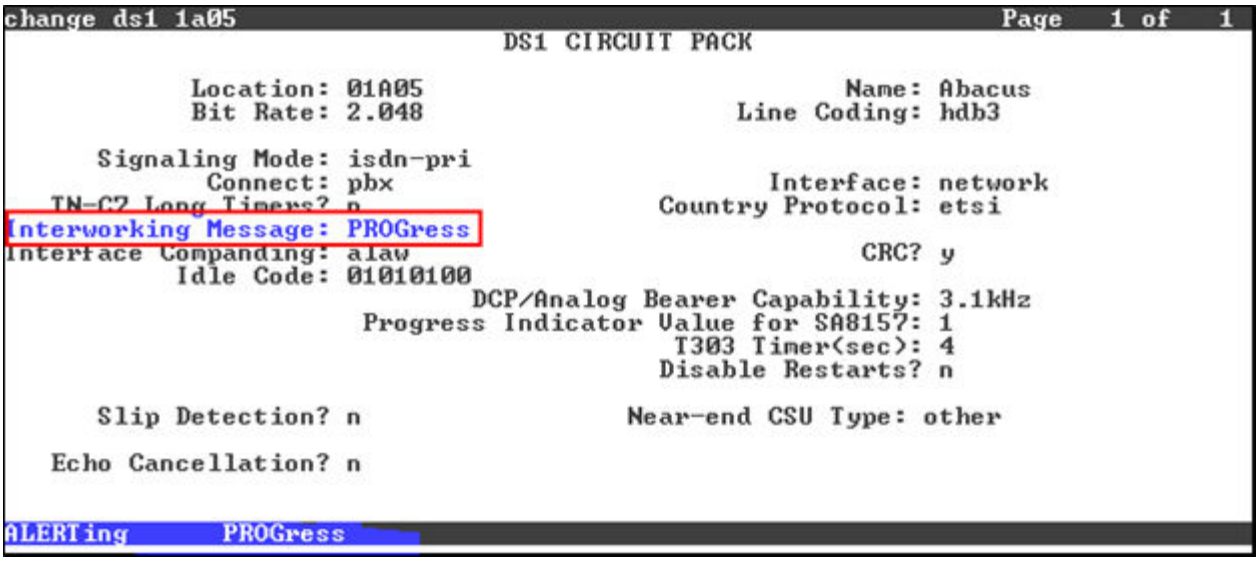
If the carrier supports Annex K, set the CALL PROGRESS interworking message on Communication Manager. This means that the caller hears ringback, RAN, IVR Play Only, or music provided by Contact Center flow applications. If the carrier does not support Annex K, set the ALERTING interworking message. This means that the caller hears ringback provided by the carrier network; the caller does not hear Contact Center treatments.

Procedure

1. Use the System Access Terminal (SAT) interface to change the circuit pack settings for each external carrier ISDN trunk.
2. If the carrier supports Annex K for this trunk, in the circuit pack page, change the **Interworking Message** setting to **PROGress**.
3. If the carrier does not support Annex K for this trunk, in the circuit pack page, change the **Interworking Message** setting to **ALERTing**.

Example

Following is a screenshot of the SAT interface displaying an ISDN trunk circuit pack with the Interworking Message set to PROGress.



Next steps

Configure Contact Center for Toll Free Queuing. For information about configuring Toll Free Queuing in Contact Center, see *Avaya Aura® Contact Center Client Administration*.

Chapter 19: Beep tone configuration for non-skillset call monitoring

Avaya Aura® Contact Center allows administrators to configure a beep tone to play when a supervisor/agent observes or barges-in to a non-skillset call. Playing a beep tone for supervisor observe and barge-in is a regulatory requirement in some jurisdictions.

Avaya Aura® Communication Manager plays the observe beep tone repeatedly while the supervisor/agent observes the call. Communication Manager plays the barge-in beep tone once when the supervisor/agent barges-in to the call.

To support this feature, create and upload beep tone files. Then configure a station, an announcement for the observe beep tone, and an announcement for the barge-in beep tone.

Complete the procedures in this chapter in sequential order.

Beep tone overrides Music on Hold configured on the Communication Manager; if a supervisor/agent is monitoring a call, and the agent puts the call on hold, the caller and the supervisor/agent hear only beep tone.

Media files for beep tone

Beep tone media files must be 8kHz sampling rate, 8 bit Mono, CCITT mu-law or CCITT a-law wav files. For the observe beep tone, create a wav file with a single tone followed by silence for the amount of time you want between tones. This ensures a repeating tone separated by the pause. For the barge-in beep tone, create a wav file with a single tone and no silence; use a different tone to the observe tone.

Avaya provides both mu-law and a-law sample beep tone files in the correct format, which are on the CCMS server in the folder `D:\Avaya\Contact Center\Common Components\wavs`.

Uploading beep tone files to the media gateway

Before you begin

- Create the media files for the observe and barge-in beep tones.

