Installing and Administering Avaya Conference Phone B199

Release 1.0.4
Issue 2
February 2021

Note

Using a cell, mobile, or GSM phone, or a two-way radio in close proximity to an Avaya IP telephone might cause interference.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

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

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. 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.

Shrinkwrap License (SR). End User 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”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

Heritage Nortel Software

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy,

reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Regulatory Statements

Industry Canada (IC) Statements

RSS Standards Statement

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. L'appareil ne doit pas produire de brouillage, et
2. L'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Radio Transmitter Statement

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential

radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Radiation Exposure Statement

This equipment complies with FCC & IC RSS102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Cet équipement est conforme aux limites d'exposition aux rayonnements ISEDétablies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Industry Canada (IC) Statements

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conformeà la norme NMB-003 du Canada.

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Japan Statements

Class B Statement

This is a Class B product based on the standard of the VCCI Council. If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。 VCCI－B

Denan Power Cord Statement

Danger:

Please be careful of the following while installing the equipment:

- Please only use the connecting cables, power cord, and AC adapters shipped with the equipment or specified by Avaya to be used with the equipment. If you use any other equipment, it may cause failures, malfunctioning, or fire.
- Power cords shipped with this equipment must not be used with any other equipment. In case the above guidelines are not followed, it may lead to death or severe injury.

警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

- 接続ケーブル、電源コード、AC アダプタなどの部品は、必ず製品に同梱されております添付品または指定品をご使用ください。添付品指定品以外の部品をご使用になると故障や動作不良、火災の原因となることがあります。
- 同梱されております付属の電源コードを他の機器には使用しないでください。上記注意事項を守らないと、死亡や大怪我など人身事故の原因となることがあります。

México Statement

The operation of this equipment is subject to the following two conditions:

1. It is possible that this equipment or device may not cause harmful interference, and
2. This equipment or device must accept any interference, including interference that may cause undesired operation.

La operación de este equipo está sujeta a las siguientes dos condiciones:

1. Es posible que este equipo o dispositivo no cause interferencia perjudicial y
2. Este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

Brazil Statement

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados

Power over Ethernet (PoE) Statement

This equipment must be connected to PoE networks without routing to the outside plant.

Taiwan Low Power Radio Waves Radiated Devices Statement

802.11b/802.11g/BT:

Article 12 — Without permission granted by the NCC, any company, enterprise, or user is not allowed to change frequency, enhance transmitting power or alter original characteristic as well as performance to an approved low power radio-frequency devices.

Article 14 — The low power radio-frequency devices shall not influence aircraft security and interfere legal communications; If found, the user shall cease operating immediately until no interference is achieved. The said legal communications means radio communications is operated in compliance with the Telecommunications Act. The low power radio-frequency devices must be susceptible with the interference from legal communications or ISM radio wave radiated devices.

低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

U.S. Federal Communications Commission (FCC) Statements

Compliance Statement

The changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating to conjunction with any other antenna or transmitter.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interferences that may cause undesired operation.

Class B Part 15 Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designated to provide reasonable protection against harmful interferences in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interferences to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment . This equipment should be installed and operated with minimum distance of 8 in or 20 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

EU Countries

This device when installed complies with the essential requirements and other relevant provisions of EMC Directive 2014/30/EU and LVD Directive 2014/35/EU. A copy of the Declaration may be obtained from https://support.avaya.com or Avaya Inc., 2605 Meridian Parkway Suite 200. Durham, NC 27713 USA.

BT transmitter

Frequencies for 2402-2479 MHz, transmit power: 10 dBm

General Safety Warning

- Use only the Avaya approved Limited Power Source power supplies specified for this product.
- Ensure that you:
  - Do not operate the device near water.
  - Do not use the device during a lightning storm.
  - Do not report a gas leak while in the vicinity of the leak.
  - For Accessory Power Supply – Use Only Limited Power Supply and products that conform to Radio Equipment Directive, EU directive 2014/53/EU.
- Do not push objects into holes and ventilation slots of the device.
- Do not place a naked flame source, such as lighted candles, on or near the device.
- Do not intentionally hit the device or place heavy or sharp objects on the device.
- Do not attempt to repair the device yourself. Always use a qualified service agent to perform adjustments and repairs.
- Keep the device away from benzene, diluents, and other chemicals.

Trademarks

Device Usage Consent

By using the Avaya device you agree that Avaya, from time to time, may collect network and device data from your device and may use such data in order to validate your eligibility to use the device.

Contents

Chapter 1: Introduction

Purpose

This document provides checklists and procedures for installing, configuring, and administering Avaya Conference Phone B199. It is intended primarily for implementation engineers and administrators.

Change history

Issue	Date	Summary of changes
Release 1.0.4	February 2021	• Updated Phone settings description on page 35 with the Allow Legacy Encryption settings. • Added Provision of the NTP server address on page 45. • Updated Voice quality monitoring on page 55 with the quality estimate metrics and analog parameters. • Added Standard encryption algorithms on page 74. • Updated Avaya Conference Assistant on page 80 in line with the change in MD5 usage. • Added Expansion microphone firmware upgrade on page 87. • Updated Bluetooth connection on page 91 with information on switching between the Bluetooth modes. • Updated Configuration file structure on page 98 with new parameters.

Table continues…

Issue	Date	Summary of changes
Release 1.0.3	October 2020	• Updated Phone settings description on page 35 with the date, date format, time, time format, Daylight Saving Time (DST) mode, timezone and Custom DST settings. • Added Daylight Saving Time on page 42. • Added Minute offset on page 43. • Added Time format on page 44. • Added Bluetooth radio on page 94. • Updated Firmware upgrade using check-sync on page 97 with the reboot parameter values. • Updated Configuration file structure on page 98 with new parameters. • Added Firmware downgrade with DES provisioning on page 112. • Updated Certificate configuration files on page 117 with the information about the paths to the certificates, MD5 checksum, and certificate configuration file structure.
Release 1.0.2	August 2020	• Added Sleep mode on page 46. • Added Voice quality monitoring on page 55. • Added Bluetooth connection on page 91. • Added LDAP settings on page 59. • Updated Configuration file structure on page 98 with new parameters.
Release 1.0.1	March 2020	• Updated the Media settings description on page 54 with SRTP disablement. • Added Firmware upgrade and downgrade on page 96. • Added a note in Firmware upgrade using check-sync on page 97. • Added Validation and migration of configuration on page 107 to the Maintenance chapter. • Updated Device Management on page 108 with information on the phone provisioning with Device Enrollment Services. • Added Upgrading multiple devices on page 122. • Added Remote syslog server on page 123 to the Device Management section. • Added a note in Factory reset on page 125 on Device Enrollment Services feature behavior after factory reset.

Chapter 2: Overview

Phone overview

Avaya Conference Phone B199 is a SIP conference phone that you can use to make calls and hold conferences with a great audio quality. It provides an improved user experience and ensures an easier connection to audio conference bridges. The phone is based on a multi-connectivity platform to leverage the “Bring your own device” approach.

The features of the conference phone include a simple-to-use 4.3 inch graphical LCD with a backlight and volume control and mute buttons. Two more mute key buttons are located along the perimeter of the device. You can attach additional expansion microphones or cascade three B199 devices in a daisy chain to expand the audio distribution and pickup in the room.

B199 Conference Phone is supported in the Avaya network through the Avaya Aura® communication solutions and IP Office.

Safety guidelines

Ensure that you are familiar with the following safety guidelines before using, installing, configuring, and administering Avaya Conference Phone B199.

Note:

This conference phone is not designed for making emergency telephone calls when the power fails. Make alternative arrangements for access to emergency services.

- Read, understand, and follow all the instructions.
- Do not place this phone on an unstable cart, stand, or table. If the phone falls, serious damages can be caused to the device.
- Do not drop, knock, or shake the phone. Rough handling can break internal circuit boards.
- Ensure that the power cord or plug is not damaged.
- Do not overload wall outlets and extension cords as this can result in the risk of fire or electric shock.
- Avoid wetting the device to prevent fire or electrical shock hazard.

- Unplug the device from the wall outlet before cleaning. Do not use liquid or aerosol cleaners, harsh chemicals, cleaning solvents, or strong detergents to clean the device. Use a damp cloth for cleaning.
- Avoid exposing the phone to high temperatures above 40°C (104°F), low temperatures below 0°C (32°F), or high humidity.
- Do not block or cover slots and openings of the phone. These openings are provided for ventilation, to protect the phone from overheating.
- Never push objects of any kind into this phone through cabinet slots as they might touch dangerous voltage points or short out parts that could result in a risk of fire or electric shock.
- Do not disassemble this product to reduce the risk of electric shock. Opening or removing covers may expose you to dangerous voltages or other risks. Incorrect reassembly can cause electric shock during subsequent use.
- Do not use the phone to report a gas leak in the vicinity of the leak.
- Do not use the phone near intensive care medical equipment or close to persons with pacemakers.
- Do not place the phone too close to electrical equipment such as answering machines, TV sets, radios, computers, and microwave ovens to avoid interference.

Important:

In case B199 Conference Phone and the corresponding accessories are damaged, the device does not operate normally or exhibits a distinct change in performance, refer for servicing to the qualified service personnel.

Physical layout

Figure 1: Front view of Avaya Conference Phone B199

The following table lists the buttons and the other elements of Avaya Conference Phone B199.

Callout number	Description
1	Mute buttons
2	Volume down button
3	Volume up button
4	NFC tag
5	Touch screen
6	LED status indicators

Connection layout

Figure 2: Connection layout of Avaya Conference Phone B199

The following table lists the sockets and ports available on Avaya Conference Phone B199 for connection.

Callout number	Description
1	PoE/Ethernet connection socket
2	USB Type A
3	Micro-USB Type B
4	Audio expansion ports
5	Kensington® security lock port
6	NFC tag for Bluetooth

Dimensions

The following table shows the dimensions of Avaya Conference Phone B199.

Parameter	Dimension
Width	326.41 mm
Length	369.87 mm
Height	74.7 mm

Icons

Icons on the home screen of Avaya Conference Phone B199

Icon	Name	Description
	Recent	To check the call list. The phone provides the following information about the calls: • Number. View the phone number of the contact. • Date. View the information when the phone received the call. This applies only to the calls preceding the current day. • Time. For the current day, the phone shows the time of the call in the convenient time format. • Direction. View the incoming, outgoing and missed calls.
	Conference Assistant	To access the Avaya® Conference Assistant settings.
	Call	To dial phone numbers and codes for telephone operations or Avaya® Conference Assistant connection.
	Settings	To check and configure the settings from the phone. View the phone status and reach the menu.
	Microphone Muted	To mute and unmute the phone.
	Volume Up	To increase the phone volume level.
	Volume Down	To decrease the phone volume level.
	NFC	To indicate the built-in NFC tag.

Other icons of B199 Conference Phone

Icon	Name	Description
	Make Call or Answer	To indicate the phone off-hook status and answer an incoming call.
	Hang Up	To indicate the phone on-hook status and end a call.
	Incoming	To show an incoming call.
	Outgoing	To show an outgoing call.
	Missed	To indicate a missed call.
	Hold or On Hold	To put a call on hold or to indicate that a call is on hold.
	Conference	To arrange a conference call.
	Split	To split a conference call into several separate calls.
	Add Participant	To add a participant to a conference call.
	Talk Private	To arrange a private discussion with a participant of a conference call.
	Caps	To type in capital letters.
	Delete	To delete an unneeded number or letter.
	Visibility	To mark whether the characters must stay visible to the user, for example, when logging in with the password.
	Invisibility	To mark whether the characters must stay invisible to the user, for example, when logging in with the password.
	Logged In	To indicate that the user logged in as the administrator.
	Microphone Muted	To indicate that the phone is in muted state.

Table continues…

Icon	Name	Description
	Enter	To confirm the input of information.
	Confirm	To confirm the information.
	Reject	To discard the information.
	Arrow Down	To move to the sections below.
	Arrow Up	To move to the sections above.
	Arrow Left	To return to the previous page.
	Arrow Right	To move to subsections of a section.
	USB Connected	To indicate an active USB connection.
	Avaya® Conference Assistant connected	To show the connection of the phone to Avaya® Conference Assistant.
	Daisy Chain Mode	To indicate that the phone is in a daisy chain mode.
	Loading	To show that the phone is loading the new version of the firmware or new setting from DES server.
	DES warning icon	To notify the user of issues which occurred during the automatic provisioning process performed using Device Enrollment Services.
	Contacts	To show that the LDAP external phone book is available.
	Bluetooth connection	To indicate an active Bluetooth Classic connection.
	Call Transfer	To show that it is possible to transfer an ongoing call to another contact person.

Prerequisites

Avaya Conference Phone B199 is based on a multi-connectivity platform to support the “Bring your own device” use case. Connect your B199 Conference Phone to a SIP server using the Ethernet.

The following table describes the tasks you must perform before setting up your B199:

No.	Task	Notes	✔
1	Review prerequisite information.	If you do not have all the required software and hardware, B199 Conference Phone might not function as expected.	
2	Gather pre-installation data.	Pre-installation data is required to perform initial parameter setup and to create user accounts for B199 Conference Phone.	
3	Ensure that the Avaya Conference Phone B199 package contains all the required components and accessories.	Connect optional components and accessories to B199 Conference Phone. Perform this task to use the optional components and accessories with your device.	
4	Connect B199 Conference Phone to a power supply and to the network.		

Software and hardware prerequisites

Install and configure:

- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- A DHCP server for providing dynamic IP addresses
- A file server, an HTTP/HTTPS for downloading software distribution packages and the settings file
- Avaya® Conference Assistant

B199 Conference Phone requires the current version of Avaya® Conference Assistant to be installed.

Server configuration checklist

The following table describes the tasks related to server configuration that you must perform for the initial installation of Avaya Conference Phone B199.

No.	Task	Notes	✔
1.	Ensure that you have all required licenses for the DHCP and file server software.	Contact your server software vendors to obtain information about server licensing.	
2.	Ensure that a DHCP server is installed and configured.	Contact your DHCP server vendor to obtain installation documentation.	
3.	Ensure that a file server is installed and configured.	Contact your file server vendor to receive installation documentation.	

Power supply connectivity

Avaya Conference Phone B199 uses 10/100/1000 Mbit Ethernet and supports PoE Type 1 and Type 2 power supply, which means either 15W or 30W at the power distribution unit.

Operation modes:

- PoE 802.3af 15W
- PoE 802.3at 30W

Note:

If your LAN does not support the PoE 802.3af 15W/PoE 802.3at 30W specification, use the AC power adapter, which you can purchase with the device.

Connection to other devices

Avaya Conference Phone B199 is based on a multi-connectivity platform and uses the following features and ports to connect to devices such as a personal computer, expansion microphones, and another B199 Conference Phone:

- Bluetooth Classic
- Bluetooth LE
- Built-in NFC tag
- USB Type A
- Micro-USB Type B
- Audio expansion ports

Specifications

The following table lists the specifications that Avaya Conference Phone B199 supports:

Name	Description
Power	• PoE 802.3af • PoE 802.3at • PoE injector available as an accessory
Connectivity	• Ethernet RJ45 10/100/1000 Mbps, PoE 802.3af, and PoE 802.3at • USB 3.0 device • Built-in Bluetooth LE and NFC • Bluetooth Classic (HFP, A2DP) • Daisy Chain (audio) ports (6-pin RJ-type)
Screen	Graphical touch screen with a resolution of approximately 480 x 800 and size of 4.3”
Acoustics	• 3 symmetrically placed MEMS microphones • Full range speaker in the sealed enclosure
Music	• PoE 802.3at: 91 dB and bass boost • PoE 802.3af: 87 dB • Daisy Chain: 91 dB
Speech	• PoE 802.3at: 91 dB • PoE 802.3af: 87 dB • Daisy Chain: 91 dB
USB	Micro USB 3.0 device Type B
Bluetooth	• Bluetooth LE • Bluetooth Classic (HFP, A2DP)
Accessories	You can additionally purchase the following accessories: • Avaya PoE kit • Avaya Smart Microphones • Avaya Daisy Chain kit
User interface	• Simplified user interface • Functional keypad and dial pad • LED indicators for call and connectivity status
Mobile app	Avaya® Conference Assistant. With the app, you can access your mobile phone contact book and calendar. The app is available for free at AppStore and Google Play
Operation environment	• Avaya Aura® • IP Office

Table continues…

Name	Description
Interoperability with PBX and platforms	• Broadsoft • Zang Office • Ring Central

Chapter 3: Initial setup and configuration

Configuration of Avaya Conference Phone B199

Configure Avaya Conference Phone B199 directly from the phone or adjust the settings through the web interface. Use the web browser of a PC connected to the same network to conduct the initial setup of the phone, its registration in the network, and settings in B199 Conference Phone. Through the web interface, you can view logs, update software, and create configuration files.

Note:

Avaya Conference Phone B199 officially supports only the Google Chrome browser.

The administrator can always change the administrator password. By default, the administrator password is not set. You must set it when you first activate B199 Conference Phone or after you reset the phone to the factory settings.

Important:

You must enter correct administrator password to change configuration of the phone. For that, you must always remember your password.

Setting the password for Avaya Conference Phone B199

About this task

Use this procedure to set the password for your B199 Conference Phone when you first activate the phone or after a reset to the factory settings.

Before you begin

Connect the PoE cable to ensure the phone power supply.

Procedure

1. Wait for the following message to appear on the phone screen:

   `For full functionality, please set administration password.`

2. Tap **Yes** to set the password.
3. **(Optional)** Tap **Skip** to avoid setting the password.

   In this case, B199 Conference Phone will be functioning in the administration mode, and you will be able to configure settings on the phone. However, you will not be able to access the web interface.

4. Using the keyboard on the phone screen, type your password. It can contain letters, numbers, and special characters.

   The password must contain at least 4 characters. As you enter the password, the phone informs if the password has acceptable length.

5. Type the password again to confirm it.
6. Tap the < icon three times to return to the home screen.

   The phone reboots.

Setting up a DHCP server

About this task

Avaya Conference Phone B199 supports any DHCP server software as long as the software is correctly configured.

Before you begin

Contact your server software vendor to obtain server software installation and configuration instructions.

Procedure

1. Install the DHCP server software according to the server software vendor's instructions.
2. Configure the IP address for the phone.

Next steps

You must configure the required DHCP options to connect to the network with DHCP.

Related links

Network settings description on page 48

Connecting to a network with DHCP

About this task

Use this procedure to connect to a network with DHCP from your phone or through the web interface.

- To connect to the network with DHCP from B199 Conference Phone, do the following:

  1. Log in as the administrator.
  2. Tap **Network**.
  3. Enable DHCP.
  4. Tap the < icon twice to return to the home screen.

     The phone reboots.

- To connect to the network with DHCP through the web interface, do the following:
  1. On the web interface, click **Network**.
  2. Enable DHCP.
  3. Click **Save**.

     The phone reboots.

Viewing the IP address

About this task

View the IP address of your Avaya Conference Phone B199. Use this address to log into the web interface of the conference phone and manage the settings in the device through the web browser.

Procedure

1. On the phone screen, tap **Settings**.
2. Tap **Status** or the > icon.

   The phone displays the following hardware details:

   - DES Status
   - IP Address
   - MAC Address
   - Bluetooth MAC Address
   - Hardware Revision
   - Software Version
   - Smart Mic 1 Version
   - Smart Mic 2 Version
3. Tap the < icon twice to return to the home screen.

Setting a static IP address

About this task

Use this procedure to connect to the network using a static IP address, and not with DHCP.

Before you begin

Disable DHCP.

Obtain the IP address, netmask, gateway, DNS 1, and DNS 2.

- To set the static IP address from the phone, do the following:
  1. Log in as the administrator and tap **Network**. If the administrator password is not set for the phone, on the phone screen, tap **Settings** > **Network**.
  2. Tap **Static IP**, and enter the following:
     - IP address
     - Netmask
     - Gateway
  3. Return to the home screen to save the changes.
- To set the static IP address through the web interface, do the following:
  1. On the web interface, click **Network**.
  2. In the Static IP section, enter the following:
     - IP address
     - Network mask
     - Gateway
  3. Click **Save**.

     The phone reboots.

Logging in to the web interface of Avaya Conference Phone B199

About this task

Use this procedure to log in to the web interface of your B199 Conference Phone. You can access the web interface only if you set the administrator password for your phone.

Note:

B199 Conference Phone officially supports only the Google Chrome browser.

The phone supports only HTTPS communication protocol.

Before you begin

Obtain the IP address and the administrator password for the phone.

Procedure

1. On the web browser, type the IP address of your phone in the following format:

   `https://111.222.33.44/.`
2. Enter password in the **Password** field.

   The password is the administrator password for your phone.

3. Click **Login** to log in to the web server of your B199 Conference Phone.

Logging out from Avaya Conference Phone B199

About this task

Use this procedure to log out from the web server of your B199 Conference Phone from your web browser.

Before you begin

You must be logged in to the web interface of your conference phone.

Procedure

On the web browser, click **Logout**.

You are forwarded to the Login page and see the prompt that you are not logged in.

Registering an account on the phone

About this task

Use this procedure to register an account on the phone.

