Administrator Guide for Avaya Equinox Management

Release 9.1
Issue 8
July 2020

© 2019-2020, Avaya Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

“Documentation” means information published in varying 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 type(s)

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.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time as indicated in the order, Documentation, or as authorized by Avaya in writing. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Named User License (NU). End User may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as

only authorized Named Users access and use the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Getting started with Avaya Equinox® Management 12
Avaya Equinox® Management overview 12
New in this release 14
Updates to this publication 15
Planning your Avaya Equinox® Management deployment 15
Implementing port security for Avaya Equinox® Management 16
Ports to open on Avaya Equinox® Management 16
Minimum requirements for Equinox Management 23
Planning user access to videoconferences 25
Localized languages in Equinox Management 27
Accessing Avaya Equinox® Management 28
Accessing the Administrator Portal to manage your video network 28
Initial configuration workflow 29
Initial workflow for Enterprise Deployments 30
Initial workflow for service provider deployments 31
Creating an initial workflow for organizations in service provider deployments 32
Chapter 2: Defining locations and organizations in your deployment 53
Adding or modifying a location 53
Defining bandwidth limits for a location 55
Chapter 3: Defining your video network devices 58
Device configuration workflow 58
Adding video network devices in Equinox Management 61
Modifying a network device's location or organization in Equinox Management 64
Planning and configuring gatekeepers in Equinox Management 65
About the Equinox Management's internal gatekeeper 65
Defining the gatekeeper's dial plan in Avaya Equinox® Management 67
Configuring a stand-alone H.323 Gatekeeper 70
Planning and configuring media servers in Equinox Management 71
Configuring the media server from Equinox Management 71
Downloading media server meeting yypes to Equinox Management 75
Increasing MCU capacity by cascading multiple MCUs 85
Enabling Auto-Attendant support 88
Integrating the Avaya Aura® Conferencing server 91
Planning and configuring gateways in Equinox Management 93
Configuring the WebRTC and Recording Gateways in Equinox Management 94
Configuring a Gateway in Equinox Management 96
Configuring a WebRTC or recording gateway in Equinox Management 100
Connecting a WebRTC client to a meeting through a TURN server 103
Configuring user portals in Equinox Management 104

Registering a gateway with a gatekeeper..... 105
Configuring a UCCS Server in Equinox Management..... 106
Planning and configuring Avaya Session Border Controller for Enterprise (ASBCE) in Equinox Management..... 108
Configuring Avaya Session Border Controller for Enterprise (ASBCE) in Equinox Management..... 109
Remotely configuring the Avaya Equinox® H.323 Edge server..... 111
Creating an Equinox H.323 Edge server cluster..... 117
Deleting an Equinox H.323 Edge server cluster..... 119
Planning and configuring endpoints in Equinox Management..... 120
Importing H.323 endpoints from the Gatekeeper..... 122
Importing H.323 endpoints from an external LDAP server..... 124
Importing Endpoints from the H.350 search base..... 126
Adding endpoints in Equinox Management manually..... 128
Planning and configuring Telepresence in Equinox Management..... 139
Managing endpoints using Equinox Management..... 141
Provisioning Avaya Room System XT Series endpoints automatically..... 145
Configuring Quality of Service and Encryption settings for an XT Series endpoint in Equinox Management..... 153
Replicating endpoint settings on multiple endpoints..... 155
Using Equinox Management's endpoint directory as a corporate address book..... 159
Managing your endpoint's user directory with LDAP..... 161
Configuring presentation layouts for single-screen endpoints..... 169
Organizing endpoints into groups with labels..... 171
Configuring Avaya Equinox® Media Server for WebRTC-based calls in Over The Top deployments..... 174
Configuring Avaya Equinox® Media Server for WebRTC-based calls in Team Engagement deployments..... 175
Planning and configuring streaming and recording servers in Equinox Management..... 176
Adding and Modifying Equinox Streaming and Recording Servers in Equinox Management 177
Chapter 4: Securing your video network..... 179
Securing web access to Equinox Management using HTTPS..... 179
Configuring the Tomcat web server to use HTTPS..... 180
Securing the connection between Equinox Management and an LDAP server..... 181
Securing your video network using TLS..... 181
Planning the required certificates for TLS..... 184
TLS connections to devices with identity certificates..... 191
Creating and uploading Equinox Management's certificate for videoconferencing components..... 192
Importing third-party root CA and intermediate CA certificates..... 196
TLS client support for extended hostname or domain validation..... 198
Certificate revocation validation..... 199
Removing trusted CA certificates..... 200
Exporting the root CA certificate of an internal or third-party CA..... 201

Configuring Equinox Management as a Certificate Authority.... 202
Securing TLS connections for Equinox Management.... 203
Securing TLS connections for a distributed AAWG/Portal.... 204
Troubleshooting TLS connections.... 205
Configuring account policies in Avaya Equinox® Management.... 206
Configuring meeting policies PIN security.... 209
Configuring Cross-Origin Resource Sharing (CORS).... 212
Configuring the Enhanced Access Security Gateway (EASG).... 213
Importing a CA certificate.... 213
Enabling hardening for the Avaya Equinox® management server.... 214
Enabling FIPS compliance for redundancy mode.... 215
Enabling composite video for virtual rooms.... 216
Chapter 5: Defining and Managing Video Users.... 218
Managing User Profiles.... 220
Creating or modifying a user profile.... 221
Exporting a list of users in Equinox Management.... 226
Enabling Streaming and Recording for a User Profile.... 228
Customizing a user profile.... 229
Deleting a User Profile.... 233
Modifying User Policies.... 234
Managing User Groups.... 235
Creating a User Group.... 236
Modifying a User Group.... 237
Removing a User Group.... 238
Managing Video Users.... 238
Managing Users from the LDAP Server.... 239
Managing users with a local user directory.... 245
Modifying a user.... 248
Limiting Users' Privileges.... 250
Assigning Groups to Multiple Users.... 250
Searching for a User.... 251
Defining Administrators in a Service Provider Deployment.... 252
Managing Virtual Rooms.... 253
Downloading Virtual Rooms from the LDAP Server.... 254
Creating or modifying a virtual room for an Equinox Management user.... 255
Creating Preferred Dial In Number Variables.... 259
Invitation Template Variables and Parameter Settings.... 260
Creating an invitation template.... 262
Configuring WebRTC calls for the Microsoft Edge browser.... 264
Chapter 6: Scheduling your videoconference from the Equinox Management User Portal.... 267
Enabling the Avaya Meeting Scheduler Outlook Add-in without the Avaya IX™ Workplace Client 275
Configuring Outlook on the web without the Avaya IX™ Workplace Client.... 276

Registering an Avaya Cloud account.... 277
Setting up a company domain in the Avaya Cloud account.... 278
Mapping your domain to the settings file URL.... 279
Configuring Equinox Streaming and Recording Server Meeting Properties in the User Portal.... 280
Configuring Advanced Meeting Properties in the User Portal.... 284
Chapter 7: Real-time Monitoring.... 291
Managing Alarm Notifications.... 292
Configuring the Log Level.... 292
Sending Trap Messages.... 294
Sending Email Alerts.... 295
Monitoring Network Devices via Equinox Management.... 297
About Management Status of Network Devices.... 298
Monitoring Network Events and Alarms.... 299
Changing the Severity Level of Alarms.... 300
Monitoring Meetings and Calls.... 301
Monitoring Ongoing Meetings or Calls.... 301
Monitoring Meeting Events.... 303
Monitoring Bandwidth and Port Utilization.... 306
Downgrading the Meeting Bandwidth.... 307
Checking the Status of Meetings.... 308
Inviting Endpoints to Join Meetings.... 309
Disconnecting Calls or Meetings.... 310
Adding a support email address to Avaya Equinox® Meetings for Web.... 310
Chapter 8: Moderating Videoconferences in Equinox Management.... 312
Accessing the In-meeting Control Interface.... 312
Customizing Participant Options.... 314
Enabling Lecture Mode.... 314
Selecting the VIP Status for a Participant.... 315
Modifying Participant Media Connections.... 316
Blocking a Participant's Camera.... 317
Blocking Incoming Video.... 317
Changing a Participant's Audio Level.... 318
Sharing a Presentation.... 319
Modifying Videoconference Views.... 320
Changing the Main Video Layout.... 320
Enabling Dynamic Layout.... 323
Positioning the Active Speaker in the Video Layout.... 324
Changing a Participant Meeting View.... 325
Changing a participant name.... 326
Activating Participant Auto-switching for Fixed Layouts.... 326
Enabling the Self-see Feature.... 328
Managing Videoconference Participants.... 329
Inviting a Participant to Join a Videoconference.... 329

Viewing Technical Details of Participant Connection in a Meeting..... 332
Re-inviting All Offline Participants..... 337
Blocking Conference Admission..... 338
Sending a Public Chat Message..... 338
Displaying Participant Names in Frames..... 339
Disconnecting a Participant..... 341
Extending a Videoconference Duration..... 341
Ending a Videoconference..... 342
Chapter 9: Working with Equinox ad hoc conferencing..... 343
Configuring Avaya IX™ Workplace Client settings..... 344
Configuring settings to enable Avaya 96xx phones for ad hoc conferencing..... 345
Configuring advanced parameters for ad hoc conferencing..... 345
Configuring the SIP Endpoint Managed Transfer Setting in Avaya Aura® Communication Manager..... 347
Configuring Avaya Aura® Communication Manager settings..... 348
Configuring Dial Plan settings..... 349
Configuring Equinox Management settings..... 350
Configuring System Manager settings..... 351
Escalating to a multipoint conference for a multiparty call using Avaya IX™ Workplace Client..... 354
Chapter 10: Configuring shuffling in Avaya Communication Manager..... 357
Chapter 11: Log server settings..... 359
Configuring the Log server settings..... 359
Configuring a secure connection using a different CA for the Log server..... 359
Configuring a SysLog Server with TLS (SSL)..... 360
Configuring a secure connection using the same CA for the Log server..... 361
Configuring a SysLog Server with TLS (SSL)..... 362
Configuring a non-secure connection for the Log server..... 363
Chapter 12: Tracking system usage with reports..... 364
About types of Equinox Management reports..... 364
Generating a report..... 369
Configuring Call Detail Records..... 376
Chapter 13: Maintaining your Videoconferencing Network..... 378
High Availability of Equinox Management..... 378
Creating a Redundant Secondary Server for Equinox Management..... 380
Creating an Off-Site Backup Server for Equinox Management..... 384
Monitoring Redundancy Status..... 386
Manually promoting the off-site backup server..... 389
Restoring primary server from off-site backup server..... 392
Disabling Redundancy..... 394
Upgrading, Backing up and Restoring Equinox Management 395
Enabling the administrator to configure a notification message..... 396
Software Update Tool..... 398
Backing up Equinox Management Manually..... 401

Backing up Equinox Management Automatically.... 402
Restoring an Equinox Management Backup File.... 404
Making the Avaya IX™ Workplace Client available to users.... 406
Upgrading All-In-One Equinox Management.... 409
Upgrading Equinox Management deployed in high-availability or geographic redundancy... 410
Upgrading the User Portal + Web Gateway.... 414
Upgrading multiple User Portal + Web Gateway nodes simultaneously.... 415
Managing Cassandra repairs of Avaya Aura® Web Gateway nodes.... 416
Upgrading the distributed H.323 Gatekeeper.... 418
Upgrading H.323 Gatekeepers in Alternate Mode.... 419
Daily Maintenance of your Video Network.... 421
Searching for a Video Device.... 421
Removing a Video Device from Equinox Management.... 422
Preparing a Device for Maintenance.... 423
Replacing a defective node in a User Portal or Web Gateway cluster.... 424
Managing Bandwidth in your Network.... 424
Upgrading, Backing Up and Restoring Video Device Software.... 425
Editing upgrade history of video devices.... 425
Upgrading the software file of a video device.... 426
Removing a software upgrade file from a video device.... 429
Backing up and duplicating a video device configuration.... 430
Updating license keys.... 431
Restoring the previous software version of a network device.... 431
Downgrading your Network Device.... 433
Defining Video Usage Defaults.... 433
Maintaining Scheduled Meetings.... 437
Searching for a Meeting.... 437
Modifying Upcoming Meetings.... 439
Disaster recovery in a geographic redundancy deployment.... 439
Activating disaster recovery in a geographic redundancy deployment.... 440
Resuming normal operations after disaster recovery.... 442
Retrieving the Customer Support Package.... 444
Chapter 14: Resources.... 446
Documentation.... 446
Finding documents on the Avaya Support website.... 450
Accessing the port matrix document.... 450
Avaya Documentation Center navigation.... 451
Training.... 452
Support.... 452
Using the Avaya InSite Knowledge Base.... 453
Appendix A: List of preferred dial in numbers examples.... 454
Appendix B: Equinox audio prompts and announcements.... 456
Appendix C: Avaya Equinox® Management reports fields.... 474

Glossary..... 479

Chapter 1: Getting started with Avaya Equinox® Management

This section provides an orientation for Equinox Management, including its features, considerations for planning and implementing its deployment, and how to access Equinox Management:

Related links

Avaya Equinox® Management overview on page 12
New in this release on page 14
Updates to this publication on page 15
Planning your Avaya Equinox® Management deployment on page 15
Localized languages in Equinox Management on page 27
Accessing Avaya Equinox® Management on page 28
Initial configuration workflow on page 29

Avaya Equinox® Management overview

System administrators use Avaya Equinox® Management to control video network devices, such as gateways, media servers, and endpoints.

You access Equinox Management from the administrator portal. Service providers and organization administrators access the administrator portal to perform network-wide management, while customers of service providers access the administrator portal to perform similar tasks that are relevant only for their organization. Meeting operators, organizers, and regular users access the user portal to perform scheduling and management relevant to them.

The system administrator defines different user profiles with varying permissions to determine the management tasks available for a specific user.

Equinox Management sits at the core of your Equinox Solution deployment and offers the following capabilities:

- Video network device management

  Remotely configure, upgrade and monitor many of your video network devices via the administrator portal. These devices include Avaya Equinox® Media Server, Avaya Web Collaboration server, Avaya Equinox® Streaming and Recording, and many gateways.

- Endpoint management

  Remotely configure, upgrade and monitor both Equinox Solution and third-party endpoints via the administrator portal.

- Resources and bandwidth management

  Configure your network devices and endpoints for effective bandwidth control. For example, you can determine when meetings are cascaded between multiple media servers. You can also monitor in real-time from the administrator portal's dashboard, or generate reports to see network statistics for a given time period.

- User management

  You can manage user access by creating profiles with a set of capabilities. You can also create virtual rooms and assign endpoints. Equinox Management also integrates with existing directory servers such as Microsoft Active Directory for easy user provisioning.

- Interface to unified communication solutions

  Equinox Management provides the interface to market leading unified communication solutions such as Avaya Aura® Power Suite.

- SIP server integration

  The smooth integration with third-party SIP servers leverages existing network call control for the videoconferencing system. The SIP server manages the call control and network usage, while Equinox Solution supplies the videoconferencing capabilities.

- Built-in gatekeeper

  Equinox Management is shipped with a built-in gatekeeper, which is called *Avaya Equinox H.323 Gatekeeper*. It supplies the correct destination IP and authorizes the appropriate bandwidth for the call. In this way, Equinox Management can manage endpoint-initiated calls and point-to-point calls.

- Call authorization

  Equinox Management integrates with the gatekeeper to authorize calls based on the settings you define for your network, such as user capabilities and allowed bandwidth.

- Multi-stream switching

  Equinox Management maximizes network bandwidth efficiency during multi-participant communication. High scalability enables resources to be redistributed among participating endpoints, as needed.

- Mixed mode video support

  Equinox Management enables maximum experience in terms of interoperability in legacy AVC room systems, and where mobile devices cannot support multiple decoding and encoding streams.

- Processed mode video support

  Equinox Management optimizes legacy environments that do not support multi-stream switching technology or have bandwidth limitations.

Related links

Getting started with Avaya Equinox® Management on page 12

New in this release

The following features are new in this release:

- Dynamic meeting ID for increased security for meetings scheduled from Avaya Meeting Scheduler Outlook Add-in. on page 26
- All new better features for customizing branding in Unified Portal , see Customized branding in Unified Portal in release 9.1.10 on page 41.
- Configuring meeting policies PIN security on page 209.
- Enabling FIPS Compliance for redundancy mode on page 215 and Enabling hardening for the Avaya Equinox management server on page 214.
- New check box **Can reserve meetings from Avaya Meeting Scheduler for Windows Outlook** in Creating or modifying a user profile on page 224 and advanced parameters for reserving meetings from Meeting Scheduler on page 226.
- Creating or Modifying VR for Conferencing User on page 255
- New check box **Insert this tag in the invitation location field for reserved meetings** in Creating an invitation template on page 262.
- New log retention fields in **Configuring the Log Level** settings, see Configuring the Log Level on page 292.
- It is now possible to change a participant name in a waiting room, seeChanging a participant name on page 326
- New dialing plan configuration options for including dynamic meeting IDs, see Configuring Dial Plan settings on page 349.
- There are new report types for virtual rooms. See About types of Equinox Management reports on page 364.
- New field **CDR retention time for local server** in CDR Settings, see Configuring Call Detail Records on page 376.
- New audio anouncements, see Table of audio prompts and announcements on page 456.

Related links

Getting started with Avaya Equinox® Management on page 12

Updates to this publication

The following sections have been updated in this publication:

- Ports to open on page 16
- Removed all Scopia® Video Gateway and SIP Gateway references from the publication starting at Ports to open on page 16.
- Minimum Requirements on page 23
- Note added to Avaya Meeting Scheduler Outlook Add-in on page 26
- Note about operator calls added to Enabling Auto-Attendant Support on page 88
- Creating or modifying a user profile on page 221
- Note added to Enabling the Avaya Meeting Scheduler Outlook Add-in without the Avaya IX Workplace Client on page 275
- Requirements for Avaya Meeting Scheduler Outlook Add-in added to Enabling the Avaya Meeting Scheduler Outlook Add-in without the Avaya IX Workplace Client on page 275
- Note added to Configuring Outlook on the web without the Avaya IX Workplace Client on page 276
- Configuring shuffling in Avaya Aura® Communication Manager on page 357
- Configuring the SIP Endpoint Managed Transfer Setting in Aura Communication Manager on page 347
- Configuring the Log server settings on page 359
- Configuring a secure connection using a different CA for the Log server on page 359
- Configuring a SysLog Server with TLS on page 360
- Configuring a secure connection using the same CA for the Log server on page 361
- Configuring a non-secure connection for the Log server on page 363
- Manually promoting the off-site backup server on page 389
- Restoring primary server from off-site backup server on page 392
- Upgrading the distributed H.323 Gatekeeper on page 418
- Upgrading H.323 Gatekeepers in alternate mode on page 419

Related links

Getting started with Avaya Equinox® Management on page 12

Planning your Avaya Equinox® Management deployment

When planning your Equinox Management deployment, it is important to understand the minimum system requirements described in this section.

You can deploy Equinox Management differently, depending on the needs of your organization. There are several solutions defined in the *Equinox Solution Guide*, each with its own deployment

scenario and network topology. Decide on the type of deployment you need based on your video requirements and your existing network topology.

The *Equinox Solution Guide* details the considerations for choosing each of the deployments, and the locations to place each of the solution components within the network topology.

When planning your deployment, it is also important to consider port security (see Implementing port security for Avaya Equinox® Management on page 16) and whether to install redundant Equinox Management servers for high availability (High Availability of Equinox Management on page 378).

For installation procedures for each of the components of the Equinox Solution, see the *Deploying Avaya Equinox Solution Guide*. For installation procedures for Equinox Management, including the technical specifications for Equinox Management, see the *Deploying Avaya Equinox Solution Guide*.

Related links

Getting started with Avaya Equinox® Management on page 12
Implementing port security for Avaya Equinox® Management on page 16
Ports to open on Avaya Equinox® Management on page 16
Minimum requirements for Equinox Management on page 23
Planning user access to videoconferences on page 25

Implementing port security for Avaya Equinox® Management

Avaya Equinox® Management is located in the enterprise (internal) network and is connected to the DMZ and public network via firewalls.

Avaya Equinox® Management can connect to H.323 endpoints in public and partner networks via Avaya Equinox® H.323 Edge, and to H.323 and SIP endpoints located in the enterprise network. For a list of TCP/IP/UDP ports supported by Avaya Equinox® Management, see Ports to open on Avaya Equinox® Management on page 16.

For a list of TCP/IP/UDP ports supported by other Equinox Solution products, see the *Port Security Reference Guide* or the *Deploying Avaya Equinox Management* guide.

Related links

Planning your Avaya Equinox® Management deployment on page 15

Ports to open on Avaya Equinox® Management

Avaya Equinox® Management is typically deployed in the enterprise network or the DMZ.

When opening ports to and from Equinox Management, use the following as a reference:

- For ports both to and from Equinox Management, see Table 1: Bidirectional ports to open on Equinox Management on page 17.

- For outbound ports from Equinox Management, see Table 2: Outbound ports to open from Equinox Management on page 19.
- For inbound ports into Equinox Management, see Table 3: Inbound ports to open on Equinox Management on page 22.

Important:

Choose the specific firewalls to open ports, depending on where your Avaya Equinox® Management and other Equinox Solution products are deployed.

Table 1: Bidirectional ports to open on Equinox Management

Port Range	Protocol	Source/ Destination	Functionality	Result of Blocking Port	Required
23	Telnet (TCP)	Sony PCS address book, MCM, Endpoints	Enables you to use Sony PCS address book, retrieve element logs, and control MCM and endpoints.	Cannot use Sony PCS address book feature or retrieve logs from various devices (such as MCM).	Recommended
80	HTTP (TCP)	Web client	**In**: Provides access to the Equinox Management web user interface. When installed with the gatekeeper, this port defaults to 8080. **Out**: Provides access to the Equinox Management web user interface, TANDBERG MXP management (XML API via HTTP) and Scopia Elite MCU.	Cannot manage TANDBERG MXP and Scopia Elite MCU from the Equinox Management administrator portal.	Mandatory You can configure this port during installation (see *Installation Guide for Avaya Equinox® Management*).
161	SNMP (UDP)	Any managed element	Enables SNMP configuration	Cannot operate the SNMP service with devices, and forward trap events do not function.	Mandatory

Table continues…

Port Range	Protocol	Source/ Destination	Functionality	Result of Blocking Port	Required
162	SNMP (UDP)	Any third-party SNMP manager	Enables sending SNMP trap events from any managed element	Cannot operate the SNMP service with devices, and forward trap events do not function.	Recommended
389	LDAP (TCP)	LDAP servers	Enables connection to LDAP servers	Cannot work with LDAP Servers	Mandatory for LDAP authentication
3336	XML (TCP)	Equinox Management/ MCU	Enables communication between Equinox Management and the MCU via the moderator's XML API (used for managing meetings via Equinox Management)	Equinox Management cannot connect to the MCU via the XML API	Mandatory if deployed with MCU
3337	SOCKS (TCP)	Equinox Management	Enables synchronization between multiple redundant Equinox Management installations	Cannot operate redundancy	Mandatory in deployments with a redundant Equinox Management server.
3346	XML (TLS)	Equinox Management	Enable secure XML Connection to Equinox Management	Cannot open secure XML connection to Equinox Management	Mandatory for any XML secure clients
3358	TCP	OVA platform	Enables PMGR XML API	Cannot manage OVA	Mandatory
3368	TLS	OVA platform	Enables PMGR XML API	Cannot manage OVA with secure connection	Mandatory when secure connection is enabled
5060	SIP (TCP/ UDP)	B2B/ Other SIP components	Enables SIP signaling	Cannot connect SIP calls	Mandatory
5061	SIP (TLS)	B2B/ Other SIP components	Enables secure SIP signaling	No TLS connection available	Mandatory

Table continues…

Port Range	Protocol	Source/ Destination	Functionality	Result of Blocking Port	Required
5432	TCP	Equinox Management	Enables master/slave data synchronization (used for Equinox Management redundant deployments with an internal database)	Cannot synchronize data between the master and slave servers	Mandatory for redundancy deployments with an internal database
7800-7802	UDP	Equinox Management	Enables data synchronization between redundant Equinox Management servers	Redundancy functionality is not available	Mandatory for redundancy deployments
8095	HTTP	OVA platform	Enables PMGR web	Cannot upload/ download packages	Mandatory
8445	HTTPS	OVA platform	Enables PMGR web	Cannot upload/ download packages with secure connection	Mandatory when secure connection is enabled

Table 2: Outbound ports to open from Equinox Management

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
7	Echo (TCP)	Video Network Devices	Detects online status of video network devices	Cannot detect online status of video network devices	Mandatory
21	FTP (TCP)	Equinox Management	Enables downloading logs from H.323 Gatekeeper or other devices that allow logs to be downloaded via FTP. Enables importing and exporting TANDBERG Local Address Book. Enables software upgrade.	Cannot download logs from H.323 Gatekeeper or from other devices via FTP, import or export TANDBERG Local Address Book, or perform software upgrades.	Mandatory
22	SSH (TCP)	Equinox Management	Detects LifeSize endpoints. Enables downloading Avaya Equinox® H.323 Edge server logs.	Cannot detect LifeSize endpoints, download Avaya Equinox® H.323 Edge server logs.	Mandatory

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
24	Telnet (TCP)	Polycom endpoints	Enables you to control Polycom endpoints	Cannot control Polycom endpoints	Optional
25	SMTP (TCP)	SMTP server	Enables connection to SMTP server for sending email notifications	Cannot send email notifications	Mandatory
53	DNS (UDP)	DNS server	Enables DNS queries	Cannot parse domain names	Mandatory
445	NTLM (TCP/ UDP)	Active Directory Server	Enables connection to the Active Directory Server	NTLM SSO does not function	Mandatory
636	LDAP over SSL	Directory Server	Enables connection to the Directory Server	Cannot connect to the Directory Server	Mandatory
3089	TCP	Avaya Equinox® H.323 Edge	Detects endpoints via Avaya Equinox® H.323 Edge	Cannot detect endpoints via Avaya Equinox® H.323 Edge	Mandatory
3271	TCP	ECS	ECS XML API listening port	H.323 calls will not work correctly	Mandatory
3281	TLS	ECS	ECS XML API listening port	H.323 calls will not work correctly	Mandatory when TLS is enabled
3338	XML (TCP)	MCU	Enables connection to MCU via the administrator's XML API (used for configuring devices via Equinox Management)	Cannot perform configuration for MCU via the XML API	Mandatory if deployed with MCU
3339	XML (TCP)	B2B	Enables you to use the Equinox Management XML API	Cannot communicate with the B2BUA component via Equinox Management XML API	Mandatory
3341	TCP	Unified Portal	Equinox Management XML API listening port	Unified Portal will not work correctly	Mandatory
3342	TCP	UCCS server	Equinox Management XML API listening port	UCCP protocol will not work correctly	Mandatory
3343	TCP	Web Gateway server	Equinox Management XML API listening port	Web RTC call will not work correctly	Mandatory

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3344	TCP	AADS	Equinox Management XML API listening port	AADS will not work correctly	Mandatory
3346	XML (TLS)	MCU	Enables secure connection to the MCU via the moderator's XML API (used for managing meetings via Equinox Management)	Cannot securely connect to the MCU via the XML API	Mandatory for a secure XML API connection with MCU
3348	XML (TLS)	MCU	Enables secure connection to MCU via the administrator's XML API (used for configuring devices via Equinox Management)	Cannot securely connect to the MCU via the administrator's XML API	Mandatory for a secure XML API connection with MCU
3351	TLS	Unified Portal	Equinox Management XML API listening port	Unified Portal will not work correctly	Mandatory when TLS is enabled
3352	TLS	UCCS server	Equinox Management XML API listening port	UCCP protocol will not work correctly	Mandatory when TLS is enabled
3353	TLS	Web Gateway server	Equinox Management XML API listening port	Web RTC call will not work properly	Mandatory when TLS is enabled
3354	TLS	AADS	Equinox Management XML API listening port	AADS will not work correctly	Mandatory when TLS is enabled
5556	TCP	Avaya Web Collaboration server	Enables Equinox Management to receive alarms from Web Collaboration server.	Web Collaboration server cannot send alarms to Equinox Management.	Mandatory when Web Collaboration server is in your deployment
7140	TCP	CMS/AAMS	AAMS soap management API	Cannot configure high audio capacity CMS	Mandatory
7141	TLS	CMS/AAMS	AAMS soap management API	Cannot configure high audio capacity CMS	Mandatory when TLS is enabled
7150	TCP	CMS/AAMS	AAMS rest API listening port	Calls to CMS/ AAMS will not work correctly	Mandatory
7151	TLS	CMS/AAMS	AAMS rest API listening port	Calls to CMS/ AAMS will not work correctly	Mandatory when TLS is enabled

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
8089	XML (TCP)	Avaya Equinox® H.323 Edge server	Enables connection to Avaya Equinox® H.323 Edge server (v7.0 and later) via Avaya Equinox® H.323 Edge server XML API	Cannot connect to Avaya Equinox® H.323 Edge server via Avaya Equinox® H.323 Edge server XML API	Optional
50000	Telnet (TCP)	Sony endpoints	Enables you to control Sony endpoints	Cannot control Sony endpoints	Optional
55003	TCP	XT Series	Enables connection to the XT Series	Cannot connect to the XT Series	Mandatory if deployed with XT Series
63148	DIIOP (TCP)	Domino server	Enables connection with the Domino server	Cannot connect to the Domino Server	Mandatory if Equinox Management works with Domino Server

Table 3: Inbound ports to open on Equinox Management

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
443	HTTPS (TCP)	Web client	Enables Tomcat to run over SSL	Cannot access Equinox Management web user interface via HTTPS	Mandatory if using HTTPS
8080	HTTP (TCP)	Web client	Provides access to the Avaya Equinox® H.323 Edge and Equinox Management web user interface	Cannot access the Avaya Equinox® H.323 Edge web user interface	Mandatory if deployed with Avaya Equinox® H.323 Edge or Equinox Management internal Gatekeeper. You can configure this port during installation (see *Installation Guide for Avaya Equinox® Management*).
9443	HTTPS (TCP)	Web client	Enables Tomcat to run over SSL	Cannot access Equinox Management web user interface via HTTPS	Mandatory if using HTTPS. You can configure this port as part of setting up HTTPS (see Configuring the Tomcat web server to use HTTPS on page 180).

Related links

Planning your Avaya Equinox® Management deployment on page 15

Minimum requirements for Equinox Management

Minimum OVA hardware requirements

For the minimum hardware requirements for OVA deployment, see the **Technical Specifications — Hardware** section in the *Avaya Equinox® Management Deployment Guide*.

Operating systems

Avaya Equinox® Management supports the Red Hat Linux operating system. Beginning in Avaya Equinox® Management version 9.0, Red Hat Linux comes pre-installed. Users migrating from Scopia Management 8.3 must first export their configuration, deploy the new Equinox Management 9.x OVA and then import the configuration (see the **Deploying the Conferencing Application Server OVA** section in the *Avaya Equinox® Management Deployment Guide*).

Equinox Management is required to be deployed on a host with VMware vSphere ESXi versions 6.0, 6.5 or 6.7.

Redundancy requirements

High availability and service preservation for Equinox Management is based on either two or three redundant servers.

You can deploy two Avaya Equinox® Management servers in the same location, one as the primary server and the other as a secondary server (local redundancy). If the primary server fails, the secondary server automatically takes over. For increased reliability, deploy a third server as an off-site backup (geographic redundancy). For details, see High Availability of Equinox Management on page 378.

For existing redundant deployments, install Equinox Management on an additional server. For new redundant deployments, install Equinox Management on two or three separate servers, depending on the redundancy method.

Supported user directories (LDAP)

Equinox Management interoperates with a number of LDAP servers:

- Microsoft Active Directory Server for Windows 2012 Server
- Microsoft Active Directory Server for Windows 2016 Server
- Microsoft Active Directory Server for Windows 2019 Server
- Lotus Domino Server version 8.0
- Lotus Domino Server version 8.5, 8.5.1, 8.5.2, 8.5.3, 9.0

Databases

Avaya Equinox® Management uses its own internal database. External databases are not supported.

Supported web browsers

The following browsers are supported by Equinox Management:

- Internet Explorer® 11. A modern browser such as Chrome or Firefox is recommended.
- Firefox® 68.3 and higher

- Safari 13.0.4 and higher on MacOS
- Google Chrome 72 and higher

Supported mail programs

The Avaya Meeting Scheduler Outlook Add-in supports Outlook 2013 SP1 or later. See Minimum requirements for Avaya Meeting Scheduler Outlook Add-in on page 27.

Supported endpoints and video network devices

Equinox Management supports these video network infrastructure devices:

- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Scopia Elite MCU
- AvayaGateway
- H.323 Gatekeeper
- Cisco IOS H.323 Gatekeeper
- Cisco Unified Communications Manager
- Cisco TelePresence Video Communications Server (VCS)
- Broadsoft IP Centrix
- User Portal
- ASBCE
- H.323 Firewall Traversal Server

Equinox Management can also manage the following endpoints:

- Equinox Streaming and Recording
- Web Collaboration server
- Equinox Solution endpoints
  - Avaya Room System XT Series
  - Avaya IX™ CU360

Each endpoint model series supports Equinox Management features to different extents (see Table 4: Supported features with various endpoint models on page 24).

Table 4: Supported features with various endpoint models

Feature	Avaya XT Series	Avaya IX™ CU360
Monitoring	✓	✓
License Update	✓	✓
Remote Configuration	✓	✓

Table continues…

Feature	Avaya XT Series	Avaya IX™ CU360
Remote Reboot	✓	✓
Upgrade Software	✓	✓
Alarm/Events	✓	✓
Retrieve CS Package	✓	✓
Retrieve Configuration File	✓	✓
Update Configuration File	✓	✓
Retrieve Address Book File	X	X
Update Address Book File	X	X
Directory Integration	✓	✓
Calendar Integration	✓	✓

Related links

Planning your Avaya Equinox® Management deployment on page 15

Planning user access to videoconferences

As part of deploying Equinox Solution, you need to plan how users in your organization start videoconferences.

Users can either schedule a meeting in advance, and reserve the required video network resources, or they can start an instant meeting. Scheduling meetings with resources ensures a high quality user experience. If there are not enough resources during the videoconference, the system may either downgrade the video quality or block additional participants from joining.

Users can schedule meetings with resources in one of two ways.

- Avaya Equinox® Unified Portal: This is a browser application which enables users to configure many aspects of their meetings.
- Avaya Meeting Scheduler Outlook Add-in: This is a plug-in which enables users to add meeting details to any Microsoft Outlook appointment or meeting.

Related links

Planning your Avaya Equinox® Management deployment on page 15
Avaya Equinox® Unified Portal on page 25
Avaya Meeting Scheduler Outlook Add-in on page 26

Avaya Equinox® Unified Portal

Unified Portal is a single solution for managing your meetings. You can plan meetings in advance, customize meeting properties, and send the details of meetings to participants. At the meeting

start time, you can launch meetings in several ways. After the meeting, you can play and distribute the recording.

You can manage all your meetings, those chaired by you and those chaired by others, by using this single, calendar-enabled interface.

You can access Unified Portal on your computer or mobile device by using different client applications:

- On your Mac or PC using the Google Chrome™ or Mozilla Firefox™ browsers, you can attend meetings by using a web-based client that does not require any installation. This client supports sharing and launches seamlessly from Unified Portal. You can also attend meetings by using other browsers in the **Presentation Only** mode.
- Alternatively, you can attend meetings by using an installed client called Avaya IX™ Workplace Client for Windows, Avaya IX™ Workplace Client for Mac, Avaya IX™ Workplace Client for Android, or Avaya IX™ Workplace Client for iOS. Once installed from Unified Portal, this client is detected and used for future meetings. For more information on this application, see *Using Avaya Equinox® for Android, iOS, Mac, and Windows* at https://support.avaya.com/

You can share and annotate files and record the meeting, depending on your application.

Related links

Planning user access to videoconferences on page 25

Avaya Meeting Scheduler Outlook Add-in

Avaya Meeting Scheduler Outlook Add-in provides a new and improved Outlook add-in for desktop platforms that includes the following features:

- Add meeting details to an appointment.
- Start and join conferences from your calendar.
- Start a call from within Outlook to a contact by using Avaya IX™ Workplace Client if you have installed the Avaya Meeting Scheduler Outlook Add-in with Avaya IX™ Workplace Client.
- Dynamic meeting ID for increased security.

Additionally:

- You can auto-configure the meeting information for Avaya Equinox® and Avaya Aura® Conferencing.
- The conferencing system provides the meeting invitation templates for Avaya Equinox® Conferencing.

Note:

The Avaya Meeting Scheduler Outlook Add-in for Mac and web mail do not reserve scheduled meetings in Equinox Management. Only the Avaya Meeting Scheduler Outlook Add-in for Windows can reserve scheduled meetings in Avaya Equinox® Management and when the user profile is enabled for this capability. Users must not change any already reserved

meetings from non-Windows devices to avoid potential out of sync issues, which may prevent participants from joining the scheduled meetings.

Note:

If you have multiple Microsoft Outlook mailboxes, your Avaya Meeting Scheduler Outlook Add-in schedule only synchronizes with your default mailbox.

Minimum requirements for Avaya Meeting Scheduler Outlook Add-in:

- Avaya Equinox® Management version 9.1.10 TE/OTT deployments
- Avaya IX™ Workplace Client for Windows version 3.8.5 and higher
- Microsoft Exchange Server 2013 SP1 and higher or Microsoft Office 365

Related links

Planning user access to videoconferences on page 25

Localized languages in Equinox Management

Equinox Management's administrator portal, user portal, and plug-ins are available in English as well as other languages.

You can view Equinox Management's administrator portal in the following languages:

- Chinese (simplified)
- English (US)
- French
- Japanese

You can view Equinox Management's user portal and Avaya Meeting Scheduler Outlook Add-in in the following languages:

- Chinese (simplified)
- English (US)
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Russian

- Spanish (international)

By default, the system displays Equinox Management in English. To view Equinox Management in another language, change your Internet browser's language settings.

Related links

Getting started with Avaya Equinox® Management on page 12

Accessing Avaya Equinox® Management

Access Avaya Equinox® Management's administrator portal to perform network-wide management, and the user portal to perform scheduling and meeting management.

The system administrator defines different user profiles with varying permissions to determine the management tasks available for a specific user.

See the following for more information about accessing and using Equinox Management's portals, and configuring users in Equinox Management to use the Windows credentials:

Related links

Getting started with Avaya Equinox® Management on page 12
Accessing the Administrator Portal to manage your video network on page 28

Accessing the Administrator Portal to manage your video network

About this task

You can access Avaya Equinox® Management either from the administrator portal (as described below), or the user portal.

Access the Avaya Equinox® Management administrator portal to do the following:

- Manage all video network devices, including 3rd party endpoints:
  - Remote monitoring, configuration, and upgrade of devices
  - Managing your endpoints, for example by enabling the address book on all endpoints
- Manage bandwidth with:
  - Dynamically routed videoconferences for lowest cost
  - Distributed media server deployments
  - Using distributed media servers to join a single videoconference, thereby conserving bandwidth
- Manage users in the organization by:
  - Creating user profiles with varying user permissions and capabilities

    For information about user profiles and Equinox Management's built-in profiles, see Managing User Profiles on page 220.

- Using Equinox Management's built-in LDAP directory to manage users, or synchronizing users in your external LDAP directory, such as Microsoft Active Directory.
- Assigning endpoints and virtual rooms to users

Note:

The Avaya WebRTC Gateway utilization data, that the system displays under **Device Usage**, is the load factor of the server. The utilization may not be 0% even though there are no calls since the load factor is what WebRTC gateway uses to determine if it is capable of accepting new calls.

Procedure

1. Navigate to the URL of the Equinox Management administrator portal, as defined during installation. This should be in the following format: https://hostname/iview, where the hostname is the name of the application server on the Equinox Management server.
2. Log in to the Equinox Management administrator portal using the credentials specified in the installation process.

   The Dashboard appears (Figure 1: Administrator portal's dashboard on page 29).

   If your organization is part of a service provider deployment, use the credentials provided by the service provider.

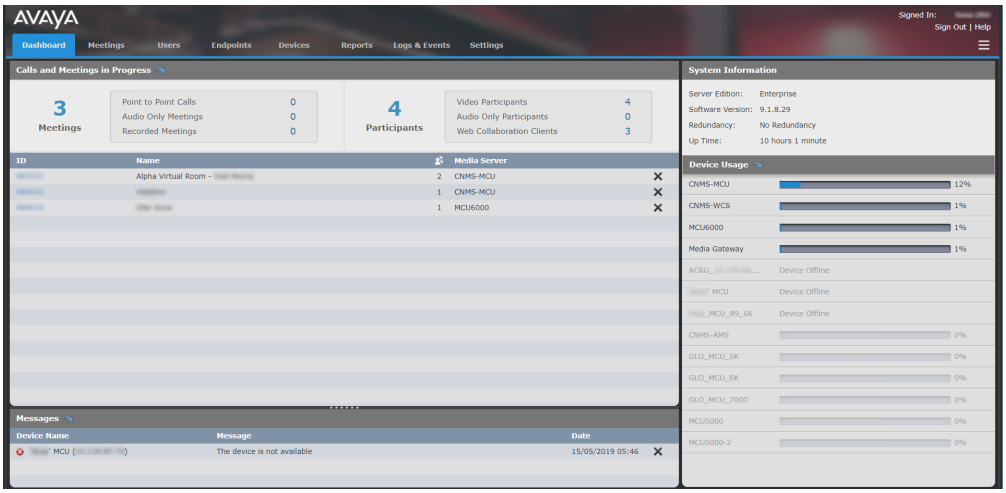


Figure 1: Administrator portal's dashboard

Related links

Accessing Avaya Equinox® Management on page 28

Initial configuration workflow

The tasks you need to perform depend on the Equinox Management you installed, and on your role in the deployment.

For enterprise editions of Equinox Management, all tasks are performed by the system administrator, defined during installation, or by additional administrators defined by the system administrator.

For service provider (multi-tenant) editions of Equinox Management, the service provider administrator performs network-wide setup of devices and locations, while the administrator of each organization defines its users and endpoints, as well as general meeting settings.

To get started in setting up your Equinox Management, follow the initial workflow relevant for you:

Related links

Getting started with Avaya Equinox® Management on page 12
Initial workflow for Enterprise Deployments on page 30
Initial workflow for service provider deployments on page 31
Creating an initial workflow for organizations in service provider deployments on page 32

Initial workflow for Enterprise Deployments

About this task

This workflow is relevant for organizations with the enterprise edition of Equinox Management. Service providers should follow the workflow described in Initial workflow for service provider deployments on page 31, and customers of service providers should follow the workflow in Creating an initial workflow for organizations in service provider deployments on page 32.

We recommend that you follow the initial configuration workflow described below, which offers an organized approach to setting up your network in Equinox Management and preparing the system for daily management. As you configure your network in Equinox Management, you can view a high-level orientation of your network topology.

Before you begin

- Verify that you have the necessary administrator permissions.

  The default system administrator was defined during initial setup of Equinox Management, and this administrator can create additional administrators. For more information, see Managing User Profiles on page 220.

- Before you start configuring your Equinox Management, make sure you have your network planned and all devices are installed and ready to run.

Procedure

1. If you have a distributed deployment (your network devices are situated in multiple locations), define the locations in Equinox Management, as described in Defining locations and organizations in your deployment on page 53.

   Important:

   If your organization has only one location, it is automatically configured during installation.

2. Add and configure the video network devices, including endpoints, in Equinox Management according to the workflow described in Device configuration workflow on page 58.

   If you are configuring Equinox Management redundancy, deploy the primary server first, referring to component FQDNs rather than IP addresses (for example, *smgmt.company.com*). This reduces maintenance when servers switch to their backups.

   See Defining your video network devices on page 58 for details about configuring your devices.

3. Define additional administrators, if necessary (see Creating or modifying a user profile on page 221). This is done by the system administrator, who is automatically configured during installation. This step can be done at any time.
4. Define the video users in your enterprise (see Defining and Managing Video Users on page 218).
5. For high availability, deploy multiple Equinox Management servers (see High Availability of Equinox Management on page 378).

   Once redundancy is configured, the database on each Equinox Management server are synchronized with each other.

Related links

Initial configuration workflow on page 29

Initial workflow for service provider deployments

About this task

This workflow is relevant for service provider administrators. If your organization is a service provider customer, follow the workflow described in Creating an initial workflow for organizations in service provider deployments on page 32.

We recommend that you follow the initial configuration workflow described below, which offers an organized approach to setting up your network in Equinox Management and preparing the system for daily management. As you configure your network in Equinox Management, you can view a high-level orientation of your network topology.

Before you begin

- Verify that you have the necessary administrator permissions.

  The default system administrator was defined during initial setup of Equinox Management, and this administrator can create additional administrators. For more information, see Managing User Profiles on page 220.
- Before you start configuring your Equinox Management, make sure you have your network planned and all devices are installed and ready to run.

Procedure

1. Define the locations in Equinox Management, as described in Defining locations and organizations in your deployment on page 53.

Important:

If there is only one location, it is automatically configured during installation.

2. Add and configure the video network devices in Equinox Management. Follow the workflow described in Device configuration workflow on page 58.

   If you are configuring Equinox Management redundancy, deploy the primary server first, referring to component FQDNs rather than IP addresses (for example, *smgmt.company.com*). This reduces maintenance when servers switch to their backups.

   See Defining your video network devices on page 58 for details about configuring your devices.

3. Define the organizations in your service deployment, including the organization's system administrator. For details on defining administrators in a service provider deployment, see Defining Administrators in a Service Provider Deployment on page 252.

4. For high availability, deploy multiple Equinox Management servers (see High Availability of Equinox Management on page 378).

   Once redundancy is configured, the database on each Equinox Management server are synchronized with each other.

Related links

Initial configuration workflow on page 29

Creating an initial workflow for organizations in service provider deployments

About this task

This workflow is relevant for organizations that are using a service provider for their videoconferencing solution. For service provider administrators, follow the workflow described in Initial workflow for service provider deployments on page 31.

We recommend that you follow the initial configuration workflow described in the following procedure, which offers an organized approach to setting up your endpoints and users in Equinox Management.

Before you begin

Verify that you have the necessary administrator permissions.

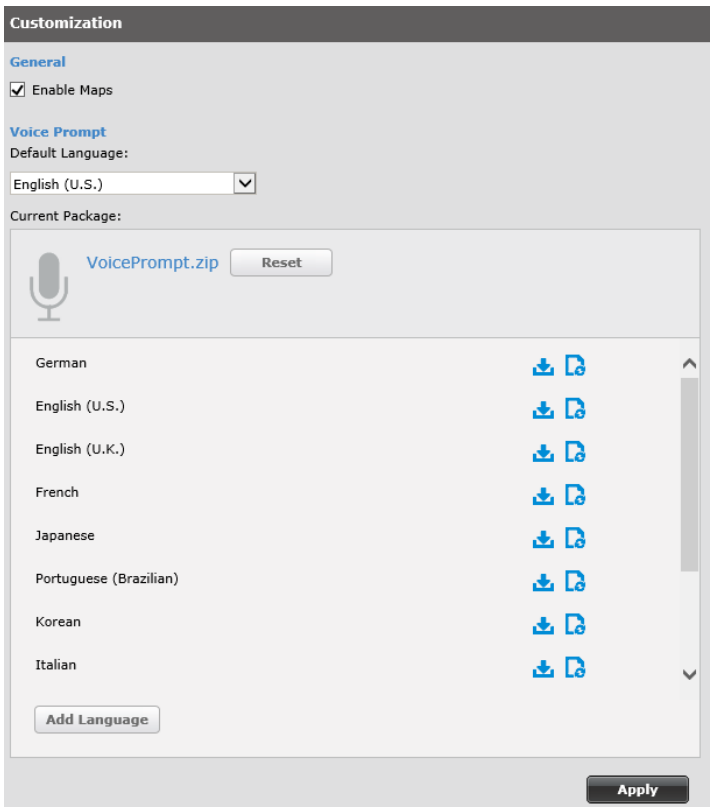
The default organization administrator was defined by the service provider during initial setup of Equinox Management, and this administrator can create additional administrators. For more information, see Managing User Profiles on page 220.

Procedure

1. Define default settings for meetings, as described in Defining a default and fallback meeting type on page 79 and Increasing MCU capacity by cascading multiple MCUs on page 85.

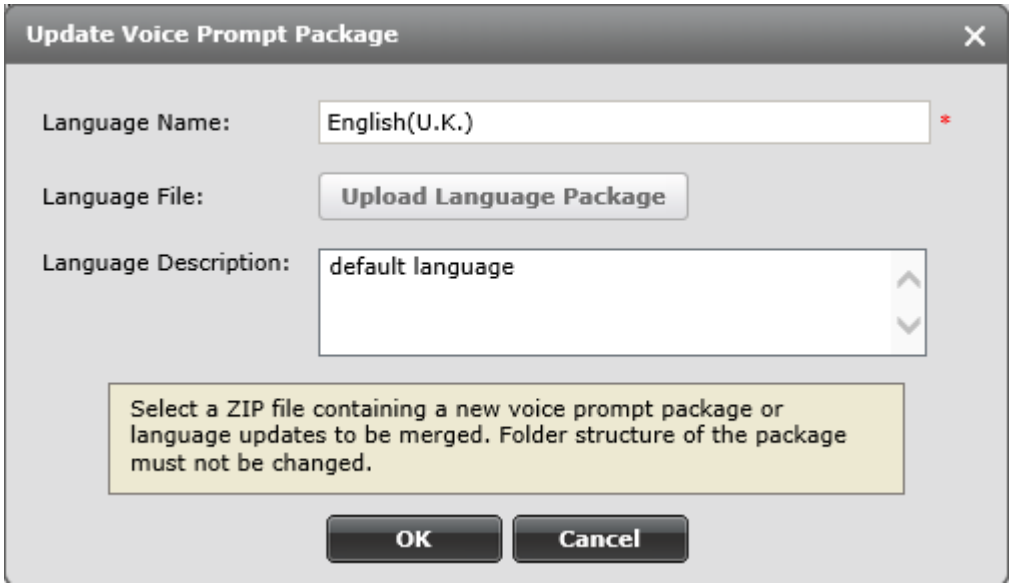
2. Define the Auto-Attendant settings, as described in Enabling Auto-Attendant support on page 88.
3. Define the video users in your organization, including additional administrators, as described in Defining and Managing Video Users on page 218. The default organization administrator is defined by the service provider.
4. Define the endpoints in your organization, as described in Planning and configuring endpoints in Equinox Management on page 120.
5. **(Optional)** You can customize the prompts and announcements transmitted by the system.
   a. Access the Equinox Management administrator portal.
   b. Click **Settings** > **Advanced** > **Customization** in the administrator portal's sidebar menu.

      The system displays the **Customization** page.



   c. Click the **Update** icon next to the relevant language.

      Equinox Management displays the **Update Voice Prompt Package** dialog box.

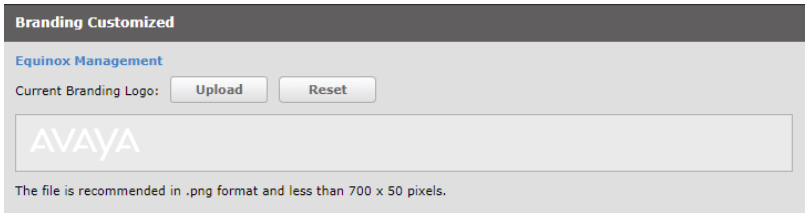


d. Click the **Upload Language Package** button to select a .zip file of voice prompts to upload.

6. If enabled by your service provider, you can modify the company logo, as follows:

   a. In the Equinox Management administrator portal, click **Settings** > **Advanced** > **Branding** in the administrator portal's sidebar menu.

   b. Click **Upload** in the Avaya Equinox Management section to upload your organization's logo.



   The updated logo appears in the administrator and user portals, and the Auto-Attendant menu. It is recommended that the image is in .png format and is less than 700 x 50 pixels.

You can also modify the background color branding in Unified Portal, as described in Customized branding in Unified Portal in release 9.1.10 on page 41.

Related links

Initial configuration workflow on page 29
Adding and modifying languages in Equinox Management on page 35
Customizing audio messages per tenant on page 37
Configuring the entry and exit announcement settings on page 39
Entry and exit announcement settings table on page 40
Customized branding in Unified Portal in release 9.1.10 on page 41

Customized branding in Unified Portal pre release 9.1.10 on page 42
Customized branding in Unified Portal with upgrade integrity pre release 9.1.10. on page 46
Preparing a .zip archive with customized files on page 50
Uploading a .zip Archive to Modify User Portal Branding on page 50

Adding and modifying languages in Equinox Management

About this task

You can customize the available voice prompt languages when working with a Media Server or an Elite MCU 6000. You can download a voice prompt package from a list of languages embedded in the system, and you can also add a new language together with a file containing voice prompts.

You can update voice prompts for all languages.

Procedure

1. Access the Equinox Management Administrator Portal.
2. Click **Settings** > **Advanced** > **Customization**.

   The system displays the **Customization** page.

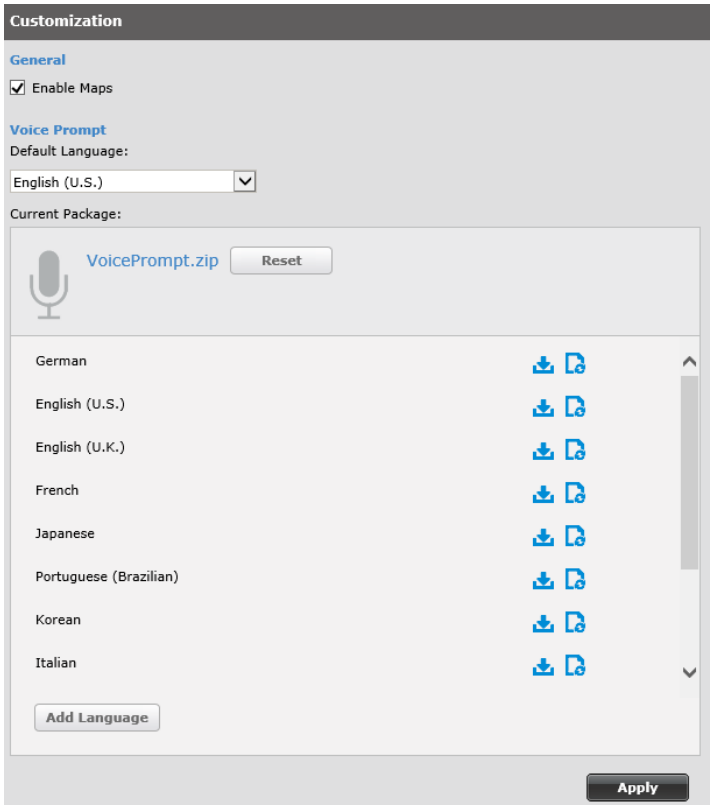


Figure 2: Customization page

Note:

When working in a multi-tenant environment, click **Settings** > **Multiple-tenant** > **Organizations**, select an organization and click the **Customization** tab to view this interface.

3. To download or update an existing package:
   a. Click the Download icon next to the language you want to download.
   b. Click the Update icon next to the language you want to update.

      The system displays the **Update Voice Prompt Package** dialog box, where you select the **Select a Voice Prompt Package** button and select a new voice prompt package to upload to the system.

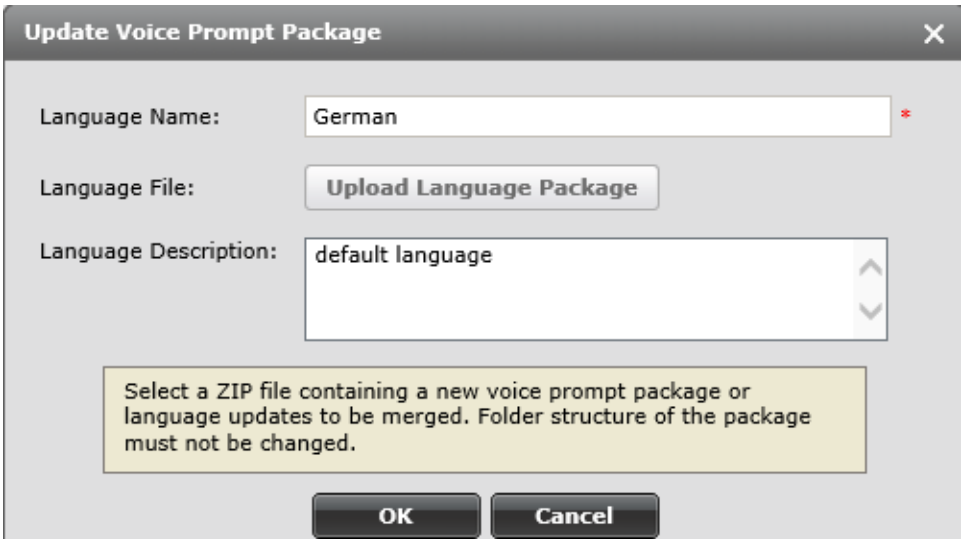


Figure 3: Update Voice Prompt Package dialog box

4. To add a new language:
   a. Click **Add Language**.

      The system displays the **Update Voice Prompt Package** dialog box.

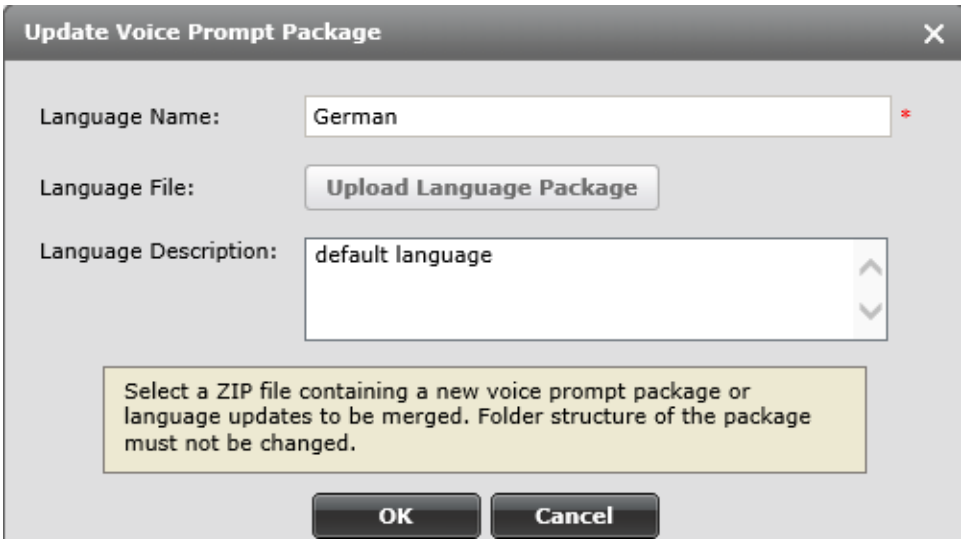


Figure 4: Update Voice Prompt Package dialog box

b. In the **Language Name** field, enter a name for the language.

c. In the **Language File** field, select **Upload Language Package** and select a language package you want to upload to the system.

d. Optionally, in the **Language Description** field, enter a description for the language.

e. Click **OK**.

Note:

- You can download or update a customized language, as you can do for an existing language.
- You can delete a customized language by selecting the Delete ✕ icon.
- You cannot delete embedded languages.

Related links

Creating an initial workflow for organizations in service provider deployments on page 32

Customizing audio messages per tenant

About this task

When working in a multi-tenant environment, you can customize the voice prompt language for each tenant. Equinox Management plays the voice prompts based on the user's selected language. If no language is selected for a user, Equinox Management plays the default language selected for the user's organization.

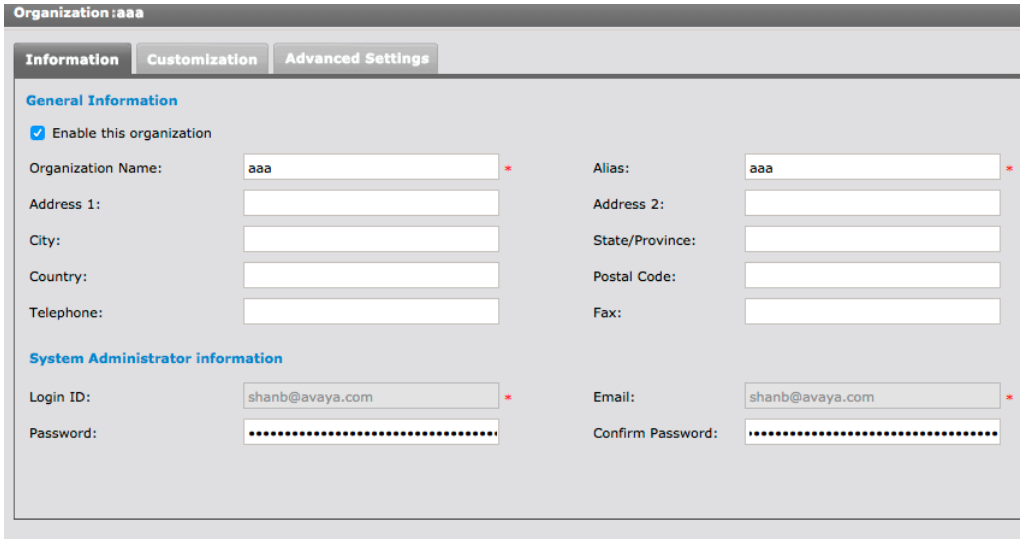
Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Multiple-tenant** > **Organizations**.

   The system displays the **Organization** page.

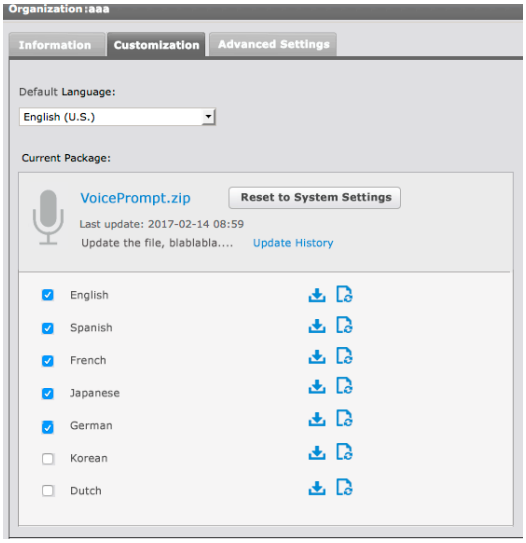
3. Select an organization, or click **Add** to create a new organization.

   The system displays the **Information** tab.

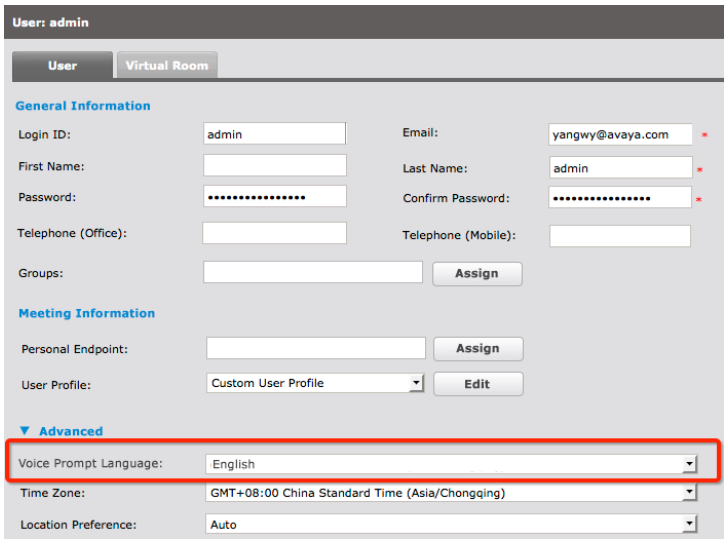


4. Click the **Customization** tag.

   The system displays the **Customization** page.



5. In the **Default Language** field, select the default language for users who do not have a specified voice prompt language.
6. Select the check boxes of the languages you want to enable for users.
7. Click **Users** and select the **All** option in either **Users from Active Directory** or **Users from Local Directory**.
8. Select a user on the **Users** page and locate the **Voice Prompt Language** field in the **Advanced** section:



The language you select is the language in which the user hears prompts when accessing the system.

The available languages are those selected for the user's organization on the **Customization** tab (see step 5 on page 38).

Related links

Creating an initial workflow for organizations in service provider deployments on page 32

Configuring the entry and exit announcement settings

About this task

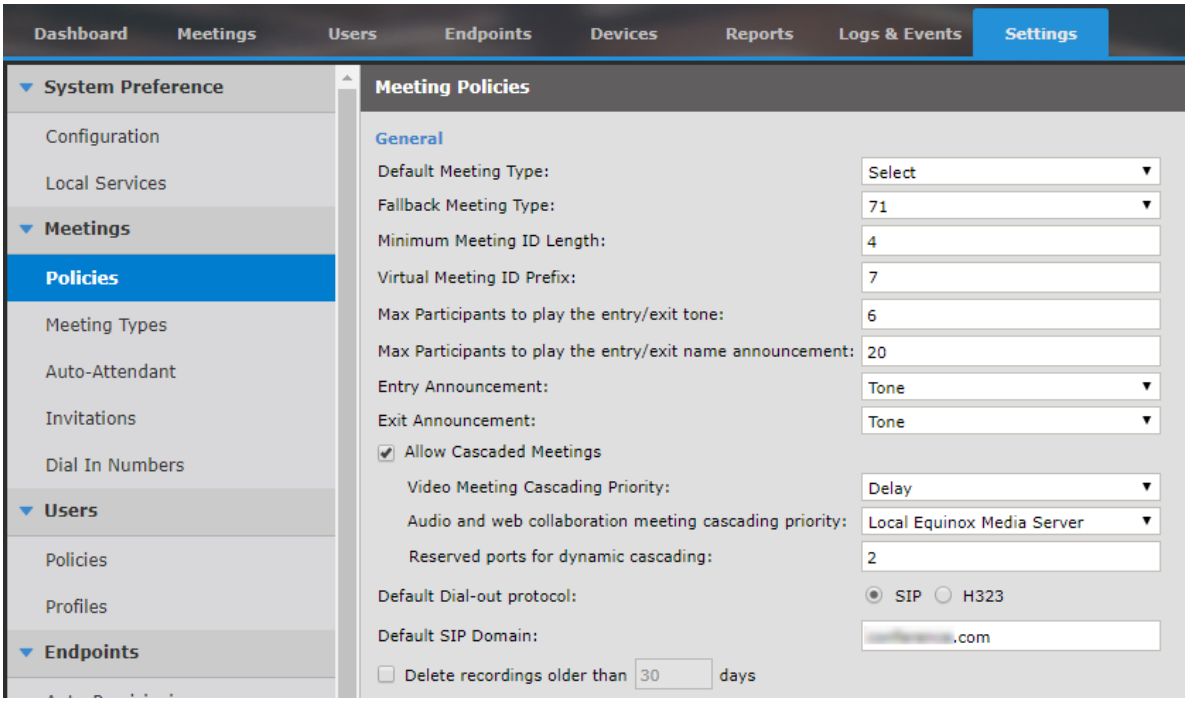
You can choose to have a tone played or a recording of the user's name played when a user enters the room. If you choose Name then the user is requested by audio to say the user's name. The name record feature only works with audio conferences. Examples are, "Roger has joined the meeting" and "Roger left the meeting.".

The user's experience is as follows:

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Meetings** > **Policies**.

   The system displays the **Meetings Policies** page.



3. Select **Tone** or **Name** for the **Entry Announcement** and **Exit Announcement** fields.
4. Click **Apply** to save your changes.

Related links

Creating an initial workflow for organizations in service provider deployments on page 32

Entry and exit announcement settings table

Field Name	Description
Entry Announcement	Default = Tone • **Tone**: Play a tone when a user enters the room. • **Name**: Play a recording of the user's name when the user enters the room.
Exit Announcement	Default = Tone • **Tone**: Play a tone when a user exits the room. • **Name**: Play a recording of the user's name when the user exits the room.

Related links

Creating an initial workflow for organizations in service provider deployments on page 32

Customized branding in Unified Portal in release 9.1.10

Before you begin

If you have not upgraded to Avaya Equinox® Management release 9.1.10 or newer then refer to the release 9.1.9 features described in Customized branding in Unified Portal pre release 9.1.10 on page 42 and Customized branding in Unified Portal with upgrade integrity pre release 9.1.10. on page 46.

About this task

If enabled by the service provider, the global administrator can greatly customize the branding of User Portal to the degree of changing almost any text and icons and even add CSS and JavaScript.

This feature supports multi-tenant deployments. The global admin can configure both global level branding and tenant level branding. If tenant level brand is not configured for a specific tenant, then global level branding is applied. If tenant level is configured, then tenant branding is used.

Note:

Currently the Avaya Equinox® Management GUI is only supported in English.

The following customizations are possible:

- User Portal
  - Logo
  - Background picture (Do not use huge file sizes. The default Portal background file size is 100 kB.)
  - Tab caption for User Portal page
  - Tab icon for User Portal page
- WebRTC client
  - Show **Enter Moderator PIN** prompt in waiting room
  - Tab caption for WebRTC client
  - Tab icon for WebRTC client
  - Roster background in WebRTC client
  - Chat background in WebRTC client
  - Post meeting page configuration
    - Show **Give Feedback** button
    - Show **Save logs** button
    - Show **Save Public Chat** button
    - Show **Save Participant List** button
    - Autoclose feedback window in n second
- Additional HTML content in multiple places such as:
  - Welcome caption for guest

  - Welcome caption for authenticated user
  - Additional HTML above logo
  - Additional HTML in footer
  - Additional HTML on Meeting started page
- Almost any text on User Portal
- CSS and JavaScript
  - Custom styles
  - Custom javaScript
  - Custom styles for WebRTC client
- The legal statement can be hidden
- Localization inside custom templates

Procedure

1. Click **Settings** > **Devices** > **User Portal/Web Gateway** > **Custom Branding**.
2. In a multi-tenant deployment ,choose the organization in the **Organization** drop-down list.
3. Select the **Enable enhanced branding** check box.
4. Perform the customization.
5. Click **Save** after making changes for them to take effect.

Related links

Creating an initial workflow for organizations in service provider deployments on page 32

Customized branding in Unified Portal pre release 9.1.10

Before you begin

If you upgraded to Avaya Equinox® Management release 9.1.10 or newer then it is recommended to use the new feature described in Customized branding in Unified Portal in release 9.1.10 on page 41.

About this task

If enabled by your service provider, you can customize the branding of User Portal. The method described in this procedure creates a customized branding which does not remain after upgrades however the branding is customizeable to the level of fonts and colors. You upload a .zip file with the customized branding in Equinox Management, and your selected company logo, background image and CSS theme are displayed in Unified Portal. You can also do the following:

- Add a custom html element to the start page (Join page)
- Add a custom html element before the logo
- Add a custom html element after the logo
- Use localization inside custom templates
- Add additional css styles

- Add powered by logo

Before uploading, you must configure the relevant .css files to be included in the .zip file.

Note:

You must update the zip archive on Avaya Equinox® Management after each upgrade on ESG bin.

Before you begin

Ensure that you have created a directory titled `up` on your desktop, to store the .css files.

Procedure

1. Build a customized .css file, as follows:
   a. Install npm to your local machine by navigating to the following URL:

      https://nodejs.org/dist/v4.5.0/node-v4.5.0-x64.msi

   b. In the command prompt, install `grunt`, using the following command: `npm install -g grunt-cli`
   c. For releases older than 9.1.0.5 for Avaya Equinox® for Team Engagementcopy `src` for the current ESG bin to the desktop of your local machine from the following directory: `/opt/Avaya/CallSignallingAgent/<ESG bin version>/tomcat/8.0.24/webapps/portal/branding`
   d. For releases older than 9.1.0.5 for Avaya Equinox® for Over The Topcopy `src` for the current ESG bin to the desktop of your local machine from the following directory: `/opt/Avaya/CallSignallingAgent/<ESG bin version>/tomcat/8.0.24/webapps/portal/branding`
   e. For releases 9.1.0.5 and later copy `src` for the current ESG bin to the desktop of your local machine from the following directory: `https://<Portal_FQDN>/portal/assets/smart-branding.zip`
   f. Open a command line on your computer.
   g. Navigate to the `/branding` directory on your local machine and run the following commands:

      ```
      npm set progress = false
      npm install
      grunt
      ```

   h. Copy the `style.min.css` file in the `/branding` directory to a file on the desktop.

      See Preparing a .zip archive with customized files on page 50 for details.

2. Modify the .css theme, as follows:
   a. Open the following file: `/branding/assets/styles/theme.less`
   b. Modify the colors to your preferred colors, as indicated in the following image:

theme.ess

```
Example:
Before
-----------------------------
@background: @off-white;
@background-white: @white;
@background-black: @navy-black;
@background-dark: @dark-gray;
@background-error: @highlight-error;
@background-front-page: fade(@background, 64%);
----------------------------------------------

After
-----------------------------
@background:#000000;
@background-white: #FF0000;
@background-black: #FFFFFF;
@background-dark: #000001;
@background-error: #000002;
@background-front-page: fade(@background, 64%);
----------------------------------------------
```

Note:

Colors must be defined in hex format.

c. If any changes were made, you must reconfigure your `style.min.css` file.

3. Change your logo, as follows:

   a. Copy your logo image to the `up` directory you created.

   See Preparing a .zip archive with customized files on page 50 for details.

   b. Open the `/branding/assets/styles/theme.less` file, and locate the following:

   ```
   @logo: @url-logo;
   @logo-height: 64px;
   @logo-width: 157px;
   ```

   c. Modify these strings to the following:

   ```
   @logo: url('<name of logo file>');
   @logo-height: <height of your logo file>px;
   @logo-width: <width of your logo file>px;
   ```

   d. If any changes were made, you must reconfigure your `style.min.css` file.

4. Modify your background image, as follows:

   a. Copy your background image to the `up` directory you created.

   See Preparing a .zip archive with customized files on page 50 for details.

   b. Open the `/branding/assets/styles/theme.less` file, and locate the following:

   ```
   @background-image: @off-white @url-background top –100px right
   no-repeat;
   ```

c. Modify this string to:

```
@background-image: @off-white url(<name of your background
image>) top –100px right no-repeat;
```

d. If any changes were made, you must reconfigure your `style.min.css` file.

5. **(Optional)** You can add a customized html element to the page that displays after logging into the system, as follows:

   a. Create the relevant html file, `Guest.html` for guest users, or `SignIn.html` for registered users.

   b. Add content with your desired style to the file.

   c. Copy your file to the `up` directory you created.

   d. To add custom html before the logo, create Custom2.html.

   e. To add custom html after the logo, create Custom3.html.

   f. Translate the custom HTML:

      - Create a file in format <locale>.json (for example, en-US.json for the English locale).
      - Insert new keys in the file according to the following example:

```
{
JOIN:     {
        LEGAL_TEXT : {
                                QUICK_START:"Quick start"
}
}
}
```

      - Use these keys in the custom html according to the following:

```
<a translate-once="JOIN.LEGAL_TEXT.QUICK_START" href="https://
downloads.avaya.com/css/P8/documents/101042623" target="_blank"></a>
```

   g. Put the custom styles in the **custom-style.css** file.

      You can change the order of the elements on the main page. The following is the default order:

      - Join form (class “join-form”)
      - Optional custom html 2
      - Logo (class “logo”)
      - Optional custom html 3

      Since all these elements are inside flexbox. The administrator is able to change the order of any element using the **order** css property. For example, if you want to move the logo to the top, add the following inside custom-style.css:

```
.logo {
        order:-1;
}
```

Note:

If you want to have identical custom content for guest and signed in user then you have to create both files (Guest.html and SignIn.html) with identical content.

If you need to place only text in your html files then you can use the default styles. The following is an example of the default file.

```
Default Guest.html
<div class="join-caption">Some text</div>
```

6. Add a Powered By logo with a file named **powered-by-logo.png** to the zip branding package.

   The filename must be **powered-by-logo.png**.

Next steps

Prepare a zip archive with your customized files, as described in Preparing a .zip archive with customized files on page 50.

Related links

Creating an initial workflow for organizations in service provider deployments on page 32

Customized branding in Unified Portal with upgrade integrity pre release 9.1.10.

Before you begin

If you upgraded to Avaya Equinox® Management release 9.1.10 or newer then it is recommended to use the new feature described in Customized branding in Unified Portal in release 9.1.10 on page 41.

About this task

If enabled by your service provider, you can customize the branding of the User Portal. To change the logo, see 6 on page 34. The method described in this procedure creates a customized branding which keeps its integrity during upgrades. However, the branding is not customizeable to the level of colors and fonts. You upload a .zip file with the customized branding in Equinox Management, and the following are displayed in User Portal:

- Background image
- CSS theme
- Custom html element to the start page (Join page)
- Custom html element before the logo
- Custom html element after the logo
- Localization inside custom templates
- Powered by logo

Before uploading, you must configure the relevant .css files to be included in the .zip file. You can find examples of the files described in the following task at **https://<AAWG FQDN>/portal/assets/branding.zip**.

Before you begin

Procedure

1. Build a customized .css file and name it **custom-style.css**.

   Refer to the following example:

```
.logo {
    order: -1;
}


a.nav-link[ui-sref='upc.schedule'] {
    display: none;
}


body {
    background-image: url(Type URL here) !important;
    background-color: black;
}
```

   a. To modify the background, set the URL in the following code to the URL of the image in custom-style.css.

```
body {
    background-image: url(Type URL here) !important;
    background-color: black;
}
```

   Note:

   If the aspect ratio of the browser window is different from the aspect ratio of the image then areas without image are displayed. You can fill it with some color using the "background-color": rule. Some examples of colors that you can use are: #000000 (black), #0000FF (blue). See CSS color references on Internet for details on CSS colors.

   b. You can change the element order on the main page.

   Refer to the following examples:

   To move the logo to the top:

```
.logo {
order: -1;
}
```

   To hide the **schedule** tab:

```
a.nav-link[ui-sref='upc.schedule'] {
    display: none;
}
```

2. You can add an additional custom html element before the logo.

   Changes you make to Custom2.html are displayed before the logo. You can apply localization to the Custom2.html file but when you add localization you must save the file in UTF-8 format. The application supports the following languages: de-DE, en-US, es-XL, fr-FR, it-IT, ja-JP, ko-KR, pt-BR, ru-RU, zh-CN and zh-TW.

```
<div class="custom-branding">
    <a translate-once="CUSTOM_BRANDING.LINK1"
```

```
        href="http://bipbap.ru/wp-content/uploads/
2017/10/0_a9e8c_fefaa1d2_XL-640x400.jpg" target="_blank">VALUE</a>
    <a translate-once="CUSTOM_BRANDING.LINK2"
        href="https://somelink" target="blank">_blank</a>
</div>
```

3. Use the translate-once Attribute to specify the key in the json-file translation.

   en-US.json

```
{
    "CUSTOM_BRANDING":  {
        "LINK1":"VALUE",
        "LINK2":"ANOTHER VALUE"
    }
}
```

   fr-FR.json

```
{
    "CUSTOM_BRANDING":  {
        "LINK1":"VALEUR",
        "LINK2":"UNE AUTRE VALUER"
    }
}
```

   After you apply these changes, the links before the logo are displayed. In the English localization the first link is named **VALUE** and the second is named **ANOTHER VALUE.**. In the French localization the first link is named **VALEUR**, and the second is named **UNE AUTRE VALUER**.

   Note:

   You can nest keys and you can use a dot to specify a child property.

```
{
    "JOIN"    :{
        "LEGAL_TEXT":    {
            "QUICK_START":    "Quick start"
        }
    }
}
```

   In html it is displayed as:

```
<a translate-once="JOIN.LEGAL_TEXT.QUICK_START" href="https://
downloads.avaya.com/css/P8/documents/101042623" target="_blank"></a>
```

   English is used as the default language if there is no json-file with a locale corresponding to the browser locale.

4. You can add an additional custom html element after the logo.

   Follow the instructions for **Adding an additional custom html element before the logo** and use Custom3.html.

5. You can add localization for the following languages: de-DE, en-US, es-XL, fr-FR, it-IT, ja-JP, ko-KR, pt-BR, ru-RU, zh-CN, zh-TW. When you add localization you must save the file in UTF-8 format.

   For an example see the step on **Adding an additional custom html element before the logo**.

6. You can add a custom html element to start page (Join page).
   - If you are a guest user, create a Guest.html file and add the required content with your style.
   - If you are signed in as a user, create a SignIn.html file and add the required content with your style.
7. Add a Powered By logo with a file named **powered-by-logo.png** to the zip branding package. The filename must be powered-by-logo.png.
8. Prepare a zip archive with your customized files, as described in Preparing a .zip archive with customized files on page 50.
9. To upload the zip archive:
   a. Log in to Equinox Management as the tenant admin.
   b. Select **Settings** > **Advanced** > **Branding**.

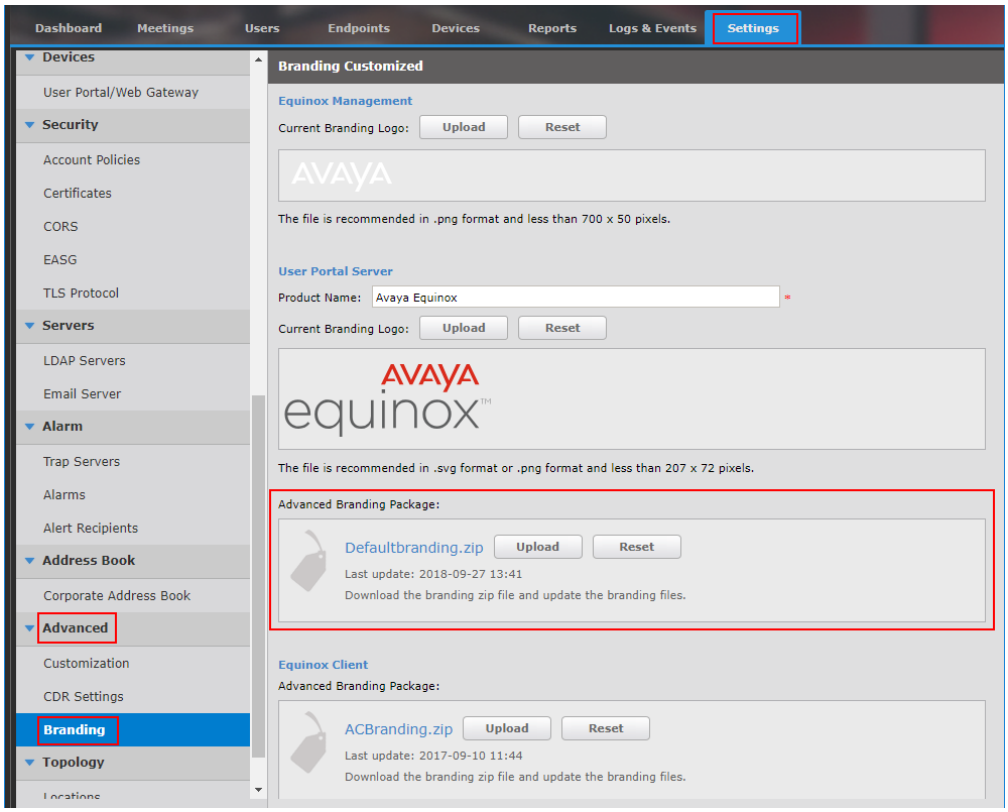


Figure 5: Advanced Branding Package Upload

   c. Click **Upload**.
   d. Click **Apply**.

Related links

Creating an initial workflow for organizations in service provider deployments on page 32

Preparing a .zip archive with customized files

About this task

After you customize elements for branding in Equinox Management, you must create a .zip archive with the customized files. The .zip is then uploaded into Equinox Management.

Before you begin

- Ensure that you have created the `up` directory on your desktop:
- Ensure that you have successfully customized the branding elements for the User Portal, as described in Customized branding in Unified Portal pre release 9.1.10 on page 42 or Customized branding in Unified Portal with upgrade integrity pre release 9.1.10. on page 46.

Procedure

1. Ensure that all of your customized files have been placed in the `up` directory.
2. Zip the `up` directory, and assign the zipped archive any name.

   There must be no additional directories inside the archive. All files must be in the root of the archive. An example of a zipped archive is as follows:

```
Archive Structure
Archive.zip
• Guest.html
• SignIn.html
• Custom2.html
• Custom3.html
• custom-style.css
• en-US.json
• fr-FR.json
• powered-by-logo.png
… the rest of the locales
```

   Note:

   All files are optional in this archive.

Related links

Creating an initial workflow for organizations in service provider deployments on page 32

Uploading a .zip Archive to Modify User Portal Branding

About this task

After you prepare the .zip archive, you can upload it into Equinox Management to enable modifying the User Portal branding.

Note:

Some branding changes can't survive upgrade. The principle is, if you include style.min.css in the branding zip package, the branding can't survive upgrade and must be rebuilt and reuploaded to the User Portal Server after the upgrade. The following is a list of upgrade-safe branding operations:

- Uploading a logo via Avaya Equinox.
- Changing the product name via Avaya Equinox.

- Adding custom HTML via zip branding package.
- Adding HTML translation via zip branding package.
- Adding **custom-styles.css** via zip branding package.
- Adding **powered-by-logo.png** via zip branding package.

The following is a list of branding operations that break the landing portal page after an upgrade:

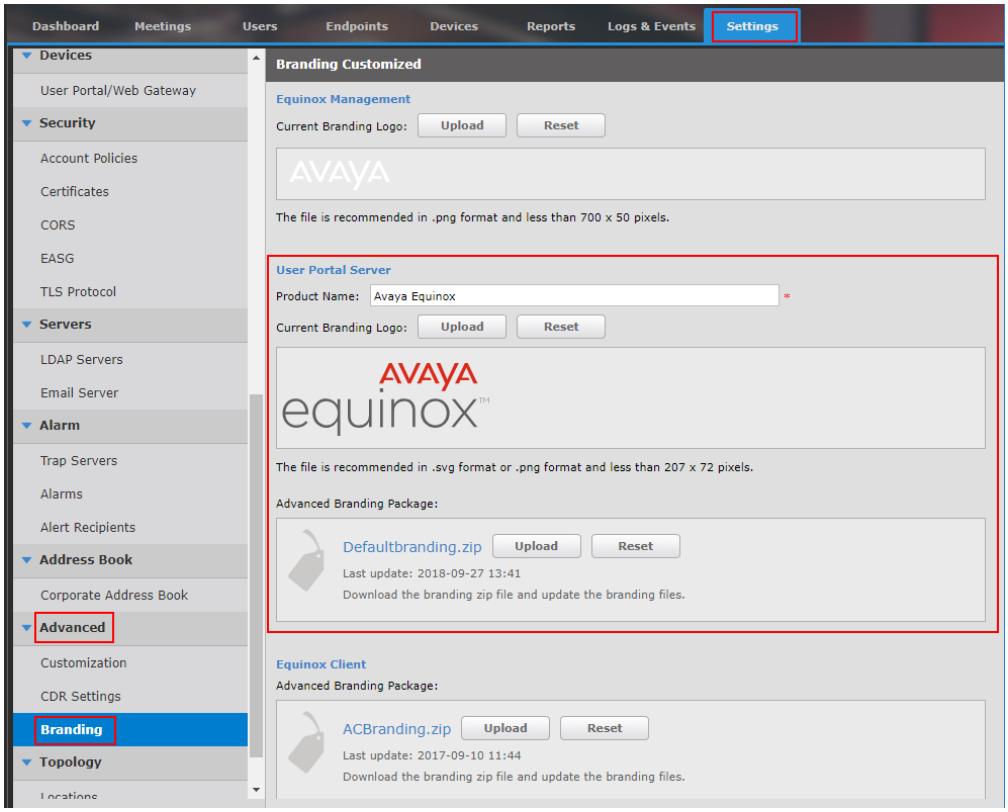
- Changing theme colors via zip branding package (using style.min.css)
- Changing theme logo via zip branding package (using **style.min.css)**
- Changing theme background-image via zip branding package (using **style.min.css)**

Before you begin

Ensure that you have successfully configured a .zip archive with the relevant customized files to be uploaded, as described in Preparing a .zip archive with customized files on page 50.

Procedure

1. Access the Equinox Management administrator portal and log in as tenant admin.
2. Click **Settings** > **Advanced** > **Branding**.
3. In the **User Portal Server** section, enter a name for the User Portal server in the **Product Name** field.
4. In the **Advanced Branding Package** sub-section, click **Upload**.



Related links

Creating an initial workflow for organizations in service provider deployments on page 32

Chapter 2: Defining locations and organizations in your deployment

This section describes how to create locations within your network and, for service providers (multi-tenant), how to add organizations to their deployment. Once you define locations, you can start building your network by adding devices to specific locations.

Locations are where network devices such as gatekeepers, MCUs, endpoints and gateways are placed.

According to the bandwidth threshold defined for each location, Equinox Management can perform least-cost or best-performance allocation of resources.

Important:

Defining locations is relevant only for service providers and administrators of distributed deployments.

Related links

Adding or modifying a location on page 53
Defining bandwidth limits for a location on page 55

Adding or modifying a location

About this task

When configuring your deployment, divide the network into locations. Then, you can start building the infrastructure by adding the network devices, such as gatekeepers, MCUs, gateways, and endpoints to specific locations.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Topology** > **Locations**.
3. Select a location name or click **Add**.

   The system displays the **Add Location** or **Location Profile** page.

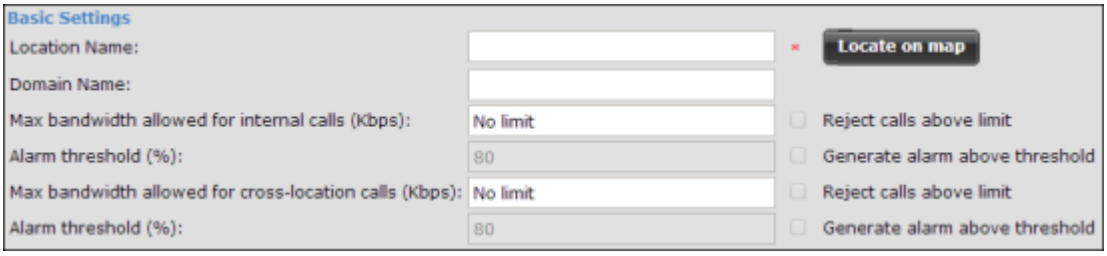


Figure 6: Adding a location

4. Define the location's basic information, as described in Table 5: Adding or modifying a location's basic information on page 54.

Table 5: Adding or modifying a location's basic information

Field Name	Description
Location Name	Define the name used to identify this location. Use the same naming conventions to identify zones when adding gatekeepers to the network. See Adding video network devices in Equinox Management on page 61.
Domain Name	(Optional) If the locations in your deployment have different domain names, enter it for this location. The domain name is useful for identifying the location of SIP endpoints in your network. For example, if an endpoint's SIP URI is `name@domain_name.com`, and this location's domain name is `domain_name`, the SIP endpoint is automatically matched to this location. If no value is specified in this field, the domain specified in the **Default SIP Domain** on the **Meeting Policies** page is used (**Settings** > **Meetings** > **Policies**).
Locate on map	(Optional) Select to display your location on the map. The location is detected from the **Location Name** field, and a flag icon appears to mark the location. If more than one location matches the **Location Name**, select the correct one from the search results.

5. Define the distance and bandwidth thresholds for the location, as described in Defining bandwidth limits for a location on page 55.

Related links

Defining locations and organizations in your deployment on page 53

Defining bandwidth limits for a location

About this task

This procedure is relevant for service providers and administrators of distributed deployments.

You can define the maximum bandwidth for calls across locations, or the bandwidth dedicated to calls within a location.

When calling across locations, you can define the maximum bandwidth usage and set alerts to be triggered if the maximum designated bandwidth is close to being exceeded.

Before you begin

Add the location to your network, as described in Adding or modifying a location on page 53.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Topology** > **Locations**.
3. Click a location in the **Name** column.

   The system displays the **Location Profile** window (Figure 7: Defining bandwidth thresholds for a new office or branch on page 55).

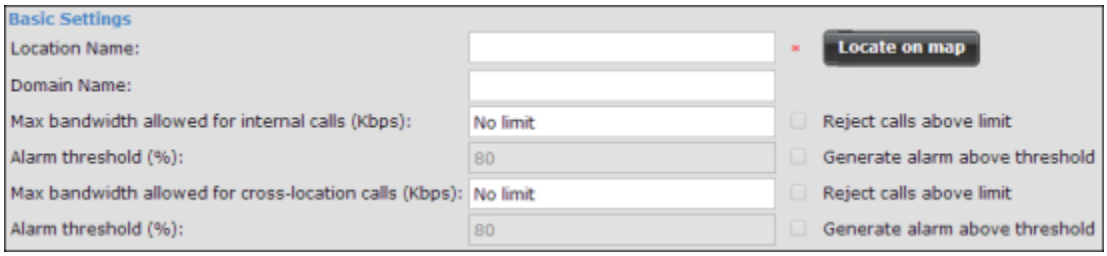


Figure 7: Defining bandwidth thresholds for a new office or branch

4. Enter the information, as described in Table 6: Defining bandwidth settings for a location on page 55.

Table 6: Defining bandwidth settings for a location

Field Name	Description
Max bandwidth allowed for internal calls (Kbps)	Define the total maximum bandwidth for all calls within this location, in kilobits per second.
Max bandwidth allowed for cross-location calls (Kbps)	Define the total maximum bandwidth for all calls between this location and another, in kilobits per second.

Table continues…

Field Name	Description
Reject calls above limit	Select to automatically disallow calls that exceed the defined maximum bandwidth. To automatically reject calls within the office, select the **Reject calls above limit** check box next to **Max bandwidth allowed for internal calls (Kbps)**. To automatically reject calls between offices, select the **Reject calls above limit** check box next to **Max bandwidth allowed for cross-location calls (Kbps)**. If a call is rejected because of bandwidth limits, the system triggers a Call Rejected alert.
Alarm threshold (%)	You can set a system alert when the maximum bandwidth is close to being exceeded. Enter the percentage bandwidth usage that would trigger the BW Utilization alert. The default value is **80%**.

5. Determine what is considered an internal call, and what is considered a cross-location call by defining the location.

   You can modify a rule by selecting the **Modify** button, or delete it by selecting **Delete**.

   a. Set the location rule by selecting **Add** in the **Advanced Settings** area.

      The system displays the **Matching Rule** dialog box.

Figure 8: Defining the rule for your location

   b. Define a location by setting one of the following rules in the **Matching Rule Type** field:

      - Any device with an IP address within a range, for example between 192.168.1.1 and 192.168.1.110.
      - Any device within an IP subnet, for example to specify 192.168.x.x, enter a base IP of 192.168.1.1 and a subnet of 255.255.0.0.
      - An E.164 dialing prefix, for example any call dialled beginning with the prefix 85.

   c. Click **Apply**.

   d. Click the rule to use in the **Matching Rule Type** column, and click **Apply**.

Related links

Defining locations and organizations in your deployment on page 53

Chapter 3: Defining your video network devices

This section provides step-by-step procedures for adding network devices and endpoints, and configuring your videoconferencing network. We recommend that you configure your endpoints and devices according to the workflow described in Device configuration workflow on page 58.

Related links

Device configuration workflow on page 58
Adding video network devices in Equinox Management on page 61
Modifying a network device's location or organization in Equinox Management on page 64
Planning and configuring gatekeepers in Equinox Management on page 65
Planning and configuring media servers in Equinox Management on page 71
Planning and configuring gateways in Equinox Management on page 93
Configuring a UCCS Server in Equinox Management on page 106
Planning and configuring Avaya Session Border Controller for Enterprise (ASBCE) in Equinox Management on page 108
Remotely configuring the Avaya Equinox® H.323 Edge server on page 111
Planning and configuring endpoints in Equinox Management on page 120
Configuring Avaya Equinox® Media Server for WebRTC-based calls in Over The Top deployments on page 174
Configuring Avaya Equinox® Media Server for WebRTC-based calls in Team Engagement deployments on page 175
Planning and configuring streaming and recording servers in Equinox Management on page 176

Device configuration workflow

About this task

This procedure describes the recommended workflow for setting up your video network devices. We recommend first adding all devices to Equinox Management by entering the device's basic information, such as a name to identify the device and its management IP address. This gives you a high-level orientation of your network topology before you configure your devices.

If you are configuring Equinox Management redundancy, deploy the primary server first, referring to component FQDNs rather than IP addresses (for example, *smgmt.company.com*). This reduces maintenance when servers switch to their backups.

After you add each device, Equinox Management connects to it and retrieves additional information. You can then perform advanced configurations, such as defining your gatekeeper's dial plan or synchronizing media server meeting types between multiple media servers.

Important:

Equinox Management retrieves information only from media servers, Avaya gatekeepers, Web Collaboration servers and gateways. You retrieve alarms and traps only from Avaya Equinox® H.323 Edge.

Before you begin

If you have multiple locations in your network, ensure that you define all the locations in Equinox Management before adding devices to the network. For details, see Adding or modifying a location on page 53.

Verify that your network connections are working and you performed the initial installation procedures for the devices (such as setting up the management IP address), as described in the *Deploying Equinox Solution* guide.

Procedure

1. If your deployment includes an external gatekeeper, add it to Equinox Management, as described in Adding video network devices in Equinox Management on page 61.

   Gatekeepers are typically relevant only for distributed or service provider deployments. Add the H.323 Gatekeeper and third-party gatekeepers to which your H.323 endpoints are registered.

2. Add and configure the SIP server. This is necessary if your deployment includes SIP endpoints.

3. Add the following video network devices relevant for your deployment to Equinox Management, as described in Adding video network devices in Equinox Management on page 61:

   - Media servers
   - Avaya Web Collaboration servers
   - Gateways:
     - A Gateway is necessary if your deployment includes ISDN/PTSN endpoints, or standard telephones or mobile phones.
     - Avaya WebRTC Gateway
     - Avaya Recording Gateway
   - Avaya Equinox® H.323 Edge servers are necessary if you require a complete firewall and NAT traversal solution for your H.323 deployment, to enable secure connectivity between enterprise networks and remote sites.
   - Avaya Equinox® Streaming and Recording Servers

- Management Servers
- Desktop Servers
- User Portals
- AADS
- ASBCE

4. Configure each device you added, in the following order:
   a. **Gatekeepers**: See Planning and configuring gatekeepers in Equinox Management on page 65 for details.
   b. **Scopia Elite MCUs and Equinox Media Servers**: See Planning and configuring media servers in Equinox Management on page 71 for details.
   c. **Gateways**: If your deployment includes multiple gateways, you can configure them in any order (see Planning and configuring gateways in Equinox Management on page 93 for details).
   d. **User Portals**: See Configuring user portals in Equinox Management on page 104 for details.
   e. **Avaya Equinox® H.323 Edges**: Necessary if you require a complete firewall and NAT traversal solution for your H.323 deployment, to enable secure connectivity between enterprise networks and remote sites (see Remotely configuring the Avaya Equinox® H.323 Edge server on page 111 for details).

      Adding an Avaya Equinox® H.323 Edge server to Equinox Management is optional. Equinox Management can retrieve alarms and traps from an Avaya Equinox® H.323 Edge server, but cannot manage it.
   f. **Avaya Equinox® Streaming and Recording Server**: See Planning and configuring streaming and recording servers in Equinox Management on page 176 for details.
5. Modify the default password of each device, as follows:
   a. Click **Devices** > **Devices by Location** > **All**. The system displays the **All Devices** page.
   b. Select the relevant device to open the device's **Info** tab.
   c. Click the **Access** tab.
   d. In the **Password** field, modify the password value and click **Apply**.
6. Add and configure the endpoints in your network to Equinox Management. See Planning and configuring endpoints in Equinox Management on page 120 for details.

   Important:

   If you are importing endpoints from an external LDAP server or H.350 search base, define the video users in Equinox Management before you import the endpoints. See Defining and Managing Video Users on page 218 for details.

   You can pre-provision Avaya Room System XT Series endpoints so that customers can receive the endpoint and set it up without the need for technical knowledge or intervention.

See *Deployment Guide for Avaya Room System XT Series*, which is available on the Avaya Support Site.

7. If your deployment includes telepresence endpoints, add and configure these endpoints, as described in Adding Telepresence Systems in Equinox Management on page 132.

   For more information about telepresence systems, see Planning and configuring Telepresence in Equinox Management on page 139.

8. If your deployment includes two Equinox Management servers, configure a redundant server, as described in High Availability of Equinox Management on page 378.

   Once redundancy is configured, the databases on the Equinox Management servers are synchronized with each other.

Related links

Defining your video network devices on page 58

Adding video network devices in Equinox Management

About this task

This section describes how to add or modify the following video network devices in Equinox Management.

If you are configuring Equinox Management redundancy, deploy the primary server first, referring to component FQDNs rather than IP addresses (for example, *smgmt.company.com*). This reduces maintenance when servers switch to their backups.

- (Optional) External gatekeepers: Typically relevant only for distributed or service provider deployments. Add the H.323 or third-party gatekeepers to which your H.323 endpoints are registered.

  Important:

  If your Avaya Equinox® Management uses the internal gatekeeper, you do not need to add it.

- Media Servers
- Avaya Web Collaboration servers for advanced desktop sharing functionality.
- Gateways:
  - A Gateway is necessary if your deployment includes ISDN/PTSN endpoints, or standard telephones or mobile phones.
  - Avaya Web RTC Gateway: Necessary to connect to meetings held on an Elite 6K Media Server, via a web client.
  - Avaya Recording Gateway
- Avaya Equinox® H.323 Edge servers: Necessary if you require a complete firewall and NAT traversal solution for your H.323 deployment, to enable secure connectivity between enterprise networks and remote sites.

- Avaya Equinox® Streaming and Recording Server for advanced recording and streaming functionality.
- UCCS distributed server, used by the Avaya IX™ Workplace Client and web client. The UCCS distributed server enables Equinox Management to handle up to 15,000 concurrent calls.

After you add a device, Equinox Management connects to it and retrieves additional information. You can then configure additional settings for your device, such as managing your bandwidth by using distributed Equinox Media Servers or Scopia Elite MCUs for a single videoconference.

Important:

Equinox Management does not retrieve information from the following devices, so you must configure all device settings when adding them:

- Third-party gatekeepers (configure as described in the steps below)
- Avaya Equinox® H.323 Edge server (configure as described in the steps below)
- SIP servers. For more information, see **Administrator Guide for Avaya Equinox® Management** .

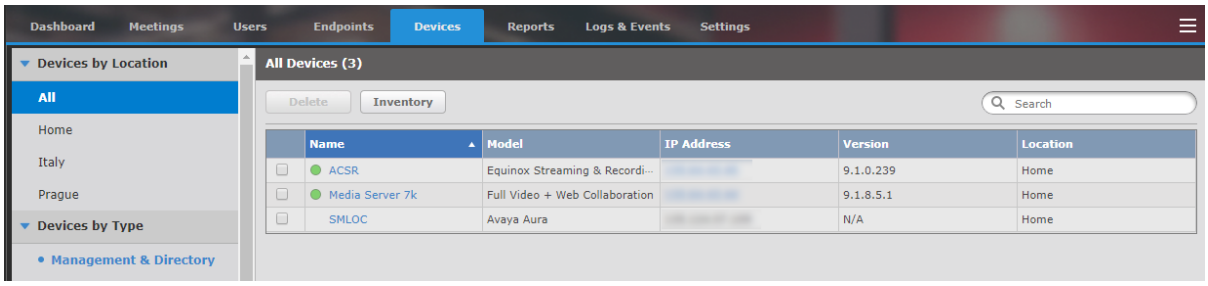
Before you begin

Verify that your network connections are working and you performed the initial installation procedures for the devices (such as setting up the management IP address), as described in the *Deploying Equinox Solution* guide. Add devices in the order listed in Device configuration workflow on page 58.

If you have multiple locations in your network, make sure you have all the locations defined in Equinox Management before adding devices to the network. See Adding or modifying a location on page 53.

Procedure

1. Access the Equinox Management administrator portal.
2. Click the **Devices** tab.



You can generate and export an inventory of the devices in .xlsx CSV format by clicking **Devices by Location** > **All** > **Inventory**.

3. Select the type of device you are adding or modifying, such as Media Server or Gatekeeper, from the list in the sidebar.
4. Do one of the following:
   - To add the device, click **Add**.

- To modify the basic attributes of the device, click the link of the device in the **Name** column, and click the **Configure** tab (if present).

5. Enter or modify the basic settings for your device, as described in Table 7: Configuring your device's basic settings on page 63. Equinox Management then connects to the devices and retrieves additional information, such as the version number.

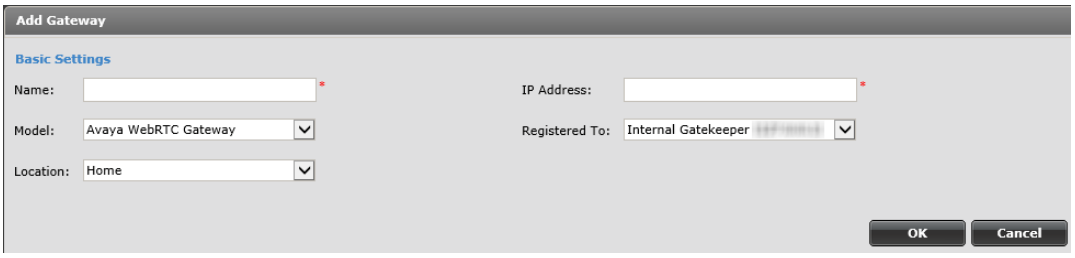


Table 7: Configuring your device's basic settings

Field Name	Description
Name	Enter the name used to identify the device. This name will be displayed in the list of devices.
IP Address	Enter the device's management IP address, as configured during device installation.
Model	This field is necessary only when adding gatekeepers and gateways: • If adding a gatekeeper profile, select the gatekeeper's vendor and model from the list. • If adding a gateway profile, select the gateway type from the list.
Registered To	(For Equinox Media Servers, Scopia Elite MCUs, and Gateways only) Select the gatekeeper to which the device is registered to from the list. If you select **None**, the device can be added to Equinox Management but will not be connected until you register the device with the gatekeeper, and select the gatekeeper here.
Location	This is relevant only for service providers or deployments with multiple locations. Select the device's location.

6. If you are adding or modifying a third-party gatekeeper, enter the additional fields as described in Table 8: Configuring a third-party gatekeeper on page 64.

Table 8: Configuring a third-party gatekeeper

Field Name	Description
Login Name **Login Password**	Enter the username and password required to access the gatekeeper's web interface.
Strip Prefixes	Select for a gatekeeper that is configured to remove zone prefixes.
Zone Prefix	Enter the zone prefix that matches the configuration of the gatekeeper.

7. Configure your devices in the following order, depending on which devices are included in your deployment (after initial configuration, you can modify the devices in any order):
   a. Gatekeepers (see Planning and configuring gatekeepers in Equinox Management on page 65 for details)
   b. Equinox Media Servers or Scopia Elite MCUs (see Planning and configuring media servers in Equinox Management on page 71 for details)
   c. Avaya Equinox® H.323 Edge (see Remotely configuring the Avaya Equinox® H.323 Edge server on page 111 for details)
   d. Equinox Streaming and Recording Server (see Planning and configuring streaming and recording servers in Equinox Management on page 176 for details)

Related links

Defining your video network devices on page 58

Modifying a network device's location or organization in Equinox Management

About this task

This procedure is relevant for service providers and administrators of a distributed deployment.

Once a device is added to Equinox Management, you can modify its location (or organization, in service provider deployments), according to your network requirements and topology.

A location is a physical space (building) or a network (subnet) where video devices can share a single set of addresses. A distributed deployment places these components in different locations, often connected via a VPN.

Procedure

1. Access the Equinox Management administrator portal.
2. Click the **Devices** tab.
3. Select the device type under **Devices by Type**.

4. Click the link in the **Name** column for the device you want to configure.
5. If the system displays the **Info** tab, click the **Configure** tab.
6. Select the device's location from the **Location** list.
7. Click **OK** to save your changes.

Related links

Defining your video network devices on page 58

Planning and configuring gatekeepers in Equinox Management

You can use the following types of gatekeepers in Equinox Management:

- Avaya Equinox H.323 Gatekeeper: Equinox Management's built-in gatekeeper, which can be used to manage and route endpoint-initiated calls and point-to-point calls. For more information, see About the Equinox Management's internal gatekeeper on page 65. You do not need to manually add Avaya Equinox H.323 Gatekeeper in Equinox Management.
- H.323 Gatekeeper or Third-Party Gatekeepers: Gatekeepers are typically only used in service provider and other large capacity deployments. You need to define these gatekeepers in Equinox Management, as described in Adding video network devices in Equinox Management on page 61.

Once defined, you can register your devices and endpoints to the gatekeeper. You can only manage H.323 Gatekeeper and Avaya Equinox H.323 Gatekeeper via Equinox Management, for example, by modifying the dial plan.

Related links

Defining your video network devices on page 58
About the Equinox Management's internal gatekeeper on page 65
Defining the gatekeeper's dial plan in Avaya Equinox® Management on page 67
Configuring a stand-alone H.323 Gatekeeper on page 70

About the Equinox Management's internal gatekeeper

Equinox Management is shipped with a built-in gatekeeper, Avaya Equinox H.323 Gatekeeper, which can be used to manage and route endpoint-initiated calls and point-to-point calls.

Gatekeepers are similar to a PBX for an IP video network. After you register the network devices with Equinox Management's internal gatekeeper, it can perform a number of key functions, including:

- Translate the alias of an address to its actual IP address. There are three types of aliases:
  - E.164 aliases are numeric addresses representing the endpoint, like a phone number.
  - H.323 aliases are alphanumeric addresses that represent endpoints, like 'user_endpoint'.
  - URI aliases are similar to email addresses, like 'user@companyname.com'.

  In each case, the gatekeeper translates the alias into its corresponding IP address and routes the call successfully.
- Negotiate the connecting and disconnecting of calls.
- Implement an organization's dial plan. A dial plan is the set of call routing rules based on the pre-defined prefixes of a number. The format can determine the location and/or the services you want.

  The most common example of a dial plan comes from the traditional telephony world, where locations are determined by the format of the phone number:
  - Numbers which do not begin with a zero are local calls.
  - Numbers starting with a single zero denote an inter-city call.
  - Numbers starting with a double-zero indicate an international call.

  Similarly, a gatekeeper can be configured to determine locations in an organization's dial plan. For example, all numbers beginning with *5*might be located in Europe, *6* routes to the west coast of the US, *7* to the east coast, and so on.

  In addition to locations, gatekeepers can also invoke services from a number format (dial plan). For example, a number beginning with *88* might be chosen to access a person's video virtual room.

Avaya Equinox H.323 Gatekeeper supplies the correct destination IP and authorizes the appropriate bandwidth for the call. In this way, Equinox Management can manage endpoint-initiated calls and point-to-point calls.

MCUs, gateways, and endpoints can be registered with the Equinox Management's internal gatekeeper.

Equinox Management can also work with the standalone H.323 Gatekeeper or third-party gatekeepers when they are configured as neighbors to its internal gatekeeper, including the Cisco IOS H.323 Gatekeeper and the Tandberg (Cisco) Video Communications Server (VCS). Only endpoints can be registered to a third-party gatekeeper.

Related links

Planning and configuring gatekeepers in Equinox Management on page 65

Defining the gatekeeper's dial plan in Avaya Equinox® Management

About this task

A dial plan is the set of call routing rules based on pre-defined number prefixes. The number prefixes are used to determine the location and/or the services a user needs.

An organization's dial plan must be implemented in Avaya Equinox® Management and also configured in any standalone gatekeepers to ensure that it is managed effectively.

The most common example of a dial plan comes from the traditional telephony world, where locations are determined by the format of the phone number:

- Numbers which do not begin with a zero are local calls.
- Numbers starting with a single zero denote an inter-city call.
- Numbers starting with a double-zero indicate an international call.

Similarly, a gatekeeper can be configured to determine locations in an organization's dial plan. For example, all numbers beginning with *5* might be located in Europe, *6* routes to the west coast of the US, *7* to the east coast, and so on.

In addition to locations, gatekeepers can also invoke services from a number format (dial plan). For example, a number beginning with *88* might be chosen to access a person's video virtual room.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **System Preference** > **Local Services**.

   The system displays the **Local Services** page.

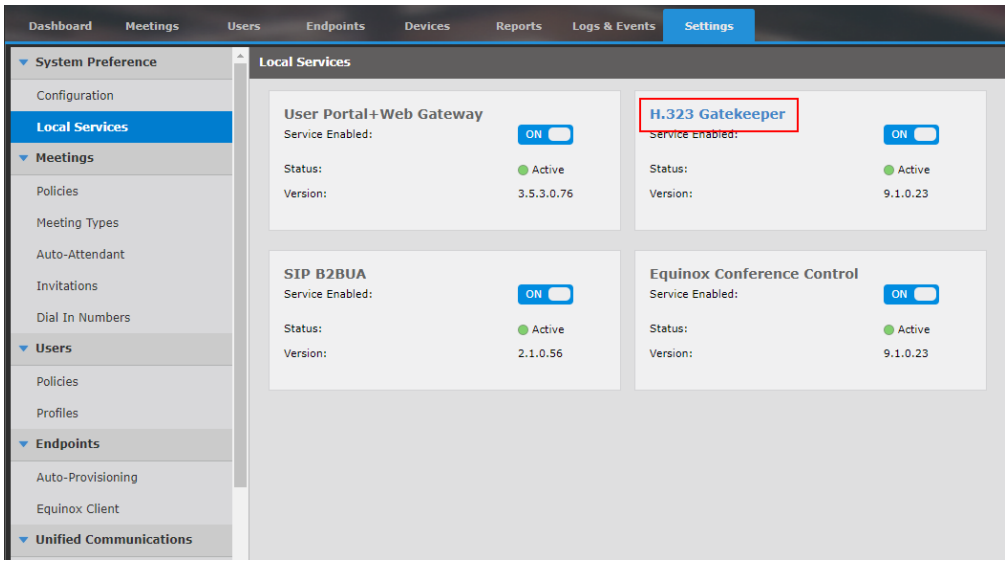


Figure 9: Local Services page

3. Click the **H.323 Gatekeeper** link.

   The system displays the gatekeeper's information page.

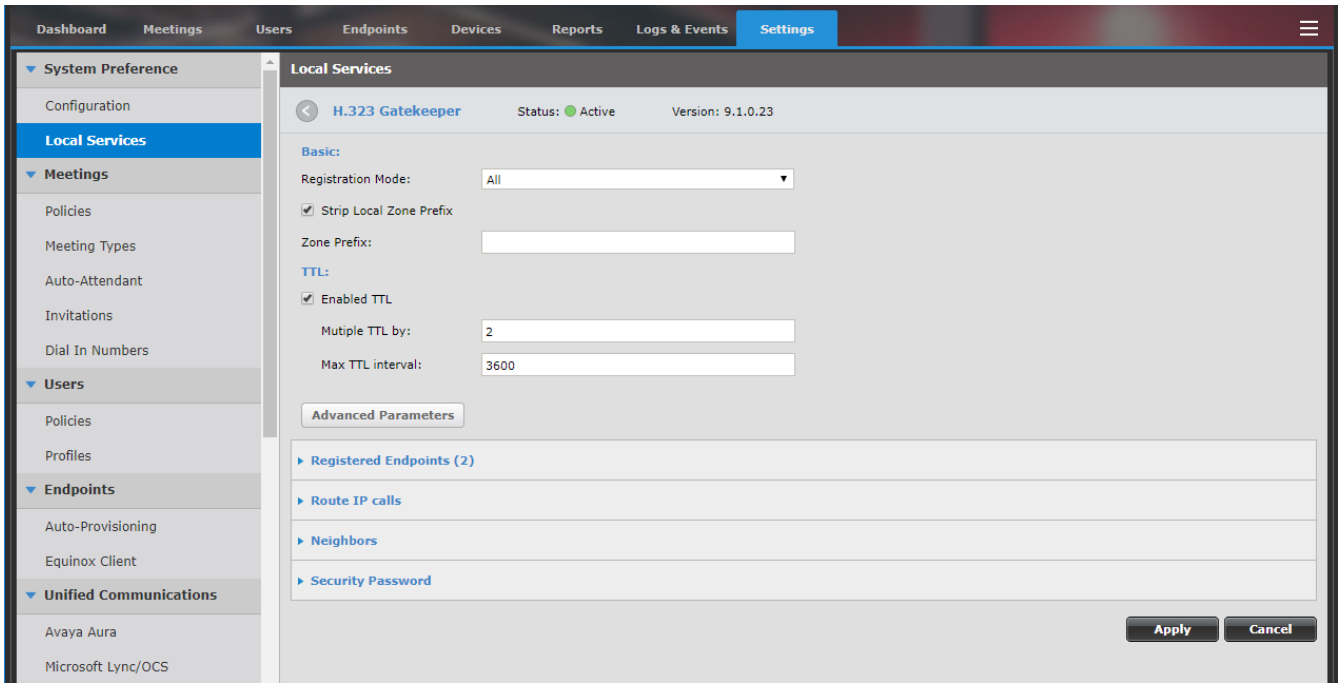


Figure 10: H.323 Gatekeeper Information page

4. Configure the fields on the page, as described in the following table:

Table 9: Configuring the H.323 Gatekeeper settings

Section Name	Field Name	Description
Basic	**Registration Mode**	Select the mode by which endpoints can register with the H.323 Gatekeeper: • **All**: Any endpoint can register with the H.323 Gatekeeper. • **None**: No endpoint can register with the H.323 Gatekeeper. • **Predefined**: Only Equinox Management endpoints can register with the H.323 Gatekeeper.
	Strip Zone Local Prefix	Select to remove the local zone prefix when calling the endpoint.
	Zone Prefix	A number which the endpoint uses as a prefix before dialing another endpoint.
TTL	**Enabled TTL**	Select to require the endpoint to re-register with the H.323 Gatekeeper when the endpoint's Time-To-Live (TTL) setting expires.

Table continues…

Section Name	Field Name	Description
	Multiple TTL by	Increases the length of time that the H.323 Gatekeeper waits for TTL expiration before an endpoint is unregistered. Enter an integer between 1–100 to indicate the factor by which you want to multiply the endpoint's TTL value. Default value = **2** The length of time that the H.323 Gatekeeper waits for TTL expiration before unregistering the endpoint is determined as follows: *(endpoint TTL) * (value entered in **Multiple TTL by** field) + 20 seconds* **Note:** If you modify either the **Enabled TTL** check box or the **Multiple TTL by** field after an endpoint has registered to the H.323 Gatekeeper, the H.323 Gatekeeper implements the new values only after the endpoint re-registers.
	Max TTL interval	The maximum amount of time (in seconds) that the H.323 Gatekeeper can wait for TTL expiration before unregistering the endpoint. Default value = **3600**
Registered Endpoints		Displays the list of endpoints that are registered to the H.323 Gatekeeper.
Route IP Calls	**Route IP Calls to Equinox H.323 EdgeServer**	Select to route IP calls to the Equinox H.323 Edge server. When selecting this check box, select the **Add** button and enter the IP Address and Port through which you want to route calls.
Neighbors	**Prefix**	The prefix of the neighboring H.323 Gatekeeper.
	IP Address	The IP address of the neighboring H.323 Gatekeeper.
	Port	The port of the neighboring H.323 Gatekeeper.
	Description	A description of the neighboring H.323 Gatekeeper.
Security Password	**Enable Security (H.235)**	Select to allow only a password-specified endpoint to register with the H.323 Gatekeeper. When this check box is cleared, any endpoint can register with the H.323 Gatekeeper.

5. Click **Apply** to save your changes.

Related links

Planning and configuring gatekeepers in Equinox Management on page 65

Configuring a stand-alone H.323 Gatekeeper

About this task

This procedure explains how to configure a stand-alone H.323 Gatekeeper.

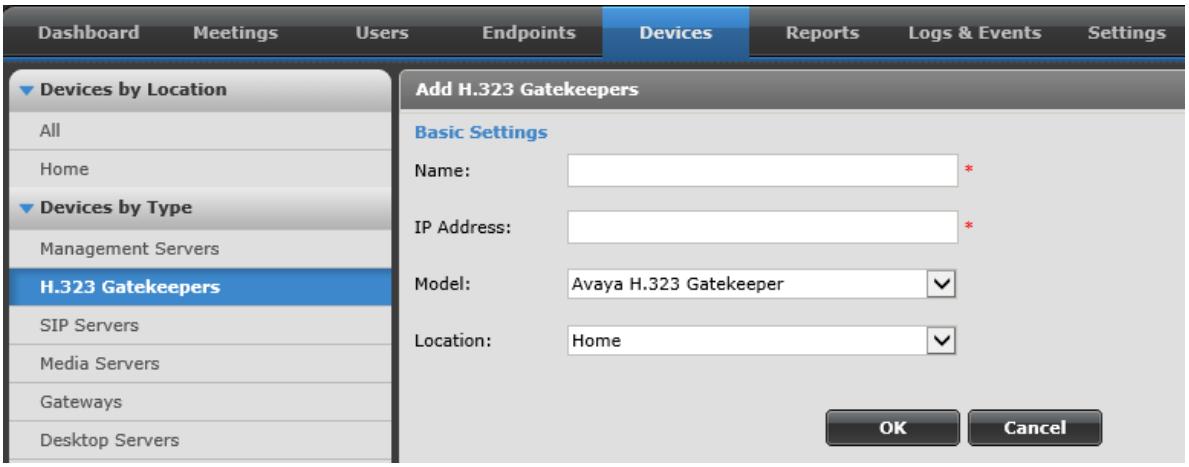
Procedure

1. In an Equinox Management environment, click **Devices** > **Devices by Type** > **H.323 Gatekeepers**.

   The system displays the **H.323 Gatekeepers** page.

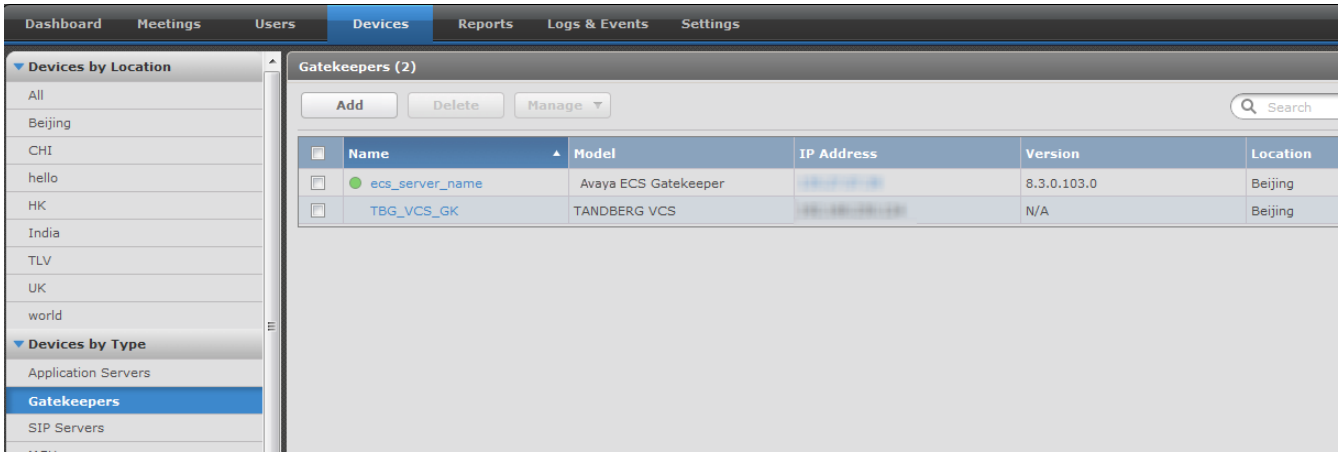
2. Click **Add** to add a new ECS Gatekeeper.

   The system displays the **Add H.323 Gatekeepers** page.



3. Configure the displayed fields and click **OK**.

   The system displays the configured gatekeeper on the **Gatekeepers** page.



If the gatekeeper is configured correctly, a green icon appears next to the gatekeeper. If no green icon appears, verify that the following services have been started on the specified machine:

- Avaya Enhanced Communication Server
- Avaya Enhanced Communication Server Watchdog
- Avaya Enhanced Communication Server Web Server

Related links

Planning and configuring gatekeepers in Equinox Management on page 65

Planning and configuring media servers in Equinox Management

An Avaya Equinox Media Server (AEMS) is a virtual or physical appliance that hosts videoconferences between multiple endpoints, both H.323 and SIP. AEMS are added to a specific organization or branch, according to pre-defined network topology. For more information about adding the AEMS and other devices to Equinox Management, see Adding video network devices in Equinox Management on page 61.

After adding your media servers profile, you can use Equinox Management to reserve resources, schedule conferences, and control in-session meetings.

This section describes how to modify media server settings in Equinox Management and configure meeting types.

Related links

Defining your video network devices on page 58
Configuring the media server from Equinox Management on page 71
Downloading media server meeting yypes to Equinox Management on page 75
Increasing MCU capacity by cascading multiple MCUs on page 85
Enabling Auto-Attendant support on page 88
Integrating the Avaya Aura Conferencing server on page 91

Configuring the media server from Equinox Management

About this task

This procedure describes how to modify and configure your media server settings, such as the media server's location and registered gatekeeper.

Before you begin

Add the media server to Equinox Management by entering its basic settings, as described in Adding video network devices in Equinox Management on page 61.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Devices** > **Devices by Type** > **Media Servers**.
3. Click the link of the media server you want to modify in the **Name** column.

   The system displays the **Equinox Media Server** page.
4. Click the **Configuration** tab to configure your media server settings, as described in Table 10: Configuring your media server on page 72.

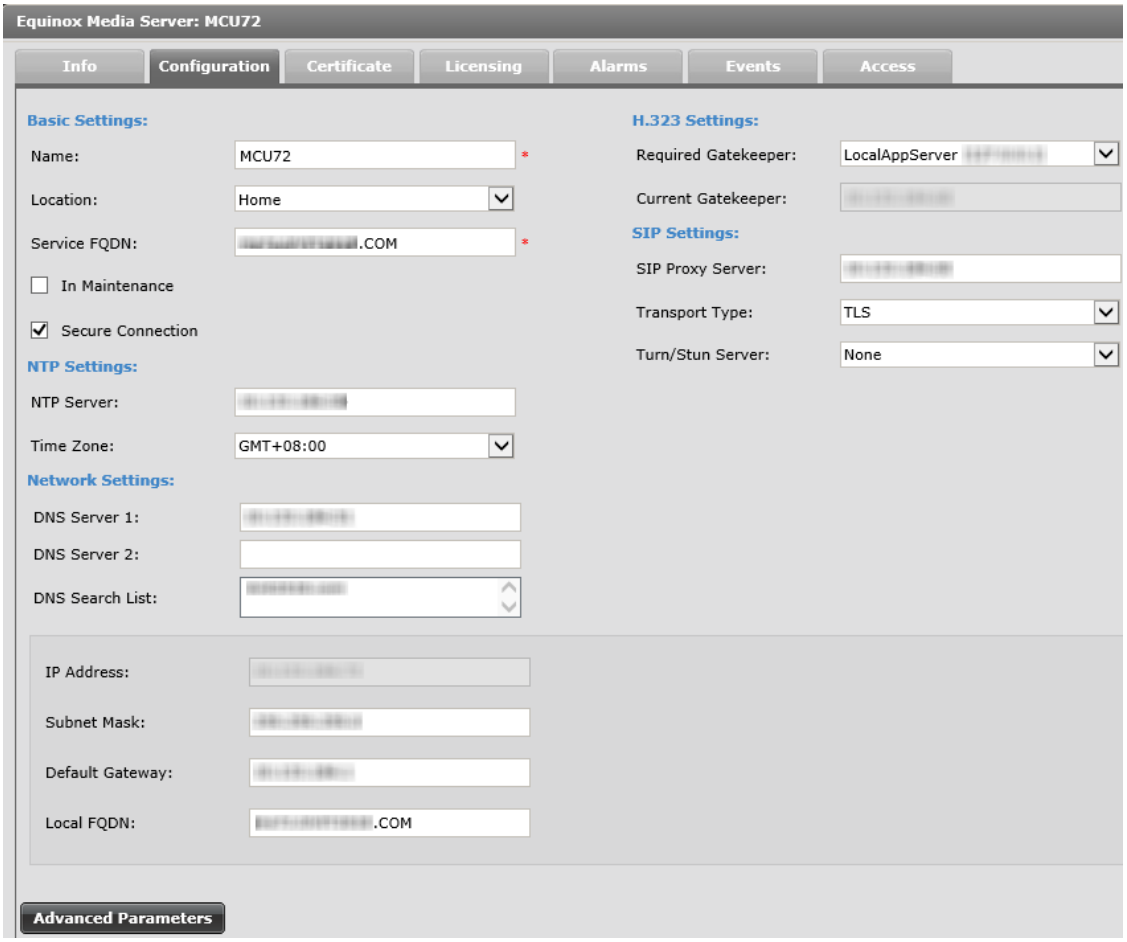


Table 10: Configuring your media server

Section	Field Name	Description
Basic Settings	**Name**	You can modify the name used to identify the media server. This is the name displayed in the list of media servers.

