Deploying Avaya Equinox® Solution

Release 9.1
Issue 7
July 2020

© 2010-2020, 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: About Avaya Equinox Conferencing 13
About this document 13
New in this release 13
Updates to this publication 16
Chapter 2: Before you begin 18
Component architecture 18
Licensing 27
Avaya Equinox® Management licenses 28
Media Server licenses 29
Before You Begin checklist 29
Downloading software from PLDS 32
Chapter 3: Avaya Converged Platform installation 34
Avaya Solutions Platform for the Avaya Equinox solution 34
Downloading documentation for the Avaya Solutions Platform installation 35
Chapter 4: Introduction to software installation 36
Prerequisites for software installation on customer-provided servers 36
Common prerequisites for software installation 39
Latest software updates and patch information 40
Software installation checklist for SMB deployment 40
Software installation procedures for medium to large deployments 45
Software installation procedure for large deployments and for Service Providers 50
Software installation procedure for adding servers 54
Changing the login password of the Platform Manager administrator 55
Changing Linux administrator user password for Scopia® Elite 6000 MCU and Equinox H.323 Edge 56
Changing the management administrator password 57
Linux user accounts for Avaya Equinox® Conferencing 59
Chapter 5: Equinox Management Deployment for Over the Top Solution 61
Deployment of Equinox Management for OTT solution — Overview 61
Technical Specifications of Equinox Management 62
Checklist for Deploying Equinox Management in an All-In-One Working Mode 65
Checklist for Deploying Equinox Management in a Distributed Working Mode 65
Downloading software from PLDS 66
Deploying the Equinox Management Server 67
Logging into Equinox Management 81
Configuring the All-In-One Equinox Management Server 88
Geographically Distributed Deployment of Equinox Management 91
Web Conference Signaling and Media in a Distributed Environment 93
Examples of Signaling and Media Paths for Clients 94

Equinox Management HTTPS Access for the UCCS Service..... 98
Disabling the Internal Load Balancer in Equinox Management..... 99
Deploying a distributed or cluster User Portal and Web Gateway..... 100
Deploying a Standalone Distributed H.323 Gatekeeper..... 104
Deploying Distributed H.323 Gatekeepers in Alternate Mode..... 106
Deploying a Distributed UCCS Server..... 109
Securing Connections With Equinox Management..... 111
Applying a Third-Party Certificate to the All-in-One Equinox Management Server..... 112
Applying a Third-Party Certificate to the Distributed Equinox Management Server..... 117
Installing the CA Certificate for Avaya Equinox® Meetings for Web..... 120
Renewing the CA Certificate for H.323 Gatekeepers in Alternate Mode..... 122
Configuring User Portal / Web Gateway Settings..... 125
Making the Avaya IX™ Workplace Client available to users..... 129
Uploading a windows installer with Equinox Management..... 129
Uploading a Mac Installer with Equinox Management..... 130
Switching Equinox Management from Port Based to User Based Licensing..... 132
Deploying and Configuring the Equinox Management Environment..... 136
Troubleshooting..... 136
Disaster recovery in a geographic redundancy deployment..... 138
Activating disaster recovery in a geographic redundancy deployment..... 139
Updating DNS and GSLB Records in Disaster Recovery for Geographically Distributed Equinox Management..... 141
Resuming normal operations after disaster recovery..... 142
Chapter 6: Equinox Management Deployment for Team Engagement solution..... 144
Deployment of Equinox Management for TE solution — Overview..... 144
Checklist for Deploying Equinox Management in Team Engagement..... 144
Deploying the Avaya Aura® Web Gateway..... 146
Configuring the Avaya Aura Web Gateway in Equinox Management..... 146
Integrating Avaya Aura® Users Into Equinox Management Via System Manager..... 147
Configuring the Equinox Conferencing Element in System Manager..... 147
Configuring SSO for Equinox Conferencing..... 151
Adding Avaya Aura® Users in Equinox Management..... 154
Deploying and Configuring the Equinox Management Environment..... 155
Configuring Session Manager for Interoperability with the SIP-based Equinox B2BUA Component..... 156
Adding a SIP Entity for the Equinox B2BUA Component..... 156
Adding a SIP Entity Link/SIP Trunk For the Equinox B2BUA Component..... 157
Adding Routing Policies For the Equinox B2BUA Component..... 157
Adding Dial Patterns for the Equinox B2BUA Component..... 158
Configuring Equinox Management for Interoperability with Avaya Aura®..... 159
Adding a SIP Trunk from the Equinox B2BUA Component to Session Manager..... 159
Changing the Default SIP Domain in Equinox Management..... 160
Configuring Ad Hoc Conferencing in a Team Engagement (TE) Environment..... 161

Configuring Avaya IX™ Workplace Client settings ... 162
Configuring advanced parameters for ad hoc conferencing ... 164
Configuring the SIP Endpoint Managed Transfer Setting in Avaya Aura® Communication Manager ... 165
Configuring Avaya Aura® Communication Manager settings ... 166
Configuring Dial Plan settings ... 167
Configuring Equinox Management settings ... 168
Configuring System Manager settings ... 169
Escalating to a multipoint conference for a multiparty call using Avaya IX™ Workplace Client ... 172
Chapter 7: Avaya Equinox Media Server deployment ... 174
Avaya Equinox® Media Server overview ... 174
Avaya Equinox® Media Server deployment checklist ... 175
Avaya Equinox® Media Server video conferencing mode administration checklist ... 175
Avaya Equinox® Media Server audio-only conferencing mode administration checklist ... 176
Avaya Equinox® Media Server web collaboration mode administration checklist ... 177
Avaya Equinox® Media Server WebRTC gateway administration checklist ... 177
Technical specifications of Avaya Equinox® Media Server ... 178
Capacity and scalability ... 179
Downloading software from PLDS ... 181
Deploying the Equinox Media Server OVA ... 182
Deploying the Avaya Equinox® Media Server virtual machine ... 182
Starting the Avaya Equinox® Media Server virtual machine ... 184
Configuring the virtual machine automatic startup settings on VMware ... 184
Equinox Media Server initial configuration ... 185
Adding Equinox Media Server in Equinox Management ... 185
Add Media Servers field descriptions ... 186
Adding Equinox Media Server in Equinox Management as a gateway ... 186
Add Gateway field descriptions ... 187
Configuring the Equinox Media Server network settings ... 188
Configuration field descriptions ... 188
Changing the Equinox Media Server working mode ... 190
Customizing audio messages ... 191
Secure connection with Equinox Management ... 191
Chapter 8: Deploying the Avaya Equinox Recording Gateway OVA ... 196
Avaya Equinox Recording Gateway deployment checklist ... 196
Deploying the Avaya Equinox® Recording Gateway virtual machine ... 196
Starting the Equinox Recording Gateway virtual machine ... 199
Configuring the virtual machine automatic startup settings on VMware ... 200
Equinox Recording Gateway initial configuration ... 201
Adding Equinox Recording Gateway in Equinox Management ... 201
Configuring the Equinox Recording Gateway network settings ... 201
Chapter 9: Avaya Scopia Elite 6000 MCU deployment ... 203

Scopia Elite MCU overview ... 203
Scopia® Elite 6000 MCU deployment checklist ... 204
Technical specifications of Scopia® Elite 6000 MCU ... 204
About the Capacity of the MCU ... 206
Ports to Open for the Scopia® Elite 6000 MCU ... 207
Configuring the IP addresses ... 210
Configuring Ports on All Models of the Scopia Elite MCU ... 215
Configuring the UDP port ranges for RTP/RTCP on Scopia® Elite 6000 MCU ... 215
Configuring the TCP Port Range for H.245 on Scopia® Elite 6000 MCU ... 216
Configuring the HTTP port on Scopia® Elite 6000 MCU ... 216
Configuring the UDP port for RAS on Scopia® Elite 6000 MCU ... 217
Configuring the UDP port for the gatekeeper on Scopia® Elite 6000 MCU ... 218
Configuring the TCP port for Q.931 on Scopia® Elite 6000 MCU ... 219
Configuring the TCP, UDP, and TLS port for SIP ... 219
Configuring the TCP port range for SIP BFCP on Scopia® Elite 6000 MCU ... 220
Verifying the Scopia® Elite 6000 MCU installation ... 221
Chapter 10: Data migration from Avaya Aura to Avaya Equinox ... 223
Introduction to Avaya Aura® Conferencing data migration ... 223
Exporting data from Avaya Aura® Conferencing ... 227
Importing Avaya Aura® Conferencing data to Avaya Equinox® Management ... 229
Chapter 11: Avaya Session Border Controller deployment for remote access in Over The Top solution ... 236
Configuration checklist for remote access in OTT — Non-tunneled and tunneled mode ... 236
Avaya SBCE deployment in the OTT solution ... 238
Small deployment ... 242
Medium deployment ... 244
Large deployment ... 245
Firewall traversal in OTT — normal security ... 248
Firewall traversal in OTT — enhanced security ... 250
Avaya SBCE technical specifications ... 252
Capacity and scalability specification ... 252
Certificates ... 256
Creating a Certificate Signing Request ... 256
Generating and installing certificates with Aura System Manager default CA ... 257
Installing a CA certificate on ASBCE ... 259
Installing a certificate and key on Avaya SBCE ... 259
Configuring the TLS Server Profile for Avaya SBCE external communication ... 260
Configuring TLS Server Profile for Avaya SBCE Media Tunneling ... 261
Configuring the TLS Client Profile on Avaya SBCE ... 262
Configuring Avaya SBCE network interfaces ... 263
Configuring Avaya SBCE signaling interface ... 264
Configuring Avaya SBCE media interface for OTT ... 265
Configuring Avaya SBCE load monitoring for OTT ... 267

Configuring Avaya SBCE server flows for OTT 267
TURN/STUN for WebRTC calls in OTT 269
Configuring Avaya SBCE STUN TURN server for OTT 271
OTT deployment — Single IP and single FQDN for HTTP traffic 272
Configuring remote client access to the Unified Portal 275
Configuring Equinox Conference Control for OTT 275
Configuring web collaboration for OTT 276
Configuring reverse proxy rules on ASBCE for OTT 276
Configuring Avaya SBCE on Equinox Management 279
Configuring Avaya SBCE support of unregistered Avaya SIP endpoints 281
Chapter 12: Avaya Session Border Controller deployment for remote access in Team Engagement solution 283
Configuration Checklist for Avaya SBCE in TE 283
Avaya SBCE technical specifications 285
Certificates 288
Configuring the TLS Server Profile for Avaya SBCE external communication 294
Configuring TLS Server Profile for Avaya SBCE Media Tunneling 295
Configuring the TLS Client Profile on Avaya SBCE 296
Configuring Avaya SBCE network interfaces 297
Configuring Avaya SBCE signaling interface 297
Configuring Avaya SBCE media interface for TE 298
Configuring Avaya SBCE load monitoring for TE 300
Configuring Avaya SBCE server flows for TE 301
Configuring the reverse proxy policy on Avaya SBCE for TE 303
Configuring the reverse proxy profile of Avaya Aura® Device Services on Avaya SBCE 304
Configuring reverse proxy rules on Avaya SBCE for TE 306
TURN/STUN for WebRTC calls in TE 309
Configuring Avaya SBCE support of unregistered Avaya SIP endpoints 313
Configuration Checklist for Avaya Aura® Device Services 315
Configuring the Front-end host, System Manager, and Certificate on Avaya Aura® Device Services 317
Configuration Checklist for Avaya Aura® Web Gateway 318
Configuring the Front-end host of Avaya Aura® Web Gateway, System Manager, and Certificate 327
Configuration Checklist for Avaya Aura® Media Server 329
Configuration Checklist for Avaya Equinox® Management in TE 332
Configuring the portal URL for Meet-Me clients 333
Configuring Avaya Equinox® Management 334
Configuring User Portal access for TE 335
Configuring Avaya Aura Device Services in Avaya Equinox Management 336
Configuring Avaya Aura® Web Gateway on Avaya Equinox® Management 336
Configuring Avaya SBCE on Equinox Management 337
Configuring Avaya Equinox® Media Server in Avaya Equinox® Management 338

Chapter 13: Avaya Equinox H.323 Edge deployment 340
Avaya Equinox® H.323 Edge Client overview 340
Equinox H.323 Edge virtual server deployment checklist 341
Avaya Equinox® H.323 Edge initial configuration checklist 342
Technical specifications of Equinox H.323 Edge 343
Ports configuration 343
Equinox H.323 Edge virtual server deployment 347
Downloading software from PLDS 347
Deploying the Equinox H.323 Edge virtual server 348
Starting the Equinox H.323 Edge virtual server 349
Configuring the virtual machine automatic startup settings 349
Equinox H.323 Edge initial configuration 350
Adding networks to Avaya Equinox® H.323 Edge 350
Adding Equinox H.323 Edge in Equinox Management 352
Configuring a second IP interface in Avaya Equinox® H.323 Edge for external traffic 352
Configuring static routes for Avaya Equinox® H.323 Edge 353
Configuring Ports on the Equinox H.323 Edge server 354
Integrating the Equinox H.323 Edge server with Other Equinox Solution Components 356
Calls between internal and external endpoints 358
Secure connection with Equinox Management 365
Configuring remote access 368
Access field descriptions 369
Configuring QoS for audio and video 369
Creating an Equinox H.323 Edge server cluster 371
Chapter 14: Avaya Equinox Streaming and Recording deployment 374
Introducing Avaya Equinox Streaming and Recording 374
Avaya Equinox® Streaming and Recording Server 374
Installing Avaya Equinox Streaming and Recording 385
Installation checklist 385
Physically connecting the new server 387
Initially configuring the new server 390
Configuring the new server 391
Configuring external addresses for public interfaces 396
Registering each of the components 397
Configuring delivery nodes 400
Configuring virtual delivery nodes 404
Configuring conference points 407
Specifying polling intervals and the network address 409
Configuring the recycle bin for recording file retention 410
Adding and Modifying Equinox Streaming and Recording Servers in Equinox Management 411
Configuring the Avaya Equinox® Recording Gateway 413
Chapter 15: Avaya Equinox Solution upgrades 414
Avaya Equinox® Solution upgrades 414

Chapter 16: Licensing all components of the solution 415
Introduction to licensing 415
Downloading software from PLDS 415
Checklist for activating licenses 416
Table of host ID sources 416
Activating license entitlements in Avaya PLDS 418
Updating the Equinox Management license 420
Managing Licenses Via the Web-based License Manager (WebLM) 422
Installing a user license on the local WebLM server 422
Installing the User License On the External WebLM Server 425
Avaya Equinox Media Server license configuration 430
Checklist for configuring Avaya Equinox® Media Server licenses 430
Activating license entitlements in Avaya PLDS 430
Applying the Avaya Equinox® Media Server licenses 432
Avaya Equinox H.323 Edge license configuration 433
Checklist for configuring Avaya Equinox® H.323 Edge licenses 433
Getting the system ID to activate Equinox H.323 Edge 433
Activating license entitlements in Avaya PLDS 433
Downloading software from PLDS 435
Adding and updating licenses 436
Checklist for configuring Avaya Equinox® Streaming and Recording Server licenses 436
Setting the IP address and hostname of the recording component (Conference Point) 437
Setting the IP address and hostname of the delivery component (Delivery Node) 442
Restarting services 442
Applying the license to the management component 443
Applying the license to the recording component (Conference Point) 443
Applying the license to the delivery component (Delivery Node or Virtual Delivery Node) 444
Viewing license information 444
Chapter 17: Resources 448
Documentation 448
Finding documents on the Avaya Support website 452
Accessing the port matrix document 452
Avaya Documentation Center navigation 453
Training 454
Support 454
Using the Avaya InSite Knowledge Base 455
Appendix A: Avaya Equinox® Team Engagement hardened deployment 456
Overview of the hardened solution 456
Configuration checklist for hardening the backend Avaya Aura® Media Server 460
Configuration checklist for hardening the frontend Avaya Aura® Media Server 462
Configuring Avaya Aura® Media Server for encrypted transfer of audit logs and syslogs to a log aggregation server 465
Configuring encrypted NTP time source messages in Avaya Aura® Media Server 466

Configuration checklist for Avaya Equinox® Management hardening..... 467
Configuration checklist for hardening Avaya Aura® Web Gateway 467
Glossary..... 469

Chapter 1: About Avaya Equinox Conferencing

About this document

This document provides procedures required to perform the initial installation and deployment of Avaya IX™ Workplace Client Release 9.x in an Aura Team Engagement and non-Aura Over The Top environment. This document also contains deployment overviews, technical requirements, and checklists for support throughout installation and deployment.

The audience includes and is not limited to implementation engineers, field technicians, business partners, and customers.

New in this release

For detailed information, see the product guides and Release Notes that you can download from http://support.avaya.com.

Release 9.1.10

Release 9.1.10 further reinforces data privacy handling at the solution level for General Data Protection Regulation (GDPR) compliancy. Avaya Equinox® Management centrally handles data privacy configuration for most components.

Avaya Equinox® Management:

- PIN security features

  The administrator can enforce strong PIN requirements and auto notifications to change the PIN.

- Enhancements on meetings that are scheduled on Avaya Meeting Scheduler Outlook Add-in for Windows

  Waiting rooms for one-time pin meetings are supported because Avaya Meeting Scheduler Outlook Add-in allows to reserve scheduled meetings in Avaya Equinox® Management.

  Each scheduled meeting adds random digits onto the virtual room number, which improves meeting security even if the virtual room is not configured for one-time pin. The user can schedule back-to-back or overlapping meetings in the same virtual room without any conflicts.

- Ability to add multiple virtual rooms per user in a Team Engagement (TE) deployment.

  The administrator can manually add a second virtual room to an existing user from the administrator portal of Avaya Equinox® Management. For example, the administrator can enable the user's first virtual room for video, and the second virtual room for audio only to save video resources.

- Ability to change the participant's name in a waiting room

  While the participant is in the waiting room, the operator can change the participant's name in the In-meeting Control interface of Avaya Equinox® Management. When the participant is online, the system displays the new name on the video screen for that participant.

- New report types for virtual rooms that allow to better track system usage.
- Users can now own multiple VMRs in an Equinox Conferencing Team Engagement deployment type. In addition, the obligation for a waiting room is now removed in the Equinox Conferencing Team Engagement deployment type.
- Meeting Operators can now change the name of participants when they are in the waiting room, and before a meeting starts. This allows operators to map and replace PSTN caller numbers with first and last names, so as to have these appear on the participant roster instead of displaying a PSTN number.

Unified Portal:

- New customizing features for branding.
- Volume indicator allows to check your voice level on the microphone panel of the Unified Portal.
- Users can save a list of participants in their Downloads folder.
- Users can view Avaya Meeting Scheduler Outlook Add-in in the Unified Portal interface.

Standalone Avaya Aura® Web Gateway:

From release 3.8.1 and above, the application integrates network separation of management services.

IP Office in Avaya Equinox Conferencing

Avaya Equinox Conferencing 9.1.10 no longer supports interoperability with IP Office. Cloud conferencing with Avaya Spaces is a better fit and the recommended solution for IP Office customers.

Product branding

Avaya Equinox Client was changed to Avaya IX™ Workplace Client.

Enhancements and bug fixes:

See the product Release Notes.

Documentation updates

The current documentation release includes features of release 9.1.9 SP1 (9.1.9.1).

For Avaya Aura® products, see the Avaya Aura® documentation and release notes.

Avaya Equinox® Management:

- Option to enable or disable the OS storage encryption during OVA deployment. The default value is **Enabled** for encryption.
- Meeting and moderator PIN security enhancements
- Personal data encryption
- Retention time of Call Detail Record (CDR) data
- Storage encryption

  Storage is encrypted together with Avaya Equinox® Management in the following modules:

  - All-In-One Avaya Equinox® Management, including All-In-One Avaya Aura® Web Gateway in Over-The-Top (OTT) deployment
  - Distributed Avaya Aura® Web Gateway in OTT deployment because the gateway has user data in its database
  - Distributed Equinox H.323 Gatekeeper and distributed Equinox Conference Control, both in TE and OTT deployments
- Server log retention time

  The administrator has the option to configure separate log retention days for the local server and for the distributed devices in the deployment.

  The local server comprises the All-In-One Avaya Equinox® Management, including All-In-One Avaya Aura® Web Gateway in OTT.

  The distributed devices include:

  - Distributed H.323 Gatekeeper
  - Distributed Equinox Conference Control
  - Avaya Aura® Web Gateway in OTT
  - Avaya Equinox® H.323 Edge
  - Avaya Equinox® Media Server

    For details, see the section about the server.
- Cleaning of management expiration logs

Avaya Equinox® Media Server:

The administrator can configure log retention time for the following uses of Avaya Equinox® Media Server on Avaya Equinox® Management:

- Avaya Aura® Media Server High Capacity Audio with Web Collaboration
- Web Collaboration Only Avaya Equinox® Media Server
- Avaya Aura® Media Server Media Gateway
- Avaya Equinox® Media Server Full Video and Web Collaboration

When Avaya Equinox® Conferencing is deployed in hardened security mode (FedRAMP), the administrator can configure log retention on the standalone Avaya Aura® Media Server with or without Web Collaboration.

Avaya Equinox® Streaming and Recording:

- Disk encryption for the Avaya Equinox® Streaming and Recording Windows Server itself and for the SAN partition, if a SAN is used for external storage.
- Personal data retention policies. This Service Pack adds the ability to define the storage period for any files containing personal data. This includes certain log files, as well as temporary recording files.
- Increased password security.

Updates to this publication

The following sections have been updated in this publication.

General

- Avaya Solutions Platform for the Avaya Equinox solution on page 34
- Prerequisites for software installation on customer provided servers on page 36
- Common prerequisites for software installation on page 39
- Avaya SBCE capacity and scalability specification on page 252
- A chapter that includes licensing information of different components
- Re-branding of Avaya Equinox Client to Avaya IX™ Workplace Client

Avaya Equinox® Management

- New topic in the publication, Equinox Conferencing Management licenses on page 28.
- New topic in the publication, Activating a license in PLDS using UUID on page 418.
- Installing the CA Certificate for Avaya Equinox® Meetings for Web on page 120
- Uploading a Windows Installer with Equinox Management on page 129
- Deploying a standalone distributed H.323 Gatekeeper on page 104r
- Deploying the distributed H.323 Gatekeeper in Alternate Mode on page 106
- Deploying a distributed Equinox Conference Control (UCCS) Server on page 109
- Renewing the CA Certificate for H.323 Gatekeepers in Alternate Mode on page 122

Avaya Equinox Recording Gateway

A chapter on deploying the Avaya Equinox Recording Gateway OVA

Avaya Equinox® Media Server

- Technical specifications of Avaya Equinox Media Server on page 178
- Deploying the Avaya Equinox® Media Server OVA and sub topics.

Avaya SBCE deployment for remote access in Over the Top solution

- Configuration Checklist for remote access on page 236 and sub topics

Avaya SBCE for deployment for remote access in Team Engagement solution

- Certificates configuration checklist and sub topics
- Configuration Checklist for remote access on page 283 and sub topics
- Configuration Checklist for Avaya Aura Device Services on page 315 and sub topic
- Configuration Checklist for Avaya Aura Web Gateway on page 318 and sub topic
- Configuration Checklist for Avaya Aura Media Server on page 329
- Configuration Checklist for Avaya Equinox® Management in TE on page 332 and sub topics

Equinox Streaming and Recording

- Avaya Equinox Streaming and Recording Server on page 374
- Installation checklist on page 385
- Registering each of the components on page 397
- Specifying polling intervals and the network address on page 409
- Configuring the recycle bin for recording file retention on page 410

Avaya Equinox® H.323 Edge

- Avaya Equinox® H.323 Edge virtual server deployment and sub topics
- Avaya Equinox® H.323 Edge license configuring and sub topics
- Configuring a second IP interface in Avaya Equinox® H.323 Edge for external traffic on page 352
- Configuring static routes for Avaya Equinox H.323 Edge on page 353
- Integrating Avaya Equinox H.323 Edhe with H.323 Gatekeeper on page 356
- Calls between internal and external endpoints and sub topics

Scopia® Elite 6000 MCU

Technical specifications of Scopia Elite MCU on page 204

Chapter 2: Before you begin

Component architecture

The architecture of the Avaya Equinox® Solution is built on new and improved existing software components using top technology operating system and applications, including video and audio codecs, web applications and edge elements. The 9.x release introduces the move from Scopia® Management suite to Equinox Management and the deployment of software-based, virtualized Equinox Media Server in addition to Scopia® Elite 6000 MCU. The solution components are distributed as Open Virtualization Appliances (OVAs), application software, or appliances. The OVAs run on Linux RH and allow components to co-reside on a single server for small deployments, or to be distributed on several servers for medium/large deployments.

The Equinox Solution, or Avaya Equinox® Conferencing, also introduces two deployment concepts:

- Team Engagement, that integrates Avaya Aura® in the solution
- Over The Top, the standalone, conferencing-only solution on the customer existing infrastructure.

The figure below illustrates the deployment of key components for Avaya Equinox® for Over The Top.

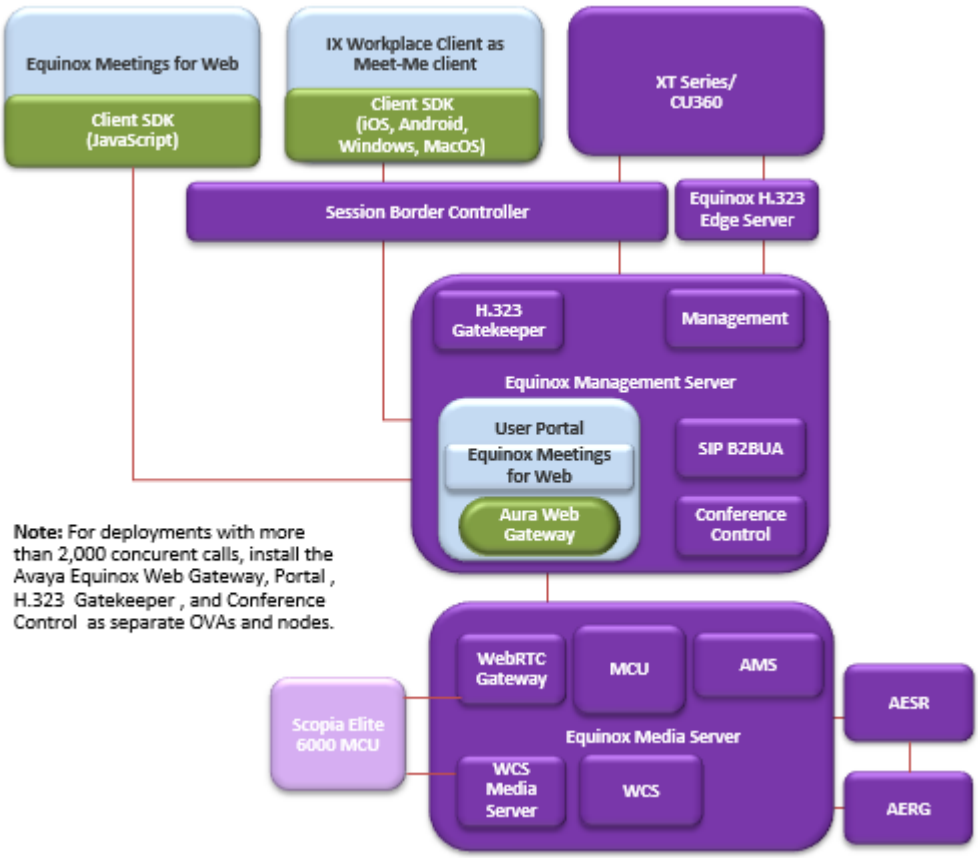


Figure 1: OTT Component architecture

The figure below illustrates the deployment of key components for Avaya Equinox® for Team Engagement.

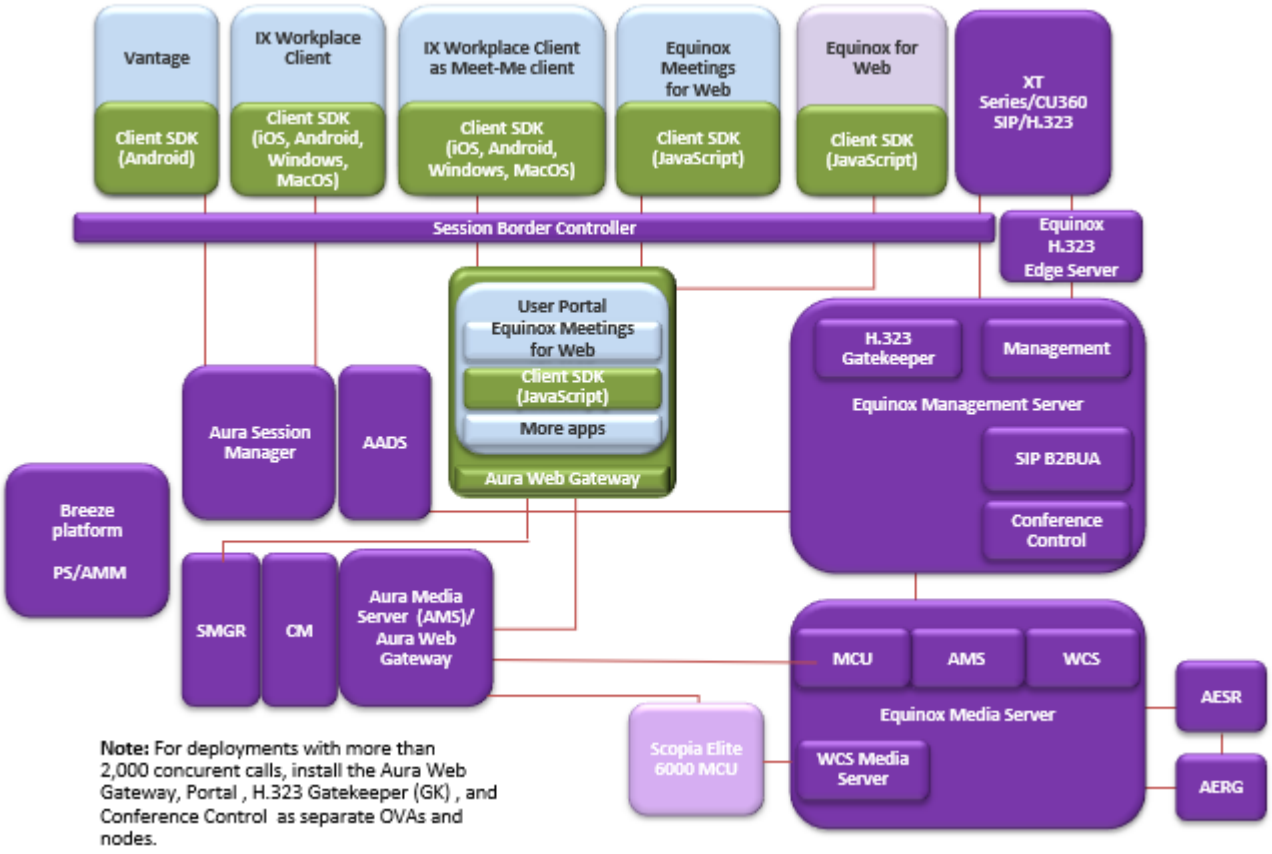


Figure 2: TE Component architecture

Table 1: Network traffic from clients

Protocol	Private net destination	Service
SIP-TLS	• Session Border Controller and Avaya Aura® Session Manager • Session Border Controller and Avaya Aura® Web Gateway • Session Border Controller and Equinox Management	SIP signaling
SRTP	Point-to-Point, media servers, gateways	Audio or video media
HTTPS	Avaya Aura® Session Manager	Personal Profile Management (PPM).

Table continues…

Protocol	Private net destination	Service
HTTPS	• Avaya Aura® Device Services (AADS) • Equinox Conferencing (UCCS) to Equinox Management • Multiple services running on Avaya Aura® Web Gateway use HTTPS as well for the Avaya Equinox® Meetings for Web client.	Auto-config, auto-update, directory service, contact service
HTTPS	Avaya Aura® Media Server(AMM)	Instant messaging
HTTPS	WCS	Web Collaboration
DNS	Internal/external DNS	Auto-config service discovery

The OTT solution has these characteristics:

- All deployments are without Avaya Aura®.
- Equinox Management manages all conferencing components.
- Unified Portal is for conferencing only.
- Equinox Management can synchronize with the organization's LDAP.
- With/without third party PBX and/or SIP proxy.

The TE solution has these characteristics:

- Calls go through Avaya Aura® Session Manager (SM)/Avaya Aura® Communication Manager (CM).
- Avaya Aura® System Manager (SMGR) manages Avaya Aura® and collect logs and alarms (except for the Equinox Management ones).
- Equinox Management manages all conferencing components.
- Equinox Management connects with Avaya Aura® Device Services (AADS). AADS authenticates Equinox Management users. Equinox Management can get the users configured via SMGR, either manually or via LDAP sync.
- The Unified Portal runs on Avaya Aura® Web Gateway.

Infrastructure components

Equinox Management Server:

This infrastructure component comprises the following modules:

Server/service	Description
Management	Previously called iVIEW. The common management framework that provides centralized management functions for provisioning and administration. Management can synchronize with the organization's LDAP with/without third party PBX and/or SIP proxy.
H.323 Gatekeeper	Previously called Avaya Scopia® ECS Gatekeeper when deployed as a standalone in the Scopia Solution. The gatekeeper provides address resolution functionality in H.323 networks. Only a distributed gatekeeper can support 15,000 concurrent calls.
SIP B2BUA	SIP Back-to-Back User Agent.
Unified Portal	Single portal from which users can access conferencing functionalities such as meetings, user settings, and recordings. In the OTT model, Avaya Aura® User Portal functionalities and Avaya Web Gateway functionalities are available as an integrated part of Equinox Management. When the OTT model is used in an Aura environment, the administrator can decide if the integrated Avaya Aura® User Portal and Avaya Web Gateway functionality, or separate instances of third components, are provided in the Avaya Aura® architecture. The User Portal is called Unified Portal in an OTT deployment. Only a distributed portal can support 15,000 concurrent calls.
Web Gateway	Web Gateway for WebRTC (HTTPS to SIP signaling). Relevant mainly for OTT and VAAS deployments. From SP 9.1.0.3, alll WebRTC calls to Avaya Equinox® Media Server pass through the gateway first. The gateway supports re-transmission, which results in improved video quality. In a TE deployment, it is provided as a separate OVA (Avaya Aura® Web Gateway) and part of Avaya Aura®. This component requires a security mode and is available only in encrypted versions. Avaya SBCE is a required component for Avaya Equinox® Meetings for Web (WebRTC) clients.

Table continues…

Server/service	Description
Equinox Conference Control	Also called UCCS. This service uses the Unified Conference Control Protocol (UCCP), a web based protocol enabling Avaya IX™ Workplace Clients and Avaya Equinox® Meetings for Web clients to have conference control such as roster, moderator commands, and user commands. The client may reside in any location (private side, public side, a different company and so on). HTTP reverse proxy handles firewall traversal. Equinox Conference Control can be embedded in Equinox Management, and is used as a standalone to support 15,000 concurrent calls. When there are multiple distributed Equinox Conference Controls, Equinox Management chooses Equinox Conference Control nearest to Equinox Media Server.

Equinox Media Server:

This infrastructure component is Avaya's virtual application for multiparty audio, video, and data conferencing. It has two working modes:

- Full Audio, Video, and Web Collaboration
- High Capacity Audio, Multi-Stream Video and Web Collaboration

You can switch working modes from the Equinox Management interface. The Equinox Media Server cannot work in a mixed mode. To deploy a solution with both working modes, you need two Equinox Media Servers: one for the Full Audio, Video, Web Collaboration mode that also has WebRTC, and another one for the High Capacity Audio + Web Collaboration mode.

You can also deploy the server as a gateway / Add-on for an existing Elite 6000 MCU series. In this mode it performs as the WebRTC Gateway to add WebRTC functionality to the Elite 6000 MCU series, or as the Web Collaboration Server (WCS) Media Server to add advanced content sharing functionalities of Web Collaboration services.

The server includes the following modules:

Server/Service	Description
MCU	Multiple Control Unit with has HD video transcoding and switching capacities.
AAMS	Avaya Aura® Media Server. High scale audio engine
WCS	Web Collaboration Server engine. The integrated server supports all the standalone Web Collaboration Server functionalities (Version 8.3 and up), including Web Conferencing Gateway (WCGW) capabilities for H.264, JPEG transcoding and JPEG/PNG encoding, and slider. The server provides advanced content sharing functionality for Elite 6000 MCU which are not available with standard H.239/BFCP based content sharing.

Platform Manager (PMGR):

Platform Manager (PMGR) is part of the web collaboration solution for Avaya Equinox® Conferencing. PMGR is the entity that manages the installation, upgrading, system monitoring and configuration of the unified platform. Each software package on the physical/virtual servers includes a PMGR application (single instance per server). PMGR is automatically activated on server power up.

PMGR performs the following tasks:

- Detecting and monitoring NICs, RAM, and CPUs for both physical and virtual appliances.
- Enabling components to open administrator connection to Equinox Management.
- Monitoring the installation progress of each component and forwards this information to Equinox Management as requested.
- Monitoring configuration changes.

Avaya Aura®:

These infrastructure components include the following modules:

Module	Description
SM	Avaya Aura® Session Manager. The SIP routing and integration tool.
AADS	Avaya Aura® Device Services, a separate OVA with its own Cassandra database from release 7.1.5, to be paired with Avaya Aura® Session Manager. AADSprovides a single place in the Aura architecture where devices (clients and endpoints) can store and retrieve data that users want to see on any device, supporting a common user experience. In addition, it is a common place for configuration and deployment data.
SMGR	Avaya Aura® System Manager. The common management framework that provides centralized management functions for provisioning and administration.
CM	Avaya Aura® Communication Manager. Open, extensible IP telephony platform that can be deployed as an IP PBX, a Session Initiation Protocol (SIP)-only environment, or a hybrid platform that supports both SIP and non-SIP environments.

Table continues…

Module	Description
PS	Avaya Aura® Presence Services, an Avaya Breeze® platform snap-in. PS collects and disseminates rich presence from Avaya and third party sources across a diverse set of business environments, enabling users throughout the network to reach the people they need, leveraging the multiple channels of communications available to them.
AMM	Avaya Multimedia Messaging, an Avaya Breeze® platform snap-in. AMM delivers powerful IM and presence capabilities for Avaya IX™ Workplace Clientand Avaya IX™ CU360 users. Individuals and groups can interact and productively handle conversations and engage across locations and time.
Avaya Aura® Media Server/Avaya Aura® Web Gateway	High scale audio engine enabling users inside or outside the Enterprise to make a secure call from their web browser to any endpoint to which Avaya Aura® can deliver calls. Needed when Elite 6000 MCU is used.

Table 2: Aura deployment details

Current element	Desk worker	Remote worker/mobile	Notes
Avaya Aura® Device Services	Yes	Yes	
Avaya Aura® Communication Manager	Yes	Yes	
Avaya Aura® Session Manager	Yes	Yes	Release 7.0.1.2 and above must be in place for AADS support.
Avaya Aura® System Manager	Yes	Yes	Release 7.0.1.2 and above must be in place for AADS support.
Avaya Aura® Presence Services on Avaya Breeze® platform	Yes	Yes	From Release 8.0.1 and above.
Avaya Aura® Application Enablement Services	Optional	Optional	No Equinox dependencies unless you have H.323 Presence collector

Table continues…

Current element	Desk worker	Remote worker/mobile	Notes
Avaya Aura® Conferencing	Optional	Optional	Can be used with Avaya IX™ Workplace Client. Best practice to update to Equinox Solution.
Avaya Multimedia Messaging on Avaya Breeze® platform	Yes	Yes	Avaya IX™ Workplace Client can be deployed against Release 2.1 but best practice is to deploy Release 3.0 and above.
Avaya IX™ Workplace Client for Android	Any combination Avaya IX™ Workplace Client	Any combination of Avaya IX™ Workplace Client	
Avaya IX™ Workplace Client for Mac	Any combination of Avaya IX™ Workplace Client	Any combination of the Avaya IX™ Workplace Client	
Avaya IX™ Workplace Client for iOS	Any combination of Avaya IX™ Workplace Client	Any combination of Avaya IX™ Workplace Client	
Avaya IX™ Workplace Client for Windows	Any combination of Avaya IX™ Workplace Client	Any combination of Avaya IX™ Workplace Client	.net framework Release 4.x and above needs to be in place. Note any security policies that restrict any application.
Avaya Session Border Controller for Enterprise	Optional	Yes	
Avaya Room System XT Series/Avaya IX™ CU360	Optional	Optional	
PC Operating System versions	Yes	Yes	
MAC	Yes	Yes	
iOS	Yes	Yes	
Android	Yes	Yes	
Browser supported on desktops	Yes	Yes	Preferred browser for a WebRTC deployment
Office version	Yes	Yes	

Scopia® Elite 6000 MCU:

Scopia® Elite 6000 MCU is the platform for high definition multi-party conferencing. The MCU harnesses revolutionary processing power for demanding conferencing applications. Dual 1080p/60fps channels for video and content, simultaneous H.264 High Profile for bandwidth efficiency and H.264 Scalable Video Coding (SVC), along with multi-stream immersive telepresence connectivity deliver uncompromised multi-party collaboration. The server uses Equinox Media Server as a WebRTC Gateway or as a WCS Media Server.

Equinox Streaming and Recording

The server provides audio, web, and HD video recording as well as high scale streaming capability. It requires an additional component, called Avaya Equinox® Recording Gateway (AERG). It facilitates recording of audio-only and web collaboration conferences or pure audio-only conferences hosted onEquinox Media Server and Scopia® Elite 6000 MCUs into AESR. For more information, see *Release Notes for Avaya Equinox® Recording Gateway* on http://support.avaya.com.

Edge components

Product	Description
Equinox H.323 Edge	Allows external H.323 Video HD Room system to connect from outside the enterprise network through firewalls. Deploy Equinox H.323 Edge only in legacy Avaya Scopia solution deployments. The H.323 protocol is used only in legacy Avaya Scopia deployments.
Avaya SBCE	Allows external users and WebRTC users to connect to conferences in the enterprise local network. It provides: • Session Border Control (SBC). It allows connection remote audio and video SIP endpoints that are registered/not registered with the solution. These can be XT Series and Avaya IX™ CU360 endoints or third-party video endpoints (Cisco and Polycom). • HTTP reverse proxy • TURN/STUN server for ICE, for connecting WebRTC end users with audio and video through firewalls.

Licensing

The licensing functionality operates in a different way, depending on your type of Avaya Equinox® Solution.

The solution is called Avaya Equinox® for Over The Top (OTT) when it ties to the customer existing infrastructure and provides services over the top of this infrastructure without requiring it to be upgraded or replaced.

The solution that tightly integrates with Avaya Aura® components is called Avaya Equinox® for Team Engagement (TE) and is deployed in medium and large enterprises.

The licenses can be grouped into these categories:

- Enterprise Edition with a port-based and user-based license model. Port-based licenses are required for the OTT solution, and user licenses (Avaya Aura® Power Suite) for the TE solution.
- Service Provider Edition, with a port-based or virtual room (cloud) based license model.

Note:

From Release 9.1 the Power Suite Equinox Management license enables switching the server from OTT to TE. See Switching Equinox Management from Port Based to User Based Licensing on page 132.

For information on how to apply license keys, see Introduction to licensing on page 415.

Avaya Equinox® Management maintains the deployment's licenses for these products and allows the administrator to easily view and update the product's license:

- Equinox Management
- Web Gateway (Equinox Management)
- Avaya Equinox Recording Gateway (AERG)
- Equinox Media Server (MCU and AMS)
- Web Collaboration Server
- Scopia Elite MCU
- Equinox H.323 Edge
- XT Series
- Avaya IX™ CU360

New upgrades and installations include a number of default licenses. If licensing limits are exceeded, Equinox Management displays full explanatory error messages to users. Licenses must be periodically renewed. If they are not renewed, they expire.

Related links

Avaya Equinox® Management licenses on page 28
Media Server licenses on page 29

Avaya Equinox® Management licenses

There must be at least one Equinox Management license. If high availability is chosen, there must be two Equinox Management licenses for the primary location.

If geographic redundancy is chosen, then the second location (non-primary location) will have one of the appropriate Equinox Management licenses. For geographic redundancy, the primary must have high availability, so there will be a total of three identical Equinox Management licenses, one for the primary location, one for high availability and one for the for the geographic redundancy management license at the second location.

Table 3: Management licenses

Deployment	License type
OTT	Enterprise
	Multi-tenant
TE	Power Suite Edition
	Power Suite JITC (indicated at System Level for TE designs only)

Related links

Licensing on page 27

Media Server licenses

An Equinox Solution must have at least one Media Server VAPP and one Equinox Media Server license.

By default, OTT designs include one WebRTC Gateway with the Media Server. The WebRTC Gateway includes one additional Media Server VAPP license to support its functionality.

By default, OTT designs include ASBCE (Avaya Session Border Controller for Enterprise) license entitlements.

TE solutions do not include ASBCE licenses because Avaya Aura® is used as the UC Platform.

Table 4: Media Server licenses

Deployment	License type
OTT	MS VAPP
	MS License
	WebRTC Gateway
TE	MS VAPP
	MS License
TE JITC	MS VAPP

Related links

Licensing on page 27

Before You Begin checklist

The following checklist provides the high level steps and considerations prior to beginning the installation of your Avaya Equinox® Solution. The checklist applies to Avaya Equinox® for Over

The Top (standalone) and Avaya Equinox® for Team Engagement solutions. The TE solution comprises the Avaya Aura® environment.

Note:

If you are migrating from Avaya Aura® Conferencing Release 8.x, see Introduction to Avaya Aura Conferencing data migration on page 223 and related topics.

If you are upgrading from Avaya Scopia® Solution 8.3.9, see the solution Release Notes that are available from http://support.avaya.com.

No.	Task	Description	Notes	✓
1	Determine your deployment layout type based on the capacity and scaling requirements for your location.		For information about deployment types, see the various Solution Guides listed in the Documentation on page 448 section of this guide.	
2	Install the Avaya Solutions Platform. Or prepare your server for the installation of Avaya IX™ Workplace Client components.		See Downloading documentation for the Avaya Solutions Platform installation on page 35.	
3	Obtain the latest Avaya Equinox® Solution software installation and patches.	Download from Avaya PLDS.	To find your downloads in PLDS, select **View Downloads**. In the **Download** field, search for **Equinox 9.x** files (for example, 9.1).	

Table continues…

No.	Task	Description	Notes	✓
4	Determine the required number of IP addresses for your deployment configuration, hostnames, and FQDNs. Register the required FQDNs with the appropriate DNS servers. FQDNs are required for single sign-on (SSO) to administer components. To use SSO, the components must belong to the same root domain.		For all deployments, you must use FQDNs. FQDNs are essential when using TLS.	
5	If you are deploying your system with TLS enabled, ensure Certificate Authorities are imported and certificates are assigned.			
6	Obtain the supported Web browsers.		For the supported web browsers, check the latest *Avaya Equinox® Solution Release Notes* which are available from http://support.avaya.com	

Table continues…

No.	Task	Description	Notes	✓
7	Obtain the licensing information from Avaya.	See application installations.	• Avaya Equinox® for Over The Top uses port-based licenses. • Avaya Equinox® Cloud Services (which is an OTT solution) uses Virtual Room licenses. • Avaya Equinox® for Team Engagement uses user-based licenses. • From Release 9.1 the Power Suite Equinox Management license enables switching the server from OTT to TE. See Switching Equinox Management from Port Based to User Based Licensing on page 132.	
8	If you are using a DMZ deployment, consider the following: • Ensure you have configured the required, servers, routers, and firewalls • Ensure the required port modifications are made.	Contact your network specialist or administrator if you require a DMZ configuration.	For more information, see *Port Security for Avaya Equinox® Solution Reference Guide* on http://support.avaya.com	

Downloading software from PLDS

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.

4. Select **View Downloads**.
5. Click the search icon () for Company Name.
6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type `Avaya` or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
   - In **Download Pub ID**, type the download pub ID.
   - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. Scroll down to the entry for the download file, and click the **Download** link.
10. Select a location where you want to save the file, and click **Save**.
11. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.
12. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Chapter 3: Avaya Converged Platform installation

Avaya Solutions Platform for the Avaya Equinox solution

The Dell PowerEdge R640 is the underlying server hardware for the Avaya provided server (Avaya Solutions Platform). It replaces the Common Server used in previous releases.

The Avaya Solutions Platform server offers include:

- Avaya Solutions Platform 120 Appliance, which supports virtualization using the Appliance Virtualization Platform. Support for Aura starts from releases 8.0.1 and 7.1.3.3.
- Avaya Solutions Platform 130 Appliance, which supports virtualization using VMware vSphere ESXi Standard License.

Feature	Avaya Solutions Platform 120 Appliance Basic	Avaya Solutions Platform 130 Appliance Standard
Hypervisor	Appliance Virtualization Platform 8.0.1 or greater	ESXi 6.5 U2
vCenter Managed	No	Yes
HA, vMotion	No	Yes **Note:** For the availability of HA and vMotion, check the Product Definition document.
Deployed OVAs	No	No
Alarming	SAL	SAL
Expandability	Limited	Limited
High Capacity Storage	No	No
Migration Path	Service Affecting	In-Service

Note:

On the Avaya Solutions Platform 130 Appliance, VMware Vsphere 6 Standard is loaded and the license key is installed. The license key label is located on the lid of the Avaya Solutions Platform 130 Appliance server.

For more information on the Avaya Solutions Platform, see https://support.avaya.com/search-landing/?query=avaya+solutions+platform

Downloading documentation for the Avaya Solutions Platform installation

About this task

Use this procedure to find and download documents on the Dell servers that you are using in your deployment. The documentation includes information on the servers and procedures for installing them in racks.

Procedure

1. Open a browser and go to https://support.avaya.com/downloads.
2. Enter Avaya Solutions Platform in the **Enter Your Product Here** field, and select the server version from the **Choose Release** dropdown.
3. Download the documents that you need:
   - Installing the Avaya Solutions Platform 120 Series
   - Installing the Avaya Solutions Platform 130 Series

Chapter 4: Introduction to software installation

Prerequisites for software installation on customer-provided servers

If you install the Avaya apps on your own servers instead of Avaya provided servers, make sure to follow the procedures described in the deployment guide for each type of server.

OVA deployment	OVA support
OVA technical specifications	See the deployment guide. In addition, download the latest product guide from the Avaya Support site at http://support.avaya.com, or contact Avaya Support.
OVA deployment	See the deployment guide.

ESXi host resource	Requirement
Performance optimization	• You must install the virtual machine on an Intel® Xeon® processor based server. Avaya does not support the installation of the virtual machine on an AMD processor based server. • Hyper-threading BIOS option is recommended, but can be disabled for some specific profiles. • For Avaya Equinox Media server, the CPU must support a feature called Intel® Advanced Vector Extensions 2 (Intel® AVX2). This support is available with ESXi 6.0, 6.5, and 6.7. • Optimize the server for performance by meeting the following requirements: - If you are using a Dell or HP server, check that it was ordered as Performance Optimized. - Optimize BIOS configuration per manufacturer recommendations. - Populate DIMMs as specified by the vendor: • All the memory channels must be populated for each CPU socket. • Make sure you have exactly one DIMM per channel. In case you have 2 or 3 DIMMs per channel, follow the vendor recommendation on how to populate each socket. • All the DIMMS are of the same capacity. • DIMM technology and specification match the highest speed and transfer rates. • Load the ESXi package from the server vendor site if available, instead of the VMware site. DELL and HP have ESXi package. • Disable energy saving features.
CPU (MHz)	See the virtual machine profile table in the technical specifications.
Memory	See the virtual machine profile table in the technical specifications.
Disk space	See the virtual machine profile table in the technical specifications.
Network bandwidth	A dedicated pair of 1 Gbps network interfaces must be available in a teamed, failover configuration. Alternatively, 1 Gbps of dedicated bandwidth on a pair of 10 Gbps network interfaces must be available in a teamed, failover configuration.
IOPS	The system must support 100 Input/Output Operations per Second (IOPS).
Hyper-threading	For media virtual machines, enable hyper-threading on the host.

ESXi Feature	OVA support
ESXi version	6.0, 6.5, or 6.7
Clone Virtual Machine	Not supported.

Table continues…

ESXi Feature	OVA support
Large Receive Offload (RLO)	Not supported.
Resize Virtual Machine	Not supported. Do not change any parameters after deploying the VM. If you need to resize the VM, you must re-deploy it and select a different profile.
CPU and Memory Reservations	Supported. Reservations are mandatory. Do not modify the CPU reservations that are set for the OVAs.
VMware Storage vMotion	Not supported.
VMware vMotion	Supported. To migrate to a different physical host, you must first shut down the VM. **Important:** If the host server is part of an Enhanced vMotion cluster, this reduces the CPU compatibility as described in https://kb.vmware.com/s/article/1003212. According to this VMware Knowledge Base, L6 Intel Haswell Generation has Advanced Vector Extensions 2 (AVX2) with vMotion. Older L5 Intel Ivy Bridge Generation and L4 Intel Sandy Bridge Generation do not have AVX2, even if the CPU itself supports AVX2. Both Ivy Bridge and Sandy Bridge come with AVX2.
VMware snapshots	Supported for temporary use when applying feature packs, service packs, or patches during maintenance windows. Snapshots adversely impact the VM disk and CPU performance. Remove the snapshots before returning the server to production.
VMware High Availability (HA)	Not supported.
VMware Distributed Resource Scheduler (DRS)	Not supported.
Distributed Power Management (DPM)	Not supported.
VMware Fault Tolerance (FT)	Not supported.
vSphere Standard Switch	Supported when the media server has a dedicated pair of 1 Gbps NICs or 1 Gbps of dedicated bandwidth on a pair of 10 Gbps NICs.
vSphere Distributed Switch	Supported if the vSphere Distributed Switch is engineered to provide same bandwidth as the vSphere Standard Switch. The media server requires a dedicated pair of 1 Gbps NICs or 1 Gbps of dedicated bandwidth on a pair of 10 Gbps NICs.
VSAN support	Not supported.

Common prerequisites for software installation

Verify the following:

- The deployment layout type is based on the capacity and scaling requirements.
- You obtained the required number of IP addresses.
- All Avaya Equinox® Conferencing components are deployed as VMware OVAs (except for Avaya Equinox® Streaming and Recording that is in WIM format).
- The target servers meet the following requirements:
  - All application servers have the same hardware type with the same disk, CPU, memory, and network interface configuration according to the appropriate deployment layout.
  - All servers meet the minimum hardware and configuration requirements for the Avaya Equinox® Solution.
  - All servers are connected and installed into the target environment including cables and network connections.
  - All servers have the Motherboard BIOS and the disk controller BIOS settings configured to ensure installation of the server platform software.
- The host environment meets the following:
  - Networking is in place to host the target servers and it is configured to route traffic between servers, firewalls, routers, switches, DMZ, and any other equipment in the host network, for example, management stations.
  - Up to two NTP clock sources available for the system to receive clocking information.
  - Up to three DNS servers available for the system to resolve addresses
  - A desktop computer or server (other than the one hosting the target server), that can execute ICMP ping requests
  - A PC/Mac with current version of Chrome, Firefox or Safari.
  - A desktop computer or server that is synchronized to the same external NTP clock sources used by the target servers.

    NTP synchronization is particularly important for TE deployments. All elements in the Avaya Aura® deployment must be aligned, including Avaya Aura® Session Manager, Avaya Aura® System Manager, Avaya Aura® Device Services, and Avaya Multimedia Messaging.
- Obtain any certificates that are to be used from either an Enterprise Certificate Authority or from some other well-known trusted Certificate Authority.
- If you are installing Avaya Equinox® for Team Engagement, the Avaya Aura® components must be installed and operational prior to installing the solution.
- If you are installing Avaya Equinox® for Over The Top with another SIP-based PBX, the PBX/SIP Entities must be installed and operational prior to installing the solution.

Latest software updates and patch information

Before you start the deployment or upgrade of an Avaya product or solution, download the latest software updates or patches for the product or solution. For more information, see the latest release notes, Product Support Notices (PSNs), and Product Correction Notices (PCNs) for the product or solution on the Avaya Support web site at https://support.avaya.com/.

After deploying or upgrading a product or solution, use the instructions in the release notes, PSNs, or PCNs to install any required software updates or patches.

For third-party products used with an Avaya product or solution, see the latest release notes for the third-party products to determine if you need to download and install any updates or patches.

Software installation checklist for SMB deployment

The following table provides a high-level view of the tasks involved in installing the applications software. Use this checklist when you perform a fresh installation of applications software.

No.	Task	Description	Notes	✓
1	Ensure you have planned your deployment layout.	See Before You Begin checklist on page 29.		
2	Review the prerequisites	See Common prerequisites for software installation on page 39.		
3	Ensure that you install the latest patches.	See the latest Avaya Equinox® Solution patches, which are available on http://support.avaya.com.	There are two types of patches for the Equinox Solution: Operating System Patches Application patches Ensure that you have the latest of both types of patch.	

Table continues…

No.	Task	Description	Notes	✓
4	Deploy the Equinox Management OVA and activate Equinox Management.	Installed modules include: Management, SIP B2BUA, H.323 Gatekeeper, Equinox Conference Control, User Portal + Web Gateway. The Avaya Aura® User Portal and Avaya Aura® Web Gateway functionalities are available as an integrated part of Equinox Management. See the chapter explaining the installation and first configuration tasks.	For deployments with more than 2,000 concurrent calls, install Avaya Equinox Web Gateway/Portal, H.323 Gatekeeper, and Equinox Conference Control as separate OVAs and nodes.	
5	Deploy Equinox Media Server OVAs and activate these servers on Equinox Management.	Installed modules include: MCU, WCS, AMS. See the chapter explaining the installation and first configuration tasks.		

Table continues…

No.	Task	Description	Notes	✓
6	Deploy other components, such as Equinox Streaming and Recording Server, Avaya Equinox® Recording Gateway, Avaya Session Border Controller for Enterprise (ASBCE), Equinox H.323 Edge server and add to Equinox Management.	• Avaya Equinox® Recording Gateway is relevant for Equinox Streaming and Recording Server. It facilitates recording of audio-only and web collaboration conferences or pure audio-only conferences hosted on Equinox Media Server and Scopia Elite MCUs into Equinox Streaming and Recording Server. For more information, see *Release Notes for Avaya Equinox® Recording Gateway* on http://support.avaya.com. • Equinox H.323 Edge server provides a complete firewall and NAT traversal solution for H.323 deployments, enabling secure connectivity between enterprise networks and remote sites.	• Deploying ASBCE is mandatory when Avaya IX™ Workplace Client as a Meet-Me client is part of the solution. • Deploy Equinox H.323 Edge only in legacy Avaya Scopia solution deployments. The H.323 protocol is used only in legacy Avaya Scopia deployments.	

Table continues…

No.	Task	Description	Notes	✓
7	Create and sign CSR and apply Equinox Management certificates.	You can use the CA in Equinox Management to sign certificates for other components. Prior to 9.1, when you had to regenerate a new certificate for Equinox Management, you had to delete the current certificate first, then generate a CSR for the CA to sign. If it took time to get the new certificate, Equinox Management had to stop service during that period of time. From 9.1 on, the new CSR can be generated in advance. Thus, when the new certificate is ready, the administrator can replace it. Equinox Management prompts for client authentication and server authentication as the Extended Key Usage attributes when generating the CSR. As a result, the third-party CA can add these attributes to the certificate and mutual TLS is achieved successfully.		
8	Create and sign CSR for each component such as Equinox Streaming and Recording Server, Avaya Equinox® Recording Gateway, ASBCE, Equinox H.323 Edge server.			
9	Restart Equinox Management server.			
10	Restart Equinox Media Server.			

Table continues…

No.	Task	Description	Notes	✓
11	Sync Meeting types from Equinox Media Server to Equinox Management. **Important:** Do not upload Equinox Media Server meeting types to Scopia® Elite 6000 MCU if this server is installed.			
12	Configure the Meeting Policies in Equinox Management.			
13	Configure Users and Virtual Rooms in Equinox Management.			
14	Install clients and endpoints.	Soft clients might include: Avaya IX™ Workplace Client Meet-Me and Avaya Equinox® Meetings for Web (WebRTC). See the product's user guide.		
15	Configure clients and endpoints in the management entities of the OTT solution.	See the product's administrator guide.		
16	Create calls.			
17	Configure the products.	See the product's administrator guide.		
18	Backup your Equinox Solution system after you install it.	See the product's administrator guide.		
19	If your deployment is a redundant deployment, install the products on secondary servers.	Return to step 1 in this checklist.		

Software installation procedures for medium to large deployments

The following table provides a high-level view of the tasks involved in installing the applications software. Use this checklist when you perform a fresh installation of applications software.

No.	Task	Description	Notes	✓
1	Ensure you have planned your deployment layout.	See Before You Begin checklist on page 29.		
2	Review the prerequisites	See Common prerequisites for software installation on page 39.		
3	Ensure that you install the latest patches.	See the latest Avaya Equinox® Solution patches, which are available on http://support.avaya.com.	There are two types of patches for the Equinox Solution: Operating System Patches Application patches Ensure that you have the latest of both types of patch.	
4	Deploy Avaya Aura® OVAs.	Only for TE deployments.		

Table continues…

No.	Task	Description	Notes	✓
5	Deploy the Equinox Management OVA and activate Equinox Management.	In the OTT solution the installed modules include: Management, SIP B2BUA, H.323 Gatekeeper, Equinox Conference Control, User Portal + Web Gateway. The Avaya Aura® User Portal and Avaya Aura® Web Gateway functionalities are available as an integrated part of Equinox Management. If the OTT solution is used in an Aura environment, the integrated Avaya Aura® User Portal and Avaya Aura® Web Gateway functionalities are provided in the Aura architecture. See the OTT/TE chapter explaining the installation and first configuration tasks for Equinox Management.	• For OTT deployments with more than 2,000 concurrent calls, install Avaya Equinox Web Gateway/Portal, H.323 Gatekeeper, and Equinox Conference Control as separate OVAs and nodes. For TE deployments with more than 2,000 concurrent calls, install Avaya Aura® Web Gateway, Portal, H.323 Gatekeeper, and Equinox Conference Control as separate OVAs and nodes.	
6	Deploy Equinox Media Server OVAs and activate these servers on Equinox Management.	Installed modules include: MCU, WCS, AMS. See the chapter explaining the installation and first configuration tasks.		

Table continues…

No.	Task	Description	Notes	✓
7	Deploy other components, such as Equinox Streaming and Recording Server, Avaya Equinox® Recording Gateway, Avaya Session Border Controller for Enterprise (ASBCE), Equinox H.323 Edge server, and add to Equinox Management.	• Avaya Equinox® Recording Gateway is relevant for Equinox Streaming and Recording Server. It facilitates recording of audio-only and web collaboration conferences or pure audio-only conferences hosted on Equinox Media Servers and Scopia Elite MCUs into Equinox Streaming and Recording Server. For more information, see *Release Notes for Avaya Equinox® Recording Gateway* on http://support.avaya.com. • Equinox H.323 Edge server provides a complete firewall and NAT traversal solution for H.323 deployments, enabling secure connectivity between enterprise networks and remote sites.	• Deploying ASBCE is mandatory when Avaya IX™ Workplace Client as a Meet-Me client is part of the solution. • Deploy Equinox H.323 Edge only in legacy Avaya Scopia solution deployments. The H.323 protocol is used only in legacy Avaya Scopia deployments.	

Table continues…

No.	Task	Description	Notes	✓
8	Create and sign CSR and apply Equinox Management certificates.	You can use the CA in Equinox Management to sign certificates for other components. Prior to 9.1, when you had to regenerate a new certificate for Equinox Management, you had to delete the current certificate first, then generate a CSR for the CA to sign. If it took time to get the new certificate, Equinox Management had to stop service during that period of time. From 9.1 on, the new CSR can be generated in advance. Thus, when the new certificate is ready, the administrator can replace it. Equinox Management prompts for client authentication and server authentication as the Extended Key Usage attributes when generating the CSR. As a result, the third-party CA can add these attributes to the certificate and mutual TLS is achieved successfully.		
9	Create and sign CSR for each component .			
10	Restart Equinox Management Server.			
11	Restart Equinox Media Server.			

Table continues…

No.	Task	Description	Notes	✓
12	Sync Meeting types from Equinox Media Server to Equinox Management. **Important:** Do not upload Equinox Media Server meeting types to Scopia® Elite 6000 MCUif this server is installed.			
13	Configure the Meeting Policies in Equinox Management.			
14	Configure Users and Virtual Rooms in Equinox Management.			
15	Install clients and endpoints.	In the OTT solution, soft clients might include: Avaya IX™ Workplace Client Meet-Me and Avaya Equinox® Meetings for Web (WebRTC). In the TE solution, clients might include: Avaya IX™ Workplace Client, Avaya H175 Video Collaboration Station, SDK customized clients, Avaya Vantage™. See the product's administrator guide.		
16	Configure clients and endpoints in the management entities of the OTT/TE solution.	See the product's user guide.		
17	Create calls.			
18	Configure the products.	See the product's administrator guide.		
19	Backup your Equinox Solution system after you install it.	See the product's administrator guide.		

Table continues…

No.	Task	Description	Notes	✓
20	If your deployment is a redundant deployment, install the products on secondary servers.	Return to step 1 in this checklist.		

Software installation procedure for large deployments and for Service Providers

The following table provides a high-level view of the tasks involved in installing the applications software. Use this checklist when you perform a fresh installation of applications software.

No.	Task	Description	Notes	✓
1	Ensure you have planned your deployment layout.	See Before You Begin checklist on page 29.		
2	Review the prerequisites	See Common prerequisites for software installation on page 39.		
3	Ensure that you install the latest patches.	See the latest Avaya Equinox® Solution patches, which are available on http://support.avaya.com.	There are two types of patches for Equinox Solution: Operating System Patches Application patches Ensure that you have the latest of both types of patch.	
4	Deploy the Avaya Aura® OVAs.	Only for TE deployments.		

Table continues…

No.	Task	Description	Notes	✓
5	Deploy the Equinox Management OVA and activate Equinox Management.	In the OTT solution the installed modules include: Management, SIP B2BUA, H.323 Gatekeeper, Equinox Conference Control, User Portal + Web Gateway. The Avaya Aura® User Portal and Avaya Aura® Web Gateway functionalities are available as an integrated part of Equinox Management. If the OTT solution is used in an Aura environment, the integrated Avaya Aura® User Portal and Avaya Aura® Web Gateway functionalities are provided in the Aura architecture. See the OTT/TE chapter explaining the installation and first configuration tasks for Equinox Management.	• For OTT deployments with more than 2,000 concurrent calls, install Avaya Equinox Web Gateway/Portal, H.323 Gatekeeper, and Equinox Conference Control as separate OVAs and nodes. For TE deployments with more than 2,000 concurrent calls, install Avaya Aura® Web Gateway/Portal, H.323 Gatekeeper, and Equinox Conference Control as separate OVAs and nodes.	
6	Deploy Equinox Media Server OVAs and activate these servers on Equinox Management.	Installed modules include: MCU, WCS, AMS. See the chapter explaining the installation and first configuration tasks.		

Table continues…

No.	Task	Description	Notes	✓
7	Deploy other components, such as Equinox Streaming and Recording Server, Avaya Equinox® Recording Gateway, Avaya Session Border Controller for Enterprise (ASBCE), Equinox H.323 Edge server, and add to Equinox Management.	• Avaya Equinox® Recording Gateway is relevant for Equinox Streaming and Recording Server. It facilitates recording of audio-only and web collaboration conferences or pure audio-only conferences hosted on Equinox Media Servers and Scopia Elite MCUs into Equinox Streaming and Recording Server. For more information, see *Release Notes for Avaya Equinox® Recording Gateway* on http://support.avaya.com. • Equinox H.323 Edge server provides a complete firewall and NAT traversal solution for H.323 deployments, enabling secure connectivity between enterprise networks and remote sites.	• Deploying ASBCE is mandatory when Avaya IX™ Workplace Client as a Meet-Me Client is part of the solution. • Deploy Equinox H.323 Edge only in legacy Avaya Scopia solution deployments. The H.323 protocol is used only in legacy Avaya Scopia deployments.	

Table continues…

No.	Task	Description	Notes	✓
8	Create and sign CSR and apply Equinox Management certificates.	You can use the CA in Equinox Management to sign certificates for other components. Prior to 9.1, when you had to regenerate a new certificate for Equinox Management, you had to delete the current certificate first, then generate a CSR for the CA to sign. If it took time to get the new certificate, Equinox Management had to stop service during that period of time. From 9.1 on, the new CSR can be generated in advance. Thus, when the new certificate is ready, the administrator can replace it. Equinox Management prompts for client authentication and server authentication as the Extended Key Usage attributes when generating the CSR. As a result, the third-party CA can add these attributes to the certificate and mutual TLS is achieved successfully.		
9	Create and sign CSR for each component.			
10	Restart Equinox Management server.			
11	Restart Equinox Media Server.			
12	Sync Meeting types to Equinox Management. **Important:** Do not upload Equinox Media Server meeting types to Scopia® Elite 6000 MCU if this server is installed.			

Table continues…

No.	Task	Description	Notes	✓
13	Configure the Meeting Policies in Equinox Management.			
14	Configure Users and Virtual Rooms in Equinox Management.			
15	Install clients and endpoints.	In the OTT solution, soft clients might include: Avaya IX™ Workplace Client Meet-Me and Avaya Equinox® Meetings for Web (WebRTC). In the TE solution, soft clients might include: Avaya IX™ Workplace Client, Avaya H175 Video Collaboration Station, SDK customized clients. See the product's user guide.		
16	Configure clients and endpoints in the management entities of the OTT/TE solution.	See the product's user guide.		
17	Create calls.			
18	Configure the products.	See the product's administrator guide.		
19	Backup your Equinox Solution system after you install it.	See the product's administrator guide.		
20	If your deployment is a redundant deployment, install the products on secondary servers.	Return to step 1 in this checklist.		

Software installation procedure for adding servers

The following table provides a high-level view of the tasks involved in installing the applications software. Use this checklist when you perform a fresh installation of applications software.

No.	Task	Description	Notes	✓
1	Install Avaya Aura® OVAs on the additional servers.	For TE deployments. See the chapter explaining the installation and first configuration tasks.		
2	Equinox Management OVA on the additional server.	See the chapter explaining the installation and first configuration tasks.		
3	Install Equinox Media Server OVAs on additional servers.	See the chapter explaining the installation and first configuration tasks.		
4	Install other components such as Equinox Streaming and Recording Server, Avaya Session Border Controller for Enterprise, Equinox H.323 Edge server, and add to Equinox Management.	See the chapter explaining the installation and first configuration tasks.		

Changing the login password of the Platform Manager administrator

About this task

Platform Manager (PMGR) is part of the web collaboration solution for Avaya Equinox® Conferencing. PMGR is the entity that manages the installation, upgrading, system monitoring and configuration of the unified platform. Each software package on the physical/virtual servers includes a PMGR application (single instance per server). PMGR is automatically activated on server power up.

Avaya recommends replacing the default passwords for accessing all the devices as soon as possible after installation, and from time to time depending on the security policy of your organization.

The procedure described below applies to the following devices of Equinox Conferencing:

- H.323 Gatekeeper as a node
- Equinox User Portal as a node
- Equinox Conference Control as a node

- Avaya Equinox® Recording Gateway
- Avaya WebRTC Gateway
- Equinox H.323 Edge

Before you begin

- Make sure you have the default pmgradmin password, which is `password`.
- From release 9.1 SP3, there is an option to change the pmgradmin password when deploying a new OVA. If the administrator used this option for one of the servers, this option must be used for every other server deployed using the same password for all the deployed devices. If one of the servers was already deployed without changing the default password, all further deployments must be done likewise with the default password. This limitation will be addressed in a future release
- Before changing the password, see the following table.

Table 5: Before changing the pmgradmin password

Device deployment	Password change
H.323 Gatekeeper as a node	If an alternate gatekeeper is installed for the node in a master/slave deployment, the password must be changed on each server separately.
Equinox H.323 Edge	From release 9.1 SP1, SSH access is blocked for this device. In this case, Avaya recommends changing the pmgradmin password via the system console (through the ESXi console or a serial connection).

Procedure

1. Use SSH to access the device.
2. Type `pmgradmin` as username, and the default password.
3. At the Linux prompt, type `sudo /opt/avaya/pmgr/external-scripts/pmgr-update-local-admin.sh pmgradmin <old_pass> <new_pass>`

Changing Linux administrator user password for Scopia® Elite 6000 MCU and Equinox H.323 Edge

About this task

Avaya recommends replacing the default passwords for accessing all the devices as soon as possible after installation, and from time to time depending on the security policy of your organization.

Before you begin

The default password of the Linux user account created upon server installation is `password`.

Before changing the password, see the following table.

Table 6: Before changing the admin password

Device	Password change
Scopia® Elite 6000 MCU	Do not change the admin password using the procedure below. Instead, access the Equinox Management administrator web interface and follow the procedure explained in Changing the management administrator password on page 57. The password of the management administrator and the SSH login password for the admin of the Linux user account are the same. Once you change the management administrator password, you can use the new password as the SSH login password for the admin of the Linux user account.
Equinox H.323 Edge	The SSH login password for the admin of the Linux user account and the management administrator password are different. From release 9.1 SP1, SSH access is blocked for this device. In this case, Avaya recommends changing the pmgradmin password via the system console (through the ESXi console or a serial connection).

Procedure

1. Use SSH to access the device.
2. Type `admin` as username, and the default password.
3. At the Linux prompt, type `passwd`
4. Type the old password.
5. Type the new password.

Changing the management administrator password

About this task

Avaya recommends replacing the default passwords for accessing all the devices immediately after installation, and then regularly depending on the security policy of your organization.

Use the Equinox Management administrator web interface to change the passwords for the following Equinox Conferencing devices:

- Equinox Management
- Scopia® Elite 6000 MCU

- Equinox Media Server
- Equinox H.323 Edge
- H.323 Gatekeeper as a node
- User Portal deployed as a node
- Equinox Conference Control deployed as a node

Before you begin

Make sure you have administrator rights to change the password.

Before changing passwords, see the following table.

Table 7: Before changing the management administrator password

Device	Password change
Equinox Management	If you installed a master/slave deployment, the password synchronizes to the slave automatically.
Scopia® Elite 6000 MCU	The password of the management administrator and the SSH login password for the administrator of the Linux user account are the same. Once you change the management administrator password, you can use the new password as the SSH login password for the administrator of the Linux user account.
H.323 Gatekeeper	If you installed an alternate gatekeeper for the node in a master/slave deployment, you must change the password on each server separately.

Procedure

1. To change the Equinox Management password:
   a. Log in to the Equinox Management administrator web interface.
   b. Select the **Users** tab.
   c. Select **Users from Local Directory** on the left of the display.
   d. Select **All**.
   e. Select the relevant administrator user.
   f. Type the new password in the **Password** field.
   g. Re-type the new password in the **Confirm Password** field.
   h. Select **OK** , and then **Apply**.
2. To change password for:
   - Scopia® Elite 6000 MCU
   - Equinox Media Server
   - Equinox H.323 Edge

- H.323 Gatekeeper deployed as a node
- User Portal deployed as a node
- Equinox Conference Control deployed as a node

a. From the Equinox Management administrator web interface, select the **Devices** tab.
b. Select the device in **Devices by Type** on the left of the display.
c. Select the relevant device listed in the **Name** column.
d. Select the **Access** tab.
e. Select **Change Password** and follow the prompts.

Linux user accounts for Avaya Equinox® Conferencing

The following table lists user accounts for implementing commands that support Avaya Equinox® Conferencing management and operation.

Operating System essential user accounts

User account	Purpose
`root:x:0:0:root:/root:/bin/bash`	OS essential. This is the default root user.
`pmgradmin:x:1002:1002::/home/pmgradmin:/bin/bash` Platform Manager (PMGR) is part of the web collaboration solution for Avaya Equinox® Conferencing. PMGR is the entity that manages the installation, upgrading, system monitoring and configuration of the unified platform. Each software package on the physical/virtual servers includes a PMGR application (single instance per server). PMGR is automatically activated on server power up.	OS essential. This is the default (non-root) user.
`sync:x:5:0:sync:/sbin:/bin/sync`	OS essential.
`shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown`	OS essential.
`halt:x:7:0:halt:/sbin:/sbin/halt`	OS essential.

Miscellaneous user accounts

User account	Purpose
`craft:x:780:555::/home/craft:/bin/bash`	An Avaya Services login to access the system remotely for troubleshooting purposes.

Table continues…

User account	Purpose
`init:x:781:555::/home/init:/bin/bash`	An Avaya Services login to access the system remotely for troubleshooting purposes.
`sroot:x:0:0::/home/sroot:/bin/bash`	An Avaya Services login to access the system remotely for troubleshooting purposes. You cannot access the `sroot` login directly from a login prompt except on the server console.
`inads:x:782:555::/home/inads:/bin/bash`	An Avaya Services login used to remotely initialize and administer Communication Manager. INADS is the Initialization and Administration System.
`rasaccess:x:783:888::/home/rasaccess:/bin/bash`	An Avaya Services login to access the system remotely for troubleshooting purposes.

User accounts that Avaya plans to deprecate

To view the list of registered users, use the following command: `[pmgradmin@PMGR ~]> cat /etc/passwd`

User account	Status
Avaya Equinox Media Gateway (Avaya Equinox® Management) . Also known as Web Gateway.	
`admin:x:1000:1000:admin:/home/admin:/bin/bash`	deprecate
`postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash`	deprecate or `nologin`
`wcsuser:x:0:0::/home/wcsuser:/bin/bash`	deprecate for Application Server
`iview:x:1004:1004::/home/iview:/bin/bash`	`nologin`
Avaya Equinox® Media Server	
`postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash`	deprecate
`wcsuser:x:0:0::/home/wcsuser:/bin/bash`	deprecate or `nologin`
`admin:x:1005:32778::/home/admin:/bin/bash`	deprecate

Chapter 5: Equinox Management Deployment for Over the Top Solution

Deployment of Equinox Management for OTT solution — Overview

Equinox Management is delivered to the customer as an OVA file, which includes the pre-installed application on VMware vSphere virtual appliances, an Operating System (OS), and startup scripts necessary to perform initial product configuration.

Equinox Management verifies the amount of virtual resources it requires to operate the virtual machine. Each virtual appliance is associated with part numbers, as described in Deploying the Equinox Management Server on page 67.

Equinox Management Components

Equinox Management includes the following configurable components:

- Equinox Management
- SIP B2BUA
- H.323 Gatekeeper
- Equinox Conference Control
- User Portal + Web Gateway (optional)

Note:

- If you select High-Medium mode during OVA deployment, the User Portal + Web Gateway service is deployed on the management server with **Status = Active**.
- If you select Avaya Aura® Power Suite (UC) License during OVA deployment, the User Portal + Web Gateway service is not deployed on the management server.

The Equinox Management Server OVA activation key requires only a UUID, which is provided after deploying the OVA.

Virtualization Software

The Equinox Management server supports the following virtualization software:

- AVP 8.0

- VMware ESXi 6.0, 6.5 and 6.7
- VMware vCenter

For details on technical requirements, see Technical Specifications of Equinox Management on page 62.

Technical Specifications of Equinox Management

The Equinox Management server OVA supports two different working modes:

- **All-In-One**: Includes all of the components working in one VM, for medium capacity deployment.
- **Distributed**: For medium or high capacity deployment, one management server works with one or multiple distributed management servers. For distributed deployment, one management server runs Equinox Management, while the distributed management server works either as an H.323 Gatekeeper, an Equinox Conference Control (UCCS), or as a User Portal + Web Gateway.

Note:

- Using low memory capacity in OVA configuration can cause the User Portal + Web Gateway to fail.
- To support high capacity calls, the network must ensure that each subnet has enough bandwidth to support all required bandwidths for both media and signaling.

The following table describes the hardware requirements for Equinox Management deployment, according to the available configuration types:

Table 8: Matching hardware server specifications with your product

Configuration Capacity	Server CPU (processor x physical cores)	Server RAM (GB)	VM Minimum vCPUs	VM CPU Reservation (MHz)	RAM Reservation (GB)	DISK Reservation	Usage	Capacity (Calls/ Registered Users)
Low	2.4 x 4	8	4	8000	6	200	Distributed Management Node server User Portal + Web Gateway or H.323 Gatekeeper	H.323 – 2,000/10,000 User Portal + Web Gateway – 1,000/10,000

Table continues…

Configuration Capacity	Server CPU (processor x physical cores)	Server RAM (GB)	VM Minimum vCPUs	VM CPU Reservation (MHz)	RAM Reservation (GB)	DISK Reservation	Usage	Capacity (Calls/ Registered Users)
Medium — High	2.5 x 8	24	8	15000	16	200	**Medium** — Scale All-In-One Management Server (with Equinox Management & Web Gateway) — OTT **High** (with Equinox Management but without User Portal + Web Gateway, OTT/TE) Internal H.323 Gatekeeper capacity limited (see **Important** note below table)	**Medium (All–In–One)** – 2,000/30,000 **High** — 15,000

Important:

- When User Portal + Web Gateway resides with Equinox Management server, select the **Medium-High** VM model.
- H.323 Gatekeeper is limited to 2,000 calls (10,000 registrations); to increase capacity, use distributed Management Node VMs.
- User Portal + Web Gateway is limited to 3,000 calls. To increase capacity, use distributed Management Node VMs.
- Equinox Conference Control is limited to 2,000 calls.

The following table describes the usability and capacities for the various VM models used in Equinox Management.

Table 9: Usability and Capacities for your product

VM Model	Usability	Required License	Set Usage By	Capacity
Low	Distributed User Portal + Web Gateway - Small	Management Server License	Activating components through the Equinox Management UI	1,000 Web Gateway calls 2,000 User Portal sessions
Low	H.323 Gatekeeper	Management Server License	Activating component through the Equinox Management UI	2,000 calls 10,000 registrations
Medium-High	All-in-one Medium (Equinox Management, B2B, H.323 Gatekeeper, Equinox Conference Control, User Portal + Web Gateway)	Management Server License	VM automatically becomes all-in-one when User Portal + Web Gateway is activated. Capacity limitations are enforced by Equinox Management.	2,000 total calls (including 1,000 Web Gateway calls) 30,000 registered users 2,000 User Portal sessions
Medium-High	High scale management (Equinox Management, B2B, H.323 Gatekeeper, Equinox Conference Control)	Management Server License	VM automatically becomes HIGH when User Portal + Web Gateway is inactive by administrator. Relevant for TE and large OTT deployments.	15,000 total calls 150,000 registered users (400,000 unregistered users) 2,000 H.323 Gatekeeper calls
Medium-High	Distributed User Portal + Web Gateway - Medium	Management Server License	VM automatically becomes User Portal + Web Gateway when receiving license	2,000 Web Gateway calls 4,000 portal sessions
Medium-High	Distributed Equinox Conference Control	Management Server License	VM automatically becomes Equinox Conference Control when receiving license	2,000 total calls

Checklist for Deploying Equinox Management in an All-In-One Working Mode

The following list of tasks enables you to configure Equinox Management in an all-in-one working mode. All-in-one deployment entails all components working in one VM, and is typically used for small or medium capacity deployment.

No.	Task	Link/Notes	✔
1	Download software from the PLDS	Downloading software from PLDS on page 32	
2	Deploy the all-in-one Equinox Management server	Deploying the Equinox Management Server on page 67	
3	Log into the Equinox Management server	Logging Into Equinox Management on page 81	
4	Configure the Equinox Management server for the all-in-one working mode	Configuring the All-In-One Equinox Management Server on page 88	
5	Install the user license on the internal Equinox Management WebLM server	Installing a user license on the local WebLM server on page 422	
6	Secure connections	Securing Connections with Equinox Management on page 111	
7	Update your license	Updating a User License on page 420	
8	Deploy and Configure the Equinox Management Environment	Deploying and Configuring the Equinox Management Environment on page 136	

Checklist for Deploying Equinox Management in a Distributed Working Mode

The following list of tasks enables you to configure Equinox Management in a distributed working mode. Distributed deployment adds one or more nodes to your deployment, as follows:

- The management server runs Equinox Management.
- The distributed management server works as either the H.323 Gatekeeper, User Portal + Web Gateway or Equinox Conference Control.

Distributed deployment is typically used for media or high-capacity deployment.

No.	Task	Link/Notes	✔
1	Download software from the PLDS.	Downloading software from PLDS on page 32	
2	Deploy Equinox Management.	Deploying the Equinox Management Server on page 67	
3	Log into the Equinox Management.	Logging Into Equinox Management on page 81	
4	Get acquainted with the distributed deployment of Equinox Management.	Geographically Distributed Deployment of Equinox Management on page 91	
5	Enable the use of an external load balancer.	Disabling the Internal Load Balancer in Equinox Management on page 99	
6	Enable SIP B2BUA per your deployment requirements.	Access the setting from Equinox Management **Settings** > **Local Services**.	
7	Add the User Portal + Web Gateway.	Deploying a distributed or cluster User Portal and Web Gateway on page 100	
8	Add the H.323 Gatekeeper.	Deploying a Standalone Distributed H.323 Gatekeeper on page 104	
9	Add the alternate H.323 Gatekeeper.	Deploying Distributed H.323 Gatekeepers in Alternate Mode on page 106	
10	Add the Equinox Conference Control.	Deploying a Distributed UCCS Server on page 109	
11	Secure connections.	Securing Connections with Equinox Management on page 111	
12	Update your license.	Updating a User License on page 420	
13	Deploy and Configure the Equinox Management Environment.	Deploying and Configuring the Equinox Management Environment on page 136	

Downloading software from PLDS

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon ( ) for Company Name.

6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type `Avaya` or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
   - In **Download Pub ID**, type the download pub ID.
   - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. Scroll down to the entry for the download file, and click the **Download** link.
10. Select a location where you want to save the file, and click **Save**.
11. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.
12. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Deploying the Equinox Management Server

About this task

The Avaya Equinox® Management server OVA deployment includes the following configurable components:

- Equinox Management
- SIP B2BUA Server
- H.323 Gatekeeper
- Equinox Conference Control
- Web Collaboration Server
- User Portal + Web Gateway (optional)

The virtual appliance is associated with the following part numbers:

- **Base part number**: A part number which enables the customer to download the OVA itself.
- **Product activation license**: Enables full product functionality. Different product activation keys are required for the various product features. Customers can purchase product activation licenses according to the needs of their system. Licensing is based on UUID.

Before you begin

Before deploying Equinox Management on an AVP server with VMware ESXi, ensure that you have the following:

- Equinox Management OVA you downloaded from PLDS.
- Virtualization Software:
  - AVP 8.0
  - VMware ESXi 6.0, 6.5 and 6.7
  - VMware vCenter
  - VMware Workstation Pro 11 or later
- Hardware: See Table 8: Matching hardware server specifications with your product on page 62

Procedure

1. Copy the Equinox Management OVA files to your local machine.
2. Open the vSphere Client and enter the virtual host's user name and password in the relevant fields.

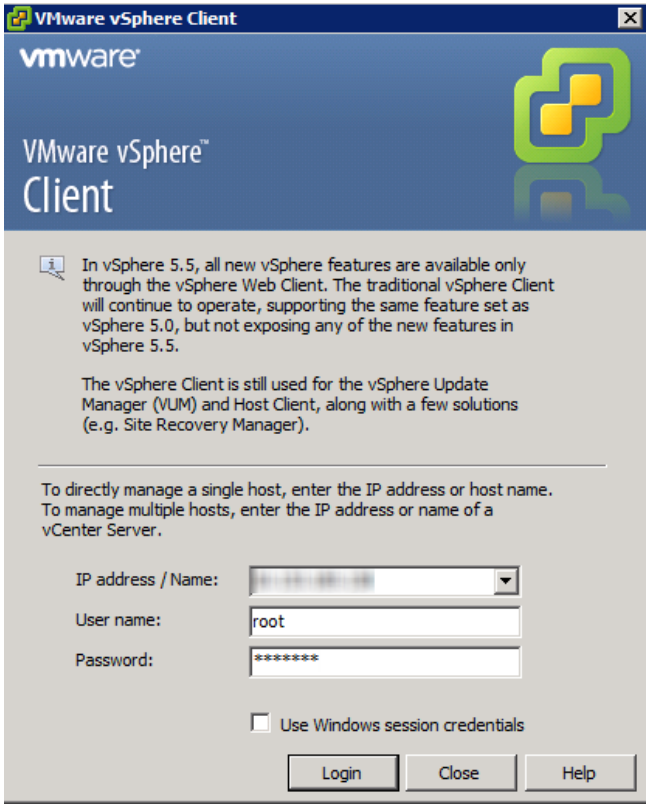


Figure 3: vSphere Client

3. Select **Login**.

The system displays the vSphere client page, where you select **File** > **Deploy OVF Template** to upload the .ova file.

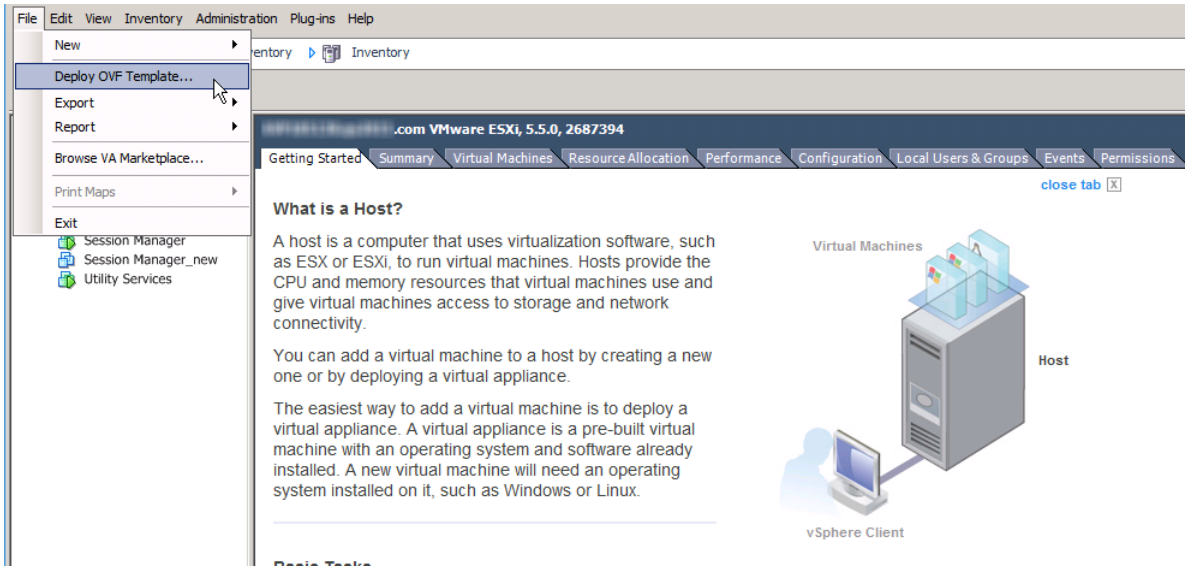


Figure 4: vSphere Client Page

4. Select the local Equinox Management OVA file, and select **Next** to open the **Deploy OVF Template** wizard.

   The system displays the **OVF Template Details** page with the product information.

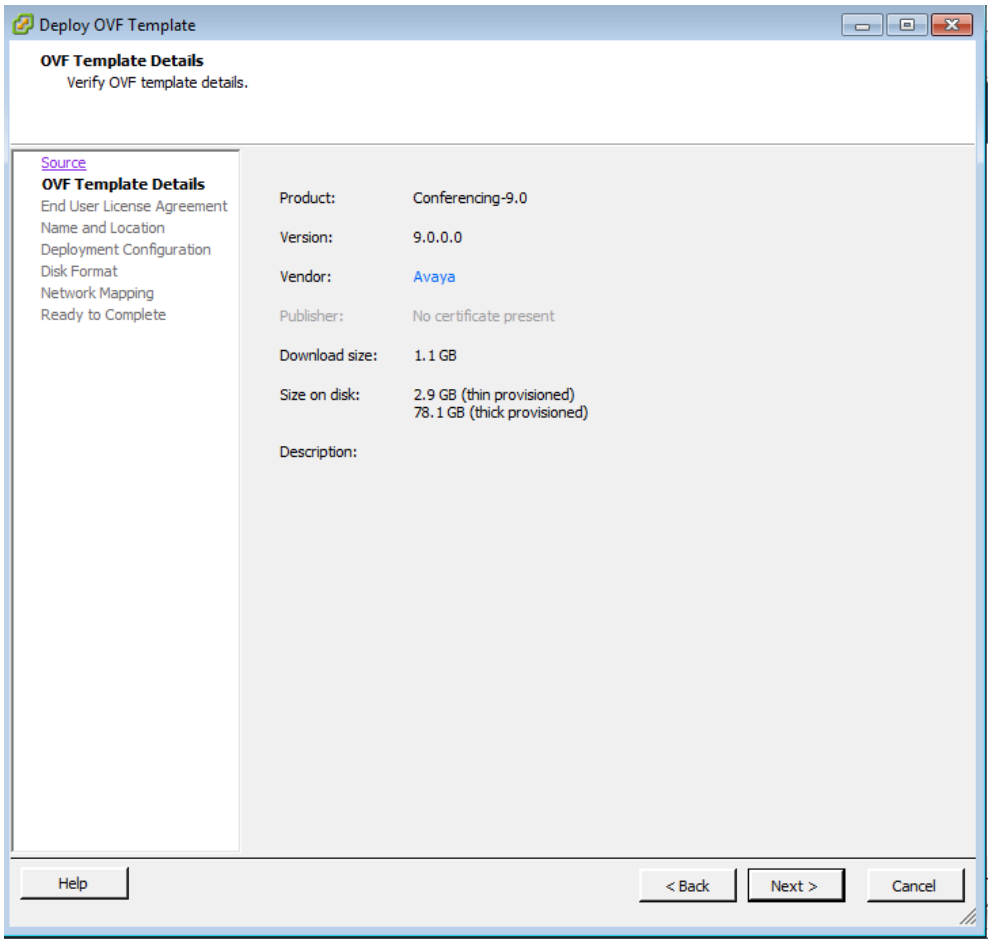


Figure 5: OVF Template Details Page

5. Select **Next**.

   The system displays the **End User License Agreement** page.

6. Select **Accept** to accept the license agreement, and select **Next**.

   The system displays the **Name and Location** page.

7. Enter a name for the OVF template in the **Name** field, and select **Next**.

   The system displays the **Deployment Configuration** page.

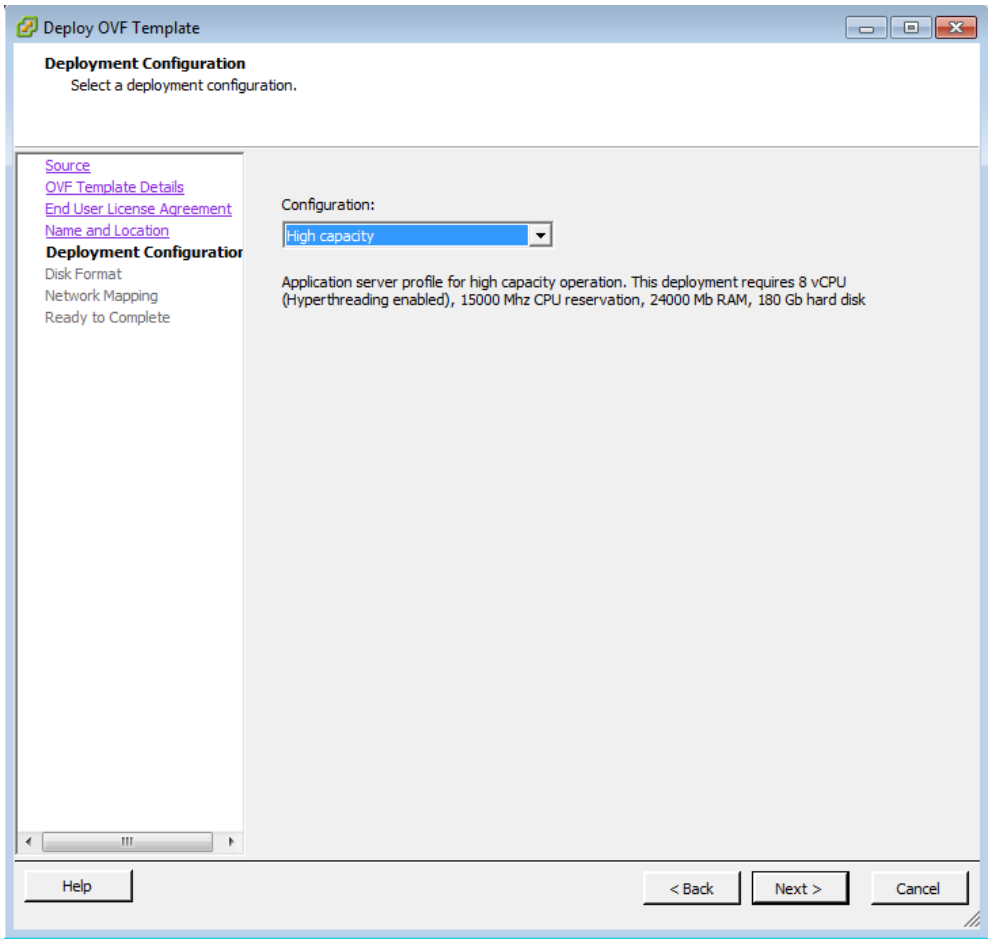


Figure 6: Deployment Configuration Page

For details on technical requirements per configuration type, see Technical Specifications of Equinox Management on page 62.

8. In the **Configuration** field, select the relevant Equinox Management profile, based on your environment, and select **Next**.

   The system displays the **Disk Format** page.

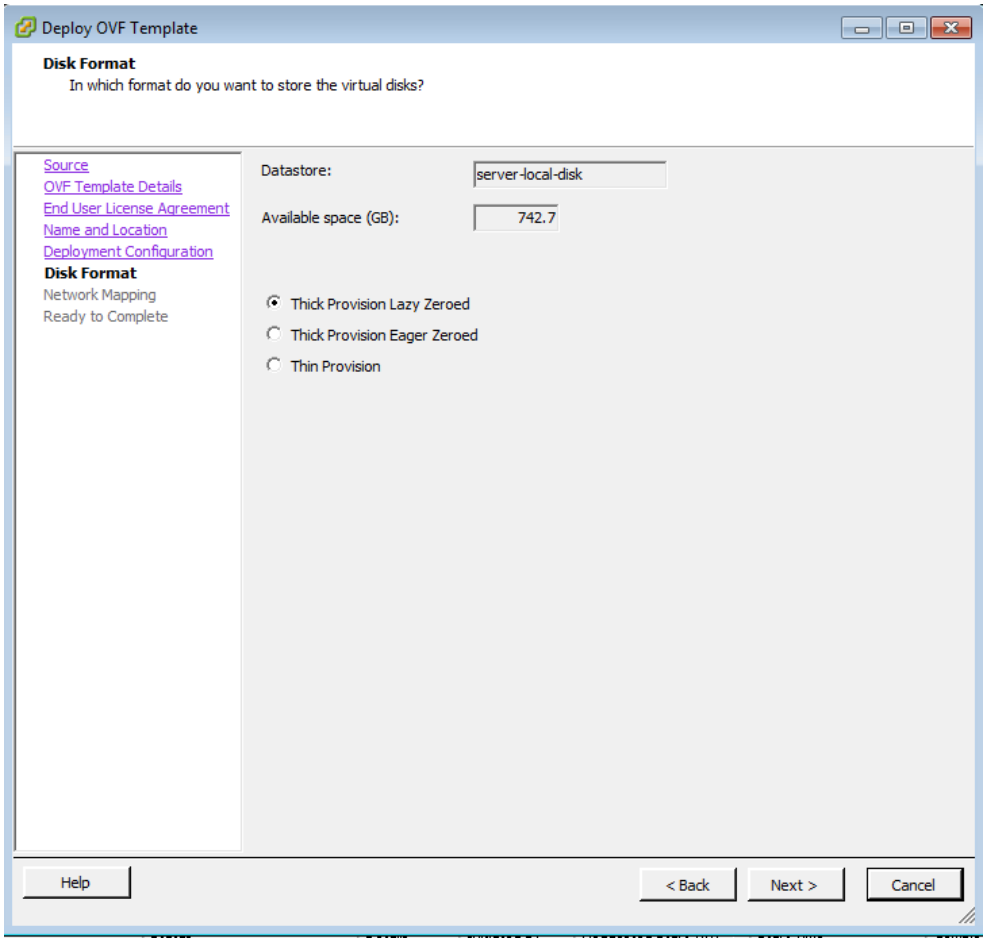


Figure 7: Disk Format Page

9. Select **Thick Provision Lazy Zeroed** and select **Next**.

   The system displays the **Network Mapping** page.

