Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration

Release 6.3
NN44400-521
Issue 04.02
May 2013

Notice

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

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its 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 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 its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

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. 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.

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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products". 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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that 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"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a

corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

Trademarks

Avaya, the Avaya logo, Avaya one-X® Portal, Avaya Aura® Communication Manager, Avaya Aura® Experience Portal, Avaya Aura® Orchestration Designer, Avaya Aura® Session Manager, Avaya Aura® System Manager, and Application Enablement Services are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: New in this release

The following sections detail what is new in *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* (NN44400-521).

Features

See the following sections for information about feature changes:

Communication Manager fallback options

Avaya Aura® Contact Center solutions that do not use High Availability can support a number of alternative fallback options. You can configure your solution to reroute customer calls to Avaya Aura® Communication Manager or Avaya Aura® Call Center Elite if Avaya Aura® Contact Center is offline or stopped for maintenance.

The two main fallback options are:

- Automatic fallback to an Avaya Aura® Communication Manager Hunt Group.
- Manual fallback to an Avaya Aura® Call Center Elite skill, split, or Hunt Group.

If Avaya Aura® Contact Center is unable to process voice contacts, Avaya Aura® Session Manager can automatically reroute customer calls intended for Contact Center to an Avaya

Aura® Communication Manager Hunt Group. This option does not require an Avaya Aura® Call Center Elite license.

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

For more information about choosing a fallback option, see Choosing a fallback option on page 20.

For more information about automatic fallback to a Communication Manager Hunt Group, see Fallback to Avaya Aura Communication Manager Hunt Group configuration on page 169.

For more information about manual fallback to an Avaya Aura® Call Center Elite skill, see Fallback to Avaya Aura Call Center Elite skill configuration on page 211.

Contact Center agent phones

Each Avaya Aura® Contact Center agent extension requires two call appearance lines to be configured on the corresponding Communication Manager station. Avaya Aura® Contact Center supports a maximum of two call appearance lines per agent station.

If your solution includes Avaya Aura® Call Center Elite, and if you plan to configure fallback to Elite, you may configure some additional features on the Communication Manager extensions used by Avaya Aura® Contact Center agents.

Communication Manager desk phones have programmable buttons. You can create feature buttons by assigning features or functionality to these programmable buttons.

In solutions with Avaya Aura® Call Center Elite and Avaya Aura® Contact Center, agents can log on to either Contact Center or Elite. Agents must not log in to both Avaya Aura® Call Center Elite and Avaya Aura® Contact Center at the same time. Agents can log on to Elite and use the Communication Manager and Elite feature buttons on their desk phone. Or agents can log on to Avaya Aura® Contact Center.

Avaya Aura® Contact Center and Avaya Aura® Agent Desktop do not provide support for Communication Manager or Elite feature buttons, but the existence of the feature buttons on agent phones does not adversely impact agent functionality or call control during normal Contact Center operation. The feature buttons are supported only on the Avaya Aura® Contact Center agent desk phones used for Elite fallback support.

For more information about Contact Center agent desk phone supported feature buttons, see Contact Center agent desk phone supported features on page 22.

Support for Coverage Path

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. For more information, see Coverage Path configuration on page 233.

Avaya Aura® Unified Communications platform support

Avaya Aura® Contact Center Release 6.3 supports integration with the Avaya Aura® Unified Communications Platform Release 6.1 and 6.2.

This integration gives Contact Center access to and control of the Avaya Aura® Unified Communications solution and phones. The Avaya Aura® Unified Communications platform benefits by accessing Contact Center skill-based routing, call treatments, reporting, and the graphical Orchestration Designer.

Avaya Aura® Solution for Midsize Enterprise platform support

Avaya Aura® Contact Center Release 6.3 supports integration with the Avaya Aura® Solution for Midsize Enterprise platform Release 6.1 and 6.2.

The Avaya Aura® Solution for Midsize Enterprise Solution Template delivers the following applications for use as virtual machines running on the Avaya Aura® System Platform:

For Avaya Aura® Solution for Midsize Enterprise (ME) platform Release 6.1:

- Avaya Aura® Communication Manager 6.0.1
- Avaya Aura® Session Manager 6.1
- Avaya Aura® System Manager 6.1
- Avaya Aura® Presence Services 6.1
- Avaya Aura® Utility Services 6.1
- Avaya Aura® Application Enablement Services 6.1

For Avaya Aura® Solution for Midsize Enterprise (ME) platform Release 6.2:

- Avaya Aura® Communication Manager 6.2
- Avaya Aura® Session Manager 6.2
- Avaya Aura® System Manager 6.2

- Avaya Aura® Presence Services 6.1
- Avaya Aura® Utility Services 6.2
- Avaya Aura® Application Enablement Services 6.1.2.0.32

Avaya Aura® System Manager support

Avaya Aura® System Manager delivers a set of shared, secure management services and a common console across multiple products. You use Avaya Aura® System Manager to manage and configure the routing policies for all Avaya Aura® Session Manager instances in your solution. Avaya Aura® System Manager communicates with Session Manager using secure links.

Avaya Aura® Session Manager support

Avaya Aura® Contact Center Release 6.3 supports integration with the Avaya Aura® Session Manager.

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 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.
- Avaya Communication Server 1000 Release 7.5 SIP-enabled PABX.

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

Contact Center default TLS certificates

Avaya Aura® Contact Center Release 6.3 supplies a set of default certificates for use with Avaya Aura® Application Enablement Services. If you do not have access to or require a third-party Certificate Authority, you can install these Contact Center default certificates on your Application Enablement Services (AES) server to quickly establish a link between the two systems.

Important:

AES 6.2 and later includes the default trust certificates. Using the default certificates Avaya Aura® Contact Center automatically communicates with AES.

For more information about Avaya Aura® Contact Center default certificates, see Application Enablement Services configuration on page 115.

SIP users and SIP Endpoint

Avaya Aura® Contact Center Release 6.3 supports a limited range of SIP Endpoints as agent stations.

For more information about SIP endpoints, see SIP Endpoints configuration on page 241.

Supported phones

Avaya Aura® Contact Center Release 6.3 supports the following additional phones:

- Avaya 1600 Series IP H.323 deskphones
- Avaya 24xx Series digital deskphones
- Avaya 64xx Series digital deskphones
- Avaya 96x0 Series SIP deskphones

For the complete list of supported phones, see Communication Manager configuration on page 31.

Chapter 2: 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 Aura® Agent Desktop supports Avaya Aura® Unified Communications phones and continues to support voice, email, and Web chat contact types.

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

Avaya Aura® component	Release	Patch level
Avaya Aura® System Platform	1.1.1.0.2	
Avaya Aura® Midsize Business Template (MBT)	5.2.1.3.6*	
Midsize Business Template Communication Manager	5.2.1*	
Midsize Business Template SIP Enablement Services	5.2.1*	
Midsize Business Template Application Enablement Services	5.2.1*	Super Patch 2 and 3
Standalone Avaya Aura® Communication Manager	5.2.1*	
Standalone Avaya Aura® SIP Enablement Services	5.2.1*	
Standalone Avaya Aura® Application Enablement Services	5.2.2*	Super Patch 2
Standalone Avaya Aura® Communication Manager	6.0.1	SP2
Standalone Avaya Aura® System Manager	6.1	SP1.1, SP2, SP4***
Standalone Avaya Aura® Session Manager	6.1	SP2, SP4****
Standalone Avaya Aura® Application Enablement Services	6.1.0.20**	Super Patch 2
Standalone Avaya Aura® Communication Manager	6.2-02.0.823.0	
Standalone Avaya Aura® System Manager	6.2.12.0	
Standalone Avaya Aura® Session Manager	6.2.0.0.620120	
Standalone Avaya Aura® Application Enablement Services	6.1.2.0.32	

Avaya Aura® component	Release	Patch level
Standalone Avaya Aura® Communication Manager	6.2-02.0.823.0	
Standalone Avaya Aura® System Manager	6.2.12.0	
Standalone Avaya Aura® Session Manager	6.2.0.0.620120	
Standalone Avaya Aura® Application Enablement Services	6.2	
Avaya Aura® Solution for Midsize Enterprise	6.1	
Midsize Enterprise Communication Manager	6.0.1	SP2
Midsize Enterprise Session Manager	6.1	SP2
Midsize Enterprise Application Enablement Services	6.1.0.20	Super Patch 2
Avaya Aura® Solution for Midsize Enterprise	6.2.0.0.3105	
Midsize Enterprise Communication Manager	6.2-02.0.823.0	
Midsize Enterprise Session Manager	6.2.0.0.620120	
Midsize Enterprise Application Enablement Services	6.1.2.0.32	
Avaya Aura® Virtualized Environment (Communication Manager, System Manager, Session Manager, Application Enablement Services)	6.2	FP2

- Note *: Avaya Aura® Contact Center Release 6.3 does not support Avaya Aura® Midsize Business Template (MBT) or the Avaya Aura® 5.2 platform for new installations. Existing Avaya Aura® Contact Center solutions using these components are supported.
- Note **: To support the Avaya Aura® Contact Center–Mission Critical High Availability feature, the Avaya Aura® Application Enablement Services server must be Release 6.1.1 or later.
- Note ***: To support the Avaya Aura® Contact Center–Mission Critical High Availability feature, the Avaya Aura® System Manager must be Release 6.1 SP4 or later.
- Note ****: To support the Avaya Aura® Contact Center–Mission Critical High Availability feature, the Avaya Aura® Session Manager must be Release 6.1 SP4 or later.

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® Contact Center Planning and Engineering* (NN44400-210).
- Read *Avaya Aura® Contact Center Installation Checklist* (NN44400-310).
- Read *Avaya Aura® Contact Center Installation* (NN44400-311).
- Read *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- Read *Avaya Aura® Session Manager Overview.*
- Read *Administering Avaya Aura® Session Manager*.

Related resources

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Support

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

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*.
- Read *Avaya Aura® Contact Center Installation Checklist* (NN44400-310).

Navigation

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® Session Manager to forward calls, based on a dial pattern, to the Contact Center.
  - Add Contact Center as a SIP Entity on the Avaya Aura® 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 (not applicable with default certificates and AES 6.2 and later)
  - Add Contact Center as a trusted host.

The 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 (not applicable with default certificates and AES 6.2 and later)
- 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* (NN44400-312).

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 via 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).

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 211.
- 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 169.

- 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 211.

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.

In solutions that support Avaya Aura® Contact Center fallback to Avaya Aura® Call Center Elite, agents may 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 Aura® 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.
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

Feature	Button Name or Label	Impact on Contact Center	Comment
			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.
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.

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

High Availability Avaya Media Server

High Availability Avaya 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 Media Server cluster, then you must disable ARP Inspection on the G430/G450. If an Avaya Media Server fails, the G430/G450 can then communicate with the other Avaya 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 Media Server and G6xx configuration

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

Chapter 4: System Platform configuration

Avaya Aura® System Platform is a real-time virtualization technology that enables unmodified versions of Avaya Aura® Communication Manager, or Avaya Aura® Session Manager, Avaya Aura® Application Enablement Services, Utility Services, and Media Services to be deployed on a single server.

The Avaya Aura® Solution for Midsize Enterprise packages four key Avaya Aura® applications on one server platform using System Platform technology. It also includes key supporting applications and utilities designed to simplify deployment and reduce ongoing ownership costs.

The Avaya Aura® Solution for Midsize Enterprise puts Unified Communications within reach of midsize enterprises. It simplifies IP/SIP telephony, streamlines management and lowers energy costs because the necessary Avaya Aura® applications and utilities are deployed on only one server instead of across multiple pieces of hardware.

This section describes how to access the System Platform Management Console when using an Avaya Aura® Solution for Midsize Enterprise with Contact Center. After you log on to the System Platform you can access the following:

- Avaya Aura® Session Manager server
- Avaya Aura® Application Enablement Services server
- System status

Prerequisites

- Commission your Avaya Aura® Session Manager server.
- Commission your Avaya Aura® Application Enablement Services server.
- Ensure that you have log on permission for System Platform.

Navigation

- Accessing the System Platform Web console on page 28
- Confirming the template version on page 30

Accessing the System Platform Web console

About this task

You can view the System Platform information by accessing the System Platform Management Console from a Web browser on a computer connected to the same network as the System Platform server.

Procedure

1. Start a Web browser.
2. In the **Address** box, type the following URL: `https://<ipaddress>/webconsole`, where <*ipaddress*> is the IP address for the Console Domain that you configure during the System Platform installation.
   A Login dialog box appears.

   Important:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. In the **User Id** box, type your user ID.

   The default log on User ID is admin.
4. Click **Continue**.
   A Password dialog box appears.
5. In the **Password** box, type your password.

   The default password is admin01.

   Avaya recommends that you change the default password after your first logon. Passwords must have at least six characters. Avaya recommends the you use only alphanumeric characters.
6. Click **Logon**.
   The system displays a Before You Begin page.
7. Click **Continue**.
   The system displays the Virtual Machine List page in the System Platform Management Console. The various administrative options are in the left navigation menu. The virtual machines are listed on the right.

Procedure job aid

The System Platform Management Console lists the virtual machines on the server, including the Session Manager (SM) server and the Application Enablement Services (AES) server. The System Platform also shows the status and some details of the individual virtual servers.

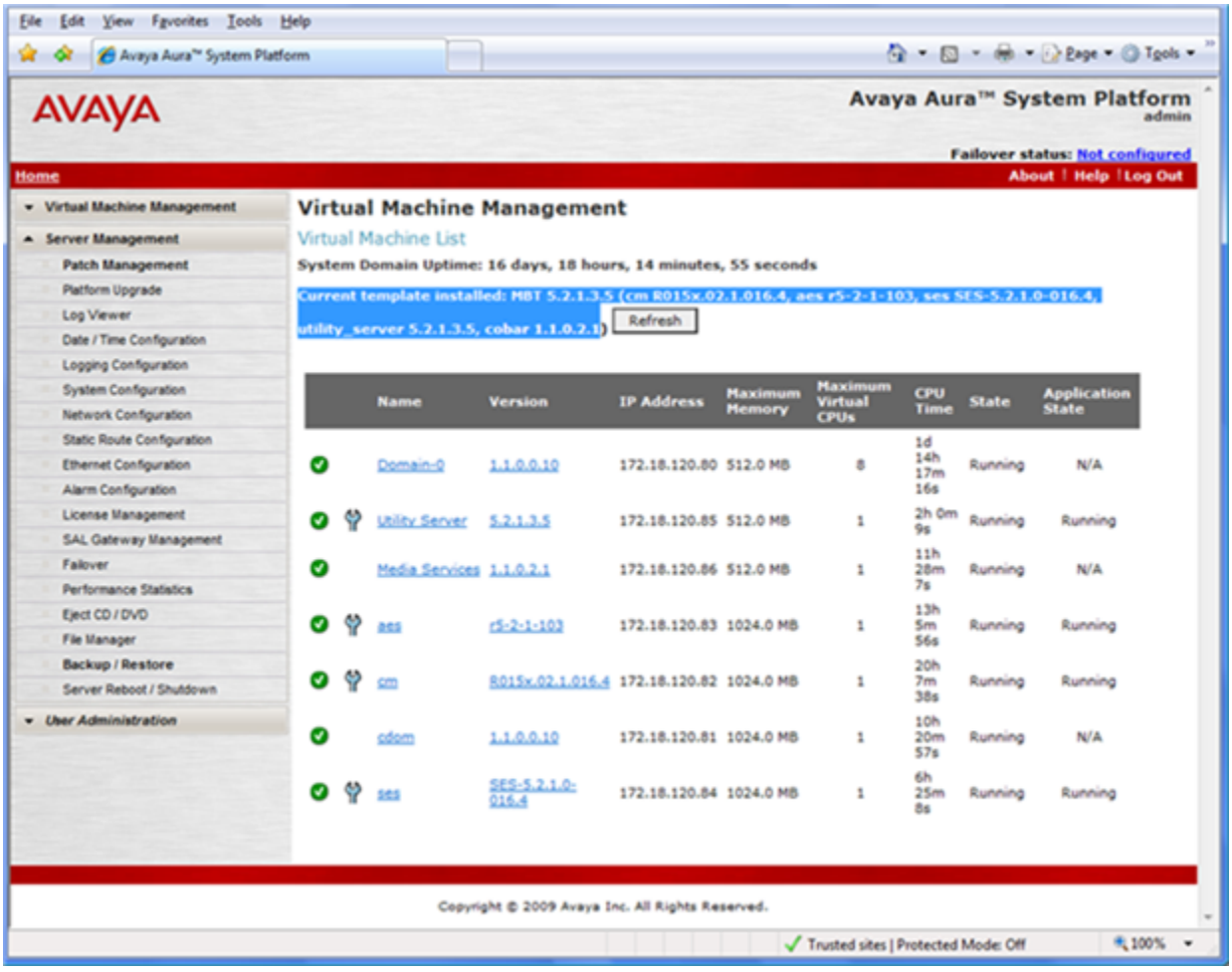


Figure 1: Example of System Platform Virtual Machine Management showing SM and AES server

Confirming the template version

Before you begin

- Log on to the System Platform Management Console from a Web browser. See Accessing the System Platform Web console on page 28.

About this task

Use the System Platform information to confirm that the Avaya Aura® Unified Communications platform template meets the minimum requirements for integration with Contact Center.

Procedure

In the top pane of the System Platform Virtual Machine Management page, confirm that the **Current template installed**: is 5.2.1.3.6, 6.0, 6.1, or 6.2.

Important:

If the **Current template installed** is less than 5.2.1.3.6, contact your Avaya Aura® Unified Communications platform Administrator and request this or a later template.

Note:

The minimum System Platform requirement is:

- 6.0.3.0.3 (required patch 6.0.3.7.3) for 6.1
- 6.2.0.0.27 for 6.2

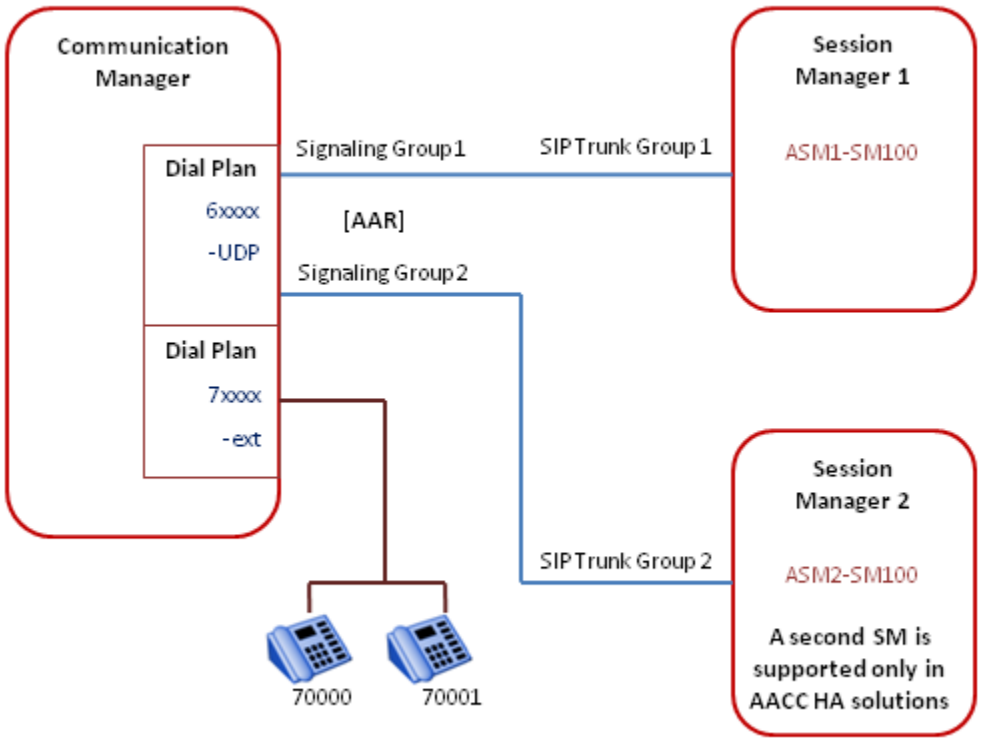
Chapter 5: Communication Manager configuration

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 2: Example Communication Manager configuration

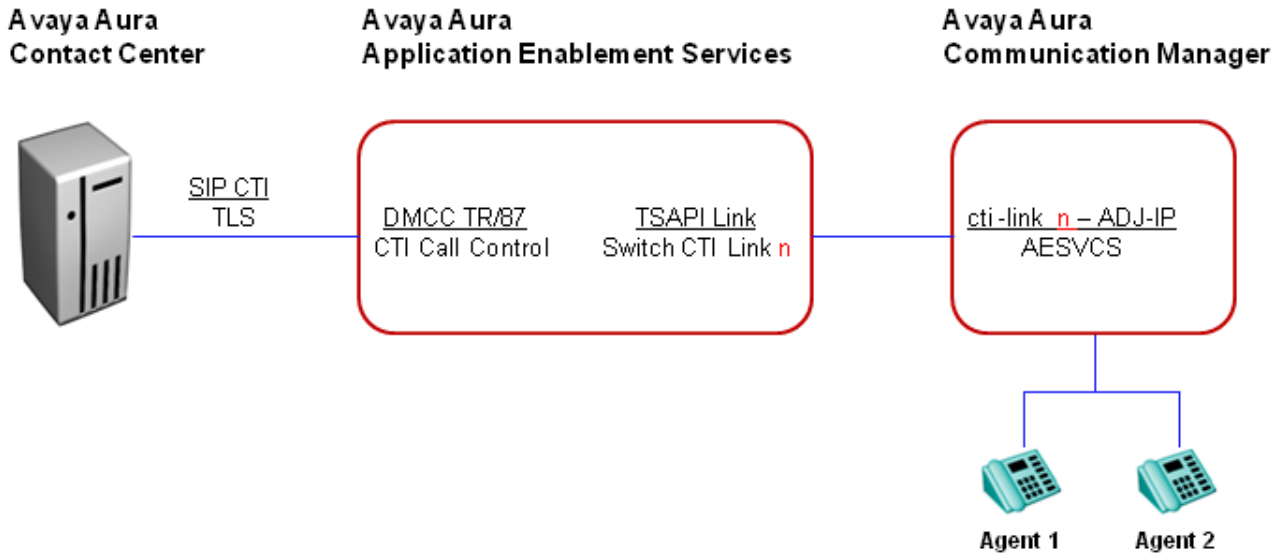


In addition to station configuration, the Communication Manager must be configured to route calls to and from Avaya Aura® Contact Center through SIP using one or more Avaya Aura® Session Managers.

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 3: 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 call scenarios:

In a SIP-enabled Contact Center with a Communication Manager, Avaya Aura® Contact Center supports a maximum of 2 call appearance lines configured per agent station with Restrict Last Appearance (RLA) configured. The following table details the call restrictions this enforces on an agent.

Table 1: Communication Manager call scenario table

Line Status / Agent Action	Receive Skillset Call	Receive Personal Call	Make Personal Call (from desk phone)	Make Personal call (from CTI)	Initiate Consult	Call Join
2 Lines Free	Yes	Yes	Yes	Yes	N/A	N/A
Skillset Call Active	No	No	Yes*	No	Yes	N/A
Personal Call Active	No	No	Yes*	No	Yes	N/A
Skillset Call and Personal Call	No	No	No	No	No	No
*Personal calls are modelled as consults.						

Communication Manager configuration procedures

About this task

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

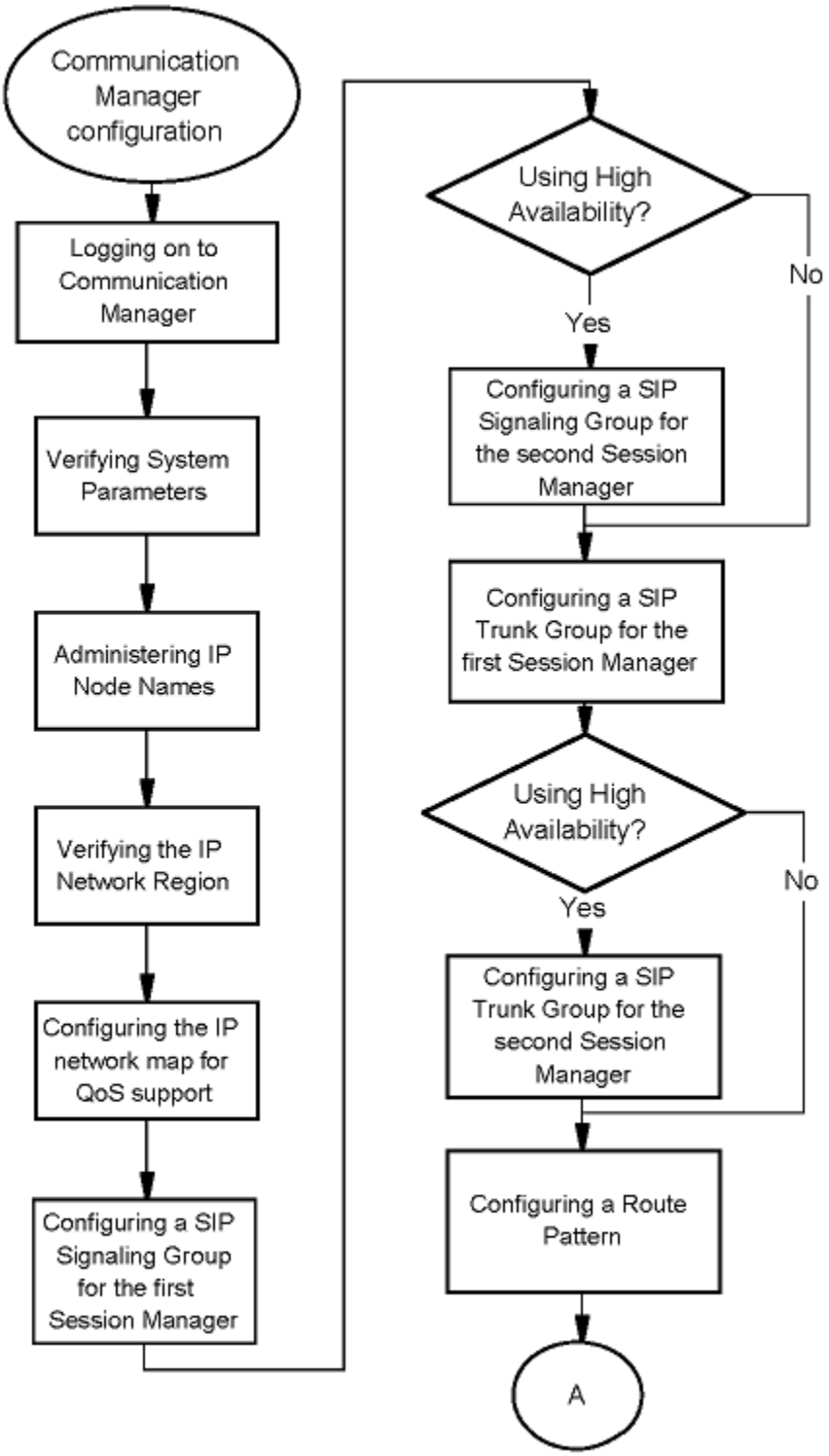


Figure 4: Communication Manager configuration procedures

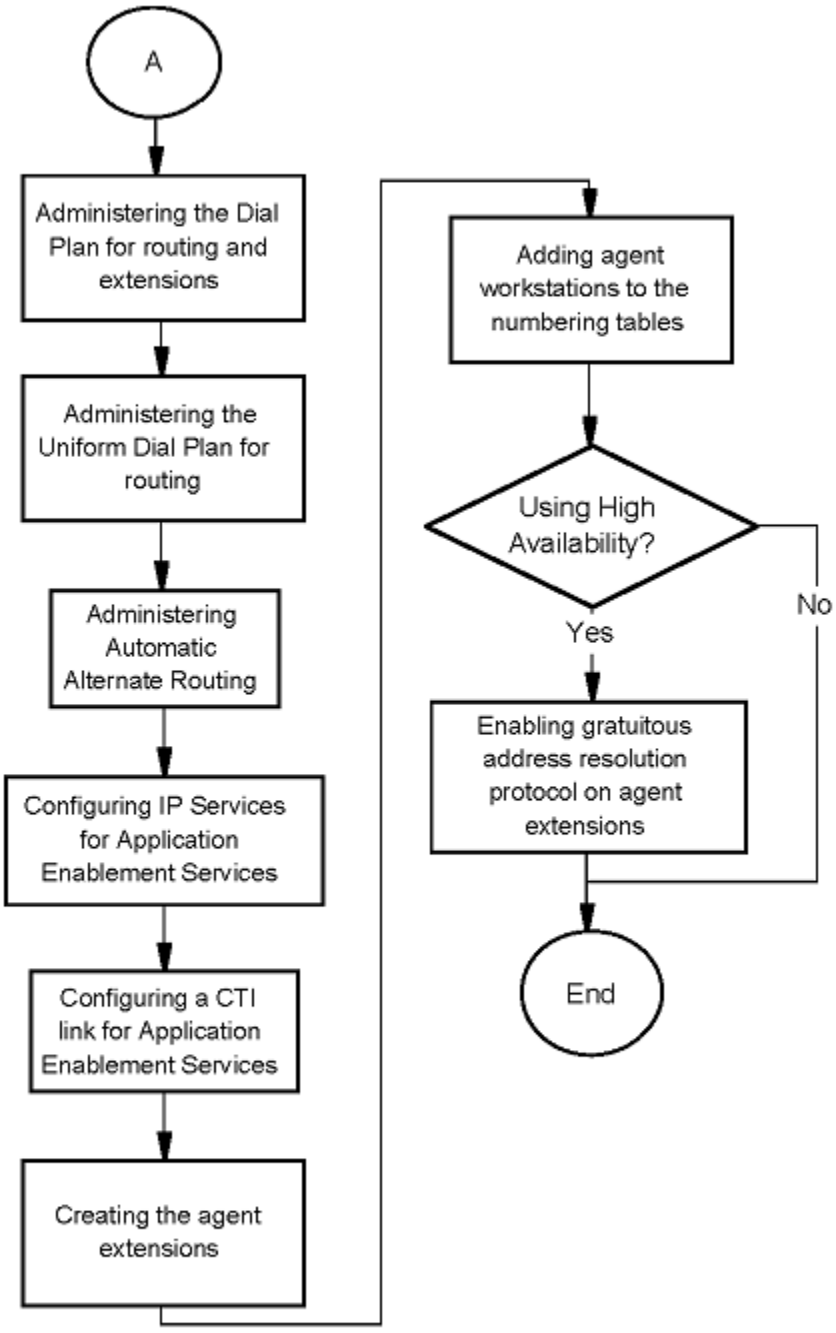


Figure 5: Communication Manager configuration procedures continued

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 Customer Options form, verify that the ISDN/SIP Network Call Redirection feature is disabled. You must disable Network Call Redirection (NCR) on your Communication Manager. There is one limitation to disabling NCR; for CDN to CDN conference scenarios, if one party goes on hold then music-on-hold is streamed by Communication Manager into the 3-party conference (provided music-on-hold is provisioned on Communication Manager).

Note:

If NCR is enabled on your Communication Manager, you must disable NCR at the trunk level before disabling it at the system level. Otherwise NCR remains enabled on the trunks even though it is disabled at the system level.

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 46.

On the Communication Manager System Parameters Features form, verify that Onhook Dialing on Terminals is disabled. This ensures phantom calls are not delivered to the soft phone.