About this task

Upload the beep tone files to the media gateway so that you can use the media files in announcements. The files must be 8kHz sampling rate, 8 bit Mono, CCITT mu-law or CCITT a-law wav files. Avaya provides both mu-law and a-law sample beep tone files in the correct format,

which are on the CCMS server in the folder `D:\Avaya\Contact Center\Common Components\wavs`.

If your solution includes multiple media gateways, you must upload the files to all the media gateways.

Procedure

1. From the computer where you prepared the media files, open an FTP session to the media gateway.
2. Transfer the beep tone files to the `annc` directory on the media gateway.

Next steps

If you have multiple media gateways, repeat this procedure to upload the files to all the media gateways. Then configure an audio group listing all the boards of the Media Gateways, and use this audio group when creating the announcement stations.

Configure an announcement on Communication Manager to use the beep tone file.

Adding a station for beep tone

Before you begin

- Ensure you have an additional agent station license.
- If you are using Application Enablement Services Release 6.3.3, apply the most recent superpatch.

About this task

Configure a CTI station so that Communication Manager can play the beep tone when a supervisor/agent observes or barges-in to the call.

To ensure non-skillset call monitoring functionality, set both the station level and the trunk level Data Restriction settings to "n".

Procedure

1. On the Communication Manager, use the System Access Terminal (SAT) interface to create an agent extension (workstation). Use the **`add station n`** command.

   For example, enter **`add station 8123456`**.
2. Ensure the station **Type** is `CTI` and the **Port** is `X`.
3. In the **Name** field, enter a meaningful description that reflects the purpose of this station.

   For example, call the station `Observe barge-in beep tone`.
4. In the **Feature Options** section, set the station **Data Restriction** value to `n`.
5. At the Communication Manager trunk configuration level, in the **Trunk Feature** section, set the trunk **Data Restriction** value to `n`.

Next steps

Create the announcements for the observe and barge-in beep tones.

Procedure job aid

The following image shows a Communication Manager CTI station configured to support AACC non-skillset call monitoring beep tones.

```
add station 8142337                                          Page   1 of   5
                                    STATION

Extension: 814-2337                    Lock Messages? n                BCC: 0
     Type: CTI                       Security Code:                   TN: 1
     Port: X                   Coverage Path 1:                      COR: 1
     Name: Beep Tone Proxy     Coverage Path 2:                      COS: 1
                               Hunt-to Station:
STATION OPTIONS
                                       Time of Day Lock Table:
             Loss Group: 1          Personalized Ringing Pattern: 1
           Data Module? n                     Message Lamp Ext: 814-2337
       Display Module? n
     Display Language: english

       Survivable COR: internal                Media Complex Ext:
  Survivable Trunk Dest? y
```

Figure 29: Adding a Communication Manager CTI station

Creating an announcement for observe

Before you begin

- Create a beep tone file for observe, and upload it to a media gateway connected to the Communication Manager.

About this task

Configure an announcement for the observe beep tone.

Procedure

1. On the Communication Manager, use the System Access Terminal (SAT) interface to create an announcement. Use the **`add announcement n`** command.

   For example, enter **`add announcement 8123457`**.

2. In the `Annc Name` field, enter the name of the announcement file that you loaded on the media gateway.

   For example, if the file on the media gateway is `observe.wav`, enter `observe` in the `Annc Name` field.

3. Ensure the `Annc Type` value is `integ-mus` to continually play the observe tone while the supervisor observes the call.

Next steps

- Test that the announcement plays correctly by dialing the number directly from a station on the Communication Manager.
- Enable and configure beep tone on the **Non-Skillset call monitoring** window in Contact Center Manager Administration (CCMA). For more information about configuring Non-Skillset call monitoring, see *Avaya Aura® Contact Center Client Administration*.

Procedure Job Aid

The following image shows a Communication Manager announcement configured to support AACC non-skillset call observe beep tones.