Avaya Conference Phone B199 supports three accounts: the primary account, the secondary account and the fallback account. The phone uses the primary account to make and receive calls. You can register the secondary account simultaneously with the primary account but the phone uses it only to receive calls. The secondary account can be used to make call if the phone fails to register to the primary account. You must register the fallback account only if the phone fails to register to both primary and secondary accounts.

Before you begin

You must have access to the account information and all necessary settings that the SIP PBX requires.

Procedure

1. Log in as the administrator and tap **SIP**. If the administrator is not set for the phone, tap **Settings** > **SIP**.
2. Tap **Primary Account**, and enter information in the following fields:
   - **Account Name**: The name that the phone shows on the screen. You can set it based on your corporate standards.
   - **User**: The account name. The phone uses the content of this field to construct the user Universal Resource Identifier (URI). Note that if **User** is not specified, the phone is not able to make a registration request.
   - **Registrar Address**: The IP address or the public name of the SIP server where the account is registered. It can be in `10.10.1.100` format for a local SIP server or in `sip.company.net` format for a public VoIP service provider.

- **Proxy**: The proxy server the company uses for Internet communication. This field can be left blank.

3. Enable **Keep Alive**.

   This will ensure a persistent connection for this account.

4. Tap **Credentials**, and enter information in the following fields:
   - **Realm**. Realm is a protection domain where the SIP authentication name and password is valid.
   - **Authentication Name**. If this parameter is not specified, the phone uses the content of the **User** field to authenticate.
   - **Password**. The phone uses this password for the **Realm** authentication.
5. Tap the < icon to return to the account registration menu.
6. **(Optional)** Enter **Registration Timeout** value in seconds.

   This is a request to the SIP server that specifies when the registration must expire. B199 Conference Phone automatically renews the registration within the set period if the phone is still on and connected to the server. By default, it is 300 seconds.

7. Tap the < icon to return to the SIP menu.

Next steps

Repeat Steps above for the secondary and fallback accounts.

Registering an account through the web interface

About this task

Use this procedure to register an account for Avaya Conference Phone B199 through the web interface.

Before you begin

You must have access to the account information and all necessary settings that the SIP PBX requires.

Procedure

1. On the web interface, click **SIP**.
2. In the Primary Account section, enter information in the following fields:
   - **Account Name**
   - **User**
   - **Registrar**
   - **Proxy**: This field can be left blank.
   - **Registration Timeout**

- **Realm**: A protection domain where the SIP authentication name and password is valid.

  The realm is usually the same as the registrar. If you enter an asterisk (*), the phone responds to any realm. If there is a specific realm, the phone responds only to that realm when asked for credentials.
- **Authentication Name**
- **Password**: The password for the **Realm** authentication.

3. Enable **Keep Alive**.
4. **(Optional)** Repeat Steps above for the secondary and fallback accounts.
5. Click **Save**.

   The phone restarts the application to apply the changes.

Chapter 4: Registration in the network

Registration in the Avaya network

You must register Avaya Conference Phone B199 in the Avaya network to use all communication solutions available. Registration starts with creating a communication profile for the phone with an Avaya Aura® Communication Manager endpoint profile and an Avaya Aura® Session Manager profile.

The Avaya Aura® Communication Manager endpoint profile associates the user with a station on Avaya Aura® Communication Manager. Avaya Aura® Communication Manager delivers rich voice and video capabilities and provides a resilient, distributed network of gateways and analog, digital, and IP-based communication devices. It includes advanced mobility features, built-in conference calling and contact center applications, and E911 capabilities.

Avaya Aura® Session Manager is the core of an Avaya Session Initiation Protocol (SIP)-based architecture. The Avaya Aura® Session Manager platform makes it possible to securely unify media, networks, devices, and applications and realtime, actionable presence across a common infrastructure. It creates an on-demand access to services and applications that define the engagement experience. The Avaya Aura® Session Manager profile creates a unique user identity and assigns to it the primary and secondary Avaya Aura® Session Manager, relevant application sequences, and the survivability server.

You must also register the phone to a SIP switch to make and receive calls. The switch can be a company PBX or located with an IP telephony service provider. The SIP switch ensures that the call is connected to the right address within the network. If the recipient is not registered as an IP telephone in the same switch, it sends the call to the public telephone network. IP Office is a single, stackable, scalable communications system, after the registration in which B199 Conference Phone receives extensions required for telephony operations.

Configuring the Avaya Aura® Session Manager profile

About this task

Use this procedure to configure the Avaya Aura® Session Manager profile for Avaya Conference Phone B199.

Before you begin

Connect to the Avaya Aura® System Manager web console. The tool is available on the Avaya Support website at http://support.avaya.com.

Procedure

1. On Avaya Aura® System Manager web console, click **Users**, and then click **User Management** > **Manage Users**.

   The screen displays a list of users.

2. On the User Management page, click **New** to create a new endpoint.

   The screen displays a new user profile.

3. Configure the settings in the Identity tab.
   a. In the **Last name** field, type your last name or `Avaya` as the brand name for the phone.
   b. In the **First name** field, type your first name or the phone model.
   c. **(Optional)** In the **Middle name** field, type your middle name or any other name of the phone that you use.
   d. In the **Login name** field, type a customized login name for the phone.
   e. In the **Authentication type** field, click **Basic**.
   f. In the **Source** field, specify **Local**.
   g. In the **Language** field, click the necessary language.

      The default option is English.

   h. **(Optional)** Specify the information in other fields.

4. Configure the settings in the Communication profile tab.
   a. Enable the **Primary** name or choose a name.
   b. Select the **Default** option.
   c. On Communication address, specify the type, handle, and domain of your phone. You can use **Avaya SIP** for the **Type**.
   d. Select **Session Manager profile** and check the information available. You can leave the **Secondary Session Manager** field empty.
   e. On the Endpoint profile, select the system version, and for **Profile type** click **Endpoint**.
   f. On the Endpoint profile, click **View Endpoint** to get the extension of the phone.
   g. On the Endpoint profile, type the port number in **Port** and the phone type in **Set Type**.

      As the type, put `9611SIP` for Avaya Aura® 7.0, and `B199SIP` for Avaya Aura® 8.0.

5. Click **Done** in the upper-right corner.

   When you add a user in Avaya Aura® Session Manager, Avaya Aura® System Manager automatically creates a station in Avaya Aura® Communication Manager.

Configuring the Avaya Aura® Communication Manager profile

About this task

Use this procedure to configure the station associated with the Avaya Aura® Communication Manager endpoint profile of the phone. You must do it to use the conference features of Avaya Conference Phone B199.

Before you begin

- Get the user credentials for Avaya Aura® Communication Manager. The software is available on the Avaya Support website at http://support.avaya.com.
- Get the ID of the B199 Conference Phone station.

Procedure

1. Log in to Avaya Aura® Communication Manager.
2. Type `sat` to open the System Administration Terminal (SAT) interface.
3. At the command: prompt, type `change station` and type the station ID.
4. In **Button assignments**, assign 4 call appearances to the phone.

   The phone displays 4 lines with the following text: `call-appr`.

Verifying the phone registration

About this task

Use this procedure to check the phone registration with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

Procedure

1. On the phone screen, check for the account name.

   The registration is complete if the phone displays the account name.
2. **(Optional)** If the phone displays `Not registered`, reconfigure the Avaya Aura® Session Manager and Avaya Aura® Communication Manager profiles to complete the registration.

Configuration of IP Office

IP Office is a hybrid PBX that you can use in your unified communications environment. The system uses a mixture of analog, proprietary digital, proprietary VoIP, and SIP protocols.

It supports Avaya Conference Phone B199 within the IP Office system. You must register B199 Conference Phone with IP Office by using an *Avaya IP Endpoint* license. The number of extensions supported is subject to available licenses and to the normal extension limits of the used IP Office control unit.

To install the phone on an IP Office system, follow the '*Generic Installation Process*' outlined in the *IP Office SIP Telephone Installation Notes* manual.

IP Office call limitation for Avaya Conference Phone B199

With R.1.0.2 and earlier, an attempt to make a call over any trunk fails if an account code is configured in IP Office for such a call. This happens because the user does not have the option to enter the account code.

Chapter 5: Settings configuration and management

Configuration of settings on Avaya Conference Phone B199

You can configure almost all settings directly on your B199 Conference Phone. For that you need to navigate through the menu and select the options you need. Using the web interface makes the settings configuration easier. This guide explains both options for you to choose the more convenient one.

The basic settings, such as the phone name, language, and ring level, can be modified by any user. To configure other settings you must log in as the Administrator.

Phone settings

You can configure the phone settings during the installation of Avaya Conference Phone B199 or any time after it. The phone settings include the following:

- Phone Name
- Phone Language
- Ringtone Level
- Key Tone
- Reboot Device
- Webapp Debug
- Daisy Chain Mode
- Factory Reset
- Admin Password
- Time and Region
- Startup Sound

Related links

Phone settings description on page 35

Configuring the phone settings on the phone

About this task

Use this procedure to configure the phone settings on the phone.

Procedure

1. On the phone screen, tap **Settings** > **Phone**.
2. Choose the parameter that you want to configure and proceed to the options available.

   You must log in as the administrator to change the password, set time settings, choose the Daisy Chain mode or reset the phone to factory settings.
3. After you made the choices, return to the home screen.

   Depending on what parameters you change, the phone restarts the application or reboots.

Configuring the settings through the web interface

About this task

Use this procedure to configure the settings through the web interface of your Avaya Conference Phone B199. Note that only administrator can configure all the settings.

Procedure

1. Log in to the web interface.
2. Click **Phone**.
3. Choose the parameter that you want to configure and proceed to the options available.
4. Click **Save**.

Phone settings description

The following table lists the basic settings of Avaya Conference Phone B199 available through the web interface in the **Phone** tab or on the phone in **Settings** > **Phone** and **Settings** > **Admin Login** > **Phone**.

Name	Description
Phone	
Phone Name	To specify the name of the phone, which is visible on the home screen when the phone is in a stand-by or on-hook mode. The default name is Conference Phone.

Table continues…

Name	Description
Phone Language	To select the language. The options are: • English. This is the default setting. • Swedish • Danish • Norwegian • Finnish • Italian • German • French • Spanish • Portuguese • Dutch • Simplified Chinese The characters on the B199 keyboard match the selected language for all languages except Simplified Chinese. For Simplified Chinese, B199 uses English keyboard layout.
Security	
Allow Legacy Encryption	To enable or disable legacy encryption for backward compatibility. By default, the legacy encryption mode is disabled. **Note:** You can configure this parameter if you logged in with the administrator password.
Admin Password	To change the administrator password. **Note:** You can configure this parameter if you logged in with the administrator password. **Important:** For security reasons, you can change the administrator password only on the phone.
Ringtone Level	To choose from six volume levels and a Silent mode. The default setting is Level 4. If you select the Silent mode, only the green LEDs on the phone flash when a call is received.
Key Tone	To enable or disable the key click sound as you tap the phone screen buttons. By default, the key tone is on.

Table continues…

Name	Description
Reboot Device	To reboot the phone when needed. **Note:** You can use this function only through the web interface.
Webapp Debug	To enable or disable the debugging function for the web application. It activates the web application logging available in the System Logs tab. By default, Webapp Debug is off. **Note:** You can use this function only through the web interface.
Daisy Chain	To choose a mode, in which your B199 Conference Phone operates in case of a daisy chain arrangement. The options are: • **Master**. This is the default setting. • **Slave** **Note:** You can configure this parameter on the phone if you log in with the administrator password. The administrator can also configure this parameter using the .xml configuration file.
Factory Reset	To reset the phone to its factory settings. By resetting the phone to its factory settings, you remove all the configurations set, imported and installed in course of the phone use. **Note:** You can do the factory reset only if you log in with the administrator password and only on the phone.
Startup Sound	To enable or disable the phone's branded startup sound. By default, the startup sound is on. **Note:** The change of this setting does not require a restart or reboot of the phone.
Time and Region	
NTP Enable	To enable or disable the Network Time Protocol (NTP). By default, NTP is enabled. **Note:** You can configure this parameter if you logged in with the administrator password.

Table continues…

Name	Description
NTP Server	To specify the NTP server when NTP is enabled. By default the phone uses the following NTP server: `0.pool.ntp.org`. **Note:** You can configure this parameter if you logged in with the administrator password.
Date	To set the current date. **Note:** You can set the current date manually only if NTP is in disabled state. Specify the date by doing the following: • Manually enter the date in the field by clicking the day, month, and year to change the value. • Select a date from the date picker. **Note:** You can use this function only through the web interface.

Table continues…

Name	Description
Date Format	To set the date format. The following date formats are available: • `dd M, D` - Date, short name for the month and day of the week. For example, *10 Jan, Mon*. • `dd MM, DD` - Date, full name for the month and day of the week. For example, *10 January, Monday*. • `M dd, D` - Short name for the month, date, and short name for the day of the week. For example, *Jan 10, Mon*. • `MM dd, DD` - Full name for the month, date, and full name for the day of the week. For example, *January 10, Monday*. • `D, dd M` - Short name for the day of the week, date, and short name for the month. For example, *Mon, 10 Jan*. • `DD, MM dd` - Full name for the day of the week, full name for the month, and date. For example, *Monday, January 10*. • `dd/mm/yy` - Date/month/short numerical designation of the year. For example, *10/01/20*. • `dd/mm/yyyy` - Date/month/full numerical designation of the year. For example, *01/10/2020*. • `mm/dd/yy` - Month/date/short numerical designation of the year. For example, *01/10/2020*. • `mm/dd/yyyy` - Month/date/full numerical designation of the year. For example, *01/10/2020*. • `yy/mm/dd` - Short numerical designation of the year/month/date. For example, *20/01/10*. • `yyyy/mm/dd` - Full numerical designation of the year/month/date. For example, *2020/01/10*. You can also leave the **Default** format of the date. In this case your B199 Conference Phone applies the date format that is standard for the selected language. For example, if your selected language is Finnish, the date format is `dd.mm.yyyy`. **Note:** You can configure this parameter only through the web interface. The administrator can also configure this parameter using the .xml configuration file.

Table continues…

Name	Description
Time	To set the current time. **Note:** You can set the time manually only if NTP is in disabled state. See the time on the home screen of the phone. Set the time by doing the following: • Manually enter the time value in the field by clicking the hours, minutes, and seconds to change the value. • Select the time from the time picker. **Note:** You can use this function only through the web interface.
Time Format	To set the time format. When you select the language, the time format automatically changes to the standard time format for the chosen language. You can manually change the convenient time format. The following time formats are available: • Default • 12 hours • 24 hours **Note:** You can configure this parameter through the web interface. The administrator can also update settings with the .xml configuration file.
Geo Timezone (auto DST)	To enable or disable the Daylight Saving Time (DST) mode based on the selected geographical timezone. By default, DST is disabled. **Note:** You can use this function only through the web interface.

Table continues…

Name	Description
Timezone	To specify a timezone and minute offset. The available timezone is based on **Geo Timezone (auto DST)** being enabled or disabled. With **Geo Timezone (auto DST)** disabled, the phone sets the time as a difference with the Coordinated Universal Time (UTC). You can specify the minute offset for the selected UTC time zone. The possible minute offset values are 0, 15, 30, and 45. With **Geo Timezone (auto DST)** enabled, the phone specifies the timezone based on the country and the city observing the DST. The default setting is UTC. **Note:** You can configure this parameter through the web interface. The administrator can also update settings with the .xml configuration file.
Custom DST	To enable or disable the custom DST mode. If **Geo Timezone (auto DST)** is enabled, **Custom DST** is automatically disabled. You can use the custom DST functions only with the enabled **Custom DST**. **Note:** You can configure this parameter through the web interface. The administrator can also update settings with the .xml configuration file.
Custom DST Settings	
Offset Hours	To specify the time in hours between the standard time and the DST. The values are 1 and 2. The default setting is 1.
Start Month	To select the month when to apply **Offset Hours**.
Start Day Mode	To select the day mode when to apply **Offset Hours**.
Start Day	To select the day when to apply **Offset Hours**.
Start Hour	To select the hour when to apply **Offset Hours**.
Stop Month	To select the month when to stop applying **Offset Hours**.
Stop Day Mode	To select the day mode when to stop applying **Offset Hours**.
Stop Day	To select the day when to stop applying **Offset Hours**.
Stop Hour	To select the hour when to stop applying **Offset Hours**.

After you click **Save** in the web interface, the phone saves the changes and restarts the application or reboots, depending on what parameters you changed. To save changes on the phone, you must return to the home screen, and the phone restarts the application or reboots to apply them.

Daylight Saving Time

Together with the UTC timezones, B199 Conference Phone supports the Daylight Saving Time (DST) feature, which advances the clock during the specified period of time. Activate this feature manually through the web interface by enabling **Custom DST**. The **Custom DST** settings card provides for defining a required transition date.

Configuring Daylight Saving Time through the web interface

About this task

Use this procedure to configure DST offset through the web interface.

Important:

When you use the DST start parameters, enable the comparable DST stop parameters.

Procedure

1. Log in to the web interface.
2. Click **Phone**.
3. Enable **Custom DST**.
4. In the **Offset Hours** field, specify the time in hours between the standard time and the period when the DST parameter is active.

   The values are 1 and 2. The default setting is **1**.
5. In the **Start Month** field, select the month to apply the DST offset.
6. In the **Start Day Mode** field, select the day mode to apply the DST offset.
7. In the **Start Day** field, specify the day to apply the DST offset.

   The value range depends on the selected **Start Day Mode**. For example, if you select **Day of month** as the day mode, the value range is from 1 to 31. The value range for the weekday is from 0 to 7. Note that in this case, **0** and **7** mean Sunday.

   When **Start Day Mode** is 0, the start day is a day of the month. In case of other values, the day is a day of the week: 1 is Monday, 5 is Friday. If **Start Day Mode** is 2 and **Start Day** is 5, you define the second Friday in the month.

   The values -1 to -5 show a weekday in the month from the month end. If **Start Day Mode** is -1 and **Start Day** is 5, this is the last Friday in the month.
8. In the **Start Hour** field, specify the hour to apply the DST offset.
9. In the **Stop Month** field, select the month to stop applying the DST offset.
10. In the **Stop Day Mode** field, select the day mode to stop applying the DST offset.
11. In the **Stop Day** field, specify the day to stop applying the DST offset.

The value range depends on the selected **Stop Day Mode**. For example, if you select **Day of month** as the day mode, the value range is from 1 to 31.

12. In the **Stop Hour** field, specify the hour to stop applying the DST offset.
13. Click **Save**.

Daylight Saving Time state

Check the Daylight Saving Time state on the status page. The following options are available:

- **On** shows that the DST is active. This happens when you configure a UTC timezone, enable **Custom DST**, and the current date is between the DST start day and DST stop day. In this case, you can add the offset to the current time.
- **Off** demonstrates that the DST is not active. This happens when you configure a UTC timezone with the **Custom DST** disabled, or the current date is not between the DST start day and DST stop day. In this case, you cannot add the offset to the current time.
- **Auto** means that there is a Geo timezone set, and the phone ignores the **Custom DST** settings. In this case, the DST settings are managed automatically.
- **Unknown** shows that the required information is currently unavailable. You must refresh the page and check it later.

Minute offset

B199 Conference Phone supports the minute offset of the specified UTC time zone. You can set the UTC time zone offset to 0, 15, 30, or 45 minutes.

Configuring the minute offset through the web interface

About this task

Use this procedure to configure the minute offset through the web interface.

Procedure

1. Log in to the web interface.
2. Click **Phone**.
3. In the Time and Region section, disable **Geo Timezone (auto DST)**.
4. In the **Timezone** field, configure the following:
   a. In the first drop-down list, select the UTC time zone.
   b. In the second drop-down list, select the minute offset for the specified UTC time zone.
5. Click **Save**.

Configuring the minute offset using the configuration file

About this task

Use this procedure to configure the minute offset using the .xml configuration file.

Before you begin

Obtain the configuration .xml file for Avaya Conference Phone B199.

Procedure

1. In the configuration file, go to the `<time>` section.
2. Set the value in the `<timezone>` tag to your preferred UTC time zone:

   ```
   <timezone>UTC+7</timezone>
   ```

3. To specify the minute offset, add the minute offset value to the specified timezone.

   ```
   <timezone>UTC+7:15</timezone>
   ```

   The UTC time zone offset is set to 15 minutes.

4. Save the configuration file.

Next steps

Upload the configuration file to the Device Management server or import the configuration file to the phone using the web interface.

Related links

Importing the configuration file on page 107
Configuring Device Management settings through the web interface on page 113
Exporting the configuration file on page 107
Configuration file on page 98

Time format

B199 Conference Phone supports various time formats so that the user get the convenient time presentation.

The following values are available for the time format parameter:

- **hh:mm** - B199 Conference Phone shows time using the 24-hour clock approach.
- **hh:mm AP** - B199 Conference Phone shows time using the 12-hour clock approach.
- **Empty value** - B199 Conference Phone shows the standard time format for the selected language.

Configuring the time format using the configuration file

About this task

Configure the time format using the .xml configuration file.

Before you begin

Obtain the .xml configuration file for B199 Conference Phone.