Procedure

1. Use the System Access Terminal (SAT) interface to verify that the ISDN/SIP Network Call Redirection feature is disabled. Use the **display system-parameters** command.

```
display system-parameters customer-options                    Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                              IP Stations? y
            Enable 'dadmin' Login? y
            Enhanced Conferencing? y                        ISDN Feature Plus? y
                      Enhanced EC500? y        ISDN/SIP Network Call Redirection? n
  Enterprise Survivable Server? n                            ISDN-BRI Trunks? y
     Enterprise Wide Licensing? n                                  ISDN-PRI? y
               ESS Administration? y                 Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                       Malicious Call Trace? y
      External Device Alarm Admin? y                    Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n      Mode Code for Centralized Voice Mail? n
                  Flexible Billing? n
    Forced Entry of Account Codes? y                    Multifrequency Signaling? y
       Global Call Classification? y             Multimedia Call Handling (Basic)? y
              Hospitality (Basic)? y          Multimedia Call Handling (Enhanced)? y
  Hospitality (G3V3 Enhancements)? y                    Multimedia IP SIP Trunking? y
                       IP Trunks? y

            IP Attendant Consoles? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

2. 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
```

3. Verify that Onhook Dialing on Terminals is disabled. Use the **display system-parameters features** command. This step is required only for contact centers that use Avaya Aura® Call Center Elite.

```
display system-parameters features                              Page  10 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

                 Pull Transfer: n            Update Transferred Ring Pattern? n
         Outpulse Without Tone? y              Wait Answer Supervision Timer? n
         Misoperation Alerting? n               Repetitive Call Waiting Tone? n
    Allow Conference via Flash? y
 Vector Disconnect Timer (min):       Network Feedback During Tone Detection? y
   Hear Zip Tone Following VOA? y    System Updates Time On Station Displays? n

                   Station Tone Forward Disconnect: silence
                            Level Of Tone Detection: precise
          Charge Display Update Frequency (seconds): 30
                             Date Format on Terminals: mm/dd/yy
                   Onhook Dialing on Terminals? n
              Edit Dialing on 96xx H.323 Terminals? n
                 Allow Crisis Alert Across Tenants? n


ITALIAN DCS PROTOCOL
  Italian Protocol Enabled? n
```

4. 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
```

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

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.

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 Avaya Aura® 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 Aura® 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.

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.

Variable	Value
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.

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. Disable Network Call Redirection (NCR) on your Communication Manager. On the Trunk Group form of Communication Manager to the 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.

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. Disable Network Call Redirection (NCR) on your Communication Manager. 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

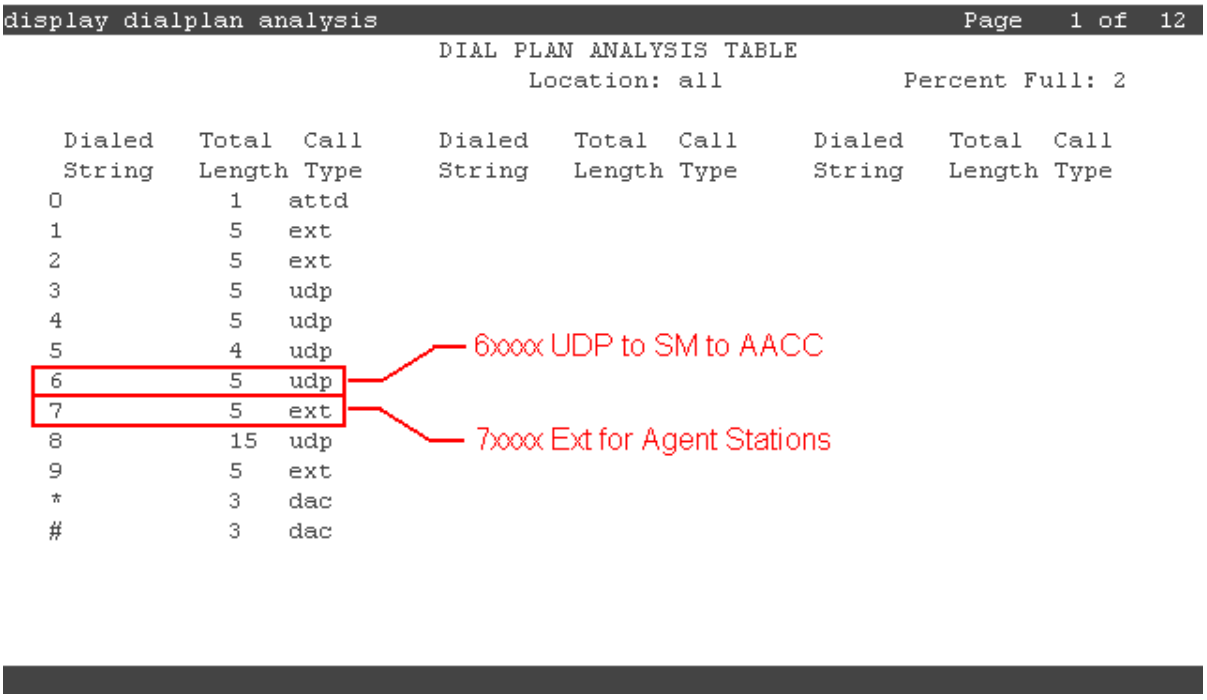
On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to create a dial plan for routing and the agent extensions. Use the **change dialplan analysis** command.

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 may 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 124.

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
```

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 2 call appearance lines 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 soft phone. When enabled, a soft phone or a desk phone can be used. When disabled, a desk phone can be used only.)

- Bridged Appearance is not supported.
- Per Station CPN - Send Calling Number enabled. Ensure this is not set to disabled, as this is not supported.

A limited configuration of Call Forwarding is supported, for more information see Coverage Path configuration on page 233.

If your solution integrates Avaya Aura® Contact Center with Avaya Aura® Call Center Elite, the following feature buttons must also be added to the Avaya Aura® Call Center Elite agent stations in Communication Manager:

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

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

- Avaya 1600 Series IP deskphones
- Avaya 4600 Series IP deskphones
- Avaya 96x0 Series IP deskphones
- Avaya 96x1 Series IP deskphones
- Avaya One-X Communicator Release 5.2 or later
- Avaya Aura® Agent Desktop embedded softphone. Provision an IP_Agent license on the Communication Manager for each softphone used by Contact Center.

Avaya Aura® Contact Center supports the following digital phones:

- Avaya 24xx Series deskphones
- Avaya 64xx Series deskphones

Avaya Aura® Contact Center supports the following SIP phones:

- Avaya 96x0 Series IP deskphones
- Avaya 96x1 Series IP deskphones
- Avaya 9608 IP deskphone
- Avaya 9611G IP deskphone
- Avaya 9621G IP deskphone
- Avaya 9641G IP deskphone

Avaya Aura® Contact Center supports SIP phones for DTMF functionality. Avaya Aura® Contact Center supports SIP phones for High Availability functionality.

Avaya Aura® 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 Avaya Aura® 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.

Communication Manager Call appearance lines on agent stations:

Avaya Aura® Contact Center supports Communication Manager stations (phones) with a maximum of 2 call appearance lines per agent station. New Communication Manager stations are automatically created with three call appearance lines, so if a station is to be used by an Avaya Aura® Contact Center agent, you must configure the new station to have a maximum of two call appearance lines. Avaya recommends that you create a custom template with 2 call-appr keys.

Procedure

1. On the Avaya Aura® 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. Use the SAT interface to create the another agent extension (workstation). Use the **`add station n`** command.

3. 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 6: 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 7: 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                                5:
 2: call-appr                                6:
 3:                                          7:
 4:                                          8:

    voice-mail
```

AACC supports only 2 call-appr buttons

Figure 8: Communication Manager station 70000 continued

Adding agent workstations to the numbering tables

About this task

Avaya Aura® Contact Center 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.
12. Press **Enter** to save your changes.

Enabling Gratuitous Address Resolution Protocol on agent extensions

About this task

If your Avaya 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 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.

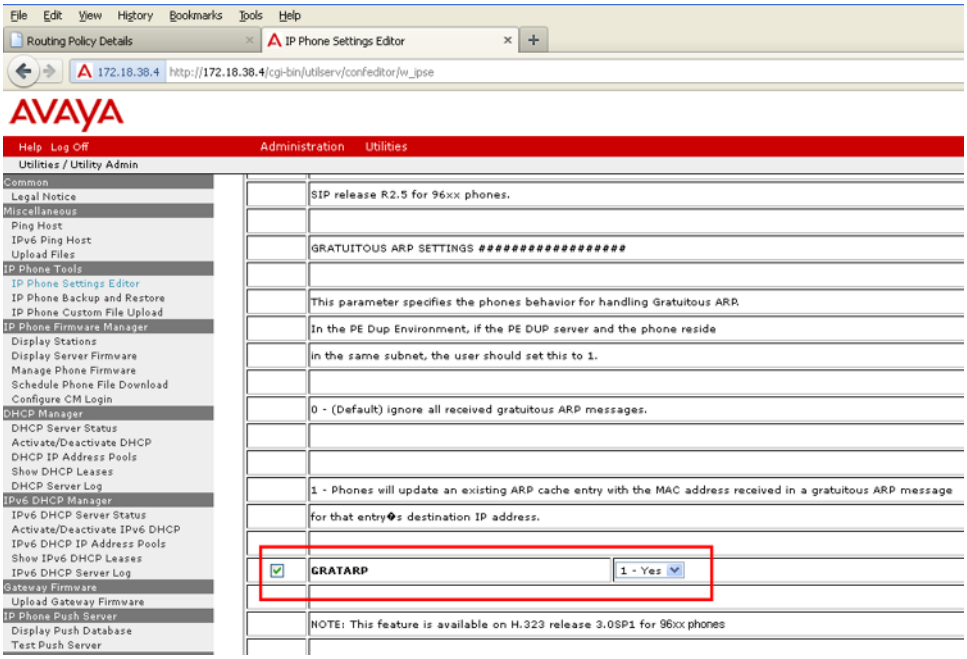
Procedure

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 Media Server in a High Availability resilient solution.

Example

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



Chapter 6: SIP Enablement Services configuration

The Avaya Aura® SIP Enablement Services (SES) provide connectivity, integration, and a smooth migration path to SIP-based communications. It is used to deploy SIP telephony alongside existing analog, digital, and IP telephones. The software is centrally managed and supports SIP trunking, SIP stations, Presence, instant messaging, and other SIP-based applications.

SIP calls to the Avaya Aura® Unified Communications platform can be redirected to Avaya Aura® Contact Center for processing, treatments, and routing to appropriate skillsets. To achieve this the Avaya Aura® SIP Enablement Services server must be configured to trust the Contact Center Manager Server (CCMS). To determine which calls to the Avaya Aura® Unified Communications platform are redirected to the Contact Center Manager Server for processing, you must configure a routing entry and contact details for the Contact Center Manager Server in SES.

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

Important:

Avaya Aura® Contact Center 6.3 does not support Avaya Aura® SIP Enablement Services (SES) for new installations. Existing Avaya Aura® Contact Center solutions that use Avaya Aura® SIP Enablement Services (SES) are supported.

Prerequisites

- Ensure that your Avaya Aura® Unified Communications platform meets the minimum template requirements for integration with Contact Center.
- Ensure that all Avaya Aura® Unified Communications platform and Contact Center servers can communicate with each other by name (host name), Fully Qualified Domain Name (FQDN), and IP address. Ensure that they can ping each other.

Navigation

Accessing the SES server Integrated Management console

Before you begin

- Log on to the System Platform Web Console, see Accessing the System Platform Web console on page 28.

About this task

When using a Midsize Business Template solution, use the System Platform to access the SIP Enablement Services server Integrated Management console.

Procedure

1. On the System Platform Virtual Machine Management, in the virtual machine list, click the spanner icon to the left of the **ses** server.
   A Before You Begin page appears.
2. Click **Continue**.
   A Logon dialog box appears.
3. In the **Logon ID** box, type your logon ID.
   The default logon ID is admin.
4. Click **Logon**.
   A Password dialog box appears.
5. In the **Password** box, type your password.

   The default password is admin01. Avaya recommends that you change the default password after your first login. Passwords must have at least six characters. Avaya recommends using only alphanumeric characters.
6. Click **Logon**.

A SIP Enablement Services System Management Interface appears.

7. On the SES System Management Interface, click **Administration**.
8. From the **Administration** list, select **SIP Enablement Services**.
   The SIP Server Management Integrated Management console opens in another browser window.

Procedure job aid

The Avaya SIP Server Management–Integrated Management is a set of applications designed to simplify system administration, provisioning, and network management, including fault and performance management.

Figure 9: Example of the SIP Server Management console

Confirming the Communication Manager Server Interface

About this task

Ensure the SIP Trunk IP Address and Server Administration Address matches the Communication Manager IP Address.

Procedure

1. In the left pane of the SIP Server Management Integrated Management console, click **Communication Manager Servers**.
   The Communication Manager Servers menu appears in the right pane.
2. Click **List Communication Managers Servers**.
   The List Communication Manager Server Address Map pane appears listing all Address Maps. The list displays the name of the Communication Manager server to which the groups of address maps apply.
3. From the list of Communication Manager Servers, identify your server and click **Edit** adjacent to that server, to view the details of your Communication Manager server.
   The Edit Communication Manager Server Interface appears.
4. In the **SIP Trunk IP Address** box, ensure that the SIP trunk IP address matches the IP address of your Communication Manager server.
5. In the **Communication Manager Server Admin Address** box, ensure that the Communication Manager server administration address matches the IP address of your Communication Manager server.
6. Click **Update**.

Procedure job aid

The Communication Manager Server Admin Logon must be created using the Communication Manager Web Interface and it must be a Privileged Administrator.

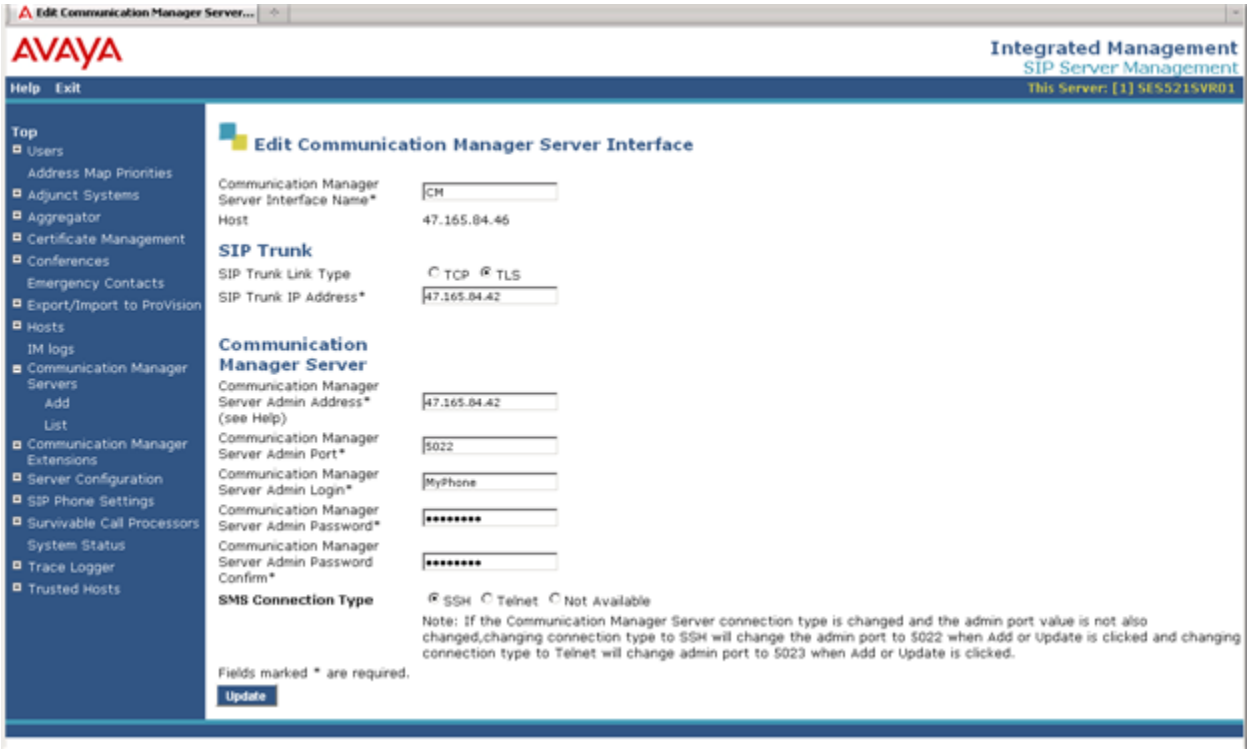


Figure 10: Example of the Communication Manager server interface

Adding a route entry to the Communication Manager

About this task

Add a route entry to the Communication Manager. The SES re-directs SIP contacts that match the route entry pattern to the Communication Manager.

Procedure

1. In the left pane of the SIP Server Management Integrated Management console, click **Communication Manager Servers**.
   The Communication Manager Servers menu appears in the right pane.
2. Click **List Communication Managers Servers**.
   The List Communication Manager Server Address Map pane appears listing all Address Maps. The list displays the name of the Communication Manager server to which the groups of address maps apply.
3. From the list of Communication Manager Servers, identify your server and click **Map** opposite that server.
4. Click **Add Map in New Group**, to add a new routing entry or address map pattern to the Communication Manager.

This also automatically creates the Communication Manager Server Interface.

5. In the **Name** box, type the name of the new map.
6. In the **Pattern** box, type the address map regular expression that matches the extension numbers to map.
7. Click **Add**.
8. Click **Continue**.
   The Address Map is added to the list.

Variable definitions

Variable	Value
Host	The name of the Communication Manager server to which this address map applies.
Name	Enter an alphanumeric name to identify the new map. This is not a network name, but a way to identify which map a set of extensions applies to.
Pattern	This is a Linux regular expression that matches the extension numbers you wish to map. Regular expressions are a way to describe text through pattern matching. The regular expression is a string containing a combination of normal text characters, which match themselves, and special meta characters, which can represent items like quantity, location, or types of characters.

Procedure job aid

An Address Map Pattern is a Linux regular expression that matches the extension numbers you wish to map. Regular expressions are a way to describe text through pattern matching. The regular expression is a string containing a combination of normal text characters, which match themselves, and special meta characters, which can represent items like quantity, location, or types of character(s).

For example, [0-9] represents any single digit and * represents any number of digits or characters. Consider the following example:

^sip:538[0-9]* matches any SIP invite message (the caret (^) matches the beginning of a line) for any extension 3 or more digits in length, beginning with the digits 538, and ending with any other sequence of digits.

Square brackets contain a selection of characters to match, with a hyphen indicating a range; so in our example, [0-9] matches any digit, or for another example, [13579] matches odd-numbered digits. Braces ({ }) which contain a whole number that matches the number of instances of the preceding item. For example, [0-9]{4} matches any four digits. Note that the braces may require escape characters: \{4\}.

Another helpful meta character is a period (.), which matches any single character; for example, the regular expression .* matches any quantity of any characters.

Figure 11: Example of routing entry or address map to Communication Manager

In the example, the SES host constructed a contact dynamically by substituting sip as the protocol, $(user) to represent the user component in the original request URI, the IP address of the host (in this case, the Home proxy server), and the port number and name of the transport to use.

Adding Contact Center Manager Server as a SES trusted host

About this task

Add the Contact Center Manager Server to the list of trusted hosts on the SIP Enablement Services (SES) server. SES does not authenticate SIP requests from trusted hosts.

Procedure

1. In the left pane of the SIP Server Management Integrated Management console, click **Trusted Hosts**.

2. Click **Add Trusted Hosts**.
   An Add Trusted Host page appears.
3. In the **IP Address** box, type the IP address of the Contact Center Manager Server server.
4. From the **Host** list, select the server to accept the SIP request from the IP address you specified.
5. Click **Add**.
6. Click **Continue**.

Adding a routing entry for the Contact Center Manager Server

About this task

Add the Contact Center Manager Server routing entry to the SIP Enablement Services (SES) server. This indicates to SES which host (SIP endpoint) to send calls to, based on the dialed number.

Procedure

1. In the left pane of the SIP Server Management Integrated Management console, click **Hosts**.
2. Click **List Hosts**.
   The list of hosts appears.
3. From the **List Hosts**, identify the host to modify.
   The host in this case is the SES server. Click **Map** for the SES server IP address.
4. Click **Add Map In New Group**.
   A new Add Host Address Map page appears.
5. In the **Name** box, type the name of the map entry.
6. In the **Pattern** box, type the pattern regular expression.
7. Uncheck **Replace URI**.
   This replaces the Communication Manager SIP domain with the SES IP address in the outgoing messages to Contact Center.
8. Click **Add**.
9. Click **Continue**.

Adding a contact for the Contact Center Manager Server pattern

Before you begin

- Ensure that there is a Contact Center Manager Server routing entry to the SIP Enablement Services (SES) server; see Adding a routing entry for the Contact Center Manager Server on page 75.

About this task

Add contact details for the Contact Center Manager Server routing entry. This configures the SIP Enablement Services (SES) server to send calls to the Contact Center Manager Server when the calls match the map.

Procedure

1. In the SIP Server Management Integrated Management console, under **Host Lists**, select the Contact Center Manager Server Address Map.
2. Click **Map**.
3. Click **Add Another Contact**.
   The Add Host Contact page appears.
4. In the **Contact** box, type the contact regular expression.
5. Click **Add**.

Procedure job aid

To determine which calls to the Avaya Aura® Unified Communications platform are redirected to the Contact Center Manager Server for processing you must configure a routing entry pattern and contact details for the Contact Center Manager Server in SES.

Routing entry pattern:

A routing entry (or map address) pattern is a string, a Linux regular expression, which is called up any time the SES receives a call that matches the expression. Consider the following example:

```
^sip:800.*
```

SES recognizes this as a matching routing entry pattern any time it receives a call with sip: 800* in it.

Contact:

After the SES identifies a routing entry pattern match, it must then decide the action to take for the call. SES uses routing entry (or map address) contacts to determine where to send the call.

Consider the following example:

```
sip:$(user)@<CCMS_IP_Address>;transport=tcp
```

Where <*CCMS_IP_Address*> is the IP address of the CCMS server. And the transport type is TCP.

When SES receives a call with sip:800* in it, SES sends the SIP call to the Contact Center Manager Server.

When a match for an address map is found, the associated contact can be a fixed destination, or it can be constructed dynamically to include any of the components in the original SIP request URI. The latter is accomplished using the syntax `$(component-name)`.

The syntax of a SIP URI (including the optional components) is as follows:
`protocol:user:password@host:port;uri-parameters?headers`

In the example shown, the proxy host has constructed a Contact by substituting “sip” as the protocol, `$(user)` to represent the user in the original request URI, the IP address of the host (in this case, the Contact Center Manager Server), and the name of the transport.

Verifying the SES to Contact Center Manager Server connection

Before you begin

- Contact Center has at least one route point configured using Contact Center Manager Administration (CCMA).
- The Contact Center—Avaya Media Server is configured and supports ringback.

About this task

Verify that the Communication Manager and SIP Enablement Services (SES) server can route calls to the Contact Center Manager Server, and that the Avaya Media Server gives the call ringback tones.

Procedure

1. Make a phone call from a Communication Manager telephone to the Contact Center route point.
2. Confirm that the call is given ringback.

Procedure job aid

At this stage of the SES configuration, Contact Center can treat telephone calls initiated on the Communication Manager telephone and give the calls ringback tones using the Avaya Media Server. If you do not hear ringback on the test call, you can debug both sides of the SES and Contact Center integration.

Contact Center debugging:

Use the Contact Center Manager Server and Communication Control Toolkit (CCT) trace log files and event logs to debug the Contact Center side of the integration. The default location for the trace log files is:

```
D:\Avaya\Logs\CCMS
```

SIP Enablement Services (SES) server debugging:

Use the traceSES utility to debug the SES side of the integration. Start the traceSES utility and then make a call to the Contact Center route point. Use the SES trace log output to debug the integration.

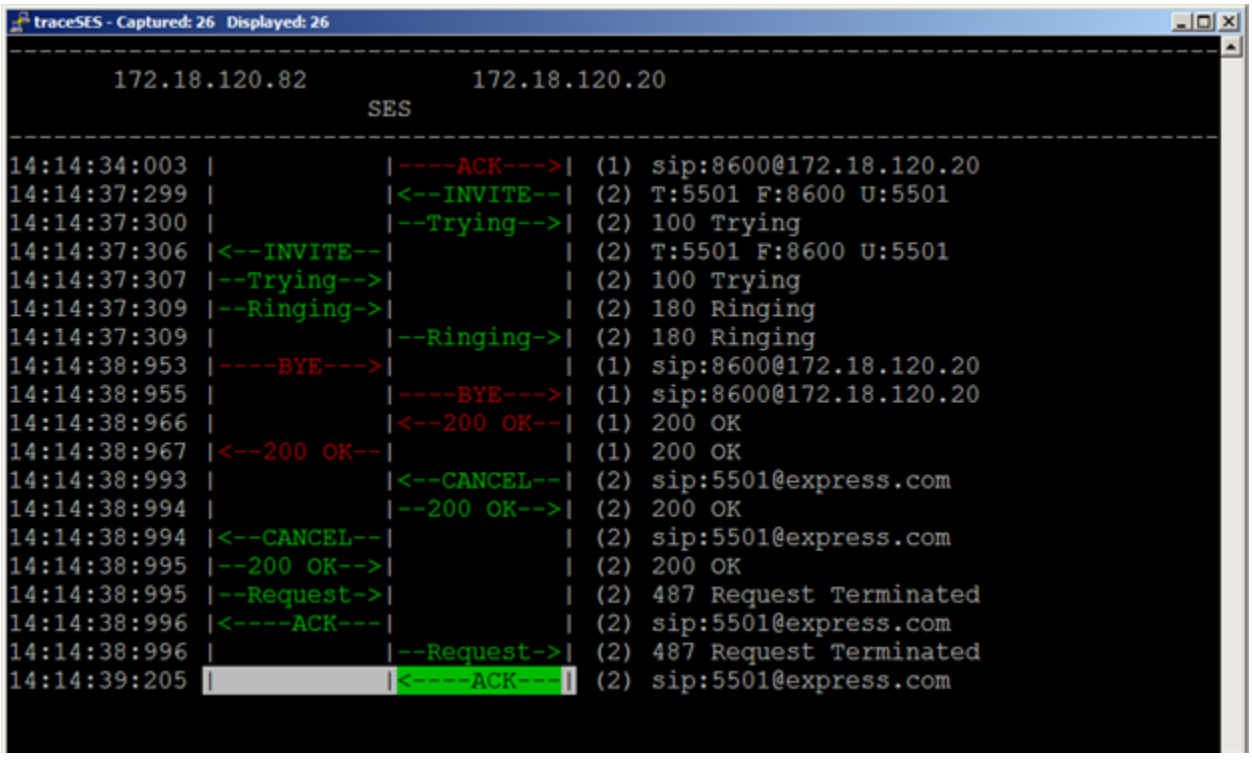


Figure 12: Example of traceSES utility debugging a SIP phone call

Chapter 7: 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.

Navigation

- Logging on to the System Manager Web interface on page 80

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 Session 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.

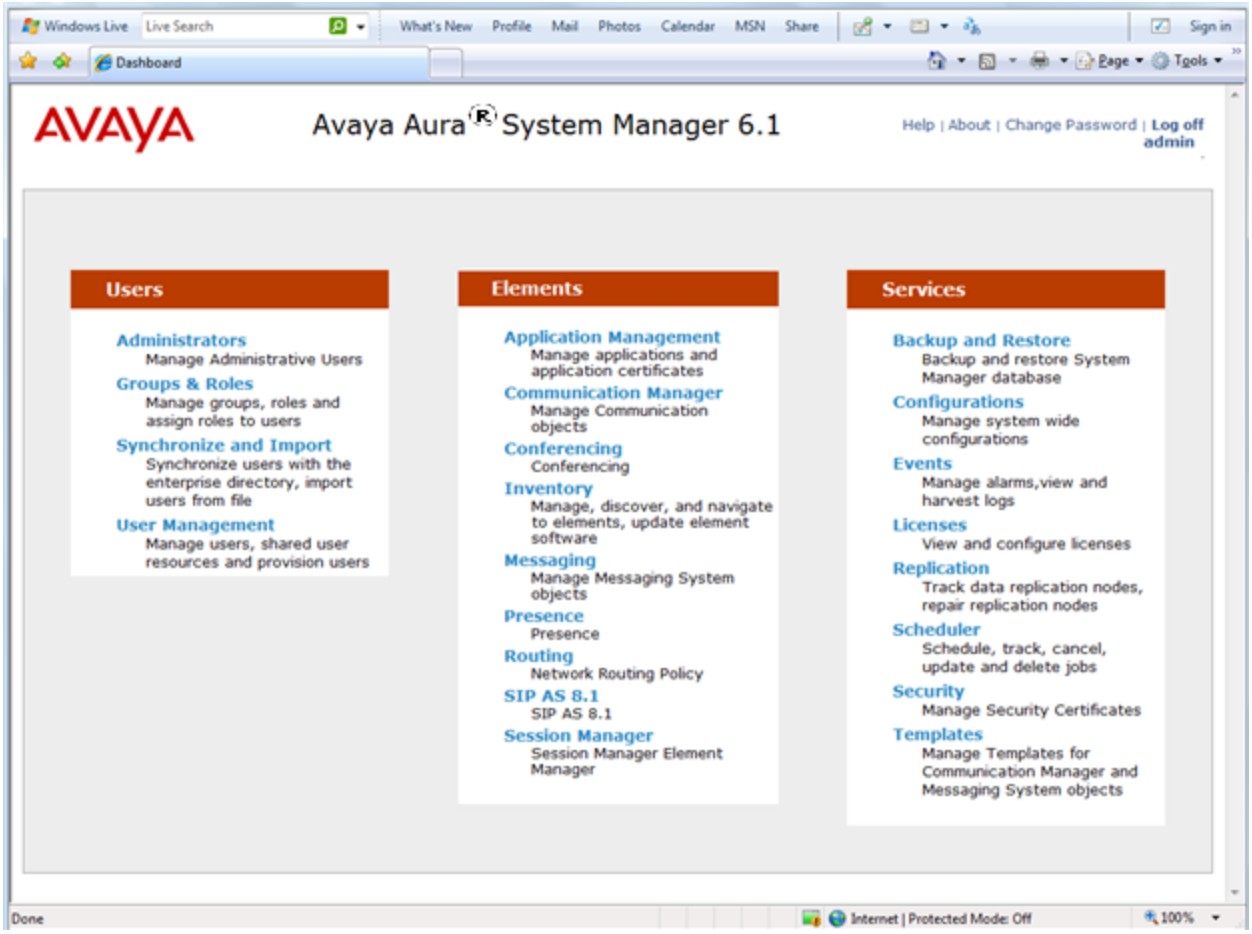


Figure 13: Example of the System Manager Web page

Chapter 8: Session Manager configuration

This section describes how to configure Avaya Aura® Session Manager Release 6.1 and Release 6.2 for use with Avaya Aura® Contact Center Release 6.3.

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.

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.

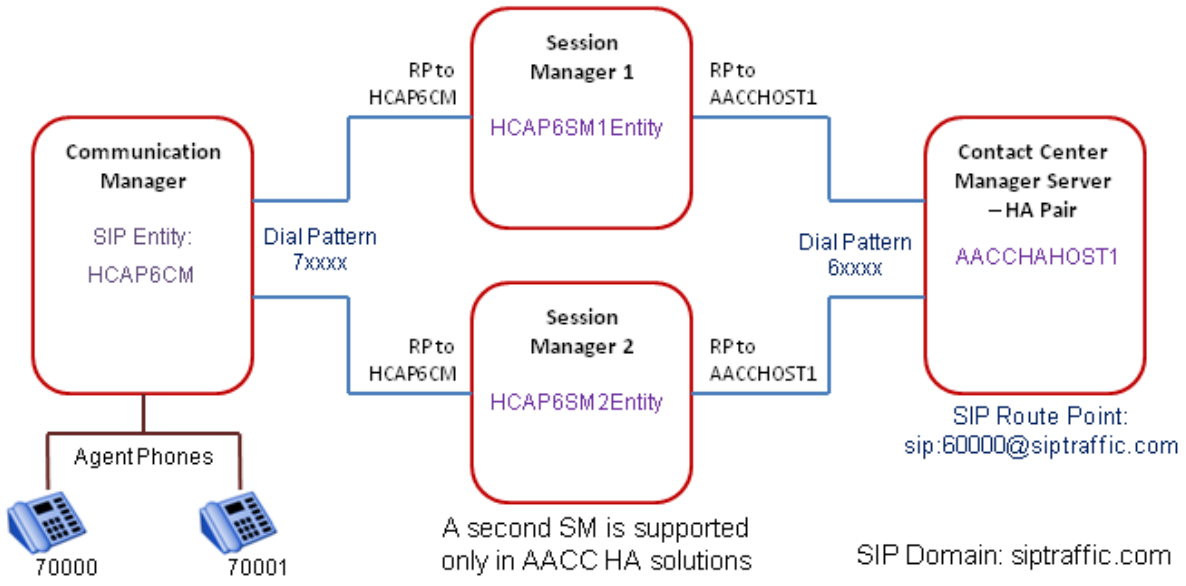


Figure 14: Example of a typical Session Manager routing solution

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 80.

Session Manager configuration procedures

About this task

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

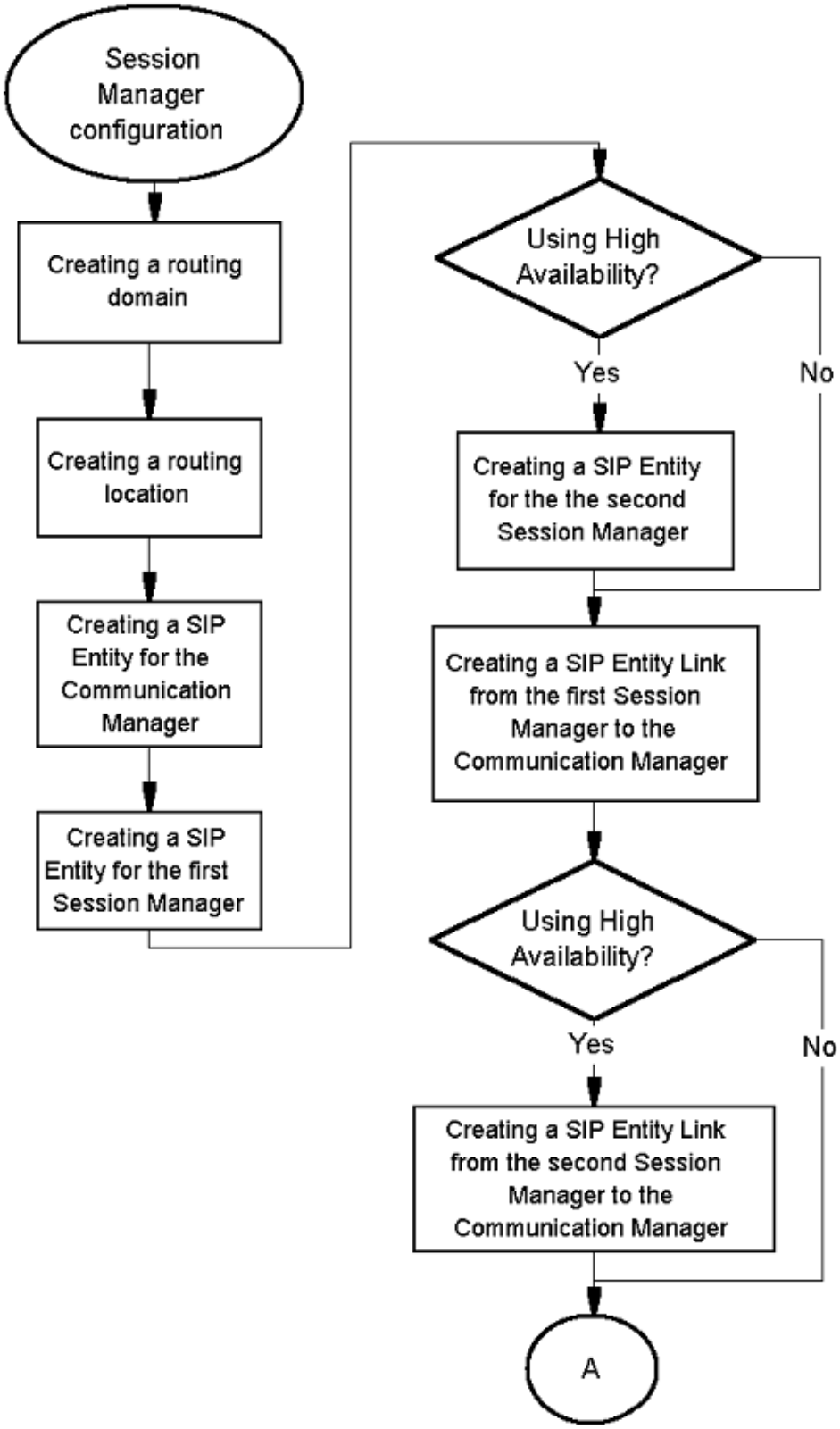


Figure 15: Session Manager configuration procedures

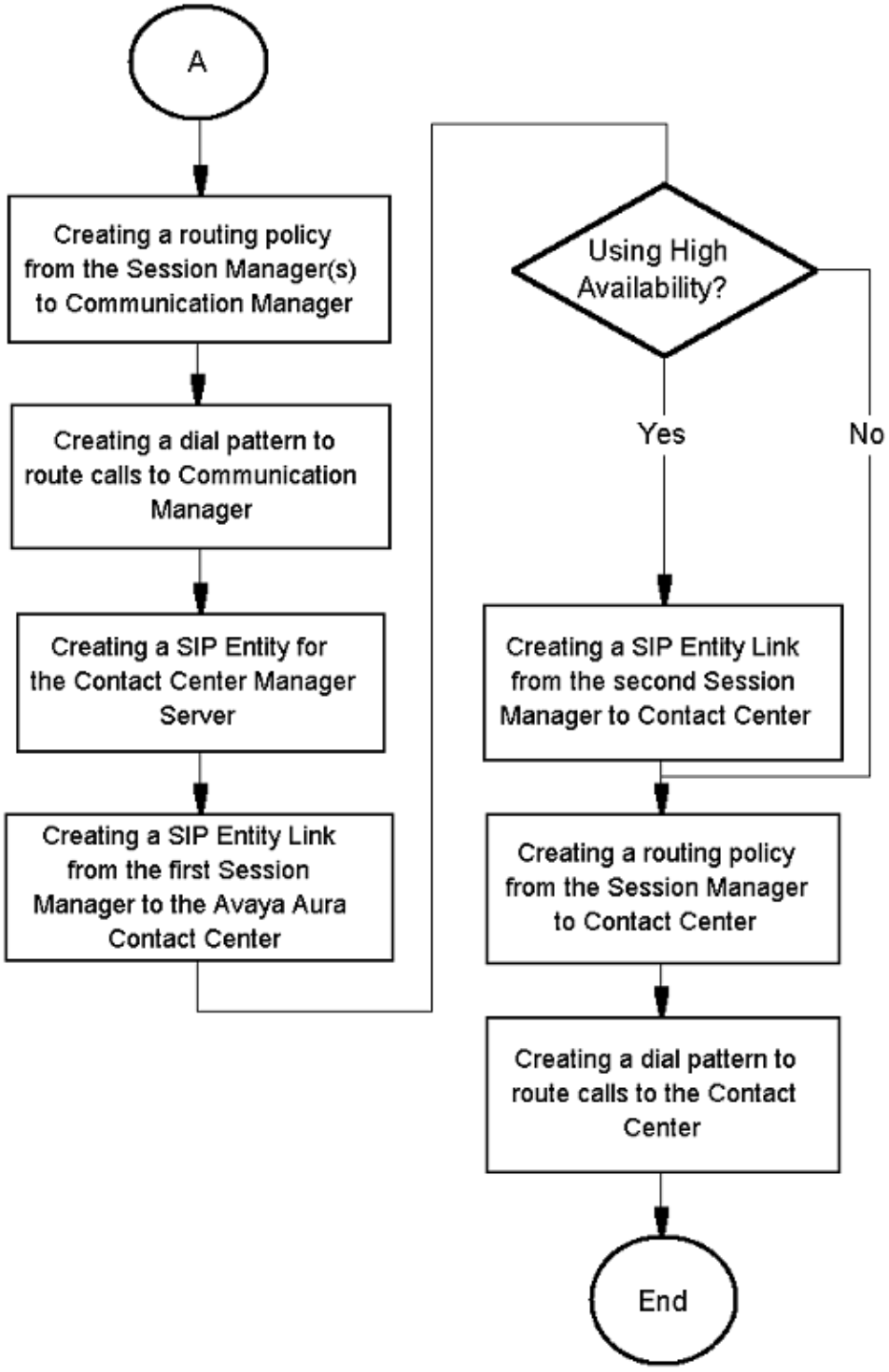


Figure 16: Session Manager configuration procedures continued

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.

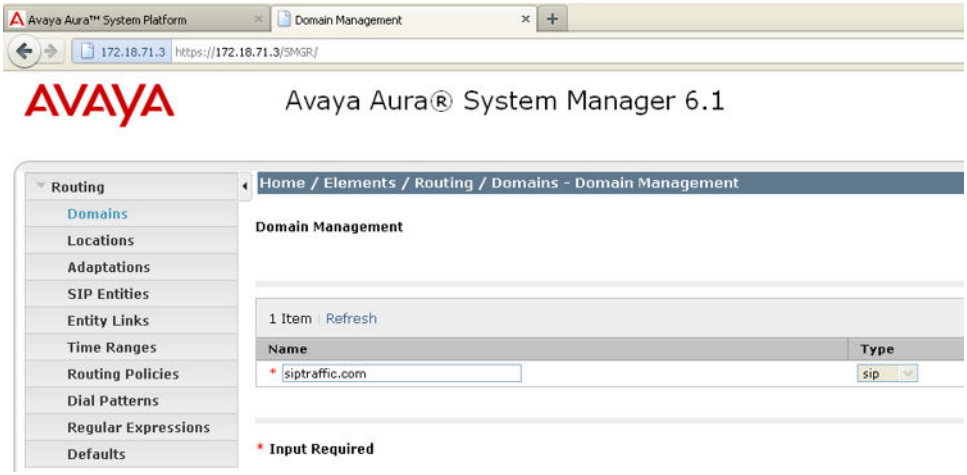
Procedure

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.

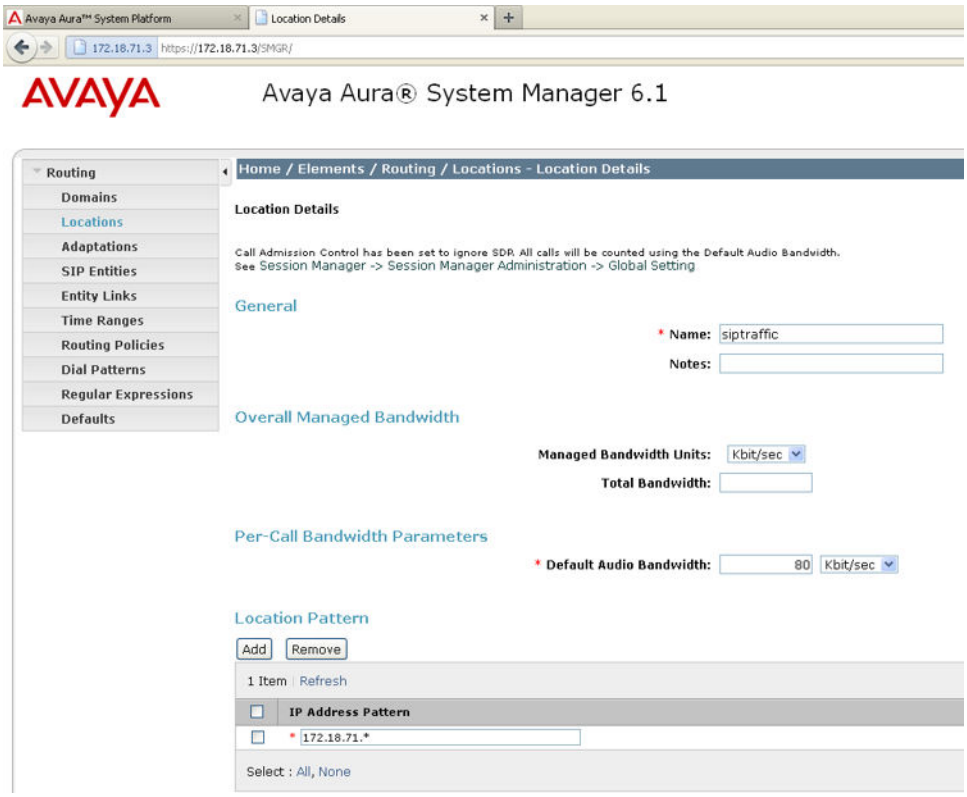
Procedure

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 172.18.71.15 and if your Session Manager has an IP address of 172.18.71.18, then

your IP Address Patterns may be 172.18.71.*. This pattern must cover the addresses that you deem part of this routing location.



Creating a SIP Entity for the Communication Manager

About this task

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

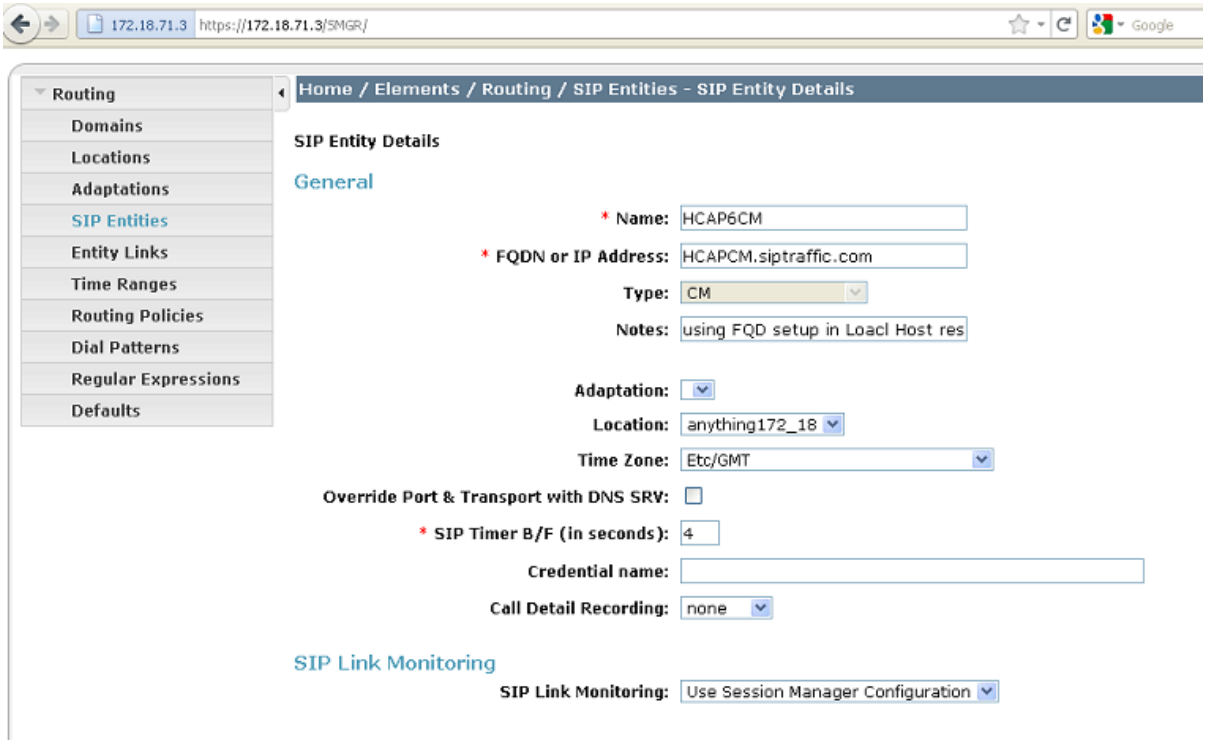
6. If you need to specify an Adaptation Module for the Communication Manager SIP entity, from the **Adaptation** list, select an adaptation value.
7. In the **Location** box, select the location for this Communication Manager.
8. In the **Credential name** box, enter a regular expression string.

   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.
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,

Variable	Value
	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 via 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.

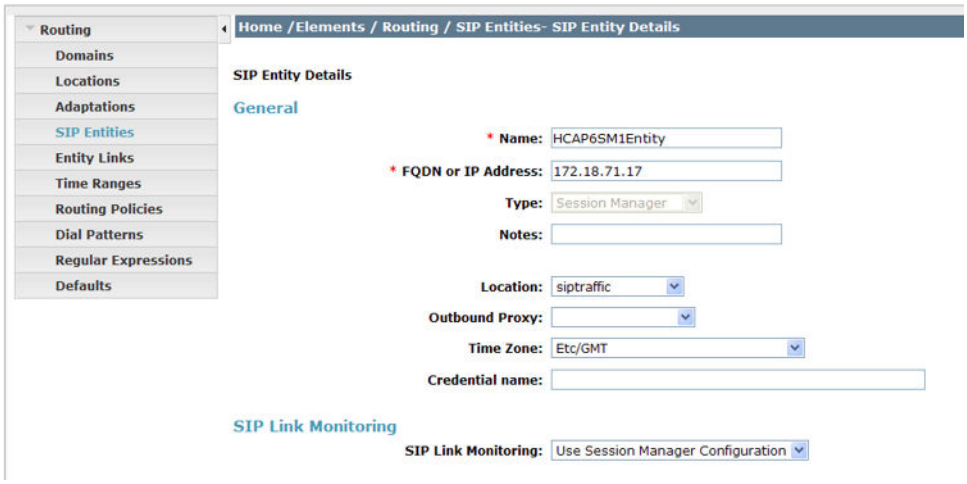
   Avaya recommends that you type a descriptive name for your Session Manager SIP entity.
4. In the **FQDN or IP address** box, type the IP address of the Session Manager.
5. From the **Type** list, select **Session Manager**.
6. If you need to specify an Adaptation Module for the Session Manager SIP entity,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

Variable	Value
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 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.

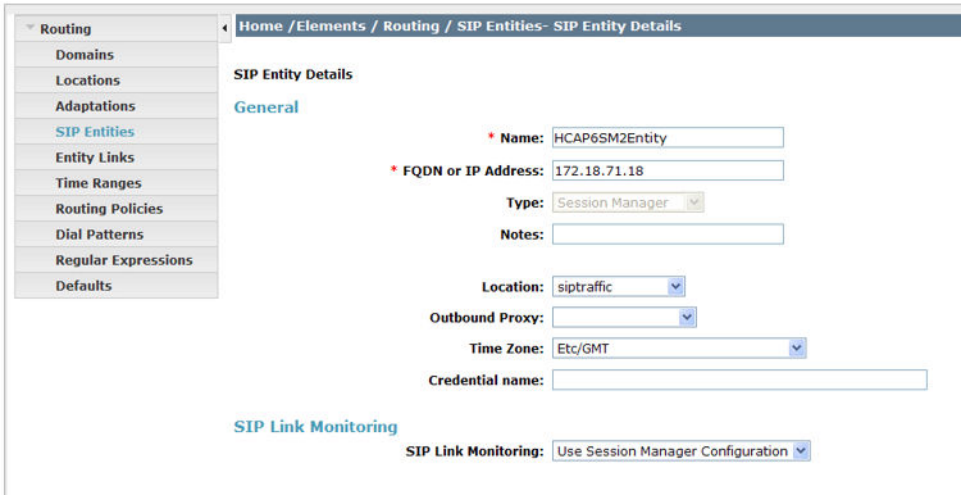
11. If you need to specify the port parameters, under **Port**, click **Add**.

    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, 172.18.71.18.



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.

Variable	Value
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 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.

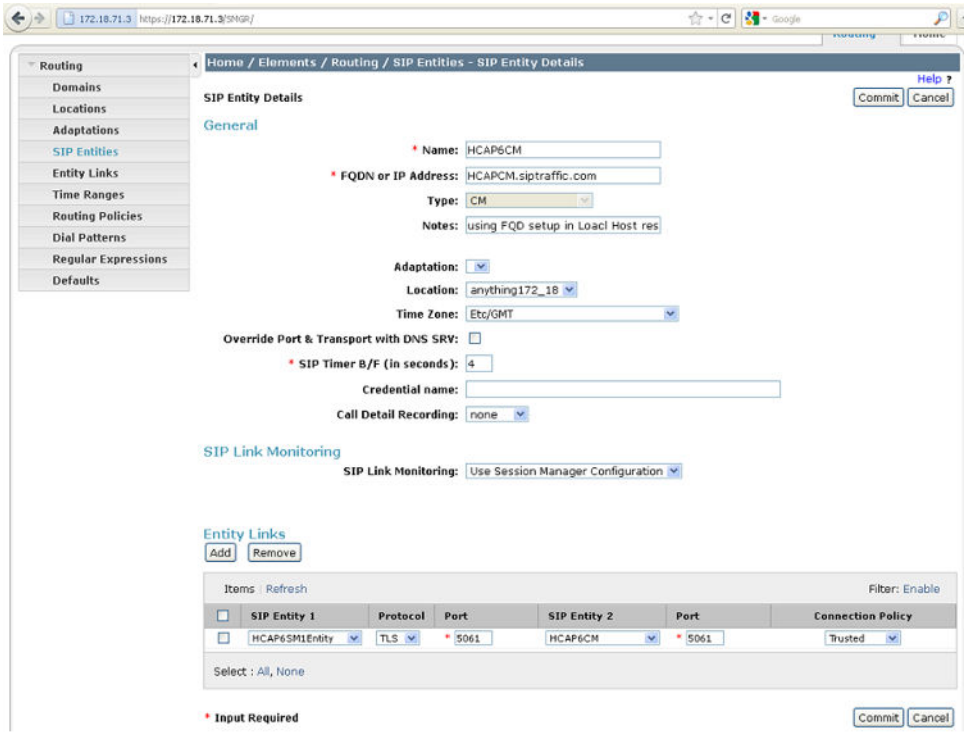
   The default port for TCP and UDP is 5060. The default port for TLS is 5061.
5. Under **SIP Entity 2**, select the required Communication Manager SIP entity from the drop-down list and provide the required port number.

   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 (HCAP6SM1Entity).



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.

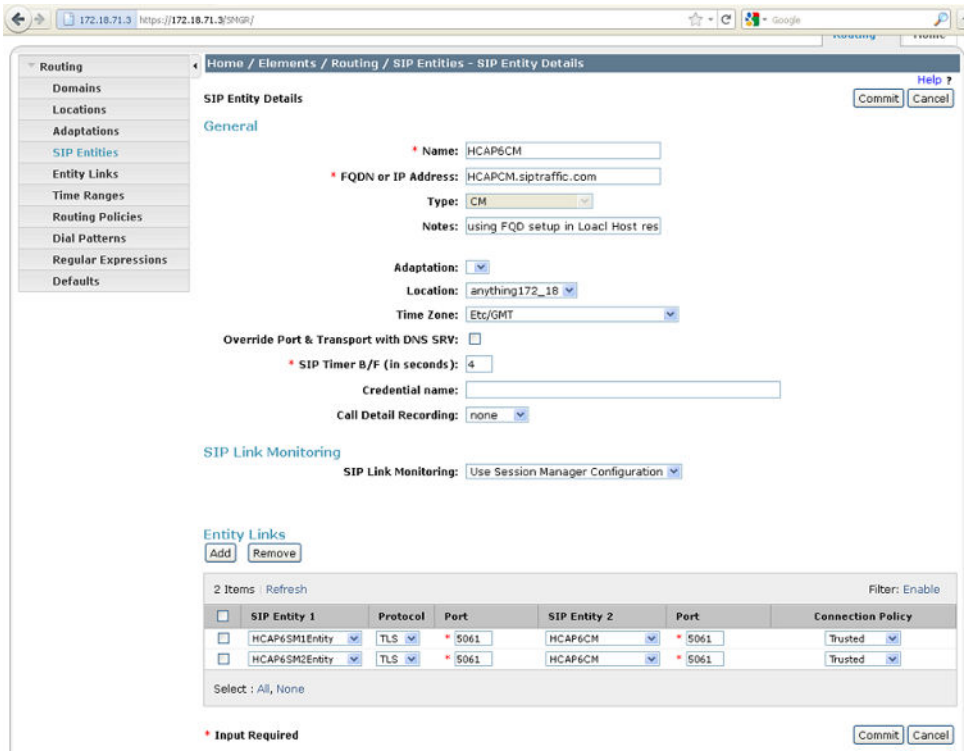
   The default port for TCP and UDP is 5060. The default port for TLS is 5061.

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. One link to the first Session Manager SIP Entity (HCAP6SM1Entity) and one link to the second Session Manager SIP Entity (HCAP6SM2Entity).



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.

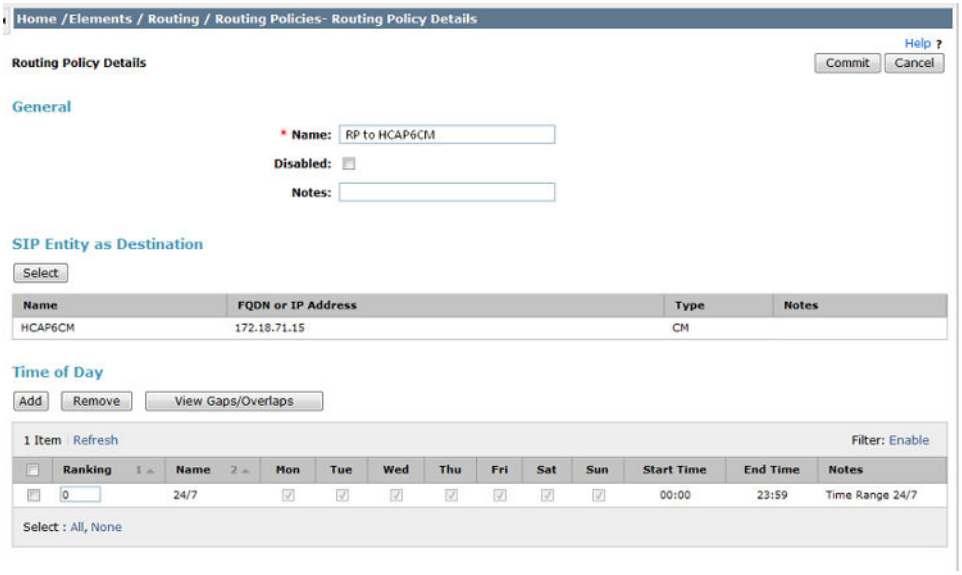
Session Manager uses the data configured in the Routing Policy to find the best match against the number (or address) of the called party.

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.

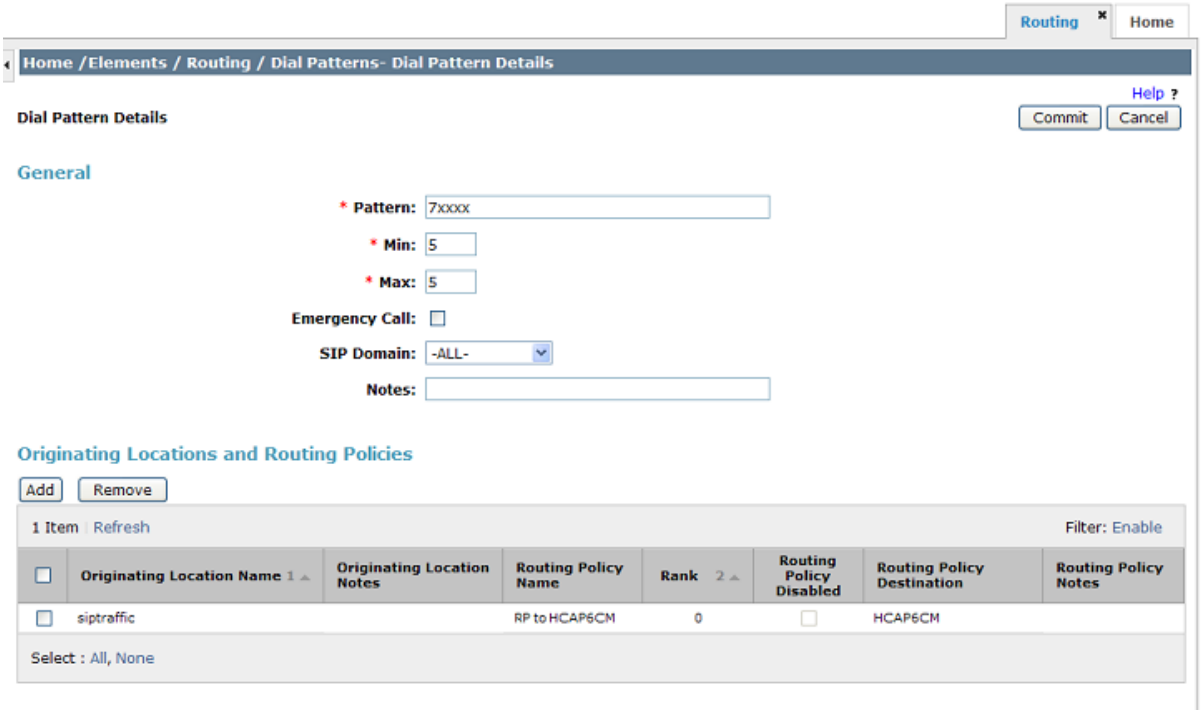
Procedure

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:

Variable	Value
	— 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.

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.

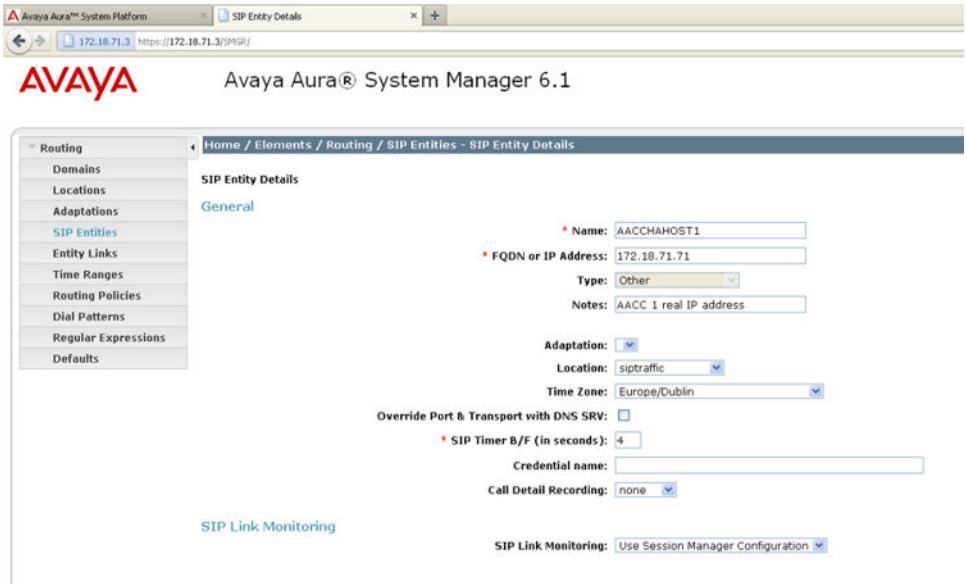
4. In the **FQDN or IP address** box, type the IP address of the Contact Center Manager Server.
5. From the **Type** list, select **Other**.
6. If you need to specify an Adaptation Module for the Contact Center Manager Server SIP entity, from the **Adaptation** list, select an adaptation value.
7. In 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

Variable	Value
	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 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.

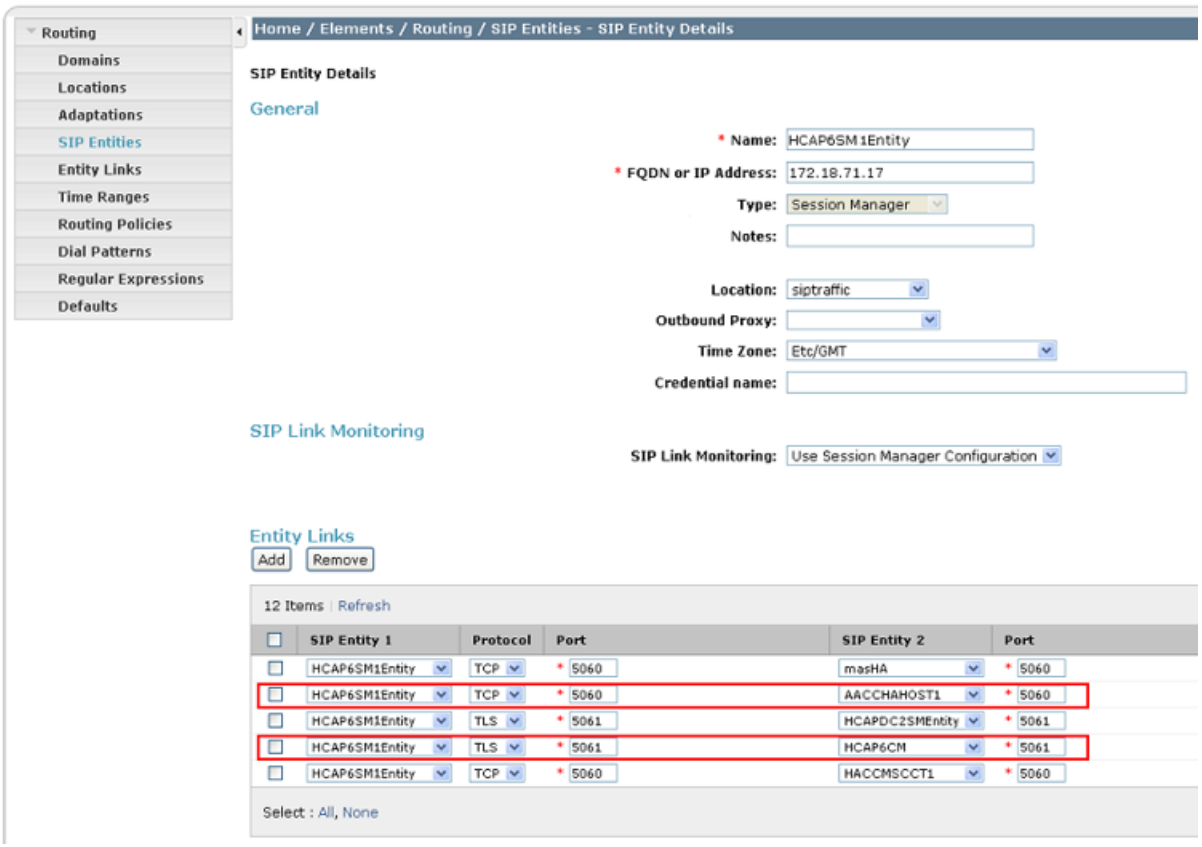
   The default port for TCP is 5060.
5. Under **SIP Entity 2**, select the required Contact Center Manager Server SIP entity from the drop-down list and provide the required port number.

   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 (AACCHAHOST1) and Avaya Aura® Communication Manager (HCAP6CM).



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.

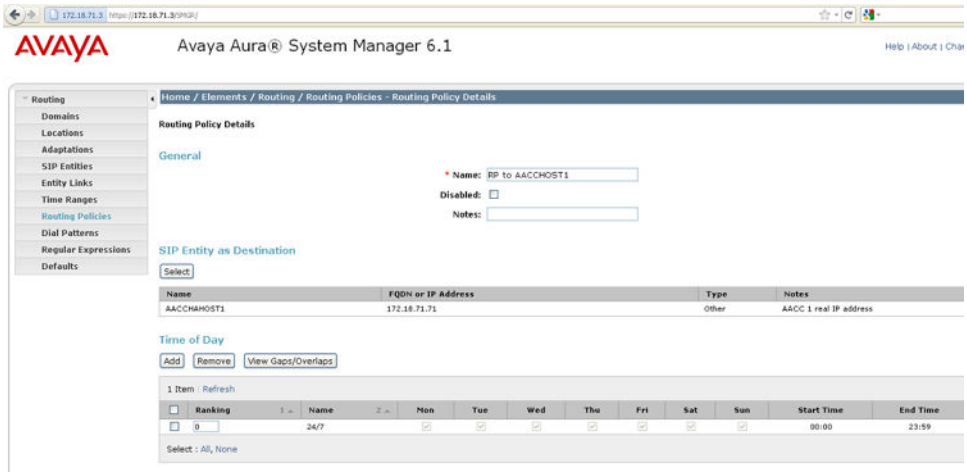
   Avaya recommends that you type a descriptive name for your Routing Policy.

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.

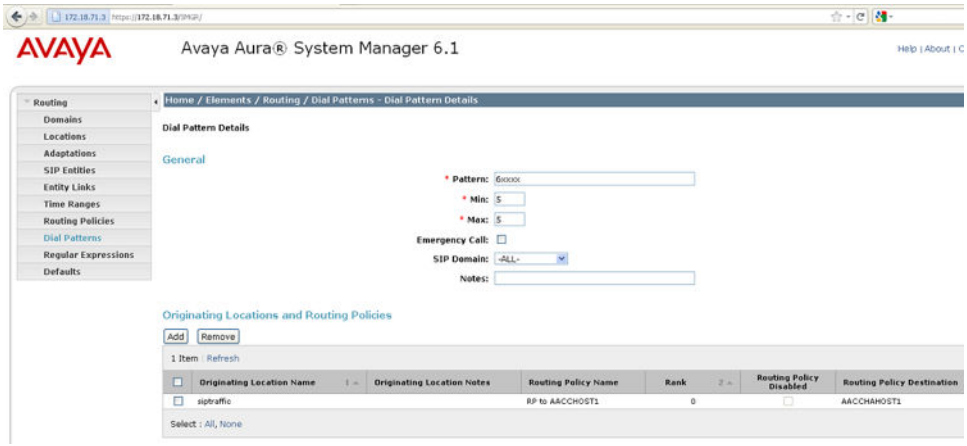
Procedure

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.

Variable	Value
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.
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 9: Application Enablement Services configuration

Avaya Aura® Application Enablement Services (AES) are 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 Avaya Aura® 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. With public key cryptography, two keys are created, one public and one private. Anything encrypted with either key can be decrypted only with the corresponding key. Thus if a message is encrypted with the server's private key, it can be decrypted only using its corresponding public key, ensuring that the data can only have come from the server. TLS uses certificates to manage the public and private keys.

Use certificates to secure the TLS link between Avaya Aura® Contact Center and the Application Enablement Services server.

Avaya Aura® Contact Center Release 6.3 supplies a set of default certificates for use with Application Enablement Services. If you do not have access to or require a third-party Certificate Authority, you can install these Contact Center default certificates on your Application Enablement Services server to quickly establish a link between the two systems.

Important:

AES 6.2 and later includes the default trust certificates. Using the default certificates Avaya Aura® Contact Center automatically communicates with AES.

Note:

The Contact Center default certificates for AES may not meet your organization's security requirements. Avaya recommends the you use a third-party Certificate Authority or follow your organization's security policies and procedures to better secure the TLS link between Avaya Aura® Contact Center and the Avaya Aura® Application Enablement Services server.

For improved security, Avaya recommends that you obtain a root certificate from your Certificate Authority. A root certificate is an unsigned public key that identifies the root Certificate Authority (CA). Add the CA root certificate to the AES server and then use it to generate a Certificate Signing Request (CSR). Send

the CSR and the Common Name (CN) of the AES server to your Certificate Authority. The CA verifies the identity of the request and issues a signed certificate (a private key) for use by the AES server. You must apply the CA root certificate and the signed certificate from your Certificate Authority to the AES server.

The Contact Center must also generate a Certificate Signing Request (CSR) and get it signed by the Certificate Authority before it can establish a secure TLS SIP link. The AES and Contact Center can then communicate securely using a TLS SIP connection.

Important:

Avaya Aura® Contact Center must use the same Certificate Authority and the same CA root certificate as the AES server.

This section describes how to configure the 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.
- If you are not using the default certificates, you must have access to a Certificate Authority and the ability to generate a root certificate and signed client certificates. For more information about installing a standalone Certificate Authority, see Installing a standalone Certificate Authority on page 152.
- Complete the *Avaya Aura® Contact Center Installation Checklist* (NN44400-310).

Application Enablement Services configuration procedures

About this task

This task flow shows you the sequence of procedures you perform to configure Application Enablement Services 6.2 and later.