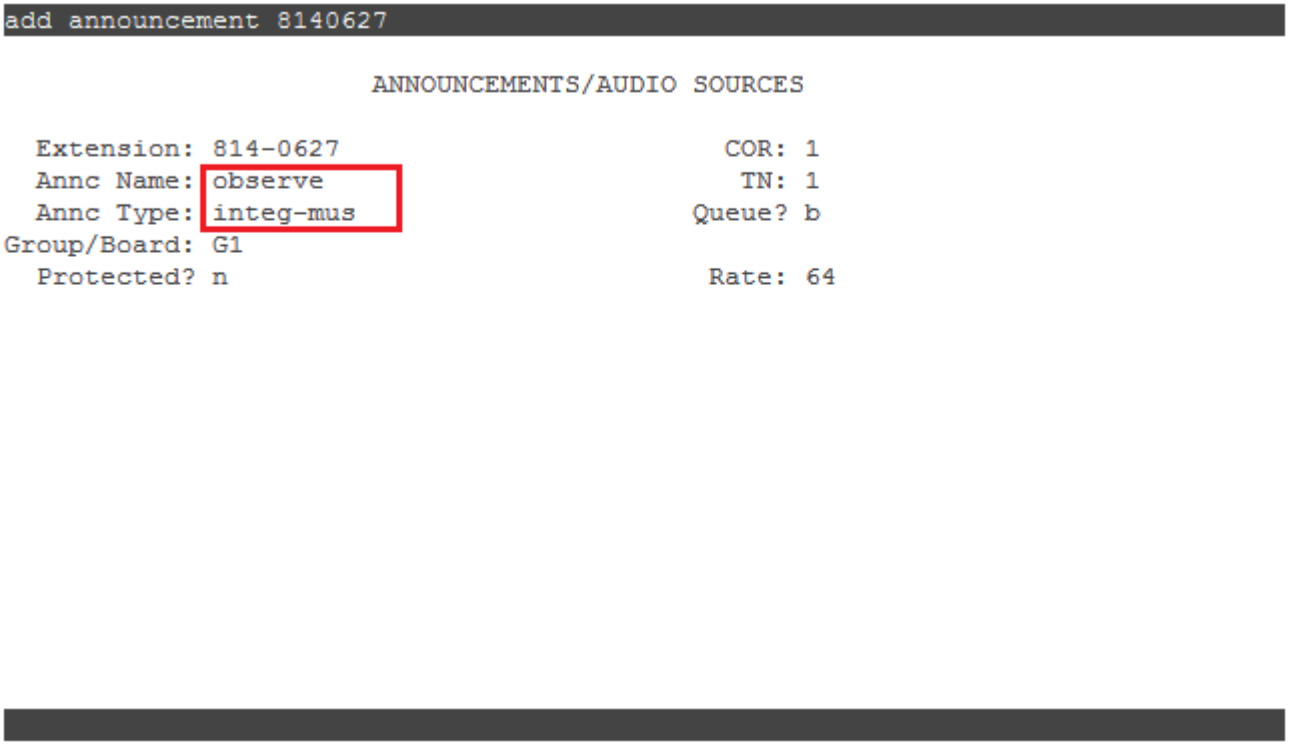


Figure 30: Adding a Communication Manager announcement

Creating an announcement for barge-in

Before you begin

- Create a beep tone file for barge-in, and upload it to a media gateway connected to the Communication Manager.

About this task

Configure an announcement for the barge-in beep tone.

Procedure

1. On the Communication Manager, use the System Access Terminal (SAT) interface to create an announcement. Use the **`add announcement n`** command.

   For example, enter **`add announcement 8123458`**.

2. In the `Annc Name` field, enter the name of the announcement file that you loaded on the media gateway.

   For example, if the file on the media gateway is `barge-in.wav`, enter `barge-in` in the `Annc Name` field.

3. Ensure the `Annc Type` value is `integrated` to play the barge-in tone only once when the supervisor barges-in to the call.

Next steps

- Test that the announcement plays correctly by dialing the number directly from a station on the Communication Manager.
- Enable and configure beep tone on the **Non-Skillset call monitoring** window in CCMA. For more information about configuring Non-Skillset call monitoring, see *Avaya Aura® Contact Center Client Administration*.

Procedure Job Aid

The following image shows a Communication Manager announcement configured to support AACC non-skillset call barge-in beep tones.