Procedure

1. In the configuration file, go to the `<time>` section.
2. Set the `<time_format>` parameter value.
3. Save the configuration file.

Next steps

Upload the configuration file to the Device Management server, or import the configuration file to the phone using the web interface.

Related links

Importing the configuration file on page 107
Configuring Device Management settings through the web interface on page 113
Exporting the configuration file on page 107
Configuration file on page 98

Provision of the NTP server address

Use DHCP option 42 to provide NTP server address to Avaya Conference Phone B199 when using 802.1x certificates. In this case, you must have DHCP enabled on the phone to display the accurate time received from this NTP server address.

Important:

Do not update the value in the configuration file while receiving the NTP address from the DHCP option 42.

If there is a configured NTP setting on the phone, and you set DHCP option 42 to provide NTP server address, then the address from DHCP option 42 overrides this setting in configuration. At that, Avaya Conference Phone B199 preserves the value in the configuration settings. The phone stores the NTP server address from DHCP option 42 separately in a volatile memory. So, when it reboots, the volatile memory becomes empty. If DHCP option 42 does not provide an NTP server address again, then the value from the configuration file becomes applicable.

Sleep mode

B199 Conference Phone supports the sleep mode feature, which saves power by turning the screen off after a specified period of inactivity. By default, the sleep mode is in disabled state. The phone administrator can enable the sleep mode and configure the time-out value.

The phone wakes up from the sleep mode when you do any of the following:

- Touch the screen
- Connect or disconnect the USB cable
- Connect or disconnect a daisy chain Slave device
- Connect or disconnect the Bluetooth Classic

The phone also wakes up from the sleep mode in case of screen activity, such as an incoming call, Avaya® Conference Assistant connection, or error prompts.

The phone cannot enter the sleep mode during an active call or when it is in the music streaming mode.

Enabling the sleep mode

About this task

Enable the sleep mode and configure the time-out value using the .xml configuration file. The default value is 0, which means that the feature is disabled. To enable the sleep mode and to specify the time-out in minutes, set the value in the range from 1 to 500.

Before you begin

Obtain the .xml configuration file for B199 Conference Phone.

Procedure

1. In the configuration file, go to the `<phone>` section.
2. Set the `<sleep_mode_timeout>` parameter to a value in the range from 1 to 500.
3. Save the configuration file.

Next steps

Upload the configuration file to the Device Management server, or import the configuration file to the phone using the web interface.

Related links

Importing the configuration file on page 107
Configuring Device Management settings through the web interface on page 113
Exporting the configuration file on page 107
Configuration file on page 98

Network settings

The network settings of Avaya Conference Phone B199 include the following:

- DHCP
- Hostname
- Domain
- Static IP
- DNS1
- DNS2
- VLAN
- VLAN ID
- LLDP
- 802.1x
- SIP DiffServ
- Media DiffServ

You can configure the network settings on the phone or through the web interface of B199 Conference Phone.

Related links

Network settings description on page 48

Configuring the network settings on the phone

About this task

Use this procedure to configure the network settings of your Avaya Conference Phone B199 on the phone.

Before you begin

Log in as the administrator.

Procedure

1. In the Settings menu, tap **Network**.
2. Choose the parameter that you want to configure and proceed to the options available.
3. Tap the < icon twice to return to the home screen.

   The phone reboots to apply the changes.

Configuring the Network settings through the web interface

About this task

Use this procedure to configure the Network settings of your Avaya Conference Phone B199 through the web interface.

Procedure

1. Log in to the web interface.
2. Click **Network**.
3. Choose the parameter that you want to configure and proceed to the options available.
4. Click **Save**.

   The phone reboots to apply the changes.

Network settings description

The following table lists the network settings of Avaya Conference Phone B199 available through the web interface in the Network tab or on the phone in **Settings** > **Network**.

Name	Description
Network	
DHCP	To enable or disable Dynamic Host Configuration Protocol (DHCP) on your phone. DHCP is used by network devices to obtain the parameters necessary for operation in the IP network. You must enable DHCP if no other specific information is given. **Note:** When DHCP option is enabled, all other information on this page is set automatically.
Hostname	To specify the hostname of your phone in the network. By default, it is set to `AvayaB199`. You can change it to another name.
Domain	To specify the domain where the device is located. **Note:** You can leave this field blank.
Static IP	
IP	To specify the IP address of the phone if DHCP is disabled. In this case, the address is provided by the network administrator or the service provider.
Netmask	To specify the network mask for your phone. Usually it is set to `255.255.255.0` to limit network traffic to the subnet.

Table continues…

Name	Description
Gateway	To specify the gateway for your phone. The gateway is the address of the device or server used for Internet communication.
DNS 1	To specify the address to the primary Domain Name System (DNS) server. **Note:** Leave the field blank for DHCP default settings.
DNS 2	To specify the address to an optional secondary DNS server. **Note:** Leave the field blank for DHCP default settings.
VLAN	To enable or disable the Virtual Local Area Network (VLAN). By enabling this option, all communication to and from B199 Conference Phone goes through the specified VLAN. **Note:** The phone also uses this VLAN to communicate through the web interface.
VLAN ID	To specify the ID number to be used for all IP telephony communication through VLAN on your phone.
SIP DiffServ	To specify a value in the range from 0 to 63 to prioritize the SIP messages as part of quality of service (QoS) mechanism. **Note:** You can configure this parameter through the web interface or through the .xml configuration file.
Media DiffServ	To specify a value in the range from 0 to 63 to prioritize the media packets (voice) as part of quality of service (QoS) mechanism. **Note:** You can configure this parameter through the web interface or through the .xml configuration file.
LLDP	
Enable	To enable and disable specification of the phone location settings. B199 Conference Phone uses Link Layer Discovery Protocol—Media Endpoint Discovery (LLDP-MED) as a data link protocol to send information about itself and receive data about other devices in the same network. You can specify a part of the parameters if some information is unavailable. By default, LLDP is enabled after the first boot, factory reset, and configuration reset. **Note:** You can configure LLDP settings only through the web interface.
Country Code	To specify the country.

Table continues…

Name	Description
Country Subdivision	To specify the part of the country.
County	To specify the county, parish, district, or other applicable administrative division.
City	To specify the city.
City Division	To specify the city district or area.
Block	To specify the block within the city district.
Street	To specify the street.
Direction	To specify the direction of moving along the street.
Trailing Street Suffix	To specify the trailing street suffix.
Street Suffix	To specify the street suffix.
Number	To specify the house number.
Number Suffix	To specify the house number suffix.
Landmark	To specify the reference point for the location.
Additional	To specify additional reference points.
Name	To specify the name of the company.
Zip	To specify the ZIP-code of the location.
Building	To specify the name or number of the building.
Unit	To specify the unit within the building.
Floor	To specify the floor of the building.
Room	To specify the room in the building.
Place Type	To specify the type of setting, for example, office.
Script	To specify the script.
ELIN	To specify Emergency Location Identification Number (ELIN).
802.1.x	
802.1x slider	To enable or disable **802.1x**. When enabled, B199 Conference Phone asks an authentication server for permission when connected to the LAN.
Authentication Name	To specify your name in the network.
EAP MD5	To enable or disable Extensible Authentication Protocol (EAP) MD5 method.
EAP TLSEAP password	To enable or disable the EAP Transport Layer Security (TLS) method.
EAP MD5	
EAP-MD5 Password	To set EAP password. **Note:** This parameter is available in the web interface if you enable **EAP-MD5 Password**.

Table continues…

Name	Description
EAP TLS **Note:** This section is available in the web interface if you enable **EAP TLS**.	
Certificate	To specify the certificate for the phone to use for authentication in case of TLS applied.
CA Certificate	To specify the public key in the root certificate which the phone uses to verify other certificates in case of TLS applied. Root certificate is also known as the Certificate Authority (CA) certificate.
Private Key	To specify the private key which the phone uses to verify other certificates in case of TLS applied.
Private Key Password	To specify the password for encryption of the private key when using TLS.

LLDP Data Units

When Avaya Conference Phone B199 uses LLDP, it sends the information as LLDP Data Units. Each LLDP Data Unit is a sequence of Time-Length-Value (TLV) strings.

The phone supports LLDP on primary Ethernet interfaces. The following table lists the TLVs typical for B199 Conference Phone:

Category	TLV Name	String length	TLV String Value
BASIC MANDATORY	CHASSIS ID	7	MAC ADDRESS OF THE PHONE
BASIC MANDATORY	PORT ID	7	IP ADDRESS OF THE PHONE
BASIC MANDATORY	TIME TO LIVE	2	LLDP_TTL
BASIC OPTIONAL	SYSTEM NAME	22	LLDP_SYSTEM_NAME
BASIC OPTIONAL	SYSTEM DESCRIPTION	28	VENDOR INFORMATION AND FIRMWARE VERSION
BASIC OPTIONAL	SYSTEM CAPABILITIES	4	THE PHONE IS WITHIN THE SYSTEM CAPABILITIES OCTET. IF THE PHONE IS REGISTERED, BIT 5 THAT IS EQUAL TO THE PHONE IS WITHIN THE ENABLED CAPABILITIES OCTET.
BASIC OPTIONAL	MANAGEMENT ADDRESS	12	MGMT ADDR STRING LENGTH = 5; MGMT ADDRESS SUBTYPE = 01; (IPV4) MGMT ADDRESS = IPADD; INTERFACE NUMBER SUBTYPE = 2; INTERFACE NUMBER = 3

Table continues…

Category	TLV Name	String length	TLV String Value
ORGANIZATION SPECIFIC	IEEE - VLAN NAME	11	OUC = 00-80-C2; IEEE 802.1 SUBTYPE = 3; VLAN IDENTIFIER = VLAN ID; VLAN NAME LENGTH = LENGTH OF VLAN NAME; VLAN NAME = NAME OF VLAN
ORGANIZATION SPECIFIC	IEEE 802.3 - LINK AGGREGATION	9	OUC = 00-12-0F; IEEE 802.3 SUBTYPE = LINK AGGREGATION 3; AGGREGATION STATUS = 1; AGGREGATED PORT ID = 0
ORGANIZATION SPECIFIC IEEE 802.3	MAC/PHY/ CONFIGURATION STATUS	9	802.3 OUC = 00-12-0F (HEX); 802.3 SUBTYPE = 1; AUTONEGOTIATION SUPPORT/ STATUS = VALUE SENT DURING AUTO-NEGOTIATION; OPTIONAL MAU TYPE = LLDP_MAU
TIA LLDP MED	LLDP-MED CAPABILITIES	7	TIA OUC = 00-12-BB (HEX); LLDP CAPABILITIES SUBTYPE = 1; LLDP-MED CAPABILITIES = 00-3F (MED CAPS, NETWORK POLICY, LOCATION ID, EXTENDED POWER, INVENTORY); LLDP-MED DEVICE TYPE = 3 (CLASS III)
ORGANIZATION SPECIFIC	CIVIC LOCATION IDENTIFICATION	63	TIA OUC = 00-12-BB; LOCATION DATA FORMAT = CIVIC ADDRESS LCI
ORGANIZATION SPECIFIC	ELIN LOCATION IDENTIFICATION	5	TIA OUC = 00-12-BB; LOCATION DATA FORMAT = ECS ELIN
TIA LLDP MED	NETWORK POLICY - VOICE	8	TIA OUC = 00-12-BB (HEX); NETWORK POLICY SUBTYPE = 2; APPLICATION TYPE = 1 (VOICE) U = 0 (NETWORK POLICY IS DEFINED) T = TAGGING X = 0 (RESERVED BIT) VLAN ID = VLAN_IN_USE
TIA LLDP MED	INVENTORY - SOFTWARE REVISION	5–36	TIA OUC = 00-12-BB (HEX); SOFTWARE REVISION SUBTYPE = 7; SOFTWARE REVISION = VALUE
ORGANIZATION SPECIFIC	EXTENDED POWER-VIA-MDI	7	OUC = 00-12-BB; AVAILABLE PARAMETERS = POWER TYPE, POWER SOURCE, POWER PRIORITY, POWER VALUE
BASIC MANDATORY	END-OF-LLDPU	0	NA

Media settings

You can configure the media settings during the installation of Avaya Conference Phone B199 or any time after it. The media settings include the following:

- Security
- Audio codecs
- Voice Quality Monitor

Related links

Media settings description on page 54

Configuring the media settings on the phone

About this task

Use this procedure to configure the media settings of your Avaya Conference Phone B199 on the phone.

Before you begin

Log in as the administrator.

Procedure

1. In the Settings menu, tap **Media**.
2. Choose the parameter that you want to configure and proceed to the options available.
3. Tap the < icon twice to return to the home screen.

   The phone restarts the application to apply the changes.

Configuring the media settings through the web interface

About this task

Use this procedure to configure the media settings of your Avaya Conference Phone B199 through the web interface.

Procedure

1. Log in as the administrator.
2. Click **Media**.
3. Choose the parameter that you want to configure and proceed to the options available.
4. Click **Save**.

Media settings description

The following table lists the media settings of Avaya Conference Phone B199 available through the web interface in the Media tab or on the phone in **Settings** > **Media**.

Note:

Starting from Release 1.0.1, the **SRTP**, **SRTCP**, and **Capability Negotiation** settings are not supported on B199 phones sold in Russia, Belarus, Kazakhstan, Kyrgyzstan, and Armenia to meet local restrictions on the use of encryption. On such phones, the settings related to SRTP, SRTCP, and Capability Negotiation are excluded both from the phone interface and the web interface, and you, as the administrator, cannot enable these settings.

Name	Description
Security	
SRTP	To select Secure Real-time Transport Protocol (SRTP) parameters to provide encryption, message authentication, and integrity for the audio and video streams. The options are: • **Disabled**: B199 Conference Phone does not use SRTP. • **Optional**: If selected, the phone uses SRTP if other devices support it. • **Mandatory**: The call is not connected if other devices do not support SRTP. By default, SRTP is disabled.
SRTCP	To enable or disable the Secure Real Time Control Protocol (SRTCP). Enabled SRTCP means using the encrypted protocol. By default, SRTCP is disabled.
Capability Negotiation	To enable or disable the Session Description Protocol (SDP) capability negotiation. If Capability Negotiation is enabled, the phone can negotiate transport protocols and attributes. By default, Capability Negotiation is disabled.
Codec	
Codec	To set the priorities to your codec preferences, where 6 is high, 1 is low, and 0 is also possible.
iLBC Priority	This is a high-complexity speech codec suitable for robust voice communication over IP. ILBC is designed for narrow band speech. It uses a block-independent linear-predictive coding algorithm and has support for two basic frame lengths: 20 ms at 15.2 kbit/s and 30 ms at 13.33 kbit/s. By default it is set to 0.

Table continues…

Name	Description
OPUS Priority	This is an audio coding format used in interactive real-time applications on the Internet. It can switch between various codecs depending on the bandwidth available. OPUS adapts to low bit-rate, narrowband speech and to high-quality stereo music. By default it is set to 0.
PCMU Priority	This is an ITU-T standard codec with U-law compression algorithm also known as G711 U-law. It is used in North America and Japan. By default it is set to 4.
PCMA Priority	This is an ITU-T standard codec with A-law compression algorithm also known as G711 A-law. It is used in Europe and the rest of the world, except North America and Japan. Companding algorithms reduce the dynamic range of an audio signal. In analog systems, this can increase the signal-to-noise ratio achieved during transmission, and in the digital domain, it can reduce the quantization error. By default it is set to 5.
G722 Priority	This is an ITU-T standard codec that provides 7 kHz wideband audio at a data rate within 64 kbit/s. It offers an improved speech quality but requires a high quality network connection between the devices. By default it is set to 6.
G729 Priority	This is an ITU-T standard codec that operates at 8 kbit/s. It is mostly used in VoIP applications with low bandwidth requirement. By default it is set to 3.
Voice Quality Monitor	
Enable RTCP XR	To enable or disable the sending of the Real Time Control Protocol Extended Report (RTCP XR). If enabled, the quality parameters are sent as SIP PUBLISH messages to the specified report collector. By default, this option is disabled.
RTCP XR Collector URI	To specify the report collector.

After you click **Save**, the phone saves the changes and restarts application.

Voice quality monitoring

Configure Avaya Conference Phone B199 to generate quality metrics and evaluate the overall quality of the calls. You can use this information to troubleshoot various quality aspects of the phone calls.

Find the detailed description of the collected parameters in the following standards: RFC 6035 and RFC 3611.

RTCP XR as voice quality monitoring report

If you enable the voice quality monitoring feature, the phone collects the metrics, generates Real-Time Control Protocol Extended Report (RTCP XR), and sends RTCP XR as a SIP PUBLISH message to the specified report collector. View the statistics of the established phone calls on a specific information collecting portal.

The phone collects the metrics in the following cases:

- One of the call parties ends the call.
- Call parameters, such as codec and far-end IP address or port, change.
- One of the call parties puts the call on hold or resumes it.

RTCP XR parameters

The following table lists parameters that the RTCP XR contains:

Parameter	Description
CallId	Party leg identifier
LocalId	Reporting device for the media session
RemoteId	Remote device of the media session
OrigID	Device that originated the session
LocalGroup	Identification for aggregation of the local phone
LocalAddr	Address information, including an IP address, a port number, and SSRC of the phone that receives the information
LocalMAC	The Media Access Control (MAC) address of the local phone
RemoteAddr	Address information, including an IP address, a port number, and SSRC of the phone that is the source of information.
Timestamps	Call start and call end in Coordinated Universal Time (UTC)
SessionDesc	A shortened version of the media session including codecs (ILBC, Opus, PCMU, PCMA, G722, or G729), silence suppression status (on or off), and number of packets per second
JitterBuffer	Jitter Buffer metric definitions
PacketLoss	Packet loss percentage and Jitter buffer discard rate percentage
BurstGapLoss	Burst-to-Gap loss metric
Delay	Network delay between the call parties
Signal	Non-packet elements of the voice over IP system. Includes a Signal level (SL) metric, which typically has a negative value
QualityEst	Measures of the established call quality

Quality estimate metrics

The following table shows the direct measures of the quality of the established call or transmission. These metrics incorporate the effects of codec type, packet loss, discard, burstiness, and delay.

Metric	Description
RLQ	Listening Rating Factor (RLQ) metric based on burst packet loss and codec selection.
RCQ	Conversational Rating Factor (RCQ) metric measures voice quality based on transmission delay, burst packet loss, and burst loss recency.
MOSLQ	A mean opinion score for listening quality (MOSLQ). The scale of speech quality is one (bad) through five (excellent).
MOSCQ	A mean opinion score for conversational quality (MOSCQ). Includes recency and delay effects, which affect conversational quality.
QoEEstAlg	A text description of the algorithm, which estimates all voice quality metrics.

Analog parameters

The following table lists the analog parameters that the RTCP XR does not provide, but they influence the call quality statistics:

Name	Description
NoiseLevel	The average silence period noise level (expressed in dBm), reported by the speech processor.
LocalRERL	The average local residual echo return loss (RERL) level (expressed in dB), reported by the echo canceller.
NewLocalLoopEPDelay	The local loop echo path delay (expressed in ms), calculated by the local echo canceller.

The analog parameter data are updated every second. The phone regularly collects the analog parameter data and sends them to generate the RTCP XR report.

Configuring RTCP XR

About this task

By default, the voice quality monitoring feature on Avaya Conference Phone B199 is disabled. To use this feature, enable it and specify the Uniform Resource Identifier (URI) of the RTCP XR collector. You can do this on the phone, through the phone web interface, or using the configuration .xml file.

The acceptable formats for the collector URI are as follows:

- hostname
- hostname:port
- user@hostname
- user@hostname:port

Before you begin

Obtain the RTCP XR collector URI from your service provider.

- To configure RTCP XR from the phone interface, do the following:
  1. Log in as the administrator.
  2. Navigate to **Media** > **Voice Quality Monitor**, and move the **Enable RTCP XR** slider to the right to activate RTCP XR.
  3. In the **RTCP XR Collector URI** field, specify the RTCP XR collector URI.

     For example, `rtcpxr@rtcpxr.ringcentral.com`.
  4. Tap the < icon three times to return to the home screen.

     The phone restarts the application to apply the changes.
- To configure RTCP XR from the web interface, do the following:
  1. Log in to the phone web interface.
  2. On the Media tab, in the Voice Quality Monitor section, move the **Enable RTCP XR** slider to the right to activate RTCP XR.
  3. In the **RTCP XR Collector URI** field, specify the RTCP XR collector URI.

     For example, `rtcpxr@rtcpxr.ringcentral.com`.
  4. Click **Save**.

     The phone restarts the application to apply the changes.
- To configure the RTCP XR using the configuration file, do the following:
  1. Obtain the configuration .xml file.

     Find the RTCP XR settings under the `<voice_quality_monitor>` section.
  2. In the `<enable_rtcp_xr>` tag, specify `true` to enable RTCP XR.
  3. In the `<rtcp_xr_collector_uri>` tag, specify the collector URI.

     For example, `rtcpxr@rtcpxr.ringcentral.com`.
  4. Save the configuration file.
  5. Import the configuration file to the phone through the web interface or to the provisioning server to configure several phones simultaneously.