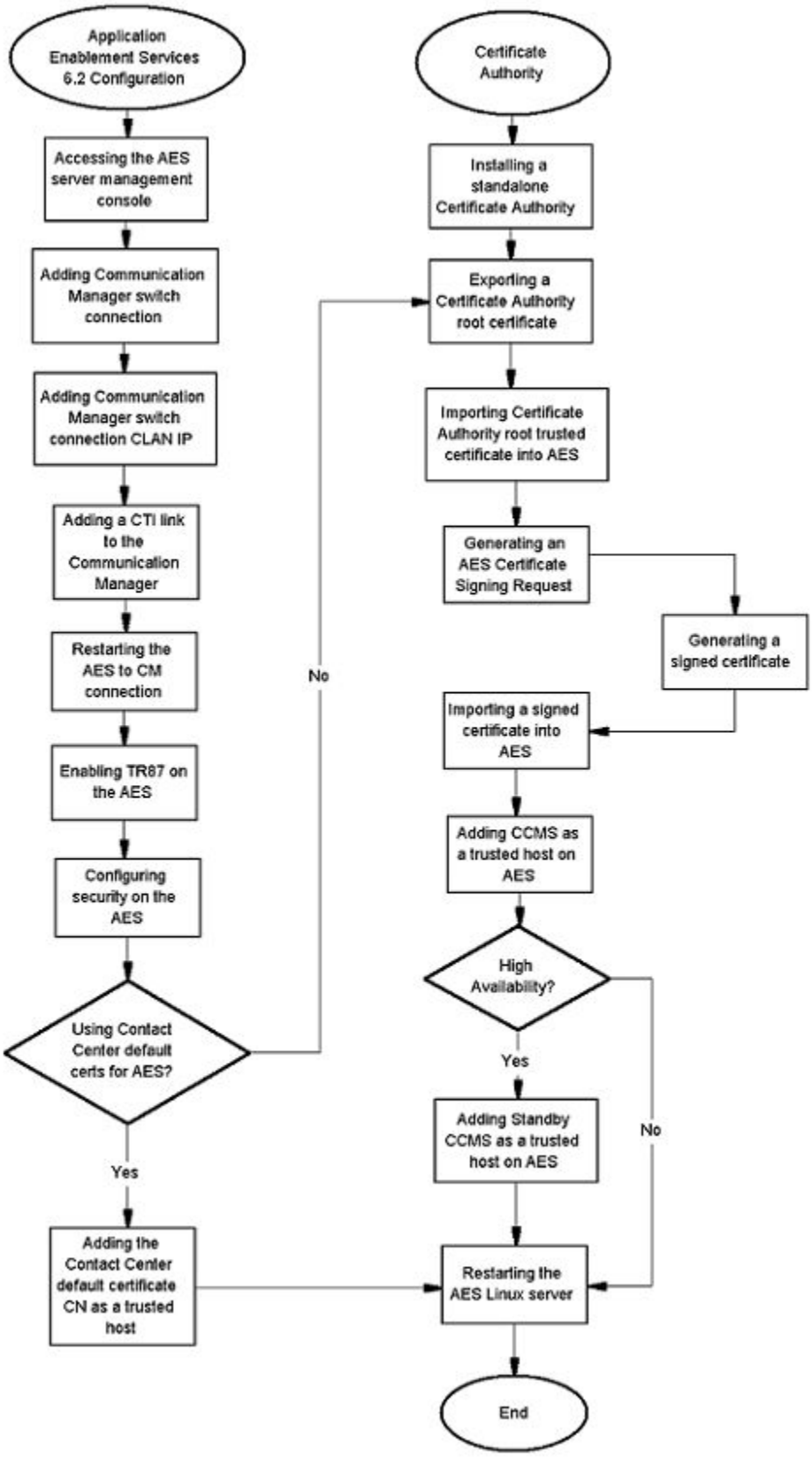


Figure 17: Application Enablement Services configuration procedures using AES 6.2 and later

This task flow shows you the sequence of procedures you perform to configure Application Enablement Services 5.2.1, 5.2.2, or 6.1.

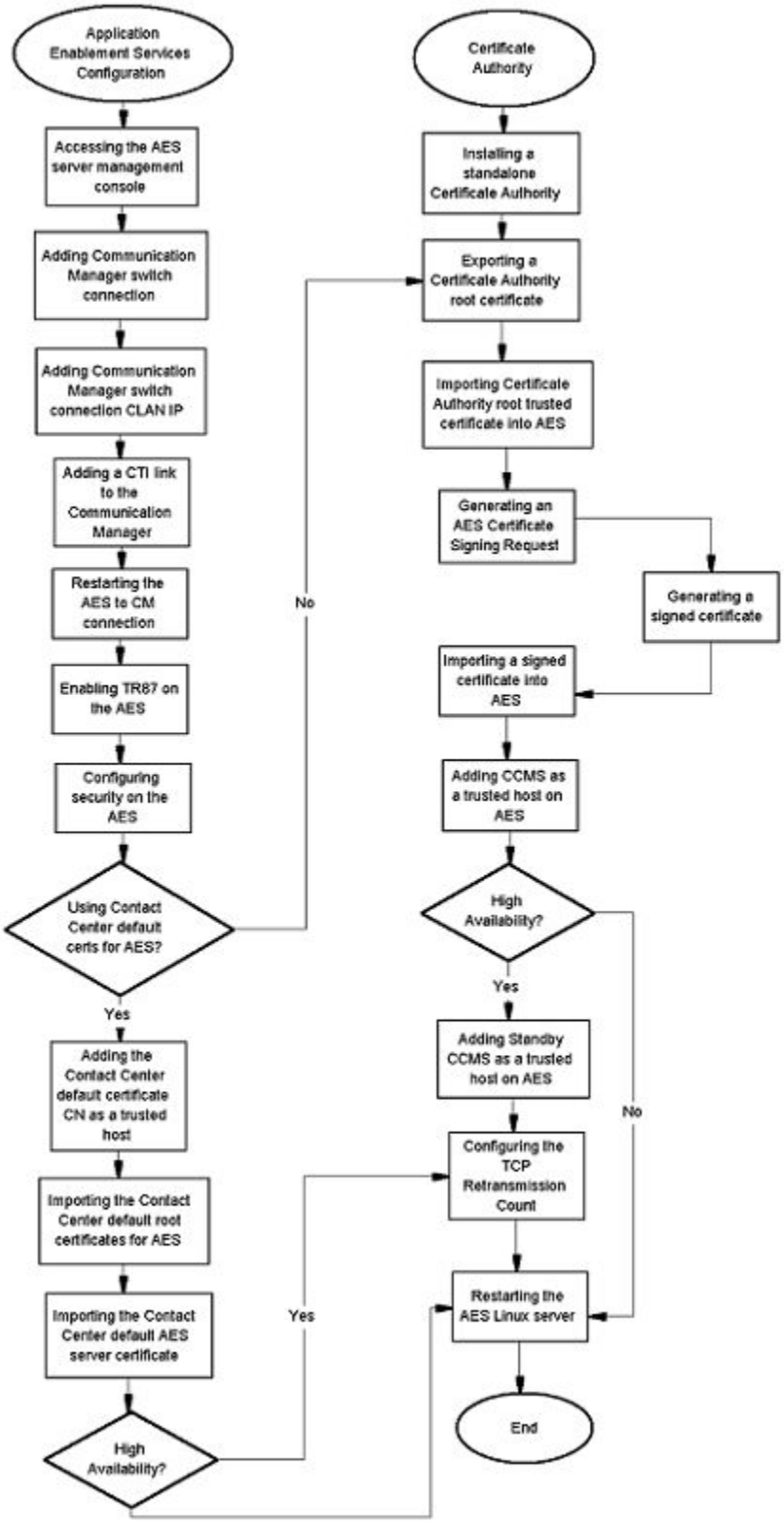


Figure 18: Application Enablement Services configuration procedures using AES 5.2.1, 5.2.2, or 6.1

Navigation

Accessing the AES server management console

Before you begin

- Log on to the System Platform Web Console; see Accessing the System Platform Web console on page 28.

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.

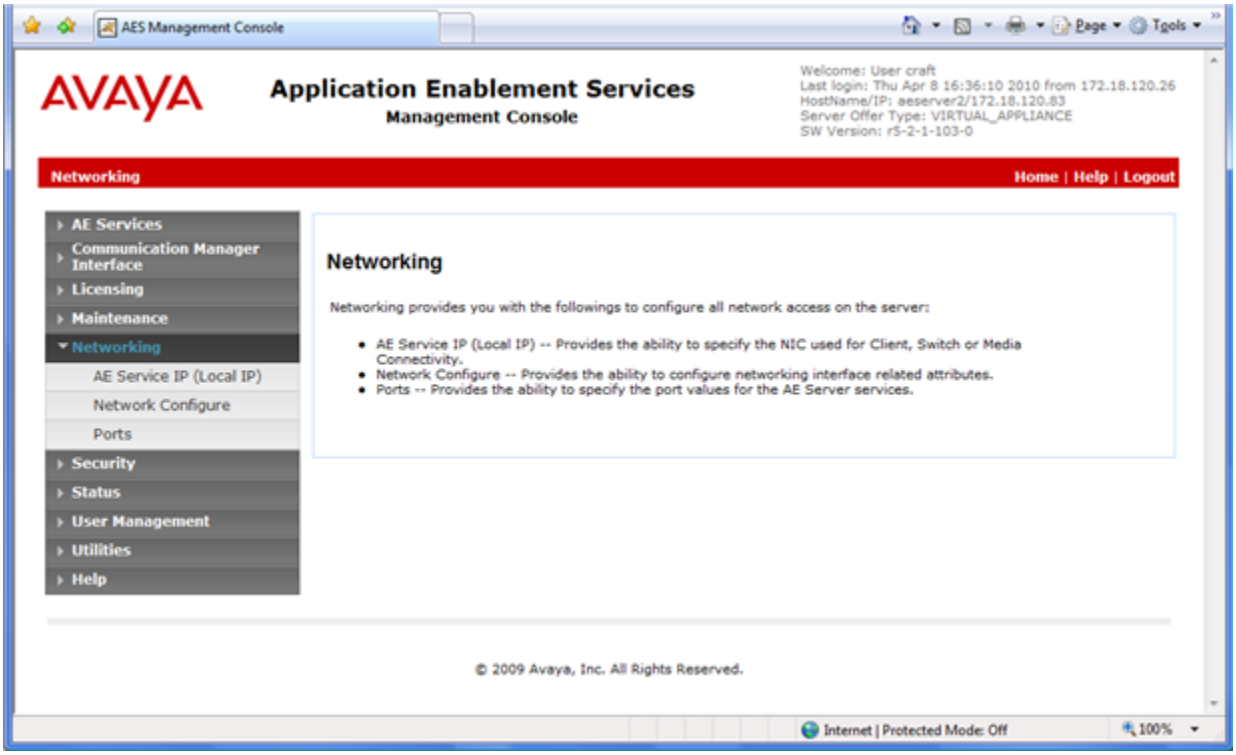


Figure 19: Example of the Application Enablement Services Management console

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.

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 the **SSL** check box.
9. Clear **Processor Ethernet**.

   By default this check box is not selected. Accept the default setting if you are administering a connection to a Communication Manager media server that uses a CLAN connection to AE Services.
10. 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 122.

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 122.
- Associate the Communication Manager switch connection with a host IP address, see Adding Communication Manager switch connection CLAN IP on page 123.

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**.
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 122.
- Associate the Communication Manager switch connection with a host IP address, see Adding Communication Manager switch connection CLAN IP on page 123.

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.

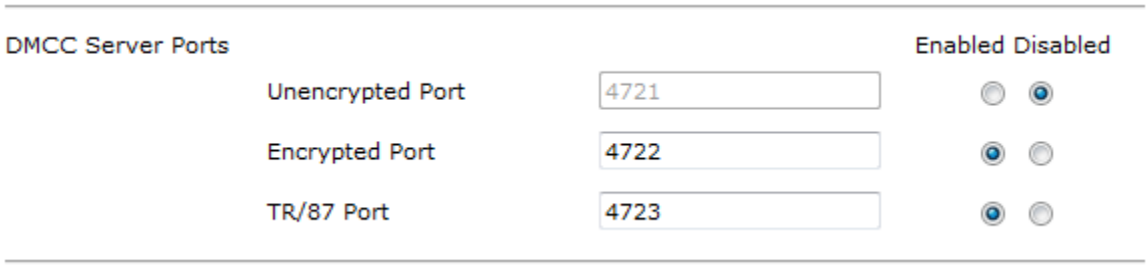


Figure 20: Example of AES TR/87 configuration

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 **Host AA**.
   The Host Authentication and Authorization page appears.
3. Click **Service Settings**.

4. Select the **TR/87** > **Require Trusted Host Entry** check box.
   When you select this setting, the DMCC service verifies the Common Name (CN) in the client certificate and verifies that it matches one of the administered authorized hosts.
5. Click **Apply Changes**.
6. On the Apply Changes to Host AA service page, click **Apply** again.

Adding the Contact Center default certificate CN as a trusted host

About this task

Add the Avaya Aura® Contact Center default certificate Common Name (Certificate CN) as a trusted host on the Application Enablement Services server. The Avaya Aura® Contact Center default certificate Common Name (Certificate CN) is AACCSGM60.

Perform this procedure when using the Avaya Aura® Contact Center default certificates for Application Enablement Services to quickly setup a link between the two systems. Avaya Aura® Contact Center uses this link with the Application Enablement Services server to control and monitor Agent desk phones and telephony devices.

Important:

The Contact Center default certificates may not meet your organization's security requirements. Avaya recommends the you use a third-party Certificate Authority or follow your organization's security policies and procedures to better secure this link. For more information about securing the link between Contact Center and the Application Enablement Services server, see Importing a Certificate Authority root trusted certificate into AES on page 133 and Certificate Authority configuration on page 151.

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 `AACCSGM60`.
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**.

Procedure job aid

Example of adding the Avaya Aura® Contact Center default certificate Common Name (Certificate CN) as a trusted host on the Application Enablement Services server.

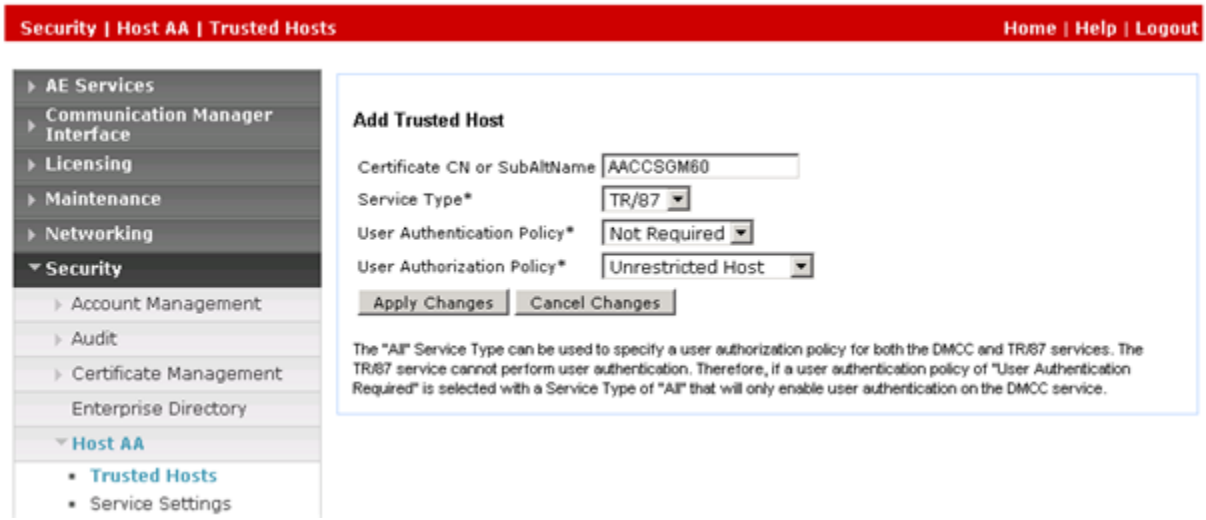


Figure 21: Example of adding AACC default Certificate Common Name as a trusted host in AES

Importing the Contact Center default root certificates for AES

Before you begin

- The default certificates are stored on the Contact Center Manager Server, at the following default location: `D:\Avaya\Contact Center\Manager Server\iccm\sgm\TLSCertificates\AESCerts\CA`.

About this task

Important:

This procedure is applicable only for configuring Application Enablement Services 5.2.1, 5.2.2, or 6.1.

Avaya Aura® Contact Center supplies two default root CA certificates. Import these two default root certificates into the Application Enablement Services (AES) server so that Avaya Aura® Contact Center and AES can communicate.

Perform this procedure when using the Avaya Aura® Contact Center default certificates for Application Enablement Services to quickly setup a link between the two systems. Avaya Aura® Contact Center uses this link with the Application Enablement Services server to control and monitor Agent desk phones and telephony devices.

Important:

The Contact Center default certificates may not meet your organization's security requirements. Avaya recommends the you use a third-party Certificate Authority or follow your organization's security policies and procedures to better secure this link. For more information about securing the link between Contact Center and the Application Enablement Services server, see Importing a Certificate Authority root trusted certificate into AES on page 133 and Certificate Authority configuration on page 151.

Procedure

1. Copy the Contact Center default certificates to a location that AES can access.
2. In the left pane of the AES management console, click **Security**.
3. Click **Certificate Management** > **CA Trusted Certificates**.
4. Click **Import**.
   A Trusted Certificate Import page appears.
5. In the **Certificate Alias** box, type the AES root certificate alias, for example `AEServicesRoot`.
6. Click **Browse**.

7. Using the File Upload dialog, navigate to the folder containing the Contact Center default certificates for AES.

   Navigate to the `AESCerts\CA` folder and select **AEServiceRoot.cer**.

8. Click **Open**.
9. Click **Apply**.
   A Certificate imported successfully message appears.
10. In the **Certificate Alias** box, type the AACC root certificate alias, for example `AACCSGM60Root`.
11. Click **Browse**.
12. Using the **File Upload** dialog, navigate to the folder containing the Contact Center default certificates for CCMS.

    Navigate to the `AESCerts\CA` folder and select **AACCSGMRoot.pem**.

13. Click **Open**.
14. Click **Apply**.
    A Certificate imported successfully message appears.
15. On the CA Trusted Certificates page, confirm that both certificates imported successfully and have a **Status** value of **valid**.

Procedure job aid

Important:

You have to import the Contact Center default root certificates for AES when you are configuring AES 5.2.1, 5.2.2, or 6.1 only.

Import the two Avaya Aura® Contact Center default root certificates into the Application Enablement Services (AES) server so Avaya Aura® Contact Center and AES can communicate.

The following example shows both root certificates imported. The default certificates are the first two on the list and both have a “valid” status.

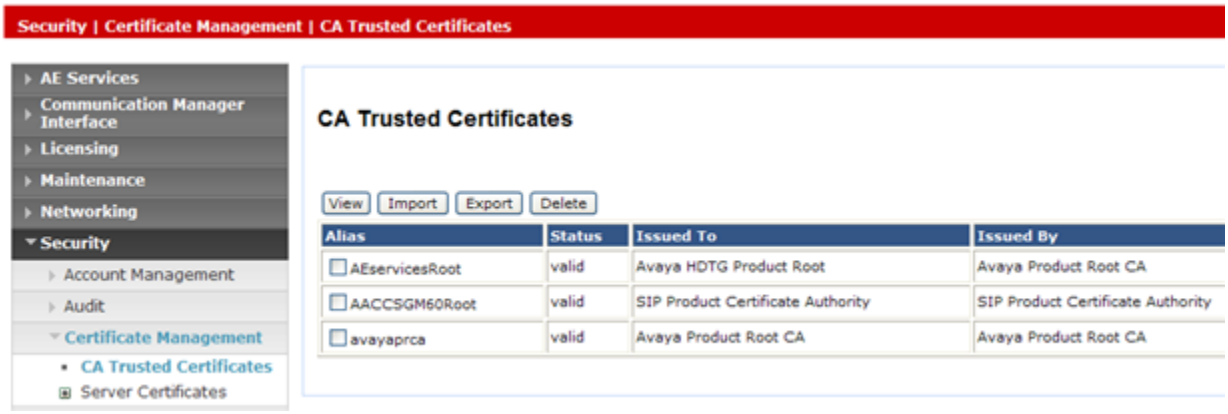


Figure 22: Example of importing default AACC certificate for AES

Importing the Contact Center default AES server certificate

Before you begin

- The default certificates are stored on the Contact Center Manager Server, at the following default location: `D:\Avaya\Contact Center\Manager Server\iccm\sgm \TLSCertificates\AESCerts\ServerCert`.

About this task

Important:

This procedure is applicable only for configuring Application Enablement Services 5.2.1, 5.2.2, or 6.1.

Avaya Aura® Contact Center supplies a default Application Enablement Services server certificate. Import this server certificate into the Application Enablement Services (AES) server so that Avaya Aura® Contact Center and AES can communicate.

Perform this procedure when using the Avaya Aura® Contact Center default certificates for Application Enablement Services to quickly setup a link between the two systems. Avaya Aura® Contact Center uses this link with the Application Enablement Services server to control and monitor Agent desk phones and telephony devices.

Important:

The Contact Center default certificates may not meet your organization's security requirements. Avaya recommends the you use a third-party Certificate Authority or follow your organization's security policies and procedures to better secure this link. For more information about securing the link between Contact Center and the Application Enablement

Services server, see Importing a Certificate Authority root trusted certificate into AES on page 133 and Certificate Authority configuration on page 151.

Procedure

1. Copy the Contact Center default certificates to a location that AES can access.
2. In the left pane of the AES management console, click **Security**.
3. Click **Certificate Management** > **Server Certificates**.
4. On the Server Certificate Import page, click **Import**.
5. From the **Certificate Alias** list, select **aesservices**.
6. Select **Establish Chain of Trust**.
7. Click **Browse**.
8. Navigate to the folder containing the default AACC certificates for AES.
   Navigate to the `AESCerts\ServerCert` folder and select **AEServices.pfx**.
9. Click **Open**.
10. Click **Apply**.
    A Server Certificate Import Continue page appears.
