Administering Avaya one-X® Communicator

Release 6.2 Feature Pack 10
November 2015

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/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

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

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

License types

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

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail

account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

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

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

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

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

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

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: 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.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

About this guide

This administration guide provides instructions for configuring Avaya Aura® for Avaya one-X® Communicator users. The guide also covers requirements for configuring and integrating Avaya one-X® Communicator with other products.

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.

Related documents

Additional Avaya one-X® Communicator documentation includes:

- *Avaya one-X® Communicator Overview and Planning*
- *Implementing Avaya one-X® Communicator*
- *Using Avaya one-X® Communicator*
- *Avaya one-X® Communicator Quick Start Guide*
- *Avaya one-X® Communicator Centralized Administration Tool Guide*
- Avaya one-X® Communicator Online Help (Integrated with the application)

Additional Avaya Aura® documentation includes:

- *Administering Avaya Aura® Communication Manager*
- *Avaya Aura® Communication Manager Feature Description and Implementation*
- *Administering Avaya Aura® Session Manager*
- *Avaya Aura® Session Border Controller System Administration*

To obtain these documents and documents about other Avaya products mentioned in this guide, see the Avaya Web site at http://www.avaya.com/support.

Related links

Accessing Online Help on page 8

Accessing Online Help

Procedure

Do either of the following:

- Press F1 on any Avaya one-X® Communicator screen.
- Click the **?** icon.

Related links

Related documents on page 8

Chapter 2: Requirements

Server requirements

Product Name	Supported versions
Avaya Aura® Communication Manager	• Release 5.2.1 • Release 6.2 • Release 6.3 (along with Avaya Aura® Release 6.2 FP2) • Release 6.3.2 (along with Avaya Aura® Release 6.2 FP3) • Release 6.3.6 (along with Avaya Aura® Release 6.2 FP4) • Release 6.3.8
Avaya Aura® Session Manager	• Release 6.3 • Release 6.3.2 (along with Avaya Aura® 6.2 FP2) • Release 6.3.4 (along with Avaya Aura® 6.2 FP3) • Release 6.3.8 (along with Avaya Aura® 6.2 FP4) • Release 6.3.9
Avaya Aura® Session Border Controller	• Release 6.2 • Release 6.3 • Release 6.2.1 (FP1)
Avaya Aura® System Manager	• Release 6.3 • Release 6.3.2 (along with Avaya Aura® 6.2 FP2) • Release 6.3.4 (along with Avaya Aura® 6.2 FP3) • Release 6.3.8 (along with Avaya Aura® 6.2 FP4) • Release 6.3.9 • Release 6.3.10
Avaya one-X® Client Enablement Services	Release 6.2
Avaya Aura® Presence Services	• Release 6.2 (along with Avaya Aura® 6.2 FP2)

Table continues…

Product Name	Supported versions
	• Release 6.2.2 (along with Avaya Aura® 6.2 FP3) • Release 6.2.4 (along with Avaya Aura® 6.2 FP4)
Avaya Aura® Conferencing Standard Edition	• Release 7.0 • Release 7.2 • Release 7.2.2 • Release 8.0
Avaya Meeting Exchange™	• Release 5.2 • Release 6.2
Avaya Aura® Messaging	• Release 6.1 • Release 6.2 • Release 6.3 • Release 6.3.1 • Release 6.3.2
Modular Messaging	Release 5.2

To check the latest versions of a product that Avaya one-X® Communicator supports, go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Note:

Upgrade Communication Manager, media servers, and Session Manager with the latest service pack for maximum client stability.

Client requirements

Avaya one-X® Communicator users must have the following hardware, software, and network connectivity:

Computer hardware without video

Computers that are not running the optional video feature must meet these hardware requirements:

- Intel Pentium 1.2 GHz processor (minimum)
- 1-GB RAM.(More for Windows 7, Windows 8, and Windows 10 as per Microsoft recommendations)
- 1.5 GB free hard disk space (3-GB free hard disk space if .NET 4.0 is not already installed)
- Keyboard
- Mouse or some other compatible pointing device
- Monitor with 1024 x 768 or higher resolution
- Network interface card

- USB headset for This Computer mode

Computer hardware with video

Computers that are running the optional video feature must meet these hardware requirements:

- Intel Pentium 4 2.0 GHz or dual-core processor
- 1-GB RAM. (More for Windows 7, Windows 8, and Windows 10 as per Microsoft recommendations)
- 100 MB dedicated video RAM
- 1.5-GB free hard disk space (3-GB free hard disk space if .NET 4.0 is not already installed)
- Keyboard
- Mouse or some other compatible pointing device
- Video adapter and Monitor with 1024 x 768 or higher resolution
- Network interface card
- USB headset for This Computer mode
- Recommended USB camera. For more information on the supported cameras, see the *Avaya one-X® Communicator Overview and Planning* guide.

Computer hardware with HD video

Computers that are running the optional HD video feature must meet these hardware requirements:

- Intel Dual Core or Core 2 Duo or Core i3
- 2-GB RAM. (More for Windows 7, Windows 8, and Windows 10 as per Microsoft recommendations)
- 100 MB dedicated Video RAM. If this is shared with main RAM, main RAM needs to be increased by 100 MB.
- 1.5-GB free hard disk space (3-GB free hard disk space if .NET 4.0 is not already installed)
- Keyboard
- Mouse or some other compatible pointing device
- Video adapter and monitor with 1024 x 768 or higher resolution
- Network interface card
- USB headset for This Computer mode
- HD camera (up to 720p that supports 30fps video)

Operating system

Computers must have one of the following 32 bit or 64 bit operating systems:

- Microsoft Windows Server 2008 as a Citrix server
- Microsoft Windows 7 Service Pack 1 or Ultimate or Professional Editions
- Microsoft Windows 8 Enterprise and Professional

Licensing requirements

The requirements are:

- You need a Communication Manager off-PBX station (OPS) license to add an extension to the OPTIM form in Communication Manager. This only applies to SIP endpoints.
- You also need a video license for making the video functionality work.

Supported Deskphones

The supported Deskphones depend on whether you have installed Avaya one-X® Communicator in the H.323 protocol mode or in the SIP protocol mode and the user mode you want to use.

H.323 protocol mode:

In the Deskphone (shared control) user mode, the Deskphone as well as Avaya one-X® Communicator client must be working in the H.323 protocol mode. Avaya one-X® Communicator supports the following IP Deskphones with H.323 protocol mode:

With H.323 Software	Heading for Column 2
6.4 and later	• 9608 • 9608G • 9611G • 9621G • 9641G • 96421GS
3.2 and later	• 9620C • 9620L • 9630G • 9640 • 9640G • 9650 • 9650C • 9670G
1.3 and later	• 1603 • 1603-I • 1608 • 1608-I • 1616

Table continues…

With H.323 Software	Heading for Column 2
	• 1616-I

SIP protocol mode

In the Desk phone (shared control) user mode, Avaya one-X® Communicator supports the following Avaya 9600 Series IP Deskphones with SIP 6.5+ firmware:

- 9601
- 9608
- 9608G
- 9611G
- 9621G
- 9641G
- 9641GS

Digital Communications Protocol (DCP) mode

Avaya one-X® Communicator supports the following series of DCP phones:

- 1400 Series Digital Deskphones 1.0
- 2400 Series Digital Telephones 1.0
- 9400 Series Digital Deskphones 2.0.2

To check the latest versions of Deskphones that are compatible with Avaya one-X® Communicator, navigate to http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Avaya one-X® Client Enablement Services integration requirements

To provide the following features, Avaya one-X® Communicator must be integrated with Avaya one-X® Client Enablement Services Release 6.2:

- Visual voice mail
- Centralized call logs
- Audio bridge conferencing
- VIP contacts
- Blocking of calls

Note:

Before starting integration with other applications, ensure that Avaya one-X® Client Enablement Services is installed and configured.