Related links

Exporting the configuration file on page 107
Device Management on page 108

LDAP settings

Avaya Conference Phone B199 supports connection to an external phone book using the Lightweight Directory Access Protocol (LDAP). When the LDAP feature is in the enabled state, you can browse and use the contact information stored in a remote company directory. The LDAP phone book is available in the Dialpad view of the phone interface.

An LDAP database can contain thousands of contacts. To facilitate the search through the directory server, Avaya Conference Phone B199 has a built-in search function, which filters the content from the LDAP database, based on the search parameters that you enter.

To make the LDAP phone book available, you must activate the LDAP feature by specifying the LDAP server to connect to and the search parameters. You can configure the LDAP settings during or after the installation of Avaya Conference Phone B199.

Configuring the LDAP settings

About this task

Configure the LDAP settings through the web interface of your Avaya Conference Phone B199.

Procedure

1. Log in to the web interface.
2. Navigate to the **LDAP** tab.
3. Choose the parameter that you want to configure and proceed to the options available.
4. Click **Save**.

   The phone restarts the application to apply the changes.

LDAP settings description

The following table lists the LDAP settings of Avaya Conference Phone B199 available through the web interface in the LDAP tab.

Parameter	Description
Connection	
Enable	To specify if the LDAP feature is enabled. By default it is disabled.
URL	To specify the URL of the LDAP server host. The phone supports LDAP and LDAP over SSL (LDAPS). URL also can contain the port that the phone connects to.
Certificate	To upload a certificate to the phone. This certificate is used for authentication on the LDAP server.

Table continues…

Parameter	Description
CA Certificate	To upload a root certificate. It contains a public key, which is used to verify other certificates when using LDAP.
Private Key	To upload a private key. It is used for authentication when using LDAP.
Username	To specify the username if the LDAP server requires one. Leave this field blank if the LDAP server does not require a username.
Password	To specify the password if the LDAP server requires one. Leave this field blank if the LDAP server does not require a password.
Search options	
Search base	To specify the distinguished name (DN) of the search base. Example: `dc=domain`, `dc=com`.
Name filter	To define how the phone applies the entered search characters. The filter complies with the string representation of LDAP search filters described in RFC2254. The search character entered by the user replaces `%` in the filter string. Example: `(|(sn=%*)(cn=%*))`: the phone displays to the user all entries with the search characters in the beginning of the `sn` or `cn` attribute.
Display name	To specify how the phone displays the search hits. Example: `%cn` shows the `cn` attribute. `%givenName %sn` shows the `givenName` attribute and the `sn` attribute with a space in between.
Sort results	To specify if the phone sorts the search hits based on the Display name. By default, this setting is enabled.
Max hits	To specify the maximum number of hits to return for each LDAP search. The default value is 20.

Table continues…

Parameter	Description
Number attributes	To define the attributes that the phone displays for a selected search hit. The phone receives the displayed information from the LDAP server. The number of the Number attribute tags inside the Number attributes tag may be 0 – 30. Each Number attribute consists of an identifier `<id>` and its value `<value>`. The identifier is the number attribute in the form in which the LDAP directory stores it. The `<id>` tag can not be empty. The value is the short description or the label that the user sees on the phone screen for a specific number attribute. You can use the same label for several ids. There are default and custom labels. The default labels are the following: • Phone number • Mobile • Home • Work • Other The `Custom` label are the labels that the user defines. The phone translates each label from the default list to the language specified for the device. The phone does not translate the custom labels and displays them as user sets. A custom label can be empty. In this case the phone gives it a default PHONENUMBER label and translates to the device language. Example: the identifier `mobile2` with the value `MOBILE` shows the second mobile phone number and the label on separate rows for the selected contact. There are maximum 30 labels of the Number attributes in the web UI.
Dial options	
Country code	To specify the country code where the phone is located. In case the country code in any phone number attribute is identical to that code, the phone ignores it.
Area code	To specify the area code where the phone is located. In case the area code in any phone number attribute is identical to that code, the phone ignores it.
External prefix	To specify a special prefix for dialing external numbers. Example: `0` to get a dialing tone in some cases.
Min length for external prefix	To restrict the external prefix that the phone adds only if the phone number is longer than the minimum length. This allows to use short internal numbers. The default setting is 0.

Table continues…

Parameter	Description
Exact length for no external prefix	To specify that the phone must not add the external prefix if the phone number is exactly of the entered length. The default setting is 0.
Number prefix for no external prefix	To specify the initial number for the phone numbers in case of using which the phone adds no external prefix. All numbers that start with this number will not have the external prefix added. You can use this option if all internal numbers start with a certain number. The default setting is 0.

Note:

If complete information is unavailable, you can configure only the known parameters.

Configuring the LDAP number attributes through the web interface

About this task

Configure the LDAP number attributes through the web interface of your Avaya Conference Phone B199.

Procedure

1. Log in to the web interface.
2. Navigate to the **LDAP** tab.
3. Scroll down to the **Number attributes** section.
4. Fill in the title for a number attribute in the **Attribute** field.
5. Choose the description label from the **Localized labels** dropdown list.

   Note that if the label stays empty, it uses the localized default label.
6. **(Optional)** Enable the **Custom** control element to edit the label.

   The **Custom** control element is in the enabled state automatically if the attribute is not in the list of the approved attributes.
7. **(Optional)** You can also do one of the following:
   - Add a number attribute entity by clicking the **Add attribute label** button. The default ID of the number attribute entity is `telephoneNumber` and the value is `PHONENUMBER`.

     Note that there can be maximum 30 number attribute labels in the web UI.
   - Delete a number attribute entity by clicking the **Delete** button next to the respective number attribute.

8. Click **Save**.

   The phone restarts the application to apply the changes.

   The order of the configured number attributes depends on the order of attributes defined on the LDAP server.

Configuring the LDAP number attributes using a configuration file

About this task

Configure the LDAP number attributes by using a configuration file for your Avaya Conference Phone B199.

Before you begin

To configure the LDAP number attributes you need to do the following:

- Make sure that the LDAP feature is in the enabled state and the external phone book is available.
- Prepare the configuration file with the needed LDAP parameters.

  The number attributes in the configuration file can contain the following information:

  - work phone number
  - home phone number
  - mobile 1 and mobile 2 phone numbers
  - fax number
  - other details

Procedure

1. On the phone screen, tap the **Call** icon.

   The Dialpad view opens.

2. Tap the **Contacts** icon.

   Open a contact card to ensure that it is empty and contains only a person’s name.

3. Import the configuration file using the web interface.
4. Click **Save**.

   The phone restarts the application to apply the changes.

   The order of the configured number attributes depends on the order of attributes defined on the LDAP server.

Related links

Importing the configuration file on page 107

SIP settings

The SIP settings can be configured during the installation of Avaya Conference Phone B199. The SIP settings include the following:

- Primary account
- Secondary account
- Fallback account
- Source port
- Transport protocol
- Transport Layer Security (TLS)
- Advanced SIP settings
- DTMF
- NAT Traversal

The SIP settings can be configured on the phone or through the web interface of B199 Conference Phone.

Configuring the SIP settings on the phone

About this task

Use this procedure to configure the SIP settings of your Avaya Conference Phone B199 on the phone.

Before you begin

Log in as the administrator.

Procedure

1. In the Settings menu, tap **SIP**.
2. Choose the parameter that you want to configure and proceed to the options available.
3. Tap the < icon to return to the home screen.

   The phone restarts the application to apply the changes.

Configuring the SIP settings through the web interface

About this task

Use this procedure to configure the SIP settings of your Avaya Conference Phone B199 through the web interface.

Procedure

1. Log in as the administrator.
2. Click **SIP**.
3. Choose the parameter that you want to configure and proceed to the options available.
4. Click **Save**.

   The phone restarts the application to apply the changes.

SIP settings description

The following table lists the SIP setting of Avaya Conference Phone B199 available through the web interface in the SIP tab or on the phone in **Settings** > **SIP**.

Name	Description
Transport	
Transport Protocol	To choose one of the following protocols: • **UDP**. This is the default setting. • **TCP** • **TLS** • **SIPS** **Note:** Even if you choose TLS, B199 Conference Phone still accepts incoming UDP or TCP signalling.
Source port	To specify the local User Datagram Protocol (UDP) port to ensure stable bidirectional traffic.
TLS **Note:** This section is available in the web interface if you choose TLS or SIPS transport protocol.	
TLS Method	To choose the security methods to be applied. The options are: • **TLSv1** • **TLSv1.1** • **TLSv1.2**. This is the default setting.
Verify Client	To enable or disable **Verify Client**. The options are: • Yes: The phone activates peer verification for incoming secure SIP connections. • No. This is the default setting.

Table continues…

Name	Description
Verify Server	To enable or disable **Verify Server**. The options are: • Yes: When B199 Conference Phone is acting as a client for outgoing connections with secure SIP, it always receives a certificate from the peer. If you select this, the phone ends the connection in case of a non-valid server certificate. • No. This is the default setting.
Require Client Certificate	To enable or disable client certificate verification. The options are: • Yes: The phone rejects incoming secure SIP connections if the client does not have a valid certificate. • No. This is the default setting.
Negotiation Timeout	To specify the time-out for the TLS settings negotiation during a call setup. You must define the time in seconds in this field. If this negotiation is not successful within the specified time, the phone stops the negotiation. Disable the time-out by entering `0`. The default setting is 0 seconds.
Certificate	To upload a certificate for TLS or SIPS communication. A certificate is a file that combines a public key with information about the owner of the public key, signed by a trusted third party. If you trust the third party, then you can be sure that the public key belongs to the person named in that file. You can also be sure that everything you decrypt with that public key is encrypted by the person named in the certificate. **Note:** This setting is available only through the web interface in the SIP section.
CA Certificate	To upload a certificate for TLS or SIPS communication received from a Certificate Authority (CA). Use it to verify other certificates. You need the CA certificate if you have **Verify Server** or **Verify Client** enabled. **Note:** This setting is available only through the web interface in the SIP section.
Private Key	To upload a private key for TLS or SIPS communication. A private key is one of the keys in a key pair in asymmetric cryptography. Messages encrypted using the public key can only be decrypted using the private key. **Note:** This setting is available only through the web interface in the SIP section.
Password	To specify the password used for encryption of the private key if it is encrypted.
Primary Account	
Account Name	To set the name for the primary account displayed on the screen according to the existing corporate standards.
User	To set the account or customer name for the primary account.

Table continues…

Name	Description
Registrar	To specify the IP address or the public name of the SIP server where the primary account is registered. For example, use the `10.10.1.100` format for a local SIP server or the `sip.company.net` format for a public VoIP service provider.
Proxy	To specify the Universal Resource Identifier (URI) of the proxy server used by the primary account.
Keep Alive	To make the phone maintain an active connection to the network. The options are: • Yes: If you select this, the phone renews the connection of the phone primary account to the network. • No. This is the default setting.
Realm	To specify the protection domain where the SIP authentication of the primary account with the name and password is valid. If the field is left blank, or marked with an asterisk (*), the phone responds to any realm. If specified, the phone only responds to the specific realm when asked for credentials.
Authentication Name	To specify the number that is assigned to the user in the primary account.
Password	To define the password for the **Realm** authentication in the primary account. **Note:** You can configure this parameter if you logged in with the administrator password. On the phone, the password can be configured in **Settings** > **SIP** > **Primary Account** > **Credentials**
Registration Timeout	To specify the time when the registration of the primary account expires and the SIP server is sent a corresponding request. B199 Conference Phone automatically renews the registration within the time interval if the phone is still on and connected to the server. The default value is 300 seconds.
Secondary Account	
Account Name	To set the name for the secondary account displayed on the screen according to the existing corporate standards.
User	To set the account or customer name for the secondary account.
Registrar	To specify the IP address or the public name of the SIP server where the secondary account is registered.
Proxy	To specify the URI of the proxy server used by the secondary account.
Keep Alive	To make the phone maintain an active connection to the network with the secondary account.
Realm	To specify the protection domain where the SIP authentication of the secondary account with the name and password is valid.
Authentication Name	To specify the number that is assigned to the user in the secondary account.

Table continues…

Name	Description
Password	To define the password for the **Realm** authentication in the secondary account. **Note:** You can configure this parameter if you logged in with the administrator password. On the phone, the password can be configured in **Settings** > **SIP** > **Secondary Account** > **Credentials**
Registration Timeout	To specify the time when the registration of the secondary account expires and the SIP server is sent a corresponding request. The default value is 300 seconds.
Fallback Account	
Account Name	To set the name for the fallback account displayed on the screen according to the existing corporate standards.
User	To set the account or customer name for the fallback account.
Registrar	To specify the IP address or the public name of the SIP server where the fallback account is registered.
Proxy	To specify the URI of the proxy server used by the fallback account.
Keep Alive	To make the phone maintain an active connection to the network with the fallback account.
Realm	To specify the protection domain where the SIP authentication of the fallback account with the name and password is valid.
Authentication Name	To specify the number that is assigned to the user in the fallback account.
Password	To define the password for the **Realm** authentication in the fallback account. **Note:** You can configure this parameter if you logged in with the administrator password. On the phone, the password can be configured in **Settings** > **SIP** > **Fallback Account** > **Credentials**
Registration Timeout	To specify the time when the registration of the fallback account expires and the SIP server is sent a corresponding request. The default value is 300 seconds.
DTMF	

Table continues…

Name	Description
DTMF Method	To define the Dual-tone multi-frequency (DTMF) signalling method. The options are: • **RFC 4733**. With this method, DTMF signals are carried in RTP packets by using a separate RTP payload format. It is set by default. • **SIP Info**. With this method, the DTMF signals are sent as SIP requests. The SIP switch creates the tones if the call is transferred to the PSTN. • **In-band**. With this method, the phone itself generates the tones and sends them in the voice frequency band. **Important:** Use **RFC 4733** or **SIP Info** as the preferred methods because they are more consistent with other tones available. Switch to **In-band** only when your SIP server does not support other DTMF signalling methods. **Note:** When **RFC 4733** is configured as the DTMF method on B199 Conference Phone, but other party does not accept such method, the phone falls back into using the **In-band** method.
RFC 4733 Payload Type	To specify the type of audio traffic. By default it is 101.
Advanced	
Disable 'rport'	To enable or disable remote port forwarding. By default, the setting is disabled.
Session Timers	To set a time-related mechanism to disconnect the sessions that the phone establishes. The options are: • **Disabled**. • **Optional**. This is the default setting. • **Mandatory**
Session Expiration	To specify the session expiration time in seconds. The default setting is 1800 seconds.
Outbound Proxy	To specify the IP address of the outbound proxy, if available.
Enable SIP Traces	To enable or disable provision of key information for troubleshooting. By default, the setting is disabled.
Allow Contact Rewrite	To enable or disable storing the IP address from the response of the register request. If a change is detected, the phone unregisters the available SIP URI (contact), and updates it with the new address. By default, the setting is in the enabled state.
Enable SIP Replaces	To enable or disable the `SIP Replaces` header.
NAT Traversal	

Table continues…

Name	Description
Enable ICE	To enable or disable the Interactive Connectivity Establishment (ICE) that provides various techniques to allow SIP-based VoIP devices to successfully traverse the variety of firewalls that might exist between the devices. The protocol provides a mechanism for the endpoints to identify the most optimal path for the media traffic to follow. By default, the setting is in the disabled state.
Enable STUN	To enable or disable the Simple Traversal of UDP through the NAT (STUN) is a protocol that assists devices behind a NAT firewall or router with their packet routing. STUN is commonly used in real-time voice, video, messaging, and other interactive IP communication applications. The protocol allows applications operating through the NAT to discover the presence and specific type of the NAT and obtain a public IP address (NAT address) and port number that the NAT allocated for the application User Datagram Protocol (UDP) connections to remote hosts. You must enable STUN if an external SIP server cannot connect to the phone behind a firewall NAT function and the SIP server supports STUN. By default, the setting is in the disabled state. **Note:** Another definition of STUN is the Session Traversal Utilities for NAT.
STUN Server	To enter the IP address or the public name of the STUN server.
Enable TURN	To enable or disable the Traversal Using Relay NAT (TURN). TURN is an extension of the TURN protocol that enables NAT traversal when both endpoints are behind symmetric NAT. With TURN, media traffic for the session will have to go to a relay server. Since relaying is expensive, in terms of bandwidth that must be provided by the provider, and additional delay for the media traffic, you must use TURN as a last resort when endpoints cannot communicate directly. By default, the setting is in the disabled state. **Note:** To enable TURN, you must enable ICE.
TURN Server	To enter the IP address or the public name of the TURN server.
User	To specify the user authentication name on the TURN server.
Password	To enter the user authentication password on the TURN server.

After you click **Save**, the phone saves the changes and restarts application.

Caller information presentation

B199 Conference Phone displays the information about the calling person to show who is calling or demonstrate that the caller ID is unknown. This data is available on the Incoming Call, Active Call and Recent Call List screens.

The phone shows the information that it receives from the caller SIP invite message. It includes the following:

- CNAM: Usually specifies the contact name.
- CID: Usually specifies the caller phone number.

For example, when B199 Conference Phone receives the SIP invite message `From: "John Doe" <sip:1234@192.168.1.4>`, `John Doe` is the CNAM and `1234` is the CID.

The following table lists the information on the screen, which B199 Conference Phone displays, depending on the parameters the server provides:

Screen	Description
Incoming Call	Avaya Conference Phone B199 displays the CID. If the server does not provide the CID, the phone displays `Unknown`.
Active Call	Avaya Conference Phone B199 displays the CNAM. If the server does not provide the CNAM, the phone displays the CID. If the server does not provide neither the CNAM, nor the CID, the phone displays `Unknown`.
Recent Call List	Avaya Conference Phone B199 displays the CID. If the server does not provide the CID, the phone displays `Unknown`.

Certificates application

Use certificates to authenticate Avaya Conference Phone B199 using TLS. You can apply certificates manually when configuring the advanced settings of your phone, or the phone can automatically download the certificates from the provisioning server if you enabled Device Management.

The application of a certificate involves the following:

- Download of the root certificate from the Certificate Server
- Creation of the server certificate from the Certificate Server
- Generation of the private key
- Conversion of the certificates and the private key to .PEM format
- Import of the .PEM files to the phone

For information about using EJBCA certificates with Avaya Aura® System Manager, see *Administering Avaya Aura® System Manager*.

Related links

Provisioning on Avaya Conference Phone B199 on page 96

Downloading the root certificate

About this task

Use this procedure to download the root certificate that the phone will apply for authentication by using TLS/SIPS and EAP-TLS.

Before you begin

Connect to Microsoft Server Certification Authority.

Procedure

1. On the **Microsoft Server Certification Authority** page, click **Download a CA certificate, certificate chain, or CRL**.
2. Click **Download CA certificate**.

Creating the server certificate

About this task

Use this procedure to create the server certificate that the phone will apply for authentication by using TLS/SIPS and EAP-TLS.

Before you begin

Connect to Microsoft Server Certification Authority.

Procedure

1. On the **Microsoft Server Certification Authority** page, click **Request a certificate**.
2. Click **Advanced certificate request**.
3. Enter the following information:
    a. In **Identifying information**, specify the name, email, company name, department, and city, state, and country of your location.
    b. In **Type of Certificate Needed**, click **Client Authentication Certificate**.
    c. In **Key option**, click **Create new key set**.
    d. In **CSP**, select **Microsoft Enhansed Cryptographic Provider v 1.0**.
    e. In **Key usage**, select **Both**.
    f. In **Key Size**, specify `1024`.
    g. Select **Automatic key container name**.
    h. Select **Mark keys as exportable**.
    i. Select **Enable strong private key protection**.
    j. In **Request Format**, select **PKCS10**.

k. In **Hash Algorithm**, select **SHA-1** from the list.

l. Enter the short name of the phone.

4. Click **Submit**.

Result

The system saves the certificate to the location specified while creating the CA.

Installing the certificate

About this task

Use this procedure to install the certificate that the phone will apply for authentication using TLS/SIPS and EAP-TLS. You can do it from your regular web browser. The following is the procedure for Google Chrome. For information about other web browser applications, see the instructions provided by the software manufacturers.

Before you begin

Open your web browser.

Procedure

1. Click **Settings** > **Advanced** > **Privacy and security** > **Manage certificates**.
2. In the Certificates window, click **Import**.
3. In the Certificate Export Wizard window, click **Next** to proceed.
4. Specify the file you want to import and click **Next**.
5. Choose the key store for the certificate and click **Next**
6. Click **Finish**.

Exporting the private key

About this task

Use this procedure to export the private key that the phone will apply for authentication using TLS/SIPS and EAP-TLS. You can use your regular web browser. The following is the procedure for Google Chrome. For information about other web browser applications, see the instructions provided by the software manufacturers.

Before you begin

Open your web browser.

Procedure

1. Click **Settings** > **Advanced** > **Privacy and security** > **Manage certificates**.
2. In the Certificates window, select the certificate to export and click **Export**.

3. In the Certificate Export Wizard window, click **Next** to proceed.
4. Click **Yes** to export the private key.
5. Select the format in which you want to export the private key file and click **Next**.
6. Specify the file name, choose the location to export the certificate, and click **Next**.
7. Click **Finish**.

