Installing and Administering Avaya Conference Phone B199

Release 1.0.8
Issue 1
September 2022

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

Hosted Service

THE FOLLOWING APPLIES 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 1.0.8	September 2022	• Updated Icons on page 19 with the Lecture mode and **Keyboard layout switch** icons. • Updated Device Enrollment Services enrollment code on page 26 with information about enrolling the devices at DES without NEC. • Updated Configuration parameters on page 39 with new parameters. • Added new section SNI support on page 96. • Added Messaging the proxy without adding a record route on page 103. • Updated Volume control and synchronization on page 112 with the information about volume level indication. • Updated Configuration retention after downgrade on page 120 with information about retention of the DHCP option after downgrade. • Added Certificates management on page 132. • Added Support of the PKCS12 file on page 132. • Updated Expansion coverage arrangement on page 149 with information about the most common arrangement types. • Added new section Headset lecture mode on page 153.

Table continues…

Issue	Date	Summary of changes
Release 1.0.7.1	April 2022	• Updated Configuration parameters on page 39 with information about new supported languages. • Added DNS mapping on page 100.
Release 1.0.7	March 2022	• Updated Phone overview on page 14 with information about the connection to other devices. • Updated Icons on page 19 with the **Volume Off** icon. • Added Deployment options on page 14. • Added Supported communication environments on page 16. • Added Out-of-box experience on page 23. • Updated Device Enrollment Services on page 25 with information about using Device Enrollment Services server as a provisioning server. • Added DHCP configuration options on page 28. • Updated Configuration parameters on page 39 with new parameters. • Added new section Configuration of the media port range on page 91. • Added Configuring the Use Static Source Port setting on page 95. • Added Hostname to IP address mapping on page 96. • Updated Bluetooth® Classic profiles on page 107 with information about the LEDs behavior during A2DP streaming. • Added Automatic reconnection to a Bluetooth device on page 109. • Added new section Volume control and synchronization on page 112. • Added new section USB ports configuration on page 113. • Added Configuration retention after downgrade on page 120. • Added Provisioning of the CA certificate through SCEP on page 139. • Added Disabling web access on page 140.
Release 1.0.6	September 2021	• Updated Icons on page 19 with the **Warning** icon. • Added new section Rebooting the phone on page 85. • Added Input validation and data type restrictions on page 84. • Added new section SIP account registration status on page 94. • Updated Standard encryption for media encryption with SRTP on page 135 with the information about support of several cryptos. • Updated Configuration parameters on page 39 with new parameters. • Added new section SCEP support on page 137.

Table continues…

Issue	Date	Summary of changes
Release 1.0.5	June 2021	• Updated Icons on page 19 with the **Clear call history** button. • Updated Standard encryption algorithms on page 134 with the information about FIPS mode. • Updated Legacy encryption mode on page 136 with the information about firmware upgrade. • Added new section FIPS mode on page 136. • Added new section USB only user mode on page 110. • Updated Expansion of the phone coverage on page 148 with the information about disabling the unused daisy chain ports during active calls. • Updated Bluetooth® connection on page 106 with the information about USB only user mode. • Added new section Firmware upgrade and downgrade using a USB mass storage device on page 118. • Updated Configuration parameters on page 39 with new parameters. • Added new section Protection against cross-site request forgery on page 141. • Added Appendix A on page 173 with the information about the list of encryption methods enabled and disabled in Legacy encryption mode.
Release 1.0.4	February 2021	• Added Provision of the NTP server address on page 87. • Updated Voice quality monitoring on page 88 with the quality estimate metrics and analog parameters. • Added Standard encryption algorithms on page 134. • Updated Avaya Conference Assistant on page 143 in line with the change in MD5 usage. • Added Expansion microphone firmware upgrade on page 154. • Updated Bluetooth® connection on page 106 with information on switching between the Bluetooth modes. • Updated Configuration parameters on page 39 with new parameters.
Release 1.0.3	October 2020	• Added Bluetooth® radio on page 109. • Updated Firmware upgrade using check-sync on page 104 with the reboot parameter values. • Updated Configuration parameters on page 39 with new parameters. • Added Firmware downgrade with DES provisioning on page 120. • Updated Certificates on page 126 with the information about the paths to the certificates, MD5 checksum, and certificate configuration file structure.

Table continues…

Issue	Date	Summary of changes
Release 1.0.2	August 2020	• Added Sleep mode on page 88. • Added Voice quality monitoring on page 88. • Added Bluetooth® connection on page 106. • Updated Configuration parameters on page 39 with new parameters.
Release 1.0.1	March 2020	• Added Firmware upgrade and downgrade on page 114. • Added a note in Firmware upgrade using check-sync on page 104. • Added Validation and migration of configuration on page 116. • Updated Device Management on page 121 with information on the phone provisioning with Device Enrollment Services. • Added Upgrading multiple devices on page 122. • Added Remote syslog server on page 160. • Added a note in Factory reset on page 161 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 great audio quality. It improves user experience and ensures an easier connection to audio conference bridges.

The conference phone features include a simple-to-use 4.3 inch graphical LCD with a backlight, volume control, and mute buttons. Two more mute key buttons are located along the perimeter of the device. There are 3 microphones in the base of B199, which support 10 users in a 30 square meters room. You can attach additional expansion microphones to increase the conference phone coverage to 70 square meters or daisy chain three B199 devices to cover up to 90 square meters.

Avaya Conference Phone B199 can act as an Audio Media Device connected to a personal computer or a laptop via USB and activated through soft client software. The conference phone can also use Bluetooth to connect to a mobile device, a personal computer, or a laptop as it supports Hands-Free and A2DP Bluetooth profiles.

Avaya Conference Phone B199 uses 10/100 Mbit Ethernet and supports PoE Class 1 and Class 2 power.

Deployment options

Avaya Conference Phone B199 provides several deployment options to match the scope and complexity of your operating environment.

USB or Bluetooth media device

You can use your B199 Conference Phone as a USB or Bluetooth media device with a personal computer, a laptop, a video conference system, and many other devices. The phone has a USB connector and ensures Bluetooth connection.

Important:

B199 Conference Phone receives power through the Ethernet power injector (there is no power supply via USB supported).

SIP Endpoint

B199 Conference Phone can function as a SIP device. For this deployment option, you must have the IP network engineered to support the excellent voice quality transmission. You must configure IPv4 via DHCP or manual configuration and specify its IP address, network mask, and gateway.

B199 Conference Phone functions as a SIP device when your communication system has SIP accounts provisioned with the following minimum parameters available:

- SIP registrar address (IP address or a fully qualified domain name (FQDN))
- SIP registrar protocol (UDP, TCP, or TLS) and SIP registrar port
- SIP account name
- SIP account password

To enable additional features, including more complex security options, you may require to have other parameters configured.

Individual device management

If you deploy a small number of devices and do not plan to establish a centralized management HTTP server, you can access the configuration of B199 Conference Phone through the web interface or using the phone user interface.

Tip:

Configure the parameters through the web interface as it allows convenient logging, easy data input and enhanced status information.

Centralized device management

If you deploy multiple B199 Conference Phone devices, to simplify their configuration, use a centralized server that provides software, generic and MAC-specific configuration and certificate files. You must specify the IP address or FQDN of the HTTP/HTTPS file server manually or through DHCP.

When the phone checks the file server, it compares its running firmware and the one available on the file server and performs an upgrade or downgrade if the versions are different. You can automate the configuration update process. B199 Conference Phone can poll the file server at a defined interval for changes and apply the changes when in Idle mode.

Avaya Device Enrollment Services

B199 Conference Phone 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 manage firmware updates.

The use of DES can greatly simplify the deployment of B199 Conference Phone. When you power up the device on the network for the first time, you can manually configure it for automatic provisioning and enter your customer-specific DES enrollment code or pre-define the MAC address of your phone on the DES server. B199 Conference Phone receives the required configuration files and firmware upgrades.

Note:

If you deploy your B199 Conference Phone in Avaya Cloud Office™, it performs the initial configuration of the device with Device Enrollment Services.

For more information about handling the device with DES, see *Using Avaya Device Enrollment Services to Manage Endpoints*.

Related links

Device Enrollment Services on page 25
DHCP configuration options on page 28
Bluetooth® connection on page 106
USB only user mode on page 110

Supported communication environments

Avaya Conference Phone B199 works as a SIP endpoint in the following environments:

System	Minimum B199 release
Avaya Aura®	B199 version 1.0.1
IP Office	B199 version 1.0.1
Avaya Cloud Office™	B199 version 1.0.1
Avaya Private Cloud	B199 version 1.0.1
Zang Office	B199 version 1.0.1
Broadsoft	B199 version 1.0.1
Generic SIP-19	B199 version 1.0.1

Avaya Conference Phone B199 works as a media device through USB and Bluetooth® in the following environments:

System	Minimum B199 release
Avaya Spaces	B199 version 1.0.1
Microsoft Teams	B199 version 1.0.5
Zoom	B199 version 1.0.7
Webex	B199 version 1.0.1

Physical layout

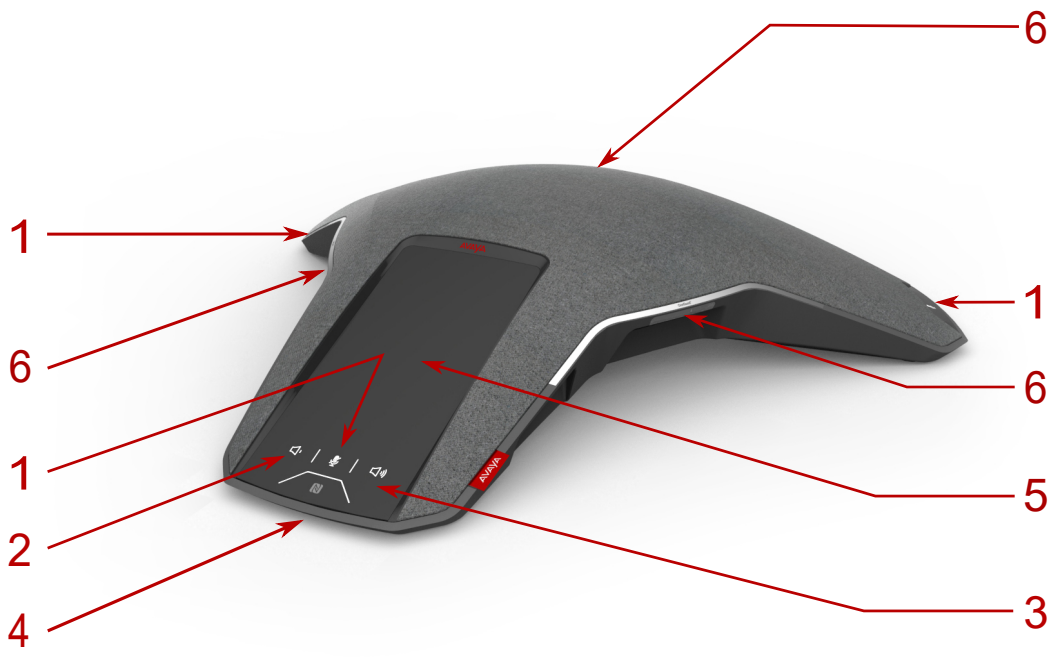


Figure 1: Front view of Avaya Conference Phone B199

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 B199 Conference Phone 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

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.
	Warning	To notify that the SIP account registration failed. When you tap the Warning icon, the phone shows the following pop-up message: `No sip service registered (Wrong username/password or registrar?).`
	Microphone Muted	To mute and unmute the phone.
	Volume Up	To increase the phone volume level.
	Volume Down	To decrease the phone volume level.
	Volume Off	To provide a phone screen indication that the volume on the phone is off when you change the volume to the lowest level on the connected USB host.
	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.
	Clear call history	To clear all the call history in the call list.

Table continues…

Icon	Name	Description
	Lecture mode	To indicate that the user connected a headset. Here, the audio signal from the built-in speakers and microphones of the phone mixes with the audio signal from the headset.
	Keyboard layout switch	To switch between the Cyrillic and Latin keyboard layouts on the phone screen. **Note:** The keyboard does not save the switched state. When you reopen the keyboard, the layout corresponds to the selected phone language.

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

Chapter 3: Initial setup and configuration

Out-of-box experience

When you power Avaya Conference Phone B199 and connect it to a routable Ethernet connection for the first time, the phone conducts the following actions:

- Internal self-tests: Avaya Conference Phone B199 confirms the hardware status and firmware sanity.
- DHCP Discovery: the phone attempts to obtain the basic IP parameters and the HTTP server, TLS server, HTTP Directory, VLAN ID, and DES parameters, which can be in the enabled or disabled state.
- LLDP Negotiation: the phone communicates the default LLDP parameters and parses any LLDP parameters provided by the L2/L3 network device to which Avaya Conference Phone B199 connects via Ethernet.

If Avaya Conference Phone B199 receives a VLAN ID via DHCP or LLDP, the phone releases the received IP address and performs DHCP Discovery with all packets tagged with the VLAN ID. Avaya Conference Phone B199 only accepts ingress packets tagged with the VLAN ID.

After the phone obtains the IP address and a routable path or VLAN, it tries to reach the Network Time Protocol server to set the correct time. This attempt may require the device to query the DNS for the following default server address: `0.pool.ntp.org`.

When Avaya Conference Phone B199 has the provisioning or Device Management server IP address or Fully Qualified Domain Name (FQDN) provided via DHCP, it attempts to establish a connection and request the following files from the server:

- Generic global certificate file `avayab199_certcfg.xml`.
- Device-specific certificate file `avayab199_certcfg-<MAC>.xml`.

  If a certificate file is obtained, the phone uses the paths from certcfg.xml to download the list of files specified therein.
- Generic configuration file `avayab199.xml`. If the device fails to find it with .xml file ending, it searches the configuration file with the following file endings: .cgi, .php, .asp, .enc, .js, or .jsp.
- Device-specific configuration file `avayab199-<MAC>.xml`. If the device fails to find it with .xml file ending, it searches the configuration file with the following file endings: .cgi, .php, .asp, .enc, .js, or .jsp.

  Avaya Conference Phone B199 compares these configuration files with the maximum version of the configuration file acceptable on the device. If the file from the HTTP server has a lower or equal value, the device reads, parses, and prepares to apply it. If this file has a higher value, the phone ignores it as it may contain unknown or changed parameter formats.

For example, `<B199 version="7">` on the top of the 1.0.7 firmware compliant .xml file for the device with 1.0.6 firmware installed indicates that the file received has a higher value than the file available on the device. Avaya Conference Phone B199 rejects such a file.

The phone stores the configuration in its non-volatile memory.

- Generic firmware version file `avayab199_fw_version.xml`. The device also compares this file with the current running firmware. If there is a difference, Avaya Conference Phone B199 requests the firmware identified in the `avayab199_fw_version.xml` file from the HTTP server.

After upgrade or downgrade, the phone reboots and repeats all the described actions. If there are no changes in the content of the various .xml files, the device ignores them and applies the configuration stored in its non-volatile memory.

If the DES parameter from DHCP is not `0` or the configuration file does not set the DES parameter to `0`, the phone asks you the following question: "`Perform auto provisioning?`". If you agree, Avaya Conference Phone B199 contacts the Avaya Device Enrollment Services server, provides its MAC address, and determines if a user or a service provider claims it. If the device belongs to a user or a service provider and DES has the required information, the conference phone receives the configuration and firmware files. Otherwise, Avaya Conference Phone B199 prompts for an enrollment code. The phone receives it from the business partner or DES administrator. After entering the enrollment code, DES considers the phone as claimed and provides the required configuration and firmware files.

Note:

If the device does not obtain an IP address and the configuration file does not specify an administrator password, Avaya Conference Phone B199 prompts you to set the administrator password. You need this password to access the phone admin menu and the web-based admin menu using an Internet browser.

Related links

Firmware upgrade and downgrade on page 114
Supported communication environments on page 16
Configuration parameters on page 39

Configuration of Avaya Conference Phone B199

Avaya Conference Phone B199 can use the following methods to obtain the required configuration parameters:

- Device Enrollment Services (DES).
- Centralized HTTP/HTTPS server.
- B199 Conference Phone web interface when you log in as the administrator.
- B199 phone interface.

Related links

Device Enrollment Services on page 25

Setting the password for Avaya Conference Phone B199

About this task

Use this procedure to set your B199 Conference Phone password when you first activate the phone or after a reset to the factory settings. By default, the administrator password is not set.

You must enter the correct administrator password to change the phone configuration. For that, always remember your password. If you forget the password, you can perform manual device recovery.

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.

   Here, B199 Conference Phone functions in the administration mode, and you can configure phone settings. However, you cannot 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 indicates if the password has an acceptable length.

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

   The phone reboots.

Related links

Factory reset on page 161
System recovery on page 159

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 Device Enrollment Services, you do not need to configure the provisioning server manually. You can use Device Enrollment Services to provide configuration parameters to B199 Conference Phone and 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 Device Enrollment Services for the MAC address of your B199 Conference Phone. To start the device setup, the manufacturer enters the device details, such as certificate information, MAC address, and serial numbers. The details are imported to the Device Enrollment Services server through a file, enabling the device to authenticate with Device Enrollment Services. The service provider or administrator can log in to Device Enrollment Services to configure customer information and provisioning settings.

You can configure B199 Conference Phone to use the Device Enrollment Services server as a provisioning server. Here, the phone uses Factory certificate to establish a successful connection to the server and download the configuration file.

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 Device Enrollment Services server prompts you to enter NEC on the phone at the beginning of provisioning with Device Enrollment Services. After entering the enrollment code, the phone contacts Device Enrollment Services 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. Here you must specify the configuration server manually.

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

If you do not have an enrollment code, then you need to associate your B199 phone with a profile in the Device Enrollment Services server. If your profile is already associated in the DES, your B199 phone contacts the DES server, and gets the provisioning server address. If your profile is not associated in the DES, then B199 requests the user to provide the enrollment code manually. B199 requires the enrollment code while booting up, to get associated with a profile.

Provisioning Avaya Conference Phone B199 using Device Enrollment Services

About this task

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

The DHCP server on the network provides an IP address, Gateway, and DNS parameters to your B199 Conference Phone.

Before you begin

Ensure that Device Enrollment Services 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 Device Enrollment Services 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 Device Enrollment Services.

  B199 Conference Phone contacts the Device Enrollment Services server. The Device Enrollment Services 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 Device Enrollment Services automatic provisioning during this boot session.

  Here 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 Device Enrollment Services functionality.

Starting automatic provisioning

About this task

You can start automatic provisioning with the Device Enrollment Services (DES) server manually from 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. Here the phone continues showing the Device Enrollment Services prompt at boot until you choose to perform automatic provisioning and tap **Yes** in the prompt.

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 `1`.

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

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

DHCP configuration options

You can configure Avaya Conference Phone B199 to automatically obtain critical configuration parameters from a DHCP server. You can use a DHCP Site Specific Option Number (SSON) to provide specific information for the B199 Conference Phone configuration. The following values are available: 43, 56, 60, 61, 66, 67, and 242. By default, the SSON value is 242. By default, the device scans all the SSON numbers to detect the availability of the parameters below.

B199 Conference Phone uses values of the following parameters from the DHCP option specified by SSON:

- HTTPSRVR
- TLSSRVR
- HTTPDIR
- L2QVLAN

- DES_STAT

B199 Conference Phone ignores other parameters included in the option, such as other Avaya™ products use.