For more information, see *Implementing Avaya one-X® Client Enablement Services guide* on the Avaya Support Web site http://www.avaya.com/support.

Visual voice mail requirements

To use visual voice mail with Avaya one-X® Communicator, you must install and administer:

- Avaya one-X® CES Release 6.2.
- Avaya Modular Messaging Release 5.2 or Avaya Aura® Messaging Release 6.1, 6.2, 6.3, 6.3 FP1, 6.3 FP2
- Avaya Communication Manager Messaging Release 6.2 and Release 6.3.

Visual audio conferencing requirements

To use visual audio conferencing with Avaya one-X® Communicator, you must install and administer:

- Avaya one-X® CES Release 6.2.
- Avaya Meeting Exchange™ Release 5.2 or 6.2.
- Avaya Aura® Conferencing Standard Edition Release 6.0, Release 7.0, or Release 8.0.

Note:

Avaya Aura® Conferencing Standard Edition supports audio and video conferencing.

Bandwidth requirement for supported codecs

Depending on the bandwidth availability and acceptable voice quality, you need to select a codec that produces compressed audio.

- G.711 A codec produces audio uncompressed to 64 kbps
- G.729 A codec produces audio compressed to 8 kbps

For more information on bandwidth requirement for different codecs, see section in the *Avaya IP voice quality network requirements guide* on the Avaya support site http://www.avaya.com/support

The following table provides a comparison between the two codecs G.711 and G.729 both of which are supported by Avaya one-X® Communicator:

Table 1: Comparison of Speech Coding Standards

Standard	Coding Type	Bit Rate (kbps)
G.711	PCM	64
G.729	CS-ACELP	8

Table 2: LAN bandwidth in kbps required for G.711 codec

	Ethernet Type	EV2 with trailer but no preamble	EV2 with trailer and preamble	EV2 with trailer and preamble and 802.1Q
G.711 Voice Payload Size	10ms	110.4	116.8	120
	20ms	87.2	90.4	92
	30ms	79.5	81.6	82.7
	40ms	75.6	77.2	78
	50ms	73.3	74.6	75.2
	60ms	71.7	72.8	73.3

Table 3: WAN bandwidth using Frame Relay or PPP L2 protocol required in kbps

	Codec Type	G.711 and G.711A	G.729 and G.729A
Voice payload size	10ms	102.4	46.4
	20ms	83.2	27.2
	30ms	76.8	20.8
	40ms	73.6	17.6
	50ms	71.7	15.7
	60ms	70.4	14.4

The other supported codecs are:

- G.711MU
- G.722-64K
- G.722.1-24K
- G.722.1-32K
- G.729
- G.729B
- G.729AB

Chapter 3: Configuring Communication Manager Release 6.x

Avaya one-X® Communicator, configured as a SIP end point on Communication Manager, utilizes the user registration feature of Session Manager. To improve the reliability of the configuration, the SIP clients are registered on Session Manager. The sample configuration includes Communication Manager as a Feature Server supporting IP Multimedia Subsystem (IMS) and SIP users registered on Session Manager. Communication Manager as a Feature Server is connected to Session Manager through IMS-enabled SIP signaling groups and associated SIP trunk groups.

Avaya 9600-series IP telephones, which are H.323 phones, and digital telephones are supported by a second Communication Manager that serves as an Evolution Server within the Session Manager architecture. The Communication Manager Evolution Server is connected over SIP trunks to Session Manager. All intra system calls are carried over these SIP trunks. Session Manager is managed by Avaya Aura® System Manager. Communication Manager as a Feature Server runs on the Avaya S8800 server with Avaya G650/G450/G430 Media Gateway.

Note:

If possible, use System Manager to administer Communication Manager features. Feature administration using System Manager ensures that the Communication Manager translation files are in synchronization with the System Manager database.

Before you begin with the configuration steps, ensure that Media Server is already configured on Communication Manager.

Related links

Verifying capacity, routing, and networking on page 17
Configuring trunk-to-trunk transfers on page 17
Configuring IP codec set on page 18
Configuring the IP network region on page 18
Adding node names on page 19
Configuring SIP signaling groups and trunk groups on page 19
Adding SIP trunks on page 21
Configuring the route pattern on page 22
Administering the numbering plan on page 22
Administering AAR digit analysis on page 23
Saving translations on page 23

Verifying capacity, routing, and networking

Procedure

1. On the SAT interface, type the `change system-parameters customer-options` command.
2. Press `Enter`.

   The system displays the OPTIONAL FEATURES screen.
3. On page 1, verify the following:

   For the **Maximum off-PBX Telephones - (OPS)** parameter, the **USED** column displays a value less than the available value.
4. On page 2, verify that the number specified for the **Maximum Administered SIP Trunks** field is enough for your use.
5. On page 4, type `y` for the following fields:
   - **ARS?**
   - **ARS/AAR Partitioning?**
6. On page 5, verify the values in the following fields:
   a. The **Enhanced Conferencing?** field displays **y**.
   b. The **Extended Cvg/Fwd Admin?** field displays **y**.
   c. The **ISDN-PRI?** field displays **y**.
   d. The **Multifrequency Signaling** field displays **y**.
   e. The **IP Trunks?** field displays **y**.

   Note:

   The values specified here are a part of the sample configuration on Communication Manager.
7. On page 6, verify that the value in the **Private Networking** field displays **y**.
8. Save the changes.

Related links

Configuring Communication Manager Release 6.x on page 16

Configuring trunk-to-trunk transfers

Procedure

1. On the SAT interface, type the `change system-parameters features` command.
2. Press `Enter`.

The system displays the FEATURE-RELATED SYSTEM PARAMETERS screen.

3. Set the value in the **Trunk-to-Trunk Transfer** field to `all`.
4. On the page that displays the AUTOMATIC EXCLUSION PARAMETERS area, set the value in the **Automatic Exclusion by COS** field to `y`.
5. Save the changes.

Related links

Configuring Communication Manager Release 6.x on page 16

Configuring IP codec set

Procedure

1. On the SAT interface, type the `change ip-codec-set n` command.

   In this command, `n` is the number to identify the codec set.
2. On the IP Codec Set window, verify the following field values:
   a. **Audio Codec**. `G.711MU`, `G729 AB`, `G.722`, and `G.711A` are supported codecs.
   b. **Silence Suppression**. Set to `n`.
   c. **Frames Per Pkt**. Set to `2`.
   d. **Packet Size (ms)**. Set to `20`.
   e. **Media Encryption**. Set to one of the following:
      - 1-srtp-aescm128-hmac80
      - 2-srtp-aescm128-hmac32
      - None
3. **Allow Direct IP multimedia** on page 2 of the Change ip-codec set. Set to Yes for all Video calls.