Table continues…

Section	Field Name	Description
	Location	This is relevant only for service providers or deployments with multiple locations. You can modify the media server's location.
	Security	Displayed only for an MCU 6K device. Select the security level for the device: • **Standard** • **High** • **Maximum** • **Locked**
	Service FQDN	Enter the fully qualified domain name (FQDN) of the service.
	In Maintenance	Select if the media server is currently being upgraded or in repair. If this option is selected, you can still configure settings and perform upgrades, but this media server cannot be used to host videoconferences.
	Secure connection	Select to secure access to the media server web interface. You can do this only if you installed certificates for the media server, either from Equinox Management or from the media server interface (see *Administrator Guide for the Scopia Elite MCU*).
	Master Media Server for Cascading	Select to set the specified server as the master server when cascading is enabled. When the option is not selected, the media server appears on the **Devices** page with an icon indicating that it can be designated only as a slave media server during cascading.
NTP Settings	**NTP Server**	The IP Address of the NTP server
	Time Zone	The time zone in which the NTP server is located
Network Settings	**DNS Server 1**	The IP Address of the DNS server
	DNS Server 2	The IP Address of the backup DNS server, in the event that DNS Server 1 is not available
	DNS Search List	Enter the short name of the DNS server when the media server searches other sites; The system searches the DNS search list for the suffix.

Table continues…

Section	Field Name	Description
	IP Address	The IP Address of the media server **Note:** When the device is online, you can change its IP address in this field.
	Subnet Mask	The subnet mask of the media server
	Default Gateway	The default gateway of the media server
	Local FQDN	The fully qualified domain name (FQDN) of the local media server
H.323 Settings	**Required Gatekeeper**	The gatekeeper to which you want to register the media server
	Current Gatekeeper	This (read-only) field displays the management IP address of the gatekeeper this media server is currently registered to. In most cases, this is the same gatekeeper selected in the **Required Gatekeeper** field. If the current gatekeeper is not the same as the gatekeeper configured in the **Required Gatekeeper** field, an alarm is issued by Equinox Management.
SIP Settings	**SIP Proxy Server**	The IP Address of the SIP Proxy Server
	Transport Type	The enabled transport type
	Turn/Stun Server	Select the Turn/Stun Server, used for the Avaya Session Border Controller for Enterprise (ASBCE).

Optionally, click **Advanced Parameters** to configure advanced parameters for the media server.

5. Click the **Access** tab and enter the media server's information, as described in Table 11: Configuring the media server's access information on page 74.

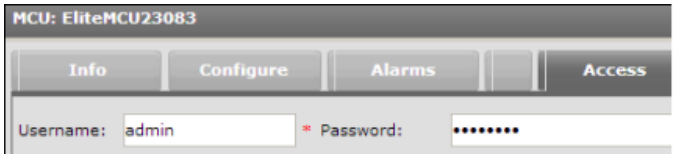


Table 11: Configuring the media server's access information

Field Name	Description
Username **Password**	Enter the login username and password of the media server web interface login.

6. Click **Apply** to save your changes.

Related links

Planning and configuring media servers in Equinox Management on page 71

Downloading media server meeting yypes to Equinox Management

You define media server meeting types in the MCU (see *Administrator Guide for Scopia Elite MCU*), and then download them to Equinox Management. When meeting operators, meeting organizers, and users schedule a videoconference, they determine its characteristics by assigning a meeting type. You can create and customize the meeting types depending on the specific needs of your organization.

Meeting types (also known as MCU/Media Server services) are meeting templates which determine the core characteristics of a meeting. For example, they determine if the meeting is audio only or audio and video, they determine the default video layout, the type of encryption, PIN protection and many other features. You can invoke a meeting type by dialing its prefix in front of the meeting ID. Meeting types are created and stored in the Avaya Equinox® Media Server, with additional properties in Equinox Management.

You can also define additional properties specific to Equinox Management functionality. These are used by Equinox Management only, and do not need to be synchronized with the media server.

When you have more than one media server in your deployment, you first define meeting types only on one of them so that it serves as a reference media server. You then add the meeting types to Equinox Management and distribute them from the reference media server to other media servers, as shown in Figure 11: Synchronizing meeting types on page 75.

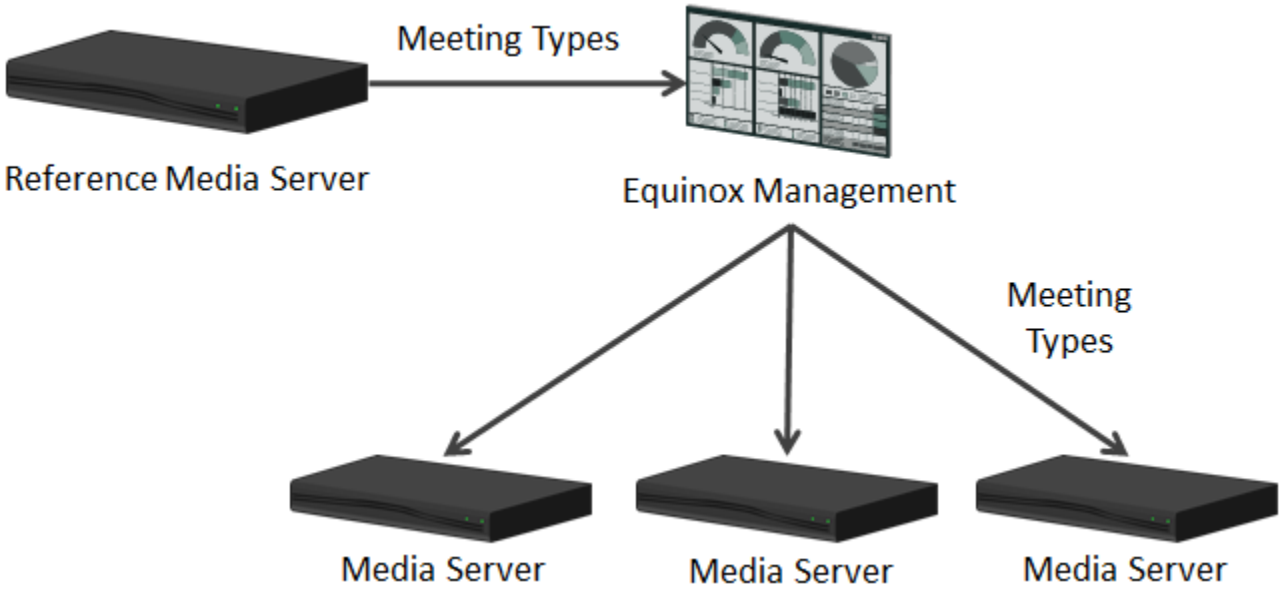


Figure 11: Synchronizing meeting types

In addition to Media Server meeting types, Equinox Management comes with a built-in meeting type for point-to-point meetings, which bypasses Media Servers. It is used only when one endpoint dials another endpoint directly. You cannot delete this built-in meeting type, and can modify its default bandwidth only.

This section explains how to manage media server meeting types in Equinox Management.

Important:

In service provider (multi-tenant) deployments, the system administrator of the service provider manages meeting types. Customers of service providers cannot modify or manage these settings.

Related links

Planning and configuring media servers in Equinox Management on page 71
Synchronizing media server meeting types with Equinox Management on page 76
Defining a default and fallback meeting type on page 79
Configuring recording expiration on page 80
Modifying a media server meeting type in Equinox Management on page 81
Searching for a meeting type on page 84
Deleting a meeting type from Equinox Management on page 84

Synchronizing media server meeting types with Equinox Management

About this task

This procedure describes how to download media server meeting types to Equinox Management and then, if relevant for your deployment, synchronize the meeting types among multiple media servers. Meeting types (also known as MCU/Media Server services) are meeting templates which determine the core characteristics of a meeting.

Once you download the meeting types to Equinox Management:

- Meeting operators, meeting organizers, and users can assign a meeting type when scheduling a videoconference.
- You can specify which users have access to certain meeting types (see Creating or modifying a user profile on page 221). For example, you can allow a VIP user to schedule meetings with a higher maximum bandwidth for better quality.
- For deployments with multiple media servers, you can propagate meeting types from the reference media server to all other media servers across your organization (Figure 12: Synchronizing meeting types across media servers on page 77), as described in the procedure below.

  If your deployment includes both Scopia Elite MCUs and media servers, you define and synchronize their meeting types separately during the same synchronization procedure, making sure that prefixes and names of the meeting types are unique. For example, if there is a Scopia Elite MCU meeting type with the prefix 70, there cannot be a Scopia Elite MCU meeting type with the same prefix.

  If you later add or remove meeting types on the reference media server, or you want to change the reference media server, you need to re-synchronize the meeting types.

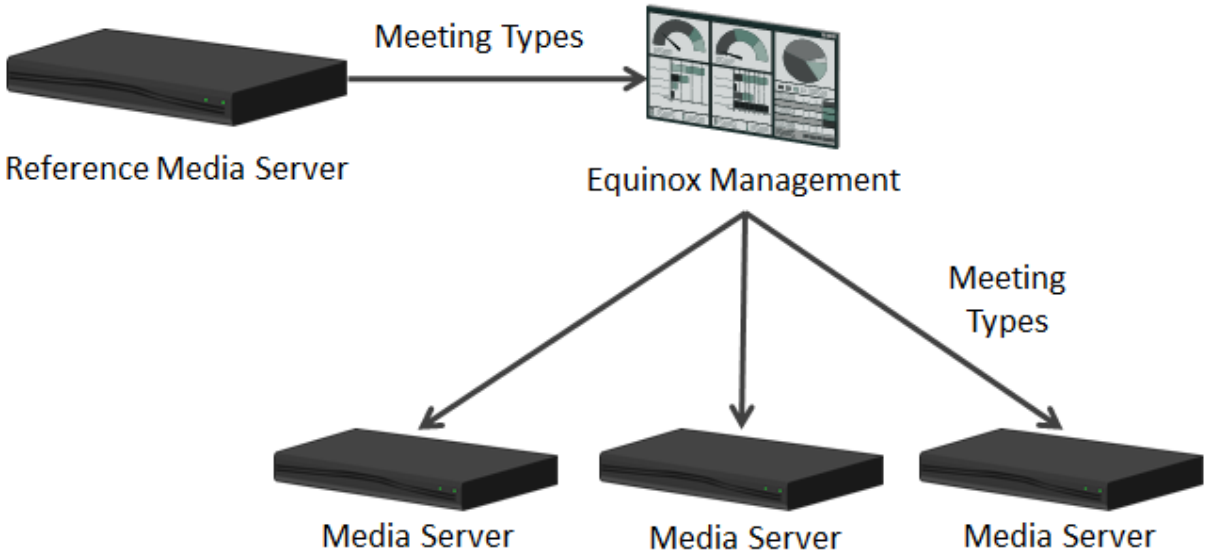


Figure 12: Synchronizing meeting types across media servers

- If you modify a meeting type setting in the media server, you need to re-synchronize the meeting types with media server.

Before you begin

If you have multiple media servers in your deployment, decide which media server you would like to use as a reference for other media servers, and verify that all meeting types are defined on your reference media server. To create media server meeting types, see *Administration Guide for Scopia Elite MCU*.

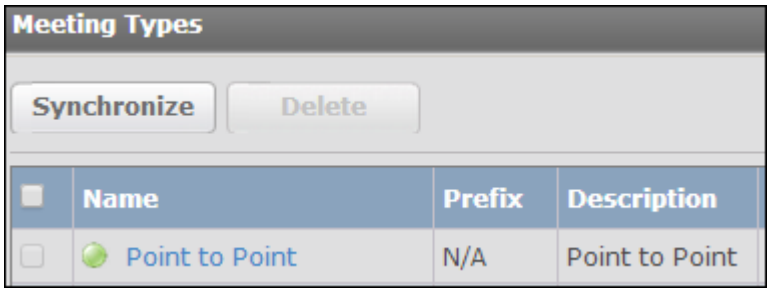
Ensure that the virtual meeting ID prefix is not the same as the prefix for the MCU meeting type, ECS zone, or other prefixes. If the prefix is the same you cannot successfully use a different language in your meeting invitation than the one selected in the virtual room.

Procedure

1. Access the Equinox Management administrator portal.
2. Click the **Settings** tab.

   The system displays the **Meeting Types** page.

   If this is the first time you are synchronizing, the system only displays the Equinox Management's built-in meeting type.



3. Click **Synchronize**.

   The system displays the **Meeting Type Synchronization** page.

4. For deployments with one media server, verify that the names of the meeting types are correct and click **Confirm**.

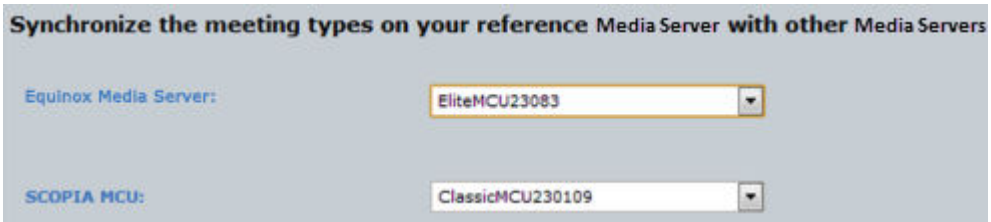
   The meeting types are now downloaded to Equinox Management and appear in the list of meeting types.

5. For deployments with multiple media servers:

   a. Select the media server to use as a reference for other media servers of that type, from the lists.

      Important:

      You can only synchronize Scopia Elite MCUs with other Scopia Elite MCUs, and non-Scopia Elite MCUs with other non-Scopia Elite MCUs. If you have both types of MCUs in your deployment, select a reference for each MCU type.

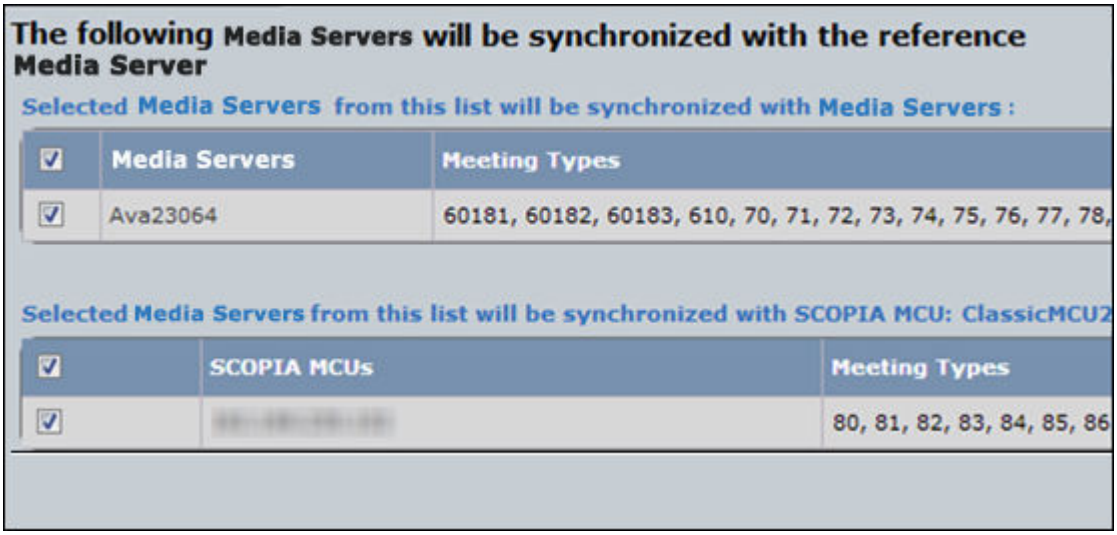


   b. Click **Next**.

   c. Select the media servers to be synchronized. By default, all media servers of that type are selected.

      Important:

      Make sure the media servers support the meeting types being uploaded. For example, you cannot upload a meeting type defined to support High Definition Continuous Presence (HDCP) conferences to a media server that is not enabled for HDCP.



d. Click **Next**.

e. Verify that the meeting type names and prefixes in the list are correct and unique.

   For example, if there is a Scopia Elite MCU meeting type with the prefix *70*, there cannot be a Scopia Elite MCU meeting type with the same prefix. In this case, modify the prefix to avoid clashes.

f. Click **Confirm**.

   The media server's meeting types are now synchronized across the selected media servers.

Related links

Downloading media server meeting yypes to Equinox Management on page 75

Defining a default and fallback meeting type

About this task

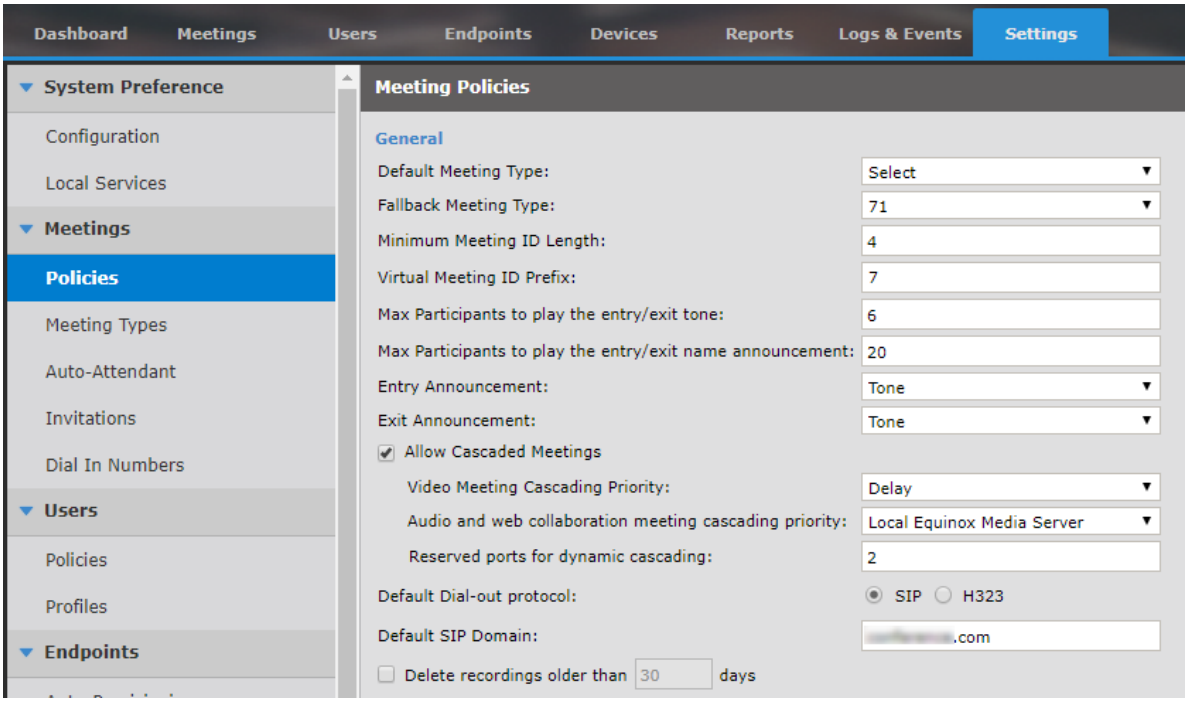
Meeting types (also known as MCU/Media Server services) are meeting templates which determine the core characteristics of a meeting. A default meeting type defines the initial settings of the default meeting type in the **Meeting Scheduling** window when creating a new scheduled meeting both from the Equinox Management user portal or when initiating a meeting from an endpoint.

Avaya Equinox® Management uses a fallback meeting type when it cannot create an ad-hoc meeting due to lack of resources. For example, if a user wants to start an ad-hoc meeting from the endpoint, Avaya Equinox® Management first tries to create a meeting using the default meeting type, and if resources are unavailable, it uses the fallback meeting type.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Meetings** > **Policies**.

   The system displays the **Meetings Policies** page.



3. Select a default meeting type from the **Default Meeting Type** list.

   We recommend that you select a default meeting type which is available to all users.

4. Select a meeting type from the **Fallback Meeting Type** list, to be used if the default meeting type is unavailable.

5. Click **Apply** to save your changes.

   Note:

   Select the default dial-out protocol for meetings in the **Default Dial-out protocol** field, either **SIP** or **H323**.

Related links

Downloading media server meeting yypes to Equinox Management on page 75

Configuring recording expiration

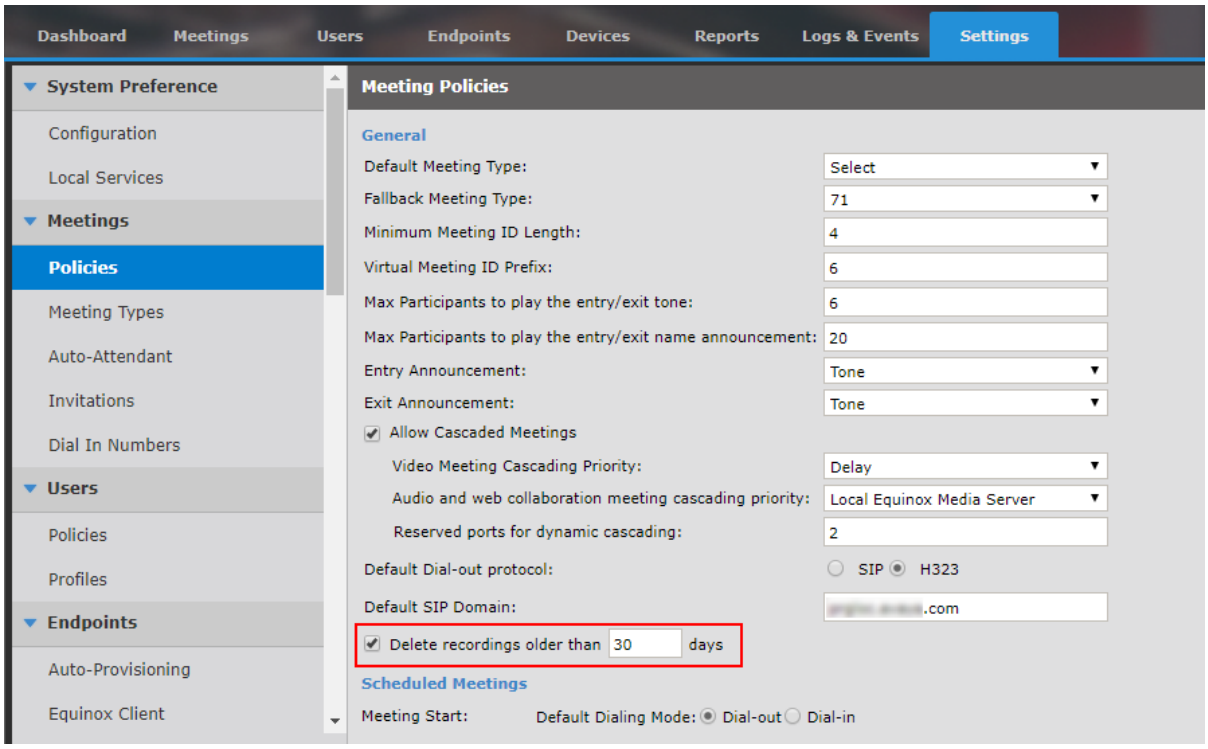
About this task

You can configure the number of days after which Equinox Management deletes conference recordings from the system. This feature enables you to conserve space in your system by deleting old recordings which are no longer needed. It also enables you to set a retention policy so as to help you comply with the GDPR guidance of not keeping data containing personal user information for longer than necessary. The number of days are counted from the date of the recording.

Procedure

1. In the Equinox Management administrator portal, click **Settings** > **Meetings** > **Policies**.

The system displays the **Meeting Policies** page.



2. Select the **Delete recordings older than** check box and enter the number of days after which you want Equinox Management to delete conference recordings from the system.

   If the check box is not selected, Equinox Management deletes recordings after 30 days, as per the GDPR recommendation.

Related links

Downloading media server meeting yypes to Equinox Management on page 75

Modifying a media server meeting type in Equinox Management

About this task

You can modify an existing Media Server meeting type in Equinox Management by defining the properties specific to Equinox Management functionality. For example, you can modify the default bandwidth (bitrate) that undefined endpoints use when connecting to a videoconference. Bitrate is the speed of data flow. Higher video resolutions require higher bitrates to ensure the video is constantly updated, thereby maintaining smooth motion.

Other properties that are defined on the Media Server, such as the prefix of the meeting type, can only be modified on Media Server.

In addition to Media Server meeting types, Equinox Management comes with a built-in meeting type for point-to-point meetings, which bypasses Media Servers. It is used only when one endpoint dials another endpoint directly. You cannot delete this built-in meeting type, and can modify its default bandwidth only.

Before you begin

To enable support for connecting to the Avaya Aura® Conferencing server, you must first integrate it with Equinox Solution.

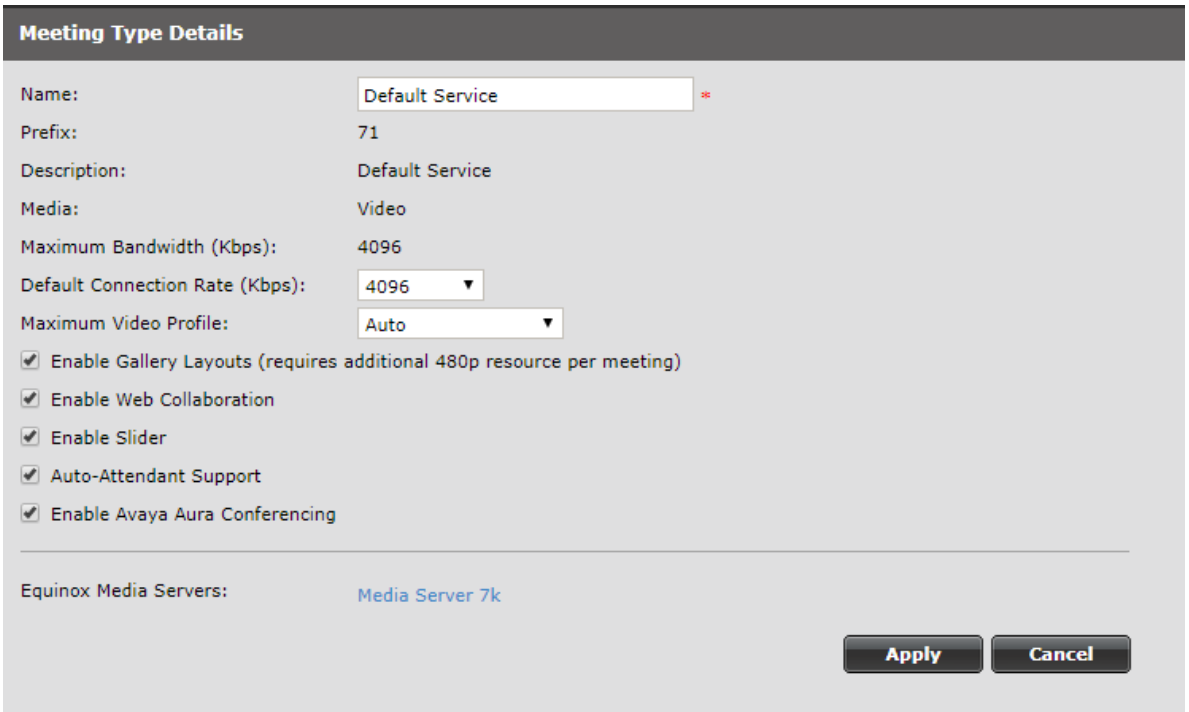
For more information, see Integrating the Avaya Aura Conferencing server on page 91.

Ensure that the virtual meeting ID prefix is not the same as the prefix for the MCU meeting type, ECS zone, or other prefixes. If the prefix is the same you cannot successfully use a different language in your meeting invitation than the one selected in the virtual room.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Meetings** > **Meeting Types**.
3. Click the link in the **Name** column for the meeting type you require.

   The system displays the **Meeting Type Details** page, displaying all the properties available for this specific meeting type.



   For descriptions of the parameters, see Meeting type parameters descriptions on page 82.

4. Click **Apply** to save your changes.

Related links

Downloading media server meeting yypes to Equinox Management on page 75
Meeting type parameters descriptions on page 82

Meeting type parameters descriptions

Parameter Name	Description
Name	Displays the name of the meeting type, as defined in Equinox Management. MCUs do not give names to meeting types. You can enter a new name if necessary.
Prefix	Displays the dial prefix for this meeting type. A dial prefix is a number added at the beginning of a dial string to route it to the correct destination, or to determine the type of call. The meeting type prefix is downloaded from the MCU and cannot be changed in Equinox Management.
Description	Displays the meeting type description, downloaded from the MCU.
Media	Displays the type of media available for this meeting type, downloaded from the MCU: • **Audio only**: The system displays no video (either from participants or a presentation), to conserve bandwidth and MCU resources. • **Video**: High Definition (HD) video, the default value for meeting types. • **Video (Switched HD)**: The system displays only one participant at a time to conserve bandwidth. • **Video (Desktop)**: Video at a lower resolution (CIF), doubling the MCU capacity (Scopia Elite MCU only).
Maximum Bandwidth (Kbps)	Displays the maximum meeting bandwidth (bitrate) between an endpoint and the MCU when using this meeting type, downloaded from the MCU.
Default Connection Rate (Kbps)	Specifies the default bandwidth (bitrate) for this meeting type, used for any endpoints that are not defined in Equinox Management, and are invited without specifying the bandwidth. The default bandwidth must be equal to or less than the **Maximum Bandwidth**. Kilobits per second (kbps) is the standard unit to measure bitrate, measuring the throughput of data communication between two devices. You can also specify the bandwidth for an endpoint when scheduling the meeting, or during the meeting. Endpoints that are defined in Equinox Management use their specified bandwidth by default. For more information, see Planning and configuring endpoints in Equinox Management on page 120.
Enable Gallery Layouts (requires additional 480p resource per meeting)	Enables gallery layouts when sharing content, which use additional MCU resources (an extra 480p connection per meeting). This is available for Scopia® Elite 6000 MCUs, Avaya Equinox® Media Servers and for **Video** meeting types (as displayed in the **Media** field). The Scopia® Elite 6000 MCU supports an additional set of layouts to optimize screen space during content sharing on single-screen endpoints (see *User Guide for Scopia Elite MCU*). The MCU processes the presentation and places it in the video layout alongside participant images, allowing endpoints with proprietary content sharing protocol to simultaneously display content and participants.

Table continues…

Parameter Name	Description
Enable Web Collaboration	Enables Web Collaboration for this meeting type. The Web Collaboration server provides advanced content sharing functionality.
Enable Slider	Enables reviewing previously shared content without interrupting the presenter.
Auto-Attendant Support	Enables Auto-Attendant support for this meeting type. Auto-Attendant is a video-based IVR which provides quick access to meetings through a set of visual menus. Users can view and join meetings from the Auto-Attendant, which displays all ongoing meetings in the organization. Disable this option if, for example, you do not want videoconferences with this meeting type to appear on the Auto-Attendant.
Enable Avaya Aura Conferencing	Enables participation in Avaya Aura® Conferencing.
Equinox Media Servers	Lists Media Servers in your deployment that support this meeting type. You can select the link to access the Media Server's administrator interface.

Related links

Modifying a media server meeting type in Equinox Management on page 81

Searching for a meeting type

About this task

You can search for a specific meeting type by name. Meeting types (also known as MCU/Media Server services) are meeting templates which determine the core characteristics of a meeting.

Procedure

1. Access Equinox Management.
2. Click **Meeting Types**.
3. Enter the partial or complete name of the meeting type in the **Name** field.

   Search results are listed.
4. To return to the complete list of meeting types, delete text in the **Name** field.

Related links

Downloading media server meeting yypes to Equinox Management on page 75

Deleting a meeting type from Equinox Management

About this task

You can permanently remove a meeting type from Equinox Management to remove it from all MCUs in your deployment. Meeting types (also known as MCU/Media Server services) are meeting templates which determine the core characteristics of a meeting.

Important:

When you delete meeting types, they cannot be restored later.

You cannot delete meeting types which are currently in use. If you need to delete a meeting type, wait until a meeting using this meeting type is over, then delete it.

Procedure

1. Access Equinox Management.
2. Click **Meeting Types**.
3. Select the meeting type you want to delete.
4. Click **Delete** and then **OK**.

   The meeting type is deleted from Equinox Management.

Related links

Downloading media server meeting yypes to Equinox Management on page 75

Increasing MCU capacity by cascading multiple MCUs

About this task

A cascaded videoconference is a meeting distributed over more than one physical Scopia Elite MCU and/or Equinox Media Server, where a master MCU/Media Server connects to one or more slave MCUs/Media Servers to create a single videoconference. It increases the meeting capacity by combining the resources of several MCUs/Media Servers. This can be especially useful for distributed deployments across several locations, reducing bandwidth usage.

You can cascade MCUs to reduce potential drain on network resources, increase the efficiency of MCU usage, and allow large conferences to be held (Figure 13: A single cascaded videoconference on page 86).

MCU cascading is enabled by default. This procedure describes how to configure the MCU's cascading behavior, which is managed by Equinox Management.

A videoconference is typically hosted on the MCU closest to the meeting organizer's location, although this can be modified when scheduling a meeting. For example, if most meeting participants are in a different location, the meeting organizer may decide to change the master MCU for this meeting. Depending on the cascading preference set below, this master MCU connects to one or more slave MCUs to form a cascaded meeting.

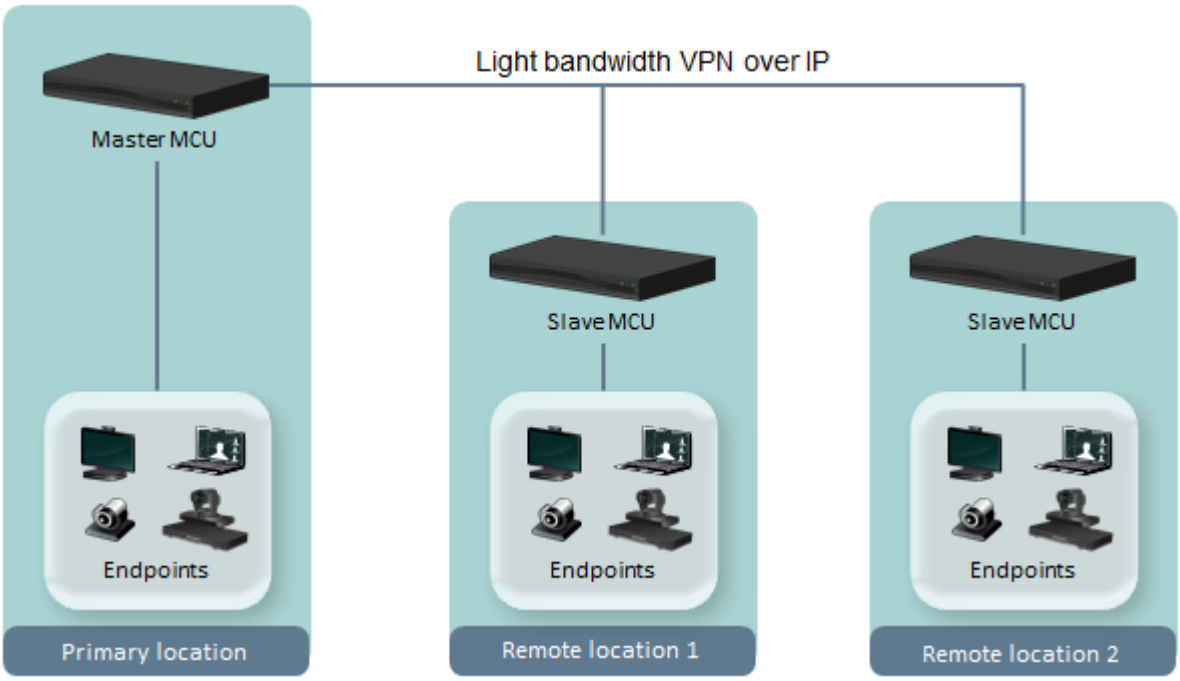


Figure 13: A single cascaded videoconference

Note:

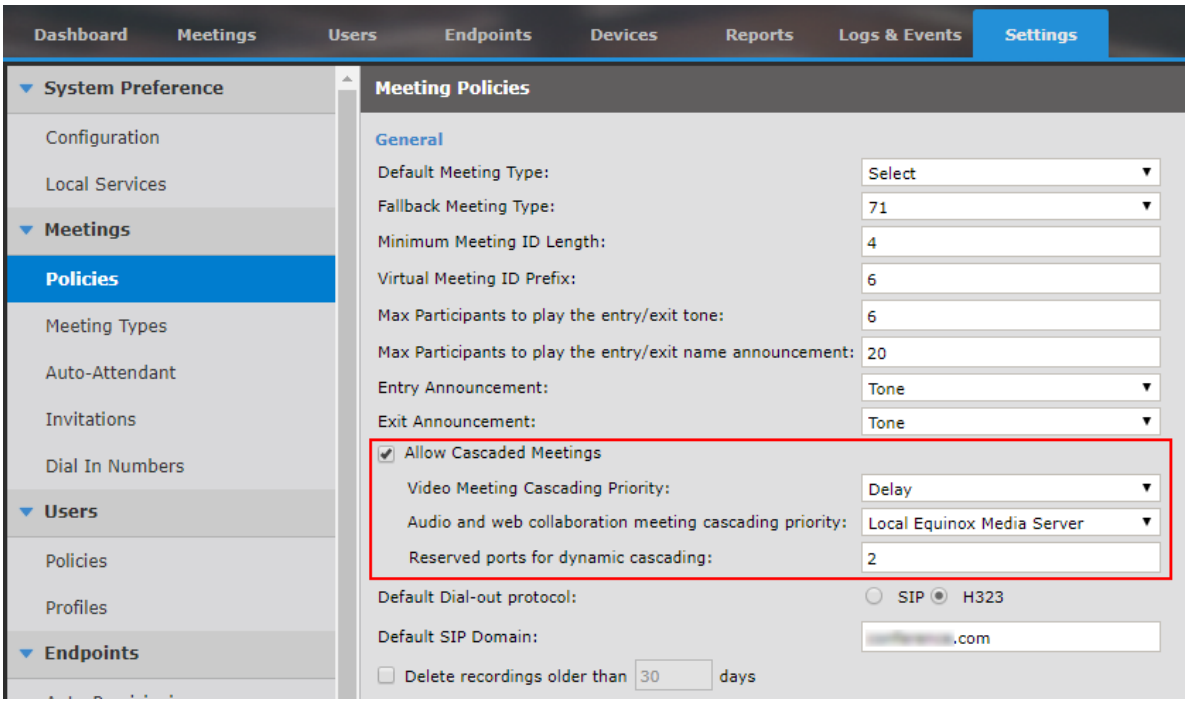
- The Meeting Type (MCU service) representing the required meeting must be available on all participating MCUs. For example, if the meeting uses MCU service 81, then 81 must exist on the master MCU and on the slave MCUs.
- A cascaded connection uses two ports—one on the master MCU, and one port on the slave MCU.
- Only one participant (typically the active speaker) connecting from each slave MCU can send video and be seen by other meeting participants in the video layout.
- Only one level of cascading is supported. All slave MCU conferences must cascade to the same master MCU conference.
- Any participant can become a lecturer.
- Participants connecting to the slave MCU:
  - View only the default meeting layout
  - Perform actions (such as joining the meeting) via their endpoint or web interface, and not via DTMF.

For information about planning your MCU's topology, including bandwidth considerations and cascading MCU, see *Administrator Guide for Scopia Elite MCU*.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Meetings** > **Policies**.

The system displays the **Meeting Policies** page.



3. In the **General** section, select the **Allow Cascaded Meetings** check box and configure the fields described in the following table:

Table 12: Configuring cascaded meeting policies

Field	Description
Video Meeting Cascading Priority	Select from the following: • **Delay**: Indicates that the media server cascades during video meetings only when its resources have filled up. • **Local Media Server**: Indicates that the media server cascades during video meetings immediately to the nearest media server.
Audio and Web Collaboration Meeting Cascading Priority	Select from the following: • **Delay**: Indicates that the media server cascades during audio and web collaboration meetings only when its resources have filled up. • **Local Media Server**: Indicates that the media server cascades during audio and web collaboration meetings immediately to the nearest media server.
Reserved ports for dynamic cascading	Enter the number of ports to be allocated for cascading.

4. Click **Apply** to save the preferred behavior as the default.

Related links

Planning and configuring media servers in Equinox Management on page 71

Enabling Auto-Attendant support

About this task

The Auto-Attendant feature provides quick access to meetings hosted on Equinox Media Servers or Scopia Elite MCUs, allowing meeting participants to access a video menu and select menu options using DTMF. This procedure describes how to enable the Auto-Attendant feature in Equinox Management. You must designate one meeting type for the Auto-Attendant. For more information about meeting types, including configuring its bandwidth and resolution, see Downloading media server meeting yypes to Equinox Management on page 75.

To enable the Auto-Attendant feature, you first configure a meeting type with Auto-Attendant support, and then configure the Auto-Attendant settings.

In service provider (multi-tenant) deployments, the service provider administrator configures the meeting type, and the organization administrator configures the Auto-Attendant settings.

Note:

- The Auto-Attendant feature is not supported for Avaya IX™ Workplace Client. It is only supported for dial-in calls and for Avaya IX™ Room System XT.
- Operator calls (*0) do not work during Auto-Attendant sessions when the Auto-Attendant service is from the Full Video Equinox Media Server.

Before you begin

1. When integrating Equinox Solution with the Avaya Aura Conferencing server, use the same number for both the Avaya and Avaya Auto-Attendant. You must also enable integration, as described in Integrating the Avaya Aura Conferencing server on page 91.
2. Choose a number you want to assign to the Auto-Attendant feature.

   Important:

   In service provider deployments, service provider administrators should allocate a range of numbers each organization can use, according to the rules listed below. Organization administrators should select a number from this range for the Auto-Attendant.

   The Auto-Attendant number must be different from the following numbers:

   - All E.164 numbers of your organization's endpoints. In service provider deployments, this number must be different from endpoints of all organizations.
   - Equinox Media Server or Scopia Elite MCU meeting type
   - Gateway service
   - H.323 Gatekeeper zone prefix
   - Auto-Route number
3. Synchronize the Equinox Media Server’s or Scopia Elite MCU’s meeting types with Equinox Management, as described in Synchronizing media server meeting types with Equinox Management on page 76.
4. If your deployment uses a third-party gatekeeper, ensure that the gatekeeper has a prefix configured to direct calls to the Auto-Attendant.

Procedure

1. Access the Equinox Management administrator portal.
2. Configure the meeting type for Auto-Attendant support, as follows:

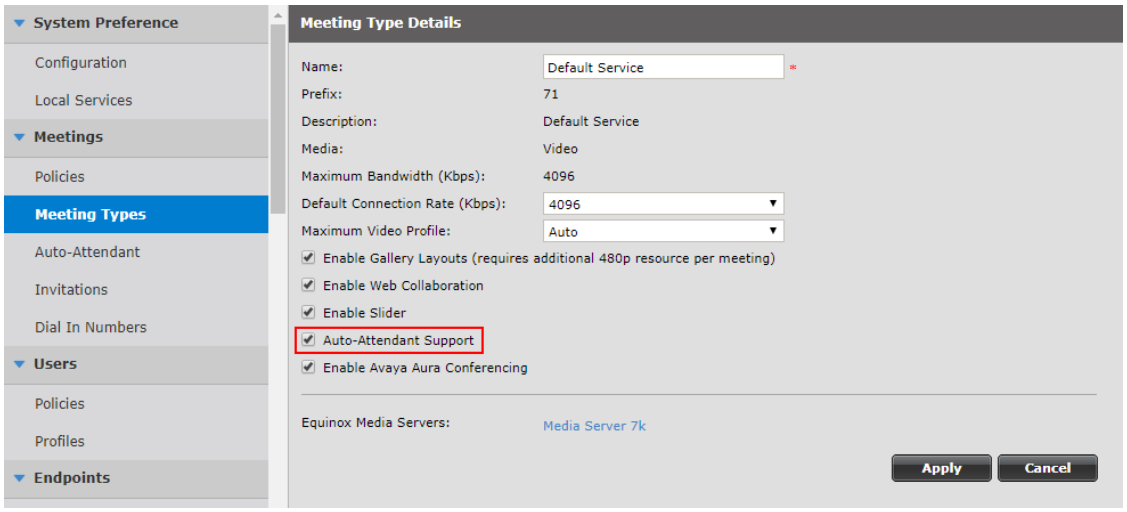
   Important:

   In service provider deployments, this step is performed by the service provider administrator.

   a. Click **Settings** > **Meetings** > **Meeting Types**.

   b. Select the meeting type for which you want to configure Auto-Attendant support, in the **Name** column.

   The system displays the **Meeting Type Details** page.



   c. Click **Auto-Attendant Support**.

   d. Click **Apply**.

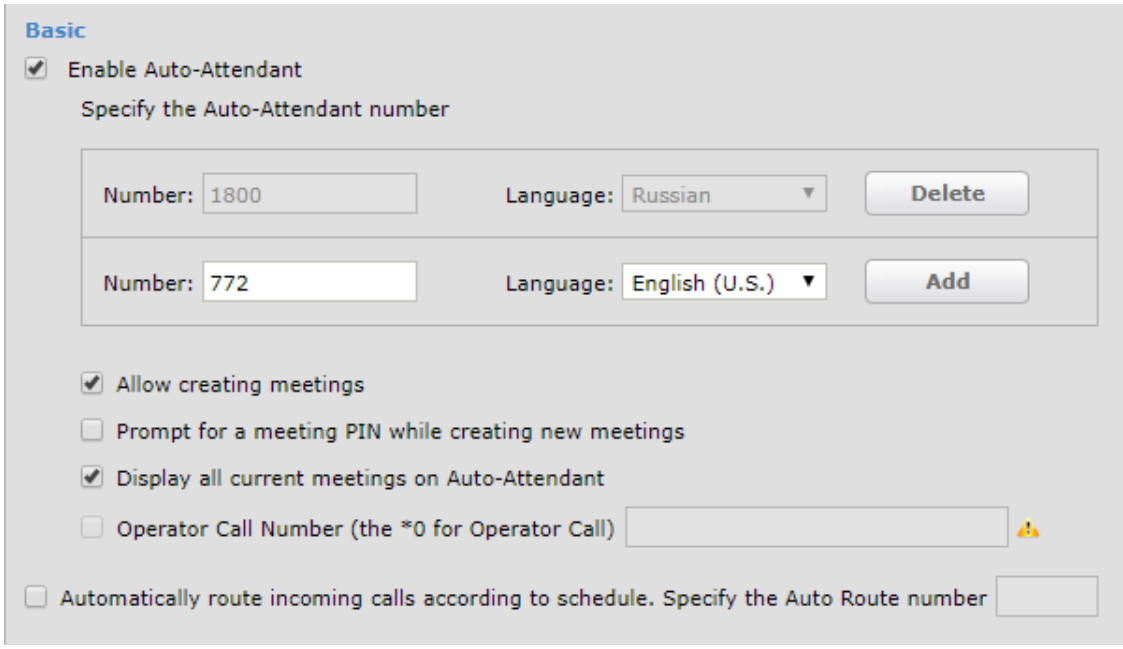
3. Configure settings for the Auto-Attendant, as follows:

   Important:

   In service provider deployments, this is done by each organization's administrator.

   a. Click **Settings** > **Meetings** > **Auto-Attendant**.

   b. Click **Enable Auto Attendant**.



c. Configure the Auto-Attendant settings, as described in Table 13: Configuring Auto-Attendant settings on page 90.

Table 13: Configuring Auto-Attendant settings

Field Name	Description
Specify the Auto-Attendant Number	Assign an Auto-Attendant number to the meeting type you configured with Auto-Attendant support. For details on choosing a number for the Auto-Attendant, see the prerequisites above.
Allow creating meetings	Select to allow guests to create meetings by dialing the Auto-Attendant.
Prompt for a meeting PIN while creating new meetings	Select to prompt regular users to enter a meeting PIN when creating new meetings.
Display all current meetings on Auto-Attendant	Select to display all ongoing meetings on the Auto-Attendant.
Operator Call Number (the *0 for Operator Call)	Enter the internal number that the system calls to reach the operator, after the user dials *0.

Table continues…

Field Name	Description
Automatically route incoming calls according to schedule. Specify the Auto Route number	Select to route all meetings hosted by the Equinox Media Server or Scopia Elite MCU to the Auto-Attendant, and assign a unique auto-route number, which is used by the gatekeeper to route calls to the Equinox Media Server or Scopia Elite MCU. This number cannot be the same as any of the following: • Auto-Attendant number • Equinox Media Server or Scopia Elite MCU meeting type • Virtual room prefix • Gateway service • H.323 Gatekeeper zone prefix

d. Click **Apply**.

Related links

Planning and configuring media servers in Equinox Management on page 71

Integrating the Avaya Aura® Conferencing server

About this task

You can extend Equinox Solution videoconferences to include video and audio endpoints hosted by the Avaya Aura® Conferencing (AAC) server.

This is a cost-effective approach, for example, when the conference includes many Avaya participants joining from an audio device. The AAC hosts Avaya endpoints, providing excellent audio quality to a large number of participants, and the Scopia Elite MCU hosts the video participants.

Important:

You can allow Avaya endpoints to join an Equinox Solution video conference directly, without connecting to the Avaya Aura® Conferencing server, by defining the Avaya Session Manager as a SIP server.

Perform the procedure below to integrate the AAC server into Equinox Management. The MCU then automatically connects to the AAC server when the meeting starts, as long as this is supported by the meeting type (see Modifying a media server meeting type in Equinox Management on page 81 for details).

This feature is available for AAC version 7 and later.

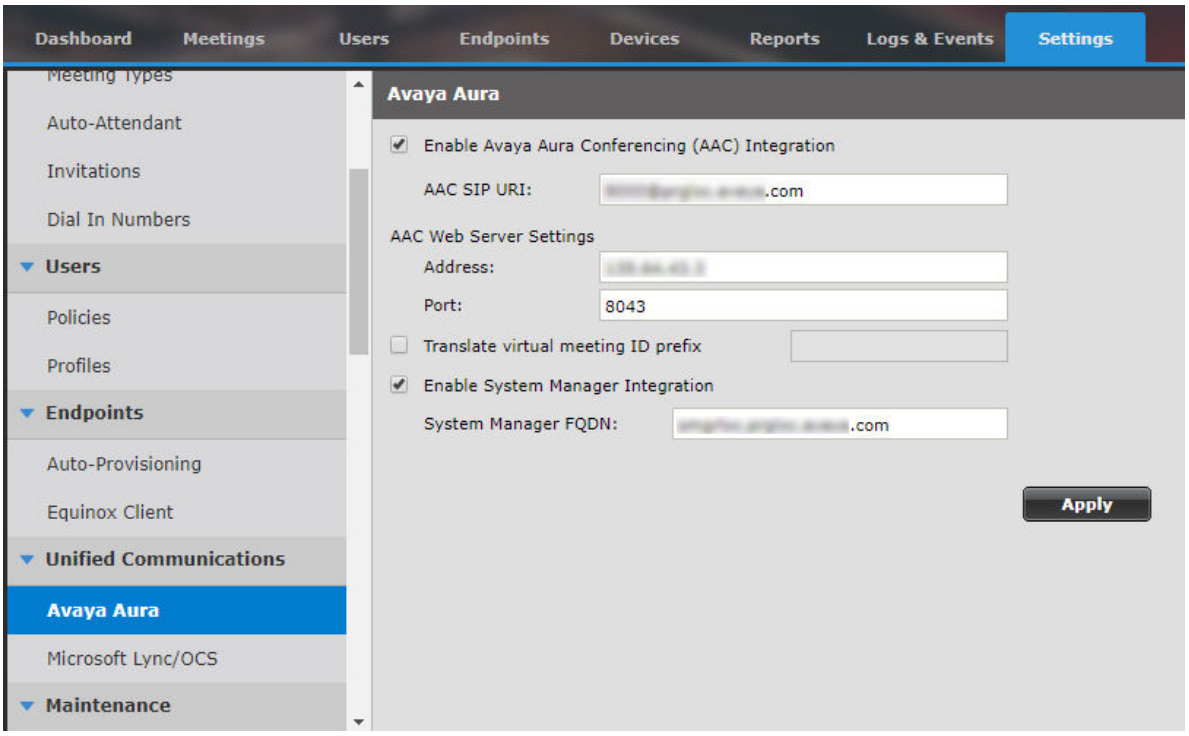
For more information about Equinox Solution integration with Avaya, see the *Equinox Solution Guide*.

Procedure

1. Access the Equinox Management administrator portal.

2. Click **Settings** > **Unified Communications** > **Avaya Aura**.

   The system displays the **Avaya Aura** page.



3. Click **Enable Avaya Aura Conferencing (AAC) Integration**.
4. Enter the settings as described in Table 14: Integrating Avaya Aura Conferencing server on page 92.

Table 14: Integrating Avaya Aura Conferencing server

Field Name	Description
AAC SIP URI	The URI dial string needed to reach the Avaya Aura Conferencing server. For example, *server_name@company.com*
AAC Web Server Address	Enter the URL of the web server.
Port	Enter the port used to connect to the web server. By default, port 8043 is used.

Table continues…

Field Name	Description
Translate virtual meeting ID prefix	Depending on your dial plan, select to remove the prefix of the Equinox Management virtual meeting ID from the meeting ID when connecting to the AAC server. If required by your dial plan, enter an alternative prefix to use. For example, if the prefix of the virtual meeting ID defined in Equinox Management is *88*, and is already in use in the AAC dial plan, you can define a different prefix here, such as *9999*. The new prefix (*9999*) replaces the prefix defined in Equinox Management (*88*) for Avaya endpoints.
Enable System Manager Integration	Select to enable Equinox Management to integrate with System Manager.
System Manager FQDN	Enter the FQDN of the System Manager with which Equinox Management is integrating. Enabled only when the **Enable System Manager Integration** check box is selected.

5. Click **Apply**.

   If you configured System Manager integration, select **Yes** on the confirmation message dialog box to restart Equinox Management.

Related links

Planning and configuring media servers in Equinox Management on page 71

Planning and configuring gateways in Equinox Management

Configure gateways in your network to enable non-H.323 endpoints, such as SIP, PSTN, ISDN, and mobile endpoints, to join a meeting. Equinox Management uses the gateway information to provide proper dialing information for meeting participants, and to dial out to endpoints to invite them to meetings. In addition, Equinox Management manages gateway resources to allow successful call scheduling using network gateways.

Caution:

Ensure that the virtual meeting ID prefix is not the same as the prefix for the MCU meeting type, ECS zone, or other prefixes. If the prefix is the same you cannot successfully use a different language in your meeting invitation than the one selected in the virtual room.

Related links

Defining your video network devices on page 58
Configuring the WebRTC and Recording Gateways in Equinox Management on page 94
Configuring a Gateway in Equinox Management on page 96

Configuring a WebRTC or recording gateway in Equinox Management on page 100
Connecting a WebRTC client to a meeting through a TURN server on page 103
Configuring user portals in Equinox Management on page 104
Registering a gateway with a gatekeeper on page 105

Configuring the WebRTC and Recording Gateways in Equinox Management

About this task

This section explains how to configure the Avaya WebRTC Gateway, Avaya Recording Gateway settings in Equinox Management.

Since the Gateway does not have its own web interface, its configuration is performed in Equinox Management.

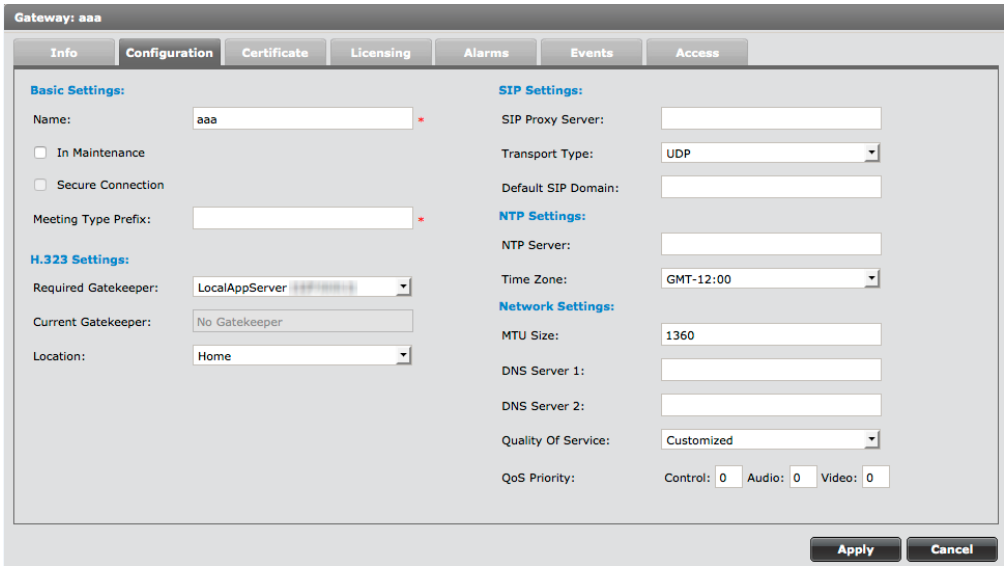
Equinox Management and gateways communicate in XML over TCP for control and configuration commands. You can secure the connection by configuring it to the TLS protocol. Make sure to generate the Avaya Equinox® Management and Gateway certificates before configuring the connection to TLS (see Securing your video network using TLS on page 181).

Before you begin

1. Add the Gateway to Equinox Management by entering its basic settings, as described in Adding video network devices in Equinox Management on page 61.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Devices** > **Devices by Type** > **Gateways**.
3. Select the gateway you are configuring.
4. Click the **Configuration** tab.



5. Configure the gateway settings, as described in Table 15: Configuring settings for the gateway on page 95.

Table 15: Configuring settings for the gateway

Field Names	Description
Name	You can modify the name that identifies the gateway in Equinox Management.
In Maintenance	Select to indicate that the gateway is not online and is therefore not available. You typically select this option while upgrading the gateway.
Secure Connection	The location of the gateway.
Meeting Type Prefix	The numeric dial prefix used by the gateway to identify this meeting type.
Required Gatekeeper	The gatekeeper to which you want to register the gateway.
Current Gatekeeper	This (read-only) field displays the management IP address of the gatekeeper that this gateway is currently registered to. In most cases, this is the same gatekeeper selected in the **Required Gatekeeper** field. If the current gatekeeper is not the same as the gatekeeper configured in the **Required Gatekeeper** field, an alarm is issued by Equinox Management.
Location	Relevant only for service providers or deployments with multiple locations. You can modify the gateway's location.
SIP Proxy Server	The IP address of the SIP Proxy Server.
Transport Type	The enable transport type.

Table continues…

Field Names	Description
Default SIP Domain	The default domain of the SIP Proxy Server.
NTP Server	The IP address of the NTP server.
Time Zone	The time zone of the NTP server.
MTU Size	The size of the maximum transmission unit, measured in bytes.
DNS Server 1, 2	The IP address(es) of the organization's DNS server(s).
Quality of Service	Select the quality of service for the gateway.
QoS Priority	The priority of different types of network traffic. During poor network conditions, prioritized traffic is still fully transmitted.

6. Click **Apply**.
7. Allow Equinox Management to access the gateway:
   a. Click the **Access** tab.
   b. Enter the login name and password of the gateway. The default username is **admin** and the default password is **password**.
   c. Click **Apply**.

Related links

Planning and configuring gateways in Equinox Management on page 93

Configuring a Gateway in Equinox Management

About this task

Gateways extend your video capabilities to include protocols outside of your main video network. For example, the Gateway extends your H.323-based network to include ISDN endpoints.

Equinox Management keeps track of the gateway's available ports to enable the successful scheduling of calls.

When you add a gateway, the settings in Equinox Management must be consistent with the configuration of the gateway device itself. This includes specifying all the services on that gateway.

A service maps a numeric dial prefix to a type of call. When the gateway receives a call with the designated prefix, it determines the properties of that call:

- Whether it is voice only or video, and
- The bandwidth allocated for this kind of call.

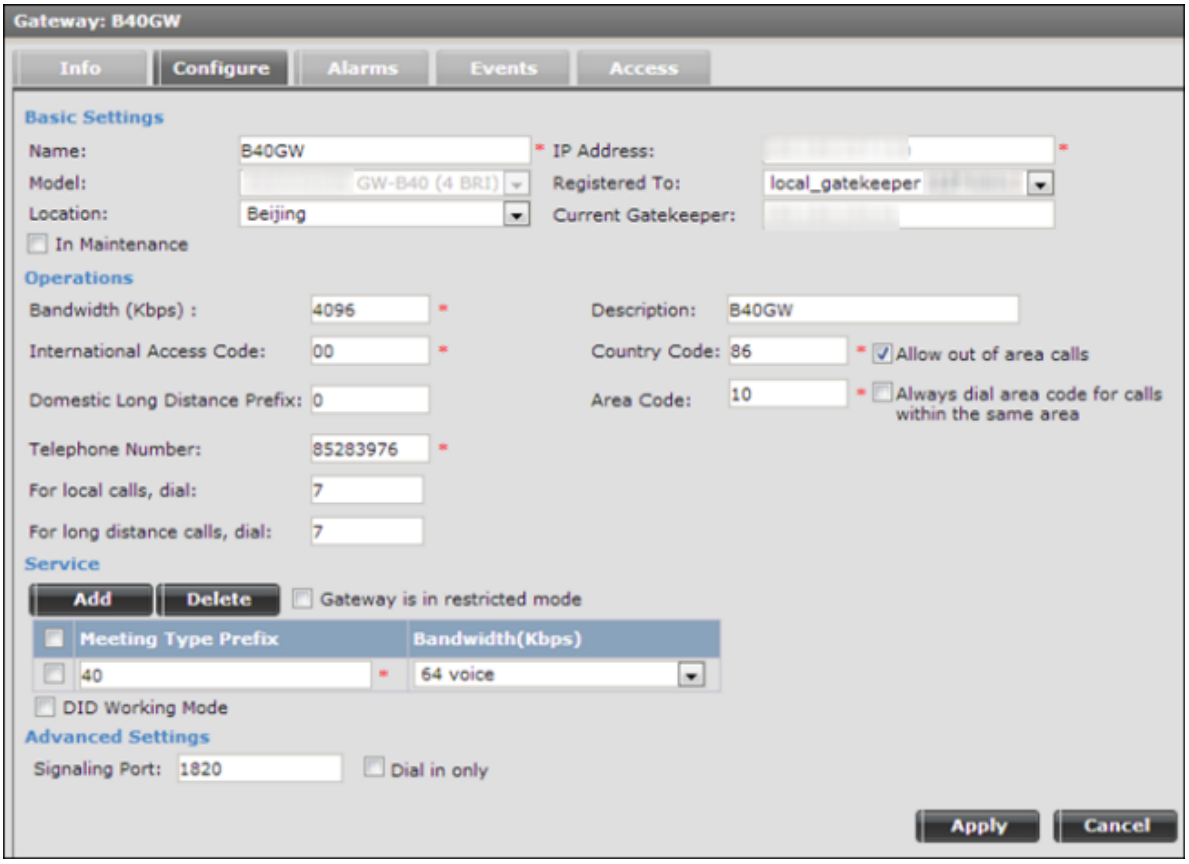
This procedure details how to configure a gateway to Equinox Management, including detailing the gateway's services.

Before you begin

Add the gateway to Equinox Management by entering its basic settings, as described in Adding video network devices in Equinox Management on page 61.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Devices** > **Devices by Type** > **Gateways**.
3. Click the gateway you are configuring.
4. Click the **Configuration** tab.



5. Enter the gateway settings in Equinox Management. The settings must be consistent with the configuration of the gateway device itself.

Field Name	Description
Name	(Optional) Modify the name of the gateway.
Model	(Read-only) Displays the type of gateway.
Registered To	Select the gatekeeper to which the gateway is registered.
Location	If there is more than one location in your deployment, assign your gateway to a location by selecting an option from the list.

Table continues…

Field Name	Description
IP Address	(Read-only) Displays the IP address of the management stream of the gateway. Equinox Management communicates with the gateway via its management stream, and does not need the media stream if different. If multiple gateways are pooled together in a local network with the same access phone number, all IP addresses are separated by a semi-colon (;).
Bandwidth	The total bandwidth allocated to this gateway. For example, for an E1 line or 30 B-channels, the bandwidth is 64 x 30 = 1920 Kbps per network interface. For gateways with two PRI interfaces, the total bandwidth would be 1920 x 2 = 3840 Kbps. If multiple gateways are pooled together in a local network with the same access phone number, enter the bandwidth of a single gateway unit in the pool.
IVR	Choose if the gateway routes calls using an Interactive Voice Response (IVR) system. For more information, see the gateway documentation.
DID	Choose if call routing is direct to an endpoint without operator intervention using Direct Inward Dialing. For more information, see the gateway documentation.
Description	A description of the phone number for the gateway.
International Access Code	The numeric dial prefix required to make an international call.
Country Code	The numeric dial prefix to dial a terminal located in a different country.
Domestic Long Distance Prefix	The numeric dial prefix required to make a long distance call within a country.
Allow Out of Area Calls	If selected, endpoints can reach Equinox Management via the gateway even when they have a different area code to that of the gateway.
Area Code	The domestic area code of the gateway number.
Telephone Number	A local telephone number to be assigned to the specific port.
For local calls, dial:	The dial prefix required for the gateway to access an outside line.
For long distance calls, dial:	The dial prefix required for the gateway to make a long distance call.

6. Click **Add** in the **Service** area to create an additional service entry for this gateway. You can add multiple services. The list of services must be identical to the services on the gateway itself.

A service maps a numeric dial prefix to a type of call. When the gateway receives a call with the designated prefix, it determines the properties of that call:

- Whether it is voice only or video, and
- The bandwidth allocated for this kind of call.

7. For each service, enter the field values as required:

Table 16: Adding a service

Field Name	Description
Meeting Type Prefix	The numeric dial prefix used by the gateway to identify this meeting type.
Bandwidth	The properties of this service, both bandwidth and whether it is voice only or video. Choose from a predefined list. If this service's bandwidth is set to **Auto** on the device itself, in Equinox Management enter the average bandwidth endpoints use when dialing that service.
Gateway is in restricted mode	Restricted mode is used for ISDN endpoints only, when the PBX and line uses a restricted form of communication, reserving the top 8k of each packet for control data only. If enabled, the bandwidth values on these lines are in multiples of 56kbps, instead of multiples of 64kbps.

8. Configure the advanced settings.

Table 17: Defining advanced settings

Field Name	Description
Signaling Port	The gateway port used for signaling. Leave this field blank to negotiate the signaling port dynamically.
Dial-in Only	Indicates the gateway is used for incoming calls only. Equinox Management does not schedule outgoing calls on this gateway.

9. Click **Apply** to save your changes.
10. Click the **Access** tab and enter the Gateway's information to enable encrypted SNMP communications between the gateway and Equinox Management, as described in Table 18: Configuring the Gateway's access information on page 99.

Table 18: Configuring the Gateway's access information

Field Name	Description
Username **Password**	Enter the login username and password of the gateway web interface login.

Table continues…

Field Name	Description
SNMP Read Community **SNMP Write Community**	Equinox Management displays the names of the SNMP communities that support the read and write operations of SNMP management in your network. Both the gateway and Equinox Management support sending and receiving SNMP alerts to track the gateway's behavior and handle any errors which may occur. SNMP community information must match the settings defined in the gateway to enable Equinox Management to retrieve information from the gateway. **Important:** The community values are case-sensitive.

11. Click **Apply**.

Related links

Planning and configuring gateways in Equinox Management on page 93

Configuring a WebRTC or recording gateway in Equinox Management

About this task

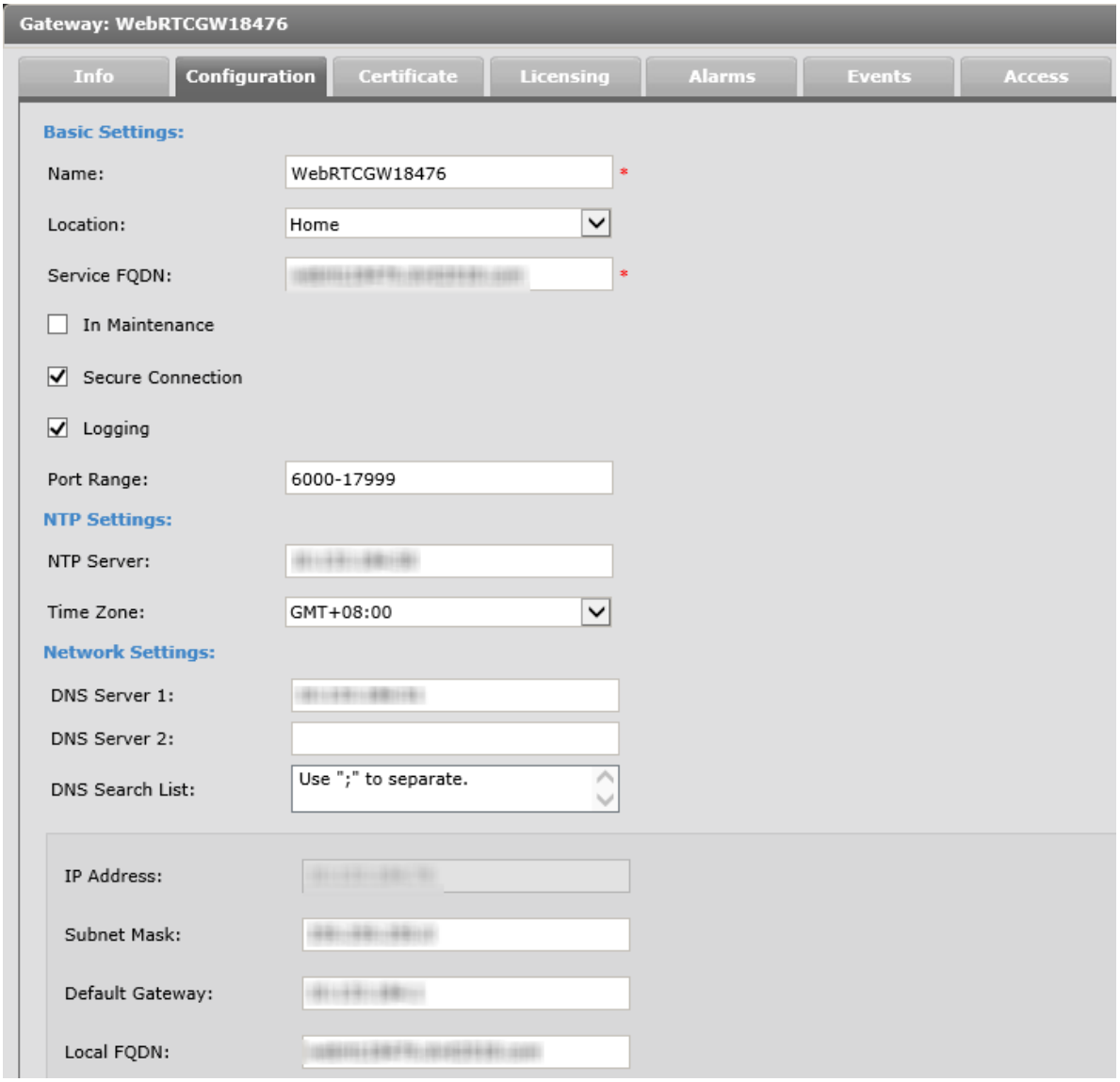
To configure a WebRTC or recording gateway in Equinox Management, follow this procedure.

Before you begin

1. Add the Gateway to Equinox Management by entering its basic settings, as described in Adding video network devices in Equinox Management on page 61.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Devices** > **Devices by Type** > **Gateways**.
3. Click the gateway you are configuring.
4. Click the **Configuration** tab.



5. Configure the gateway settings, as described in Table 19: Configuring settings for the gateway on page 101.

Table 19: Configuring settings for the gateway

Field Names	Description
Name	You can modify the name that identifies the Gateway in Equinox Management.
Location	The location of the gateway.
Service FQDN	Enter the fully qualified domain name (FQDN) of the service.

Table continues…

Field Names	Description
In Maintenance	Select to indicate that the gateway is not online and is therefore not available. You typically select this option while upgrading the gateway.
Logging	Select to indicate that the gateway is keeping logs.
Port Range	Enter the range of port numbers which are available on the gateway.
NTP Server	The IP address of the NTP server.
Time Zone	The time zone of the NTP server.
DNS Server 1, 2	The IP address(es) of the organization's DNS server(s).
DNS Search List	Enter the short name of the DNS server when the media server searches other sites. The system searches the DNS search list for the suffix.
IP Address	The unique IP address of the gateway. **Note:** When the device is online, you can change its IP address in this field.
Subnet Mask	The subnet mask of the gateway.
Default Gateway	The IP address of the default gateway server which connects you to outside your network.
Local FQDN	The fully qualified domain name (FQDN) of the local gateway.
THE FOLLOWING FIELDS APPEAR ONLY WHEN CONFIGURING A RECORDING GATEWAY	
Required Gatekeeper	Select the gatekeeper to which the recording gateway is registered. If you select **None**, you can add the gateway to Equinox Management, but it will not be connected until you register the gateway with the gatekeeper, and select the gatekeeper here.
Current Gatekeeper	This (read-only) field displays the management IP address of the gatekeeper to which the gateway is currently registered. In most cases, this is the same gatekeeper selected in the **Required Gatekeeper** field. If the current gatekeeper is not the same as the gatekeeper configured in the **Required Gatekeeper** field, an alarm is issued by Equinox Management.
SIP Proxy Server	The IP Address of the SIP Proxy Server.
Transport Type	The enabled transport type.
Turn/Stun Server	The IP Address of the Turn/Stun Server.

6. Click **Apply**.
7. Allow Equinox Management to access the Gateway, as follows:
   a. Click the **Access** tab.

b. Enter the login name and password of the Gateway. The default username is **admin** and the default password is **password**.

c. Click **Apply**.

Related links

Planning and configuring gateways in Equinox Management on page 93

Connecting a WebRTC client to a meeting through a TURN server

About this task

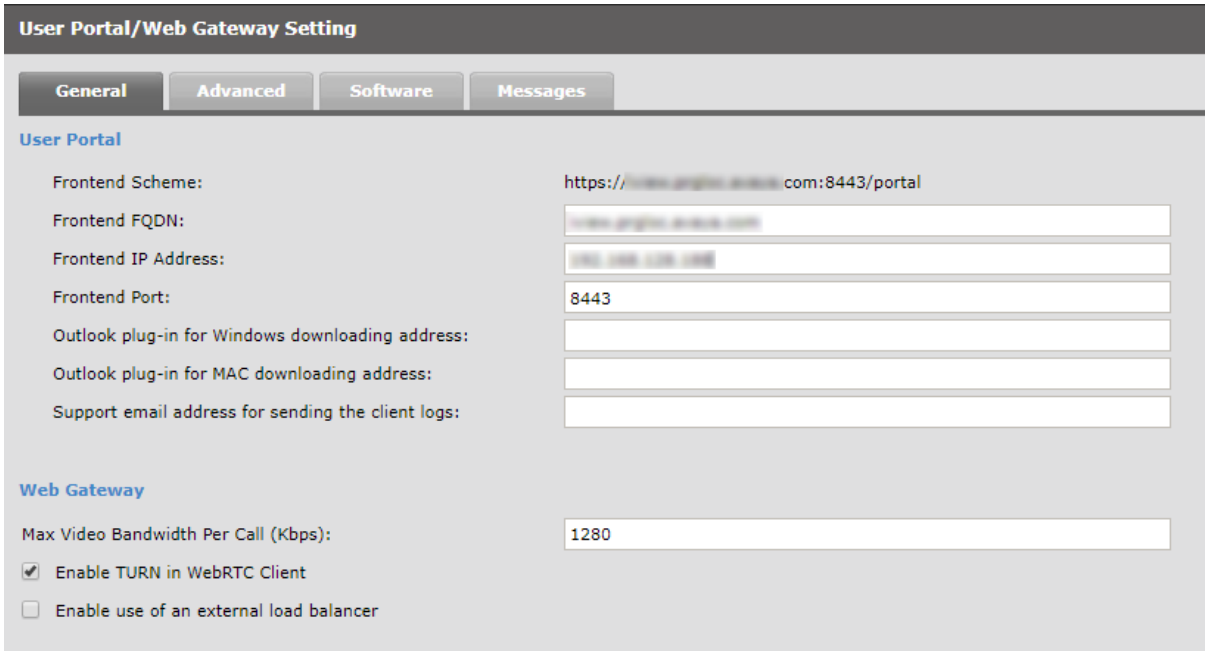
You can connect an external WebRTC client to a meeting through a TURN TCP, even if your browser is behind a firewall that blocks UDP traffic.

This feature is supported when working with SBC version 7.2.2 or higher.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Devices** > **User Portal/Web Gateway**.

   The system displays the **User Portal/Web Gateway Setting** page.



3. Select the **Enable TURN in WebRTC Client** check box.
4. Click **Apply**.

Related links

Planning and configuring gateways in Equinox Management on page 93

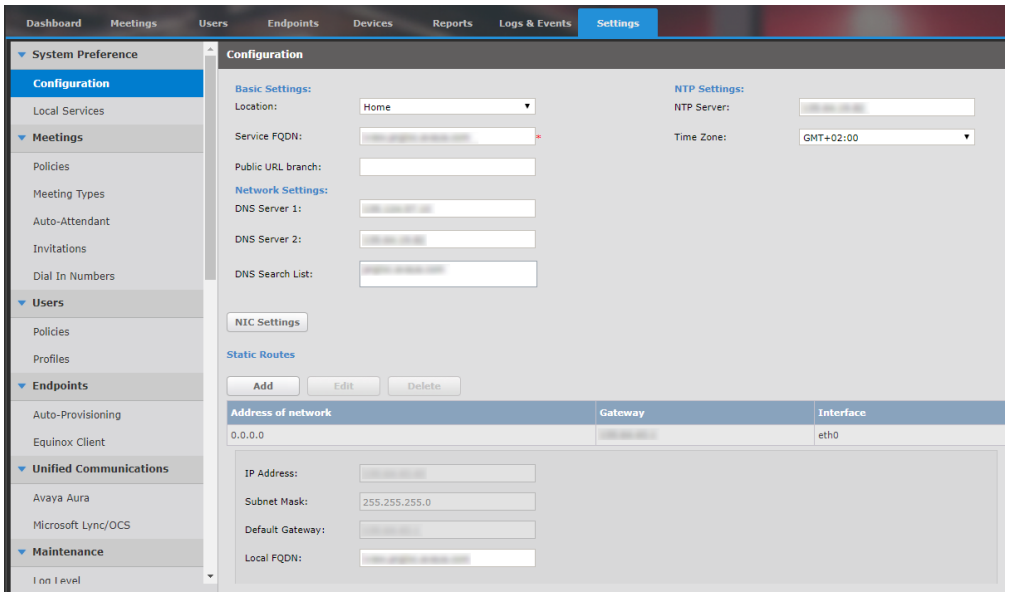
Configuring user portals in Equinox Management

About this task

You can configure user portals in Equinox Management. User portals are also called Avaya Aura® Web Gateways.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Devices** > **Devices by Type** > **User Portals**.
3. Click the user portal to view detailed information, and select the **Configuration** tab.



Configure the fields on the page, as described in the following table:

Table 20: Configuring your user portal

Section	Field Name	Description
Basic Settings	**Name**	You can modify the name used to identify the user portal. This is the name displayed in the list of user portals.
	Location	You can modify the user portal's location. This field is relevant only for service providers or deployments with multiple locations.
	Service FQDN	Enter the fully qualified domain name (FQDN) of the service.

Table continues…

Section	Field Name	Description
	Secure connection	Select to secure access to the user portal web interface. You can do this only if you installed certificates for the media server, either from Equinox Management or from the media server interface (see *Administrator Guide for the Scopia Elite MCU*).
NTP Settings	**NTP Server**	The IP Address of the NTP server
	Time Zone	The time zone in which the NTP server is located
Network Settings	**DNS Server 1**	The IP Address of the DNS server
	DNS Server 2	The IP Address of the backup DNS server, in the event that DNS Server 1 is not available
	DNS Search List	Enter the short name of the DNS server when the media server searches other sites. The system searches the DNS search list for the suffix.
	IP Address	The IP Address of the user portal **Note:** When the device is online, you can change its IP address in this field.
	Subnet Mask	The subnet mask of the user portal
	Default Gateway	The default gateway of the user portal
	Local FQDN	The fully qualified domain name (FQDN) of the local user portal

4. Click **Apply**.

Related links

Planning and configuring gateways in Equinox Management on page 93

Registering a gateway with a gatekeeper

About this task

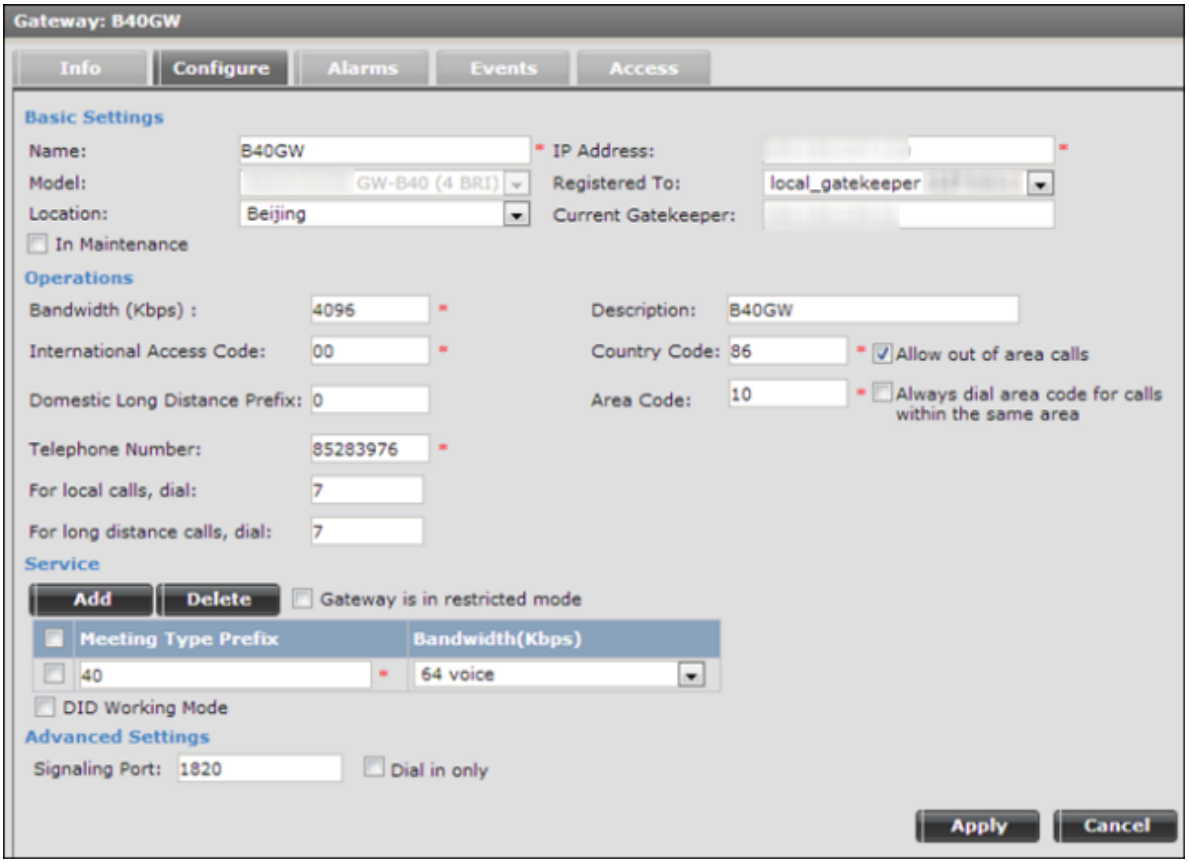
Gatekeepers, which maintain the register of aliases in a video network, sometimes include endpoints working under a different network protocol, and therefore must be routed through a gateway. Gateways bridge between the H.323 protocol and other video protocols, like ISDN.

The gatekeeper must register a network's gateways, to ensure safe call routing across different protocols.

Procedure

1. Access the Avaya Equinox® Management administrator portal.

2. Click the **Devices** tab.
3. Click the gateway you are configuring.
4. Click the **Configure** tab.



5. Select the gatekeeper to register your gateway in the **Required Gatekeeper** list.
6. Click **Apply**.

Related links

Planning and configuring gateways in Equinox Management on page 93

Configuring a UCCS Server in Equinox Management

About this task

You configure UCCS servers in Equinox Management to enable load balancing. UCCS server is also referred to as Equinox Conference Control.

After deploying and configuring the main Equinox Management server, you then deploy an additional management server OVA which serves as the distributed H.323 Gatekeeper. If you

need more than 2000 Equinox Conference Control calls you must deploy multiple UCCS servers to increase concurrent capacity.

Before you begin

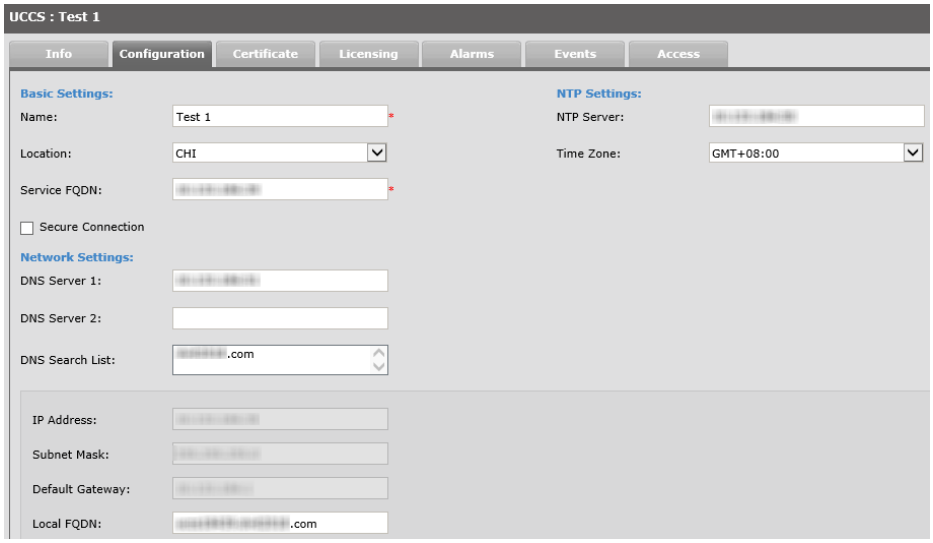
Ensure that you have deployed an additional Equinox Management server.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Devices** > **Devices by Type** > **UCCS Servers**.

   The system displays the **UCCSs** page.
3. Select the server.
4. On the **Info** tab, verify that the server's status is **Online** and that the version is correct to ensure that the distributed server deployment was successful.
5. Click the **Configuration** tab.

   The The system displays the UCCS Configuration tab.



6. Configure the displayed fields, as described in the following table:

Table 21: Configuring your UCCS server

Section	Field Name	Description
Basic Settings	**Name**	You can modify the name used to identify the UCCS server. This is the name displayed in the list of UCCS servers.
	Location	This is relevant only for service providers or deployments with multiple locations. You can modify the UCCS server's location.

Table continues…

Section	Field Name	Description
	Service FQDN	Enter the fully qualified domain name (FQDN) of the service.
	Public URL Branch	Enter the public branch URL to enable supporting multiple UCCS servers.
	Secure connection	Select to secure access to the UCCS server web interface. You can do this only if you installed certificates for the media server, either from Equinox Management or from the media server interface (see *Administrator Guide for the Scopia Elite MCU*).
NTP Settings	**NTP Server**	The IP Address of the NTP server.
	Time Zone	The time zone in which the NTP server is located.
Network Settings	**DNS Server 1**	The IP Address of the DNS server.
	DNS Server 2	The IP Address of the backup DNS server, in the event that DNS Server 1 is not available.
	DNS Search List	Enter the short name of the DNS server when the media server searches other sites; The system searches the DNS search list for the suffix.
	IP Address	The IP Address of the UCCS server. **Note:** When the device is online, you can change its IP address in this field.
	Subnet Mask	The subnet mask of the UCCS server.
	Default Gateway	The default gateway of the UCCS server.
	Local FQDN	The fully qualified domain name (FQDN) of the local UCCS server.

7. Click **Apply**.

Related links

Defining your video network devices on page 58

Planning and configuring Avaya Session Border Controller for Enterprise (ASBCE) in Equinox Management

The Avaya Session Border Controller for Enterprise (ASBCE) server enables communication through a firewall when an external device is trying to establish communication with devices inside

the firewall. Communication is enabled after you configure the reverse proxy and TURN/STUN settings for the ASBCE. You must first complete virtual deployment of the ASBCE before you can configure the reverse proxy and TURN/STUN functionality. For details on ASBCE deployment, see *Avaya Session Border Controller Deployment* in the *Avaya Equinox® Solution Deployment Guide*.

ASBCE settings are also configured in Equinox Management, which enables Equinox Management to utilize the ASBCE functionality. You assign a TURN/STUN server when configuring media servers, and you also configure the internal and external IP addresses to be used by the ASBCE.

Related links

Defining your video network devices on page 58

Configuring Avaya Session Border Controller for Enterprise (ASBCE) in Equinox Management on page 109

Configuring Avaya Session Border Controller for Enterprise (ASBCE) in Equinox Management

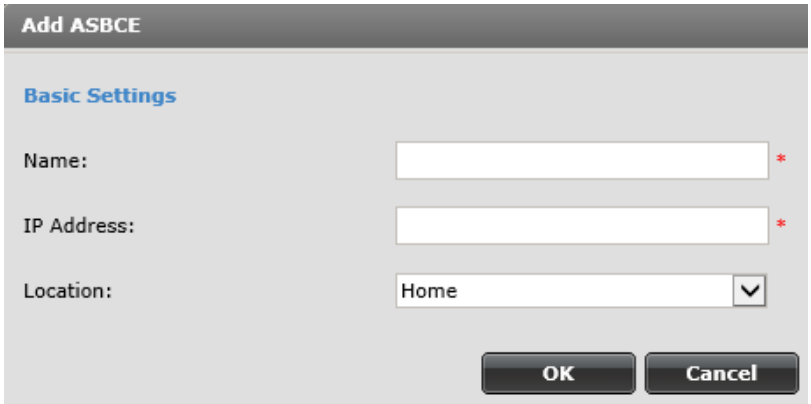
About this task

This procedure describes how to configure the Avaya Session Border Controller for Enterprise (ASBCE) in Equinox Management.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Devices** > **Devices by Type** > **ASBCE**, and click the **Add** button.

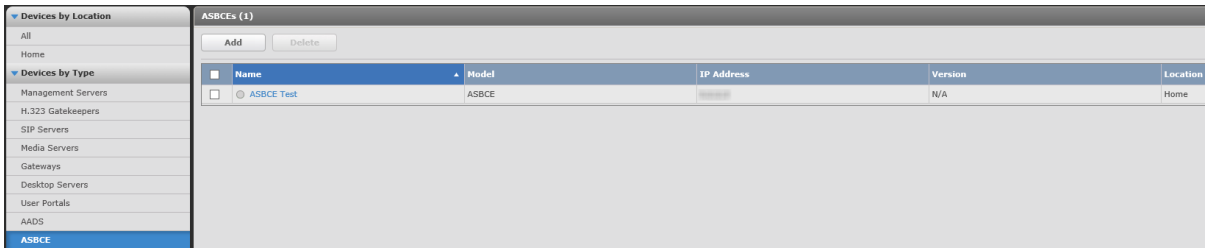
   The system displays the **Add ASBCE** page.



3. In the **Name** field, enter a name for the ASBCE server.
4. In the **IP Address** field, enter the IP address of the Element Management System (EMS), the management interface of ASBCE.
5. In the **Location** field, select the location of the ASBCE server, as defined in Equinox Management.

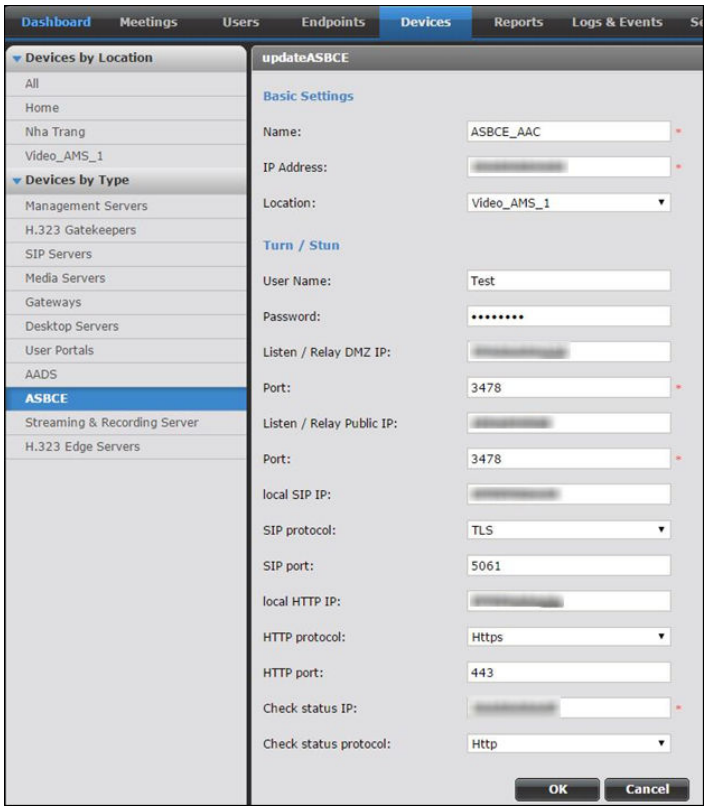
6. Click **OK**.

   The system displays the ASBCE server on the **ASBCEs** page.



7. Click the link in the **Name** column for the ASBCE for which you want to configure additional settings.

   The system displays the **Update ASBCE** page.



8. Enter the relevant values in the **Turn/Stun** fields, as described in the following table:

Table 22: Turn/Stun Fields

Field Names	Description
User Name	The username of the turn/stun server.
Password	The password of the turn/stun server.

Table continues…

Field Names	Description
Listen/Relay DMZ IP	By default, the management server IP address displays. Modify to be the ASBCE server's external IP address.
Port	The port number of the Listen/Relay DMZ IP.
Listen/Relay Public IP	By default, the management server IP address displays. Modify to be the ASBCE server's public IP address.
Port	The port number of the Listen/Relay Public IP.
Local SIP IP	The local IP address of the SIP server.
SIP Protocol	The SIP server protocol, either **TCP** or **TLS**.
SIP Port	The port number of the SIP server.
Local HTTP IP	The IP address of the HTTP server.
HTTP Protocol	The HTTP server protocol, either **HTTP** or **HTTPS**.
HTTP Port	The port number of the HTTP server.
Check status IP	The IP address of the internal interface.
Check status protocol	The protocol of the internal interface, either **HTTP** or **HTTPS**.

9. Click **OK**.

Note:

The ASBCE status must be green to ensure that the High Capacity Audio Media server and the WebRTC Gateway work properly.

Related links

Planning and configuring Avaya Session Border Controller for Enterprise (ASBCE) in Equinox Management on page 108

Remotely configuring the Avaya Equinox® H.323 Edge server

About this task

Equinox H.323 Edge provides a complete firewall and NAT traversal solution enabling secure connectivity between enterprise networks and remote sites.

See *Deployment Guide for Avaya Equinox® H.323 Edge* for information on the device's configuration.

Before you begin

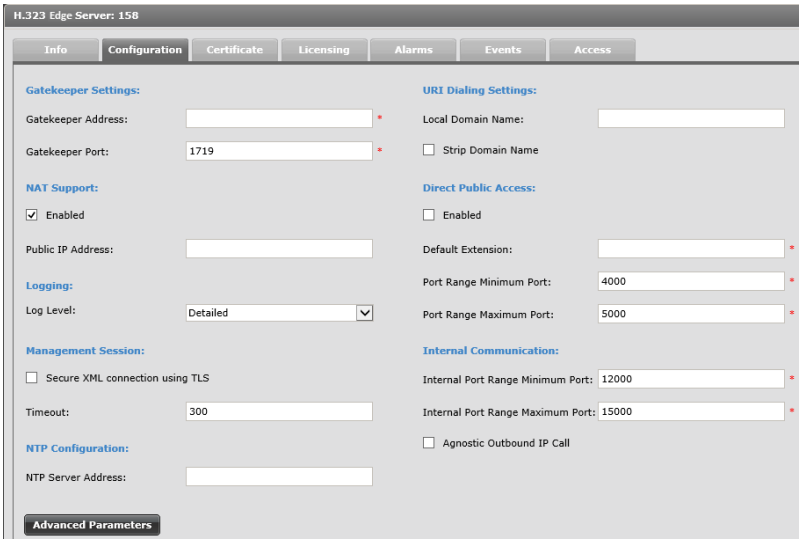
Add Equinox H.323 Edge to Equinox Management, as described in Adding video network devices in Equinox Management on page 61.

Procedure

1. Access the Equinox Management administrator portal.
2. Click the **Devices** tab.
3. Click **H.323 Edge Servers**.

   The **H.323 Edge** page opens.
4. Click the name of the relevant Equinox H.323 Edge server in the list of devices.

   The system displays the **H.323 Edge Server** window.
5. Click the **Configuration** tab.



6. Configure the Equinox H.323 Edge server's settings, as described in Table 23: Configuring the Equinox H.323 Edge server's basic information on page 112.

   You can select the **Restore Factory Defaults** button to set all fields to their factory default values and restart the Equinox H.323 Edge server.

   See *Deployment Guide for Avaya Equinox® H.323 Edge* for more information on the server configuration.

Table 23: Configuring the Equinox H.323 Edge server's basic information

Section Name	Field Name	Description
Gatekeeper Settings	**Gatekeeper Address**	The IP address of the gatekeeper, used to serve all H.323 calls.
	Gatekeeper Port	The port number of the gatekeeper.
NAT Support	**Enabled**	Select to enable NAT support.
	Public IP Address	The IP address used by external access.

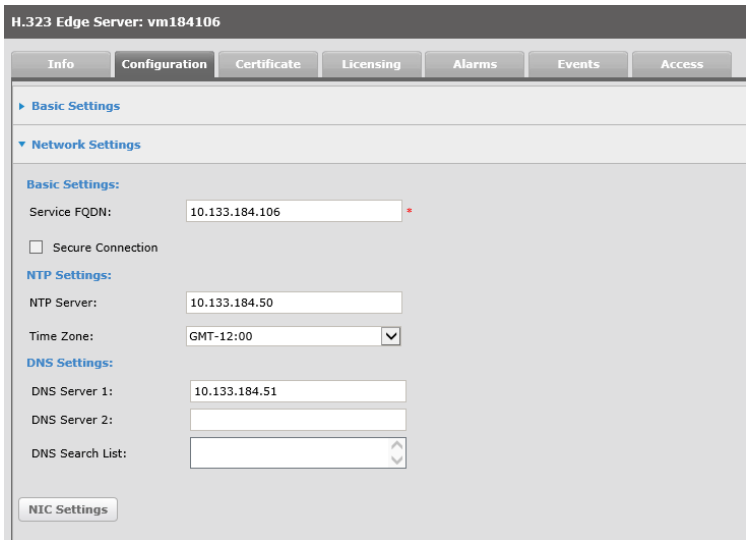
Table continues…

Section Name	Field Name	Description
Logging	**Log Level**	Select the level of the logs to be generated. Select from the following options: • Detailed • Warning • Error • Disabled
Management Session	**Secure XML connection using TLS**	Select to run an XML API using TLS, and for Equinox Management to secure the XML connection. Equinox H.323 Edge runs its XML API service on TLS, and Equinox Management has to connect to Equinox H.323 Edge via TLS. Otherwise, Equinox Management has to connect to the Equinox H.323 Edge server by TLS instead of TCP.
	Timeout	The session timeout value (in ms) for the connection between the Equinox H.323 Edge server and Equinox Management. When no message is exchanged over the connection, the connection is terminated when the session is idle for the indicated amount of time.
NTP Configuration	**NTP Server Address**	The IP address of the NTP server with which the Equinox H.323 Edge server synchronizes its local time.
URI Dialing Settings	**Local Domain Name**	The local domain name of the Equinox H.323 Edge server URI.
	Strip Domain Name	When selected, the Equinox H.323 Edge server removes the domain portion (hostport) of the URI dialing string if a URI call request arrives and the Equinox H.323 Edge server and the domain name in the URI dialing string match the configured **Local Domain Name**. Only the user portion of the string is retained before transferring the call request to the Gatekeeper. When not selected, the URI dialing string remains as it is in this scenario.
Direct Public Access	**Enabled**	Select to assign the **Public Access Proxy Address** displayed in the **Info** tab as the **PaProxy Call Signal Address**, even though a public Equinox H.323 Edge server is connected. Otherwise, it displays the relevant address introduced by the public PFC (or the internal PFS IP with a port number “0” if no public PFC is connected). When not selected, the relevant address introduced by the public Equinox H.323 Edge server is used. If no Equinox H.323 Edge server is connected, the internal Equinox H.323 Edge server IP with port number **0** is used.

Table continues…

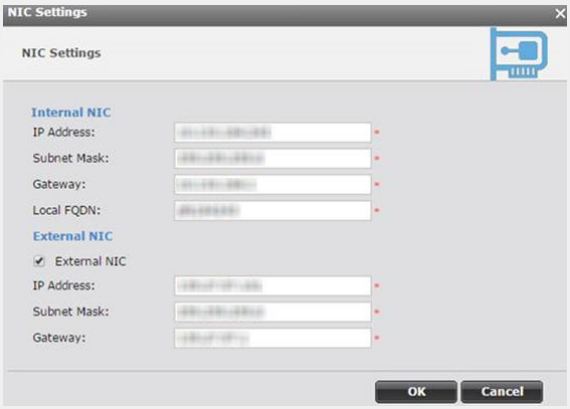
Section Name	Field Name	Description
	Default Extension	The default extension that is reached when dialing the Equinox H.323 Edge server, when an extension is not specified.
	Port Range Minimum Port	The lowest number port available on the Equinox H.323 Edge server.
	Port Range Maximum Port	The highest number port available on the Equinox H.323 Edge server.
Internal Communication	**Internal Port Range Minimum Port**	The lowest number port available for internal communication on the Equinox H.323 Edge server.
	Internal Port Range Maximum Port	The highest number port available for internal communication on the Equinox H.323 Edge server.
	Agnostic Outbound IP Call	When selected, the Equinox H.323 Edge server does not check a dialed IP and treats all IP calls as external. When not selected, the Equinox H.323 Edge server listener connects the dialing endpoint to the IP address directly if the IP address is private.

7. Click **Apply**.
8. Expand the **Network Settings** section; the system displays the following:



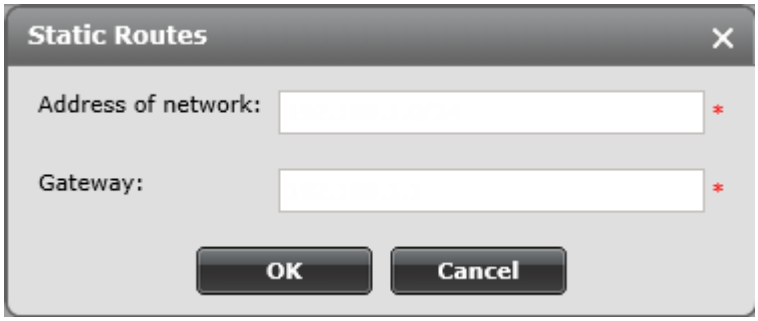
Configure the fields on the page, as described in the following table:

Table 24: Configuring the Equinox H.323 Edge server's basic information

Section Name	Field Name	Description
Basic Settings	**Service FQDN**	The IP address of the gatekeeper, used to serve all H.323 calls.
	Secure Connection	Select to indicate that the connection is secure. You can select this check box only if a media server certificate is configured.
NTP Settings	**NTP Server**	The IP Address of the NTP server.
	Time Zone	The time zone in which the NTP server is located.
Network Settings	**DNS Server 1**	The IP address of the DNS server.
	DNS Server 2	The IP Address of the backup DNS server, in the event that DNS Server 1 is not available.
	DNS Search List	Enter the short name of the DNS server when the H.323 Edge server searches other sites. The system searches the DNS search list for the suffix
	NIC Settings	Select to open the **NIC Settings** dialog box, where you configure NIC settings.  Configure the settings for the Internal NIC in the relevant fields. You can select **External NIC** to designate an additional NIC to be responsible for the external network connection. If you do not select **External NIC**, the internal NIC handles both the internal and external network connections.

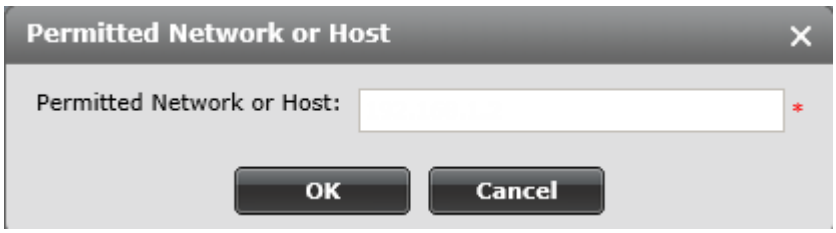
9. Expand the **Static Routes** section to configure routing between H.323 Edge servers, based on IP address and sub mask.
10. Click **Add**.

    The system displays the **Static Routes** dialog box.



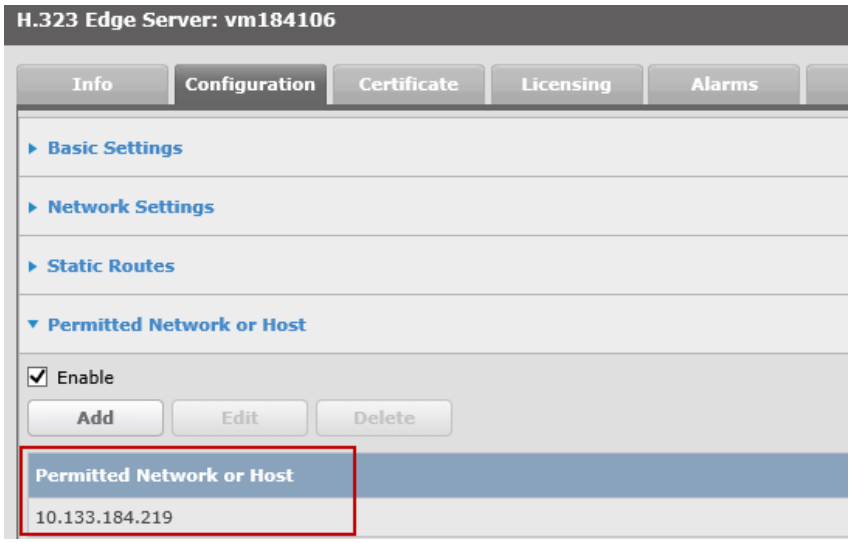
11. Enter the network address and gateway in the relevant fields, and click **OK**.
12. Expand the **Restricted Access List** section to restrict access to the H.323 Edge server, based on IP address and sub mask.
13. Select the **Enable** check box and click the **Add** button.

    The system displays the Permitted Network or Host dialog box.



14. Enter the IP address of the permitted network or host, and click **OK**.

    The system displays the IP address in the **Permitted Network or Host** section of the **Configuration** tab:



Related links

Defining your video network devices on page 58
Creating an Equinox H.323 Edge server cluster on page 117

Deleting an Equinox H.323 Edge server cluster on page 119

Creating an Equinox H.323 Edge server cluster

About this task

You can create a cluster of Equinox H.323 Edge servers. H.323 Edge server clusters enable you to increase your call volume. Equinox Management treats a cluster as if it is a single server, so if you have three servers in a cluster, the cluster can handle three times as many calls as a single H.323 Edge server.

Note:

The built-in virtual machine clustering mechanism relies on a multicast MAC address to distribute the network traffic to all the virtual machines. Typically, network routers and firewalls deny multicast MAC addressing. You might need to update the router and firewall policy for the clustering mechanism to work.

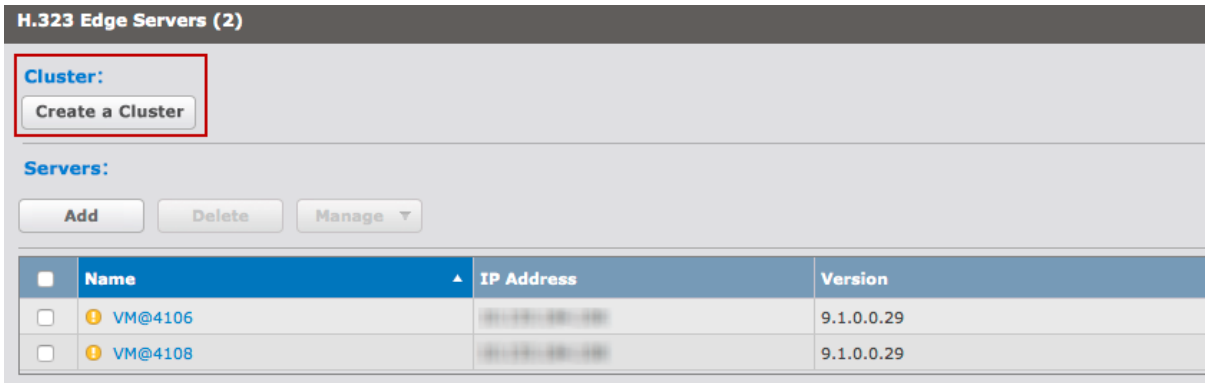
Before you begin

Ensure that you have more than one H.323 Edge server configured in your deployment.

Procedure

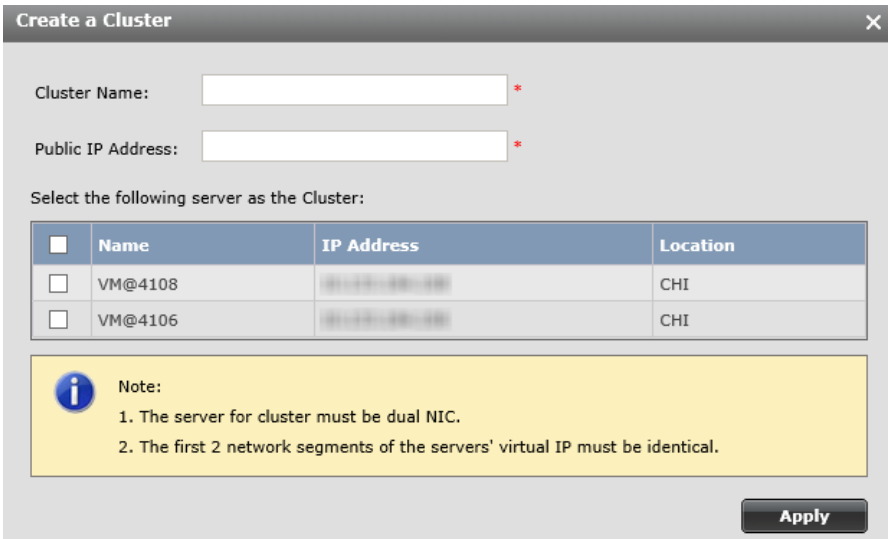
1. Access the Equinox Management administrator portal.
2. Click **Devices** > **Devices by Type** > **Media & Signaling** > **H.323 Edge Servers**.

   The system displays the **H.323 Edge Servers** page.



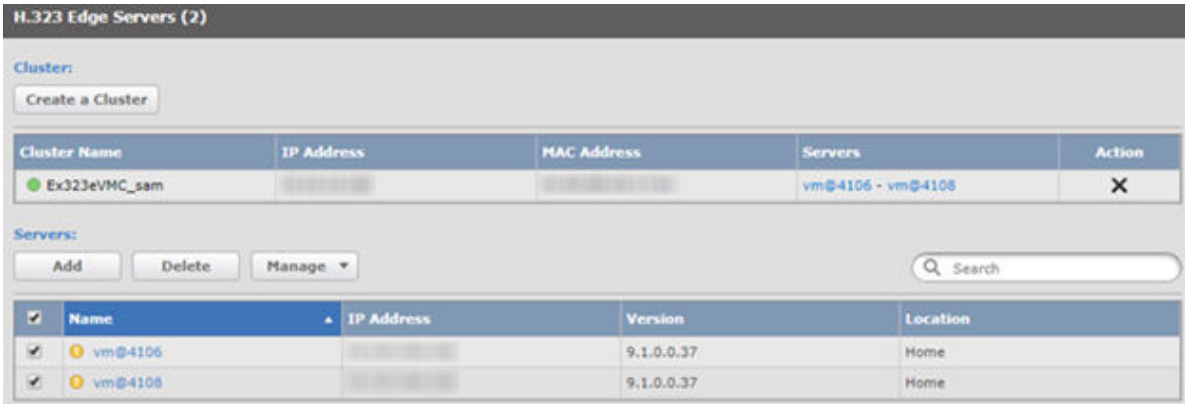
3. Click **Create a Cluster**.

   The system displays the **Create a Cluster** dialog box.



4. Configure a Cluster Name and Public IP Address in the relevant fields, and select the check boxes of the servers you want to add to the cluster.
5. Click **Apply**.

   The system displays the cluster in the list on the **H.323 Edge Servers** page.



A cluster has one of the following statuses:

- **Green**: Normal
- **Yellow**: Alarm

Note:

If the cluster is deployed inside a private address DMZ, the cluster's public IP address must be mapped to an actual global IP address. The global IP address must be configured to the public IP address in the NAT support section of the cluster's H.323 Edge server.

If the cluster is deployed in the public network, the cluster's IP address does not need to be mapped and therefore can be set to the public IP address in the NAT support section of the cluster's H.323 Edge server.

Related links

Remotely configuring the Avaya Equinox® H.323 Edge server on page 111

Deleting an Equinox H.323 Edge server cluster

About this task

You can delete an H.323 Edge server cluster in Equinox Management. You must ensure that all of the cluster's servers are online before deleting the cluster. When deleting a cluster, the servers in the cluster remain in the system, but they no longer exist as a cluster.

Servers that exist in a cluster cannot be deleted from the server list on the **H.323 Edge Servers** page.

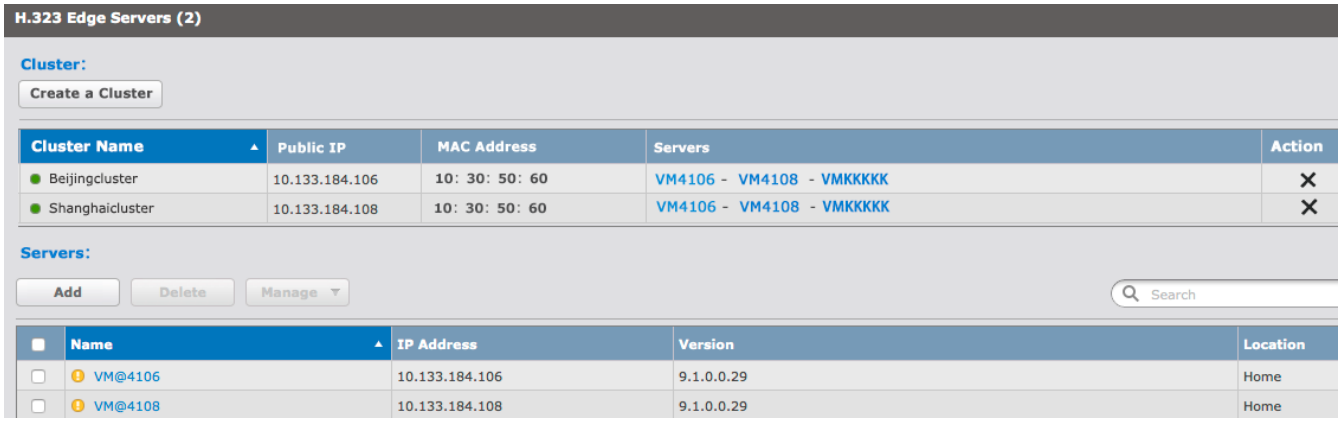
Before you begin

Ensure that you have created an H.323 Edge server cluster, as described in Creating an Equinox H.323 Edge server cluster on page 117.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Devices** > **Devices by Type** > **Media & Signaling** > **H.323 Edge Servers**.

   The system displays the **H.323 Edge Servers** page.



3. In the **Action** column, click the delete icon ✕ for the cluster you want to delete.
4. Click **Yes** in the confirmation dialog box to delete the cluster.

Related links

Remotely configuring the Avaya Equinox® H.323 Edge server on page 111

Planning and configuring endpoints in Equinox Management

Equinox Management supports both Avaya and third-party endpoints. After importing endpoints to Equinox Management, you can configure Equinox Management to manage your endpoints. The main management tasks include the following, depending on the endpoint type:

- Simultaneously upgrading all endpoints (of the same type).
- Controlling your endpoint's bandwidth.
- Configuring your endpoint's resolution settings.
- Configuring your endpoints to display the corporate address book, as described in Using Equinox Management's endpoint directory as a corporate address book on page 159.
- Monitoring your endpoints via alarms and traps sent by Equinox Management.

All Equinox Solution endpoints are automatically managed by Equinox Management. Equinox Management can manage enterprise endpoints protected by a firewall as if they are deployed on the same LAN as Equinox Management.

You can configure Equinox Management to manage the following endpoint types: Avaya IX™ CU360 and Avaya Room System XT Series (see Managing endpoints using Equinox Management on page 141).

When working in Team Engagement (TE) mode, you can view the third-party endpoints that are available to join meetings in progress. This parameter appears on the Dashboard, under **System Information** > **3rd Party Video Connectivity**.

Figure 14: 3rd Party Video Connectivity

You can import endpoints to Equinox Management in the following ways (see Figure 15: Importing endpoints into Equinox Management on page 121):

- Import from the H.350 search base: Use this method for endpoints that are defined in your LDAP server and your LDAP server is configured with an H.350 search base.
- Import from the LDAP server: Use this method when your H.323 endpoints are defined in your LDAP server and your LDAP server is not configured with an H.350 search base.
- Import from the gatekeeper: Use this method to import H.323 endpoints registered to your gatekeeper.

- Add endpoints manually: Use this method to import SIP, ISDN/PTSN, Dual H.320 and H.323, and H.323 endpoints. Endpoints imported manually are automatically managed by Equinox Management.

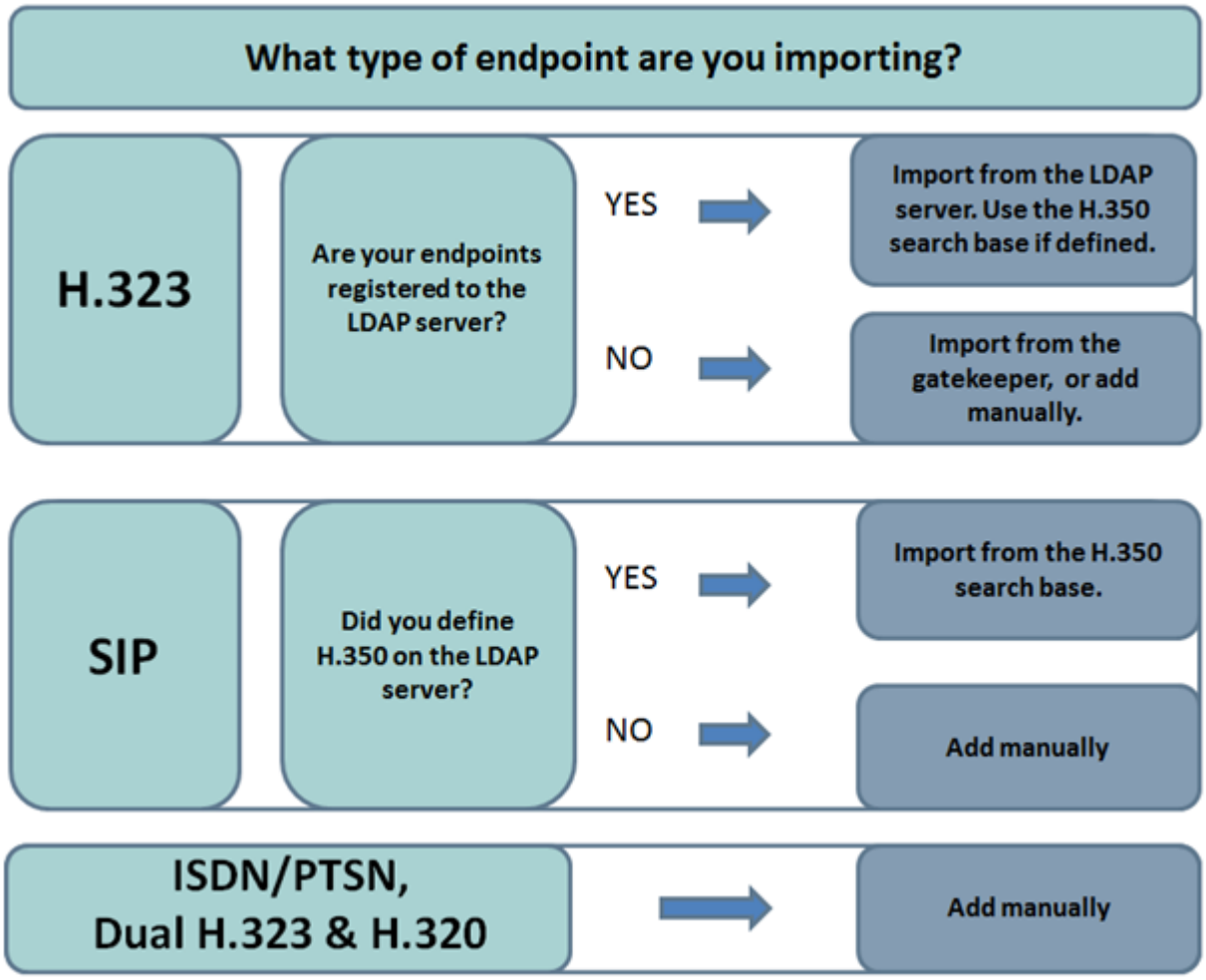


Figure 15: Importing endpoints into Equinox Management

Related links

Defining your video network devices on page 58
Importing H.323 endpoints from the Gatekeeper on page 122
Importing H.323 endpoints from an external LDAP server on page 124
Importing Endpoints from the H.350 search base on page 126
Adding endpoints in Equinox Management manually on page 128
Planning and configuring Telepresence in Equinox Management on page 139
Managing endpoints using Equinox Management on page 141
Provisioning Avaya Room System XT Series endpoints automatically on page 145
Configuring Quality of Service and Encryption settings for an XT Series endpoint in Equinox Management on page 153
Replicating endpoint settings on multiple endpoints on page 155

Using Equinox Management's endpoint directory as a corporate address book on page 159
Managing your endpoint's user directory with LDAP on page 161
Configuring presentation layouts for single-screen endpoints on page 169
Organizing endpoints into groups with labels on page 171

Importing H.323 endpoints from the Gatekeeper

About this task

This procedure describes how to import endpoints registered to H.323 Gatekeeper, Avaya Equinox H.323 Gatekeeper (Equinox Management's internal gatekeeper), or third-party gatekeepers to Equinox Management.

The Avaya Room System XT Series endpoint imported from the gatekeeper is automatically managed by Equinox Management.

This procedure is not relevant for service providers.

Follow this procedure when:

- You want to import multiple or all endpoints registered to the gatekeeper.
- You want all Avaya Room System XT Series endpoints to be automatically managed by Equinox Management.

Managed endpoints communicate with Equinox Management to provide events and alarms management, and store endpoint information. Endpoints that are not managed by Equinox Management only have basic endpoint dialing information needed to call or invite the endpoint to meetings. For more information about managed endpoints, see Managing endpoints using Equinox Management on page 141.

Before you begin

If you are importing endpoints from H.323 Gatekeeper or a third-party gatekeeper, you must first define the gatekeeper, as described in Adding video network devices in Equinox Management on page 61.

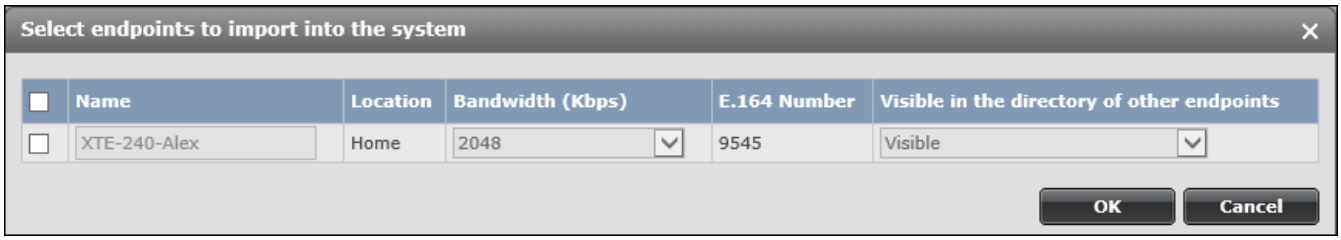
If you are using Avaya Equinox H.323 Gatekeeper, Equinox Management's internal gatekeeper, you do not need to define it before importing endpoints.

Procedure

1. Access the Equinox Management web interface.
2. Click the **Endpoints** tab.
3. Click **Add** > **Import from Gatekeeper**.

   The system displays a gatekeeper list.

4. Select the gatekeeper whose endpoints you would like to import, and select **OK**. A list of all endpoints registered to the gatekeeper that are not already in Equinox Management is displayed.



5. Select the endpoints you want to import.
6. Configure settings for each selected endpoint, as described in Table 25: Configuring endpoint settings on page 123.

   Note:

   The endpoint's dialing information (E.164 number) and location (relevant for distributed or service provider deployments) are retrieved from the gatekeeper.

   XT Series endpoints are automatically managed by Equinox Management.

   Table 25: Configuring endpoint settings

Field Name	Description
Name	The endpoint's name appears, as it is configured in the gatekeeper. If necessary, you can modify the endpoint's name as it is displayed in Equinox Management.
Bandwidth	Define the default maximum bandwidth for the endpoint by selecting bandwidth settings in the list (in Kbps). Equinox Management uses the bandwidth value to reserve resources for this endpoint.
Visible in the directory of other endpoints	To display this endpoint in the corporate address book, select **Display** from the list.

7. Click **OK**.

The system displays a confirmation page, listing the endpoints that were added to Equinox Management. These endpoints are now listed in the **Endpoints** tab.

Important:

If any endpoints were not successfully imported, the system displays them in the list as well, with an explanation of why the import failed.

Related links

Planning and configuring endpoints in Equinox Management on page 120

Importing H.323 endpoints from an external LDAP server

About this task

This procedure describes how to import H.323 endpoints from your external LDAP server. Endpoints are predefined in the LDAP server and can be imported to Equinox Management as room systems and personal endpoints. Follow the procedure described below when:

- Your endpoints are defined in your LDAP server and your LDAP server is not configured with an H.350 search base. If your LDAP server is configured with an H.350 search base, follow the procedure described in Importing Endpoints from the H.350 search base on page 126.
- You are importing endpoints from the LDAP server for the first time. After this initial import, you can add endpoints by just synchronizing Equinox Management with the LDAP server.
- You want to synchronize only endpoints, and not users, in your LDAP directory with Equinox Management.

  To synchronize both users and endpoints in your LDAP server, see Synchronizing users from the LDAP server on page 244.
- You are modifying the endpoints' import settings, such as the E.164 dialing number.