Converting the certificates to .PEM format

About this task

Use this procedure to convert the certificates for the phone to .PEM format. Avaya Conference Phone B199 supports certificates in the .PEM format only.

Procedure

1. Use the following Openssl commands to convert the files:
   a. From .DER to .PEM:

      ```
      openssl x509 -inform der -in certificate.cer -out certificate.pem
      ```

   b. From .PFX to .PEM:

      ```
      openssl pkcs12 -in certificate.pfx -out certificate.cer -nodes
      ```

2. On the web interface, browse to the .PEM files to use TLS mode of authentication.

Standard encryption algorithms

Avaya Conference Phone B199 uses encryption algorithms that comply with the current industry standards. Currently, the phone supports the data integrity algorithms with no publicly known vulnerabilities and are the US National Institute of Standards and Technology approved.

Standard encryption algorithms for the external connections to the system (for example, TLS) include the following:

- Symmetric Encryption:
  - AES 256 (required), except the Cipher Block Chaining (CBC) mode
  - AES 192 and AES 128 (optional), except the CBC mode
- Asymmetric Encryption:
  - RSA: 2048 (required) and 4096 (optional)
  - DH: 2048 (required) and 4096 (optional)
  - ECC: secp384r1 and secp256r1 (required)

- Hash Algorithms
  - SHA2 (required)
  - SHA3 (optional)
- Hashed Message Authentication Code:
  - HMAC-SHA2 (required)
  - HMAC-SHA1 (used for integrity and routing)

When you need legacy or non-standard encryption algorithms for the external connections, you can use legacy encryption mode. In this case the phone works with the encryption algorithms applied before R.1.0.4.

Standard encryption application areas:

- Web pages for administration
- SIP with TLS
- Device management to HTTPS server
- DES
- LDAP with TLS
- Media encryption with SRTP
- 802.1x

Standard encryption for 802.1x

You can configure Avaya Conference Phone B199 to allow 802.1x authentication to use EAP MD5 method.

If you need to use EAP MD5 method for 802.1x, ensure that you set the **Allow Legacy Encryption** option to true.

When you upgrade the phone from a version without the legacy encryption option and enable EAP MD5 method, the phone automatically enables the **Allow Legacy Encryption** option.

Configure Avaya Conference Phone B199 to allow 802.1x authentication to use EAP MD5 method on the phone, through the web interface, or using a configuration file.

Note:

When you import a configuration file, the phone settings update in line with the imported configuration file. If the value of `<eap_md5>` is set to `true`, you must also set the value of `<allow_legacy_encryption>` to `true`.

Related links

Importing the configuration file on page 107
Configuration file structure on page 98
Network settings description on page 48

Enabling EAP MD5 for 802.1x on the phone

About this task

Use this procedure to configure 802.1x and EAP MD5 method for 802.1x on the phone.

Before you begin

Enable **Allow Legacy Encryption**.

You cannot enable **EAP MD5** if **Allow Legacy Encryption** is disabled. If you try to enable it, the phone shows the following warning message: `EAP MD5 requires Allow Legacy Encryption to be enabled`.

Procedure

1. Log in as the administrator.
2. Navigate to **Network** > **802.1x**, and move the **802.1x** slider to the right to enable 802.1x.
3. In the **Authentication Name** field, enter the authentication name.
4. Activate **EAP MD5 Enable**.
5. In the **EAP-MD5 Password** field, enter the password for EAP MD5.
6. Tap the < icon three times to return to the home screen.

   The phone reboots to apply the changes.

Related links

Standard encryption algorithms on page 74
Configuring the legacy encryption mode on the phone on page 77

Enabling EAP MD5 for 802.1x through the web interface

About this task

Use this procedure to configure 802.1x and EAP MD5 method for 802.1x through the web interface.

Before you begin

Enable **Allow Legacy Encryption**.

You cannot enable **EAP MD5** if **Allow Legacy Encryption** is disabled. If you try to do it, the phone shows the following warning message: `EAP MD5 requires Allow Legacy Encryption to be enabled`.

Procedure

1. Log in as the administrator.
2. Choose the Network tab.

3. In the 802.1x section, enable **Enable 802.1x**.
4. In the Username field, enter the user name.
5. To activate EAP MD5 method for 802.1x, enable **EAP MD5 Enable**.

   The EAP MD5 section becomes visible.
6. In the **Password** field, enter the password for EAP MD5.
7. Click **Save**.

   The phone reboots to apply the changes.

Related links

Standard encryption algorithms on page 74
Configuring the legacy encryption mode through the web interface on page 78

Standard encryption for media encryption with SRTP

When the key exchange for media encryption with SRTP occurs, Avaya Conference Phone B199 supports the `AES_256_CM_HMAC_SHA1_80` mandatory crypto.

Some servers do not support this mandatory crypto. In this case you must enable the **Allow Legacy Encryption** option to make an SRTP call. By default, it is disabled.

In this case, with the legacy encryption mode enabled, the phone offers `AES_CM_128_HMAC_SHA1_80` crypto only.

You must enable the **Allow Legacy Encryption** option when you register the phone to IP Office. IP Office supports only the following cryptos:

- `AES_CM_128_HMAC_SHA1_80`
- `AES_CM_128_HMAC_SHA1_32`

Legacy encryption mode

Avaya Conference Phone B199 also supports specific legacy encryption algorithms. If you enable the legacy encryption mode, the phone offers all the previously supported ciphers for the SSL negotiation and cryptos for SRTP. Check the offered ciphers using a specialized network protocol analyzer. At that, the phone supports the legacy encryption algorithms only for backward compatibility. By default, this feature is disabled.

Configuring the legacy encryption mode on the phone

About this task

Use this procedure to configure the legacy encryption mode of your Avaya Conference Phone B199 on the phone.

If you configure the phone to allow 802.1x authentication to use method EAP MD5, you cannot disable legacy encryption. The phone warns you with a message: `Allow Legacy Encryption cannot be turned off while 802.1x with EAP MD5 is enabled.`

Before you begin

Log in as the administrator.

Procedure

1. In the Settings menu, tap **Phone** > **Security**.
2. Enable **Allow Legacy Encryption**.
3. Tap the < icon three times to return to the home screen.

   The phone reboots to apply the changes.

Configuring the legacy encryption mode through the web interface

About this task

Use this procedure to configure the legacy encryption mode of your Avaya Conference Phone B199 through the web interface.

If you configure the phone to allow 802.1x authentication to use EAP MD5 method, you cannot disable legacy encryption. The phone warns you with a message: `Allow Legacy Encryption cannot be turned off while 802.1x with EAP MD5 is enabled.`

Before you begin

Log in to the web interface as the administrator.

Procedure

1. Click **Phone**.
2. In the Advanced section, enable **Allow Legacy Encryption**.
3. Click **Save**.

   The phone reboots to apply the changes.

Configuring the legacy encryption mode using the configuration file

About this task

Use this procedure to configure the legacy encryption mode of your Avaya Conference Phone B199 using the .xml configuration file. When you boot the phone after successful provisioning, the setting file changes, depending on the configuration of the standard encryption use.

Before you begin

Get the configuration .xml file for Avaya Conference Phone B199.

Procedure

1. Open the configuration file.
2. In the `<phone>` section, locate `<allow_legacy_encryption>` tag and set the value to true.

   By default, the value is false.
3. Save the configuration file.

Next steps

Upload the configuration file to the Device Management server or import the configuration file to the phone using the web interface.

Related links

Importing the configuration file on page 107
Configuration file structure on page 98

Chapter 6: Features and accessories

Avaya® Conference Assistant

You can manage your Avaya Conference Phone B199 from a mobile phone or a tablet if you have Avaya® Conference Assistant installed on the device. Download and install Avaya® Conference Assistant free from App Store and Google Play like any other application. Use the NFC tag to easily start downloading the application. For that, you must bring the mobile device with the NFC enabled to the NFC tag on the conference phone, and the web browser on the mobile device opens the web page with the application in App Store or Google Play.

With Avaya® Conference Assistant, you can call contacts from your local address book, create conference groups, and control a call. For example, answer and hang up the call, mute and unmute the microphone, dial a number, adjust the volume level, and hold and resume the call.

The mobile device with Avaya® Conference Assistant is connected to the phone over the built-in Bluetooth LE. B199 Conference Phone is always discoverable for this connection.

Starting from R 1.0.4, Avaya Conference Phone B199 uses SHA256 method for challenge-response authentication to connect to Avaya® Conference Assistant.

Note:

If your conference phone fails to connect to Avaya® Conference Assistant, you must download a newer version of the application from App Store or Google Play. It works both with R 1.0.4 and earlier released firmware.

Configure Avaya® Conference Assistant parameters on the phone and from the mobile device with the application installed.

Pairing and connecting devices

About this task

Use this procedure to pair your Avaya Conference Phone B199 with Avaya® Conference Assistant on your mobile device the first time when you use them together. After that, they connect with one touch when you run the application near the conference phone.

The connection range is up to 20 meters. The connection breaks if this range is exceeded. You see a request to reconnect when Avaya® Conference Assistant is within the range of B199 Conference Phone. Reconnection requires only one touch.

Important:

You can pair up to 100 mobile phones or tablets with your B199 Conference Phone. But only one user connection is active at a time.

Before you begin

Install Avaya® Conference Assistant on your mobile device.

Procedure

1. On your mobile device, open Avaya® Conference Assistant.

   The mobile phone displays the closest B199 Conference Phone.

2. To select the phone you want to connect, perform one of the following actions:

   - If your mobile device displays B199 Conference Phone you want to connect, tap **Connect** on the mobile device screen.
   - If your mobile device does not display B199 Conference Phone you want to connect, tap **Skip** and then tap the connection symbol in the upper left corner of your mobile device screen.

     The mobile device displays the list of available conference phones.

   The mobile phone displays a pairing code for about 30 seconds.

3. Enter the code with the keypad on the conference phone.
4. Tap **Enter** on the conference phone to start pairing.

   When the devices are paired, both Avaya® Conference Assistant and B199 Conference Phone display the connection symbol.

   The conference phone and Avaya® Conference Assistant remain paired while they are close to one another.

   Note:

   You cannot connect B199 Conference Phone to a Bluetooth device for call handling or audio streaming while the Avaya® Conference Assistant connection is active.

Disconnecting devices

About this task

Use this procedure to disconnect your Avaya Conference Phone B199 from the mobile device with Avaya® Conference Assistant installed.

Before you begin

Ensure that B199 Conference Phone is connected to a mobile device with Avaya® Conference Assistant installed.

- To disconnect from the mobile device, do the following:
  1. In Avaya® Conference Assistant, tap the connection symbol in the upper left corner of the screen.
  2. **(Optional)** Under **Change device**, select another conference phone to connect to.

     You can do it if there are other conference phones available nearby.

     The application starts connecting to the selected conference phone.
  3. Tap the **Disconnect** button near the highlighted connected device name.

     The connection symbol in the upper left corner of the screen becomes inactive.
- To disconnect from B199 Conference Phone, do one of the following:
  - Tap **Conference Assistant** > **Disconnect Device**.
  - Tap **Settings** > **Conference Assistant** > **Disconnect Device**.

  The phone displays the following question: `Disconnect device <Device Name>?`

  To confirm, tap **Ok**.

  The phone shows the Avaya® Conference Assistant icon and informs that the application is disconnected.

Deleting pairing

About this task

Use this procedure to delete the pairing between the conference phone and the mobile device. You can delete the paring only from the conference phone.

Before you begin

Pair Avaya Conference Phone B199 with a mobile device with Avaya® Conference Assistant.

Procedure

1. To delete the pairing from the conference phone, on the home screen, do one of the following:
   - Tap **Conference Assistant**.
   - Tap **Settings** > **Conference Assistant**.
2. Tap **Remove Bonding Information**.
3. Tap **Ok** to confirm removal of all bonding information from the device.

   This function both disconnects the current connection and deletes the pairing. You must start a new pairing process the next time you want to connect to the phone.

Configuring the Avaya® Conference Assistant settings

About this task

Use this procedure to configure the Avaya® Conference Assistant settings from the application installed on a mobile device.

Procedure

1. Run Avaya® Conference Assistant on your mobile device.
2. **(Optional)** Connect to Avaya Conference Phone B199.

   The phone displays a connection symbol on the screen.
3. Tap **Settings** and proceed with configuration.

Avaya® Conference Assistant settings

The following table lists the parameters for Avaya Conference Phone B199, which you can set from the Avaya® Conference Assistant interface:

Name	Description
Connection	To enable or disable the connection to Avaya Conference Phone B199. The options are: • On: The default option. • Off: To use Avaya® Conference Assistant without connection to any Avaya Conference Phone B199. You can use the conferencing application from your mobile device within your mobile phone subscription.
Moderator code	To join the scheduled conference calls as a moderator. You must enter respective codes in the following fields: • **Use moderator code**: To host conference calls over a bridge service. For every call you join, Avaya® Conference Assistant uses your moderator code instead of your guest code. • **Instead of guest code**: To specify the guest code instead of which Avaya® Conference Assistant uses your moderator code.
Dial prefix	To enter the prefix digits in the **Use prefix** field.
My bridge	To enter the phone number and optional PIN code of the most frequently used conference service. You can use the **My bridge** button to join the conference call. The **My bridge** button appears in the calendar view.

Table continues…

Name	Description
Meeting notification	To set a reminder about a call. The options are: • 5 minutes before • 10 minutes before • 15 minutes before • Never
Calendars to show	To select the calendars in the mobile phone from which you want Avaya® Conference Assistant to take the information.
Tell a colleague	To share information about Avaya® Conference Assistant with a person that you want. You can do it by using an email application. After you confirm that Avaya® Conference Assistant can access your email application, you see a message created. Along with the description of the application, it contains links to Avaya® Conference Assistant in App Store and Google Play so that the person can easily start the download.
Read more about Conference Assistant	To get additional information about Avaya® Conference Assistant. The application forwards you to the web site with the corresponding information.
Diagnostics	To select a log of the events for Avaya® Conference Assistant. You can send the created log by tapping **Send** through an email application. The log can be used in troubleshooting. You can also delete the logs from the application by tapping **Clear**.
Show tutorial	To read information about Avaya® Conference Assistant features.
About Conference Assistant	To check the version of the application installed on your mobile device.

Expansion of the phone coverage

Use your Avaya Conference Phone B199 on larger conference tables or when the number of a meeting participants is greater than 10. In this case you can ensure high-level quality of audio signal by expanding the phone coverage in the room without a PA system. Do it by connecting Smart Mic expansion microphones to the phone or by cascading several B199 devices in a daisy chain.

Expansion of the phone coverage helps to improve the audio quality in large rooms. The conference phone and two Smart Mics increase the capture range from 30 square meters to up to 70 square meters. Three phones in a daisy chain increase the range from 30 square meters to up to 90 square meters.

Expansion coverage arrangement

Arrange a daisy chain with your conference phone and another B199 Conference Phone or connect Smart Mic expansion microphones. The maximum number of devices connected in a

daisy chain is 3. One B199 phone acts as a central device (a “master”) and one or two other units act as expansion devices (“slaves”).

The typical arrangements when the phone’s coverage is expanded are the following:

- Master phone — Slave phone
- Slave phone — Master phone — Slave phone
- Master phone — Expansion microphone
- Expansion microphone — Master phone — Expansion microphone
- Expansion microphone — Master phone — Slave phone

Functions of the Master and Slave devices

When B199 Conference Phone acts as a master, it performs all its configured functions.

When B199 Conference Phone is in a subordinate position (a “slave”), it performs the following functions:

- Play audio received from the master device. The master phone defines the audio characteristics.
- Send its microphone audio to the master device.
- Receive and indicate mute state changes made on the master device.
- Send information to the master device, when you tap **Microphone Muted**.
- Send information to the master device when you adjust the volume on it.

Note:

You cannot make calls between the Master and the Slave devices.

In a daisy chain, the Slave device follows the signal from the Master device to enter the sleep mode or the active mode.

In a daisy chain, each phone is powered by its own PoE injector. The phone powers the Smart Mics when these are connected. The power available from each port is around 5 W.

Arranging a daisy chain

About this task

Use this procedure to arrange a daisy chain of one master B199 phone and one or two slave conference phones or expansion microphones.

Before you begin

If you arrange the daisy chain made of several conference phones, prepare the connection cables. The cables in the Avaya Daisy Chain kit are 5 and 10 meters long. You can purchase the Avaya Daisy Chain kit as an accessory.

The cable of the Avaya Smart Mic is 3 m long.

Procedure

1. Connect the cable to the audio expansion port on the phone.

   There are 2 audio expansion ports on B199 Conference Phone.
2. Connect the other end of the cable to the audio expansion port of the other phone.

   In case of expansion microphones, the other end of the cable is fixed in the device.

Defining the mode of the phone

About this task

Use this procedure to define the mode of your Avaya Conference Phone B199 in a daisy chain.

- To define the mode of your B199 on the phone, do the following:
  1. Log in as the administrator.
  2. In the Settings menu, tap **Phone** > **Daisy Chain**.
  3. Select the required mode.

     The options are:

     - **Master**
     - **Slave**
  4. Tap < three times to return to the home screen.

  The phone restarts the application to apply the changes.
- To define the mode of your B199 Conference Phone through the web interface, do the following:
  1. On the web interface, click **Phone**.
  2. In Daisy Chain Mode, select the required mode from the drop-down list.

     The options are:

     - **Master**. This is the default mode.
     - **Slave**
  3. Click **Save**.

  The slave unit displays the Daisy Chain Mode icon and the following message: `Daisy Chain`. This message remains for the period when the phone is in the slave mode within the daisy chain arrangement.

Disabling the daisy chain mode

About this task

Use this procedure to disable the Daisy Chain mode through the web interface or from the phone.

Before you begin

Ensure that the phone displays the Daisy Chain icon.

- To disable the Daisy Chain mode from the web interface, do the following:
  1. On the web interface, click **Phone**.
  2. In Daisy Chain Mode, select **Master**.
  3. Click **Save**.
- To disable the Daisy Chain mode from the phone, do the following:
  1. Touch the phone screen and enter the administrator password.
  2. Tap **Phone** > **Daisy Chain**.
  3. Select the **Master** mode.
  4. Tap the < icon three times to return to the home screen.

     Application restarts and restores the Master status.

Expansion microphone firmware upgrade

You can upgrade the expansion microphone firmware to the Avaya Conference Phone B199 firmware version when your Smart Mic has an older firmware installed. Regularly updating the expansion microphone firmware to match the phone firmware ensures the best possible audio performance.

The phone suggests an automatic upgrade of the expansion microphone firmware when you connect your Smart Mic to B199. You can connect one or two Smart Mics simultaneously.

You can also initiate the expansion microphone firmware upgrade manually.

If you connect the expansion microphone to Avaya Conference Phone B199 during an active call, the upgrade does not start until the call ends.

During the upgrade, the phone rejects all incoming and outgoing calls and does not activate the **Call Transfer** feature. At that B199 indicates that it is `Busy`.

Expansion microphone and conference phone firmware upgrade

You can upgrade the Avaya Conference Phone B199 firmware by downloading the .xml configuration file and .xml certificate configuration file from the provisioning server. If the phone has DES enabled, its firmware upgrade starts automatically.

The expansion microphones can have their firmware upgrade simultaneously with the Avaya Conference Phone B199 firmware. In this case, the phone reboots automatically only after its firmware and Smart Mic firmware upgrade complete.

Upgrading expansion microphone firmware

About this task

Use this procedure to upgrade the expansion microphone firmware when the Smart Mic and your device have different firmware installed.

Before you begin

Make sure B199 is in the Idle Mode.

Procedure

1. Connect the expansion microphone to your conference phone using the available audio expansion port.

   The expansion microphone LEDs flash red once.

   A pop-up dialog window shows the following message: `A connected microphone needs firmware upgrade. Upgrade now?`

2. On the pop-up dialog window, tap **Yes** to start the upgrade.

   The LEDs on the phone turn red to indicate that it is busy with the microphone upgrade. The expansion microphone LEDs start flashing green.

   The phone displays the `Upgrade in progress` message and shows the upgrade progress in percentage (0%-100%).

   When you connect one Smart Mic to B199, the phone shows the upgrade status for Smart Mic 2 as `N/A`.

   ```
   Smart Mic 1: 10%
   Smart Mic 2: N/A
   ```

3. **(Optional)** To cancel the upgrade, tap **No**.

   In this case, you postpone the upgrade until the phone reboots.

Result

If the upgrade is complete, the microphone LEDs turn off, and Avaya Conference Phone B199 displays the following message:

```
Upgrade in progress
Smart Mic 1: Done
Smart Mic 2: N/A
```

In 10 seconds, the pop-up dialog window hides, and the phone enters the Idle mode.

If the Smart Mic firmware upgrade fails, the microphone LEDs turn off, and the phone displays the `Smart Mic 1: Failed` message.

Upgrading two expansion microphones

About this task

Use this procedure to upgrade two expansion microphones connected to your device simultaneously.

Before you begin

Connect Smart Mic 1 to the first audio expansion port of your conference phone.