Related links

Configuring Communication Manager Release 6.x on page 16

Configuring the IP network region

Procedure

1. On the SAT interface, type the `change ip-network-region n` command, where `n` is the network region number in use for the client application call routing.
2. Press `Enter`.

The system displays the IP NETWORK REGION screen.

3. Specify the values in the following fields:
   a. **Authoritative Domain**: Enter the current SIP domain for the configuration.
   b. **Name**: Enter a descriptive name for the network region.
   c. **Codec Set**: Enter the number of the configured IP codec set.
   d. **Intra-region IP-IP Direct Audio**: Type `y`.
   e. **Inter-region IP-IP Direct Audio**: Type `y`.
4. Save the changes.

Related links

Configuring Communication Manager Release 6.x on page 16

Adding node names

About this task

Use this procedure to add an entry for the trunk.

Procedure

1. On the SAT interface, type the `change node-names ip` command.
2. Press `Enter`.

   The system displays the IP NODE NAMES screen.
3. Specify the node names and IP addresses for Communication Manager.
4. Save the changes.

Related links

Configuring Communication Manager Release 6.x on page 16

Configuring SIP signaling groups and trunk groups

About this task

The SIP signaling group defines the characteristics of a signaling connection. When using SIP, the system does not include any physical trunk. Hence, there is no limit on how many calls or trunk members you can set up with a particular signaling connection.

If the Avaya Aura® configuration includes signaling groups, you might not need to add a new signaling group.

Procedure

1. On the SAT interface, type the `add signaling-group n` command, where `n` is the signaling group number.

   To change a signaling group, use the `change signaling-group n` command and verify the field values specified in this procedure.

2. Press `Enter`.

   The system displays the SIGNALING GROUP screen.

3. Specify the values in the following fields:

   a. **Group Type**: Type `sip`.

   b. **IMS Enabled**: Type `y`.

      Note:

      The value specified here is part of the sample configuration on Communication Manager that supports IMS-enabled SIP signaling groups.

   c. **Transport Method**: Type `tls`.

   d. **Peer Detection Enabled**: Type `y`.

   e. **Peer Server**: Use the default value.

   f. **Near-end Node Name**: Enter the node name that you defined for Communication Manager.

   g. **Far-end Node Name**: Enter the node name that you defined for Session Manager.

   h. **Near-end Listen Port**: Type `5061`.

   i. **Far-end Listen Port**: Type `5061`.

   j. **Far-end Network Region**: Enter the network region that you entered while configuring the IP network region.

   k. **Far-end Domain**: Enter the same domain name that you entered for the **Authoritative Domain** field while configuring the IP network region.

   l. **DTMF over IP**: Type `rtp-payload`.

      The **DTMF over IP** field must remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF tones using RFC 2833.

4. Save the changes.

Related links

Configuring Communication Manager Release 6.x on page 16

Adding SIP trunks

About this task

If the Avaya Aura® configuration includes trunk groups, you might not need to add a new trunk group.

Procedure

1. On the SAT interface, type the `add trunk-group n` command, where `n` is the trunk group number.
2. Press `Enter`.

   The system displays the TRUNK GROUP screen.
3. On page 1, specify the values in the following fields:
   a. **Group Type**: Type `sip`.
   b. **Group Name**: Enter a name for the group.
   c. **TAC**: Enter a trunk access code.
   d. **Direction**: Type `two-way`.
   e. **Outgoing Display**: Type `y`.
   f. **Service Type**: Type `tie`.
   g. **Signaling Group**: Enter the number of the signaling group.
   h. **Number of Members**: Enter the number of members in the SIP trunk.
4. On page 3, specify the values in the following fields:
   a. **Numbering Format**: Type `private`.

      Note:

      The value specified here is part of the sample configuration on Communication Manager.
   b. **Show ANSWERED BY on Display**: Type `y`.
5. On page 4, specify the values in the following fields:
   a. **Support Request History**: Type `y`.
   b. **Telephone Event Payload Type**: Type `120`.
6. Save the changes.

Related links

Configuring Communication Manager Release 6.x on page 16

Configuring the route pattern

Procedure

1. On the SAT interface, type the `change route-pattern n` command, where `n` is an available route pattern.
2. Press `Enter`.

   The system displays the Route Pattern screen.
3. Specify the values in the following fields:
   a. **Grp No**: Enter a row for each trunk group that you created.
   b. **FRL**: Type `0`.
   c. **Numbering Format**: Type `lev0-pvt`.

      The value depends on the value in the **Numbering Format** field, which you specified in the sample SIP Trunk Group.
   d. **LAR**: Type `next` for the first row. Use the default value for the second row.
4. Save the changes.

Related links

Configuring Communication Manager Release 6.x on page 16

Administering the numbering plan

About this task

This procedure is part of the sample configuration on Communication Manager.

Procedure

1. On the SAT interface, type the `change private-numbering n` command, where `n` is the length of the private number.
2. Press `Enter`.

   The system displays the NUMBERING - PRIVATE FORMAT screen.
3. Specify the values for the following fields:
   a. **Ext Len**: Enter the length of the extension number.
   b. **Ext Code**: Enter the leading digit of the extension number.
   c. **Trk Grp (s)**: Enter the name of the trunk group.
   d. **Private Prefix**: Leave this field blank.

      Enter a value in the **Private Prefix** field only if you defined an enterprise canonical numbering scheme on Session Manager.

e. **Total Len**: Enter a number to indicate the total dial plan length.

4. Save the changes.

Related links

Configuring Communication Manager Release 6.x on page 16

Administering AAR digit analysis

About this task

This procedure is part of the sample configuration on Communication Manager.

Procedure

1. On the SAT interface, type the `change aar analysis n` command, where `n` is the first digit of the extension number you have defined.
2. Press `Enter`.

   The system displays the AAR DIGIT ANALYSIS TABLE screen.
3. Specify the values for the following fields:
   a. **Dialed String**: Enter the leading digit of the extension number.
   b. **Min**: Enter the minimum number of digits that the user must dial.
   c. **Max**: Enter the maximum numbers of digits that the user must dial.
   d. **Route Pattern**: Enter the routing pattern.
   e. **Call Type**: Enter `unkn`.
4. Save the changes.

Related links

Configuring Communication Manager Release 6.x on page 16

Saving translations

About this task

Use this procedure to save the changes that you made while configuring Communication Manager.

Procedure

1. On the SAT interface, type the `save translation` command.
2. Press `Enter`.

Related links

Configuring Communication Manager Release 6.x on page 16

Chapter 4: Configuring Session Manager

Adding SIP users

About this task

Use this procedure to add a user to System Manager. However, the preferred option is to add users using directory synchronization with System Manager. For more information about directory synchronization, see *Administering Avaya Aura® System Manager*.

