Administering Avaya one-X® Communicator for Mac OS X

Release 2.0.1
January 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)

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use 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”).

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.

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 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. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

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.

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 7
- About this guide 7
- Related documents 7
- Avaya one-X® Communicator for Mac OS X overview 7
- Basic features 7

Chapter 2: Prerequisites 9
- Server side prerequisites for Avaya one-X® Communicator for Mac OS X 9
- Client side prerequisites for Avaya one-X® Communicator for Mac OS X 10
- Bandwidth requirement for supported codecs 10
- Downloading Avaya one-X® Communicator for Mac OS X 11

Chapter 3: Configuring Communication Manager Release 6.x 13
- Verifying capacity, routing, and networking 15
- Configuring trunk-to-trunk transfers 16
- Configuring IP codec set 16
- Configuring the IP network region 17
- Adding node names 17
- Configuring SIP signaling groups and trunk groups 18
- Adding SIP trunks 19
- Configuring Avaya one-X® Communicator as an Endpoint for video calling 20
- Configuring the route pattern 20
- Administering the numbering plan 21
- Administering AAR digit analysis 21
- Saving translations 22

Chapter 4: Configuring Session Manager 23
- Adding SIP users 23
- Synchronizing with Communication Manager 24

Chapter 5: Verifying Communication Manager and Session Manager configurations 27
- Verifying the Communication Manager SIP trunk group status 27
- Verifying registrations of the SIP endpoints 27
- Verifying the SIP Entity Link status 28
- Verifying if Session Manager is operational 28

Chapter 6: Configuring your preferences 31
- Configuring the account settings 31
  - Account field descriptions 32
- Configuring the general preferences 32
  - General preferences field descriptions 33
- Configuring dialing rules 33
  - Dialing Rules field descriptions 34
- Configuring the directory 35
  - Directory field descriptions 36
- Configuring advanced preferences 36
  - Advanced field descriptions 37
- Configuring an emergency number 38
  - Emergency field descriptions 38

Chapter 7: Port usage 39
Chapter 8: Troubleshooting Avaya one-X® Communicator for Mac OS X 41
Appendix A: Appendix A: Security recommendations for administrators 43
Index 45

Chapter 1: Introduction

About this guide

This administration guide provides information on server requirements, client requirements, and procedures to configure Avaya Aura® and the Avaya one-X® Communicator for Mac OS X application.

Related documents

- *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*
- *Using Avaya one-X® Communicator for Mac OS X*

You can download the latest copies of these documents from the Avaya Support website at www.avaya.com.

Avaya one-X® Communicator for Mac OS X overview

Avaya one-X® Communicator for Mac OS X is a desktop communication tool to manage your telephony tasks. Avaya one-X® Communicator for Mac OS X provides you with simple, intuitive access to all your contacts and the features of the desk telephone in a simple soft phone on your Apple computer.

Basic features

Avaya one-X® Communicator for Mac OS X provides users with the following features:

- Full set of call-control features, including transfer and ad-hoc audio conferencing
- User preference settings to configure dial plans and emergency number
- Point-to-point video calling
- Failover feature to ensure high availability. An alternate registration on Avaya Aura® Session Manager is required to avail this feature. Users must be provided with a secondary Avaya Aura® Session Manager server address for alternate registration.
- Conversion of audio calls to video calls and video calls to audio calls
- Option to select a camera and size video windows according to convenience
- Option to dial from the list of recent calls
- Option to navigate and use the application using keyboard shortcuts
- PSTN access through Avaya Aura® Communication Manager
- Option to select and control microphone and speaker
- Click-to-Dial capability
- Option to add a contact as a Favorite contact
- Option to operate in the compact mode
- Provision to add, modify, and remove contacts.
- User preference settings to control connections to the Avaya Aura® environment and to the corporate directory
- Provision for click to gain access to voicemail

Avaya one-X® Communicator for Mac OS X 2.0 supports the My Computer mode.

Chapter 2: Prerequisites

Server side prerequisites for Avaya one-X® Communicator for Mac OS X

- Avaya Aura® Communication Manager Release 6.2 SP4 (Feature Pack 1) or Release 6.3 (Feature Pack 2)
- Avaya Aura® Session Manager Release 6.3 (Feature Pack 1) or Release 6.3.2 (Feature Pack 2)
- Avaya Aura® Session Border Controller for Enterprise Release 6.2
- Avaya Aura® System Manager Release 6.3 (Feature Pack 1) or Release 6.3.2 (Feature Pack 2)
- Avaya Aura® Conferencing Standard Edition Release 6.0, 7.0, or 7.2
- Avaya Meeting Exchange™ Release 5.2
- Avaya Aura® Messaging Release 6.2
- Wireless enabled enterprise campus 802.11b/g/n.

