Deploying Avaya Equinox Solution

Release 9.0.2
Issue 2
August 2017

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

Heritage Nortel Software

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

Copyright

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

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that 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 G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. 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

Contents

Chapter 1: An introduction to Avaya Equinox Conferencing... 11
About this document.. 11
New in this release.. 11
Audience... 12
How to use the document... 13
License key.. 13
Chapter 2: Deployment options.. 15
Choosing the appropriate solution for your organization.. 15
Component architecture.. 16
Specifications for small enterprises.. 22
Reference configurations.. 22
Specifications for medium enterprises.. 24
Reference configurations for Over The Top deployments.................................... 24
Reference configuration for Team Engagement deployment................................ 27
Reference configuration for Over The Top deployment with Avaya IP Office......... 28
Reference configuration for Over The Top deployment with Microsoft Unified Communications... 29
Specifications for large enterprises.. 30
Reference configurations for Over The Top deployments.................................... 30
Reference configuration for Over The Top deployment with Microsoft Unified Communications... 32
Reference configuration for Over The Top deployment for Service Providers and Cloud services.. 33
Reference configuration for Team Engagement deployment................................ 34
Chapter 3: Network planning and design considerations....................................... 36
Avaya Aura network planning and design considerations.. 36
Firewall and NAT traversal options.. 36
Securing Your Deployment... 40
Authentication and Encryption.. 42
About Media Security... 43
About Signaling Security.. 44
About Management Security... 45
Securing Access to Functionality with User Profiles.. 45
Planning a Centralized or Distributed Topology (Cascading) for MCU....................... 45
Planning Scalability and High Availability in the Equinox Solution............................. 48
High Availability of Equinox Management.. 49
Scalability and High Availability of Scopia Desktop Server and Equinox H.323 Edge server... 51
Scalability and High Availability with Scopia® Video Gateway 51
Scalability and High Availability with Multiple MCUs... 52
Scalability with Equinox Streaming and Recording.. 52

Planning User Access to Videoconferences 56
Assessing Bandwidth for Large Organizations 58
Setting WAN Bandwidth Limits 63
Using Network Traffic Priorities Across your Deployment 63
Updating the Dial Plan 64
Chapter 4: Before you begin 67
Before You Begin checklist 67
Chapter 5: Installing VMware-ready Common Servers 70
Downloading documentation 70
Deploying the Solution Deployment Manager client 70
Chapter 6: Installing customer-provided servers 72
Prerequisites for OVA installation 72
Chapter 7: Before you begin software installation 73
Prerequisites for software installation 73
Latest software updates and patch information 74
Software installation checklist for SMB deployment 74
Software installation procedures for medium to large deployments 77
Software installation procedure for large deployments and for Service Providers 80
Software installation procedure for adding servers 84
Chapter 8: Equinox Management Deployment for Over the Top (OTT) Solution 85
Deployment of Equinox Management for OTT solution — Overview 85
Equinox Management Technical Specifications 86
Checklist for Deploying Equinox Management in an All-In-One Working Mode 88
Checklist for Deploying Equinox Management in a Distributed Working Mode 89
Downloading software from PLDS 90
Deploying the Equinox Management Server 91
Logging into Equinox Management 105
Configuring the All-In-One Equinox Management Server 110
Configuring the Distributed Equinox Management Server as an H.323 Gatekeeper 112
Configuring Gatekeepers in Avaya Equinox Management 114
Configuring Deployment of User Portal + Web Gateway 117
Securing Connections With Equinox Management 121
Applying a Third-Party Certificate to the All-in-One Equinox Management Server 122
Applying a Third-Party Certificate to the Distributed Equinox Management Server 126
Installing the CA Certificate for Avaya Equinox Meetings for Web 129
Configuring User Portal / Web Gateway Settings 134
Updating a User License 138
Deploying and Configuring the Equinox Management Environment 139
Troubleshooting 140
Chapter 9: Equinox Management Deployment for Team Engagement (TE) solution 143
Deployment of Equinox Management for TE solution — Overview 143
Checklist for Deploying Equinox Management in Team Engagement 143

Deploying the Avaya Aura® Web Gateway.......... 145
Managing Licenses Via the Web-based License Manager (WebLM).......... 145
Installing a User License On the Local WebLM Server.......... 145
Installing the User License On the External WebLM Server.......... 149
Integrating Avaya Aura® Users Into Equinox Management Via System Manager.......... 153
Configuring the Equinox Conferencing Element in System Manager.......... 154
Configuring SSO for Equinox Conferencing.......... 157
Adding Avaya Aura® Users in Equinox Management.......... 160
Deploying and Configuring the Equinox Management Environment.......... 160
Configuring Session Manager for Interoperability with the SIP-based Equinox B2BUA Component.......... 161
Adding a SIP Entity for the Equinox B2BUA Component.......... 161
Adding a SIP Entity Link/SIP Trunk For the Equinox B2BUA Component.......... 162
Adding Routing Policies For the Equinox B2BUA Component.......... 163
Adding Dial Patterns for the Equinox B2BUA Component.......... 163
Configuring Equinox Management for Interoperability with Avaya Aura®.......... 164
Adding a SIP Trunk from the Equinox B2BUA Component to Session Manager.......... 164
Changing the Default SIP Domain in Equinox Management.......... 165
Chapter 10: Migrating from Avaya Aura to Avaya Equinox.......... 167
Introduction to migrating AAC8 data.......... 167
Exporting data from Avaya Aura® Conferencing 8.0.......... 171
Importing Avaya Aura Conferencing data to Avaya Equinox Management.......... 172
Chapter 11: Equinox Media Server deployment.......... 178
Equinox Media Server overview.......... 178
Equinox Media Server deployment checklist.......... 179
Equinox Media Server video conferencing mode administration checklist.......... 179
Equinox Media Server audio-only conferencing mode administration checklist.......... 180
Equinox Media Server web collaboration mode administration checklist.......... 181
Equinox Media Server WebRTC gateway administration checklist.......... 181
Technical specifications.......... 182
Capacity and scalability.......... 183
Downloading software from PLDS.......... 184
Deploying the Equinox Media Server virtual machine.......... 185
Starting the Equinox Media Server virtual machine.......... 190
Configuring the Equinox Media Server IP addresses using vSphere Client Console.......... 190
Configuring the virtual machine automatic startup settings.......... 192
Adding Equinox Media Server in Equinox Management.......... 192
Add Media Servers field descriptions.......... 193
Adding Equinox Media Server in Equinox Management as a gateway.......... 194
Add Gateway field descriptions.......... 194
Configuring the Equinox Media Server network settings.......... 195
Configuration field descriptions.......... 196
Adding or updating the Equinox Media Server licenses.......... 197

Changing the Equinox Media Server working mode........ 198
Customizing audio messages........ 199
Secure connection with Equinox Management........ 200
Creating security certificates........ 200
Uploading security certificates........ 201
Securing the connection between Equinox Media Server and Equinox Management........ 202
Chapter 12: Scopia Elite 6000 MCU deployment........ 203
Scopia Elite MCU overview........ 203
Scopia® Elite 6000 MCU deployment checklist........ 203
Technical specifications........ 204
About the Capacity of the MCU........ 206
Ports to Open for the Scopia® Elite 6000 MCU........ 208
Configuring the IP addresses........ 210
Configuring IP separation........ 215
Adding or updating licenses........ 220
Configuring Ports on All Models of the Scopia Elite MCU........ 221
Configuring the UDP port ranges for RTP/RTCP on Scopia® Elite 6000 MCU........ 221
Configuring the TCP Port Range for H.245 on Scopia® Elite 6000 MCU........ 222
Configuring the HTTP port on Scopia® Elite 6000 MCU........ 223
Configuring the UDP port for RAS on Scopia® Elite 6000 MCU........ 223
Configuring the UDP port for the gatekeeper on Scopia® Elite 6000 MCU........ 224
Configuring the TCP port for Q.931 on Scopia® Elite 6000 MCU........ 225
Configuring the TCP, UDP, and TLS port for SIP........ 225
Configuring the TCP port range for SIP BFCP on Scopia® Elite 6000 MCU........ 226
Verifying the MCU Equinox H.323 Edge Installation........ 227
Chapter 13: Avaya Aura deployment........ 229
Deploying Avaya Aura components........ 229
Chapter 14: Avaya Session Border Controller deployment........ 230
Overview of the Avaya Session Border Controller for Enterprise........ 230
ASBCE deployment checklist........ 230
Deploying the ASBCE in a virtualized environment........ 231
Configuring licenses for ASBCE deployment........ 237
Configuring ASBCE TLS management certificates........ 237
Associating a certificate with the TLS Client and Server Profiles........ 238
Configuring the ASBCE interfaces........ 239
Configuring the ASBCE for remote access to multiple servers using a single FQDN and a single IP address........ 240
Configuring multiple server access using URL rewriting 242
Configuring the ASBCE STUN TURN server........ 246
Configuring the ASBCE in Equinox Management........ 247
Chapter 15: Equinox H.323 Edge deployment........ 249
Equinox H.323 Edge overview........ 249
Equinox H.323 Edge hardware server deployment checklist........ 250

- Equinox H.323 Edge virtual server deployment checklist....... 251
- Equinox H.323 Edge initial configuration checklist....... 251
- Technical specifications of the Equinox H.323 Edge server....... 252
- Ports configuration....... 253
- Equinox H.323 Edge virtual server deployment....... 257
  - Downloading software from PLDS....... 257
  - Deploying the Equinox H.323 Edge virtual server....... 258
  - Starting the Equinox H.323 Edge virtual server....... 259
  - Configuring the virtual machine automatic startup settings....... 260
- Equinox H.323 Edge initial configuration....... 260
  - Configuring the IP addresses of the Equinox H.323 Edge hardware server....... 260
  - Adding networks to the Equinox H.323 Edge virtual server....... 264
  - Configuring IP separation of the Equinox H.323 Edge virtual server....... 266
  - Configuring Ports on the Equinox H.323 Edge server....... 268
  - Integrating the Equinox H.323 Edge server with Other Equinox Solution Components....... 269
  - Enabling Internal Endpoints to Call External Endpoints....... 271
  - Secure connection with Equinox Management....... 279
  - Adding and updating licenses....... 283
  - Configuring remote access....... 284
  - Access field descriptions....... 285
  - Configuring QoS for audio and video....... 286

Chapter 16: Avaya Scopia Desktop Server deployment....... 288

- Planning your Avaya Scopia Desktop Server deployment....... 288
  - Planning your Avaya Scopia Desktop Deployment....... 288
  - Minimum Requirements and Specifications of Scopia Desktop Server....... 289
  - Planning your Topology for Scopia Desktop Server....... 292
  - Deploying Scopia Desktop Server with Dual-NIC....... 300
  - Estimating and Planning your Bandwidth Requirements....... 301
  - Ports to Open on Avaya Scopia Desktop....... 309
- Installing Avaya Scopia Desktop Server....... 318
  - Installing or upgrading your Avaya Scopia Desktop deployment....... 318
  - Installing All Scopia Desktop Components on a Single Server....... 319
  - Installing the Conference Server for Scopia Desktop on a Dedicated Server....... 323
  - Installing the Content Center for Scopia Desktop on a Dedicated Server....... 327
  - Installing the Invitation and Presence Server for Scopia Desktop on a Dedicated Server....... 333
  - Centrally Deploying Scopia Desktop Clients in your Organization....... 335
  - Upgrading Scopia Desktop....... 335

Chapter 17: Avaya Equinox Streaming and Recording deployment....... 341

- Introducing Avaya Equinox Streaming and Recording....... 341
  - Avaya Equinox Streaming and Recording Server....... 341
- Installing Avaya Equinox Streaming and Recording....... 352
  - Installation checklist....... 352
  - Physically connecting the new server....... 354

Starting the new server...... 358
Configuring the new server...... 359
Licensing checklist...... 362
Configuring external addresses for public interfaces...... 369
Registering each of the components...... 371
Configuring delivery nodes...... 374
Configuring virtual delivery nodes...... 378
Configuring conference points...... 380
Specifying polling intervals and the network address...... 381
Configuring the recycle bin...... 382
Adding and Modifying Equinox Streaming and Recording Servers in Equinox Management 383
Configuring the Avaya Equinox Recording Gateway...... 385
Chapter 18: Upgrading to the Avaya Equinox solution...... 387
Upgrading the Equinox Solution...... 387
Chapter 19: Resources...... 388
Documentation...... 388
Finding documents on the Avaya Support website...... 392
Training...... 392
Support...... 393
Using the Avaya InSite Knowledge Base...... 393
Glossary...... 394

Chapter 1: An introduction to Avaya Equinox Conferencing

About this document

This document provides procedures required to perform the initial installation and deployment of Avaya Equinox™ Release 9.0 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.

New in this release

Release 9.0.2 of the Equinox Solutionhas the following enhancements:

- Avaya Equinox™ Meet-Me Client now integrates the Meet-Me functionality and replaces the Scopia client. This replacement is optional for an OTT deployment. Contact your administrator to continue using Scopia Desktop in the following cases: your deployment includes a third party session border controller (and not the Avaya SBCE required for Avaya Equinox™ Meet-Me); you currently need the Scopia Content Slider (which will be part of future releases).
- Documentation now includes:
  - Updated User Portal/Web Gateway topic in Chapter 8. Equinox Management Deployment for Over The Top (OTT) Solution, according to the usage.
  - New topics with important information on creating a SIP trunk between Avaya Aura® Session Manager and Avaya Equinox Management, in Chapter 9. Equinox Management Deployment for Team Engagement (TE) solution.
  - Updated Chapter 14. Avaya Session Border Controller for Enterprise deployment. The chapter describes how to configure the ASBCE for access by remote Equinox Meet Me and Meetings for Web clients.

    Guest clients who need to participate in conferences have to interact with multiple components. 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. The URL rewriting can be used in all Equinox deployments.

  - Updated topics with reference to the Avaya Equinox™ Meet-Me Client.
  - Updated topics about the Scopia Desktop Serveraccording to the usage.

Audience

The intended audience for this document is:

- Tier 1 Avaya technical support
- Avaya Professional Services
- Authorized Business Partners

You must have the following core competencies:

- The ability to access servers using:
  - a locally attached keyboard and monitor or KVM (Keyboard, Video, Mouse) switch
  - the ssh remote access protocol
- Basic Linux operations:
  - navigating the file system (changing directories)
  - managing the implications of uninformed or careless use of system commands while logged in as the root user
- Basic server tasks:
  - powering servers up
  - powering servers down
  - resetting servers
  - inserting and removing CD-ROM and DVD-ROM disks
- Basic Microsoft knowledge:

  Windows:

  - editing text files
  - creating folders
  - Microsoft Excel:
    - transitioning between worksheets of a workbook
    - entering data into cells
    - copying/pasting between cells and commands, such as Control+c, Control+v, and Edit > Paste Special menu

- The ability to operate a supported Web browser (such as Firefox or Internet Explorer):
  - Interacting with pop-up windows
  - Inspecting and accepting x.509 certificates and installing CA certificates that are presented by the browser
  - Downloading and installing software through the browser
- Basic Public Key Infrastructure (PKI) tasks:
  - Creating Certificate Signing Requests (CSR)
  - Inspecting the details of a certificate
  - Installing Certificate Authority certificates on Windows Certificate Store
  - Installing Personal certificates on Windows Certificate Store
  - Installing Certificate Authority certificates on Firefox Certificate Manager
  - Installing Your Certificates on Firefox Certificate Manager

How to use the document

As prerequisites, you must complete the following courses before deploying Avaya Equinox™:

- *Avaya Video Conferencing Solutions Overview*
- *Avaya Equinox™ Administration*

The courses are available on Avaya Learning website at http://www.avaya-learning.com.

You must also complete a given task successfully before beginning the next one. If you encounter issues while performing a step, contact the Avaya Support Web site at http://support.avaya.com to open a service request. Use this document to guide you through the preparatory requirements and installation and configuration steps for Equinox Solution.

License key

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 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.

For information on how to apply the conferencing license keys, see the license installation topic in each component deployment chapter. For license key activation in Avaya Aura® components, see the Avaya Aura® Conferencing documentation.

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

- Scopia Elite MCU
- Scopia® Video Gateway (TIP/Lync/SIP)
- Equinox H.323 Edge
- XT Series
- Equinox Management
- Web Gateway (Equinox Management)
- Avaya Conferencing Recording Gateway (ACRG)
- Equinox Media Server (MCU and AMS)
- Web Collaboration Server

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.

Chapter 2: Deployment options

Choosing the appropriate solution for your organization

The most appropriate solution for your organization is dependent on the organization size and the required capacity (number of concurrent sessions per ports in Avaya Equinox for Over The Top or number of users in Avaya Equinox for Team Engagement). These considerations together with the customer's major planned usage of the deployment towards video conferencing or high capacity audio conferencing will derive the selection of OVA size at installation.

To choose the configuration that best suits your requirements, consider the following:

- Do you need a small, medium, or large-sized solution?

  Within the context of Avaya Equinox™, a small deployment is defined as a deployment with up to 5,000 registered users. A medium deployment is defined as a deployment with up to 30,000 registered users. A large deployment is defined as a deployment with up to 150,000 registered users.

- Is your Avaya Equinox™ going to be a standalone Over The Top solution, or will it include Avaya Aura® (Team Engagement)?

  The Avaya Aura® solution is also called a Unified Communications (UC) Team Engagement solution.

- How are you going to host Avaya Equinox™?

  Avaya Equinox™ is available to purchase as a Virtual Appliance on an Avaya Common Server, with pre-installed VMware and Avaya Virtualization Platform. Alternatively, some customers buy their own servers, and then Avaya Equinox™ is available as a Virtual Appliance in a Virtualized Environment.

Offer	Virtual Appliance	Virtualized Environment
Server provided by	HP ProLiant DL360 G9 Dell™ PowerEdge™ R630	Customer
Hypervisor	Avaya Virtualization Platform (AVP)	Customer-provided VMware
VMware licenses	Included in Virtual Appliance offer from Avaya	Customer-provided

Table continues…

Offer	Virtual Appliance	Virtualized Environment
Server and virtualization management	Solution Deployment Manager as an external application for Avaya Equinox for Over The Top Solution Deployment Manager with Avaya Aura® for Avaya Equinox for Team Engagement.	VMware vCenter and Solution Deployment Manager
VMware training required	None	VMware certification

- How many business site locations do you wish to serve and what is the distance between these locations?

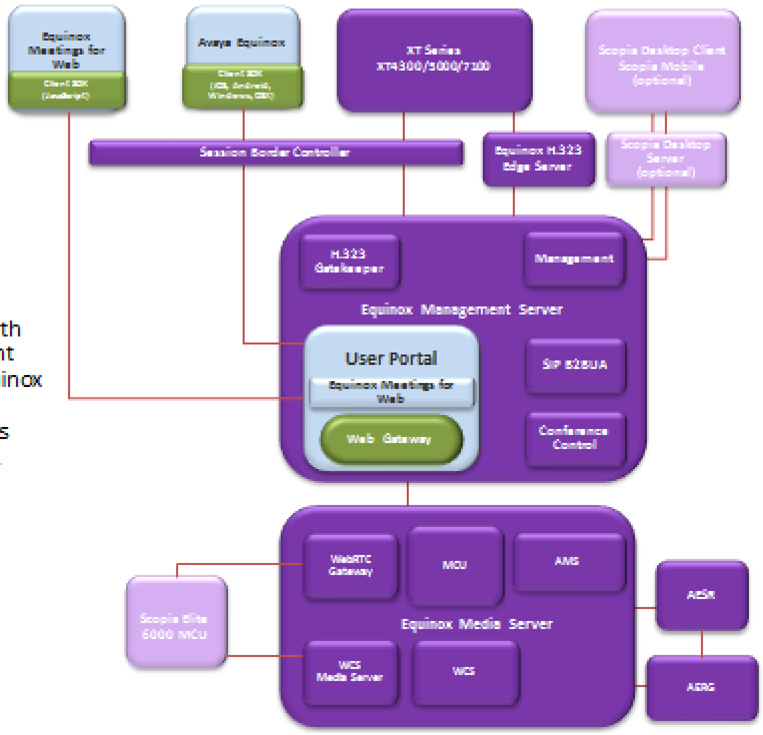
  The global distribution of your end users will drive the number and location of servers.

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 9.0 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 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 also introduces two deployment concepts: t to ask the question.Team Engagement (integrating Avaya Aura® in the solution) and Over The Top (standalone, conferencing-only on the customer existing infrastructure).

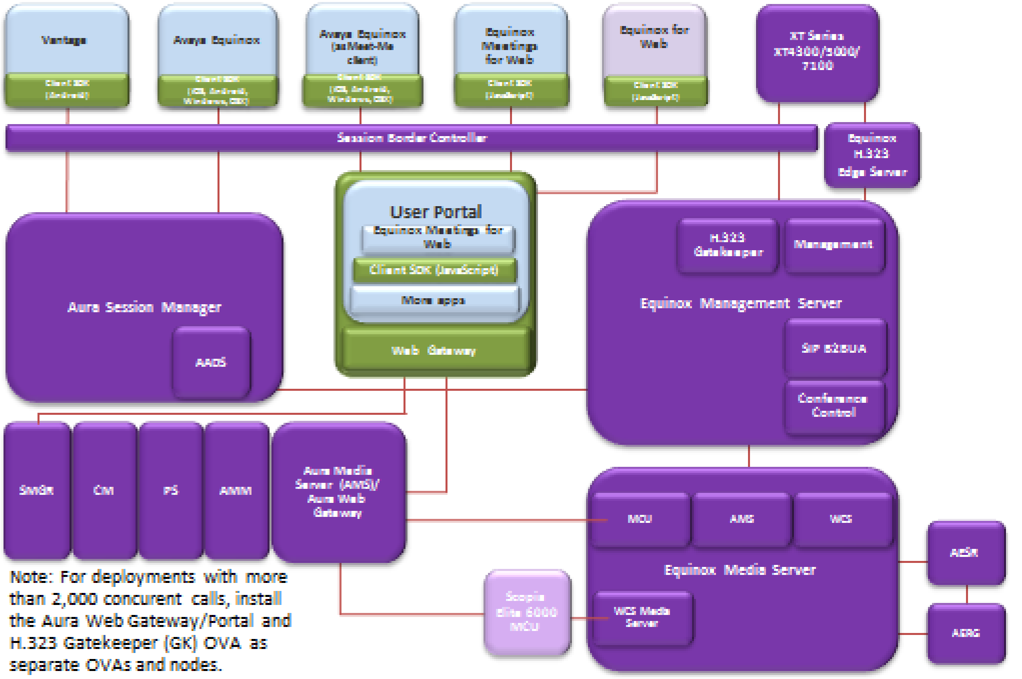
The figure below illustrates the deployment of key components for Avaya Equinox for Over The Top.



- Note: For deployments with more than 2,000 concurent calls, install the Avaya Equinox Web Gateway/Portal and H.323 Gatekeeper OVA as separate OVAs and nodes.

Figure 1: OTT Component architecture

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



- Note: For deployments with more than 2,000 concurent calls, install the Aura Web Gateway/Portal and H.323 Gatekeeper (GK) OVA as separate OVAs and nodes.

Figure 2: TE Component architecture

The OTT solution has these characteristics:

- All deployments are without Avaya Aura® (including IP Office).
- 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.
- Has Microsoft Lync support.

The TE solution has these characteristics:

- Calls go through Avaya Aura® Session Manager (SM)/Avaya Aura® Communication Manager (CM).
- SMGR manages Avaya Aura® and collect logs and alarms (except for the Equinox Management ones).
- Equinox Management manages all conferencing components.
- Equinox Management synchronizes with Avaya Aura® Device Services (AADS) .
- In future releases, Equinox Management will be synchronized and managed through Avaya Aura® System Manager (SMGR).
- The Unified Portal is not only used for conferencing and is not managed by Equinox Management. See the Avaya Aura® Conferencing documentation.

Infrastructure components

Equinox Management Server:

This infrastructure component comprises the following modules:

Server/service	Description
Management	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.
SIP B2BUA	SIP Back-to-Back User Agent.
Unified Portal	Single portal from which the administrator can access can access conferencing functionalities such as meetings, user settings, recordings, and web collaboration libraries. In the OTT model, Avaya Aura user portal functionalities and Avaya Web Gateway functionalities

Table continues…

Server/service	Description
	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.
Web Gateway	Web Gateway for WebRTC (HTTPS to SIP signaling). Relevant mainly for OTT and VAAS deployments. 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.
Equinox Conference Control	This service uses the Unified Conference Control Protocol (UCCP) , a web based protocol allowing 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 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

  In this mode it supports from 10x HD 720p30 up to 40x HD 720p30 video transcoded channels per single OVA

- High Capacity Audio + Web Collaboration

  In this mode it supports from 500 audio-web collaboration connection, up to 2,000 audio-web collaboration connection per single OVA.

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 Scopia® Elite 6000 MCU series. In this mode it performs as the WebRTC Gateway to add WebRTC functionality to the Scopia® 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 Scopia® Web Collaboration server functionalities (from Version 8.3), 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 Scopia® Elite 6000 MCU which are not available with standard H.239/BFCP based content sharing and are used by Scopia Desktop Clients.

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. Provide a single place in the Aura architecture where devices (clients and endpoints) can store and retrieve data that users would 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.
PS	Avaya Aura® Presence Services. 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. Delivers powerful IM and presence capabilities for Avaya Equinox™ users. Individuals and groups can interact and productively

Table continues…

Module	Description
	handle conversations and engage across locations and time.
Avaya Aura® Media Server/Avaya Aura® Web Gateway	High scale audio engine/enables 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 for Scopia® Elite 6000 MCU.

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 on Avaya Equinox Media Servers and Scopia Elite MCUs into AESR. For more information, see *Release Notes for Avaya Equinox Recording Gateway* on http://support.avaya.com.

Edge components

Product	Description
Scopia Desktop Server	(Legacy only, for customers who need to keep a third party session border controller in their deployment, or need the Scopia Content Slider functionality for their conferences). The server enables video and conferencing for remote and local desktop users for voice, video and data communications. It includes HD H.264 video for meeting participants and H.264 or Advanced Web based data collaboration. The latest technology in desktop video collaboration is supported including H.264 Scalable Video Coding (SVC) for error resiliency along with H.264 High Profile for bandwidth efficiency and reduced network costs. Scopia Desktop is a simple web browser plug-in that is centrally managed, distributed and deployed without complex licensing fees or installation issues. Automatic firewall traversal allows users to participate regardless of where they are. Advanced capabilities including user provisioning and managing personal virtual conference rooms are also available.

Table continues…

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 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.

Specifications for small enterprises

Reference configurations

The centralized Avaya Equinox for Over The Top solution deploys the complete set of conferencing facilities at the company's site. There are two configurations for the solution:

Basic configuration

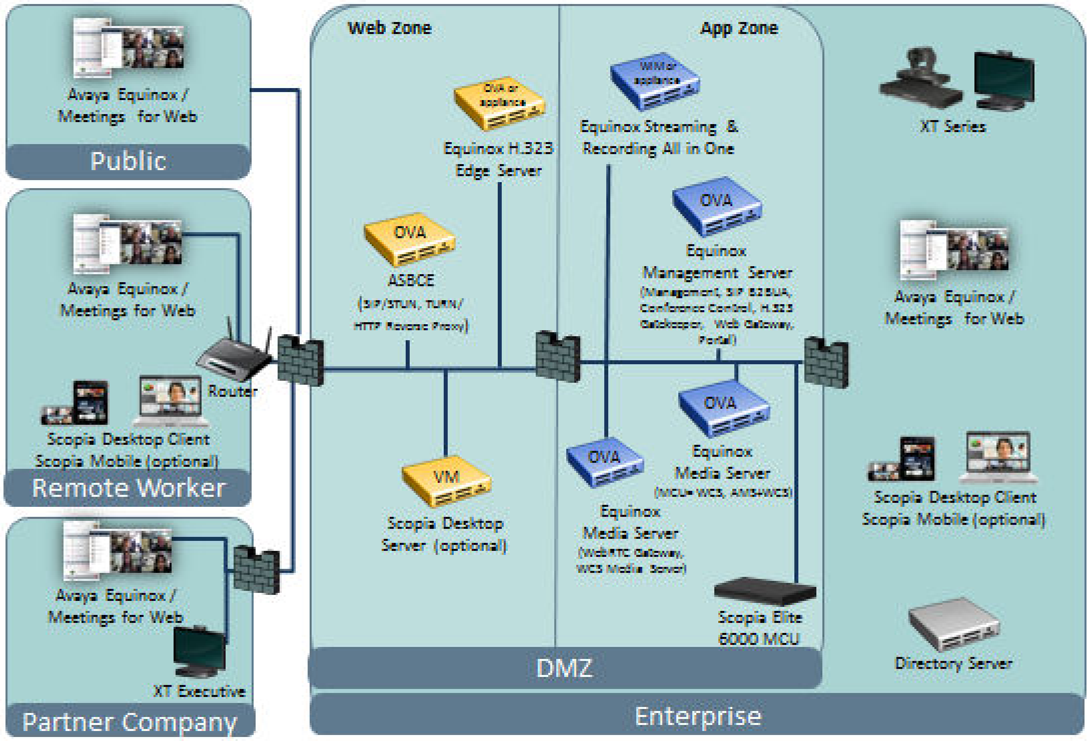


Figure 3: Basic configuration

Redundant configuration

The solution is highly scalable and fully redundant. To increase capacity, you can add more of the same components, like extra Equinox Management, Equinox Media Server, Equinox Streaming and Recording, Avaya Session Border Controller for Enterprise and others.

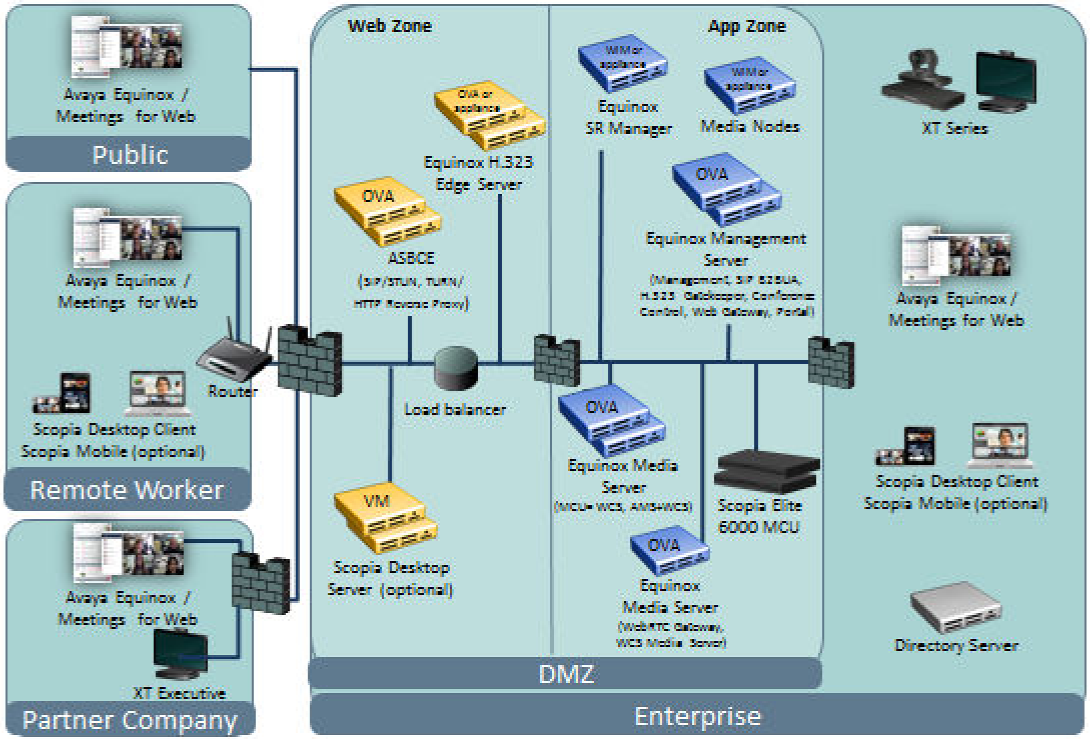


Figure 4: Redundant configuration

Specifications for medium enterprises

Reference configurations for Over The Top deployments

Centralized deployment

The Centralized solution offers the full range of conferencing features, particularly multiple simultaneous video, audio and data conferences that can be recorded and streamed for reliable delivery of high scale, high quality video. The solution is deployed with a minimal set of conferencing infrastructure at the company's site, allowing to call from endpoints and soft clients such as Avaya Equinox™ or Scopia Desktop (optional). Reverse proxy and STUN/TURN functionalities are required for accessing infrastructure components such the Web Gateway and the Unified Portal. The Avaya Session Border Controller for Enterprise (ASBCE) or an approved third party edge device can provide these functionalities.

- Basic deployment

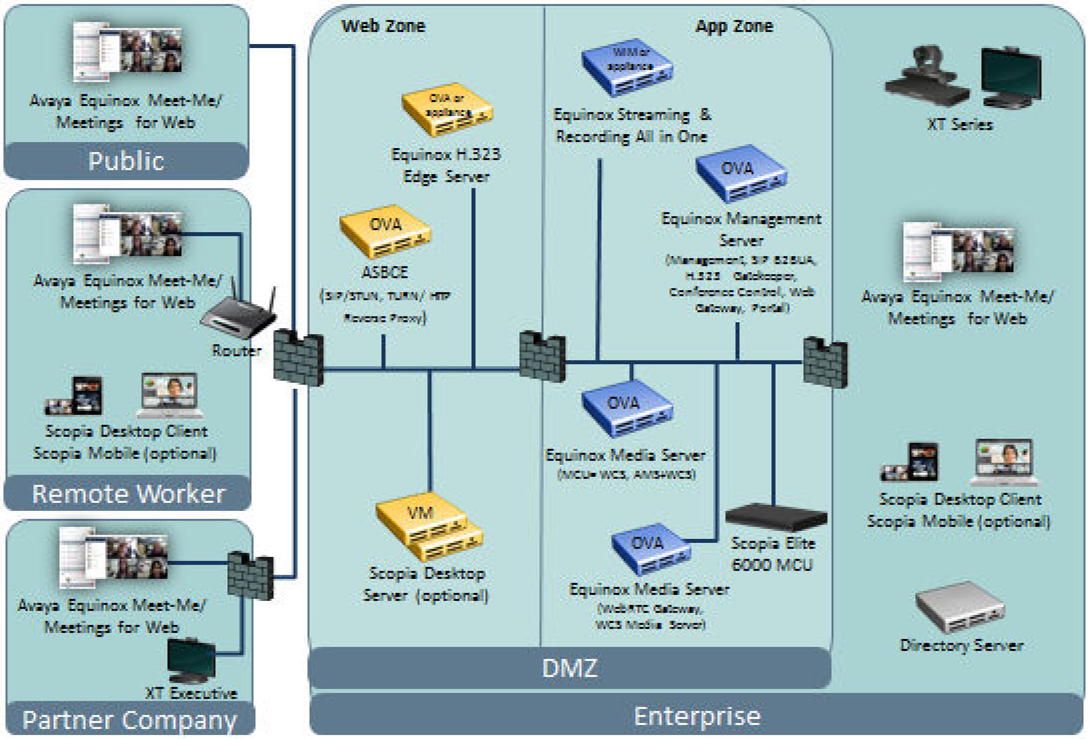

Avaya Equinox Meet-Me/ Meetings for Web
Public
Avaya Equinox Meet-Me/ Meetings for Web
Router
Scopia Desktop Client
Scopia Mobile (optional)
Remote Worker
Avaya Equinox Meet-Me/ Meetings for Web
XT Executive
Partner Company
Web Zone
OVA or appliance
Equinox H.323 Edge Server
OVA
ASBCE
(SIP/STUN, TURN/ HTTP Reverse Proxy)
VM
Scopia Desktop Server (optional)
App Zone
WM or appliance
Equinox Streaming & Recording All in One
OVA
Equinox Management Server
(Management, SIP B2BUA, H.323 Gatekeeper, Conference Control, Web Gateway, Portal)
OVA
Equinox Media Server
(MCU+ WCS, AMS+WCS)
OVA
Equinox Media Server
(WebRTC Gateway, WCS Media Server)
Scopia Elite 6000 MCU
DMZ
XT Series
Avaya Equinox Meet-Me/ Meetings for Web
Scopia Desktop Client
Scopia Mobile (optional)
Directory Server
Enterprise

Figure 5: OTT Centralized basic deployment

- Redundant deployment

  The solution is highly scalable and fully redundant. To increase capacity, you can add more of the same components, like extra Equinox Media Server, Equinox Streaming and Recording, and Avaya Session Border Controller for Enterprise (ASBCE). Equinox Management is duplicated for redundancy and high availability. Avaya Equinox H.323 Edge servers can be clustered behind a load balancing system for scalability and high availability. Scopia Desktop servers (optional) are clustered behind the same load balancer for scalability and high availability. This solution also accommodates the deployment of one or more Scopia Desktop servers in the enterprise private network to facilitate internal calls and meetings. ASBCEs are clustered and load balanced from Equinox Management.