Procedure

1. On the web browser, type `xx.xx.xx.xx/smgr`, where `xx.xx.xx.xx` is the IP address of System Manager.
2. Log in with your administrative credentials.
3. On the Home page in the **Users** section, select **User Management**.
4. In the left navigation pane, expand **User Management** and select **Manage Users**.
5. To add a new SIP user, click **New**.
6. In the **Identity** area, specify the values for the following fields:
    a. **Last Name**: Enter the last name of the user.
    b. **First Name**: Enter the first name of the user.
    c. **Login Name**: Enter *extension number@domain*.
    d. **Authentication Type**: Select *Basic*.
    e. **Password**: Enter the password to log in to System Manager.
    f. **Confirm Password**: Reenter the password.
    g. **Localized Display Name**: Enter the display name of the user.
7. In the **Communication Profile** area, click **New**.
8. In the **Name** field, enter **Primary**.
9. Select the **Default** check box.
10. In the **Communication Address** area, click **New**.
11. Specify the values for the following fields:
    a. **Type**: Select *Avaya SIP* from the list.

b. **Fully Qualified Address**: Enter the same extension number as the value in the **Login Name** field.

c. **@**: Select the value that is the same as the System Manager domain to support SIP endpoints.

12. Click **Add**.
13. In the **Session Manager Profile** area, specify the values for the following fields:
    a. **Primary Session Manager**: Select the Session Manager instance that is the home server for the particular user profile.
    b. **Secondary Session Manager**: Select the Session Manager instance that provides continued service to SIP devices.
    c. **Origination Application Sequence**: Select the same application sequence as defined in System Manager to support SIP users for Communication Manager.
    d. **Termination Application Sequence**: Select the same application sequence as defined in System Manager to support SIP users for Communication Manager.
    e. **Survivability Server**: Select *None*.
    f. **Home Location**: Select the same location as defined to identify the logical or physical location of the SIP entity.
14. In the **CM Endpoint Profile** area, specify the values for the following fields:
    a. **System**: Select the Management Element defined for Communication Manager Feature Server.
    b. **Use Existing Endpoints**: Select this field if you defined an endpoint while adding a station in Communication Manager as OPS.
    c. **Extension**: Enter the same extension number as the value in the **Login Name** field.
    d. Click **Endpoint Editor**.
    e. **Template**: Select a template for the SIP clients.
    f. **Security Code**: Enter the security code for authorized access to the user endpoint.
    g. **Port**: Select IP.
    h. **Delete Endpoint on Unassign of Endpoint from User or on Delete User**: Select to automatically delete the station when the endpoint profile is unassigned from the user.
15. Click **Commit**.

Synchronizing with Communication Manager

About this task

After making the changes on System Manager, synchronize System Manager with Communication Manager.

Procedure

1. On System Manager Web Console, click **Services** > **Inventory** > **Synchronization** > **Communication System**.

   The system displays the Synchronize CM Data and Configure Options page.
2. Expand the **Synchronize CM Data/Launch Element Cut Through** table.
3. Select the check box next to the *Communication Manager Feature Server* name.
4. Select **Incremental Sync data for selected devices**.
5. To perform the incremental synchronization now, click **Now**.
6. Verify the status of the synchronization by clicking the **Refresh** link on the table header.

Chapter 5: Verifying Communication Manager and Session Manager configurations

Verifying Communication Manager SIP trunk group status

Procedure

1. Verify the status of one of the SIP trunk groups on Communication Manager Evolution Server by using the `status trunk n` command.

   In this command, `n` is one of the trunk group numbers.

2. Verify that all trunks in the trunk group are in the **in-service/idle** state.
3. Verify the status of a SIP signaling group by using the `status signaling-group` command.
4. Verify that the signaling group is **in-service** as indicated in the **Group State** field.

Verifying registrations of the SIP endpoints

About this task

Use this procedure to verify that the SIP endpoints have successfully registered with Session Manager.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager** > **System Status** > **User Registrations**.

   The system displays the User Registrations page.

2. Verify that the SIP endpoints have successfully registered with Session Manager.

Verifying the SIP Entity Link status

About this task

Use this procedure to verify the entity link status for SIP entities.

Procedure

1. To view detailed status information about a SIP entity link, on System Manager Web Console, click **Elements** > **Session Manager** > **System Status** > **SIP Entity Monitoring**.
2. To open the SIP Entity, Entity Link Connection Status page, select the SIP entity for Communication Manager Evolution Server from the **All Monitored SIP Entities** table.
3. In the **All Entity Links to SIP Entity: <name of the Communication Manager>** table, verify that the **Conn. Status** for the link is **UP**.
4. To verify the entity link status for other SIP entities, repeat Step 1 to Step 3.

Verifying if Session Manager is operational

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager** > **Dashboard**.
2. In the Session Manager Instances area, verify the following:
   a. The **Tests Pass** column displays a check mark (✔).
   b. The **Security Module** column displays **Up**.
   c. The **Service State** column displays **Accept New Service**.
3. To view detailed status information about the security module for the Session Manager system, click **Elements** > **Session Manager** > **System Status** > **Security Module Status**.
4. Verify that the **Status** column displays **Up**.

Chapter 6: Configuring Avaya one-X® Communicator

Configuration Checklist

To administer the Avaya one-X® Communicator configuration settings, you must have the following information:

Note:

If you configure the Auto-configure feature properly,Avaya one-X® Communicator populates the following fields when the user clicks the Auto-configure button in the corresponding dialog box.

Note:

Avaya one-X® Communicator does not support defining speaker volume level before installation. The default volume level for all users is fixed at 100. However, users can modify these settings using the volume slider on the user interface. Refer to the *Using Avaya one-X® Communicator Communicator* guide for more information.

Phone Settings

Requirement/Information needed	Value	Notes
The IP address of the Avaya telephone server:	_____	
The domain of Session Manager (SIP mode only):	_____	
The transport protocol for Session Manager (SIP mode only):	TLS	

Avaya one-X® Client Enablement Services account settings

Requirement/Information needed	Value	Notes
The URL of Avaya one-X® Client Enablement Services server (FQDN):	_____	
Username	_____	
Password	_____	

Dialing rules settings

Requirement/Information needed	Value	Notes
Number to dial to access an outside line:	_____	
Your country code:	_____	
Your area/city code:	_____	
PBX Main Prefix:	_____	
Number to dial for long distance calls:	_____	
Number to dial for international calls:	_____	
Extension length for internal extension calls:	_____	
Length of national phone numbers (including area/city code):	_____	
Do you have to dial the area/city code when making a local call?	Yes No	

Note:

If the dialing rule fields are kept blank, Avaya one-X® Communicator uses United States dialing rules as the default.

Public directory settings

Requirement/Information needed	**Value**	**Notes**
Directory Type	Active Directory Domino Novell Sun One	
IP address of the directory server:	_____	
Search root:	_____	
Server port:	_____	
Username	_____	
Password	_____	
Do you want to use Active Directory GSS Bind?.	Yes No	If No, then you must instruct the users to add the domain name to their user name in <Domain> \<User Name> format for LDAP search to work.

Setting Auto-configure parameters

After Avaya one-X® Communicator is installed on the personal computer of a user, the user must specify the configuration settings. Users cannot log in and use Avaya one-X® Communicator until they configure these settings.