To check the latest versions of a product that Avaya one-X® Communicator for Mac OS X supports, go to https://support.avaya.com/CompatibilityMatrix/Index.aspx. You can also refer to the Avaya one-X® Communicator for Mac OS X Release Notes for latest information on supported Aura configurations and other requirements.

Other requirements

- You need a Communication Manager off-PBX station (OPS) license to add an extension to the OPTIM form in Communication Manager.
- For each user, you must have a station form on Communication Manager and a user ID and media extension on Session Manager.

Note:

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

Client side prerequisites for Avaya one-X® Communicator for Mac OS X

Your device must meet the following minimum requirements to use Avaya one-X® Communicator for Mac OS X:

Hardware

- Processor: Intel 1.6 GHz
- Memory: 1-GB of RAM
- Hard disc space: 1 GB
- Web camera, needed if you want to use video

Note:

Avaya one-X® Communicator for Mac OS X supports 64-bit operation.

Software

- Avaya one-X® Communicator for Mac OS X Release 2.0
- Mac OS X Mountain Lion (10.8)
- Mac OS X Mavericks (10.9)

To check the latest versions of a product that Avaya one-X® Communicator for Mac OS X supports, go to https://support.avaya.com/CompatibilityMatrix/Index.aspx. You can also refer to the Release Notes for latest information on required software and hardware for installing and using Avaya one-X® Communicator for Mac OS X.

Bandwidth requirement for supported codecs

Avaya one-X® Communicator for Mac OS X needs a minimum bandwidth of 64 kbps to support the following codecs for audio calls:

- G.711 Mu-Law
- G.711 A-law
- G.729A
- G.729B

- G.729AB
- G.722

Downloading Avaya one-X® Communicator for Mac OS X

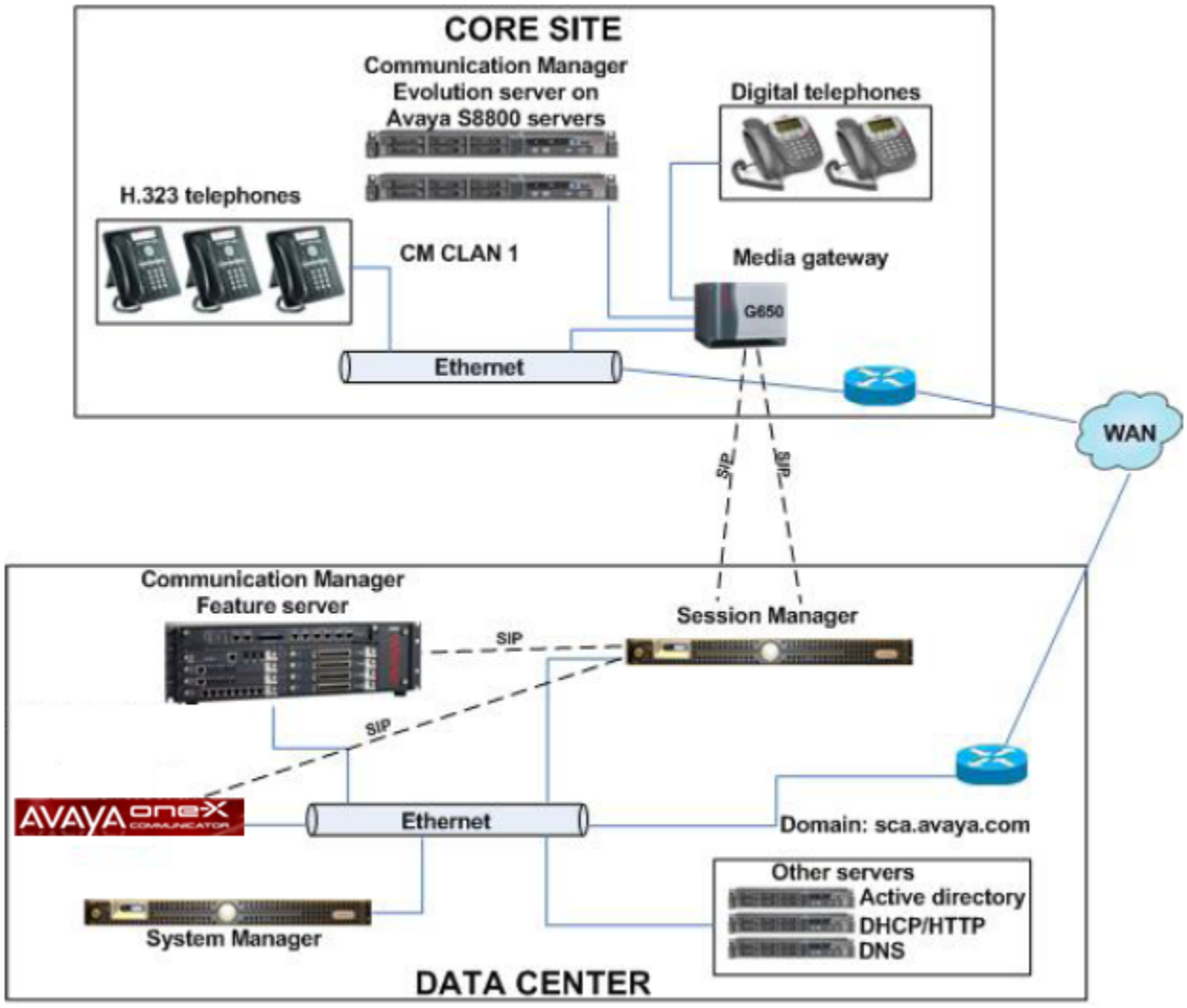
Procedure

1. Using your Web browser, go to http://www.avaya.com/support
2. In the navigation pane on the left side of the screen, click **Downloads**.
3. Enter the product name in the dialog box and download the Avaya one-X® Communicator for Mac OS X application.
4. If you have not registered as a PLDS user, complete a one-time registration.
5. Download the installer.

Chapter 3: Configuring Communication Manager Release 6.x

Avaya one-X® Communicator for Mac OS X, 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 650 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.

Verifying capacity, routing, and networking

Procedure

1. On the SAT interface, type the `display system-parameters customer-options` command.
2. Press `Enter`.
   The system displays the OPTIONAL FEATURES screen.
3. On page 1, verify the following:
   a. For the **Maximum off-PBX Telephones - (EC500)** parameter, the **USED** column displays a value less than the available value.
   b. For the **Maximum off-PBX Telephones - (OPS)** parameter, the **USED** column displays a value lesser than the available value.
4. On page 2, verify that the number specified for the **Maximum Administered SIP Trunks** field is sufficient for your use.
5. On page 3, type `y` for the following fields:
   - **ARS?**
   - **ARS/AAR Partitioning?**
   - **ARS/AAR Dialing without FAC?**
6. On page 4, verify the values in the following fields:
   a. The **Enhanced Conferencing?** field displays **y**.
   b. The **Enhanced EC500?** field displays **y**.
   When the **Enhanced EC500** field displays **y**, all screens which relate to the *off-pbx-telephone* commands are available.
   c. The **Extended Cvg/Fwd Admin?** field displays **y**.
   d. The **ISDN-BRI Trunks?** field displays **y**.
   e. The **ISDN-PRI?** field displays **y**.
   f. The **Multifrequency Signaling** field displays **y**.
   g. The **IP Trunks?** field displays **y**.

   Note:

   The value specified here is part of the sample configuration on Communication Manager.
7. On page 5, verify that the value in the **Private Networking** field displays **y**.
8. To save the changes, press `Enter`.

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 page 17 of the FEATURE-RELATED SYSTEM PARAMETERS screen, in the **AUTOMATIC EXCLUSION PARAMETERS** area, set the value in the **Automatic Exclusion by COS** field to `y`.
5. To save the changes, press `Enter`.

Configuring IP codec set

Procedure

1. On the SAT interface, type the `change ip-codec-set n` command, where `n` is the number to identify the codec set.
2. On the IP Codec Set screen, verify the following field values:
   a. **Audio Codec**. `G.711MU`, `iSAC`, `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. To save the changes, press `Enter`.

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 `yes`.
   e. **Inter-region IP-IP Direct Audio**: Type `yes`.
4. To save the changes, press `Enter`.