During this procedure, you can define a prefix for endpoints you import (this is optional). The prefix is like an area code which is added to the start of a phone number. In this case, the prefix helps to route a call to a specific endpoint.

Before you begin

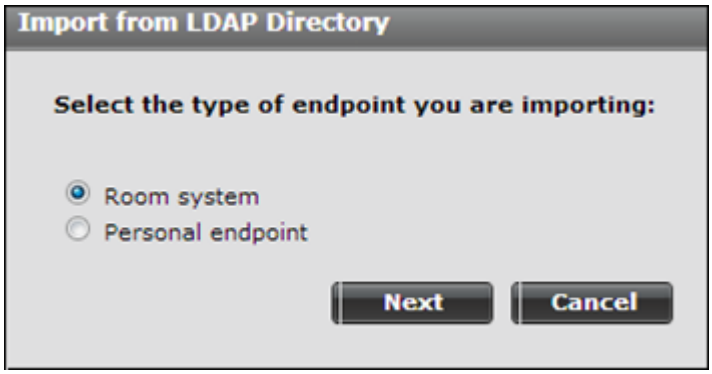
1. Define your LDAP server in Equinox Management, as described in Connecting Equinox Management with the LDAP server on page 239.
2. Synchronize your LDAP server with Equinox Management.

   Otherwise, personal endpoints belonging to users recently added to the LDAP but not listed in Equinox Management, are not imported to Equinox Management.

Procedure

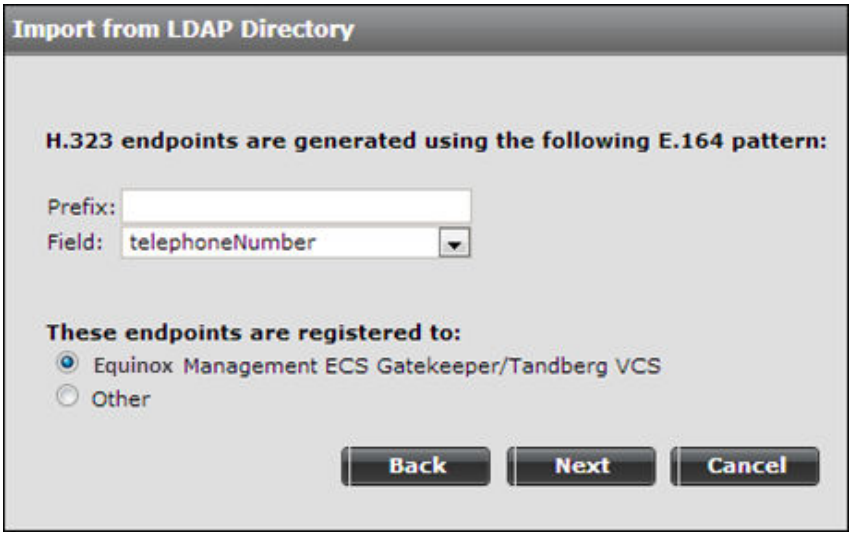
1. Access the Equinox Management administrator portal.
2. Click the **Endpoints** tab.
3. Click **Add** > **Import from LDAP**, and click the LDAP server's IP address in the list.

4. Select the type of endpoint you are importing, as follows:
   - **Room system**: Select this option if you are importing room system endpoints.
   - **Personal endpoint**: Select this option if you are importing personal endpoints.



5. Click **Next**.
6. Select the user group to which you want to assign personal endpoints or import room systems.
7. Click **Next**.

   The system displays the **Import from LDAP Directory** window.



8. Configure the endpoints or room systems, as described in Table 26: Configuring import settings for these endpoints on page 126.

Table 26: Configuring import settings for these endpoints

Field Name	Description
Prefix	If required by your dialing plan, enter a number to use as a prefix for these endpoints. The configured prefix: • Must contain less than 11 digits • Cannot already be used as a prefix for the auto-attendant, auto-routing, or for other deployment components. Personal endpoints cannot have the same prefix as personal virtual rooms, when configuring the same LDAP attribute (such as **telephoneNumber**).
Field	Select the LDAP attribute you want to use to retrieve the endpoint's information from the LDAP server, depending on your organization's dialing plan. The most commonly used attribute is **telephoneNumber**. **Important:** Do not select non-numerical attributes, such as streetAddress or OU.
Those endpoints are registered to	Select the gatekeeper to which the endpoints are registered.

9. Click **Next** > **Finish**.

   The endpoints are added to Equinox Management.

10. Verify that endpoints were downloaded correctly:

    a. Click **Endpoints** > **Imported Endpoints** > **From Active Directory**.

    b. Verify that all endpoints defined in the LDAP server were downloaded and appear in the **Endpoints** tab.

Related links

Planning and configuring endpoints in Equinox Management on page 120

Importing Endpoints from the H.350 search base

About this task

This procedure describes how to import endpoints using your LDAP server's H.350 search base. The H.350 search base allows you to search your LDAP database for users based on videoconferencing-specific attributes. Follow the procedure described below when:

- Your endpoints are defined in your LDAP server and your LDAP server is configured with an H.350 search base.
- You are importing endpoints from the H.350 search base for the first time. After this initial import, you can add endpoints by just synchronizing Equinox Management with the LDAP server.

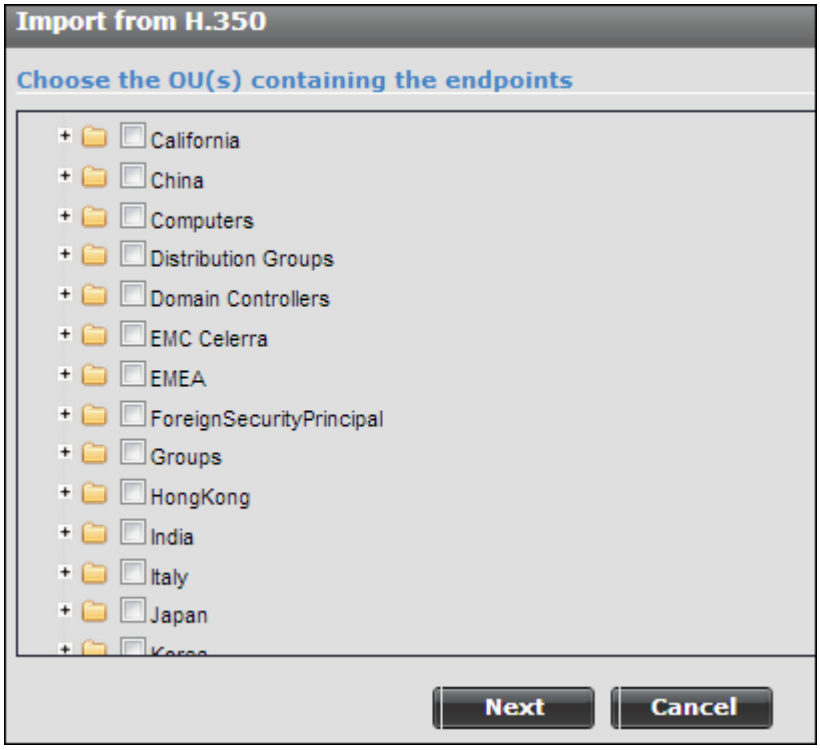
Before you begin

1. Define your LDAP server in Equinox Management, as described in Connecting Equinox Management with the LDAP server on page 239.
2. Define a schema with specific user attributes to be imported from the LDAP server to Equinox Management on your LDAP server. For example, you can define the type of endpoint to be imported, or you can you can define a schema to import endpoints with a specific video profile. In addition, you can define new fields in the LDAP server to add more endpoint details.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Endpoints**.
3. Click **Add** > **Import from H.350**.

   The system displays a tree structure showing all the organizational units (OU) defined on the LDAP server:



4. Select the relevant organizational units (OU) where your endpoints are defined.
5. Click **Next**.
6. Click **Finish**.

Related links

Planning and configuring endpoints in Equinox Management on page 120

Adding endpoints in Equinox Management manually

You can manually add H.323, SIP, and ISDN/PSTN H.320 endpoints to Equinox Management. Endpoints imported manually are automatically managed by Equinox Management. Add endpoints manually when:

- You are adding SIP or ISDN/PSTN H.320 endpoints. If your LDAP server is configured with an H.350 search base, you can import the endpoints as described in Importing Endpoints from the H.350 search base on page 126. Otherwise, you can only add these types of endpoints manually.

  H.323 endpoints can be added manually or imported from the gatekeeper, your LDAP server, or the H.350 search base.

- You are adding endpoints that you want automatically managed by Equinox Management.

  Managed endpoints communicate with Equinox Management to provide events and alarms management, and store endpoint information. Endpoints that are not managed by Equinox Management only have basic endpoint dialing information needed to call or invite the endpoint to meetings. For more information about managed endpoints, see Managing endpoints using Equinox Management on page 141.

Add endpoints to Equinox Management manually, as described in the following procedures:

Related links

Planning and configuring endpoints in Equinox Management on page 120
Adding H.323 IP endpoints on page 128
Adding SIP IP Endpoints on page 130
Adding Telepresence Systems in Equinox Management on page 132
Adding ISDN/PSTN H.320 endpoints on page 136
Adding mobile endpoints on page 138

Adding H.323 IP endpoints

About this task

This procedure describes how to manually import H.323 endpoints registered to gatekeepers that are configured in Equinox Management.

Before you begin

If you are adding endpoints registered to H.323 Gatekeeper or a third-party gatekeeper, you must first define the gatekeeper, as described in Adding video network devices in Equinox Management on page 61.

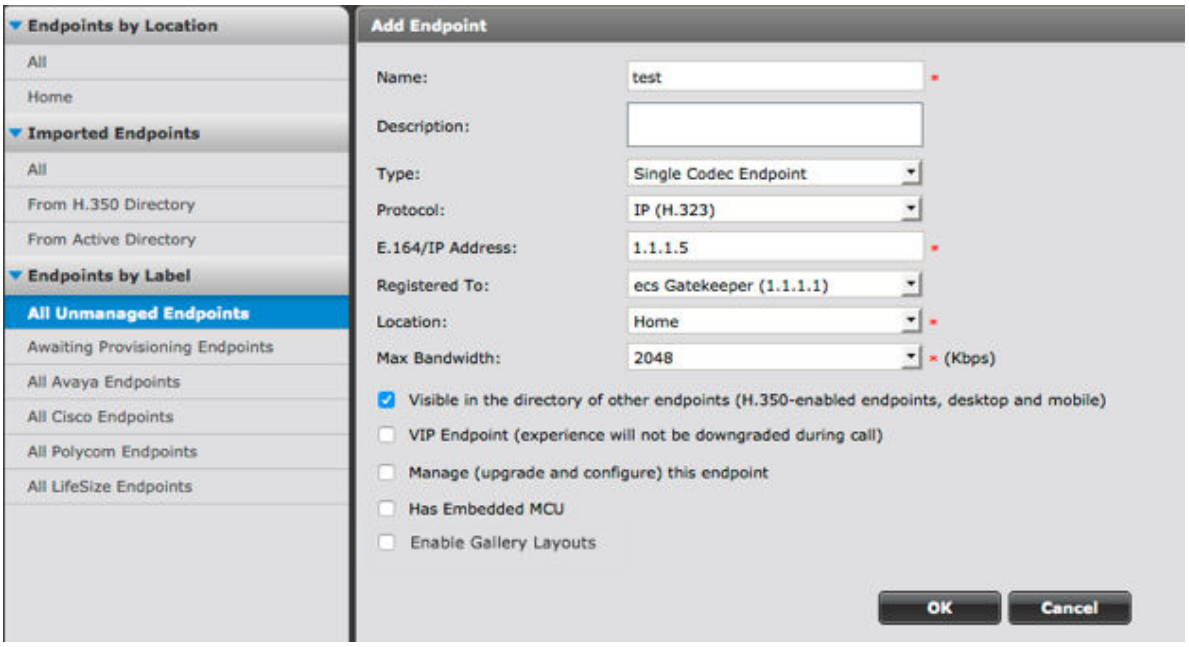
If you are using Avaya Equinox H.323 Gatekeeper, Equinox Management's internal gatekeeper, you do not need to define it before importing endpoints.

Procedure

1. Access the Equinox Management administrator portal.

2. Click the **Endpoints** tab.
3. Click **Add** > **Add manually**.

   The system displays the **Add Endpoint** dialog box.



4. Configure your endpoint as described in Table 27: Adding H.323 endpoints on page 129.

Table 27: Adding H.323 endpoints

Field Name	Description
Name	Enter a name used to identify the endpoint. This the name displayed in the list of endpoints.
Description	Enter any description text that you may have for this endpoint.
Type	Select the model of the endpoint.
Protocol	Select **IP(H.323)** from the list.
E.164/IP Address	Enter one of the following: • If the endpoint is registered to a gatekeeper, enter the E.164 number of the endpoint. • If the endpoint is not registered to a gatekeeper, enter the IP address of the endpoint.

Table continues…

Field Name	Description
Manage (upgrade and configure) this endpoint	Select to manage this endpoint using Equinox Management. If selected, you can configure the endpoint and upgrade its software via Equinox Management. When selecting this option, the following fields appear: • **Management IP Address**: Enter the IP address of the endpoint • **Model**: Select the endpoint model
Registered To	Select the gatekeeper to which the endpoint is registered. If you select **None**, the endpoint can be added to Equinox Management but is not connected until you register the endpoint with the gatekeeper, and select the gatekeeper here.
Location	Select the location or organization (in service provider deployments) of the endpoint, from the list. The **Location** field is visible only for distributed and service provider deployments.
Max IP Bandwidth	Define the default maximum bandwidth for the endpoint by selecting bandwidth settings in the list (in Kbps). Equinox Management uses the bandwidth value to reserve resources for this endpoint.
Visible in the directory of other endpoints	Select to display this endpoint in the corporate address book.
VIP Endpoint	Select to indicate that this is an important endpoint whose video resolution should not be scaled down to below HD quality even when the available effective bandwidth is less than optimal. A VIP endpoint is marked with this icon VIP. This option is only available when the effective available bandwidth is above 1800 Kbps.
Has embedded MCU	Select if the endpoint has a built-in MCU.
Enable Gallery Layouts	Select to enable support of gallery layout for the endpoint.

5. Click **Apply** to save your changes.

Related links

Adding endpoints in Equinox Management manually on page 128

Adding SIP IP Endpoints

About this task

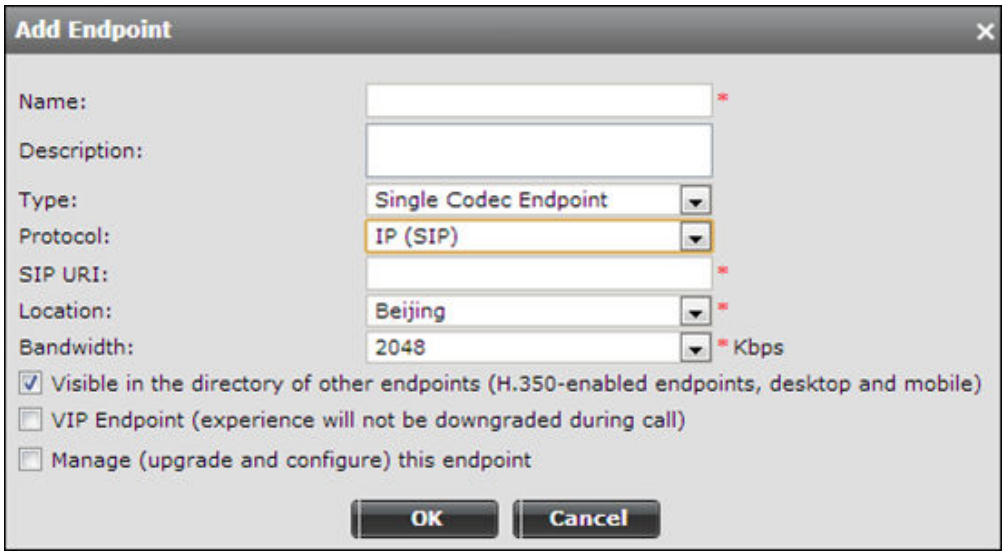
This procedure describes how to manually import SIP endpoints into Equinox Management.

Procedure

1. Access the Equinox Management web browser interface.

2. Click the **Endpoints** tab.
3. Click **Add** > **Add manually**.

   The system displays the **Add Endpoint** dialog box.



4. Configure your endpoint as described in Table 28: Adding SIP endpoints on page 131.

Table 28: Adding SIP endpoints

Field Name	Description
Name	Enter a name used to identify the endpoint. This the name displayed in the list of endpoints.
Description	Enter description text for this endpoint.
Type	Select the endpoint type.
Protocol	Select **IP(SIP)** from the list.
SIP URI	Define the endpoint name or endpoint number, followed by the SIP server domain name and a suffix derived from the domain name of the SIP server. For example, *<terminal name>@<SIP server domain name> or "user@domain_name.com"*.
Location	Select the location or organization (in service provider deployments) of the endpoint, from the list. The **Location** field is visible only for distributed and service provider deployments.
Bandwidth	Define the default maximum bandwidth for the endpoint by selecting bandwidth settings in the list (in Kbps). Equinox Management uses the bandwidth value to reserve resources for this endpoint.

Table continues…

Field Name	Description
Visible in the directory of other endpoints	Select to display this endpoint in the corporate address book.
VIP Endpoint	Select to indicate that this is an important endpoint whose video resolution should not be scaled down to below HD quality even when the available effective bandwidth is less than optimal. This option is only available when the effective available bandwidth is above 1800 Kbps.
Manage (upgrade and configure) this endpoint	Select to manage this endpoint using Equinox Management. If selected, you can configure the endpoint and upgrade its software via Equinox Management. When selecting this option, the following fields appear: • **Management IP Address**: Enter the IP address of the endpoint • **Model**: Select the endpoint model

5. Click **Apply** to save your changes.

Related links

Adding endpoints in Equinox Management manually on page 128

Adding Telepresence Systems in Equinox Management

About this task

Avaya XT Telepresence is a videoconferencing system which is used to create video meetings with a telepresence effect.

There are telepresence systems that can be assembled using regular single endpoints; for example, Avaya XT Telepresence can use three Avaya XT5000 Series endpoints (see Planning and configuring Telepresence in Equinox Management on page 139).

Unlike other endpoints, you must always add telepresence systems to Equinox Management manually. You need to integrate the Avaya XT Telepresence with the Equinox Management to add it as a resource to your video network.

If you use regular endpoints to create a telepresence system, define them in Avaya Equinox® Management as components of the telepresence system, not as single endpoints. You cannot directly change an existing single endpoint in Avaya Equinox® Management into a telepresence endpoint, and vice versa.

If your organization uses an LDAP directory, only the primary endpoint should be defined in the LDAP directory.

Your telepresence system's primary endpoint depends on the system's configuration. Typically, the primary endpoint is defined as follows:

- Telepresence systems with three monitors, such as Avaya XT Telepresence: the central monitor
- Telepresence systems with two monitors: the left monitor
- Telepresence systems with four endpoints: the left-central monitor

Before you begin

- Ensure the gatekeeper to which you registered your telepresence system is defined and configured in Equinox Management.
- If the endpoints you want to define as part of your telepresence system already exist in Equinox Management as separate single endpoints, you must delete them. You then redefine these endpoints as part of your telepresence system, as described in the procedure below.
- If your organization uses the LDAP directory and the endpoints forming the telepresence system are defined there, we strongly recommend that you define only the primary endpoint in your LDAP directory and remove non-primary endpoints from it.

Procedure

1. Access the Equinox Management administrator portal.
2. Click the **Endpoints** tab.
3. Click **Add** > **Add manually**.

   The system displays the **Add Endpoint** window. See Figure 16: Example of the Add Endpoint window as it appears for a Avaya XT Telepresence endpoint on page 133 and Figure 17: Example of the Add Endpoint window as it appears for a Cisco CTS on page 134.

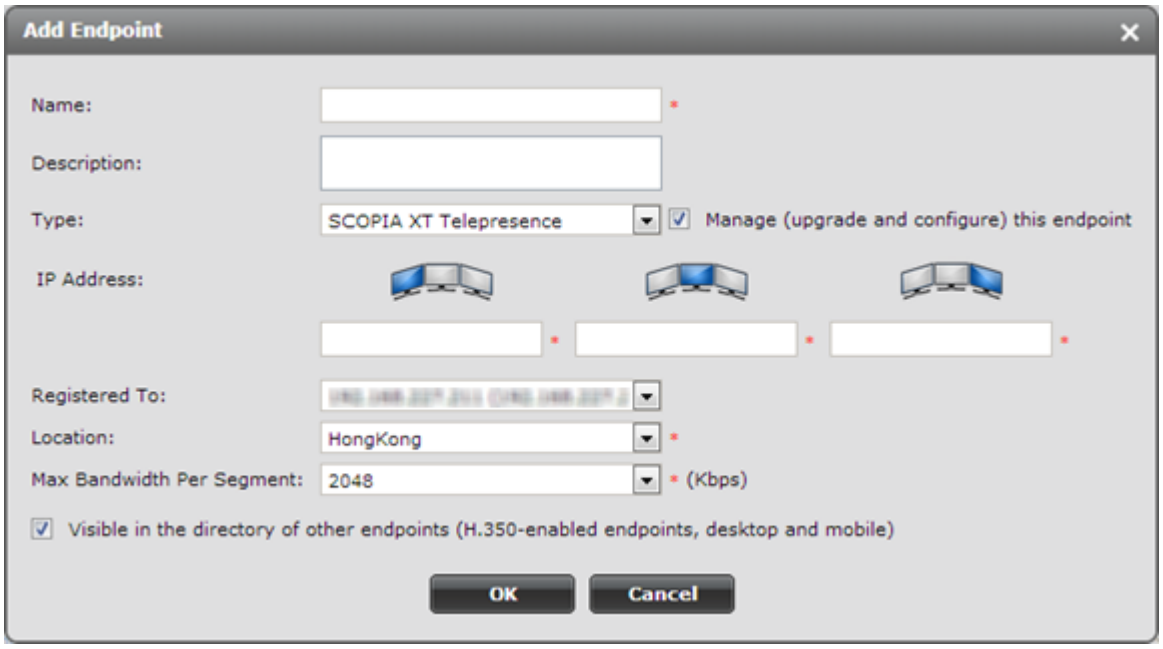


Figure 16: Example of the Add Endpoint window as it appears for a Avaya XT Telepresence endpoint

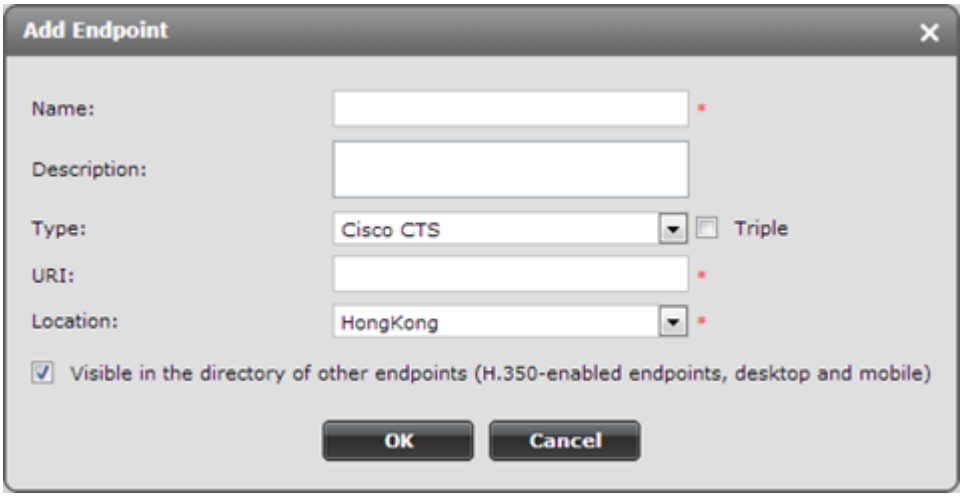


Figure 17: Example of the Add Endpoint window as it appears for a Cisco CTS

4. Configure your telepresence endpoint, as described in Table 29: Configuring telepresence endpoints on page 134.

   Important:

   The settings you need to configure vary, depending on the model of the telepresence system you are adding.

Table 29: Configuring telepresence endpoints

Field Name	Description
Name	Enter a name used to identify the telepresence system as a whole. This is the name displayed in the list of endpoints.
Description	Enter description text for this endpoint.
Type	Select the telepresence system. If your telepresence endpoint has three monitors and is not listed, select **Generic Telepresence**.
Cameras are cross-connected	Select this check box for systems where the left camera is connected to the right codec and visa versa.
Triple	Select this check box if you are adding a Cisco 3-monitor CTS-3000 Series endpoint to the deployment.
Required Gatekeeper	Select the gatekeeper to which the telepresence system is registered. If you select **None**, you can add the endpoint to Equinox Management but it will not be connected until you register the endpoint with the gatekeeper, and then select the gatekeeper here.

Table continues…

Field Name	Description
Location	A location is a physical space (building) or a network (subnet) where video devices can share a single set of addresses. A distributed deployment places these components in different locations, often connected via a VPN. This is relevant only for deployments with multiple locations. Select the location of the telepresence system from the list of locations you defined earlier in Equinox Management.
Max Bandwidth per Segment	Equinox Management uses the bandwidth value to reserve resources for this endpoint. Enter the default maximum bandwidth for a single codec in the telepresence system. For example, for the telepresence system to use 6144 Kbps, define 2048 Kbps for one codec. When there is enough bandwidth available, video is displayed in the highest possible resolution. This value is also subject to the bandwidth settings of the meeting type (MCU service) used in a meeting.
Visible in the directory of other endpoints	Select to display the telepresence system in the corporate address book. The telepresence endpoint is represented in the address book as a single endpoint. The number which the system displays is the number assigned to the primary monitor. The following solution components can access the telepresence system via this single entry: • Equinox Management • XT Series • Avaya Meeting Scheduler Outlook Add-in • Room systems via H.350 • Cisco telepresence devices
IP Address	Enter the IP address for all components in these cases: • If this telepresence system is not registered to a gatekeeper Or • If you want Equinox Management to manage this telepresence system
Prefix	If you are adding a Cisco CTMS telepresence endpoint, enter the prefix. A dial prefix is a number added at the beginning of a dial string to route it to the correct destination, or to determine the type of call.

Table continues…

Field Name	Description
URI	If you are adding a Cisco CTS telepresence endpoint, enter the URI. URI is an address format where the address consists of the endpoint's name or number, followed by the domain name of the server to which the endpoint is registered, such as <endpoint name>@<server_domain_name>.

5. Click **OK**.

   The telepresence system appears on the **Endpoints** tab. The telepresence icon indicates that the type of the endpoint is telepresence. The **Dialing Info** field shows the E.164, the URI or the IP address of the primary component of the telepresence system.

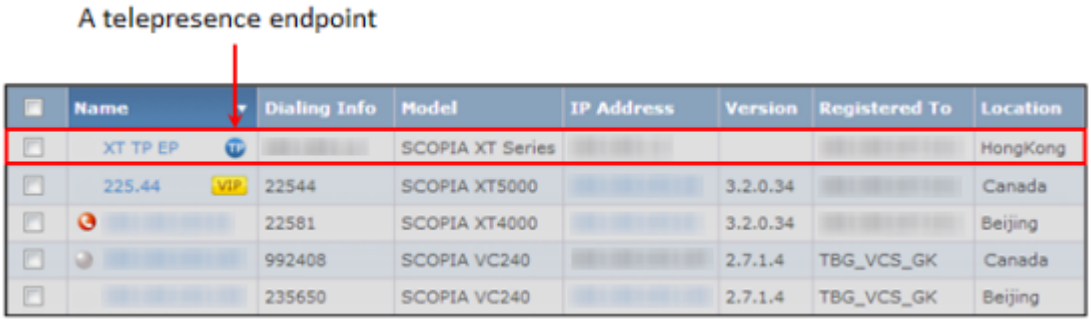


Figure 18: Example of a telepresence endpoint on the Endpoints tab

Related links

Adding endpoints in Equinox Management manually on page 128

Adding ISDN/PSTN H.320 endpoints

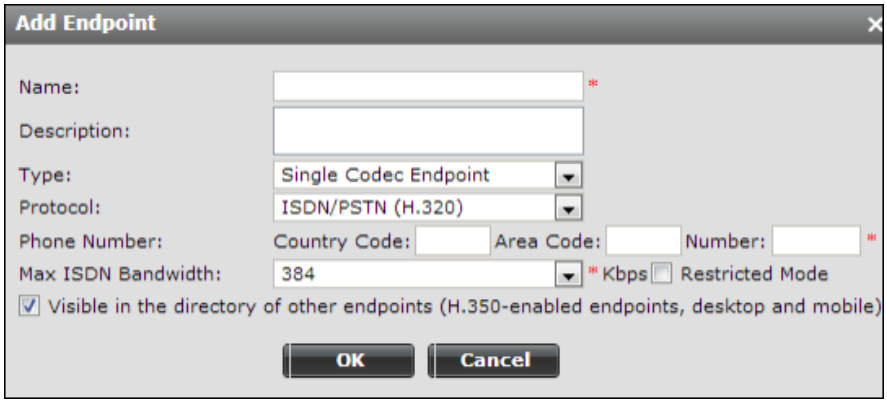
About this task

This procedure describes how to manually import H.320 endpoints that you want Equinox Management to automatically invite to a meeting and manage their availability.

Procedure

1. Access the Equinox Management administrator portal.
2. Click the **Endpoints** tab.
3. Click **Add** > **Add manually**.

   The system displays the **Add Endpoint** dialog box.



4. Configure your endpoint as described in Table 30: Adding ISDN/PSTN H.320 endpoints on page 137.

Table 30: Adding ISDN/PSTN H.320 endpoints

Field Name	Description
Name	Enter a name used to identify the endpoint. This the name displayed in the list of endpoints.
Description	Enter any description text that you may have for this endpoint.
Type	Select the endpoint type.
Protocol	Select **ISDN/PSTN(H.320)** from the list.
Phone Number	Enter the complete phone number of the endpoint in the **Country Code**, **Area Code** and **Number** fields. If you do not specify this information, Equinox Management cannot find the optimal gateway for the endpoint when scheduling a conference.
Max ISDN Bandwidth	Define the default maximum bandwidth for the endpoint by selecting bandwidth settings in the list (in Kbps). Equinox Management uses the bandwidth value to reserve resources for this endpoint.
Restricted Mode	Restricted mode is used for ISDN endpoints only, when the PBX and line uses a restricted form of communication, reserving the top 8k of each packet for control data only. If enabled, the bandwidth values on these lines are in multiples of 56kbps, instead of multiples of 64kbps.
Visible in the directory of other endpoints	Select to display this endpoint in the corporate address book.

5. Click **Apply** to save your changes.

Related links

Adding endpoints in Equinox Management manually on page 128

Adding mobile endpoints

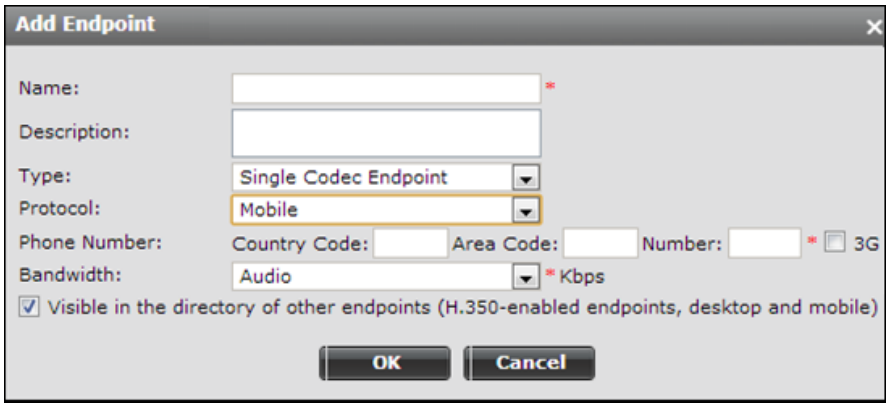
About this task

This procedure describes how to manually import mobile endpoints that you want Equinox Management to automatically invite to a meeting and manage their availability.

Procedure

1. Access the Equinox Management administrator portal.
2. Click the **Endpoints** tab.
3. Click **Add** > **Add manually**.

   The system displays the **Add Endpoint** dialog box.



4. Configure your endpoint as described in Table 31: Adding mobile endpoints on page 138.

Table 31: Adding mobile endpoints

Field Name	Description
Name	Enter a name used to identify the endpoint. This the name displayed in the list of endpoints.
Description	Enter description text for this endpoint.
Type	Select the endpoint type.
Protocol	Select **Mobile** from the list.
Phone Number	Enter the complete phone number of the endpoint in the **Country Code**, **Area Code** and **Number** fields. Select **3G** for 3G endpoints. If you do not specify this information, Equinox Management cannot find the optimal gateway for the endpoint when scheduling a conference.
Bandwidth	Define the default maximum bandwidth for the endpoint by selecting bandwidth settings in the list (in Kbps). Equinox Management uses the bandwidth value to reserve resources for this endpoint.

Table continues…

Field Name	Description
Visible in the directory of other endpoints	Select to display this endpoint in the corporate address book.

5. Click **Apply** to save your changes.

Related links

Adding endpoints in Equinox Management manually on page 128

Planning and configuring Telepresence in Equinox Management

Avaya XT Telepresence is a videoconferencing system which is used to create video meetings with a telepresence effect. A telepresence system consists of two or more endpoints which work together to create a wider image, creating a simulated experience of participants being present in the same room.

With telepresence interoperability support, Equinox Management can establish connections with third-party telepresence systems from Cisco, Logitech/LifeSize, Polycom and Tandberg, allowing telepresence users to view all meeting participants in a videoconference, including those on traditional videoconferencing systems or telepresence systems from other vendors.

Note the following restrictions and guidelines:

- Telepresence is supported only for IP (H.323) endpoints.
- When there is enough bandwidth available, video is displayed in the highest possible resolution.
- Telepresence endpoints cannot be associated with a specific user.
- Telepresence endpoints cannot be set as VIP (an important endpoint whose video resolution is not scaled down to below HD quality even when the available effective bandwidth is less than optimal).
- In cascaded meetings, telepresence endpoints always connect to the Master MCU. For more information about cascaded meetings, see Increasing MCU capacity by cascading multiple MCUs on page 85.

To add telepresence systems to Equinox Management, see Adding Telepresence Systems in Equinox Management on page 132.

The Scopia Elite MCU and Equinox Management support the following telepresence (TP) systems:

- Avaya XT Telepresence
- Polycom ATX 300
- Polycom RPX 200
- Polycom RPX 400
- Polycom TPX HD 306

- Tandberg T3
- LifeSize Conference
- Cisco CTS
- Cisco CTMS
- Generic (other telepresence endpoints that have 3 screens)

Equinox Management does not require any specific license for supporting telepresence, but is aware of the Scopia Elite MCU telepresence license to deliver warning messages to administrators and for display purposes.

Related links

Planning and configuring endpoints in Equinox Management on page 120
Hosting Telepresence Meetings on page 140
Calculating Resources for Telepresence on page 140
Scheduling Telepresence Systems on page 141

Hosting Telepresence Meetings

Telepresence meetings are managed by Equinox Management and hosted by the MCUs in the network. Equinox Management assigns MCUs to telepresence meetings according to the network deployment:

- In mixed deployments with both telepresence enabled MCUs and telepresence disabled MCUs, Equinox Management chooses the MCU host according to the endpoint specifications.
- In centralized deployments with telepresence meetings, Equinox Management chooses a telepresence enabled MCU. For centralized deployments with non-telepresence meetings, Equinox Management gives preference to an MCU with no telepresence support. If there are no resources on the non-telepresence MCU, it uses a telepresence enabled MCU.
- In distributed deployments with telepresence meetings, Equinox Management chooses a telepresence enabled MCU according to the best location. For distributed deployments in non-telepresence meetings, Equinox Management chooses the best MCU according to location, even if the MCU is telepresence enabled; location has a higher priority than telepresence.

Related links

Planning and configuring Telepresence in Equinox Management on page 139

Calculating Resources for Telepresence

Resources are calculated according to the number of supported screens.

For example: For scheduled telepresence endpoints which have two screens, Equinox Management calculates 2 HD ports. For scheduled telepresence endpoints which have four screens, Equinox Management calculates 4 HD ports.

If a telepresence system is dialing into the system (which can be done from each one of the pre-configured numbers), Equinox Management attempts to allocate the total number of ports on the master conference, and if managed to do so, it authorizes to connect the call.

Related links

Planning and configuring Telepresence in Equinox Management on page 139

Scheduling Telepresence Systems

When scheduling a telepresence system, the following restrictions apply:

- Enabled telepresence MCU must be selected.
- Telepresence must be scheduled to the master conference.
- Pre-positioning the telepresence endpoint in a specific sub frame is not supported for the telepresence endpoint.

Related links

Planning and configuring Telepresence in Equinox Management on page 139

Managing endpoints using Equinox Management

About this task

This procedure describes how to manually set endpoints to be managed by Equinox Management. Follow the procedure below to manage endpoints that were imported from the LDAP server or H.350 search base, or manually added endpoints that were not configured to be managed by Equinox Management at the time they were added.

Equinox Management can manage the following endpoint types: Avaya IX™ CU360 and Avaya Room System XT Series.

By default, all Equinox Solution endpoints are automatically managed by Equinox Management, provided they are registered to a gatekeeper defined in Equinox Management.

The main management tasks include the following:

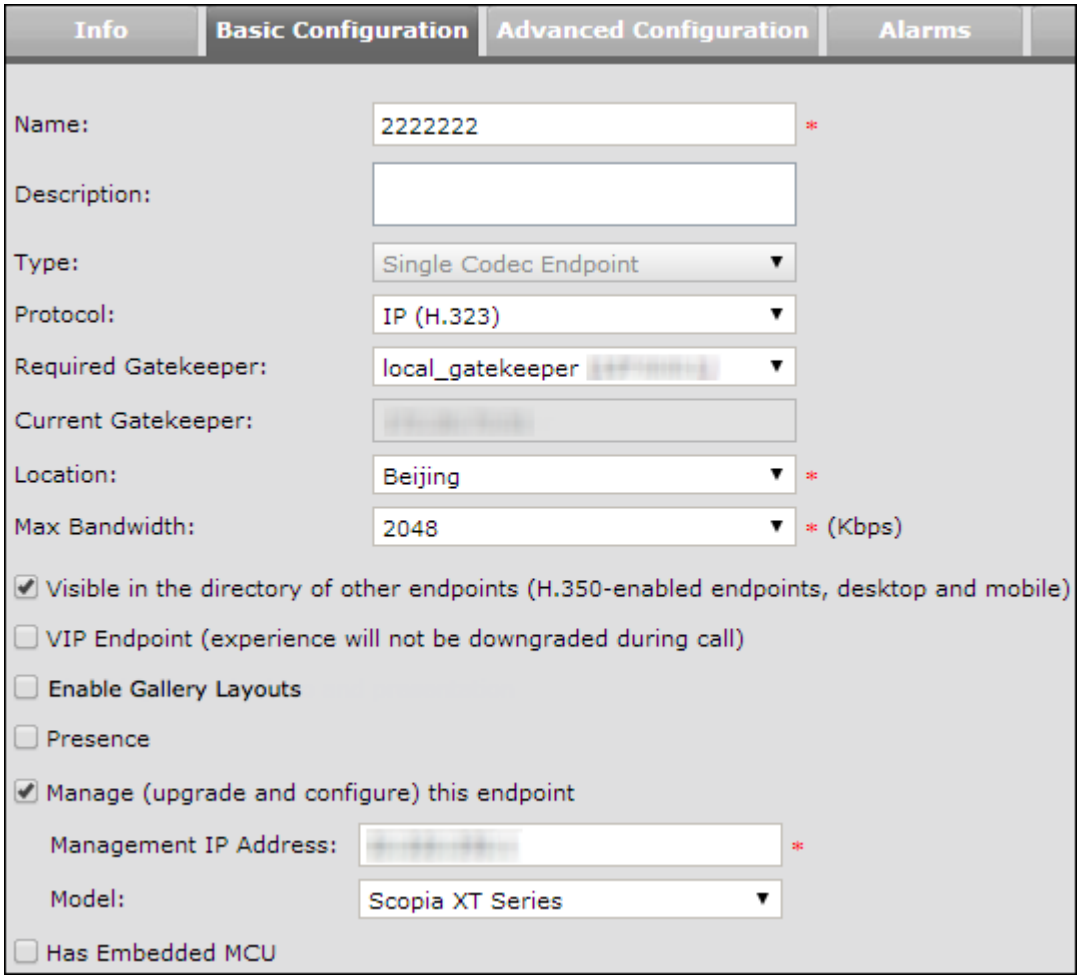
- Simultaneously upgrading all endpoints of the same type.

  To quickly select all endpoints for simultaneous upgrades, you can assign labels to all endpoints of the same type. For details, see Organizing endpoints into groups with labels on page 171.
- Controlling your endpoint's bandwidth.
- Configuring your endpoint's resolution settings.
- Configuring your endpoints to display the corporate address book, as described in Configuring endpoints to be displayed in the corporate address book on page 160.
- Monitoring your endpoints via alarms and traps sent by Equinox Management.

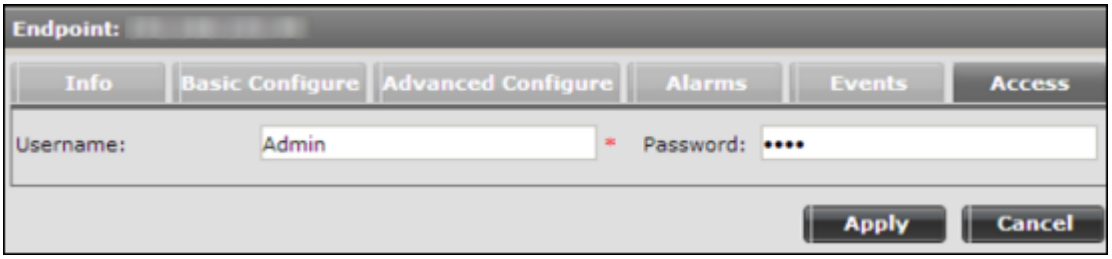
Procedure

1. Access the Equinox Management administrator portal.

2. Click the **Endpoints** tab.
3. Select the endpoint you want to manage.
4. Click the **Basic Configuration** tab.



5. Select **Manage (upgrade and configure) this endpoint**.
6. Click **Apply**.
7. Click the **Access** tab.



8. Enter the username and password for the endpoint's web interface login.

9. Click **Apply**.

Related links

Planning and configuring endpoints in Equinox Management on page 120
Configuring Remote Access to an XT Series Endpoint in Equinox Management on page 143
Configuring an XT Series endpoint for mobile link support on page 144

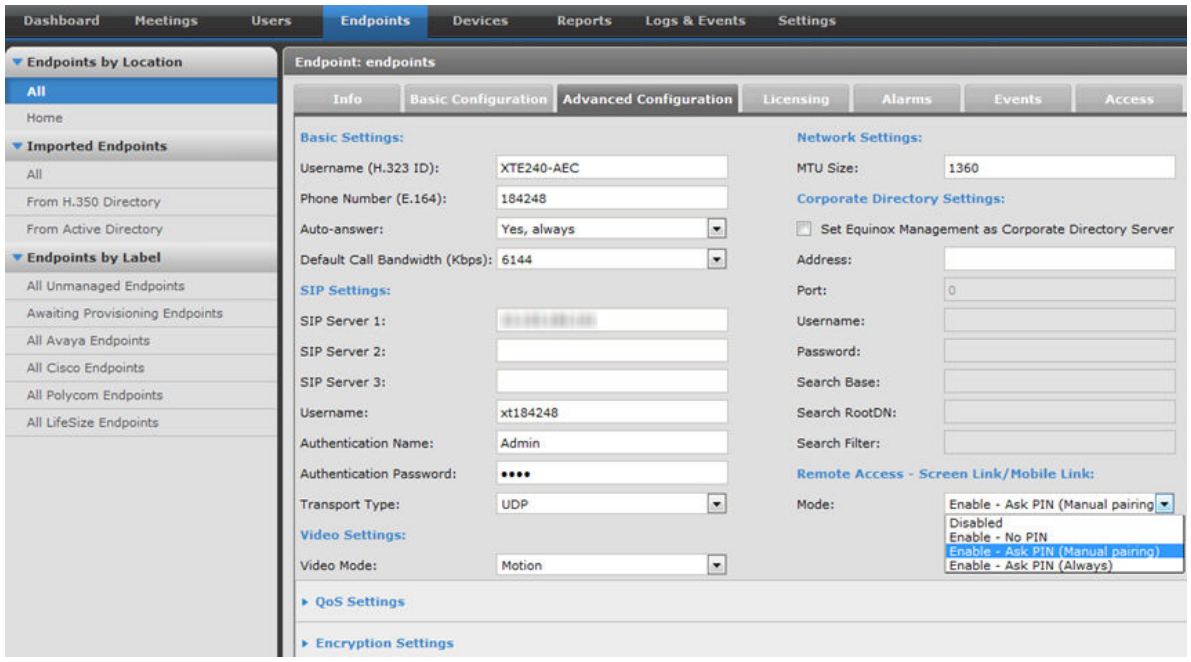
Configuring Remote Access to an XT Series Endpoint in Equinox Management

About this task

This procedure describes how to configure XT Series endpoints so that you can remotely access them in the middle of a videoconference. You can either remotely use the endpoint to share your screen (screen link) or you can remotely take over the XT from your device (mobile link).

Procedure

1. Access the Equinox Management administrator portal.
2. Click the **Endpoints** tab.
3. Click the endpoint you want to configure.
4. Click the **Advanced Configuration** tab.



5. In the **Remote Access** section, select **Mode**.
6. Select one of the following options:
   - **Disabled**: Disables the remote access feature.
   - **Enable — No PIN**: Enables users to automatically access the endpoint remotely without a PIN.

- **Enable — Ask PIN (Manual Pairing)**: Requires users to enter a PIN only when accessing the endpoint manually.
- **Enable — Ask PIN (Always)**: Always requires users to enter a PIN when accessing the endpoint remotely.

7. Click **Apply**.

Related links

Managing endpoints using Equinox Management on page 141

Configuring an XT Series endpoint for mobile link support

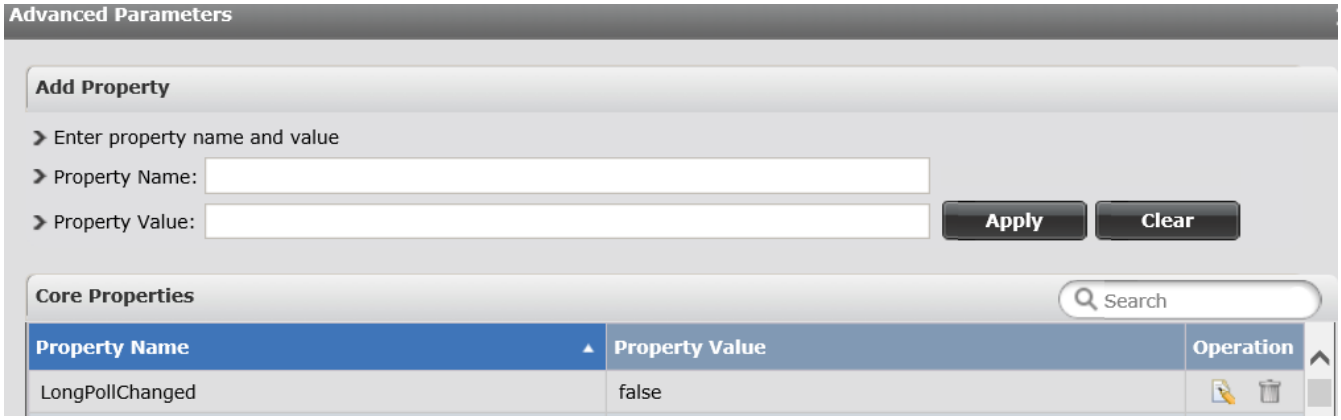
About this task

If all XT endpoints are configured in an internal network, mobile link support is enabled by default (no additional configuration is necessary). However, if there are XT endpoints which are deployed in a public, home, or external private network, the settings described below must be configured.

Procedure

1. Access the Equinox Management administrator portal.
2. Click ≡ > **Advanced Parameters**.

   The system displays the **Advanced Parameters** dialog box.



3. Configure the following parameters: `com.radvision.airpair.forceuseproxyIP=true` and `com.radvision.airpair.proxyIP=x.x.x.x` where `x.x.x.x` is a reverse proxy IP which can be accessed by both an internal and external XT endpoint.

   The reverse proxy must support the following forwarding rule: Forward URL `https://x.x.x.x:443/scopia/icmhttpopenproxy` to `https://iview_IP_address/scopia/icmhttpopenproxy`.

Related links

Managing endpoints using Equinox Management on page 141

Provisioning Avaya Room System XT Series endpoints automatically

About this task

You can provision an Avaya Room System XT Series endpoint remotely, so that the customer can receive the endpoint and set it up without any technical knowledge or intervention from the Support team. During auto-provisioning, a service code is generated in Equinox Management to identify the XT Series as a managed endpoint. When this service code is inserted into the XT Series endpoint, the endpoint uses this service code to connect to a cloud service, to establish communication with the relevant Equinox Management server.

This feature is supported for an endpoint installed in any location, provided you:

- Have a compatible Equinox Management available for association with the endpoint.
- Enable the auto-provisioning endpoint feature on Equinox Management.
- Connect the endpoint to the Internet.
- Enable your DHCP server to assign a valid DNS address to the endpoint.

This method of endpoint management is called cloud mode. In cloud mode, the endpoint connects using a secure web socket to Equinox Management for services such as configuration, LDAP, upgrades, meeting scheduling, and meeting properties management.

The following types of auto-provisioning are enabled:

- **Pre-provisioning**: The endpoint receives a full service code, consisting of a 5-digit server service code identifying the Equinox Management server, and a 7-digit endpoint service code identifying the provisioned endpoint. During pre-provisioning, the endpoint profile is fully prepared before it is installed at the customer site.
- **Post-provisioning**: The endpoint receives a partial service code, consisting only of the 5-digit server service code identifying the Equinox Management server, while the 7-digit endpoint service code is either empty or consists only of zeros. During post-provisioning, the endpoint is added to the list of manageable endpoints, but is prepared (provisioned) at a later time.

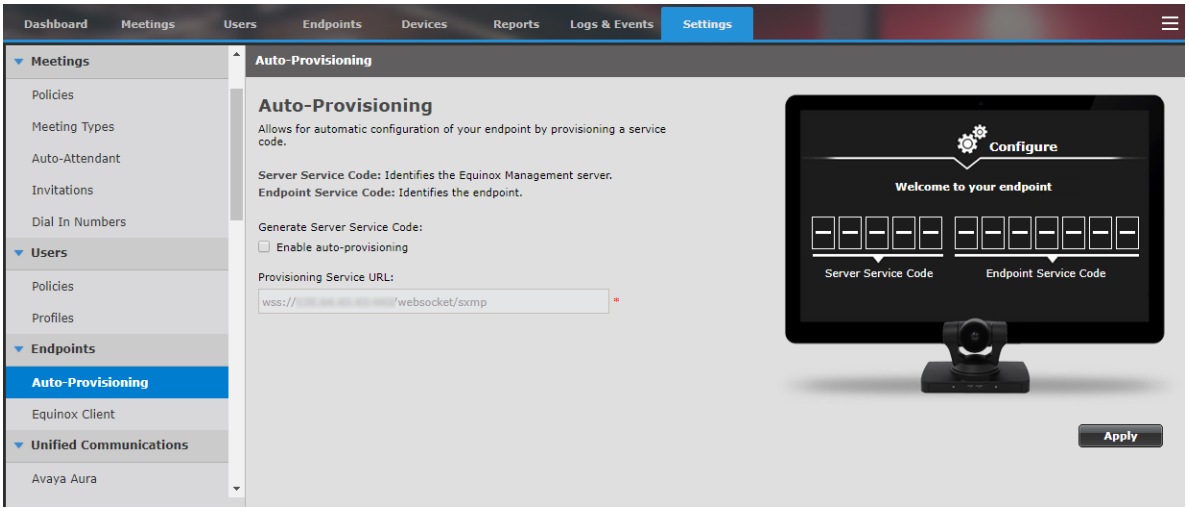
Note:

The XT Series Auto-Provisioning Service may be interrupted for maintenance, repairs, upgrades, or equipment or network failures. Avaya may discontinue certain features and the support for certain XT Series devices at any time. Events beyond Avaya's control may affect our service, such as force majeure events.

Procedure

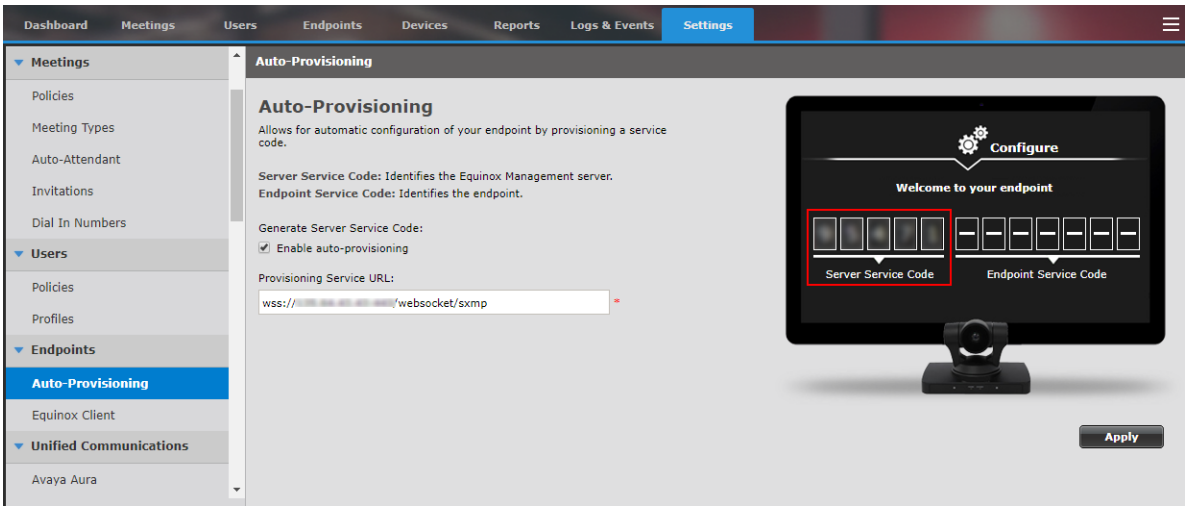
1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Endpoints** > **Auto-Provisioning**.

   The system displays the Auto-Provisioning page.



3. Select the **Enable auto-provisioning** check box and click **Apply**.

   The system displays the server service code for the Equinox Management server.



   This code can be used as a partial code for post-provisioning an endpoint.

4. **(Optional)** If any of the XT Series endpoints is outside of the enterprise, in the **Provisioning Service URL** field, enter the public IP address or Fully Qualified Domain Name (FQDN) of the Equinox Management server.

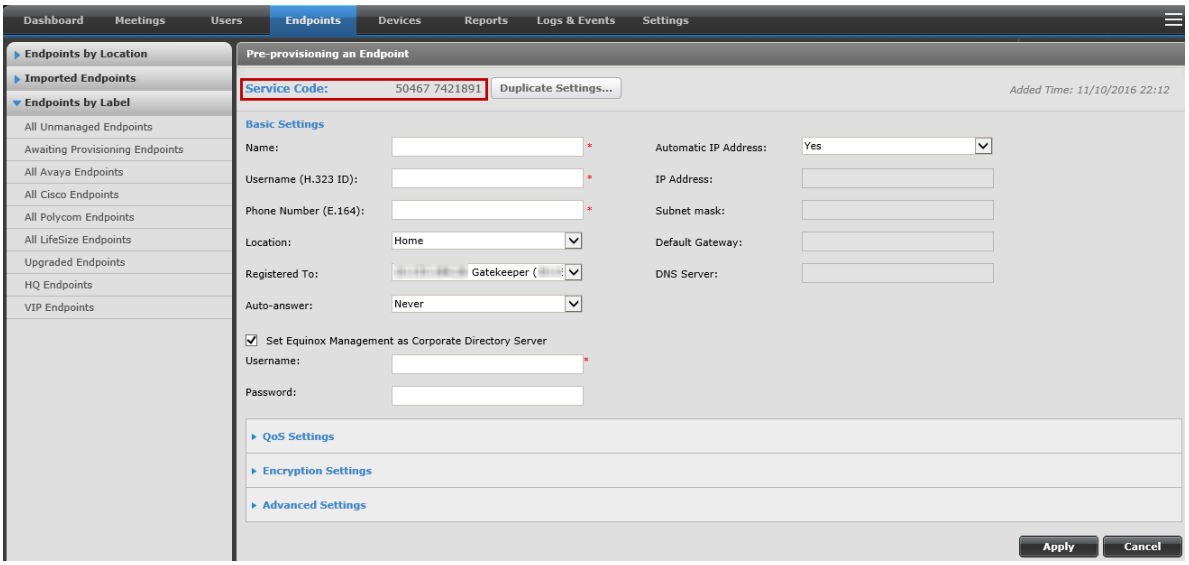
   Use this format: `wss://PublicAddressOfEquinox Management:port/websocket/sxmp`

   Avaya recommends using secure web sockets. The default value is 443 for HTTPS.

5. To pre-provision the endpoint and generate an endpoint service code, click **Endpoints** > **Add** > **Pre-provisioning an Endpoint**.

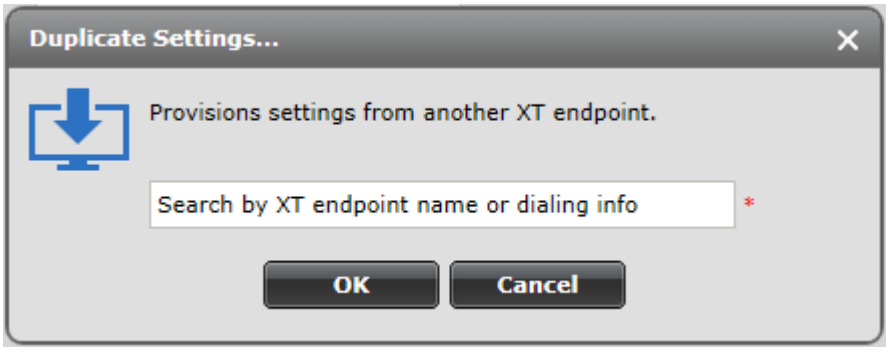
   The **Pre-provisioning an Endpoint** page opens, and the 5-digit server service code generated in Step 2 on page 146 displays at the top of the page, together with the 7-digit

endpoint service code. This full code enables the XT Series endpoint to connect to the Equinox Management server when the XT Series administrator activates the pre-provisioned endpoint, and the endpoint is automatically configured according to the pre-provisioned profile.



6. Optionally, click **Duplicate Settings...** at the top of the page to copy settings from another endpoint.

   The system displays the following dialog box, where you enter the XT endpoint name in the provided cell to indicate from where you want to copy settings.



7. On the **Pre-provisioning an Endpoint** page, configure the values for the endpoint in the **Basic Settings** section:

Table 32: Basic Settings Fields

Field Name	Description
Name	The name of the endpoint
Username (H.323 ID)	The H.323 username of the endpoint (displayed in H.323 calls)

Table continues…

Field Name	Description
Phone number (E.164):	The phone number of the endpoint
Location	The location of the endpoint
Registered To	The gatekeeper to which the endpoint is registered or the first SIP server
Auto-answer	The frequency policy by which the endpoint answers incoming calls. Select from the following: • Yes, always • Never • Yes, if not in a call • Yes, trusted always • Yes, trusted if not in a call **Note:** When selecting either of the last two options, only contacts configured as **trusted** are accepted when the specified condition is met. For details on configuring trusted contacts, see *Blocking All Calls Except From Trusted Contacts* in the *Avaya Equinox® Solution XT Series User Guide*.
Automatic IP Address	Indicates whether the IP address is to be obtained automatically by the system.
IP Address	The IP address of the endpoint; enabled only when the **Automatic IP Address** field value is **No**.
Subnet Mask	The subnet mask of an endpoint's IP network; enabled only when the **Automatic IP Address** field value is **No**.
Default Gateway	The default gateway server to which the H.323 endpoint is connected; enabled only when the **Automatic IP Address** field value is **No**.
DNS Server	The server used to resolve the domain name of the endpoint; enabled only when the **Automatic IP Address** field value is **No**. Ensure that a valid DNS is assigned. It can be manually configured or automatically filled by the DHCP server. If the DNS resolution of the cloud service address does not work, the provisioning is not applied and the XT Series cannot be managed in cloud mode.
Set Equinox Management as Corporate Directory Server	Sets Equinox Management as the corporate directory, so that user searches are done in the Equinox Management corporate directory. When selecting this check box, the **Username** and **Password** fields appear, where you enter the username and password of the corporate directory server.

8. Expand the **QoS Settings** section, and configure the relevant options.

Table 33: QoS Settings Options

Field Name	Description
Use QoS	Select to activate QoS (Quality of Service) and either guarantee a specified level of data stream performance (**Precedence/ TOS**) or configure the priority of the different data streams (**DiffServe**). When this check box is not selected, the other fields in this section are disabled.
Precedence/TOS	When selecting this option, the data stream sections (**Audio**, **Video**, **Data**, and **Signal**) display the following fields: • **TOS**: Select the type of service for the data stream • **Precedence**: Select the precedence value for the data stream The selected values must be identical across all other network components, and for all remote endpoints that connect in videoconferences.
DiffServe	When selecting this option, the data stream sections (**Audio**, **Video**, **Data**, and **Signal**) display the **DiffServ.(0–63)** field, where you configure the custom priority value, also known as differentiated service or **DiffServe**. The values must be identical for all elements in your network, and for all remote endpoints that connect in videoconferences.

9. Expand the **Encryption Settings** section, and configure the relevant options:

Table 34: Encryption Settings Options

Field Name	Description
Enable Encryption	Select to enable encrypted communication with the endpoint. When selecting the **Enable Encryption** check box, the following fields are enabled: • **Enable Encryption MCU**: Select to enable encryption with the MCU. • **SIP Proprietary Encryption**: Select to encrypt SIP calls with XT Series terminals, where TLS is not supported. When TLS is supported in the remote XT Series terminal, this field is not relevant, as TLS encrypts the calls. We recommend upgrading your XT Series terminals to enable TLS in SIP calls, to ensure maximum security. • **Audio Alert**: Select to generate an audio message with the encryption status for meeting participants. • **Unprotected Calls**: Select the desired behavior for unprotected calls: - Disconnect - Ask Confirmation - Inform - Show Status When the **Enable Encryption** check box is not selected, the **Accepted Protected Calls** option is enabled.

10. Expand the **Advanced Settings** section, and configure the relevant options:

Table 35: Advanced Settings Options

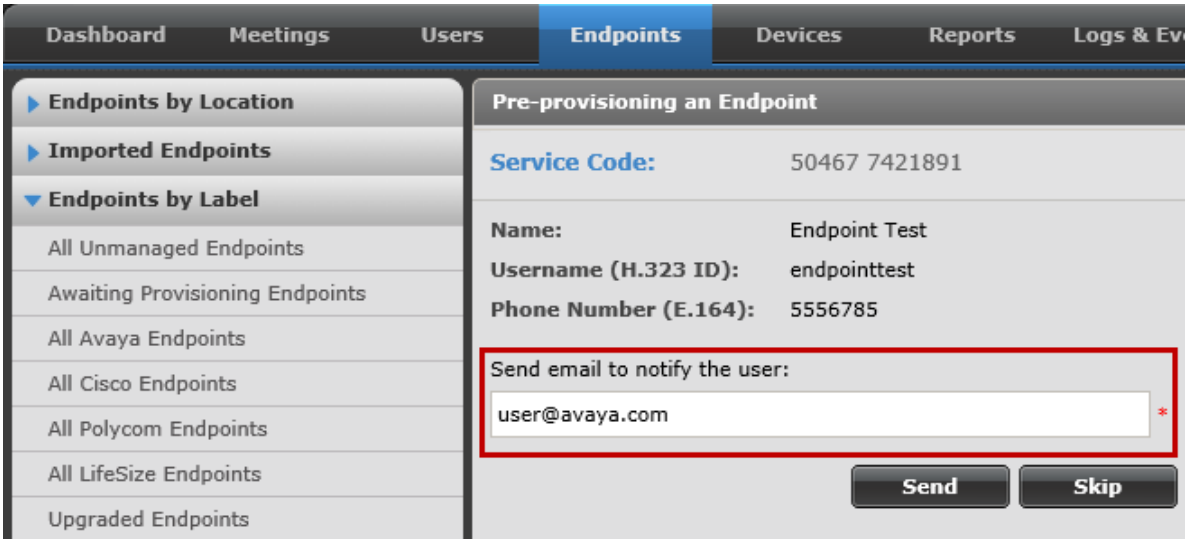
Field Name	Description
Visible in the directory of other endpoints (H.350–enabled endpoints, desktop and mobile)	Select to indicate that the endpoint is to appear in the directory of H.350–enabled endpoints.
VIP Endpoint (experience will not be downgraded during call)	Select to assign the endpoint as a VIP endpoint without diminishing call quality.
Has Embedded MCU	Select to indicate that the endpoint has an embedded MCU.
SIP Server 1	The first SIP server through which the endpoint registers for calls. It may be Equinox Management.

Table continues…

Field Name	Description
SIP Server 2	The second SIP server through which the endpoint registers for calls. The endpoint uses this server if **SIP Server 1** is not available.
SIP Server 3	The third SIP server through which the endpoint registers for calls. The endpoint uses this server if **SIP Server 1** and **SIP Server 2** are not available.
SIP Username	The username used to connect to the SIP server.
Authentication Name	Enter a name used for authentication of the SIP server.
Authentication Password	Enter the password used for authentication of the SIP server.
SIP Transport Type	Select the protocol used by the SIP server: • UDP • TCP • TLS
Max Bandwidth	Select the maximum bandwidth of the endpoint.
Default Call Bandwidth (Kbps)	Select the maximum bandwidth of the call managed by the endpoint, measured in kilobytes per second (kbps).
MTU Size	The size of the maximum transmission unit, measured in bytes.
Video Mode	Select the video mode, according to the type of picture displayed in the endpoint. • **Motion**: Select when the displayed picture is in motion. • **Sharpness**: Select when the displayed picture is stationary.
Pairing Mode	Select the pairing mode for Screen Link/Mobile Link: • Disabled • Enable - No PIN • Enable - Ask PIN (Manual pairing) • Enable - Ask PIN (Always)

11. Click **Apply**.

    Equinox Management generates an endpoint service code to be used by the XT Series endpoint. Furthermore, the endpoint details appear, where you enter an email address for the user to receive notification that the endpoint has been pre-provisioned.



12. Click **Send** to send an email to the indicated user and open the **All Endpoints** page, or click **Skip** to proceed directly to the **All Endpoints** page.
13. The endpoint is added to the **All Endpoints** table, with a blue “clock” icon indicating that the endpoint is pre-provisioned, and will receive the configuration after the insertion of the full service code in the quick setup wizard at first start up. The ‘envelope’ icon enables you to send a notification email to the specified user.

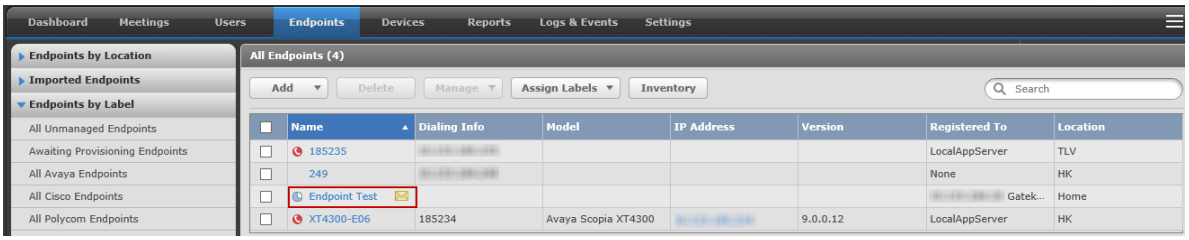


Figure 19: All Endpoints table - Pre-provisioned endpoint with icon

If the endpoint has been post-provisioned (that is, only a server service code was provided by Equinox Management with the endpoint, with no endpoint service code), the endpoint displays in the table with a red “clock” icon. This icon indicates that the endpoint is not yet provisioned and needs the Equinox Management administrator to configure it.

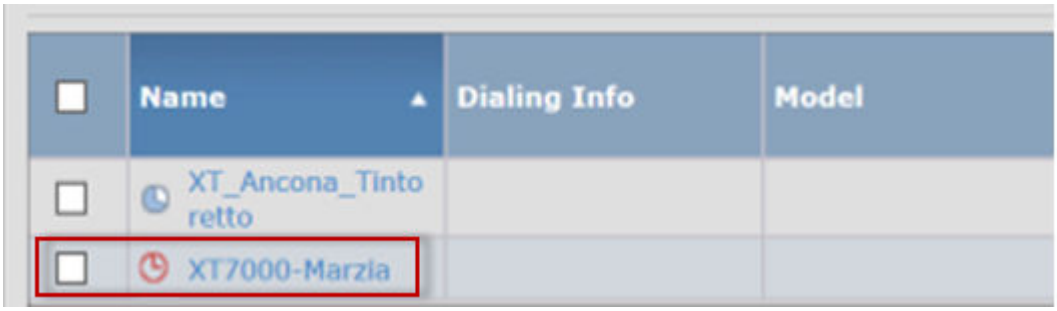


Figure 20: Post-provisioned endpoint with icon

Related links

Planning and configuring endpoints in Equinox Management on page 120

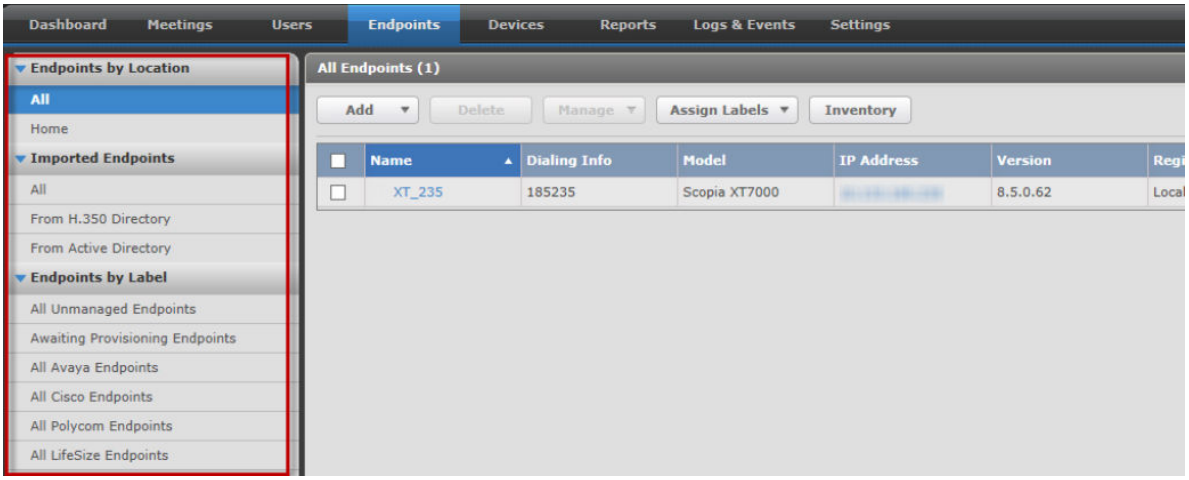
Configuring Quality of Service and Encryption settings for an XT Series endpoint in Equinox Management

About this task

This procedure describes how to configure Quality of Service (QoS) and Encryption settings for an XT Series endpoint in Equinox Management. QoS settings ensure specified levels of data stream performance, and encryption settings ensure security when XT Series endpoints communicate with each other.

Procedure

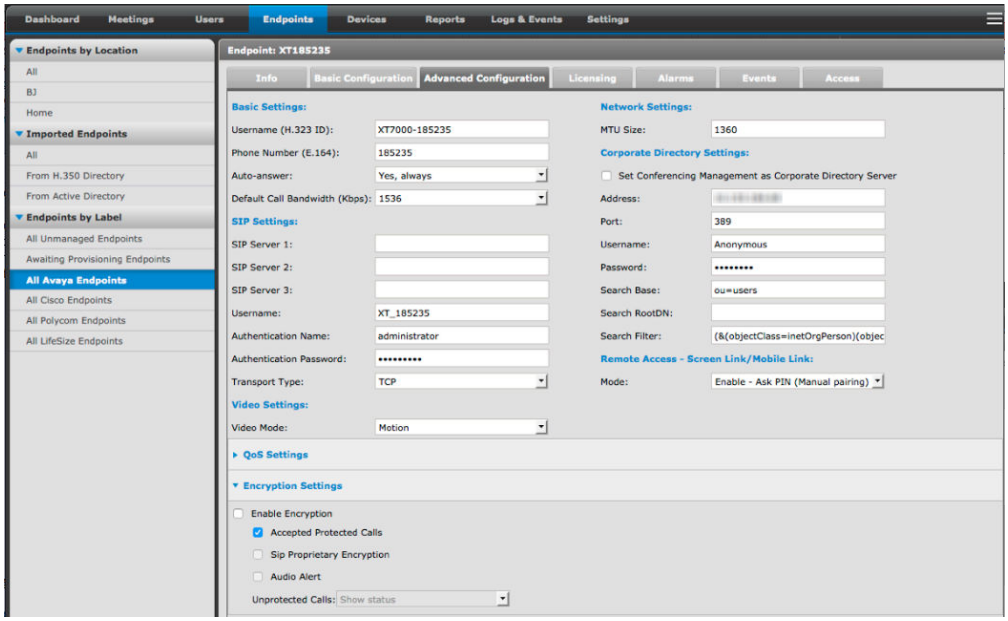
1. Click the **Endpoints** tab and filter the results using the facets on the left side of the page, as needed.



2. In the table, click the relevant endpoint.

   The system displays the **Info** tab, displaying information about the endpoint.

3. Click the **Advanced Configuration** tab.



4. Expand the **QoS Settings** section, and configure the relevant options.

Table 36: QoS Settings Options

Field Name	Description
Use QoS	Select to activate QoS (Quality of Service) and either guarantee a specified level of data stream performance (**Precedence/ TOS**) or configure the priority of the different data streams (**DiffServe**). When this check box is not selected, the other fields in this section are disabled.
Precedence/TOS	When selecting this option, the data stream sections (**Audio**, **Video**, **Data**, and **Signal**) display the following fields: • **TOS**: Select the type of service for the data stream • **Precedence**: Select the precedence value for the data stream The selected values must be identical across all other network components, and for all remote endpoints that connect in videoconferences.
DiffServe	When selecting this option, the data stream sections (**Audio**, **Video**, **Data**, and **Signal**) display the **DiffServ.(0–63)** field, where you configure the custom priority value, also known as differentiated service or **DiffServe**. The values must be identical for all elements in your network, and for all remote endpoints that connect in videoconferences.

5. Expand the **Encryption Settings** section, and configure the relevant options:

Table 37: Encryption Settings Options

Field Name	Description
Enable Encryption	Select to enable encrypted communication with the endpoint. When selecting the **Enable Encryption** check box, the following fields are enabled: • **Enable Encryption MCU**: Select to enable encryption with the MCU. • **SIP Proprietary Encryption**: Select to encrypt SIP calls with XT Series terminals, where TLS is not supported. When TLS is supported in the remote XT Series terminal, this field is not relevant, as TLS encrypts the calls. We recommend upgrading your XT Series terminals to enable TLS in SIP calls, to ensure maximum security. • **Audio Alert**: Select to generate an audio message with the encryption status for meeting participants. • **Unprotected Calls**: Select the desired behavior for unprotected calls: - Disconnect - Ask Confirmation - Inform - Show Status When the **Enable Encryption** check box is not selected, the **Accepted Protected Calls** option is enabled.

Related links

Planning and configuring endpoints in Equinox Management on page 120

Replicating endpoint settings on multiple endpoints

About this task

You can replicate an endpoint's settings on other endpoints of the same model and vendor. This is useful, for example, to save time by configuring the settings only once.

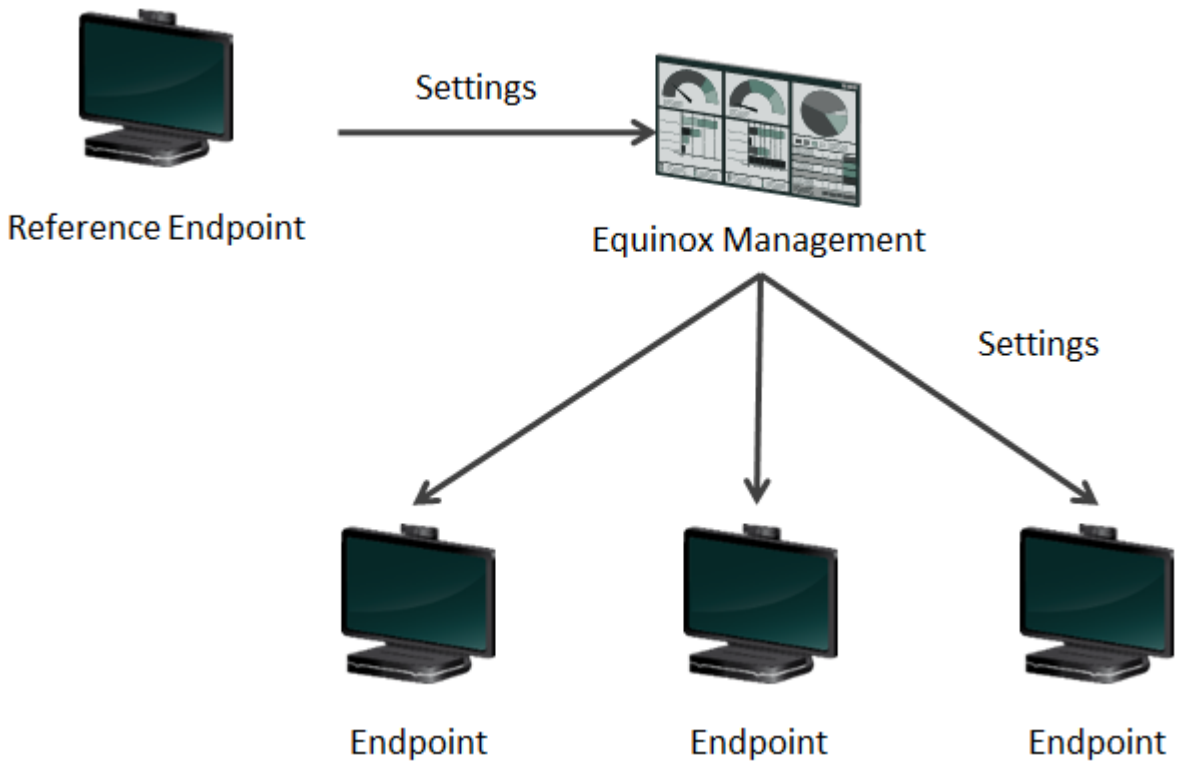


Figure 21: Replicating endpoint settings on multiple endpoints

You can replicate settings for these endpoints: Avaya IX™ CU360 and Avaya Room System XT Series.

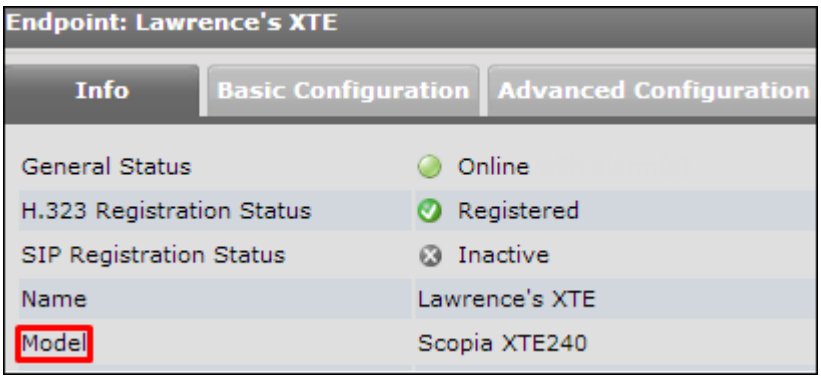
This is done by accessing an endpoint's configuration file and applying it to other endpoints. The following information can be replicated:

- Basic settings (**Current Gatekeeper**, **Auto-Answer**, and **Default Call Bandwidth** fields)
- SIP settings (**SIP Proxy Server**, **SIP Registrar**, and **Transport Type** fields)
- Monitoring settings (**Trap Server Address** field)
- Video settings (**Video Mode** and **Enable Gallery Layouts** fields)
- Passwords (XT Series only)

You cannot replicate information that is specific to the endpoint, such as its name and whether it has a built-in MCU.

Before you begin

Decide which endpoint you would like to use as a reference for other endpoints, and verify that all settings are defined on your reference endpoint. The reference endpoint must have the same model and vendor as the endpoints to which you are replicating the settings, as listed on the endpoint's info page:

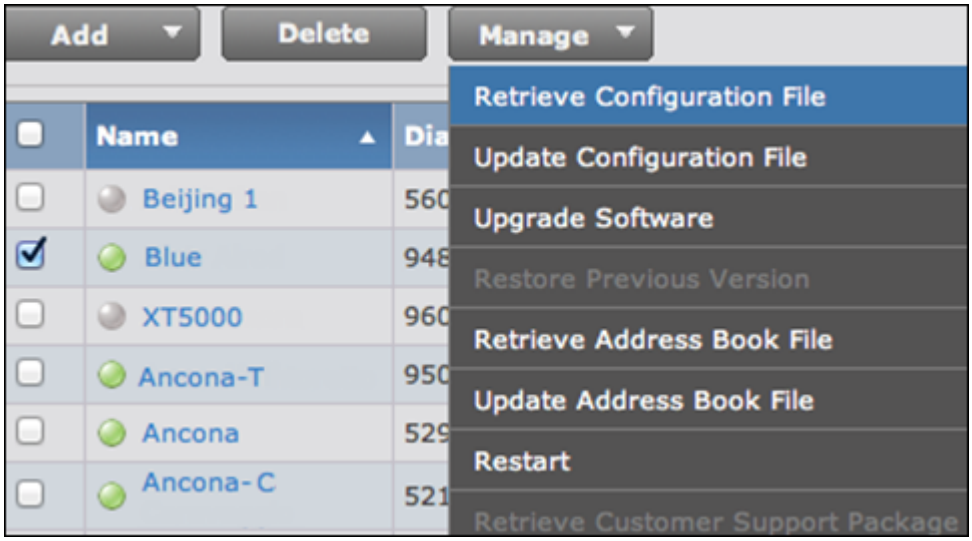


For example, you can replicate Avaya XTE240 settings only to other Avaya XTE240s, and not to other Avaya IX™ CU360 or Avaya Room System XT Series endpoints.

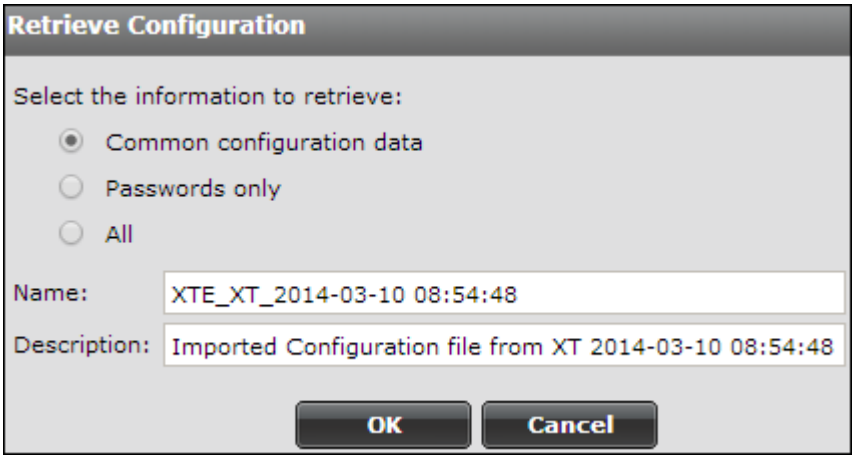
Verify that the endpoints are managed by Equinox Management: Navigate to the **Basic Configuration** tab in the endpoint's page and verify that **Manage (upgrade and configure) this endpoint** is selected (see Managing endpoints using Equinox Management on page 141).

Procedure

1. Access the Equinox Management administrator portal.
2. Click the **Endpoints** tab.
3. From the list, select the endpoint you are using as a reference and click **Manage** > **Retrieve Configuration File**.



4. For XT Series and Avaya IX™ CU360 endpoints only, you can choose which information to replicate:
   a. Select the information to replicate:

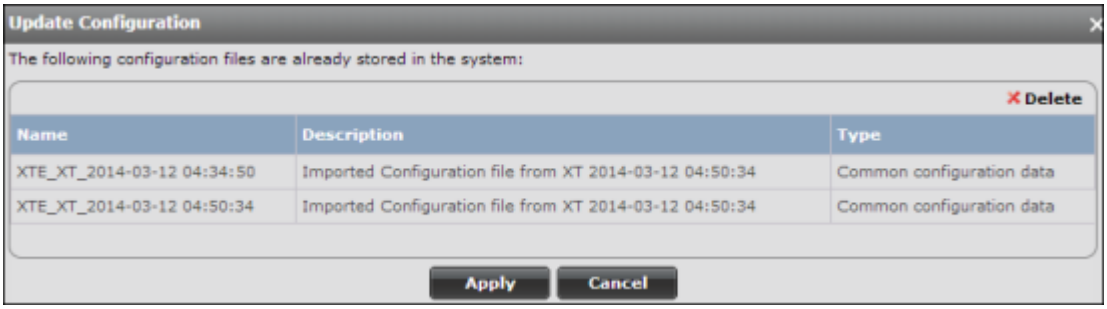


- **Common configuration data** (includes the fields listed in the introduction of this section)
- **Passwords only** (includes all endpoint passwords, such as the administrator PIN, user PIN, and web interface password)
- **All** (both the passwords and the configuration data)

b. Click **OK**.

5. Select the endpoints to which you want to apply this configuration file.
6. Click **Manage** > **Update Configuration File**.

   The system displays the list of imported configuration files.



7. Select the configuration file you want to use.
8. Select **Apply**.

   The **Update Log** displays the status of the configuration file update.

Related links

Planning and configuring endpoints in Equinox Management on page 120

Using Equinox Management's endpoint directory as a corporate address book

The corporate address book feature turns Equinox Management's list of endpoints into a directory, allowing dedicated endpoints (H.350-enabled) to search through and find contact information for other endpoints. When you add an endpoint to Equinox Management, you define if it is displayed in the address book.

In a service provider deployment, you configure the corporate address book feature for every organization.

The following endpoints support this feature:

- Life-Size: Team, Conference
- Polycom: HDX Series, VSX Series
- Avaya Room System XT Series
- All Tandberg endpoints via TMS

This section includes the following topics for configuring corporate address books:

Related links

Planning and configuring endpoints in Equinox Management on page 120
Configuring corporate address books on page 159
Configuring endpoints to be displayed in the corporate address book on page 160

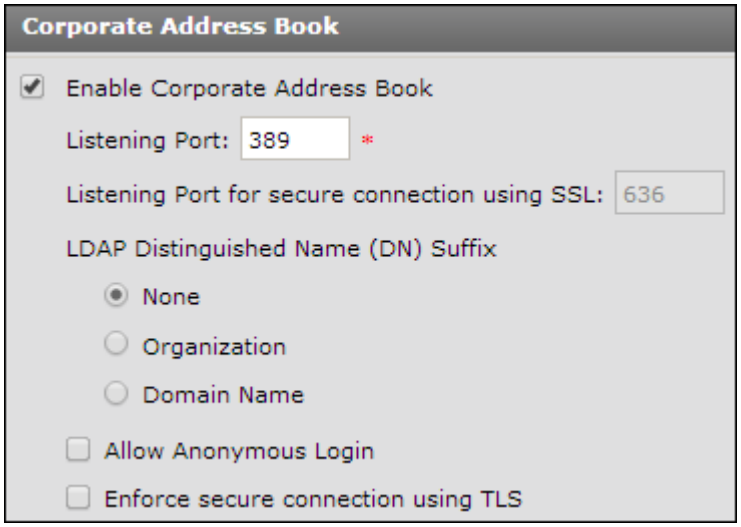
Configuring corporate address books

About this task

This procedure describes how to enable the corporate address book feature, which allows dedicated endpoints (H.350-enabled) to search through Equinox Management's directory of endpoints. This feature is disabled by default.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Address Book** > **Corporate Address Book**.



3. Select **Enable Corporate Address Book**.
4. Enter the port to receive the LDAP request in the **Listening Port** field.

   --Or--

   If your organization requires a secure connection, select **Enforce secure connection using TLS** and enter the port in the **Listening Port for secure connection using SSL** field.
5. **(Optional)** Define the search base for endpoints by selecting one of the following options for **LDAP Distinguished Name (DN) Suffix** (the root DN):
   - Select **None** to set the search base to "ou=name".
   - Select **Organization** to limit the search base to a specific organization and enter its name: " o=<organization>".
   - Select **Domain Name** to limit the search base to a specific domain and enter the domain name: " ou=name, dc=<domain>,dc=com".
6. **(Optional)** To allow endpoints to search data in the LDAP service without logging in, select **Allow Anonymous Login**.
7. Click **Apply** to save your changes.

Related links

Using Equinox Management's endpoint directory as a corporate address book on page 159

Configuring endpoints to be displayed in the corporate address book

About this task

You can define if an endpoint is displayed in the corporate address book, or if it is a private number and other endpoints will not have access to this information.

Important:

This is not supported for Polycom and Tandberg endpoints.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Endpoints** tab.
3. Navigate to the endpoint using the facets on the sidebar.
4. Click the endpoint you want to configure.
5. Click **Basic Configuration**.
6. **(Optional)** Select **Visible in the directory of other endpoints (H.350-enabled endpoints, desktop and mobile)**.
7. Click **Apply** to save your changes.

Related links

Using Equinox Management's endpoint directory as a corporate address book on page 159

Managing your endpoint's user directory with LDAP

You can manage the contact list of your endpoints using one of the following LDAP servers:

- Equinox Management's built-in LDAP server

  Configure your endpoints to use Equinox Management as your LDAP server via Equinox Management or the endpoint's web interface.

- A third-party LDAP server (such as or Microsoft Active Directory)

  Configure your endpoints to use a third-party LDAP server via Equinox Management or the endpoint's web interface.

  For XT Series endpoints, this is done via the XT Series endpoint's web interface only. For more information, see the *Administrator Guide for XT Series*.

- An endpoint's built-in LDAP server

  Configure your endpoints to use one of the built-in LDAP servers via Equinox Management or the endpoint's web interface.

  For XT Series endpoints, this is done via the XT Series endpoint's web interface only. For more information, see the *Administrator Guide for XT Series*.

Avaya Equinox® Management's LDAP functionality includes the H.350 extension, which allows you to set up your user directory with specific attributes that are useful in a videoconferencing environment. For example, you can add a meeting room as a user, or define multiple endpoints for one user, and have a directory of endpoints.

Use the following procedures to use Avaya Equinox® Management's built-in LDAP directory to keep track of users and their endpoints:

Related links

Planning and configuring endpoints in Equinox Management on page 120

Configuring Endpoints to use an LDAP Directory on page 162
Configuring Third-Party Endpoints to use Equinox Management as LDAP Directory on page 166

Configuring Endpoints to use an LDAP Directory

About this task

This procedure describes how to manage the contact list of your endpoints using an LDAP server, such as Equinox Management's built-in LDAP server. This can be done for XT Seriesand endpoints from LifeSize, Polycom, and Tandberg. Depending on the endpoint model, you configure the LDAP server either from Equinox Management or from the endpoint's web interface (see details in the list below).

A centralized solution like Equinox Management enables synchronizing the same list of contacts across all the endpoints in your organization, and has other benefits such as remote centralized upgrading and backing up of all endpoints in your video network.

LDAP servers are accessed using the H.350 protocol, which enhances the LDAP standard to include video endpoint information.

You can define three types of LDAP servers:

- Equinox Management's built-in LDAP server

  The contacts of this server are read-only from the endpoint. You can define more than one such server, specifying each IP address, port, and its LDAP username and password. The resulting list shows all the organization's endpoints known to Equinox Management.

  From Equinox Management's administrator portal, you can define it as the LDAP server for XT Series and LifeSize endpoints. For Polycom and Tandberg endpoints, you must do this from the endpoint's web interface only (see Configuring Third-Party Endpoints to use Equinox Management as LDAP Directory on page 166).

- The endpoint's built-in LDAP server

  From Equinox Management's administrator portal, you can define the endpoint's own LDAP server for LifeSize endpoints. For XT Series endpoints, this is done via the XT Series endpoint's web interface only (see the *Administrator Guide for Avaya Room System XT Series*). For Polycom and Tandberg endpoints, see Configuring Third-Party Endpoints to use Equinox Management as LDAP Directory on page 166.

  Important:

  You cannot remove the endpoint's local LDAP server.

- A third-party LDAP server, such as Microsoft Active Directory

  The contacts of a third party LDAP are read-only from the endpoint.

  The LDAP tree must have the following specific structure and naming conventions. For more information, see your endpoint’s documentation.

  From Equinox Management's administrator portal, you can define a third-party LDAP server for LifeSize endpoints. For XT Series endpoints, this is done via the XT Series endpoint's web interface only (see the *Administrator Guide for Avaya Room System XT Series*). For Polycom and Tandberg endpoints, see Configuring Third-Party Endpoints to use Equinox Management as LDAP Directory on page 166.

Before you begin

- Make sure that your endpoint is configured to be managed in Equinox Management, as described in Managing endpoints using Equinox Management on page 141.
- If you are using Equinox Management as the LDAP directory, configure its LDAP settings as described in Configuring corporate address books on page 159.
- If you are using Equinox Management as the LDAP directory, associate LDAP usernames to video endpoints; otherwise, the endpoints displayed on the XT Series are listed without the correct username.
- When connecting to a third-party LDAP server, the network administrator must verify that the video endpoint information is stored in the H.323 Identity and SIP Identity object classes, according to the H.350 protocol.

  Note:

  For XT Seriesand LifeSize endpoints that are managed by Equinox Management, parameters such as the Gatekeeper address and the name of the LDAP server are set.
- If you are configuring an XT Series endpoint to use any LDAP server other than Equinox Management, this is done via the XT Series endpoint's web interface only (see the *Administrator Guide for Avaya Room System XT Series*).

Procedure

1. Access the Equinox Management administrator portal.
2. Select the **Endpoints** tab.
3. Select the required endpoint.
4. Select the **Advanced Configuration** tab.
5. Configure the LDAP server settings, as described below.

   The fields displayed depend on the type of endpoint.

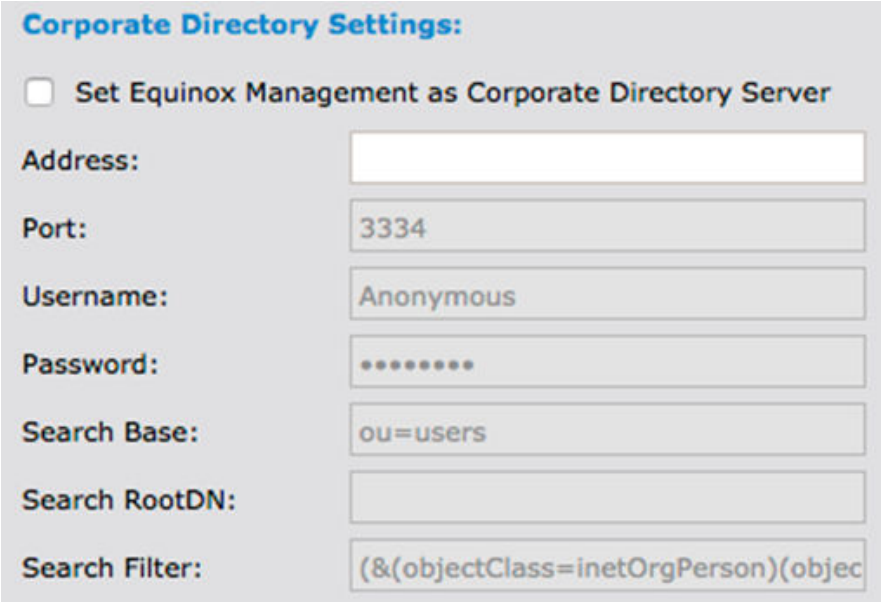


Figure 22: Configuring LDAP server settings from Equinox Management

Table 38: Configuring LDAP server settings

Field Name	Description
Set Equinox Management as Corporate Directory Server	(For XT Series only) Select to use Equinox Management as your LDAP directory.
Address	Enter the LDAP server address. When using Equinox Management as the LDAP server, this field displays its IP address.
Port	Enter the port used to connect to the LDAP server. Use port *389* for a standard connection, and use *636* for a secure connection. When configuring the User Portal + Web Gateway, use port *3268* for a standard connection, and port *3269* for a secure connection.

Table continues…

Field Name	Description
Username **Password**	Enter the username and password required to access the LDAP server. The format of the username is in the form of a Distinguished Name (DN). Some standard components of DN are: domain controller (dc), organizational unit (ou), common name (cn), country (c), state or province (st), locality (l), organization (o). When using Equinox Management as the LDAP server: • If you enabled anonymous login, these fields cannot be modified. You can verify this in Equinox Management in **Settings** > **Address Book** > **Corporate Address Book**. • If you did not enable anonymous login, enter the administrator's Equinox Management credentials. To enable anonymous login, see Configuring corporate address books on page 159. The login to the third-party LDAP servers is via a Simple Bind LDAP v3 operation. When using the endpoint's built-in LDAP server, you can modify its LDAP password here.
Search Base	For third-party LDAP servers, enter the root node of the LDAP tree under which all the contacts (**inetOrgPerson** entities) are defined. For example *ou=people*. This value is predefined when the LDAP server is Equinox Management or an XT Series, and cannot be modified.
Search Root DN	This is relevant only for XT Series using Equinox Management as the LDAP server. If you are using Equinox Management and you defined its Root DN (see the **LDAP Distinguished Name (DN)** field in **Settings** > **Address Book** > **Corporate Address Book**), the value is displayed here.
Search Filter	The filter applied to the LDAP tree, so you view only the relevant contacts. This value is predefined when the LDAP server is Equinox Management or an XT Series, and cannot be modified. The phrase is required to navigate the remote LDAP tree, which depends on the way the tree was structured. For example, if the LDAP tree is built from objects known as inetOrgPerson, the filter would be `objectclass=inetOrgPerson`.
Authentication Mode	When using Equinox Management as the LDAP server, this value is retrieved from **Settings** > **Address Book** > **Corporate Address Book** > **Allow Anonymous Login** and cannot be modified (see Configuring corporate address books on page 159).
Secure Connection Using TLS	When using Equinox Management as the LDAP server, this value is retrieved from **Settings** > **Address Book** > **Corporate Address Book** > **Enforce secure connection using TLS** and cannot be modified (see Configuring corporate address books on page 159).

6. Select **Apply**.

Related links

Managing your endpoint’s user directory with LDAP on page 161

Configuring Third-Party Endpoints to use Equinox Management as LDAP Directory

About this task

To configure third-party endpoints to use Equinox Management as their LDAP server from the endpoint's web interface, use the settings detailed in this section. This process synchronizes each endpoint's contacts list with the corporate address book.

To configure third-party endpoints with any LDAP server via Equinox Management's administrator portal, see Configuring Endpoints to use an LDAP Directory on page 162.

For LifeSize endpoints, apply these settings (Figure 23: LifeSize Endpoint Settings on page 167):

- **LDAP Enable**: This must be enabled.
- **LDAP Host name**: The Equinox Management address.
- **LDAP Username**: Set this field to the Equinox Management's user, or to *anonymous*.
- **LDAP Password**: Set to the user's password.
- **LDAP Base**: The data input in one of the fields is the suffix of the LDAP Distinguished Name of an entry supplied by the LDAP service. LifeSize searches the terminals by **ou=endpoints**.

  For example:

  - If Equinox Management configured the LDAP Distinguished Name (DN) Suffix as **None**, in LifeSize the Base DN would be **ou=endpoints**.
  - If Equinox Management configures the LDAP Distinguished Name (DN) Suffix as **mycompany** for the Organization Name, in LifeSize the Base DN would be **ou=endpoints,o=mycompany**.
  - If Equinox Management configured the LDAP Distinguished Name (DN) Suffix as: **mycompany.com**, in LifeSize the Base DN would be **ou=endpoints,dc=radvision,dc=com**.
- **LDAP Filter**: Set its value to **(objectClass=*)**.

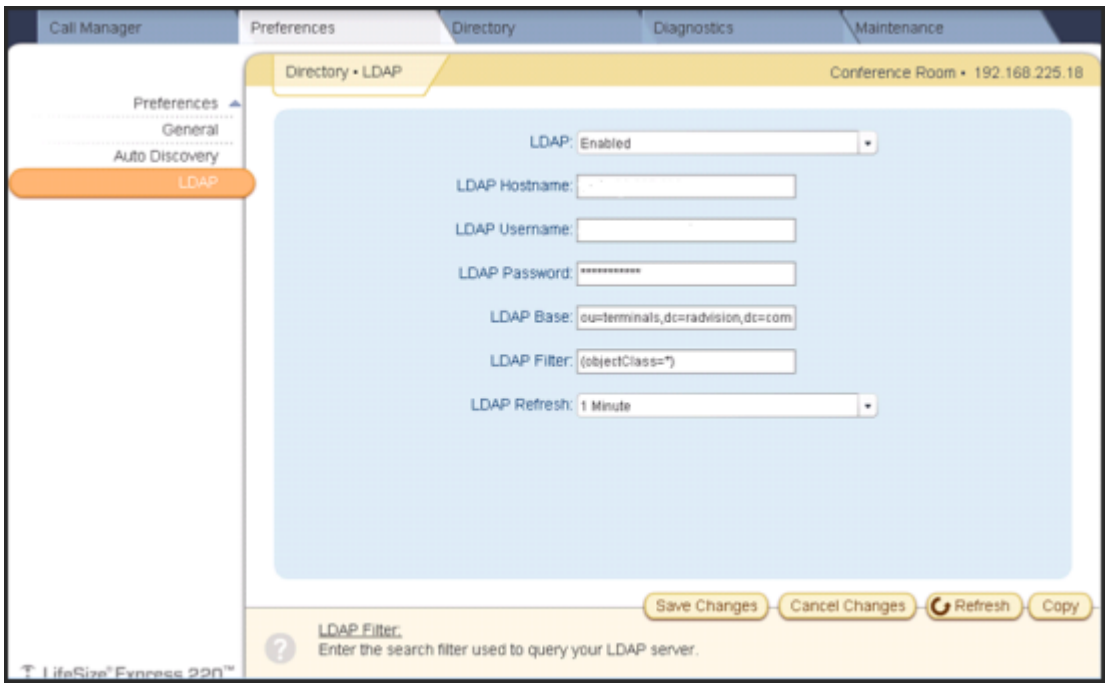


Figure 23: LifeSize Endpoint Settings

Important:

You can perform this configuration via Equinox Management by entering the LDAP settings in **Setting** > **Endpoint Management** > **Lifesize** > **Corporate Directory**.

For Polycom endpoints, apply these settings (Figure 24: Polycom endpoint settings on page 168):

- **Server Address**: Set to the Equinox Management server address.
- **Server Port**: Must be the same as the settings of Equinox Management. For example: **389**.
- **Group Name**: Define a group name.
- **Base DN (Distinguished Name)**: The data input in one of the fields is the suffix of the LDAP Distinguished Name of an entry supplied by the LDAP service. Polycom must use the **ou=users** because Polycom endpoints access via the users to reach the endpoints.

  For example:

  - If Equinox Management configured the **LDAP Distinguished Name (DN) Suffix** as **None**, in Polycom the **Base DN** should be: **ou=users**.
  - If Equinox Management configured the **LDAP Distinguished Name (DN) Suffix** as **mycompany** for the Organization Name, in Polycom the Base DN should be **ou=users,o=mycompany**.
  - If Equinox Management configured the **LDAP Distinguished Name (DN) Suffix** as **mycompany.com** for the Domain Name, in Polycom the Base DN should be: **ou=users,dc=mycompany,dc=com**.
- **Authentication Type**: Define as **Basic**.
- **Bind DN (Distinguished Name)**: Set to Equinox Management's username.

- **Change Password**: Set to your user's password.

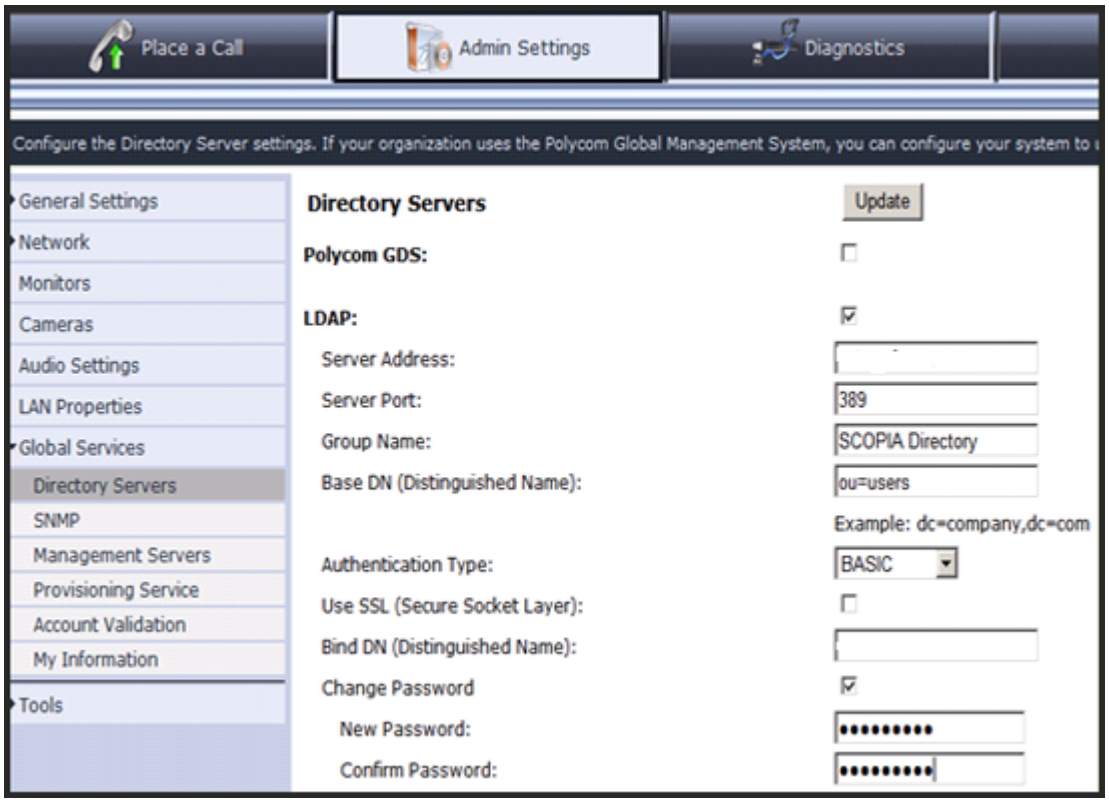


Figure 24: Polycom endpoint settings

For Tandberg endpoints, apply the following settings:

Important:

You can configure Tandberg endpoints to use Equinox Management as the LDAP directory only if they are configured to work with Tandberg Management Suite (TMS).

- **IP address/DNS**: Set this field to the Equinox Management's address.
- **Username**: Set this field to the Equinox Management's user.
- **Password**: Set to the user's password.
- **LDAP Port Number**: This must be the same as the settings for Equinox Management. For example, **389**.
- **LDAP Base**: The data input in the field will be the suffix of the LDAP Distinguished Name of an entry supplied by the LDAP service. Tandberg's TMS searches terminals by **ou=terminals**.

  For example:

  - If Equinox Management configured the LDAP Distinguished Name (DN) Suffix as **None**, in TMS the Base DN would be **ou=terminals**.
  - If Equinox Management configured the LDAP Distinguished Name (DN) Suffix as mycompany for the Organization Name, on the TMS side the Base DN would be **ou=terminals,o=mycompany**.

- If Equinox Management configured the LDAP Distinguished Name (DN) Suffix as: mycompany.com, in the TMS the Base DN would be: **ou=terminals,dc=mycompany,dc=com**.

- **Custom LDAP Filter**: Enter **(commUniqueId=*)**.
- **Field to use for Display Name in TMS**: Enter **cn**.

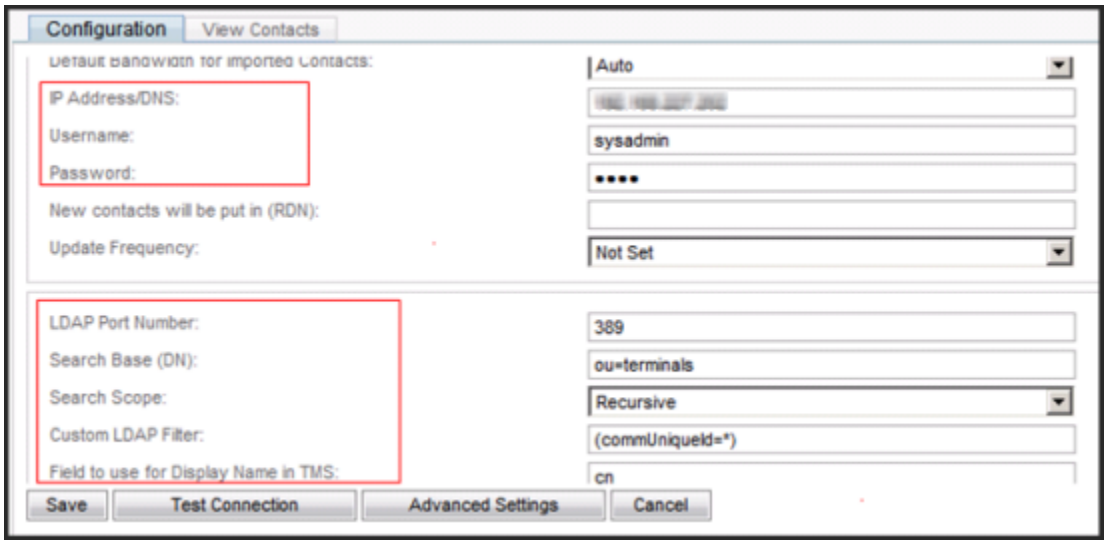


Figure 25: Tandberg Endpoint Settings

Related links

Managing your endpoint's user directory with LDAP on page 161

Configuring presentation layouts for single-screen endpoints

About this task

To improve user experience on a dedicated single-screen endpoint, enable an additional set of video layouts called gallery layouts. Specifically designed for viewing shared content, these video layouts optimize screen space by displaying the presentation as the main part of the screen, with participants as a strip either alongside or underneath. By contrast, a standard video layout might display participants as an image overlay (as an example).

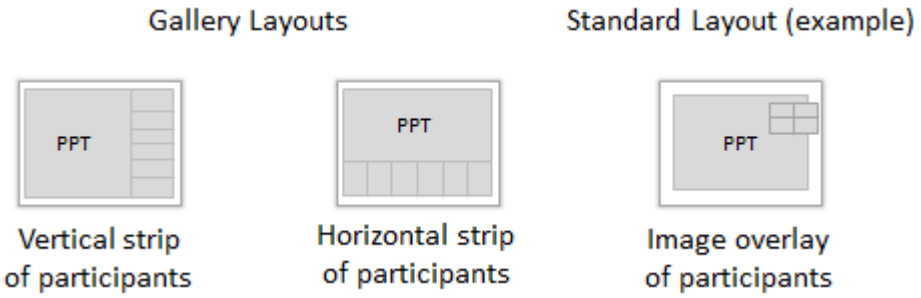


Figure 26: Comparing gallery and standard layouts

These layouts also support a higher resolution by using bandwidth more efficiently: All bandwidth is used for one video stream that includes both the presentation and the participant video, instead of being split between two separate streams. For example, if the XT Series connects using 2048 Kbps, the resulting resolution for a gallery layout is up to 1080p (for a list of video resolutions for a given bandwidth, see *Deployment Guide for Avaya Room System XT Series*). For other video layouts, the same bandwidth is split so that each stream uses 1024 Kbps, lowering the maximum resolution to 720p.

By default, gallery layouts are enabled for XT Series endpoints (Avaya XT5000 Series/Avaya XT4000 Series/Avaya XTE240), and disabled for dedicated third-party endpoints.

Gallery layouts are available only for meetings hosted by Scopia® Elite 6000 MCUs, and must be supported by the meeting type.

These video layouts require extra MCU resources (an additional 480p connection per meeting). If your MCU capacity is limited, you can disable gallery layouts for specific meeting types, as described in Modifying a media server meeting type in Equinox Management on page 81.

Before you begin

- For XT Series endpoints only, verify that the endpoint is managed by Equinox Management: Navigate to the **Basic** tab in the endpoint's page and verify that **Manage (upgrade and configure) this endpoint** is selected (see Managing endpoints using Equinox Management on page 141).

  You can configure third-party endpoints to use gallery layouts even if they are not managed by Equinox Management.

- Configure the meeting types to also support gallery layouts (see Modifying a media server meeting type in Equinox Management on page 81). Otherwise, gallery layouts are not available (even if enabled on the endpoint).

Procedure

1. Access the Equinox Management administrator portal.
2. Click the **Endpoints** tab.
3. Navigate to and click an endpoint.
4. Do one of the following:
   - For XT Series endpoints, navigate to **Advanced Configuration** > **Video Settings** and select **Enable Gallery Layouts**.
   - For third-party endpoints, select **Basic Configuration** > **Enable Gallery Layouts**.

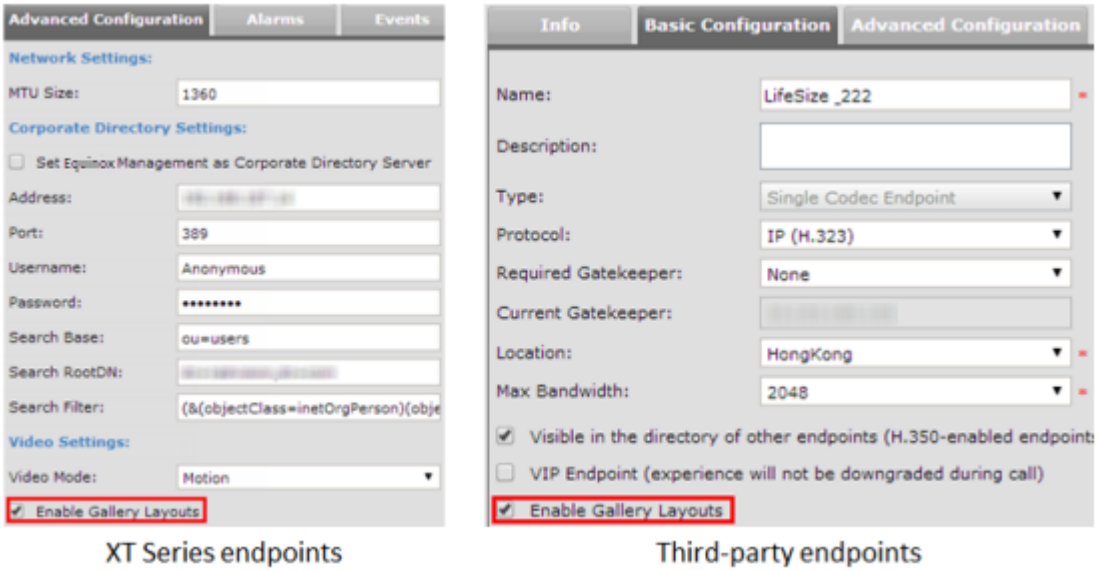


Figure 27: Enabling gallery layouts on your dedicated endpoint

5. Click **Apply**.

Related links

Planning and configuring endpoints in Equinox Management on page 120

Organizing endpoints into groups with labels

About this task

Labels allow you to easily search for and manage endpoints belonging to the same group like department in your organization or vendor. This is useful, for example, when performing management tasks for many endpoints at once. Equinox Management comes with preconfigured labels for vendor names such as Avaya video endpoints, Cisco endpoints, or Lifesize endpoints. When you import or add an endpoint to Equinox Management, the relevant vendor label is assigned to it automatically. You can also create labels that serve your needs. You can assign your own labels to endpoints after creating them in Equinox Management.

Assigning labels to endpoints is a very powerful and flexible way to manage your endpoints. You can for example with a few clicks filters all the Avaya XTE240 endpoints of the Vice Presidents of your company and upgrade them.

An endpoint can have multiple labels. Labels are displayed in the sidebar for you to navigate easily to all endpoints with this label, as shown in Figure 28: Viewing endpoints by preconfigured labels on page 172.

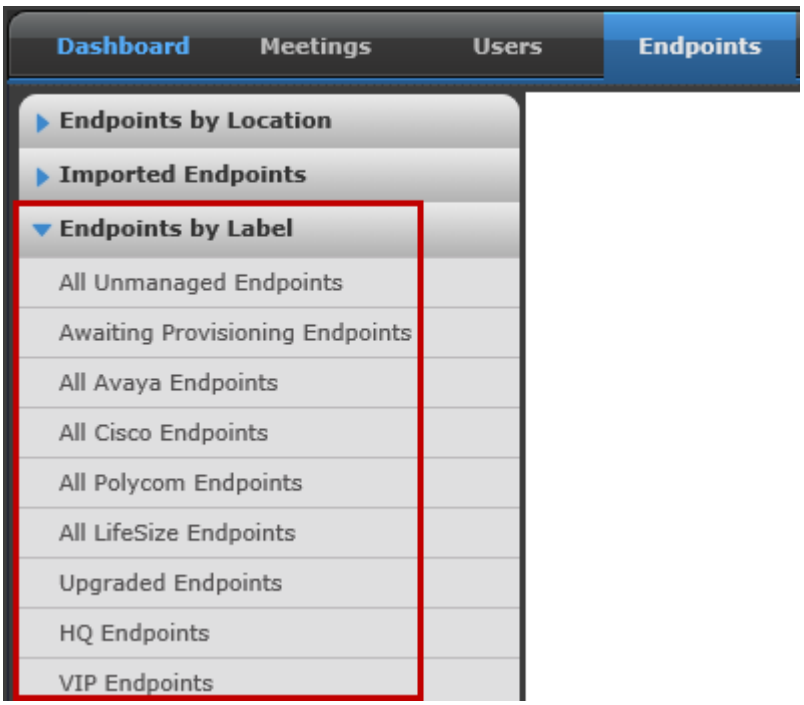


Figure 28: Viewing endpoints by preconfigured labels

After you organized endpoints using labels, you can easily filter the endpoint list to navigate to specific endpoints. For example, instead of navigating to Avaya XTE240 endpoints of vice presidents in your organization one by one, you can select the relevant label and see all these endpoints in one list.

This procedure describes how to organize your endpoints with labels. You can create and modify labels, assign labels to endpoints or remove labels from endpoints, and delete labels from the system.

Procedure

1. Access the Equinox Management administrator portal.
2. Click the **Endpoints** tab.
3. To create a new label:
   a. Click an endpoint group that is not under **Endpoints by Label**.
   b. Click **Assign Labels** > **Create new**.
   c. Enter a name for this label.
   d. Click **Create**.
4. To assign a label to an endpoint or multiple endpoints:
   a. Select the endpoints to which you are assigning the label.
   b. Click **Assign Labels**.

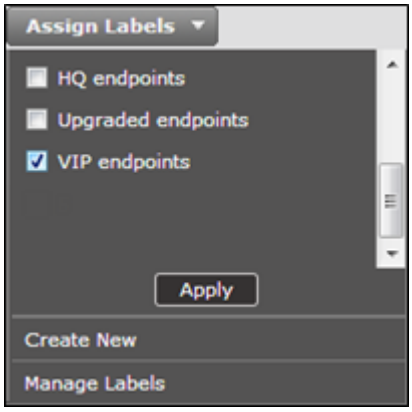


Figure 29: Assigning a label to an endpoint

c. Select the label and click **Apply**.

5. To remove a label from an endpoint, navigate to the label under **Endpoints by Label**:
   a. Select the endpoint from which you want to remove the label.
   b. Click **Unassign Label**.

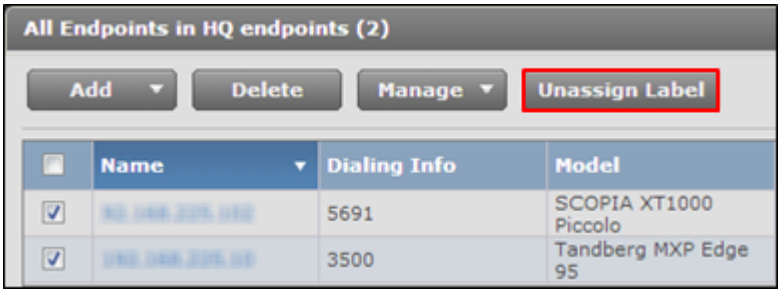


Figure 30: Unassigning labels from endpoints

   c. Click **Yes** to confirm.

6. To modify or delete a label from the system, click **Assign Labels** > **Manage labels**:

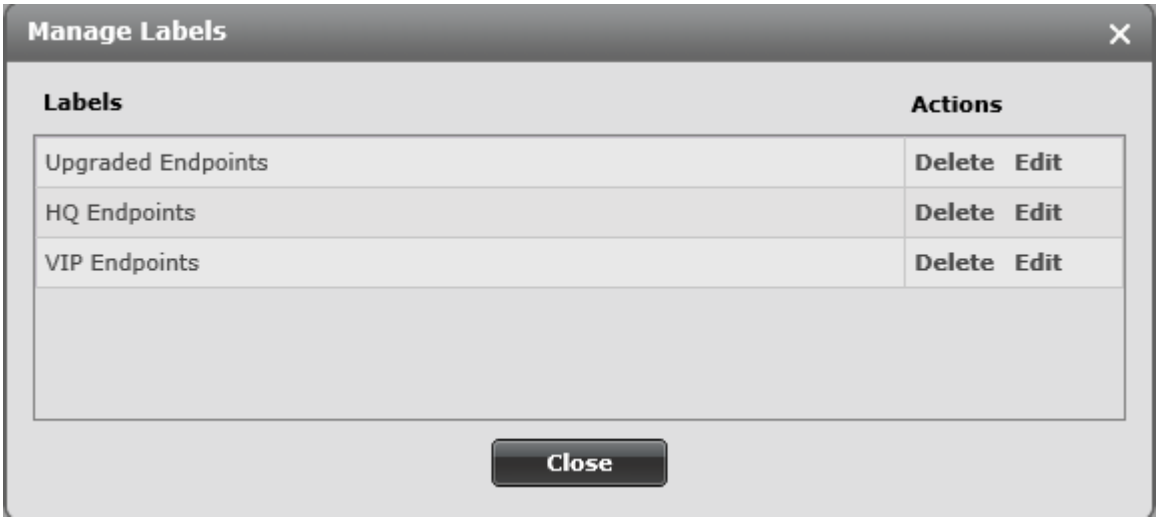


Figure 31: Managing endpoint labels

- Click **Delete** to remove the label from Equinox Management and click **OK**.
- Click **Edit** to modify the label name and select **OK**.

Related links

Planning and configuring endpoints in Equinox Management on page 120

Configuring Avaya Equinox® Media Server for WebRTC-based calls in Over The Top deployments

About this task

If you have two instances of Avaya Equinox® Media Server where one instance is deployed as a media server and the other instance is deployed as a WebRTC gateway, you can configure the WebRTC gateway to process all WebRTC-based calls.

Before you begin

Check if Avaya Equinox® Media Server in your Over The Top deployment has one of the following:

- Two instances, one of which is deployed as a media server and the other deployed as a WebRTC gateway.
- One instance that is deployed as a media server.

Procedure

1. Log in to the Avaya Equinox® Management administrator portal.
2. Click ☰, and click **Advanced Parameters**.

   Avaya Equinox® Management displays the Advanced Parameters window.

3. In the **Property Name** field, type the following advanced command:
   `com.avaya.aawg.aemsWebrtcCapability`
4. In the **Property Value** field, do one of the following:
   - If you have two instances of Avaya Equinox® Media Server where one instance is deployed as a media server and the other instance is deployed as WebRTC gateway, type `false`.

     If you have only one instance of Avaya Equinox® Media Server deployed as a media server, type `true`.
5. Click **Apply**.

Result

If you set **`com.avaya.aawg.aemsWebrtcCapability`** to:

- *false*, Avaya Equinox® Media Server deployed as a WebRTC gateway processes all WebRTC-based calls.
- *true*, Avaya Equinox® Media Server deployed as a media server processes all WebRTC-based calls.

Related links

Defining your video network devices on page 58

Configuring Avaya Equinox® Media Server for WebRTC-based calls in Team Engagement deployments

About this task

Depending on your Team Engagement deployment, you can configure either Avaya Equinox® Media Server or Avaya Aura® Media Server to process all WebRTC-based calls.

Before you begin

Using Avaya Aura® System Manager, check whether your Team Engagement deployment contains Avaya Aura® Media Server.

Procedure

1. Log in to the Avaya Equinox® Management administrator portal.
2. Click ☰, and click **Advanced Parameters**.

   Avaya Equinox® Management displays the Advanced Parameters window.
3. In the **Property Name** field, type the following advanced command:
   `com.avaya.aawg.aemsWebrtcCapability`

4. In the **Property Value** field, do one of the following:
   - If you have bothAvaya Equinox® Media Server and Avaya Aura® Media Server deployed, type `false`.
   - If you have only Avaya Equinox® Media Server deployed, type `true`.
5. Click **Apply**.

Result

If you set **`com.avaya.aawg.aemsWebrtcCapability`** to:

- *false*, Avaya Aura® Media Server processes all WebRTC-based calls.
- *true*, Avaya Equinox® Media Server processes all WebRTC-based calls .

Next steps

Disable the **Force Media Server usage for Webrtc call** option for Avaya Aura® Media Server on the Avaya Aura® Web Gateway administration portal.

For more information, see *Administering the Avaya Aura® Web Gateway* on the Avaya Support website at http://support.avaya.com/.

Related links

Defining your video network devices on page 58

Planning and configuring streaming and recording servers in Equinox Management

This section describes how to configure and manage Avaya Equinox® Streaming and Recording Servers.

The following Avaya Equinox® streaming and recording solutions are available:

- The Recording and Streaming Content Center solution, which has all the basic recording and streaming functionalities.
- The Avaya Equinox® Streaming and Recording solution, which has many advanced recording and streaming capabilities, including:
  - Publishing events, programs, and playlists throughout your organization, or to remote users using a Content Delivery Network (CDN).
  - Advanced scalability of up to 100,000 live views.
  - Up to 400 concurrent playbacks (VOD).
  - A YouTube-like portal, to enable convenient video management and quick searches.
  - Distributed deployments for large organizations.
  - MP4 download for offline viewing.

For more details, see Avaya Equinox® Streaming and Recording documentation.

The BurstPoint Video Communication Platform (VCP) is an end-to-end video distribution and communications solution that allows you to publish events, programs, and playlists throughout your organization, or to remote users using a Content Delivery Network (CDN).

The Avaya Equinox® Streaming and Recording is a video network device that provides advanced recording and streaming functionality for your Avaya Scopia® Solution.

You add Equinox Streaming and Recording Servers to a specific organization or branch, according to pre-defined network topologies. For more information see the *Equinox Solution Guide*.

Related links

Defining your video network devices on page 58
Adding and Modifying Equinox Streaming and Recording Servers in Equinox Management on page 177

Adding and Modifying Equinox Streaming and Recording Servers in Equinox Management

About this task

This section explains how to configure Avaya Equinox® Streaming and Recording Server settings in Equinox Management.

Procedure

1. Access the Equinox Management administrator portal.
2. In the **Devices** tab, select **Streaming & Recording Server**.
3. If you are modifying the Equinox Streaming and Recording Server, select the link in the **Name** column, or select **Add** to create the Equinox Streaming and Recording Server profile. The **Add Streaming & Recording Server** page appears (Figure 32: Adding an Avaya Equinox® Streaming and Recording server on page 177).

