



Installing and Administering Avaya Room System C100 Series

Release 1.2.1
Issue 6
February 2026

Notices

© 2026 Avaya LLC. All Rights Reserved.

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided 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](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 Global Software License Terms ("Software License Terms") are available on the following website <https://www.avaya.com/en/legal-license-terms/> or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

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, 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

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](http://www.mpegla.com).

Service Provider

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](http://www.mpegla.com).

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply 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, please contact your Avaya Sales Representative.

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 Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud 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 license-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 A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A 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 ISÉ établies 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.

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

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.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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 the EMC Directive 2014/30/EU, Safety LV Directive 2014/35/EU, and Radio Equipment Directive 2014/53/EU. A copy of the Declaration may be obtained from <https://support.avaya.com> or Avaya LLC, 350 Mt. Kemble Avenue, Morristown, NJ 07960 USA.

WiFi transmitter

- Frequencies for 2412-2472 MHz, transmit power: 18 dBm
- Frequencies for 5180-5240 MHz, transmit power: 17 dBm



Warning:

This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

General Safety Warning

Use only the Avaya approved Limited Power Source power supplies specified for this product.

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Avaya LLC is under license.

Android, Google and Google Play are trademarks of Google Inc.

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	9
Purpose	9
Required skills and knowledge	9
Safety precautions	9
Emergency calls	11
Change history	12
Chapter 2: Overview	14
Avaya Room System C100 Series overview	14
Avaya Room System C100 Series camera overview	15
Avaya Room System C130 overview	15
Avaya Room System C130 physical layout	15
Avaya Room System C170 overview	17
Avaya Room System C170 physical layout	18
Avaya Room System C190 overview	20
Avaya Room System C190 physical layout	20
Indicator status	22
Remote control	23
Supported languages	25
Package list	25
Chapter 3: Initial setup and connectivity	26
Installation checklist	26
Installation	26
Wall-mounting Avaya Room System C130	27
TV-mounting Avaya Room System C130	28
Wall-mounting Avaya Room System C170	31
Avaya Room System C130 cables	33
Avaya Room System C170 cables	35
Avaya Room System C190 cables	36
Powering on Avaya Room System C130	38
Powering on Avaya Room System C170 and Avaya Room System C190	38
Chapter 4: Configuration in the GUI menu	40
GUI menu overview	40
Accessing the Settings menu	41
Performing basic configuration from the Quick Config menu	41
Configuring global settings	43
Configuring SIP account settings	44
Configuring H.323 account settings	45
Configuring network settings	46
Viewing network details	47

Configuring audio settings.....	47
Configuring video settings.....	48
Configuring layout settings.....	49
Viewing codec details.....	49
Performing a factory reset.....	50
Upgrading the codec software.....	50
Chapter 5: Configuration in the web interface.....	52
Web interface Settings menu overview.....	52
Changing the web interface language before logging in.....	54
Accessing the web interface.....	54
Changing the web interface language from the Settings menu.....	55
Global settings.....	56
Configuring the codec display name for calls.....	56
Configuring an H.323 account.....	56
Configuring a SIP account.....	57
Configuring global security settings.....	58
Device management platform configuration.....	59
Call settings.....	60
Configuring call options.....	60
Configuring the codec as an MCU.....	61
Audio settings.....	62
Configuring audio input.....	62
Configuring audio output.....	63
Setting up echo elimination.....	66
Configuring USB audio.....	67
Configuring audio codecs.....	68
Configuring the digital microphone.....	69
Video settings.....	69
Adding a video input.....	69
Configuring video output.....	70
Configuring a screen layout for an HDMI output.....	70
Configuring video codecs.....	71
Configuring video encoding and decoding.....	71
Recording management.....	72
Network settings.....	75
Configuring IP settings.....	75
Configuring firewall settings.....	76
Configuring quality of service.....	76
Configuring SNMP settings.....	78
Configuring the H.323 protocol.....	79
Configuring H.323 encryption.....	79
Configuring the SIP protocol.....	80
Configuring SIP encryption.....	81

Configuring LDAP settings.....	82
Certificate management.....	83
Adding an IP address to the blocklist.....	85
Display settings.....	85
Configuring a codec name.....	85
Configuring a banner.....	86
Configuring scrolling captions.....	86
Other settings.....	87
Setting up the date and time.....	87
Setting up logging.....	88
Log levels.....	88
Exporting the codec configuration to a USB drive.....	88
Importing the codec configuration from a USB drive.....	89
Upgrade process for Avaya Room System C100 Series.....	89
Upgrading the codec software.....	91
Performing a factory reset.....	92
White list management.....	92
Chapter 6: Codec diagnostics	93
Diagnostics menu overview.....	93
Viewing the audio volume level.....	93
Testing the audio input.....	94
Viewing video input details.....	94
Refreshing video encoding parameters.....	94
Testing the network connection.....	95
Capturing codec network traffic.....	96
Viewing call quality details.....	96
Viewing codec details.....	96
Downloading log files.....	97
Clearing log information.....	97
Chapter 7: Troubleshooting	98
The codec is stuck at boot-up.....	98
The codec displays a black screen after boot-up.....	98
No audio output from the speakers.....	99
No audio input from the microphone.....	99
Echo during calls.....	99
The local video image is flickering.....	99
The video resolution cannot reach 4K.....	100
Presentation issues.....	100
Cannot manage PTZ settings with the remote control.....	100
Chapter 8: Resources	101
Documentation.....	101
Avaya Documentation Center navigation.....	101
Finding documents on the Avaya Support website.....	103

Support.....	103
Using the Avaya InSite Knowledge Base.....	103
Glossary	105

Chapter 1: Introduction

Purpose

This document describes how to install and set up Avaya Room System C130, Avaya Room System C170, and Avaya Room System C190. It is intended for the administrators who install and connect Avaya Room System C100 Series to other devices, such as cameras and microphones.

Required skills and knowledge

As an Avaya Room System C100 Series administrator, your main responsibilities are:

- Codec installation, configuration, and management.
- Routine maintenance.
- Troubleshooting.
- Dealing with user queries.

You must have the following skills and knowledge before using this document to install and administer Avaya Room System C100 Series:

- Microsoft Windows.
- Gatekeeper (GK) and Session Initiation Protocol (SIP) server.
- Computer network knowledge such as Ethernet, TCP/IP, and Client/Server.
- H.323 and SIP protocols.
- Familiarity with common maintenance tools.
- Familiarity with video conferencing system functions and services.
- Electrical and electronic equipment operating skills.

Safety precautions

Basic requirements

- Keep equipment dry during use, storage, and transportation.

- Avoid heavy impacts when storing, transporting, and using the equipment.
- Do not disassemble the device by yourself. If the device is faulty, contact Avaya.
- Do not change the structural, safety, and performance design of the equipment without authorization.
- The administrator must understand the correct operation methods and safety precautions before installing, operating, maintaining, removing the safety equipment, and repairing the equipment.
- When using this device, follow relevant laws and regulations and respect the legal rights of others.

Environmental requirements

- Install the equipment according to the instructions.
- Place the equipment on a stable workbench or on a wall-mounted bracket according to the instructions.
- Place the device in a ventilated, non-glare environment.
- Do not place the device and its accessories in an environment with extremes of temperature.
- Do not place the device near water or in a damp area.
- Do not place anything on the device. Leave more than 10cm of heat dissipation space around the device.
- Do not place the device near flammable objects.
- Keep the equipment clean and dust-free.
- Keep away from heat sources and open flames.
- Avoid appliances with strong magnetic or electric fields, such as microwave ovens, refrigerators, and mobile phones.

Usage guidelines

- Do not allow children to play with the equipment.
- To avoid the risk of suffocation, do not allow children to play with product packaging bags.
- To avoid damaging sensitive components, wear an anti-static wrist strap and ground the other end before touching the internal components.
- Use accessories that come with the product or that the manufacturer recommends, such as power adapters and batteries.
- Ensure that the power supply voltage meets the input voltage requirements of the device and use a surge protector.
- Ensure that the three-pin socket is effectively grounded and that the neutral line and the live line are not reversed.
- Keep the power plug clean and dry. To avoid the risk of electric shock, do not use damaged or aged cables.
- Do not step on, pull, or excessively bend the device cable.
- Do not scratch or abrade the outer casing of the device.

- Prevent foreign objects such as metal from entering the device through the ventilation holes.
- Keep your hands dry when plugging and unplugging the device cables.
- Before plugging or unplugging the device cable, stop using the device and disconnect the power.
- Do not allow water or other liquids to flow into the device. If any liquid flows into the device, disconnect the power supply and unplug all the cables connected to the device.
- Stop using the device if there is any abnormality, such as smoke, abnormal sound, or odor. Disconnect the power supply and remove all cables connected to the device.
- During a thunderstorm, disconnect the power and unplug all the cables connected to the device.
- When not using the device for a long time, disconnect the power supply and unplug all the cables connected to the device.

Cleaning instructions

- Before cleaning, stop using the device, disconnect the power supply, and unplug all the cables connected to the device.
- Do not use cleaning liquid or spray cleaner to clean the device casing.
- Wipe the device case with a soft cloth.

Remote control battery usage instructions

- Use the correct type of battery and install the battery using the correct polarity.
- When the battery does not fit into the device, do not squeeze the battery hard.
- If the battery leaks, emits smoke, or emits an odor, replace it immediately.
- Do not mix old and new batteries. When replacing batteries, replace all batteries simultaneously.

Emergency calls

In North America, the management of emergency calls (E911) is regulated and there are several features that enable first responders to locate and arrive at the caller's location. Avaya Room System C100 Series uses a SIP RFC compliant UUID parameter that 911inform can use to provide a location cross-reference. Avaya Room System C100 Series also provides a proprietary SIP parameter +av.mac, which can be used by 911inform and the 911 Secure SENTRY™ system for call location identification.

Change history

Release	Issue	Date	Summary of changes
1.2.1	6	February 2026	Added details on disabling the camera when idle or by default when joining a conference call at Configuring video settings on page 48.
			Added digital signature and file server details at Configuring recording to a USB drive on page 74.
1.2.0.1	5	October 2025	Added HTTPS connection details at: • Configuring global settings on page 43 • Web interface Settings menu overview on page 52 • Changing the web interface language before logging in on page 54 • Accessing the web interface on page 54 • Configuring global security settings on page 58 • Capturing codec network traffic on page 96
1.2	4	August 2025	Added the details on enabling the recording functionality from the web interface at Recording management on page 72.
1.2	3	July 2025	Added LDAP configuration steps at Configuring LDAP settings on page 82.
			Added and updated the details on certificates in the Certificate management on page 83 section.
			Added the details on the forced default password change at Accessing the web interface on page 54.
			Added the details on the Avaya Room System C190 model without the Wi-Fi capability at: • Avaya Room System C190 overview on page 20 • Performing basic configuration from the Quick Config menu on page 41 • Configuring global settings on page 43 • Configuring network settings on page 46 • Configuring global security settings on page 58

Table continues...

Release	Issue	Date	Summary of changes
			Added the details on the remote control range at: • Remote control on page 23 • Wall-mounting Avaya Room System C130 on page 27 • TV-mounting Avaya Room System C130 on page 28 • Wall-mounting Avaya Room System C170 on page 31
			Updated the built-in camera specifications for Avaya Room System C130 at Avaya Room System C100 Series overview on page 14.
			Added built-in microphone range limitations at Avaya Room System C170 overview on page 17.
			Updated indicator status details for Avaya Room System C130 at Indicator status on page 22.
			Added the list of supported languages for the Avaya Room System C100 Series UI at Supported languages on page 25.
			Added a reference to enabling web interface access at: • Web interface Settings menu overview on page 52 • Accessing the web interface on page 54
			Added TV-mounting instructions and updated the package list details for Avaya Room System C130 at: • Package list on page 25 • Installation checklist on page 26 • TV-mounting Avaya Room System C130 on page 28
			Added Glossary on page 105.
			Added links to video tutorials at: • Avaya Room System C100 Series overview on page 14 • Avaya Room System C130 overview on page 15 • Avaya Room System C170 overview on page 17 • Avaya Room System C190 overview on page 20 • GUI menu overview on page 40 • Web interface Settings menu overview on page 52

Chapter 2: Overview

Avaya Room System C100 Series overview

The Avaya Room System C100 Series provides a range of models to meet your video collaboration and in-room conferencing needs. Each model supports:

- SIP/H.323.
- H.265.
- MCU capability.
- Pan, tilt, and zoom (PTZ) camera movements.
- Dual monitors.
- Ethernet, Wi-Fi, HDMI, and USB connection options.

Model	Room configuration	Built-in camera	Video resolution	Microphones
Avaya Room System C130	Huddle or medium room	4K UHD PTZ with 5x digital zoom, 121° diagonal field of view (FOV), 110° horizontal FOV, and 74° vertical FOV	4K	Four built-in directional microphones with a speaker
Avaya Room System C170	Medium or large room	4K UHD PTZ with 12x digital zoom and 72° horizontal FOV	4KP30 2048Kbps Ultra HD	Dual built-in microphones or external microphones
Avaya Room System C190	• With Avaya Room Camera RC212 or Avaya Room Camera RC220: medium or large room • With Avaya Room Camera RC240: 4K room experience	None	4KP30 2048Kbps Ultra HD	Up to four external microphones

Related links

[Introduction to Avaya Room System C100 Series](#)

Avaya Room System C100 Series camera overview

Model	Maximum number of cameras	Camera ports	Maximum number of simultaneous streams
Avaya Room System C130	2	• 1 x HDMI • 1x built-in camera	1
Avaya Room System C170	2	• 1 x HDMI • 1x built-in camera	1
Avaya Room System C190	2	• 2 x HDMI • VCH	2

Avaya Room System C130 overview

Designed specifically for corporate meetings, the Avaya Room System C130 integrated video conferencing unit, or codec, delivers high-quality images and sound reproduction, ensuring excellent remote meeting experiences with clear audiovisual transmission. Avaya Room System C130 is suitable for applications such as cloud conferencing and remote healthcare. Avaya Room System C130 helps businesses enhance meeting efficiency and productivity.

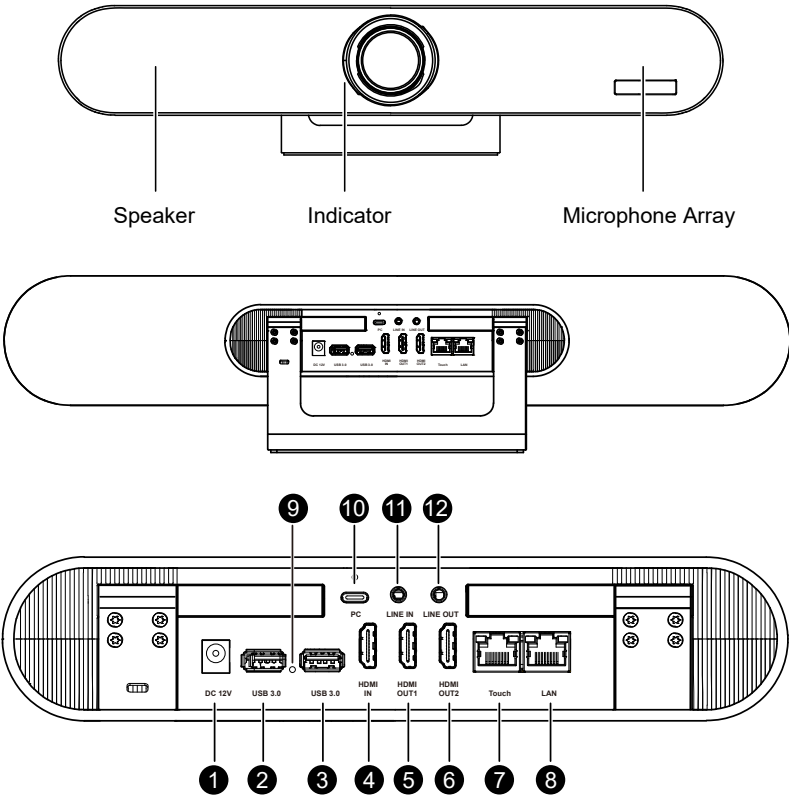


Related links

[Setting up Avaya Room System C130](#)

Avaya Room System C130 physical layout

The following images and table give an overview of the physical layout of the Avaya Room System C130. The labels on the devices that you purchased might slightly differ, but the port function remains the same.



Number	Name	Description
1.	DC 12V	Power interface.
2.	USB 3.0	USB 3.0 Type-A interface: to connect to an external USB drive, mouse, keyboard, and Avaya Room Microphone Speaker RA63.
3.	USB 3.0	USB 3.0 Type-A interface: to connect to an external USB drive, mouse, keyboard, and Avaya Room Microphone Speaker RA63.
4.	HDMI IN	HDMI IN interface: to connect to a computer for sharing a presentation.
5.	HDMI OUT1	HDMI OUT1 interface: to connect to an external HDTV or other display devices or support audio output.
6.	HDMI OUT2	HDMI OUT2 interface: to connect to an external HDTV or other display devices or support audio output.
7.	Touch/DMIC	To connect to a digital microphone. The digital microphone supports cascading.
8.	LAN	To connect to an Ethernet network or power the codec using PoE.

Table continues...

Number	Name	Description
9.	RESET	Reset button: - To retain the current software version when resetting in a powered and idle state, press and hold the Reset button until the codec displays the start-up logo. Release the button to boot up the device. - To restore the factory-installed software version in a powered off state, press and hold the Reset button and then power on the codec. Release the button after the primary HDMI output displays <i>Installing System Update</i>.
10.	PC	To connect to a computer using USB-C. The computer detects the codec as a media device.
11.	LINE IN	3.5 mm audio input interface.
12.	LINE OUT	3.5 mm audio output interface.

Avaya Room System C170 overview

The Avaya Room System C170 integrated 4K UHD video conference unit, or codec, is equipped with an 8.42 million-pixel CMOS sensor chip. It delivers smooth 4K30 video, supports 4K30 + 4K30 dual-stream capabilities, and has a 12X optical zoom lens. Avaya Room System C170 is suitable for various online conferences, including internal and external corporate meetings, administrative meetings, and meetings for command centers.

Avaya Room System C170 has two built-in microphones that you can use for capturing audio within the range of 3 meters in small conference rooms. For medium and large conference rooms, Avaya recommends that you use Avaya Room Microphone RM61 or Avaya Room Microphone Speaker RA63.

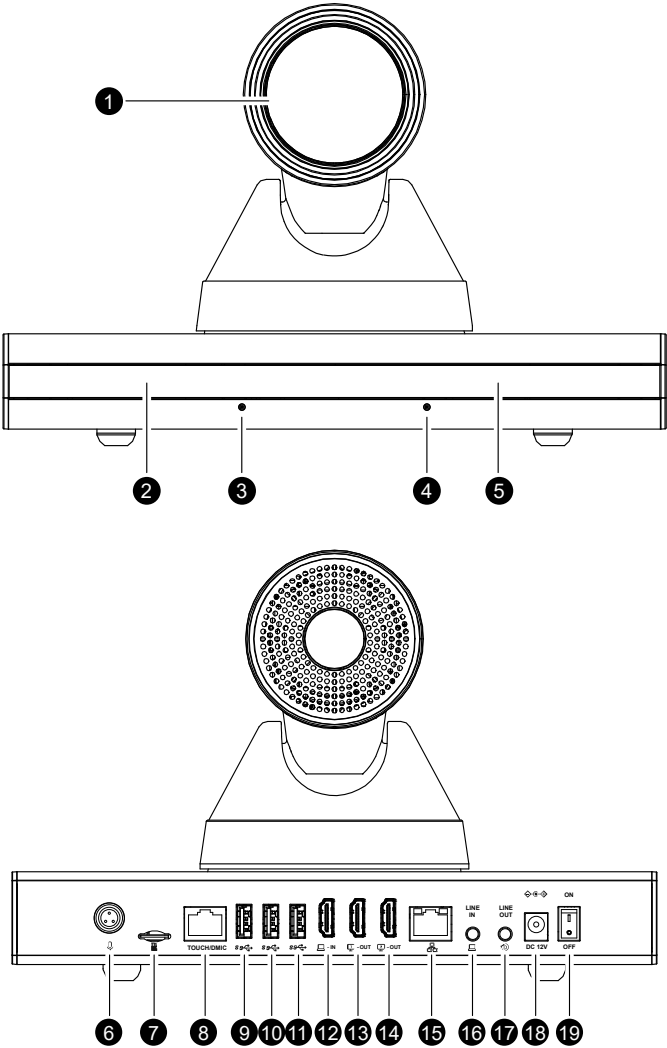


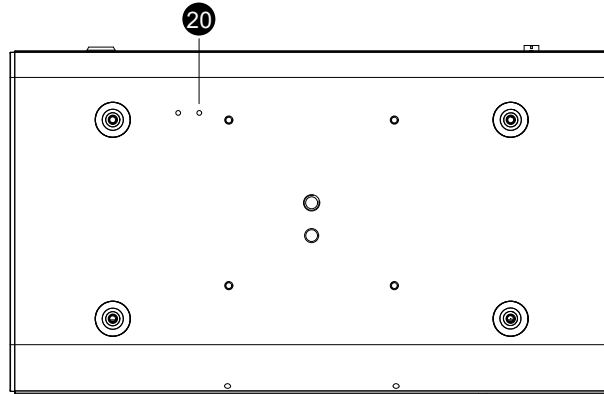
Related links

[Setting up Avaya Room System C170](#)

Avaya Room System C170 physical layout

The following images and table give an overview of the physical layout of the Avaya Room System C170. The labels on the devices that you purchased might slightly differ, but the port function remains the same.





Number	Name	Description
1.	Camera	Built-in camera.
2.	Indicator	Status indicator.
3.	Microphone	Built-in microphone 1.
4.	Microphone	Built-in microphone 2.
5.	IR window	IR receiving window.
6.	MIC IN	MIC IN interface: to connect to an external microphone to receive audio.
7.	MicroSD card slot	Not supported.
8.	Touch/DMIC	To connect to a digital microphone. The digital microphone supports cascading.
9.	USB 3.0	USB 3.0 interface: to connect to an external USB drive, mouse, keyboard, or Avaya Room Microphone Speaker RA63.
10.	USB 3.0	USB 3.0 interface: to connect to an external USB drive, mouse, keyboard, or Avaya Room Microphone Speaker RA63.
11.	USB 3.0	USB 3.0 interface: to connect to an external USB drive, mouse, keyboard, or Avaya Room Microphone Speaker RA63.
12.	HDMI IN	HDMI IN interface: to connect to an external HD camera or computer.
13.	HDMI OUT1	HDMI OUT1 interface: to connect to an external HDTV or other display devices.
14.	HDMI OUT2	HDMI OUT2 interface: to connect to an external HDTV or other display devices.
15.	LAN	To connect to an Ethernet network.
16.	LINE IN	3.5 mm audio input interface.
17.	LINE OUT	3.5 mm audio output interface.
18.	DC 12V	Power interface.
19.	ON/OFF	Power switch.