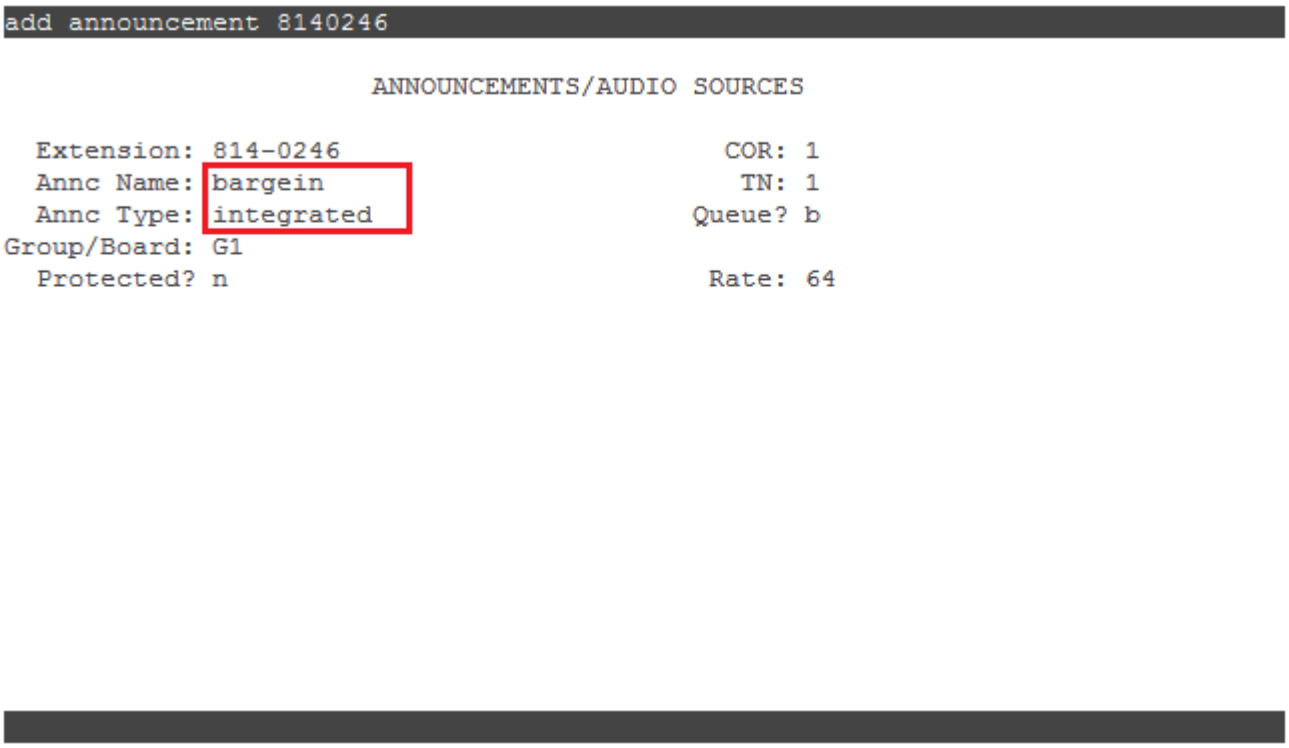


Figure 31: Adding a Communication Manager announcement file

Chapter 20: Troubleshooting

This section describes the procedures you perform when handling Avaya Aura® Contact Center and Avaya Aura® Unified Communications platform integration issues.

Prerequisites

- Ensure that your servers, client computers, and network meet the minimum system requirements. For more information about hardware and network requirements, see *Avaya Aura® Contact Center Overview and Specification*.
- Ensure that you have installed Contact Center correctly.

Troubleshooting phone calls from Communication Manager to Avaya Aura® Contact Center

Before you begin

- On the Communication Manager, configure the numbering tables. For more information, see Adding agent workstations to the numbering tables on page 63.
- In Contact Center, ensure at least one agent is logged on to the skillset associated with the test CDN (Route Point).
- Ensure the agent's Agent Desktop client is Ready to handle voice calls.

About this task

This section introduces some of the Contact Center, Communication Manager, and Session Manager troubleshooting utilities. For more detailed information about troubleshooting with the Session Manager traceSM utility, see the Session Manager documentation. For more detailed information about troubleshooting with the Communication Manager list trace command, see the Communication Manager documentation.

This section introduces the Communication Manager and Session Manager tools that you can use the troubleshoot calls that go from the Communication Manager, through Session Manager, to Contact Center.

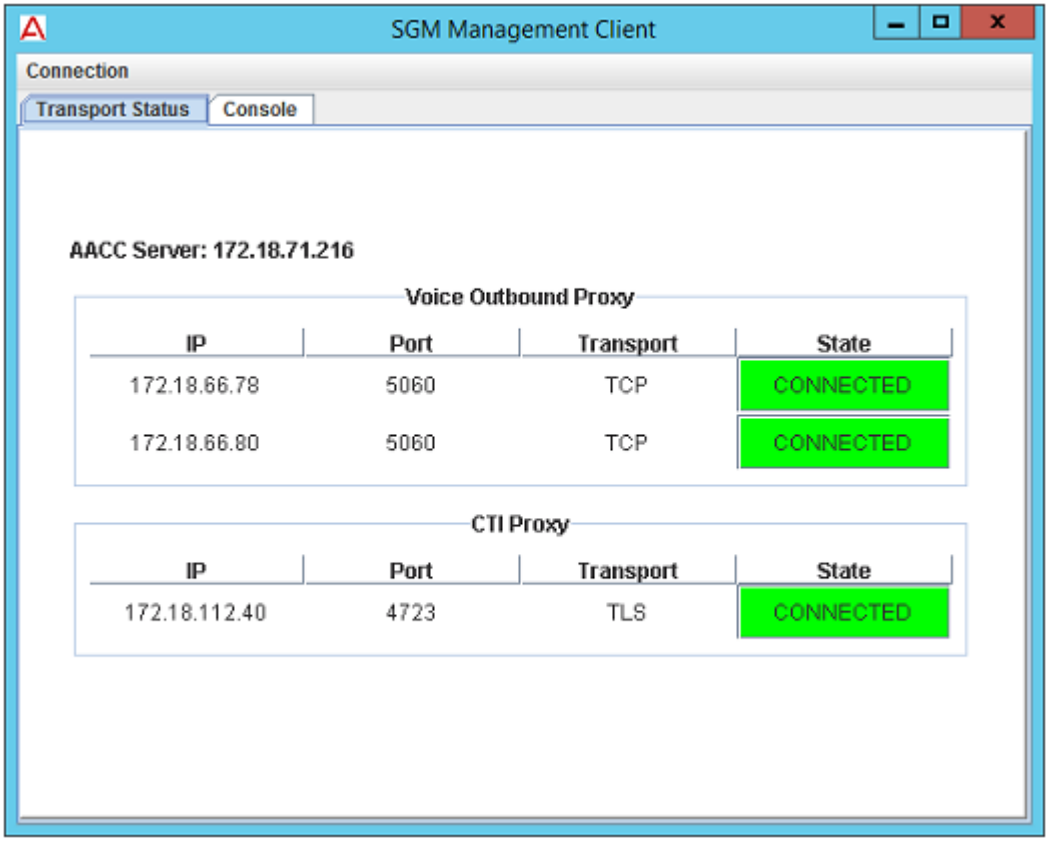
In the following worked example, a Communication Manager extension (43001) dials a Contact Center CDN (Route Point) 53000. Contact Center then routes the call to an agent. The contact center agent is using Communication Manager extension (43000).