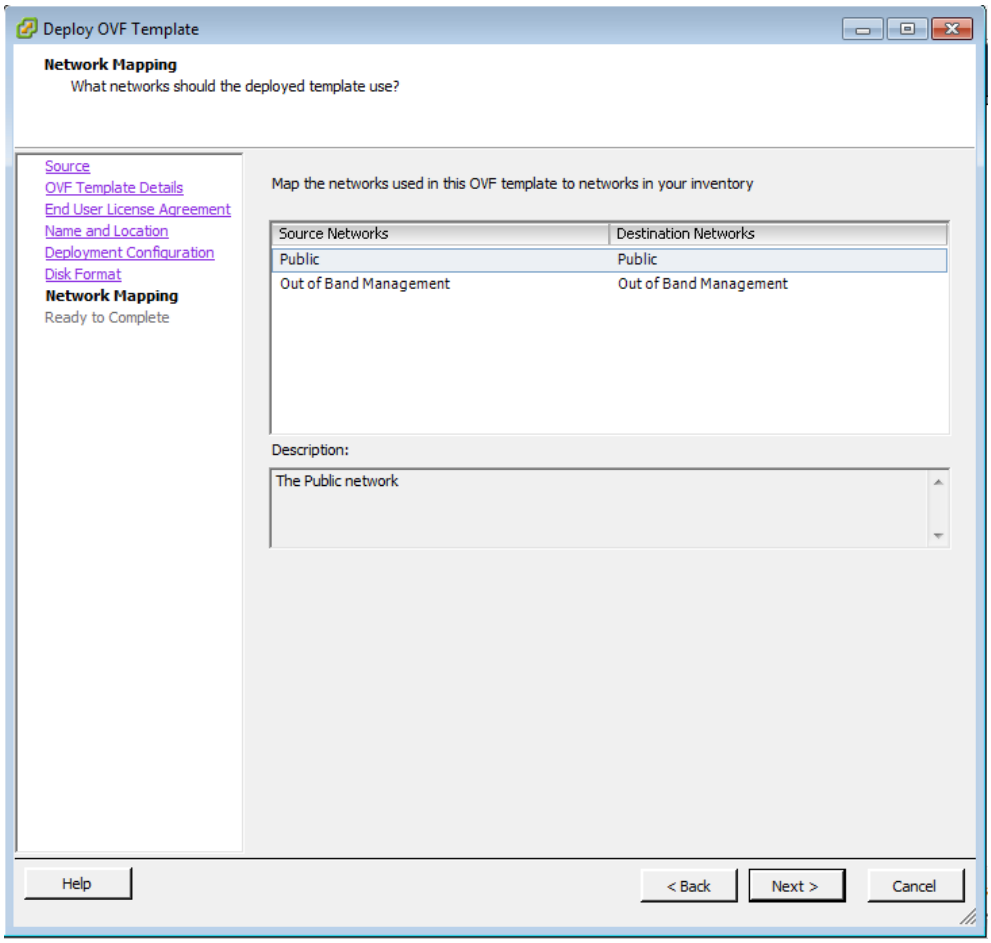


Figure 8: Network Mapping Page

Note:

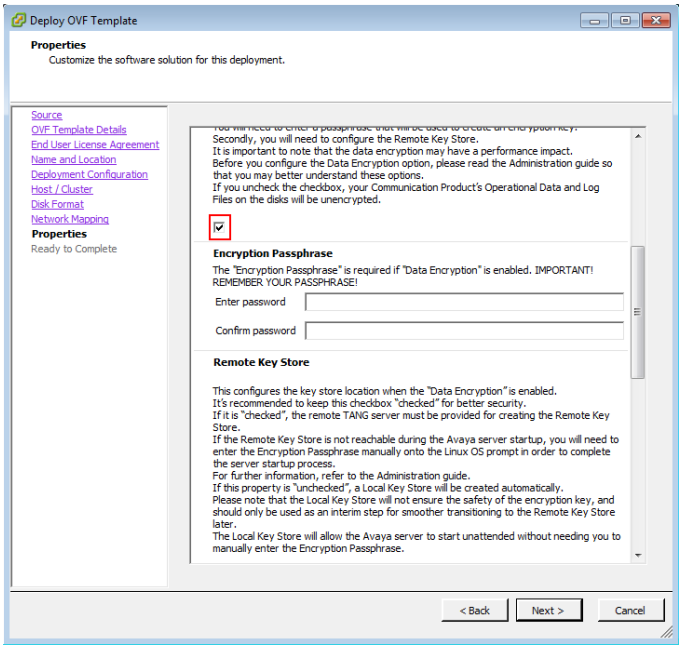
Out of Band Management is not supported for Equinox Management.

10. Map the networks used in your OVF template to networks in your inventory, and select **Next**.

11. If you want the communication product's operational data and log files to be encrypted, you must select the box *and* enter a passphrase.

Note:

The system does not force you to enter a passphrase. If the check box is selected and you do not enter a passphrase, the data is *not* encrypted.



The system displays the **Ready to Complete** page with your deployment settings.

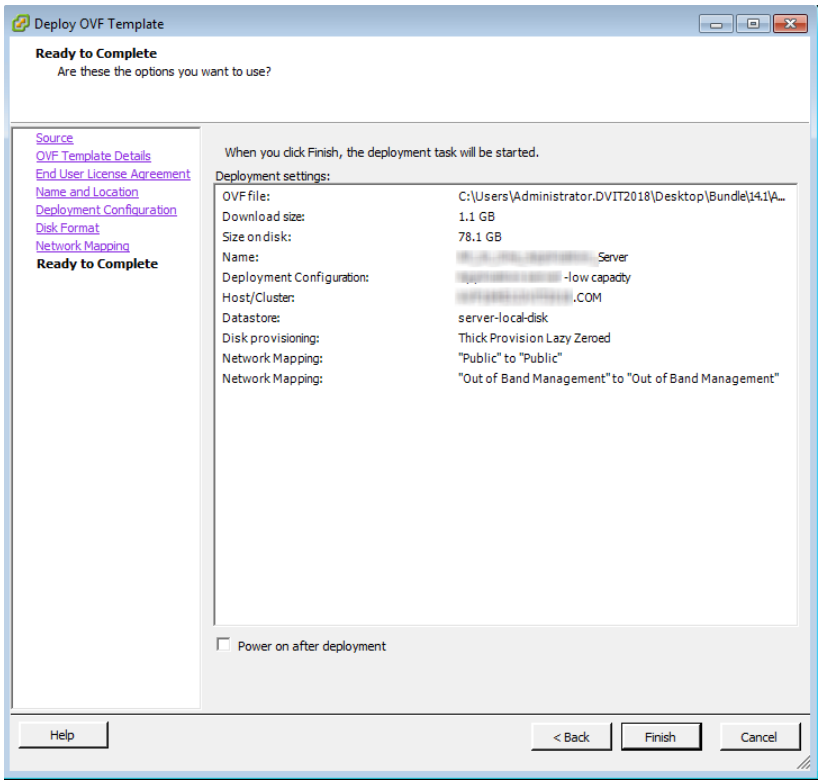


Figure 9: Ready to Complete Page

Optionally, select the **Power on after deployment** check box to activate Equinox Management after completing deployment.

12. Verify that your settings are correct, and select **Finish**.

    The system deploys the OVA to the virtual host server.

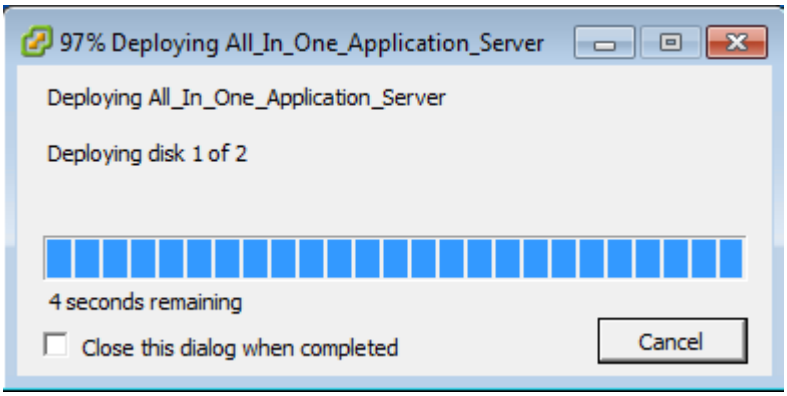


Figure 10: Deploying the OVA

The system closes the dialog box when deployment finishes, and displays the **Virtual Machine Properties** page with the properties of the virtual machine.

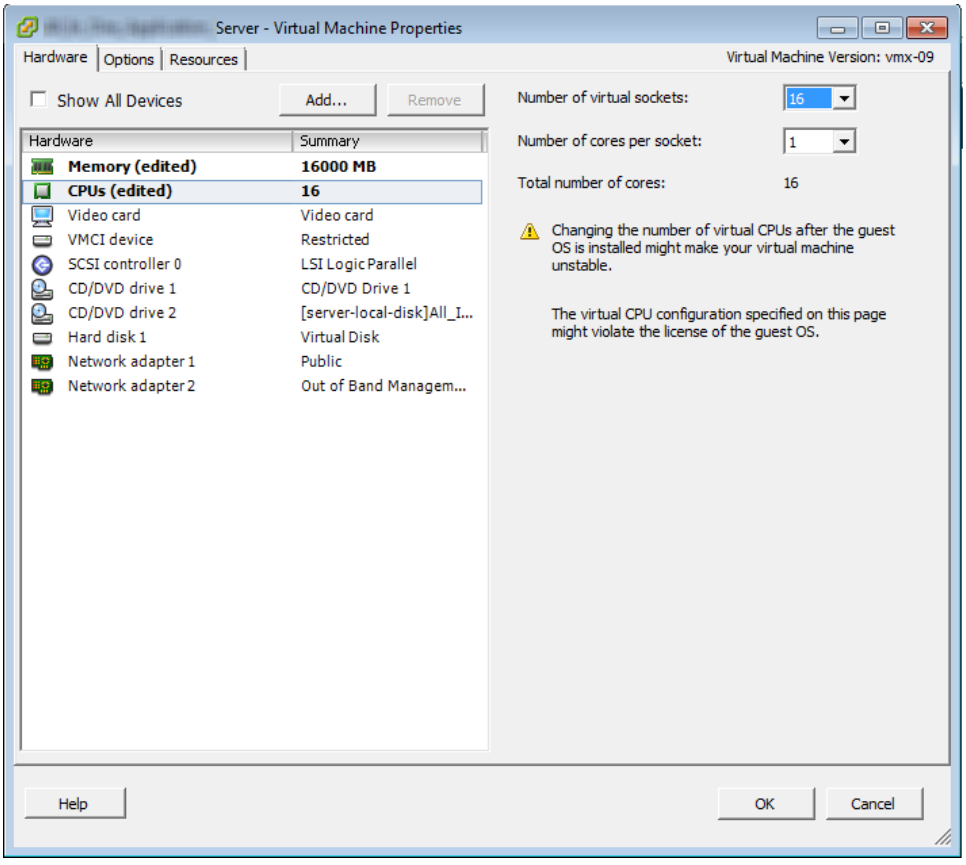


Figure 11: Virtual Machine Properties Page

13. Ensure that at least 8 CPU cores and 16 GB of memory are allocated.

14. Select **OK** to complete the deployment.
15. In the resulting window, right-click the OVA and select **Open Console**.

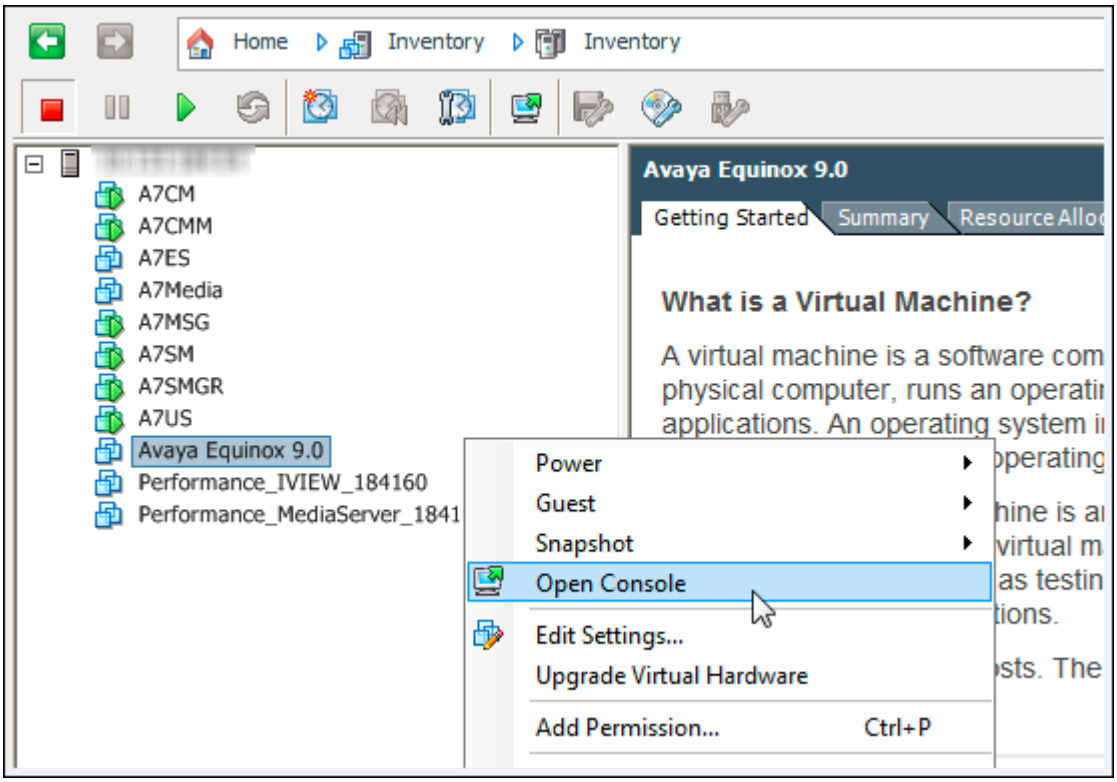


Figure 12: vSphere Client — Open Console Option

16. Select the green arrow icon to start the virtual server.

    The system displays the Command Prompt window in the vSphere Client.

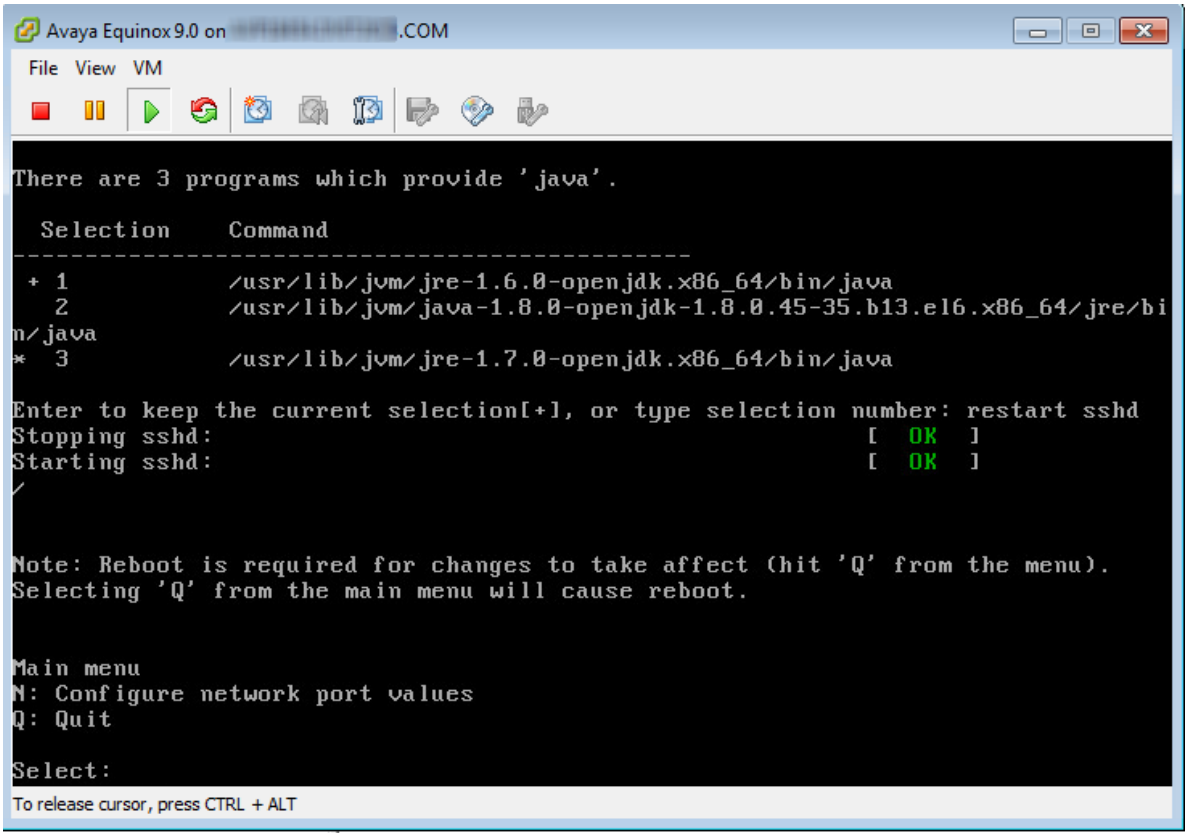


Figure 13: Server Command Prompt Window

17. Enter **N** next to the **Select** prompt to configure network port values.

    The system displays a new **Select** prompt, with the options for configuring network port values.

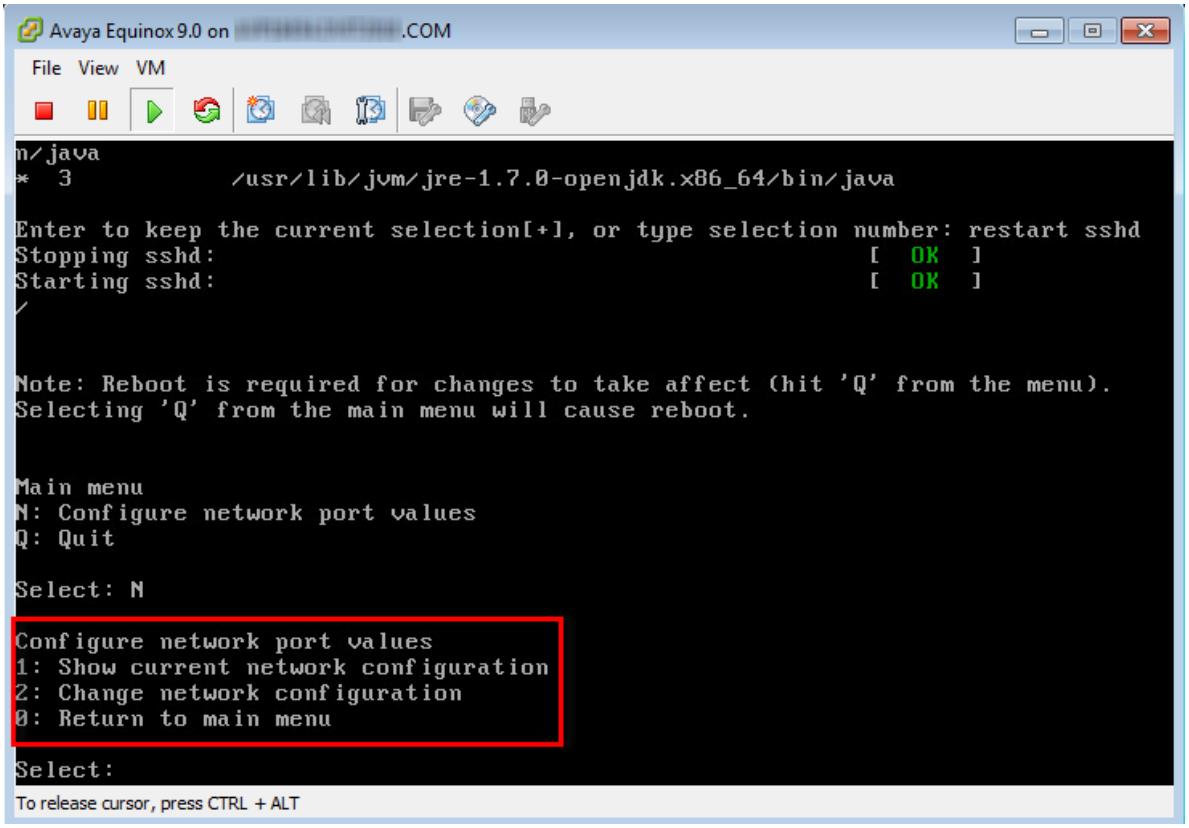


Figure 14: Configure Network Port Values Options

18. Enter **2** next to the **Select** prompt to change the network configuration.
19. On the resulting Command Prompt window, enter the IP address, subnet mask, and default router address. Press **Enter**.

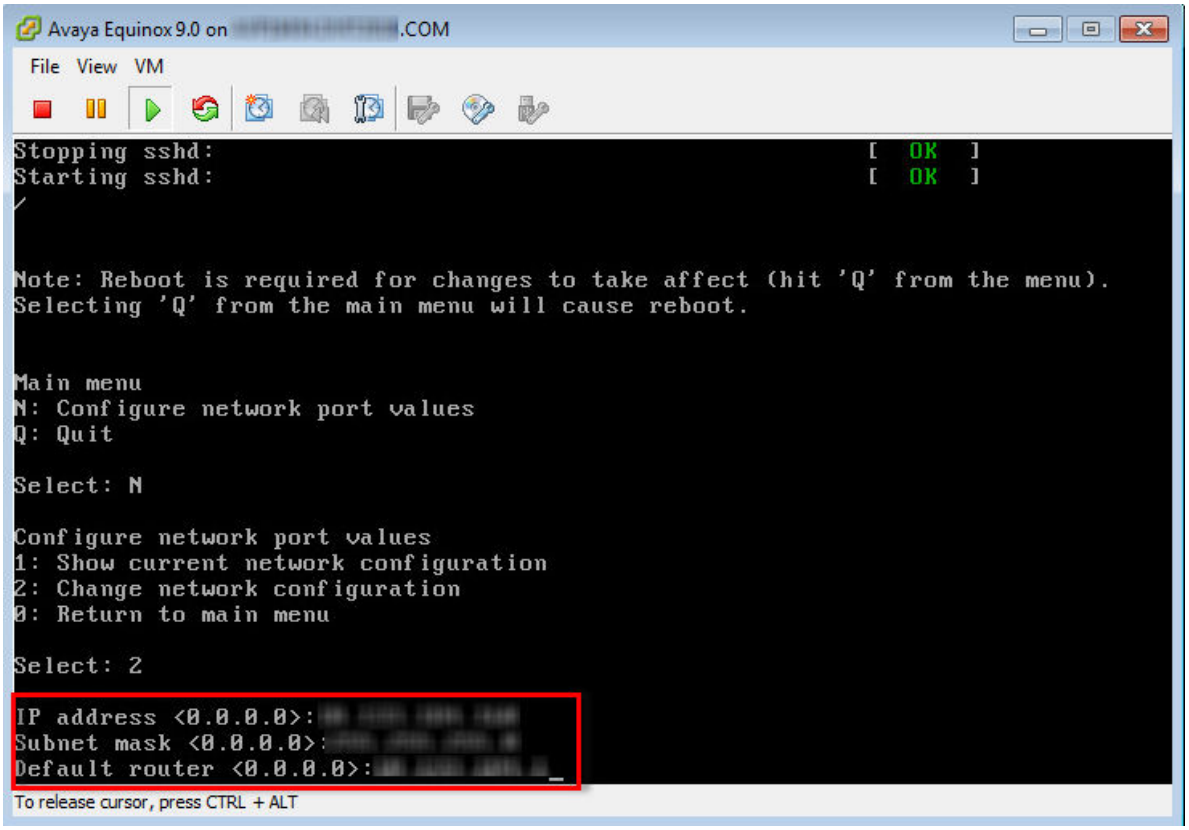


Figure 15: Changing Network Configuration

The system saves the parameters and refreshes the Command Prompt window .

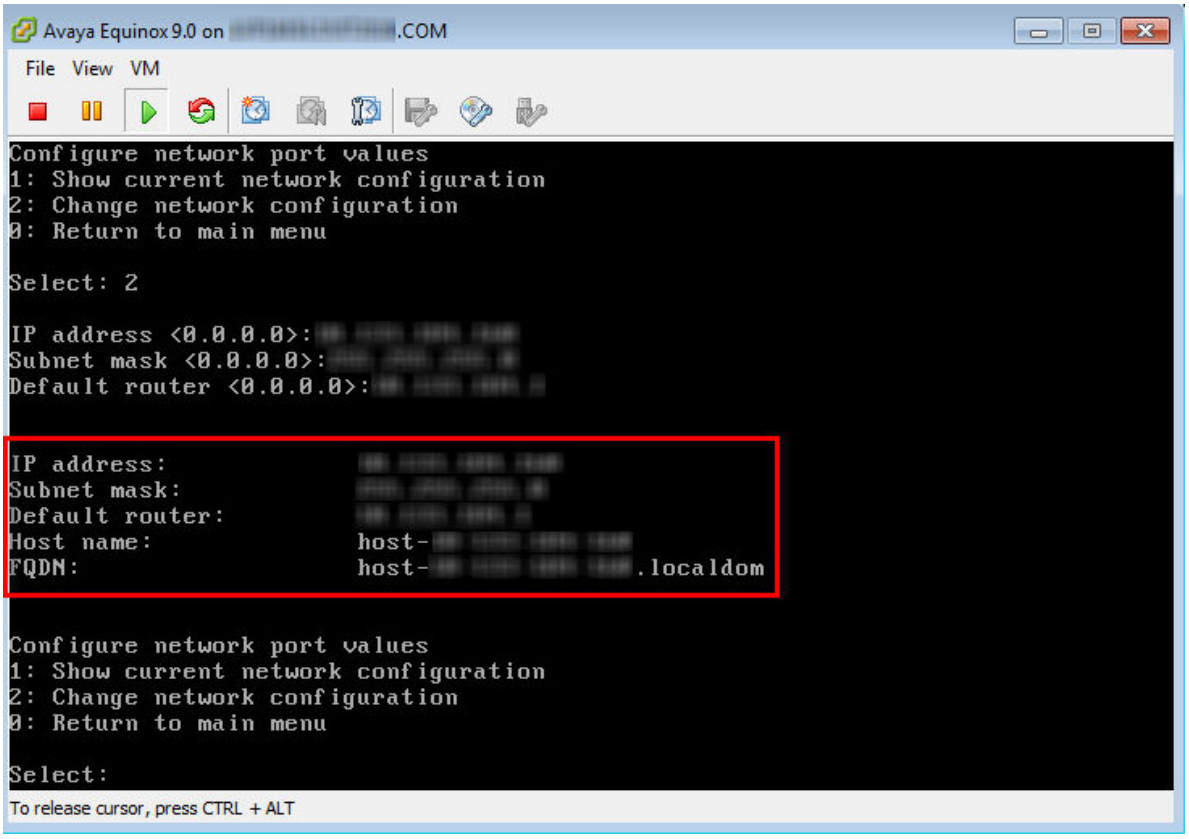


Figure 16: Network Configuration Values

20. Enter **0** next to the **Select** prompt to return to the main menu.

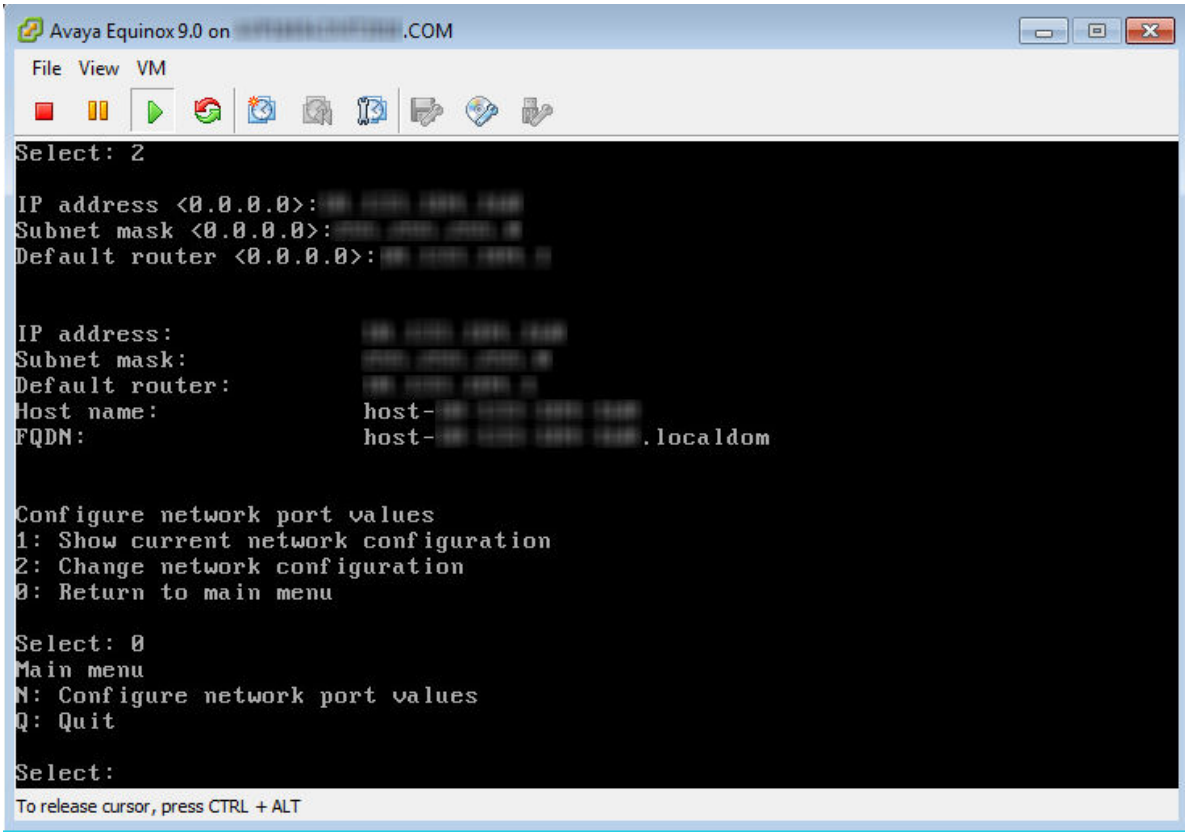


Figure 17: Main Menu

21. Enter **Q** next to the **Select** prompt to exit the vSphere Client and restart the virtual server with the updated network configurations.

    The Equinox Management OVA deployment is complete. Before logging on, wait 2-3 minutes for the server to complete initialization.

Next steps

Log into Equinox Management, as described in Logging into Equinox Management on page 81.

Logging into Equinox Management

About this task

After completing the Equinox Management deployment, log into Equinox Management.

Before you begin

- Ensure that you have successfully completed deployment of Equinox Management (see Deploying the Equinox Management Server on page 67).

- Ensure that you have set up the following components, with their respective IP addresses:
  - All-In-One server FQDN
  - NTP server

    Note:

    We recommend using the Linux NTP server, as the Windows NTP server may not work properly.
  - DNS server
- For licensing information, see Avaya Equinox® Management licenses on page 28.

Procedure

1. Access the Equinox Management server. By default, the URL is `https://<Your Server IP>:443/iview/`

   The system displays the introduction page of the Equinox Management Installation Wizard.

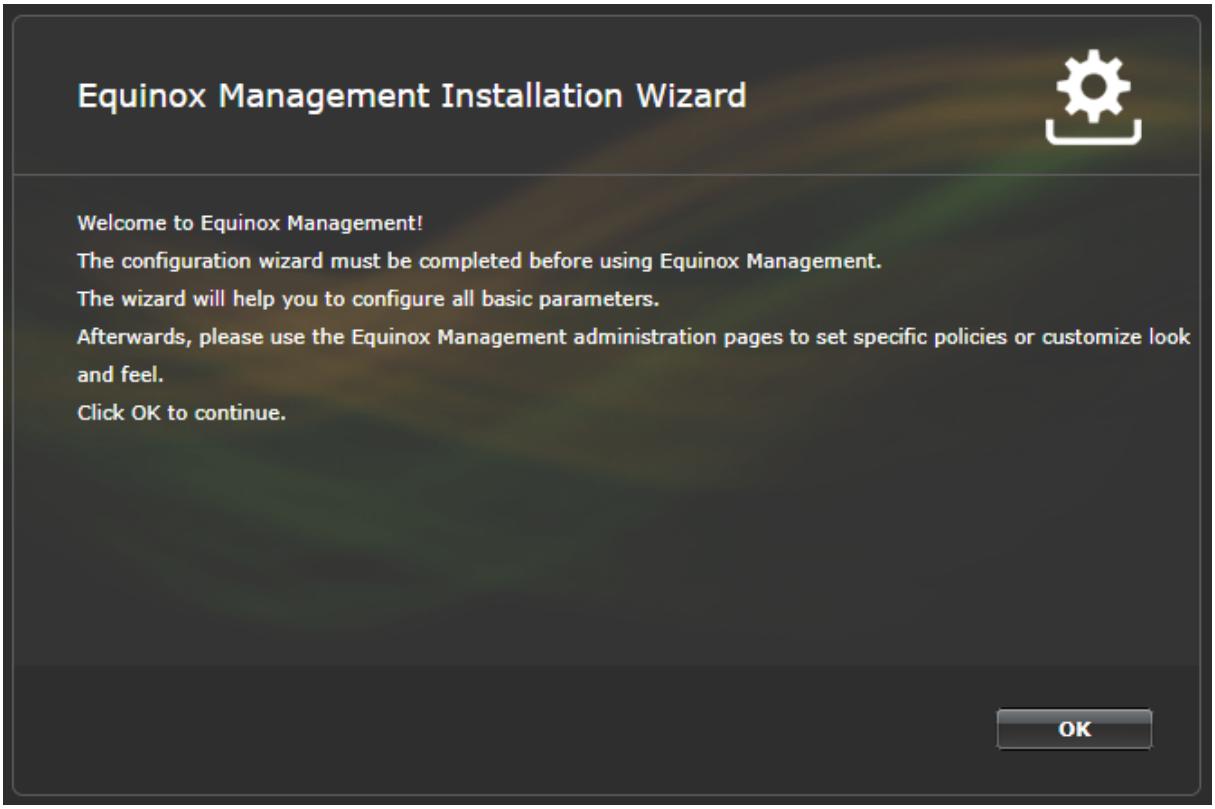


Figure 18: Equinox Management Installation Wizard — Introduction Page

2. Select **OK**.

   The system displays the first page of the install wizard.

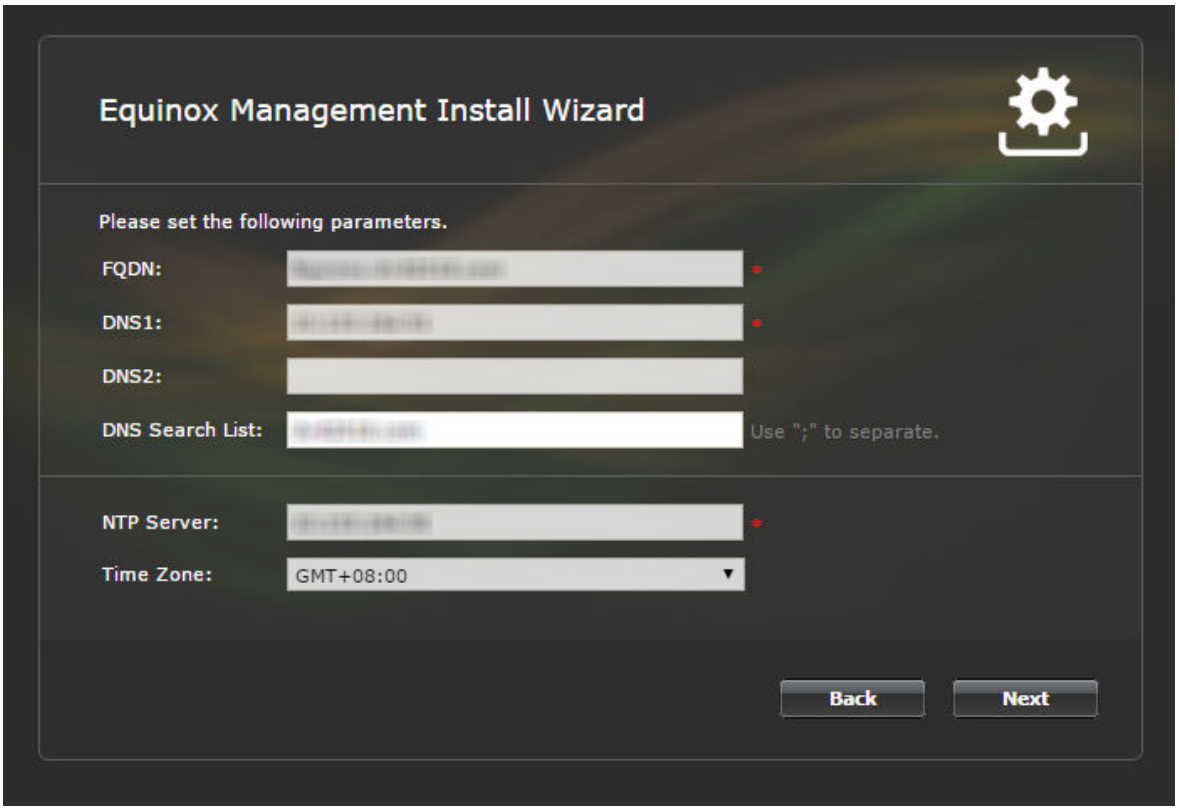


Figure 19: Equinox Management Installation Wizard — Parameters

3. Enter the server's parameters in the **FQDN**, **DNS**, **DNS Search**, **NTP Server**, and **Time Zone** fields, and select **Next**.

   The system displays the next page with your Equinox Management server UUID.

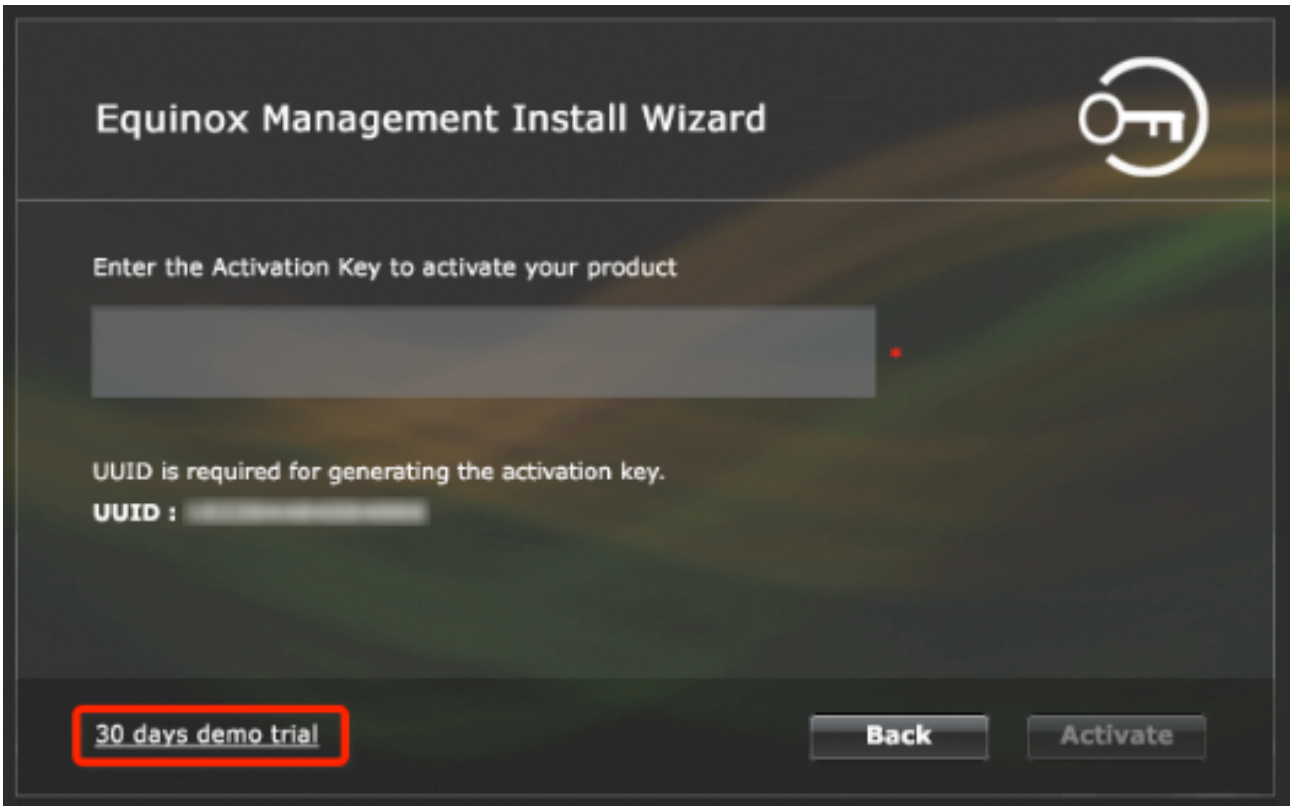


Figure 20: Equinox Management Installation Wizard — Activation Key

Version and license section

4. To use a 30 day demo version of the software without entering an activation key:
    a. Select **30 days demo trial**.

       The system displays the deployment types.



Figure 21: Equinox Management Install Wizard — Deployment Type

b. Select the Equinox Management deployment type to use.

c. If you select either the **Over the Top (OTT)** or **Team Engagement (TE)** options, the system displays the next page of the wizard.

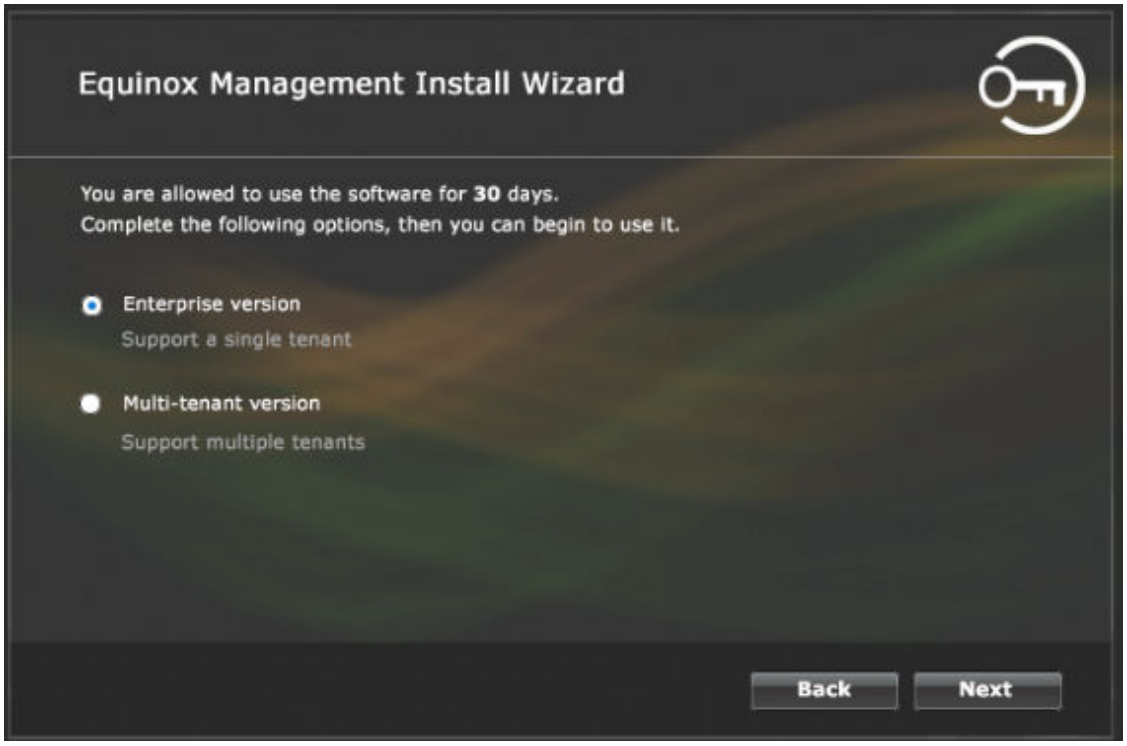


Figure 22: Equinox Management Install Wizard — Version

d. Select the Equinox Management version that you want to install, and select **Next**.

   The system displays the login page.

e. Enter login credentials in the fields. The default credentials are:

   - **Username**: admin
   - **Password**: admin

   The system displays the Equinox Management dashboard.

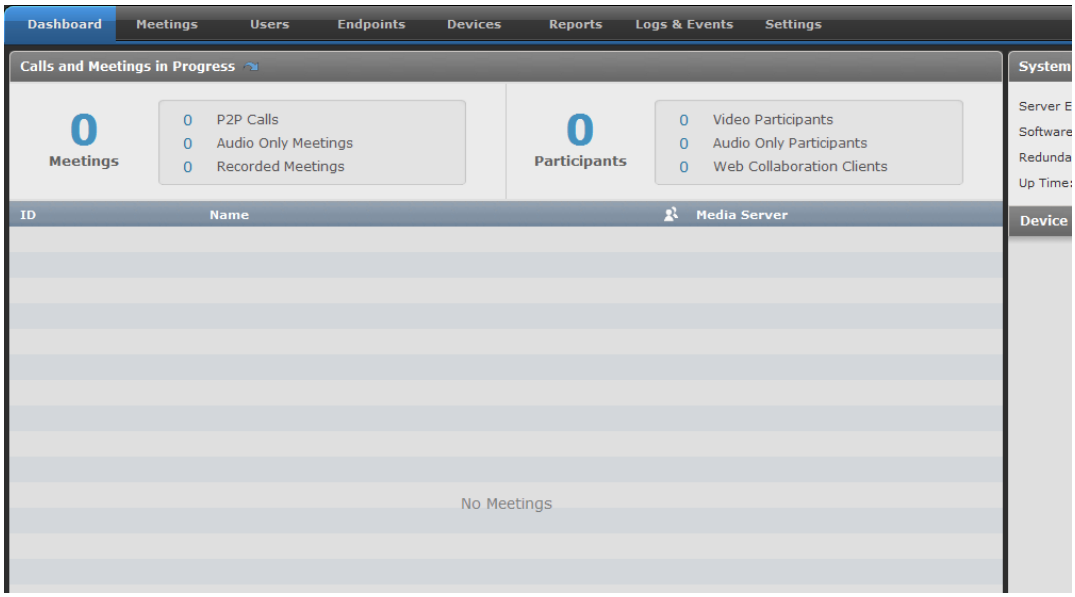


Figure 23: Equinox Management Dashboard

f. To view licensing information, select the Settings icon on the right side of the page and select **License Information**.

   The **License Status** field displays **30 days**.

5. To use a regular licensed version of the software:

   a. Retrieve the license key from PLDS, see Activating license entitlements in Avaya PLDS on page 418).

   b. Enter the activation key in the field on the second page of the install wizard, and select **Activate**.

      Note:

      If the virtual machine is corrupted, an earlier license cannot be used to restore from a backup server since the UUID changes with each new virtual machine.

      Equinox Management automatically determines whether you are configuring an Over-the-Top (OTT) or a Team Engagement (TE) solution, based on the license key you use.

   c. Wait approximately 3–5 minutes for the system to activate, at which time you are logged into Equinox Management automatically.

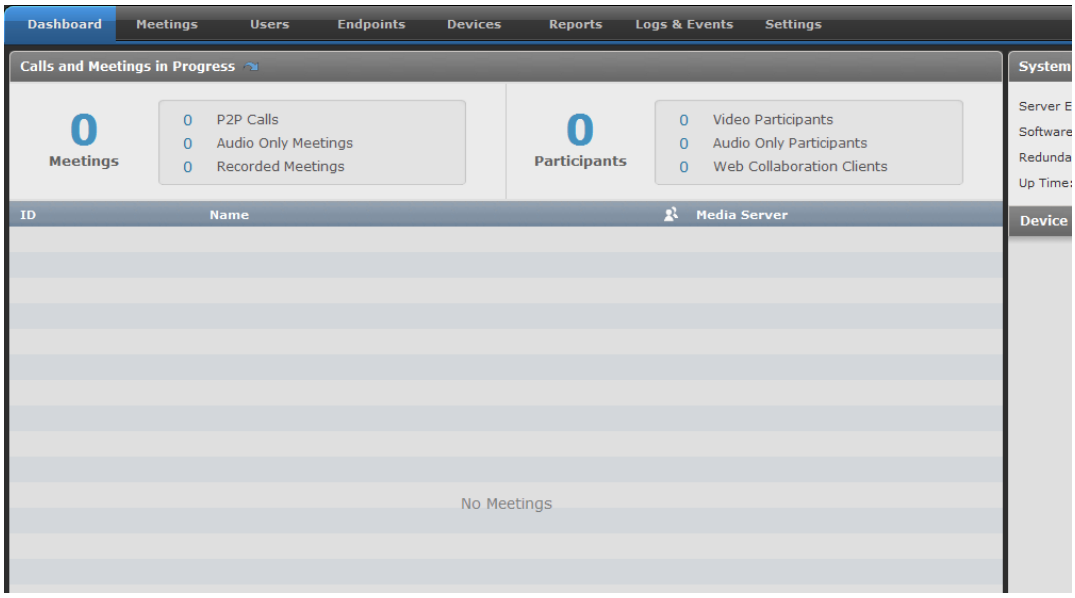


Figure 24: Equinox Management Entry Page (Dashboard)

d. To view licensing information, select the Settings icon on the right side of the page and select **License Information**.

   The **License Status** field displays **Permanent**.

Next steps

Configure the all-in-one Equinox Management server, as described in Configuring the All-In-One Equinox Management Server on page 88.

Configuring the All-In-One Equinox Management Server

About this task

The Equinox Management OVA supports the following working modes:

- **All-in-one**: Includes all of the components working in one VM, for medium capacity deployment.
- **Distributed**: For media or high capacity deployment, one management server works with either one or multiple distributed management servers, as follows:
  - One management server runs Equinox Management
  - The distributed management server works as either the H.323 Gatekeeper, the Equinox Conference Control, or the User Portal + Web Gateway

Procedure

1. Navigate to **Settings** > **System Preference** > **Local Services**.
2. Verify that the status of the **User Portal + Web Gateway** module is **Active**.

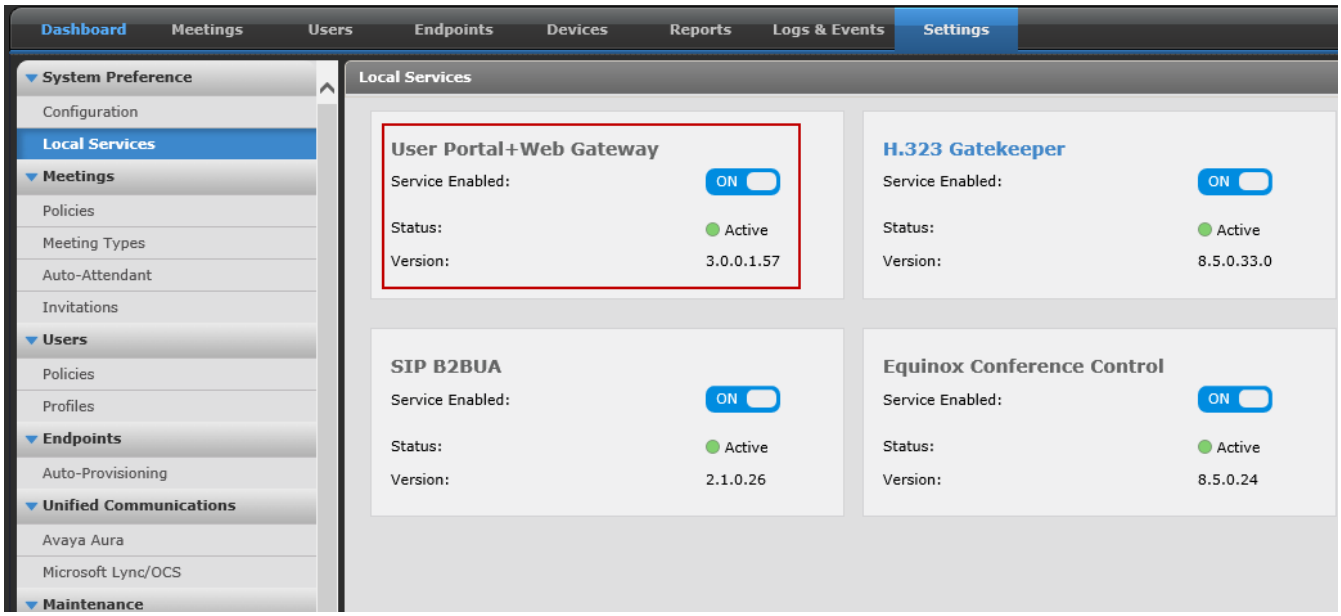


Figure 25: Local Services Page — User Portal + Web Gateway

Note:

If the User Portal + Web Gateway status is **Not Installing**, wait approximately five minutes for the status to change to **Installing**. The User Portal + Web Gateway installation takes approximately 15–20 minutes.

Important:

Do not restart the server during User Portal + Web Gateway installation; doing so will cause the installation to fail and require you to redeploy the OVA.

3. Navigate to the **Configuration** page (**Settings** > **System Preference** > **Configuration**). and verify that the **FQDN**, **DNS**, **Public URL Branch**, and **NTP** settings are correct.
4. Configure the fields on the page, as described in the following table.

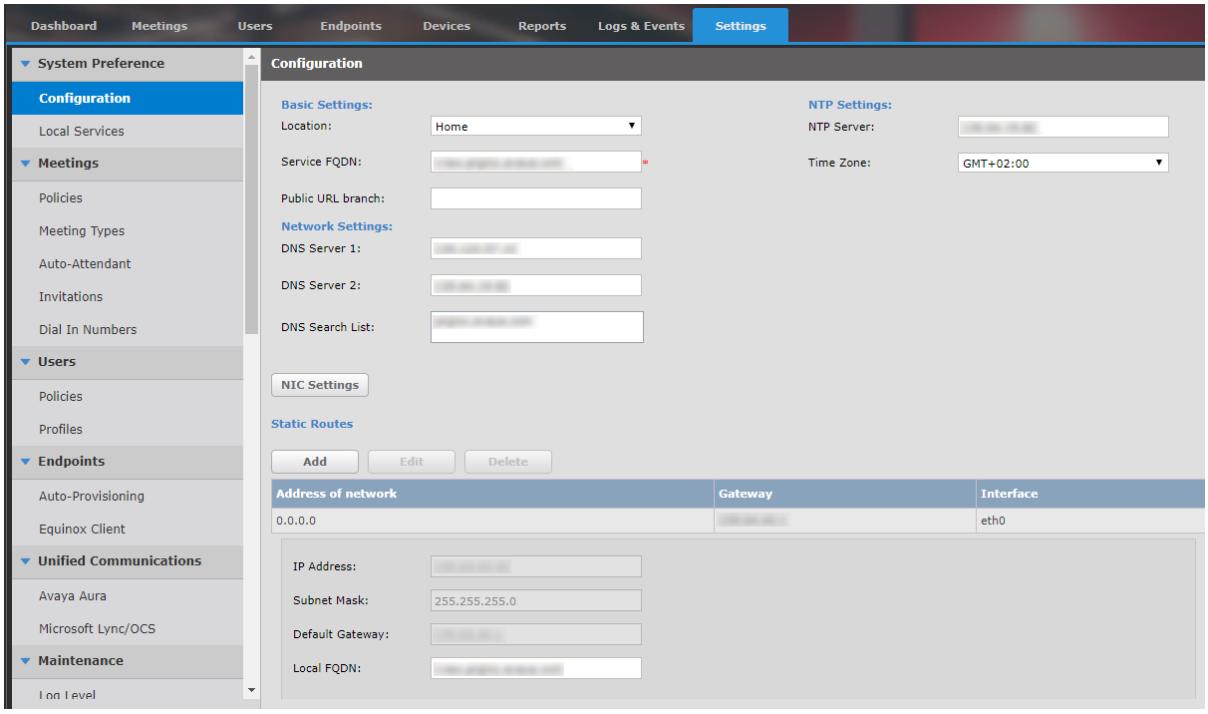


Figure 26: Configuration Tab

Table 10: Configuring your user portal

Section	Field Name	Description
	Location	This is relevant only for service providers or deployments with multiple locations. You can modify the user portal's location.
	Service FQDN	Enter the fully qualified domain name (FQDN) of the service.
	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

Table continues…

Section	Field Name	Description
	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.
Static Routes	**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

5. Select **Apply**.

Geographically Distributed Deployment of Equinox Management

When Equinox Management deployment is geographically distributed, servers are placed in multiple locations (data centers) to reduce media delays. Geographically distributed deployments do not require a virtual IP address; you must ensure that IP takeover is disabled on all servers.

The following components are deployed in each data center:

- Avaya Session Border Controller for Enterprise (ASBCE)
- Audio and Video Media Servers
- Media Server as a webRTC Gateway
- Media Server as a Web Conferencing Server
- 6K MCU

Equinox Management routes native and webRTC clients to the closest available data center relative to the client's location. When upgrading nodes, the initial node must be upgraded first; subsequent nodes can then be upgraded simultaneously.

You must also install the following components:

- Load balancer, which balances traffic between two or more Avaya Aura® Web Gateway nodes, which may be located in the same data center or in different data centers.
- Global Server Load Balancing (GSLB), which provides different routes and addresses based on the location of the client.

  The following table describes the GSLB requirements for Equinox Management:

Table 11: GSLB Requirements

Requirement	Description
Route requests based on the user's location	The GSLB can be part of the DNS server. Its route is based on the location of the browser initiating the request.
Support session affinity	Must be based on cookies. The reverse proxy uses a cookie for incoming HTTP requests, and subsequent requests with the same cookie are sent to the AAWG/ Portal server.
Support web sockets	Must permit web socket requests, and must relay the web socket connections between the client and the server. Configure the HTTP request timeout to the maximum duration of the conference, to ensure that the web socket session does not time out.
Support URL routing	Route requests to the relevant backend servers, based on the URL sending the request.
Support URL re-writing	Modify the request's URL path, based on rules to remove or rename portions of the path.
Support TLS v1.2 with the backend server	This is the only connection type that is supported.
Support indicated ciphers when communicating with backend server	A portion of the following ciphers must be supported: - ECDHE-RSA-AES128-GCM-SHA256 - ECDHE-ECDSA-AES128-GCM-SHA256 - ECDHE-ECDSA-AES256-GCM-SHA384 - ECDHE-RSA-AES128-SHA256 - ECDHE-ECDSA-AES128-SHA256 - ECDHE-RSA-AES128-SHA - ECDHE-ECDSA-AES128-SHA - AES128-GCM-SHA256 - AES256-GCM-SHA384 - AES128-SHA
User TCP health checks	Must verify the health check of the backend AAWG/Portal servers using TCP responses. You must be able to configure the TCP health check to work for half-opened connections, to prevent leaving multiple TCP sockets opened.
Use standard headers to communicate the FQDN used to reach the system by the original request	AAWG/Portal uses the host header to identify the FQDN used by the client to reach the system. This requirement is necessary only if the customer uses multiple FQDNs simultaneously to reach the Portal service. If only one FQDN is used globally, this requirement is not needed.
Relay client certificates	Necessary only when the customer needs clients to be authenticated by a client certificate.

Table continues…

Requirement	Description
Insert custom headers into the HTTP request	A simple configuration enabling inserting custom headers. **Note:** When incoming traffic is tagged at the AAWG/Portal system using different ports, this requirement is not needed.

You must disconnect the User Portal + Web Gateway internal load balancer before configuring the external one. For details, see Disabling the Internal Load Balancer in Equinox Management on page 99.

For additional details on geographically distributed deployment of Equinox Management, see the following sections:

Related links

Web Conference Signaling and Media in a Distributed Environment on page 93
Examples of Signaling and Media Paths for Clients on page 94
Equinox Management HTTPS Access for the UCCS Service on page 98

Web Conference Signaling and Media in a Distributed Environment

The Equinox Management server chooses a web conferencing server from the virtual room's location. If there is no web conferencing server in that location, a web conferencing server is chosen from the nearest location. Web conferencing servers are available through a reverse proxy. The web conferencing server URL resolves to the relevant reverse proxy that enables access to the specific Equinox Management server.

Web conferencing traffic travels through the internet for external clients until it reaches the SBC, where the route is configured to reach the specific web conferencing server. The web conferencing server is usually in the same data center as the SBC.

The following diagram displays the flow of web conferencing signaling in a distributed environment:

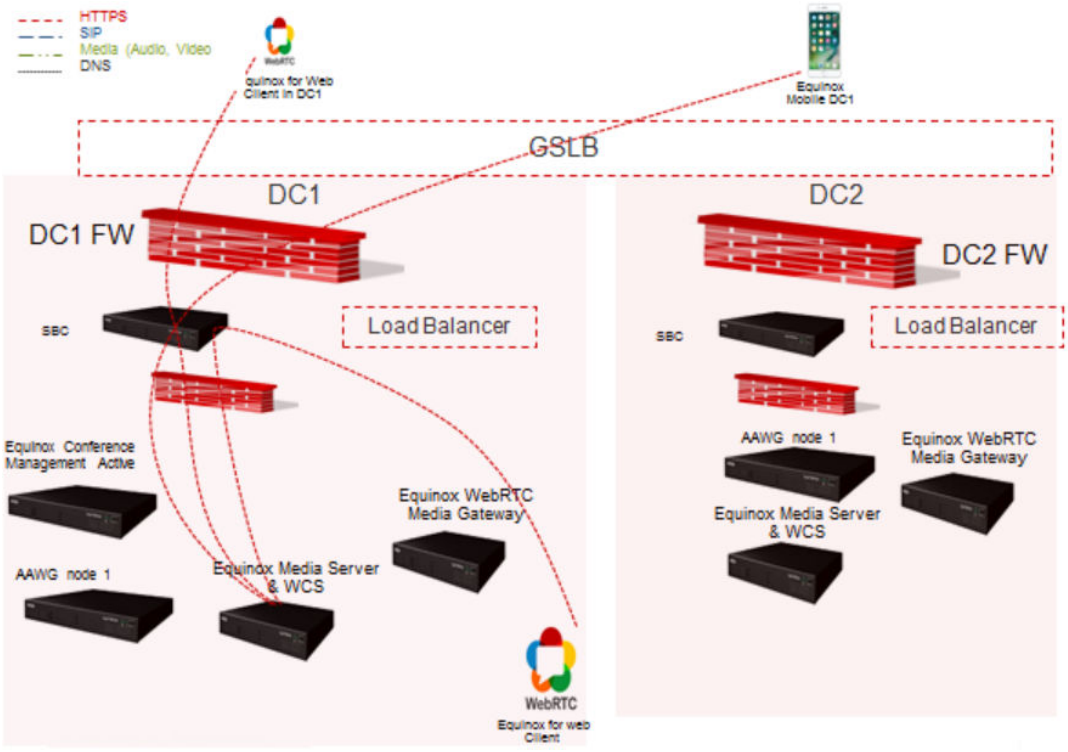


Figure 27: Web Conferencing Signaling in a Distributed Environment

Related links

Geographically Distributed Deployment of Equinox Management on page 91

Examples of Signaling and Media Paths for Clients

Configured users each have a location setup which indicates to which location the user belongs. Equinox Management allocates a virtual room to one of the MCUs in the user's location. For more information on virtual rooms, see *Managing Virtual Rooms* in the *Administrator Guide for Equinox Management*.

For details on Equinox Management deployment topology, see Component architecture on page 18.

The media path used depends on the location of the client or user, relative to the system's data centers. The media paths displayed in this section use the ASBCE as a reverse proxy; you can replace this component with your own reverse proxy, as needed.

Following are examples of clients' signaling and media paths in a geographically distributed system:

Signaling and media paths for an external client near DC1

When an external client near DC1 joins a virtual room belonging to a user in DC1, the following happens:

1. The FQDN resolves to the IP address of the load balancer in DC1.

2. HTTP requests are sent to the portal and join the meeting to the load balancers' IP in DC1.
3. Load balancers locate the AAWG in DC1.
4. AAWG allocates the SBC and AMS in DC1 for media routing.
5. AAWG sends a SIP call to AEMG.
6. Equinox Management allocates the MCU in DC1.

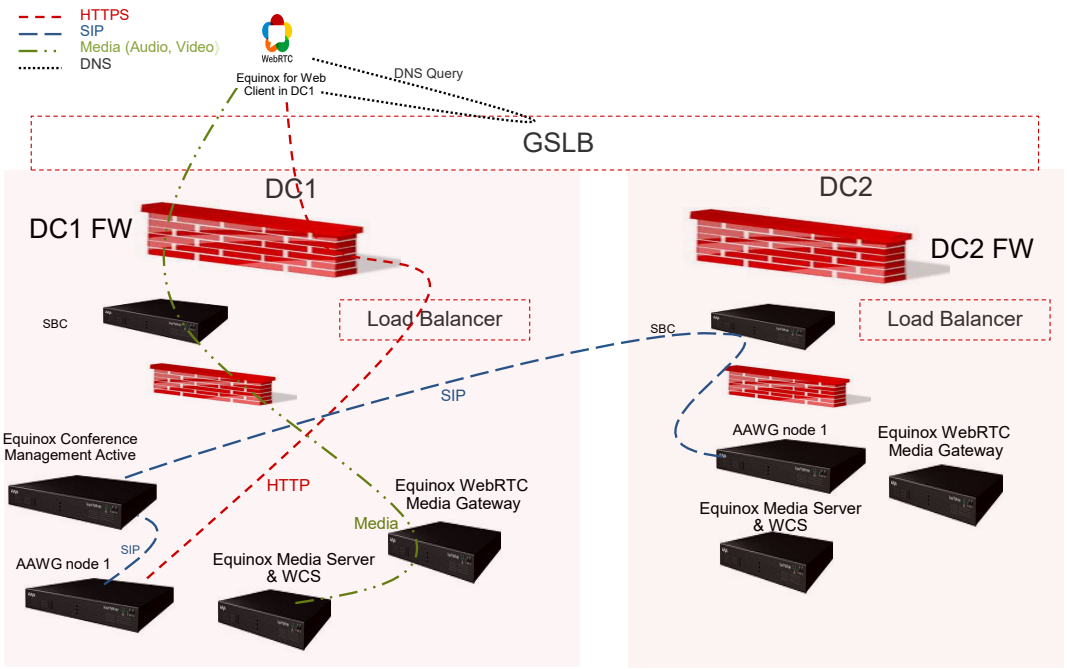


Figure 28: External Client Near Data Center 1

Signaling and media paths for an external client near DC2

When an external client near DC2 joins a virtual room belonging to a user in DC1, the following happens:

1. The client resolves the FQDN with GSLB. In this scenario, the FQDN resolves to the IP address of the load balancers in DC2.
2. The client sends all HTTP requests to the portal, and joins the meeting to the load balancer's IP in DC2.
3. Load balancers locate the AAWG in DC2.
4. AAWG in DC2 allocates the SBC and AMS in DC2 for media routing.
5. AAWG sends a SIP call to Equinox Management.
6. Equinox Management allocates the MCU in DC1.

   Media flows from the AMS in DC2 to the MCU in DC1.

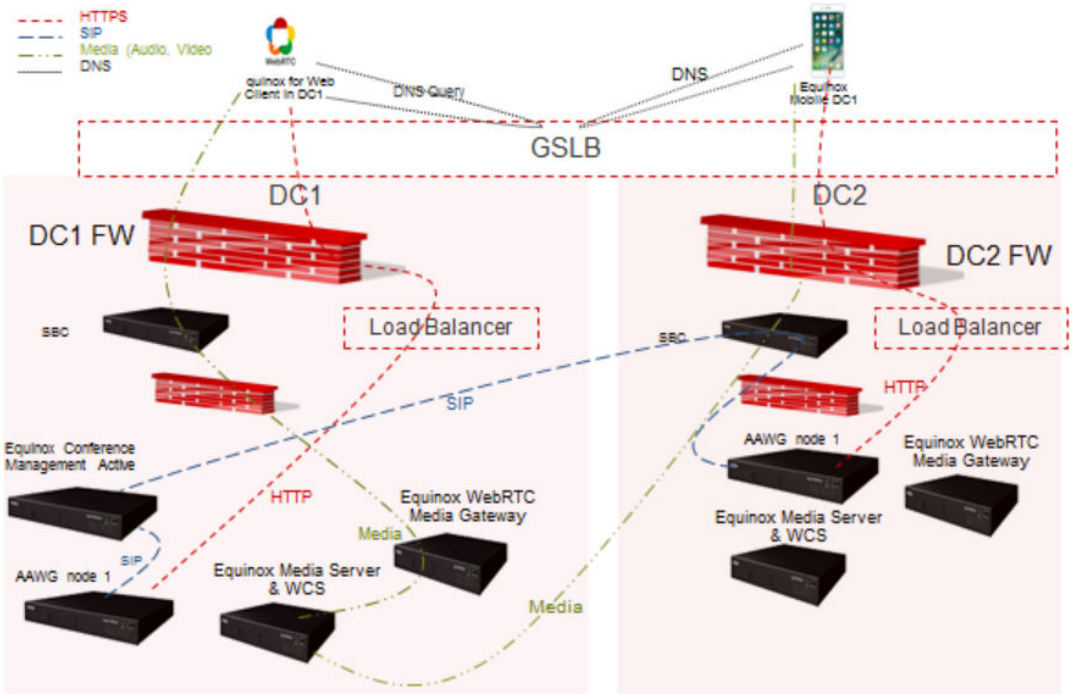


Figure 29: External Client Near Data Center 2

Internal client in DC1 joining a virtual room for a DC1 user

When an internal client in DC1 joins a virtual room belonging to a user in DC1, the following happens:

1. The client resolves the FQDN with the GSLB. In this scenario, the FQDN resolves to the IP address of the load balancers in DC1.
2. The client sends all HTTP requests to the portal, and joins the meeting to the load balancers' IP in DC1.
3. Load balancers locate the AAWG in DC1.
4. AAWG allocates the AMS in DC1 for media routing.

   Note:

   Turn candidates are not used or allocated for an internal client.
5. AAWG sends a SIP call to Equinox Management.
6. Equinox Management allocates the MCU in DC1.

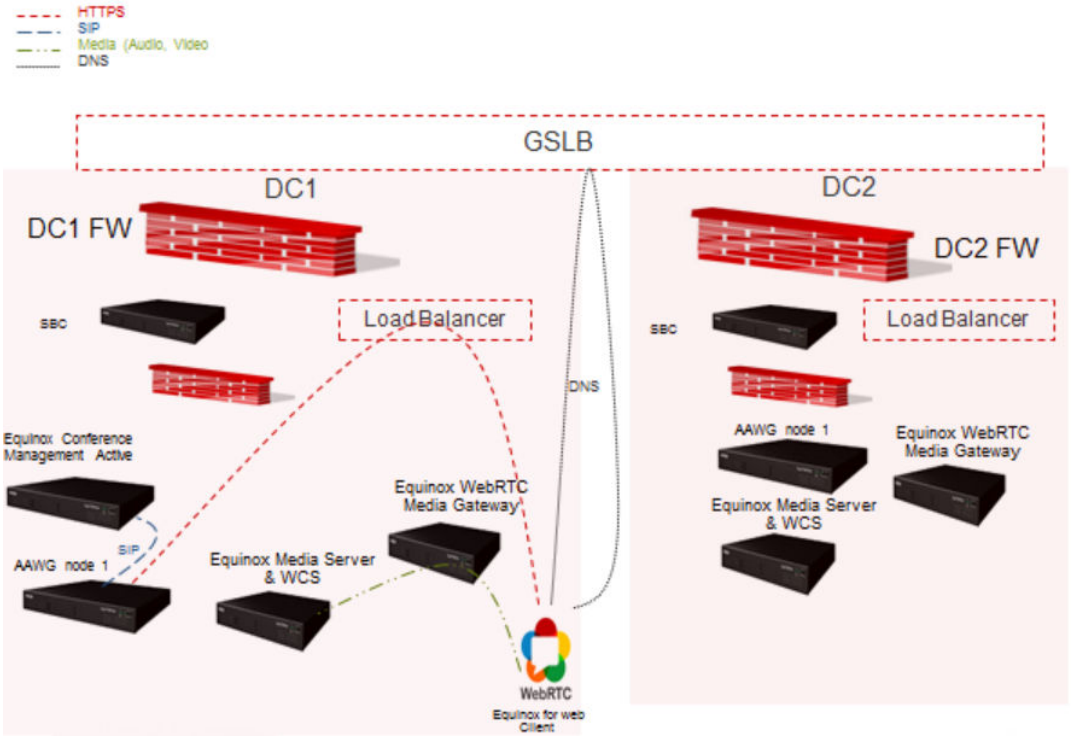


Figure 30: Internal Client in Data Center 1

Following is the overall diagram of the three users joining from different locations:

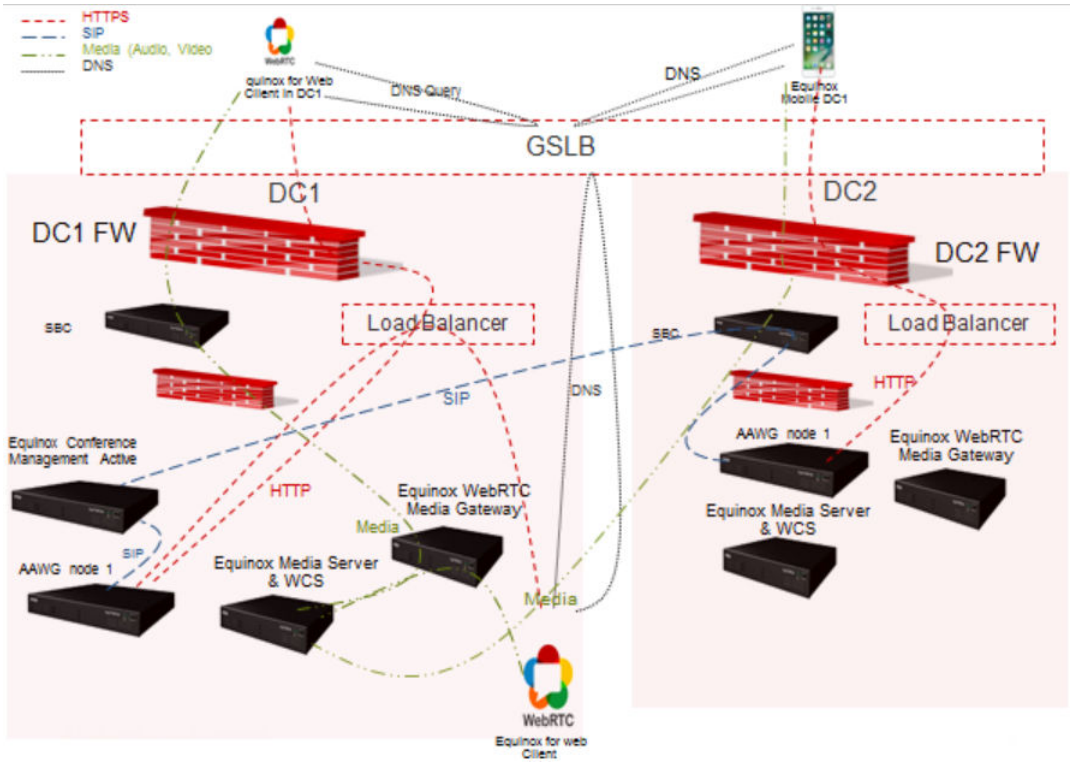


Figure 31: Overall Diagram — Three Users Joining

Related links

[Geographically Distributed Deployment of Equinox Management](#) on page 91

Equinox Management HTTPS Access for the UCCS Service

When a URL is sent to the UCCS service, it resolves to the Equinox Management servers' route. This FQDN resolves to the ASBCE in DC1, which forwards any HTTPS request to the Equinox Management Virtual IP address in DC1.

The diagram depicting this flow is as follows:

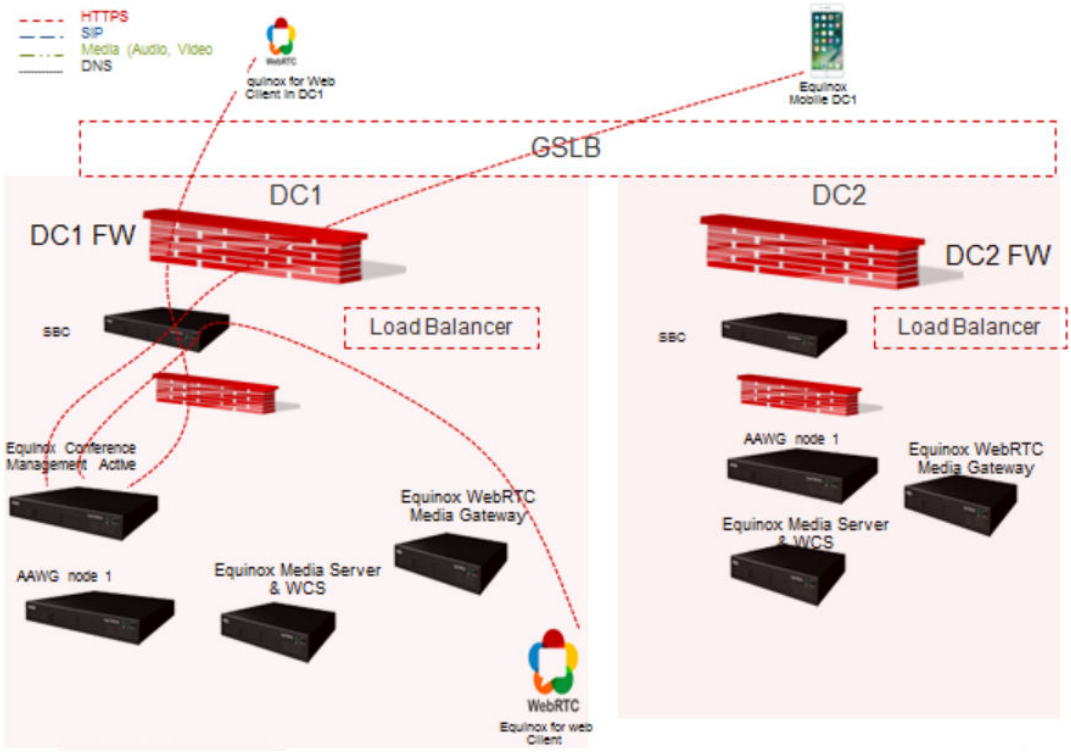


Figure 32: HTTPS Access for UCCS

Related links

Geographically Distributed Deployment of Equinox Management on page 91

Disabling the Internal Load Balancer in Equinox Management

About this task

The Equinox Management internal load balancer for the User Portal + Web Gateway works only with nodes in a single LAN. When working with multiple nodes simultaneously across different locations, you must disable the internal load balancer and install a third-party load balancer. Installing a third-party load balancer also requires you to specify a GSLB.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Settings** > **Devices** > **User Portal**.

   The **User Portal** page appears.

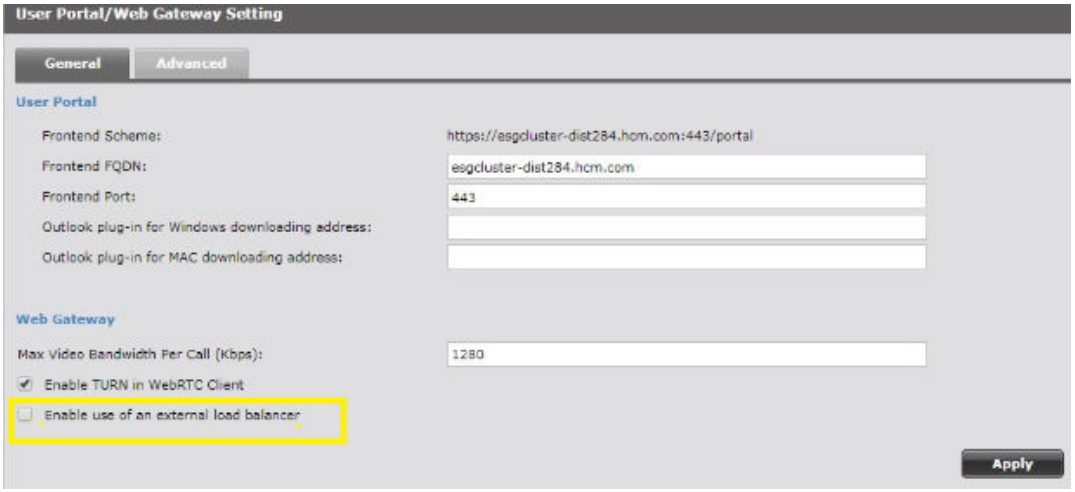


Figure 33: User Portal/Web Gateway Page

3. Select **Enable Use of an External Load Balancer**. By default, this setting is cleared.
4. Select **Apply**.

   The internal load balancer is disabled. The third-party load balancer must be configured by the customer.

Deploying a distributed or cluster User Portal and Web Gateway

About this task

You can deploy a single User Portal + Web Gateway in your environment. Once you deploy more than one User Portal + Web Gateway, they form a cluster. During cluster deployment, do not deploy a server until the previous server has finished deploying. However, when upgrading an existing Equinox Management deployment, you can upgrade non-seed nodes simultaneously after completing the seed node upgrade.

During cluster deployment of User Portal + Web Gateway, you configure multiple User Portal + Web Gateway servers in your environment. The servers work together to ensure that client requests are balanced between the servers, so that no single server is overloaded with requests.

Cluster deployment of User Portal + Web Gateway consists of a seed node (the first node you deploy, which is the master User Portal + Web Gateway) and non-seed nodes (subsequent nodes you deploy, which are subservient to the seed node). The procedure for deploying seed nodes and non-seed nodes is identical.

When deploying a User Portal + Web Gateway, the User Portal + Web Gateway must be able to communicate with the LDAP server through any firewalls that are in place.

Equinox Management automatically connects to the deployed nodes and installs the User Portal + Web Gateway with the required properties to form a cluster. Additionally, Equinox Management

passes the service Frontend FQDN to each cluster node. Each cluster node then looks up the associated IP to configure the required virtual IP.

Before you begin

Deploy the All-In-One Equinox Management, which is the seed node.

Ensure that the FQDNs (portal front-end FQDN, node local FQDNs) and IPs are defined on your network in DNS. The front-end FQDN must be bound to a virtual IP address. Node local FQDNs are bound to node physical IPs.

The portal front-end FQDN must not be resolved to the same IP as one of the node local FQDN.

Activate a license in PLDS if you will use a licensed deployment, see Activating license entitlements in Avaya PLDS on page 418.

Procedure

1. Access the Avaya Equinox® Management administrator portal.
2. Select **Settings** > **Local Services** and turn off the local User Portal + Web Gateway, if it is still active.
3. Select **Settings** > **Devices** > **User Portal/Web Gateway** > **General** and configure the **Frontend FQDN** and **Frontend Port**.

   These are the values used to access the User Portal + Web Gateway web page.
4. In the Equinox Management administrator portal, navigate to **Dashboard >** **> Advanced Parameters**.
5. In the **Property Name** field, enter `com.avaya.aawg.loadbalancer.virtualIPAddress`
6. In the **Property Value** field, enter the load balancer virtual IP address.

   By default the virtual IP address is taken from **Frontend FQDN**.
7. Select **Devices** > **User Portal & Recording** > **User Portals** and add the management User Portal + Web Gateway node.

   The **Add User Portal** page appears.

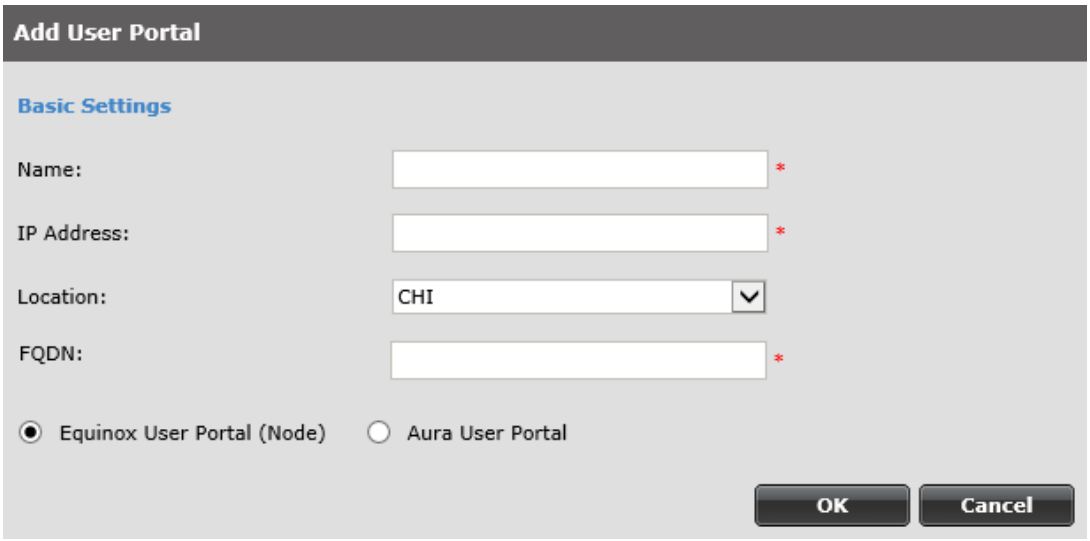


Figure 34: Add User Portal Page

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

Table 12: Add User Portal Fields

Field	Description
Name	The name of the User Portal.
IP Address	The IP Address of the User Portal.
Location	Select the location of the User Portal.
FQDN	Enter the service FQDN for the User Portal. When the **Aura User Portal** option is selected, this field does not appear.
Equinox User Portal (Node)	Select this setting for an OTT deployment.
Aura User Portal	Select this setting for a TE deployment.

Important:

Make sure to configure the cluster service FQDN in **Settings** > **Devices** > **User Portal/Web Gateway** > **User Portal** > **Frontend FQDN**. The values entered are not the same as the local service FQDN which you can find in **Settings** > **System Preference** > **Configuration** > **Service FQDN**.

The node that is being added is a utility node, not a management node. It must not have been used as an all-in-one Equinox Management and it does not have the application server license.

9. Retrieve the license key from PLDS, see Activating license entitlements in Avaya PLDS on page 418).
10. Select **OK**.

The configured User Portal appears on the **User Portals** page. Equinox Management starts connecting to the platform manager of the application server. After about 2 minutes, the User Portal icon turns yellow, which indicates a warning.

11. Select the User Portal and then the **Events** tab.

    A message is displayed, reminding you to add a license for that device.

12. Obtain the license:

    a. On the **Info** tab, copy the UUID.

    b. Retrieve the license key from PLDS, see Activating license entitlements in Avaya PLDS on page 418.

13. Copy and paste the license key for the management node in the relevant field in the **License** tab, and select **Apply** > **OK**.

    The system installs the User Portal + Web Gateway. Installation takes about 10 minutes.

14. When the installation completes, apply a third-party certificate for the node.

    Use the Front-end FQDN as the Common Name and Subject Alternative Name when creating the CSR. For information on installing the certificate, see Applying a Third-Party Certificate to the Distributed Equinox Management Server on page 117.

15. Once the certificate is installed, restart the User Portal + Web Gateway service.

16. After a few minutes, check the **Events** page of the distributed application server for possible alarms.

17. Select the User Portal **Configuration** page.

    a. Select **Secure Connection**, and then **Test Connection**.

    b. Select **OK** to let the User Portal work in secure mode.

       The icon next to the User Portal in the **User Portals** page lights green.

18. After the seed node is added successfully, add one or more User Portal + Web Gateways following the procedure above.

Note:

- You cannot add a non-seed node if the seed node status is not active. A seed node is active when its status icon is green, or yellow due to minor issues such as a resource limit related to VM reservation (Cores=8, CPU=0 MHz, RAM=0 MB).
- When working with a regional User Portal, you must utilize a third-party load balancer to determine the correct User Portal to land on, as the internal load balancer picks a User Portal randomly. For details on deleting an internal load balancer and creating a third-party load balancer, see Disabling the Internal Load Balancer in Equinox Management on page 99.

Deploying a Standalone Distributed H.323 Gatekeeper

About this task

In a deployment where there is a large amount of H.323 calls, you must deploy an Avaya Equinox® Management node that serves as a distributed H.323 Gatekeeper to handle these calls.

You need to deploy the low capacity Equinox Management node.

The node is a utility node, not a management node. You must not have deployed it as an all-in-one Equinox Management.

Note:

If you want to delete a previously installed H.323 Gatekeeper node and then redeploy the same node, you must first remove/delete the VM and then reinstall it.

Before you begin

Deploy the All-In-One Equinox Management as the seed node. See Deploying the Equinox Management Server on page 67.

Procedure

1. Deploy the low-capacity Equinox Management node. See Deploying the Equinox Management Server on page 67.
2. Access the Equinox Management administrator portal.
3. To add the gatekeeper:
   a. Select **Devices** > **Devices by Type** > **H.323 Gatekeepers**.
   b. Select **Add**.

      Equinox Management displays the **Add H.323 Gatekeepers** page.

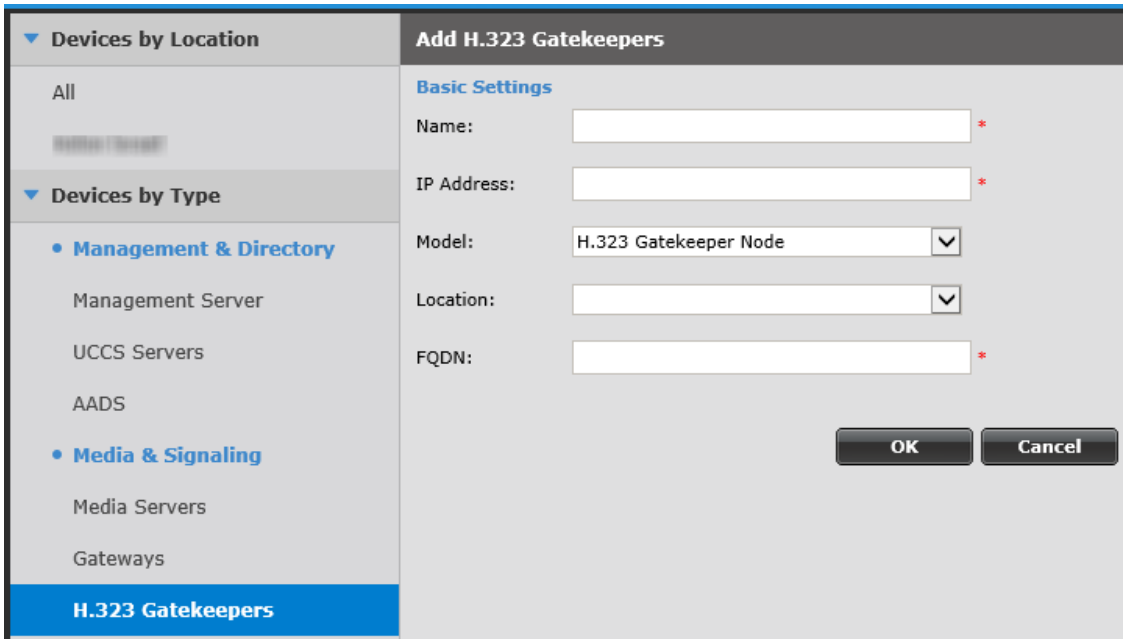


Figure 35: Add H.323 Gatekeepers page

c. Configure the fields on the page as described in the following table.

Table 13: Configuring H.323 Gatekeeper

Field	Description
Name	The H.323 Gatekeeper name in the deployment.
IP Address	The H.323 Gatekeeper IP Address.
Model	Select the H.323 Gatekeeper node from the dropdown list.
Location	Select the location of the H.323 Gatekeeper from the dropdown list.
FQDN	Enter the H.323 Gatekeeper FQDN.

d. Select **OK**.

The **H.323 Gatekeepers** page displays the new gatekeeper.

Equinox Management starts connecting to the gatekeeper's platform manager.

4. Select the gatekeeper's **Configuration** tab.

The **Configuration** page displays pre-configured fields that Equinox Management retrieves from **Settings** > **System Preference** > **Configuration**.

a. (Optional) Change the **Time Zone**.

b. In the **Service FQDN** field, enter the same address as in **Local FQDN** under the **Address of network** section.

5. Obtain the license:
   a. On the **Info** page, copy the UUID.
   b. Retrieve the license key from PLDS, see Activating license entitlements in Avaya PLDS on page 418.
6. Add the license key:
   a. On the **Licensing** page, paste the license key for the gatekeeper's node.
   b. Select **Apply** > **OK**.

   The license key installation takes about 10 minutes.
7. Install the certificate.
   - If Equinox Management uses a third-party certificate, you need to apply for a certificate with the same certificate authority as the one used by Equinox Management.

     If Equinox Management uses a certificate it has created, the gatekeeper uses that certificate and you do not need to install any certificate.
   - To install the certificate, see Applying a Third-Party Certificate to the Distributed Equinox Management Server on page 117.
   - When creating the CSR, use the Service FQDN for the Common Name and Subject Alternative Name.
   - After Equinox Management installs the certificate, restart the gatekeeper.
8. Check the gatekeeper's **Logs & Events** page for possible alarms.
9. Verify that the server is online and shows the correct version.
10. Secure the connection with Equinox Management:
    a. On the gatekeeper's **Configuration** page, select **Secure Connection**.
    b. Select **Test Connection**.
    c. Select **OK**.
    d. On the **H.323 Gatekeepers** page, verify that the icon next to the gatekeeper node lights green.
11. To deploy additional gatekeepers, follow the above procedure.

Deploying Distributed H.323 Gatekeepers in Alternate Mode

About this task

To implement the high availability option in H.323 Gatekeeper, use the Alternate Gatekeeper feature that is based on the deployment of identical H.323 Gatekeepers. One gatekeeper assumes the role of the primary gatekeeper and the other has the role of the secondary or

alternate gatekeeper. When the primary gatekeeper goes offline, the secondary gatekeeper becomes the primary one. These roles remain unchanged until the new primary gatekeeper goes offline.

When the primary gatekeeper goes offline, the management of calls in progress passes to the endpoints participating in the call. High availability makes gatekeeper failures transparent to the endpoints that are registered to it. Each online gatekeeper can have its own alternate gatekeeper that copies and uploads the registration table of the primary table of the primary gatekeeper. If the gatekeeper goes offline, the alternate version replaces its services within ten seconds of downtime.

Before you begin

- Deploy two distributed H.323 Gatekeeper nodes. See Deploying a Standalone Distributed H.323 Gatekeeper on page 104.
- Make sure that the IP addresses of the first node, second node, and Virtual IP have the same subnet mask.

  The first node is the primary gatekeeper. The second node is the secondary gatekeeper.

  For example:

  - First node: IP: *10.123.4.56*; FQDN: *ecs-gk56.abc.com*
  - Second node: IP: *10.123.4.57*; FQDN: *ecs-gk57.abc.com*
  - Public IP of the cluster formed by both nodes: *10.123.4.58*; FQDN: *ecs-gkvirtual58.abc.com*

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Devices** > **Devices by Type** > **H.323 Gatekeepers**
3. Select the first node. For example: *10.123.4.56*

   Equinox Management displays the gatekeeper **Info** page.
4. Select **Advanced Configuration** > **Alternate Gatekeeper Setup**.

   Equinox Management displays the **Alternate Gatekeeper Setup** page.
5. Configure the alternate gatekeeper:
   a. Configure the fields as described in the following table.

      Table 14: Configuring the alternate gatekeeper

Field	Description
Alternate Gatekeeper	The secondary gatekeeper's IP Address. For example: *10.123.4.57*
Public IP Address	The virtual IP address of the cluster formed by the primary and alternate gatekeeper. For example: *10.123.4.58*

   b. Select **OK**.

      Equinox Management displays the following message:

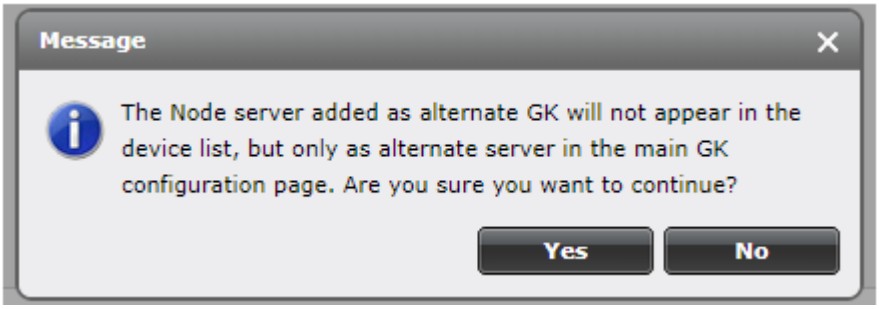


Figure 36: Alternate gatekeeper alert message

c. Select **Yes**.

After a few minutes, Equinox Management displays a working alternate mode setup.

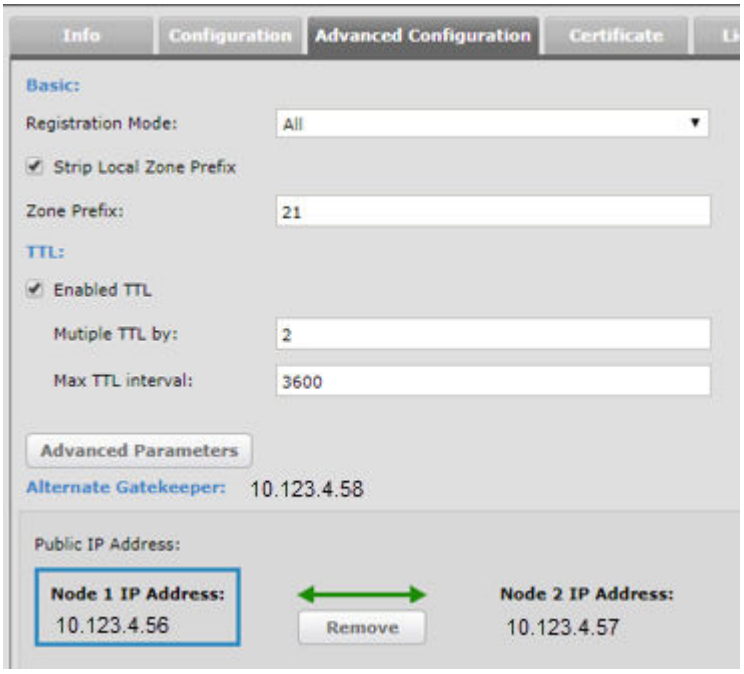


Figure 37: Alternate gatekeeper mode setup

6. Select the **Configuration** tab.

   The Configuration page displays the pre-configured **Name** and **Service FQDN** of the primary gatekeeper.

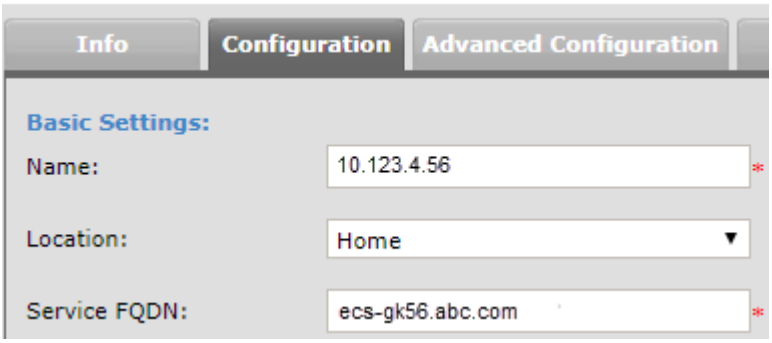


Figure 38: Alternate gatekeeper configuration

a. Replace the **Name** value. For example: *gkvirtual*

b. Replace the **Service FQDN** value with the FQDN of the Public IP Address. For example: *ecs-gkvirtual58.abc.com*

c. Select **Apply**.

d. On the dialog box message, select **Yes** to restart Equinox Management.

Deploying a Distributed UCCS Server

About this task

In a deployment where there is a large amount of calls, you must deploy a low capacity Avaya Equinox® Management node that serves as a distributed UCCS to enhance the concurrent call capacity.

The node is a utility node, not a management node. You must not have deployed it as an all-in-one Equinox Management.

The UCCS server is also called Equinox Conference Control.

Before you begin

Deploy the All-In-One Equinox Management as the seed node. See Deploying the Equinox Management Server on page 67.

Procedure

1. Deploy the low-capacity Equinox Management node. See Deploying the Equinox Management Server on page 67.
2. Access the Equinox Management administrator portal.
3. To add UCCS:
   a. Select **Devices** > **Devices by Type** > **UCCS Servers**.
   b. Select **Add**.

      Equinox Management displays the **Add UCCS** page.

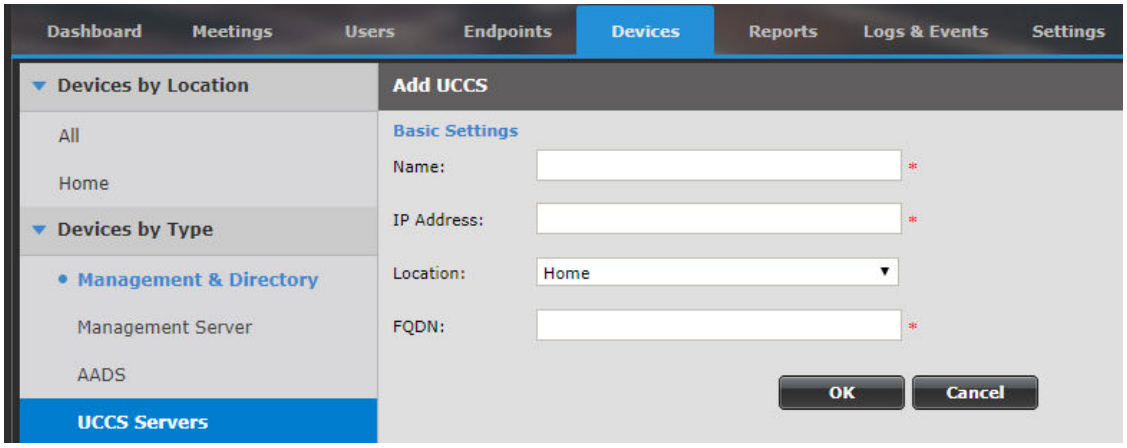


Figure 39: Add UCCS page

c. Configure the fields on the page as described in the following table.