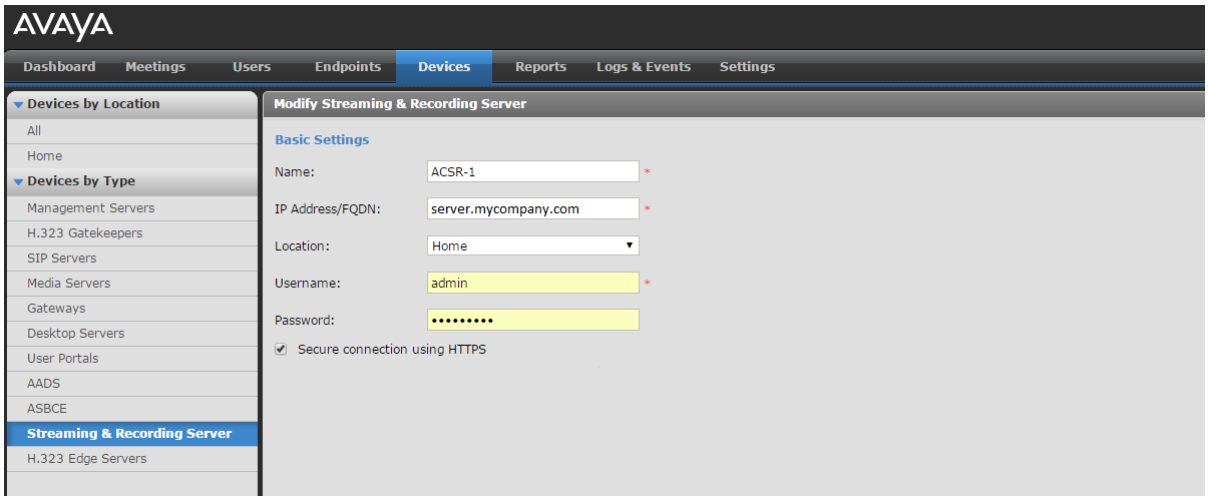


Figure 32: Adding an Avaya Equinox® Streaming and Recording server

4. Configure the Equinox Streaming and Recording Server's settings, as described in (Table 39: Configuring the Avaya Equinox® Streaming and Recording on page 178).

Table 39: Configuring the Avaya Equinox® Streaming and Recording

Field Name	Description
Name	Enter a name to identify the Equinox Streaming and Recording Server.
IP address/FQDN	Enter the management IP address or the FQDN of the Equinox Streaming and Recording Server. If the server is being deployed in the DMZ, this value must be an FQDN or an IP address that everyone can access. If the server is being deployed inside the network but is accessible externally using reverse proxy, this value must be an FQDN which resolves to the reverse proxy when outside the network.
Username	Enter the administrative username used to login to the Equinox Streaming and Recording Server portal. The default is **admin**. If you change the username in the Equinox Streaming and Recording Server, you must update the username here.
Password	Enter the administrative password used to login to the Equinox Streaming and Recording Server portal. The default is **admin**. If you change the password in the Equinox Streaming and Recording Server, you must update the password here.
Secure connection using HTTPS	Select to enable HTTPS, which encrypts the communication between the Equinox Streaming and Recording Server and the client. To enable HTTP, deselect the checkbox. **Important:** This option is not available until you first configure the server in Equinox Management, and it connects to the Equinox Streaming and Recording Server. When you subsequently open this page, the option becomes available only if you have a regular license. If you have a non-encrypted license, you cannot secure the connection.

5. Select **OK** to save your changes.

Related links

Planning and configuring streaming and recording servers in Equinox Management on page 176

Chapter 4: Securing your video network

This chapter describes how to secure the communication between Equinox Management and other components (such as other Equinox Solution products, Avaya Session Manager, and your LDAP server), and how to secure your browser access to Equinox Management using the HTTPS protocol.

Related links

Securing web access to Equinox Management using HTTPS on page 179
Securing the connection between Equinox Management and an LDAP server on page 181
Securing your video network using TLS on page 181
Configuring account policies in Avaya Equinox® Management on page 206
Configuring meeting policies PIN security on page 209
Configuring Cross-Origin Resource Sharing (CORS) on page 212
Configuring the Enhanced Access Security Gateway (EASG) on page 213
Importing a CA certificate on page 213
Enabling hardening for the Avaya Equinox management server on page 214
Enabling FIPS compliance for redundancy mode on page 215
Enabling composite video for virtual rooms on page 216

Securing web access to Equinox Management using HTTPS

HTTPS is the secured version of the standard web browser protocol HTTP. It secures communication between a web browser and a web server through authentication of the web site and encrypting communication between them. For example, you can use HTTPS to secure web browser access to the web interface of many Equinox Solution products.

You can use HTTPS to encrypt communications between Equinox Management and anyone logging in to manage it using a web browser.

Important:

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

Once Equinox Management's computer (application server) installs the full (private key) certificate, its communications are encrypted, and only browsers with a corresponding matching (public key) certificate can understand the communication. A private key certificate and its public key certificate are created as a matching pair.

Typically, you request a trusted third party certification authority (CA) to issue a certificate which contains the encryption keys to be used for secure communications. A trusted CA signs all the certificates they issue. A trusted signature ensures that Equinox Management is who it claims to be, and not an imposter. Popular web browsers are preconfigured to trust certificates that are signed by well-known CAs.

In your deployment, it may be good enough for you to issue your own certificates as an administrator if you are solely responsible for both the server's installation (Equinox Management) and the client side (the browser). Certificates that you issue are self-signed. Most web browsers will issue an alert when communicating with servers whose certificate is not signed by a well-known CA, questioning the trustworthiness of the server.

When securing web access to Equinox Management using HTTPS, you must also configure the tomcat webserver to use HTTPS (see Configuring the Tomcat web server to use HTTPS on page 180).

Related links

Securing your video network on page 179
Configuring the Tomcat web server to use HTTPS on page 180

Configuring the Tomcat web server to use HTTPS

About this task

This procedure details how to configure the Tomcat web server to use HTTPS (SSL).

Important:

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

Procedure

1. Open the *server.xml* file, located in *tomcat\conf*:

```
<Connector connectionTimeout="20000" port="8080"
     protocol="org.apache.coyote.http11.Http11NioProtocol"
redirectPort="9443"/>

<Connector port="9443"
     protocol="org.apache.coyote.http11.Http11NioProtocol"
SSLEnabled="true"
     maxThreads="150" scheme="https" secure="true"
     keystoreFile="conf/iview.keystore" keystorePass="avaya"
     clientAuth="false" sslProtocol="TLS" />
```

2. Comment out the following line by adding a comment indicator at the beginning and the end:

```
<!--Connector connectionTimeout="20000" port="8080"
     protocol="org.apache.coyote.http11.Http11NioProtocol"
redirectPort="9443"/-->
```

3. Restart the Equinox Management service.

   You can now access Equinox Management from your web browser using HTTPS.

Related links

Securing web access to Equinox Management using HTTPS on page 179

Securing the connection between Equinox Management and an LDAP server

About this task

There are two ways to secure Equinox Management's connection to your LDAP server:

- Securing the connection with SSL/TLS. This is available for both Microsoft Active Directory and IBM Domino.

  For this option, you need to enable SSL/TLS on your LDAP server and then to configure Equinox Management to use the *ldaps://* prefix for the LDAP, as described in Connecting Equinox Management with the LDAP server on page 239.

- Securing the login credentials with MD5 (see Downloading Users from the LDAP Server on page 242). This is available only for Microsoft Active Directory.

Important:

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

Related links

Securing your video network on page 179

Securing your video network using TLS

You can configure your video network devices, both Equinox Solution and third-party, to support Transport Layer Security (TLS) for the SIP protocol and for connection to the XT Series web server when using HTTPS. TLS enables network devices to communicate securely using certificates, to provide authentication of the devices and encryption of the communication between them.

Important:

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

TLS is used to secure the connection between Equinox Management and the following solution components:

- Scopia Elite MCU
- Avaya Room System XT Series
- Avaya Web Collaboration server
- Avaya Session Manager

Every network component must have its own TLS certificate to authenticate itself. Some of the components have a pre-installed TLS certificate. You must create a TLS certificate for components that do not have a pre-installed TLS certificate.

Note:

Equinox Management does not support wildcard certificates.

Communication between Equinox Management and the LDAP server can also be secured using TLS, but it does not require a TLS certificate for Equinox Management.

Pre-installed certificates of some of the components are not unique and cannot guarantee strong authentication. For more reliable security, create a new, unique certificate for these components.

Important:

Changing certificates can cause major service interruptions. Ensure that your device possesses the root CA certificate of the CA that issued the identity certificate, and that the root CA certificate is stored in a trust store.

To create a TLS or HTTPS web certificate, you need to generate a certificate signing request (CSR) and send it to the certification authority (CA) for signing. A CA has its own certificate, known as the CA root certificate. When the CA signed certificate is ready, you upload it into the component for which it was created, together with the CA root certificate. Once this is done, the component can authenticate itself and is ready for TLS connection.

In some cases, when different CAs are used for signing certificates in your deployment, you must obtain an additional certificate vouching for the trustworthiness of these CAs. These certificates are known as intermediary certificates, and must be signed by a trusted CA. For more information, see Planning the required certificates for TLS on page 184.

Each time a video network device starts the TLS communication session, it sends its own signed certificate together with the CA root certificate and requests the same certificates from the other devices to which it wants to connect. After both devices verify each other's identity, a secure TLS connection can be established. Exchanging certificates between devices is part of the TLS protocol; it happens in the background and is transparent to a user.

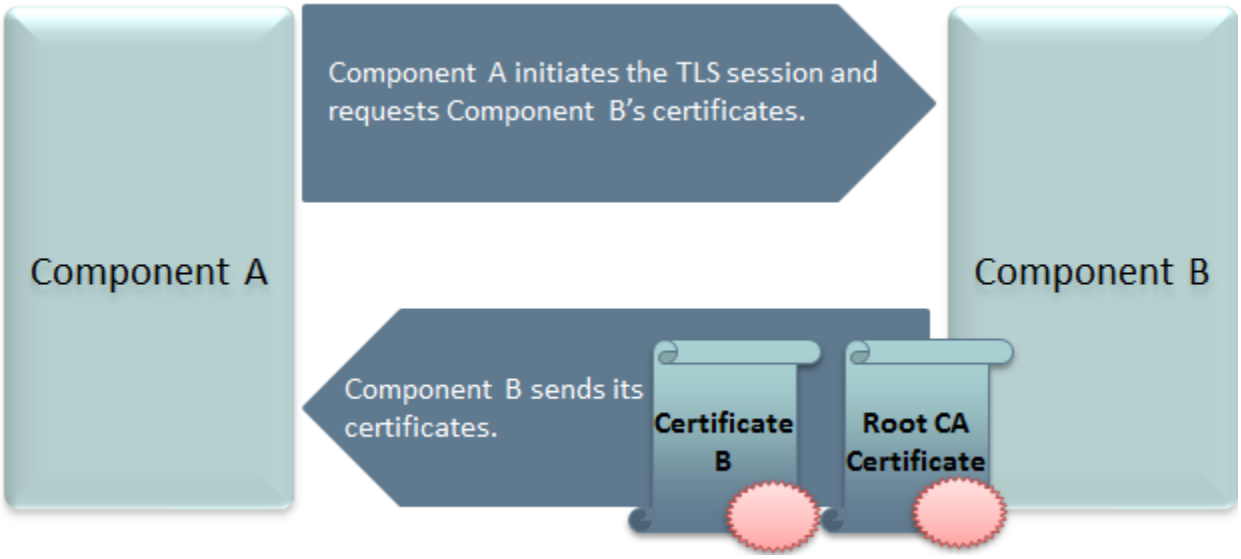


Figure 33: Establishing TLS connection

The following set of procedures secure the connection between Equinox Management and other devices. Perform these tasks in the order listed below:

1. Decide your deployment's TLS requirements, as described in Planning the required certificates for TLS on page 184.
2. Prepare the TLS certificate for Equinox Management, as described in Creating and uploading Equinox Management's certificate for videoconferencing components on page 192.
3. Create TLS certificates for components listed below and upload certificates onto the components for which they are created. Enable TLS encryption on the following components:
   - Web Collaboration server (see Web Collaboration server documentation)
   - MCU (see the *Administrator Guide for Scopia Elite MCU*)
   - XT Series (see the *Deployment Guide for XT Series*)
   - Avaya Session Manager, as detailed in the product's documentation
   - Other videoconferencing components, as detailed in the product's documentation.
4. If the CA used to identify some devices is different from the CA which identifies Equinox Management, perform Importing third-party root CA and intermediate CA certificates on page 196.

Related links

Securing your video network on page 179
Planning the required certificates for TLS on page 184
TLS connections to devices with identity certificates on page 191
Creating and uploading Equinox Management's certificate for videoconferencing components on page 192

Importing third-party root CA and intermediate CA certificates on page 196
TLS client support for extended hostname or domain validation on page 198
Certificate revocation validation on page 199
Removing trusted CA certificates on page 200
Exporting the root CA certificate of an internal or third-party CA on page 201
Configuring Equinox Management as a Certificate Authority on page 202
Securing TLS connections for Equinox Management on page 203
Securing TLS connections for a distributed AAWG/Portal on page 204
Troubleshooting TLS connections on page 205

Planning the required certificates for TLS

When a device establishes a secure TLS connection with another component, it requests a signed certificate verifying the other component's identity. The signature on the certificate must be from a known (trusted) certification authority (CA).

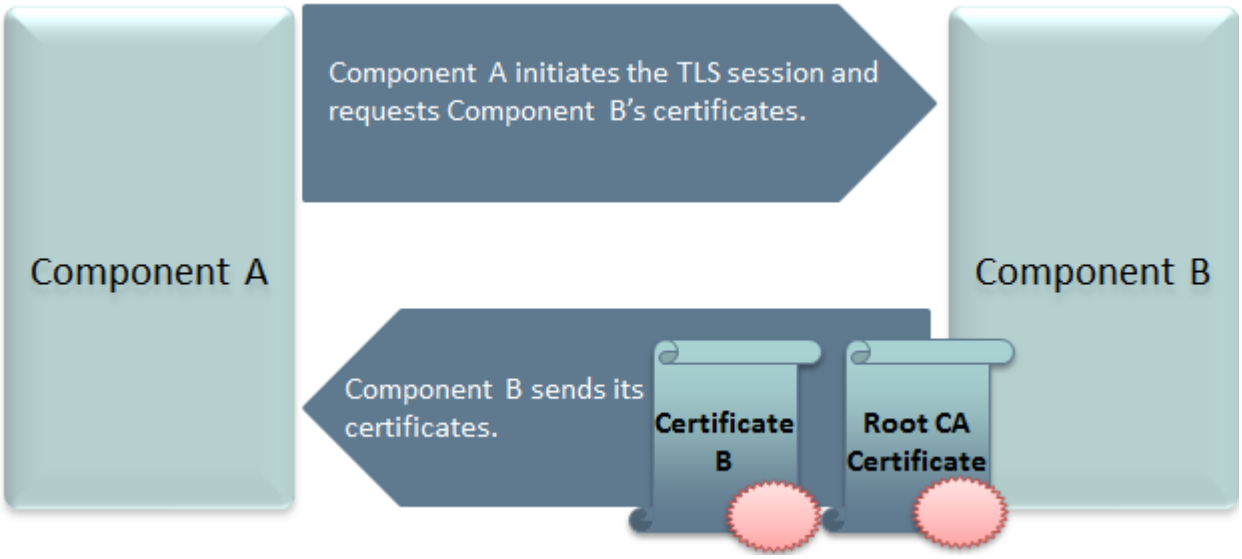


Figure 34: Certificate request

Important:

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

There are several types of TLS connections:

- Standard TLS, where all certificates are signed by the same CA.
- Unique CAs, where each certificate is signed by a different CA.
- Unknown gateway CA, where the gateway's certificate is signed by an unknown (untrusted) CA.

- Unknown Equinox Management CA, where Equinox Management's certificate is signed by an unknown (untrusted) CA.
- Mutually unknown CAs, where both components carry certificates signed by CAs that are unknown to each other.

Each situation requires a different set of certificates to be uploaded to each of the components. Typically, the certificates are all signed by the same CA. Some unique deployments, such as service provider deployments, may use multiple CAs.

A CA's signature is always verified by its root certificate, which identifies the CA and is self-signed by that CA. When a device receives a certificate as part of TLS negotiations, it must verify that the CA signing the certificate is trusted, so it must have the CA's root certificate uploaded.

All the Equinox Management services support validation of peer Identity Certificates that have a SHA2 signature and have a public key length of 2048 bits. Equinox Management verifies that the peer identity certificate can be traced all the way to a trusted root CA certificate. The root CA certificate must reside in the service's trust store.

For the TLS connection, the identity certificate is validated using standard path validation which complies with the RFC5280 section *Certificate Path Validation*. For trusted SIP TLS connections, the Equinox Management SIP server applies mutual TLS authentication, where both the SIP entity and Equinox Management SIP server validate each other's certificates.

- **Standard TLS**

  These connections use the same CA for signing all certificates on both sides. In this case, you need to upload two certificates to Equinox Management and two for the gateway (Figure 35: Standard TLS: Component certificates and a CA root certificate on page 185).

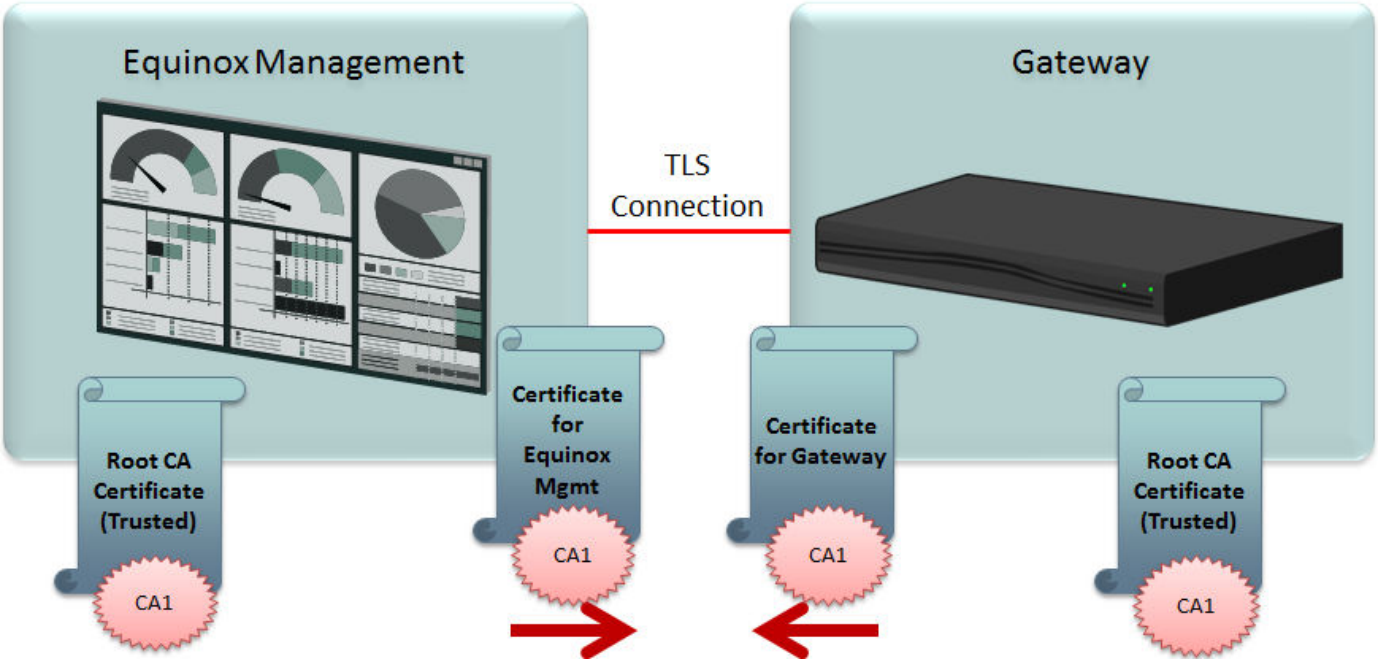


Figure 35: Standard TLS: Component certificates and a CA root certificate

Upload the following certificates to Equinox Management:

- A certificate identifying Equinox Management, signed by the CA. This is sent to the gateway as part of the TLS negotiation.
- A root certificate verifying the CA's identity, self-signed by that CA. This is used by Equinox Management to verify the certificate sent by the gateway.

On the gateway side, upload the following certificates:

- A certificate identifying the gateway, signed by the same CA. This is sent to Equinox Management as part of the TLS negotiation.
- A copy of the root certificate verifying the CA's identity, self-signed by the CA. This is used by the gateway to verify the certificate sent by Equinox Management.

• **Unique CAs**

When certificates are signed by different CAs, each CA requires its own root certificate to be uploaded for authentication.

For example, in Figure 36: TLS connection using certificates signed by different CAs on page 186, the certificate identifying Equinox Management is signed by CA1, while the gateway's certificate is signed by CA2. This requires three certificates to be uploaded to Equinox Management and two for the gateway.

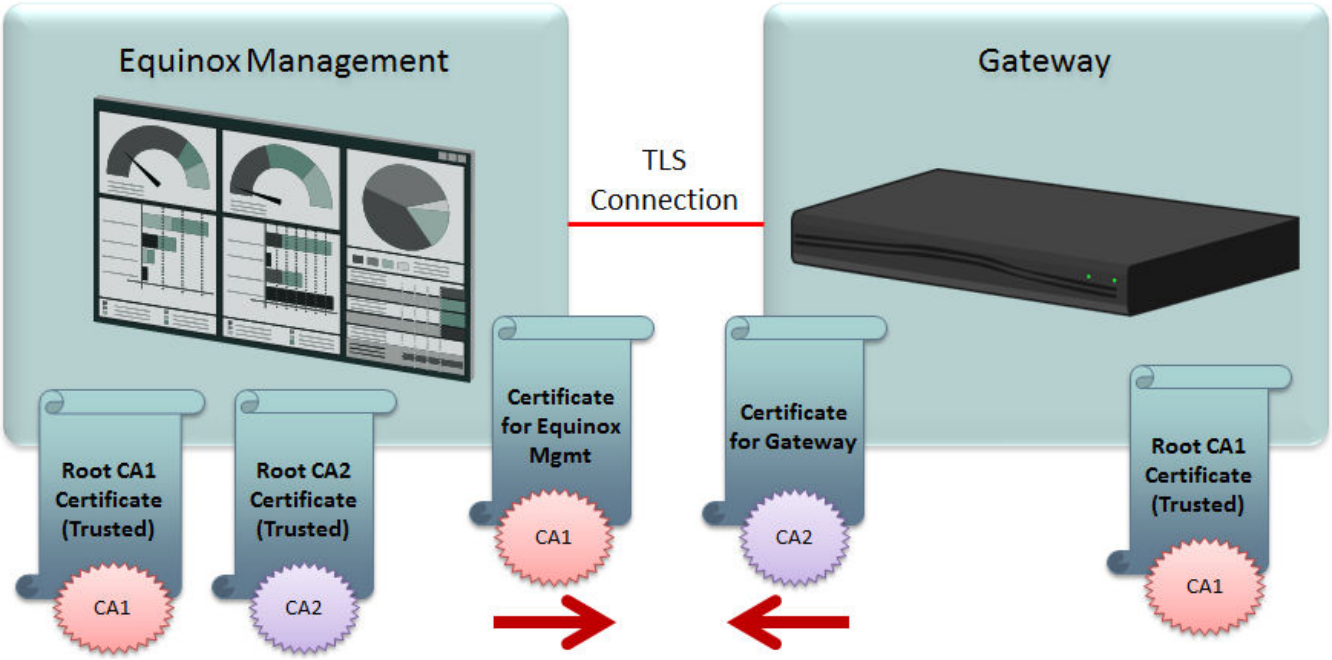


Figure 36: TLS connection using certificates signed by different CAs

When each certificate is signed by a different CA, upload the following certificates to the Equinox Management:

- A certificate identifying Equinox Management, signed by trusted CA1. This is sent to the gateway as part of the TLS negotiation.

- A root certificate from the trusted CA1 verifying CA1's identity, self-signed by CA1. This is used by Equinox Management to authenticate its certificate.
- A root certificate from the trusted CA2 verifying CA2's identity, self-signed by CA2. This is used by Equinox Management to authenticate the certificate sent by the gateway, which is signed by CA2.

On the gateway side, upload the following certificates:

- A certificate identifying the gateway, signed by trusted CA2. This is sent to Equinox Management as part of the TLS negotiation.
- A root certificate verifying CA1's identity, self-signed by trusted CA1. This is used by the gateway to verify the certificate sent by Equinox Management, which is signed by CA1.

• **Unknown gateway CA**

If the CA of the gateway's certificate is unknown, it cannot be trusted unless it comes with an intermediate certificate, which vouches for the trustworthiness of the unknown CA. Intermediate certificates must be signed by a trusted CA.

For example, in Figure 37: Signature of Gateway Certificate from Unknown CA on page 187, the certificate identifying the gateway is signed by CA3, which may be known and trusted by those who installed the gateway, but in this scenario, CA3 is not trusted by Equinox Management. Meanwhile, Equinox Management's certificate is signed by CA1, a trusted CA. This scenario requires four certificates to be uploaded to Equinox Management and two for the gateway.

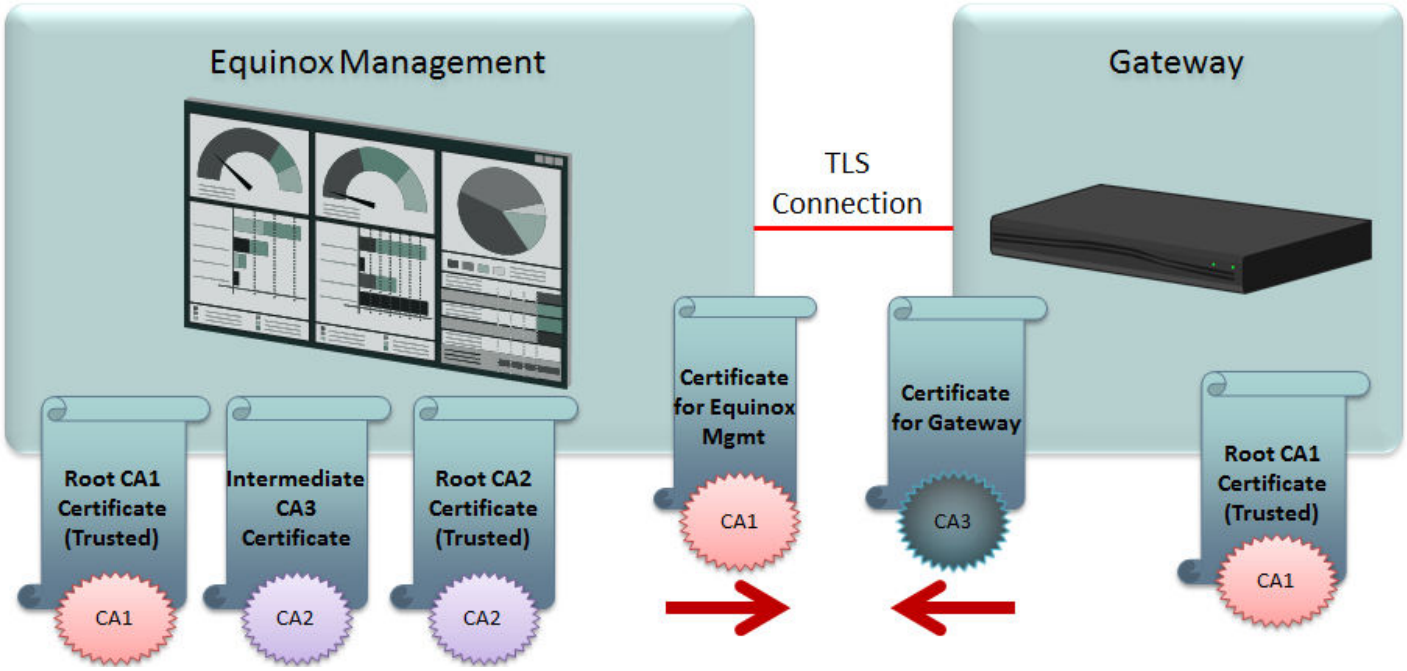


Figure 37: Signature of Gateway Certificate from Unknown CA

When CA3 is untrusted, the certificates to upload to Equinox Management are:

- A certificate identifying Equinox Management, signed by trusted CA1. This is sent to the gateway as part of the TLS negotiation.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by Equinox Management to authenticate its certificate.
- An intermediate certificate vouching for the trustworthiness of CA3, signed by trusted CA2. This is used to trust the certificate sent by the gateway, which is signed by CA3.
- A root certificate from CA2 verifying CA2's identity, self-signed by trusted CA2. This is used by Equinox Management to authenticate the intermediate certificate, which is signed by CA2.

On the gateway side, the certificates to be uploaded are (Figure 37: Signature of Gateway Certificate from Unknown CA on page 187):

- A certificate identifying the gateway, signed by CA3, an unknown CA. This certificate is sent to Equinox Management as part of the TLS negotiation.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by the gateway to verify the certificate sent by Equinox Management, which is signed by CA1.

• **Unknown Equinox Management CA**

When Equinox Management's certificate is signed by a CA unknown to the gateway, you must upload an intermediate certificate for the untrusted CA signed by a trusted CA to vouch for its authenticity.

In the example of Figure 38: Signature of Equinox Management certificate from unknown CA on page 189, Equinox Management's certificate is signed by CA3, an unknown CA, while the gateway's certificate is signed by CA2, a trusted CA. This requires four certificates to be uploaded to Equinox Management and three for the gateway.

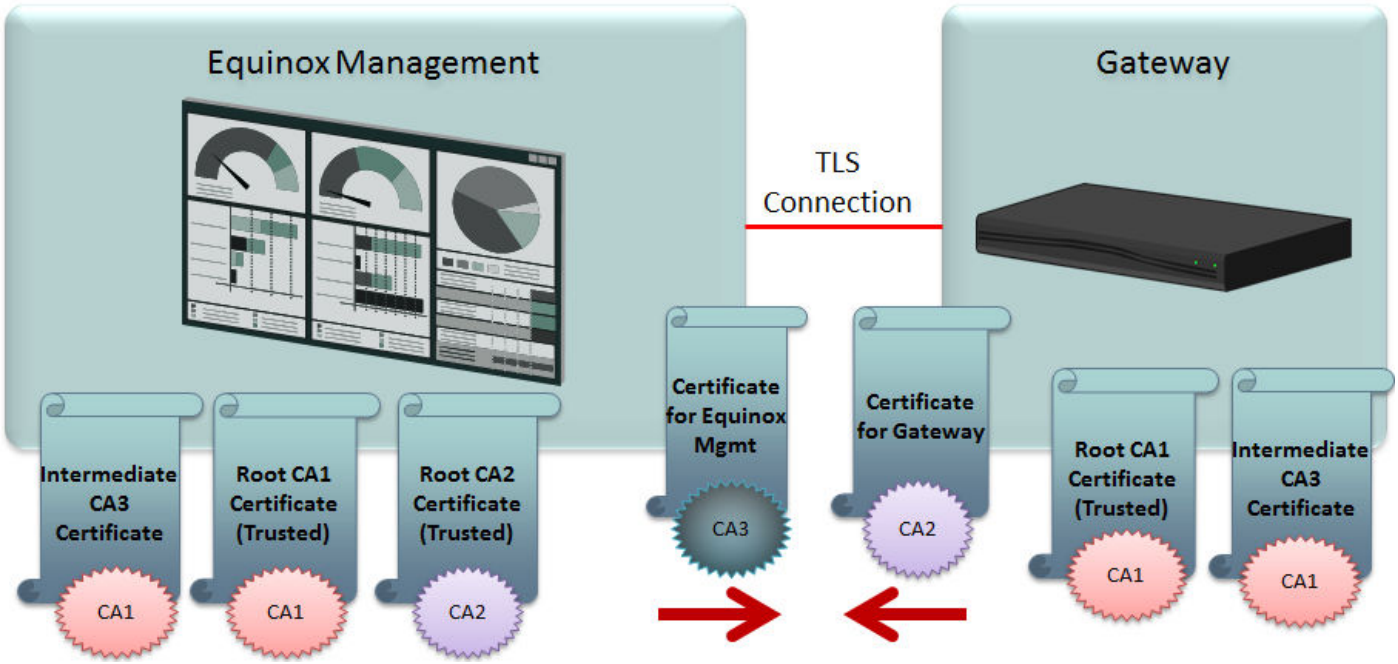


Figure 38: Signature of Equinox Management certificate from unknown CA

When CA3 is untrusted by the gateway, the certificates to upload to the Equinox Management are:

- A certificate identifying Equinox Management, signed by CA3, a CA unknown to the gateway. This is sent to the gateway as part of the TLS negotiation.
- An intermediate certificate vouching for the trustworthiness of CA3, signed by trusted CA1. This is used to trust Equinox Management's identity certificate, which is signed by CA3.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by Equinox Management to authenticate the intermediate certificate, which was signed by CA1.
- A root certificate from CA2 verifying CA2's identity, self-signed by trusted CA2. This is used by Equinox Management to authenticate the gateway's certificate, which is signed by CA2.

On the gateway side, the certificates to be uploaded are:

- A certificate identifying the gateway, signed by trusted CA2. This certificate is sent to Equinox Management as part of the TLS negotiation.
- An intermediate certificate vouching for the trustworthiness of CA3, signed by trusted CA1. This is used to trust Equinox Management's identity certificate, which is signed by CA3.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by the gateway to verify the intermediate certificate, which is signed by CA1.

• **Mutually unknown CAs**

In the final scenario, both components use certificates signed by CA's which are not recognized by each other. In this case, there must be two intermediate certificates, one for each of the untrusted CAs, to vouch for their authenticity.

For example, in Figure 39: Signature of Both Certificates are from Untrusted CAs on page 190, the certificate identifying the gateway is signed by CA4, an unknown CA, while Equinox Management's certificate is signed by CA3, also untrusted. This would require five certificates to be uploaded to Equinox Management and three for the gateway.

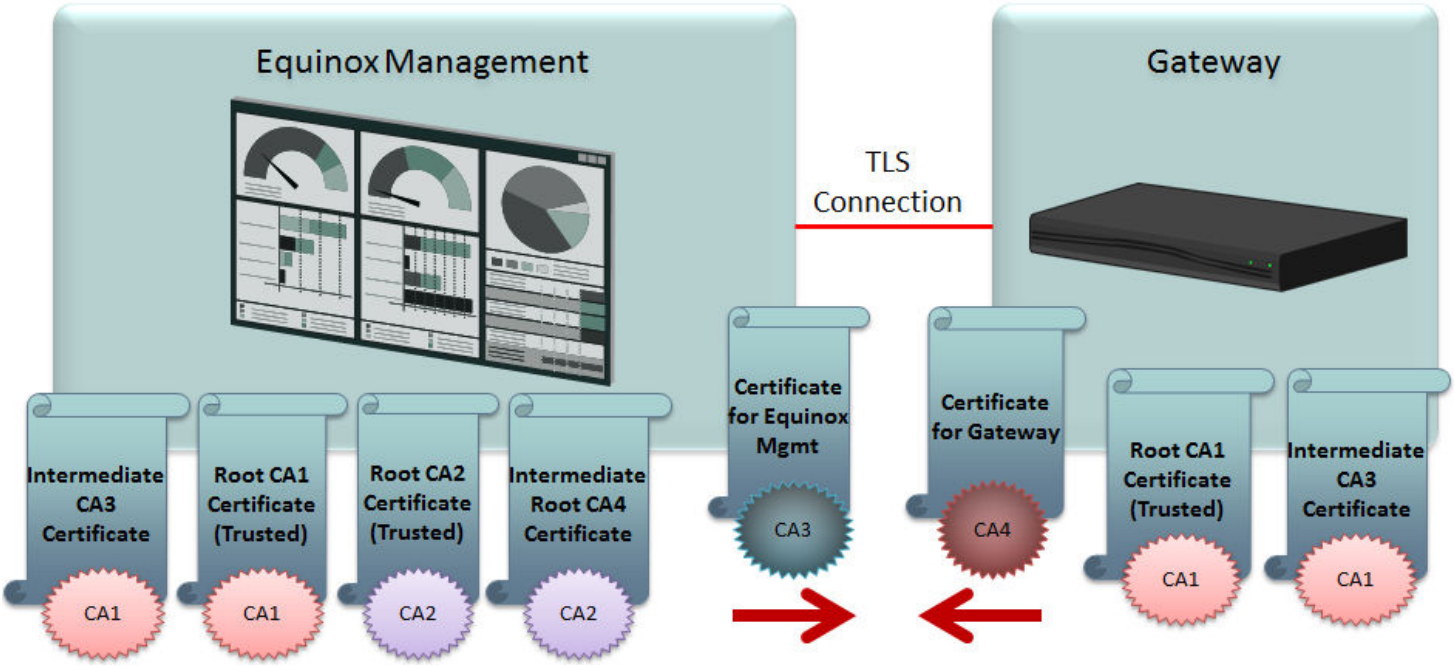


Figure 39: Signature of Both Certificates are from Untrusted CAs

When CA3 is untrusted by the gateway and CA4 is untrusted by Equinox Management, the certificates to upload to the Equinox Management are:

- A certificate identifying Equinox Management, signed by CA3, a CA unknown to the gateway. This is sent to the gateway as part of the TLS negotiation.
- An intermediate certificate vouching for the trustworthiness of CA3, signed by trusted CA1. This is used to trust Equinox Management's identity certificate, which is signed by CA3.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by Equinox Management to authenticate CA3's intermediate certificate, which was signed by CA1.
- A root certificate from CA2 verifying CA2's identity, self-signed by trusted CA2. This is used by Equinox Management to authenticate CA4's intermediate certificate, which is signed by CA2.
- An intermediate certificate vouching for the trustworthiness of CA4, signed by trusted CA2. This is used to trust the gateway's identity certificate, which is signed by CA4.

On the gateway side, the certificates to be uploaded are:

- A certificate identifying the gateway, signed by CA4, a CA unknown to Equinox Management. This is sent to Equinox Management as part of the TLS negotiation.
- An intermediate certificate vouching for the trustworthiness of CA3, signed by trusted CA1. This is used to trust Equinox Management's identity certificate, which is signed by CA3.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by the gateway to verify the intermediate certificate, which is signed by CA1.

For more information on uploading certificates to the gateway and to Equinox Management, see Securing your video network using TLS on page 181.

If you have the Equinox Management redundant solution, it is important to configure redundancy before proceeding with TLS configuration. See Creating a Redundant Secondary Server for Equinox Management on page 380 for details.

Related links

Securing your video network using TLS on page 181

TLS connections to devices with identity certificates

The following table describes the TLS connections between Equinox Management and devices with identity certificates. All connections support 2048 key length and SHA2 signature.

Additionally, the table also indicates the trusted CA certificates (saved in the Equinox Management trust store) which Equinox Management uses to verify the certificate of the device with which it is connected.

Connections to Devices with Identity Certificates

The column headers of the table are as follows:

- **Service name**: The purpose of the connection.
- **To/From**: The direction of the connection. The first component listed is responsible for verifying the connection; a double arrow (**<>**) indicates that there is mutual verification between the components.
- **Protocol**: The protocol used in the connection.
- **Port**: The port number used in the connection.

Table 40: TLS connections

Service name	To/From	Protocol	Port
Administration	Equinox Management > MCU	TLS	3346
Control	Equinox Management > MCU	TLS	3348
Control	WCS > Equinox Management	HTTPS	9943
Administration — JMX	Equinox Management <> WCS	JMX	5556

Table continues…

Service name	To/From	Protocol	Port
File Transfer	Equinox Management > MCU	HTTPS	8445
Administration	Equinox Management > PF	TLS	8089
Administration/Control	Equinox Management > SDS	TLS	3340
Administration/Control	Equinox Management > UCCS	TLS	3352
Administration/Control	Equinox Management > Portal	TLS	3351
Administration/Control	Equinox Management > ESG	TLS	3353
Administration/Control	Equinox Management > AADS	TLS	3354
Administration/Control	Equinox Management > PMGR	TLS	3368
File Transfer	Equinox Management > PMGR	HTTPS	8445
SIP	MCU/AAMS <> Equinox Management	SIPS	5061
Web UA	Equinox Management <> AAMS	HTTPS	7151
SOAP Server	Equinox Management <> AAMS	HTTPS	7411

Related links

Securing your video network using TLS on page 181

Creating and uploading Equinox Management's certificate for videoconferencing components

About this task

This section explains how to generate and upload the TLS certificate for Avaya Equinox® Management that is used for encrypting communications between Equinox Management and other components of your video deployment.

Important:

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

To create a TLS or HTTPS web certificate, you need to generate a certificate signing request (CSR) and send it to the certification authority (CA) for signing. A CA has its own certificate, known as the CA root certificate. When the CA signed certificate is ready, you upload it into the component for which it was created, together with the CA root certificate. Once this is done, the component can authenticate itself and is ready for TLS connection.

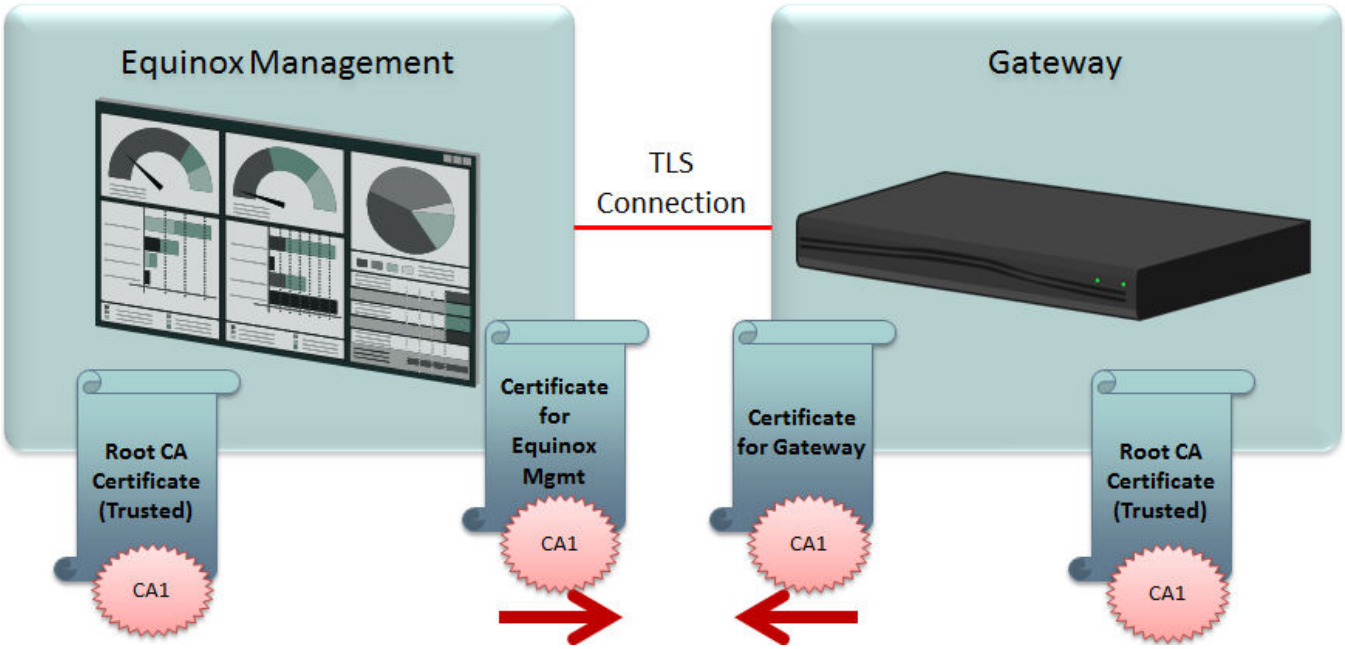


Figure 40: Typical TLS communication with a gateway

However, if the component certificates are signed by a different CA than Equinox Management's certificate, you may need to upload more certificates to establish authenticity, as described in Importing third-party root CA and intermediate CA certificates on page 196.

For details on configuring Equinox Management as a certificate authority, see Configuring Equinox Management as a Certificate Authority on page 202.

For details on which certificates are required, see Planning the required certificates for TLS on page 184.

Identity certificates signed by a third-party CA have a limited lifetime. An alarm is generated prior to their expiration, and the PKI Administrator renews them at that time.

Before you begin

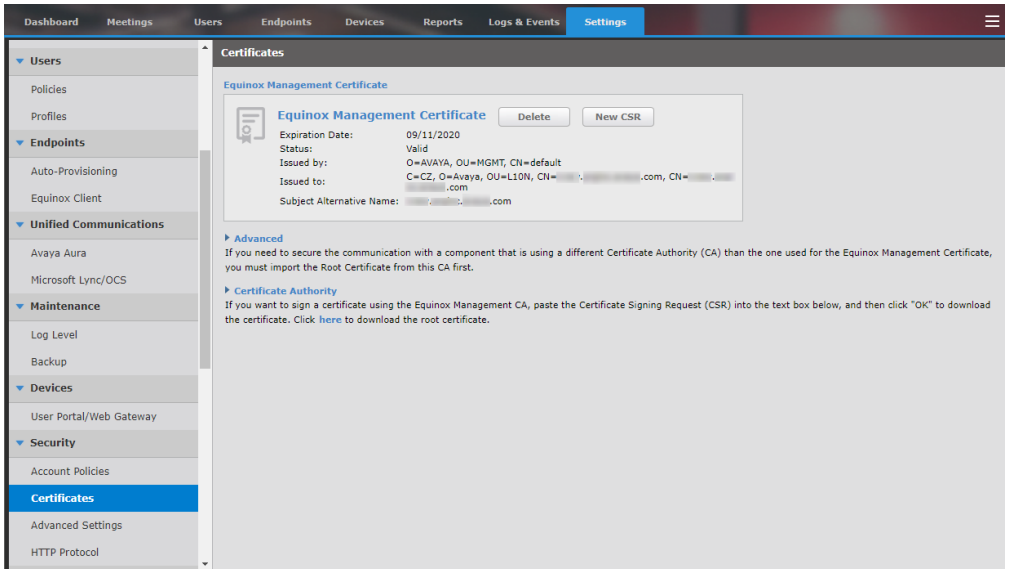
- If you have the Equinox Management redundant solution, you must configure redundancy before proceeding with TLS configuration. See Creating a Redundant Secondary Server for Equinox Management on page 380 for details.
- Verify that Equinox Management has a default identity certificate, as follows:

  Click **Settings** > **Security** > **Certificates**. If the value of the **Issued by** field is **CN=Equinox Management**, **CA,OU=MGMT**, or **O=AVAYA**, a default identity certificate is in the system and needs to be replaced.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Security** > **Certificates**.

   The system displays the **Certificates** page.



Click **New CSR** to replace the currently installed certificate.

The system displays the **Generate CSR** dialog box.

3. Enter your organization's details as described below:

Field	Description
Common Name	Enter the Equinox Management FQDN, for example, `rvcn-sm.company.com`. For a redundancy deployment, the common name must be the public virtual FQDN.

Table continues…

Field	Description
Subject Alternative Name	Enter an FQDN or IP address as the subject alternative name for the CSR. If this field is left blank, the value of the **Common Name** field is used.
Organization	The name of the organization.
Organization Unit	The unit to which the organization belongs.
City	The city in which the organization is located.
State	The state in which the organization is located.
Country code	Enter the standard country code that consists of two characters, for example *uk* for United Kingdom or *jp* for Japan. This field is not case sensitive.
Encryption Strategy	Select the code for your organization's encryption strategy.
Signature Algorithm	Select the algorithm to use when generating the signature on the certificate. This algorithm is a combination of the private keys of both the CA and the device.

4. Click **Generate CSR**.
5. Click **Save** to view the certificate content.

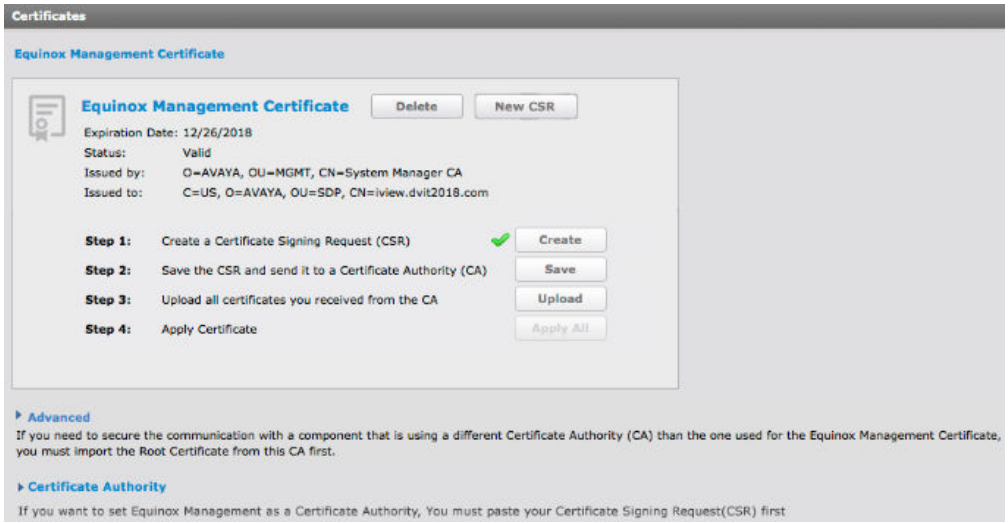
   The system displays the certificate content in the **Download** window.
6. Save the certificate in an appropriate folder.

   The system saves the certificate as a text file compatible with Base-64 ASCII code.
7. Send the text file containing the certificate for signing as a certificate compatible with Base-64 ASCII code. Select **Web Server** as the certificate template when submitting a certificate request.

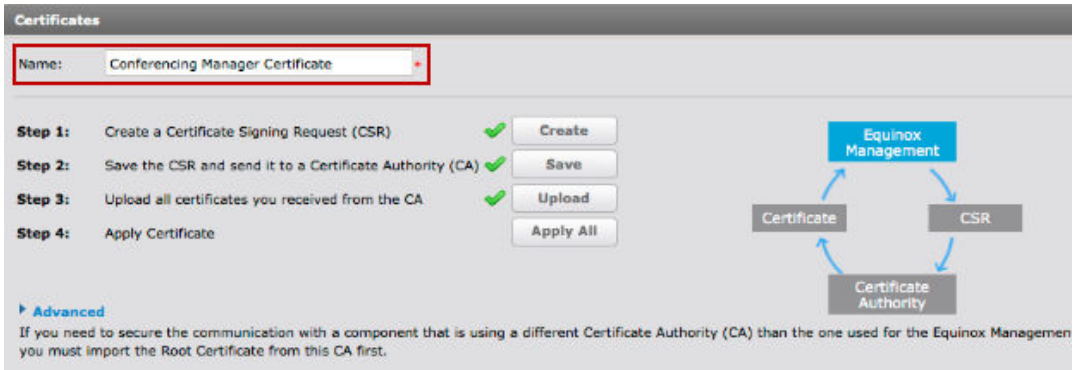
   Important:

   If other components communicating with Equinox Management also have their own certificates, we recommend using a common CA for all certificates for a more efficient implementation.
8. In the Equinox Management administrator portal, click **Settings** > **Security** > **Certificates**.

   The system displays the new certificate process on the **Certificates** page.



9. Click **Save** to save the certificate content. Click **Yes** in the confirmation dialog box to download the CSR.
10. Click **Upload** and click **Yes** in the confirmation dialog box to delete the existing certificate.
11. In the **Name** field at the top of the page, enter a name for the certificate.



12. Click **Apply All**.

    The certificate is added to Equinox Management.

Related links

Securing your video network using TLS on page 181

Importing third-party root CA and intermediate CA certificates

About this task

If you need to secure the communication with a component that uses a different certificate authority (CA) than the one used for the Equinox Management certificate, you must import the root certificate from this CA first. Perform this procedure only if the component's certificates are signed by a different CA than Equinox Management's certificate.

You can import the root and intermediate certificates to Equinox Management for devices in your deployment. Root and intermediate certificates establish the trustworthiness of each CA's signature by vouching for the CA in question. These certificates are stored in a trust store. To learn about different types of certificates, see Planning the required certificates for TLS on page 184.

Important:

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

Before you begin

- Ensure that you have the signed certificate, root certificate, and all intermediate certificates required for proper authentication of the device.
- Ensure that the root certificate is compatible with the Base-64 ASCII code.
- Upload the certificate identifying the device. For details, see the product's Administrator Guide.

Procedure

1. Click **Settings** > **Security** > **Certificates**.
2. Click **Advanced**.

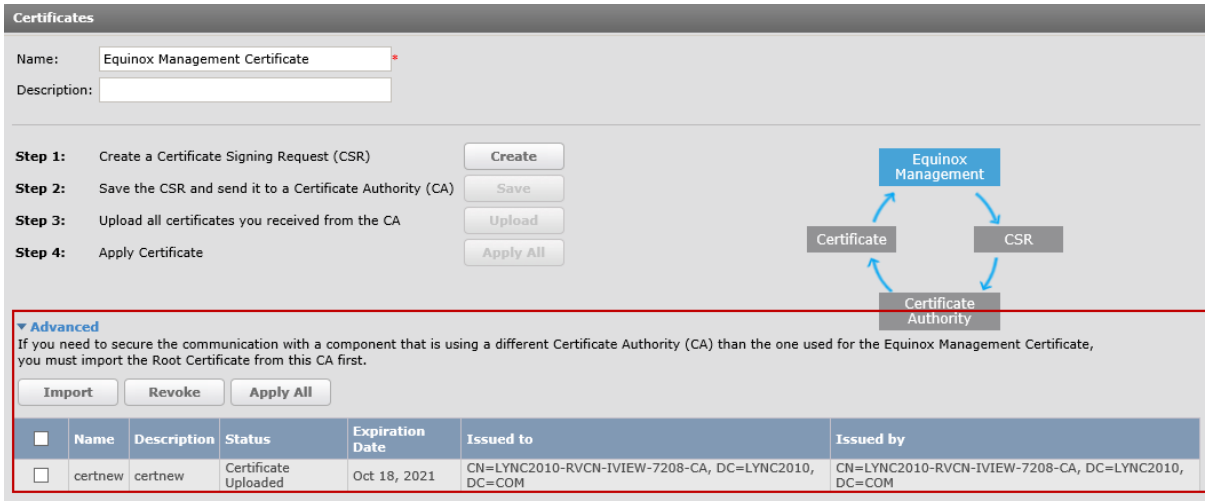


Figure 41: Certificates page — Uploading certificates for other devices

The system displays the trusted certificates in the Advanced section.

3. Click **Import**.
4. Click **Add**, browse to the required root or intermediate certificate, and click **Open**.
5. **(Optional)** Repeat the preceding step to add a root or intermediate certificate that you need to upload.
6. Click **Upload**.

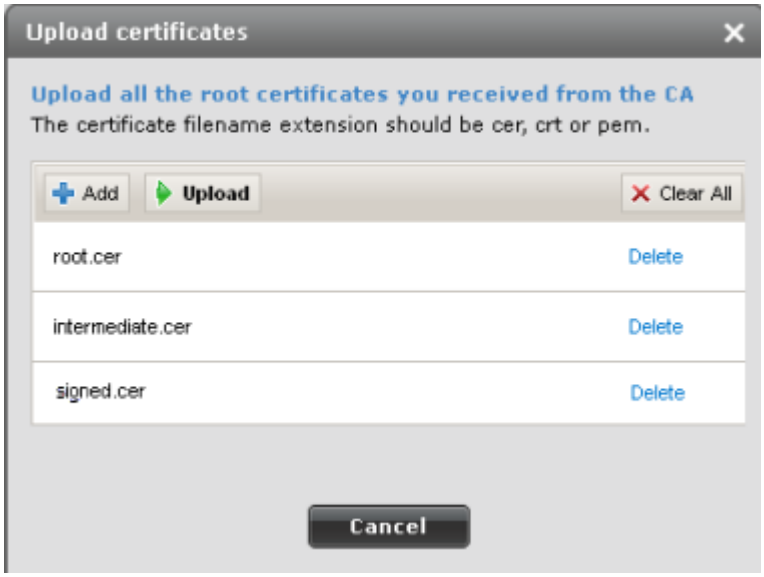


Figure 42: Importing certificates for other devices into Equinox Management

7. Select all certificates that you uploaded, and click **Apply**.

Result

The system prompts for a restart to implement the newly uploaded certificates.

Related links

Securing your video network using TLS on page 181

TLS client support for extended hostname or domain validation

About this task

You can enable and disable extended hostname validation using the vnex.vcms.core.security.hostnameVerify.enabled advanced parameter. When extended hostname validation is enabled, TLS clients verify that the certificate asserts an identity in the certificate's Subject Common Name and/or Subject Alternate Name that matches the FQDN of the established connection. If it does not match, the connection is dropped.

Procedure

1. In the Equinox Management administrator portal, click ☰ > **Advanced Parameters**

   The system displays the **Advanced Parameters** dialog box.

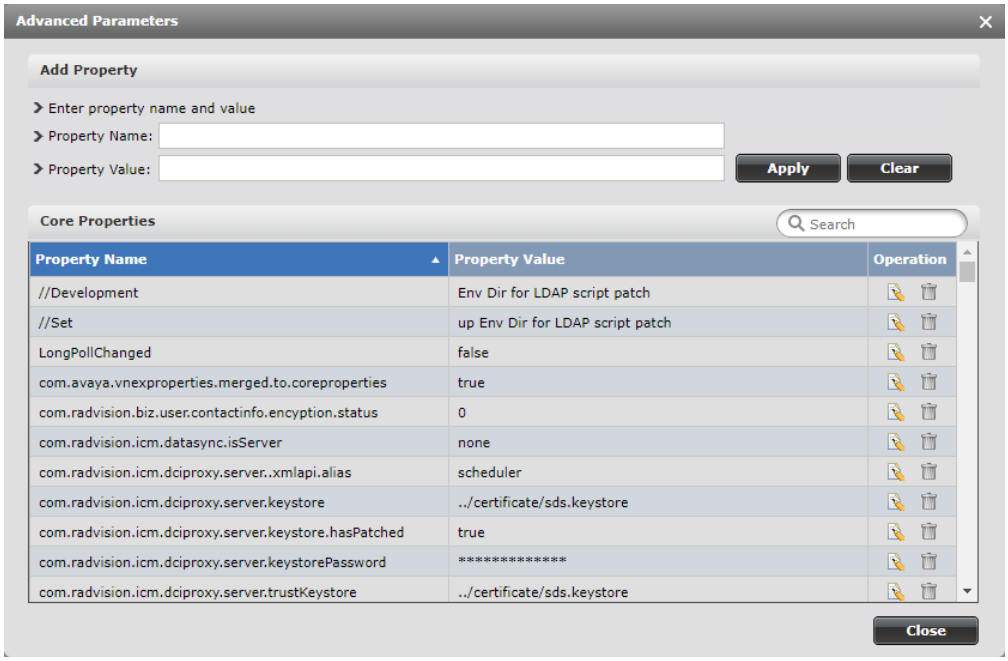


Figure 43: Advanced Parameters dialog box

2. In the **Property Name** field, enter `vnex.vcms.core.security.hostnameVerify.enabled`
3. In the **Property Value** field, enter `True` or `False`, and click **Apply**.

Related links

Securing your video network using TLS on page 181

Certificate revocation validation

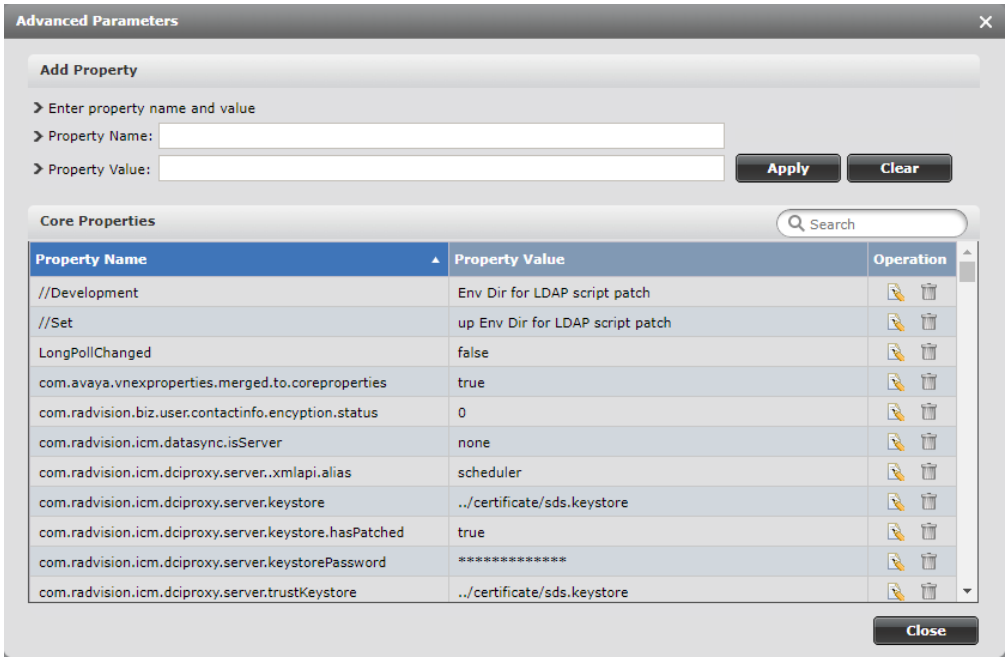
About this task

Avaya Equinox® enables you to check that certificates have not been revoked. It checks certificates all the way up the chain and honors the validity interval. All certificate validation failures due to revocation, including, TLS and IKE are logged in the audit log. The following procedure is only required if OCSP is enabled.

Procedure

1. When Avaya Equinox®starts up, in the Equinox Management administrator portal, click ☰ > **Advanced Parameters**

   The system displays the **Advanced Parameters** dialog box.



Configure the following property to enable CRL check.

2. In the **Property Name** field, enter `com.sun.net.ssl.checkRevocation`
3. In the **Property Value** field, enter `True` and click **Apply**.

Configure the following property to enable OCSP check.

4. In the **Property Name** field, enter `vnex.vcms.coresecurity.OCSP.enable`
5. In the **Property Value** field, enter `True` and click **Apply**.
6. Restart Equinox Management.

Related links

Securing your video network using TLS on page 181

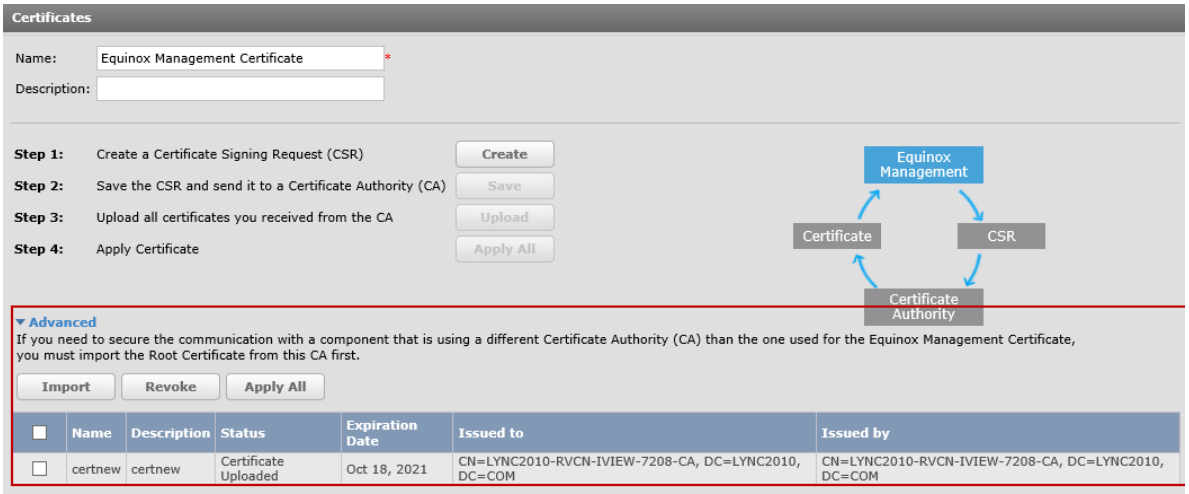
Removing trusted CA certificates

About this task

This procedure describes how to remove a trusted CA certificate.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Security** > **Certificates** > **Advanced**.



3. Select the checkbox of the trusted CA certificate you want to remove.
4. Click **Revoke**.
5. Click **Apply**. The system prompts for a restart to implement removal of the trusted CA certificate.

Note:

Equinox Management does not automatically remove revoked certificates; the PKI administrator must ensure that they are removed.

Related links

Securing your video network using TLS on page 181

Exporting the root CA certificate of an internal or third-party CA

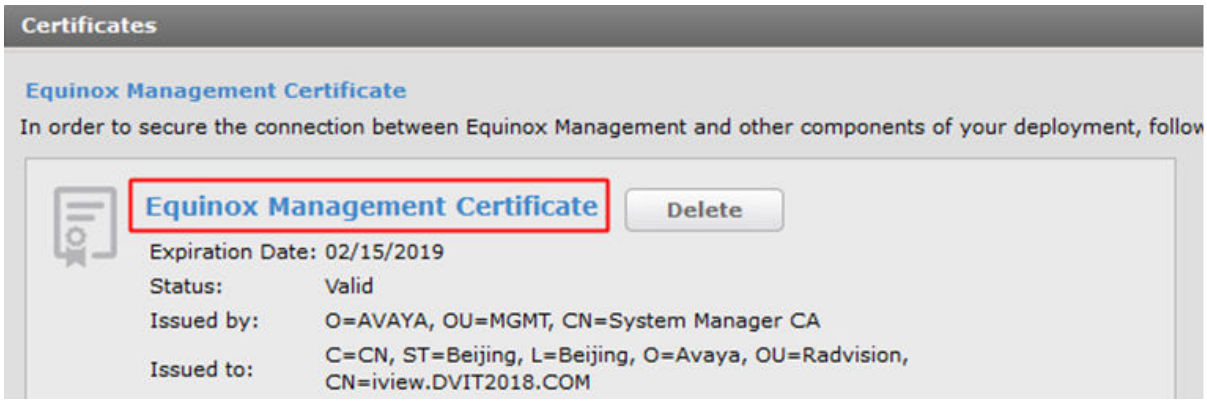
About this task

When Equinox Management uses its internal CA or third party CA-signed identity certificates, you must obtain the root CA certificate to be added to the trust store of peer devices that connect to Equinox Management. This section describes how to obtain the root CA certificate.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Security** > **Certificates**.

   The system displays the **Certificates** page.



3. Click the certificate name (default is **Equinox Management Certificate**), and click **Save** on the resulting pop-up message.

Related links

Securing your video network using TLS on page 181

Configuring Equinox Management as a Certificate Authority

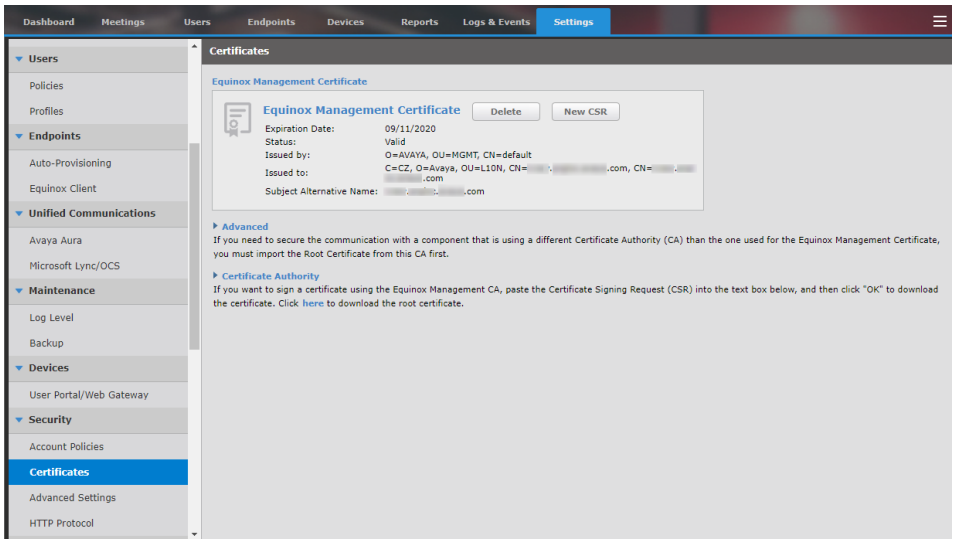
About this task

Equinox Management can serve as a certificate authority to approve a certificate signing request (CSR).

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Security** > **Certificates**.

   The system displays the **Certificates** page.



3. Click the arrow next to **Certificate Authority** to expand the section.

Figure 44: Certificate Authority Section

4. Paste the CSR into the text box, and click **OK** to download the certificate.

Related links

Securing your video network using TLS on page 181

Securing TLS connections for Equinox Management

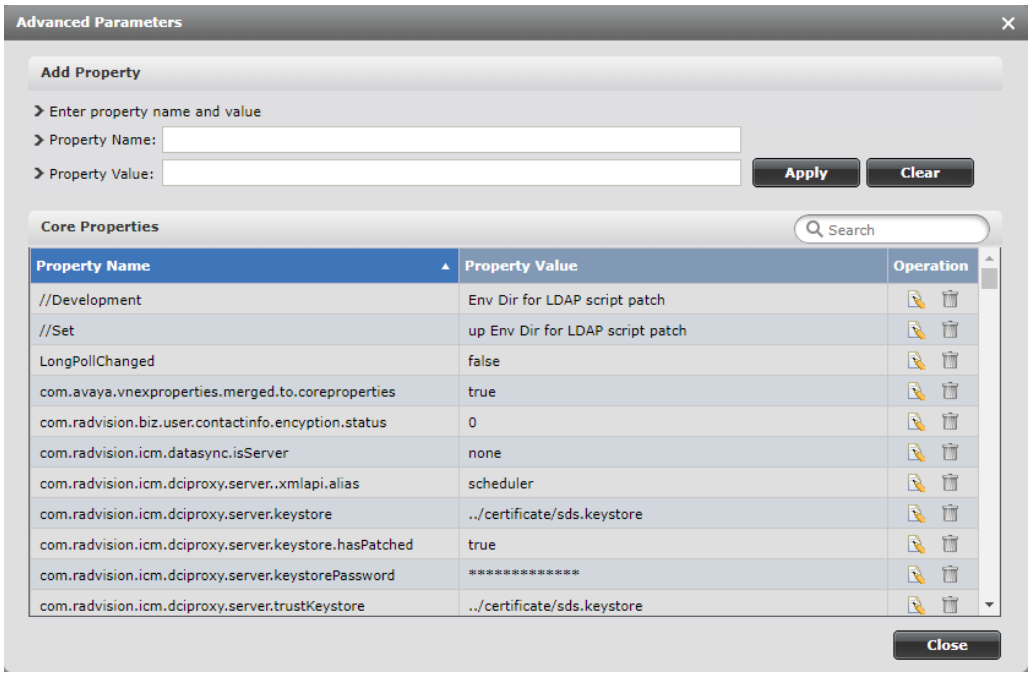
About this task

To protect your system against security vulnerabilities, you must invoke TLSv1.2. This procedure explains how to turn off TLSv1 and TLSv1.1 and replace them with TLSv1.2.

Procedure

1. In the Equinox Management administrator portal, click ≡ > **Advanced Parameters**.

   The system displays the **Advanced Parameters** dialog box.



2. In the **Property Name** field, enter `vnex.vcms.core.tls.protocols`
3. In the **Property Value** field, enter `TLSv1.2`, and click **Apply**.
4. Connect to the host via SSH using a client such as PuTTY, and edit the following parameters:
   a. **`/opt/avaya/iview/tomcat/conf/server.xml`**: locate `sslEnabledProtocols=TLSv1,TLSv1.1,TLSv1.2` and delete `TLSv1` and `TLSv1.1`.
   b. **`/etc/nginx/conf.d/nginx_iview.conf`**: locate `ssl_protocols TLSv1 TLSv1.1 TLSv1.2` and delete `TLSv1` and `TLSv1.1`.
5. Restart Equinox Management.

Related links

Securing your video network using TLS on page 181

Securing TLS connections for a distributed AAWG/Portal

About this task

To protect the distributed AAWG/Portal from security vulnerabilities, you must invoke TLSv1.2. This procedure explains how to turn off TLSv1 and TLSv1.1 and replace them with TLSv1.2.

Procedure

1. Connect to the host via SSH using a client such as PuTTY, and edit the following parameter:

/etc/nginx/conf.d/nginx_iview.conf: locate `ssl_protocols TLSv1 TLSv1.1 TLSv1.2` and delete `TLSv1` and `TLSv1.1`.

2. Restart Equinox Management.

Related links

Securing your video network using TLS on page 181

Troubleshooting TLS connections

TLS connections may fail due to certificate issues. Possible reasons are:

Certificate expired

The lifespan of Identity Certificates is usually shorter than the CA certificates. When attempting to use a certificate after the *Valid to* date has passed, the TLS connection fails with *certificate_expired (45)* as the TLS alert message. This can be seen with a port capturing tool on the specific port. Some services may fail to start if their Identity Certificate has expired. This can be viewed in their corresponding log files.

Identity certificate not trusted (Unknown CA)

When a TLS service connects to a peer device and the peer device presents its identity certificate, the certificate issuer must be trusted to establish the connection. If it is not, the TLS handshake fails with *unknown_ca (48)* as the TLS alert message.

Unsupported certificate

An identity certificate missing specific attributes causes the TLS handshake to fail with *unsupported_certificate (43)* as the TLS alert message. The certificate attributes commonly misconfigured are those in the extensions **Key Usage** and/or **Extended Key Usage**.

Certificate not yet valid

A newly generated Identity Certificate with a current *Valid From* date and time may not be valid for the peer device validating it. Ensure that clocks on both devices are synchronized.

SIP TLS connection fails to/from remote device

Access the `/var/avaya/log/sipserver/sipserver.log` file. You can use Wireshark or tshark to capture the SIP interface *eth1* and port 5061 (or the custom port, if one is in use). The TLS handshake failing message is usually an Alert message with a description.

TLS connection issues between Equinox Management and an Equinox Device

Access the `/var/avaya/log/iview/server.log` file. A newly generated identity certificate with a current *Valid From* date and time may not be valid for the peer device validating it. Ensure that clocks on both devices are synchronized.

Related links

Securing your video network using TLS on page 181

Configuring account policies in Avaya Equinox® Management

About this task

You can configure password policies for users in Avaya Equinox® Management. The password settings you can configure are:

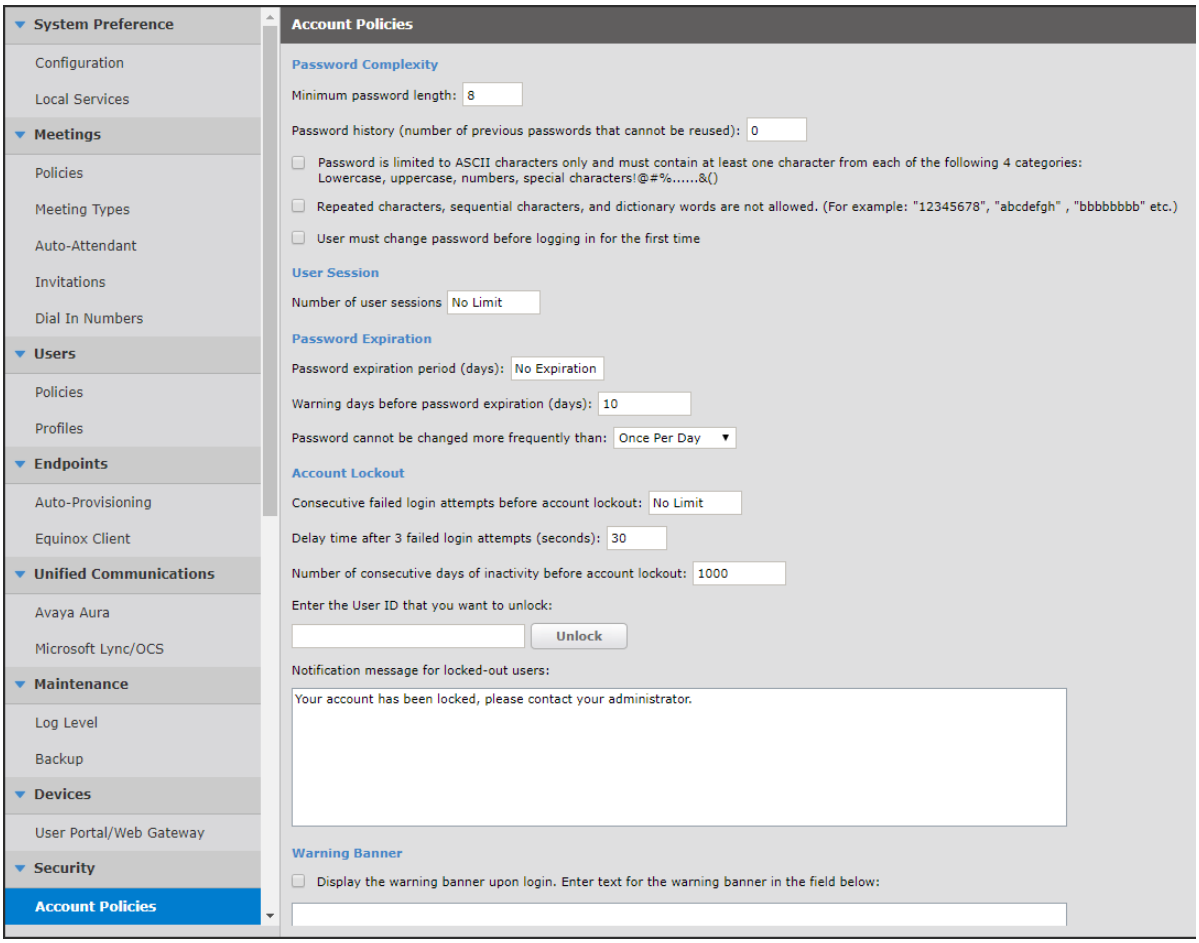
- **Password Complexity**: Includes configuring the characters that can be used in a password, and minimum password length.
- **Password Expiration**: Includes the number of days after which a password expires, and the number of days before the password expires when a warning message is generated.
- **Account Lockout**: Includes the permitted number of failed login attempts before accounts are locked, and the delay that users must wait to login after three failed login attempts.

You can also configure a security warning message to display on the login page.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Security** > **Account Policies**.

   The system displays the **Account Policies** page.



3. Configure the fields on the page, as described in Table 41: Configuring the Account Policies Settings on page 207.

Table 41: Configuring the Account Policies Settings

Section Name	Field Name	Description
Password Complexity	**Minimum password length**	Enter the minimum amount of characters required for passwords. **Default value**: 8
	Password history (number of previous passwords that cannot be reused)	The number of previous passwords that cannot be reused. For example, if the value is set to 3, the new password cannot match any of the previous 3 passwords. • **Permitted values**: 0–12 • **Default value**: 1

Table continues…

Section Name	Field Name	Description
	Password is limited to AASCII characters...	Select to limit passwords to ASCII characters. Password strings must contain at least one of the following characters: • Lowercase letter • Uppercase letter • Number • Special character (! @ # $ ^ & *)
	Repeated characters...	Select to forbid use of repeated or sequential characters, such as **bbbbbb**, **12345678**, **abcdefg**, or **asdf**.
	You must change your password before logging in for the first time	Select for Equinox Management to require users to change their password upon initial login to the system.
Password Expiration	**Password expiration period (days)**	The number of days after which a user's password expires. **Default value**: 0 (no expiration)
	Warning days before password expiration (days)	The number of days before the password expires upon which a warning message is sent to the user. **Default value**: 10
	Password cannot be changed more frequently than	Select the maximum frequency upon which a user's password can be changed. Available values are: • **Once Per Day** (default) • **Once Per Week** • **Once Per Month**
Account Lockout	**Consecutive failed login attempts before account lockout**	The number of consecutive login attempts that can fail for a user before their account is locked. **Default value**: 0 **Note:** Failures are counted only for consecutive logins. The lockout count is reset after a successful login.
	Delay time after 3 failed login attempts (seconds)	The amount of time (in seconds) users must wait to log in after 3 failed login attempts. **Default value**: 60

Table continues…

Section Name	Field Name	Description
	Number of consecutive days of inactivity before account locked	The number of days of inactivity after which accounts are locked. **Default value**: 0 (no lockout)
	Enter the User ID that you want to unlock	The User ID of the user whose account you want to unlock. Enter the User ID and select the **Unlock** button.
	Notification message for locked-out users	A message displayed for users who are locked out of their account, such as **Your account has been locked, please contact your administrator**.
Warning Banner	**Display the warning banner upon login...**	Select the check box to display a warning banner on the login page. When selecting the check box, the field below it is enabled, where you can configure the text to be displayed. Text can be configured either in plain text or HTML.

4. Click **Apply**.

Related links

Securing your video network on page 179

Configuring meeting policies PIN security

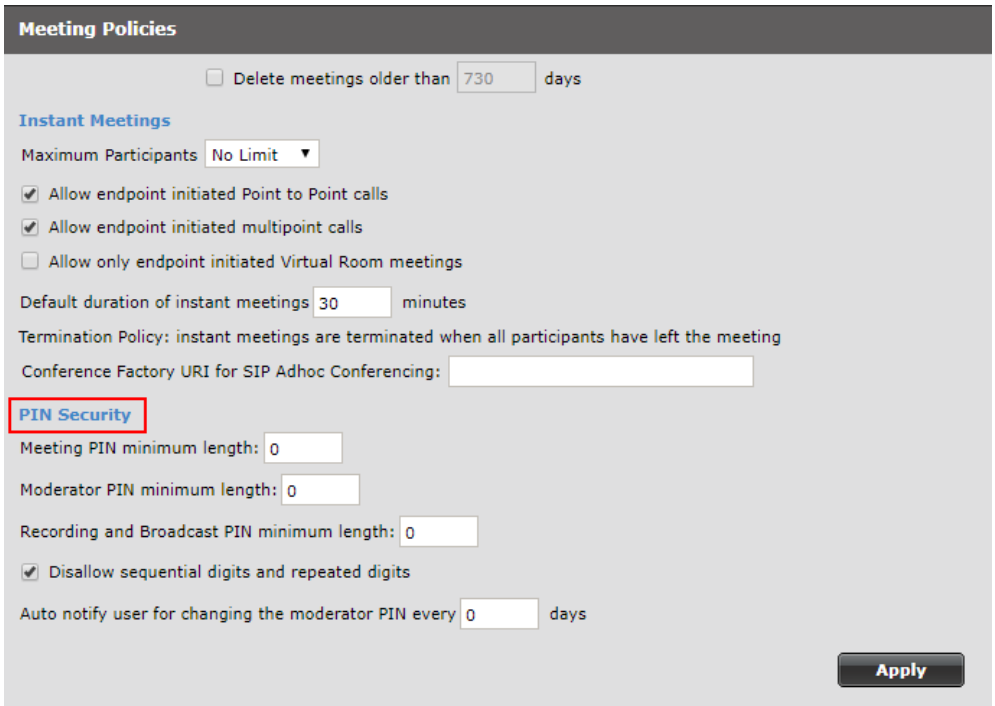
About this task

These PIN security features enable the administrator to enforce strong PIN requirements and auto notifications to change the PIN.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Meetings** > **Policies**.

   The system displays the **Meeting Policies** page.



3. Configure the fields on the page as in the following table:

Field	Description
Meeting PIN minimum length	Enter the minimum number of digits required for the meeting PIN. • A *0* means the PIN can be empty. A non-zero value means the PIN cannot be empty. • This setting does not apply to the VMR that is enabled for a *one-time* PIN. • This rule only applies when the administrator or user manually updates the PIN from the admin portal or Unified Portal in the UI. • **Permitted values**: 0–16 • **Default value**: 0
Moderator PIN minimum length	Enter the minimum number of digits required for the moderator PIN. • A *0* means the PIN can be empty. A non-zero value means the PIN cannot be empty. • This rule only applies when the administrator or user manually updates the PIN from the admin portal or Unified Portal in the UI. • **Permitted values**: 0–16 • **Default value**: 0

Table continues…

Field	Description
Recording and Broadcast PIN minimum length	Enter the minimum number of digits required for the recording and broadcast PIN. • A *0* means the PIN can be empty. A non-zero value means the PIN cannot be empty. • This setting is only for the Unified Portal UI. • **Permitted values**: 0–255 • **Default value**: 0
Disallow sequential digits and repeated digits	• Applies to all PINs including meeting PINs, the moderator PIN, recording PINs, and broadcast PINs. • This rule applies to the whole PIN. If it is enabled, then: - 123456 is disallowed - 222222 is disallowed - 123455 is allowed - 222223 is allowed • This rule only applies when the administrator or user manually updates the PIN from the admin portal or Unified Portal in the UI. • **Default**: Enabled (with check box)
Auto notify user for changing moderator PIN <x> days	• A *0* means *do not notify*. • The notification email is sent to the VMR owner, and the User Portal page displays notification of the PIN expiration. • The notification is only sent when the user's VMR PIN is not empty. • Every time a user or the admin saves the VMR settings that contain the new PIN value, the timer is reset. Entering the same PIN as the previous one is not recognized as a PIN change. • **Permitted values**: 0–365 days • **Default value**: 0 **Note:** The email server must be configured to send email notifications.

4. Click **Apply**.

Related links

Securing your video network on page 179

Configuring Cross-Origin Resource Sharing (CORS)

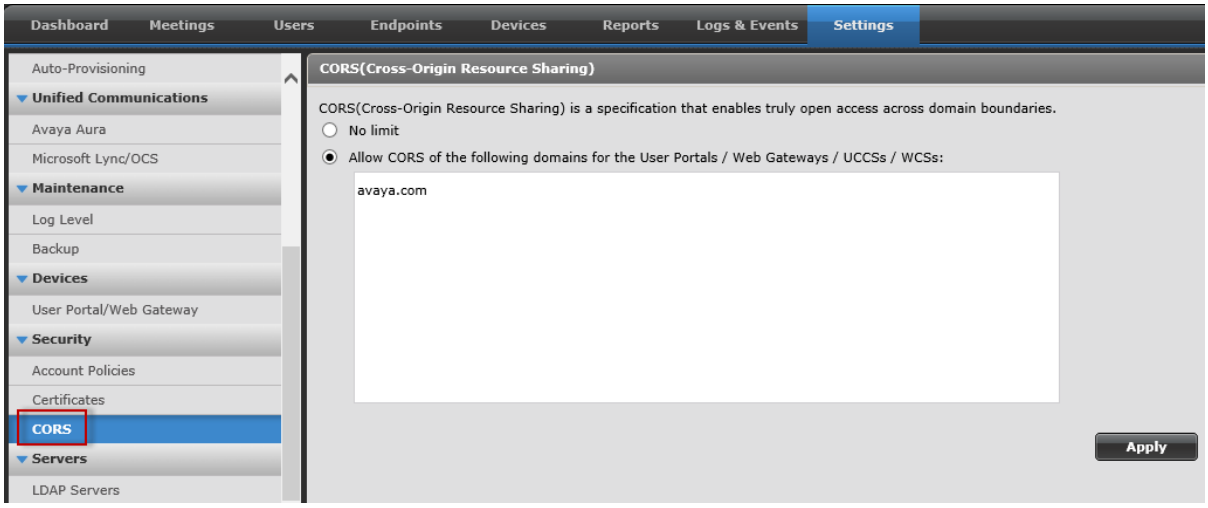
About this task

Cross-Origin Resource Sharing (CORS) enables you to share resources across specified domains. You can select to share resources either across all domains without limit, or across only specific domains.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Security** > **CORS**.

   The system displays the **CORS (Cross-Origin Resource Sharing)** page.



3. Choose:
   - **No limit**: Enables sharing resources across all domains, without limit.
   - **Allow CORS of the following domains**: Enables you to specify the domains across which sharing resources is permitted. When selecting this option, insert the pointer in the provided cell and enter the domain with which you want to permit sharing of resources.
4. Click **Apply**.

Related links

Securing your video network on page 179

Configuring the Enhanced Access Security Gateway (EASG)

About this task

This procedure explains how to configure the Enhanced Access Security Gateway (EASG). EASG provides enhanced security to Equinox Management; when enabled, users must retrieve a password from an ASG web application before they can change their password in Equinox Management.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Settings** > **Security** > **EASG**.

   The **EASG** page appears.

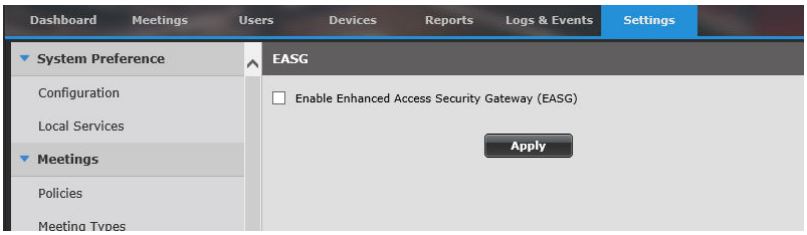


Figure 45: EASG Page

3. Select the checkbox and select **Apply**.

Related links

Securing your video network on page 179

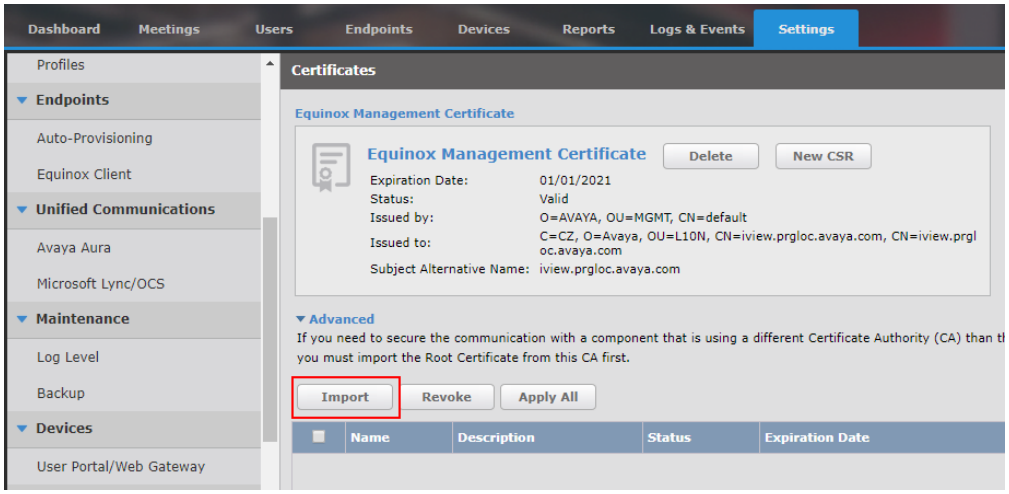
Importing a CA certificate

About this task

Perform the following to import a certificate signed by a certificate authority (CA).

Procedure

1. Access the Avaya Equinox® Management administrator portal. The default management URL is http://<FQDN>:8080/iview/
2. Navigate to **Settings** > **Security** > **Certificates** > **Advanced**.



3. Click **Import**.
4. Click **Add**, browse to the required root or intermediate certificate, and click **Open**.
5. Repeat the previous step for each root or intermediate certificate that you need to upload.
6. Click **Upload**.

Related links

Securing your video network on page 179

Enabling hardening for the Avaya Equinox® management server

About this task

The hardening configuration properties in Avaya Equinox® are hidden by default. Use this procedure to display and enable the hardening configuration. It is mandatory to change the SSH user password because hardening has greater password requirements.

Before you begin

- A stand alone Avaya Aura® Media Server is required. You cannot enable FIPS compliance when other media servers are required.
- You cannot enable FIPS Compliance in Equinox Management in redundancy mode. See Enabling FIPS compliance for redundancy mode on page 215 for the basic steps to enable FIPS Compliance to use in redundancy mode.

Procedure

1. Access the Avaya Equinox® Management administrator portal. The default management URL is https://<FQDN>:443/iview/

2. To display the hardening configuration options:
   a. Click on the menu icon under the **Sign Out** link located on the upper-right of any Avaya Equinox® administration page.
   b. Click **Advanced Parameters**.
   c. In the **Property Name** field, enter `com.avaya.security.settings.displayManagementSecurityModes`.
   d. In the **Property Value** field, enter `true`.
   e. To add the property to the system, click **Apply**.
   f. Click **Close**.
3. To enable the hardening mode:
   a. Click **Settings** > **Security** > **Advanced Settings**.
   b. Select **Enable FIPS Compliance**.
4. Click **Apply**.

   The system displays a warning that you cannot turn FedRAMP/FIPS off after you activate it.
5. Click **OK**.

   The deployment reboots.
6. To change the password, use SSH to access the device.
   a. Type `pmgradmin` as username, and the default password.
   b. At the Linux prompt, type `sudo /opt/avaya/pmgr/external-scripts/pmgr-update-local-admin.sh pmgradmin <old_pass> <new_pass>`
7. Click **CORS Settings** (see Configuring Cross-Origin Resource Sharing (CORS) on page 212).

Related links

Securing your video network on page 179

Enabling FIPS compliance for redundancy mode

About this task

You cannot enable FIPS Compliance *in* Equinox Management in redundancy mode. *To use* FIPS Compliance in redundancy mode, you must enable FIPS Compliance *before* setting up redundancy mode. See the following basic steps:

Procedure

1. Deploy two standalone Equinox Management servers, see the *Deploying Avaya Equinox® Solution* publication.

2. Apply third-party certificates, see the *Deploying Avaya Equinox® Solution* publication.
3. Enable FIPS Compliance on each of the two standalone Equinox Management servers separately, see Enabling hardening for the Avaya Equinox management server on page 214.
4. Setup redundancy in Equinox Management.

Related links

Securing your video network on page 179

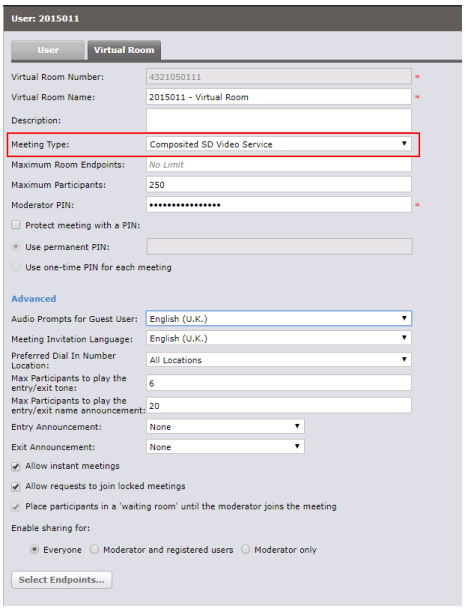
Enabling composite video for virtual rooms

About this task

Use the following procedure to enable standard definition (SD) or high definition (HD) composite video for a virtual room.

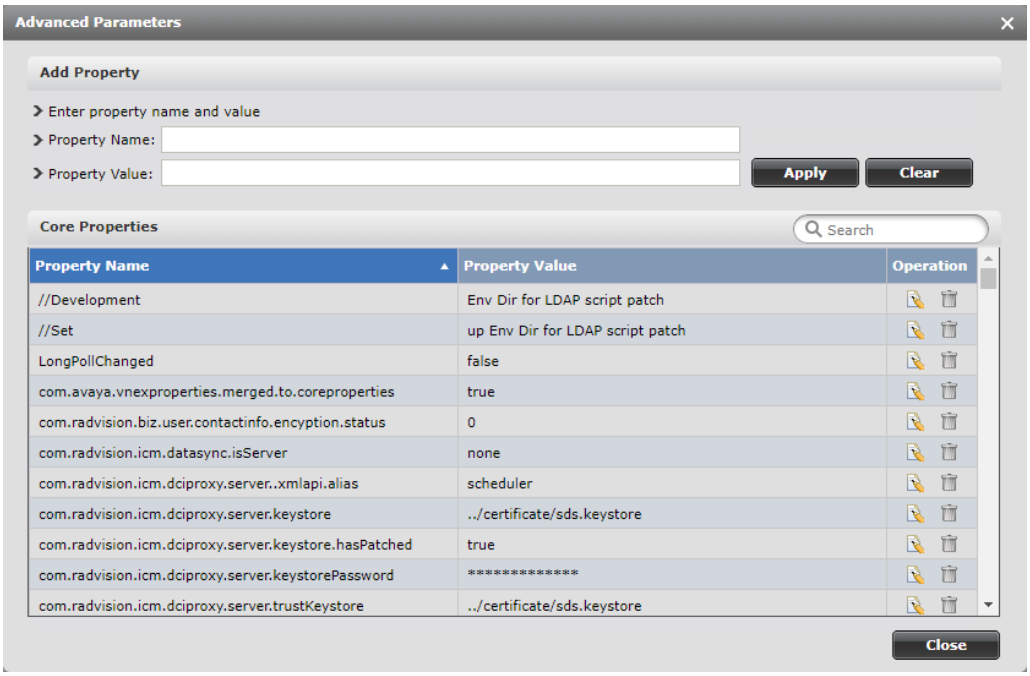
Procedure

1. Access the Avaya Equinox® Management administrator portal. The default management URL is http://<FQDN>:8080/iview/
2. Click the **User** tab.
3. Select a user to modify by clicking on the user name.
4. Click the **Virtual Room** tab.
5. Set the **Meeting Type** video sharing quality, select **Composited SD Video Service** or **Composited HD Video Service**.



6. Click **OK**.
7. To change the maximum number of participants' frames in a mixed video layout:
   a. Click ☰ > **Advanced Parameters**.

      The system displays the Advanced Parameters dialog box.



   b. In the **Property Name** field, enter `vnex.vcms.core.conference.compositevideo.compositor.maxwindows`
   c. In the **Property Value** field, enter the maximum number of frames (the default is 16).
   d. Click **Apply**.

Related links

Securing your video network on page 179

Chapter 5: Defining and Managing Video Users

This section is relevant for enterprise deployments, and explains how administrators can add and manage users.

After adding new users, you can organize users in groups and assign profiles to them. Usually, users are grouped based on their location (time zone) or organization unit (for example, a branch, department or workgroup). A user profile is a group of user-related capabilities and rights, such as available meeting types and ability to schedule meetings (Figure 46: Using groups and profiles to define a user on page 218).

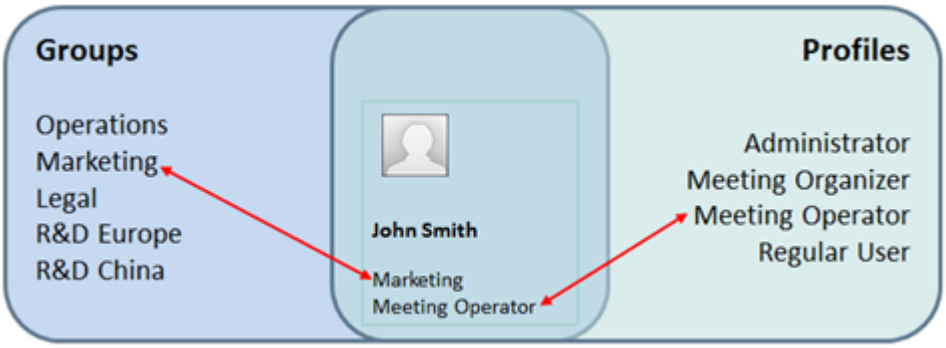


Figure 46: Using groups and profiles to define a user

Users, user profiles and user groups can be defined within Equinox Management, or sourced directly from the organization's external LDAP server, interfacing with Microsoft's Active Directory or IBM's Domino. When an LDAP server is used, the connection between Equinox Management and the LDAP server must be configured (see Connecting Equinox Management with the LDAP server on page 239).

When you add users for the first time in Avaya Equinox® Management, we recommend following this workflow:

1. Define user profiles, as described in Creating or modifying a user profile on page 221. A user profile is a compilation of user-related capabilities and rights, such as the ability to schedule meetings. The purpose of having user profiles in Equinox Management is to configure and modify rights and capabilities for all users sharing this profile, instead of doing it for every user individually.
2. Define user groups, as described in Creating a User Group on page 236. You can unify users into groups to manage and maintain users on a group level. Users are typically joined

together based on their location (time zone) or organization unit (for example, a branch, department or workgroup).

3. If you are using a third-party LDAP server such as Microsoft Active Directory, download users as described in Downloading Users from the LDAP Server on page 242.

   --Or--

   If you are using Equinox Management's internal LDAP server, create users as described in Creating a user within Equinox Management on page 245.

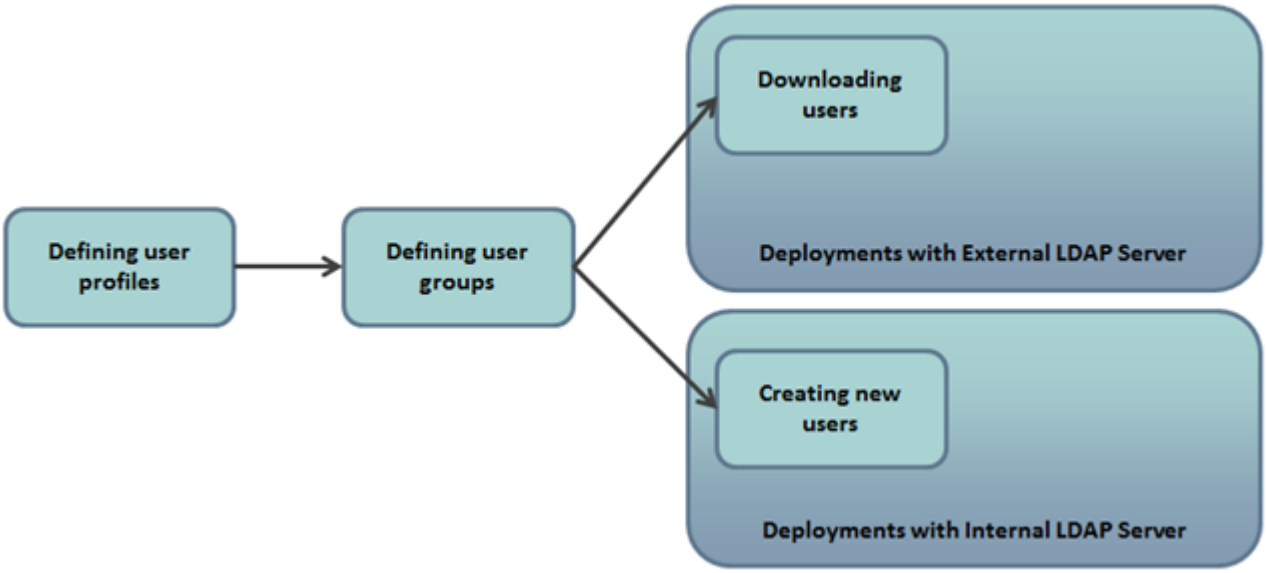


Figure 47: Workflow for defining users in Avaya Equinox® Management

You can modify and delete user profiles and user groups. To delete a user group or a user profile you need to make sure no users are assigned to it.

Avaya Session Border Controller for Enterprise (SBCE) is part of the Equinox Solution. The server provides firewall traversal for SIP, HTTP, and WebRTC devices used by participants joining conferences and tunnels media where the firewall blocks media ports. The server allows streams to come in through known ports for TLS/TCP. It also supports the dialing-in of unregistered guest users. For deploying Avaya SBCE with the Equinox Solution, see *Deploying Avaya Equinox® Solution.*

Note:

Avaya SBCE release 8.0 and above is required for launching WebRTC calls from the Microsoft Edge browser.

Related links

Managing User Profiles on page 220
Modifying User Policies on page 234
Managing User Groups on page 235
Managing Video Users on page 238
Defining Administrators in a Service Provider Deployment on page 252

Managing Virtual Rooms on page 253
Creating Preferred Dial In Number Variables on page 259
Invitation Template Variables and Parameter Settings on page 260
Creating an invitation template on page 262
Configuring WebRTC calls for the Microsoft Edge browser on page 264

Managing User Profiles

This section is relevant only for enterprise deployments.

A user profile is a compilation of user-related capabilities and rights, such as available meeting types, ability to schedule meetings, access to functionality, and allowed bandwidth for calls. The purpose of having user profiles in Equinox Management is to configure and modify rights and capabilities for all users sharing this profile, instead of doing it for every user individually. Typically, you create profiles that correlate with user roles in the organization (for example, administrators, read-only users) or profiles using different features (for example, users who use the lecture meeting type and are not allowed to schedule meetings).

There are four preconfigured user profiles:

- Administrator
- Meeting Organizer
- Meeting Operator
- Regular User

You can modify settings for the preconfigured profiles, except their names and short descriptions. You cannot delete preconfigured profiles.

You can assign profiles to individual users and to user groups. When you assign a user profile to a group, you can still assign a different profile to individual users within this group.

Defining user profiles is the first stage of user definition, as shown in Figure 47: Workflow for defining users in Avaya Equinox® Management on page 219.

Related links

Defining and Managing Video Users on page 218
Creating or modifying a user profile on page 221
Exporting a list of users in Equinox Management on page 226
Enabling Streaming and Recording for a User Profile on page 228
Customizing a user profile on page 229
Deleting a User Profile on page 233

Creating or modifying a user profile

About this task

A user profile is a compilation of user-related features and rights, such as available meeting types and the ability to schedule meetings. This section explains how to create a new user profile or modify an existing one.

For more information, see Managing User Profiles on page 220.

Note:

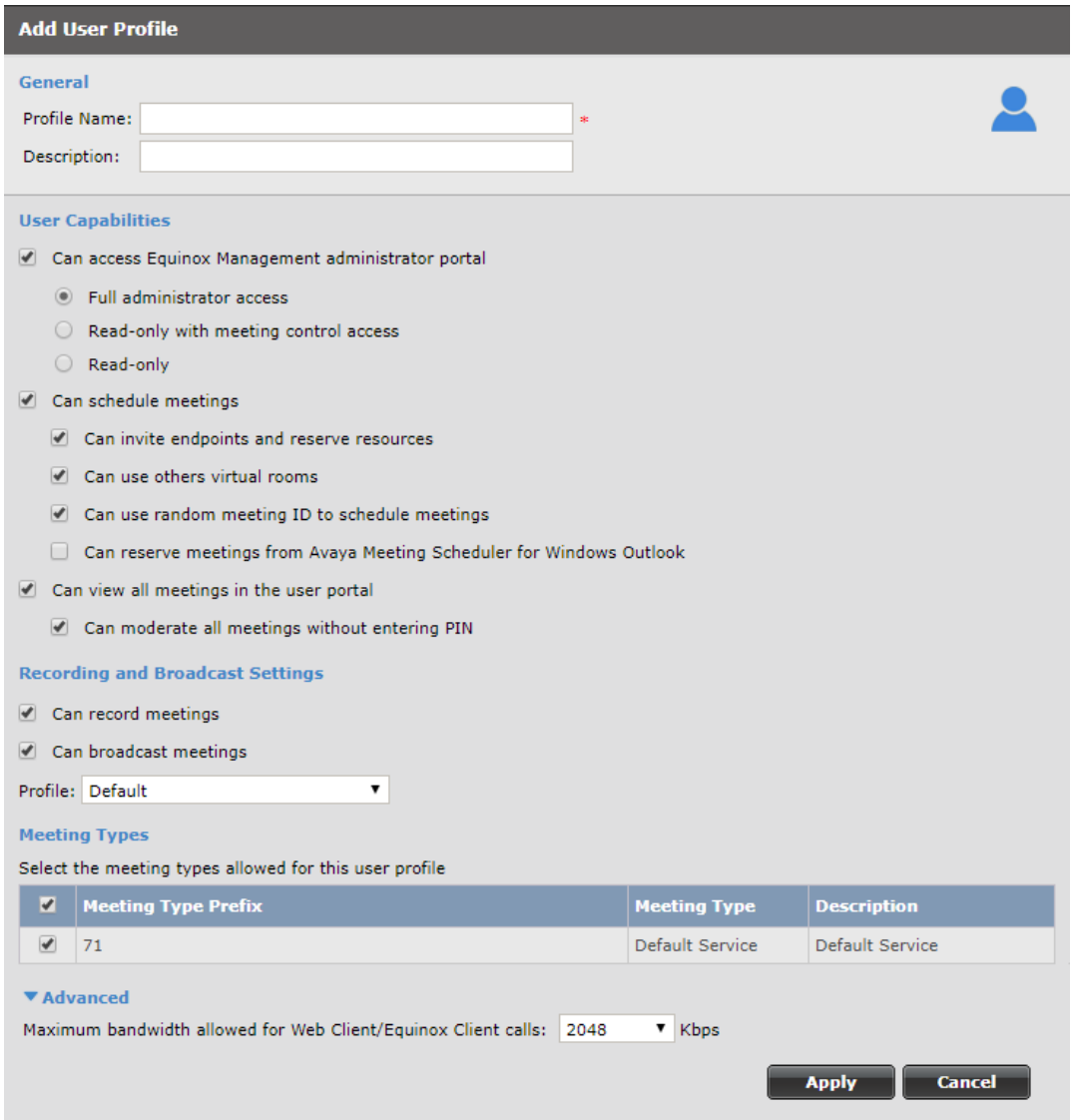
In service provider (multi-tenant) deployments, this is done by each organization's administrator.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Users** > **Profiles**.
3. Click **Add**.

   or

   Click the user profile that you want to modify.



4. Enter the profile name and a short description in the **Profile Name** and **Description** fields.

   This option is available only when adding a new profile. You can only modify a newly added profile. We recommend that the profile name be self explanatory.

5. Select the user capabilities and functionality that you want to enable for this user:

   Table 42: User profile capabilities

Capability	Description
Guest (No License)	Relevant if Equinox Management is part of a Team Engagement deployment. Select this option for a client/endpoint without a license to own a virtual room.

Table continues…

Capability	Description
Power Suite Licenses (users)	Relevant if Equinox Management is part of a Team Engagement deployment. Select this option for a client/endpoint with a license to own virtual room. A Power Suite Licenses user was previously called a Golden User.
Can access Avaya Equinox® Management administrator portal	A user can log into the Avaya Equinox® Management administrator portal. You can choose from the following permissions: • **Full administrator access**: A user can view and modify all settings. • **Read-only with meeting control access**: A user can view all settings without modifying, but can schedule, moderate, and delete meetings. • **Read-only**: A user can only check settings or monitor meetings in progress, without changing any settings.

Table continues…

Capability	Description
Can schedule meetings	A user can schedule meetings from the Avaya Equinox® Management Web Portal. • **Can invite endpoints and reserve resources**: A user can schedule meetings which require inviting endpoints and reserving resources, for example, an MCU. • **Can use others virtual rooms**: When scheduling a meeting, a user can choose to use somebody else's virtual room in addition to his or her virtual room or public virtual rooms. **Note:** This feature only operates successfully if the other person's login id matches to either the other person's email address or the username portion of the other person's email address. • **Can use random meeting ID to schedule meetings**: Select to enable users to schedule meetings outside of their virtual room. • **Can reserve meetings from Avaya Meeting Scheduler for Windows Outlook**: Selected means Windows Outlook add-in synchronizes the Outlook meetings in Equinox and reserves the meeting using *dynamic meeting id*. See the associated advanced parameters. **Default**: Cleared
Can view all meetings in the user portal	If this option is enabled, a user can view all upcoming and ongoing meetings at the Avaya Equinox® Management portal; if this option is disabled, the user can see only his or her meetings: meetings started by this user or meetings this user joined by the invitation of others.
Can moderate all meetings without entering PIN	A user can have moderator rights in other users' virtual rooms even without entering the moderator PIN.

Table continues…

Capability	Description
Can record meetings	This option is relevant only for deployments with Avaya Equinox® Streaming and Recording server. A user can record meetings in one of the following ways: • Start recording a meeting in progress using the Equinox Management user portal. • Enable recording during scheduling a meeting using the Equinox Management user portal. For more information, refer to Enabling Streaming and Recording for a User Profile on page 228.
Can broadcast meetings	This option is relevant only for deployments with Avaya Equinox® Streaming and Recording server. Meetings are broadcast automatically when they start.
Profile	Select a recording profile for the user.

6. Select the required meeting types.
7. Expand the **Advanced** section and select a value for the **Maximum bandwidth allowed for Web Client/IX Workplace Client calls**, in kbps. The default value is 2048.
8. Click **Apply**.
9. To configure the advanced parameters for the **Can reserve meetings from Avaya Meeting Scheduler for Windows Outlook** check box:
   a. Click ≡ > **Advanced Parameters**.

      The system displays the **Advanced Parameters** dialog box.

   b. Enter the indicated values in the fields described in the following table, click **Apply** after each one:

Property Name field	Property Value field
`vnex.vcms.core.conference.childmeetingid.suffix.length`	The number of digits to be appended to the VR number when generating the Dynamic meeting id. **Note:** Avaya recommends that you do not set the value to `0`. Setting the value to `0` blocks the ability to schedule conflicting meetings, and affects the user experience when scheduling back to back meetings with the same VMR. **Range**: 0–4 **Default value**: 3
`vnex.vcms.core.conference.childmeetingid.prefix.strip.length`	The number of prefix digits to be stripped from the VR number when generating the dynamic meeting id. 0 means do not strip. If the property value is greater than the VR length, it means strip the whole VR number. **Default value**: 0
`vnex.vcms.core.conference.childmeetingid.prefix`	The prefix to be added to the VR number when generating the dynamic meeting id. **Default value**: "“

Example

Assuming:

- VR = 71555
- Prefix length to be stripped = 2
- Prefix to be added = 82
- Length of random digits to be appended = 3

Result: Dynamic meeting id = 82555xxx

Related links

Managing User Profiles on page 220

Exporting a list of users in Equinox Management

About this task

You can export a list of recently created Equinox Management users, enabling third-party applications to send a welcome email to new users.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Users** > **Users From Active Directory** > **All** in the sidebar.
3. Click the **Export Users** button.

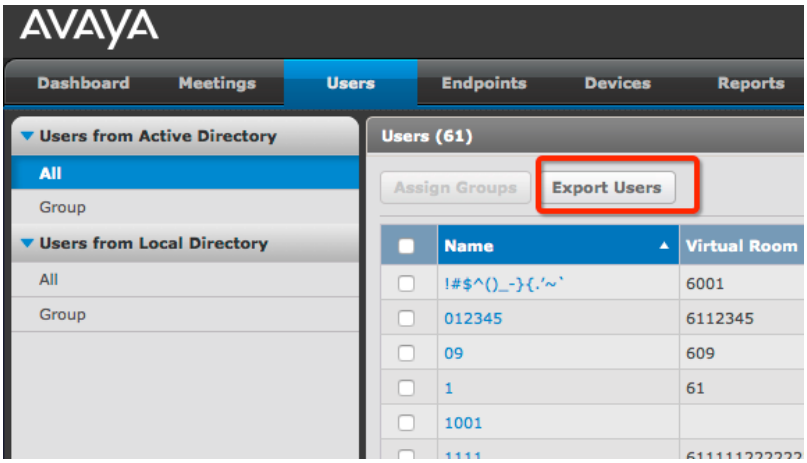


Figure 48: Export Users button

The system displays the **Export Users** dialog box.

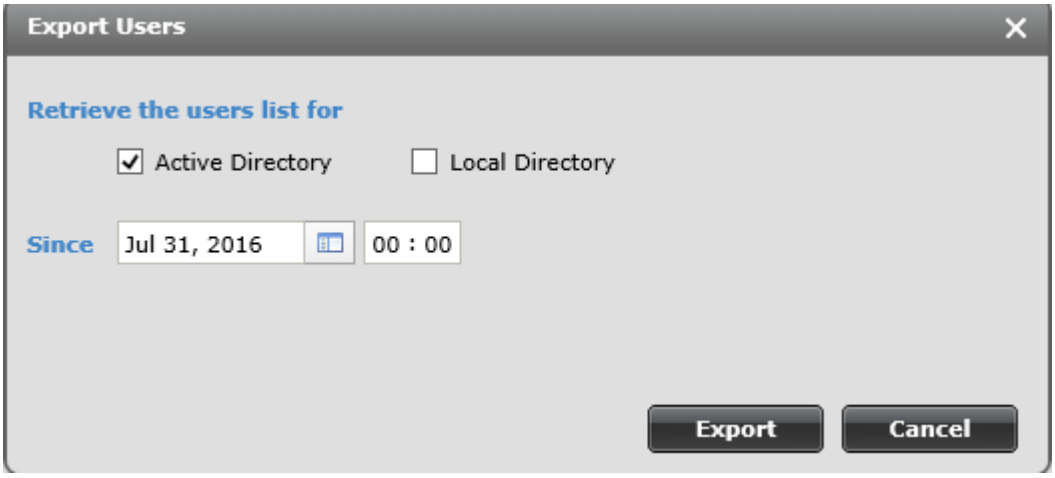


Figure 49: Export Users dialog box

4. Select the directory from which you want to retrieve the users list: **Active Directory** or **Local Directory**.
5. In the **Since** field, select the calendar icon and select a date and time. The **Export** action will export users created since the selected date and time. For example, if you select July 15, 2016 at 11:00, you will export all users created since July 15, 2016 at 11:00.

Note:

The time is configured in 24-hour format.

6. Click the **Export** button.

   An Excel file is created, containing the list of users created since the date and time selected in the **Export Users** dialog box in Step 5 on page 227. In the dialog box at the bottom of the page, select whether you want to open or save the Excel file.

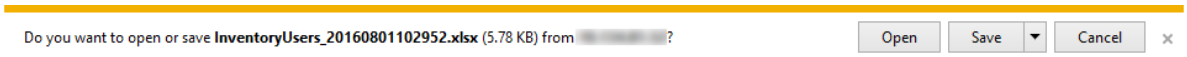


Figure 50: Export Users — Open/Save dialog box

Related links

Managing User Profiles on page 220

Enabling Streaming and Recording for a User Profile

About this task

When streaming and recording is enabled in Equinox Management, you can narrow the streaming and recording services by granting streaming and recording permissions to specific user profiles. Users with streaming and recording permissions can configure their virtual room settings to always stream or record meetings, or they can enable streaming and recording when scheduling a specific meeting.

By default, only users with certain user profiles, such as meeting operators and meeting organizers, can stream and record meetings. You can enable or disable streaming and recording capability per user profile, as described in the procedure below. After enabling streaming and recording for a user profile, you can set a specific user's virtual room to always stream and record meetings, as described in Creating or modifying a virtual room for an Equinox Management user on page 255.

Before you begin

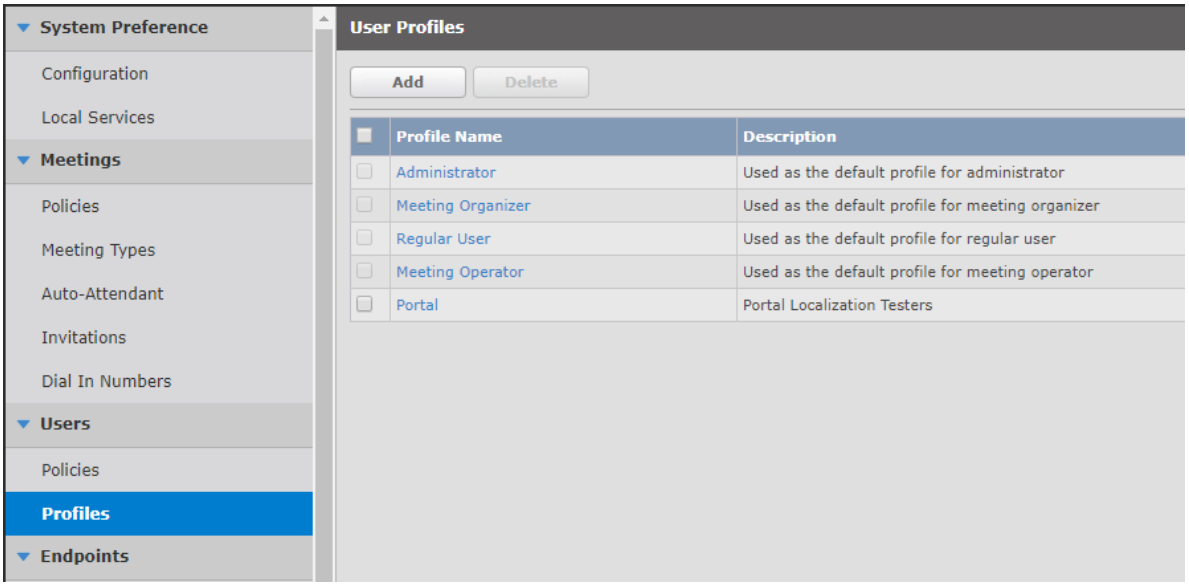
Ensure that streaming and recording is enabled in Equinox Management. See Adding and Modifying Equinox Streaming and Recording Servers in Equinox Management on page 177.

Important:

If you are using the Avaya Scopia® Content Center Streaming and Recording solution, ensure that it is enabled. For further details about different streaming and recording solutions, see Planning and configuring streaming and recording servers in Equinox Management on page 176.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Users** > **Profiles**.



3. Select the user profile from the **Profile Name** list.
4. Select recording and streaming options from the **Can record meetings** area in the **Recording and Broadcast Settings** section.

   To disable this functionality for the user profile, clear the recording and streaming check boxes.
5. Click **Apply** to save your changes.

Related links

Managing User Profiles on page 220

Customizing a user profile

About this task

You can customize a user profile for a particular user, if preconfigured profiles do not match needs of this particular user.

Important:

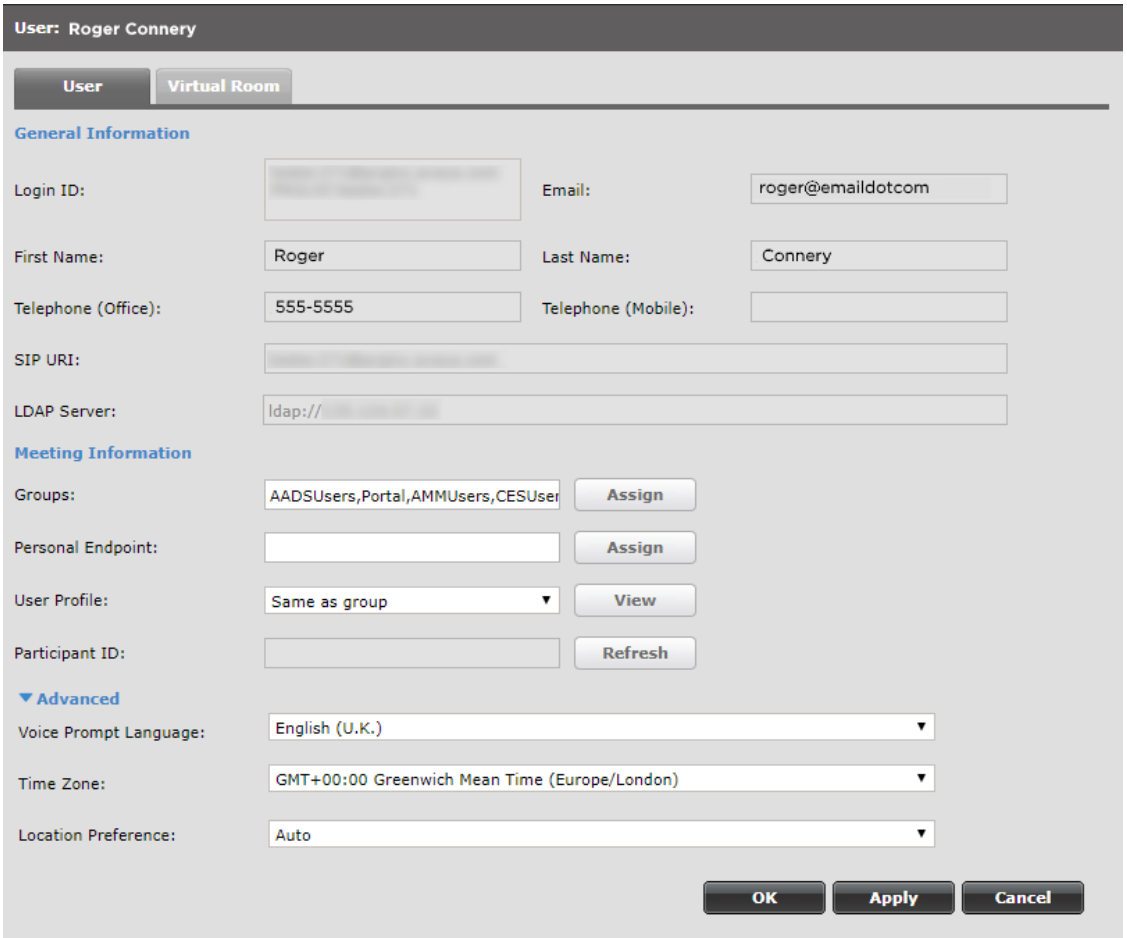
After you separate a username from its profile, any future changes to the profile will not impact the user, since it now has a custom profile. However, too many custom profiles adds to the management overhead of user rights.

For example, if you customize the `Guest` profile for one of the users not to view all meetings in the user portal, the rest of the users who are assigned the same profile will still be able to do it.

To edit the properties of a profile for all users in that profile, or to create a new profile, see Creating or modifying a user profile on page 221.

Procedure

1. Access the Avaya Equinox® Management administrator portal.
2. Click the **Users** tab.
3. Click **All** under **Users from Local Directory** or **Users from Active Directory**.
4. Select the user for whom you want to assign a different profile.



5. Select **Custom User Profile** in the **User Profile** list.
6. Click **Edit**.

   The system displays the **Custom User** profile, where you can modify the user capabilities.