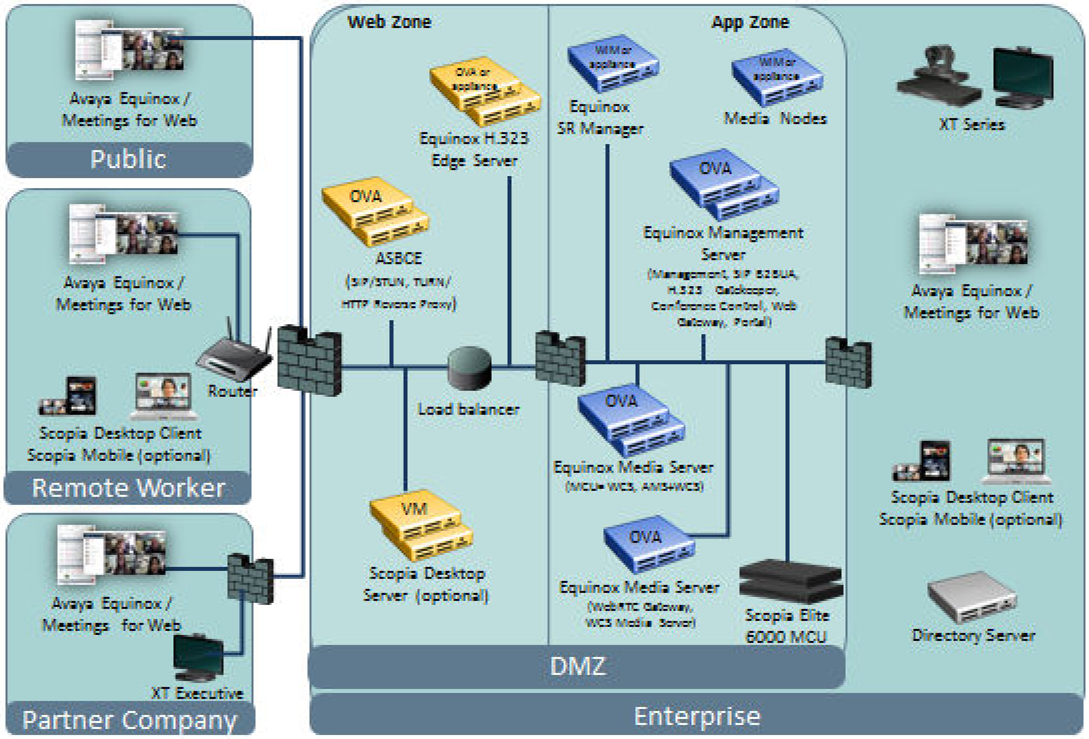


Figure 6: OTT Centralized redundant deployment

Distributed deployment

The solution is aimed at medium enterprises structured as a headquarter and several branches. Typically, each branch would have one or more meeting rooms, and a headquarter would have several meeting rooms. In this deployment, the infrastructure is distributed in both headquarter and branches. The Equinox Management application is split into management applications in the headquarter office, and the Web Gateway, Unified Portal, and Gatekeeper applications in branches to support service distribution. ASBCE is required for supporting Avaya Equinox™ clients and SIP endpoints. The solution is highly scalable. To increase capacity, you can add more of the same components like extra Equinox Media Servers and Scopia Desktop servers (optional).

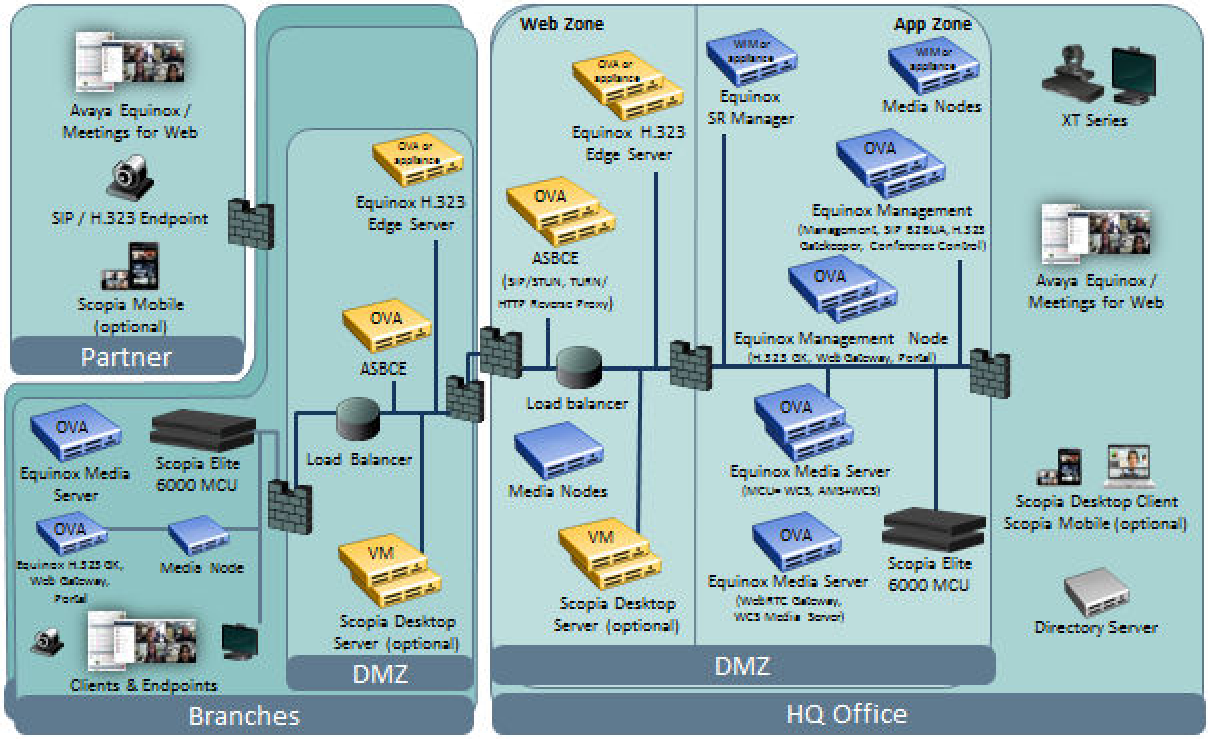


Figure 7: OTT Distributed deployment

Reference configuration for Team Engagement deployment

The Avaya Equinox for Team Engagement solution integrates Avaya Equinox™ conferencing with Avaya Aura® existing and new customer solutions. An Aura environment including Session Manager, Communications Manager, System Manager, Presence Server along with Conferencing 9.0 (and up) providing Unified Communications services for an Enterprise including internal/external voice, audio/video conferencing, IM/Presence. Some users are assigned a virtual room. Both internal and external users join conferences in a guest role. The TE solution provides the full range of conferencing features, and particularly multiple simultaneous video, audio and data conferences that can be recorded and streamed for reliable delivery of high scale, high quality video. The solution supports products such as Avaya Equinox™ clients, Avaya H175 Video Collaboration Station, Avaya Vantage™, ASBCE, and SIP telephony infrastructure.

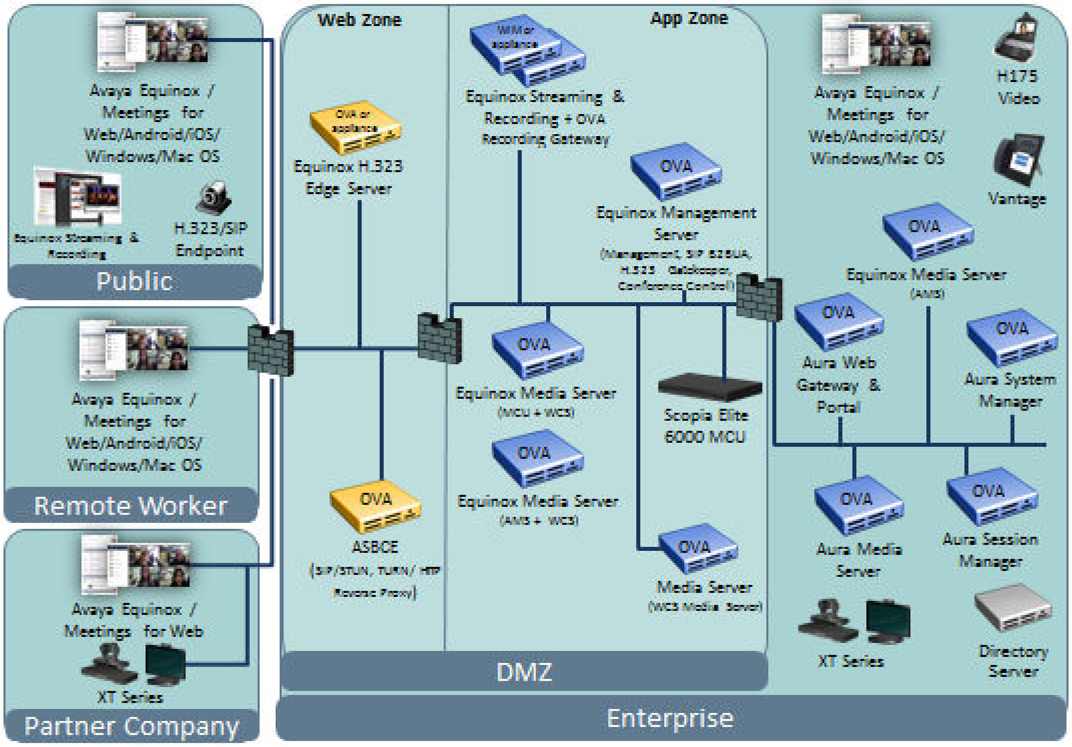

Avaya Equinox / Meetings for Web/Android/iOS/ Windows/Mac OS
Equinox Streaming & Recording
H.323/SIP Endpoint
Public
Avaya Equinox / Meetings for Web/Android/iOS/ Windows/Mac OS
Remote Worker
Avaya Equinox / Meetings for Web
XT Series
Partner Company
Web Zone
OVA or appliance
Equinox H.323 Edge Server
OVA
ASBCE (SIP/STUN, TURN/ HTP Reverse Proxy)
App Zone
VM or appliance
Equinox Streaming & Recording + OVA Recording Gateway
OVA
Equinox Management Server (Management, SIP B2BUA, H.323 Gatekeeper, Conference Control)
OVA
Equinox Media Server (MCU + WCS)
OVA
Equinox Media Server (AMS + WCS)
Scopia Elite 6000 MCU
OVA
Media Server (WCS Media Server)
DMZ
Avaya Equinox / Meetings for Web/Android/iOS/ Windows/Mac OS
H175 Video
Vantage
OVA
Equinox Media Server (AMS)
OVA
Aura Web Gateway & Portal
OVA
Aura System Manager
OVA
Aura Media Server
OVA
Aura Session Manager
XT Series
Directory Server
Enterprise

Figure 8: TE Deployment

Reference configuration for Over The Top deployment with Avaya IP Office

IP Office is the telephony solution for organizations of up to 1,000 users, providing easy communication for users inside the organization's private network. For business with IP Office deployments of 250 to 1,000 employees, the recommended OTT deployment is the centralized conferencing solution for medium enterprises.

In this solution, the Equinox Management server is connected to IP Office using SIP, while being connected to conferencing components using H.323 or SIP. The Equinox Management server is connected to the Equinox Media Server (or to Scopia® Elite 6000 MCU) using both SIP to allow SIP endpoints and clients (such as Avaya Equinox™) to participate in conferences hosted on the Equinox Media Server. XT Series endpoints are registered as H.323 endpoints to the H.323 Gatekeeper (part of the Equinox Management server), and also to IP Office via native SIP registration.

Communicating with remote H.323 endpoints outside the organization is performed via Avaya Equinox H.323 Edge. Scopia Desktop Clients and Scopia Mobiles (optional) have their own built-in firewall traversal feature and are connected directly to the Scopia Desktopserver located in the DMZ. Avaya Equinox™ clients can participate as guests. Avaya Session Border Controller for Enterprise is required in this deployment.

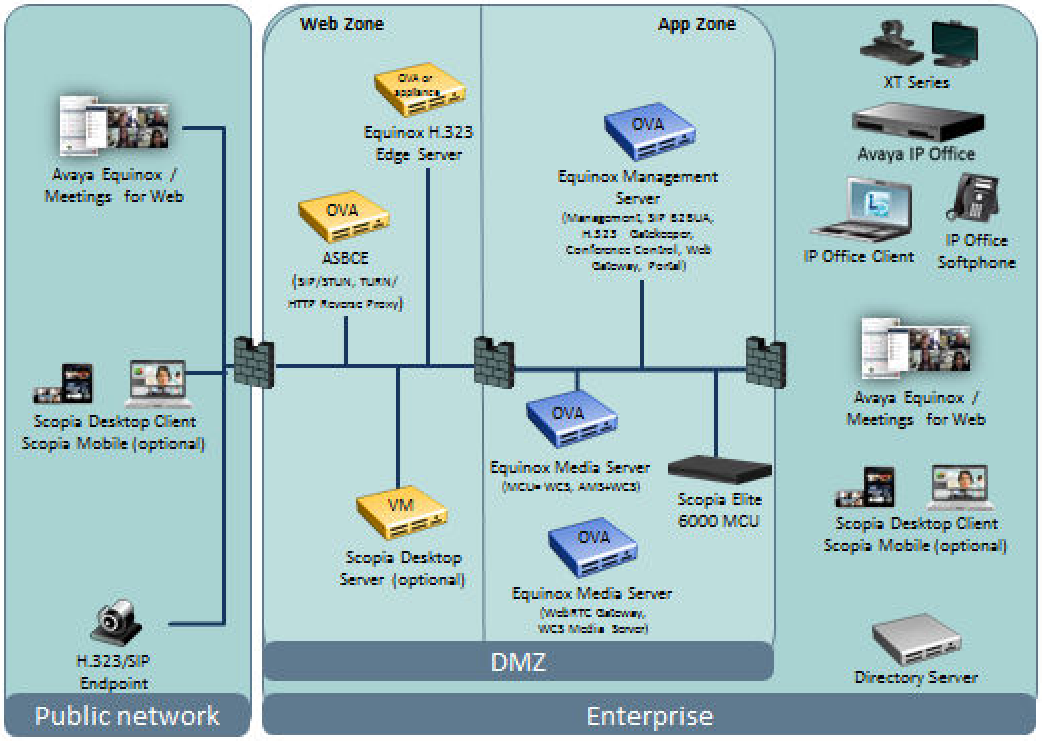


Figure 9: OTT Deployment with IP Office

Reference configuration for Over The Top deployment with Microsoft Unified Communications

Avaya Equinox for Over The Top supports UC integrations with Microsoft Lync or Microsoft Skype for Business (S4B). Integrating a Lync/Skype deployment offers text chat or instant messaging, voice and video communications, and content sharing between H.323 endpoints and Microsoft Lync or Microsoft Skype for Business (S4B) clients. The MS A/V Edge Server with TURN/STUN and ICE Servers, located in the DMZ, supports communication across networks. The Scopia® Video Gateway acts as a bridge between Lync/Skype endpoints and H.323 endpoints. Calls from Lync/Skype clients are routed through Microsoft servers. Scopia® Video Gateway connects H.323 endpoints. Equinox Management manages the deployment.

Communicating with remote H.323 endpoints outside the organization is performed via Avaya Equinox H.323 Edge.

Avaya Equinox™ Meet-Me Client now integrates the Meet-Me functionality and replaces the Scopia client. This replacement is optional for an OTT deployment. Contact your administrator to continue using Scopia Desktop in the following cases: your deployment includes a third party session border controller (and not the Avaya SBCE required for Avaya Equinox™ Meet-Me); you currently need the Scopia Content Slider (which will be part of future releases).

The full extent of third party servers required for MS UC deployments is not listed here. For a complete list of UC servers required, refer directly to the vendor’s documentation. Deployment diagrams focus on their integration with Avaya Equinox™ components only.

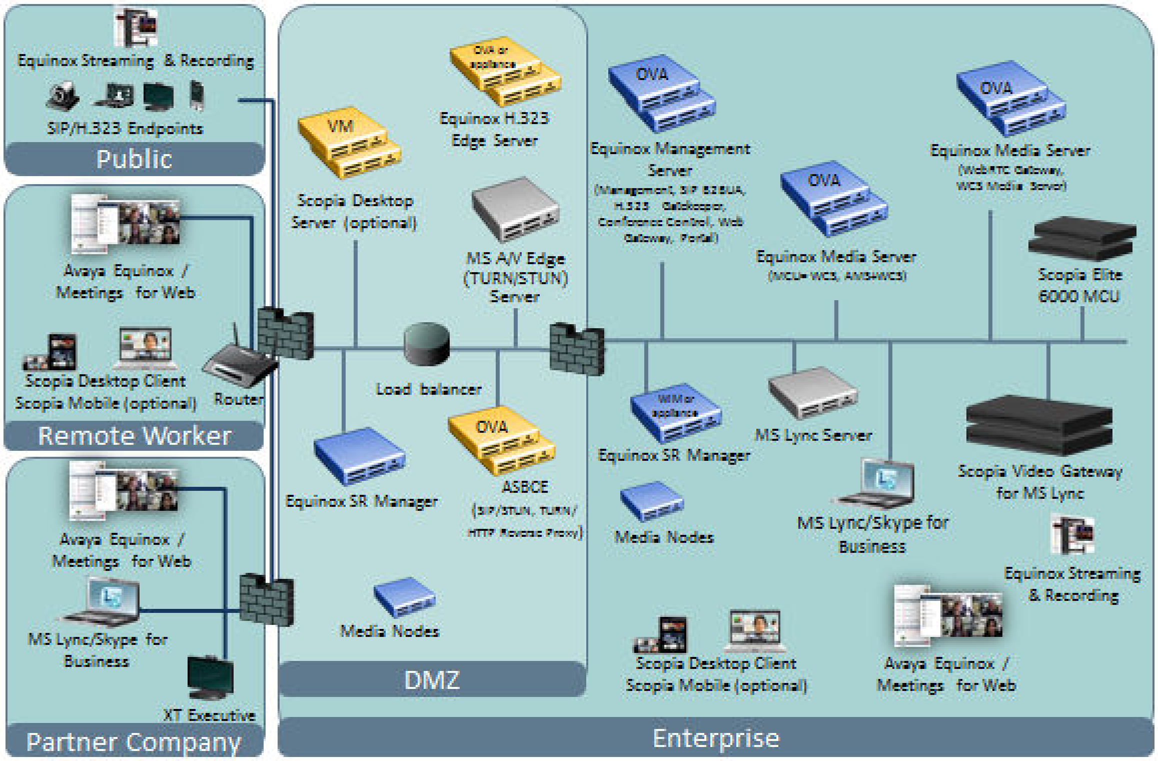

Equinox Streaming & Recording
SIP/H.323 Endpoints
Public
Avaya Equinox / Meetings for Web
Scopia Desktop Client
Scopia Mobile (optional)
Router
Remote Worker
Avaya Equinox / Meetings for Web
MS Lync/Skype for Business
XT Executive
Partner Company
VM
Scopia Desktop Server (optional)
OVA or appliance
Equinox H.323 Edge Server
MS A/V Edge (TURN/STUN) Server
Load balancer
Equinox SR Manager
OVA
ASBCE (SIP/STUN, TURN/ HTTP Reverse Proxy)
Media Nodes
DMZ
OVA
Equinox Management Server (Management, SIP B2BUA, H.323 Gatekeeper, Conference Control, Web Gateway, Portal)
OVA
Equinox Media Server (MCU+ WCS, AMS+WCS)
OVA
Equinox Media Server (WebRTC Gateway, WCS Media Server)
Scopia Elite 6000 MCU
VM or appliance
Equinox SR Manager
MS Lync Server
Scopia Video Gateway for MS Lync
Media Nodes
MS Lync/Skype for Business
Equinox Streaming & Recording
Scopia Desktop Client
Scopia Mobile (optional)
Avaya Equinox / Meetings for Web
Enterprise

Figure 10: MS Lync UC in OTT deployment

Specifications for large enterprises

Reference configurations for Over The Top deployments

The solution is aimed at large organizations. It can also be used by service providers, offering a scalable solution with high availability and service preservation for up to 30,000 H.323 users or 150,000 SIP users in a TE deployment.

The solution is called Avaya Equinox for Over The Top when it functions as a standalone infrastructure without Avaya Aura® components.

OTT Large Centralized configuration

The Large Centralized solution offers the full range of conferencing features, particularly multiple simultaneous video, audio and data conferences that can be recorded and streamed for reliable delivery of high scale, high quality video. The solution is deployed with a minimal complete set of conferencing infrastructure at the company's site, allowing to call from endpoints and soft clients such as Avaya Equinox™ Meet—Me or Meetings for Web clients.

Avaya Equinox™ Meet-Me Client now integrates the Meet-Me functionality and replaces the Scopia client. This replacement is optional for an OTT deployment. Contact your administrator to continue using Scopia Desktop in the following cases: your deployment includes a third party session border controller (and not the Avaya SBCE required for Avaya Equinox™ Meet-Me); you currently need the Scopia Content Slider (which will be part of future releases).

In such deployment Avaya Equinox Management is split into management applications in headquarters, and Unified Portal , Web Gateway and Gatekeeper applications in branches to support service distribution. Reverse proxy and STUN/TURN functionalities are required for accessing infrastructure components such the Web Collaboration Server (WCS) and Portal. The Avaya Session Border Controller for Enterprise (ASBCE) or an approved third party edge device can provide these functionalities. This solution is highly scalable. For more capacity, add more of the same components such as ASBCE for Avaya Equinox™ Meet-Me clients.

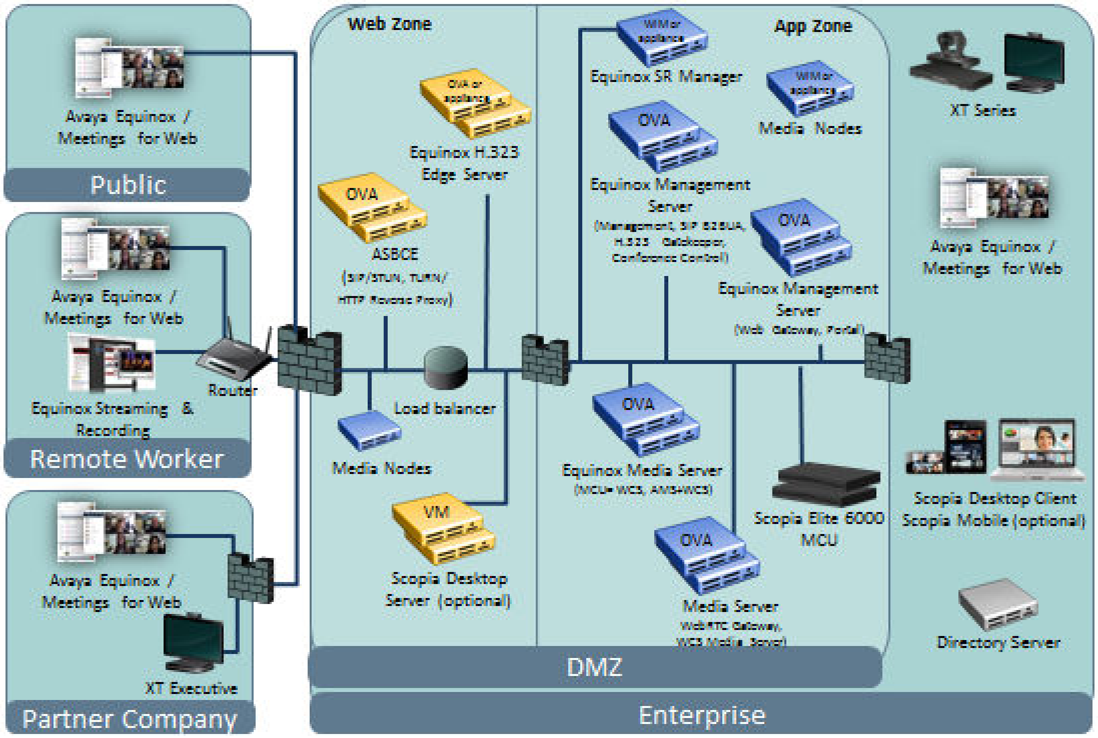


Figure 11: OTT Large Centralized configuration

OTT Large Distributed configuration

The Large Distributed solution is aimed at enterprises structured as headquarter and several branches. Typically, each branch would have one or more meeting rooms, and headquarters would have several meeting rooms. In this deployment, the video infrastructure is distributed in both headquarters and branches. The solution's capacity is still a maximum of 50 Avaya Equinox Media Servers, which can accommodate a total of 400,000 users in a variety of ways, including up to 7,500 simultaneous conference users (known as multipoint ports) such as endpoints and soft clients (for example, Avaya Equinox™ clients).

Avaya Equinox™ Meet-Me Client now integrates the Meet-Me functionality and replaces the Scopia client. This replacement is optional for an OTT deployment. Contact your administrator to continue using Scopia Desktop in the following cases: your deployment includes a third party session border controller (and not the Avaya SBCE required for Avaya Equinox™ Meet-Me); you currently need the Scopia Content Slider (which will be part of future releases).

In such a deployment Avaya Equinox Management is split into management applications in headquarters, and Unified Portal , Web Gateway and Gatekeeper applications in branches to support service distribution. ASBCE is required for supporting Avaya Equinox™ clients. The solution is highly scalable. For more capacity, add more of the same components such as ASBCE for Avaya Equinox™ Meet-Me clients.

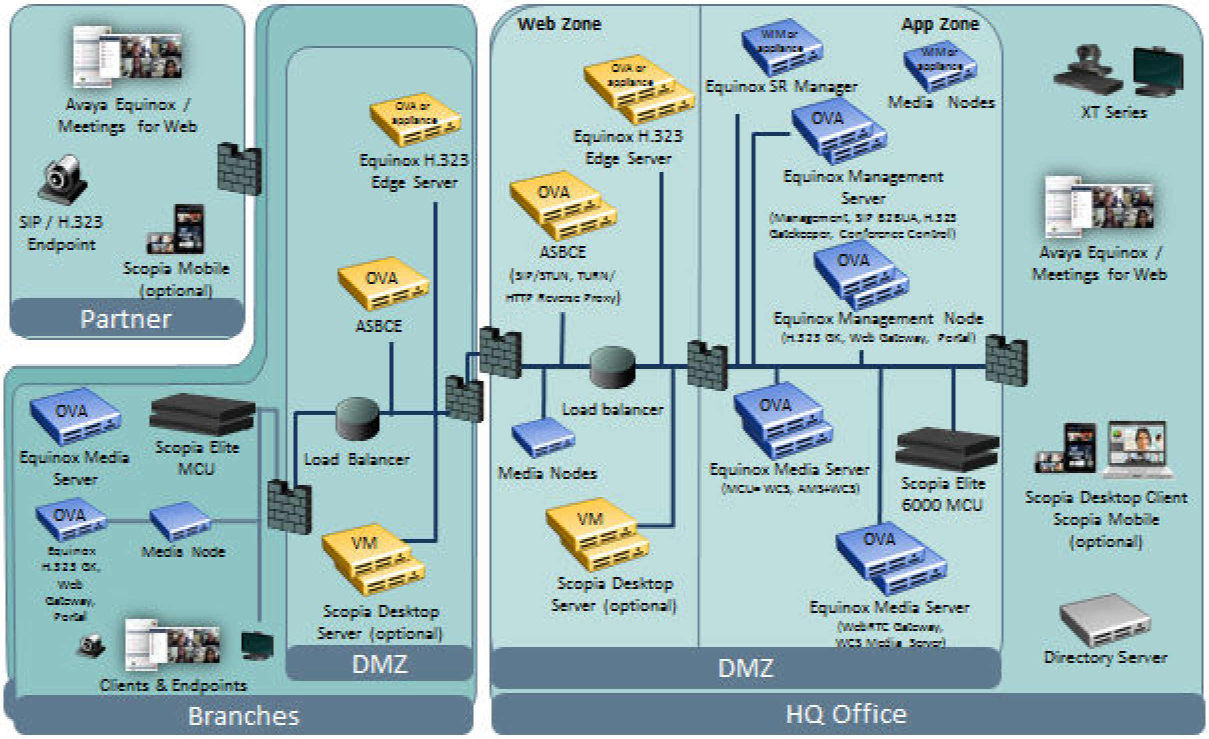


Figure 12: OTT Large Distributed configuration

Reference configuration for Over The Top deployment with Microsoft Unified Communications

Avaya Equinox for Over The Top supports UC integrations with Microsoft Lync or Microsoft Skype for Business (S4B). Integrating a Lync/Skype deployment offers text chat or instant messaging, voice and video communications, and content sharing between H.323 endpoints and Microsoft Lync or Microsoft Skype for Business (S4B) clients. The MS A/V Edge Server with TURN/STUN and ICE Servers, located in the DMZ, supports communication across networks. The Scopia® Video Gateway acts as a bridge between Lync/Skype endpoints and H.323 endpoints. Calls from Lync/ Skype clients are routed through Microsoft servers. Scopia® Video Gateway connects H.323 endpoints. Equinox Management manages the deployment.

Communicating with remote H.323 endpoints outside the organization is performed via Avaya Equinox H.323 Edge.

Avaya Equinox™ Meet-Me Client now integrates the Meet-Me functionality and replaces the Scopia client. This replacement is optional for an OTT deployment. Contact your administrator to continue using Scopia Desktop in the following cases: your deployment includes a third party session border controller (and not the Avaya SBCE required for Avaya Equinox™ Meet-Me); you currently need the Scopia Content Slider (which will be part of future releases).

The full extent of third party servers required for MS UC deployments is not listed here. For a complete list of UC servers required, refer directly to the vendor's documentation. Deployment diagrams focus on their integration with Avaya Equinox™ components only.

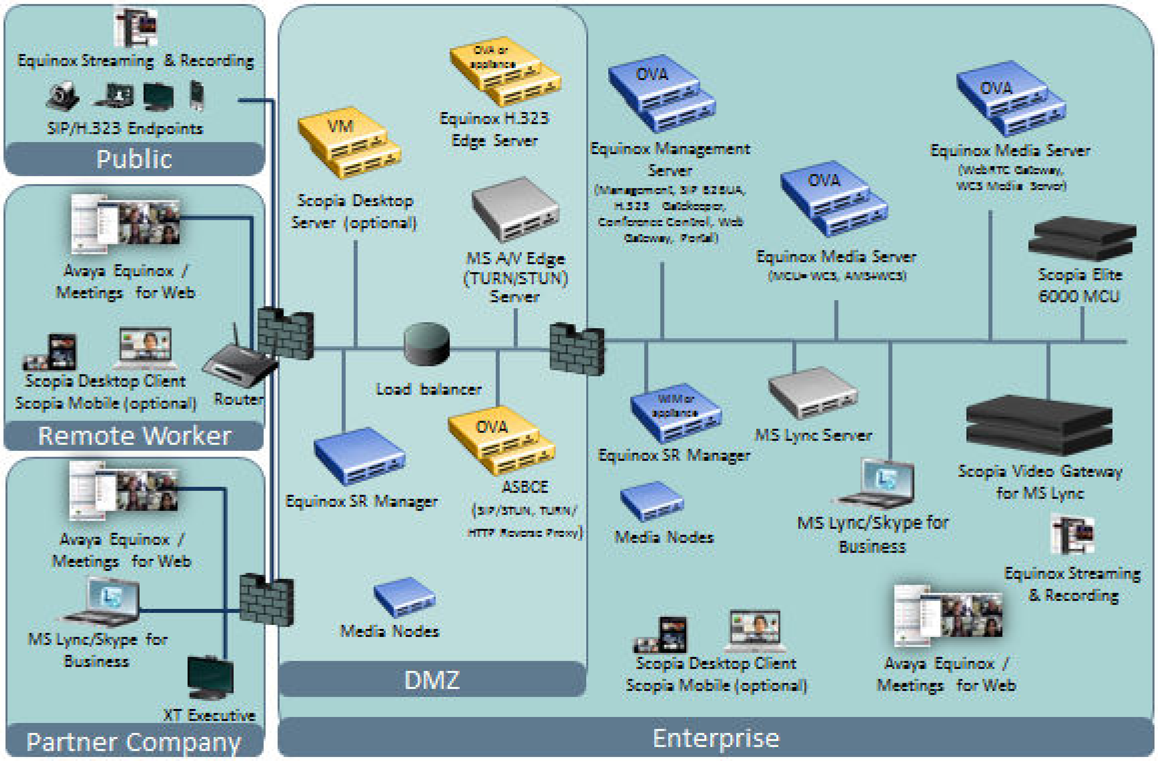

Equinox Streaming & Recording
SIP/H.323 Endpoints
Public
Avaya Equinox / Meetings for Web
Scopia Desktop Client
Scopia Mobile (optional)
Router
Remote Worker
Avaya Equinox / Meetings for Web
MS Lync/Skype for Business
XT Executive
Partner Company
VM
Scopia Desktop Server (optional)
OVA or appliance
Equinox H.323 Edge Server
MS A/V Edge (TURN/STUN) Server
Load balancer
Equinox SR Manager
OVA
ASBCE
(SIP/STUN, TURN/ HTTP Reverse Proxy)
Media Nodes
DMZ
OVA
Equinox Management Server
(Management, SIP B2BUA, H.323 Gatekeeper, Conference Control, Web Gateway, Portal)
OVA
Equinox Media Server
(MCU+ WCS, AMS+WCS)
OVA
Equinox Media Server
(WebRTC Gateway, WCS Media Server)
Scopia Elite 6000 MCU
VMM or appliance
Equinox SR Manager
MS Lync Server
Media Nodes
MS Lync/Skype for Business
Scopia Video Gateway for MS Lync
Equinox Streaming & Recording
Scopia Desktop Client
Scopia Mobile (optional)
Avaya Equinox / Meetings for Web
Enterprise

Figure 13: MS Lync UC in OTT deployment

Reference configuration for Over The Top deployment for Service Providers and Cloud services

With Avaya Equinox for Over The Top, service providers host the video infrastructure, while their customers deploy only endpoints like personal endpoints, telepresence systems, room systems, PCs or mobile devices. Customers enjoy the benefits of full HD video communications as VMR (Virtual Meeting Room) or Port Paid service. Communicating with remote H.323 endpoints outside the Cloud is performed via Avaya Equinox H.323 Edge, and with SIP endpoints and Avaya Equinox™ clients through the ASBCE.

Avaya Equinox™ Meet-Me Client now integrates the Meet-Me functionality and replaces the Scopia client. This replacement is optional for an OTT deployment. Contact your administrator to continue using Scopia Desktop in the following cases: your deployment includes a third party session border controller (and not the Avaya SBCE required for Avaya Equinox™ Meet-Me); you currently need the Scopia Content Slider (which will be part of future releases).

