Installing and Administering Avaya IX Collaboration Unit CU360

Release 11.0
Issue 1
April 2020

Note

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Regulatory Statements

Industry Canada (IC) Statements

RSS Standards Statement

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

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

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

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

Radio Transmitter Statement

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that necessary for successful communication.

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

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

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

Radiation Exposure Statement

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

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

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

Industry Canada (IC) Statements

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

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

Japan Statements

Class B Statement

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

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

Denan Power Cord Statement

Danger:

Please be careful of the following while installing the equipment:

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

警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

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

México Statement

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

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

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

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

Class A warning statement for Taiwan EMC certificate

Warning:

This is Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

警告使用者：

此為甲類資訊技術設備，於居住的環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策。

Taiwan Low Power Radio Waves Radiated Devices Statement

802.11b/802.11g/BT:

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

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

低功率電波輻射性電機管理辦法

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

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

U.S. Federal Communications Commission (FCC) Statements

Compliance Statement

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

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

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

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

When using IEEE 802.11a wireless LAN, this product is restricted to indoor use, due to its operation in the 5.15 to 5.25GHz frequency range. The FCC requires this product to be used indoors for the frequency range of 5.15 to 5.25GHz to reduce the potential for harmful interference to co channel mobile satellite systems. High-power radar is allocated as the primary user of the 5.25 to 5.35GHz and 5.65 to 5.85GHz bands. These radar stations can cause interference with and/or damage to this device.

Class B Part 15 Statement

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

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

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

Radiation Exposure Statement

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

EU Countries

This device when installed complies with the essential requirements and other relevant provisions of EMC Directive 2014/30/EU, Radio Equipment Directive 2014/53/EU (RED), and LVD Directive 2014/35/EU. A copy of the Declaration may be obtained from http://support.avaya.com or Avaya Inc., 4655 Great America Parkway, Santa Clara, CA 95054–1233 USA.

WiFi transmitter

- Frequencies for 2412-2472 MHz, transmit power: 17.8 dBm
- Frequencies for 5180-5240 MHz, transmit power: 19.14 dBm

Brazil Statement

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

General Safety Warning

- Use only the Avaya-approved Limited Power Source power supplies specified for this product.
- Ensure that you:
  - Do not operate the device near water.
  - Do not use the device during a lightning storm.
  - Do not report a gas leak while in the vicinity of the leak.
  - For Accessory Power Supply: Use Only Limited Power Supply EDAC EA1019AVRS Output 5Vdc, 3A, and products that conform to Radio Equipment Directive, EU directive 2014/53/EU.
- Do not push objects into holes and ventilation slots of the device.
- Do not place a naked flame source, such as lighted candles, on or near the device.
- Do not intentionally hit the device or place heavy or sharp objects on the device.
- Do not attempt to repair the device yourself. Always use a qualified service agent to perform adjustments and repairs.
- Keep the device away from benzene, diluents, and other chemicals.

Avertissement de sécurité général

- Utilisez uniquement les alimentations par source à puissance limitée approuvées par Avaya et spécifiées pour ce produit.
- Assurez-vous de prendre les précautions suivantes:
  - N'utilisez pas l'appareil à proximité d'une source d'eau.
  - N'utilisez pas l'appareil en cas d'orage.
  - En cas de fuite de gaz, éloignez-vous avant de la signaler.
  - Pour l'alimentation électrique d'un auxiliaire : utilisez uniquement une alimentation à puissance limitée EDAC EA1019AVRS sortie 5Vdc, 3A, et des produits conformes à la directive relative aux équipements radioélectriques, directive UE 2014/53/UE.
- N'enfoncez pas d'objets dans les trous et les orifices de ventilation de l'appareil.
- Ne placez par sur l'appareil ou à proximité de ce dernier une flamme libre, telle que des bougies allumées.
- Ne heurtez pas intentionnellement l'appareil et ne placez pas d'objets lourds ou pointus sur celui-ci.
- Ne tentez pas de réparer vous-même l'appareil. Utilisez toujours un prestataire de services qualifié pour effectuer les réglages et les réparations.
- Conservez l'appareil loin de sources de benzène, de diluants et d'autres produits chimiques.

Trademarks

Contents

Chapter 1: Introduction

Purpose

This document contains information about installing, administering, and maintaining Avaya IX™ CU360. Implementation engineers, administrators, and support personnel will find this document useful.

Chapter 2: Avaya IX™ CU360 overview

Avaya IX™ Collaboration Unit CU360 is an all-in-one video conference endpoint. Avaya IX™ CU360 has a built-in codec, camera, and microphone, and is ideal for video conferences in small rooms.

Avaya IX™ CU360 conferences can be hosted on Avaya Equinox® Media Server, Avaya Equinox® Meetings Online, and Avaya Scopia® Elite 6000 MCU. You can manage Avaya IX™ CU360 using Avaya Equinox® Management. You can also remotely control Avaya IX™ CU360 through Avaya Collaboration Control using IOS and Android devices.

Avaya IX™ CU360 has the following features:

- Excellent video quality with maximum resolution of 1080p@30fps.
- Dual HD video streams that support seamless content sharing at maximum resolution of 1080p@15fps, along with video.
- DVD-quality audio encoding.
- High-quality video and audio using H.263 and H.264. Avaya IX™ CU360 maintains the conference experience even with limited bandwidth or poor network conditions by using the following compression methods.
  - H.264 SVC in point-to-point calls for decoding. SVC extends the H.264 codec standard to dramatically increase error resiliency and video quality without the need for higher bandwidth.
  - H.264 High Profile is a standard for compressing video by up to 25% over H.264 Baseline Profile which supports high definition calls to be held over lower call speeds.
  - NetSense is a proprietary Avaya Equinox® Conferencing technology which optimizes the video quality according to the available bandwidth and minimizes packet loss. As the available bandwidth of a connection varies depending on the data traffic, NetSense's sophisticated algorithm dynamically scans the video stream and changes the video resolution to maximize quality with the available bandwidth.

  These compression methods work only when all endpoints participating in a conference support the protocol.
- Ability to record video conferences to a locally connected USB drive, a network drive, or to a remote server, such as Avaya Equinox® Streaming and Recording, using FTP. You can record video conferences to a remote server only if your Avaya Equinox® Conferencing deployment includes Avaya Equinox® Streaming and Recording.

Avaya IX™ CU360 interfaces

Avaya IX™ CU360 supports the following interfaces:

- A compatible touch screen monitor or external keyboard and mouse connected to Avaya IX™ CU360.
- The Avaya IX™ CU360 remote control unit. You can view the user interface on a connected monitor.
- The Avaya IX™ CU360 web interface.
- Avaya Collaboration Control using iOS and Android devices. You cannot configure Avaya IX™ CU360 using the application.

  For more information, see *Using Avaya Collaboration Control for iOS* and *Using Avaya Collaboration Control for Android* at the Avaya Support website: http://support.avaya.com/.
- Avaya Equinox® Management

Supported functions

Functions	Remote control unit	Touch screen monitor or keyboard and mouse	Web interface	Avaya Collaboration Control	Avaya Equinox® Management
Navigate the GUI menu	✔	✔	✔	✔	—
Perform user functions	✔	✔	✔	✔	—
Split and launch appications	✔	✔	✔ Mouse only	✔ Mouse only	—
Chat with conference participants	—	—	✔	✔	—
Configure Avaya IX™ CU360	✔	✔	✔	—	✔
Configure OS settings	✔	✔	✔ Mouse only	✔ Mouse only	—
Upgrade Avaya IX™ CU360	✔	✔	✔	✔ Mouse only	✔

Table continues…

Functions	Remote control unit	Touch screen monitor or keyboard and mouse	Web interface	Avaya Collaboration Control	Avaya Equinox® Management
Mass Avaya IX™ CU360 upgrades	—	—	—	—	✔
Get logs	—	—	✔	—	✔

Mouse only: You can perform these functions using only mouse emulation in the application or web interface.

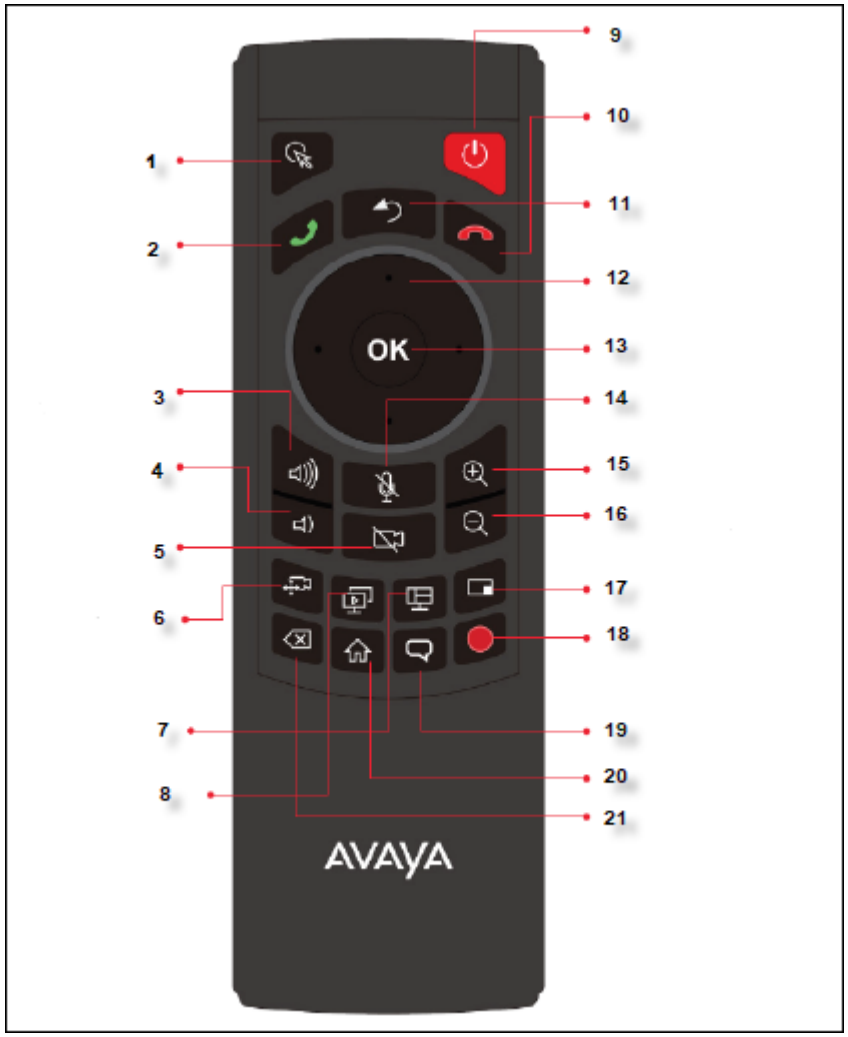
Related links

Logging in to the Avaya IX CU360 web interface on page 27

Avaya IX™ CU360 remote control unit

Avaya IX™ CU360 supports a remote control unit with 2.4GHz optical air mouse and keyboard features.

Using the Avaya IX™ CU360 remote control unit, you can scroll through menus with the arrow key and pressing the OK key to select options. You can also display or hide the mouse pointer using the Mouse key.



Key no.	Key name
1	Mouse
2	Call or accept call
3	Increase volume
4	Decrease volume

Table continues…

Key no.	Key name
5	Video disable or enable
6	Control far or near camera
7	Change layout
8	Start or stop presentation
9	Power button
10	Decline call or disconnect
11	Back
12	Arrow keys to pan, tilt, and zoom camera and navigate menus
13	OK button
14	Audio mute or enable
15	Zoom in
16	Zoom out
17	Change PiP position
18	Start or stop recording
19	Enable/Disable Tracking Camera
20	Home
21	Delete

Related links

Pairing the remote control unit with Avaya IX CU360 on page 27

Avaya IX™ CU360 camera and LED indicators

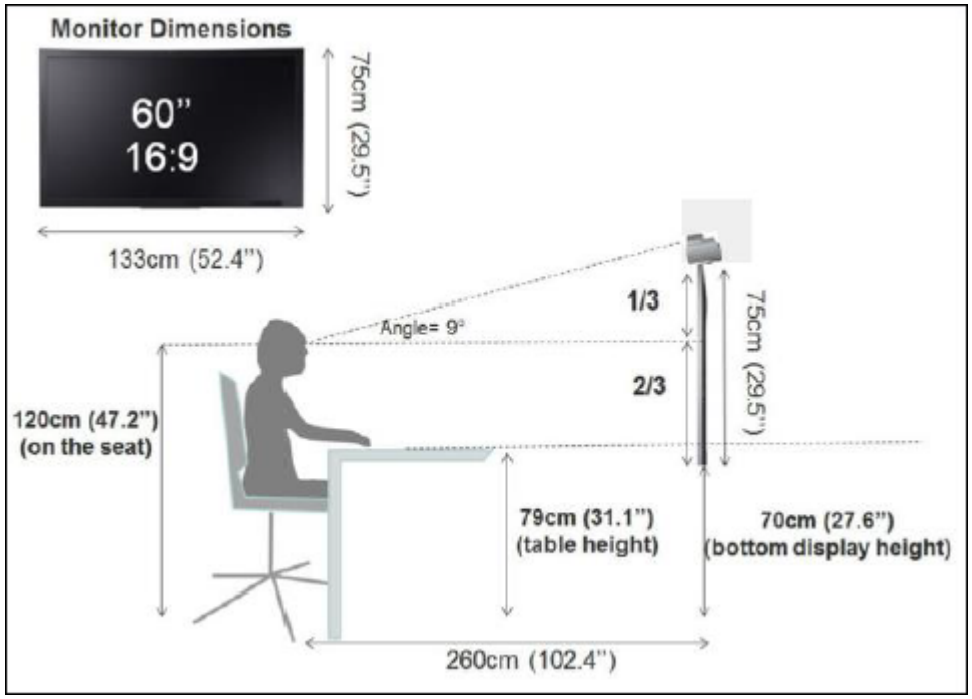
The Avaya IX™ CU360 endpoint has a camera and LED indicators. The camera also has a pan and tilt mechanism.

The Avaya IX™ CU360 camera is equipped with two rows of lateral LED strips on the front with a circular crown of LEDs around the camera lens. The LEDs display different colors and animation effects based on the camera status. The camera supports zooming the video from the web

interface, the remote control unit, and Avaya Collaboration Control. When the camera is zoomed in, you can also digitally pan and tilt the camera.

Status	Circular LED crown	Lateral LED strips
Alarms	Red	Red
Idle	Yellow	—
Idle, muted, or sleep mode	Blue	Blue
In a conference	Green	—
In a conference with audio muted	Blue	Blue
In a conference with video privacy mode	Green Blue, if audio is muted	Red
Calls being established	Red, rotating	Red
Upgrade in progress	Red, rotating	Red

Avaya IX™ CU360 optimum room setup



The Avaya IX™ CU360 experience can be optimized in the following manner:

- Choose a huddle room with a capacity to seat up to four people.
- Place Avaya IX™ CU360 on the top of a 1080p or 4k resolution monitor.

The Avaya IX™ CU360 embedded microphone efficiently captures audio in huddle rooms, while the monitor plays the audio output. You can manually adjust the camera to focus on an individual

seated in front of the camera and digitally pan and tilt the camera or use the auto tracking feature of the camera.

Microsoft Exchange calendar integration

Avaya IX™ CU360 integrates with Microsoft Outlook calendar using Exchange Web Services (EWS).

- Use Avaya IX™ CU360 to view your personal calendar.
- Configure an email account for Avaya IX™ CU360 to use the endpoint as a participant in meetings.
- Associate a room with Avaya IX™ CU360 to use the endpoint as a room in meetings.