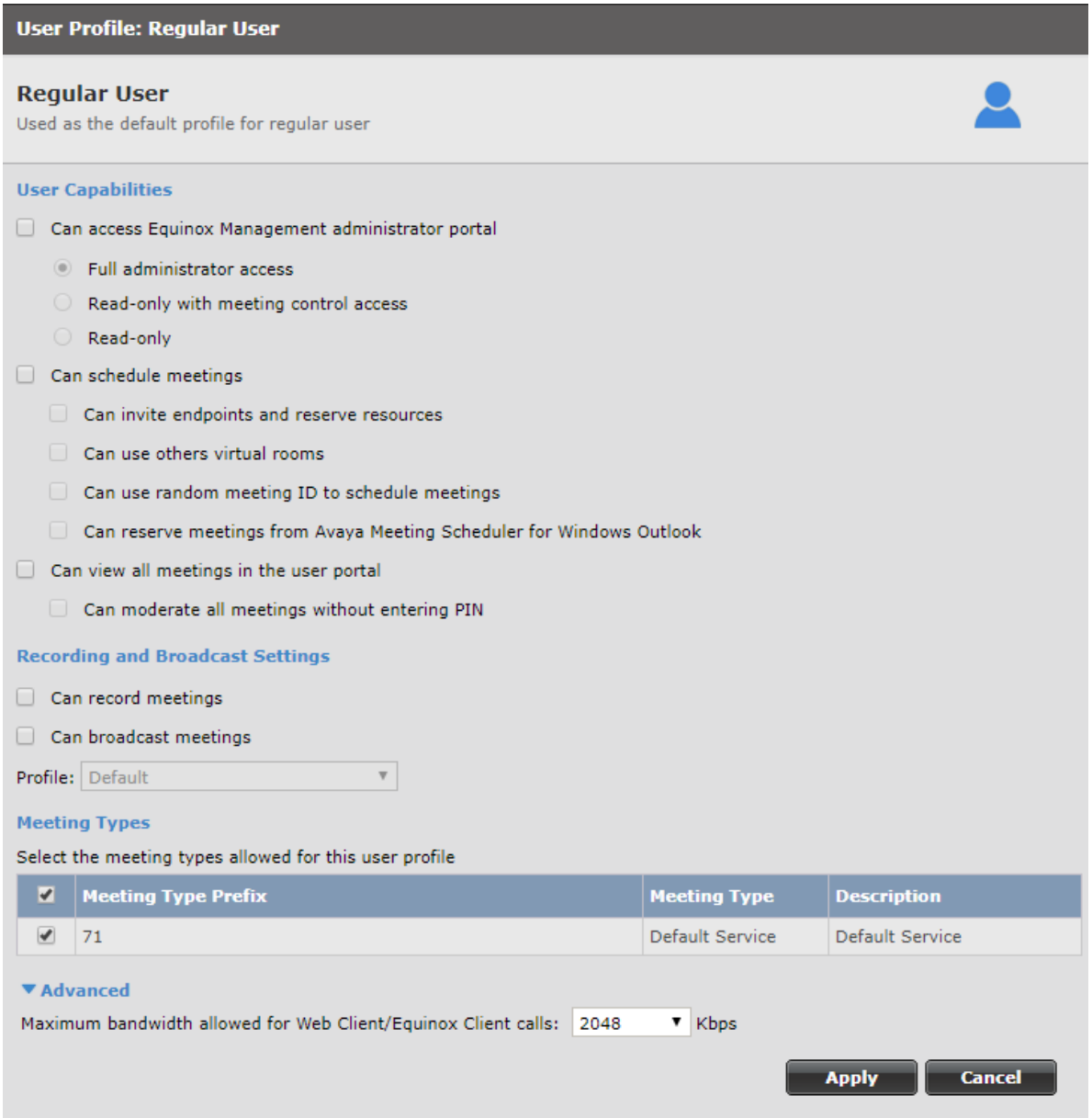


Figure 51: Custom User profile

Table 43: User profile capabilities

Capability	Description
Can access Avaya Equinox® Management administrator portal	A user can log into the Avaya Equinox® Management administrator portal. You can choose from the following permissions: • **Full administrator access**: A user can view and modify all settings. • **Read-only with meeting control access**: A user can view all settings without modifying, but can schedule, moderate, and delete meetings. • **Read-only**: A user can only check settings or monitor meetings in progress, without changing any settings.
Can schedule meetings	A user can schedule meetings from the Avaya Equinox® Management Web Portal. • **Can invite endpoints and reserve resources**: A user can schedule meetings which require inviting endpoints and reserving resources, for example, an MCU. • **Can use others virtual rooms**: When scheduling a meeting, a user can choose to use somebody else's virtual room in addition to his or her virtual room or public virtual rooms. **Note:** This feature only operates successfully if the other person's login id matches to either the other person's email address or the username portion of the other person's email address. • **Can use random meeting ID to schedule meetings**: Select to enable users to schedule meetings outside of their virtual room. • **Can reserve meetings from Avaya Meeting Scheduler for Windows Outlook**: Selected means Windows Outlook add-in synchronizes the Outlook meetings in Equinox and reserves the meeting using *dynamic meeting id*. See the associated advanced parameters. **Default**: Cleared

Table continues…

Capability	Description
Can view all meetings in the user portal	If this option is enabled, a user can view all upcoming and ongoing meetings at the Avaya Equinox® Management portal; if this option is disabled, the user can see only his or her meetings: meetings started by this user or meetings this user joined by the invitation of others.
Can moderate all meetings without entering PIN	A user can have moderator rights in other users' virtual rooms even without entering the moderator PIN.
Can record meetings	This option is relevant only for deployments with Avaya Equinox® Streaming and Recording server. A user can record meetings in one of the following ways: • Start recording a meeting in progress using the Equinox Management user portal. • Enable recording during scheduling a meeting using the Equinox Management user portal.
Can broadcast meetings	This option is relevant only for deployments with Avaya Equinox® Streaming and Recording server.
Profile	Select a recording profile for the user.

7. Select the meeting types to be enabled for the selected profile.
8. Click **Apply**.

Related links

Managing User Profiles on page 220

Deleting a User Profile

About this task

This section is relevant only for enterprise deployments.

A user profile is a compilation of user-related features and rights, such as available meeting types, ability to schedule meetings, and access to the Scopia Mobile functionality.

For more information, see Managing User Profiles on page 220.

You can only delete empty user profiles which are not assigned to any users or user groups.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Users** > **Profiles**.

3. Select the user profiles you want to delete.
4. Click **Delete**.
5. Click **Yes** in the confirmation message.

Related links

Managing User Profiles on page 220

Modifying User Policies

About this task

User policies determine a user's general parameters, such as defining the user's time zone and the name and date format when logged into Equinox Management. They also indicate the privileges and settings for users as they interact with the User Portal and Web Client/Equinox Client.

User policies are enabled with default settings in Equinox Management. You can customize settings per user (see Creating a user within Equinox Management on page 245).

This section explains how to modify default user policies.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Users** > **Policies**.

   The system displays the **User Polices** page.
3. Select the parameters and capabilities that you want to enable for users, as described in the following table:

Table 44: User Policies page

Field/Capability	Description
Default Time Zone	Select the default time zone in which users are located.
Name Display Format	Select the format for user names to be displayed.
Date Display Format	Select the format for dates to be displayed.

Table continues…

Field/Capability	Description
Allow Web Client/Equinox Client user authentication	Select to enable a Web Client/Avaya IX™ Workplace Client to perform user authentication, instead of Equinox Management. When selected, you can allow guest access to specified areas of Equinox Management by selecting from the following options: • **Allow guests to access meetings** • **Allow guests to access webcasts** • **Allow guests to start recordings** • **Allow guests to access recordings** • **Only authenticated user can invite**
Enable Web SSO	Select to enable single sign-on for a group of web servers. When selecting this option, the **Web SSO URL** and **Public key** fields are enabled. The **Enable Web SSO** field is hidden by default. To display this field, you must configure the following parameter in the **Advanced Parameters** dialog box (> **Advanced Parameters**): `vnex.vcms.core.newportal.websso.show=true`
Enable sharing for	Select from the following options to determine who can perform presentations: • **Everyone** • **Moderator and registered users** • **Moderator only**
Web SSO URL	Enter the URL used to enable Web SSO.
Public key	Enter the public key used for Web SSO.

4. Click **Apply**.

Related links

Defining and Managing Video Users on page 218

Managing User Groups

This section is relevant only for enterprise deployments.

You can unify users into groups to manage and maintain users on a group level. Typically, users are joined together based on their location (time zone) or organization unit (for example, a branch, department or workgroup). You can assign the same user to more than one group. For example, if you have separate user groups for departments and locations, you can assign a user to both the "R&D" group and the "China" group.

There are two types of user groups:

- Directory user groups

  Directory groups are user groups defined in the external user directory (LDAP server) and imported to Equinox Management as part of user provisioning. Directory groups cannot be edited or deleted from Equinox Management. Changes to these user groups must be performed on the LDAP server.

- Local user groups

  Local groups are created within Equinox Management. You can modify and delete these groups in Equinox Management. You cannot export local user groups into the LDAP server.

This section explains how to create and manage local user groups:

Related links

Defining and Managing Video Users on page 218
Creating a User Group on page 236
Modifying a User Group on page 237
Removing a User Group on page 238

Creating a User Group

About this task

You can unify users into groups to manage and maintain users on a group level. For more information about Equinox Management user groups, refer to Managing User Groups on page 235.

Typically, you create user groups before creating or downloading users who need to use these user groups, as shown in Figure 47: Workflow for defining users in Avaya Equinox® Management on page 219.

While creating a new user group, you can assign a user profile to it which enables defining settings for all users in this group, instead of doing it individually for every user. When you assign a user profile to a group, all users belonging to the group are automatically assigned the same profile.

Note:

If necessary, you can assign a unique profile to specific users in a group.

User groups are created within Equinox Management, and are *not* synchronized with LDAP servers, if your organization uses an LDAP server.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Users** > **Users from Local Directory** > **Group**.
3. Select **Add**.
4. Enter a name for the group in the **Name** field.
5. To assign a user profile to all users belonging to this group, select a user profile.
6. Select **OK** to save your changes.

   The group appears on the **Groups** tab.

Related links

Managing User Groups on page 235

Modifying a User Group

About this task

Only user groups created within Equinox Management can be modified. User groups imported from the external active directory cannot be edited or deleted.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Users** > **Users from Local Directory** > **Group**.
3. Select the link in the **Name** column for the user group you want to modify.
4. Modify the name of the user group.
5. Change the default user profile of the group by selecting a different user profile from the **User Profile** list.
6. To assign the default user profile to users who had different profiles from the rest of the group, select **Reset**.

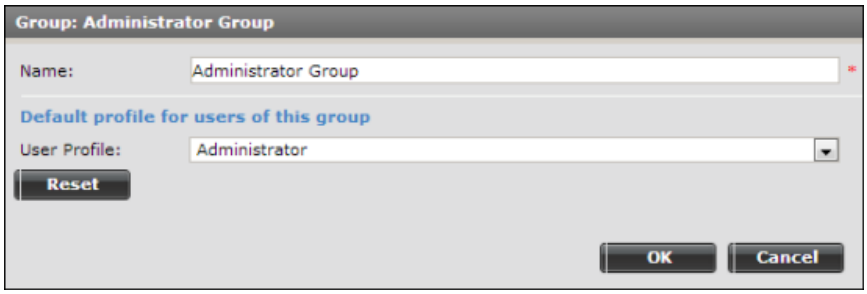


Figure 52: Clearing customized user profiles in a group

7. Select **Apply** to save your changes.

Related links

Managing User Groups on page 235

Removing a User Group

About this task

User groups are used to manage and maintain users on a group level. Only user groups created within Equinox Management can be deleted. User groups imported from the external LDAP server cannot be deleted.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Users** > **Users from Local Directory** > **Group**.
3. Select the group you want to delete.
4. Select **Delete** and then **Yes**.

   The user group is deleted from the scheduler.

Related links

Managing User Groups on page 235

Managing Video Users

This section is relevant only for enterprise deployments.

You can download users from an LDAP server, or you can manually add users to an Equinox Management local directory.

In both cases you can modify users; however, if your organization is synchronized with an LDAP server to provision users, you can only modify the settings stored in Equinox Management, such as virtual room, default endpoints, allowed meeting types, groups, and time zone. See Managing Users from the LDAP Server on page 239. The rest of the settings are overridden each time Equinox Management synchronizes with the LDAP server.

Related links

Defining and Managing Video Users on page 218
Managing Users from the LDAP Server on page 239
Managing users with a local user directory on page 245
Modifying a user on page 248
Limiting Users' Privileges on page 250
Assigning Groups to Multiple Users on page 250
Searching for a User on page 251

Managing Users from the LDAP Server

Equinox Management integrates with Microsoft Active Directory for easy user provisioning. When your organization uses an LDAP server, each user defined in this directory is downloaded to Equinox Management, along with all the information associated with it.

You can associate Equinox Management LDAP users or groups with Equinox Management profiles and virtual rooms. For example, an LDAP group can have Equinox Management administrator permissions or can automatically be assigned a virtual room. Endpoints are also defined in the LDAP server as users and can be downloaded and managed by Equinox Management. See Importing H.323 endpoints from an external LDAP server on page 124.

Once all users are downloaded to Equinox Management, Equinox Management frequently synchronizes with the LDAP server to keep this information up-to-date.

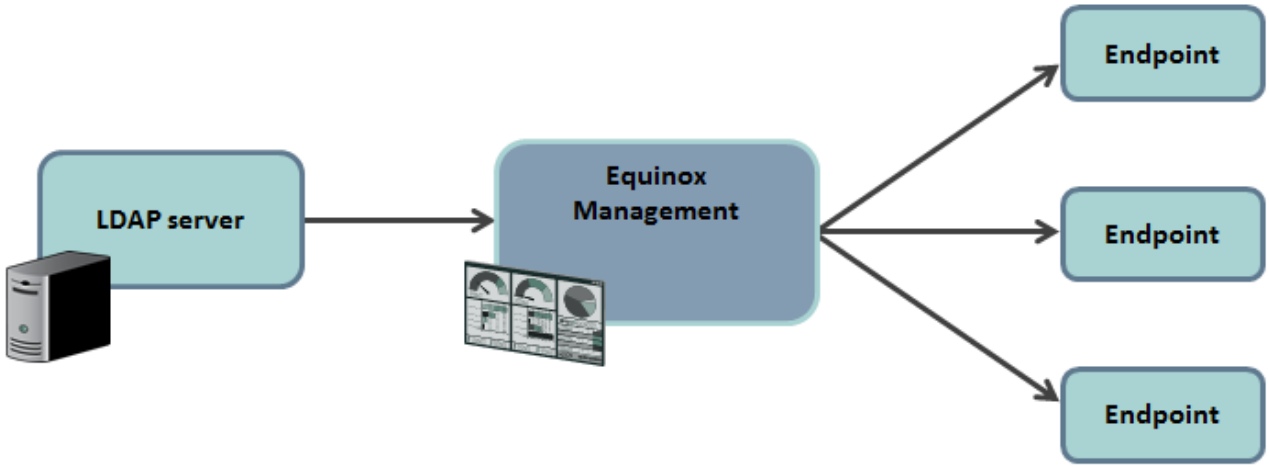


Figure 53: Synchronizing Equinox Management with the LDAP server

You cannot delete users which are downloaded from the LDAP server.

Related links

Managing Video Users on page 238
Connecting Equinox Management with the LDAP server on page 239
Equinox Management LDAP Information Attributes on page 242
Downloading Users from the LDAP Server on page 242
Synchronizing users from the LDAP server on page 244

Connecting Equinox Management with the LDAP server

About this task

To allow user provisioning and synchronization of user profiles using an LDAP server, you have to configure the connection between Equinox Management and the LDAP server.

Note:

When you add more than one LDAP server to Equinox Management ensure that the LDAP server URLs do not resolve to the same server.

Before you begin

Depending on your organization's policies and the LDAP server you are using, decide whether to secure its connection with Equinox Management, as described in Securing the connection between Equinox Management and an LDAP server on page 181.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Servers** > **LDAP Servers**.
3. Click **Add** to add a new LDAP server, or select the required LDAP server entry to modify an existing LDAP server connection.
4. Select the type of LDAP server in the **Directory Server Type** list.

5. Enter the directory server domain or directory server URL in the **URL/Domain** field, using the *ldap://* prefix.

   For a secured connection between the Equinox Management and the LDAP server, do one of the following:

   - Secure the connection with SSL certificates using the *ldaps://* prefix (with an *s*), and specify the port number as *3269* by appending it to the end of the URL. You also need to set up SSL on the LDAP server itself, as described in its documentation.
   - Secure the credentials with MD5 (Microsoft Active Directory only): Enter the FQDN here (not the IP address). You then secure the credentials at a later stage, as part of Downloading Users from the LDAP Server on page 242.

   It is not possible to perform both of these options.

   When securing the connection for User Portal + Web Gateways, you must restart each User Portal for the secure connection to take effect.

   The format of the URL is as follows: `<prefix>://<URL>:<port number>`. For the relevant port numbers, see the **Port** field description in Configuring Endpoints to use an LDAP Directory on page 162.

6. Enter the directory server login ID and password in the relevant fields.

Important:

The user account needs to have read access to all user accounts that you want to synchronize to Equinox Management. This user account does not have to be part of the search base.

7. Click **Configure** to configure the **LDAP Search Base** field.

   The system displays the LDAP Tree, showing all OUs (Organization Units) defined on the directory server. Figure 54: Tree structure in an enterprise deployment on page 241 illustrates the tree structure for an enterprise deployment.

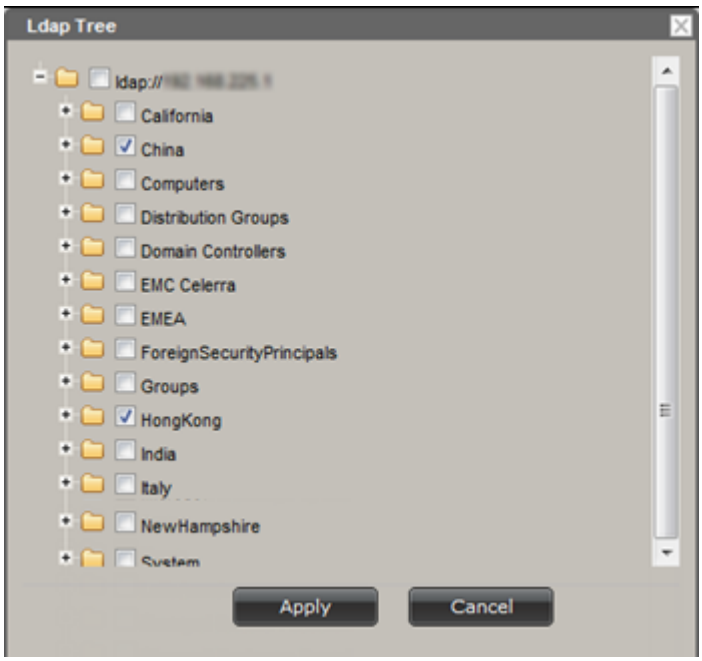


Figure 54: Tree structure in an enterprise deployment

8. Select the OUs whose users you want to download.
9. Click **Apply**.

   The system displays the selected OUs in the **LDAP Search Base** field.

10. Click **Apply**.
11. After your Equinox Management is connected to the LDAP server, you can download users, as well as endpoints and virtual rooms:
    - To download users from the LDAP server, see Downloading Users from the LDAP Server on page 242.
    - To download endpoints, see Importing H.323 endpoints from an external LDAP server on page 124.
    - To download virtual rooms, see Downloading Virtual Rooms from the LDAP Server on page 254.

Related links

Managing Users from the LDAP Server on page 239

Equinox Management LDAP Information Attributes

The table below presents a list of standard schema attributes and their naming convention used by Equinox Management to synchronize with the LDAP server.

Table 45: Equinox Management LDAP Information Attributes

Equinox Management Name	LDAP Attribute name (Active Directory)	LDAP Attribute name (Domino Directory)
User Login Identifier	userPrincipalName	cn
	sAMAccountName	uid
email	email	email
telephone	telephoneNumber	telephoneNumber
mobile	mobile	mobile
givenName	givenName	givenName
sn	sn	sn
sipUri	msRTCSIP-PrimaryUserAddress	N/A
sipUriEnabled	msRTCSIP-UserEnabled	N/A
Organizational Unit	ou	ou
Role	memberOf	member

Related links

Managing Users from the LDAP Server on page 239

Downloading Users from the LDAP Server

About this task

This procedure describes how to download users from the LDAP server. Users are then displayed in the **User** tab and you can modify settings, such as the user profile of a group, and synchronize the database with Equinox Management. See Synchronizing users from the LDAP server on page 244 for details.

Before you begin

- Make sure your Equinox Management is connected to the LDAP server as described in Connecting Equinox Management with the LDAP server on page 239.
- If you are using the Microsoft Outlook delegation feature in your Avaya Meeting Scheduler Outlook Add-in, ensure that the usernames, the part of the email address before the @, is identical in the LDAP definitions and the Equinox Management table.
- You can assign an Equinox Management user profile to users and user groups defined in the LDAP server. When doing so and downloading users from the LDAP server to Equinox Management, roles and permissions are automatically assigned. If user profiles are not defined, a default user profile is assigned to all users. For more information about user profiles, see Managing User Profiles on page 220.

Procedure

1. Access the Equinox Management administrator portal.
2. Select the **Settings** > **Servers** > **LDAP Servers**.

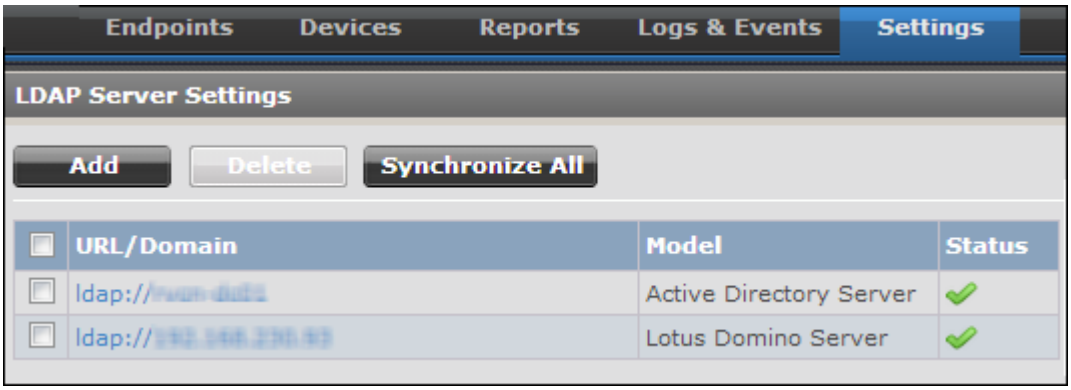


Figure 55: LDAP Server Settings page

3. Select the LDAP server from which you want to download users.
4. Click **Select** next to each user profile to assign LDAP user groups to a specific Equinox Management user profile.

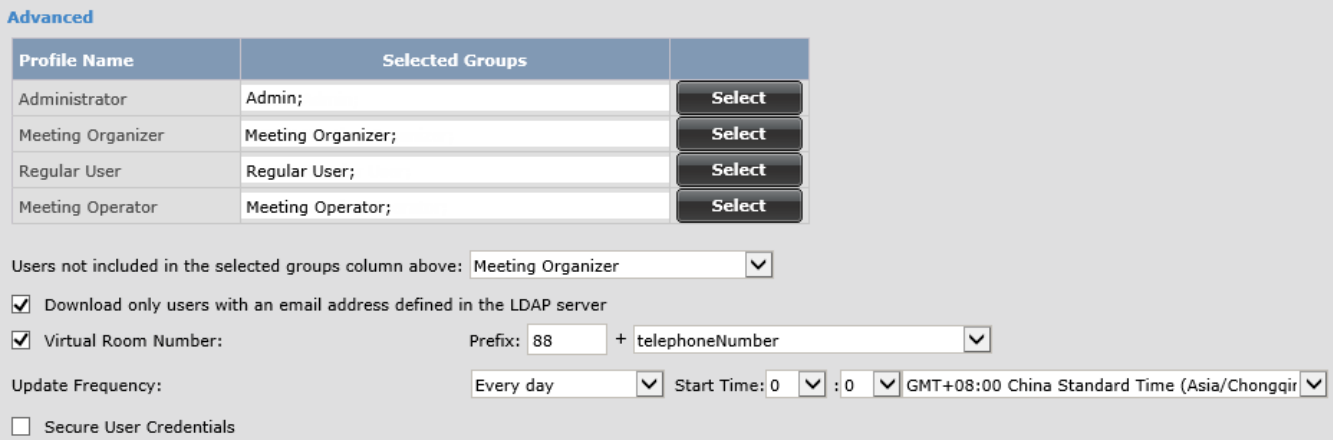


Figure 56: Advanced section of LDAP Server Settings page

You can assign multiple LDAP user groups to each Equinox Management user profile.

By default, all users are assigned the **Meeting Organizer** profile.

When configuring users in a service provider deployment, only select user groups belonging to the organization that you are currently configuring.

5. In the **Users not included in the Selected Groups column above** field, select a user profile you want to assign to all users for whom you did not specify a user profile, or set the field to **Leave on LDAP server** to instruct Equinox Management not to download users that are not assigned to any Equinox Management user type.

The profiles displayed in this field are those that are configured on the User Profiles page (**Settings** > **Users** > **User Profiles**).

6. To download only LDAP users with an email address to Equinox Management, select **Download only users with an email address defined in the LDAP server**.
7. If necessary, assign virtual rooms to the users, as described in Downloading Virtual Rooms from the LDAP Server on page 254.
8. Define how often users and meeting rooms are synchronized with the LDAP server by selecting a value from the **Update Frequency** list.
9. (Optional) If using Microsoft Active Directory, you can encrypt the user's LDAP credentials with MD5 by selecting **Secure User credentials**.

   Important:

   To use this feature, you must also:

   - Define the LDAP server using its FQDN (not its IP address), as described in Connecting Equinox Management with the LDAP server on page 239.
   - In Microsoft Active Directory, enable the **Store password using reversible encryption** option.

   Do not secure user credentials if you secured the connection between the LDAP server and Equinox Management.

10. Select **Apply**.

Related links

Managing Users from the LDAP Server on page 239

Synchronizing users from the LDAP server

About this task

This procedure describes how to synchronize the users in your LDAP server with Equinox Management. Perform this procedure if you have added users to your LDAP server since you first configured it in Equinox Management, or if you made changes to the user attributes, either in the LDAP server, or in Equinox Management. For example, if you modified the default user profile, perform this procedure to assign a new profile to users that do not have customized profiles.

Before you begin

Verify that your LDAP server is configured and make any necessary changes, such as the default user profile, before synchronizing. See Downloading Users from the LDAP Server on page 242 for details.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Servers** > **LDAP Servers**.

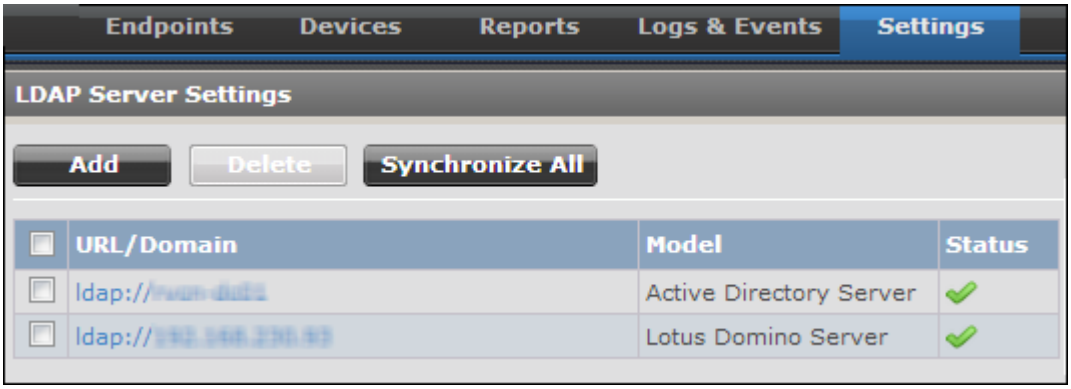


Figure 57: Synchronizing your LDAP database with Equinox Management

3. Click **Synchronize All**.

   The system synchronizes the LDAP database with Equinox Management. You can verify that the synchronization completed successfully by checking the result on the **Logs & Events** tab.

Related links

Managing Users from the LDAP Server on page 239

Managing users with a local user directory

You can add or modify a user profile if Equinox Management uses its own database for storing user information.

Related links

Managing Video Users on page 238
Creating a user within Equinox Management on page 245
Removing a User on page 247

Creating a user within Equinox Management

About this task

You can manually add a user in Equinox Management when a local database is used for storing users.

During this procedure you must assign a user profile and user groups to the user, as described in Creating or modifying a user profile on page 221 and Creating a User Group on page 236.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Users** > **Users from Local Directory** > **All** .
3. Click **Add** to create a new user.
4. Define settings as described in Table 46: Defining a new user on page 246.

Table 46: Defining a new user

Field	Description
Login ID	Enter the new user login ID. The field has a 64 character limit.
Email	Enter the email for the new user. Users who have an email can receive messages and warnings from Equinox Management. The field has a 64 character limit.
First Name	Enter the first name for the new user. The field has a 64 character limit.
Last Name	Enter the last name for the new user. The field has a 64 character limit.
Password	Enter the password for accessing Avaya Equinox® Management.
Telephone (Office)	Enter the office phone number for the new user.
Telephone (Mobile)	Enter the mobile phone number for the new user.
Groups	Assign one or more user groups to the new user: a. Click **Assign**. b. Select one or more user groups. c. Click **Add** or **Add All**. d. Click **OK**.
Personal Endpoint	If this user has a personal endpoint, configure it as described below: a. Click **Assign**. b. Select an endpoint. c. Click **OK**.
Account Status	Select **Enabled** (the default option) to allow the user to access Equinox Management. The status changes to **Disabled** when a user enters an incorrect password more than three times (configurable) and is blocked from the system. This is relevant for users in the Local Directory only.

Table continues…

Field	Description
User Profile	Select a user profile depending on what rights and capabilities you want to give to this user: a. Select a user profile from the list of preconfigured profiles. b. Click **View** to check the settings of the profile you selected.
Participant ID	
Voice Prompt Language	
Time Zone	Select the time zone. This setting is used to correctly schedule meetings for this contact.
Location Preference	To use the user's virtual room location for the user's location in a meeting, select **Auto**, or select another location from the list. Equinox Management uses this location when selecting the MCU to host meetings.

5. If necessary, configure the virtual room for the new user as described in Creating or modifying a virtual room for an Equinox Management user on page 255.
6. Click **OK** to save your changes.

   The user is saved and Equinox Management sends the user a notification e-mail containing login access information.

Related links

Managing users with a local user directory on page 245

Removing a User

About this task

You can only delete users stored on the local directory server. When Equinox Management uses an external directory for user provisioning, users must be deleted from the external directory.

You cannot remove a user profile if:

- You are provisioning users via an external directory server; the **Delete** button is hidden.
- The user is the administrator created during installation.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Users** > **Local Directory** > **All** or **Group** from the sidebar.
3. Select the check box for the user you want to delete.

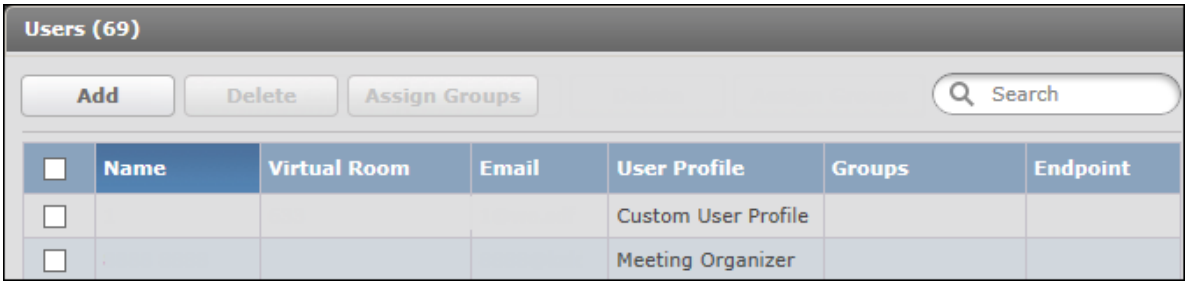


Figure 58: Users tab

4. Select **Delete** and then **OK**.

   The user is deleted from the local directory.

Related links

Managing users with a local user directory on page 245

Modifying a user

About this task

After a user is created locally within Equinox Management or downloaded from the external LDAP server, you can modify the user. Note that while for a local user you can modify all settings, for a downloaded user you can modify only the following settings:

- Personal endpoint
- Groups
- User profile
- Time zone
- Location preference

Procedure

1. Access the Equinox Management administrator portal.
2. Click the **Users** tab.
3. Navigate to the user you want to modify, either under **Users from Active Directory** or **Users from Local Directory** on the sidebar.
4. Modify settings as necessary (see Table 47: Modifying a user on page 248 for details):

Table 47: Modifying a user

Field Name	Description
Login ID	Modify the user login ID.
First Name	Modify the first name for the user.

Table continues…

Field Name	Description
Last Name	Modify the last name for the user.
Password	Enter the password for accessing Avaya Equinox® Management.
Email	Enter the email for the user. Users who have an email can receive messages and warnings from Equinox Management.
Telephone (Office) and **Telephone (Mobile)**	Modify the phone numbers for the user.
Personal Endpoint	If this user has a personal endpoint, configure it as follows: a. Click **Assign**. b. Select an endpoint. c. Click **OK**.
Groups	Assign one or more user groups to the user: a. Click **Assign**. b. Select one or more user groups. c. Click **OK**.
User Profile	Assign a user profile depending on what rights and capabilities you want to give to this user: a. Select a user profile from the list of preconfigured profiles. b. Click **View** to check the settings of the profile you selected.
Time Zone	Select the time zone. This setting is used to correctly schedule meetings for this contact.
Location Preference	To use the user's virtual room location for the user's location in a meeting, select **Auto**, or select another location from the list. Equinox Management uses this location when selecting the MCU to host meetings.
Account Status	This is relevant for users in the Local Directory only. This is set to **Enabled** by default. The status changes to **Disabled** when a user enters an incorrect password more than three times (configurable) and is blocked from the system. Click **Enabled** to allow the user to access Equinox Management.

5. To customize the user's capabilities instead of using those associated with its user profile, see Customizing a user profile on page 229.

6. Click **OK**.

Related links

Managing Video Users on page 238

Limiting Users' Privileges

About this task

After a user is created locally within Equinox Management or downloaded from the external LDAP server, you can remove a user's permission to change the meeting type.

Before you begin

User profiles must be created.

Procedure

1. Select ☰ > **Advanced Parameters**.
2. Enter **com.avaya.conference.virtualroom.meetingtype.fixed** in the **Property Name** and set the **Property Value** to **true**.
3. Select **Apply** > **Close**.

   When the user logs into the User Portal settings and selects the **Virtual Room** tab, the **Meeting Type** field is grayed out. The read-only tenant administrator cannot modify the setting of the virtual room meeting type from the Equinox Management web interface.

Related links

Managing Video Users on page 238

Assigning Groups to Multiple Users

About this task

A user can have more than one group assigned to it. Typically, the first group is assigned to a user as you create or download this user. You can assign other groups to the same user at a later stage, as described in Modifying a user on page 248. For more information about user groups in Equinox Management, see Managing User Groups on page 235.

This procedure explains how to assign groups to multiple users.

Procedure

1. Access the Equinox Management administrator portal.
2. Select the **Users** tab.
3. Select **All** under **Users from Active Directory** or **Users from Local Directory**.
4. Select check boxes for the users to which you want to assign groups.
5. Select **Assign Groups**.

The **Select the groups** window opens.

6. Select check boxes for groups you want to assign and select **OK**.

   The groups are assigned to the selected users.

Related links

Managing Video Users on page 238

Searching for a User

About this task

You can search the **Users** list by the user name or the virtual room number assigned to the user.

Procedure

1. Access the Equinox Management administrator portal.
2. Select the **Users** tab.
3. Select the group in which you want to perform the search.

   The default is **All Groups**.
4. Start typing the name or the virtual room number of the user in the **Search** field, as shown in Figure 59: Searching for a user on page 251.

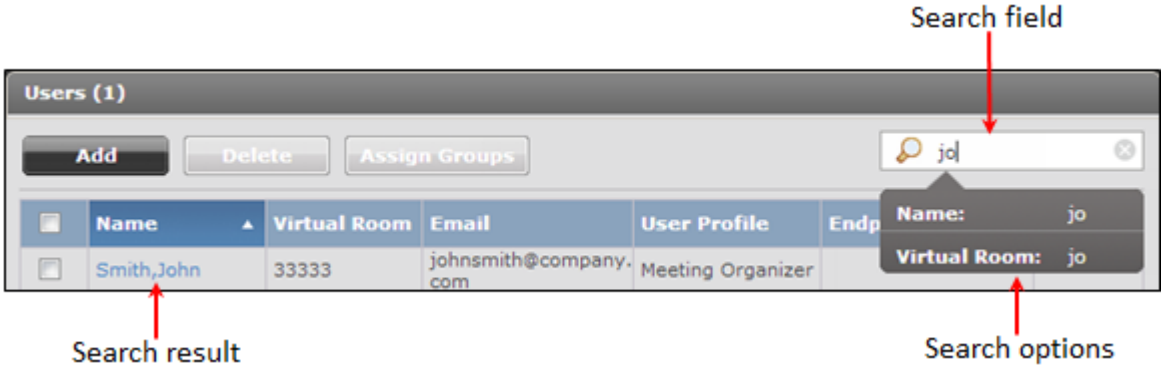


Figure 59: Searching for a user

5. To narrow the search, select **Name** or **Virtual Room** from the **Search** options.

   Search results are listed.
6. To return to the complete list of users, clear the **Search** field.

Related links

Managing Video Users on page 238

Defining Administrators in a Service Provider Deployment

About this task

The default system administrator for a service provider (multi-tenant) deployment is defined during installation. This system administrator can define additional system administrators for the service provider, as described in the procedure below.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Users** > **Add**.

   The **Add User** page appears.

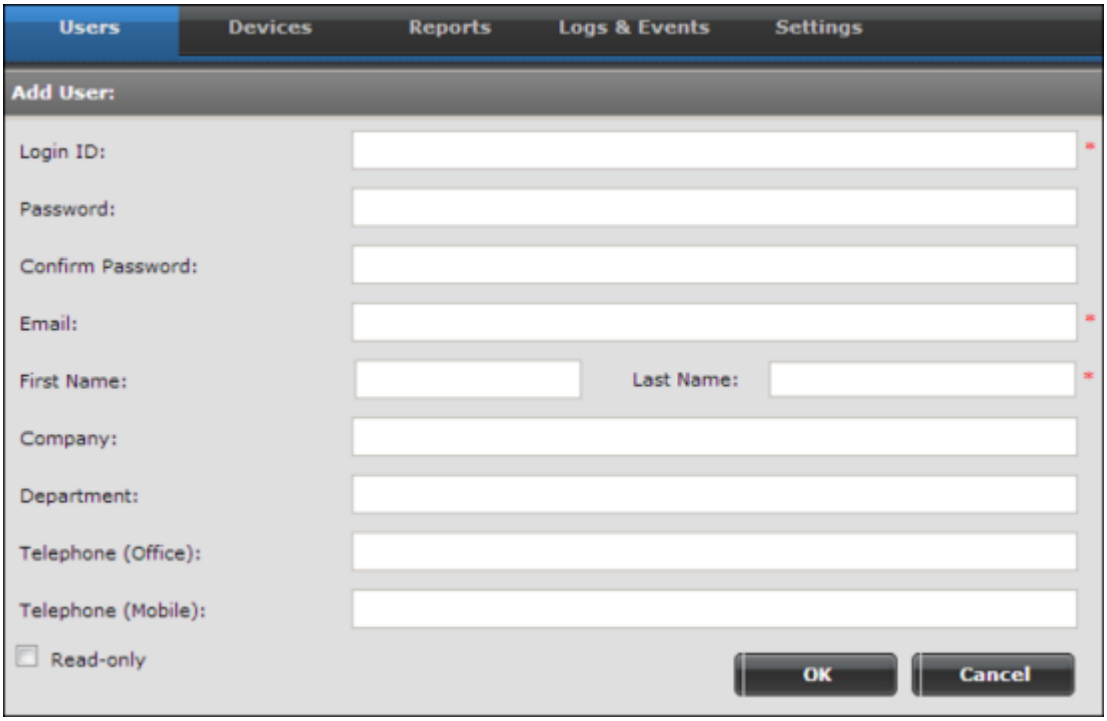


Figure 60: Adding system administrators

3. Enter the administrator's information, as described in Table 48: Defining a new system administrator on page 252.

Table 48: Defining a new system administrator

Field	Description
Login ID **Password** **Confirm Password**	Define the new administrator's login ID and password.

Table continues…

Field	Description
Email	Enter the administrator's email address, used for receiving messages and warnings from Equinox Management.
First Name **Last Name**	Enter the administrator's first and last name.
Company **Department**	(Optional) You can specify these additional details for this administrator.
Telephone (Office) **Telephone (Mobile)**	Enter the phone numbers for the administrator.
Read-only	Select to prevent this administrator from modifying any information in the administrator portal, such as adding organizations.

4. Select **OK**.

Related links

Defining and Managing Video Users on page 218

Managing Virtual Rooms

A virtual meeting room is an online space used to connect multiple Equinox Solution participants in a videoconference. Virtual rooms are hosted by MCUs. In addition to hosting videoconferences, virtual rooms offer features to enhance the videoconferencing experience: it is possible to protect meetings with a PIN number, enable streaming and automatic recording of a meeting, as well as put participants who want to join the meeting on hold (in a "waiting room"), until the moderator joins the meeting.

Virtual rooms can be created manually within Equinox Management, or downloaded from the LDAP server, if your organization uses an LDAP server for user provisioning. If your organization uses an LDAP server, and the virtual rooms are not automatically created for LDAP users downloaded into Equinox Management, you can manually create virtual rooms for users.

Important:

If Equinox Management is configured to automatically create virtual rooms for users, the configuration settings defined manually are overridden every time Equinox Management synchronizes with the LDAP server.

Related links

Defining and Managing Video Users on page 218
Downloading Virtual Rooms from the LDAP Server on page 254
Creating or modifying a virtual room for an Equinox Management user on page 255

Downloading Virtual Rooms from the LDAP Server

About this task

Virtual rooms are literally virtual rooms that serve as a meeting place for your video network users. Virtual meeting rooms can be public (available for any user), or personal (assigned to a specific user, who is the only one allowed to schedule meetings in this room).

When downloading virtual rooms from the LDAP server, the value of the LDAP field mapped to the virtual room must be numeric. The virtual room number is not editable in the virtual room profile window. If the same virtual room number is defined for two users on the LDAP server, the virtual room is created and downloaded to Equinox Management for only one of the users.

Virtual rooms are available only if an Equinox Media Server or Scopia Elite MCU is deployed.

Before you begin

Check the prefixes used for the auto-attendant and for other components within your network, such as Equinox Media Servers or Scopia Elite MCUs, and Gateway. You cannot assign the prefixes already used in the system, because the prefixes assigned to virtual rooms must be unique.

Decide on SIP URIs for the users to whom virtual rooms are assigned (for example, bfmyvr@anymail.com).

Procedure

1. Access the Equinox Management portal.
2. Select **Settings** > **Servers** > **LDAP Servers**.
3. Select the LDAP server to which organization users were added.

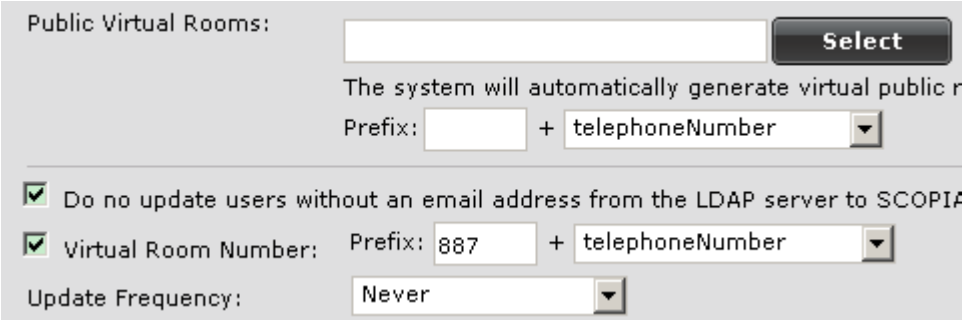


Figure 61: Defining virtual rooms

4. Configure personal and public virtual rooms, as described in Table 49: Configuring settings for downloading virtual meeting rooms on page 255.

Table 49: Configuring settings for downloading virtual meeting rooms

Field	Description
Select	Select the LDAP user group to which you assigned the public virtual rooms on the LDAP server. A public virtual room is not associated with any user, and therefore can be assigned to a group of users.
Virtual Room Number	This is relevant for both personal and public virtual rooms. Define the virtual room number as follows: a. Enter a number that you want to use for a prefix. Use any number that is shorter than 11 digits and is not used as a prefix for the auto attendant or for other deployment components. b. Select the LDAP attribute to use when generating the number of the virtual rooms, according to your dialing plan. Typically, the **telephoneNumber** attribute is used.

5. Define how often users and meeting rooms are synchronized with the LDAP server by selecting a value from the **Update Frequency** list.
6. Select **Apply**.
7. Select **Synchronize All** on the **LDAP Server Settings** page.

   Users from the LDAP server are downloaded into Equinox Management as virtual meeting rooms.
8. Verify that the virtual meeting rooms were downloaded correctly:
   a. Select **Users** > **Active Directory** > **All**.
   b. Verify that the virtual meeting rooms defined in the LDAP server were downloaded and appear on the Users tab.

Related links

Managing Virtual Rooms on page 253

Creating or modifying a virtual room for an Equinox Management user

About this task

After you created or downloaded users into Equinox Management, you can manually create or assign virtual rooms to them. This procedure is relevant for creating and assigning virtual rooms for local users, as well as assigning additional virtual rooms to users downloaded from the external LDAP server.

Note:

To use a second virtual room in a TE deployment with a user created before release 9.1.10, the administrator must manually create the second virtual room.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Users** > **Users from Local Directory** > **All**.
3. Click the link in the **Name** column for the user you require.
4. Enter the user ID and last name in the relevant fields.
5. Click the **Virtual Room** tab.

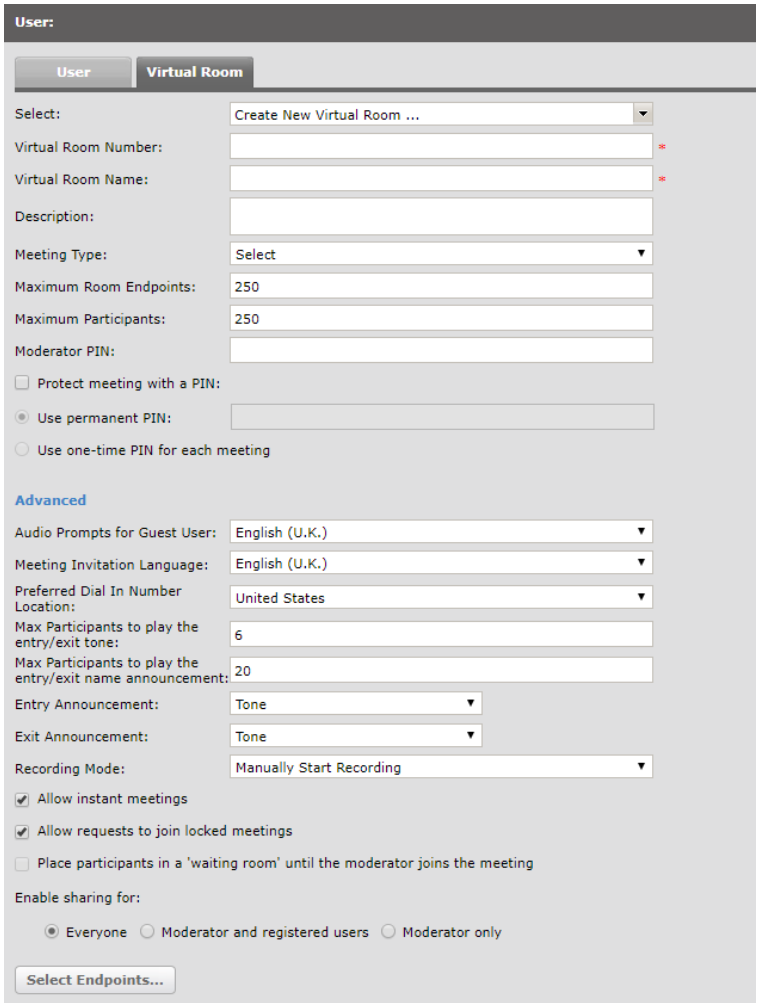


Figure 62: Configuring the user's virtual room settings

6. Configure the virtual room as described in Table 50: Configuring the virtual room settings on page 257.

Table 50: Configuring the virtual room settings

Field	Description
Select	Either select from the list of available virtual rooms, or set this field to **Create New Virtual Room**.
Virtual Room Number	Enter the number of the virtual room. Users dial this number to start a meeting in this virtual room. You can enter any number that does not start with the prefix of the auto attendant, auto routing, or other deployment components.
Virtual Room Name	Enter the name of this virtual room. This name is displayed during the meeting.
Description	Enter a short description of this virtual room.
Meeting Type	Select the meeting type that can be used by this virtual room.
Maximum Participants	Specify the maximum number of participants for an ad-hoc meeting in this virtual room. This setting depends on the number of available ports you want to dedicate to an ad-hoc meeting in this virtual room. This field is read-only in the User Portal.
Maximum Room Endpoints	Specify the maximum number of room endpoints permitted in the user's virtual room. This field is read-only in the User Portal.
Moderator PIN	Enter the PIN that is used to enable in-meeting control and moderation operations.
Protect Meeting with a PIN	Select if you want to protect meetings using this virtual room so that all new participants must enter a PIN to access the meeting. You can define a permanent PIN or to choose the one-time PIN option, when a meeting operator or meeting organizer defines PIN during scheduling. Select this check box and configure the PIN: • Select **Use permanent PIN** and enter the number or • Select **Use one-time PIN for each meeting**.
Audio Prompts for Guest User	Select the language in which audio prompts are played for guest users.
Meeting Invitation Language	Select the language in which meeting invitations sent by the user are displayed.

Table continues…

Field	Description
Preferred Dial In Number	Select the number to be displayed at the top of the invitation number list.
Max Participants to play the entry/exit tone	Select the maximum number of participants that enter the room at the same time to play the entry/exit tone for.
Max Participants to play the entry/exit name announcement	Select the maximum number of participants that enter the room at the same time to play the entry/exit name announcement for.
Entry Announcement	Select whether to play the entry tone or entry name recording announcement.
Exit Announcement	Select whether to play the exit tone or exit name recording announcement.
Allow instant meetings	Select this check box to allow ad hoc meetings using this virtual room. If not selected, this virtual room can only be used for scheduled meetings.
Allow requests to join locked meetings	This enables the user to request permission to join a meeting if the meeting is locked.
Always record meetings	Select to enable recording at the beginning of the meeting. The meeting moderator can enable or disable recording at any time during the meeting.
Always stream meetings	Select to enable streaming at the beginning of the meeting. The meeting moderator can enable or disable streaming at any time during the meeting.
Place participants in a “waiting room” until the moderator joins the meeting	Select to place connected participants in a waiting room before the moderator joins the videoconference, where they cannot hear or see one another. The meeting begins when the moderator joins.
Enable sharing for	Select from the following options to determine who can perform presentations: • **Everyone** • **Moderator and registered users** • **Moderator only**

Table continues…

Field	Description
Select Participants	To automatically invite endpoints to any meeting in this meeting room, assign the endpoints and configure settings as described below: a. Click the **Select Endpoints** button. The system displays the **Select Endpoints** dialog. b. Select endpoints on the **By Directory** tab or on the **By Address** tab. c. Click **Invite**. d. Click **OK**.

7. Click **OK** to save the settings for the virtual room.

Related links

Managing Virtual Rooms on page 253

Creating Preferred Dial In Number Variables

About this task

Use this page to create preferred dial-in phone number variables for the meetings invitations. The preferred dial-in phone numbers are displayed above other phone numbers in the invitations. Use a separate line for each phone number in the following format with vertical bar symbols between each component, Key=Dial-In Number Location|Dial-In Label|Dial-In Number. An example is **dialin_en_us=United States|United States|+1-989-256-0855**. For a complete list of examples see List of preferred dial in numbers examples on page 454.

Label	Definition
Key	Variable name
Dial-In Number Location	Country name in English
Dial-In Label	Country name in the local language
Dial-In Number	The phone number in international format

Procedure

1. Access the Avaya Equinox® Management administrator portal.
2. Click **Settings** > **Meetings** > **Dial In Numbers**.
3. Edit the text box by following the template.
4. Click **Apply**.

Next steps

Proceed to the Creating an invitation template on page 262 topic.

Related links

Defining and Managing Video Users on page 218

Invitation Template Variables and Parameter Settings

You can freely add spaces to the meeting ID string for legibility and commas to add delays.

You can use the user variables to add spaces and dialling pauses to the meeting ID string.

Table of Advanced Parameter Settings for the Invitation Template

Label	Effect	Description
com.radvision.icm.invitation.dialinstring.meetingIdDelayInDialString	Insert a number of commas, according to the parameter value, before the meeting ID.	**Default value**: 2. **Range**: 1–10. This is a global parameter setting and is always used in the dial string.
com.radvision.icm.invitation.dialinstring.meetingPinDelayInDialString	Insert a number of commas, according to the parameter value, before the access PIN.	**Default value**: 5. **Range**: 1–10. This is a global parameter setting and is always used in the dial string.
com.radvision.icm.invitation.dialinstring.meetingIdwithBreakInDialString	Insert a comma between every number of digits, according to the parameter value, of the meeting ID string.	**Default value**: 4. **Range**: 1–10. When the parameter is set and the **Location** field uses variables [DIAL-IN-LABEL]: [DIAL-IN-STRING], it breaks the meeting invitation.

Table of User Variables for the Invitation Template

Label	Effect	Description
MEETING_ID_WITH_SPACE_X	Insert a space between every X number of digits of the meeting ID string.	**Range of X**: 1–10. This makes long meeting IDs more legible.
MEETING_ID_WITH_COMMA_Y	Insert a comma between every Y number of digits of the meeting ID string.	**Range of Y**: 1–10. This adds dialling pauses in long meeting ID strings.
MEETING_ID_WITH_DASH_Z	Insert a dash between every Z number of digits of the meeting ID string.	**Range of Z**: 1–10. This adds dialling pauses in long meeting ID strings.

Note:

Equinox supports the following dynamic access pin expressions requirement so that the invitation template displays correctly when PIN is empty:

Example

Assuming:

- [DIAL-IN-NUMBER] = +1555555555
- [MEETING_ID] = 12345678901234
- [PIN] = 1234
- com.radvision.icm.invitation.dialinstring.meetingIdDelayInDialString= 2
- com.radvision.icm.invitation.dialinstring.meetingIdwithBreakInDialString= 4
- com.radvision.icm.invitation.dialinstring.meetingIdDelayInDialString= 5

Then [DIAL-IN-STRING] = +1555555555,,1234,5678,9012,34#,,,,,1234#

Example

Assuming:

- [DIAL-IN-NUMBER] = +1555555555
- [PIN] = Empty
- com.radvision.icm.invitation.dialinstring.meetingIdDelayInDialString= 2
- com.radvision.icm.invitation.dialinstring.meetingIdwithBreakInDialString= 0
- com.radvision.icm.invitation.dialinstring.meetingIdDelayInDialString= 5

Then [DIAL-IN-STRING] = +1555555555,,12345678901234#

Example

Assuming [MEETING_ID] = 12345678901234, then:

- [MEETING_ID_WITH_SPACE_3] = 123 456 789 012 34
- [MEETING_ID_WITH_SPACE_4] = 1234 5678 9012 34
- [MEETING_ID_WITH_COMMA_3] = 123,456,789,012,34
- [MEETING_ID_WITH_COMMA_4] = 1234,5678,9012,34
- [MEETING_ID_WITH_DASH_3] = 123–456–789–012–34
- [MEETING_ID_WITH_DASH_4] = 1234–5678–9012–34

PIN start and end tags useage

The [PIN_START] and [PIN_END] tags are placeholders for the meeting PIN. When the invitation template has the pattern, [PIN_START]xxxxxxxx[PIN]xxxx[PIN_END], then Equinox applies the following:

- If PIN is empty, then it removes everything between [PIN_START] and [PIN_END].
- If PIN is not empty, then it only removes the [PIN_START] and [PIN_END] tags but keeps everything in between.

Example

Assuming the pattern is [MEETING_ID]#[PIN_START],,,[PIN]#[PIN_END], then:

- If PIN is empty, then it is equivalent to [MEETING_ID]#.

- If PIN is not empty, then it is equivalent to [MEETING_ID]#,,,[PIN]#.

Example

Assuming the pattern is [MEETING_ID]#[PIN_START] and [PIN]#[PIN_END], then:

- If PIN is empty, then it is equivalent to [MEETING_ID]#.
- If PIN is not empty, then it is equivalent to [MEETING_ID]# and [PIN]#.

Related links

Defining and Managing Video Users on page 218

Creating an invitation template

About this task

Users can invite each other to videoconferences from either the Equinox User Portal, or from Microsoft Outlook, using the Avaya Meeting Scheduler Outlook Add-in. You can create the template for the text that is displayed in invitations.

The template text can contain links for participants to easily access the videoconference from different applications and devices.

Before you begin

You have the option to create preferred dial in number variables, see Creating Preferred Dial In Number Variables on page 259, and dial string variables, see Invitation Template Variables and Parameter Settings on page 260.

Procedure

1. Access the Avaya Equinox® Management administrator portal.
2. Click **Settings** > **Meetings** > **Invitations**.

   The system displays the **Meeting Invitations** page.
3. In the **Location** field, enter the [DESKTOP_MOBILE_ACCESS_LINK] [DIAL-IN-LABEL]: [DIAL-IN-STRING].
4. Select the **Insert this tag in the invitation location field for reserved meetings** check box when using a one-time PIN for a meeting that is reserved in Avaya Equinox® Management.

   It adds a *Reservation* tag at the beginning of the invitation template location field for all one-time PIN meetings that are reserved in Avaya Equinox® Management. This tag is to warn the user that this meeting is synchronized in Avaya Equinox® Management and must not be rescheduled in a non-Windows Outlook add-in. The tag default value is *Reserved*. You can change this value for different languages. Avaya Equinox® Management does not add a *Reservation* tag for any meetings that are not reserved in Avaya Equinox® Management therefore users that have *Reserve meetings from Windows Outlook Add-in* disabled.

5. In the **Languages** field, select the template's language edit mode. This is the language in which the template is displayed while you edit it.
6. Toggle between the **Format** options by selecting either **HTML** or **Plain** for plain text.

Figure 63: Changing the invitation formatting

The Outlook plugin uses **HTML** format. The Avaya IX™ Workplace Client uses **Plain** format. You must create invitation templates for both HTML and Plain formats.

7. Use the **Insert** menu to include placeholders for the following links:
   - **Meeting Info**: Meeting ID, PIN and E164 values of the videoconference.

     The E164 value is determined as follows:

     - If there is no specified PIN: E164 = **[MEETING_ID]**
     - If there is a specified PIN: E164 = **[MEETING_ID]***[PIN]**
   - **Desktop and Mobile Access Links**: Link for participants to access the videoconference.

     Appears when an FQDN is configured on the **User Portal/Web Gateway Setting** page (**Settings** > **Devices** > **User Portal/Web Gateway**).
   - **Phone Numbers**: Number for participants who need to dial into the videoconference.

     Appears when a P20 Gateway is configured on the **Gateways** page (**Devices** > **Gateways**).
   - **UC Access Links**: Link for participants joining from their unified communications applications, such as Avaya Aura® Conferencing.

     Appears when a Video Gateway is configured on the **Gateways** page (**Devices** > **Gateways**).
8. To enter a URL for users to join the meeting directly from their computer or mobile device:
   a. Click **Insert** > **Desktop and Mobile Access Link** and copy the link address.
   b. Select the **Click to Join** text.
   c. Click the **Add Hyperlink** icon:

Figure 64: Adding a URL

   d. Enter the URL in the format `http://<DESKTOP_MOBILE_ACCESS_LINK>` and click **OK**.

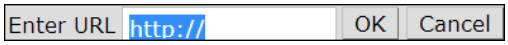


Figure 65: Entering URL

The URL link and configured phone number display in the **Location** field of the meeting invitation.

9. Modify the text of the invitation as necessary.
10. Click **Apply**.

    Repeat step 3 and the ensuing steps of the procedure to configure any other another language that you want to support.

Related links

Defining and Managing Video Users on page 218

Configuring WebRTC calls for the Microsoft Edge browser

About this task

Microsoft supports WebRTC 1.0 in its Edge browser. For the user, there is no need to download a native client to join a meeting. The user can join an Equinox meeting or an Avaya Equinox® Meetings Online with audio and video using the Edge WebRTC browser in Windows.

Note:

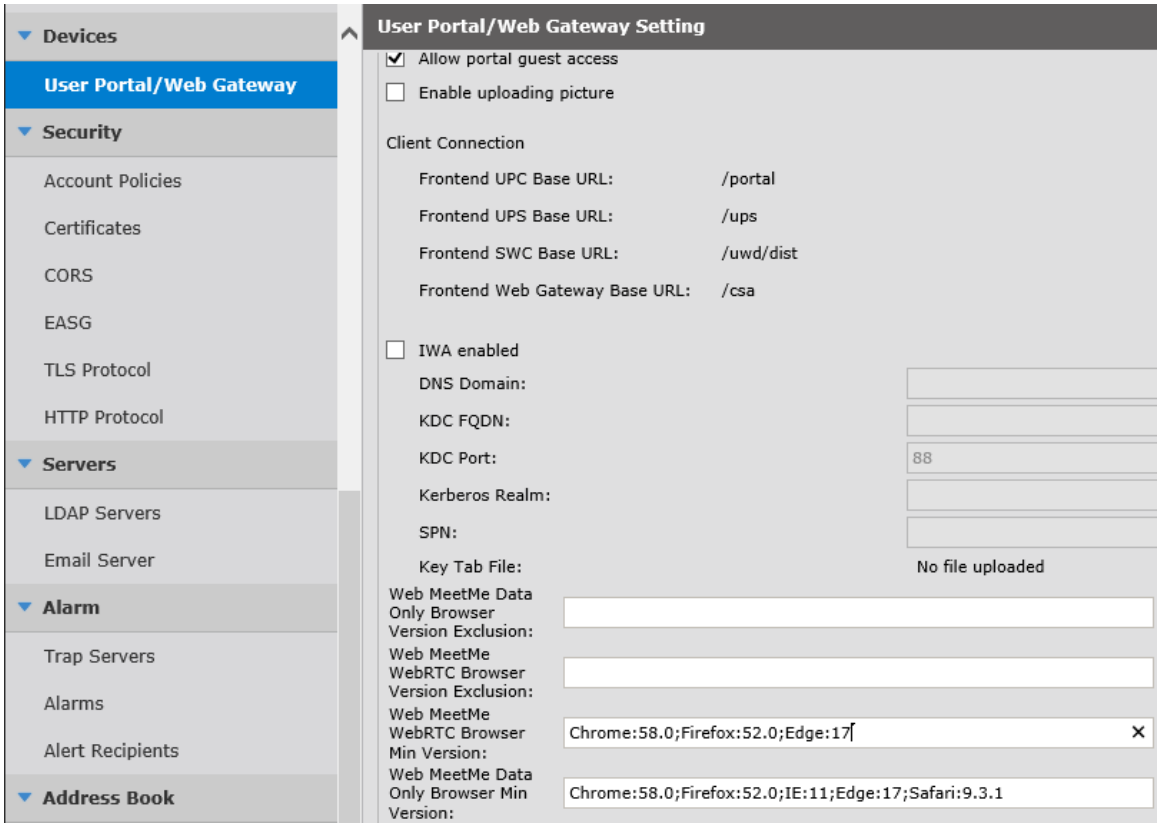
- The Edge browser does not support TCP and TLS TURN. If the enterprise firewalls block the UDP ports, the participant cannot use the Edge browser client to join the Avaya Equinox® Meetings Online or external enterprise meetings.
- Only the desktop browser is currently supported.
- The Edge browser supports changing the camera and microphone. The user must use the operating system to change the default speaker.

Before you begin

- The Edge browser does not support STUN. You must enable the TURN UDP in the Avaya Session Border Controller for Enterprise to support the Edge browser NAT/firewall traversal.
- For an Over The Top deployment you must have a WebRTC gateway deployed.
- For a Team Engagement deployment you must have an Avaya Aura® Media Server deployed.
- Use this feature from Avaya Equinox® Conferencing 9.1 FP5 in Over The Top and Team Engagement deployments and with Edge desktop browser version 42 (EdgeHTML version 17) or above.
- For a Team Engagement deployment the minimum browser version settings must be entered in the Avaya Aura® Web Gateway administrator user interface. See the *Administering the Avaya Aura® Web Gateway* publication for more information.

Procedure

1. (Over The Top) Configure Equinox Management as follows:
   a. Click **Settings** > **User Portal/Web Gateway** > **Advanced**. and add `Edge:17` in the field because this value is not added automatically.



   A message appears informing on configuring settings listed in the following steps of this procedure.

   b. In the **Web MeetMe WebRTC Browser Min Version** field, add `Edge:17` to the other default setting as shown in the above figure.
   c. In the **Web MeetMe Data Only Browser Min Version** field, add `Edge:17` to the other default settings.
   d. Click **Apply**.
   e. For Configuring Avaya Equinox® Media Server for WebRTC-based calls in Over The Top deployments see the *Administering Avaya Equinox Media Server* publication.
2. (Team Engagement) For Configuring Avaya Equinox® Media Server for WebRTC-based calls in Team Engagement deployments see the *Administering Avaya Equinox Media Server* publication.
3. Configure the Avaya Session Border Controller for Enterprise for the client side TURN and the NONCE refresh timer to 4 hours.

See the Avaya Session Border Controller for Enterprise documentation for detailed information.

Related links

Defining and Managing Video Users on page 218

Chapter 6: Scheduling your videoconference from the Equinox Management User Portal

About this task

You can use the Avaya Equinox® Management user portal to schedule meetings and reserve the necessary video network resources for the meeting.

Scheduling a videoconference is similar to creating a regular meeting. You must select the participants, and then set the time, date, and location of your meeting. Often, an endpoint is associated with a virtual room, so the endpoints of a reserved room are automatically added to the meeting resources. You can also add more resources, like a shared endpoint in a meeting room (room system).

Equinox Management checks that the required video network resources are available for the scheduled time, including the media server connections, and then sends the invitation by email to those listed in the **To** field of the invitation.

Important:

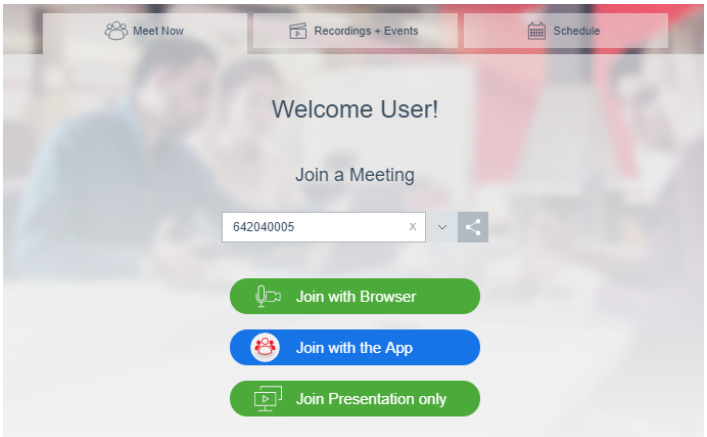
Equinox Management requires an SMTP server such as Microsoft Exchange in your deployment to send meeting invitations by email.

When you schedule a meeting, Equinox Management uses the default settings in your user profile and the chosen virtual room, such as the time zone and whether participants need a PIN to join the meeting. You can override the settings for this meeting by defining the meeting properties. To change the default settings in your user profile and virtual room, see *User Guide for Avaya Equinox® Management*. Administrators can also change settings for a user; see Defining and Managing Video Users on page 218.

As a user, you can schedule a videoconference only if your administrator enabled this functionality in your user profile.

Procedure

1. As a user, access the Equinox Management user portal and click **Schedule**.



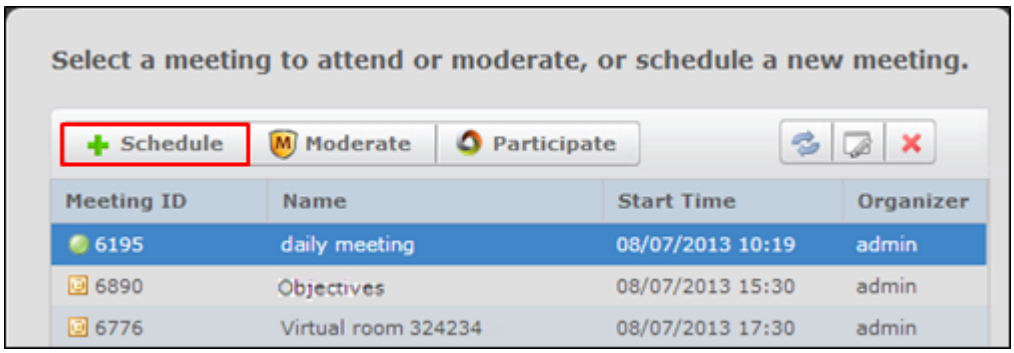
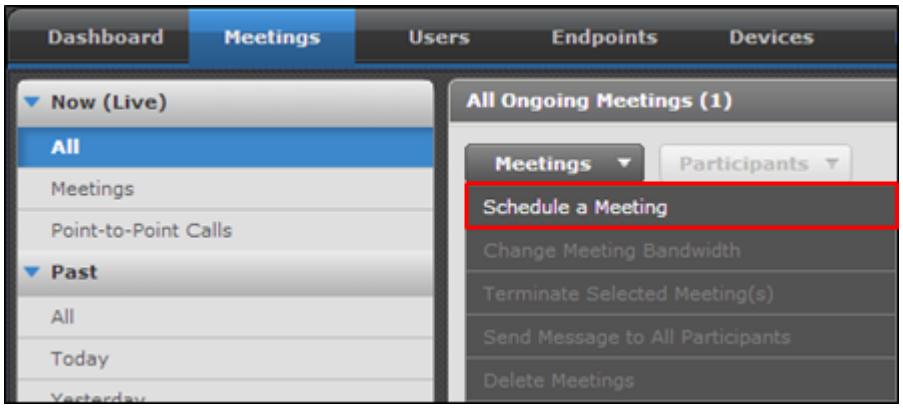


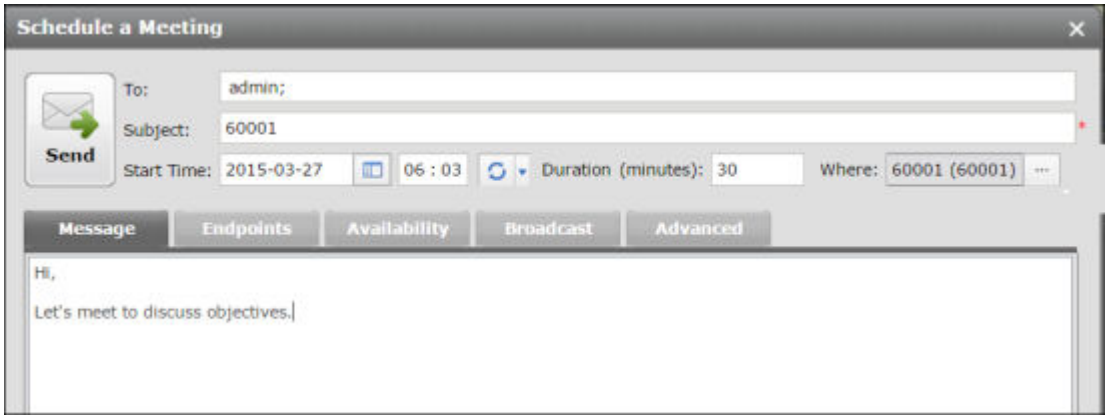
Figure 66: Access meeting scheduling from the Equinox Management user portal

Or

2. As an administrator, access the Equinox Management administrator portal and click **Meetings** > **Meetings** > **Meetings** > **Schedule a Meeting**.



Enter the meeting invitation details.



3. Enter the general meeting information, as described in the following table:

Table 51: General Meeting Information

Field	Description
To	Enter the first characters of a participant to choose from the list of users. If this username is associated with a dedicated endpoint, Equinox Management automatically adds the endpoint to the list of endpoints required for this meeting, listed in the **Endpoints** tab. **Tip:** If you are also one of the participants, add your own name to this list. To designate yourself as the moderator in the **Advanced** tab, see Configuring Advanced Meeting Properties in the User Portal on page 284.
Subject	Enter the subject of the meeting.

Table continues…

Field	Description
Start Time	Click to choose the scheduled start date. • Click **<<** or **>>** to change the year. • Click **<** or **>** to change the month. Select the scheduled start time by clicking on the hours and minutes and entering the time.

Table continues…

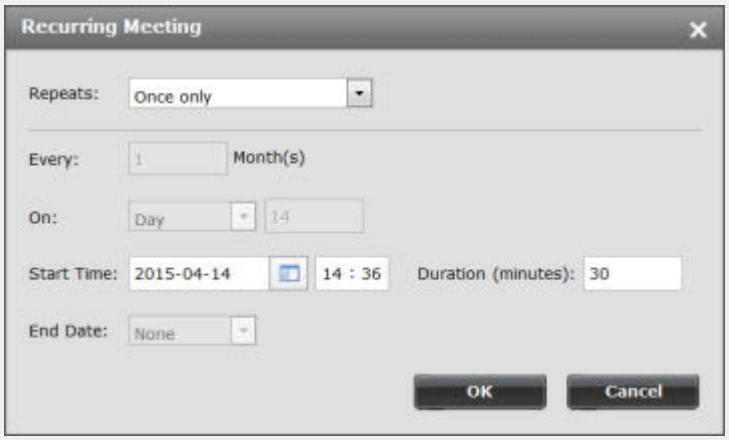
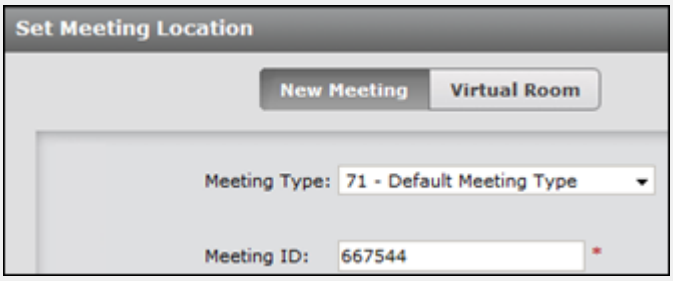
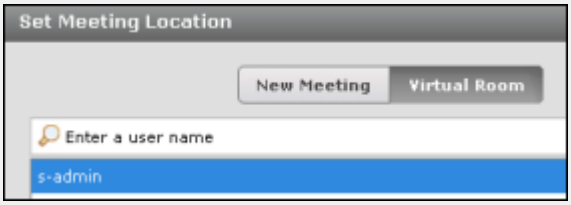
Field	Description
Recurring	Enter information for meetings that take place at regular intervals.  Select the relevant option in the **Repeats** field to change the frequency of the meeting's recurrence: • **Once only** indicates the meeting occurs only once. • **Daily** indicates it repeats every day. Set **Every** to select an interval of days between meetings. • **Weekly** indicates it repeats once a week. Set **Every** to select an interval of weeks between meetings, and set **On** to select which day of the week to schedule the weekly meeting. • **Monthly** indicates it repeats according to a specified number of months. Set **Every** to select the interval of months between meetings. Set **On** to select when in the month to schedule the meetings, either according to a specific date in the month, or according to a day in the month. Enter the meeting's start time in **Start Time**. You can also enter this value directly on the calendar. Enter the meeting duration in **Duration**. You can also enter it in the main invitation window. By default, Equinox Management does not end the meeting if participants are still connected and there is no resource conflict with other scheduled meetings. Enter the last date of the meeting's repetition in **End Date**: • **None** indicates the meeting repeats indefinitely. • **By** requires you to enter the last date of the meeting recurrence. • **After** requires you to enter the number of recurring meetings to schedule.
Duration	Enter the meeting length in minutes. By default, Equinox Management does not end the meeting if participants are still connected and there is no resource conflict with other scheduled meetings. To end the meeting at the specified time, even if participants are still connected, see Configuring Advanced Meeting Properties in the User Portal on page 284.

Table continues…

Field	Description
Where	Click **...** to change the automatically assigned virtual room.  Click **New Meeting** to manually enter the meeting ID: • **Meeting Type** determines the default settings of the meeting. Each meeting type corresponds to a dial prefix. • **Meeting ID** corresponds to the ID of the virtual room which is the virtual location of the meeting. Alternatively, select **Virtual Room** to choose your own or someone else's virtual room as the location of the meeting. The room's default settings define the properties of the meeting. 
Message	The system automatically inserts text into the body of the invitation, containing instructions on how to connect to the videoconference. This text is configured by the administrator. You can add to this text by entering additional information in this field, such as the list of items on the agenda.

4. Optionally, you can configure an Advanced Parameter to hide the email address of the sender, as follows:
   a. Click ≡ > **Advanced Parameters**.
   b. Configure the parameter `com.avaya.conference.sender.email` with the value `NoReply@Avaya.com`
5. To reserve a dedicated video endpoint for the meeting, select the **Endpoints** tab above the message body of the invitation.

   XT Series endpoints include calendar functionality which alerts users when a meeting is about to start.

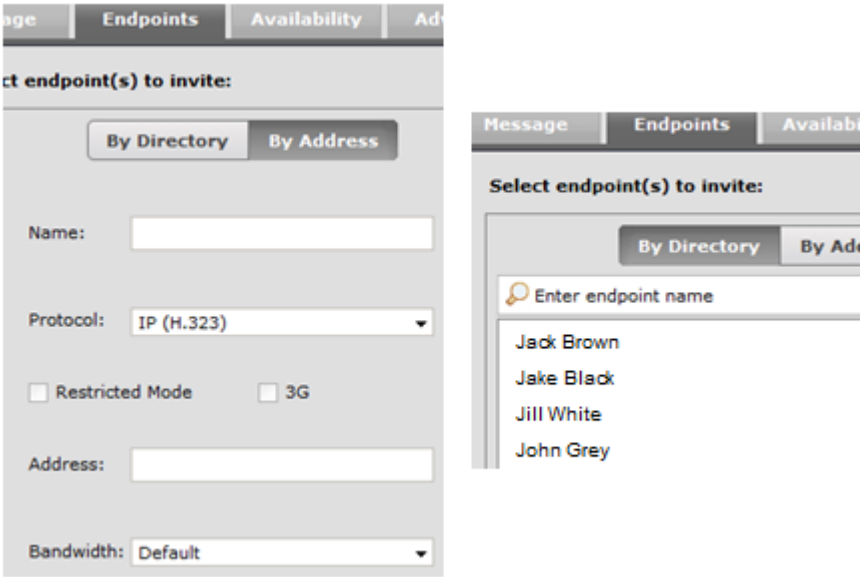


Figure 67: Reserving endpoints for the meeting

Configure the following fields. To associate an endpoint with a user, or for other advanced endpoint options, see Configuring Advanced Meeting Properties in the User Portal on page 284.

Table 52: Endpoints Tab Fields

Field	Description
By Directory	Click the endpoint listed in the address book, or use the search field to narrow the list.
By Address	Click this tab to manually enter the endpoint's details if it is not listed in the endpoint directory.
Protocol	Select the videoconferencing standard used to communicate with this endpoint: • Click **IP (H.323)** if you invite an H.323 endpoint. • Click **IP (SIP)** if you invite a SIP endpoint. • Click **ISDN/PSTN (H.320)** if you invite an ISDN/PSTN device, using the H.320 standard for devices outside the organization. • Click **Mobile** if you invite a 3G device.
Restricted Mode	Restricted mode is used for ISDN endpoints only, when the PBX and line uses a restricted form of communication, reserving the top 8k of each packet for control data only. If enabled, the bandwidth values on these lines are in multiples of 56kbps, instead of multiples of 64kbps.

Table continues…

Field	Description
Address	Enter the endpoint's address. • If you invite an H.323 or SIP endpoint, enter the E.164 number, IP address or domain name you received for the endpoint. • If the invited endpoint is a mobile device (not Scopia Mobile) or an ISDN/PSTN device, enter the country code, area code, and phone number for this device.
Bandwidth	Select the bandwidth used to communicate with this device, measured in kbps. Kilobits per second (kbps) is the standard unit to measure bitrate, measuring the throughput of data communication between two devices. Since this counts the number of individual bits (ones or zeros), you must divide by eight to calculate the number of kilobytes per second (KBps). • **Default** supports all layouts and endpoints with various resolutions. • **<bandwidth_values>** determines the maximum bandwidth for this endpoint to connect to the meeting.

6. Click the **Availability** tab to check if the endpoints are available and if there are enough media server resources (displayed in the **Virtual Media Server** row) for this meeting.

   The system displays the week in which the meeting is scheduled to occur (Figure 68: Verifying participant availability (example) on page 274) and indicates availability using these colors:

   - **No color**: Indicates the endpoint is available and there are enough media server resources for this time slot.
   - **Blue**: Indicates the endpoint is already booked for another meeting or there are not enough media server resources for this time slot.
   - **Gray** (in the **Virtual Equinox Media Server** row only): Indicates the system does not know the media server's availability. By default, the system displays availability for the four hours before and after the scheduled time slot. Time slots outside this period are colored gray.

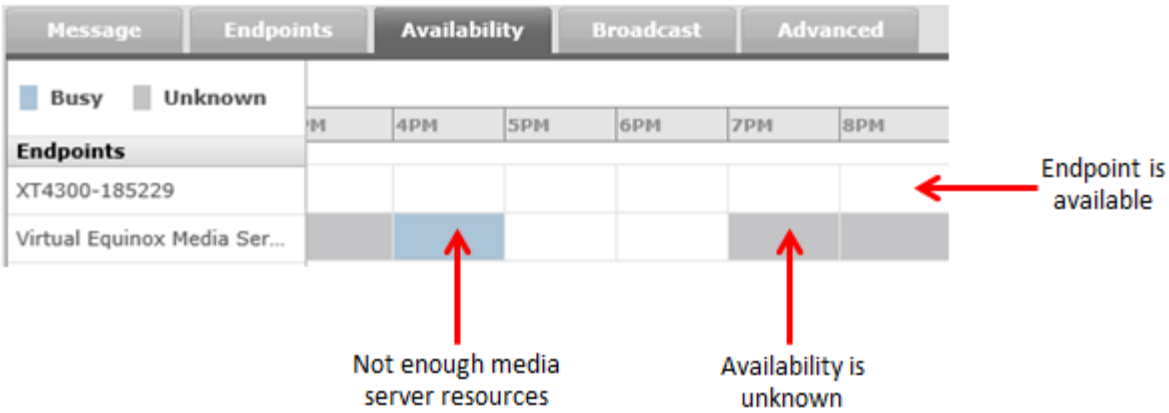


Figure 68: Verifying participant availability (example)

7. (Optional) If you are using the Avaya Equinox® Streaming and Recording solution, click the **Broadcast** tab to configure streaming and recording properties (see Configuring Recording and Streaming Meeting Properties in the User Portal on page 280). For information about the different Avaya Scopia recording and streaming solutions, see Planning and configuring streaming and recording servers in Equinox Management on page 176.
8. (Optional) Click the **Advanced** tab to configure advanced meeting properties (see Configuring Advanced Meeting Properties in the User Portal on page 284).
9. If you have completed the scheduling procedure, click **Send**.

   If all required resources are available, Equinox Management schedules the meeting, reserves the resources and sends invitations to the participants. If non-essential resources (such as optional endpoints or users) are not available, Equinox Management schedules the meeting but notifies you of the conflicts.

   If essential resources are not available, Equinox Management does not schedule the meeting and instead notifies you of the conflicts.
10. To change a scheduled meeting, click **Properties**.

    To delete a scheduled meeting, click **Delete**.

Related links

Enabling the Avaya Meeting Scheduler Outlook Add-in without the Avaya IX Workplace Client on page 275
Configuring Outlook on the web without the Avaya IX Workplace Client on page 276
Configuring Equinox Streaming and Recording Server Meeting Properties in the User Portal on page 280
Configuring Advanced Meeting Properties in the User Portal on page 284

Enabling the Avaya Meeting Scheduler Outlook Add-in without the Avaya IX™ Workplace Client

About this task

You can set the Avaya Meeting Scheduler Outlook Add-in to work with an Avaya Vantage™ device or the Avaya Equinox® Meetings for Web (WebRTC) client, without having to install the Avaya IX™ Workplace Client. The Outlook plug-in can be enabled for both Windows and Mac environments.

Note:

The Avaya Meeting Scheduler Outlook Add-in for Mac and web mail do not reserve scheduled meetings in Equinox Management. Only the Avaya Meeting Scheduler Outlook Add-in for Windows can reserve scheduled meetings in Equinox Management and when the user profile is enabled for this capability. Users must not change any already reserved meetings from non-Windows devices to avoid potential out of sync issues, which may prevent participants from joining the scheduled meetings.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Devices** > **User Portal/Web Gateway**.

   The system displays the **User Portal/Web Gateway Setting** page.
3. In the **Outlook plug-in for Windows downloading address** field, enter the Microsoft Office Store URL from which the Avaya Meeting Scheduler Outlook Add-in can be enabled for Windows.
4. In the **Outlook plug-in for MAC downloading address** field, enter the Microsoft Office Store URL from which the Avaya Meeting Scheduler Outlook Add-in can be enabled for Mac.
5. Click **Apply**.

Related links

Scheduling your videoconference from the Equinox Management User Portal on page 267

Configuring Outlook on the web without the Avaya IX™ Workplace Client

About this task

A user with premise based Avaya Equinox® for Over The Top or Avaya Equinox® for Team Engagement can use a plug-in for **Outlook on the web** without Outlook or a client installed locally on Windows or macOS. The customer administrator must create an Avaya Cloud (Zang) account and add the company profile to the Cloud account. He must have proof that the customer owns the e-mail domain address.

If the customer only has Avaya Equinox® Meetings Online accounts, then there is no need to manually configure anything for **Outlook on the web**. The Outlook plugin auto discovers the user's Avaya Equinox® Meetings Online account and configurations.

The recommended way to allow users to configure theAvaya IX™ Workplace Client is by entering an email address. If you are unable to configure the required PTR records in DNS, use Avaya Cloud accounts to create a mapping for your company domain to one or more settings files.

Note:

The Avaya Meeting Scheduler Outlook Add-in for Mac and web mail do not reserve scheduled meetings in Equinox Management. Only the Avaya Meeting Scheduler Outlook Add-in for Windows can reserve scheduled meetings in Equinox Management and when the user profile is enabled for this capability. Users must not change any already reserved meetings from non-Windows devices to avoid potential out of sync issues, which may prevent participants from joining the scheduled meetings.

Before you begin

- Register a company domain

Procedure

1. Register an Avaya Cloud (Zang) account on page 277
2. Set up a company domain in the Avaya Cloud on page 278
3. Map your domain to the settings file URL on page 279
4. Test the configurations by entering the following URL in a browser and replace **companydomain** with the real domain:

   https://accounts.zang.io/api/1.0/companies/companydomain.com/products/equinoxcloudclient/public_application_setting/

Related links

Scheduling your videoconference from the Equinox Management User Portal on page 267
Registering an Avaya Cloud account on page 277
Setting up a company domain in the Avaya Cloud account on page 278
Mapping your domain to the settings file URL on page 279

Registering an Avaya Cloud account

About this task

You must register an Avaya Cloud (Zang) account to use the **Outlook on the web** plugin.

Procedure

1. In your web browser, enter https://accounts.zang.io.
2. In the **Email or Phone** field, enter your email address.
3. Click **Yes, sign me up!**.

   Avaya Cloud sends a confirmation e-mail to the e-mail address you specified.
4. In your mailbox, open the confirmation e-mail and click the **Confirm** button.

   You are redirected to the Avaya Cloud My Account page.
5. Provide your first name, last name, password, and, optionally, a photo and then click **Create an account**.

Next steps

- Setting up a company domain in the Avaya Cloud account on page 278
- Mapping your domain to the settings file URL on page 279

Related links

Configuring Outlook on the web without the Avaya IX Workplace Client on page 276

Setting up a company domain in the Avaya Cloud account

About this task

The key part of the Avaya Cloud (Zang) account integration is to associate the customer's domain address with their Avaya Cloud account.

Before you begin

- Registering an Avaya Cloud account on page 277
- Ensure that your customer domain matches the e-mail address domain for logging in to Avaya Equinox®.

Procedure

1. Log in to the Avaya Cloud account at https://accounts.zang.io.
2. (Optional) If you have not set up your company or want to configure a new company, do the following:
   a. Click on your user name in the top-right of the screen, and click **Add Company**.
   b. Type a name and description for your company.
   c. Click **Save**.
3. Click **Manage Companies**.
4. Click the **Domains** tab.
5. Click **Add Domain**.
6. Enter the work email's domain name when prompted.
7. Click **OK**.
8. To verify ownership of the domain, next to the domain name, click **Verify**.

   Avaya Cloud displays a verification code.
9. Copy the verification code and add it as a text record to the DNS entries on the domain's DNS server.
10. Click **Verify**.

Next steps

- Mapping your domain to the settings file URL on page 279

Related links

Configuring Outlook on the web without the Avaya IX Workplace Client on page 276

Mapping your domain to the settings file URL

About this task

Add the Equinox Cloud Client application to the company domain on https://accounts.zang.io and put the settings file URL in the public settings in the correct JSON format.

You can specify multiple systems in the network by adding multiple Profile_Name sections, one for each system that can be used for Avaya Equinox® registration. You can use this procedure while waiting for the company domain to be verified.

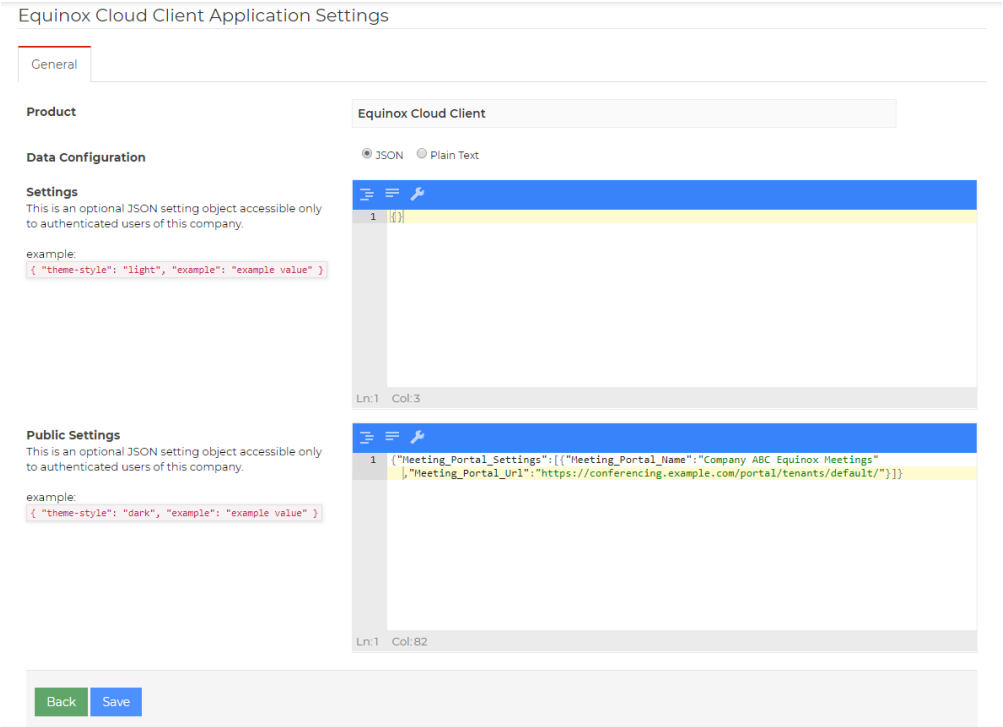
Before you begin

- Register an Avaya Cloud account.
- Set up a company domain in the Avaya Cloud account.

Procedure

1. Log in to your Avaya Cloud account.
2. Click **Manage Companies**.
3. Click the company name.
4. In the **Company Profile**, select the **Apps** tab on the ribbon.
5. Click **Configure New App**.
6. In the **Product** field, select **Equinox Cloud Client**.
7. Click **JSON**.
8. Configure the **Public Settings**.

```
{
  "Meeting_Portal_Settings": [
    {
      "Meeting_Portal_Name": "Enter any name you like.",
      "Meeting_Portal_Url": "https://conferencing.domain.com/portal"
    },
  ]
}
```



Related links

Configuring Outlook on the web without the Avaya IX Workplace Client on page 276

Configuring Equinox Streaming and Recording Server Meeting Properties in the User Portal

About this task

As part of scheduling meetings in the user portal, you can configure streaming and recording properties to override the default settings of the user profile. In addition, there are advanced streaming configurations that you can set up. For example, you can write a description of the meeting to help identify it in a search.

Important:

This procedure is relevant only for the Avaya Equinox® Streaming and Recording solution. For further information about the different Avaya Equinox® Streaming and Recording solutions, see Planning and configuring streaming and recording servers in Equinox Management on page 176.

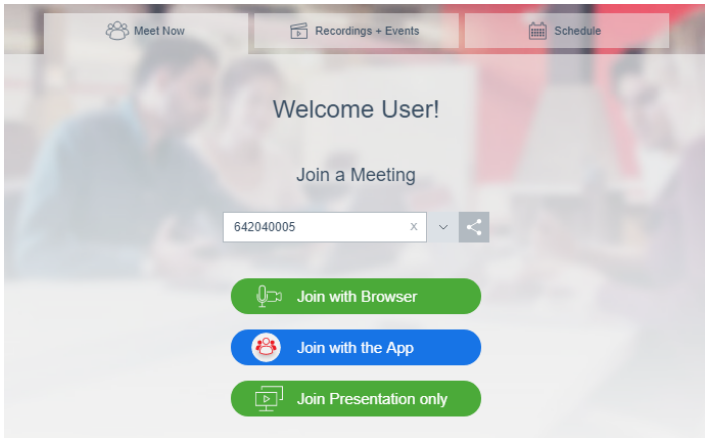
As a user, you can only schedule a videoconference if your administrator enabled this functionality in your user profile.

Before you begin

Define the core meeting parameters, including the list of participants, the date and time, and the virtual location of the meeting (see Scheduling your videoconference from the Equinox Management User Portal on page 267).

Procedure

1. As a user, access the Equinox Management user portal and click **Schedule**.



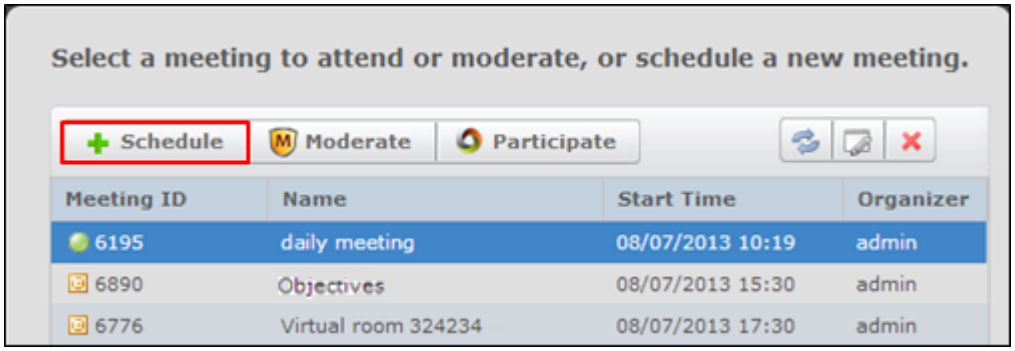
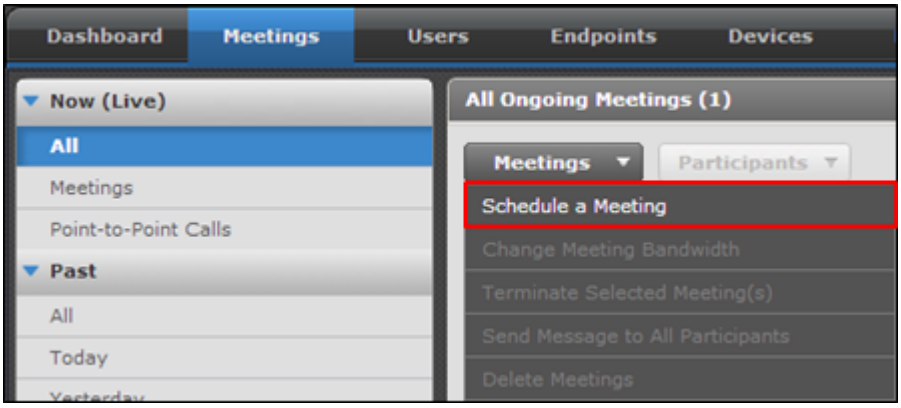


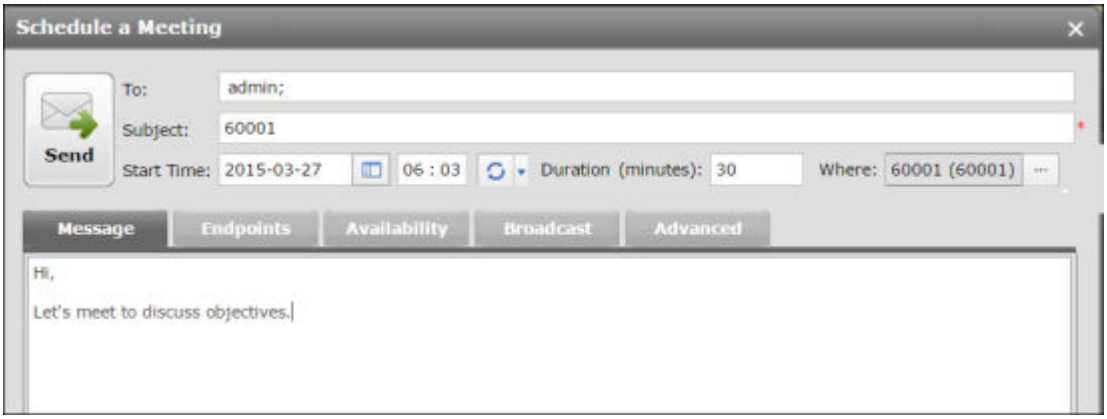
Figure 69: Access meeting scheduling from the Equinox Management user portal

Or

2. As an administrator, access the Equinox Management administrator portal and click **Meetings** > **Meetings** > **Meetings** > **Schedule a Meeting**.



Enter the meeting invitation details.



3. To configure recording this meeting without broadcasting, select the **Advanced** tab, and select the **Record the meeting** checkbox.

   To configure streaming for this meeting, select the **Broadcast** tab.

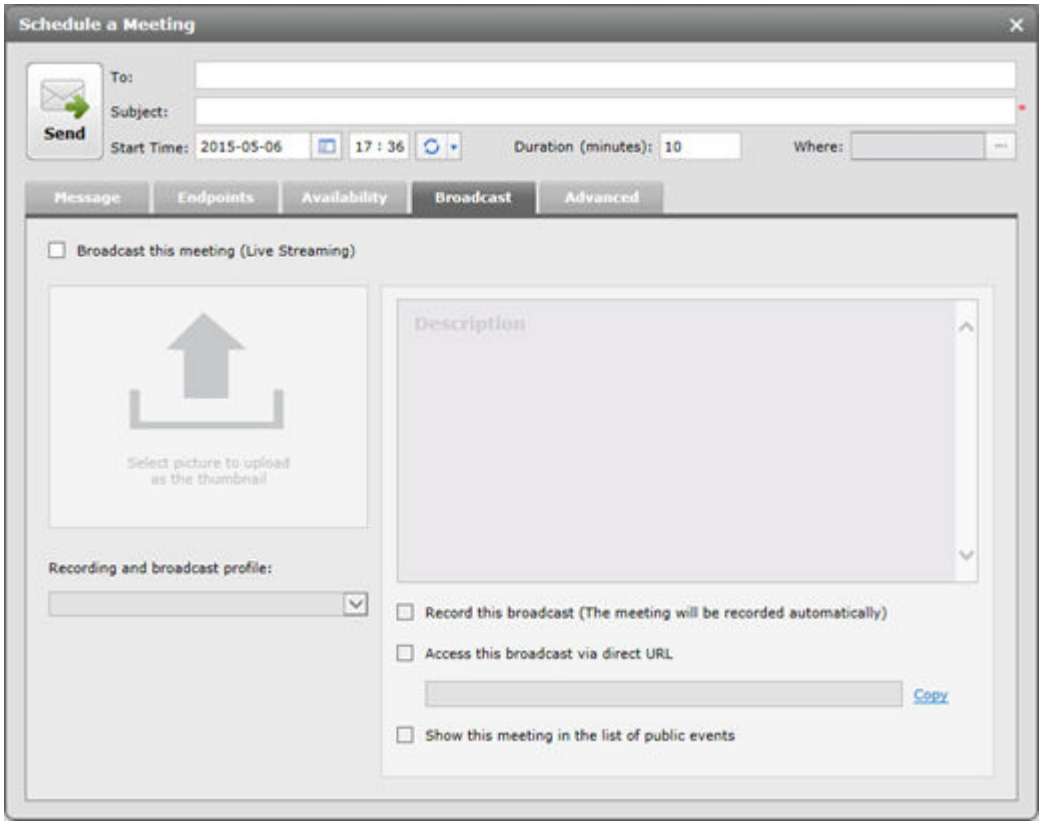


Figure 70: The Broadcast tab

Configure broadcast meeting properties, as described in Table 53: Broadcast meeting properties on page 283.

Table 53: Broadcast meeting properties

Field	Description
Broadcast this meeting (Live Streaming)	Select to automatically broadcast this meeting when it begins.
Select picture to upload as the thumbnail	Select a thumbnail for this broadcast.
Recording and broadcast profile	Select a profile for the broadcast.
Description	Enter a description for the meeting.
Record this broadcast	When you select **Broadcast this meeting**, the system automatically selects this check box to also record the meeting. You cannot select this option independently. To broadcast the meeting without recording it, deselect this check box. To record a meeting without broadcasting, select the **Advanced** tab, and select the **Record the meeting** check box.

Table continues…

Field	Description
Access this broadcast via direct URL	Select **Copy** to the right of the field, to generate a URL where you can view the broadcast. The URL appears in the field.

Related links

Scheduling your videoconference from the Equinox Management User Portal on page 267

Configuring Advanced Meeting Properties in the User Portal

About this task

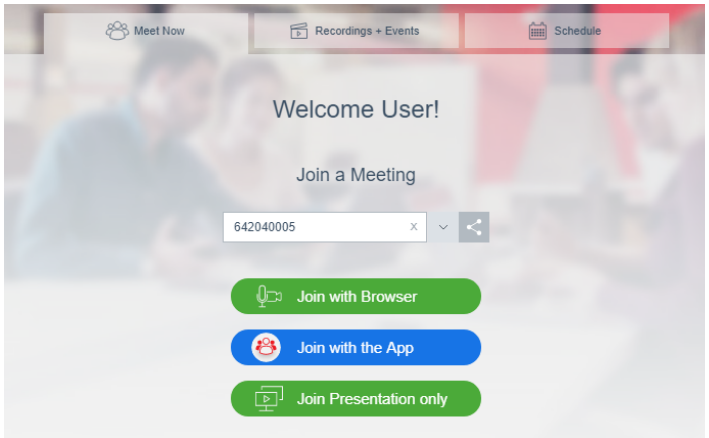
As part of scheduling meetings in the user portal to reserve video network resources, you can configure advanced properties to override the default settings of the virtual room, meeting type, or user profile.

Before you begin

Define the core meeting parameters including the list of participants, the date and time, and also the virtual location of the meeting (see Scheduling your videoconference from the Equinox Management User Portal on page 267).

Procedure

1. As a user, access the Equinox Management user portal and click **Schedule**.



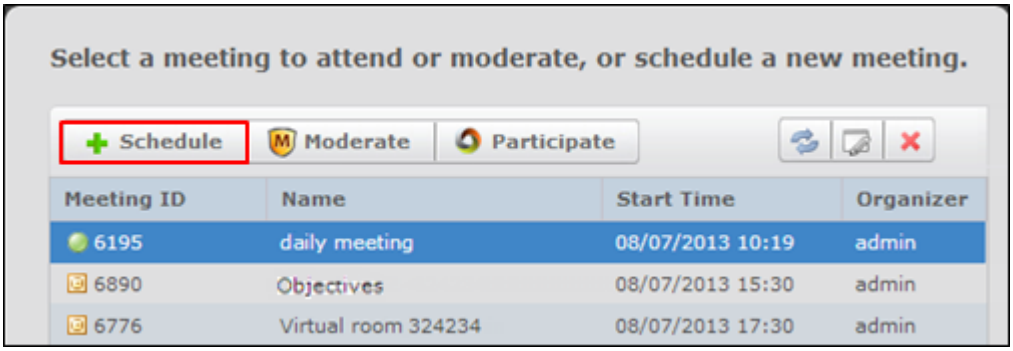
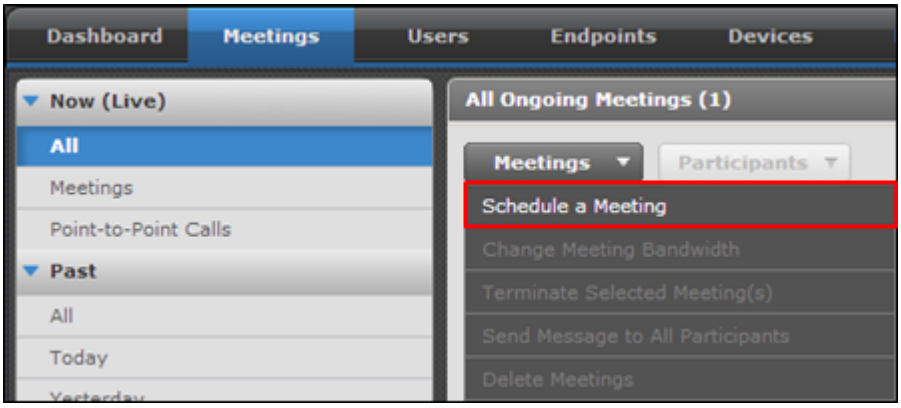


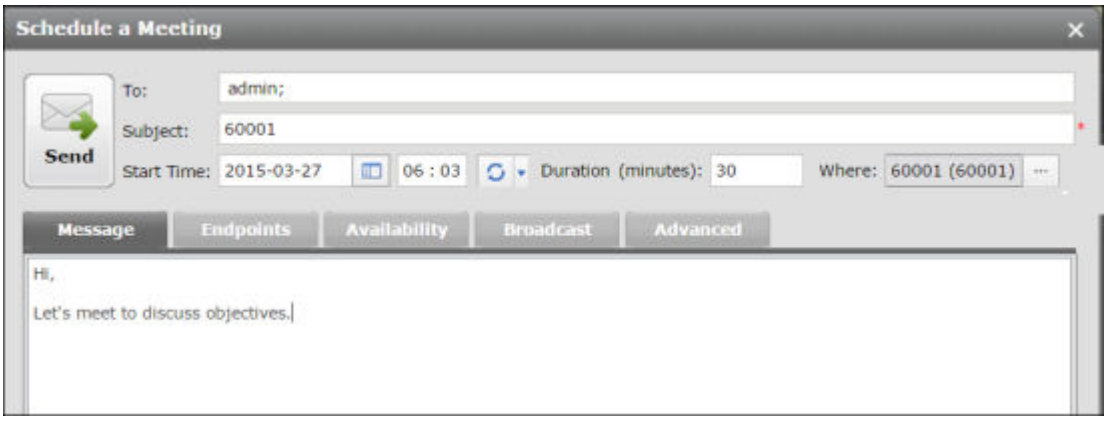
Figure 71: Access meeting scheduling from the Equinox Management user portal

Or

2. As an administrator, access the Equinox Management administrator portal and click **Meetings** > **Meetings** > **Meetings** > **Schedule a Meeting**.



Enter the meeting invitation details.



3. Select the **Advanced** tab.

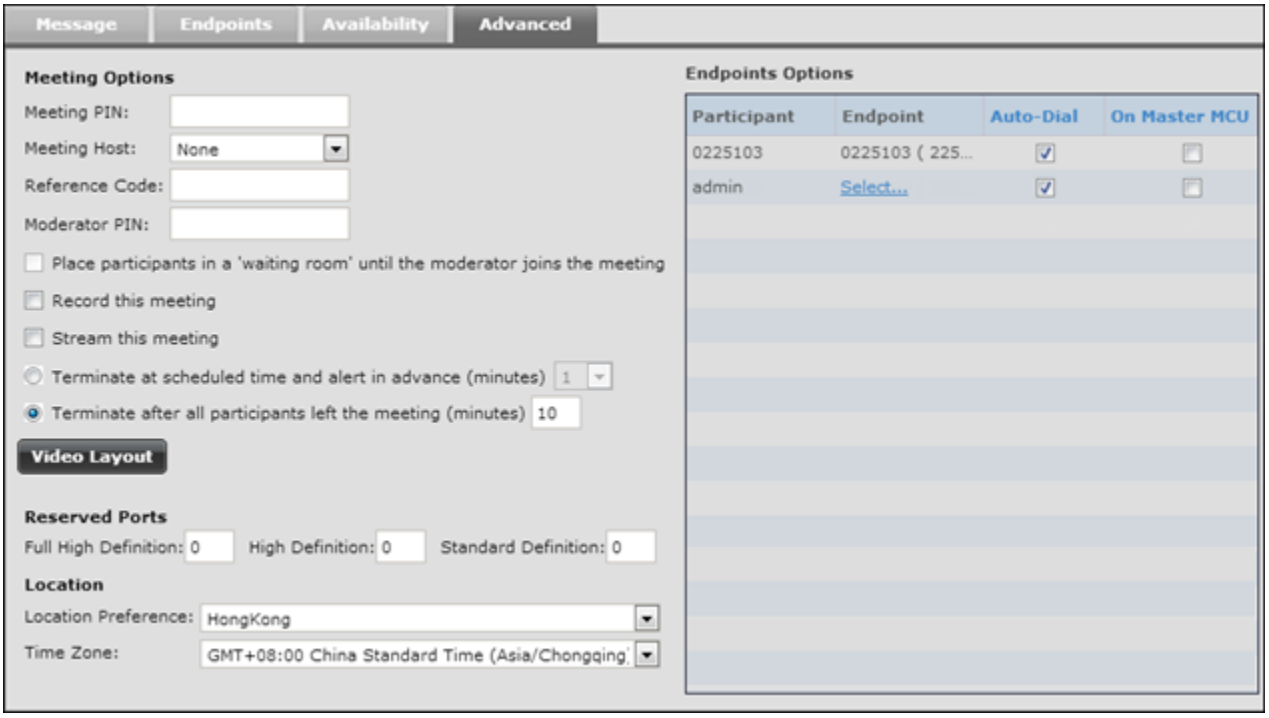


Figure 72: Defining advanced meeting properties

Configure advanced meeting properties, as described in Table 54: Advanced meeting properties on page 286.

Table 54: Advanced meeting properties

Field	Description
Meeting PIN	Enter a numeric-only PIN to require participants to enter this meeting using a password.
Meeting Host	Choose the moderator of the meeting from the list of participants. A moderator has special rights in a videoconference, including blocking the sound and video of other participants, inviting new participants, disconnecting others, determining video layouts, and closing meetings. From Equinox Management, moderators can perform these actions by accessing the In-Meeting Control interface. If configured, participants may be required to stay in the waiting room until the meeting's host joins.
Reference Code	Enter a billing code or other internal audit code if required.

Table continues…

Field	Description
Moderator PIN	If you want to protect the moderator function with a different password, enter a numeric PIN in the **Moderator PIN** field. A moderator PIN also allows you to place participants in a waiting room until the meeting host arrives. A moderator has special rights in a videoconference, including blocking the sound and video of other participants, inviting new participants, disconnecting others, determining video layouts, and closing meetings. A participant who enters the moderator PIN can also unlock the waiting room when joining the meeting.
Place participants in a 'waiting room' until the moderator joins the meeting	Select to place connected participants in a waiting room before the moderator joins the videoconference, where they cannot hear or see one another. The meeting begins when the moderator joins. To enable the waiting room, you must first define a Moderator PIN.
Record this meeting	Select to record the meeting. **Important:** If you are using the Avaya Equinox® Streaming and Recording solution and you have already configured the **Broadcast** tab to set up streaming and recording, this option is unavailable. For more information about the different Avaya Equinox® Streaming and Recording solutions, see Planning and configuring streaming and recording servers in Equinox Management on page 176.
Stream this meeting	Select to stream the meeting. This option is available only if you are using the Avaya Scopia® Recording and Streaming Content Center solution. If you are using the Avaya Equinox® Streaming and Recording solution, configure streaming options in the **Broadcast** tab. See Configuring Recording and Streaming Meeting Properties in the User Portal on page 280 for details about configuring the **Broadcast** tab. For more details about the different Avaya Equinox® Streaming and Recording solutions, see Planning and configuring streaming and recording servers in Equinox Management on page 176.
Terminate at scheduled time and alert in advance (minutes)	Select to end the meeting at the scheduled end time, such as if the same resources must be freed for another meeting. Enter the number of minutes warning required to notify participants that the meeting is due to end shortly.
Terminate after all participants left the meeting (minutes)	Select to keep the meeting open until all participants have left, and only then automatically close the meeting. Enter the number of minutes to wait before closing the meeting. If your administrator defined a maximum time for meetings, you cannot automatically extend Equinox Management meetings beyond this time.

Table continues…

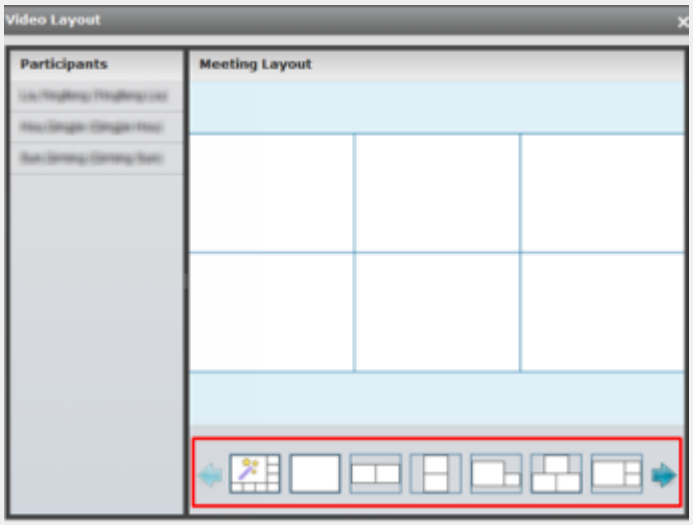
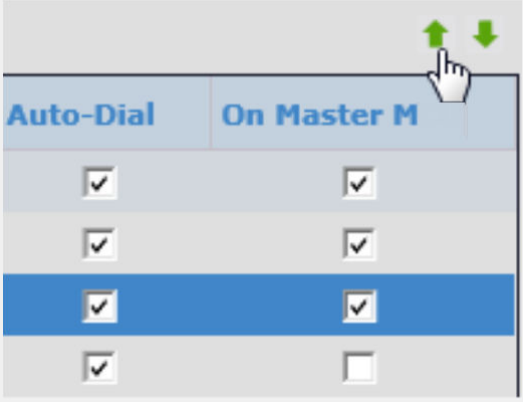
Field	Description
Video Layout	Select from the lower bar at the bottom of this pane to determine the initial video layout for endpoints to which the MCU dials out. A video layout is the arrangement of participant images as they appear on the monitor in a videoconference. If the meeting includes a presentation, a layout can also refer to the arrangement of the presentation image together with the meeting participants.  The default dynamic video layout automatically adjusts based on the number of participants in the meeting. To predetermine a fixed layout, choose one of the layouts in the lower bar. Verify that the meeting type (service) on the MCU is not dynamic. Dynamic layout conserves bandwidth, eliminates the display of empty frames in the video image, and makes optimal use of the video image display. Dynamic layout is especially suited to a meeting that has a high rate of participant traffic joining and exiting the meeting, or to an adaptive meeting type that has a variety of meeting sizes. To fix one endpoint's image in a specific subframe of the screen layout, drag and drop the participant name into the meeting layout.
Reserved Ports	Select to reserve more connections on the MCU for this call, such as if you might add more participants during the meeting. If a participant leaves a meeting before the end time is reached, Equinox Management releases the video ports used by the participant immediately. Enter the number of connections at the following video resolutions: • **Full High Definition** reserves connections at up to full HD 1080p. • **High Definition** reserves connections at up to 720p. • **Standard Definition** reserves connections at up to 352p.

Table continues…

Field	Description
Location Preference	In a distributed MCU deployment, select the preferred location of the MCU which would host this meeting. Choosing a specific MCU location limits the availability of MCU connections to just this device. If you select **Auto**, Equinox Management knows the endpoints' location and can therefore automatically select the MCU closest to the endpoints. For example, if only one endpoint in the meeting is in Europe while the remainder are in the Far East, Equinox Management selects an MCU located in the Far East. We strongly recommend selecting **Auto** to let the system choose the optimal settings matching your organization's bandwidth policies. This ensures efficient bandwidth use and maximum quality for the videoconference.
Time Zone	Select a time zone for your meeting if it extends beyond one time zone. The start time of the meeting is expressed in the time zone selected here.
Endpoint	Select a dedicated video endpoint for each participant. The XT Series includes calendar functionality which warns users when a scheduled meeting is about to start. It also offers a simple way to join a scheduled meeting by selecting **Join** on the reserved endpoint.
Auto-Dial	Select to instruct the MCU to automatically dial this endpoint at the start of the meeting. Depending on the settings of the endpoint, it would either ring or join automatically.

Table continues…

Field	Description
On Master Equinox Media Server	Select to determine that this endpoint connects only to the master Equinox Media Server for a higher quality experience in cascaded meetings. If Equinox Management cascades this meeting across multiple media servers to reduce bandwidth costs, the meeting would be hosted by a master media server with one or more slave media servers. Endpoints connected to a master media server have their video viewed by all participants, while from the slave media server, only the active speaker is displayed. You can allocate a higher priority to an endpoint to increase its likelihood of connecting to the master media server using the green arrows above the endpoint list. The arrows appear after you select an endpoint to connect to the master media server.  **Figure 73: Prioritizing endpoints' connections to the master media server**

Related links

Scheduling your videoconference from the Equinox Management User Portal on page 267

Chapter 7: Real-time Monitoring

Equinox Management keeps network administrators informed about events related to video devices that are part of the Equinox Solution deployment.

All video devices that are managed by Equinox Management communicate by sending SNMP traps or XML messages to it. Equinox Management analyzes received information and generates its own messages that allow you to monitor and troubleshoot your videoconferencing deployment:

- **Alarms** require immediate attention, notifying about the video device's abnormal behavior. These could be hardware, software, or environmental problems that affect system operation and require the administrator's intervention. Equinox Management clears an alarm automatically when the problem causing it is solved and the alarm is no longer relevant.
- **Events** reflect past alarms and information about general change in a video device's behavior or status. No immediate action is necessary.

For example, if a video device is reported offline, Equinox Management generates an alarm. After you troubleshoot this video device, the alarm is cleared and an event is generated notifying you that the device is online. The event history shows two events: one recording the alarm and one recording its clearance.

Figure 74: The flow of generating alarms and events in Equinox Management

Both alarms and events are grouped according to their level of severity, which you can customize to better serve the needs of your deployment. For details, see Changing the Severity Level of Alarms on page 300.

Alongside the events and alarms, Equinox Management displays some of the SNMP trap messages from video devices in their original format.

Important:

You can forward SNMP trap messages to a central SNMP trap server, as described in Forwarding traps to a third-party trap server on page 294.

In addition to displaying messages for real-time monitoring, Equinox Management provides the following tools for notifying administrators about alarms and events in your deployment:

- Generating log files
- Sending email alerts

Related links

Managing Alarm Notifications on page 292
Monitoring Network Devices via Equinox Management on page 297
Monitoring Meetings and Calls on page 301
Adding a support email address to Avaya Equinox® Meetings for Web on page 310

Managing Alarm Notifications

These topics explain how to configure the tools Equinox Management provides to notify the network administrator of alarms and events that require troubleshooting.

Related links

Real-time Monitoring on page 291
Configuring the Log Level on page 292
Sending Trap Messages on page 294
Sending Email Alerts on page 295

Configuring the Log Level

About this task

Equinox Management is configured to automatically create logs to help maintain your deployment and troubleshoot problems.

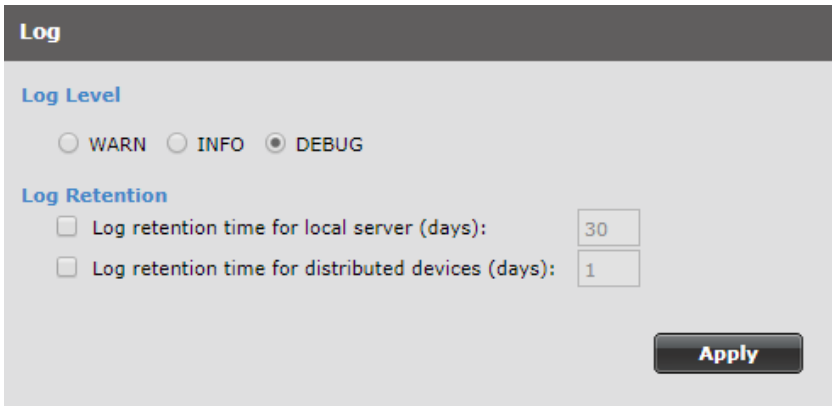
You can select three levels of details for a log file. Storing more details will obviously increase the size of the log file.

Equinox Management supports log retention for:

- Avaya Equinox® Management
- Equinox Conference Control (UCCS)
- Equinox H.323 Gatekeeper
- Equinox Media Servers
- H.323 Edge
- SIP B2BUA
- Web Gateway (Gateways)

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Maintenance** > **Log Level**.



3. Select the required level of details for the log files:

Table 55: Log levels

Field Name	Description
WARN	Provides indications on unexpected issues. Service is still provided.
INFO	Includes general information.
DEBUG	Provides detailed information required for troubleshooting.

4. Configure the following log retention fields:

Field Name	Description
Log retention time for local server (days)	Select or clear the check box to enable or disable log retention for the local server. Log retention on the local server includes: • All-in-1 Equinox Conference Control (UCCS) • All-in-1 H.323 Gatekeeper • All-in-1 Web Gateway (Gateways) in OTT • Avaya Equinox® Management • SIP B2BUA **Range**: 1 – 365 days **Recommended value**: 30 days
Log retention time for distributed devices (days)	Select or clear the check box to enable or disable log retention for distributed devices. Log retention on distributed devices includes: • Distributed Equinox Conference Control (UCCS) • Distributed H.323 Gatekeeper • Distributed Web Gateway (Gateways) in OTT • Equinox Media Servers • H.323 Edge **Range**: 1 – 365 days **Recommended value**: 30 days

5. Click **Apply**.

Related links

Managing Alarm Notifications on page 292

Sending Trap Messages

You can configure Equinox Management to forward all traps received from managed video devices to another trap server. These include Equinox Management self-generated traps, such as the one resulting from MCU port usage exceeding the configured threshold.

Related links

Managing Alarm Notifications on page 292
Forwarding traps to a third-party trap server on page 294
Removing Trap Forwarding to a Third-party Trap Server on page 295

Forwarding traps to a third-party trap server

About this task

You can forward traps received by Equinox Management to one or more third party trap servers.

You first must configure the trap server in Equinox Management by providing the trap server's IP address and SNMP port (usually, port 162).

You then need to set the alarm threshold of an event that, when reached, causes Equinox Management to send a trap to the configured trap server(s).

For more information on alarms, events, and traps, see Real-time Monitoring on page 291.

Procedure

1. Log in to the Equinox Management administrator portal.
2. Click **Settings** > **Alarm** > **Trap Servers**.
3. Do one of the following:
   - To add a trap server, click **Add**.
   - To modify the settings of an existing trap server, select the IP address of the relevant trap server.
4. Specify the IP address and port number of the trap server to which Equinox Management forwards traps received from managed elements.
5. Click **OK** to save your settings.
6. Enter the threshold value in percent for port usage in these devices:
   - MCU
   - Gateways

Related links

Sending Trap Messages on page 294

Removing Trap Forwarding to a Third-party Trap Server

About this task

You can remove a trap server that is no longer used. Deleted trap servers are removed from the database.

For more information on alarms, events, and traps, see Real-time Monitoring on page 291.

Procedure

1. Log in to the Equinox Management administrator portal.
2. Select **Settings** > **Alarm** > **Trap Servers** in the sidebar menu.
3. Select the specific trap server.
4. Select **Delete**.
5. Select **Yes** at the prompt.

   The trap server is removed from the database.

Related links

Sending Trap Messages on page 294

Sending Email Alerts

You can configure Equinox Management to send emails to specific users, with notifications of alarms registered by the system. You can also define the minimum severity level for sending alarms. For example, you can define that notifications are sent only for critical alarms.

Related links

Managing Alarm Notifications on page 292
Creating or Modifying an Alert Recipient Profile on page 295
Removing an Alert Recipient Profile on page 296

Creating or Modifying an Alert Recipient Profile

About this task

You can define a recipient for email notifications sent by Equinox Management regarding traps.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Settings** > **Alarm** > **Alert Recipients** in the sidebar menu.
3. Do one of the following:
   - To create a new alert recipient profile, select **Add**.
   - To modify an existing alert recipient profile, select the relevant **Recipient Name**.
4. Configure the alert recipient profile as follows:

Field Name	Description
Recipient Name	Enter the name of the alert recipient.
Email Address	Enter the email address of the alert recipient.
Minimum Severity	Select the minimum severity level of alerts to be sent to the alert recipient. The corresponding **Alarm Threshold** field in the **Alert Recipients** list indicates the selected severity level.
Notify on alarms clearing	When selected, enables alerting the email recipient that alarms have been cleared. The corresponding **Cleared** field in the **Alert Recipients** list is set to **yes**.
Use custom subject line	To include a custom subject line in the email, select this field and enter a string for the custom subject line in the relevant field.
Include element info	When selected, adds details of the elements reported in the alerts in the custom subject line.
Custom subject line	To include a custom subject line in the email, first select **Use custom subject line** and then enter a string for the custom subject line in the relevant field.

5. Select **OK** to save your settings.

Related links

Sending Email Alerts on page 295

Removing an Alert Recipient Profile

About this task

You can remove a recipient defined to receive notifications about traps.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Settings** > **Alarm** > **Alert Recipients** in the sidebar menu.
3. Select the check box next to the alert recipient you want to delete.
4. Select **Delete**.

   The alert recipient profile is removed from the database.

Related links

Sending Email Alerts on page 295

Monitoring Network Devices via Equinox Management

You can use Equinox Management to monitor the functionality of devices, alarms and events, within your network, and to monitor bandwidth usage and port availability for the videoconferencing network resources. You can monitor your video network devices, including endpoints, in the following ways:

- Recent critical alarms regarding devices

  The most recent and critical events and alarms are displayed on the **Dashboard** tab, which appears when you first access Equinox Management.

Figure 75: Messages area of the Dashboard tab

  - Select the **Messages** link to view the complete alarm list.
  - Select the ✕ icon to hide an alarm from the dashboard.

- All alarms and events for the system

  You can view all events and alarms in the system from the **Logs & Events** tab.

- Alarms and events per device

  You can monitor the status of video network devices from the **Devices** and **Endpoints** tabs. The device status is indicated by an icon, as described below:

  - Online

    The device is online and operating normally. You can use this device to schedule meetings.

  - Online with an alarm

    The device is online, but a critical error occurred, such as device failure. Navigate to the list of alarms for more information about the alarm and what to do.

  - In a call (for endpoints only)

    The device is in a call and cannot be used for ad-hoc meetings.

  - In Maintenance

    The device is not online, typically while being upgraded. You cannot use this device to schedule meetings.

- Offline

  The device is offline. You cannot use this device to schedule meetings.

A list of alarms and events is displayed in the device's profile.

Related links

Real-time Monitoring on page 291
About Management Status of Network Devices on page 298
Monitoring Network Events and Alarms on page 299
Changing the Severity Level of Alarms on page 300

About Management Status of Network Devices

Video network devices managed by Equinox Management can send alarms and events to Equinox Management for monitoring purposes. You can view events, alarms, and network status information for your video network devices in the **Endpoints** and **Devices** tabs. The following video network devices are managed by Equinox Management:

- Avaya gatekeepers
- Avaya MCUs
- Avaya gateways
- Avaya Equinox® H.323 Edge server
- Endpoints

  You can manually configure Equinox Management to manage XT Series and Avaya IX™ CU360. For more information about managing endpoints, see Managing endpoints using Equinox Management on page 141.

All network status information is updated in real time by the Avaya Equinox® Management database.

There are two types of network devices management status:

- **Managed**

  The device exists in the Avaya Equinox® Management database and provides monitoring information and access to configuration settings.

- **Not managed**

  The device exists in the Avaya Equinox® Management database but has no open communication channels with Avaya Equinox® Management and provides no monitoring information or access to configuration settings.

Related links

Monitoring Network Devices via Equinox Management on page 297

Monitoring Network Events and Alarms

About this task

You can monitor events and alarms reported by the system for the entire network and for specific network devices. You can sort the list of events or alarms according to severity, time, message and device, and filter traps by severity and time interval. See Real-time Monitoring on page 291 for an explanation of alarms and events.

This procedure describes how to view all network events and alarms, or monitor a specific device, including endpoints.

Procedure

1. Access the Equinox Management administrator portal.
2. You can monitor alarms or events for a specific device, or on a network level, as follows:
   - To monitor a specific device, select the video network device from the **Devices** or **Endpoints** tab, and then select the **Events** or **Alarms** tab to view messages about the device.
   - To view the most recent and critical alarms in the network by navigating to the **Messages** area of the **Dashboard** tab (see Figure 76: Messages area on page 299).

Figure 76: Messages area

   - To hide a message from the **Message** area of the Dashboard, select ☒.

     This message still appears on the **Logs & Events** tab.
   - To view detailed information about all network events, select **Messages** or the **Logs & Events** tab, which displays the following information:
     - **Severity**

       Event or alarm severity level (Cleared, Information, Warning, Critical).
     - **Device Name**

       The name of the device that coursed the event.
     - **Time**

       Date and time the event or alarm was generated.