To simplify the configuration process, Avaya one-X® Communicator provides the Auto-configure feature. When a user clicks the Auto-configure button in the General Settings dialog box, Avaya one-X® Communicator retrieves the appropriate information from the DHCP server. This information is defined in the 46xxsettings.txt file hosted on an HTTP server. Avaya one-X® Communicator retrieves the HTTP server IP address from the DHCP server.

Note:

The Auto-configure feature does not work properly if the user is using Avaya one-X® Communicator through a VPN connection.

There are two separate headers in 46xxsettings.txt file - SETTINGS1XCSIP and SETTINGS1XCH323 for SIP and H.323 protocols respectively. You can set the following parameters under any of these two headers depending on the protocol so that the users can use the Auto-configure feature:

Phone-related parameters

- MCIPADD: The list of servers. The first server is the Primary, and the other servers are Alternate. This is an H.323-specific parameter.
- DISCOVER_AVAYA_ENVIRONMENT: This parameter must be set to *Avaya Environment*. This is a SIP-specific parameter.
- SIPDOMAIN: The SIP domain. This is a SIP-specific parameter.
- SIP_MODE: The SIP mode. This can be simultaneous or peer-to-peer.
- SIP_CONTROLLER_LIST: The Session Manager IP addresses, ports, and transport type. Ports and transport types are optional.

  Note:

  The IP addresses of Avaya Aura® Session Manager must be specified in the same order as it is in the user interface. In case of a mismatch in the order, users cannot make calls using Avaya one-X® Communicator in the Deskphone mode.
- PHNEMERGNUM: The emergency number. This is a SIP-specific parameter.
- FAILBACK_POLICY: The failback policy to use. This is a SIP-specific parameter.
- SIPREGPROXYPOLICY: The policy to treat a list of proxies. This is a SIP-specific parameter.

Dialing rules-related parameters

- PHNOL: The digits you must dial to access an outside line.
- PHNCC: Your country code.
- PHNDPLENGTH: The extension length for internal extension calls.
- PHNIC: The digits users must dial for international calls.
- PHNLD: The digits for long distance calls.

- PHNLDLENGTH: The national phone number length.
- DIALPLANAREACODE: The area or the city code. This parameter isAvaya one-X® Communicator-specific. You must enter this parameter in the file manually.
- DIALPLANLOCALCALLPREFIX: Whether users must dial the area and the city code when they make a local call. Any value for the check box **Include are/city code when making a local call** on the user interface is accepted as a selected check box. However, empty strings in quotes represent a cleared check box in the user interface. To keep the check box unchecked, administrators must include the parameter SET DIALPLANLOCALCALLPREFIX in the auto-config file. This parameter is Avaya one-X® Communicator-specific. You must enter this parameter in the file manually.
- DIALPLANNATIONALPHONENUMLENGTHLIST: A comma-separated list of national telephone number length. This parameter is Avaya one-X® Communicator-specific. You must enter this parameter in the file manually.
- DIALPLANPBXPREFIX: The main prefix of PBX.

LDAP Search Directory-related parameters

- SP_DIRSRVR: The IP address or FQDN of the LDAP directory server name or address.
- SP_DIRSRVRPORT: The TCP port number of the LDAP directory server. The default is 389.
- SP_DIRTOPDN: The topmost distinguished name in the directory.
- SP_DIRTYPE: The directory type. The value should be in capital letters, for example, *ACTIVEDIRECTORY*, *DOMINO*, or *NOVELL*. This parameter is Avaya one-X® Communicator-specific. You must enter this parameter in the file manually.
- ENABLEGSSBIND: Option to enable or disable Active Directory GSS Bind. Select 0 to disable and 1 to enable the Active Directory GSS Bind option in the Public Directory settings.

Avaya one-X® Client Enablement Services related parameters

ONEXPORTAL_URL: The Client Enablement Services URL. This parameter is Avaya one-X® Communicator-specific. You must enter this parameter in the file manually.

Voicemail related parameters

MSGNUM: Specify the message access number.

SRTP related parameters

The following settings enable the best effort CAPNEG for both audio and video media (no separated settings for audio and video):

SET SIPSIGNAL: Specify the type of transport to use for SIP signaling: 0 for UDP, 1 for TCP, 2 for TLS (default).

SET SIP_PORT_SECURE: Specify the port for sure SIP signalling: 5061

SET ENFORCE_SIPS_URI: The setting controls the enforcement of SIPS URI with SRTP. The range is from 0-1. The default value for ENFORCE SIPS URI is 1.

SET SDPCAPNEG: The setting controls the SDP capability negotiation. The range is from 0-1. The default value for this SDPCAPNEG is 1.

SET MEDIAENCRYPTION: Media Encryption Support specifies media encryption (SRTP) options supported by Avaya one-X® Communicator. Values are in comma-separated list. Options should match those specified in CM IP-codec-set form:

- 1 = aescm128-hmac80
- 2 = aescm128-hmac32
- 3 = aescm128-hmac80-unauth
- 4 = aescm128-hmac32-unauth
- 5 = aescm128-hmac80-unenc
- 6 = aescm128-hmac32-unenc
- 7 = aescm128-hmac80-unenc-unauth
- 8 = aescm128-hmac32-unenc-unauth
- 9 = none (default)

Any combination of 1-8 and 9, means the best effort CAPNEG for both audio and video media. The recommended setting is 1,2,9. The following settings turn off the media encryption:

- SET ENFORCE_SIPS_URI 1
- SET SDPCAPNEG 1
- SET MEDIAENCRYPTION 9

Note:

If you configure Avaya one-X® Communicator Release 6.2 to use TCP (not TLS) to register to Session Manager, the MediaEncryption setting must always be 9. Avaya one-X® Communicator Release 6.2 does not support AES 256 encryption that is available with Avaya Aura® 7.0. If your setup is Avaya Aura® 7.0, Avaya one-X® Communicator negotiates the encryption based on the available encryption support. If the negotiation fails, calls are not established.

Instant messaging related parameters

- PRESENCE_SERVER: Specify the IP address of the Presence Server. This is a SIP-specific parameter.
- PRESENCE_DOMAIN: Specify the value for the Presence Domain field under IM and Presence Settings. For example, pres.ips.avaya.com

Configure security settings

Avaya one-X® Communicator supports the following certificates:

- Avaya Product Root Certificate Authority (CA): Embedded in Avaya one-X® Communicator.
- Certificate issued by the Trusted Third Party Certificate Authority (TTP CA) and stored in the system certificate store: X.509 certificates other than the Avaya Root certificate that are loaded to your computer.

Avaya one-X® Communicator supports certificates with 2048–bit RSA keys and SHA-256 digests and uses the selected certificate for two-way Transport Layer Security (TLS) authentication during the handshake stage of establishing secure connections with:

- SIP
- Extensible Messaging and Presence Protocol (XMPP)
- HTTPS
- Session Border Controller
- Avaya one-X® Client Enablement Services
- Lightweight Directory Access Protocol (LDAP)

The client identity certificate is distributed by administrators and must be installed on Avaya one-X® Communicator.