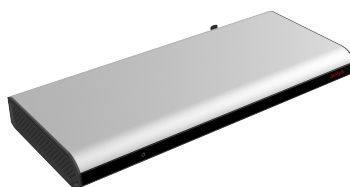
Table continues...

Number	Name	Description
20.	RESET	Reset button: - To retain the current software version when resetting in a powered and idle state, press and hold the Reset button until the codec displays the start-up logo. Release the button to boot up the device. - To restore the factory-installed software version in a powered off state, press and hold the Reset button and then power on the codec. Release the button after the primary HDMI output displays <i>Installing System Update</i>.

Avaya Room System C190 overview

The Avaya Room System C190 4K UHD video conferencing unit, or codec, supports dual 4K@30fps streams, delivering an excellent meeting experience to users. It accommodates various devices for medium to large-sized rooms, featuring three video inputs, two outputs, and three audio inputs and outputs. Avaya Room System C190 is suitable for various online conferences, including internal and external corporate meetings, town hall meetings with remote participants, board meetings, and meetings for distance education and command centers.

Avaya also provides a Avaya Room System C190 model without the Wi-Fi capability. This codec model has no Wi-Fi module and is marked as "C190 w/o RF" on the bottom label. The Wi-Fi settings are unavailable on the GUI menu and in the web interface.

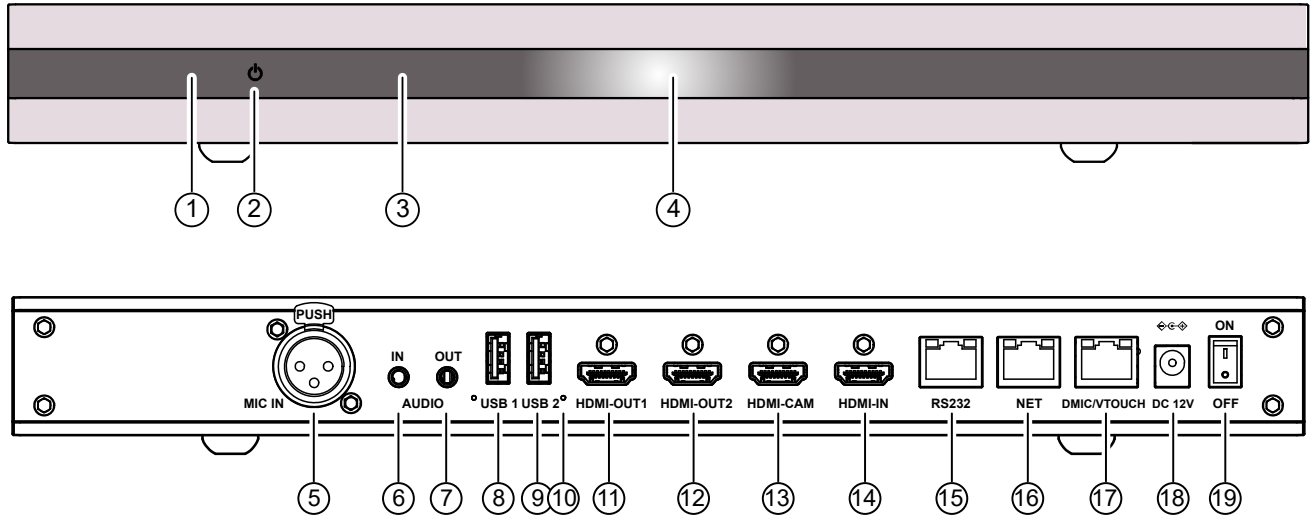


Related links

[Setting up Avaya Room System C190](#)

Avaya Room System C190 physical layout

The following images and table give an overview of the physical layout of the Avaya Room System C190. The labels on the devices that you purchased might slightly differ, but the port function remains the same.



Number	Name	Description
1.	Indicator	Status indicator.
2.	Standby button	Standby touch button.
3.	OLED display	Displays the codec IP address.
4.	IR window	IR receiving window.
5.	MIC IN	To connect to an external microphone to receive audio.
6.	AUDIO IN	3.5 mm audio input interface.
7.	AUDIO OUT	3.5 mm audio output interface.
8.	USB 1	USB interface: to connect to an external USB drive, mouse, keyboard, or Avaya Room Microphone Speaker RA63.
9.	USB 2	USB interface: to connect to an external USB drive, mouse, keyboard, or Avaya Room Microphone Speaker RA63.
10.	RESET	Reset button: - To retain the current software version when resetting in a powered and idle state, press and hold the Reset button until the codec displays the start-up logo. Release the button to boot up the device. - To restore the factory-installed software version in a powered off state, press and hold the Reset button and then power on the codec. Release the button after the primary HDMI output displays <i>Installing System Update</i>. Account and network settings are not preserved when performing a factory reset using the Reset button.
11.	HDMI-OUT1	HDMI OUT1 interface: to connect to an external HDTV or other display devices.

Table continues...

Number	Name	Description
12.	HDMI-OUT2	HDMI OUT2 interface: to connect to an external HDTV or other display devices.
13.	HDMI-CAM	Primary HDMI input: to connect to an external HD camera or computer. By default, you use the primary HDMI input to connect to an external camera.
14.	HDMI-IN	Secondary HDMI input: to connect to an external HD camera or computer. By default, you use the secondary HDMI input to connect to a presentation device such as a laptop.
15.	RS232	• To connect to an external HD camera to control it or pass through the infrared signals. • To connect to external control devices to control the codec.
16.	NET	To connect to an Ethernet network.
17.	DMIC/VTOUCH	To connect to a digital microphone. The digital microphone supports cascading.
18.	DC 12V	Power interface.
19.	ON/OFF	Power switch.

Indicator status

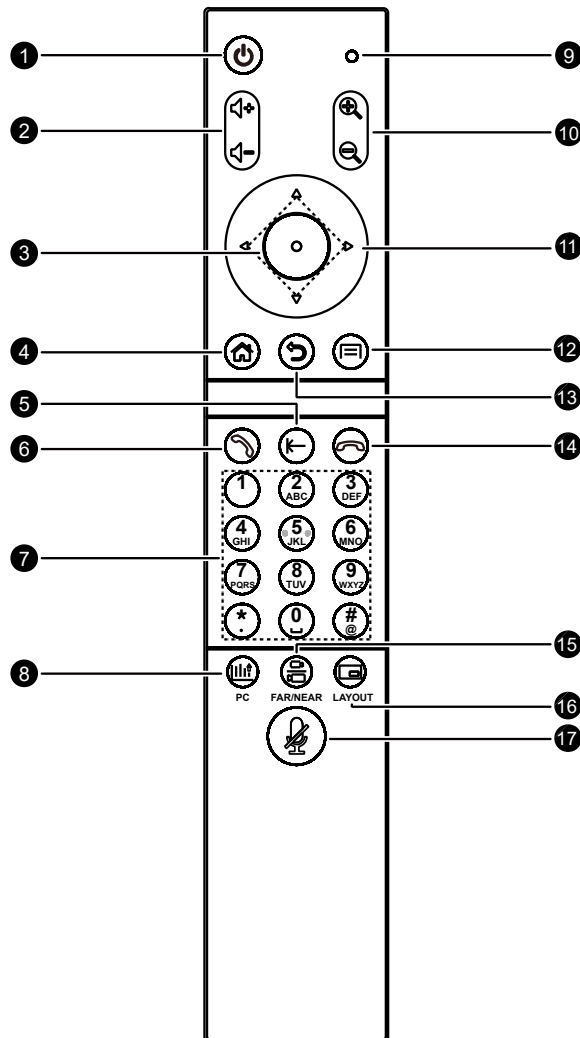
The following table shows the indicator statuses of the Avaya Room System C100 Series codec:

State	Avaya Room System C130	Avaya Room System C170	Avaya Room System C190
Power on process	Red indicator flashing	Red indicator flashing	Red indicator flashing
Network cable disconnected	Red indicator flashing If a USB Type-C cable is connected to a computer, the blue indicator is steady	Red indicator flashing	Red indicator flashing
Standby mode or power connected	Red indicator steady	Red indicator steady	Red indicator steady
Powered off by remote control	Off	Off	Green indicator steady
Receiving infrared signal	Blue indicator steady	Blue indicator flashing	Green indicator flashing
Idle	Blue indicator steady	Blue indicator steady	Green indicator steady
Call operations	Blue indicator steady	Blue indicator steady	Green indicator steady
Power disconnected	Off	Off	Off

Remote control

All codec models support a remote control unit. You can use the remote control within the range of 15 meters from the device. You must use it by either directly pointing at the codec or at a horizontal or vertical angle of up to 15°. To increase the remote control range, you can use a third-party IR repeater.

The following image and table show and describe the remote control buttons and their function:



Number	Name	Description
1.	Power button	Use to go into Standby mode, restart the codec or lock the screen.
2.	Volume +/- button	Use to adjust the volume level.
3.	OK button	Use to confirm selection.

Table continues...

Number	Name	Description
4.	Home button	Use to go to the main menu.
5.	Delete button	Use to delete entered characters.
6.	Call button	Use to start a call, join a conference, or go to the Meeting menu.
7.	Character buttons	Use to enter numbers, letters, or characters.
8.	PC button	Use to manage presentation from the connected media source such as a laptop.
9.	IR indicator	Flashes when you press a remote control button.
10.	Zoom +/- button	Use to zoom in or out a built-in or connected external camera.
11.	Arrow buttons	Use to navigate in the GUI menu.
12.	Menu button	Use to open a submenu.
13.	Back button	Use to return to the previous menu.
14.	End Call button	Use to end a two-party call or leave a conference call.
15.	Far/Near button	• Short-press to switch between local connected and far-end cameras. • For Avaya Room System C130, long-press to manage AI tracking mode for the built-in camera.
16.	Layout button	Use to change the screen layout during an active call.
17.	Mute button	Use to turn on or off codec audio.

Remote control shortcuts

The following table lists the remote control shortcut combinations and provides their description. When using the remote control shortcuts, press the buttons sequentially in the order described in the table.

Shortcut keys	Function
End Call + 1 or End Call + 2	Switch the output resolution of HDMI OUT1 and HDMI OUT2.
Delete + buttons 1–9	Call PTZ presets.
* # 1/2	On C130 and C170, switch the main video source: built-in camera or HDMI.
* # 1/2/3/4	On C190, switch the main video source: HDMI 1, HDMI 2, Camera Compose (a combination of HDMI 1 and HDMI 2), or USB.
ZOOM +/-	Enter PTZ control mode.
ZOOM +/- + any button other than an arrow button	Exit PTZ control mode.

Supported languages

Avaya Room System C100 Series supports the localization of the GUI menu and web interface for all codec and camera models.

An administrator can select the preferred language from the menu and web interface before configuring the device. For the web interface, language selection is also available before logging in to the menu.

The Avaya Room System C100 Series UI is localized to the following languages:

- English (US)
- French
- German
- Italian
- Korean
- Portuguese (Brazil)
- Simplified Chinese
- Spanish
- Traditional Chinese
- Turkish

Package list

The room system package includes the following components:

Component name	Avaya Room System C130	Avaya Room System C170	Avaya Room System C190
Codec	1	1	1
Power adapter	1	1	1
Remote control	1	1	1
HDMI cable	1 (1.5 m)	1 (3 m)	2 (3 m)
Wall-mounting bracket with screws	1	1	0
TV-mounting brackets with screws	1: The mounting kit contains two TV-mounting brackets and an L-shaped codec-mounting bracket.	0	0
Important Notice Document	1	1	1

Chapter 3: Initial setup and connectivity

Installation checklist

The following checklist lists the actions that you must perform to install Avaya Room System C100 Series and provides links to the corresponding procedures:

No.	Task	Reference	✓
1.	Place Avaya Room System C100 Series at a suitable location in the venue or room.	Installation on page 26	
2.	(Optional) For Avaya Room System C130 and Avaya Room System C170, mount the codec on a wall. You can also mount Avaya Room System C130 to a TV.	• Wall-mounting Avaya Room System C130 on page 27 • TV-mounting Avaya Room System C130 on page 28 • Wall-mounting Avaya Room System C170 on page 31	
3.	Connect the peripheral devices to Avaya Room System C100 Series.	• Avaya Room System C130 cables on page 33 • Avaya Room System C170 cables on page 35 • Avaya Room System C190 cables on page 36	
4.	Connect Avaya Room System C100 Series to a power outlet and turn on the power.	• Powering on Avaya Room System C130 on page 38 • Powering on Avaya Room System C170 and Avaya Room System C190 on page 38	

Installation

You can place Avaya Room System C100 Series on surfaces, such as a desk, a cabinet, or other pieces of furniture. You can also install Avaya Room System C130 or Avaya Room System C170 on the enclosed bracket.

When placing the codec on a desk, ensure that it is stable to prevent it from slipping. When placing the codec on a cabinet or furniture, ensure it is secure.

You can mount Avaya Room System C130 and Avaya Room System C170 to a wall using the provided wall-mounting bracket, and you can mount Avaya Room System C130 to a TV back panel. Avaya Room System C190 was designed to be installed on a flat horizontal surface, such as a desk or rack shelf, and the mounting kit is not provided for this model.

Use screws when installing the codec on a bracket.

Avoid facing the codec towards bright light sources such as windows.

 Caution:

Operating the device in a residential environment can cause radio interference.

Wall-mounting Avaya Room System C130

About this task

You can mount Avaya Room System C130 to a wall using the wall-mounting bracket and screws provided in the package. You must choose a smooth, level, drywall surface to install the codec. For more information about the environmental requirements for your device, see [Safety precautions](#) on page 9.

When wall-mounting Avaya Room System C130, place it so that you can either directly point at it with the remote control or at a vertical or horizontal angle of up to 15°. The remote control range is within 15 meters, but you can use a third-party IR repeater to increase the range.

Before you begin

Ensure that you obtain six wall anchors corresponding to the type of wall-mounting surface.

Procedure

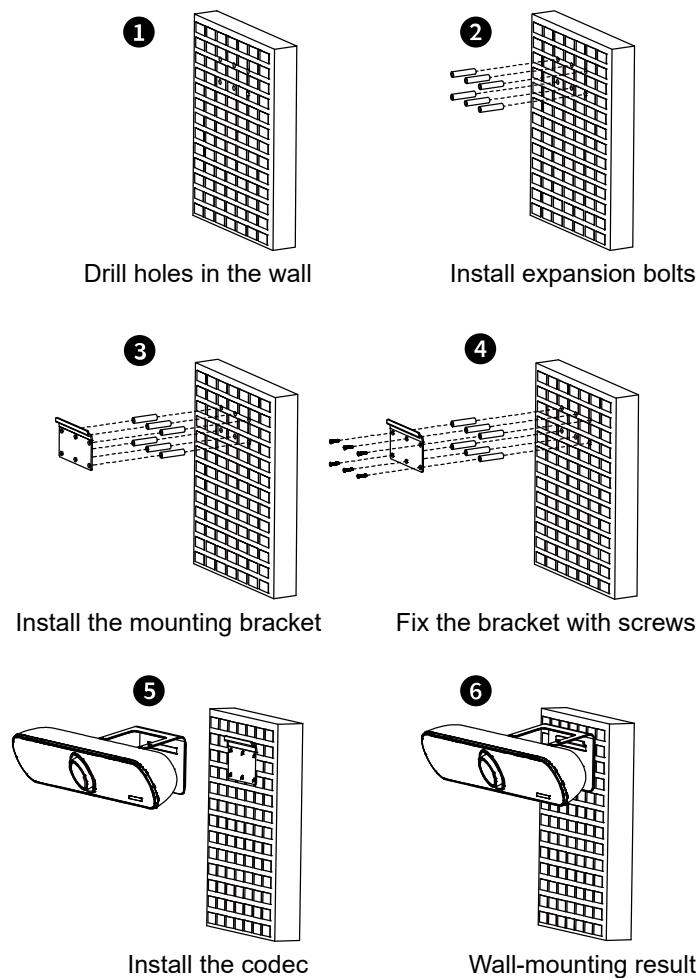
1. Locate the area on the wall to place the codec.

The codec must face the call participants and be at eye level or higher to correctly capture all audio and video data.

2. Drill six holes in the wall and install wall anchors.
3. Install the mounting bracket and fix it with the screws provided in the package.
4. Install the codec on the mounting bracket.

Example

The following diagram shows a high-level wall-mounting process for Avaya Room System C130:



TV-mounting Avaya Room System C130

About this task

You can mount Avaya Room System C130 to a TV back panel using the TV-mounting brackets, an L-shaped codec-mounting bracket, screws and washers provided in the package. You can attach the assembled brackets with the codec to the upper or lower part of the TV back panel. The back panel must have industry-standard VESA mounting holes so that you can attach the brackets.

When TV-mounting Avaya Room System C130, place it so that you can either directly point at it with the remote control or at a vertical or horizontal angle of up to 15°. The remote control range is within 15 meters, but you can use a third-party IR repeater to increase the range.

Before you begin

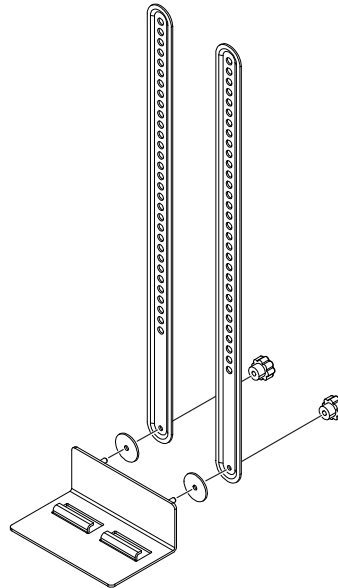
Ensure that you check the TV-mounting package before installing the codec. The package must include the following items:

- Two TV-mounting brackets with a hole diameter of 8.3 mm
- An L-shaped codec-mounting bracket
- Two screws and two washers

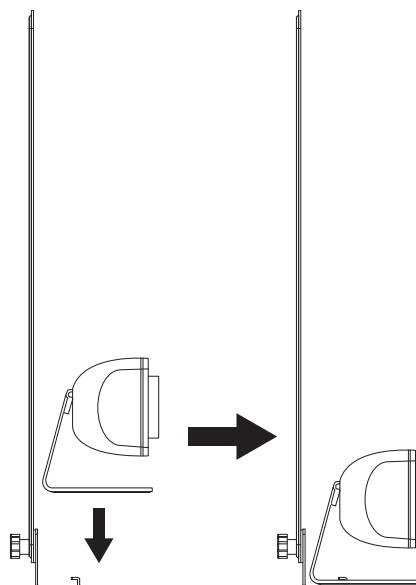
Ensure that you also obtain two appropriate screws to attach the assembled brackets to the TV back panel.

Procedure

1. Fasten the TV-mounting brackets to the codec-mounting bracket with a pair of screws and washers.



2. Install the codec on the L-shaped bracket.

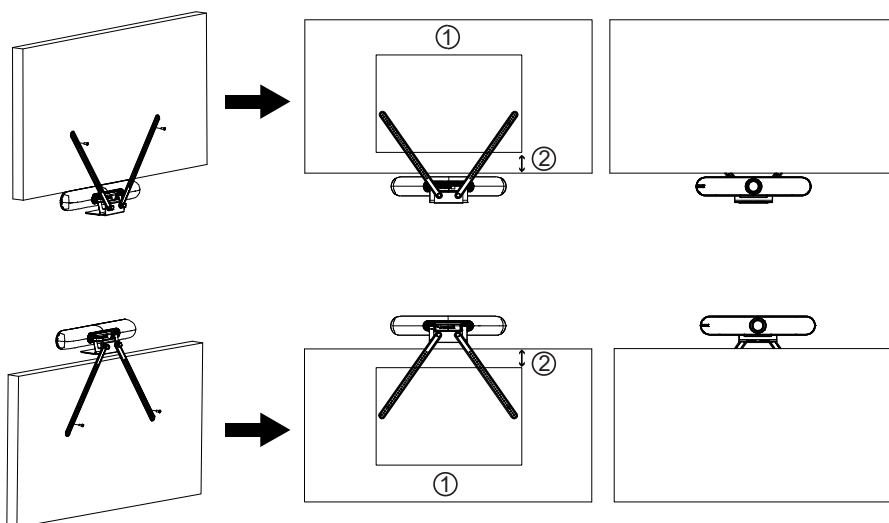


3. Attach the assembled brackets to the back panel of the TV.

You can attach the brackets to the upper or lower part of the TV back panel.

Example

The following diagram shows an example of attaching the brackets to the upper and lower part of the TV back panel, where "1" is a mounting pattern of 800 x 600 mm, and "2" is a reserved space of up to 210 mm:



Wall-mounting Avaya Room System C170

About this task

You can mount Avaya Room System C170 to a wall using the wall-mounting bracket and screws provided in the package. You must choose a smooth, level, drywall surface to install the codec. For more information about the environmental requirements for your device, see [Safety precautions](#) on page 9.

When wall-mounting Avaya Room System C170, place it so that you can either directly point at it with the remote control or at a vertical or horizontal angle of up to 15°. The remote control range is within 15 meters, but you can use a third-party IR repeater to increase the range.

The codec package includes:

- Mounting bracket
- Cross recessed, pan head with tail machine teeth screw, UNC 1/4"-20*8
- Cross recessed, pan head with dielectric flat tail machine screws, PWM3*6

Before you begin

Ensure that you obtain four wall anchors corresponding to the type of wall-mounting surface and four M5 screws.

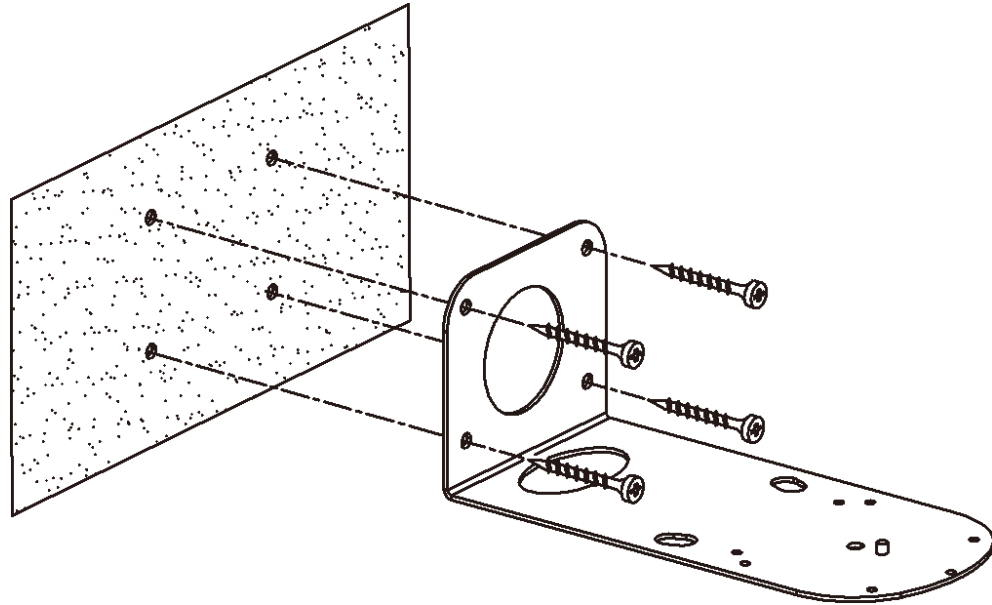
Procedure

1. Locate the area on the wall to place the codec.

The codec must face the call participants and be at eye level or higher to correctly capture all audio and video data.