- **Message**

  Event or alarm description.

Note:

Select the column headings in the table to sort the information displayed.

Related links

Monitoring Network Devices via Equinox Management on page 297

Changing the Severity Level of Alarms

About this task

You can modify the severity level of alarms generated by the system, and create events for a specific alarm.

Important:

You can disable all Equinox Management alarms before performing selected maintenance procedures, such as upgrading endpoints, to ensure you do not generate hundreds of irrelevant alarms. You can mute Equinox Management's alarms by selecting **Settings** > **Alarm** > **Alarms** > **Disable All Alarms** in the Equinox Management administrator portal.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Settings** > **Alarm** > **Alarms**.
3. Select the alarm whose severity you want to change from the list.

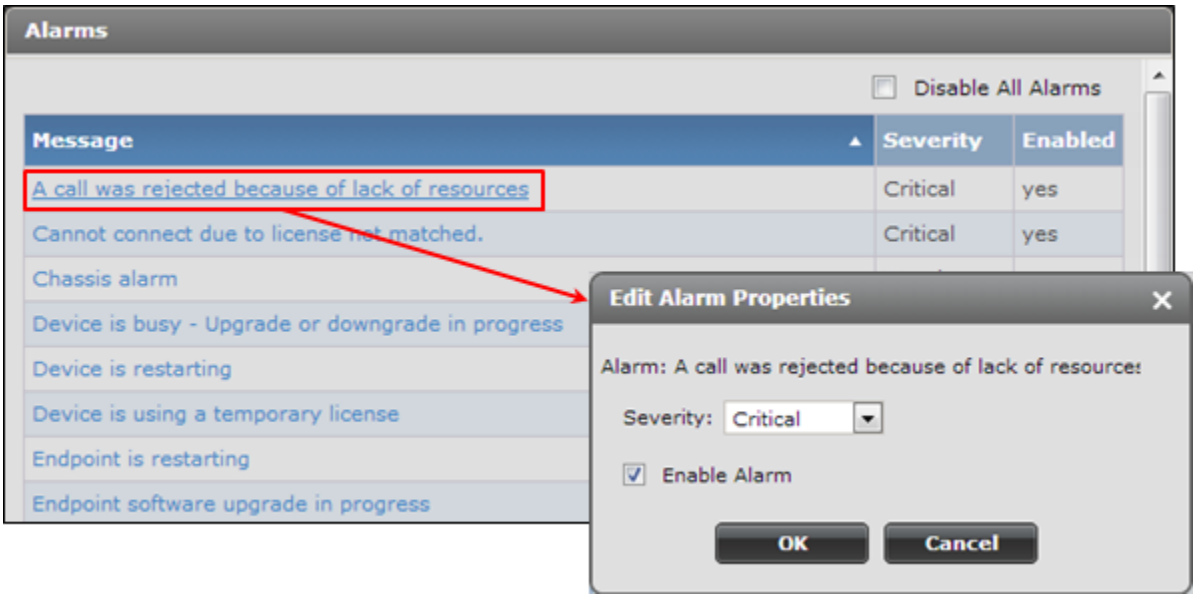


Figure 77: Changing the severity level of an alarm

4. Modify the severity level from the **Severity** list, as needed.
5. If necessary, you can disable the alarm altogether by clearing the **Enable Alarm** check box.
6. Select **OK** to save your changes.

Related links

Monitoring Network Devices via Equinox Management on page 297

Monitoring Meetings and Calls

You can monitor ongoing meetings and upcoming meetings scheduled in your videoconferencing network. In addition, you can monitor system utilization status.

You can view general information regarding the overall bandwidth and device usage, and bandwidth for all current and past meetings. For a detailed, graphical presentation of meeting and call data, generate a report as described in Generating a report on page 369.

Related links

Real-time Monitoring on page 291
Monitoring Ongoing Meetings or Calls on page 301
Monitoring Meeting Events on page 303
Monitoring Bandwidth and Port Utilization on page 306
Downgrading the Meeting Bandwidth on page 307
Checking the Status of Meetings on page 308
Inviting Endpoints to Join Meetings on page 309
Disconnecting Calls or Meetings on page 310

Monitoring Ongoing Meetings or Calls

About this task

You can view and monitor all meetings and calls scheduled in the system by:

- Monitoring bandwidth and port utilization to make sure values do not exceed the limits set for the videoconference
- Becoming a moderator. For more details about moderators, refer to *User Guide for Avaya Equinox® Management*.
- Terminating meetings
- Viewing detailed information regarding meetings and calls as a report, as described in Generating a report on page 369.
- Viewing meeting details, such as the meeting ID or hosting media server, by clicking the meeting link.

Procedure

1. Access the Equinox Management administrator portal.
2. Select the **Meetings** tab.

   Or

   Select the link in the **Calls and meetings in progress** section, as shown in Figure 78: Displaying meetings in progress from the Dashboard tab on page 302.

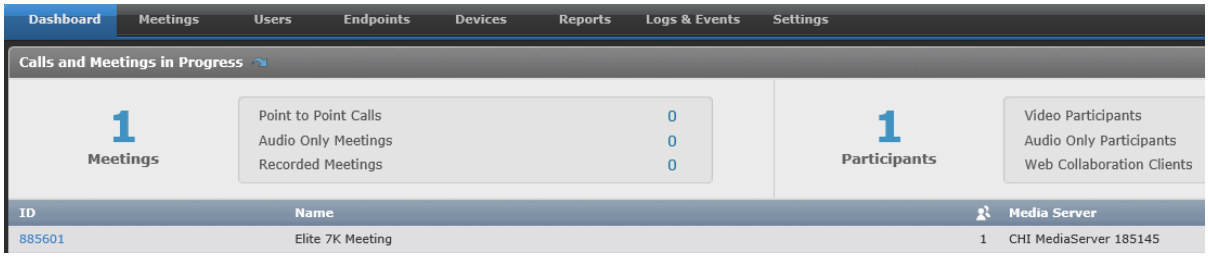


Figure 78: Displaying meetings in progress from the Dashboard tab

The **Meetings** tab opens, showing all ongoing meetings. See Figure 79: Ongoing meetings displayed on the Meetings tab on page 302.

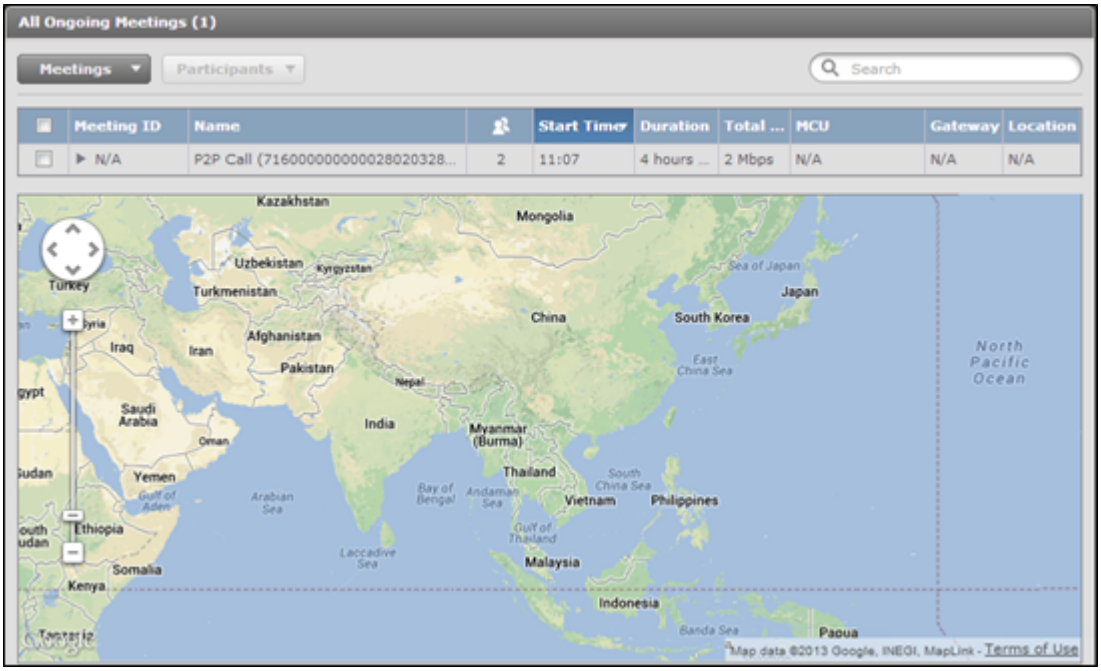


Figure 79: Ongoing meetings displayed on the Meetings tab

3. Select the meeting or call you want to monitor.

   Use the **Search** field to quickly search by the meeting ID, meeting name, endpoint number or endpoint name.

Use the **Advanced Search** feature to search by the meeting type or time when the meeting started or ended. This feature appears only after entering data in the **Search** field. See Figure 80: Using the Search feature on the Meetings tab on page 303.

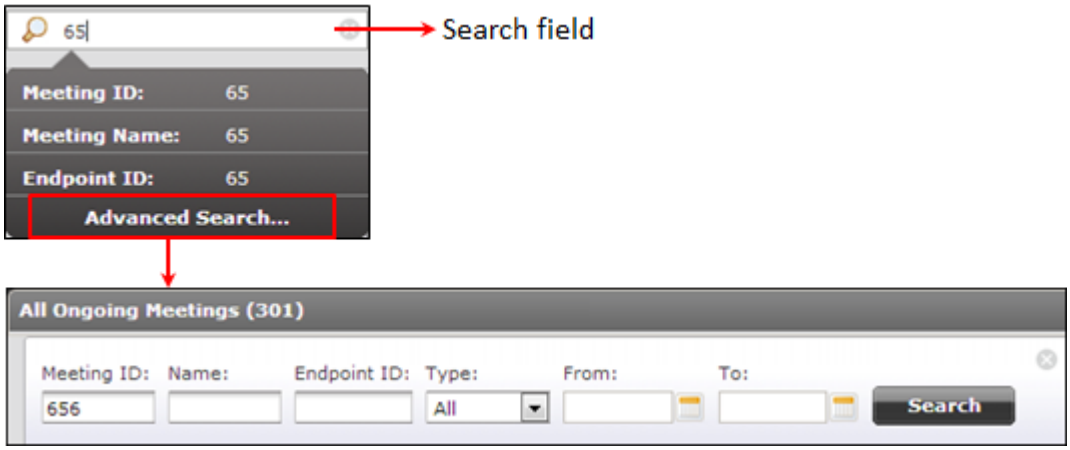


Figure 80: Using the Search feature on the Meetings tab

All host media servers are listed in the **Media Server** column, with an indication of whether the meeting is cascaded.

All gateways are listed in the **Gateway** column.

4. Select **Moderate**.

   The In-meeting Control interface is not available for meetings or calls in which you are not a participant or the organizer.

5. Enter the moderator PIN if one is used for this meeting or call.

Related links

Monitoring Meetings and Calls on page 301

Monitoring Meeting Events

About this task

You can view an event timeline for a meeting that has concluded, to help troubleshoot events of the meeting. You can view information such as which users joined and left the meeting, network issues that occurred, and users which experienced errors during the meeting. You can export text files for the timeline of events and for individual meetings.

Procedure

1. Access the Equinox Management administrator portal.
2. Select the **Meetings** tab. The **All Ongoing Meetings** page appears.
3. To monitor meeting events for past meetings, select **Past > All** from the facets on the left side of the page. The list of previous meetings appears on the **Past Meetings** page.

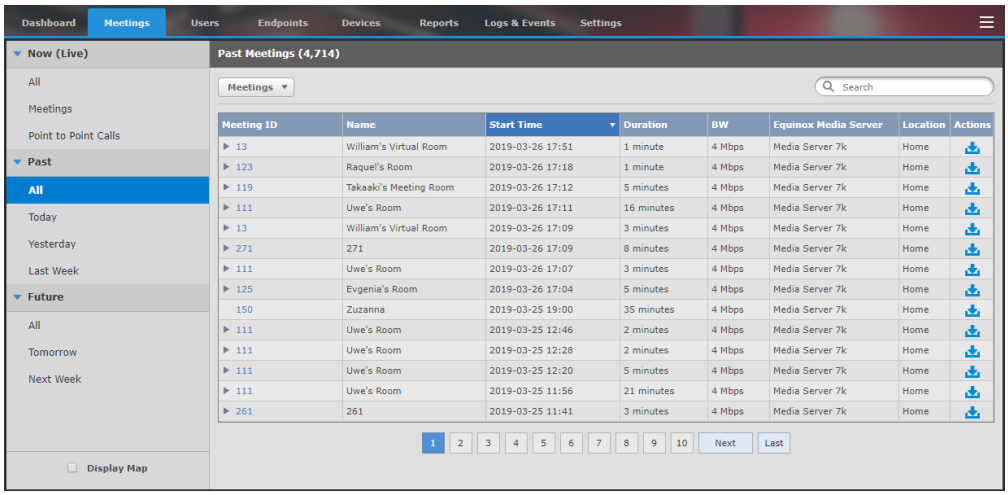


Figure 81: Past Meetings Page

4. Optionally, select the **Display Map** check box to display a map indicating meeting locations. To hide the map, clear the check box.
5. To export a meeting in .xlsx CSV format, click the **Actions** icon for the respective meeting.
6. In the **Meeting ID** column of either the **All Ongoing Meetings** page or the **Past Meetings** page, select the meeting you want to monitor. The **Meeting ID:** page for the specified meeting opens, displaying the **Timeline** tab.

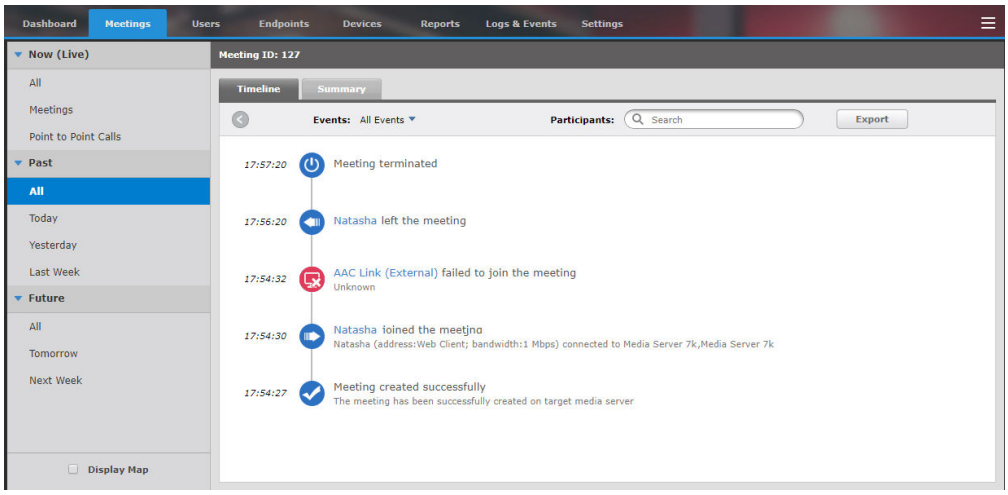


Figure 82: Meeting ID Page — Timeline Tab

The meeting events proceed chronologically from the bottom of the page to the top.

7. You can perform the following actions on this page:
   - Select the arrow next to **Events:** to filter the events displayed on the timeline.

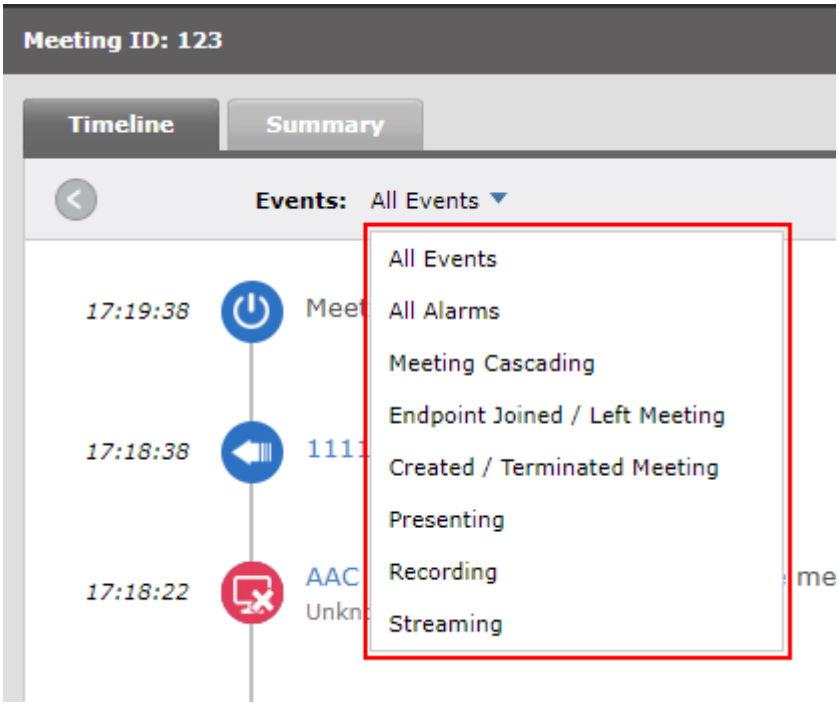


Figure 83: Filtering Meeting Events

- Enter a participant name in the **Participants:** field to filter the participants displayed on the timeline.
- Click **Export** to export the timeline in text format.

8. Select the **Summary** tab to view a summary of the meeting.

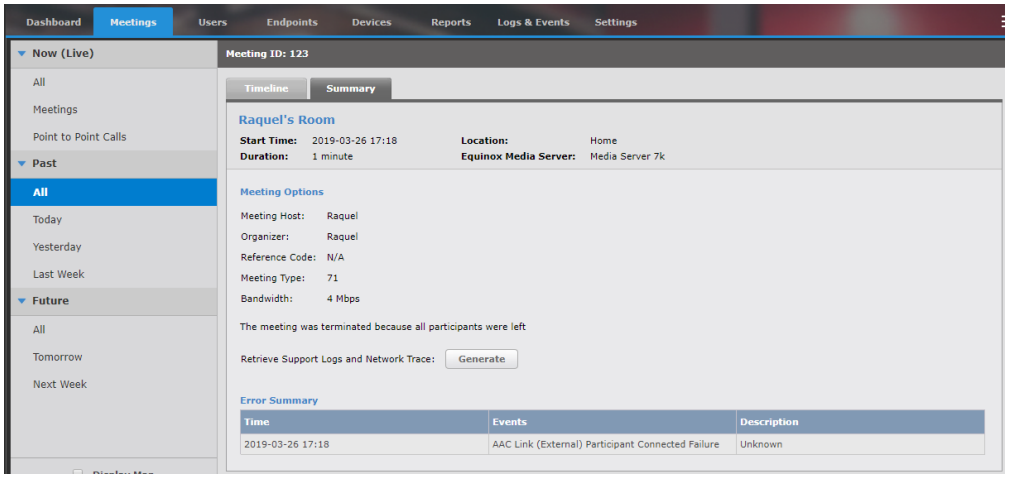


Figure 84: Meeting ID Page — Summary Tab

Related links

Monitoring Meetings and Calls on page 301

Monitoring Bandwidth and Port Utilization

About this task

You can monitor port and bandwidth utilization for MCUs and Gateways configured in the system, to ensure that video traffic does not exceed the maximum utilization defined for the devices. Monitoring includes the following:

- Viewing the overall bandwidth and device usage.
- Viewing the bandwidth for all current and past meetings.
- Viewing detailed information regarding bandwidth and port utilization as a report, as described in Generating a report on page 369.

Procedure

1. Access the Equinox Management administrator portal.

   Overall status for bandwidth and device usage appears in the **Information** area of the **Dashboard** tab (Figure 85: Bandwidth and Port Utilization on page 306).

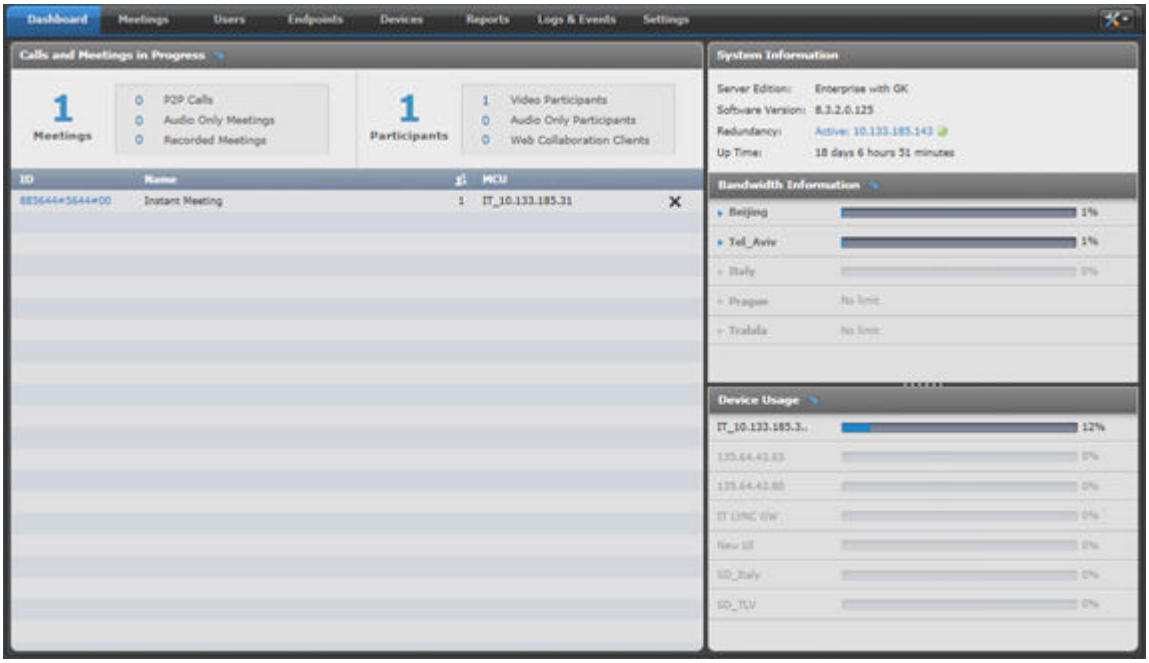


Figure 85: Bandwidth and Port Utilization

2. To view bandwidth utilization per meeting, select the **Meetings** tab.

   The bandwidth for each meeting is displays in the **Total BW** column.

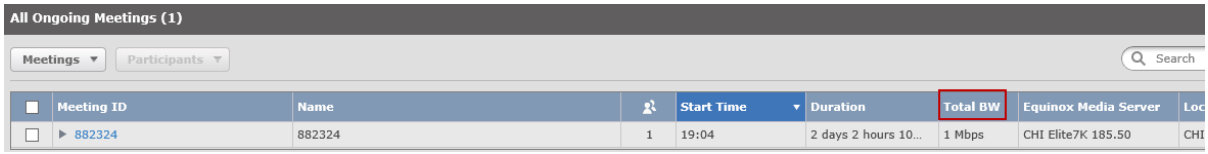


Figure 86: All Ongoing Meetings Page — Bandwidth Utilization

Related links

Monitoring Meetings and Calls on page 301

Downgrading the Meeting Bandwidth

About this task

You can downgrade the bandwidth for current meetings if, for example, the bandwidth is exceeded, or you want more bandwidth available for another meeting occurring at the same time. If you downgrade the bandwidth for a meeting, all participants are downgraded to the same bandwidth.

Procedure

1. Access the Equinox Management administrator portal.

   The Dashboard tab appears.

2. Select the meeting for which you want to downgrade bandwidth in the **Bandwidth Information** section of the **Dashboard** tab as shown in Figure 87: Locating the Bandwidth Information section of the Dashboard tab on page 307.

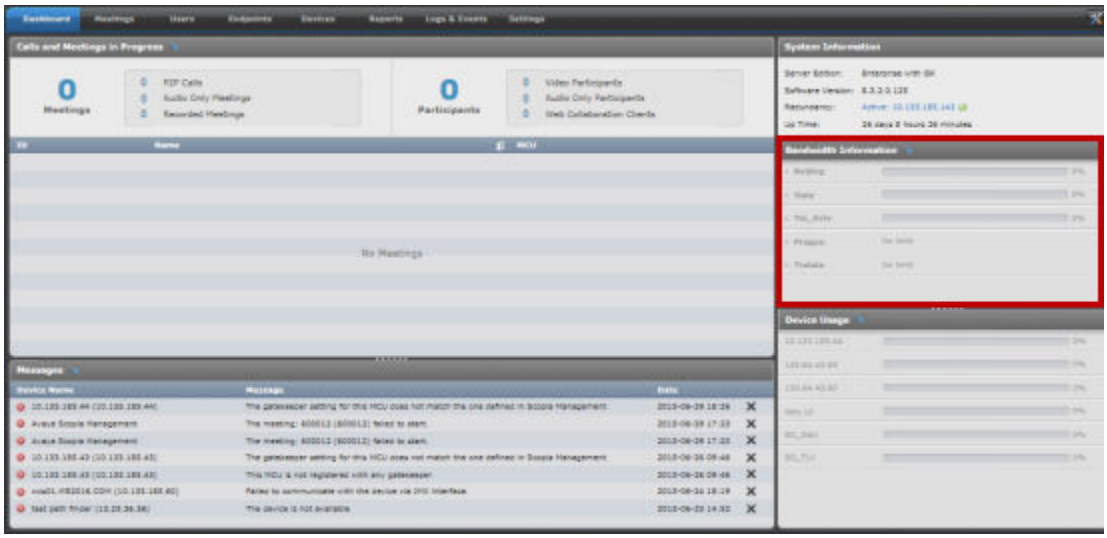


Figure 87: Locating the Bandwidth Information section of the Dashboard tab

3. Select the **Actions** button and then select **Change Meeting Bandwidth**. See Figure 88: Downgrading the meeting bandwidth from the Dashboard tab. on page 308

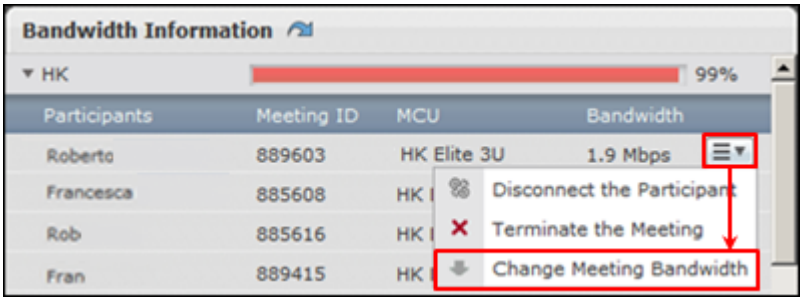


Figure 88: Downgrading the meeting bandwidth from the Dashboard tab.

The **Select Meeting Bandwidth** window appears.

4. Select the new meeting bandwidth.
5. Select **OK**.

Related links

Monitoring Meetings and Calls on page 301

Checking the Status of Meetings

About this task

You can monitor the status of ongoing and upcoming meetings, and view the reason for a failure status.

Procedure

1. Access the Equinox Management administrator portal.
2. Select the **Meetings** tab.

   A list of all ongoing meetings appears.

   If a meeting failed to create, for example, because of an MCU failure, the icon appears next to the **Meeting ID**.

   If meeting creation fails due to device failure, Equinox Management attempts to recreate the meeting whenever it receives a dial-in call from a meeting participant. This allows the system multiple attempts at creating the meeting after the initial failure.
3. Select **Meetings** or **Point-to-Point calls** to filter the results for ongoing meetings.
4. Select **Future** > **All** to see all meetings that have not yet started.

Related links

Monitoring Meetings and Calls on page 301

Inviting Endpoints to Join Meetings

About this task

You can invite participants (endpoints) to join a scheduled conference, on the **All Ongoing Meetings** page (**Meetings > Meeting list table**), without having to open a new window.

Procedure

1. Access the Equinox Management administration portal.
2. Select the **Meetings** tab. The **All Ongoing Meetings** page opens, displaying all meetings currently in session.

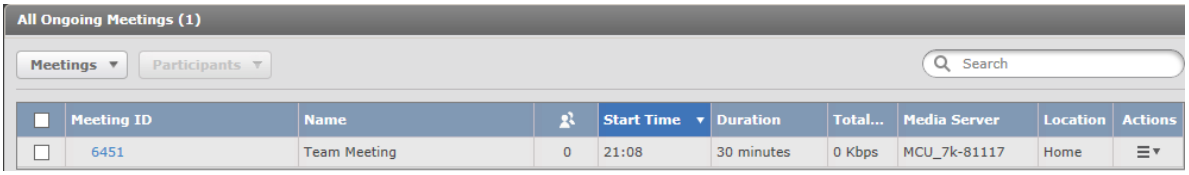


Figure 89: All Ongoing Meetings Page

3. Select the icon in the **Actions** column and select **Quick Invite**. The **Quick Invite** dialog box opens.

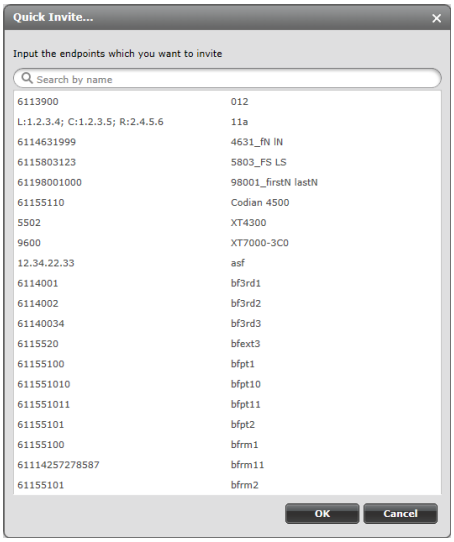


Figure 90: Quick Invite Dialog Box

4. Enter the endpoints you want to invite in the search field, and select **OK**.

   The endpoint is added to the meeting.

Related links

Monitoring Meetings and Calls on page 301

Disconnecting Calls or Meetings

About this task

You can disconnect ongoing calls or meetings when a threshold is exceeded, such as when the duration of the call exceeds the configured limits, or when the bandwidth used for that meeting or call exceeds the maximum bandwidth.

Procedure

1. Access the Equinox Management administrator portal.
2. If the meeting you want to disconnect appears in the **Calls and meetings in progress** section of the **Dashboard** tab, select the ✕ icon, as shown in Figure 91: Disconnecting a meeting from the Dashboard tab on page 310.

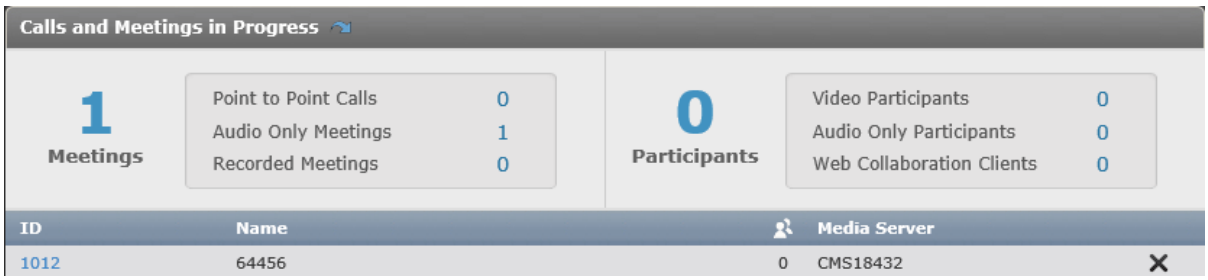


Figure 91: Disconnecting a meeting from the Dashboard tab

3. If the meeting you want to disconnect does not appear on the **Dashboard** tab, select the **Meetings** tab.
4. Select the meeting or call you want to disconnect.
5. Select **Meetings** > **Terminate Selected Meeting(s)**.

Related links

Monitoring Meetings and Calls on page 301

Adding a support email address to Avaya Equinox® Meetings for Web

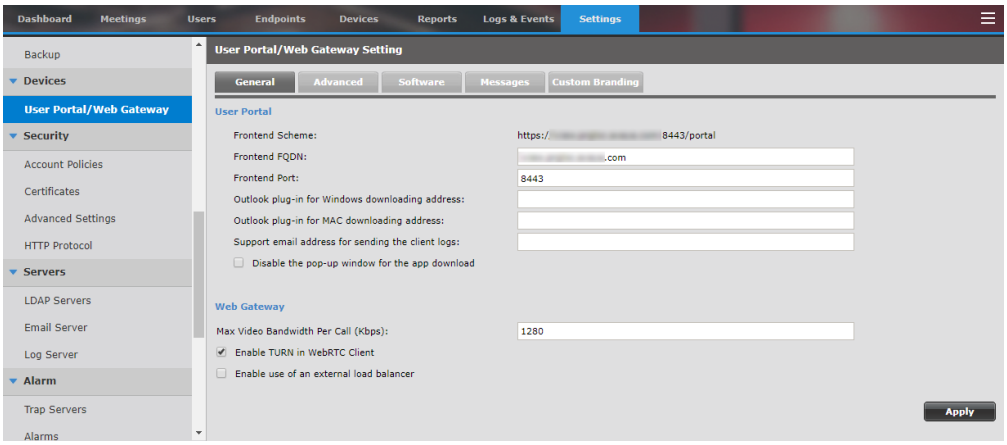
About this task

This feature enables you to set a support email address for the Avaya Equinox® Meetings for Web user to email the log to the support team. The default is empty.

Procedure

1. Click **Settings**.
2. For Avaya Equinox® for Team Engagement click **User Portal.**

3. For Avaya Equinox® for Over The Top click **User Portal/Web Gateway**.
4. Click the **General.** tab.



5. Enter an email address in the **Support email address for sending the client logs** field.

Related links

Real-time Monitoring on page 291

Chapter 8: Moderating Videoconferences in Equinox Management

You can moderate videoconferences using Equinox Management's In-meeting control interface. Depending on your user privileges, you can fix many aspects of the videoconference including screen layout of each participant, blocking and unblocking audio and video, and enabling or disabling a wide range of features for each user.

Related links

Accessing the In-meeting Control Interface on page 312
Customizing Participant Options on page 314
Modifying Participant Media Connections on page 316
Modifying Videoconference Views on page 320
Managing Videoconference Participants on page 329

Accessing the In-meeting Control Interface

About this task

You can monitor and moderate a videoconference as a participant or the organizer via the In-Meeting Control interface of the administrator portal.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Meetings** > **All**. The **All Ongoing Meetings** list appears.
3. Select the meeting you want to moderate.

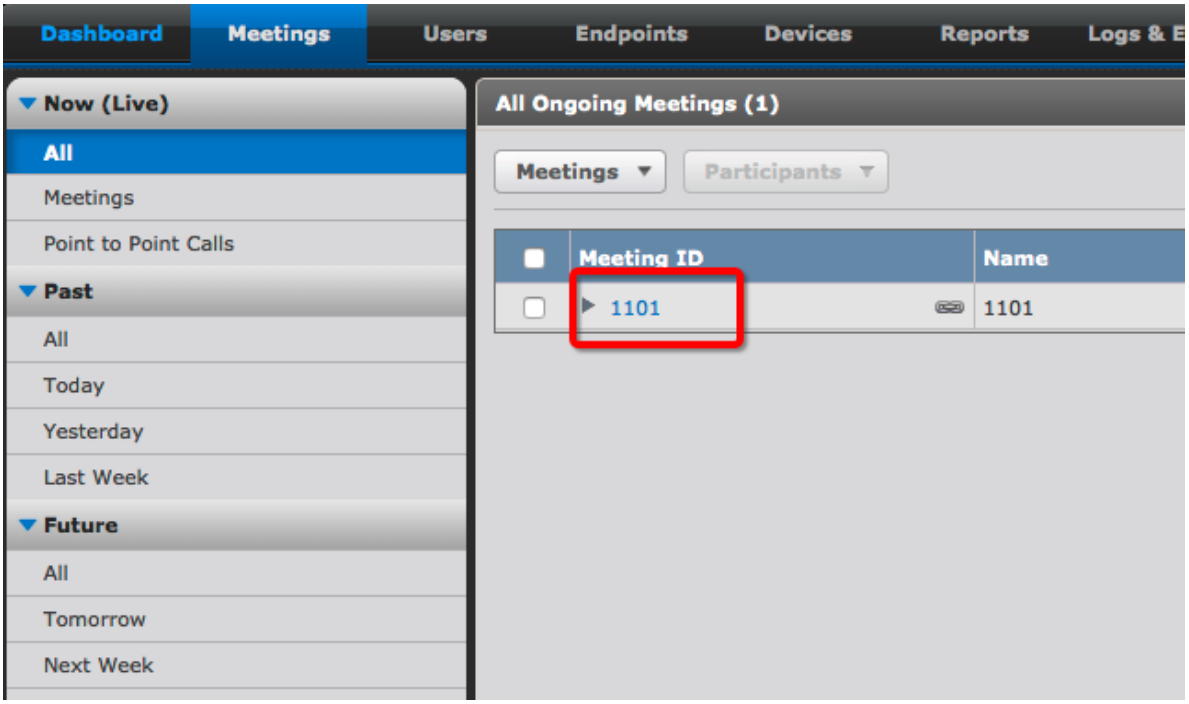


Figure 92: All Ongoing Meetings List

4. Select the meeting ID. The In-meeting control interface opens, displaying the list of meeting participants.

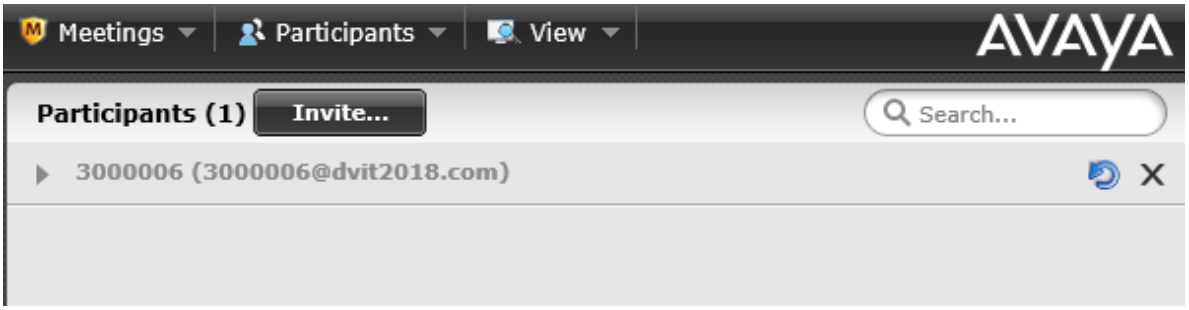


Figure 93: List of Participants

Note:

You can also access the In-meeting control interface by selecting the button in the **Actions** column on the All Ongoing Meetings page, and selecting **Moderate Meeting**.

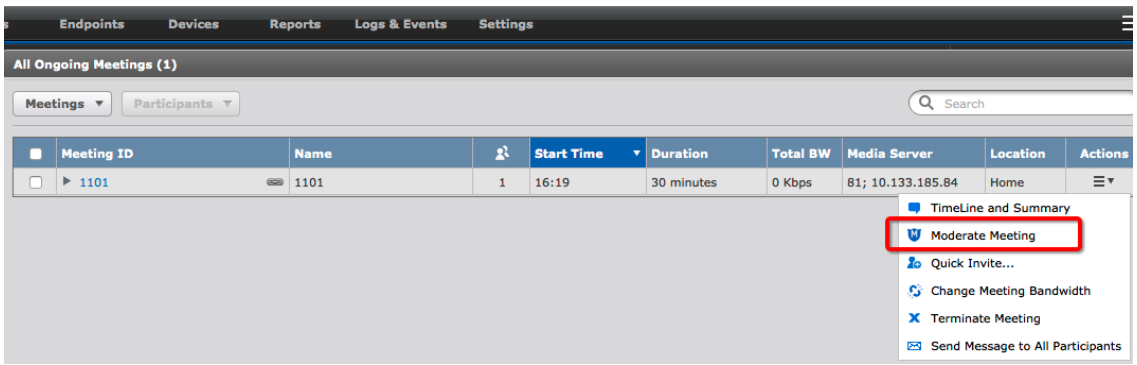


Figure 94: Moderate Meeting Option

5. Enter the moderator PIN, if prompted.

   You are automatically granted moderator rights, if another user is not moderating this videoconference.

Related links

Moderating Videoconferences in Equinox Management on page 312

Customizing Participant Options

Inviting participants to a meeting requires the system to know which endpoints are associated with specific users. You can also customize the settings of each participant's endpoint to define the VIP and lecturer of a meeting.

Related links

Moderating Videoconferences in Equinox Management on page 312
Enabling Lecture Mode on page 314
Selecting the VIP Status for a Participant on page 315

Enabling Lecture Mode

About this task

In lecture mode, the lecturer sees all the participants while the participants see only the lecturer. You can enable lecture mode setting by following this procedure.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting control interface, select **View** > **Participant List View** or select the MCU hosting the conference.

4. Select the relevant participant.
5. Select the **Action button** > **Lecturer** to open a popup window.

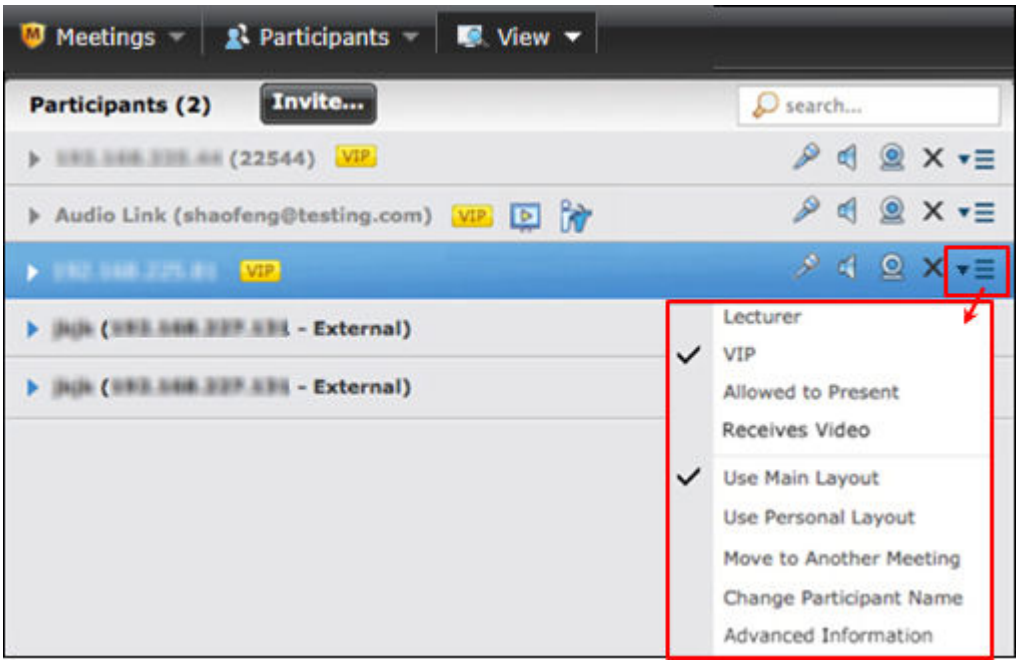


Figure 95: Accessing the Action menu

The icon appears next to the participant's name.

6. To cancel lecture mode, select **Moderate** > **Set Lecturer** > **No Lecturer**.
7. As a shortcut to select a lecturer, select the lecturer from the list of participants in **Moderate** > **Set Lecturer**. This setting also overrides the participant custom layout.

Related links

Customizing Participant Options on page 314

Selecting the VIP Status for a Participant

About this task

When you select the VIP status for an endpoint, Equinox Management cannot downgrade its bandwidth. The video from the VIP endpoint is always displayed. In addition, the VIP can start a presentation without any additional configuration.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting control interface, select **View** > **Participant List View** or select the MCU hosting the conference.

4. Select the relevant participant.
5. Select the **Action button** > **VIP** to open a popup window.

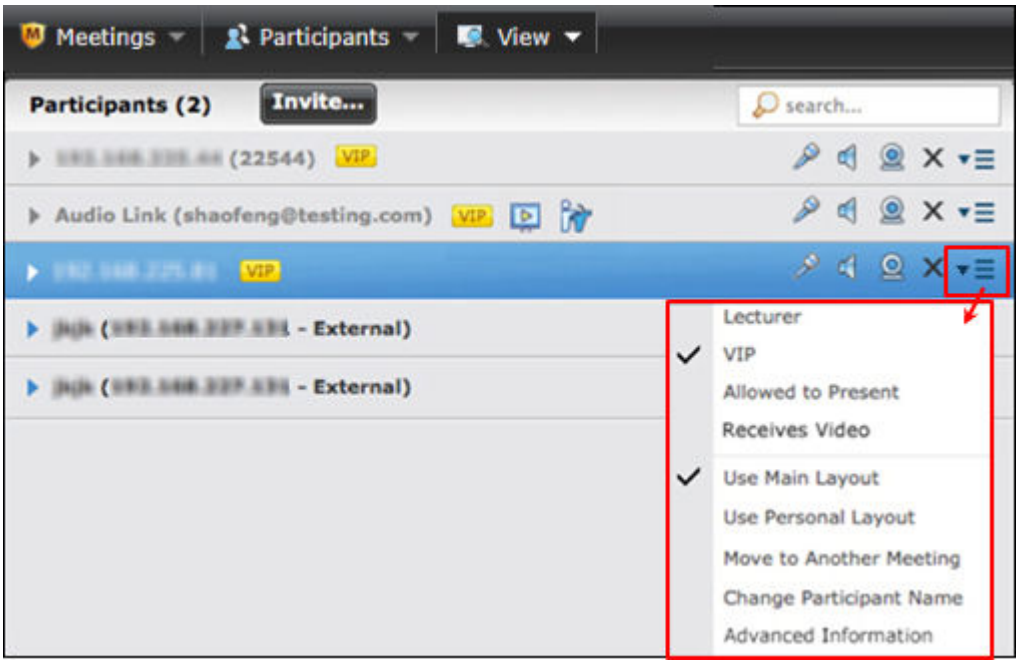


Figure 96: Accessing the Action menu

The VIP icon appears next to the participant's name.

Related links

Customizing Participant Options on page 314

Modifying Participant Media Connections

You can easily modify the settings of accessories a participant uses during the videoconference, as explained in these topics.

Related links

Moderating Videoconferences in Equinox Management on page 312
Blocking a Participant's Camera on page 317
Blocking Incoming Video on page 317
Changing a Participant's Audio Level on page 318
Sharing a Presentation on page 319

Blocking a Participant's Camera

About this task

While moderating a videoconference, you can block or unblock a video stream sent by a meeting participant. For example, if a participant’s video connection affects meeting processing and degrades performance, you can block the participant's video connection until the endpoint issues are resolved.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting control interface, select **View** > **Participant List View** or select the MCU hosting the conference.
4. Select the relevant participant.
5. To block the camera, select the icon next to the participant's name.

Related links

Modifying Participant Media Connections on page 316

Blocking Incoming Video

About this task

While moderating a videoconference, you can prevent a participant from viewing another's endpoint video.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting control interface, select **View** > **Participant List View** or select the MCU hosting the conference.
4. Select the relevant participant.
5. To block the video, select the icon.

Related links

Modifying Participant Media Connections on page 316

Changing a Participant's Audio Level

About this task

Users with moderator access can change the volume of a participant's microphone or speaker. This option is useful in case there is unwanted background noise caused by a specific participant or endpoint.

A moderator can also mute all conference participants by performing a single action.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting control interface, select **View** > **Participant List View** or select the media server hosting the conference.
4. Select the relevant participant.
5. To mute the participant, select the icon next to the name.
6. To turn of the participant’s audio, select the icon next to the name.
7. To decrease or increase the audio level, follow these steps:
   a. Select the icon and then select **Advanced Information** in the participant's information window.
   b. Select the **Audio** tab and drag the slider to the required volume level (Figure 97: The audio level page on page 319).

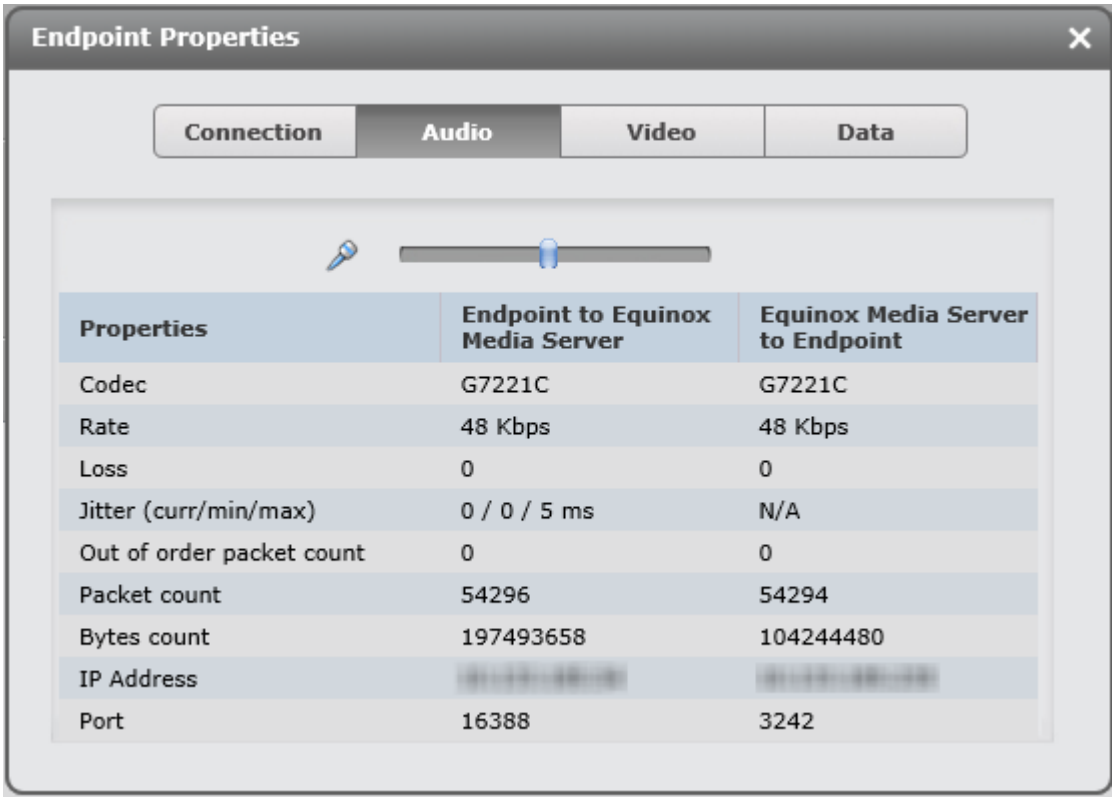


Figure 97: The audio level page

8. To mute all conference participants, select **Participants** > **Mute** > **Mute All Participants** in the List of Participants Interface. The moderator is not muted.

   To unmute all conference participants, select **Participants** > **Mute** > **Unmute All Participants** in the List of Participants Interface.

Related links

Modifying Participant Media Connections on page 316

Sharing a Presentation

About this task

A user can connect to a videoconference from a SIP or H.323 endpoint to share content such as presentations, spreadsheets, documents, and movies. As a moderator, you can enable the presentation feature for one or more participants.

Note:

Apple Safari®, Microsoft Internet Explorer®, and Microsoft Edge® do not support full screen sharing.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting control interface, select **Particpants** > **Presentation**.
4. Select **Enable for all participants**.

   To disable the feature, select **Disable for all participants**.
5. Enable presentation for one participant as follows:
   a. Select the relevant participant.
   b. Select **Action** > **Allowed to present** in the Information window.

Related links

Modifying Participant Media Connections on page 316

Modifying Videoconference Views

These topics describe how to define the way videoconferences appear on participants' screens, such as video layouts, whether participants' names appear, and whether participants can see themselves in the videoconference.

Related links

Moderating Videoconferences in Equinox Management on page 312
Changing the Main Video Layout on page 320
Enabling Dynamic Layout on page 323
Positioning the Active Speaker in the Video Layout on page 324
Changing a Participant Meeting View on page 325
Changing a participant name on page 326
Activating Participant Auto-switching for Fixed Layouts on page 326
Enabling the Self-see Feature on page 328

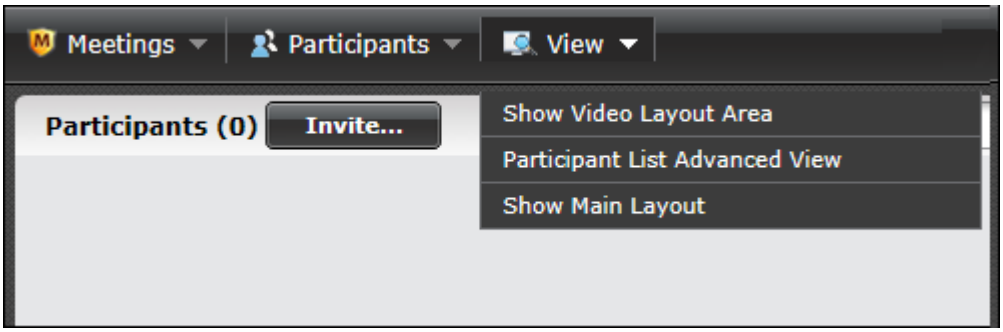
Changing the Main Video Layout

About this task

A video layout is the arrangement of participant images as they appear on the monitor in a videoconference. If the meeting includes a presentation, a layout can also refer to the arrangement of the presentation image together with the meeting participants. As a moderator, you can choose the main video layout of the videoconference that is seen by all participants, as described in this procedure. If necessary, you can also change a participant's video layout to a layout different from the main layout as described in Changing a Participant Meeting View on page 325.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting Control interface, click **View** > **Show Video Layout Area**.



4. Select a layout from the options in the window, as shown in Figure 98: Selecting a layout on page 321.

   The meeting type you selected while scheduling this videoconference defines which video layouts are available.

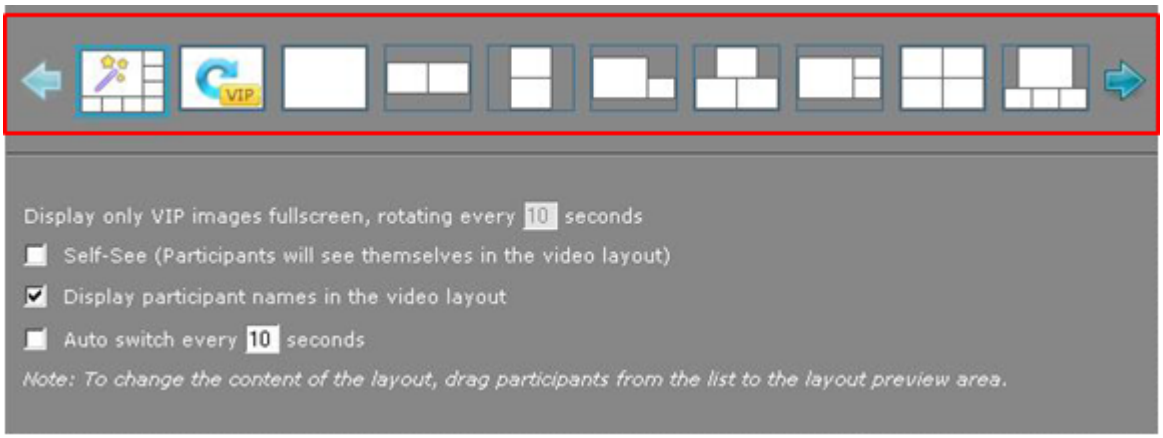


Figure 98: Selecting a layout

Table 56: Video layouts

Layout	Description
Dynamic	The dynamic video layout is a meeting layout that switches dynamically to include the maximum number of participants it can display on the screen (up to 9 on the XT Series, or up to 28 on Scopia Elite MCU and/or Equinox Media Server). The largest image always shows the active speaker.

Table continues…

Layout	Description
VIP	This option appears only in lecture mode. A lecturer sees only VIP endpoints in the single video frame. VIP participants and all other participants see only the lecturer. If you selected this layout, define how often VIP participants are rotated on the lecturer's screen, as explained below.
Fixed (any icon showing a fixed number of participants, for example, or)	A fixed video layout limits the number of the participants shown in the meeting video to the number of frames in the layout you chose.

5. Configure the fixed position of a participant in the video layout by dragging and dropping a participant from the selected layout area to the video display area, as shown in Figure 99: Mapping meeting participants in the selected video layout on page 322.

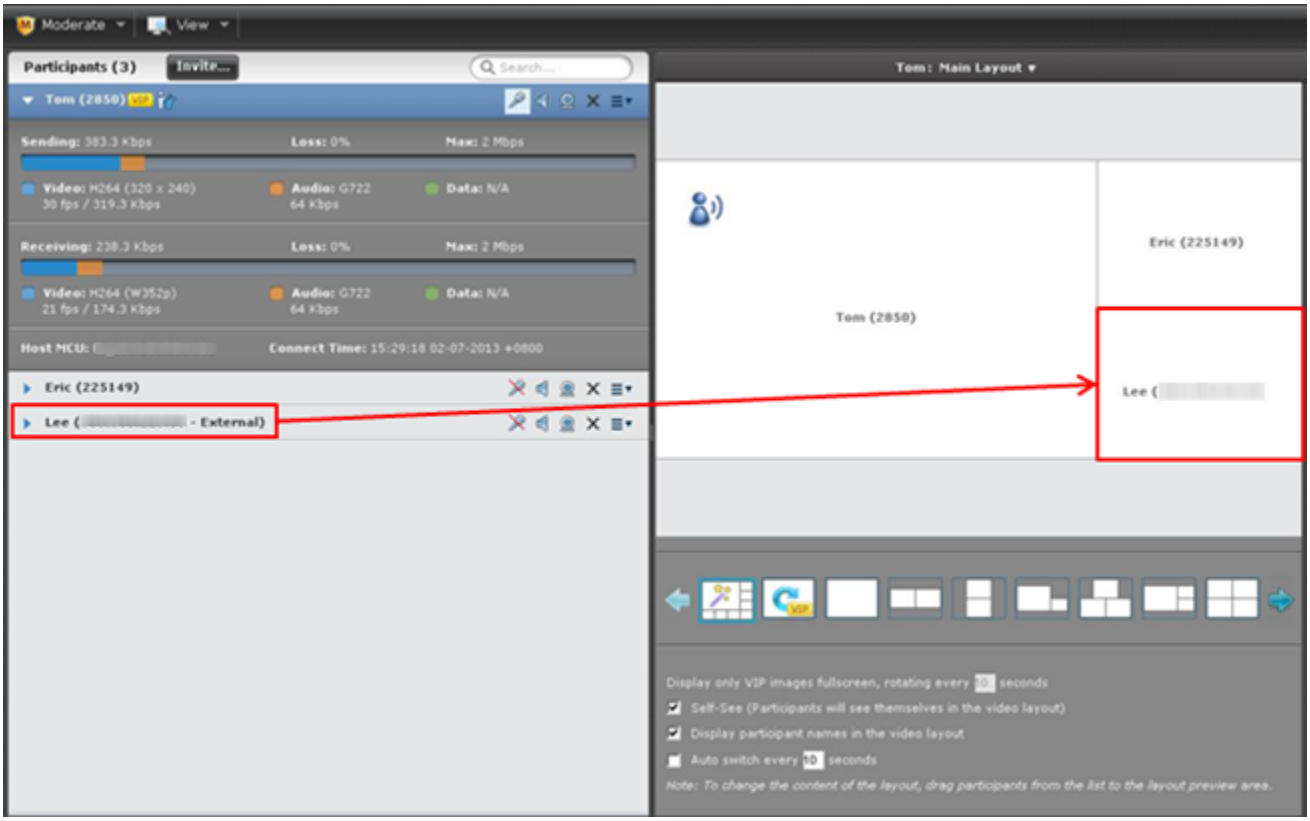


Figure 99: Mapping meeting participants in the selected video layout

6. If you selected the VIP layout, define how often VIP participants are rotated on the lecturer's video layout, as shown in Figure 100: Defining how often VIP endpoints are switched on page 323.

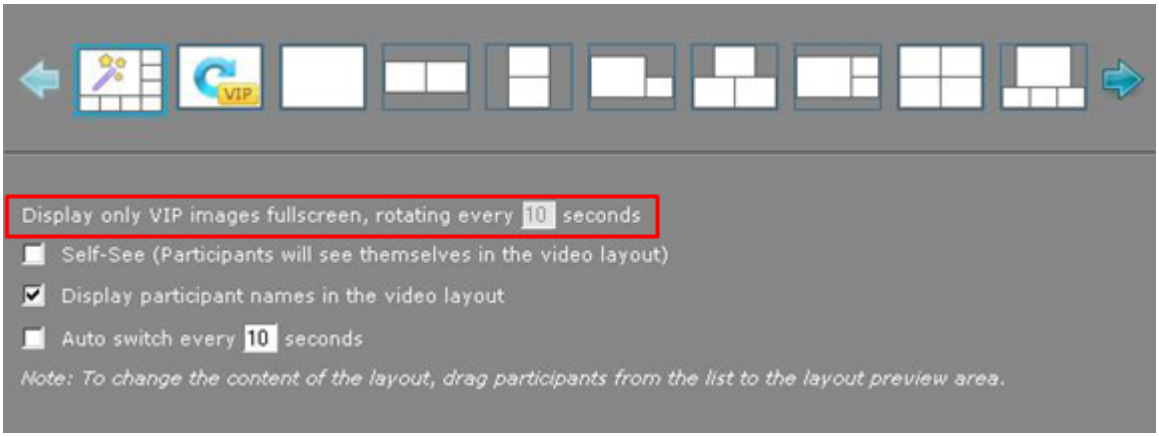


Figure 100: Defining how often VIP endpoints are switched

Related links

Modifying Videoconference Views on page 320

Enabling Dynamic Layout

About this task

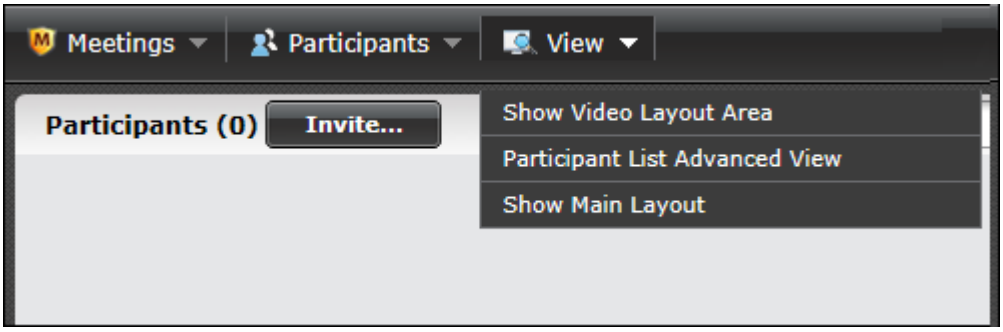
Without a dynamic layout, you can switch between a wide range of video layouts for the meeting. With dynamic layout, the video image automatically includes the number of frames equal to the number of participant images (up to a maximum of 28). The layout changes according to the number of participants that join or exit the meeting.

Dynamic layout conserves bandwidth, eliminates the display of empty frames in the video image, and makes optimal use of the video image display. Dynamic layout is especially suited to a meeting that has a high rate of participant traffic joining and exiting the meeting, or to an adaptive meeting type that has a variety of meeting sizes.

Since this functionality pertains to video layouts, this option is not available for non-video conferences.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting Control interface, click **View** > **Show Video Layout Area**.



4. Select to enable the dynamic layout and dynamically allocate the largest video window to the active speaker.

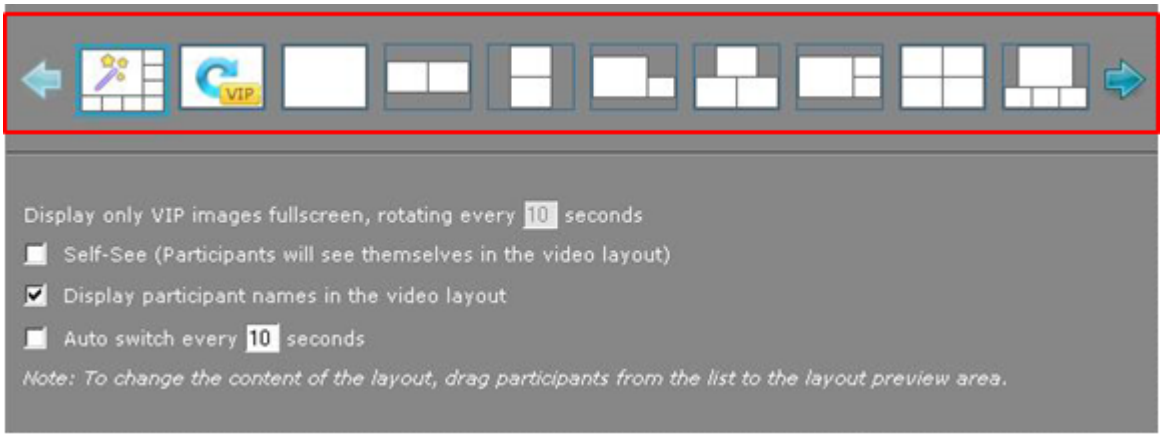


Figure 101: Selecting a layout

Related links

Modifying Videoconference Views on page 320

Positioning the Active Speaker in the Video Layout

About this task

If you have moderator privileges, you can show the active speaker in the pane of your choice. For example, you can choose to show the current speaker in the largest part of the video display, while the other participants are displayed in smaller panes. Or, you can choose to display the active speaker in one pane, while the other participants are not displayed at all.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. Drag the icon into the required position within the video layout frame.

Related links

Modifying Videoconference Views on page 320

Changing a Participant Meeting View

About this task

While moderating the videoconference, you can change the meeting view for a selected participant.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting Control interface, select **View** > **Participant List View** or select the MCU hosting the conference.
4. Select the participant for whom you want to change the view.
5. Select the **Action button** > **Use Personal Layout** and select a view in the personal layout window.

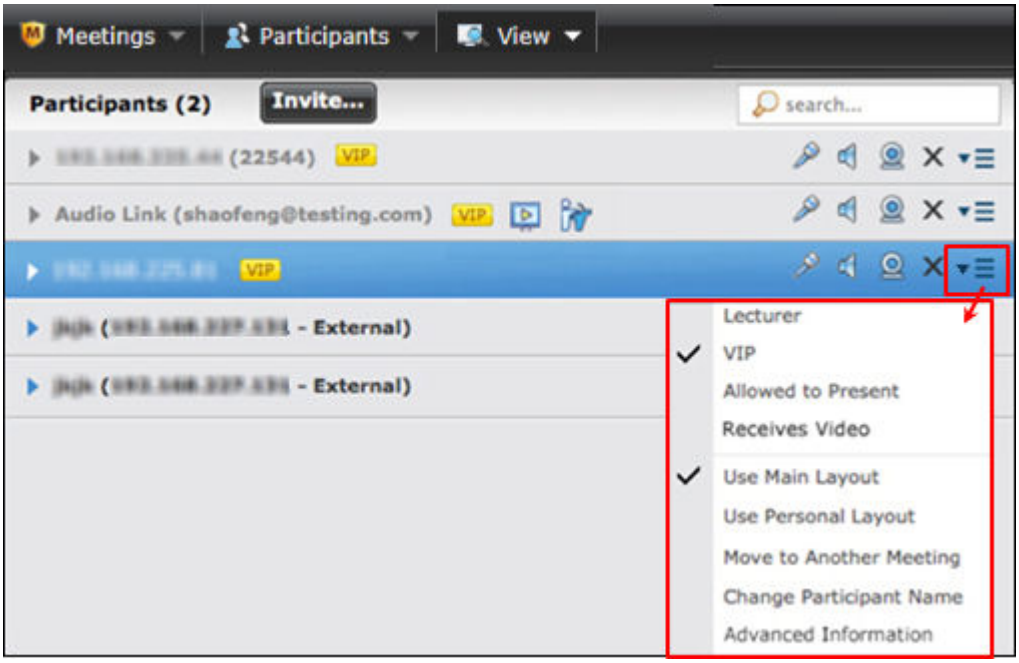


Figure 102: Accessing the Action menu

6. To return to the participants' layout view, select **Action button** > **Use Main Layout**.

Related links

Modifying Videoconference Views on page 320

Changing a participant name

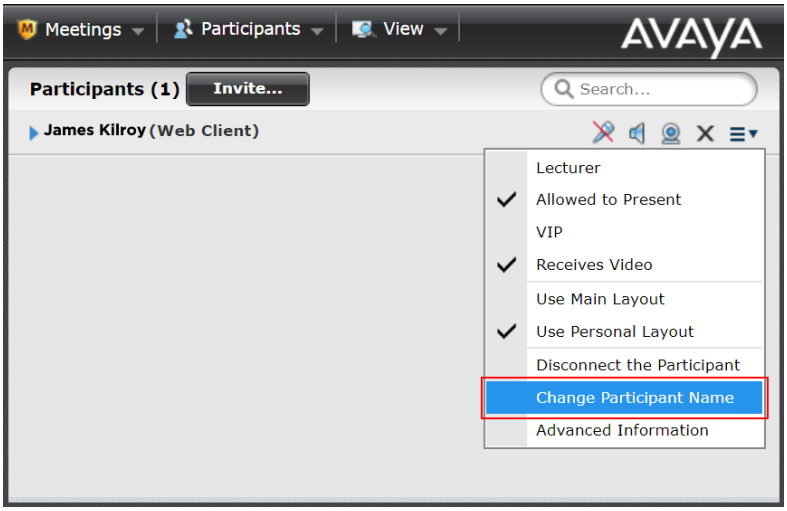
About this task

You can change a participant's name while a meeting is in progress or the participant is in the waiting room.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Meetings** > **Meetings**.
3. Click the meeting or waiting room where the participant name is.

   The system displays the In-meeting Control interface window.
4. In the row of the participant in the In-meeting Control interface click the **Action button** > **Change Participant Name**.



5. Enter a new name for that participant in the popup.

   If the participant is online, the system displays new name on the video screen for that participant.

Related links

Modifying Videoconference Views on page 320

Activating Participant Auto-switching for Fixed Layouts

About this task

Sometimes a fixed video layout has fewer video frames than the number of participants in the meeting. For example, there are 5 participants in a meeting, but you use a video layout with 4 video frames because you want larger video frames. You can configure your Equinox

Management to show participants' images in turns, so that your video layout rotates to include all participants, as shown in Figure 103: Example of a video layout with auto-switching enabled on page 327.

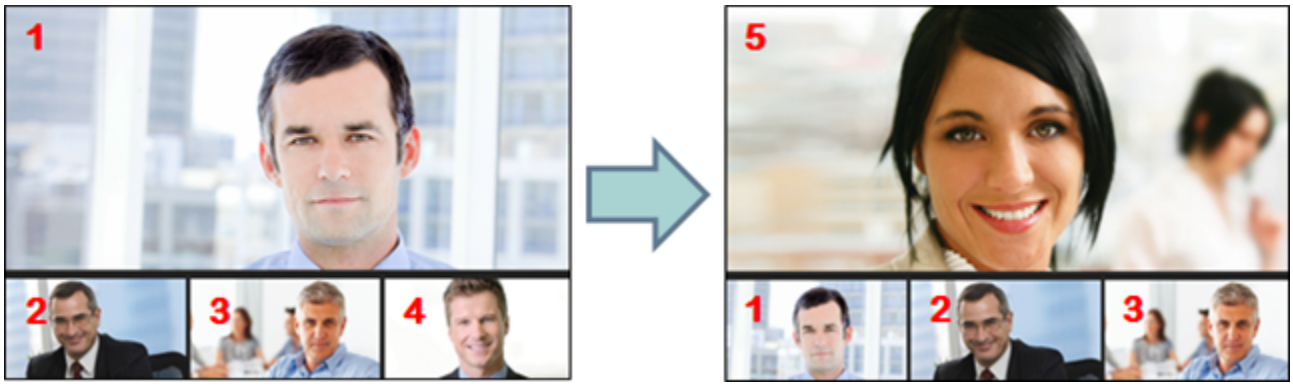


Figure 103: Example of a video layout with auto-switching enabled

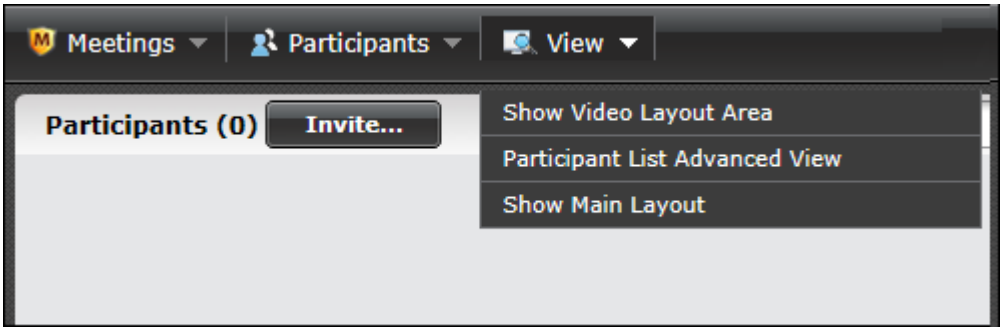
When using the dynamic layout, the auto-switching feature is enabled automatically. Every time a new participant joins the meeting in the dynamic layout, it adds a video frame to the layout until the number of video frames reaches the maximum of 28. After that, the video layout begins to rotate participants to include everyone.

Note:

Auto-switching overrides any existing video display options. Auto-switching is supported only on Scopia® Elite 6000 MCU, not older Scopia Elite MCU deployments.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting Control interface, click **View** > **Show Video Layout Area**.



4. Select the **Auto switch every n seconds** field.

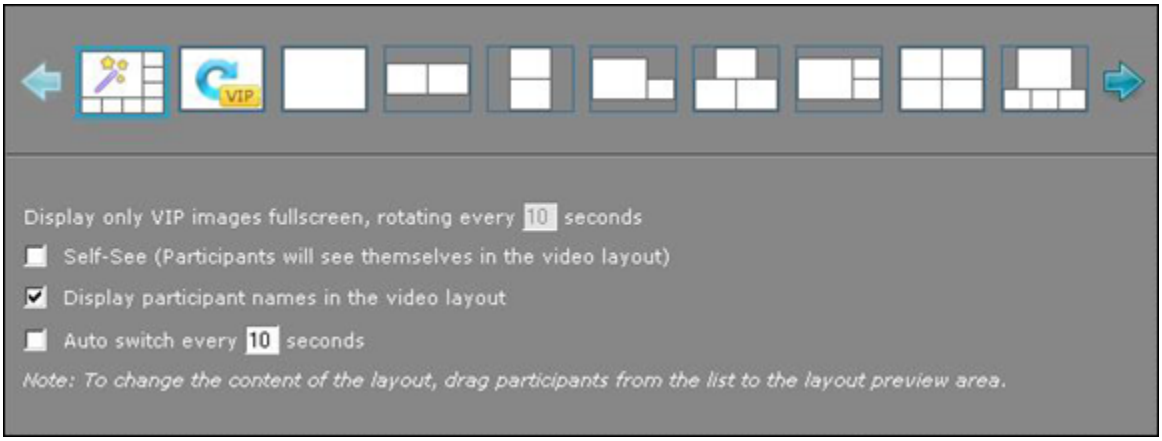


Figure 104: Video layout options

5. Define how often Equinox Management switches the participants' video by entering a value between 10 and 99 seconds.

Related links

Modifying Videoconference Views on page 320

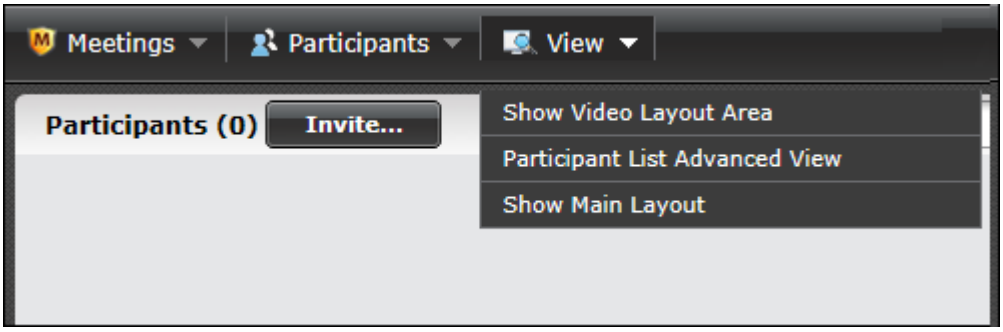
Enabling the Self-see Feature

About this task

The self-see feature allows participants to see their own video in a separate sub-frame in the videoconference. While moderating the videoconference, you can enable this feature.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting Control interface, click **View** > **Show Video Layout Area**.



4. Select the **Self-see** field.

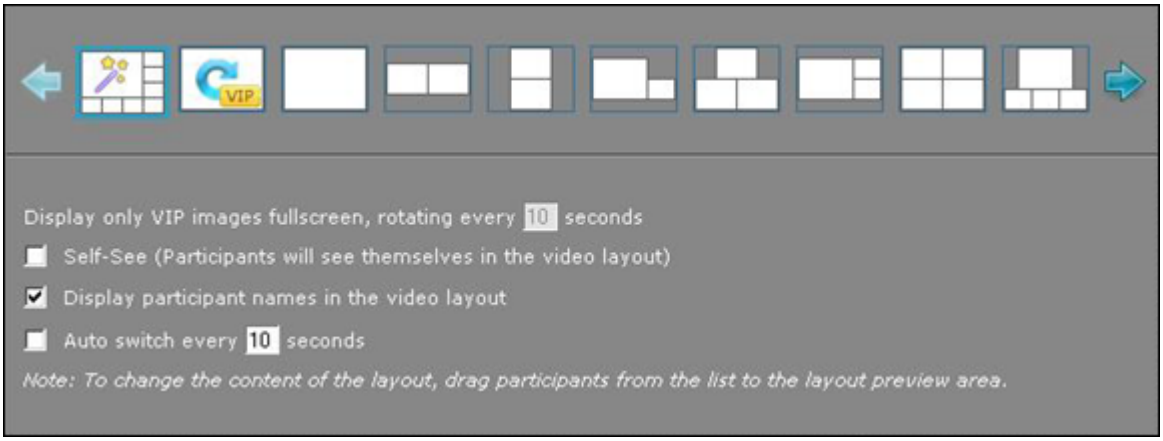


Figure 105: Layout options

All participants can see themselves in the conference video.

Related links

Modifying Videoconference Views on page 320

Managing Videoconference Participants

While moderating a videoconference, you can manage the participants, as described in these topics:

Related links

Moderating Videoconferences in Equinox Management on page 312
Inviting a Participant to Join a Videoconference on page 329
Viewing Technical Details of Participant Connection in a Meeting on page 332
Re-inviting All Offline Participants on page 337
Blocking Conference Admission on page 338
Sending a Public Chat Message on page 338
Displaying Participant Names in Frames on page 339
Disconnecting a Participant on page 341
Extending a Videoconference Duration on page 341
Ending a Videoconference on page 342

Inviting a Participant to Join a Videoconference

About this task

You can invite a participant to join an ongoing meeting by following this procedure.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting Control interface, select **Invite**.
4. To invite a participant from the corporate address book, select **Directory** (Figure 106: Inviting a participant from the Directory tab on page 330).

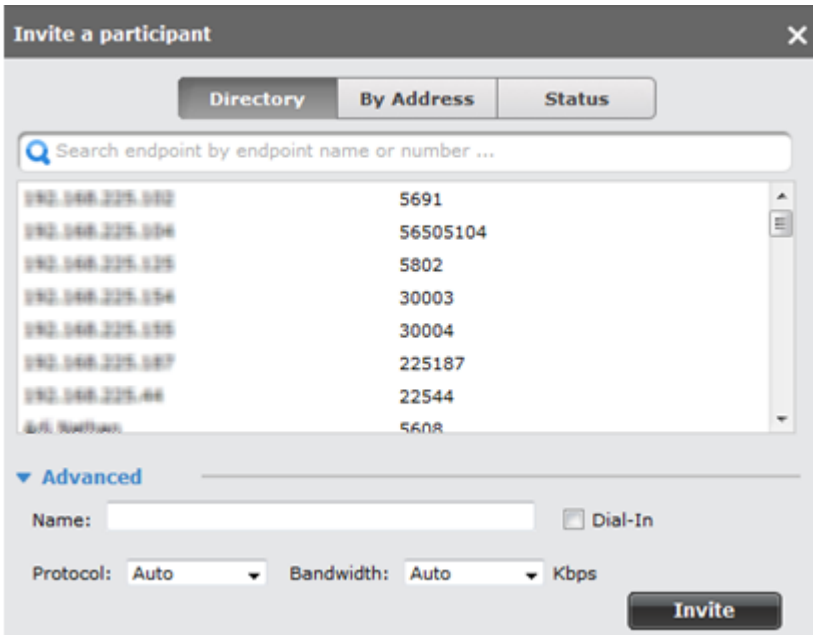


Figure 106: Inviting a participant from the Directory tab

   a. Select the participant listed in the address book.
   b. If the participant is not displayed in the list, alter your search by entering the partial or complete participant's name, number, or address in the **Search** field.
5. To invite an endpoint that is external to the organization, manually enter the participant's details in the **By Address** page (Figure 107: Inviting an external participant on page 331).

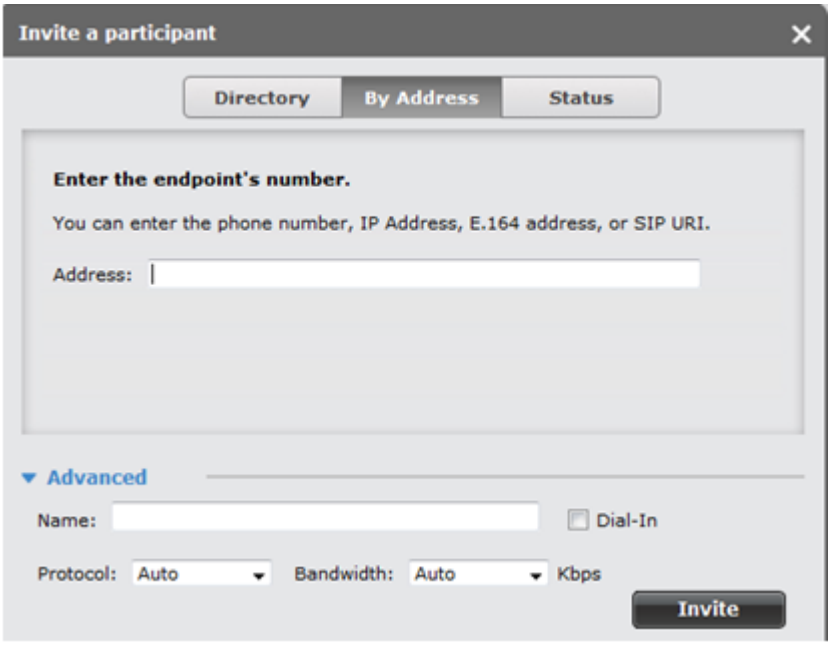


Figure 107: Inviting an external participant

6. You can give a name to the endpoint so the user see this name instead of its IP address, as follows.
   a. Select **Advanced**.
   b. Enter a name in the **Name** field.
7. You can select the videoconferecing standard used with the invited endpoint, as follows:
   a. Select **Advanced**.
   b. Select the specific **Protocol** from the dropdown list:
      - Select **H.323** if you invite an H.323 endpoint.
      - Select **SIP** if you invite an SIP endpoint.

      Important:

      The default **Auto** setting lets Equinox Management automatically select the videoconferencing standard.
8. You can adjust the bandwidth required for the call by selecting the required setting in **Advanced** > **Bandwidth**.

   Important:

   The default **Auto** setting lets Equinox Management automatically select the bandwidth required for the call. The setting supports all layouts and endpoints with various resolutions.
9. If you want the participant to call into the videoconference instead of you calling, select **Advanced** > **Dial In**.

10. Select **Invite**.

    Verify the call success or failure by selecting the **Status** window (Figure 108: The Status tab on page 332):

    - Select ✕ to remove the participant from the meeting.
    - Select to reconnect a participant after network issues were solved.

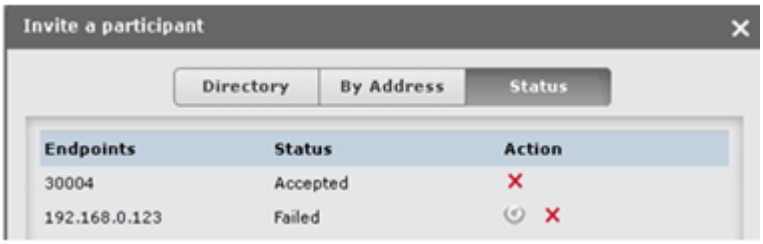


Figure 108: The Status tab

Related links

Managing Videoconference Participants on page 329

Viewing Technical Details of Participant Connection in a Meeting

About this task

You can use the statistics accumulated during a videoconference when calling customer support for solving any issue that might occur in a call.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting Control interface select the **View** > **Participant List View** or select the MCU hosting the conference.
4. Select the relevant participant.
5. Select the **Action button** > **Advanced Information** (Figure 109: Accessing endpoint information on page 333).

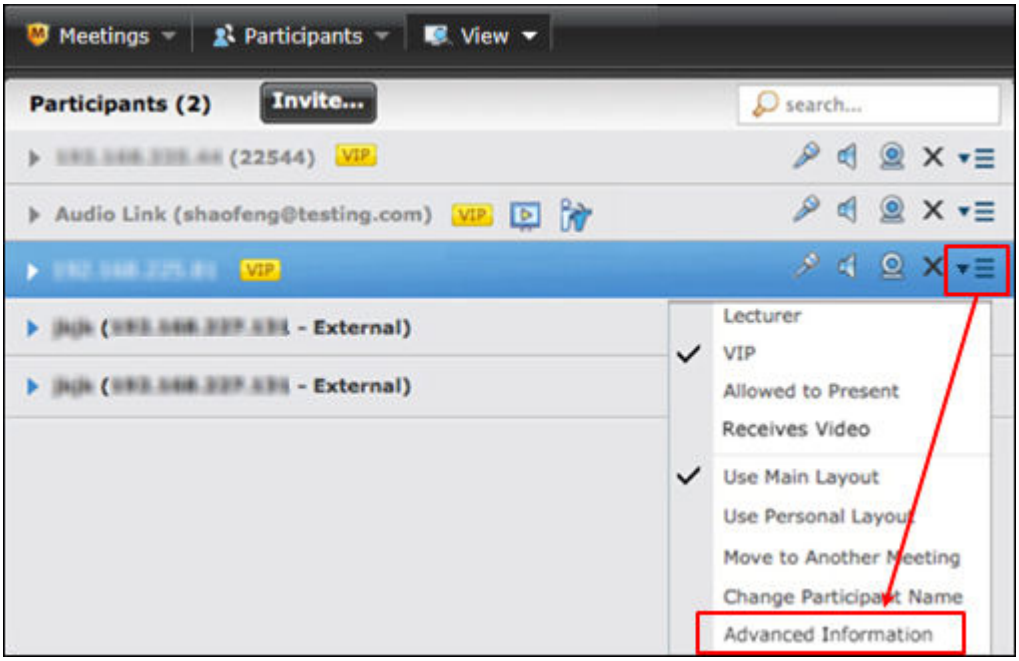


Figure 109: Accessing endpoint information

The window displays the endpoint properties.

6. Select the **Connection** tab to view details relating to the connection made by this endpoint to the videoconference (Figure 110: The Connection tab on page 334).

Figure 110: The Connection tab

Table 57: The Connection tab settings

Participant or Endpoint Detail	Description
Endpoint Name	Participant name.
Endpoint Address	Participant number such as IP address, E.164 number, or SIP URI.
Host MCU	Name of the MCU used for the call.
Type	The device used by the participant in the videoconference. This could be: • Video Endpoint • Via gateway • Videoconference connection • Cascaded Videoconference • Undetermined
Description	Participant description (displays the endpoint vendor identifier, if available).
Connection Time	Time the participant connected to the meeting.

Table continues…

Participant or Endpoint Detail	Description
Connection Method	Indicates whether the endpoint: • Dialed into the meeting, or • Was invited to the meeting from the In-meeting Control screen.
Bitrate	Maximum bit rate of audio, video, and data streams transferred per call, in megabits per second

7. Select the **Audio** tab to view the statistics related to the audio connection of this endpoint. The information lists values for calls from the endpoint to the MCU, and vice-versa (Figure 111: The Audio tab on page 335).

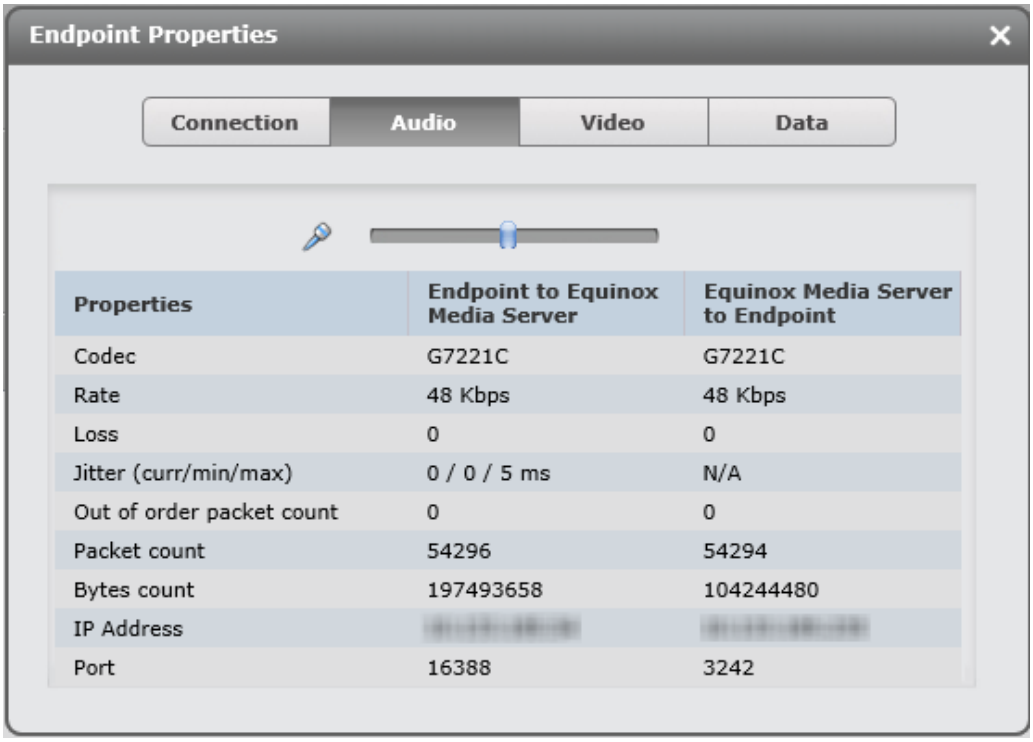


Figure 111: The Audio tab

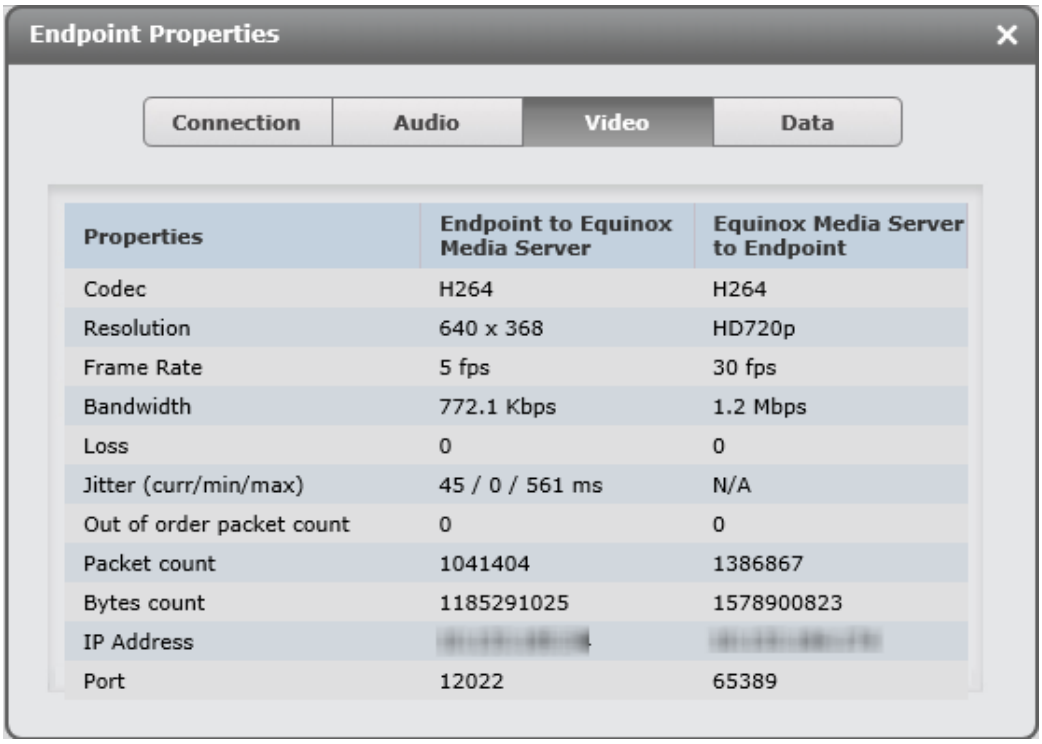
Table 58: Settings of the Audio, Video and Data tab

Participant or Endpoint Detail	Description
Codec	Standard used for compressing and decompressing audio streams.
Rate	Amount of audio data transferred in kilobits per second.
Loss	Missing audio in the transferred packets, expressed in percentage.

Table continues…

Participant or Endpoint Detail	Description
Jitter (curr/min/max)	The delay in transferred audio packets, calculated at current, minimum, and maximum values and expressed in milliseconds.
Out of order packet count	The number of media packets that reached the recipient in the wrong sequence.
Packet count	The total number of media packets sent between the endpoint and the MCU.
Bytes count	The total number of bytes sent between the endpoint and the MCU.
IP Address	The IP address of the endpoint or the MCU.
Port	The port for media transfer. **Important:** The ports used for audio, video, and data are different.

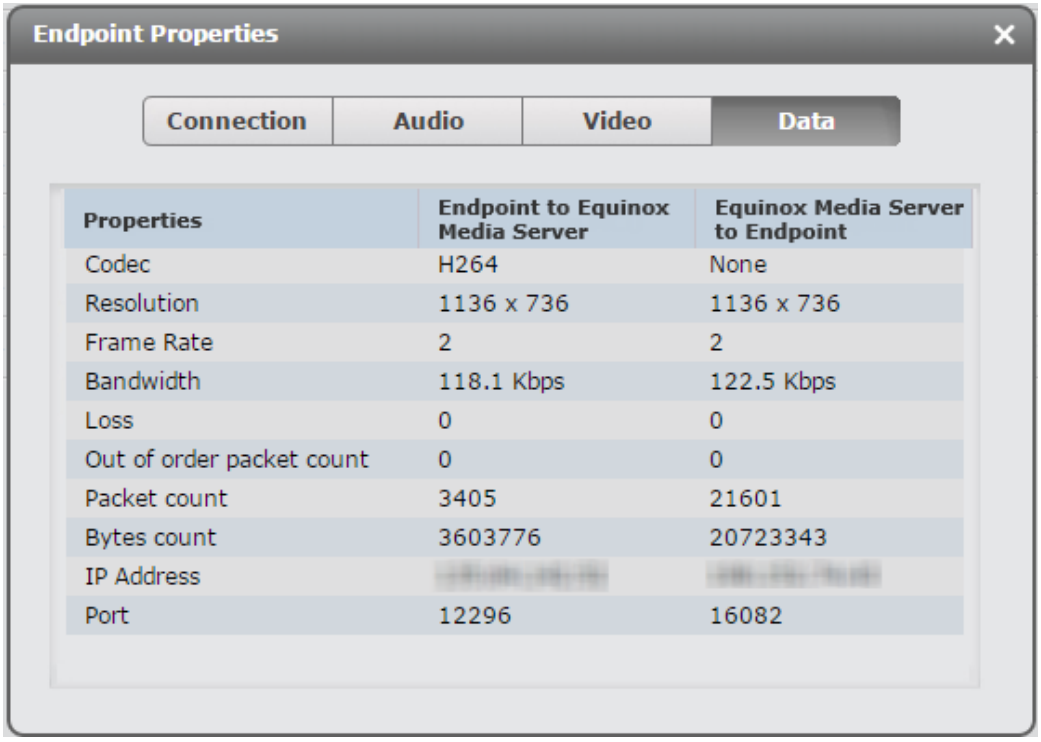
8. Select the **Video** tab to view the statistics related to the video connection of this endpoint. The information lists values for calls from the endpoint to the MCU, and vice-versa (Figure 112: The Video tab on page 336).



Properties	Endpoint to Equinox Media Server	Equinox Media Server to Endpoint
Codec	H264	H264
Resolution	640 x 368	HD720p
Frame Rate	5 fps	30 fps
Bandwidth	772.1 Kbps	1.2 Mbps
Loss	0	0
Jitter (curr/min/max)	45 / 0 / 561 ms	N/A
Out of order packet count	0	0
Packet count	1041404	1386867
Bytes count	1185291025	1578900823
IP Address	[illegible]	[illegible]
Port	12022	65389

Figure 112: The Video tab

9. Select the **Data** tab to view the statistics related to the video connection of this endpoint. The information lists values for calls from the endpoint to the MCU, and vice-versa (Figure 113: The Data tab on page 337).



Properties	Endpoint to Equinox Media Server	Equinox Media Server to Endpoint
Codec	H264	None
Resolution	1136 x 736	1136 x 736
Frame Rate	2	2
Bandwidth	118.1 Kbps	122.5 Kbps
Loss	0	0
Out of order packet count	0	0
Packet count	3405	21601
Bytes count	3603776	20723343
IP Address	[illegible]	[illegible]
Port	12296	16082

Figure 113: The Data tab

Related links

Managing Videoconference Participants on page 329

Re-inviting All Offline Participants

About this task

Users with moderator-level access can re-invite all offline participants that had been originally invited to the scheduled conference.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting Control interface, select **Participants** > **Re-invite all Offline Participants**. Original invitees automatically receive another invitation to join the meeting.

   Note:

   When participants rejoin a meeting, they can view chat sessions that have been ongoing since the beginning of the meeting.

Related links

Managing Videoconference Participants on page 329

Blocking Conference Admission

About this task

Users with moderator-level access can block the admission of additional participants to a conference.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting Control interface, select **Meetings** > **Lock Meeting**. This blocks any further participants from entering the videoconference.

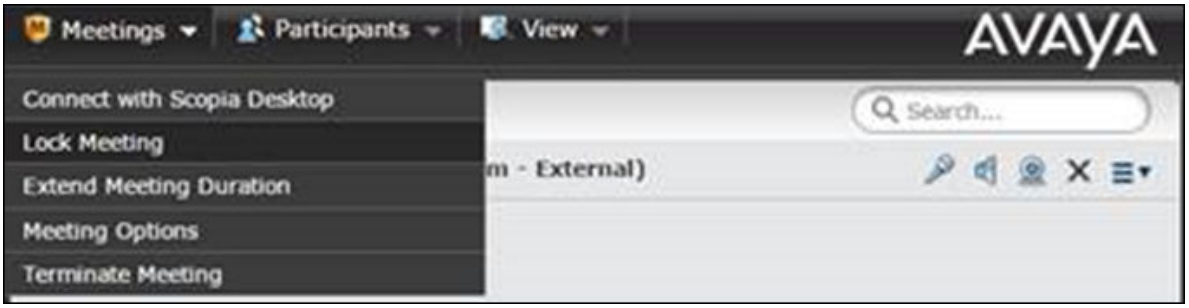


Figure 114: Lock Meeting Option

Note:

To re-admit participants, select **Unlock Meeting**.

Related links

Managing Videoconference Participants on page 329

Sending a Public Chat Message

About this task

While moderating the videoconference, you can send an instant message to all participants.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting Control interface, select **Participants** > **Send Message to All Participants**.
4. Type the message text in the window.
5. Select **Send**.

Related links

Managing Videoconference Participants on page 329

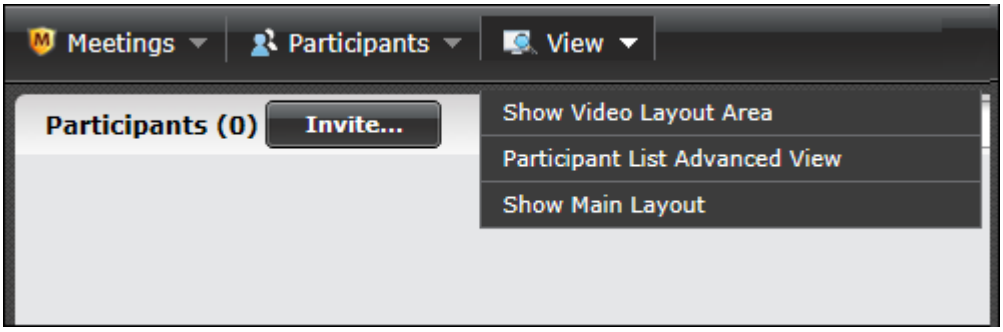
Displaying Participant Names in Frames

About this task

Users with moderator-level access can optionally display the name of endpoints or participants in specific positions of the video layout frame.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting Control interface, click **View** > **Show Video Layout Area**.



4. Select the **Display participant names in the video layout** check box as shown in Figure 115: Video Layout area on page 340.

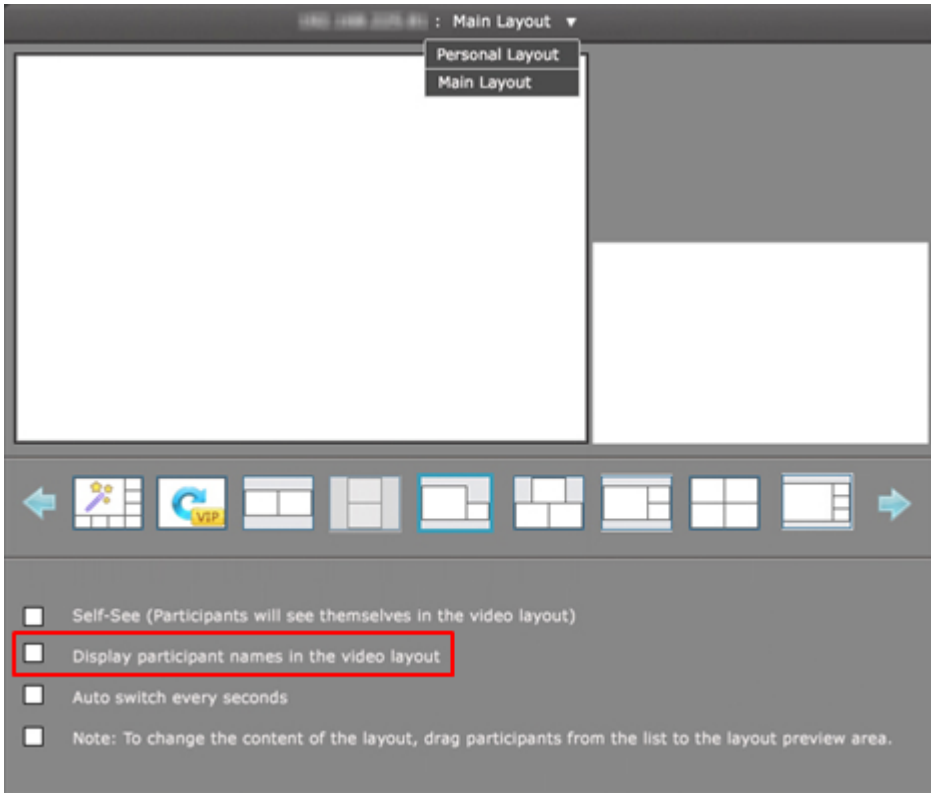


Figure 115: Video Layout area

Each participant or endpoint is clearly identified by name, in a text overlay on the video image (Figure 116: Names displayed in conference (example) on page 340).

Figure 116: Names displayed in conference (example)

Related links

Managing Videoconference Participants on page 329

Disconnecting a Participant

About this task

Follow this procedure to disconnect a participant from an ongoing videoconference. You can also disconnect multiple participants by performing a single action.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting Control interface, select **View** > **Participant List View** or select the MCU hosting the conference.
4. Select the participant you want to disconnect from the on-going videoconference (Figure 117: Disconnecting a participant on page 341).

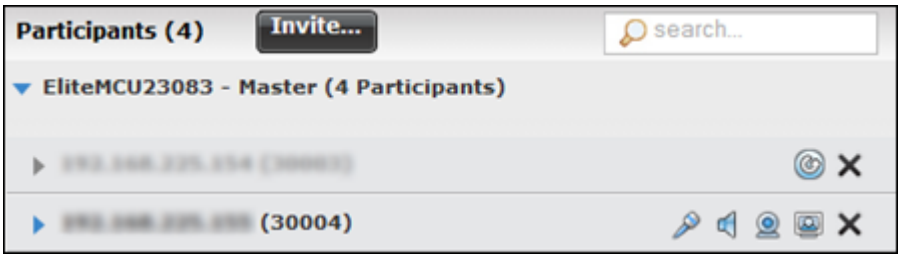


Figure 117: Disconnecting a participant

5. Select the × icon next to the participant's name.

   The participant is removed from the list and disconnected from the meeting.

   Important:

   The system might disconnect a participant due to network issues. When this happens, the participant's name is grayed. To reconnect, select the icon.

Related links

Managing Videoconference Participants on page 329

Extending a Videoconference Duration

About this task

You can extend the duration of a videoconference while it is in progress. A small counter at the bottom of the window indicates the time left in minutes before the meeting ends.

Procedure

1. Access the Equinox Management administrator portal.

2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting Control interface, select **Meetings** > **Extend Meeting Duration**.
4. Enter the number of additional minutes by which you want to extend the duration of the meeting in the **Extend** field of the **Extend Duration** window.

   Note:

   Sony PCS endpoint users can automatically extend a meeting via the Sony PCS terminal remote control.
5. Select **OK**.

Related links

Managing Videoconference Participants on page 329

Ending a Videoconference

About this task

Users with moderator-level access can immediately terminate a videoconference at any time.

Procedure

1. Access the Equinox Management administrator portal.
2. Access the In-meeting Control interface by selecting the meeting you want to moderate.
3. In the In-meeting Control interface, select **Meetings** > **Terminate Meeting**.
4. Select **OK**.

Related links

Managing Videoconference Participants on page 329

Chapter 9: Working with Equinox ad hoc conferencing

When working in a Team Engagement (TE) environment, you can create an ad hoc conference using Avaya IX™ Workplace Clients. The ad hoc conference starts in the user's virtual room.

You create an ad hoc conference by doing any of the following:

- Merge two P2P calls
- Add a new participant to an existing P2P call
- Share from a P2P call
- Create a conversation by dialing multiple participants at the same time
- Escalate a multi-party call to a conference call

You must configure Avaya IX™ Workplace Client and Avaya Communication Manager settings before starting the ad hoc conference. Following are the minimum versions of the clients and servers necessary to create an ad hoc conference:

- **Clients**:
  - Equinox Desktop Client: 3.2
  - Equinox Mobile Client: 3.2
  - Equinox Conference Web Client: N/A
- **Servers**:
  - Equinox Conferencing: 9.0.2
  - Unified Portal/AAWG: 3.2

Related links

Configuring Avaya IX Workplace Client settings on page 344
Configuring settings to enable Avaya 96xx phones for ad hoc conferencing on page 345
Configuring advanced parameters for ad hoc conferencing on page 345
Configuring the SIP Endpoint Managed Transfer Setting in Avaya Aura Communication Manager on page 347
Configuring Avaya Aura Communication Manager settings on page 348
Configuring Dial Plan settings on page 349
Configuring Equinox Management settings on page 350
Configuring System Manager settings on page 351
Escalating to a multipoint conference for a multiparty call using Avaya IX Workplace Client on page 354

Configuring Avaya IX™ Workplace Client settings

About this task

Before creating an ad hoc conference, you must configure settings in Avaya IX™ Workplace Client.

Procedure

1. In the Avaya IX™ Workplace Client interface, click the **Settings** icon and click **Services** > **Meetings**.

   The system displays the **Meetings** pop-up dialog:

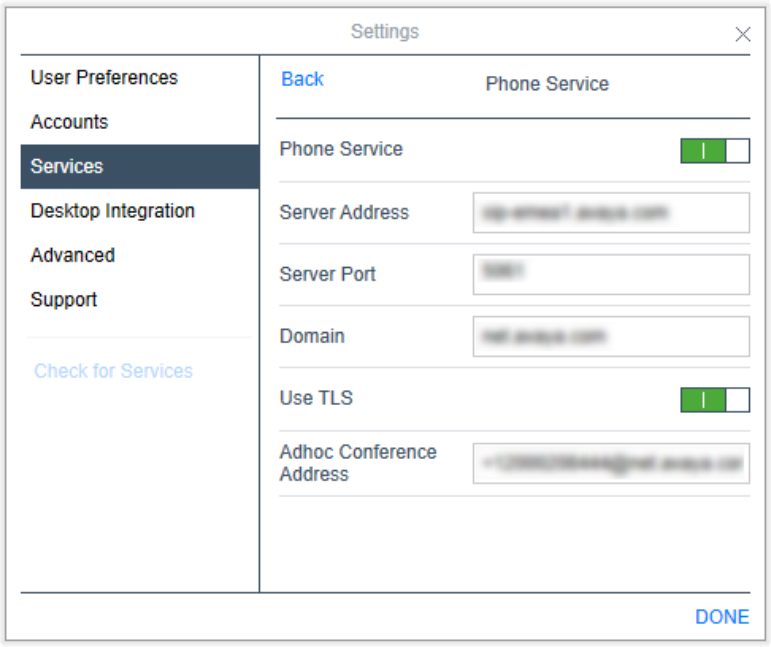


Figure 118: Meetings Pop-up Dialog

2. In the **Adhoc Conference Address** field, enter the ID of the user you want to join the ad hoc conference, in the following format: `<meetingID@sipdomain>`

   For example, enter `8571555@sip.avaya.com`, where:

   - **85** = the ID prefix
   - **7** = the SIP trunk
   - **71555** = the virtual room number, which includes the MCU prefix (71)
   - **sip.avaya.com** = the SIP domain

   Note:

   The SIP URI used must be configured in SMGR Routing or Dialing Pattern or Route Policy and under AEMG Meeting Policies and must be the same. The VMR is not a

user specific VMR rather a service number that uses the initiator or moderator user's VMR.

3. Click **Done**.

Related links

Working with Equinox ad hoc conferencing on page 343

Configuring settings to enable Avaya 96xx phones for ad hoc conferencing

About this task

To enable ad hoc conferencing to work on Avaya 96xx phones, you must configure the `CONFERENCE_FACTORY_URI` setting in the 46xxsettings.txt file. You must use the same URI that is in the Avaya IX™ Workplace Client.

Procedure

1. Access the 46xxsettings.txt file.
2. Locate the `CONFERENCING SETTINGS (SIP ONLY)` section.

   The guidelines for configuring this setting appear in the settings file.
3. Locate the `CONFERENCE_FACTORY_URI` line and set the value to `"<meetingID@sipdomain>"` (including the quotation marks). For example, `"93375000@avaya.com"`

Related links

Working with Equinox ad hoc conferencing on page 343

Configuring advanced parameters for ad hoc conferencing

About this task

You must configure advanced parameters in Equinox Management to enable creating an ad hoc conference.

Procedure

1. Access the Equinox Management administrator portal.
2. Click the Settings icon ≡ > **Advanced Parameters**.

   The system displays the **Advanced Parameters** dialog box.

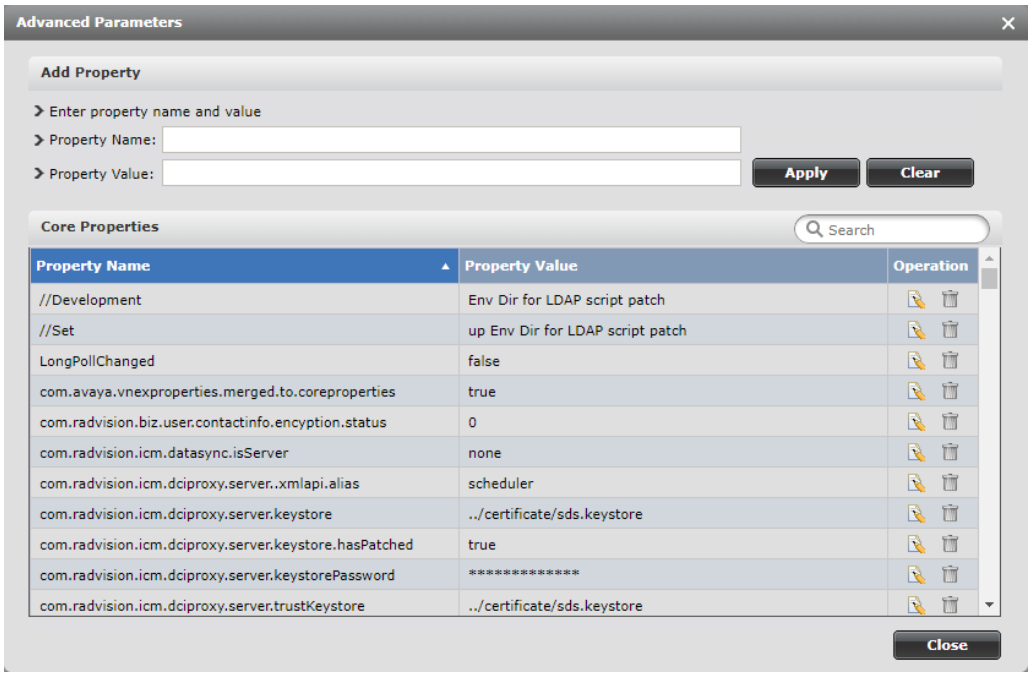


Figure 119: Advanced Parameters dialog box

3. Enter the indicated values in the fields described in the following table, click **Apply** after each one:

Table 59: Advanced Parameters Properties

Property Name Field	Property Value Field
vnex.vxmd.core.conference.factoryURI	<conference factory URI> For example: `816543@avayamcs.com`
vnex.vxmd.core.conference.defaultDomain	<default conference domain> For example: `avayamcs.com`
vnex.vxmd.core.conference.enableDialoutAsSIP	true

4. Click **Devices** > **Devices by Type** > **SIP Servers** and select a SIP server.

   The system displays the **Modify SIP Server** page.

Figure 120: Modify SIP Server page

5. In the **SIP Domain** field, enter the domain of the outbound SIP server.

   This serves as the default domain for outbound calls.

Related links

Working with Equinox ad hoc conferencing on page 343

Configuring the SIP Endpoint Managed Transfer Setting in Avaya Aura® Communication Manager

About this task

Configuring this setting enables support for Advanced SIP Telephony (AST) 2 call flow. You do not need to configure the **SIP Endpoint Managed Transfer** setting in Avaya Aura® Communication Manager to enable transferring the call to the virtual conference room. If the same Communication Manager supports both Avaya Aura® Contact Center and Unified Communication applications, it is possible to set SEMT to `n`.

Note:

For ad hoc conferencing support when the Avaya Aura® Communication Manager **SIP Endpoint Managed Transfer** (SEMT) field in the **system-parameters features** form is enabled, you must set the following fields in the Avaya Aura® Communication Manager SIP signalling group form to `y`:

- **Direct IP-IP** Audio Connections
- **Initial IP-IP** Direct Media

Before you begin

Ensure that you have successfully configured Avaya IX™ Workplace Client settings, as described in Configuring Avaya IX Workplace Client settings on page 344.

Procedure

1. In Communication Manager, type **change system-parameter features** to access the **Feature-Related System Parameters**.
2. Configure the value of the **SIP Endpoint Managed Transfer**.

```
change system-parameters features
                        FEATURE-RELATED SYSTEM PARAMETERS
IP PARAMETERS
Direct IP-IP Audio Connections? y         IP Audio Hairpinning? n
Synchronization over IP? n Allow SIP-H323 Video in SDES? n
Initial INVITE with SDP for secure calls? y
SIP Endpoint Managed Transfer? Y
```

Figure 121: SIP Endpoint Managed Transfer Setting

Related links

Working with Equinox ad hoc conferencing on page 343

Configuring Avaya Aura® Communication Manager settings

About this task

Before ad hoc conferencing can be enabled, you must configure settings in Communication Manager.

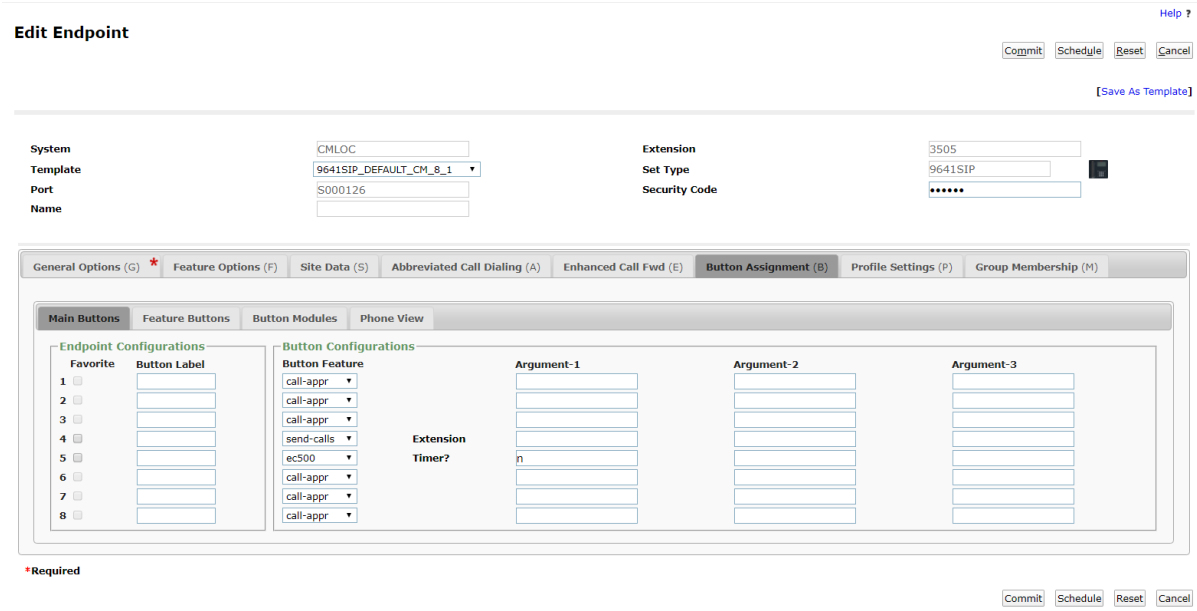
These configurations ensure that the phone interface displays the most frequently used buttons on the main screen, to optimize efficiency. You must configure eight call appearances for each Avaya IX™ Workplace Client extension.

Before you begin

Ensure that you have configured the SIP Endpoint Managed Transfer setting in Communication Manager, as described in Configuring the SIP Endpoint Managed Transfer Setting in Avaya Aura Communication Manager on page 347.

Procedure

1. Access the Communication Manager interface.



2. When using Avaya 9600 Series IP Deskphones with the same MDA extension as the Avaya IX™ Workplace Client, configure the call appearances as follows:
   a. Configure features, such as `send-call` and `ec500`, on the **Feature Buttons** tab.
   b. Configure the last 5 call appearances (`call-appr`) on the **Feature Buttons** tab.

   The line appearances are invoked as follows:

   - Call participants — 2 lines
   - Point to point calls being merged — 2 lines
   - Conference call leg to conference bridge — 1 line
   - Transfer operation — 2 lines
   - Outgoing emergency calls — 1 line (the last line)

Related links

Working with Equinox ad hoc conferencing on page 343

Configuring Dial Plan settings

About this task

Dial plan settings inform your system of how to interpret dialed digits. For example, if you must dial 9 to access an outside line, this is because the dial plan tells the system to find an external trunk when a dialed string begins with a 9. Dial plan settings also inform the system how many digits to expect for calls. For example, the dial plan may indicate that all internal extensions are 4-digit numbers that begin with 1 or 2.

You must verify that the Avaya Aura® Communication Manager can correctly route calls from the Avaya IX™ Workplace Client to an Equinox conference. If it cannot, you must add the Equinox conference virtual room number to the Communication Manager dial plan.

Before configuring dial plan settings, ensure that you have successfully configured the SIP Endpoint Managed Transfer setting, as described in Configuring the SIP Endpoint Managed Transfer Setting in Avaya Aura Communication Manager on page 347.

You must ensure that the new dynamic meeting ID numbering range is correctly configured in the Communication Manager dial plan for TE deployments to include the extra three digits. There are two options for doing this:

- Option 1
  - Assuming virtual room number range = 71xxxx.
  - Target dynamic meeting ID range = 71xxxxnnn.
  - If your existing Communication Manager dial plan was configured only for the virtual room number ranges , you must update the dial plan routing rules for prefix 71 and increase the total length from 6 to 9.
  - Limitation – A user who dials the original 6 digit virtual room number from a desk phone must wait for a few seconds before the call is connected to the conference.
- Option 2
  - Assuming virtual room number range = 71xxxx.
  - Target dynamic meeting ID range = 82xxxxnnn.
  - If your existing Communication Manager dial plan was configured only for the virtual room number ranges, you must add new dial plan routing rules for prefix 81 and set the total length to 9. The existing routing rule for prefix 71 remains unchanged.
  - A user who dials the original 6 digit virtual room number from a desk phone is connected to the conference without any delay.

For details on configuring dial plan settings, refer to the Communication Manager documentation.

Related links

Working with Equinox ad hoc conferencing on page 343

Configuring Equinox Management settings

About this task

To enable creating an ad hoc conference, you must configure settings in Equinox Management.

Before you begin

Ensure that you have completed the following configuration tasks:

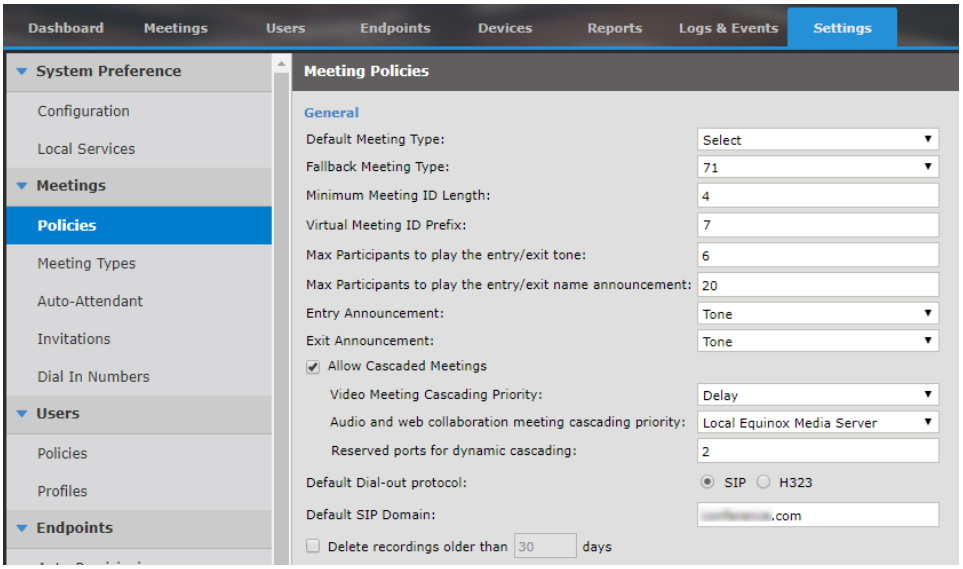
- Configuring Avaya IX Workplace Client settings on page 344
- Configuring the SIP Endpoint Managed Transfer Setting in Avaya Aura Communication Manager on page 347

- Configuring Dial Plan settings on page 349

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Meetings** > **Policies**.

   The system displays the **Meeting Policies** page.



3. In the **Default Dial-out protocol** field, select **SIP**.
4. In the **Default SIP Domain**, enter the default domain for the SIP server.
5. In the **Conference Factory URI for SIP Adhoc Conferencing** field, the URI must match the Avaya IX™ Workplace Client adhoc address and the 96xx CONFERENCE_FACTORY_URI.

Related links

Working with Equinox ad hoc conferencing on page 343

Configuring System Manager settings

About this task

To enable creating an ad hoc conference using a random meeting number (for a user without a virtual room), you must configure settings in System Manager.

Before you begin

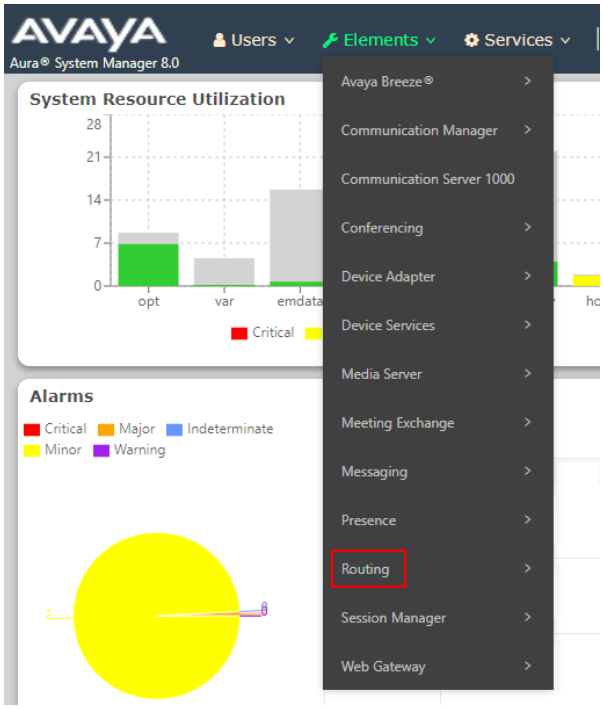
Ensure that you have completed the following configuration tasks:

- Configuring Avaya IX Workplace Client settings on page 344

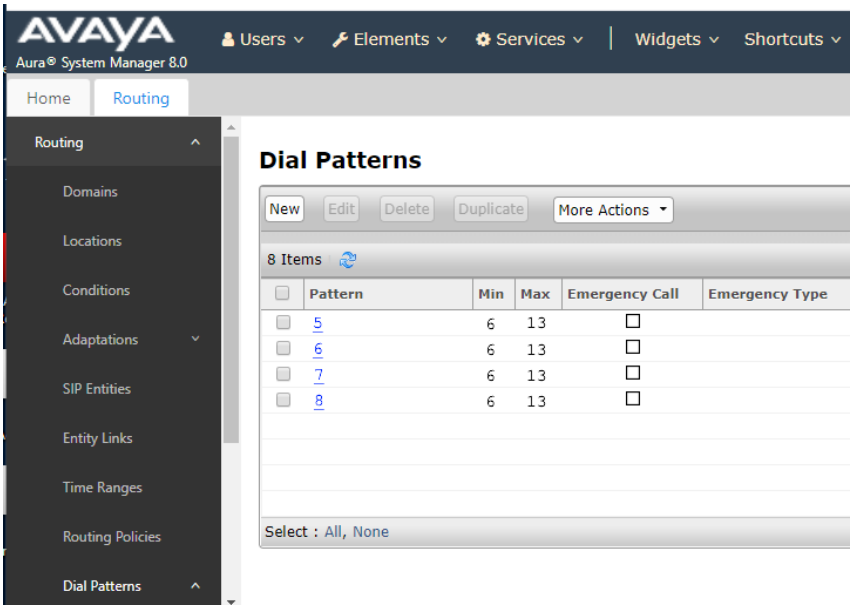
- Configuring the SIP Endpoint Managed Transfer Setting in Avaya Aura Communication Manager on page 347
- Configuring Dial Plan settings on page 349
- Configuring Equinox Management settings on page 350

Procedure

1. In Avaya Aura® System Manager, click **Elements** > **Routing** > **Dial Patterns**.

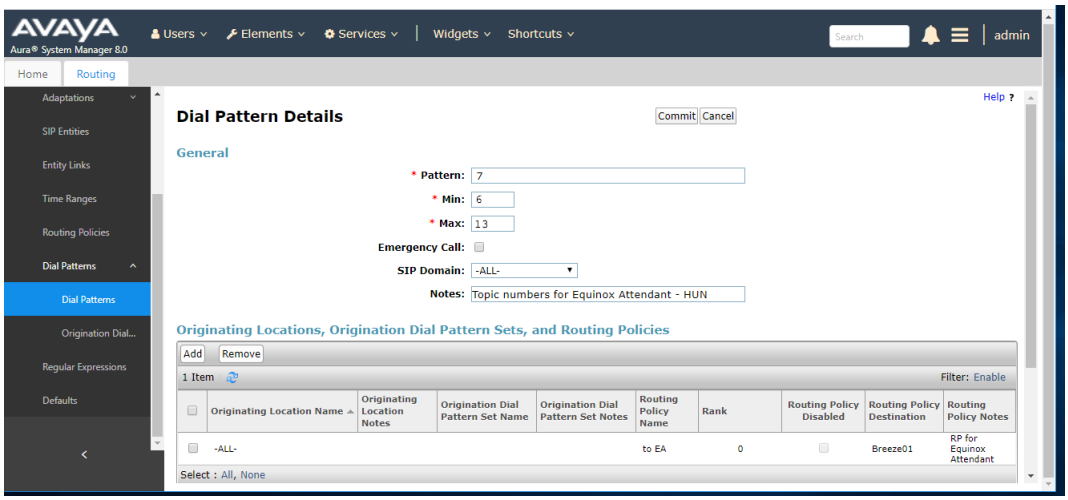


2. Configure the SIP trunk prefix (**7** in the following image, configured in the **Virtual Meeting ID Prefix** field on the **Meeting Policies** page; see Configuring Equinox Management settings on page 350.