Avaya IX™ CU360 must be able to gain access to the EWS URL on the Internet or a private network. Avaya IX™ CU360 must also be able to connect to the Microsoft Exchange server address using an HTTPS connection through your enterprise network firewalls and proxies.

Personal Account Mode

You can view your personal calendar on Avaya IX™ CU360 using your credentials. When you mark a calendar item as private, Avaya IX™ CU360 replaces the title with Private Meeting.

Video Endpoint Account Mode

You can create a dedicated email account for Avaya IX™ CU360, using which you can add the endpoint to meetings as a participant. You can also use the account credentials to view the endpoint calendar, which displays the meetings where the endpoint is added as a participant.

You must have administrator-level access to Microsoft Exchange Server to create the email account for Avaya IX™ CU360.

Room Resource and Delegate Account Mode

You can create a room as a resource and a delegate account to view the room calendar in Avaya IX™ CU360. You must associate the room with Avaya IX™ CU360, using which you can add the endpoint to meetings as a room. Microsoft Outlook account credentials contain an email address and a password, while room resource accounts contain only an email address.

You must have administrator-level access to Microsoft Exchange Server to create room resources and delegate accounts.

Related links

Configuring a Microsoft Exchange calendar in Avaya IX CU360 on page 49

Avaya Spaces integration

Avaya Spaces is a cloud-based team collaboration and meeting application with all forms of modern communications, such as voice, video, email, and instant messaging and features such as

screen sharing, file sharing, and scheduling meeting. You can use Avaya Spaces from anywhere on any device, such as computers, tablets, and mobile phones. Using the combined collaboration features of Avaya Spaces, users can manage projects and perform various tasks without having to juggle different tools.

Designed for teams that need an effective way to enable communications, manage tasks, and be more productive without being overwhelmed by email, Avaya Spaces provides you with just the right balance of features and simplicity. Avaya Spaces has a user-friendly interface for users who need a simple and effective way to track communications and manage tasks.

Avaya Spaces integrates with Avaya IX™ CU360 to support seamless collaboration among users. Users can add Avaya IX™ CU360 as an independent participant in meetings after entering a verification code from computers or scanning a QR code from tablets or mobile phones.

For more information, see:

- *Avaya Spaces User Manual* on the Avaya Spaces application.
- *Avaya IX™ Collaboration Unit CU360 Quick Setup Guide for Avaya Spaces Room* at the Avaya Support website: https://support.avaya.com
- Introductory information: Getting Started with Avaya Spaces
- Avaya Spaces trial: Spaces Trial

Supported web browsers

Avaya IX™ CU360 supports the following web browsers for its web interface:

- Microsoft Internet Explorer Release 8 or later
- Google Chrome Release 11 or later
- Mozilla Firefox Release 3.6 or later
- Apple Safari Release 5 or later
- Opera Release 11 or later
- Microsoft Edge Release 38 or later

Supported resolutions

Conference type	Video resolution	Web collaboration resolution	Recording resolution	Playback resolution
Video conference	1080p@30fps	—	—	—

Table continues…

Conference type	Video resolution	Web collaboration resolution	Recording resolution	Playback resolution
Video conference with web collaboration	1080p@15fps	1080p@15fps	—	—
Video conference with web collaboration and recording	1080p@7fps	1080p@7fps	720p@25fps	—
Video conference with recording playback	1080p@7fps	—	—	720p@25fps
Video through Avaya AV Grabber	• 1920x1080 @60fps: HD 1080p • 1680x1050 @60fps: WXGA+ • 1360x768 @60fps • 1280x1024 @60fps: SXGA • 1280x768 @60fps: WXGA • 1280x720 @60fps: HD 720p • 1024x768 @60fps: XGA • 800x600 @60fps: SVGA	1080p@15fps	—	—

Third-party applications in Avaya IX™ CU360

Avaya IX™ CU360 supports installation and use of free Android-based third-party applications. You can install the applications using the Apps & Tools option or the default web browser of Avaya IX™ CU360.

Before you install applications, you must authorize installation of applications from unknown sources in the Android settings of Avaya IX™ CU360. Administrators can restrict installation of third-party applications to select users by configuring a PIN, a pattern, or a password.

The following applications are popularly used in Avaya IX™ CU360:

- Microsoft Office Word: Split and share supported, along with use as a standalone application.
- Microsoft Office Powerpoint: Split and share supported, along with use as a standalone application.
- VLC media player: Split and share supported, along with use as a standalone application.
- Dropbox: Split and share supported, along with use as a standalone application.
- Bluejeans: Supported as a standalone application. You can use the Bluejeans application or configure the Bluejeans SIP server to use with the Avaya IX™ CU360 video conferencing application.
- Cisco WebEx: Screen sharing from WebEx supported for users with premium accounts. You can use the WebEx application or configure the WebEx SIP and H.323 servers to use with the Avaya IX™ CU360 video conferencing application.
- Microsoft Skype for Business: Supported as a standalone application.
- Microsoft Teams: Supported as a standalone application. If required by your company:
  - The Mobile Application Management software for Microsoft Teams must be configured.
  - The Microsoft InTune Company Portal application must be installed on Avaya IX™ CU360 and registered to the InTune server.
- Zoom: Supported as a standalone application. You can use the Zoom application or configure the Zoom SIP server to use with the Avaya IX™ CU360 video conferencing application.
- Open GApps: Supported for Google Play Store applications and Google Mobile Services.

The Avaya IX™ CU360 video conferencing application must be minimized before you use third-party applications. Minimizing the third-party application gives third-party applications access to the audio and video peripherals.

Important:

- Avaya cannot certify its products for all third-party applications because of the multiple variations and complex interactions of the application versions and deployment options.
- Avaya does not test or support the third-party applications installed on Avaya IX™ CU360.
- Google Play Store and Google Mobile Services are not installed or supported on Avaya IX™ CU360. Some third-party applications might not work properly without these services.
- Ensure the following when you Install third-party application and antivirus software:
  - Test third-party applications before installing the third-party applications.
  - Availability of adequate hardware and software capacity for third-party applications.
  - No conflicts in TCP and UDP ports.
  - No conflicts in protocols.

- Monitor the third-party applications and OS for alarms, connectivity issues, and performance degradation.

For more information about:

- Interoperability with third-party applications, see *Reference Guide for Interoperability Avaya IX Collaboration Unit CU360*, at https://downloads.avaya.com/css/P8/documents/101062424.
- The latest and most accurate compatibility information for Avaya IX™ CU360, use the Compatibility Matrix tool on the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx. You must sign up for an Avaya Support Account to gain access the website.

Related links

Installing third-party applications in Avaya IX CU360 on page 49

Support for third-party applications on Avaya IX™ CU360

- Avaya Spaces does not support:
  - Changing Bluetooth settings when an Avaya IX™ CU360 meeting is in progress.
  - Audio Rx
- GoToMeeting does not support the frame grabber feature.

Features	Avaya Spaces	Microsoft Teams Microsoft Skype	BlueJeans Video Conferencing	Google Hangouts	Pexip	Cisco Webex Meetings	StarLeaf	Zoom	Rainbow	RingCentral Meetings RingCentral Glip	GoToMeeting
Features that the Avaya IX™ CU360 remote control unit supports											
Camera PTZ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Camera flip	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Voice tracking	No	No	No	No	No	No	No	No	No	No	No
Audio and video muting	Yes	No	No	No	No	No	No	No	No	No	No
Volume	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Call	No	No	No	No	No	No	No	No	No	No	No
Presentation	No	No	No	No	No	No	No	No	No	No	No
Recording	No	No	No	No	No	No	No	No	No	No	No
Features that Avaya IX™ CU360 supports											
Echo canceller	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bluetooth	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
GLAN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Wifi	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Touch screen	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table continues…

Features	Avaya Spaces	Microsoft Teams Microsoft Skype	BlueJeans Video Conferencing	Google Hangouts	Pexip	Cisco Webex Meetings	StarLeaf	Zoom	Rainbow	RingCentral Meetings RingCentral Glip	GoToMeeting
Audio and video grabber	No	No	No	No	No	No	No	No	No	No	No
USB devices	No	No	No	No	No	No	No	No	No	No	No
Miracast screen sharing	Yes USB mouse and keyboard	Yes USB mouse, keyboard, microphone, and speakers	Yes USB mouse and keyboard	Yes USB mouse, keyboard, microphone, and speakers	Yes USB mouse and keyboard	Yes USB mouse and keyboard	Yes USB mouse and keyboard	Yes USB mouse and keyboard	Yes USB mouse and keyboard	Yes USB mouse and keyboard	Yes USB mouse and keyboard
Video resolution	720p	640 x 480p	288p	480p, 288p	480p	720p	352 x 288p	640 x 480p	576p	640 x 480p	320 x 240p

Related links

Installing third-party applications in Avaya IX CU360 on page 49
Third-party applications in Avaya IX CU360 on page 19

Chapter 3: Initial setup and connectivity

Checklist for setting up Avaya IX™ CU360

No.	Task	Description	Notes	✔
1	Set up the Avaya IX™ CU360 hardware.	Connecting Avaya IX CU360 on page 25	—	
2	Switch on Avaya IX™ CU360.	Switching Avaya IX CU360 on or off on page 26	—	
3	Pair the Avaya IX™ CU360 remote control unit.	Pairing the remote control unit with Avaya IX CU360 on page 27	—	
4	Configure basic settings	Configure the basic settings: • Automatically: Configuring Avaya IX CU360 automatically on page 28 • Automatically for Avaya Equinox® Conferencing: Configuring Avaya IX CU360 automatically for Avaya Equinox® Conferencing on page 29 • Manually: Configuring Avaya IX CU360 manually on page 30	You can use one of the following interfaces to configure settings: • The Avaya IX™ CU360 remote control unit. • The Avaya IX™ CU360 web interface • Avaya Scopia® Control using iOS devices • Avaya Collaboration Control using Android devices	

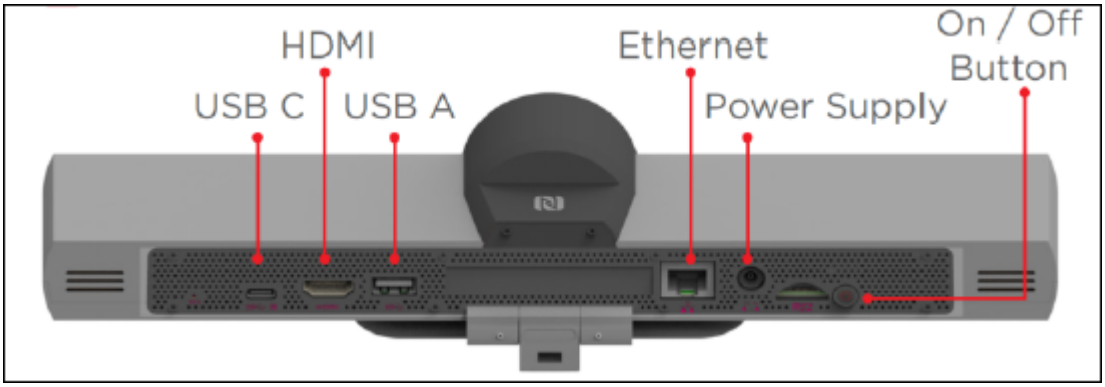
Connecting Avaya IX™ CU360

About this task

Avaya IX™ CU360 contains the following standard equipment:

- Endpoint
- Remote control unit with batteries

- HDMI cable
- Power adapter
- Rubber cap for camera



Procedure

1. Secure the Avaya IX™ CU360 endpoint on an external monitor using the hinge at the bottom of the endpoint.
2. Connect the HDMI cable in the HDMI ports of Avaya IX™ CU360 and the external monitor.
3. Connect the power adapter.

Switching Avaya IX™ CU360 on or off

About this task

The power button of Avaya IX™ CU360 on the rear of the device. You can use the power button to:

- Switch Avaya IX™ CU360 on or off.
- Change the Avaya IX™ CU360 mode to standby or wake up the device from the standby mode.

Procedure

Do one of the following:

- To switch Avaya IX™ CU360 on or off, press and hold the power button.
- To change the mode of Avaya IX™ CU360 to standby or wake up the device from the standby mode, press the power button.

Pairing the remote control unit with Avaya IX™ CU360

Before you begin

Insert two AAA batteries in the remote control unit.

Procedure

1. Remove the power cable of Avaya IX™ CU360.
2. On the remote control unit, simultaneously press the following two keys until the small blue LED indicator on Avaya IX™ CU360 flashes:
   - Back
   - OK
3. When the LED indicator is flashing, insert the power cable plug of Avaya IX™ CU360 in the power socket.

   Ensure that the remote control unit is in proximity to Avaya IX™ CU360 when you insert the power cable.

Result

The LED indicator of the remote control unit stops flashing to indicate successful pairing with Avaya IX™ CU360.

Next steps

If the remote control unit pairing fails, remove all cables from Avaya IX™ CU360, and repeat the procedure.

Related links

Avaya IX CU360 remote control unit on page 13

Logging in to the Avaya IX™ CU360 web interface

About this task

The home page of Avaya IX™ CU360 displays the IP address of the endpoint on the top.

Change the default login credentials when you log in to the web interface for the first time.

Procedure

1. In a web browser, navigate to the IP adress of Avaya IX™ CU360.

   Avaya IX™ CU360 displays the login page.
2. Enter the following:
   - **User Name**: The default user name is Admin.
   - **Password**: The default password is 1234.

- **Language**: Select a language from the drop-down list. This field is optional.

3. Click **Login**.

Configuration of Avaya IX™ CU360 basic settings

Avaya IX™ CU360 supports the following three methods to configure the basic settings:

- Easy to Start
- Auto Provisioning
- Manual Setup

Easy to Start

An automatic configuration option to set up Avaya IX™ CU360 as a SIP endpoint if you have Avaya Equinox® Conferencing deployed in your enterprise network. The auto configuration feature, which uses DNS discovery, must be enabled for your Avaya Equinox® Conferencing deployment. Avaya IX™ CU360 automatically receives the SIP configuration and other settings from the Avaya Equinox® Conferencing deployment. You will need to enter your personal credentials or the phone number and extension of your video endpoint for the configuration.

Auto Provisioning

An automatic configuration option using a service code that you must provision for Avaya IX™ CU360. When you switch on Avaya IX™ CU360 for the first time, it prompts you to enter the service code, after which the basic settings are automatically configured. Using this option, Avaya IX™ CU360 can be provisioned as an H.323 or SIP endpoint, automatically connects to the enterprise directory, and can be set up to upgrade automatically.

Manual Setup

A manual configuration option using the quick setup wizard to configure Avaya IX™ CU360 and the network settings yourself. You can also use this option to modify the existing configuration.

Configuring Avaya IX™ CU360 automatically

About this task

Avaya IX™ CU360 prompts you to enter the service code that initiates the automatic configuration when you start the endpoint for the first time. The administrator must provision Avaya IX™ CU360 for automatic configuration and to send the service code to users.

Procedure

1. Start Avaya IX™ CU360.

   Avaya IX™ CU360 displays the quick setup wizard.

2. From the drop-down list, select your preferred language.
3. **(Optional)** To configure Wi-Fi, click **Wi-Fi**, and configure your wireless network settings.

4. Click **Next**.
5. Click **Auto Provisioning**.

   Avaya IX™ CU360 displays the window to enter the service code.
6. Enter the service code.