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 Node Name screen.
3. Specify the node names and IP addresses for Communication Manager.
4. To save the changes, press `Enter`.

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**: Enter `sip`.
   b. **IMS Enabled**: Enter `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**: Enter `tls`.
   d. **Peer Detection Enabled**: Enter `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**: Enter `5061`.
   i. **Far-end Listen Port**: Enter `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**: Enter `rtp-payload`.

4. To save the changes, press `Enter`.

Adding SIP trunks

About this task

If the Avaya Aura® configuration includes tunk 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**: Enter `sip`.
   b. **Group Name**: Enter a name for the group.
   c. **TAC**: Enter a trunk access code.
   d. **Direction**: Enter `two-way`.
   e. **Outgoing Display**: Enter `y`.
   f. **Service Type**: Enter `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**: Enter `private`.

      Note:

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

Configuring Avaya one-X® Communicator as an Endpoint for video calling

Procedure

1. Use the **`display system-parameters customer-options`** command to verify the **Maximum Video Capable IP Softphones** (page 2 of form). This number is provided by the RFA license file.
2. Use the **`change cos`** command to set **Priority Video Calling** (page 2 of form) for the appropriate COS levels.
3. Use the **`add station`** command to add an Avaya IP Softphone station, and set the following parameters for that station:
   - **IP Softphone** to `y`.
   - **IP Video Softphone** to `y`.
   - If you want this station to be able to make priority video calls, make sure you select a COS level that has **Priority Video Calling** enabled.
   - On page 2 of the form, set **Direct IP-IP Audio Connections** to `y`.

   Repeat steps 1 to 3 for each Avaya one-X® Communicator endpoint you want to configure for video calling.

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

Note:

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. To save the changes, press `Enter`.

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 numbers.
   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 in Session Manager.
   e. **Total Len**: Enter a number to indicate the total dial plan length.
4. To save the changes, press `Enter`.

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. To save the changes, press `Enter`.

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. To save the changes, press `Enter`.

Chapter 4: Configuring Session Manager

Adding SIP users

About this task

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

Procedure

1. On your web browser, type `xx.xx.xx.xx/admin`.
   In this URL, `xx.xx.xx.xx` is the IP address of System Manager.
2. Log in with your administrative credentials.
3. On the Home page under **Users** section, select **User Management**.
4. In the left navigation menu, expand **User Management** and select **Manage Users**.
5. Under **Manage Users**, click **New**.
6. In the **Identity** area, specify 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 password to log in to System Manager.
   f. **Confirm Password**. Re enter the password.
   g. **Localized Display Name**. Enter a display name for 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 following fields:
    a. **Type**. Select Avaya SIP from the list.

b. **Fully Qualified Address**. Enter the same extension number as the **Login Name**.
c. **@**. Select the value that must be same as System Manager domain to support SIP endpoints.

12. Click **Add**.
13. In the **Session Manager Profile** area, specify the following fields:
    a. **Primary Session Manager**. Select the Session Manager system you want to add.
    b. **Original Sequence**. Select the same application sequence as defined in System Manager to support SIP IMS users for Communication Manager Feature Server.
    c. **Termination Sequence**. Select the same application sequence as defined in System Manager to support SIP IMS users for Communication Manager Feature Server.
    d. **Survivability Server**. Select None.
    e. **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** section, specify the following fields:
    a. **System**. Select the Management Element defined for Communication Manager Feature Server.
    b. **Use Existing Endpoints**. Select this field if you have already defined an endpoint while adding station in Communication Manager as OPS.
    c. **Extension**. Use the same extension number as you have used in **Login Name** field.
    d. **Template**. Select a template for type of SIP clients.
    e. **Security Code**. Enter the same numeric value that you entered in step 6.
    f. **Port**. Select IP.
    g. **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 user.
15. To save the changes, 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 the Communication Manager SIP trunk group status

Procedure

1. Verify the status of the SIP trunk groups on Communication Manager Evolution Server by using the `status trunk n` command, where `n` is a trunk group number.
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.
5. Use the `list trace tac #` command, where `tac #` is the trunk access code for one of the trunk groups.

   Use the trunk access code to trace the trunk group activity for the SIP trunk between Session Manager and Communication Manager.
6. On Communication Manager, use the `list trace station xxx` command, where `xxx` is the extension number of a SIP telephone.