Table 15: Configuring UCCS

Field	Description
Name	The UCCS name in the deployment.
IP Address	The UCCS IP Address.
Location	Select the UCCS location from the dropdown list.
FQDN	Enter the UCCS FQDN.

d. Select **OK**.

The **UCCS** page displays the new server.

4. (Optional) To change the time zone, navigate to the UCCS **Configuration** page. It displays field values that Equinox Management has automatically configured for the newly added UCCS.
5. Obtain the license:
   a. On the **Info** page, copy the UUID.
   b. Using UUID, retrieve the license key from PLDS. See Activating license entitlements in Avaya PLDS on page 418.
6. Add the license key:
   a. On the **Licensing** page, paste the license key for the UCCS node.
   b. Select **Apply** > **OK**.

   Equinox Management installs the UCCS license key.
7. Install the certificate.
   - If Equinox Management uses a third-party certificate, you need to apply for a certificate with the same certificate authority as the one used by Equinox Management.

If Equinox Management uses a certificate it has created, UCCS uses that certificate and you do not need to install any certificate.

- To install the certificate, see Applying a Third-Party Certificate to the Distributed Equinox Management Server on page 117.
- When creating the CSR, use the Service FQDN for the Common Name and Subject Alternative Name.
- After Equinox Management installs the certificate, restart UCCS.

8. Check the UCCS **Alarms** page for possible events.
9. Verify that UCCS is online and shows the correct version.
10. Secure the connection with Equinox Management:
    a. On the UCCS **Configuration** page, select **Secure Connection.**
    b. Select **Test Connection**.
    c. Select **OK** .
    d. On the **UCCS** page, verify that the icon next to the UCCS node lights green.
11. To deploy additional UCCS servers, follow the above procedure.

Securing Connections With Equinox Management

This section describes the procedures that invoke certificates when working with Equinox Management.

By default, Equinox Management applies a self-signed certificate for itself, other media servers, and application servers. For enhanced security, you can choose to replace the self-signed certificate with a third-party certificate.

The required procedure for installing a third-party certificate is determined by the type of environment in which you are working, either all-in-one or distributed.

When deploying Avaya Equinox in a Team Engagement (TE) environment, you can use multiple CAs as long as all components trust all CAs involved in signing the identity certificates.

Related links

Applying a Third-Party Certificate to the All-in-One Equinox Management Server on page 112
Applying a Third-Party Certificate to the Distributed Equinox Management Server on page 117
Installing the CA Certificate for Avaya Equinox® Meetings for Web on page 120
Renewing the CA Certificate for H.323 Gatekeepers in Alternate Mode on page 122

Applying a Third-Party Certificate to the All-in-One Equinox Management Server

About this task

You must generate a signed certificate to ensure a secure connection between Equinox Management and other components of your deployment.

The Equinox Management server currently supports a bulit-in, self-generated certificate. For added security when setting the management server to work in TLS mode, it is recommended that you delete the existing certificate and upload a third-party certificate.

Before you begin

Ensure that you have successfully configured the all-in-one management server, as described in Configuring the All-In-One Equinox Management Server on page 88.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Settings** > **Security** > **Certificates**.

   The **Certificates** page opens.

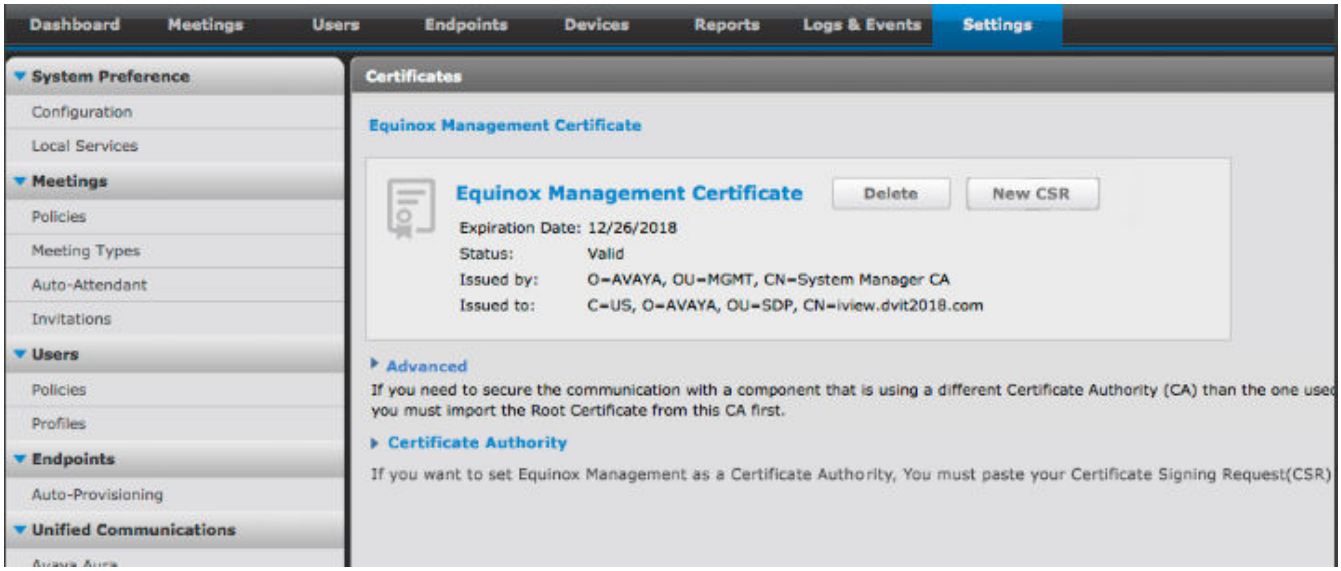


Figure 40: Certificates Page

3. Select the **New CSR** button to create a new CSR.

   The **Generate CSR** dialog box opens.

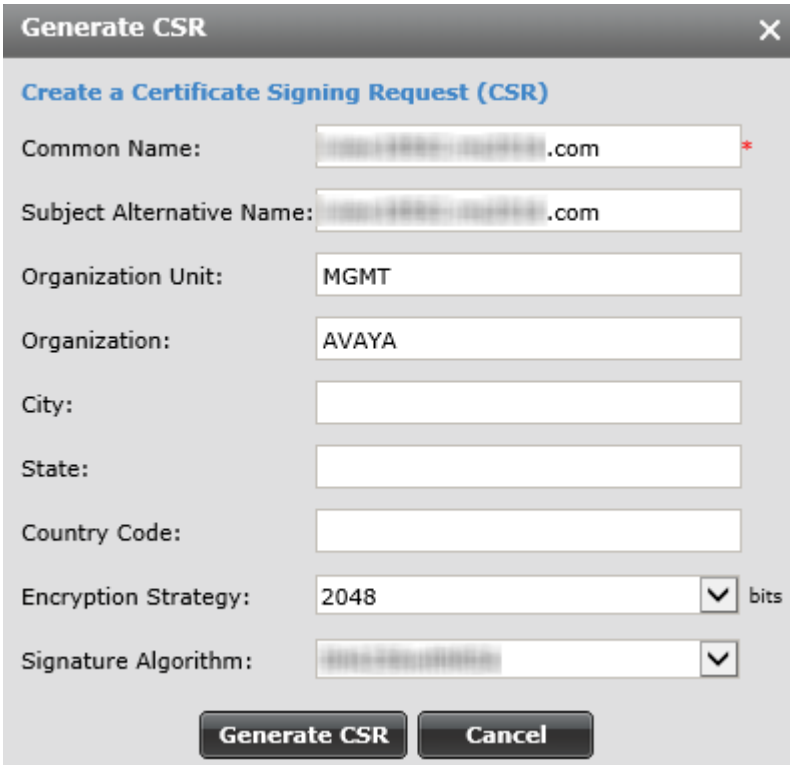


Figure 41: Generate CSR Dialog Box

Note:

Ensure that the **Common Name** value is the Server FQDN or Public FQDN, and that the FQDN can be resolved on your DNS.

4. 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.
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. Multiple SAN entries must be separated by a comma.
Organization	The name of the organization.
Organization Unit	The unit to which the organization belongs.
City	The city in which the organization is located.

Table continues…

Field	Description
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.

5. Select **Generate CSR**. A green check mark appears next to **Step 1**, and the **Save** button is enabled.

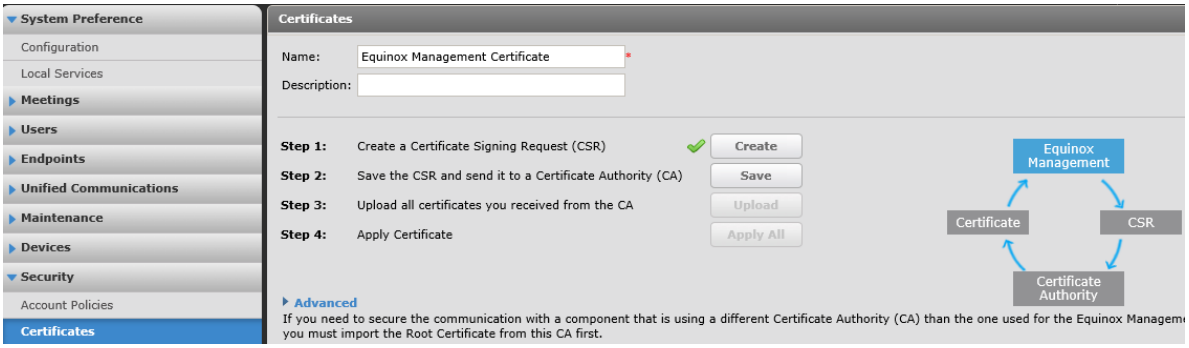


Figure 42: Certificates Page — Generated Certificate Indicator

6. Select **Save** to save the CSR. A green check mark appears next to **Step 2**, and the **Upload** button is enabled.
7. Send the CSR to the Certificate Authority (CA) for signing.

   Do not proceed to the next step until you receive the signed certificate back from the CA.
8. Select **Upload** to upload the certificate to Equinox Management. Ensure that you upload the CA root certificate (**Root.cer**), the all-in-one certificate (**allinone.cer**) and any intermediate CA certificates as well that were used in the signing process to have the full chain.

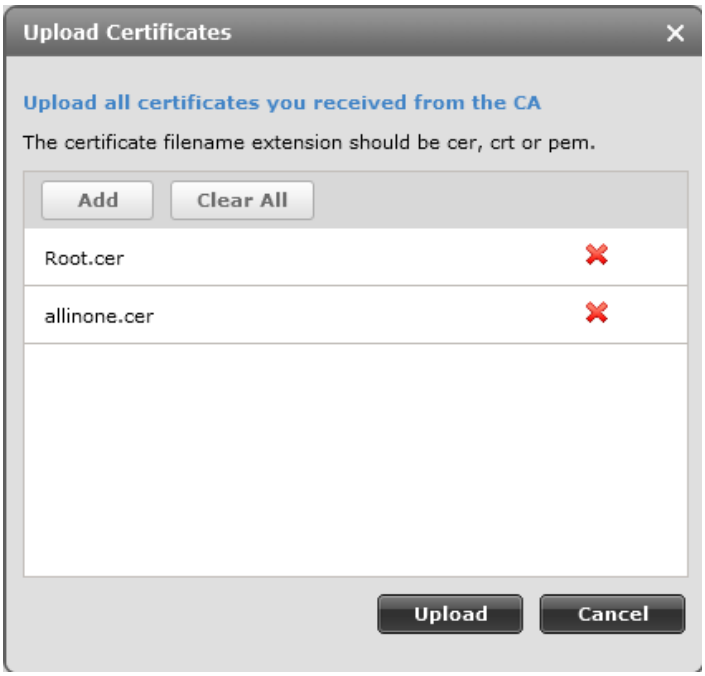


Figure 43: Upload Certificates Dialog Box

9. Click **Yes** to upload the certificate and overwrite the old one.
10. Select **Apply All** to apply the certificate. A dialog box appears, prompting you to restart the server.

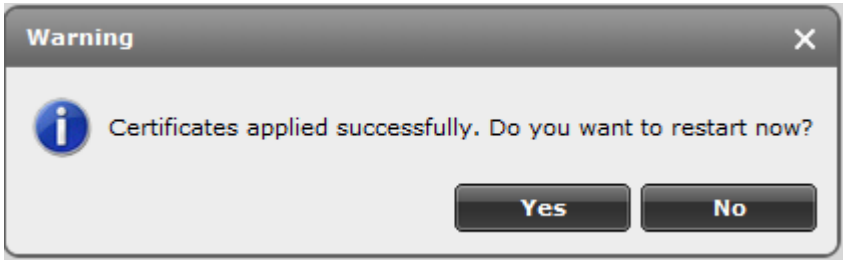


Figure 44: Restart Dialog Box

11. Select **Yes**. The server restarts after 3–5 minutes.
12. Navigate to **Settings** > **System Preference** > **Local Services**.

    On the **Local Services** page, verify that the User Portal + Web Gateway status is **Active**.

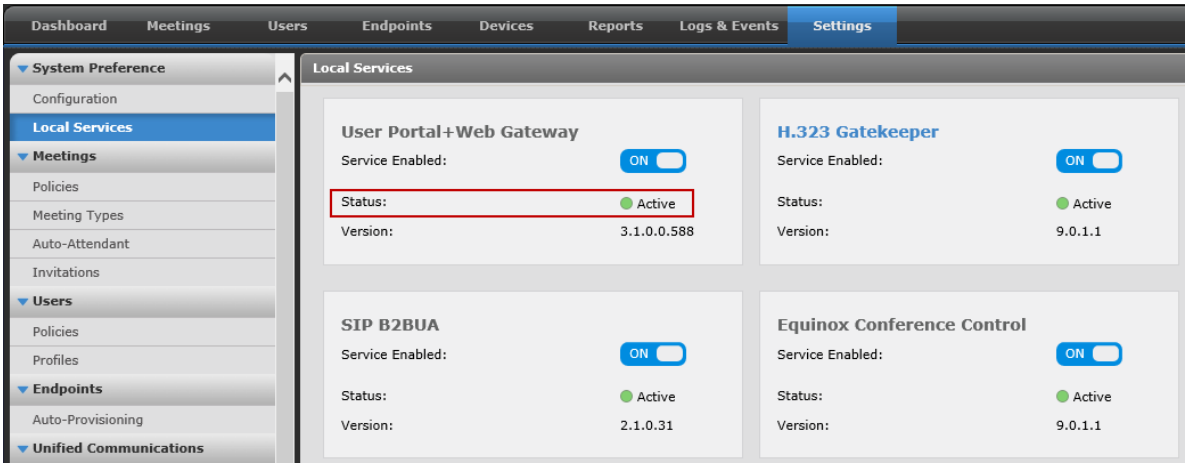


Figure 45: Local Services Page — User Portal + Web Gateway Status

Related links

Securing Connections With Equinox Management on page 111
Configuring Equinox Management as a Certificate Authority on page 116

Configuring Equinox Management as a Certificate Authority

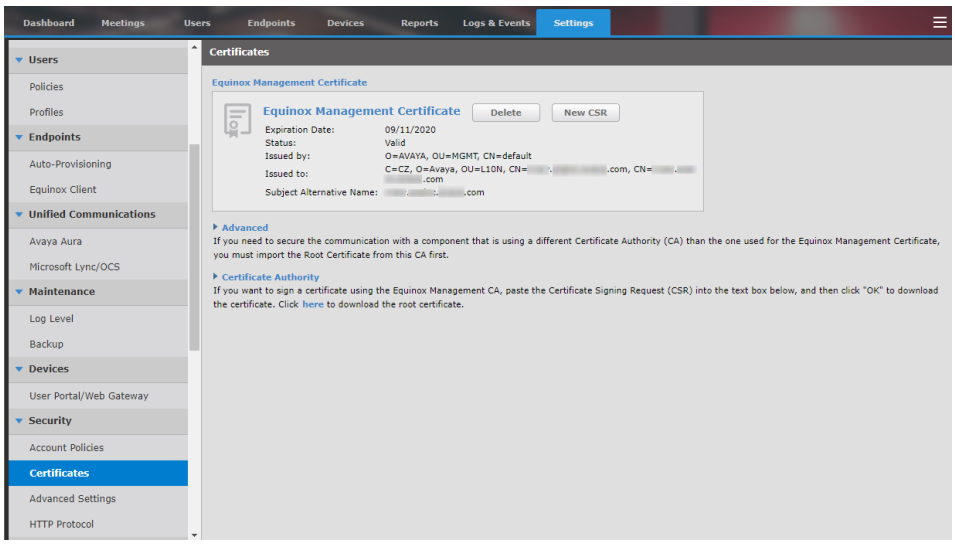
About this task

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 46: Certificate Authority Section

4. Paste the CSR into the text box, and click **OK** to download the certificate.

Related links

Applying a Third-Party Certificate to the All-in-One Equinox Management Server on page 112

Applying a Third-Party Certificate to the Distributed Equinox Management Server

About this task

For added security when setting the management server to work in TLS mode, it is recommended that you delete the existing certificate and upload a third-party certificate.

Before you begin

Ensure that you have set up the distributed Equinox Management server as described in Deploying a distributed or cluster User Portal and Web Gateway on page 100.

Procedure

1. Navigate to **Settings** > **Security** > **Certificates**.

   The **Certificates** page appears.

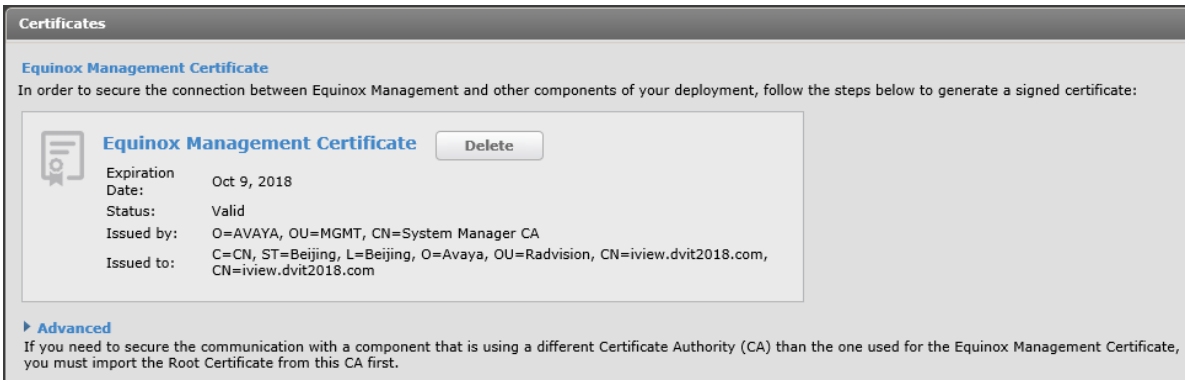


Figure 47: Certificates Page

2. Select **Delete** and then select **Yes** in the confirmation dialog box to delete the existing Equinox Management certificate.

   The **Certificates** page refreshes.

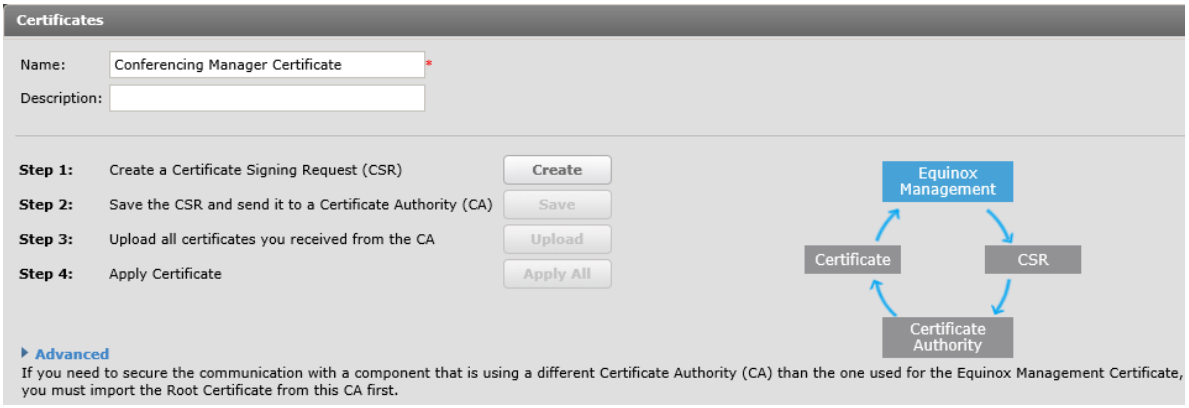


Figure 48: Certificates Page

3. Select the **Create** button to create a Certificate Signing Request (CSR) for the management server.

   The **Generate CSR** dialog box opens.

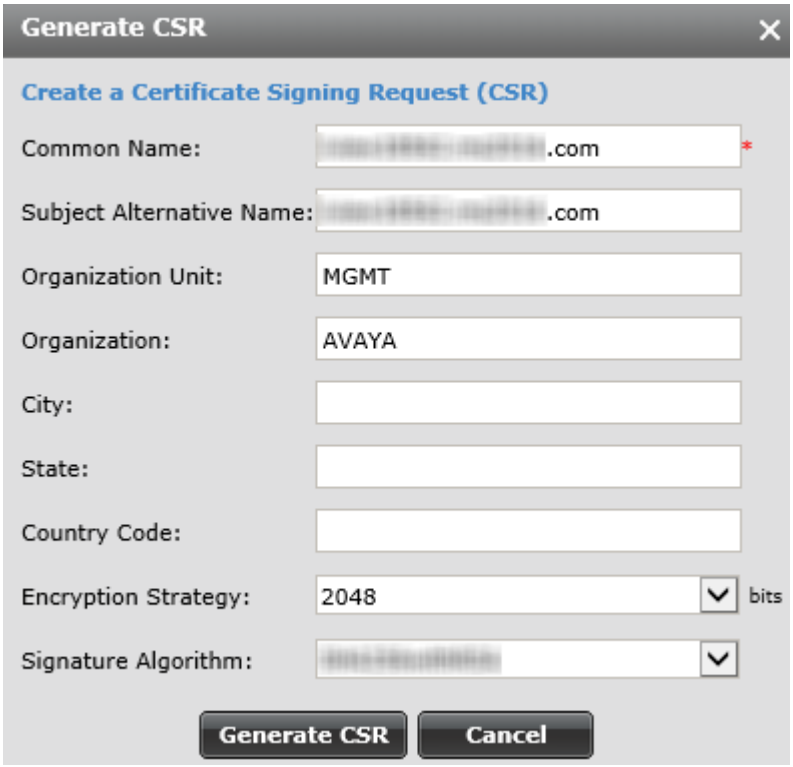


Figure 49: Generate CSR Dialog Box

4. Configure the relevant fields to create a CSR. Ensure that the **Common Name** field value is the server FQDN, resolvable on your DNS. When using redundancy mode, use the public FQDN instead of the server FQDN.

   Select **Generate CSR**.

5. On the **Certificates** page, select **Save** to save the generated CSR.
6. Send the CSR to the Certificate Authority (CA) for signing.

   Do not proceed to the next step until you receive the signed certificate back from the CA.

7. Select **Upload** to upload the certificate to Equinox Management. Ensure that you upload the CA root certificate (**Root.cer**), the all-in-one certificate (**allinone.cer**) and any intermediate CA certificates as well that were used in the signing process to have the full chain.

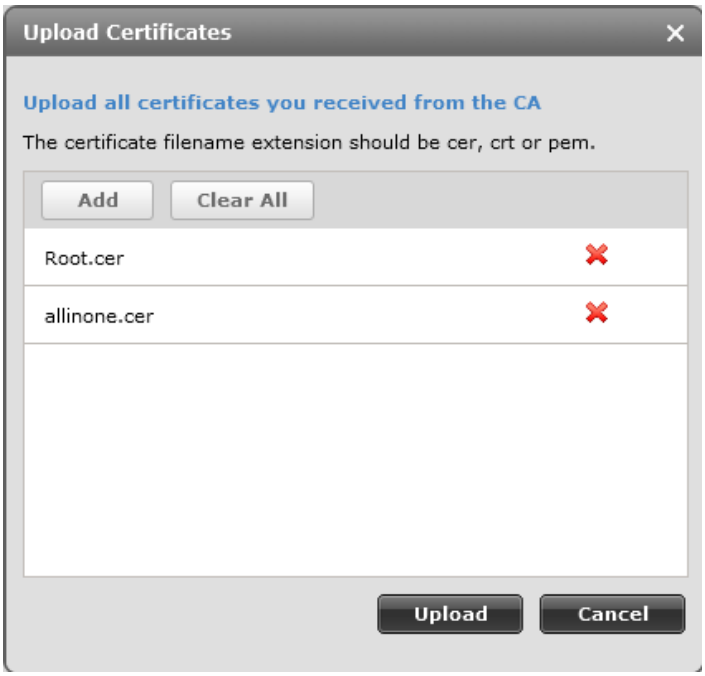


Figure 50: Upload Certificates Dialog Box

8. Select **Upload**.
9. Select **Apply All** to apply the certificate. The resulting dialog box prompts you to restart your machine.

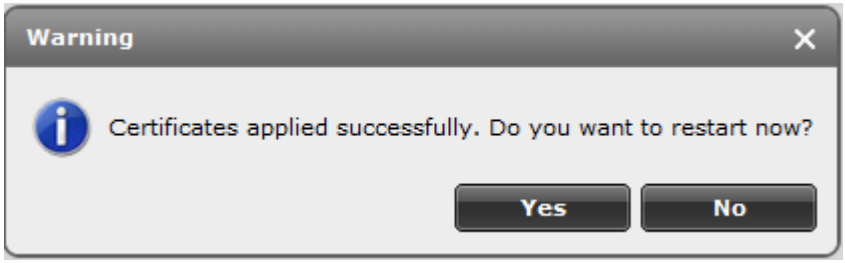


Figure 51: Restart Dialog Box

10. Select **Yes**. The server restarts after 3–5 minutes.

Related links

Securing Connections With Equinox Management on page 111

Installing the CA Certificate for Avaya Equinox® Meetings for Web

About this task

This task describes the procedure for configurations that must be done on the user's local PC during virtual deployment of Equinox Management. This task covers Chrome and Firefox procedures. If you used the Avaya System Manager to sign the certificate created during configuration of the all-in-one Equinox Management server deployment (see Applying a Third-Party Certificate to the All-in-One Equinox Management Server on page 112) or if you used the internally signed certificate and the client PC uses Chrome, the client must install the root certificate as a trusted root CA.

Before you begin

- Ensure that you have successfully deployed the Equinox Management server (Deployment of Equinox Management for OTT solution — Overview on page 61), and that you have configured the all-in-one management server for the new portal (Configuring the All-In-One Equinox Management Server on page 88).
- Ensure that your client PC can resolve the all-in-one management server FQDN.

Procedure

1. Access the Equinox Management administrator portal.
2. Navigate to **Settings** > **Security** > **Certificates**.

   The system displays the **Certificates** page.

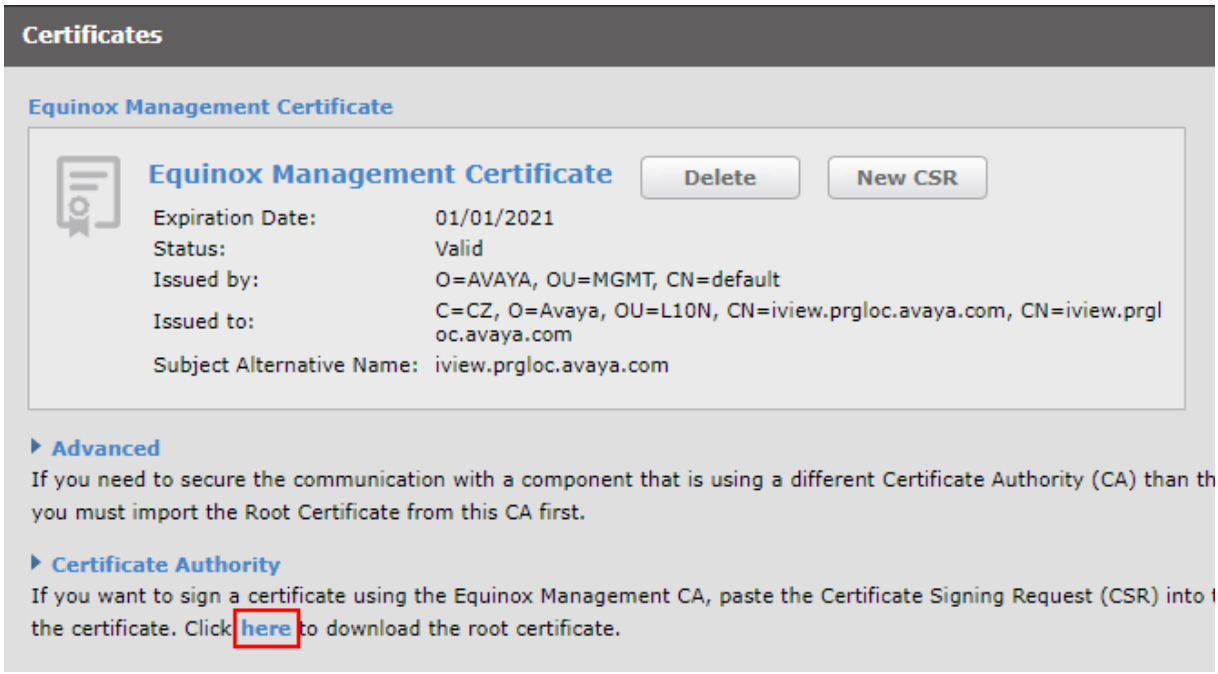


Figure 52: Certificates Page

3. Click the word **here** to download the certificate.

   Equinox Management saves the certificate to your local machine.
4. Send the certificate to the client.
5. The client must follow the following steps on the client PC to import the certificate.
6. To import the certificate with Chrome:
   a. Click **Manage certificates** in the **Advanced** section of Chrome's settings.
   b. Click the **Trusted Root Certification Authorities** tab.
   c. Click **Import**.

      The system displays the **Certificate Import Wizard**.
   d. Browse to the certificate that Equinox Management saved to your local machine.
   e. Verify that your information is correct, and complete the wizard.
7. To import the certificate with Firefox:
   a. Click **View Certificates** in the **Certificates** section of **Privacy & Security** in Firefox's settings.
   b. Click **Import**.
   c. Browse to the certificate that Equinox Management saved to your local machine.
   d. Select the **Trust this CA to identify websites** check box.
   e. Click **OK**.

f. Click **OK**.

8. In your browser accept the certificates located at the following links:
   - `https://<your media server IP address>/proxy/api/version`
   - `https://<all-in-one management server IP address>:8453/uwd/`

   Warning:

   If either of these URLs generates a warning message that your connection is not private, proceeding to the URL destination would likely lead to a security breach.
9. Access the local Unified Portal URL (`https://<your local server FQDN>:8443/portal/tenants/default`).
10. Enter the **Virtual Room Number** in the relevant field and select **Join In Meeting** to join the meeting from your client.

Related links

Securing Connections With Equinox Management on page 111

Renewing the CA Certificate for H.323 Gatekeepers in Alternate Mode

About this task

This procedure describes how to install a renewed third party CA certificate in primary and secondary gatekeepers.

Before you begin

Ensure that the alternate mode is operational.

Procedure

1. Access the Equinox Management administrator portal.
2. To access the primary gatekeeper:
   a. In the gatekeeper list, select the primary gatekeeper.
   b. On the **Configuration** page, uncheck **Secure Connection**.
   c. The primary gatekeeper restarts automatically. Wait for a few minutes.
   d. In the gatekeeper list, verify that the primary gatekeeper status icon lights green.
3. To delete the current certificate:
   a. In the gatekeeper list, select the primary gatekeeper.
   b. On the **Certificate** page, select **Delete**.

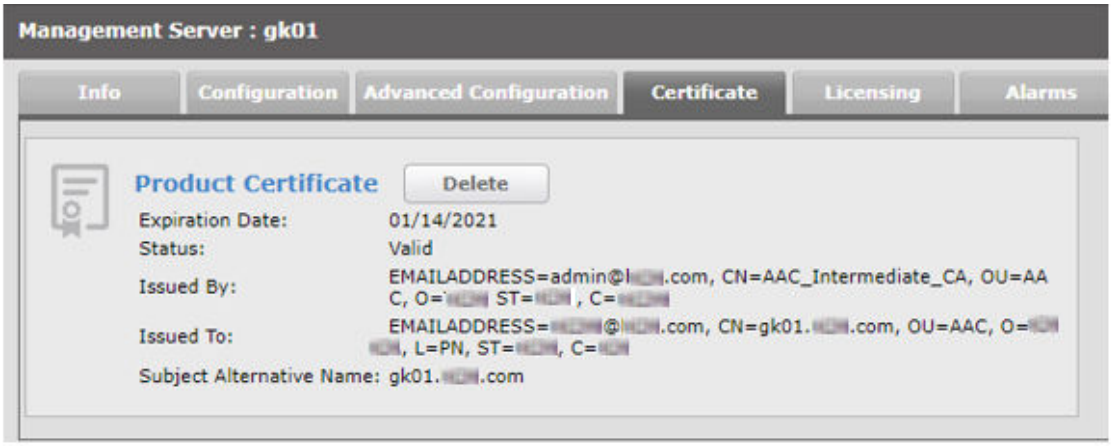


Figure 53: Product certificate removal

Equinox Management displays a confirmation dialog box to delete the existing gatekeeper certificate.

c. Select **Yes** in the dialog box.

Equinox Management displays a step-by-step procedure to install a new certificate.

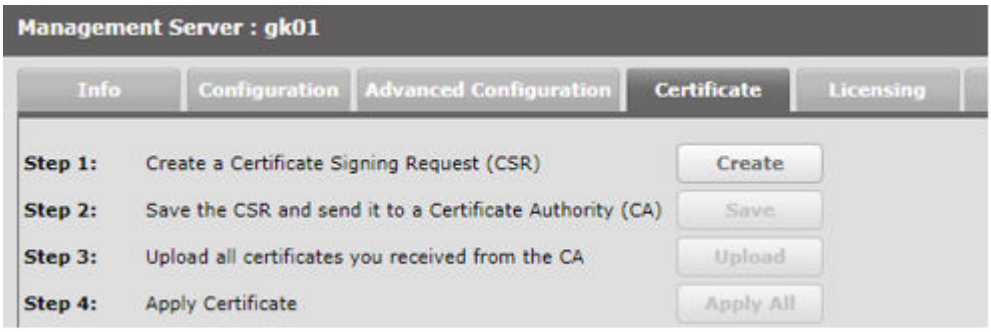


Figure 54: Certificate installation procedure

4. To generate a Certificate Signing Request (CSR) for the primary gatekeeper:

   a. Select **Create**.

   Equinox Management displays the **Generate CSR** dialog box.

   b. Configure the relevant fields to create the CSR.

   Ensure that:

   - The **Common Name** field has the virtual FQDN.
   - The **Subject Alternative Name** field has the FQDN and IP address of the primary, secondary, and virtual gatekeepers.

   c. Select **Generate CSR**.

5. On the **Certificate** page, select **Save** to retrieve the CSR to the local computer you are using to access Equinox Management.

6. Send the CSR to the Certificate Authority (CA).

   Proceed to the next step only when you receive the cert file, CA root and intermediate file back from the CA.

7. To upload the certificates to Equinox Management:
   a. On the **Certificate** page of the primary gatekeeper, select **Upload**.
   b. Add the certificates that came back from the signing process to have the full chain as shown in the following figure.

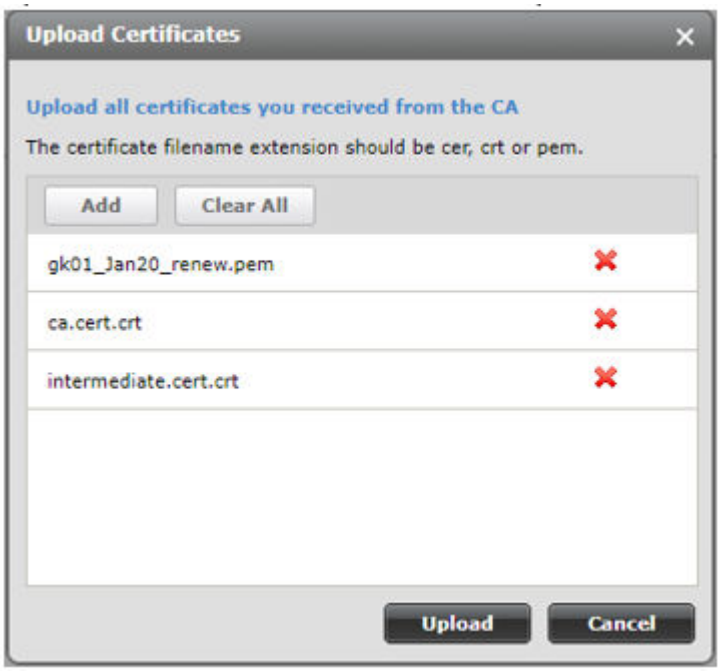


Figure 55: CA Certificate upload to Equinox Management

   c. Select **Upload**.

8. After Equinox Management completes the upload process, apply the new certificates to the primary gatekeeper:
   a. Select the **Certificate** page and select **Apply All**.

      A success dialog box prompts you to restart the gatekeeper.

   b. Select **OK**.

      The gatekeeper restarts. Wait for a few minutes.

   c. In the gatekeeper list, verify that the primary gatekeeper icon lights green.
   d. On the **Certificate** page, check the primary gatekeeper's new certificate.

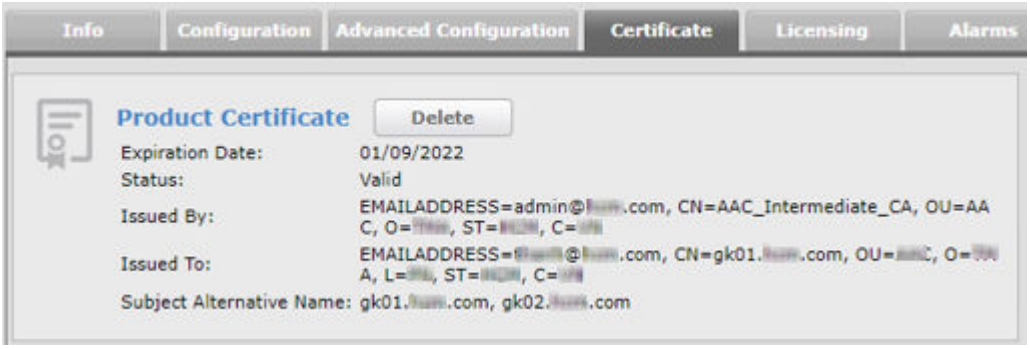


Figure 56: Renewed product certificate installation

9. On the **Configuration** page, select **Secure Connection**.

   The primary gatekeeper restarts. Wait for 10 minutes to ensure the secondary gatekeeper gets synchronized with the primary gatekeeper.

   Note:

   If the secondary gatekeeper does not synchronize with the primary gatekeeper, perform the above steps for the secondary gatekeeper.

10. To complete synchronization with the secondary gatekeeper:

    a. Restart the secondary gatekeeper by navigating to its **Configuration** page and unchecking **Secure Connection**.

       - The secondary gatekeeper restarts automatically.
       - Wait for about 10 minutes until the secondary gatekeeper is up again and completes synchronization.

    b. Select the **Alarms** tab, and solve alarms if any.

    c. On the **Advanced Configuration** page, verify that the bi-directional arrow lights green in the **Alternate Gatekeeper** section. This indicates that the alternate mode is operational.

Related links

Securing Connections With Equinox Management on page 111

Configuring User Portal / Web Gateway Settings

About this task

After generating a signed certificate, you configure User Portal / Web Gateway settings to complete the Equinox Management deployment.

You can choose to accept the default settings, or customize your settings, as needed. However, you must verify that the **Front End FQDN** setting in the **Client Connection** section is the value specified during OVA deployment.

Before you begin

Ensure that you have successfully created a signed certificate, as described in Applying a Third-Party Certificate to the All-in-One Equinox Management Server on page 112.

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. Configure settings on the **General** tab, as described in the following table:

Table 16: General tab fields

Section	Field	Description
User Portal	**Frontend Scheme**	The system displays the full frontend address
	Frontend FQDN	Verify that the value is the same as that specified during OVA deployment. It is important to configure a virtual IP when **Frontend FQDN** is configured, see Deploying a distributed or cluster User Portal and Web Gateway on page 100.
	Frontend Port	Enter 443
	Outlook plug-in for Windows downloading address	
	Outlook plug-in for MAC downloading address	
	Support email address for sending the client logs	
	Disable the pop-up window for the app download	In TE deployments where the Avaya IX™ Workplace Client is installed by IT it is necessary to disable the Avaya IX™ Workplace Client app download pop-up. **Default**: Unchecked
Web Gateway	**Max Video Bandwidth Per Call (Kbps)**	Enter **1280** To disable video, enter **0**.
	Enable TURN in WebRTC Client	

Table continues…

Section	Field	Description
	Enable use of an external load balancer	

4. Configure settings on the **Advanced** tab, as described in the following table:

Table 17: Advanced tab fields

Section	Field	Description
User Portal	**Allow recording guest access**	Select to enable guest users to record a conference.
	Allow portal guest access	Select to enable Unified Portal users to access Equinox Management as a guest.
	Enable uploading picture	Select to enable users to upload their picture into the system.
	Client Connection	
	Frontend UPC Base URL	The path for the Unified Portal, typically **/portal**
	Frontend UPS Base URL	The path for the Unified Portal server, typically **/ups**
	Frontend SWC Base URL	The path for the WebRTC client, typically **/uwd/dist**
	Frontend Web Gateway Base URL	The path for the Web Gateway, typically **/csa**
	IWA enabled	Select to enable Integrated Windows Authentication (IWA) in your browser. When selecting this field, you must enter values for the following sub fields: • DNS Domain • KDC FQDN • KDC Port • Kerberos Realm • SPN • Key Tab File
	Web MeetMe Data Only Browser Version Exclusion	Browsers that do not support the Web MeetMe Data Only client
	Web MeetMe WebRTC Browser Version Exclusion	Browsers that do not support Web MeetMe RTC
	Web MeetMe WebRTC Browser Min Version	The minimum browser version needed to support the Web MeetMe WebRTC

Table continues…

Section	Field	Description
	Web MeetMe Data Only Browser Min Version	The minimum browser version needed to support the Web MeetMe Data Only client
	Avaya Equinox Client MeetMe Min Version	The minimum browser version needed to support Avaya Equinox Client MeetMe
	Avaya Equinox Client Aura Min Version	The minimum browser version needed to support Avaya Equinox Client Aura
Web Gateway	**Web Gateway WebRTC Audio Codec Order**	The order in which we want to use the indicated audio codecs offered to WebRTC clients.
	Web Gateway SIP Audio Codec Order	The order in which we want to use the indicated audio codecs offered to SIP clients.
	Web Gateway WebRTC Video Codec Order	The order in which we want to use the indicated video codecs offered to WebRTC clients.
	Web Gateway SIP Video Codec Order	The order in which we want to use the indicated video codecs offered to SIP clients.
	Web Gateway SRTP Policy	The SIP and SRTP security policy for sessions. • Select **Best effort** to attempt to establish secure SIP and SRTP connections. If the SIP endpoint does not support secure connections, unsecured connections are used. • Select **Enforced** to ensure that sessions establish only secure SIP and SRTP connections. If the SIP endpoint does not support secure connections, the session is not established.
	Web Gateway Opus Profile	Select from the following options to define the audio bandwidth: • Constrained narrow band • Narrow band • Wide band
	Media Encryption Settings	Select the ciphers that you want to support for media encryption.

5. Manually restart the all-in-one Equinox Management server:
   a. On the upper-right side of the page, select ☰ > **Restart**.
   b. Select **Yes** in the confirmation dialog box.

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

Uploading a windows installer with Equinox Management on page 129
Uploading a Mac Installer with Equinox Management on page 130

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.

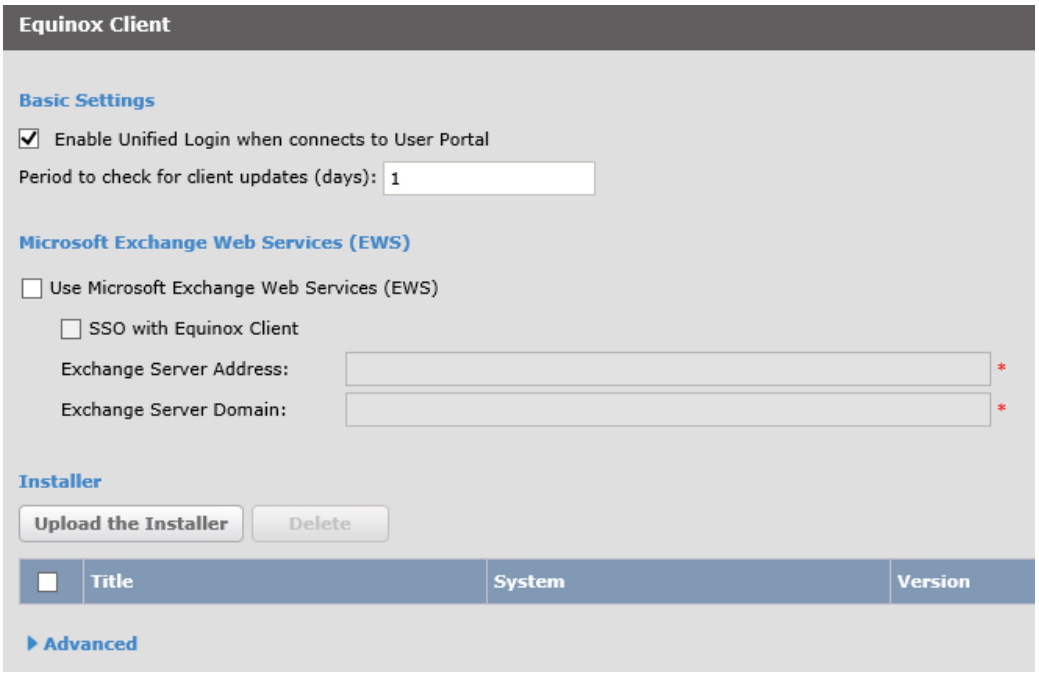
Before you begin

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 129

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*.

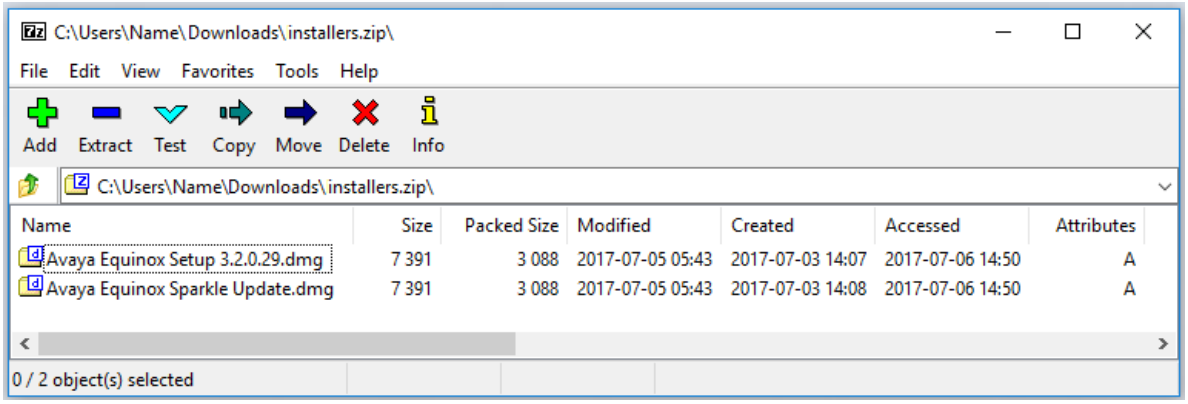
Before you begin

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.

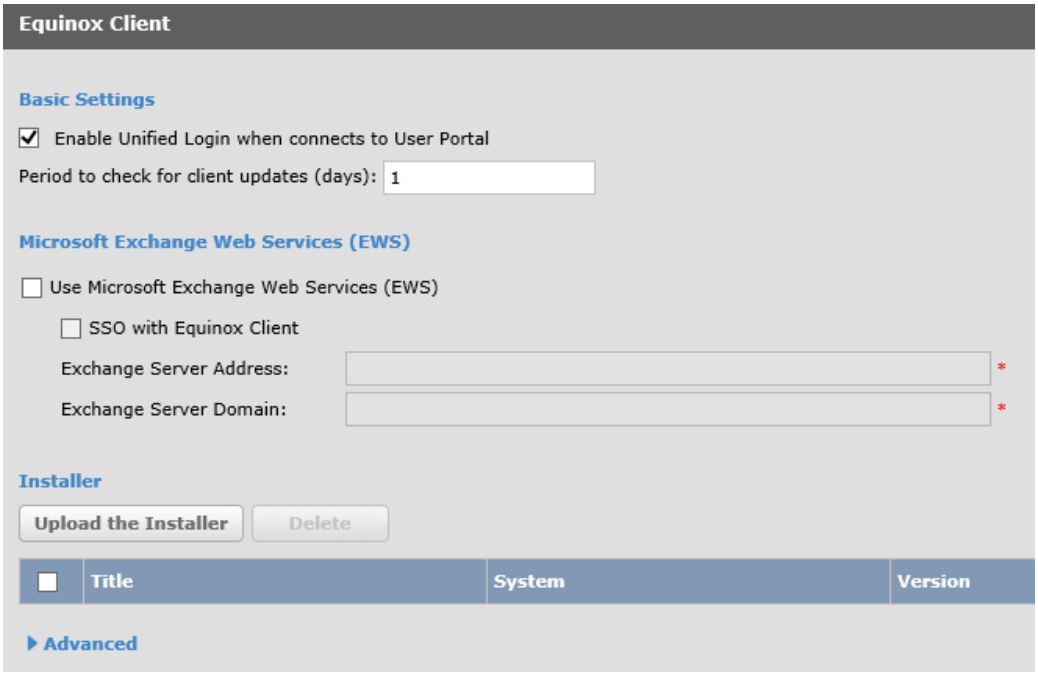


Figure 57: Equinox Client Page

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 129

Switching Equinox Management from Port Based to User Based Licensing

About this task

Enterprises can switch from a port-based licensing model to a user-based licensing model when upgrading from an OTT solution to a TE solution.

This procedure explains how to switch Equinox Management from using port-based licenses to user-based licenses.

Procedure

1. On your virtual machine, right-click the current Equinox Management server name and select **Snapshot** > **Take Snapshot** to back up your environment. (Optional)

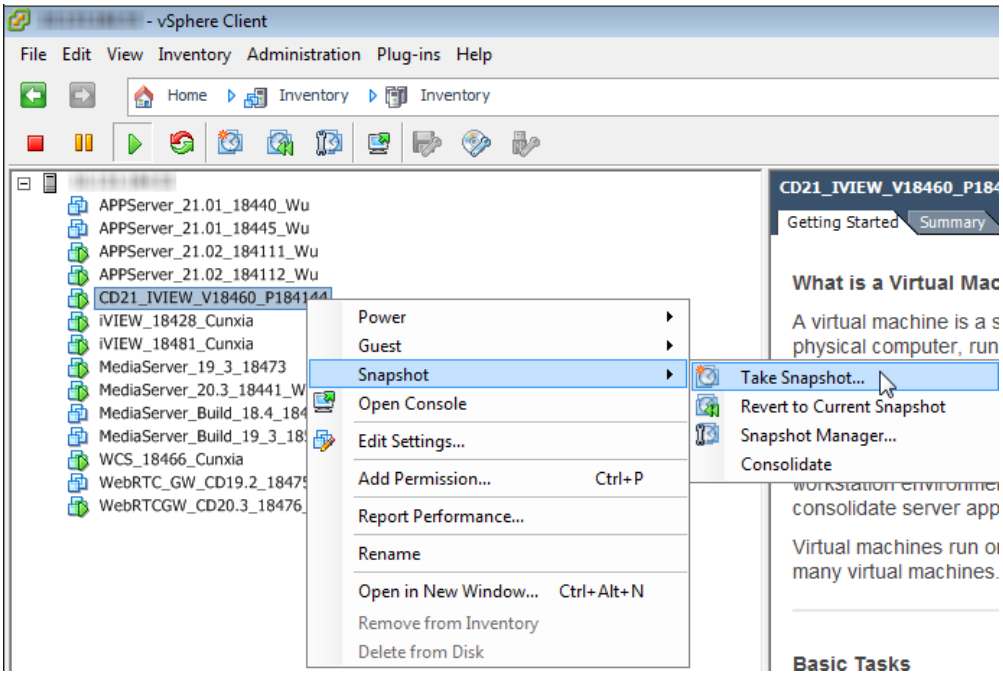


Figure 58: Virtual Machine Backup

2. Ensure that you have received the following from PLDS:
   - A user-based Equinox Management license.
   - A WebLM License file for Power Suite users.
   - Third-party video connectivity
3. Access the Equinox Management administrator portal.
4. Select **Settings** > **System Preference** > **Local Services** and ensure that the **User Portal + Web Gateway** is disabled.

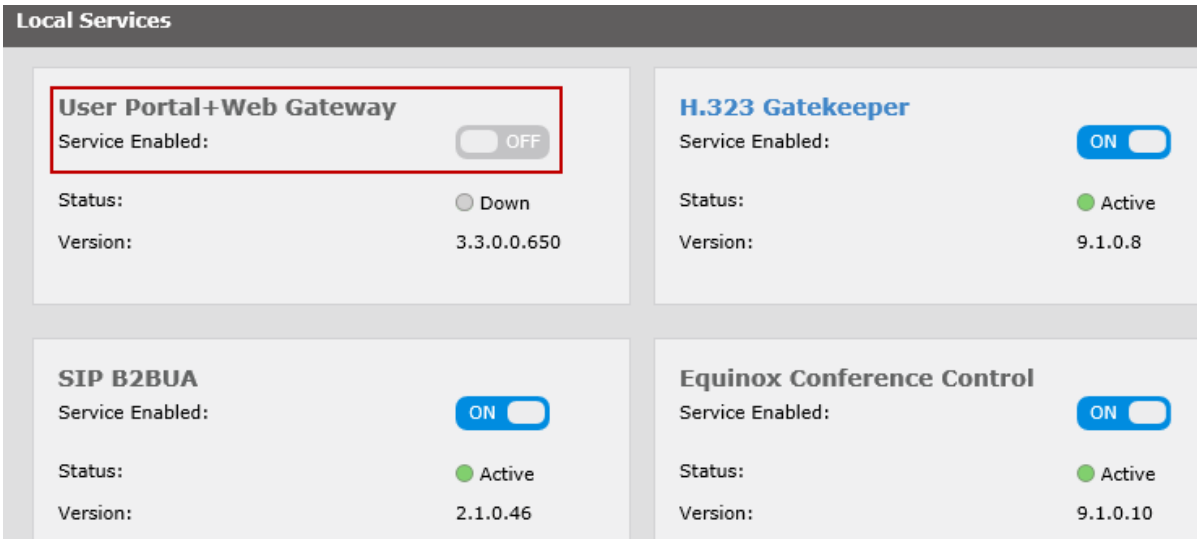


Figure 59: Local Services Page

5. Apply Equinox Management Power Suite Edition license, as described in Updating the Equinox Management license on page 420.
6. On the WebLM server, upload the Equinox Conferencing User license and 3rd Party Video Connectivity license files.
7. From the Equinox Management administrator portal, select **Settings** > **Servers** > **License Server**.

   The **License Server** page appears.

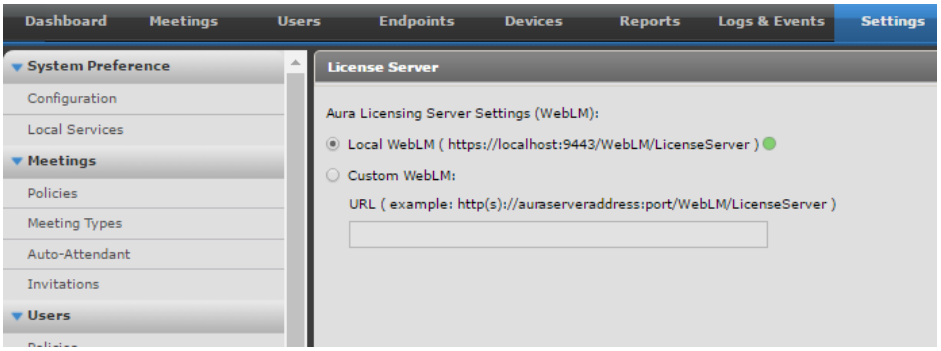


Figure 60: License Server Page

8. Select either **Local WebLM** or **Custom WebLM**, depending on the license you applied above.

   Ensure that the license you select has a green status (online).
9. On the License Information page, select ☰ > **License Information**, to open the License Information page.

   Ensure that the **Power Suite Users** and **3rd Party Video Connectivity** licenses are displayed as expected.

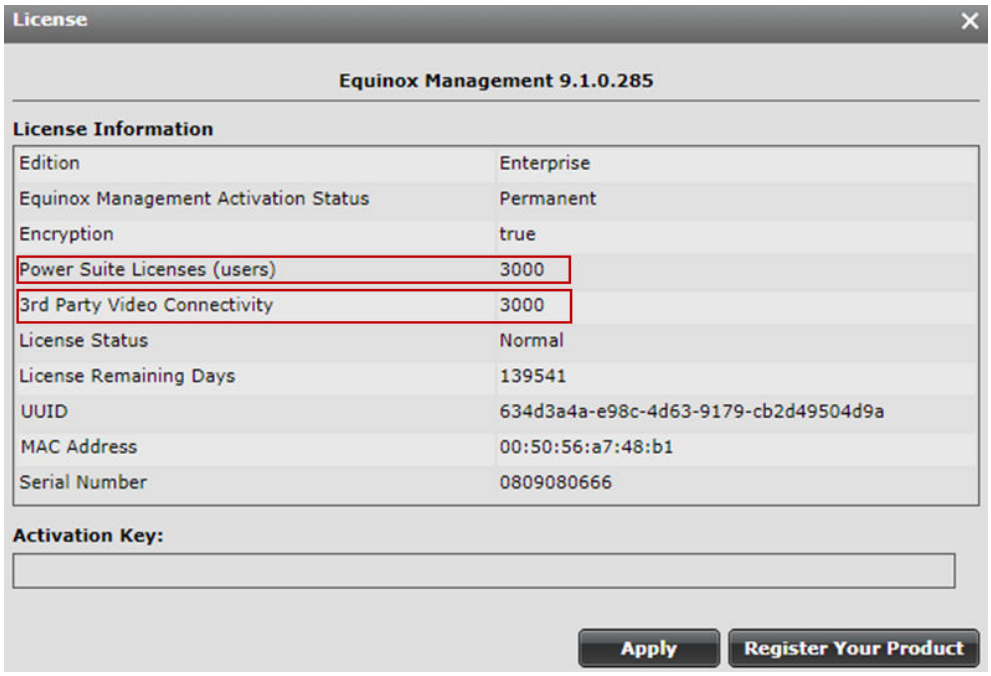


Figure 61: License Information Page

10. Select **Settings** > **Users** > **Profiles** and select a profile.

    The system displays the **User Profile** page for the selected profile.

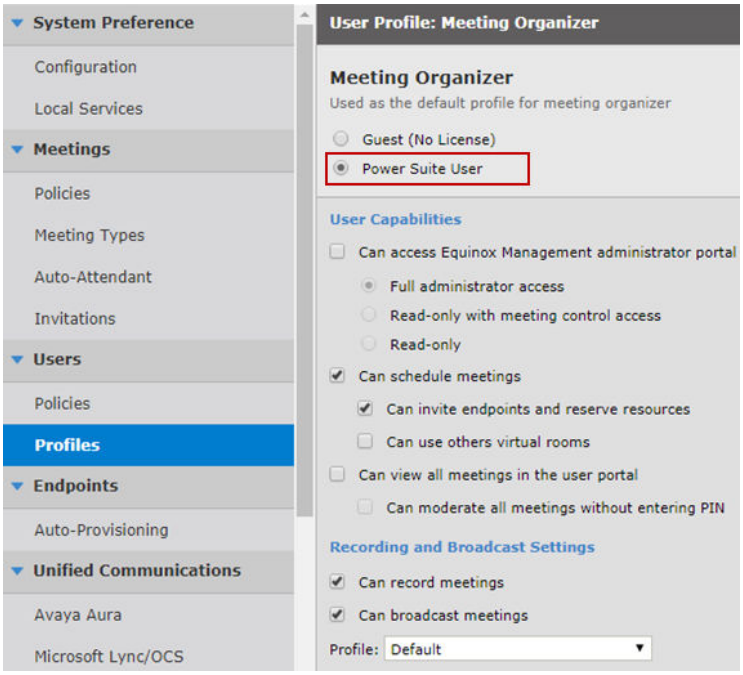


Figure 62: User Profile Page

11. Select **Power Suite User** to designate the selected profile as one for licensed users.

Only Power suite users have access to virtual rooms

Note:

The media server does not require a new user license.

Deploying and Configuring the Equinox Management Environment

After deploying Avaya Equinox® Management, you must deploy and configure your Equinox Management environment. Perform the following procedures:

1. Deploy and configure the media server and gateway (see the *Equinox Media Server deployment* chapter).
2. (Optional) Deploy and configure Avaya Equinox® H.323 Edge server (see the *Equinox H.323 Edge deployment* chapter).
3. (Optional) Deploy and configure Avaya Session Border Controller for Enterprise (see the *Avaya Session Border Controller deployment* chapter).
4. (Optional) Deploy and configure Avaya Equinox® Streaming and Recording (see the *Avaya Equinox® Streaming and Recordingdeployment* chapter).
5. (Optional) Deploy and configure an external H.323 Gatekeeper (see the *Administrator Guide for Avaya Equinox® Management*).

Once you have deployed these components, you can add them to the all-in-one Equinox Management server.

Troubleshooting

This section helps you troubleshoot problems that may cause Equinox Management to perform less effectively than desired.

Upgrade Failure

If Equinox Management fails to upgrade from a previous version to the most recent version, verify that the package description file (either `components-scopia-app-package.txt` or `components-media-server-package.txt`) contains the following strings:

```
[package]
```

or

```
name=management-server
```

or

```
name=media-server
```

or

```
name=application
version=8.5.0.13
[component]
```

You cannot upload an app server package to CMS, or a CMS package to an Equinox Management server.

Change the MCU Log Level

You may want to change the MCU log level to more precisely monitor the system behavior. To do so, perform the following actions:

1. In the MCU Web Portal, select the Settings icon and click **Advanced Parameters**. The system displays the **Advanced Parameters** page.
2. In the **Unit Notify Level** section, modify the value to **100**, and click **Apply**.
3. Modify the log level using SSH, as follows:
   - [admin@MCU~]>rvcli
   - Avaya_Scopia_MCU>logLevelSet 0x100
   - Multiple matches found for [logLevelSet] — specify the server or select:
     - mcu1 <IP Address:port>
     - mvp1 <IP Address:port>
     - ics1 <IP Address:port>
     - map1 <IP Address:port>
     - :1
     - [logLevelSet] done
     - Avaya_Scopia_MCU>
4. print XML in log `rvcli  mcuXmlSetPrintMsg 1`
5. print sip stack log `rvcli AdapSipShowStack 1`
6. print h.323 stack log `rvcli AdapH323ShowStack 1`

Device Availability

When a **Device is Not Available** message is generated for an Avaya Media Server, the reason may be one of the following:

- Equinox Management cannot connect to the device PMGR component. Search for the keyword **Cannot connect and monitor the PMGR server** in the Equinox Management log.
- Equinox Management cannot connect to the CMS's MCU component. If it is in Video+Web mode, search for the keyword string, **Cannot connect the v9 MCU to refresh the status** in the Equinox Management log.
- Equinox Management cannot connect to the CMS's AMS component. If it is in Audio+Web mode, search for the keyword string, **Cannot connect and configure the AMS** in the Equinox Management log.

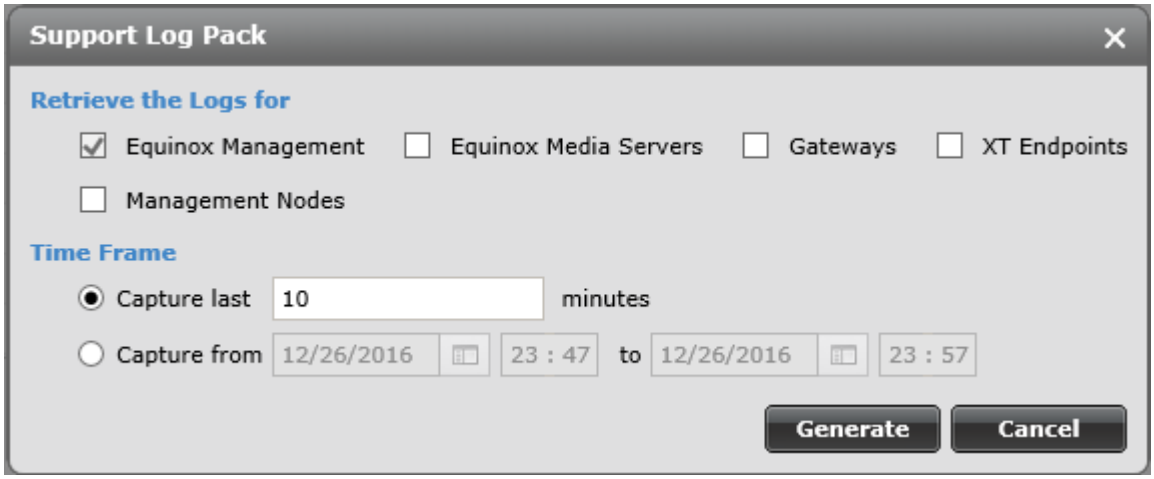
When a **Device is Not Available** message is generated for a Scopia Elite MCU 6000 or for a UC-GW, the reason may be one of the following:

- Equinox Management cannot connect to the MCU admin manager port (3338/3348). Search for the keyword string, **Cannot connect and monitor the MCU/GW** in the Equinox Management log.
- Equinox Management cannot connect to the MCU call control port (3336/3346). Search for the string, **MCUIP:3336** or **MCUIP:3346** in the Equinox Management log.

Retrieve the Equinox Management Support Log

To retrieve the Equinox Management support log and view actions performed in Equinox Management, do the following:

1. On the Administration Portal home page, click the **Settings** icon and click **Support Log Pack**. The system displays the **Support Log Pack** dialog box.



2. In the **Retrieve the Logs** for section, select the relevant options for the logs you want to receive:
   - Equinox Management
   - Equinox Media Servers
   - Gateways
   - XT Endpoints
   - Management Nodes
3. In the **Time Frame** section, select a time period for which you want to capture logs.
4. Click **Generate**.

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:

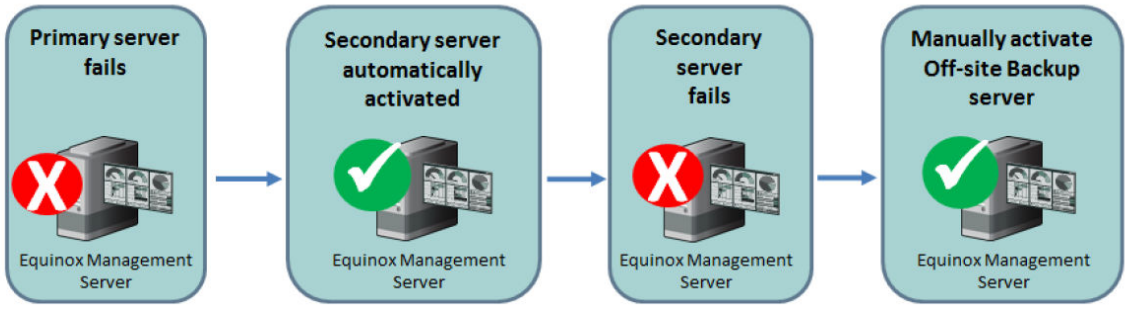


Figure 63: Disaster Recovery Decision Making Process

Related links

Activating disaster recovery in a geographic redundancy deployment on page 139
Updating DNS and GSLB Records in Disaster Recovery for Geographically Distributed Equinox Management on page 141
Resuming normal operations after disaster recovery on page 142

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 64: 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 138

Updating DNS and GSLB Records in Disaster Recovery for Geographically Distributed Equinox Management

About this task

This section describes the steps you must take to preserve your data when an Equinox Management data center (DC) fails. Performing this task ensures that all traffic is routed to another DC, known as the disaster recovery site. You must have DNS records to enable redirecting the Equinox Management server FQDN, and for the User Portal + Web Gateway FQDN to resolve to the disaster recovery site. The DNS must have a secondary record for both the Equinox Management server FQDN and the User Portal + Web Gateway FQDN to enable the client to connect to the secondary record if it cannot connect to the primary record.

To perform failover to the disaster recovery site, do the following:

Procedure

1. Activate the Equinox Management server in the disaster recovery (DR) site. See Activating disaster recovery in a geographic redundancy deployment on page 139.
2. Update the internal DNS server so that the Equinox Management FQDN points to the Equinox Management DR IP address in DC2, instead of the Virtual IP address in DC1.
3. Update the external DNS record for the Equinox Management FQDN so it points to the ASBCE DR site instead of DC1.

   See Web Conference Signaling and Media in a Distributed Environment on page 93 for information on DCs.
4. Update the external GSLB records so that the User Portal + Web Gateway FQDN routes traffic away from DC1 and to another DC with User Portal + Web Gateway servers.

Related links

Disaster recovery in a geographic redundancy deployment on page 138

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 65: 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 139.

9. Verify that the devices are registered correctly. See Activating disaster recovery in a geographic redundancy deployment on page 139.

Related links

Disaster recovery in a geographic redundancy deployment on page 138

Chapter 6: Equinox Management Deployment for Team Engagement solution

Deployment of Equinox Management for TE solution — Overview

The Equinox Management Team Engagement (TE) Solution is intended for customers who already have deployed or plan to deploy a full Avaya UC platform that includes System Manager (SMGR), Session Manager (SM) 7.x, and all other Avaya UC components. These customers use the *per named user* business model and obtain Equinox as part of the Power Suite (permanent or subscription) licensing entitlement. In this deployment, the connection of third party videoconferencing terminals requires a specific enabling license, known as the *Third Party Videoconferencing Connectivity*. Each license enables 10 ports.

Checklist for Deploying Equinox Management in Team Engagement

Use the following checklist for deploying the Equinox Management server in a Team Engagement (TE) solution.

#	Action	Link/Notes	✔
1	Download software from the PLDS	Downloading software from PLDS on page 32	

Table continues…

#	Action	Link/Notes	✔
2	Deploy the Equinox Management server	Deploying the Equinox Management Server on page 67 **Note:** The User Portal + Web Gateway component referenced in this topic is external to Equinox Management and is called *Avaya Aura Web Gateway* in TE deployments (see *Deploying the Avaya Aura Web Gateway* guide on the Avaya Support Site).	
3	Log into Equinox Management	Logging into Equinox Management on page 81	
4	Configure Equinox Management	Configuring the All-In-One Equinox Management Server on page 88 **Note:** The User Portal + Web Gateway component referenced in this topic is external to Equinox Management and is called *Avaya Aura Web Gateway* in TE deployments (see *Deploying the Avaya Aura Web Gateway* guide on the Avaya Support Site).	
5	Configure the H.323 Gatekeeper	Deploying a Standalone Distributed H.323 Gatekeeper on page 104	
6	Manage Licenses	Managing Licenses Via the Web-based License Manager (WebLM) on page 422	
7	Secure Connections	Securing Connections With Equinox Management on page 111	
8	Integrate Avaya Aura® Web Gateway and Equinox Management	Deploying the Avaya Aura Web Gateway on page 146	
9	Deploy and configure the Equinox Management environment	Deploying and Configuring the Equinox Management Environment on page 136	
10	Add Avaya Aura® users into Equinox Management	Integrating Avaya Aura Users Into Equinox Management Via System Manager on page 147	
11	Configure Session Manager to work with SIP-based Equinox B2BUA component	Configuring Session Manager for Interoperability with the SIP-based Equinox B2BUA Component on page 156	
12	Configure Equinox Management to work with Avaya Aura®	Configuring Equinox Management for Interoperability with Avaya Aura on page 159	

Deploying the Avaya Aura® Web Gateway

The Avaya Aura® Web Gateway is an Aura server which acts as a gateway to Aura for clients and applications by utilizing browser-based WebRTC signaling and media. It consists of the following:

- In Aura (Team Engagement/TE) deployments, the components of this gateway (the Unified Portal and Web Gateway) are provided in a separate OVA for deployment on a customer-supplied VMware environment. These components are shared and utilized by different Aura clients and applications.
- In non-Aura (Over The Top/OTT) deployments, these components are hosted within Equinox Conferencing.

For details on deploying the Avaya Aura® Gateway, Avaya Aura® media server configuration, and Avaya Aura® Device Services (AADS), see *Deploying the Avaya Aura® Gateway* on the Avaya Support Site.

Related links

Configuring the Avaya Aura Web Gateway in Equinox Management on page 146

Configuring the Avaya Aura Web Gateway in Equinox Management

About this task

This procedure describes how to configure Avaya Aura Web Gateway into Equinox Management in a Team Engagement (TE) environment.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Devices** > **Devices by Type** > **User Portals** and select **Add**.

   The **Add User Portal** page appears.
3. Enter a name, IP address, and FQDN in the relevant fields.
4. Select **Aura User Portal**.
5. Select **OK** and wait for the user portal to connect.

   The user portal's status displays as green.

   Note:

   If AAWG is a cluster with multiple nodes, all of the nodes must be added into Equinox Management. The IP Address should be the physical IP address of each node.

Related links

Deploying the Avaya Aura Web Gateway on page 146

Integrating Avaya Aura® Users Into Equinox Management Via System Manager

System Manager is the central management system that delivers a set of shared management services and provides a common console for Avaya Aura® applications and systems. System Manager 7.0.1.3 is the primary management solution for Avaya Aura® 7.0.1.3 and is therefore required with all Avaya Aura® 7.0.1.3 deployments. The topics in this section explain the procedure for integrating Avaya Aura® users into Equinox Management.

For information about configuring System Manager, see *Administering Avaya Aura® System Manager* on the Avaya Support Site.

Related links

Configuring the Equinox Conferencing Element in System Manager on page 147
Configuring SSO for Equinox Conferencing on page 151
Adding Avaya Aura Users in Equinox Management on page 154

Configuring the Equinox Conferencing Element in System Manager

About this task

This procedure describes how to configure the Equinox Conferencing element in the System Manager web console. For details on configuring the System Manager, see *Administering Avaya Aura® System Manager for Release 7.0.1* on the Avaya Support Site.

Note:

Equinox Management is currently referred to as **Equinox Conferencing** in the System Manager web console.

Procedure

1. On the System Manager web console, select **Services** > **Inventory**.

   The **Inventory** page appears.

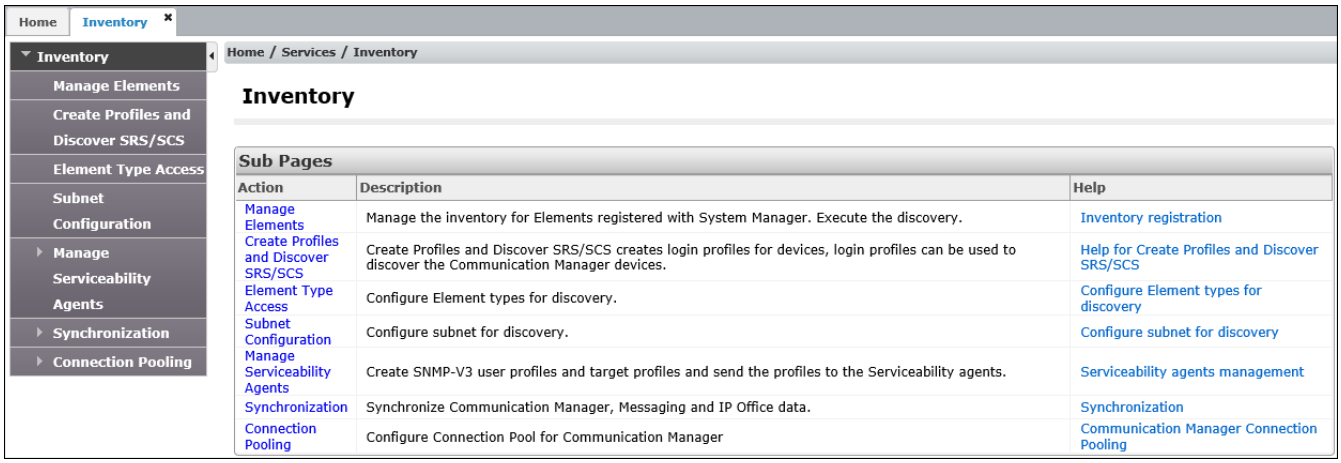


Figure 66: System Manager — Inventory Page

2. In the left navigation pane, select **Manage Elements**.

   The **Manage Elements** page appears.

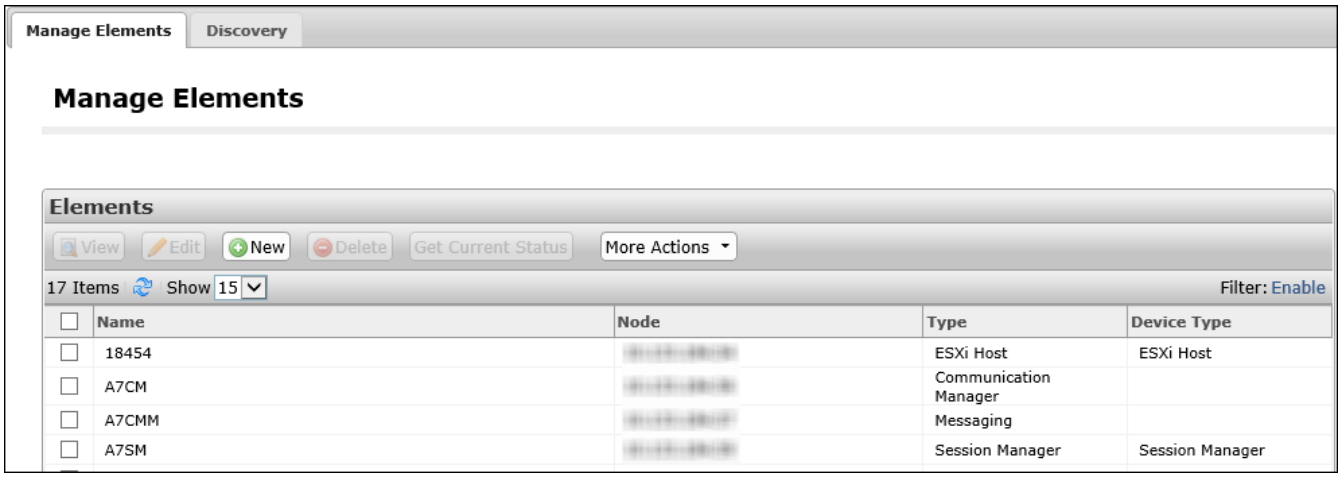


Figure 67: System Manager — Manage Elements Page

3. Select **New**.

   The **New Elements** page appears.

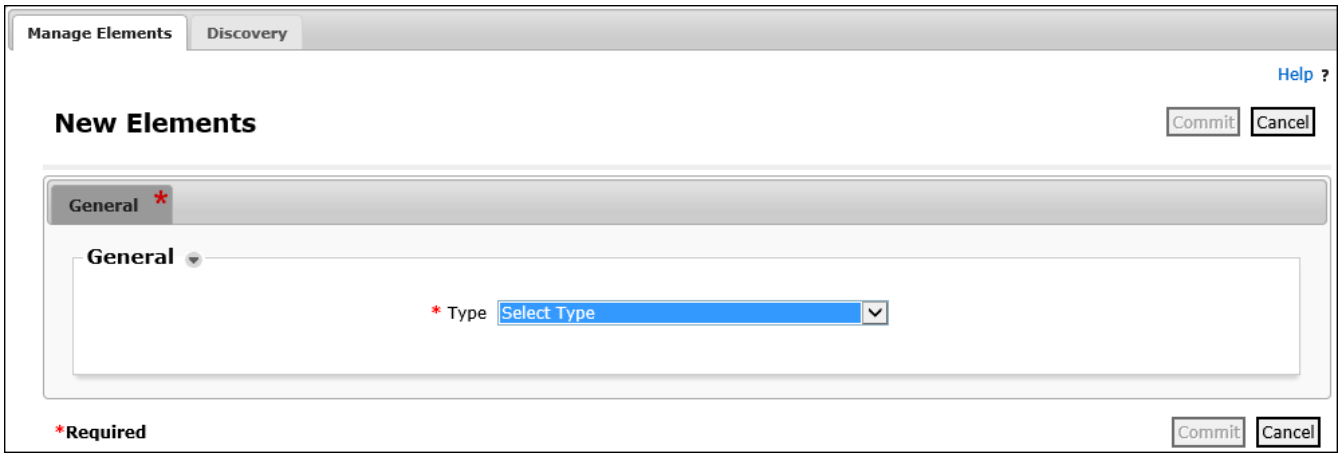


Figure 68: System Manager — New Elements Page

4. In the **Type** drop down, select **Equinox Conferencing**.

   The **New Equinox Conferencing** page appears.

5. On the **General** page, in the **General** section, configure the following fields:
   - Name
   - Type
   - Description
   - Node

6. On the **General** page, in the **Access Profile** section, select **New**.

   System Manager displays the **Application System Supported Protocol** section.

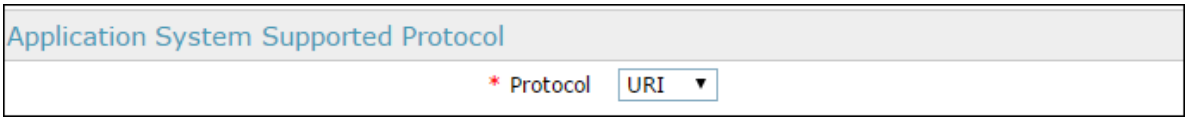


Figure 69: Application System Supported Protocol Section

7. In the **Protocol** field, select **URI**.

   System Manager displays the **Access Profile Details** section.

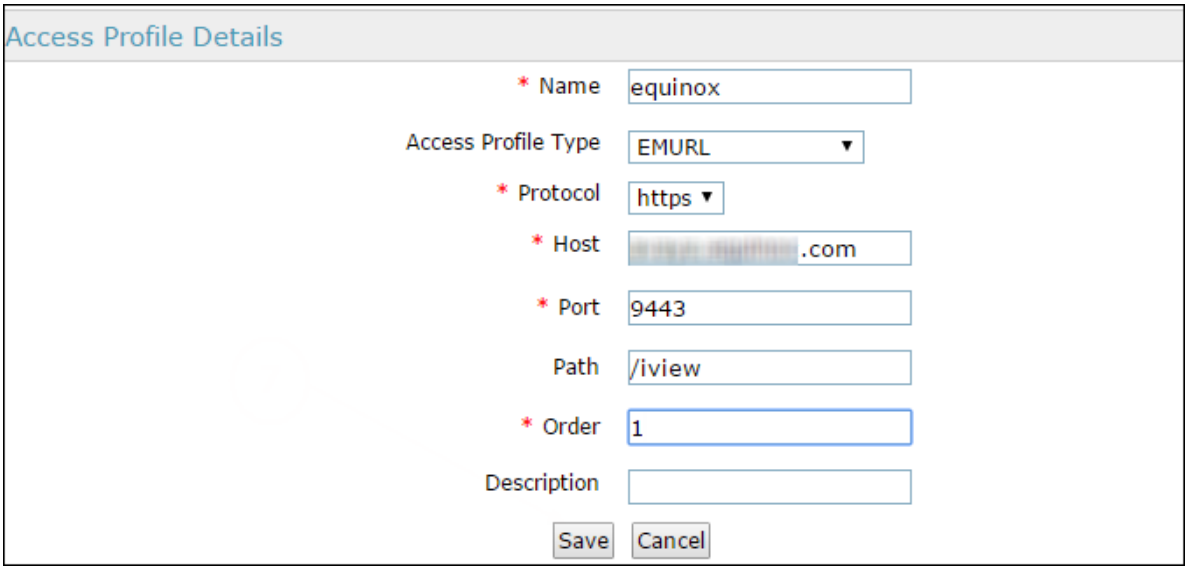


Figure 70: Access Profile Details Section

8. Configure the following fields:
   - Name
   - Access Profile Type
   - Protocol
   - Host
   - Port
   - Path
   - Order
   - Description
9. Select **Save**.

   System Manager displays the **New Equinox Conferencing** page.

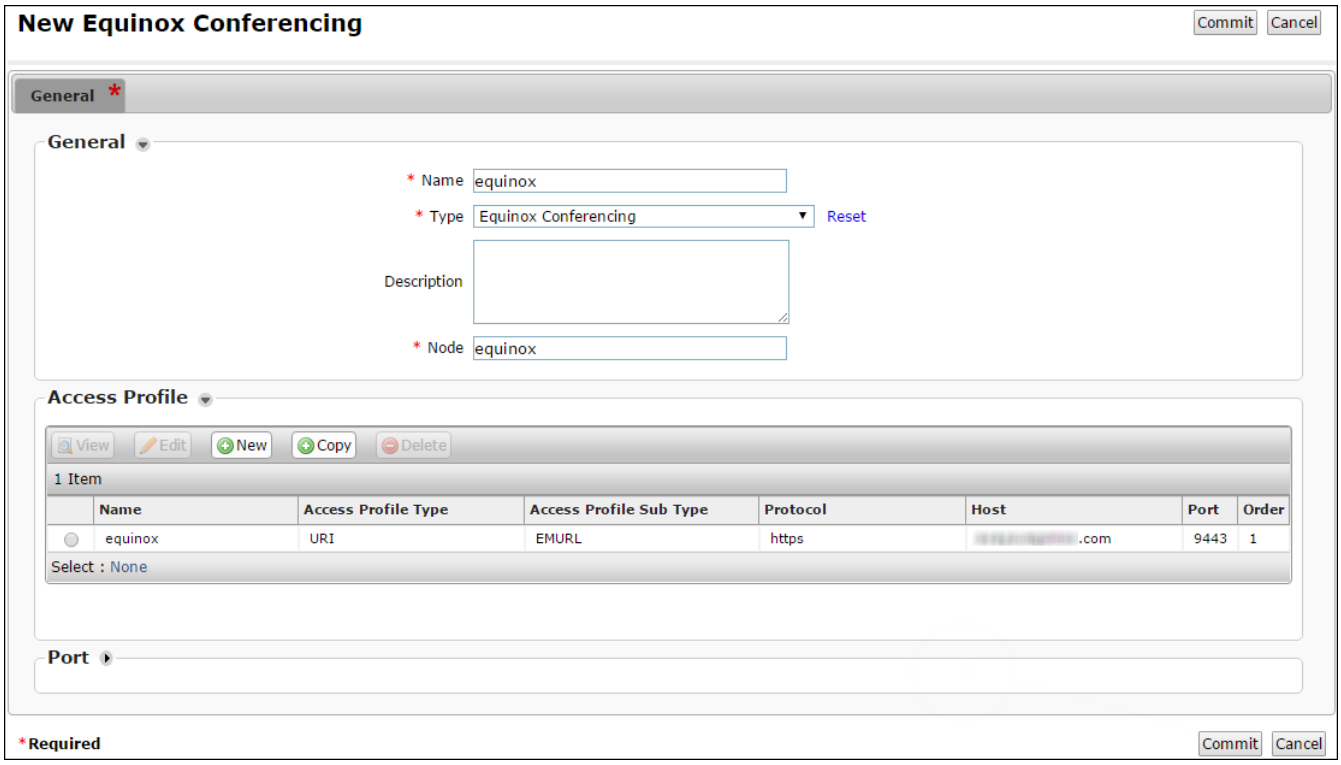


Figure 71: New Equinox Conferencing Page

10. Select **Commit**.

    System Manager creates the new element.

Next steps

Configure SSO for Equinox Conferencing, as described in Configuring SSO for Equinox Conferencing on page 151.

Related links

Integrating Avaya Aura Users Into Equinox Management Via System Manager on page 147

Configuring SSO for Equinox Conferencing

The procedures in this section describe the actions a System Manager administrator must perform to enable accessing Equinox Conferencing directly from the System Manager, without having to re-enter login information.

Related links

Integrating Avaya Aura Users Into Equinox Management Via System Manager on page 147
Downloading the System Manager CA Root Certificate on page 152
Exchanging CA Certificates between System Manager and Avaya Equinox® Management on page 152
Configuring SSO in Avaya Equinox® Management on page 153

Downloading the System Manager CA Root Certificate

About this task

This task explains how to download the System Manager CA root certificate as a preliminary step for exchanging certificates between System Manager and Equinox Management.

Procedure

1. On the System Manager web console, select **Services** > **Security**.

   The **Security** page appears.



Figure 72: System Manager — Security Page

2. Select the **Certificates** link and in the left navigation pane, select **Certificates** > **Authority**.
3. Select **CA Functions** > **CA Structure & CRLs**.
4. Select **Download PEM file**.

   The system downloads the `.pem` file onto your system.

Related links

Configuring SSO for Equinox Conferencing on page 151

Exchanging CA Certificates between System Manager and Avaya Equinox® Management

About this task

If the Avaya Equinox® Management CA certificate is not issued by the System Manager CA, perform the following task.

Procedure

1. Download the root CA certificate from System Manager.

   For more information, see Downloading the System Manager CA Root Certificate on page 152.

2. Log into the Equinox Management administrator portal.
   a. Select **Settings** > **Security** > **Certificates** to import the CA PEM file into Equinox Management.
   b. Select **Advanced** > **Import**.

c. Select **Add** in the **Import Certificates** dialog box to select the downloaded CA PEM file, and select **Apply**.

d. Restart Equinox Management.

e. Select **Settings** > **Security** > **Certificates** to download the Equinox Management CA certificate.

3. Log into the System Manager web console.

   The CA signs the certificate used by Equinox Management when it connects to Session Manager . You must add that CA to the Trusted list of Session Managers.

   Use the following procedure to add the CA certificate in System Manager.

   a. In the **Services** menu, select **Inventory** > **Manage Elements**.

   b. In the **Elements** section, select the Session Manager to which Equinox Management is connected.

   c. Click **More Actions** > **Manage Trusted Certificates**.

      The system displays the certificates that are currently installed on the managed element you selected.

   d. Click **Add**.

   e. On the **Add Trusted Certificates** page, in the **Select Store Type to add trusted certificate** field, click **All**.

   f. Choose a method to upload the CA certificate used to sign the Equinox Management certificate and then click **Retrieve Certificate**.

      Note:

      After changing certificates, verify that the SIP Entity link is working.

      Select **Elements** > **Session Manager** > **System status** > **SIP Entity Monitoring** and find the entity that represents your Equinox Management. The connection status must be UP.

Related links

Configuring SSO for Equinox Conferencing on page 151

Configuring SSO in Avaya Equinox® Management

Before you begin

If the Avaya Equinox® Management CA certificate is not issued by the System Manager CA, you must exchange CA certificates between Equinox Management and System Manager.

For more information, see Exchanging CA Certificates between System Manager and Avaya Equinox® Management on page 152.

Procedure

1. Access the Equinox Management administrator portal.

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

   The **Avaya Aura** page appears.

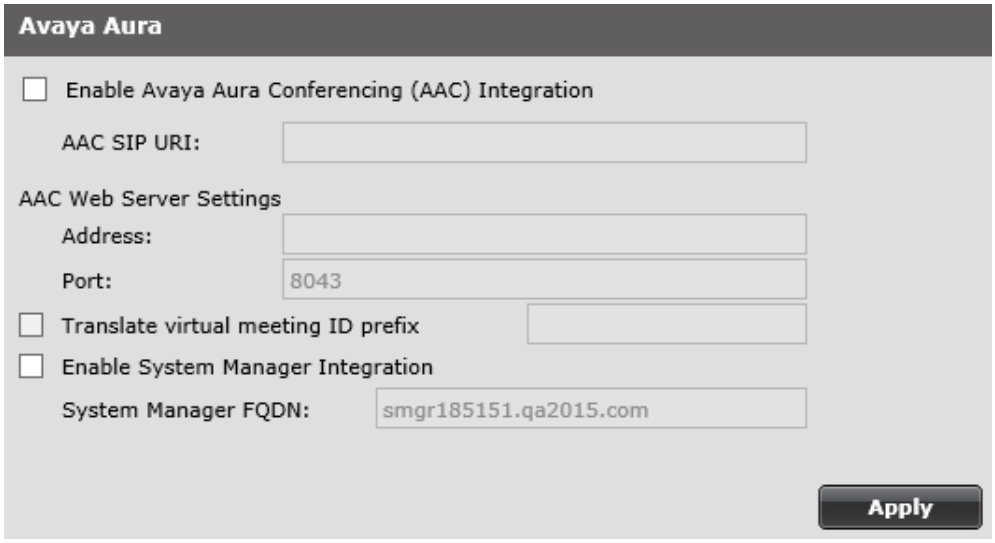


Figure 73: Avaya Aura Page

3. Select the **Enable System Manager Integration** check box.

   The **System Manager FQDN** field is enabled.

4. Enter the FQDN of the System Manager.
5. Select **Apply**.

   A dialog box appears, prompting you to restart the system. Select **Yes**.

Related links

Configuring SSO for Equinox Conferencing on page 151

Adding Avaya Aura® Users in Equinox Management

About this task

You can add only one Avaya Aura® user with Equinox Management at a time. Repeat this procedure for each Avaya Aura® user you want to add.

Note:

For information on adding Avaya Aura® users in Equinox Management automatically, see the *Migrating from Avaya Aura® to Avaya Equinox®* chapter in this guide.

Before you begin

Configure SSO for Equinox Conferencing, as described in Configuring SSO for Equinox Conferencing on page 151.

Procedure

1. On the System Manager web console, select **Users** > **User Management**.
2. In the left navigation pane, select **Manage Users**.

   System Manager displays the **User Management** page.
3. To add a communication profile to an existing user, select the user and select **Edit**.

   System Manager displays the **User Profile Edit** page.
4. Select the **Communication Profile** tab.
5. Select the **Equinox Conferencing** check box, and configure the following fields:
   - Equinox User Password
   - Virtual Room Number
6. Select **Commit**.

Related links

Integrating Avaya Aura Users Into Equinox Management Via System Manager on page 147

Deploying and Configuring the Equinox Management Environment

After deploying Avaya Equinox® Management, you must deploy and configure your Equinox Management environment. Perform the following procedures:

1. Deploy and configure the media server and gateway (see the *Equinox Media Server deployment* chapter).
2. (Optional) Deploy and configure Avaya Equinox® H.323 Edge server (see the *Equinox H.323 Edge deployment* chapter).
3. (Optional) Deploy and configure Avaya Session Border Controller for Enterprise (see the *Avaya Session Border Controller deployment* chapter).
4. (Optional) Deploy and configure Avaya Equinox® Streaming and Recording (see the *Avaya Equinox® Streaming and Recordingdeployment* chapter).
5. (Optional) Deploy and configure an external H.323 Gatekeeper (see the *Administrator Guide for Avaya Equinox® Management*).

Once you have deployed these components, you can add them to the all-in-one Equinox Management server.

Configuring Session Manager for Interoperability with the SIP-based Equinox B2BUA Component

The procedures in this section are guidelines on how to administer the system. Depending on your system's configuration, parameter values may differ.

Logging into System Manager

In your browser's address bar, enter the System Manager FQDN in the following format:

```
https://<FQDN_of_SystemManager>
```

Related links

[Adding a SIP Entity for the Equinox B2BUA Component](#) on page 156
[Adding a SIP Entity Link/SIP Trunk For the Equinox B2BUA Component](#) on page 157
[Adding Routing Policies For the Equinox B2BUA Component](#) on page 157
[Adding Dial Patterns for the Equinox B2BUA Component](#) on page 158

Adding a SIP Entity for the Equinox B2BUA Component

Before you begin

Log into System Manager by entering the following FQDN into your browser:

```
https://<FQDN_of_SystemManager>
```

Procedure

1. Navigate the **Elements** > **Routing** > **SIP Entities**.
2. Select **New**.
3. Enter values for the displayed fields, as indicated in the following table:

Table 18: SIP Entities Field Descriptions

Field Name	Description
Name	The name of the SIP entity.
FQDN or IP Address	The FQDN or IP address of the Equinox B2BUA component.
TYPE	Enter **SIP Trunk**
Adaptation	Depending on the dial plan of the system, create and select an adaptation.
Location	The location of the B2BUA component.
Time Zone	The time zone of the B2BUA component's location.

4. Select **Commit**.

Related links

Configuring Session Manager for Interoperability with the SIP-based Equinox B2BUA Component on page 156

Adding a SIP Entity Link/SIP Trunk For the Equinox B2BUA Component

Before you begin

Log into System Manager by entering the following FQDN into your browser:

`https://<FQDN_of_SystemManager>`

Procedure

1. Navigate to **Elements** > **Routing** > **Entity Links**.
2. Select **New**.
3. Enter values for the displayed fields, as indicated in the following table:

Table 19: SIP Entity Link Field Descriptions

Field Name	Description
Name	The name of the SIP entity.
SIP Entity 1	Select the relevant Session Manager.
Protocol	Enter **TLS**
Port	Enter **5061**
SIP Entity 2	Select the Equinox B2BUA component.
Port	Enter **5061**

4. In the **SIP Entity as Destination** section, click **Select**.
5. Select the relevant Equinox B2BUA component, and click **Select**.
6. Select **Commit**.

Related links

Configuring Session Manager for Interoperability with the SIP-based Equinox B2BUA Component on page 156

Adding Routing Policies For the Equinox B2BUA Component

Before you begin

Log into System Manager by entering the following FQDN into your browser:

`https://<FQDN_of_SystemManager>`

Procedure

1. Select **Elements** > **Routing** > **Routing Policies**.
2. Select **New**.
3. In the **Name** field, enter a name for the routing policy.
4. In the **SIP Entity as Destination** section, click the **Select** button.
5. Select the relevant Equinox B2BUA component, and click the **Select** button.
6. Select **Commit**.

Related links

Configuring Session Manager for Interoperability with the SIP-based Equinox B2BUA Component on page 156

Adding Dial Patterns for the Equinox B2BUA Component

Before you begin

Log into System Manager by entering the following FQDN into your browser:

`https://<FQDN_of_SystemManager>`

Procedure

1. Select **Elements** > **Routing** > **Dial Patterns**.
2. Select **New**.
3. Enter values for the displayed fields, as indicated in the following table:

Table 20: Dial Pattern Field Descriptions

Field Name	Description
Pattern	Enter a pattern, based on the system's dial plan.
Min	Enter a value, based on the system's dial plan.
Max	Enter a value, based on the system's dial plan.

4. In the **Originating Locations and Routing Policies** section, select **Add**.
5. Select the relevant Originating Location and Routing Policy, and click the **Select** button.
6. Select **Commit**.

Related links

Configuring Session Manager for Interoperability with the SIP-based Equinox B2BUA Component on page 156

Configuring Equinox Management for Interoperability with Avaya Aura®

The procedures in this section describe how to log into Equinox Management, how to add a SIP trunk from the Equinox B2BUA component to Session Manager, and how to change the default SIP domain in Equinox Management.

Logging into Equinox Management

In your browser's address bar, enter the Equinox Management FQDN in the following format:

```
https://<FQDN_or_IP_of_EquinoxManagement>:<port>/iview
```

Note:

Unless specified differently in the Equinox Management installation guidelines, use the default port **443** or **9443**.

Related links

Adding a SIP Trunk from the Equinox B2BUA Component to Session Manager on page 159
Changing the Default SIP Domain in Equinox Management on page 160

Adding a SIP Trunk from the Equinox B2BUA Component to Session Manager

Before you begin

Log into Equinox Management by entering the following FQDN in your browser:

```
https://<FQDN_or_IP_of_EquinoxManagement>:<port>/iview
```

Note:

Unless specified differently in the Equinox Management installation guidelines, use the default port **8080**.

Related links

Configuring Equinox Management for Interoperability with Avaya Aura on page 159
Adding a SIP Trunk in Equinox Management on page 159

Adding a SIP Trunk in Equinox Management

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Devices** > **Devices by Type** > **SIP Servers**, and select **Add**.
3. Enter values for the displayed fields, as indicated in the following table:

Table 21: SIP Entities Field Descriptions

Field Name	Description
Name	The name for the Session Manager.
IP Address/FQDN	The IP address of the SIP entity of Session Manager.
Port	Enter **5061**
Transport Type	Enter **TLS**
Model	Enter **Avaya Aura**
SIP Domain	Enter the SIP domain configured in System Manager.
Location	Select the appropriate location.

4. Select **OK** to submit.

Related links

Adding a SIP Trunk from the Equinox B2BUA Component to Session Manager on page 159

Changing the Default SIP Domain in Equinox Management

About this task

You can change the default SIP domain in the **From** header of Scopia Elite MCU calls to match the domain administered in Avaya Aura®.

Procedure

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

   The **Meeting Policies** page appears.