   You can enter the service code in the following two formats:

   - A full 12–digit service code: The first 5 digits identify the Avaya Equinox® Management server, and the subsequent 7 digits identify the Avaya IX™ CU360 endpoint.
   - A partial 5–digit service code: The 5 digits identify the Avaya Equinox® Management server, while the subsequent 7 digits can be either empty or contain zeros.

   Avaya IX™ CU360 displays the name of the Avaya IX™ CU360 endpoint configuration that matches the service code.
7. Click **Next**.

Result

- If you entered the full 12–digit service code, the Avaya IX™ CU360 configuration is complete.
- If you entered a partial 5–digit service code, Avaya Equinox® Management displays a red clock icon against the Avaya IX™ CU360 name. The administrator must complete the Avaya IX™ CU360 configuration, which is pushed to the endpoint.

Configuring Avaya IX™ CU360 automatically for Avaya Equinox® Conferencing

About this task

Configure Avaya IX™ CU360 automatically as a video conferencing endpoint in Avaya Equinox® Conferencing. Use a wired network connection for best results.

The quick setup wizard automatically configures the SIP settings for Avaya IX™ CU360. The setup wizard gets the SIP settings from the network server discovered during the automatic configuration process.

Procedure

1. Start Avaya IX™ CU360.

   Avaya IX™ CU360 displays the quick setup wizard.
2. From the drop-down list, select your preferred language.
3. **(Optional)** To configure Wi-Fi, click **Wi-Fi**, and configure your wireless network settings.
4. Click **Next**.
5. Click **Easy to Start**.

   Avaya IX™ CU360 prompts you to enter your email address.

6. Type your email address, and click **Next**.

   Avaya IX™ CU360 prompts you to choose your environment.

7. Select your environment from the drop-down list, and click **Next**.

   Avaya IX™ CU360 prompts you to enter your login credentials.

8. Enter your login credentials, and click **Next**.

   Based on your network configuration, you might have to enter your:

   - Network login credentials.
   - SIP phone extension number and password.

   Avaya IX™ CU360 prompts you that the configuration is complete.

9. Click **Done**.

Configuring Avaya IX™ CU360 manually

About this task

Manually configure the Avaya IX™ CU360 basic settings, such as the system name, language, and network settings, using the quick setup wizard. Some settings might be customized for your enterprise.

Avaya IX™ CU360 automatically displays the quick setup wizard when you switch on Avaya IX™ CU360 or log in to the web interface for the first time.

Procedure

1. Start Avaya IX™ CU360.

   Avaya IX™ CU360 displays the quick setup wizard.

2. From the drop-down list, select your preferred language.
3. **(Optional)** To configure Wi-Fi, click **Wi-Fi**, and configure your wireless network settings.
4. Click **Next**.
5. Select **Manual Setup**.

   Avaya IX™ CU360 displays the Welcome to Avaya cu360 window.

6. Configure the following fields:

   - **System Name**
   - **Country**
   - **Language**
   - **Protocol Type**

7. Click **Next**.

   Avaya IX™ CU360 displays the Configure TCP/IP (GLAN) window.

8. Configure the following fields:
   - **IP Address Mode**
   - **IP Address**
   - **Subnet Mask**
   - **Gateway**
   - **DNS**
9. Click **Next**.

   Avaya IX™ CU360 displays the Configure more window.
10. **(Optional)** Configure the following features:
    - **Wi-Fi**
    - **Bluetooth**
    - **Graphic Adjustment**: Adjust the graphic to fit your monitor.
11. Click **Next**.

    Avaya IX™ CU360 displays the Configure Gatekeeper window.
12. Configure the following fields:
    - **Use Gatekeeper**
    - **Mode**
    - **Gatekeeper Address**
    - **E.164**
13. **(Optional)** Click **Next**.

    Avaya IX™ CU360 displays the SIP settings only if you select **SIP** or **H.323 and SIP** in **Protocol Type**.

    Avaya IX™ CU360 displays the Configure SIP window.
14. **(Optional)** Configure the following fields:
    - **User**
    - **Authentication Name**
    - **Authentication Password**
    - **Use SIP Server**
    - **Server Address**
15. Click **Done**.

Quick Setup field descriptions

Name	Description
System Name	The name of the Avaya IX™ CU360 endpoint. Avaya IX™ CU360 also uses the system name as the user name to register for SIP and H.323.
Country	The country where Avaya IX™ CU360 is located. The value of **Language** and the language of the menu automatically changes based on the language of the country you select.
Language	The language of the menu. You can select different languages for the web interface and the endpoint interface.
Protocol Type	The protocol that Avaya IX™ CU360 must use. • **H.323**: Select this option to register Avaya IX™ CU360 to only a gatekeeper. • **SIP**: Select this option to register Avaya IX™ CU360 to only a SIP server. For redundant SIP-based deployments, you can register the endpoint to maximum three SIP servers. • **H.323 and SIP**: Select this option to register Avaya IX™ CU360 to a gatekeeper and a SIP server. The selection of the protocol, such as SIP or H.323, depends on the protocol that the enterprise network uses.
IP Address Mode	The option to determine whether the IP address is allocated dynamically using DHCP or designated a static IP address. Use static IP addresses for Avaya IX™ CU360 deployed on: • Public networks. • SIP networks where the endpoint is secured using TLS certificates and the certificate requests need static IP addresses.
IP Address	The static IP address. If you do not enter a static IP address, this field displays the allocated dynamic IP address.

Table continues…

Name	Description
Subnet Mask	The subnet mask associated with the static IP address. If you use dynamic IP addresses, this field displays the allocated subnet mask.
Gateway	The default gateway static IP address. If you do not enter a static IP address, this field displays the allocated dynamic gateway IP address.
DNS	The DNS server IP address. Enter a valid IP address for web collaboration and the cloud-based connection to Avaya Equinox® Management. If you do not enter a static IP address, this field displays the allocated dynamic DNS server IP address.
Use Gatekeeper	The option to choose whether Avaya IX™ CU360 is registered to an H.323 gatekeeper.
Mode	The option to choose whether Avaya IX™ CU360 automatically detects gatekeepers.
Gatekeeper Address	The IP address or the DNS name of the gatekeeper.
E.164	The H.323–based number of Avaya IX™ CU360.
User	The system name. Avaya IX™ CU360 is registered to the SIP server using this name. Avaya IX™ CU360 displays this name in conferences.
Authentication Name	The name to authenticate Avaya IX™ CU360 with the SIP server. This name can be the same as the system name in **User**. This field is optional.
Authentication Password	The password to authenticate Avaya IX™ CU360 with the SIP server. This field is optional.
Use SIP Server	The option to enable registration of Avaya IX™ CU360 with SIP servers. For redundant SIP-based deployment, you can register Avaya IX™ CU360 with maximum three SIP servers.
Server Address	The IP address or the DNS name of the SIP server.

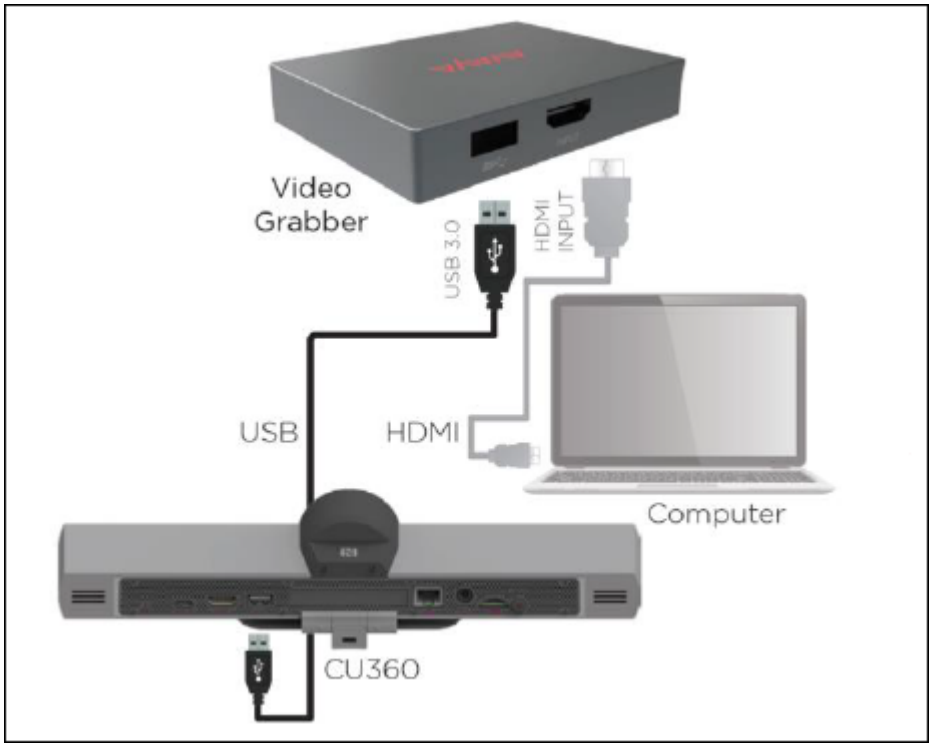
Connecting Avaya AV Grabber to Avaya IX™ CU360

About this task

Avaya AV Grabber is an optional cable kit for Avaya IX™ CU360. Using Avaya AV Grabber, you can connect a computer to Avaya IX™ CU360 with a cable and use the computer to share content in meetings.

The Avaya AV Grabber kit contains:

- An Ethernet cable.
- A USB cable.
- An HDMI swivel connector cable.



When you connect Avaya AV Grabber to Avaya IX™ CU360, the video conferencing application detects the video input from Avaya IX™ CU360 as an additional USB video input. You can use the USB option to share content from Avaya AV Grabber.

Avaya AV Grabber supports sharing video and content in Avaya IX™ CU360 meetings.

Procedure

1. Using an HDMI cable, connect a computer to the HDMI input connector of Avaya AV Grabber.

   The HDMI cable is not included in the optional Avaya AV Grabber kit.

2. Using the USB cable, connect Avaya AV Grabber to the USB port of Avaya IX™ CU360.

If you use a USB hub, ensure that the USB hub supports the USB 3.0 standard and is switched on.

Connecting Avaya B109 Conference Phone to Avaya IX™ CU360 using Bluetooth

About this task

When you pair a Bluetooth device with Avaya IX™ CU360, Avaya IX™ CU360 automatically disables the default audio output to the HDMI connection.

This procedure is specific to Avaya B109 Conference Phone.

Before you begin

Enable Bluetooth on Avaya IX™ CU360 and Avaya B109 Conference Phone.

Procedure

1. On Avaya B109 Conference Phone, press the Bluetooth button for two seconds.
   - Avaya B109 Conference Phone becomes visible to other Bluetooth devices.
   - The Bluetooth window of Avaya IX™ CU360 displays Avaya B109 Conference Phone in the list of available devices.
2. On Avaya IX™ CU360, select Avaya B109 Conference Phone to complete the pairing.

Related links

Configuring Bluetooth connectivity in Avaya IX CU360 on page 48

Chapter 4: Initial administration

Configuring call answering preferences in Avaya IX™ CU360

Procedure

1. Do one of the following:
   - From the endpoint, click **Configure** > **Calling**.
   - From the web interface, click **Basic Settings** > **Call-Answer mode** > **General**.
2. Configure the following fields:
   - **Mute**
   - **Volume**
   - **Video Privacy**
   - **Do not Disturb**
   - **DnD Mode**
   - **Automatic Answer**
   - **Answer after (Rings)**
   - **Ringing Volume**
   - **Confirm Disconnect**
3. On the web interface, click **Save**.

Calling field descriptions

Name	Description
Automatic Answer	Automatically answer incoming calls. The behavior of this feature depends on the configuration. The options are: • **Yes always**: Avaya IX™ CU360 automatically answers all incoming calls. If the endpoint interface is on the home page, Avaya IX™ CU360 does not prompt you before automatically answering calls. • **Yes trusted always**: Avaya IX™ CU360 automatically answers all incoming calls from trusted contacts. If the endpoint interface is on the home page, Avaya IX™ CU360 does not prompt you before automatically answering calls. • **Never**: Avaya IX™ CU360 does not automatically answer calls.
Answer after (Rings)	The option to configure a specific number of rings after which Avaya IX™ CU360 automatically answers calls. This optional field is active only if you configure **Automatic Answer**.

Enabling the Avaya IX™ CU360 advanced settings

Procedure

1. Click **Configure** > **General**.

   Avaya IX™ CU360 displays the General settings window.

2. Select **Yes** for **Show Advanced Settings**.

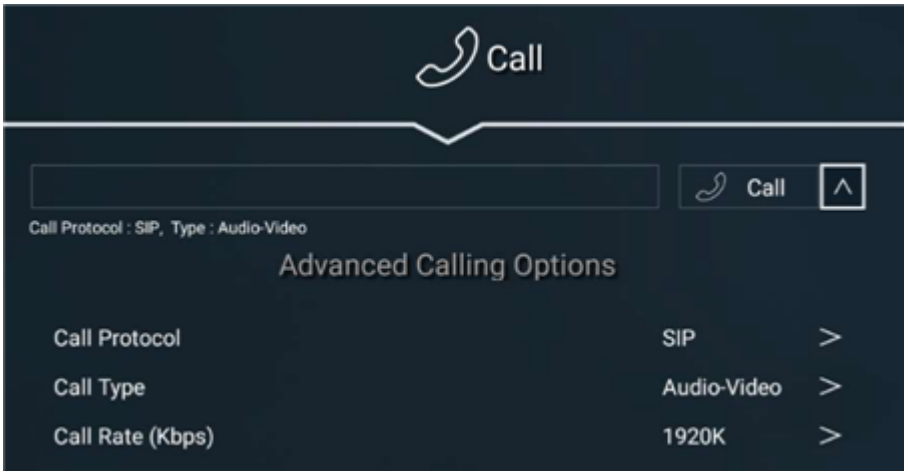
Result

Avaya IX™ CU360 displays the advanced settings.

Configuring the Avaya IX™ CU360 advanced calling options

About this task

Configure advanced settings of calls for new dial strings.



Procedure

1. Select **Call**.

   Avaya IX™ CU360 displays the Call window.

2. Click .

   Avaya IX™ CU360 displays the Advanced Calling Options window.

3. Configure the following fields:
   - **Call Protocol**
   - **Call Type**
   - **Call Rate (Kbps)**

Advanced Calling Options field descriptions

Name	Description
Call Protocol	The protocol to use in calls. The options are: • **H.323**: The protocol for calls to H.323–based endpoints, such as Avaya endpoints, and for meetings that are hosted on Avaya Scopia® Elite 6000 MCU and Avaya Equinox® Media Server. • **SIP**: The protocol for calls to SIP-based endpoints.
Call Type	The type of the call. The options are: • **Audio-Video** • **Audio-Only**
Call Rate (Kbps)	The specific bandwidth to use for calls. This field is optional. If you do not configure a specific bandwidth to use, Avaya IX™ CU360 uses the maximum available bandwidth.

Configuring Avaya IX™ CU360 to automatically share content

About this task

Configure Avaya IX™ CU360 to automatically share content when you connect your computer with Avaya IX™ CU360 using **Avaya Screen Link**.

Before you begin

Your computer:

- Must have Avaya IX™ Workplace Client installed.
- Must be connected to the same network as Avaya IX™ CU360. If your computer and Avaya IX™ CU360 are connected to different networks, NAT or a firewall must not be configured between the two networks.

Procedure

1. Select **Configure**.

   Avaya IX™ CU360 displays the Configure window.

2. Select **Advanced**.

The default PIN is 1234.

If your administrator configured a PIN to gain access to the advanced settings, Avaya IX™ CU360 prompts you to the enter PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.