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 your preferences

Configuring the account settings

About this task

Use this procedure to configure the account settings. You must configure your account before using Avaya one-X® Communicator for Mac OS X application.

Procedure

1. Click the menu icon on your Mac computer, and select **one-X Communicator** > **Preferences**
   Avaya one-X® Communicator for Mac OS X displays the Preferences window.
2. Select the **Account** tab.
3. In the **Server** field, enter the IP address of the Avaya Aura® Session Manager server.
4. In the **Extension** field, enter your extension number.
5. In the **Password** field, enter your password.
6. In the **Domain** field, enter the domain name of the Avaya Aura® Session Manager server.
7. In the **Voicemail** field, enter your voicemail number.
8. From the **Mode** drop-down menu, select a mode.
9. From the **Transport Type** drop-down menu, select the type of protocol.

Related topics:

Account field descriptions on page 32

Account field descriptions

Name	Description
Server	The Internet Protocol (IP) address of the Avaya Aura® Session Manager server.
Extension	Your telephone extension.
Password	Your password.
Domain	The domain name of the Avaya Aura® Session Manager server.
Voicemail	Your Voicemail number.
Mode	The field to select a mode using a drop-down menu.
Transport Type	The field to select a protocol using a drop-down menu. The available options are: • TCP • TLS

Configuring the general preferences

About this task

Use this procedure to configure the preferences for Avaya one-X® Communicator for Mac OS X using the **General preferences** tab.

Procedure

1. From the menu bar, select **one-X Communicator** > **Preferences**
   Avaya one-X® Communicator for Mac OS X displays the Preferences window.
2. Select the **General** tab.
3. Select the **Display alerts for incoming calls** check box if you want to see desktop alerts when someone calls you. You can also answer or reject the call from the call alert window. If you do not select this option, the communicator rings, but does not display any alerts.
4. Select the **Pause iTunes™ playback when receiving or placing calls** check box if you want the communicator to pause iTunes playback when you receive or make a call.

5. Select the **Change iChat™ status to busy when receiving or placing calls** check box if you want the communicator to change your iChat status to busy when you receive or make calls.
6. In the **Status message** field, enter a status message that you want to appear as iChat status when making or receiving a call.

Related topics:

General preferences field descriptions on page 33

General preferences field descriptions

Name	Description
Display alerts for incoming calls	The check box to indicate if display alerts for incoming calls must be activated.
Pause iTunes playback when receiving or placing calls	The check box to indicate if iTunes playback must be paused when placing or receiving calls through Avaya one-X® Communicator for Mac OS X.
Change iChat status to busy when receiving or placing calls	The check box to indicate if iChat status must be changed to busy when placing or receiving calls through Avaya one-X® Communicator for Mac OS X.
Status message	The status message to be displayed on Avaya one-X® Communicator for Mac OS X.

Configuring dialing rules

Before you begin

Ensure you have the following information:

- Number to dial to access an local outside line
- Number to dial for long distance calls
- Number to dial for international calls

About this task

Perform the following actions to configure the dialing rules for your communicator:

Procedure

1. From the menu bar, click **one-X Communicator** > **Preferences**.
   The communicator displays the Preferences window.
2. Select the **Dialing Rules** tab.
3. Enter the following information:
   a. In the **Number to dial to access an outside line** field, enter the number that you need to dial before dialling a local outside telephone number.
   b. In the **Your country code** field, enter your country code.
   c. In the **Your area/city code** field, enter your area code.
   d. In the **PBX main prefix** field, enter the PBX main prefix number.
   e. In the **Number to dial for long distance calls** field, enter the number that you need to dial before dialling a long distance number.
   f. In the **Number to dial for international calls**, enter the number that you need to dial before dialling an international telephone number.
   g. In the **Extension length for internal extension calls**, enter the length of the extension numbers in your organization.
   h. In the **Length of national phone numbers (including area/city code)**, enter the length of the national telephone numbers including the area code.
4. Select the **Include area/city code when making a local call** if you want to include the area code while dialling a local telephone number.

Related topics:

Dialing Rules field descriptions on page 34

Dialing Rules field descriptions

Name	Description
Number to dial to access an outside line	The digits to dial to access an outside line.
Your country code	Your country code.
Your area/city code	The code assigned to your area or city.
PBX main prefix	The main prefix number of your PBX.
Number to dial for long distance calls	The number to dial for making a long distance call.
Number to dial for international calls	The code for gaining access to dial an international phone number.