Procedure

1. Connect Smart Mic 2 to your conference phone using the second audio expansion port.

   The LEDs on the phone turn red to indicate that it is busy with the microphone upgrade. The Smart Mic 2 LEDs start flashing green.

   A pop-up dialog window provides the expansion microphones upgrade status in the following format:

   ```
   Smart Mic 1: 20%
   Smart Mic 2: 10%
   ```

2. **(Optional)** Terminate Smart Mic 2 upgrade by detaching the expansion microphone from the phone.

   In this case, you postpone the upgrade until you connect Smart Mic 2 again.

Result

When the upgrade is complete for Smart Mic 1 and Smart Mic 2 is still upgrading, the LED turns off on Smart Mic 1, and Avaya Conference Phone B199 displays the following message:

```
Upgrade in progress
Smart Mic 1: Done
Smart Mic 2: 86%
```

When the upgrade is complete for both microphones, their LEDs turn off, and Avaya Conference Phone B199 displays the following message:

```
Upgrade in progress
Smart Mic 1: Done
Smart Mic 2: Done
```

In 10 seconds, the pop-up dialog window hides, and the phone enters the Idle mode.

If the firmware upgrade for any of the expansion microphones fails, the microphone LEDs turn off, and the phone displays the message stating the `Failed` status of the corresponding Smart Mic.

Terminating expansion microphone upgrade

About this task

Use this procedure to terminate the expansion microphone upgrade.

You can do it in the following cases:

- The phone has one Smart Mic 1 connected; or
- The phone has both Smart Mic 1 and Smart Mic 2 connected simultaneously.

Before you begin

Connect Smart Mic 1 and Smart Mic 2 to the phone and start the upgrade process for both expansion microphones.

Procedure

1. Detach Smart Mic 2 from the phone.

   Smart Mic 1 continues upgrading with the value for the upgrade progress being updated.

   Smart Mic 2 upgrade dialog indicates an error and aborts the mic upgrade. Avaya Conference Phone B199 displays the following message:

   ```
   Upgrade in progress
   Smart Mic 1: 50%
   Smart Mic 2: Failed
   ```

   When Smart Mic 1 upgrade is complete, its LED turns off, and Avaya Conference Phone B199 displays the following message:

   ```
   Upgrade in progress
   Smart Mic 1: Done
   Smart Mic 2: Failed
   ```

   This message disappears in 10 seconds.

2. **(Optional)** To upgrade Smart Mic 2, connect it to the conference phone and proceed with the upgrade.

Upgrading Smart Expansion Microphone manually

About this task

Upgrade your expansion microphone manually when it is convenient to you.

Procedure

1. Hold the **Microphone Muted** button on the Smart Mic while you connect the microphone cable, and keep holding the button for 5 seconds after you inserted the cable.

When you release the button, it flashes red one time and then starts flashing green to indicate that the upgrade process has started. The LEDs on the phone turn red to indicate that it is busy with the microphone upgrade. The upgrade process takes about 7 minutes. When the upgrade is completed, the microphone LEDs turn off.

2. Check the microphone version by doing one of the following:
   - On the phone screen, tap **Settings** > **Status**.
   - On the web interface, go to the **Status** tab.

Bluetooth connection

Avaya Conference Phone B199 can establish wireless communication over Bluetooth with devices equipped with Bluetooth connectivity, such as mobile phones, tablets, or computers. With Bluetooth, you can use the phone as a speakerphone for call handling, or as an audio receiver for audio streaming.

The following table lists the Bluetooth technologies that B199 Conference Phone supports:

Bluetooth technology	B199 icon	Functionality
Bluetooth LE		To connect to a mobile device with Avaya® Conference Assistant application installed on it. For more information, see Avaya Conference Assistant on page 80. This is the default mode.
Bluetooth Classic		To connect to Bluetooth devices, such as mobile phones, tablets, and personal computers, for call handling or audio streaming.

B199 Conference Phone has a modified Pulse-code modulation (PCM) bus installed. This provides for a better audio transmission compared to the previous releases of the phone.

Note:

You cannot use Bluetooth LE and Bluetooth Classic connection simultaneously.

If you connect B199 Conference Phone to a Bluetooth device, you cannot connect it to a mobile device with the Avaya® Conference Assistant application until you end the connection to the Bluetooth device.

If you connect B199 Conference Phone to a mobile device using the Avaya® Conference Assistant application, you cannot connect it to another Bluetooth device until you end the connection to Avaya® Conference Assistant.

Switching between the Bluetooth modes

The default mode is Bluetooth LE. To switch to Bluetooth Classic, you must pair and connect B199 Conference Phone to a Bluetooth device. When you select the Bluetooth Classic mode, the phone turns off Bluetooth LE. If there is no Bluetooth Classic connection, the phone switches back to Bluetooth LE after a timeout.

In case of a successful Bluetooth Classic connection, B199 Conference Phone restores the Bluetooth LE mode when you end the Bluetooth Classic connection.

Bluetooth Classic profiles

The following table describes the Bluetooth Classic profiles that B199 Conference Phone supports:

Bluetooth profile	B199 role	Functionality description
Hands-Free Profile (HFP)	Speakerphone	When B199 Conference Phone is paired with a Bluetooth device, and the two devices are connected, the phone acts as a speakerphone. You can use the phone to handle Bluetooth calls. B199 Conference Phone synchronizes the volume level with the volume level of the Bluetooth device, and you can control the volume from both devices.
Advanced Audio Distribution Profile (A2DP)	Audio receiver	When B199 Conference Phone is paired with a Bluetooth device, and the two devices are connected, B199 Conference Phone acts as an audio receiver. You can use the phone to stream multimedia audio from the Bluetooth device. **Note:** You cannot activate A2DP during SIP or USB calls.

Note:

To use the Bluetooth Classic functionality on B199 Conference Phone, your Bluetooth device must support HFP or A2DP or both.

Pairing and connecting Bluetooth devices

About this task

To enable Bluetooth communication between B199 Conference Phone and another Bluetooth device, you must pair the two devices and ensure that they are in a connected state. The devices stay in a paired state until you remove the pairing.

Note:

You can connect only one device supporting Bluetooth at a time.

Procedure

1. On the B199 Conference Phone screen, tap **Settings** > **Bluetooth** > **Pair with device**.

   The LEDs start flashing blue, and the phone displays the following message: `This phone is now discoverable as "<Phone Name>".`

   The time-out value for discoverable mode is 120 seconds.

Tip:

Tap **Cancel** to cancel pairing, for example, if you do not want to make the phone discoverable. In this case, you return to the Bluetooth menu.

2. On your Bluetooth device, find B199 Conference Phone in the list of devices available for Bluetooth connection and tap the phone name.

   B199 Conference Phone establishes the connection with the Bluetooth device and displays the Bluetooth icon and one of the following messages:

   - If B199 Conference Phone retrieves the device name from your Bluetooth device, it displays `Connected to <your Bluetooth device name>`. For example, `Connected to My Smartphone`.
   - If B199 Conference Phone does not retrieve the device name from your Bluetooth device, it displays `Connected to <your device Bluetooth address>`. For example, `Connected to 00:11:22:33:FF:EE`.

Note:

B199 Conference Phone is not visible in the Avaya® Conference Assistant application while the conference phone and the Bluetooth device are in the connected state.

Related links

Phone settings description on page 35

Removing Bluetooth pairing

About this task

Use this procedure to remove the pairing between Avaya Conference Phone B199 and your other Bluetooth device to delete unwanted pairings.

B199 Conference Phone also deletes the Bluetooth pairing information when you reset the phone to factory settings or perform system recovery.

Note:

Removing Bluetooth pairing as described below does not affect Avaya® Conference Assistant pairing information.

Before you begin

Ensure that B199 Conference Phone and the Bluetooth device are in the paired state.

Procedure

1. Tap **Settings** > **Bluetooth** > **Remove pairing**.

   The phone displays the following question: `Do you want to remove all Bluetooth pairing information from the phone?`

2. To confirm that you want to delete the Bluetooth pairing information, tap **Ok**.

The phone restarts the application to apply the changes.

Related links

Logging in to the web interface of Avaya Conference Phone B199 on page 26
Setting the password for Avaya Conference Phone B199 on page 23

Connection between paired Bluetooth devices

Connection

After you pair B199 Conference Phone and your Bluetooth device, the two devices establish the connection.

Disconnection

The connection ends if you manually disconnect B199 Conference Phone from the Bluetooth device or if the distance between the devices does not allow to maintain the communication.

When the Bluetooth device ends the connection, B199 Conference Phone displays the following message: `Disconnected` and then stops displaying the Bluetooth icon.

Reconnection

You can reconnect your Bluetooth device to B199 Conference Phone if the two devices are in a paired state. You can reconnect B199 Conference Phone to the paired Bluetooth device only from the paired Bluetooth device.

Bluetooth radio

B199 Conference Phone supports the Bluetooth radio feature, which makes the device visible to other Bluetooth devices. By default, the Bluetooth radio is in the enabled state. The administrator can disable the Bluetooth radio. When disabled, Bluetooth LE and Bluetooth Classic connection are not available on B199 Conference Phone.

Related links

Bluetooth connection on page 91

Disabling Bluetooth radio

About this task

Use this procedure to disable Bluetooth radio using the .xml configuration file. The default value is true, which means that the feature is enabled.

Before you begin

Obtain the .xml configuration file for B199 Conference Phone.

Procedure

1. In the configuration file, go to the `<bluetooth>` section.
2. Set the `<enable>` parameter to false.

```
<bluetooth>
      <enable type = "bool">false</enable>
</bluetooth>
```

3. Save and import the configuration file.

   The phone restarts the application.

Related links

Importing the configuration file on page 107
Configuration file on page 98

Chapter 7: Maintenance

Provisioning on Avaya Conference Phone B199

To ensure effective operation of your Avaya Conference Phone B199, you can upload to the phone the latest firmware version with the software update packages and configuration file with the necessary settings. You can upgrade and configure a single phone or multiple phones simultaneously.

Provisioning option	Upgrade and configuration description
Single phone	Use the phone web interface to upload a firmware file as well as to export and import a configuration file to B199 Conference Phone.
Multiple phones	Use the Device Management feature to upgrade and configure multiple B199 phones simultaneously over a provisioning server. The Device Management settings are available both on the phone and through the web interface.

Firmware upgrade and downgrade

Starting from Release 1.0.1, you can both upgrade and downgrade the firmware of Avaya Conference Phone B199 using the Device Management. The phone application installs the firmware whenever the firmware version found in the firmware file downloaded from the provisioning server differs from the version of the currently running firmware.

Note:

The downgrade causes a factory reset and sets all user settings, configurations, and data to factory default.

Uploading a firmware file

About this task

Upgrade or downgrade your Avaya Conference Phone B199 using a firmware file stored on the local hard disk. When the phone starts to install the firmware file you uploaded, it identifies the firmware version and follows the upgrade or downgrade scenario based on the firmware version.

Before you begin

Download the appropriate firmware file from http://support.avaya.com/ and save it in a specified location on your personal computer.

Procedure

1. On the web interface, click **Provisioning**.
2. In the Firmware section, click the **Choose file** button.
3. Locate and select the downloaded firmware file.

   The name of the chosen file is near the **Choose file** button.
4. Click **Save**.

   The system displays the upgrade in the browser window and on the screen of B199 Conference Phone.

   Note that the phone must be in the idle state. If the phone is not in the idle state, you see the following message on the web interface: `Phone is currently in "Busy" state, please retry later.`

Next steps

If DHCP is used in the network, the IP address might change. If the web browser loses contact with B199 Conference Phone, check the IP address on the phone.

Related links

Viewing the IP address on page 25

Firmware upgrade using check-sync

Avaya Conference Phone B199 automatically starts the firmware upgrade procedure when it receives a check-sync event from your SIP server. To use this feature, you must enable Device Management on your phone.

Note:

The phone checks the firmware and starts the firmware upgrade only if it the new firmware differs from the firmware installed.

Note:

IP Office does not support check-sync for firmware upgrades. IP Office supports check-sync only for the settings file changes.

If Avaya Conference Phone B199 receives a check-sync NOTIFY event in the Idle Mode, it automatically starts the Device Management procedure, which includes downloading the firmware file. The phone is in the Idle Mode when there are no active calls, it is not streaming music over USB or Bluetooth, and the idle screen is active. If the phone receives the check-sync NOTIFY event during an active call, it waits till the end of the call and then immediately starts downloading the provisioning data.

Avaya Conference Phone B199 checks the check-sync message for the reboot parameter value:

```
Event: check-sync;reboot=true
```

or

```
Event: check-sync;reboot=false
```

If the reboot value is **true**, Avaya Conference Phone B199 will reboot regardless of any firmware upgrades or new configuration files available. The phone applies the new configuration of firmware before the forced reboot. If the reboot value is **false** or not defined, the phone restarts the application, reboots, or does nothing depending on the requirements of the firmware upgrade or new configuration parameters in the configuration file.

Configuration file

Create an .xml configuration file on Avaya Conference Phone B199. This file contains information about all the settings that were configured on the phone as of the moment of the file creation.

The configuration file can be used as:

- Backup. This is applicable if the system has been reset to factory default.
- Configuration interface. Some settings are not configured through the web interface.
- Management tool. Export, edit, and import settings to several phones instead of configuring the settings on each phone.
- Configuration file for Device Management.

Note:

You can export and import a configuration file only through the web interface.

Related links

Device Management on page 108

Configuration file structure

The following table shows the default structure of the .xml file:

String	Description
<xml>	To specify the number of the phone configuration version and encoding.
<B199>	To specify the model of the conference phone.
<time>	To specify the time and region parameters.
<time_format>	To specify the time format for the phone.

Table continues…

String	Description
<timezone>	To specify the type of the time zone set for the phone. If you set the string value to the name of a time zone, for example, to Europe/Amsterdam, it automatically enables the Geo Timezone (auto DST) parameter on the phone web UI.
<ntp>	To specify whether NTP is applied.
<server>	To specify the server which the phone uses to set the time.
<enable>	To specify whether NTP is enabled. The default setting is true.
<date_format>	To specify the date format for the phone.
<custom_dst>	To specify the Daylight Saving Time parameters.
<enable>	To specify whether the Daylight Saving Time is enabled. The default setting is false.
<offset_hours>	To specify the time in hours between the standard time and daylight saving time. The values are 1 and 2. The default setting is 1.
<dst_start>	To specify when to apply the offset for daylight saving time.
<month>	To specify the month when to apply the offset.
<day>	To specify the day when to apply the offset.
<day_mode>	To specify the day mode when to apply the offset.
<hour>	To specify the hour when to apply the offset
<dst_stop>	To specify when to stop the offset for daylight saving time.
<month>	To specify the month when to stop the offset.
<day>	To specify the day when to stop the offset.
<day_mode>	To specify the day mode when to stop the offset.
<hour>	To specify the hour when to stop the offset.
<media>	To specify the media settings.
<security>	To specify the means of encryption configured for the phone.
<srtp>	To specify the SRTP parameters that the phone uses.
<srtcp>	To specify whether SRTCP is enabled.
<capneg>	To specify whether Capability Negotiation is enabled.
<codec>	To specify the codec settings.
<iLBC>	To specify the internet Low Bitrate Codec (iLBC) codec settings.
<prio>	To specify the codec priority (0–6).
<mode>	To specify the frame length in ms.

Table continues…

String	Description
<OPUS>	To specify the OPUS codec settings.
<prio>	To specify the codec priority (0–6).
<PCMU>	To specify the PCMU codec settings.
<prio>	To specify the codec priority (0–6).
<PCMA>	To specify the PCMA codec settings.
<prio>	To specify the codec priority (0–6).
<G722>	To specify the G722 codec settings.
<prio>	To specify the codec priority (0–6).
<G729>	To specify the G729 codec settings.
<prio>	To specify the codec priority (0–6).
<voice_quality_monitor>	To specify the Voice Quality Monitor settings.
<enable_rtcp_xr>	To specify whether the sending of RTCP XR is enabled.
<rtcp_xr_collector_uri>	To specify the Uniform Resource Identifier (URI) of the RTCP XR collector.
<rtp_pt_98_ilbc>	To specify that the server gets iLBC packets as payload type 98. By default it is set to 104. You can also set the value to 98 to ensure interoperability with specific systems.
<sip>	To specify SIP settings.
<primary_account>	To specify the primary account settings.
<name>	To specify the name of the account.
<user>	To specify the user-defined name of the account.
<registrar>	To specify the request URI for registration.
<proxy>	To specify the optional URI of the proxy to visit for all outgoing requests from the account.
<keep_alive>	To specify whether the keep-alive transmission for the account is enabled.
<cred>	To specify the array of credentials. In case of registration, at least one credential must be available to successfully authenticate the service provider. If you want proxies to challenge the requests in the route set, you must specify more credentials.
<realm>	To specify the realm.
<username>	To specify an authentication name.
<password>	To specify the password used for the account.
<reg_timeout>	To specify the optional interval for registration in seconds. If zero, the phone uses the default interval. The default setting is 300.
<secondary_account>	To specify the secondary account settings.

Table continues…

String	Description
<name>	To specify the name of the account.
<user>	To specify the user-defined name of the account.
<registrar>	To specify the request URI for registration.
<proxy>	To specify the optional URI of the proxy to visit for all outgoing requests from the account.
<keep_alive>	To specify whether the keep-alive transmission for the account is enabled.
<cred>	To specify the array of credentials. In case of registration, at least one credential must be available to successfully authenticate the service provider. If you want proxies to challenge the requests in the route set, you must specify more credentials.
<realm>	To specify the realm.
<username>	To specify an authentication name.
<password>	To specify the password used for the account.
<reg_timeout>	To specify the optional interval for registration in seconds. If zero, the phone uses the default interval. The default setting is 300.
<fallback_account>	To specify the fallback account settings.
<name>	To specify the name of the account.
<user>	To specify the user-defined name of the account.
<registrar>	To specify the request URI for registration.
<proxy>	To specify the optional URI of the proxy to visit for all outgoing requests from the account.
<keep_alive>	To specify whether the keep-alive transmission for the account is enabled.
<cred>	To specify the array of credentials. In case of registration, at least one credential must be available to successfully authenticate the service provider. If you want proxies to challenge the requests in the route set, you must specify more credentials.
<realm>	To specify the realm.
<username>	To specify an authentication name.
<password>	To specify the password used for the account.
<reg_timeout>	To specify the optional interval for registration in seconds. If zero, the phone uses the default interval. The default setting is 300.
<source_port>	To specify the source port to listen to.
<transport_protocol>	To specify the transport protocol which the phone must use.

Table continues…

String	Description
<tls>	To specify that TLS is selected as the transport protocol. This is followed by the corresponding transport protocol settings.
<tls_method>	To specify the TLS protocol method.
<tls_neg_timeout>	To specify the TLS negotiation time-out in seconds for both outgoing and incoming connections. If zero, the phone uses no time-out.
<tls_password>	To specify the password for the private key.
<verify_client>	To specify whether the phone must verify the client.
<verify_server>	To specify whether the phone must verify the server.
<require_client_cert>	To specify whether the phone requires the client certificate.
<advanced>	To specify the configured advanced SIP settings.
<disable_rport>	To specify whether the remote port forwarding is enabled. The default setting is disabled.
<session_timers>	To specify the chosen time-related mechanism to disconnect the sessions.
<session_expiration_minimum>	To specify the minimum session expiration value in seconds. The default value is 90 seconds.
<session_expiration>	To specify the session expiration value in seconds. The default setting is 1800 seconds.
<outbound_proxy>	To specify the IP address of the outbound proxy.
<enable_sip_traces>	To specify whether the provision of key information for troubleshooting is enabled. The default setting is disabled.
<allow_contact_rewrite>	To specify whether the storing of the IP address from the response of the register request is enabled.
<enable_sip_replaces>	To specify whether the SIP Replaces header must be used.
<contact_use_src_port_even_with_dns>	To specify whether the SIP stack should continue to retrieve the local ephemeral port even if the stack is configured with DNS.
<enable_lock_codec>	To specify whether the lock codec feature is enabled.
<dtmf>	To specify DTMF signalling settings.
<method>	To specify the DTMF signalling method.
<rfc4733_payload_type>	To specify the type of audio traffic.
<nat_traversal>	To specify the configured NAT traversal settings.
<ice>	To specify whether ICE is configured for the phone.
<enable>	To specify whether ICE is enabled.
<stun>	To specify whether STUN is configured for the phone.