3. Select **Presentation**.

   Avaya IX™ CU360 displays the Presentation window.

4. Configure **Local Presentation Mode** to **Automatic**.

Result

Avaya IX™ CU360 automatically displays shared content on the screen to local participants when the endpoint is not participating in meetings. The endpoint also displays alerts for incoming calls.

Disabling the Avaya IX™ CU360 video

About this task

Configure meetings to start with video disabled.

Procedure

1. Do one of the following:
   - From the endpoint, click **Configure** > **Calling**.
   - From the web interface, click **Basic Settings** > **Call-Answer mode** > **General**.
2. Configure **Video Privacy** to **Yes**.
3. On the web interface, click **Save**.

Configuring meeting recording in Avaya IX™ CU360

About this task

Avaya IX™ CU360 saves meeting recordings in the MP4 format. The video stream is recorded in the H.264 format, while the audio stream is recorded in the AAC-LC format.

You can save meeting recordings on a USB device or on the enterprise network. When you save recordings on a USB device, you can transfer the recordings to an external server, such as a generic FTP server or Avaya Equinox® Streaming and Recording Server. To save recordings on the enterprise network:

- The Avaya Equinox® Conferencing deployment must have a recording server.
- The Avaya IX™ CU360 endpoint must be managed by Avaya Equinox® Management, and Avaya Equinox® Management must have remote access to the endpoint.

- The meeting must be hosted on Avaya Scopia® Elite 6000 MCU or Avaya Equinox® Media Server.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure** > **Advanced** > **Utilities** > **Recording**.
   - On the web interface, click **Administrator Settings** > **Utilities** > **Recording** > **General**.
2. Configure the following fields:
   - **Location**
   - **Resolution**
   - **Bitrate**
   - **Audio Alert**
   - **Ignore Mute on Playback**
   - **Video Upload/Delete**: This option is available only on the endpoint menu.
   - **Digital Signature**
   - **Save to External Server**
   - **External Server Type**
   - **FTP Server URL**
   - **FTP Server User**
   - **FTP Server Password**
   - **FTP Secure Connection**
   - **AESR File Owner**
   - **AESR Server Tenant ID**
3. On the web interface, click **Save**.

General field descriptions

Name	Description
Location	The location to store meeting recordings. The options are: • **No Recording**: Disable recording meetings. • **Automatic**: Choose the location every time you start recording meetings. Avaya IX™ CU360 displays the location options when you start recording. This is the default option. • **USB Storage**: Record meetings in a USB storage device. • **Equinox Recording Server**: Record meetings in a location on the enterprise network. - The Avaya Equinox® Conferencing deployment must have a recording server. - The Avaya IX™ CU360 endpoint must be managed by Avaya Equinox® Management, and Avaya Equinox® Management must have remote access to the endpoint. - The meeting must be hosted on Avaya Scopia® Elite 6000 MCU or Avaya Equinox® Media Server.
Resolution	The video resolution of meeting recordings that are stored on USB storage devices. The default 720p@25fps resolution using the H.264 codec is the best supported resolution. If your media player does not support higher resolutions, choose a lower resolution. When you change the resolution, Avaya IX™ CU360 automatically selects the optimal bit rate. You cannot change the resolution of meeting recordings stored on the enterprise network. If you configure **Location** as **Automatic**, Avaya IX™ CU360 applies the configured resolution only to meeting recordings stored on USB storage devices.

Table continues…

Name	Description
Bitrate	The bit rate of the meeting recordings. The bit rate determines the size of the recordings stored on USB storage devices. To use less storage capacity, select a lower bit rate. The bit rate that Avaya IX™ CU360 automatically selects when you configure **Resolution** provides best results. You cannot change the bit rate of meeting recordings stored on the enterprise network. If you configure **Location** as **Automatic**, Avaya IX™ CU360 applies the configured bit rate only to meeting recordings stored on USB storage devices.
Audio Alert	Plays an alert message to meeting participants that the meeting is recorded. The options are: • **Yes** • **No** You can configure **Audio Alert** only for the meeting recordings stored on USB storage devices. Avaya IX™ CU360 always plays the alert message when meeting recordings are stored on the enterprise network.
Ignore Mute on Playback	Plays audio on the endpoints of remote participants while playing back meeting recordings even when the remote participants mute their audio. The options are: • **Yes** • **No**
Video Upload/Delete	Uploads videos to USB storage devices from local computers.
Date & Time	Inserts a time stamp in meeting recordings. The options are: • **Yes** • **No** The format of the date and time depend on the configuration of the date and time in Avaya IX™ CU360.

Table continues…

Name	Description
Digital Signature	Inserts a digital signature to verify the authenticity of meeting recordings. You can upload your digitally signed certificate to authenticate meeting recordings. If you do not upload your certificate, Avaya IX™ CU360 inserts a self-signed certificate to authenticate meeting recordings. When you reset Avaya IX™ CU360 to factory settings, your uploaded certificate is deleted.
Save to External Server	Saves meeting recordings on external FTP servers. The options are: • **Yes** • **No**
External Server Type	The type of the external server where meeting recordings are saved. The options are: • **AESR**: Select if your Avaya Equinox® Conferencing deployment is managed by Avaya Equinox® Management with Avaya Equinox® Streaming and Recording Server configured to accept file transfers. • **Generic**: Select if you want to store meeting recordings in standard FTP servers. The Passive Transfer Mode feature on the FTP server must be enabled.
FTP Server URL	The URL of the FTP server, which contains: • The name or IP address. • The port number, if the port is different from the default port 21. • The path to subdirectories where meeting recordings are stored. For example, `[ftp://]servername_or_serveraddress[:port][/remotedir/.../]`
FTP Server User	The user name to log in to the external FTP server where meeting recordings are stored.
FTP Server Password	The password to log in to the external FTP server where meeting recordings are stored.

Table continues…

Name	Description
FTP Secure Connection	Encrypts the transfer of meeting recordings to the external FTP server using FTPS. The options are: • **Yes** • **No**
AESR File Owner	The name of the owner of meeting recordings in Avaya Equinox® Streaming and Recording Server. Usually, the owner of recordings in Avaya Equinox® Streaming and Recording Server is an Avaya Equinox® Management user, so the name of the owner corresponds to a user defined in Avaya Equinox® Management
AESR Server Tenant ID	The identification number of the enterprise of the meeting recordings owner defined in **AESR File Owner**. The identification number of the user is defined in Avaya Equinox® Management. If your deployment is not configured in multi-tenant mode, enter 999.

Configuring the Avaya IX™ CU360 screen saver

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure** > **General**.
   - On the web interface, click **Basic Settings** > **Preferences** > **General**.
2. Configure one of the following time delay periods for **Screen Saver**:
   - Never
   - 2 minutes
   - 5 minutes
   - 10 minutes
   - 30 minutes

Configuring Avaya IX™ CU360 to verify before disconnecting calls

About this task

Configure Avaya IX™ CU360 to ask for confirmation before disconnecting calls to prevent accidently disconnecting calls.

Procedure

1. Do one of the following:
   - From the endpoint, click **Configure** > **Calling**.
   - From the web interface, click **Basic Settings** > **Call-Answer mode** > **General**.
2. Configure **Confirm Disconnect** to **Yes**.
3. On the web interface, click **Save**.

Configuring LAN connectivity for Avaya IX™ CU360

About this task

Manually configure LAN or modify the LAN connection configured during the initial setup.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. Click **Networks** > **GLAN**.
3. Configure the following fields:

Endpoint menu	Web interface
IP Address Mode	**Automatic IP Address**
IP Address	**IP Address**
Subnet Mask	**Subnet Mask**
Gateway	**Gateway IP Address**
DNS	**DNS Server IP Address**

4. On the web interface, click **Save**.

Configuring an H.323 gatekeeper for Avaya IX™ CU360

About this task

Manually configure an H.323 gatekeeper or modify the H.323 gatekeeper connection configured during the initial setup.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. Do one of the following:
   - On the endpoint, click **Networks**.
   - On the web interface, click **Protocols**.
3. Click **H.323**.
4. Configure the following fields:

Endpoint menu	Web interface
E.164	**H.323 Name**
Use Gatekeeper	**E.164**
Mode	**Refuse Calls by IP Address**
Gatekeeper Address	**Use Gatekeeper**
—	**Gatekeeper Address Mode**
—	**Gatekeeper Address**
—	**Use H.460**
—	**Re-Registration Interval Time**
—	**Authentication**
—	**Mode**
—	**Gatekeeper ID**
—	**User Name**
—	**Password**

5. On the web interface, click **Save**.

Configuring WiFi network connectivity in Avaya IX™ CU360

About this task

To connect Avaya IX™ CU360 to the WiFi network, you must select the WiFi network and enter the credentials and authentication type.

Important:

Do not connect both Ethernet and WiFi networks simultaneously in Avaya IX™ CU360.

Before you begin

Ensure that the Ethernet cable is not connected to Avaya IX™ CU360.

Procedure

1. Click **Configure** > **Networks**.
2. Click **Wi-Fi**.

   Avaya IX™ CU360 displays the Wi-Fi window.
3. Enable WiFi.
4. Select and configure your WiFi network.

   If you do not need to install security certificates for your WiFi network, set **CA Certificate** to *Do Not Validate*.

Configuring Bluetooth connectivity in Avaya IX™ CU360

Before you begin

Enable the Avaya IX™ CU360 advanced settings.

Procedure

1. Select **Configure**.

   Avaya IX™ CU360 displays the Configure window.
2. Select **Advanced**.

   The default PIN is 1234.

   If your administrator configured a PIN to gain access to the advanced settings, Avaya IX™ CU360 prompts you to the enter PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **System**.

   Avaya IX™ CU360 displays the System window.
4. Select **Security**.

   Avaya IX™ CU360 displays the Security window.
5. Select **Settings**.

   Avaya IX™ CU360 displays the Settings window.
6. Click **Bluetooth**.

Avaya IX™ CU360 displays the window to enable Bluetooth.

7. Enable Bluetooth.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Installing third-party applications in Avaya IX™ CU360

About this task

Avaya does not support or test third-party applications. Avaya IX™ CU360 does not contain Google Play or Google Mobile Services. Some third-party applications might not work properly without these services.

Before you begin

Authorize applications from unknown sources in Android Settings > Security in Avaya IX™ CU360.

Procedure

1. Click **Apps & Tools**.

   Avaya IX™ CU360 displays a list of suggested applications.

2. Do one of the following:

   - Click the application and follow the instructions to install the application.
   - Click **Search** to find application.

3. If you search for an application, click the application to install it.

Related links

Third-party applications in Avaya IX CU360 on page 19

Configuration of Microsoft Exchange calendar

Configuring a Microsoft Exchange calendar in Avaya IX™ CU360

Before you begin

If you want to associate a room resource with Avaya IX™ CU360, create a delegate account in Microsoft Exchange calendar that can gain access to all calendar items where the room is added as a participant. You must have administrator-level privileges to create delegate accounts.

Procedure

1. Do one of the following:
   - From the endpoint, click **Configure** > **Advanced** > **Calendar**.
   - From the web interface, click **Administrator Settings** > **Calendar** > **General**.
2. Configure the following settings:
   - **Exchange Server Enabled**
   - **Exchange Server Address**
   - **Email**
   - **Password**
   - **Room email**
   - **Automatic Join to Important Meeting**
   - **FQDN List**
3. On the web interface, click **Save**.

Next steps

Map FQDNs of the meeting locations to the number of the virtual room resource.

Related links

Microsoft Exchange calendar integration on page 17

Calendar field descriptions

Name	Description
Exchange Server Enabled	The option to enable the connection with EWS to get the calendar. Avaya IX™ CU360 send a query to the EWS every minute to update the calendar. Avaya IX™ CU360 displays only the current and future meetings, and removes the expired meetings 15 minutes after the meetings expire.
Exchange Server Address	The Microsoft Exchange Server address in the `https://<server name>/EWS/Exchange.asmx` format. If your Microsoft Exchange Server is based on Microsoft Office 365, leave this field blank.

Table continues…

Name	Description
Email	The email address in the standard format. Depending on the calendar you configure, you can enter: • A personal email address. • A video endpoint email address. • A delegate email address.
Password	The password for the email account that you entered in **Email**.
Room email	The email address of the physical room resource to associate with Avaya IX™ CU360. This field is applicable only if you use the Room Resource and Delegate Account Mode and have an email account for the room associated with Avaya IX™ CU360. To use the Room Resource and Delegate Account Mode, you must configure a delegate account that can gain access to all calendar items where the room is added as a participant.
Automatic Join to Important Meeting	The option to enable Avaya IX™ CU360 to automatically join meetings marked with High Importance in Microsoft Outlook.

Mapping FQDNs with Microsoft Exchange calendar meetings

About this task

When you map FQDNs of the meeting locations to the number of the virtual room resource, meeting participants can join meetings directly from the Avaya IX™ CU360 GUI or web interface with a single click. Avaya IX™ CU360 automatically generates the meeting numbers to dial based on the FQDN mapping.

Each FQDN entry in the list represents a mapping rule between the FQDN of the meeting location and the number to dial to join the virtual room specified in the meeting location. By default, the FQDN list contains some FQDNs. You can also add more FQDNs in the list.

Procedure

1. Do one of the following:
   - From the endpoint, click **Configure** > **Advanced** > **Calendar**.
   - From the web interface, click **Administrator Settings** > **Calendar** > **General**.
2. Click **New FQDN**.
3. Configure the following settings:
   - **Meeting FQDN**
   - **Dialing FQDN**
   - **Prefix**
   - **Call Protocol**

4. On the web interface, click **Save**.

New FQDN field descriptions

Name	Description
Meeting FQDN	The FQDN in the meeting location. The meeting location is the virtual room associated with Avaya IX™ CU360. The meeting location is in the `https://<Meeting FQDN>/portal/tenants/default/?ID=<MeetingID>` format.
Dialing FQDN	The FQDN of the SIP or H.323 server deployed in your Avaya Equinox® Solution deployment • If the Avaya IX™ CU360 is registered to a SIP or H.323 server that can establish calls by adding a prefix to the virtual room number, leave this field blank. • If the Avaya IX™ CU360is located outside the enterprise network and not registered to a SIP or H.323 server, enter the domain address specified after the at (@) symbol in the meeting invitation.
Prefix	The prefix to the virtual room number of Avaya IX™ CU360registered to a SIP or H.323 server that can establish calls by adding a prefix.
Call Protocol	The call protocol that Avaya IX™ CU360 uses. The options are: • **SIP** • **H.323**

Avaya IX CU360 security

Configuring PIN protection for Avaya IX™ CU360 settings

About this task

Configure PIN for users to enter the PIN when users change the Avaya IX™ CU360 configuration, such as changing the interface language.

Before you begin

To configure PIN from:

- The endpoint, enable advanced configuration.
- The web interface, log in to the web interface using HTTPS.

Procedure

1. Do one of the following:
   - On the endpoint, click **Configure** > **Advanced** > **Utilities** > **PIN Protect Settings**.
   - On the web interface, click **Administrator Settings** > **Utilities** > **Pin Code**.
2. Do one of the following: From the drop-down options, select **Yes** to enable PIN protection for one or both of the following settings:
   - On the endpoint, configure the following fields:
     - **Advanced Settings**
     - **Basic Settings**
   - On the web interface, under **PIN Protect Settings**, configure the following fields:
     - **Administrator**
     - **Basic**

   Avaya IX™ CU360 displays a window to enter PIN.
3. Do the following to set PIN:
   a. Enter the current PIN. The default PIN is 1234.
   b. Enter the new PIN.
4. On the web interface, click **Save**.