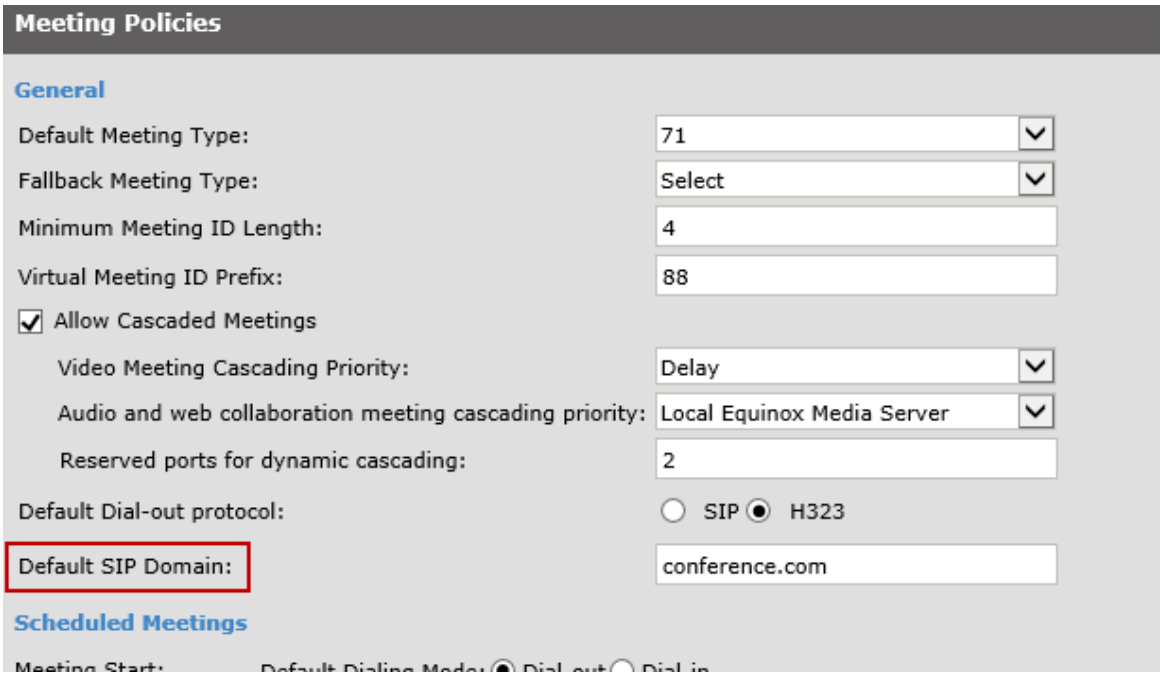


Figure 74: Meeting Policies Page

3. Enter the default SIP domain in the **Default SIP Domain** field.
4. Select **Apply**.

Related links

Configuring Equinox Management for Interoperability with Avaya Aura on page 159

Configuring Ad Hoc Conferencing in a Team Engagement (TE) Environment

When working in a 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 Aura® 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
  - Avaya IX™ Workplace Client version 3.2 and above
  - Avaya Equinox® Meetings for Web
- Servers
  - Avaya Equinox® Management version 9.0.2 and above
  - Avaya Aura® Web Gateway version 3.2 and above

Related links

Configuring Avaya IX Workplace Client settings on page 162
Configuring advanced parameters for ad hoc conferencing on page 164
Configuring the SIP Endpoint Managed Transfer Setting in Avaya Aura Communication Manager on page 165
Configuring Avaya Aura Communication Manager settings on page 166
Configuring Dial Plan settings on page 167
Configuring Equinox Management settings on page 168
Configuring System Manager settings on page 169
Escalating to a multipoint conference for a multiparty call using Avaya IX Workplace Client on page 172

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:

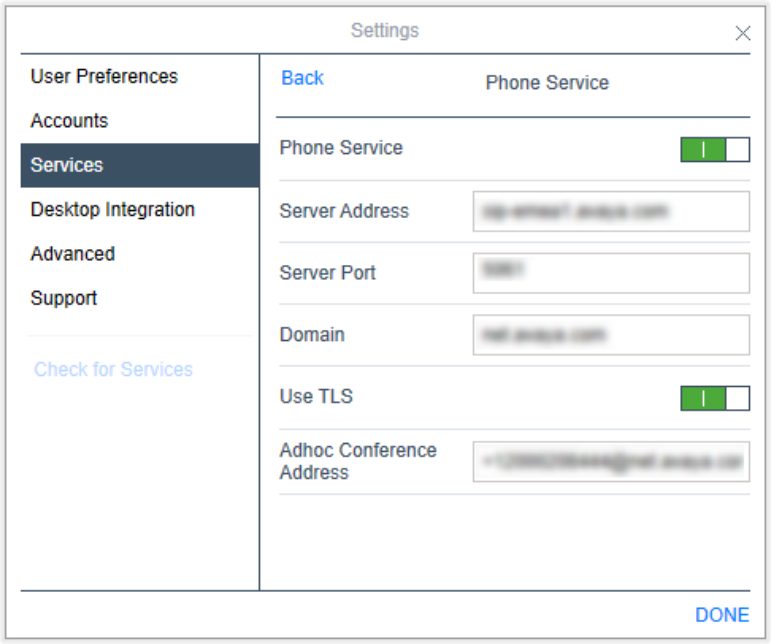


Figure 75: Meetings Pop-up Dialog

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

Configuring Ad Hoc Conferencing in a Team Engagement (TE) Environment on page 161

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.

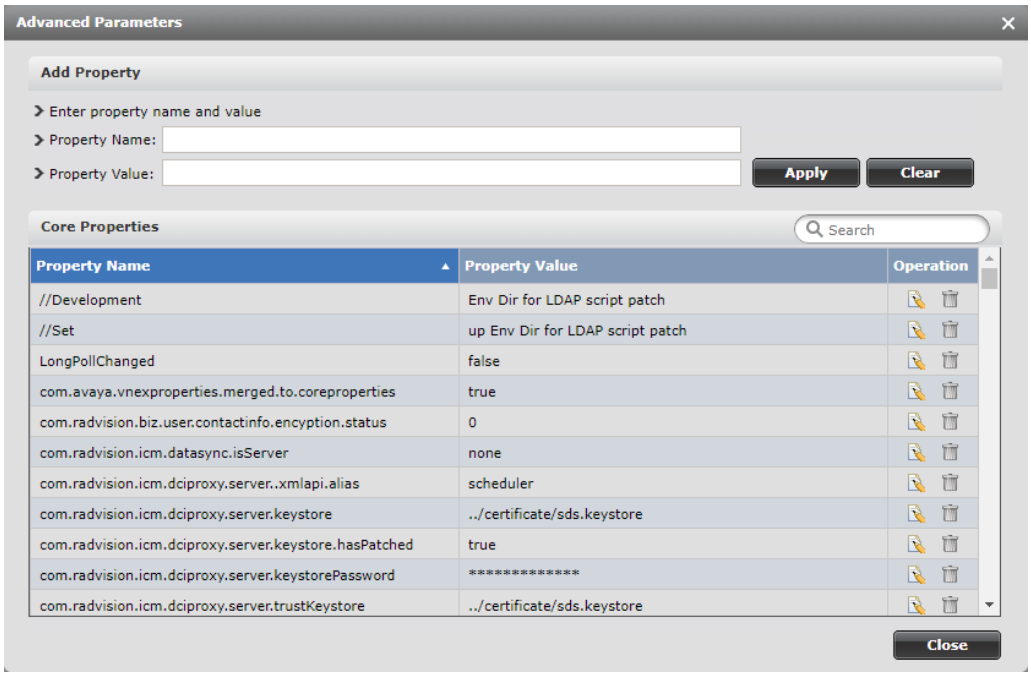


Figure 76: Advanced Parameters dialog box

3. Enter the indicated values in the fields described in the following table, click **Apply** after each one:

Table 22: Advanced Parameters Properties

Property Name Field	Property Value Field
vnex.vxmd.core.conference.factoryURI	<conference factory URI> For example: `816543@avayamcs.com`

Table continues…

Property Name Field	Property Value Field
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.

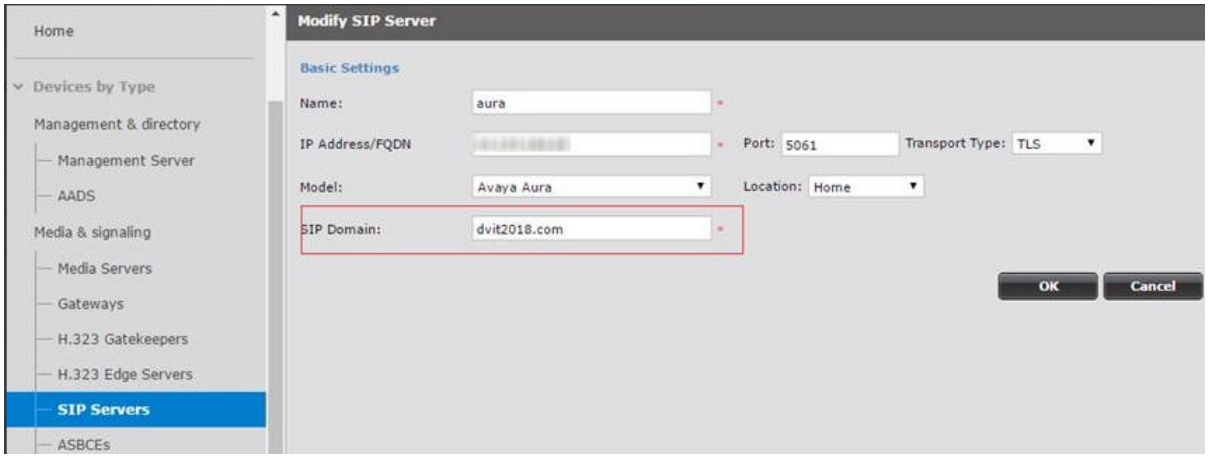


Figure 77: Modify SIP Server page

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

Configuring Ad Hoc Conferencing in a Team Engagement (TE) Environment on page 161

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 162.

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 78: SIP Endpoint Managed Transfer Setting

Related links

Configuring Ad Hoc Conferencing in a Team Engagement (TE) Environment on page 161

Configuring Avaya Aura® Communication Manager settings

About this task

Before ad hoc conferencing can be enabled, you must configure settings in Communication Manager.

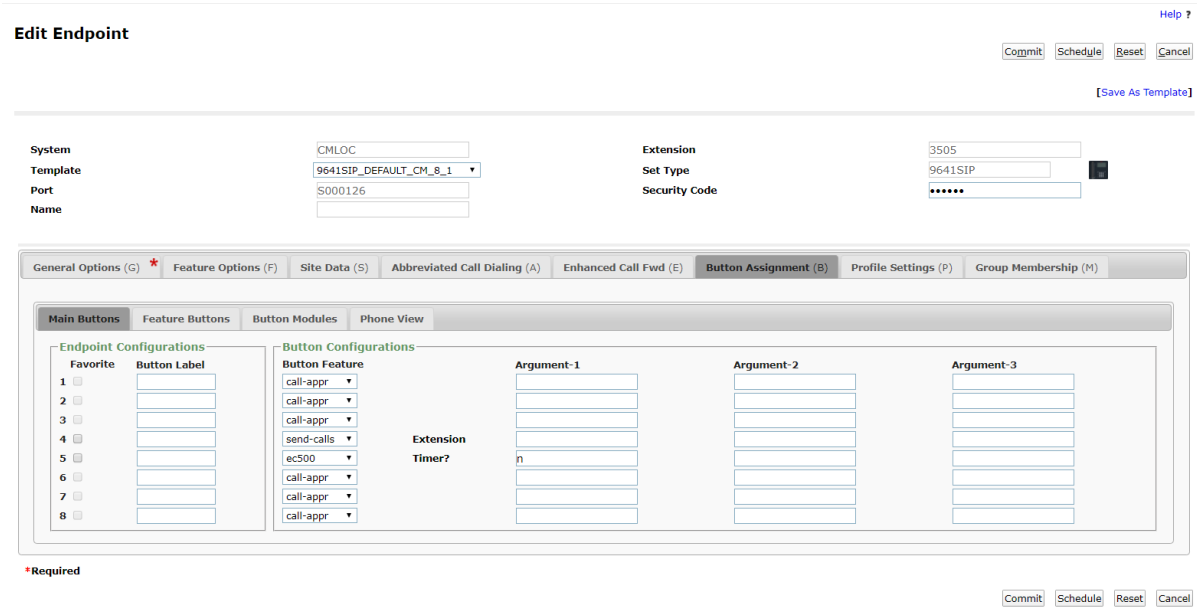
These configurations ensure that the phone interface displays the most frequently used buttons on the main screen, to optimize efficiency. You must configure eight call appearances for each Avaya IX™ Workplace Client extension.

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 165.

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

Configuring Ad Hoc Conferencing in a Team Engagement (TE) Environment on page 161

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 165.

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

Configuring Ad Hoc Conferencing in a Team Engagement (TE) Environment on page 161

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:

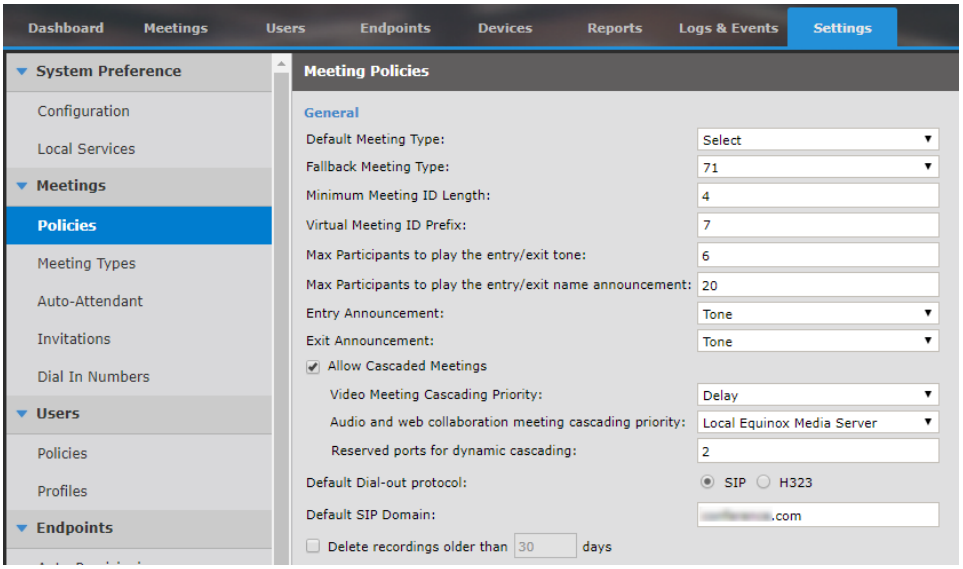
- Configuring Avaya IX Workplace Client settings on page 162
- Configuring the SIP Endpoint Managed Transfer Setting in Avaya Aura Communication Manager on page 165

- Configuring Dial Plan settings on page 167

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

Configuring Ad Hoc Conferencing in a Team Engagement (TE) Environment on page 161

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

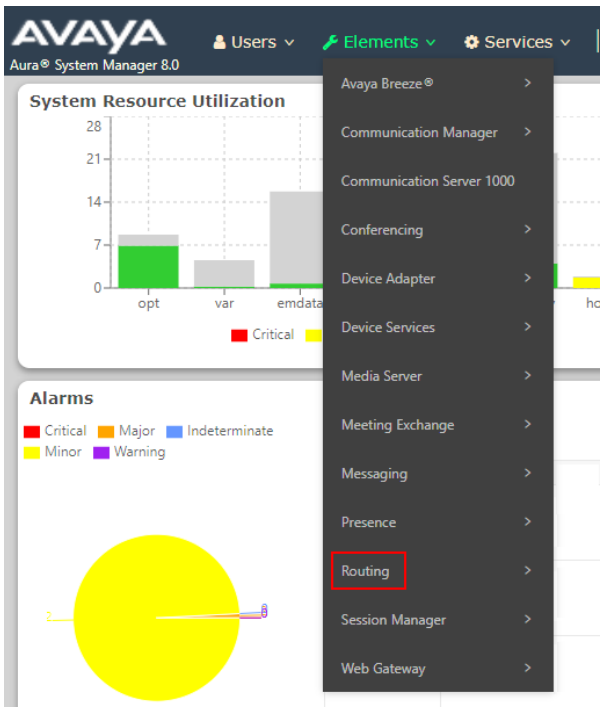
Ensure that you have completed the following configuration tasks:

- Configuring Avaya IX Workplace Client settings on page 162
- Configuring the SIP Endpoint Managed Transfer Setting in Avaya Aura Communication Manager on page 165

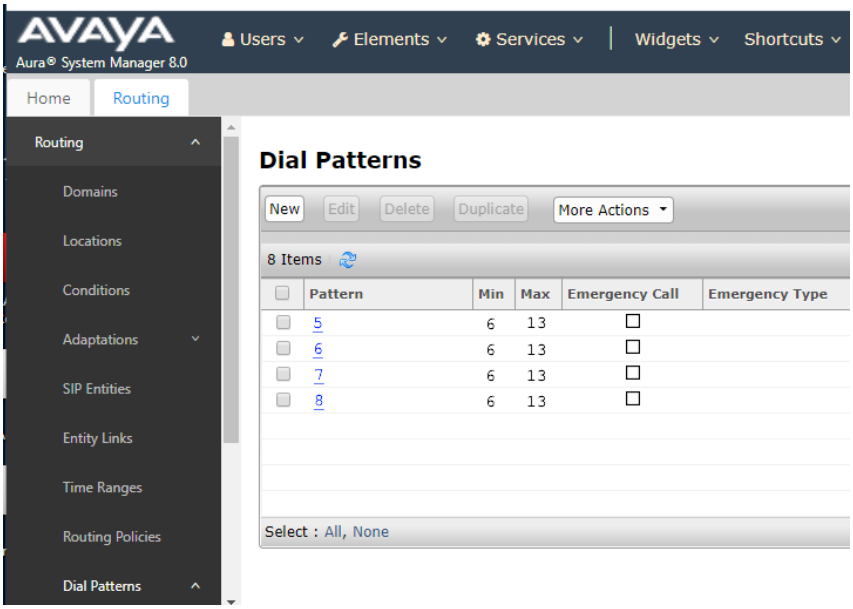
- Configuring Dial Plan settings on page 167
- Configuring Equinox Management settings on page 168

Procedure

1. In Avaya Aura® System Manager, click **Elements** > **Routing** > **Dial Patterns**.

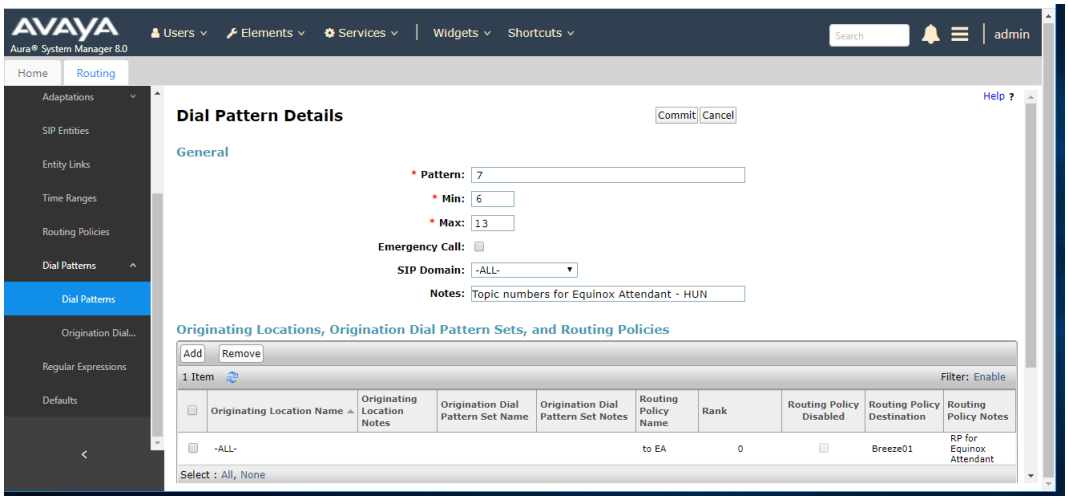


2. Configure the SIP trunk prefix (**7** in the following image, configured in the **Virtual Meeting ID Prefix** field on the **Meeting Policies** page; see Configuring Equinox Management settings on page 168.



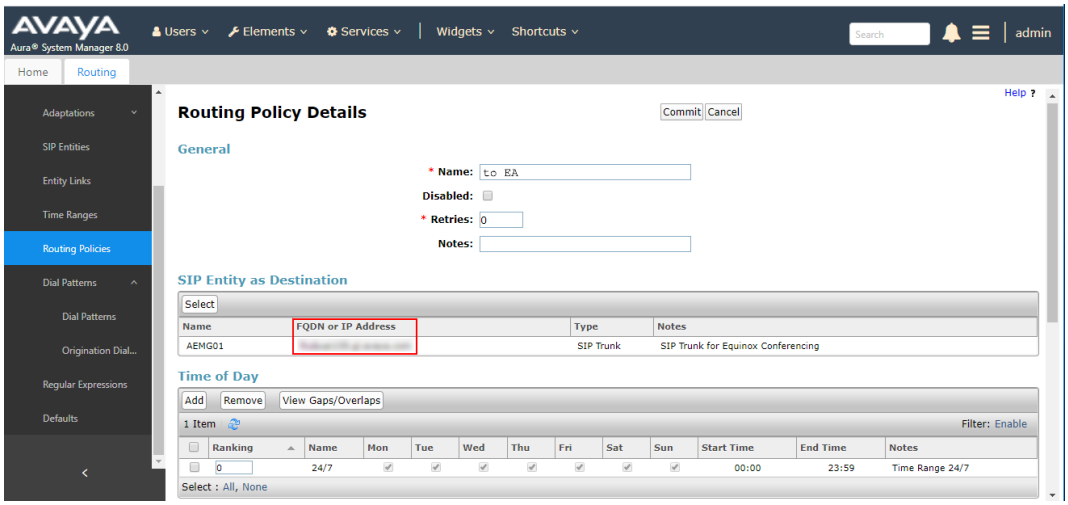
3. Select the relevant pattern.

   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

[Configuring Ad Hoc Conferencing in a Team Engagement (TE) Environment](#) on page 161

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 168) and System Manager (see Configuring System Manager settings on page 169), 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 162
- Configuring the SIP Endpoint Managed Transfer Setting in Avaya Aura Communication Manager on page 165
- Configuring Dial Plan settings on page 167

Procedure

1. Create a point-to-point call in Avaya IX™ Workplace Client.

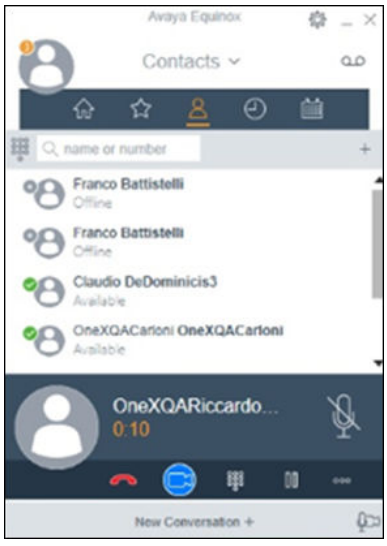


Figure 79: Point-to-point call

2. Drag and drop the relevant contact onto the active conversation.

   The system displays the following confirmation pop-up:



Figure 80: 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.

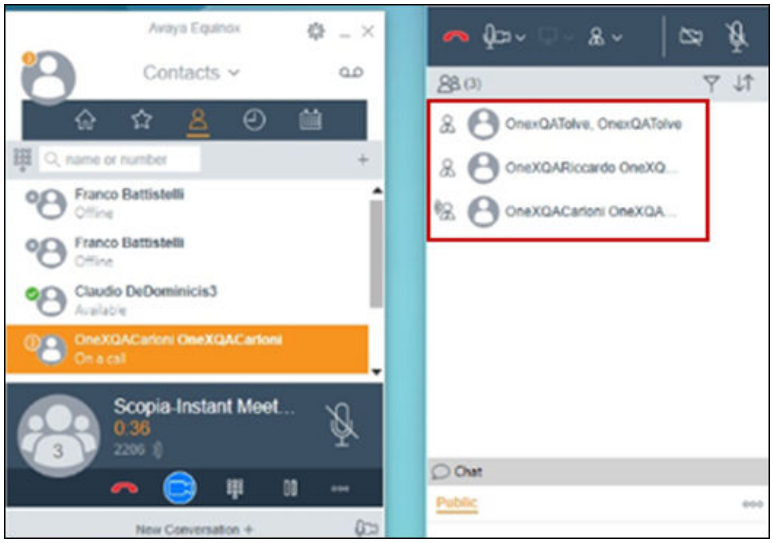


Figure 81: Multipoint conference

Related links

[Configuring Ad Hoc Conferencing in a Team Engagement (TE) Environment](#) on page 161

Chapter 7: Avaya Equinox Media Server deployment

Avaya Equinox® Media Server overview

Avaya Equinox® Media Server is a virtual media server with the following built-in components for media processing and real-time collaboration:

Component	Supports
MCU	• Transcoding and composition of video • Audio and video support for WebRTC-based thin clients • Web collaboration
Media server	• High-scale audio and multi-stream video • WebRTC gateway
Web collaboration server	Web collaboration

Avaya Equinox® Media Server processes all media on the server CPU and does not need media accelerator blades. Avaya Equinox® Media Server supports multiple technologies for processing audio and video, such as transcoding and switching, and is compatible with different types of enterprise deployments.

Avaya Equinox® Media Server is part of the Avaya Equinox® solution. Components of Avaya Equinox® can be combined to fit the existing network topology and video conferencing requirements of the organization. Avaya Equinox® Media Server is required in the Over The Top and Team Engagement deployments of Avaya Equinox®.

You can configure Avaya Equinox® Media Server as a master or slave server in distributed enterprise networks to support high-quality video, high-capacity audio, and web collaboration. You can configure Avaya Equinox® Media Server as a dedicated web collaboration server. You can also configure Avaya Equinox® Media Server as a cascaded gateway to Scopia® Elite 6000 MCU. As a cascaded gateway, Avaya Equinox® Media Server acts as a WebRTC gateway or as a dedicated web collaboration server.

Avaya Equinox® needs a WebRTC gateway deployed with Avaya Equinox® Media Server to process WebRTC calls. In Over The Top deployments, an instance of Avaya Equinox® Media Server configured as a WebRTC gateway processes WebRTC calls. In Team Engagement deployments, Avaya Aura® Media Server acts as the WebRTC gateway.

The performance and capacity of each Avaya Equinox® Media Server deployment depends on the physical cores, RAM, disk space, and the network interfaces allocated to the virtual machine.

Avaya Equinox® Media Server deployment checklist

No.	Task	Link/Notes	✔
1	Download the Avaya Equinox® Media Server software from Avaya PLDS.	Downloading software from PLDS on page 32	
2	Deploy the Avaya Equinox® Media Server virtual machine.	Deploying the Equinox Media Server virtual machine on page 182	
3	Start the Avaya Equinox® Media Server virtual machine.	Starting the Equinox Media Server virtual machine on page 184	
4	Configure the Avaya Equinox® Media Server virtual machine automatic startup settings.	Configuring the virtual machine automatic startup settings on page 184	
5	Add Avaya Equinox® Media Server in Avaya Equinox® Management	Adding Equinox Media Server in Equinox Management on page 185	
6	Configure the Avaya Equinox® Media Server network settings.	Configuring the Equinox Media Server network settings on page 188	

Avaya Equinox® Media Server video conferencing mode administration checklist

Use this checklist to configure Avaya Equinox® Media Server as a media server for video conferencing and web collaboration.

No.	Task	Link/Notes	✔
1	Deploy the Avaya Equinox® Media Server virtual machine.	Deploying the Equinox Media Server virtual machine on page 182	
2	Start the Avaya Equinox® Media Server virtual machine.	Starting the Equinox Media Server virtual machine on page 184	
3	Add Avaya Equinox® Media Server in Avaya Equinox® Management	Adding Equinox Media Server in Equinox Management on page 185	
4	Apply the Avaya Equinox® Media Server video conferencing and web collaboration license.	Checklist for configuring Avaya Equinox® Media Server licenses on page 430	

Table continues…

No.	Task	Link/Notes	✔
5	Secure the connection between Avaya Equinox® Media Server and Avaya Equinox® Management	Securing the connection between Equinox Media Server and Equinox Management on page 194	

Avaya Equinox® Media Server audio-only conferencing mode administration checklist

Use this checklist to configure Avaya Equinox® Media Server as a media server for audio-only conferencing and web collaboration.

No.	Task	Link/Notes	✔
1	Deploy the Avaya Equinox® Media Server virtual machine.	Deploying the Equinox Media Server virtual machine on page 182	
2	Start the Avaya Equinox® Media Server virtual machine.	Starting the Equinox Media Server virtual machine on page 184	
3	Add Avaya Equinox® Media Server in Equinox Management.	Adding Equinox Media Server in Equinox Management on page 185	
4	Apply the Avaya Equinox® Media Server audio-only conferencing and web collaboration license.	Checklist for configuring Avaya Equinox® Media Server licenses on page 430	
5	Install security certificates for TLS.	• Creating security certificates on page 191 • Uploading security certificates on page 193	
6	Secure the connection between Avaya Equinox® Media Server and Avaya Equinox® Management.	Securing the connection with Equinox Management using TLS on page 194	
7	Change the working mode of Avaya Equinox® Media Server to High Capacity Audio + Web Collaboration.	Changing the Equinox Media Server working mode on page 190	
8	Upload the audio prompts.	Customizing audio messages on page 191	

Avaya Equinox® Media Server web collaboration mode administration checklist

Use this checklist to configure Avaya Equinox® Media Server as a media server for only web collaboration.

No.	Task	Link/Notes	✔
1	Deploy the Avaya Equinox® Media Server virtual machine.	Deploying the Equinox Media Server virtual machine on page 182	
2	Start the Avaya Equinox® Media Server virtual machine.	Starting the Equinox Media Server virtual machine on page 184	
3	Add Avaya Equinox® Media Server in Avaya Equinox® Management.	Adding Equinox Media Server in Equinox Management on page 185	
4	Apply the Avaya Equinox® Media Server web collaboration-only license.	Checklist for configuring Avaya Equinox® Media Server licenses on page 430	
5	Secure the connection between Avaya Equinox® Media Server and Avaya Equinox® Management	Securing the connection between Equinox Media Server and Equinox Management on page 194	

Avaya Equinox® Media Server WebRTC gateway administration checklist

Use this checklist to configure Avaya Equinox® Media Server as a WebRTC gateway.

No.	Task	Link/Notes	✔
1	Deploy the Avaya Equinox® Media Server virtual machine.	Deploying the Equinox Media Server virtual machine on page 182	
2	Start the Avaya Equinox® Media Server virtual machine.	Starting the Equinox Media Server virtual machine on page 184	
3	Add Avaya Equinox® Media Server as a gateway in Avaya Equinox® Management.	Adding Equinox Media Server as a gateway on page 186	
4	Apply the Avaya Equinox® Media Server WebRTC-only license.	Checklist for configuring Avaya Equinox® Media Server licenses on page 430	
5	Install security certificates for TLS.	• Creating security certificates on page 191 • Uploading security certificates on page 193	

Table continues…

No.	Task	Link/Notes	✔
6	Secure the connection between Avaya Equinox® Media Server and Avaya Equinox® Management.	Securing the connection with Equinox Management using TLS on page 194	

Technical specifications of Avaya Equinox® Media Server

- The Huge configuration requires customer-provided servers that support the 2S-3 UPI topology. The 2S-3 UPI topology supports three UPI links between server CPUs, which improves the server performance and efficiency.
- The Medium configuration requires the following CPU configuration to support the 1080p*60fps video resolution:
  - Server CPU speed: More than 2.4Ghz
  - CPU reservation: 27000MHz

Deployment-specific virtual machine requirement

Requirement	Huge configuration	Ultra High configuration	Ultra High configuration with 60fps video	High configuration	High configuration with 60fps video	Medium configuration	Medium configuration with 60fps video	Low configuration
Server CPU cores	48	24	24	16	16	12	12	6
Virtual cores	48	48	24	32	16	12	12	6
CPU reservation in MHz	120000	55000	54780	35000	34860	21800	27000	9900
2.5” SAS hard disk capacity in MB	122800	122800	122800	122800	122800	122800	122800	122800
RAM reservation in MB	147000	58000	58000	20000	20000	13000	13000	10000

Table continues…

Requirement	Huge configuration	Ultra High configuration	Ultra High configuration with 60fps video	High configuration	High configuration with 60fps video	Medium configuration	Medium configuration with 60fps video	Low configuration
Disk space reservation in MB	120000	120000	120000	120000	120000	120000	120000	120000
NIC	2	2	2	2	2	2	2	2
Maximum licenses applicable in Over The Top deployment	8	4	4	2	2	1	1	Only for migrations from existing Avaya Aura® Conferencing deployments

Capacity and scalability

Maximum ports supported

- In the Full Audio, Video, and Web Collaboration working mode, the maximum supported ports for 720p*30fps video is exclusive of audio ports.
- In the High Capacity Audio, Multi-Stream Video and Web Collaboration mode, the maximum supported ports for audio in each deployment type also includes support for web collaboration.
- The Low configuration deployment is only for migrations from existing Avaya Aura® Conferencing deployments when you need to use the existing server. The Low configuration applies only to Avaya Equinox® Team Engagement deployments and supports a maximum of 200 audio-only ports with web collaboration.

Deployment configuration	Maximum ports supported for a specific video resolution				
	1080p*60fps	1080p*30fps	720p*60fps	720p*30fps	480p*30fps
Huge	20	40	40	80	120
Ultra High	—	20	—	40	80
Ultra High with 60fps video	10	20	20	40	80

Table continues…

Deployment configuration	Maximum ports supported for a specific video resolution				
	1080p*60fps	1080p*30fps	720p*60fps	720p*30fps	480p*30fps
High	—	10	—	20	40
High with 60fps video	5	10	10	20	40
Medium	—	5	—	10	20
Medium with 60fps video	3	5	5	10	20

Full Audio, Video, and Web Collaboration mode ports capacity

The port allocation is based on the resources that each user needs. Different users need different amount of resources based on the video resolution of the connections. Meetings can have multiple users that need a different amount of resources based on the video resolution of the connection. For example, users with connections at 480p*30fps video resolution use 25% of the resources of users with connections at 1080p*30fps video resolutions or 50% of the resources of users with connections at 720p*30fps.

Equinox Media Server supports 1080p*60fps and 720p*60fps video resolutions as optional features. You must manually enable the video resolutions for video calls.

Deployment configuration	Port-based licenses for Over The Top deployments	Maximum ports supported for video				Audio using G.711 codec	Web collaboration
		1080p*60fps using H.264 codec	1080p*30fps and 720p*60fps using H.264 codec 720p*30fps using VP8 codec	720p*30fps using H.264 codec 480p*30fps using VP8 codec	480p*30fps using H.264 codec		
Huge	8	20	40	80	120	120	120
Ultra High	4	10	20	40	80	80	160
Ultra High	3	7	15	30	60	60	120
High	2	5	10	20	40	40	80
Medium	1	3	5	10	20	20	40

High Capacity Audio, Multi-Stream Video and Web Collaboration mode ports capacity

The Low configuration deployment is only for migrations from existing Avaya Aura® Conferencing deployments when you need to use the existing server. The Low configuration applies only to Avaya Equinox® Team Engagement deployments and supports a maximum of 200 audio-only ports with web collaboration.

The video stream uses H.264 SVC for receiving video and H.264 AVC for transmitting video. The multi-stream video uses one H.264 SVC stream for receiving and four H.264 SVC streams for transmitting video.

Deployment configuration	Port-based licenses for Over The Top deployments	Maximum support ports for audio, multi-stream video, and web collaboration			Audio-only Audio and web collaboration	
		720p*30fps video using H.264 codec and audio using G.711 codec Single active speaker window	360p*30fps video using H.264 codec and audio using G.711 codec Single active speaker window	360p*30fps video using H.264 codec and audio using G.711 codec Multi-stream 4–window switching	Audio using G.711 codec	Web collaboration
Ultra High	4	1200	1400	700	2000	2000
Ultra High	3	900	1050	525	1500	1500
High	2	600	700	350	1000	1000
Medium	1	300	350	175	500	500
Low	Only for migrations from existing Avaya Aura® Conferencing deployments	—	—	—	200	200

Ports configuration

For information about configuring ports for Equinox Media Server, see *Avaya Port Matrix — Avaya Equinox® Product Offerings* on the Avaya Support website at http://support.avaya.com/.

Downloading software from PLDS

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon ( ) for Company Name.
6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type `Avaya` or the Partner company name.
   b. Click **Search Companies**.

c. Locate the correct entry and click the **Select** link.

7. Search for the available downloads by using one of the following:
   - In **Download Pub ID**, type the download pub ID.
   - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. Scroll down to the entry for the download file, and click the **Download** link.
10. Select a location where you want to save the file, and click **Save**.
11. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.
12. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Deploying the Equinox Media Server OVA

Deploying the Avaya Equinox® Media Server virtual machine

About this task

The Avaya Equinox® Media Server virtual machine software for VMware is available in the .OVA package format. If you have vCenter, deploy the OVA image with vCenter. Use an ESXi host client only if VCenter does not manage the host. The virtual machine configuration file and virtual disk files are stored in a data store. The data store can be local to the host or a mounted shared storage, such as NFS or SAN.

If multiple virtual machine networks are configured on the host ESXi server, associate networks specified in the OVA with networks available on the host server.

Before you begin

- Download the Avaya Equinox® Media Server OVA to your computer.
- If you deploy Avaya Equinox® Media Server on:
  - VMware ESXi host, ensure that the host server software is Release 6.5 or 6.7.
  - Appliance Virtualization Platform, ensure that the platform version is Release 8.1 or later.

Procedure

1. Log in to VMware vSphere.
2. Click **Launch vSphere Client (HTML5)**.
3. Click **File** > **Deploy OVF Template**.

vSphere Client displays the Deploy OVF Template wizard.

4. Do one of the following:
   - Select **URL**, and enter the full URL of the HTTP server where the Avaya Equinox® Media Server OVA file is located.
   - Select **Local File**, and choose the Avaya Equinox® Media Server OVA file from the local folder.
5. Click **Next** .
6. Do the following for the new virtual machine:
   a. Type the name.
   b. Select the location from the inventory tree.
7. Click **Next** .
8. Select a compute resource from the inventory tree, and click **Next**.
9. Verify the details of the OVA template, and click **Next**.
10. Read the license agreement, and select **I accept all license agreements**.
11. Click **Next**.
12. Select the deployment capacity, and click **Next**.

    The deployment capacity must be within the server hardware limits and the license capacity.
13. Do the following:
    a. In **Select virtual disk format**, select **Thick Provision Eager Zeroed**.
    b. Select a data store to store the virtual machine files.

       Select a data store large enough to accommodate the virtual machine and the virtual disk files.
14. Click **Next** .

    If the host server has multiple virtual machine networks, vSphere Client displays the Network Mapping window to associate networks specified in the OVA with the networks on the host server.
15. From the **Destination Network** drop-down list, select a network, and click **Next**.
16. Configure the following fields:
    - **Default Gateway**
    - **Public IP Address**
    - **Public Netmask**

    This configuration is for the internal network.

Note:

vSphere Client displays the Customize template window to configure IP addresses only if you use VMWare vSphere. You cannot configure the IP addresses in the vSphere console.

17. Click **Next**.
18. Verify the deployment settings, and click **Finish**.

Result

vSphere Client starts the Avaya Equinox® Media Server OVA deployment.

Related links

Configuring the Equinox Media Server IP addresses using vSphere Client Console
Configuring the Equinox Media Server network settings on page 188
Technical specifications of Avaya Equinox® Media Server on page 178

Starting the Avaya Equinox® Media Server virtual machine

Before you begin

Deploy the Avaya Equinox® Media Server virtual machine.

Procedure

1. Log in to vSphere Client.
2. Click **Inventory**.
3. Click **Virtual Machine** > **Power** > **Power On**.

Result

The Avaya Equinox® Media Server virtual machine starts.

Related links

Technical specifications of Avaya Equinox® Media Server on page 178

Configuring the virtual machine automatic startup settings on VMware

About this task

When a vSphere ESXi host restarts after a power failure, the virtual machines that are deployed on the host do not start automatically. You must configure the virtual machines to start automatically.

In high availability (HA) clusters, the VMware HA software does not use the startup selections.

Before you begin

Verify with the ESXi system administrator that you have the permissions to configure the automatic startup settings.

Procedure

1. In the web browser, type the vSphere vCenter host URL.
2. Click one of the following icons: **Hosts and Clusters** or **VMs and Templates** icon.
3. In the navigation pane, click the host where the virtual machine is located.
4. Click **Configure**.
5. In Virtual Machines, click **VM Startup/Shutdown**, and then click **Properties**.

   The software displays the Edit VM Startup and Shutdown window.
6. Click **Automatically start and stop the virtual machines with the system**.
7. Click **OK**.

Equinox Media Server initial configuration

Adding Equinox Media Server in Equinox Management

About this task

Manage Equinox Media Server using Equinox Management.

Before you begin

Get the following details:

- IP address of Equinox Media Server
- IP address of the gatekeeper
- Location of Equinox Media Server if the deployment has multiple locations

Procedure

1. Log in to Equinox Management.
2. Click **Devices**.
3. Click **Media Servers** in the left pane.

   Equinox Management displays the Media Servers window.
4. Click **Add**.

   Equinox Management displays the Add Media Server window.

5. Configure the following fields:
   - **Name**
   - **IP Address**
   - **Registered To**
   - **Location**

Result

Equinox Management adds the Equinox Media Server instance as a device.

Add Media Servers field descriptions

Name	Description
Name	The name of the media server. The name is used to identify specific media server instances in the list of media servers.
IP Address	The management IP address configured during the installation.
Registered To	The drop-down list containing the registered gatekeepers. If you select **None**, you can add the media server to Equinox Management, but the media server will not be connected to the network.
Location	The location of the media server. The location of the media server is only relevant in deployments with multiple locations.

Adding Equinox Media Server in Equinox Management as a gateway

About this task

Equinox Media Server as a WebRTC gateway is deployed as a cascaded server of Scopia® Elite 6000 MCU and manages all the WebRTC traffic of conference participants who join conferences using web browsers.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**.
3. Click **Gateways** in the left pane.

   Equinox Management displays the Gateways window.

4. Click **Add**.
5. Configure the following fields:
   - **Name**
   - **IP Address**
   - **Model**
   - **Registered To**
   - **Location**

Result

Equinox Management adds Equinox Media Server as a WebRTC gateway.

Next steps

Configure Equinox Media Serverdeployed as a WebRTC gateway to process all WebRTC-based calls.

Related links

Applying the Avaya Equinox® Media Server licenses on page 432

Add Gateway field descriptions

Name	Description
Name	The name of the WebRTC gateway. The name is used to identify specific media server instances in the list of media servers.
IP Address	The management IP address configured during the installation.
Model	The role of the gateway. **Avaya WebRTC Gateway** is specifically used to configure Equinox Media Server as a gateway for web browser-based conferences.
Registered To	The drop-down list containing the registered gatekeepers. If you select **None**, you can add the media server to Equinox Management, but the media server will not be connected to the network.
Location	The location of the media server. The location of the media server is only relevant in deployments with multiple locations.

Configuring the Equinox Media Server network settings

Before you begin

- Decide a descriptive name for Equinox Media Server.
- If the deployment has multiple locations, get the location of the Equinox Media Server instance.
- If you deploy Equinox Media Server as a web collaboration gateway, get FQDN.
- Get the network IP addresses of:
  - NTP server
  - DNS servers
  - Default gateway
  - SIP proxy server

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Equinox Media Server instance.

   Equinox Management opens the media server window.
3. Click the **Configuration** tab.
4. Configure the network settings.
5. Click **Apply**.

Configuration field descriptions

Name	Description
Basic Settings	
Name	The name of the Equinox Media Server instance. Enter a name that indicates the location and working mode of Equinox Media Server.
Location	The location of Equinox Media Server in the enterprise network. This field is relevant only if there are multiples locations in the deployment.
Service FQDN	The FQDN of Equinox Media Server. This field is relevant only if you deploy Equinox Media Server as a web collaboration server.

Table continues…

Name	Description
Public URL branch	The public URL branch of Equinox Media Server. The public URL branch supports deploying multiple Equinox Media Server instances using one public FQDN. For example, `<FQDN>/Equinox Media Server1`. The public URL branch configuration must be identical in all Equinox Media Server instances.
In Maintenance	The option to change Equinox Media Server to inactive mode for maintenance. In the maintenance mode, you can configure settings and perform upgrades, but you cannot use the Equinox Media Server instance.
Secure Connection	The option to enable a permanent secure connection between Equinox Media Server and Equinox Management using TLS. You can use this option only if you installed security certificates for TLS.
Master Media Server for Cascading	The option 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 that sets the time for Equinox Media Server. If there is no NTP server, the value of the field must be `0.0.0.0`.
NTP Time Zone	The time zone where the NTP server is configured.
Network Settings	
DNS Server 1	The IP address of the DNS server.
DNS Server 2	The IP address of the secondary DNS server.
DNS Search List	The short name of the DNS server that Equinox Media Server uses to search other websites. Equinox Media Server searches the DNS search list for the suffix.
IP Address	The IP address of Equinox Media Server
Subnet Mask	The subnet mask of Equinox Media Server.
Default Gateway	The default gateway of Equinox Media Server.

Table continues…

Name	Description
Local FQDN	FQDN of Equinox Media Server. The local FQDN must be identical to the service FQDN.
H.323 Settings	
Required Gatekeeper	The drop-down list of the available gatekeepers.
Current Gatekeeper	The IP address of the current gatekeeper.
SIP Settings	
SIP Proxy Server	The IP address of the SIP server.
Transport Type	The transport protocol of the SIP server. The options are: • **TCP** • **UDP** • **TLS**
Turn/Stun Servers	The IP address of the session border controller. This field is applicable only if you deploy Equinox Media Server as a WebRTC gateway.

Changing the Equinox Media Server working mode

Before you begin

- Add the Media Server license to the Equinox Media Server instance.
- To change the working mode to High Capacity Audio, Multi-Stream Video and Web Collaboration, do the following:
  - Deploy and configure Equinox Media Server for the audio-only conferencing mode.
  - Install the security certificate for TLS.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Equinox Media Server instance.

   Equinox Management opens the media server window.
3. Click **Change** next to **Working Mode**.

   You can change the working mode to one of the following two modes:

   • Full Video + Web Collaboration: This is the default mode.

   • High Capacity Audio, Multi-Stream Video and Web Collaboration

   Equinox Management displays a confirmation message.

4. Click **Yes**.

Customizing audio messages

About this task

You can customize the default audio messages. You can upload a single customized audio message or a compressed file containing all the customized messages.

Before you upload your customized audio messages, download the existing audio messages pack. You can also use this messages pack to inspect the message file naming convention.

Procedure

1. Log in to Equinox Management.
2. Click **Settings**.
3. On the left pane, click **Advanced** > **Customization**.

   Equinox Management displays the Customization window.
4. In **Current Package**, select a language, and click the Update icon.

   Equinox Management displays the Update Voice Prompt Package dialog box.
5. Click **Update Language Package**, and select the compressed file pack containing the audio messages.

   The audio messages in the compressed file pack must be in the `.wav` format and encoded with G.711 (CCITT), 8-bit, 8kHz mono. The file pack must be maximum 3Mb.
6. Click **OK**.
7. Click **Apply**.

Secure connection with Equinox Management

Creating security certificates

About this task

TLS certificates, issued by a trusted certification authority, contain the public encryption keys of Equinox Media Server that are used over the network to ensure authentication and encryption of the network connection.

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.

Note:

Equinox Media Server does not support wildcard certificates.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and click the name of the Equinox Media Server instance.

   Equinox Management displays the Equinox Media Server instance window.
3. Click the **Certificate** tab.
4. Click **Create**.

   Equinox Management displays the Generate CSR window.
5. Configure the following fields:
   - **Common name**
   - **Subject Alternative Name**
   - **Organizational Unit**
   - **Organization**
   - **City**
   - **State**
   - **Country Code**
   - **Encryption Strategy**
   - **Signature Algorithm**
6. Click **Generate CSR**.
7. Click **Save** to view the certificate.

   Equinox Management displays the certificate in the Download window.
8. Save the certificate signing request.

   Equinox Management saves the certificate as a CSR file that is compatible with the Base-64 ASCII code.
9. Send the CSR file containing the certificate to the certification authority for signing.

   Select **Web Server** as the certificate template when you submit the certificate request.

Result

The certification authority will send back a signed certificate.

Next steps

Upload the certificates.

Generate CSR field descriptions

Name	Description
Common Name	The Equinox Media Server FQDN. For a redundant deployment, the common name must be the public virtual FQDN.
Subject Alternative Name	The alternate host name of Equinox Media Server to include in the certificate.
Country Code	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	The code for the encryption strategy. The options are: • **1024**: Choosing this option might cause weak encryption. • **2048** • **4096**
Signature Algorithm	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. The options are: • **SHA1withRSA**: Choosing this option might cause weak encryption. • **SHA256withRSA**

Uploading security certificates

About this task

TLS certificates from CA must be uploaded to Equinox Media Server to ensure authentication and encryption of the network connection.

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

Generate the certificates.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and click the name of the Equinox Media Server instance.

   Equinox Management displays the Equinox Media Server instance window.

3. Click the **Certificate** tab.
4. Click **Upload**.

   Equinox Management displays the Upload certificates window.
5. Click **Add**, and browse to the certificates.

   Repeat this step for all certificates.

   Equinox Management displays a confirmation message after each certificate is uploaded.
6. Click **Apply All**.

Result

Equinox Media Server automatically restarts.

Securing the connection between Equinox Media Server and Equinox Management

About this task

Equinox Management might restart Equinox Media Server to secure the connection when you change the transport type to TLS.

Note:

Before you remove an Equinox Media Server instance from Equinox Management, clear the **Secure connection** check box.

Before you begin

Install the security certificates for TLS.

Procedure

1. Log in to Equinox Media Server.
2. Click **Devices**.
3. In the left pane, click **Media Servers**.

   Equinox Management displays the Media Servers page.
4. Click the name of the Equinox Media Server instance.

   Equinox Management displays the Equinox Media Server instance page.
5. Click the **Configuration** tab.
6. Select the **Secure connection** check box.
7. Click **Test Connection** to check the secure connection.

   Equinox Management displays a confirmation that the test is successful.
8. Click **OK**.
9. Click **Apply**.

Equinox Management displays a prompt to warn that Equinox Media Server will be restarted and all meetings in progress will be disconnected.

10. Click **Yes**.

Result

- Equinox Management restarts Equinox Media Server.
- The connection between Equinox Media Server and Equinox Management is secured using TLS.

Chapter 8: Deploying the Avaya Equinox Recording Gateway OVA

Avaya Equinox Recording Gateway deployment checklist

No.	Task	Link/Notes	✔
1	Download theEquinox Recording Gateway software from Avaya PLDS.	Downloading software from PLDS on page 32	
2	Deploy the Equinox Recording Gateway virtual machine.	Deploying the Avaya Equinox Recording Gateway virtual machine on page 196	
3	Start the Equinox Recording Gateway virtual machine.	Starting the Avaya Equinox Recording Gateway virtual machine on page 199	
4	Configure the Equinox Recording Gateway virtual machine automatic startup settings.	Configuring the virtual machine automatic startup settings on page 184	
5	Add Equinox Recording Gateway in Equinox Management	Adding Equinox Recording Gateway in Equinox Management on page 201	
6	Configure the Equinox Recording Gateway network settings.	Configuring the Equinox Recording Gateway network settings on page 201	

Deploying the Avaya Equinox® Recording Gateway virtual machine

About this task

The Avaya Equinox® Recording Gateway virtual machine software for VMware is available in the .OVA package format. If you have vCenter deployed you must deploy the OVA image with vCenter, you must only use an ESXi host client if the host is not managed by vCenter. The virtual machine configuration file and virtual disk files are stored in a data store. The data store can be local to the host or a mounted shared storage, such as NFS or SAN.

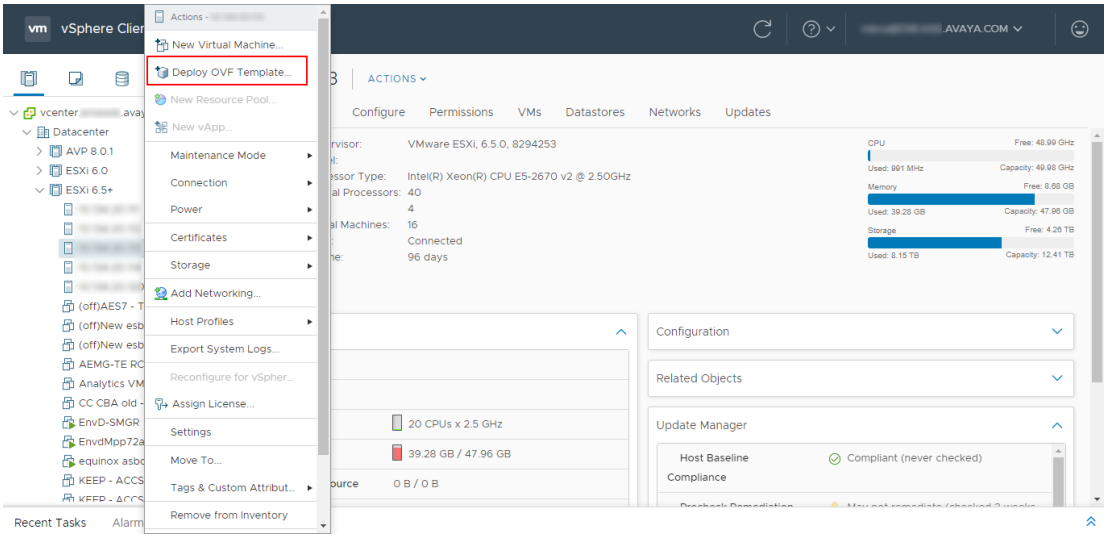
If multiple virtual machine networks are configured on the host ESXi server, you must associate networks specified in the OVA with networks available on the host server.

Before you begin

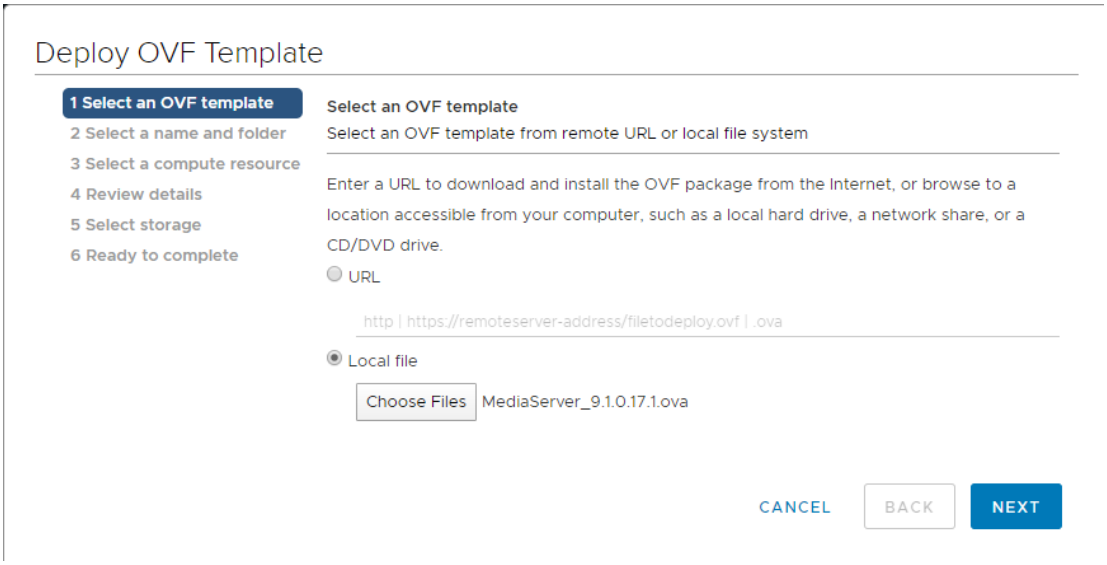
- Download the Avaya Equinox® Recording Gateway OVA to your computer.
- Ensure that the VMware ESXi host server software is Release 6.0, 6.5, or 6.7.
- If you deploy Avaya Equinox® Recording Gateway on Appliance Virtualization Platform, ensure that the Appliance Virtualization Platform version is Release 8.0 or 8.1.
- Review the prerequisites for software installation on the customer's hardware.
- Review the technical specifications for Avaya Equinox® Media Server. The Avaya Equinox® Recording Gateway technical specifications are the same, see Technical specifications of Avaya Equinox® Media Server on page 178.

Procedure

1. Log in to VMware vSphere.
2. Launch vSphere Client (HTML5).
3. Click **File** > **Deploy OVF Template**.
4. Highlight the datacenter, cluster or host to deploy the new media server instance, right-click and select **Deploy OVF Template**.



5. Do one of the following to deploy the Avaya Equinox® Recording Gateway OVF package:
   - Click **Browse** and provide the Avaya Equinox® Recording Gateway OVA file location.
   - In the **Deploy from a file or URL** field, enter the full URL of the HTTP server where the Avaya Equinox® Recording Gateway OVA file is located.



6. Click **Next** to display the OVF Template wizard.
7. Verify the details of the OVA template, and click **Next**.
8. In the **Virtual machine name** field, enter the name of the new virtual machine, and click **Next**.
9. Select a compute resource from the inventory location tree where you want this virtual machine to reside, and click **Next**.
10. Review the details, and click **Next**.
11. Accept the license agreements, and click **Next**.
12. Select the deployment capacity in the **Configuration** list, and click **Next**.

    The deployment capacity must be within the server hardware limits and the license capacity.
13. Select a data store location to store the virtual machine files.

    Select a data store large enough to accommodate the virtual machine and the virtual disk files.
14. Select **Thick Provision Lazy Zeroed**, and click **Next**.

    If the host server has multiple virtual machine networks, vSphere Client displays the Network Mapping page to associate networks specified in the OVA with the networks on the host server.
15. From the **Destination Network** drop-down list, select a network option, and click **Next**.

    vSphere Client displays the properties on the Customize template page.
16. Configure the following IP addresses:
    - **Default Gateway**

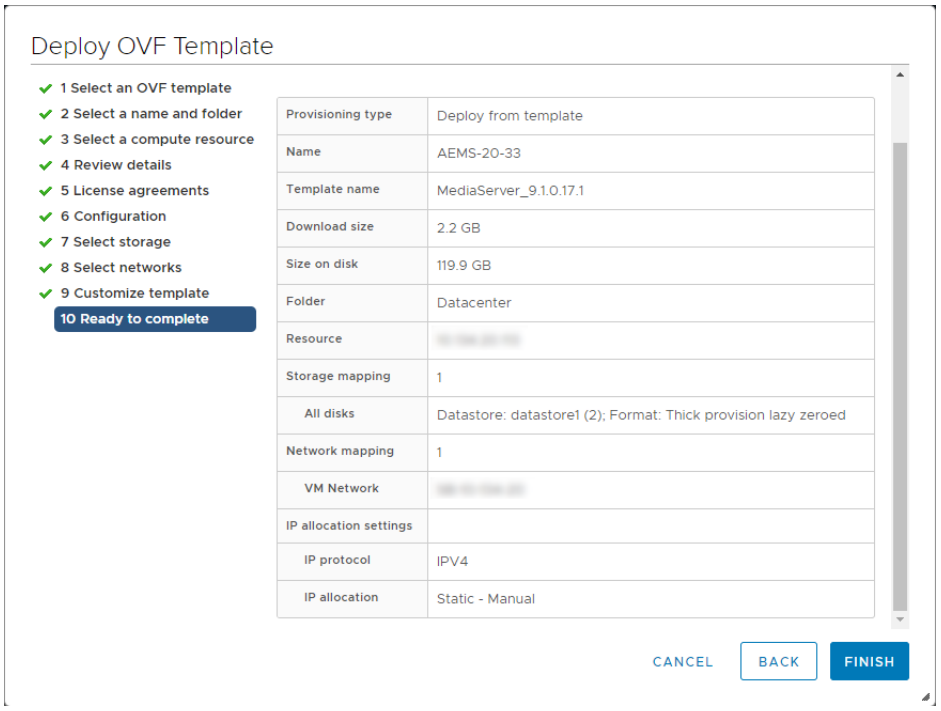
- **Public IP Address**
- **Public Netmask**

This configuration is for the internal network.

Note:

vSphere Client displays the Customize template page to configure IP addresses only if you use VMware vSphere. From Avaya Equinox® release 9.1.10 it is not possible to configure the IP addresses in the vSphere console after the Avaya Equinox® Recording Gateway virtual machine deployment is complete.

17. Click **Next** to display the Ready to Complete page.



18. Verify the deployment settings, and click **Finish**.

Result

vSphere Client starts the Avaya Equinox® Recording Gateway OVA deployment.

Starting the Equinox Recording Gateway virtual machine

Before you begin

Deploy the Avaya Equinox® Recording Gateway virtual machine.

Procedure

1. Log in to vSphere Client.
2. Click **Inventory**.
3. Click **Virtual Machine** > **Power** > **Power On**.

   The Avaya Equinox® Recording Gateway virtual machine starts.

Configuring the virtual machine automatic startup settings on VMware

About this task

When a vSphere ESXi host restarts after a power failure, the virtual machines that are deployed on the host do not start automatically. You must configure the virtual machines to start automatically.

In high availability (HA) clusters, the VMware HA software does not use the startup selections.

Before you begin

Verify with the ESXi system administrator that you have the permissions to configure the automatic startup settings.

Procedure

1. In the web browser, type the vSphere vCenter host URL.
2. Click one of the following icons: **Hosts and Clusters** or **VMs and Templates** icon.
3. In the navigation pane, click the host where the virtual machine is located.
4. Click **Configure**.
5. In Virtual Machines, click **VM Startup/Shutdown**, and then click **Properties**.

   The software displays the Edit VM Startup and Shutdown window.
6. Click **Automatically start and stop the virtual machines with the system**.
7. Click **OK**.

Equinox Recording Gateway initial configuration

Adding Equinox Recording Gateway in Equinox Management

About this task

You must add the Equinox Recording Gateway to Equinox Management to be able to manage it.

Before you begin

Get the following details:

- IP address of Equinox Recording Gateway
- IP address of the gatekeeper
- Location of Equinox Recording Gateway if the deployment has multiple locations

Procedure

1. Log in to Equinox Management.
2. Click **Devices**.
3. Click **Gateways** in the left pane.
4. Click **Add**.

   Equinox Management displays the Add Gateway page.
5. Configure the following fields:
   - **Name**
   - **IP Address**
   - **Model** — Select **Avaya Recording Gateway**
   - **Registered To**
   - **Location**

Result

Equinox Management adds the Equinox Recording Gateway instance as a device.

Configuring the Equinox Recording Gateway network settings

About this task

You must configure the Equinox Recording Gateway network settings.

Before you begin

- Decide a descriptive name for Equinox Recording Gateway.
- If the deployment has multiple locations, get the location of the Equinox Recording Gateway instance.

- If you deploy Equinox Recording Gateway as a web collaboration gateway, get FQDN.
- Get the network IP addresses of:
  - NTP server
  - DNS servers
  - (Optional) SIP proxy server

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Equinox Recording Gateway instance.

   Equinox Management displays the Gateways page.
3. Click the **Configuration** tab.
4. Configure the network settings.
5. Click **Apply**.

Chapter 9: Avaya Scopia Elite 6000 MCU deployment

Scopia Elite MCU overview

The Scopia Elite MCU is Equinox Solution’s flagship platform for high definition multi-party videoconferencing.

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.

The MCU harnesses revolutionary processing power for the most demanding videoconferencing applications using the latest DSP technologies. For an uncompromised videoconferencing experience, the MCU supports dual channels of Full HD 1080p at 60 frames per second for video and content, H.264 High Profile for bandwidth efficiency, H.264 Scalable Video Coding (SVC) for high network error resiliency, and full support for many telepresence systems.

With the MCU, each videoconference participant receives a quality experience optimized to their individual capabilities, from wireless mobile devices to HD room systems and immersive telepresence systems. The MCU leads in video interoperability, working with the broadest range of video systems on the market from leading UC clients to mobile devices and telepresence systems.

The MCU also features a patented, distributed architecture approach known as the Virtual MCU or cascaded videoconferences, which brings unparalleled scalability to its superb videoconferencing experience.

Scopia® Elite 6000 MCU deployment checklist

#	Action	Link/Notes	✔
1	• Check the site to ensure that the site is suitable for the Scopia® Elite 6000 MCU server installation. • Unpack the Scopia® Elite 6000 MCU server and check for damages. • Add a power supply unit to the Scopia® Elite 6000 MCU server. • Mount the Scopia® Elite 6000 MCU server onto the rack. • Connect the power and serial cables to the Scopia® Elite 6000 MCU server.	See *Rack Mounting Guide for Avaya Scopia® Elite 6000 MCU*.	
2	Configure the Scopia® Elite 6000 MCU IP addresses.	See Configuring the Device IP Addresses on page 210.	
3	Configure the ports on Scopia® Elite 6000 MCU.	See Configuring Ports on All Models of the MCU on page 215.	
4	Verify the installation of the Scopia® Elite 6000 MCU server.	See Verifying the Installation on page 221.	

Technical specifications of Scopia® Elite 6000 MCU

Hardware requirements

	Scopia Elite MCU 6105, 6110 and 6120	Scopia Elite MCU 6140
System power requirements		
Input	100-240 VAC, 50/60 Hz	100-240 VAC, 50/60 Hz with hot-swap redundant AC power supply and feed (optional)
AC Input	600W output @ 100-240V, 7.5A, 50-60Hz	1000W output @ 100-120V, 12-10A, 50-60Hz 1200W output @ 120-140V, 12-10A, 50-60Hz 1800W output @ 200-240V, 10-8.5A, 50-60Hz
Maximum power consumption at 35°C	200W, 250VA (682 BTU/h)	360W, 450VA (1228 BTU/h)

Table continues…

	Scopia Elite MCU 6105, 6110 and 6120	Scopia Elite MCU 6140
Environmental requirements		
Operating temperature	10°C to 35°C (50°F to 95°F)	
Relative humidity	5% to 90% non-condensing	
Storage and transit temperature	-40°C to 70°C (-40°F to 158°F), ambient	
Acoustics	Low noise fan speed control	
Physical requirements		
Dimensions	Width: 437mm (17.2"); height: 43mm (1.7"); depth 664mm (26.1")	Width: 437mm (17.2"); height: 43mm (1.7"); depth: 790mm (31.1")
Approximate net weight	11kg (24.25lbs)	14.5kg (32lbs) with one power supply
Approximate gross weight (with packaging)	21kg (46.3lbs)	23kg (50.7lbs)
Rack mounting	19-inch rack-mountable with flanges	

Software Specifications

These technical specifications of the protocols and software requirements apply to all Scopia® Elite 6000 MCU models:

Software and protocol	Supported
Signaling protocol	• H.323 • SIP
Audio	• Codecs: G.711. G.722, G.722.1, G.729, G.722.1 Annex C • DTMF tone detection (in-band, H.245 tones and RFC2833)
Video	• High Definition Continuous Presence video with a resolution of 1080p at up to 60fps • Codecs: H.263, H.263+, H.264, H.264 SVC, H.264 High Profile • Live video resolutions: CIF up to 1080p • Presentation video resolution: VGA, SVGA, SXGA, XGA, 720p, 1080p, WUXGA • Video bandwidth: up to 12Mbps for 1080p resolutions and up to 6Mbps for 720p or lower

Table continues…

Software and protocol	Supported
Web browser	• Microsoft Internet Explorer version 11 and later • Microsoft Edge • Mozilla Firefox • Google Chrome • Apple Safari

About the Capacity of the MCU

The MCU's capacity is measured in terms of the maximum number of simultaneous connections to a videoconference supported by this device.

The impact of a connection on the MCU's capacity depends on the bandwidth of the connection, which in turn is dependent on the resolution and frame rate of that connection. Therefore the same meeting can support a mix of HD and SD connections.

For example, a connection at 1080p at 30fps or 720p at 60fps uses half the capacity of a 1080p connection at 60fps. Similarly, a connection at 480p at 30fps uses a quarter of the resources of a 1080p connection at 30fps, or one-eighth of the resources of a 1080p 60fps connection.

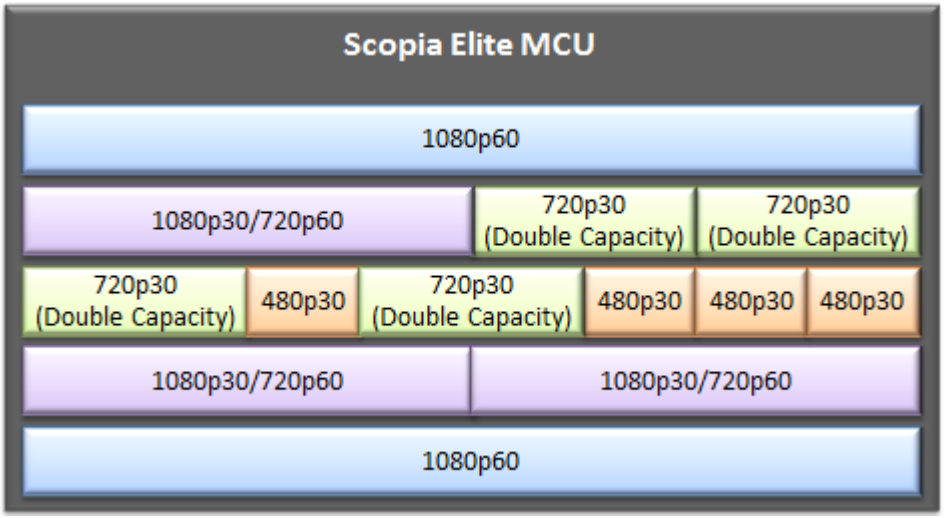


Figure 82: A connection uses its proportion of resources on the MCU

Important:

To enable connections at 720p at 30fps to use half the capacity of a 1080p 30fps connection, install the Double Capacity license.

The following table details the number of simultaneous connections available for each of the devices when all the connections have the same video resolution and frame rate.

Table 23: Number of simultaneous connections available at different video quality settings

Scopia® Elite 6000 MCU Model	1080p at 60fps	1080p at 30fps, 720p at 60fps, 720p at 30fps (no double capacity license)	720p at 30fps (with double capacity license)	480p at 30fps
Scopia Elite MCU 6105	3	5	10	20
Scopia Elite MCU 6110	5	10	20	40
Scopia Elite MCU 6120	10	20	40	80
Scopia Elite MCU 6140	20	40	80	160

Important:

You can increase the device's capacity at any resolution (including 1080p at 60fps) to the same capacities listed under 480p by enabling **Switched Video** in the meeting type (or service). For more information on enabling switching, see *Administrator Guide for Avaya Scopia® Elite 6000 MCU*.

However, if you encrypt the media and enable switching in the same MCU service, the resolution may be dynamically lowered slightly in some cases, but overall MCU capacity remains constant.

If you want to limit the resolution and frame rate of all connections to a meeting, define a meeting type (MCU service) in the MCU and place the limit there. For more information, see *Administrator Guide for Avaya Scopia® Elite 6000 MCU*. Alternatively, you can limit the bandwidth using the global bandwidth policies in Equinox Management.

Audio ports capacity

Audio ports capacity is exclusive of the video ports capacity.

Scopia® Elite 6000 MCU Model	Audio ports
Scopia Elite MCU 6105	20
Scopia Elite MCU 6110	40
Scopia Elite MCU 6120	80
Scopia Elite MCU 6140	160

Ports to Open for the Scopia® Elite 6000 MCU

The Scopia® Elite 6000 MCU is typically located in the enterprise network and is connected to the DMZ. When opening ports on the Scopia Elite MCU, use the following as a reference:

- If you are opening ports that are both in and out of the Scopia® Elite 6000 MCU, see Table 24: Bidirectional Ports to Open on the Scopia® Elite 6000 MCU on page 208.

- If you are opening ports inbound to the Scopia® Elite 6000 MCU, see Table 26: Inbound Ports to Open to the Scopia® Elite 6000 MCU on page 210.

Important:

The specific firewalls you need to open ports on depends on where your MCU and other Equinox Solution products are deployed.

Table 24: Bidirectional Ports to Open on the Scopia® Elite 6000 MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
1024-1324	H.245 (TCP)	Any H.323 device	Enables H.245 signaling	Cannot connect H.323 calls	Mandatory To configure, see Configuring the TCP Port Range for H.245 on Scopia® Elite 6000 MCU on page 216
1719	RAS (UDP)	H.323 gatekeeper	Enables RAS signaling	Cannot communicate with H.323 gatekeeper	Mandatory To configure, see Configuring the UDP port for RAS on Scopia® Elite 6000 MCU on page 217 and Configuring the UDP port for the gatekeeper on Scopia® Elite 6000 MCU on page 218
1720	Q.931 (TCP)	Any H.323 device	Enables Q.931 signaling	Cannot connect H.323 calls	Mandatory To configure, see Configuring the TCP port for Q.931 on Scopia® Elite 6000 MCU on page 219
3336	XML (TCP)	Conference Control web client endpoint, Equinox Management, or third-party controlling applications	Enables you to manage the MCU via the XML API	Cannot use MCU Conference Control web user interface. Cannot use XML API to control MCU.	Mandatory if deployed with Equinox Management
3337	XML (TCP)	Other MCUs	Enables use of MCU Cascading XML API	Cannot cascade between two MCUs	Mandatory if multiple MCUs are deployed with Equinox Management

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3338	XML (TCP)	Equinox Management, or third-party configuration applications	Enables you to configure the MCU via the XML API	Cannot configure MCU via the XML API	Mandatory if deployed with Equinox Management
3400-3580	SIP BFCP (TCP)	Any SIP video network device	Enables SIP content sharing	Cannot share SIP contents	Mandatory if using content sharing with SIP over TCP To configure, see Configuring the TCP port range for SIP BFCP on Scopia® Elite 6000 MCU on page 220
5060	SIP (TCP/ UDP)	Any SIP video network device	Enables SIP signaling	Cannot connect SIP calls	Mandatory if using SIP over TCP/ UDP To configure, see Configuring the TCP, UDP, and TLS port for SIP on page 219
5061	SIP (TLS)	Any SIP video network device	Enables secure SIP signaling	Cannot connect SIP calls over TLS	Mandatory if using SIP over TLS To configure, see Configuring the TCP, UDP, and TLS port for SIP on page 219
12000-13200 16384-16984	RTP/ RTCP/ SRTP (UDP)	Any H.323 or SIP media-enabled video network device	Enables real-time delivery of video and audio media	Cannot transmit/ receive video media streams	Mandatory To configure, see Configuring the UDP port ranges for RTP/RTCP on Scopia® Elite 6000 MCU on page 215

Table 25: Outbound ports to open from Scopia® Elite 6000 MCU

Port range	Protocol	Destination	Function	Result of blocking port	Required
162	SNMP (UDP)	Equinox Management or any SNMP manager station	Enables sending SNMP trap events	Cannot send SNMP traps	Recommended
53	DNS (TCP/UDP)	DNS server	Enable querying DNS for FQDN	DNS is disabled	Mandatory

Table 26: Inbound Ports to Open to the Scopia® Elite 6000 MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
21	FTP (TCP)	FTP Server	Enables audio stream recording	Cannot record audio streams	Optional
22	SSH (TCP)	SSH Client	Enables you to view logs	Cannot view logs in real-time (logs are collected on the compact flash card)	Optional
80	HTTP (TCP)	Web client	Provides access to the MCU Administrator and Conference Control web user interfaces; used for software upgrade	Cannot configure MCU	Mandatory if using HTTP To configure, see Configuring the HTTP port on Scopia® Elite 6000 MCU on page 216
443	HTTPS (HTTP over SSL)	Web client	Provides secure access to the MCU Administrator and Conference Control web user interfaces; used for software upgrade	Cannot configure MCU	Mandatory if using HTTPS

Configuring the IP addresses

About this task

The MCU supports the following format of IP addresses:

- IPv4 (default)
- Both IPv4/IPv6 (Internet Protocol Version 6). This dual mode allows deploying servers using both protocols in your solution.

Caution:

The device is shipped with a static IPv4 address, which might conflict with an existing address on your network. Configure the MCU to its new IPv4 address before connecting the MCU to the network.

You can add an IPv6 address if necessary, after the MCU has its new IPv4 address.

This procedure describes how to configure the management IP address on the left-hand NIC port (see Figure 83: Rear panel of the device on page 211). Use this address to access the MCU web interface.

Before you begin

Make sure you have these items:

- Dedicated IP address for the device
- Dedicated subnet mask for the device
- IP address of the default router which the device uses to communicate over the network
- A PC with an available serial port. It should have a terminal emulator software installed like SecureCRT or PuTTY.
- Power, network, and serial cables supplied with the device accessories kit.

Use the serial port on the back panel of the device to connect it directly to a PC to assign an IP address. You must assign the IP address before you connect the device to the network.

Procedure

1. Connect the power cable, but do not switch on the device.

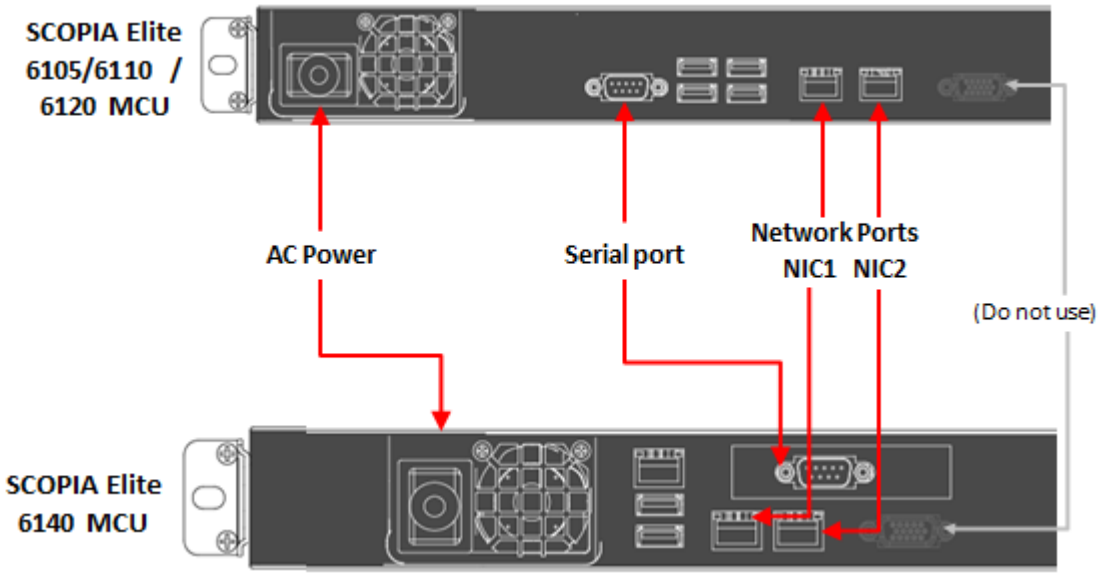


Figure 83: Rear panel of the device

2. Connect the device serial port to a PC with the terminal emulator software installed.
3. Start the terminal emulation application on the PC.
4. Set the communication settings in the terminal emulation application on the PC as follows (Table 27: Configuring the communication settings on page 211):

Table 27: Configuring the communication settings

Field Name	Value
Baud Rate	9600
Data bits	8

Table continues…

Field Name	Value
Parity	None
Stop bits	1
Flow Control	None

5. Power the device (see Figure 84: Device front panel on page 212).

   Verify the power LED is lit green (Figure 84: Device front panel on page 212).

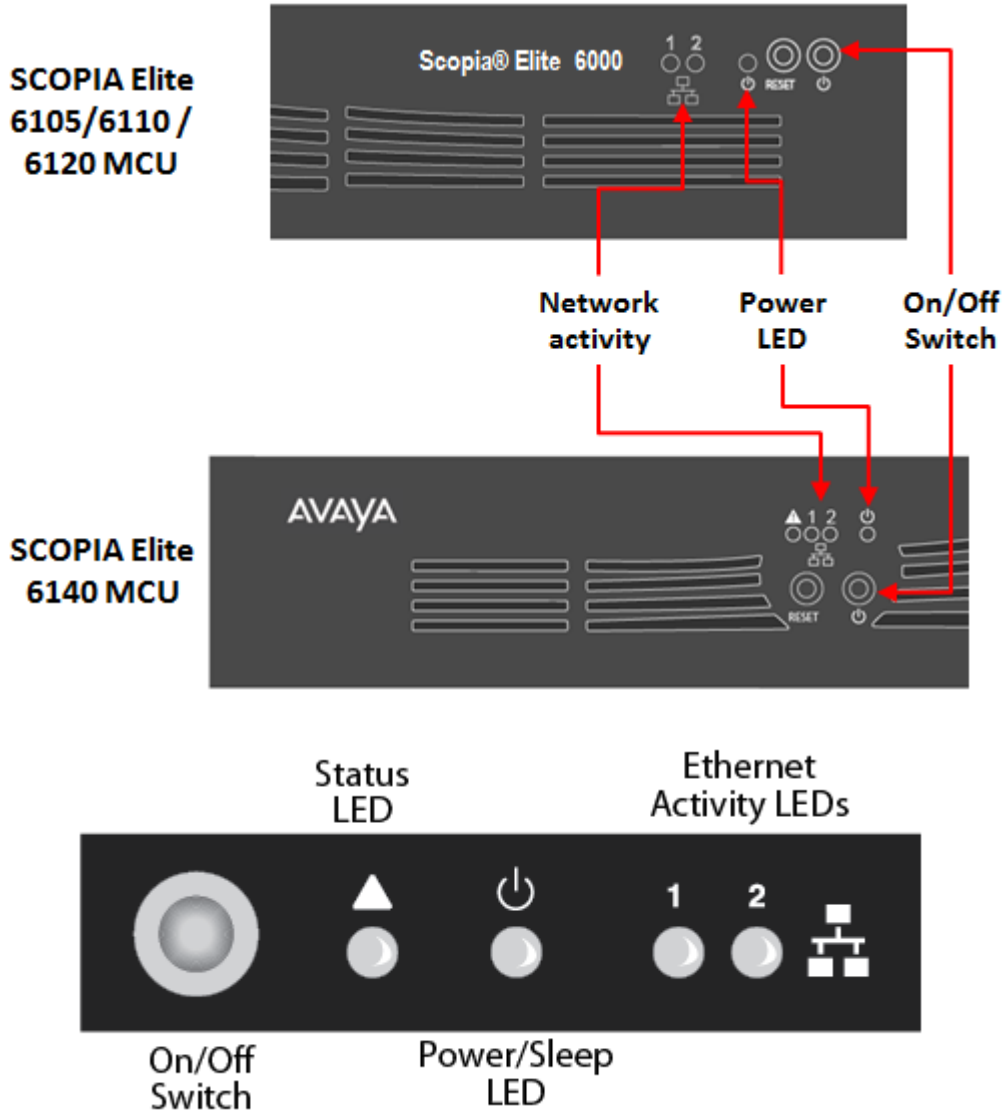


Figure 84: Device front panel

   A log of the auto-boot events is displayed in the terminal emulator.

6. When the message `Press any key to start configuration` appears on the screen, press a key and wait for the following message:

```
Main menu
```

```
Main Menu
N: Configure network port values
R: Restore factory defaults
Q: Quit

Select:
```

```
Main menu
N: Configure network port values
R: Restore to factory defaults
T: Set the XML connection mode to TCP (Reboot is not required)
S: Set Board Security Level
Q: Quit
```

If you do not see this output, contact customer support.

7. Enter **N** at the prompt to configure network port values.

   The terminal displays the following message:

```
Configure network port values
1: Show current network configuration
2: Change network configuration
0: Return to main menu

Select:
```

8. Enter **2** to change the network configuration.
9. Enter the new settings at each prompt (Table 28: Configuring network settings on page 213).

Table 28: Configuring network settings

Field	Description
IP Address	IP address of the device
Subnet mask	IP address of the subnet mask to which the device belongs. If you are not using a subnet mask, press **Enter**.
Default router	IP address of the default router the device uses to communicate over the network

Important:

The new settings configure both NICs since they are paired by default as a primary NIC and a redundant NIC.

10. Allow the device to complete the reboot process. A new emulator session begins.
11. Close the terminal emulator session.
12. Connect the network cable to the ethernet connector on the rear panel of the device. Use one of the following connections:
    - If you do not need network redundancy, connect the network cable either to NIC1 or to NIC2.

- To achieve network redundancy, connect a network cable routed from the same switch to each NIC.

13. (Recommended) Set the network switch to 1Gbps Auto Negotiation full duplex, if it can support this configuration.

    The throughput of the network switch should always be the same as the setting in the MCU, whose default value is also 1Gbps.

    You can change the default value from the MCU administrator web interface by navigating to **Configuration** > **Network** > **Port Settings** (Figure 85: Configuring the MCU throughput on page 214).



Figure 85: Configuring the MCU throughput

14. To configure the following IPv6 and DNS server IP addresses, navigate to **Configuration** > **Network** (Figure 85: Configuring the MCU throughput on page 214).

    - **IPv6 Address** > **Set manually** > **Primary IP address**
    - **DNS server 1**
    - **DNS server 2**

    If you do not configure valid IP addresses for the DNS servers, you might face SIP call disconnections.

15. Select **Apply** at the bottom of the page.
16. Make sure no videoconferences are running on the MCU, and select **Yes** to restart the device.

Configuring Ports on All Models of the Scopia Elite MCU

This section provides instructions of how to configure the following ports and port ranges on all models of the Scopia Elite MCU:

Related links

[Configuring the UDP port ranges for RTP/RTCP on Scopia® Elite 6000 MCU](#) on page 215
[Configuring the TCP Port Range for H.245 on Scopia® Elite 6000 MCU](#) on page 216
[Configuring the HTTP port on Scopia® Elite 6000 MCU](#) on page 216
[Configuring the UDP port for RAS on Scopia® Elite 6000 MCU](#) on page 217
[Configuring the UDP port for the gatekeeper on Scopia® Elite 6000 MCU](#) on page 218
[Configuring the TCP port for Q.931 on Scopia® Elite 6000 MCU](#) on page 219
[Configuring the TCP, UDP, and TLS port for SIP](#) on page 219
[Configuring the TCP port range for SIP BFCP on Scopia® Elite 6000 MCU](#) on page 220

Configuring the UDP port ranges for RTP/RTCP on Scopia® Elite 6000 MCU

About this task

Scopia® Elite 6000 MCU uses 360 ports for audio and 1080 ports for video. It has the following designated UDP port ranges for RTP/RTCP:

- Video: 12000 to 13200
- Audio: 16384 to 16984

Important:

Do not reduce the number of UDP ports that Scopia® Elite 6000 MCU uses for RTP/RTCP.

The number of UDP ports required for RTP/RTCP is fixed. You can determine the exact port numbers that Scopia® Elite 6000 MCU uses by defining the lower-end of the port range called the Base port.

Procedure

1. Log in to Avaya Equinox® Management.
2. Click **Devices**, and select the Scopia® Elite 6000 MCU instance.
3. Click **Configuration** > **Advanced Parameters**.

   Equinox Management opens the Restore window.
4. Click one of the following port entries:
   - **Video Base Port**
   - **Audio Base Port**
5. Type the new lower-end port number in the **Value** field.

6. Click **Apply**.
7. Click **Close**.

Related links

Configuring Ports on All Models of the Scopia Elite MCU on page 215

Configuring the TCP Port Range for H.245 on Scopia® Elite 6000 MCU

About this task

Scopia® Elite 6000 MCU uses 300 ports. It has a TCP port range of 1024 to 1324 ports designated for H.245.

You can set the Base port, which is the lower end of the TCP port range. H.245 is a control channel protocol used for multimedia communication. This protocol processes transfer of information about the device capabilities and opening and closing of the logical channels that carry media streams.

Procedure

1. Log in to Avaya Equinox® Management.
2. Click **Devices**, and select the Scopia® Elite 6000 MCU instance.
3. Click **Configuration** > **Advanced Parameters**.
4. Click **Click** > **More**.
5. Type the following command in the **Command** field: `h245baseport`

   To see the current port number, click **Execute**.
6. Type the port number in the **Value** field.
7. Click **Execute**.
8. Click **Close**.

Related links

Configuring Ports on All Models of the Scopia Elite MCU on page 215

Configuring the HTTP port on Scopia® Elite 6000 MCU

About this task

Scopia® Elite 6000 MCU has port 80 designated for HTTP. You can also configure port 20 for HTTP.

Note:

If you configure a new HTTP port on Scopia® Elite 6000 MCU, update the new port number in the Scopia® Elite 6000 MCU URL to gain access to the web server. For example, if your new HTTP port value is 8080, type http://<URL>:8080.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Scopia® Elite 6000 MCU instance.
3. Click **Configuration** > **Advanced Parameters**.
4. Click **Click** > **More**.
5. Type the following command in the **Command** field: `webserverport`

   To see the current port number, click **Execute**.
6. Type the port number in the **Value** field.
7. Click **Execute**.

   Important:

   After selecting **Execute**, a warning message appears, notifying you that the unit will be reset and any active conferences will be disconnected.

   Avaya Equinox® Management displays a message warning that Scopia® Elite 6000 MCU will be reset and all active conferences will be disconnected.
8. Click **Yes** to continue.
9. Click **Close**.

Related links

Configuring Ports on All Models of the Scopia Elite MCU on page 215

Configuring the UDP port for RAS on Scopia® Elite 6000 MCU

About this task

Scopia® Elite 6000 MCU has port 1719 designated for RAS. You can configure a different port for RAS.

Port 1719 is also used to communicate with the gatekeeper. If you configure this port for RAS, you must configure a different port for the gatekeeper.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Scopia® Elite 6000 MCU instance.
3. Click **Configuration** > **Advanced Parameters**.

4. Click the **H323 RAS port number** entry.
5. Type the port number in the **Value** field.
6. Click **Apply**.
7. Click **Close**.

Related links

Configuring Ports on All Models of the Scopia Elite MCU on page 215

Configuring the UDP port for the gatekeeper on Scopia® Elite 6000 MCU

About this task

Scopia® Elite 6000 MCU has designated port 1719 for gatekeeper use. You can configure a different port to enable communication with the gatekeeper (for example, if port 1719 is busy). Port 1719 is also used for RAS (to configure the UDP port for RAS, see Configuring the UDP port for RAS on Scopia® Elite 6000 MCU on page 217).

Important:

If you close port 1719, you must configure another port for both the gatekeeper and RAS. If you configure a different port for the gatekeeper, you do not need to configure a different port for RAS.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**.
3. In the left pane, click **Media Servers**.
4. Click the name of the media server instance.

   Equinox Management displays the page of the media server instance.
5. In the **Info** tab, click the IP address of the media server.

   Equinox Management displays the management UI in a new window.
6. Click the **Configuration** > **Protocols** tab.
7. In the **Enable H.323 protocol** section, enter the port value in the **Gatekeeper port** field. (Figure 86: H.323 Protocol section of the Protocols tab on page 219).

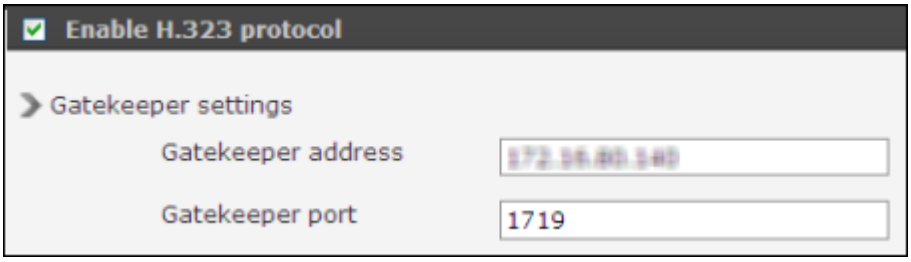


Figure 86: H.323 Protocol section of the Protocols tab

8. Click **Apply**.

Related links

Configuring Ports on All Models of the Scopia Elite MCU on page 215

Configuring the TCP port for Q.931 on Scopia® Elite 6000 MCU

About this task

Scopia® Elite 6000 MCU has port 1720 designated for Q.931. You can configure a different port for Q.931.

Q.931 is a telephony protocol used for establishing and terminating the connections in H.323 calls.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Scopia® Elite 6000 MCU instance.
3. Click **Configuration** > **Advanced Parameters**.
4. Click **H323 SIG port number** entry.
5. Type the port number in the **Value** field.
6. Click **Apply**.
7. Click **Close**.

Related links

Configuring Ports on All Models of the Scopia Elite MCU on page 215

Configuring the TCP, UDP, and TLS port for SIP

About this task

Scopia® Elite 6000 MCU has ports 5060 and 5061 designated for SIP. You can configure a different port for SIP.

Procedure

1. Log in to Equinox Management.

2. Click **Devices**, and click the name of the Scopia® Elite 6000 MCU instance.

   Equinox Management displays the Scopia® Elite 6000 MCU instance page.
3. Click the **Configuration** tab.
4. In **SIP Settings**, configure the following fields:
   - **SIP Proxy Server**
   - **Transport Types**: Choose UDP or TCP if you do not want to secure the SIP data traffic; choose TLS to secure the SIP traffic. If you choose TLS, you must install TLS certificates for encryption and authentication of the SIP traffic.
5. Click **Apply**.

Related links

Configuring Ports on All Models of the Scopia Elite MCU on page 215

Configuring the TCP port range for SIP BFCP on Scopia® Elite 6000 MCU

About this task

Scopia® Elite 6000 MCU has a TCP port range of 3400 to 3580 designated for SIP BFCP.

BFCP is a protocol which coordinates shared videoconference features in SIP calls, often used by one participant at a time. For example, when sharing content to others in the meeting, one participant is designated as the presenter, and is granted the floor for presenting. All endpoints must be aware that the floor was granted to that participant and react appropriately.

The number of ports required for SIP BFCP is fixed. You can determine the exact port numbers that Scopia® Elite 6000 MCU uses by defining the lower-end of the port range called the Base port.

Procedure

1. Log in to Avaya Equinox® Management.
2. Click **Devices**, and select the Scopia® Elite 6000 MCU instance.
3. Click **Configuration** > **Advanced Parameters**.
4. Click the **SIP BFC Base Port** entry.
5. Type the new lower-end port number in the **Value** field.
6. Click **Apply**.
7. Click **Close**.

Related links

Configuring Ports on All Models of the Scopia Elite MCU on page 215

Verifying the Scopia® Elite 6000 MCU installation

About this task

After you installed the device and performed its initial configuration, you need to verify that it is installed and configured correctly.

Procedure

1. On the front panel, verify that the power LED is lit green.

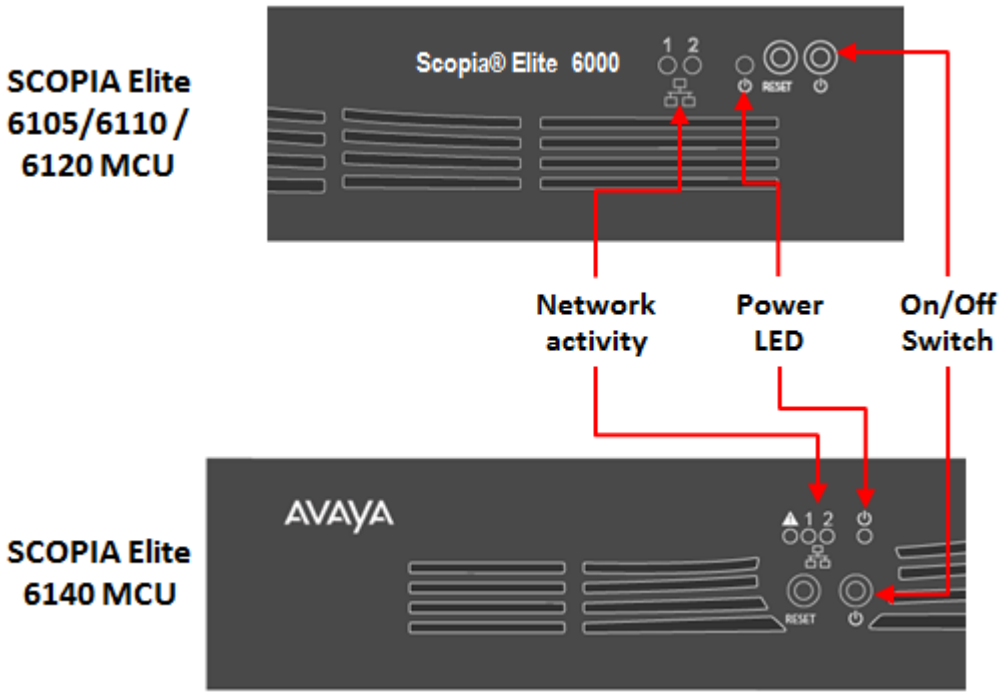


Figure 87: Locating the front panel LEDs

2. Verify that the status LED is lit green (selected models only).
3. Check the network connection by verifying that the Ethernet activity LED is lit green.
4. Verify the device is ready for use by creating a videoconference:
   a. From an endpoint dial the MCU IP address.

      The MCU Auto-Attendant service plays the video and audio prompts.
   b. Press **0** to create a new videoconference.
   c. At the prompt, enter the meeting ID followed by **#**.

      The MCU creates the conference and opens the Conference window.
   d. Exit the conference by disconnecting the call.

5. Verify the device is ready.
   a. Configure this MCU in Equinox Management as explained in *Administrator Guide for Avaya Equinox® Management*.
   b. Take other MCUs offline (if any) to make sure you hold the videoconference on this MCU.
   c. From an endpoint dial the IP address (or the Auto-Attendant number if configured).
   d. Press **0** to create a new conference.
   e. At the prompt, enter the meeting ID followed by **#**.

      The MCU creates the videoconference. If it is successful, the MCU is properly installed and configured.

      You can view the videoconference status in these pages:

      - The MCU's **Status Map** which shows the connection to Equinox Management and conference use statistics.



Figure 88: The MCU Status Map

      - The Equinox Management **Dashboard** which shows the details of the current videoconference.

ID	Name	Participants	MCU	Terminate
716194	IVR Session	1	MCU230192	X

Figure 89: The Equinox Management Dashboard status

   f. Exit the videoconference by disconnecting the call.

Chapter 10: Data migration from Avaya Aura to Avaya Equinox

Introduction to Avaya Aura® Conferencing data migration

This section is intended for Avaya Aura® Conferencing 8.x (AAC8) customers who need to migrate their deployment data to Avaya Equinox® for Over The Top (OTT) or Avaya Equinox® for Team Engagement (TE), Release 9.1.x.

There are four types of data migration:

Migration type	Description
AAC8 data to non-Aura Equinox	For migrating data of Avaya Aura® Conferencing Turnkey solution to OTT Equinox Solution.
Aura AAC8 data to non-Aura Equinox	For migrating data of Avaya Aura® Conferencing and Avaya Aura® environment to OTT Equinox Solution.
Aura AAC8 to Aura Equinox	For migrating data of Avaya Aura® Conferencing and Avaya Aura® to TE Equinox Solution.
AAC8 to Aura Equinox	For migrating data of Avaya Aura® Conferencing Turnkey solution to TE Equinox Solution.

Avaya has created a migration tool for migrating users and conferencing data. The migration tool is part of the Equinox Management application and is downloaded from PLDS together with the application.

The migration tool has the following functionalities:

- Simple Java Standalone application distributed as JAR file.
- Uses AAC8 OPI to export data, and Equinox XML API to import data.
- Converts AAC8 entities to Equinox entities.
- Stores AAC8 raw data in the Equinox database, for future usage.

The following content is migrated:

- Only User Basic Data and User Conference Data are migrated.
- User Basic Data are settings like first name, last name, email, phone, login. The data is mapped to the Equinox User entity.

- User Conference Data are conference specific settings like access codes, waiting room checkbox, recording checkbox, maximum number of participants. The data is mapped to the Equinox Virtual Room entity.
- Two types of user are considered: Local users and LDAP users. For LDAP users, only User Conference Data is migrated. User Basic Data is already synchronized and no update is required.
- AAC8 has up to two conference rooms per user (primary and secondary profile), Equinox can have many conference rooms if license allows it. If the Equinox license allows only one VR, AAC8 and user already have one VR, In this case, the AAC8 conference room is not migrated at all and the system displays a warning.
- User locations are not migrated. AAC8 and Equinox location usage differs so they do not map well. Users locations are set as AUTO so other Equinox rules are applied to determine location.

The migration tool generates XML files for the System Manager bulk import tool so all required data are imported to System Manager, and System Manager pushes all required data to Equinox Management. The current version of Equinox System Manager Extension Pack (EP) does not support bulk import yet. The tool generates XML files which cannot be used for now. The only limitation with direct import is that the System Manager user profile does not have the Equinox profile checkbox set and the administrator must be aware of this. When the Equinox System Manager EP bulk import tool is ready, those XML files can be used with the **Merge** option so the Equinox profile will be populated on System Manager as well.

Migration of user base profiles

The migration tool imports existing user fields from AAC User Base Profiles, creates users on Equinox Management, and opens Virtual Meeting Rooms (VMRs).