Note:

If you install Avaya one-X® Communicator in the Silent mode, you must enable the Avaya Product Root Certificate Authority (CA). The Avaya CA certificate is installed and configured on Session Manager and Avaya one-X® Communicator uses the Avaya CA client identity certificate by default, unless you configure certificates issued by a Trusted Third Party Certificate Authority (TTP CA).

Related links

Configuring server certificate on a Windows computer on page 35
Configuring client identity certificate on a Windows computer on page 36
Checking the certificate details on page 36
Configuring client identity certificate on Avaya one-X Communicator on page 37
Configuring client identity certificate on System Manager on page 38

Configuring server certificate on a Windows computer

The Trusted CA server certificate is distributed by administrator and must be installed on the Windows computer of the user.

About this task

To install the trusted CA certificate on your system, perform the following steps:

Procedure

1. Double click the certificate file.
2. In the Certificate window, click **Install certificate**.
3. In the Certificate Import Wizard window, click **Next**.
4. Select **Place all certificates in the following store** and click **Browse**.
5. Click **Show physical stores**.
6. Select **Trusted Root Certification Authorities** > **Registry** and click **OK**.

7. Click **Next**.
8. Click **Finish**.

Related links

Configure security settings on page 34

Configuring client identity certificate on a Windows computer

The Trusted CA client identity certificate is distributed by administrator and must be installed on the Windows system.

About this task

To install the client identity certificate on your Windows operating system, perform the following steps:

Procedure

1. Double click the certificate container file.
2. In the Certificate Import Wizard window, click **Next**.
3. In the File to import window, click **Next**.
4. In the Password window, enter the password for the certificate container in the **Password** field, select **Mark this key as exportable** and click **Next**.
5. Select **Place all certificates in the following store** and click **Browse**.
6. Click **Show physical stores**.
7. Select **Trusted Root Certification Authorities** > **Registry** and click **OK**.
8. Click **Next**.
9. Click **Finish**.

Related links

Configure security settings on page 34

Checking the certificate details

If you are going to use client identity certificate issued by TTP CA, ensure the certificate is available in the Personal Certificates store and is valid.

About this task

To check the client identity certificate details, perform the following steps:

Procedure

1. Log on to the system as an administrator.

2. From the command prompt, run the `mmc` command.
3. Click **File** > **Add/Remove Snap-in**, and then click **Add**.
4. Under **Snap-in**, double-click **Certificates**, click **Computer account**, and then click **Next**.
5. Click **Local computer**, and then click **Finish**. Click **Close**.

   The Certificates (Computer Name) snap-in appears on the list of selected snap-ins for the new console.
6. Browse to **Certificates** > **Personal** > **Certificates**.
7. Double-click the client identity certificate and verify the following certificate information:
   - The value for **KeyUsage** extension field is **Digital Signature** and **keyEncipherment bits** set to **1**.
   - The **EnhancedKeyUsage** extension includes object identifiers either for the **Server Authentication (1.3.6.1.5.5.7.3.1)** or the **Client Authentication (1.3.6.1.5.5.7.3.2)** or both.
   - The certificate and the trust chain is valid and does not have any errors such as incorrect signature, and expired validity period.
   - The certificate has passed through revocation checking.
   - The certificate is trusted. The client non-default identity certificate is validated against the Trusted Root Certification Authorities system certificate store.
   - The private key of the certificate is marked as exportable.

Related links

Configure security settings on page 34

Configuring client identity certificate on Avaya one-X® Communicator

Avaya one-X® Communicator supports a client identity certificate issued by the Trusted Third Party Certificate Authority (TTP CA) and stored in the system certificate store: X.509 certificates.

Before you begin

Verify your client identity certificate is installed on your computer and is valid. Refer to Checking the certificate details on page 36

About this task

To install the client identity certificate on Avaya one-X® Communicator, perform the following steps:

Procedure

1. Click the Menu icon > **Settings** to open the General setting window.
2. Click **Security** in the left pane of the General Settings window.
3. Click **Browse** to select a certificate from the Certificate store in your computer.

Note:

If you install Avaya one-X® Communicator in the Silent mode, you can enable the Avaya Product Root Certificate Authority (CA). The Avaya CA certificate is installed and configured on Session Manager and Avaya one-X® Communicator uses the Avaya CA client identity certificate by default, unless you configure certificates issued by a Trusted Third Party Certificate Authority (TTP CA).

4. Click **OK**.

Related links

Configure security settings on page 34

Configuring client identity certificate on System Manager

If you configure a client identity certificate on Avaya one-X® Communicator, the corresponding certificate must be trusted Avaya Aura® System Manager.

About this task

To ensure that the client identity certificate is trusted on Avaya Aura® System Manager, perform the following steps:

Procedure

1. Log on to System Manager.
2. In the Services list, select **Inventory** > **Manage Elements**.
3. Perform any one of the following:
   - If the Avaya Aura® Session Manager instance is not present in the Elements list, refer to the System Manager online help for the steps to add a new element.
   - If the Session Manager instance is present, select the check box for the SM instance, click **More Actions**, and select **Configure Trusted Certificates** from the drop-down menu.
4. On the Trusted Certificates page, click **Add** and import the required certificate to the Session Manager trust store.

Related links

Configure security settings on page 34

Configuring RTCP monitoring

Avaya one-X® Communicator supports collecting endpoint statistic data and sending it in RTCP packets to the VoIP monitoring server.

Before you begin

Ensure that you have closed Avaya one-X® Communicator.

Procedure

1. Open the `config.xml` file. For Microsoft Windows7, Windows 8, and Windows 10, you can find the file at: `C:\Users\<user>\AppData\Roaming\Avaya\Avaya one-X Communicator directory`.
2. Enter the IP Address of the VoIP Monitoring server, for example, `192.168.1.200`:

   <parameter>

   <name>RtcpMonitoringIPAddress</name>

   <value>192.168.1.200</value>

   </parameter>
3. Enter the port of the VoIP Monitoring server, for example, `8888`:

   <parameter>

   <name>RtcpMonitoringPortNumber </name>

   <value>8888</value>

   </parameter>
4. Enter the time period in seconds for sending RTCP packets to the VoIP Monitoring server, for example, `5`.

   <parameter>

   <name>RtcpMonitoringPeriod </name>

   <value>5</value>

   </parameter>
5. Save the `config.xml` file.

Enhancing the limit on Favorite contacts

You can add 50 contacts as your favorite contacts in Avaya one-X® Communicator. However, you can increase the limit to 100 using this procedure.

Before you begin

Ensure that you have closed Avaya one-X® Communicator.

Procedure

1. Open the `config.xml` file. For Microsoft Windows7, Windows 8, and Windows 10, you can find the file at: `C:\Users\<user>\AppData\Roaming\Avaya\Avaya one-X Communicator directory`.

2. Enhance the limit on number of Favorite contacts. The following is an example of the limit being enhanced to 100:

   <parameter>

   <name>FavoritesLimit</name>

   <value>100</value>

   </parameter>

3. Save the `config.xml` file.

Modifying the configuration file for Citrix

Avaya one-X® Communicator supports Citrix XenApp (Release 6.5 and later) and Citrix XenDesktop (Release 6.5 and later). Users can install Avaya one-X® Communicator in the supported Citrix environments using the command: **`Avaya one Communicator.exe /silent / ISFeatureInstall=OneXC /ISCITRIX=true`**. However, prior to installing Avaya one-X® Communicator in Citrix environment, administrators must modify the `config.xml` as shown:

Before you begin

Ensure that you have closed Avaya one-X® Communicator.