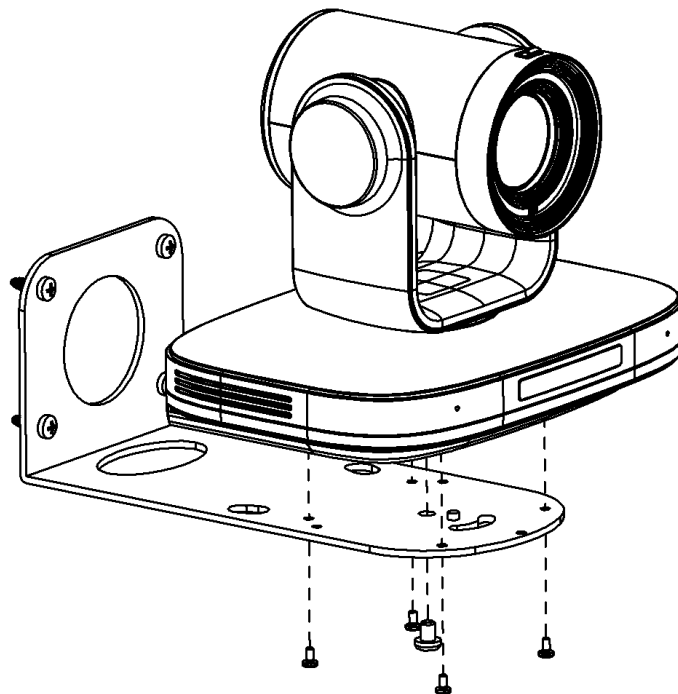
2. Drill four holes in the wall and install wall anchors.
3. Install the mounting bracket and fix it with M5 screws.

The following image shows a high-level view of attaching the mounting bracket to the wall:



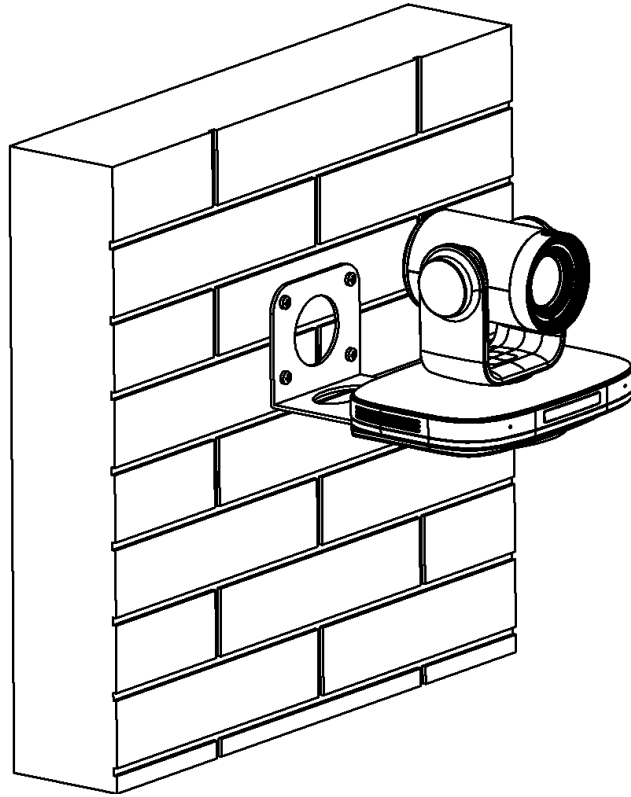
4. Install the codec on the mounting bracket and secure it with PWM3 screws and a UNC 1/4"-20 screw.

The following image shows a high-level view of attaching the codec to the bracket:



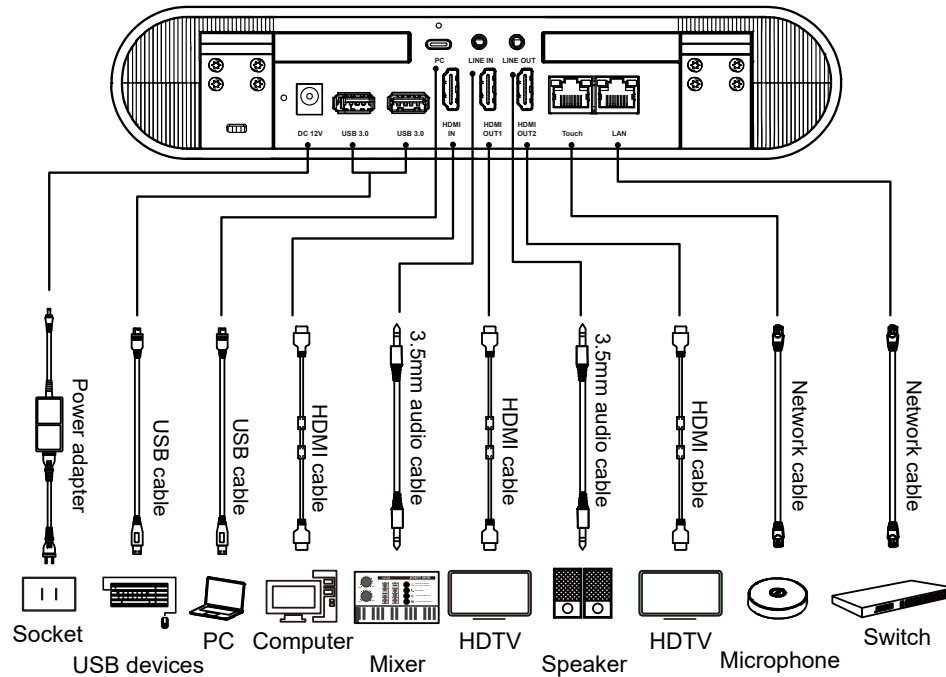
Result

The following image shows an example of a wall-mounted Avaya Room System C170:



Avaya Room System C130 cables

The following image shows optional configurations and is for reference only. Connect the cables according to your requirements.



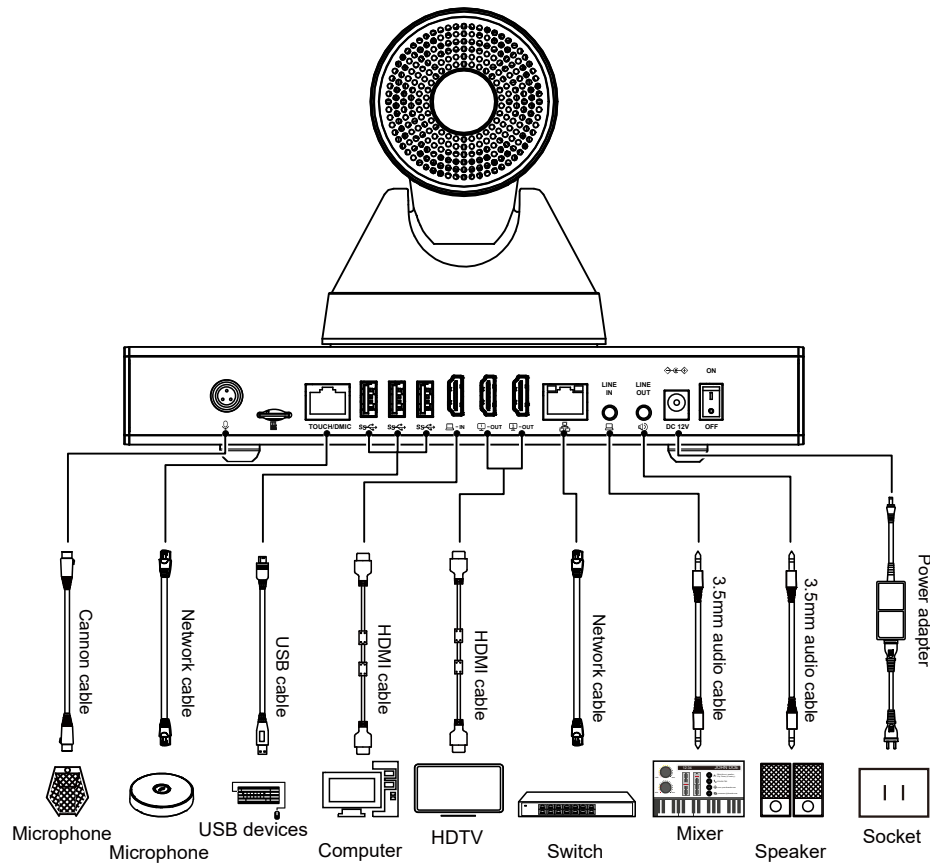
Port type	Description
Input	
First Video Stream Input	Built-in camera.
Second Video Stream Input	Connect an HD camera or the second video stream to the HDMI IN interface to input the second video source.
Audio Input	For audio input, use the following options: - Built-in microphone. - LINE IN: Use a 3.5 mm audio cable to connect a computer or a telephone audio source to the LINE IN interface.
USB	Connect a USB microphone or a USB device, such as a keyboard or mouse. Avaya Room System C130 is compatible with Avaya microphones. For Avaya microphones, you must use the following connection options: - RM61: Connect through the Touch/DMIC port. - RA63: Connect through a USB port.
Output	
Audio Output	For audio output, use the following options: - Built-in speaker. - Connect a loudspeaker to the LINE OUT interface using a 3.5 mm audio cable.

Table continues...

Port type	Description
First Video Stream Output	Connect an HDTV to the HDMI OUT1 interface using an HDMI cable.
Second Video Stream Output	Connect an HDTV to the HDMI OUT2 interface using an HDMI cable.
Connectivity and power	
Network	- Connect to an Ethernet network using a network cable. - Connect using Wi-Fi.
Power Supply	Connect Avaya Room System C130 to the power outlet using the supplied power adapter.

Avaya Room System C170 cables

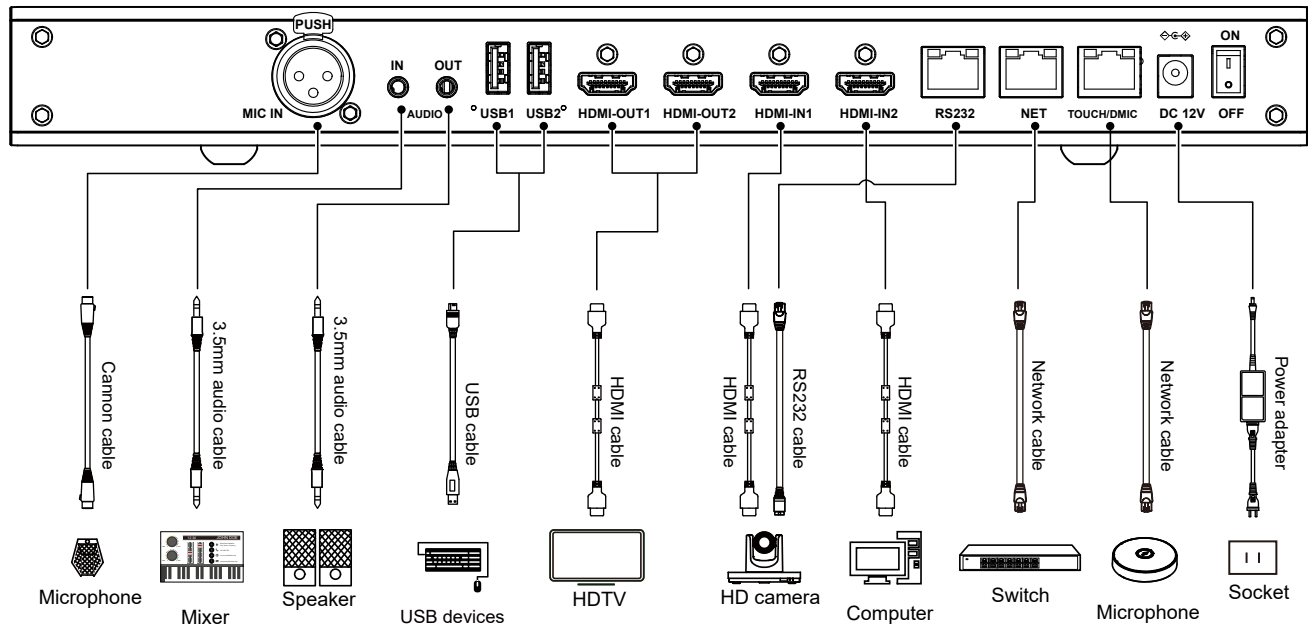
The following image shows optional configurations and is for reference only. Connect the cables according to your requirements.



Port type	Description
Input	
First Video Stream Input	Built-in camera.
Second Video Stream Input	Connect an HD camera or the second video stream to the HDMI IN interface to input the second video source.
Audio Input	For audio input, use the following options: • MIC IN: Connect one or more microphones to the MIC IN interface using a cannon cable. • LINE IN: Use a 3.5 mm audio cable to connect a computer or a telephone audio source to the LINE IN interface. • Touch/DMIC: Use a network cable to connect a digital microphone to the Touch/DMIC interface.
USB	Connect a USB microphone or a USB device, such as a keyboard or mouse. Avaya Room System C170 is compatible with Avaya microphones. For Avaya microphones, you must use the following connection options: • RM61: Connect through the Touch/DMIC port. • RA63: Connect through a USB port.
Output	
Audio Output	Connect a loudspeaker to the LINE OUT interface using a 3.5 mm audio cable.
First Video Stream Output	Connect an HDTV to the HDMI OUT1 interface using an HDMI cable.
Second Video Stream Output	Connect an HDTV to the HDMI OUT2 interface using an HDMI cable.
Connectivity and power	
Network	Connect to an Ethernet network using a network cable.
Power Supply	Connect Avaya Room System C170 to the power outlet using the supplied power adapter.

Avaya Room System C190 cables

The following image shows optional configurations and is for reference only. Connect the cables according to your requirements.



Port type	Description
Input	
First Video Stream Input	Connect an HD camera to the HDMI IN1 interface to input the first video source.
Second Video Stream Input	Connect an HD camera or the second video stream to the HDMI IN2 interface to input the second video source.
Audio Input	For audio input, use the following options: • MIC IN: Connect one or more microphones to the MIC IN interface using a cannon cable. • AUDIO IN: Use a 3.5 mm audio cable to connect a computer or a telephone audio source to the AUDIO IN interface. The AUDIO IN interface can also support multiple audio sources.
USB	Connect a USB microphone or a USB device, such as a keyboard or mouse. Avaya Room System C190 is compatible with Avaya microphones. For Avaya microphones, you must use the following connection options: • RM61: Connect through the Touch/DMIC port. • RA63: Connect through a USB port.
Output	
Audio Output	Connect a loudspeaker to the AUDIO OUT interface using a 3.5 mm audio cable.

Table continues...

Port type	Description
First Video Stream Output	Connect an HDTV to the HDMI OUT1 interface using an HDMI cable.
Second Video Stream Output	Connect an HDTV to the HDMI OUT2 interface using an HDMI cable.
Connectivity and power	
Network	Connect to an Ethernet network using a network cable.
Power Supply	Connect Avaya Room System C190 to the power outlet using the supplied power adapter.

Powering on Avaya Room System C130

About this task

For optimal performance, you must check the power adapter and its function when connecting and powering on Avaya Room System C130.

Before you begin

Ensure that you use the power adapter from the codec package and that the power source is accessible.

Procedure

1. Connect all necessary devices to the corresponding ports on the codec, including HDMI OUT1.
2. Connect the power adapter to the power jack at the back of the codec.
3. **(Optional)** To use PoE as the power source, connect the codec to your network.
4. Plug the other end of the power adapter into a power outlet.

The codec displays the main menu display interface on the device connected to HDMI OUT1.

Powering on Avaya Room System C170 and Avaya Room System C190

About this task

For optimal performance, you must check the power adapter and its function when connecting and powering on the Avaya Room System C100 Series.

Before you begin

Ensure that you use the power adapter that comes with the codec and that the power source is accessible.

Procedure

1. Connect all necessary devices to the corresponding ports on the codec, including HDMI OUT1.
2. Connect the power adapter to the power jack located on the back of the codec.
3. Plug the other end of the power adapter into a power outlet.
4. Turn on the power switch after connecting the power adapter.

The codec displays the main menu display interface on the device connected to HDMI OUT1.

Chapter 4: Configuration in the GUI menu

GUI menu overview

You can access the GUI menu by connecting a display to the HDMI output of the codec and pressing the **Menu** button on the remote control. The following table describes the GUI menu submenus and lists the user roles that have access to them:

Submenu name	User role	Description
Meeting	End user and administrator	You can make two-party calls, access the address book, and manage the list of contacts. If you have purchased an MCU license, you can also manage conference calls. For more information about the MCU license, contact Avaya Support. For more information about the call operations you can perform from the Meeting submenu, see Using Avaya Room System C100 Series .
Camera	End user and administrator	For the codec models with an integrated HD camera, such as Avaya Room System C130 and Avaya Room System C170, you can manage pan, tilt, and zoom parameters and view the video frame changes in real time.
Settings	Administrator	You can access basic codec configuration and set up advanced settings for SIP and H.323 accounts, audio, video, and screen layout. You can also view general codec information, perform a factory reset, and upgrade the codec software to a newer version. You can manage the administrator password for the Settings submenu when configuring global security settings in the web interface.

Related links

[Administering Avaya Room System C100 Series](#)

Accessing the Settings menu

About this task

You can access the Settings menu from the GUI menu Home screen. From the Settings menu, you can go to the **Quick Config** submenu and perform the basic configuration or go to each submenu separately for more advanced settings.

You can restrict access to the Settings menu by selecting the **Enable Admin Password** check box when configuring global security settings. By default, the administrator password is enabled.

Procedure

1. On the GUI menu Home screen, select **More > Settings**.
2. **(Optional)** Enter the administrator password and select **Confirm**.

You can obtain the default password from the release notes.

You can see the Settings menu tiles, including Quick Config, Network, Account, and other submenus.

Performing basic configuration from the Quick Config menu

About this task

From the Quick Config menu, you can configure the main codec settings to quickly start using its features. The basic configuration includes setting up the codec language and time, checking the port connections and audio input, configuring the network and account parameters, and other settings.

Procedure

1. On the Settings menu, select **Quick Config**.
2. On the Welcome screen, select **Confirm** to proceed with basic configuration.
3. On the Language and Time screen, from the **Language** list, select the GUI menu language.
4. From the **TimeZone** list, select the time zone corresponding to your location.

The codec displays the time according to the selected time zone on the Home screen of the GUI menu.

5. For the **Time Format** setting, select one of the following options:
 - **24 hour clock:** The Home screen clock uses the numbers 00:00 to 23:59, and 00:00 indicates midnight.

- **12 hour clock:** The Home screen clock runs from 1 a.m. to 12 o'clock noon and then from 1 p.m. to 12 o'clock midnight. "12 p.m." indicates 12 o'clock noon, and "12 a.m." indicates 12 o'clock midnight.
6. To set the codec time automatically using the Network Protocol Time (NTP), for the **Time Setting** setting, select **Enable Automatic Settings**.
 7. Select **Confirm** to save the configured settings or **Skip** to go to the next screen without saving.
 8. On the Interface Detection screen, check the back panel port connections.
The ports with no connection detected are highlighted in red.
 9. Select **Confirm** to go to the next screen.
 10. On the Network screen, configure the Ethernet, Wi-Fi, and proxy server settings.
If you purchased a Avaya Room System C190 model without the Wi-Fi capability, the Wi-Fi settings are unavailable. For more information about configuring network settings, see [Configuring network settings](#) on page 46.
 11. Select **Confirm** to save the configured settings or **Skip** to go to the next screen without saving.
 12. On the Account screen, configure the settings for a SIP and H.323 account.
For more information about configuring account settings, see [Configuring SIP account settings](#) on page 44 and [Configuring H.323 account settings](#) on page 45.
 13. Select **Confirm** to save the configured settings or **Skip** to go to the next screen without saving.
 14. On the Microphone Detection screen, check your audio input by speaking into the microphone.
 15. Select **Confirm** to go to the next screen.
 16. On the Volume Adjustment screen, for the **Audio Input Volume** and **Audio Output Volume** settings, select the level of volume for the audio input and output.
 17. Select **Confirm** to go to the next screen.
 18. On the General screen, to enable the Auto Answer feature for incoming calls, enable the **Auto Answer** switch.
If you disable Auto Answer, you receive a dialog box for each incoming call to the codec, requesting you to accept the call. With Auto Answer enabled, all incoming calls are automatically answered, and you do not need to accept them.
 19. In the **Venue Name** field, enter the codec display name for conferences and streaming.
 20. Select **Confirm** to save the configured settings or **Skip** to go to the next screen without saving.
 21. On the Setup Completed screen, click **Confirm** to complete the basic configuration.

The GUI menu takes you to the Home page and you can continue the codec configuration or using its features.

Configuring global settings

About this task

Configure global codec settings, including the display text, basic call features, Standby mode, web interface access, language, and time. You can also enable SRTP encryption to protect your call data and select the transmission protocol for SIP calls.

Procedure

1. From the Settings menu, select **General**.
2. On the General screen, in the **Venue Name** field, enter the codec display name for conferences and streaming.
3. From the **Color** list, select the font color for the codec display.
4. From the **Font Size** list, select the font size for the codec display.
5. For Avaya Room System C190, if you select a customizable font size, in the **Text Pixels** field, enter the font height in pixels.
6. From the **Position** list, select the relative text position for the codec display.
7. To enable the Auto Answer feature for incoming calls, enable the **Auto Answer** switch.
If you disable Auto Answer, you receive a dialog box for each incoming call to the codec, requesting you to accept the call. With Auto Answer enabled, all incoming calls are automatically answered, and you do not need to accept them.
8. To set the status to Do Not Disturb (DND) and block all incoming calls, enable the **No Disturbing** switch.
For example, you can enable the DND status during presentations and streaming. The codec does not play a ringtone or display a notification for an incoming call.
9. For the **Auto Standby** setting, select the time of inactivity after which the codec goes into Standby mode.
10. To enable access to the web interface through HTTPS, enable the **Web Access** switch.
11. If you enable web interface access, to end a web interface session after 30 minutes, enable the **Automatically close in 30 minutes** switch.
If you enable the **Automatically close in 30 minutes** switch, the session access ends after 30 minutes. You can enable it again through the GUI menu.
12. To enable an HTTPS connection for the web interface, toggle on the **Enable WEB Service** switch.
13. For the **SIP Transmission Mode** setting, select the transmission protocol for SIP calls.