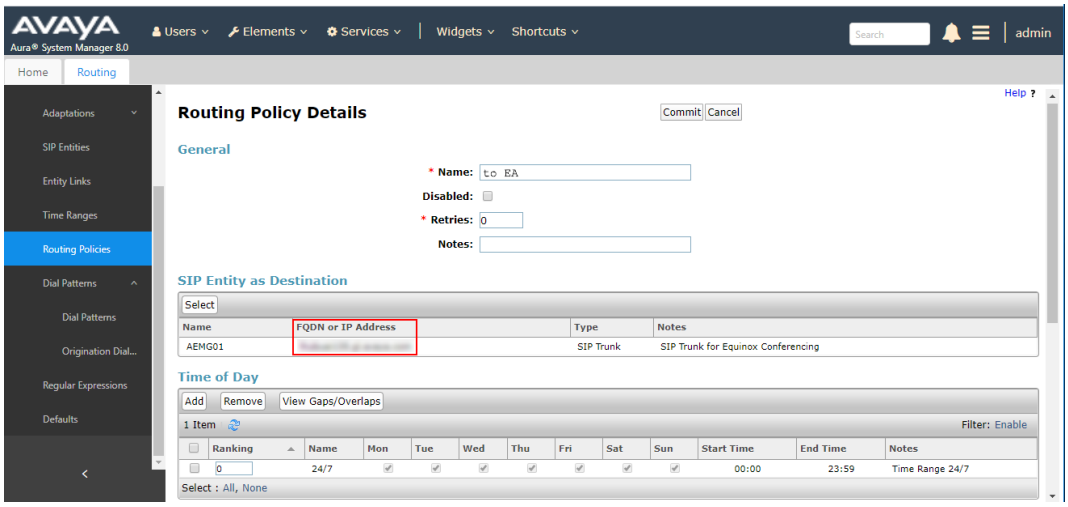
3. Select the relevant pattern.

   The system displays the **Dial Pattern Details** page.



4. In the **Originating Locations and Routing Policies** section, select the routing policy that routes to Equinox Management.

   The system displays the **Routing Policy Details** page, with the IP Address of the Equinox Management environment which is the destination of the routing policy.



Related links

Working with Equinox ad hoc conferencing on page 343

Escalating to a multipoint conference for a multiparty call using Avaya IX™ Workplace Client

About this task

During a point-to-point call, you can create an ad hoc conference by dragging additional participants into the call using Avaya IX™ Workplace Client. The conference moves to your virtual room, and the selected participants are added to the conference.

Alternatively, you can create an ad hoc conference that takes place in a temporary virtual room, which closes when the conference is finished. You would select this option if your virtual room is occupied, for example. When using this option, you must configure relevant settings in Equinox Management (see Configuring Equinox Management settings on page 350) and System Manager (see Configuring System Manager settings on page 351), in addition to the configuration tasks listed below.

Before you begin

Ensure that you have completed the following configuration tasks:

- Configuring Avaya IX Workplace Client settings on page 344
- Configuring the SIP Endpoint Managed Transfer Setting in Avaya Aura Communication Manager on page 347
- Configuring Dial Plan settings on page 349

Procedure

1. Create a point-to-point call in Avaya IX™ Workplace Client.

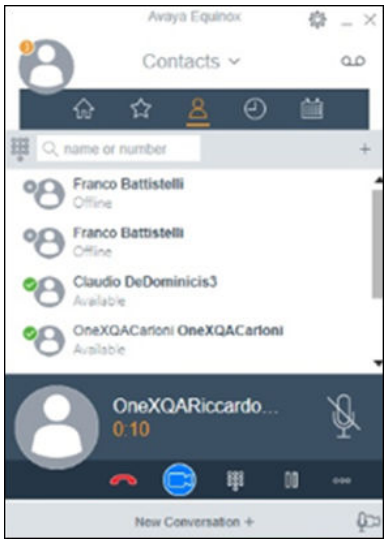


Figure 122: Point-to-point call

2. Drag and drop the relevant contact onto the active conversation.

   The system displays the following confirmation pop-up:

Figure 123: Confirmation pop-up

3. Click **Merge** to merge the contact with the existing call.

   The multipoint conference is activated, and all participants appear in Avaya IX™ Workplace Client.

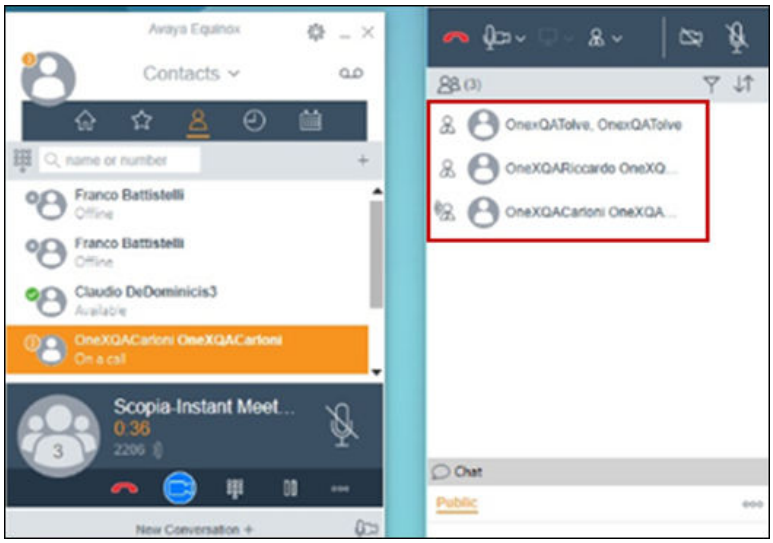


Figure 124: Multipoint conference

Related links

Working with Equinox ad hoc conferencing on page 343

Chapter 10: Configuring shuffling in Avaya Communication Manager

About this task

The system supports the following two shuffling configurations:

- A
  - Direct IP-IP Audio connection = y
  - Initial IP-IP Direct Media = y
  - SIP Endpoint Managed Transfer = y
- B
  - Direct IP-IP Audio connection = y
  - Initial IP-IP Direct Media = y
  - SIP Endpoint Managed Transfer = n

Configuration A is recommended for the Communication Manager that is not used for the Avaya Aura® Call Center Elite application.

Configuration B is recommended for the Communication Manager that is used for the Avaya Aura® Call Center Elite application.

Procedure

1. Access the Communication Manager configuration in the terminal emulator.
2. Set the configuration fields on the **Signaling Group** page as shown in the following figure.

```
change signaling-group 1                                        Page   1 of   3
                              SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n         Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority Video? y        Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM                       Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr            Far-end Node Name: sv-sm
 Near-end Listen Port: 5061           Far-end Listen Port: 5061
                                   Far-end Network Region: 1

Far-end Domain: [redacted]
                                      Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate          RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload     Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3            IP Audio Hairpinning? n
         Enable Layer 3 Test? y          Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n     Alternate Route Timer(sec): 6
```

3. Set the **SIP Endpoint Managed Transfer** field on the **Feature-Related System Parameters** page as shown in the following figure.

```
change system-parameters features                               Page  19 of  19
                      FEATURE-RELATED SYSTEM PARAMETERS
IP PARAMETERS
              Direct IP-IP Audio Connections? y         IP Audio Hairpinning? y
                     Synchronization over IP? n Allow SIP-H323 Video in SDES? n
    Initial INVITE with SDP for secure calls? y
              SIP Endpoint Managed Transfer? n

  Expand ISDN Numbers to International for 1XCES? n

CALL PICKUP
  Maximum Number of Digits for Directed Group Call Pickup: 4
                  Call Pickup on Intercom Calls? y     Call Pickup Alerting? y
     Temporary Bridged Appearance on Call Pickup? n     Directed Call Pickup? y
                     Extended Group Call Pickup: none
                  Enhanced Call Pickup Alerting? y
 Enhanced Call Pickup Delay Timer (sec.) Display: 1     Audible Notification: 15
   Call Pickup for Call to Coverage Answer Group? n
                      Display Information With Bridged Call? y
  Keep Bridged Information on Multiline Displays During Calls? y
                 PIN Checking for Private Calls? n
```

Chapter 11: Log server settings

Configuring the Log server settings

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Servers** > **Log Server**.
3. Enter the log server FQDN or IP address and port.
4. Click **Apply**.
5. Do one of the following:

Choice Option	Choice Description
Configure a secure connection using a different CA for the Log server on page 359.	The connection is a *secure connection* using a *different* CA than the one used for Equinox Management.
Configure a secure connection using the same CA for the Log server on page 361.	The connection is a *secure connection* using the *same* CA than the one used for Equinox Management.
Configure a non-secure connection for the Log server on page 363.	The connection is a non-secure connection.

Configuring a secure connection using a different CA for the Log server

Before you begin

Perform Configuring the Log server settings on page 359.

Procedure

1. It is recommended to rename the remote syslog server CA file to `rsyslog_remote_ca.crt` before you import it.
2. Click **Settings** > **Security** > **Certificates** > **Advanced** > **Import**.
3. Select the `rsyslog_remote_ca.crt` file.

4. Click **Add**.
5. Click **Apply**.
6. Log in to the vSphere console as the root user.
7. Run the following command to configure the secure connection:

```
/opt/avaya/pmgr/external-scripts/jitc/pmgr-remote-syslog.sh syslog_remote_ip:port
tls certificte-name-during-import
```

Example

To configure the tls connection to port 1468 on remote IP address 10.0.0.15 using CA named rsyslog_remote_ca.crt.

```
/opt/avaya/pmgr/external-scripts/jitc/pmgr-remote-syslog.sh 10.0.0.15:1468 tls
rsyslog_remote_ca.crt
```

Next steps

- Configuring a SysLog Server with TLS (SSL) on page 360.
- If you want to use a third party certificate, you must import the certificate into Equinox Management, see Configuring a SysLog Server with TLS on page 360.

Configuring a SysLog Server with TLS (SSL)

Before you begin

CA must be set up.

Procedure

1. Install the rsyslog-gnutls package.

```
yum install rsyslog-gnutls
```

2. Create an Equinox Management CA certificate for your syslog server, see Creating and uploading Equinox Management's certificate for videoconferencing components on page 192.
3. Copy the following to the syslog server:
   - ca.pem
   - machine-key.pem
   - machine-cert.pem
4. To configure the server, you must tell it where the certificate files are, to use the gtls driver and start up a listener in the rsyslog.conf. See the following example.

```
#make gtls driver the default
$DefaultNetstreamDriver gtls
# certificate files
$DefaultNetstreamDriverCAFile /path/to/contrib/gnutls/ca.pem
$DefaultNetstreamDriverCertFile /path/to/contrib/gnutls/cert.pem
```

```
$DefaultNetstreamDriverKeyFile /path/to/contrib/gnutls/key.pem

$ModLoad imtcp # load TCP listener

$InputTCPServerStreamDriverMode 1 # run driver in TLS-only mode
$InputTCPServerStreamDriverAuthMode anon # client is NOT authenticated
$InputTCPServerRun 10514 # start up listener at port 10514
```

5. Upload the ca.pem (the root certificate of the CA) to Equinox Management, see Importing a CA certificate on page 213.
6. Restart the rsyslog service with the following command.

   ```
   service rsyslog restart
   ```

7. Configure the audit server.
8. Log onto the syslog server you created before and use tail to monitor the audit log with the following command.

   ```
   tail -f /var/log/messages
   ```

Configuring a secure connection using the same CA for the Log server

Before you begin

Perform Configuring the Log server settings on page 359.

Procedure

1. Log in to the vSphere console as the root user.
2. Run the following command to configure the secure connection:

   ```
   /opt/avaya/pmgr/external-scripts/jitc/pmgr-remote-syslog.sh syslog_remote_ip:port
   tls
   ```

Example

To configure the tls connection to port 1468 on remote IP address 10.0.0.15 using the Equinox Management CA certificate.

```
/opt/avaya/pmgr/external-scripts/jitc/pmgr-remote-syslog.sh 10.0.0.15:1468 tls
```

Next steps

- Configuring a SysLog Server with TLS (SSL) on page 360
- If you want to use a third party certificate, you must import the certificate into Equinox Management, see Importing third-party root CA and intermediate CA certificates on page 196.

Configuring a SysLog Server with TLS (SSL)

Before you begin

CA must be set up.

Procedure

1. Install the rsyslog-gnutls package.

```
yum install rsyslog-gnutls
```

2. Create an Equinox Management CA certificate for your syslog server, see Creating and uploading Equinox Management's certificate for videoconferencing components on page 192.
3. Copy the following to the syslog server:
   - ca.pem
   - machine-key.pem
   - machine-cert.pem
4. To configure the server, you must tell it where the certificate files are, to use the gtls driver and start up a listener in the rsyslog.conf. See the following example.

```
#make gtls driver the default
$DefaultNetstreamDriver gtls
# certificate files
$DefaultNetstreamDriverCAFile /path/to/contrib/gnutls/ca.pem
$DefaultNetstreamDriverCertFile /path/to/contrib/gnutls/cert.pem
$DefaultNetstreamDriverKeyFile /path/to/contrib/gnutls/key.pem

$ModLoad imtcp # load TCP listener

$InputTCPServerStreamDriverMode 1 # run driver in TLS-only mode
$InputTCPServerStreamDriverAuthMode anon # client is NOT authenticated
$InputTCPServerRun 10514 # start up listener at port 10514
```

5. Upload the ca.pem (the root certificate of the CA) to Equinox Management, see Importing a CA certificate on page 213.
6. Restart the rsyslog service with the following command.

```
service rsyslog restart
```

7. Configure the audit server.
8. Log onto the syslog server you created before and use tail to monitor the audit log with the following command.

```
tail -f /var/log/messages
```

Configuring a non-secure connection for the Log server

Before you begin

Perform Configuring the Log server settings on page 359.

Procedure

1. Log in to the vSphere console as the root user.
2. Run the following command to configure the non-secure connection:

```
/opt/avaya/pmgr/external-scripts/jitc/pmgr-remote-syslog.sh syslog_remote_ip:port
```

Example

To configure the tls connection to port 1468 on remote IP address 10.0.0.15.

```
/opt/avaya/pmgr/external-scripts/jitc/pmgr-remote-syslog.sh 10.0.0.15:1468
```

Chapter 12: Tracking system usage with reports

The reports in Equinox Management provide information about your video network, including the frequency of videoconferences and device usage. Reports are an essential part of managing and administering your video network, and can be used to reassess bandwidth policies, decide which endpoints should always use the highest bandwidth (even in poor network conditions), or even decide whether you should switch to a distributed deployment topology.

Related links

About types of Equinox Management reports on page 364
Generating a report on page 369
Configuring Call Detail Records on page 376

About types of Equinox Management reports

There are many reasons why you may want to view and analyze specific reports. We list a few examples in the report descriptions below:

- **Calls** (**Multipoint** or **Point-to-Point**): Shows the total number or duration of videoconferences, for either meetings with more than two endpoints (**Multipoint**) or calls between two endpoints (**Point-to-Point**).

  Use this to track trends of videoconference usage, such as identifying the most popular time of day for calls (peak usage time), the average meeting duration, or average number of participants per meeting.

  For example, you can respond by implementing maximum bandwidth ceilings at different times or different days of the week. You may even decide to use off-site media servers at specific times of day to help with the load.

  - **Multipoint** — Generates a graph and a table on the screen using a date range you select, and you can save them as a PDF. Expand the **Advanced** section to select the following criteria:
    - Category
    - Sub-Category
    - Display by

- Locations

For a complete list of the table fields, see Equinox Management reports fields on page 474.

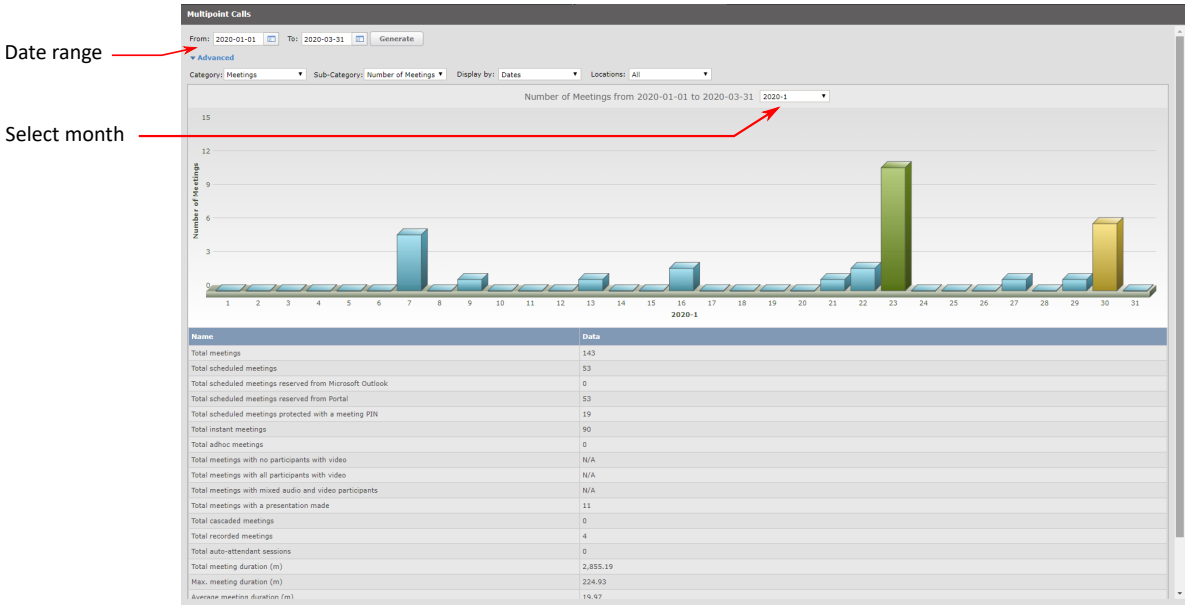


Figure 125: Multipoint Calls graph with table

- **Point-to-Point** — Generates a graph and a table on the screen that you can save as a PDF.

- **Device Usage**: Shows the total number or length of calls for one or more devices, the average capacity usage of a server, or data on new Avaya IX™ Workplace Client installations for a date range. For maximum capacity, see the **Peak Usage** report.

  Use this to track trends of device usage, such as the number of calls hosted by the most active media servers or the number of calls an endpoint participated in.

  After viewing the report results, you may want to:

  - Decrease the bandwidth of endpoints that are frequently used for very long durations.
  - Change your topology to allocate resources differently among various locations.

    For example, if you see that a media server is consistently close to reaching its full capacity, you may want to deploy more media servers in this location or implement cascading to share the load with other media servers. If cascading is already enabled, you can reserve additional resources for cascading media servers (see Increasing MCU capacity by cascading multiple MCUs on page 85).

  - **Endpoints** — Generates a device usage graph and a table on the screen using a date range you select, and you can save them as a PDF. You can select the endpoint by the following criteria:

    - Most used

    - Less used
    - <By name>

    Expand the **Advanced** section to choose a sort order and select the following criteria:

    - Number of calls
    - Call duration (m.)
    - Locations

  - **Equinox Media Servers** — Generates a device usage graph and a table on the screen using a date range you select, and you can save them as a PDF. You can select the device by the following criteria:

    - Most used
    - Less used
    - <By name>

    Expand the **Advanced** section to choose a sort order and select the following criteria:

    - Number of calls
    - Call duration (m.)
    - Locations

  - **Gateways** — Generates a device usage graph and a table on the screen using a date range and device name you select, and you can save them as a PDF.
  - **Unified Portals** — Generates a device usage graph and a table on the screen using a date range you select, and you can save them as a PDF.

- **Meeting Statistics**: Use this to track meeting trends and which meeting features are most used. For example, you can see how often various meeting types were used, how many meetings were recorded and how many were cascaded.

  The reports include a detailed breakdown of the way people in your organization are participating in videoconferences:

  - Total number of meetings, with a breakdown into scheduled and instant meetings (initiated spontaneously).
  - Number of meetings that were cascaded among multiple media servers.
  - Number of meetings that were recorded or used the Auto-Attendant (IVR) function.
  - Total meeting duration for all meetings combined.
  - Maximum and average duration of meetings.
  - Maximum and average number of calls (participant connections) within one meeting.

  You can use meeting reports to show the impact of introducing videoconferencing on your organization and how often employees use its services.

- **General** — Generates two pie charts and a table on the screen using a date range you select showing how many times each meeting type (media server service) was used, and the breakdown between scheduled and instant meetings.

  If you see that most meetings were instant and not scheduled, you may want to provide users with more information about how and why to schedule meetings (to make sure that the required resources are available for the meeting).

  If there is a frequently used meeting type that you did not already synchronize across all media servers, you may want to do so to provide more resources for this meeting type (see Synchronizing media server meeting types with Equinox Management on page 76). You can save the pie charts and table as a PDF.

- **Virtual Rooms**:

  Comprises the following tabs:

  - **Usage Statistics** — Generates a graph and a table on the screen using a month and year you select showing the number of meetings and total time spent on calls for one or more virtual rooms in the month, and is used to track the activity of virtual rooms. If, for example, you see that many users are using virtual rooms extensively, you may want to roll out virtual room ownership to more users in your organization. You can export the data as a CSV spreadsheet, or save as a PDF.
  - **Individual Usage** — Generates a bar graph on the screen for one month using a date range you select showing the number of meetings on each day of the month.

    Expand the **Advanced** section to select the following criteria:

    - Number of meetings
    - Meeting duration (m)
    - <Display order>

    You can save the graph as a PDF.
  - **Usage Summary (CSV)** — Generates a CSV spreadsheet. For a complete list of the table fields, see Equinox Management reports fields on page 474.
  - **Inventory (CSV)** — Generates a CSV spreadsheet. For a complete list of the table fields, see Equinox Management reports fields on page 474.

- **Meeting Size** — Use this to track the range of meeting sizes across the organization.

  Based on the report results, you may want to:

  - Promote video in your organization, if you see that there are only small meetings. If you see that there are many large meetings, you can use this report to show how implementing videoconferencing saved money on transportation costs.
  - Limit the number of maximum participants for instant meetings (see Defining Video Usage Defaults on page 433). This requires users to reserve resources for larger meetings by scheduling them beforehand.

    You can save the graph as a PDF.

- **Meeting Duration** — Generates a pie chart and a table on the screen using a date range you select to show the length of meetings across the organization.

  Based on this analysis, for example, if you see that most meetings last longer than 30 minutes, you can increase the default end time for both scheduled and instant meetings (see Defining Video Usage Defaults on page 433). Or, for example, if management decides to cut on bandwidth costs and reports show some video meetings last several hours, you can limit the default meeting duration to help participants focus on shorter meetings.

  You can save the graph as a PDF.

- **Reserved Meetings** — Generates and saves a CSV spreadsheet using a date range you select. For a complete list of the table fields, see Equinox Management reports fields on page 474.

- **System Reports** — Shows the maximum capacity reached per device (**Peak Usage** report), or the average/peak bandwidth used by video network devices, internally and cross-location (**Bandwidth Used** report). To see a device's average usage, see the **Device Usage** report.

  For example, you can view a media server's peak capacity over a specific time period, or track the bandwidth used for each location.

  You can use this analysis to re-evaluate whether your current topology suits your organization. For example, if you see that a media server is consistently reaching capacity, you may want to add another media server. If you see that a location is consistently reaching its bandwidth, you may want to adjust your bandwidth policies or upgrade the bandwidth for this location. You can save the report as a PDF.

- **Advanced**:

  Export Raw Data. Saves a ZIP archive with Meetings with participants and Point to Point ZIP archives with CSV spreadsheets.

- **VaaS Billing** — For service provider VaaS (Video as a Service) deployments, this option enables service providers (not organization administrators) to see the peak usage of virtual meeting rooms per customer over a period of time predetermined by the administrator. Service providers can use this report for calculating how to bill customers. You access this report via the **Export Raw Data (CSV)** report option.

  This report is similar to the **Peak Usage** report mentioned above; however, it shows the peak usage of virtual meeting rooms for each customer as opposed to the aggregate peak usage of devices for all customers.

To generate a report, follow the instructions described in Generating a report on page 369.

Figure 126: Report data on page 369 shows a few examples of generated reports. Depending on the report, the data is displayed as either a line graph, bar graph or a pie chart.

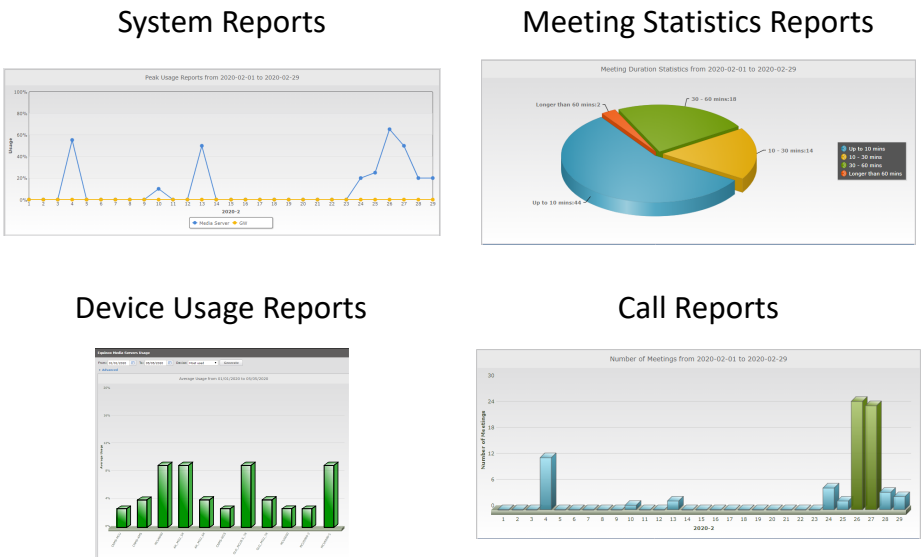


Figure 126: Report data

For service provider (multi-tenant) deployments, the reports you can generate depend on your role in the deployment. Service providers can generate all reports except for **Virtual Room** and **Endpoint** reports. Organizations using a service provider can generate all reports except for **System**, **Media Server**, **Gateway**, and **VaaS Billing** reports.

Related links

Tracking system usage with reports on page 364

Generating a report

About this task

This procedure describes how to generate Equinox Management reports based on various criteria. For example, you can generate a report to see the call duration of all meetings that included a specific endpoint within a time period. For an explanation of all reports, see Tracking system usage with reports on page 364.

Procedure

1. Access the Equinox Management administrator portal.

   The system displays the **Dashboard** tab.

2. You can access the **Device Usage** report directly from the dashboard. Click the link as shown in the figure.

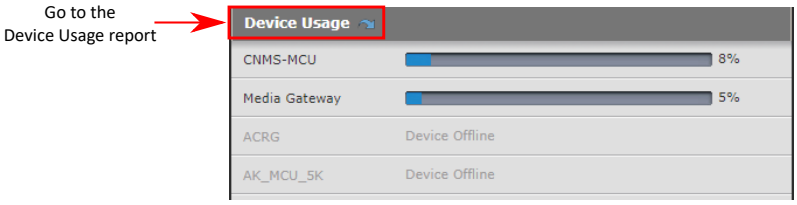


Figure 127: Accessing reports from the Dashboard

3. To access all other reports, click the **Reports** tab.
4. Click the report type in the sidebar menu. For an explanation of all reports, see Tracking system usage with reports on page 364.

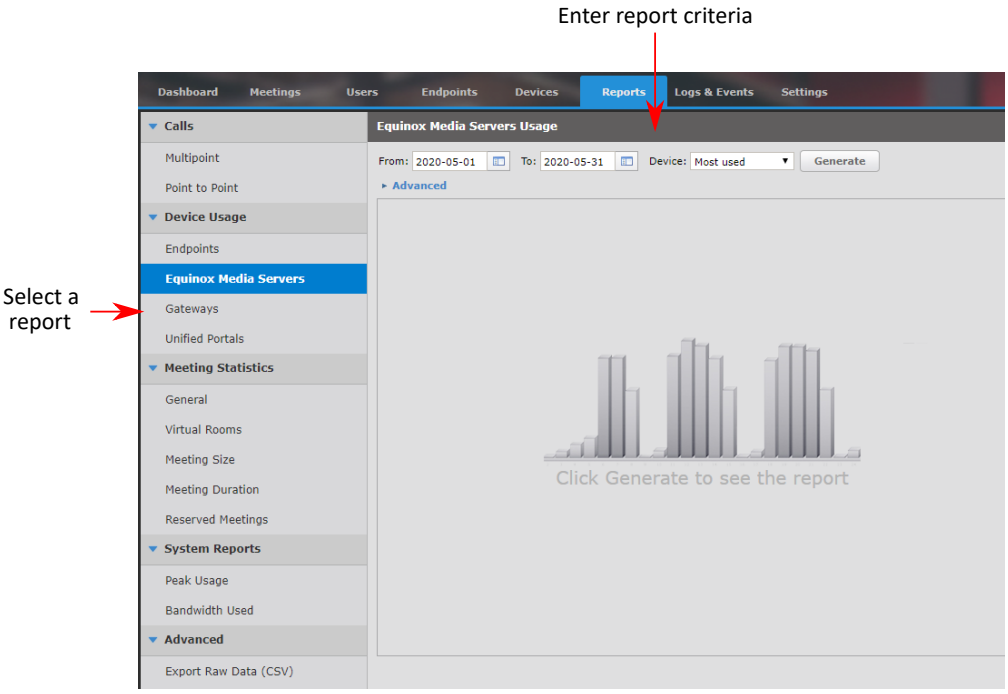


Figure 128: Selecting the report type

5. Enter the required criteria in the fields above the report area (see Table 60: Setting basic report criteria on page 371).

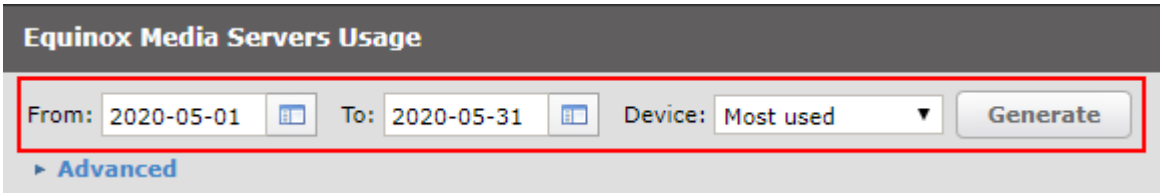


Figure 129: Setting basic report criteria

Not all the fields are visible for every type of report.

Table 60: Setting basic report criteria

Field Name	Description	Reports
From	Select a start date for the report.	All
To	Select an end date for the report.	All
Endpoint/Device	Select the devices to be included in your report: • **Most Used** to include only the most active endpoints/ media servers in the report. • **Least Used** to include only the least active endpoints/ media servers in the report. • **Select** and choose up to five endpoints, or a specific endpoint for which you want to generate the report. The most and least used devices can refer to either the number of calls, call duration, or percentage of total capacity used (media servers only). You can define this by selecting **Advanced** (see step 6 on page 371).	**Device Usage** reports for: • **Endpoints** • **Media Servers**
Device	Select **All** or the specific device for which to generate the report.	**Device Usage** reports for: • **Gateways**
Virtual Room	Select up to five virtual rooms for which you want to generate the report, and click **OK**.	**Virtual Rooms** report
Device Type	Select **All** or specify the type of video network device (media server or gateway) for which to generate the report.	**Peak Usage** report
Locations	This field is relevant only for deployments with multiple locations. Select **All** or choose a specific location from the list.	**Bandwidth Used** report

6. (Optional) Click **Advanced** to narrow the focus of your report by entering additional criteria. For example, you can view the data for a specific location only, or by day of the week.

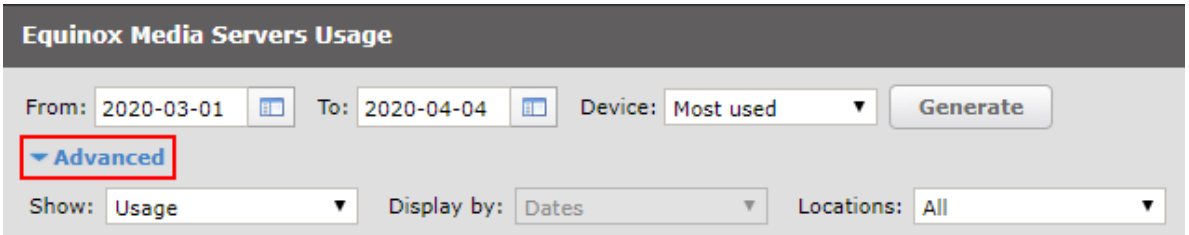


Figure 130: Setting advanced report criteria (example)

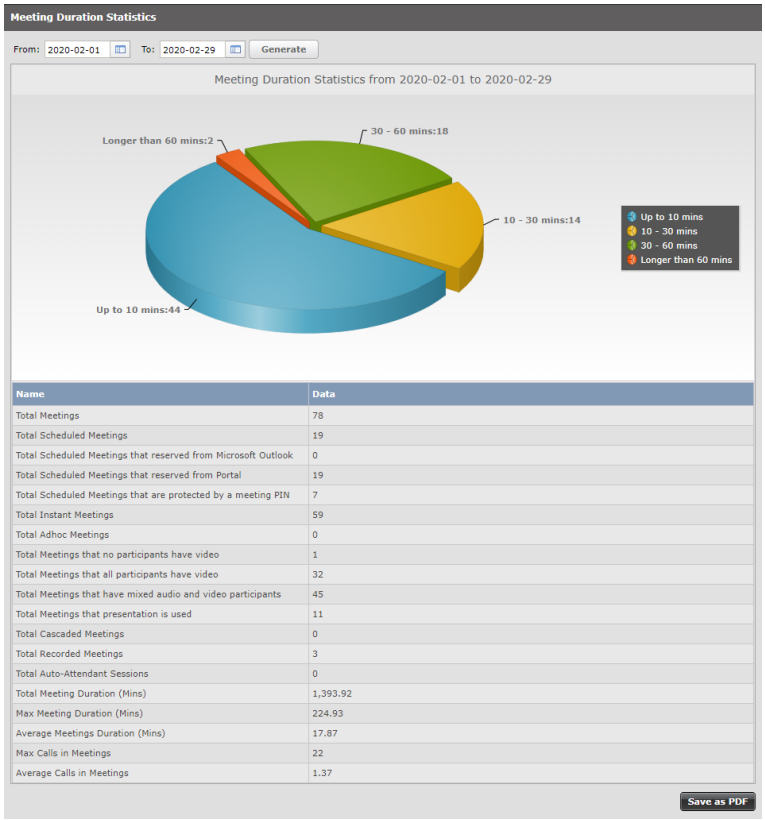
The advanced criteria varies according to the report you are generating, and is available only for **Calls**, **Device Usage**, and **Virtual Room** reports.

Table 61: Setting advanced report criteria

Field Name	Description
Show	Select the information to display in the report, as follows: • **Number of Calls**: Shows the number of active endpoint connections in calls. For multipoint meetings, this refers to the number of endpoints connected to the MCU. Each point-to-point call includes only one connection between two endpoints, and is counted as one call. • **Number of Meetings**: Shows the number of meetings matching the report criteria (only available for **Multipoint** reports). • **Call Duration (Mins)**: Shows the total call duration, in minutes, matching the report criteria. • **Usage**: Shows the percentage of total connections used by the device (available for media servers and gateways). The options available depend on the report selected.
Display by	Select how to display the data: by date, time of day, day of week or month, or month of the year. For example, select **Time of the day** to see for which hours the highest number of meetings are held.
Locations	This field is relevant only for deployments with multiple locations. Select **All** or choose a specific location from the list.

7. Click **Generate**.

   The system displays reports in either graph or chart format, depending on the report.



Name	Data
Total Meetings	78
Total Scheduled Meetings	19
Total Scheduled Meetings that reserved from Microsoft Outlook	0
Total Scheduled Meetings that reserved from Portal	19
Total Scheduled Meetings that are protected by a meeting PIN	7
Total Instant Meetings	59
Total Adhoc Meetings	0
Total Meetings that no participants have video	1
Total Meetings that all participants have video	32
Total Meetings that have mixed audio and video participants	45
Total Meetings that presentation is used	11
Total Cascaded Meetings	0
Total Recorded Meetings	3
Total Auto-Attendant Sessions	0
Total Meeting Duration (Mins)	1,393.92
Max Meeting Duration (Mins)	224.93
Average Meetings Duration (Mins)	17.87
Max Calls in Meetings	22
Average Calls in Meetings	1.37

Decoding the report

Additional data

Save report as PDF

Figure 131: Example of a generated report

- You can view additional information below the graph or chart, such as the number of scheduled meetings, for **Meeting Statistic** reports (Figure 131: Example of a generated report on page 373).
- **Peak Usage** (for all or a specific device) line graphs have their own color scheme, shown directly below the graph:

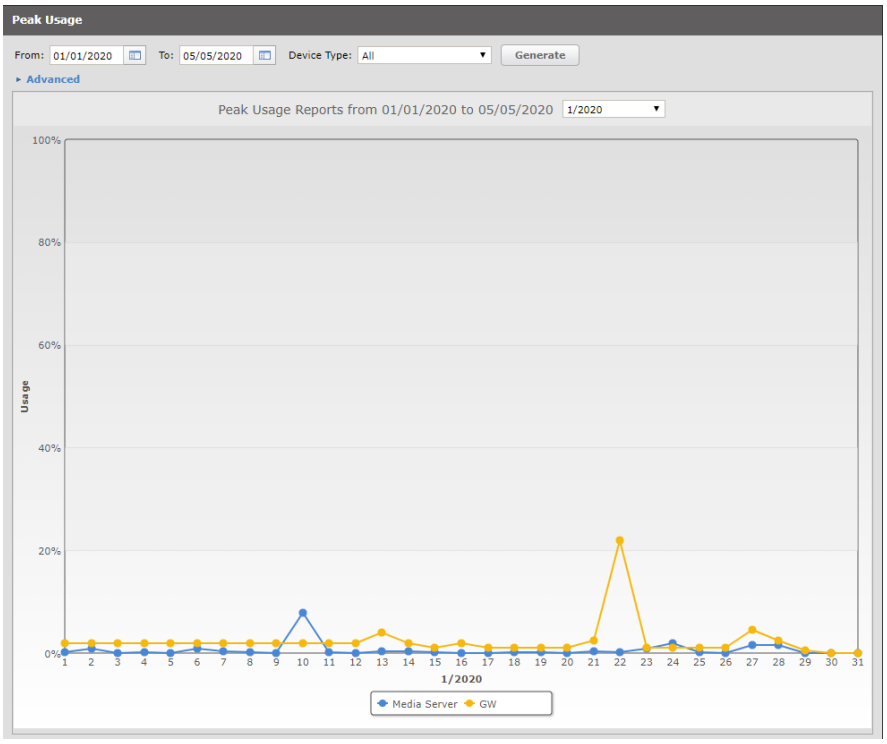


Figure 132: A report's color scheme

The graph shows the entire spectrum of usage for the selected type of device over the indicated time frame.

- For **Device Usage** reports:

  If the media server and endpoint report is based on most or least used devices, the report displays the average value. For **media server** reports based on all or a specific media server, the report displays both the average and peak values.

  Gateway **Device Usage** reports display both the average and peak values.

8. (Optional) Click **Save as PDF** to export your report to PDF (Figure 131: Example of a generated report on page 373).

   Or

   For further analysis of meeting data, you can save export it as a .csv file and view the details in Microsoft Excel. Click **Advanced** > **Export Raw Data (CSV)** from the sidebar menu, enter the required information (see Table 62: Exporting report data to a CSV file on page 375) and click **Generate**.

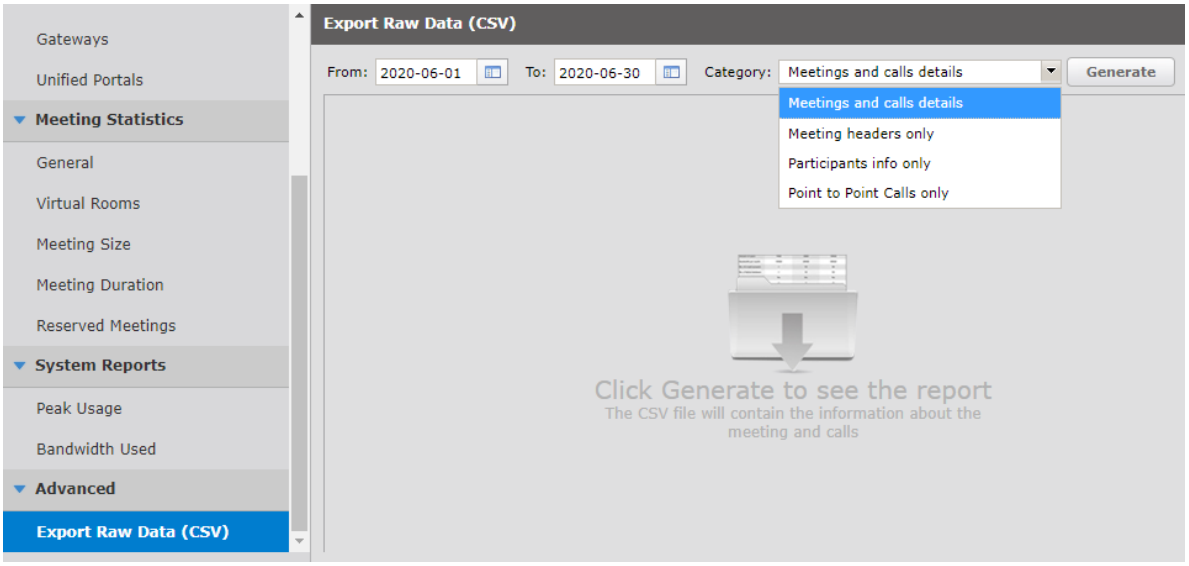


Figure 133: Exporting report data to a CSV file

Table 62: Exporting report data to a CSV file

Field	Description
From	Select a start date for the report.
To	Select an end date for the report.
Category	Select whether to generate data for meetings, calls, or both: • **Meeting headers only**: Includes the following details regarding multipoint meetings: the meeting ID and name (subject), duration and start time, the bandwidth used, the hosting media server, and the location. • **Meetings with participants info only**: Includes all the information for multipoint meetings listed in **Meeting headers only**, as well as information about each participant (identified as the party name) in the meeting. • **Point to Point calls only**: Includes the following details for calls between two participants only: the name and number of each participant, the duration and start time, the bandwidth consumed, and the location of the initiating endpoint. • **All**: Includes the **Meetings with participants info only** and **Point to Point calls only** reports, as two separate Microsoft Excel files.

Click **Download Now** to save the **.zip** file containing the CSV files.

Related links

Tracking system usage with reports on page 364

Configuring Call Detail Records

About this task

A Call Detail Record (CDR) contains comprehensive records of each call. With Equinox Management, you can create and store CDR reports in XML format. These records are useful for analyzing and tracking system usage, as well as for supporting diagnostics and billing.

Procedure

1. Access the Equinox Management administrator portal.
2. Click **Settings** > **Advanced** > **CDR Settings**.

   The system displays the **CDR Settings** page.

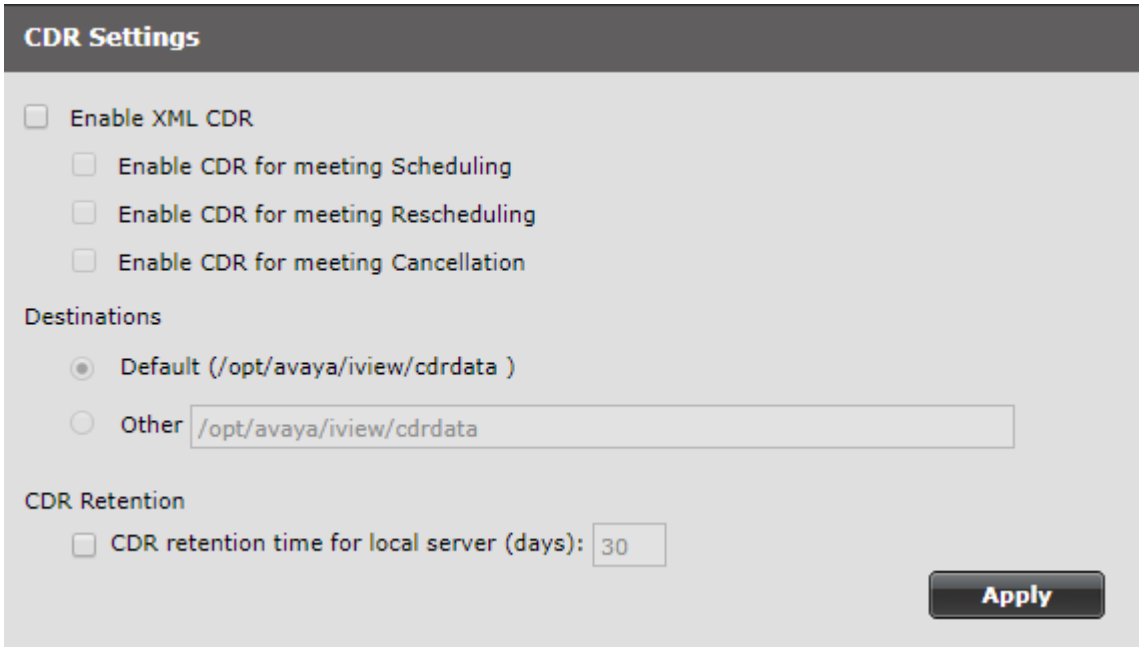


Figure 134: CDR Settings page

3. Select **Enable CDR XML**.
4. Configure the relevant settings:

Table 63: Configuring CDR

Field	Description
Enable CDR for meeting Scheduling	Records data related to meeting scheduling, such as which resources are reserved and which attendees and/or terminals are invited as part of scheduling.

Table continues…

Field	Description
Enable CDR for meeting Rescheduling	Records data related to meeting rescheduling, such as which resources are reserved and which attendees and/or terminals are invited as part of rescheduling.
Enable CDR for meeting Cancellation	Records whether a meeting was cancelled prior to its scheduled start time.

5. In the **Destinations** section, select the location of the CDR file on the PMGR server. Select **Default** to accept the default location (`/opt/avaya/iview/cdrdata`), or select **Other** to configure a custom location.
6. Select the CDR retention time for local server (days) check box to enable, disable or change the retention time.

   Range = 1 – 365 days

   Default for new installation = 365 days

   Default for upgrade from a release that does not support this setting is *disabled*
7. Click **Apply**
8. To access the CDR report:
   a. Using SFTP, connect to the PMGR server.

      The default login credentials for the `pmgradmin` account are:

      - **Username**: `pmgradmin`
      - **Password**: `password`

   b. Navigate to `/home/pmgadmin` and change the directory to the default location of the CDR file (`/opt/avaya/iview/cdrdata`), or to its custom location if previously specified.

   c. Download the XML files.

      For more information on the structure of the XML file, see *Reference Guide for Avaya Equinox® Management CDR Files*.

Related links

Tracking system usage with reports on page 364

Chapter 13: Maintaining your Videoconferencing Network

This section details to the ongoing administrator tasks required to maintain your video network, including backing up, restoring, and reflecting changes in the video devices and topology of your video network.

Related links

High Availability of Equinox Management on page 378
Upgrading, Backing up and Restoring Equinox Management on page 395
Daily Maintenance of your Video Network on page 421
Upgrading, Backing Up and Restoring Video Device Software on page 425
Defining Video Usage Defaults on page 433
Maintaining Scheduled Meetings on page 437
Disaster recovery in a geographic redundancy deployment on page 439
Retrieving the Customer Support Package on page 444

High Availability of Equinox Management

To provide high availability and continued service, you can deploy redundant Avaya Equinox® Management servers, in one of the following ways:

- Local redundancy

  Deploy two Equinox Management servers in the same location: a primary server and a secondary server. If the primary server fails, the secondary server automatically takes over without disrupting Equinox Management functionality (does not include load balancing).

- Geographic redundancy

  Deploy three Equinox Management servers. Set up two servers as primary/secondary servers in the same location (local redundancy), and deploy the third as an off-site backup server in a different location. You can manually activate this server if the other servers fail, ensuring continued service even if there is a major failure or disaster at the main location.

  Important:

We recommend configuring the backup server while the system is inactive. This is because a huge amount of data is transferred to the remote site, which can deplete network bandwidth resources.

Figure 135: Local and geographic redundancy on page 379 illustrates the different options of deploying Equinox Management redundancy.

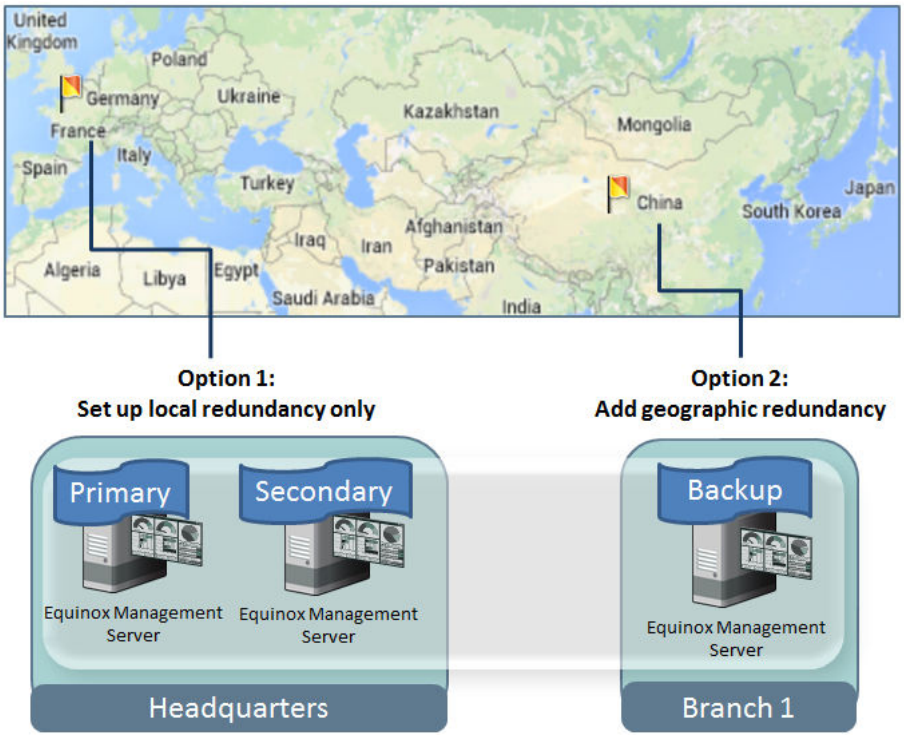


Figure 135: Local and geographic redundancy

Equinox Management's redundant solution requires a license, but does not require third-party load balancers. Data is continuously synchronized between all Equinox Management servers, including the internal database, system property files, and device upgrade packages.

Deploy your Equinox Solution by referring to component names rather than IP addresses. Using a server name (or FQDN), like *aemg.company.com*, reduces maintenance when servers switch to their backups.

Note:

For all deployments, you must use FQDNs. FQDNs are essential when using TLS.

Local redundancy can be deployed with an internal or external database. Geographic redundancy supports only the internal database. See *Deploying Avaya Equinox® Solution*.

Once Equinox Management's high availability is configured, you can view the redundancy status in real-time, including the current status and server addresses (see Monitoring Redundancy Status on page 386 for details).

Related links

Maintaining your Videoconferencing Network on page 378

Creating a Redundant Secondary Server for Equinox Management on page 380
Creating an Off-Site Backup Server for Equinox Management on page 384
Monitoring Redundancy Status on page 386
Manually promoting the off-site backup server on page 389
Restoring primary server from off-site backup server on page 392
Disabling Redundancy on page 394

Creating a Redundant Secondary Server for Equinox Management

About this task

You can deploy two Avaya Equinox® Management servers in the same location, one as the primary server and the other as a secondary server (local redundancy). If the primary server fails, the secondary server automatically takes over. For increased reliability, deploy a third server as an off-site backup (geographic redundancy). For details, see High Availability of Equinox Management on page 378.

This procedure describes how to deploy two Equinox Management servers in the same location for high availability (it does not include load balancing functionality). Even if you are deploying geographic redundancy, you must first set up local redundancy, as described below.

Before you begin

- Verify the same version of Equinox Management is installed on two separate physical servers, in the same location, connected on a local LAN and using the same subnet. Spanning across two locations connected by a cable or fiber is not supported.
- The Equinox Management servers must be able to ping the gateway.
- Decide on the primary Equinox Management server, and set up all video network devices and users on this server first, following the instructions in Initial configuration workflow on page 29.
- Allocate a new IP address as the public virtual IP address of both servers.
- Decide whether to deploy local redundancy or geographic redundancy (see High Availability of Equinox Management on page 378).

Important:

If you are securing your network using TLS, you must first configure redundancy and then generate and install your TLS certificates (see Securing your video network using TLS on page 181). Otherwise, you will need to reconfigure TLS on the other Equinox Management servers.

Procedure

1. Access the Equinox Management administrator portal.
2. Select the icon and then select **Redundancy Setup**.

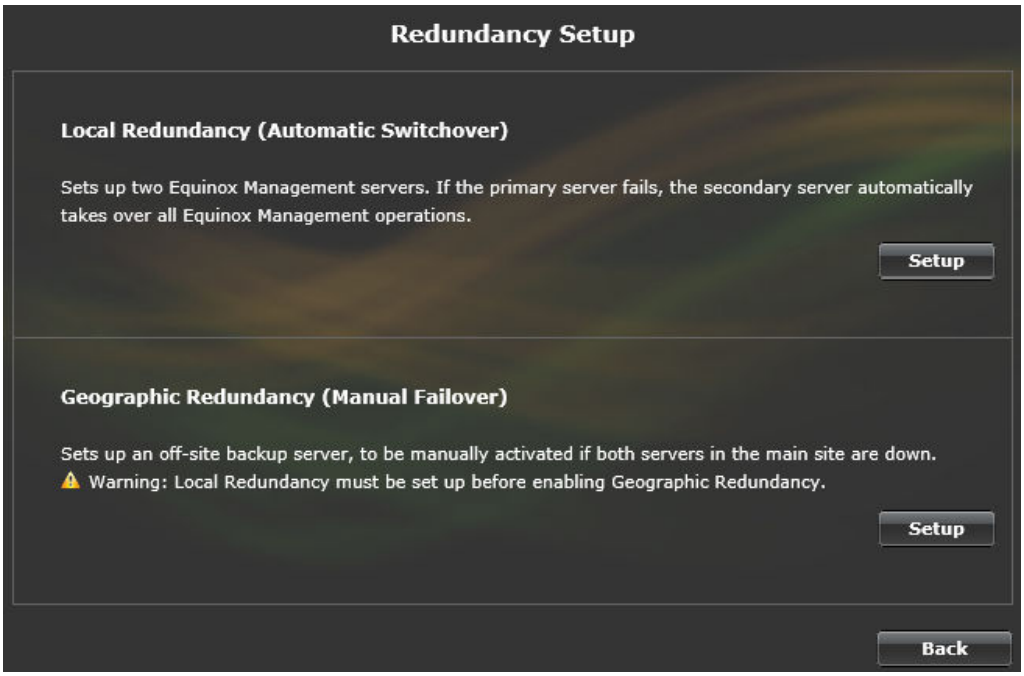


Figure 136: Setting up local redundancy

3. In the **Local Redundancy** area, select **Setup**.

   Even if you are deploying geographic redundancy, you must first set up local redundancy.

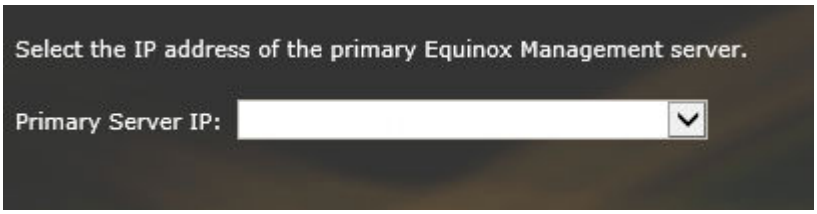


Figure 137: Selecting the primary server

4. Select the IP address of the primary Equinox Management server from the list, and select **Next**. The following page appears:

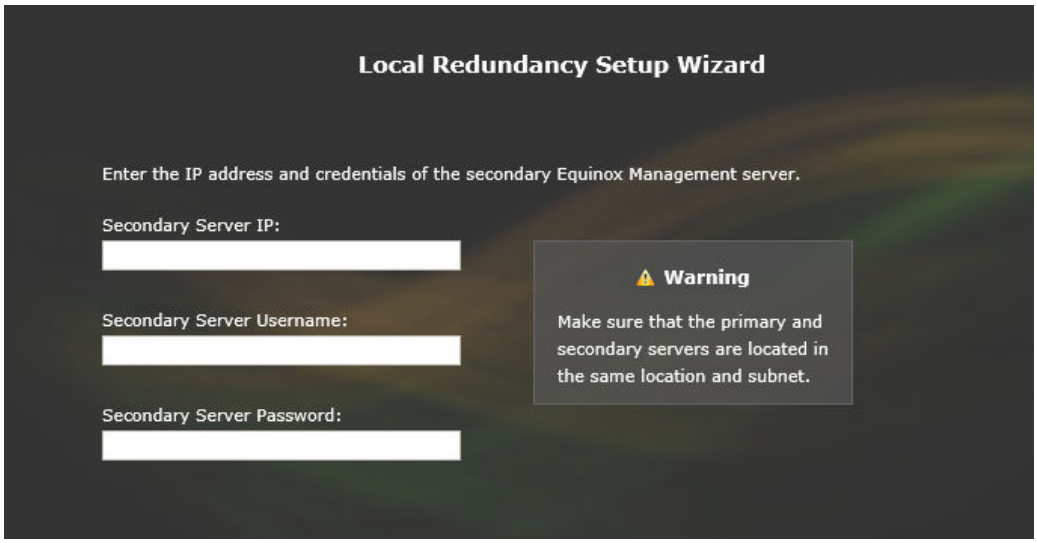


Figure 138: Setting up the secondary server

5. Enter the following information for the secondary Equinox Management server, and then select **Next**.

Table 64: Setting up the secondary server

Field	Description
Secondary Server IP	Enter the IP address of the secondary server.
Secondary Server Username	Enter the administrator login credentials required to access the secondary server.
Secondary Server Password	

6. Enter the virtual IP and FQDN as described below, and then select **Next**.

   This creates a common destination address to represent the redundant servers to other components.

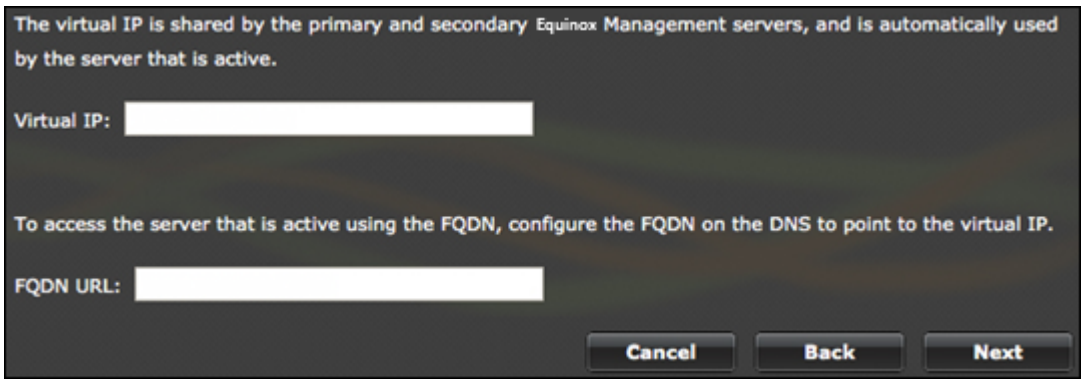


Figure 139: Setting up the virtual IP

Table 65: Setting up the virtual IP

Field	Description
Virtual IP	Enter the public virtual IP address representing both the primary and secondary Equinox Management servers to other components.
FQDN URL	Enter the URL that represents the virtual IP, as defined on your DNS server. If you are deploying an off-site backup server as well, this URL represents all redundant Equinox Management servers. We recommend accessing Equinox Management via its FQDN, which represents all Equinox Management servers and always redirects to the server that is currently active.

7. Enter the following settings for the subnet to which the primary and secondary Equinox Management servers belong, and then select **Next**.

   The primary server continuously pings the gateway to indicate that it is connected. If it fails to do so, the secondary server automatically takes over.

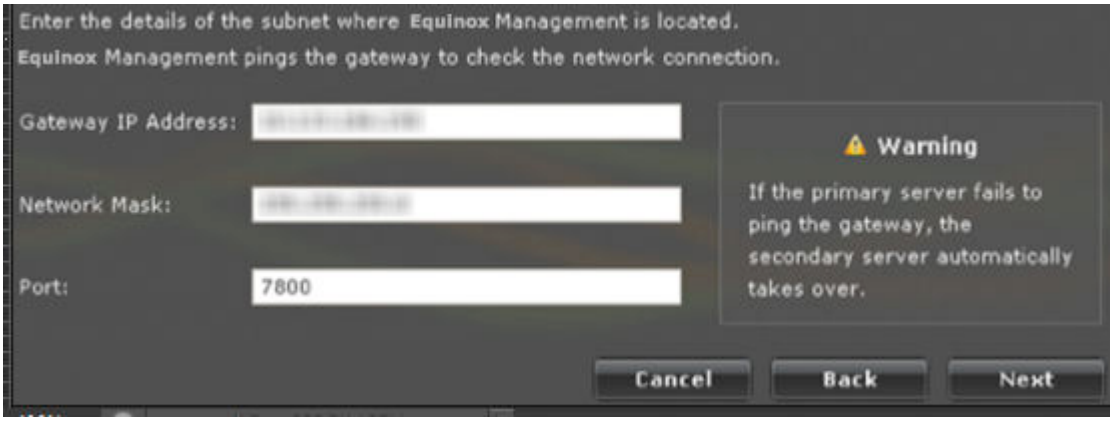


Figure 140: Configuring gateway settings

Table 66: Configuring gateway settings

Field	Description
Gateway IP Address	Enter the subnet's gateway (router) IP address.
Network Mask	Enter the dedicated subnet mask, which represents the range of IP addresses in the network.
Port	Enter the port Equinox Management uses to check whether the specific gateway is available.

8. Select **Proceed** to finish setting up local redundancy.

   The system confirms that the secondary server is now set up.

9. To test, access the Equinox Management cluster from a web browser by entering the URL of the newly assigned virtual IP or FQDN.

The dashboard shows the **System Information** section in the top right hand side of the screen listing the redundancy status (Figure 141: Redundancy status in System Information section of Dashboard on page 384). Select the **Active** link for details.

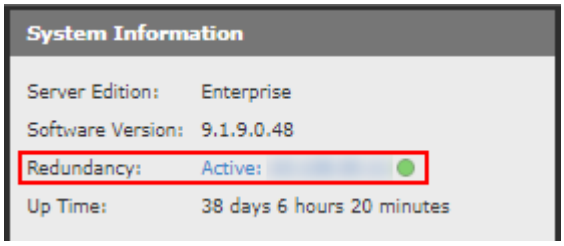


Figure 141: Redundancy status in System Information section of Dashboard

10. (Optional) You can now secure your network with TLS, using Equinox Management's FQDN (see Securing your video network using TLS on page 181).

    If you are deploying an off-site backup server, you can configure TLS now or after setting up the backup server.

11. (Optional) For increased reliability, add an off-site backup server in a different location (see Creating an Off-Site Backup Server for Equinox Management on page 384).

Related links

High Availability of Equinox Management on page 378

Creating an Off-Site Backup Server for Equinox Management

About this task

You can deploy two Avaya Equinox® Management servers in the same location, one as the primary server and the other as a secondary server (local redundancy). If the primary server fails, the secondary server automatically takes over. For increased reliability, deploy a third server as an off-site backup (geographic redundancy). For details, see High Availability of Equinox Management on page 378.

If the secondary server fails, you need to manually promote the backup server to become active (see Manually promoting the off-site backup server on page 389). We recommend accessing Equinox Management via its FQDN, which represents all Equinox Management servers and always redirects to the server that is currently active.

Equinox Management's internal database is synchronized between all redundant Equinox Management servers. You do not need to configure an additional database for the off-site backup server.

Important:

Geographic redundancy supports only Equinox Management's internal database.

Before you begin

- Set up two Equinox Management servers in the main site, as described in Creating a Redundant Secondary Server for Equinox Management on page 380.

- Verify that a third server (with the same version of Equinox Management) is installed in a different location.

Procedure

1. Access the Equinox Management administrator portal using the FQDN.
2. Select ≡ > **Redundancy Setup** (see Figure 142: Setting up geographic redundancy on page 385).

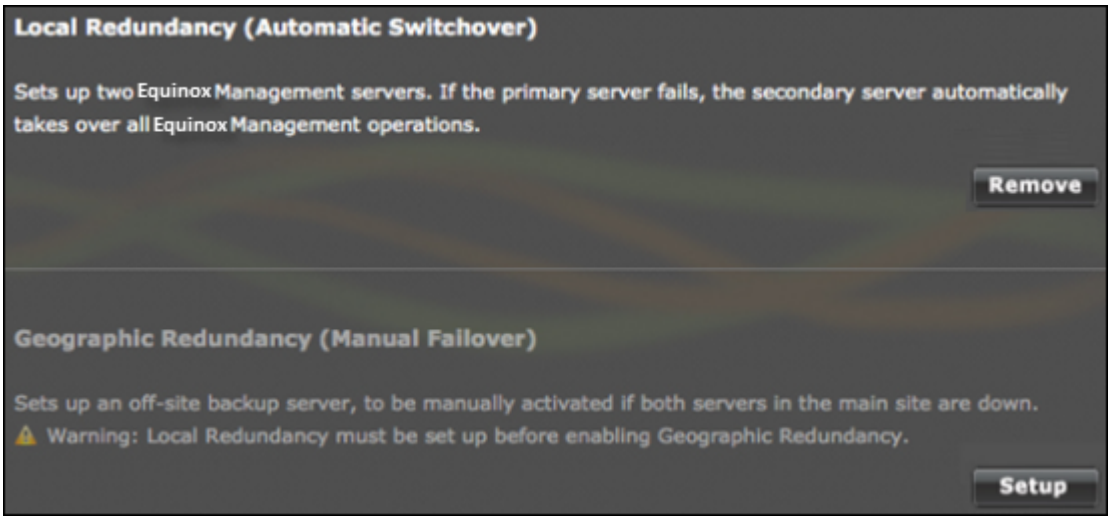


Figure 142: Setting up geographic redundancy

3. In the **Geographic Redundancy** area, select **Setup**.

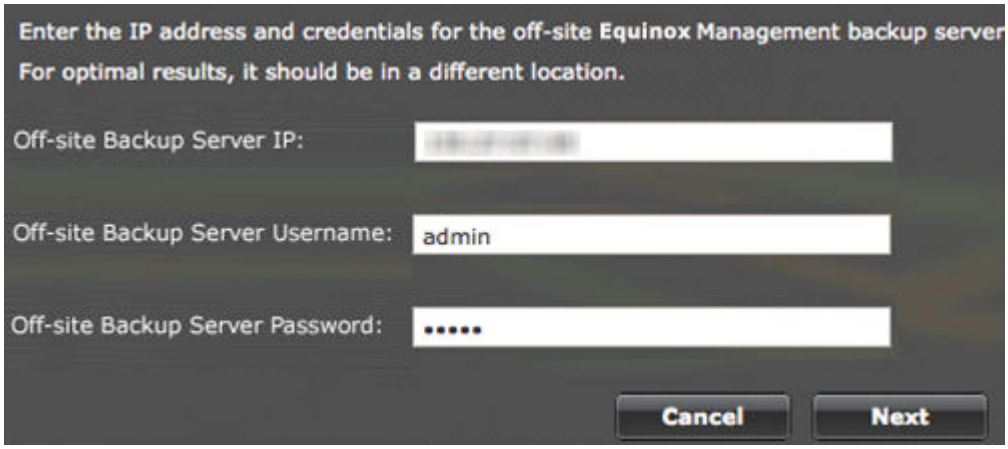


Figure 143: Setting up the backup server

4. Enter the following information for Equinox Management's off-site backup server, and then select **Next**.

Table 67: Setting up the backup server

Field	Description
IP Address	Enter the IP address of the off-site backup server.
Username	Enter the Equinox Management login credentials required to access the off-site backup server.
Password	

5. Select **Proceed** to finish setting up geographic redundancy.

   The system confirms that the off-site backup server is now set up.

6. Configure Equinox Management's FQDN records to enable timely re-configuration of the FQDN value from the HA pair to the Geographic Redundant instance. To facilitate this, configure the **Time To Live (TTL)** parameter on the DNS to 30 minutes. This ensures that when promoting the Geographic Redundant instance into production, subsequent DNS requests for the VIP FQDN are correctly routed to the Geographic Redundant instance.

   If you set the **Time To Live (TTL)** parameter to a value less than 30 minutes, DNS requests are sent more often but the access pressure on the DNS server increases. Therefore, it is recommended to set the **Time To Live (TTL)** parameter to 30 minutes.

7. (Optional) You can secure your network with TLS, using Equinox Management's FQDN (see Securing your video network using TLS on page 181).

Related links

High Availability of Equinox Management on page 378

Monitoring Redundancy Status

About this task

Once you configure redundancy, Equinox Management alerts you if it is not working properly. System administrators receive email alerts when:

- A switch occurs between the primary and secondary servers.
- The CPU on the active Equinox Management server reaches 100% (contact Customer Support to configure).

To customize the email alert, see Creating or Modifying an Alert Recipient Profile on page 295. Equinox Management also generates an alarm that is added to the event log, and can be forwarded to a third-party SNMP server (see Real-time Monitoring on page 291).

You can always check the redundancy status in the **System Information** area of the **Dashboard**:

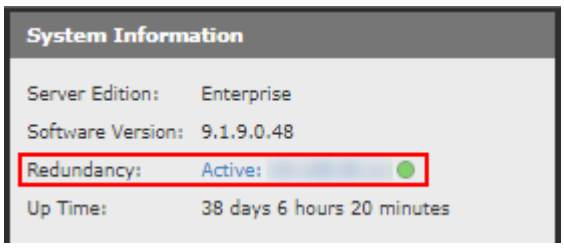


Figure 144: Redundancy status

The green icon indicates that the active server is currently connected and functioning properly.

The red icon indicates an error; select the **Active** link for details, including:

- Connection status of each redundant Equinox Management server
- IP address of the current active server
- Time that the server has been active
- Date of the last hot swap
- Details of the redundancy configuration (such as the IP address of the standby server, the virtual IP address, and the FQDN)
- Data synchronization status

Procedure

1. Access the Equinox Management administrator portal using the FQDN.
2. Navigate to the **System Information** area in the **Dashboard** tab (Figure 144: Redundancy status on page 387) to see the following information:

   Table 68: Basic redundancy details

Field Name	Description
Redundancy	The IP address for the Equinox Management server that is currently active. Typically, this is the IP address of the primary server, unless it is down. The green icon indicates that the active server is currently connected and functioning properly, and the red icon indicates a failure, either with one of the Equinox Management servers or with the database synchronization.
Up Time	The period of time that the current server has been active (since the last switch).
Last Switch	The time and date of the last switch between the redundant Equinox Management servers.

3. Select the IP address of the active server to view the following details:

Table 69: Monitoring redundancy status

Field Name	Description
Last Switch	The time and date of the last switch between the redundant Equinox Management servers.
Master Server/Standby Server	• **Master IP/Standby IP**: IP address of the primary/secondary Equinox Management server. • **Status**: Indicates whether the server is currently active, or is in standby mode. The green icon indicates that the server is currently connected and functioning properly, and the red icon indicates a failure, either with one of the Equinox Management servers or with the database synchronization.
Virtual IP	The public virtual IP address representing the primary and secondary Equinox Management servers to other components.
FQDN URL	The URL that represents the virtual IP on your DNS server.
Gateway IP	The gateway (router) IP address used for the subnet to which your virtual IP address is part of.
Network Mask	The dedicated subnet mask, which represents the range of IP addresses in the network.

Table continues…

Field Name	Description
Replication Status	Indicates whether data is successfully synchronized between the redundant servers, with the following possible states: • **Error**: Data failed to synchronize due to an internal database error. • **Replicating**: Data synchronized and up to date on all redundant servers. • **Syncing**: Data is currently being synchronized between the redundant servers. • **Waiting**: Data is not being synchronized between redundant servers, possibly due to a failure in the network or in one of the servers. Check that the secondary and off-site backup servers are functioning.

Related links

High Availability of Equinox Management on page 378

Manually promoting the off-site backup server

About this task

This procedure describes how to manually promote the off-site backup server, which is necessary if both Equinox Management servers on the main site failed. This is not relevant if you deployed local redundancy only.

When the primary server on the main site fails, the secondary server automatically takes over. If both the primary and secondary servers fail (due to a major failure or disaster, for example), you need to change the role of the off-site backup server to active. The off-site backup server cannot automatically take over since the connection with the main site failed.

Figure 145: When to promote the off-site backup server on page 389 illustrates the event flow that occurs before you need to activate the backup server.

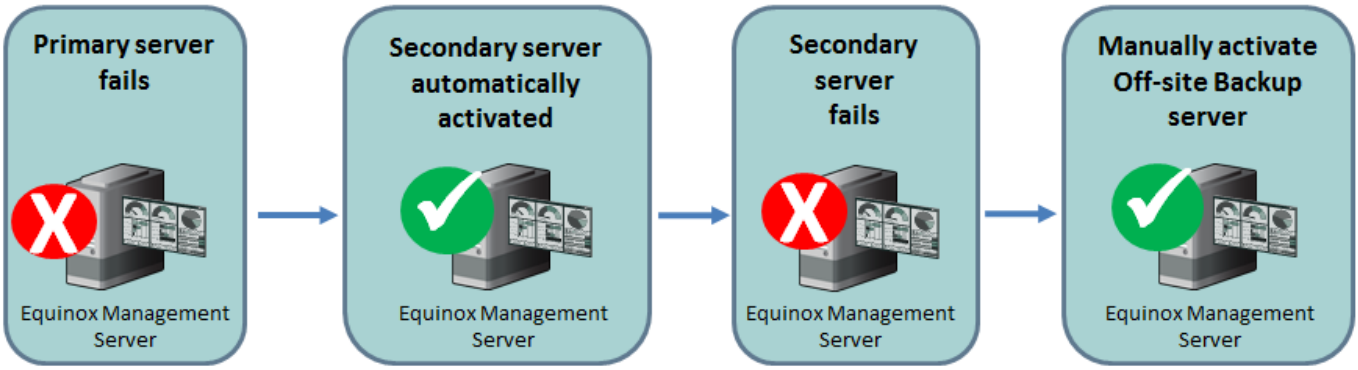


Figure 145: When to promote the off-site backup server

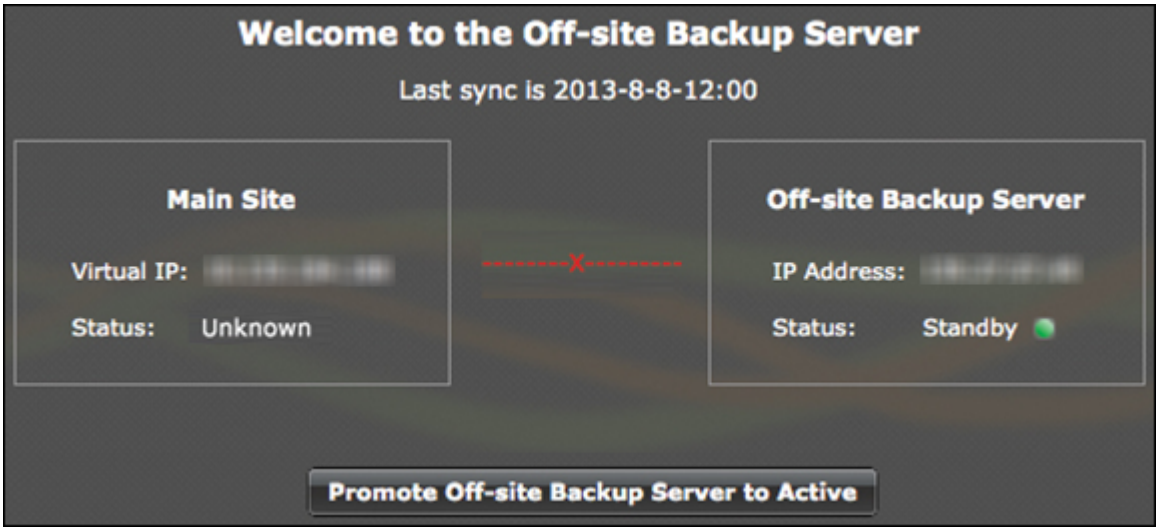
Before you begin

- You must have deployed an off-site backup server, as described in Creating an Off-Site Backup Server for Equinox Management on page 384.
- Verify that both the primary and secondary servers on the main site are not functioning, as described in Monitoring Redundancy Status on page 386.
- Verify that you configured Equinox Management's FQDN on the DNS server to point to both the virtual IP address (as the first IP address) and the off-site backup server's IP address. This ensures that the FQDN always automatically directs you to the Equinox Management server that is currently active.

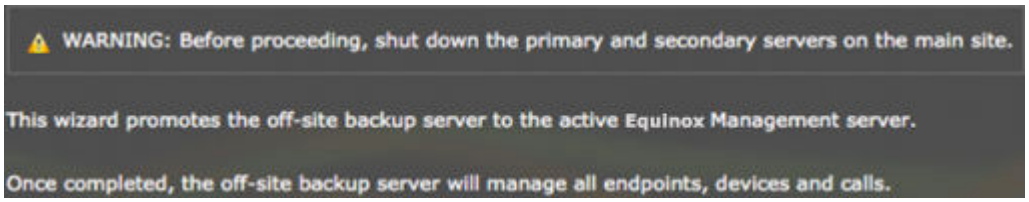
Procedure

1. Access the administrator portal of the off-site backup Equinox Management server.

   The system displays the redundancy status.



2. Click **Promote Off-site Backup Server to Active**, and then click **Process**:

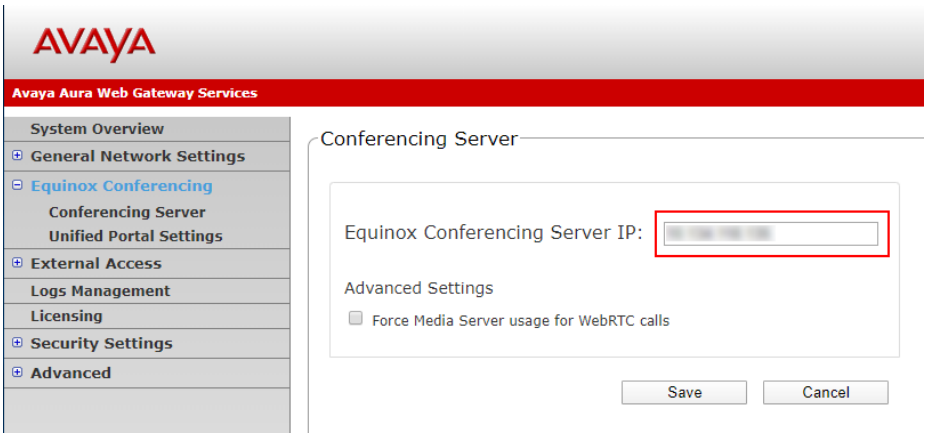


3. In the confirmation prompt, click **Yes** to promote the off-site backup server.

   The system displays a confirmation page, indicating that the backup server is now running as the active Equinox Management server.

4. (Recommended) Verify that all devices are working properly, as described in *Administrator Guide for Avaya Equinox Management*.

5. For TE deployments, the Web Gateway servers (managed by Avaya Aura® System Manager) must be directed to the new management backup server IP.
   a. In Avaya Aura® Web Gateway Services click **Equinox Conferencing**.



   b. Enter the new management backup server IP in the **Equinox Conferencing Server IP** field.

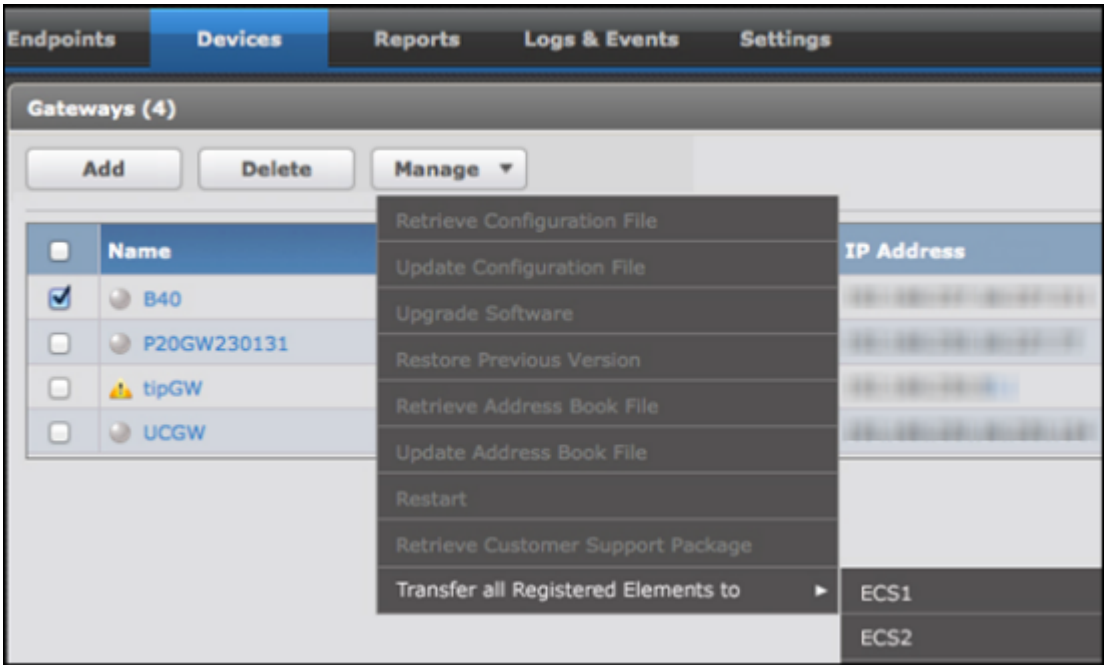
6. If there is any gatekeeper that is not functioning properly after promoting the backup server, move all endpoints and devices registered to it to another gatekeeper, as described below.

   This is necessary if you are using the internal gatekeeper of the main site's Equinox Management servers, or a standalone gatekeeper that is not running due to a general network failure at the main site.

   If there is a network failure at the main site, you cannot move devices and endpoints in that location, since they are offline.

   a. Access the administrator portal of the off-site backup Equinox Management server.
   b. Click **Devices** > **Manage** > **Transfer all Registered Elements to**, and choose the target gatekeeper.

      This process typically takes a few seconds, and may take up to a few minutes.



7. When the primary Equinox Management is functioning properly again (the main site's redundancy status displays a green icon and switches to **Standby**, see Monitoring Redundancy Status on page 386), you can restore its role as the active server, as described in Restoring primary server from off-site backup server on page 392.

Related links

High Availability of Equinox Management on page 378

Restoring primary server from off-site backup server

About this task

The off-site backup server takes over when the primary and secondary server have failed. Once the primary server is functioning properly, restore its status to Active.

This is not relevant for local redundancy, where the primary server automatically resumes its active role once it is functioning.

Alternatively, you can create a new location with two new Equinox Management servers as the primary and secondary servers (for example, if there was a natural disaster at the main location).

Before you begin

Verify that the primary Equinox Management is functioning properly (the main site's redundancy status displays a green icon and switches to **Standby**, see Monitoring Redundancy Status on page 386).

If you are creating a new location with two new Equinox Management servers as the primary and secondary servers, install the same version of Equinox Management on two separate servers, in the same location and subnet (see *Deploying Avaya Equinox® Solution*).

Procedure

1. Access the administrator portal of the off-site backup Equinox Management server.
2. Click ≡ > **Redundancy Setup**.

   The system displays the **Redundancy Setup** page.

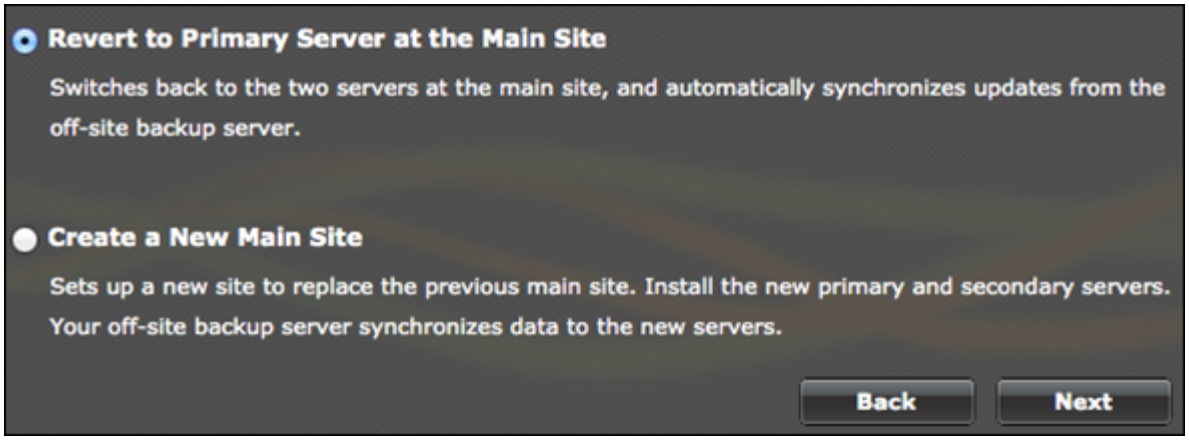


Figure 146: Setting up local redundancy

3. Select one of the following, and then click **Next**.
   - **Revert to Primary Server at the Main Site**: Restores the original redundancy setup, where the primary server is active and the secondary and backup servers are in standby.
   - **Create a New Main Site**: Creates a new location with new Equinox Management primary and secondary servers. The off-site backup server in the original setup continues functioning as the backup server. This option is typically used only if there is a natural disaster at the main site.

     If you create a new main site, the wizard guides you through reconfiguring local redundancy, as described in Creating a Redundant Secondary Server for Equinox Management on page 380.
4. If you are restoring the servers at the main site, select the IP address of the server to use as the active primary server, and then click **Next**.

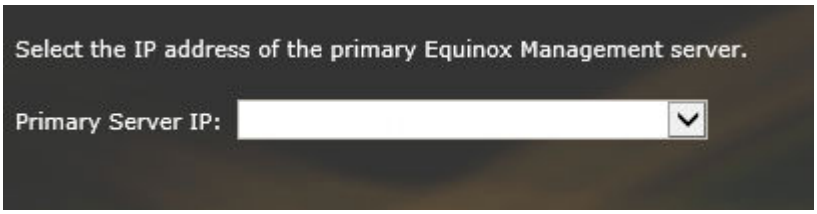
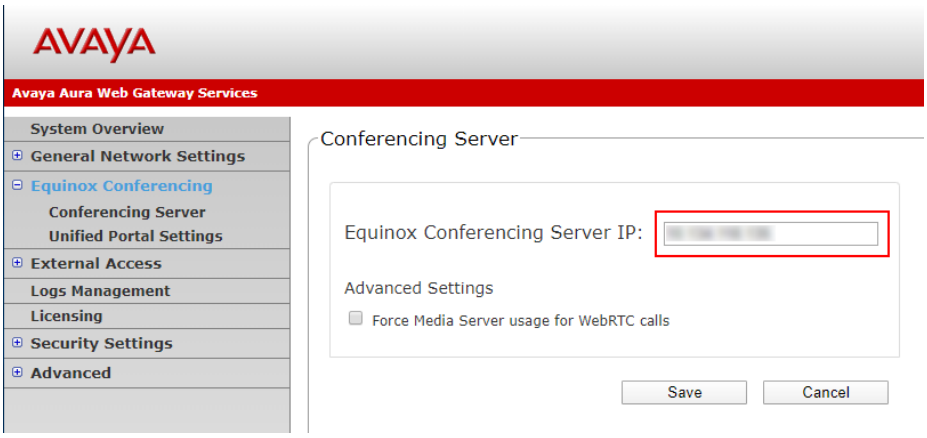


Figure 147: Selecting the primary server

The system displays a confirmation page, indicating that the primary and secondary servers are now functioning properly and the primary server resumed its role as the active server.

5. If you directed the Web Gateway servers to the management backup server IP, you must redirect them to the main site virtual IP.
   a. In Avaya Aura® Web Gateway Services click **Equinox Conferencing**.



   b. Enter the main site virtual IP in the **Equinox Conferencing Server IP** field.

Related links

High Availability of Equinox Management on page 378

Disabling Redundancy

About this task

When disabling redundancy, you remove the connection between the redundant Equinox Management servers. This is necessary, for example, if you need to replace the secondary server.

If you deployed an off-site backup server, first disable its redundancy, and then remove the secondary server's redundancy.

Important:

Once you disable redundancy, you cannot restore it. To set up redundancy later, you need to reconfigure it from the beginning (see Creating a Redundant Secondary Server for Equinox Management on page 380).

Procedure

1. Access the Equinox Management administrator portal using the FQDN.
2. Select ≡ > **Redundancy Setup**.
   a. If you configured an off-site backup server, select **Remove** next to **Geographic Redundancy (Manual Failover)**, and then **Yes** at the prompt.

Figure 148: Disabling redundancy in Equinox Management

The system confirms when geographic redundancy has been disabled.

b. Select **Remove** next to **Local Redundancy (Automatic Switchover)**, and then **Yes** at the prompt.

The system confirms when local redundancy has been disabled.

3. If you are replacing the secondary server, reconfigure redundancy as follows:

a. Uninstall the current secondary server (see *Administrator Guide for Avaya Equinox® Management*).

b. Install a new secondary server (see *Installation Guide for Avaya Equinox® Management*).

c. Reconfigure redundancy (see Creating a Redundant Secondary Server for Equinox Management on page 380).

Related links

High Availability of Equinox Management on page 378

Upgrading, Backing up and Restoring Equinox Management

You can restore the Avaya Equinox® Management database and configuration files from a backup copy. You should back up your database and configuration files on a regular basis.

There are many reasons for performing system backups, such as:

- Hardware failure
- Software failure
- Data corruption
- User errors
- Before a software upgrade

You must upload an installer to perform the upgrade process. The upload procedure depends on the operating system you are using (see Uploading a windows installer with Equinox Management on page 406 and Uploading a Mac Installer with Equinox Management on page 407).

Additionally, the upgrade procedure may vary depending on the release number and the size of the jump from the current installation to the new release. For more information, see Upgrading All-In-One Equinox Management on page 409.

Related links

Maintaining your Videoconferencing Network on page 378
Enabling the administrator to configure a notification message on page 396
Software Update Tool on page 398
Backing up Equinox Management Manually on page 401
Backing up Equinox Management Automatically on page 402
Restoring an Equinox Management Backup File on page 404
Making the Avaya IX Workplace Client available to users on page 406
Upgrading All-In-One Equinox Management on page 409
Upgrading Equinox Management deployed in high-availability or geographic redundancy on page 410
Upgrading the User Portal + Web Gateway on page 414
Upgrading multiple User Portal + Web Gateway nodes simultaneously on page 415
Managing Cassandra repairs of Avaya Aura Web Gateway nodes on page 416
Upgrading the distributed H.323 Gatekeeper on page 418
Upgrading H.323 Gatekeepers in Alternate Mode on page 419

Enabling the administrator to configure a notification message

About this task

You can send a message to the HTML text block using the Avaya Equinox® Management user interface. This feature works with Avaya Equinox® for Over The Top for single and multi-tenant and Avaya Equinox® for Team Engagement for single tenant installations.

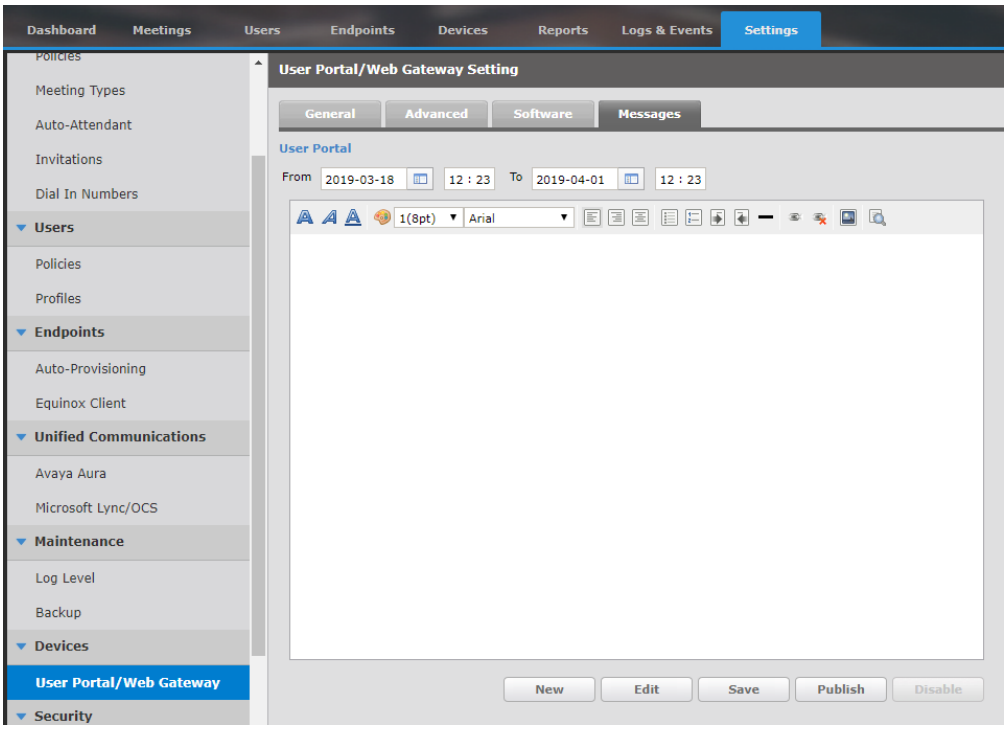
You must set the start and end dates and times of the message.

You can configure the font, justification and other formatting. You can save the message but it will not be scheduled to display until you click **Publish**. After you have clicked **Publish** you can

always cancel the scheduling by clicking **Disable**. You must disable the scheduling to edit or type a new message. Only one scheduled message at a time is supported.

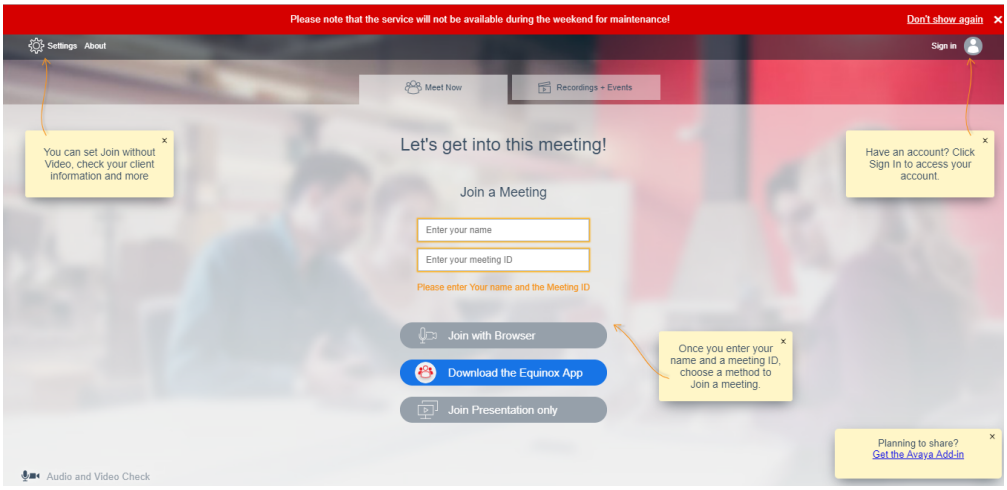
Procedure

1. Click **Settings**.
2. For Avaya Equinox® for Team Engagement click **User Portal.**
3. For Avaya Equinox® for Over The Top click **User Portal/Web Gateway**.
4. Click **Messages.**



5. Click **New** or **Edit**.
6. Set the date and time range to display the notification.
7. Type the notification and set the formatting.
8. Click **Save**.
9. Click **Publish**.

   The notification displays in the **User Portal** or **Web Gateway** when the clock and date on the Avaya Equinox® Management server reaches the time and date set on the **Messages** tab.



Related links

Upgrading, Backing up and Restoring Equinox Management on page 395

Software Update Tool

Use the Software update tool in the Avaya Equinox® Management administration user interface to upgrade Avaya Equinox® Unified Portal and software web browser client (SWC-webRTC) versions.

In Avaya Equinox® for Over The Top deployments (embedded/cores AAWG/User Portal) the software update tool is located at **Settings** > **User Portal/Web Gateway** > **Software**.

In Avaya Equinox® for Team Engagement deployments (Standalone AAWG/User Portal) the software update tool is located at **Settings** > **User Portal** > **Software**.

Related links

Upgrading, Backing up and Restoring Equinox Management on page 395
Upgrading the Web Client and User Portal Client with client.war or portal.war on page 398
Upgrading the Portal Server with ups.war or acs.war on page 399
Upgrading Only Some Servers with an *.war file on page 400
Restoring Previous Versions of Servers on page 400

Upgrading the Web Client and User Portal Client with client.war or portal.war

About this task

Use this task to patch the Web Client and User PortalClient with client.war or portal.war without creating a full software release in the following deployments:

- Cloud based multi-tenant deployments
- Premise based single tenant Avaya Equinox® for Over The Top and Avaya Equinox® for Team Engagement deployments

- Both distributed and non-distributed AAWG deployments

Before you begin

You need a client.war or portal.war file.

Procedure

1. Click **Settings**.
2. For Avaya Equinox® for Team Engagement deployment click **User Portal**.
3. For Avaya Equinox® for Over The Top deployment click **User Portal/Web Gateway**.
4. Click **Software**.
5. Upload the client.war or portal.war file from your computer.
6. Confirm the application's upgrade.

   All servers in the cluster are upgraded.

Related links

Software Update Tool on page 398

Upgrading the Portal Server with ups.war or acs.war

About this task

Use this task to patch the portal server with a ups.war or acs.war file and without creating a full software release in the following deployments:

- Cloud based multi-tenant deployments
- Premise based single tenant Avaya Equinox® for Over The Top and Avaya Equinox® for Team Engagement deployments
- Both distributed and non-distributed AAWG deployments

Before you begin

You need a ups.war or acs.war file.

Procedure

1. Click **Settings**.
2. For Avaya Equinox® for Team Engagement deployment click **User Portal**.
3. For Avaya Equinox® for Over The Top deployment click **User Portal/Web Gateway**.
4. Click **Software**.
5. Upload the ups.war or acs.war file from your computer.
6. Select the server in the **Application status** table to update.
7. Click **Apply updates**.

   All servers in the cluster are upgraded.

Related links

Software Update Tool on page 398

Upgrading Only Some Servers with an *.war file

About this task

Use this task to patch some servers with an *.war file and without creating a full software release in the following deployments:

- Cloud based multi-tenant deployments
- Premise based single tenant Avaya Equinox® for Over The Top and Avaya Equinox® for Team Engagement deployments
- Both distributed and non-distributed AAWG deployments

Before you begin

You need an *.war file.

Procedure

1. Click **Settings**.
2. For Avaya Equinox® for Team Engagement deployment click **User Portal**.
3. For Avaya Equinox® for Over The Top deployment click **User Portal/Web Gateway**.
4. Click **Software**.
5. Upload the *.war file from your computer.
6. Close the **Confirmation** window with the **Cancel** button.
7. Select one or several servers to perform the application upgrade from the **Application status** table.
8. Select one or several required war files from the **Uploaded files** table and click **Apply Update**.
9. Confirm the application's upgrade.
10. If you want to restart servers manually later, clear the **Restart automatically** check box.
11. Click **Apply updates** to apply.
12. To use the new portal server versions, click **Restart**.

Related links

Software Update Tool on page 398

Restoring Previous Versions of Servers

About this task

A backup of the initial version of the application is created automatically during upgrading. Use this task to restore the initial version.

Before you begin

You need a backup of the initial version.

Procedure

1. Click **Settings**.
2. For Avaya Equinox® for Team Engagement deployment, click **User Portal**.
3. For Avaya Equinox® for Over The Top deployment, click **User Portal/Web Gateway**.
4. Click **Software**.
5. Click servers to perform the application upgrade from the **Application status** table.
6. Select one or several required war files from the **Uploaded files** table and click **Apply Update**.

   The backup files are marked with **backup** in the version's column. You must restart the servers to upgrade the application with the ups or acs.war files.

   Restart is triggered in 10 seconds after the application's upgrade confirmation, usually it takes about two minutes.
7. If you want to restart servers manually later, clear the **Restart automatically** check box.
8. Confirm the application's upgrade.

   Restart is triggered in 10 seconds after the application's upgrade confirmation, usually it takes about two minutes.

Related links

Software Update Tool on page 398

Backing up Equinox Management Manually

About this task

The backup procedure saves Equinox Management's internal database and settings, which contains configuration and meeting scheduling information stored in local text files (known as property files).

Equinox Management backs up all configuration files.

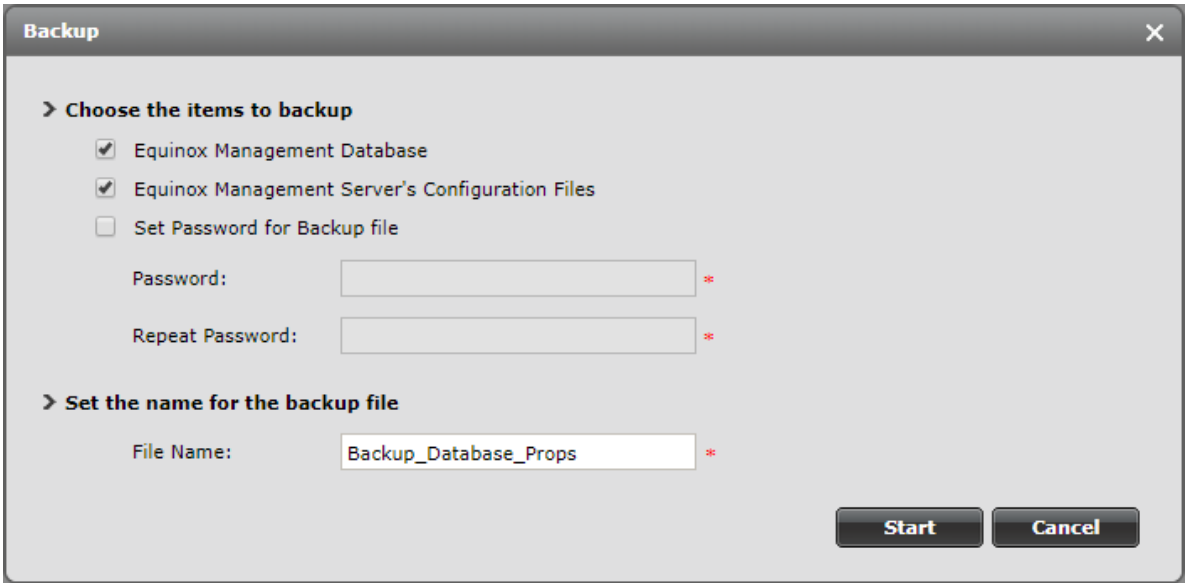
We recommend that you back up Avaya Equinox® Management manually before you perform maintenance procedures such as upgrade to save the latest configuration.

In redundant deployments, back up the primary Equinox Management server only.

Procedure

1. Access the Equinox Management administrator portal (on the primary server, for redundant deployments).
2. In the Equinox Management administrator portal, select ≡ > **Backup**.

   The **Backup** dialog box displays.



3. Select the components you want to back up:
   - **Equinox Management Database**
   - **Equinox Management Server's Configuration Files**
4. Set the password for the backup file.
5. Set the name for the backup file.
6. Click **Start**.

Related links

Upgrading, Backing up and Restoring Equinox Management on page 395

Backing up Equinox Management Automatically

About this task

To ensure that the files are backed up regularly, we recommend that you configure Avaya Equinox® Management to perform the backup procedure automatically.

If necessary, you can also perform the backup procedure manually, as described in Backing up Equinox Management Manually on page 401.

In redundant deployments, back up the primary Equinox Management server only.

Procedure

1. Access the Equinox Management administrator portal (on the primary server, for redundant deployments).
2. Select **Settings** > **Maintenance** > **Backup**.

   The **Backup** window opens.

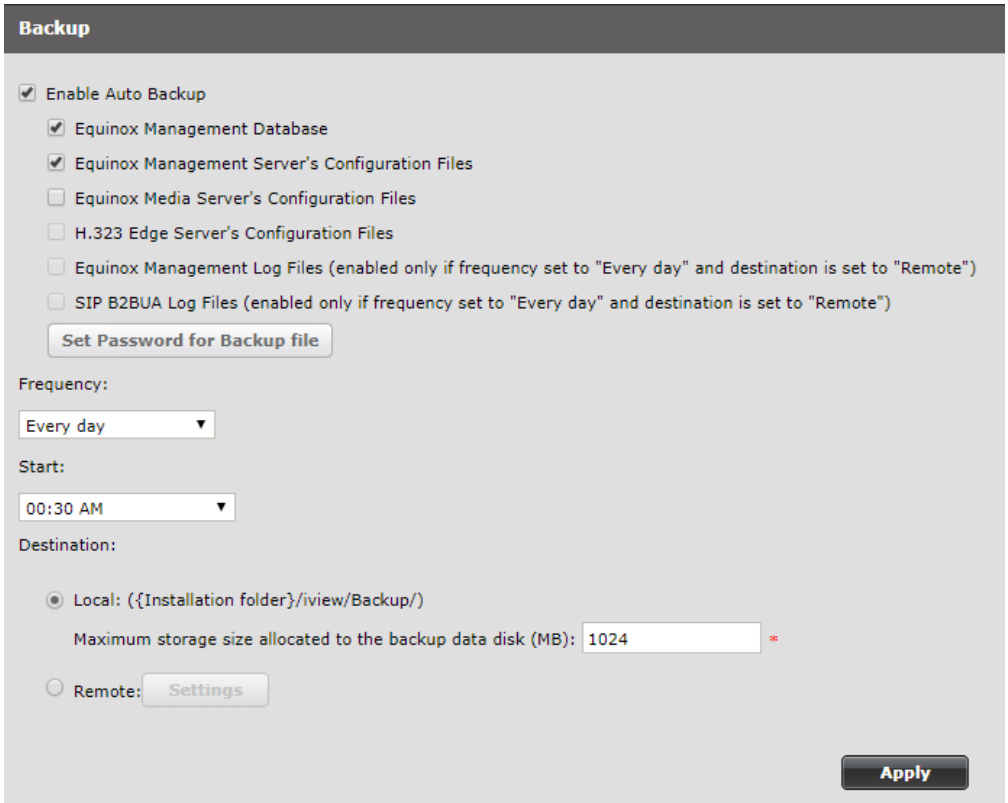


Figure 149: Defining Settings for the Automatic Backup

3. Select the components you want to back up:
   - **Equinox Management Database**
   - **Equinox Management Server's Configuration Files**
   - **Equinox Media Servers' Configuration Files**
   - **H.323 Edge Servers' Configuration Files**
   - **Equinox Management Log Files (enabled only if frequency set to "Every day" and destination is set to "Remote"**
   - **SIP B2BUA Log Files (enabled only if frequency set to "Every day" and destination is set to "Remote"**
4. Set the password for the backup file.

   The password is required and there are no other password requirements.
5. Select **Enable Auto Backup**.
6. Define the backing up settings as described in Table 70: Configuring Avaya Equinox® Management to perform automatic backup on page 404.

Table 70: Configuring Avaya Equinox® Management to perform automatic backup

Field Name	Description
Frequency	Set the day on which Avaya Equinox® Management performs automatic backup.
Start	Set the time when Avaya Equinox® Management performs automatic backup.
Destination	Select the location where Avaya Equinox® Management stores the backup file: • Select **Default** to use the predefined location: <installation folder>/iview/Backup. Or • Select **Remote** and enter the path to the location on the network where you want to save the backup file (cannot be a local path).
Maximum storage size allocated to the backup data disk	Enter the value for the maximum storage space on the Avaya Equinox® Management server. When backup files reach this size, Avaya Equinox® Management starts overwriting the oldest backup files with the new ones.

7. Click **Apply**.

Related links

Upgrading, Backing up and Restoring Equinox Management on page 395

Restoring an Equinox Management Backup File

About this task

You can restore a previously backed up Equinox Management server, including its internal database, configuration files and branding, using the Equinox Management Backup and Restore tool. After the backup file is successfully restored, the Equinox Management server automatically restarts.

In redundant deployments, restore the backup file only on the primary Equinox Management server. The restored backup file is later transferred to the other Equinox Management servers during synchronization.

Before you begin

Verify the following before restoring:

- The backup file you are restoring is from the same Equinox Management edition and the same version as your current implementation.
- If you deployed Equinox Management redundancy, you restore the backup file on the primary server only. Therefore, you must stop Equinox Management services first on the off-site backup server (only for geographic redundancy), and then on the secondary server. Otherwise, the internal database can be damaged.

Procedure

1. Access the Equinox Management administrator portal (on the primary server, for redundant deployments).
2. Select ≡ > **Restore**.

   The **Restore** window appears with the list of backup files.

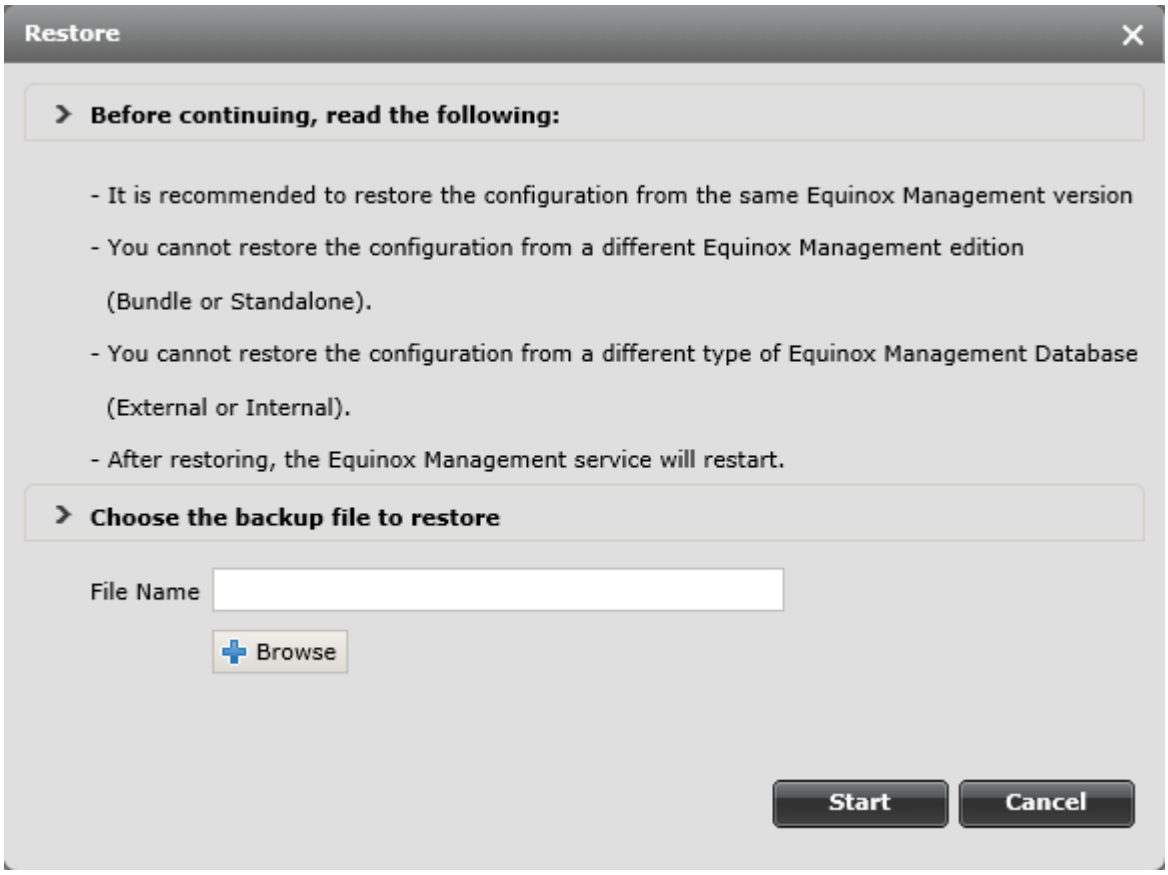


Figure 150: Restore Window

3. Select **Browse** to locate and upload the backup file to restore.

   Important:

   The backup file must be from the same edition, version, and database type as your current Equinox Management.

4. Select **Start**.

   The restore process begins. The system confirms when the restore is completed, and the Equinox Management server restarts.

5. If restoring the backup file in a redundant deployment, complete the procedure as follows:
   a. Disable redundancy settings on all servers.

b. Reconfigure server settings.

c. Verify that the primary Equinox Management service restarted correctly.

d. Start the Equinox Management services on both the secondary server and the off-site backup Equinox Management server (for geographic redundancy only), to automatically synchronize restored settings to that server.

Related links

Upgrading, Backing up and Restoring Equinox Management on page 395

Making the Avaya IX™ Workplace Client available to users

You must upload the Windows client installer to enable users to download the Avaya IX™ Workplace Client from the Unified Portal web page. For Avaya Equinox® for Over The Top implementations, the installer is uploaded to Equinox Management. For Avaya Equinox® for Team Engagement implementations, the installer is uploaded to *Administering Avaya Aura® Device Services*.

Related links

Upgrading, Backing up and Restoring Equinox Management on page 395
Uploading a windows installer with Equinox Management on page 406
Uploading a Mac Installer with Equinox Management on page 407

Uploading a windows installer with Equinox Management

About this task

You upload an installer to enable upgrading Equinox Management. This procedure describes uploading an installer using a Windows operating system with Avaya Equinox® for Over The Top. For information on the Avaya Equinox® for Team Engagement procedure see the *Administering Avaya Aura® Device Services* publication.

Note:

If one of the nodes is down and the new Avaya IX™ Workplace Client is uploaded to Equinox Management, the client is not uploaded to the nodes and is not available to users until all the nodes are up.

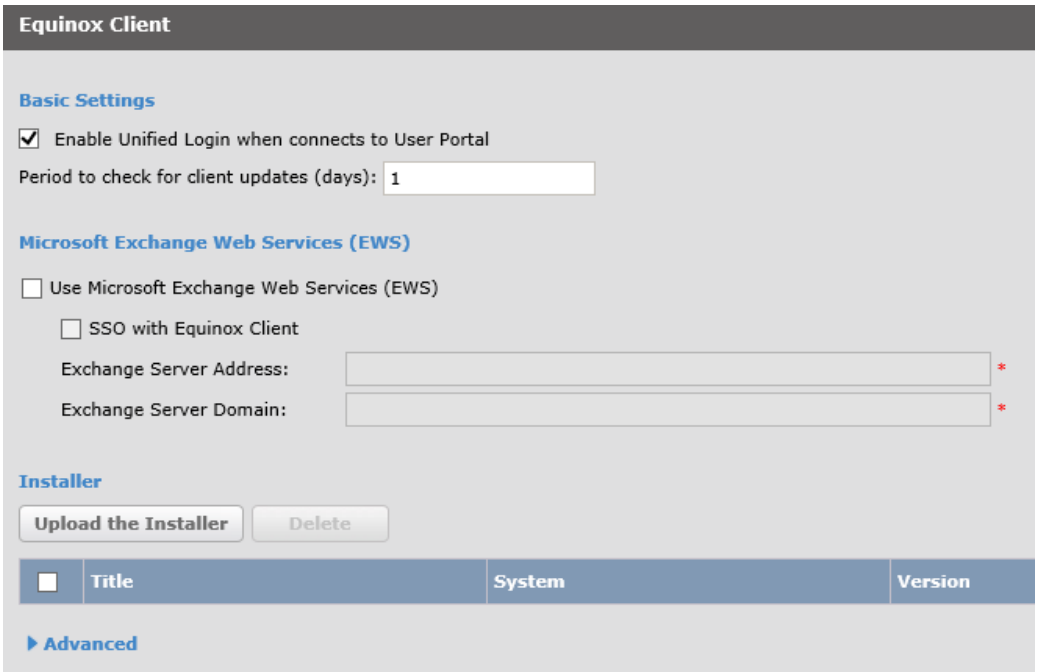
Before you begin

You must set the version with 3 or 4 numbers as x.x.x.x.

Procedure

1. Log in as global admin.
2. Access the Equinox Management administrator portal.
3. Click **Settings** > **Endpoints** > **IX Workplace Client**.

   The system displays the **IX Workplace Client** page.



4. Click **Upload the Installer** and select the relevant .msi or .exe installer file to upload.
5. Enter the version number and a description in the relevant fields.

   The version number must be 4 digits long, in the following format: *x.x.x.x*
6. Click **OK**.
7. Click **Apply**.

Related links

Making the Avaya IX Workplace Client available to users on page 406

Uploading a Mac Installer with Equinox Management

About this task

You upload an installer to enable upgrading Equinox Management. This procedure describes uploading an installer using a Mac operating system with Avaya Equinox® for Over The Top. For information on the Avaya Equinox® for Team Engagement procedure see *Administering Avaya Aura® Device Services*.

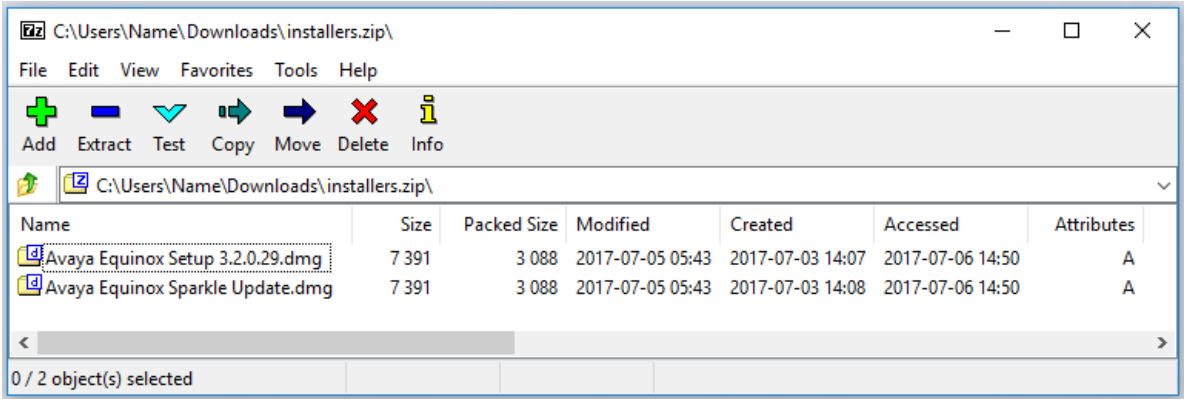
Before you begin

Ensure that you have placed the *installers.zip* file in the root directory of the archive. You must set the version with 3 or 4 numbers as x.x.x.x. The version number must not have 5 numbers otherwise it causes Sparkle upgrading issues with Avaya Scopia Desktop Client.

Procedure

1. Download the zip file that contains both Avaya Equinox.dmg and Avaya Equinox Sparkle Update.dmg, or download these two files separately and zip them together.

You must put them in the root of the archive, do not create additional directories. You can create any name for the zip file as long as the file extension is .zip. See the following example of such an archive (with mocked clients):



2. Log in as global admin.
3. Access the Equinox Management administrator portal.
4. Select **Settings** > **Endpoints** > **Equinox Client**.

   The system displays the **Equinox Client** page.

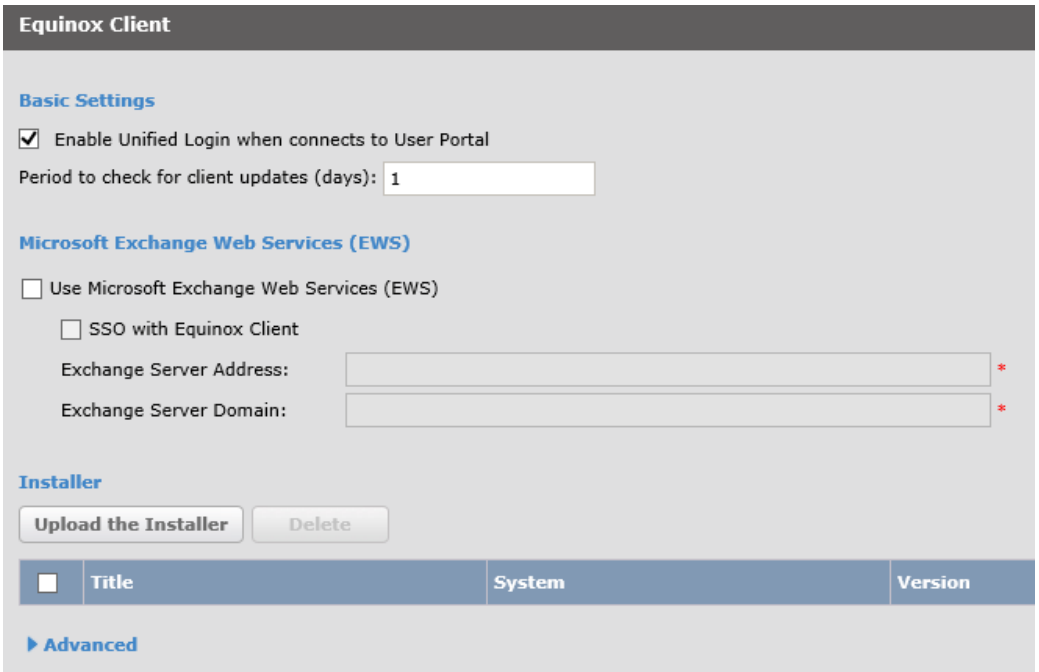


Figure 151: Equinox Client Page

5. Select **Upload the installer** and select the *installers.zip* file containing both the *Avaya Equinox.dmg* and *Avaya Equinox Sparkle Update.dmg* files.
6. Enter the version number and a description in the relevant fields.

The version number must be 4 digits long, in the following format: *x.x.x.x*

7. Select **OK**.
8. Select **Apply**.

Related links

Making the Avaya IX Workplace Client available to users on page 406

Upgrading All-In-One Equinox Management

About this task

The upgrade procedure may vary, depending on the following factors:

- The release number
- The size of the jump from the current installation to the new release

The upgrade procedure may take up to ten minutes. For more information on upgrading, see the *Release Notes for Avaya Equinox® Management* for the relevant version.

Important:

- Do not attempt to restore the database and configuration files from an old Equinox Management version. You can back up and restore database and configuration files only within the same Equinox Management release number.
- The upgrade order is as follows, after each one of these upgrades has completed successfully: 1. Equinox Management, followed by the security upgrade if any; 2. Equinox Media Server; 3. other solution server.

This procedure describes the generic procedure to be performed for the upgrade. For names of the specific files used in the upgrade, refer to the release notes.

Before you begin

Back up your Equinox Management configuration files before performing the upgrade, as described in Backing up Equinox Management Manually on page 401.

Download the software upgrade archive from the PLDS portal to the folder you created.The archive may also contain security and platform related upgrade .zip files.

Procedure

1. Access the Equinox Management administrator portal.
2. Select ≡ > **Upgrade Software**.

   The **Upgrade Software Wizard** opens, displaying a warning that the software update requires the device to shut down for a few minutes. All active calls will be disconnected.
3. Select **OK**
4. Select **I want to upload a new upgrade file** and select **Next**.
5. Select the Search icon to search for the software upgrade archive you previously downloaded.

6. Select the software upgrade .zip file.

   The grayed out **File Name** field displays the name of the zipped software file.

7. (Optional) In the **Save As** field, change the file name, and enter a short description of the upgrade in the text box.

8. Select **Next**.

   The Upgrade Progress window opens, displaying the progress of your upgrade.

   After the upgrade successfully completes, Equinox Management restarts and you are prompted to log into the system again.

9. Enter your login credentials.

10. On the Equinox Management dashboard, hover over the **Software Version** number to verify all versions in the Equinox Management deployment.

11. For security upgrade, follow the above steps. To verify that the security upgrade was successful:

    a. Navigate to **Logs & Events** > **Upgrade Results**.

    b. Select the management server in the dropdown list of the **Device management Log List** page.

    c. Browse to the security update file and verify that the upgrade status is **Completed**.

    To further verify that the security update was installed correctly, perform an SSH and enter the following command:

    ```
    cat/opt/avaya/common_services/installed_cves
    ```

    For example, the output has the following format:

    ```
    CVE-PHASE-1---Sun Nov 26 16:11:19 +03 2017
    CVE-PHASE-2---Sun Jul 8 11:38:07 +03 2018
    CVE-PHASE-3---Sun Jul 8 11:38:19 +03 2018
    CVE-PHASE-4---Sun Jul 8 11:54:33 +03 2018
    ```

Related links

Upgrading, Backing up and Restoring Equinox Management on page 395

Upgrading Equinox Management deployed in high-availability or geographic redundancy

About this task

The upgrade procedure may vary, depending on the following factors:

- The release number
- The size of the jump from the current installation to the new release

The upgrade procedure may take up to thirty minutes for Equinox Management in a high-availability deployment that includes two servers: a primary server and a secondary server.

Equinox Management in a geographic redundancy deployment includes three servers: an active server (primary) and a standby server (secondary) at the main site, and a backup server at the remote site.

You should review the Upgrading section of the latest *Release Notes for Avaya Equinox® Management* before proceeding.

Important:

- Do not attempt to restore the database and configuration files from an old Equinox Management version. You can back up and restore database and configuration files only within the same Equinox Management release number.
- The upgrade order is as follows, after each one of these upgrades has completed successfully: 1. Equinox Management, followed by the security upgrade if any; 2. Avaya Equinox® Media Server; 3. other solution server.

This procedure describes the details of a generic upgrade for high-availability and geographic redundancy. There is no need to shut down the standby server to upgrade the active server. For names of the specific files used in the upgrade, refer to the release notes.

Before you begin

Back up your Equinox Management configuration files on the primary server before performing the upgrade, as described in Backing up Equinox Management Manually on page 401.

Download the software upgrade archive from the PLDS portal to the folder you created. The archive may also contain security and platform related upgrade .zip files.

Procedure

1. Access the Equinox Management web interface.
2. Click ≡ > **Upgrade Software** > **OK**.

   The system displays the upgrade wizard.
3. Select the secondary Equinox Management server, and click **Next**.
4. Click **I want to upload a new upgrade file**.
5. Click the Search icon to search for the software upgrade archive you previously downloaded.
6. Select the upgrade file and click **Next**.