Preventing calls to Avaya IX™ CU360 from invalid numbers

About this task

Prevent calls from invalid numbers to enhance security, especially if users can gain access to Avaya IX™ CU360 from public networks. Preventing such calls blocks hackers from attacking your SIP and H.323–based networks.

You can prevent calls from invalid numbers separately for each network interface. If Avaya IX™ CU360 is not registered to:

- A SIP server, incoming SIP-based calls using IP addresses are rejected. Calls must be established using:
  - The user@host syntax.
  - The host##user syntax where *host* is the Avaya IX™ CU360 IP address and *user* is the SIP user name.
- A gatekeeper, incoming H323–based calls using IP addresses are rejected. Calls must be established using:
  - The alias@host syntax.
  - The host##alias syntax where *host* is the Avaya IX™ CU360 IP address and *alias* is the H.323 alias.

Procedure

1. Do one of the following:
   - On the endpoint, click **Configure** > **Advanced**.

     If you configured a PIN to gain access to the advanced settings, Avaya IX™ CU360 prompts you to enter PIN.
   - On the web interface, click **Administrator Settings**.

   On the endpoint, Avaya IX™ CU360 displays the Advanced window.
2. Click **Protocols** > **General**.
3. Do one of the following:
   - On the endpoint, select **Yes** for **Reject SIP/H323 Invalid Number Calls**.
   - On the web interface, select **Yes** for the following fields:
     - **Reject SIP invalid number calls**
     - **Reject H.323 invalid number calls**

Restricting access to Avaya IX™ CU360 features

About this task

Restricting access to some Avaya IX™ CU360 features prevents users from using the Android-based features. Users cannot gain access to the Android-based applications and cannot installed new applications.

Users also cannot minimize the Avaya IX™ CU360 video conferencing application to gain access to the Avaya IX™ CU360 desktop and the Android settings.

Procedure

1. Do one of the following:
   - On the endpoint, click **Configure** > **Advanced** > **System** > **Security**.

     If you configured a PIN to gain access to the advanced settings, Avaya IX™ CU360 prompts you to enter PIN.
   - On the web interface, click **Administrator Settings** > **System** > **Security**.

   On the endpoint, Avaya IX™ CU360 displays the Advanced window.
2. On the endpoint, click **Restricted Access**.
3. Select **Yes** for **Enabled**.

Restricting installation of third-party applications to select users on Avaya IX™ CU360

About this task

Prevent users from installation third-party applications from unknown sources. Users will not be able to install applications from application stores, websites, or USB drives.

Procedure

1. Click **Configure**.
2. Click **Advanced**.

   If you configured a PIN to gain access to the advanced settings, Avaya IX™ CU360 prompts you to enter PIN. After you enter PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **System** > **Security** > **Settings**.

   Avaya IX™ CU360 displays the Settings window.
4. Select one of the following options for **App Installation Restrictions**.
   - **None**: Users will not face any restrictions.
   - **Pattern**: Users must enter a pattern to be allowed to install applications.
   - **PIN**: Users must enter a PIN to be allowed to install applications.
   - **Password**: Users must enter a password to be allowed to install applications.

Chapter 5: Advance administration

Configuring date and time in Avaya IX™ CU360

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **System** > **Date & Time** > **General**.
4. Configure the following fields:
   - **Day**
   - **Month**
   - **Year**
   - **Time Format**
   - **Hour**
   - **AM/PM**
   - **Minutes**
   - **Internet Time**
   - **Use Default NTP Servers**
   - **Server 1**
   - **Server 2**
   - **Refresh Time (min.)**

5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Date & Time General field descriptions

Name	Description
Internet Time	The option to synchronize the system clock with the network clock. If you configure **Internet Time** to **Yes**, you cannot modify the date and time fields.
Use Default NTP Servers	The option to synchronize the system clock with the NTP server clock. • If you select **Yes** to use an external SNTP server for synchronizing the system clock, Avaya IX™ CU360 uses SNTP servers returned by available DHCP. If DHCP is not available, Avaya IX™ CU360 uses a list of well-known public servers on the Internet. • If you select **No** to use one or two internal NTP servers for synchronizing the system clock, provide the IP addresses of **Server 1** and **Server 2**.
Server 1	The IP address of the internal NTP server.
Server 2	The IP address of the internal NTP server.
Refresh Time (min.)	The option refreshes the system clock after the set time period.

Manually configuring time zone in Avaya IX™ CU360

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.

3. Click **System** > **Date & Time** > **Time Zone**.
4. Configure the following fields:
   - **Enable Geolocation**
   - **Time Zone**
   - **Enable Daylight Time**
   - **Start (dd/mm)**
   - **Stop (dd/mm)**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Time Zone field descriptions

Name	Description
Enable Geolocation	The option to enable Avaya IX™ CU360 to automatically detect the correct time zone and to apply the appropriate daylight time value. The options are: • **Yes**: This is the default option. • **No**: Select **No** to manually specify the time zone using the **Time Zone** list. **Start (dd/mm)** and **Stop (dd/mm)** to apply daylight saving adjustment.
Time Zone	The time zone to which Avaya IX™ CU360 belongs.
Enable Daylight Time	The option to enable the daylight savings time.
Start (dd/mm)	The date when the daylight saving time starts.
Stop (dd/mm)	The date when the daylight saving time ends.

Configuring the advanced system names in Avaya IX™ CU360

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **System** > **Location**.
4. Configure the following settings:
   - **System Name**
   - **System Name Unicode**: This option is available only on the web interface.
   - **System Name Display Mode**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

System name field descriptions

Name	Description
System Name	The name of the Avaya IX™ CU360 endpoint. This field displays the initial name you entered during the quick setup wizard.
System Name Unicode	The name of the Avaya IX™ CU360 endpoint with non-alphanumeric characters. For example, Chinese or Japanese letters.

Table continues…

Name	Description
System Name Display Mode	The title bar of the Avaya IX™ CU360 endpoint displays the system name based on the mode that you select. The options are: • **Automatic**: Automatically displays the name based on deployment. • **System Name Unicode**: Displays the name in **System Name Unicode**. • **SIP**: Displays the SIP username. • **H.323**: Displays the H.323 name. • **System Name**: Displays the name that you entered in **System Name**.

Configuring advanced regional audio and video settings in Avaya IX™ CU360

About this task

After you set the country and language of Avaya IX™ CU360 in the quick setup wizard, Avaya IX™ CU360 defaults to the audio and video standards of that country.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **System** > **Location**.
4. Configure the following fields:
   - **Country**
   - **Language**
   - **Audio Coding**
   - **Video Frequency**

- **International Call Prefix (IDD)**

5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Location field descriptions

Name	Description
Country	The country where Avaya IX™ CU360 is located. The value of **Language** and the language of the menu automatically changes based on the language of the selected country.
Language	The language of the menu. You can select different languages for the web interface and the endpoint interface.
Audio Coding	Specifies the audio format. Configure the **European** or **US** audio coding that the audio equipment in your location use.
Video Frequency	The video refresh frequency depends on the country. If you configure the video frequency to **<auto>**, Avaya IX™ CU360 assigns the standard of the chosen country. In countries where the video frequency can vary, you must manually choose the value for your location.
International Call Prefix (IDD)	The numeric code to replace the plus sign (+) prefix for outgoing calls. If you want to disable this option, you must clear the field.

Configuring external user directories in Avaya IX™ CU360

About this task

You can configure the LDAP directory of Avaya IX™ CU360 to store users SIP-based and H323-based call information that integrates with directory and identity management systems.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.

- On the web interface, click **Administrator Settings**.

2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.

3. Do one of the following:

   - On the web interface, click **System** > **LDAP** > **Add Server**.
   - On the endpoint menu, click **System** > **LDAP** > **Add**.

4. Configure the following settings:

   - **Type**
   - **Preferred**
   - **Address**
   - **Port**
   - **User**: This option is available only on the **Equinox Management**, **Cloud**, and **Remote H.350 (generic)** servers.
   - **Password**
   - **Base**: This option is available only on the **Remote H.350 (generic)** server.
   - **RootDN**: This option is available only on the **Equinox Management**, **Cloud**, and **Remote H.350 (generic)** servers.
   - **Filter**: This option is available only on the **Remote H.350 (generic)** server.

5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

LDAP field descriptions

Name	Description
Type	Displays the types of LDAP servers that you can use to view the contacts and call these contacts from Avaya IX™ CU360 endpoint. The options are: • **Avaya XTSeries**: Refers to the built-in LDAP server of a different **Avaya XTSeries**. • **Avaya cu360**: Refers to the built-in LDAP server of Avaya IX™ CU360. • **Equinox Management**: Refers to the built-in LDAP server of **Equinox Management**. • **Cloud**: Refers to the built-in LDAP server in a cloud. • **Remote H.350 (third party)**: Refers to a third-party LDAP server to support the directories of other video communication vendors. For example, Polycom CMA. • **Remote H.350 (generic)**: Refers to a generic H.350-compliant LDAP server.
Preferred	The option to view the LDAP contacts in the **Contacts** page.
Address	The address of the LDAP server. If you select the LDAP server type as **Cloud**, Avaya IX™ CU360 configures this field automatically.
Port	The port that Avaya IX™ CU360 uses to connect to the LDAP server. The default port is 389. If you select the LDAP server type as **Cloud**, Avaya IX™ CU360 configures this field automatically.
User	The username of the LDAP server. The format of the username is in the form of a Distinguished Name.
Password	The password of the LDAP server.
Base	The root node of the LDAP tree under which all the contacts are defined. For example, ou=people.
RootDN	If the LDAP server has a **RootDN** defined, you must specify the **RootDN** field when accessing that LDAP server. For example, dc=company and dc=com.
Filter	Applies to the LDAP tree to view only the relevant contacts.

Preventing users from modifying the local directory in Avaya IX™ CU360

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **System** > **LDAP** > **Favorites** > **Lock**.
4. Click one of the following:
   - **Yes**: Prevent users from modifying the local directory.
   - **No**: Allow users to modify the local directory.
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Automatically displaying contacts from external user directories in Avaya IX™ CU360

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Before you begin

Configure external user directories in Avaya IX™ CU360.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.

2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.

3. Click **System** > **Customization** > **Search Contacts in Directory**.
4. Click one of the following:
   - **Manual**: To configure manual search. This is the default option.
   - **Automatic**: To configure automatic search.
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37
Configuring external user directories in Avaya IX CU360 on page 61

Hiding the recent calls list in Avaya IX™ CU360

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.

3. Click **System** > **Customization**.
4. Select **Yes** for **Hide Recent Calls**.
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Hiding the call rate selection list in Avaya IX™ CU360

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **System** > **Customization**.
4. Select **Yes** for **Hide Call Rate In Advanced Calling**.
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Disabling the Avaya IX™ CU360 startup tone

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **System** > **Customization**.

4. Select **No** for **Play Startup Sound**.
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Configuring wrap-around navigation in Avaya IX™ CU360

About this task

You can configure the Avaya IX™ CU360 to enable the user to cycle among available menu items in the user interface panels using the arrows.

You can apply wrap-around navigation only to the home screen panel, camera control panel, and call control panel.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **System** > **Customization** > **Wrap Around Menu**.
4. Click one of the following:
   - **Yes**: To enable wrap-around navigation. This is the default option.
   - **No**: To disable wrap-around navigation.
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Customizing the Avaya IX™ CU360 home screen

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **System** > **Customization** > **Home Screen Background**.
4. Click one of the following:
   - **Image**: To show the presentation. This is the default option.
   - **Video**: To show the video.
   - **Calendar**: To show the calendar panel.
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Configuring Avaya IX™ CU360 to remember your favorite layouts

About this task

You can configure Avaya IX™ CU360 to change the default display to your preferred display according to the number of video flows and your multi-image preferences. The available video flows are local video, remote video, local or remote presentation.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.

- On the web interface, click **Administrator Settings**.

2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.

3. Click **System** > **Customization** > **Remember Favorite Layouts**.
4. Click one of the following:
   - **Never**: Avaya IX™ CU360 always reverts to the default layout. This is the default option.
   - **During the call**: Avaya IX™ CU360 uses the last layout used in the same call for the combination of video flows. When you receive a presentation in the same call next time, Avaya IX™ CU360 automatically displays the last layout that you chose.
   - **Yes always**: Avaya IX™ CU360 uses the last layout used in the same call for the combination of video flows. When you receive a presentation in the same call or a different call next time, Avaya IX™ CU360 automatically displays the last layout that you chose.

     Do not use this option for Avaya IX™ CU360 that is shared by multiple users.
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Hiding calendar panel in Avaya IX™ CU360

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **System** > **Customization**.

4. Select **Yes** for **Hide Calendar Panel**.
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Configuring the maximum call bandwidth and preferred codec in Avaya IX™ CU360

About this task

You can specify the maximum bandwidth that Avaya IX™ CU360 can use in meetings. The bandwidth is measured in bit rate.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Calls** > **Preferences** > **General**.
4. Configure the following fields:

IP	ISDN
Rate (K)	**Rate (K)**
Audio Coding	—
Video Coding	—
Dual Video Coding	—
Use Manual Dual Video Bandwidth	—
Dual Video/Live Bandwidth	—

5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Preferences General field descriptions

IP section

Name	Description
Rate (K)	The maximum bitrate used for a single point-to-point call.
Audio Coding	The preferred audio codec that Avaya IX™ CU360 tries to send.
Video Coding	The preferred video codec that Avaya IX™ CU360 tries to send.
Dual Video Coding	The preferred video codec that Avaya IX™ CU360 tries to send as presentation content.
Use Manual Dual Video Bandwidth	The option allows to change the bandwidth for presentation content and live video.
Dual Video/Live Bandwidth	The bandwidth of live video or presentation content video.

ISDN section

Name	Description
Rate (K)	The maximum call rate that Avaya IX™ CU360 uses for ISDN call.

Setting a time limit for Avaya IX™ CU360 video conferences

About this task

Set a time limit for video conferences to alert users that the time allocated for the meeting is about to end and also to end video conferences that participants did not end.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Calls** > **Preferences** > **General**.
4. Select the **Call Time Limit** from the drop-down list.

   The default time limit is **Unlimited**. The maximum limit you can configure is **24 hours**.

5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Configuring touch-tone setting in Avaya IX™ CU360

About this task

You can use the touch-tone feature to display menus and change layouts.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Calls** > **Preferences** > **IP**.
4. Configure the following fields:
   - **SIP DTMF**
   - **H.323 DTMF RFC2833**
   - **H.323 DTMF H.245 UII**
   - **Use H.323 Generic Vendor Code**
   - **Dialing Number Format Mode**
   - **Separator**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

IP field descriptions

Name	Description
SIP DTMF	The option to send DTMF audio tones in the RTP stream for SIP calls. This is the default option.
H.323 DTMF RFC2833	The option to send DTMF audio tones in the RTP stream for H.323–based calls.
H.323 DTMF H.245 UII	The option to enable or disable the out-of-band DTMF transmissions in H.323–based calls.
Use H.323 Generic Vendor Code	The option to enable the H.323 application uses a generic vendor code identity instead of its default vendor code. So, the remote H.323 devices do not recognize it as an Avaya endpoint.
Dialing Number Format Mode	The dial number format of the H.323 or SIP gatekeeper. You can use any of the following valid formats: • `<gatekeeper number><separator><extension of the called endpoint>` • `<extension><separator><number>`
Separator	The option is used when dialing to the gatekeeper. The default separator is the pound sign (##).

