Using Avaya 96X1 SIP Agent Deskphones with Avaya Aura® Call Center Elite

Release 6.3.6
Issue 1
June 2014

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 may generally make available to users of its products and Hosted Services. 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 Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

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

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

License 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 or an Instance of the Software.

Copyright

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

Virtualization

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

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. 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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

The document describes the prerequisites for setting up the 96X1 SIP agent deskphones with Avaya Aura® Call Center Elite.

Intended audience

This document is intended for implementation engineers and system administrators.

Related resources

Documentation

See the following related documents.

Table 1: Avaya Aura® Session Manager documents

Title	Use this document to:	Audience
Deploying Avaya Aura® Session Manager on Avaya Aura® System Platform	Deploy Session Manager.	Implementation engineers and system administrators
Maintaining and troubleshooting Avaya Aura® Session Manager	Resolve basic problems and maintain the system.	All users

Table 2: Call Center Elite documents

Title	Use this document to:	Audience
Administering Avaya Aura® Call Center Elite	Administer Call Center Elite features.	Implementation engineers and system administrators
Avaya Aura® Call Center Elite Overview and Specification	Know about Call Center Elite features, performance	Implementation engineers, sales engineers, and solution engineers

Title	Use this document to:	Audience
	specifications, security, and licensing information.	
Avaya Aura® Call Center Elite Feature Reference	Know about Automatic Call Distribution (ACD) and Call Vectoring features.	All users

Table 3: Communication Manager documents

Title	Use this document to:	Audience
Administering Avaya Aura® Communication Manager	Administer Communication Manager.	Implementation engineers and system administrators
Avaya Aura® Communication Manager Denial Events	Resolve basic problems and maintain the system.	All users

Table 4: SIP Agent Deskphones documents

Title	Use this document to:	Audience
96X1 SIP Setting File Parameters SIP 6.2 or later	Administer 96X1 SIP agent deskphones.	Implementation engineers and system administrators
Avaya Deskphone SIP 9600 Series IP deskphones - API Guide	Develop APIs.	API developers
Avaya 9608/9608G/9611G IP Deskphones SIP Quick Reference	Read about the 9608 and 9611G SIP agent deskphones.	All users
Avaya Deskphone SIP for 9621G/9641G Quick Reference	Read about the 9621G and 9641G SIP agent deskphones.	All users
Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP	Install, configure, administer, and maintain 96X1 SIP agent deskphones.	Implementation engineers and system administrators
Using Avaya 9608/9608G/9611G IP Deskphones SIP for Call Center Agents	Use the 9608 and 9611G SIP agent deskphones in a call center environment.	All users
Using Avaya 9621G/9641G IP Deskphones SIP for Call Center Agents	Use the 9821G and 9641G SIP agent deskphones in a call center environment.	All users
Using Avaya 9608/9608G/9611G IP Deskphones SIP	Use the 9608 and 9611G SIP agent deskphones.	All users
Using Avaya 9621G/9641G IP Deskphones SIP	Use the 9621G and 9641G SIP agent deskphones.	All users

Table 5: Other related documents

Title	Use this document to:	Audience
Deploying Avaya Aura® System Manager on System Platform	Deploy Avaya Aura® System Manager.	Implementation engineers and system administrators
Implementing End-to-End SIP	Configure SIP endpoints.	Implementation engineers and system administrators

Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and check the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, 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.

  Note:

  Videos are not available for all products.

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 2: Implementation checklist

Use the following checklist to ensure that you have set up all components for use with the 96X1 SIP agent deskphones.

#	Task	Description	✔
1	Install System Manager	For information about installing System Manager, see *Deploying Avaya Aura® System Manager on System Platform*.	
2	Install Session Manager	For information about installing Session Manager, see *Deploying Avaya Aura® Session Manager on Avaya Aura® System Platform*.	
3	Create an enrollment password for trust management	For information about enrolling passwords, see *Deploying Avaya Aura® Session Manager on Avaya Aura® System Platform*.	
4	Administer Session Manager	For information about administering Session Manager, see *Deploying Avaya Aura® Session Manager on Avaya Aura® System Platform*.	
5	Install Communication Manager	For information about installing Communication Manager, see *Deploying Avaya Aura® Communication Manager on System Platform*.	
6	Install the Communication Manager templates	For Communication Manager at the core, download CM_Duplex.ovf file from Product Licensing and Delivery System (PLDS). For remote Communication Manager, download the CM_SurvRemote.ovf file. For information about installing the Communication Manager templates, see *Deploying Avaya Aura® Communication Manager on System Platform*.	
7	Use the Communication Manager System Management Interface (SMI) to complete the configuration tasks	For information about configuring Communication Manager, see *Deploying Avaya Aura® Communication Manager on System Platform*.	