Name	Description
Extension length for internal extension calls	The number of digits to dial (including area/ city code) for a call within your country.
Length of national phone numbers	The number of digits to dial for making a call to a national phone number.
Include area/city code when making a local call	The check box to indicate if the area or city code must be included in the number for making a local call.

Configuring the directory

Before you begin

To add the enterprise directory of your organization to Avaya one-X® Communicator for Mac OS X, obtain the following information from the system administrator of your organization:

- Domain name of the directory server
- Port number for communication with the directory server
- Search base
- Scope
- Authentication type

About this task

Use this procedure when your Avaya one-X® Communicator for Mac OS X is offline:

Procedure

1. From the menu bar, select **one-X Communicator** > **Preferences**.
   The communicator displays the **Preferences** window.
2. Select the **Directory** tab.
3. In the **LDAP Server** field, enter the domain name of the directory server.
4. In the **Port** field, enter the port number for communication with the directory server.
5. In the **Search base** field, enter the search base.
6. From the **Scope** drop-down menu, select a scope for the directory.
7. From the **Authentication** drop-down menu, select the type of authentication method.
8. In the **User name** field, enter your user name.

9. In the **Password** field, enter your password.

Related topics:

Directory field descriptions on page 36

Directory field descriptions

Name	Description
LDAP Server	The domain name of the public directory server.
Port	The port number of the directory server. The default value is 389.
Search base	The search base. An example is **ou=people**, **o=company**
Scope	The drop-down menu to select a type of scope. The available options are: • Base • One Level • Subtree
Authentication	The drop-down menu to select a type of authentication. The available options are: • None • Simple
User name	User name on the directory server.
Password	Password for the user name.

Configuring advanced preferences

About this task

Perform the following actions to configure advanced preferences for Avaya one-X® Communicator for Mac OS X:

Procedure

1. From the menu bar, select **one-X Communicator** > **Preferences**.
   The communicator displays the **Preferences** window.
2. Select the **Advanced** tab.
3. To use audio QoS, select **Use DSCP / TOS value[1..63]** and specify a value.
4. To use signaling QoS, select **Use DSCP / TOS value[1..63]** and specify a value.
   Differentiated Services Code Point (DSCP) designates different levels of service to be assigned to network traffic. Each packet on the network is marked with a DSCP code corresponding to a level of service.
5. To set diagnostic setting, select **Advanced** > **Diagnostic**.

Related topics:

Advanced field descriptions on page 37

Advanced field descriptions

Name	Description
Audio QoS	The field to enable a measurement type for Quality of Service for audio calls. • None • Use DSCP / TOS value (1...63)
Signaling QoS	The field to enable a measurement type for signalling Quality of Service. • None • Use DSCP / TOS value (1...63)
Video QoS	The field to enable a measurement type for Quality of Service for video calls. • None • Use DSCP / TOS value (1...63)
Turn on logging for troubleshooting	Check box to indicate if logging must be enabled for troubleshooting.

Configuring an emergency number

About this task

Avaya one-X® Communicator for Mac OS X uses the number provided here to reach you during an emergency. Perform the following actions to set an emergency number in Avaya one-X® Communicator for Mac OS X:

Procedure

1. From the menu bar, select **one-X Communicator** > **Preferences**.
   The communicator displays the **Preferences** window.
2. Select the **Emergency** tab.
3. In the **Emergency Number** field, enter the emergency number.

Related topics:

Emergency field descriptions on page 38

Emergency field descriptions

Name	Description
Emergency Number	Emergency phone number

Chapter 7: Port usage

Avaya one-X® Communicator for Mac OS X release 2.0 provides telephony, video, and directory support and do not support Unified Communications functions such as Visual Voicemail and Presence, that Avaya one-X® Communicator for Windows supports. Hence, Avaya one-X® Communicator for Mac OS X uses a subset of the ports used by Avaya one-X® Communicator for Windows.