Configuring the Avaya IX™ CU360 calls encryption

About this task

You can encrypt SIP-based and H.323-based calls on Avaya IX™ CU360 for greater security. Avaya IX™ CU360 can secure video conference sessions through encrypted connections in point-to-point calls and video conferences.

- For SIP connections, you can encrypt the media of SIP connections using SRTP.
- For H.323 connections, you can enable the encryption using H.235.

Important:

Using encryption is subject to local regulations. In some countries it is restricted or limited for usage. For more information, consult your local reseller.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

The default PIN for Advanced settings on the endpoint is 1234.

If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.

3. Click **Calls** > **Encryption**.
4. Select **Yes** for **Enable Encryption**.
5. Configure the following fields for securing calls:
   - **Accept Protected Calls**
   - **Unprotected Calls**
   - **Length of AES key**
   - **Minimum Key Size for DH**
   - **SIP Proprietary Encryption**
   - **Audio Alert**
6. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Enabling the RTP firewall in Avaya IX™ CU360

About this task

Configure Avaya IX™ CU360 to check the source of the received audio, video, and presentation (RTP packets) to verify that the source matches the remote endpoint's IP address.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Calls** > **Preferences** > **IP**.

4. Select **Yes** to enable **RTP Firewall**.
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Encryption field descriptions

Name	Description
Accept Protected Calls	The option to enable or disable encryption when receiving an encrypted call.
Unprotected Calls	The option to specify the policy for unprotected calls. Select the policy to apply when a remote endpoint does not support protected calls: • **Disconnect**: Automatically disconnects the call. • **Ask Conformation**: Asks permission to accept the unprotected call. • **Inform**: Displays a warning message on the endpoint and web interface. • **Show status**: Displays a notification message on the endpoint and web interface.
Length of AES key	The length of the AES key. The options are: • 128, 256 bits • 128 bits • 256 bits
Minimum Key Size for DH	The minimum key size for the Diffie-Hellman encryption. The options are: • **Very High Security (2048)**: Accepts 2048 bits and larger key sizes. • **High Security (1024)**: Accepts 1024 bits and larger key sizes.
SIP Proprietary Encryption	The option to use the encryption for SIP calls. The options are: • **Yes** • **No**
Audio Alert	An audio jingle for the encryption status of the call or the meeting.

Configuring calling number in Avaya IX™ CU360

About this task

Configure a number to call automatically by pressing 

. You can also specify the call protocol.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Calls** > **Predefined Party**.
4. Configure the following fields:
   - **Enabled**
   - **Number**
   - **Call Protocol**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Predefined Party field descriptions

Name	Description
Enabled	The option to enable or disable the predefined party feature in Avaya IX™ CU360.
Number	The number that Avaya IX™ CU360 calls.

Table continues…

Name	Description
Call Protocol	The protocol to use in calls. The options are: • **H.323**: The protocol for calls to H.323–based endpoints. • **SIP**: The protocol for calls to SIP-based endpoints. • **ISDN**: The protocol for calls to ISDN-based endpoints.

Configuring the Avaya IX™ CU360 gallery layout

About this task

Configure Avaya IX™ CU360 to use the gallery layout when meeting participants to present content in video conferences. Avaya IX™ CU360 uses the gallery layout only in video conferences that support the gallery layout.

Using this feature, Avaya IX™ CU360 endpoints can receive and change the gallery layout.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Do one of the following:
   - On the web interface, click **Presentation** > **General** > **Gallery Layout**.
   - On the endpoint main menu, click **Presentation** > **Gallery Layout**.
4. Click one of the following:
   - **Automatic**: Avaya IX™ CU360 automatically provides the gallery layout. This is the default option.
   - **Always**: Avaya IX™ CU360 always displays the gallery layout.
   - **Never**: Avaya IX™ CU360 never displays the gallery layout.
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Configuring the Avaya IX™ CU360 camera

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **I/O Connections** > **Cameras** > **General**.
4. Configure the following fields:
   - **Default Camera**
   - **Camera Control by Far Site**
   - **Bring Back to Place**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37
Avaya IX CU360 camera and LED indicators on page 15

Cameras General field descriptions

Name	Description
Default Camera	Avaya IX™ CU360 connects the default camera through **HD 1** or **USB** port. To configure the **Default Camera**, the options are: • **HD 1**: The built-in camera. • **USB**: Select if you connect the Avaya video grabber to the USB port.
Camera Control by Far Site	The option to control the Avaya IX™ CU360 camera from remote endpoint.
Bring Back to Place	Avaya IX™ CU360 stores the camera positions when the camera is turned off and restores this position when the camera is turned on.

Configuring the Avaya IX™ CU360 HD1 port

About this task

Configure the settings of each camera that you connect to the HD1 port of Avaya IX™ CU360.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **I/O Connections** > **Cameras** > **HD1**.
4. Select **Yes** for **Enable** the camera.

   You cannot disable **Default Camera**.
5. Configure the following fields:
   - **Control Camera**
   - **Tracking**
   - **White Balance Mode**

- **Exposure Compensation**

6. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

HD1 port field descriptions

Name	Description
Control Camera	The option to control the digital pan, tilt, and zoom functions of the camera.
Tracking	The option to focus on the active speaker in the room.
White Balance Mode	The option to adjust the white balance of the camera to control color tint in the room. The options are: • **Automatic**: Automatically determine any color tint and adjust colors to compensate. • **Indoor**: Sets the color compensation for artificial light. • **Outdoor**: Set the color compensation for natural sunlight. • **Fluorescent Light**: Reflects more green color wash than the conventional colors.
Exposure Compensation for end points	The option to enable the camera to compensate the exposure level manually, when the camera image is too bright or dark.
Exposure Level for web interface	The option to enable the camera to compensate the exposure level manually, when the camera image is too bright or dark.

Configuring the Avaya IX™ CU360 USB port

About this task

Configure the settings of each camera that you connect to the USB port of Avaya IX™ CU360.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.

2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.

3. Click **I/O Connections** > **Cameras** > **USB**.
4. Select **Yes** for **Enable** the camera.
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Configuring the monitor settings in Avaya IX™ CU360

About this task

After you connect the monitor to the HDMI port on Avaya IX™ CU360, you can configure it.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **I/O Connections** > **Monitors** > **General**.
4. Configure the following fields:
   - **Number of Monitors**
   - **Resolution HD1**
   - **CEC – Select as Source on Incoming Calls**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Monitors General field descriptions

Name	Description
Number of Monitors	The option to display available monitors that are connected to Avaya IX™ CU360. Activate the HDMI port on Avaya IX™ CU360 which connects to a monitor through the HD1 port. The options are: • **<auto>**: Avaya IX™ CU360 automatically detects the connected monitor. • **HD1**: Avaya IX™ CU360accepts input only from the monitor connected through the HD1 port.
Resolution HD1	The option to define the resolution of the connected monitor through the HD1 port.
CEC – Select as Source on Incoming Calls for endpoint only	The option to use a video source for the monitor which is different from the Avaya IX™ CU360 connected monitor. For an incoming call, if you select the option to **Yes**, the monitor is automatically switched to Avaya IX™ CU360 video source.

Configuring the Avaya IX™ CU360 video layouts

About this task

After you connect the monitor to the HDMI port on Avaya IX™ CU360, you can configure the video layouts.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **I/O Connections** > **Monitors** > **PIP-PaP-PoP**.

4. Configure the following fields:
   - **MultiImage Mode**
   - **MultiImage Type**
   - **PIP – Position**
   - **PIP – Rotation**
   - **PIP – Size**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

PIP-PaP-PoP field descriptions

Name	Description
MultiImage Mode	The option to enable or disable PIP, PaP, or PoP video layouts, depending on the number of video streams available on the monitor. The options are: • **<auto>**: Enables PiP, PaP, or PoP automatically when the number of video streams is greater than the number of available monitors. The order of the video streams is set automatically with precedence to the presentation video streams. • **Off**: Always disables PIP, PaP, or PoP. • **On**: Always enables PiP, PaP or PoP with two video streams.
MultiImage Type	The option to configure the video layouts available to users. The options are: • **<auto>**: Automatically enables PIP, PaP and PoP layouts. • **PIP**: Enables only PiP. • **PaP**: Enables only PaP. • **PoP**: Enables only PoP. If you use a 4K UHD or 2160p (3840x2160) monitor, by default **MultiImage Type** is set to PaP .
PIP – Position	The option to configure the position of the small overlapped image on the monitor.
PIP – Rotation	The option to enable or disable image rotation and controls the direction of the image rotation.
PIP – Size	The option to select the size of the small overlapped image on the monitor.

Configuring echo canceler on external microphones in Avaya IX™ CU360

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **I/O Connections** > **Audio** > **Echo Canceler**.
4. Configure the following fields:
   - **AGC**
   - **Noise Reduction**
   - **Audio Delay Automatic Estimation**
   - **Delay**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Echo Canceler field descriptions

Name	Description
AGC	Automatic Gain Control adjusts audio signals to equalize the average volume. This setting effectively lowers the volume if the audio signal is strong and raises the volume when the audio signal is weak.
Noise Reduction	Reduces the background noise of the conference room.

Table continues…

Name	Description
Audio Delay Automatic Estimation	Improves the echo canceler performance and the audio delay automatically when you connect a new monitor to Avaya IX™ CU360. • **Yes**: Enables the echo cancellation performance automatically. • **No**: Disables the automatic echo cancellation performance and you can configure **Delay** manually for better performance.
Delay	Avaya IX™ CU360 estimates the audio delay introduced by the monitor. You can calculate the audio delay in milliseconds and use the value to calculate the audio delay and improve the echo cancellation performance.

Enabling the use of IPV6 addresses in Avaya IX™ CU360

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Networks** > **Preferences** > **General**.
4. Click **Use IPv6**.
5. Select **Yes** to enable the IPv6 support.
6. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Configuring LAN for advanced IP address settings in Avaya IX™ CU360

About this task

After you save the settings on Avaya IX™ CU360 web interface, you must log in to Avaya IX™ CU360 web interface again.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Networks** > **GLAN** > **Addresses**.
4. Configure the following fields:

Endpoint menu	Web interface
IP Address Mode	**Automatic IP Address**
IP Address	**IP Address**
Subnet Mask	**Subnet Mask**
Gateway	**Gateway IP Address**
DNS	**DNS Server IP Address**

5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Configuring network priority settings in Avaya IX™ CU360

About this task

Configure Avaya IX™ CU360 to prioritize a specific network connection when Avaya IX™ CU360 cannot determine the network port from the destination address in the call signal.

When Avaya IX™ CU360 cannot determine the route of a call by matching the destination address, Avaya IX™ CU360 uses the preferred network port.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Networks** > **Preferences** > **General** > **Priority**.
4. Click one of the following:
   - **GLAN**: To use the LAN as preferred network.
   - **Wi-Fi**: To use the WiFi as preferred network.
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Configuring bandwidth threshold for LAN in Avaya IX™ CU360

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Networks** > **GLAN** > **Bandwidth**.

4. Select **Yes** for **Enable** the bandwidth limit.
5. Configure the following fields:
   - **Max. Bandwidth Rx (KB)**: The incoming bandwidth limit.
   - **Max. Bandwidth Tx (KB)**: The outgoing bandwidth limit.
6. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Configuring bandwidth threshold for WiFi in Avaya IX™ CU360

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Networks** > **Wi-Fi** > **Bandwidth**.
4. Select **Yes** for **Enable** the bandwidth limit.
5. Configure the following fields:
   - **Max. Bandwidth Rx (KB)**: The incoming bandwidth limit.
   - **Max. Bandwidth Tx (KB)**: The outgoing bandwidth limit.
6. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Configuring advanced LAN connectivity in Avaya IX™ CU360

About this task

Configure advanced properties of the network connections in each network port which include the network speed and packet size.

Before you begin

Enable the Avaya IX™ CU360 advanced settings and Avaya IX™ CU360 network priority.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Networks** > **GLAN** > **Parameters**.
4. Configure the following fields:
   - **MTU**
   - **Speed\Duplex Mode**
   - **Speed**
   - **Duplex Mode**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37
Configuring network priority settings in Avaya IX CU360 on page 86

GLAN Parameters field descriptions

Name	Description
MTU	The maximum size of data packets sent around the network. The default MTU size is 1360. If you transmit data packet of a larger MTU size, the network drops or fragments the packet. To avoid packet loss or fragmentation, all network components must use the same MTU size. For IPv4 address, set the MTU size in the range of 576 through 1500. For IPv6 address, set the MTU size in the range of 1280 through 1500.
Speed\Duplex Mode	The option to select the speed of the network port that defines the data transmission speed in the network. The options are: • **Automatic**: Avaya IX™ CU360 selects the speed and duplex mode automatically. This is the default option. • **Auto - up to 100/Full**: Semi-automatic mode with a specified maximum speed and data transmission. • **Auto - up to 100/Half**: Semi-automatic mode with a specified maximum speed and data transmission. • **Auto - up to 10/Full**: Semi-automatic mode with a specified maximum speed and data transmission. • **Auto - up to 10/Half**: Semi-automatic mode with a specified maximum speed and data transmission. • **Manual**: Configure the speed and duplex mode manually for the network.
Speed	The speed of the network port. The options are: • **10 Mbps** • **100 Mbps**
Duplex Mode	The data transmission mode that is defined for the network router or switch. The options are: • **Half**: The half duplex mode provides communication in both directions, but only in one direction at a time. • **Full**: The full duplex mode provides communication in both directions simultaneously.

Configuring advanced WiFi network connectivity in Avaya IX™ CU360

Before you begin

Enable the Avaya IX™ CU360 advanced settings and Avaya IX™ CU360 network priority.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Networks** > **Wi-Fi** > **Parameters**.
4. Configure **MTU**.
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37
Configuring network priority settings in Avaya IX CU360 on page 86

Wi-Fi Parameters field descriptions

Name	Description
MTU	The maximum size of data packets sent around the network. The default MTU size is 1360. If you transmit data packet of a larger MTU size, the network drops or fragments the packet. To avoid packet loss or fragmentation, all network components must use the same MTU size. For IPv4 address, set the MTU size in the range of 576 through 1500. For IPv6 address, set the MTU size in the range of 1280 through 1500.

Configuring the Avaya IX™ CU360 port ranges

About this task

You can configure the base port to any value between 1024 and 65535.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Networks** > **Preferences** > **Dynamic Ports**.
4. Configure the following fields:

TCP	UDP	BFCP UDP
Automatic	**Automatic**	**Automatic**
Ports	**Ports**	**Ports**

   If you select **No** in the **Automatic** field, you should manually configure the TCP, UDP, or BFCP UDP base ports in **Ports**.
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Configuring NAT and firewall in Avaya IX™ CU360

About this task

Configure a NAT router and firewall for Avaya IX™ CU360.

This configuration is available only if your administrator enables the advanced settings for users.

Before you begin

Configure the Avaya IX™ CU360 port ranges.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Networks** > **Preferences** > **NAT**.
4. Configure the following fields:
   - **NAT Traversal**
   - **NAT Discovery**
   - **Public IP Address**:

     This option is available when you select **Manual**.
   - **Server**:

     This option is available when you select **STUN autodiscovery**.
   - **Port**:

     This option is available when you select **STUN autodiscovery**.
   - **Pinhole Refresh Time (sec.)**
   - **Pinhole Keepalive**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37
Configuring the Avaya IX CU360 port ranges on page 92

NAT field descriptions

Name	Description
NAT Traversal	The option to enable a NAT router and firewall for Avaya IX™ CU360. Configure the Avaya IX™ CU360 port ranges. Select **No** if Avaya IX™ CU360 has a public IP address.