#	Task	Description	✔
8	Configure Communication Manager as an Evolution Server	For information about configuring Communication Manager as an Evolution Server, see *Administering Avaya Aura® Communication Manager*.	
9	Administer Communication Manager	For information about the SAT administration commands, see *Administering Avaya Aura® Communication Manager Server Options*.	
10	Synchronize Communication Manager data	For information about synchronizing the Communication Manager data with the System Manager database, see *Administering Avaya Aura® Communication Manager Server Options*.	
11	Add users and stations	For information about adding users, see *Administering Avaya Aura® Communication Manager Server Options*.	
12	Install the 96X1 SIP agent deskphones	For information about installing SIP phones, see *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*.	
13	Gain access to CRAFT procedures	For information about accessing local procedures, see *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*.	
14	Configure SIP settings	For information about configuring the SIP settings, see *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*.	
15	Configure the time server settings	For information about configuring time server settings, see *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*.	
16	Set the Site-Specific Option Number (SSON)	For information about setting SSON, see *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*.	
17	Administer the 96X1 SIP agent deskphone options	For information about administering the options, see *Administering Avaya Deskphone SIP for 9601/9608/9611G/9621G/9641G*.	
18	Administer the 96X1 SIP agent deskphones for survivability	For information about system failover and survivability, see *Administering Avaya Deskphone SIP for 9601/9608/9611G/9621G/9641G*.	

Chapter 3: Administering Communication Manager

Before you begin

Communication Manager must connect with Session Manager in a non-IP Multimedia Subsystem (IMS) signaling group for Call Center functionality.

Ensure that the field option in the **IMS Enabled** field on the SIP Signaling Group screen is **n** to prevent *Feature Invocation Failure* when an agent logs in to the system.

Verify the field settings and values in the following fields on the System-Parameters Customer-Options screen:

- **ISDN-PRI**
- **IP Trunk**
- **Expert Agent Selection (EAS)**
- **Maximum Administered SIP Trunks**
- **Maximum Off-PBX Telephones-OPS**

Ensure that the field option in the **DID/Tie/ISDN/SIP Intercept Treatment** field is **attd** and the **Trunk-to-Trunk Transfer** field is **restricted**.

About this task

You can use SIP agents when you administer Communication Manager as an evolution server.

As an evolution server, Communication Manager uses the full-call model. In the full-call model, call processing is a single step procedure, that is, Communication Manager processes the origination and termination parts of the call without a break.

For information about IMS signaling flow and full-call model, see *Implementing End-to-End SIP*.

Procedure

1. Change the dialplan analysis.
2. Change the Feature Access Codes (FAC) for Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS).
3. Add a SIP domain in each network region, and administer an IP node name for the IP address of the Session Manager Security Module.
4. Add a SIP signaling group for each Session Manager Security Module. For message interchange between Communication Manager and the SIP server, select **y** in the **Peer Detection Enabled** field on the Signaling Group screen.

5. Add a trunk group of type **SIP** for call routing from Communication Manager to Session Manager.
6. Administer the route pattern, and add the route pattern number as a proxy route.
7. Administer private numbering plan.
8. Administer the uniform dial plan.
9. Administer AAR and ARS.
10. Save translations.

Communication Manager templates

Communication Manager (CM) runs on System Platform as a virtualized version called a solution template, which includes all the features supported by Communication Manager.

Avaya offers the following Communication Manager templates:

- Communication ManagerMain/Core
  - Duplex CM Main or Survivable Core
  - Simplex CM Main or Survivable Core
  - Embedded CM Main
- Communication Manager Survivable Remote
  - Simplex CM Survivable Remote
  - Embedded Survivable Remote

Note:

You must install System Platform on Avaya servers before installing the solution template.

For the simplex and duplex templates, use the HP ProLiant DL360 G7 or Dell™ PowerEdge™ R610 servers. For the embedded templates, use the Avaya S8300D server.

Administration tips

Note:

For more information about SIP configuration and related administration, see *Implementing End-to-End SIP*.

- Use System Manager to administer Communication Manager features to ensure that Communication Manager synchronizes translation files with the System Manager database.
- Ensure that the field option in the **Expert Agent Selection (EAS) Enabled** field on the Feature-Related System Parameters screen is **y**.

- Administer the **SIP Endpoint Managed Transfer** field on the Feature-Related System Parameters screen as **n**. You must select **n** to prevent unexpected events, such as inaccurate reporting or loss of User-to-User Information (UUI).
- Communication Manager provides the SIP Agent functionality only with the Evolution Server configuration and not with the Feature Server configuration. Therefore, you must administer the **IMS Enabled** field as **n** for all SIP signaling groups. If the field option is **y**, Communication Manager sends a `Feature Invocation Failure` error message when an agent attempts to log in to the system.
- Add a domain on each IP Network Region screen for all 96X1 SIP agent deskphones within a network region. Ensure that the **authoritative domain** field on the IP Network Region screen is equal to the SIP domain. If the domain entry is blank, SIP agent deskphones register with Session Manager but do not display agent buttons, such as **auto-in**, **manual-in**, **aux**, or **acw**.
- SIP agent deskphones must have dedicated SIP trunk groups for:
  - Call traffic with service providers and other Communication Manager servers.
  - Call signaling with Session Manager.

  Furthermore, Call Management System (CMS) or Avaya IQ must not measure Off-PBX Station (OPS) SIP trunk groups that carry signaling data because signaling data is inconsistent with the format of call traffic data. Sharing of SIP trunk groups and measuring of signaling data can lead to loss of call traffic data and reporting errors.