Table 1: Data Connections Initiated by Avaya one-X® Communicator for Mac OS X

Port number	Protocol	Purpose of the port
80	HTTP	Used to retrieve user profile information from the Personal Profile Manager (PPM) as well as feature and configuration settings as part of Avaya Advanced SIP Telephony (AST). Port 80 is used for HTTP only when SIP TLS is OFF.
443	HTTPS	Used to retrieve user profile information from the Personal Profile Manager (PPM) as well as feature and configuration settings as part of Avaya Advanced SIP Telephony (AST). Port 443 is used for HTTPS only when SIP TLS is ON.
1024~64511	TCP	Used to send messages to SIP Enablement Services or Session Manager.
5000~5040	RTP	Used to transmit audio.
389		Used to communicate with the Lightweight Directory Access Protocol (LDAP) server. **Note:** Customers whose directory services are provided using Active Directory may need to use the *Global Catalog* port instead of producing proper LDAP responses, , see port number 3268.
5060 (TCP) or 5061 (TLS)	SIP	SIP clients use TCP on port number 5060 and TLS on port number 5061 to connect to SIP servers and other SIP end points. Port 5060 is used for non-encrypted signaling traffic, whereas port 5061 is used for traffic encrypted with Transport Layer Security (TLS). Avaya one-X® Communicator for Mac OS X does not support SIP signalling over UDP. Avaya one-X® Communicator for Mac OS X supports SIP signaling over TCP and TLS.
5004-5045	RTP	Used to accept incoming media for voice calls. The exact port is negotiated for each call. However, Avaya one-X® Communicator for Mac OS X limits the range of incoming ports for RTP media to 5004-5045.

Port number	Protocol	Purpose of the port
3268		The use of LDAP to access a corporate directory is optional. Typically port 3268 is used, but an IT department may choose to use a different port for their LDAP server. Avaya one-X® Communicator for Mac OS X has preferences settings for directory access, where the port number can be specified. Both LDAP directory lookup and contacts synchronized from external address books such as Microsoft Exchange and Google are supported.

Chapter 8: Troubleshooting Avaya one-X® Communicator for Mac OS X

The following table provides a basic troubleshooting checklist for Avaya one-X® Communicator for Mac OS X:

Table 2: Troubleshooting Avaya one-X® Communicator for Mac OS X

Problem	Check
Unable to login?	The call server IP extension number and password.
Unable to access voicemail?	Voicemail password
Poor voice quality?	• QoS value • Echo cancellation • Gain control • Noise cancellation
Unable to dial?	Dialing rules
Unable to access the corporate directory?	Corporate directory configuration
Unable to dial external numbers?	Ensure that the dialing rules are properly configured. By default, Communicator prefixes a 1 to the dialed number as the long-distance code.

Appendix A: Appendix A: Security recommendations for administrators

- Use role assignments and assign security groups to appropriately restrict access to operations.
- Instruct users not to share their login ID and password. For accountability, each user must have a unique login ID.
- Periodically review and update the list of administered users, roles, and permissions of the administered users.
- Review administration logs on a regular basis to ensure that the system is operating properly.
- Review audit logs on a regular basis to ensure that the system is operating properly.
- Review security logs and alarms on a regular basis to monitor possible security events.

Index

A

account 31
add 17, 19
    node name 17
    SIP trunks 19
Add 23
    SIP users 23
administer 21
    AAR digit 21
    number plan 21
advanced preferences 36
Avaya one-X Communicator as an endpoint for video calling 20
Avaya one-X Communicator for mac os x 7

C

Communication Manager 13, 27
    configure 13
    SIP trunk group 27
configure 16–18, 20
    IP codec 16
    IP network 17
    route pattern 20
    SIP signaling group 18
    trunk group 18
    trunk transfer 16
configuring 20, 31–33, 35, 36, 38

D

dialing rules 33
directory 35
downloading Avaya one-X® Communicator 11

E

emergency number 38

F

field description 32, 34, 36–38
    account 32
    advanced 37
    dialing rules 34
    directory 36
    emergency 38
field descriptions 33
    general preferences 33

G

general preferences 32

I

IP codec set 16

O

one-X Communicator 39, 41
    port 39
    troubleshooting 41
one-X communicator for mac os x 7, 9, 10, 43
    bandwidth requirement 10
    basic features 7
    overview 7
    prerequisite 9
    prerequisites 10
    related documents 7
    security recommendations 43

R

register 27
    SIP endpoint 27

S

save 22
    translations 22
status 28
    Session Manager 28
    SIP entity 28
synchronize 24
    Communication Manager 24

T

translations 22

V

verify 15
capacity 15
network 15