Table continues…

Name	Description
NAT Discovery	The options to discover the public IP address of Avaya IX™ CU360. The options are: • **Manual**: Enter the public IP address manually in **Public IP Address**. • **HTTP autodiscovery**: Uses a public HTTP server to get the Avaya IX™ CU360 public IP address. • **STUN autodiscovery**: Uses a public STUN server to get the Avaya IX™ CU360 public IP address. If you select this option, enter the server name and port number of the STUN server in the **Server** and **Port** fields respectively.
Pinhole Refresh Time (sec.)	The number of seconds to open a pinhole through the firewall.
Pinhole Keepalive	The connection is kept open by sending periodic pings to the remote control unit.

Defining the priority of media in Avaya IX™ CU360

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Networks** > **Preferences** > **QoS**.
4. Configure the following fields:
   - **Use QoS**
   - **Quality of Service**
   - **Precedence/TOS**
   - **DiffServ.**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

QoS field descriptions

Name	Description
Use QoS	The option to enable QoS. If you enable with QoS, Avaya IX™ CU360 provides the configured priority to different data streams and guarantees a certain level of performance to the data streams.
Quality of Service	The option to select network priorities. Network components such as routers or switches use the following two methods to implement QoS settings: • **Precedence/TOS**: • **DiffServ.**
Precedence/TOS	The option to define network components as a designated type of service (TOS) and an assign precedence ranking for each type of data.
DiffServ.	The option to define priority values for network components and different data types.

Registering Avaya IX™ CU360 with SIP servers

About this task

Register Avaya IX™ CU360 endpoints with SIP servers to maintain the mapping list of names or numbers and successfully establish call routes.

This configuration is available only if your administrator enables the advanced settings for users.

Before you begin

Verify the following information about your SIP environment:

- The DNS name or IP address of the SIP server. You can define up to three servers.
- The transport protocol and port used in your SIP environment.
- For the SIP infrastructure that requires a SIP user authentication, the credentials for authenticating Avaya IX™ CU360 with the SIP server.
- The model of the SIP server.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Protocols** > **SIP**.
4. Configure the following fields:
   - **User**
   - **Authentication Name**
   - **Authentication Password**
   - **Use Server 1**
   - **Server 1 DNS Name**
   - **Use Server 2**
   - **Server 2 DNS Name**
   - **Use Server 3**
   - **Server 3 DNS Name**
   - **Server Model**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

SIP field descriptions

Name	Description
User	The system name or number. You register Avaya IX™ CU360 with SIP servers using this name or number.
Authentication Name	The name for authenticating Avaya IX™ CU360 with SIP servers.

Table continues…

Name	Description
Authentication Password	The password for authenticating Avaya IX™ CU360 with SIP servers.
Use Server 1 **Use Server 2** (Optional) **Use Server 3** (Optional)	The SIP servers to which Avaya IX™ CU360 registers for calls. For redundant SIP deployments, you can enter information for maximum three SIP servers. • Avaya IX™ CU360 uses the Server 1 as the default SIP server. • If the Server 1 fails, Avaya IX™ CU360 uses the Server 2 and Server 3.
Server 1 DNS Name **Server 2 DNS Name** (Optional) **Server 3 DNS Name** (Optional)	The DNS name or IP address of each SIP server.
Server Model	The model of the SIP server for the best interaction.

Configuring TLS in Avaya IX™ CU360

About this task

With TLS, network devices can communicate securely by using certificates. TLS provides device authentication and communications encryption.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Protocols** > **SIP** > **Advanced**.
4. Configure the following fields:
   - **Transport Outbound Call**
   - **Use TLS**
   - **Verify Certificate**

- **Certificate Hostname Validation**
- **Verify Certificate Key Usage**
- **Verify Certificate Revocation**

5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Advanced SIP field descriptions

Name	Description
Transport Outbound Call	The option to configure the protocol to use for the outgoing calls. You can use **TLS** to secure the calls.
Use TLS	The option to configure Avaya IX™ CU360 to enable the TLS functionality.
Verify Certificate	The option to configure Avaya IX™ CU360 to use only TLS to connect to other devices. These devices must have security certificates that Avaya IX™ CU360 can verify.
Certificate Hostname Validation	The option to configure the host name validation level. • **Accept Validated Only**: Avaya IX™ CU360 only processes security certificates with validates host names. This is the default policy for certificate host name and key use validation. • **Accept Validated or same default certificate**: Avaya IX™ CU360 processes certificates that are validated or are the same as the certificates that Avaya IX™ CU360 uses. • **Accept All**: Avaya IX™ CU360 processes all security certificates and does not validate host names.
Verify Certificate Key Usage	The option to configure the certificate key use level. If you enable this option, Avaya IX™ CU360 processes only certificates that contain values for the key use parameters — Key Usage or Extended Key Usage.
Verify Certificate Revocation	The option to configure Avaya IX™ CU360 to verify security certificate revocation. • **Yes always**: Avaya IX™ CU360 checks all certificates for revocation. Avaya IX™ CU360 rejects certificates for which it cannot verify revocation. • **Yes if possible**: Avaya IX™ CU360 checks all certificates for revocation. Avaya IX™ CU360 rejects revoked certificates, but processes certificates for which it cannot verify revocation. • **No**: Avaya IX™ CU360 does not check certificates for revocation.

Configuring the presence status of Avaya IX™ CU360 users

About this task

Register Avaya IX™ CU360 to an XMPP server to publish its presence status and view the presence status of other contacts such as other Avaya IX™ CU360 and devices registered to the presence server.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Protocols** > **Presence**.
4. Configure the following fields:
   - **Use XMPP**
   - **User Name**
   - **Password**
   - **Domain**
   - **Port**
   - **IP Address**
   - **Server Type**
   - **Always Accept Subscriptions**
   - **Automatic Mutual Subscription**
   - **Automatic Favorites Subscription**
   - **Show Advanced Subscription Options**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Presence field descriptions

Name	Description
Use XMPP	The option to configure Avaya IX™ CU360 to use the XMPP presence server.
User Name	The user name of the presence account.
Password	The password of the presence account.
Domain	The domain name of the presence server. This is a mandatory field.
Port	The XMPP server port. The default port is 5222.
IP Address	The IP address of the presence server. IP address of the presence server is optional. You require the IP address only when DNS cannot resolve the domain name of the presence server.
Server Type	The type of server for the presence account. The options are: • **Avaya Aura** • **Generic**: The default server type • **Avaya One-X Portal for IP Office**
Always Accept Subscriptions	The option to configure Avaya IX™ CU360 to accept all subscription requests automatically. By default, this option is enabled state. If you disable this option, Avaya IX™ CU360 users can choose to accept or reject subscription requests. If you select **Avaya Aura** in **Server Type**, you do not need to configure this option. **Avaya Aura** always accepts subscription requests. This option is available when you select **Generic** and **Avaya One-X Portal for IP Office**.
Automatic Mutual Subscription	The option to ensure that if a user receives a subscription request, the access is reciprocated. Both users can see their status. By default, this option is in enabled state. This option is available when you select **Generic** and **Avaya One-X Portal for IP Office**.
Automatic Favorites Subscription	The option to configure Avaya IX™ CU360 to automatically subscribe users to other users added as favorite users. By default, this option is in enabled state.

Table continues…

Name	Description
Show Advanced Subscription Options	The option to configure Avaya IX™ CU360 to provide users with the following advanced subscription request settings: • Subscribe or unsubscribe users. • Grant or revoke operations for users. By default, this option is in enabled state.

Disabling SIP–based calls in Avaya IX™ CU360

About this task

Configure Avaya IX™ CU360 to disable SIP–based calls on GLAN, WiFi, or both network interfaces.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Protocols** > **General** > **Reject SIP calls**.
4. Select one of the following options in the **Reject SIP calls** field:
   - **No**
   - **GLAN & Wi-Fi**
   - **GLAN**
   - **Wi-Fi**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Disabling H.323–based calls in Avaya IX™ CU360

About this task

Configure Avaya IX™ CU360 to disable H.323-based calls on GLAN, WiFi, or both network interfaces.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Protocols** > **General** > **Reject H.323 calls**.
4. Select one of the following options in the **Reject H.323 calls** field:
   - **No**
   - **GLAN & Wi-Fi**
   - **GLAN**
   - **Wi-Fi**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Activating the Avaya IX™ CU360 licenses

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Before you begin

Get the Avaya IX™ CU360 license keys.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Utilities** > **Licenses**.
4. Do one of the following:
   - On the endpoint, enter the license keys in the **Serial Number** field.
   - On the web interface, enter the license keys in the License Codes field.
5. Do one of the following:
   - On the endpoint, click **Activate Licenses**.
   - On the web interface, click **Enable License**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Generating certificate signing requests for Avaya IX™ CU360

About this task

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.

3. Click **Utilities** > **Certificates** > **General**.
4. Configure the following fields:
   - **Certificates Key Length**
   - **Warning days before expiration**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Certificates General field descriptions

Name	Description
Certificates Key Length	The number of bits in a key. The options are: • **Very High Security (2048)**: Accepts 2048 bits. • **High Security (1024)**: Accepts 1024 bits.
Warning days before expiration	The option to configure Avaya IX™ CU360 to send alerts a specified number of days before security certificates expire. The minimum is 30 days. The default is 60 days.

Configuring web access for Avaya IX™ CU360

About this task

You can configure remote web access either from any IP address or restrict access from only a specific range of IP addresses.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.

3. Click **Utilities** > **Remote Access** > **Web**.
4. Configure the following fields:
   - **Web Management**
   - **Enable All Addresses**
   - **Address**
   - **Subnet Mask**
   - **User Name**
   - **Password**
   - **Disconnection due to inactivity**
   - **Enable Login Attempts**
   - **Login Denied Time**
   - **Disable TLS 1.0/1.1**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Web field descriptions

Name	Description
Web Management	The option to enable remote access to Avaya IX™ CU360 using the web interface.
Enable All Addresses	The option to allow remote access to Avaya IX™ CU360 using all IP addresses or restrict remote access to a specific range of IP addresses. The options are: • **Yes**: Enables remote access from any IP address. • **No**: Restricts remote access to a specific range of IP addresses. You can define the range of IP addresses in **Address** and **Subnet Mask**.
Address	The IP addresses of the devices that you allow to gain access Avaya IX™ CU360 remotely through the web interface. You can enter a value in this field only if you configure **Enable All Addresses** to **No**.

Table continues…

Name	Description
Subnet Mask	The range of addresses that you allow to gain access Avaya IX™ CU360 remotely through the web interface. You can enter a value in this field only if you configure **Enable All Addresses** to **No**.
User Name	The user name for the remote web access. The default user name is Admin.
Password	The password for the remote web access. The default password is 1234.
Disconnection due to inactivity	The duration after which the web interface disconnects inactive users. The options are: • **Never** • **5 minutes** • **10 minutes** • **15 minutes** • **30 minutes**
Enable Login Attempts	The option to block users after five consecutive incorrect login attempts within a ten-minute time span. Avaya IX™ CU360 blocks users for the duration specified in **Login Denied Time**. Avaya IX™ CU360 displays a message inviting the user to retry later.
Login Denied Time	The period during which Avaya IX™ CU360 blocks users from logging in to the web interface. The options are: • **30 minutes** • **1 hour** • **2 hours** • **4 hours**
Disable TLS 1.0/1.1	The option to enable or disable the TLS 1.0 and TLS 1.1 protocol.

Configuring the Avaya IX™ CU360 web-video

About this task

Use the web-video feature to define the video refresh rate and zoom. With this feature, you can take video snapshots and save the snapshots to your computer.

When you use web-video, Avaya IX™ CU360 displays an eye icon for  in the title bar, beside the time stamp.

You can monitor local and remote video from the Avaya IX™ CU360 web interface.

You cannot change **Web Video** settings using the web interface.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. On the endpoint main menu, click **Configure**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Utilities** > **Remote Access** > **Web Video**.
4. Configure the following fields:
   - **Web Video Management**
   - **Enable All Addresses**
   - **Address**
   - **Subnet Mask**
   - **Password Protect**
   - **Password**

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Web Video field descriptions

Name	Description
Web Video Management	The option to enable or disable web-video remote access to Avaya IX™ CU360 using TCP.

Table continues…

Name	Description
Enable All Addresses	The option to allow web-video remote access to Avaya IX™ CU360 from all IP addresses or restrict web-video access to Avaya IX™ CU360 using TCP through a specific range of IP addresses. The options are: • **Yes**: Enables web-video remote access from any IP address. • **No**: Restricts web-video remote access to Avaya IX™ CU360 using TCP through a specific range of IP addresses. You can define the range of IP addresses in **Address** and **Subnet Mask**.
Address	The IP addresses of the devices that you allow to gain access Avaya IX™ CU360 remotely through the web interface. You can enter a value in this field only if you configure **Enable All Addresses** to **No**.
Subnet Mask	The range of addresses that you allow to gain access Avaya IX™ CU360 remotely through the web interface. You can enter a value in this field only if you configure **Enable All Addresses** to **No**.
Password Protect	The option to configure Avaya IX™ CU360 to add password protection.
Password	The password for the web-video access.

Configuring remote updates for Avaya IX™ CU360

About this task

You can remotely upgrade Avaya IX™ CU360 with new firmware from a remote computer running the Avaya IX™ CU360 upgrade program.

The Avaya Certificate Root Authority signs Avaya IX™ CU360 software packages. Avaya IX™ CU360 accepts verified signed software packages.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.

3. Click **Utilities** > **Remote Access** > **Download**.
4. Configure the following fields:
   - **Download Management**
   - **Enable All Addresses**
   - **Address**
   - **Subnet Mask**
   - **Password Protect**
   - **Password**
   - **Verify Signature**
   - **OTA Update Enable**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Download field descriptions

Name	Description
Download Management	The option to enable or disable remote upgrade to Avaya IX™ CU360.
Enable All Addresses	The option to allow remote upgrade of Avaya IX™ CU360 using all IP addresses or restrict remote upgrade to a specific range of IP addresses. The options are: • **Yes**: Enables remote upgrade from any IP address. • **No**: Restricts remote upgrade to a specific range of IP addresses. You can define the range of IP addresses in **Address** and **Subnet Mask**.
Address	The IP addresses of the devices that you allow to make the upgrade. You can enter a value in this field only if you configure **Enable All Addresses** to **No**.
Subnet Mask	The range of addresses that you allow to make the upgrade. You can enter a value in this field only if you configure **Enable All Addresses** to **No**.
Password Protect	The option to configure Avaya IX™ CU360 to add password protection.
Password	The password for remote upgrade.
Verify Signature	The option to enable or disable the signature verification.

Table continues…

Name	Description
OTA Update Enable	The option to enable or disable remote access to the Over the Air upgrade information on the public internet, and to alert users that a new software version is available to upgrade Avaya IX™ CU360.

Controlling Avaya IX™ CU360 with AT commands

About this task

You can use AT commands to control the functions of Avaya IX™ CU360 on the endpoint and web interface.

Avaya IX™ CU360 can receive AT commands from:

- The device network connection to the controller's IP address through the 55003 port.
- The device USB connection to the controller's serial port through a standard RS232 cable.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Utilities** > **Remote Access** > **AT Commands**.
4. Click one of the following in the **AT Commands Management** field.
   - **No**: Disables the remote access to Avaya IX™ CU360 using AT commands through the TCP, SSH and RS232 serial port.
   - **IP only**: Restricts the remote access to Avaya IX™ CU360 using AT commands to only the TCP connection.
5. Configure the following fields:

IP	SSH	RS232 Serial Port
Enable All Addresses	**Enabled**	**Always Initialized**
Address	**User Name**	**Baud Rate**
Subnet Mask	**Password**	—

6. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

AT Commands field descriptions

AT Commands section

Name	Description
AT Commands Management	The option to enable or disable remote access to Avaya IX™ CU360 using AT commands through the TCP, SSH and RS232 serial ports. The options are: • **No**: Disables the remote access to Avaya IX™ CU360 using AT commands through the TCP, SSH and RS232 serial port. • **IP only**: Restricts the remote access to Avaya IX™ CU360 using AT commands to only the TCP connection.