11. In the **PKCS12 Private Password** box, type the password.
    The default password is password.
12. Click **Apply**.

Procedure job aid

Important:

You need to import the Contact Center default AES server certificate when you are configuring AES 5.2.1, 5.2.2, or 6.1 only.

Import the Avaya Aura® Contact Center default Application Enablement Services server certificate into the AES server so that Avaya Aura® Contact Center and AES can communicate.

Figure 23: Example of importing the default server certificate

Importing a Certificate Authority root trusted certificate into AES

Before you begin

- Ensure the Certificate Authority, Application Enablement Services (AES) server, and the Contact Center servers can all ping each other using a fully qualified domain name (FQDN).

About this task

Endpoints that need to communicate securely use a trusted third-party, such as a Certificate Authority. The Certificate Authority (CA) issues digital certificates to both endpoints so they can communicate securely. For the Application Enablement Services server to communicate securely with the Contact Center a common CA root certificate must be installed on both systems. A root certificate is a self-signed certificate that identifies the root certificate Authority. It contains the CA public key. The CA holds onto the private key. The root certificate is installed on the AES as a CA trusted certificate.

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 your root certificate.

6. Click **Apply**.
   A Certificate imported successfully message appears 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.

The same CA root certificate must be applied to Contact Center so that AES can communicate securely with it using TLS. For more information about configuring Contact Center certificates, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

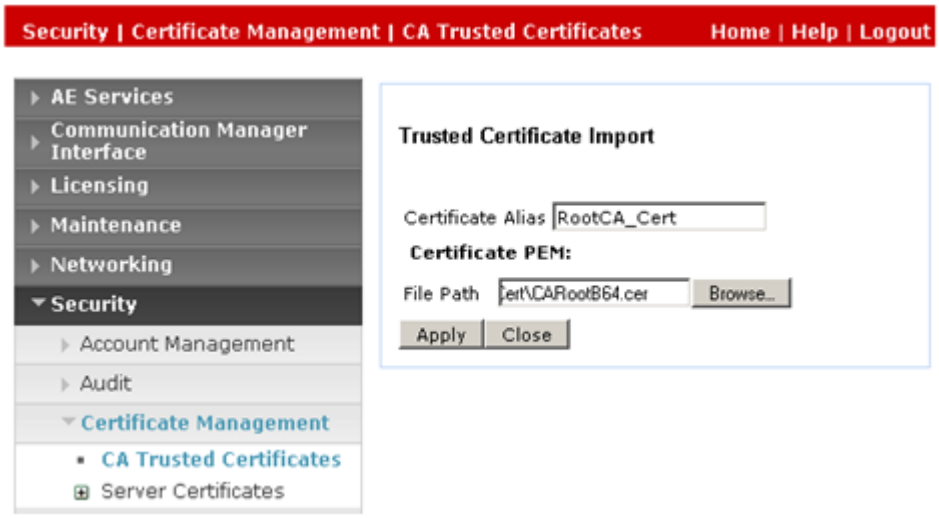


Figure 24: Example of importing a CA Trusted Certificate into AES

Generating an AES Certificate Signing Request

Before you begin

- Ensure the Certificate Authority, Application Enablement Services (AES) server, and the Contact Center servers can all ping each other using a fully qualified domain name (FQDN).
- Obtain a Certificate Authority root certificate from your Certificate Authority. For more information about importing CA root certificates, see Exporting a Certificate Authority root certificate on page 154.
- Import the root certificate into AES, see Importing a Certificate Authority root trusted certificate into AES on page 133.

About this task

For the Application Enablement Services server to communicate securely with the Contact Center, a common Certificate Authority root certificate must be installed on both systems. The root certificate is installed on the AES as a Certificate Authority (CA) trusted certificate. The AES server can then request a signed client certificate from the Certificate Authority by creating a Certificate Signing Request (CSR). Use the CSR text to download a signed 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**.
   The Add Server Certificate page appears.
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.

    Note:

    Leave the Server Certificate Manual Enrollment Request page open while you use the Certificate Signing Request (CSR) text to generate a certificate with your Certificate Authority.
13. Use the Certificate Signing Request (CSR) text file to request a certificate from your Certificate Authority.

Procedure job aid

Use the Certificate Signing Request (CSR) text in your clipboard 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 client certificate returned by the CA is only valid on the AES server.

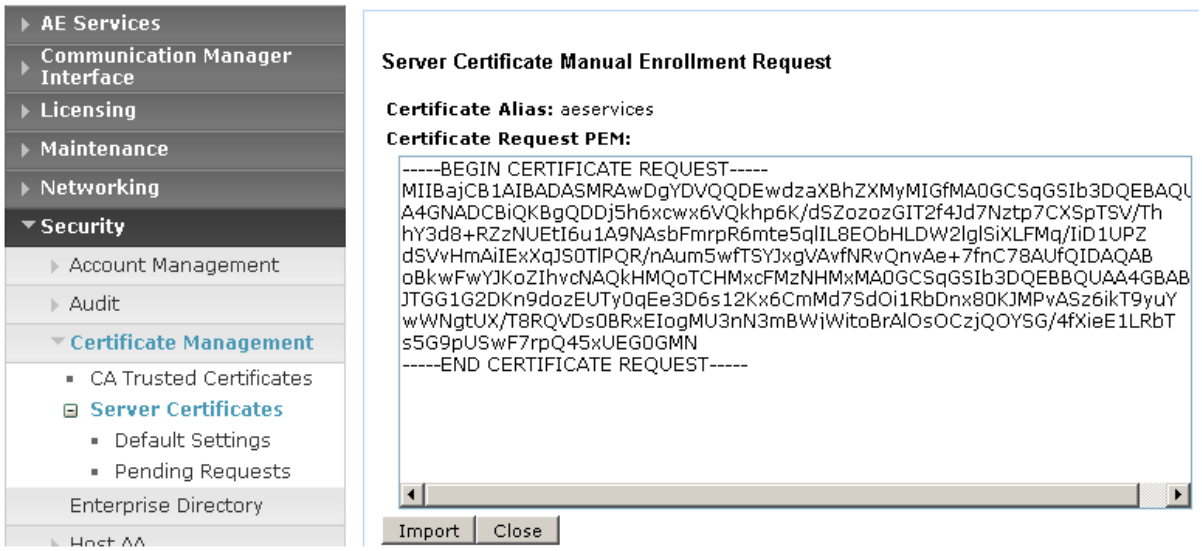


Figure 25: Example of Certificate Signing Request (CSR) text

After the signed client certificate is imported, the AES can communicate securely using TLS for the SIP CTI connection.

Importing a signed certificate into AES

Before you begin

- Ensure the Certificate Authority, Application Enablement Services (AES) server, and the Contact Center servers can all ping each other using a fully qualified domain name (FQDN).
- Import the root certificate into AES, see Importing a Certificate Authority root trusted certificate into AES on page 133.
- Copy the signed certificate to the Application Enablement Services server.

About this task

For the Application Enablement Services (AES) server to communicate securely with the Contact Center a common CA root certificate must be installed on both systems. The root certificate is installed on the AES as a CA trusted certificate. The AES server can then request a signed client certificate from the Certificate Authority by creating a Certificate Signing Request (CSR). Use the CSR text to download a signed certificate from your Certificate Authority. Import the signed client certificate into AES so that AES can communicate securely 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**.
   The Server Certificate Import page appears.
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**.
   A Server Certificate Import - Certificate imported successfully, message appears.
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.

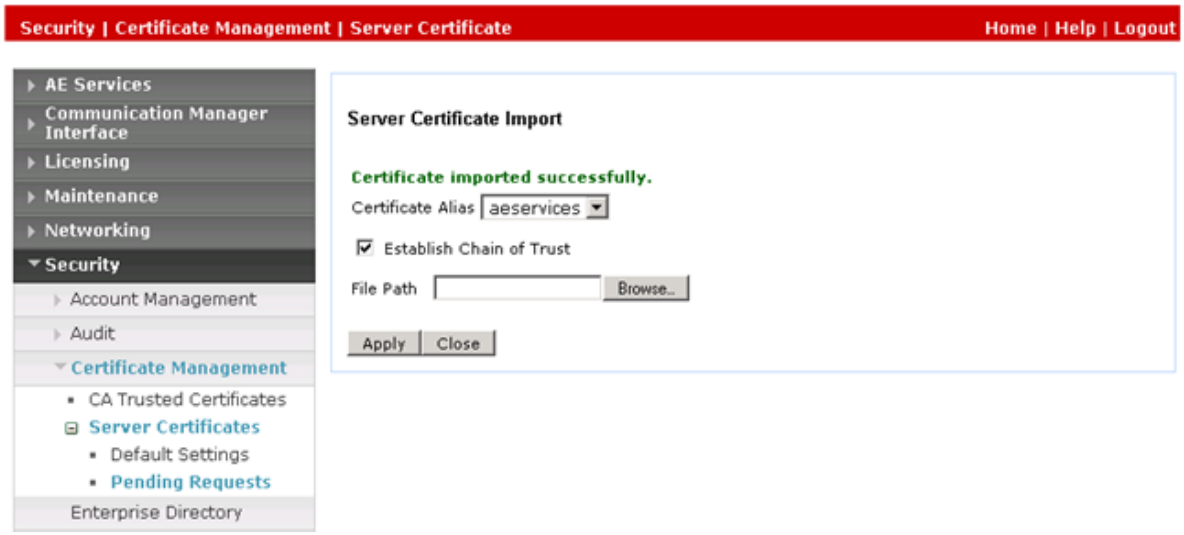


Figure 26: Example of importing a signed certificate into AES

After the signed client certificate is imported, the AES can communicate securely using TLS for the SIP CTI connection.

Adding Contact Center Manager Server as a trusted host on AES

About this task

Add Contact Center Manager Server (CCMS) as a trusted host on the Application Enablement Services server.

Note:

If you are using the Avaya Aura® Contact Center High Availability feature, you must add both the Active CCMS and the Standby CCMS 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 Manager 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 the Avaya Aura® Contact Center High Availability feature, repeat this procedure for the standby CCMS to add the standby CCMS 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 Certificate Manager.

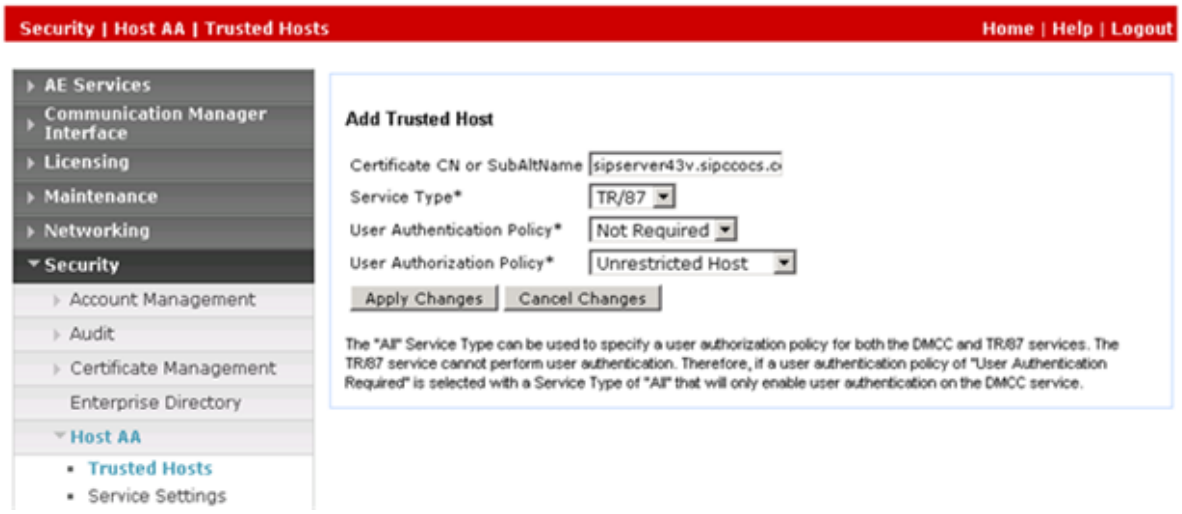


Figure 27: Example of adding the Contact Center Manager Server as a trusted host

Figure 28: Example of Contact Center Manager Server Certificate Manager FQDN setting

Configuring the TCP Retransmission Count

About this task

Configure the Application Enablement Services (AES) TCP retransmission count. A smaller TCP retransmission count reduces the amount of time that the AES server waits for a TCP

acknowledgement before closing the socket. To support Avaya Aura® Contact Center, the AES TCP retransmission count must be set to 2.

Important:

This procedure is applicable only for configuring Application Enablement Services 5.2.1, 5.2.2, or 6.1.

Procedure

1. In the left pane of the AES management console, click **Networking** > **TCP Settings**.
2. In the **TCP Retransmission Count [2-15]** box, type `2`.
3. Click **Apply Changes**.
4. Click **Apply**.

Procedure job aid

Configure the AES TCP retransmission count to support Avaya Aura® Contact Center High Availability.

Important:

The following screenshot is applicable only to Application Enablement Services 5.2.1, 5.2.2, or 6.1.

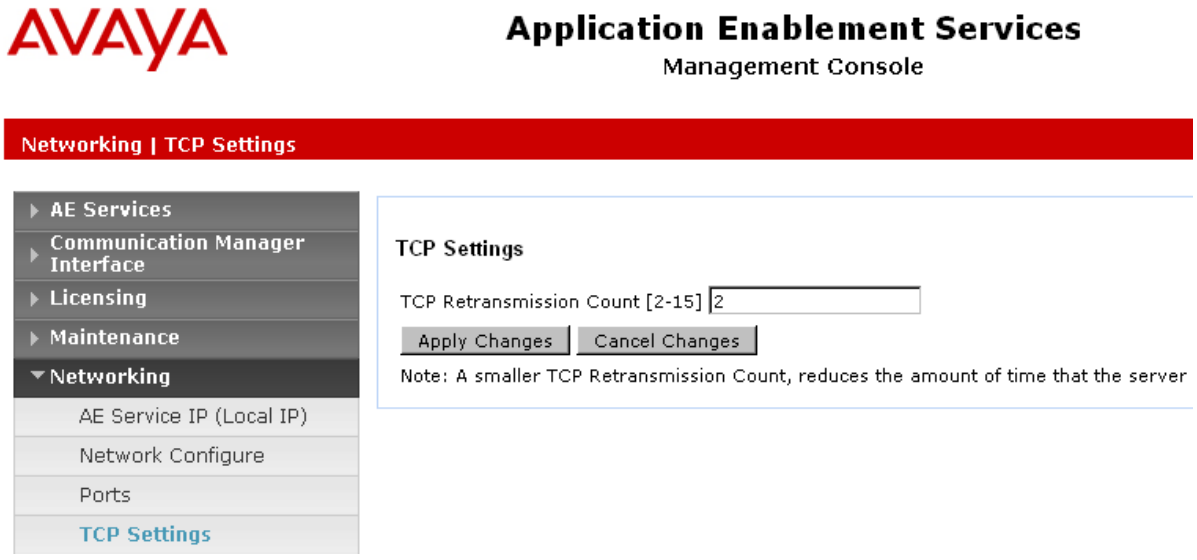


Figure 29: Example of configuring the AES TCP retransmission count

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.

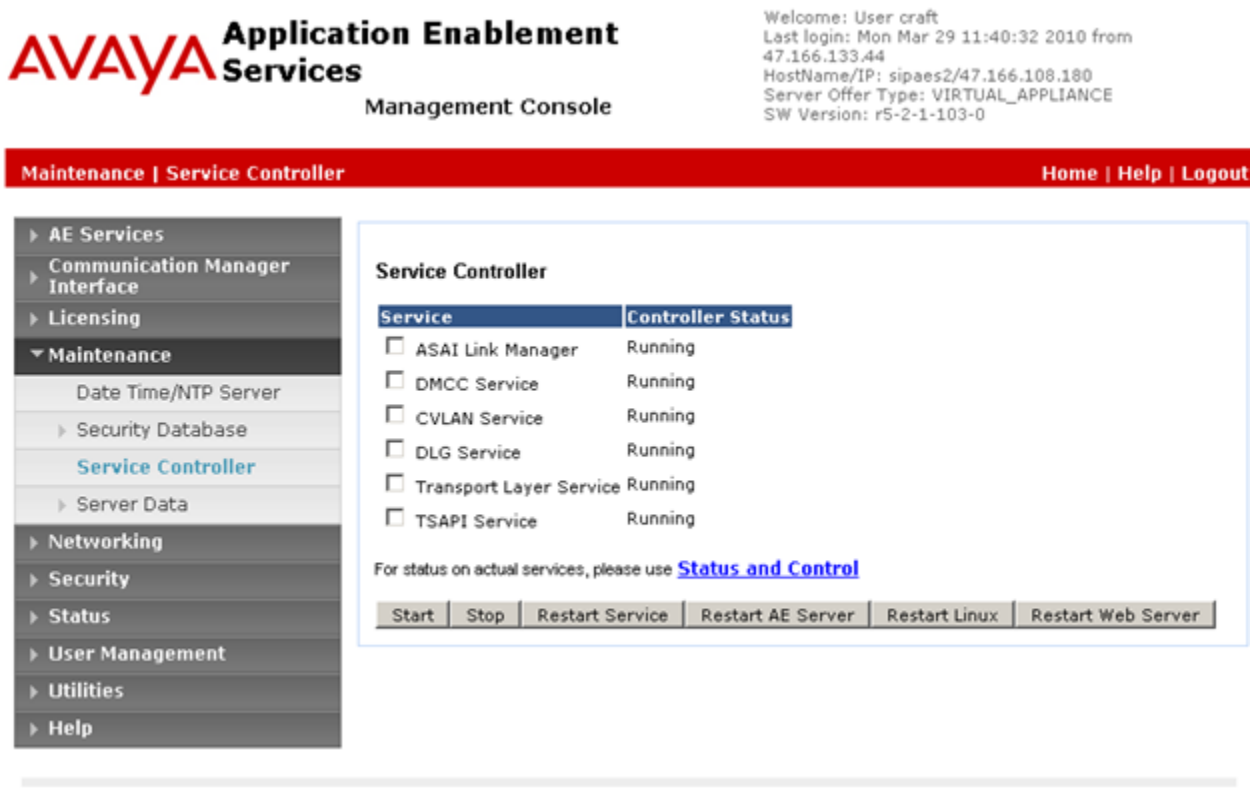


Figure 30: Example of restarting the AES Linux server

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 **Status**.
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.

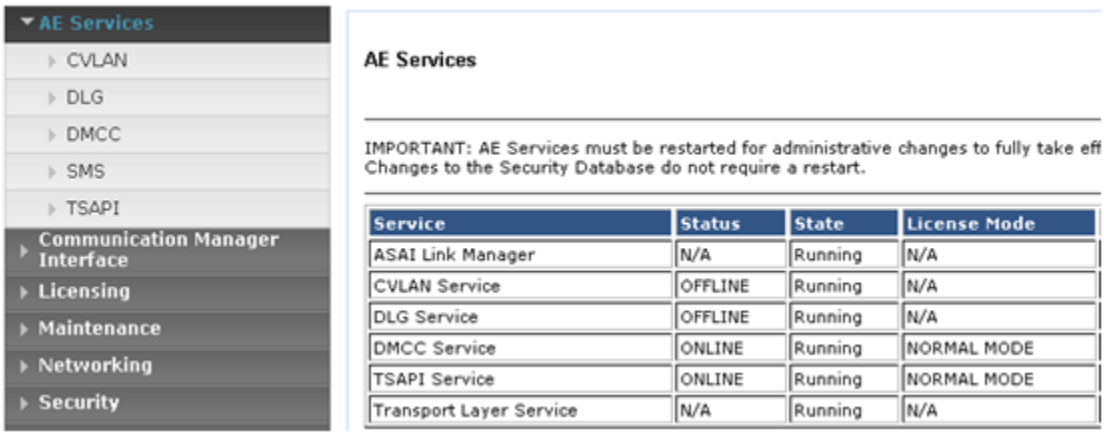


Figure 31: Example of verifying the AES services after a restart

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.

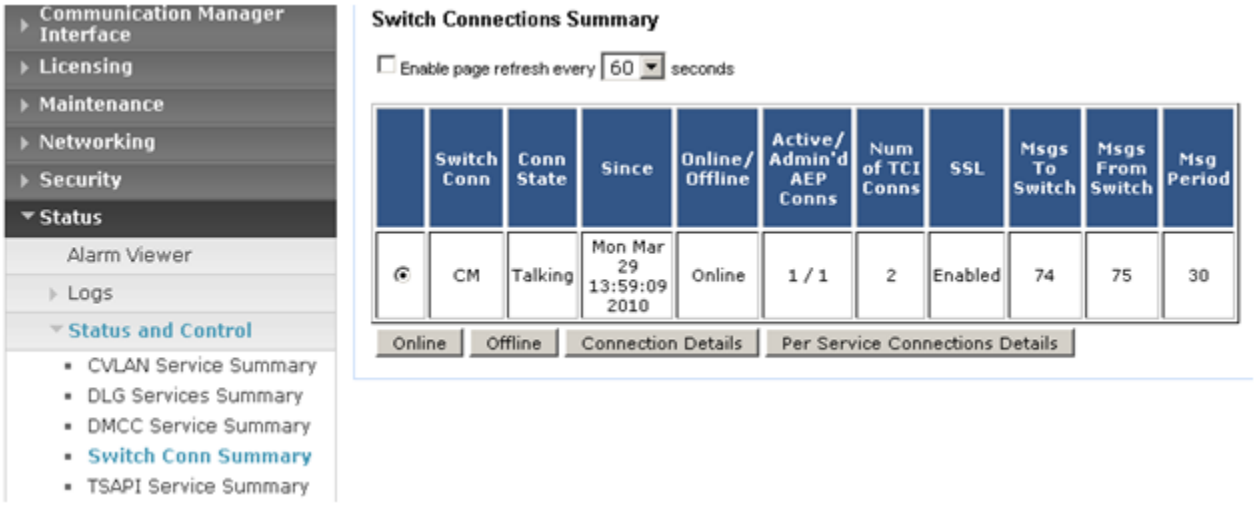


Figure 32: Example of verifying the AES connectivity with the Communication Manager after a restart

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.

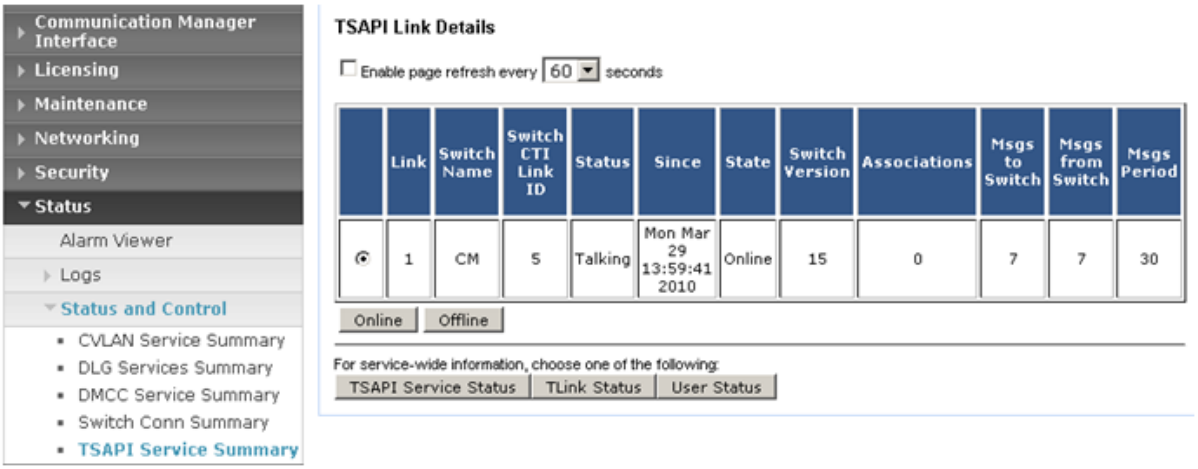


Figure 33: Example of verifying the AES connectivity with the Communication Manager after a restart

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.

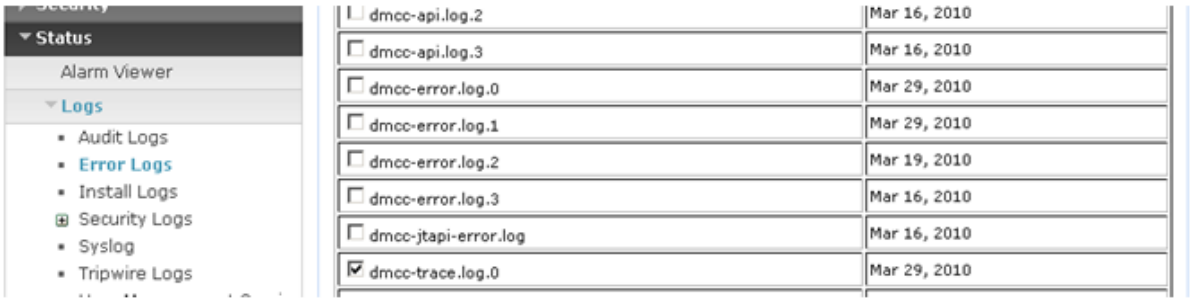


Figure 34: Example of AES Error Logs list

Confirming the AES and CCMS are communicating

Before you begin

- Enable TR87 SIP CTI, see Enabling TR87 on the AES on page 125.
- Configure security, see Configuring security on the AES on page 126.
- Import CA and Server certificates.
- Add CCMS as a trusted host, see Adding Contact Center Manager Server as a trusted host on AES on page 138.
- The Contact Center Manager Server (CCMS) is commissioned. For more information about commissioning CCMS for SIP, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- Log on to the Application Enablement Services (AES) server using Secure Shell (SSH).

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 10: Certificate Authority configuration

Certificate Authorities are used for issuing and managing certificates in secure systems that use public key technologies, such as telecoms systems that use Transport Layer Security (TLS) communication.

The Avaya Aura® Application Enablement Services (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 cryptographic protocol that helps secure a communications channel from danger or loss, and thus helps provide privacy and safety. With public key cryptography, two keys are created, one public and one private. Anything encrypted with either key can be decrypted only with the corresponding key. Thus if a message is encrypted with the server's private key, it can be decrypted only using its corresponding public key, ensuring that the data can only have come from the server.