Data field name in AAC	Description	Mapping in Equinox Management
Aura Login Name	Aura Login Name	User - Login ID User - Email if User's Email in AAC is empty
Cell Phone	Cell Phone Number	User - Cell Phone
Email	User Email Address	User - Email
First Name	User First Name	User - First Name Virtual Room - User First Name
Last Name	User Last Name	User - Last Name Virtual Room - User Last Name
Business Phone	Business Phone Number	User - Office Phone Virtual Room - Number (Optional. The administrator can choose.)
Time Zone	User Time Zone	User - Time Zone

This is a set of expected values for approved constants mapped in Equinox Management:

- User - Local

  True if Local user, False if LDAP

- User - Named = TRUE

Migration of user conferencing profiles

The migration tool imports existing fields from the AAC User Conferencing Profiles and maps the selected fields into the user VMR in Equinox Management. The tool differentiates between video-enabled and non-enabled users and maps into video and audio-only services.

Data field name in AAC	Description	Mapping in Equinox Management
Allow Fast Start	Whether conference fast start is allowed	Virtual Room is in waiting room mode **Note:** For video enabled meeting room, fast start is allowed by default. For audio only meeting room, this value is taken from AAC. First set a moderator pin, then enable the waiting room. In OTT deployment, if the waiting room is false, the moderator PIN is not mandatory.
Conference Class of Service - Conference Flow	Collaboration flow or Pass code flow	Virtual Room - Protected Meeting
Conference Class of Service — Maximal Number of Participants	The maximal number of participants allowed in conference	Virtual Room - Max Participants
Enable Operator Control	Whether operator control is enabled	User - Allow Moderate Without Pin User - Allow Use Others Virtual Room User - View All Meetings By User Portal
Enable Recording	Whether recording is enabled	User - Allow Recordings Virtual Room - Allow Recordings

Table continues…

Data field name in AAC	Description	Mapping in Equinox Management
Enable Video	Whether video is enabled	User - Default Meeting Type Virtual Room - Meeting Type **Note:** Check Equinox Management default meeting type. The administrator must select the default meeting type for other media (audio or video). If video is enabled and the default type is video, use it for user and her/his virtual room; otherwise use administrator selection. Perform the same procedure for audio.
Moderator Collaboration Code	Moderator Code	Virtual Room - Number Optional. The administrator can choose.
Moderator Pass Code	Moderator Pass Code	Virtual Room - Moderator Pin In TE deployment the Moderator PIN is required. If the Moderator Passcode is empty for user, then her/his moderator access code is used. The list of such users is shown at the end of migration process.
Participant Collaboration Code	Participant Code	Virtual Room - Number (Default option)
Participant Pass Code	Participant Pass Code	Virtual Room - Conference Pin
Video Class - Maximum average bandwidth per participant	The maximal average bandwidth allowed for each participant in the conference	User - Max Bandwidth

This is a set of expected values for approved constants mapped in Equinox Management:

- User - Allow Streaming = ON

  Virtual Room - Allow Streaming = ON
- User - Reservable = TRUE
- User - Schedulable = TRUE
- User - User Profile ID = CUSTOM
- Virtual Room - Auto Extend = TRUE
- Virtual Room - Block Dial IN = FALSE
- Virtual Room - Default = TRUE (for Local users only)

- Virtual Room - Description
- Virtual Room - Name
- Virtual Room - One Time Pin Required = FALSE
- Virtual Room - Public = TRUE

Exporting data from Avaya Aura® Conferencing

About this task

Use the following procedure to export your existing data from Avaya Aura® Conferencing (AAC8).

Before you begin

- Read Introduction to Avaya Aura Conferencing data migration on page 223 for an overall understanding of the data migration process.
- Make sure you upgraded Avaya Equinox® Management to the latest release version, which must be from release 9.1 SP4 and above. For the latest information on upgrading, see *Administrator Guide for Avaya Equinox® Management* and *Avaya Equinox® Management Release Notes*.
- Make sure you upgraded Avaya Aura® Conferencing to the latest release version, which must be from release 8.0 SP9 Patch 2 and above.

  Important:

  In SP9 patch 2 release, Avaya Aura® Conferencing has Java 7. The migration tool requires at least Java 8 to run without issues. If you need to run the tool from the server, you must patch Avaya Aura® Conferencing to SP11. Otherwise, you must run the tool from the local machine of the Equinox Management server.

  The minimum requirement for Avaya Aura® Conferencinginstallation is 8.0 SP7.

  For the latest information on upgrading, see *Avaya Aura® Conferencing Release Notes*.
- Make sure you have your PMGR administrator credentials ready.

Procedure

1. Login to Equinox Management as **`pmgradmin`**.

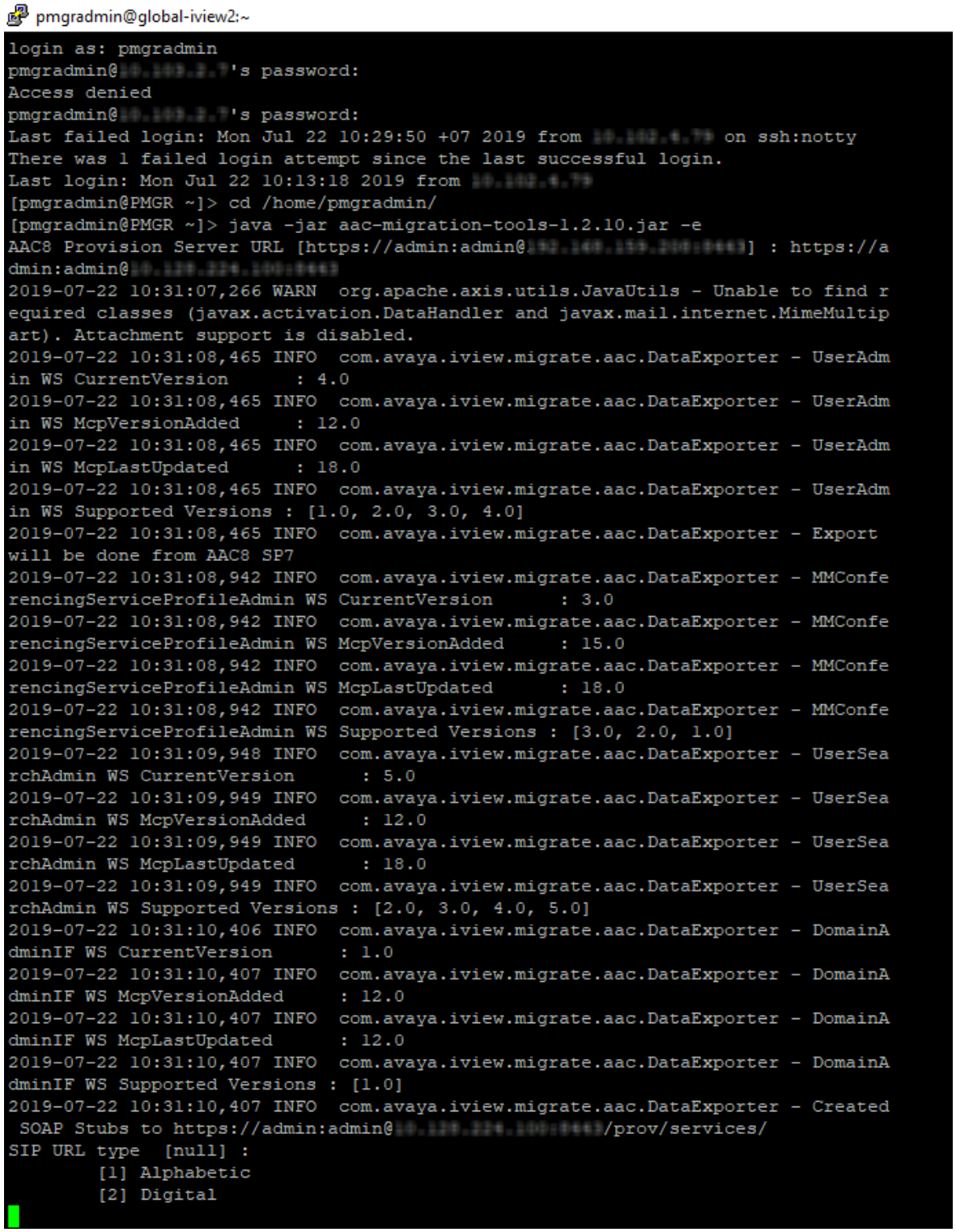


Figure 90: Example of data export procedure

2. Enter:

   `cd/home/pmgradmin/`

3. Run:

   ```
   java -jar aac-migration-tools-1.2.10-jar-with-dependencies.jar -e
   ```

4. Provide the AAC OPI URL with administrator credentials. It has the format:

   ```
   AAC8 Provision Server URL [https://
   admin:admin@123.456.789.111:8443]]
   ```

   This URL is required to execute OPI SOAP requests to AAC PROV.

   `admin:admin` in the command is the username:password for logging into the Provisioning page. The username and password can be changed, depending on the customer's configuration.

5. Enter the SIP URL type that the system adds to Equinox Management:

   ```
   SIP URL type [Alphabetic] :
                            [1] Alphabetic
                            [2] Digital
   ```

   AAC8 has multiple SIP communication addresses like `23441101@avaya.com` or `jbrown@avaya.com`; Equinox Management has only one. Only one SIP URI is currently supported in Equinox Management, so you can use only one AAC8 SIP communication address to Equinox Management.

   The Address template (alphabetic, digital) allows selecting the address type that will be used for Equinox calls. If there are no matches in one template, the first one from the list of user communication addresses will be selected. If there is more than one match, the first one in the array will be used.

6. Select `Y` to start exporting.

   The tool exports data from AAC8 and saves it in the AAC8Data.ser file.

Next steps

See Importing Avaya Aura Conferencing data to Avaya Equinox® Management on page 229.

Importing Avaya Aura® Conferencing data to Avaya Equinox® Management

About this task

Use the following procedure to import data you previously exported.

Before you begin

- Make sure you have successfully completed the AAC8 data export procedure.
- (Optional. Only for multi-tenancy) Equinox Management has multi-tenant and enterprise versions. Multi-tenancy means there are multiple different members and organizations, each one with its member ID. AAC is enterprise only. Make sure you have your member ID as you will be prompted for your organization member ID before starting the migration process.

- Decide whether you run the migration tool from Equinox Management server or from a PC.

  If you are running the tool from the server, unmapped AAC fields will be kept in the Equinox Management database for future releases.

  If you are running the tool from a PC, AAC8 raw data are not stored in the Equinox Management database. Migration setting prompts are also slightly different as some data are retrieved automatically when running the tool on Equinox Management.

Procedure

1. Upload aac-migration-tools-1.2.10-jar-with-dependencies.jar and AAC8Data.ser to Equinox Management as root.

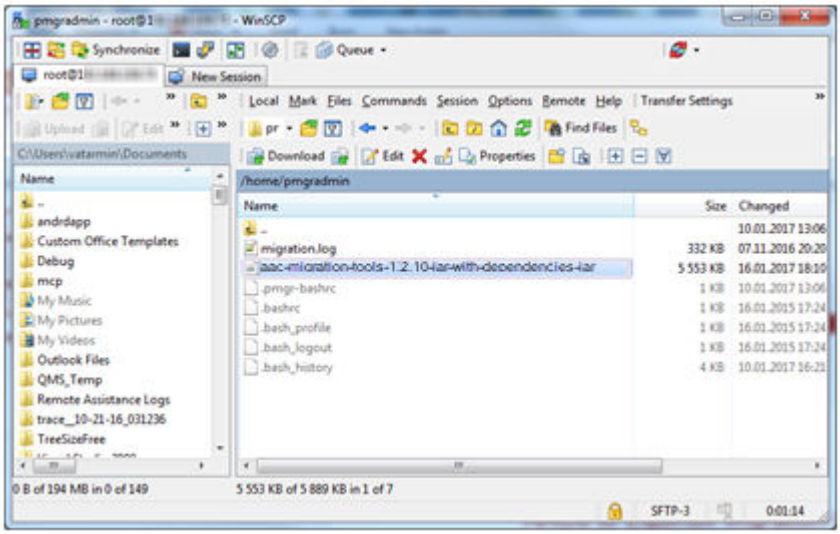


Figure 91: Uploading the migration tool

2. Execute `java -jar aac-migration-tools-1.2.10-jar-with-dependencies.jar -i`
3. Select your deployment type.

Note:

The solution is called Avaya Equinox® for Over The Top (OTT) when it ties to the customer existing infrastructure and provides services over the top of this infrastructure without requiring it to be upgraded or replaced.

The solution that tightly integrates with Avaya Aura® components is called Avaya Equinox® for Team Engagement (TE) and is deployed in medium and large enterprises.

Field	Description
`[1] Aura AAC to Aura Equinox`	Enter `1` for migrating data from AAC8 (with Avaya Aura®) to TE Equinox Solution.
`[2] Non-Aura AAC to Non-Aura Equinox`	Enter `2` for migrating data from AAC8 Turnkey (no Aura) to OTT Equinox Solution.

Table continues…

Field	Description
`[3] Non-Aura AAC to Aura Equinox`	Enter `3` for migrating data from Avaya Aura® Conferencing (without Avaya Aura®) to TE Equinox Solution.
`[4] Aura AAC to Non-Aura Equinox`	Enter `4` for migrating data from Avaya Aura® Conferencing (with Avaya Aura®) to OTT Equinox Solution.

4. (Only for the `to Aura Equinox` deployment type) Enter the Avaya Aura® Session Manager (SM) name.
5. Enter `Y` to import AAC8 raw data into the Equinox Management database.

   Equinox Management will use these data when new features similar to those of AAC8 appear in future releases.

   The tables added to the Equinox Management database are: `t_aac8_conf_class; t_aac8_video_class; t_aac8_system_profile; t_aac8_user; t_aac8_user_comm_addr`. This option is available only if you run the tool from Equinox Management.
6. Enter the Equinox Management database credentials.

   The default user name is `icm_core_user`. The default password is `icm_core_1111`.
7. Enter `Y` to do mapping and import into Equinox Management.
8. The following alert message appears on the screen:

   ```
   Is LDAP synchronization done on Equinox, Aura and AAC8? If not,
   perform it right now and then continue. Usually sync is done daily
   at midnight automatically, sometimes more rare. Without sync it
   right now, you can miss migration for a few LDAP users that were
   added after last sync time. Continue (Y/N) [N] :
   ```

   If you enter `Y` and LDAP synchronization is missed, nothing critical happens. Usually, LDAP synchronization is configured to be done daily, so you might only loose a few users that were added to LDAP after the last synchronization.
9. Enter the username and password of the Equinox Management HTTP user.

   The default use name is `admin`. The default password is `admin`.
10. Enter the Equinox Member ID.

    The Equinox Solution has multi-tenant and enterprise versions, multi-tenant meaning multiple different members and organizations (different member IDs), which is not the case with Avaya Aura® Conferencing. If the Equinox Solution is an enterprise version, enter the default value `999` of the Equinox Member ID.
11. Enter the preferred Equinox Audio Meeting Type.

    It is used as a meeting type for audio-only AAC8 users and their virtual rooms. The screen displays a Meeting Type list, the content of which depends on the meeting type configured

in Equinox Management. Meeting types named `6K` refer to Scopia Elite MCU. Those named `7K` refer to Equinox Media Server.

12. Enter the preferred Equinox Video Meeting type.

    It is used as a meeting type for audio and video AAC8 users and their virtual rooms. The screen displays a Meeting Type list, the content of which depends on the meeting type configured in Equinox Management. Meeting types named `6K` refer to Scopia Elite MCU; those named `7K` refer to Equinox Media Server.

13. Enter the relevant user password (or code) type.

    The default user password is `2`.

    ```
    User password type  [Moderator code] :
                 [1] Participant code
                 [2] Moderator code
                 [3] Office phone
                 [4] Provide another password (the same for every user)
    ```

    For an LDAP user, the system stores the password on the LDAP server. For local users, the system resets the password to the default value after migration. You cannot get the user's plain password from AAC8.

    If you enter `3`, the following message appears:

    ```
    NOTE: if office phone of AAC8 user is blank then the participant
    code will be used. You will see the list of such users at the end
    of migration process
    ```

14. Enter the relevant Virtual Room number template at the prompt.

    The default number template is `1`.

    ```
    Virtual Room Number Template [Participant code] :
            [1] Participant code
            [2] Moderator code
            [3] Office phone
    ```

    If you enter `3`, and the business phone of the AAC8 user is blank, the system uses the participant code.

15. (Only if the migration tool runs on Equinox Management) Enter `Y` so the system retrieves the prefix of the Virtual Room number automatically from the Equinox Management configuration file. Otherwise, enter `N` and then enter the prefix manually.

    The prefix is used for routing purposes.

    The migration settings are completed. A summary message appears on the display.

16. To continue exporting with these settings, enter `Y`.

    The tool performs the required migration operations. Upon completion, the following message typically appears on the display:

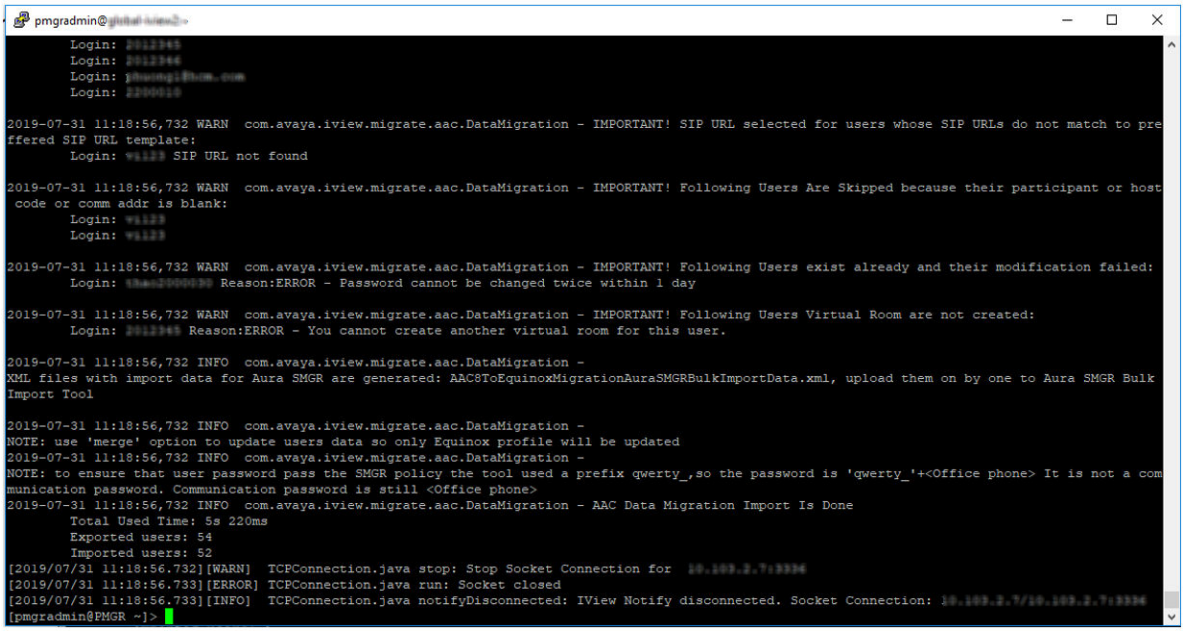


Figure 92: Example of successful migration message

- The screen displays warnings like: failed users, no SIP URL matches selected template, email is blank, or passcode encrypted.
- The screen displays a summary that contains information such as how many users are migrated.
- (Only for the `to Aura` deployment type) The tool generates XML files for SMGR bulk import (for example, AAC8ToEquinoxMigrationAuraSMGRBulkImportData_1.xml). Each file contains up to 1,000 users. This tool is required for importing LDAP and local user types into Equinox Management via System Manager and will be available for future releases. For the current release, data is pushed directly to Equinox Management.
- For the `to Non-Aura Equinox` deployment type, data is pushed directly to Equinox Management.

17. You are done with the migration process! Access Equinox Management to check that the local user basic data and their virtual rooms was migrated from AAC8 and created in the Equinox Management database:

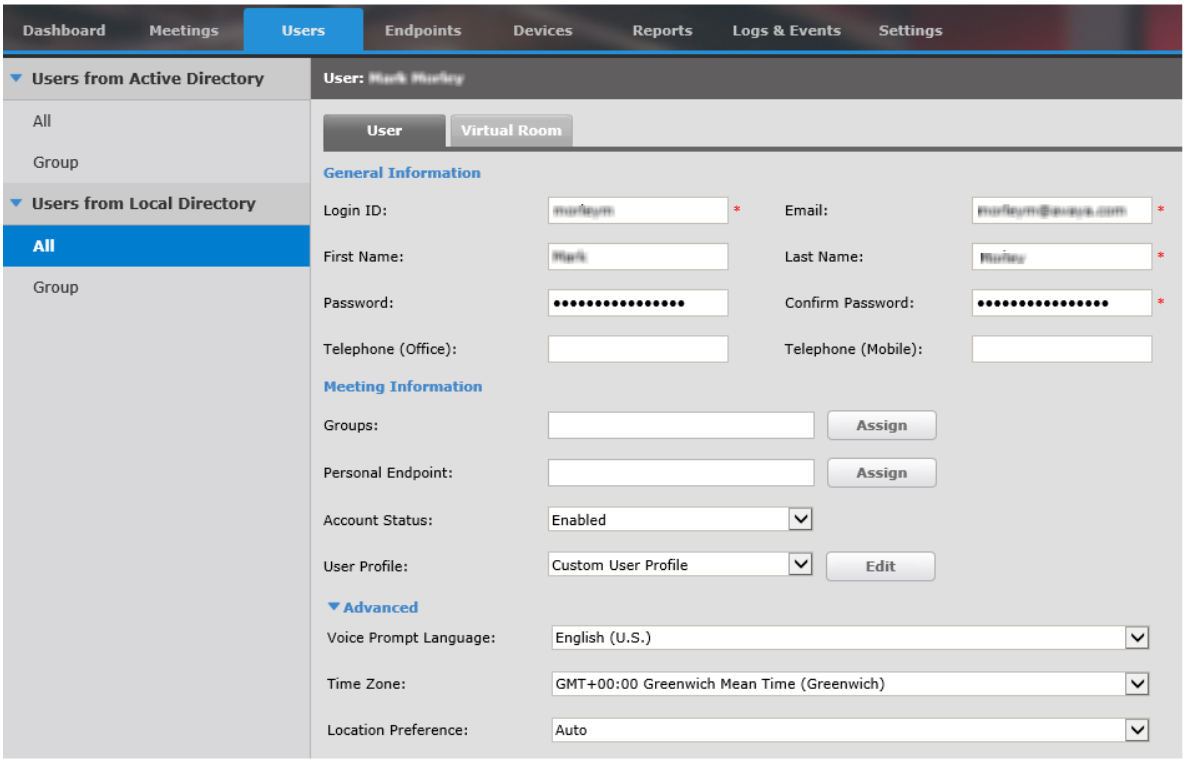


Figure 93: Example of user basic data in Equinox Management after migration

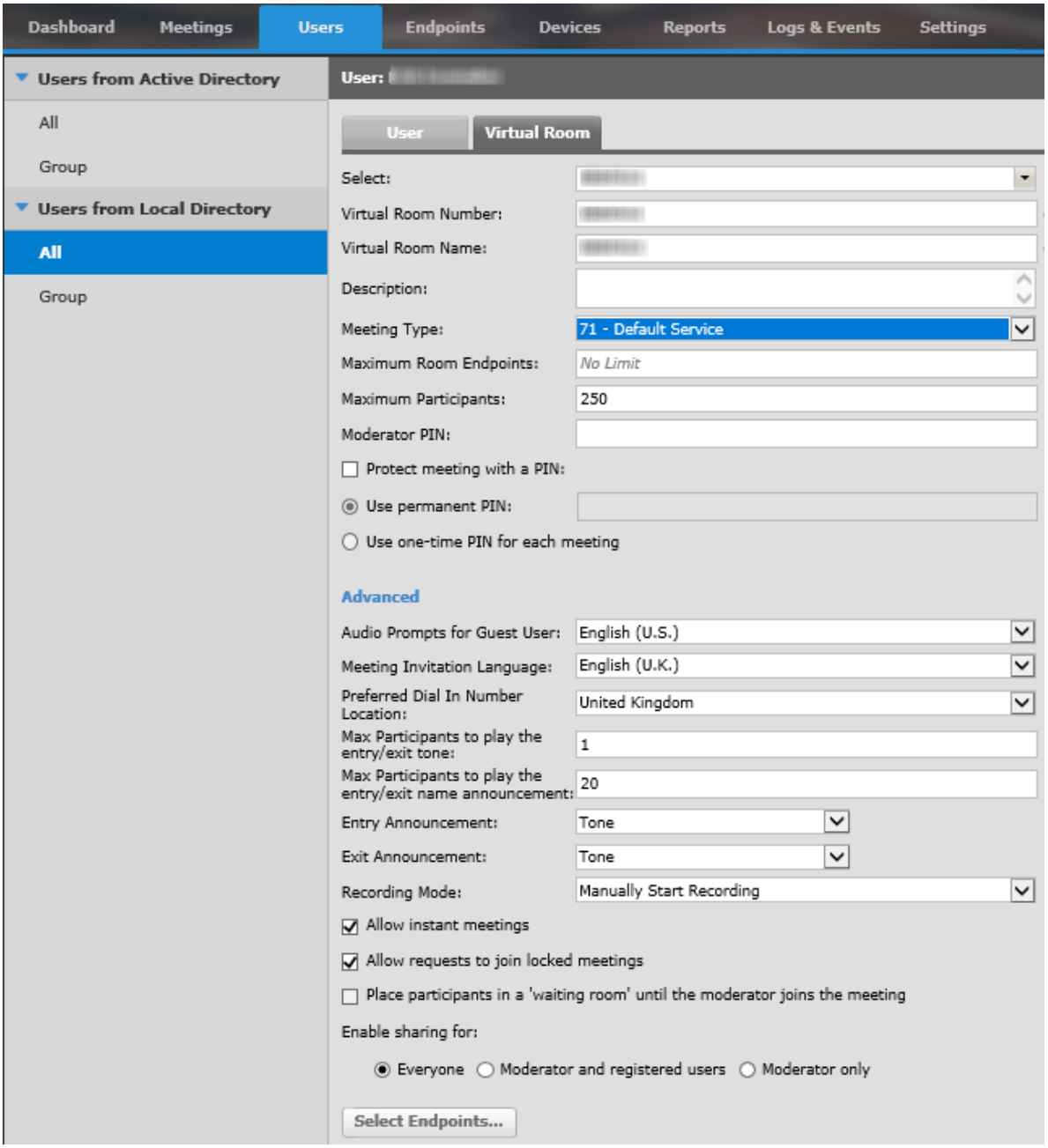


Figure 94: Example of user's virtual room in Equinox Management after migration

Chapter 11: Avaya Session Border Controller deployment for remote access in Over The Top solution

Configuration checklist for remote access in OTT — Non-tunneled and tunneled mode

This chapter describes how to configure Avaya SBCE for conferencing with remote Avaya Equinox® Meetings for Web (WebRTC) Clients, Avaya IX™ Workplace Clients (Meet-me), and Avaya approved SIP endpoints.

Participants in conferences have to interact with multiple servers through HTTPS. To avoid using multiple external public IPs, FQDNs, and certificates, the solution uses ASBCE URL rewriting. The method solves this interfacing complexity by allowing guests to access a conference via a single FQDN and a single IP address, using port 443. As each FQDN needs a certificate, and there is only one FQDN to interact with, this method also allows saving on the costs of commercial certificates. URL rewriting can be used in all Equinox deployments.

You must set up and configure the solution components as described in each server documentation. For a full explanation on configuring servers that are part of the deployment, download documents from the Avaya Support website at http://support.avaya.com. See Capacity and scalability specification on page 252 for important information specific to Equinox Conferencing.

The procedures in this chapter describe only a few of the device settings that are required for the deployment.

Use this checklist as an example of deploying an ASBCE that supports up 250 calls in non-tunneled mode, using the URL rewriting method.

No.	Task	Link/Notes	✔
1	Plan your deployment.	Avaya SBCE deployment in the OTT solution on page 238	

Table continues…

No.	Task	Link/Notes	✔
2	Ensure that the Equinox system is up and internally operational in the enterprise.		
3	Install ASBCE (version 7.2 and up) in a virtualized environment.	For a full explanation on deploying ASBCE, download the document on *Deploying Avaya Session Border Controller in Virtualized Environment* from the Avaya Support website at http://support.avaya.com	
4	Ensure that you have administrator privileges on the Equinox system.	See the administration guides of the Equinox system components. You can download the documents from the Avaya Support website at http://support.avaya.com.	
5	Ensure that you have administrator privileges on ASBCE.	For a full explanation on deploying ASBCE, download the document on *Administering Avaya Session Border Controller for Enterprise* from the Avaya Support website at http://support.avaya.com.	
6	Configure TLS certificates.	See Certificates on page 256.	
7	Configure the external TLS Server profile.	Configuring the TLS Server Profile for Avaya SBCE external communication on page 260	
8	Configure the TLS Server Profile for media tunneling.	Configuring TLS Server Profile for Avaya SBCE Media Tunneling on page 261	
9	Configure the TLS Client Profile.	Configuring the TLS Client Profile on Avaya SBCE on page 262	
10	Configure network interfaces.	Configuring Avaya SBCE network interfaces on page 263	
11	Configure signaling interface.	Configuring Avaya SBCE signaling interface on page 264	
12	Configure media interface.	Configuring Avaya SBCE media interface for OTT on page 265	
13	Configure load monitoring.	Configuring Avaya SBCE load monitoring for OTT on page 267	
14	Configure server flows.	Configuring Avaya SBCE server flows for OTT on page 267	

Table continues…

No.	Task	Link/Notes	✔
15	Configure multiple server access using a single FQDN, a single IP address, and port 443. This is for a non-tunneled mode.	OTT deployment — Single IP and single FQDN for HTTP traffic on page 272	
16	Configure TURN/STUN for WebRTC calls.	For an introduction to TURN on browser or media server, see TURN/STUN for WebRTC calls in OTT on page 269. For configuration of TURN/STUN, see Configuring Avaya SBCE STUN TURN server for OTT on page 271.	
17	Configure ASBCE on Equinox Management.	Configuring Avaya SBCE on Equinox Management on page 279	
18	Configure ASBCE to support SIP calls from unregistered endpoints.	Configuring Avaya SBCE support of unregistered Avaya SIP endpoints on page 281	

Avaya SBCE deployment in the OTT solution

Consider a number of criteria when planning the Avaya SBCE deployment in your organization.

Network zones

The deployment assumes there are two zones: DMZ for edge devices, and Equinox internal for most servers. See the following figure.

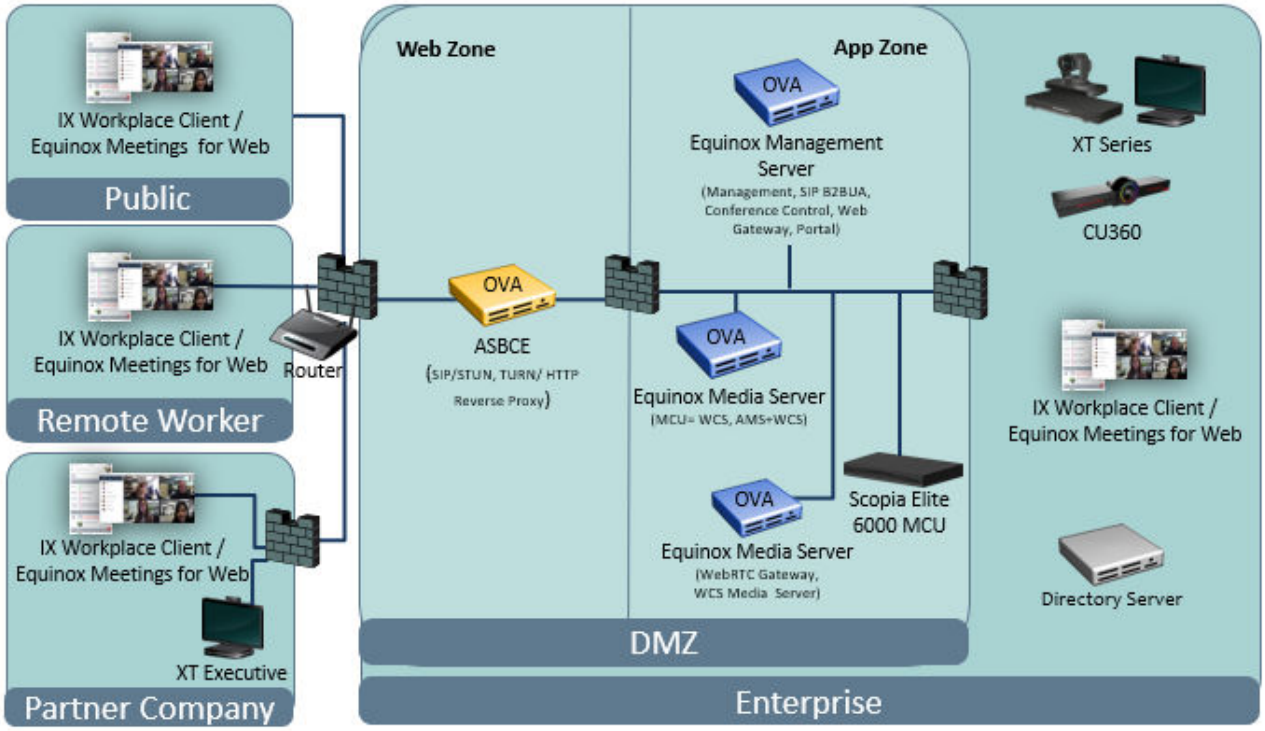


Figure 95: Network zones

The Equinox internal network can be the private network, or can be a zone that a firewall separates from the private network. There is no NAT between the Equinox internal network and the private one.

Most components are installed in the private network. This includes the Management and Media servers.

The edge devices include:

- Avaya SBCE: the main edge device for SIP, HTTPS and all clients. It has one interface in the DMZ and another one in the Equinox internal network.
- Reverse proxy: it can be part of Avaya SBCE in small deployments, or can be handled by an Avaya approved, third party load balancer (like A10). If the third-party load balancer is used, it must have one interface in the DMZ and the other one in the Equinox internal network.

  To use a third-party load balancer, you must disable the Equinox Management internal load balancer. For details, see Disabling the Internal Load Balancer in Equinox Management on page 99.

Avaya SBCE

Avaya SBCE is the key element for firewall traversal.

Avaya recommends that all HTTPS traffic goes through Avaya SBCE, as well as all traffic from outside the VPN.

Avaya SBCE serves four different (but similar) functionalities:

- HTTPS reverse proxy for all HTTPS traffic from outside and inside the VPN.

- SIP Avaya SBCE for external SIP entities (room systems).
- Media relay for Avaya IX™ Workplace Client.
- Media relay for Avaya Equinox® Meetings for Web.

Three functionalities use port 443, which means that Avaya SBCE needs three different external IP addresses (as well as certificates to match). If there is no need for 443 fallback, a single IP address can be used.

Single IP address and reverse proxy

Internal servers (such as Media and Management servers) use HTTPS. To avoid having an external IP address (and certificate) for each internal server, most traffic is multiplexed over a single IP address and FQDN, with the reverse proxy distributing the traffic to the different internal servers. HTTPS traffic for internal traffic must also be multiplexed, and the internal traffic go also through the reverse proxy. This can be done using the same reverse proxy with the internal interface and might require an additional IP address.

Media tunneling

By default, media (audio and video) use UDP as the transport protocol. Voice and video over IP are designed to use UDP, which provides the best conferencing quality.

Clients from various locations must be able to join a conference, including guests that are located behind a remote organizational firewall. Because this type of firewall sometimes blocks UDP traffic, a TCP fallback solution must be provided. Fallback to port 443 which is typically outbound open in most organizations also needs to be part of the solution.

Equinox Solution provides the following:

- By definition, SIP cannot use port 443.
- For client signaling and control, the solution always uses HTTPS over 443.
- For client's media, the solution prefers using UDP, but has a fallback to TCP 443 (also known as HTTP tunneling). Avaya SBCE handles the tunneling.
- Avaya IX™ Workplace Client and Avaya Equinox® Meetings for Web client use two different tunneling modes, due to browser limitations. Both use TCP 443, but in a different way.
  - Avaya IX™ Workplace Client uses TLS session port 443. The client does not validate the trust chain for this certificate, but uses fingerprints provided during signaling (similar to DTLS). Hence, the certificate used by Avaya SBCE does not need to be from a trusted CA.
  - Avaya Equinox® Meetings for Web uses TCP session on port 443.

Certificates

Because there are several services and several IP addresses, Avaya SBCE needs a certificate with multiple SAN, signed by a trusted third party CA that includes FQDN for the reverse proxy and SIP interfaces, and FQDNS for all public facing services. Depending on the type of deployment, the certificate can include up to five SANs.

Certificate map

The deployment is based on the concept of two CAs:

- A third party CA (such as go Daddy, Entrust, or VeriSign) that sign certificate for the client facing components.

- An internal CA that signs certificates for most servers. It is possible to have all certificate signed by a third party.

For servers, the concept is implemented as follows:

- Avaya SBCE must be aware of both CAs (third party and internal) and must have self certificates from both. The certificate from the external CA is used to client facing interface (external and internal) while internal CA certificate is used for server facing interfaces (internal only).
- Management server must be aware of both CAs. It must have the self certificate from the internal CA only. The Management server must also be aware of and trust other CAs because it interacts with non Equinox components such as the LADP server.
- All other servers (such as Media and Portal) must only be aware of and trust the internal CA, from which they need to have a certificate.

Note:

For client tunneling, the concept is implemented as follows:

- Web-RTC tunneling for Avaya Equinox® Meetings for Web Clients

  WebRTC requires an additional B1 IP address on Avaya SBCE. As such, another third party external CA is required for the WebRTC tunneling address.

- Avaya IX™ Workplace Client Meet-Me tunneling

  Avaya IX™ Workplace Client connecting as Meet-Me to the Equinox Portal URL via Avaya SBCE requires an additional B1 meet-me tunneling IP address on Avaya SBCE. Avaya IX™ Workplace Client is usually downloaded from the portal with the organization's internal CA already installed. As such, an internal CA certificate for the Avaya SBCE tunneling address is sufficient in most cases.

  A third party external CA certificate is required when using Avaya IX™ Workplace Client downloaded from organization X and used as Meet-Me to connect to organization Y.

Capacity

A single Avaya SBCE can handle up to 1,000 clients for reverse proxy (internal or external), 300 clients for media (UDP) and 100 clients for 443 media tunneling if needed.

If the required capacity is higher, more servers need to be installed.

Server redundancy and capacity

Consider the following when planning redundancy:

- Media servers: any number of servers can be installed, and they have internal load balancing. There is no need for an external load balancer. The redundancy module is N+1.

  Note:

  In the N+1 redundancy, all the servers are active and in normal operation mode the solution capacity is higher. When one of the servers fails, the system drops capacity to N, which is the originally desired capacity.

- Management server: it is possible to install an extra server for redundancy. There is no option to install more than one server for extra capacity. The redundancy module is an active-standby HA pair with virtual IP.

- Portal: in a small deployment, the Portal co-resides on the Management server with the same redundancy module. For a larger deployment, the Portal can be distributed from Management, and more than one server can be installed for capacity. There is internal load balancing with N+1 redundancy using virtual IP.
- UCCS (also called Equinox Conference Control): the Conference Control manager. In a small deployment, UCCS co-resides on the Management server with the same redundancy module. For larger cases, UCCS can be distributed from management, and more than one server can be installed for capacity. There is internal load balancing and redundancy. There is no need for a virtual IP.
- Avaya SBCE for reverse proxy: no internal load balancing exists, so capacity is limited to a single server. However, it is possible to install tow servers for redundancy HA pair using virtual IP.
- Avaya SBCE for SIP (room systems): no internal load balancing exists, so capacity is limited to a single server. However, it is possible to install tow servers for redundancy HA pair using virtual IP.
- Avaya SBCE for clients: the server supports HA pairs (1+1).
- For large deployments with HTTP reverse proxy: Avaya recommends to use an approved, external load balancer (such as A10). Capacity and the redundancy module depend on the server.

Related links

Small deployment on page 242
Medium deployment on page 244
Large deployment on page 245
Firewall traversal in OTT — normal security on page 248
Firewall traversal in OTT — enhanced security on page 250

Small deployment

A small deployment has the following characteristics:

- Up to 500 concurrent calls altogether, up to 50 outside the VPN, and needs tunneling.
- Portal and UCCS co-reside with Management.
- Avaya SBCE handles reverse proxy.

Table 29: Small deployment configuration requirements

Component	Private network IP	DMZ IP	Internal CA certificate	External CA certificate	Redundancy module	Comments
Management	One IP address with FQDN		FQDN based		For HA pair: 2 servers and 3 IPs	Including UCCS and portal

Table continues…

Component	Private network IP	DMZ IP	Internal CA certificate	External CA certificate	Redundancy module	Comments
Media servers	One IP address, no FQDN except if WCS is required.		IP based		N+1	All kinds: Scopia® Elite 6000 MCU, Equinox Media Server, standalone WCS Media Server (AMS), Web Gateway
SBCE	Two addresses: 1. For incoming reverse proxy with FQDN 2. For all other traffic, no FQDN	Three addresses: 1. For reverse proxy and SIP, with FQDN 2. For Avaya IX™ Workplace Clienttunneled and non-tunneled media , no FQDN 3. For all Web Client media (TURN), tunneled and non-tunneled , no FQDN	For 2., under the *Private network IP address* column: IP based for DMZ IP; IP based for private IP.	Multiple SAN. Public facing CAs must have FQDNs defined.	HA pair	

Related links

Avaya SBCE deployment in the OTT solution on page 238

Medium deployment

The deployment has the following characteristics:

- Up to 1,000 concurrent calls altogether, more than 50 outside the VPN, and needs tunneling.
- Portal and UCCS co-reside with Management.
- Avaya SBCE handles reverse proxy.
- One SBCE (HA pair) for reverse proxy and standard SIP (room systems).
- Multiple SBCEs for client media (tunneled and none tunneled).

Table 30: Medium deployment configuration requirements

Component	Private network IP	DMZ IP	Internal CA certificate	External CA certificate	Redundancy module	Comments
Management	One IP address with FQDN		FQDN based		For HA pair: 2 servers and 3 IPs	Including UCCS and portal
Media servers	One IP address, no FQDN except if WCS is required		IP based		N+1	All kinds: Scopia® Elite 6000 MCU, Equinox Media Server, standalone WCS, Media Server (AMS)
Main SBCE	Two IP addresses: 1. For incoming reverse proxy with FQDN 2. For all other traffic no FQDN	One IP address with FQDN for reverse proxy and SIP	See 2., under the *Private network IP address* column: IP based for private IP	Multiple SAN. Public facing CAs must have FQDNs defined.	HA pair	For reverse proxy and standard SIP – room systems outside the VPN

Table continues…

Component	Private network IP	DMZ IP	Internal CA certificate	External CA certificate	Redundancy module	Comments
Media SBCE	One IP address, no FQDN	Two IP addresses: 1. For Avaya IX™ Workplace Clienttunneled and non tunneled media no FQDN 2. For all Web Client media (TURN), tunneled and non-tunneled no FQDN	IP based for private IP	Multiple SAN. Public facing CAs must have FQDNs defined.	N+1	For client media

Related links

Avaya SBCE deployment in the OTT solution on page 238

Large deployment

The deployment has the following characteristics:

- Over 1,000 concurrent calls.
- More than one Portal, separated from Management. Internal load balancing.
- More than one UCCS, separated from Management. Management load balancing.
- External load balancer acting as reverse proxy (A10 or other Avaya approved) .
- One Avaya SBCE (HA pair) for standard SIP.
- Multiple SBCEs for client media (tunneled and non-tunneled).

Table 31: Large deployment configuration requirements

Component	Private network IP	DMZ IP	Internal CA certificate	External CA certificate	Redundancy module	Comments
Management	One IP address with FQDN		FQDN based		For HA pair: 2 servers and 3 IPs	Including UCCS and Portal
Portal servers	One address, no FQDN for each server + one virtual IP (VIP) address with FQDN		IP based for each server plus one FQDN based for the VIP		N+1	Internal load balance using VIP
UCCS	One IP address with FQDN		FQDN based		N+1	
Media servers	One IP address, no FQDN except if WCS is required.		IP based		N+1	All kinds: Scopia® Elite 6000 MCU, Equinox Media Server, standalone WCS, Media Server (AMS), Web Gateway
SIP SBCE	One IP address, no FQDN	One IP address with FQDN	IP based for private IP address	FQDN based for DMZ IP address	HA pair	For room systems outside the VPN

Table continues…

Component	Private network IP	DMZ IP	Internal CA certificate	External CA certificate	Redundancy module	Comments
Media SBCE	One IP address, no FQDN	Two IP addresses: 1. For Avaya IX™ Workplace Clienttunneled and non-tunneled media no FQDN 2. For all Web Client media (TURN), tunneled and non-tunneled no FQDN	IP based for private IP address	Multiple SAN – two DMZ IP addresses	N+1	For client media
Load balancer	Two IP addresses: 1. For incoming reverse proxy (listen) with FQDN 2. For all outgoing (toward servers), no FQDN	One IP addresses with FQDN	IP based for internal IP. See 2., under the*Private network IP address* column.	FQDN based for DMZ IP and private IP. See 1., under the *Private network IP address* column. Same FQDN, same certificate.	HA pair	Depending on the type of load balancer, it may be able to use only one internal leg.

Related links

Avaya SBCE deployment in the OTT solution on page 238

Firewall traversal in OTT — normal security

The figure below illustrates how the components interact with the means for protecting the organization against intrusive attempts.

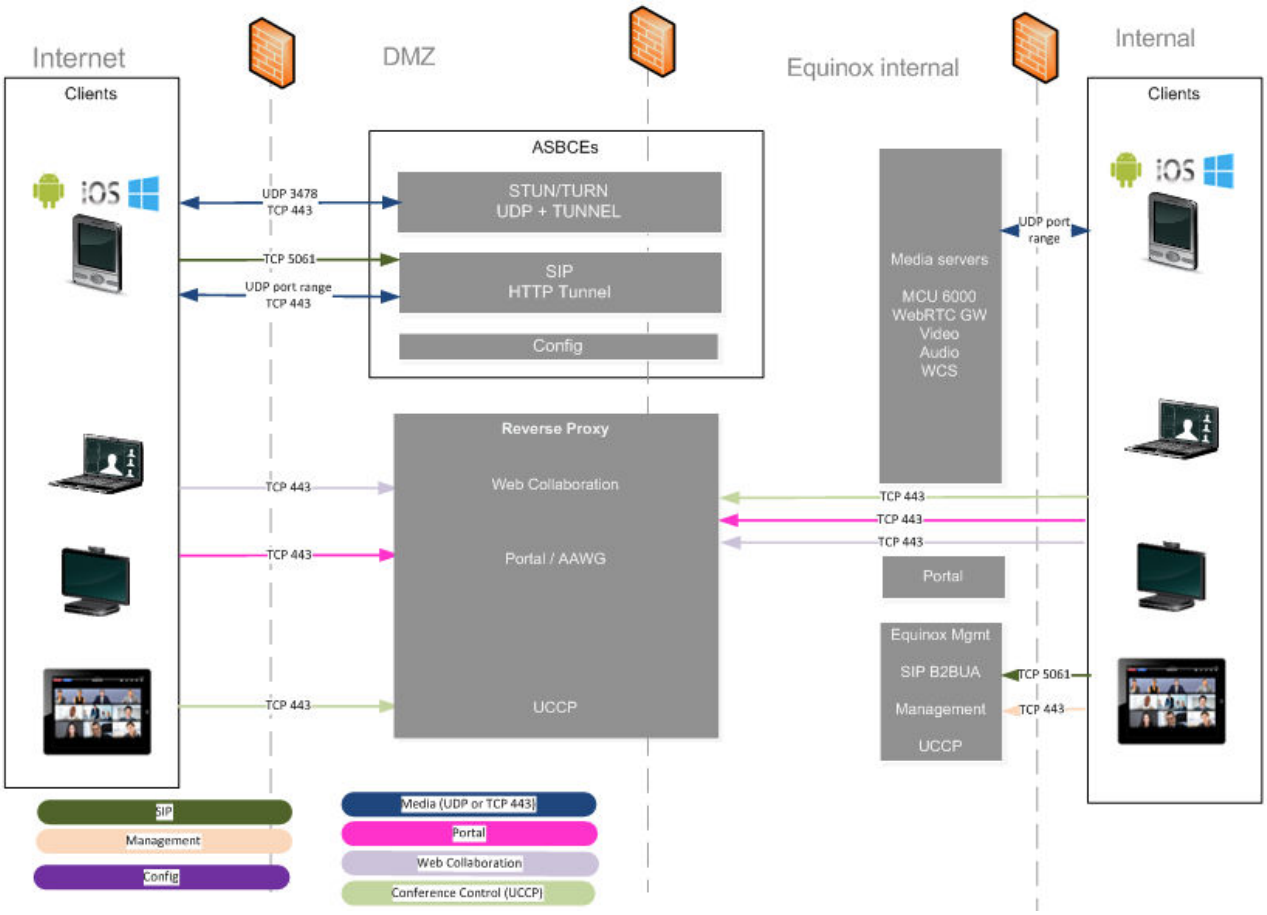


Figure 96: Normal security

When opening ports between the DMZ and the public, use the following as a reference:

Table 32: External firewall

External IP	External Port	DMZ IP	DMZ Port	Traffic type	Comments
Any	Any	SBCE Equinox leg	TCP 5061	SIP signaling	Always initiated from outside

Table continues…

External IP	External Port	DMZ IP	DMZ Port	Traffic type	Comments
Any	Any	SBCE Equinox leg	UDP - Configurable port range	UDP media for SIP endpoints and Avaya IX™ Workplace Clients	Bi-directional traffic
Any	Any	SBCE Equinox leg	TCP 443	Avaya IX™ Workplace Client media HTTP tunneling	Always initiated from outside
Any	Any	SBCE Equinox web leg	UDP 3478	UDP media for Equinox web clients	Always initiated from outside
Any	Any	Reverse proxy	TCP 443	HTTPS traffic - portal, conference control and web collaboration	Always initiated from outside

When opening ports between the Equinox servers and the clients inside the enterprise, use the following as reference:

Table 33: Between Equinox internal and private

Equinox Internal IP	Equinox Internal Port	Private IP	Private Port	Traffic type	Comments
Any media server	UDP - Configurable port range	Any client	UCP - any	RTP media	Bi-directional traffic
Management	TCP 5061	Any client	TCP - any	SIP signaling	Always initiated from inside
Reverse proxy	TCP 443	Any client	TCP - any	HTTPS traffic - portal, conference control and web collaboration	Always initiated from inside
Management	TCP 443	Any admin	TCP - any	Admin access	Can have whitelist IP for administrators

Related links

[Avaya SBCE deployment in the OTT solution](#) on page 238

Firewall traversal in OTT — enhanced security

The figure below illustrates how the components interact with the means for protecting the organization against intrusive attempts.

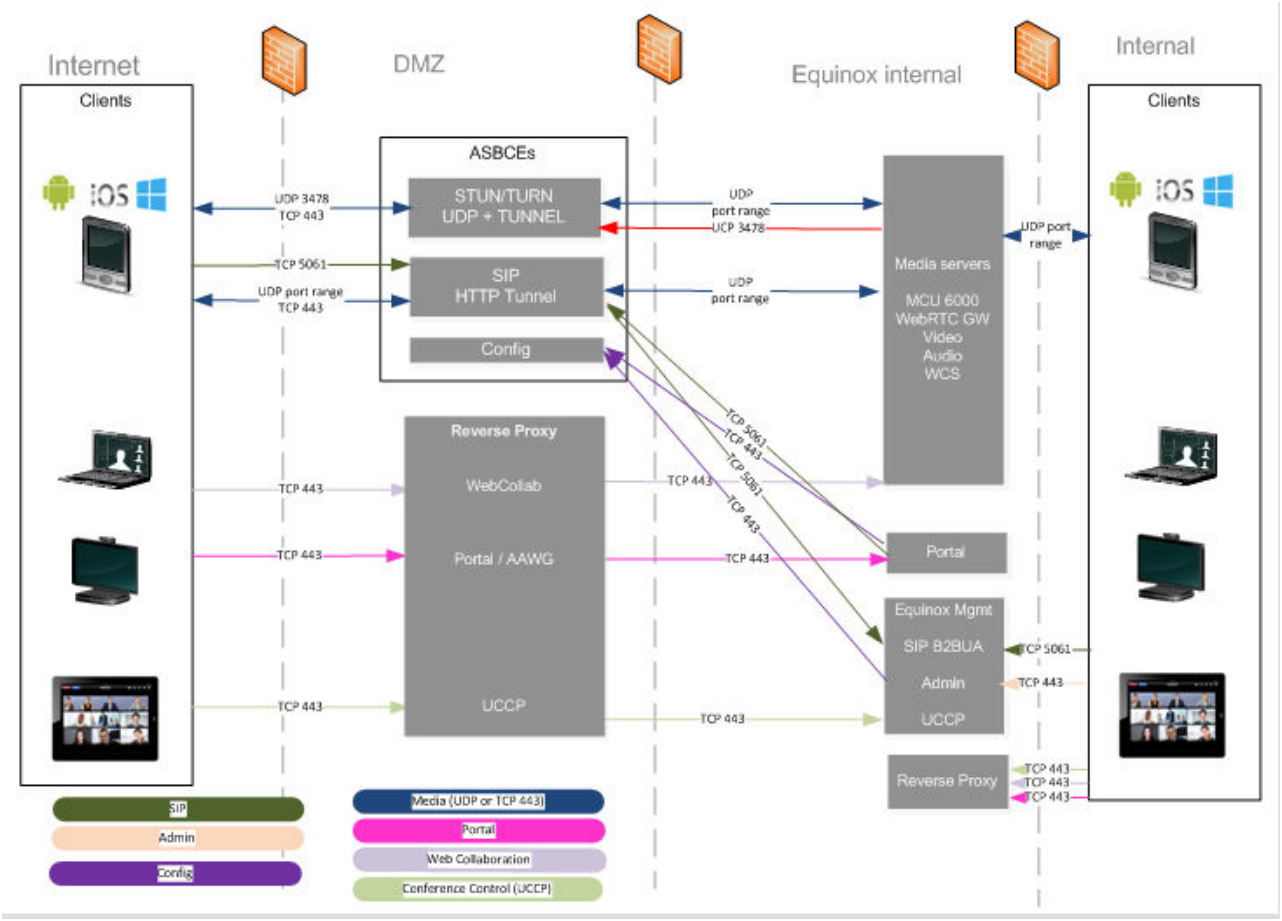


Figure 97: Enhanced security

When opening ports between the DMZ and the public, use the following as a reference:

Table 34: External firewall

External IP	External Port	DMZ IP	DMZ Port	Traffic type	Comments
Any	Any	SBCE Equinox leg	TCP 5061	SIP signaling	Always initiated from outside

Table continues…

External IP	External Port	DMZ IP	DMZ Port	Traffic type	Comments
Any	Any	SBCE Equinox leg	UDP - Configurable port range	UDP media for SIP endpoints and Avaya IX™ Workplace Clients	Bi-directional traffic
Any	Any	SBCE Equinox leg	TCP 443	Avaya IX™ Workplace Client media HTTP tunneling	Always initiated from outside
Any	Any	SBCE Equinox web leg	UDP 3478, UCP 3478	UDP media for Equinox web clients	Always initiated from outside
Any	Any	Reverse proxy	TCP 443	HTTPS traffic - portal, conference control and web collaboration	Always initiated from outside

When opening ports between the DMZ and the Equinox servers, use the following as a reference:

Table 35: Between DMZ and Equinox internal

DMZ IP	DMZ Port	Equinox Internal IP	Equinox Internal Port	Traffic type	Comments
SBCE internal leg	UDP - Configurable port range	Any media server	UDP - Configurable port range	RTP media	Bi-directional traffic
SBCE internal leg	UDP 3478	Any media server	UDP - Configurable port range	STUN	Always initiated from inside
SBCE internal leg	TCP 443	Portal	TCP - any	Configuration	Always initiated from inside
SBCE internal leg	TCP 443	Management	TCP - any	Configuration	Always initiated from inside
SBCE internal leg	TCP - any	Management	TCP 5061	SIP signaling	Always initiated from inside
SBCE internal leg	TCP 5061	Portal	TCP - any	SIP signaling	Always initiated from outside
Reverse proxy	TCP - any	Any media server	TCP 443	Web collaboration	Always initiated from outside
Reverse proxy	TCP - any	Portal	TCP 443	Portal and signaling	Always initiated from outside
Reverse proxy	TCP - any	Management	TCP 443	Conference control	Always initiated from outside

When opening ports between the Equinox servers and the clients inside the enterprise, use the following as reference:

Table 36: Between Equinox internal and private

Equinox internal IP	Equinox internal port	Private IP	Private port	Traffic type	Comments
Any media server	UDP - Configurable port range	Any client	UCP - any	RTP media	Bi-directional traffic
Management	TCP 5061	Any client	TCP - any	SIP signaling	Always initiated from inside
Reverse proxy	TCP 443	Any client	TCP - any	HTTPS traffic - portal, conference control and web collaboration	Always initiated from inside
Management	TCP 443	Any admin	TCP - any	Admin access	Can have whitelist IP for administrators

Related links

Avaya SBCE deployment in the OTT solution on page 238

Avaya SBCE technical specifications

Capacity and scalability specification

High-capacity servers

Solutions	Server Type					
	Dell™ PowerEdge™ R640 Avaya Solutions Platform 100 series server with profile 5	Dell R630 server with TILEncore-Gx36 Intelligent Application Adapter	HP DL360 G9 server with TILEncore-Gx36 Intelligent Application Adapter	Dell™ PowerEdge™ R640 Avaya Solutions Platform 100 series server with profile 3	Dell R630 server	HP DL360 G9 server
Remote Worker Users (Sessions)	20,000 (10,000)	20,000 (7,500)	20,000 (7,500)	20,000 (8,000)	20,000 (7,500)	20,000 (7,500)

Table continues…

Solutions	Server Type					
	Dell™ PowerEdge™ R640 Avaya Solutions Platform 100 series server with profile 5	**Dell R630 server with TILEncore-Gx36 Intelligent Application Adapter**	**HP DL360 G9 server with TILEncore-Gx36 Intelligent Application Adapter**	**Dell™ PowerEdge™ R640 Avaya Solutions Platform 100 series server with profile 3**	**Dell R630 server**	**HP DL360 G9 server**
Avaya Equinox® Conferencing Video Sessions	800	800	800	800	800	800
TURN/STUN Audio-only Sessions	6,000	6,000	6,000	5,000	5,000	5,000
TURN/STUN Audio and Video Sessions	1,000	1,000	1,000	1,000	1,000	1,000
TURN/STUN Tunneling Audio-only Sessions	600	600	600	600	600	600
TURN/STUN Tunneling Audio and Video Sessions	300	300	300	300	300	300
HTTP Media Audio-only Tunneling Sessions	220	220	220	220	220	220
HTTP Media Audio and Video Tunneling Sessions	110	110	110	110	110	110

Mid-capacity servers

Solutions	Server Type					
	Dell™ PowerEdge™ R340 Avaya Solutions Platform 100 series server	**Dell R330 server**	**HP DL360 G9 server**	**VMware ESXi 6.x-based server**	**Avaya Aura® Appliance Virtualization Platform**	**Nutanix AHV on Nutanix server**
Remote Worker Users (Sessions)	5,000 (2,000)	5,000 (2,000)	5,000 (2,000)	6,000 (3,000)	6,000 (3,000)	6,000 (3,000)
Avaya Equinox® Conferencing Video Sessions	200	200	200	200	200	200
TURN/STUN Audio-only Sessions	1,200	1,200	1,200	1,800	1,200	1,200
TURN/STUN Audio and Video Sessions	300	300	300	300	300	300
TURN/STUN Tunneling Audio-only Sessions	220	220	220	220	220 (4 vCPU) 550 (10 vCPU)	220
TURN/STUN Tunneling Audio and Video Sessions	110	110	110	110	110 (4 vCPU) 275 (10 vCPU)	110
HTTP Media Audio-only Tunneling Sessions	220	220	220	220	220 (4 vCPU) 550 (10 vCPU)	220
HTTP Media Audio and Video Tunneling Sessions	110	110	110	110	110 (4 vCPU) 275 (10 vCPU)	110

Additional capacity values for high-capacity and mid-capacity servers

Avaya SBCE supports up to 250 Internet telephony service providers (ITSPs) per system.

Avaya SBCE supports up to 250 tenants per system.

Avaya SBCE supports the following reverse proxy capacities per system:

- 500 HTTP requests per second
- 50 TLS connections per second
- 2,000 concurrent webSockets

General capacity considerations

Each value in the tables represent the maximum capacity supported by Avaya SBCE for that solution and cannot be combined for overall capacity calculations.

The capacity specifications are based on:

- Codec specification: the G729 and G711 codecs are used for measuring transcoded capacities. Different codecs will have varying results.
- Call model: the SIP RFC call model in trunk mode is used to establish these capacity specifications.
- IPv4 vs. IPv6: IPv4 as the transport protocol for calculating non-encrypted sessions with trunking for the Avaya Solutions Platform 100 series server with profile 5 (Dell™ PowerEdge™ R640). With IPv6, the value may decrease by 20%.
- All the audio and video session counts are calculated by assuming Avaya SBCE anchors media. For all other platforms except Portwell CAD-0230 and Portwell CAF-0251, the performance metrics are calculated by testing with the dedicated SBCE device managed by a separate EMS.

Remote Worker capacity considerations

One exception to the standard capacity values is for remote users and Remote Worker call capacity because registration is required for Remote Worker functionality. Mixed usage of the traffic capacities for solutions will vary and must be determined based on these requirements.

While implementing Remote Worker at maximum capacity limits, set registration expiry timers in Session Manager and in every client at a minimum of 3,600 seconds or one hour.

While implementing Remote Worker at maximum capacity limits in one Avaya SBCE or HA pair, under worst-case failover conditions, re-registration for 10,000 users can take up to 20 minutes. During re-registration, all ongoing calls continue uninterrupted. However, under worst-case conditions, a user cannot receive or make new calls during this re-registration time period. Distributing users across multiple Avaya SBCE systems significantly reduces this re-registration time.

VMware ESXi capacity considerations

For VMware ESXi 6.x, it is recommended that capacities are measured with 4 CPU and 8 GB RAM. For more information, see *Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform*.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Certificates

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.

Unregistered remote clients use HTTPS to connect to an Equinox meeting. In HTTPS, Transport Layer Security (TLS) enables network devices to communicate securely using certificates, to provide authentication of the devices and encryption of the communication between them.

The folllowing procedures describe how to generate and install an SBCE Portal and services certificate for internal and external reverse proxy.

Related links

Creating a Certificate Signing Request on page 256
Generating and installing certificates with Aura System Manager default CA on page 257
Installing a CA certificate on ASBCE on page 259
Installing a certificate and key on Avaya SBCE on page 259

Creating a Certificate Signing Request

About this task

The portal and services certificate is the most important certificate. It must be signed by a third party Certificate Authority. For information on certificates and TLS profile management, refer to *Administering Avaya Session Border Controller for Enterprise*.

Procedure

1. In the ASBCE UI, select **TLS Management** > **Certificates**. The **Certificates** tab page appears.
2. Select **Generate CSR**. The **TLS Management Generate CSR** window appears. Configure all the fields in the window:
   - **Country Name**: The name of the country within which the certificate is being created.
   - **State/Province Name**: The state/province where the certificate is being created.
   - **Locality Name**: The locality (city) where the certificate is being created.
   - **Organization Name**: The name of the company or organization creating the certificate.
   - **Organizational Unit**: The group within the company or organization creating the certificate.
   - **Common Name**: The name used to refer to or identify the company or group creating the certificate. You cannot provide wildcard (*) characters in this field.
   - **Algorithm**: The hash algorithms (SHA256) to be used with the RSA signature algorithm.
   - **Key Size (Modulus Length)**: 2048 in bits.

- **Key Usage Extension(s)**: The purpose for which the public key might be used: Key Encipherment, Non-Repudiation, Digital Signature.
- **Extended Key Usage**: Server Authentication, Client Authentication.
- **Subject Alt Name**: A text field used to further identify this certificate. It must have the following format:
  `DNS:<portalFQDN>,IP:<PublicIP_of_SBCE_for_TLS_Tunneling_WEbRTC>`
- **Passphrase**: The password used when encrypting the private key.
- **Confirm Passphrase**: A verification field for the Passphrase.
- **Contact Name**: The name of the individual within the issuing organization acting as the point-of-contact for issues relating to this certificate.
- **Contact E-mail**: The e-mail address of the contact.

3. Select **Generate CSR**.
4. Download and save the CSR request (.csr) and the key (.key).
5. Delete the key generated and saved on ASBCE - it has a wrong name and will cause issues later. If you cannot see it, navigate to a different page on the ASBCE and return to the previous page.
6. Send the certificate to the third party Certificate Authority to have it signed.

Related links

Certificates on page 256

Generating and installing certificates with Aura System Manager default CA

About this task

Use the System Manager as a Certificate Authority, or send the certificate to a third party Certificate Authority for validation. For detailed information, see *Administering Avaya Aura® System Manager*

information

Before you begin

Take the following into consideration:

- A Certificate Signing Request (CSR) is used by a server to apply for an SSL/TLS certificate.
- Certificate profiles determine the specific behavior of a certificate type, mainly through particular extensions. There are default certificate profiles available, and this procedure assumes you will use the built-in ID_CLIENT_SERVER profile.
- End entities are users such as a browser, an email client, or a server. This procedure assumes you are adding a server, using the default INBOUND_OUTBOUND_TLS end entity profile. This profile is used for client and server authentication.

Procedure

1. Login to Aura System Manager.
2. Navigate to **Security > Certificates > Authority**.
3. Navigate to **CA Structure & CRLs > Download PEM file** of the CA Certificate.
4. Click **Get CRL** and save them.
5. Check that the Certificate Profile is set as follows:
   - **Key Usage Extension**: Digital Signature and Key encipherment
   - **Extended Key Usage**: Server Authentication and Client Authentication
6. If you already configured an end entity, navigate to **Search End Entity**, enter the username and click **Search**. Select **Edit End Entity** link. In **Status**, select **New** and enter the missing password.

   To create an entity for the first time, navigate to **Add End Entity**. Enter the Username and Password, and save them for the next time you want to issue a certificate for same system. Use this procedure to accumulate certificates per user.

   Then configure these fields as follows:

   - **Subject DN > CN**: FQDN of server that provides TLS support.
   - **Subject Alternative Name**:
     - **DNS name**: FQDN of server that provides TLS support.
     - **IP Address**: IP address of the IP requiring TLS. It has the following format: `PublicIP_of_SBCE_for_TLS_Tunneling_WebRTC`
   - **Certificate Profile**: **ID_CLIENT_SERVER** with its relevant key features.
   - **CA**: **tmdefaultca**.
   - **Token**: **User Generated** .
   - Click **Add** (if new entity) or **Save** (in case of an existing entity).
7. Navigate to **Public Web**.
8. Navigate to **Enroll > Create Certificate from CSR** .
9. Enter the Username and Password used when adding the end entity.
10. Open the CSR request (.csr) in a text editor and copy paste its content into the designated text box.
11. Roll Type: PEM certificate only (or PEM full certificate chain when certificate chain is needed)
12. Click **OK**. A certificate in PEM format is created (or a PEM full certificate chain is created when the certificate chain is needed).
13. Save the Certificate PEM file.

Related links

Certificates on page 256

Installing a CA certificate on ASBCE

Procedure

1. In the ASBCE GUI, go to **TLS Management > Certificates** and press **Install** .

   Configure these fields as follows:

   - **Type**: Select CA Certificate.
   - **Name**: Enter its name.
   - **Overwrite Existing**: Select if replacing CA with same name.
   - **Allow weak Certificate key**: Select if the CA certificate is signed with a weak key.
   - **Certificate File**: select the CA certificate file.
2. Press **Upload**.

Related links

Certificates on page 256

Installing a certificate and key on Avaya SBCE

About this task

For detailed information on uploading certificates, see TLS Management in *Administering Avaya Session Border Controller for Enterprise*.

Procedure

1. Rename the certificate (.pem) and key (.key) files to the same name, for example qs1.pem and qs1.key. The name must not contain a dot (".")
2. In the ASBCE GUI, navigate to **TLS Management > Certificates**.
3. Click **Install** and configure these fields as follows:

   - **Type**: the type of certificate you want to install.
   - **Name**: the name of the certificate you want to install.

     This field is optional, and if not specified, the filename of the uploaded certificate is used as the certificate name. Additionally, specifying a name same as another certificate will overwrite the existing certificate with the one being uploaded.
   - **Overwrite Existing**: An option to control whether uploading a certificate with the same name is permitted.

If this field is cleared, uploading a certificate with the same name as another certificate causes failure. If this field is selected, uploading a certificate with the same name overwrites an existing certificate.

- **Allow Weak Certificate Key**: An option to permit usage of a weak private keys. This option bypasses the check that requires strong private keys. EMS rejects private keys lesser than 2048 bits or signed with an MD5 based hash by default.
- **Certificate File**: The location of the certificate on your system. Click **Browse** or **Choose file** to browse for the file. If the third party CA provides separate Root CA and Intermediate certificates, you must combine both files into a single certificate file for ASBCE. To combine the files, add the contents of each certificate file one after the other, with the root certificate at the end.
- **Key**: The private key that you want to use. You can opt to use the existing key from the file system or select a file containing another key.
- **Key File**: The button that is displayed when you select **Upload Key File** in the **Key** field. Click **Browse** to locate the file.
- **Trust Chain File**: The trust chain file used to verify the authenticity of the certificate. Depending on the browser, click **Browse** or **Choose File** to locate the file.

4. Click **Upload**.
5. Copy the PEM-encoded certificate and associated private key to the EMS server.
6. To encrypt the RSA private key, type `enc_key` *`path_to_key_file private_key_passphrase`*.

   path_to_key_file is the path where the private key file is stored, and *private_key_passphrase* is the passphrase for the key. If the private key does not have a passphrase, use `""` as the *private_key_passphrase*

   Type this command while SSH accessing on EMS server.

Related links

Certificates on page 256

Configuring the TLS Server Profile for Avaya SBCE external communication

About this task

Avaya SBCE uses a TLS server profile to process an incoming connection over TLS from a remote client.

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **TLS Management** > **Server Profiles**.
4. Click **Add**.
5. In the **New Profile** page, configure the fields as follows:
   - **Profile Name**: enter a descriptive name to identify this profile.
   - **Certificate**: select the certificate for external communication.
   - **SNI Options**: set to *None.*
   - **Peer Verification**: select *None*.
   - **Extended Hostname Verification**: leave unchecked.
   - **Renegotiation Time**: set to *0*.
   - **Renegotiation Byte Count**: set to *0.*
   - **Version** of handshake options: set to **TLS 1.2**.
   - **Ciphers**: set to **Default**.

     For information on the fields, see *Administering Avaya Session Border Controller for Enterprise*.
6. Click **Finish**.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring TLS Server Profile for Avaya SBCE Media Tunneling

About this task

A TLS profile allows Avaya SBCE to control parameters when it performs a TLS handshake with a remote entity.

HTTPS media tunneling requires its own TLS server profile. Avaya SBCE supports media tunneling for sign-in and guest users. This configuration is required only for Meet-Me calls that are inbound towards Avaya SBCE.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **TLS Management** > **Server Profiles**.
4. Click **Add**.

5. In the **New Profile** page, configure the fields as follows:
   - **Profile Name**: enter a descriptive name to identify this profile.
   - **Certificate**: select the external certificate used by the TLS Server Profile for external communication.
   - **SNI Options**: set to *None.*
   - **Peer Verification**: select *Optional*.
   - **Peer Certificate Authorities**: leave empty.
   - **Peer Certificate Revocation Lists**: leave empty.
   - **Verification Depth**: select *1*.
   - **Extended Hostname Verification**: leave unchecked.
   - **Renegotiation Time**: set to *0*.
   - **Renegotiation Byte Count**: set to *0.*
   - **Version** of handshake options: set to **TLS 1.2**.
   - **Ciphers**: set to **Default**.

   For information on the fields, see *Administering Avaya Session Border Controller for Enterprise*.
6. Click **Finish**.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring the TLS Client Profile on Avaya SBCE

About this task

A TLS client profile is used when Avaya SBCE starts an outgoing connection towards a remote entity over TLS.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **TLS Management** > **Server Profiles**.
4. Click **Add**.
5. In the **New Profile** page, configure the fields as follows:
   - **Profile Name**: enter a descriptive name.
   - **Certificate**: select the certificate for internal communication.

- **SNI**: leave unchecked.
- **Peer Verification**: select *Required*.
- **Peer Certificate Authorities**: select the System Manager Certificate Authority certificate.
- **Peer Certificate Revocation Lists**: leave empty.
- **Verification Depth**: select *1*.
- **Extended Hostname Verification**: leave unchecked.
- **Renegotiation Time**: set to *0*.
- **Renegotiation Byte Count**: set to *0*.
- **Version** of handshake options: set to **TLS 1.2**.
- **Ciphers**: set to **Default**.

For information on the fields, see *Administering Avaya Session Border Controller for Enterprise*.

6. Click **Finish**.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring Avaya SBCE network interfaces

About this task

See the *Administering Avaya Session Border Controller for Enterprise* guide for detailed information on:

- System configuration
- Server and network configuration
- Device configuration
- WebRTC-enabled call processing

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **Network & Flows** > **Network Management > Networks**.
4. In addition to the M1, the management interface that was configured upon ASBCE installation, configure:
   - A1, the internal interface with at least 2 IP addresses associated to it.

- B1, the external IP addresses with at least 2 IP addresses associated to it.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring Avaya SBCE signaling interface

About this task

See the *Administering Avaya Session Border Controller for Enterprise* guide for detailed information on configuring the signaling interface in the system.

In this procedure, you configure the external and internal signaling interfaces for your deployment.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **Network & Flows** > **Signaling Interface** and select **Add**.
4. Configure the external signaling interface.
   - **Name**: enter the name for the external signaling interface (B1).
   - **IP Address**: the network name, identified by the interface name and VLAN tag, and IP address of the ASBCE used by SIP signaling messages traversing the network.
   - **TCP Port**: leave the field blank.
   - **UDP Port**: leave the field blank for a non-tunneled mode.
   - **TLS Port**: enter `5061`.
   - **TLS Profile**: select the previously configured TLS profile.
   - **Enable Shared Control**: do not select the checkbox
   - **Shared Control Port**: leave empty
5. Configure the internal signaling interface:
   - **Name**: enter the name for the internal signaling interface (A1).
   - **IP Address**: the network name, identified by the interface name and VLAN tag, and IP address of the ASBCE used by SIP signaling messages traversing the network.
   - **TCP Port**: leave the field blank.
   - **UDP Port**: leave the field blank for a non-tunneled mode.
   - **TLS Port**: enter `5061`.
   - **TLS Profile**: select the previously configured TLS profile.
   - **Enable Shared Control**: do not select the checkbox

- **Shared Control Port**: leave empty

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring Avaya SBCE media interface for OTT

About this task

Refer to the *Administering Avaya Session Border Controller for Enterprise* guide for detailed information on:

- Media tunneling
- Media interface
- Media video
- End point policy groups

Before you begin

Take note of the following:

- To configure the media interface in this procedure, you must use the same listen IP interface selected for STUN/TURN. For details, see Configuring Avaya SBCE STUN TURN server for OTT on page 271.
- The **Listen/Relay Public IP** configured in Equinox Management must match the external Media IP address used in this procedure. For details, see how to configure the ASBCE in Equinox Management, as described in the *Administrator Guide for Avaya Equinox® Management*.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. (Media tunneling only) Navigate to **Network & Flows** > **Advanced Options** > **Feature Control** tab. Select the **Media Tunneling** checkbox, and select **Save**.
4. To configure the external media interface, navigate to **Network & Flows** > **Media Interface** and select **Add** or clone an existing media rule (recommended).

   Configure these fields:

   - **Name**: enter media interface name
   - **IP Address**: select B1 IP address, taking the following into account:
     - Do not use this IP address for any other interface bound to port 443 (HTTP tunneling configuration).
     - Do not use VLAN tag for media tunneled interface.

- **Port Range**: for example, *35000–40000*
- **TLS Profile**: if media tunneling is disabled, keep this field set to **None**. Otherwise, select a TLS server profile for the media interface that was created as explained above. For self-signed certificates on the client, use the TLS server profile created for the external media interface.
- **Buffer Size**: select the buffer size from the list containing values from 400 to 1000 in KB.
- Click **Finish**.

5. To configure the internal media interface, navigate to **Network & Flows** > **Media Interface** and select **Add** or clone an existing media rule (recommended).

   Configure these fields:

   - **Name**: select a friendly name for this media interface. For example, `media TunnelingInternal`.
   - **IP Address**: Select the A1 IP address for media tunneling
   - **Port Range**: for example, *35000–40000*
   - **TLS Profle**: select a TLS server profile for the media interface, if media tunneling is enabled. For self-signed certificates on the client, use the TLS server profile created for the internal media interface.
   - **Buffer Size**: select the buffer size from the list containing values from 400 to 1000 in KB. For example, *500*
   - Click **Finish**.

6. To enable video media, navigate to **Domain Policies > Application Rules** page, and clone an existing application rule or add a new one.

   Configure these fields:

   - Enable **In/Out Audio/Video** application types.
   - Configure **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint**

7. (Not for media tunneling) To configure media encryption and enable BFCP and/or FECC, navigate to **Domain Policies > Media Rules** and clone an existing media rule or add a new one.

   Configure these fields:

   - On the **Encryption** tab, in the **Miscellaneous** section, select the **Capability Negotiation** checkbox.
   - On the **Advanced** tab, select the **BFCP Enabled** and **FECC Enabled** checkboxes.

8. To configure the policy group with the newly created application and media rules, navigate to **Domain Policies** > **> End Point Policy Groups** and clone an existing policy group or add a new one.

9. You must disable interworking when using HTTP tunneling. To disable interworking, navigate to **Domain Policies > Media Rules > Encryption** and uncheck the **Interworking** checkbox.

Configuring Avaya SBCE load monitoring for OTT

About this task

Refer to the *Administering Avaya Session Border Controller for Enterprise* guide for detailed information on load monitoring.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. n the left navigation pane, click **Network & Flows** > **Load Monitoring** > **Advanced Options**
4. Select **Add** to create the new load balancer profile.
5. Configure these fields as follows:
   - **Load Balancer Type**: select **INTERNAL**. Load Balancer on the A1 side of the network. Equinox Management does load balancing towards the internal side. All HTTP requests sent for dialing out use the internal load balancer logic to identify the appropriate ASBCE.
   - **Transport**: select the Load Balancer protocol.
   - **Listen IP**: select the internal interface (A1). It can be a separate IP address.
   - **Service Type**: select **TURN**.
6. Select **Finish**.

Configuring Avaya SBCE server flows for OTT

About this task

See the *Administering Avaya Session Border Controller for Enterprise* guide for detailed information on server flows. This procedure details the settings for the OTT solution.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. To create an Interworking Profile or update an existing profile, navigate to **Global Profiles > Server Interworking** and select **Add** for a new profile.

Configure these fields as follows:

- For a new profile, set all options as default.
- In **Advanced Options > Has Remote SBC**: select **No** (disabled).
- Ensure to select the right profile in the **Extensions** field.

  The setting directs the ASBCE security device to use functionality specific to different environments.

3. To add a configuration for Equinox Management, navigate to **Global Profiles > Server Configuration** and select **Add**.

   Configure these fields as follows:

   - **Server Type**: select **Trunk Server**.
   - **SIP domain**: you can leave it blank.
   - **TLS Client Profile**: select the previously created Equinox Management client profile if TLS port is specified.
   - Add the Equinox Management FQDN with port and protocol specified (TCP and/or TLS).
   - In **Advanced Options**, select the **Enable Grooming** checkbox and select the previously created Interworking Profile.
   - You can leave other settings with their default values.

4. To add a flow for Equinox Management, navigate to **Device Specific Settings > End Point Flows > Server Flows** and select **Add**.

   Configure these fields as follows:

   - **Flow Name**: enter a name such as `EqMngFlow`.
   - **Server Configuration**: select the configuration you previously created for Equinox Management.
   - **Received Interface**: select the internal interface (A1).
   - **Signaling Interface**: select the internal interface (A1).
   - **Media Interface**: select the internal interface (A1).
   - Select the **Endpoint Policy Group** as required.
   - You can leave other settings with their default values.

5. To add a configuration for the AAWG server, navigate to **Global Profiles > Server Configuration** and select **Add**.

   Configure these fields as follows:

   - **Server Type**: select **Trunk Server**.
   - **SIP domain**: you can leave it blank.
   - **TLS Client Profile**: select the previously created AAWG client profile if TLS port is specified.

- Add the AAWG FQDN with port and specified protocol (TCP and/or TLS). Add all cluster nodes.
- In **Advanced Options**, select the **Enable Grooming** checkbox and select the previously created Interworking Profile.
- You can leave other settings with their default values.

6. To add a flow for an AAWG server, navigate to **Device Specific Settings > End Point Flows > Server Flows** and select **Add**.

   Configure these fields as follows:

   - **Flow Name**: enter a name such as `AAWGFlow`.
   - **Server Configuration**: select the configuration you previously created for AAWG.
   - **Received Interface**: select the internal interface (A1).
   - **Signaling Interface**: select the internal interface (A1).
   - **Media Interface**: select the external interface (B1).
   - Select the **Endpoint Policy Group** as required.
   - You can leave other settings with their default values.

TURN/STUN for WebRTC calls in OTT

Up to Avaya SBCE release 7.2.1, Avaya based its WebRTC solution on a TURN client residing on the Media Server inside the enterprise. This solution forced traffic to go through inside the enterprise using the WebRTC Media Server (MCU or AMS) as the anchor point in a WebRTC call. This solution had some deficiencies, specifically in certain topologies where the browser was behind a corporate firewall that blocked all UDP traffic sent to an enterprise WebRTC Media Server.

For release 7.2.2 and up, Avaya has solved the issue by moving the TURN client to the browser.

Note:

The administrator can use both solutions, but not in the same deployment.

The following figure illustrates the WebRTC call flow with a browser based TURN client.

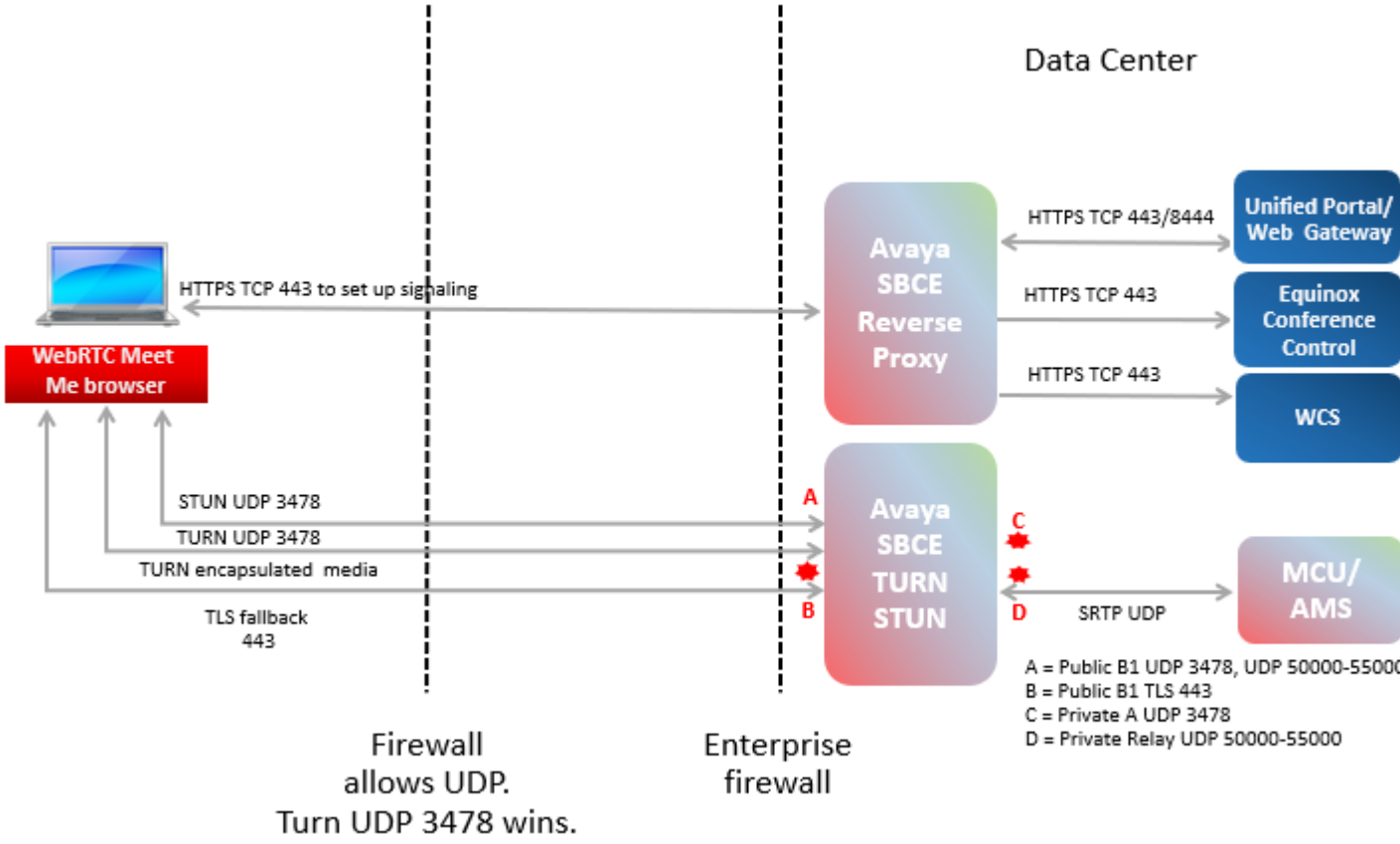


Figure 98: TURN Client on browser

For information on the component architecture, see Component architecture on page 18.

From the browser, the user launches the soft client. It tries to access the conference server running in the data center at the far end.

Call signaling uses the HTTPS channel, and goes through the Avaya SBCE reverse proxy to Equinox Conference Control.

One HTTP channel goes to the portal, and the configuration data comes in from the portal back to the browser. The configuration data includes the TURN server settings.

To present content, start/stop the presentation and share the screen on a device, the setup requires an HTTP channel with Web Collaboration Server (WCS).

Then, the browser initiates a call setup to Equinox Conference Control (UCCS) through reverse proxy.

The TURN and STUN server gathers the ICE candidates and handles media packet traversal through firewalls.

The REST control port is needed between the Web Gateway and the WebRTC Gateway.

If corporate firewalls block UDP, the TURN client on browser can use port TLS/443 to tunnel TURN messages through the firewall that blocks UDP. TURN on TLS encapsulates the media packets that the TURN Server on Avaya SBCE decodes at the enterprise edge.

Avaya SBCE is not aware of the far end topology. For that reason, the administrator must configure Avaya SBCE to accept STUN on UDP, TURN on UDP, and TURN on TLS. Depending on the TURN packets flowing through Avaya SBCE, it keeps one TURN relay open for the TURN encapsulated RTP flow, and closes the other TURN relay through which no TURN encapsulated packet flows.

Table 37: Client traffic through Avaya SBCE in an OTT deployment

Traffic type through ASBCE	Avaya Equinox® Meetings for Web for remote user, guest or sign-in (WebRTC	Avaya IX™ Workplace Client for remote user, guest or sign-in (HTTP)
STUN	If user is not behind a restricted firewall	N/A
TURN	If user is behind a restricted firewall	N/A
SRTP over UDP	N/A	If user is not behind a restricted firewall
HTTP Tunneling (SRTP over TLS)	N/A	If user is behind a restricted firewall

Related links

Configuring Avaya SBCE STUN TURN server for OTT on page 271

Configuring Avaya SBCE STUN TURN server for OTT

About this task

This procedure describes how to configure the ASBCE STUN TURN server that Avaya IX™ Workplace Client as Meet-me client and Avaya Equinox® Meetings for Web (WebRTC) clients use for media connection. See *Administering Avaya Session Border Controller for Enterprise* for detailed information on WebRTC-enabled call processing.

In addition to this procedure, you must also add the ASBCE STUN TURN server to Equinox Management, and then configure the STUN TURN server on the Media Server Configuration page for video media servers. For details, see *Configuring the Equinox Media Server from Equinox Management* in *Administrator Guide for Avaya Equinox® Management*.

Procedure

1. On the ASBCE UI, select **Device Specific Settings** > **TURN/STUN Service**.
2. On the **TURN/STUN Profiles** page, select **Add**.

   The **Add TURN STUN Profile** page opens. Configure the following fields as required:

   - **Profile Name**: Enter the name of the TURN/STUN profile.

- **UDP Listen Port**:Enter 3478.
- **Media Relay Port Range**: Enter the port range.
- **Media Learning**: Select the Media Learning check box in TURN/STUN Profiles only for deployments with TURN on AMS or MCU. Clear the Media Learning check box for TURN/STUN profile deployment on browser.

3. Select **Finish**.

   The results display on the **TURN/STUN Profiles** page.

4. Select the **TURN Relay** page and select **Add**. The **Add TURN STUN IP Pairing** page opens.

   Configure the following fields, as required:

   - **Listen IP**: Listen IP of TURN server. It shows the IP that was created in the TURN/STUN Profiles tab for that ASBCE device.
   - **Media Relay IP**: Media Relay IP of TURN server. It shows the IP that was created in the TURN/STUN Profiles tab for that ASBCE device.
   - **Service FQDN**: TURN server listen FQDN
   - **TURN / STUN Profile**: Displays the TURN/STUN profiles.

5. Select **Finish**.

Related links

TURN/STUN for WebRTC calls in OTT on page 269

OTT deployment — Single IP and single FQDN for HTTP traffic

Remote clients and endpoints that need to participate in conferences have to interact with multiple components through HTTPS. In a non-tunneled mode, the solution uses the ASBCE URL rewriting method to eliminate the need of multiple external public IPs, FQDNs, and certificates. With this method, guests can access a conference via a single FQDN and a single IP address, using port 443. As each FQDN needs a certificate, and there is only one FQDN to interact with, this method also allows saving on the costs of commercial certificates. URL rewriting can be used in all Equinox deployments.

The URL rewriting method enables using a single FQDN and a single IP address for accessing multiple media and management servers, via port 443.

You must set up and configure the solution components as described in the server documentation. The procedures described in this section are examples of configuration and include only a few of the settings required for the deployment.

Servers and services

These servers and services utilize HTTPS:

- User Portal (Avaya Aura® Web Gateway server).
- Equinox Conference Control (also called UCCS).
- Web Collaboration Server (WCS).

  This example describes a centric OTT deployment, so the User Portal and Equinox Conference Control reside on the same server as Equinox Management.

  WCS can be a standalone server (if it provides web collaboration for a legacy Scopia® Elite 6000 MCU) or be part of the Equinox Media Server (audio or video).

  Multiple Web Collaboration Servers are deployed for scalability and high capacity. Each server has a unique IP address and unique FQDN. Equinox Management is doing the load balancing among the multiple WCSs. If more than one portal or UCCS are needed, they share the same IP and FQDN using an external load balancer.
- Avaya Session Border Controller for Enterprise (ASBCE).

Firewall traversal

For Equinox Management, the client can be inside or outside the VPN. The setup requires the use of a split horizon DNS and a reverse proxy for firewall traversal.

In this example, the split horizon DNS means that the internal DNS resolves wcs1.mydomain.com to 10.0.0.11, while the external DNS resolves wcs1.mydomain.com to the reverse proxy's external leg. Thus, when the client tries to contact wcs1.mydomain.com externally, it reaches the reverse proxy.

Note:

For a successful deployment of the Equinox solution, it is mandatory to provision a split horizon DNS of the User Portal URL.

The following table lists the details of the servers used in this example.

Table 38: Configuring IP addresses and FQDNs in internal DNS

Type of server	Server IP address	Server FQDN	Listening port
Equinox Management that includes User Portal and Equinox Conference Control.	10.0.0.1	app.mydomain.com	443
WCS1	10.0.0.11	wcs1.mydomain.com	
WCS2	10.0.0.12	wcs2.mydomain.com	
WCS3	10.0.0.13	wcs3.mydomain.com	

Table 39: Configuring IP address and FQDN in External DNS

Type of server	Server IP address	Server FQDN	Listening port
ASBCE	150.50.0.1	equinox.mydomain.com	443

Take the following into consideration:

- The IP address of the ASBCE's internal leg is set to 10.0.0.21. There is no FQDN.
- The ASBCE does not support a reverse proxy where the incoming and outgoing traffic goes to the same IP address, so you must create an additional internal IP address (10.0.0.22) to be used by listeners.
- You can configure the port for the User Portal and Equinox Conference Control. The User Portal actually listens to two different ports: one port for the internal traffic, and another port for the external traffic. The external traffic is a port that only the reverse proxy knows. To implement remote firewall traversal (for guests from remote organizations), all HTTPS traffic use port 443.

URLs

Each service uses a different path in its URL. For example, the User Portal home page is `https://app.mydomain.com/portal/tenants/default/`.

Each service uses multiple URLs, and all URLs have the same format: `<FQDN>/service prefix>/<unique URL>`. For example, the portal home page is `https://app.mydomain.com/portal/tenants/default/`, where `/portal` is the service prefix.

Each service has more than one prefix:

Table 40: Service prefixes

Prefix	Service
/acs	AAWG
/ups	AAWG
/csa	AAWG
/uwd/dist	AAWG
/notification	AAWG
/portal	AAWG
/uwd/rest	UCCS
/uwd/ws	UCCS
/viewer	WCS
/wcsws	WCS
/plugins	WCS
/slider	WCS

Related links

Configuring remote client access to the Unified Portal on page 275
Configuring Equinox Conference Control for OTT on page 275
Configuring web collaboration for OTT on page 276
Configuring reverse proxy rules on ASBCE for OTT on page 276

Configuring remote client access to the Unified Portal

About this task

Login to Equinox Management to configure client access to the User Portal.

Before you begin

Follow the steps in the checklist.

Procedure

1. In Equinox Management, navigate to **Settings > Devices > User Portal/Web Gateway**.
2. Configure the following fields:
   - **Frontend FQDN** : the ASBCE FQDN (`equinox.mydomain.com`)
   - **Frontend Port**: `443`
   - **Enable TURN in WebRTC Client**: check the field.
3. Select **Apply**. The Frontend Scheme appears on the screen, formatted as `https://equinox.mydomain.com:443/portal`.

Related links

OTT deployment — Single IP and single FQDN for HTTP traffic on page 272

Configuring Equinox Conference Control for OTT

About this task

Log in to Equinox Management to configure Equinox Conference Control.

Before you begin

Follow the steps in the deployment checklist.

Procedure

1. In the Equinox Management administrator portal, navigate to **Dashboard > ☰ > Advanced Parameters**.
2. In the **Property Name** field, enter `com.visionnex.vcms.core.uccp.customizedUCCPURL`
3. In the **Property Value** field, enter (for example) `https://equinox.mydomain.com:443/uwd/ws?ticket=`
4. Select **Apply**.

Related links

OTT deployment — Single IP and single FQDN for HTTP traffic on page 272

Configuring web collaboration for OTT

About this task

Login to Equinox Management to configure client access to web collaboration. The Web Collaboration Server (WCS) is a component in the Equinox Media Server. WCS can also be used as standalone server when a Scopia® Elite 6000 MCU is deployed in the Equinox Solution.

Before you begin

Procedure

1. In Equinox Management, navigate to **Devices > Devices by Type >** `<Web Collaboration Server name (WCS1 in this example)>` **> Configuration**.
2. Configure the following fields
   - **Service FQDN** and Local FQDN **IP Address**: same IP address
   - **Local FQDN**: `wcs1.mydomain.com`
   - **Public URL Branch**: `equinox.mydomain.com/wcs1`

   Note:

   Repeat the configuration for each WCS that is part of the deployment. The Public URL Branch setting is unique for every additional server.

Related links

OTT deployment — Single IP and single FQDN for HTTP traffic on page 272

Configuring reverse proxy rules on ASBCE for OTT

About this task

This solution can include multiple Web Collaboration servers and the Application server (also called Equinox Management) hiding behind a single external IP and FQDN using port 443 only.

Before you begin

- Generate and upload a matching certificate (named `equinox.mydomain.com`) and create a matching server profile (named `equinox_server`). Generate a certificate from the CA used internally with Subject Alternate Name (SAN) for the internal leg `10.0.0.21`, and create a matching client profile (call it `client`).
- The ASBCE does not support a reverse proxy where the incoming and outgoing traffic goes to the same IP address, so you must create an additional internal IP address (10.0.0.22) to be used by listeners.

Procedure

1. Navigate to **System Management > Device Specific Settings > DMZ Services > Relay Services > Reverse Proxy**.

2. Select **Add** to create the external Reverse Proxy Profile.

   Configure the following parameters:

   - **Name**: enter a descriptive name.
   - **Listen IP**: select the external media interface and the ASBCE external leg IP address (B1, **150.50.0.01**).
   - **Listen Port**: enter `443`.
   - **Listen TLS Profile**: select **equinox_server**.
   - **Connect IP**: select the internal media interface and the internal leg IP address (A1, **10.0.0.21**) .
   - **Server TLS Profile**: select **client**.
   - Enable the **Rewrite URL** checkbox.

3. Select **Add** at the bottom of the page to create an external rewriting rule for the Equinox Management Server component.

   For the Equinox Conference Control and User Portal/Web Gateway, configure the parameters as shown in the figure below. The system appends the parameter in the **URL replace** column to the server address.

   Table 41: Creating external URL rewrite rules for the User Portal/Web Gateway and Equinox Conference Control — Internet to Equinox internal

Server Addresses	Whitelisted URL	URL replace	Note
app.mydomain.com:8444	/acs	/acs	Portal
app.mydomain.com:8444	/ups	/ups	
app.mydomain.com:8444	/csa	/csa	
app.mydomain.com:8444	/uwd/dist	/uwd/dist	
app.mydomain.com:8444	/notification	/notification	
app.mydomain.com:8444	/portal	/portal	
app.mydomain.com:443	/uwd/rest	/uwd/rest	Equinox Conference Control (UCCS)
app.mydomain.com:443	/uwd/ws	/uwd/ws	

4. Select **Add** at the bottom of the page to create an external rewriting rule for WCS1.

   Configure parameters as shown in the table below.

Note:

Make sure to enter trailing slashes (/) in the **Whitelisted URL** and **URL Replace** columns, so the system replaces the Whitelisted URL parameter with the server address.

Repeat the configuration for each WCS that is part of the deployment.

Table 42: Creating an external URL rewrite rule for WCS1 — Internet to Equinox internal

Server Addresses	Whitelisted URL	URL replace	Note
wcs1.mydomain.com:443	/wcs1/	/	Media server
wcs2.mydomain.com:443	/wcs2/	/	
wcs1.mydomain.com:443	/wcs3/	/	

5. Select **Finish** to save the external rules.
6. In the **Reverse Proxy** tab, select **Add** to create the internal Reverse Proxy Profile.

   Configure the following parameters:

   - **Name**: enter a descriptive name.
   - **Listen IP**: select the internal media interface and the ASBCE internal leg IP address (A1, **10.0.0.22**).
   - **Connect IP**: select the internal media interface and select the ASBCE internal leg IP address (A1, **10.0.0.21**).
   - Configure the **Listen Port**, **Listen TLS Profile**, **Server TLS Profile**, and **Rewrite URL** fields, as explained for the external Reverse Proxy Profile above.
7. Select **Add** at the bottom of the page to create an internal rewriting rule for the Equinox Management Server component.

   For the Equinox Conference Control and User Portal/Web Gateway, configure parameters as shown in the table below. The system appends the parameter in the **URL replace** column to the server address.

Table 43: Creating internal URL rewrite rules for the User Portal/Web Gateway and Equinox Conference Control — Private to Equinox internal

Server Addresses	Whitelisted URL	URL replace	Note
app.mydomain.com:443	/acs	/acs	Portal
app.mydomain.com:443	/ups	/ups	
app.mydomain.com:443	/csa	/csa	

Table continues…

Server Addresses	Whitelisted URL	URL replace	Note
app.mydomain.com:443	/uwd/dist	/uwd/dist	
app.mydomain.com:443	/notification	/notification	
app.mydomain.com:443	/portal	/portal	
app.mydomain.com:443	/uwd/rest	/uwd/rest	Equinox Conference Control (UCCS)
app.mydomain.com:443	/uwd/ws	/uwd/ws	

8. Select **Add** at the bottom of the page to create an internal rewriting rule for WCS1.

   Configure parameters as shown in the figure below. In the **URL replace** column, enter a trailing slash (/). The system replaces the whitelisted URL with the server address.

   Repeat the configuration for each WCS that is part of the deployment.