The following table shows the details of the components used in this worked example:

Component	Value
Communication Manager phone extension (Substituting for a Customer's phone)	43001
Communication Manager phone 43001 IP address	172.18.120.187
Media Gateway	172.18.112.101
Avaya Aura® Contact Center Route Point (CDN)	53000
Avaya Aura® Contact Center (HA managed) IP address	172.18.71.217
Avaya Aura® Contact Center SIP Entity name	AACCMANTESTBG
Session Manager SIP Entity name	Vedupsm1
Communication Manager SIP Entity name	CommunicationManagerOne
Avaya Aura® Media Server	172.18.71.219

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **SIP Gateway Management Client**.
3. Click **Connect**.
4. Confirm that Contact Center can communicate with the Application Enablement Services (**CTI Proxy**), and the Session Manager (**Voice Outbound Proxy**). The example High Availability solution has two Session Managers.



In this example, the Contact Center server 172.18.71.216 (the active server of the AACCMANTESTBG High Availability pair) is communicating with two Session Managers and Avaya Aura® Application Enablement Services.

If your Contact Center server does not connect to the Session Manager(s) or Application Enablement Services, verify the Contact Center configuration details using the Contact Center Manager Server Server Configuration utility.

5. Log on to the Communication Manager System Access Terminal (SAT) interface.
6. On the Communication Manager SAT interface, to define a trace filter for the station 43001, enter the following command:

   ```
   list trace station 43001
   ```

```
display station 43001
                                    STATION

Extension: 43001                        Lock Messages? n               BCC: 0
     Type: 9640                         Security Code: 12345678         TN: 1
     Port: S09017                     Coverage Path 1:                 COR: 1
     Name:                            Coverage Path 2:                 COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
             Loss Group: 19          Personalized Ringing Pattern: 1
                                               Message Lamp Ext: 43001
          Speakerphone: 2-way               Mute Button Enabled? y
       Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
         Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                         IP SoftPhone? y

                                          IP Video Softphone? n
                                 Short/Prefixed Registration Allowed: default

                                          Customizable Labels? y
Command aborted
Command: list trace stat 43001
```

The Communication Manager trace is now configured and ready to record activity on extension 43001.

```
list trace station 43001                                              Page   1

                                LIST TRACE

time            data

08:11:17 TRACE STARTED 02/15/2013 CM Release String cold-02.0.823.0-20199
```

7. Log on to the Session Manager management console.
8. On the Session Manager management console, enter `traceSM -x -m`

```
login as: cust
This system is restricted solely to authorized users for legitimate business pur
poses only. The actual or attempted unauthorized access, use, or modification of
 this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or crimina
l and civil penalties under state, federal, or other applicable domestic and for
eign laws.

The use of this system may be monitored and recorded for administrative and secu
rity reasons.  Anyone accessing this system expressly consents to such monitorin
g and recording, and is advised that if it reveals possible evidence of criminal
 activity, the evidence of such activity may be provided to law enforcement offi
cials.
All users must comply with all corporate instructions regarding the protection o
f information assets.

Using keyboard-interactive authentication.
Password:
Last login: Mon Feb 11 17:13:29 GMT 2013 from vistaclient01.siptraffic.com on pt
s/1
[cust@vedupsm1 ~]$ traceSM -x -m
```

9. After the traceSM utility starts, press **f**, to define a trace filter.
10. To define a traceSM filter for the Communication Manager extension 43001, enter, `-u 43001`

```
/-------------------------------------------------------------------------\
|Filter Usage:                                                            |
|  -u <URI|NUMBER>  Filter calls that contain <URI|NUMBER> in             |
|                   the 'From' or 'To' field.                             |
|  -i <IP>          Filter SIP messages from/to <IP> address.             |
|  -c <CALL-ID>     Filter based on the SIP 'Call-ID' header field.       |
|  -g <HEA>=<VALUE> Filter SIP header field <HEA> for value <VALUE>.      |
|  -or              Use a logical OR operator instead of the implicit     |
|                   AND when using multiple filter options.               |
|  -nr              Do not display REGISTER messages.                     |
|  -ns              Do not display SUBSCRIBE/NOTIFY messages.             |
|  -no              Do not display OPTIONS messages.                      |
|  -na              Do not display SM related messages.                   |
|Filter examples:                                                         |
| To display a call to/from 3035556666 and not REGISTER messages:         |
|    -u 3035556666 -nr                                                    |
| To display SIP messages from/to 1.1.1.1 and 2.2.2.2:                    |
|    -i "1.1.1.1|2.2.2.2"                                                 |
|                                                                         |
|Current Filter: <NO FILTER>                                              |
|New Filter: -u 43001                                                     |
\-------------------------------------------------------------------------/
```

11. On the traceSM utility, press **s**, to start a trace filter.

The Session Manager trace is now configured and ready to record activity for the Communication Manager extension 43001.