You must obtain a root certificate from your Certificate Authority. A root certificate is an unsigned public key that identifies the root Certificate Authority (CA). Add the CA root certificate to the AES server and then use it to generate a Certificate Signing Request (CSR). Send the CSR and the Common Name (CN) of the AES server to your Certificate Authority. The CA verifies the identity of the request and issues a signed certificate (a private key) for use by the AES server. You must apply the CA root certificate and the signed certificate from your Certificate Authority to the AES server.

The Contact Center must also generate a Certificate Signing Request (CSR) and get it signed by the Certificate Authority before it can establish a secure TLS SIP link. The AES and Contact Center can then communicate securely using a TLS SIP connection.

Note:

Avaya Aura® Contact Center must use the same Certificate Authority and the same CA root certificate as the AES server.

Certificate Authority deployments vary depending on IT infrastructure and security requirements. As a worked example, this section describes how to add a standalone Certificate Authority role to a Microsoft Windows Server 2008 Release 2 server. And then how to use this standalone Certificate Authority to generate signed certificates.

Navigation

Installing a standalone Certificate Authority

About this task

Install a standalone Certificate Authority server by adding the Certificate Authority role to a Contact Center Manager Server.

When you are installing a standalone Certificate Authority you are asked for a validity period. The default Validity Period value is 12 months (1 year). Any certificate signed by this Certificate Authority with this validity period expires after 12 months. If the certificate expires, Contact Center Manager Server loses call control of the Avaya Aura® Unified Communications platform agent phones. Certificates then have to be resigned by the Certificate Authority before call control is reestablished.

Carefully consider the Certificate Authority Validity Period and your certificate requirements, before installing a standalone Certificate Authority.

Procedure

1. Log on to the server.
2. Click **Start** > **Administrative Tools** > **Server Manager**.
3. Under **Roles Summary**, click **Add Roles**.
4. Click **Next**.
5. Under **Roles**, select **Active Directory Certificate Services**.
6. Click **Next**.
7. On the **Active Directory Certificate Services** page, click **Next**.
8. Under **Role services**, select **Certificate Authority**.
9. Click **Next**.
10. Under **Specify Setup Type**, select **Standalone**.
11. Click **Next**.
12. Select **Root CA**.

13. Click **Next**.
14. Select **Create a new private key**.
15. Click **Next**.
16. On the Configure Cryptography for CA page, click **Next**.
17. On the Configure CA Name page, click **Next**.
18. On the Set Validity Period page, select a number of years appropriate to your certificate requirements.
19. Click **Next**.
20. On the Configure Certificate Database page, click **Next**.
21. On the Confirm Installation Selections page, review your selections and click **Install**.
22. After the Certificate Authority installs, click **Close**.

Procedure job aid

Example of installing a standalone Certificate Authority.

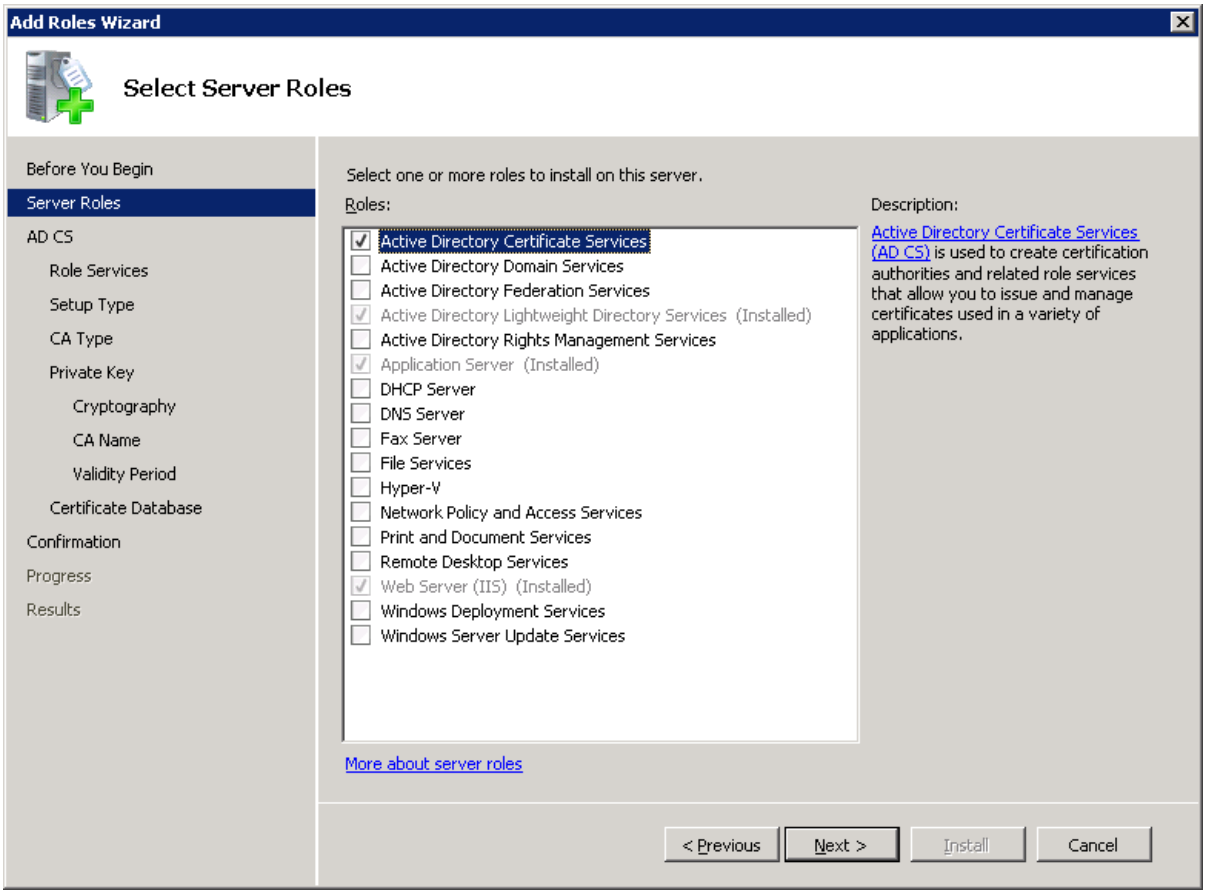


Figure 35: Example of installing a standalone Certificate Authority

Exporting a Certificate Authority root certificate

Before you begin

- Install a standalone Certificate Authority server. For more information about installing a Certificate Authority server, see Installing a standalone Certificate Authority on page 152.

About this task

Export a Certificate Authority root certificate for use in a secure system.

Procedure

1. Log on to the server.
2. Click **Start** > **Administrative Tools** > **Certification Authority**.
3. From the menu tree on the left side of the Certificate Authority, right-click on the Certificate Authority and select **Properties**.

4. On the Properties dialog, select the **General** tab.
5. Click **View Certificates**.
6. On the Certificate dialog, select the **Details** tab.
7. Click **Copy to File**.
   A Certificate Export Wizard appears.
8. Click **Next**.
9. Under **Select the format you want to use**, select **Base-64 encoded X.509 (.CER)**.
10. Click **Next**.
11. On the File to Export dialog, in the **File name** box, type the name of the Certificate Authority root certificate to export.
12. Click **Next**.
13. Click **Finish**.
    A Certificate Export Wizard - The Export was successful message box appears.
14. To close the message box click **OK**.
15. Click **OK**.

Procedure job aid

Example of exporting a Certificate Authority root certificate for use in a secure system.

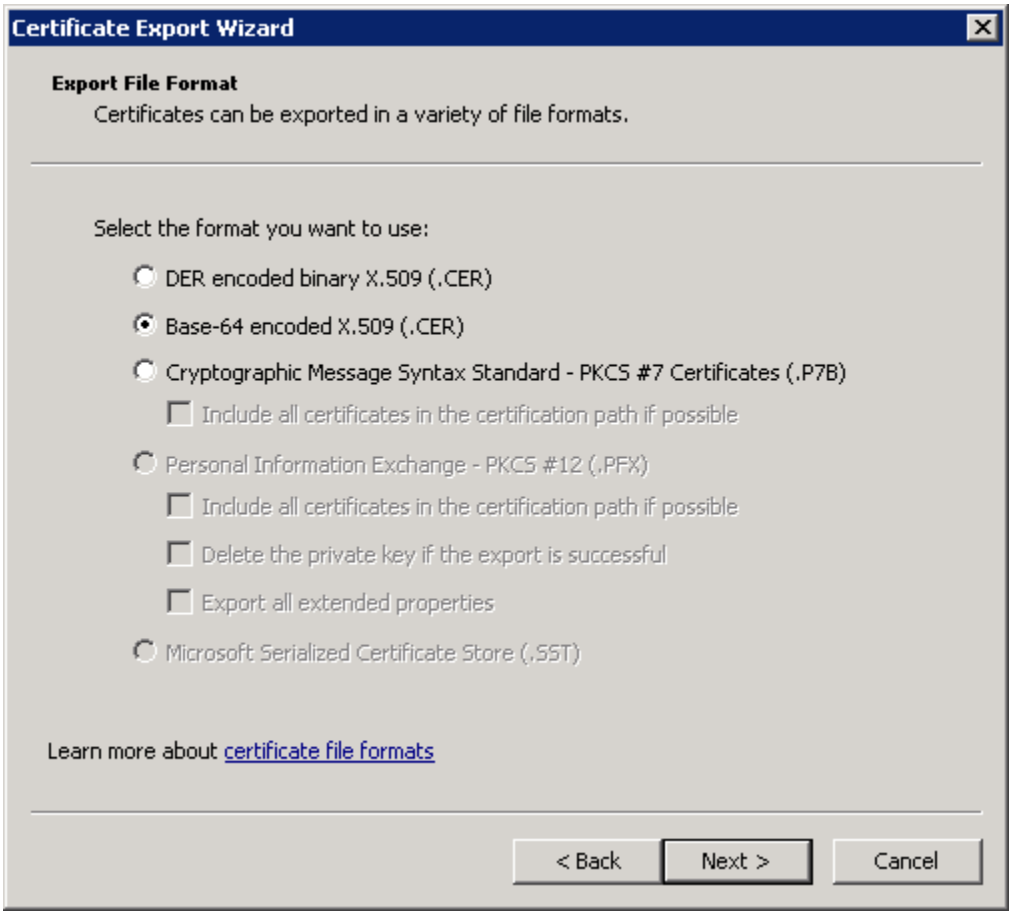


Figure 36: Example of exporting a root certificate from a standalone Certificate Authority

Generating a signed certificate

Before you begin

- Install a standalone Certificate Authority server. For more information about installing a Certificate Authority server, see Installing a standalone Certificate Authority on page 152.
- Copy the Certificate Signing Request (CSR) text file to the standalone Certificate Authority server.

About this task

Generate a signed certificate using a Certificate Signing Request (CSR) and a standalone Certificate Authority server and then export the signed certificate for use in a secure system.

Procedure

1. Log on to the server.
2. Click **Start** > **Administrative Tools** > **Certification Authority**.
3. Right-click on the Certificate Authority snap-in, and select **All Tasks** > **Submit new request**.
4. On the Open Request File dialog, select the Certificate Signing Request (CSR) notepad text file.
5. Click **Open**.
6. From the menu tree on the left side of the Certificate Authority, select **Pending Requests**.
7. From the list of **Pending Requests**, select your request, right-click and select **All Tasks** > **Issue**.
8. From the menu tree on the left hand side of the Certificate Authority, select **Issued Requests**.
9. From the list of issued requests, select your request.
10. Right-click on the request and select **Open**.
    A Certificate Information dialog appears.
11. Select the **Details** tab.
12. Click **Copy to File**.
    A Certificate Export Wizard appears.
13. Click **Next**.
14. Under **Select the format you want to use**, select **Base-64 encoded X.509 (.CER)**.
15. Click **Next**.
16. On the File to Export dialog, in the **File name** box, type the name of the signed certificate to export.
17. Click **Next**.
18. Click **Finish**.
    A Certificate Export Wizard - The Export was successful message box appears.
19. To close the message box click **OK**.
20. Click **OK**.

Procedure job aid

Example of generating a signed certificate.

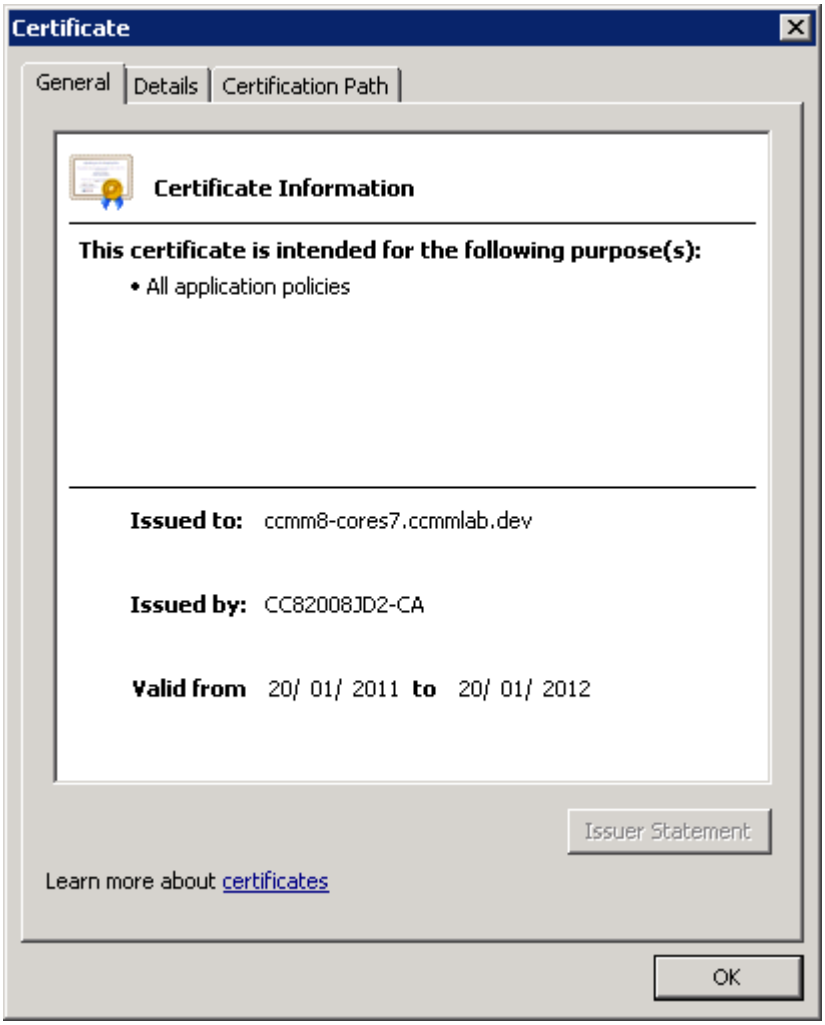


Figure 37: Example of generating a signed certificate using a standalone Certificate Authority

Chapter 11: 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.

DNIS support using Session Manager configuration procedures

About this task

This task flow shows you the sequence of procedures you perform to support Dialed Number Identification Service (DNIS) using Session Manager configuration.

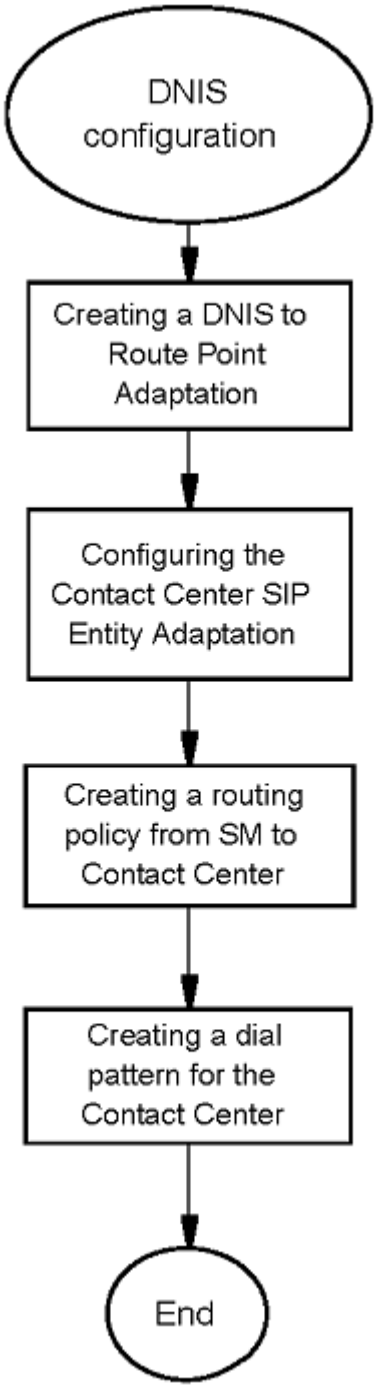


Figure 38: DNIS support using Session Manager configuration

Creating a DNIS to Route Point Adaptation

About this task

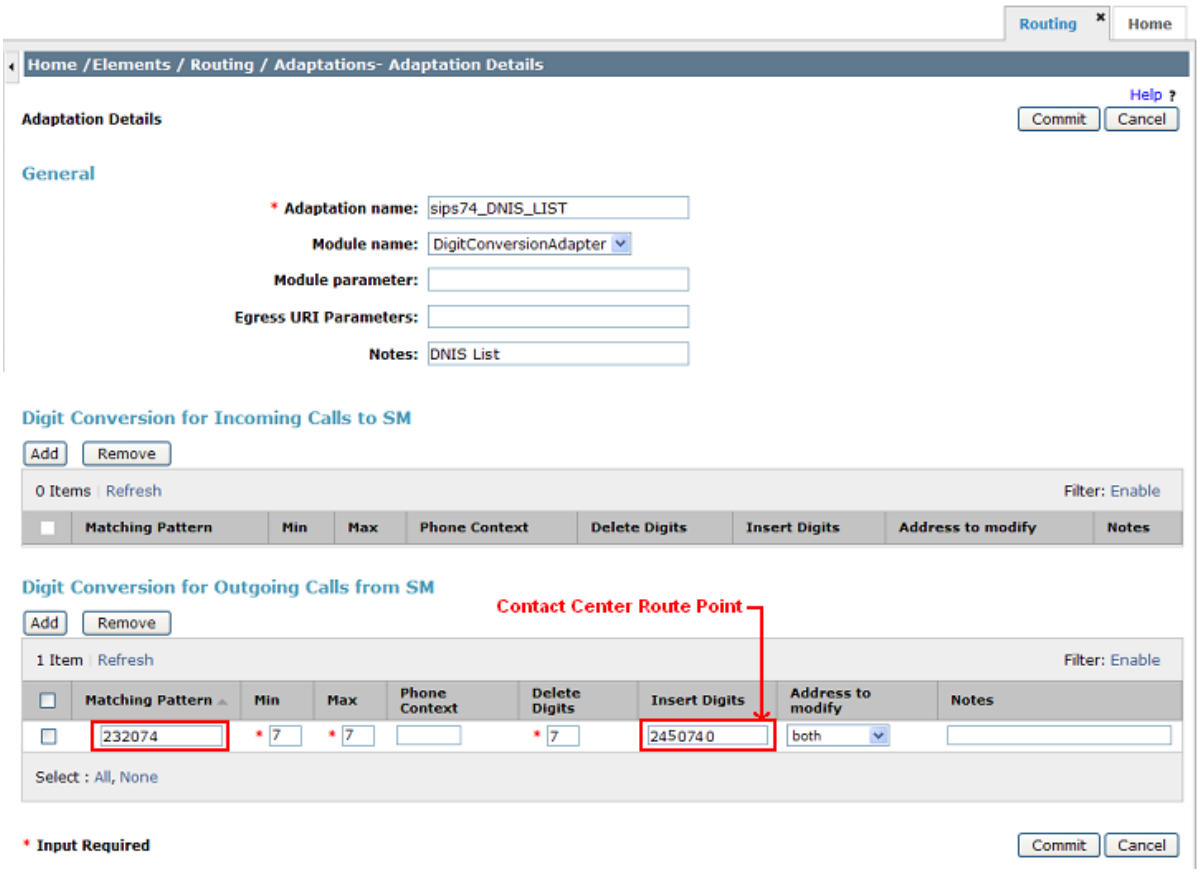
Create a Digit Conversion Adapter adaptation to convert a Dialed Number Identification Service (DNIS) number to an Avaya Aura® Contact Center Route Point number.

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.

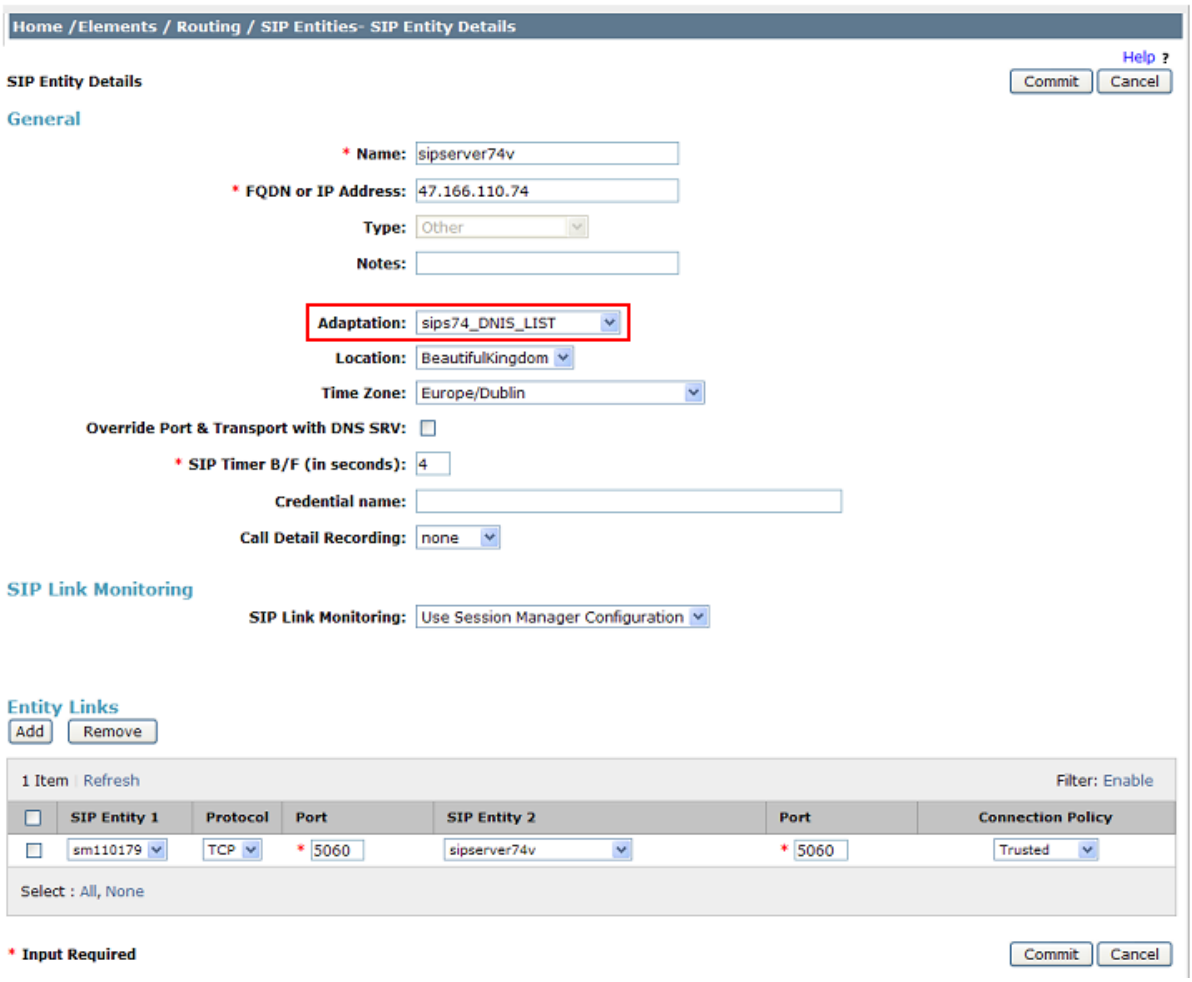
Procedure

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.

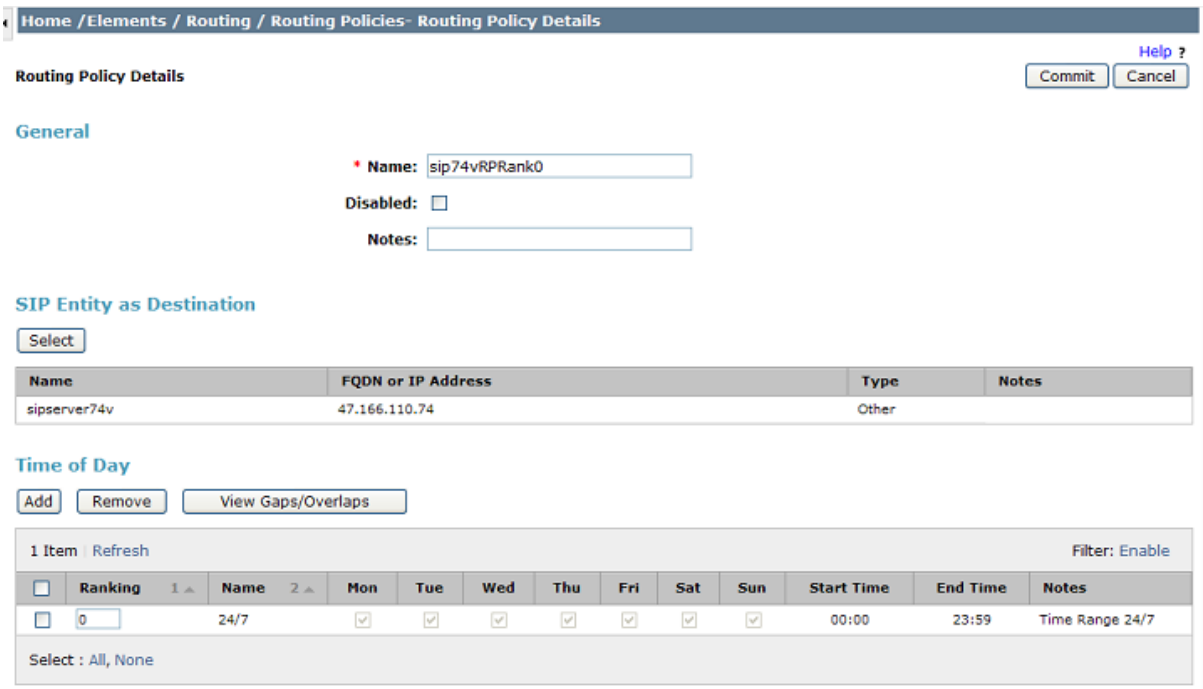
Session Manager uses the data configured in the Routing Policy to find the best match against the number (or address) of the called party.

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.

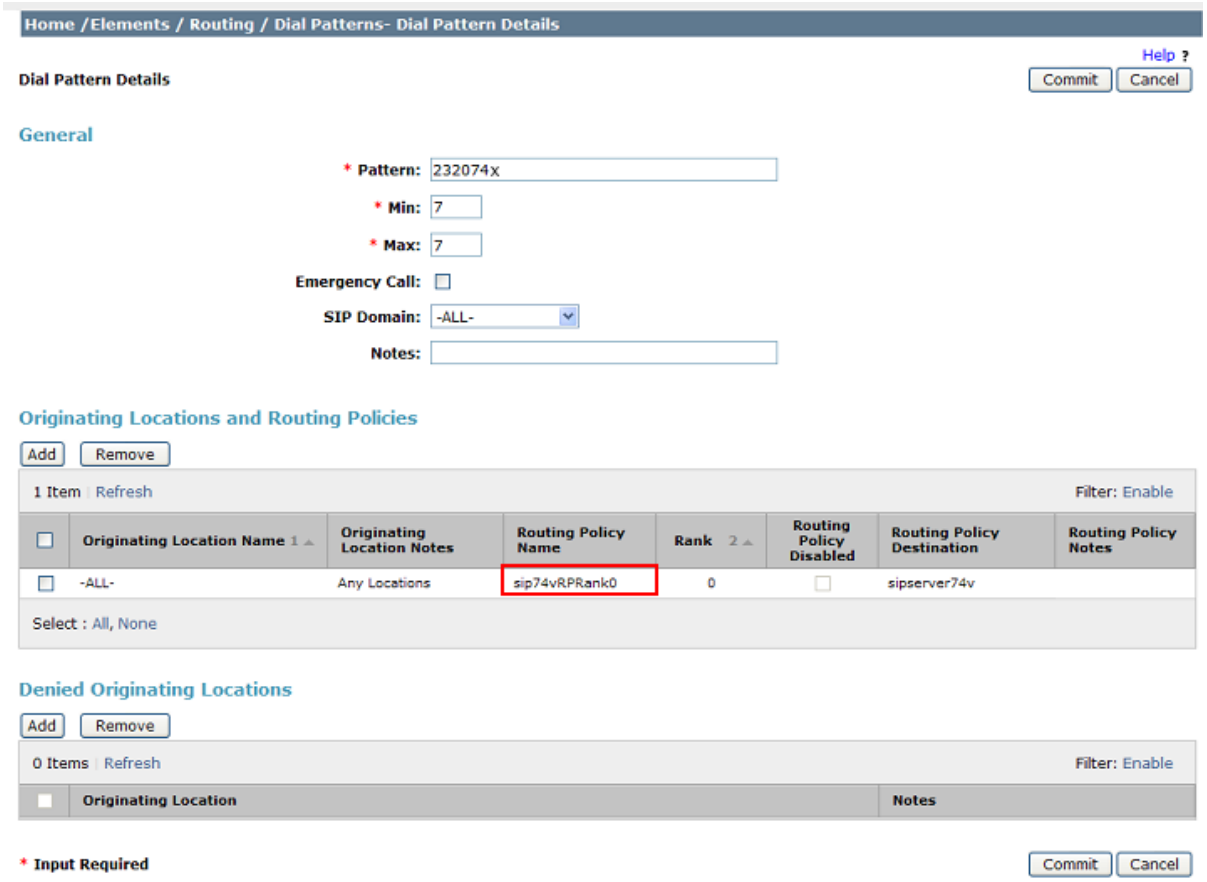
Procedure

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 12: 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. In solutions with Avaya Aura® Call Center Elite, Avaya Aura® Session Manager can also reroute customer voice contacts intended for Contact Center to an Avaya Aura® Communication Manager split or Elite skill.

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.

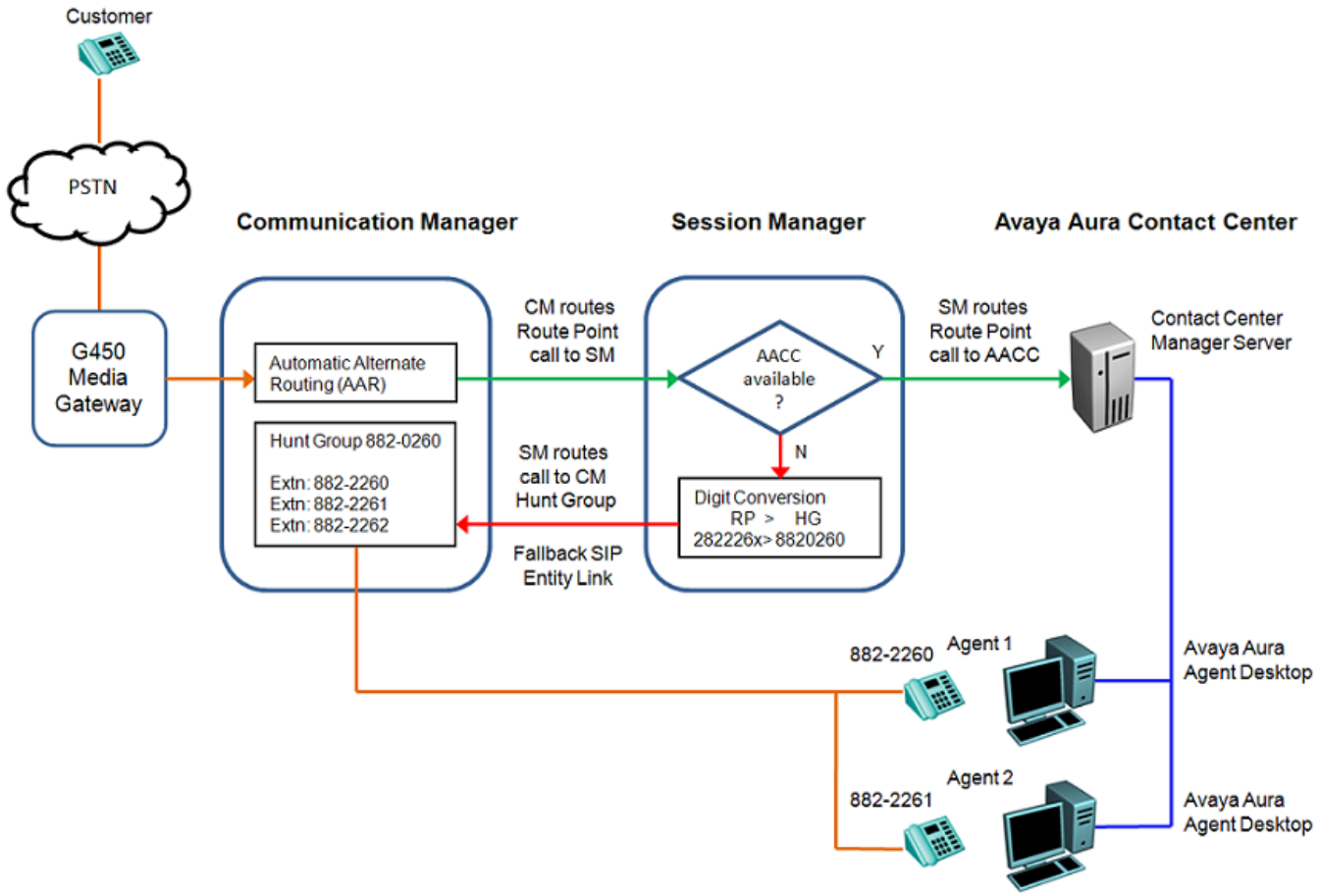
A Communication Manager Hunt Group is a group of agent stations that can handle multiple calls to a single phone number. For each call to the Hunt Group number, Communication Manager hunts for an available agent station in the Hunt Group, and it then connects the customer call to that station. There 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.



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

Fallback to an Avaya Aura Communication Manager Hunt Group configuration procedures

About this task

This task flow shows you the sequence of procedures you perform to configure Avaya Aura® Contact Center fallback to an Avaya Aura® Communication Manager Hunt Group.

Figure 39: Fallback to an Avaya Aura® Communication Manager Hunt Group configuration