Table 44: Creating an internal URL rewrite rule for WCS — Private to Equinox internal

Server Addresses	Whitelisted URL	URL replace	Note
app.mydomain.com:443	/wcs1/	/	Media server
app.mydomain.com:443	/wcs2/	/	
app.mydomain.com:443	/wcs3/	/	

9. Select **Finish** to save the internal rules.

Related links

OTT deployment — Single IP and single FQDN for HTTP traffic on page 272

Configuring Avaya SBCE on Equinox Management

About this task

Add ASBCE to Equinox Management and then configure TURN/STUN.

In addition to this procedure, you must configure the STUN TURN Server on the Media Server Configuration page for video media servers. For details, see *Configuring the Equinox Media Server from Equinox Management* in *Administrator Guide for Avaya Equinox® Management*.

Important:

ASBCE must be operational once you add it into Equinox Management, so the Media Server and Web Gateway can start the meeting. When ASBCE is operational, it displays a green status LED in the ASBCE list.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Devices** > **Devices by Type** > **ASBCE**, and select **Add**.

   The **Add ASBCE** page appears.
3. Configure these fields as follows:
   - **Name**: enter a name for the ASBCE server.
   - **IP Address**: enter the IP address of the Element Management System (EMS), or any of the ASBCE IP addresses.

     EMS is the ASBCE management interface.
   - **Location**: select the location of the ASBCE server.
4. Select **OK**.

   The ASBCE server displays on the **ASBCEs** page.
5. Select the ASBCE name in the ASBCE list and configure additional settings.

   The **Update ASBCE** page appears.
6. Configure these fields as follows:
   - **Listen/Relay Internal IP**: enter the ASBCE server's internal IP address (A1).
   - **Port**: enter `3478`.
   - **Listen/Relay Public IP**: enter the ASBCE server's public IP address as seen from the public Internet (B1 if public, or firewall NAT public address of B1).
   - **Port**: enter `3478`.
   - **Internal SIP IP**: enter the IP address of the internal interface configured for signaling on ASBCE (A1).
   - **SIP protocol**: select **TLS**.
   - **SIP port**: enter `5061`.
   - **Check status IP**: enter the internal address configured for the load monitoring entry (A1).
   - **Check status protocol**: select **Http** .
   - **HTTP port**: enter `443` .
7. Select **OK**.

Related links

Configuration Checklist for Avaya Equinox® Management in TE on page 332

Configuring Avaya SBCE support of unregistered Avaya SIP endpoints

About this task

See *Administering Avaya Session Border Controller for Enterprise* for detailed information on:

- URI Groups
- Endpoint policy groups
- Server flows
- Subscriber flows

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **Configuration Profiles > URI Groups**. The system displays the URI Groups window.
4. In the Application pane, click **Add**. The system displays the Add URI window.

   Configure the fields as follows:

   - For the URI scheme, enable the **sip:/sips** checkbox for Session Initiation Protocol or Secure Session Initiation Protocol.
   - For the URI type of the URI group, enable the **Plain** checkbox.
   - In the URIs text box, add the URI by using the format selected in the URI Type.
   - Click **Finish**.
5. In the left navigation pane, click **Network & Flows > End Point Flows**. The Application pane lists the registered ASBCE security devices for which the new flow is applied. In the content area, the system displays an ordered list of call flows, Subscriber or Server, for the selected ASBCE security devices.
6. From the application pane, select the ASBCE Device for which you create the new Subscriber End-Point Flow. The system displays the End-Point Flows window showing the flows that are currently defined for that ASBCE device.
7. Click the **Server Flows** tab to add a SIP endpoint to Equinox Management server flow.
8. In the Server Flows window, click **Add**. The system displays the Add Flow window.

   Configure the fields as follows:

   - **Flow Name**: type a meaning name. For example, `sip-endpoints-to-iview`.
   - **SIP Server Profile**: select the server for that flow. For example, Equinox Management (iVIEW).
   - **Received Interface**: select the external SIP signaling interface configured for this ASBCE.

- **Signaling Interface**: select the internal SIP signaling interface configured for this ASBCE.
- **Media Interface**: select the internal media interface configured for this ASBCE.
- **End Point Policy Group**: select the relevant policy group.
- Click **Finish**.

9. On the End Point Flows window, select the **Subscriber Flows** tab.
10. Click **Add** to add a subscriber flow for the internal and external interfaces. The system displays the Add Flow window.

    Configure the fields as follows:

    - **Flow Name** : enter a meaningful name for the flow.
    - **Signaling Interface**: select the internal SIP signaling interface configured for this ASBCE.
    - In the next page, click **Click To Call** in the **Source** field.
    - **Media Interface**: select the external media interface configured for this ASBCE.
    - **End Point Policy Group**: select the policy configured for remote endpoints.
    - **Routing Profile**: select the relevant routing profile.
    - Click **Finish**.

Next steps

If you need BFCP and FECC, configure these features as explained in the ASBCE media interface configuration.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Chapter 12: Avaya Session Border Controller deployment for remote access in Team Engagement solution

Configuration Checklist for Avaya SBCE in TE

The deployment uses Avaya SBCE to connect remote Avaya IX™ Workplace Client (Meet-Me), Avaya Equinox® Meetings for Web client (WebRTC), and Avaya approved SIP endpoints to conferences that take place in the enterprise local network. Avaya SBCE provides three functionalities for that purpose: reverse proxy, session border controller, and STUN/TURN.

You must deploy Avaya SBCE as described in the server documentation. See Capacity and scalability specification on page 252 for important information specific to Equinox Conferencing.

For a full explanation on deploying and configuring Avaya SBCE, download the documentation from the Avaya Support website at http://support.avaya.com or from the Avaya Documentation Portal.

Ensure to perform the procedures listed in the following table. They are required steps in the overall configuration procedure.

No	Task	Link/Notes	✔
1	Create the Certificate Revocation List.	Creating a CRL on Avaya Aura System Manager on page 288	
2	Install the Certificate Revocation List.	Installing the Avaya Aura System Manager CRL on Avaya SBCE on page 289	
3	Use Avaya Aura® System Manager as a Certificate Authority.	Downloading the System Manager CA Root Certificate on page 152	
4	Install the System Manager CA certificate.	Installing the Root CA Certificate on Avaya SBCE on page 290	
5	Create the System Manager end entity profile.	Creating an end entity profile in Avaya Aura System Manager on page 291	

Table continues…

No	Task	Link/Notes	✔
6	Generate the System Manager certificate keystore.	Generating the identity certificate keystore in Avaya Aura System Manager on page 292	
7	Install the System Manager identity certificate.	Installing the Avaya Aura System Manager identity certificate on to encrypt the private key on page 293	
8	Configure the external TLS Server Profile.	Configuring the TLS Server Profile for Avaya SBCE external communication on page 260	
9	Configure the TLS Server Profile for media tunneling.	Configuring TLS Server Profile for Avaya SBCE Media Tunneling on page 261	
10	Configure the TLS Client Profile.	Configuring the TLS Client Profile on Avaya SBCE on page 262	
11	Configure network interfaces.	Configuring Avaya SBCE network interfaces on page 263	
12	Configure signaling interface.	Configuring Avaya SBCE signaling interface on page 264	
13	Configure media interface.	Configuring Avaya SBCE media interface for TE on page 298	
14	Configure load monitoring.	Configuring Avaya SBCE load monitoring for TE on page 300	
15	Configure server flows.	Configuring Avaya SBCE server flows for TE on page 301	
16	Configure reverse proxy rules	Configuring reverse proxy rules on Avaya SBCE for TE on page 306	
17	Configure TURN/STUN for WebRTC calls.	For an introduction to TURN on browser or media server, see TURN/STUN for WebRTC calls in TE on page 309. For configuration of the TURN/STUN profile, see Configuring a browser based TURN/STUN profile for WebRTC calls on page 311	
18	Configure TURN relay for WebRTC calls	Configuring the TURN relay service for WebRTC calls in Avaya SBCE on page 312	
19	Configure support of SIP calls from unregistered endpoints.	Configuring Avaya SBCE support of unregistered Avaya SIP endpoints on page 281	

Related links

Configuring the TLS Server Profile for Avaya SBCE external communication on page 260
Configuring TLS Server Profile for Avaya SBCE Media Tunneling on page 261
Configuring the TLS Client Profile on Avaya SBCE on page 262
Configuring Avaya SBCE network interfaces on page 263
Configuring Avaya SBCE signaling interface on page 264
Configuring Avaya SBCE media interface for TE on page 298

Configuring Avaya SBCE load monitoring for TE on page 300
Configuring Avaya SBCE server flows for TE on page 301
Configuring the reverse proxy policy on Avaya SBCE for TE on page 303
Configuring the reverse proxy profile of Avaya Aura Device Services on Avaya SBCE on page 304
Configuring reverse proxy rules on Avaya SBCE for TE on page 306
TURN/STUN for WebRTC calls in TE on page 309
Configuring Avaya SBCE support of unregistered Avaya SIP endpoints on page 281

Avaya SBCE technical specifications

Capacity and scalability specification

High-capacity servers

Solutions	Server Type					
	Dell™ PowerEdge™ R640 Avaya Solutions Platform 100 series server with profile 5	**Dell R630 server with TILEncore-Gx36 Intelligent Application Adapter**	**HP DL360 G9 server with TILEncore-Gx36 Intelligent Application Adapter**	**Dell™ PowerEdge™ R640 Avaya Solutions Platform 100 series server with profile 3**	**Dell R630 server**	**HP DL360 G9 server**
Remote Worker Users (Sessions)	20,000 (10,000)	20,000 (7,500)	20,000 (7,500)	20,000 (8,000)	20,000 (7,500)	20,000 (7,500)
Avaya Equinox® Conferencing Video Sessions	800	800	800	800	800	800
TURN/STUN Audio-only Sessions	6,000	6,000	6,000	5,000	5,000	5,000
TURN/STUN Audio and Video Sessions	1,000	1,000	1,000	1,000	1,000	1,000
TURN/STUN Tunneling Audio-only Sessions	600	600	600	600	600	600

Table continues…

Solutions	Server Type					
	Dell™ PowerEdge™ R640 Avaya Solutions Platform 100 series server with profile 5	Dell R630 server with TILEncore-Gx36 Intelligent Application Adapter	HP DL360 G9 server with TILEncore-Gx36 Intelligent Application Adapter	Dell™ PowerEdge™ R640 Avaya Solutions Platform 100 series server with profile 3	Dell R630 server	HP DL360 G9 server
TURN/STUN Tunneling Audio and Video Sessions	300	300	300	300	300	300
HTTP Media Audio-only Tunneling Sessions	220	220	220	220	220	220
HTTP Media Audio and Video Tunneling Sessions	110	110	110	110	110	110

Mid-capacity servers

Solutions	Server Type					
	Dell™ PowerEdge™ R340 Avaya Solutions Platform 100 series server	Dell R330 server	HP DL360 G9 server	VMware ESXi 6.x-based server	Avaya Aura® Appliance Virtualization Platform	Nutanix AHV on Nutanix server
Remote Worker Users (Sessions)	5,000 (2,000)	5,000 (2,000)	5,000 (2,000)	6,000 (3,000)	6,000 (3,000)	6,000 (3,000)
Avaya Equinox® Conferencing Video Sessions	200	200	200	200	200	200
TURN/STUN Audio-only Sessions	1,200	1,200	1,200	1,800	1,200	1,200

Table continues…

Solutions	Server Type					
	Dell™ PowerEdge™ R340 Avaya Solutions Platform 100 series server	**Dell R330 server**	**HP DL360 G9 server**	**VMware ESXi 6.x-based server**	**Avaya Aura® Appliance Virtualization Platform**	**Nutanix AHV on Nutanix server**
TURN/STUN Audio and Video Sessions	300	300	300	300	300	300
TURN/STUN Tunneling Audio-only Sessions	220	220	220	220	220 (4 vCPU) 550 (10 vCPU)	220
TURN/STUN Tunneling Audio and Video Sessions	110	110	110	110	110 (4 vCPU) 275 (10 vCPU)	110
HTTP Media Audio-only Tunneling Sessions	220	220	220	220	220 (4 vCPU) 550 (10 vCPU)	220
HTTP Media Audio and Video Tunneling Sessions	110	110	110	110	110 (4 vCPU) 275 (10 vCPU)	110

Additional capacity values for high-capacity and mid-capacity servers

Avaya SBCE supports up to 250 Internet telephony service providers (ITSPs) per system.

Avaya SBCE supports up to 250 tenants per system.

Avaya SBCE supports the following reverse proxy capacities per system:

- 500 HTTP requests per second
- 50 TLS connections per second
- 2,000 concurrent webSockets

General capacity considerations

Each value in the tables represent the maximum capacity supported by Avaya SBCE for that solution and cannot be combined for overall capacity calculations.

The capacity specifications are based on:

- Codec specification: the G729 and G711 codecs are used for measuring transcoded capacities. Different codecs will have varying results.

- Call model: the SIP RFC call model in trunk mode is used to establish these capacity specifications.
- IPv4 vs. IPv6: IPv4 as the transport protocol for calculating non-encrypted sessions with trunking for the Avaya Solutions Platform 100 series server with profile 5 (Dell™ PowerEdge™ R640). With IPv6, the value may decrease by 20%.
- All the audio and video session counts are calculated by assuming Avaya SBCE anchors media. For all other platforms except Portwell CAD-0230 and Portwell CAF-0251, the performance metrics are calculated by testing with the dedicated SBCE device managed by a separate EMS.

Remote Worker capacity considerations

One exception to the standard capacity values is for remote users and Remote Worker call capacity because registration is required for Remote Worker functionality. Mixed usage of the traffic capacities for solutions will vary and must be determined based on these requirements.

While implementing Remote Worker at maximum capacity limits, set registration expiry timers in Session Manager and in every client at a minimum of 3,600 seconds or one hour.

While implementing Remote Worker at maximum capacity limits in one Avaya SBCE or HA pair, under worst-case failover conditions, re-registration for 10,000 users can take up to 20 minutes. During re-registration, all ongoing calls continue uninterrupted. However, under worst-case conditions, a user cannot receive or make new calls during this re-registration time period. Distributing users across multiple Avaya SBCE systems significantly reduces this re-registration time.

VMware ESXi capacity considerations

For VMware ESXi 6.x, it is recommended that capacities are measured with 4 CPU and 8 GB RAM. For more information, see *Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform*.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Certificates

Management of the Avaya Aura System Manager CRL

Creating a CRL on Avaya Aura® System Manager

About this task

You can create a new updated Certificate Revocation List (CRL) to immediately revoke or unrevoke a certificate issued by System Manager as a certificate authority.

See the *Administering Avaya Aura® System Manager* guide for details on CRL management.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.

3. Click **CA Functions** > **CA Structure & CRLs**.
4. Click **Create CRL**. The system creates an updated CRL and displays the time stamp of the updated CRL.
5. Click **Get CRL**. The **Certificate Revocation List** dialog box displays the serial numbers of revoked certificates.

Next steps

[Installing the Avaya Aura System Manager CRL on Avaya SBCE](#) on page 289

Related links

[Configuration Checklist for Avaya SBCE in TE](#) on page 283

Installing the Avaya Aura® System Manager CRL on Avaya SBCE

About this task

The Certificate Revocation List file that you create on System Manager is in the CRL format. The CRL file that you upload to Avaya SBCE must be in the PEM format.

Convert the CRL file to the proper format by using an SSL tool, such as the publicly available OpenSSL tool at: https://www.openssl.org/

Before you begin

Create the CRL.

Procedure

1. Use PSCP or a similar tool, to connect to Avaya SBCE.
2. Copy CRL in the Avaya SBCE home folder.
3. Convert CRL into PEM format by typing `openssl crl -inform der -in filename.crl -out filename.pem`
4. Download the converted file to the administrator server.
5. Log on to the EMS web interface with administrator credentials.
6. In the **Device** drop-down list, click the Avaya SBCE you want to administer.
7. Navigate to **TLS Management** > **Certificates**.
8. Click **Install** and proceed as follows:
   - **Type**: select **Certificate Revocation List**
   - **Name**: type the name of the CRL file.
9. In the **Certificate File** field, click **Browse** and browse to the location of the Certificate File.
10. Click **Upload**.
11. Click **Install**, then **Finish**.

    The **Installed Certificate Revocation Lists** displays the update CRL file.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Management of Root CA Certificate

Downloading Avaya Aura® System Manager Root CA certificate

About this task

You can use Avaya Aura® System Manager as a Root Certificate Authority, and install the CA certificate in Avaya SBCE.

Before installing the CA certificate, download it from System Manager as explained in the following procedure.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **CA Structure & CRLs**.
4. Click **Download PEM file**.
5. Click **Save** to save the certificate to a file.

Next steps

Installing the Root CA Certificate on Avaya SBCE on page 290.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Installing the Root CA Certificate on Avaya SBCE

About this task

You can use Avaya Aura® System Manager as a Certificate Authority, and install the CA certificate on Avaya SBCE.

Before you begin

Download the CA certificate from System Manager.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, click the Avaya SBCE you want to administer.
3. Navigate to **TLS Management** > **Certificates**.
4. Click **Install** and proceed as follows:
   - **Type**: select **CA Certificate**
   - **Name**: type the name of the Certificate file.

- **Allow Weak Certificate/Key**: select the check box to permit usage of a weak private key. This option bypasses the check that requires strong private keys. EMS rejects private keys lesser than 2048 bits or signed with an MD5 based hash by default.
- **Certificate File**: click **Choose file** to browse for the SMGRCA.PEM certificate.

5. Click **Upload**.

   Avaya SBCE issues a warning because the root CA certificate is self-signed. Disregard this warning.

6. Click **Install**, then **Finish**.

   The **Installed CA Certificates** section displays the SMGRCA.PEM certificate.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Management of Identity Certificates

Creating an end entity profile in Avaya Aura® System Manager

About this task

The task is the first procedure required before installing the identity certificate and private key in Avaya SBCE.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. Click **RA Functions** > **Add End Entity**.
4. On the **Add End Entity** page, in **End Entity Profile**, select **INBOUND_OUTBOUND_TLS**.
5. Type the username and password.

   The password is mandatory. You need it to generate the certificate from System Manager.

   Make a note of the password to use it when you install the identity certificate in Avaya SBCE.

6. Enter the relevant information in the fields.
   - **CN**: enter the FQDN of the server that provides TLS support.

     Other fields under **Subject DN Attributes**: complete per customer specific requirements.
   - Under Subject Alternative Name, enter the same FQDN in **DNS name** as above.

     If there is no DNS resolution, use IP addresses of A1 and B1 interfaces in CN and DNS settings.
   - The system automatically selects the following:
     - **ID_CLIENT_SERVER** in **Certificate Profile**.

To verify the contents of the ID_CLIENT_SERVER certificate, click **CA Functions** > **Certificate Profiles** > **Edit**. Ensure that under:

- **Available bit lengths**: **2048 bits** and **4096 bits** are selected.
- **Validity or end date of the certificate**: the setting does not show more than 825 days.
- **Key Usage**: **Digital Signature** and **Key Encipherment** are enabled.
- **Extended Key Usage**: **Server Authentication** and **Client Authentication** are both selected. These settings are required because in some flows Equinox Management is the client and in Avaya SBCE is the server, and vice versa.

- **CA** : select **tmdefaultca**.
- **Token**: select **P 12 file** because the request for certificate and key is generated on System Manager CA.

7. Click **Add**.

   The system displays the message `End Entity added successfully`.

Next steps

Generate the certificate keystore.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Generating the identity certificate keystore in Avaya Aura® System Manager

About this task

The task is the second procedure required before installing the identity certificate and private key in Avaya SBCE.

Before you begin

Create the end entity profile in System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. In the navigation pane, click **Public Web**.
4. On the public **EJBCA** page, click **Enroll** > **Create Keystore**.
5. On the **Keystore Enrollment** page, type the **Username** and **Password** that you entered while creating the end entity on the **Add End Entity** page.
6. Click **OK**.
7. Proceed as follows:
   - **Key length** : select 2048 bits or 4096 bits. Do not use 1024 bits because it is too weak.

- **Certificate Profile**: select `ID_CLIENT_SERVER`.

8. Click **OK**

   The system generates a PKCS12 format keystore with the identity certificate that contains values provided in the end entity.

9. (Optional) View the contents of the P12 file with a tool like X Certificate and Key Management. It is a Windows frontend for the OpenSSL. The P 12 file contains the CA certificate, signed identity certificate, and private key.

Next steps

Install the identity certificate and key in Avaya SBCE.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Installing the Avaya Aura® System Manager identity certificate on to encrypt the private key

Before you begin

Generate keystore file in System Manager.

Procedure

1. Use PSCP, or a similar tool, to connect to Avaya SBCE.
2. Upload the .p12 keystore files to the /home/ipcs/ directory in Avaya SBCE.
3. Extract the certificate from the keystore file by typing `openssl pkcs12 -in filename.p12 -out filename.crt -nokeys -clcerts`.

   Provide the password you used in the **Add end entity** procedure.

4. Extract the key from the keystore file by typing `openssl pkcs12 -in filename.p12 -out filename.key -nocerts`

   To decrypt the key file, provide the password you used in the **Add end entity** procedure.

   To encrypt the private key, you can use the same password.

   This is the password you also provide when you upload the private key to Avaya SBCE.

5. Download .crt and .key files to the administrator server.
6. Log on to the EMS web interface with administrator credentials.
7. In the **Device** drop-down list, click the ASBCE instance you want to administer.
8. Navigate to **TLS Management** > **Certificates**.
9. Click **Install** and proceed as follows:
   - Select **Certificate**.
   - **Name**: type the Certificate name.
   - **Certificate File**: select the ID_CLIENT_SERVER profile.

- **Trust Chain File**: select the SMGRCA.PEM file.
- **Key**: click **Upload Key File**.
- **Key File**: select the key file.
- **Key Passphrase**: provide the password you used to encrypt the private key.

10. Click **Upload**.
11. Click **Install**, then **Finish**.

    The **Installed Certificates** section displays the identity certifcate.
12. Reboot Avaya SBCE:
    a. On the **Device Management** page, click the **Devices** tab.
    b. Click **Reboot** corresponding to the Avaya SBCE device you want to reboot. The EMS server displays a pop-up window to confirm your selection.
    c. Click **OK**. The EMS server displays the notification pop-up window when the reboot of the device is successful.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring the TLS Server Profile for Avaya SBCE external communication

About this task

Avaya SBCE uses a TLS server profile to process an incoming connection over TLS from a remote client.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **TLS Management** > **Server Profiles**.
4. Click **Add**.
5. In the **New Profile** page, configure the fields as follows:
   - **Profile Name**: enter a descriptive name to identify this profile.
   - **Certificate**: select the certificate for external communication.
   - **SNI Options**: set to *None.*
   - **Peer Verification**: select *None*.
   - **Extended Hostname Verification**: leave unchecked.
   - **Renegotiation Time**: set to *0*.

- **Renegotiation Byte Count**: set to *0.*
- **Version** of handshake options: set to **TLS 1.2**.
- **Ciphers**: set to **Default**.

  For information on the fields, see *Administering Avaya Session Border Controller for Enterprise*.

6. Click **Finish**.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring TLS Server Profile for Avaya SBCE Media Tunneling

About this task

A TLS profile allows Avaya SBCE to control parameters when it performs a TLS handshake with a remote entity.

HTTPS media tunneling requires its own TLS server profile. Avaya SBCE supports media tunneling for sign-in and guest users. This configuration is required only for Meet-Me calls that are inbound towards Avaya SBCE.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **TLS Management** > **Server Profiles**.
4. Click **Add**.
5. In the **New Profile** page, configure the fields as follows:
   - **Profile Name**: enter a descriptive name to identify this profile.
   - **Certificate**: select the external certificate used by the TLS Server Profile for external communication.
   - **SNI Options**: set to *None.*
   - **Peer Verification**: select *Optional*.
   - **Peer Certificate Authorities**: leave empty.
   - **Peer Certificate Revocation Lists**: leave empty.
   - **Verification Depth**: select *1*.
   - **Extended Hostname Verification**: leave unchecked.
   - **Renegotiation Time**: set to *0*.
   - **Renegotiation Byte Count**: set to *0.*

- **Version** of handshake options: set to **TLS 1.2**.
- **Ciphers**: set to **Default**.

For information on the fields, see *Administering Avaya Session Border Controller for Enterprise*.

6. Click **Finish**.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring the TLS Client Profile on Avaya SBCE

About this task

A TLS client profile is used when Avaya SBCE starts an outgoing connection towards a remote entity over TLS.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **TLS Management** > **Server Profiles**.
4. Click **Add**.
5. In the **New Profile** page, configure the fields as follows:
   - **Profile Name**: enter a descriptive name.
   - **Certificate**: select the certificate for internal communication.
   - **SNI**: leave unchecked.
   - **Peer Verification**: select *Required*.
   - **Peer Certificate Authorities**: select the System Manager Certificate Authority certificate.
   - **Peer Certificate Revocation Lists**: leave empty.
   - **Verification Depth**: select *1*.
   - **Extended Hostname Verification**: leave unchecked.
   - **Renegotiation Time**: set to *0*.
   - **Renegotiation Byte Count**: set to *0*.
   - **Version** of handshake options: set to **TLS 1.2**.
   - **Ciphers**: set to **Default**.

   For information on the fields, see *Administering Avaya Session Border Controller for Enterprise*.

6. Click **Finish**.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring Avaya SBCE network interfaces

About this task

See the *Administering Avaya Session Border Controller for Enterprise* guide for detailed information on:

- System configuration
- Server and network configuration
- Device configuration
- WebRTC-enabled call processing

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **Network & Flows** > **Network Management > Networks**.
4. In addition to the M1, the management interface that was configured upon ASBCE installation, configure:
   - A1, the internal interface with at least 2 IP addresses associated to it.
   - B1, the external IP addresses with at least 2 IP addresses associated to it.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring Avaya SBCE signaling interface

About this task

See the *Administering Avaya Session Border Controller for Enterprise* guide for detailed information on configuring the signaling interface in the system.

In this procedure, you configure the external and internal signaling interfaces for your deployment.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **Network & Flows** > **Signaling Interface** and select **Add**.

4. Configure the external signaling interface.
   - **Name**: enter the name for the external signaling interface (B1).
   - **IP Address**: the network name, identified by the interface name and VLAN tag, and IP address of the ASBCE used by SIP signaling messages traversing the network.
   - **TCP Port**: leave the field blank.
   - **UDP Port**: leave the field blank for a non-tunneled mode.
   - **TLS Port**: enter `5061`.
   - **TLS Profile**: select the previously configured TLS profile.
   - **Enable Shared Control**: do not select the checkbox
   - **Shared Control Port**: leave empty
5. Configure the internal signaling interface:
   - **Name**: enter the name for the internal signaling interface (A1).
   - **IP Address**: the network name, identified by the interface name and VLAN tag, and IP address of the ASBCE used by SIP signaling messages traversing the network.
   - **TCP Port**: leave the field blank.
   - **UDP Port**: leave the field blank for a non-tunneled mode.
   - **TLS Port**: enter `5061`.
   - **TLS Profile**: select the previously configured TLS profile.
   - **Enable Shared Control**: do not select the checkbox
   - **Shared Control Port**: leave empty

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring Avaya SBCE media interface for TE

About this task

This configuration is required for Avaya IX™ Workplace Client in Meet-Me mode and Avaya Equinox® Meetings for Web (WebRTC) Client that join the meeting from the public/external network.

- Media tunneling
- Media interface

The following settings are needed for unregistered SIP calls from Avaya Room System XT Series, CU360 and 3rd party SIP endpoints dial-in and dial-out, and for Avaya IX™ Workplace Client (both for SIPUA and HTTPUA flows):

- Video media

- Media encryption
- End point policy groups

See the *Administering Avaya Session Border Controller for Enterprise* guide for detailed information on:

Before you begin

Verify ASBCE has a self-signed certificate or CA certificate installed.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. To configure media tunneling, navigate to **Network & Flows** > **Advanced Options** > **Feature Control**.
   - Select **Media Tunneling**.
   - Select **Save**.
4. To configure the external media interface, navigate to **Network & Flows** > **Media Interface** and select **Add** or clone an existing media rule (recommended).

   Configure these fields.
   - **Name**: enter media interface name. For example, *MedTurnExt*
   - **IP Address**: select B1 IP address, taking the following into account:
     - Do not use this IP address for any other interface bound to port 443 (HTTP tunneling configuration).
     - Do not use VLAN tag for media tunneled interface.
   - **Port Range**: for example, *35000–40000*
   - **TLS Profle**: select a TLS server profile for the media interface, if media tunneling is enabled. For self-signed certificates on the client, use the TLS server profile created for the external media interface.
   - **Buffer Size**: select the buffer size from the list containing values from 400 to 1000 in KB. For example, *500*
   - Click **Finish**.
5. To configure the internal media interface, navigate to **Network & Flows** > **Media Interface** and select **Add** or clone an existing media rule (recommended).
   - **Name**: enter media interface name. For example, *MedTurnInt*
   - **IP Address**: select the A1 IP address that is not matched with the IP address used to redirect requests to AAWG in the Reverse Proxy settings.
   - **Port Range**: for example, *35000–40000*

- **TLS Profle**: select a TLS server profile for the media interface, if media tunneling is enabled. For self-signed certificates on the client, use the TLS server profile created for the internal media interface.
- **Buffer Size**: select the buffer size from the list containing values from 400 to 1000 in KB. For example, *500*
- Click **Finish**.

6. To enable video media, navigate to **Domain Policies > Application Rules** page, and clone an existing application rule or add a new one.

   Configure these fields:

   - Enable **In/Out Audio/Video** application types.
   - Configure **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint**

7. (Not for media tunneling) To configure media encryption and enable BFCP and/or FECC, navigate to **Domain Policies** > **Media Rules** and clone an existing media rule or add a new one.

   Configure these fields:

   - On the **Encryption** tab, in the **Miscellaneous** section, select the **Capability Negotiation** checkbox.
   - On the **Advanced** tab, select the **BFCP Enabled** and **FECC Enabled** checkboxes.

8. To configure the policy group with the newly created application and media rules, navigate to **Domain Policies** > **End Point Policy Groups** and clone an existing policy group or add a new one.
9. You must disable interworking when using HTTP tunneling. To disable interworking, navigate to **Domain Policies** > **Media Rules** > **Encryption** and uncheck the **Interworking** checkbox.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring Avaya SBCE load monitoring for TE

About this task

Refer to the *Administering Avaya Session Border Controller for Enterprise* guide for detailed information on load monitoring.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **Network & Flows** > **Load Monitoring** > **Advanced Options**.

4. Select **Add** to create the load balancer profile.
5. Configure these fields as follows:
   - **Load Balancer Type**: select **INTERNAL**.
   - **Transport**: select the Load Balancer protocol.
   - **Listen IP**: select the internal interface (A1). It can be a separate IP address or match the IP address used for signaling to AAWG.
   - **Service Type**: select **TURN**.
6. Select **Finish**.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring Avaya SBCE server flows for TE

About this task

See the *Administering Avaya Session Border Controller for Enterprise* guide for detailed information on server flows.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. To create an Interworking Profile, navigate to **Configuration Profiles > Server Interworking** and select **Add** for a new profile.

   Configure these fields as follows:

   - For a new profile, set all options as default.
   - In **Advanced Options** > **Has Remote SBC**: select **No** (disabled).
   - Ensure to select the right profile in the **Extensions** field.

     The setting directs the ASBCE security device to use functionality specific to different environments.
4. To add a server profile for Equinox Management, navigate to **Services** > **SIP Servers** > **General** and select **Add**.

   Configure these fields as follows:

   - Enter a **Profile Name**.
   - **Server Type**: select **Trunk Server**.
   - **SIP domain**: you can leave it blank.
   - **DNS Query Type**: select *NONE/A*

- **TLS Client Profile**: select the previously created client profile when TLS port is specified.
- Add the Equinox Management FQDN with port 5061 and TLS protocol specified.
- On **Advanced Options**, select the **Enable Grooming** checkbox and select the previously created Interworking Profile.
- Select the **Interworking Profile**.
- You can leave other settings with their default values.

5. To add a server profile for the AAWG server, navigate to **Services** > **SIP Servers** and select **Add**.

   Configure these fields as follows:

   - Enter a **Profile Name**.
   - **Server Type**: select **Trunk Server**.
   - **SIP domain**: you can leave it blank.
   - **DNS Query Type**: select *NONE/A*.
   - **TLS Client Profile**: select the previously created client profile when TLS port is specified. For example, *InternalClient*
   - Add the AAWG FQDN with port `5061` and TLS protocol. Add all AAWG nodes.
   - On **Advanced Options**, select the **Enable Grooming** checkbox and select the previously created Interworking Profile.
   - Select the **Interworking Profile**.
   - You can leave other settings with their default values.

6. To add a flow for an AAWG server, navigate to **Network & Flows** > **End Point Flows** > **> Server Flows** and select **Add**.

   Configure these fields as follows:

   - **Flow Name**: enter a name such as `AAWGFlow`.
   - **SIP Server Profile**: select the configuration you previously created for AAWG.
   - **Received Interface**: select the signaling interface (A1).
   - **Signaling Interface**: select the signaling interface (A1).
   - **Media Interface**: select the external interface (B1).
   - Select the **Endpoint Policy Group** as required.
   - You can leave other settings with their default values.

7. To add a flow for Equinox Management, navigate to **Network & Flows** > **End Point Flows** > **> Server Flows** and select **Add**.

Configure these fields as follows:

- **Flow Name**: enter a name such as `EqMngFlow`.
- **SIP Server Profile**: select the configuration you previously created for Equinox Management.
- **Received Interface**: select the signaling interface (A1).
- **Signaling Interface**: select the signaling interface (A1).
- **Media Interface**: select the media interface (A1).
- Select the **Endpoint Policy Group** as required.
- You can leave other settings with their default values.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring the reverse proxy policy on Avaya SBCE for TE

About this task

Remote clients and endpoints that need to participate in conferences have to interact with multiple components through HTTPS. Each component has its own IP address and FQDN. The ASBCE URL rewriting method solves this interfacing complexity by allowing guests to access a conference via a single FQDN and a single IP address, using port 443. As each FQDN needs a certificate, and there is only one FQDN to interact with, this method also allows saving on the costs of commercial certificates. You can use URL rewriting in all Equinox deployments.

This procedure is part of the reverse proxy configuration process.

For more information, see *Administering Avaya Session Border Controller for Enterprise*.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, navigate to **Configuration Profiles** > **Relay** > **Reverse Proxy Policy**.
4. Click **Add** or **Clone** a rule.
5. In the **Rule Name** field, enter a descriptive Reverse Proxy Profile name. For example, *ws* to indicate a Web Service.
6. Configure the following fields:
   - **Allow Web Socket**: *Y*. The web connection enables a bi-directional communication between the client browser and the remote Web Collaboration Server.
   - **Request Max body Size**: *32 MB*. The field indicates the maximum size of the client request body.

- **Client Body Timeout**: *60 seconds*. The field indicates the timeout for reading the client request body.
- **Client Header Timeout**: *60 seconds*. The field indicates the timeout for reading the client request header.
- **DNS Resolver Timeout**: *3 seconds*. The field indicates the timeout for resolving domain name of server address.
- **TLS/SSL Session Timeout**: *300 seconds*. The field indicates the time for which the client can reuse the SSL session parameters.
- **Server Read Timeout**: *60 seconds*. The field indicates the maximum time for which reverse proxy waits to read data from the server before marking it as unavailable.

7. Click **Finish.**

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring the reverse proxy profile of Avaya Aura® Device Services on Avaya SBCE

About this task

You can use Avaya SBCE for relaying HTTP and HTTPS traffic between Avaya Aura® Device Services enabled application clients (such as Avaya IX™ Workplace Client) and Avaya Aura® Device Services.

For more information about relay configuration in Avaya SBCE, see *Administering Avaya Session Border Controller for Enterprise*.

Before you begin

- Because the reverse proxy or relay is configured to listen on port 443, set the **Override port for reverse proxy** setting from the **Front-end host, System Manager and Certificate Configuration** menu to **y** (yes). You must also set a value for the **Front-end port for reverse proxy** parameter.
- Configure the reverse proxy with the Listen IP towards the enterprise and Connect IP to the network outside the enterprise.

Note:

To use the remote worker functionality, you must configure one of the following:

- Implement Split-Horizon DNS. Avaya recommends the use of this configuration. This configuration optimizes traffic so that clients connect to Session Manager directly on the internal network and only use Avaya SBCE when external.
- Use Public cloud model. All FQDNs or URLs must point to the reverse proxy or Avaya SBCE. This configuration is used for cloud deployments and also for on premise deployments. By using this configuration, calls are preserved during any network

transition from Wi-Fi to cellular data when the client IP address can change during an active call.

- Internal access only and all remote devices must use VPN. This configuration is used when a security policy is in place such that all traffic must be either internal or via VPN. The VPN solution that is deployed must have sufficient bandwidth and latency to support the expected volume of VoIP calls.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **DMZ Services > Relay > Reverse Proxy**.
4. In the **Reverse Proxy** tab, click **Add**.
5. On the **Profile** page, configure the fields as follows:
   - **Service Name** : type AADS as the reverse proxy profile name. Select the **Enabled** check box.
   - **Listen IP** : click the external Avaya SBCE IP address.
   - **Listen Port** : type `443`.
   - **Listen Protocol** : select the protocol published towards remote workers.

     When you select the HTTPS protocol, the system enables the **Listen TLS Profile** field.
   - **Listen TLS Profile** : click the TLS profile you created. The default TLS profiles, like `ExternalServer`, have demonstration certificates. For optimum security, Avaya recommends that you do not use demonstration certificates.
   - **Connect IP**: click the internal IP address that Avaya SBCE must use for communicating with the file servers.
   - **Server Protocol**: select **HTTPS**.
   - **Server TLS Profile**: click the TLS profile that you created, like `InternalClient`.
   - Do not select **Rewrite URL**.
   - **Reverse Proxy Policy Profile**: click the required profile. For example: *ws*
   - **Whitelisted IPs**: leave empty.
   - Select **Add** and configure the field as follows:
     - In the **Server Addresses** field, type the Avaya Aura® Device Services FQDN and port 443.

       This field accepts an IP address or FQDN and port. Preferably, specify the FQDN and port in the Server Addresses field. This field must match the **Subject Alt Name** defined in the Avaya Aura® Device Services server certificate.
     - **Received Server Host**: displays a grayed out *Any*.

- **Whitelisted URL**: displays a grayed out slash sign (*/*).
- **URL Replace**: displays an empty grayed out field.

6. Click **Finish**.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuring reverse proxy rules on Avaya SBCE for TE

About this task

Remote clients and endpoints that need to participate in conferences have to interact with multiple components through HTTPS. Each component has its own IP address and FQDN. The ASBCE URL rewriting method solves this interfacing complexity by allowing guests to access a conference via a single FQDN and a single IP address, using port 443. As each FQDN needs a certificate, and there is only one FQDN to interact with, this method also allows saving on the costs of commercial certificates. You can use URL rewriting in all Equinox deployments.

Follow the procedure to configure the ASBCE URL rewriting rules.

Before you begin

- Generate and upload a matching certificate (name is ASBCE FQDN) and create a matching server profile (name it `<name>server`). Generate a certificate from the CA used internally with Subject Alternate Name (SAN) for the internal leg (per IP address), and create a matching client profile (name it `<name>client`).
- The ASBCE does not support a reverse proxy where the incoming and outgoing traffic goes to the same IP address, so you must create an additional internal IP address on A1 to be used by listeners.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, navigate to **DMZ Services** > **Relay** > **Reverse Proxy**.
4. Select **Add** to create the external Reverse Proxy Profile.

   Configure the following parameters:

   - **Service Name**: enter a descriptive name. For example, *Conferencing*.
   - Select the **Enabled** checkbox.
   - **Listen IP**: select the external media interface (B1) and the ASBCE external leg IP address.
   - **Listen Port**: enter *443*.
   - **Listen Protocol**: *HTTPS*
   - **Listen TLS Profile**: select the relevant TLS Server Profile. For example, a profile named *ExternalServer*.

- **Connect IP**: select the internal media interface and the internal leg IP address (A1).
- **Server TLS Profile**: select the relevant TLS Client Profile. For example, a profile named *InternalClient*.
- Enable the **Rewrite URL** checkbox.
- **PPM Mapping Profile**: select *None*
- **Reverse Proxy Policy Profile**: click the required profile. For example: *ws*
- **Whitelisted IPs**: leave the field empty.

5. Select **Add** at the bottom of the page to create an external rewriting rule for these devices: Portal (AAWG), Equinox Conference Control (UCCS), Equinox Management, Media Server.

   Configure parameters as shown in the table below. Each service uses a different path in its URL. All URLs have the same format: `<FQDN>/service prefix>/<unique URL>`. The system appends the parameter in the **URL replace** column to the server address.

Table 45: Creating external URL rewrite rules

Server Address Example	Whitelisted URL	URL Replace	Comment
rtsawg1.xxxx:8444	/portal	/portal	Portal (Avaya Aura® Web Gateway)
rtsawg1.xxxx:8444	/notification	/notification	
rtsawg1.xxxx:8444	/uwd/dist	/uwd/dist	
rtsawg1.xxxx:8444	/ups	/ups	
rtsawg1.xxxx:8444	/csa	/csa	
rtsawg1.xxxx:8444	/acs	/acs	
rtsemgr1.xxxx:443	/uwd/rest	/uwd/rest	Equinox Conference Control (also called UCCS, part of the Equinox Management Server)
rtsemgr1.xxxx:443	/uwd/ws	/uwd/ws	
rtsems1.xxxx:443	/wcsws	/wcsws	Web Collaboration Server (WCS). WCS is a standalone server if it provides web collaboration for a legacy Scopia® Elite 6000 MCUor it is part of the Equinox Media Server (audio or video).
rtsems1.xxxx:443	/viewer	/viewer	

   If your deployment includes multiple Media Servers, enter the following in the URL rewrite table:

Table 46: Example of URL rewrite configuration for multiple media servers

Server Address Example	Whitelisted URL Example	URL Replace	Note
rtsems1.xxxx.com:443	/ems1/	/	Make sure to enter trailing slashes (/) so the system replaces the Whitelisted URL parameter with the server address.
rtsems2.xxxx.com:443	/ems2/	/	
rtsems3.xxxx.com:443	/ems3/	/	

6. Select **Finish** to save each external rule.
7. In the **Reverse Proxy** tab, select **Add** to create the internal Reverse Proxy Profile.

   Configure the following parameters:

   - **Service Name**: enter a descriptive name.
   - Select the **Enabled** checkbox.
   - **Listen IP**: select the internal media interface and the ASBCE internal leg IP address (A1).
   - **Connect IP**: select the internal media interface and select the ASBCE internal leg IP address (A1).
   - **Server TLS Profile**: select the relevant client name.
   - Configure the **Listen Port**, **Listen TLS Profile**, **Rewrite URL** and **Reverse Proxy Policy Profile**as explained for the external Reverse Proxy Profile above.
8. Select **Add** at the bottom of the page to create an internal rewriting rule for these devices: Portal (AAWG), Equinox Conference Control (UCCS), Equinox Management, Media Server.

   Configure parameters as shown in the table below. The system appends the parameter in the **URL replace** column to the server address.

   Note:

   Make sure to add the `/slider` parameter to get the slider functionality working in Avaya Equinox® Conferencing.

Table 47: Creating internal URL rewrite rules

Server Address Example	Whitelisted URL	URL Replace	Comment
rtsawg1.xxxx:443	/portal	/portal	Portal (AAWG)
rtsawg1.xxxx:443	/notification	/notification	
rtsawg1.xxxx:443	/uwd/dist	/uwd/dist	
rtsawg1.xxxx:443	/ups	/ups	
rtsawg1.xxxx:443	/csa	/csa	

Table continues…

Server Address Example	Whitelisted URL	URL Replace	Comment
rtsawg1.xxxx:443	/acs	/acs	
rtsemgr1.xxxx:443	/uwd/rest	/uwd/rest	Equinox Conference Control (UCCS)
rtsemgr1.xxxx:443	/uwd/ws	/uwd/ws	
rtsems1.xxxx:443	/wcsws	/wcsws	Web Collaboration Server (WCS)
rtsems1.xxxx:443	/viewer	/viewer	
rtsems1.xxxx:443	/slider	/slider	

If your deployment includes multiple WCS, enter the following in the URL rewrite table:

Table 48: Example of URL rewrite configuration for multiple WCS

Server Address Example	Whitelisted URL Example	URL Replace	Comment
rtsems1.xxxx:443	/ems1/	/	Make sure to enter trailing slashes (/) so the system replaces the Whitelisted URL parameter with the server address.
rtsems2.xxxx:443	/ems2/	/	
rtsems3.xxxx:443	/ems3/	/	

9. Select **Finish** to save each internal rule.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

TURN/STUN for WebRTC calls in TE

Up to Avaya SBCE release 7.2.1, Avaya based its WebRTC solution on a TURN client residing on the Media Server inside the enterprise. This solution forced traffic to go through inside the enterprise using the WebRTC Media Server (MCU or AMS) as the anchor point in a WebRTC call. This solution had some deficiencies, specifically in certain topologies where the browser was behind a corporate firewall that blocked all UDP traffic sent to an enterprise WebRTC Media Server.

For release 7.2.2 and up, Avaya has solved the issue by moving the TURN client to the browser.

Note:

The administrator can use both solutions, but not in the same deployment.

The following figure illustrates the WebRTC call flow with a browser based TURN client.

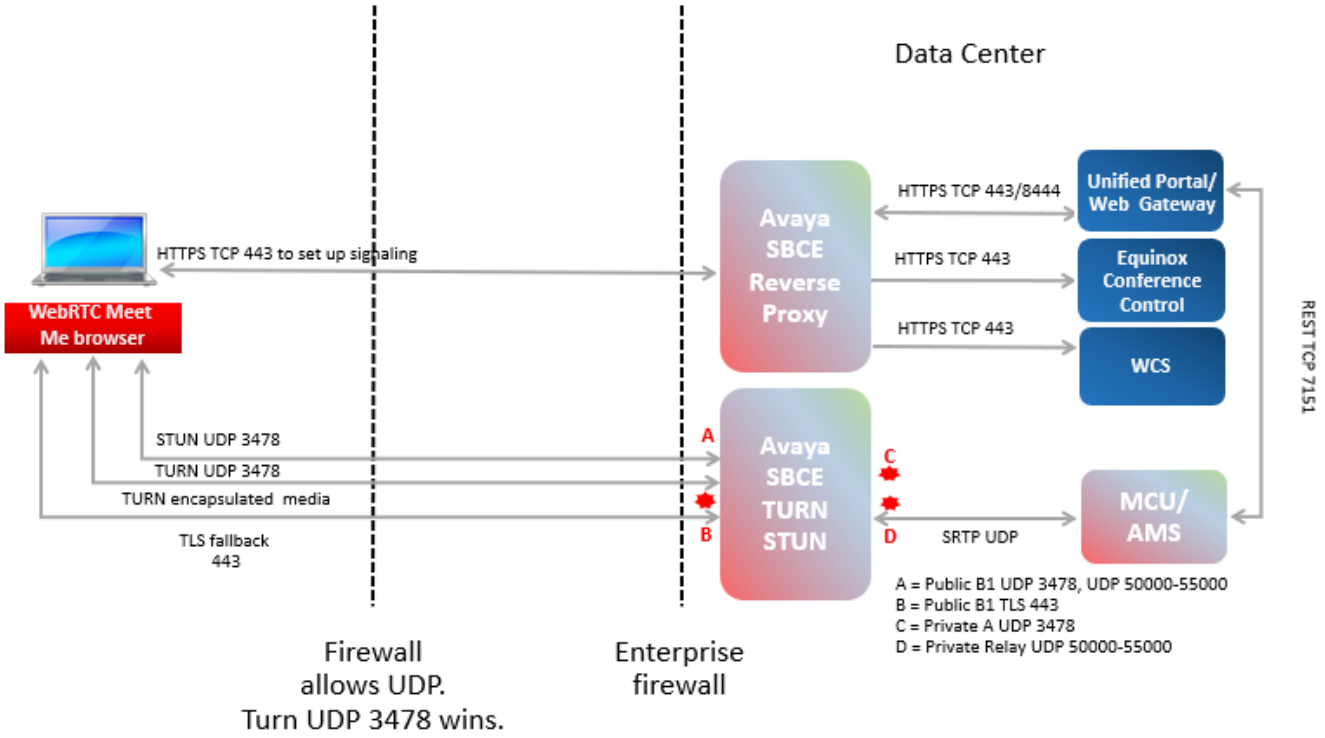


Figure 99: TURN Client on browser

For information on the component architecture, see Component architecture on page 18.

From the browser, the user launches the soft client. It tries to access the conference server running in the data center at the far end.

Call signaling uses the HTTPS channel, and goes through the Avaya SBCE reverse proxy to Equinox Conference Control.

One HTTP channel goes to the portal, and the configuration data comes in from the portal back to the browser. The configuration data includes the TURN server settings.

To present content, start/stop the presentation and share the screen on a device, the setup requires an HTTP channel with Web Collaboration Server (WCS).

Then, the browser initiates a call setup to Equinox Conference Control through reverse proxy.

The TURN and STUN server gathers the ICE candidates and handles media packet traversal through firewalls.

The REST control port is needed between the Web Gateway and the WebRTC Gateway.

If corporate firewalls block UDP, the TURN client on browser can use port TLS/443 to tunnel TURN messages through the firewall that blocks UDP. TURN on TLS encapsulates the media packets that the TURN Server on Avaya SBCE decodes at the enterprise edge.

Avaya SBCE is not aware of the far end topology. For that reason, the administrator must configure Avaya SBCE to accept STUN on UDP, TURN on UDP, and TURN on TLS. Depending on the TURN packets flowing through Avaya SBCE, it keeps one TURN relay open for the TURN

encapsulated RTP flow, and closes the other TURN relay through which no TURN encapsulated packet flows.

The TURN service authorization and authentication comply with RFC 7635.

Table 49: Client traffic through Avaya SBCE in a TE deployment

Traffic type through ASBCE	Avaya Equinox® Meetings for Web for remote user, guest or sign-in (WebRTC)	Avaya IX™ Workplace Client for remote guest user (HTTP)	Avaya IX™ Workplace Client for remote TE user (SIP)
STUN	If user is not behind a restricted firewall	N/A	N/A
TURN	If user is behind a restricted firewall	N/A	N/A
SRTP over UDP	N/A	If user is not behind a restricted firewall	If user is not behind a restricted firewall
HTTP Tunneling (SRTP over TLS)	N/A	If user is behind a restricted firewall	Not supported

Related links

Configuration Checklist for Avaya SBCE in TE on page 283
Configuring a browser based TURN/STUN profile for WebRTC calls on page 311
Configuring the TURN relay service for WebRTC calls in Avaya SBCE on page 312

Configuring a browser based TURN/STUN profile for WebRTC calls

About this task

You need to create an Avaya SBCE TURN/STUN profile that the TURN client uses to access Equinox Conferencing.

Certain topologies do not allow UDP through firewalls, and require TURN on TLS instead. Therefore, you can configure Avaya SBCE to accept both TURN on UDP and TURN on TLS simultaneously. Then, Avaya SBCE keeps open only the relay through which DTLS/SRTP flows.

Avaya SBCE release 7.2.2 and above supports multiple TURN/STUN profiles.

Procedure

1. Log in to the EMS web interface with the administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **DMZ Service** > **TURN/STUN** > **TURN/STUN Profiles**.
4. Click **Add** to create a new TURN profile.

Important:

If you edit the existing TURN/STUN profile that you associated with TURN Relay IP mappings, you must delete the existing TURN Relay IP mappings and add them again.

5. Configure the fields as follows.
   - **Profile Name**: enter the name of the TURN/STUN profile.
   - **UDP Listen Port**: enter *3478*.
   - **TCP/TLS Listen Port**: enter *443*.
   - **TLS Server Profile**: enter TLS server profile used for the TCP/TLS listen port. Select the TLS profile that you created for TURN.
   - **Media Relay Port Range**: If you use a different port range than the default *50000 — 55000*, verify there is no conflict with port ranges that Avaya SBCE uses for other protocols like SIP.
   - **Authentication**: enable authentication for the TURN/STUN profile.
   - **Client Authentication**: enable token based authentication for the client when the browser is enabled with TURN.
   - **Nonce Expiry**: timer indicating how long the authentication service functions during a call.
   - **UDP Relay**: enable the checkbox.
   - **Media Learning**: ensure to clear the **Media Learning** check box for TURN/STUN profile deployment on browser.
6. Leave the remaining optional fields with their default values. For information on the optional fields, see *Administering Avaya Session Border Controller for Enterprise*.
7. Click **Finish** to save and exit.

Next steps

Configuring the TURN relay service for WebRTC calls in Avaya SBCE on page 312

Related links

TURN/STUN for WebRTC calls in TE on page 309

Configuring the TURN relay service for WebRTC calls in Avaya SBCE

About this task

You need to create an Avaya SBCE TURN relay service for a TURN/STUN profile deployed on a browser. Each TURN/STUN relay corresponds to a TURN Listen IP address and TURN Media Relay IP Address and must have a TURN/STUN profile associated with it.

Avaya SBCE release 7.2.2 and above supports multiple TURN/STUN relays.

Before you begin

Create a TURN/STUN profile. See Configuring a browser based TURN/STUN profile for WebRTC calls on page 311.

Procedure

1. Log in to the EMS web interface with the administrator credentials.

2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **DMZ Services** > **> TURN Relay**.
4. Click **Add** to create a new TURN relay service.
5. In the **Add TURN STUN IP Pairing** page, configure fields as follows:
   - **Listen IP**: the Listen IP address of TURN server. Enter the browser facing IP address.
   - **Media Relay IP**: the Media Relay IP of TURN server. Enter the MCU/AMS facing IP address.
   - **Service FQDN**: the TURN server listen FQDN. The Service FQDN resolves to the TURN **Listen IP** address.

   Important:

   If you edit the existing TURN/STUN profile that you associated with TURN Relay IP mappings, you must delete the existing TURN Relay IP mappings and add them again.
6. Click **Finish** to save and exit.

Related links

TURN/STUN for WebRTC calls in TE on page 309

Configuring Avaya SBCE support of unregistered Avaya SIP endpoints

About this task

See *Administering Avaya Session Border Controller for Enterprise* for detailed information on:

- URI Groups
- Endpoint policy groups
- Server flows
- Subscriber flows

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** dropdown list, select the ASBCE.
3. In the left navigation pane, click **Configuration Profiles > URI Groups**. The system displays the URI Groups window.
4. In the Application pane, click **Add**. The system displays the Add URI window.

   Configure the fields as follows:

   - For the URI scheme, enable the **sip:/sips** checkbox for Session Initiation Protocol or Secure Session Initiation Protocol.

- For the URI type of the URI group, enable the **Plain** checkbox.
- In the URIs text box, add the URI by using the format selected in the URI Type.
- Click **Finish**.

5. In the left navigation pane, click **Network & Flows > End Point Flows**. The Application pane lists the registered ASBCE security devices for which the new flow is applied. In the content area, the system displays an ordered list of call flows, Subscriber or Server, for the selected ASBCE security devices.
6. From the application pane, select the ASBCE Device for which you create the new Subscriber End-Point Flow. The system displays the End-Point Flows window showing the flows that are currently defined for that ASBCE device.
7. Click the **Server Flows** tab to add a SIP endpoint to Equinox Management server flow.
8. In the Server Flows window, click **Add**. The system displays the Add Flow window.

   Configure the fields as follows:

   - **Flow Name**: type a meaning name. For example, `sip-endpoints-to-iview`.
   - **SIP Server Profile**: select the server for that flow. For example, Equinox Management (iVIEW).
   - **Received Interface**: select the external SIP signaling interface configured for this ASBCE.
   - **Signaling Interface**: select the internal SIP signaling interface configured for this ASBCE.
   - **Media Interface**: select the internal media interface configured for this ASBCE.
   - **End Point Policy Group**: select the relevant policy group.
   - Click **Finish**.
9. On the End Point Flows window, select the **Subscriber Flows** tab.
10. Click **Add** to add a subscriber flow for the internal and external interfaces. The system displays the Add Flow window.

    Configure the fields as follows:

    - **Flow Name** : enter a meaningful name for the flow.
    - **Signaling Interface**: select the internal SIP signaling interface configured for this ASBCE.
    - In the next page, click **Click To Call** in the **Source** field.
    - **Media Interface**: select the external media interface configured for this ASBCE.
    - **End Point Policy Group**: select the policy configured for remote endpoints.
    - **Routing Profile**: select the relevant routing profile.
    - Click **Finish**.

Next steps

If you need BFCP and FECC, configure these features as explained in the ASBCE media interface configuration.

Related links

Configuration Checklist for Avaya SBCE in TE on page 283

Configuration Checklist for Avaya Aura® Device Services

Avaya Aura® Device Services provides a single place in the Aura architecture where clients and endpoints can store and retrieve data that users want to see on any device, supporting a common user experience. In addition, it is a common place for configuration and deployment data.

Avaya Aura® Device Services also provides a set of services to Avaya IX™ Workplace Client release 3.0 and up.

For a full explanation on deploying and configuring Avaya Aura® Device Services, download the documentation from the Avaya Support website at http://support.avaya.com or from the Avaya Documentation Portal.

Ensure to perform the procedures listed in the following table. They are required steps in the overall configuration procedure. For details on these procedures, see *Administering Avaya Aura® Device Services*. If the procedure is in another document, the configuration checklist refers to the document.

Use these procedures with Avaya Aura® Device Services release 8.0.x and above.

No.	Task	Link/Notes	✔
1	Configure resource sharing (CORS).	Enable CORS to ensure there is no communication issues among the different servers in the deployment. On the Avaya Aura® Device Services web administration portal, click **Server Connections** > **CORS Configuration** > **Service Interface** Ensure to select: • **Enable Cross-Origin Resource Sharing** • **Allow access from any origin**	
2	Configure Avaya Aura® Device Services Front-end host, Avaya Aura® System Manager, and use of System Manager for certificate management.	Use the Command Line Interface (CLI) utility to configure the settings. See Configuring the Front-end host of Avaya Aura Web Gateway, System Manager, and Certificate on page 327.	

Table continues…

No.	Task	Link/Notes	✔
3	Configure service control.	To start Avaya Aura® Device Services, log in to the web administration portal. On the **Service Control** page, select **Device Services** and click **Start**. In **Application Properties**, manage application sessions: • Set a timeout period for terminating inactive, idle, or unattended sessions. • Manage concurrent HTTP sessions.	
4	Configure the Client-device Certificate Policy.	On the Avaya Aura® Device Services web administration portal, click **Client Administration** > **HTTP Clients**. Ensure to configure **REST** to **NONE**, and **OAMP** to **OPTIONAL**.	
5	Configure trusted hosts.	On the Avaya Aura® Device Services web administration portal, click **Server Connections** > **Trusted Hosts**. Ensure to enter: • Avaya Aura® Web Gateway FQDN • Avaya Equinox® Management FQDN If there are multiple Avaya Aura® Web Gateway servers, you have to add each and every server.	
6	Synchronize Avaya Aura® Device Services and Equinox Management.	On the Avaya Aura® Device Services web administration portal, click **Server Connections** > **iVIEW Synchronization**. For the detailed procedure, see *Deploying Avaya Aura® Device Services* Ensure to enter: • **Version number**: Equinox Management released version number. • **IP address**: Equinox Management IP. **Connection status** shows **CONNECTED** and a green status icon.	
7	Generate identity certificates.	If you must change the Front-end FQDN, use CLI to regenerate the certificates. After the certificate validity expires, you can regenerate the certificates from the SMGR Certificates page. You need the enrollment password to get the new certificates from System Manager. On the Avaya Aura® Device Services administration portal, click **Security Settings** > **Certificate Management** > **SMGR Certificates**.	

Table continues…

No.	Task	Link/Notes	✔
8	Manage the following identity certificate tasks: • CSRs • Keystore data • Server interfaces.	This procedure allows to double-check the certificates System Manager automatically generated after you implemented procedure 2 in this table. On the Avaya Aura® Device Services web administration portal, click **Security Settings** > **Certificate Management** > **Identity Certificates** Ensure System Manager has assigned a certificate to each server interface: • Application • Internal • OAM	
9	View the details of each server interface certificate.	This procedure allows to double-check the certificates System Manager automatically generated after you implemented procedure 2 in this table. On the Avaya Aura® Device Services administration portal, click **Security Settings** > **Certificate Management** > **Identity Certificates** > **Server Interfaces** > **Application** > **Details**.	

Related links

Configuring the Front-end host, System Manager, and Certificate on Avaya Aura Device Services on page 317

Configuring the Front-end host, System Manager, and Certificate on Avaya Aura® Device Services

About this task

You can perform these configurations from the Avaya Aura® Device Services administration portal or from the Command Line Interface (CLI).

The following procedure describes the configuration from the CLI utility. The CLI utility provides a complete picture of the fields you need to configure. Once you complete the configuration, Avaya Aura® Device Services automatically configures reverse proxy, generates certificates and restarts the system.

Use CLI for further changes.

If you use the administration portal for these configurations, you must restart the system manually and regenerate certificates.

Procedure

1. Log in to the Linux shell on the initial node by using the Linux administrator account credentials.

2. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
3. Select **Front-end host, System Manager and Certificate Configuration**.
4. Configure the following settings in the fields.

Field	Description
Front-end FQDN	Reverse Proxy FQDN of Avaya Aura® Device Services.
System Manager FQDN	The FQDN of the Avaya Aura® System Manager that signs the certificates.
System Manager HTTPS Port	Ensure to configure to *443*.
System Manager Enrollment Password	The Avaya Aura® System Manager enrollment password. **Note:** To get the password, log in to System Manager and navigate to **Service** > **Security** > **Certificates** > **Enrollment Password**.
Override port for reverse proxy	Ensure to configure to *n* (disabled).
Current Listen port	Ensure to configure to *443*.
Use System Manager for certificates	Ensure to configure to *y*.
Local frontend host	The Avaya Aura® Device Services FQDN. The configuration utility uses this value to generate certificates for the node.
Keystore password	The password to use for the local keystore. You need this password for any certificate management tasks.

Related links

Configuration Checklist for Avaya Aura Device Services on page 315

Configuration Checklist for Avaya Aura® Web Gateway

The Avaya Aura® Web Gateway server acts as a gateway to Avaya Aura® clients and applications utilizing WebRTC signaling and media. Avaya Aura® Web Gateway also provides the push notification service, enabling clients to receive incoming call alerts and other notifications from the Apple Push Notification service (APNs).

For a full explanation on deploying and configuring Avaya Aura® Web Gateway, download the documentation from the Avaya Support website at http://support.avaya.com or from the Avaya Documentation Portal.

Ensure to perform the procedures listed in the following table. They are required steps in the overall configuration procedure. For details on these procedures, see *Administering the Avaya Aura® Web Gateway* . If the procedure is in another document, the configuration checklist refers the document.

Note:

Use these procedures for Avaya Aura® Web Gateway release 3.7.x and up.

Conference clients and services have new names:

Old client/service name	New client/service name
WebRTC client	Avaya Equinox® Meetings for Web
Avaya Equinox, Avaya Equinox for Web	Avaya IX™ Workplace Client
Avaya Conferencing Server, Avaya Equinox® Conferencing	Avaya Equinox® Management

No.	Task	Link/Notes	✔
1	Configure resource sharing (CORS).	Enable CORS to ensure there is no communication issues among the different servers in the deployment. On the Avaya Aura® Web Gateway administration portal, click **Advanced** > **CORS Configuration** Ensure to select: • **Enable Cross-Origin Resource Sharing** • **Allow access from any origin**	
2	Configure Avaya Aura® Web Gateway Front-end host, Avaya Aura® System Manager, and use of System Manager for certificate management.	Use the Command Line Interface (CLI) utility to configure the settings. See Configuring the Front-end host of Avaya Aura Web Gateway, System Manager, and Certificate on page 327.	
3	Add Avaya Aura® System Manager to Avaya Aura® Web Gateway.	On the Avaya Aura® Web Gateway administration portal, click **General Network Settings** > **System Manager**. Ensure to configure the following settings: • **FQDN**: Enter the System Manager FQDN • **Port**: *443* • **Protocol**: **https** • **Username**: For example, *admin* • **Password** Ensure to add Avaya Aura® Web Gateway to Avaya Aura® System Manager. See *Deploying Avaya Aura® Web Gateway*.	

Table continues…

No.	Task	Link/Notes	✔
4	Add Avaya Aura® Device Services to Avaya Aura® Web Gateway.	Avaya Aura® Device Services is used here to process all logins to the Unified Portal. for the Web clients. If the AADS configuration does not match, the client gets an error message when it tries to sign in. On the Avaya Aura® Web Gateway administration portal, click **General Network Settings** > **Devices**. Ensure to configure the following settings: • **FQDN**: the Avaya Aura® Device Services reverse proxy FQDN. • **Client Interface Port**: *443* This setting matches the **Front-end Port** setting in procedure 10, *HTTPS Reverse Proxy configuration*. • **Server-to-server interface port**: *8440* • **Protocol**: **https** This setting matches the **Front-end Protocol** setting in procedure 10, *HTTPS Reverse Proxy configuration*.	
5	Assign a location to each Avaya Aura® Web Gateway.	A Web Gateway location represents a grouping of one or more Web Gateways. On the Avaya Aura® Web Gateway administration portal, click **General Network Settings** > **Location** > **Web Gateway Locations**. The Web Gateway retrieves the information from Avaya Aura® System Manager. For detailed information on location management, see also *Administering Avaya Aura® Session Manager*.	
6	Assign and prioritize locations for each Avaya Aura® Web Gateway location.	All Web Gateways in a location use Avaya Aura® Media Servers in the assigned server locations. The order you set in the Assigned Locations list determines how the Avaya Aura® Media Server locations serve the selected Web Gateway location. On the Avaya Aura® Web Gateway administration portal, click **General Network Settings** > **Location** > **Location Assignments and Priorities**. To configure the Media Server in System Manager, see *Deploying Avaya Aura® Web Gateway*.	
7	View and manage the connectivity status of Avaya Aura® Media Server for a specific node in a cluster.	Click **General Network Settings** > **Media Services**.	

Table continues…

No.	Task	Link/Notes	✔
8	Add Avaya Equinox® Management to Avaya Aura® Web Gateway.	On the Avaya Aura® Web Gateway administration portal, click **Equinox Conferencing** > **Conferencing Server**. Ensure to configure the following settings: • **Equinox Conferencing Server IP**: For a single server, enter the Equinox Management IP address. If there is High Availability with the server, enter the server's virtual IP. • Uncheck the **Force Media Server usage for WebRTC calls** checkbox because Equinox Management governs WebRTC calls and not Media Server.	

Table continues…

No.	Task	Link/Notes	✔
9	Configure the Unified Portal of Avaya Aura® Web Gateway.	On the Avaya Aura® Web Gateway administration portal, click **Equinox Conferencing** > **Unified Portal Settings**. The following fields have default settings: • **Avaya Equinox Client Aura Video Ignore**: *true* • **Allow Recording Guest Access**: *false* This setting is considered as best practice because not everyone wants guests to access the recording. • **Allow Portal Guest Access**: *true* • **Allow ESG Guest Access**: *true* In **Avaya Equinox Client Aura Domain**, enter the SIP domain FQDN. This is the SIP domain of enterprise users. Avaya IX™ Workplace Client need this domain FQDN to join a meeting. To avoid issues with SIP traffic, ensure that SIP domains are identical across all the deployment: • Session Manager On the home page of the System Manager Web Console, click **Elements** > **Routing** > **Domains**. For the detailed procedure, see *Administering Avaya Aura® Session Manager*. • SIP users For detailed information, see *Administering Avaya Aura® Session Manager*. • Equinox Management - On the administrator web interface of Equinox Management, click **Settings** > **Policies** > **Meeting Policies** > **Default SIP Domain**. - On the administrator web interface of Equinox Management, click **Devices** > **All** > **<SIP Server>** > **SIP Domain**. For the detailed procedure, see *Deploying Avaya Equinox® Solution*. Under **Advanced Settings**, customize the browsers and browser versions.	

Table continues…

No.	Task	Link/Notes	✔
10	Review/configure Avaya SBCE HTTP Reverse Proxy service on Avaya Aura® Web Gateway.	On the Avaya Aura® Web Gateway administration portal, click **External Access** > **HTTP Reverse Proxy**. If you implemented procedure 2 in this table, CLI automatically configures the reverse proxy fields on this page. Use this page to double-check the following settings: • **Front-end Host**: Equinox conferencing reverse proxy FQDN. • **Front-end Port**: 443 • **Front-end Protocol**: https • **Enable port for remote access**: checkbox enabled • **Front-end port for remote access**: 8444 If you do not use the internal load balancer of the Web Gateway, you must enable the use of an external load balancer from this page, by selecting **Enable use of an external load balancer**. To keep the Web Gateway fully functional, make any other setting change through CLI.	
11	Add Avaya SBCE STUN service to Avaya Aura® Web Gateway.	This configuration allows web traffic. On the Avaya Aura® Web Gateway administration portal, click **External Access** > **STUN Servers** > **STUN Servers**. Ensure to configure as follows: • **Address**: enter the FQDN of Equinox Conferencing TURN/ STUN service. • **Port**: *443*. • Match Avaya SBCE configuration and STUN TURN settings with Equinox Management.	
12	Configure STUN priority to prioritize STUN servers for each web location.	If you have multiple Avaya SBCEs, you can customize the server location. On the Avaya Aura® Web Gateway administration portal, click **External Access** > **STUN Servers** > **STUN Priority**.	

Table continues…

No.	Task	Link/Notes	✔
13	Add Avaya SBCE to Avaya Aura® Web Gateway for remote client access.	On the Avaya Aura® Web Gateway administration portal, click **External Access** > **Session Border Controller**. Select **Enable TURN in WebRTC Client**. Select the **Node address**: Avaya Aura® Web Gateway FQDN. It is the Local Frontend host FQDN that you configured in procedure 2. For load monitoring, match the following settings across all devices: • Configure **HTTP Port** to *443* and **HTTP Protocol** to **https**. Depending on the customer's preferences, you can also configure **HTTP Port** to *80* and **HTTP Protocol** to **http**. • Enter the **HTTP Address** (same as **SIP Address**). • On Avaya SBCE, under **ASBCE** > **Network & Flows** > **Advanced Options** > **Load Monitoring** , match internal **Listen IP** with **HTTP Address**. • On Equinox Management, under **Devices** > **All** > **<ASBCE>**: - Match **Internal SIP IP** with **HTTP Address**. - Match **Check status IP** with **HTTP Address**. - Match protocol in **Check status protocol**.	
14	Select a WebLM server for Avaya Aura® Web Gateway.	On the Avaya Aura® Web Gateway administration portal, click **Licensing**. Ensure to select **Use SMGR url for license server**. Ensure to properly load the license on System Manager.	
15	Configure Avaya Aura® Web Gateway to request identity certificates from Avaya Aura® System Manager.	If you must change the Front-end FQDN, use CLI to regenerate the certificates. After the certificate validity expires, you can regenerate the certificates from the SMGR Certificates page. You need the enrollment password to get the new certificates from System Manager. On the Avaya Aura® Web Gateway administration portal, click **Security Settings** > **Certificate Management** > **SMGR Certificates**.	

Table continues…

No.	Task	Link/Notes	✔
16	Manage the following identity certificates tasks: • CSRs • Keystore data • Server interfaces.	This procedure allows to double-check the certificates System Manager automatically generated after you implemented procedure 2 in this table. On the Avaya Aura® Web Gateway administration portal, click **Security Settings** > **Certificate Management** > **Identity Certificates** Ensure System Manager has assigned a certificate to each server interface: • Application • Internal • OAM • SIP	
17	View the details of each server interface certificate.	This procedure allows to double-check the certificates System Manager automatically generated after you implemented procedure 2 in this table. On the Avaya Aura® Web Gateway administration portal, click **Security Settings** > **Certificate Management** > **Identity Certificates** > **Server Interfaces** > **Application** > **Details**.	
18	Configure the Client-device Certificate Policy.	On the Avaya Aura® Web Gateway administration portal, click **Security Settings** > **HTTP Clients**. Ensure to configure **REST** and **OAMP** to **OPTIONAL**.	
19	Configure trusted hosts.	On the Avaya Aura® Web Gateway administration portal, click **Security Settings** > **Trusted Hosts**. Ensure to enter: • Avaya Aura® Device Services FQDN • Avaya Equinox® Management FQDN. If there are multiple Avaya Aura® Device Services servers, you have to add each and every server.	
20	Configure the SIP and SRTP security policy for sessions.	On the Avaya Aura® Web Gateway administration portal, click **Security Settings** > **Session Security**.	
21	Configure audio codec preferences for SIP and Web clients.	Configure if you want to limit WebRTC clients to use a certain codec and always use encryption, based on the security policy for these clients. On the Avaya Aura® Web Gateway administration portal, click **Advanced** > **Media Settings** > **Audio**.	

Table continues…

No.	Task	Link/Notes	✔
22	Configure video codec preferences for SIP and Web clients.	Configure if you want to limit WebRTC clients to use a certain codec and always use encryption, based on the security policy for these clients. On the Avaya Aura® Web Gateway administration portal, click **Advanced** > **Media Settings** > **Video**.	
23	Configure Avaya Aura® Media Server credentials in Avaya Aura® Web Gateway.	On the Avaya Aura® Web Gateway administration portal, click **Advanced** > **Media Settings** > **AAMS Credentials**. Ensure to uncheck **Use Credentials for Authentication**. **Important:** Ensure to uncheck the corresponding authentication settings in Avaya Aura® Media Server. On the Avaya Aura® Media Server web interface, click **Home** > **EM** > **System Configuration** > **Signaling Protocols** > **REST** > **General Settings**. For the detailed procedure, see *Implementing and Administering Avaya Aura® Media Server*. Uncheck the following fields: • **Basic Authentication** • **Digest Authentication**	
24	Ensure that all connections are up, showing green status icons.	This is a sanity check to see if the servers are properly configured. For example, if Avaya Aura® Media Server credentials do not match, the green status icon is turned off. On the Avaya Aura® Web Gateway administration portal, click **System Overview**. You get detailed information and manage the connection status of the following deployment servers: • LDAP • Avaya Aura® Device Services • Avaya Aura® System Manager • Avaya Equinox® Management • Avaya Aura® Media Server.	

Related links

[Configuring the Front-end host of Avaya Aura Web Gateway, System Manager, and Certificate](#) on page 327

Configuring the Front-end host of Avaya Aura® Web Gateway, System Manager, and Certificate

About this task

You can perform these configurations from the Avaya Aura® Web Gateway administration portal or from the Command Line Interface (CLI).

The following procedure describes the configuration from the CLI utility. The CLI utility provides a complete picture of the fields you need to configure. Once you complete the configuration, Avaya Aura® Web Gateway automatically configures reverse proxy, generates certificates and restarts the system.

By default, Avaya Aura® Web Gateway uses a single network interface for all traffic types. For additional security, you can use the out-of-band management functionality to isolate client traffic from system management traffic by using different network interfaces for these traffic types. For details, see the out-of-band management configuration checklist in *Administering the Avaya Aura® Web Gateway* .

Avaya Aura® Web Gateway includes an internal load balancer. To configure an external load balancer, click **External Access** > **HTTP Reverse Proxy**, and select **Enable use of an external load balancer**.

Use CLI for further changes.

If you use the administration portal for these configurations, you must restart the system manually and regenerate certificates.

Procedure

1. Log in to the Linux shell on the initial node by using the Linux administrator account credentials.
2. Run the Avaya Aura® Web Gateway configuration utility using the `app configure` command.
3. Select **Front-end host, System Manager and Certificate Configuration**.
4. Configure the following settings in the fields.

Field	Description
Front-end FQDN	Equinox conferencing reverse proxy FQDN. End-user clients use the front-end FQDN to access the services provided by Avaya Aura® Web Gateway. For a cluster deployment, you must configure the front-end FQDN as the FQDN of the virtual IP address. If the deployment uses an external load balancer, set this value to the FQDN of the load balancer.

Table continues…

Field	Description
System Manager FQDN	The FQDN of the Avaya Aura® System Manager that signs the certificates.
System Manager HTTPS Port	Configure to *443*. The HTTPS port used for the Alarm Agent for the current Avaya Aura® Web Gateway.
System Manager Enrollment Password	The Avaya Aura® System Manager enrollment password. **Note:** To get the password, log in to System Manager and navigate to **Service** > **Security** > **Certificates** > **Enrollment Password**.
Override port for reverse proxy	Configure to *n* (disabled).
Override port for remote access	Configure to *y*. Enables the Avaya Aura® Web Gateway port. Reverse proxy Avaya SBCE uses the port for remote HTTP based clients that request access to the enterprise. The Avaya SBCE reverse proxy receives conferencing access requests from external clients on port 443, and then forwards them to the Avaya Aura® Web Gateway on the reverse proxy port. Clients within the enterprise continue to access Avaya Aura® Web Gateway directly using port 443.
Front-end port for remote access	Configure to *8444*.
Use System Manager for certificates	Configure to *y*.
Local frontend host	The Avaya Aura® Web Gateway FQDN. The configuration utility uses this value to generate certificates for the node.
Keystore password	The password to use for the local keystore. You need this password for any certificate management tasks.

Related links

Configuration Checklist for Avaya Aura Web Gateway on page 318

Configuration Checklist for Avaya Aura® Media Server

Avaya Aura® Media Server (MS) (AAMS) performs all multimedia processing. AAMS supports standard media processing features, such as play announcement, collect DTMF, audio and video conferencing, and automatic tone detection, as well as more advanced capabilities including encryption (SIP TLS, SRTP), VoiceXML 2.1, CCXML 1.0, MLPP, quality of service (QoS) monitoring,

For a full explanation on deploying and configuring Avaya Aura® Media Server for WebRTC calls, download the documentation from the Avaya Support website at http://support.avaya.com or from the Avaya Documentation Portal.

Ensure to perform the procedures listed in the following table. They are required steps in the overall configuration procedure. For details on these procedures, see *Implementing and Administering Avaya Aura® Media Server*. If the procedure is in another document, the configuration checklist refers to the document.

No.	Task	Link/Notes	✔
1	Manage the Media Server cluster configuration.	A cluster is a collection of Avaya Aura® Media Server (MS) working together to provide scalability, redundancy, and high availability. Media Servers use Avaya Aura® System Manager to provide an integrated point of management. To use Avaya Aura® MS Element Manager (EM) to enroll Media Servers in System Manager, see *Managing Avaya Aura® Media Server from System Manager*. On the Avaya Aura® System Manager web console, click **Elements** > **Media Server** > **Cluster Administration**. Ensure to configure the following settings: • **Cluster Name**: enter the cluster FQDN. • **Status**: select *Available*. • **Type**: select *LoadSharing* Avaya Aura® Web Gateway does not support Media Server High Availability cluster configuration when using WebRTC. • **Primary Server**: the element administrative name of the Primary Media Server of the cluster. Click the link to lead to the Element Manager of the Media Server. • **Enable/Disable**: set to *Enable* to filter the cluster search.	

Table continues…

No.	Task	Link/Notes	✔
2	Manage the Media Server configuration.	You can only view the name, role, SIP IPv4, SIP TCP Port, and SIP TLS Port. You can configure the location of the Media Server. For information about editing the location, see *Administering Avaya Aura® Session Manager*. On the Avaya Aura® System Manager web console, click **Elements** > **Media Server** > **Server Administration**.	
3	Manage the Media Server cluster assignment to the application.	For details, see *Managing Avaya Aura® Media Server from System Manager*. On the Avaya Aura® System Manager web console, click **Elements** > **Media Server** > **Application Assignment**. Assign a Media Server cluster to the application.	
4	Manage the Media Server key store and service profiles.	See security configuration in *Implementing and Administering Avaya Aura® Media Server*. On the Media Server UI, click **EM** > **Home** > **Security** > **Certificate Management** > **Key Store** During deployment, the Media Server creates a default staging certificate. Use System Manager to create an identity certificate for the Media Server. The Media Server has five service profiles. Each service profile holds an identity certificate. You can use the same identity certificate for all five service profiles.	

Table continues…

No.	Task	Link/Notes	✔
5	Manage the Media Server profile.	On the Media Server UI, click **EM** > **Home** > **System Configuration** > **Server Profile** > **General Settings** The Media Server automatically selects a capacity profile that matches the performance limits of the physical or virtual hardware on which the system is installed. The selected profile restricts the maximum number of sessions the Media Server concurrently supports. You can select a capacity profile that lowers the maximum number of sessions to conserve system resources, such as CPU and memory. This is useful when the Media Server is co-resident with other servers. Ensure that the server profile includes the following functions: • **Firewall NAT Tunneling Media Process**: select the checkbox. • **Recording Audio/Video Transformer**: clear the checkbox. • **Video Media Processor**: select the checkbox when you require video relay and switching capabilities. • **VoiceXML Interpreter**: select the checkbox. • **Web Collaboration**: clear the checkbox.	
6	View and manage REST configuration.	On the Media Server UI, click **EM** > **Home** > **System Configuration** > **Signaling Protocols** > **REST** > **General Settings** Ensure to configure the fields as follows: • **Enable TLS Transport**: select the checkbox. • **Enable TLS Mutual Authentication**: select the checkbox. • **Basic Authentication**: clear the checkbox. • **Digest Authentication**: clear the checkbox. • **Authentication Realm**: clear the checkbox. • **Authentication Username**: enter the administrator user name. • **Authentication Password**: enter the password. • **Confirm Authentication Password**: re-enter the password.	

Table continues…

No.	Task	Link/Notes	✔
7	View and manage ICE configuration.	On the Media Server UI, click **EM** > **Home** > **System Configuration** > **Media Processing** > **ICE** > **General Settings** For TURN on Client deployments, ensure to clear the **Force Media Through a Configured TURN Server** checkbox. For TURN on Media Server deployments, click the checkbox,.	
8	View and manage ICE on TURN/ STUN servers.	On the Media Server UI, click **EM** > **Home** > **System Configuration** > **Media Processing** > **ICE** > **STUN/TURN Servers** For TURN on Client deployments, ensure to clear the **Accounts** and **Servers** sections. For TURN on Media Server deployments, activate the sections.	

Configuration Checklist for Avaya Equinox® Management in TE

Equinox Management provides the common management framework of centralized management functions for provisioning and administration of the deployment components.

For a full explanation on deploying and configuring Equinox Management, download the documentation from the Avaya Support website at http://support.avaya.com or from the Avaya Documentation Portal.

Ensure to perform the following procedures in Equinox Management. They are required steps in the overall configuration procedure.

No.	Task	Link/Notes	✔
1	Configure the portal URL for Meet-Me clients.	Configuring the portal URL for Meet-Me clients on page 333	
2	Configure Equinox Management.	Configuring Avaya Equinox® Management on page 334	
3	Configure the User Portal.	Configuring User Portal access for TE on page 335	
4	Configure Avaya Aura® Device Services.	Configuring Avaya Aura Device Services in Avaya Equinox Management on page 336	

Table continues…

No.	Task	Link/Notes	✔
5	Configure Avaya Aura® Web Gateway.	Configuring Avaya Aura Web Gateway on Avaya Equinox® Management on page 336	
6	Configure Avaya SBCE .	Configuring Avaya SBCE on Equinox Management on page 279	
7	Configure Avaya Equinox® Media Server.	Configuring Avaya Equinox® Media Server in Avaya Equinox® Management on page 338	
8	Configure Avaya Equinox® Media Server certificate.	Creating security certificates on page 191	

Related links

Configuring the portal URL for Meet-Me clients on page 333
Configuring Avaya Equinox® Management on page 334
Configuring User Portal access for TE on page 335
Configuring Avaya Aura Device Services in Avaya Equinox Management on page 336
Configuring Avaya Aura Web Gateway on Avaya Equinox® Management on page 336
Configuring Avaya SBCE on Equinox Management on page 279
Configuring Avaya Equinox® Media Server in Avaya Equinox® Management on page 338

Configuring the portal URL for Meet-Me clients

About this task

When you use URL rewriting to establish a call, you must configure an advanced parameter that enables external clients to use the UCCP service hosted on Equinox Management. If you do not configure this parameter, external clients try to resolve the connection to the internal FQDN of Equinox Management and this does not work in the URL rewriting scenario.

Log in to Equinox Management to configure Equinox Conference Control.

Procedure

1. In the Equinox Management administrator portal, navigate to **Dashboard > ☰ > Advanced Parameters**.
2. In the **Property Name** field, enter `com.visionnex.vcms.core.uccp.customizedUCCPURL`
3. In the **Property Value** field, enter `https://<single Equinox Management service FQDN>:443/uwd/ws?ticket=`

   For the single Equinox Management service FQDN, enter the Equinox Conferencing Reverse Proxy FQDN.
4. Select **Apply**.

Related links

Configuration Checklist for Avaya Equinox® Management in TE on page 332

Configuring Avaya Equinox® Management

About this task

Use the following procedure to configure Equinox Management in a TE deployment that uses Avaya SBCE for remote access to conferencing.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Devices** > **Configuration**.
3. Configure the fields on the page, as described in the following table:

Field	Description
Basic Settings	
Location	Select the Equinox Management location. This field is relevant only for service providers or deployments with multiple locations.
Service FQDN	Enter the Equinox Management FQDN.
Public URL branch	FQDN of Equinox Conferencing Reverse Proxy with URL rewrites for TE.
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 Equinox Management **Note:** When the device is online, you can change its IP address in this field.
Subnet Mask	The subnet mask of the user portal

Table continues…

Field	Description
Default Gateway	The default gateway of the user portal
Local FQDN	Enter the Equinox Management FQDN.

4. Select **Apply**.

Related links

Configuration Checklist for Avaya Equinox® Management in TE on page 332

Configuring User Portal access for TE

About this task

Avaya Aura® Web Gateway includes two modules:

- Web Gateway
- User Portal. Configure the User Portal in Equinox Management as described in the following procedure.

Before you begin

You must set up and configure the solution components as described in the server documentation. The following procedure describes only a few of the device settings that are required for the deployment.

Procedure

1. Log in to Equinox Management administrator portal.
2. Navigate to **Settings** > **User Portal**.
3. Enter the following parameters in the fields:
   - **Frontend FQDN**: the public FQDN for Equinox Conferencing. This is the FQDN that clients use for browsing to the Equinox Portal. For example, the Equinox Conferencing Reverse Proxy FQDN.
   - **Frontend Port**: `443`
   - **Enable TURN in WebRTC Client**: check the box to allow WebRTC media tunneling.
4. Select **Apply** .

Related links

Configuration Checklist for Avaya Equinox® Management in TE on page 332

Configuring Avaya Aura Device Services in Avaya Equinox Management

About this task

You can use Avaya Aura® Device Services to search for clients and endpoints only after you configure Avaya Aura® Device Services in Equinox Management.

Procedure

1. Select **Devices > Devices by Type > AADS**, and select **Add**.
2. Configure these fields on the page:
   - **Name**: Enter the FQDN of Avaya Aura® Device Services.
   - **IP Address**: The IP Address of Avaya Aura® Device Services.
   - **Location**: Select the location that matches the Avaya Aura® Device Services location assignment on Session Manager.
   - Select **Secure connection between this server and Equinox Management using TLS**.
3. Select **OK**.

   The configured Avaya Aura® Device Services appears on the Avaya Aura® Device Services page, with detailed information. Wait for a few minutes until the newly added Avaya Aura® Device Services indicator changes from gray to green.

Related links

Configuration Checklist for Avaya Equinox® Management in TE on page 332

Configuring Avaya Aura® Web Gateway on Avaya Equinox® Management

About this task

Add Avaya Aura® Web Gateway as a managed server device on Avaya Equinox® Management.

Procedure

1. Select **Devices** > **Devices by Type** > **User Portals**, and select **Add**.
2. Configure these fields on the page:
   - **Name**: enter the Avaya Aura® Web Gateway FQDN.
   - **IP Address**: enter the IP Address of Avaya Aura® Web Gateway.
   - **Location**: select *Home* as the Avaya Aura® Web Gateway location.
3. Select **OK**. The **User Portals** page displays Avaya Aura® Web Gateway, with detailed information. Wait for a few minutes until the server icon changes from gray to green.

Related links

Configuration Checklist for Avaya Equinox® Management in TE on page 332

Configuring Avaya SBCE on Equinox Management

About this task

Add ASBCE to Equinox Management and then configure TURN/STUN.

In addition to this procedure, you must configure the STUN TURN Server on the Media Server Configuration page for video media servers. For details, see *Configuring the Equinox Media Server from Equinox Management* in *Administrator Guide for Avaya Equinox® Management*.

Important:

ASBCE must be operational once you add it into Equinox Management, so the Media Server and Web Gateway can start the meeting. When ASBCE is operational, it displays a green status LED in the ASBCE list.

Procedure

1. Access the Equinox Management administrator portal.
2. Select **Devices** > **Devices by Type** > **ASBCE**, and select **Add**.

   The **Add ASBCE** page appears.
3. Configure these fields as follows:
   - **Name**: enter a name for the ASBCE server.
   - **IP Address**: enter the IP address of the Element Management System (EMS), or any of the ASBCE IP addresses.

     EMS is the ASBCE management interface.
   - **Location**: select the location of the ASBCE server.
4. Select **OK**.

   The ASBCE server displays on the **ASBCEs** page.
5. Select the ASBCE name in the ASBCE list and configure additional settings.

   The **Update ASBCE** page appears.
6. Configure these fields as follows:
   - **Listen/Relay Internal IP**: enter the ASBCE server's internal IP address (A1).
   - **Port**: enter `3478`.
   - **Listen/Relay Public IP**: enter the ASBCE server's public IP address as seen from the public Internet (B1 if public, or firewall NAT public address of B1).
   - **Port**: enter `3478`.
   - **Internal SIP IP**: enter the IP address of the internal interface configured for signaling on ASBCE (A1).

- **SIP protocol**: select **TLS**.
- **SIP port**: enter `5061`.
- **Check status IP**: enter the internal address configured for the load monitoring entry (A1).
- **Check status protocol**: select **Http** .
- **HTTP port**: enter `443` .

7. Select **OK**.

Related links

Configuration Checklist for Avaya Equinox® Management in TE on page 332

Configuring Avaya Equinox® Media Server in Avaya Equinox® Management

About this task

This procedure describes the configuration of client access to web collaboration. The Web Collaboration Server (WCS) is a component in Equinox Media Server.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the server instance in the list.

   Equinox Management opens the media server window.
3. Click the **Configuration** tab.
4. Configure the fields as described in the table.

Table 50: Configuration field descriptions

Field name	Description
Basic Settings	
Name	Enter the Management FQDN of Equinox Media Server.
Location	The server location in the enterprise network. This field is relevant only if there are multiples locations in the deployment.
Service FQDN	Enter the Management FQDN of Equinox Media Server.
Public URL branch	To support multiple WCS with a single public FQDN, define a public branch URL defined for each WCS. For example, enter `<ASBCE FQDN> /WCS1`. The FQDN is the Equinox Conferencing Reverse Proxy with URL rewrites for TE.

Table continues…

Field name	Description
Secure connection	Click the checkbox to enable a secure connection between Equinox Media Server and Equinox Management using TLS. You can use this option only if you installed security certificates for TLS.
Master Media Server for Cascading	The option to set the specified server as the master server when cascading is enabled. When the option is not selected, Equinox 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 that sets the time for Equinox Media Server. If there is no NTP server, the value of the field must be 0.0.0.0.
Time Zone	The time zone where the NTP server is configured.
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 Equinox Media Server
Subnet Mask	The subnet mask of Equinox Media Server.
Default Gateway	The default gateway of Equinox Media Server.
Local FQDN	Enter the Management FQDN of Equinox 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 to which this Equinox Media Server 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, Equinox Management issues an alarm.
SIP Settings	
SIP Proxy Server	The IP Address of the SIP Proxy Server
Transport Type	Enter **TLS**.
Turn/Stun Server	Enter **None**.

Related links

[Configuration Checklist for Avaya Equinox® Management in TE](#) on page 332

Chapter 13: Avaya Equinox H.323 Edge deployment

Avaya Equinox® H.323 Edge Client overview

Avaya Equinox® H.323 Edge provides a complete firewall and NAT traversal solution and support for secure connectivity between enterprise networks and remote locations.

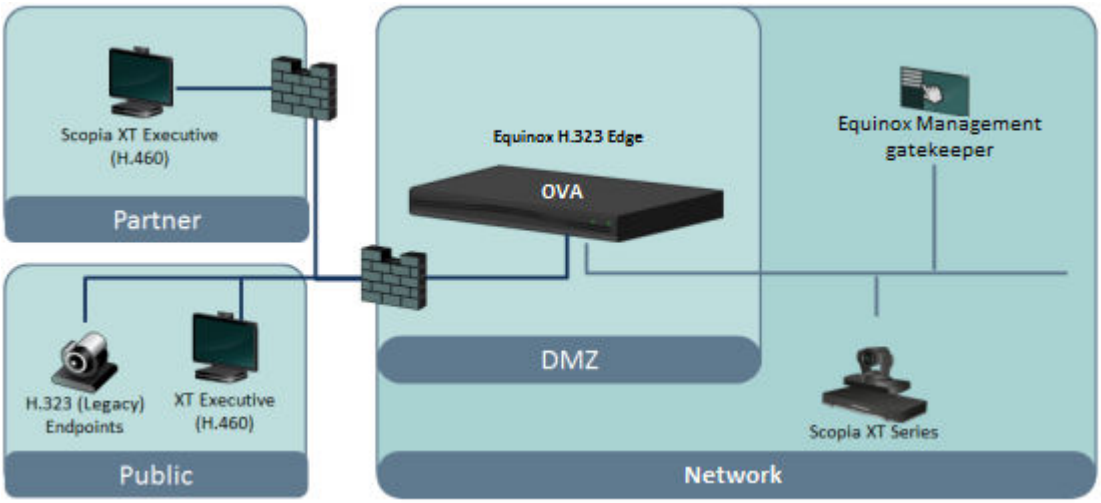
Note:

Equinox H.323 Edge is an optional component. Equinox H.323 Edge is required when you need to connect remote H.323–based video conferencing endpoints to an Avaya Equinox® solution conference through firewalls.

Equinox H.323 Edge is part of the Avaya Equinox® solution. Components of Avaya Equinox® can be combined to fit the existing network topology and video conferencing requirements of the enterprise. Equinox H.323 Edge is an optional Avaya Equinox® solution component which is deployed in Over The Top and Team Engagement deployments. Equinox H.323 Edge is deployed in network DMZs when enterprises need H.323–based calls to traverse the network firewall.

Equinox H.323 Edge is also deployed in multi-tenant deployments when service providers need to connect the remotely-located H.323–based endpoints of tenants with the Avaya Equinox® solution deployment of the service providers.

Equinox H.323 Edge maintains the security and advantages of firewall and NAT over heterogeneous video networks and supports seamless integration with existing video endpoints and infrastructure components.



Equinox H.323 Edge uses the H.460 protocol. 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.

Endpoints in private networks can communicate with the endpoints in public networks through Equinox H.323 Edge. Endpoints in public networks can join conferences hosted in private networks through Equinox H.323 Edge if there is an open connection through the firewall. H.323 Gatekeeper provides standalone address resolution functionality in H.323–based networks.

Equinox H.323 Edge supports static addresses for external endpoints for conferences hosted on the enterprise network. Users located outside the enterprise firewall can join conferences using addresses such as `1234@h323edge.company.com`, while users with endpoints logged in to Equinox H.323 Edge can directly dial numbers such as 1234 to join conferences.

Equinox H.323 Edge virtual server deployment checklist

No.	Task	Link/Notes	✔
1	Download the Equinox H.323 Edge software from PLDS	Downloading software from PLDS on page 32	
2	Deploy the Equinox H.323 Edge virtual server	Deploying the Equinox H.323 Edge virtual server on page 348	
3	Start the Equinox H.323 Edge virtual server	Starting the Equinox H.323 Edge virtual server on page 349	
4	Configure the Equinox H.323 Edge virtual server automatic startup settings	Configuring the virtual machine automatic startup settings on page 349	

Avaya Equinox® H.323 Edge initial configuration checklist

No.	Task	Link/Notes	✔
1	(Optional) Add more networks to the Avaya Equinox® H.323 Edge.	Adding networks to Equinox H.323 Edge on page 350	
2	Add Avaya Equinox® H.323 Edge as a device in Avaya Equinox® Management	Adding Equinox H.323 Edge in Equinox Management on page 352	
3	(Optional) Configure separate IP interfaces for the internal and external network traffic on the Avaya Equinox® H.323 Edge virtual server.	Configuring a second IP interface in Avaya Equinox® H.323 Edge for external traffic on page 352	
4	Configure the ports on Avaya Equinox® H.323 Edge.	Configuring Ports on Equinox H.323 Edge on page 354	
5	Configure the gatekeeper .	Integrating with the gatekeeper on page 356	
6	Configure NAT.	Integrating with NAT on page 357	
7	Configure the NTP server.	Configuring the NTP server on page 357	
8	Configure access to calls to H.323 legacy endpoints.	Configuring access for calls to H.323 legacy endpoints on page 358	
9	Configure URI-based dialing.	URI Dialing Functionality on page 359	
10	Configure IP address-based dialing.	Configuring IP address-based dialing to external endpoints on page 363	
11	Secure the connection with Avaya Equinox® Management.	Securing the connection with Equinox Management using TLS on page 368	
12	Update the Avaya Equinox® H.323 Edge license	Adding or updating licenses on page 436	
13	Configure remote access to administer Avaya Equinox® H.323 Edge from Avaya Equinox® Management.	Configuring remote access on page 368	
14	Configure QoS.	Configuring QoS for audio and video on page 369	
15	(Optional) Create Avaya Equinox® H.323 Edge server clusters to optimize the server use without load balancers.	Creating an Equinox H.323 Edge server cluster on page 371	

Technical specifications of Equinox H.323 Edge

Requirement	Specification
Communications	• H.323 • IPv4 • Bit rate: up to 4Mbps per call
Call capacity	• Up to 120 concurrent calls • Up to 720 registered devices
Hardware load balancers for clusters Load-balancers are optional. Load balancers are needed only when you cannot configure dual NIC virtual machines to use the built-in virtual machine clustering mechanism.	• Radware AppDirector 208 • Radware AppDirector 1000 • F5 BIG-IP Load Traffic Manager 1600 Series
Firewall traversal	• H.460.18, H.460.19 including support for multiplexed media • Direct Public Access (DPA) solution for direct communication between internal endpoints in the internal network and external ones in the public network. • If the remote system has Equinox H.323 Edge Client, you can send the communications data securely through the firewall by establishing a route for the data through Equinox H.323 Edge Client
Security	H.235 for call privacy in all traversal modes, such as H.460, tunneling, and DPA

Ports configuration

Equinox H.323 Edge is Equinox Solution's answer to firewall traversal. Equinox H.323 Edge is an H.460 server, typically deployed in the DMZ, while Equinox H.323 Edge Client is a tunneling client, typically deployed outside the enterprise firewall alongside the remote H.323 endpoint (see Figure 100: H.323 connections to Equinox H.323 Edge on page 344).

Many recent H.323 endpoints have built-in H.460 functionality (which enables secure communication), thereby avoiding the need for Equinox H.323 Edge Client. If an H.323 endpoint located in a partner company does not have H.460 capabilities, it must communicate via Equinox H.323 Edge Client to access Equinox H.323 Edge in the DMZ (see Figure 100: H.323 connections to Equinox H.323 Edge on page 344).

Important:

There must be no firewall between the H.323 endpoint (device) and Equinox H.323 Edge Client.

An H.323 endpoint in the public network can also directly dial Equinox H.323 Edge using direct port access (ports 4000-5000).

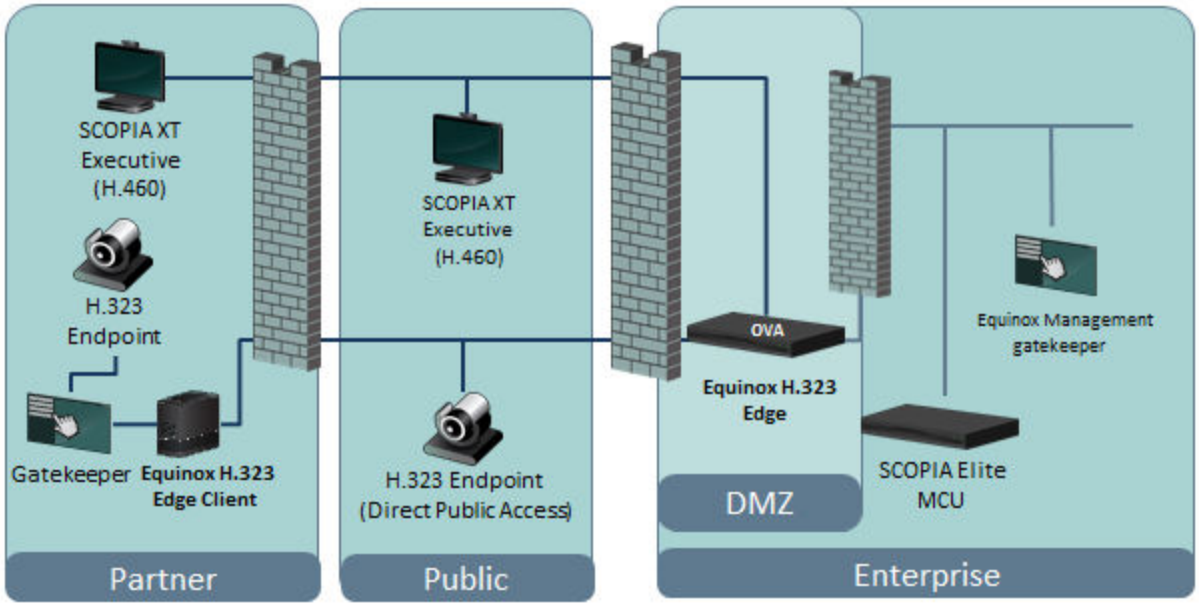


Figure 100: H.323 connections to Equinox H.323 Edge

When opening ports to and from Equinox H.323 Edge, use the following as a reference:

- If opening ports that are both to and from Equinox H.323 Edge, see Table 51: Bidirectional Ports to Open Equinox H.323 Edge on page 345.
- If opening ports that are both to and from Equinox H.323 Edge Client, see Table 52: Bidirectional Ports to Open on the Equinox H.323 Edge Client on page 347.