14. To enable SRTP encryption of call data, toggle on the **SRTP Encryption** switch.
15. From the **Language** list, select the GUI menu language.
16. From the **TimeZone** list, select the time zone corresponding to your location.
The codec displays the time according to the selected time zone on the Home screen of the GUI menu.
17. From the **WiFi Country/Region Code** list, select the option corresponding to your region.
If you purchase an Avaya Room System C190 model without the Wi-Fi capability, this setting is unavailable.
18. For the **Time Format** setting, select one of the following options:
 - **24 hour clock**: The Home screen clock uses the numbers 00:00 to 23:59, and 00:00 indicates midnight.
 - **12 hour clock**: The Home screen clock runs from 1 a.m. to 12 o'clock noon and then from 1 p.m. to 12 o'clock midnight. "12 p.m." indicates 12 o'clock noon, and "12 a.m." indicates 12 o'clock midnight.
19. To set the codec time automatically using the Network Protocol Time (NTP), enable the **Set Time Automatically** switch.
20. On the remote control, press **Back** to return to the Settings menu.

Configuring SIP account settings

About this task

Configure the SIP account to make calls from the codec using the SIP protocol. You can also specify the name and realm for SIP authentication and the proxy server to use.

Procedure

1. On the Settings menu, select **Account**.
2. On the Account screen, select the SIP account to configure and select **Edit**.
3. From the **Account Type** list, select **SIP**.
4. To register the codec as a SIP endpoint, enable the **Register SIP** switch.
5. In the **Account** field, enter the SIP username to authenticate the device before a VoIP session.
6. In the **Register Password** field, enter the SIP password.
The password must match the password value specified on the SIP server to authenticate the codec successfully.
7. In the **Register Server** field, enter the domain name of the SIP server, gateway, or session border controller to use for SIP authentication.

8. In the **Proxy Server** field, enter the IP address or FQDN of the proxy server.
9. In the **Authentication Username** field, enter the username to verify that the device is part of the SIP profile.
10. Select **Confirm** to save the configuration and return to the Settings menu.

Configuring H.323 account settings

About this task

Configure the H.323 account to make calls from the codec using the H.323 protocol. You can also specify the gatekeeper address and the name that gatekeepers and gateways use to identify the codec.

Procedure

1. On the Settings menu, select **Account**.
2. On the Account screen, select the H.323 account to configure and select **Edit**.
3. From the **Account Type** list, select **H.323**.
4. To make calls using the H.323 account, toggle on the **Enable H.323** switch.
5. To use a gatekeeper for H.323 calling, toggle on the **Enable GK** switch.
6. To enable the H.460 extension, toggle on the **Enable H.460** switch.
7. For the **GK Discovery Mode** setting, select one of the following options:
 - **Auto**: To automatically assign the gatekeeper address.
 - **Manual**: To manually specify the gatekeeper address.
8. If you selected the manual assignment of the gatekeeper address, in the **GK Address** field, enter the IP address of the gatekeeper.
9. In the **Account** field, enter the name that gatekeepers and gateways use to identify the codec.
10. In the **Authentication Username** field, enter the username for H.235 authentication.
11. In the **Authentication Password** field, enter the password for H.235 authentication.
12. Select **Confirm** to save the configuration and return to the Settings menu.

Configuring network settings

About this task

Configure the basic network settings, such as IP address assignment, the use of a Wi-Fi network, and proxy server configuration. When configuring IP settings, you can determine whether to choose automatic or static address assignment and select the version of the IP protocol.

Before you begin

To access and configure Wi-Fi settings on the Wireless Network tab, ensure that you have enabled the Wi-Fi capability from the System Security submenu of the Settings web interface menu.

Procedure

1. On the Settings menu, select **Network**.
2. On the Wired Network tab, for the **Acquisite Way** setting, select one of the following options:
 - **Static IP**: You manually specify the IP address and other related settings.
 - **Auto Obtain**: The codec obtains the IP address from the DHCP server.
3. For the **Category** setting, select the IP protocol version to use.
4. If you selected manual IP assignment, in the **IP Address** field, enter the codec IP address.
5. In the **Netmask** field, enter the subnet mask address.
6. In the **Gateway** field, enter the default gateway IP address.
7. In the **DNS1 Address** field, enter the primary DNS server IP address.
8. In the **DNS2 Address** field, enter the secondary DNS server IP address.

The secondary DNS server IP address is used if the primary DNS server is unavailable.

9. Go to the **Wireless Network** tab.

If you purchased a Avaya Room System C190 model without the Wi-Fi capability, the Wireless Network tab and the Wi-Fi settings in steps 10–11 are unavailable.
10. To switch from an Ethernet connection to a Wi-Fi network, for the **WIFI Status** setting, select **Open**.
11. To connect to a different Wi-Fi network, select **Other Networks**.
12. Go to the **Proxy Settings** tab.
13. To use a proxy server for the codec, for the **Use Proxy** setting, select **Open**.
14. Select **Confirm** to save the configuration and return to the Settings menu.

Viewing network details

About this task

In the Network section of the One Click Detection screen, you can view the IP addresses and domain names of the codec, gateway, gateway keeper, session border controller, and other detected network devices. In the Detection section, you can view the details on the data packet loss, average network delay, and maximum jitter. You can also learn about the SIP and H.323 account status and the connected peripherals from the Account and Peripherals sections.

Procedure

1. On the Settings menu, select **Detection**.
2. On the One Click Detection screen, view the network connection, SIP and H.323 account, and peripheral details.
3. On the remote control, press **Back** to return to the Settings menu.

Configuring audio settings

About this task

Configure the basic audio settings, including available audio inputs and outputs and their volume level, incoming call ringtone, and microphone settings. You can also enable the 3A algorithm so that third-party applications can use the codec 3A for audio processing. 3A combines three algorithms: Acoustic Echo Cancellation (AEC), Background Noise Suppression (ANS), and Automatic Gain Control (AGC).

Procedure

1. On the Settings menu, select **Audio**.
2. On the Audio screen, from the **Audio Input** list, select one of the following options:
 - **Auto**: The codec automatically determines the audio input.
 - **Customize**: You can manually select the audio input to use.
3. If you selected the manual setting for the audio input, select the audio inputs that you want to use.
4. For the **Input Detection** setting, select **Detection** to speak into the microphone and test the audio input.
5. For the **Input Volume** setting, select the volume level for the audio input.
6. From the **Audio Output** list, select one of the following options:
 - **Auto**: The codec automatically determines the audio output.
 - **Customize**: You can manually select the audio output to use.
7. For the **Output Volume** setting, select the volume level for the audio output.

8. From the **Ring** list, select the ringtone for an incoming call.
9. To allow third-party applications to use the codec 3A audio processing, toggle on the **APP 3A** switch.

Installing third-party applications is not currently supported.

10. On the remote control, press **Back** to return to the Settings menu.

Configuring video settings

About this task

Configure the basic video settings, including video input and output sources and resolution, pan, tilt, and zoom (PTZ) for a connected camera, and video image mode. You can also enable media optimization for a smoother video image and configure PTZ presets for the camera.

Procedure

1. On the Settings menu, select **Video**.
2. In the Mainstream Input and Presentation Input sections, from the **Signal Source** list, select the video signal source for the main video and presentation inputs.

The resolution value updates depending on the selected input and the connected device. For Avaya Room System C190, the Camera Compose input is the combination of HDMI 1 and HDMI 2 inputs.
3. In the Video Output HDMI1 and Video Output HDMI2 sections, from the **Output Mode** list, select the output signal source.
4. For the **Resolution** setting, select the video output resolution.
5. To reduce jitter and achieve a smoother video image, toggle on the **Media Optimization** switch.
6. In the Camera Settings section, for the **Focusing** setting, select **Start**.

The GUI menu displays the real-time video screen, and you can manage the pan, tilt, and zoom settings.
7. After adjusting the PTZ settings, on the remote control, press **Back** to return to the Video screen.
8. For the **Image Mode** setting, select the video image mode corresponding to your location and lighting conditions.

For example, you can select **Outdoor** for sporting events and outdoor conferences.
9. For the **Preset Position** setting, select **Edit**.
10. On the Preset Position screen, select the slot to configure and save a PTZ preset.

11. On the real-time video screen, adjust the C130 or C170 PTZ settings with the remote control and select **Save**.
12. To access the camera OSD menu on C130 or C170, for the **Built-in Menus** setting, select **Camera**.
13. To disable the camera when the codec is in an idle state, toggle on the **Turn Off Camera When Idle** switch.
14. To disable the camera by default when joining a conference call, toggle on the **Join And Turn Off The Camera** switch.
15. On the remote control, press **Back** to return to the Settings menu.

Configuring layout settings

About this task

You can select the video output and the layout for it to use in Presentation and Conference modes. For example, for Presentation mode, the codec takes the video from the local source, remote video, and presentation and sends them to the HDMI output using the layout that you selected. You determine the layout options available for selection from the Video submenu of the Settings web interface menu.

Procedure

1. On the Settings menu, select **Layout**.
2. At the top of the Layout screen, select the video output for which you want to configure the layout.
3. On the Presentation Layout and Conference Layout tabs, select the layout to use for the video output.
4. On the remote control, press **Back** to return to the Settings menu.

Viewing codec details

About this task

You can view general codec information from the Settings menu, such as the device model, serial number, MAC address, software version, and check code.

Procedure

1. On the Settings menu, select **About**.
2. On the About screen, view the codec details.
3. On the remote control, press **Back** to return to the Settings menu.

Performing a factory reset

About this task

Restore the codec software to the factory settings. Perform this procedure with caution: after the factory reset, all the configured settings will be reset to their default values and all customized or stored data will be lost.

If saving the account and IP information is enabled on the web interface Settings menu, these details are retained after the factory reset. You can check if this is enabled by going to **Settings > Others > Factory Reset**.

TLS certificates get deleted after a factory reset regardless of the reset option that you choose.

Procedure

1. On the Settings menu, select **About**.
2. On the About screen, for the **Reset to Factory Settings** setting, click **Start**.
3. In the confirmation dialog box, select **Confirm**.

The codec restarts to complete the factory reset.

Upgrading the codec software

About this task

You can obtain the codec software updates from a server or a USB drive. Depending on the option that you select, the codec automatically detects if there is a newer version of the upgrade file available and starts the upgrade process.

Important:

Do not power off the codec during the upgrade process as this action might corrupt the file system and require a factory reset.

Before you begin

Ensure the following:

- If you want to obtain the upgrades from a USB drive, upload the `update.xml` and `<codec model>-ota-AVAYA-v<version>.zip` files to its root directory and insert it into a USB slot on the back panel.
- If you want to obtain the upgrades from an HTTP server, specify the server IP address and the folder with the upgrade files in the Others submenu of the Settings web interface menu. For more information about the upgrade process flow, prerequisites, and the web interface configuration, see [Upgrade process for Avaya Room System C100 Series](#) on page 89 and [Upgrading the codec software](#) on page 91.

Procedure

1. On the Settings menu, select **About**.

2. On the About screen, do one of the following:

- To obtain the upgrade file from an HTTP server, for the **Remote Upgrade** setting, click **Start**.
- To obtain the upgrade file from a USB drive, for the **USB Upgrade** setting, click **Start**.

The codec restarts to complete the upgrade process.

Chapter 5: Configuration in the web interface

Web interface Settings menu overview

You can access the web interface by entering the codec IP address in the Google Chrome browser. The web interface supports only an HTTPS connection and converts HTTP links into HTTPS. Before accessing the codec web interface, ensure that the HTTPS connection is enabled from the GUI menu. For more information about enabling the web interface connection, see [Configuring global settings](#) on page 43.

Google Chrome is the supported browser for codec administration and configuration. In certain instances, Google Chrome might cache web interface pages, preventing you from viewing all the available details. If that occurs, press `Ctrl+F5` to refresh the page and view up-to-date information.

The Settings menu is located at the bottom of the web interface side pane. If the system administrator password is enabled, you need to enter it to access the Settings menu.

The following table lists the Settings menu subtabs and describes the configuration you can perform from them:

Subtab name	Description
Network	Configure IP, firewall, quality of service, and SNMP settings. For IP configuration, you can use DHCP address assignment or set a static IP address. When configuring SNMP parameters, you can select version 1, 2c, or 3.
Account	Set up the codec display name for calls and configure account settings. For H.323, and SIP accounts, you can unregister an unused account or manually configure the settings for authentication and calling. The device management platform configuration from the MQTT Configuration subtab is not currently supported.
Call	Configure calling features and parameters, such as Auto Answer, call blocking with incorrect SIP passwords, and obtaining a presentation from the secondary video stream. You can also configure the codec as a multipoint control unit (MCU) to use video conferencing features.

Table continues...

Subtab name	Description
Audio	Configure audio input and output settings, echo elimination, USB audio, and digital microphone. You can also select audio codecs. When configuring audio input and output, you can enable one or more channels to use different audio devices with the codec. With echo elimination features, you can eliminate echo, unwanted background noises, and repetitive sounds.
Video	Set up video input and output, screen layout, and video encoding. From the HDMI-1 Layout or HDMI-2 Layout subtabs, you can determine what screen layouts are available for selection on the Layout GUI menu.
Record	Choose between the Real-time Messaging Protocol (RTMP) and H.323 protocols for recording audio and video received from cameras. You can also save the recorded video on a USB drive and select the recording mode.
Security	Configure global security settings, import a PKCS #12 certificate bundle, and set up H.323 and SIP encryption. Global security settings include TLS version, USB mode, administrator password for the Settings menu, and screensaver. From the Security subtab, you can also add an IP address to the blocklist to prevent the use of non-secure and outdated IP addresses for web interface access.
Protocol	Enable H.323 and SIP protocols and configure the related settings to call inbound and outbound phone numbers. When configuring the H.323 protocol, you can also enable H.239 for dual video streaming.
Subtitles	Set up the codec name, banner, and scrolling captions to show on top of the video output coming from the codec. You can also define the position of each type of text relative to the central horizontal and vertical lines of the video, ensuring that the texts do not overlap.
Language	Change the web interface language for easier configuration. When you select the new language, the web interface reloads and then displays the Login page in the selected language. You can also change the web interface language from the Login page.
Others	Set up the codec date and time, logging levels, export and import the current configuration, upgrade the codec software, and perform a factory reset. Before upgrading the Avaya Room System C100 Series software, read carefully Upgrade process for Avaya Room System C100 Series on page 89 and choose the upgrade method applicable to your environment. Adding applications to the allowlist from the White List subtab is not currently supported.

Related links

[Administering Avaya Room System C100 Series from the web interface](#)

Changing the web interface language before logging in

About this task

You can select your preferred language for the web interface from the menu before signing in to your account.

Before you begin

Ensure that you have the codec IP address to access the Login page.

Procedure

1. In the Google Chrome browser, enter the codec IP address in the following format:

`https://<IP address>:port.`

The default port number for the HTTPS connection is 65443. For example, you can enter

`https://<IP address>:65443.`

2. At the top of the Login page, click the language drop-down list and select the language.

The web interface language reloads the Login page and displays it in the selected language.

Accessing the web interface

About this task

You can access the web interface from a Google Chrome browser using the codec IP address. After logging in to the web interface, you can see the side navigation pane and the Place A Call page.

If you log in to the web interface for the first time, you are required to change the default password and re-enter the new credentials. After you enter the default credentials, the web interface automatically displays the window to change the password and then redirects you to the Login page again. You must change the default password to protect your configuration data in case of a security breach.

Before you begin

Ensure you do the following:

- Enable the HTTPS web interface connection from the GUI menu. For more information about enabling the web interface connection, see [Configuring global settings](#) on page 43.
- Obtain the codec IP address to access the web interface.
- Obtain the web interface username and password. You can get the default username and password from the release notes.

Procedure

1. In the Google Chrome browser, enter the codec IP address in the following format:

`https://<IP address>:port.`

Configure an HTTPS connection for the web interface from the System Security page on the Settings menu.

The default port number for the HTTPS connection is 65443. For example, you can enter `https://<IP address>:65443`.

2. On the Login page, enter your username and password.
3. **(Optional)** To clear the entered username and password and re-enter them, click **Reset**.
4. **(Optional)** If you do not want to enter the username and password at the next login, select the **Remember Account** check box.
5. Click **Login**.
6. Do one of the following:
 - If you have already changed the default password, proceed with the codec configuration.
 - If you log in to the web interface for the first time, continue with steps 7–9 to change the default password.

7. In the **Original password** field, type the default password.

8. In the **Latest password** and **Verify password** fields, type the new password.

You must type a password that is 8 to 16 characters long, including upper- and lower-case letters, numbers, and special characters.

9. Click **OK**.

The web interface redirects you to the Login page, and you must re-enter the credentials with the new password.

Changing the web interface language from the Settings menu

About this task

You can change the language of the web interface menu from the Settings menu when performing the codec configuration.

Before you begin

Ensure that you have the Settings menu password.

Procedure

1. On the Settings menu, go to **Language**.
2. On the Language page, select the web interface language.

The web interface reloads and then displays the Login page in the selected language.

Global settings

Configuring the codec display name for calls

About this task

You can configure the codec name to display during calls and on the incoming call window. You can also select the encoding and decoding types to display the codec name correctly.

Procedure

1. On the Settings menu, go to **Account > Display Name**.
2. On the Display Name page, in the **Terminal Name** field, type the codec display name.
3. For the **H.323 Displays Name Encoding As** setting, select one of the following options:
 - **Unicode**: To use the Unicode encoding for the codec name.
 - **GBK**: To use the GBK, or character, encoding for the codec name.
4. For the **H.323 Displays Name Decoding As** setting, select one of the following options:
 - **Auto**: The codec automatically determines the decoding type for the display name.
 - **Unicode**: To use the Unicode decoding for the codec name.
 - **GBK**: To use the GBK, or character, decoding for the codec name.
5. Click **Save**.

Configuring an H.323 account

About this task

Configure the H.323 account to make calls from the codec using the H.323 protocol. You can also unregister the account or pre-configure and disable it.

Procedure

1. On the Settings menu, go to **Account > H323 Account**.
2. On the H323 Account page, to make calls using the H.323 account, toggle on the **Enable H.323** switch.
3. For the **Way Of Collocation** setting, select one of the following options:
 - **Manual**: To manually configure the H.323 account.
 - **Unregister**: To unregister the account from the call server.
4. If you selected manual configuration, in the **Gatekeeper Address** field, type the IP address of the gatekeeper.
5. In the **Registered Name** field, type the name that gatekeepers and gateways use to identify the codec.
6. In the **Terminal Number** field, type the H.323 extension.

7. In the **Username** field, type the username for H.235 authentication.
8. In the **Password** field, type the password for H.235 authentication.
9. Click **Save**.

Configuring a SIP account

About this task

Configure the SIP account to make calls from the codec using the SIP protocol. You can also specify the name and realm for SIP authentication and an alternative proxy server to use in case the default server is unavailable.

Procedure

1. On the Settings menu, go to **Account > SIP Account**.
2. On the SIP Account page, to make calls using the SIP account, toggle on the **Enable SIP** switch.
3. For the **Way Of Collocation** setting one of the following options:
 - **Manual**: To manually configure the SIP account.
 - **Unregister**: To unregister the account from the call server.
4. If you selected manual configuration, for the **Transport Protocol** setting, select one of the following options:
 - **Auto**: The codec automatically determines the protocol to use for SIP calls.
 - One of the protocols for SIP calls, including TCP, UDP, and TLS.
5. In the **Username** field, type the SIP username to authenticate the device before a VoIP session.
6. In the **Password** field, type the SIP password.

The password must match the password value specified on the SIP server to authenticate the codec successfully.
7. In the **Proxy Server** field, type the IP address of the proxy server.
8. Skip the **Alternate Proxy Server** field as the alternative proxy server is not currently supported.
9. In the **Authentication Username** field, type the username to determine that the device is part of the SIP profile.
10. In the **Authentication Realm** field, type the IP address or domain name of the server, gateway, or session border controller to use for SIP authentication.
11. Click **Save**.

Configuring global security settings

About this task

Configure global security settings, such as TLS version, USB mode, administrator password for the Settings menu, and screensaver. You can configure an HTTPS and SSH connection for the web interface. You can also disable the Wi-Fi capability to configure the web interface settings only through an Ethernet connection.

Procedure

1. On the Settings menu, go to **Security > System Security**.
2. On the System Security page, for the **TLS** setting, select the TLS protocol version.
To apply the new TLS protocol version, after clicking **Save**, go to **Settings > Account > SIP Account** and toggle the **Enable SIP** switch off and on.
3. For the **USB Management** setting, select one of the following options:
 - **USB Enabled:** To enable data exchange with a USB drive or connection to a USB device, such as a keyboard or mouse.
 - **External Data Storage Disabled:** To connect to a USB device, such as a keyboard or mouse, and disable data exchange with a USB drive.
 - **USB Disabled:** To disable data exchange with a USB drive and connection to USB devices.
4. To set the number of failed login attempts after which your web interface account gets locked, select the **Failed Login Attempt Lockout** check box.
5. If you enable failed login attempt configuration, for the **Login Attempts Limit** setting, select the number of failed login attempts before locking your account.
After a configured number of failed login attempts, you must reactivate the HTTPS connection to the web interface. For more information, see [Configuring global settings](#) on page 43.
6. To set an expiration time for the web interface password, select the **Enable Password Expiry** check box.
7. If you enable password expiration time configuration, for the **Password Expiry Period** setting, select the number of days after which you need to change your web interface password.
8. To enable an HTTPS connection for the web interface, select the **Enable WEB Service** check box.
9. If you enable an HTTPS connection, in the **WEB Access Password** field, type the web interface password.
You must type a password that is 8 to 16 characters long, including upper- and lower-case letters, numbers, and special characters.
10. After enabling an HTTPS connection, in the **WEB Port** field, type the HTTPS port number.

11. To enable an SSH connection for the web interface, select the **Enable SSH Service** check box.

You can enable and access an SSH connection only under the guidance of Avaya Support personnel.

12. If you enable an SSH connection, in the **SSH Access Password** field, type the web interface password, and in the **SSH Port** field, type the SSH port number.