This solution is highly scalable. For more capacity, add more of the same components such as ASBCE for Avaya Equinox™ Meet-Me clients.. MS Lync is part of the solution and is supported with additional Microsoft and Gateway components.

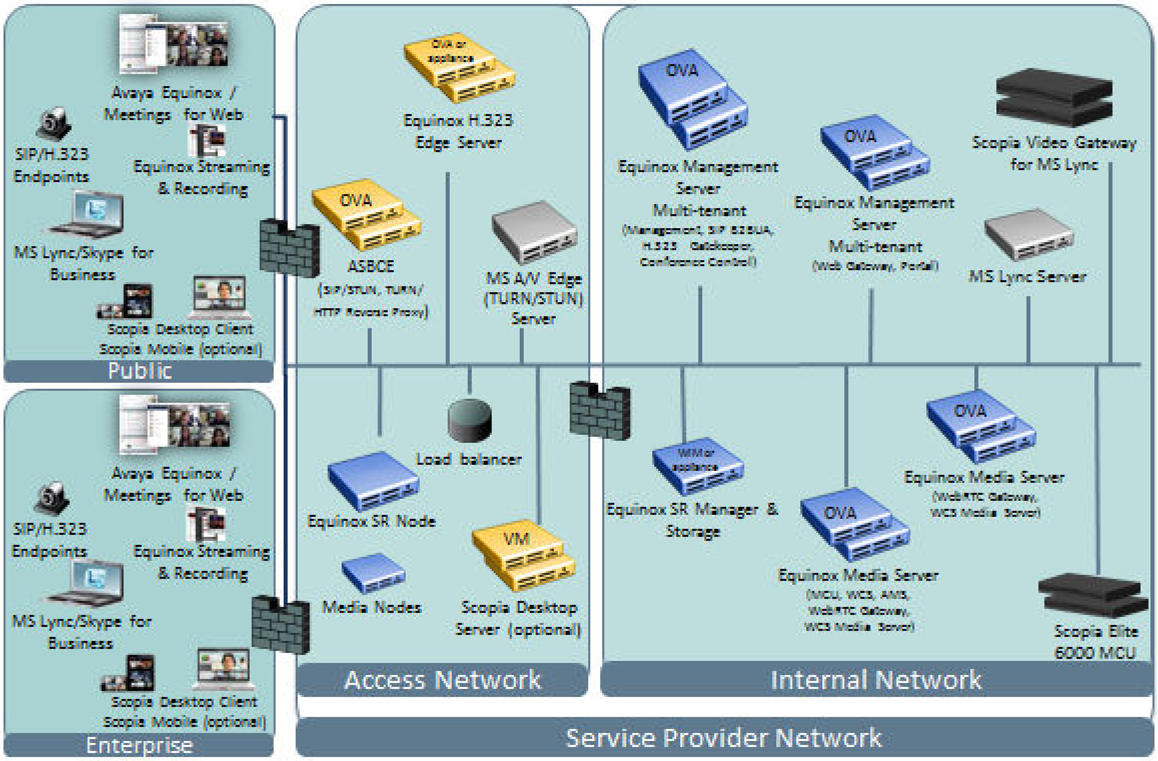

Avaya Equinox / Meetings for Web
SIP/H.323 Endpoints
Equinox Streaming & Recording
MS Lync/Skype for Business
Scopia Desktop Client
Scopia Mobile (optional)
Public
OVA or appliance
Equinox H.323 Edge Server
OVA
ASBCE
(SIP/STUN, TURN/ HTTP Reverse Proxy)
MS A/V Edge (TURN/STUN) Server
OVA
Equinox Management Server
Multi-tenant
(Management, SIP B2BUA, H.323 Gatekeeper, Conference Control)
OVA
Equinox Management Server
Multi-tenant
(Web Gateway, Portal)
Scopia Video Gateway for MS Lync
MS Lync Server
Avaya Equinox / Meetings for Web
SIP/H.323 Endpoints
Equinox Streaming & Recording
MS Lync/Skype for Business
Scopia Desktop Client
Scopia Mobile (optional)
Enterprise
Load balancer
Equinox SR Node
Media Nodes
VM
Scopia Desktop Server (optional)
Access Network
VM or appliance
Equinox SR Manager & Storage
OVA
Equinox Media Server
(WebRTC Gateway, WCS Media Server)
OVA
Equinox Media Server
(MCU, WCS, AMS, WebRTC Gateway, WCS Media Server)
Scopia Elite 6000 MCU
Internal Network
Service Provider Network

Figure 14: OTT Configuration for Service Providers and Cloud services

Reference configuration for Team Engagement deployment

The Avaya Equinox for Team Engagement solution integrates Avaya Equinox™ conferencing with Avaya Aura® existing and new customer solutions. An Aura environment including Session Manager, Communications Manager, System Manager, Presence Server along with Conferencing 9.0 (and up) providing Unified Communications services for an Enterprise including internal/external voice, audio/video conferencing, IM/Presence. Some users are assigned a virtual room. Both internal and external users join conferences in a guest role. The TE solution provides the full range of conferencing features, and particularly multiple simultaneous video, audio and data conferences that can be recorded and streamed for reliable delivery of high scale, high quality video. The solution supports products such as Avaya Equinox™ clients, Avaya H175 Video Collaboration Station, Avaya Vantage™, ASBCE, and SIP telephony infrastructure.

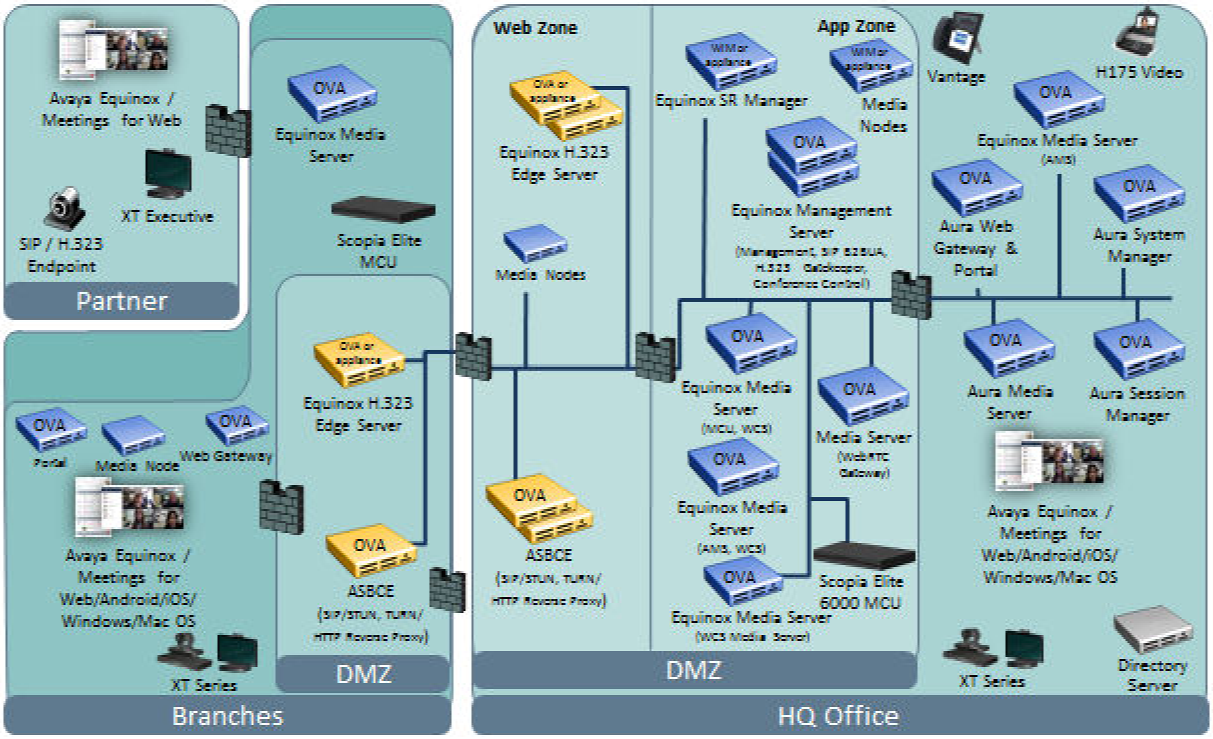


Figure 15: TE UC Distributed configuration

Chapter 3: Network planning and design considerations

Avaya Aura network planning and design considerations

For the latest and most accurate information on planning and designing your network for use with Avaya Aura components, go to https://support.avaya.com/

Firewall and NAT traversal options

The Equinox Solution provides a number of firewall and NAT traversal options allowing remote endpoints and clients to securely access the organization's protected network and initiate or join videoconferences.

These figures illustrate how the components interact with the means for protecting the organization against intrusive attempts:

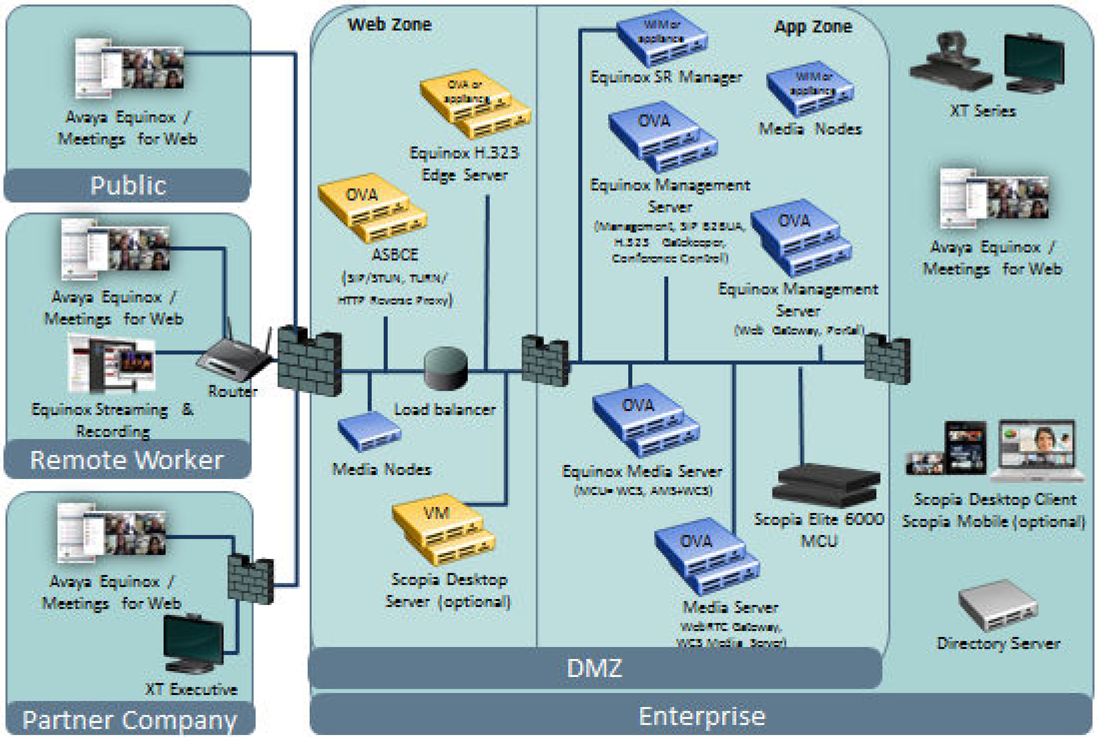

Web Zone
App Zone
Avaya Equinox / Meetings for Web
Public
Avaya Equinox / Meetings for Web
Router
Equinox Streaming & Recording
Remote Worker
Avaya Equinox / Meetings for Web
XT Executive
Partner Company
OVA or appliance
Equinox H.323 Edge Server
OVA
ASBCE
(SIP/STUN, TURN/ HTTP Reverse Proxy)
Load balancer
Media Nodes
VM
Scopia Desktop Server (optional)
WIM or appliance
Equinox SR Manager
WIM or appliance
Media Nodes
OVA
Equinox Management Server
(Management, SIP B2BUA, H.323 Gatekeeper, Conference Control)
OVA
Equinox Management Server
(Web Gateway, Portal)
OVA
Equinox Media Server
(MCU+ WCS, AMS+WCS)
Scopia Elite 6000 MCU
OVA
Media Server
WebRTC Gateway, WCS Media Server)
DMZ
XT Series
Avaya Equinox / Meetings for Web
Scopia Desktop Client
Scopia Mobile (optional)
Directory Server
Enterprise

Figure 16: Firewall and NAT traversal in the Equinox Solution — OTT deployment

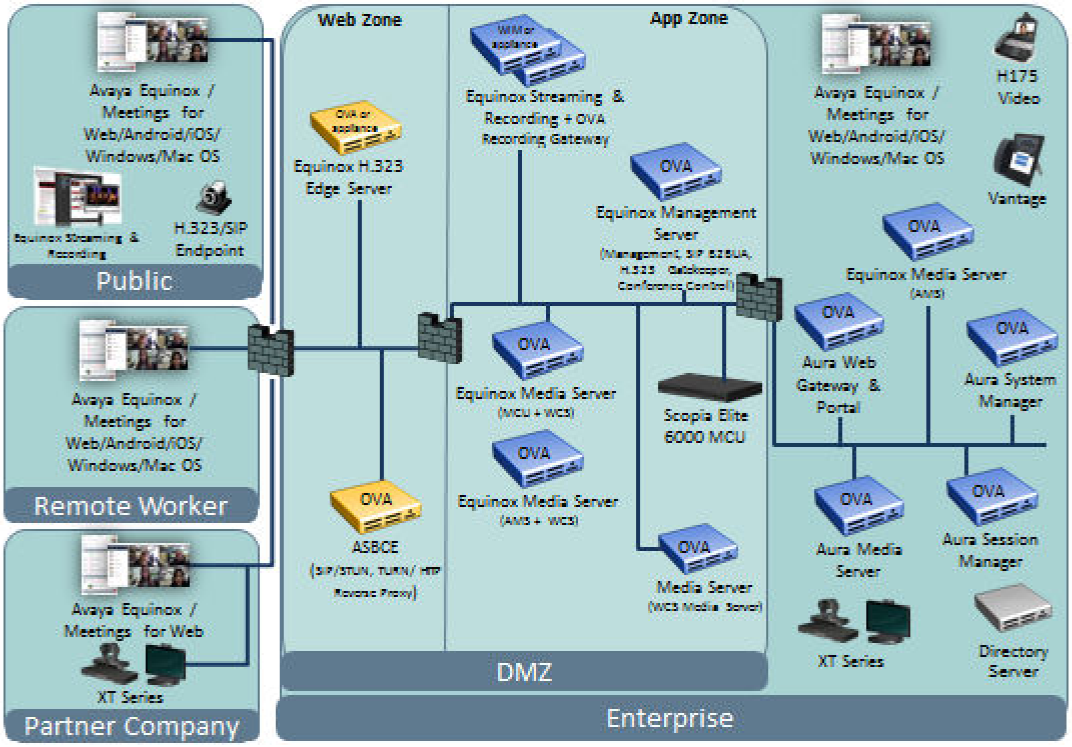

Web Zone
App Zone
Avaya Equinox / Meetings for Web/Android/iOS/ Windows/Mac OS
Equinox Streaming & Recording
H.323/SIP Endpoint
Public
Avaya Equinox / Meetings for Web/Android/iOS/ Windows/Mac OS
Remote Worker
Avaya Equinox / Meetings for Web
XT Series
Partner Company
OVA or appliance
Equinox H.323 Edge Server
OVA
ASBCE
(SIP/STUN, TURN/ HTTP Reverse Proxy)
WIM or appliance
Equinox Streaming & Recording + OVA Recording Gateway
OVA
Equinox Management Server
(Management, SIP B2BUA, H.323 Gatekeeper, Conference Control)
OVA
Equinox Media Server
(MCU + WCS)
OVA
Equinox Media Server
(AMS + WCS)
Scopia Elite 6000 MCU
OVA
Media Server
(WCS Media Server)
DMZ
Avaya Equinox / Meetings for Web/Android/iOS/ Windows/Mac OS
H175 Video
Vantage
OVA
Equinox Media Server
(AMS)
OVA
Aura Web Gateway & Portal
OVA
Aura System Manager
OVA
Aura Media Server
OVA
Aura Session Manager
XT Series
Directory Server
Enterprise

Figure 17: Firewall and NAT traversal in the Equinox Solution — Team Engagement deployment

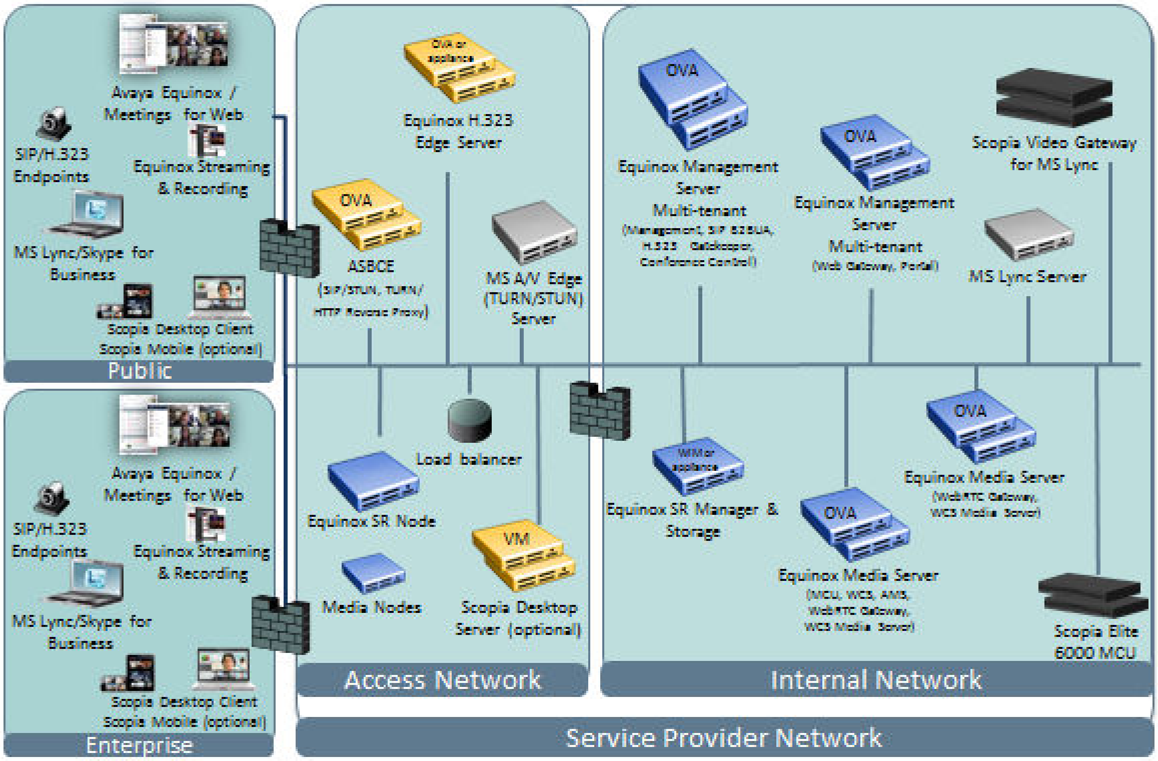

Avaya Equinox / Meetings for Web
SIP/H.323 Endpoints
Equinox Streaming & Recording
MS Lync/Skype for Business
Scopia Desktop Client
Scopia Mobile (optional)
Public
Avaya Equinox / Meetings for Web
SIP/H.323 Endpoints
Equinox Streaming & Recording
MS Lync/Skype for Business
Scopia Desktop Client
Scopia Mobile (optional)
Enterprise
OVA or appliance
Equinox H.323 Edge Server
OVA
ASBCE
(SIP/STUN, TURN/ HTTP Reverse Proxy)
MS A/V Edge (TURN/STUN) Server
Load balancer
Equinox SR Node
Media Nodes
VM
Scopia Desktop Server (optional)
Access Network
OVA
Equinox Management Server
Multi-tenant
(Management, SIP B2BUA, H.323 Gatekeeper, Conference Control)
OVA
Equinox Management Server
Multi-tenant
(Web Gateway, Portal)
Scopia Video Gateway for MS Lync
MS Lync Server
WM or appliance
Equinox SR Manager & Storage
OVA
Equinox Media Server
(MCU, WCS, AMS, WebRTC Gateway, WCS Media Server)
OVA
Equinox Media Server
(WebRTC Gateway, WCS Media Server)
Scopia Elite 6000 MCU
Internal Network
Service Provider Network

Figure 18: Firewall and NAT traversal in the Equinox Solution— Service Providers

- Two DMZ, one external (web zone) and one internal (application zone) with three firewalls.
- The Service Provider hosts the video infrastructure while their customers deploy only endpoints and soft clients. Connectivity is managed over a dedicated VPN or over the public Internet using standard firewall protocols such as H.460 and STUN/ICE/TURN. As privacy is crucial, all communications are fully secured using standard protocols like H.235 and TLS/SRTP.
- Remote H.323–standards endpoints can directly and securely dial into a meeting or an endpoint via Avaya Equinox H.323 Edge that provides a complete firewall and NAT traversal solution for H.323 deployments:

  This includes:

  - XT Series endpoints that are registered to Equinox H.323 Edge server via H.323 (with or without H.460)
  - H.460 compliant endpoints that are registered to Equinox H.323 Edge server
  - Guest endpoints (unregistered H.323 endpoints)
  - Multiple endpoints (can include non-H.460 endpoints) at a remote site that use Avaya Equinox H.323 Edge Client as a proxy to communicate with Equinox H.323 Edge server. This is useful if, for example, the organization has insufficient IP addresses available or if they have non-H.460 endpoints.

Other key features of Avaya Equinox H.323 Edge for seamless and intuitive connectivity between enterprises, partners, and home workers include:

- Full compatibility with H.323 Gatekeeper features such as enhanced dial plan, hierarchy, conference hunting, CDR records, and API for integration.
- Solving enterprise and remote site traversal issues without reconfiguring current security measures in existing firewalls.
- Using Equinox H.323 Edge server in a single or dual NIC configuration depending on the customer security policy and firewall utilization.
- URI dialing (for details, see URI Dialing Functionality on page 273).

- Remote XT Series SIP endpoints can use the Avaya Session Border Controller for Enterprise (Avaya SBCE) to securely traverse the organization's firewall and call into a meeting or an endpoint. The Avaya SBCE only supports remote workers using registered endpoints that are controlled by the enterprise.

  For information on the Avaya SBCE, see *Avaya Session Border Controller for Enterprise Overview and Specification*. For configuring the XT Series SIP endpoints and Avaya SBCE to work together, see the *Deployment Guide for Avaya Scopia® XT Series* and *Administering Avaya Session Border Controller for Enterprise*.

  Other key features of the Avaya SBCE include support of Far End Camera Control (FECC) and Binary Floor Control Protocol (BFCP).

- Remote Avaya Equinox™ Meet me and Meetings for Web (WebRTC) clients connect directly with the Avaya SBCE located in the DMZ. Avaya SBCE includes the URL rewriting feature, which enables clients to interact with different servers in the deployment via a single IP address and a single FQDN. As each FQDN needs a certificate, and there is only one FQDN to interact with, this feature also allows saving on the costs of commercial certificates. For more information, see *Deploying Avaya Equinox Solution*.
- (Optional in OTT) Scopia Desktop Client and Scopia Mobile have their own secure traversal methods and are connected directly to the Scopia Desktop Server located in the DMZ.
- Streaming clients use the Avaya SBCE reverse proxy functionality (or Avaya authorized, third party proxies) to connect the Media Node and Manager of the Equinox Streaming and Recording server. For a list of third party reverse proxies, see *Administration Guide for Avaya Equinox Streaming and Recording Server*.

  A reverse proxy is a web server that terminates connections with clients and makes new connections to backend servers on their behalf. A backend server is defined as a server to which the reverse proxy makes a connection to fulfill the request from the client. These backend servers can take various forms, and reverse proxy can be configured differently to handle each of them.

- Remote Microsoft Lync or Skype for Business clients traverse firewalls using the Microsoft Audio/Video (MS A/V) Edge Server. The server integrates the TURN/STUN which enables remote endpoints to securely access the organization network. With the Scopia® Video Gateway bridging between Lync and H.323 networks, remote Microsoft Lync clients can join an H.323 videoconference.

Securing Your Deployment

Equinox Solution deployments offer robust security in video communications based on standard protocols and powerful encryption algorithms, resulting in a well-integrated and secure solution.

Note:

Avaya recommends encrypted SIP as the preferred protocol, with TLS and SRTP for secure data transfer.

There are several aspects to the security of a deployment:

- The content of a video call, including its video, audio and data presentations can be encrypted to protect from eavesdroppers. Connections can also be authenticated to ensure each member of the call is who they claim to be.

  In addition to the media content of a call, the signaling and management streams can also be secured when crossing network zones, depending on the nature of your deployment and network topology.

- The permissions and rights of users can be defined via user groups, to determine the functionality available to each user of the system. Enabling or disabling a feature can be achieved by defining groups and moving users among the various groups.

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.

The figure below gives an overview of the security of media, signaling, and management connections in an Equinox Solution deployment, which recommends the use of two DMZ zones with three firewalls: the web zone for publicly accessed servers; the application zone for application servers.

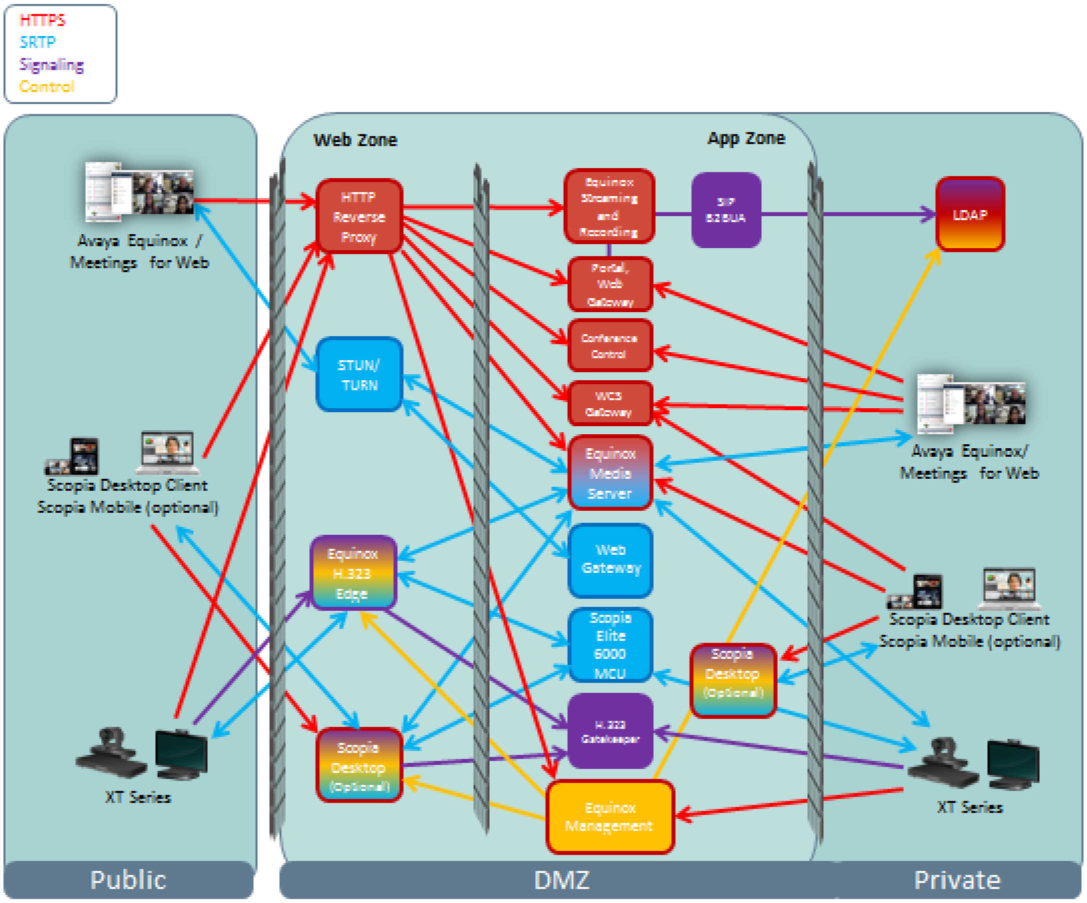


Figure 19: Encrypted media, signaling, and control connections of the OTT Equinox Solution

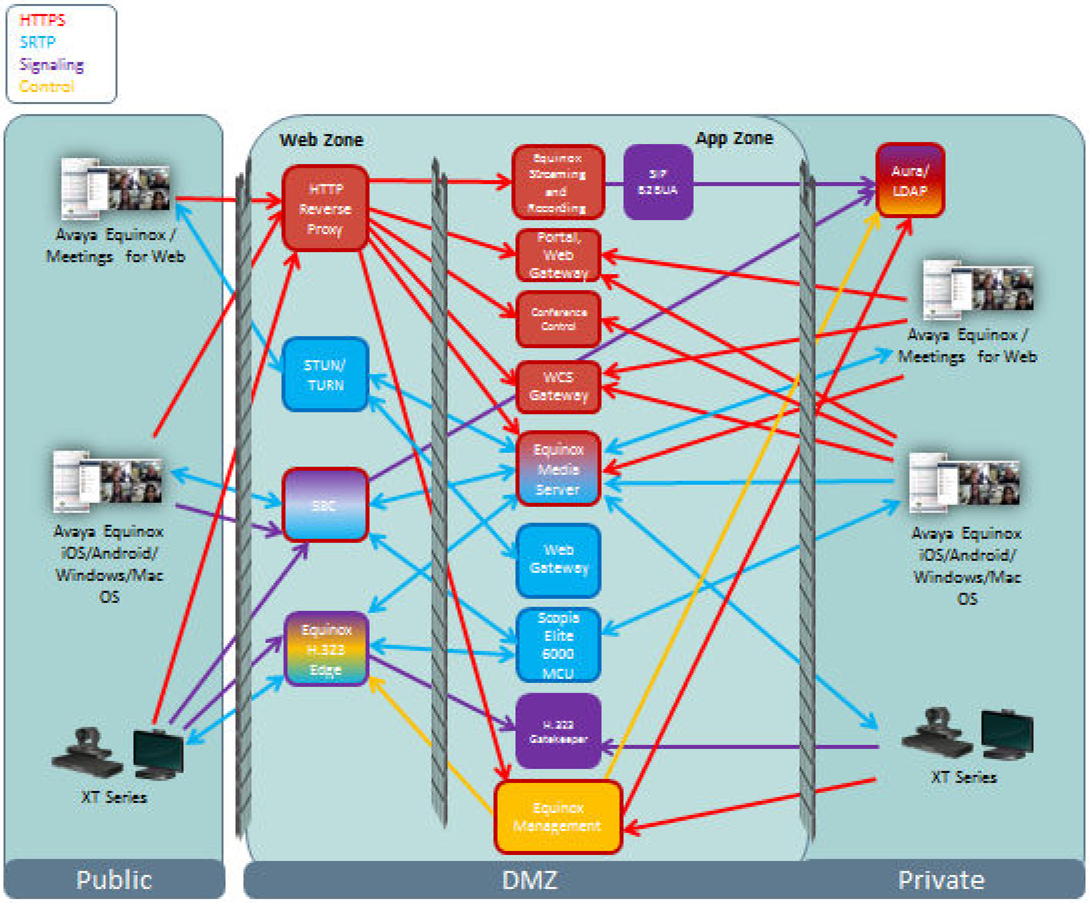


Figure 20: Encrypted media, signaling, and control connections of the TE Equinox Solution

The sections in this chapter are:

Related links

[Authentication and Encryption](#) on page 42
[About Media Security](#) on page 43
[About Signaling Security](#) on page 44
[About Management Security](#) on page 45

Authentication and Encryption

The authentication and encryption of the Equinox Solution's infrastructure uses standard protocols and algorithms to provide a solution that is secure, effective and reliable. There are three types of data streams to a video communication in the Equinox Solution infrastructure which can be secured:

- Media

  Media refers to the live audio, video and shared data streams sent during a call.

- Signaling (call and media control)

  Signaling, also known as call control, sets up, manages and ends a connection or call. Control, or media control, sets up and manages the media of a call (its audio, video and data).

- Management

  Management refers to the administration messages sent between components of the Equinox Solution as they manage and synchronize data between them.

Important:

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

The sections in this chapter are:

Related links

Securing Your Deployment on page 40

About Media Security

Securing the media communications in the Equinox Solution refers to encrypting the content of a call, including its audio, video, and data presentations.

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.

In a Equinox Solution deployment, call content in both SIP and H.323 environments are encrypted:

- In SIP environments, the media is encrypted and authenticated using the Secure Real-time Transport Protocol (SRTP).
- In H.323 environments, encryption of call content is secured with the H.235 encryption annex standard. H.323 endpoints can access the Avaya Equinox H.323 Edge server with an encrypted H.235 connection, provided the endpoint itself supports the H.235 standard.

Note:

- Avaya recommends encrypted SIP as the preferred protocol, with TLS and SRTP for secure data transfer.
- Deploy Equinox H.323 Edge server only in legacy Avaya Scopia solution deployments. The H. 323 protocol is used only in legacy Avaya Scopia deployments.

WebRTC for Avaya Equinox Meetings for Web is only supported in a secured environment (HTTPS). Media from/to the browser is encrypted.

(Optional in OTT deployments) The Scopia Desktop Server's secure connection with the Scopia Desktop Client is another line of communication that must be secured, since it often stretches across network zones and outside the corporate network. Scopia Desktop's media over a TCP connection is encrypted using HTTPS, while under UDP connections, media is encrypted using S-RTP, using random encryption keys exchanged over HTTPS.

Equinox Streaming and Recording does encrypted HTTPS media on the recording playback or HLS live stream.

H.460 endpoints can access the Equinox H.323 Edge server directly with an encrypted data stream.

❗ **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.

Components associated with coordinating and directing calls, such as the Equinox Management or H.323 Gatekeeper, do not directly send or receive call content, since their function is to direct traffic and manage network connections. Therefore they do not feature in the media layer of the solution.

Related links

Securing Your Deployment on page 40

About Signaling Security

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.

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.

In a SIP environment, much of the signaling that crosses network zones is encrypted and authenticated using the Transport Layer Security (TLS) standard.

For example, all signaling messages sent from Avaya Equinox Management’s Back-to-Back User Agent to SIP servers are secured via the Transport Layer Security (TLS) protocol.

Avaya Equinox™Meet-Me Clients and Scopia Desktop software-based clients (optional, for OTT deployments) might be outside a VPN in the public network, and are encrypted and authenticated over HTTPS, using TLS.

Streaming and recording media streams are encrypted with HTTPS / SSL. If media encryption is set up for Scopia Desktop Server, it must also be enabled in Equinox Streaming and Recording.

Related links

Securing Your Deployment on page 40

About Management Security

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.

When management communications are performed via a web interface, they are secured and authenticated via the HTTPS protocol.

When management messages cross network zones, they are typically encrypted and authenticated. For example, Equinox Management's management messages to the Equinox media Server are protected using TLS.

Related links

Securing Your Deployment on page 40

Securing Access to Functionality with User Profiles

User groups and the functionality granted to each group can be defined in a number of components of the Equinox Solution. Each server component can only be accessed with a login, and depending on the privileges of that username, different functionality is visible to that user. However, from the perspective of the Equinox Solution, you can define a single repository of users and user groups with Avaya Equinox Management.

Equinox Management can define its own user database, or it can use the LDAP corporate database like Microsoft's Active Directory. The Equinox Management user database can be pushed or downloaded to the various components of a Equinox Solution deployment, so they are all synchronized with the same user profiles and rights.

For more information on setting up a unified user database, see the *Administrator Guide for Equinox Management*.