  To prevent data loss and reporting errors, Communication Manager, starting with this release, does not send station signaling-related messages to CMS or Avaya IQ. Furthermore, if CMS or Avaya IQ measure OPS SIP trunk groups, Communication Manager logs a `SIP OPTIM TG Meas Error` denial event 5073.

  Use private settings to ensure that SIP trunks for Off-PBX Telephone Integration and Mobility (OPTIM) OPS signaling are from dedicated SIP trunk groups. To prevent agent extension manipulation, administer the trunk group as **private** and the number format on the route pattern as **unk-unk**.

  - Add SIP trunk numbers on the Private Numbering and the Public Unknown Numbering screens.
  - Do not add extra digits to station extensions and agent extensions on the Private Numbering or the Public Unknown Numbering screens. The extra digits can cause Session Manager to send calls to Communication Manager for further processing without terminating calls to SIP agent deskphones. If private unknown numbering modifies agent extensions, agents can log out and then log in to the system. However, agents cannot use feature buttons to change work modes.
  - Ensure that Session Manager has two entities for Communication Manager: One for inbound call traffic and the other for agent deskphone traffic. All SIP trunks must be on the Processor Ethernet (PE) interface.
  - Administer different listen port numbers for inbound trunks and SIP agent deskphone signaling trunks. Ensure that each function has dedicated trunk groups. For more information, see *Administering the Signaling Group screen*.
  - The Session Manager Profile configuration for SIP agent deskphones must point to the Communication Manager entity that you define for OPS trunk (station) signaling in the **Origination Application Sequence** field and the **Termination Application Sequence** field. For more information, see *Administering the Signaling Group screen*. Without this

administration, Session Manager cannot use relevant signaling trunks for call delivery to SIP agent deskphones. This administration is important for a configuration where you use the same Communication Manager entity for all traffic, but now you want to separate the entity into dedicated inbound call traffic and OPS signaling data.

  - Administer sequenced applications for users based on whether the user is on the originating or on the terminating side of a call. When you design the sequence for applications that act on deskphones that Communication Manager Evolution Server controls, you must ensure that Communication Manager is the last application that you define on the origination side of a call and the first application on the termination side of the call. This sequence is critical because the evolution server uses the full-call model for call processing, and all origination and termination feature processing occurs on the origination side of the call.

    For more information, see *Implementing End-to-End SIP*.

  - For dedicated SIP trunk groups for deskphone signaling with Session Manager, administer the **Measured** field on the Trunk Group screen as **none**. This administration prevents CMS or Avaya IQ reporting issues, including loss of reporting.

- Use the phone number as the primary handle when you administer Session Manager. Do not use alphabets.
- Ensure that the phone type on the Station screen is one of the 96X1SIPCC types, and assign an **agnt-login** button on the Station screen for each SIP agent deskphone.
- The following are some guidelines for Secure Real-time Transport Protocol (SRTP):

  Use the Transport Layer Security (TLS) protocol for signaling between Session Manager and SIP agent deskphones and between Communication Manager and Session Manager. Connection to Avaya Aura® Presence Services requires TLS.

  However, if you must use Transmission Control Protocol (TCP), ensure that you add the following parameters in the SIP settings file:

  - Administer ENABLE_OOD_MSG_TLS_ONLY as 0. If you administer ENABLE_OOD_MSG_TLS_ONLY as `1`, third-party call control Computer Telephony Integration (CTI) applications and Supervisor Assist do not work.
  - Administer the configuration parameter ENABLE_PPM_SOURCED_SIPPROXYSRVR as `0`. If the parameter is not `0`, the proxy server information from Personal Profile Manager (PPM) overwrites the information in the settings file.

  For more information, see *Implementing End-to-End SIP*.

- Configure the Simple Network Time Protocol (SNTP) server for SIP agent deskphones because Communication Manager checks the time on the certificate to validate the certificate.
- Administer media encryption parameters with the same cryptosuites on Communication Manager and SIP agent deskphones. The default cryptosuite is **aescm128–hmac80**.
- Administer **none** on the IP Codec Set screen for no encryption. The default setting is **9** that corresponds to the setting on the Communication Manager administration screen.
- Do not configure SIP agent deskphones with EC500 buttons because Communication Manager as an evolution server does not support EC500.

Related Links

Administering the Signaling Group screen on page 15

Configuring IP node names and addresses

About this task

If you do not configure IP node names, System Manager ignores the IP interfaces, which can result in unsuccessful IP synchronization of Communication Manager.

Perform the following procedure for each Survivable Core server, Survivable Remote server, and adjunct.

Procedure

1. At the command prompt, type `change node-names ip`. Press **Enter**.
2. In the **Name** field on the IP Node Names screen, type node names.
3. In the **IP Address** field, type the IP address.
4. Press **Enter** to save the changes.