13. To enable the administrator password for the Settings menu, select the **Enable Admin Password** check box.

You enter the administrator password only once during a login session before accessing the Settings menu. Enable the administrator password to secure your administering level configurations.

14. If you enable the administrator password, in the **Admin Password** field, type the password for the Settings menu.

You must type a password that is 8 to 16 characters long, including upper- and lower-case letters, numbers, and special characters.

15. To enable a screensaver for the web interface, select the **Enable Screensaver** check box.

16. If you enabled the screensaver, for the **Start Screensaver Time** setting, select the screen idle time after which the screensaver is activated.

17. To lock the computer screen after the screensaver time elapses, select the **Enable Lock Screen** check box.

18. If you enable the lock screen, in the **PIN** field, type a PIN code to unlock the screen.

19. To disable the Wi-Fi capability for the codec, select the **Disable WiFi** check box.

If you purchase an Avaya Room System C190 model without the Wi-Fi capability, this setting is unavailable.

20. Click **Save**.

Device management platform configuration

From the device management platform, you can view the basic codec information and manage the device remotely. To connect to the platform, you must specify the platform URL, username, and password for authentication and select the MQTT protocol type. The codec automatically connects to the platform after you save the configuration.

Skip the MQTT Configuration subtab when configuring the codec as this functionality is not currently supported.

Call settings

Configuring call options

About this task

On the Call Options page, you can enable call features, such as Auto Answer and requesting a password for incoming calls. You can also select the protocol to use during calls, configure DNS lookup and other network settings. To achieve the best video and presentation quality, you can select the appropriate mode for primary and secondary video streams.

Procedure

1. On the Settings menu, go to **Call > Call Options**.
2. On the Call Options page, to enable the Auto Answer feature for incoming calls, select the **Auto Answer** check box.

If you disable Auto Answer, you receive a dialog box for each incoming call to the codec, requesting you to accept the call. With Auto Answer enabled, all incoming calls are automatically answered, and you do not need to accept them.

3. To set up a password for incoming calls, select the **Refuse The Incoming-call Automatically When The Password Does Not Match** check box.

You can define the password for incoming calls for security purposes. To call the codec, the user must dial `<codec IP address>##**<password>`. The codec blocks the incoming calls with non-matching or missing passwords.

4. If you enabled the password for incoming calls, in the **Incoming-call Password** field, type the password.

You can type a maximum of 32 alphanumeric characters.

5. To use the secondary video stream when there is an active presentation from another codec or video endpoint during a conference, select the **Grab Presentation** check box.

When **Grab Presentation** is not enabled, the secondary video stream must be idle before the codec can take control.

This feature applies to H.323-based conferences. When using the SIP protocol, the codec can take control of the secondary video stream at any time.

6. To manage remote cameras during a call, select the **Enable Farcamera Control** check box.
7. To translate readable domain names to IP addresses and port numbers through DNS SRV records, select the **Enable Lookup From DNS SRV Record** check box.
8. For the **Default Call Type** setting, select one of the following options:
 - **Auto**: The codec automatically defines the protocol to use for calls.
 - **H.323**: To use the H.323 protocol for calls.
 - **SIP**: To use the SIP protocol for calls.

9. For the **Default Call Rate** setting, select the default call bandwidth in kilobits per second.
10. For the **Maximum Transmission Bandwidth** setting, select the maximum bandwidth for transmitting data during calls.
11. For the **Maximum Receiving Bandwidth** setting, select the maximum bandwidth for receiving data during calls.
12. For the **Presentation Bandwidth Percentage** setting, select the bandwidth percentage that the codec takes from the main video stream bandwidth and uses for presentations.
13. For the **Primary Video Mode** setting, select one of the following options:
 - **Clear**: To prioritize image resolution for the primary video.
 - **Smooth**: To prioritize frame rate for the primary video.
 - **Very Smooth** (only for Avaya Room System C190): To achieve the highest possible frame rate at up to 60fps for the primary video.
14. For the **Secondary Video Mode** setting, select one of the following options:
 - **Clear**: To prioritize image resolution for the secondary video.
 - **Smooth**: To prioritize frame rate for the secondary video.
 - **Very Smooth** (only for Avaya Room System C190): To achieve the highest possible frame rate at up to 60fps for the secondary video.
 - **PPT**: To prioritize presentation quality for the secondary video.
15. For the **Media Waiting Time** setting, select the waiting time in seconds to establish a media session between the endpoints.
16. For the **I Frame Requests Filter Time** setting, select the filter time in seconds for intra-frame (I-frame) requests.
17. For the **Interval Time of IDR Frame** setting, select the time interval between two I-frames.
18. Click **Save**.

Configuring the codec as an MCU

About this task

You can configure the codec as a multipoint control unit (MCU) and use the corresponding features for video conferencing, including audio and video mixing and transcoding. You can also select the appropriate conference mode for a live discussion or lecture.

For more information about using MCU conferencing features, see the Call Operations chapter in *Using Avaya Room System C100 Series*.

Before you begin

Ensure that you have purchased an MCU license from Avaya before proceeding with this configuration. For more information about purchasing the MCU license, contact Avaya Support.

Procedure

1. On the Settings menu, go to **Call > EMCU**.
2. On the EMCU page, for the **EMCU Authentication** setting, click **Import**.
3. In the new window, browse to the location of the license file and select it.
4. To test the EMCU connection for 20 minutes, select the **Try MCU(20 minutes)** check box.
5. If you selected to test the EMCU connection, for the **Conference Mode** setting, select one of the following options:
 - **Discussion Mode**: All conference participants can hear and talk to each other.
 - **Lecture Mode**: The codec identifies only one video source as the primary one, all other participants can hear its audio and view the presentation but cannot talk to each other.
6. Click **Save**.

Audio settings

Configuring audio input

About this task

You can enable and configure one or more audio inputs, including LINE IN, HDMI, and microphone inputs. The HDMI and microphone settings vary depending on your codec model. You can also select an audio input to use for presentations and mute all incoming audio during conferences.

Procedure

1. On the Settings menu, go to **Audio > Audio Input**.
2. On the Audio Input page, for the **Input Volume** setting, select the level of the audio input volume.
3. To enable and adjust the LINE IN audio input, select the **Enable Linear In** check box.
4. If you enabled the LINE IN audio input, for the **Linear Input Digital Gain** setting, select the level of digital signal amplification for this input.
5. Do one of the following:
 - For C130 and C170, select the **Enable HDMI-IN** check box to enable and adjust the HDMI audio input.
 - For C190, select the **Enable HDMI1 Audio In** check box to enable and adjust the HDMI 1 audio input.
6. If you enabled the HDMI or HDMI 1 audio input, select the level of digital signal amplification for this input.

7. For C190, to enable and adjust the HDMI 2 audio input, select the **Enable HDMI2 Audio In** check box and select the input signal level.
8. Do one of the following:
 - For C130 and C170, select the **Enable Inner Mic Audio In** check box to enable and adjust the built-in microphone audio input.
 - For C190, select the **Enable Cannon-mic Audio In** check box to enable and adjust the MIC IN audio input to which you attached a microphone with a cannon cable.
9. If you enabled the microphone audio input, select the level of digital signal amplification for this input.
10. For C170, select the **Enable Mini Canon-mic audio in** check box to enable and adjust the MIC IN audio input to which you attached a microphone with a cannon cable.
11. Do one of the following:
 - For C130 and C170, select the **Take hdmiin as presentation audio** check box to use the HDMI input audio for presentations.
 - For C190, select the **Take HDMI IN2 As Presentation Audio** check box to use the HDMI 2 input audio for presentations.
12. To use the audio from the LINE IN input for presentations, select the **Take LINE IN As Presentation Audio** check box.
13. To mute the codec audio during conferences, select the **Mute During Conference** check box.
14. Click **Save**.

Configuring audio output

About this task

On the Audio Output page, you can adjust the overall audio output level and enable one or more audio outputs, including LINE OUT, HDMI 1, and HDMI 2. You can also determine to what outputs to send the audio coming from different inputs.

Procedure

1. On the Settings menu, go to **Audio > Audio Output**.
2. On the Audio Output page, for the **Audio Output Digital Gain** setting, select the level of digital signal amplification for the audio output.
3. To adjust the level of output tone, select the **Output Tone** check box.
4. If you enabled the output tone adjustment, for the **Ring Out Gain** setting, select the level of digital signal amplification.
5. For C130, to use the built-in speakers as the audio output, select the **Enable Speaker Audio Out** check box.
6. To use the HDMI 1 output as the audio output, select the **Enable HDMI-1 Audio Out** check box.

7. To use the HDMI 2 output as the audio output, select the **Enable HDMI-2 Audio Out** check box.
8. To use the LINE OUT output as the audio output, select the **Enable Linear Out** check box.
9. Scroll to the top of the Audio Output page and select the **Show Advanced Settings** check box.
10. Configure advanced audio output settings.
11. Click **Save**.

C130 Audio Output advanced settings

The following table lists the settings available on the Audio Output page when you select the **Show Advanced Settings** check box in the Avaya Room System C130 web interface:

Setting name	Description
Enable Speaker Including LINE IN	Select to send the LINE IN audio to the built-in speaker output.
Enable Speaker Including HDMI IN	Select to send the HDMI In audio to the built-in speaker output.
Enable HDMI-1 Including LINE IN	Select to send the LINE IN audio to the HDMI 1 output.
HDMI-1 Output Contains HDMI-IN	Select to send the HDMI input audio to the HDMI 1 output.
Enable HDMI-2 Including Line In	Select to send the LINE IN audio to the HDMI 2 output.
Enable HDMI-2 including HDMI in	Select to send the HDMI input audio to the HDMI 2 output.
Enable LINE OUT Left Channel Including Inner MIC In	Select to send the built-in microphone input audio to the LINE OUT left channel.
Linear Output Left Channel Including Linear Input	Select to send the LINE IN audio to the LINE OUT left channel.
Enable LINE OUT Right Channel Including INNER MIC In	Select to send the built-in microphone input audio to the LINE OUT right channel.
Linear Output Right Channel Including Linear Input	Select to send the LINE IN audio to the LINE OUT right channel.
Innemic reference delay	Select the delay time in milliseconds to send the audio received from the built-in microphones to the output device.
Speaker reference delay	Select the delay time in milliseconds for audio playback on built-in speakers.

C170 Audio Output advanced settings

The following table lists the settings available on the Audio Output page when you select the **Show Advanced Settings** check box in the Avaya Room System C170 web interface:

Setting name	Description
Enable HDMI-1 Including Microphone	Select to send the MIC IN audio to the HDMI 1 output.
Enable HDMI-1 Including LINE IN	Select to send the LINE IN audio to the HDMI 1 output.
HDMI-1 Output Contains HDMI-IN	Select to send the HDMI input audio to the HDMI 1 output.
Enable HDMI-2 Including Microphone	Select to send the MIC IN audio to the HDMI 2 output.
Enable HDMI-2 Including Line In	Select to send the LINE IN audio to the HDMI 2 output.
Enable HDMI-2 including HDMI in	Select to send the HDMI input audio to the HDMI 2 output.
Linear Output Left Channel Including Mini Canon Mic Input	Select to send audio received from the microphone that you attached with a cannon cable to the LINE OUT left channel.
Enable LINE OUT Left Channel Including Inner MIC In	Select to send the built-in microphone input audio to the LINE OUT left channel.
Linear Output Left Channel Including Linear Input	Select to send the LINE IN audio to the LINE OUT left channel.
Linear Output Right Channel Including Mini Canon Mic Input	Select to send audio received from the microphone that you attached with a cannon cable to the LINE OUT right channel.
Enable LINE OUT Right Channel Including INNER MIC In	Select to send the built-in microphone input audio to the LINE OUT right channel.
Linear Output Right Channel Including Linear Input	Select to send the LINE IN audio to the LINE OUT right channel.
Speaker reference delay	Select the delay time in milliseconds for audio playback on built-in speakers.

C190 Audio Output advanced settings

The following table lists the settings available on the Audio Output page when you select the **Show Advanced Settings** check box in the Avaya Room System C190 web interface:

Setting name	Description
Enable HDMI-1 Including LINE IN	Select to send the LINE IN audio to the HDMI 1 output.
Enable HDMI-1 Including HDMI2 IN	Select to send the HDMI 2 input audio to the HDMI 1 output.
Enable HDMI-1 Including Microphone	Select to send the MIC IN audio to the HDMI 1 output.
Enable HDMI-2 Including Line In	Select to send the LINE IN audio to the HDMI 2 output.
Enable HDMI-2 Including HDMI2 IN	Select to send the HDMI 2 input audio to the HDMI 2 output.
Enable HDMI-2 Including Microphone	Select to send the MIC IN audio to the HDMI 2 output.
Enable Line Out Left Channel Including Microphone	Select to send the MIC IN audio to the LINE OUT left channel.
Linear Output Left Channel Including Linear Input	Select to send the LINE IN audio to the LINE OUT left channel.
Line Output Left Channel Including Remote Audio	Select to send the remote audio to the LINE OUT left channel.
Enable Line Out Right Channel Including Microphone	Select to send the MIC IN audio to the LINE OUT right channel.
Linear Output Right Channel Including Linear Input	Select to send the LINE IN audio to the LINE OUT right channel.
Linear Output Right Channel Including Remote Audio	Select to send the remote audio to the LINE OUT right channel.

Setting up echo elimination

About this task

During online meetings and conferences, echo might occur when the sound from a speaker is picked up by a microphone and retransmitted. The created sound loop might disrupt communication. You can eliminate echo, unwanted background noises, voices, and repetitive sounds using the AI Voice Noise Reduction, Acoustic Echo Cancellation, Automatic Gain Control, and Active Noise Reduction features.

Procedure

1. On the Settings menu, go to **Audio > Echo Elimination**.
2. For C130 and C170, to enable echo elimination for the built-in microphones, select the **Enable Echo Elimination On The Input Of Microphone** check box.

3. To enable echo elimination for the LINE IN input, select the **Enable Echo Elimination On Linear Input** check box.
4. To enable the AI Voice Noise Reduction feature, select the **Enable AI Voice Noise Reduction** check box.

With AI Voice Noise Reduction, you can remove unwanted background voices and echos.

5. At the top of the Echo Elimination page, select the **Show Advanced Settings** check box.
6. To enable Acoustic Echo Cancellation (AEC), select the **Enable AEC** check box.

AEC eliminates the echo or feedback during audio and video conferencing.

7. To enable Automatic Gain Control (AGC), select the **Enable AGC** check box.

AGC determines the volume level of audio signals and makes the output consistent even if input levels vary.

8. If you enabled automatic gain control, for the **Auto Gain** setting, select the audio signal volume level.
 9. To enable Active Noise Reduction (ANR), select the **Enable ANR** check box.
- ANR reduces unwanted background noises from an audio signal. You can use ANR for eliminating continuous and predictable noises.
10. To detect if participants are on physical mute, select the **Enable Mute Detection** check box.
 11. If you enabled mute detection, for the **Silence detection mode** setting, select one of the following options:

- **Adaptive:** The codec determines the audio threshold value.

The codec uses the specified threshold value as the starting point and then adjusts it depending on the average audio level of call participants.

- **Fixed:** You can manually select the audio threshold value.

All participants with an audio level above the threshold are identified as muted.

12. For the **Silence detection threshold** setting, select the audio threshold value.
13. Click **Save**.

Configuring USB audio

About this task

You can configure the audio for the USB input and output and determine if other microphones or output devices are muted when a USB microphone is connected to the codec. You can also enable automatic echo cancellation for a USB microphone or echo elimination for the USB audio input.

Procedure

1. On the Settings menu, go to **Audio > USB Audio**.

2. On the USB Audio page, to enable the USB port as the audio input, select the **Enable USB Audio In** check box.
3. To enable the USB port as the audio output, select the **Enable USB Audio Out** check box.
4. To mute other microphones when a USB microphone is connected to the codec, select the **Mute Other Microphone When USB Phone Connected** check box.
5. To use only the connected USB audio output device, do one of the following:
 - For C130, select the **Mute HDMI-OUT And SPEAKER When USB Phone Connected** check box to mute the audio from the HDMI output and built-in speaker when a USB microphone is connected to the codec.
 - For C170 and C190, select the **Mute HDMI-OUT When USB Phone Connected** check box to mute the audio from the HDMI output when a USB microphone is connected to the codec.
6. To enable automatic echo cancellation for the connected USB microphone, select the **Auto Echo Cancellation On USB Microphone** check box.

Automatic echo cancellation eliminates the echo during audio and video conferencing. You can disable automatic echo cancellation on the codec if you are already using echo cancellation on the connected microphone and speakers.
7. If you disabled automatic echo cancellation for the USB microphone, to eliminate echo for the USB audio input, select the **Enable Echo Elimination On USB Audio Input** check box.
8. Scroll to the top of the USB Audio page and select the **Show Advanced Settings** check box.
9. To send the USB input audio to the HDMI 1 output, select the **Enable HDMI-1 including USB audio in** check box.
10. To send the USB input audio to the USB output, select the **USB output contains USB audio input** check box.
11. Click **Save**.

Configuring audio codecs

About this task

From the web interface, you can select the codecs to use for compressing and decompressing your audio.

Procedure

1. On the Settings menu, go to **Audio > Audio Capabilities**.
2. On the Audio Capabilities page, select the audio codecs to use.
3. Click **Save**.

Configuring the digital microphone

About this task

You can configure the digital microphone settings, including the volume level, noise and echo suppression, double talk sensitivity, and reverberation time.

Procedure

1. On the Settings menu, go to **Audio > Digital Mic**.
2. On the Digital Mic page, select the **Enable** check box.
3. For the **Volume Adjusting** setting, select the level of the digital microphone volume.
4. For the **Auto Gain** setting, select the level of audio signal amplification.
5. For the **Noise Intensity Suppression** setting, select the noise suppression level for the digital microphone audio.
6. For the **Echo Intensity Suppression** setting, select the echo suppression level for the digital microphone audio.
7. For the **Double-Talk Detection Level** setting, select the sensitivity level to detect double talk.

Double talk occurs when near-end and far-end call participants are talking at the same time.

8. For the **RT60** setting, select the reverberation time in milliseconds.

Reverberation time determines the time duration by which the emitted audio decreases by 60 dB.

9. Click **Save**.

Video settings

Adding a video input

About this task

For Avaya Room System C190, you can add an RTSP address of the camera or another streaming device, such as a broadcasting server, to send a feed to the codec. The device RTSP address has the following format: `rtsp://<device IP address> or rtsp://<device IP address>:<port number>`.

Procedure

1. On the Settings menu, go to **Video > Video Input**.
2. On the Video Input page, in the **VCH** field, type the RTSP address of the camera to receive the feed.

3. Click **Save**.

Configuring video output

About this task

Configure video output settings to determine the resolution for HDMI-1 and HDMI-2 outputs, set the presentation parameters, and enable Extended Display Identification Data (EDID).

Procedure

1. On the Settings menu, go to **Video > Video Output**.
2. On the Video Output page, for the **HDMI-1 Resolution** setting, select the resolution for the HDMI-1 output.
3. For the **HDMI-2 Resolution** setting, select the resolution for the HDMI-2 output.
4. To automatically send a presentation from the device connected to the HDMI output, select the **Send Presentation Automatically** check box.
5. To preview a presentation on the device connected to the HDMI output, select the **Auto Start Preview When Presentation Has Signal** check box.
6. To display a presentation on the device connected to the HDMI output, select the **Show Presentation** check box.
7. To enable Extended Display Identification Data (EDID), select the **Enable Edid** check box.
The EDID standard determines the data exchange between the codec and a display.
8. Click **Save**.

Configuring a screen layout for an HDMI output

About this task

On the HDMI-1 Layout or HDMI-2 Layout web interface page, you can determine what screen layouts are available for selection in Presentation and Conference modes. After configuring the layout options, you can select the screen layout for both modes from the Layout menu in the GUI settings.

Procedure

1. Depending on which HDMI output layout you want to configure, on the Settings menu, go to **Video > HDMI-1 Layout** or **Video > HDMI-2 Layout**.
2. To make available Picture-on-Picture (PoP) layouts, select the **Enable POP** check box.
On the Layout GUI menu, you get the layouts with a larger window and smaller ones outside of the main window. You can switch between the windows to determine which video to make the main one.
3. To make available Picture-in-Picture (PiP) layouts, select the **Enable PIP** check box.

On the Layout GUI menu, you get the layouts with a larger window and smaller ones within the main window. You can switch between the windows to determine which video to make the main one.

4. To make available equally sized layouts, select the **Enable Equal Size Layout** check box.

On the Layout GUI menu, you get the layouts with equally sized windows.

5. For the **Layout When Idle With Presentation** setting, select the screen layout when the presentation is active, there is no call, and **Presentation Preview** is enabled in **Control > Presentation**.
6. For the **Without Presentation** setting, select the screen layout without an active presentation.
7. For the **With Presentation** setting, select the screen layout with a presentation.
8. Click **Save**.

Configuring video codecs

About this task

From the web interface, you can select one or more video codecs to use for compressing and decompressing your video. You can use the standard H.264 codec, which is used in most devices, and the H.264 HP video codec, which is compliant with the ITU-T H.264 standard, high profile. To use the H.264 HP codec, you must also enable the H.264 codec.

You can also select the H.265 codec that corresponds to a newer video compression standard.

Procedure

1. On the Settings menu, go to **Video > Video Capabilities**.
2. On the Video Capabilities page, select the video codecs to use.
3. Click **Save**.

Configuring video encoding and decoding

About this task

You can define the encoding and decoding parameters for your video. The camera can encode, or create, video with the built-in processor or using the camera software. The processor also converts the encoded camera stream into the video of the appropriate format. You can determine the resolution of the decoded video.

Procedure

1. On the Settings menu, go to **Video > Encoding**.
2. On the Encoding page, for the **Encoder Type** setting, keep the default option **encoder_camera**.
3. For the **Decoder Resolution** setting, select the decoder resolution value.
4. Click **Save**.

Recording management

You can record audio and video received from remote and built-in microphones and cameras using one of the following methods:

- Real-time Messaging Protocol (RTMP) protocol: to send the recorded data to a streaming server
- H.323 protocol: to send the data to a remote server for storage
- Connected USB drive

You can manage recording options from the Record subtab of the Video tab on the Settings menu. By default, the recording capability is disabled. After configuring RTMP, H.323, or USB recording options, you must enable the corresponding recording type from the Record Control tab of the Control menu in the codec web interface. If required, you can also keep the recording capability disabled. For more information about managing recordings, see the call setup section in [Using Avaya Room System C100 Series](#).