Planning a Centralized or Distributed Topology (Cascading) for MCU

When your organization has more than one site, like a headquarters and several branches, the Equinox Solution offers a unique method of cutting video bandwidth costs, known as cascaded meetings.

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.

Without cascading, if you choose a centralized MCU deployment, frequent videoconferences between branches can be expensive (Figure 21: Centralized MCU deployment, where all branches use the HQ MCU on page 46).

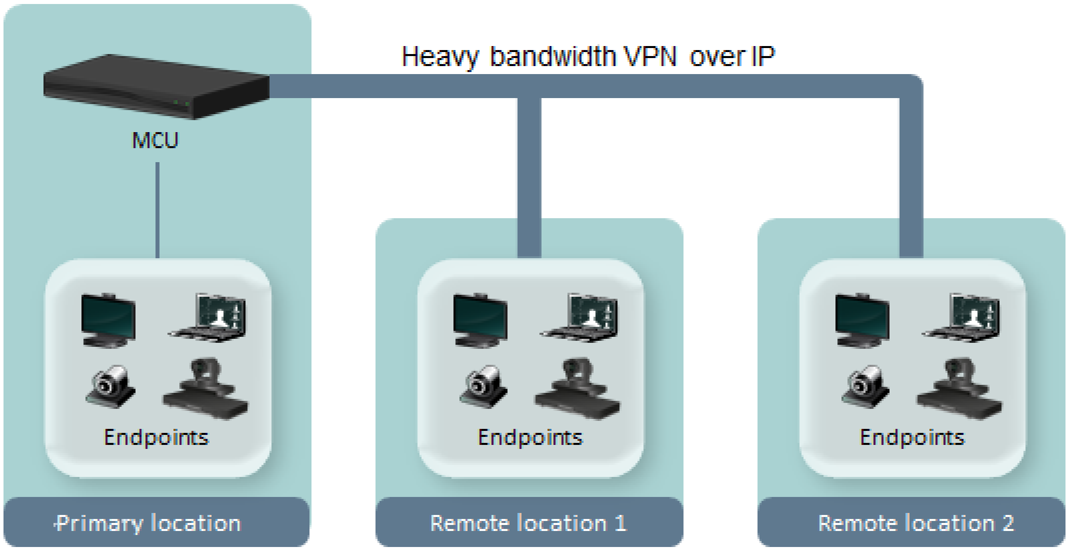


Figure 21: Centralized MCU deployment, where all branches use the HQ MCU

To reduce cross-site bandwidth costs, a distributed MCU deployment (Figure 22: Distributed MCU deployment cascading meetings for reduced WAN bandwidth on page 47) can perform cascaded conferences. Participants connect to their local MCU, and the conference is cascaded by connecting between the MCUs using a fraction of the bandwidth compared to the centralized deployment. The same principles apply to an MCU in the same location, thus increasing call capacity by cascading conferences between them.

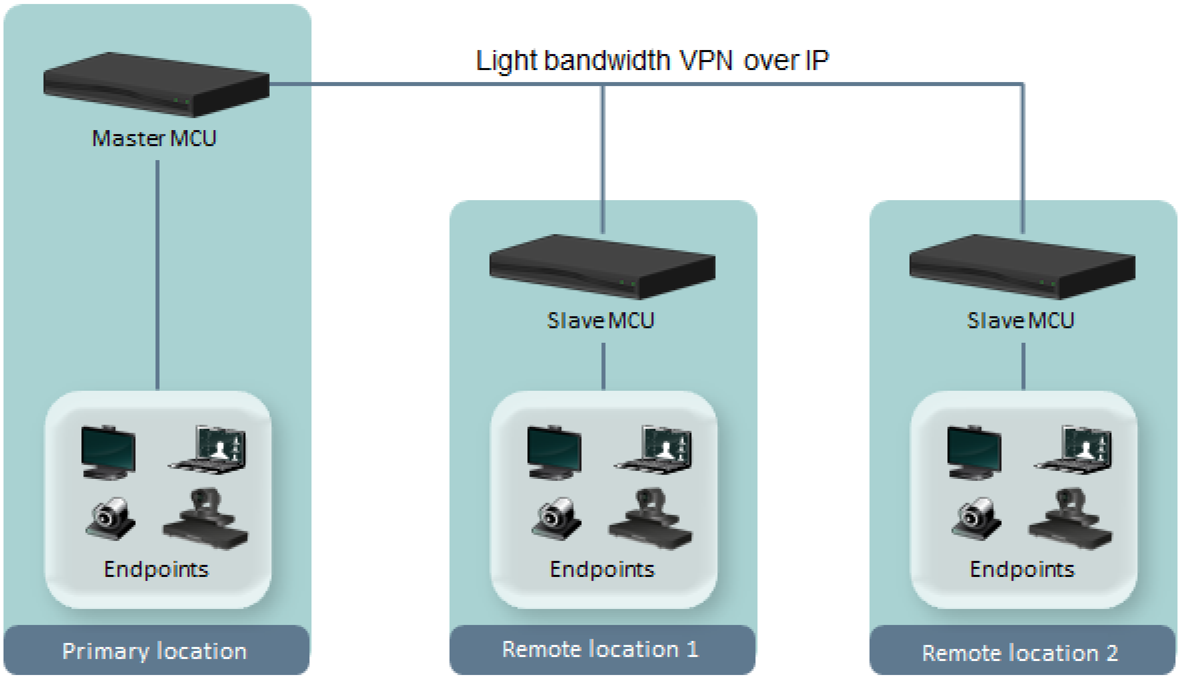


Figure 22: Distributed MCU deployment cascading meetings for reduced WAN bandwidth

The bandwidth used by a cascaded link is equivalent to only a single client connection in each direction: upload and download. The bandwidth value is determined by the MCU meeting type (or service), which is invoked when choosing a dial prefix for the meeting. You define the maximum bandwidth for each meeting type in the MCU. For more information on defining meeting types, see *Administrator Guide for Scopia® Elite 6000 MCU*.

Users do not need to choose a specific MCU. The powerful functionality of virtual rooms enables you to dial the same number anywhere in the world, while the Equinox Solution infrastructure transparently directs you to the correct meeting on the correct MCU.

The maximum supported number of participants in a single videoconference is 500 for both the centralized and distributed MCU deployment.

Users do not need to manually enable cascading when creating meetings. This is performed transparently by Avaya Equinox Management using sophisticated cascading algorithms.

When an endpoint initiates a meeting on an MCU, that MCU becomes the master MCU. Other MCUs which participate in the meeting are designated as slave MCUs. There are a number of factors that might influence when the system automatically chooses to cascade to a different MCU. For example, to avoid reaching the maximum bandwidth threshold, the system would attempt cascading with a different MCU, a slave MCU. Endpoints would then join the videoconference from the slave MCU. Only one level of cascading is supported: all slave MCU conferences must cascade to the same master MCU conference. Administrators can also customize the priority given to cascading in a distributed topology, as explained in *Administrator Guide for Avaya Equinox Management* .

Cascading has the following characteristics:

- A cascaded connection uses two ports —one port on the master MCU, and one port on the slave MCU.
- Make sure that the Meeting Type (MCU service), representing the required meeting properties and accessed with a dial prefix, is available on all participating MCUs. For example, if the meeting uses MCU service 81, then 81 must exist on the master MCU and on the slave MCUs.
- Participants connecting to the slave MCU:
    - View only the default meeting layout
    - Can send and receive video with a resolution up to 1080p x 60fps for Scopia® Elite 6000 MCU and 720p x 30fps for Scopia® Elite 5000 Series MCU. The video resolution depends on the cascading connection settings.
    - Perform actions (such as joining the meeting) via their endpoint or web interface, and not via DTMF.
- Only one participant at a time (typically the active speaker) connecting from each slave MCU can send video and be seen by other meeting participants in the video layout.
- The lecturer and any telepresence endpoint always connect to the videoconference from the master MCU. Port s are reserved on the master MCU to support these features.
- Endpoints seamlessly join a videoconference according to the cascading logic implemented on the sites. An endpoint connected to a slave MCU and trying to launch a feature which is not supported by the slave MCU gets a relevant error message. You can move an endpoint to a master MCU when scheduling your videoconference. For more information, see *User Guide for Avaya Equinox Management*.
- Scopia Elite MCU does not support cascading to legacy Scopia MCU instances.

You can customize the cascading priorities in Equinox Management in a number of ways:

- Default to using a local MCU first, and only cascade conferences if required.
- Prioritize cascading wherever possible, to keep bandwidth costs to an absolute minimum.
- Avoid cascading as often as possible.

For more information on implementing cascading in Equinox Management, see *Administrator Guide for Avaya Equinox Management* .

Planning Scalability and High Availability in the Equinox Solution

Scalability describes the ability to increase the capacity of a network device by adding another identical device (one or more) to your existing deployment. In contrast, a non-scalable solution would require replacing existing components to increase capacity.

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.

There are several ways to ensure your deployment of the Equinox Solution maintains a very high degree of availability, and also add extra capacity to your video infrastructure:

Related links

High Availability of Equinox Management on page 49
Scalability and High Availability of Scopia Desktop Server and Equinox H.323 Edge server on page 51
Scalability and High Availability with Scopia® Video Gateway on page 51
Scalability and High Availability with Multiple MCUs on page 52
Scalability with Equinox Streaming and Recording on page 52

High Availability of Equinox Management

To provide high availability and continued service, you can deploy redundant Avaya Equinox Management servers, in one of the following ways:

- Local redundancy

  Deploy two Equinox Management servers in the same location: a primary server and a secondary server. If the primary server fails, the secondary server automatically takes over without disrupting Equinox Management functionality (does not include load balancing).

- Geographic redundancy

  Deploy three Equinox Management servers. Set up two servers as primary/secondary servers in the same location (local redundancy), and deploy the third as an off-site backup server in a different location. You can manually activate this server if the other servers fail, ensuring continued service even if there is a major failure or disaster at the main location.

  ❗ **Important:**

  We recommend configuring the backup server while the system is inactive. This is because a huge amount of data is transferred to the remote site, which can deplete network bandwidth resources.

Figure 23: Local and geographical redundancy on page 50 illustrates the different options of deploying Equinox Management redundancy.

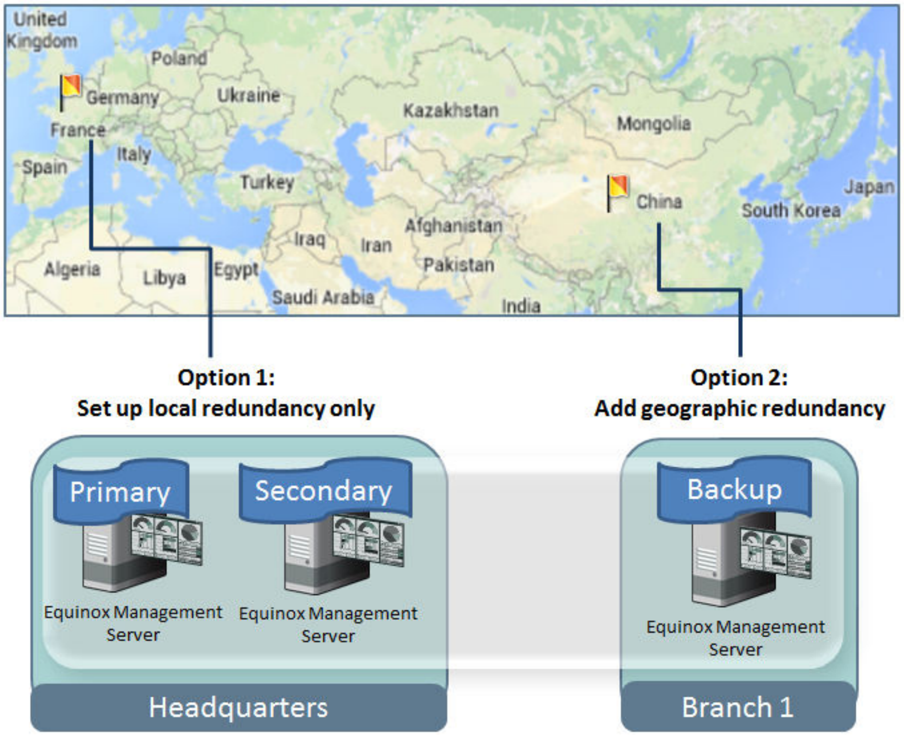


Figure 23: Local and geographical redundancy

Equinox Management's redundant solution requires a license, but does not require third-party load balancers. Data is continuously synchronized between all Equinox Management servers, including the internal database, system property files, and device upgrade packages.

Deploy your Equinox Solution by referring to component names rather than IP addresses. Using a server name (or FQDN), like *smgmt.company.com*, reduces maintenance when servers switch to their backups.

Note:

For all deployments, you must use FQDNs. FQDNs are essential when using TLS.

Local redundancy can be deployed with an internal or external database; geographical redundancy supports only the internal database (see *Administrator Guide for Avaya Equinox Management*).

Once Equinox Management's high availability is configured, you can view the redundancy status in real-time, including the current status and server addresses (see *Administrator Guide for Avaya Equinox Management* for details).

For more details on setting up additional Equinox Management servers, see the *Administrator Guide for Avaya Equinox Management*.

Related links

Planning Scalability and High Availability in the Equinox Solution on page 48

Scalability and High Availability of Scopia Desktop Server and Equinox H.323 Edge server

You can configure Scopia Desktop Server and Equinox H.323 Edge server for scalability and high availability. More servers translates to higher capacity, and with a load balancer in place, if one server fails, the remaining servers can continue working, offering even higher reliability in video services. Equinox H.323 Edge servers and Scopia Desktop Servers can share the same load balancing deployment

Add Equinox H.323 Edge servers to increase capacity and reliability of remote access endpoints connecting to videoconferences in your organization.

(Optional, for OTT deployments) Add Scopia Desktop Server to increase the reliability and number of Scopia Desktop Clients connecting to your enterprise with video and data at the same time.

Note:

Equinox Solution release 9.0.2 provides the Scopia Desktop Client and Scopia Mobile functionality in the Avaya Equinox™ Meet-Me Client. Contact your administrator to continue using Scopia Desktop in the following cases: you do not wish to deploy the Avaya SBCE (required for Avaya Equinox™ Meet-Me); you currently need the Scopia Content Slider (which will be part of future releases).

You can choose one of the following:

- You can deploy multiple Scopia Desktop Servers, using Avaya's authorized load balancers.
- You can deploy multiple Equinox H.323 Edge servers, using Avaya's authorized load balancers.

When dialing out, you can configure the H.323 Gatekeeper to find an Equinox H.323 Edge server at one of several IP addresses, thereby enabling the gatekeeper to perform a round robin search for an available Equinox H.323 Edge server. From Release 9.0, the gatekeeper is an application service in Equinox Management.

For more information on the configuration of each of these deployments, see the components' administrator guides.

Related links

Planning Scalability and High Availability in the Equinox Solution on page 48

Scalability and High Availability with Scopia® Video Gateway

You can deploy multiple Scopia® Video Gateways to make more simultaneous calls from endpoints with these protocols available in your video network. For more information on scaling your gateway deployments, see the *Lync Deployment Guide for Scopia® Video Gateway for Microsoft Lync* .

Avaya Equinox Management acts as the load balancer in these deployments and can hot switch to an alternative unit if one of the gateways fails to maintain and preserve high availability of the service.

Related links

Planning Scalability and High Availability in the Equinox Solution on page 48

Scalability and High Availability with Multiple MCUs

You can deploy multiple MCUs to make more simultaneous calls available in your video network. For more information on scaling your MCU deployment, see *Administrator Guide for Avaya Equinox Media Server* or *Administrator Guide for Scopia® Elite 6000 MCU*.

You do not need to deploy a load balancer for multiple MCUs. Equinox Management can be configured to maintain high availability of video call service by coordinating amongst multiple MCUs. Equinox Management can hot switch to an alternative unit if an MCU fails to maintain and preserve high availability of the service.

For details of how to configure Equinox Management for high availability, see the *Administrator Guide for Avaya Equinox Management*.

Related links

Planning Scalability and High Availability in the Equinox Solution on page 48

Scalability with Equinox Streaming and Recording

You can deploy multiple Equinox Streaming and Recording Media Nodes in multiple locations to get higher capacity for simultaneous recording and outgoing streaming to users. Consider the following:

- A scalable deployment is built on multiple Equinox Streaming and Recording Servers. It uses one centralized Manager running on a dedicated server and Media Nodes for delivering the streaming and/or recording functionalities on separate servers. For example, if you need a large audience watching live streaming, focus on deploying more Media Nodes with streaming functionality.

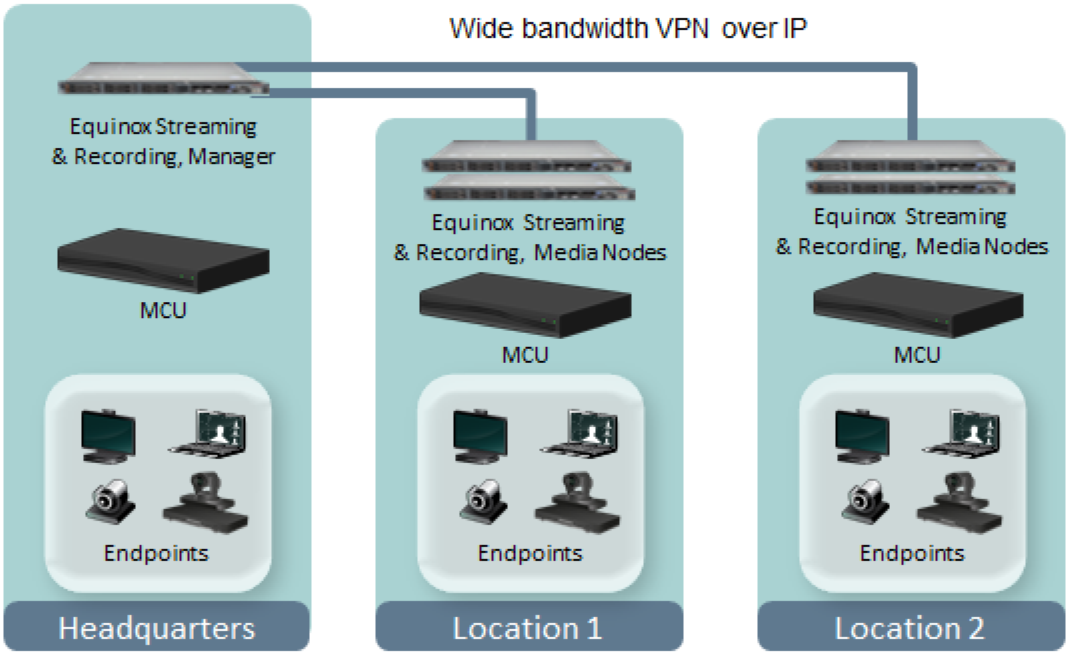

Wide bandwidth VPN over IP
Equinox Streaming & Recording, Manager
MCU
Endpoints
Headquarters
Equinox Streaming & Recording, Media Nodes
MCU
Endpoints
Location 1
Equinox Streaming & Recording, Media Nodes
MCU
Endpoints
Location 2

Figure 24: Scaling up streaming and recording

The maximum number of live stream viewers in the system is 100,000. You can have 3,500 live stream viewers per Media Node configured for streaming only, and 1,500 viewers for combined recording and streaming Media Nodes.

- Level of required scalability

  Decide how to scale up Media Nodes at each location. You can put a Media Node for local recording and streaming at each site to increase capacity and quality and minimize bandwidth over the WAN or VPN. You can also cluster Media Nodes for playback, recording, and streaming. This allows, for example, sending one copy of the stream over the WAN to other locations and have it replicated there.

  If possible, install Media Nodes near Equinox Media Server or Scopia Elite MCU to avoid video loss due to bad network connection. For example, if you have MCUs in three or four different locations, and if you want people in these locations to be able to record and watch without the latency of going across long distances, consider installing one or more Media Nodes in each of the locations where the MCUs are located.

  You can create viewer mappings to have users in IP zones mapped to Media Nodes in the same zone and map recording servers to the same zone (or location) as the MCU. For more information, see the *Administrator Guide for Equinox Streaming and Recording Server*.

- Using a Private Content Delivery Network (CDN), a 3rd Party CDN, or a combination of both

  You can build your own private CDN with clusters of Media Nodes located within one location, or a small cluster in the main location and a large distributed environment across your organization. Viewers belonging to the organization can get their recordings and live media from their local Media Nodes without affecting the network.

If you have many viewers wanting to access streaming and recording from external networks, you can add CDN ability to your deployment by turning on a Virtual Delivery Node (VDN) that communicates with a third-party CDN such as Highwinds. External customers buy an account with Highwinds and decide how much bandwidth and storing they need.

Or, you can work with a combination of private and third-party CDNs. With this type of deployment, you can keep contents inside your private network and choose which live events and recordings go out to the CDN for external customers to watch and view.

Note:

Only Highwinds is supported as cloud CDN at this time.

For more information on deploying additional servers, see *Deploying Avaya Equinox Solution* and *Administration Guide for Equinox Streaming and Recording Server*.

Related links

Planning Scalability and High Availability in the Equinox Solution on page 48

Scalability on page 54

Scalability

Introduction

The Equinox Streaming and Recording is installed on a Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, or HP ProLiant DL360 G9 server, provided by Avaya. Alternatively, you can purchase a Microsoft™ Windows Image (WIM) and install Equinox Streaming and Recording on your own server. If you are providing your own server, the specifications must match those of the Avaya-provided servers. 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.

Note:

The Avaya-provided servers: Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, and HP ProLiant DL360 G9 are often referred to as the Avaya Common Server(s).

Recording (Dell™ PowerEdge™ R620)

Equinox Streaming and Recording supports up to 10 high definition (1080p) or 30 standard definition (480p) recordings with H.239 simultaneously. The system negotiates high definition whenever possible.

The resolution negotiated is based on the configuration of the MCU/Media Server service as well as the Equinox Streaming and Recording profile. By limiting the profile to 480p or less, you can do 30 simultaneous recordings (trading off higher quality recordings versus the ability to do more recordings).

Equinox Streaming and Recording supports a mix of resolutions, and can do three standard definition calls for every one high definition call. So, for example, if the system is licensed for 10 concurrent recordings, you can do any of the combinations of calls in Table 1: Call Combinations on the Dell PowerEdge R620 on page 55.

Table 1: Call Combinations on the Dell™ PowerEdge™ R620

High Definition	Standard Definition
0	30
1	27
2	24
3	21
4	18
5	15
6	12
7	9
8	6
9	3
10	0

Recording (Dell™ PowerEdge™ R630 and HP ProLiant DL360 G9)

The Dell™ PowerEdge™ R630 and HP ProLiant DL360 G9 (or Avaya-approved equivalent[1]) offers higher scalability than the Dell™ PowerEdge™ R620. When the CP is configured on an all-in-one server or when it is configured with a DN, Equinox Streaming and Recording supports 20 high definition and 50 low definition simultaneous recordings. These values are an increase from 10 high definition and 30 low definition in a Dell™ PowerEdge™ R620 deployment, as listed in Table 2: Concurrent recordings on the Dell PowerEdge R630 and HP ProLiant DL360 G9 on page 55. When the CP is on a separate server, it offers even higher scalability with 40 medium definition and 60 low definition simultaneous recordings.

Table 2: Concurrent recordings on the Dell™ PowerEdge™ R630 and HP ProLiant DL360 G9

	CP-only	All-in-one or with a DN
1080p	10	10
720p	20	20
480p	40	30
360p	60	50

Playback

On a standalone media node configured for DN only, Equinox Streaming and Recording supports up to 3,500 viewers at 720p / 768K for live broadcast or video on demand playback simultaneously.

On all-in-one servers or media nodes configured with DN and CP, Equinox Streaming and Recording supports up to 1,500 viewers at 720p / 768K for live broadcast or video on demand playback simultaneously.

Related links

Scalability with Equinox Streaming and Recording on page 52

[1] For more information on supported servers, contact Avaya using https://support.avaya.com.

Planning User Access to Videoconferences

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

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

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

- From Microsoft Outlook (2010 or later), using an Equinox Management plug-in for Microsoft Outlook.
- From the Equinox Management User Portal.

When scheduling from either one of these plug-ins for Microsoft Outlook, Equinox Management reserves both the endpoint resources and their required media server connections.

Users can start instant meetings in one of the following ways:

- Dialing an endpoint directly from another endpoint. To dial more than one endpoint, users dial a virtual room number (personal or public), or an IVR session (a default room with a generic greeting).
- Dialing an endpoint from their virtual room with a client such as Avaya Equinox™ Meet-Me, using the MCU dial prefix.

You set up the media server prefix and virtual room numbers according to your organization's dial plan.

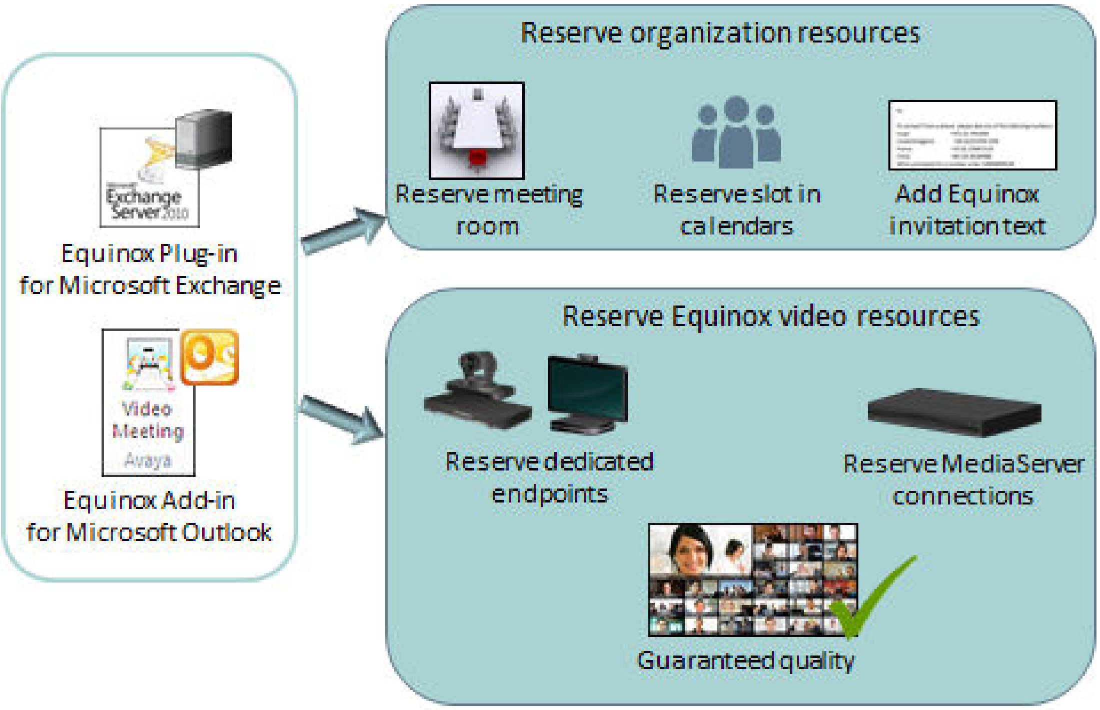

Equinox Plug-in for Microsoft Exchange
Exchange Server 2010
Video Meeting Avaya
Equinox Add-in for Microsoft Outlook
Reserve organization resources
Reserve meeting room
Reserve slot in calendars
Add Equinox invitation text
Reserve Equinox video resources
Reserve dedicated endpoints
Reserve MediaServer connections
Guaranteed quality

Figure 25: Planning User Access to Scheduling Meetings

The most common way for users to schedule videoconferences is from Microsoft Outlook, since they are already familiar with its interface and are using it to schedule all other (non-video) meetings. This requires deploying one of the Equinox Management plug-ins for Microsoft Outlook.

Decide which plug-in is right for your organization by using Table 3: Comparing features of the different Microsoft Outlook Plug-ins on page 57 as a guide. For example, if users in your organization have Mac computers or schedule meetings on-the-go from their mobile devices, deploy Equinox Plug-in for Microsoft Exchange (see *Administrator Guide for Avaya Equinox Management*). The Avaya Equinox Add-in for Microsoft Outlook (64-bit), allows more settings to be configured from Outlook, but requires installation on each client (see *User Guide for Avaya Equinox Add-in for Microsoft Outlook*).

Table 3: Comparing features of the different Microsoft Outlook Plug-ins

Features	Equinox Plug-in for Microsoft Exchange	Avaya Equinox Add-in for Microsoft Outlook
Supported clients	Microsoft Outlook clients on PC Microsoft Outlook clients on Mac Microsoft Outlook Web Application Other calendar applications (such as iOS and Windows-based mobile devices connected to Exchange)	Microsoft Outlook clients on Windows-based PC only (64-bit)

Table continues…

Features	Equinox Plug-in for Microsoft Exchange	Avaya Equinox Add-in for Microsoft Outlook
Installation	Installed on Microsoft Exchange server only (not on each client)	Requires installation on each user's computer
User access	All users with a virtual room (even if connecting from a public network)	Only internal users with a virtual room (cannot connect from a public network)
Advanced Meeting Settings (such as reserving extra resources)	Configured from the Equinox Management user portal	Configured directly from Outlook

(Optional, for OTT deployments) There is an additional plug-in available that does not require a user account in Equinox Management (see *Administrator Guide for Avaya Scopia Desktop Server*). Users cannot reserve video network resources with this plug-in.

Assessing Bandwidth for Large Organizations

About this task

As part of planning your videoconferencing solution, you must assess the bandwidth required for videoconferencing in your organization.

Most large organizations manage their data in one or more data centers around the globe. Typically, with the arrival of videoconferencing you need to increase amount of data incoming and outgoing from the data center. You must assess the bandwidth for every data center in your organization separately as described in the following steps.

For bandwidth considerations for Equinox Streaming and Recording, see *Administrator Guide for Avaya Equinox Streaming and Recording Server*.

Procedure

1. Estimate the number video users allocated to this data center.

   Often, not every employee in an organization is a video user. Look at your organization and decide which departments and employees need video capabilities. This decision often depends on your organization's field of expertise, the kind of services or products it offers. While for some organizations it is important to add video to their technical support service, for instance, other organizations may choose to provide video capabilities for management executives only.

   To illustrate how to assess bandwidth, we use an example of 10,000 video users in this topic.

2. Decide what endpoint types these users will have.

   Note:

   Scopia Desktop is optional in OTT deployments

The videoconferencing experience greatly depends on the endpoint type and has a significant impact on bandwidth.

Different videoconferencing endpoints have different bandwidth requirements, depending on the resolution they support. There are five types of Equinox Solution endpoints:

- Avaya™ Equinox Meet-Me for iOS, Avaya™ Equinox Meet-Me for Android, or Scopia Mobile for access on mobile devices (low bandwidth consumption)
- Avaya™ Equinox Meet-Me for Windows, Avaya™ Equinox Meet-Me for Mac, or Scopia Desktop Client for access on desktop computers (low bandwidth consumption)
- XT Executive for premium HD experience on a dedicated endpoint (low bandwidth consumption)
- XT Series to participate in a videoconference from a meeting room (medium bandwidth consumption)
- XT Telepresence for conducting the most life-like videoconferences (high bandwidth consumption).

3. Estimate to how many users will be assigned each endpoint type.

   For example, the distribution of the 10,000 video users allocated to this data center may be like this:

Table 4: Example of estimation of users per endpoint type

Endpoint type	Number of users
Avaya™ Equinox Meet-Me for iOS, Avaya™ Equinox Meet-Me for Android, or Scopia Mobile	200
Avaya™ Equinox Meet-Me for Windows, Avaya™ Equinox Meet-Me for Mac, or Scopia Desktop Client	10,000
XT Executive	50
XT Series	80
XT Telepresence	10

4. Define the ratio of users in concurrent videoconferences to all users allocated to this data center.

   Define the peak for how many simultaneous recordings and streaming viewers are required in this data center.

   Define the peak ratio for every endpoint type separately.

   Ratios may significantly vary depending on the nature of your organization. For example, in a hi-tech organization where most employees are tech-savvy, the ratio is likely to be higher than average.

   Important:

   Even if the initial implementation of Equinox Solution is done on a smaller scale and the learning curve in your organization is very long, focus on the target. Think what the ratio will be when Equinox Solution is fully deployed and people feel comfortable using it. For example, even if during the first year it is likely that only 1 in 30 Scopia Desktop users will be in a concurrent call, the ratio you use to calculate bandwidth should be 1 in 15, which is your target.

Table 5: Typical peak ratios per endpoint type

Endpoint type	Ratios
Avaya™ Equinox Meet-Me for iOS. Avaya™ Equinox Meet-Me for Android, or Scopia Mobile	Between 1/20 and 1/10
Avaya™ Equinox Meet-Me for Windows, Avaya™ Equinox Meet-Me for Mac, or Scopia Desktop Client	Between 1/20 and 1/10
XT Executive	Between 1/15 and 1/10
XT Series	Between 1/15 and 1/8
XT Telepresence	Between 1/10 and 1/5

5. Calculate peak usage per endpoint type.

   Peak usage is the maximum number of users of the same endpoint type in videoconferences happening at the same time. Calculate this value for each endpoint type separately according to the following formula:

   ```
   Peak usage = number of users / ratio
   ```

   For instance, if you have 10,000 Scopia Desktop users allocated to this data center and the ratio is average, the peak usage for Scopia Desktop is 10,000/15 = 666.

6. Calculate the peak bandwidth per endpoint type according to the formula:

   ```
   Peak bandwidth = peak usage x max bandwidth for this endpoint type
   ```

   Table 6: Bandwidth consumed by different endpoint types on page 60 shows possible values of maximum bandwidth for this endpoint type.

Table 6: Bandwidth consumed by different endpoint types

Endpoint type	Resolution	Maximum bandwidth consumption
Avaya™ Equinox Meet-Me for iOS, Avaya™ Equinox Meet-Me for Android, or Scopia Mobile	720p	768 Kbps
Avaya™ Equinox Meet-Me for Windows, Avaya™ Equinox Meet-Me for Mac, or Scopia Desktop Client	720p	768 Kbps
XT Executive	720p at 30fps	768 Kbps
XT Series	1080p at 60fps	2560 Kbps
XT Telepresence	1080p at 60fps	7680 Kbps

In our example, the peak bandwidth (under condition that the ratio is average) is going to be as follows:

Table 7: Example of peak bandwidth calculation per endpoint types

Endpoint type	Peak Usage	Maximum bandwidth consumption	Peak bandwidth
Avaya™ Equinox Meet-Me for iOS, Avaya™ Equinox Meet-Me for Android, or Scopia Mobile	13	512 Kbps	6,656 Kbps
Avaya™ Equinox Meet-Me for Windows , Avaya™ Equinox Meet-Me for Mac, or Scopia Desktop Client	666	768 Kbps	523,476 Kbps
XT Executive	4	768 Kbps	3,072 Kbps
Avaya Scopia® XT Series	8	2,560 Kbps	20,480 Kbps
XT Telepresence	1	7,680 Kbps	7,680 Kbps

Calculate the number of live streams you want to support, what type of streaming (for example 1080P 2M), and figure how many streaming Media Nodes need to be deployed in this data center.

7. Calculate the total bandwidth for this data center by adding all values of peak bandwidth per endpoint type. This value is your rough bandwidth estimation.

   In our example your total bandwidth value is 561,364 Mbps.

8. Fine-tune your estimation by deciding on the following bandwidth effective policies supported in Equinox Solution:

   - Compressing video by using 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. See Table 8: Optimized bandwidth consumption on page 61.