Administering the IP Network Region screen

Procedure

1. At the command prompt, type `change ip-network-region xxx`, where *xxx* is the number of the network region. Press **Enter**.
2. In the **Authoritative Domain** field, select **SIP**.
3. In the **Allow SIP URI Conversion** field, select **y**.
4. In the **Intra-region IP-IP Direct Audio** field, select **y**.
5. Administer the Real-time Transport Control Protocol (RTCP) monitor server parameters.
6. Press **Enter** to save the changes.

Administering the Feature-Related System-Parameters screen

Procedure

1. At the command prompt, type `change system-parameters features` and press **Enter**.
2. In the **Expert Agent Selection (EAS) Enabled** field, select **y**.
3. In the **SIP Endpoint Managed Transfer** field on the Feature-Related System-Parameters screen, select **n**.
4. Administer the other fields that are relevant to the configuration in your organization.

5. Press **Enter** to save the changes.

Administering Call Center Elite features

The following are the primary screens for administering the Call Center Elite features:

- System-Parameters Customer-Options
- Feature-Related System Parameters

For information about administering all Call Center Elite features, see *Administering Avaya Aura® Call Center Elite*.

Administering the Signaling Group screen

Procedure

1. In the **Group Type** field, select **SIP**.
2. In the **IMS Enabled** field, select **n**.
3. In the **Transport Method** field, select **tls**.
4. Administer **Near-end Listen Port** and **Far-end Listen Port**. You must administer separate SIP entities on Session Manager that map to different signaling groups in Communication Manager to configure dedicated trunking for inbound trunks and for OPS station signaling trunks. Session Manager must have two entities for Communication Manager: One for inbound traffic and the other for agent phone traffic. For example, use the following settings for the Transport Layer Security (TLS) protocol.

Communication Manager side settings	Session Manager side settings
Station signaling	*SIP entities*
Signaling-group 1: Set **Near-end Listen Port** to `5062` and **Far-end Listen Port** to `5062`	CM1OPS, CMTRNK1, and SM1. Both the CM1xx entities must point to the same Communication Manager Fully Qualified Domain Name (FQDN)
Inbound trunk signaling	*Entity links*
Signaling-group 2: Set **Near-end Listen Port** to `5061` and **Far-end Listen Port** to `5061`	• Entity Link 1: SM1 port 5062 to CM1OPS port 5062 • Entity Link 2: SM1 port 5061 to CM1TRNK port 5061

For TCP, use port 5060 instead of 5061.

Note:

With the sample configuration, signaling-group 1 and entity link 1 are logically paired-up to handle SIP OPS station signaling, and signaling-group 2 and entity link 2 are logically paired-up to handle inbound call signaling. However, you must administer appropriate routing in Session Manager, as well as in Communication Manager, to ensure that the appropriate traffic is routed over the appropriate signaling facilities. You can add additional signaling groups on Communication Manager by using the same entity links defined in Session Manager, as indicated in the table, as more OPS signaling trunks and more inbound signaling trunks might be required in Communication Manager to handle the required call traffic load and the required number of SIP agent deskphones.

5. In the **DTMF over IP** field, select **rtp-payload**.
6. In the **Session Establishment Timer** field, enter `3`, which is the recommended time period for call center use.
7. In the **Far-end Network Region** field, assign a number from `1` to `250` that represents the region of Session Manager.
8. In the **Far-end Domain** field, assign the IP address of the SIP domain.
9. In the **Initial IP-IP Direct Media** field, select **n**. This field option is necessary to prevent unexpected interactions with the Call Center Elite features as some features depend on the media that Communication Manager handles during the first few seconds.
10. In the **Direct IP-IP Audio Connections** field, select **y**.

Administering the Trunk Group screen

The following procedure and settings refer to the trunk groups that are used only for SIP signaling to the SIP agent deskphones. For more information, see Administration tips on page 11.

Procedure

1. In the **Group Type** field, select **SIP**.
2. In the **Signaling Group** field, assign the number of the signaling group defined on the Signaling Group screen.
3. In the **Number of Members** field, assign the number of 96X1 SIP phones that the trunk must support. Communication Manager automatically assigns the IP port numbers.
4. In the **Redirect on OPTIM Failure (ROOF)** field, enter `5000` (5 seconds).
5. In the **Preferred Minimum Session Refresh Interval (sec)** field, assign a value from `90` to `64800`. The default setting is `600`. To prevent spikes in the processor occupancy, assign a value that is greater than the sum of the average call handling time and the average call queuing time. For example, if the average call queuing time is 3 minutes and the average call handling time is 10 minutes, assign a field value that is greater than 780 seconds.

Note:

Although Communication Manager uses the configured value for *outbound* calls when the traffic is relatively low, during peak traffic conditions Communication Manager increases the session refresh interval value dynamically for protection against the processor occupancy spikes.

If the service provider network for SIP uses a session refresh interval value that is higher than the configured value for **Preferred Minimum Session Refresh Interval** but relatively low compared to the amount of SIP traffic that Communication Manager currently handles, Communication Manager rejects the calls with a *4xx* response and includes the suggested session refresh interval value for call attempt. Therefore, large call centers must ensure that the service provider network uses a session refresh interval value that is greater than 1800 seconds within the INVITE message to ensure that Communication Manager accepts calls in the first attempt, regardless of the SIP call traffic load that Communication Manager might be handling.