Procedure

1. Open the `config.xml` file. For Microsoft Windows 7, Windows 8, and Windows 10, you can find the file at: `C:\Users\<user>\AppData\Roaming\Avaya\Avaya one-X Communicator`.

2. Add the following configuration parameters:

   <parameter>

   <name> SigPortLow </ name>

   <value> 5061 </ value>

   </parameter>

   <parameter>

   <name> SigPortRange</ name>

   <value> 32</ value>

   </parameter>

3. Save the `config.xml` file.

Configuring ad hoc Presence for non-Favorite contacts

The default settings in Avaya one-X® Communicator disables Presence for Non-Favorite contacts. Avaya one-X® Communicator users can view the Presence status of only the Favorite contacts on third party applications such as Microsoft Outlook. If the contact is a non-Favorite, Presence status for the contact is not displayed. Avaya recommends keeping the default settings as it is to reduce the risk of the Presence services application being overloaded.

Before you begin

Ensure that you enable the feature for users in groups of 100 at a time.

Procedure

1. Open the Centralized Administration Tool.
2. Click the **Features** tab.
3. Click **Open**.
4. Select the `InstallConfig.xml` file. You can find the file at:
   - For 32–bit Microsoft Windows 7, 8, and 10: `C:\Program Files\Avaya\Avaya one-X Communicator`.
   - For 64–bit Microsoft Windows 7, 8, and 10: `C:\Program Files (x86)\Avaya\Avaya one-X Communicator`.
5. Click **Open** to populate the existing Features settings.
6. From the **Enable Non-Favorite Presence in Collaboration Services** drop-down menu, select **Yes**.
7. Click **Save**.
8. Save the `InstallConfig.xml` file.

Next steps

- After enabling the feature for a group of users the system administrator must monitor the Presence server and ensure that SIP entity link failures and CPU spikes are not observed.
- The system must be monitored for a period of at least 24 hours before the feature is enabled for additional users.
- In the event that SIP entity link failures or CPU spikes are seen, the Desktop integration setting must be returned to the default settings as a service outage is likely to occur.

Configuring ad hoc Presence for search results

Avaya one-X® Communicator displays Presence status of Contacts in search results if ad hoc presence subscriptions are available. The presence status of the following types of contacts are displayed:

- Avaya one-X® Communicator LDAP contacts

- Avaya one-X® Client Enablement Services contacts
- Personal Profile Manager (PPM) contacts

About this task

The presence status of a contact in search results is available for the time duration that you select using the Centralized Administration Tool. Use the following procedure to configure ad hoc presence for search results:

Procedure

1. Open the Centralized Administration Tool.
2. Click the **Features** tab.
3. Click **Open**.
4. Select the `Installconfig.xml` file. You can find the file at:
   - For 32–bit Microsoft Windows 7, 8, and 10: `C:\Program Files\Avaya\Avaya one-X Communicator`.
   - For 64–bit Microsoft Windows 7, 8, and 10: `C:\Program Files (x86)\Avaya\Avaya one-X Communicator`.
5. Click **Open** to populate the existing Features settings.
6. From the **Enable Presence for the Contact Search Result** drop-down menu, select **Yes**.
7. Click **Save**.
8. Save the `Installconfig.xml` file.

Chapter 7: Integrations

Integrating Avaya one-X® Communicator with Avaya one-X® Client Enablement Services

Before you begin

Ensure Avaya one-X® Client Enablement Services Release 6.2 is installed and is operating.

Procedure

1. In the Web browser, type the Avaya one-X® Client Enablement Services Web page address.
2. Type your administrator **Login ID** and **Password**.
3. Click **Logon**.

Next steps

Ensure the following services are configured on the Avaya one-X® Client Enablement Services server:

- Call History

  Provides access to the Avaya one-X® Client Enablement Services call logs.
- Contacts

  Provides access to the Avaya one-X® Client Enablement Services contacts.
- Modular Messaging (MM)

  Provides access to voice messages.
- Meeting Exchange (MX)

  Provides access to Meeting Exchange bridge conferences.
- User Assistant

  Provides access to the Avaya one-X® Client Enablement Services server log-in modes.

Integrating Office Communication Server for Instant Messaging

This section describes how to integrate MOC 2007 Release 1 or Release 2 with Avaya one-X® Communicator.

Before you begin

- Office Communication Server (OCS) is integrated with Avaya Aura®Presence Services
- Avaya one-X® Communicator is installed and functioning on the computer of the end user.

About this task

The following procedure provides a scenario where two users - User A and User B are configured for instant messaging using Avaya one-X® Communicator and Microsoft Office Communicator.

Procedure

1. Create two users (for example User A and User B) in the Active Directory (AD). The two users must be able to log in to the Microsoft Office Communicator (MOC) and communicate with each other

   Note:

   Ensure that you add the telephone number in the E.164 format in the AD.
2. Synchronize System Manager and the AD.
3. From the User Management page of System Manager, modify User A and User B, and add the Communication Address as Avaya E.164 and Microsoft OCS SIP respectively.
4. Log in User A to Avaya one-X® Communicator.
5. Log in User B to Microsoft Office Communicator.
6. In Avaya one-X® Communicator client, add User B as a favorite.
7. In the MOC client, add the Jabber ID of User A.
8. To send an Instant Message to User B from Avaya one-X® Communicator client of User A:
   - Click the IM icon appearing for User B.
   - From the two options available, select MOC.
9. In the chat window, you can type your message and communicate with User B.

Appendix A: Appendix A: Dial plans

Avaya one-X® Communicator supports the Dialing Rules feature. When a phone number is presented to Avaya one-X® Communicator to be dialed as a new call, a set of dialing rules are applied in order to prefix the number with required access codes. If you need to configure an area code and a country code for the dialing rules in Avaya one-X® Communicator, follow the guidelines and examples as described in this topic.

Note:

Communication Manager must be configured to handle all required digit manipulation. The dialing rules on the clients are complicated and can cause difficulties while troubleshooting. In general it is preferred that no dialing rules configuration is present on theAvaya one-X® Communicator side.

Codes

When you configure Avaya one-X® Communicator dialing rules, you can enter the following call codes:

Code	Description
Outside Access Line	This is the number that identifies that the call is external. This number is typically “9” or “0”.
Country Code	This is the local country code such as “1” or “49”.
Area/City Code	This is the area or city code. Since some localities have multiple area codes, this can be a comma-separated value list such as “303,720”.
PBX Main Prefix	This is the prefix numbers on the local PBX are configured with. This field is used to determine whether a number is an internal extension or not. For instance, if PBX extensions are 5 digits in length and always start with 30353, the PBX prefix is 30353.
Long Distance Code	This is the number to dial when a number is long distance. A long distance number is determined by evaluating the area code of the submitted number versus the configured area/city code(s).
International Access Code	This is the number to dial when a number is international. This is typically “011” or “00”.