DHCP Site Specific Option Number parameters

The following table describes the parameters that DHCP SSON contains:

Parameter	Description
HTTPSRVR	The IP Address or FQDN of an HTTP file server, which the device uses to obtain configuration, firmware, or certificates.
TLSSRVR	The IP Address or FQDN of an Avaya™ file server, which the device uses to obtain configuration, firmware, or certificates using the Transport Layer Security (TLS) protocol as the security protocol.
HTTPDIR	The path name to prepend to all file names that the device uses in HTTP and HTTPS GET operations during its start-up. The path is relative to the root of the TLS or HTTP file server. The path length is from 0 to 127 ASCII characters without spaces.
L2QVLAN	The VLAN ID of the voice Virtual Local Area Network (VLAN). The default value is `0` which means “untagged”.
DES_STAT	The specification of the DES enablement setting. The following values are available: 0, 1, or 2. A DES_STAT value provided by DHCP takes priority over a parameter provided in the .xml configuration file. DES_STAT must be set to `0` if you use the HTTPSRVR or TLSSRVR parameters.

The following is an example of the syntax of the DHCP SSON Option as provided within a DHCP Offer: `L2QVLAN=114,HTTPSRVR=111.222.232.234,HTTPDIR=B199, DES_STAT=0.`

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 **Arrow Left** 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.

Avaya Conference Phone B199 .xml configuration files

Avaya Conference Phone B199 uses .xml files through the centralized management server during provisioning. Sample .xml configuration files are available at http://support.avaya.com.

The following table lists the available .xml configuration files:

.xml file	Description
avayab199_certcfg.xml	This is the first file that B199 Conference Phone requests. The phone obtains 802.1X, SIP, provisioning server, and LDAP certificates from this file.
avayab199_certcfg-<MAC>.xml	This is the second file that B199 Conference Phone requests. Here, <MAC> is the MAC address of the specific phone. Ensure that the input MAC address contains only letters and numbers and no colons. This file replaces the default 802.1X, SIP, provisioning server, and LDAP certificates with device-specific certificates.
avayab199.xml	A global configuration file that contains the basic configuration.
avayab199-<MAC>.xml	A configuration file where <MAC> is the MAC address of the specific phone. Ensure that the input MAC address contains only letters and numbers and no colons. Parameters available in this device-specific file override the default configuration file settings.
avayab199_fw_version.xml	A file that contains details about the firmware version of the phone. This file comes with each Avaya Conference Phone B199 firmware build download. **Important:** Do not modify this file.

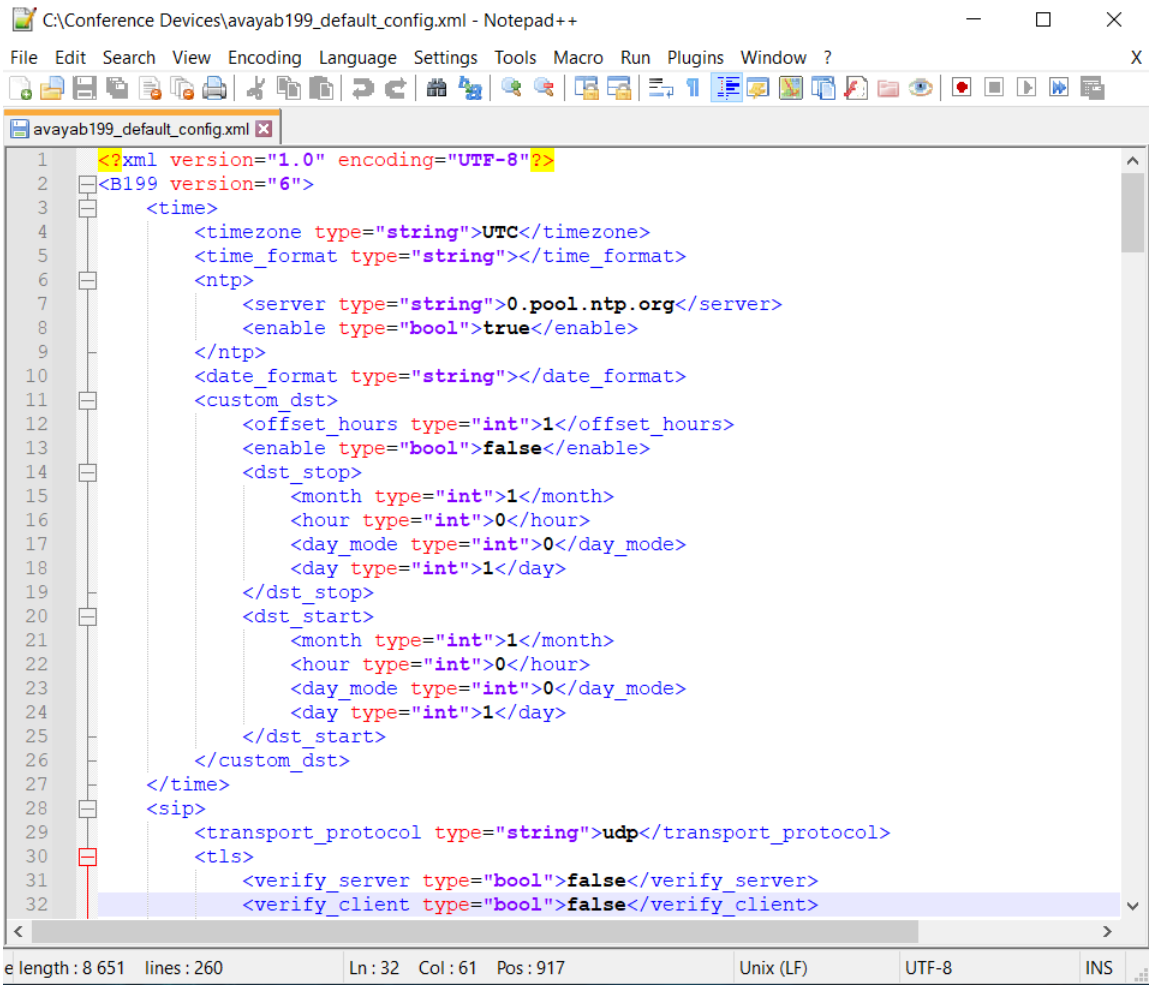
Related links

Device Management on page 121
Configuration parameters on page 39

Modification of an .xml configuration file

You can open and edit a .xml configuration file using an application to import and export XML files. You can also choose the editor that can read .xsd files to verify the syntax and content of the modified .xml file. You can use such software as Notepad++, Coda, TextWrangler, or any other that you find suitable.

The following screenshot is an example of a .xml configuration file in the Notepad++ editor:



When you open a default B199 Conference Phone configuration file, the second line, `<B199 version=”6”>`, indicates the firmware version. This number automatically increases when the B199 Conference Phone firmware version is upgraded.

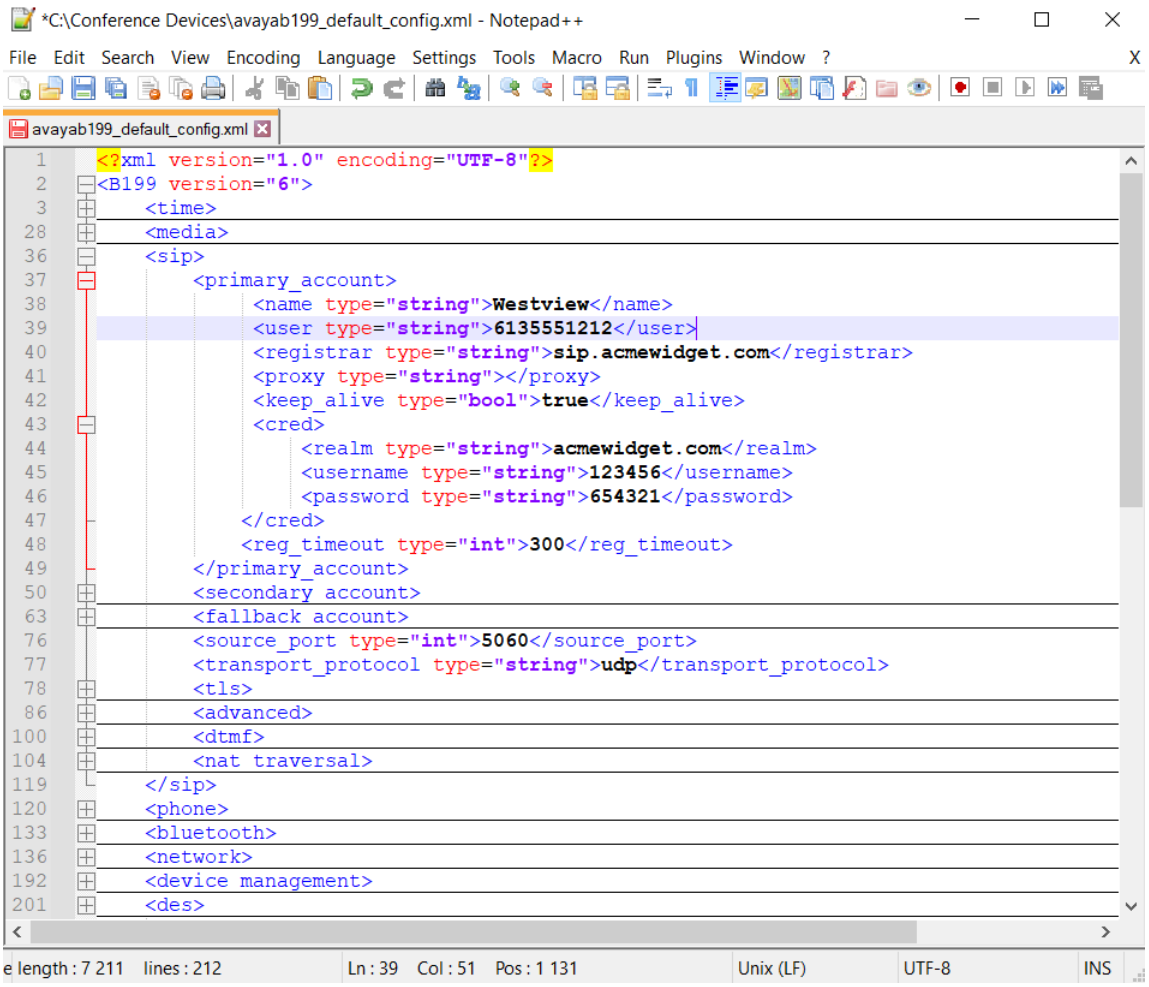
Important:

Do not modify the version number.

In the configuration file, the *”-”* icons indicate the beginning of a branch. When you click this icon, the branch collapses. Clicking the *”-”* icon does not delete the branch. To expand the branch back to the original view, click the *”+”* icon.

The name of the example configuration file is `avayab199_default_config.xml`. To deploy this configuration file through a centralized management server, change the file name to `avayab199.xml` or `avayab199-<MAC>.xml`. If you upload the file through the web interface, you can use any file name.

You can modify the .xml file to configure the parameters of your B199 Conference Phone. Here, add specific data to the file section. In the example you can see the expanded SIP Primary account section with the parameters set:



Here, the specified parameters are the following:

System: Avaya Aura® in “ACME Widgets” enterprise on the 3rd floor in the "Westview" room
SIP Domain: acmewidget.com
SIP Registrar: `sip.acmewidget.com` using UDP on port `5060`
Outbound Proxy: no outbound proxy
SIP User: `6135551212@acmewidget.com`
SIP User Authentication Name: 123456
SIP User Password: 654321
Keep Alive: 300 second timer enabled

Validation of a configuration file

The release-specific firmware contains a .xsd file for the configuration file review for errors in the parameters set. B199 Conference Phone performs a .xsd file validation when a configuration file is uploaded through the web interface or a management server. If the validation fails, the device rejects the complete configuration file.

You can also use the editor to validate the configuration file. For example, in Notepad++, install the XMLTools plugin in the Plugin Manager and validate the .xsd file.

Administration through the web interface

You can access the Avaya Conference Phone B199 administration pages by using the HTTPS web interface from your laptop, PC, or tablet.

Note:

Use the Google Chrome browser to optimize the B199 web pages.

The prerequisite steps for logging in to the web administration pages are the following:

1. You must obtain the IP address of B199 by using the phone's touch screen. You can use a dynamic or a static IP address to connect to the network.
2. You must configure the administrator password by using the .xml configuration file or the phone's touch screen. By default, there is no password for web administration set.

Important:

Ensure that B199 is in Idle mode, that is it shows the normal idle screen, before attempting to log in to the web administration server. It is not possible to be in the configuration menu on the phone and through the web interface at the same time.

The web administration portal contains the following pages:

- Status
- Phone
- Network
- Media
- LDAP
- SIP
- Provisioning
- System Logs
- Network Logs
- Licenses
- Logout

You can open the required page by clicking the corresponding tab in the Navigation pane on the top.

The web administration server launches on the **Status** page. If you log in to the web interface when the conference phone is still booting and establishing connectivity, this page may require updating. You can update it by pressing `F5` on your keyboard.

When you make a configuration change on a page, click **Save** in the bottom right to save the configuration to the non-volatile memory. To apply the change, B199 may restart a specific software layer or reboot. If the device reboots, you must wait until the procedure completion, press `F5` to refresh the web page, and log in again.

Configuration import and export

When you finalize the conference phone configuration, B199 reliable operates in the required environment, you can save a copy of this configuration on the **Provisioning** tab. Here, the device exports a copy of the non-volatile configuration capturing the non-default parameters and forms an .xml configuration file. Whenever you decide to restore the configuration parameters, import this file, and save the configuration. Then the device reads and attempts to parse the configuration file. If there is an error in the configuration file, or the web application cannot parse the file, B199 shows a corresponding error message.

Note:

The device does not export passwords in the configuration file.

Related links

Firmware upgrade and downgrade on page 114
Configuration parameters on page 39

Viewing the IP address

About this task

Use this procedure to view the IP address of your Avaya Conference Phone B199.

Procedure

1. On the phone screen, tap **Settings** > **Admin Login**.
2. Enter the administrator password.
3. Tap **Status** or the **Arrow Right** 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
   - SIP Registration
4. Tap the **Arrow Left** 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.

After five incorrect login attempts, the web interface becomes blocked for 15 minutes. The web interface shows the following message: `Login has been suspended for 15 minutes due to too many invalid password entries.` If you enter the invalid password less than five times, then you have another five attempts after five minutes break.

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 the password in the **Password** field.

   The password is the administrator password for your phone.

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

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.

Procedure

1. Log in to the web interface.
2. On the Navigation pane, click the required tab.
3. Choose the parameter that you want to configure and proceed to the options available.
4. Click **Save**.

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.

Administration by using the phone's touch screen

Avaya Conference Phone B199 allows for configuration by using its touch screen once the user logs in with the administration password. When you modify a parameter, the device verifies its syntax and then automatically saves it to the non-volatile memory. After you exit the menu levels to the idle screen, the conference phone restarts or reboots as required to apply the configuration.

The Settings menu that you can access from your B199 is as follows:

Settings

Status

Phone
Name, Language, Security, Admin Password, Ring Level, Key Tone, Call Log, , Daisy Chain, Startup Sound, Factory Reset, Reboot,
Media
SRTP, SRTCP, Codec, Capability Negotiation, Voice Quality Monitor
Advanced
First Media Port, Last Media Port
SIP
Primary Account, Secondary Account, Fallback Account, Port, Transport Protocol, TLS, SNI, DTMF, NAT Traversal
Advanced
Disable 'rport', Session Timers, Session Expiration, Outbound Proxy, Allow Contact Rewrite, Allow Via Rewrite, Enable SIP Replaces, Use Static Source Port
Network
DHCP, Hostname, Domain, Static IP, DNS1, DNS2, VLAN, VLAN ID
802.1x
802.1x Enable/Disable, Auth Name, EAP MD5, EAP MD5 Password, EAP TLS Enable/ Disable, Private Key Password
Time
Enable NTP, NTP Server
Device Management
Enable, Provisioning Server, Check Server Certification, Lowest TLS Version, DHCP Option, DES Provisioning, Web Access
Conference Assistant
Disconnect Device, Remove Bonding Information
Bluetooth
Pair Device, Disconnect Device, Remove Pairing

You must enter the admin password to configure most of the device's settings.

Related links

Configuration parameters on page 39
Phone settings on page 85
Media settings on page 88
SIP settings on page 93
Network settings on page 97
Bluetooth® connection on page 106
Avaya Conference Assistant on page 143

Logging in to Avaya Conference Phone B199

About this task

Use this procedure to log in as the administrator by using the touch screen of your B199.

Procedure

1. On the touch screen, type **Settings** > **Admin Login**.

2. Enter the administration password.

Configuring the settings on the phone

About this task

Use this procedure to configure the 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 the required Settings group.
2. Choose the parameter that you want to configure and proceed to the options available.
3. Tap the **Arrow Left** icon twice to return to the home screen.

   The phone reboots to apply the changes.

Chapter 4: Settings configuration and management

Configuration parameters

The following table contains all configurable parameters in the order of the default configuration file. You can see the XML variable name definition for each parameter in the left column. The right column shows a brief description of the parameter and provides the title in the web administration and the B199 User Interface (the touch screen administration menus).

XML parameter name	Description
<B199 version="x">	Here x is the version number of the .xml parameters list. **Important:** Do not modify.
<time>	The top line of the time management section.
<time_format>	To specify the time format for the phone as follows: • **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. **Terminology reference:** **Web interface**: Time Format **Phone UI**: Not configurable

Table continues…

XML parameter name	Description
`<timezone>`	To specify the Region/City location in line with the definitions from the common Timezone databases. For more information, see https://en.wikipedia.org/wiki/List_of_tz_database_time_zones. 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. **Terminology reference:** **Web interface**: Timezone **Phone UI**: Not configurable
`<ntp>`	The top line of the NTP configuration section.
`<server>`	To specify the IP address or FQDN of an NTP server. If DHCP Option 42 provides the NTP server value, B199 uses the DHCP provided value. If DHCP Option 42 is not available, the phone applies this XML parameter. **Terminology reference:** **Web interface**: NTP Server **Phone UI**: NTP Server
`<enable>`	To specify whether NTP is enabled. The options are the following: • True. This is the default setting. • False. **Terminology reference:** **Web interface**: NTP Enable **Phone UI**: Enable NTP

Table continues…

XML parameter name	Description
<date_format>	To specify the date format which consists of the day, month and year. Here, dd indicates the day of the month, D is a shortened version of the day of week, DD is the full version of the day of the week, M is a shortened version of the month, MM is the full version of the month, yy is the last 2 digits of the calendar year, yyyy is the full calendar year. **Important:** You can configure this parameter only through the web interface. The following date format options 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, *10/01/2020*. • mm/dd/yy - Month/date/short numerical designation of the year. For example, *01/10/20*. • 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*. • The default value. Here, your B199 Conference Phone applies the date format that is standard for the selected language. For example, if you choose Finnish, the date format is dd.mm.yyyy.
<custom_dst>	The top line of the DST section.