6. In the **Measured** field, select **none** for the signaling trunks to Session Manager.
7. In the **Numbering Format** field, select **private**, which is the default for SIP.
8. In the **Show ANSWERED BY on Display** field, select **y**.
9. In the **Support Request History** field on the Protocol Variations page, select **y**. If the field setting is **n**, the SIP agent deskphone displays do not function correctly.

Administering call routing

Procedure

1. On the Locations screen, assign a proxy selection route pattern for locations that use Session Manager.
2. On the IP Network Map screen, assign a calling party number for relaying to Public Safety Answering Points (PSAPs) for 911 calls. Define the **From** and **To** IP addresses on the IP Address Mapping screen to relay the correct emergency number.
3. On the Incoming Call Handling Treatment screen, define call handling for Session Manager trunk groups.

Administering the Numbering-Private Format screen

Private numbering plans ensure unique numbers for call routing. To administer the numbering plan, use the `change private-numbering x` command, where x is the extension length.

Administering the Station screen

Procedure

1. At the command prompt, type `change station xxx`, where xxx is the extension number. Press **Enter**.
2. In the **Type** field on the Station screen, select a 96X1SIPCC station type, that is, **9608SIPCC**, **9611SIPCC**, **9621SIPCC**, or **9641SIPCC**.
3. Assign a coverage path for each 96X1 SIP agent deskphone.
4. Administer the **auto-answer** field on the Station or Agent LoginID screen.

   The field option on the Agent LoginID screen overrides the option on the Station screen.
5. In the **Restrict Last Appearance** field, select **y**.
6. Assign an **agnt-login** button on the Station screen in addition to the agent work buttons.
7. Administer the SIP feature options on page 6 of the Station screen. If you use an Application Enablement Services (AES)-based application to control the agent deskphone, administer the **Type of 3PCC Enabled** field as **Avaya**. AES-based applications do not work if you do not administer this field.
8. Press **Enter** to save the changes.

Administering the Off-PBX-Telephone Station-Mapping screen

About this task

The following procedure is optional. Administer the screen to change the default values.

Procedure

1. At the command prompt, type `change off-pbx-telephone station-mapping xxx`, where *xxx* is the extension number. Press **Enter**.
2. In the **Application** field, select **OPS**.
3. In the **Mapping Mode** field, select **both**.
4. In the **Calls Allowed** field, select **all**.
5. In the **Bridged Calls** field, select **none**.
6. Press **Enter** to save the changes.

Synchronizing Communication Manager and System Manager data

Procedure

1. Click **Elements** > **Inventory** > **Synchronization** > **Communication System**.
2. On the Synchronize CM Data and Configure Options screen, expand the **Synchronize CM Data/Launch Element Cut Through** table and the click the check box of the desired Communication Manager Evolution Server.
3. Select **Save Translations for selected devices** and click **Now** to start the synchronization.
4. Refresh the Web page, and verify that the Sync Status column of the desired Communication Manager Evolution Server shows *Completed*.

Adding users and stations

About this task

For each SIP user that you define in Session Manager, you must add a corresponding station in Communication Manager. After administering a user, perform the following steps to automatically generate a corresponding SIP station.

Procedure

1. Click **Elements** > **Inventory** > **Synchronization** > **Communication System**.
2. On the Synchronize CM Data and Configure Options screen, click **Launch Element Cut Through**.

   If you log on to System Manager as an administrator, you do not require separate login credentials to gain access to the Element Cut Through screen. If you are a custom user, you must have the login credentials to gain access to the Element Cut Through screen.
3. On the Element Cut Through screen, enter the **`add station`** command.

   Note:

   If you administer stations directly on Communication Manager, you must administer a user communication profile for each extension.

Chapter 4: Avaya 96X1 SIP agent deskphones

9608, 9611G, 9621G, and 9641G are part of the multiline 9600 Series IP Deskphones. The deskphones are signaling protocol independent with two telephony applications, Avaya Deskphone H.323 and Avaya Deskphone SIP, that support H.323 and SIP respectively.

9621G and 9641G are touch-based deskphones with a color display. 9611G and 9608 are button-based deskphones. 9611G has a color display while 9608 has a monochrome display. With the 9641G, 9608, and 9611G models, you can use a dual headset adapter so that two persons can listen to calls. You can also attach more than one Button Module (BM) to these deskphone models to extend call appearances, bridge appearances, or feature keys. For an agent, the deskphones offer convenient features and capabilities, including a phone screen to view and manage calls, and icons that indicate agent status, call state, feature status, queued calls, and missed calls.