Table continues…

String	Description
<enable>	To specify whether STUN is enabled.
<server>	To specify the IP address or the public name of the STUN server.
<turn>	To specify whether TURN is configured for the phone.
<enable>	To specify whether TURN is enabled.
<server>	To specify the IP address or the public name of the TURN server.
<user>	To specify the user authentication name on the TURN server.
<password>	To specify whether the user authentication password on the TURN server is set.
<phone>	To specify the configured basic settings of the phone.
<name>	To specify the name of the phone.
<language>	To specify the language selected.
<allow_legacy_encryption>	To specify whether the legacy encryption mode is enabled. The default setting is false.
<password>	To specify the password used.
<ringlevel>	To specify the volume level configured.
<key_tone>	To specify whether the key tone is enabled.
<is_daisy_chain_slave>	To specify the mode of the phone in case of a daisy chain arrangement.
<phone_status_api>	To specify whether the phone status API feature is enabled.
<sleep_mode_timeout>	To specify the time-out value in minutes.
<enable_startup_sound>	To specify whether the start-up sound is enabled. The default setting is true.
<bluetooth>	To specify the Bluetooth parameters.
<enable>	To specify whether Bluetooth is enabled. The default setting is true.
<network>	To specify the network parameters.
<dhcp>	To specify whether the phone uses DHCP to obtain network settings.
<hostname>	To specify the hostname of the phone.
<domain>	To specify the domain name of the phone.
<dns1>	To specify Domain Name Server (DNS) 1 of the phone.
<dns2>	To specify DNS 2 of the phone. You can use maximum two DNS.
<static_ip>	To specify the static IP settings.

Table continues…

String	Description
<ip>	To specify the IP address of the phone if DHCP is disabled.
<netmask>	To specify the network mask for your phone.
<gateway>	To specify the gateway for the phone.
<vlan>	To specify whether VLAN is enabled. The default setting is disabled.
<vlanid>	To specify the ID number that the phone uses for all IP telephony communication through VLAN.
<ieee_8021x>	To specify IEEE 802.1x parameters.
<enable>	To specify whether IEEE 802.1x is enabled. It is disabled by default.
<username>	To specify the phone username if IEEE 802.1x is enabled.
<eap_md5>	To specify whether the phone uses MD5 EAP method.
<enable>	To specify whether MD5 EAP method is enabled.
<password>	To specify the password for MD5 EAP method.
<eap_tls>	To specify whether the phone uses TLS EAP method.
<enable>	To specify whether TLS EAP method is enabled.
<password>	To specify the password for the TLS EAP method.
<lldp>	To specify the LLDP settings.
<enable>	To specify whether the LLDP settings are enabled. These settings are enabled by default.
<country>	To specify the country of the phone location.
<country_subdivision>	To specify the region of the country of the phone location.
<county>	To specify the county, parish, district, or other applicable administrative division.
<city>	To specify the city of the phone location.
<city_division>	To specify the city district or area of the phone location.
<block>	To specify the block within the city district.
<street>	To specify the street of the building where the phone is located.
<direction>	To specify the direction of moving towards the location of the phone.
<trailing_street_suffix>	To specify the trailing street suffix.
<street_suffix>	To specify the street suffix.
<number>	To specify the number of the building where the phone is located.

Table continues…

String	Description
<number_suffix>	To specify the building number suffix.
<landmark>	To specify the reference point for the location of the phone.
<additional>	To specify any additional information related to the phone location.
<name>	To specify the name of the company that owns the phone.
<zip>	To specify the ZIP-code of the phone location.
<building>	To specify the name or number of the building of the phone location.
<unit>	To specify the unit within the building where the phone is located.
<floor>	To specify the floor of the building for the location of the phone.
<room>	To specify the room in the building where the phone is located.
<place_type>	To specify the type of setting, for example, office.
<script>	To specify the script.
<elin>	To specify Emergency Location Identification Number (ELIN).
<qos>	To specify the quality of service (QoS) parameters.
<dscp_sip>	To specify a value in the range from 0 to 63 to prioritize the SIP messages.
<dscp_media>	To specify a value in the range from 0 to 63 to prioritize the media packets.
<device_management>	To specify the Device Management settings.
<enable>	To specify whether Device Management is enabled.
<update_interval>	To specify the update interval in the range from 1 minute to 21,000 minutes. The default setting is 60 minutes.
<update_max_wait>	To specify the maximum time in seconds the phone waits for the update.
<server>	To specify the Device Management server address if it is not provided by the DHCP option.
<check_server_certificate>	To specify whether the Check certificate is enabled.
<lowest_tls_version>	To specify the lowest TLS version for the phone.
<dhcp_option>	To select the DHCP option used for the Device Management server address.
<des>	To specify the Device Enrollment Services settings.
<des_stat>	To specify user setting of DES enablement.

Table continues…

String	Description
<logging>	To specify the syslog settings.
<remote_syslog_enable>	To specify whether the remote syslog feature is enabled.
<remote_syslog_host>	To specify the IP address or the host of the remote syslog server.
<ldap>	To configure the LDAP options.
<enable>	To enable the LDAP feature. By default it is disabled.
<name_filter>	To define how the phone applies the entered search characters.
<server_url>	To specify the URL of the LDAP server host. It includes the protocol (LDAP/LDAPS) and the port number.
<search_base>	To specify the distinguished name of the search base.
<username>	To specify the username for the LDAP server.
<password>	To specify the password for the LDAP server.
<max_hits>	To specify the maximum number of hits to return for each LDAP search.
<country_code>	To specify the country code of the phone location.
<area_code>	To specify the area code of the phone location.
<external_prefix>	To specify a special prefix for dialing external numbers.
<min_length_for_ext_prefix>	To restrict the external prefix that the phone adds only if the phone number is longer than the minimum length.
<exact_length_for_no_ext_prefix>	To specify the exact length for the phone numbers if the phone adds no external prefix.
<number_prefix_for_no_ext_prefix>	To specify the initial number for the phone numbers in case of using which the phone adds no external prefix.
<number_attributes>	To specify if there are configured number attributes.
<display_name>	To specify how the phone displays the name it searched for.
<sort_results>	To specify if the phone sorts the search hits based on the Display name.
<use_dm_certificates_for_ldaps>	To specify if the phone uses any device management certificates for LDAPS.
<httpd>	To configure the web server options.
<min_allowed_tls_version>	To specify the minimum allowed TLS version. The default setting is 1.2. To enable support of TLS v.1.0 and TLS v.1.1, set the value to `all`.

Exporting the configuration file

About this task

Use this procedure to export the configuration file from your Avaya Conference Phone B199.

Before you begin

Decide where the exported configuration file will be saved. By default, it is saved in the folder for downloaded files on your PC.

Procedure

1. On the web interface, click **Provisioning**.
2. In the Configuration section, click **Export Configuration** button.

   The web browser shows the configuration file.
3. Save the page in an .xml format in the dedicated folder.
4. **(Optional)** Edit the .xml file in a suitable application.

Importing the configuration file

About this task

Use this procedure to import the previously saved configuration file to your Avaya Conference Phone B199.

Procedure

1. On the web interface, click **Provisioning**.
2. Go to the Configuration section.
3. In **Import Configuration**, click the **Choose file** button.
4. Locate the configuration file in the folder where it is stored.
5. Select the file in an .xml format and open it.

   The name of the chosen file is near the **Choose file** button.
6. Click **Save**.

   The phone reboots or restarts to import the configuration if the configuration file application requires this reboot or restart.

Validation and migration of configuration

Starting from Release 1.0.1, Avaya Conference Phone B199 validates and migrates the phone configuration to ensure consistency of the configuration file with the firmware version. With this

feature, the phone provides reliable automatic migration of the configuration file to match the newer firmware version if necessary.

Configuration validation

B199 Conference Phone validates compatibility of the configuration with the firmware against an xml schema file based on the configuration file version.

Starting from Release 1.0.1, a configuration file has a version number attribute. The phone application compares the configuration file version to the firmware version running on the phone to determine the migration steps required to make the configuration file consistent with the firmware.

All the configuration files that B199 Conference Phone generated before Release 1.0.1 acquire the `<B199 version="0">` attribute in the xml root element. The configuration files generated with Release 1.0.1 acquire the `<B199 version="1">` attribute. With each new release, the configuration service increases the configuration file version number by one leaving the incompatible configuration changes attributed to previous file versions.

Note:

The phone does not support downgrade of a configuration file.

Important:

To avoid failure of the configuration file import or automatic provisioning, ensure that you do not change the version number in a configuration file manually.

Configuration migration

The migration feature ensures seamless import of the configuration data in the following cases:

- During the phone boot
- During the configuration file import using the web interface
- During automatic provisioning of the phone using Device Management

Configuration import can fail if the configuration file does not match the xml schema file. In this case, you see the following message on the phone web interface: `Failed to migrate configuration file`.

Device Management

The Device Management feature facilitates upgrade and configuration of multiple conference phones. To use this feature, you must configure it. By default, Device Management is enabled.

Avaya Conference Phone B199 upgrades and sets configuration by using the Device Management files. The necessary files must be available on a server reachable from all the phones. This server is called the provisioning server. The service provider is in charge of uploading the necessary files to the provisioning server.

The device controls the configuration and firmware download with a frequency of 1 hour.

Files on the provisioning server

The following files must be available on the provisioning server:

- Firmware file
- Firmware metadata file
- Global configuration file
- Device-specific configuration file (optional)
- Global certificate configuration file
- Device-specific certificate configuration file (optional)

Configuration priorities

The following table describes the priorities for files downloaded to the phone during the Device Management configuration upgrade:

File type	Description
Configuration file	The global configuration file has the highest priority. If the device-specific configuration file is present on the provisioning server, the phone downloads it after the global configuration file. If the new configuration file contains the same parameters as already configured by the user, all user configurations are overridden during the Device Management update.
Certificate configuration file	The device-specific certificate configuration file has the highest priority. The phone downloads the global configuration file only after it tried to download the device-specific configuration file. The certificates the phone downloads from the provisioning server overwrite any certificates you downloaded manually using the phone web interface.

Related links

Certificate configuration files on page 117
Configuration file on page 98

Device Enrollment Services

Avaya Conference Phone B199 supports the Device Enrollment Services (DES) solution which simplifies and automates the discovery of the provisioning server. If you install the phone using DES, you do not need to configure the provisioning server manually. You can use DES to provide configuration parameters to B199 Conference Phone and to manage firmware updates.

Note:

The Device Enrollment Services feature is not supported in IP Office.

The Device Enrollment Services feature works only if a provisioning server is configured in the Avaya DES for the MAC address of your B199 Conference Phone. The manufacturer starts the device setup by entering the device details, such as certificate information, MAC address, and

serial numbers. The details are imported to the DES server through a file, which enables the device to authenticate with DES. Then, the service provider or administrator can log in to DES to configure customer information and provisioning settings.

For more information, see *Using Avaya Device Enrollment Services to Manage Endpoints*.

Device Enrollment Services enrollment code

The service provider can enroll the devices at Device Enrollment Services (DES) with or without a numeric enrollment code (NEC).

Note:

Avaya Conference Phone B199 supports only 8-digit NECs.

If your phone is configured to be enrolled with an enrollment code, the DES server prompts you to enter NEC on the phone at the beginning of provisioning with DES. After you enter the enrollment code, the phone contacts DES to obtain data stored on its configuration server and then contacts the configuration server to download the settings.

You can cancel the operation of entering the enrollment code. In this case, you must specify the configuration server manually.

The service provider or the seller is in charge of providing the enrollment code to the customer.

Provisioning Avaya Conference Phone B199 using Device Enrollment Services

About this task

An out-of-the-box phone supports the discovery of the configuration file server from Device Enrollment Services (DES) during the initial boot. You can accept or bypass the automatic provisioning with DES.

Before you begin

Ensure that DES contains the configuration file server for your B199 Conference Phone. Also, ensure that you have the enrollment code, if needed. You can obtain the necessary information from the service provider.

After the phone boots up, it prompts you to enable or disable DES discovery by showing the following question: `Perform auto provisioning?` When you see this message, do one of the following:

- Tap **Yes** to start automatic provisioning with DES.

  B199 Conference Phone contacts the DES server. The DES server redirects the phone to the configured file server from which the phone receives all the configuration parameters and the upgrade file for installation.

- Tap **No** to skip DES automatic provisioning during this boot session.

In this case, the administrator must provide all the parameters related to configuration through the phone interface or the web interface.

Note:

If you do not choose any of the options within the next 30 seconds, the phone closes the prompt and skips the automatic provisioning as if you tapped **No**.

Next steps

After the first boot session, as an administrator, you can disable the DES functionality.

Starting automatic provisioning

About this task

You can start automatic provisioning with the Device Enrollment Services (DES) server manually from either the DES menu on Avaya Conference Phone B199 or the phone web interface.

Procedure

1. Log in as the administrator.
2. To start automatic provisioning, do one of the following:
   - On the phone, tap **Settings** > **Device Management** > **DES Provisioning** > **DES Auto Provisioning**.
   - On the web interface, go to the **Provisioning** tab, and in the DES Provisioning section, click **DES Auto Provisioning**.

   The phone prompts you to start or cancel auto provisioning with the following question:
   `Perform auto provisioning?`
3. In the dialogue box, tap **Yes** to start automatic provisioning.

   Tap **No** to cancel automatic provisioning. In this case, the phone will continue showing the DES prompt at boot until you choose to perform automatic provisioning and tap **Yes** in the prompt.

Device Enrollment Services error prompt

In certain cases, for example, when the phone fails to send request to the Device Enrollment Services (DES) server, or when the provisioning server fails to verify the CA certificate, the DES server responds with an error message. In such cases, Avaya Conference Phone B199 displays DES warning icon and an error prompt with the following question:

`Do you want to report the issue?`

In the prompt, you can choose one of the following options:

- Yes: To send the report about the error and to remove the DES warning icon.
- No: To not send the report and to leave the DES warning icon.

- Never: To not send the report and to remove the DES warning icon.

Note:

With R.1.0.2 and earlier, B199 Conference Phone does not have the reporting feature. Therefore, the phone does not send the report when you choose Yes.

Disabling Device Enrollment Services

About this task

After the first boot, as the administrator, you can disable Device Enrollment Services (DES) directly on the phone or through the web interface.

Procedure

Do one of the following:

- On the phone, navigate to **Settings** > **Device Management** > **DES Provisioning** > **DES Enablement**, and tap **Disabled**.
- On the web interface, navigate to **Provisioning** > **DES Provisioning**, and click **Disabled**.
- In DHCP option 242, set **DES_STAT** to `0`.
- In the configuration file, set **DES_STAT** to `0` or `1`.

The **DES_STAT** parameter received in DHCP option 242 can have one of the three values: `0`, `1`, or `2`. The following table describes the values:

DES_STAT value	Description
`DES=0`	DES is completely disabled and you cannot see any settings related to DES on the phone or on the web interface. After factory reset, the DES feature is enabled in the configuration file.
`DES=1`	DES is disabled, and you can enable or disable DES using the phone interface or the web interface.
`DES=2`	DES is enabled and you cannot disable DES from the phone or the web interface. The provisioning using DES is performed automatically during the phone start-up. You can start the automatic provisioning by pressing the **DES Auto Provisioning** button in the phone interface or the web interface. `DES=2` is the default option.

Firmware downgrade with DES provisioning

You can initiate a downgrade by uploading an older firmware than the one currently available on the DES server. In this case, DES provisioning starts automatically. Avaya Conference Phone B199 applies the received configuration and restarts with the downloaded settings.

After a downgrade, the phone tries to make provisioning with each reboot. The reboot attempts happen if previously the phone used DES for provisioning. After completion of the first successful provisioning, the phone stops provisioning attempts on the next reboot.

You can also do a factory reset to stop the phone provisioning attempts on reboot.

Note:

If the phone has DES enabled, provisioning starts automatically. In case of any failure after the downgrade, the phone displays a DES provisioning error message. In this case, you can disable DES in the phone settings and reboot.

Related links

Factory reset on page 125

Configuring Device Management settings on the phone

About this task

Use this procedure to configure the Device Management settings on the phone.

Procedure

1. Log in as the administrator.
2. On the phone screen, tap **Settings** > **Device Management**.
3. Choose the parameter that you want to configure and proceed to the options available.
4. After you made the choices, return to the home screen.

   The phone reboots to apply the changes.

Configuring Device Management settings through the web interface

About this task

Use this procedure to configure the Device Management settings through the web interface.

Procedure

1. Log in as the administrator.
2. On the web interface, click **Provisioning**.
3. Make the appropriate configurations.
4. Click **Save**.

   The phone reboots to apply the changes.

Device Management settings

The following table lists the Device Management settings of Avaya Conference Phone B199 available through the web interface in the Provisioning tab in the Device Management section or on the phone in **Settings** > **Device Management**.

Note:

Starting from R.1.0.1, Device Management functionality works only if DES functionality is disabled. If Device Management and DES are both enabled, only DES functionality works. To use Device Management, you need to disable DES using the phone interface or the web interface.

Name	Description
Enable	To enable or disable Device Management. The options are: • On: Device Management is enabled. This is the default setting. • Off: Device Management is disabled.
Update interval	To specify the update interval in minutes the phone waits to re-sync with the provisioning server. The default value is 60 minutes. The phone accepts values in the range from 1 to 21,000. **Note:** You can configure this parameter through the web interface or through the .xml configuration file.
Maximum time to wait to update	To specify the maximum time in seconds the phone waits for the update. By default, it is 1 minute. This time-out is not used during the first start of Device Management. Device Management starts for the first time as soon as the network is configured. After that, Device Management starts at the intervals you specified using the **Update interval** parameter and uses the **Maximum time to wait to update** value. **Note:** You can configure this parameter through the web interface or through the .xml configuration file.
Provisioning Server	To specify the Device Management server address if it is not provided by the DHCP option.
Check Server Certificate	To enable or disable the verification of the authentication with a certificate. The options are: • On: Server certificates are checked. • Off: Server certificates are not checked. This is the default setting.
Lowest TLS Version	To specify the lowest TLS version for the phone. The options are: • **1** • **1.1** • **1.2**

Table continues…

Name	Description
DHCP Option	To select the DHCP option used for the Device Management server address. With all DHCP options, the phone obtains the URL and directory of the server where the configuration file is located. The Device Management server then looks for `avayab199.xml` as a global configuration file, and `avayab199-<MAC>.xml` for a device-specific file. The DHCP options are: • **43**: Vendor specific. • **56**: DHCP message. • **60**: Class ID. • **61**: Client ID. • **66**: Server name. • **67**: Bootfile name. • **242**: The brand-specific option. • **Off** • **Auto**: This is the default setting.
DES Provisioning	To enable or disable provisioning using DES.
Certificate	To upload a certificate to the phone. This certificate is used for authentication in Device Management.
CA Certificate	To upload a root certificate. It contains a public key, which is used to verify other certificates when using Device Management.
Private Key	To upload a private key. It is used for authentication when using Device Management.

Related links

Disabling Device Enrollment Services on page 112

Files on the provisioning server

The following files must be available on the provisioning server:

- Firmware file
- Firmware metadata file
- Global configuration file
- Device-specific configuration file (optional)
- Global certificate configuration file
- Device-specific certificate configuration file (optional)

Global configuration file

The global configuration file contains the basic configuration, that is, all settings that are common for all conference phones in your location. The easiest way to create this file is to configure Avaya Conference Phone B199 and export the configuration file, or use the built-in configuration file creator.

The default name for this file is `avayab199.xml`.

Instead of the .xml file format, you can also use cgi, php, asp, js, or jsp file formats. B199 Conference Phone first searches for the configuration file in .xml format. If the phone fails to find the .xml file on the provisioning server, it searches for the configuration file in other formats specified above.

Creating the global configuration file

About this task

Use this procedure to create the global configuration file. This file contains the general information about the phone settings and must be created after you set all the basic configurations of Avaya Conference Phone B199.

Before you begin

Enable the **Device Management** option and ensure that all the required server information is filled in.

Procedure

1. On the web interface, click **Provisioning**.
2. In the Configuration section, click **Export Configuration**.

   The configuration file is created.
3. **(Optional)** Edit the .xml file in a suitable editor.
4. Save the file as `avayab199.xml` in the dedicated folder. The folder is located at the address specified in the **Provisioning Server** field.

   Important:

   Do not use a custom name for this file because the file name `avayab199` is hardcoded in Device Management configuration and it will not search for files with a different name.

Next steps

Delete the local information from the global configuration file to avoid confusion in the future. Local information is information specific to the device, for example, account information.

Device-specific configuration file

The device-specific configuration file contains configuration parameters that are unique for every phone. The settings in this file have priority over the settings in the global configuration file.

The default name for this file is `avayab199-<MAC>.xml`, where <MAC> is the MAC address of the specific phone.

Instead of the .xml file format, you can also use cgi, php, asp, js, or jsp file formats. B199 Conference Phone first searches for the configuration file in .xml format. If the phone cannot find the .xml file on the provisioning server, it searches for the configuration file in the other formats.

Creating the device-specific configuration file

About this task

Use this procedure to create the device-specific configuration files. They contain information about the unique settings of each Avaya Conference Phone B199.

Before you begin

Obtain MAC addresses of all your B199 phones. Ensure that you write the MAC address without colons.

Procedure

1. On the web interface, click **Provisioning**.
2. In the Configuration section, click **Export Configuration**.

   The phone creates a configuration file.
3. Edit the .xml file in a suitable editor.

   The file must contain only the elements that are unique for a specific phone.
4. Save the file as `avayab199-<MAC>.xml` in the dedicated folder located at the address specified in the **Provisioning Server** field.

   Important:

   Do not use a custom name for this file because the file name `avayab199-<MAC>` is hardcoded in Device Management configuration and it will not search for files with a different name.