Table continues…

XML parameter name	Description
<enable>	To specify whether the **Daylight Saving Time (DST)** configuration is enabled. The options are the following: • True. • False. This is the default setting. The phone ignores the **Custom DST** parameter if you configure the **Timezone** parameter, and the NTP server provides it. Thus, you must disable **Geo Timezone (auto DST)** to enable **Custom DST**. **Terminology reference:** **Web interface**: Custom DST **Phone UI**: Not configurable
<offset_hours>	To specify the DST hours offset. The options are the following: • 1. This is the default setting. • 2. **Terminology reference:** **Web interface**: Offset Hours **Phone UI**: Not configurable
<dst_start>	The top line of DST start date and time section. To indicate when the DST parameters become applicable.
<month>	To specify the month to apply the DST parameters. Month number as an integer with the values of 1 to 12. **Terminology reference:** **Web interface**: Start Month **Phone UI**: Not configurable
<day>	To specify the day to apply the DST parameters. Day number as an integer with the values of 1 to 31. **Terminology reference:** **Web interface**: Start Day **Phone UI**: Not configurable
<day_mode>	To specify the advance or delay to apply the DST parameters. The value range is from -5 to 5. **Terminology reference:** **Web interface**: Start Day Mode **Phone UI**: Not configurable

Table continues…

XML parameter name	Description
<hour>	To specify the hour to apply the DST parameters. The hour format is a 24-hour format with values from 0 to 23. **Terminology reference:** **Web interface**: Start Hour **Phone UI**: Not configurable
<dst_stop>	The top line of DST stop date and time section. To indicate when the DST parameters become inapplicable.
<month>	To specify the month to end the DST parameters application. Month number as an integer with the values of 1 to 12. **Terminology reference:** **Web interface**: Stop Month **Phone UI**: Not configurable
<day>	To specify the day to end the DST parameters application. Day number as an integer with the values of 1 to 31. **Terminology reference:** **Web interface**: Stop Day **Phone UI**: Not configurable
<day_mode>	To specify the advance or delay to end the DST parameters application. The value range is from -5 to 5. **Terminology reference:** **Web interface**: Stop Day Mode **Phone UI**: Not configurable
<hour>	To specify the hour to end the DST parameters application. The hour format is a 24-hour format with values from 0 to 23. **Terminology reference:** **Web interface**: Stop Hour **Phone UI**: Not configurable
<media>	The top line of the media and codec section.
<security>	The top line of the media security section.

Table continues…

XML parameter name	Description
<srtp>	To enable or disable the ability to negotiate Secure Real-time Transport Protocol (SRTP) parameters to provide encryption, message authentication, and integrity for the audio and video streams. The options are the following: • **Disabled**. This is the default option. • **Optional**. • **Mandatory**. **Terminology reference:** **Web interface**: SRTP **Phone UI**: SRTP
<srtcp>	To enable the ability to generate secure RTCP reports. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: SRTCP **Phone UI**: SRTCP
<capneg>	To determines if during the SIP offer and answer procedure the SDP protocols and attributes can be negotiated. • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Capability Negotiation (RFC5939) **Phone UI**: Capability Negotiation
<codec>	The top line of the codec selection and priority section. Here, 6 stands for the highest priority, 1 - for the lowest, and 0 - for the disabled (not offered during negotiation). **Important:** You must enable at least 1 codec.
<iLBC>	The top line of the iLBC codec section.
<prio>	To specify the iLBC priority. Here, 6 stands for the highest priority, 1 - for the lowest, and 0 - for the disabled (not offered during negotiation). **Terminology reference:** **Web interface**: ILBC **Phone UI**: ILBC Priority

Table continues…

XML parameter name	Description
<mode>	To specify the iLBC coded frame length in milliseconds. The options are the following: • 20 for 15.2 kbps. This is the default setting. • 30 for 13.33 kbps. **Terminology reference:** **Web interface**: ILBC Mode **Phone UI**: Not configurable
<OPUS>	The top line of the OPUS codec section. OPUS offers excellent bandwidth versus audio quality performance. It supports bandwidths up to wide-band fidelity. Avaya™ recommends using it whenever possible.
<prio>	To specify the OPUS priority. Here, 6 stands for the highest priority, 1 - for the lowest, and 0 - for the disabled (not offered during negotiation). **Terminology reference:** **Web interface**: OPUS **Phone UI**: OPUS Priority
<PCMU>	The top of the PCMU section. PCMU is a narrow-band codec operating at 64kbps with 20ms payload. The other name of this codec is G.711 ulaw.
<prio>	To specify the PCMU priority. Here, 6 stands for the highest priority, 1 - for the lowest, and 0 - for the disabled (not offered during negotiation). **Terminology reference:** **Web interface**: PCMU **Phone UI**: PCMU Priority
<PCMA>	The top of the PCMA section. PCMA is a narrow-band codec operating at 64kbps with 20ms payload. The other name of this codec is G.711 alaw.
<prio>	To specify the PCMA priority. Here, 6 stands for the highest priority, 1 - for the lowest, and 0 - for the disabled (not offered during negotiation). **Terminology reference:** **Web interface**: PCMA **Phone UI**: PCMA Priority
<G722>	The top of the G722 section. G722 is a wide-band codec providing excellent quality.
<prio>	To specify the G722 priority. Here, 6 stands for the highest priority, 1 - for the lowest, and 0 - for the disabled (not offered during negotiation). **Terminology reference:** **Web interface**: G722 **Phone UI**: G722 Priority

Table continues…

XML parameter name	Description
<G729>	The top of the G729 section. G729 is a narrow-band codec providing good audio quality under good network conditions. **Note:** OPUS is a preferred option.
<prio>	To specify the G729 priority. Here, 6 stands for the highest priority, 1 - for the lowest, and 0 - for the disabled (not offered during negotiation). **Terminology reference:** **Web interface**: G729 **Phone UI**: G729 Priority
<voice_quality_monitor>	The top of the Voice Quality Monitor configuration section. Voice Quality Monitor is a physical or Cloud server or a collector that you can use to track call audio quality information.
<enable_rtcp_xr>	To enable the Real-Time Transport Control Protocol with the Extended Reports capability. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Enable RTCP XR **Phone UI**: Enable RTCP XR
<rtcp_xr_collector_uri>	To specify the Uniform Resource Identifier (URI) of the RTCP collector. **Terminology reference:** **Web interface**: RTCP XR Collector URI **Phone UI**: RTCP XR Collector URI
<rtp_pt_98_ilbc>	To set iLBC to use payload type 98. The options are the following: • True. • False. This is the default setting. **Important:** This parameter is only available in the .xml configuration file.
<advanced>	The top line of the advanced media settings section.
<first_media_port>	To specify the First Media Port value. The value range is from 2048 to 65528. The default value is 4000.
<last_media_port>	To specify the Last Media Port value. The value range is from 2055 to 65535. The default value is 65535.
<sip>	The top line of the SIP parameters section.
<primary_account>	The top line of the primary account section. After registration, the primary account is applicable for inbound and outbound calls.

Table continues…

XML parameter name	Description
`<name>`	To specify the name visible on the phone screen on the primary line. This name is not a part of the SIP messaging. **Important:** This is a mandatory setting. **Terminology reference:** **Web interface**: Account Name **Phone UI**: Account Name
`<user>`	To specify the SIP account name as configured on the SIP Registrar. The phone uses the content of this field to construct the user URI. **Important:** Do not use the following characters: # % @. Do not include `@sipdomain` data. This is a mandatory setting. **Terminology reference:** **Web interface**: User **Phone UI**: User
`<registrar>`	To specify the IP address or a fully qualified domain name (FQDN) of the SIP server where you register the account. The format options are the following: `10.10.1.100` and `10.10.1.100:5060` for a local SIP server, or `sip.company.net` for a FQDN. **Important:** This is a mandatory setting. **Terminology reference:** **Web interface**: Registrar **Phone UI**: Registrar Address
`<proxy>`	To specify the proxy server which the company uses for the SIP peer communication. The format options are the following: `10.10.1.100:1234` for a local proxy with an optionally specified port or `proxy.company.net:port` for a FQDN. If you append `;hide` to the end of the proxy string, B199 avoids adding a record route to the SIP messaging. For more information, see Messaging the proxy without adding a record route on page 103. **Terminology reference:** **Web interface**: Proxy **Phone UI**: Proxy

Table continues…

XML parameter name	Description
<keep_alive>	To specify if the phone maintains an active connection to the network. The device can use Keep Alive messages to ensure that the IP path to the Registrar is always available by sending periodic SIP messages. If the network fails and there are no messages received, the phone attempts to switch to the Secondary account for outbound calls, or the Fallback account. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Keep Alive **Phone UI**: Keep Alive
<cred>	The top of the SIP credentials for the primary account section.
<realm>	To specify the network domain which the phone accepts incoming calls from. For example, company.com. The other name is the SIP domain. You can leave this field blank or put an asterisk (*) to accept all incoming call invites from any SIP domain. **Terminology reference:** **Web interface**: Realm **Phone UI**: Realm
<username>	To specify the SIP authentication name. If you leave it blank, the phone uses the content of the <user> parameter to authenticate and register the account. **Terminology reference:** **Web interface**: Authentication Name **Phone UI**: Authentication Name
<password>	To specify the SIP password for authentication with the Registrar. **Important:** This is a mandatory setting. When you export a configuration file for the device, the system comments the password out for security reasons. **Terminology reference:** **Web interface**: Password **Phone UI**: Password

Table continues…

XML parameter name	Description
`<reg_timeout>`	To specify the period in seconds after which the SIP registration expires. The phone automatically renews the registration within the set period if it is still on and connected to the server. The default setting is 300 seconds. **Terminology reference:** **Web interface**: Registration Timeout **Phone UI**: Registration Timeout
`<secondary_account>`	The top line of the secondary account section. After registration, the secondary account is normally applicable for inbound calls only, but it also makes outbound calls if the primary account becomes unregistered or fails.
`<name>`	To specify the name visible on the phone screen on the primary line. This name is not a part of the SIP messaging. **Important:** This is a mandatory setting. **Terminology reference:** **Web interface**: Account Name **Phone UI**: Account Name
`<user>`	To specify the SIP account name as configured on the SIP Registrar. The phone uses the content of this field to construct the user URI. **Important:** Do not use the following characters: # % @. Do not include `@sipdomain` data. This is a mandatory setting. **Terminology reference:** **Web interface**: User **Phone UI**: User
`<registrar>`	To specify the IP address or a fully qualified domain name (FQDN) of the SIP server where you register the account. The format options are the following: `10.10.1.100` and `10.10.1.100:5060` for a local SIP server, or `sip.company.net` for a FQDN. **Important:** This is a mandatory setting. **Terminology reference:** **Web interface**: Registrar **Phone UI**: Registrar Address

Table continues…

XML parameter name	Description
<proxy>	To specify the proxy server which the company uses for SIP peer communication. The format options are the following: 10.10.1.100:1234 for a local proxy with an optionally specified port or proxy.company.net:port for a FQDN. If you append ;hide to the end of the proxy string, B199 avoids adding a record route to the SIP messaging. For more information, see Messaging the proxy without adding a record route on page 103. **Terminology reference:** **Web interface**: Proxy **Phone UI**: Proxy
<keep_alive>	To specify if the phone maintains an active connection to the network. The device can use Keep Alive messages to ensure that the IP path to the Registrar is always available by sending periodic SIP messages. If the network fails and there are no messages received, the phone attempts to switch to the Secondary account for outbound calls, or the Fallback account. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Keep Alive **Phone UI**: Keep Alive
<cred>	The top of the SIP credentials for the Secondary account section.
<realm>	To specify the network domain which the phone accepts incoming calls from. For example, company.com. The other name is the SIP domain. You can leave this field blank or put an asterisk (*) to accept all incoming call invites from any SIP domain. **Terminology reference:** **Web interface**: Realm **Phone UI**: Realm
<username>	To specify the SIP authentication name. If you leave it blank, the phone uses the content of the <user> parameter to authenticate and register the account. **Terminology reference:** **Web interface**: Authentication Name **Phone UI**: Authentication Name

Table continues…

XML parameter name	Description
`<password>`	To specify the SIP password for authentication with the Registrar. **Important:** This is a mandatory setting. When you export a configuration file for the device, the system comments the password out for security reasons. **Terminology reference:** **Web interface**: Password **Phone UI**: Password
`<reg_timeout>`	To specify the period in seconds after which the SIP registration expires. The phone automatically renews the registration within the set period if it is still on and connected to the server. The default setting is 300 seconds. **Terminology reference:** **Web interface**: Registration Timeout **Phone UI**: Registration Timeout
`<fallback_account>`	The top line of the fallback account section. After registration, the fallback account is applicable for inbound and outbound calls only if the primary and secondary accounts become unregistered or fail.
`<name>`	To specify the name visible on the phone screen on the primary line. This name is not a part of the SIP messaging. **Important:** This is a mandatory setting. **Terminology reference:** **Web interface**: Account Name **Phone UI**: Account Name
`<user>`	To specify the SIP account name as configured on the SIP Registrar. The phone uses the content of this field to construct the user URI. **Important:** Do not use the following characters: # % @. Do not include `@sipdomain` data. This is a mandatory setting. **Terminology reference:** **Web interface**: User **Phone UI**: User

Table continues…

XML parameter name	Description
`<registrar>`	To specify the IP address or a fully qualified domain name (FQDN) of the SIP server where you register the account. The format options are the following: `10.10.1.100` and `10.10.1.100:5060` for a local SIP server, or `sip.company.net` for a FQDN. **Important:** This is a mandatory setting. **Terminology reference:** **Web interface**: Registrar **Phone UI**: Registrar Address
`<proxy>`	To specify the proxy server which the company uses for SIP peer communication. The format options are the following: `10.10.1.100:1234` for a local proxy with an optionally specified port or `proxy.company.net:port` for a FQDN. If you append `;hide` to the end of the proxy string, B199 avoids adding a record route to the SIP messaging. For more information, see Messaging the proxy without adding a record route on page 103. **Terminology reference:** **Web interface**: Proxy **Phone UI**: Proxy
`<keep_alive>`	To specify if the phone maintains an active connection to the network. The device can use Keep Alive messages to ensure that the IP path to the Registrar is always available by sending periodic SIP messages. If the network fails and there are no messages received, the phone attempts to switch to the Secondary account for outbound calls, or the Fallback account. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Keep Alive **Phone UI**: Keep Alive
`<cred>`	The top of the SIP credentials for the Fallback account section.

Table continues…

XML parameter name	Description
`<realm>`	To specify the network domain which the phone accepts incoming calls from. For example, `company.com`. The other name is the `SIP domain`. You can leave this field blank or put an asterisk (*) to accept all incoming call invites from any SIP domain. **Terminology reference:** **Web interface**: Realm **Phone UI**: Realm
`<username>`	To specify the SIP authentication name. If you leave it blank, the phone uses the content of the `<user>` parameter to authenticate and register the account. **Terminology reference:** **Web interface**: Authentication Name **Phone UI**: Authentication Name
`<password>`	To specify the SIP password for authentication with the Registrar. **Important:** This is a mandatory setting. When you export a configuration file for the device, the system comments the password out for security reasons. **Terminology reference:** **Web interface**: Password **Phone UI**: Password
`<reg_timeout>`	To specify the period in seconds after which the SIP registration expires. The phone automatically renews the registration within the set period if it is still on and connected to the server. The default setting is 300 seconds. **Terminology reference:** **Web interface**: Registration Timeout **Phone UI**: Registration Timeout
`<source_port>`	To specify the source port which indicates the UDP, TCP, or TLS port or socket that the phone uses during outbound SIP signaling. • UDP and TCP: `5060`. • TLS and SIPs: `5061`. **Terminology reference:** **Web interface**: Source Port **Phone UI**: Port

Table continues…

XML parameter name	Description
<transport_protocol>	To specify the SIP Messaging protocol which the phone must use. It must match the capabilities of the communications server for the Primary, Secondary and Fallback accounts. UDP and TCP typically do not require any further adjunct configuration. Being secure and encrypted, TLS and SIPs may require adjustment of the supported TLS versions of certificate installation. **Terminology reference:** **Web interface**: Transport Protocol **Phone UI**: Transport Protocol
<tls>	The top of the TLS configuration section. The parameters in this section are applicable if you choose TLS or SIPs as the transport_protocol.
<sni>	To enable or disable using the Server Name Indication (SNI) extension for TLS connections to a SIP server. The options are the following: • True. • False. This is the default value. **Terminology reference:** **Web interface**: SNI **Phone UI**: SNI
<tls_method>	To identify the lowest version of the TLS protocol that the phone supports. The options are: • TLSv1 • TLSv1_1 • TLSv1_2 **Terminology reference:** **Web interface**:TLS Method **Phone UI**: TLS Method
<tls_neg_timeout>	To specify the TLS negotiation time-out in seconds for both outgoing and incoming connections during call setup. If this negotiation is not successful within the specified time defined in seconds, the phone stops the negotiation. You can disable the timer by entering 0. **Terminology reference:** **Web interface**:Negotiation Timeout **Phone UI**: TLS Negotiation

Table continues…

XML parameter name	Description
<tls_password>	To specify the password for the private key if it is encrypted. **Terminology reference:** **Web interface**: Device Private Key Password **Phone UI**: TLS Password
<verify_client>	To specify whether the phone challenges and verifies the peer during each incoming SIP connection attempt. This is a required feature when the SIP realm is not defined and the device accepts incoming call requests from any domain. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Verify Client **Phone UI**: Verify Client
<verify_server>	To specify whether the phone challenges and verifies the peer during each incoming SIP connection attempt. This is a required feature when the SIP realm is not defined and the device accepts incoming call requests from any domain. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Verify Server **Phone UI**: Verify Server
<require_client_cert>	To enable validation of the client certificate during each incoming call attempt. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Require Client Certificate **Phone UI**: Require Client Certificate
<advanced>	The top line of the Advanced settings section which contains miscellaneous SIP configuration parameters. These parameters often contain the default values.

Table continues…

XML parameter name	Description
`<disable_rport>`	To enable the remote port forwarding. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Disable rport **Phone UI**: Disable 'rport'
`<session_timers>`	To specify whether the phone uses SIP timers during SIP negotiation. The options are the following: • `0` - **Disabled**. • `1` - **Optional**. This is the default setting. • `2` - **Mandatory** **Terminology reference:** **Web interface**: Session Timers **Phone UI**: Session Timers
`<session_expiration_minimum>`	To specify the minimum timer value which the phone negotiates during SIP negotiation. The default value is 90 seconds. **Important:** This parameter is only available in the .xml configuration file. Do not modify.
`<session_expiration>`	To specify the target session timer which the phone negotiates during SIP negotiation. The default setting is 1800 seconds (30 minutes). **Terminology reference:** **Web interface**: Session Expiration **Phone UI**: Session Expiration
`<outbound_proxy>`	To specify the IP address or FQDN of the outbound call proxy. If the `<outbound_proxy>` parameter contains an IP address or FQDN, all SIP messages for the primary, secondary and fallback accounts are sent to the outbound proxy. **Terminology reference:** **Web interface**: Outbound Proxy **Phone UI**: Outbound Proxy

Table continues…

XML parameter name	Description
<enable_sip_traces>	To enable provision of key information for troubleshooting. The default setting is disabled. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Enable SIP Traces **Phone UI**: Not configurable
<allow_contact_rewrite>	To enable storing the IP address from the response of the register request. If there is any change detected, the phone unregisters the available SIP URI and updates it with a new address. The options are the following: • True. This is the default setting. • False. **Terminology reference:** **Web interface**: Allow Contact Rewrite **Phone UI**: Allow Contact Rewrite
<allow_via_rewrite>	To enable rewriting of the VIA header in the SIP Register requests. If there is any change detected, the phone overwrites the VIA header with the new data. The options are the following: • True. This is the default setting. • False. **Terminology reference:** **Web interface**: Enable Via Rewrite **Phone UI**: Allow Via Rewrite
<enable_sip_replaces>	To enable the use of the SIP Replaces header. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Enable SIP Replaces **Phone UI**: Enable SIP Replaces

Table continues…

XML parameter name	Description
<contact_use_src_port_even_with_dns>	To enable ignoring of the DNS provided source port. The options are the following: • True. • False. This is the default setting. **Important:** This parameter is only available in the .xml configuration file.
<enable_lock_codec>	To enable the lock codec feature. The options are the following: • True. This is the default setting. • False. **Important:** This parameter is only available in the .xml configuration file.
<use_static_source_port>	To enable the phone to use the port identified in <source_port> or the default values for <source_port>. When disabled, the device uses ephemeral ports from the port usage table. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Use Static Source Port **Phone UI**: Use Static Source Port
<dtmf>	The top of the DTMF section.
<method>	To configure the Dual-tone multi-frequency (DTMF) signaling method. The options are the following: • **RFC 4733**. With this method, DTMF signals are carried in RTP packets by using a separate RTP payload format. This is the default option. • **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 generates the tones and sends them in the voice frequency band. This is the least preferred method for interoperability. **Terminology reference:** **Web interface**: DTMF Method **Phone UI**: DTMF Method

Table continues…

XML parameter name	Description
<rfc4733_payload_type>	To specify the DTMF payload media value to use in SIP negotiations. The value range is from 96 to 127. The default setting is 101. **Terminology reference:** **Web interface**: RFC 4733 payload type **Phone UI**: RFC 4733 payload type
<nat_traversal>	The top line of the Network Address Translation Traversal (NAT) section.
<ice>	The top line of the Interactive Connectivity Establishment (ICE) section.
<enable>	To enable ICE. ICE uses various techniques to allow SIP-based VoIP devices to successfully traverse the variety of firewalls that may exist between the devices. The protocol provides a mechanism for the endpoints to identify the most optimal path for the media traffic to follow. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: ICE **Phone UI**: Enable ICE
<stun>	The top line of the Simple Traversal of UDP through the NAT (STUN) section.
<enable>	STUN is a protocol to assist devices behind a NAT firewall or router with packet routing. The protocol allows applications operating through the NAT to discover the presence and type of the NAT and obtain a public IP address (NAT address) and port number that the NAT allocates 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*. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: STUN **Phone UI**: Enable STUN
<server>	To configure the IP address or FQDN of the STUN Server. **Terminology reference:** **Web interface**: STUN Server **Phone UI**: STUN Server
<turn>	The top line of the Traversal Using Relay NAT (TURN) section.