Differences between 96X1 SIP and 96X1 H.323 deskphones

96X1 H.323	96X1 SIP
Communication Manager connection	
H.323 deskphone connections are made on the *line* side of Communication Manager.	SIP deskphone connections are made on the *trunk* side of Communication Manager.
Server requirement	
H.323 deskphones register with Communication Manager.	SIP deskphones register with Session Manager.
Backup and restore	
H.323 deskphones use HTTP to store backup files.	SIP deskphones use Personal Profile Manager (PPM) to store backup files.
Settings file and system parameters	
The settings file is the same for the both types of deskphones, but some system parameters vary. In H.323 deskphones, the OPSTAT and APPSTAT parameters control each user interface function.	In SIP deskphones, parameters such as ENABLE_CONTACTS and ENABLE_CALL_LOG control each user interface function. In place of APPSTAT, there are parameters such as ENABLE_REDIAL, ENABLE_REDIAL_LIST, ENABLE_MODIFY_CONTACTS, ENABLE_CONTACTS and ENABLE_CALL_LOG. In

96X1 H.323	96X1 SIP
	place of OPSTAT, there are parameters such as PROVIDE_OPTIONS_SCREEN, PROVIDE_LOGOUT, and PROVIDE_NETWORKINFO_SCREEN.
Quality of Service (QoS)	
H.323 deskphones use Communication Manager to set QoS.	SIP deskphones use parameters, such as L2QUAD, L2QSIG, DSCPAUD, and DSCPSIG, to set QoS.
Language support	
• H.323 deskphones do not support Hebrew and Korean. • H.323 language files have a .txt file extension.	• SIP deskphones support text entry in Hebrew and Korean. • All SIP language files have a .xml file extension.

96X1 SIP agent deskphone feature support

The 96X1 SIP agent deskphones support the following call center features:

- Agent login and logout buttons instead of Feature Access Codes (FACs): The phone shifts the button for agent login to agent logout after the agent logs in.
- Display of active VDN.
- Auto and manual answer.
- Button for Stroke/Event Count from 0 to 9.
- Button for Call Work Codes (CWCs).
- Message Waiting Indicator (MWI) tracking for the EAS agent login ID.
- Buttons for third-party MWI.
- Manual-in and Auto-in work modes.
- Interruptible Auxiliary (AUX) work.
- Display of ASAI User-to-User (UUI) information.
- Buttons for AUX work and After Call Work (ACW).
- Release calls by using the **release** button, thereby maintaining login status.
- Entry of reason codes for change to the AUX work mode and for logout.
- Automatic display of collected digits with an incoming call that follows a call transfer.
- Correct messaging to the reporting adjuncts.
- Insertion of VDN of Origin Announcements (VOA) after answer with manual-answer operation or accompanying zip tone for auto-answer operation.
- Queue Status button: The **q-calls** button displays the number of calls in queue and the time the oldest call has been in queue.
- Visible and audible confirmation of feature activation and status change to the agent.

- Hold, mute, transfer, conference, message waiting, elapsed call timer, date and time display, exit, and a minimum of three call appearances.
- VuStats button.

Note:

Agent Greetings is unavailable with the 96x1 SIP deskphones. Phones that use the Avaya Deskphone H.323 application support this feature. Call Center features, such as login and logout, function differently in the 96X1 SIP deskphones because these features use the capabilities of the Avaya SIP architecture.

Agent login, logout, and work mode changes

The 96X1 SIP agent deskphones support the following basic call center features.

For more information about features and operations, see *Using Avaya Deskphone SIP for 9608/9611G for Call Center Agents* and *Using Avaya Deskphone SIP for 9621G /9641G for Call Center Agents*.

Agent login and logout

A single **login/logout** button is available for agent login and logout. Once an agent logs in, the button toggles to logout. The logged in agent can view the skills associated with the login ID. If the agent is on an ACD call and presses **logout**, the phone lamp lights to indicate a pending logout.

You can also administer a `requested` or `forced` logout reason code to request or compel an agent to enter a reason code.

Agent work mode change

The **auto-in** and **manual-in** feature buttons are available for agents to change the work mode. You can administer **auto-in** so that Communication Manager delivers calls to agents automatically. In the manual-in work mode, the agent must receive calls manually.

Agent state change to Auxiliary (AUX) Work

The **aux-work** feature button, if administered as `forced` or `requested`, is available with entry of an AUX Work reason code.

If an agent is on an ACD call and presses **aux-work**, Communication Manager accepts the request for change of agent work state and displays a pending indication on the phone display until the agent drops the call. Communication Manager then notifies the agent of the work state change.

Agent state change to After Call Work (ACW)

When an agent is on an ACD call and presses **acw**, Communication Manager accepts the request for change of agent work state and displays a pending indication on the phone display until the agent drops the call. Communication Manager then notifies the agent of the work state change.

Communication Manager invoked changes

Communication Manager notifies the deskphone of changes to the agent work state, agent login, or logout to account for situations such as the following:

- When an agent state automatically changes to ACW after releasing or disconnecting the call, Communication Manager notifies the SIP phone of an agent state change to the Manual-in work mode.
- When an agent in the Auto-in work mode disconnects an ACD call, Communication Manager notifies the SIP phone of an agent state change to Timed ACW.
- When Maximum Agent Occupancy (MAO) is less than the threshold, Communication Manager notifies the SIP phone of an agent state change from AUX work to Available. The SIP phone displays the reason code for the state change.
- When the administered forced logout from ACW or clock time for an agent is reached, Communication Manager plays a tone if the agent is on an ACD call. The agent can press **logout-ovr** to cancel the forced logout. If the agent does not press **logout-ovr**, a pending logout indication displays on the SIP phone and Communication Manager logs the agent out after the agent disconnects the ACD call.
- When you administer an agent AUX work mode as interruptible, Communication Manager notifies the SIP phone if the agent state changes from AUX work to Available.
- When agents in a particular skill or location are forced to logout or enter the AUX Work mode, Communication Manager notifies the SIP phone.