     Table 8: Optimized bandwidth consumption

Endpoint type	Resolution	Maximum bandwidth	Maximum bandwidth with High Profile
Avaya™ Equinox Meet-Me for iOS, Avaya™ Equinox Meet-Me for Android, or Scopia Mobile	480p	512 Kbps	384 Kbps
Avaya™ Equinox Meet-Me for Windows, Avaya™ Equinox Meet-Me for Mac, or Scopia Desktop Client	720p	768 Kbps	512 Kbps
XT Executive	720p at 30fps	768 Kbps	512 Kbps

Table continues…

Endpoint type	Resolution	Maximum bandwidth	Maximum bandwidth with High Profile
XT Series	1080p at 60fps	2,560 Kbps	2 Mbps
XT Telepresence	1080p at 60fps	7,680 Kbps	6 Mbps

Tip:

Some Avaya endpoints do not support H.264 High Profile, for example some older XT Series models, Avaya Equinox VC240 or legacy third-party endpoints.

- Diverting videoconferences from an MCU that reached its capacity limit during peak hours to an idle MCU in a data center in a different time zone.
- Guaranteeing bandwidth for VIP endpoints at the expense of other endpoints.

  This method suits hierarchical organizations where fluctuations in quality of the video for high-ranking managers are not acceptable.

  In this case you can assign the VIP status to XT Series and XT Executive endpoints used by management and configure Equinox Management not to downgrade their video quality even at times when there is not enough bandwidth. This is achieved by downgrading experience of regular users and using the saved bandwidth to provide premium experience to the VIP endpoints, as shown in Figure 26: Example of a hierarchical organization on page 62.

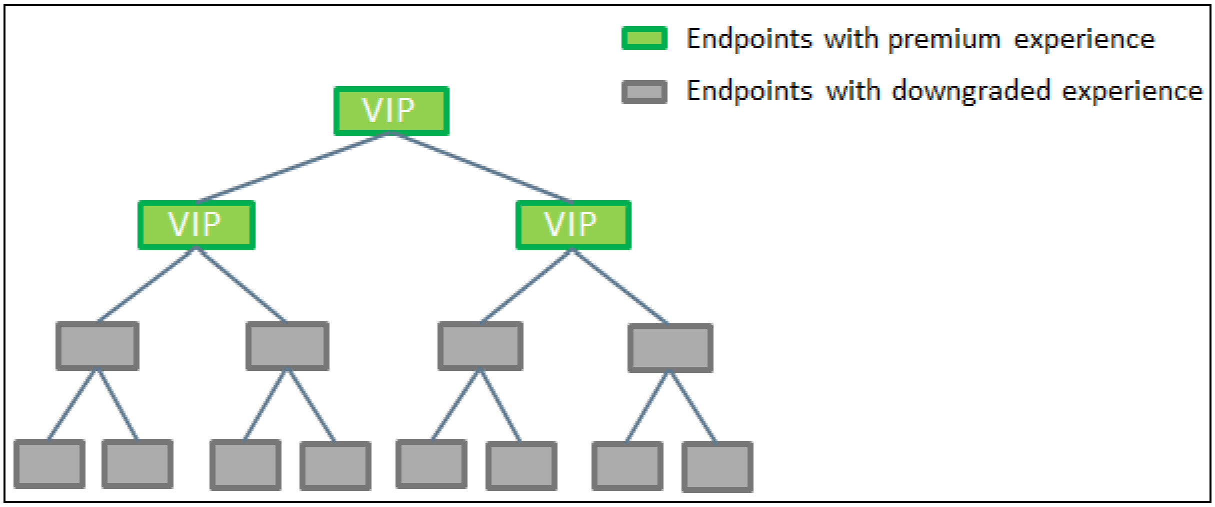

Endpoints with premium experience
Endpoints with downgraded experience
VIP
VIP
VIP

Figure 26: Example of a hierarchical organization

- Setting bandwidth limits for Scopia Desktop users.

  You can define different maximum bandwidth for Scopia Desktop authenticated users and guests using Equinox Management. The maximum bandwidth configured in Equinox Management cannot exceed the maximum bandwidth configured on a Scopia Desktop to which the users connect. For more information see *Administrator Guide for Equinox Management*.

- Setting bandwidth limits for Equinox Streaming and Recording

  In the Media Node configuration of Equinox Streaming and Recording, you can control the amount of bandwidth used for caching Media Node recordings from one zone to another to not fill up the WAN pipe.

- Rejecting calls upon reaching the maximum bandwidth.

  You can use your Equinox Management to setting the bandwidth limits for calls across locations, or the bandwidth dedicated to calls within a location and defining the system behavior. For more information see *Administrator Guide for Equinox Management*.

9. Finally, you need to add margins to make sure that even in poor network conditions video quality does not drop below the standard you decided on.

   Consider your organization's culture and practices: how tolerant will videoconference participants be to noticeable fluctuations in video quality? If participants, especially VIP endpoint owners, do not expect degraded video quality, make sure that the margin you add is enough to guarantee sufficient bandwidth at any time.

   Important:

   An average margin is 20% of your fine-tuned estimation.

Setting WAN Bandwidth Limits

Avaya Equinox Management includes a bandwidth management functionality which enables administrators to set limits on WAN bandwidth usage, and trigger system alerts when that usage rises above a defined threshold. You can also define the system behavior when the bandwidth limit has been reached.

This powerful feature enables administrators to monitor and manage WAN bandwidth usage and keep it under a defined limit at all times.

Using Network Traffic Priorities Across your Deployment

Quality of Service (QoS) determines the priorities of different types of network traffic (audio, video and control/signaling), so in poor network conditions, prioritized traffic is still fully transmitted.

QoS priorities are expressed as a number for each traffic type. The higher the number, the higher its priority.

If you are adding videoconferencing to your current deployment, it is important to ensure that all Equinox Solution components have QoS settings that match the QoS priorities of the organization:

- If QoS is not used by your organization, disable the QoS feature on the Equinox Solution components.

- If QoS is used by your organization, find out the QoS values of the network entities used inside the private network in your organization and modify the QoS values on the Equinox Solution components to match them.

  There are three types of traffic in Scopia Solution as described in Table 9: Types of traffic and their priorities in Equinox Solution on page 64.

Table 9: Types of traffic and their priorities in Equinox Solution

Traffic type	Description	Priority	Default value
Audio	Real-time voice	First	46
Video	Real-time video and presentations	Second	34
Control/ signaling	Data related to the call connection and media management	Third	26

Important:

Do not change the priorities of the traffic types when you modify the QoS values. For example, if you change the value for audio, make sure it is still the highest number for all three traffic types.

If you are planning a new deployment, we recommend that you use the default QoS settings of the Equinox Solution to ensure consistent optimum throughput of traffic across all solution components. Configure the routers and switches to match these settings.

You must introduce QoS together with the lip-sync feature. Lip-sync is a method of marking matching packets of audio and video traffic so that they are reproduced together upon arrival. You must use QoS only in deployments where videoconferencing devices (including all endpoints) support lip-sync, because otherwise audio and video packets arrive even with a bigger time lapse than when QoS is not used. All Avaya videoconferencing endpoints support lip-sync.

Updating the 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.

Adding video to a typical, phone-only deployment requires changing the dial plan of your organization.

To plan the update to your current dial plan, you begin with analyzing the existing deployment. There are two types of dial plans as described in Table 10: Types of dial plans on page 65:

Table 10: Types of dial plans

Type	Description	Example
International	The dial plan duplicates exactly the same dialing prefixes as traditional telephone networks, where the prefixes denote geographic locations. Locations are classified: internal extensions, local numbers, long distance and international numbers. Each location class has a prefix class to match. Result: if users are in different locations, they must dial all prefixes to reach a destination, but if they are in the same location, they can omit the shared prefixes.	+1-212-282-9248 for a destination in USA, where "**+**" is for an international call, "**1**" is for the US, "**212**" is for the state of New York, "**282**" is for the area in the state, and "**9248**" is the actual number within the area.
Proprietary	The dial plan uses proprietary prefixes created for destinations inside your organization that replace traditional external prefixes which can be very long. Result: A user dials a short combination of a prefix and an extension.	49248, for a destination in USA, where "**4**" denotes the country, the state and the area and "**9248**" is the actual number within the area.

When you add videoconferencing to your existing deployment, every video user has at least two devices: a regular audio phone, which has a defined number, and one or several new videoconferencing endpoints. Your task is, essentially, deciding what number to assign to the videoconferencing endpoints.

You can define the dial plan for the video device in one of the following ways:

- Using ID dialing (forking).

  The user has only one number (ID) for all devices assigned; it may be a phone, a XT Executive, an Avaya Equinox™ Meet-Me client (desktop or mobile), a Scopia Desktop Client and a Scopia Mobile device (Scopia Desktop is optional for OTT deployments). When this number is dialed, all devices ring. The user takes the call on the device most suitable at this moment. The type of the call and its quality depend on the device used to answer the call. The moment the user takes the call, the other devices stop ringing. For example, you dial 6789 to reach a user, and both his phone and XT Executive start ringing. If the user accepts the call on his phone, he joins the videoconference with audio only. If the user accepts the call on his XT Executive, he joins the videoconference with audio and video in HD at up to 1080p at 60 frames per second.

  This is the simplest dial plan from the end-user perspective, as people only need to remember one number, and they always reach users wherever they may be. However, this method may require more time to implement.

  Important:

  This option may require upgrading your dial plan system if your current system does not support ID dialing.

- Assigning a prefix for the video device.

  The user keeps the old number for the phone and is assigned a prefix for the videoconferencing endpoint. You may add one prefix for all videoconferencing endpoints or separate prefixes for different types of videoconferencing endpoints assigned to this user. For example, to call a user on his phone, you need to dial 6789; to reach him on his XT Executive, you must dial 11-6789, because 11 is the prefix for his videoconferencing endpoint.
- Assigning a separate number for the video device.

  The user has two different numbers: one for the phone and one for the videoconferencing endpoint. For example, to call a user on his phone, you need to dial 6789; to reach him on his XT Executive, you must dial 1234.

Table 11: Adding video to an existing telephone dial plan

	Phone number	ID dialing	Prefix for video endpoint	Separate number for video endpoint
Proprietary dial plan	6789	6789	11-6789	1234
International dial plan	1-212-282-6789	1-212-282-6789	11-1-212-282-6789	1-212-282-1234
User experience		Users need to remember only one number for all devices.	Users must remember the main number and one or more prefixes.	Users need to remember a number for every assigned device.

Chapter 4: Before you begin

Before You Begin checklist

The following checklist provides the high level steps and considerations prior to beginning your 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 *Migrating from Avaya Aura® Conferencing 8.x to Avaya Equinox Solution*, which is available from http://support.avaya.com.

If you are upgrading from Avaya Scopia® Solution 8.3.6, see *Upgrading from Avaya Scopia® Solution 8.3.6 to Avaya Equinox Solution* , which is 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 388 section of this guide.	
2	Install the Avaya Common Server. Or prepare your server for the installation of Avaya Equinox™ components.		See Downloading documentation on page 70 for installing Avaya Common Server.	
3	Obtain the latest Avaya Equinox Solution software installation and patches.	Download from Avaya PLDS.		
4	Determine the required number of IP addresses for your deployment configuration,		For all deployments, you must use FQDNs. FQDNs are essential when using TLS.	

Table continues…

No.	Task	Description	Notes	✓
	hostnames, and FQDNs. Register the required FQDNs with the appropriate DNS servers. FQDNs are required for single sign-on (SSO) to enable you to administer components. To use SSO, the components must belong to the same root domain.			
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	
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.	

Table continues…

No.	Task	Description	Notes	✓
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	

Chapter 5: Installing VMware-ready Common Servers

Downloading documentation

About this task

The Avaya Common Server is offered only as an Appliance Virtualization Platform (AVP), and is delivered with a pre-installed and licensed VMware ESXi 5.5 or 6.0 hypervisor. This license is hardened and you cannot modify it. The Avaya Common Server must be installed on the HP ProLiant server or on a Dell server.

Use this procedure to find and download documents on HP or 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 `Common Servers` in the **Enter Your Product Here** field, and select the server version from the **Choose Release** dropdown.
3. Download the documents that you need.

Deploying the Solution Deployment Manager client

About this task

To manage the system and deploy OVAs, you need to install the Solution Deployment Manager (SDM) client on a PC. The SDM application requires a PC running 64–bit Windows 7 OS.

Before you begin

Download the SDM user guide from https://downloads.avaya.com/css/P8/documents/101023857. The guide also explains how to access the AVP host for a fresh installation. The AVP host is shipped with default IP and login.

Procedure

1. Download the SDM client application from the Avaya PLDS.

   The SDM version must match the AVP version (for example, 7.0.1 for both).

2. Install the SDM application.
3. In the **SDM Client Dashboard**, select the **VM Management** page.
4. In the **Location Management page**, create a location for your hosts' cluster by selecting **Location > New**.
    a. Add a name for the location.
    b. Leave the optional fields empty.
5. In the **Host Management** page, enter the AVP host name, FQDN or IP, user name, and password.
6. Open the SDM client, and select the host for the OVA you want to install. This opens a page showing the host details. Select **Next**.
7. Add the OVA file you need to deploy: full pathname (for example, c:\download \MediaServer_Build_14.8 ova) and select **Submit**.
8. Enter the virtual machine name and configure the network properties: default gateway, public IP address, public netmask. Select **Deploy**.
9. In the EULA acceptance page, select **Accept**.

Chapter 6: Installing customer-provided servers

Prerequisites for OVA installation

If you use your own servers, make sure to follow these recommendations:

- ESXi must be VMware version 5.5 or 6.0.
- For optimized performance, load the ESXi package from the hardware vendor site if available (DELL and HP have them), instead of the VMware site.
- For the media virtual machines, you need to enable hyper-threading on the host.
- We do not recommend using vMotion (DRS or manual), as it may break active sessions.
- Deploy OVAs via the VMware vSphere Client connected to vCenter or to a standalone host.

Chapter 7: Before you begin software installation

Prerequisites for software installation

Verify the following:

- The deployment layout type has been chosen based on the capacity and scaling requirements.
- The required number of IP addresses obtained.
- Obtain the latest installation disks for Linux and software installation:
- 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 Windows based PC with Internet Explorer 8.0 or 9.0, or Firefox 4.0 or later.
    - 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 (PSN), and Product Correction Notices (PCN) 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 67.		
2	Review the prerequisites	See Prerequisites for software installation on page 73.		
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	

Table continues…

No.	Task	Description	Notes	✓
			Ensure that you have the latest of both types of patch.	
4	Deploy the Equinox Management OVA and activate the Equinox Management server.	Installed modules include: Management, SIP B2BUA, H.323 Gatekeeper, Equinox Conference Control, User Portal + Web Gateway. The Avaya Aura® User Portal functionalities and Avaya Aura® Web Gateway functionalities are available as an integrated part of the Equinox Management application. See the chapter explaining the installation and first configuration tasks.	For deployments with more than 2,000 concurent calls, install the Avaya Equinox Web Gateway and H.323 Gatekeeper 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.		
6	Deploy other components if required (Scopia Desktop, Equinox Streaming and Recording Server,Avaya Equinox Recording Gateway, Avaya Session Border Controller for Enterprise (ASBCE), Equinox H.323 Edge server, etc.), 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,	• Deploying the ASBCE is mandatory when the Avaya Equinox™ Meet-Me Client is part of the solution. • Scopia Desktop is deployed in the OTT solution, only if the customer requires a third party session border controller or needs to use Scopia Desktop clients for their Scopia Content Slider (which will be added to Avaya Equinox™ Meet-Me Client in a future release). • Deploy Equinox H.323 Edge only in legacy Avaya Scopia solution deployments. The H. 323 protocol is used	

Table continues…

No.	Task	Description	Notes	✓
		enabling secure connectivity between enterprise networks and remote sites.	only in legacy Avaya Scopia deployments.	
7	Create and sign CSR and apply Equinox Management certificates.			
8	Create and sign CSR for each component (Scopia Desktop, Equinox Streaming and Recording Server, Avaya Equinox Recording Gateway, ASBCE, Equinox H.323 Edge server, etc.).			
9	Restart Equinox Management server.			
10	Restart Equinox Media Server.			
11	Sync Meeting types from Equinox Media Server to Equinox Management. **Note:** 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 Equinox™ Meet-Me and Avaya Equinox™ Meetings for Web (WebRTC). See the product's user guide.		
15	Configure the clients and endpoints in the	See the product's administrator guide.		

Table continues…

No.	Task	Description	Notes	✓
	management entities of the OTT solution.			
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 67.		
2	Review the prerequisites	See Prerequisites for software installation on page 73.		
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 the Avaya Aura® OVAs.	Only for TE deployments.		

Table continues…

No.	Task	Description	Notes	✓
5	Deploy the Equinox Management OVA and activate the Equinox Management server.	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 the Equinox Management application. 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 concurent calls, install the Avaya Equinox Web Gateway and H.323 Gatekeeper as separate OVAs and nodes. For TE deployments with more than 2,000 concurent calls, install the Avaya Aura® Web Gateway and H.323 Gatekeeper 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.		
7	Deploy other components if required (Scopia Desktop, Equinox Streaming and Recording Server, Avaya Equinox Recording Gateway, Avaya Session Border Controller for Enterprise (ASBCE), Equinox H.323 Edge server, etc.), 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.	• Deploying the ASBCE is mandatory when the Avaya Equinox™ Meet-Me Client is part of the solution. • Scopia Desktop is deployed in the OTT solution, only if the customer requires a third party session border controller or needs to use Scopia Desktop clients for their Scopia Content	

Table continues…

No.	Task	Description	Notes	✓
		- 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.	Slider (which will be added to Avaya Equinox™ Meet-Me Client in a future release). - Deploy Equinox H.323 Edge only in legacy Avaya Scopia solution deployments. The H.323 protocol is used only in legacy Avaya Scopia deployments.	
8	Create and sign CSR and apply Equinox Management certificates.			
9	Create and sign CSR for each component (Scopia Desktop, Equinox Streaming and Recording Server, Avaya Equinox Recording Gateway, ASBCE, Equinox H.323 Edge server, etc.).			
10	Restart Equinox Management Server.			
11	Restart Equinox Media Server.			
12	Sync Meeting types from Equinox Media Server to Equinox Management. **Note:** Do not upload Equinox Media Server meeting types to Scopia® Elite 6000 MCUif 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 Equinox™ Meet-Me and Avaya Equinox™ Meetings for Web (WebRTC). In the TE solution, clients might include: Avaya Equinox™, Avaya H175 Video Collaboration Station, SDK customized clients, Avaya Vantage™. See the product's administrator guide.		
16	Configure the 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 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 67.		
2	Review the prerequisites	See Prerequisites for software installation on page 73.		
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..		
5	Deploy the Equinox Management OVA and activate the Equinox Management server.	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 the Equinox Management application. 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 concurent calls, install the Avaya Equinox Web Gateway and H.323 Gatekeeper as separate OVAs and nodes. For TE deployments with more than 2,000 concurent calls, install the Avaya Aura® Web Gateway and H.323 Gatekeeper as separate OVAs and nodes.	
6	Deploy Equinox Media Server OVAs and activate these servers	Installed modules include: MCU, WCS, AMS. See the chapter explaining the		

Table continues…

No.	Task	Description	Notes	✓
	on Equinox Management.	installation and first configuration tasks.		
7	Deploy other components if required (Scopia Desktop, Equinox Streaming and Recording Server, Avaya Equinox Recording Gateway, Avaya Session Border Controller for Enterprise (ASBCE), Equinox H.323 Edge server, etc.), 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 the ASBCE is mandatory when the Avaya Equinox™ Meet-Me Client is part of the solution. • Scopia Desktop is deployed in the OTT solution, only if the customer requires a third party session border controller or needs to use Scopia Desktop clients for their Scopia Content Slider (which will be added to Avaya Equinox™ Meet-Me Client in a future release). • Deploy Equinox H.323 Edge only in legacy Avaya Scopia solution deployments. The H.323 protocol is used only in legacy Avaya Scopia deployments.	
8	Create and sign CSR and apply Equinox Management certificates.			
9	Create and sign CSR for each component (Scopia Desktop, Equinox Streaming and Recording Server, Avaya Equinox Recording Gateway			

Table continues…

No.	Task	Description	Notes	✓
	(AERG), Session Border Controller, Equinox H.323 Edge server, etc.).			
10	Restart Equinox Management server.			
11	Restart Equinox Media Server.			
12	Sync Meeting types to Equinox Management. **Note:** Do not upload Equinox Media Server meeting types to Scopia® Elite 6000 MCU if 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 Equinox™ Meet-Me and Avaya Equinox™ Meetings for Web (WebRTC). In the TE solution, soft clients might include: Avaya Equinox™, Avaya H175 Video Collaboration Station, SDK customized clients. See the product's user guide.		
16	Configure the 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.		

Table continues…

No.	Task	Description	Notes	✓
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 if required (Scopia Desktop, Equinox Streaming and Recording Server, Avaya Session Border Controller for Enterprise, Equinox H.323 Edge server, etc.), and add to Equinox Management.	See the chapter explaining the installation and first configuration tasks.		

Chapter 8: Equinox Management Deployment for Over the Top (OTT) Solution

Deployment of Equinox Management for OTT solution — Overview

Equinox Management is deployed virtually, without physical hardware, pre-installed common servers, or an .exe file. 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 91.

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 7.0
- VMware ESXi 5.5 and 6.0
- VMware Workstation Pro 11 or later
- VMware vCenter

For details on technical requirements, see Equinox Management Technical Specifications on page 86.

Equinox Management Technical Specifications

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 media 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 or as a User Portal + Web Gateway.

Note:

Using low memory capacity in OVA configuration can cause the User Portal + Web Gateway to fail.

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

Table 12: 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** — 7,500/150,000

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.

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

Table 13: 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.	7,500 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

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 90	
2	Deploy the all-in-one Equinox Management server	Deploying the Equinox Management Server on page 91	
3	Log into the Equinox Management server	Logging Into Equinox Management on page 105	
4	Configure the Equinox Management server for the all-in-one working mode	Configuring the All-In-One Equinox Management Server on page 110 Configuring Gatekeepers in Avaya Equinox Management on page 114 Configuring Deployment of User Portal + Web Gateway on page 117	
5	Secure connections	Securing Connections with Equinox Management on page 121	
6	Update your license	Updating a User License on page 138	
7	Deploy and Configure the Equinox Management Environment	Deploying and Configuring the Equinox Management Environment on page 139	

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 management servers to your deployment, as follows:

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

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 90	
2	Deploy the Equinox Management server	Deploying the Equinox Management Server on page 91	

Table continues…

No.	Task	Link/Notes	✔
3	Log into the Equinox Management server	Logging Into Equinox Management on page 105	
4	Configure the Equinox Management server for distributed working mode	Enable SIP B2BUA and/or Equinox Conference Control, per your deployment requirements (see the *Administrator Guide for Avaya Equinox Management*).	
5	Add the H.323 Gatekeeper	Configuring Gatekeepers in Equinox Management on page 114	
6	Add the User Portal + Web Gateway	Configuring Deployment of User Portal + Web Gateway on page 117	
7	Secure connections	Securing Connections with Equinox Management on page 121	
8	Configure User Portal + Web Gateway settings	Configuring User Portal / Web Gateway Settings on page 134	
9	Update your license	Updating a User License on page 138	
10	Deploy and Configure the Equinox Management Environment	Deploying and Configuring the Equinox Management Environment on page 139	

Downloading software from PLDS

When you place an order for an Avaya PLDS-licensed software product, PLDS creates the license entitlements of the order and sends an email notification to you. The email includes a license activation code (LAC) and instructions for accessing and logging into PLDS. Use the LAC to locate and download the purchased license entitlements.

In addition to PLDS, you can download the product software from http://support.avaya.com using the **Downloads and Documents** tab at the top of the page.

Note:

Only the latest service pack for each release is posted on the support site. Previous service packs are available only through PLDS.

Procedure

1. Enter http://plds.avaya.com in your Web browser to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS home page, select **Assets**.
4. Click **View Downloads**.
5. Click on the search icon (magnifying glass) for **Company Name**.

6. In the **%Name** field, enter **Avaya** or the Partner company name.
7. Click **Search Companies**.
8. Locate the correct entry and click the **Select** link.
9. Enter the Download Pub ID.
10. Click **Search Downloads**.
11. Scroll down to the entry for the download file and click the **Download** link.
12. In the **Download Manager** box, click the appropriate download link.

    ✱ **Note:**

    The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.
13. If you use Internet Explorer and get an error message, click the **install ActiveX** message at the top of the page and continue with the download.
14. Select a location where you want to save the file and click **Save**.
15. If you used the Download Manager, click **Details** to view the download progress.

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
- 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.

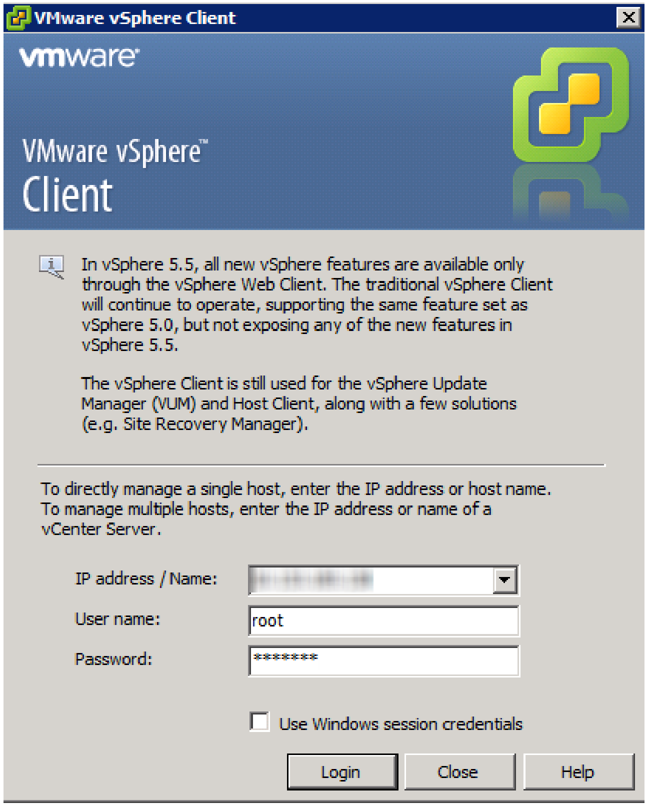
Before you begin

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 7.0
  - VMware ESXi 5.5 or 6.0
  - VMware vCenter
  - VMware Workstation Pro 11 or later
- Hardware: See Table 12: Matching hardware server specifications with your product on page 86

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.



In vSphere 5.5, all new vSphere features are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0, but not exposing any of the new features in vSphere 5.5.

The vSphere Client is still used for the vSphere Update Manager (VUM) and Host Client, along with a few solutions (e.g. Site Recovery Manager).

To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.

IP address / Name: [redacted]

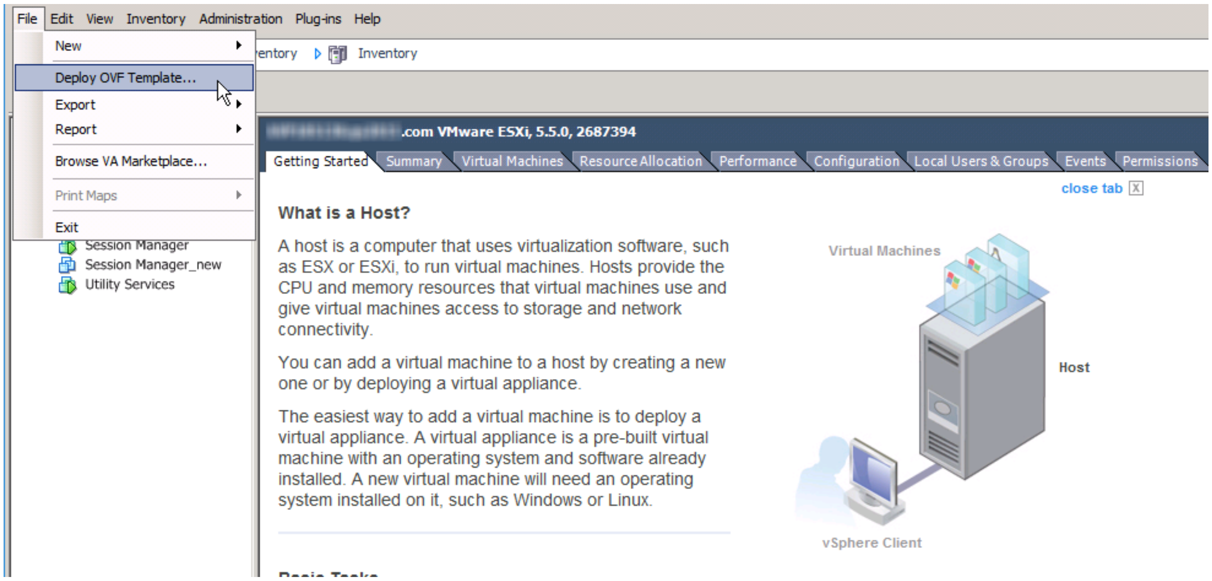
User name: root

Password: ********

□ Use Windows session credentials

Figure 27: vSphere Client

3. Select **Login**. The vSphere client page opens, where you select **File** > **Deploy OVF Template** to upload the .ova file.



[redacted].com VMware ESXi, 5.5.0, 2687394

What is a Host?

A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

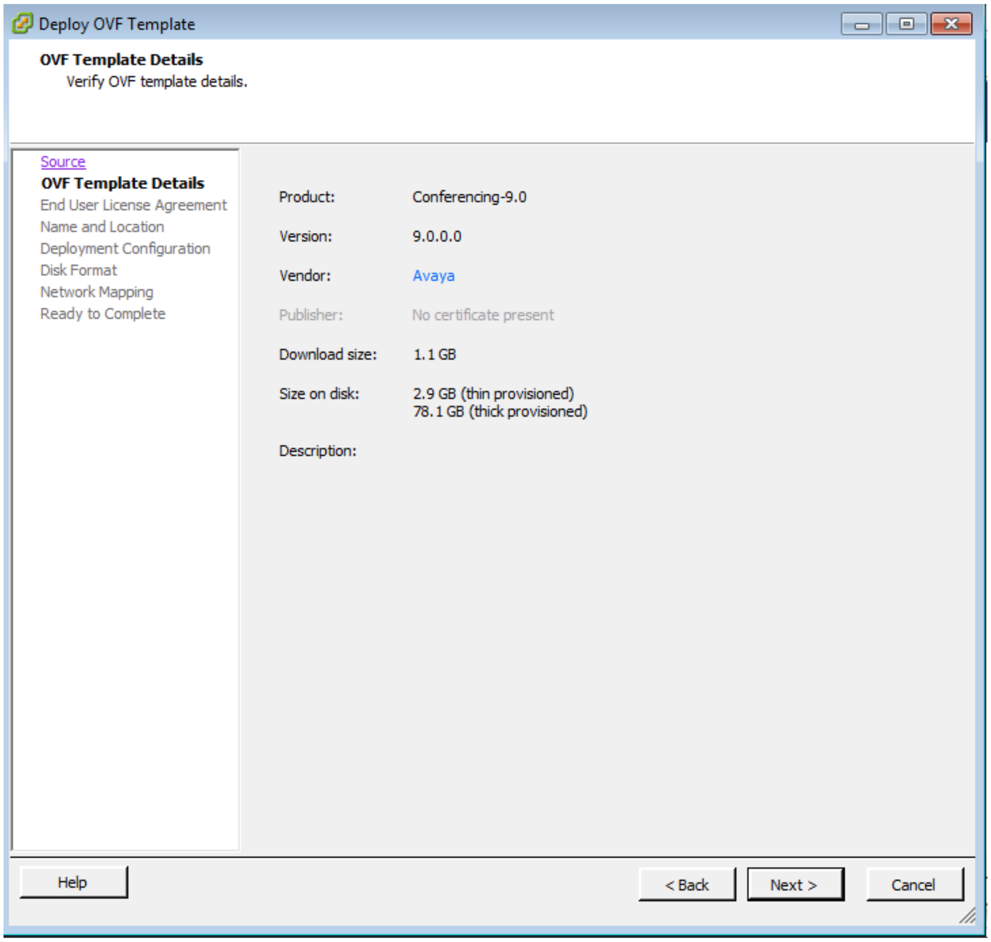
You can add a virtual machine to a host by creating a new one or by deploying a virtual appliance.

The easiest way to add a virtual machine is to deploy a virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux.

Basic Tasks

Figure 28: vSphere Client Page

4. Select the local Equinox Management OVA file, and select **Next** to open the **Deploy OVF Template** wizard. The **OVF Template Details** page opens, displaying the product information.



Product: Conferencing-9.0

Version: 9.0.0.0

Vendor: Avaya

Publisher: No certificate present

Download size: 1.1 GB

Size on disk: 2.9 GB (thin provisioned)
78.1 GB (thick provisioned)

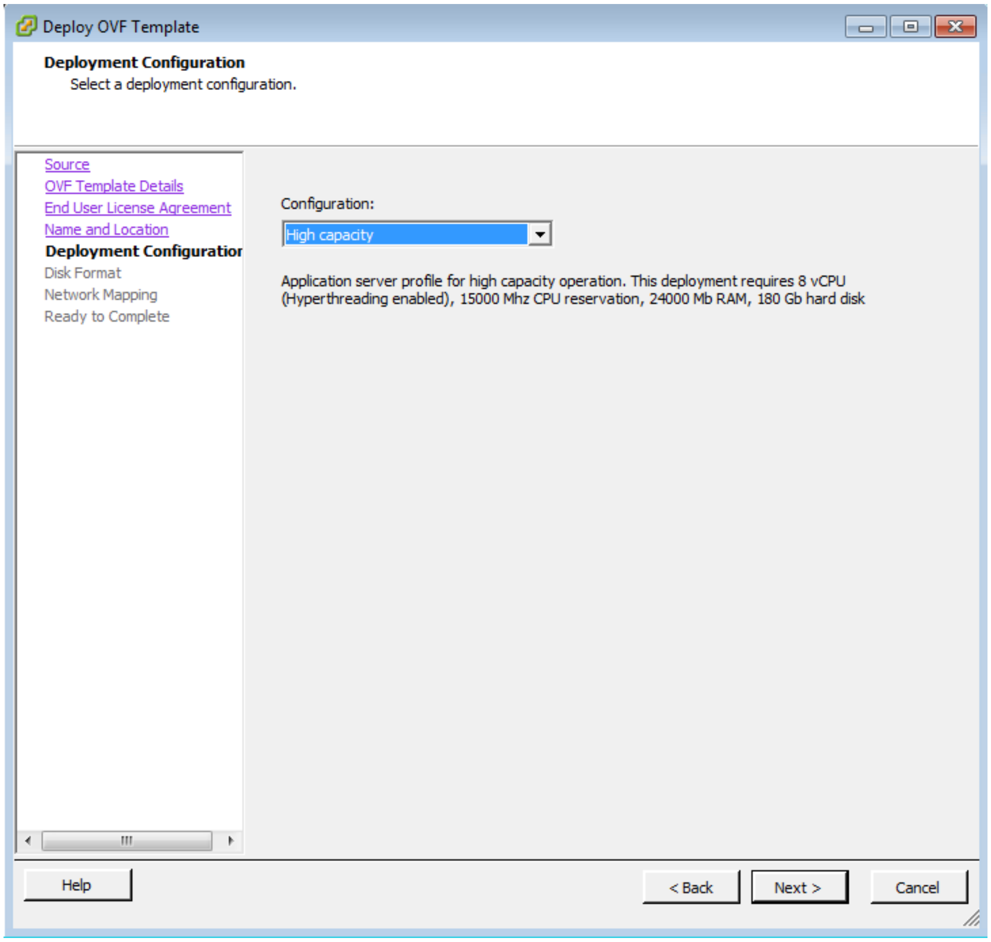
Description:

Figure 29: OVF Template Details Page

5. Select **Next**. The **End User License Agreement** page opens.

6. Select **Accept** to accept the license agreement, and select **Next**. The **Name and Location** page opens.

7. Enter a name for the OVF template in the **Name** field, and select **Next**. The **Deployment Configuration** page opens.