Important:

In order for an H.323 endpoint (or other H.323 device) within the enterprise to successfully connect to Equinox H.323 Edge in the DMZ via the enterprise firewall (see Figure 101: Contacting Equinox H.323 Edge from within the enterprise on page 345), you must do the following:

- Install Equinox H.323 Edge Client within the enterprise or use H.460-enabled endpoints.
- Open the internal firewall to Equinox H.323 Edge (12000 to 15000, bidirectional).

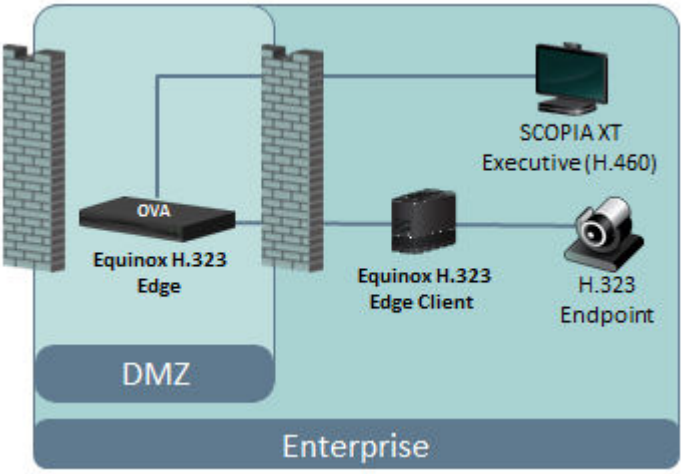


Figure 101: Contacting Equinox H.323 Edge from within the enterprise

Important:

The specific firewalls to open ports depends on where Equinox H.323 Edge Client and other Avaya Equinox® Solution components are deployed.

Table 51: Bidirectional Ports to Open Equinox H.323 Edge

Port Range	Protocol	Source	Functionality	Result of Blocking Port	Required
53	DNS (UDP)	DNS server	Enables querying the DNS for domains per call	Cannot support domain name calls and dialing by URI	Mandatory if using URI dialing
1719	UDP	H.460.18–based endpoint or H.460.18–based client gatekeeper	Enables registration of H.460–based endpoints	H.460.18–based endpoints cannot register through Equinox H.323 Edge	Mandatory for H.460–based endpoints
1720	TCP	Any H.323 device using Q.931 signaling in DPA mode	Enables IP call signaling	No signaling capabilities: guest users cannot dial into internal endpoints	Mandatory if in DPA mode
2776	TCP, UDP	H.460.18 endpoint/ H.460.18 client gatekeeper	Enables H.460.18 Call Signaling, H.460.19 Multiplex Media Channel	Firewall traversal function based on H.460.18 and H.460.19 cannot function.	Mandatory for H.460 endpoints

Table continues…

Port Range	Protocol	Source	Functionality	Result of Blocking Port	Required
2777	TCP, UDP	H.460.18 endpoint/ H.460.18 client gatekeeper	Enables H.460.18 and H.460.19 Call Control, H.460.19 Multiplex Media Control Channel	H.460.18 endpoints cannot set up Call Control channels or logical channels. Firewall traversal function based on H.460.18 and H.460.19 cannot function.	Mandatory for H.460 endpoints
3089	TCP, UDP	Equinox H.323 Edge Client	Enables signaling and media traversal	If the TCP port is blocked, Equinox H.323 Edge Client cannot connect to Equinox H.323 Edge. Legacy H.323 endpoints behind the Equinox H.323 Edge Client cannot call external endpoints. If the UDP port is blocked, Equinox H.323 Edge Client can only traverse media via TCP.	Mandatory if using Equinox H.323 Edge Client
4000-5000	TCP, UDP	Any H.323 device using Q.931 signaling in DPA mode	Enables Direct Public Access (DPA) for H.323 call signaling, control and media traversal	Cannot setup/ connect DPA mode calls	Mandatory if in DPA mode To limit range, see Configuring the TCP/UDP port range for H.323 Direct Public Access calls on page 354
8089	XML (TCP)	XML API Client	Enables managing Equinox H.323 Edge via XML API	The External Management System cannot get Equinox H.323 Edge status or receive traps from Equinox H.323 Edge	Optional

Table 52: Bidirectional Ports to Open on the Equinox H.323 Edge Client

Port Range	Protocol	Source	Functionality	Result of Blocking Port	Required
3478	STUN (UDP)	STUN server	Enables an endpoint located in the remote network to send a STUN Binding Request when connecting to another endpoint in the same network	Equinox H.323 Edge Client cannot determine its public IP address. Smart Direct Media Connect cannot function.	Recommended

Important:

If there is a firewall between the H.323 client and the Equinox H.323 Edge Client, all high ports must be opened in both directions (1024-65535). We therefore recommend no firewall between the endpoint and the Equinox H.323 Edge Client.

Equinox H.323 Edge virtual server deployment

Downloading software from PLDS

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon ( ) for Company Name.
6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type `Avaya` or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
   - In **Download Pub ID**, type the download pub ID.
   - In the **Application** field, click the application name.

8. Click **Search Downloads**.
9. Scroll down to the entry for the download file, and click the **Download** link.
10. Select a location where you want to save the file, and click **Save**.
11. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.
12. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Deploying the Equinox H.323 Edge virtual server

About this task

The Equinox H.323 Edge virtual server software for VMware is available in the .OVA package format. You can install the OVA file using vSphere Client. The virtual server configuration file and virtual disk files are stored on a data store. The data store can be local to the host or a mounted shared storage, such as NFS or SAN.

If multiple virtual machine networks are configured on the host ESXi server, you must associate networks specified in the OVA with networks available on the host.

Procedure

1. Log in to vSphere Client.
2. Select the host ESXi server to deploy the Equinox H.323 Edge virtual server.

   If you do not choose a host before deploying the OVA, vSphere Client prompts you for the host or cluster name to deploy the virtual server.
3. Click **File** > **Deploy OVF Template**.
4. Do one of the following:
   - Click **Browse** and provide the Equinox H.323 Edge OVA file location.
   - In the **Deploy from a file or URL** field, enter the full URL of the HTTP server where the Equinox H.323 Edge OVA file is located.
5. Click **Next** to display the OVF Template Details window.
6. Verify the details of the OVA template, and click **Next**.
7. Read the license agreement, and click **Accept**.
8. Click **Next**.
9. In the **Name** field, enter the name of the new virtual server.
10. Click **Next** to display the Disk Format window.
11. Select **Thick Provision Eager Zeroed**.

12. Click **Next** to display the Network Mapping window.
13. Map the networks in the OVF to the networks in the inventory.
14. Click **Next** to display the Ready to Complete window.
15. Verify the deployment settings.

    If you need to modify any of the settings, use the **Back** option.
16. Click **Finish**.

Result

1. vSphere Client starts the Equinox H.323 Edge virtual server deployment.
2. After completing the deployment, in the Recent Tasks window, vSphere Client updates the status of the **Deploy OVT Template** task to **Completed**.

Starting the Equinox H.323 Edge virtual server

Before you begin

Deploy the Equinox H.323 Edge virtual server.

Procedure

1. Log in to vSphere Client.
2. Click **Inventory**.
3. Click **Virtual Machine** > **Power** > **Power On**.

   The Equinox H.323 Edge virtual server starts.

Configuring the virtual machine automatic startup settings

About this task

When a vSphere ESXi host restarts after a power failure, the virtual machines that are deployed on the host do not start automatically. You must configure the virtual machines to start automatically.

In high availability (HA) clusters, the VMware HA software ignores the startup selections.

Before you begin

Verify with the system administrator that you have the proper level of permissions to configure the automatic startup settings.

Procedure

1. In the vSphere Client inventory, select the host where the virtual machine is located.
2. Click the **Configuration** tab.

3. In the **Software** section, click **Virtual Machine Startup/Shutdown**.
4. Click **Properties** in the upper-right corner of the screen.
5. In the **System Settings** section, select **Allow virtual machines to start and stop automatically with the system**.
6. In the **Manual Startup** section, select the virtual machine.
7. Use the **Move up** button to move the virtual machine to the **Automatic Startup** section.
8. Click **OK**.

Equinox H.323 Edge initial configuration

Adding networks to Avaya Equinox® H.323 Edge

About this task

Add more networks to Avaya Equinox® H.323 Edge to configure separate IP interfaces for the external and internal networks. You can also use this procedure to configure separate subnets for different networks.

This procedure is relevant only if you have a dual NIC deployment of Avaya Equinox® H.323 Edge.

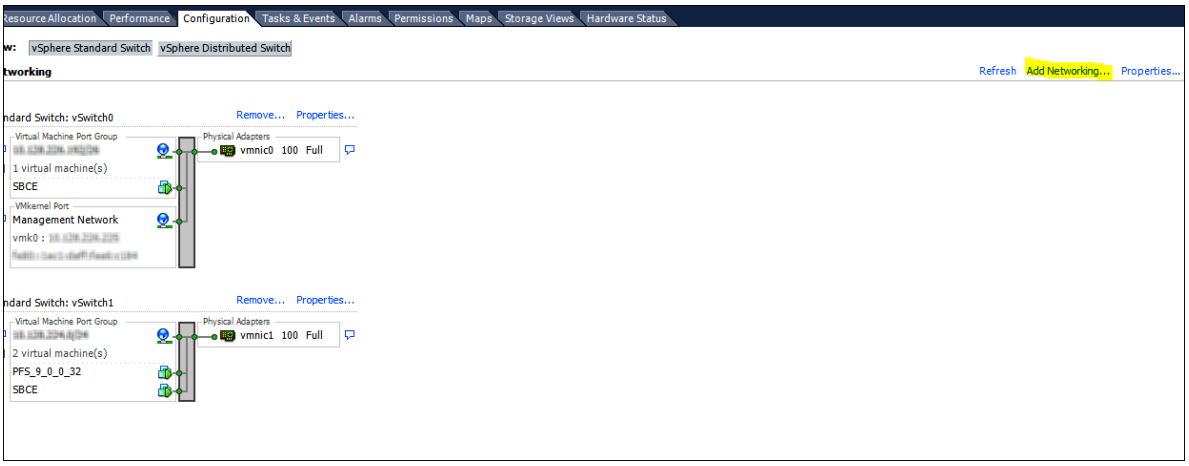
Before you begin

Connect a network cable to the second NIC of the host server.

Procedure

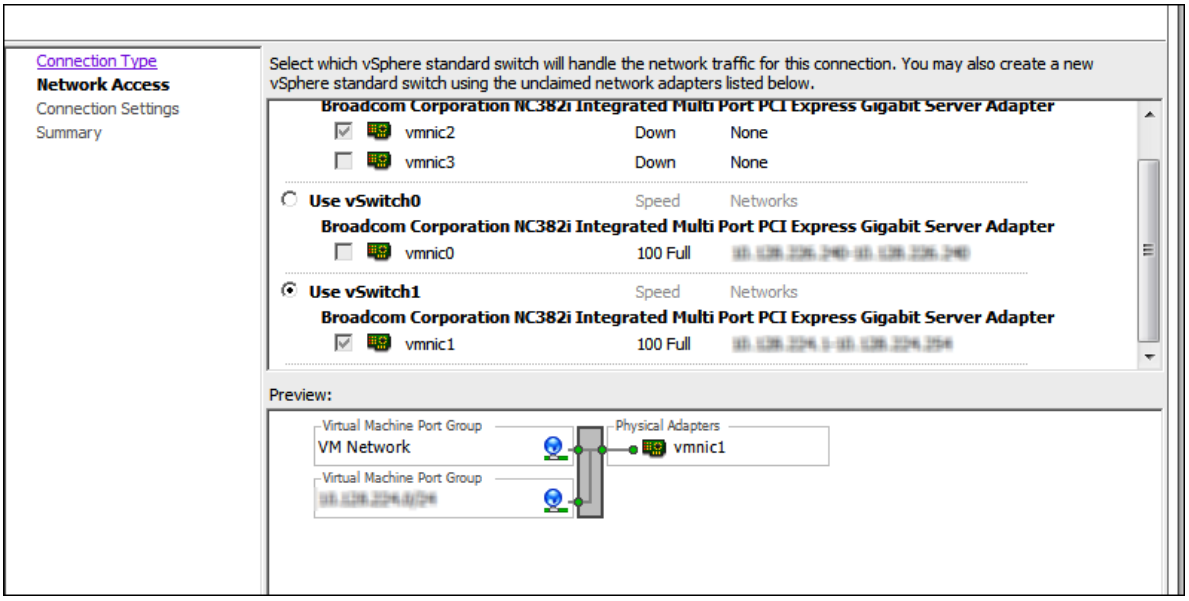
1. Log in to vSphere Client.
2. In the vSphere Client inventory, select the host where you deployed Avaya Equinox® H.323 Edge.
3. Click the **Configuration** tab.
4. In the **Hardware** section, click **Networking** .

5. Click **Add Networking...**.



VSphere Client displays the Add Networking Wizard window.

6. In **Connection Type**, select **Virtual Machine**, and click **Next**.
7. In **Network Access**, select the vSwitch corresponding to the second NIC of the host server, and click **Next**.



8. In **Connection Settings**, configure the following fields:
   - **Network Label**
   - **VLAN ID (Optional)**: If you do not have a VLAN ID, select **None**.
9. Click **Next**.
10. In **Summary**, verify the configuration, and click **Finish**.

Result

vSphere Client adds another network to the host server.

Next steps

1. Add the Avaya Equinox® H.323 Edge instance in Avaya Equinox® Management for the eth0 interface.
2. Configure separate IP interfaces for the external and internal traffic in Avaya Equinox® Management.

Adding Equinox H.323 Edge in Equinox Management

About this task

Manage Equinox H.323 Edge using Equinox Management.

Before you begin

Get the IP address of the Equinox H.323 Edge eth0 interface.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**.
3. Click **H.323 Edge Servers** in the left pane.

   Equinox Management displays the Equinox H.323 Edge server window.
4. Click **Add**.

   Equinox Management displays the Add Equinox H.323 Edge server window.
5. Configure the following fields:
   - **Name**
   - **IP Address**
6. Click **OK**.

Result

Equinox Management adds the Equinox H.323 Edge instance as a device.

Configuring a second IP interface in Avaya Equinox® H.323 Edge for external traffic

About this task

Configure a different IP address and subnet for the second virtual NIC of Avaya Equinox® H.323 Edge to process the external traffic.

This procedure does not describe the steps to configure IP separation of the signaling and media traffic.

Before you begin

Configure vSwitches in vSphere Client.

Procedure

1. Log in to Avaya Equinox® Management.
2. Click **Devices**, and select the Avaya Equinox® H.323 Edge instance.

   Avaya Equinox® Management opens the Avaya Equinox® H.323 Edge instance window.
3. Click the **Configuration** tab.
4. In the **Network Settings** section, click **NIC Settings**.

   Avaya Equinox® Management displays the NIC Settings window.
5. Configure the following:

Internal NIC	External NIC
IP Address: The IP address of the eth0 interface.	**External NIC**: Select to enable dual NIC.
Subnet Mask	**IP Address**: The IP address of the eth1 interface.
Gateway	**Subnet Mask**
Local FQDN	**Gateway**

6. Click **OK**.

Result

Avaya Equinox® Management enables dedicated NICs for the external and internal network traffic.

Next steps

In a dual NIC configuration, the internal NIC can connect only to its subnet. You must configure static routes between the internal NIC and other subnets.

Configuring static routes for Avaya Equinox® H.323 Edge

About this task

Configure static routes between the internal NIC of Avaya Equinox® H.323 Edge and the internal network subnets. For example, configure a static route between Avaya Equinox® H.323 Edge and Avaya Equinox® Media Server.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Equinox H.323 Edge instance.

Equinox Management opens the Equinox H.323 Edge instance window.

3. Click the **Configuration** tab.
4. Click **Static Routes**.
5. Click **Add**, and configure the following fields:
   - **Address of network**
   - **Gateway**
6. Click **OK**.

Configuring Ports on the Equinox H.323 Edge server

This section provides instructions of how to configure the following ports and port ranges on the Avaya Equinox® H.323 Edge server:

Related links

Configuring the TCP/UDP port range for H.323 Direct Public Access calls on page 354
Configuring the TCP/UDP port range on the internal interface on page 355

Configuring the TCP/UDP port range for H.323 Direct Public Access calls

About this task

Equinox H.323 Edge has a port range of 4000 to 5000 ports designated for H.323 Direct Public Access. Using H.323 Direct Public Access, non-H.460 public endpoints can call internal endpoints without being registered to Equinox H.323 Edge. To add more security to your firewall, you can limit the port range for H.323 Direct Public Access.

If the external NIC of Equinox H.323 Edge is protected by a firewall, you must give the following ports access to the firewall:

- The TCP/UDP port range you configure
- Port 1720 for H.323-based signaling

To calculate the number of ports Equinox H.323 Edge uses, multiply the number of simultaneous Direct Public Access calls by 10. The multiplication factor is lower for audio-only calls and higher for calls with dual video. Use 10 as an approximate multiplication factor.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Equinox H.323 Edge instance.
3. Click **Configuration**.
4. In **Direct Public Access**, select **Enabled**.

5. Type the values in the following fields:
   - **Default Extension**: The extension configured for the media server IVR. Equinox H.323 Edge redirects the calls from endpoints that contain only the IP address of the server to the default extension.
   - **Port Range Minimum Port**: The range of ports for direct H.323-based calls.
   - **Port Range Maximum Port**
6. Click **Apply**.

   Equinox Management displays a confirmation message.
7. Click **Yes**.

Related links

Configuring Ports on the Equinox H.323 Edge server on page 354

Configuring the TCP/UDP port range on the internal interface

About this task

Equinox H.323 Edge has a port range of 12000 to 15000 ports designated for H.323–based calls to the internal interface. To add more security to your firewall, you can limit the port range for H.323 calls.

To calculate the number of ports Equinox H.323 Edge uses, add the two figures that you get by the following methods:

- Multiply the number of simultaneous H.323 calls by 10.

  The multiplication factor is lower for audio-only calls and higher for calls with dual video. Use 10 as an approximate multiplication factor.
- Count one port for each endpoint registration.

  For example, if you have 100 endpoints, count 100 ports.

You must restart Equinox H.323 Edge after you modify the port range.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Equinox H.323 Edge instance.
3. Click **Configuration**.
4. In **Internal Communication**, change the port range in the following fields:
   - **Internal Port Range Minimum Port**
   - **Internal Port Range Maximum Port**

   Select a port range between 12000 to 15000. The maximum port range is from 9000 to 65535. The port range requires a minimum range of 300 ports.
5. Click **Apply**.

   Equinox Management displays a confirmation message.

6. Click **Yes**.

Next steps

Restart Equinox H.323 Edge

Related links

Configuring Ports on the Equinox H.323 Edge server on page 354

Integrating the Equinox H.323 Edge server with Other Equinox Solution Components

Your Avaya Equinox® H.323 Edge server is part of the Equinox Solution and must be integrated with other components:

Related links

Integrating Equinox H.323 Edge with H.323 Gatekeeper on page 356
Integrating Equinox H.323 Edge with NAT on page 357

Integrating Equinox H.323 Edge with H.323 Gatekeeper

About this task

The integration of Equinox H.323 Edge and H.323 Gatekeeper supports the communication between endpoints from external networks and endpoints in the internal network. You need to configure the IP address of H.323 Gatekeeper in Equinox H.323 Edge.

The external endpoints can be endpoints that are compliant with H.323 and H.460. Conference participants dial in to call using IP addresses, URI, or the E.164 number.

For example, dialing in to conferences using URI involves the gatekeeper resolving the host name, such as name@company.com or number@company.com, with the IP address of the endpoint being used. When the URI address contains a destination to an external network, Equinox H.323 Edge and H.323 Gatekeeper work together to resolve the URI address.

Before you begin

Get the IP address of the H.323 Gatekeeper.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select Equinox H.323 Edge instance.
3. Click the **Configuration** tab.
4. In the **Gatekeeper Settings** section, enter gatekeeper address and port in the following fields:
   - **Gatekeeper Address**
   - **Gatekeeper Port**

Related links

Integrating the Equinox H.323 Edge server with Other Equinox Solution Components on page 356

Integrating Equinox H.323 Edge with NAT

About this task

If the external NIC of Equinox H.323 Edge uses a private IP address to communicate with endpoints in external networks, enable NAT traversal.

Do not enable NAT traversal if the external NIC communicates with the Internet by using a public IP address.

Before you begin

Get the NAT traversal IP address.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Equinox H.323 Edge instance.

   Equinox Management opens the Equinox H.323 Edge instance window.
3. Click the **Configuration** tab.
4. Click **Basic Settings**.
5. In the **NAT Support** section, do the following:
   a. Select **Enabled**.
   b. Enter the IP address in **Public IP Address**.

Next steps

In the firewall or NAT device, verify that the NAT address is mapped to the private IP address of the external NIC of Equinox H.323 Edge.

Related links

Integrating the Equinox H.323 Edge server with Other Equinox Solution Components on page 356

Configuring the NTP server

Before you begin

Get the IP address of the NTP server.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Equinox H.323 Edge instance.

   Equinox Management opens the Equinox H.323 Edge instance window.
3. Click the **Configuration** tab.
4. Click **Network Settings**.

5. In **NTP Settings** section, do the following:
   a. **NTP Server Address**: Type the IP address of the NTP server.
   b. **Time Zone**: Select the time zone.
6. Click **Apply**.

Calls between internal and external endpoints

Calls between internal endpoints of enterprises and external endpoints are established using the IP address or URI of external endpoints. The call establishment using IP addresses and URI involves the following sequence:

1. Dialing and connecting to external endpoints
2. Entering the pound (#) symbol
3. Entering the meeting ID

If external endpoints are registered to Equinox H.323 Edge, calls to the endpoints can also be established using the E.164 number. Usually, external endpoints are not registered in the gatekeeper, so the gatekeeper must forward call requests to external endpoints in other networks to Equinox H.323 Edge to process and establish the call.

You must configure Equinox H.323 Edge and H.323 Gatekeeper to support IP-based and URI-based dialing.

Related links

Configuring access for calls to H.323 video endpoints on page 358
URI-based dialing on page 359
Configuring URI-based dialing to external endpoints on page 360
Configuring IP address-based dialing to external endpoints on page 363

Configuring access for calls to H.323 video endpoints

About this task

Direct Public Access supports a direct connection to Equinox H.323 Edge for calls to external endpoints. To set up this connection, you need to configure:

- Equinox H.323 Edge to process H.323–based calls.
- H.323 Gatekeeper as a neighbor of Equinox H.323 Edge to process the routing of the calls.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Equinox H.323 Edge instance.
3. Click the **Configuration** tab.
4. In the **Direct Public Access** section, select **Enabled**.

5. Enter the direct line extension number and the port range in the following fields:
   - **Default Extension**: The default extension configured in the MCU IVR. Equinox H.323 Edge redirects a call to the default extension when the endpoint dials only the server's IP address without any extension.
   - **Port Range Minimum Port**: Define the range of ports used for direct H.323 calls in the field. If the external NIC of the Equinox H.323 Edge server is located behind a firewall, the defined port range and port 1720 for H.323 signaling must also be opened in the firewall.
   - **Port Range Maximum Port**
6. Click **Apply**.

   Equinox Management displays a confirmation message.
7. Click **Yes**.
8. Click **Settings**.
9. On the left pane, under **System Preferences**, click **Local Services**.

   Equinox Management displays the Local Services page.
10. Click **H.323 Gatekeeper**.

    Equinox Management displays the internal H.323 gatekeeper page.
11. Click **Route IP calls**.
12. Select **Route IP calls to H.323 Edge Server**, and click **Add**.

    Equinox Management displays the Add IP Calls window.
13. Configure the following fields:
    - **IP Address**
    - **Port**

    The value of these fields must match the IP address and port number in **Public Access Proxy Address** on the **Info** tab of the Equinox H.323 Edge instance window.
14. Click **OK**.
15. Click **Apply**.

Result

- Equinox H.323 Edge is configured to directly process all H.323–based calls.
- Equinox Management adds Equinox H.323 Edge as a neighbor of the internal gatekeeper.

Related links

Calls between internal and external endpoints on page 358

URI-based dialing

The Avaya Equinox® solution supports URI-based dialing, which is a dialing format to make and receive calls from external endpoints.

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.

All Avaya Equinox® solution endpoints work transparently with URI-based dialing, including the Avaya Room System XT Series. You can also perform URI-based dialing from the conference control feature of Avaya Equinox® Management.

Avaya Equinox® H.323 Edge supports URI-based dialing for H.323–based endpoints. Outgoing and incoming calls to and from external endpoints traverse through the enterprise firewall.

DNS configuration to allow inbound DNS-based URI calls

Configure DNS to ensure that calls to your enterprise can be dialed using the shortest possible name. Use SRV records under the host name record to configure services under the same domain as the host. You can also map the SRV records to sub-domains.

Create the following two new resource records and map them with the same domain to allow inbound DNS-based URI calls to your enterprise:

- A resource record called the Host (A or AAAA) record for the enterprise host address.
- Service records called SRV records for the H.323 services in the following format:

```
<_service name._protocol name.domain name>    <class>        <type>
<priority>        <weight>        <port number>        <target host name>
```

Create the following SRV records for Avaya Equinox® H.323 Edge:

Descriptive name of service	Service, Protocol and Domain name	Class	Type	Priority	Weight	Port number	Target host name
Call Signaling	_h323cs._tcp.company.com	IN	SRV	0	0	1720	pfs.company.com
Location Service	_h323ls._udp.company.com	IN	SRV	0	0	1719	pfs.company.com
Registration Service	_h323rs._udp.company.com	IN	SRV	0	0	1719	pfs.company.com

Related links

Calls between internal and external endpoints on page 358

Configuring URI-based dialing to external endpoints

About this task

Callers can establish calls to endpoints using the IP address, URI, or the E.164 number of endpoints. Configure Equinox H.323 Edge to accept H.323-based calls and forward the calls. Configure the internal gatekeeper of Equinox Management to define the Equinox H.323 Edge instances as neighbors of the internal gatekeeper, which establishes routes for the H.323-based calls.

The internal gatekeeper of Equinox Management forwards URI-based calls from internal to external endpoints in another enterprise through Equinox H.323 Edge. The internal gatekeeper must also forward the URI-based calls from external endpoints through Equinox H.323 Edge because external endpoints are not registered to the internal gatekeeper. The external endpoints can be H.323-based and H.460-based.

If the enterprise deployment has multiple Equinox H.323 Edge instances, which includes several servers deployed as one server behind a load balancer, perform this procedure for each Equinox H.323 Edge instance.

Before you begin

- Configure Direct Public Access on Equinox H.323 Edge for calls to H.323–based endpoints. Using Direct Public Access, internal endpoints can call external H.323–based endpoints that do not support H.460.

  If you are configuring multiple Avaya Equinox® H.323 Edges, with or without a load balancer, do this for each Avaya Equinox® H.323 Edge.
- Integrate Equinox H.323 Edge with the H.323 gatekeeper to enable communication between external and internal endpoints.
- Get the IP address of the Equinox H.323 Edge internal NIC.

  If you are configuring multiple Avaya Equinox® H.323 Edges, with or without a load balancer, do this for each Avaya Equinox® H.323 Edge.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Equinox H.323 Edge instance.

   Equinox Management opens the Equinox H.323 Edge instance window.
3. On the **Info** tab, note the IP address and port number in **Public Access Proxy Address**.
4. Click the **Configuration** tab.
5. Configure the following fields in the **URI Dialing Settings** section:
   - **Local Domain Name**: Enter the public FQDN of Avaya Equinox® H.323 Edge.
   - **Strip Domain Name**: Select the check box.
6. Click **Settings**.
7. On the left pane, under **System Preferences**, click **Local Services**.

   Equinox Management displays the Local Services page.
8. Click **H.323 Gatekeeper**.

   Equinox Management displays the internal H.323 gatekeeper page.
9. Click **Neighbors** > **Add**.

   Equinox Management displays the Add Neighbors window.

10. Configure the following fields:
    - **Prefix**: Keep this field empty.
    - **IP Address**: The IP address of the internal NIC of Equinox H.323 Edge.
    - **Port**: 1719
    - **Description**
11. Click **OK**.
12. Click **Apply**.

Result

- Equinox H.323 Edge is configured to support URI-based dialing.
- Equinox Management adds Equinox H.323 Edge as a neighbor of the internal gatekeeper.

Related links

Calls between internal and external endpoints on page 358

Configuration field descriptions

Name	Description
Local Domain Name	The domain name of the enterprise where Equinox H.323 Edge is physically located.
Strip Domain Name	The option to strip the domain name and IP address from the dialed string before transferring the signaling message to the main gatekeeper. This setting optimizes the processing of call transfers. Do not select this option if the enterprise has a policy of transferring messages by using the complete dial string of endpoints. For example, 1234@5.6.7.8, instead of the 1234 alias.

Add Neighbors field descriptions

Name	Description
Prefix	The local zone prefix of the gatekeeper. Do not configure this field. URI-based dialing does not establish call routes to zones using dial prefixes. URI-based dialing establishes call routes using the domain name in the URI string, which is resolved to all zone worldwide.
Description	The name of Equinox H.323 Edge.
IP Address	The IP address of the Equinox H.323 Edge internal NIC, which is connected to the internal network.

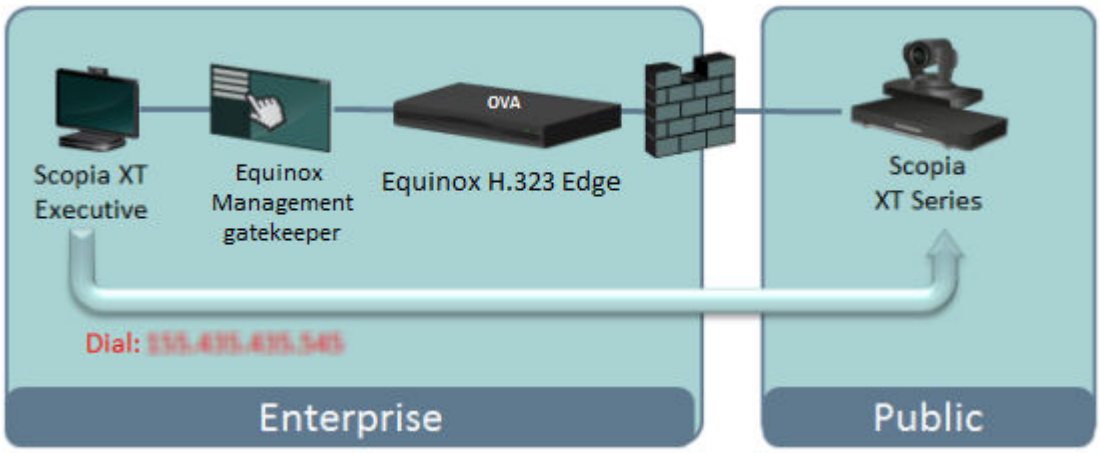
Table continues…

Name	Description
Port	The port for URI-based calls. The default 1719 port is mandatory for URI-based dialing.

Configuring IP address-based dialing to external endpoints

About this task

Callers can establish calls to endpoints using the IP address, URI, or the E.164 number of endpoints. Configure the internal gatekeeper of Equinox Management to forward IP address-based calls from internal endpoints to external endpoints through Equinox H.323 Edge. The internal gatekeeper must forward the IP address-based calls from external endpoints through Equinox H.323 Edge because external endpoints are not registered to the internal gatekeeper.



If the enterprise deployment has multiple Equinox H.323 Edge instances, which includes several servers deployed as one server behind a load balancer, perform this procedure for each Equinox H.323 Edge instance.

Before you begin

- Get the IP address of the Equinox H.323 Edge internal NIC.

  If you are configuring multiple Avaya Equinox® H.323 Edges, with or without a load balancer, do this for each Avaya Equinox® H.323 Edge.
- Get the Direct Public Access address of Equinox H.323 Edge.

  If you are configuring multiple Avaya Equinox® H.323 Edges, with or without a load balancer, do this for each Avaya Equinox® H.323 Edge.
- Configure Direct Public Access on Equinox H.323 Edge for calls to external endpoints. Using Direct Public Access, internal endpoints can call external endpoints that do not support H.460.

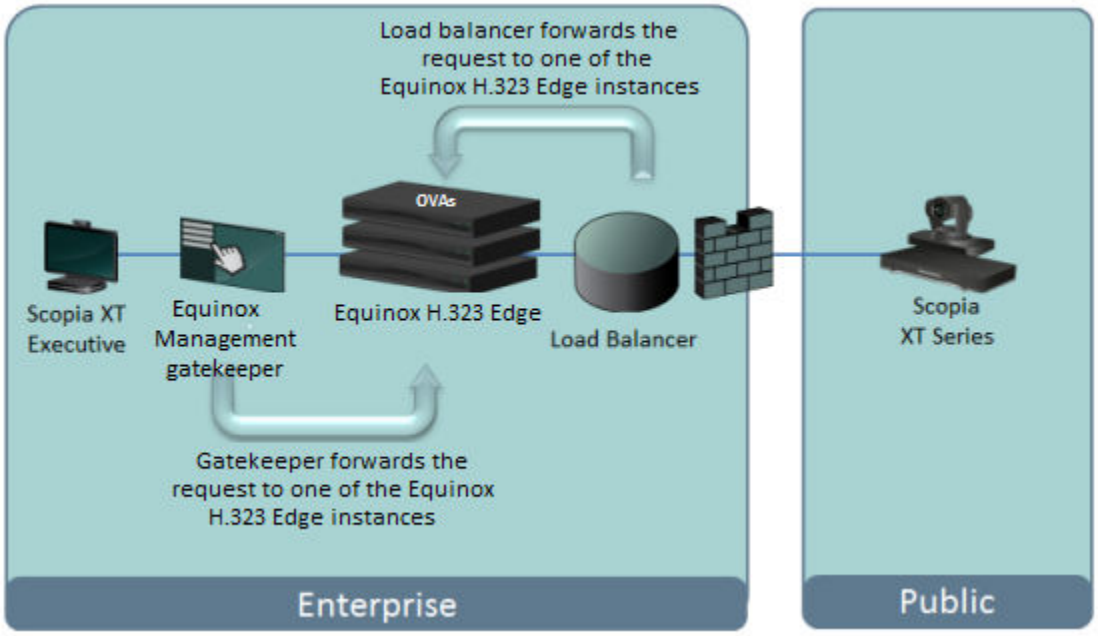
  If you are configuring multiple Avaya Equinox® H.323 Edges, with or without a load balancer, do this for each Avaya Equinox® H.323 Edge.
- If the enterprise deployment has multiple Equinox H.323 Edge instances, verify that the correct redundancy policy is configured between the internal gatekeeper of Equinox Management and each Equinox H.323 Edge instance.

The internal gatekeeper of Equinox Management has its own load balancing method to work with multiple Equinox H.323 Edge instances for outgoing calls from internal endpoints to external endpoints. By default, the internal gatekeeper is configured to the Scalability policy, which enables the internal gatekeeper to send requests to each Equinox H.323 Edge instance using the round robin method.

You can also configure the internal gatekeeper of Equinox Management to work with the Priority policy where the internal gatekeeper can establish the route of the call to the first Equinox H.323 Edge instance in the list and send the call to the next Equinox H.323 Edge instance if the first Equinox H.323 Edge instance fails. Contact Customer Support to configure the Equinox H.323 Edge redundancy policy.

Note:

The Equinox H.323 Edge redundancy policy configuration is different from the redundancy policy for the load balancer, which instructs it how to direct incoming traffic from the external network to the internal network.



Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Equinox H.323 Edge instance.

   Equinox Management opens the Equinox H.323 Edge instance window.
3. On the **Info** tab, note the IP address and port number in **Public Access Proxy Address**.
4. Click **Settings**.
5. On the left pane, under **System Preferences**, click **Local Services**.

   Equinox Management displays the Local Services page.
6. Click **H.323 Gatekeeper**.

Equinox Management displays the internal H.323 gatekeeper page.

7. Click **Route IP calls**.
8. Select **Route IP calls to H.323 Edge Server**, and click **Add**.

   Equinox Management displays the Add IP Calls window.
9. Configure the following fields:
   - **IP Address**
   - **Port**

   The value of these fields must match the IP address and port number in **Public Access Proxy Address** on the **Info** tab of the Equinox H.323 Edge instance window.
10. Click **OK**.

Result

The internal gatekeeper of Equinox Management forwards all IP address-based calls from external endpoints through Equinox H.323 Edge.

Related links

Calls between internal and external endpoints on page 358

Add IP Calls field descriptions

Name	Description
IP Address	The IP address in the **Public Access Proxy** Address field on the **Info** tab of the Equinox H.323 Edge instance. Equinox H.323 Edge automatically creates the IP address when you enable Direct Public Address.
Port	The port number in the **Public Access Proxy** Address field on the **Info** tab of the Equinox H.323 Edge instance.

Secure connection with Equinox Management

Creating security certificates

About this task

TLS certificates, issued by a trusted certification authority, contain the public encryption keys of Equinox H.323 Edge that are used over the network to ensure authentication and encryption of the network connection.

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. Log in to Equinox Management.
2. Click **Devices**, and click the name of the Equinox H.323 Edge instance.

   Equinox Management displays the Equinox H.323 Edge instance window.
3. Click the **Certificate** tab.
4. Click **Create**.

   Equinox Management displays the Generate CSR window.
5. Configure the following fields:
   - **Common name**
   - **Organizational Unit**
   - **Organization**
   - **City**
   - **State**
   - **Country Code**
   - **Encryption Strategy**
   - **Signature Algorithm**
6. Click **Generate CSR**.
7. Click **Save** to view the certificate.

   Equinox Management displays the certificate in the Download window.
8. Save the certificate.

   Equinox Management saves the certificate as a CSR file that is compatible with the Base-64 ASCII code.
9. Send the CSR file containing the certificate to the certification authority for signing.

   Select **Web Server** as the certificate template when you submit the certificate request.

Result

The certification authority will send back a signed certificate.

Next steps

Upload the certificates.

Generate CSR field descriptions

Name	Description
Common Name	The Equinox H.323 Edge FQDN. For a redundant deployment, the common name must be the public virtual FQDN.
Country Code	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	The code for the encryption strategy. The options are: • **1024** • **2048** • **4096**
Signature Algorithm	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. The options are: • **SHA1withRSA** • **SHA256withRSA**

Uploading security certificates

About this task

TLS certificates from the certification authority must be uploaded to Equinox H.323 Edge to ensure authentication and encryption of the network connection.

If Equinox Management is configured as the certificate authority, Equinox Management automatically generates a self-signed certificate to upload to Equinox H.323 Edge when the connection between Equinox Management and Equinox H.323 Edge establishes. You can replace the Equinox Management self-signed certificate.

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

Generate the certificates.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and click the name of the Equinox H.323 Edge instance.

Equinox Management displays the Equinox H.323 Edge instance window.

3. Click the **Certificate** tab.
4. Click **Upload**.

   Equinox Management displays the Upload certificates window.
5. Click **Add**, and browse to the certificates.

   Repeat this step for all certificates.

   Equinox Management displays a confirmation message after each certificate is uploaded.
6. Click **Apply All**.

Result

Equinox Management uploads the security certificate to Equinox H.323 Edge.

Next steps

1. Restart Equinox H.323 Edge.
2. Enable the secure connection between Equinox H.323 Edge and Equinox Management.

Securing the connection with Equinox Management using TLS

Before you begin

Upload the security certificates.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and click the name of the Equinox H.323 Edge instance.

   Equinox Management displays the Equinox H.323 Edge instance window.
3. Click the **Configuration** tab.
4. Click **Network Settings**.
5. Select **Secure Connection**,

Result

The connection between Equinox H.323 Edge and Equinox Management is secured using TLS.

Configuring remote access

About this task

Configure remote access to Equinox H.323 Edge. You can use these remote access logins to administer Equinox H.323 Edge using Equinox Management.

Before you begin

To enable a secure connection between Equinox H.323 Edge and Equinox Management, configure the security certificates in the **Certificate** tab.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Equinox H.323 Edge instance.

   Equinox Management displays the Equinox H.323 Edge instance page.
3. Click the **Access** tab.
4. Configure the following settings:
   - **Username**: The user name of the administrator.
   - **Password**: The password of the administrator.
5. Click **Apply**.

Access field descriptions

Name	Description
Username	The user name of the administrator. You can change the user name.
Password	The password of the administrator. The password must match the password configured for the administrator in Equinox H.323 Edge. You can change the password.

Configuring QoS for audio and video

About this task

Quality of Service helps solve network performance issues by assigning relative priorities to the following packets:

- Audio, which is one of the media sent during a call. For example, by assigning high priority to audio under poor network conditions with high packet loss, you determine that audio is the most important element of the videoconference to be maintained at the expense of better video quality. Audio is transmitted via the RTP and RTCP protocols in H.323 calls.

  Video, which includes shared data stream like a presentation, also known as dual video. Far end camera control (FECC) is another example of information carried on the data stream. Video is transmitted via the RTP and RTCP protocols in H.323 calls.

Control, which includes signaling and media control.

- Signaling 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. Signaling occurs before the control aspect of call setup.
- 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. Control occurs within the framework of an established call, after signaling.

During low-bandwidth conditions, Equinox Management uses these priority settings to adjust the quality of the meeting. Follow this procedure to determine the relative priorities for audio, video, and control transmitted via Equinox H.323 Edge.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and click the Equinox H.323 Edge instance.

   Equinox Management displays the Equinox H.323 Edge instance page.
3. Click **Configuration** > **Advanced Parameters**.

   Equinox Management displays the Advanced Parameters window.
4. Select **Options of QoS Settings**, and set the value to one of the following settings:

Field	Description
None	Select this setting when the network has sufficient bandwidth for each stream (audio, video, and media control) and does not require any prioritization of the different streams.
Default	Select this setting to use the following default priority values for each stream: • **48** for the media **Control** stream. This highest priority ensures that calls are set up properly even if it means that other calls ongoing may reduce their video or audio during a call setup. All TCP connections use the QoS value set in this field. • **46** for the **Audio** stream. This priority ensures that audio is always given precedence over video. This audio applies to multiple video channels (e.g., sound stream for endpoint microphones and presentations). • **34** for the **Video** stream. The lowest default priority is given to video image quality. It applies to endpoint camera images and also covers data streams like far end camera control.

Table continues…

Field	Description
Customized	The QoS options to configure the relative priority of the audio, video, and control channels. Use the following advanced parameters to set the priority of the audio, video, and control channels. The valid value range is from 0 to 255: • **QoS value for Audio Channel** • **QoS value for Video Channel** • **QoS value for Control Channel**

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.

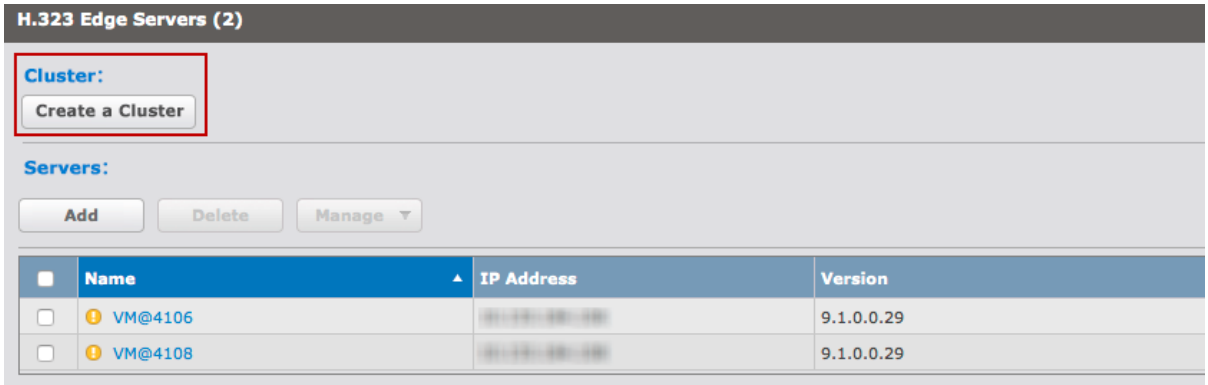
Before you begin

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

Procedure

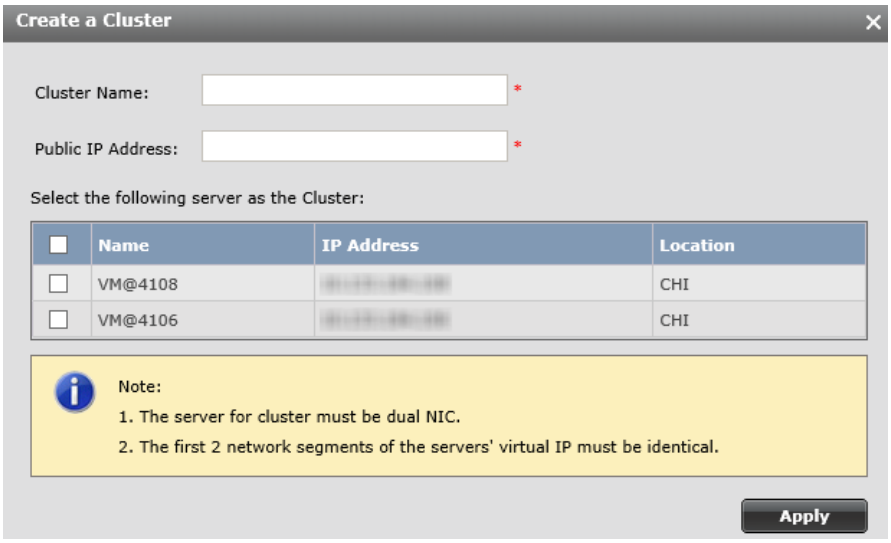
1. Access the Equinox Management administrator portal.
2. Click **Devices** > **Devices by Type** > **Media & Signaling** > **H.323 Edge Servers**.

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



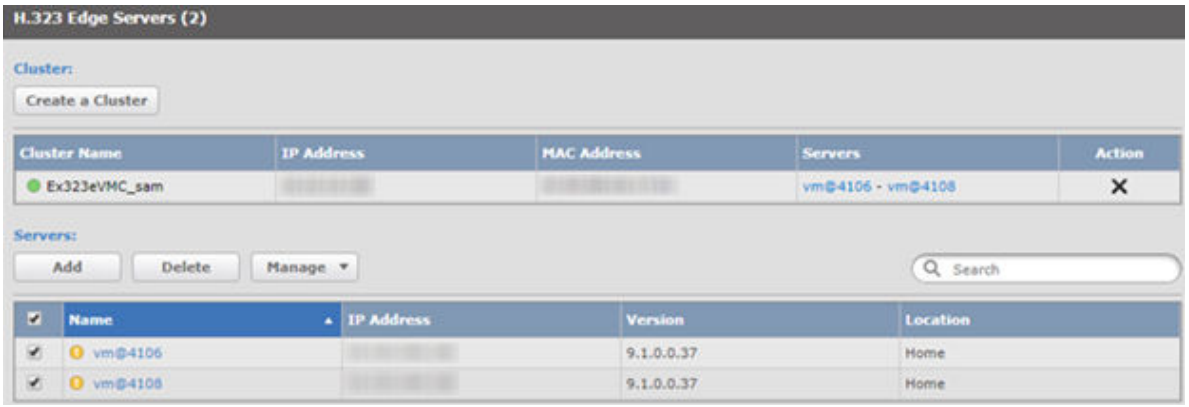
3. Click **Create a Cluster**.

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.

Chapter 14: Avaya Equinox Streaming and Recording deployment

Introducing Avaya Equinox Streaming and Recording

Avaya Equinox® Streaming and Recording Server

For the streaming and recording of conferences, Avaya has developed the Avaya Equinox® Streaming and Recording Server (Equinox Streaming and Recording). Equinox Streaming and Recording is the Avaya platform for HD streaming and recording.

Before you install Equinox Streaming and Recording, you must make a number of decisions in order to ensure that the solution exactly matches the requirements of your deployment. For example, you must make a decision about scalability in accordance with the size of your enterprise. For a small enterprise, you can choose a single appliance which houses all of the Equinox Streaming and Recording components. For a large enterprise, you can choose a distributed solution with multiple media nodes. Equinox Streaming and Recording is highly flexible and easily adaptable, whatever your requirements. In addition, you must decide if you require a high degree of redundancy[1] and whether you would like to enable external access and storage in the 'cloud'. In both the Over The Top (OTT) and Team Engagement (TE) solutions, Equinox Streaming and Recording is optional, however if you want to record and playback videoconferences, you must install it.

If you would like users outside of the enterprise to access recordings, you can deploy Equinox Streaming and Recording in a Demilitarized Zone (DMZ) or use a reverse proxy server. In this way, the Equinox Streaming and Recording is similar to the Avaya Web Collaboration server (WCS). If you would like users outside of the enterprise to access the videoconference, you must deploy the WCS in a DMZ or use a reverse proxy server. Equinox Streaming and Recording and WCS also support a Network Address Translation NAT Firewall configuration in a DMZ deployment. NAT Firewall is an additional layer of security. It blocks unrequested inbound traffic.

Components

The Avaya Equinox® Streaming and Recording Server consists of the following components:

- Equinox Streaming and Recording Conference Point™ (CP)
- Equinox Streaming and Recording Delivery Node™ (DN)

[1] High Availability is not supported for the Manager in this release. High Availability is not supported for All-in-one servers.

- Equinox Streaming and Recording Virtual Delivery Node™ (VDN)
- Equinox Streaming and Recording Manager™
- Equinox Recording Gateway™

Equinox Streaming and Recording Conference Point™

You must configure a conference point to capture H.323 video content and deliver live and on demand webcasting. The Equinox Streaming and Recording conference point includes an embedded transcoder to convert H.323 calls into .MP4 format.

Each conference point must be associated with a delivery node. A delivery node streams and optionally archives the content captured by the conference point and delivers it to client systems.

You can configure a conference point to be in a geographic location. This means that you can assign a location to one or more conference points which coincide with locations set for Scopia Elite MCUs and/or Equinox Media Servers in Equinox Management. When a program starts, Equinox Management includes the desired location, and a conference point close to the MCU/Media Server can be selected. If there are no conference points matching the location passed by Equinox Management, then any conference points without a location are treated as a single pool of conference points, and one of those is selected. If there are no conference points available, the call fails.

Each conference point has a limit to the number of simultaneous high definition or standard definition calls it can handle.

The CP includes the following features:

- Video conferencing H.323 capture and transcoding
- High definition support
- Scalability for up to 40 480p, or up to 60 360p recordings, or up to 75 audio-only recordings
- Scalability for up to 10 1080p recordings, or for up to 20 720p recordings
- G.711 and AAC-LC audio capture and transcoding
- H.263, H.263+, H.264 capture and transcoding

The media node or all-in-one server can include the CP and transcoder components. The H.323 video and audio and the optional H.239 stream received by the CP are sent to the internal encoder for transcoding into H.264/AAC MP4/MPEGTS/HLS formats.

- Operating Systems: The transcoder runs on the Windows Server 2012 R2 or Windows Server 2016 64-bit operating system with Hyper-V (an add-on to the Windows Server that allows a Linux operating system to run on the same server). The CP runs on the CentOS 6.6 64-bit operating system. Using virtualization software, this enables both applications to run two different operating systems on the same server.
- Licensing: The server requires a single media node license for the CP. The license defines the number of simultaneous H.323 connections. An H.323 connection includes audio, video, and an optional H.239 secondary stream.
- Transcoding H.323 audio and Video: The CP connects H.323 calls to the Scopia Elite MCUs (Multipoint Control Units) and/or Equinox Media Servers. When it establishes a video connection, the CP sends the audio and video data from the MCU/Media Server to the internal transcoder. The transcoder converts the data into a format that is suitable for streaming.

- Transcoding with H.239: H.239 is an ITU recommendation that allows for establishment of multiple channels within a single H.323 session. Existing videoconference equipment can be used to stream audio and video and a secondary channel can stream a slide presentation or another data stream to the viewers of a program. This function is typically used to stream slide presentations synchronized with live audio and video. If a program uses a secondary H.239 channel, the encoder inputs the second stream, decodes, scales and mixes it with the main video input for transcoding/streaming. The streams are then sent to the DN for delivery to the distribution network. The dual stream can also be recorded as a single MP4 program.
- High definition support: The CP supports high definition video and higher rate streaming quality and bandwidth. The CP supports the following ITU recommendations:
  - H.261 up to CIF Video
  - H.262 up to CIF video
  - H.263 up to CIF video
  - H.264 up to 1080p video
  - H.263+ up to 1024 x 768 H.239 data
  - H.264 up to 1080p H.239 data
  - G.711 audio
  - AAC-LC audio

  The CP negotiates up to H.264 Level 3.2 video at 1.92 Mbps, and accepts up to 1080p and down to H.261 QCIF along with G.711 or AAC-LC audio. The streaming resolution and bandwidth rate depend on what you select for the bitrate when creating the program and what the Scopia Elite MCU and/or Equinox Media Server negotiates.

For more information, see *Administrator Guide for Avaya Equinox® Streaming and Recording Server* which is available on https://support.avaya.com/.

Equinox Streaming and Recording Delivery Node™

The DN provides on-demand and broadcast video delivery. Used alone or in a hierarchy of devices, the DN supports thousands of concurrent streams. The DN uses intelligent routing, content caching, and inherent redundancy to ensure transparent delivery of high-quality video.

Delivery nodes (DN) store all content that is created by the conference point and deliver the content to client systems at playback time. You must associate the conference point with the delivery nodes.

A source DN is the original DN that receives a recording file from its associated conference point. A source DN sends the recording file to all of the other DNs in the network.

The Delivery Node Details dialog displays a list of recording files, known as **Source Programs** and **Distributed Programs**. Source programs are programs (recording files) for which this delivery node is the main source for storage. Distributed programs are programs which other delivery nodes have forwarded to this delivery node.

Equinox Streaming and Recording Virtual Delivery Node™ (VDN)

A virtual delivery node (VDN) delivers content to a global content delivery network (CDN) provider for cloud-based viewer playback. The appliance and the network of the CDN act as one delivery mechanism. Therefore, the VDN appliance and the CDN together create the Equinox Streaming and Recording VDN solution.

Upon program creation, the publisher includes the options of distributing the program to delivery nodes and to the Equinox Streaming and Recording VDN solution. VDN supports publishing recordings as well as live broadcast.

You can view the programs distributed to the VDN appliance and to be delivered to the CDN with the associated status of the program.

Equinox Streaming and Recording currently only supports the Highwinds Cloud CDN.

Equinox Streaming and Recording Manager™

The Equinox Streaming and Recording Manager provides a web-based interface to configure and manage streaming and recording software, devices, services, and users. The Equinox Streaming and Recording Manager application resides on a single hardware platform and provides access to all content in the Equinox Streaming and Recording environment.

There are two Equinox Streaming and Recording Manager portals:

- Equinox Streaming and Recording Manager Administrator Portal: Administrators use this portal to perform the following tasks:
  - Configure and manage video communications devices
  - Manipulate content
  - Monitor user roles
  - Create and set global policies
  - Identify best practices and usage effectiveness through comprehensive reporting
  - Allow access to the VDN for CDN deployment or programs
  - Manage organizations, in a multi-tenant deployment (including what profiles, categories and CDN settings they can access)
  - Create and manage viewer mappings to associate viewers with the appropriate distribution node location
- Avaya Equinox® Unified Portal: Viewers select the **Recordings and Events** tab on the main Avaya Equinox® Unified Portal page to access the viewer portal. Users can select the **Schedule** tab to schedule an event. Users can perform the following tasks in relation to recordings:
  - View programs
  - Navigate categories
  - View live or on-demand programs

Avaya Equinox® Recording Gateway™

You can configure Equinox Streaming and Recording to record:

- Audio-only conferences
- Audio and web collaboration conferences and MSS video

Audio-only and audio and web collaboration conferences use SIP. Video, audio, and web collaboration conferences use H.323. In order to support this mix of protocols, you must deploy an Avaya Equinox® Recording Gateway. You can deploy the Equinox Recording Gateway using the Avaya Equinox® Management interface. The Equinox Recording Gateway is similar to an Avaya Equinox® Media Server but does not accept regular client connections and is only used for

recording purposes. When you add the media server (MCU) configured for high scale audio, you get three additional meeting types - Audio Service, Audio Service with Web Collaboration and MSS video, Audio and Web Collaboration. Each meeting type is also matched to a particular rate of encoding and screen resolution. This means that recordings do not use unnecessary resources and disk space if they are not required by the meeting type.

When a user records a conference, Equinox Management identifies the type of recording that is required by the user. It routes the media to the appropriate gateway, if one is required. Equinox Management also determines the most appropriate capture rate, resolution, frame rate, and encode rate for the Equinox Streaming and Recording Conference Point.

The Equinox Recording Gateway does not require a separate license. When you buy a media node, you receive an Equinox Recording Gateway as well. For more information on adding the gateway to Equinox Management and for information on configuring the meeting types, see *Administering Avaya Equinox® Management*, which is available on support.avaya.com.

Note:

Multicasting is not supported any longer. You cannot configure multicast settings.

Related links

Example of a direct DMZ deployment on page 378
Example of a reverse proxy deployment on page 379
Example of a distributed deployment on page 380
Example of a cloud deployment on page 383
System requirements for Equinox Streaming and Recording on page 384

Example of a direct DMZ deployment

Figure 102: Example of a Direct DMZ Deployment on page 379 displays an example of an Equinox Streaming and Recording deployment that is situated directly in the demilitarized zone (DMZ). The deployment is a centralized or all-in-one solution, which means that all of the Equinox Streaming and Recording components reside on a single server. An all-in-one solution is suitable for a small or medium deployment that does not require redundancy.

In a typical small deployment, all of the Equinox Streaming and Recording components reside on a single server. The Equinox Streaming and Recording Manager and the transcoder run directly on the host server. The conference point (CP), delivery node (DN), and, optionally, a virtual delivery node (VDN) run as virtual servers. VDNs enable enterprises to host recordings in the cloud.

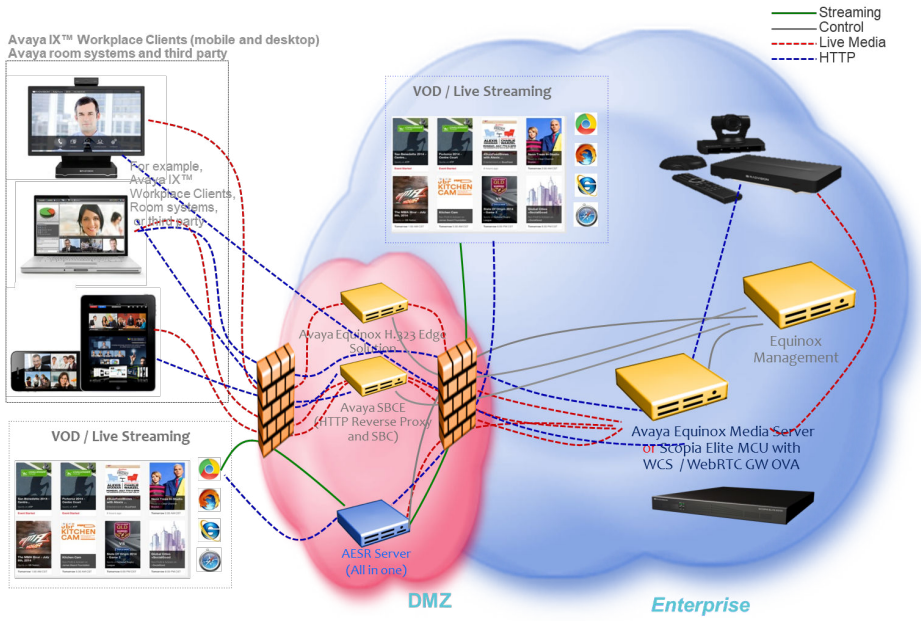


Figure 102: Example of a Direct DMZ Deployment

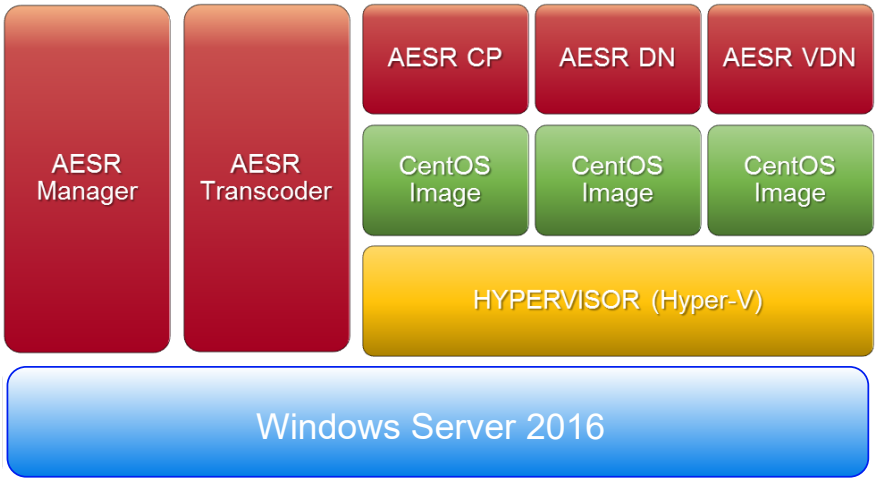


Figure 103: Components in an All-In-One Deployment with Virtual Software

Related links

Avaya Equinox Streaming and Recording Server on page 374

Example of a reverse proxy deployment

Figure 104: Example of a Reverse Proxy Deployment on page 380 displays an example of an Equinox Streaming and Recording deployment that includes a reverse proxy server. The deployment is a centralized or all-in-one solution.

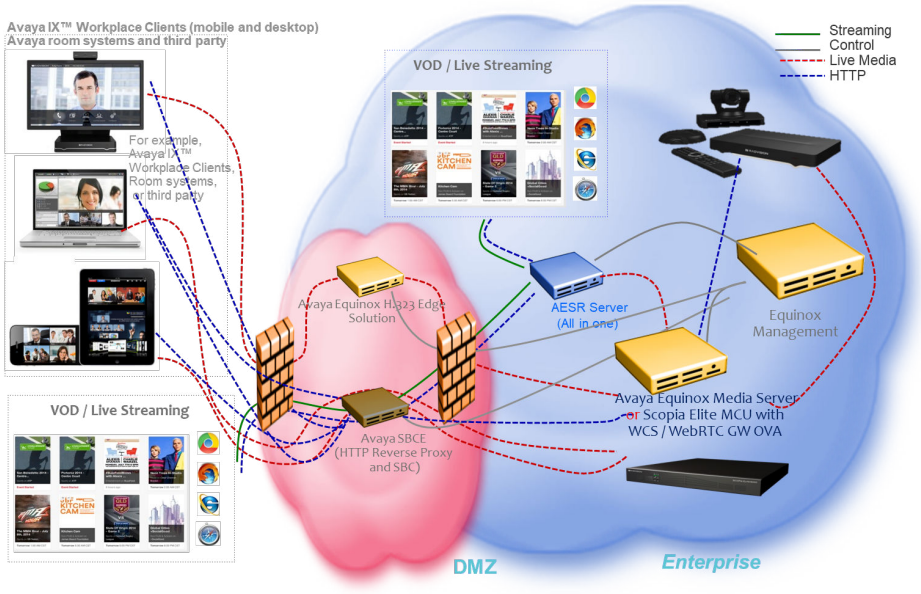


Figure 104: Example of a Reverse Proxy Deployment

Related links

[Avaya Equinox Streaming and Recording Server](#) on page 374

Example of a distributed deployment

[Figure 105: Example of a Distributed Deployment](#) on page 381 displays an example of a distributed Equinox Streaming and Recording deployment. The deployment also uses a reverse proxy server. In this example, there are several delivery nodes (DNs) and/or conference points (CPs). This configuration enables Equinox Streaming and Recording to host large numbers of recordings. A configuration with multiple media nodes can also provide redundancy.

In a typical distributed deployment, the Equinox Streaming and Recording Manager resides on a separate, dedicated server. The various media nodes can operate as CPs, DNs, or virtual delivery nodes (VDNs). VDNs enable enterprises to host recordings in the cloud.

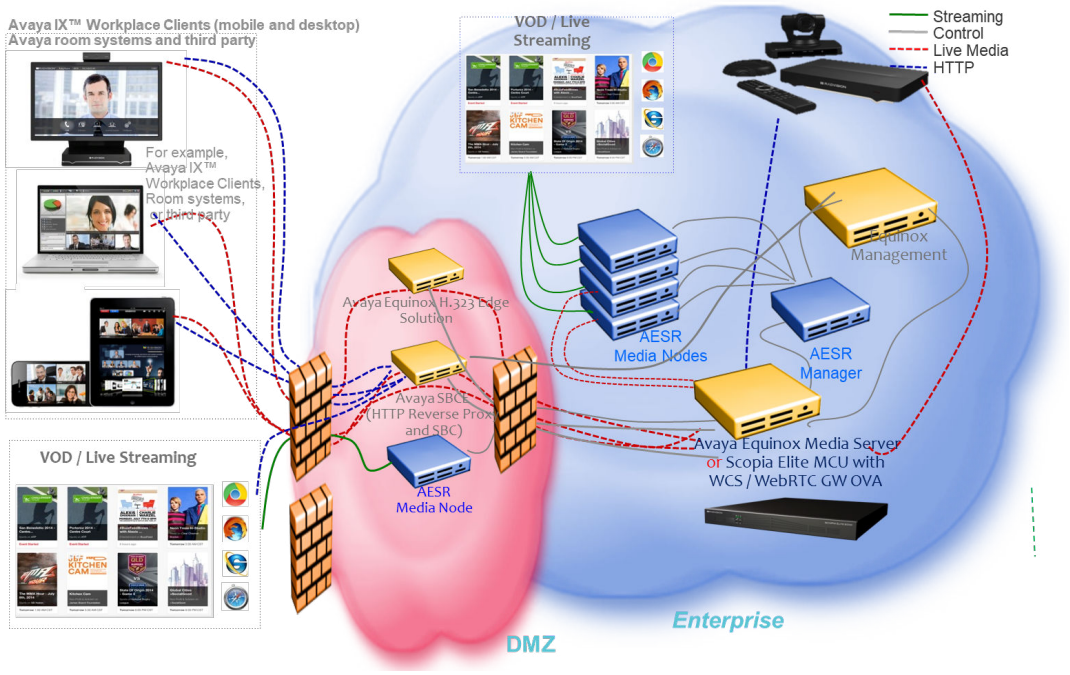


Figure 105: Example of a Distributed Deployment

Related links

[Avaya Equinox Streaming and Recording Server](#) on page 374
[Deployment choices for centralized and distributed solutions](#) on page 381

Deployment choices for centralized and distributed solutions

The Equinox Streaming and Recording server performs three functions:

- Content recording
- Content delivery
- Content management

Content delivery, in this context, refers to streaming.

When you run the configuration utility (or *wizard*), you choose between three deployment options for the Avaya Equinox® Streaming and Recording Server (Equinox Streaming and Recording). You can choose to house all three functions on a single server. Alternatively, you can choose to house the management function on one server and the recording and delivery functions on another server or servers. This configuration involving multiple servers is called a distributed system.

If you intend to house all three functions on a single server, you must run the configuration utility on that server. On the selection screen, you must choose **All-in-One**..

Note:

Avaya does not support the expansion of an All-in-One system to a Distributed System. You must carefully plan your deployment in view of your future capacity needs. If it is likely that your recording needs will go beyond the capacity of an All-in-One system in the future, Avaya recommends that you start with a small Distributed System (one standalone Manager and one Media Node) from day one. You can then add more Media Nodes to the system as needed.

If you intend to install a distributed system, you must run the configuration utility on each server in the system. On the selection screen, you must choose whether the server will house the content management or the recording and delivery functions.

Related links

Example of a distributed deployment on page 380
All-in-one on page 382
Content Management components only on page 382
Media Node only on page 382

All-in-one

If your Equinox Streaming and Recording deployment is an all-in-one system, all Equinox Streaming and Recording components reside on a single server.

For more information, see *Administrator Guide for Avaya Equinox® Streaming and Recording Server* which is available on https://support.avaya.com/.

Related links

Deployment choices for centralized and distributed solutions on page 381

Content Management components only

If your Equinox Streaming and Recording deployment is a distributed system, the Equinox Streaming and Recording components reside on multiple servers. You must install the content management components on one server and install the recording and delivery components on another server or servers.

For a distributed system, you must run the Equinox Streaming and Recording Configuration Utility on each of the servers. When you are running the configuration utility on the server which will act as the content management server, you must select **Content management components only** on the Select Configuration dialog of the configuration wizard.

Related links

Deployment choices for centralized and distributed solutions on page 381

Media Node only

If your Equinox Streaming and Recording deployment is a distributed system, the Equinox Streaming and Recording components reside on multiple servers. You must install the content management components on one server and install the recording and delivery components on another server or servers.

For a distributed system, you must run the Equinox Streaming and Recording Configuration Utility on each of the servers. You can install the recording component on one server and the delivery component on another server. Alternatively, you can install both aspects on a single server. In this distributed configuration, these servers act as media nodes. When you are running the configuration utility on a server which will act as a media node, you must select **Media Node only** on the Select Configuration dialog of the configuration wizard.

A media node that is used for the recording component is called a Conference Point (CP).

A media node that is used for the delivery component is called a Delivery Node (DN).

Related links

Deployment choices for centralized and distributed solutions on page 381

Example of a cloud deployment

Example of a cloud deployment on page 383 displays an example of an Equinox Streaming and Recording deployment that hosts recordings in the cloud. The deployment is a centralized or all-in-one solution that uses a reverse proxy server. A cloud deployment uses a virtual delivery node (VDN) to host recordings remotely.

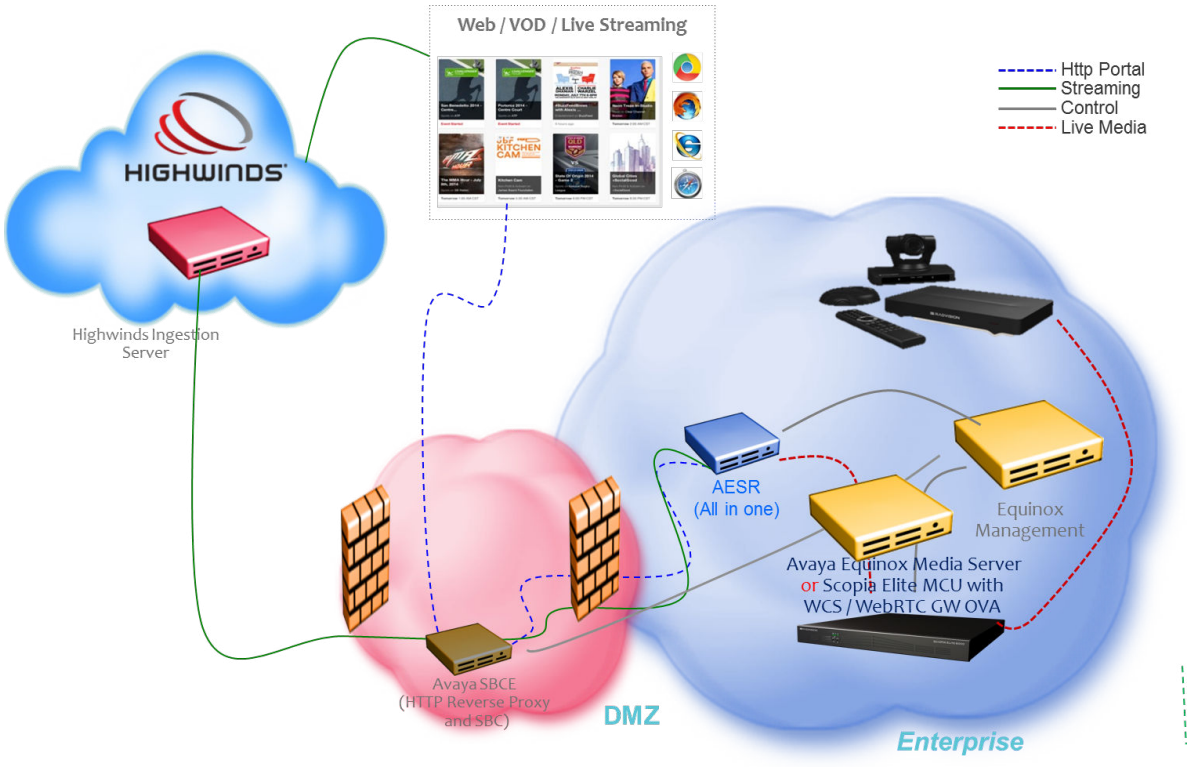


Figure 106: Example of a Cloud Deployment

Related links

Avaya Equinox Streaming and Recording Server on page 374

System requirements for Equinox Streaming and Recording

Before you log on to Equinox Streaming and Recording Manager user pages (in other words, Avaya Equinox® Unified Portal), your client system must meet the system requirements listed in Table 53: Requirements on page 384.

Table 53: Requirements

Component	Requirement
Web browser	• Microsoft Internet Explorer 11 • Microsoft Edge™ N-1 or later • Mozilla Firefox™ N-1 or later (Mac or Windows) • Chrome™ N-1 or later (Mac, Windows, or Android) • Safari™ N-2 or later (Mac, iOS) JavaScript must be enabled.
Operating system	• Mac OS X 10.7 (Lion) or later • Windows™ 10 • iOS N-1 or later • Android 4.0.3. or later
HTMLV5 Browsers	A select number of browsers support video playback directly for MP4 VoD files including: • Microsoft Internet Explorer 11 • Safari 6™ or later • Chrome 30™ or later • Microsoft Edge™
IOS Tablet and Phones, Android Tablets and Phones, Windows Phones/Tablets	Playback function for MP4 VoD files

Note:

To support non-Western language character sets, install the particular language pack on the client system from which you are accessing the Equinox Streaming and Recording Manager. Refer to the operating system documentation for your system.

For the browsers and operating system combinations listed in Table 54: Flash Not Required on page 385, users can play recordings without the requirement of the Adobe Flash Plugin.

Table 54: Flash Not Required

Desktop Browser	Desktop Browser version	Operating System
Google Chrome	34+	All Equinox Streaming and Recording Supportive Desktop OS (Win 10+, MAC)
Mozilla Firefox	42+	All Equinox Streaming and Recording Supportive Desktop OS (Win 10+, MAC)
Microsoft Internet Explorer	11+	Windows 10
Apple Safari	6.0+	MAC OS X 10.6+
Microsoft Edge	All	Windows 10

Related links

Avaya Equinox Streaming and Recording Server on page 374

Installing Avaya Equinox Streaming and Recording

Installation checklist

Follow the steps in this checklist to install the Avaya Equinox® Streaming and Recording Server (Equinox Streaming and Recording).

Tip:

It is a good idea to print out this checklist and to mark each task as you complete it.

No.	Task	Description	Notes	✔
1	Learn more about the new streaming and recording server and figure out your deployment type.	Avaya Equinox Streaming and Recording Server on page 374		

Table continues…

No.	Task	Description	Notes	✔
2	Connect the LAN cables, keyboard, mouse, and monitor for your new server.	• Physically connecting the new server on page 387 • For more information about obtaining and installing the Equinox Streaming and Recording WIM, see the *Equinox Streaming and Recording Disaster Recovery Guide*, which is available from support.avaya.com.		
3	Start up the server.	Starting the new server on page 390	You require the Microsoft Windows product key.	
4	Configure the server using the Avaya Equinox® Streaming and Recording Server Configuration Wizard.	Configuring the new server on page 391		
5	Set the IP addresses and apply the licenses.	Checklist for configuring Avaya Equinox Streaming and Recording Server licenses on page 436		
6	Configure the network that each device will use to communicate with the Equinox Streaming and Recording Manager.	Configuring external addresses for public interfaces on page 396	Before registering devices, you may want to set which network each device uses to communicate with the Equinox Streaming and Recording Manager. This forces the proper communication path to and from the Equinox Streaming and Recording Manager no matter which IP the Equinox Streaming and Recording Manager uses to communicate with the Equinox Streaming and Recording device.	
7	Register each of the components with the main server.	Registering each of the components on page 397		
8	On the delivery node (DN), configure the parent delivery node.	Configuring delivery nodes on page 400		

Table continues…

No.	Task	Description	Notes	✔
9	On the conference point (CP), configure the gatekeeper IP and source DN.	Configuring conference points on page 407		
10	On Equinox Streaming and Recording, configure the network address for device communication.	Specifying polling intervals and the network address on page 409		
11	Register Equinox Streaming and Recording with Equinox Management.	Adding and Modifying Equinox Streaming and Recording Servers in Equinox Management on page 411		
12	Configure the Avaya Equinox® Recording Gateway.	Configuring the Avaya Equinox® Recording Gateway on page 413		
13	Replace the default security certificates.	For more information, see *Administrator Guide for Avaya Equinox® Streaming and Recording Server* which is available on https://support.avaya.com/.	In order to access live streaming, you must replace the default security certificates.	

Physically connecting the new server

Before you begin

The Avaya Equinox® Streaming and Recording Server is a Dell™ PowerEdge™ R640 Server and uses profile #5 specifications.

You require a keyboard, a mouse, and a monitor. You also require several IP addresses and up to six category 5e LAN cables. Ensure that you received the following items with your Equinox Streaming and Recording:

- Power cords
- Rack mount kit

Procedure

1. Connect the keyboard, mouse, and monitor.
2. Connect the LAN cable(s).

   All of the Avaya Equinox® Streaming and Recording Server NICs are 1GBit bonded. Connect to at least one. They all respond with a single IP address.
3. Connect the power cable.
4. Power up the unit.

Next steps

Return to the Installation checklist on page 385 to see your next task.

Related links

Front view of Dell™ PowerEdge™ R640 Server on page 388
Back view of Dell™ PowerEdge™ R640 Server on page 389

Front view of Dell™ PowerEdge™ R640 Server



Figure 107: Front view of Dell PowerEdge R640 server

No.	Item	Icon	Description
1	Left control panel	NA	Displays the system health, system ID, and status LED indicators. • Status LED: Enables you to identify failed hardware components. There are up to five status LEDs and an overall system health LED (Chassis health and system ID) bar.
2	Optical drive	N/A	One slim SATA DVD-ROM drive. **Note:** DVD devices are data only.
3	USB port		The USB port is USB 3.0 compliant.
4	VGA port		Enables you to connect a display device to the system.
5	Right control panel	NA	Contains the power button, USB port, iDRAC Direct micro port, and the iDRAC Direct status LED.
6	Drive slots	NA	Enable you to install hard drives that are supported on your system.

Related links

Physically connecting the new server on page 387

Back view of Dell™ PowerEdge™ R640 Server

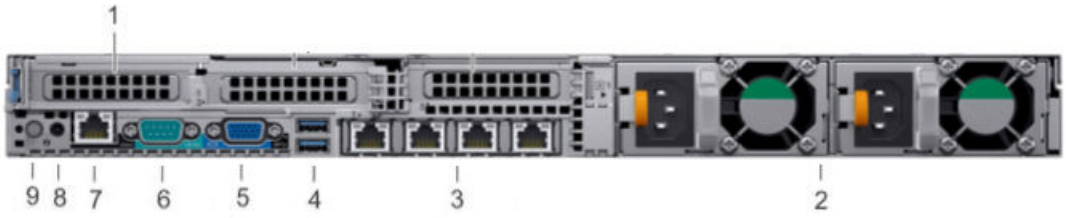


Figure 108: Back view of Dell PowerEdge R640 single CPU server

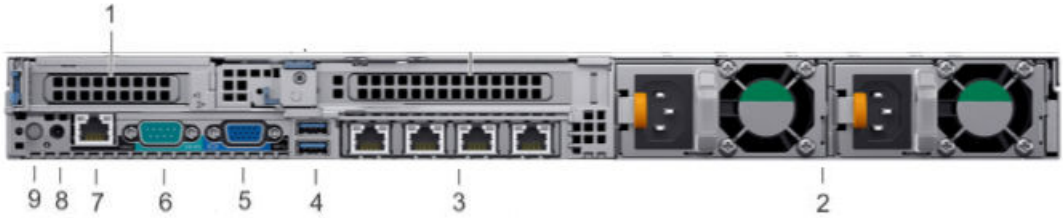


Figure 109: Back view of Dell PowerEdge R640 dual CPU server

No.	Item	Icon	Description
1	PCIe expansion card slot(s)	N/A	Enables you to install PCI Express expansion cards.
2	Drive slots	N/A	Enables you to install hard drives that are supported on your system.
3	Power supply unit (2)	N/A	Wattage and voltage type depends on configuration.
4	NIC port (4)		The NIC ports that are integrated on the network daughter card (NDC) provide network connectivity.
5	USB 3.0 port		The USB ports are of 9-pin and 3.0-compliant. These ports enable you to connect USB devices to the system.
6	VGA port		Enables you to connect a display device to the system.
7	USB Connectors (2)		Allows you to connect USB devices to the system. These ports are USB 3.0-compliant.
8	Serial port		Enables you to connect a serial device to the system.
9	iDRAC9 Enterprise port		Enables you to remotely access iDRAC.
10	CMA power port	N/A	The Cable Management Arm (CMA) power port enables you to connect to the CMA.

Table continues…

No.	Item	Icon	Description
11	System identification button		The System Identification (ID) button is available on the front and back panel of the systems. Press the button to identify a system in a rack by turning on the system ID button. You can also use the system ID button to reset iDRAC and to access BIOS using the Step Through mode.

Related links

Physically connecting the new server on page 387

Initially configuring the new server

If you have the Avaya-provided server (The Avaya Solutions Platform), it includes a pre-licensed copy of Windows Server 2016. The software image includes Windows Server 2016 and you are required to provide a license key during the initial configuration.

Procedure

1. Start up the server.
2. Press Ctrl+Alt+Delete to log in.

   The default username is `Administrator`.

   The default password is `Avaya123!`.
3. Choose **C** to configure the network settings.

   You can configure the network addresses statically or dynamically. Avaya recommends using statically assigned IP addresses, as the IP address needs to remain constant. If you do choose to use dynamically assigned IP addresses, your network must be DHCP-enabled.
4. Choose **S** for statically assigned IP addresses or **D** for dynamically assigned IP addresses.

   If you choose **D**, the setup tries to obtain an address. If you choose **S**, you are prompted to enter the IP address.
5. Enter your subnet mask by choosing an appropriate prefix length.
6. Enter the gateway address.

   You must enter a valid gateway address that fits within the IP and subnet mask that you previously entered. The system provides a valid range of IPs that you can use for the gateway. You must pick one of these IP addresses.
7. Enter your primary DNS Server IP.

   This is a mandatory step.
8. **(Optional)** Enter a secondary DNS IP or press **Enter** if you want to skip this step.
9. **(Optional)** Enter a DNS suffix.

   You should enter a DNS suffix for FQDN/SSL configurations.

10. Enter the server host name, or press **Enter** to use the default generated hostname.

    You should enter a hostname for FQDN/SSL configurations.

    You are then prompted to enter a new password.

11. At the **You must choose a new Administrator password. Enter new Administrator password:** prompt, type a new password.
12. At the **Reenter new Administrator password to confirm:** prompt, re-type your new password.
13. Confirm the configuration and select **Y** if it is correct, or **N** if you would like to reenter the data.

    When you enter **Y**, the server reboots.

14. When the server starts up again, press Ctrl+Alt+Delete to log in.
15. **(Optional)** Synchronize the time on the new server with the time on your NTP server.
    a. Click on the time and date in the task bar.
    b. Click **(Change date and time settings...)**.
    c. On the Date and Time tab, perform the following actions:
       - Set the correct date and time using the **Change date and time** button.
       - Set the correct timezone using the **Change timezone** button.
    d. On the Internet Time tab, click **Change settings...** and perform the following actions:
       - Ensure that **Synchronize with an Internet time server** is selected.
       - Enter the NTP server in the **Server** list.
       - Click **OK**.
16. Click **OK**.

Next steps

Return to the Installation checklist on page 385 to see your next task.

Configuring the new server

The Avaya Equinox® Streaming and Recording Server Configuration Utility launches automatically when the operating system is loaded for the first time. You can also run the configuration utility at any time from the Start menu or from the desktop shortcut.

If you previously installed a Delivery Node (DN), either as part of an all-in-one deployment or on its own, you can add or remove a Virtual Delivery Node (VDN) or an external storage device called a storage area network (SAN), without disrupting the server configuration. If you have not previously installed a DN, the configuration utility erases any previous configurations on the Equinox Streaming and Recording server.

About this task

Ths task describes how to configure Equinox Streaming and Recording in an enterprise deployment. If yours is a service provider deployment, the steps vary slightly.

Procedure

1. In the **Choose Setup Language** dialog, select your preferred language.
2. On the next screen, click **Next**.

   The first time you run the configuration utility, the system displays a Welcome screen.

   If you have not configured a delivery node (DN) and you run the configuration utility again, the system displays a Warning screen because you may be about to perform a harmful action.

   If you have configured a DN and you run the configuration utility again, you can add or remove a virtual delivery node (VDN) or an external storage device without disturbing the server configuration.
3. On the **End-User License Agreement** screen, select **I accept the terms of the License Agreement** to accept the license agreement.
4. Click **Next**.
5. On the **Select Configuration** screen, select your deployment type.

   For more information, see Deployment types on page 381.



Figure 110: Select Configuration

6. On the **Deployment Type** screen, perform one of the following actions:
   - If you have selected **All-in-One** on the **Select Configuration** screen, select **Enterprise deployment** or **Multi-tenant** to match your Equinox Management deployment.



Figure 111: Deployment Type

- If you have selected **Content management components only** on the **Select Configuration** screen, select **Enterprise deployment** or **Multi-tenant** to match your Equinox Management deployment. The screen is similar to Figure 111: Deployment Type on page 394.
- If you have selected **Media Node only** on the **Select Configuration** screen, select whether you want to install the recording and delivery (streaming) components, the recording components, or the delivery components by selecting **Configure content recording and streaming components**, **Configure content recording components only**, or **Configure content streaming components only**.



Figure 112: Deployment Type

7. Click **Next**.
8. **(Optional)** At this point, you can choose to install a Virtual Delivery Node (VDN).
9. **(Optional)** At this point, you can choose to install a SAN.
10. Click **Next** to skip the optional screens.
11. On the **Finish Configuration** screen, click **Finish**.

    The Equinox Streaming and Recording Configuration Utility installs the Equinox Streaming and Recording components.
12. On the **Complete Configuration** screen, click **View Addresses** to display the MAC addresses of the Equinox Streaming and Recording server.

    You require these MAC addresses in order to license the Equinox Streaming and Recording server. The MAC addresses are also stored in `C:\assrconfigtool\MAC_Addresses.txt`.
13. Make a note of the MAC addresses.

    This information is required when you access the Avaya PLDS system to obtain a license key.

Next steps

Return to the Installation checklist on page 385 to see your next task.

Configuring external addresses for public interfaces

About this task

To secure the Equinox Streaming and Recording public interfaces, proper certificates have to be generated. The certificates have to match the fully qualified domain name (FQDN) or the IP address of the machine. Avaya recommends setting the use of FQDNs.

When you configure your system to use FQDNs, they need to be used to register every device with the Equinox Streaming and Recording Manager.

You must also configure Equinox Streaming and Recording to use external addresses, using the FQDN, and not the IP address.

Procedure

1. Configure the external address of the Equinox Streaming and Recording Manager.
    a. Log in to Equinox Streaming and Recording.
    b. Click the **Global Policies** tab.
    c. Click **General Options**.
    d. Type the external address in the **Network Address for Device Communication** field.
    e. Click **Save**.
2. Configure the external address of the delivery node.
    a. Type `https://<DN FQDN/IP Address>:8445/` in a web browser.
    b. Log in to the system using the credentials that you configured when you updated the default username and password.
    c. Click the **Network** tab.
    d. Type the external address in the **External Address (optional)** field in the **Global Network Configuration** section.
    e. Click **Submit**.
3. Configure the external address for the conference point.
    a. Type `https://<CP FQDN/IP Address>:8445/` in a web browser.
    b. Log in to the system using the credentials that you configured when you updated the default username and password.
    c. Navigate to **System Configuration** > **Network Configuration**.
    d. Type the external address in the **External Address (optional)** field in the **Global Network Configuration** section.

    You can now optionally enter a DNS name or specific external or internal IP address that you want to use when communicating with the Equinox Streaming and Recording

Manager. This functionality enables you to enter externally statically mapped IP addresses and so on. If you leave this field empty then Equinox Streaming and Recording automatically uses the IP addresses assigned to the operating system statically or from DHCP. This address is passed to the Equinox Streaming and Recording Manager when the device registers and is used by the Equinox Streaming and Recording Manager to access the device. The Equinox Streaming and Recording Web GUI reports the IP address and other network information and on some of the Equinox Streaming and Recording devices, you can set the IP address and other key network settings. This functionality is especially helpful for the systems that are virtualized to ensure the proper network device IP address set. The CP and DN show up as one “eth0” virtualized NIC to the host windows machine taking advantage of the bonded NICS of the host.

e. Click **Finish**.

4. Configure the external address for the transcoder.
   a. Type `https://<CP FQDN/IP Address>:8445/` in a web browser.
   b. Log in to the system using the credentials that you configured when you updated the default username and password.
   c. Navigate to **System Configuration** > **Transcoder Configuration**.
   d. Type the external address in the **Transcoder Address**.

      This is the address of the transcoder, which is the Windows server hosting the CP virtual machine.

   e. Click **Finish**.

Note:

If you are using IP addresses, the certificates have to be generated for the IP address. The IP address has to be included on both the **Common Name** field and the **Subject Alternative Name** field when generating the certificates. If the IP address is not included in the **Subject Alternative Name** field, certain devices, such as Mac computers or Android mobile devices may not operate correctly.

Registering each of the components

After you have applied a license to each of the components of the Avaya Equinox® Streaming and Recording Server, you must register them with the Avaya Equinox® Streaming and Recording Server Manager.

You must register all delivery nodes, virtual delivery nodes, and conference points with the Manager. In addition, you must register the transcoder with the conference point. You do not have to register the transcoder with the Manager.

About this task

The registration process is the same for all delivery nodes, virtual delivery nodes, and conference points.

Procedure

1. Type `https://<Equinox Streaming and Recording manager FQDN/IP address>:8445` in a web browser.
2. Log in to Equinox Streaming and Recording. The following credentials are the default credentials, but when you first log in, you are prompted to update your password:
   - Username: `admin`
   - Password: `admin`
3. Select the **Devices** tab.
4. Click on **Register Devices** from the left **Actions** menu.
5. Enter the IP address or FQDN of the component that you want to register and click **Register**.
6. Repeat this step for each of the components.
7. **(Optional)** Verify the registration for the conference point.
   a. Type `https://<CP FQDN/IP Address>:8445/` in a web browser.
   b. Log in using the following credentials:
      - Username: `administrator`
      - Password: `administrator`
   c. **(Optional)** If this is the first time that you have logged in, you are prompted to update your password.
   d. From the left menu bar, click **System Configuration**.
   e. Click **Enable Services**.
   f. Under Manage Device, click **Configure**.
   g. Verify that the **Manage Registration State** is Registered and the **Manager Host** is the proper manager IP.
8. **(Optional)** Verify the registration for the delivery node or virtual delivery node.
   a. Type `https://<DN FQDN/IP Address>:8445/` in a web browser.
   b. Log in using the following credentials:
      - Username: `administrator`
      - Password: `administrator`
   c. **(Optional)** If this is the first time that you have logged in, you are prompted to update your password.
   d. From the menu bar, click **Configuration**.
   e. Verify that the **Manage Registration State** is Registered and the **Network Address** is the proper manager IP.

9. Register the transcoder.
    a. Type `https://<CP FQDN/IP Address>:8445` in a web browser.
    b. Log in using the following credentials:
        - Username: `administrator`
        - Password: `administrator`
    c. **(Optional)** If this is the first time that you have logged in, you are prompted to update your password.
    d. From the left menu bar, click **System Configuration**.
    e. Click **Transcoder Configuration**.
    f. Enter the IP address or FQDN of the transcoder and click **Finish**.

    The transcoder is running on the host operating system. The CP is running on a virtual machine which runs on the host. The IP address/FQDN of the transcoder is the IP of the host Windows server. When you are securing the system with certificates, this address must match the address that you specify in the transcoder server certificate.

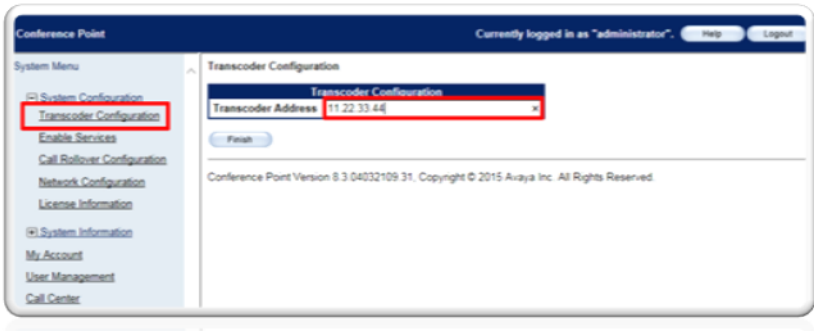


Figure 113: Transcoder Registration

Next steps

Return to the Installation checklist on page 385 to see your next task.

Related links

Unregistering each of the components on page 399

Unregistering each of the components

If you plan to move a device to a different Equinox Streaming and Recording environment, unregister the device before changing its location. If you do not unregister the device using the Equinox Streaming and Recording Manager, you must unregister it using its local web interface before you can register it to the new Equinox Streaming and Recording environment.

About this task

The process of unregistering is the same for all delivery nodes, virtual delivery nodes, and conference points.

Procedure

1. Log in to Equinox Streaming and Recording.
2. Click the **Devices** tab.
3. From the **Browse** menu, select the device you want to access.

   A list of devices of that type is displayed.
4. Click **Advanced Options**.
5. Select one of the devices.

   The device details dialog is displayed.
6. Click **Unregister**.

Related links

[Registering each of the components](#) on page 397

Configuring delivery nodes

Delivery nodes (DN) store all content that is created by the conference point and deliver the content to client systems at playback time. You must associate the conference point with the delivery nodes.

A source DN is the original DN that receives a recording file from its associated conference point. A source DN sends the recording file to all of the other DNs in the network.

Equinox Streaming and Recording supports deployments containing a mix of different servers with varying amounts of storage capacities. You can have DNs with large amounts of free space and DNs with limited space. To maximize available storage, you can configure DNs which delete old recordings when the disk is almost full and you can configure DNs which permanently store all recordings.

- An edge DN is a DN on which content is stored wherever possible but this content can expire. Older content makes way for newer content.
- A master DN is a delivery node which permanently holds all content. Typically, you assign master status to the DN with the largest storage capacity. If your deployment only contains a single DN, that DN is automatically added as the master DN.

For playback, you can configure rules to determine which DN is selected when a user wants to access a recording. For example, you might want to use the DN closest to the user location, or you might want to direct the user to the original source DN. The DN closest to the user location or the original source DN may be edge DNs. Typically, if you have a master DN, that DN becomes the source DN for all recordings. If you want to expand your storage capabilities with an external storage device, it is a good idea to make the DN which is connected to the external storage device the master DN.

Edge DNs are programmed with rules which determine how recordings are selected for deletion. When the disk capacity reaches 90%, content is removed until the capacity reaches 70%. Only

recordings which have been copied to other DNs can be deleted. Recordings are scheduled for deletion as follows:

- Recordings created over a week ago and never accessed.
- Recordings created over a week ago with the greatest amount of elapsed time since the last access attempt.
- Recordings created less than a week ago and never accessed, oldest creation time first.
- Recordings created less than a week ago with the greatest amount of elapsed time since the last access attempt.

Equinox Streaming and Recording stops creating new recordings and triggers an alert when capacity on the master DN reaches 90%. Equinox Streaming and Recording stops any recordings in progress and triggers an alert when capacity on the master DN reaches 95%. If the capacity on an edge DN reaches 90%, Equinox Streaming and Recording stops creating new recordings on that particular edge DN. Technically, this should never happen because of the intelligent expiration and deletion rules.

Avaya recommends performing regular backups on the master DN. You do not have to perform backups on the edge DNs. Equinox Streaming and Recording enables you to redistribute and synchronize any media if you have to restore a master DN using the **Replace with new DN** field in the **Advanced Options** panel.

The Delivery Node Details dialog displays a list of recording files, known as **Source Programs** and **Distributed Programs**. Source programs are programs (recording files) for which this delivery node is the main source for storage. Distributed programs are programs which other delivery nodes have forwarded to this delivery node.

Procedure

1. Log in to Equinox Streaming and Recording. The following credentials are the default credentials, but when you first log in, you are prompted to update your password:
   - Username: `admin`
   - Password: `admin`
2. Select the **Devices** tab.
3. From the **Browse** menu on the left, click **Delivery Nodes**.
4. Click the name of the delivery node to display the delivery node details.

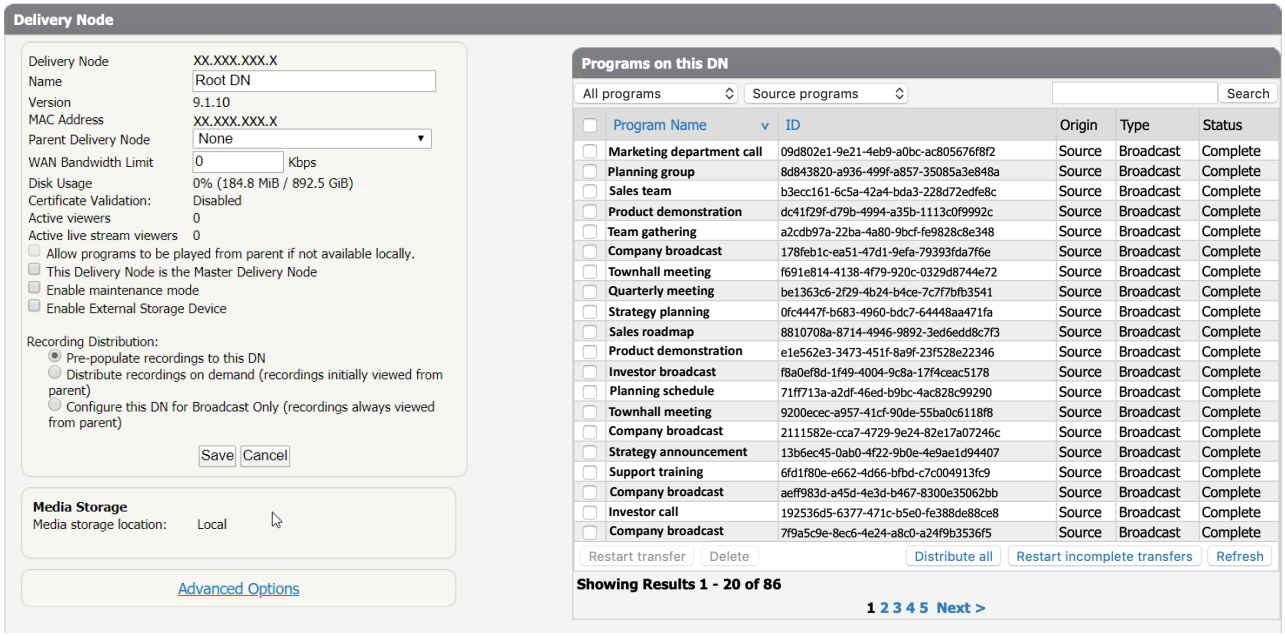


Figure 114: Delivery Node Details

5. Configure the settings, as described in Table 55: Delivery Node Details on page 402.

Table 55: Delivery Node Details

Field Name	Description
Name	Enter a name for the delivery node.
Version	Verify the version and MAC address of the delivery node.
Parent Delivery Node	Select a delivery node. The **Parent Delivery Node** distributes content to the delivery node and vice versa (child to parent). If this is a core or parent for the system then change the value from **Not Configured** to **None**.
WAN Bandwidth Limit	Specify the maximum bandwidth, in Kbps, that this delivery node can use when receiving/ transferring content. If you enter **0** (zero), the bandwidth is unlimited.
Disk Usage	The percentage of storage space that is currently used to store recordings. You can also view the number of users who are currently accessing recordings or broadcasts.
Certificate Validation	You can check whether server certificate validation is enabled.
Active Viewers	You can view the number of users who are currently accessing recordings.