Types of calls

If you dial a number with the configured area code and without entering a Long distance code, you make a Local call.

Note:

Local calls can include an area code or not depending on if the location uses 10 or 7 digit dialing in North America.

If you dial a number starting with '+' and not followed by the configured country code, you make an International call.

If a number matches the configured Length of national numbers and doesn't include an area code, you make a Long distance code.

Area code and Country code

The Country code is added if the following conditions are met:

- the entered number length matches the configured Length of national numbers
- the first digits do not match the configured Area code

The Area code can be kept or removed according to the configured settings. The Area code is removed and no Country code is added if the following conditions are met:

- the entered number length matches the configured Length of national numbers
- the first digits match the configured Area code
- the **Remove area code for local calls** setting is enabled

The Area code is not removed and the digits are dialed without changes if the following conditions are met:

- the entered number matches he configured Length of national numbers
- he first digits match the configured Area code
- the **Remove area code for local calls** setting is disabled

Examples of the dialing plan configuration

Example 1.Configuring Multiple Area Codes/ NPA in the same 10-digit local calling area.

Number pattern: 404-686-xxxx and 770-222-xxxx (Atlanta GA)

Solution: Separate the multiple Local area codes with a comma in the dialing rules configuration.

Setting	Value
Country code	1
Area code	404,770
Long Distance Code	1
International Access Code	011
Length of national numbers	10
Remove area code for local calls	disabled

Example 2. Configuring 1-NPA-Number where 1 is required even for local calls in the same area.

Number pattern: 212-xxx-xxxx (New York City)

Solution: Use a blank area code.

Setting	Value
Country code	1
Area code	<blank>
Long Distance Code	1
International Access Code	011
Length of national numbers	10
Remove area code for local calls	disabled

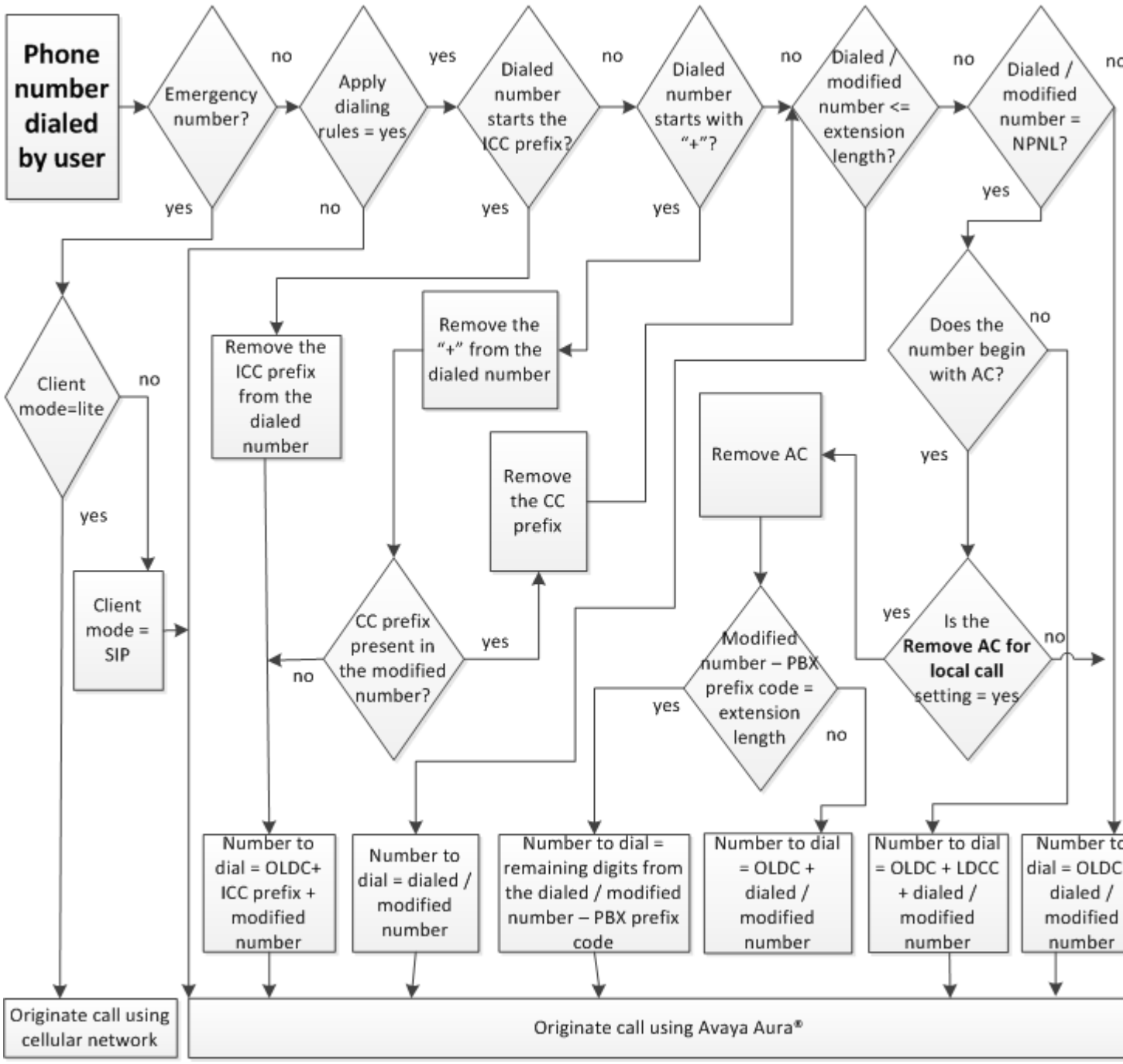
Example 3. Configuring 7-digit local and 1+10-digit Toll calls in the same Area Code/NPA.

Number pattern: 231-xxxx and 1-701-333-xxxx (North Dakota)

Solution: This pattern cannot be handled by client dialing rules since the list of local exchanges is not available and should be handled by call type analysis or code conversion on Communication Manager. Communication Manager can be configured to mask the need for 7 against 11 digit dialing from the end-users or clients.

Dialing Rules algorithm

Follow the diagram to learn the algorithm applied to the dialed number according to the configured dialing rules:


Phone number dialed by user
Emergency number?
no
yes
Apply dialing rules = yes
no
yes
Dialed number starts the ICC prefix?
no
yes
Dialed number starts with "+"?
no
yes
Dialed / modified number <= extension length?
no
Dialed / modified number = NPNL?
no
yes
Does the number begin with AC?
no
yes
Client mode=lite
no
yes
Client mode = SIP
Remove the ICC prefix from the dialed number
Remove the "+" from the dialed number
Remove the CC prefix
Remove AC
CC prefix present in the modified number?
yes
no
Modified number – PBX prefix code = extension length
yes
no
Is the Remove AC for local call setting = yes
yes
no
Number to dial = OLDC+ ICC prefix + modified number
Number to dial = dialed / modified number
Number to dial = remaining digits from the dialed / modified number – PBX prefix code
Number to dial = OLDC + dialed / modified number
Number to dial = OLDC + LDCC + dialed / modified number
Number to dial = OLDC dialed / modified number
Originate call using cellular network
Originate call using Avaya Aura®

Index

S

T

V