Deployment Configuration

Select a deployment configuration.

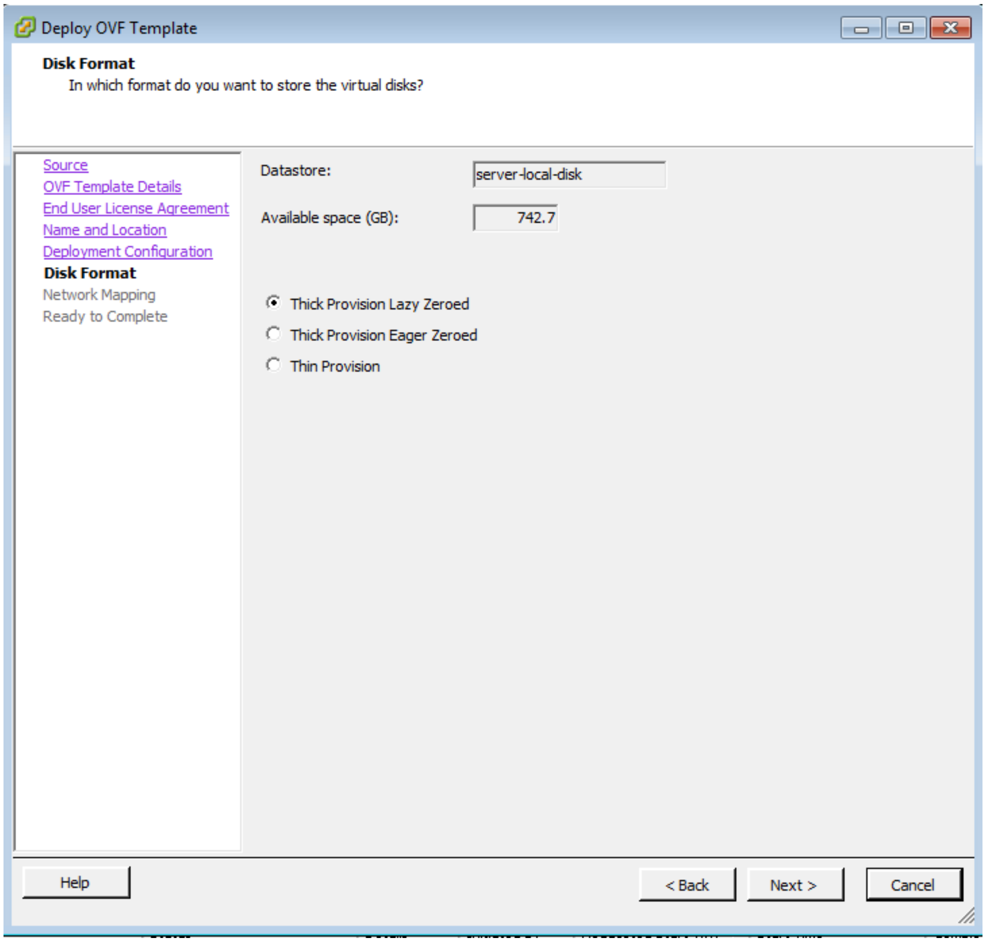
Configuration: High capacity

Application server profile for high capacity operation. This deployment requires 8 vCPU (Hyperthreading enabled), 15000 Mhz CPU reservation, 24000 Mb RAM, 180 Gb hard disk

Figure 30: Deployment Configuration Page

For details on technical requirements per configuration type, see Equinox Management Technical Specifications on page 86.

8. In the **Configuration** field, select the relevant Equinox Management profile, based on your environment, and select **Next**. The **Disk Format** page opens.



Disk Format

In which format do you want to store the virtual disks?

Datastore: server-local-disk

Available space (GB): 742.7

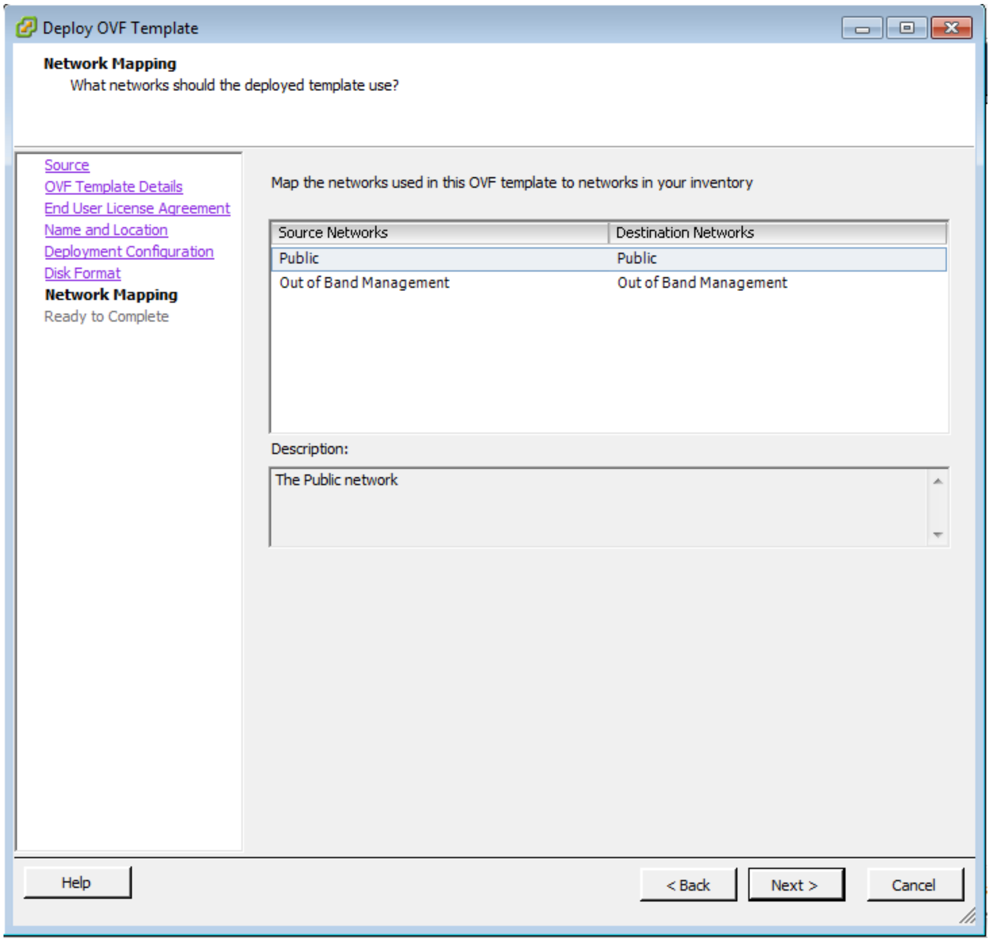
● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

Figure 31: Disk Format Page

9. Select **Thick Provision Lazy Zeroed** and select **Next**. The **Network Mapping** page opens.



Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
Public	Public
Out of Band Management	Out of Band Management

Description:

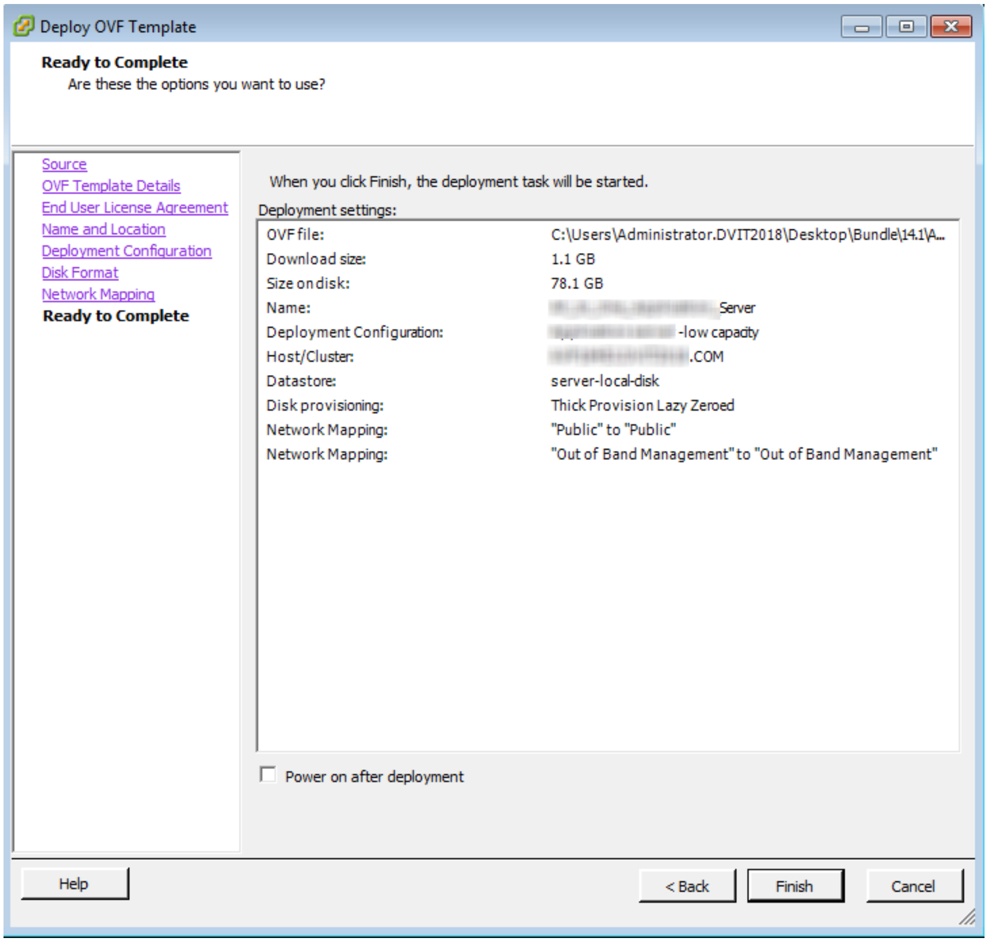
The Public network

Figure 32: Network Mapping Page

Note:

Dual NIC and DHCP are not supported for Equinox Management.

10. Map the networks used in your OVF template to networks in your inventory, and select **Next**.
    The **Ready to Complete** page opens, displaying your deployment settings.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\Users\Administrator.DVIT2018\Desktop\Bundle\14.1\A...
Download size:	1.1 GB
Size on disk:	78.1 GB
Name:	[redacted] Server
Deployment Configuration:	[redacted] -low capacity
Host/Cluster:	[redacted] .COM
Datastore:	server-local-disk
Disk provisioning:	Thick Provision Lazy Zeroed
Network Mapping:	"Public" to "Public"
Network Mapping:	"Out of Band Management" to "Out of Band Management"

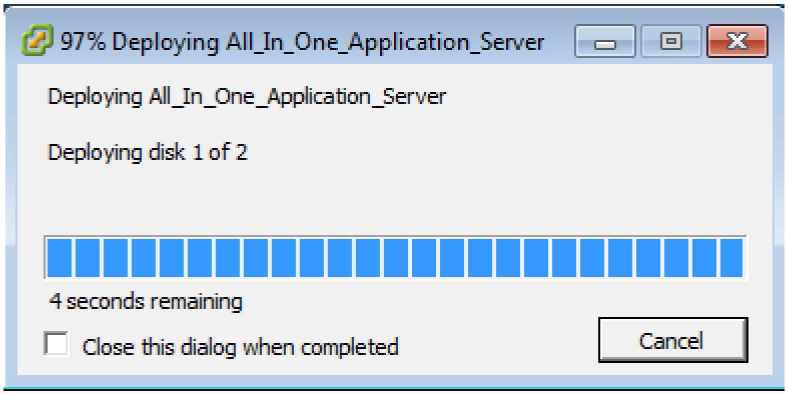
□ Power on after deployment

Figure 33: Ready to Complete Page

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

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

    The system deploys the OVA to the virtual host server.



Deploying All_In_One_Application_Server

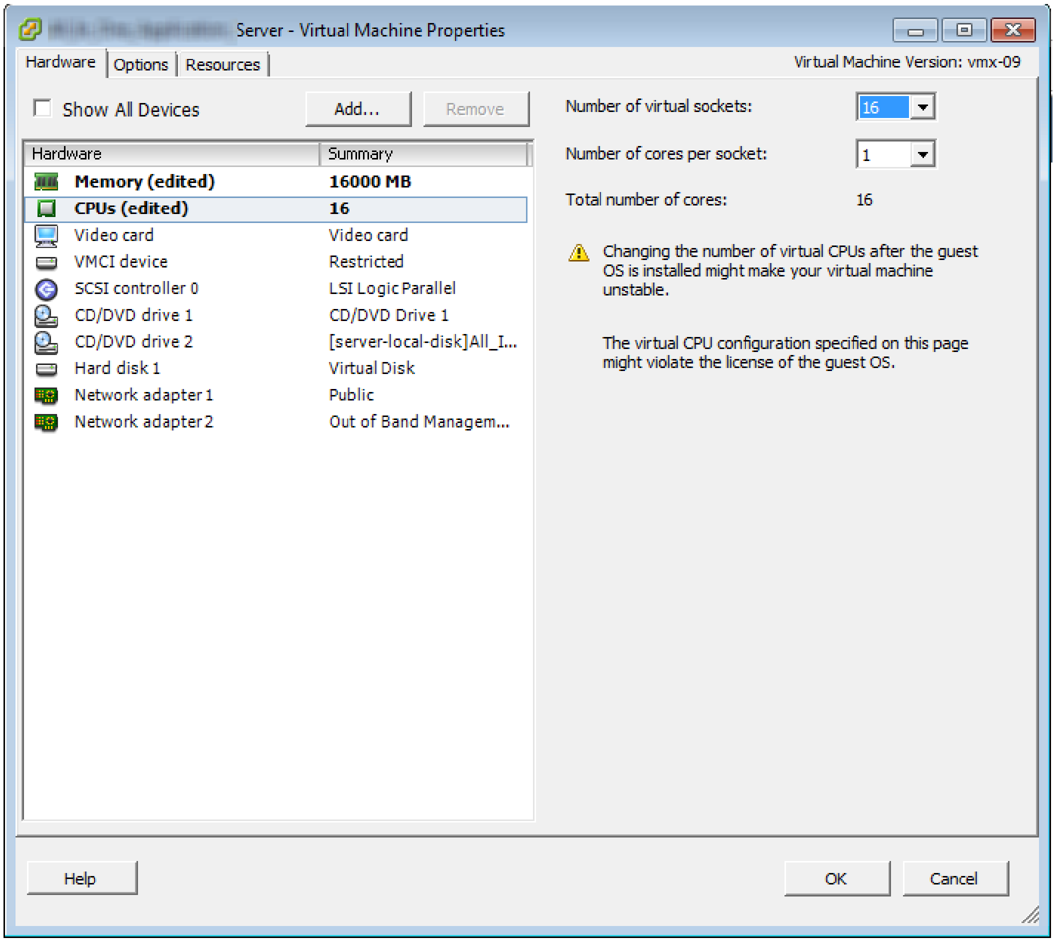
Deploying disk 1 of 2

4 seconds remaining

□ Close this dialog when completed

Figure 34: Deploying the OVA

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



[redacted] Server - Virtual Machine Properties

Virtual Machine Version: vmx-09

☐ Show All Devices

Hardware	Summary
Memory (edited)	**16000 MB**
CPUs (edited)	**16**
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
CD/DVD drive 1	CD/DVD Drive 1
CD/DVD drive 2	[server-local-disk]All_I...
Hard disk 1	Virtual Disk
Network adapter 1	Public
Network adapter 2	Out of Band Managem...

Number of virtual sockets: 16

Number of cores per socket: 1

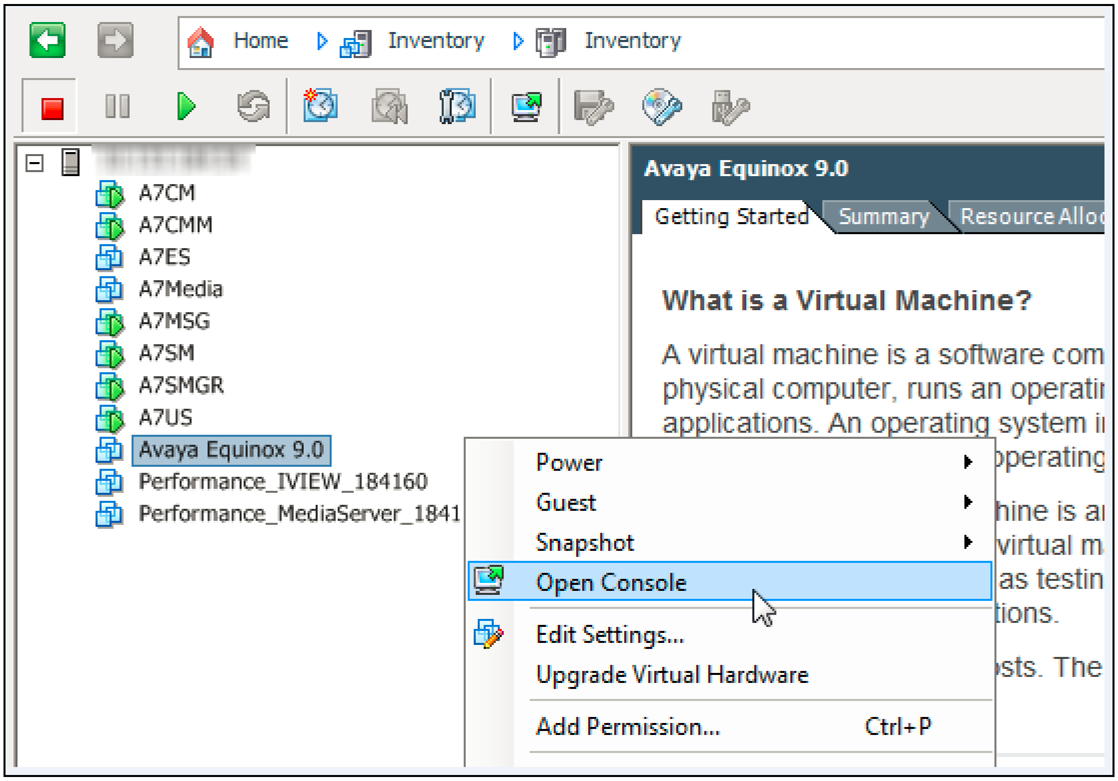
Total number of cores: 16

⚠ Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine unstable.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

Figure 35: Virtual Machine Properties Page

12. Ensure that at least 8 CPU cores and 16 GB of memory are allocated. We recommend allocating 16 CPU cores for enhanced performance.
13. Select **OK** to complete the deployment.
14. In the resulting window, right-click the OVA and select **Open Console**.



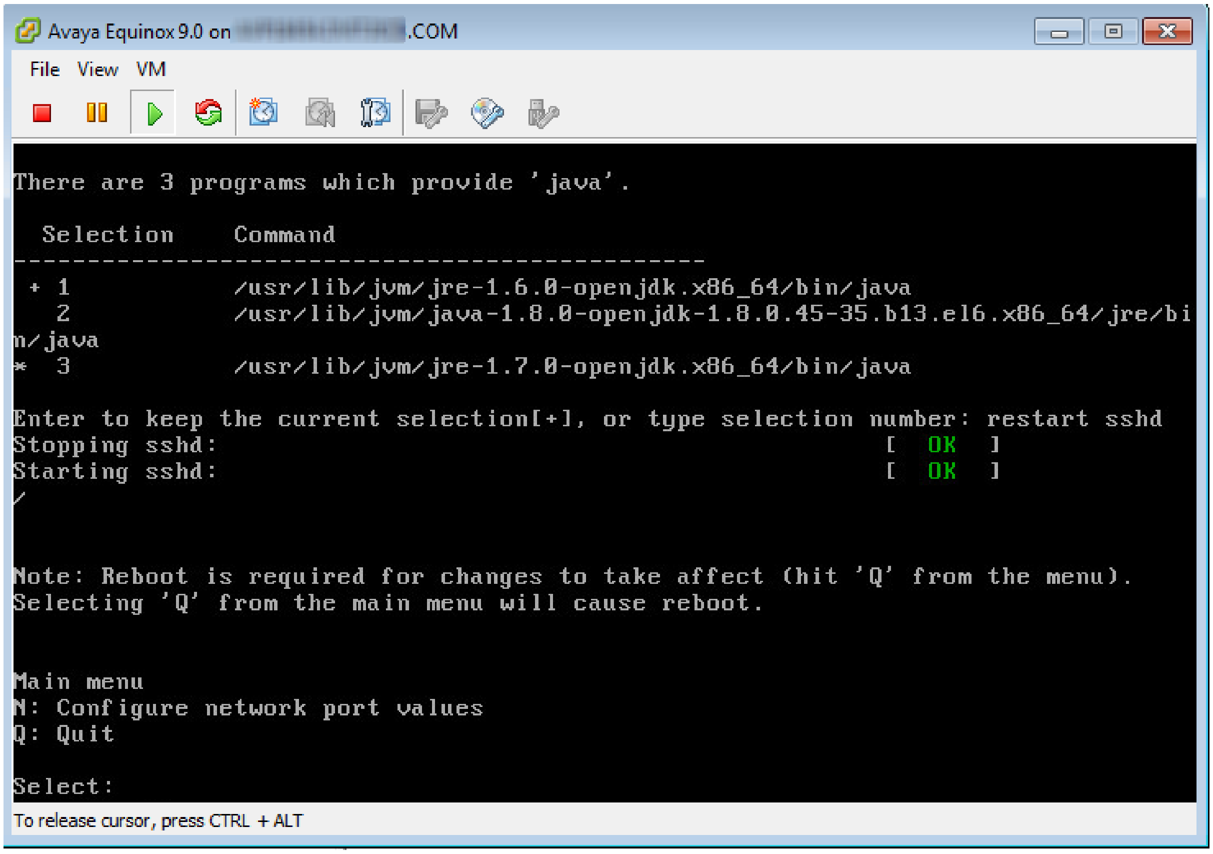
What is a Virtual Machine?

A virtual machine is a software com physical computer, runs an operati applications. An operating system i operating hine is a virtual m as testin tions. sts. The

Figure 36: vSphere Client — Open Console Option

15. Select the green arrow icon ▶ to start the virtual server.

    The Command Prompt window displays in the vSphere Client.

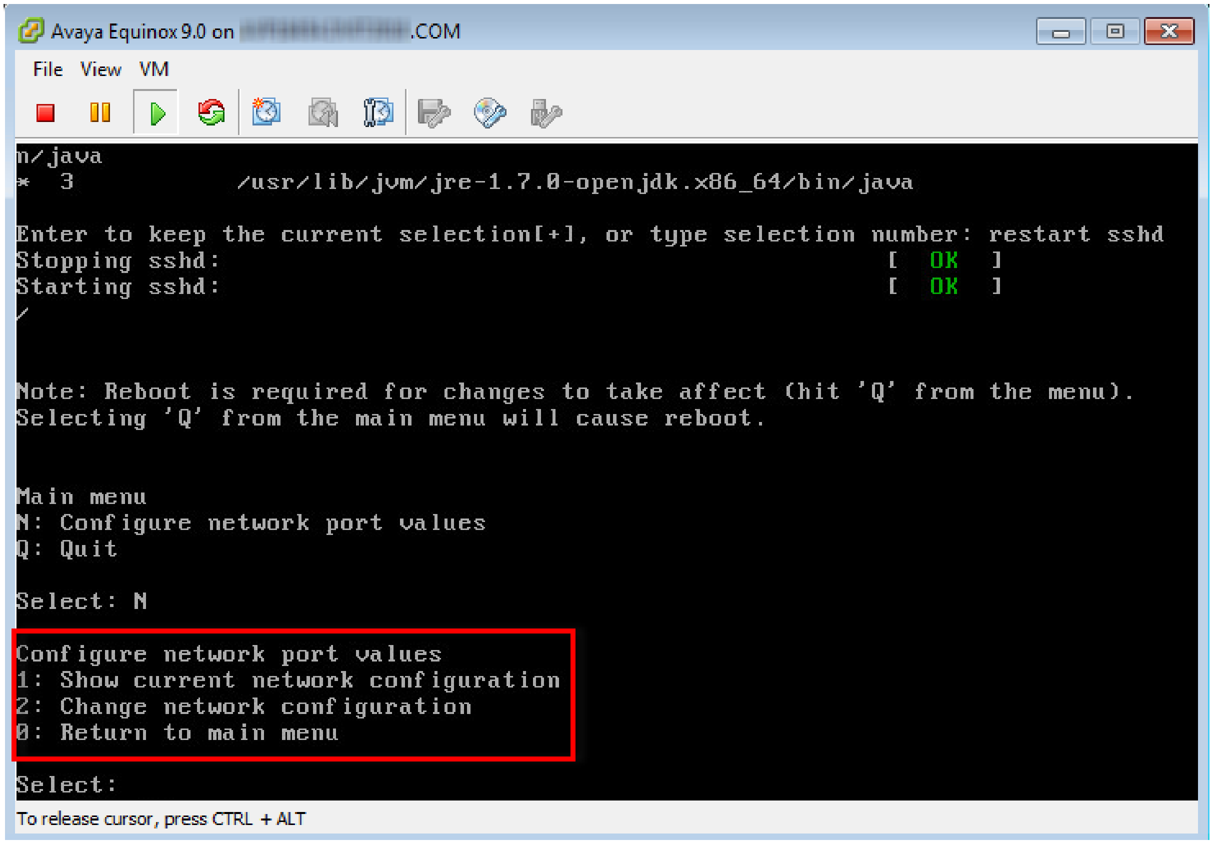

Avaya Equinox 9.0 on [redacted].COM
File
View
VM
To release cursor, press CTRL + ALT

```
There are 3 programs which provide 'java'.

  Selection    Command
-----------------------------------------------
 + 1           /usr/lib/jvm/jre-1.6.0-openjdk.x86_64/bin/java
   2           /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.45-35.b13.el6.x86_64/jre/bi
n/java
*  3           /usr/lib/jvm/jre-1.7.0-openjdk.x86_64/bin/java

Enter to keep the current selection[+], or type selection number: restart sshd
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
/


Note: Reboot is required for changes to take affect (hit 'Q' from the menu).
Selecting 'Q' from the main menu will cause reboot.


Main menu
N: Configure network port values
Q: Quit

Select:
```

Figure 37: Server Command Prompt Window

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

    A new **Select** prompt appears, with the options for configuring network port values.



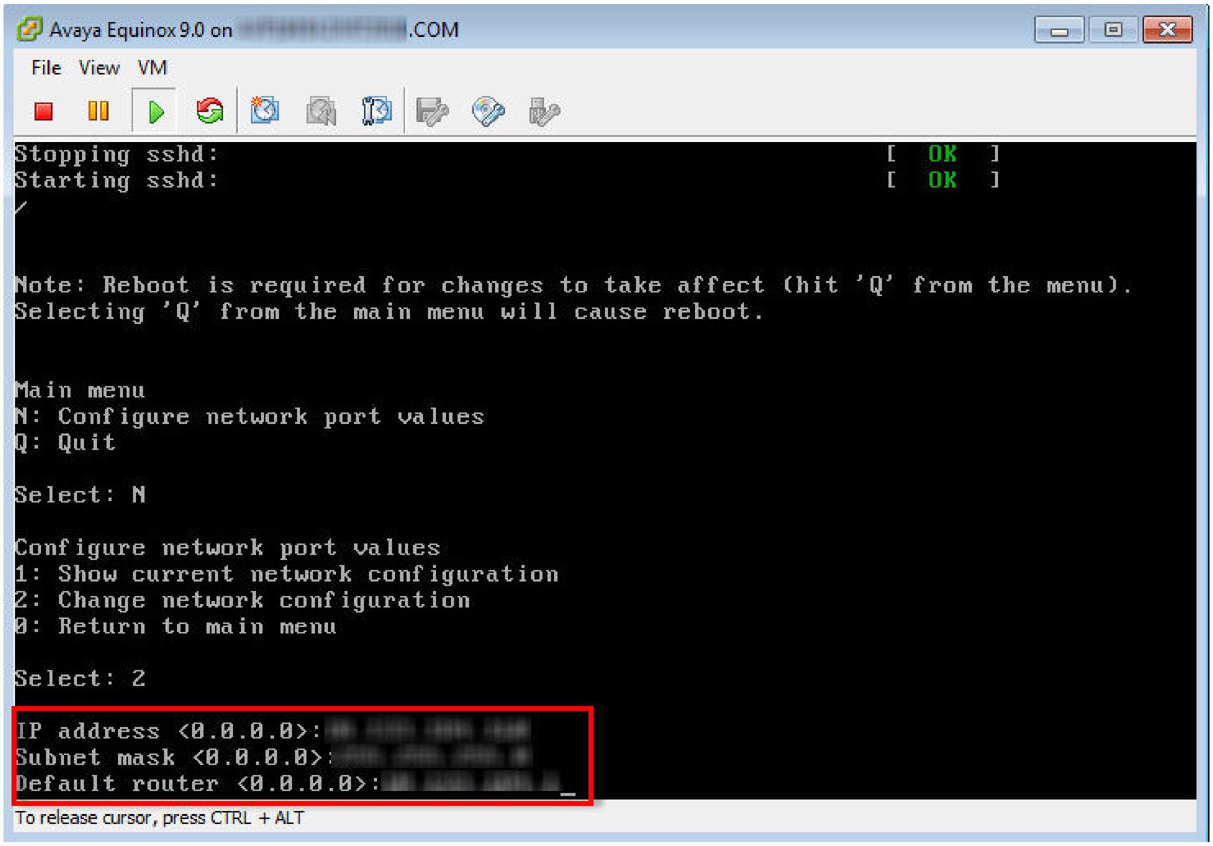
```
n/java
*  3          /usr/lib/jvm/jre-1.7.0-openjdk.x86_64/bin/java

Enter to keep the current selection[+], or type selection number: restart sshd
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
/


Note: Reboot is required for changes to take affect (hit 'Q' from the menu).
Selecting 'Q' from the main menu will cause reboot.


Main menu
N: Configure network port values
Q: Quit

Select: N

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

Select:
```

To release cursor, press CTRL + ALT

Figure 38: Configure Network Port Values Options

17. Enter **2** next to the **Select** prompt to change the network configuration.

18. On the resulting Command Prompt window, enter the IP address, subnet mask, and default router address.

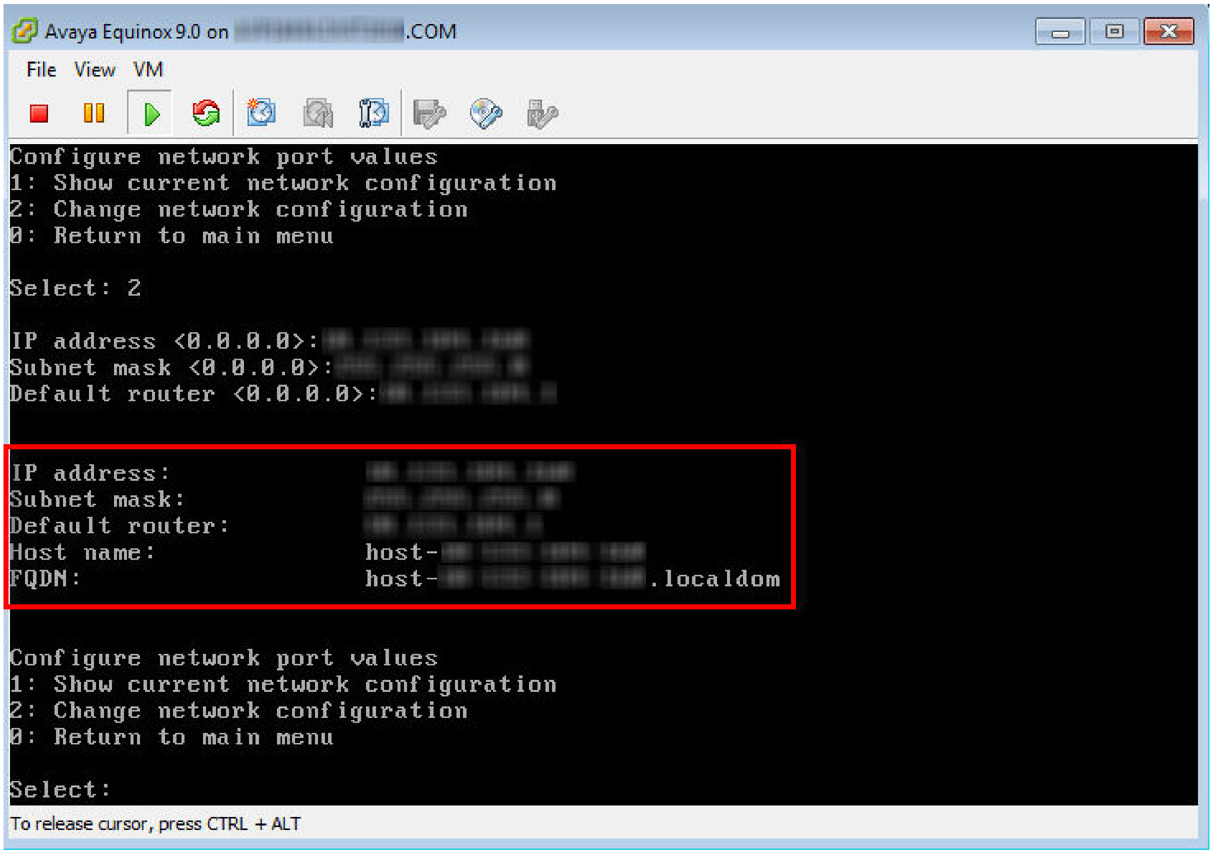


```
Stopping sshd:                                            [  OK  ]
Starting sshd:                                            [  OK  ]
/


Note: Reboot is required for changes to take affect (hit 'Q' from the menu).
Selecting 'Q' from the main menu will cause reboot.


Main menu
N: Configure network port values
Q: Quit

Select: N

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

Select: 2

IP address <0.0.0.0>:[redacted]
Subnet mask <0.0.0.0>:[redacted]
Default router <0.0.0.0>:[redacted]_
```

To release cursor, press CTRL + ALT

Figure 39: Changing Network Configuration

Press **Enter**. The parameters are saved and the Command Prompt window refreshes.