Table continues…

XML parameter name	Description
<enable>	To enable TURN. TURN is an extension of the ICE protocol that enables NAT traversal when both endpoints are behind symmetric NAT. With TURN, media traffic for the session has 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. The options are the following: • True. • False. This is the default setting. **Important:** To enable TURN, you must enable ICE. **Terminology reference:** **Web interface**: TURN **Phone UI**: Enable TURN
<server>	To specify the IP address:port or FQDN of the TURN server. **Terminology reference:** **Web interface**: TURN Server **Phone UI**: TURN Server
<user>	To specify the TURN server user authentication name. **Terminology reference:** **Web interface**: User **Phone UI**: TURN User
<password>	To TURN server user authentication password. **Terminology reference:** **Web interface**: Password **Phone UI**: TURN Password
<phone>	The top line of the phone general parameters section.
<name>	To enter the name to be displayed on the phone screen above the line appearances. This name is available in any SIP messaging. The maximum input length is 28 characters. **Terminology reference:** **Web interface**: Phone Name **Phone UI**: Name

Table continues…

XML parameter name	Description
`<language>`	To select the language. The options are: • `en` - English. This is the default setting. • `se` - Swedish • `da` - Danish • `no` - Norwegian • `fi` - Finnish • `it` - Italian • `de` - German • `fr` - French • `sp` - Spanish • `br` - Portuguese • `nl` - Dutch • `zh` - Simplified Chinese • `ru` - Russian • `tr` - Turkish **Terminology reference:** **Web interface**: Phone Language **Phone UI**: Language
`<allow_legacy_encryption>`	To enable or disable legacy encryption for backward compatibility. The phone's R 1.0.4 firmware is disabled by default for older less secure encryption algorithms. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Allow Legacy Encryption **Phone UI**: Allow Legacy Encryption
`<password>`	To specify the Administrator password. The maximum input length is 32 characters. **Terminology reference:** **Web interface**: Not configurable **Phone UI**: Admin Password

Table continues…

XML parameter name	Description
`<ringlevel>`	To configure the default ringing level after reboot. The levels are the following: • **Level 0** - The phone stays silent. LED flash indication only. • **Level 1** • **Level 2** • **Level 3** • **Level 4**. This is the default setting. • **Level 5** • **Level 6**. The loudest ringing level. **Terminology reference:** **Web interface**: Ringtone Level **Phone UI**: Ring Level
`<key_tone>`	To specify whether the phone provides audible feedback of key presses. The options are the following: • True. This is the default setting. • False. **Terminology reference:** **Web interface**: Key Tone **Phone UI**: Key Tone
`<is_daisy_chain_slave>`	To specify the mode of the phone in case of a daisy chain arrangement. When using multiple B199 devices cabled to provide increased room coverage, you must configure the Main (Leader) and Expansion (Follower) arrangement. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Daisy Chain Mode **Phone UI**: Daisy Chain

Table continues…

XML parameter name	Description
<phone_status_api>	To enable WebApp Debug which is a debug tool for development and troubleshooting the Web Admin pages via the System Logs. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Webapp Debug **Phone UI**: Not configurable
<sleep_mode_timeout>	To enable Sleep mode and configure the time-out value. The default value is 0, which means that the feature is disabled. To enable Sleep mode and to specify the time-out in minutes, set the value in the range from 1 to 500. **Important:** This parameter is only available in the .xml configuration file.
<enable_startup_sound>	To specify whether the branded start-up sound plays when the device boots. The options are the following: • True. This is the default setting. • False. **Terminology reference:** **Web interface**: Startup Sound **Phone UI**: Startup Sound
<fips_mode>	To enable FIPS mode which uses encryption and cryptographic functions compliant with the Federal Information Processing Standards (FIPS). When you enable FIPS mode, the phone employs approved key exchange algorithms, cryptographic algorithms and authentication techniques to meet the FIPS 140-2 and 140-x requirements. The options are the following: • True. This is the default setting. • False. **Note:** Legacy Encryption or EAP MD5 can not operate with FIPS enabled. **Terminology reference:** **Web interface**: FIPS Mode **Phone UI**: FIPS Mode

Table continues…

XML parameter name	Description
`<call_log_enable>`	To enable Call Log and view the Recent call list on the phone. The options are the following: • True. This is the default setting. • False. When you set this setting to `false`, the Recent calls list becomes unavailable. Here, if you tap **Recent**, the phone displays the following message: `Call Log is disabled by administrator.` **Note:** The phone records information about the calls only with the enabled Call Log. When the administrator disables the Call Log, the phone does not register calls and the call log becomes invisible to everyone. Disabling Call Log does not delete call records from the call log. To see this information, the administrator must enable Call Log. If the administrator enables and disables Call Log as needed, the phone keeps the call records only for the periods of the active Call Log. **Terminology reference:** **Web interface**: Call Log **Phone UI**: Call Log
`<ceiling_audio_mode>`	To enable or disable Ceiling audio mode. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Ceiling Audio Mode **Phone UI**: Ceiling Audio Mode
<bluetooth>	The top line of the Bluetooth section.
`<enable>`	To enable the Bluetooth Radio and functionality. The options are the following: • True. This is the default setting. • False. **Important:** This parameter is only available in the .xml configuration file. When you enable Bluetooth, the ability to pair, disconnect and remove pairing becomes available in the phone's Bluetooth menu as well as Avaya® Conference Assistant.
<usb>	To specify the USB parameters.

Table continues…

XML parameter name	Description
`<enable>`	To specify whether USB ports are enabled. The default setting is True. **Important:** This parameter is only available in the .xml configuration file.
`<echo_cancelling_speakerphone>`	To specify whether the phone is used as an Echo Cancelling Speakerphone. When you set this setting to true, Windows discovers B199 Conference Phone as default speaker and communication device. Here, Windows Device Manager shows the phone as one device with the name Echo Cancelling Speakerphone. The USB Product ID (PID) is 095E. When you set this setting to `false`, Windows Device Manager shows the phone as two separate devices with different names: Speakers and Microphone. Here, the USB Product ID (PID) is 0971. The default setting is true. **Important:** This parameter is only available in the .xml configuration file.
`<network>`	The top line of the Network section.
`<dhcp>`	To enable DHCP process. The options are the following: • True. This is the default setting. • False. **Terminology reference:** **Web interface**: Enable DHCP **Phone UI**: DHCP
`<hosts_map>`	To specify the FQDN/IP mapping information that stays persistent for the device. This arrangement provides for the SIP operation even if DNS is not available. **Important:** This parameter is only available in the .xml configuration file. **Terminology reference:** **Web interface**: Not configurable **Phone UI**: Not configurable

Table continues…

XML parameter name	Description
<host>	To specify the FQDN to IP mapping. The administrator can add several host entities or leave the parameter empty. **Note:** The device supports the mappings for the primary, secondary and fallback SIP accounts. **Important:** This parameter is only available in the .xml configuration file. **Terminology reference:** **Web interface**: Not configurable **Phone UI**: Not configurable
<ip>	To specify an IP address for the FQDN to IP mapping. **Important:** This parameter is only available in the .xml configuration file. **Terminology reference:** **Web interface**: Not configurable **Phone UI**: Not configurable
<name>	To specify a name for the FQDN to IP mapping in the following format: sipserver1.com. **Important:** This parameter is only available in the .xml configuration file. **Terminology reference:** **Web interface**: Not configurable **Phone UI**: Not configurable
<hostname>	To specify the hostname of the phone to use when performing DHCP, DNS and other network transactions. The default name is AvayaB199. **Terminology reference:** **Web interface**: Network Hostname **Phone UI**: Hostname

Table continues…

XML parameter name	Description
<domain>	To specify the domain name of the phone to be used to indicate the network domain B199 is part of. **Note:** With DHCP enabled, DHCP server may provide this parameter, and therefore you can leave this field blank. **Terminology reference:** **Web interface**: Domain Hostname **Phone UI**: Domain
<dns1>	To specify the IP Address of the primary Domain Name Server. **Note:** With DHCP enabled, DHCP server may provide this parameter, and therefore you can leave this field blank. **Terminology reference:** **Web interface**: DNS1 **Phone UI**: DNS 1
<dns2>	To specify the IP Address of the secondary Domain Name Server. **Note:** With DHCP enabled, DHCP server may provide this parameter, and therefore you can leave this field blank. **Terminology reference:** **Web interface**: DNS2 **Phone UI**: DNS 2
<static_ip>	The top line of the static IP configuration section.
<ip>	To specify the IPv4 address for the phone to use. **Terminology reference:** **Web interface**: IP **Phone UI**: IP
<netmask>	To specify the network mask for your phone to determine on subnet versus off subnet addresses and when the gateway is the path to use. **Terminology reference:** **Web interface**: Network Mask **Phone UI**: Netmask
<gateway>	To specify the IPv4 address of the subnet gateway. **Terminology reference:** **Web interface**: Gateway **Phone UI**: Gateway

Table continues…

XML parameter name	Description
<vlan>	To enable the VLAN tagging of the Ethernet packets. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: VLAN Enable **Phone UI**: VLAN
<vlanid>	To specify the VLAN ID for the phone to use when tagging Ethernet packets. The device accepts only ingress packets tagged with the configured VLAN. The options are the following: from 0 to 4094. **Note:** With LLDP enabled, the L2/3 switch may broadcast a Network Policy LLDP packet that sets the VLAN ID for the phone. The LLDP broadcast packet overrides the manually configured VLAN value. **Terminology reference:** **Web interface**: VLAN ID **Phone UI**: VLAN ID
<ieee_8021x>	The top line of the 802.1x section.
<enable>	To enable 802.1x that is a network security and authentication mechanism aimed to ensure that only authorized IP devices obtain access to the network. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Enable 802.1X **Phone UI**: 802.1x
<username>	To specify the 802.1x username as provision in the security server for the network. **Terminology reference:** **Web interface**: Username **Phone UI**: Authentication Name
<eap_md5>	The top line of the EAP MD5 section.

Table continues…

XML parameter name	Description
<enable>	To enable the EAP MD5 authentication method for the phone to use with the 802.1x authentication server. **Note:** You must enable **Legacy Encryption** to use **EAP MD5**. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: EAP MD5 Enable **Phone UI**: EAP MD5
<password>	To specify the EAP MD5 password for the phone to use during authentication. **Terminology reference:** **Web interface**: Password **Phone UI**: EAP-MD5 Password
<eap_tls>	The top line of the EAP TLS section.
<enable>	To enable the EAP TLS authentication method. The TLS is a state-of-art method which is more secure than the MD5 method. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Enable EAP TLS **Phone UI**: EAP TLS
<password>	To specify the EAP TLS password to be used during authentication. **Terminology reference:** **Web interface**: Device Private Key Password **Phone UI**: Private Key Password
<lldp>	The top line of the LLDP section. There are character limitations (number of characters and type of characters) for a number of the parameters below. Avaya™ recommends to validate the .xml configuration file using the .vsd file provided.

Table continues…

XML parameter name	Description
<enable>	To enable the Link Layer Discovery Protocol (LLDP). When enabled, the phone broadcasts information about itself to the neighboring devices. The device also receives and may act in line with the LLDP information broadcast from Layer 2 or 3 devices managing the subnet. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Enable **Phone UI**: Not configurable
<country>	To specify the country of the phone installation. The country indication may be 2 or 3 uppercase letters or 3 digits as defined by the ISO-3166 format. **Terminology reference:** **Web interface**: Country Code **Phone UI**: Not configurable
<country_subdivision>	To specify the region, province, state or other country subdivision of the phone installation. The country indication may be 2 or 3 uppercase letters or 3 digits as defined by the ISO-3166 format. **Terminology reference:** **Web interface**: Country Subdivision **Phone UI**: Not configurable
<county>	To specify the county, parish, district, or other applicable administrative division. The maximum input length is 50 characters. **Important:** Do not use the following characters: ! @ # $ % ^ * . - _. **Terminology reference:** **Web interface**: County **Phone UI**: Not configurable
<city>	To specify the city of installation. The maximum input length is 40 characters. **Important:** Do not use the following characters: ! @ # $ % ^ * . ,. **Terminology reference:** **Web interface**: City **Phone UI**: Not configurable

Table continues…

XML parameter name	Description
<city_division>	To specify the subdivision or section of the city. The maximum input length is 60 characters. **Important:** Do not use the following characters: *! @ # $ % ^ ? / *. **Terminology reference:** **Web interface**: City Division **Phone UI**: Not configurable
<block>	To specify the block name within the city. **Terminology reference:** **Web interface**: Block **Phone UI**: Not configurable
<street>	To specify the street name. **Important:** Do not use the following characters: *! @ # $ % ^ ? / *. **Terminology reference:** **Web interface**: Street **Phone UI**: Not configurable
<direction>	To specify the direction or orientation of the street. **Important:** Do not use the following characters: *^ ! @ # $ % ^ * / \ _ 0-9*. **Terminology reference:** **Web interface**: Direction **Phone UI**: Not configurable
<trailing_street_suffix>	To specify the trailing street suffix. The maximum input length is 10 characters. **Important:** Do not use the following characters: *! @ # $ % ^ * / \ _ 0-9*. **Terminology reference:** **Web interface**: Trailing Street Suffix **Phone UI**: Not configurable

Table continues…

XML parameter name	Description
`<street_suffix>`	To specify the freeform or standard street suffix. For example, Alley, ALY, CENTER, CTR. The maximum input length is 15 characters. **Important:** Do not use the following characters: *! @ # $ % ^ * / \ _* or digits. **Terminology reference:** **Web interface**: Street Suffix **Phone UI**: Not configurable
`<number>`	To specify the building number with relation to the street. **Terminology reference:** **Web interface**: Number **Phone UI**: Not configurable
`<number_suffix>`	To specify the subdivision of the street number such as a unit. For example, `B` to indicate that the phone is at 16B Street. The maximum input length is 20 characters. **Important:** Do not use the following characters: *! @ # $ % ^ **. **Terminology reference:** **Web interface**: Number Suffix **Phone UI**: Not configurable
`<landmark>`	To specify the reference or commonly known location or landmark. The maximum input length is 30 characters. **Important:** Do not use the following characters: *! @ # $ % ^ / * or digits. **Terminology reference:** **Web interface**: Landmark **Phone UI**: Not configurable
`<additional>`	To specify any additional reference points. The maximum input length is 30 characters. **Important:** Do not use the following characters: *! @ # $ % ^ / * or digits. **Terminology reference:** **Web interface**: Additional **Phone UI**: Not configurable

Table continues…

XML parameter name	Description
`<name>`	To specify the device name. The default name is `Avaya B199`. The maximum input length is 60 characters. **Important:** Do not use the following characters: *! @ # $ % ^ ?*. **Terminology reference:** **Web interface**: Name **Phone UI**: Not configurable
`<zip>`	To specify the ZIP or postal code of the location. The maximum input length is 20 characters. **Important:** Do not use the following characters: *! @ # $ % ^ **. **Terminology reference:** **Web interface**: Zip **Phone UI**: Not configurable
`<building>`	To specify the name of the building. The maximum input length is 60 characters. **Important:** Do not use the following characters: *! @ # $ % ^ ?*. **Terminology reference:** **Web interface**: Building **Phone UI**: Not configurable
`<unit>`	To specify a unit within a building. The maximum input length is 30 characters. **Important:** Do not use the following characters: *! @ # $ % ^ ?*. **Terminology reference:** **Web interface**: Unit **Phone UI**: Not configurable
`<floor>`	To specify the floor within the building. The value range is from -5 to 250. **Terminology reference:** **Web interface**: Floor **Phone UI**: Not configurable

Table continues…

XML parameter name	Description
`<room>`	To specify the room name. The maximum input length is 60 characters. **Important:** Do not use the following characters: *!* @ # *$* % ^ *?*. **Terminology reference:** **Web interface**: Room **Phone UI**: Not configurable
`<place_type>`	To specify the premises type. For example, `office` or `laboratory`. The maximum input length is 60 characters. **Important:** Do not use the following characters: *!* @ # *$* % ^ *?* / \. **Terminology reference:** **Web interface**: Place Type **Phone UI**: Not configurable
`<script>`	To specify the script. The maximum input length is 60 characters. **Important:** Do not use the following characters: *!* @ # *$* % ^ *?* / \. **Terminology reference:** **Web interface**: Script **Phone UI**: Not configurable
`<elin>`	To specify the Emergency Location Identification Number (ELIN) to support e911 systems that utilize LLDP for location gathering and monitoring. The maximum input length is 31 characters. **Terminology reference:** **Web interface**: ELIN **Phone UI**: Not configurable
`<qos>`	The top line of the Quality of service section.
`<dscp_sip>`	To specify the diffserv codepoint to tag SIP messages. The options are the following: from 0 to 63 in line with IETF RFC-4594. The default setting is 0, which is untagged. **Terminology reference:** **Web interface**: SIP DiffServ **Phone UI**: Not configurable

Table continues…

XML parameter name	Description
<dscp_media>	To specify the diffserv codepoint to tag RTP/SRTP audio packets. The options are the following: from 0 to 63 in line with IETF RFC-4594. The default setting is 0, which is untagged. **Terminology reference:** **Web interface**: Media DiffServ **Phone UI**: Not configurable
<device_management>	The top line of the Device Management section.
<enable>	To enable Device Management service within the phone. The options are the following: • True. This is the default setting. • False. **Terminology reference:** **Web interface**: Enable **Phone UI**: Enable
<update_interval>	To indicate how often the phone contacts the server to see if an update is available. The value range is from 1 minute to 21,000 minutes. The default setting is 60 minutes. **Terminology reference:** **Web interface**: Update Interval **Phone UI**: Not configurable
<update_max_wait>	To specify a waiting time that expires if the server and the phone cannot complete the provisioning check due to network failure. The default setting is 1 second. **Terminology reference:** **Web interface**: Maximum Time To Wait To Update **Phone UI**: Not configurable
<server>	To specify the IP address, FQDN or URL of the provisioning server unless DHCP provides the data. The string can be complex such as https://laboratory.northamerica.acme.com:443/webroot/avayaFiles. Here, the phone uses TLS to reach port 443 and specifies the path to the files. **Terminology reference:** **Web interface**: File Server **Phone UI**: Provisioning Server

Table continues…

XML parameter name	Description
<check_server_certificate>	To enable the Check certificate when the phone validates the server certificate credentials each time it contacts the server. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Check Certificate **Phone UI**: Check Server Certificate
<lowest_tls_version>	To specify the lowest TLS version for the phone to use during secure communications with the provisioning server. The options are the following: • **TLSv1**. This is the default setting. • **TLSv1_1** • **TLSv1_2** **Terminology reference:** **Web interface**: Lowest TLS Version **Phone UI**: Lowest TLS Version
<dhcp_option>	To select the DHCP option which indicates with DHCP Option number how the system parses packets to obtain the phone specific configuration parameters. The options are the following: • **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. Here, it searches the DHCP provided offer for the correct parameters. For more information, see DHCP configuration options on page 28. **Terminology reference:** **Web interface**: DHCP Option **Phone UI**: DHCP Option

Table continues…

XML parameter name	Description
<des>	The top line of the Device Enrollment Services section.
<des_stat>	To specify user setting of DES enablement. The options are the following: • 1. This value indicates that the feature is disabled, but you can see it on the phone and in the web interface to administer it accordingly. • 2. This value indicates that DES is enabled, and you can not see the option to disable the feature on the phone and in the web interface. This is the default setting. **Note:** The system sets the value to 2 after a factory reset. **Terminology reference:** **Web interface**: DES Provisioning **Phone UI**: DES Enablement
<logging>	The top line of the Logging section.
<pjsip_log_level>	To change the level of logging for the SIP application in the phone. The options are the following: • 0 - Fatal • 1 - Error • 2 - Warning • 3 - Info. This is the default setting. • 4 - Debug. • 5 - Trace. **Terminology reference:** **Web interface**: PJSIP Log Level **Phone UI**: Not configurable
<remote_syslog_enable>	To enable the use of a remote syslog server. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Not configurable **Phone UI**: Not configurable
<remote_syslog_host>	To specify the IP address or FQDN of the syslog server. **Terminology reference:** **Web interface**: Not configurable **Phone UI**: Not configurable
<ldap>	The top line of the Lightweight Directory Access Protocol (LDAP) section.