procedures

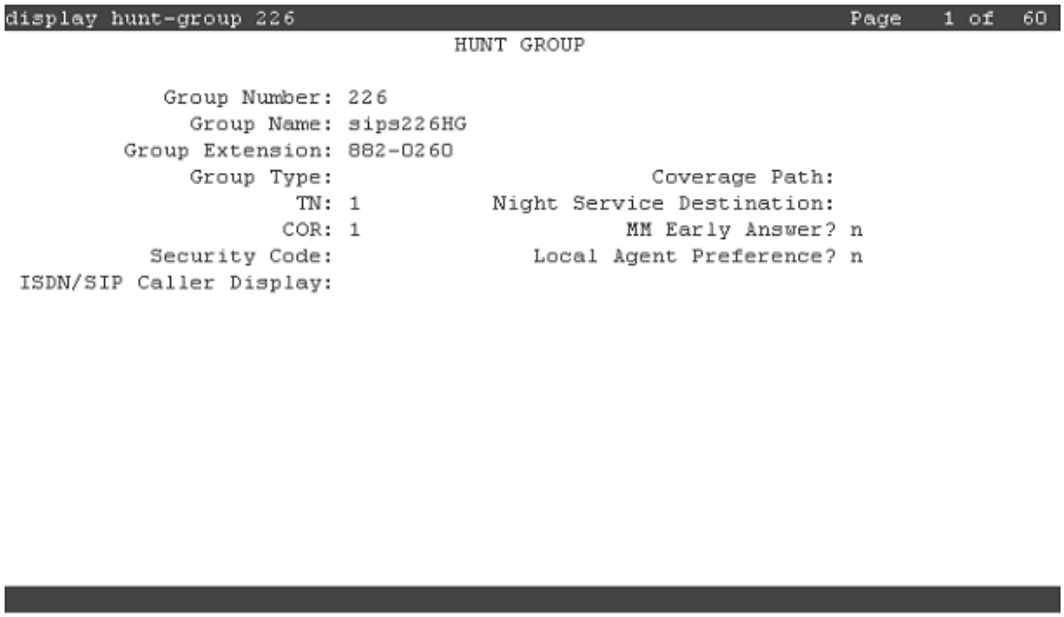
Adding a Hunt Group

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.



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.

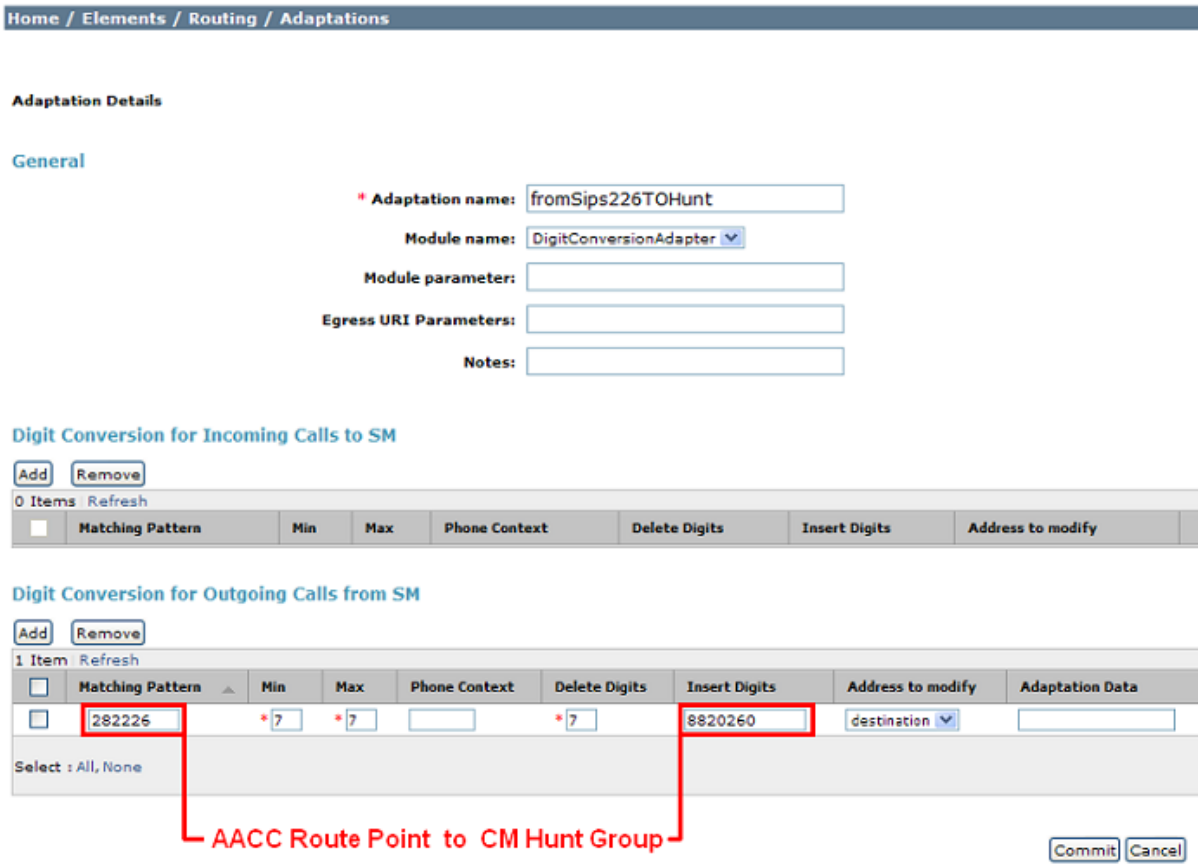
Procedure

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, for example 5070. 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 42.
4. In the **Far-end Listen Port** field, type the port number, for example 5070. 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 181.
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 89.

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.

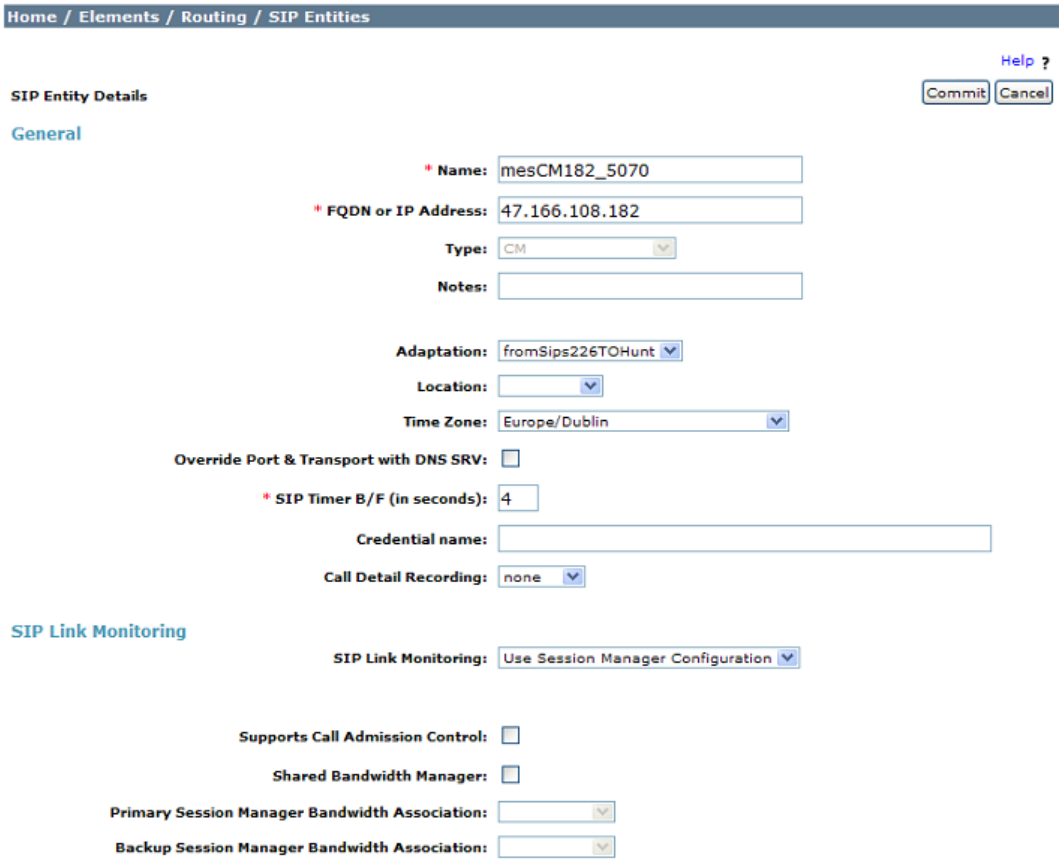
Assign an adaptation to the Communication Manager SIP Entity. The Digit Conversion Adaptation converts an Avaya Aura® Contact Center Route Point number into a Communication Manager Hunt Group number. If Avaya Aura® Contact Center is not available to process a call, the dialed Route Point number is replaced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

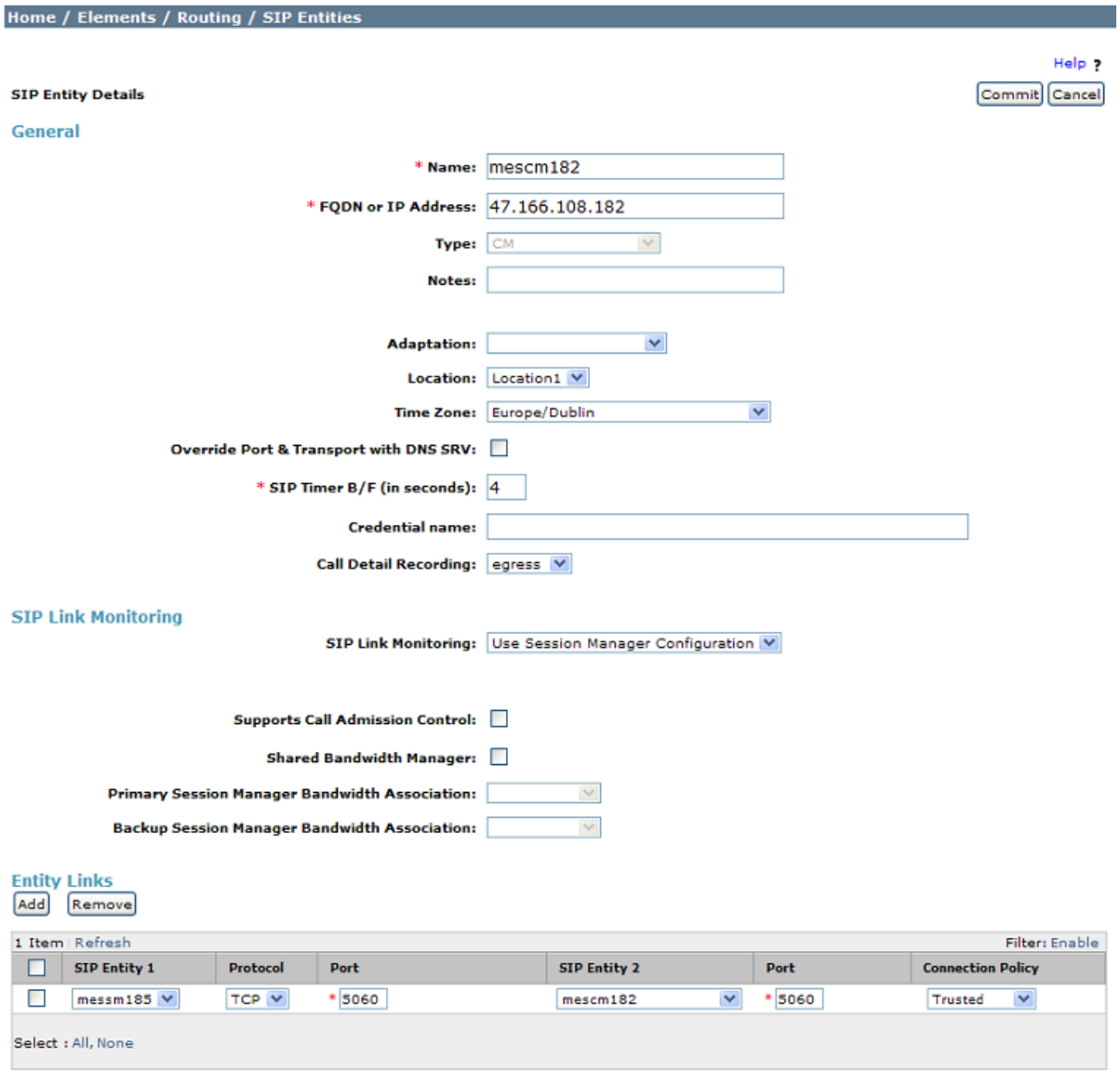
2. Click **New**.
3. In the **Name** box, type the name of the Communication Manager SIP Entity.

   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.


Home / Elements / Routing / SIP Entities
Help ?
SIP Entity Details
Commit
Cancel
General
* Name: mescm182
* FQDN or IP Address: 47.166.108.182
Type: CM
Notes:
Adaptation:
Location: Location1
Time Zone: Europe/Dublin
Override Port & Transport with DNS SRV:
* SIP Timer B/F (in seconds): 4
Credential name:
Call Detail Recording: egress
SIP Link Monitoring
SIP Link Monitoring: Use Session Manager Configuration
Supports Call Admission Control:
Shared Bandwidth Manager:
Primary Session Manager Bandwidth Association:
Backup Session Manager Bandwidth Association:
Entity Links
Add
Remove
1 Item Refresh
Filter: Enable
SIP Entity 1
Protocol
Port
SIP Entity 2
Port
Connection Policy
messm185
TCP
* 5060
mescm182
* 5060
Trusted
Select : All, None

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 177.

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.

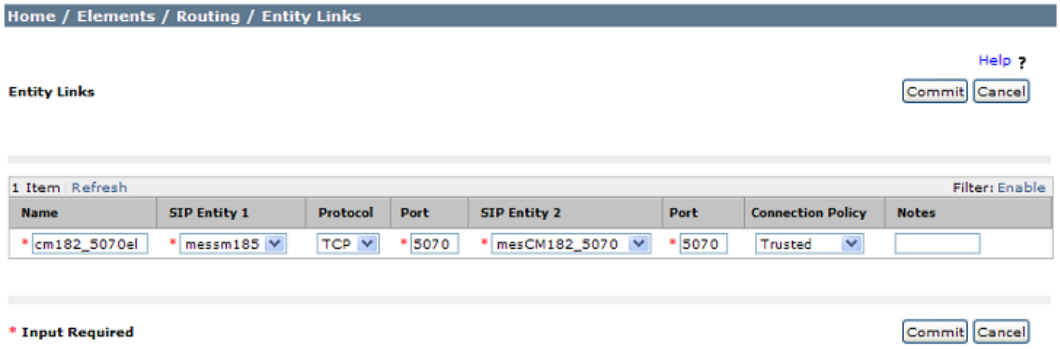
Procedure

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.

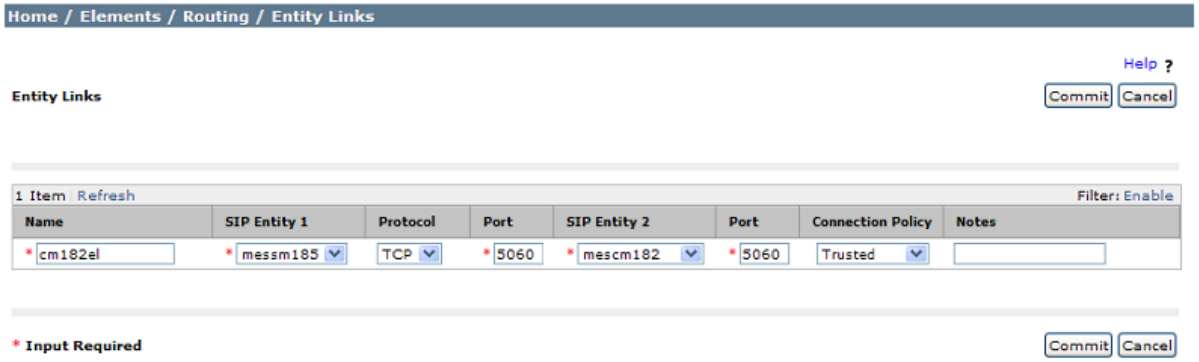
   SIP entity 1 must always be a Session Manager instance.
5. In the **Port** box, type 5070.
6. Under **SIP Entity 2**, select the required Communication Manager SIP entity from the drop-down list. For example, select the additional Communication Manager SIP Entity mesCM182_5070.
7. In the **Port** box, type 5070.
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.

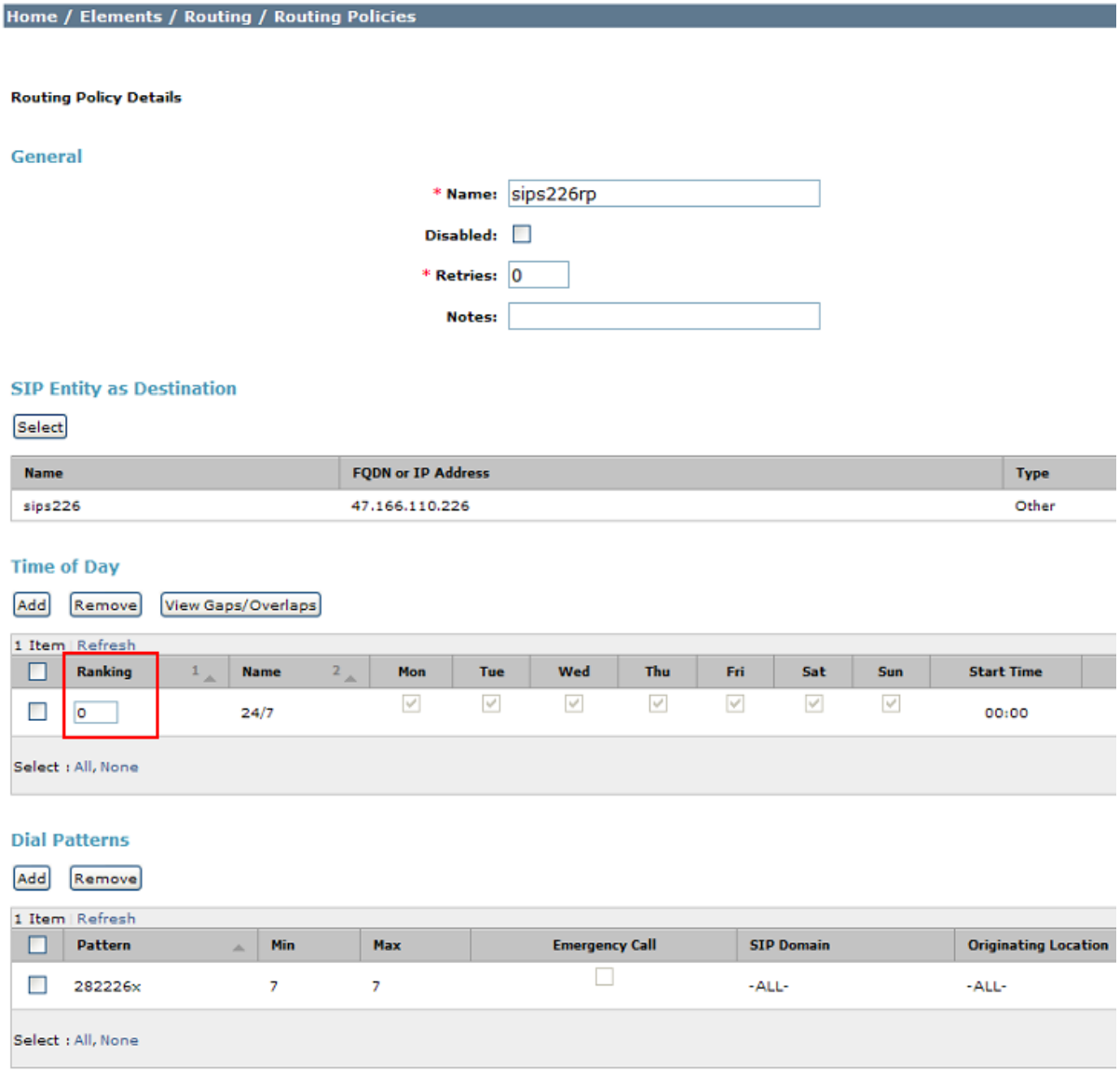
Procedure

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

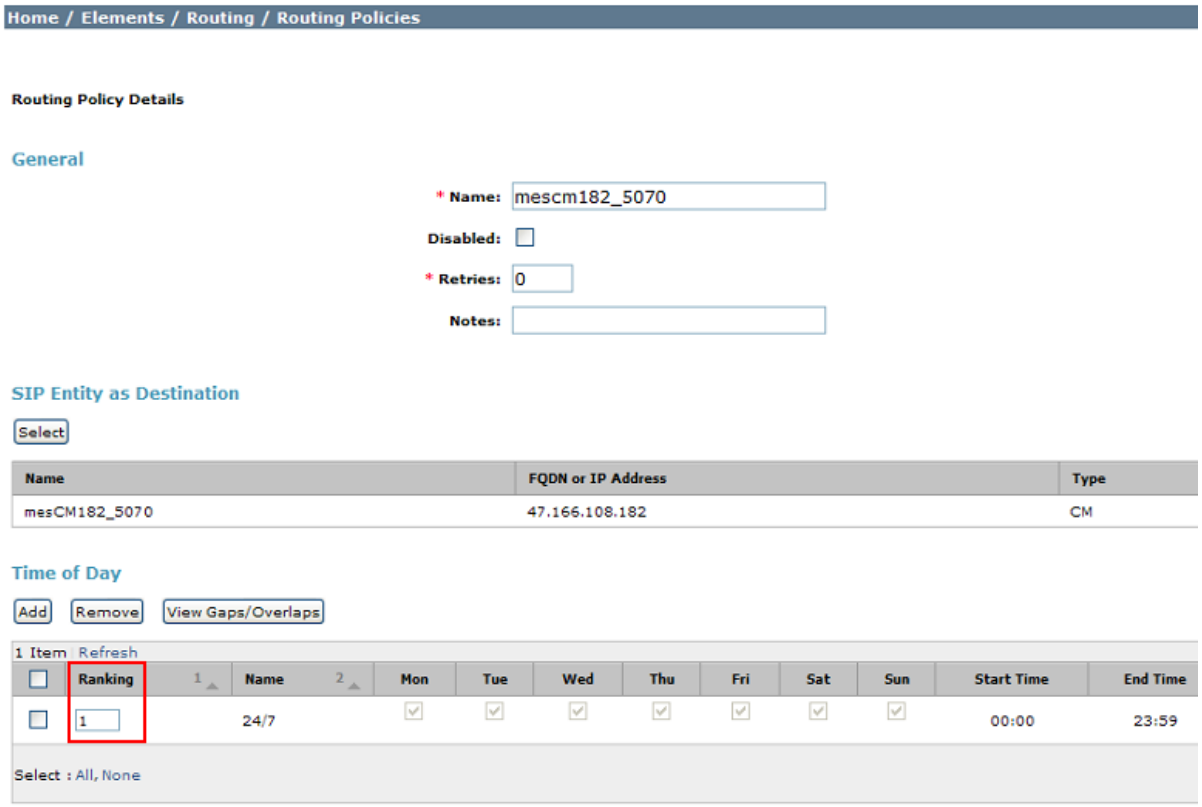
Create a routing policy from Session Manager to Avaya Aura® Communication Manager. Session Manager uses the data configured in the Routing Policy to find the best match against the number (or address) of the called party.

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.

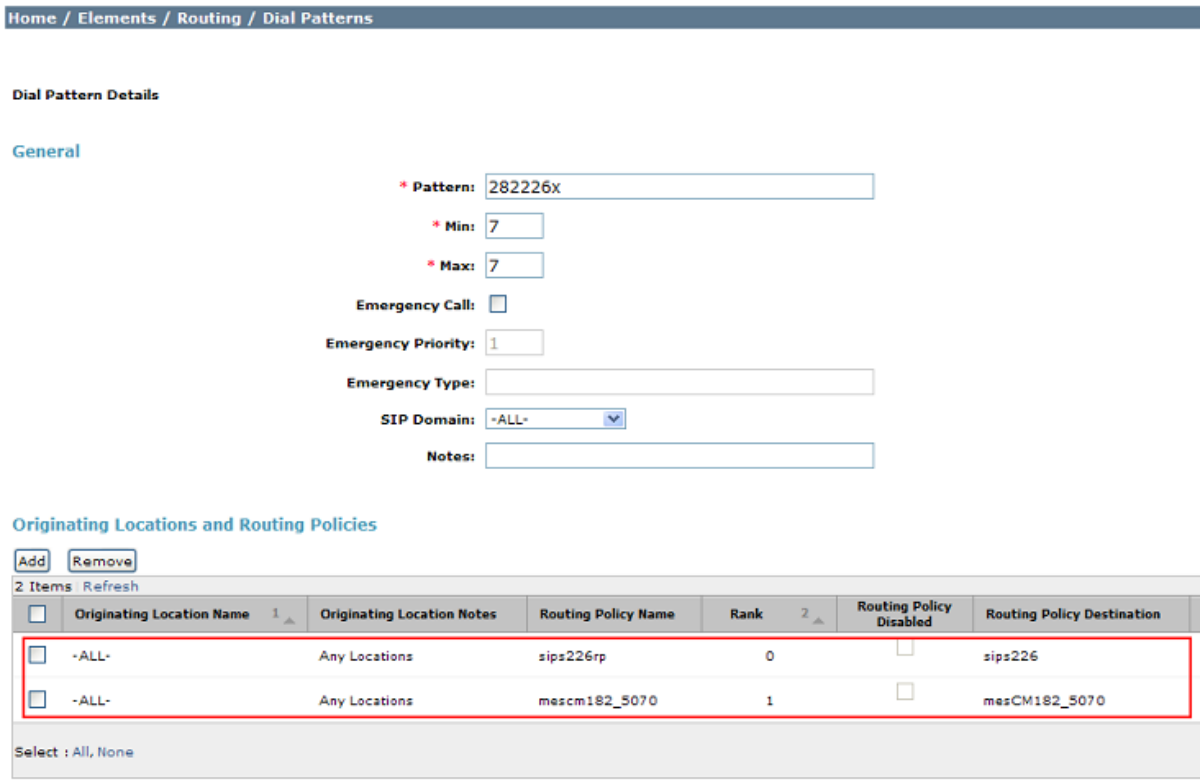
Note:

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.
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.

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.

Chapter 13: 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.

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.

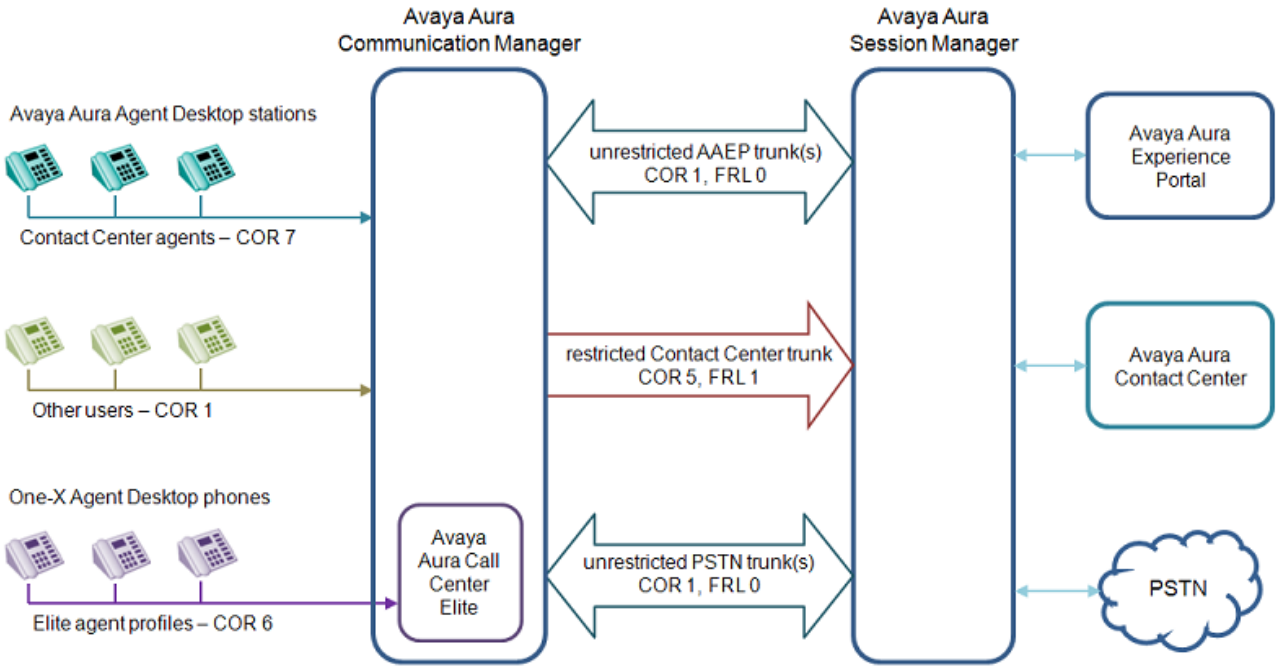
There are many methods to achieve this logical separation but the example method used here is one of the simplest and easiest to implement.

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.

The following diagram shows an 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 via 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 Aura® 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 Aura® 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.

Avaya Aura® Call Center Elite and Avaya Aura® Contact Center configuration procedures

Before you begin

- Configure Avaya Aura® Communication Manager for integration with Avaya Aura® Contact Center as normal. For more information see, Communication Manager configuration on page 31.

About this task

This task flow shows you the sequence of additional procedures you perform to configure Avaya Aura® Call Center Elite and Avaya Aura® Contact Center on the same Avaya Aura® Communication Manager.

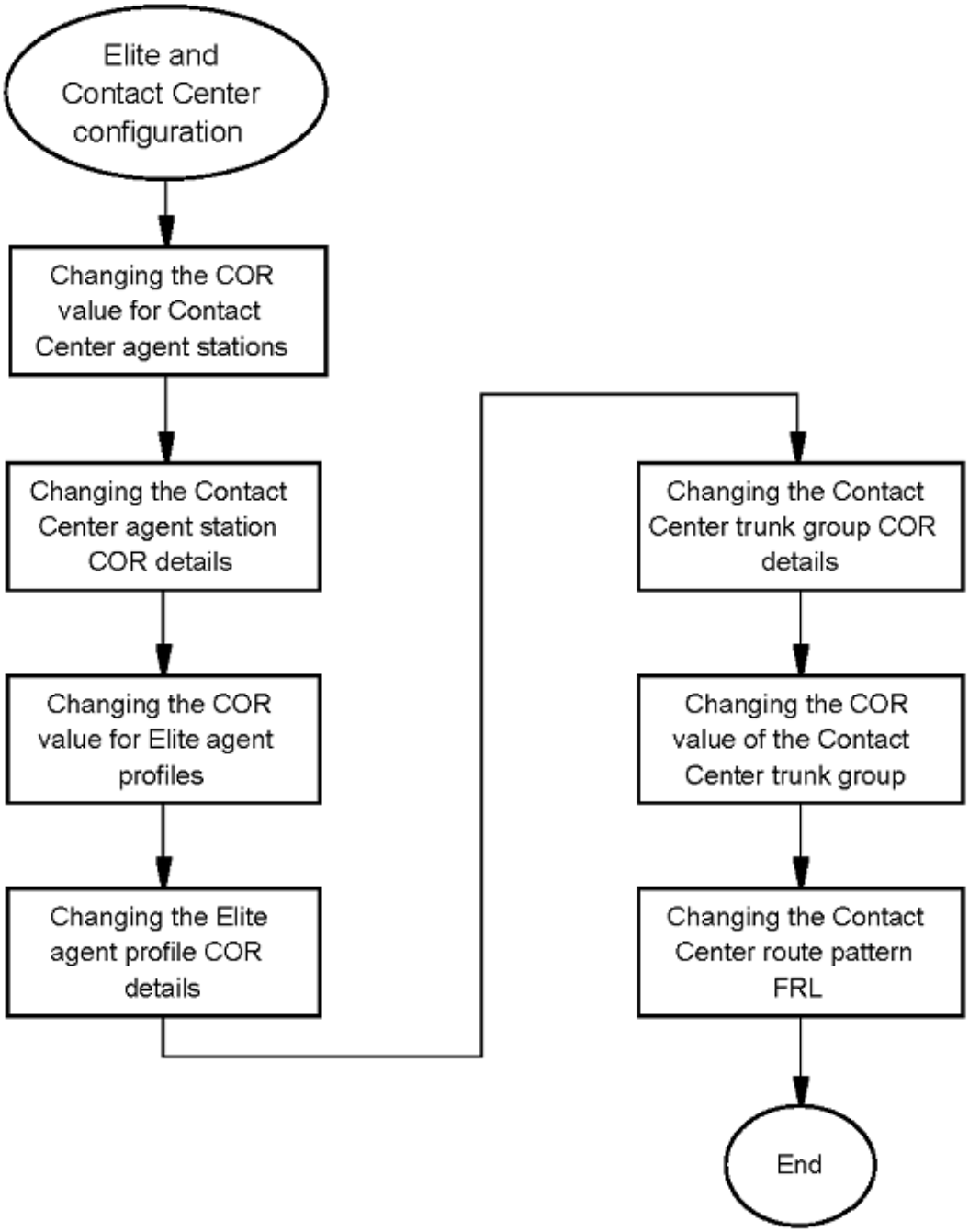


Figure 40: Avaya Aura® Call Center Elite and Avaya Aura® Contact Center configuration procedures

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 51.

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 14: 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.

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:

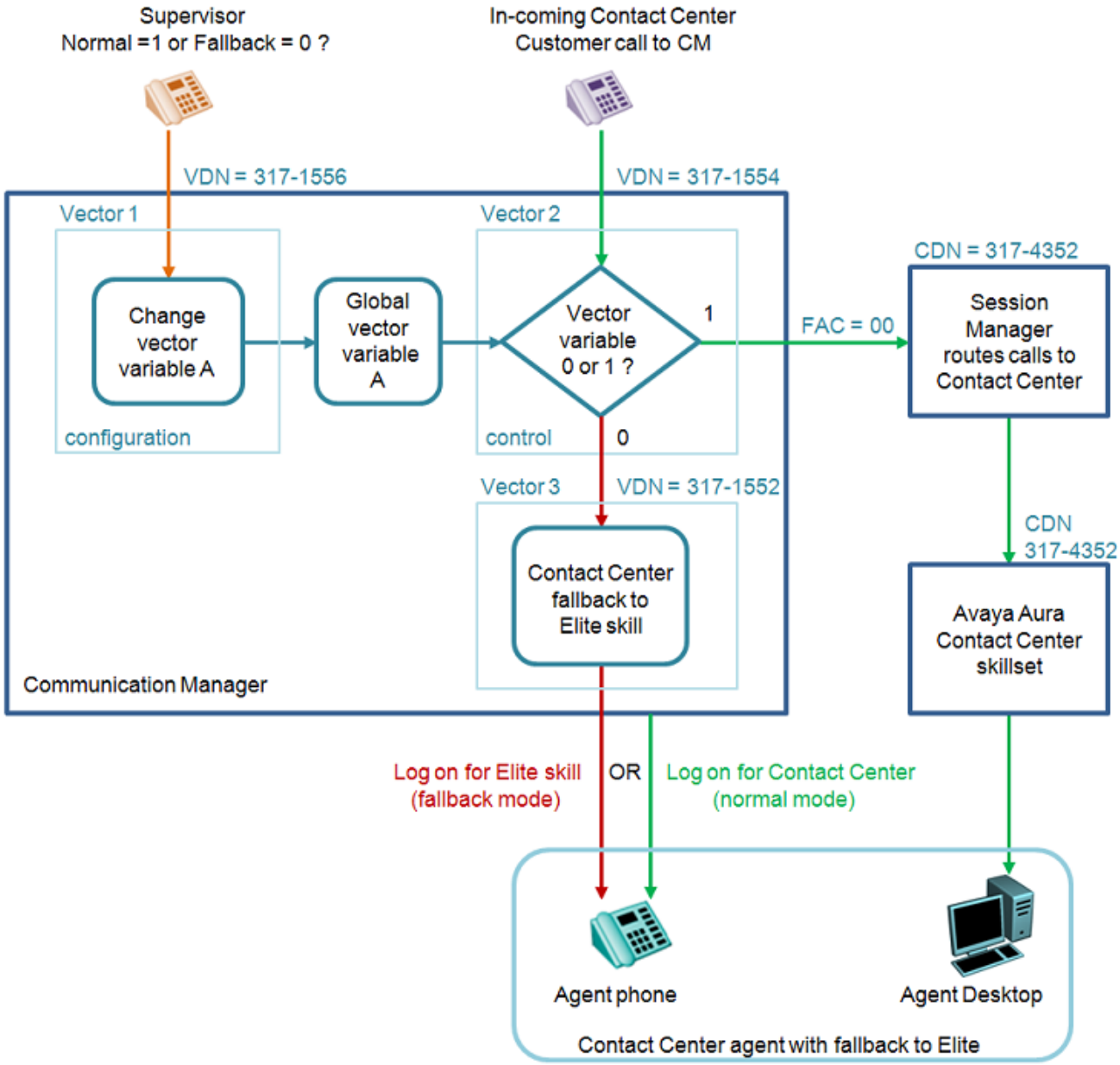
- VDN and associated vector which allows a supervisor to dial in and set value of a fallback vector variable. This vector is used to *configure* whether Communication Manager reroutes calls intended for Contact Center to Elite or not.
- VDN and associated vector which routes calls either to Avaya Aura®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



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 Aura® 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 Aura® 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 22.

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 Aura® Agent Desktop as logging on to both applications simultaneously is not supported.
- Only Avaya Aura® Contact Center agents that use a physical station may be able to handle voice contacts in a fallback mode. Agents that use the embedded H.323 Softphone may or may 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.

Fallback to an Avaya Aura® Call Center Elite skill configuration procedures

Before you begin

- 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 191.

About this task

This task flow shows you the sequence of procedures you perform to configure Avaya Aura® Communication Manager to support Avaya Aura® Contact Center fallback to an Avaya Aura® Call Center Elite skill.

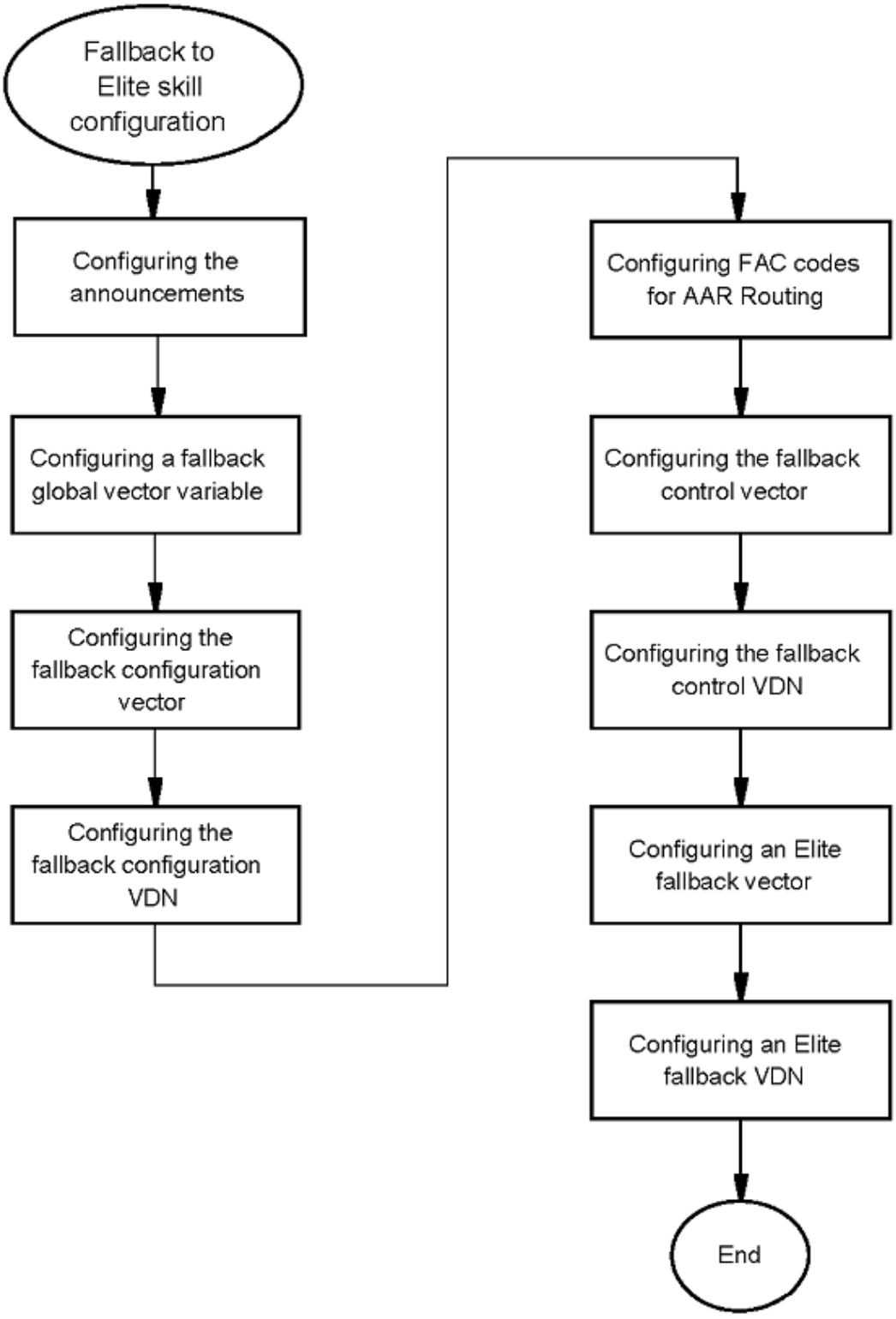


Figure 41: Avaya Aura® Contact Center fallback to an Avaya Aura® Call Center Elite skill configuration procedures

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 219.
- Configure three announcements. For more information about configuring announcements, see Configuring the announcements on page 217.

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

Step	Command			Comment
				value of zero and Avaya Aura® Contact Center CDN calls are routing to Elite.
13	announcement		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			
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 220.

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.

Step	Command			Comment
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 226.

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 229.

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 15: 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 via Session Manager):

- Modular Messaging 5.2
- Avaya Aura® Messaging
- Communication Manager 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.

Coverage Path configuration procedures

About this task

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

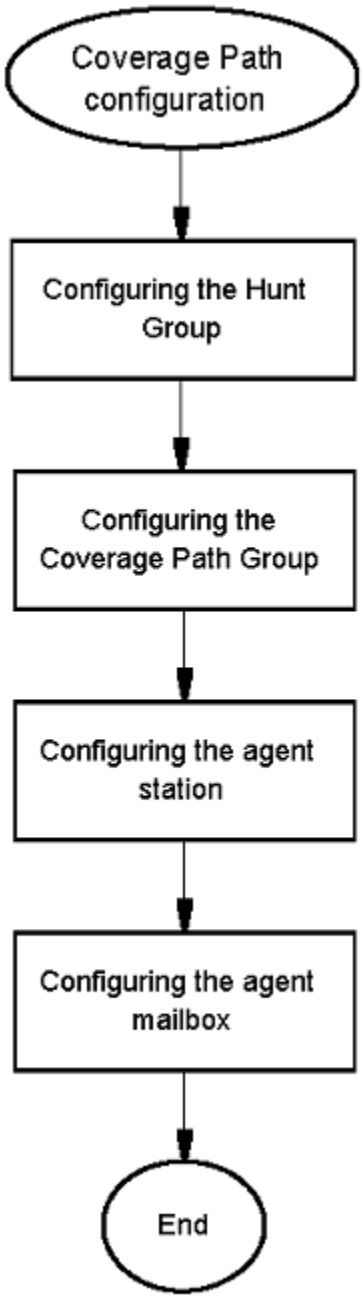


Figure 42: Coverage Path configuration procedures

Configuring the Hunt Group

Before you begin

Add a Communication Manager Hunt Group. For more information, see Adding a Hunt Group on page 173.

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 236.

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 236.
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 237.

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 16: 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 (CM) is administered using System Access Terminal (SAT).

Avaya Aura® Contact Center supports Communication Manager stations (phones) with a maximum of 2 Call Appearance lines per agent station. New Communication Manager stations are automatically created with 3 Call Appearance lines, so if a station is to be used by an Avaya Aura® Contact Center agent, you must configure the new station to have a maximum of 2 Call Appearance lines. You can use the Endpoint Editor in Avaya Aura® System Manager to remove one of the Call Appearance lines.

Navigation

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 CM application, the CM 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.

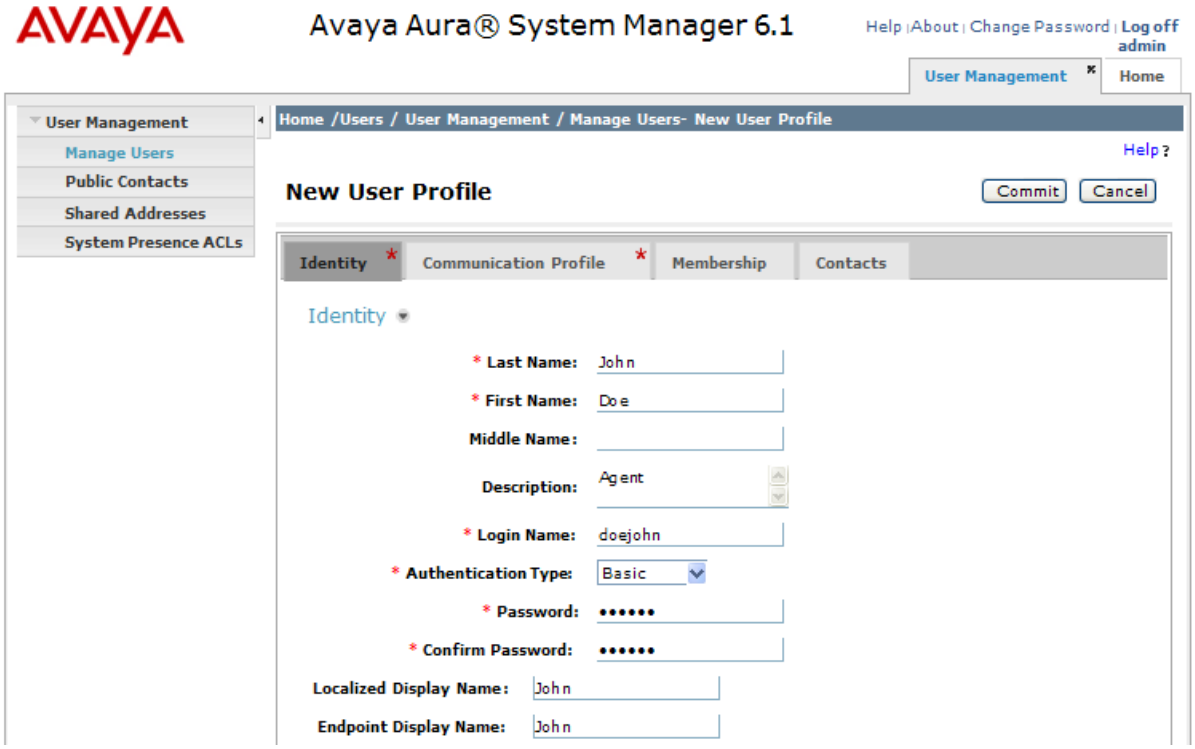


Figure 43: Example of adding a new User in System Manager

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

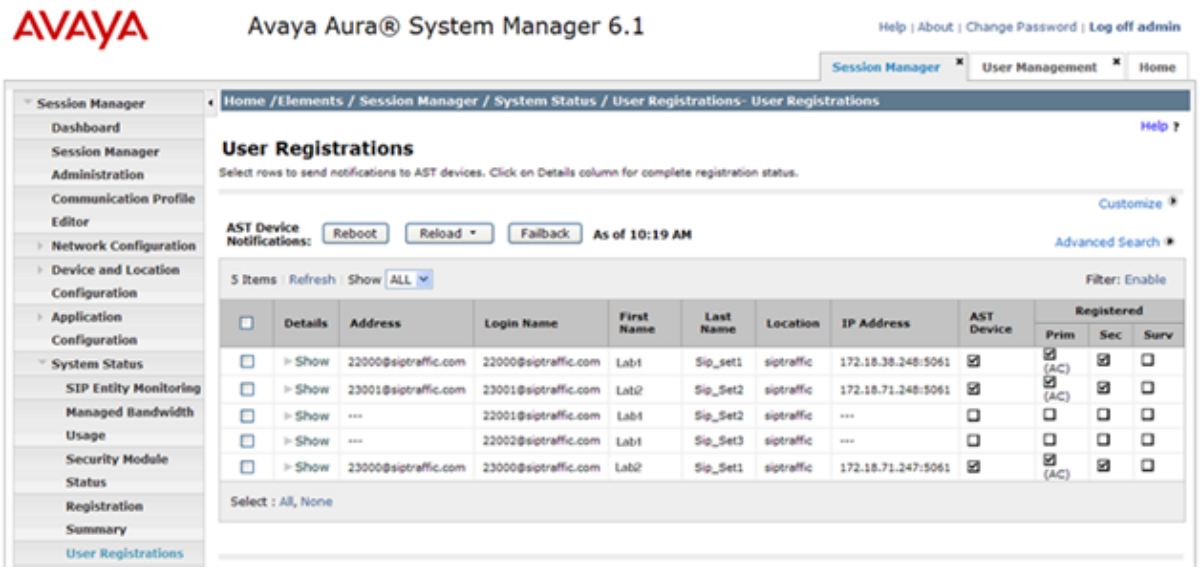


Figure 44: Example of verifying the user is registered with a Session Manager

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.

Note:

Avaya Aura® Contact Center supports Communication Manager stations (phones) with a maximum of 2 Call Appearance lines per agent station. New Communication Manager stations are automatically created with 3 Call Appearance lines, so if a station is to be used

by an Avaya Aura® Contact Center agent, you must configure the new station to have a maximum of 2 Call Appearance lines.

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 2 Call Appearance lines.

   If the station has 3 Call Appearance lines, you can use the Endpoint Editor in Avaya Aura® System Manager to remove one of the Call Appearance lines.

Procedure job aid