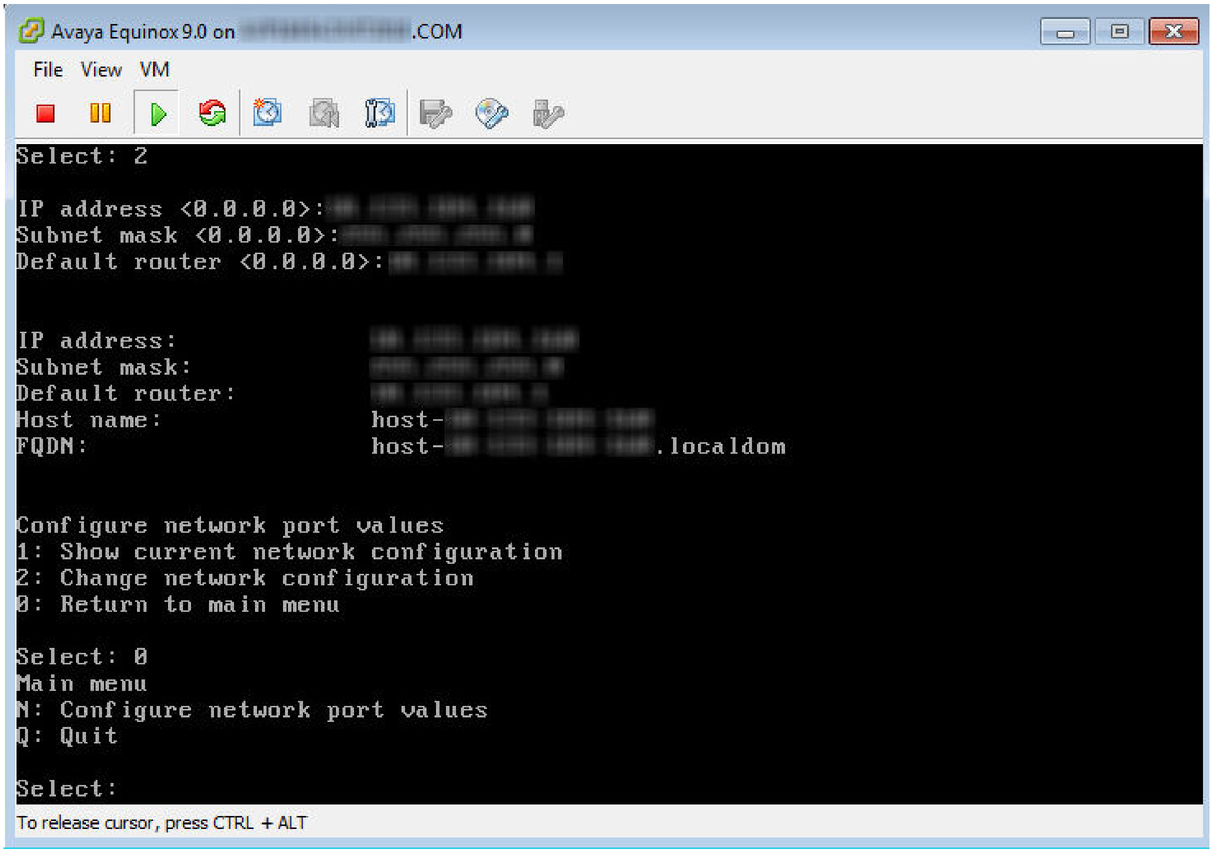


```
Configure network port values
1: Show current network configuration
2: Change network configuration
0: Return to main menu

Select: 2

IP address <0.0.0.0>:[redacted]
Subnet mask <0.0.0.0>:[redacted]
Default router <0.0.0.0>:[redacted]

IP address:              [redacted]
Subnet mask:             [redacted]
Default router:          [redacted]
Host name:               host-[redacted]
FQDN:                    host-[redacted].localdom

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

Select:
```

To release cursor, press CTRL + ALT

Figure 40: Network Configuration Values

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


Avaya Equinox 9.0 on [redacted].COM
File
View
VM
To release cursor, press CTRL + ALT

```
Select: 2

IP address <0.0.0.0>:[redacted]
Subnet mask <0.0.0.0>:[redacted]
Default router <0.0.0.0>:[redacted]


IP address:               [redacted]
Subnet mask:              [redacted]
Default router:           [redacted]
Host name:                host-[redacted]
FQDN:                     host-[redacted].localdom


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

Select: 0
Main menu
N: Configure network port values
Q: Quit

Select:
```

Figure 41: Main Menu

20. 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 105.

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 91).

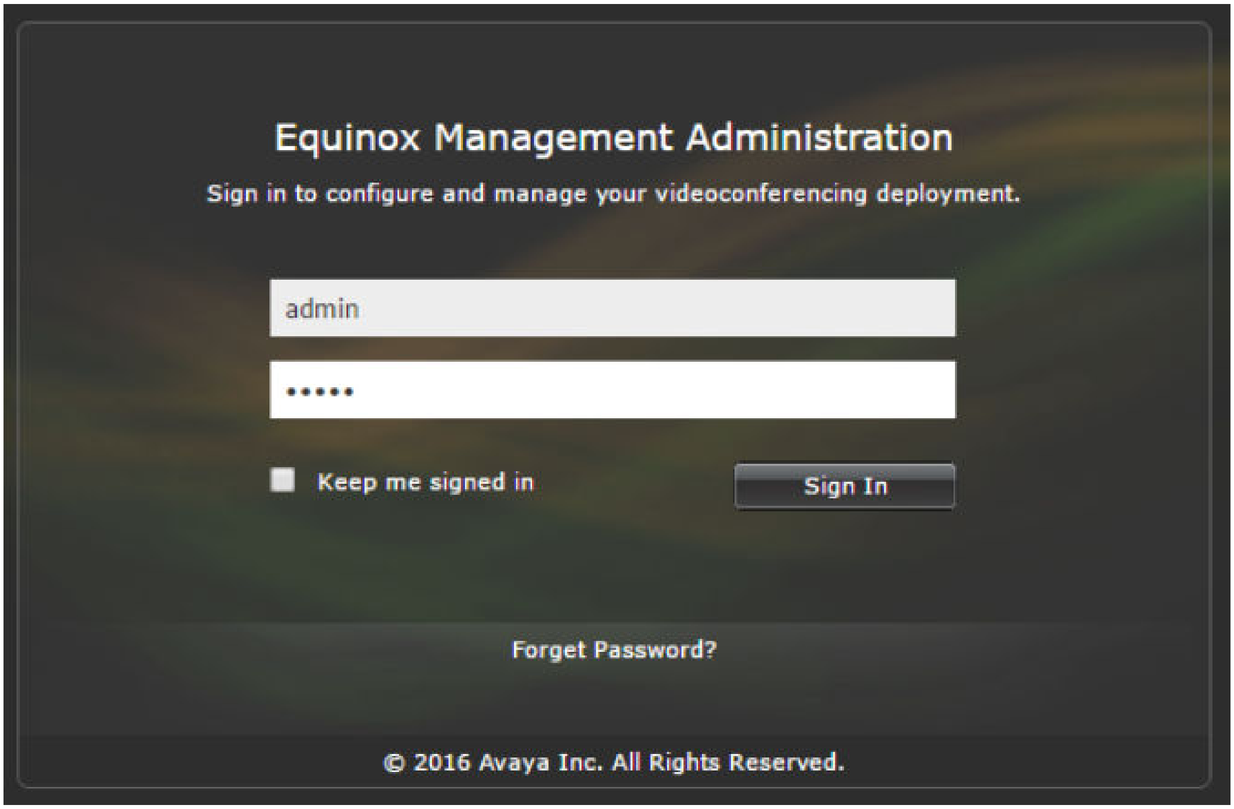
- Ensure that you have set up the following components, with their respective IP addresses:
  - All-In-One server FQDN
  - NTP server

    Note:

    We recommend using the Linux NTP server, as the Windows NTP server may not work properly.
  - DNS server

Procedure

1. Access the Equinox Management server. By default, the URL is `http://<Your Server IP>:8080/iview/`
2. Verify that the Equinox Management login page appears.



Equinox Management Administration

Sign in to configure and manage your videoconferencing deployment.

admin

•••••

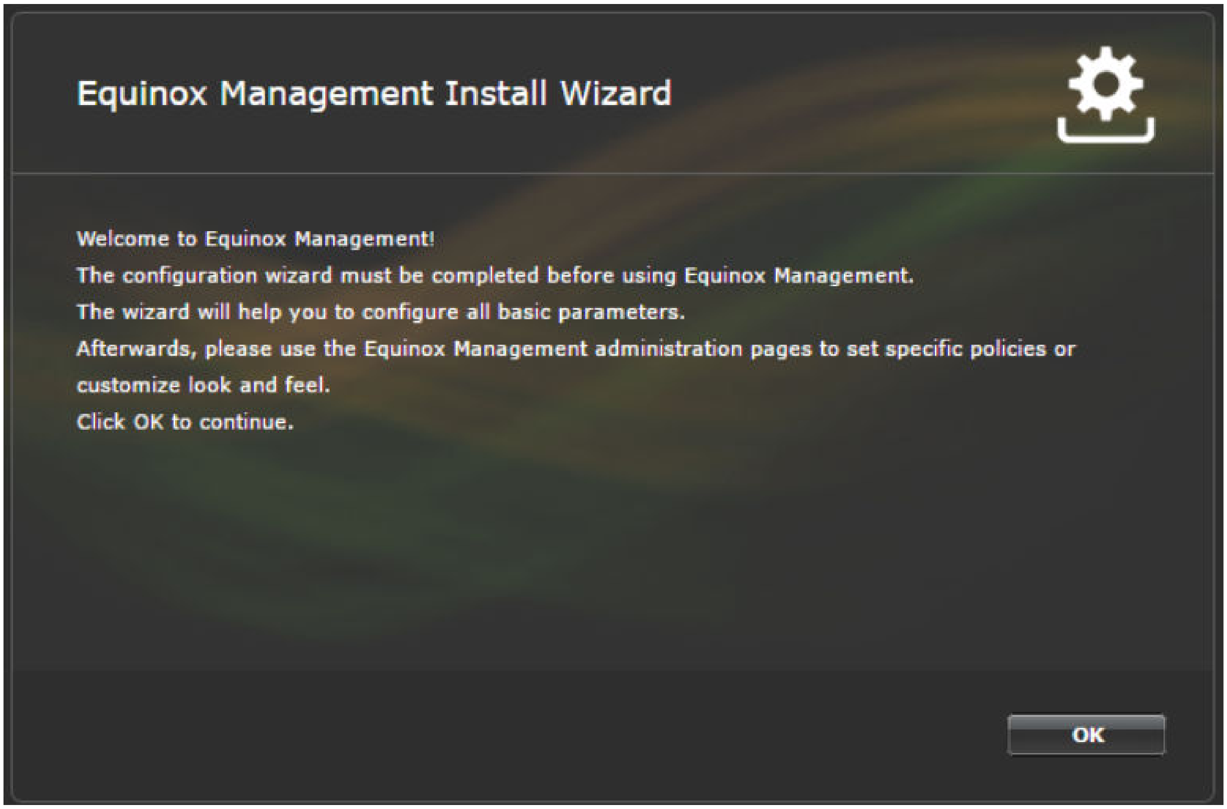
□ Keep me signed in

© 2016 Avaya Inc. All Rights Reserved.

Figure 42: Equinox Management Login Page

3. Enter login credentials in the fields. The default credentials are:
   - **Username**: admin
   - **Password**: admin

   The Equinox Management Installation Wizard opens.
4. Select **OK**. The introductory page of the wizard opens.



Equinox Management Install Wizard

Welcome to Equinox Management!

The configuration wizard must be completed before using Equinox Management.

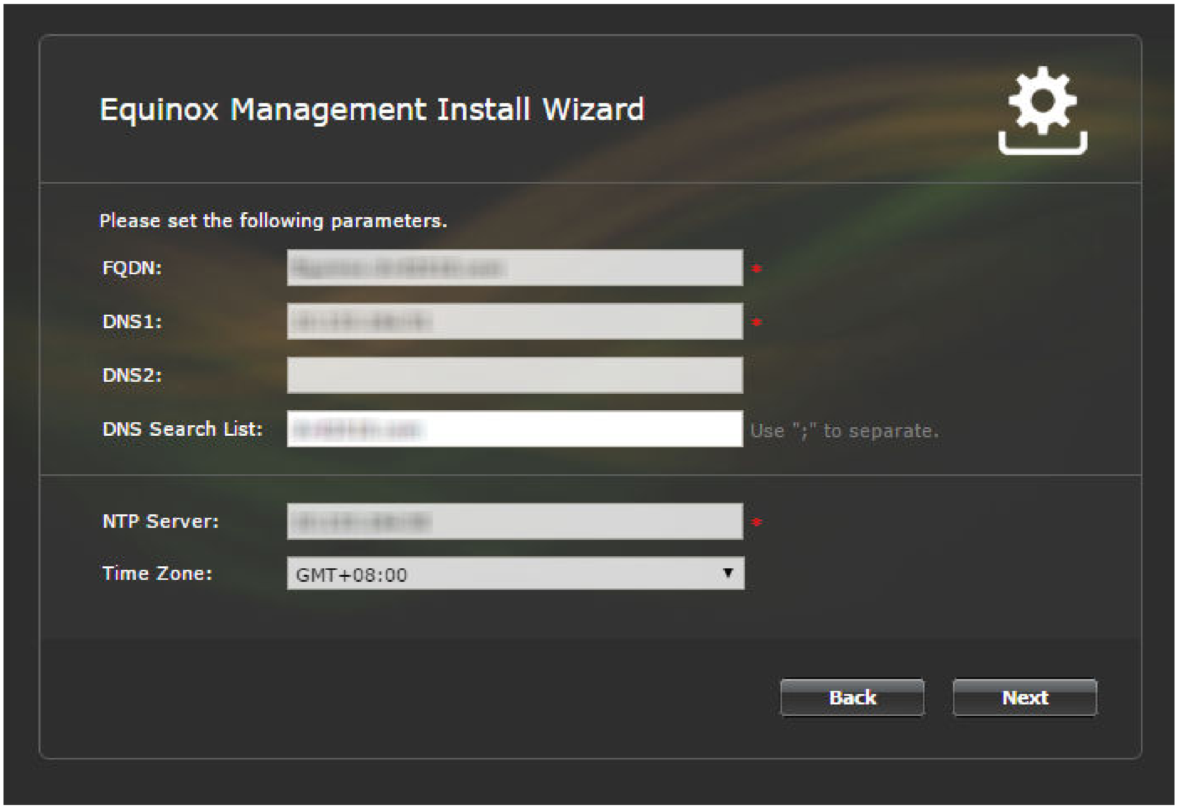
The wizard will help you to configure all basic parameters.

Afterwards, please use the Equinox Management administration pages to set specific policies or customize look and feel.

Click OK to continue.

Figure 43: Equinox Management Installation Wizard — Introduction Page

5. Select **OK**. The first page of the install wizard opens.



Equinox Management Install Wizard

Please set the following parameters.

FQDN: [redacted] *

DNS1: [redacted] *

DNS2:

DNS Search List: [redacted] Use ";" to separate.

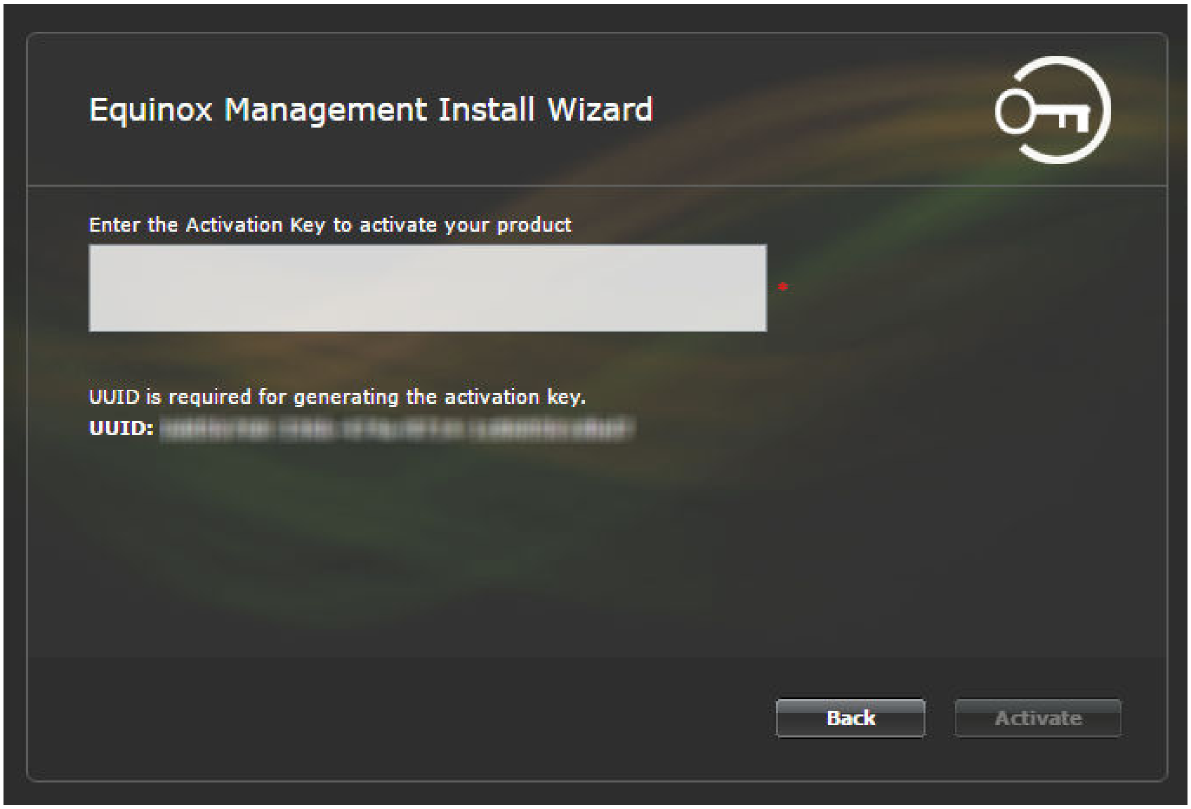
NTP Server: [redacted] *

Time Zone: GMT+08:00

Figure 44: Equinox Management Installation Wizard — Page 1

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

   The second page of the wizard opens and displays your Equinox Management server UUID.



Equinox Management Install Wizard

Enter the Activation Key to activate your product

UUID is required for generating the activation key.
UUID: [illegible]

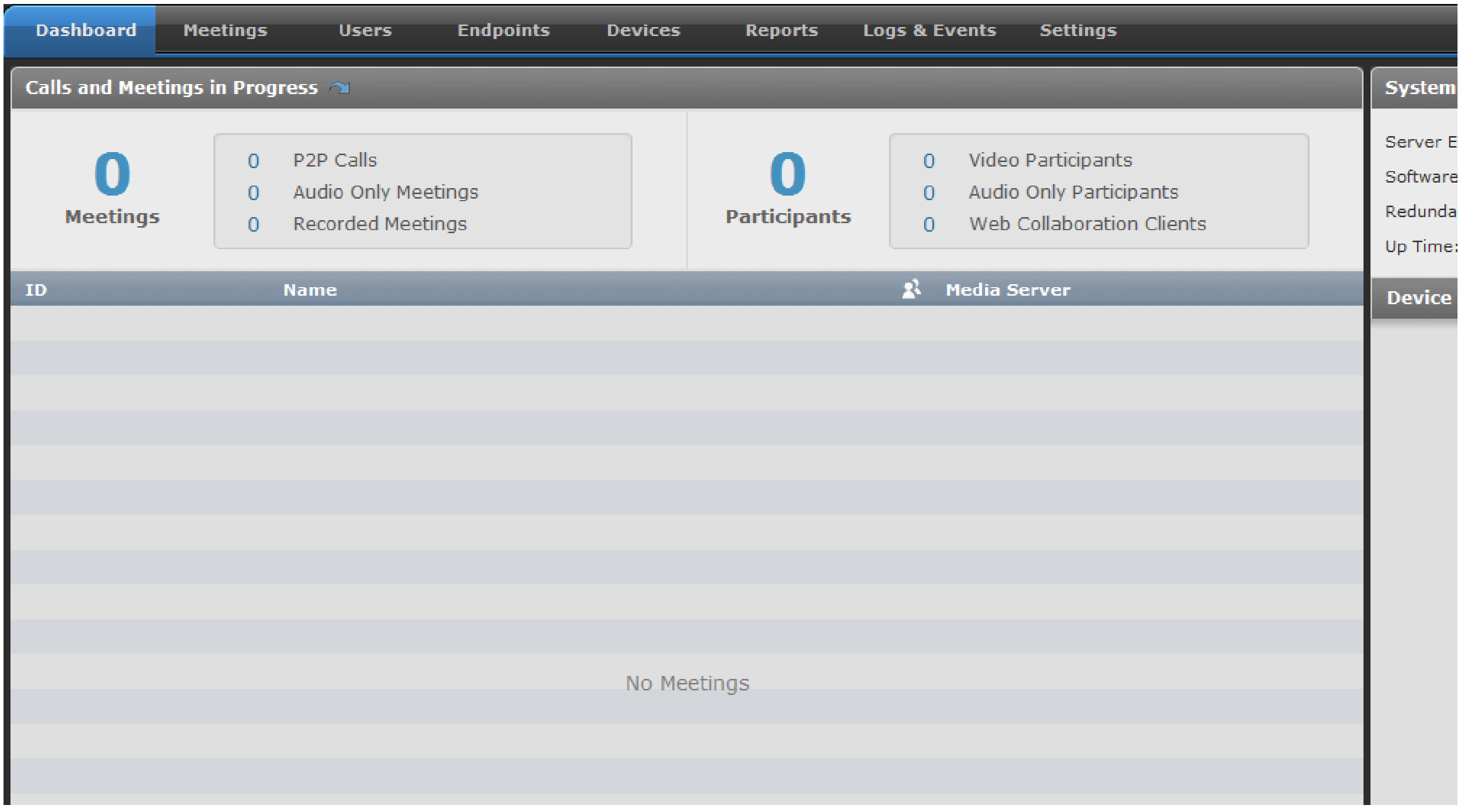
Figure 45: Equinox Management Installation Wizard — Page 2

7. Download a license activation key from PLDS (see Downloading software from PLDS on page 90).
8. Enter the activation key in the field on the page, 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.
9. Wait approximately 3–5 minutes for the system to activate, at which time you are logged into Equinox Management automatically.



0 Meetings

0 P2P Calls
0 Audio Only Meetings
0 Recorded Meetings

0 Participants

0 Video Participants
0 Audio Only Participants
0 Web Collaboration Clients

No Meetings

Figure 46: Equinox Management Dashboard

Next steps

Configure the all-in-one Equinox Management server, as described in Configuring the All-In-One Equinox Management Server on page 110.

Configuring the All-In-One Equinox Management Server

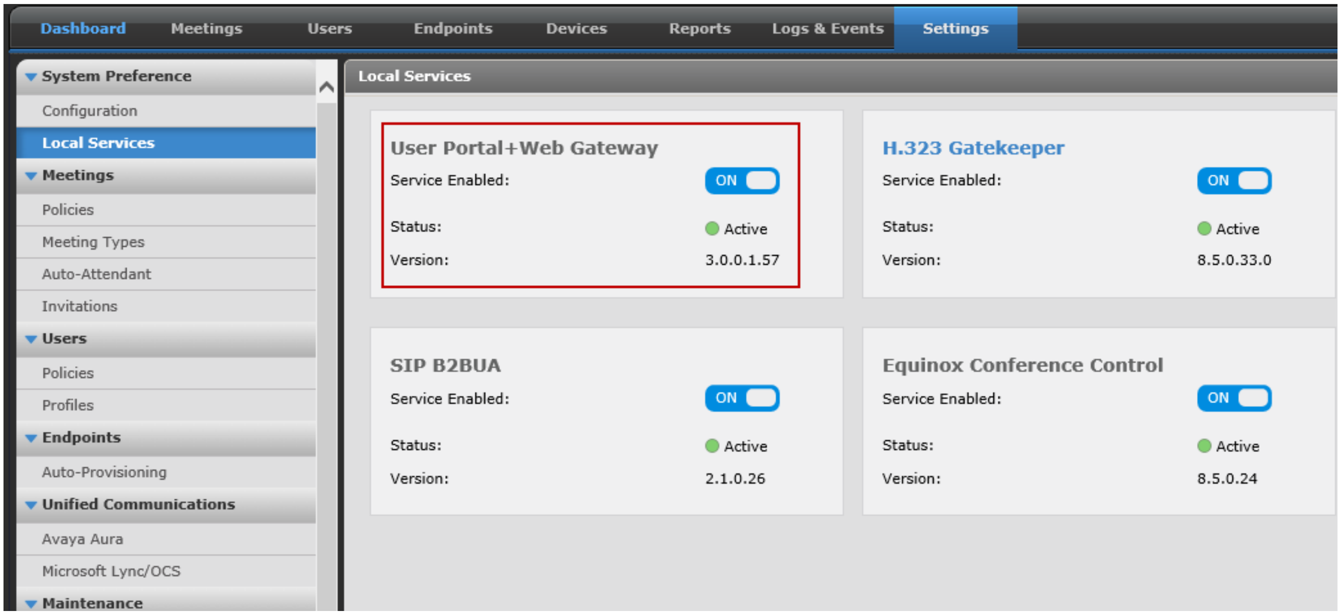
About this task

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 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**.



User Portal+Web Gateway
Service Enabled: ON
Status: Active
Version: 3.0.0.1.57

H.323 Gatekeeper
Service Enabled: ON
Status: Active
Version: 8.5.0.33.0

SIP B2BUA
Service Enabled: ON
Status: Active
Version: 2.1.0.26

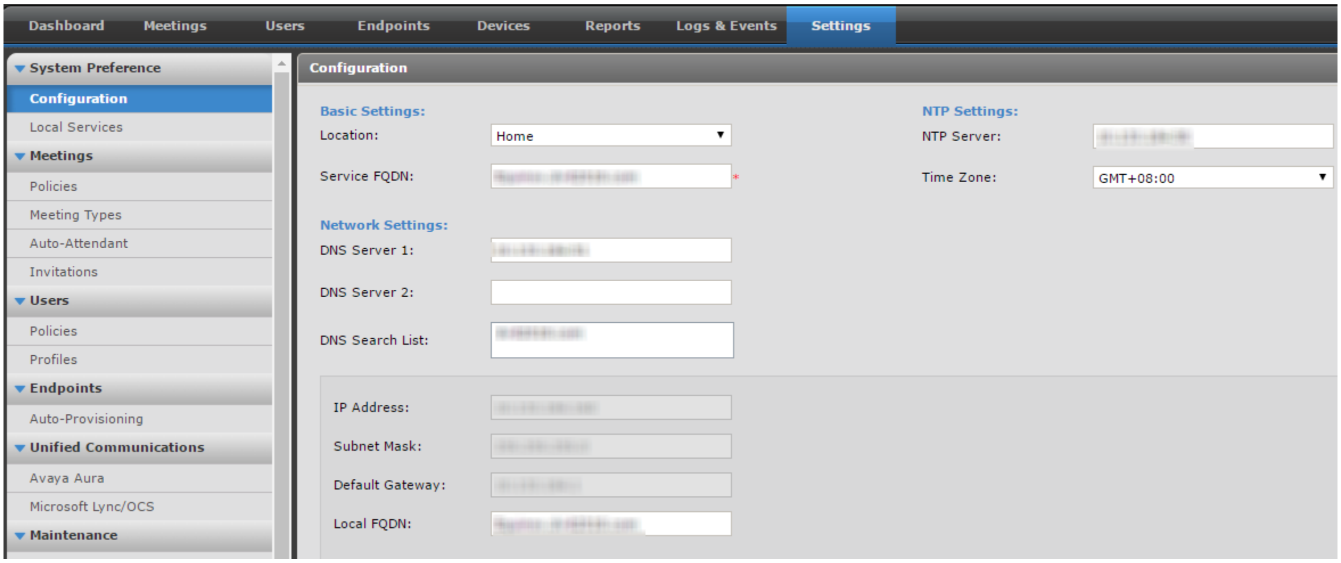
Equinox Conference Control
Service Enabled: ON
Status: Active
Version: 8.5.0.24

Figure 47: 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**, and **NTP** settings are correct.



Configuration

Basic Settings:

Location: Home

Service FQDN: [redacted] *

NTP Settings:

NTP Server: [redacted]

Time Zone: GMT+08:00

Network Settings:

DNS Server 1: [redacted]

DNS Server 2:

DNS Search List: [redacted]

IP Address: [redacted]

Subnet Mask: [redacted]

Default Gateway: [redacted]

Local FQDN: [redacted]

Figure 48: Configuration Page

Configuring the Distributed Equinox Management Server as an H.323 Gatekeeper

About this task

After deploying and configuring the Equinox Management server, you then deploy an additional management server OVA which serves as the distributed management server. You can distribute this server to an H.323 Gatekeeper.

This step is optional.

Note:

- If you want to delete an H.323 Gatekeeper that has been deployed and then add the same H.323 Gatekeeper again, you must first delete the virtual machine before doing so.
- You must specify the **Time Zone** on the **Configuration** page (**Settings** > **System Preference** > **Configuration**) before setting up a distributed management server.

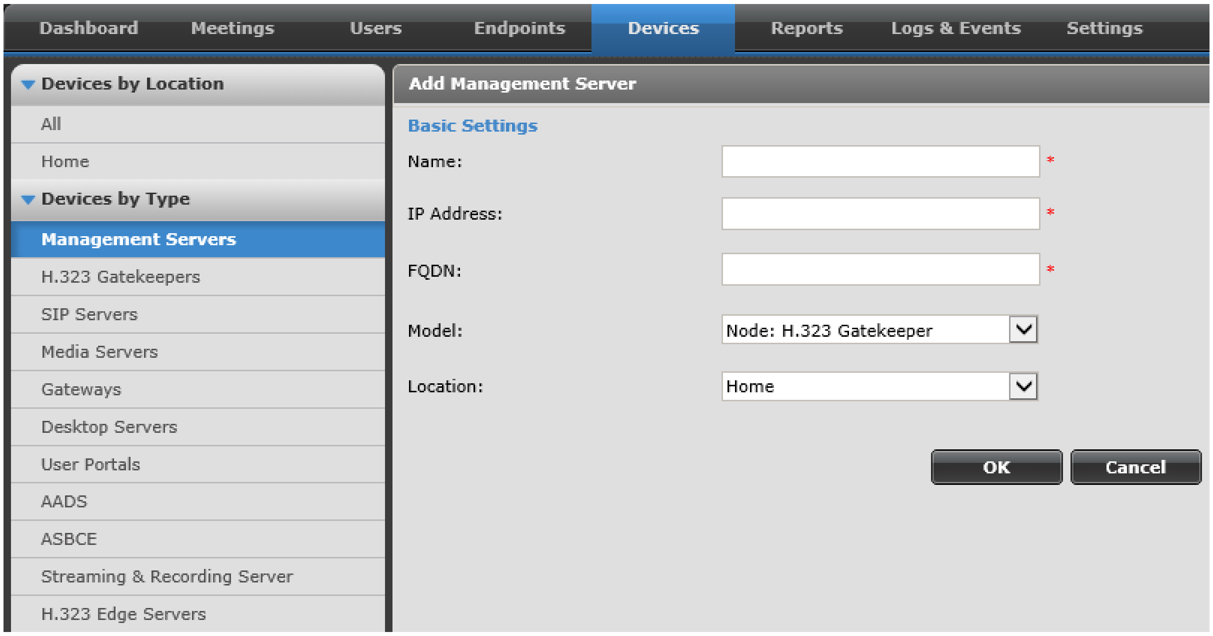
Before you begin

Ensure that you have deployed the management server OVA, as described in Deploying the Equinox Management Server on page 91.

Procedure

1. In Avaya Equinox Management, select **Devices** > **Devices by Type** > **Management Servers**.

   The **Add Management Server** page appears.



Add Management Server

Basic Settings

Name: *

IP Address: *

FQDN: *

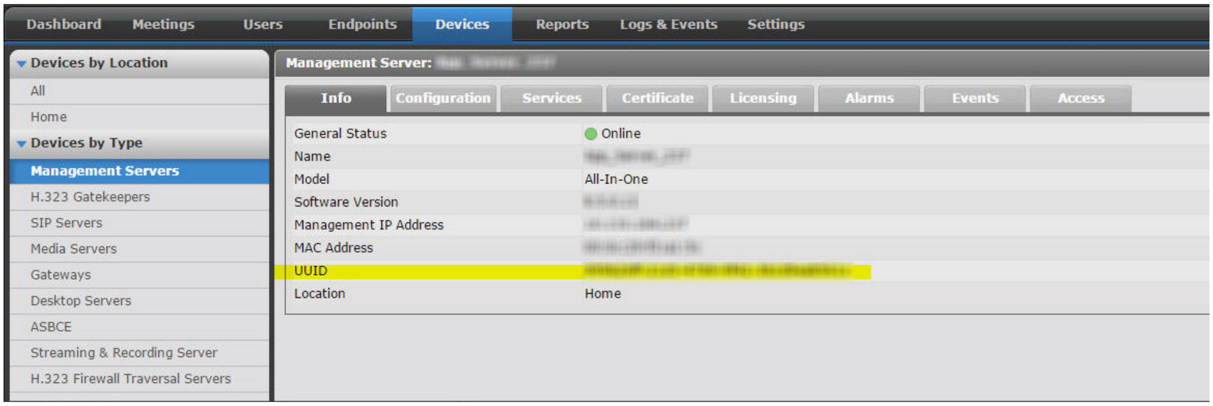
Model: Node: H.323 Gatekeeper

Location: Home

Figure 49: Add Management Server Page

2. Configure the **Name**, **IP Address**, **FQDN**, **Model** and **Location** of the server. Ensure that you select **Node: H.323 Gatekeeper** for the **Model**, and select **OK**.

3. Wait 1-2 minutes for initialization to complete, and then select the server and retrieve the server's UUID from the **Info** tab.



Management Server: [redacted]

General Status	● Online
Name	[redacted]
Model	All-In-One
Software Version	[redacted]
Management IP Address	[redacted]
MAC Address	[redacted]
UUID	[redacted]
Location	Home

Figure 50: Info Tab — Management Server UUID

4. Using the UUID, retrieve the license key from PLDS (http://plds.avaya.com).

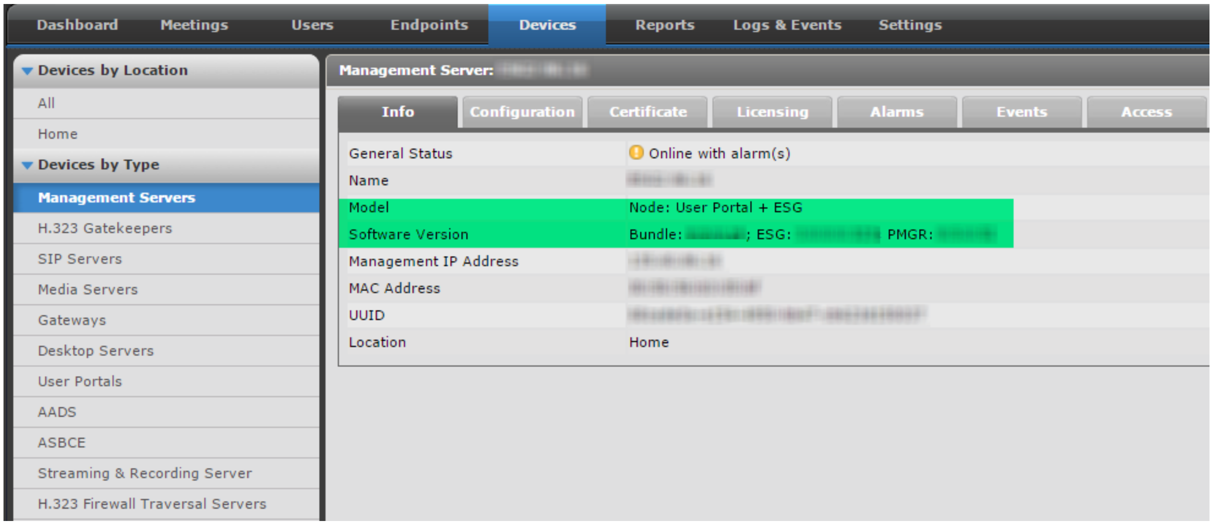
5. On the **Management Servers** page (**Devices** > **Devices by Type** > **Management Servers**), select the **Licensing** tab and enter the distributed management server license key into the **Update License Key** field, and select the **Apply** button.

Note:

Updating the license may take between 30–60 seconds.

After applying the license, the distributed H.323 Gatekeeper installs. This process may take up to 10 minutes to complete.

6. On the Management Server's **Info** tab (**Devices** > **Devices by Type** > **Management Servers**, select a management server), verify that the server's status is **Online** and that the version is correct to ensure that the distributed H.323 Gatekeeper deployment was successful.



Management Server: [redacted]

General Status	Online with alarm(s)
Name	[redacted]
Model	Node: User Portal + ESG
Software Version	Bundle: [redacted]; ESG: [redacted] PMGR: [redacted]
Management IP Address	[redacted]
MAC Address	[redacted]
UUID	[redacted]
Location	Home

Figure 51: Management Server — Status and Version

Related links

Configuring Gatekeepers in Avaya Equinox Management on page 114

Configuring Gatekeepers in Avaya Equinox Management

Equinox Management is shipped with a built-in gatekeeper, the Avaya Equinox gatekeeper, which can be used to manage and route endpoint-initiated calls and point-to-point calls. Equinox Management can also work with the standalone Avaya Equinox H.323 Gatekeeper or third party gatekeepers when they are configured as neighbors to its internal gatekeeper. Available third-party gatekeepers include the Cisco IOS H.323 Gatekeeper and the Tandberg (Cisco) Video Communications Server (VCS). Only endpoints can be registered to a third-party gatekeeper. For details on deploying and configuring an external gatekeeper, see the *Administrator Guide for Avaya Equinox Management*.