USB recordings are saved in the .MP4 format. If you use an RC212, RC220, or RC240 camera for recording and configure time overlay, the camera timestamp is displayed on the recorded video. You can configure time overlay settings on the Overlay tab of the camera web interface. For more information about configuring video overlay settings, see the web interface section in [Using Avaya Room Camera RC212 and Avaya Room Camera RC220](#) and [Using Avaya Room Camera RC240](#).

Configuring RTMP settings for remote recording

About this task

You can enable and use Real-time Messaging Protocol (RTMP) for recording audio and video received from cameras. A camera captures both audio and video, and then the RTMP encoder breaks them down into data packets and sends them to a streaming server, which transforms the received data for live streaming.

You can determine whether to record local and remote audio, the IP address of the RTMP server, and remote recording mode.

Procedure

1. On the Settings menu, go to **Record > Remote Record**.
2. On the Remote Record page, for the **Record Protocol** setting, select **RTMP**.
3. In the **RTMP Server Address** field, type the IP address of the streaming server.
4. To bind the specified RTMP server address with the SIP username, select the **Auto Complete Address** check box.

For example, if you specify the RTMP server address as `rtmp://1.2.3.4` and the SIP username is 888888, and you select this check box, the address changes to `rtmp://1.2.3.4/live/888888`.

5. For the **Bit Rate** setting, select the bitrate value.

The bitrate value controls the amount of audio and video data processed over some time. A higher bitrate provides better audio and video quality.

6. For the **Audio** setting, select one of the following options:
 - **Local**: Record only the local audio from the room where the codec is installed.
For example, you can select local audio when broadcasting to avoid capturing extra noises.
 - **Local And Remote**: Record both local and remote audio.
For example, you can select local and remote audio when conferencing to capture audio from all the participants.
7. For the **Video** setting, select one of the following options:
 - **HDMI-1 Output**: To record the video from the HDMI 1 output.
 - **Primary Video Source**: To record the video from the primary video source.
8. For the **Start Mode** setting, select one of the following options:
 - **Manual Start**: To manually start a remote recording from the Record Control tab on the Control menu.
 - **Auto Start Once Power On**: To start a remote recording when the codec boots up.
 - **Auto Start Once Conferencing**: To start a remote recording when going into Conference mode.
9. Click **Save**.

Configuring H.323 settings for remote recording

About this task

You can enable and use the H.323 protocol for recording audio and video received from cameras. You can specify the IP address of the server where you want to store the recordings and select the video source.

Procedure

1. On the Settings menu, go to **Record > Remote Record**.
2. On the Remote Record page, for the **Record Protocol** setting, select **H.323**.
3. In the **Record Server Address** field, type the IP address of the server to store the recordings.
4. For the **Video** setting, select one of the following options:
 - **HDMI-1 Output**: To record the video from the HDMI output.
 - **Primary Video Source**: To record the video from the primary video source.
5. To start recording automatically in Conference mode, select the **Auto Start Once Conferencing** check box.
6. Click **Save**.

Configuring recording to a USB drive

About this task

You can record the audio and video received from cameras and store it on a USB drive. You can manage the recording source and mode for security purposes, for example, if you want to limit the data exchange with the USB drive.

You can also enable a digital signature to protect your recording files and specify file transfer server settings to upload the recordings.

Before you begin

Ensure you enable USB data storage. To enable USB data storage, you must go to **Security > System Security** and adjust the **USB Management** setting.

Procedure

1. On the Settings menu, go to **Record > USB Record**.
2. On the USB Record page, for the **Video** setting, select one of the following options:
 - **HDMI-1 Output**: To record the video from the HDMI output.
 - **Primary Video Source**: To record the video from the primary video source.
3. For the **Bit Rate** setting, select the bitrate value.

The bitrate value controls the amount of audio and video data processed over a period of time. A higher bitrate provides better audio and video quality.
4. For the **Record Mode** setting, select one of the following options:
 - **Disable**: To disable recording to a USB drive.
 - **Auto Start Once Power On**: To start recording to a USB drive when the codec is switched on.
 - **Auto Start Once Conferencing**: To start recording to a USB drive in Conference mode.
 - **Manual Start**: To manually start recording to a USB drive.
5. For the **USB Record Time** setting, select the time limit for USB recording.

When the time expires, the USB recording stops. You can use this setting to manage the storage space.
6. To protect your video with a digital signature, select the **Enable Digital Signature** check box.
7. For the **USB Record Digital Signature Algorithm** setting, select the algorithm to use for the digital signature.

The default algorithm is MD5.
8. To automatically upload completed recordings to a file transfer server, select the **Enable Record File Upload** check box.
9. For the **Record File Upload Protocol** setting, select the protocol to use for file transfer.

10. In the **Record File Upload Server Addr** field, type the IP address of the file transfer server.
11. In the **Record File Upload Username** field, type the username to use for server access.
12. In the **Record File Upload Password** field, type the password to use for server access.
You can see the status of the connected file transfer server at the bottom of the page.
13. Click **Save**.

Next steps

Go to **Control > Record Control** to enable USB recording and access the recording files. For more information about enabling USB recording and managing recording files, see the Call setup chapter in *Using Avaya Room System C100 Series* or go to [Managing call recording](#).

Network settings

Configuring IP settings

About this task

Configure the IP network parameters for the codec and determine if you want to use automatic DHCP assignment or manually specify the IP address and other related settings.

Procedure

1. On the Settings menu, go to **Network > IP**.
2. On the IP page, for the **Work Mode** setting, one of the following IP network work modes:
 - **Auto**: The codec automatically determines the network work mode.
 - One of the values corresponding to your network parameters.
3. For the **Connection Type** setting, select one of the following options:
 - **DHCP**: The codec obtains the IP address from the DHCP server.
 - **Static IP**: You manually specify the IP address and other related settings.
4. If you selected manual IP assignment, in the **IP Address** field, type the codec IP address.
5. In the **Netmask** field, type the subnet mask address.
6. In the **Gateway** field, type the default gateway IP address.
7. In the **DNS1 Address** field, type the primary DNS server IP address.
8. In the **DNS2 Address** field, type the secondary DNS server IP address.
The secondary DNS server IP address is used if the primary DNS server is unavailable.
9. Click **Save**.

Configuring firewall settings

About this task

You can configure firewall settings, including TCP and UDP port ranges, static network address translation (NAT) options, and UDP hole punching. These settings determine the access of external devices to the codec and might impact data flow during calls and conferencing.

Procedure

1. On the Settings menu, go to **Network > Firewall**.
2. On the Firewall page, in the **TCP Port Range** fields, type the range of ports to open for TCP.
3. In the **UDP Port Range** field, type the range of ports to open for UDP.
4. For the **NAT Keep Alive Time** setting, select the time interval for sending NAT keepalive messages.
5. To enable the H.460 extension for firewall traversal, select the **Enable H.460 For NAT Traversal Of H.323 Calls** check box.

With firewall traversal, video conferencing data can bypass the firewall without compromising security.
6. To enable static mapping from private to public IP addresses, select the **Enable Static NAT** check box.
7. If you enabled static NAT, in the **Public IP** field, type the codec public IP address.
8. For the **Static NAT Type** setting, select the type of the static IP address mapping.
9. To automatically obtain the public IP address for the codec, select the **Auto acquire public IP** check box.
10. To send messages directly between the codec and a network node behind a different NAT, select the **Enable UDP Hole Punching** check box.
11. Click **Save**.

Configuring quality of service

About this task

Configure the quality of service parameters, including packet priority, jitter buffer, the size of Maximum Transmission Unit (MTU), network redundancy, and other settings. You can also enable RTP and TCP packet retransmission and traffic control. Quality of service eliminates data loss, reduces network latency and jitter, and provides an optimal audio and video experience for call and streaming participants.

Procedure

1. On the Settings menu, go to **Network > Service Quality**.

2. On the Service Quality page, for the **Type Of Service** setting, select one of the following options:
 - **IP Priority**: To determine the outbound port queue for IP packets based on the precedence bits in the packet header.
 - **Differentiated Services**: To determine the network traffic priority based on the differentiated services code point (DSCP) value in the packet header.
3. For the **Audio** setting, select the audio traffic precedence value.
4. For the **Video** setting, select the video traffic precedence value.
5. For the **Control** setting, select the signaling traffic precedence value.
6. For the **Maximum Jitter Buffer** setting, select the delay in milliseconds with which the jitter buffer sends the queued data packets to the recipient.

By adjusting this setting, you can reduce the network jitter and ensure a smoother audio and video.

7. For the **Packet MTU** setting, select the maximum size of data packets in bytes.
This setting determines the largest packet size that you can send over the network.
8. For the **Maximum Transmission Unit(MTU)** setting, select the maximum size of any data unit in bytes, including packets and frames.
9. To enable Rapid Transfer Protocol (RTP) packet loss retransmission, select the **Enable Media Optimization** check box.
10. If you enabled media optimization, for the **Maximum delay of packet loss recovery** setting, select the maximum delay for restoring lost data packets in milliseconds.
11. For the **Redundancy** setting, select the level of redundancy to provide alternate paths for sending traffic in case of a network failure.
12. To resend the lost RTP packets using Automatic Repeat Request (ARQ), select the **Enable RTP Packet Loss Retransmission** check box.
13. To enable adaptive mode for the RTP connection data flow, select the **Enable RTP Auto Adaptive Rate** check box.
If adaptive mode is enabled, the video resolution decreases during calls if the network bandwidth is low until it is restored.
14. To resend RTP packets using Forward Error Correction (FEC), select the **Enable Simple Retransmission** check box.
15. If you enabled simple retransmission, for the **Redundancy Rate** setting, select the level of redundancy for resending RTP packets.
The level of redundancy corresponds to the number of times for resending packets. For example, if you select **Small**, the packets are sent only once, and if you select **Large**, the packets are resent three times.
16. To resend only audio packets, select the **Valid For Audio Only** check box.

17. To enable traffic control based on the network bandwidth and packet delivery feedback, select the **Enable Traffic Control** check box.
18. If you enabled traffic control, for the **Call Offset Rate** setting, select the call rate value in kilobits per second.

The **Default Call Rate** value that you set on the Call Options page includes both audio and video traffic. The audio traffic mostly remains static, but you can determine how the video bit rate can change depending on the network bandwidth by setting the **Call Offset Rate** value. With a higher **Call Offset Rate** value, you can achieve a higher video encoding bit rate.

19. Click **Save**.

Configuring SNMP settings

About this task

You can use the Simple Network Management Protocol (SNMP) to monitor the codec status from a network management station (NMS).

Procedure

1. On the Settings menu, go to **Network > SNMP**.
2. On the SNMP page, to enable and configure the SNMP protocol, toggle on the **Enable SNMP** switch.
3. For the **SNMP Version** setting, select the SNMP protocol version.

Version 1 is a basic SNMP version that uses community strings and provides two types of communities: read-only and read-write. Version 2c has an improved security and communication and additionally supports GetBulk and Inform messages. Version 3 provides enhanced security features.
4. In the **NMS Address** field, type the NMS IP address to which the codec sends SNMP messages.
5. In the **NMS Trap Port** field, type the port number for sending trap messages.
6. In the **Community** field, type the community string to access the NMS.

The community string must match on the codec and NMS.
7. In the **Contact** field, type the contact information about the person managing the SNMP server.
8. In the **Location** field, type the SNMP server location details.
9. In the **System Name** field, type the codec name that the NMS uses.
10. In the **System Description** field, type the codec description that the NMS uses.
11. Click **Save**.

Configuring the H.323 protocol

About this task

Enable the H.323 protocol and configure the related settings to call inbound and outbound phone numbers. You can also enable and configure the H.239 protocol for dual video streaming and manage the Dual Tone Multi-Frequency (DTMF) options.

Procedure

1. On the Settings menu, go to **Protocol > H.323**.
2. To call other devices using their IP address when your H.323 account is registered on the domain, select the **Enable Call IP Address Directly When Registered** check box.
3. To enable H.245 tunneling, select the **Enable H.245 Tunnel** check box.
4. To obtain a gatekeeper and send a gatekeeper request, select the **Send GRQ** check box.
5. To enable the H.239 protocol extension for parallel video streaming, select the **Enable H.239 Control** check box.
6. To enable static dual streaming with H.239, select the **Enable H.239 Static Dual Stream** check box.

If the check box is selected, during an H.323 call, the secondary video stream channel is open on the firewall to interact with certain multipoint control units (MCUs).

7. For the **Send DTMF As** setting, select one of the following options:
 - **RFC2833**: To transmit DTMF tones separately from the audio stream in Real-Time Protocol (RTP) packets.
 - **Q.931**: To transmit DTMF tones using the Q.931 protocol.
 - **In Band**: To transmit DTMF tones as part of the regular audio stream.
 - **String**: To transmit DTMF tones as a string.
 - **Audio Frequency**: To transmit DTMF tones as an audio frequency.

You use the DTMF interface to perform certain actions during a call.

8. Click **Save**.

Configuring H.323 encryption

About this task

You can use the Advanced Encryption Standard (AES) algorithm for encrypting your voice and video calls made from the codec. You can choose the length of the AES secret key as 128 or 256 bits. A higher value of the key length provides more security to your call data.

Procedure

1. On the Settings menu, go to **Security > H323 Media Security**.
2. To use AES 256-bit encryption, select the **H.235.6 AES-256** check box.

3. To use AES 128-bit encryption, select the **H.235.6 AES-128** check box.
4. To disable AES encryption, select the **Plaintext (unencrypted)** check box.
For example, you can disable AES encryption for interoperability reasons or troubleshooting to be able to capture network packets.
5. Click **Save**.

Configuring the SIP protocol

About this task

Enable the SIP protocol and configure the related settings to call inbound and outbound phone numbers. You can also enable Binary Floor Control Protocol (BFCP), configure SIP monitoring, and manage the Dual Tone Multi-Frequency (DTMF) options.

Procedure

1. On the Settings menu, go to **Protocol > SIP**.
2. On the SIP page, for the **Send DTMF As** setting, select one of the following options:
 - **Auto**: To enable negotiating the DTMF tone option in the SIP INVITE request.
 - **RFC2833**: To transmit DTMF tones separately from the audio stream in Real-Time Protocol (RTP) packets.
 - **INFO**: To transmit DTMF tones as separate SIP INFO messages.
 - **In Band**: To transmit DTMF tones as part of the regular audio stream.
3. For the **Keep Alive Mode** setting, select one of the following options:
 - **By OPTION**: To send a SIP OPTIONS message to keep the session open.
 - **No Keep Alive**: Not to send keep-alive messages.
 - **By CRLF**: To send a double CRLF, or the "ping", from the client and then receive a single CRLF, or the "pong".
4. For the **Keep Alive Cycle** setting, select the value for the keep-alive cycle in seconds.
5. For the **PRACK Mode** setting, select one of the following options:
 - **Auto**: To enable negotiating the PRACK mode option in the SIP INVITE request.
 - **Disabled**: To disable sending PRACK messages.
 - **Supported**: To enable sending PRACK messages.

A PRACK request is similar to ACK but it is used for provisional purposes and has its own response.

6. To enable the compact format for SIP messages, select the **Enable Compact Mode To Encode Large Packet** check box.
7. To enable an older version of Binary Floor Control Protocol (BFCP), select the **Enable BFCP Control** check box.

With a BFCP stream, you can see shared desktops and presentations during a video call.

8. To enable the BFCP client mode for the codec, select the **BFCP Client As Default** check box.
You can deselect this check box if you operate the codec as a hosting server.
9. For the **BFCP Transmission Mode** setting, select one of the following options:
 - **TCP**: To use TCP for BFCP transmission.
 - **UDP**: To use UDP for BFCP transmission.
10. To use the UDP port for SIP monitoring, select the **Enable UDP Monitoring** check box.
11. If you enabled UDP for SIP monitoring, for the **UDP Monitoring Port** setting, select the UDP port number.
12. To use the TCP port for SIP monitoring, select the **Enable TCP Monitoring** check box.
13. If you enabled TCP for SIP monitoring, for the **TCP Monitoring Port** setting, select the TCP port number.
14. To block calls from the servers that are not registered in the network, select the **Ignore Calls From Unregistered Servers** check box.
15. To disable additional SIP encryption for audio, video, and other call data, select the **TLS Mode Disable Prefix Sips** check box.
For example, you can disable additional SIP encryption for interoperability reasons or for increasing the network bandwidth.
16. To send the SIP INVITE message only once, select the **Caller Does Not Send Re-invitation** check box.
The calling party sends a SIP INVITE message before establishing a connection.
17. To send a request for a key frame for starting a call, select the **Send Info Request Key Frame** check box.
The codec sends the request for a key frame in a SIP INFO message.
18. To enable the latest version of Binary Floor Control Protocol (BFCP), select the **BFCP Support RFC8855** check box.
19. Click **Save**.

Configuring SIP encryption

About this task

You can use the Advanced Encryption Standard (AES) algorithm for encrypting your voice and video calls made from the codec. If you enable AES encryption, it encrypts both audio and video data simultaneously.

Procedure

1. On the Settings menu, go to **Security > SIP Media Security**.
2. To use AES encryption, select the option corresponding to your security requirements.

3. To disable AES encryption, select the **Plaintext (unencrypted)** check box.

For example, you can disable AES encryption for interoperability reasons or troubleshooting to be able to capture network packets.

4. Click **Save**.

Configuring LDAP settings

About this task

Configure LDAP settings to connect to an external database, specify the name and password for authentication, and set search parameters. You can also select the LDAP protocol version and specify the base Distinguished Name (DN). At the bottom of the LDAP page, you can view the LDAP link connection status for the saved LDAP configuration.

With the LDAP Directory feature enabled, users can search for contacts in an external database instead of using locally saved contacts. The LDAP search is available only on the codec GUI menu.

When configuring LDAP settings, you can set up the LDAP filter to limit the scope of data retrieved from the LDAP server. The LDAP server searches the directory entries and displays the results based on the listed criteria. For example, to search for users by their common name, surname, and phone number, you can type `cn,sn,telephoneNumber`.

You can use the following common LDAP filter types:

- `(attribute=value)`: for exact matching
- `(attribute=*value*)`: for wildcard matching
- `(&(cond1)(cond2))`: for conditions with the AND operator
- `(|(cond1)(cond2))`: for conditions with the OR operator

Procedure

1. On the Settings menu, go to **Network > LDAP**.
2. On the LDAP page, to enable and configure LDAP, enable the **LDAP Enable** switch.
3. For the **LDAP Type** setting, select one of the following LDAP protocol versions:
 - **LDAP**: To use an insecure protocol version. Avaya recommends using the insecure protocol version only for troubleshooting purposes.
 - **LDAPS**: To use a secure protocol version. You can use this version for all purposes other than troubleshooting.

The LDAP protocol type setting is related to the LDAP port setting. If you change the protocol type, you must also update the LDAP port number.

4. In the **LDAP Address** field, type the IP address or FQDN of the LDAP directory server.
You cannot use the `ldap://<IP address or FQDN>` or `ldaps://` entry format.
5. In the **LDAP Port** field, type the directory server port number.

The default port number for the LDAP protocol is 389. The default port number for the LDAPS protocol is 636.

6. In the **LDAP User** field, type the name of the user that can access the LDAP directory entries.

For example, you can type `cn=admin,dc=example,dc=com`.

7. In the **LDAP Password** field, type the password for binding to the LDAP server.

The password must match the LDAP password for the user that you specified in step 6.

8. In the **LDAP Base DN** field, type the base Distinguished Name (DN) from where the LDAP server searches for users.

For example, if you want to start the search from an organizational unit "people" created in the "example.com" enterprise, you can type the following:
`ou=people,dc=example,dc=com`.

9. Skip the **LDAP Root DN** field as this setting is not currently supported.

10. In the **LDAP Filter** field, type the criteria for the LDAP filter.

The filter criteria you can type correspond to the attributes set on the connected LDAP server.

11. Click **Save**.

Certificate management

For all codec models, you can upload your own PKCS #12 certificate bundle to use for SIP TLS encryption. The bundle must contain a root certificate, a device, or client certificate, and a private key. When uploading a PKCS #12 certificate bundle, the web interface requests you to enter the password that you used for package encryption. After uploading the certificate bundle, the web interface displays only the root and client certificates with the details on the certificate authority (CA) and recipient.

You can encrypt the root, client certificates and private key with RSA encryption up to 4096 bits. The private key can be in PKCS #1 or PKCS #8 X509 format. Elliptic Curve and Ed25519/Ed448 encryption methods are not supported.

On the TLS Authentication page, you can also view the issuer for the uploaded certificates, the organization it was issued to, and the certificate type. You can delete an expired or unused certificate and view additional details for each file, including the start and end time of the validity period.

If a certificate expires in 60 days or earlier, you can see a corresponding notification on the GUI menu, after logging in to the web interface, and when going to **Security > TLS Authentication** on the Settings menu.

Uploading a PKCS #12 certificate bundle

About this task

On the TLS Authentication page, upload a PKCS #12 certificate bundle for SIP TLS encryption. The bundle contains a root certificate, a client certificate, and a private key. The package is encrypted with a password, and you need to enter that password when uploading the certificate bundle.

Before you begin

Ensure you obtain the password that was used for PKCS #12 bundle encryption.

Procedure

1. On the Settings menu, go to **Security > TLS Authentication**.
2. On the TLS Authentication page, click **Upload PKCS**.
3. Browse to the certificate location and select the file.
4. In the **Password** field, enter the password that you used for file encryption.
5. Click **OK**.

The TLS Authentication page displays the uploaded root and client certificates with the details on the certificate authority (CA) and recipient.

Viewing certificate details

About this task

You can view the details for an uploaded root or client certificate, including the start and end dates of the validity period, serial number, fingerprint, and other data. You can view the certificate details to check the expiration date if you see a notification about certificate expiry. The web interface displays the notification when you go to the **TLS Authentication** page if a certificate expires in 60 days or earlier.

Procedure

1. On the Settings menu, go to **Security > TLS Authentication**.
2. On the TLS Authentication page, for the certificate to view, click **Details**.

In the window at the bottom of the page, you can see the certificate details.

Deleting a certificate

About this task

You can delete an expired or unused certificate from the TLS Authentication page.

Important:

The web interface instantly deletes a certificate and does not display a confirmation window.

Procedure

1. On the Settings menu, go to **Security > TLS Authentication**.
2. On the TLS Authentication page, for the certificate to delete, click **Delete**.

The web interface removes the certificate from the certificate list. If you deleted a certificate by mistake, you need to upload the PKCS #12 certificate bundle again.

Adding an IP address to the blocklist

About this task

You can add an IP address to the blocklist so that it is not used for web interface access. You can add non-secure or outdated IP addresses to control access for other users.

Procedure

1. On the Settings menu, go to **Security > Web Login Apply Black List**.
2. On the Web Login Apply Black List page, click the **Add** icon.
3. On the Add window, in the **IP** field, type the IP address to add to the blocklist.
4. Click **OK**.
5. **(Optional)** To update an IP address, select it and click the **Edit** icon.
6. **(Optional)** To delete an IP address, select it and click the **Delete** icon.