```
display station 22000                                    Page   1 of   6
                                    STATION

Extension: 22000                      Lock Messages? n                BCC: 0
     Type: 9640SIP                    Security Code: 12345678          TN: 1
     Port: S00026                   Coverage Path 1:                  COR: 1
     Name: Lab1 Sip_set1            Coverage Path 2:                  COS: 1
                                    Hunt-to Station:
STATION OPTIONS
                                        Time of Day Lock Table:
             Loss Group: 19
                                              Message Lamp Ext: 22000

        Display Language: english               Button Modules: 0

          Survivable COR: internal
   Survivable Trunk Dest? y                       IP SoftPhone? n

                                                  IP Video? n
```

Figure 45: Example of verifying the user station on the Communication Manager

Chapter 17: 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 18: 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 displays default data (when the station is configured to do so) as follows:

- When Contact Center routes a call to an agent, the UUI data contains the skillset name.
- 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.
- When an agent uses the Emergency feature, the UUI data for the supervisor contains "EMERGENCY" followed by the agent's first name and last name.
- When an agent makes a consult call (conference) from a voice contact, the UUI data for the consulted agent contains "CONSULT" followed by the skillset name.

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 may 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.

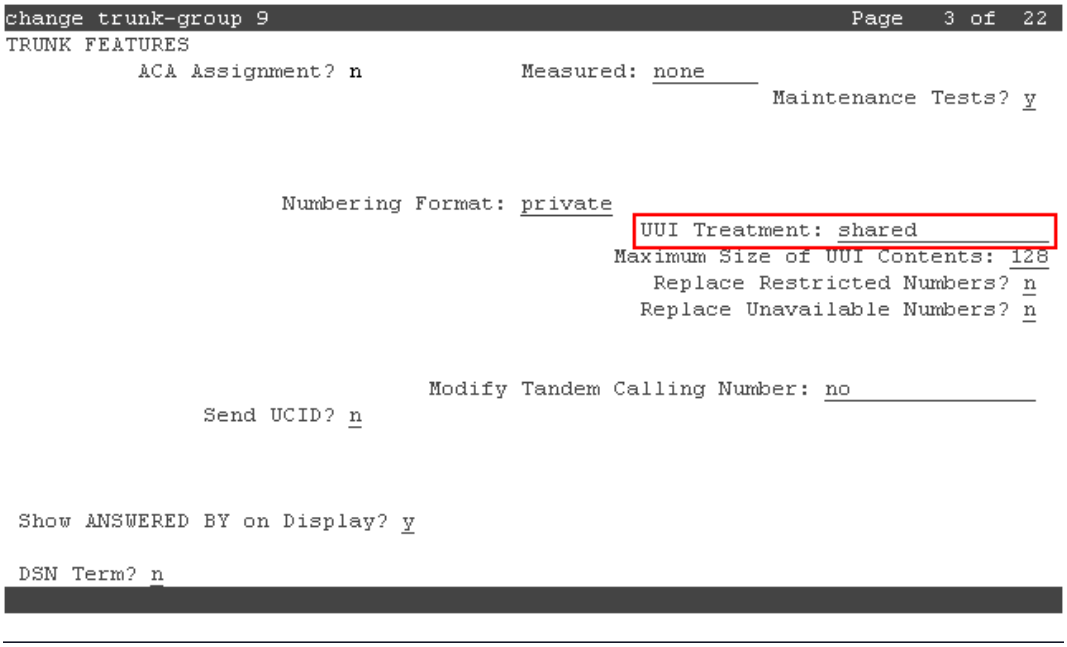
Modifying the SIP Trunk Group for UUI Data

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**.



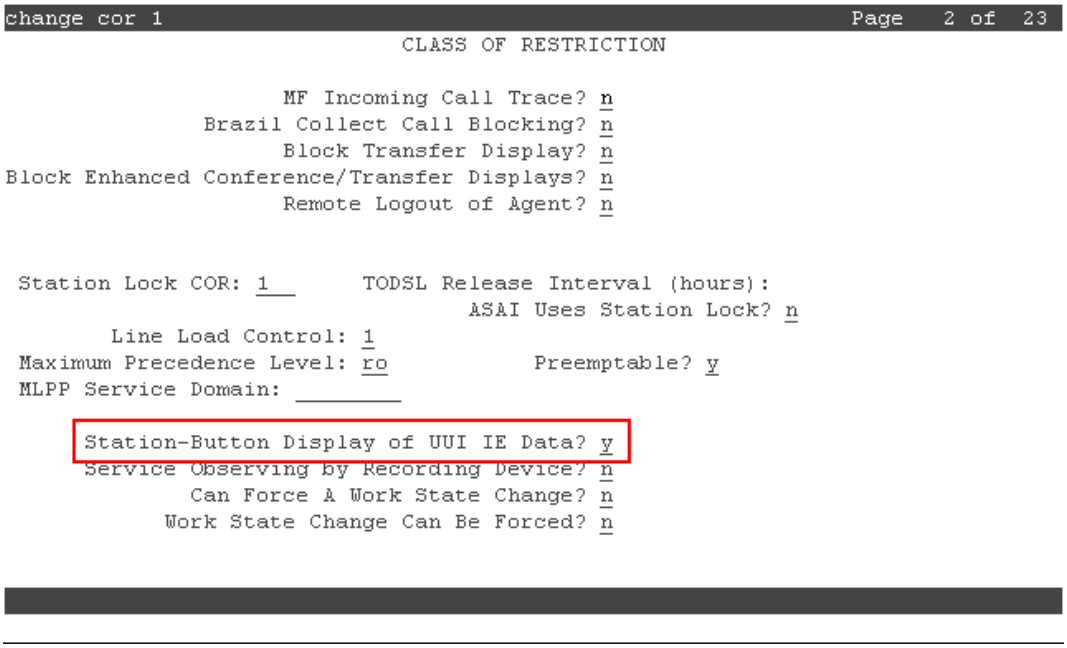
Changing Class Of Restriction Properties for UUI Data Display

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**.



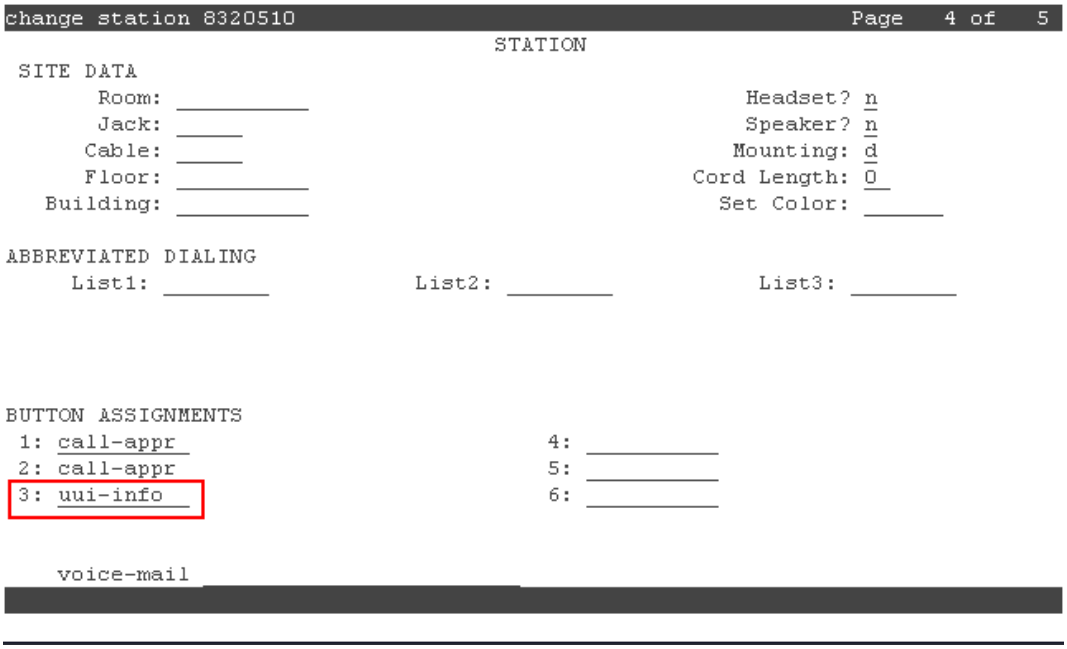
Creating a Button Assignment for UUI Data

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.



Chapter 19: 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 Planning and Engineering* (NN44400-210).
- Complete the Avaya Aura® Unified Communications platform pre-installation checklist. For more information about the checklist, see *Avaya Aura® Contact Center Installation Checklist* (NN44400-310).
- Complete the SIP-enabled Contact Center pre-installation checklist. For more information, see *Avaya Aura® Contact Center Installation Checklist* (NN44400-310).
- Ensure that you have installed Contact Center correctly. For more information about installing Contact Center, see *Avaya Aura® Contact Center Installation* (NN44400-311).

Navigation

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 Avaya Aura® Contact Center, ensure at least one agent is logged on to the skillset associated with the test CDN (Route Point).
- Ensure the agent's Avaya Aura® Agent Desktop client is Ready to handle voice calls.

About this task

This section introduces some of the Avaya Aura® 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 Avaya Aura® Contact Center.

In the following worked example, a Communication Manager extension (43001) dials an Avaya Aura® Contact Center CDN (Route Point) 53000. Avaya Aura® Contact Center then routes the call to an agent. The contact center agent is using Communication Manager extension (43000).

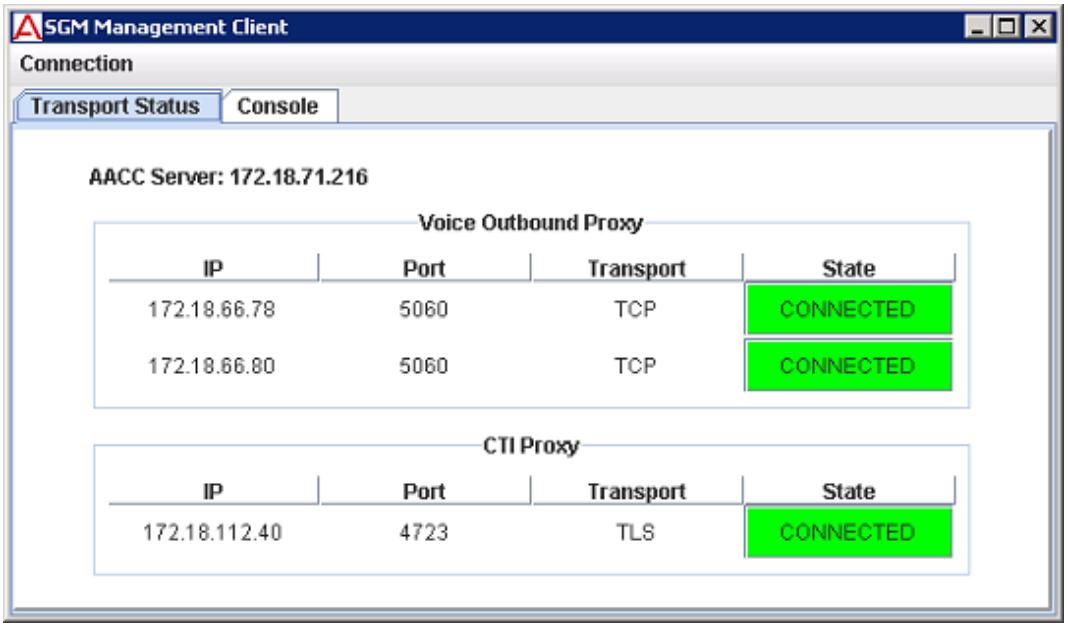
The following table shows the details of the components used in this worked example:

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

Component	Value
Communication Manager SIP Entity name	CommunicationManager One
Avaya Media Server (Avaya MS)	172.18.71.219

Procedure

1. On the Avaya Aura® Contact Center server, click **Start** > **All Programs** > **Avaya** > **Manager Server** > **SGM Management Client**.
2. Click **Connect**.
3. Confirm that Avaya Aura® 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 Avaya Aura® 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 Avaya Aura® Contact Center 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.

4. Log on to the Communication Manager System Access Terminal (SAT) interface.
5. 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
```

6. Log on to the Session Manager management console.

7. 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
```

8. After the traceSM utility starts, press **f**, to define a trace filter.
9. To define a traceSM filter for the Communication Manager extension 43001, enter, `-u 43001`

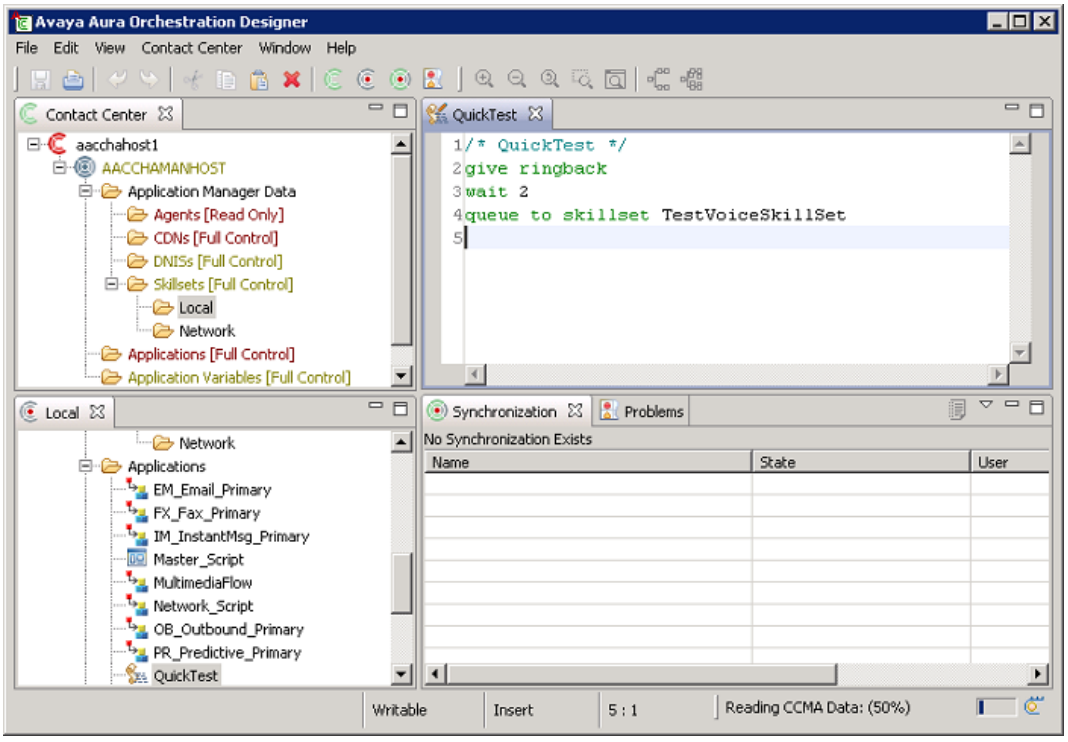
```
/------------------------------------------------------------------------\
|Filter Usage:                                                           |
|  -u <URI|NUMBER>  Filter calls that contain <URI|NUMBER> in            |
|                   the 'From' or 'To' field.                            |
|  -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                                                    |
\------------------------------------------------------------------------/
```

10. 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.

11. Using the Communication Manager desk phone (extension 43001), dial the Avaya Aura® 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 Avaya Aura® Contact Center.
12. If the calls is offered on the agent Avaya Aura® Agent Desktop client, accept or answer the call.
    If the call from the Communication Manager extension to the Avaya Aura® 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.
13. If the call from the Communication Manager extension does get to Avaya Aura® Contact Center, but is not offered to an agent, your Contact Center Orchestration Designer flow may need 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 Avaya Aura® 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 Media Server (172.18.71.219) associated with Avaya Aura® 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 MS (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 Avaya Aura® 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 Avaya Aura® 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 stations (phones)

About this task

To ensure proper integration and Contact Center control, Avaya Aura® Communication Manager stations (phones) must be configured as follows:

- A maximum of 2 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 233.
- Priority call feature is not support 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 phone.

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.

   Two 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 treatments when dialing the Contact Center Route Point Address

About this task

Add the Contact Center Manager Server to the list of trusted hosts on the Avaya Aura® SIP Enablement Services (SES) server. Add a Contact Center Manager Server (CCMS) routing entry to the SES server. This indicates to SES which host (SIP endpoint) to send calls to, based on the dialed number. Add contact details for the CCMS routing entry. This configures the SES server to send calls to the CCMS when the calls match the map.

If you dial the Contact Center Route Point Address (RPA) and do not receive any treatments, perform the following checks.

Procedure

1. Verify that the Contact Center Manager Server is a trusted host of the SIP Enablement Services (SES) server.

   For more information, see Adding Contact Center Manager Server as a SES trusted host on page 74.

2. Verify that the SIP Enablement Services (SES) server has a routing entry to the Contact Center Manager Server.

   For more information, see Adding a routing entry for the Contact Center Manager Server on page 75.

3. Verify that the SIP Enablement Services (SES) server has contact details for the Contact Center Manager Server routing entry.

   For more information, see Adding a contact for the Contact Center Manager Server pattern on page 76.

Troubleshooting routing calls from Contact Center to agents on Communication Manager

About this task

If you cannot route calls from the Contact Center to agents on the Communication Manager, perform the following checks.

On the SIP Enablement Services (SES) server, add a route entry to the Communication Manager. The SES re-directs SIP contacts that match the route entry pattern to the Communication Manager.

Add the Contact Center Manager Server to the list of trusted hosts on the SIP Enablement Services (SES) server. SES does not authenticate SIP requests from trusted hosts.

Procedure

1. Verify that there is a routing entry from the SES to the Communication Manager.

   For more information, see Adding a route entry to the Communication Manager on page 72.
2. Verify that the Contact Center Manager Server is a trusted host of the SIP Enablement Services (SES) server.

   For more information, see Adding Contact Center Manager Server as a SES trusted host on page 74.

Troubleshooting when agents cannot log on to Agent Desktop

About this task

If agents cannot log on to Avaya Aura® 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 125.
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 133.
3. Verify that you imported certificates into the AES server.

   For more information see Importing a signed certificate into AES on page 137.
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 138.
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

C

D

E

F

G

H

T

U

V