12. Using the Communication Manager desk phone (extension 43001), dial the Contact Center Route Point (53000).

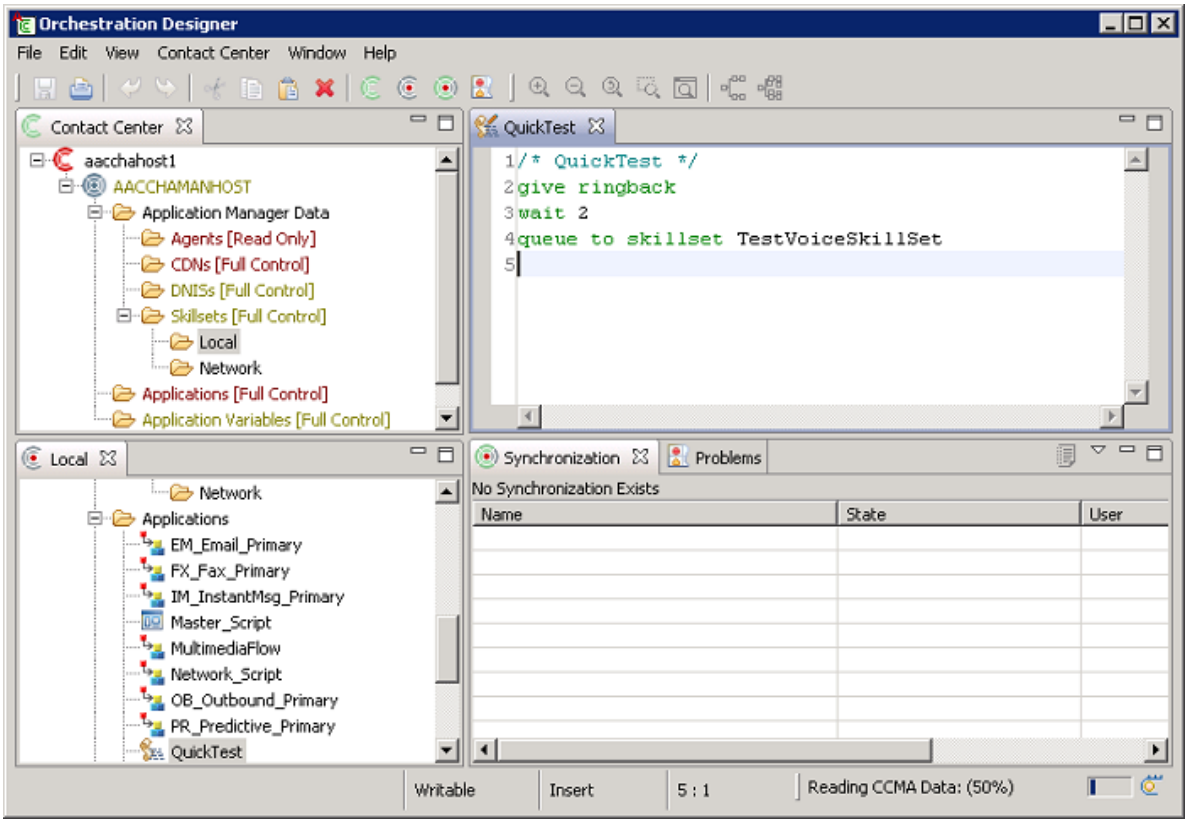
    On the Communication Manager desk phone (extension 43001), listen for the dial-tone and then ring back tones as the call is sent to Contact Center.

13. If the call is offered on the agent Agent Desktop client, accept or answer the call.

    If the call from the Communication Manager extension to the Contact Center agent was successful, continue to commission your solution.

    If the call was not successful, examine the Communication Manager and Session Manager trace logs for additional troubleshooting information.

14. If the call from the Communication Manager extension does get to Contact Center, but is not offered to an agent, your Contact Center Orchestration Designer flow needs troubleshooting. Consider temporarily replacing your Orchestration Designer flow with a simple script, similar to the script shown below. If the calls are then successful, you can start to debug your Orchestration Designer flow.



Example

The following is a matching set of Communication Manager and Session Manager logs for the above troubleshooting example. In this example, the call from the Communication Manager

extension through Session Manager to Contact Center is successful. It is easier to troubleshoot solutions when the components are all set to the same time and date.