Personal Profile Manager

Personal Profile Manager (PPM) downloads the SIP phone-related data from the local Session Manager to the 96X1 SIP agent deskphones. When data changes in Communication Manager, Session Manager sends a `PUBLISH or NOTIFY` message to the 96X1 SIP agent deskphones. The deskphones then request PPM for the updated data.

PPM downloads the following call center feature buttons in addition to the other basic functions:

- **agnt-login**
- **aux-work**
- **after-call**
- **auto-in**
- **manual-in**
- **auto-msg-wt** with the extension number
- **stroke-cnt** code
- **call work code**
- **vu-display** with aux data for **Fmt**
- **q-calls** with aux data for **Grp**

- **uui-info**
- **logout-ovr**
- **assist**

After an agent logs in, the 96X1 SIP agent deskphones send a `SUBSCRIBE` message to PPM or SM to download agent characteristics through the Call Center Information (CC-Info) Event package. The package includes agent information (AgentInfo) and CC statistical information (CCStatsInfo).

Note:

PPM does not override the values that you set using the CRAFT menu on the phone. You must manually clear the values.

Scalability of 96X1 SIP agent deskphones

The Dell™ PowerEdge™ R610 and HP ProLiant DL360 G7 servers support up to 5000 concurrently logged-in SIP Expert Agent Selection (EAS) agents who use the 96X1 SIP agent deskphones.

Chapter 5: Troubleshooting

96X1 SIP agent deskphone troubleshooting

For information about troubleshooting the 96X1 SIP agent deskphones, see *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*.

Communication Manager troubleshooting

Use the following **`list trace`** commands to capture information on a specific station or trunk:

- **`list trace sip-station <extension number>`**
- **`list trace station <station number>`**
- **`list trace tac <tac number>`**

You can use the list trace commands to troubleshoot the following:

- Misdirected calls
- Call denials
- Trunking and routing problems
- DS1 connectivity to other vendor equipment

Communication Manager denial events

Note:

For more information about denial events, see *Avaya Aura® Communication Manager Denial Events*.

Event type	Event description	Explanation
1039	ACD login failed	Group Manager or User Manager set up of the ACD Logical Agent login information failed before password matching, if any.
1363	SIP Agent logins maximum	Maximum number of simultaneous SIP EAS Agents logins exceeded.
1375	Double agent login to station	Agent is logging in to a physical station that has another agent already logged in.

Event type	Event description	Explanation
1380	Agent login failure	Agent login failure in getting the number of digits in the Logical Agent password. The system cannot find the login ID or user ID or the ID is invalid.
1381	Agent login failure	Possible causes: • An agent who logs in to a Multiple Call Handling (MCH) split or adjunct-controlled split is already logged in to the system. • The **Expert Agent Selection (EAS)** field on the Feature-Related System-Parameters screen is **n**.
1382	Agent login invalid/ error	Login is invalid.
1383	Agent login failure/ error	Logical Agent failure in getting the agent login ID. Possible causes are as follows: • Error in initializing agent-stat table. • Login for the skill failed. • Logging in to skill that the agent has already logged in to before. • Maximum number of logged in skill reached.
1384	Agent logins maximum	Maximum number of simultaneous logins exceeded or agent login failed.
1385	Agent password digits failed	Failure in getting the Logical Agent password digits from the Dial Plan Manager.
1386	Agent password mismatch	Agent entered a password that does not match the administered password.
1387	Agent login invalid/ error	Login is invalid.
1388	Login acceptance fails	Logical Agent login processing of agent login messages failed.
2120	Advocate agents exceed maximum	Maximum number of Business Advocate agents already logged in.
2127	Over BCMS agent login cap	Reached maximum BCMS capacity.
5073	SIP OPTIM TG Meas Error	Trunk groups for SIP OPTIM OPS signaling are defined as measured and SPI events have been blocked.

Session Manager troubleshooting

Use SIP message tracing to troubleshoot Session Manager instances. The SIP Trace Viewer displays SIP message trace logs based on the configured filters.