Certificate configuration files

Certificate configuration files stored on the provisioning server allow you to automatically download certificate files to Avaya Conference Phone B199. These files are required for the server validation by the phone and TLS authentication by the server.

The service provider can upload a global certificate configuration file and a device-specific certificate configuration file.

The default name for global configuration file is `avayab199_certcfg.xml`. The default name for device-specific configuration file is `avayab199_certcfg-<MAC>.xml`, where

`<MAC>` is the MAC address of the specific phone.

Instead of the .xml file format, the service provider can also use cgi, php, asp, js, or jsp file formats. B199 Conference Phone first searches for the configuration file in .xml format. If the phone fails to find the .xml file on the provisioning server, it searches for the configuration file in other formats specified above.

The typical certificate configuration file consists of 4 sections:

- 802.1x. The section specifies the 802.1x certification arrangements of the phone.
- SIP. The section contains the Session Initiation Protocol (SIP) certification arrangements of the phone.
- Provisioning. The section runs through the provisioning server certification arrangements of the phone.
- LDAP. The section specifies the LDAP server certificate arrangements of the phone.

Note:

In some cases the certificate configuration file can lack some sections. This happens if the relevant certificates are not available for the phone.

Each section includes the following certificate files:

- CA certificate
- Device certificate
- Device private key.

Each section contains the path details for CA certificate, Device certificate, and Device private key.

Note:

The path to the certificate can be a relative path or a complete URI. For example, a relative path can look like `<ca_uri>ca.crt</ca_uri>` or `<ca_uri>certs/ca.crt</ca_uri>`. In the first case, the phone looks for the `ca.crt` file in the same catalog with the configuration file. In the second case, the phone looks for the `ca.crt` file in the `certs` catalog relative to the configuration file.

The file can have the path to the certificate in the form of a complete URI, like `<ca_uri>https://hostname.io/path/ca.crt</ca_uri>`. In this case, the phone uses a specific URI to download the certification file.

The section also specifies an MD5 checksum for each element in it. MD5 checksum (also called MD5 hash algorithm) is a type of digests of the specified certificates.

Note:

The phone starts downloading the certificate if the MD5 hash value is different from the MD5 hash of the certificate file that Avaya Conference Phone B199 stores or if no certificate has

been uploaded before. That means, that the phone downloads one certificate file only once and then checks that it is still the same.

Certificate configuration file structure

The table below shows the format of the certificate file:

String	Description
<certificates>	To specify the certificates that the phone applies.
<ether_8021x>	To specify the 802.1x certification arrangements of the phone.
<ca_uri>	To specify 802.1x path to check the CA certificate.
<ca_hash algo="md5">	To specify the MD5 hash algorithm that the phone uses to verify 802.1x CA certificate.
<cert_uri>	To specify 802.1x path to get the device certificate.
<cert_hash algo="md5">	To specify the MD5 hash algorithm that the phone uses to verify 802.1x device certificate.
<privkey_uri>	To specify 802.1x path to get the private key.
<privkey_hash algo="md5">	To specify the MD5 hash algorithm that the phone uses to verify 802.1x private key.
<sip>	To specify the SIP certification arrangements of the phone.
<ca_uri>	To specify the path to get the CA certificate for the SIP connection.
<ca_hash algo="md5">	To specify the MD5 hash algorithm that the phone uses to verify the CA certificate for the SIP connection.
<cert_uri>	To specify the path to get the device certificate for the SIP connection.
<cert_hash algo="md5">	To specify the MD5 hash algorithm that the phone uses to verify device certificate for the SIP connection.
<privkey_uri>	To specify the path to get the private key for the SIP connection.

Table continues…

String	Description
<privkey_hash algo="md5">	To specify the MD5 hash algorithm that the phone uses to verify the private key for the SIP connection.
<provisioning>	To specify the provisioning server certification arrangements of the phone.
<ca_uri>	To specify the path to get the CA certificate for connection to the provisioning server.
<ca_hash algo="md5">	To specify the MD5 hash algorithm that the phone uses to verify the CA certificate for connection to the provisioning server.
<cert_uri>	To specify the path to get the device certificate for connection to the provisioning server.
<cert_hash algo="md5">	To specify the MD5 hash algorithm that the phone uses to verify the device certificate for connection to the provisioning server.
<privkey_uri>	To specify the path to get the private key for connection to the provisioning server.
<privkey_hash algo="md5">	To specify the MD5 hash algorithm that the phone uses to verify the private key for connection to the provisioning server.
<ldap>	To specify the LDAP server certificate arrangements of the phone.
<ca_uri>	To specify the path to get the CA certificate for connection to the LDAP server.
<ca_hash algo="md5">	To specify the MD5 hash algorithm that the phone uses to verify the CA certificate for connection to the LDAP server.
<cert_uri>	To specify the path to get the device certificate for connection to the LDAP server.
<cert_hash algo="md5">	To specify the MD5 hash algorithm that the phone uses to verify the device certificate for connection to the LDAP server.
<privkey_uri>	To specify the path to get the private key for connection to the LDAP server.
<privkey_hash algo="md5">	To specify the MD5 hash algorithm that the phone uses to verify the private key for connection to the LDAP server.

The following is the example of the certificate configuration file for Avaya Conference Phone B199. Note that it contains only 2 out of 4 sections.

```
<certificates>
        <ether_8021x>
            <ca_uri>8021x_ca.crt</ca_uri>
```

```
            <ca_hash algo="md5">c49d8fd0cbb6bfc26ef752296d6d17f7</ca_hash>
            <cert_uri>8021x_dev.crt</cert_uri>
            <cert_hash algo="md5">ca059972d02b2853a92704a7a7640f3f</cert_hash>
            <privkey_uri>8021x_priv.key</privkey_uri>
            <privkey_hash algo="md5">f4728d6356204c6fcce91989ef733553</privkey_hash>
        </ether_8021x>
        <provisioning>
            <ca_uri>prov_ca.crt</ca_uri>
            <ca_hash algo="md5">e5116932d3685ea18ead10a55b825145</ca_hash>
        </provisioning>
    </certificates>
```

Firmware binary

This file contains the firmware binary that is downloaded and installed by Avaya Conference Phone B199 if the metadata file shows that it is newer than the currently installed version.

The binary file can be downloaded from http://support.avaya.com/.

Firmware metadata file

Firmware metadata file is file in .xml format with information of the firmware version in the binary file. The file is used to check whether the binary file must be downloaded to the phone.

The name of this file is set as `avayab199_fw_version.xml`. The file contains the following elements in xml format:

- Firmware version
- Filename
- Checksum of the firmware binary

The following is the example of the firmware binary file:

```
<firmware_version>
    <version>2.3.9</version>
    <filename>avayab199_v2.3.9.kt</filename>
    <checksum>XXXX</checksum>
</firmware_version>
```

Note:

If the firmware binary file which is specified in the firmware metadata file is not uploaded to the provisioning server, the phone fails to upgrade and shows the following error message after reboot: `Upgrade failed`.

Creating firmware binary and metadata files

About this task

Use this procedure to create the firmware binary and metadata files manually. Apply them to check if a newer firmware version for your Avaya Conference Phone B199 is available.

Before you begin

Collect the information about the version, file name, and checksum of the firmware binary for the phone.

Procedure

1. Place the firmware binary file on the Device Management server.
2. Create a firmware metadata file containing the version, file name, and checksum of the firmware binary.
3. Save the file as `<file name>.kt` in the dedicated folder located at the address specified in the **Provisioning Server** field.
4. **(Optional)** Add the file type .kt to the MIME settings on the server after the files creation.

Upgrading multiple devices

About this task

You can upgrade firmware on multiple Avaya Conference Phone B199 devices using Device Management instead of upgrading each phone individually. For this purpose, Device Management must be enabled for the devices, the provisioning server must be specified for the devices, and the firmware binary file and the firmware metadata file must be available on the provisioning server.

Before you begin

Ensure that the firmware filename matches the `<filename>` value in the metadata file, and that the firmware version in both files is the same.

Procedure

1. Check if Device Management is enabled on the phones you want to upgrade and enable if necessary.

   You can do this on the phone by logging in as an administrator and navigating to **Settings** > **Device Management** or through the web interface on the **Provisioning** tab in the **Device Management** section.

2. Check if the provisioning server is configured for the phones you want to upgrade and configure if necessary.

   You can do this on the phone by logging in as an administrator and navigating to **Settings** > **Device Management** or through the web interface on the **Provisioning** tab in the **Device Management** section.

3. Upload the binary file and the firmware metadata file to the provisioning server.

   When the phones contact the provisioning server, the upgrade process starts.

Next steps

You can check the firmware version from the phone by navigating to **Settings** > **Status** or through the web interface in the **Status** tab.

Related links

Device Management settings on page 113
Firmware metadata file on page 121
Firmware binary on page 121

Configuring multiple devices

About this task

You can configure multiple Avaya Conference Phone B199 devices using the configuration file as a management tool instead of configuring the settings on each phone individually. For this purpose, you need to export the configuration file, edit the settings as necessary, and then place the configuration file to the provisioning server.

Before you begin

Ensure that you or the service provider have configured the provisioning server for your phones.

Procedure

1. Log in to the web interface.
2. Export the configuration file by clicking **Export Configuration** on the Provisioning tab.

   The phone generates the global configuration `avayab199.xml` file.
3. **(Optional)** Edit the configuration file using a suitable application.

   Note:

   The settings file might not contain some settings if they represent a default value. To include such settings in the configuration file, you need to change them to a non-default value using the phone interface or the web interface.
4. Upload the file to the provisioning server.

   During the next Device Management configuration upgrade, the system applies the configuration file to the phones. After the phones reboot, they all have the same settings specified in the configuration file.

Related links

Creating the global configuration file on page 116
Configuration file on page 98
Device Management on page 108

Remote syslog server

Avaya Conference Phone B199 supports syslog protocol to allow centralized log management. You can configure the phone so that it logs to a remote server and sends the syslog messages to your own system or a third-party system.

With the remote syslog feature enabled, the phone sends the syslog messages to the syslog server and also logs them in the local log.

By default, the remote logging feature on B199 Conference Phone is in the disabled state.

Configuring remote syslog settings

About this task

To use the remote syslog feature, you need to do the following:

- Enable your phone to deliver syslog messages to the syslog server.
- Configure the destination server which receives the syslog events.

You can do this using the configuration file stored on the Device Management server. You can find the syslog settings under the `<logging>` section of the configuration file.

Note:

The default syslog port is 514, and you cannot change this setting.

The `<remote_syslog_host>` tag can be missing in the `<logging>` section if you use a configuration file exported from the phone application. This can happen because the `<remote_syslog_host>` default value is blank, and the phone application does not export blank tags.

Before you begin

Obtain the configuration .xml file for Avaya Conference Phone B199.

Procedure

1. In the configuration file, go to the `<logging>` section.
2. Set the value in the `<remote_syslog_enable>` tag to `true` as shown in the following example:

   ```
   <remote_syslog_enable>true</remote_syslog_enable>
   ```

3. Specify the host URL in the `<remote_syslog_host>` tag as shown in the following example:

   ```
   <remote_syslog_host>1.2.3.4</remote_syslog_host>
   ```

   Replace the 1.2.3.4 with the IP address or hostname of your remote syslog server.

4. Save the configuration file.

Next steps

Upload the configuration file to the Device Management server or import the configuration file to the phone using the web interface.

The phone sends syslog messages to the syslog server after the next reboot. The phone continues sending syslog messages until you set the `<remote_syslog_enable>` parameter in the configuration file to `false`.

Related links

Importing the configuration file on page 107
Configuring Device Management settings through the web interface on page 113
Exporting the configuration file on page 107
Configuration file on page 98

Fall back server support

Avaya Conference Phone B199 registers concurrently with the primary and secondary proxy servers. The phone also supports provisioning of a third-party fall back server when a connection with the primary or secondary server cannot be established. You can configure the third-party server details by using the web interface and the configuration file.

Factory reset

If for any reason, you must restore the factory settings on your Avaya Conference Phone B199, you can do it by means of the factory reset. In this case the phone removes all user-specific settings and returns to the factory settings. After the procedure is completed, you can repeatedly configure the settings.

Note:

The factory reset does not delete the self-signed certificate from the phone.

Also, the Device Enrollment Services feature is enabled after the factory reset in the configuration file. However, if it is disabled on DHCP server in 242 option (`DES_STAT=0`), you will not see the DES prompt during the phone start-up.

Performing factory reset

About this task

You can reset your Avaya Conference Phone B199 to factory default. You can do the factory reset only on the phone after you log in as the administrator.

If you need to perform the factory reset without logging in as the administrator, follow the procedure described in Performing system recovery on page 126.

Procedure

1. Log in to the phone as the administrator.
2. On the phone screen, tap **Settings** > **Phone**.
3. Tap **Factory Reset**.

The phone shows the following message: `Reset configuration to factory default. Press OK to confirm.`

4. Tap **Ok** to confirm the reset.
5. **(Optional)** Tap **Cancel** to return to the **Phone** settings.

System recovery

As an administrator, you can perform system recovery on Avaya Conference Phone B199 to return the phone to operable state, for example, after a faulty upgrade or when the phone application fails. System recovery replaces the current firmware with the previously installed operable firmware version.

You can also perform system recovery to reset the administrator password.

Note:

System recovery erases all settings including the account information.

Performing system recovery

Before you begin

Ensure that you save the configuration file from your B199 Conference Phone. System recovery erases all settings.

Procedure

1. Power cycle the phone to start the boot process.
2. When the LEDs turn green, start tapping the **Microphone Muted** button on the phone and continue tapping until the LEDs turn off.
3. Tap the **Microphone Muted** button once again.
4. When the LEDs turn red, tap the **Volume up** button once to confirm the system recovery.

   The LEDs turn off. The phone starts regular boot. After the boot up, the phone displays the following message: `Upgrade the phone to complete recovery`.

   Tip:

   If you want to cancel the system recovery, do not tap **Volume up** button on the phone when the LEDs turn red.
5. After the phone boots up, set the administrator password.
6. Upgrade the phone to complete system recovery.

Next steps

Upload the configuration file with necessary settings.

Related links

Setting the password for Avaya Conference Phone B199 on page 23
Provisioning on Avaya Conference Phone B199 on page 96

Web interface settings

The web server in Avaya Conference Phone B199 supports secure connections using HTTPS. You can configure this parameter only through the web interface.

Important:

The phone supports connection to the web interface only through `https`.

The following table shows the web interface settings that you can configure for B199 Conference Phone in the **Provisioning** tab:

Name	Description
Secure HTTP	
Webapp HTTPs Certificate	To upload a .PEM certificate to B199 Conference Phone to use HTTPS. **Note:** B199 Conference Phone supports certificates in the .PEM format only. You must convert the certificates and private keys to .PEM before using in the phone. For more information, see Converting the certificates to .PEM format on page 74

You can use the following command to generate a HTTPS web interface certificate:

```
openssl req -new -x509 -keyout https _ web _ certificate.pem -out
https _ web _ certificate.pem -day <number of days>-nodes
```

Device status view

You can view the configured settings of your Avaya Conference Phone B199 through the web interface and get information about the device, logs, and licenses.

You can use this information for troubleshooting.

Device status

You can find the information about Avaya Conference Phone B199 status, including its current settings, through the web interface. This information can be useful for troubleshooting.

The following table describes the type of the information available in each of the Status tab sections.

Section name	Description
General	To show the status information of B199 Conference Phone, including the following: • Phone Name • Product Name • Build Version • HW Revision • Serial Number • Smart Microphone 1 Version • Smart Microphone 2 Version
Network	To show the information about the network settings of the phone. You can see the following information: • IP Address • MAC Address • Bluetooth MAC Address • Hostname • Network Mask • Domain • Gateway • Primary DNS • Secondary DNS
SIP	To show the information about the SIP settings of the phone. You can see the following information: • Primary Account Status • Secondary Account Status • Fallback Account Status
Time and Region	To show the information about the time and region settings of the phone. You can see the following information: • NTP Status • Time • Date • Timezone • Daylight Saving Time

Table continues…

Section name	Description
DES	To show the DES status. The options are: • Enabled. Cannot be changed • Enable • Disabled. Cannot be changed • Disable

Note:

You can not change settings in the Status tab.

Viewing the phone status

About this task

Use this procedure to view the status and settings of Avaya Conference Phone B199 through the web interface.

Procedure

1. Log in to the web interface.
2. Select the **Status** tab.

System logs

Information about log messages is available through the web interface in the System Logs tab. These log types can be useful for troubleshooting.

You can select the following log types:

- All Logs. This is the default setting.
- System Logs
- PhoneApp Logs
- Linux Kernel Logs
- Bluetooth Stack Logs
- PJSIP logs
- Device Management
- SIP traces
- Device Management Debug

You can also specify custom logs type in the **Custom logs type** field.

Note:

You can not access logs through the phone user interface.

Viewing system logs

About this task

Use this procedure to choose and form the log messages through the web interface.

Procedure

1. On the web interface, click **System logs**.
2. Under **Select Logs Type**, select the log from a drop-down list.
3. Click the **Filter** button.

   You can see the logs of the selected type in the field below.
4. **(Optional)** You can do the following:
   - Click the **Download All Logs** button to download all the logs available. In this case the system downloads a .zip archive with the logs available.
   - Click the **Download Selected Logs** button to download the logs of a selected type. In this case, the system downloads a .txt file with the logs of the selected type.
   - Click the **Clear All Logs** button to clear the list of available logs.

Network logs

You can get the traces of the phone network activities through the web interface in the Network Logs tab. The network logs can be useful for troubleshooting.

Note:

You can get network logs only after the phone reboots into the Network logs mode.

Viewing network logs

About this task

Use this procedure to choose and form the network log messages through the web interface.

Procedure

1. On the web interface, click **Network logs**.
2. You can do the following:
   - Click the **Reboot Into Network Log Mode** button to reboot the phone into the network log mode.

- Click the **Download Network Logs** button to download the archive with the available network logs.

Licenses

Some parts of the phone software are subject to open source license agreements. You can get the information about the use and redistribution conditions for the following:

- BSD. This is the Berkeley Software Distribution system for distribution of the source code to the operating system.
- GPL v2.0. This is the General Public License, version 2.0, which guarantees the end users the freedom to run, study, share and modify the software.
- LGPL v2.1. This is the Lesser General Public License, version 2.1, which is applicable to specially designated software packages of the Free Software Foundation and some other authors.
- GFDL v1.2. This is the GNU Free Documentation License, version 1.2, providing the freedom to copy and redistribute specific documentation.
- GFDL v1.3. This is the GNU Free Documentation License, version 1.3.
- ISC. This is the Internet Systems Consortium permissive free software license.
- MIT. This is the Massachusetts Institute of Technology permissive free software license.
- OpenSSL. This is the license to use OpenSSL being a software library for applications that secure network communications and help to identify the party at the other end.
- PHP v3.0. This is the license under which the PHP scripting language is released.
- Bzip2. This is the license to a free and open-source file compression software that compresses single files.
- Socat. This is the license to a relay for bidirectional data transfer between two independent data channels.
- Libpng. This is the license which defines the terms under which the libpng software library can be distributed.
- Qt-Company-Commercial. This is the license for development of proprietary software when the source code is not to be shared with third parties or there are other inconsistencies with the terms of the LGPL license.
- TI-TSPA. This is the Texas Instruments Incorporated license to publicly available technology and software.
- Zlib. This is the license which defines the terms under which the zlib software library can be distributed.
- MPL v2.0. This is the simple copyleft Mozilla Public License (MPL) version 2.0.

Note:

You can get the license information only through the web interface.

Viewing licenses

About this task

Use this procedure to view the status and settings of Avaya Conference Phone B199 through the web interface.

Procedure

1. Log in to the web interface.
2. Select the **Licenses** tab.
3. Select the license that you want to view from the list of licenses available.

Chapter 8: Related resources

Documentation

The following table lists related documents, which you can see at http://support.avaya.com:

Title	Use this document to:	Audience
Deploying		
Administering Avaya Aura® System Manager	Get an understanding of Avaya Aura® System Manager.	Implementation personnel and administrators
Administering Avaya Aura® Communication Manager	Get an understanding of Avaya Aura® Communication Manager.	Implementation personnel and administrators
Administering Avaya Aura® Session Manager	Get an understanding of Avaya Aura® Session Manager.	Implementation personnel and administrators
Avaya IP Office™ Platform SIP Telephone Installation Notes	Get an understanding of IP Office system installation.	Implementation personnel and administrators
Deploying Avaya IP Office™ Platform IP500/IP500 V2	Get an understanding of Avaya IP Office 500.	Implementation personnel and administrators
Installing and Administering Avaya Conference Phone B199	Install, configure, and maintain Avaya Conference Phone B199.	Implementation personnel and administrators
Using		
Using Avaya Conference Phone B199	Set up and use Avaya Conference Phone B199.	End users
Quick Reference		
Avaya Conference Phone B199 Quick Reference Guide	Reference Avaya Conference Phone B199 features quickly.	End users

Finding documents on the Avaya Support website

Procedure

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

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

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

Support

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

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

  Note:

  Videos are not available for all products.

Index

Numerics

A

B

C

D

E

F

G

I

L

M

N

O

P

R

S

T

V

W