Table continues…

XML parameter name	Description
`<enable>`	To enable the LDAP service in the phone. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Enable **Phone UI**: Not configurable
`<name_filter>`	When the phone uses the LDAP search, it contacts the LDAP server with the search parameter as defined by the name filter. The default is `(|(sn=%*)(cn=%*))` which uses the search text and requests a search against the Surname (SN) and the Common Name (CN) values on the LDAP server. **Terminology reference:** **Web interface**: Name Filter **Phone UI**: Not configurable
`<server_url>`	To enter the URL that specifies the protocol (LDAP or LDAPS), the FQDN and the port to be used when communicating with the phone. For example, `ldaps://cd.lab.acme.com:636`. **Terminology reference:** **Web interface**: URL **Phone UI**: Not configurable
`<search_base>`	To specify the search base that indicates the range or domain of the searchable base. The default value is `dc=example, dc=com` that shows the domain components of `example.com`. **Important:** Do not use the following characters: *( ), !,* |*, &, *, -*. **Terminology reference:** **Web interface**: Search base **Phone UI**: Not configurable
`<username>`	The phone needs a username and a password to authenticate with the LDAP server to perform searches. The username format can be simple such as `JohnDoe` which stands for a user network, or it can base on the LDAP directory structure such as `uid=400130352125,dc=acme,dc=com`. **Terminology reference:** **Web interface**: Username **Phone UI**: Not configurable

Table continues…

XML parameter name	Description
<password>	To specify the password that the phone uses when authenticating with the LDAP server. **Terminology reference:** **Web interface**: Password **Phone UI**: Not configurable **Important:** This parameter is not in .xml configuration files if you export them through the web interface.
<max_hits>	To determine the number of search results to request. The value range is from 0 to 1000. The default value is 20 which nicely displays on the phone. **Terminology reference:** **Web interface**: Max hits **Phone UI**: Not configurable
<country_code>	To specify the country code based on ISO 3166. If you enter it, the LDAP searches, that match the country code, remove it from the displayed search results. When you specify the country code, all number_attributes must be void of non-number characters before the number conversion starts. **Terminology reference:** **Web interface**: Country code **Phone UI**: Not configurable
<area_code>	To specify the Numbering Plan Area (NPA) or Area Code. If you enter it, the LDAP searches, that match the area code, remove it from the displayed search results. The maximum input length is 10 digits. **Terminology reference:** **Web interface**: Area code **Phone UI**: Not configurable
<external_prefix>	To specify a special prefix for dialing external numbers. If you define it, the phone appends it at the start of all outbound calls when making calls to external numbers. For example, 9 to seize an outbound trunk. **Terminology reference:** **Web interface**: External prefix **Phone UI**: Not configurable

Table continues…

XML parameter name	Description
<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. If you set this parameter, the phone only adds the external prefix to the dialed number if the dialed digits exceed the minimal length for external prefix value. For example, parameter value 8 allows for 7 digit direct internal dialing. The value range is from 0 to 32. The default value is 0. **Terminology reference:** **Web interface**: Min length for external prefix **Phone UI**: Not configurable
<exact_length_for_no_ext_prefix>	To specify the exact length for the external prefix. If you define it, the phone does not append the external prefix. For example, parameter value 11 allows if the outbound user dials 012225551212 which includes the trunk access code, country code and NPA-NXX. **Terminology reference:** **Web interface**: Exact length for no external prefix **Phone UI**: Not configurable
<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. **Terminology reference:** **Web interface**: Number prefix for no external prefix **Phone UI**: Not configurable

Table continues…

XML parameter name	Description
<number_attributes>	A successful LDAP query results in a number of details for the requested contact. The Default telephone number related LDAP IDs reflect the following: • Phone number • Mobile phone • Home phone • Work phone • Other **Note:** The LDAP administrator can also use custom parameters. The number attributes parameter matches the needed LDAP <id> and sets the text to display <value> as follows: <number_attributes type="xml"> <number_attribute> <id>telephoneNumber</id> <value>PHONENUMBER</value> </number_attribute> <number_attribute> <id>mobile</id> <value>MOBILE</value> </number_attribute> </number_attributes> Number attributes are attributes containing phone numbers and their value forms part of the "INVITE" message during a SIP call. The attributes must only contain number characters to make a SIP call. **Terminology reference:** **Web interface**: Number Attributes → Add attribute label **Phone UI**: Not configurable
<display_name>	To define which parameter that the LDAP query returns is used as the Display Name. Default is %cn (Common Name). **Terminology reference:** **Web interface**: Display name **Phone UI**: Not configurable

Table continues…

XML parameter name	Description
<sort_results>	To enable sorting of the query results in alphabetical order based on the Display name. The options are the following: • True. This is the default setting. • False. **Terminology reference:** **Web interface**: Sort results **Phone UI**: Not configurable
<use_dm_certificates_for_ldaps>	To enable the use of the Device Management certificates when communicating with the LDAP server securely. The options are the following: • True. • False. This is the default setting. **Terminology reference:** **Web interface**: Not configurable **Phone UI**: Not configurable
<SCEP>	The top line of the Simple Certificate Enrollment Protocol(SCEP) section.
<MYCERTURL>	To enter the URL of the SCEP server. **Terminology reference:** **Web interface**: SCEP Server **Phone UI**: Not configurable
<MYCERTCN>	To enter the Common Name (CN) for the phone to use when requesting a certificate. By default, the CN is the B199 serial number. **Terminology reference:** **Web interface**: Common Name **Phone UI**: Not configurable
<MYCERTDN>	To specify the DN which is the Subject of the certificate request. For example, `/C=US/ST=NJ/L=MyTown/O=MyCompany` is a DN for a New Jersey based company in the United States, in `MyTown` at `MyCompany.subject` of the SCEP certificate request. **Terminology reference:** **Web interface**: Subject **Phone UI**: Not configurable

Table continues…

XML parameter name	Description
<MYCERTCAID>	To specify the CA identifier. The phone generates the SCEP certificate request and signs it with a certificate on the device. The CA ID tells the SCEP server which CA the certificate used at generation of the request. The default value is **CAIdentifier**. **Terminology reference:** **Web interface**: CA Identifier **Phone UI**: Not configurable
<MYCERTKEYLEN>	To specify the length of the public and private keys. The options are the following: • 1024. This is the default setting. • 2048. **Terminology reference:** **Web interface**: Key Length **Phone UI**: Not configurable
<MYCERTRENEW>	The phone generates a certificate renewal request prior to the expiry of the current certificate based on the following formula: (Date of Expiry – Date of Issue) * Key Renew Percentage. The MYCERTKEYRENEW parameter indicates the percentage of certificate life that passes prior to a renewal request. The value range is from 1 to 99. The default value is 90. **Terminology reference:** **Web interface**: Initiate renewal on % of Validity Interval **Phone UI**: Not configurable
<PASSWORD>	To specify the SCEP system password. The default is the phone's serial number. **Terminology reference:** **Web interface**: Password **Phone UI**: Not configurable
<SCEP_ENTITY_CLASS>	To identify the entity class for which the SCEP server generates the identity certificates. **Terminology reference:** **Web interface**: Entity Class **Phone UI**: Not configurable
<SCEPENCALG>	To specify the SCEP encryption algorithm. If the value is 0, then SCEP operates using the DES encryption. If the value is 1, then SCEP operates using the AES-256 encryption. If you put any other value than 0 or 1, or skip the parameter, then SCEP also operates using the DES encryption. **Terminology reference:** **Web interface**: Encryption Algorithm **Phone UI**: Not configurable

Table continues…

XML parameter name	Description
<httpd>	The top line of http daemon section.
<enable>	To enable the Web Admin access to access the phone through the web interface. The options are the following: • True. This is the default setting. • False. **Terminology reference:** **Web interface**: Enable **Phone UI**: Web Access
<min_allowed_tls_version>	To define the minimum allowed TLS version which the web server uses for Web Admin capability. The default setting is 1.2. The options are the following: • all. This allows TLS 1.0 and TLS 1.1 connections. • 1.2. This is the default setting. **Important:** This parameter is only available in the .xml configuration file.

Input validation and data type restrictions

The user's input validation takes place during the configuration of the settings on the phone, through the web interface, and by using the configuration file.

When the user tries to input invalid data on the phone or through the web interface, the phone does not accept or save the changed settings.

When the user tries to input invalid data during the configuration file import using the web interface or automatic provisioning of the phone, the server does not accept or save the invalid input. Avaya Conference Phone B199 does not accept configuration of the settings when:

- The user tries to import a file with invalid content for its type using the web interface or automatic provisioning.
- The user tries to import a large file using the web interface or automatic provisioning.

Input Data Type and Length Restrictions

Avaya Conference Phone B199 provides input data type and length validation. All validation rules take a stand on the existing requirements. For example, if the data input is a URL, validation rules are based on RFC for URLs.

When the user inputs data that do not meet the requirements, the system highlights the fields with the invalid data. The phone and the web server do not accept or process any data that does not meet the defined data type and length requirements.

If you input valid data, the phone reboots and applies the new configuration.

You can find the specific requirements and rules for valid data input in the settings description sections.

Related links

Configuration parameters on page 39

Phone settings

The Avaya Conference Phone B199 phone settings include the following:

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

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

Related links

Configuration parameters on page 39

Rebooting the phone

About this task

Use this procedure to reboot your Avaya Conference Phone B199 using the user interface of the phone. Here you can reboot the phone without making additional power cycles.

You can reboot Avaya Conference Phone B199 from the user interface of the phone only if you log in as the administrator.

You can also reboot the phone from the web user interface.

Procedure

1. On the phone screen, tap **Settings** > **Admin Login** > **Phone**.
2. Tap **Reboot**.

   The phone shows the following pop-up message: `Reboot the phone. Press OK to confirm` for 2 minutes and then hides it.
3. To confirm the reboot, tap **Ok**.

   The phone starts the reboot process and shows the following message: `Rebooting phone`.
4. **(Optional)** To return to the **Phone** settings, tap **Cancel**.

Related links

Configuration parameters on page 39

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**.

Related links

Configuration parameters on page 39

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.

Related links

Configuration parameters on page 39

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.

When DHCP includes option 42 providing a valid NTP server address, Avaya Conference Phone B199 uses this value even if you configure the NTP server in the .xml configuration file. When the DHCP option 42 does not provide an NTP server address, the value from the configuration file becomes applicable.

Related links

DHCP configuration options on page 28
Configuration parameters on page 39

Sleep mode

B199 Conference Phone supports Sleep mode feature, which saves power by turning the screen off after a specified period of inactivity. By default, Sleep mode is in disabled state.

The phone administrator can enable Sleep mode and configure the time-out value.

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

- Touch the screen
- Connect or disconnect the USB cable
- Connect or disconnect the Bluetooth® Classic

The phone also wakes up from Sleep mode during screen activity, such as an incoming call, Avaya® Conference Assistant connection, or error prompts.

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

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

Related links

Configuration parameters on page 39

Media settings

The Avaya Conference Phone B199 media settings include the following:

- Security
- Audio codecs
- Voice Quality Monitor
- Advanced settings including the media ports range.

Related links

Configuration parameters on page 39

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

Related links

Configuration parameters on page 39

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.

Related links

Configuration parameters on page 39

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 **Arrow Left** 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 114
Device Management on page 121
Configuration parameters on page 39

Configuration of the media port range

When the Avaya Conference Phone B199 system operates, it assigns two media ports - RTP and RTCP - to each session. The phone uses the media port values from the specified media port range. To configure this parameter, you must enter the **First Media Port** and the **Last Media Port** values. The acceptable values are the following:

- For **First Media Port**: from 2048 to 65528.
- For **Last Media Port**: from 2055 to 65535.

When you specify the values for the first and the last media ports, the phone uses two consecutive unoccupied ports from this media port range: RTP port to transfer audio signal and RTCP to send statistic data. For each new call the device applies the next two ports, even if you end the previous session and its ports become available. B199 uses the ports this way until it reaches the last port within the configured media port range, and then it switches to the first port. For example, if you set the **First Media Port** parameter to 4000 and the **Last Media Port** to 4007, Avaya Conference Phone B199 uses the following port pairs: 4000 for RTP and 4001 for RTCP, 4002 for RTP and 4003 for RTCP, and further.

For successful configuration, the media port range must be at least 8 as this is the number of ports B199 uses for a conference call with the maximum allowed number of participants. If it is less than 8, the phone shows the following error message: `There should be at least 8`

`media ports in total`. As a result, the device does not accept the configuration and uses the following default values:

- First Media Port: `4000`.
- Last Media Port: `65535`.

As the phone always uses two ports, it prefers to have an even media port range to correctly form port pairs. Thus, if the check shows that the number is odd, B199 shows the following warning message: `Number of media ports is expected to be even`. Here, the device ignores the last value of the range to make the number of media ports even.

You must take into consideration that, unlike B199, some implementations do not follow RFC 3605 and do not recognize when the peer specifies its RTCP port separately. If such an implementation receives an odd RTP port number from your conference device, it follows the RFC 3550 rule to change the RTP port to the next lower even number, and this results in the loss of RTP. Thus, you must account for this possibility of a session failure if you enter an odd **First Media Port** number. If so, the phone warns you with the following message: `First Media Port is expected to be an even number`. Nevertheless, the device accepts an odd RTP port value and continues its operation.

Note:

There is no dependencies check for the media port range during the .xml configuration file import.

When you specify the media port range correctly, Avaya Conference Phone B199 accepts it and restarts to apply changes.

You can configure the Media Port Range parameter on the phone, through the web interface, by importing the .xml configuration file, or through auto-provisioning.

Related links

Configuration parameters on page 39

Configuring the media port range on the phone

About this task

Use this procedure to configure the media port range on your Avaya Conference Phone B199.

Procedure

1. Log in as administrator.
2. In the **Settings** menu, tap **Media** > **Advanced**.
3. Set the **First Media Port** parameter.
4. Set the **Last Media Port** parameter.
5. Tap the **Arrow Left** icon three times to return to the home screen.

   If the parameters values are valid, the phone restarts to apply changes.

Related links

Configuration parameters on page 39

Configuring the media port range through the web interface

About this task

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

Procedure

1. Log in as administrator.
2. Navigate to **Media** > **Advanced**.
3. Set the **First Media Port** parameter.
4. Set the **Last Media Port** parameter.
5. Click **Save**.

   If the parameters values are valid, the phone restarts to apply changes.

Related links

Configuration parameters on page 39

SIP settings

The Avaya Conference Phone B199 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

Important:

If you do not configure the SIP account for B199 Conference Phone, the phone operates in USB only user mode.

Related links

Configuration parameters on page 39

SIP account registration status

SIP account is a specifically configured set of credentials that provides access to SIP telephony and allows users to make calls from the phone. The SIP settings on B199 Conference Phone provide for configuring the primary account, the secondary account, and the fallback account.

If the phone has several configured SIP accounts, but there is only one registered account, the phone displays the name of the registered account on its idle home screen.

You can tell if the phone has a configured and registered SIP account or problems with the SIP account registration by looking at its home screen. The following options are available:

- The phone has no SIP account configured. B199 Conference Phone displays the phone name, the Bluetooth and Settings buttons on its idle home screen. The phone does not display the account name.
- The phone has the SIP account configured but not registered. For example, this can be due to invalid credentials of the SIP account or network problems. B199 Conference Phone displays the Warning icon, the account name, the Recent, Call, Conference Assistant, and Settings buttons on its idle home screen. When you tap the account name or the Warning icon, the phone displays the following pop-up message: `No sip service registered (Wrong username/password or registrar?)`. It disappears automatically after a certain timeout, or you can tap **Ok** to return to the home screen.
- The phone has the SIP account configured and registered. The phone displays the phone name, the account name, the Recent, Call, Conference Assistant, and Settings buttons on the idle home screen.

You can use B199 Conference Phone via USB regardless of the SIP account registration status. When the phone has no SIP account configured or registered, it acts as a speakerphone that you can use to conduct virtual meetings and listen to audio files.

Related links

Configuration parameters on page 39

Caller information presentation

B199 Conference Phone displays the calling person information to show who is calling or display 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's SIP invite message. It includes the following:

- CNAM: Usually specifies the contact name.
- CID: Usually specifies the caller's 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 screen information, which B199 Conference Phone displays, depending on the parameters the server provides:

Screen	Description
Incoming Call	Avaya Conference Phone B199 displays the CNAM and the CID. If the server does not provide the CID, the phone displays the CNAM. If the server does not provide the CNAM or 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 the CNAM or 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`. **Note:** When the administrator disables the Call Log functionality, the Recent Call List becomes unavailable.

Related links

Configuration parameters on page 39

Configuring the Use Static Source Port setting

About this task

Use this procedure to configure the Use Static Source Port setting through the web interface or on the phone.

- To configure the Use Static Source Port setting through the web interface, do the following:
  1. Log in as the administrator.
  2. On the web interface, navigate to **SIP** > **Advanced**.
  3. Enable **Use Static Source Port**.
  4. **(Optional)** Disable **Use Static Source Port**.
- To configure the Use Static Source Port setting on the phone, do the following:
  1. Log in as the administrator.
  2. Tap **SIP** > **Advanced**.
  3. Enable **Use Static Source Port**.
  4. **(Optional)** Disable **Use Static Source Port**.

When you change the Use Static Source Port value though the web interface or on the phone, the value in the configuration file changes accordingly.