   The software upgrade starts uploading, showing a progress bar. When the software is uploaded, the grayed out **File Name** field displays the name of the uploaded zipped software file.
7. (Optional) In the **Save As** field, change the file name, and enter a short description of the upgrade in the text box.
8. Click **Next.**

   The system displays the **Upgrade Progress** window.

9. In the Equinox Management web interface, monitor database replication from the **Redundancy Status** page until the process is completed. The connection line between servers is green and the **Replication Status** is **Replicating**.
10. Click ▤ > **Upgrade Software** > **OK**.

    The system displays the upgrade wizard.
11. Select the primary Equinox Management server, and click **Next**.
12. If you want to upload a new upgrade file perform the following:
    a. Select **I want to upload a new upgrade file**.
    b. Click the Search icon 🔍 to search for the software upgrade archive you previously downloaded.
    c. Select the upgrade file and click **Next**.

       The software upgrade starts uploading, showing a progress bar. When the software is uploaded, the grayed out **File Name** field displays the name of the uploaded zipped software file.
    d. (Optional) In the **Save As** field, change the file name, and enter a short description of the upgrade in the text box.
    e. Click **Next.**

       The system displays the **Upgrade Progress** window.
13. If you want to select one of the current upgrade files to upgrade perform the following:
    a. Select **Select one of the current upgrade files to upgrade** and select the file.
    b. Click **Next.**
14. After the upgrade has completed Avaya Equinox® restarts.
15. Wait 1 – 2 minutes for the secondary server to become active and launch the Equinox Management web interface.
16. The system requires you to change the password before logging in for the first time if you did not change the password from the default in the previous build.
17. On the Equinox Management dashboard, hover over the **Software Version** number and verify that the Equinox Management and its components were correctly upgraded.
18. In the Equinox Management web interface, monitor database replication from the **Redundancy Status** page until the process is completed. The connection line between servers is green and the **Replication Status** is **Replicating**.
19. (Geographic redundancy) Continue as follows:
    a. Before you start the off-site backup server upgrade, make sure the **Redundancy Status** on the main site is **Replicating** and the connection line between the servers is green.
    b. Click ▤ > **Upgrade Software** > **OK**.

       The system displays the upgrade wizard.

c. Select the off-site backup server Equinox Management server, and click **Next**.

d. Select **I want to upload a new upgrade file**.

e. Click the Search icon to search for the software upgrade archive you previously downloaded.

f. Select the upgrade file and click **Next**.

The software upgrade starts uploading, showing a progress bar. When the software is uploaded, the grayed out **File Name** field displays the name of the uploaded zipped software file.

g. (Optional) In the **Save As** field, change the file name, and enter a short description of the upgrade in the text box.

h. Click **Next.**

The system displays the **Upgrade Progress** window.

i. In the Equinox Management web interface, monitor **Off-site Backup Server Status** in **Redundancy Status**. The status is green and Standby.

Figure 152: Database replication before upgrading the off-site backup server

For security upgrade, follow the previous steps after upgrading Equinox Management system completely with the Application file.

20. To verify that the security upgrade was successful:

a. Click **Logs & Events** > **Upgrade Results**.

b. Select the management server in the dropdown list of the **Device management Log List** page.

c. Browse to the security update file and verify that the upgrade status is **Completed**.

d. To further verify that the security update was installed correctly, perform an SSH and enter the following command:

```
cat /opt/avaya/common_services/installed_cves
```

For example with the CVE-4 file, the output has the following format:

```
CVE-PHASE-1---Sun Nov 26 16:11:19 +03 2017
CVE-PHASE-2---Sun Jul 8 11:38:07 +03 2018
CVE-PHASE-3---Sun Jul 8 11:38:19 +03 2018
CVE-PHASE-4---Sun Jul 8 11:54:33 +03 2018
```

Related links

Upgrading, Backing up and Restoring Equinox Management on page 395

Upgrading the User Portal + Web Gateway

About this task

When upgrading the User Portal + Web Gateway, ensure that the server is in an **Active** state before beginning the upgrade.

You must first upgrade the seed node before upgrading additional nodes. You must select additional nodes one at a time, but you can select a node before the previous one finishes upgrading.

To upgrade the User Portal + Web Gateway, perform the following procedure for each of the User Portal's servers.

Procedure

1. Access the Equinox Management administrator portal.
2. If the load balancer virtual IP address is not set, perform the following:
   a. Click ≡ > **Advanced Parameters**.
   b. In the **Property Name** field, enter `com.avaya.aawg.loadbalancer.virtualIPAddress`
   c. In the **Property Value** field, enter the load balancer virtual IP address.

      By default the virtual IP address is taken from **Frontend FQDN** using Look Up.
3. Click **Devices** > **Devices by Type** > **User Portals**.
4. Select the check box of the relevant User Portal and click **Manage** > **Upgrade**.

Related links

Upgrading, Backing up and Restoring Equinox Management on page 395

Upgrading multiple User Portal + Web Gateway nodes simultaneously

About this task

You can upgrade multiple User Portal + Web Gateway nodes at the same time, including nodes in a cluster that are not up and running. This can be done when working with a cluster which has nodes in different locations.

Simultaneous upgrading of nodes reduces upgrade time. You must first upgrade the seed node, and when the upgrade completes, you can then upgrade remaining nodes in any order you want. Upgrading nodes at different sites can be done at different times; you do not have to upgrade all nodes at once. Ensure that you do not make any configuration changes to nodes during the upgrade.

The Equinox Management UI does not enable you to actually select multiple nodes to upgrade at the same time. However, after upgrading the seed node, you can upgrade subsequent nodes without first waiting for the previously upgraded node to finish its upgrade.

The maximum number of nodes which can be upgraded at once is 5; therefore, after upgrading a group of 5 nodes, you can upgrade another group of up to 5, and so forth.

Procedure

1. Access the Equinox Management administrator platform.
2. Click **Devices** > **Devices by Type** > **User Portals**.

   The system displays the **User Portal** page.
3. Select the seed node from the list of nodes.

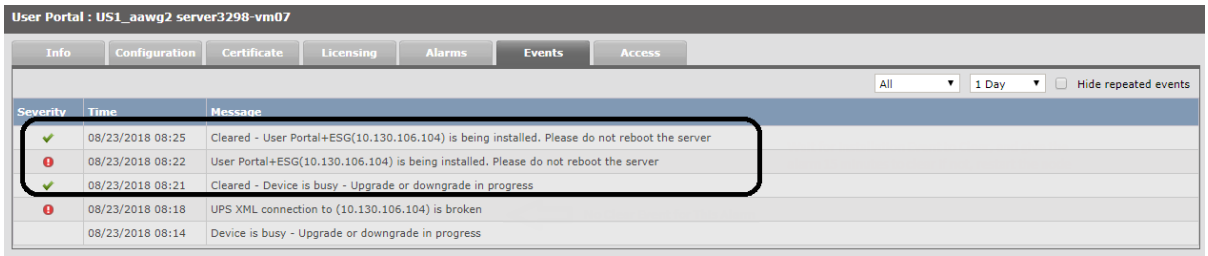
   Note:

   - To determine which is the seed node in an OTT environment: Click ☰ > **Advanced Parameters** and locate the following setting:
     `com.avaya.iview.esg.seednode.ip`
   - To determine which is the seed node in a TE environment: Log into the Avaya Aura® Web Gateway and on the **System Overview** page, locate the **Initial Node**.
4. Click **Manage/Upgrade Software**.
5. Click **Upgrade Now**, and select the application .zip file to begin the upgrade.

   After approximately 20 minutes, the node's upgrade should be complete.
6. Click **Next**.
7. Wait for the node upgrade to complete and restart, and click **Close**.
8. Click the **Events** tab for the node and verify that the following events have a status of **Cleared** (**Severity** = green).

   - **Device is busy - Upgrade or downgrade in progress**

- **User Portal+ESG(<nodeIPaddress>) is being installed. Please do not reboot the server.**
- **UPS XML connection to (<nodeIPaddress>) is broken**



Note:

If the **UPS XML connection to (<nodeIPaddress>) is broken** alarm does not clear after upgrade, wait 15 minutes after all other events have cleared. If this alarm still does not clear, do the following:

a. Return to the **User Portals** page and manually restart the node.

b. Wait 5–10 minutes.

c. Return to the **Events** tab and verify that the node has a status of **Cleared**.

9. After performing this procedure for the seed node, repeat the upgrade steps above for each node you want to upgrade. You do not have to wait for a node to finish upgrading before beginning the upgrade of subsequent nodes.
10. On the **Events** tab, verify that each event/alarm has cleared, as described above.

Related links

Upgrading, Backing up and Restoring Equinox Management on page 395

Managing Cassandra repairs of Avaya Aura® Web Gateway nodes

About this task

The repair process synchronizes the data between Avaya Aura® Web Gateway nodes for Avaya Equinox® for Over The Top to provide consistency. Use this procedure to set up the date and time for the Cassandra repair process. You can run the repair on a weekly or monthly basis. You can also disable the repair.

The Avaya Aura® Web Gateway performs the repair on one node at a time. By default, the Avaya Aura® Web Gateway performs the repair once a week on Sundays at 01:20 a.m.

Tip:

Set the time when the system usage is low to minimize impact on system performance.

Cassandra repair results are stored in the `CAS.log` file.

Procedure

1. Log in to the seed node as a root user by using an SSH connection.
2. Run the following commands to open the `catalina.properties` file in the vi editor:

   ```
   cdto active
   sudo vi mss/<tomcat_version>/conf/catalina.properties
   ```

3. To run the repair on a weekly basis, do the following:
   a. Edit the `com.avaya.cas.cassandra.repair.time.hour=<hour>` string to set the hour when the procedure starts.

      This parameter uses a 24-hour notation. For example, if you want to start the procedure at 4 p.m., enter `16`.

   b. Edit the `com.avaya.cas.cassandra.repair.time.minute=<minute>` string to set the minute when the procedure starts.

   c. Edit the `com.avaya.cas.cassandra.repair.time.weekday=<day_of_week>` string to set the required day of the week.

      The week starts from Sunday. For example, for Sunday, enter `1`, for Monday, enter `2`, and so on.

   d. In the `com.avaya.cas.cassandra.repair.time.monthday=<day_of_month>` string, set `<day_of_month>` to `0`.

   For example, to run the repair procedure on Wednesdays at 8:30 p.m., edit the entries as follows:

   ```
   com.avaya.cas.cassandra.repair.time.hour=8
   com.avaya.cas.cassandra.repair.time.minute=30
   com.avaya.cas.cassandra.repair.time.weekday=4
   com.avaya.cas.cassandra.repair.time.monthday=0
   ```

4. To run the repair on a monthly basis, do the following:
   a. Edit the `com.avaya.cas.cassandra.repair.time.hour=<hour>` string to set the hour when the procedure starts.

      This parameter uses a 24-hour notation. For example, if you want to start the procedure at 4 p.m., enter `16`.

   b. Edit the `com.avaya.cas.cassandra.repair.time.minute=<minute>` string to set the minute when the procedure starts.

   c. In the `com.avaya.cas.cassandra.repair.time.weekday=<day_of_week>` string, set `<day_of_week>` to `0`.

   d. Edit the `com.avaya.cas.cassandra.repair.time.monthday=<day_of_month>` string to set the required day of the month.

For example, to run the repair procedure on the second day of each month at 2:40 p.m., edit the entries as follows:

```
com.avaya.cas.cassandra.repair.time.hour=14
com.avaya.cas.cassandra.repair.time.minute=40
com.avaya.cas.cassandra.repair.time.weekday=0
com.avaya.cas.cassandra.repair.time.monthday=2
```

5. To disable the repair, set both `com.avaya.cas.cassandra.repair.time.weekday` and `com.avaya.cas.cassandra.repair.time.weekday` to `0` or to any other valid non-zero value.

   For example:

```
com.avaya.cas.cassandra.repair.time.weekday=0
com.avaya.cas.cassandra.repair.time.monthday=0
```

6. Save the file.
7. Run the `svc telportal restart` command to restart services.
8. In a cluster environment, repeat the previous steps on all non-seed nodes in the cluster.

Related links

Upgrading, Backing up and Restoring Equinox Management on page 395

Upgrading the distributed H.323 Gatekeeper

About this task

This procedure describes how to upgrade the distributed gatekeeper. If your deployment includes several gatekeepers, you can upgrade all the servers simultaneously. Do not shut down the servers for upgrading.

To upgrade redundant gatekeepers, see Upgrading H.323 Gatekeepers in Alternate Mode on page 419.

Before you begin

- Ensure that the gatekeeper status icon lights green.
- Download the software upgrade file from the PLDS portal.

Procedure

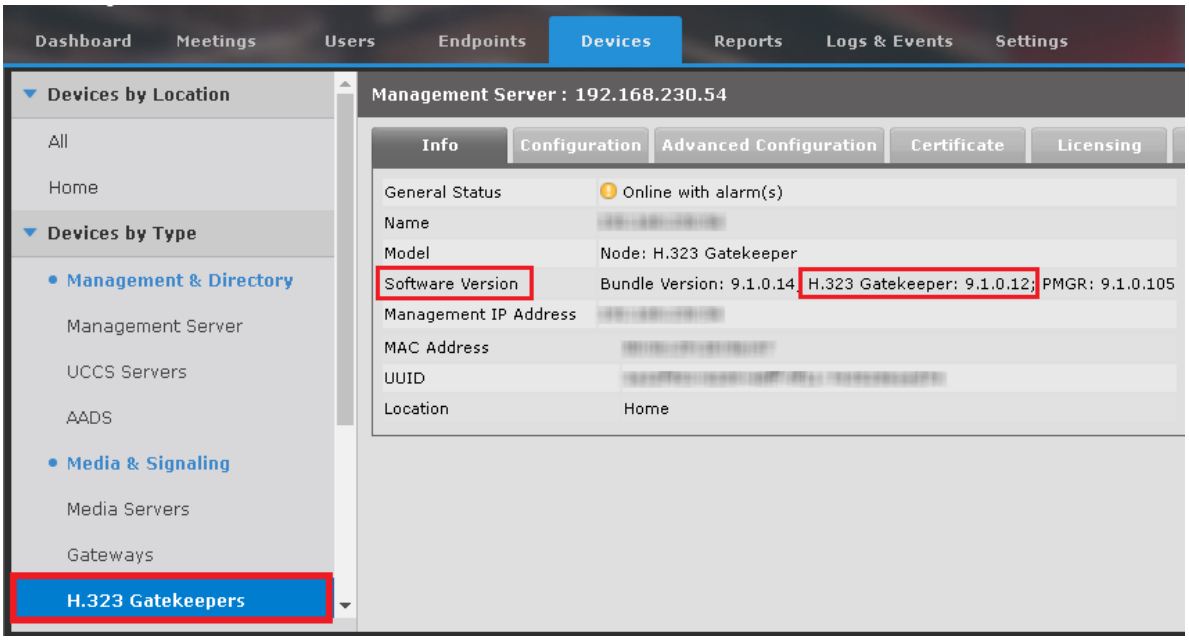
1. In **Devices** > **Devices by Type** > **H.323 Gatekeepers**, select the gatekeeper that needs the upgrade.
2. Click **Manage** > **Upgrade Software**.

   The **Upgrade** page displays the upgrade wizard.
3. To upload the new upgrade file, click **Upgrade Now** > **Next**.
4. Click the Search icon to search for the upgrade file you previously downloaded.
5. Select the upgrade file, and then click **Next**.

   The software upgrade starts uploading, showing a progress bar.

6. (Optional) Change the upgrade file name:
   a. Click **Save As**
   b. Change the upgrade file name.
   c. Enter a short description of the upgrade in the text box.
   d. Click **Next**.
7. When Equinox Management completes the upgrade, click **Close**.
8. Verify that Equinox Management successfully completed the upgrade:
   a. Click **Devices** > **Devices by Type** > **H.323 Gatekeepers**.
   b. Select the upgraded gatekeeper.

   The **Info** tab displays information about the software version update.



Related links

Upgrading, Backing up and Restoring Equinox Management on page 395

Upgrading H.323 Gatekeepers in Alternate Mode

About this task

This procedure describes how to upgrade redundant gatekeepers without breaking the alternate mode.

Before you begin

Download the software upgrade files from the PLDS portal. They include the application and CVE files.

Procedure

1. Verify that the alternate mode is operational:
   a. On the Equinox Management administrator portal, click **Devices** > **Devices by Type** > **H.323 Gatekeepers**.
   b. Verify that the gatekeeper status icons light green.
   c. Select the primary gatekeeper.
   d. Click the **Advanced Configuration** tab.

      Equinox Management displays the **Advanced Configuration** page.
   e. Write down the primary and secondary nodes IP addresses.

      The primary gatekeeper has a blue frame around it.
2. On the VM console, shut down the secondary gatekeeper.

   Wait until Equinox Management displays the following status:
   - The status icon of the secondary gatekeeper lights yellow.
   - The alarm indicates a disconnected secondary gatekeeper.
3. Upgrade the primary gatekeeper:
   a. Upgrade the primary gatekeeper to its newest version. See Upgrading the distributed H.323 Gatekeeper on page 418.
   b. Verify that Equinox Management displays the following status:
      - The secondary gatekeeper icon lights yellow.
      - The alarm indicates a disconnected secondary gatekeeper.
   c. Upgrade the primary gatekeeper with the CVE package.
   d. Verify that Equinox Management displays the following status:
      - The secondary gatekeeper icon lights yellow.
      - The alarm indicates a disconnected secondary gatekeeper.
4. On the VM console, power on the secondary gatekeeper.

   Wait until Equinox Management displays a green status icon next to the secondary gatekeeper.
5. On the VM console, shut down the primary gatekeeper.
   - The secondary gatekeeper becomes the new primary gatekeeper.
   - Wait until Equinox Management displays the following status:
     - The new secondary gatekeeper icon lights yellow.
     - The alarm indicates a disconnected secondary gatekeeper.

6. Upgrade the new primary gatekeeper:
   a. Upgrade the new primary gatekeeper to its newest version.
   b. Wait until Equinox Management displays the following status:
      - The new secondary gatekeeper icon lights yellow.
      - The alarm indicates a disconnected secondary gatekeeper.
   c. Upgrade the new primary gatekeeper with the CVE package.

      Wait until Equinox Management displays the following status:
      - The new secondary gatekeeper icon lights yellow.
      - The alarm indicates a disconnected secondary gatekeeper.
7. On the VM console, power on the new secondary gatekeeper.
   - Wait until Equinox Management establishes the alternate mode.
   - Verify that the gatekeeper status icons light green.

Related links

Upgrading, Backing up and Restoring Equinox Management on page 395

Daily Maintenance of your Video Network

This section provides daily procedures for maintaining your network devices, meeting types, meeting groups and scheduled meetings.

Related links

Maintaining your Videoconferencing Network on page 378
Searching for a Video Device on page 421
Removing a Video Device from Equinox Management on page 422
Preparing a Device for Maintenance on page 423
Replacing a defective node in a User Portal or Web Gateway cluster on page 424
Managing Bandwidth in your Network on page 424

Searching for a Video Device

About this task

You can search for a specific endpoint or network device and modify some of its settings, such as maximum bandwidth or location.

Procedure

1. Access the Equinox Management administrator portal.

2. Select the **Endpoints** or **Devices** tab.

   You can search through the displayed list, or narrow the list by selecting one of the tabs in the sidebar menu.

3. For a basic search, enter the first few characters of the device's name or IP address in the **Search** field.

4. For an advanced search, select the icon and enter the following information, as required:

   Table 71: Searching for a video device

Field Name	Description
Name	Enter the first few characters of the device you want to find.
Dialing Info	Enter the first few characters of the endpoint's dialing string.
Version	Enter the first few characters of the device's software version number.
IP Address	Enter the first few characters of the device's IP address.
Vendor	Search for the required endpoint in the supplier global list by selecting **All**. You can narrow your search by selecting an endpoint from the supplier's list.

5. Select **Search**.

Related links

Daily Maintenance of your Video Network on page 421

Removing a Video Device from Equinox Management

About this task

Deleted video devices are not added to the Equinox Management database in any subsequent auto-detect operations.

You can add a deleted video device manually by selecting the **Add** icon in one of the device views.

Before you begin

- If you are removing an endpoint that is still listed in your organization's LDAP server, you must first remove the endpoint from the LDAP server and then remove it from Equinox Management. Otherwise, the endpoint will be added back to Equinox Management the next time it is synchronized with the LDAP server.
- If you are removing an endpoint that is still registered to your gatekeeper, we suggest that you first remove the endpoint from the gatekeeper and then remove it from Equinox

Management. Otherwise, you must deselect the endpoint the next time Equinox Management is synchronized with the gatekeeper, to prevent the endpoint from being added back.

Procedure

1. Log in to the Equinox Management administrator portal.
2. Select the **Endpoints** or **Devices** tab.
3. Search for an online video device, as explained in Searching for a Video Device on page 421.
4. Select the check box of the video device to be removed. To remove all the devices, select the list heading.

   Only service providers or administrators of a distributed environment can delete network devices.
5. Select **Delete**.
6. At the prompt select **Yes**.

   The device profile, as well as any information about the device, is removed from Equinox Management.

Related links

Daily Maintenance of your Video Network on page 421

Preparing a Device for Maintenance

About this task

Before performing maintenance on MCUs, Web Collaboration servers and Gateways, you can change their status to **In-maintenance**. For example, this feature is used for upgrading the device. When a device's status is **In-maintenance**, it is still part of the network, and can be put back online at any time.

Equinox Management cannot schedule meetings for an MCU that is **In-maintenance**. Equinox Management attempts to reschedule upcoming meetings on other MCUs that use the same services and have sufficient, available resources. If no replacement MCUs are available when the MCU status is changed back to online, upcoming meetings are lost and not restored.

Procedure

1. Log in to the Equinox Management administrator portal.
2. Select the **Devices** tab.
3. Select the **MCUs, Web Collaboration servers,** or **Gateways** tab in the sidebar menu.
4. Select the link in the **Name** column for the relevant device.
5. Select the **Configure** tab.
6. Select the **In Maintenance** checkbox.
7. Select **Apply** to save your changes.

Related links

Daily Maintenance of your Video Network on page 421

Replacing a defective node in a User Portal or Web Gateway cluster

About this task

You can recover every node in an Avaya Equinox® for Over The Top cluster. Previously you had to redeploy the whole cluster if there were any issues.

Note:

Replacing a defective node requires the deployment of a new license key and certificates must be re-generated, see the topic on updating an Equinox license in the Deploying Avaya Equinox® Solution publication and Creating and uploading Equinox Management's certificate for videoconferencing components on page 192 in this publication.

Procedure

1. Access the Equinox Management administrator portal.
2. Delete the node:
   a. Click **Devices** > **Devices by Type** > **User Portals**.
   b. Select the node.
   c. Click **Delete**.
3. Delete the virtual machine in the VM management tool.
4. To reinstall the Avaya Aura® Web Gateway, refer to the Deploying a distributed or cluster User Portal and Web Gateway topic in the Deploying Avaya Equinox® Solution publication.

   Note:

   The reinstalled node must have the same IP address.

Related links

Daily Maintenance of your Video Network on page 421

Managing Bandwidth in your Network

Bandwidth for in-zone, cross-zone and pro-to-pro calls are managed within Equinox Management. The following topics describe how to configure bandwidth thresholds.

- Defining bandwidth limits for a location on page 55
- Downgrading the Meeting Bandwidth on page 307

Related links

Daily Maintenance of your Video Network on page 421

Upgrading, Backing Up and Restoring Video Device Software

Equinox Management enables you to manage software upgrades for MCUs, gateways, Web Collaboration servers and third party endpoints. Upgrades are managed by applying an upgrade file to chosen devices in Avaya Equinox® Management.

Before upgrading these devices, you must retrieve their configuration file using Equinox Management.

Related links

Maintaining your Videoconferencing Network on page 378
Editing upgrade history of video devices on page 425
Upgrading the software file of a video device on page 426
Removing a software upgrade file from a video device on page 429
Backing up and duplicating a video device configuration on page 430
Updating license keys on page 431
Restoring the previous software version of a network device on page 431
Downgrading your Network Device on page 433

Editing upgrade history of video devices

About this task

You can view or remove entries from the Device Upload log, which displays the history of all your attempts to upload a software upgrade file, update configuration files, update the endpoint's address book file, and shows all scheduled future upload attempts, via Equinox Management.

If using Application Server P/N 55876-00002, make sure to remove log files on a regular basis to ensure that there is enough disk space.

You can view and edit the upgrades of the following devices:

- Gatekeepers
- Media servers
- Web Collaboration server
- Endpoints: Avaya Room System XT Series, Polycom, Tandberg, and Sony endpoints only.

Procedure

1. Access the Equinox Management administrator portal.
2. Click the **Logs & Events** tab.
3. Click **Upgrade Results** or **Configuration Updates**.
4. Select the type of device in the dropdown list.

The device history is displayed, with a log of each attempt to upload a software upgrade file, update configuration files, update the endpoint's address book file, and all scheduled future upload attempts.

5. (Optional) You can delete upload logs that are no longer necessary by selecting the relevant logs and **Delete**. To delete all upload logs for this device, click **Delete All**.

Related links

Upgrading, Backing Up and Restoring Video Device Software on page 425

Upgrading the software file of a video device

About this task

You can quickly and easily perform remote software upgrades of video devices from Avaya Equinox® Management by uploading an upgrade file and applying it to the device. Upgrade files are supplied by the device vendor.

You can upgrade the following devices via Avaya Equinox® Management:

- Scopia Elite MCU
- Gateways, including Web Collaboration server
- Room systems and personal endpoints, including Avaya Room System XT Series and third-party endpoints from Sony or Polycom.

Note:

For gateways, perform the upgrade remotely using the Equinox Management. You cannot upgrade the firmware of the gateway directly on the device.

Depending on your support contract, you can upgrade to:

- The next major version.

  Upgrading a major version requires a new license.

  This kind of upgrade changes one of the first two digits in a version number. For example, upgrading from version 8.0 to version 8.1 requires a new license.

- An incremental version.

  Upgrading an incremental version does not require a new license.

  This kind of upgrade changes the third, fourth and fifth digits in the version number. For example, upgrading from 8.0.0.34.0 to 8.0.0.36.1 or to 8.0.0.36.2 does not require a new license.

Upgrades may require first applying the major upgrade and then the incremental upgrade within that major version. For example, to upgrade from 8.0.0.38.2 to 8.1.0.0.1, first apply the major upgrade to 8.1.0.0.0, and then the incremental upgrade to 8.1.0.0.1.

Before you begin

Before upgrading your video network devices, including endpoints, do the following:

- Before upgrading a video device software, back up its configuration by retrieving its configuration file. For more information on remote backups, see Backing up and duplicating a video device configuration on page 430.
- Go to https://plds.avaya.com to apply for and download your upgrade package.
- If you upgrade to a major version, ensure you have a new license key. The upgrade procedure is different when upgrading to a major new version compared with smaller incremental upgrades. See Updating license keys on page 431 for details.
- Navigate to the device and select the **Access** tab. Enter a name and password for automatic login to the video device during the upgrade process. We recommend using the same name across the deployment.
- If you are upgrading endpoints, verify that it is managed by Avaya Equinox® Management.

  See Managing endpoints using Equinox Management on page 141 for details.
- If you are simultaneously upgrading multiple endpoints (of the same type), it is useful to first assign labels to the endpoints, to help you quickly select these endpoints.

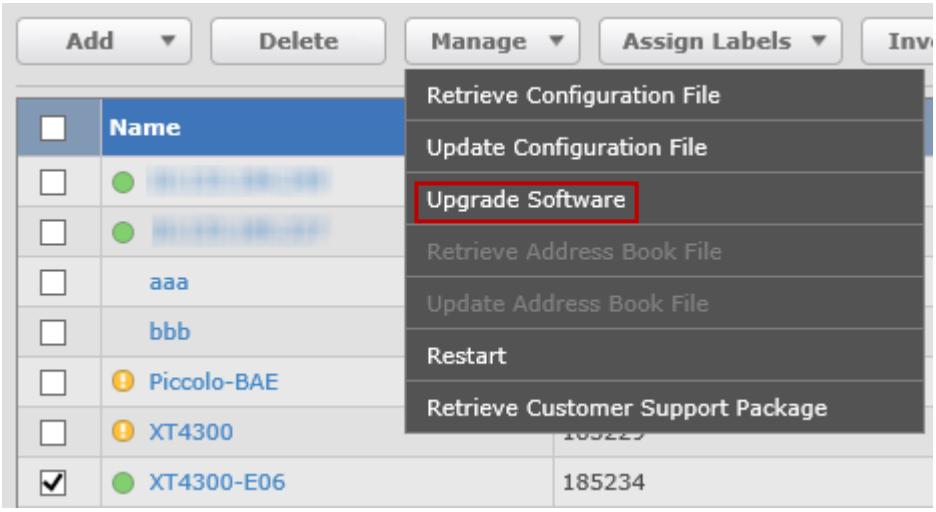
  See Organizing endpoints into groups with labels on page 171 for details.

Procedure

1. Access the Avaya Equinox® Management administrator portal.
2. Click the **Endpoints** tab.
3. Locate the video device as explained in Searching for a Video Device on page 421.
4. Select the check box of the device to be upgraded.

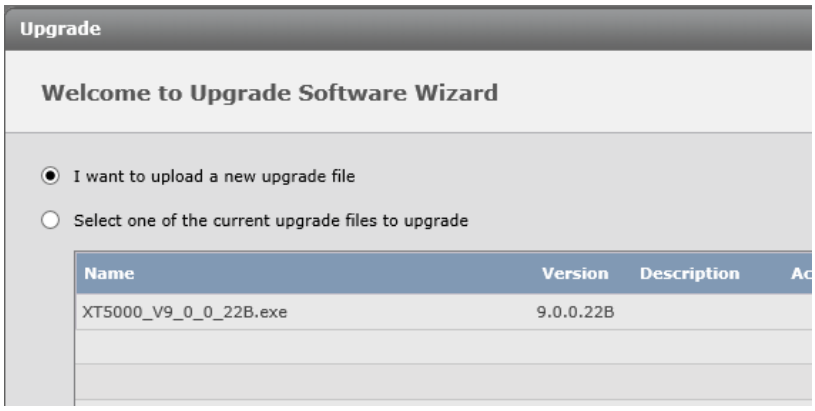
   Important:

   - You can simultaneously upgrade all endpoints of the same type.
   - You cannot upgrades LifeSize endpoints via Equinox Management.
5. Click **Manage** > **Upgrade Software**.



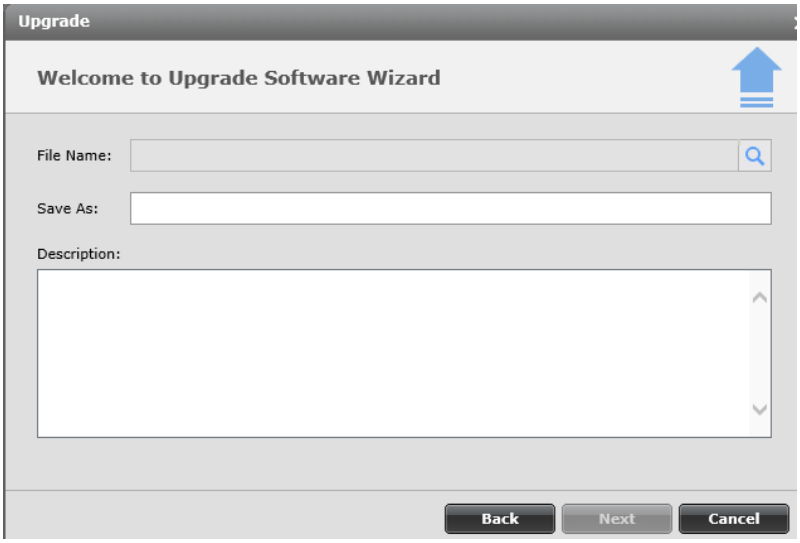
6. At the prompt, click **OK** to shut down the video device for a few minutes.

   This disconnects all active calls, and the system displays the first page of the Upgrade Software Wizard.



7. Either select one of the current upgrade files to upgrade, or select **I want to upload a new upgrade file** and click the **Next** button.

   The system displays the second page of the wizard.



8. Select the search icon to search for the package you want to upload.

   The package displays in the **File Name** field.

9. In the **Save As** field, enter a name by which you want to save the package, and optionally, add a description in the **Description** field.
10. Click **Next** to save the upgrade file and its information in Equinox Management.
11. If required, enter license keys.
12. Click **Apply**.

The system notifies that the video device shuts down for several minutes, causing all the active calls to be disconnected.

If using Application Server P/N 55876-00002, make sure to remove upgrade packages on a regular basis to ensure that there is enough disk space.

Related links

Upgrading, Backing Up and Restoring Video Device Software on page 425

Removing a software upgrade file from a video device

About this task

You can quickly and easily perform remote software upgrades of video devices from Avaya Equinox® Management by selecting the video device and applying an upgrade file. Upgrade files are supplied by the vendor of the video device.

For example, you can upgrade the Scopia Elite MCU, Web Collaboration server, room systems such as the Avaya Room System XT Series, and third party endpoints from Sony or Polycom.

This section describes how to remove the software upgrade file if it is no longer required in Equinox Management's list of upgrade files.

If using Application Server P/N 55876-00002, make sure to remove upgrade packages on a regular basis to ensure that there is enough disk space.

Procedure

1. Log in to the Equinox Management administrator portal.
2. Click the **Endpoints** or **Devices** tab.
3. Click the video device(s).

   Note:

   You can narrow your search of video devices by sorting them with one of the sidebar menu tabs. See Searching for a Video Device on page 421 for more information.

4. Click **Manage** > **Upgrade Software**.
5. At the prompt, click **OK** to shut down the video device for a few minutes. This disconnects all active calls.
6. Select the software upgrade file you require.
7. Click **Delete**.
8. Click **Apply** to save your changes.

   The software upgrade file is removed from the database.

Related links

Upgrading, Backing Up and Restoring Video Device Software on page 425

Backing up and duplicating a video device configuration

About this task

You can retrieve the configuration file for purposes of backup, before upgrade, or for remote configuration.

For example, you can retrieve and backup the configuration settings of Scopia Elite MCU, Web Collaboration server room systems such as the Avaya Room System XT Series, and third party endpoints from Sony or Polycom.

You can also apply those configuration settings across multiple video devices in your organization. The retrieved settings are only generic, therefore settings such as the endpoint's IP address are not stored.

This procedure describes how to retrieve the configuration file and store it in Equinox Management, and how to apply the settings to other video devices.

Procedure

1. Login to the Avaya Equinox® Management administrator portal.
2. Click the **Endpoints** or **Devices** tab.
3. Select the check box of the specific, online video device.

   Important:

   You can narrow your search of video devices by sorting them.

   Fore more information, see Searching for a Video Device on page 421.
4. Follow these steps to retrieve the configuration file:
   a. Click **Manage** > **Retrieve configuration file**.
   b. Click **Yes**.
   c. If required, change the filename and a description of the new configuration file.
   d. Click **OK** to save the file in the Equinox Management database.
5. Follow these steps to apply or retrieve a configuration file to other online video devices:
   a. Select the devices you want to update.
   b. Click **Update** > **Update configuration**.
   c. Click **Yes** to start updating the video device configuration.
   d. Click the file with which to update the selected video devices.

      The system displays a list of the configuration files that were previously retrieved, and are associated with the selected video device types in the Update Configuration window.
   e. Click **Apply**.

Related links

Upgrading, Backing Up and Restoring Video Device Software on page 425

Updating license keys

About this task

Network administrators can update license keys from Equinox Management when they increase capacity or increase ports with a flexible license.

The remote license update functionality is available for these network devices:

- MCUs except Scopia Elite MCU
- Web Collaboration server

Before you begin

Go to https://plds.avaya.com to apply for and download your upgrade package. If you upgrade to a major version, ensure you have a new license key.

Procedure

1. Login to the Equinox Management administrator portal.
2. Click **Devices** > **Devices by Type**.
3. Click the **Media Servers** or **Gateways**.
4. Click the link in the **Name** field of the required MCU.
5. Click the **Licensing** tab.

   If the license is temporary, the **Remaining Days** field displays the number of days before the license expires.
6. Enter the new license key in the **Update License Key** field.
7. Click **Apply**.

   The system confirms the license has been updated. If there are any problems with this process, verify the license key is accurate and that the system can properly access the MCU.

Related links

Upgrading, Backing Up and Restoring Video Device Software on page 425

Restoring the previous software version of a network device

About this task

This section explains how to restore a previous software version after you upgrade your network device. You can restore the same software version only once.

The following network devices can be restored:

- Scopia® Elite 6000 MCU

Only the most recent version of the device's software can be restored. During this procedure, the network device shuts down for a few minutes, causing all active calls to be disconnected.

The following parameters are not backed up and cannot be restored:

- IP address
- Default router IP address
- MTU size - the size of the packets received from the gateway
- DNS suffix
- DNS primary address
- DNS secondary address

Procedure

1. Access the Equinox Management administrator portal.
2. Search for an online network device.

   For more information, see Searching for a Video Device on page 421.
3. Select the network device whose software version you want to restore.
4. Click **Manage** > **Restore Previous Version**.

   The system informs you that all active calls on the device will be disconnected when you begin the process.

5. Click **Yes** in the confirmation message.

   The system displays the **Update Log** window, showing the task progress.

Related links

Upgrading, Backing Up and Restoring Video Device Software on page 425

Downgrading your Network Device

If necessary, you can downgrade your network device in one of the following ways:

- To downgrade one version back after you upgraded your network device, perform the procedure in Restoring the previous software version of a network device on page 431.
- To downgrade to a version earlier than the previous version, see Upgrading the software file of a video device on page 426.

Related links

Upgrading, Backing Up and Restoring Video Device Software on page 425

Defining Video Usage Defaults

About this task

As part of managing your MCU and other video network resources, you can define meeting policies for both scheduled and instant meetings (meetings initiated spontaneously). This is especially useful if you have limited MCU capacity or want to limit the bandwidth consumption.

These settings allow you to carefully monitor how meetings start and end, and their duration. You can also limit the number of participants in an instant meeting, or the default duration of meetings.

We recommend using Equinox Management meeting reports to inform you about the videoconferencing usage in your organization (Tracking system usage with reports on page 364). Devise company policies based on the reports, and then adjust the default meeting policies to suit the needs of your organization. For example, if management decides to cut on bandwidth costs and reports show some video meetings last several hours, you can limit the default meeting duration to help participants focus on shorter meetings.

Procedure

1. Access the Equinox Management administrator portal.

2. Select **Settings** > **Meetings** > **Policies**.
3. Define settings for meetings that users schedule in advance to reserve video network resources, such as MCUs and endpoints.

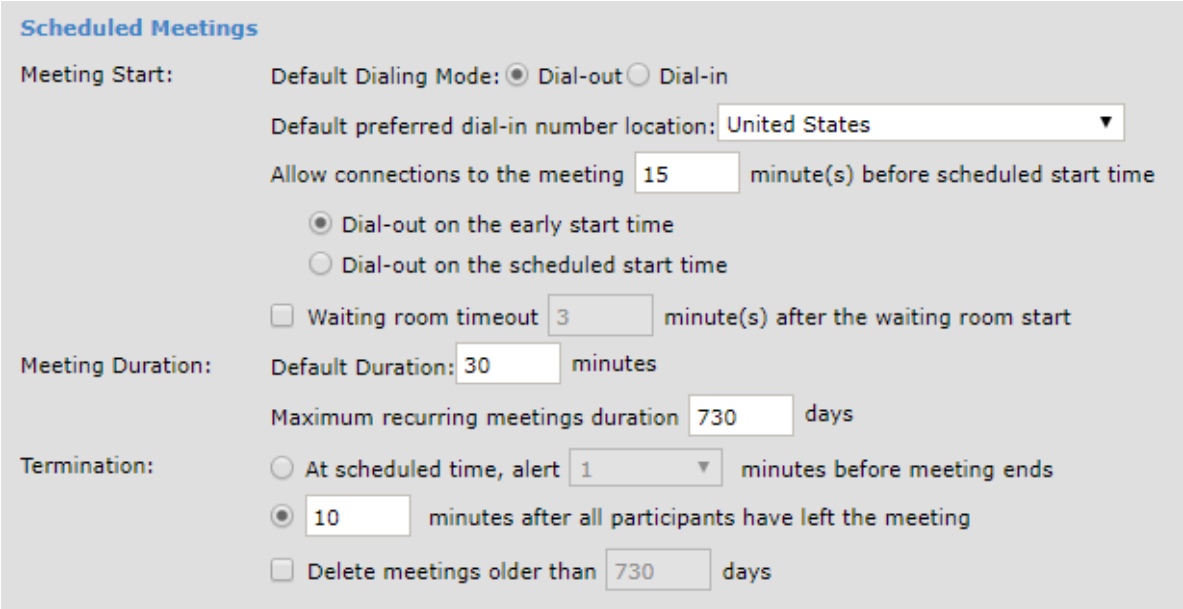


Figure 153: Defining policies for scheduled meetings

Table 72: Defining policies for scheduled meetings

Field	Description
Default Duration	Enter the default meeting duration for all meetings scheduled from the Equinox Management user portal. Users can modify this when scheduling a meeting. A few minutes before the default end time, users see an alert and can extend the meeting. For example, if management decides to cut on bandwidth costs and reports show some video meetings last several hours, you can limit the default meeting duration to help participants focus on shorter meetings. This does not apply to meetings scheduled from Microsoft Outlook.

Table continues…

Field	Description
Default Dialing Mode	Define how participants join a videoconference, based on your corporate culture: • **Dial-out**: The system automatically calls out to each participant on their dedicated endpoint. This option is best if most users just want to join in the quickest way possible, without having to look up the meeting information. • **Dial-in**: Each participant joins the videoconference from the meeting invitation link or by dialing the meeting ID. This option is best if most users prefer to control when they join the meeting, without any disruptions.
Termination	Define when the videoconference ends, according to the available resources in your organization: • **At scheduled time**: Select this option to end meetings automatically at the scheduled end time. Even if a meeting ends early, the resources are reserved for this meeting until the end time. Select the number of minutes before the meeting ends, to send an alert to the meeting moderator/organizer. • **After all participants left the meeting**: Enter the number of minutes after participants have left to end the meeting. If a meeting ends early, the resources can be used for other videoconferences.
Maximum Recurring Meetings Duration	Define the maximum number of occurrences a user can schedule for recurring meetings. This can be useful to keep more time slots open for future meetings, and prevent users from cluttering the meeting slots by scheduling meetings very far in advance.
Launch Meetings [ ] Minute(s) Before Scheduled Time	Define when participants can join the meeting, if they try to join before the scheduled time. If there are many meetings scheduled for adjacent time slots, this can help manage resources by preventing users from starting meetings before the designated time. If the virtual room is already being used for another meeting, users cannot join until that meeting ends.
Waiting Room Timeout	You can define a time by which, if the host does not enter the waiting room, the meeting automatically ends. This frees up resources used by a meeting that is not taking place.
Meeting Auto Extend Length	Define the number of minutes to automatically extend a videoconference if participants are still connected.
Maximum Length of Meeting Extension	Define the maximum time that a videoconference can be automatically extended beyond its original end time.

Table continues…

Field	Description
Delete Meetings Older than	Define when to delete meetings from the list in the **Meeting** tab. This is useful when monitoring bandwidth and other statistics from past meetings. You can modify this value depending on whether you want a more comprehensive list, or you are tracking only the most recent meetings.

4. Define settings for instant meetings, which are initiated spontaneously by users without reserving MCUs and other video network resources:

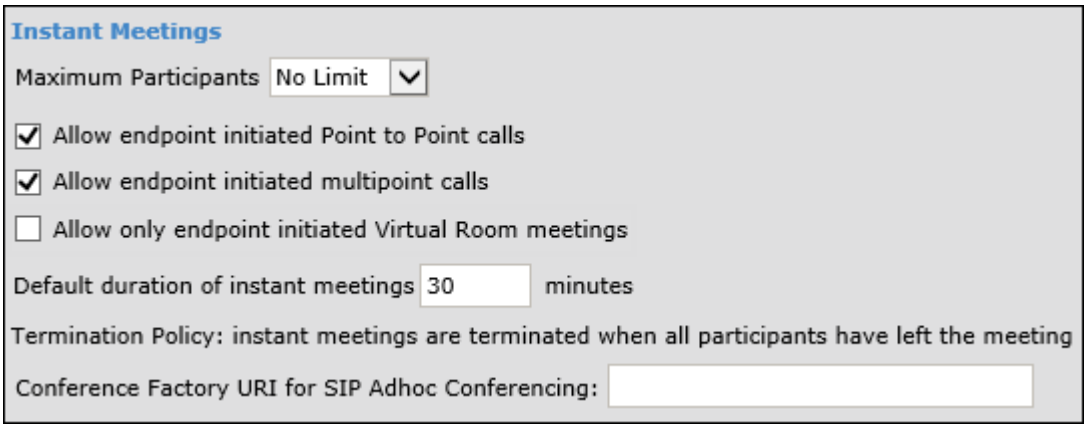


Figure 154: Defining policies for instant meetings

Table 73: Defining policies for instant meetings

Field	Description
Maximum Participants	Define the maximum number of participants that can be invited to a meeting initiated spontaneously. When meeting organizers reach the limit, they receive an error message when trying to invite additional participants. This is useful to manage resources, since larger meetings must be scheduled in advance.
Allow endpoint initiated Point to Point calls	Allow dedicated video endpoints to initiate direct calls to another endpoint, without routing it via an MCU. Disable this option to allow only calls that go through the MCU. This is especially useful for service providers. For example, you may want to disable this field to conserve bandwidth, using it only for meetings with more than two participants.
Allow endpoint initiated multipoint calls	Allow dedicated video endpoints to start a meeting with multiple endpoints. Disable this option to make sure that all meetings with more than two participants are scheduled.

Table continues…

Field	Description
Allow only endpoint initiated Virtual Room meetings	Allow dedicated video endpoints to initiate meetings with multiple endpoints from a virtual room only, allowing you to maintain stricter control over how videoconferences are started. Endpoints cannot dial other endpoints or the MCU to start a meeting. This is especially useful for service providers. You may want to disable this field, for example, to allow users without a virtual room to start meetings.
Default duration of instant meetings	Enter the default meeting duration for all instant meetings. Participants are notified when this time is reached, and if there are enough resources, meetings are auto-extended until all participants disconnect. For example, if you see from the meeting reports that most meetings last longer than 30 minutes, you can increase the default end time.

5. Select **Apply**.

Related links

Maintaining your Videoconferencing Network on page 378

Maintaining Scheduled Meetings

This section explains how to maintain scheduled meetings.

Related links

Maintaining your Videoconferencing Network on page 378
Searching for a Meeting on page 437
Modifying Upcoming Meetings on page 439

Searching for a Meeting

About this task

You can search for a specific meeting, to monitor or terminate the meeting. You can also access meeting information by selecting the meeting name link.

Procedure

1. Log in to the Equinox Management administrator portal.
2. Select the **Meetings** tab.

   The list of all ongoing meetings is displayed in the window.

3. Select the **Now (Live)** tab in the sidebar menu to narrow the meeting search to current multipoint or point-to-point videoconferences, as required.
4. Select the **Past** or **Future** tabs to search for past or upcoming meetings, respectively.
5. Perform any of the following:
   - Enter the partial or complete name of the meeting in the search field.

     If any part of the meeting name matches the search string, the meeting record is displayed in the search results.
   - Select the icon to set up any of the advanced search fields described in this table:

     Table 74: Searching for a meeting

Field Name	Description
Name	Enter the partial or complete name of the meeting in the field.
Meeting ID	Enter the partial or complete meeting ID in the field. If any part of the meeting ID matches the search string, the meeting record is displayed in the search results.
E.164	Enter the E.164 number of an attending endpoint in the field. If any part of the E.164 number matches the search string, the meeting record is displayed in the search results.
Type	Search in one of these meeting lists: - All the meetings - Multipoint meetings - Point-to-point calls
From	Select the calendar icon in the **From** field, and select a date and time in the window that opens. Meetings scheduled after the selected time are listed.
To	Select the calendar icon in the **To** field, and select a date and time in the window that opens. Meetings scheduled before the selected time are listed.

Related links

Maintaining Scheduled Meetings on page 437

Modifying Upcoming Meetings

About this task

You can reschedule upcoming meetings to another time, change meeting parameters or delete the meeting request through the user portal. See the *How to Start a Videoconference* for more information.

You can access the user portal from the administrator web interface by selecting the Avaya logo.

You can also delete an upcoming meeting from the administrator web interface, as described in this procedure.

Procedure

1. Log in to the Equinox Management administrator portal.
2. Select the **Meetings** tab in the sidebar menu.
3. Display the list of future meetings by selecting one of these tabs under the **Future** tab in the sidebar menu:
   - **All** lists future meetings.
   - **Tomorrow** displays meetings scheduled for the following day.
   - **Next Week** lists meetings scheduled for the upcoming week.
4. Select the meeting you want to delete. To delete all the meetings in the current view, select the list heading.
5. Select **Delete**.
6. At the prompt, select **Yes**.

   The participants receive an email indicating that the meeting is cancelled.

Related links

Maintaining Scheduled Meetings on page 437

Disaster recovery in a geographic redundancy deployment

With disaster recovery, you can restore system functionality in the event of a technological disaster in Equinox Management, such as an entire data center being nonfunctional. Typically, failure of one of the Equinox Management servers, with no resolution possible in an agreed-upon timeframe, requires disaster recovery.

With a geographic redundancy deployment, you can restore functionality during disaster recovery. However, after you start disaster recovery, not all system functions operate as required.

During disaster recovery, only the following components become operational:

- Geographic redundancy Equinox Management server
- Equinox Media Server
- Equinox H.323 Edge server

The local Avaya Aura Web Gateway and WebRTC are not operational after disaster recovery. Additionally, joining a meeting through an Avaya IX™ Workplace Client is also unavailable, although you can dial a virtual room directly.

When performing disaster recovery, you configure only those devices that are located in the same failed data center. You must shut down these devices before entering disaster recovery mode.

The following diagram outlines the decision making process of disaster recovery:

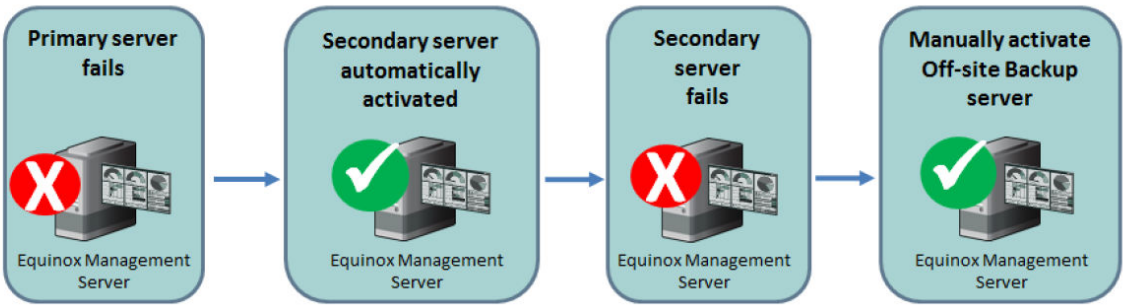


Figure 155: Disaster Recovery Decision Making Process

Related links

Maintaining your Videoconferencing Network on page 378
Activating disaster recovery in a geographic redundancy deployment on page 440
Resuming normal operations after disaster recovery on page 442

Activating disaster recovery in a geographic redundancy deployment

Before you begin

- Ensure that you have access to the following components:
  - Customer DNS Server
  - VCentre
  - Customer Load Balancer or Customer Reverse Proxy
- Modify the Infoblox DNS so that **Time To Live (TTL)** = **30 minutes**. This automatically changes the IP address of the DNS record after 30 minutes.
- For external clients, Customer Load Balancer or Customer Reverse Proxy for reverse proxy must also have a modified IP address so that it points to the same IP address to which the DNS record points. This change takes effect immediately.

Procedure

1. Log on to the Equinox Management administrator portal.

   The portal displays the following page with the system's current status.

Figure 156: System Status Page

2. Click **Promote Off-site Backup Server to Active** to activate the off-site backup server.

   The portal displays a warning page.

3. Ensure that you shut down the primary and secondary servers at the main site, and then click **Process**.

   On the Equinox Management administrator portal, the **Redundancy** status displays in red while disaster recovery is being processed.

   After processing has completed, a confirmation page displays, indicating that the backup server is now active.

4. Select **OK**. The offsite backup server restarts automatically, and you are directed to the login page to re-login.

5. If a message appears stating that the page is unavailable, refresh your browser.

6. To modify the media server settings:

   a. After logging in to the administrator portal, click **Devices** > **Media Servers**.

   b. Select the hyperlink of the relevant IP address.

      The portal displays the device's configuration page.

   c. Click **Configuration** > **Protocols**.

   d. In both the **H.323 Protocol** and **SIP Protocol** sections, modify the value to the backup server's IP address.

   e. Click **Apply**.

   f. Click (**Devices** > **Media Servers**) to return to the **Media Servers** page.

g. Click the **Configurations** tab and modify the value of the **SIP Proxy Server** field to the same IP address you specified for the **SIP Protocol**, above.

h. On the **Media Servers** page (**Devices** > **Media Servers**), click the hyperlink of the media server's IP address and verify that all connections are active.

7. To modify the H.323 Edge Server settings:

   a. In the administrator portal, select **Devices** > **H.323 Edge Servers**.

   b. Select the hyperlink of the relevant IP address.

   c. Select the **Configuration** tab.

   d. In the **Gatekeeper Address** field, modify the value to the backup server's IP address.

   e. Click **Apply**.

8. Ensure that the devices are registered correctly by doing the following:

   a. In the administrator portal, click **Settings** > **Local Services**.

      The portal displays the **Local Services** page.

   b. Click **H.323 Gatekeeper**.

   c. Expand the **Registered Endpoints** section and verify that the correct IP addresses are registered.

Related links

Disaster recovery in a geographic redundancy deployment on page 439

Resuming normal operations after disaster recovery

About this task

Use this procedure to resume normal system operations after completing disaster recovery for Equinox Management.

Procedure

1. Reset the Customer DNS Server and Customer Load Balancer or Customer Reverse Proxy to the main server's IP address, and wait 30 minutes for the change to take effect.

2. Verify that the original Equinox Management instances are operational by pinging each.

3. In a web browser, enter the IP address of the Equinox Management main server.

   The webpage displays a message indicating that the server is in standby mode and is inaccessible.

4. Log into the Equinox Management administrator portal and click ≡ > **Redundancy Setup**.

   The portal displays the first page of the Redundancy Setup Recovery Wizard.

5. Click **Revert to Primary server at the Main Site**, and then click **Next**.

   The portal displays the second page of the Redundancy Setup Recovery Wizard.

6. Select the server to which you want to return service, and click **Next**.

   The portal displays the third page of the Redundancy Setup Recovery Wizard and all servers on which Equinox Management is running. A green light indicates that the servers are running. If you do not see a green light, restart the server by using VMWare.

Figure 157: Redundancy Setup Recovery Wizard — Page 3

7. Click **Proceed**.

   The portal displays the fourth page of the Redundancy Setup Recovery Wizard and the recovery process' progress.

   When the process is complete, the servers restart automatically, and the screen displays the Equinox Management administrator portal login page. If it does not, wait 30 minutes for the DNS records to take effect. If the webpage still does not display the login page, ensure that Infoblox is configured correctly.

8. To return devices to normal operations, set all devices to refer to the main server's IP address. See Activating disaster recovery in a geographic redundancy deployment on page 440.

9. Verify that the devices are registered correctly. See Activating disaster recovery in a geographic redundancy deployment on page 440.

Related links

Disaster recovery in a geographic redundancy deployment on page 439

Retrieving the Customer Support Package

About this task

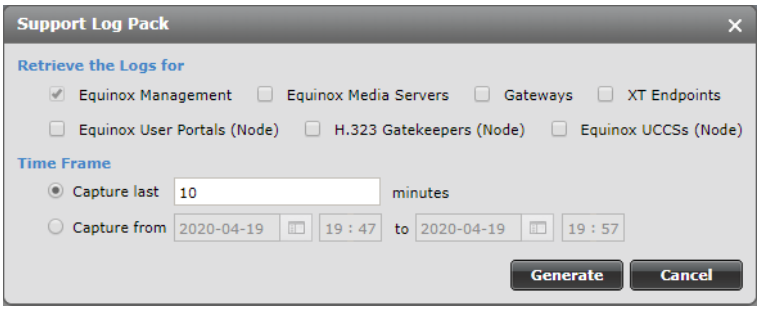
The customer support package is a zipped file of bundled logs and configuration files which you can download and send to Customer Support for debugging. You can retrieve the package for these products:

- Avaya Room System XT Series
- Media server products except Scopia Elite MCU
- Avaya Equinox® H.323 Edge server
- Avaya Web Collaboration server

Procedure

1. Access the Equinox Management administrator portal.
2. Click ≡ > **Support Log Pack**.

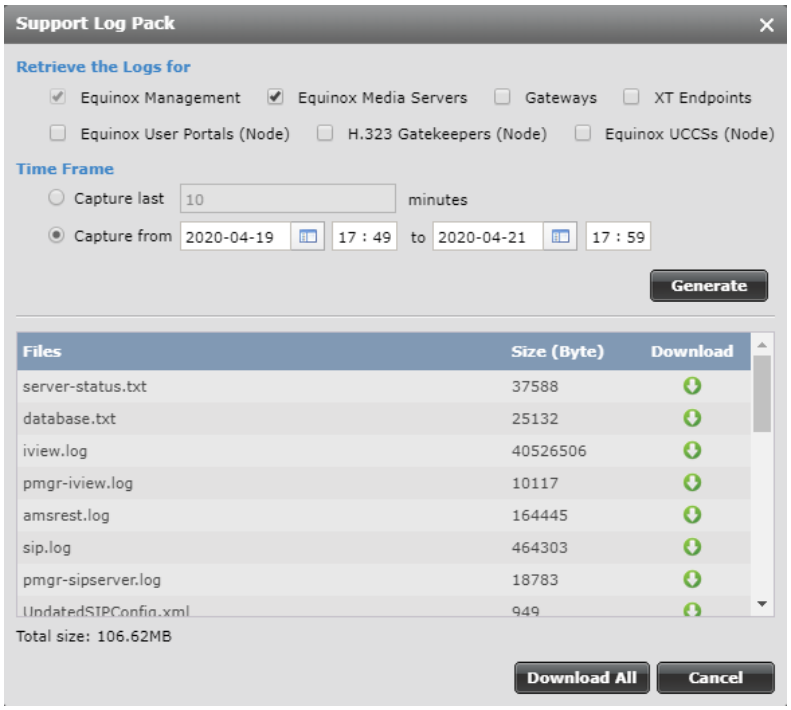
   The system displays the **Support Log Pack** dialog.



3. Select the check boxes of the components and at least a two day date range.
4. Click **Generate** to generate the log file for the customer support package.

   Avaya Equinox® Management takes a few minutes to create the package, depending on the amount of information.

   The system displays a list of the generated logs for download.



5. Click green download arrows to download individual logs or click the **Download All** button to download a zip file containing all the generated logs to your PC.

Related links

Maintaining your Videoconferencing Network on page 378

Chapter 14: Resources

Documentation

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

Title	Use this document to:	Audience
Implementing		
Deploying Avaya Equinox® Solution	Plan for and deploy Avaya Equinox® Solution	Partners, Services, and Support personnel
Deployment Guide for Avaya Equinox® H.323 Edge	Plan for and deploy Avaya Equinox® H.323 Edge	Partners, Services, and Support personnel
Deployment Guide for Avaya Room System XT Series	Plan for and deploy Avaya Room System XT Series	Partners, Services, and Support personnel
Installing and Administering Avaya Collaboration Unit CU360	Plan for and deploy Avaya Collaboration Unit CU360	Partners, Services, and Support personnel
Deployment Guide for Avaya XT Telepresence	Plan for and deploy Avaya XT Telepresence	Partners, Services, and Support personnel
Avaya Equinox® Solution Guide for Small to Medium (SMB) Enterprises	Plan for and deploy Avaya Equinox® Solution for small and medium enterprises	Partners, Services, and Support personnel
Avaya Equinox® Solution Guide for Medium to Large Enterprises	Plan for and deploy Avaya Equinox® Solution for medium and large enterprises	Partners, Services, and Support personnel
Avaya Equinox® Solution Guide for Large Enterprises and Service Providers	Plan for and deploy Avaya Equinox® Solution for large enterprises and service providers	Partners, Services, and Support personnel
Installation Notes — Discovering the IP address of the XT Server	Install XT Server	Partners, Services, and Support personnel

Table continues…

Title	Use this document to:	Audience
Rack Mounting Guide for Avaya Scopia® Elite 6000 MCU	Install the Avaya Scopia® Elite 6000 MCU hardware	Partners, Services, and Support personnel
Avaya Aura® Core Solution Description	Overview of the Avaya Aura® components and information on the deployment of these components	Partners, Services, and Support personnel
Avaya Aura® Communication Manager Overview and Specification	Overview of Avaya Aura® Communication Manager components and information on the deployment of these components	Partners, Services, and Support personnel
Avaya Aura® Presence Services Overview and Specification	Overview of Avaya Aura® Presence Services components and information on the deployment of these components	Partners, Services, and Support personnel
Avaya Aura® Session Manager Overview and Specification	Overview of Avaya Aura® Session Manager components and information on the deployment of these components	Partners, Services, and Support personnel
Avaya Aura® System Manager Overview and Specification	Overview of Avaya Aura® System Manager components and information on the deployment of these components	Partners, Services, and Support personnel
Avaya Multimedia Messaging Overview and Specification	Overview of Avaya Multimedia Messaging components and information on the deployment of these components	Partners, Services, and Support personnel
Avaya Session Border Controller for Enterprise Overview and Specification	Overview of Avaya Session Border Controller for Enterprise components and information on the deployment of these components	Partners, Services, and Support personnel
Deploying Avaya Aura® Device Services	Plan for and deploy Avaya Aura® Device Services	Partners, Services, and Support personnel
Deploying Avaya Aura® Web Gateway	Plan for and deploy Avaya Aura® Web Gateway	Partners, Services, and Support personnel
Deploying and Updating Avaya Aura® Media Server Appliance	Plan for and deploy Avaya Aura® Media Server on either of the following appliances: • Virtual appliances: Avaya Aura® MS appliances on the Appliance Virtualization Platform or VMware® virtualized environment. • Physical appliances: Avaya Aura® MS appliances on Avaya Common Servers.	Partners, Services, and Support personnel

Table continues…

Title	Use this document to:	Audience
Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS	Plan for and deploy Avaya Aura® Media Server application. Avaya provides a non-appliance, software-only, application version of Avaya Aura® MS which is installed on servers that you provide.	
Administering		
Administrator Guide for Avaya Scopia® Elite 6000 MCU	Perform administration tasks for Avaya Scopia® Elite 6000 MCU	System administrators
Administrator Guide for Avaya Scopia® Elite 6000 MCU for Avaya Aura® Power Suite	Perform administration tasks for Avaya Scopia® Elite 6000 MCU for Avaya Aura® Power Suite	System administrators
Administering Avaya Equinox® Media Server	Perform administration tasks for Avaya Equinox® Media Server	System administrators
Administrator Guide for Avaya Equinox® Management	Perform administration tasks for Avaya Equinox® Management	System administrators
Administrator Guide for Avaya Equinox® Streaming and Recording Server	Perform administration tasks for Avaya Equinox® Streaming and Recording Server	System administrators
Quick Setup Guide for Avaya XT5000 Series Codec Only	Perform administration tasks for the Avaya XT5000 Series codec	System administrators
Avaya XT5000 Series Codec Only	Perform administration tasks for the Avaya XT5000 Series codec	System administrators
Avaya XTE240	Perform administration tasks for Avaya XTE240	System administrators
Avaya XT Series Premium 3–way Microphone Pod	Perform administration tasks for Avaya XT Series Premium 3–way Microphone Pod	System administrators
Avaya XT4300	Perform administration tasks for Avaya XT4300	System administrators
Avaya XT4300 Codec Only	Perform administration tasks for the Avaya XT4300 codec	System administrators
Avaya Room System XT7100 Codec Only	Perform administration tasks for the Avaya Room System XT7100 codec	System administrators
Avaya XT Series Deluxe Camera	Perform administration tasks for Avaya XT Series Deluxe Camera	System administrators
Avaya XT Series Flex Camera	Perform administration tasks for Avaya XT Series Flex Camera	System administrators
Quick Tips for Avaya Room System XT Series	Perform administration tasks for Avaya Room System XT Series	System administrators
Supporting		

Table continues…

Title	Use this document to:	Audience
Reference Guide for Avaya Equinox® Management XML API	Understand how to perform administration tasks on Avaya Equinox® Management	System administrators, Customers, Partners, Services, and Support personnel
SAMPLE Reference Guide for Avaya Equinox® Management XML API	Understand how to perform administration tasks on Avaya Equinox® Management	System administrators, Customers, Partners, Services, and Support personnel
Reference Guide for Avaya Equinox® Management SNMP Traps	Understand how to configure Avaya Equinox® Management to send information to a remote SNMP management client of its operational status	System administrators, Customers, Partners, Services, and Support personnel
Reference Guide for Avaya Equinox® Management CDR Files	Understand how to perform administration tasks on Avaya Equinox® Management	System administrators, Customers, Partners, Services, and Support personnel
Reference Guide for Port Security for Avaya Equinox® Solution	Understand how to perform the administration tasks on Avaya Equinox® Solution	System administrators, Customers, Partners, Services, and Support personnel
Avaya WebRTC Snap-in Reference	Understand how to perform the administration tasks on Avaya WebRTC Snap-in	System administrators, Customers, Partners, Services, and Support personnel
Using		
User Guide for Avaya Equinox® Management	Understand the features of and use Avaya Equinox® Management	Customers
Using Avaya Equinox® Unified Portal	Understand the features of and use Avaya Equinox® Unified Portal	Customers
User Guide for Avaya Equinox® H.323 Edge Client	Understand the features of and use Avaya Equinox® H.323 Edge Client	Customers
User Guide for Avaya Room System XT Series	Understand the features of and use Avaya Room System XT Series	Customers
Using Avaya Collaboration Unit CU360	Understand the features of and use Avaya Collaboration Unit CU360	Customers
Avaya Collaboration Unit CU360 Quick Setup Guide	Understand the features of and use Avaya Collaboration Unit CU360	Customers

Table continues…

Title	Use this document to:	Audience
Avaya Collaboration Unit CU360 Quick Tips Guide	Understand the features of and use Avaya Collaboration Unit CU360	Customers
Using Avaya Collaboration Control for Android	Understand the features of and use Avaya Collaboration Control	Customers
Using Avaya Collaboration Control for iOS	Understand the features of and use Avaya Collaboration Control	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**.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support By Product** > **Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or more of the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

The list displays the product-specific Port Matrix document.

7. Click **Enter**.

Avaya Documentation Center navigation

The latest 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 on 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 by doing one of the following:
  - Click **Filters** to select a product and then type key words in**Search**.
  - From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- 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 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.

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field and press **Enter** or click **>** to search for the course.

Course code	Course title
Avaya Equinox® administration training course	
2038W	Avaya Equinox® Administration
Avaya Equinox® Team Engagement solution courses	
3140W	Avaya Equinox® Solutions Overview
3170W	Avaya Equinox® Solutions Customer Field Study
3171T	APDS Avaya Enterprise Team Engagement Solutions Online Test
Avaya Equinox® Over The Top solution courses	
3281W	Avaya Video Conferencing Solutions Overview
3283W	Avaya Video Conferencing Solutions Customer Field Study
3271T	APDS Avaya Video Conferencing Solutions Online Test
Avaya Equinox® Sales course	
3140WD02	Designing Avaya Equinox® Clients & Breeze Client SDK Sales Readiness Quiz
3140WD03	Avaya Equinox® Sales Readiness — Design Delta Training

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.

Appendix A: List of preferred dial in numbers examples

This list is provided as examples only. Replace <dialin number> with the actual phone number starting with the country code.

- dialin_es_ar=Argentina|Argentina|+<dialin number>
- dialin_en_au_mel=Australia, Melbourne|Australia, Melbourne|+<dialin number>
- dialin_en_au_syd=Australia, Sydney|Australia, Sydney|+<dialin number>
- dialin_fr_be=Belgium|Belgique|+<dialin number>
- dialin_pt_br=Brazil|Brasil|+<dialin number>
- dialin_en_ca_bel=Canada, Belleville|Canada, Belleville|+<dialin number>
- dialin_en_ca_ott=Canada, Ottawa|Canada, Ottawa|+<dialin number>
- dialin_es_co=Colombia|Colombia|+<dialin number>
- dialin_hr_hr=Croatia|Croatia|+<dialin number>
- dialin_da_dk=Denmark|Danmark|+<dialin number>
- dialin_de_de=Germany|Deutschland|+<dialin number>
- dialin_es_es=Spain|España|+<dialin number>
- dialin_fr_fr=France|France|+<dialin number>
- dialin_en_in_ban=India, Bangalore|India, Bangalore|+<dialin number>
- dialin_en_in_gur=India, Gurgaon|India, Gurgaon|+<dialin number>
- dialin_en_in_hyd=India, Hyderabad|India, Hyderabad|+<dialin number>
- dialin_en_in_mum=India, Mumbai|India, Mumbai|+<dialin number>
- dialin_en_in_pun=India, Pune|India, Pune|+<dialin number>
- dialin_id_id=Indonesia|Indonesia|+<dialin number>
- dialin_en_ie=Ireland|Ireland|+<dialin number>
- dialin_he_il=Israel|Israel|+<dialin number>
- dialin_it_it=Italy|Italia|+<dialin number>
- dialin_hu_hu=Hungary|Magyarország|+<dialin number>

- dialin_en_my=Malaysia|Malaysia|+<dialin number>
- dialin_es_mx=Mexico|México|+<dialin number>
- dialin_nl_nl=Netherlands|Nederland|+<dialin number>
- dialin_en_nz=New Zealand|New Zealand|+<dialin number>
- dialin_nb_no=Norway|Norge|+<dialin number>
- dialin_en_ph=Philippines|Philippines|+<dialin number>
- dialin_pl_pl=Poland|Polska|+<dialin number>
- dialin_ar_sa=Saudi Arabia, Riyadh|Saudi Arabia, Riyadh|+<dialin number>
- dialin_en_za=South Africa|South Africa|+<dialin number>
- dialin_fr_ch=Switzerland|Suisse|+<dialin number>
- dialin_sv_se=Sweden|Sverige|+<dialin number>
- dialin_tr_tr=Turkey|Türkiye|+<dialin number>
- dialin_en_us_east=US East Region|US East Region|+<dialin number>
- dialin_en_us_west=US West Region|US West Region|+<dialin number>
- dialin_en_ustf=US/Canada Toll Free|US/Canada Toll Free|+<dialin number>
- dialin_ar_ae=United Arab Emirates|United Arab Emirates|+<dialin number>
- dialin_en_gb=United Kingdom|United Kingdom|+<dialin number>
- dialin_de_at=Austria|Österreich|+<dialin number>
- dialin_cs_cz=Czech Republic|Česká republika|+<dialin number>
- dialin_ru_ru=Russia|Россия|+<dialin number>
- dialin_th_th=Thailand|ประเทศไทย|+<dialin number>
- dialin_zh_cn=Shanghai|上海|+<dialin number>
- dialin_zh_cn_zho=China, Zhongshan|中国中山|+<dialin number>
- dialin_zh_cn_bei=China, Beijing|中国北京|+<dialin number>
- dialin_zh_cn_dal=China, Dalian|中国大连|+<dialin number>
- dialin_zh_cn_gua=China, Guangzhou|中国广州|+<dialin number>
- dialin_zh_tw=Taiwan|台灣|+<dialin number>
- dialin_zh_sg=Singapore|新加坡|+<dialin number>
- dialin_ja_jp=Japan|日本|+<dialin number>
- dialin_zh_hk=Hong Kong|香港特別行政區|+<dialin number>
- dialin_ko_kr=South Korea|대한민국|+<dialin number>

Appendix B: Equinox audio prompts and announcements

The supported Avaya Equinox® audio prompts and announcements are separated into the following two groups:

- Audio prompts that are heard when the participant is using *(number) on the dial pad. It is only relevant for phones (mobile / PSTN), Avaya IX™ Workplace Client and XT. It is not relevant for Avaya Equinox® Meetings for Web as there is no dial pad in the GUI.
- Audio prompts that are heard when the participant performs an action like join or leave the conference.

To hear these voice prompts you must be in a virtual room conference and the following parameters must be set in the My Meeting portal of the virtual room owner:

- Meeting Type — Audio Service or Audio Service with Web Collaboration
- Entry Announcement — Name

DTMF tones and prompt file names

DTMF Tone	Name	Prompt transcript	Prompt file name	Description	Room Owner	Guest / No moderator
*	Moderator Menu	If you are the moderator the following is played: To return to the meeting press pound. To stop moderating press one. To un-mute your line press two. To play back roster, press three. To show or hide participants' names press four. To terminate the meeting press five. To change the main video layout press six. To block admission to the meeting press seven. To dial out press eight. To mute unmute all lines except yourself press nine. To start or stop the recording press zero.	• PlayModeratorRecordRosterMenu.wav • PlayModeratorRecordMenu.wav	Start playing the menu. While the menu is playing the participant cannot hear the conference. The audio **To play back roster, press three.** is only played when the Virtual Room Meeting Type selected does not support video.	Moderator	

Table continues…

DTMF Tone	Name	Prompt transcript	Prompt file name	Description	Room Owner	Guest / No moderator
*	User Menu	If you are not the moderator the following is played: To return to the meeting press pound. To become the moderator press one. To un-mute your line press two.	PlayMenuNoLPP.wav	Start playing the menu. While the menu is playing the participant cannot hear the conference.	User	
*#	Return to meeting	No recording		Return to the meeting from the menu at any time.	Moderator or User	
*1	Become moderator or cease being moderator.	If you are not the moderator, the following is played followed by the Moderator Menu. You are now the moderator. If you are moderator, the following is played: You are no longer the meeting moderator.	• YouAreTheModerator.wav • ModeratorReleased.wav	Become the **moderator** and moderate the call using other codes. If there is a moderator PIN it must be entered.	N/A	
*2	Un-mute your line	The following is played: Un-muted	Unmuted.wav	Un-mute your line in the conference.	Moderator or User	Yes

Table continues…

DTMF Tone	Name	Prompt transcript	Prompt file name	Description	Room Owner	Guest / No moderator
*3	Playback roster			Play back the recorded audio of only the participants names in order. **Note:** This feature requires a **high capacity** audio media server.	Moderator	Yes
*4	Show / Hide participants names			Toggle **Show** or **Hide** the participants names. The video participants are able or unable to see the other participants' names in the video sub frames or squares depending on the toggle setting.	Moderator	N/A
*5	Terminate the meeting	The following is played: The meeting is about to terminate.	ConferenceTerminating.wav	Terminate the meeting. End the conference and disconnect all participants.	Moderator	N/A

Table continues…

DTMF Tone	Name	Prompt transcript	Prompt file name	Description	Room Owner	Guest / No moderator
*6	Change the main video layout	The following is played: Change layout. Please enter the number of participants to be seen on the screen or press zero for automatic layout.	LayoutControl.wav	Change the main video layout.	Moderator	N/A
*7	Block/Allow admission to the meeting	If admission to the meeting is allowed, the following is played: Admission to the meeting is now blocked. If admission to the meeting is blocked, the following is played: Admission to the meeting is now allowed.	• Freezed.wav • Unfreezed.wav	Toggle **Block** or **Allow** admission to the meeting. Participants can not join or re-join the conference.	Moderator	N/A
*8	Invite participants	To dial out press eight	EnterPartNumber.wav	The moderator can dial out and invite participants to the call.	Moderator	N/A

Table continues…

DTMF Tone	Name	Prompt transcript	Prompt file name	Description	Room Owner	Guest / No moderator
*9	Mute / Un-mute all lines except yourself	The following is played: To mute all participants except yourself, press zero. To un-mute all participants, press one. After pressing zero, the following is played, “All participants are now muted.” and you hear “unmuted” which is only for you.	• MuteUnmuteAllControl.wav • AllMuted.wav	Mute or un-mute all lines except yourself. This is the same function as lecture mode.	Moderator	N/A
*0	Start / Stop Recording		• RecordingStarted.wav • RecordingNotStarted.wav • RecordingEnded.wav	Toggle **Start** or **Stop Recording**. The meeting is recorded.	Moderator	N/A
#	Return to the meeting		No prompt	Return to the meeting.	Moderator or User	Pass

Table 75: Audio prompts file names and transcripts

#	Prompt file name	Prompt transcript	Description
1	SayYourName1.wav	After the tone, please say your name.	
2	SayYourName2.wav	After the tone, please say your name, then press the number sign key.	Number sign key is dialpad key with # label.

Table continues…

#	Prompt file name	Prompt transcript	Description
3	SayYourName3.wav	After the tone, please say your name, then press the pound sign.	Pound key is dialpad key with # label. Enter a virtual room. The following parameters must be set in the My Meeting portal of the virtual room owner: • Meeting Type — Audio Service or Audio Service with Web Collaboration • Entry Announcement — Name
4	SayYourName4.wav	After the tone, please say your name, then press the hash key.	Hash key is dialpad key with # label.
5	SingleJoinedMeeting.wav	<name> has joined the meeting.	Name is spoken first, for example "Roger Connery has joined the meeting."
6	MultiJoinedMeeting.wav	Participants have joined the meeting <name+name+name>	This string is played when more participants join the meeting. For example "Participants have joined the meeting, Roger Connery, Jennifer, Jane Crowley."
7	SingleLeftMeeting.wav	<name> has left the meeting.	<Name> is spoken first, for example "Roger Connery has left the meeting."
8	MultiLeftMeeting.wav	Participants have left the meeting <name+name+name>	This string is played when more participants have left the meeting. For example "Participants have left the meeting - Roger Connery, Mike Smith, Jane Crowley."
9	Someone.wav	Someone…	This prompt is played together with prompt 5 or 7 if the user did not record his own name and it plays **someone**. For example "Someone has joined the meeting."
10	NoName.wav	no name	This prompt is played after prompt 6 or 8 so that the user will hear “Participants are joining the meeting, Roger Connery, **no name**, Mike Smith, …”
11a	ThereIs.wav	There is <number>…	This prompt is played together with prompt 13a if there is only one participant

Table continues…

#	Prompt file name	Prompt transcript	Description
11b	ThereAre.wav	There are <number>…	This prompt is played together with prompt 13b or 13c if there are two or more participants
13a	ParticipantInMeeting.wav	… participant in your meeting.	This prompt is played after prompt 11a.
13b	ParticipantsFewInMeeting.wav	… participants in your meeting.	For Russian only - if there are 2+3+4 participants or number of participants ends with 2+3+4.
13c	ParticipantsInMeeting.wav	… participants in your meeting.	This prompt is played after prompt 11b if there are five or more participants.
16	NumOfRecords.wav	The number of recorded names is <number> …	
17	Including.wav	… including <name+name +name>	
18	Zero.wav	Zero	The number fragment is combined with other fragments that contain <number> variable
19	One.wav	One	The number fragment is combined with other fragments that contain <number> variable
20	Two.wav	Two	The number fragment is combined with other fragments that contain <number> variable
21	Three.wav	Three	The number fragment is combined with other fragments that contain <number> variable
22	Four.wav	Four	The number fragment is combined with other fragments that contain <number> variable
23	Five.wav	Five	The number fragment is combined with other fragments that contain <number> variable
24	Six.wav	Six	The number fragment is combined with other fragments that contain <number> variable
25	Seven.wav	Seven	The number fragment is combined with other fragments that contain <number> variable
26	Eight.wav	Eight	The number fragment is combined with other fragments that contain <number> variable

Table continues…

#	Prompt file name	Prompt transcript	Description
27	Nine.wav	Nine	The number fragment is combined with other fragments that contain <number> variable
28	Ten.wav	Ten	The number fragment is combined with other fragments that contain <number> variable
29	Eleven.wav	Eleven	The number fragment is combined with other fragments that contain <number> variable
30	Twelve.wav	Twelve	The number fragment is combined with other fragments that contain <number> variable
31	Thirteen.wav	Thirteen	The number fragment is combined with other fragments that contain <number> variable
32	Fourteen.wav	Fourteen	The number fragment is combined with other fragments that contain <number> variable
33	Fifteen.wav	Fifteen	The number fragment is combined with other fragments that contain <number> variable
34	Sixteen.wav	Sixteen	The number fragment is combined with other fragments that contain <number> variable
35	Seventeen.wav	Seventeen	The number fragment is combined with other fragments that contain <number> variable
36	Eighteen.wav	Eighteen	The number fragment is combined with other fragments that contain <number> variable
37	Nineteen.wav	Nineteen	The number fragment is combined with other fragments that contain <number> variable
38	Twenty.wav	Twenty	The number fragment is combined with other fragments that contain <number> variable
39	Thirty.wav	Thirty	The number fragment is combined with other fragments that contain <number> variable
40	Forty.wav	Forty	The number fragment is combined with other fragments that contain <number> variable

Table continues…

#	Prompt file name	Prompt transcript	Description
41	Fifty.wav	Fifty	The number fragment is combined with other fragments that contain <number> variable
42	Sixty.wav	Sixty	The number fragment is combined with other fragments that contain <number> variable
43	Seventy.wav	Seventy	The number fragment is combined with other fragments that contain <number> variable
44	Eighty.wav	Eighty	The number fragment is combined with other fragments that contain <number> variable
45	Ninety.wav	Ninety	The number fragment is combined with other fragments that contain <number> variable
46	Hundred.wav	Hundred	The number fragment is combined with other fragments that contain <number> variable
47	Hundreds.wav	Hundreds	The number fragment is combined with other fragments that contain <number> variable
48	PlaybackRoster.wav	To playback roster press three.	
49	ToCallOperator.wav	To call the operator press star zero.	
50	PleaseHoldMusic.wav	Please hold, we are transferring you to operator.	
51	OperatorBusy.wav	Operator is busy now, please press one to keep waiting.	
52	TypePin.wav	Thank you for attending the meeting. Enter the meeting PIN followed by the pound key.	
53	WrongPinDisconnecting.wav	Incorrect PIN. Disconnecting	
54	WrongPinTryAgain.wav	Incorrect PIN. Enter the correct PIN followed by the pound key.	
	FirstParticipant.wav	Thank you for attending the meeting. You are the first participant. Please hold.	
55	EnterPartNumber.wav	To dial out, please dial the number of the party you wish to invite to the meeting, followed by the pound key.	

Table continues…

#	Prompt file name	Prompt transcript	Description
56	TakeModeratorFirst.wav	This action requires moderator privileges.	
57	ModeratorAlreadyTaken.wav	Another participant is already moderating the meeting.	
58	PlayMenu.wav	To return to the meeting - press pound key. To become the moderator, press one. To mute or unmute your line, press two. To control the volume of your line, press three.	
59	EnterModeratorPIN.wav	Enter the moderator PIN followed by the pound key.	
60	PlayModeratorMenu.wav	To return to the meeting, press pound key. To stop moderating, press one. To mute or unmute your line, press two. To control the volume of your line, press three. To show or hide participants' names, press four. To terminate the meeting, press five. To change the main video layout, press six. To block admission to the meeting, press seven. To dial out, press eight. To mute or unmute all lines except yourself, press nine.	
61	PlayModeratorMenu.wav	To return to the meeting, press pound key. To stop moderating, press one. To unmute your line, press two. To show or hide participants' names, press four. To terminate the meeting, press five. To change the main video layout, press six. To allow admission to the meeting, press seven. To dial out, press eight. To mute unmute all lines except yourself, press nine.	Avaya Scopia® Elite 6000 MCU and Equinox Media Server.
62	EnterBreakoutSession.wav	You have joined a sub-conference.	
63	LeaveBreakoutSession.wav	You have left the sub-conference.	
64	JoinNotAllowed.wav	For security reasons, please join from the MeetingPlace web conferencing interface. Goodbye.	

Table continues…

#	Prompt file name	Prompt transcript	Description
65	NoVideoResources.wav	All video resources are currently in use. Please try again later.	
66	ConferenceTerminating.wav	The meeting is about to terminate.	Select the **End Meeting for Everyone** conference feature.
67	OrganizerNotYetJoined.wav	Please wait for the meeting moderator.	
68	ConferenceStarts.wav	The meeting will now begin.	
69	OrganizerLeft.wav	You have been moved to the waiting room, please wait.	
70	ConferenceResume.wav	The meeting will now resume.	
71	ModeratorPINIsNotValidTryAgain.wav	You have entered an incorrect moderator PIN.	
72	YouAreTheModerator.wav	You are now the moderator.	
73	Muted.wav	Muted	
74	Unmuted.wav	Unmuted	
75	VolumeControl.wav	To decrease the volume, press zero. To increase, press one.	
76	Freezed.wav	Admission to the meeting is now blocked.	Select the **Lock Meeting** conference feature.
77	Unfreezed.wav	Admission to the meeting is now allowed.	Select the **Lock Meeting** conference feature.
78	Dialing.wav	Dialling.	
79	InvalidInput.wav	Invalid input.	
80	ModeratorReleased.wav	You are no longer the meeting moderator.	
81	LayoutControl.wav	Change layout. Please enter the number of participants to be seen on the screen or press zero for automatic layout.	
82	MuteUnmuteAllControl.wav	To mute all participants except yourself, press zero. To unmute all participants, press one.	
83	AllMuted.wav	All participants are now muted.	• Select the **Mute Everyone** conference feature. • Select the **Lecture Mode** conference feature.
84	AllUnmuted.wav	All participants are now unmuted.	• Select the **Unmute Everyone** conference feature. • Select the **Lecture Mode** conference feature.

Table continues…

#	Prompt file name	Prompt transcript	Description
86	PlayModeratorFreezedMenu.wav	To return to the meeting, press pound key. To stop moderating, press one. To mute or unmute your line, press two. To control the volume of your line, press three. To show or hide participants' names, press four. To terminate the meeting, press five. To change the main video layout, press six. To allow admission to the meeting, press seven. To dial out, press eight. To mute or unmute all lines except yourself, press nine.	
86b	PlayModeratorFreezedMenu.wav	To return to the meeting, press pound key. To stop moderating, press one. To unmute your line, press two. To show or hide participants' names, press four. To terminate the meeting, press five. To change the main video layout, press six. To allow admission to the meeting, press seven. To dial out, press eight. To mute unmute all lines except yourself, press nine.	Avaya Scopia® Elite 6000 MCU and Equinox Media Server.
87	ConfList.wav	Thank you for calling. To create a new meeting or join by ID, press zero. To select a meeting from the list, press the entry number.	
88	EnterConfId.wav	Enter the meeting ID followed by the pound key.	
89	InvalidConfId.wav	You have entered an incorrect meeting ID.	
90	CreateConfPin.wav	To create a PIN code to protect this meeting, enter a PIN code followed by the pound key. Enter only the pound key if you do not want PIN protection.	
91	CreateConfFailed.wav	Failed to create a meeting.	
92	CreateConfInvalidPin.wav	You have entered an invalid PIN. Enter a valid PIN using digits only followed by the pound key.	
93	TransferFailed.wav	Failed to connect to the meeting. Disconnecting.	

Table continues…

#	Prompt file name	Prompt transcript	Description
94	InvalidConfIdEnterConf.wav	You have entered an incorrect meeting ID. Please enter your meeting ID followed by the pound key.	
95	CreateConfFailedEnterConf.wav	Failed to create a meeting. To join an existing meeting, enter the meeting ID followed by the pound key.	
96	ConfEndin10min.wav	The meeting is about to end in less than ten minutes.	
97	ConfEndin5min.wav	The meeting is about to end in less than five minutes.	
98	ConfEndin2min.wav	The meeting is about to end in less than two minutes.	
99	ConfEndin1min.wav	The meeting is about to end in less than one minute.	
100	Disconnecting.wav	Disconnecting	
101	NoInputDetected.wav	No input has been detected	
103	PlayMenuNoLPP.wav	To return to the meeting, press pound key. To become the moderator, press one. To mute or unmute your line, press two. To control the volume of your line, press three.	
103	PlayMenuNoLPP.wav	To return to the meeting, press pound key. To become the moderator, press one. To unmute your line, press two.	Avaya Scopia® Elite 6000 MCU and Equinox Media Server
104	FirstParticipantModerator.wav	Thank you for attending the meeting. You are the first participant. You have moderation privileges.	
105	ConnectedAudioOnly.wav	You are connected with audio only due to resource limitations. Please contact your system administrator if needed.	
106	FailureTermination.wav	The meeting is about to terminate due to a temporary failure. Please redial the meeting ID and report the incident to your system administrator.	
107	ConfExtendedAutomatically.wav	The meeting has been automatically extended.	

Table continues…

#	Prompt file name	Prompt transcript	Description
108	ConfExtendedModerator.wav	The meeting has been extended by the moderator.	
109	PleaseHold.wav	Thank you, please hold.	
110	ConfListNoCreate.wav	Thank you for calling. To join a meeting by ID, press zero. To select a meeting from the list, press the entry number.	
111	PleaseHoldULaw.wav	Please hold while we transfer you to your meeting	
112	DisconnectingDueToLicense.wav	Your endpoint cannot be connected to this meeting due to licensing issues. Please contact your administrator for assistance.	
113	WaitingRoomBackground.wav	The meeting has not yet started. You will be automatically placed in the meeting when the moderator joins. If you are the moderator press star one now.	
114	WaitingRoomBackgroundNoStar.wav	The meeting has not yet started, you'll be automatically placed in the meeting when the moderator joins.	
115	RecordingStarted.wav	Please note the meeting is being recorded.	Select the **Recording** conference feature.
116	PinEnterExpiredTryAgain.wav	You did not enter a PIN. Please enter a PIN followed by the pound key.	
117	ModeratorPINEnterExpiredTryAgain.wav	You did not enter the moderator PIN. Please enter the moderator PIN followed by pound key.	
118	RecordingEnded.wav	Please note the meeting is no longer being recorded.	Select the **Stop Recording** conference feature.
119	MeetingLockedEnterPIN.wav	This meeting is locked. Enter the meeting PIN followed by the pound key and then wait for the moderator to give you permission to join.	
120	MeetingLockedNotification.wav	This meeting is locked. Press pound key to ask the moderator to join or hang up.	
121	PinEnterExpiredDisconnecting.wav	You did not enter a PIN. Disconnecting.	

Table continues…

#	Prompt file name	Prompt transcript	Description
122	JoinRequestDenied.wav	Sorry, you have not been given permission to join the meeting. Thank you and goodbye.	
123	JoinRequestNotification.wav	Someone wants to join your meeting. Press star to allow them to join, press pound key to reject.	
124	PlayModeratorRecordMenu.wav	To return to the meeting, press pound key. To stop moderating, press one. To unmute your line, press two. To show or hide participants' names, press four. To terminate the meeting, press five. To change the main video layout, press six. To block admission to the meeting, press seven. To dial out, press eight. To mute unmute all lines except yourself, press nine. To start or stop the recording, press zero.	Similar to segment 125, only difference is in word "block vs allow" (highlighted in red)
125	PlayModeratorFreezedRecordMenu.wav	To return to the meeting, press pound key. To stop moderating, press one. To unmute your line, press two. To show or hide participants' names, press four. To terminate the meeting, press five. To change the main video layout, press six. To allow admission to the meeting, press seven. To dial out, press eight. To mute unmute all lines except yourself, press nine. To start or stop the recording, press zero.	Similar to segment 124, only difference is in word "block vs allow" (highlighted in red)
126	RecordingNotStarted.wav	The recording could not be started.	
127	ProblemTryRejoin.wav	Sorry, there is a problem with the meeting controls. Please try ending the call and rejoining the meeting.	
128	RecordingPaused.wav	Recording is paused.	
129	RecordingResumed.wav	Recording is resumed.	
130	UnmuteToSpeak.wav	You can now unmute to speak.	
131	ReturnToMeetingOption.wav	To return to the meeting, press pound.	

Table continues…

#	Prompt file name	Prompt transcript	Description
132	BecomeTheModeratorOption.wav	To become the moderator, press one.	
133	UnmuteYourLineOption.wav	To unmute your line, press two.	
134	PlaybackRosterOption.wav	To playback roster, press three.	
135	KnockerWithRecordedName.wav	<name> wants to join your meeting. Press star to allow them to join, press pound to reject.	Do not translate or record <name>, this item is dynamically replaced by the participant's name. In the second sentence the term "them" refers to a single user but it is used this way to be gender neutral.
136	StopModeratingOption.wav	To stop moderating, press one.	
137	ShowHidePartsOption.wav	To show or hide participants names, press four.	
138	TerminateMeetingOption.wav	To terminate the meeting, press five.	
139	ChangeMainLayoutOption.wav	To change the main video layout, press six.	
140	BlockAdmissionOption.wav	To block admission to the meeting, press seven.	
141	AllowAdmissionOption.wav	To allow admission to the meeting, press seven.	
142	DialOutOption.wav	To dial out, press eight.	
143	MuteUnmuteAllOption.wav	To mute or unmute all lines except yourself, press nine.	
144	StartStopRecording.wav	To start or stop recording, press zero.	
145	BlastDialInitiated.wav	The Blast Dial has been initiated.	Blast dial is a feature which enables moderators to dial out from a conference to a number of callers simultaneously. Moderators use a dial list, which contains the names and telephone numbers of their contacts during a blast dial. The Blast Dial feature enables a meeting host to start a meeting quickly with a predetermined group of people and is protected by a password.

Table continues…

#	Prompt file name	Prompt transcript	Description
146	BlastDialCannotInitiated.wav	The Blast Dial cannot be initiated.	Blast dial is a feature which enables moderators to dial out from a conference to a number of callers simultaneously. Moderators use a dial list, which contains the names and telephone numbers of their contacts during a blast dial. The Blast Dial feature enables a meeting host to start a meeting quickly with a predetermined group of people and is protected by a password.
147	RequestedToJoinTheMeeting.wav	Hi, you are requested to join the meeting.	
148	PressAnyKey.wav	Please press any number key to continue.	
149	EnterParticipantID.wav	Please enter the participant ID followed by the pound sign.	
150	ParticipantIDInvalid.wav	The participant ID is invalid.	
151	MuteYourLineOption.wav	To mute your line, press two.	

Appendix C: Avaya Equinox® Management reports fields

Lists of fields in Avaya Equinox® Management reports.

Calls - Multipoint

- Category
  - Meetings
  - Calls
- Sub-Category (for Meetings category)
  - Number of meetings
  - Number of scheduled meetings
  - Number of instant meetings
  - Number of adhoc meetings
- Sub-Category (for Calls category)
  - Number of calls
  - Number of video calls
  - Number of transcoded video calls
  - Number of multi-stream video calls
  - Number of audio calls
  - Number of audio calls on full-video media server
  - Number of audio calls on audio media server
  - Number of WebRTC calls
  - Number of IX Workplace for Windows calls
  - Number of IX Workplace for Mac calls
  - Number of IX Workplace for iOS calls
  - Number of IX Workplace for Android calls
  - Number of SIP audio calls other than IX Workplace
  - Number of SIP video calls other than IX Workplace

    - Number of auto-attendant calls
    - Call duration (m)
  - Display by
    - Time of the day
    - Day of the week
    - Day of the month
    - Month of the year
  - Locations
    - All
    - <Defined locations>
    - N/A

The generated table with Meetings category selected has the following fields:

- Total meetings
- Total scheduled meetings
- Total scheduled meetings reserved from Microsoft Outlook
- Total scheduled meetings reserved from Portal
- Total scheduled meetings protected with a meeting PIN
- Total instant meetings
- Total adhoc meetings
- Total meetings where no participants have video
- Total meetings where all participants have video
- Total meetings with mixed audio and video participants
- Total meetings where presentation is used
- Total cascaded meetings
- Total recorded meetings
- Total auto-attendant sessions
- Total meeting duration (m)
- Max. meeting duration (m)
- Average meetings duration (m)
- Max. calls in meetings
- Average calls in meetings

The generated table with Calls category selected has the following fields:

- Total calls
- Total incoming calls

- Total outgoing calls
- Total video calls
- Total transcoded video calls
- Total multi-stream video calls
- Total audio calls
- Total presentation only calls
- Total IX Workplace for Windows calls
- Total IX Workplace for Mac calls
- Total IX Workplace for Android calls
- Total IX Workplace for iOS calls
- Total Web Gateway calls
- Total WebRTC calls
- Total SIP calls
- Total SIP video calls other than IX Workplace Client
- Total SIP audio calls other than IX Workplace Client
- Total H.323 calls
- Total H.320 calls
- Total WCS calls
- Total auto-attendant calls
- Total call duration (m)
- Maximum call duration (m)
- Average call duration (m)

Virtual Rooms

- **Usage Summary (CSV)** — Generates a CSV spreadsheet with the following fields:
  - VMR number
  - User's first name
  - User's last name
  - User's email address
  - Number of meetings
  - Number of video meetings
  - Number of audio meetings
  - Number of meetings with mixed audio and video participants
  - Average meeting duration (m)
  - Total meeting duration (m)

- **Inventory (CSV)** — Generates a CSV spreadsheet with the following fields:
  - VMR number
  - VMR name
  - VMR description
  - User's first name
  - User's last name
  - User's email address
  - User profile
  - User's location preference
  - User's audio prompt language
  - Account status
  - Meeting type
  - VMR meeting invitation language
  - Entry Announcement
  - Exit Announcement
  - Max. participants to play entry/exit tone
  - Max. participants to play the entry/exit name
  - Preferred dial-in location
  - Enable sharing mode
  - Enable/disable moderator PIN
  - Enabled/disabled permanent meeting PIN
  - Enabled/disabled one-time meeting PIN
  - Allow requests to join locked meeting
  - Auto recording
  - Waiting room

Reserved Meetings

Generates and saves a CSV spreadsheet using a date range you select, with the following fields:

- Meeting start time
- Duration, min
- Organizer's user first name
- Organizer's user last name
- User's email address
- Meeting ID
- Meeting type

- Has meeting PIN or not
- Scheduled by plugin or not

Glossary

1080p	See Full HD on page 483.
720p	See HD on page 485.
AAC	Avaya Aura® Conferencing is an enterprise conferencing and collaboration product providing ondemand audio, video, and Web conferencing and advanced conference controls for a seamless unified communications experience. The AAC video conferencing supports high-definition resolutions up to 720p through a software video routing technology that is based on the H.264 AVC and SVC standard. The distributed architecture of AAC utilizes advanced bandwidth management and optimization techniques where Avaya Aura® Media Servers are deployed at the edge of the network to optimize the WAN bandwidth usage. This supports large scale, high quality audio and video conferencing in an enterprise network.
AGC (Automatic Gain Control)	Automatic Gain Control (AGC) smooths audio signals through normalization, by lowering sounds which are too strong and strengthening sounds which are too weak. This is relevant with microphones situated at some distance from the speaker, like room systems. The result is a more consistent audio signal within the required range of volume.
Alias	An alias in H.323 represents the unique name of an endpoint. Instead of dialing an IP address to reach an endpoint, you can dial an alias, and the gatekeeper resolves it to an IP address.
Auto-Attendant	Auto-Attendant is a video-based IVR which provides quick access to meetings through a set of visual menus. Participants can select the DTMF tone-based menu options using the standard numeric keypads of endpoints. Auto-Attendant works with H.323 and SIP endpoints.
Avaya Content Slider	See Content Slider on page 480.
Avaya Equinox® Streaming and Recording Manager	The Avaya Equinox® Streaming and Recording Manager provides a web-based interface to configure and manage Equinox Streaming and Recording Server software, devices, services, and users. The Equinox Streaming and Recording Server Manager application resides on a single hardware platform and provides access to all content in the Equinox Streaming and Recording Server environment.

Avaya Equinox® Streaming and Recording Manager Portals	The Equinox Streaming and Recording Server Manager provides a portal for administering content. When you log in to the web interface, you can access the Administrator portal.
Balanced Microphone	A balanced microphone uses a cable that is built to reduce noise and interference even when the cable is long. This reduces audio disruptions resulting from surrounding electromagnetic interference.
Bitrate	Bitrate is the speed of data flow. Higher video resolutions require higher bitrates to ensure the video is constantly updated, thereby maintaining smooth motion. If you lower the bitrate, you lower the quality of the video. In some cases, you can select a lower bitrate without noticing a significant drop in video quality; for example during a presentation or when a lecturer is speaking and there is very little motion. Bitrate is often measured in kilobits per second (kbps).
Call Control	See Signaling on page 490.
Cascaded Videoconference	A cascaded videoconference is a meeting distributed over more than one physical Scopia Elite MCU and/or Equinox Media Server, where a master MCU/Media Server connects to one or more slave MCUs/Media Servers to create a single videoconference. It increases the meeting capacity by combining the resources of several MCUs/Media Servers. This can be especially useful for distributed deployments across several locations, reducing bandwidth usage.
CDN	Equinox Streaming and Recording enables you to publish content to the cloud, using a virtual delivery node (VDN) and a content delivery network (CDN). The VDN and the network of the CDN act as one delivery mechanism. When a user creates a recording (program), they can choose to distribute it to the CDN, as well as to the regular delivery node (DN).
CIF	CIF, or Common Intermediate Format, describes a video resolution of 352 × 288 pixels (PAL) or 352 x 240 (NTSC). This is sometimes referred to as Standard Definition (SD).
Conference Point	The Avaya Equinox® Streaming and Recording Conference Point is a video conferencing gateway appliance that captures standard or high definition video conferences. It transcodes, creates, and records the video conferences in a streaming media format. You can use it to capture H.323 video for instant video webcasting or on-demand publishing.
Content Slider	The Avaya Content Slider stores the data already presented in the videoconference and makes it available for participants to view during the meeting.

Continuous Presence

Continuous presence enables viewing multiple participants of a videoconference at the same time, including the active speaker. This graphics-intensive work requires scaling and mixing the images together into one of the predefined video layouts. The range of video layouts depends on the type of media processing supported, typically located in the MCU/Media Server.

Control

Control, or media control, sets up and manages the media of a call (its audio, video and data). Control messages include checking compatibility between endpoints, negotiating video and audio codecs, and other parameters like resolution, bitrate and frame rate. Control is communicated via H.245 in H.323 endpoints, or by SDP in SIP endpoints. Control occurs within the framework of an established call, after signaling.

CP

See Continuous Presence on page 481.

Dedicated Endpoint

A dedicated endpoint is a hardware endpoint for videoconferencing assigned to a single user. It is often referred to as a personal or executive endpoint, and serves as the main means of video communications for this user. For example, Avaya XTE240. It is listed in the organization's LDAP directory as associated exclusively with this user.

Delivery Node

The Avaya Equinox® Streaming and Recording Delivery Node provides on-demand and broadcast video delivery. You can use it alone or in a hierarchy of devices. It supports thousands of concurrent streams. The Delivery Node uses intelligent routing, content caching, and inherent redundancy to ensure transparent delivery of high-quality video.

Dial Plan

A dial plan defines a way to route a call and to determine its characteristics. In traditional telephone networks, prefixes often denote geographic locations. In videoconferencing deployments, prefixes are also used to define the type and quality of a call. For example, dial 8 before a number for a lower bandwidth call, or 6 for an audio-only call, or 5 to route the call to a different branch.

Dial Prefix

A dial prefix is a number added at the beginning of a dial string to route it to the correct destination, or to determine the type of call. Dial prefixes are defined in the organization's dial plan. For example, dial 9 for an outside line, or dial 6 for an audio only call.

Distributed Deployment

A distributed deployment describes a deployment where the solution components are geographically distributed in more than one network location.

DNS Server

A DNS server is responsible for resolving domain names in your network by translating them into IP addresses.

DTMF	DTMF, or touch-tone, is the method of dialing on touch-tone phones, where each number is translated and transmitted as an audio tone.
Dual Video	Dual video is the transmitting of two video streams during a videoconference, one with the live video while the other is a shared data stream, like a presentation.
Dynamic Video Layout	The dynamic video layout is a meeting layout that switches dynamically to include the maximum number of participants it can display on the screen (up to 9 on the XT Series, or up to 28 on Scopia Elite MCU and/or Equinox Media Server). The largest image always shows the active speaker.
Endpoint	An endpoint is a tool through which people can participate in a videoconference. Its display enables you to see and hear others in the meeting, while its microphone and camera enable you to be seen and heard by others. Endpoints include dedicated endpoints, like Avaya XTE240, software endpoints, mobile device endpoints, room systems like XT Series, and telepresence systems like Avaya XT Telepresence.
Endpoint Alias	See Alias on page 479.
FEC	Forward Error Correction (FEC) is a proactive method of sending redundant information in the video stream to preempt quality degradation. FEC identifies the key frames in the video stream that should be protected by FEC. There are several variants of the FEC algorithm. The Reed-Solomon algorithm (FEC-RS) sends redundant packets per block of information, enabling the sender (like the Scopia Elite MCU and/or Equinox Media Server) to manage up to ten percent packet loss in the video stream with minimal impact on the smoothness and quality of the video.
FECC	Far End Camera Control (FECC) is a feature of endpoint cameras, where the camera can be controlled remotely by another endpoint in the call.
Forward Error Correction	See FEC on page 482.
FPS	See Frames Per Second on page 482.
Frame Rate	See Frames Per Second on page 482.
Frames Per Second	Frames Per Second (fps), also known as the frame rate, is a key measure in video quality, describing the number of image updates per second. The average human eye can register up to 50 frames per second. The higher the frame rate, the smoother the video.
FTP	The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files from one host to another host over a TCP-based

network, such as the Internet. FTP is built on a client-server architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves using a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it.

Full HD

Full HD, or Full High Definition, also known as 1080p, describes a video resolution of 1920 x 1080 pixels.

Full screen Video Layout

The full screen view shows one video image. Typically, it displays the remote presentation, or, if there is no presentation, it displays the other meeting participant(s).

Gatekeeper

A gatekeeper routes audio and video H.323 calls by resolving dial strings (H.323 alias or URI) into the IP address of an endpoint, and handles the initial connection of calls. Gatekeepers also implement the dial plan of an organization by routing H.323 calls depending on their dial prefixes. Equinox Management includes a built-in Avaya Equinox H.323 Gatekeeper, while H.323 Gatekeeper is a standalone gatekeeper.

Gateway

A gateway is a component in a video solution which routes information between two subnets or acts as a translator between different protocols. For example, a gateway can route data between the headquarters and a partner site, or between two protocols like the 100 Gateway and another.

Geographic Redundancy

Geographic redundancy is a deployment of a redundant server in a geographically different location in case a local disaster happens. This server is an addition to the local high availability servers.

GLAN

GLAN, or gigabit LAN, is the name of the network port on the XT Series. It is used on the XT Series to identify a 10/100/1000MBit ethernet port.

H.225

H.225 is part of the set of H.323 protocols. It defines the messages and procedures used by gatekeepers to set up calls.

H.235

H.235 is the protocol used to authenticate trusted H.323 endpoints and encrypt the media stream during meetings.

H.239

H.239 is a widespread protocol used with H.323 endpoints, to define the additional media channel for data sharing (like presentations) alongside the videoconference, and ensures only one presenter at a time.

H.243

H.243 is the protocol used with H.323 endpoints enabling them to remotely manage a videoconference.

H.245

H.245 is the protocol used to negotiate call parameters between endpoints, and can control a remote endpoint from your local endpoint. It is part of the H.323 set of protocols.

H.261

H.261 is an older protocol used to compress CIF and QCIF video resolutions. This protocol is not supported by the XT Series.

H.263

H.263 is an older a protocol used to compress video. It is an enhancement to the H.261 protocol.

H.264

H.264 is a widespread protocol used with SIP and H.323 endpoints, which defines video compression. Compression algorithms include 4x4 transforms and a basic motion comparison algorithm called P-slices. There are several profiles within H.264. The default profile is the H.264 Baseline Profile, but H.264 High Profile uses more sophisticated compression techniques.

H.264 Baseline Profile

See H.264 on page 484.

H.264 High Profile

H.264 High Profile is a standard for compressing video by up to 25% over the H.264 Baseline Profile, enabling high definition calls to be held over lower call speeds. It requires both sides of the transmission (sending and receiving endpoints) to support this protocol. H.264 High Profile uses compression algorithms like:

- CABAC compression (Context-Based Adaptive Binary Arithmetic Coding)
- 8x8 transforms which more effectively compress images containing areas of high correlation

These compression algorithms demand higher computation requirements, which are offered with the dedicated hardware available in Equinox Solution components. Using H.264 High Profile in videoconferencing requires that both the sender and receiver's endpoints support it. This is different from SVC which is an adaptive technology working to improve quality even when only one side supports the standard.

H.320

H.320 is a protocol for defining videoconferencing over ISDN networks.

H.323

H.323 is a widespread set of protocols governing the communication between endpoints in videoconferences and point-to-point calls. It defines the call signaling, control, media flow, and bandwidth regulation.

H.323 Alias

See Alias on page 479.

H.350

H.350 is the protocol used to enhance LDAP user databases to add video endpoint information for users and groups.

H.460

H.460 enhances the standard H.323 protocol to manage firewall and NAT traversal using ITU-T standards. H.460–compliant endpoints can directly communicate with Equinox H.323 Edge. The endpoints act as H.460 clients and Equinox H.323 Edge acts as an H.460 server.

HD

A HD ready device describes its high definition resolution capabilities of 720p, a video resolution of 1280 x 720 pixels.

High Availability

High availability is a state where you ensure better service and less downtime by deploying additional servers. There are several strategies for achieving high availability, including deployment of redundant servers managed by load balancing systems.

High Definition

See HD on page 485.

High Profile

See H.264 High Profile on page 484.

HTTP

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

HTTPS

HTTPS is the secured version of the standard web browser protocol HTTP. It secures communication between a web browser and a web server through authentication of the web site and encrypting communication between them. For example, you can use HTTPS to secure web browser access to the web interface of many Equinox Solution products.

Image Resolution

See Resolution on page 489.

IVR

Pre-recorded greetings to participants and announcements as each new participant joins a meeting. You can record messages to provide custom greetings and announcements, but typically Equinox Management supplies these messages across all media servers in the organization.

kbps

Kilobits per second (kbps) is the standard unit to measure bitrate, measuring the throughput of data communication between two devices. Since this counts the number of individual bits (ones or zeros), you must divide by eight to calculate the number of kilobytes per second (KBps).

KVM

Kernel-based Virtual Machine

LDAP

LDAP is a widespread standard database format which stores network users. The format is hierarchical, where nodes are often represented as*branch location* > *department* > *sub-department*, or*executives* > *managers* > *staff members*. The database standard is employed by most user directories including Microsoft Active Directory. H.350 is an extension to the LDAP standard for the videoconferencing industry.

Lecture Mode

Lecture mode allows the participant defined as the lecturer to see all the participants, while they see only the lecturer. All participants are muted

except the lecturer, unless a participant asks permission to speak and is unmuted by the lecturer. This mode is tailored for distance learning, but you can also use it for other purposes like when an executive addresses employees during company-wide gatherings.

Legacy endpoints

Legacy endpoints are H.323–based endpoints that do not support H.460.

Load balancer

A load balancer groups together a set (or cluster) of servers to give them a single IP address, known as a virtual IP address. It distributes client service requests amongst a group of servers. It distributes loads according to different criteria such as bandwidth, CPU usage, or cyclic (round robin). Load balancers are also known as application delivery controllers (ADC).

Location

A location is a physical space (building) or a network (subnet) where video devices can share a single set of addresses. A distributed deployment places these components in different locations, often connected via a VPN.

Management

Management refers to the administration messages sent between components of the Equinox Solution as they manage and synchronize data between them. Management also includes front-end browser interfaces configuring server settings on the server. Management messages are usually transmitted via protocols like HTTP, SNMP, FTP or XML. For example, Equinox Management uses management messages to monitor the activities of an MCU/Media Server, or when it authorizes the MCU/Media Server to allow a call to proceed.

MBps

Megabytes per second (MBps) is a unit of measure for the bitrate. The bitrate is normally quoted as kilobits per second (kbps) and then converted by dividing it by eight to reach the number of kilobytes per second (KBps) and then by a further 1000 to calculate the MBps.

MCU

A Multipoint Control Unit (MCU) connects several endpoints to a single videoconference. It can manage multiple separate conferences simultaneously. It manages the audio mixing and creates the video layouts, adjusting the output to suit each endpoint's capabilities (transcoding). The term MCU refers to any Avaya or third party MCU.

Media

Media refers to the live audio, video and shared data streams sent during a call. Presentation and Far end camera control (FECC) are examples of information carried on the data stream. Media is transmitted via the RTP and RTCP protocols in both SIP and H.323 calls. The parallel data stream of both live video and presentation, is known as dual video.

Media Control

See Control on page 481.

Media Server

A Media Server connects several endpoints to a single videoconference and can manage multiple separate conferences simultaneously. It

manages the audio mixing and creates the video layouts, adjusting the output to suit each endpoint's capabilities (transcoding). The term Media Server refers to Avaya Equinox® Media Server. See also MCU.

Meeting type

Meeting types (also known as MCU/Media Server services) are meeting templates which determine the core characteristics of a meeting. For example, they determine if the meeting is audio only or audio and video, they determine the default video layout, the type of encryption, PIN protection and many other features. You can invoke a meeting type by dialing its prefix in front of the meeting ID. Meeting types are created and stored in the Avaya Equinox® Media Server, with additional properties in Equinox Management.

Moderator

A moderator has special rights in a videoconference, including blocking the sound and video of other participants, inviting new participants, disconnecting others, determining video layouts, and closing meetings. An owner of a virtual room is the moderator when the room is protected by a PIN. Without this protection, any participant can assume moderator rights.

MTU

The MTU, or Maximum Transmission Unit, is the maximum size of data packets sent around your network. This value must remain consistent for all network components, including servers like the MCU and/or Equinox Media Server and endpoints like XT Series and other network devices like network routers.

Multi-Point

A multi-point conference has more than two participants.

Multi-tenant

Service provider, or multi-tenant, deployments enable one installation to manage multiple organizations. All the organizations can reside as tenants within a single service provider deployment. For example, Equinox Management can manage a separate set of users for each organization, separate local administrators, separate bandwidth policies etc. all within a single multi-tenant installation.

NAT

A NAT, or Network Address Translation device, translates external IP addresses to internal addresses housed in a private network. This enables a collection of devices like endpoints in a private network, each with their own internal IP address, can be represented publicly by a single, unique IP address. The NAT translates between public and private addresses, enabling users toplace calls between public network users and private network users.

NetSense

NetSense is a proprietary Equinox Solution technology which optimizes the video quality according to the available bandwidth to minimize packet loss. As the available bandwidth of a connection varies depending on data traffic, NetSense's sophisticated algorithm dynamically scans the

video stream, and then reduces or improves the video resolution to maximize quality with the available bandwidth.

Nonce

A parameter that varies with time. A nonce can be a time stamp, a visit counter on a web page, or a special marker intended to limit or prevent the unauthorized replay or reproduction of a file.

Because a nonce changes with time, it is easy to tell whether or not an attempt at replay or reproduction of a file is legitimate; the current time can be compared with the nonce. If it does not exceed it or if no nonce exists, then the attempt is authorized. Otherwise, the attempt is not authorized.

In SSL / TLS, a nonce is a 32-bit timestamp and a 28-byte random field that is used during key exchange to prevent replay attacks.

OVA

Open Virtualization Appliance. An OVA contains the virtual machine description, disk images, and a manifest zipped into a single file. The OVA follows the Distributed Management Task Force (DMTF) specification.

Over The Top deployments

Over The Top deployments of Avaya Equinox® Solution are independent of Avaya Aura®. The deployments use port-based licensing.

Over The Top deployments are also called standalone deployments.

Packet Loss

Packet loss occurs when some of the data transmitted from one endpoint is not received by the other endpoint. This can be caused by narrow bandwidth connections or unreliable signal reception on wireless networks.

PaP Video Layout

The PaP (Picture and Picture) view shows up to three images of the same size.

Phantom Power

Microphones which use phantom power draw their electrical power from the same cable as the audio signal. For example, if your microphone is powered by a single cable, it serves both to power the microphone and transmit the audio data. Microphones which have two cables, one for sound and a separate power cable, do not use phantom power.

PiP Video Layout

The PiP (Picture In Picture) view shows a video image in the main screen, with an additional smaller image overlapping in the corner. Typically, a remote presentation is displayed in the main part of the screen, and the remote video is in the small image. If the remote endpoint does not show any content, the display shows the remote video in the main part of the screen, and the local presentation in the small image.

PLDS

Avaya’s Product Licensing Delivery System

Point-to-Point

Point-to-point is a feature where only two endpoints communicate with each other without using MCU/Media Server resources.

PoP Video Layout

The PoP (Picture out Picture) view shows up to three images of different size, presented side by side, where the image on the left is larger than the two smaller images on the right.

Prefix

See Dial Prefix on page 481.

PTZ Camera

A PTZ camera can pan to swivel horizontally, tilt to move vertically, and optically zoom to devote all the camera's pixels to one area of the image. For example, the XT Standard Camera is a PTZ camera with its own power supply and remote control, and uses powerful lenses to achieve superb visual quality. In contrast, fixed cameras like webcams only offer digital PTZ, where the zoom crops the camera image, displaying only a portion of the original, resulting in fewer pixels of the zoomed image, which effectively lowers the resolution. Fixed cameras also offer digital pan and tilt only after zooming, where you can pan up to the width or length of the original camera image.

QCIF

QCIF, or Quarter CIF, defines a video resolution of 176 × 144 pixels (PAL) or 176 x 120 (NTSC). It is often used in older mobile handsets (3G-324M) limited by screen resolution and processing power.

Redundancy

Redundancy is a way to deploy a network component, in which you deploy extra units as 'spares', to be used as backups in case one of the components fails.

Registrar

A SIP Registrar manages the SIP domain by requiring that all SIP devices register their IP addresses with it. For example, once a SIP endpoint registers its IP address with the Registrar, it can place or receive calls with other registered endpoints.

Resolution

Resolution, or image/video resolution, is the number of pixels which make up an image frame in the video, measured as the number of horizontal pixels x the number of vertical pixels. Increasing resolution improves video quality but typically requires higher bandwidth and more computing power. Techniques like SVC, H.264 High Profile and FEC reduce bandwidth usage by compressing the data to a smaller footprint and compensating for packet loss.

Restricted Mode

Restricted mode is used for ISDN endpoints only, when the PBX and line uses a restricted form of communication, reserving the top 8k of each packet for control data only. If enabled, the bandwidth values on these lines are in multiples of 56kbps, instead of multiples of 64kbps.

Room System

A room system is a hardware videoconferencing endpoint installed in a physical conference room. Essential features include its camera's ability to PTZ (pan, tilt, zoom) to allow maximum flexibility of camera angles

	enabling participants to see all those in the meeting room or just one part of the room.
RTCP	Real-time Control Transport Protocol, used alongside RTP for sending statistical information about the media sent over RTP.
RTP	RTP or Real-time Transport Protocol is a network protocol which supports video and voice transmission over IP. It underpins most videoconferencing protocols today, including H.323, SIP and the streaming control protocol known as RTSP. The secured version of RTP is SRTP.
RTSP	RTSP or Real-Time Streaming Protocol controls the delivery of streamed live or playback video over IP, with functions like pause, fast forward and reverse. While the media itself is sent via RTP, these control functions are managed by RTSP
Sampling Rate	The sampling rate is a measure of the accuracy of the audio when it is digitized. To convert analog audio to digital, it must collect or sample the audio at specific intervals. As the rate of sampling increases, it raises audio quality.
SBC	A Session Border Controller (SBC) is a relay device between two different networks. It can be used in firewall/NAT traversal, protocol translations and load balancing.
SD	Standard Definition (SD), is a term used to refer to video resolutions which are lower than HD. There is no consensus defining one video resolution for SD.
Service	Also known as MCU/Media Server service. See Meeting type on page 487.
SIF	SIF defines a video resolution of 352 x 240 pixels (NTSC) or 352 x 288 (PAL). This is often used in security cameras.
Signaling	Signaling, also known as call control, sets up, manages and ends a connection or call. These messages include the authorization to make the call, checking bandwidth, resolving endpoint addresses, and routing the call through different servers. Signaling is transmitted via the H.225.0/Q.931 and H.225.0/RAS protocols in H.323 calls, or by the SIP headers in SIP calls. Signaling occurs before the control aspect of call setup.
Single Sign On	Single Sign On (SSO) automatically uses your network login and password to access different enterprise systems. Using SSO, you do not need to separately login to each system or service in your organization.
SIP	Session Initiation Protocol (SIP) is a signaling protocol for starting, managing and ending voice and video sessions over TCP, TLS or UDP.

Videoconferencing endpoints typically are compatible with SIP or H.323, and in some cases (like Avaya Room System XT Series), an endpoint can be compatible with both protocols. As a protocol, it uses fewer resources than H.323.

SIP Registrar See Registrar on page 489.

SIP Server A SIP server is a network device communicating via the SIP protocol.

SIP URI See URI on page 493.

Slider See Content Slider on page 480.

SNMP Simple Network Management Protocol (SNMP) is a protocol used to monitor network devices by sending messages and alerts to their registered SNMP server.

Software endpoint A software endpoint turns a computer or portable device into a videoconferencing endpoint via a software application only. It uses the system's camera and microphone to send image and sound to the other participants, and displays their images on the screen.

SQCIF SQCIF defines a video resolution of 128 x 96 pixels.

SRTP Secure Real-time Transport Protocol (SRTP) adds security to the standard RTP protocol, which is used to send media (video and audio) between devices in SIP calls. It offers security with encryption, authentication and message integrity. The encryption uses a symmetric key generated at the start of the call, and being symmetric, the same key locks and unlocks the data. So to secure transmission of the symmetric key, it is sent safely during call setup using TLS.

SSO See Single Sign On on page 490.

Standard Definition See SD on page 490.

Streaming Streaming is a method to send live or recorded videoconferences in one direction to viewers. Recipients can only view the content; they cannot participate with a microphone or camera to communicate back to the meeting.

STUN A STUN server enables you to directly dial an endpoint behind a NAT or firewall by giving that computer’s public internet address.

SVC SVC extends the H.264 codec standard to dramatically increase error resiliency and video quality without the need for higher bandwidth. It is especially effective over networks with high packet loss (like wireless networks) which deliver low quality video. It splits the video stream into layers, comprising a small base layer and then additional layers on top which enhance resolution, frame rate and quality. Each additional layer is

only transmitted when bandwidth permits. This allows for a steady video transmission when available bandwidth varies, providing better quality when the bandwidth is high, and adequate quality when available bandwidth is poor.

SVGA

SVGA defines a video resolution of 800 x 600 pixels.

Switched video

Switching is the process of redirecting video as-is without transcoding, so you see only one endpoint's image at a time, usually the active speaker, without any video layouts or continuous presence (CP). Using video switching increases the port capacity of Scopia Elite MCU and Avaya Equinox® Media Server equal to the number of standard definition ports.

Important:

Use switched video only when all endpoints participating in the videoconference support the same resolution. If a network experiences high packet loss, switched video might not be displayed properly for all endpoints in the videoconference.

SXGA

SXGA defines a video resolution of 1280 x 1024 pixels.

Team Engagement deployments

Team Engagement deployments of Avaya Equinox® Solution are integrated with Avaya Aura®. The deployments use user-based licensing for the main components.

Telepresence

A telepresence system combines two or more endpoints together to create a wider image, simulating the experience of participants being present in the same room. Telepresence systems always designate one of the endpoints as the primary monitor/camera/codec unit, while the remainder are defined as auxiliary or secondary endpoints. This ensures that you can issue commands via a remote control to a single codec base which leads and controls the others to work together as a single telepresence endpoint.

Telepresence - Dual row telepresence room

Dual row telepresence rooms are large telepresence rooms with two rows of tables that can host up to 18 participants.

TLS

TLS enables network devices to communicate securely using certificates, to provide authentication of the devices and encryption of the communication between them.

Transcoding

Transcoding is the process of converting video into different sizes, resolutions or formats. This enables multiple video streams to be combined into one view, enabling continuous presence, as in a typical videoconferencing window.

Unbalanced Microphone An unbalanced microphone uses a cable that is not especially built to reduce interference when the cable is long. As a result, these unbalanced line devices must have shorter cables to avoid audio disruptions.

Unicast Streaming Unicast streaming sends a separate stream of a videoconference to each viewer. This is the default method of streaming.

Unified Portal Unified Portal is a graphic user interface (GUI) for Avaya Equinox® Solution users. Using this GUI, users can schedule and attend meetings. They can also access their recordings and broadcasts. It is the typical way that users interact with and access Avaya Equinox® Streaming and Recording. There is a user guide for Unified Portal available on https://support.avaya.com/. Avaya recommends distributing this guide to all users.

URI URI is an address format where the address consists of the endpoint's name or number, followed by the domain name of the server to which the endpoint is registered, such as <endpoint name>@<server_domain_name>. For example, 5000@198.51.100.51.

URI Dialing Accessing a device via its URI on page 493.

User profile A user profile is a set of capabilities or parameter values which can be assigned to a user. This includes available meeting types (services), access to functionality, and allowed bandwidth for calls.

UUID Universally unique identifier

VAPP Virtual Application Instance

VGA VGA defines a video resolution of 640 x 480 pixels.

Video Layout A video layout is the arrangement of participant images as they appear on the monitor in a videoconference. If the meeting includes a presentation, a layout can also refer to the arrangement of the presentation image together with the meeting participants.

Video Resolution See Resolution on page 489.

Video Switching See Switched video on page 492.

Videoconference A videoconference is a meeting of more than two participants with audio and video using endpoints. Professional videoconferencing systems can handle many participants in single meetings, and multiple simultaneous meetings, with a wide interoperability score to enable a wide variety of endpoints to join the same videoconference. Typically you can also share PC content, like presentations, to other participants.

Viewer Portal The Avaya Equinox® Streaming and Recording Viewer Portal is embedded in the Unified Portal. To access the Viewer Portal, you can

select **Recordings and Events** on the main page of the Unified Portal. From the Viewer Portal, you can watch recordings and navigate through the categories.

Virtual Delivery Node

The Avaya Equinox® Streaming and Recording Virtual Delivery Node (VDN) is a device to push content to an external Content Delivery Network (CDN). The method for publishing content to a CDN is tightly coupled to the Avaya Equinox® Streaming and Recording platform which allows a company's video assets to be managed from a central location.

If you want to use a VDN and a CDN, you must buy cloud storage and services from Highwinds, with the appropriate bandwidth and capacity for your needs. You apply the credentials you receive from Highwinds in the Avaya Equinox® Streaming and Recording Manager to securely access the CDN.

Virtual Room

A virtual room offers a virtual meeting place for instant or scheduled videoconferences. An administrator can assign a virtual room to each member of the organization. Users can send invitations to each other via a web link which brings you directly into their virtual room. Virtual meeting rooms are also dialed like phone extension numbers, where a user's virtual room number is often based on that person's phone extension number. You can personalize your virtual room with PIN numbers, custom welcome slides and so on. External participants can use a zero-download web application to access a registered user's virtual room and participate in a videoconference.

VISCA Cable

A crossed VISCA cable connects two PTZ cameras to enable you to use the same remote control on both.

Waiting Room

A waiting room is a holding place for participants waiting for the host or moderator to join the meeting. While waiting, participants see a static image with the name of the owner's virtual room, with an optional audio message periodically saying the meeting will start when the host arrives.

Webcast

A webcast is a streamed live broadcast of a videoconference over the internet. Enable webcasts by enabling the streaming feature. To invite users to the webcast, send an email or instant message containing the webcast link or a link to the Unified Portal and the meeting ID.

WUXGA

WUXGA defines a video resolution of 1920 x 1200 pixels.

XGA

XGA defines a Video resolution of 1024 x 768 pixels.

Zone

Gatekeepers like H.323 Gatekeeper split endpoints into zones, where a group of endpoints in a zone are registered to a gatekeeper. Often a zone is assigned a dial prefix, and usually corresponds to a physical location like an organization's department or branch.