For information about SIP tracing, see *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

Troubleshooting scenarios

Problem	Troubleshooting actions
You cannot register stations.	• Check that the Communication Manager signaling group and Session Manager media server have a consistent media type (TCP/ TLS). • Check that the Off-PBX-Telephone Station-Mapping screen has the correct trunk. • Check that the deskphone has the correct sip-server IP address.
The Phone is registered, but the feature buttons are not available or are not working.	• Ensure that you have added a domain to all the IP network regions associated with the 96X1 SIP agent deskphones. For more information, see Administration tips on page 11. • Restart PPM via service tomcat4 restart. If restarting does not resolve the issue, set Session Manager using stop -acfn; start -ac /var/log/sip-server/ppm.log.
An agent cannot log in.	• Look at the denial events using **`display events`** with type = denial. • Check that the deskphone is administered as a 96X1SIPCC station type on the Station screen. • On the Call Center pages of the System-Parameters Customer screen, verify that the **Logged-In SIP EAS Agents** field is greater than 0. • Check that the subscriptions are set up between Communication Manager and Session Manager. Use **`tcm`** and enter `rdd :sus Vmem`. Navigate to the next page. Verify that the cAgentStatusSub number equals the number of signaling groups going to a Session Manager. • Other errors might be existing agent errors, such as multiple agent login and incorrect login ID and password.
The 96X1 SIP agent deskphone does not support third-party call forwarding and send all calls.	Check that administration of third-party support for call forwarding and send all calls exists. When buttons are administered for **call forwarding all**, **call forwarding busy/does not answer**, or **send all calls**, leave the corresponding extension fields on the feature button assignments portion of the Station screen blank.
Multiple call appearances on an incoming call.	On page 2 of the Off-PBX-Telephone Station-Mapping screen, verify that the **Bridged Calls** field is set to **none**. The field must be set to `none` for any SIP station that has bridged to the station. For instance, consider three SIP stations in this scenario: • SIP station A is administered with three primary call appearances and one bridged appearance for SIP station B. • SIP station C is administered with three primary call appearances and two bridged appearances for SIP station A. Administer the **Bridged Calls** field for all phones to **none**.

AAR

When resources are unavailable, Communication Manager uses the Automatic Alternate Routing (AAR) feature to route calls to a different route than the first-choice route.

adjunct

A processor that does tasks for another processor and is optional in the configuration of the other processor. See also application on page 32.

AES

Application Enablement Services (AES) is an Avaya product that provides a platform for the development of CTI-based applications for Communication Manager 3.0 or later.

appearance

A software process that is associated with an extension and whose purpose is to supervise a call. An extension can have multiple appearances. Also called call appearance, line appearance, and occurrence.

application

An adjunct that requests and receives ASAI services or capabilities. Applications can reside on an adjunct. However, Communication Manager cannot distinguish among several applications residing on the same adjunct. Hence, Communication Manager treats the adjunct and all resident applications as a single application. The terms application and adjunct are used interchangeably throughout the document.

ARS

Automatic Route Selection (ARS) is a feature that Communication Manager uses to automatically select the least cost route to send a toll call.

ASAI

Adjunct-Switch Application Interface (ASAI) is an Avaya protocol that applications use to gain access to the call-processing capabilities of Communication Manager.

auto-in

A call-answering mode in which an agent automatically receives ACD calls without pressing any button to receive calls.

AUX work

Agents enter the Auxiliary (AUX) work mode for non-ACD activities, such as taking a break, going for lunch, or making an outgoing call. Agents in the AUX work mode are unavailable to receive ACD calls.

Avaya Aura®

A converged communications platform unifying media, modes, network, devices, applications. Avaya Aura® is based on the SIP architecture with Session Manager at the core.

bridged appearance

A call appearance on a telephone that matches a call appearance on another telephone for the duration of a call.

CMS

A software program for reporting and managing agents, splits, trunks, trunk groups, vectors, and VDNs. With Call Management System (CMS), you can also administer some ACD features.

CWC

Call Work Codes (CWCs) are up to 16–digit sequences that agents type to record the occurrence of customer-defined events, such as account codes or social security numbers.

EAS

A feature that Communication Manager uses to distribute calls based on agent skills. With Expert Agent Selection (EAS), you can ensure that callers connect to agents with the required skills.

IMS

IP Multimedia Subsystem (IMS) is an architectural framework for delivering IP multimedia services.

manual-in

A call-answering mode in which an agent must press **manual-in** to receive an ACD call.

MAO

Maximum Agent Occupancy (MAO) is a feature that Communication Manager uses to set thresholds on the amount of time that an agent spends on a call. The MAO threshold is a system-administered value that places an agent in the AUX work mode when the agent exceeds the MAO threshold for calls.

network region

A group of IP endpoints and Communication Manager IP interfaces that are interconnected by an IP network.

node

A network element that connects more than one link and routes voice or data from one link to another. Nodes are either tandem or terminal. Tandem nodes receive and pass signals. Terminal nodes originate a transmission path or terminate a transmission path. A node is also known as a switching system.

principal

A terminal that has the primary extension bridged on other terminals.

private network

A network used exclusively for the telecommunications needs of a particular customer.

public network

A network that can be openly accessed by all customers for local and long-distance calling.

SIP

Session Initiation Protocol (SIP) is an application-layer control signaling protocol for creating, modifying, and terminating sessions with more than one participant using http like text messages.

trunk

A dedicated telecommunications channel between two communications systems or Central Offices (COs).

trunk allocation

The manner in which trunks are selected to form wideband channels.

work mode

A function that an agent performs during the work shift. ACD work modes include AUX work, auto-in, manual-in, and ACW.

Index