Related links

Configuration parameters on page 39

Hostname to IP address mapping

Avaya Conference Phone B199 supports hostname to IP address mapping to resolve configured IP address from hostnames. In case you do not have a DNS server configured, you can manually map a hostname to the IP address using the configuration file.

You can configure host entities for the following services:

- NTP server
- RTCP XR Collector URI
- LDAP server
- SIP Registrar
- SIP Proxy
- STUN server
- TURN server
- Device Enrollment Services server
- Provisioning server
- SCEP server
- Syslog server

Note:

If you use a Fully Qualified Domain Name (FQDN) in the SIP Registrar field for the Primary, Secondary or Fallback SIP account, the SIP URI contains the configured FQDN instead of the IP address of the SIP Registrar.

If you plan to use a fictional SIP Registrar hostname, you must add it to the SIP server for its subsequent identification in SIP URI. SIP server checks if the received hostname from SIP URI matches the hostname configured on the server. If the hostnames do not match, the SIP server rejects the configuration with the following error code: `code 403, Forbidden`.

SNI support

Avaya Conference Phone B199 supports using the Server Name Indication (SNI) extension for TLS connections to a SIP server.

There are setups when several customers share one physical SIP server. The customers get unique domain names, which resolve to the same IP address. When the phone attempts to connect to one of these domain names via TLS, it needs to specify the exact FQDN for connection for the SIP server to present the corresponding TLS certificate. Here, the SNI extension serves as the means for FQDN specification.

When the phone starts a TLS connection with the SIP server, it sends a request with an extension that specifies the required hostname. The SIP server responds with a certificate containing the requested FQDN for B199 to verify. If the received data matches the requested FQDN, the phone proceeds with the TLS connection. Otherwise, the phone terminates the TLS connection.

Related links

Configuration parameters on page 39

Configuring the SNI setting

About this task

Use this procedure to configure the Server Name Indication (SNI) setting on the phone or through the web interface.

You can also use the configuration file to enable or disable the SNI parameter.

Before you begin

Ensure that your phone uses TLS as the transport protocol.

- To enable the SNI setting on the phone, do the following:
  1. Log in as the administrator.
  2. On the phone screen, tap **Settings** > **SIP** > **TLS**.
  3. Enable **SNI**.
  4. Tap the **Arrow Left** icon three times to return to the home screen.

     The phone restarts the application to apply the changes.
- To enable the SNI setting through the web interface, do the following:
  1. Log in to the web interface.
  2. Click **SIP**.
  3. In the TLS section, enable **SNI**.
  4. Click **Save**.

     The phone restarts the application to apply the changes.

  When you configure the SNI setting through the web interface or phone, the value in the configuration file changes accordingly.

Related links

Configuration parameters on page 39

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

Important:

When you type in values (text-based input), do not use the following characters: *!@#$%^?/\-_*.

Related links

Configuration parameters on page 39

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

Related links

Configuration parameters on page 39

DNS mapping

If Avaya Conference Phone B199 operates in an environment with no DNS available or the DNS server has no connectivity, you can configure settings to pass the device FQDN-to-IP mapping information. The phone stores and retains these parameters persistently, and a DNS failure does not impact the B199 operation.

Avaya Conference Phone B199 considers the configured host table part of its active configuration. When the phone boots up or performs a Device Management polling, it first searches for the DNS server configuration. If host entries change, the phone updates the host table with the new values. When the phone receives new settings for the host entities, it reboots to apply the changes.

To configure the host table, you must use the .xml configuration file. It contains the `<hosts_map>` parameter, which has the following two elements for each host entity:

- `<ip>`. This is the IP address of the server.
- `<name>`. This is the hostname, that you assign to the host entity. After the phone reboots and applies the configuration, you can specify this value in any FQDN data field in the web interface. For example, in the Registrar field of a SIP account.

You can add several host entities or leave the parameter empty.

Note:

If the parameter stays blank or is not available in the .xml configuration file, the phone deletes all existing FQDN-to-IP mapping settings.

The following is an example of the configured `<hosts_map>` parameter.

```
<hosts_map type="xml">
            <host>
                <ip>192.168.1.101</ip>
                <name>sipserver1.com</name>
            </host>
            <host>
                <ip>192.168.1.102</ip>
                <name>sipserver2.com</name>
            </host>
            <host>
                <ip>192.168.1.103</ip>
                <name>sipserver3.com</name>
            </host>
</hosts_map>
```

Along with configuring the hostname and IP address on your Avaya Conference Phone B199, you must add the same host entry values into the SIP server configuration. During SIP operation, SIP URI uses the specified Registrar parameter value, which contains the hostname from the configured host entity. SIP server checks if it knows the hostname and IP address it receives in SIP URI. When the values do not match the parameters of the server, it does not resolve the hostname to the IP address and responds with an error message.

Chapter 5: Call server administration

Avaya Aura® administration

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 real-time, 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.

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.

Messaging the proxy without adding a record route

About this task

In the SIP peer communication, Avaya Conference Phone B199 adds a record route to registration or any other message to the proxy. This appending indicates another device in the SIP path. If you want your conference phone not to send this message and correctly register in the Avaya Aura® environment, you must configure the SIP settings for the device in a special way.

Before you begin

Ensure that your B199 has the following settings for its Avaya Aura® deployment:

Domain: `name.com`
Registrar: `sip.name.com`
User Name: `user@name.com`

Procedure

1. Log in to the web interface.
2. On the Navigation pane, click the **SIP** tab.
3. Configure the parameters as follows:

   Registrar: `name.com`
   Proxy: `sip.name.com;hide`

Appending the `;hide` parameter results in messaging the proxy without a record route added.

4. **(Optional)** To control the inbound calls, configure **Realm** as follows:

   Realm: `name.com`

   You can also configure the SIP settings on the phone.

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.

If Avaya Conference Phone B199 receives a check-sync NOTIFY event in Idle Mode, it automatically starts the Device Management procedure, which includes downloading the firmware file. The phone is in 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 call ends 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 reboots regardless of any available firmware upgrades or new configuration files. 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 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.

IP Office provides an option for HTTP redirection if the requested firmware is too big to accommodate. In response to your request for firmware IP Office sends the phone a redirection response. It includes a path to the server hosting the firmware. B199 Conference Phone follows the redirection to obtain the firmware.

Avaya Conference Phone B199 in IP Office also receives check-sync events from your SIP server for the settings file changes. IP Office does not support check-sync for firmware upgrades.

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

Chapter 6: Bluetooth and USB connection

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 143. 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.

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.

In USB only user mode, the phone supports connection to Bluetooth® devices using Bluetooth® Classic.

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 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.

When you end a successful Bluetooth® Classic connection, B199 Conference Phone restores Bluetooth® LE mode.

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 connected to it, the phone acts as a speakerphone. You can use the phone to handle Bluetooth® calls. B199 Conference Phone synchronizes the volume level with that 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 connected to it, B199 Conference Phone acts as an audio receiver. You can use the phone to stream multimedia audio from the Bluetooth® device. The volume level of the streamed audio does not change. B199 Conference Phone keeps the volume level it had before it started playing audio. When B199 Conference Phone is in Idle mode, and you start A2DP streaming from the connected Bluetooth® device, the LEDs on the phone remain turned off. **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

Configuration parameters on page 39

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 35
Setting the password for Avaya Conference Phone B199 on page 25

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 from the paired Bluetooth® device.

Automatic reconnection to a Bluetooth device

You can use a Bluetooth® USB dongle to connect your Avaya One Cable Connect (OCC) Hub or computer to B199. When the conference phone loses power, it needs time to boot up. During this period, it has no connection to the Bluetooth® device. When B199 enters Idle mode after reboot, it automatically tries to reconnect to the last paired Bluetooth® device. If the reconnection fails, B199 tries to reconnect in 30 seconds. If the device does not respond, the phone stops the reconnection attempts.

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 106

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

Bluetooth® connection on page 106
Importing the configuration file on page 115

USB only user mode

Avaya Conference Phone B199 supports USB only user mode. With this feature, the conference phone can operate with no SIP account and SIP register configured. In USB only user mode B199 acts as a speakerphone that the user can use to conduct virtual meetings and listen to audio files.

USB and Bluetooth® connection

In USB only user mode, the phone operates as a USB device connected to a USB host.

In this mode, the phone supports connection to Bluetooth® devices using Bluetooth® Classic.

Note:

The administrator can use the configuration file to disable Bluetooth®. The **Bluetooth** button becomes inactive, and if the user taps it, the phone shows the following message: `Bluetooth is disabled by the administrator.`

When idle, B199 does not display **Account Name** on the home screen in USB only user mode. The user can see the phone name and the connection option as follows:

- When the user connects the phone using USB, B199 indicates `USB audio` on the home screen.
- When the user uses Bluetooth® to connect the phone, B199 indicates `Bluetooth® audio` on the home screen.
- When the user uses both Bluetooth® and USB for connection, B199 indicates `Bluetooth® audio` on the home screen.

Related links

Provision of the NTP server address on page 87
Firmware upgrade and downgrade on page 114

Time presentation in USB only user mode

When the phone has NTP server settings enabled but it cannot connect to the NTP server in USB only user mode, B199 does not display time on the home screen and in the settings menu.

When the phone has NTP server settings disabled, the user can set the time manually. Then the options of the time presentation are the following:

- On the home screen when there is no active Bluetooth® or USB connection.
- On the status bar when the user connects to B199 using Bluetooth® or USB.

USB only user mode icons

The following table shows the icons on the home screen of Avaya Conference Phone B199 in USB only user mode:

Icon	Name	Description
	USB Connected	To indicate an active USB connection. The phone displays the USB Connected icon and shows `USB audio` on the idle home screen.
	Bluetooth connection	To configure Bluetooth® Classic settings and to indicate an active Bluetooth® Classic connection. The phone shows the Bluetooth connection icon and `Bluetooth® audio` indication on the idle home screen. **Note:** If the administrator uses the .xml configuration file to disable Bluetooth®, then the **Bluetooth connection** icon is inactive.
	Settings	To check and configure the settings from the phone. View the phone status and reach the menu. The following settings are available in USB only user mode: • Status • Phone • Avaya® Conference Assistant • Bluetooth • Admin Login

Note:

When Avaya Conference Phone B199 shows the USB Connected or the Bluetooth connection icon on the idle home screen, the phone displays time on the status bar.

Volume control and synchronization

Volume level indication

Avaya Conference Phone B199 provides the following volume levels: Level 0 to Level 12. Here, Level 0 is volume off, and Level 12 is the loudest volume level. You can turn the volume down to Level 0 only when the phone is connected to a USB host. Here, the phone displays the Volume Off icon and the audio on the phone is muted.

When you start a call, the phone automatically sets the volume to Level 10. During an active call, to manually increase the volume up to Level 12, tap the **Volume Up** or **Volume Down** icons. The phone shows the volume bar on the screen to reflect the volume change.

If you set the volume lower than Level 10, the next call starts with this new level. If you increase the volume to Level 11 or Level 12, the phone automatically decreases the volume to Level 10 for the next call.

Note:

The phone does not show the volume bar when it automatically sets the volume to Level 10 for a call.

Volume synchronization with USB host

When you connect Avaya Conference Phone B199 to the USB host and select it as an audio device, the phone synchronizes its volume level with the connected USB host.

Avaya Conference Phone B199 also synchronizes the volume level with the USB host when it switches between Playback and Call mode. If you receive a call during audio playback, the phone automatically changes the volume level for the call. The phone synchronizes the volume with the USB host and applies the Call mode volume. When the call ends, the phone changes the volume back to the Playback mode volume.

Note:

Avaya Conference Phone B199 supports volume synchronization if the USB host has Windows 10 as its operating system.

You can adjust the volume level either on the phone or on the connected USB host. When you set the maximum or the minimum volume level, the USB host responds as follows:

- If you decrease the phone volume to the lowest level, the volume on the USB host turns off.
- If you increase the phone volume to the highest level, the volume on the USB host changes to 100. This is the highest level for the USB host permitted.

Volume synchronization in Daisy chain mode

If you adjust the volume on the USB host for B199 Conference Phone acting as the main phone in a Daisy chain, the volume on the expansion phone changes accordingly. The expansion phone reflects the change showing the volume bar on the screen.

If you change the volume level on Avaya Conference Phone B199 acting as an expansion phone in a Daisy chain, the volume on the main phone and the USB host changes accordingly.

Note:

If you turn the volume down to the lowest level, the Primary and Secondary phones display the **Volume Off** icon.

Related links

Expansion of the phone coverage on page 148
Icons on page 19

USB ports configuration

You can enable or disable the USB ports of your Avaya Conference Phone B199. When the USB ports on the phone are enabled, you can use the USB audio port for audio transmission and the USB upgrade port for a device upgrade.

To configure this parameter, you can insert the required value in the `<usb> - <enable>` section of the configuration file as follows:

- `True` to enable the USB ports. This is the default setting.
- `False` to disable the USB ports.

Note:

The power supply does not switch off when you disable the USB ports.

Chapter 7: Firmware upgrade and downgrade

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 web administration interface, automatically through DES or a centralized file server. The firmware files are available at support.avaya.com. The phone application installs the firmware whenever the firmware version in the downloaded firmware file differs from the version of the currently running firmware.

You must select the file to upgrade the firmware on your device. The filename ends with `.kt`, for example, `firmware-1.0.6.1.0-release.kt`. With the firmware selected, Avaya Conference Phone B199 immediately starts the installation process. It performs the firmware upgrade file validation to ensure absence of corrupted data as well as that the firmware version is higher than the current one. If the firmware version is higher than the running version (it is an upgrade), the phone imports the configuration in full. Starting from Release 1.0.7, if the firmware version is older than the running version (it is a downgrade), B199 retains some of the configured parameters including the administrator password.

Note:

A downgrade to the firmware version lower than 1.0.1.0.2 causes a factory reset and sets all user settings, configurations, and data to factory default.

Exporting the configuration file

About this task

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

When you exporting the running configuration, the resulting .xml file contains the following:

- All configured non-default values.
- Lines with the commented out passwords.

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.

Editing the configuration file

About this task

Use this procedure to edit the exported configuration file.

Before you begin

To edit the configuration file, install a source-code editor that supports the import and export of .xml files. To verify the syntax and content of a .xml file, choose an editor that also supports .xsd files.