Display settings

Configuring a codec name

About this task

You can configure a codec name to show on top of the video output coming from the codec. You can also define the name position relative to the video central horizontal and vertical lines so that the name does not overlap with the banner text.

Avaya Room System C170 and Avaya Room System C190 do not display the codec name on the HDMI2 output.

Procedure

1. On the Settings menu, go to **Subtitles > Terminal Name**.
2. On the Terminal Name page, for the **Subtitle Display** setting, select **Enable**.
3. For the **Font Size** setting, select the codec name font size.
4. If you selected the custom font size option, in the **Text Pixel** field, type the font size in pixels.
5. For the **Font Position** setting, select the codec name position relative to the OLED display center.
6. For the **Lateral Offset** setting, select the codec name position relative to the OLED display horizontal central line.
7. For the **Vertical Offset** setting, select the codec name position relative to the OLED display vertical central line.

8. If you selected the custom option for the offset, in the **Offset Pixel** field, type the number of pixels between the codec name and the central horizontal or vertical line of the display.
9. Select the font and background color.
10. For the **Background Transparency** setting, select one of the following options:
 - **Transparent**: To set a transparent background.
 - **Opaque**: To set a non-transparent background.
11. In the text box, type the codec name.
12. To send the name to the codec display, click **Send**.

Configuring a banner

About this task

You can configure a banner to show on top of the codec video output. For example, you can configure a banner saying that the meeting ends in 15 minutes to display a reminder for the call participants. If the banner text is too long, it is displayed as a running line.

Procedure

1. On the Settings menu, go to **Subtitles > Banner**.
2. On the Banner page, for the **Font Size** setting, select the banner font size.
3. If you selected the custom font size option, in the **Text Pixel** field, type the font size in pixels.
4. For the **Font Position** setting, select the banner position relative to the OLED display center.
5. Select the font and background color.
6. In the text box, type the banner text.
7. To send the banner text to the codec display, click **Send**.
8. To stop sending the banner text, click **Stop**.

Configuring scrolling captions

About this task

To add a lot of text to the codec video output, configure scrolling captions. You can also define the caption position relative to the video central horizontal and vertical lines so that the text does not overlap with the banner and codec name.

Procedure

1. On the Settings menu, go to **Subtitles > Scroll Caption**.
2. On the Scroll Caption page, for the **Font Size** setting, select the text font size.
3. If you selected the custom font size option, in the **Text Pixel** field, type the font size in pixels.

4. For the **Font Position** setting, select the scrolling caption position relative to the OLED display center.
5. For the **Scrolling Mode** setting, select the horizontal or vertical scrolling of the captions.
6. For the **Horizontal Rolling** or **Vertical Rolling** setting, select the scrolling direction of the captions.
7. For the **Rolling Speed** setting, select the scrolling speed.
8. Select the caption offset position relative to the central horizontal or vertical line of the display.
9. If you selected the custom option for the offset, in the **Offset Pixel** field, type the number of pixels between the captions and the central horizontal or vertical line of the display.
10. Select the font and background color.
11. For the **Background Transparency** setting, select one of the following options:
 - **Transparent:** To set a transparent background.
 - **Opaque:** To set a non-transparent background.
12. In the text box, type the caption text.
13. To send the captions to the codec display, click **Send**.
14. To stop sending the captions, click **Stop**.

Other settings

Setting up the date and time

About this task

Configure the Network Protocol Time (NTP) settings to synchronize the codec time with other devices in the network. You can use the default NTP settings or specify a custom NTP server IP address.

Procedure

1. On the Settings menu, go to **Others > Date**.
2. On the Date page, for the **NTP Server Mode** setting, select one of the following options:
 - **System Preset:** To use the default NTP settings.
 - **Custom:** To specify a custom NTP server IP address.
3. If you selected custom server mode, in the **NTP Server Address** field, type the IP address of the NTP server.
4. Click **Save**.

Setting up logging

About this task

Select the log level and configure how you want to obtain the log file archive. You can download the log file archive from the Log Information page on the Diagnostics menu. You can also specify the log server IP address and port number to obtain the file archive from the server.

Procedure

1. On the Settings menu, go to **Others > Logging**.
2. On the page, for the **Log Level** setting, select the log level.
3. To save the log data to a file archive, select the **Save Log To File** check box.
4. To save the log file archive on a log server, select the **Send Log To Log Server** check box.
5. If you selected to save the log file archive on a server, in the **Log Server Address** field, type the log server IP address.
6. In the **Log Server Port** field, type the log server port number.
7. Click **Save**.

Log levels

The following table lists available Avaya Room System C100 Series log levels and their names:

Log level number	Log level name
0	NULL
1	ERROR
2	WARN
3	INFO
4	DEBUG
5	VERBOSE

Exporting the codec configuration to a USB drive

About this task

Insert a USB drive to the codec pack panel and export the current configuration. Configuration export generates `c9-account.ini` and `c9-settings.ini` files. The `c9-account.ini` file contains basic SIP and H.323 parameter details and the `c9-settings.ini` file contains all other configuration information. You can then import the exported configuration to a different codec to not perform manual configuration again.

Procedure

1. Insert a USB drive to the back panel USB port 1 or port 2.
2. On the Settings menu, go to **Others > Configuration**.

3. On the Configuration page, click **Export The Configuration To A USB Drive**.

The web interface saves and exports the current configuration as `c9-account.ini` and `c9-settings.ini` files on the inserted USB drive.

Importing the codec configuration from a USB drive

About this task

You can import the configuration exported from a different codec using a USB drive. Before importing, you need to save `c9-account.ini` and `c9-settings.ini` files in a root directory on the USB drive. The `c9-account.ini` file contains basic SIP and H.323 parameter details and the `c9-settings.ini` file contains all other configuration information. Exporting and importing the settings saves your time as you do not need to perform manual configuration of the codec.

Before you begin

Ensure that you saved the codec configuration files on a USB drive.

Procedure

1. Insert the USB drive with the configuration file to the back panel USB port 1 or port 2.
2. On the Settings menu, go to **Others > Configuration**.
3. On the Configuration page, click **Import Configuration From USB Drive**.

The web interface imports the configuration files and then reloads and displays the Login page.

Upgrade process for Avaya Room System C100 Series

You can upgrade the Avaya Room System C100 Series software by obtaining the upgrade files from the following sources:

- File server: you need to specify the HTTP server IP address and the upgrade file folder in the Others submenu of the Settings web interface menu.
- USB drive: before starting the upgrade, you must upload the upgrade files to the root directory and insert the drive into a USB slot on the codec back panel.
- Folder on your computer: you can use this method only from the web interface menu. After selecting this option, you need to navigate to the upgrade file location.

You can initiate the upgrade process from the following locations:

- By going to **Settings > About** in the GUI menu. You can only start the upgrade process from the GUI menu and select an HTTP server or USB drive as the upgrade file source.
- By going to **Settings > Others > Upgrade** in the web interface. You can select an HTTP server, USB drive, or folder on your computer as the upgrade file source. You can also configure the upgrade details, including the HTTP server IP address and folder, forced upgrades, and checking a newer upgrade file version at boot-up.

Upgrade process flow

The upgrade process from the file server and USB drive has the following flow:

1. The codec obtains the `update.xml` file from the specified location and compares the version parameter to the current software version. On the web interface or GUI menu, you can see the notification about the available and current software versions and you can choose to start or cancel the upgrade.
2. The codec obtains the upgrade file based on the `<newurl>` parameter in the `update.xml` file. The upgrade file name format is `<codec model>-ota-AVAYA-v<version>.zip`.
3. The codec calculates the checksum to verify data integrity. You can see a dialog box and confirm to proceed with the upgrade.
4. The upgrade process starts with updating the operating system and feature application data. The upgrade also impacts connected RM61 microphones if there is an available update for them. Avaya Room System C130 and Avaya Room System C170 built-in cameras might also be upgraded. You receive a notification about a pending camera upgrade.
5. After the upgrade, the codec goes into an idle state. The upgrade process might take up to 5 minutes depending on your network bandwidth.

Upgrade files and folder structure

To upgrade the codec software, you need two files: `update.xml` and `<codec model>-ota-AVAYA-v<version>.zip`. If you have only one codec model in your environment and you use the file server as the upgrade method, you can place these files in the server root directory or any other appropriate folder. Do not unpack the `.zip` archive.

If you have more than codec model in your environment and you use the file server as the upgrade method, you must create separate folders for each model and place the `update.xml` and `.zip` files accordingly. For example, if you have C130 and C190, create a `/C190` folder on your file server for C190 upgrades, upload the upgrade files to it, and specify the following file location on the web interface Upgrade menu: `http://<server IP address>/C190`.

For a USB drive, you must copy the upgrade files directly to the root directory.

Upgrade from a USB drive

Before using a USB drive for upgrades, ensure that you do the following:

- Check if your USB drive has a storage capacity of 2 GB or more.
- Format the drive using the FAT32 file system.
- Copy the `update.xml` and `<codec model>-ota-AVAYA-v<version>.zip` files to the root directory on the drive.

You can upgrade only one codec model at a time from the USB drive.

- Insert the USB drive into a USB slot on the codec back panel. You can see a notification on the GUI or web interface menu that the drive has been detected. If the drive is not detected, in the web interface, go to **Settings > Security > System Security** and check if USB is enabled in the **USB Management** setting.

Downgrade process

If you need to downgrade the codec software, replace the `update.xml` and `<codec model>-ota-AVAYA-v<version>.zip` files with earlier versions at the selected location. The downgrade process flow is the same as for the upgrade.

Upgrading the codec software

About this task

You can obtain the codec software updates from a server, USB drive, or folder on your computer. If you want to obtain the updates from a server, you need to specify the server IP address and the upgrade file folder. You can also determine if you want to check and apply the updates immediately or at the next reboot of the codec.

Important:

Do not power off the codec during the upgrade process as this action might corrupt the file system and require a factory reset.

Before you begin

Ensure the following:

- If you want to obtain the upgrades from a USB drive, check that it has a storage capacity of 2 GB or more and format it using the FAT32 file system. Upload the `update.xml` and `<codec model>-ota-AVAYA-v<version>.zip` files to the root directory and insert the drive into a USB slot on the codec back panel. For more information about using a USB drive as the upgrade file source, see [Upgrade process for Avaya Room System C100 Series](#) on page 89.
- If you want to obtain the upgrades from a file server, upload the `update.xml` and `.zip` files to the file server directory that you later specify as the upgrade file source.
- If you have more than codec model in your environment and you use the file server as the upgrade method, create separate folders for each model and place the `update.xml` and `.zip` files accordingly.

Procedure

1. On the Settings menu, go to **Others > Upgrade**.
2. On the Upgrade page, select the **Enable Upgrade** check box.
3. To check if there is a newer version of the upgrade file on the server when the codec boots up, select the **Check New Version On Startup** check box.
4. To upgrade the codec immediately after saving the configuration, select the **Forced Upgrade** check box.
5. For the **Select Upgrade Mode** setting, select one of the following options:
 - **Upgrade Via Network:** To obtain the upgrades from an HTTP server.
 - **Upgrade Via USB Storage:** To obtain the upgrades from a USB drive.
 - **Upgrade By Uploading Via Browser:** To browse and select the upgrade archive from a folder on your computer.

Uploading the upgrade archive manually is less secure as the codec does not use the `update.xml` file and checksum validation.

6. If you selected upgrades from an HTTP server, in the **Upgrade Server Address** field, type the IP address of the server and the folder to obtain the upgrade files in the following format: `http://<server IP address><folder name>`.

For example, if you created separate folders for different codec models, you can type `http://<server IP address>/C190`. For more information about the folder structure and upgrade files, see [Upgrade process for Avaya Room System C100 Series](#) on page 89.

7. If you selected upgrades from your computer, click **Select Zip File** and browse to the folder to select the `<codec model>-ota-AVAYA-v<version>.zip` file.
8. To check if there is a newer version of the upgrade file on the server or USB drive now, select the **Check New Version Right Now** check box.
9. Click **Save**.

Performing a factory reset

About this task

Restore the codec software to the factory settings. You can save the account information to log in with the same credentials after the reset. You can also save the IP configuration details not to perform this configuration again.

TLS certificates get deleted after a factory reset regardless of the reset option that you choose.

Procedure

1. On the Settings menu, go to **Others > Factory Reset**.
2. To save your account information for logging in after the reset, select the **Enable Save Account Information** check box.
3. To save the IP configuration of the codec after the reset, select the **Enable Save IP Information** check box.
4. To reset the codec to the factory settings after saving the configuration, select the **Enable Start Factory Reset** check box.
5. Click **Save**.

White list management

The White List subtab is designed for loading third-party applications to extend codec capabilities. Skip the White List subtab when configuring the codec as this functionality is not currently supported.

Chapter 6: Codec diagnostics

Diagnostics menu overview

You can access the Diagnostics menu from the web interface side pane. You do not need the administrator password to access the menu. However, Avaya recommends that only administrators and trained personnel perform codec diagnostics.

From the Diagnostics menu, you can perform the following operations:

- View and adjust the audio level for all connected devices. You can also test audio input volume level and quality.
- View video input resolution and refresh encoding parameters.
- Test the network connection for different nodes and capture traffic for troubleshooting purposes.
- View quality and network information for an active call.
- View codec details, such as the serial number, device model, MAC address, and software version.
- Download log files and clear all log entries.

Viewing the audio volume level

About this task

You can view audio volume level from the Diagnostics menu for all audio input and output devices, including built-in or external microphones and speakers.

Procedure

1. On the Diagnostics menu, click **Volume information**.
2. On the Volume information page, view the volume level for the audio input and output.

Testing the audio input

About this task

You can test the volume level and audio quality for a local input device, such as an built-in or external microphone or camera. For example, you can perform this test before making a call or if you are having issues with a microphone.

Procedure

1. On the Diagnostics menu, click **Near Audio Loopback**.
2. To start the audio input test, enable the **Near Audio Loopback Test** switch.

Viewing video input details

About this task

After you connect a video source device to the codec, you can view input details, such as the connected port name and video resolution.

For Avaya Room System C130 and Avaya Room System C170, you can also view built-in camera resolution.

For Avaya Room System C190, if you are streaming video from a camera or broadcasting server, you can see the video resolution in the VCH section.

* Note:

The Diagnostics menus are generic and might contain parameters that do not apply to the specific model in use.

Procedure

1. On the Diagnostics menu, click **Video Input**.
2. On the Video Input page, next to the video input name, view the video resolution.
For example, 1920x1080 pixels.

Refreshing video encoding parameters

About this task

After configuring the video encoding parameters from the Settings menu, you can refresh them on the Video Intra Update page of the Diagnostics menu to apply the updates for a current video call. You configure video encoding, including the encoder type and decoder resolution, on the Video page of the Settings menu.

Procedure

1. On the Diagnostics menu, click **Video Intra Update**.
2. On the Video Intra Update page, click **Video Refreshing**.

Testing the network connection

About this task

Test your network performance to assess the quality of your network connection and identify any issues that could impact audio and video during calls. You can test the connection to a specific IP address or to one of the following network nodes:

- DNS server
- Gatekeeper
- Gateway
- SIP proxy server

After you complete the network test, you can view the following information:

- Number of packets transmitted
- Number of packets received
- Percentage of the packet loss
- Ping time

A high packet loss rate can indicate network instability, while increased ping times can indicate a slower Internet connection.

Procedure

1. On the Diagnostics menu, click **Network Test**.
2. On the Network Test page, select a connection type.
3. If you selected an IP connection, in the **Input Address** field, enter the IP address to ping.
4. In the **Byte Size** field, type the size of the data packets to send.

The maximum packet size is 65,500 bytes.

5. Click **Ping** to initiate the network test.

You can see the `On Ping` message.

6. To stop the network test and view the results, click **Cancel**.

You can see the `Cancel Ping` message.

7. At the bottom of the network test window, view the test results.

Capturing codec network traffic

About this task

You can capture network traffic from the codec to use for diagnostics and troubleshooting. After capturing network packets, open an SSH session to access the file containing the intercepted traffic.

Procedure

1. On the Diagnostics menu, click **Packet Interception**.
2. On the Packet Interception page, for the **Protocol** setting, select the transport protocol to capture the network packets.
3. To start capturing the traffic, click **Start**.
4. To stop capturing the traffic, click **Stop**.
5. In the Google Chrome browser, go to `https://<codec IP address>:65443/log`.
6. In the `/log` directory, locate the `tcp-1.pcap` file to view the captured traffic details.

If a USB drive is connected to the codec, the `tcp-1.pcap` file is automatically downloaded to the drive.

Viewing call quality details

About this task

You can view real-time details on the quality and network parameters of an active call. For example, you can view if AES encryption is used and check the type of encryption. You can also view various audio and video parameters, call and frame rate, and the presence of jitter and packet loss.

Procedure

1. During a call, on the Diagnostics menu, click **Call Information**.
2. On the Call Information page, view the call quality details and network parameters.

Viewing codec details

About this task

You can view general codec information from the Diagnostics menu, such as the serial number, device model, MAC address, software version, and check code.

Procedure

1. On the Diagnostics menu, click **System information**.
2. On the System information page, view the codec details.

Downloading log files

About this task

You can set up the logging level and determine if you want to save the log information as a file archive or send it to a log server from the Others submenu of the Settings menu. After configuring the logging details, you can download the log file archive from the Diagnostics menu. You can then unpack the archive and search for the relevant details for diagnostics and troubleshooting. For example, you can search for errors in the `c9root.txt` file.

Procedure

1. On the Diagnostics menu, click **Log Information**.
2. On the Log Information page, click **Download Log**.

The web interface starts generating the log file archive and displays the download countdown. When the archive is generated, you can see the corresponding message on the web interface page and you can access the archive in your `Downloads` folder.

Clearing log information

About this task

From the Log Information page, you can clear the log entries to start logging again, free up the storage space on the log server, and reduce the size of the log file archive. You can clear only non-active log entries, currently written log files are not cleared during this operation.

Procedure

1. On the Diagnostics menu, click **Log Information**.
2. On the Log Information page, click **Clear Log**.
3. In the confirmation dialog box, click **Yes**.

Chapter 7: Troubleshooting

The codec is stuck at boot-up

The codec is stuck at boot-up and displays the Avaya logo or animation.

Solution

1. Disconnect all cables from the codec except for the power adapter and HDMI 1 OUT.
2. Restart the codec.
3. If the codec boots up, connect one cable at a time and restart the codec after connecting each cable to determine the issue.
4. If, after performing steps 1 to 3, the codec is stuck at the start-up animation, press and hold the **Reset** button until the codec displays the Avaya logo.

This action retains the current software version.

5. If the codec is stuck at the Avaya logo, power off the codec, press and hold the **Reset** button, and then power on the codec.

You must release the button after the primary HDMI output displays `Installing System Update`. This action restores the factory-installed software version.

The codec displays a black screen after boot-up

The codec boots up but then displays a black screen.

The following causes can lead to this issue:

- The video output device is not powered on.
- The output device cable is not connected correctly.
- The codec does not support the video resolution of the output device.

Solution

1. Ensure the video output device is powered on.
2. Check the output device cable connection to the codec.
3. In the codec web interface, go to **Settings > Video > Video Output** to change the video output resolution.

No audio output from the speakers

The following causes can lead to this issue:

- The HDMI audio output is not enabled.
- The audio output volume level is low.

Solution

1. In the codec web interface, go to **Settings > Audio > Audio Output** and enable the audio output that you use.
2. On the web interface Audio Output page or with the remote control **Volume +/-** buttons, increase the audio output volume level.

No audio input from the microphone

You might receive no audio input from a microphone if the audio input is not enabled.

Solution

In the codec web interface, go to **Settings > Audio > Audio Input** and enable the audio input that you use.

Echo during calls

Remote participants can hear an echo when they are speaking during a call.

Solution

In the codec web interface, go to **Settings > Audio > Echo Elimination** and configure the echo cancellation settings.

You can eliminate echo, unwanted background noises, voices, and repetitive sounds.

The local video image is flickering

Video image flickering can be caused by indoor lightning frequency.

Solution

In the camera OSD menu or web interface, adjust the anti-flicker setting from the Exposure menu.

You must select the anti-flicker value corresponding to the local utility frequency. The default value is 50 Hz.

The video resolution cannot reach 4K

During calls, the video resolution on the codec cannot reach 4K.

The following causes can lead to this issue:

- The conferencing service does not support 4K video resolution.
- The H.265 codec is not selected in the video settings.

Solution

1. Ensure that the conferencing service that you use supports 4K video resolution.
2. In the codec web interface, go to **Settings > Video > Video Capabilities** and ensure that the H.265 codec is selected.

Presentation issues

The presentation sent from the codec does not display correctly.

The following causes can lead to this issue:

- The secondary video source is not connected.
- The video streaming device cable is not connected correctly.
- The SIP protocol is not configured correctly.

Solution

1. Connect an external HD camera or secondary video source device to the HDMI input.
2. Check the streaming device cable connection to the codec.
3. In the codec web interface, go to **Settings > Protocol > SIP > BFCP Transmission Mode** and select **TCP**.

Cannot manage PTZ settings with the remote control

You cannot manage pan, tilt, and zoom camera settings from the codec GUI menu with the remote control.

The cause of this issue is that the RS232 cable is not connected or is connected incorrectly.

Solution

Ensure that you connect the network port connector of the RS232 cable to the codec RS232 port and the 8-pin DIN connector to the RS232 IN port of the camera.

Chapter 8: Resources

Documentation

Avaya Room System C100 Series customer documentation is available in HTML and PDF format on the [Avaya Documentation Center](#) and [Avaya Support](#) website.

Title	Use this document to:	Audience
Administering		
<i>Installing and Administering Avaya Room System C100 Series</i>	Perform initial installation and administration tasks from the codec GUI menu and web interface.	End users and administrators
Using		
<i>Using Avaya Room System C100 Series</i>	Set up and use Avaya Room System C130, Avaya Room System C170, and Avaya Room System C190.	End users
<i>Avaya Room System C130 Quick Start Guide</i>	Obtain an overview of features and use Avaya Room System C130.	End users
<i>Avaya Room System C170 Quick Start Guide</i>	Obtain an overview of features and use Avaya Room System C170.	End users
<i>Avaya Room System C190 Quick Start Guide</i>	Obtain an overview of features and use Avaya Room System C190.	End users
<i>Using Avaya Room Camera RC212 and Avaya Room Camera RC220</i>	Set up and use Avaya Room Camera RC212 and Avaya Room Camera RC220.	End users
<i>Using Avaya Room Camera RC240</i>	Set up and use Avaya Room Camera RC240.	End users
<i>Using Avaya Room Microphone RM61 and RM61-EXP</i>	Set up and use Avaya Room Microphone RM61 and Avaya Room Expansion Microphone RM61-EXP.	End users
<i>Using Avaya Room Microphone Speaker RA63</i>	Set up and use Avaya Room Microphone Speaker RA63.	End users

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at <https://documentation.avaya.com>. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

 Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the [Avaya Support website](#).