Example of Communication Manager list trace:

This trace log for Communication Manager extension 43001 shows the test call progressing through the route pattern, dial plan, Uniform Dial Plan (UDP), Automatic Alternate Routing (AAR), and trunks group to the Session Manager, and onto the Avaya Aura® Media Server (172.18.71.219) associated with Contact Center.

```
list trace station 43001

06:18:37 TRACE STARTED 02/18/2013 CM Release String cold-02.0.823.0-20199
06:19:17     active station      43001 cid 0x25b
06:19:17     G711MU ss:off ps:20
                rgn:1 [172.18.120.187]:3132
                rgn:1 [172.18.112.101]:2074
[Comment: CM ext 43001 goes off-hook and gets dial-tone from the Media Gateway]
06:19:20     dial 53000 route:UDP|AAR
[Comment: Ext 43100 dials AACC Route Point (CDN) 53000]
06:19:20     term trunk-group 1      cid 0x25b
06:19:20     dial 53000 route:UDP|AAR
[Comment: The CM dial Plan uses Uniform Dial Plan and Automatic Alternate Routing]
06:19:20     route-pattern  1 preference 1 location 1/ALL  cid 0x25b
06:19:20     seize trunk-group 1 member 3    cid 0x25b
[Comment: CM uses route-pattern 1 to send the call (to AACC CDN) out on trunk group 1
to SM1]
06:19:20     Calling Number & Name NO-CPNumber NO-CPName
06:19:20 SIP>INVITE sip:53000@siptraffic.com SIP/2.0
06:19:20     Call-ID: 06484a0ee7be21ee24512e233a00
06:19:20     Setup digits 53000
06:19:20     Calling Number & Name *43001 EXT 43001

06:19:20 SIP<SIP/2.0 100 Trying06:19:20     Call-ID: 06484a0ee7be21ee24512e233a00
06:19:20     Proceed trunk-group 1 member 3    cid 0x25b
06:19:20 SIP<SIP/2.0 180 Ringing
06:19:20     Call-ID: 06484a0ee7be21ee24512e233a00
06:19:20     Alert trunk-group 1 member 3    cid 0x25b
06:19:20 SIP<SIP/2.0 200 OK
06:19:20     Call-ID: 06484a0ee7be21ee24512e233a00
06:19:20 SIP>ACK sip:53000@172.18.71.217:5060;transport=tcp SIP/2.0
06:19:20     Call-ID: 06484a0ee7be21ee24512e233a00
06:19:20     active trunk-group 1 member 3    cid 0x25b
06:19:20     G711MU ss:off ps:20
                rgn:1 [172.18.71.219]:14002
                Rgn:1 [172.18.112.101]:2068
06:19:20     xoip options: fax:Relay modem:off tty:US  uid:0x50003
                xoip ip: [172.18.112.101]:2068

06:19:20 SIP>INVITE sip:53000@172.18.71.217:5060;transport=tcp SIP/206:19:20 SIP>.0
06:19:20     Call-ID: 06484a0ee7be21ee24512e233a00
06:19:20 SIP<SIP/2.0 100 Trying06:19:20     Call-ID: 06484a0ee7be21ee24512e233a00
06:19:21 SIP<SIP/2.0 200 OK06:19:21     Call-ID: 06484a0ee7be21ee24512e233a00
06:19:21     G711MU ss:off ps:20
                    rgn:1 [172.18.120.187]:3132
                    rgn:1 [172.18.71.219]:14002
06:19:21 SIP>ACK sip:53000@172.18.71.217:5060;transport=tcp SIP/2.0
06:19:21     Call-ID: 06484a0ee7be21ee24512e233a00
06:19:21     G711MU ss:off ps:20
[Comment: The call to the AACC CDN is anchored on the Avaya Aura© Media Server
(172.18.71.219) conference port]
                    rgn:1 [172.18.71.219]:14002
```

```
                rgn:1 [172.18.120.187]:3132
```

Example of Session Manager trace log:

This Session Manager trace log for Communication Manager extension 43001 shows the test call routed to the Contact Center HA managed IP address 172.18.71.217. The trace shows the messaging between the Communication Manager SIP Entity (CommunicationManagerOne), the Session Manager SIP Entity (Vedupsm1), and the Contact Center (AACC) SIP Enitiy (AACCMANTESTBG).

```
Capturing... | s=Stop q=Quit ENTER=Details f=Filters w=Write a=SM c=Clear i=IP >
------------------------------------------------------------------------------------------
--------------------------
   CommunicationManagerOne      AACCMANTESTBG
                       SM100
------------------------------------------------------------------------------------------
--------------------------
10:15:12,765 |        Routing SIP request        | SipEntity: AACCMANTESTBG
EntityLink: Vedupsm1->TCP:5060
10:15:12,770 |  No hostname resolution required  | Routing to:
sip:172.18.71.217;transport=tcp;lr;phase=terminating
10:15:12,770 |          Location found           | Location: Galway
10:15:12,773 |           |--INVITE-->|           | (1) T:53000 F:+43001 U:53000
P:terminating
10:15:12,822 |           |<--Trying--|           | (1) 100 Trying
10:15:12,822 |           |<--Ringing-|           | (1) 180 Ringing
10:15:12,860 |<--Ringing-|           |           | (1) 180 Ringing
10:15:12,901 |           |<--200 OK--|           | (1) 200 OK (INVITE)
10:15:12,916 |<--200 OK--|           |           | (1) 200 OK (INVITE)
10:15:12,920 |----ACK--->|           |           | (1) sip:53000@172.18.71.217
10:15:12,932 |           |----ACK--->|           | (1) sip:53000@172.18.71.217
10:15:12,959 |--reINVIT->|           |           | (1) T:53000 F:+43001 U:53000
10:15:12,964 |<--Trying--|           |           | (1) 100 Trying
10:15:12,974 |           |--reINVIT->|           | (1) T:53000 F:+43001 U:53000
10:15:13,140 |           |<--Trying--|           | (1) 100 Trying
10:15:13,180 |           |<--200 OK--|           | (1) 200 OK (INVITE)
10:15:13,199 |<--200 OK--|           |           | (1) 200 OK (INVITE)
10:15:13,208 |----ACK--->|           |           | (1) sip:53000@172.18.71.217
10:15:13,215 |           |----ACK--->|           | (1) sip:53000@172.18.71.217
Capturing... |            s=Stop q=Quit ENTER=Details f=Filters w=Write a=SM c=Clear
i=IP r=RTP d=Calls
```