Table continues…

Field Name	Description
Active Live Stream Viewers	You can view the number of users who are currently accessing broadcasts.
Allow programs to be played from parent if not available locally	If your deployment contains a hierarchical relationship between DNs, you can enable playback from a ‘parent’ DN if the recording is not available on the ‘child’ DN. Select this checkbox to enable playback from a parent. If you have not configured hierarchical relationships in your deployment, this checkbox is not available.
This Delivery Node is the Master Delivery Node	Select this checkbox to assign master status to this DN. This means that programs on this delivery node are protected from automatic expiration (deletion). A master DN is a delivery node which permanently holds all content. Typically, you assign master status to the DN with the largest storage capacity. If your deployment only contains a single DN, that DN is automatically added as the master DN.
Enable maintenance mode	Select to disable the device so that you can add or remove external storage (DN) or take it out of service (CP and DN). When a device is in maintenance mode, it does not accept new recordings and users cannot playback recordings that are stored on it.
Enable External Storage Device	You can expand your storage capacity by installing and configuring an external storage device called a storage area network (SAN), which uses the SCSI protocol over TCP/IP (iSCSI). Select this checkbox to enable this configuration.

6. **(Optional)** Select a recording distribution policy, as described in the table below.

Table 56: Recording Distribution Policy

Recording Distribution Policy	Description
Pre-populate recordings to this DN	Distribute all recordings and broadcasts to this delivery node. This is the default value.
Configure this DN for Broadcast-only	Distribute all broadcasts to this delivery node but do not download any recordings.
Distribute recordings on demand	Distribute recordings to this delivery node only if they are requested by a user.

7. **(Optional)** Click **Advanced Options** and configure the settings as described in Table 57: Advanced Options on page 404.

Table 57: Advanced Options

Field	Description
Replace with new DN	Use this setting when bringing on a replacement delivery node for an older or broken system.
Unregister	If you plan to move a device to a different Equinox Streaming and Recording environment, unregister the device before changing its location. If you do not unregister the device using the Equinox Streaming and Recording Manager, you must unregister it using its local web interface before you can register it to the new Equinox Streaming and Recording environment.

8. Click **Save**.

Configuring virtual delivery nodes

A virtual delivery node (VDN) delivers content to a global content delivery network (CDN) provider for cloud-based viewer playback. The appliance and the network of the CDN act as one delivery mechanism. Therefore, the VDN appliance and the CDN together create the Equinox Streaming and Recording VDN solution.

When you configure a VDN, you can choose to transfer the recordings to Highwinds CDN using File Transfer Protocol (FTP) or you can choose to transfer the recordings to Highwinds Cloud Storage (HCS) using secure, authenticated, APIs. If your account is HCS-enabled, it supports a more secure method for transferring recordings. FTP does not use any encryption to transfer the files to CDN. The HCS APIs use Secure Sockets Layer (SSL). For more information, see Highwinds Cloud Storage.

Upon program creation, the publisher includes the options of distributing the program to delivery nodes and to the Equinox Streaming and Recording VDN solution. VDN supports publishing recordings as well as live broadcast.

You can view the programs distributed to the VDN appliance and to be delivered to the CDN with the associated status of the program.

Procedure

1. Log in to Equinox Streaming and Recording. The following credentials are the default credentials, but when you first log in, you are prompted to update your password:
   - Username: `admin`
   - Password: `admin`

2. Select the **Devices** tab.
3. From the **Browse** menu on the left, click **VDN**.
4. Click the name of the VDN to display the VDN details.

   Equinox Streaming and Recording supports a single VDN in any deployment.
5. Configure the settings, as described in the table below.

Table 58: VDN Details

Field Name	Description
Name	Enter a name for the delivery node.
Version MAC Address	Verify the version and MAC address of the delivery node.
Source DN	Select a delivery node from where this VDN retrieves content.
Status Disk Usage	View the status of the VDN. It can be Up or Unreachable. View the disk usage. The delivery node supports a total of approximately 900GB at RAID level 1 or 2TB at RAID level 5.
Certificate Validation	You can check whether server certificate validation is enabled.
Allow programs to be played from the source DN if not on CDN	Select to enable the redundancy logic to revert to the source delivery node if a requested recording is not on the CDN.

6. Select a recording distribution policy, as described in the table below.

Table 59: Recording Distribution Policy

Recording Distribution Policy	Description
Pre-populate recordings to this DN	Distribute all recordings and broadcasts to this delivery node. This is the default value.
Configure this DN for Broadcast-only	Distribute all broadcasts to this delivery node but do not download any recordings.
Distribute recordings on demand	Distribute recordings to this delivery node only if they are requested by a user.

Note:

If this system is in enterprise mode, the CDN panel is displayed here. If this system is in multi-tenant mode, the CDN panel is displayed in the **Organizations** tab.

7. Do one of the following:
   - Select **Highwinds CDN** to transfer recordings to Highwinds CDN using File Transfer Protocol (FTP) and configure the settings, as described in Table 60: Highwinds CDN on page 406.

Table 60: Highwinds CDN

Field	Description
Account Hash	Enter the account hash value taken from Strike Tracker 3 Portal.
Host Hash	Enter the host hash value taken from Strike Tracker 3 Portal Host Configuration.
Username Password	Enter the StrikeTracker 3 username and password that you used to purchase the CDN service.
FTP User Name FTP Password	This field enables the uploading of recordings to the CDN. Enter proper cloud storage FTP credentials specific to the customer account. You receive these credentials when you purchase the CDN service.
Enable maintenance mode	Select to disable the device so that you can add or remove external storage (DN) or take it out of service (CP and DN). When a device is in maintenance mode, it does not accept new recordings and users cannot playback recordings that are stored on it.

   - Select **Highwinds Cloud Storage** to transfer recordings to Highwinds Cloud Storage (HCS) using secure, authenticated, APIs and configure the settings, as described in Table 61: Highwinds Cloud Storage on page 406. For this option, you must enable HCS on your Highwind's account.

Table 61: Highwinds Cloud Storage

Field	Description
Account Name	Enter the account name taken from Strike Tracker 3 Portal.
Host Hash	Enter the host hash value taken from Strike Tracker 3 Portal Host Configuration.
HCS Username HCS Password	Enter the StrikeTracker 3 username and password that you used to purchase the CDN service.

Table continues…

Field	Description
Enable maintenance mode	Select to disable the device so that you can add or remove external storage (DN) or take it out of service (CP and DN). When a device is in maintenance mode, it does not accept new recordings and users cannot playback recordings that are stored on it.

8. Click **Save**.

Next steps

In order for the VDN to push content to the CDN, you must configure your network to enable external access because the VDN must have access to the Internet in order to communicate with the CDN. If you have a firewall, you can place the VDN in a DMZ or you can open the appropriate ports on the firewall to enable external communication. Specifically, the VDN must be able to access `upload.hwcdn.net` using FTP on port 21. In addition, the VDN requires HTTP or HTTPS acccess to the CDN.

Configuring conference points

You must configure a conference point to capture H.323 video content and deliver live and on demand webcasting. The Equinox Streaming and Recording conference point includes an embedded transcoder to convert H.323 calls into .MP4 format.

Each conference point must be associated with a delivery node. A delivery node streams and optionally archives the content captured by the conference point and delivers it to client systems.

You can configure a conference point to be in a geographic location. This means that you can assign a location to one or more conference points which coincide with locations set for Scopia Elite MCUs and/or Equinox Media Servers in Equinox Management. When a program starts, Equinox Management includes the desired location, and a conference point close to the MCU/Media Server can be selected. If there are no conference points matching the location passed by Equinox Management, then any conference points without a location are treated as a single pool of conference points, and one of those is selected. If there are no conference points available, the call fails.

Each conference point has a limit to the number of simultaneous high definition or standard definition calls it can handle.

Procedure

1. Log in to Equinox Streaming and Recording. The following credentials are the default credentials, but when you first log in, you are prompted to update your password:
   - Username: `admin`
   - Password: `admin`
2. Select the **Devices** tab.
3. From the **Browse** menu on the left, click **Conference Points**.

4. Click the name of the conference point to display the conference point details.

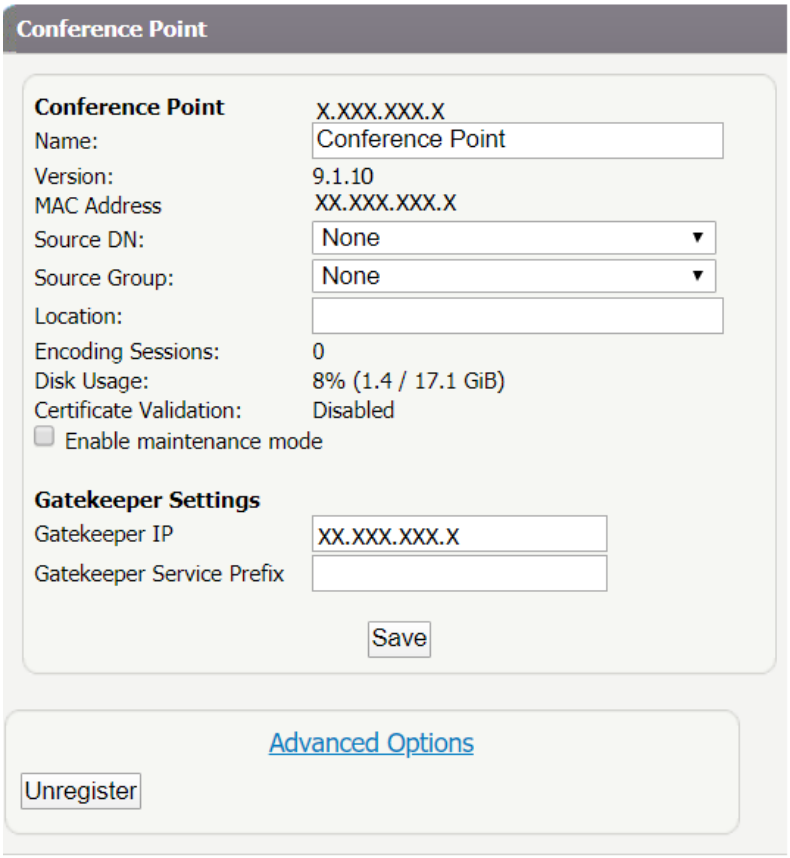


Figure 115: Conference Point Details

5. Configure the settings, as described in Table 62: Conference Point Details on page 408.

Table 62: Conference Point Details

Field Name	Description
Name	Enter a name for the conference point.
Version	Verify the version and MAC address of the conference point.
Source DN	Select a delivery node. Alternatively, you can select a delivery node from the **Source Group** field.

Table continues…

Field Name	Description
Source Group	Select a delivery node viewer group. Alternatively, you can select a delivery node from the **Source DN** field. The Source Group field displays any viewer groups. A viewer group is a group of delivery nodes and these groups offer redundancy. If one of the delivery nodes in a group is not available, an alternative delivery node from the same group is selected.
Location	Enter a location. The location must match a location specified for a Scopia Elite MCU and/or Equinox Media Server in Equinox Management. If you are not specifying locations in Equinox Management, you should leave it blank.
Disk Usage	The percentage of storage space that is currently used to store recordings.
Certificate Validation	You can check whether server certificate validation is enabled.
Enable maintenance mode	Select to disable the device so that you can add or remove external storage (DN) or take it out of service (CP and DN). When a device is in maintenance mode, it does not accept new recordings and users cannot playback recordings that are stored on it.
Gatekeeper IP	Enter the IP address for the gatekeeper with which you plan to register. The gatekeeper must be the same as the one used by Equinox Management.
Gatekeeper Service Prefix	This is an optional field. Enter the service prefix designator for this conference point. You should leave this field as blank.

6. Click **Save**.

Specifying polling intervals and the network address

About this task

You must specify how frequently the Equinox Streaming and Recording communicates with the other components, such as the conference points and delivery nodes. You must also specify the network on which the Equinox Streaming and Recording resides. The polling interval should be in proportion to the number of devices. The fewer the devices, the shorter the intervals. For example, if you have over 200 delivery nodes, Avaya recommends setting the polling to 5 minutes.

The polling frequency affects the latency between the status transitions of the remote device and the appearance of the status on the details page for the device.

Procedure

1. Log in to Equinox Streaming and Recording.
2. Click the **Global Policies** tab.
3. Click **General Options**.
4. Configure the settings, as described in Table 63: Settings on page 410.

Table 63: Settings

Field Name	Description
Conference Point Polling Frequency	Specify how often the Equinox Streaming and Recording Manager checks for device configuration or status changes for each of the conference points.
Delivery Node Polling Frequency	Specify how often the Equinox Streaming and Recording Manager checks for device configuration or status changes for each of the delivery nodes.
Network Address for Device Communication	Enter the IP address or DNS name of the Equinox Streaming and Recording Manager. This is the address that the other devices (delivery nodes, conference points, virtual delivery nodes) will use to communicate with the Equinox Streaming and Recording Manager. If split-horizon DNS is being used, use the DNS name for the Equinox Streaming and Recording Manager. Since this address is used by the other devices to communicate back to the Equinox Streaming and Recording Manager, it is important to specify the correct routable address.
Retain Deleted Recordings For	
Recording Expiration Policy	
Log Retention Policy	

5. Click **Save**.

Configuring the recycle bin for recording file retention

For multi-tenant deployments, the same options are available for recycling, but they are on a per-tenant basis and so are displayed in the **Organization** tab.

Procedure

1. Log in to Equinox Streaming and Recording.
2. Click the **Global Policies** tab.

3. Click **General Options**.
4. Configure the settings, as described in Table 64: Retain deleted recordings for: on page 411.

Table 64: Retain deleted recordings for:

Field Name	Description
Forever	Select to ensure that recordings/programs are never deleted from the recycle bin.
For X days	Type the number of days for which the recycle bin should keep recordings/programs. The default value is 30.
Do not retain deleted recordings (once deleted, they cannot be recovered)	Select to disable the recycle bin feature. If you select this option, as soon as a user deletes a recording, Equinox Streaming and Recording permanently deletes it.

5. Click **Save**.

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 116: Adding an Avaya Equinox® Streaming and Recording server on page 412).

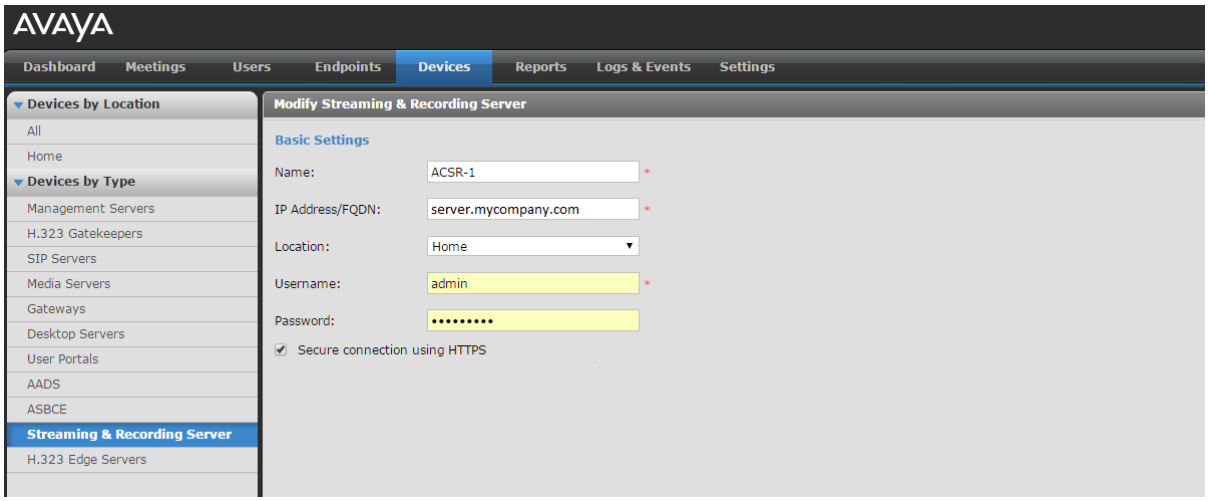


Figure 116: Adding an Avaya Equinox® Streaming and Recording server

4. Configure the Equinox Streaming and Recording Server's settings, as described in (Table 65: Configuring the Avaya Equinox® Streaming and Recording on page 412).

Table 65: 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.

Table continues…

Field Name	Description
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.

Configuring the Avaya Equinox® Recording Gateway

Audio-only and audio and web collaboration conferences use SIP. Video, audio, and web collaboration conferences use H.323. In order to support this mix of protocols, you must deploy an Avaya Equinox® Recording Gateway. You can deploy the Equinox Recording Gateway using the Avaya Equinox® Management interface.

When a user records a conference, Equinox Management identifies the type of recording that is required by the user. The Audio Service and Audio Service with Web Collaboration meeting types are used when a user requests the recording of an audio-only or audio and web collaboration conference. When a user requests the recording of a full video, audio, and web collaboration conference, Equinox Recording Gateway is not used except in the case of a multi-stream video switched conference. Since Equinox Streaming and Recording does not support recording multi-stream video switched conferences, the Equinox Recording Gateway is needed in this case as well. In this release, the Equinox Recording Gateway records only the active speaker video when no content is shared or records the content along with a smaller window showing the active speaker video (gallery layout).

About this task

This section summarizes the steps for configuring the Equinox Recording Gateway to enable it to be used for the recording of conferences that use SIP. For more information on adding the gateway to Equinox Management and for information on configuring the meeting types, see *Administering Avaya Equinox® Management*, which is available on support.avaya.com.

- Add the Equinox Recording Gateway as a gateway, in Equinox Management. There is a drop-down menu, called **Avaya Recording Gateway**.
- Upload the default audio prompts to the Equinox Recording Gateway.
- Verify that the two new meeting types are displayed in the Equinox Management interface.
- Ensure that you are logged into Equinox Management as an administrator.
- Two meeting types are available and can be selected when configuring your virtual room or scheduling a meeting. They are Audio Service and Audio Service with Web Collaboration.

Chapter 15: Avaya Equinox Solution upgrades

Avaya Equinox® Solution upgrades

For the latest and detailed upgrade procedures (including the backup and restoration of configurations files), see the product's release notes and administrator guides on http://support.avaya.com. Administrator guides are listed in Documentation on page 448.

Chapter 16: Licensing all components of the solution

Introduction to licensing

- Download software from PLDS.
- Activate license entitlement in Avaya PLDS.

See the Version and license steps on page 84 for information on selecting the version and license type after installing Equinox Management.

Equinox Streaming and Recording

After you have applied a license to each of the components of the Avaya Equinox® Streaming and Recording Server, you must register them with the Avaya Equinox® Streaming and Recording Server Manager.

You must register all delivery nodes, virtual delivery nodes, and conference points with the Manager. In addition, you must register the transcoder with the conference point. You do not have to register the transcoder with the Manager.

Downloading software from PLDS

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon ( ) for Company Name.
6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type `Avaya` or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.

7. Search for the available downloads by using one of the following:
   - In **Download Pub ID**, type the download pub ID.
   - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. Scroll down to the entry for the download file, and click the **Download** link.
10. Select a location where you want to save the file, and click **Save**.
11. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.
12. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Checklist for activating licenses

No.	Task	Link/Notes	✔
1	Activate license entitlements on Avaya PLDS.	See Activating license entitlements in Avaya PLDS on page 418. Enter the UUID as the host ID. You can get the UUID from the Equinox Management Installation Wizard (during first install) or from the Equinox Management License information page.	
2	Download the Avaya Equinox® Management software from Avaya PLDS.	See Downloading software from PLDS on page 32	

Related links

Table of host ID sources on page 416
Activating license entitlements in Avaya PLDS on page 418

Table of host ID sources

Product	Host ID Type	Host ID Location
Equinox Management	UUID	• Equinox Management Installation Wizard (during the first install run) • Equinox Management administrator portal **License** information page located at ☰ > **Licensing**.
Equinox Conferencing User License	WebLM Host ID	• **Server Properties** page of the WebLM server.
Equinox Media Server	UUID	• **Info** tab of the Media Server's Device in the Equinox Management administrator portal located at **Devices** > **Media Servers** > **<media server name>** > **Info**.
Equinox WebRTC Gateway	UUID	• **Info** tab of the Gateway's Device in the Equinox Management administrator portal located at **Devices** > **Gateways** > **<gateway name>** > **Info**.
Equinox Web Collaboration Server Scopia® Web Collaboration server?	UUID **Note:** The UUID required here is not the same UUID of the Equinox Media Server OVA. The Scopia® Web Collaboration server requires its own OVA and provides its own UUID.	• **Info** tab of the Web Collaboration Server's Device in the Equinox Management administrator portal located at **Devices** > **Media Servers** > **<web collaboration server name>** > **Info**.
Equinox H.323 Edge (OVA)	UUID **Note:** The Edge Appliance requires MAC Address and Serial Number instead of UUID)	• **System ID** field on the **Info** tab of the H.323 Edge's Device in the Equinox Management administrator portal located at **Devices** > **H.323 Edge Servers** > **<edge server name>** > **Info**.
Equinox Streaming and Recording Server	MAC Address	• **Complete Configuration** screen of the AESR Configuration Utility located at **View Address** or C:\assrconfigtool \MAC_Addresses.txt, see step 12 on page 395 of Configuring the new server on page 391 for details.

Table continues…

Product	Host ID Type	Host ID Location
Equinox Streaming and Recording Media Node	MAC Address	• **Conference Point** license screen, see Applying the license to the recording component (Conference Point) on page 443 for details.
Equinox Streaming and Recording Conference Point	MAC Address	• **Delivery Node** license screen, see Applying the license to the delivery component (Delivery Node or Virtual Delivery Node) on page 444 for details.

Related links

Checklist for activating licenses on page 416

Activating license entitlements in Avaya PLDS

About this task

Use License Activation Code (LAC) to activate license entitlements from the available licenses. After you activate the license entitlements, Avaya PLDS creates an Activation Record and sends an Activation Notification email to the recipient registered with the entitlements, along with anyone added as an email recipient during the activation.

The Activation Record and Activation Notification email contain details of the number of activated licenses and the license host. The email also contains an attachment with the license file or key. You can view the license file or key on the **License/Keys** tab of the Activation Record in Avaya PLDS.

The SAP order and the host ID must be listed under the same company ID.

The easiest way to search for a license entitlement in PLDS is by using the LAC.

Before you begin

Get the following information:

- LAC from the Avaya customer email.
- If you activate license entitlements on:
  - A new license host, get the host ID.
  - An existing license host, get the license host name.
- See, Table of host ID sources on page 416 for the host ID source.

Procedure

1. Go to the Avaya PLDS website at http://plds.avaya.com.
2. Log in to Avaya PLDS using your login credentials.
3. To view your license entitlements, click **Assets** > **View Entitlements**.

   Avaya PLDS displays the Search Entitlements window.

4. In **License Activation Code (LAC)**, type LAC.

   You can get LAC from the Avaya customer email.

5. Click **Search Entitlements**.

   Avaya PLDS displays your license entitlements.

6. To activate a license entitlement, click **Options** > **Activate**.

   Avaya PLDS displays the list of available licenses in the Search Entitlements to Activate window. Avaya PLDS automatically selects all licenses in the window with the maximum quantity for activation.

   Note:

   For each OVA (UUID) you must activate the license on a unique license host.

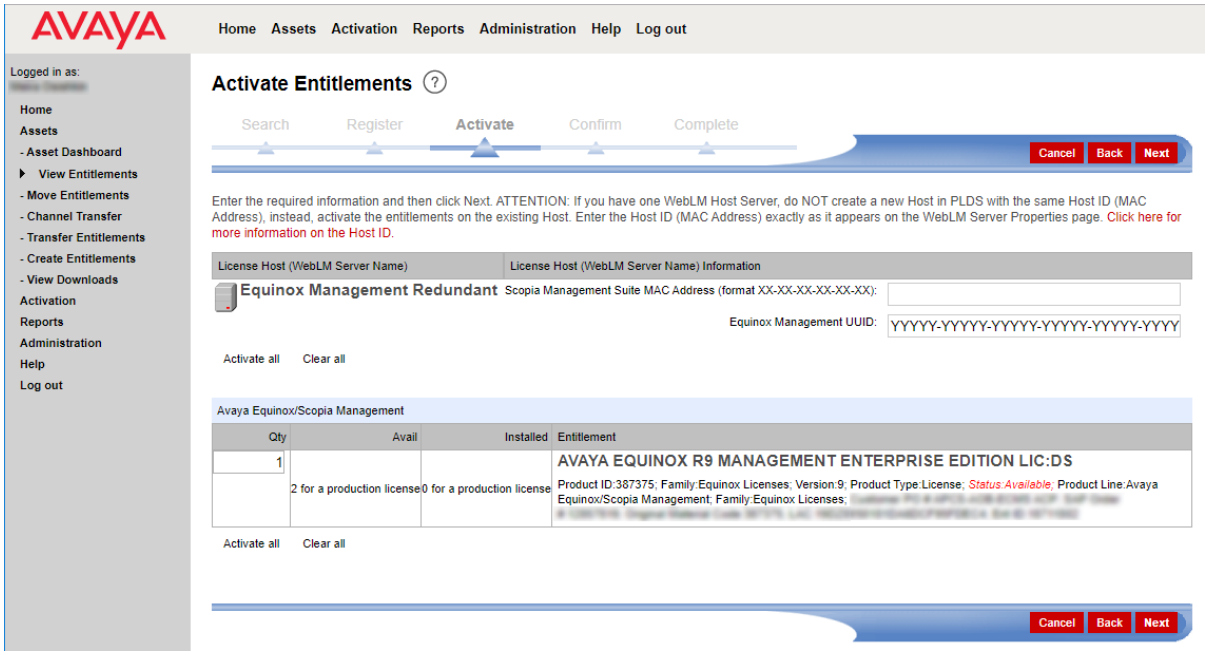
7. Select the license entitlements that you want to activate.

8. Click **Activate**.

9. In the **Search License Hosts** window search for a license host name or enter the host ID, and click **Search License Hosts (WebLM Server Name)**.

   You can also create a new license host using the **Add a License Host** option.

   Avaya PLDS displays the list of selected licenses to activate in the Activate Entitlements window.



10. Enter the quantity of licenses to activate for each license entitlement, and click **Next**.

    The default quantity the system displays in the Qty box is the maximum available. You must change this to a quantity of 1.

11. Review and accept the Avaya end user license agreement.
12. To send the license activation record in an email, in the **Confirmation Information** section, enter the following information for the email recipient:
    - **Result output**
    - **Email to**
    - **Language**
    - **Comments**
13. **(Optional)** In the **Notes for this transaction** section, enter the notes for the license activation transaction.
14. Click **Finish**.

Example

A customer purchases two AEMG licenses for an Equinox Management deployment with redundancy. PLDS displays it as a single license entitlement with a quantity of two.

The customer must activate each license separately using a quantity of 1 each time, each on a unique license host and with a unique UUID.

Related links

Checklist for activating licenses on page 416

Updating the Equinox Management license

About this task

This task describes how to update the Equinox Management license.

Procedure

1. In Avaya Equinox® Management, click ☰ > **Licensing**.

   The system displays the **License Information** page.

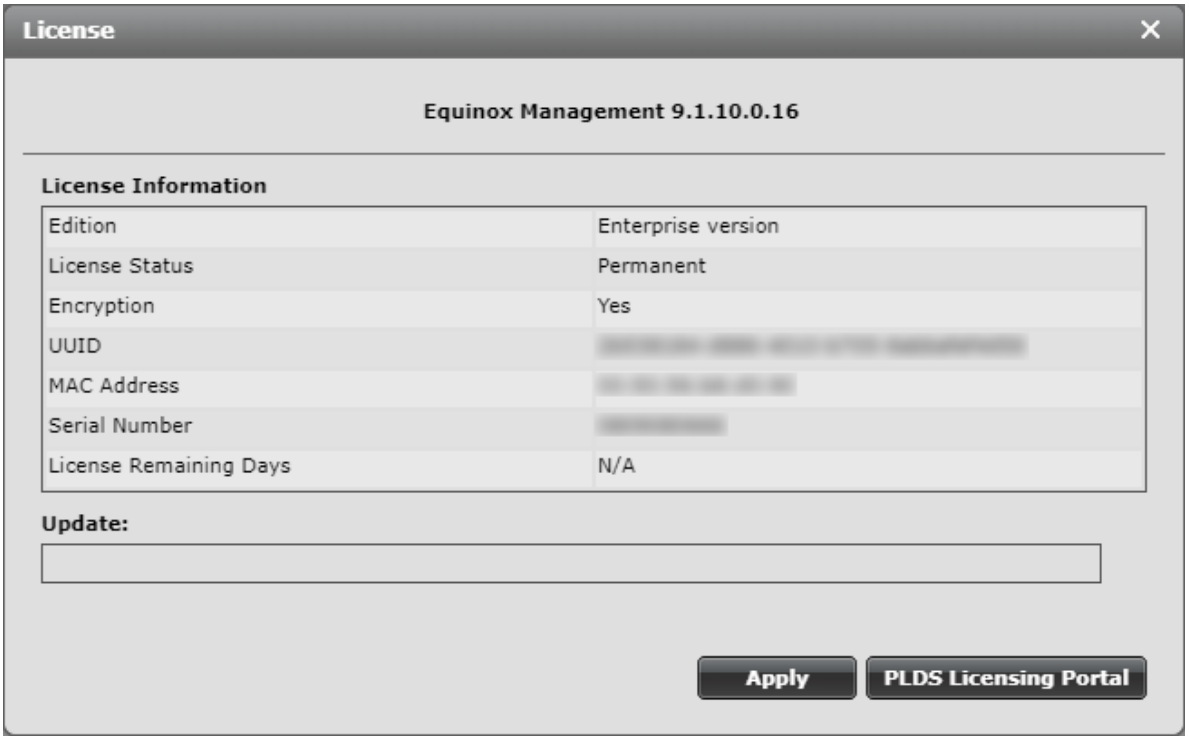


Figure 117: License information page

An explanation of the fields on this page is in Table 66: License information page on page 421.

Table 66: License information page

Field Name	Description
Edition	The license edition.
License Status	When value = **Permanent**, indicates that the activation key input is correct. When value = **Temporary**, the license is valid only for 30 days.
Encryption	Indicates whether the license is encrypted (**Yes**) or non-encrypted (**No**).
UUID	The Equinox Management's Universally Unique Identifier. It is used as the host ID for generating the Equinox Management license in PLDS.
MAC Address	The Equinox Management's MAC Address.
Serial Number	The Equinox Management's serial number.
License Remaining Days	The number of days remaining before the license expires.

2. To update the system with a new license, enter the license key in the **Update** field.

3. Click **Apply**.

Managing Licenses Via the Web-based License Manager (WebLM)

Avaya provides a Web-based License Manager (WebLM) to manage licenses of one or more Avaya software products for your organization. WebLM facilitates easy tracking of licenses. To track and manage licenses in an organization, WebLM requires a license file from the Avaya Product Licensing and Delivery System (PLDS) web site at https://plds.avaya.com.

The license file of a software product is in XML format and contains information regarding the product, the major release, the licensed features of the product, and the licensed capacities of each feature that you purchase. After purchasing a licensed Avaya software product, you must activate the license file for the product in PLDS and install the license file on the WebLM server. License activations in PLDS require the host ID of the WebLM server for inclusion in the license file. The host ID displays on the Server Properties page of the WebLM server.

You can choose to manage your licenses with a local WebLM server or with an external WebLM server. The internal WebLM server conserves hardware resources, while the external WebLM server can be used to support redundancy and other Avaya products which are part of the deployment.

Related links

Installing a user license on the local WebLM server on page 422
Installing the User License On the External WebLM Server on page 425

Installing a user license on the local WebLM server

About this task

This procedure describes how to install a license on the local WebLM server. A local WebLM server is installed in the same application zone as the Equinox Management server.

Before you begin

Deploy the Equinox Management OVA, as described in Deploying the Equinox Management Server on page 67.

Procedure

1. Log into your local WebLM server, using the following URL: `https://<Your Server IP>:443/WebLM/LicenseServer`.

   The default login credentials are:

   - Username: **admin**
   - Password: **weblmadmin**

   After initial login, you are prompted to change your password.

2. On the local WebLM server UI, click **Server properties**.

   The system displays the **Server Properties** page, with the server's host ID which you use to get a license from the PLDS site.

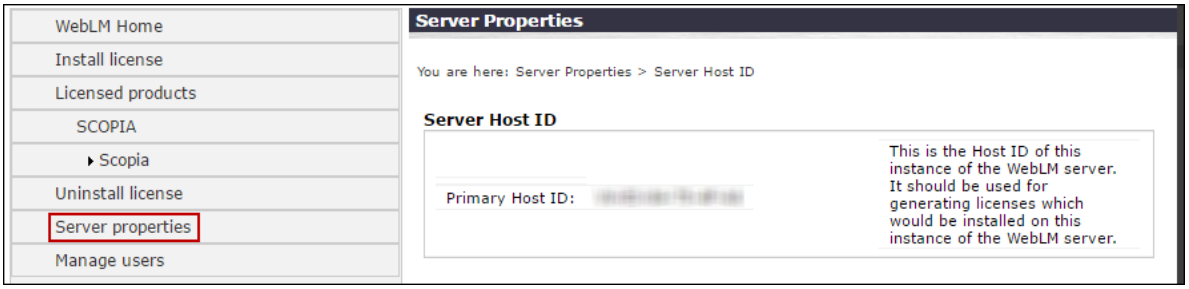


Figure 118: Server Properties page

3. Retrieve the license from the PLDS site. For details on using PLDS, see *Getting Started with Avaya PLDS - Avaya Partners and Customers* at https://plds.avaya.com.

4. Click **Install license** on the WebLM server UI.

   The system displays the **Install License** page.

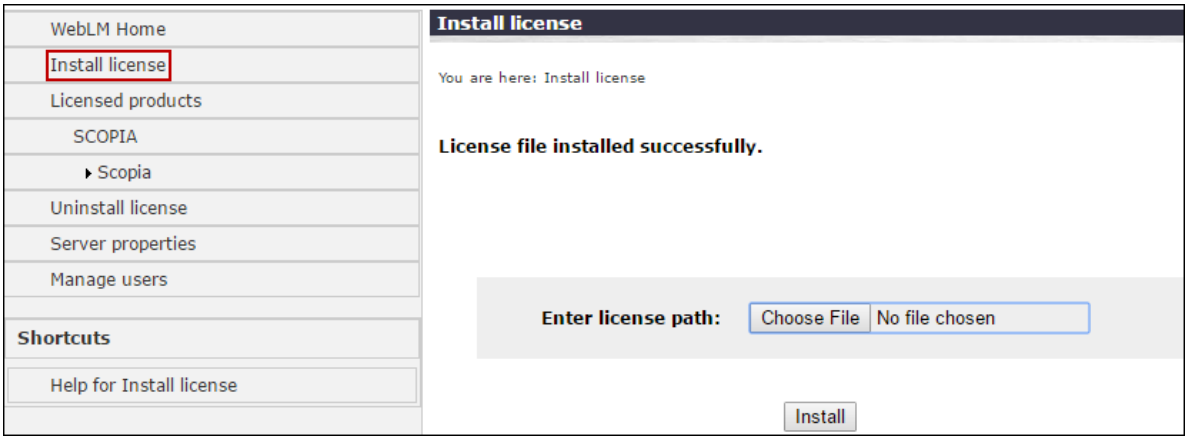


Figure 119: Install License page

5. Click **Choose File** in the **Enter license path** field, and after choosing your license file, click **Install** to install the license file.

   The system displays the **Licensed Features** page, where you verify the license status.

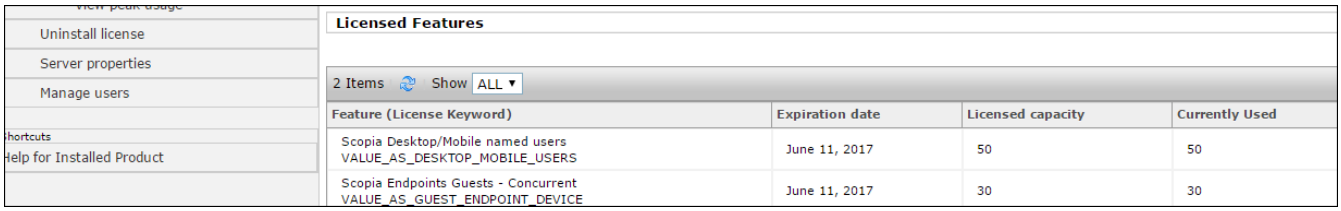


Figure 120: Licensed Features page

6. Verify the license in Equinox Management, as follows:
   a. In the Equinox Management administrator portal, click **Settings** > **Servers** > **License Server**.

      The system displays the **License Server** page.

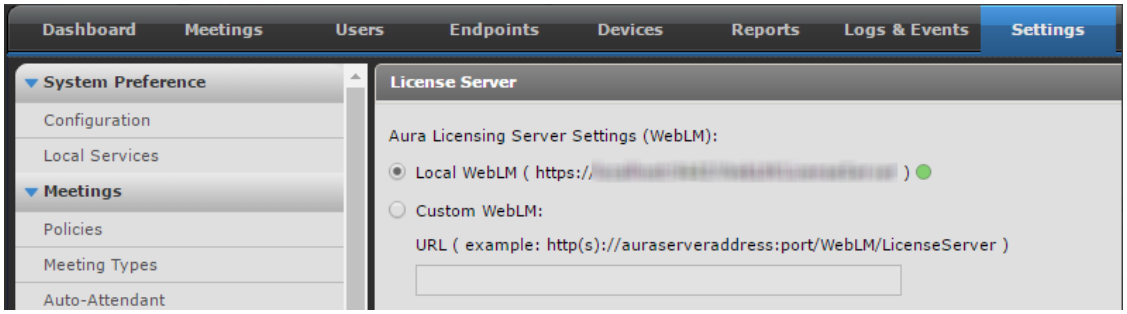


Figure 121: License Server page

   b. Click **Apply**.

   c. Click ☰ > **Restart** to restart the Equinox Management server OVA.

      The system displays the local WebLM status with a green icon (active).

   d. To verify license installation, click ☰ > **Licensing**. The system displays the **License Information** page, displaying information on the installed license.

License Information

Edition	Enterprise
Equinox Management Activation Status	Permanent
Encryption	true
Golden Users	50
Endpoint Guest Access Licenses	30
License Status	Normal
License Remaining Days	121
UUID	
MAC Address	
Serial Number	0809080666

Figure 122: License Information page

      There is an explanation of the fields on this page in Table 67: License Information page on page 425.

Table 67: License Information page

Field Name	Description
Edition	The license edition.
Equinox Management Activation Status	When value = **Permanent**, indicates that the activation key input is correct. When value = **Temporary**, the license is valid only for 30 days.
Encryption	Indicates whether the license is encrypted (**true**) or non-encrypted (**false**).
Power Suite Licenses (users)	The number of users who have recording privileges. Power suite license users also have their own virtual meeting room.
3rd Party Video Connectivity	The number of third party (non-Avaya) video room systems that can connect to a conference.
License Status	• **Normal**: Indicates that there is no license error. • **Error**: Indicates that there is a license error. A grace period exists for the license, and the operation mode is normal. • **Restricted**: Indicates that there is a license error, the grace period has expired, and the operation mode is restricted. When the license status is **Restricted**, the administrator must request a new license and apply it to the license server.
License Remaining Days	The number of days remaining before the license expires.
UUID	Used to generate the user based license.
MAC Address	Used for displaying the user based license.
Serial Number	The license's serial number.

Related links

Managing Licenses Via the Web-based License Manager (WebLM) on page 422

Installing the User License On the External WebLM Server

About this task

This procedure describes how to install the user license on the external WebLM server.

Before you begin

Deploy the Equinox Management OVA, as described in Deploying the Equinox Management Server on page 67.

Procedure

1. Update the Equinox Management server and remote WebLM server with third party certificates. Both certificates must be signed by the same server and have the same root certificate.
2. Log into the Avaya Aura® System Manager WebLM server, using the following URL: `https://<System Manager IP>:443/WebLM/LicenseServer`.

   The default login credentials are:

   - Username: **admin**
   - Password: **weblmadmin**

   After initial login, you are prompted to change your password.
3. On the WebLM server UI, click **Server properties**.

   The system displays the **Server Properties** page with the server's host ID, which you use to get a license from the PLDS site.

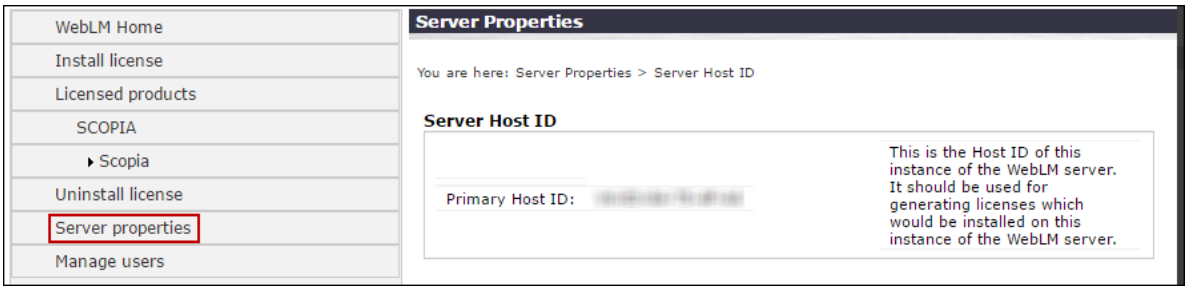


Figure 123: Server Properties page

4. Retrieve the license from the PLDS site. For details on using PLDS, see *Getting Started with Avaya PLDS - Avaya Partners and Customers* at https://plds.avaya.com.
5. Click **Install license** on the WebLM server UI.

   The system displays the **Install License** page.

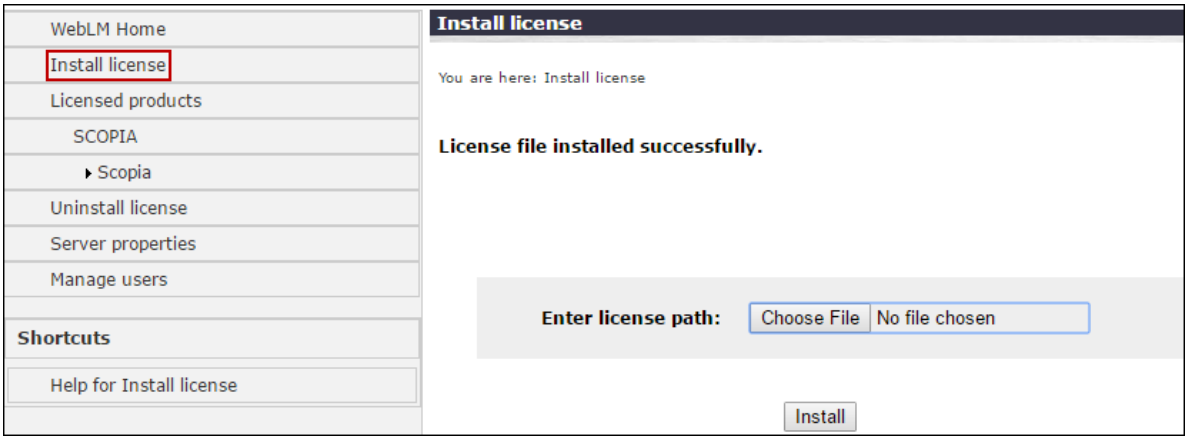


Figure 124: Install License page

6. Click **Choose File** in the **Enter license path** field, and after choosing your license file, click **Install** to install the license file.

   The system displays the **Licensed Features** page, where you verify the license status.

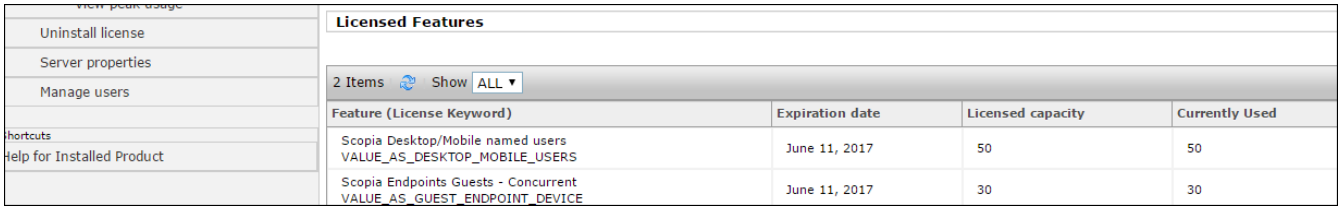


Figure 125: Licensed Features page

7. In the Equinox Management administrator portal, click **Settings** > **Servers** > **License Server**, and click the **Apply** button.

   The system displays the **License Server** page.

8. Select **Custom WebLM** and enter the URL of your external WebLM server. The address must be entered in the following format: `https://<FQDN management server address>/WebLM/LicenseServer`

   The system displays the remote WebLM server status next to the URL field with a red icon (inactive).

   Note:

   No authentication is necessary for Equinox Management to connect to the WebLM server.

9. Click **Apply** to restart and activate Equinox Management's connection to the WebLM server.

   The system displays the remote WebLM server status with a green icon (active).

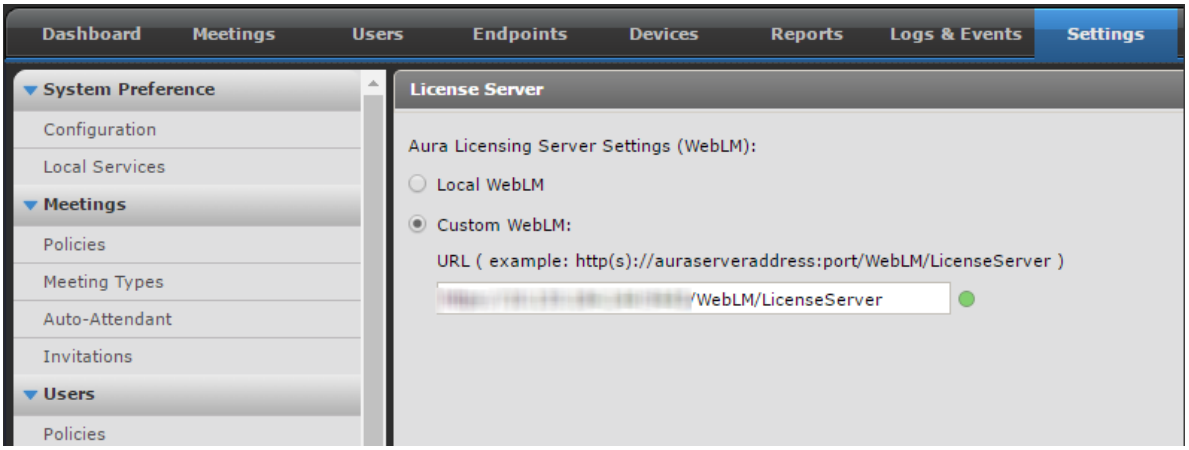


Figure 126: License Server page

10. Verify license installation by clicking ☰ > **License Information**.

The system displays the **License Information** page, displaying information on the installed license.



Figure 127: License Information page

There is an explanation of the fields on this page in Table 68: License Information page on page 428.

Table 68: License Information page

Field Name	Description
Edition	The license edition.
Equinox Management Activation Status	When value = **Permanent**, indicates that the activation key input is correct. When value = **Temporary**, the license is valid only for 30 days.
Encryption	Indicates whether the license is encrypted (**true**) or non-encrypted (**false**).

Table continues…

Field Name	Description
License Status	• **Normal**: Indicates that there is no license error. • **Error**: Indicates that there is a license error. A grace period exists for the license, and the operation mode is normal. • **Restricted**: Indicates that there is a license error, the grace period has expired, and the operation mode is restricted. When the license status is **Restricted**, the administrator must request a new license and apply it to the license server.
Power Suite Licenses (users)	The number of users who have recording privileges. Power suite license users also have their own virtual meeting room.
3rd Party Video Connectivity	The number of third party (non-Avaya) video room systems that can connect to a conference.
License Remaining Days	The number of days remaining before the license expires.
UUID	Used to generate the user based license.
MAC Address	Used for displaying the user based license.
Serial Number	The license's serial number.

11. In the **Activation Key** field, enter the activation key for the Equinox Management server.
12. Click **Apply** to apply the activation key.

Related links

Managing Licenses Via the Web-based License Manager (WebLM) on page 422

Avaya Equinox Media Server license configuration

Checklist for configuring Avaya Equinox® Media Server licenses

No.	Task	Link/Notes	✔
1	Activate license entitlements on Avaya PLDS.	See Activating license entitlements in Avaya PLDS on page 430 Enter the Avaya Equinox® Media Server UUID as the host ID. You can get UUID from the Info tab of the specific Avaya Equinox® Media Server registered to Avaya Equinox® Management.	
2	Download the Avaya Equinox® Media Server software from Avaya PLDS.	See Downloading software from PLDS on page 32	
3	Apply the Avaya Equinox® Media Server license in Avaya Equinox® Management.	See Applying the Avaya Equinox® Media Server licenses on page 432	

Activating license entitlements in Avaya PLDS

About this task

Use License Activation Code (LAC) to activate license entitlements from the available licenses. After you activate the license entitlements, Avaya PLDS creates an Activation Record and sends an Activation Notification email to the recipient registered with the entitlements, along with anyone added as an email recipient during the activation.

The Activation Record and Activation Notification email contain details of the number of activated licenses and the license host. The email also contains an attachment with the license file or key. You can view the license file or key on the License/Keys tab of the Activation Record in Avaya PLDS.

Before you begin

Get the following information:

- LAC from the Avaya customer email.
- If you activate license entitlements on:
  - A new license host, get the host ID.
  - An existing license host, get the license host name.

Procedure

1. Go to the Avaya PLDS website at http://plds.avaya.com.
2. Log in to Avaya PLDS using your login credentials.

3. To view your license entitlements, click **Assets** > **View Entitlements**.

   Avaya PLDS displays the Search Entitlements window.

4. In **License Activation Code (LAC)**, type LAC.

   You can get LAC from the Avaya customer email.

5. Click **Search Entitlements**.

   Avaya PLDS displays your license entitlements.

6. To activate a license entitlement, click **Options** > **Activate**.

   Avaya PLDS displays the list of available licenses in the Search Entitlements to Activate window. Avaya PLDS automatically selects all licenses in the window with the maximum quantity for activation.

7. Clear the selection of licenses that you do not want to activate.

8. Click **Activate**.

   Avaya PLDS displays the list of available license hosts in the Search License Hosts window.

9. Click **Add a License Host**.

   Avaya PLDS displays the Add License Host window.

10. In **License Host**, enter the name of the license host, and click **Save**.

    For example, enter `Avaya Equinox H.323 Edge`.

    Avaya PLDS displays the Registration window.

11. Verify the license entitlement details, and click **Next**.

    Avaya PLDS displays the Activate Entitlements window.

12. In **Equinox H.323 Edge UUID/System ID**, enter the Avaya Equinox® H.323 Edge system ID.

13. Enter the quantity of licenses to activate for each license entitlement, and click **Next**.

14. Review and accept the Avaya end user license agreement.

15. **(Optional)** To send the license activation record in an email, in the **Confirmation Information** section, enter the following information for the email recipient:

    - **Result output**
    - **Email to**
    - **Language**
    - **Comments**

16. **(Optional)** In the **Notes for this transaction** section, type the notes for the license activation transaction.

17. Click **Finish**.

Applying the Avaya Equinox® Media Server licenses

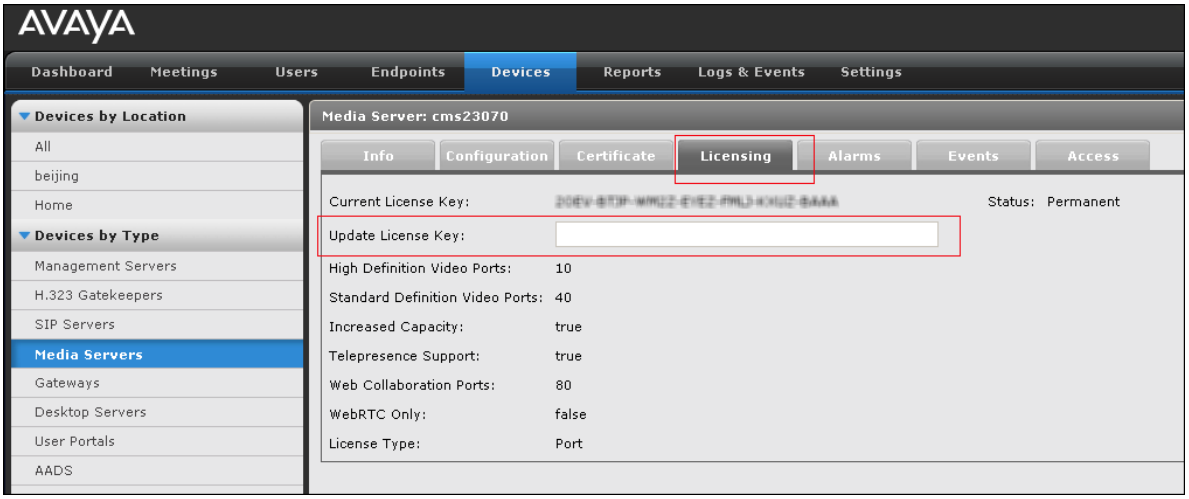
Before you begin

- Get the License Authentication Code (LAC) file from the Avaya customer email.
- Activate the license entitlements for Avaya Equinox® Media Server.
- Ensure that new Avaya Equinox® Media Server license supports encryption.

Procedure

1. Log in to Avaya Equinox® Management.
2. Click **Devices**, and select the Avaya Equinox® Media Server instance from the list of media servers.

   Avaya Equinox® Management displays the Avaya Equinox® Media Server instance page.
3. Click the **Licensing** tab.



4. In **Update License Key**, copy and paste or type the license key.
5. Click **Apply**.

Result

Avaya Equinox® Management restarts Avaya Equinox® Media Server to apply the new license.

Avaya Equinox H.323 Edge license configuration

Checklist for configuring Avaya Equinox® H.323 Edge licenses

No.	Task	Link/Notes	✔
1	Get the Avaya Equinox® H.323 Edge UUID, also called the host ID or the system ID.	See Getting the system ID to activate Equinox H.323 Edge on page 433	
2	Activate license entitlements on Avaya PLDS.	See Activating license entitlements in Avaya PLDS on page 430	
3	Download the Avaya Equinox® H.323 Edge software from Avaya PLDS.	See Downloading software from PLDS on page 32	
4	Apply the Avaya Equinox® H.323 Edge license in Avaya Equinox® Management.	See Adding and updating licenses on page 436	

Getting the system ID to activate Equinox H.323 Edge

About this task

You need the system ID of Equinox H.323 Edge to activate the server.

If you deploy the hardware server, see the customer letter for the system ID.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Equinox H.323 Edge instance.
3. On the Info tab, note **UUID**.

Next steps

Add the Equinox H.323 Edge license to activate the server.

Activating license entitlements in Avaya PLDS

About this task

Use License Activation Code (LAC) to activate license entitlements from the available licenses. After you activate the license entitlements, Avaya PLDS creates an Activation Record and sends an Activation Notification email to the recipient registered with the entitlements, along with anyone added as an email recipient during the activation.

The Activation Record and Activation Notification email contain details of the number of activated licenses and the license host. The email also contains an attachment with the license file or key.

You can view the license file or key on the License/Keys tab of the Activation Record in Avaya PLDS.

Before you begin

Get the following information:

- LAC from the Avaya customer email.
- If you activate license entitlements on:
  - A new license host, get the host ID.
  - An existing license host, get the license host name.

Procedure

1. Go to the Avaya PLDS website at http://plds.avaya.com.
2. Log in to Avaya PLDS using your login credentials.
3. To view your license entitlements, click **Assets** > **View Entitlements**.

   Avaya PLDS displays the Search Entitlements window.
4. In **License Activation Code (LAC)**, type LAC.

   You can get LAC from the Avaya customer email.
5. Click **Search Entitlements**.

   Avaya PLDS displays your license entitlements.
6. To activate a license entitlement, click **Options** > **Activate**.

   Avaya PLDS displays the list of available licenses in the Search Entitlements to Activate window. Avaya PLDS automatically selects all licenses in the window with the maximum quantity for activation.
7. Clear the selection of licenses that you do not want to activate.
8. Click **Activate**.

   Avaya PLDS displays the list of available license hosts in the Search License Hosts window.
9. Click **Add a License Host**.

   Avaya PLDS displays the Add License Host window.
10. In **License Host**, enter the name of the license host, and click **Save**.

    For example, enter `Avaya Equinox H.323 Edge`.

    Avaya PLDS displays the Registration window.
11. Verify the license entitlement details, and click **Next**.

    Avaya PLDS displays the Activate Entitlements window.
12. In **Equinox H.323 Edge UUID/System ID**, enter the Avaya Equinox® H.323 Edge system ID.

13. Enter the quantity of licenses to activate for each license entitlement, and click **Next**.
14. Review and accept the Avaya end user license agreement.
15. **(Optional)** To send the license activation record in an email, in the **Confirmation Information** section, enter the following information for the email recipient:
    - **Result output**
    - **Email to**
    - **Language**
    - **Comments**
16. **(Optional)** In the **Notes for this transaction** section, type the notes for the license activation transaction.
17. Click **Finish**.

Downloading software from PLDS

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon ( ) for Company Name.
6. In the Search Companies dialog box, do the following:
    a. In the **%Name** field, type `Avaya` or the Partner company name.
    b. Click **Search Companies**.
    c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
    - In **Download Pub ID**, type the download pub ID.
    - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. Scroll down to the entry for the download file, and click the **Download** link.
10. Select a location where you want to save the file, and click **Save**.
11. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.
12. **(Optional)** When the system displays the security warning, click **Install**.

When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Adding and updating licenses

About this task

Update licenses when you increase the Equinox H.323 Edge capacity or increase the number of ports with a flexible license.

If you upgrade Equinox H.323 Edge to a major version, you must have a new license.

Before you begin

- Download the Equinox H.323 Edge upgrade package at https://plds.avaya.com/.
- Ensure that new license of the upgrade package supports encryption.
- Get the Equinox H.323 Edge System ID.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Equinox H.323 Edge instance.

   Equinox Management displays the Equinox H.323 Edge instance page.
3. Click the **Licensing** tab.
4. In **Update License Key**, type the license key.
5. Click **Apply**.

Result

Equinox Management activates the new Equinox H.323 Edge license.

Checklist for configuring Avaya Equinox® Streaming and Recording Server licenses

Follow the steps in this checklist to license the Avaya Equinox® Streaming and Recording Server (Equinox Streaming and Recording).

No.	Task	Description	Notes	✔
1	Set the IP address of each of the remaining components. You have already set the IP address of the Equinox Streaming and Recording Manager.	Setting the IP address of the recording component (Conference Point) on page 437 Setting the IP address of the delivery component (Delivery Node) on page 442		
2	Restart services.	Restarting services on page 442		
3	Apply the license to each of the components.	Applying the license to the management component on page 443 Applying the license to the recording component (Conference Point) on page 443 Applying the license to the delivery component (Delivery Node) on page 444	You must apply the license to all components.	
4	Verify license information.	Viewing license information on page 444		

Related links

Setting the IP address and hostname of the recording component (Conference Point) on page 437
Setting the IP address and hostname of the delivery component (Delivery Node) on page 442
Restarting services on page 442
Applying the license to the management component on page 443
Applying the license to the recording component (Conference Point) on page 443
Applying the license to the delivery component (Delivery Node or Virtual Delivery Node) on page 444
Viewing license information on page 444

Setting the IP address and hostname of the recording component (Conference Point)

The recording component is known as the conference point or CP.

You can configure the IP address in the Equinox Streaming and Recording Administration GUI but you can only configure the hostname using the following method.

About this task

You should set an IPv4 address.

Before you begin

Obtain the Avaya Equinox® Streaming and Recording Server license keys from the Avaya Product Licensing and Delivery System (PLDS).

Procedure

1. Double-click on the Hyper-V Manager shortcut on the desktop.
2. In the Virtual Machines panel, double-click on the **CP** entry.

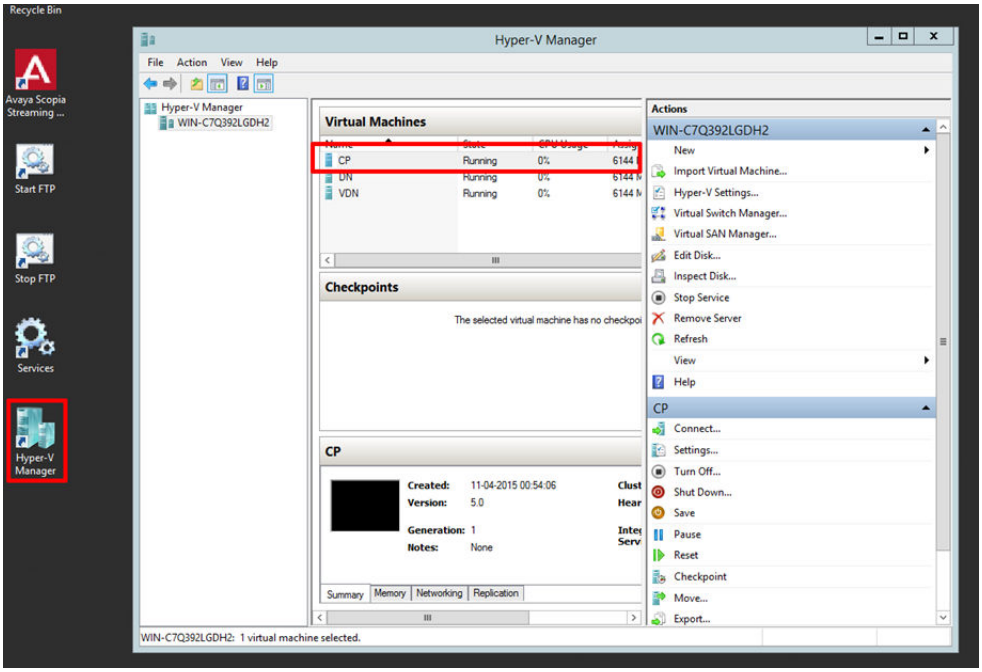


Figure 128: Hyper-V Manager

3. Log in to the Conference Point (CP) on the console as `admin`.

   The default password is `admin`.

   If this is the first time that you have logged into the CP, you are prompted to change your password.

4. **(Optional)** If you are using DHCP, retrieve your IP address and make a note of it.
   a. Run `ifconfig`.
   b. Look at `inet addr` for `eth0`.

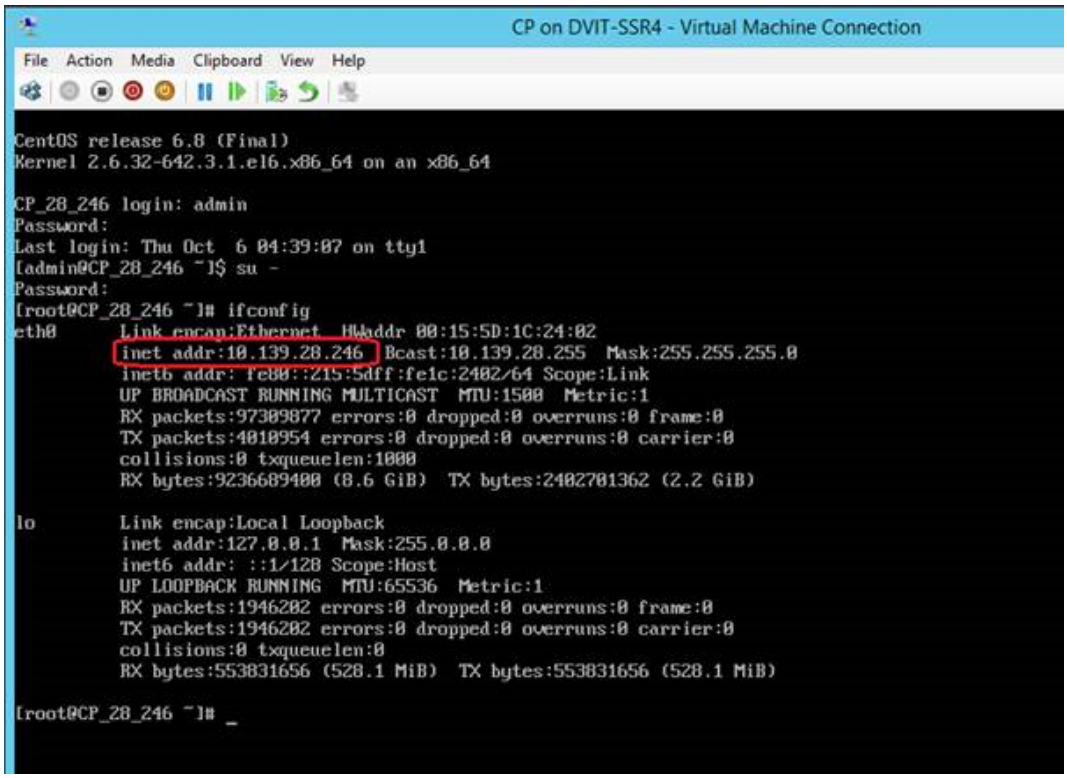


Figure 129: Retrieving the IP Address

5. Type `network` to open the configuration screens.
6. On the Terminal window, highlight **Device configuration** and press `Enter`.

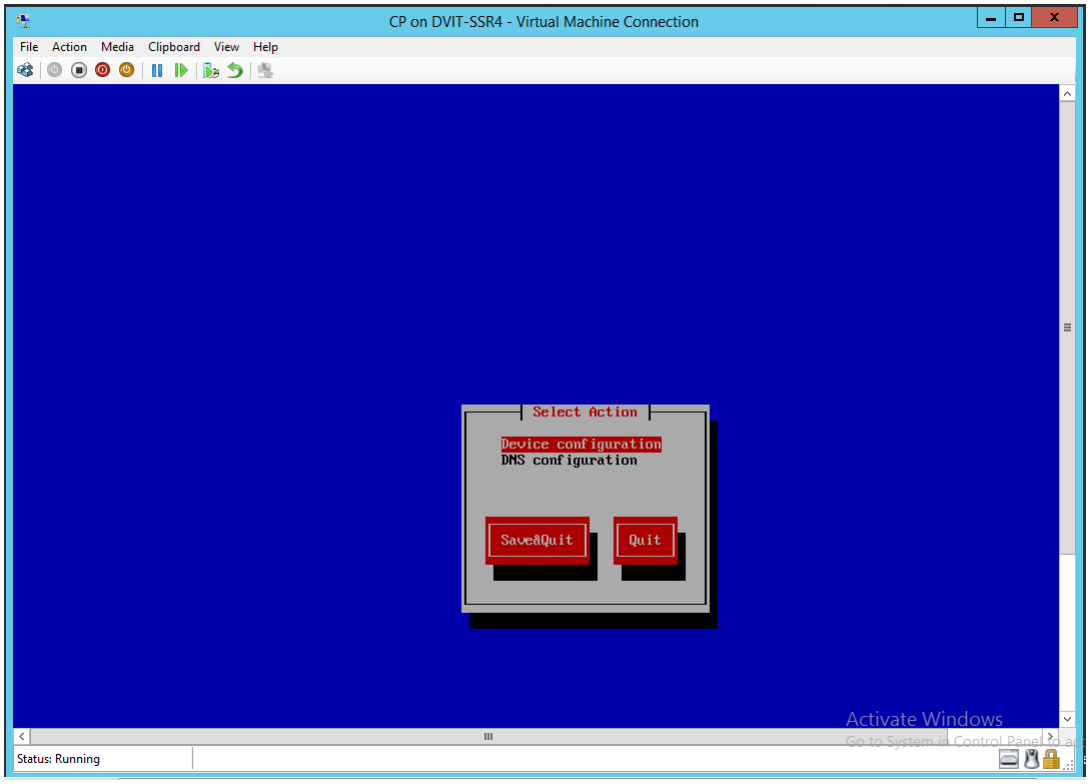


Figure 130: Device Configuration

7. On the Select A Device window, highlight **eth0** and press `Enter`.
8. Use the **Tab** key to navigate to the other fields and configure the following details:
   - **Use DHCP**: Disable DHCP by pressing the **Spacebar**.
   - **Static IP**: Enter a value.
   - **Netmask**: Enter a value.
   - **Default gateway IP**: Enter a value.
   - **Primary DNS Server**: Leave blank.
   - **Secondary DNS Server**: Leave blank.
   - **Peer DNS**: Disable.
   - **On boot**: Enable.
   - **Controlled by NeworkManager**: Enable.

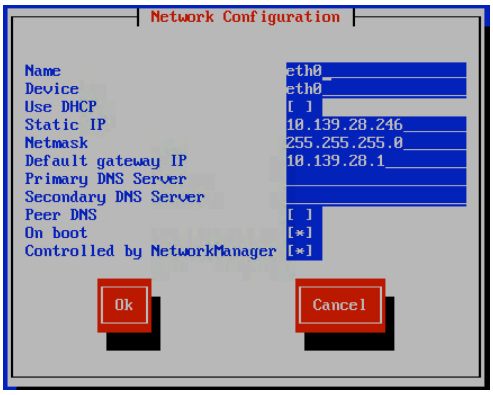


Figure 131: Network Configuration

9. Use the **Tab** key to highlight **Ok** and press `Enter`.
10. On the Select A Device window, use the **Tab** key to highlight **Save** and press `Enter`.
11. On the Select Action window, use the **Tab** key to highlight **DNS Configuration** and press `Enter`.
12. Use the **Tab** key to navigate to the other fields and configure the following details:
    - **Hostname**: Enter a value.
    - **Primary DNS**: Enter a value.
    - **Secondary DNS**: Optionally, enter a value.
    - **Tertiary DNS**: Optionally, enter a value.
    - **DNS search path**: Optionally, enter a value.

    Note:

    This is the only menu that enables you to configure the hostname.

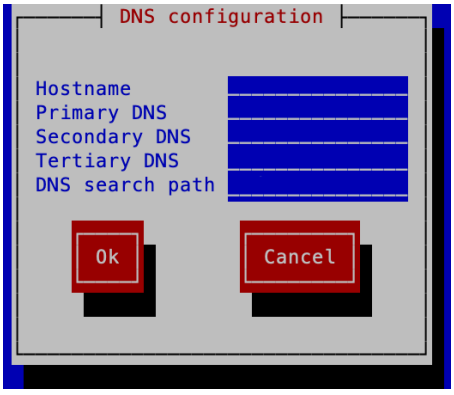


Figure 132: DNS Configuration

13. Use the **Tab** key to highlight **Ok** and press `Enter`.
14. On the Select Action window, use the **Tab** key to highlight **Save** and press `Enter`.

15. In the terminal window, type `sudo service network restart` to restart network services.

Next steps

Return to the Licensing checklist on page 436 to see your next task.

Related links

Checklist for configuring Avaya Equinox Streaming and Recording Server licenses on page 436

Setting the IP address and hostname of the delivery component (Delivery Node)

A Delivery Node (DN) can be a Virtual Delivery Node (VDN). You should only use a VDN if you subscribe to the Highwinds Content Delivery Network (CDN). CDN is a cloud-based streaming system. The delivery component is also called streaming.

Procedure

Use the same set of steps that you used for Setting the IP address and hostname of the recording component (Conference Point) on page 437.

Next steps

Return to the Licensing checklist on page 436 to see your next task.

Related links

Checklist for configuring Avaya Equinox Streaming and Recording Server licenses on page 436

Restarting services

About this task

The services that you must restart are:

- Apache Tomcat
- Apache 2.4
- Avaya Equinox® Streaming and Recording Server Transcoder

Procedure

1. Double-click on the Services icon on the desktop.
2. On the Services screen, right-click **Apache Tomcat 7.0 Tomcat7** and select **Restart** from the menu options.
3. Right-click **Apache2.4** and select **Restart** from the menu options.
4. Right-click **Avaya Equinox Streaming & Recording Transcoder** and select **Restart** from the menu options.

Next steps

Return to the Licensing checklist on page 436 to see your next task.

Related links

Checklist for configuring Avaya Equinox Streaming and Recording Server licenses on page 436

Applying the license to the management component

Procedure

1. Type `https://<Equinox SR Manager FQDN/IP address>:8445` in a web browser.
2. If this is the first time that you have logged in to the system, you are prompted to update your password.

   The preset credentials are:

   - Username: `admin`
   - Password: `admin`
3. At the prompt, enter the license key in the **License Information** field and click **Update**.
4. Refresh the browser.

Next steps

Return to the Licensing checklist on page 436 to see your next task.

Related links

Checklist for configuring Avaya Equinox Streaming and Recording Server licenses on page 436

Applying the license to the recording component (Conference Point)

Procedure

1. See Configuring the new server on page 391 for the location of the MAC address.
2. Open a browser and type the Conference Point (CP) IP address or fully qualified domain name (FQDN).
3. On the Conference Point license screen, enter the license key in the **License Key** field and click **Submit**.

Next steps

Return to the Licensing checklist on page 436 to see your next task.

Related links

Checklist for configuring Avaya Equinox Streaming and Recording Server licenses on page 436

Applying the license to the delivery component (Delivery Node or Virtual Delivery Node)

There can only be a single virtual delivery node (VDN) in a deployment.

Procedure

1. Open a browser and type the delivery node (DN) or virtual delivery node (VDN) IP address or fully qualified domain name (FQDN).
2. On the Delivery Node license screen, enter the license key in the **License Key** field and click **Submit**.
3. Select the type of delivery node.

   The available options are:

   - DN (Delivery Node)
   - VDN (Virtual Delivery Node)
4. Click **Submit**.

   The DN or VDN is ready for use. The login screen is displayed.

Next steps

Return to the Installation checklist on page 385 to see your next task.

Related links

Checklist for configuring Avaya Equinox Streaming and Recording Server licenses on page 436

Viewing license information

You can view license information for the management component, the delivery component (Delivery Node), and the recording component (Conference Point).

Related links

Checklist for configuring Avaya Equinox Streaming and Recording Server licenses on page 436
Viewing license information for the management component on page 444
Viewing license information for the conference point on page 445
Viewing license information for the delivery node on page 446

Viewing license information for the management component

Procedure

1. Log in to Equinox Streaming and Recording. The following credentials are the default credentials, but when you first log in, you are prompted to update your password:

   - Username: `admin`

- Password: `admin`

2. Select the **Devices** tab.
3. View the license information for the management component in the **License Information** panel.

Note:

If you have a demonstration license, you can view the expiration date.

Related links

Viewing license information on page 444

Viewing license information for the conference point

The recording component is called a conference point or CP.

Procedure

1. Log in to Equinox Streaming and Recording. The following credentials are the default credentials, but when you first log in, you are prompted to update your password:
   - Username: `admin`
   - Password: `admin`
2. Select the **Devices** tab.
3. From the **Browse** menu on the left, click **Conference Points**.
4. On the Conference Points page, view the **License Status** column to see the status of the license.
5. Follow the remaining steps if you require more detailed license information.
6. Click the name of the conference point to display the conference point details.

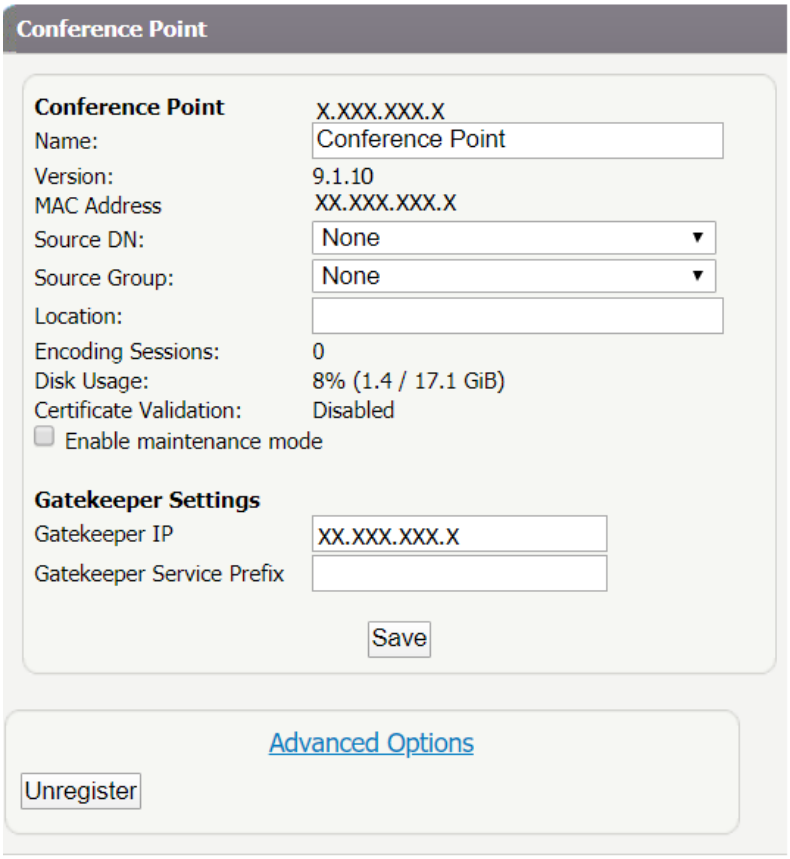


Figure 133: Conference Point Details

7. Click the **Conference Point** IP address link to access the conference point.
8. Log in to the conference point. The following credentials are the default credentials, but when you first log in, you are prompted to update your password:
   - Username: `administrator`
   - Password: `administrator`
9. Click **System Configuration** > **License Information** to view the license information for the recording component.

Related links

Viewing license information on page 444

Viewing license information for the delivery node

The delivery component is called a delivery node or DN.

Procedure

1. Log in to Equinox Streaming and Recording. The following credentials are the default credentials, but when you first log in, you are prompted to update your password:
   - Username: `admin`

- Password: `admin`

2. Select the **Devices** tab.
3. From the **Browse** menu on the left, click **Delivery Nodes**.
4. On the Delivery Nodes page, view the **License Status** column to see the status of the license.
5. Follow the remaining steps if you require more detailed license information.
6. Click the name of the delivery node to display the delivery node details.
7. Click the **Delivery Node** IP address link to access the delivery node.
8. Log in to the delivery node. The following credentials are the default credentials, but when you first log in, you are prompted to update your password:
   - Username: `administrator`
   - Password: `administrator`
9. From the menu across the top, click **Upgrade**.
10. View the license information for the delivery component in the **Current License Information** panel.

Related links

Viewing license information on page 444

Chapter 17: 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: Avaya Equinox® Team Engagement hardened deployment

This section lists procedures for hardening Avaya Equinox® Conferencing components in Team Engagement deployments.

Disclaimer

In order to deploy a fully hardened solution, you must implement hardening for each component on your network.

If you wish to deploy a hardened solution, as described here, you must contact Avaya Support for assistance. This hardening method is only available for new installations of Avaya Equinox® Team Engagement 9.1.9.

Related links

Overview of the hardened solution on page 456
Configuration checklist for hardening the backend Avaya Aura Media Server on page 460
Configuration checklist for hardening the frontend Avaya Aura Media Server on page 462
Configuring Avaya Aura Media Server for encrypted transfer of audit logs and syslogs to a log aggregation server on page 465
Configuring encrypted NTP time source messages in Avaya Aura Media Server on page 466
Configuration checklist for Avaya Equinox® Management hardening on page 467
Configuration checklist for hardening Avaya Aura Web Gateway on page 467

Overview of the hardened solution

With Release 9.1.9, Avaya provides a hardened version of Avaya Equinox® for Team Engagement. The Team Engagement deployment includes Avaya Equinox® Conferencing and Avaya Aura® components.

The solution implements FIPS-compliant security standards in commercial organizations and is only available for new installations of Release 9.1.9.

The solution also uses the Avaya Aura® Media Server software to support the video switching fabric feature, as shown in the following figure.

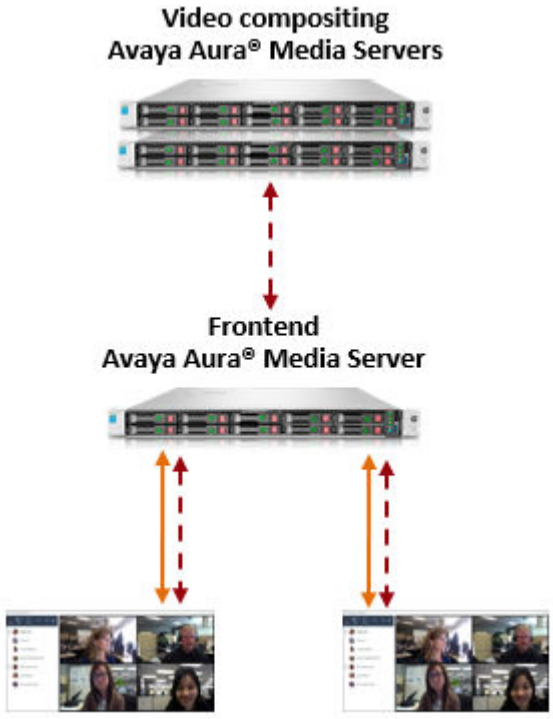


Figure 134: Frontend and video compositing Avaya Aura® Media Servers

The feature has the following characteristics:

- Endpoints connect to the same Avaya Aura® Media Server if they need audio, MSS video, hybrid or processed. Endpoints are never moved between media servers.
- The frontend Avaya Aura® Media Server performs audio mixing for all participants. Resources can be requested on demand, without signaling to the endpoint or moving the endpoint. Resources can be shuffled, re-organized and packed without moving participants.
- The video compositing server performs video processing, which is more efficient than with a mixed load. Video processing resources can be added on demand without requiring endpoints to connect directly to the servers. Resources can be added to conferences already in progress without disrupting endpoints.
- The same Avaya Aura® Media Server is used in all cases with varying server profiles.
  - The default server profile is referred to as the frontend Avaya Aura® Media Server. The profile provides audio, video switching, conferencing, and web collaboration.
  - The video compositing resource server profile is referred to as the backend or video compositing Avaya Aura® Media Server. The profile provides video processing and composite services.

The solution also provides multi-shared video. This new composite mode is provided by the video compositing Avaya Aura® Media Server. In this mode, the visible meeting layout can be

programmed to show a certain number of participants, leaving additional participants to see the meeting layout without being seen. When one of these participants becomes the active speaker, the visible layout changes and the new active speaker replaces the least active speaker in the layout.

Solution architecture

The following figure illustrates the hardened solution deployment. For a detailed description of each component, see Component architecture on page 18.

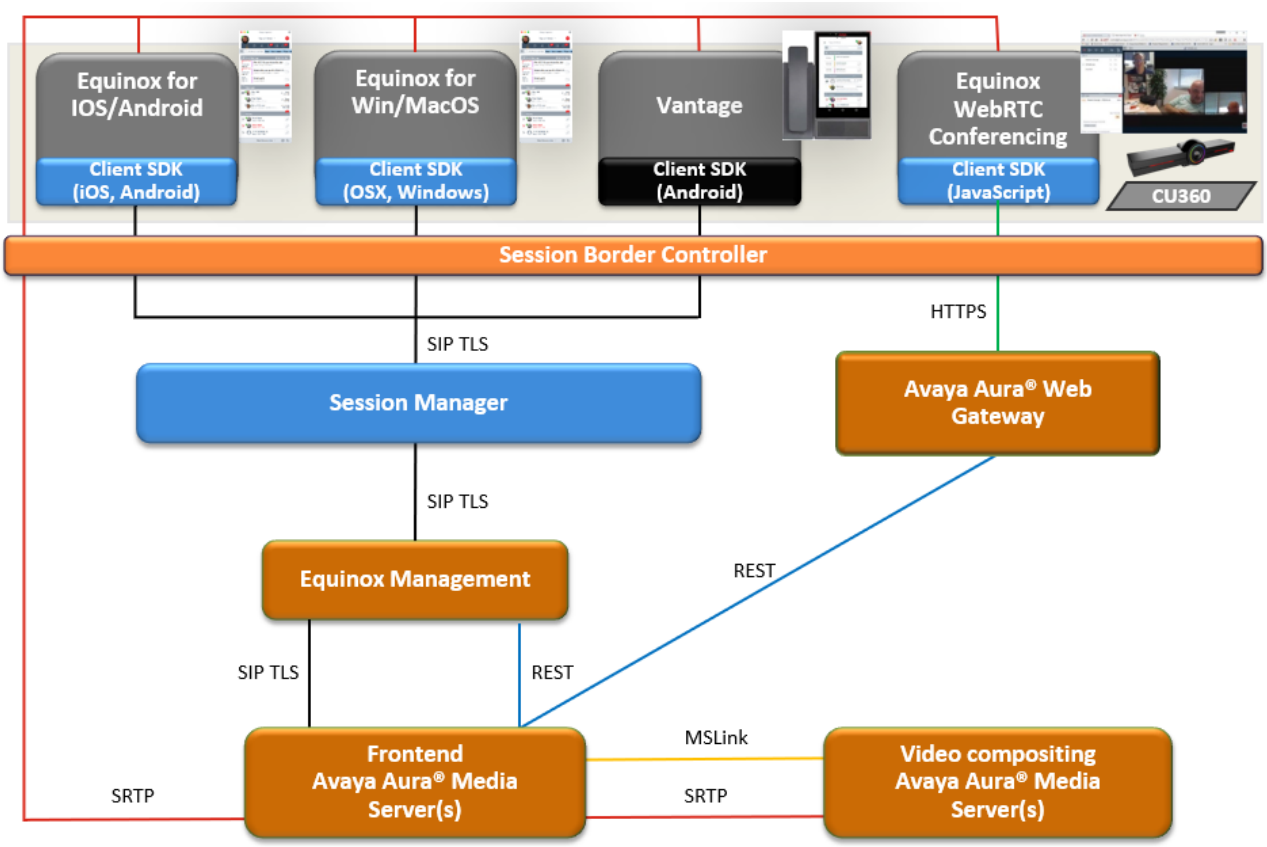


Figure 135: Components of the Avaya Equinox® Team Engagement hardened deployment

The solution has the following characteristics:

- Video compositing servers communicate with the frontend Avaya Aura® Media Server using MSLink, a proprietary protocol.
- Media flows from the video compositing server to the frontend Avaya Aura® Media Server, and then through the Session Border Controller directly to the endpoints.
- Equinox Management communicates with the frontend Avaya Aura® Media Server using SIP TLS and REST over HTTPS.
- Avaya Aura® Web Gateway communicates with the frontend Avaya Aura® Media Server using REST.

Hardened solution features

The following table lists the conferencing features available in the current release.

Table 69: Solution features

Category	Feature
Components	
	Avaya Equinox® Management, SIP Back-to-Back User Agent. (SIPB2B), Platform Manager (PMGR)
	Equinox Conference Control (also called UCCS)
	Avaya Aura® Media Server
	Web Collaboration Servers in Avaya Aura® Media Server
	Avaya Aura® Web Gateway, which includes the User Portal.
Avaya interoperability	
	Avaya Aura® SIP
	Avaya Aura® Device Services
	Avaya Session Border Controller for Enterprise
	Avaya IX™ Workplace Client on Android, Mac, iOS, Windows
	Avaya Equinox® Meetings for Web
	Avaya Room System XT Series
	Avaya IX™ CU360
	Avaya Vantage™
3rd Party interoperability	
	Polycom, SIP audio/video only
	Cisco/Tandberg, SIP audio/video only
	Lifesize, SIP audio/video only
Video	
	Automatic video layouts
	Video participant name in video
	Fully processed and multi-shared video mode
Web collaboration	
	Screen and application sharing
	Whiteboard
	Remote desktop keyboard and mouse control, supported on desktop clients. Not supported on mobile and Web clients.
Conference control	
	Unified Conference Control Protocol (UCCP) roster
	Conference control (UCCP)
	In-meeting DTMF control

Table continues…

Category	Feature
Meeting scheduler	
	IX Workplace 3.x Outlook Plug-in
	Schedule through user portal
Join meeting	
	Dial through SIP in Avaya Aura®
	Join through HTTP UA
	Join through User Portal
	Ad-hoc conferencing through Avaya Aura®
Meeting features	
	Active talker indication
	Meeting PIN protection
	Terminate meeting
	Extend meeting
	Add someone to the meeting (UCCP)
	Drop someone from the meeting
	Mute/unmute all participants
	Lecturer mode, audio only
	Lock/unlock meeting
	Knock on door (UCCP)
	Raise Hand (UCCP)
	Conference chat (UCCP)
	Far End Camera Control (UCCP)
	Mobile/Screen link

Related links

Avaya Equinox® Team Engagement hardened deployment on page 456

Configuration checklist for hardening the backend Avaya Aura® Media Server

For a full explanation on setting up and configuring servers that are part of the deployment, download documents from the Avaya Support website at http://support.avaya.com.

Checklist of general configuration procedures for Avaya Aura® Media Server

Perform the procedures listed below when configuring Avaya Aura® Media Server for the hardened deployment.

No.	Task	Link/Notes	✔
1	Set up certificates.	See *Implementing and Administering Avaya Aura® Media Server* to implement security configuration.	
2	Configure TLS for external connections.	See *Implementing and Administering Avaya Aura® Media Server* to configure the following settings: • **Enable TCP TLS Transport** • **Verify Host Name of TLS Client Connections** • **Enable OCSP** • **Use TCP TLS Transport for Remote Database Connections** • **Verify Host Name of the Remote DB secure connection**	
3	Enable FIPS in the Avaya Aura® Media Server software.	See *Implementing and Administering Avaya Aura® Media Server*.	
4	Enable FIPS mode in the OS layer of Avaya Aura® Media Server.	See *Deploying and Updating Avaya Aura® Media Server Appliance*.	
5	Configure Simple Object Access Protocol (SOAP) attributes.	See *Implementing and Administering Avaya Aura® Media Server*.	
6	Configure Avaya Aura® Media Server enrollment with Avaya Aura® System Manager.	See *Implementing and Administering Avaya Aura® Media Server*.	
7	(Optional) Configure Role Based Access Control (RBAC) in Avaya Aura® System Manager.	See the following documents to use centralized RBAC for managing the level of access the system grants to authorized administrators: • *Implementing and Administering Avaya Aura® Media Server* • *Administering Avaya Aura® System Manager*	
8	Configure EM mutual authentication.	See *Implementing and Administering Avaya Aura® Media Server*.	

Checkist for configuring additional security settings in Avaya Aura® Media Server

No.	Task	Link/Notes	✔
1	(Optional) Disable the Avaya support account.	To disable the Enhanced Access Security Gateway (EASG) account, see *Deploying and Updating Avaya Aura® Media Server Appliance*.	

Table continues…

No.	Task	Link/Notes	✔
2	Configure password complexity.	See *Deploying and Updating Avaya Aura® Media Server Appliance*.	
3	Configure the login banner.	See *Implementing and Administering Avaya Aura® Media Server*	
4	If required, enable SELinux.	See *Deploying and Updating Avaya Aura® Media Server Appliance*.	
5	If required, configure GRUB2 boot password.	See *Deploying and Updating Avaya Aura® Media Server Appliance*.	
6	If required, run antivirus scan and update checks.	To manage the antivirus software, see *Deploying and Updating Avaya Aura® Media Server Appliance*.	
7	If required, run File System Integrity checks.	To use the File System Integrity Tool (FSIT), see *Deploying and Updating Avaya Aura® Media Server Appliance*.	
8	If required, configure encrypted transfer of audit logs and syslogs.	See Configuring Avaya Aura Media Server for encrypted transfer of audit logs and syslogs to a log aggregation server on page 465.	
9	If required, configure encrypted NTP time source messaging.	See Configuring encrypted NTP time source messages in Avaya Aura Media Server on page 466.	
10	If required, configure out of band management.	To update network configuration, see *Deploying and Updating Avaya Aura® Media Server Appliance*.	

Configuration procedure specific to the backend Avaya Aura® Media Server

To enable video composite services in the backend Avaya Aura® Media Server, see *Implementing and Administering Avaya Aura® Media Server*.

Related links

Avaya Equinox® Team Engagement hardened deployment on page 456

Configuration checklist for hardening the frontend Avaya Aura® Media Server

For a full explanation on setting up and configuring servers that are part of the deployment, download documents from the Avaya Support website at http://support.avaya.com.

Checklist of general configuration procedures for Avaya Aura® Media Server

Perform the procedures listed below when configuring Avaya Aura® Media Server for the hardened deployment.

No.	Task	Link/Notes	✔
1	Set up certificates.	See *Implementing and Administering Avaya Aura® Media Server* to implement security configuration.	
2	Configure TLS for external connections.	See *Implementing and Administering Avaya Aura® Media Server* to configure the following settings: • **Enable TCP TLS Transport** • **Verify Host Name of TLS Client Connections** • **Enable OCSP** • **Use TCP TLS Transport for Remote Database Connections** • **Verify Host Name of the Remote DB secure connection**	
3	Enable FIPS in the Avaya Aura® Media Server software.	See *Implementing and Administering Avaya Aura® Media Server*.	
4	Enable FIPS mode in the OS layer of Avaya Aura® Media Server.	See *Deploying and Updating Avaya Aura® Media Server Appliance*.	
5	Configure Simple Object Access Protocol (SOAP) attributes.	See *Implementing and Administering Avaya Aura® Media Server*.	
6	Configure Avaya Aura® Media Server enrollment with Avaya Aura® System Manager.	See *Implementing and Administering Avaya Aura® Media Server*.	
7	(Optional) Configure Role Based Access Control (RBAC) in Avaya Aura® System Manager.	See the following documents to use centralized RBAC for managing the level of access the system grants to authorized administrators: • *Implementing and Administering Avaya Aura® Media Server* • *Administering Avaya Aura® System Manager*	
8	Configure EM mutual authentication.	See *Implementing and Administering Avaya Aura® Media Server*.	

Checklist for configuring additional security settings in Avaya Aura® Media Server

No.	Task	Link/Notes	✔
1	(Optional) Disable the Avaya support account.	To disable the Enhanced Access Security Gateway (EASG) account, see *Deploying and Updating Avaya Aura® Media Server Appliance*.	

Table continues…

No.	Task	Link/Notes	✔
2	Configure password complexity.	See *Deploying and Updating Avaya Aura® Media Server Appliance*.	
3	Configure the login banner.	See *Implementing and Administering Avaya Aura® Media Server*	
4	If required, enable SELinux.	See *Deploying and Updating Avaya Aura® Media Server Appliance*.	
5	If required, configure GRUB2 boot password.	See *Deploying and Updating Avaya Aura® Media Server Appliance*.	
6	If required, run antivirus scan and update checks.	To manage the antivirus software, see *Deploying and Updating Avaya Aura® Media Server Appliance*.	
7	If required, run File System Integrity checks.	To use the File System Integrity Tool (FSIT), see *Deploying and Updating Avaya Aura® Media Server Appliance*.	
8	If required, configure encrypted transfer of audit logs and syslogs.	See Configuring Avaya Aura Media Server for encrypted transfer of audit logs and syslogs to a log aggregation server on page 465.	
9	If required, configure encrypted NTP time source messaging.	See Configuring encrypted NTP time source messages in Avaya Aura Media Server on page 466.	
10	If required, configure out of band management.	To update network configuration, see *Deploying and Updating Avaya Aura® Media Server Appliance*.	

Checklist for configuration procedures specific to the frontend Avaya Aura® Media Server

No.	Task	Link/Notes	✔
1	Configure the frontend media server.	See *Implementing and Administering Avaya Aura® Media Server* to perform the following procedures: • Video compositor configuration • Web collaboration configuration	
2	Configure secure REST requests.	See *Implementing and Administering Avaya Aura® Media Server* to configure the following settings: • **Enable TLS Transport** • **Enable TLS Mutual Authentication**	

Table continues…

No.	Task	Link/Notes	✔
3	Configure SIP general settings.	See *Implementing and Administering Avaya Aura® Media Server* to configure the following settings: • **Enable SIP TLS Transport** • **Enable SIP TLS Mutual Authentication** • **Enable SIP UDP transport**. Disable this setting for the hardened deployment. • **Enable SIP TCP Transport**. Disable this setting for the hardened deployment.	

Related links

Avaya Equinox® Team Engagement hardened deployment on page 456

Configuring Avaya Aura® Media Server for encrypted transfer of audit logs and syslogs to a log aggregation server

About this task

This configuration sends security and non-security logs from the Avaya Aura® Media Server to a centralized server. rsyslog is a secure mechanism to achieve the transmission off the server. Both secure and non-secure log streams can be configured to the same or separate destinations.

Avaya Aura® Media Server is configured so that both syslog and audit logs from audisp are directed to the rsyslog stream for dispatch to a log aggregation server.

If required, follow this procedure to enable encrypted remote log aggregation.

Procedure

1. Create the required certificates for each server. The rsyslog system requires the following on the Avaya Aura® Media Server appliance and the central log aggregation server:
   - The certificate of the Certificate Authority (CA)
   - The private key of the server
   - The certificate of the server signed by the CA
2. Log in to the Avaya Aura® Media Server using the vShpere console and the root account credentials.
3. Use SFTP to transfer the CA signed server certificate and the CA certificate to the Avaya Aura® Media Server.

4. To configure the remote log aggregation server address and port, run the rsyslog configuration tool.

   For example:

   ```
   $MASHOME/bin/rsyslogconf.sh --enableRemoteLogging logs.company.com:514
   ```

5. To ingest a copy of the certificates and configure TLS for encrypted rsyslog connections, run the rsyslog configuration tool.

   For example:

   ```
    $MASHOME/bin/rsyslogconf.sh --enableTLS logs.company.com ca-cert.pem signed-cert.pem server-key.pem
   ```

   If the server key file and signed certificate file must be combined into one file, specify that file for both the server key and signed certificate file arguments.

   For example:

   ```
   $MASHOME/bin/rsyslogconf.sh --enableTLS logs.company.com ca-cert.pem signed-cert.pem  signed-cert.pem
   ```

6. Delete the temporary copies of the certificates that you transferred to the Avaya Aura® Media Server.

   Use the shred command to overwrite the file contents before deletion:

   ```
   shred -u <filename>
   rm <filename>
   ```

Related links

Avaya Equinox® Team Engagement hardened deployment on page 456

Configuring encrypted NTP time source messages in Avaya Aura® Media Server

About this task

If required, use this procedure to enable encrypted NTP time source messaging.

Before you begin

- Enable Linux FIPS mode.
- Do not configure NTP time source servers using the Element Manager of Avaya Aura® Media Server task located at **System Configuration** > **Network Settings** > **General Settings**. This configuration does not provide the required security.

Procedure

1. Log in to a Linux® shell by using SSH to Avaya Aura® Media Server and gain root access.
2. To replace all existing NTP time source servers with up to three new servers, use the following command:

   ```
   ntpconf.sh --setNtpAuth --svr <addr> <id> <type> <key>[--svr <addr> <id> <type> <key>][--svr <addr> <id> <type> <key>]
   ```

For example, to add one server type:

```
ntpconf.sh --setNtpAuth --svr ntp.example.mil 23 SHA1
098ff1800ff00ff00ff1722c72faf7c345833119
```

3. After a few minutes, verify the configuration by entering the following command:

   ```
   ntpq -c as
   ```

   Verify that the result indicates that `auth` is `ok` and that the `condition` is `sys.peer`. For example:

   ```
   ind assid status  conf reach auth condition  last_event cnt

   ===========================================================

     1 43956  f63a   yes   yes   ok   sys.peer    sys_peer  3
   ```

Related links

Avaya Equinox® Team Engagement hardened deployment on page 456

Configuration checklist for Avaya Equinox® Management hardening

This checklist contains relevant procedures for Avaya Equinox® Management hardening:

No.	Task	Link/Notes	✔
1	Import a certificate signed by a certificate authority (CA).	See *Administrator Guide for Avaya Equinox® Management*.	
2	Enable hardening for the Avaya Equinox® Management server.	See *Administrator Guide for Avaya Equinox® Management*.	
3	Enable standard definition (SD) or high definition (HD) composite video for a virtual room.	See *Administrator Guide for Avaya Equinox® Management*.	

Related links

Avaya Equinox® Team Engagement hardened deployment on page 456

Configuration checklist for hardening Avaya Aura® Web Gateway

For a full explanation on setting up and configuring Avaya Aura® Web Gateway, download documents from the Avaya Support website at http://support.avaya.com.

Perform the procedures listed below when configuring Avaya Aura® Web Gateway for the hardened deployment.

No.	Task	Link/Notes	✔
1	Enable FIPS in the system layer.	To use the `sys secconfig --fips --enable` command for enabling FIPS in the system layer, see *Administering the Avaya Aura® Web Gateway* .	
2	Secure connection to LDAP servers.	To enable **Secure LDAP**, see *Administering the Avaya Aura® Web Gateway*.	
3	(For Kerberos authentication) Add the Avaya Aura® Web Gateway SPN to a domain user on the Windows Domain Controller or the Active Directory server.	See *Administering the Avaya Aura® Web Gateway*.	
4	(For Kerberos authentication) Enable encryption support for the domain user that is mapped to the Avaya Aura® Web Gateway SPN.	See *Administering the Avaya Aura® Web Gateway*.	

Related links

Avaya Equinox® Team Engagement hardened deployment on page 456

Glossary

1080p	See Full HD on page 473.
720p	See HD on page 475.
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 470.
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 480.
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 471.
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 469.
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 472.
FPS	See Frames Per Second on page 472.
Frame Rate	See Frames Per Second on page 472.
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 474.

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 469.

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 475.
High Profile	See H.264 High Profile on page 474.
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 479.
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 471.
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 471.
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 477.
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 479.
SIP Server	A SIP server is a network device communicating via the SIP protocol.
SIP URI	See URI on page 483.
Slider	See Content Slider on page 470.
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 480.
Standard Definition	See SD on page 480.
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 483.
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 479.
Video Switching	See Switched video on page 482.
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.