Procedure

1. Open the configuration file using a suitable editor.
2. Locate the parameter to change and type the required value.

   For example, to specify the name of a SIP account, in the SIP section, locate the `<name type="string"></name>` line and type the account name: `<name type="string">Westview</name>`.
3. **(Optional)** To add a comment, enter your text below the first line.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Acme Widgets Avaya B199 config file for Westview Conference Room Created Nov
2021-->
<B199 version="6">
```

4. Click **Save** to save the modified file with the required file name.

   To deploy the configuration file through a centralized management server, change the default file name to `avayab199.xml` or `avayab199-<MAC>.xml`.

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.

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 34

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 importing a configuration file from a newer version of firmware. The .xml configuration file version must be the same or lower than the firmware version.

Firmware release	XML file index No.
1.0.0 and Maintenance releases (MRs)	0
1.0.1 and MRs	1
1.0.2	2
1.0.3	3
1.0.4	4
1.0.5	5
1.0.6	6
1.0.7	7
1.0.8	8

Note:

You can add and delete .xml branches and move parameters within the configuration file structure. The default .xml files are available on support.avaya.com.

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`.

Firmware upgrade and downgrade using a USB mass storage device

Avaya Conference Phone B199 uses the USB mass storage device to support firmware upgrade and downgrade without the web interface. For that, the USB parameter must be enabled in the configuration file. If you have the USB parameter disabled, USB is inaccessible and unavailable for upgrade or downgrade.

When you connect the USB mass storage device to Avaya Conference Phone B199, the phone starts auto-mounting and finds the firmware file stored on the USB mass storage device. The auto-mounting and parsing process takes up to 30 seconds depending on your flash drive.

Before performing upgrade or downgrade, the phone does not compare the firmware version on the USB mass storage device and the currently used firmware version.

If the firmware file is invalid, the phone shows the following message: `Invalid upgrade file`.

Note:

The phone starts the upgrade or downgrade procedure immediately if it is in Idle Mode. Otherwise, Avaya Conference Phone B199 ends an active operation and then starts the upgrade process.

It is impossible to make calls or enter any menu on the phone during the upgrade.

Avaya Conference Phone B199 blocks the upgrade procedure using the USB mass storage device, if the phone already starts the upgrading procedure using the Device Management provisioning server.

The phone supports several USB flash drive file systems including FAT32 and NTFS.

Note:

Avaya Conference Phone B199 supports only one partition USB flash drives for the upgrade.

If you set **Admin Password** in **Settings** > **Phone**, enter a valid administrator password before the phone starts the upgrade procedure.

Note:

You can upgrade or downgrade the out-of-the-box Avaya Conference Phone B199 during the initial boot if you connect the USB mass storage device to the phone and follow the upgrade procedure.

Upgrading firmware using a USB mass storage device without the administrator password

About this task

Use this procedure to upgrade or downgrade your Avaya Conference Phone B199 using a USB mass storage device if you have no administrator password set.

Before you begin

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

- Upload the firmware file from your personal computer to the USB mass storage device root folder. The file name must be `upgrade.kt`.
- Make sure Avaya Conference Phone B199 is in Idle Mode.

Procedure

1. Connect the USB mass storage device to Avaya Conference Phone B199 USB port.

   When checking for the appropriate firmware upgrade file, the phone shows the following message: `Checking upgrade file`. Then the phone displays the following message: `Firmware version x.x.x.x.x found on USB. Upgrade now?`, where `x.x.x.x.x` is the version of the valid firmware file.

2. Tap **Yes** to proceed with the upgrade.

   The phone starts the upgrade procedure, showing the following message: `Upgrade in progress, please wait`. When the upgrade procedure ends, the phone reboots to apply the changes.

3. **(Optional)** Tap **No** to discontinue the upgrade.

   If you tap **No** accidentally, to restart the procedure, reconnect a USB mass storage device to Avaya Conference Phone B199 USB port.

Related links

Uploading a firmware file on page 116

Upgrading the firmware using a USB mass storage device with the administrator password

About this task

Use this procedure to upgrade or downgrade your Avaya Conference Phone B199 using a USB mass storage device if you have an administrator password set.

Before you begin

- Download the appropriate firmware file from http://support.avaya.com/ and save it in a specified location on your personal computer.
- Upload the firmware file from your personal computer to the USB mass storage device root folder. The file name must be `upgrade.kt`.
- Make sure Avaya Conference Phone B199 is in Idle Mode.

Procedure

1. Connect a USB mass storage device to Avaya Conference Phone B199 USB port.

   While checking for the appropriate firmware upgrade file, the phone shows the following message: `Checking upgrade file`. Then the phone displays the following message: `Firmware version x.x.x.x.x found on USB. Upgrade now?`, where `x.x.x.x.x` is the version of the valid firmware file.

2. Tap **Yes** to proceed with the upgrade.

The phone displays the **Admin Password** popup.

3. In the **Admin Password** field, type the administrator password.
4. **(Optional)** If you enter an incorrect administrator password, the phone displays the following message: `Invalid password`. Do the following:
   a. Tap **Ok**.
   b. Type the correct administrator password.
5. Tap **Upgrade**.

   The phone starts the upgrade procedure, showing the following message: `Upgrade in progress, please wait`. When the upgrade procedure ends, the phone reboots to apply the changes.
6. **(Optional)** Tap **Cancel** to discontinue.

   If you tap **Cancel** accidentally, to restart the procedure, reconnect a USB mass storage device to Avaya Conference Phone B199 USB port.

Related links

Uploading a firmware file on page 116

Firmware downgrade with DES provisioning

To initiate a downgrade, you can upload an older firmware than currently available on the DES server. Here, DES provisioning starts automatically. Avaya Conference Phone B199 applies the received configuration and restarts with the downloaded settings.

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

You can also initiate 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. Consequently, disable the DES in the phone settings and reboot the device.

Related links

Factory reset on page 161

Configuration retention after downgrade

When you downgrade the firmware of your Avaya Conference Phone B199, the phone retains some of the configured parameters. The phone keeps configuration for the following:

- DHCP. B199 keeps the previously configured DHCP option value if you downgrade the firmware.
- Static IP Address

- Static IP Gateway
- Static IP Network mask
- DNS
- VLAN
- Administrator password
- Provisioning address
- Provisioning certificates. This can be a DES-provided client certificate.
- NTP
- DES

Note:

The phone does not save the configured parameters if you downgrade the firmware to a version lower than 1.0.1.0.2. The downgrade causes a factory reset and sets all user settings, configurations, and data to factory default.

Device Management

Avaya Conference Phone B199 provides the Device Management feature to facilitate upgrade and configuration of multiple conference phones. When enabled and configured correctly, Device Management obtains firmware and configuration automatically by polling the centralized server on a defined basis. 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.

Configure the Device Management feature in line with the description in Configuration parameters on page 39. By default, Device Management is enabled.

Files on the provisioning server

The following files must be available on the provisioning server:

- Firmware file (filename ends in `.kt`)
- Firmware metadata file (as provided in the Avaya Firmware bundle)
- 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
Global configuration file	If available, the device obtains the global configuration file `avayab199.xml` and parses it. During the Device Management update all parameters from the file are loaded into the Avaya Conference Phone B199 running configuration.
Device-specific configuration file	If the device-specific configuration file `avayab199-<MAC>.xml` is available on the provisioning server, the phone downloads and parses it. The parameters from this file overwrite the parameters set by the global configuration file.
Global certificate configuration file	If available, the device obtains the global certificate configuration file and uses it for its operations. The certificates the phone downloads from the provisioning server overwrite any certificates you downloaded manually using the phone web interface.
Device-specific certificate configuration file	The device-specific certificate configuration file has priority over the global certificate configuration file. All its parameters overwrite the parameters loaded by the global certificate configuration file.

Important:

After Avaya Conference Phone B199 obtains the configuration from the provisioning server, parses it, adds and saves the parameters in a local configuration file, all changes you make using the web interface or the phone UI replace the parameters stored as the current running configuration. To clear a manually set parameter, the administrator must first provide a configuration file with the parameter having no value assigned to it, and then push a configuration that contains the new parameter.

Related links

Certificates on page 126
Avaya Conference Phone B199 .xml configuration files on page 30

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.

Note that you must have separate `avayab199-<MAC>.xml` configuration files for each Avaya Conference Phone B199. Here, `<MAC>` is the MAC address of a specific phone.

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.

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

Device Management on page 121

Chapter 8: Security and protection

Security methods and protocols

Avaya Conference Phone B199 supports a number of security methods and protocols to protect the integrity of its configuration and operation.

802.1X Ethernet Authentication

With 802.1X Ethernet authentication enabled, B199 must authenticate as a recognized device before getting an authorization to communicate on the network.

You can secure the 802.1X Ethernet authentication process by configuring one of the following options:

- **EAP TLS**. The device uses the applicable TLS version to communicate with the 802/1X authentication server. You can manually install TLS certificates can on B199 by using the web administration interface or the certificates .xml file.
- **EAP MD5**. The device uses the MD5 method to communicate with the 802/1X authentication server. You must enable **Legacy Encryption** to use **EAP MD5**.

It is possible to configure both TLS and MD5, and then the authentication server (RADIUS server) selects the protocol to use.

FIPS

Enabling the Federal Information Processing Standards (FIPS) results in the use of an enhanced suite of encryption algorithms as well as supporting timers and processes to meet the FIPS 140-2 requirements. With FIPS enabled, you can not have the Legacy Encryption methods enabled at the same time.

TLS

The device uses Transport Layer Security (TLS) protocols for SIP authentication, HTTPS connectivity for the centralized file server, and LDAP authentication and communication. The following TLS protocols are available:

- **SIP-TLS** to secure the communications with the SIP Registrar.
- **LDAP-TLS** to secure the communications with the LDAP server. The device uses this protocol by default.

You can manually install TLS certificates can on B199 by using the web administration interface or the certificates .xml file.

Certificates

There are several factory-installed security certificates on the Avaya Conference Phone B199. You can install additional certificates through the centralized configuration server, Device Enrollment Services, SCEP or manually through the web interface.

Pre-installed certificates

Avaya Conference Phone B199 has a factory-installed device specific private key. You cannot view or delete this private certificate. You can use this certificate to authenticate with the Device Enrollment Services server.

Installable certificates

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 the global configuration file is `avayab199_certcfg.xml`. The default name for the 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 four sections:

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

Note:

There is no requirement to populate all four sections in the .xml file. Insert the data only to the sections used.

Each section includes the following certificate files:

- CA certificate
- Device certificate
- Device private key.

Each section contains the path details for the 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 as 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 a SHA256 or an MD5 checksum for each element in it. This checksum (also called SHA256 hash algorithm or MD5 hash algorithm) is a type of digests of the specified certificates.

Important:

Avaya Conference Phone B199 uses MD5 checksum only when **Allow Legacy Encryption** is enabled. In this case, both SHA256 and MD5 hash algorithms are supported. When **Allow Legacy Encryption** is disabled, Avaya Conference Phone B199 supports only SHA256 hash algorithm. Then the phone does not use MD5 as the checksum for certificates if it downloads and stores them during provisioning.

When you have the Device Management enabled or after the restart, the phone starts downloading the certificate if the hash algorithm value is different from the one of the certificate file that Avaya Conference Phone B199 stores. That means that the phone downloads one certificate file only once and subsequently checks that the certificate file is still the same.

Related links

Legacy encryption mode on page 136

Certificate configuration file structure

The following table 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 the 802.1x path to check the CA certificate.
`<ca_hash algo="SHA256">`	To specify the SHA256 hash algorithm that the phone uses to verify the 802.1x CA certificate.
`<cert_uri>`	To specify the 802.1x path to get the device certificate.
`<cert_uri format>`	To specify the file format. You can add a file in .p12 or .PEM format.

Table continues…

String	Description
<cert_hash algo="SHA256">	To specify the SHA256 hash algorithm that the phone uses to verify the 802.1x device certificate.
<privkey_uri>	To specify the 802.1x path to get the private key.
<privkey_hash algo="SHA256">	To specify the SHA256 hash algorithm that the phone uses to verify the 802.1x private key.
<cert_pkcs12_password>	To specify password for the PKCS12 file.
<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="SHA256">	To specify the SHA256 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_uri format>	To specify the file format. You can add a file in .p12 or .PEM format.
<cert_hash algo="SHA256">	To specify the SHA256 hash algorithm that the phone uses to verify the device certificate for the SIP connection.
<privkey_uri>	To specify the path to get the private key for the SIP connection.
<privkey_hash algo="SHA256">	To specify the SHA256 hash algorithm that the phone uses to verify the private key for the SIP connection.
<cert_pkcs12_password>	To specify password for the PKCS12 file.
<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="SHA256">	To specify the SHA256 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_uri format>	To specify the file format. You can add a file in .p12 or .PEM format.
<cert_hash algo="SHA256">	To specify the SHA256 hash algorithm that the phone uses to verify the device certificate for connection to the provisioning server.

Table continues…

String	Description
<privkey_uri>	To specify the path to get the private key for connection to the provisioning server.
<privkey_hash algo="SHA256">	To specify the SHA256 hash algorithm that the phone uses to verify the private key for connection to the provisioning server.
<cert_pkcs12_password>	To specify password for the PKCS12 file.
<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="SHA256">	To specify the SHA256 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_uri format>	To specify the file format. You can add a file in .p12 or .PEM format.
<cert_hash algo="SHA256">	To specify the SHA256 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="SHA256">	To specify the SHA256 hash algorithm that the phone uses to verify the private key for connection to the LDAP server.
<cert_pkcs12_password>	To specify password for the PKCS12 file.

The following is an 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="SHA256">c49d8fd0cbb6bfc26ef752296d6d17f7</ca_hash>
           <cert_uri>8021x_dev.crt</cert_uri>
           <cert_hash algo="SHA256">ca059972d02b2853a92704a7a7640f3f</cert_hash>
           <privkey_uri>8021x_priv.key</privkey_uri>
           <privkey_hash algo="SHA256">f4728d6356204c6fcce91989ef733553</privkey_hash>
       </ether_8021x>
       <provisioning>
           <ca_uri>prov_ca.crt</ca_uri>
           <ca_hash algo="SHA256">e5116932d3685ea18ead10a55b825145</ca_hash>
       </provisioning>
   </certificates>
```

Note:

With Allow Legacy Encryption enabled, the certificate configuration file can contain MD5 and SHA256. If you disable Allow Legacy Encryption, then only the SHA256 hash algorithm is supported.

Related links

Legacy encryption mode on page 136

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

Certificates on page 126

Downloading the root certificate

About this task

The administrator must obtain a root certificate from a Certificate Authority (CA). This CA certificate has the key size of 2048, is in PKCS10 format and is generated using SHA-1 hash algorithm.

Use this procedure to download the Microsoft generated 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**.

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.

Before you begin

Ensure that you have OpenSSL installed on your computer. If you don't have it, you can download this toolkit from the OpenSSL Project web page and install on Windows OS or MAC OS.

Procedure

1. Run OpenSSL.
2. 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
      ```
3. On the web interface, browse to the .PEM files to use TLS mode of authentication.

Certificates management

In the web interface of your Avaya Conference Phone B199, you can view the information about the certificates available on the phone. The web interface displays the fields of the Root Certificate (CA) and Device Certificate for TLS connections, web self-generated certificate and SCEP.

The following certificate fields are available for display:

- Serial Number
- Subject Name
- Issuer Name
- Validity Period. This includes `notBefore` and `notAfter` dates.
- Thumbprint. This is the hash of the certificate.
- Basic Constraints
- Subject Alternative Name
- Key Usage Extensions
- Extended Key Usage

Note:

You cannot view the information about the Device Private Key. When you press **View**, the web interface shows the following message: `Device Private Key Content Hidden`.

Support of the PKCS12 file

You can import the Identity certificate and the Private key for any TLS connection in a single PKCS12 file format. The encrypted PKCS12 file contains both the private key and the corresponding certificate.

In the certificate .xml configuration file, provide a valid PKCS12 file, password, and hash for the required TLS connection. The configured parameters are the following:

- `<cert_uri format>`
- `<cert_hash algo>`
- `<cert_pkcs12_password>`

The following is the example of the corresponding section in the certificate .xml configuration file:

```
<certificates>
…
 <sip>
   <ca_uri></ca_uri>
   <ca_hash algo="md5"></ca_hash>
   <cert_uri format="pkcs12/pem"></cert_uri>
   <cert_hash algo="md5"></cert_hash>
   <privkey_uri></privkey_uri>
   <privkey_hash algo="md5"></privkey_hash>
   <cert_pkcs12_password></cert_pkcs12_password >
 </sip>
…
</certificates>
```

Note:

Ensure that the firmware version of your Avaya Conference Phone B199 supports the import of the PKCS12 file. If the firmware version is lower than 1.0.8, the phone does not install the certificate configured with the PKCS12 file.

Configuration of the file format

To configure imported file format, locate the `<cert_uri format>` parameter in the certificate .xml configuration file. The format can be .p12 (for the PKCS12 file) or .PEM, but you can specify only one format for this parameter in the certificate .xml configuration file.

The following are examples of the configured `<cert_uri format>` parameter for different file formats:

- To install the certificate in the .p12 format, specify `"pkcs12"` as in the following example:

  ```
  <certificates>
          <sip>
              <cert_uri format="pkcs12">file.p12</cert_uri>
          </sip>
      </certificates>
  ```

- To install the certificate in the .PEM format, specify `"pem"` as in the following example:

  ```
  <certificates>
          <sip>
              <cert_uri format="pem">file.pem</cert_uri>
          </sip>
      </certificates>
  ```

  You can also leave this parameter empty to install the certificate in the .PEM format.

Configuration of the PKCS12 file and the private key

In the certificate .xml configuration file, you can add the PKCS12 file and the private key. After the phone reboots, it imports the PKCS12 file and ignores the private key.

The following is an example of the certificate .xml file for the SIP connection configured with the PKCS12 file format and the private key:

```
<certificates>
        <sip>
            <cert_uri format = "pkcs12">file.p12</cert_uri>
            <cert_hash
algo="SHA256">11b121edc782f81aa9852bd8455a8824b7f2471419761eadae2217a4e9b58408</
cert_hash>
            <privkey_uri>priv.key</privkey_uri>
            <privkey_hash
algo="SHA256">11b121edc782f81aa9852bd8455a8824b7f2471419761eadae2217a4e9b58408</
privkey_hash>
            <cert_pkcs12_password>5678</cert_pkcs12_password>
        </sip>
    </certificates>
```

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)
  - AES 192 and AES 128 (optional)
- 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)

Avaya Conference Phone B199 provides support to specific FIPS-related encryption algorithms, which makes it ready for operation in FIPS mode.

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

Related links

Encryption methods in Legacy encryption mode on page 173

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 and **FIPS Mode** to false. When you try to enable **EAP MD5** while **Allow Legacy Encryption** is disabled, the phone warns you with the following message: `EAP MD5 requires Allow Legacy Encryption to be enabled`. When you try to enable **Allow Legacy Encryption** while **FIPS Mode** is enabled, the phone warns you with the following message: `Allow Legacy Encryption cannot be enabled while FIPS mode is enabled`.

You can 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.

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.

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 115
Configuration parameters on page 39

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 case you enable the **Capability Negotiation** setting for the phone to negotiate transport protocols and attributes, the phone supports one crypto only. The supported crypto depends on the Legacy encryption mode configuration as follows:

- If you disable the Legacy encryption mode, the phone offers `AES_256_CM_HMAC_SHA1_80` crypto only.
- If you enable the Legacy encryption mode, the phone offers `AES_CM_128_HMAC_SHA1_80` crypto only.

When you disable the **Capability Negotiation** setting, there are several crypto solutions available for the SRTP negotiation. The options are the following:

- With the **Allow Legacy Encryption** setting disabled, the phone supports the `AES_CM_128_HMAC_SHA1_80` and `AES_256_CM_HMAC_SHA1_80` cryptos.
- With the **Allow Legacy Encryption** setting enabled, the phone supports the `AES_CM_128_HMAC_SHA1_80` and `AES_256_CM_HMAC_SHA1_80` cryptos.

Note:

In the configuration file the configured parameters are `<capneg>` and `<allow_legacy_encryption>`

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 Legacy encryption mode, the phone offers all the previously supported ciphers for the SSL negotiation and cryptos for SRTP. You can 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, Legacy encryption is disabled.

Firmware upgrade

When upgrading, the phone automatically enables the **Allow Legacy Encryption** option, if **802.1x** with **EAP MD5** is enabled.

Related links

Encryption methods in Legacy encryption mode on page 173

FIPS mode

Avaya Conference Phone B199 supports a specific FIPS mode to make the encryption and cryptographic functions compliant with Federal Information Processing Standards (FIPS). When

you enable FIPS mode, the phone employs approved key exchange algorithms, cryptographic algorithms, and authentication techniques to meet the FIPS 140-2 requirements.

When Avaya Conference Phone B199 needs cryptographically secure numbers, it uses random number generator functions from FIPS 140-x compliant cryptographic libraries. A specific FIPS-approved random number generator renders cryptographic number initialization vectors.

With FIPS mode enabled, the device management with HTTPS server occurs using the SSL encryption method.

By default, FIPS mode is disabled.

Note:

If you configure the phone to allow legacy encryption, you cannot enable FIPS mode. You see the following popup message: `FIPS mode cannot be enabled while Allow Legacy Encryption is enabled.`

If you configure the phone to use 802.1x with EAP MD5, you cannot enable FIPS mode. The phone warns you with the following message: `FIPS mode cannot be enabled while 802.1x with EAP MD5 is enabled.`

Related links

Standard encryption for 802.1x on page 135
Legacy encryption mode on page 136

FIPS mode for media encryption with SRTP

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

The conference phone supports the same mandatory crypto `AES_256_CM_HMAC_SHA1_80` when **FIPS Mode** and **Allow Legacy Encryption** are disabled.

When the administrator disables **FIPS Mode** and enables **Allow Legacy Encryption**, Avaya Conference Phone B199 supports `AES_CM_128_HMAC_SHA1_80` for media encryption with SRTP.

SCEP support

Avaya Conference Phone B199 supports Simple Certificate Enrollment Protocol (SCEP) required for managing digital certificate obtainment. SCEP is used to contact a SCEP server to get an Identity certificate. The device uses this certificate for all TLS connections if they do not have manually configured certificates (SIP TLS, 802.1x EAP-TLS, Provisioning via TLS, LDAP). You can also obtain a CA certificate if the SCEP server has corresponding configurations.

SCEP enrollment

You can configure SCEP through the web interface and importing the configuration file with the specific SCEP settings. After Avaya Conference Phone B199 reboots, it attempts to connect the specified SCEP server. If the server is reachable, it provides the certificates with the settings

matching the server configuration. If the received certificate is valid and the SCEP enrollment is successful, the phone saves the configuration and reboots.

When the device requests an SCEP server to get or renew a certificate, the request must be approved. The following types of request approval are available:

- Manual approval. The SCEP server receives your request, and then the SCEP server administrator must approve it. The next request of the device results in the certificate provision.
- Automatic approval. The SCEP server checks your request for validity, then if the parameters are accurate, approves the request and sends you the certificate.

The enrollment fails if the settings configuration on the phone and the server do not match. Here, Avaya Conference Phone B199 triggers the next enrollment in 24 hours.

If you upload a certificate to the phone through the web interface or using automatic provisioning only for one connection, for example, for the LDAP connection, that connection continues to use the configured certificate. Other connections use the SCEP Identity certificate received from the SCEP server.

Mandatory SCEP parameters

Successful enrollment is only possible if you configure the relevant SCEP server and valid SCEP settings. When you enter the URL of the dedicated SCEP server, you must specify the following parameters:

- Common Name
- CA Identifier
- Initiate renewal on % of Validity interval
- Key Length
- Password

Important:

There is no check of mandatory parameters in automatic provisioning and configuration file import. You must always provide valid data.

Background polling

If you configure SCEP with the valid data, the phone attempts to connect to the SCEP server. If the server is reachable, it immediately starts processing the enrollment or renewal request. If the connection fails, Avaya Conference Phone B199 attempts to contact the SCEP server in the background.

For manual approval of a certificate, the phone sends the first request after the reboot and repeats it 20 times within 300 seconds. If the request stays unapproved, the phone tries to connect again in 24 hours.

Auto-renewal

The SCEP server provides a device certificate with a specified validity period, meaning that the device certificate expires in a pre-set amount of days. After it expires, you must get a new device certificate from the SCEP server. You can configure the date and time to send the renewal request for the certificate. You must specify the renewal date and time in percent of the expired validity period of the valid certificate. For example, you can configure to send the renewal request when

the current certificate validity period expires by 95%. You must enter `95` in the **Initiate renewal on % of Validity Interval** field.

When the auto-renewal of the certificates is complete, the phone reboots as soon as it enters Idle mode. After the reboot, Avaya Conference Phone B199 starts using the new device certificate.

Note:

The phone can also boot up with an expired certificate. If you have the renewal request parameter configured, the phone sends the renewal request after the phone boots up.

Configuring SCEP renewal request

About this task

When Avaya Conference Phone B199 receives a device certificate from a SCEP server, the certificate has a specified validity period, after which the certificate expires. Use this procedure to configure a SCEP renewal request through the web interface.