Troubleshooting anonymous or invalid SIP headers

About this task

Troubleshoot when SIP From headers are populated with anonymous@anonymous.invalid mailto:anonymous@anonymous.invalid.

Procedure

Ensure the agent workstations are added to the private/public numbering tables. Adding agent workstations to the numbering tables ensures that the incoming SIP requests contain “From” headers that contain the agent's Uniform Resource Identifier (URI). For more information, see Adding agent workstations to the numbering tables on page 63.

Verifying Communication Manager station phones

About this task

To ensure proper integration and Contact Center control, Avaya Aura® Communication Manager stations (telephones) must match these configuration requirements:

- Contact Center supports a maximum of three Call Appearance lines per agent station.
- Restrict Last Appearance must be enabled on all agent stations.
- Call Forwarding is not supported on agent stations, apart from the coverage path settings. For more information about coverage path setting, see Coverage Path configuration on page 181.
- Priority call feature is not supported on agent stations.
- Bridged Appearance is not supported on agent stations.

Perform the following checks on each Communication Manager station to be controlled by Contact Center and used as an agent telephone.

Procedure

1. Verify that each Communication Manager station has button number one configured for Call Appearance, for example; **BUTTON ASSIGNMENTS 1: call-appr**.
2. Verify that each Communication Manager station has button number two configured for Call Appearance, for example; **BUTTON ASSIGNMENTS 2: call-appr**.
3. Verify that Call Appearance is not set on the remaining buttons.

   Three Call Appearance buttons are supported. Disable Call Appearance on the other buttons.
4. Verify **Restrict Last Appearance** is enabled on all agent stations, for example; **Restrict Last Appearance? y**.
5. Verify IP Softphone is enabled on all agent stations using a softphone, for example; **IP SoftPhone? y**.

Troubleshooting when agents cannot log on to Agent Desktop

About this task

If agents cannot log on to Avaya Agent Desktop, perform the following checks.

Procedure

1. Verify that TR87 is enabled on the Avaya Aura® Application Enablement Services (AES) server.

   For more information, see Enabling TR87 on the AES on page 106.

2. Verify that you imported certificates into the AES server.

   For more information see Importing a Certificate Authority root trusted certificate into AES on page 107.

3. Verify that you imported certificates into the AES server.

   For more information see Importing a signed certificate into AES on page 111.

4. Ensure that the Contact Center Manager Server is a trusted host on the AES server.

   For more information, see Adding Contact Center Manager Server as a trusted host on AES on page 112.

5. Ensure network connectivity is configured between the Avaya Aura® Unified Communications platform, CCMS, and Agent Desktop computers in the network and that all computers can ping each other.

6. Ensure that all Avaya Aura® Unified Communications platform and Contact Center servers can communicate with each other by host name, Fully Qualified Domain Name (FQDN), and IP address. Ensure that they can ping each other.

Troubleshooting AES certificate errors

About this task

Troubleshoot when, on the AE Services page of the AES Management Console, the following error appears: “The installed AE Server Certificate is invalid. Use Certificate Management -> Server Certificate page to to resolve this issue.”

Perform the following procedure to resolve this issue.

Procedure

1. Log on to the AES management console.
2. Click **Security** > **Certificate Management** > **CA Trusted Certificates**.
3. Select the avayaprca certificate, and click **Export**.
4. Copy the CA certificate text contents into a text editor, such as Notepad.
5. Save the file, for example save the file as OAMCert.txt.
6. On the **CA Trusted Certificates** page, click **Import**.
7. Under **Trusted Certificate Import**, click **Browse**.
8. Navigate to the OAMCert.txt file and click **Open**.
9. In the **Certificate Alias** box, type an alias for the certificate, for example OAMCert.
10. Click **Apply**.

    On the AE Services page of the AES Management Console, verify the error is now cleared.

Index

A

B

C

D

E

F

G

H

I

L

M

O

P

Q

R

S

T

U

V