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** () in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

You can select multiple items in each filter category. For example, you can select a product and multiple user roles.

- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click < or > next to the document title to navigate to the previous topic or the next topic.
- Click **Share** () to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** (). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
- Set a collection as the default or favorite collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collections that others have shared with you.
- Click **Watch** () to add a topic to your watchlist so you are notified when the content is updated or removed.

- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

You can do the following:

- Enable **Email notifications** to receive email alerts.
- Unwatch the selected content or all topics.
- Send feedback for a topic.

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.
For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click  to display the search results.

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 <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Glossary

3A algorithm	An audio processing algorithm that combines Echo Cancellation, Automatic Gain Control, and Automatic Noise Reduction.
Acoustic Echo Cancellation	An audio feature that helps to remove the echo caused by reflections in the environment where the room system is installed. For example, Acoustic Echo Cancellation can eliminate the echo or feedback during a conference call.
Active Noise Reduction	A type of noise reduction that adjusts audio intensity based on the noise source. For example, you can use Active Noise Reduction for eliminating continuous and predictable noises.
AI tracking	A functionality that helps you track a person, a group of people, or a particular zone automatically. The camera follows the tracked person, group of people, or zone based on the selected mode.
AI Voice Noise Reduction	A type of noise reduction that adapts and focuses on removing redundant speech noises.
Audio compression	A process of adjusting the dynamic range of the audio by reducing its level when it rises above a specified threshold. The dynamic range is the difference between the loudest and quietest moments of an audio signal.
Audio loopback	A test feature that routes audio from an input to an output for testing purposes.
Auto Answer	A calling feature that helps you automatically answer all incoming calls without the need to accept them.
Automatic Gain Control	An audio feature that automatically applies gain or loss to incoming call audio to reach the target average audio level. You can use this feature to compensate for the differences in call participant audio level.
BFCP	Binary Floor Control Protocol, which is a SIP signaling protocol supporting video and audio collaboration.
Bitrate	Amount of video and audio bandwidth used for a call. A higher bitrate provides better audio and video quality.
Broadcasting server	A server that is specifically deployed and configured to support the live broadcasting of videos. The broadcasting server helps to encode a live

stream in real time and send stream bits to the codec so that the video can be delivered to viewers on multiple devices with minimal latency.

Call rate	Requested or negotiated network bandwidth for an audio or video stream within a call. In the codec web interface settings, the call rate value is in kilobits per second.
Camera Compose	A combination of HDMI 1 and HDMI 2 inputs for Avaya Room System C190 that an administrator can select when configuring video settings.
Cascading	A method of deploying microphones when you connect expansion microphones to the main one to capture audio from a larger area.
Codec	A video conferencing device, also known as terminal, that is used for mixing and transcoding audio and video from different sources, such as HD cameras and microphones.
Digital microphone	An audio recording device that captures analog sound waves and converts them into digital packets to send to the codec.
DSCP	Differentiated Services Code Point, which is a method of tagging IP packets so that an intermediate routing device can process them based on the packet priority.
DTMF	Dual Tone Multi Frequency, which is a method of encoding keypad entries to a discrete audio signal. You use the DTMF interface to perform certain actions during a call.
Dual streaming	A functionality that helps to obtain two separate video streams from an IP camera and send them to the codec. Each stream can have different settings, such as frame rate and image quality.
Dynamic IP address assignment	A method of assigning IP addresses to network devices. This method is equivalent to DHCP assignment when a network node controls and assigns IP addresses.
Echo elimination	Or echo cancellation, a method used in telephony to improve voice quality by preventing echo or removing it in post-processing.
EDID	Extended Display Identification Data, which is an industry standard used between video devices to declare and then select a supported video resolution and frame rate.
External HD camera	An HD camera that is not integrated physically into the codec. For example, for Avaya Room System C100 Series, these are Avaya Room Camera RC212, Avaya Room Camera RC220, and Avaya Room Camera RC240.

Factory reset	A process of reverting the configured device settings to their default values. When you perform a factory reset for a codec, you can choose to retain account and IP information.
Far camera control	A functionality that helps you remotely control external HD cameras connected to the codec. During a conference call, you can remotely change pan, tilt, and zoom settings for these cameras.
FQDN	Fully Qualified Domain Name, which is the complete address of any entity on the network, including hosts and computers. For example, host.domain.com.
Gatekeeper	A management tool in H. 323 multimedia networks that is used to convert phone numbers to IP addresses for VoIP sessions. The gatekeeper also provides interoperability between different networks.
H.235 authentication	An authentication method based on the H.235 protocol that is used for trusted H.323 endpoints and encrypting the media stream during calls.
H.245 tunneling	A method used in VoIP telephony to encapsulate H.245 messages within other protocols, thus reducing call setup time and improving call efficiency in the H.323 environment.
H.264 HP	H.264 High Profile, which is an advanced profile of the H.264 video compression standard used for broadcasting and data storage. H.264 HP is the most efficient profile in the H.264 family and can achieve the highest compression ratio.
H.460 extension	A series of extensions for the H.323 video conferencing standard developed by the International Telecommunication Union (ITU). This series of extensions is primarily used for managing firewall and NAT traversal.
I-frame interval	The time interval between two intraframes (I-frames) of the video stream. A smaller I-frame interval means a higher bitrate value and bandwidth.
IR	Infra-Red, which is the signaling method used between the remote control and codec.
Keep alive mode	Functional mode which determines how keep-alive messages are sent. An administrator can choose not to send keep-alive messages, to open a session with a <code>SIP OPTIONS</code> message, or keep the session by sending CRLF characters.
Lateral offset	Text position relative to the horizontal central line of the codec OLED display.
LDAP	Lightweight Directory Access Protocol, which is an industry standard access method to directory services. From the codec web interface, an administrator can enable LDAP Directory for connecting to an external

database and making calls to enterprise contacts. You can also save these contacts locally to access them when LDAP Directory is disabled.

Maximum jitter buffer

A jitter buffer is used to compensate for variation in packet delivery time in a network. A larger jitter buffer is more tolerant, but results in an increased delay in the end-to-end audio path.

MCU

Media Conferencing Unit, which is a device that mixes audio and video so that multiple callers can view the same streams.

MQTT

Message Queuing Telemetry Transport, which is a lightweight messaging protocol designed for communication in low-bandwidth, high-latency, or unreliable networks.

MTU

Maximum Transmission Unit, which is the size of the largest protocol data unit (PDU) that can be sent in a single network layer transaction.

NAT

Network Address Translation, which is a method of mapping one IP address space into another by modifying the IP header network address information for data packets when they are transmitted by a traffic routing device.

NAT keepalive

Functionality that consists in sending small UDP data packets from a VoIP phone to the router to indicate that the port is still in use.

Network redundancy

The process of providing alternative devices, pathways, and other network components so that data can keep flowing even in case of failure.

NMS

Network Monitoring System, which is a server that runs a network management application. NMS can be also referred to as a Simple Network Management Protocol (SNMP) manager.

Packet retransmission

The process of resending the data packets which are damaged or lost during their initial transmission.

PEM

Privacy Enhanced Mail, which is a type of Public Key Infrastructure (PKI) file used for storing certificates and keys. PEM is the most common format type that Certificate Authorities (CAs) use for issuing certificates. PEM certificates usually have the following extensions: .pem, .crt, .cer, and .key. As compared to a more secure PKCS #12 type, PEM files are text-based and simply list the certificates and keys in the format of Base64 encoded ASCII strings.

Picture-in-Picture

A type of multi-window mode for conference calls and presentations when you have a larger window and smaller ones within the main window. You can switch between the windows to determine which video to make the main one.

Picture-on-Picture	A type of multi-window mode for conference calls and presentations when you have a larger window and smaller ones outside of the main window.
PKCS #12	Certificate type based on public key cryptography standards (PKCS). PKCS #12 certificates usually have .p12 or .pfx filename extensions. As compared to the PEM certificate type, PKCS #12 is more secure and stores multiple certificates and a private key in a single file. PKCS #12 is the preferred way to transport and exchange private keys because of the stronger encryption.
PRACK mode	A mode invoking a SIP request that is similar to the ACK request but it is used for provisional purposes and has its own response.
PTZ	Pan, tilt, and zoom movements of the camera head that allow to control the video frame settings remotely. Pan corresponds to horizontal, or left and right, movements of the head. Tilt corresponds to vertical, or up and down, movements of the head. PTZ movements also include zooming in and out of the scene.
Remote recording	The process of recording and saving audio and video received from PTZ cameras on a remote server.
Reverberation	Audio reflections that are quick in delay and decaying over time.
Room system	A group of audio and video devices, such as codec, cameras, and microphones, that are used as a whole for providing conferencing features. For example, in a room system, the codec takes audio and video from HD cameras and microphones and processes it.
RTMP	Real-time Messaging Protocol, which is a protocol for recording audio and video received from cameras.
Silence detection	A functionality that helps to detect muted call participants during a conference. For example, if a person goes on mute on their local device but not from the conference menu, the codec can detect this and display a corresponding notification.
SIP authentication	The process of authenticating a user agent (UA). There are two types of SIP user authentication: by a proxy, redirect, or registration server and the authentication of one UA by another.
SIP registration	The process of binding an endpoint Address of Record (AOR) with its location. During SIP registration, a SIP endpoint sends a SIP REGISTER request to a registrar, containing its AOR, location, authentication, and other information.
SNMP	Simple Network Management Protocol, which is a standard internet protocol for collecting and managing information about IP network

devices. An administrator can configure SNMP settings to monitor the device status from a network management station (NMS).

SRTP

Secure Real-time Transport Protocol, which is a profile for Real-time Transport Protocol (RTP). This profile is used to provide encryption, message authentication, confidentiality, and replay protection for VoIP communications.

Static IP assignment

A method of assigning IP addresses to network devices. This method consists in the manual assignment of specific addresses to devices within the network.

Super wideband audio

Audio with a frequency range wider than traditional narrowband or even wideband audio. The range typically extends from 50 to 14000 Hz and the sample rate is typically 32 kHz.

Touch/DMIC port

The port on the codec back panel that you can use to connect to a C100 digital microphone. The digital microphone supports cascading.

Transcoding

A process of decoding, reformatting, and re-encoding video files by taking footage from different sources and recoding it into a single video codec or file format.

UDP Hole Punching

The functionality that allows to send messages directly between the codec and a network node behind a different NAT.

UDP monitoring

The process of scanning a UDP port number on a given IP address and checking whether the connection is successful. If the connection is unsuccessful, the UDP Monitoring service marks it as DOWN.

Vertical offset

Text position relative to the vertical central line of the codec OLED display.

Video conferencing unit

A synonym for "codec" and "terminal", a device that is used for mixing and transcoding audio and video from different sources, such as HD cameras and microphones.

Video decompression

The process of decompressing audio and video files with the codec software. An administrator can select audio and video codecs to use from the web interface.

Video mixing

A process of combining, or "mixing", multiple video sources into one or more output channels.

VoIP session

A call session that is done with Voice over Internet Protocol (VoIP). VoIP is a set of protocols used for voice calling over the Internet.

Index

A

accessing	
GUI menu settings	41
web interface	54
adding	
banner	86
codec name	85
scrolling captions	86
to white list	92
administrator requirements	9
advanced settings	
audio output	64 , 65
audience	9
audio	
configuring codecs	68
configuring digital microphone	69
configuring USB audio	67
echo during calls	99
eliminating echo	66
no input	99
no output	99
testing input from web interface	94
viewing volume level from web interface	93
audio input	
configuring	62
audio output	
advanced settings	64 , 65
configuring	63
audio settings	
configuring from GUI menu	47
Avaya InSite Knowledge Base	103
Avaya Room System C100 Series	
camera overview	15
feature comparison	14
installation checklist	26
overview	14
upgrade process	89
Avaya Room System C130	
cabling	33
physical layout	15
Avaya Room System C170	
cabling	35
physical layout	18
Avaya Room System C190	
cabling	36
physical layout	20
Avaya support website	103

B

banner	
configuring	86

basic configuration	
performing from GUI menu	41
black screen	98
blocklist	
adding IP address	85
boot-up issues	98

C

C100	
installation checklist	26
C100 series	
indicator	22
safety precautions	9
C100 Series	
connecting	38
emergency call handling	11
powering on	38
C130	
cabling	33
description	15
overview	15
physical layout	15
TV-mounting	28
wall-mounting	27
C170	
cabling	35
description	17
overview	17
physical layout	18
wall-mounting	31
C190	
cabling	36
description	20
overview	20
physical layout	20
cabling	
Avaya Room System C130	33
Avaya Room System C170	35
Avaya Room System C190	36
calls	
configuring	60
configuring codec display name	56
viewing quality details from web interface	96
cannot join calls	98
capturing	
network traffic from web interface	96
certificates	
deleting	84
managing in the web interface	83
viewing details	84
codec	
upgrading from GUI menu	50

codec (<i>continued</i>)		
viewing details	49	
viewing details from web interface	96	
codec name		
configuring	85	
configuring for calls	56	
collection		
delete	101	
edit	101	
generating PDF	101	
sharing content	101	
components	25	
C130	15	
C170	18	
C190	20	
configuration		
exporting from web interface	88	
factory reset from GUI menu	50	
factory reset from web interface	92	
importing from web interface	89	
configuring		
audio codecs	68	
audio output advanced settings	64, 65	
audio settings from GUI menu	47	
banner	86	
basic settings from GUI menu	41	
blocklist	85	
call options	60	
codec as MCU	61	
codec name	85	
codec name for calls	56	
date and time	87	
firewall settings	76	
global security settings	58	
global settings from GUI menu	43	
H.323 account	56	
H.323 account settings from GUI menu	45	
H.323 protocol	79	
H.323 protocol encryption	79	
H.323 recording	73	
IP settings	75	
layout settings from GUI menu	49	
LDAP settings	82	
logging	88	
network settings from GUI menu	46	
quality of service	76	
recording to USB	74	
RTMP recording	72	
scrolling captions	86	
SIP account	57	
SIP account settings from GUI menu	44	
SIP protocol	80	
SIP protocol encryption	81	
SNMP settings	78	
video codecs	71	
video encoding and decoding	71	
video settings from GUI menu	48	
connecting		
device management platform	59	
power adapter	38	
content		
publishing PDF output	101	
searching	101	
sharing	101	
sort by last updated	101	
watching for updates	101	
D		
date and time		
web interface	87	
deleting		
certificates	84	
log information from web interface	97	
description		
C130	15	
C170	17	
C190	20	
device management platform		
connecting	59	
Diagnostics		
web interface menu	93	
Diagnostics menu		
capturing network traffic	96	
clearing log information	97	
downloading log files	97	
log levels	88	
refreshing video encoding	94	
testing audio input	94	
testing network connection	95	
viewing audio volume level	93	
viewing call quality details	96	
viewing codec details	96	
viewing video input details	94	
digital microphone		
configuring	69	
display name		
configuring for calls	56	
document changes	12	
document purpose	9	
documentation center	101	
finding content	101	
navigation	101	
documentation portal	101	
downloading		
log files from web interface	97	
upgrades from GUI menu	50	
upgrades from web interface	91	
E		
echo		
troubleshooting	99	
echo elimination		

echo elimination (<i>continued</i>)		Home screen (<i>continued</i>)	
configuring	66	accessing GUI menu settings	41
EMCU authentication	61		
exporting		I	
configuration to USB	88	importing	
F		configuration to USB	89
factory reset		input	
from web interface	92	adding for video	69
performing from GUI menu	50	configuring for audio	62
finding content on documentation center	101	input audio	99
firewall settings		installation	26
configuring	76	installation checklist	26
flickering		installing	
video troubleshooting	99	connecting	38
flow		powering on	38
upgrade process	89	TV-mounting	28
G		wall-mounting	27 , 31
global security settings		IP settings	
configuring	58	configuring	75
global settings		K	
configuring from GUI menu	43	KB	
GUI menu		Support site	103
accessing settings	41	L	
configuring audio settings	47	language	
configuring global settings	43	web interface before login	54
configuring H.323 account settings	45	web interface from Settings	55
configuring layout settings	49	languages	
configuring network settings	46	supported list	25
configuring SIP account settings	44	layout	
configuring video settings	48	configuring for HDMI output	70
overview	40	layout settings	
performing basic configuration	41	configuring from GUI menu	49
performing factory reset	50	LDAP settings	
upgrading codec	50	configuring	82
viewing codec details	49	list	
viewing network details	47	supported languages	25
H		log files	
H.323		clearing from web interface	97
configuring recording	73	downloading from web interface	97
H.323 account		log levels	88
configuring	56	logging	
H.323 account settings		web interface	88
configuring from GUI menu	45	logging in	
H.323 protocol		web interface	54
configuring	79	M	
configuring encryption	79	managing	
HDMI output		certificates	83
configuring layout	70	recording	72
Home page	54	MCU mode	
Home screen			

MCU mode (<i>continued</i>)		quick configuration	
configuring for codec	61	performing from GUI menu	41
microphone		R	
configuring digital microphone	69	recording	
MQTT		configuring audio codecs	68
connecting to device management platform	59	configuring for USB	74
N		configuring H.323	73
network		configuring RTMP	72
capturing traffic from web interface	96	configuring video codecs	71
testing connection from web interface	95	configuring video encoding and decoding	71
viewing details	47	overview	72
network settings		related documentation	101
configuring from GUI menu	46	remote control	23
O		cannot manage PTZ	100
output		resetting	
configuring for audio	63	configuration from GUI menu	50
configuring for video	70	resolution	
configuring HDMI layout	70	low for video output	100
output audio	99	RS232 connection	100
overview		RTMP	
C130	15	configuring recording	72
C170	17	RTSP	
C190	20	adding camera address	69
Diagnostics menu in web interface	93	S	
GUI menu	40	scrolling captions	
Settings menu in web interface	52	configuring	86
P		searching for content	101
package list	25	security settings	
pan, tilt, and zoom		adding IP address to blocklist	85
cannot manage with remote control	100	configuring	58
password		H.323 protocol encryption	79
for GUI menu administrator	40	SIP protocol encryption	81
peripherals		setting up	
viewing details	47	audio output advanced settings	64, 65
physical layout		date and time	87
C130	15	firewall configuration	76
C170	18	IP configuration	75
C190	20	LDAP configuration	82
PKCS #12 certificate bundle		logging	88
uploading	83	quality of service	76
placement	26	SNMP configuration	78
positioning	26	web interface language before login	54
power adapter	38	web interface language from Settings	55
presentation		settings	
troubleshooting	100	accessing from Home page	41
Q		audio configuration from GUI menu	47
quality of service		global configuration from GUI menu	43
configuring	76	H.323 account configuration from GUI menu	45
		layout configuration from GUI menu	49
		network configuration from GUI menu	46
		quick configuration from GUI menu	41
		SIP account configuration from GUI menu	44
		video configuration from GUI menu	48

Settings	
GUI menu	40
web interface menu	52
sharing content	101
shortcuts	
remote control	23
signing in	
web interface	54
SIP account	
configuring	57
SIP account settings	
configuring from GUI menu	44
SIP protocol	
configuring	80
configuring encryption	81
SIP TLS encryption	
certificate management	83
uploading PKCS #12 certificate bundle	83
SNMP settings	
configuring	78
software	
factory reset	92
upgrading	89
upgrading from GUI menu	50
upgrading from web interface	91
sort documents	101
start-up issues	98
support	103
supported languages	25

T

target audience	9
testing	
audio input from web interface	94
network connection from web interface	95
TLS authentication	
deleting certificates	84
viewing certificate details	84
troubleshooting	
black screen after boot-up	98
cannot manage PTZ settings	100
echo during calls	99
no input audio	99
no output audio	99
presentation issues	100
stuck at boot-up	98
video flickering	99
video output resolution	100
TV-mounting	28

U

unregistering	
H.323 account	56
SIP account	57
updating	

updating (<i>continued</i>)	
video encoding from web interface	94
upgrading	
codec software from GUI menu	50
codec software from web interface	91
flow	89
uploading	
PKCS #12 certificate bundle	83
USB	
configuring recording	74
exporting configuration	88
importing configuration	89
USB audio	
configuring	67

V

video	
configuring codecs	71
configuring video encoding and decoding	71
flickering	99
low output resolution	100
presentation issues	100
refreshing encoding from web interface	94
viewing input details from web interface	94
video input	
adding	69
video output	
configuring	70
video settings	
configuring from GUI menu	48
viewing	
audio volume level from web interface	93
call quality details from web interface	96
certificate details	84
codec details	49
codec details from web interface	96
log levels	88
network and peripheral details	47
video input details from web interface	94

W

wall-mounting	27 , 31
watchlist	101
web interface	
accessing	54
adding IP address to blocklist	85
adding video input	69
capturing network traffic	96
certificate management	83
changing language before login	54
changing language from Settings	55
clearing log information	97
configuring audio codecs	68
configuring audio input	62
configuring audio output	63

web interface (<i>continued</i>)	white list	92
configuring banner		86
configuring call options		60
configuring codec as MCU		61
configuring codec display name for calls		56
configuring codec name		85
configuring digital microphone		69
configuring echo elimination		66
configuring firewall settings		76
configuring global security settings		58
configuring H.323 account		56
configuring H.323 encryption		79
configuring H.323 protocol		79
configuring H.323 recording		73
configuring HDMI output layout		70
configuring IP settings		75
configuring LDAP settings		82
configuring quality of service		76
configuring recording to USB		74
configuring RTMP recording		72
configuring scrolling captions		86
configuring SIP account		57
configuring SIP encryption		81
configuring SIP protocol		80
configuring SNMP settings		78
configuring USB audio		67
configuring video codecs		71
configuring video encoding and decoding		71
configuring video output		70
connecting to device management platform		59
deleting certificates		84
Diagnostics menu overview		93
downloading log files		97
exporting configuration to USB		88
factory reset		92
importing configuration to USB		89
log levels		88
logging in		54
recording management		72
refreshing video encoding		94
setting up date and time		87
setting up logging		88
Settings menu overview		52
testing audio input		94
testing network connection		95
upgrading codec		91
uploading PKCS #12 certificate bundle		83
viewing audio volume level		93
viewing call quality details		96
viewing certificate details		84
viewing codec details		96
viewing video input details		94
white list		92
web settings		
accessing		54
changing language before login		54
changing language from Settings		55