IP section

Name	Description
Enable All Addresses	The option to allow remote access to Avaya IX™ CU360 using AT commands from all IP addresses or restrict the AT commands access to a specific range of IP addresses. The options are: • **Yes**: Enables the remote access to Avaya IX™ CU360 using AT commands from any IP address. • **No**: Restricts the remote access to Avaya IX™ CU360 using AT commands to a specific range of IP addresses. You can define the range of IP addresses in **Address** and **Subnet Mask**.
Address	The IP addresses of the devices that you allow to send AT command. You can enter a value in this field only if you configure **Enable All Addresses** to **No**.
Subnet Mask	The range of addresses that you allow to send AT command. You can enter a value in this field only if you configure **Enable All Addresses** to **No**.

SSH section

Name	Description
Enabled	The option to enable the AT commands API through SSH.

Table continues…

Name	Description
User Name	The user name for the SSH management. The default user name is Admin.
Password	The password for the SSH management. The default password is 1234.

RS232 Serial Port section

Name	Description
Always Initialized	The option to accept an AT initialization command before accepting other commands, when required by the API. Use this option when the controlling device cannot detect whether Avaya IX™ CU360 restarted.
Baud Rate	The baud rate of the devices that you allow to remotely gain access to Avaya IX™ CU360. The baud rate must be the same as the baud rate of the controlling device.

Configuring telnet in Avaya IX™ CU360

About this task

With telnet, you can control Avaya IX™ CU360 by using CLI commands.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Utilities** > **Remote Access** > **Telnet**.
4. Configure the following fields:
   - **Telnet Management**
   - **Enable All Addresses**

- **Address**
- **Subnet Mask**
- **Password**

5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Telnet field descriptions

Name	Description
Telnet Management	The option to enable or disable remote access to Avaya IX™ CU360 through the telnet.
Enable All Addresses	The option to allow remote access through telnet to Avaya IX™ CU360 using all IP addresses or restrict the remote access to a specific range of IP addresses. The options are: • **Yes**: Enables remote access through telnet from all IP addresses. • **No**: Restricts remote access through telnet to a specific range of IP addresses. You can define the range of IP addresses in **Address** and **Subnet Mask**.
Address	The IP addresses of the devices that you allow to gain access Avaya IX™ CU360 remotely through the telnet. You can enter a value in this field only if you configure **Enable All Addresses** to **No**.
Subnet Mask	The range of addresses that you allow to gain access Avaya IX™ CU360 remotely through the telnet. You can enter a value in this field only if you configure **Enable All Addresses** to **No**.
Password	The password for the telnet access.

Managing Avaya IX™ CU360 from Equinox Management

About this task

With Equinox Management, you can manage all the endpoints, including Avaya IX™ CU360 in a video network.

You must enable AT commands to work with Equinox Management. You can select the cloud mode to manage Avaya IX™ CU360.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Utilities** > **Remote Access** > **Equinox Management**.
4. Configure the following fields:
   - **Mode**
   - **Automatic IP Address**
   - **IP Address**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Equinox Management field descriptions

Name	Description
Mode	The option to configure Avaya IX™ CU360 to gain remote access using the local server or cloud server. • **Local**: To provision Avaya IX™ CU360 using local server. • **Cloud**: To auto-provision Avaya IX™ CU360 from Equinox Management.
URL	The URL of Equinox Management that you moves Avaya IX™ CU360 from local management to cloud management. This is a read-only field.
Automatic IP Address	The option to enable Avaya IX™ CU360 to display the Equinox Management IP address automatically. This option is available when you select **Local** in **Mode**.

Table continues…

Name	Description
IP Address	The IP address of the Equinox Management server. You can enter a value in this field only if you configure **Automatic IP Address** to **No**. This option is available when you select **Local** in **Mode**.

Configuring screen link and mobile link in Avaya IX™ CU360

About this task

You can configure the screen link and mobile link to share your desktop automatically.

When you connect your computer to Avaya IX™ CU360, by default Avaya IX™ CU360 requests you to enter a PIN. You can disable the PIN request.

You can also configure how the Avaya IX™ CU360 endpoint can remove a connected screen link client.

This configuration is available only if your administrator enables the advanced settings for users.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure**.
   - On the web interface, click **Administrator Settings**.
2. On the endpoint, click **Advanced**.

   The default PIN for Advanced settings on the endpoint is 1234.

   If your administrator configured a PIN to gain access to the advanced settings on the endpoint, Avaya IX™ CU360 prompts you to enter the PIN. After you enter the PIN, Avaya IX™ CU360 displays the Advanced window.
3. Click **Utilities** > **Remote Access** > **Screen Link/Mobile Link**.
4. Configure the following fields:
   - **Mode**
   - **Remote Presentation Mode**
   - **Screen Link Unpair Mode**
5. On the web interface, click **Save**.

Related links

Enabling the Avaya IX CU360 advanced settings on page 37

Screen Link/Mobile Link field descriptions

Name	Description
Mode	The option to enable or disable the screen link and mobile link. The options are: • **Enable - No PIN**: Enables the screen link and mobile link without a PIN. • **Enable - Ask PIN (manual pairing)**: Enables the screen link and mobile link, and requires a PIN to select Avaya IX™ CU360 other than the automatically-paired device. • **Enable - Ask PIN (always)**: Enables the screen link and mobile link and requires a PIN for automatic pairing and manual pairing. • **Disable**: Disables the screen link and mobile link.
Remote Presentation Mode	The option to enable remote access to view, send, and download presentations in meetings. The options are: • **Automatic**: Sends presentations automatically in meetings when you activate the screen link and mobile link. • **Manual**: Sends presentations in meetings when you click **Present**.
Screen Link Unpair Mode	The option to configure the mode of removing linked devices. The options are: • **Automatic**: Automatically removes devices linked during meeting when the meeting ends but only if the pairing was started during the meeting. • **Manual**: Removes linked devices only when you manually initiate the removal . • **When the meeting ends**: Removes linked devices when meeting ends.

Chapter 6: Maintenance

Exporting the Avaya IX™ CU360 contact details

Procedure

1. Do one of the following:
   - On the endpoint main menu, click
   - On the web interface, click **Make your Call**.
2. Click **Export Contacts**.

Result

Avaya IX™ CU360 generates an LDAP directory file in the LDAP Data Interchange Format.

Next steps

Save the LDAP directory file on your computer.

Importing the Avaya IX™ CU360 contact details

Procedure

1. Do one of the following:
   - On the endpoint main menu, click
   - On the web interface, click **Make your Call**.
2. Click **Choose File**
3. Click **Import Contacts**.

Result

Avaya IX™ CU360 imports the contacts to the endpoint.

Avaya IX™ CU360 software upgrades

Avaya provides upgrades to the Avaya IX™ CU360 software, OS, and the web interface through an auto-extracting software package.

Avaya IX™ CU360 software packages are signed by the Avaya Certificate Root Authority. You can update the Avaya IX™ CU360 software using only Avaya-verified software packages.

Before the software upgrades, Avaya IX™ CU360 verifies that the software package:

- Is verified by the Avaya Certificate Root Authority.
- Is not tampered.

You can upgrade Avaya IX™ CU360 using:

- The endpoint
- A computer
- A USB drive
- A web browser
- Avaya Equinox® Management

Enabling Avaya IX™ CU360 software upgrades using the endpoint

About this task

Avaya IX™ CU360 displays a green icon to notify that a software upgrade is available.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure** > **Advanced**.
   - On the web interface, click **Administrator Settings**.
2. Click **Utilities** > **Remote Access** > **Download**.
3. Configure **OTA Update Enabled** to **Yes**.

Upgrading Avaya IX™ CU360 using the endpoint

About this task

Avaya IX™ CU360 displays a green icon to notify that a software upgrade is available. Avaya IX™ CU360 displays the notification only if you enable the option to automatically upgrade the software from the endpoint.

Do not switch off Avaya IX™ CU360 till the software upgrade process is complete. If the upgrade process is interrupted, repeat the upgrade procedure. Do not restart Avaya IX™ CU360.

During the upgrade process, Avaya IX™ CU360 displays rotating LEDs on the endpoint.

Before you begin

Do the following:

- Download the software upgrade package from the Avaya PLDS at https://plds.avaya.com/.
- Back up the current Avaya IX™ CU360 configuration.

Procedure

1. Click **Configure**.
2. Click **System Status** > **Software Upgrade**.
3. Click **Install**.

Result

Avaya IX™ CU360 starts the software upgrade process.

Next steps

After the software upgrade process is complete, if Avaya IX™ CU360 cannot connect to the LAN or WiFi network, repeat the upgrade process using a USB drive.

Upgrading Avaya IX™ CU360 using a USB drive

About this task

The file name of the upgrade package is in the `CU-360_Vx_y_z.exe` format. Do not change the file name.

Do not switch off Avaya IX™ CU360 until the software upgrade process is complete.

Before you begin

- Save the Avaya IX™ CU360 software upgrade package in the USB drive.
- Ensure that Avaya IX™ CU360 is not active in a meeting.

Procedure

Plug in the USB drive in the USB port of Avaya IX™ CU360.

Result

Avaya IX™ CU360 automatically detects the USB drive and starts the software upgrade process. After the upgrade process is complete, the Avaya IX™ CU360 restarts the video conferencing application.

Upgrading Avaya IX™ CU360 using a computer

About this task

Use a computer connected to LAN to upgrade Avaya IX™ CU360. If you use a wireless network, the upgrade process might be very slow.

The file name of the upgrade package is in the `CU-360_Vx_y_z.exe` format. Do not change the file name.

Before you begin

- Save the Avaya IX™ CU360 software upgrade package in the computer.
- Ensure that the computer is connected to LAN.

Procedure

1. Run the Avaya IX™ CU360 software upgrade executable file.

   Avaya IX™ CU360 starts the software upgrade application.
2. Accept the terms and conditions of the software license.
3. Type the IP address of Avaya IX™ CU360, and click **Start**.

Result

Avaya IX™ CU360 starts the software upgrade process. After the upgrade process is complete, the Avaya IX™ CU360 restarts the video conferencing application.

If the Avaya IX™ CU360 video conferencing application does not restart, the software upgrade application might indicate that the upgrade process must be repeated.

Upgrading Avaya IX™ CU360 using the web interface

About this task

You can use a computer or a mobile device to upgrade Avaya IX™ CU360 using the web interface.

The file name of the upgrade package is in the `CU-360_Vx_y_z.exe` format. Do not change the file name.

Before you begin

Save the Avaya IX™ CU360 software upgrade package in the computer.

Procedure

1. Click **Administrator Settings**.
2. Click **Utilities** > **Software Update**.
3. Accept the terms and conditions of the software license, and click **Next**.
4. Click **Browse file**, and select the Avaya IX™ CU360 software upgrade package file.

   Avaya IX™ CU360 uploads the software upgrade package file to the endpoint.
5. Click **Upload-Install**.

Result

Avaya IX™ CU360 starts the software upgrade process. After the upgrade process is complete, the web interface restarts. You might need to log in again.

Chapter 7: Troubleshooting

Verifying the status of the Avaya IX™ CU360 network connections

About this task

You can view the following system information:

- Software version
- Host ID or MAC address
- IP addresses
- Serial number
- System name and model
- Licenses
- Network, gatekeeper, and SIP settings

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure** > **System Status**.
   - On the web interface, click **Home**.
2. **(Optional)** Click **More** for the status of the following connections:
   - Presence server
   - Cloud server
   - Calendar

Result

Avaya IX™ CU360 displays the status of the network connections.

Testing the Avaya IX™ CU360 network connections

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure** > **System Status** > **Diagnostics** > **Network** > **Tests**.
   - On the web interface, click **Diagnostics** > **Network**.
2. Do one of the following:
   - On the endpoint, enter an IP address, and click **Ping**.
   - On the web interface, click **Ping**.
3. On the web interface, enter the IP address, and click **Ping**.

Verifying acoustic pairing in Avaya IX™ CU360

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure** > **System Status** > **Diagnostics** > **I/O Connections** > **Audio** > **Streams**.
   - On the web interface, click **Diagnostics** > **I/O Connections** > **Audio** > **Streams**.
2. Select one of the following streams to view the status:
   - **Tx**: Transmitting audio stream
   - **Rx**: Receiving audio stream

Testing acoustic pairing in Avaya IX™ CU360

About this task

Test acoustic pairing between Avaya IX™ CU360 and other devices to check for interference from ambient noises.

Procedure

1. Do one of the following:
   - On the endpoint main menu, click **Configure** > **System Status** > **Diagnostics** > **I/O Connections** > **Audio** > **Tests**.
   - On the web interface, click **Diagnostics** > **I/O Connections** > **Audio** > **Tests**.

2. Click the Play button next to one of the following tests:
   - **Local Tone**: The audio input that Avaya IX™ CU360 receives.
   - **Tx Tone**: The audio output sent that Avaya IX™ CU360 sends.

Testing the monitor image of Avaya IX™ CU360

About this task

Test the monitor image of Avaya IX™ CU360 to check for the optimization of the aspect ratio and color rendering of the monitor display.

You can use the test image to finely tune monitor colors and aspect ratio using the remote control of the monitor provided by the vendor.

Procedure

1. Click **Configure** > **System Status** > **Diagnostics** > **I/O Connections** > **Monitor** > **Tests**.
2. Click the Play button to generate the test image.

Verifying the status of the equipment connected to Avaya IX™ CU360

About this task

Check the status of the external monitor and other equipment connected to Avaya IX™ CU360, such as Avaya AV Grabber and Avaya B109 Conference Phone.

Procedure

Do one of the following:

- On the endpoint main menu, click **Configure** > **System Status** > **Diagnostics** > **I/O Connections** > **Status**.
- On the web interface, click **Diagnostics** > **I/O Connections** > **Status**.

Result

Avaya IX™ CU360 displays the status of the connected equipment.

Chapter 8: Resources

Documentation

See the following related documents at http://support.avaya.com.

Title	Use this document to:	Audience
Avaya IX™ Collaboration Unit CU360 Quick Setup Guide	Understand the features of and use Avaya IX™ CU360	Customers
Avaya IX™ Collaboration Unit CU360 Quick Tips Guide	Understand the features of and use Avaya IX™ CU360	Customers
Using Avaya Collaboration Control for iOS	Understand the features of and use Avaya Scopia® Control	Customers
Using Avaya Collaboration Control for Android	Understand the features of and use Avaya Collaboration Control	Customers
User Guide for Avaya IX™ Room System XT Series	Understand the features of and use Avaya IX™ Room System XT Series	Customers

Finding documents on the Avaya Support website

Procedure

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

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

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

7. Click **Enter**.

Avaya Documentation Center navigation

Customer documentation for some programs is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available at Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for content using one of the following:
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release.
  - From **Products & Solutions**, select a solution and product, and select the appropriate document from the list.
- Sort documents on the search results page by last updated dated and relevance.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:
  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.
- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log on to the website. The available functionality depends on the role with which you are logged in.

Support

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

Using the Avaya InSite Knowledge Base

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

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

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

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

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

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

Index

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W