Before you begin

Log in to the web interface as administrator.

Procedure

1. On the web interface, click **Provisioning**.
2. In the SCEP section, enter the value in **Initiate renewal on % of Validity Interval**.

   The value range is from `1` to `99`. The default value is `90`.
3. Click **Save**.

   The phone reboots to apply the changes.

   The web interface shows `Save Succeeded` pop-up message.

Related links

SCEP support on page 137

Provisioning of the CA certificate through SCEP

The SCEP server supports the provisioning of CA certificates, which Avaya Conference Phone B199 uses as the default CA certificates for all TLS connections.

If any of the TLS connections requires a specific CA certificate, you can do the following:

- Install the certificate manually. Here, the phone uses the manually installed CA certificate and ignores the certificate received from the SCEP server.
- Request and receive the certificate from the SCEP server.

If you have a CA certificate from the SCEP server and initiate the SCEP renew enrollment process, the phone continues using this CA certificate after the SCEP renew enrollment process ends.

Related links

Certificates on page 126

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:** 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 131

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
```

Disabling web access

About this task

Use this procedure to disable the web access setting of your Avaya Conference Phone B199 for security reasons. By default, web access is enabled.

After you disable this setting, you cannot access your phone through the web interface. You can restore access to the web interface by enabling the web access setting on the phone or through auto-provisioning.

Before you begin

Ensure that you have the administrator password configured on the phone.

Obtain the .xml configuration file.

- To disable web access on the phone, do the following:
  1. Log in as the administrator.

2. On the phone screen tap **Settings** > **Admin** > **Device Management**.
3. Disable **Web Access**.
4. Tap the **Arrow Left** icon twice to return to the home screen.

   The phone reboots to apply the changes.

- To disable web access through the web interface, do the following:
  1. Log in to the web interface.
  2. Click **Provisioning**.
  3. In the Device Management section, disable **Web Access**.

     You can see the following warning message: `You will not be able to access phone administration web interface after disabling Web Access.`
  4. Click **Save**.
- To disable web access by using the .xml configuration file, do the following:
  1. Locate the `<httpd>` section in the configuration file.
  2. In the `<enable>` line, change the value to `false`.
  3. Save the file.
  4. Import the configuration file through the web interface.

     The phone reboots to apply the changes.

Protection against cross-site request forgery

When the user logs in to the web interface of Avaya Conference Phone B199 with the administrator password, the web application of the phone uses specific tokens to protect against Cross-Site Request Forgery (CSRF) attacks.

CSRF is an attack that tricks the user into submitting a malicious request. The attacker takes the identity and privileges of the user to make undesired actions on the user’s behalf. CSRF attacks target functionality that causes a state change, for example changing the user's password. If the user stays authenticated to the website during the attack, the website can not distinguish between forged and legitimate requests.

B199 generates a new CSRF token on each request. Each link or parameter change in the web interface needs to have a CSRF token as a request parameter. The web application checks if the token in the request is the correct one. For example, if the attacker copies an existing link from the open web interface of B199, the server responds with the following error code: `HTTP status code 403, forbidden`.

Important:

You are recommended to administer the settings in the web UI only from one computer and one browser simultaneously. This way you can minimize the risk of getting the error code message due to incorrect token use.

Chapter 9: Calls handling application

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 3.0, 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 3.0 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.

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. 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.

   Avaya Conference Phone B199 restarts the application to apply the changes.

   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.
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.

Table continues…

Name	Description
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.

Chapter 10: Coverage expansion

Expansion of the phone coverage

Use your Avaya Conference Phone B199 on larger conference tables or when the number of meeting participants is greater than 10. In this case, to ensure the high-level quality of audio signal, you can expand the phone coverage in the room without a PA system. To expand the phone coverage, connect Avaya™ Smart Mic expansion microphones to the phone or cascade 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 Avaya™ 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.

Physical layout

You can connect up to two Avaya™ Smart Mic expansion microphones to get an extended pick-up area. Each microphone has a pick-up range of 4 meters.

Figure 1: Front view of Avaya™ Smart Mic.

The following table lists the buttons and the other elements of Avaya™ Smart Mic:

Callout number	Description
1	Mute button
2	LED status indicator
3	Connection cable

Smart Mic characteristics

The following table shows the dimensions, weight, and other characteristics of Avaya™ Smart Mic:

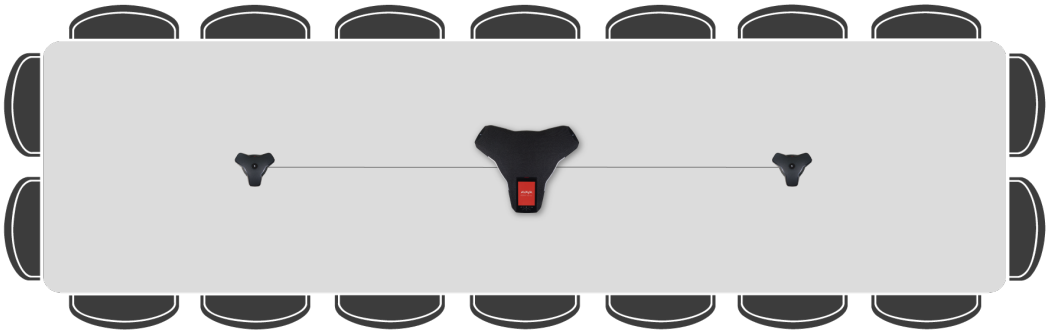
Parameter	Value
Width	160 mm
Length	190 mm
Height	60 mm
Weight	220 g
Pick-up range	4 m
Connection	Modular 6/6 jack

Expansion coverage arrangement

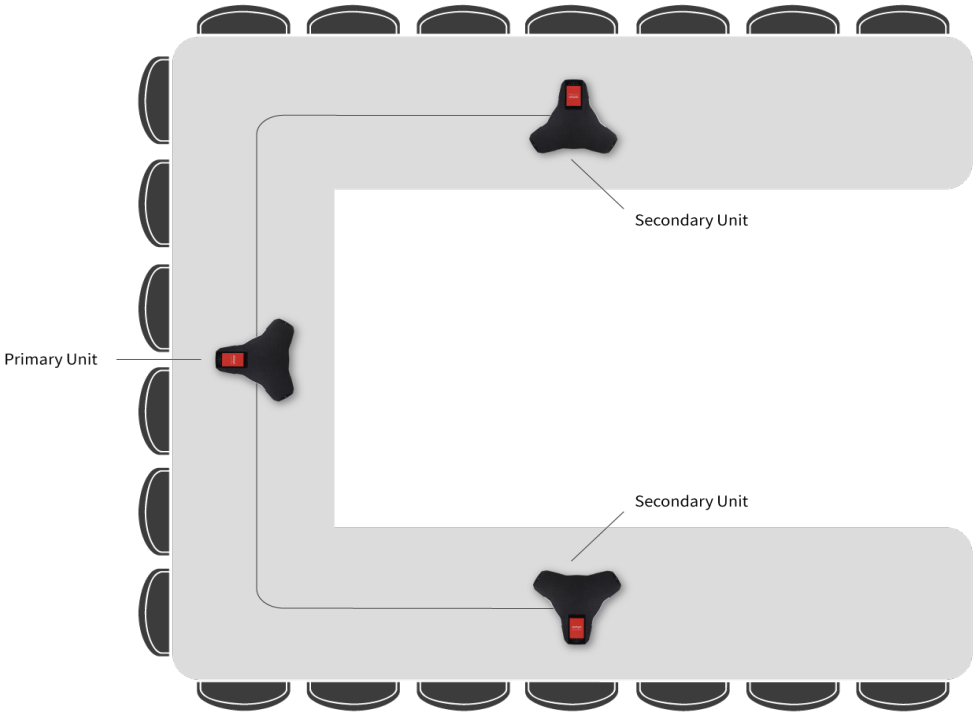
You can arrange a daisy chain with your conference phone and another B199 Conference Phone or connect Smart Mic expansion microphones. The maximum number of devices in a daisy chain is three. One B199 phone acts as a central device (the “Primary” phone), and one or two other units act as expansion devices (the "Secondary" devices).

The expansion coverage arrangement depends on the size and the furnishing of the conference room and the number of participants. The most common are the following arrangements:

- Expansion microphone — Primary phone — Expansion microphone. This arrangement is typical for middle conference rooms and best suits meetings with up to 20 participants.



- Secondary phone — Primary phone — Secondary phone. This arrangement is typical for large and very large conference rooms with more than 20 people present.



Depending on your needs and preferences, you can also use one of the following less common arrangements:

- Primary phone — Secondary phone
- Primary phone — Expansion microphone
- Expansion microphone — Primary phone — Secondary phone

Note:

To connect several B199 phones, use one or two daisy-chain cables. To connect Avaya™ Smart Mic to the Primary phone, use the connecting cable supplied with the expansion microphone.

Functions of the Primary and Secondary devices

When B199 Conference Phone acts as the Primary device, it performs all its configured functions.

When B199 Conference Phone is in a subordinate position (a Secondary device), it performs the following functions:

- Plays audio received from the Primary device. The Primary phone defines the audio characteristics.
- Sends its microphone audio to the Primary device.
- Receives and indicates mute state changes made on the Primary device.
- Sends information to the Primary device when you tap **Microphone Muted** on it.
- Sends information to the Primary device when you adjust the volume on it.

Note:

You cannot make calls between the Primary and the Secondary devices.

In a daisy chain, the Secondary device follows the signal from the Primary device to enter Sleep mode or 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.

Connection of the Secondary devices to the Primary phone

In a daisy chain, B199 Conference Phone disables all unused daisy chain ports during active calls to ensure the best possible audio experience. That means, that the time, when a Secondary device activates, is dependent on the Primary phone status as follows:

- The Primary phone is in the Idle state. When the user connects an expansion microphone or a Secondary device to the Primary phone, B199 Conference Phone immediately detects it, and the connected device becomes directly available for operation.
- The Primary phone has an active call. When the user connects an expansion microphone or a Secondary device to the Primary phone, the connected device becomes available for operation only after the call ends.

The same approach is applicable when the user disconnects and reconnects an expansion microphone or a Secondary device to the Primary phone during an active call. Here, the connected device also becomes available for operation only after the call ends.

Arranging a daisy chain

About this task

Use this procedure to arrange a daisy chain of one main B199 phone and one or two expansion 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:

     - **Primary**
     - **Secondary**
  4. Tap the **Arrow Left** icon 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:

- **Primary**. This is the default mode.
- **Secondary**

3. Click **Save**.

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

Disabling Daisy Chain mode

About this task

Use this procedure to disable 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 Daisy Chain mode from the web interface, do the following:
  1. On the web interface, click **Phone**.
  2. In Daisy Chain Mode, select **Primary**.
  3. Click **Save**.
- To disable 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 **Primary**.
  4. Tap the **Arrow Left** icon three times to return to the home screen.

     Application restarts and restores the Primary phone status.

Headset lecture mode

You can use your Avaya Conference Phone B199 in various setups that require remote lecturing and presentation during an active call. In this Headset lecture mode, the lecturer gets primary attention, and all other call participants can actively participate.

To enable Headset lecture mode, you must connect the headset to the USB host port of the phone. Here, Headset lecture mode activates, and B199 transmits audio signals from the speakers and microphones of the phone and from the headset. The priority of the audio signal from the headset is higher, and the lecturer's words override all other sounds.

Important:

Headset lecture mode activates only with the enabled USB ports. Here, you must have the `<USB enable>` parameter set to `true`. If you disable the USB ports on the phone, Headset lecture mode becomes unavailable.

B199 activates Headset lecture mode only when you connect a supported headset model. For B199 the supported headset is Jabra Engage 65.

The phone does not activate Headset lecture mode if you connect an unsupported headset.

When you connect the headset, B199 shows the Headset lecture mode icon on the status bar to indicate the active Headset lecture mode.

Note:

In a daisy chain, if you connect the headset to a Secondary device, B199 does not show the Headset lecture mode icon on the status bar. Here, the connection of the headset to the Secondary phone does not activate Headset lecture mode. You must connect the headset to the Primary device to enable Headset lecture mode.

Volume level adjustments

In Headset lecture mode, when you adjust the volume level on your B199, the volume level of the headset does not change. Volume level change on the headset does not affect the volume level on the device. This is true for audio signals from the speakers and microphones of your conference phone.

If during a call in Headset lecture mode you press the **Mute** button on your Avaya Conference Phone B199, the phone mutes itself and audio from the headset microphone. If you mute audio on the headset, the phone remains unmuted.

Configuring Headset lecture mode

About this task

Use this procedure to enable or disable Headset lecture mode on your Avaya Conference Phone B199.

Before you begin

Obtain a Jabra Engage 65 headset. The minimum supported headset firmware version is 5.6.0.

Procedure

1. To enable Headset lecture mode, connect the headset to the phone through USB.

   On the status bar, B199 Conference Phone displays the Lecture mode icon.

2. **(Optional)** To disable Headset lecture mode, disconnect the headset from the phone.

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 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 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 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.

Chapter 11: Maintenance

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 25

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 115
[Exporting the configuration file](#) on page 114
[Configuration parameters](#) on page 39

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 159.

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.

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

Table continues…

Section name	Description
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
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 the 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. Here, the system downloads a .zip archive with the logs available.
   - Click the **Download Selected Logs** button to download the logs of a selected type. Here, 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.

PJSIP log levels

Avaya Conference Phone B199 uses the PJSIP library in its real-time media communication. PJSIP is a free and open-source multimedia communication library working with standard-based protocols such as SIP, STUN, and TURN. This library also combines three main components of real-time multimedia communication: signaling, media features, and NAT traversal.

You can use PJSIP logs for information and troubleshooting.

Avaya Conference Phone B199 provides the following PJSIP log levels:

- **Fatal.** This is the least detailed printout. You can see those events that are fatal for the operation.
- **Error.** You can see the list of error events.
- **Warning.** You can see the list of warnings relevant to the device operation.
- **Info.** You can see information about the actions of the device. This is the default option.
- **Debug.** You can get information about specific actions of the device and use it for debugging.
- **Trace.** This is the most detailed printout. You can see all the actions made by the device.

You can set the PJSIP log level through the web interface or using a configuration .xml file.

Setting PJSIP log level through the web interface

About this task

Use this procedure to manually set the PJSIP log level to generate a log message printout with the required details. For example, when you enable a higher log level, you receive useful information for troubleshooting.

Before you begin

Log in to the web interface.

Procedure

1. On the web interface, click the **System logs** tab.
2. Choose the required value from the **PJSIP Log Level** list.

   The value depends on the level of printout details provision you need.
3. Click **Save**.

   The phone restarts the application to apply the changes.

Next steps

Check the PJSIP printout information.

Setting PJSIP log level using the configuration file

About this task

Set PJSIP log level using the .xml configuration file to generate a detailed log message printout. For example, when you set a higher log level, you receive useful information for troubleshooting. When you boot the phone after provisioning, the setting file is changed depending on the configuration of the standard encryption use.

Before you begin

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

Procedure

1. Open the configuration file.
2. In the `<logging>` section, locate the `<pjsip_log_level>` tag and set the necessary value.

   The value range is from 0 to 5. The values correspond to the following five levels with different printout detalization:

   - 0: Fatal
   - 1: Error
   - 2: Warning
   - 3: Info
   - 4: Debug
   - 5: Trace. This is the most detailed printout.
3. Save the configuration file.

   The phone reboots if the PJSIP log level value differs from the previously configured value.

   On the web interface, the **PJSIP Log Level** value changes to reflect the value from 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

Configuration parameters on page 39

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

Licenses

On the **Licenses** web page, you can get the general information about the use and other conditions for the third party components. This web page also contains a copyright URL by using which you can find and download the document with a complete list of the third party components and licenses.

Note:

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

Chapter 12: Specifications

Device 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 Mbps, PoE 802.3af, and PoE 802.3at • USB 2.0 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 (audio output reduced due to lower PoE power level) • Daisy Chain: 91 dB
Speech	• PoE 802.3at: 91 dB • PoE 802.3af: 87 dB (audio output reduced due to lower PoE power level) • Daisy Chain: 91 dB
USB	• Micro USB 2.0 device Type B • USB Type A
Bluetooth®	• Bluetooth® LE • Bluetooth® Classic (HFP, A2DP)

Table continues…

Name	Description
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 • Avaya Cloud Office™
Interoperability with PBX and platforms	• Broadsoft • Zang Office
Device Configuration	• Global .xml or MAC specific .xml configuration files • Web GUI administration

Chapter 13: 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
IP Office SIP Telephone Installation Notes	Get an understanding of IP Office system installation.	Implementation personnel and administrators
IP Office Platform Solution Description	Get an understanding of Avaya IP Office.	Implementation personnel and administrators
Avaya OneCloud™ Private - Administrator Trial Guide	Get an understanding of Avaya OneCloud™ Private.	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
Using Avaya Device Enrollment Services to Manage Endpoints	Use the Device Enrollment Services web portal to manage endpoints or devices.	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.

Appendix A: Encryption methods in Legacy encryption mode

Encryption methods in Legacy encryption mode

The following table lists the encryption methods enabled and disabled in Legacy encryption mode:

Cipher	802.1X	LDAP	SIP TLS	DES	HTTPS	Legacy Cipher
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA256	Y	Y				Y
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	Y	Y				Y
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Y	Y	Y	Y	Y	N
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Y	Y	Y	Y	Y	N
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	Y	Y	Y	Y	Y	N
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	Y	Y	Y	Y	Y	N
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	Y	Y	Y	Y	Y	N
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	Y	Y	Y	Y	Y	N
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Y	Y	Y	Y	Y	N
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Y	Y	Y	Y	Y	N
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Y	Y	Y	Y	Y	N
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Y	Y	Y	Y	Y	N
TLS_RSA_WITH_AES_128_GCM_SHA256	Y	Y	Y	Y	Y	N

Table continues…

Cipher	802.1X	LDAP	SIP TLS	DES	HTTPS	Legacy Cipher
TLS_RSA_WITH_AES_256_GCM_SHA384	Y	Y	Y	Y	Y	N
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	Y	Y			Y	Y
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Y	Y	Y		Y	Y
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Y	Y	Y		Y	Y
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Y	Y	Y		Y	Y
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Y	Y	Y		Y	Y
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	Y	Y			Y	Y
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	Y	Y	Y		Y	Y
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	Y	Y	Y		Y	Y
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	Y	Y	Y		Y	Y
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	Y	Y	Y		Y	Y
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	Y	Y			Y	Y
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	Y	Y	Y		Y	Y
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	Y	Y	Y		Y	Y
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	Y	Y	Y		Y	Y
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	Y	Y	Y		Y	Y
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	Y	Y			Y	Y
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Y	Y	Y		Y	Y
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	Y	Y	Y		Y	Y
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Y	Y	Y		Y	Y

Table continues…

Cipher	802.1X	LDAP	SIP TLS	DES	HTTPS	Legacy Cipher
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	Y	Y	Y		Y	Y
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	Y	Y			Y	Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Y	Y	Y		Y	Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Y	Y	Y		Y	Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Y	Y	Y		Y	Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Y	Y	Y		Y	Y
TLS_RSA_WITH_3DES_EDE_CBC_SHA	Y	Y			Y	Y
TLS_RSA_WITH_AES_128_CBC_SHA	Y	Y	Y		Y	Y
TLS_RSA_WITH_AES_128_CBC_SHA256	Y	Y	Y		Y	Y
TLS_RSA_WITH_AES_256_CBC_SHA	Y	Y	Y		Y	Y
TLS_RSA_WITH_AES_256_CBC_SHA256	Y	Y	Y		Y	Y
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA					Y	Y
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256					Y	Y

Index

Special Characters

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W