Related links

Configuring the Distributed Equinox Management Server as an H.323 Gatekeeper on page 112

Defining the Gatekeeper's Dial Plan in Avaya Equinox Management on page 115

Defining the Gatekeeper’s Dial Plan in Avaya Equinox Management

About this task

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

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

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

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

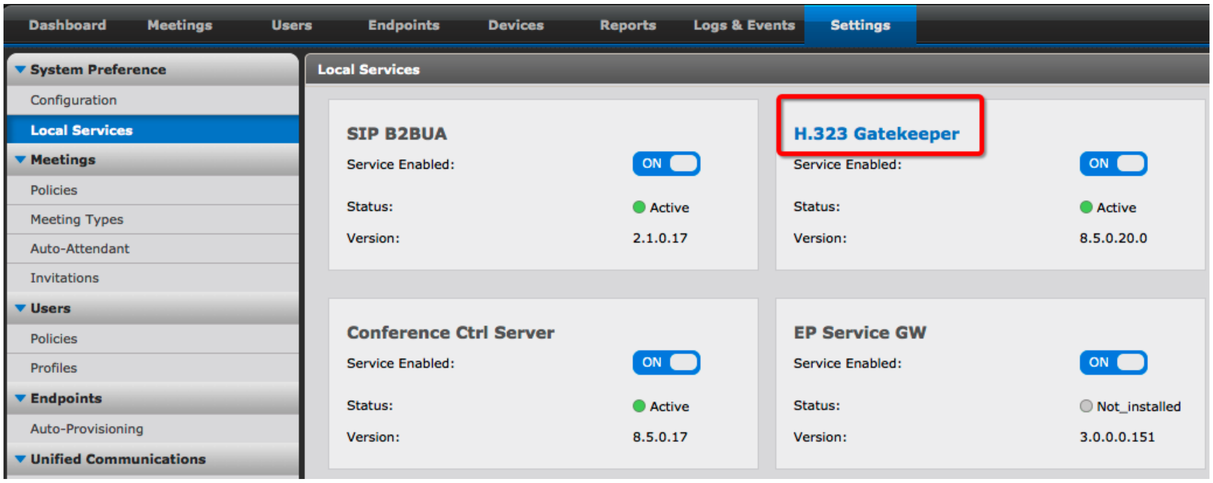
Similarly, a gatekeeper can be configured to determine locations in an organization’s dial plan. For example, all numbers beginning with ‘5’ might be located in Europe, ‘6’ routes to the west coast of the US, ‘7’ to the east coast, and so on.

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

Procedure

1. Access the Equinox Management administrator portal.
2. In the **Settings** tab, navigate to **System Preference** > **Local Services**.

   The **Local Services** page opens.



SIP B2BUA
Service Enabled: ON
Status: Active
Version: 2.1.0.17

H.323 Gatekeeper
Service Enabled: ON
Status: Active
Version: 8.5.0.20.0

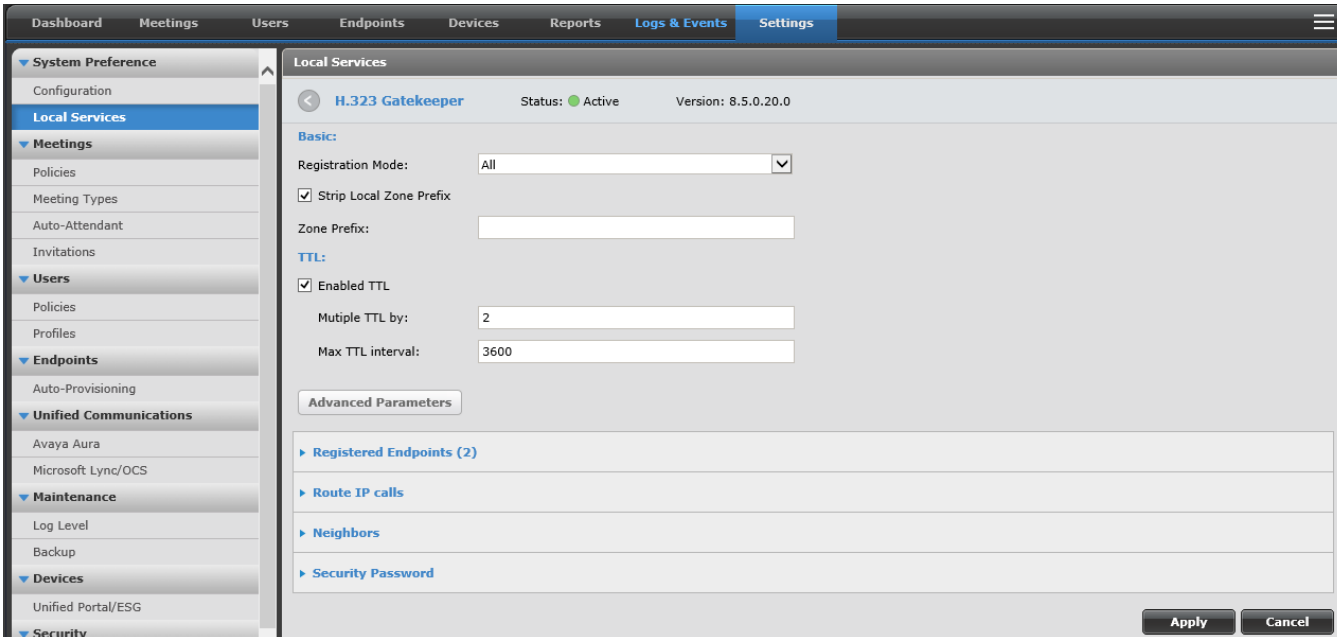
Conference Ctrl Server
Service Enabled: ON
Status: Active
Version: 8.5.0.17

EP Service GW
Service Enabled: ON
Status: Not_installed
Version: 3.0.0.0.151

Figure 52: Local Services Page

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

   The gatekeeper's information page opens.



Status: Active

Version: 8.5.0.20.0

Basic:

Registration Mode: All

☑ Strip Local Zone Prefix

Zone Prefix:

TTL:

☑ Enabled TTL

Mutiple TTL by: 2

Max TTL interval: 3600

Figure 53: H.323 Gatekeeper Information Page

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

Table 14: Configuring the H.323 Gatekeeper Settings

Section Name	Field Name	Description
Basic	**Registration Mode**	Select the mode by which endpoints can register with the H.323 Gatekeeper: • **All**: Any endpoint can register with the H.323 Gatekeeper • **None**: No endpoint can register with the H.323 Gatekeeper • **Predefined**: Only Equinox Management endpoints can register with the H.323 Gatekeeper
	Strip Zone Local Prefix	Select to remove the local zone prefix when calling the endpoint.
	Zone Prefix	A number which the endpoint uses as a prefix before dialing another endpoint.
TTL	**Enabled TTL**	Select to require the endpoint to re-register with the H.323 Gatekeeper when the endpoint's Time-To-Live (TTL) setting expires.
	Multiple TTL by	Increases the length of time that the H.323 Gatekeeper waits for TTL expiration before an endpoint is unregistered. Enter an integer between 1–100 to indicate the factor by which you want to multiply the endpoint's TTL value. Default value = **2**

Table continues…

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

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

Related links

Configuring Gatekeepers in Avaya Equinox Management on page 114

Configuring Deployment of User Portal + Web Gateway

About this task

You can deploy a single distributed User Portal + Web Gateway in your environment. Once you deploy more than one User Portal + Web Gateway, they are formed as a cluster.

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.

To deploy User Portal + Web Gateway, follow this procedure.

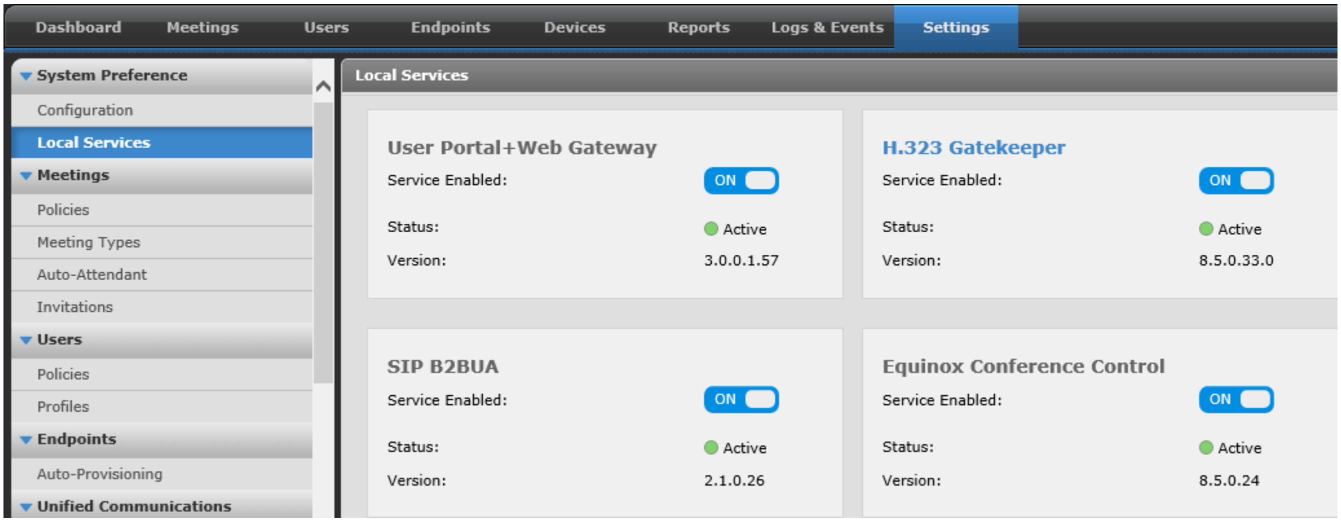
Before you begin

Specify the NTP Server on the **Configuration** page (**Settings** > **System Preference** > **Configuration**) before setting up a distributed management server.

Procedure

1. Access the Avaya Equinox Management Administrator portal.
2. Select **Settings** > **System Preference** > **Local Services**.

   The **Local Services** page appears.



User Portal+Web Gateway
Service Enabled: ON
Status: Active
Version: 3.0.0.1.57

H.323 Gatekeeper
Service Enabled: ON
Status: Active
Version: 8.5.0.33.0

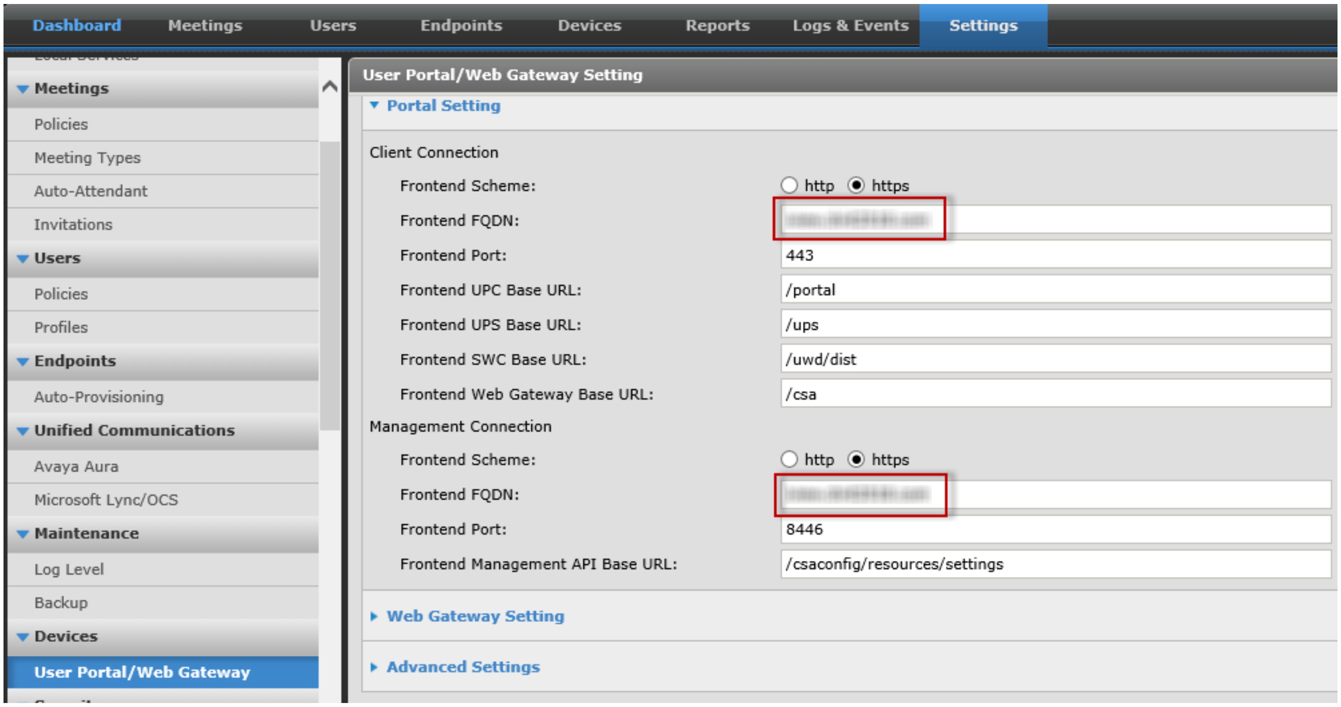
SIP B2BUA
Service Enabled: ON
Status: Active
Version: 2.1.0.26

Equinox Conference Control
Service Enabled: ON
Status: Active
Version: 8.5.0.24

Figure 54: Local Services Page

3. Turn off the **User Portal + Web Gateway** service (if its status is **Active**).
4. Select **Settings** > **Devices** > **User Portal/Web Gateway**.

   The **User Portal/Web Gateway** page appears.
5. Expand the **Portal Setting** section, and configure the **Frontend FQDN** for both the client connection and management connection.



User Portal/Web Gateway Setting

Portal Setting

Client Connection

Frontend Scheme:	○ http ● https
Frontend FQDN:	[redacted]
Frontend Port:	443
Frontend UPC Base URL:	/portal
Frontend UPS Base URL:	/ups
Frontend SWC Base URL:	/uwd/dist
Frontend Web Gateway Base URL:	/csa

Management Connection

Frontend Scheme:	○ http ● https
Frontend FQDN:	[redacted]
Frontend Port:	8446
Frontend Management API Base URL:	/csaconfig/resources/settings

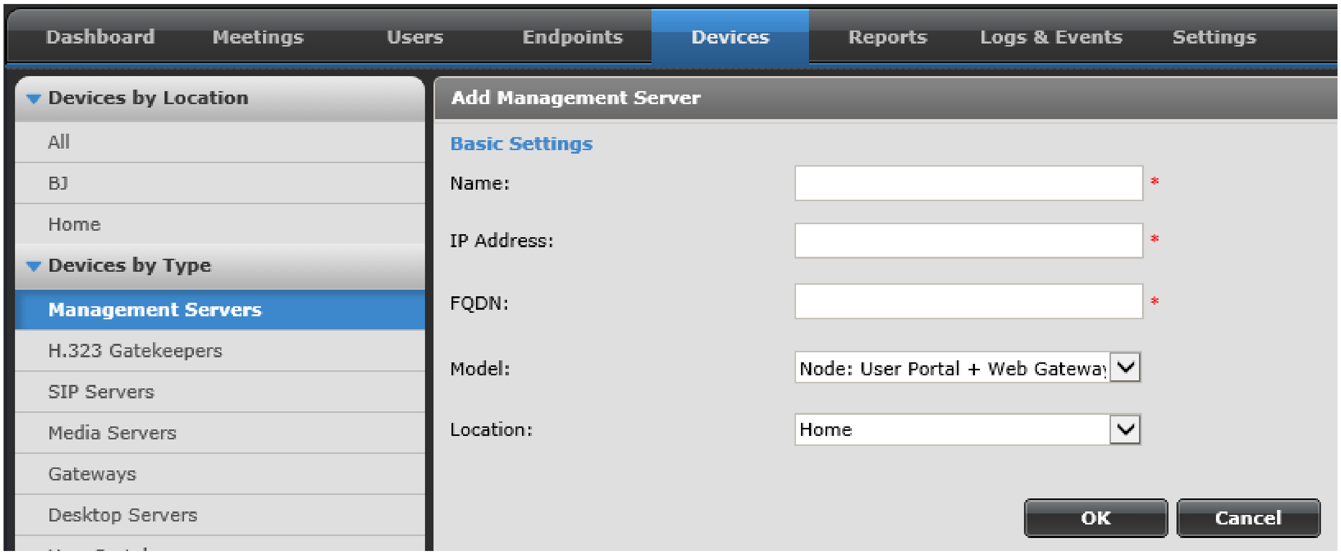
Web Gateway Setting

Advanced Settings

Figure 55: User Portal/Web Gateway Setting Page — Portal Setting Section

6. Select **Apply**.
7. Select **Devices** > **Devices by Type** > **Management Servers**, and select **Add**.

   The **Add Management Server** page appears.



Add Management Server

Basic Settings

Name:	*
IP Address:	*
FQDN:	*
Model:	Node: User Portal + Web Gateway
Location:	Home

Figure 56: Add Management Server Page

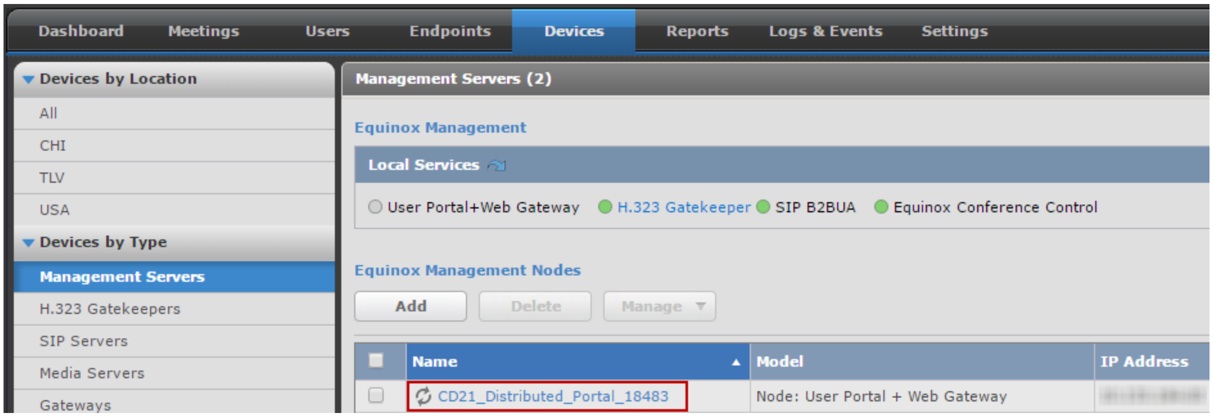
8. Configure management server settings, as follows:
   a. Configure the management server **Name**, **IP address**, and **FQDN**.

   b. In the **Model** field, select **User Portal + Web Gateway** from the dropdown list.

   c. In the **Location** field, select the location of the management server.

9. Select **OK**.

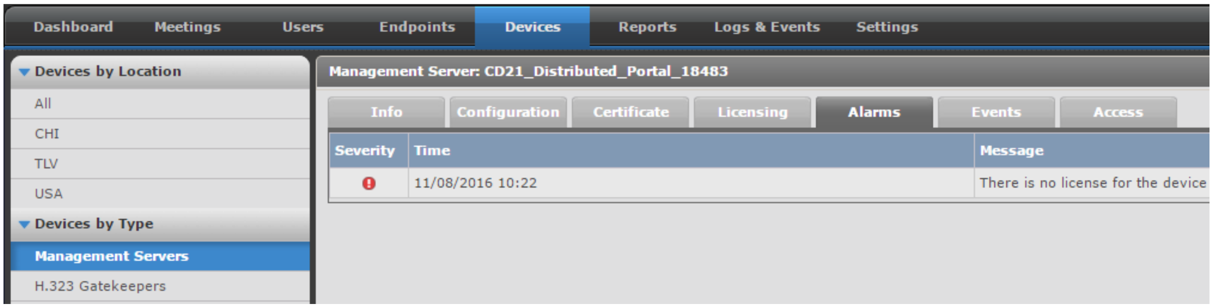
   The **Management Servers** page appears, where the node is shown as connecting.



□	Name ▲	Model	IP Address
□	CD21_Distributed_Portal_18483	Node: User Portal + Web Gateway	[redacted]

Figure 57: Management Servers Page — Node Connecting

10. After approximately two minutes, the icon next to the node becomes yellow, indicating a warning. Select the icon; the **Alarms** tab for the management server appears.



Severity	Time	Message
●	11/08/2016 10:22	There is no license for the device

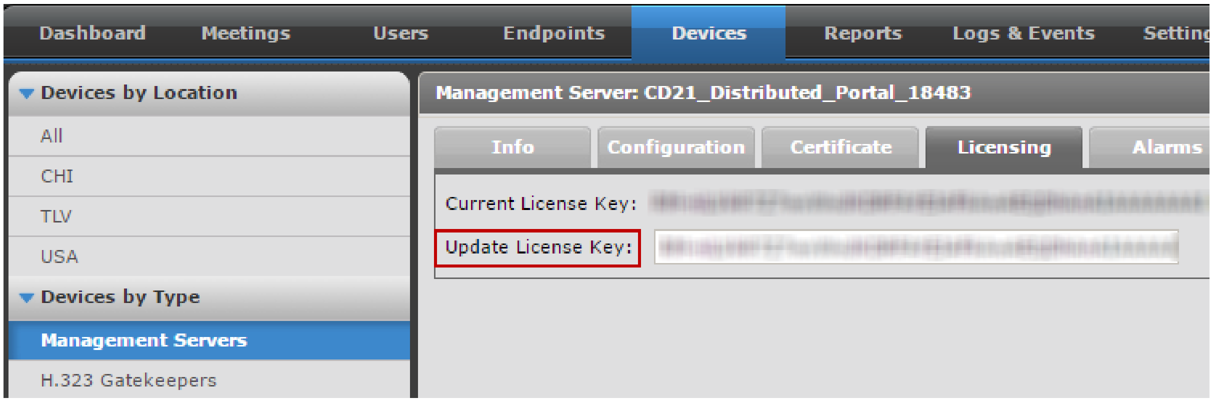
Figure 58: Management Server Alarms Tab

11. Retrieve the server's UUID from the **Info** tab.

12. Use the UUID to retrieve the license from PLDS (http://plds.avaya.com).

    The generated license ID displays on the PLDS interface.

13. Select the **Licensing** tab on the **Management Server** page (**Devices** > **Management Servers** > **Licensing**) and enter the generated license ID in the **Update License Key** field.



Management Server: CD21_Distributed_Portal_18483

Current License Key: [redacted]

Update License Key: [redacted]

Figure 59: Update License Key Field

14. Select **OK**. Equinox Management installs the User Portal + Web Gateway. You must wait up to 10 minutes for installation to complete.
15. When the installation completes, apply a third-party certificate to the User Portal + Web Gateway, as described in Applying a Third-Party Certificate to the Distributed Equinox Management Server on page 126.

    The User Portal + Web Gateway server restarts automatically.
16. On the **Management Server** page, the User Portal + Web Gateway server displays with a green icon, indicating that it is connected.

    If the service displays with a yellow icon, check the **Alarms** tab. Alarms relating to resource limits do not affect the User Portal + Web Gateway performance.

    Note:

    After successfully deploying the seed node, you can add additional User Portal + Web Gateways, which are non-seed nodes. When deploying non-seed nodes, the seed node's status must be either **Active** (green icon) or **Warning** (yellow icon) with non-critical alarms to enable deploying non-seed nodes.

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.

Related links

Applying a Third-Party Certificate to the All-in-One Equinox Management Server on page 122

Applying a Third-Party Certificate to the Distributed Equinox Management Server on page 126
Installing the CA Certificate for Avaya Equinox Meetings for Web on page 129

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.

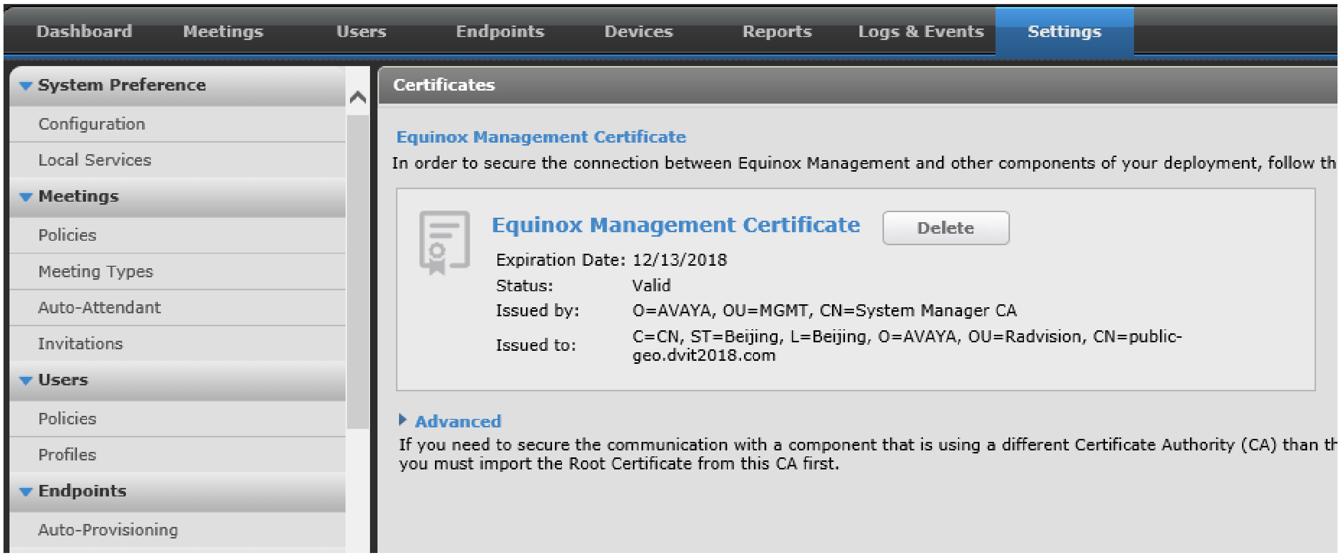
Before you begin

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 110.

Procedure

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

   The **Certificates** page opens.



Certificates

Equinox Management Certificate

In order to secure the connection between Equinox Management and other components of your deployment, follow th

Equinox Management Certificate

Expiration Date: 12/13/2018
Status: Valid
Issued by: O=AVAYA, OU=MGMT, CN=System Manager CA
Issued to: C=CN, ST=Beijing, L=Beijing, O=AVAYA, OU=Radvision, CN=public-geo.dvit2018.com

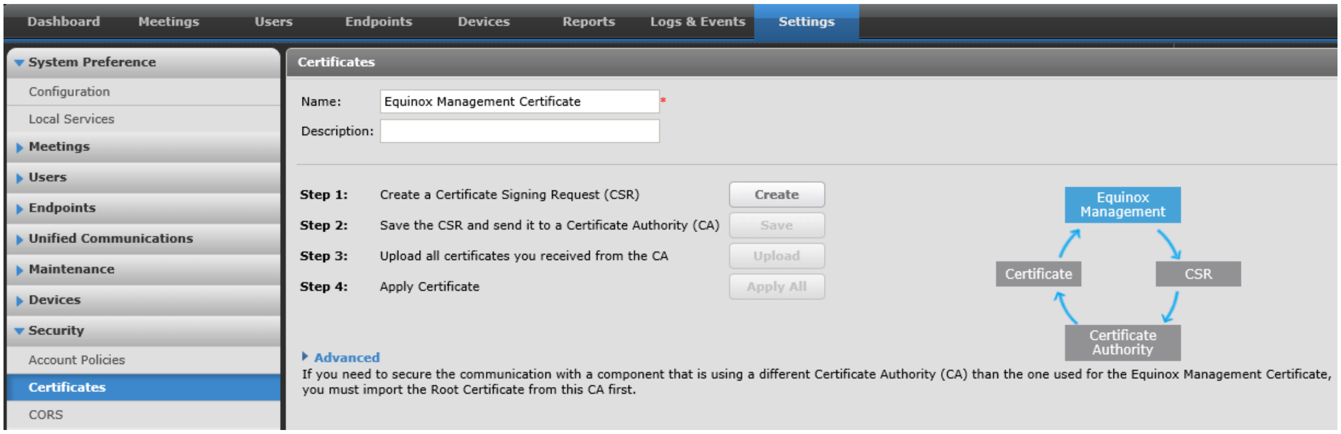
Advanced

If you need to secure the communication with a component that is using a different Certificate Authority (CA) than th you must import the Root Certificate from this CA first.

Figure 60: Certificates Page

3. Select the **Delete** button to delete the internal certificate.

   The **Certificates** page refreshes:



Name: Equinox Management Certificate *

Description:

Step 1: Create a Certificate Signing Request (CSR)

Step 2: Save the CSR and send it to a Certificate Authority (CA)

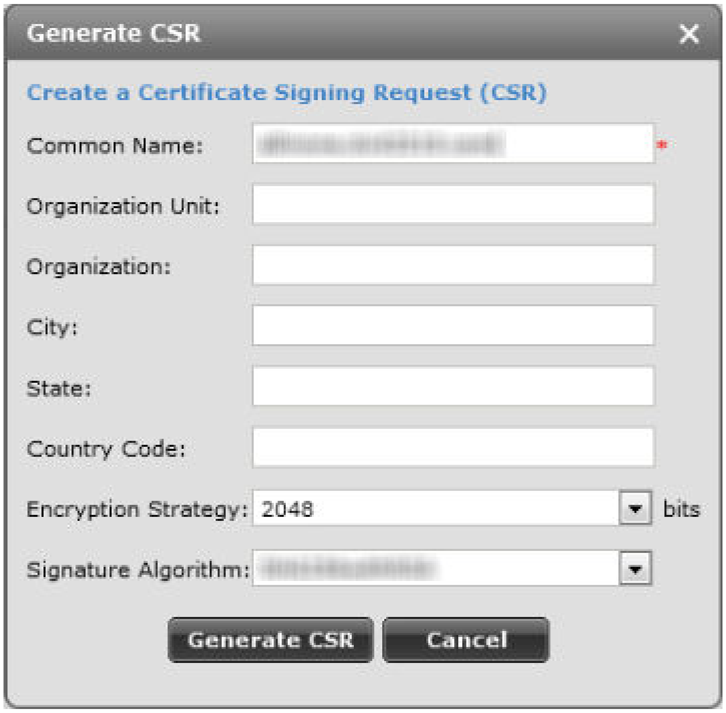
Step 3: Upload all certificates you received from the CA

Step 4: Apply Certificate

If you need to secure the communication with a component that is using a different Certificate Authority (CA) than the one used for the Equinox Management Certificate, you must import the Root Certificate from this CA first.

Figure 61: Certificates Page

4. Select **Create**. The **Generate CSR** dialog box opens.



Common Name: [redacted] *

Organization Unit:

Organization:

City:

State:

Country Code:

Encryption Strategy: 2048 bits

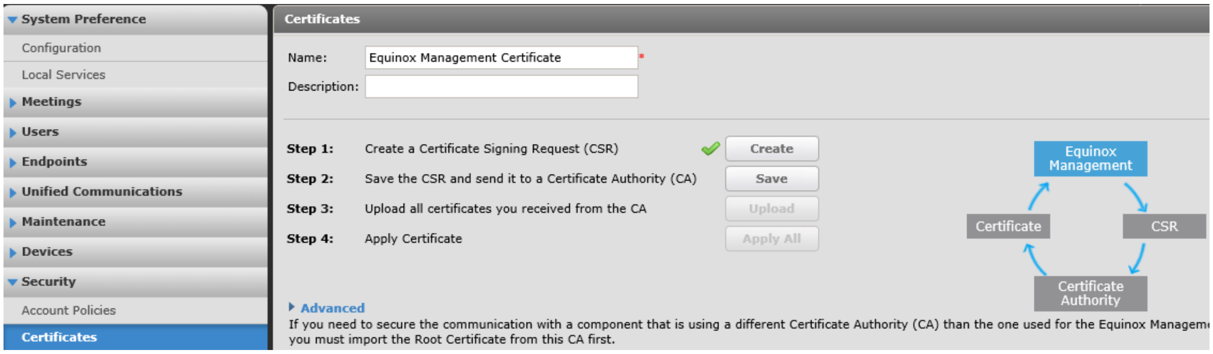
Signature Algorithm: [redacted]

Figure 62: 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.

5. Enter the **Common Name** and other parameters for the certificate, and then select **Generate CSR**. A green check mark appears next to **Step 1**, and the **Save** button is enabled.



Certificates

Name: Equinox Management Certificate *

Description:

Step 1: Create a Certificate Signing Request (CSR) ✓

Step 2: Save the CSR and send it to a Certificate Authority (CA)

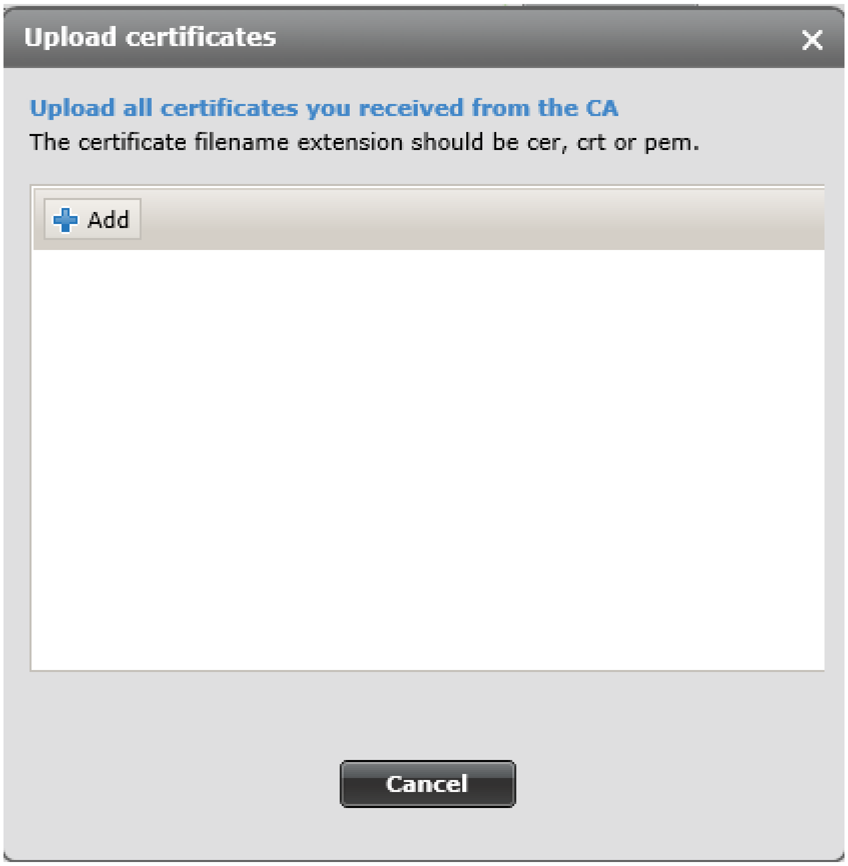
Step 3: Upload all certificates you received from the CA

Step 4: Apply Certificate

If you need to secure the communication with a component that is using a different Certificate Authority (CA) than the one used for the Equinox Managem
you must import the Root Certificate from this CA first.

Figure 63: 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. Select **Upload**. The **Upload Certificates** dialog box opens.



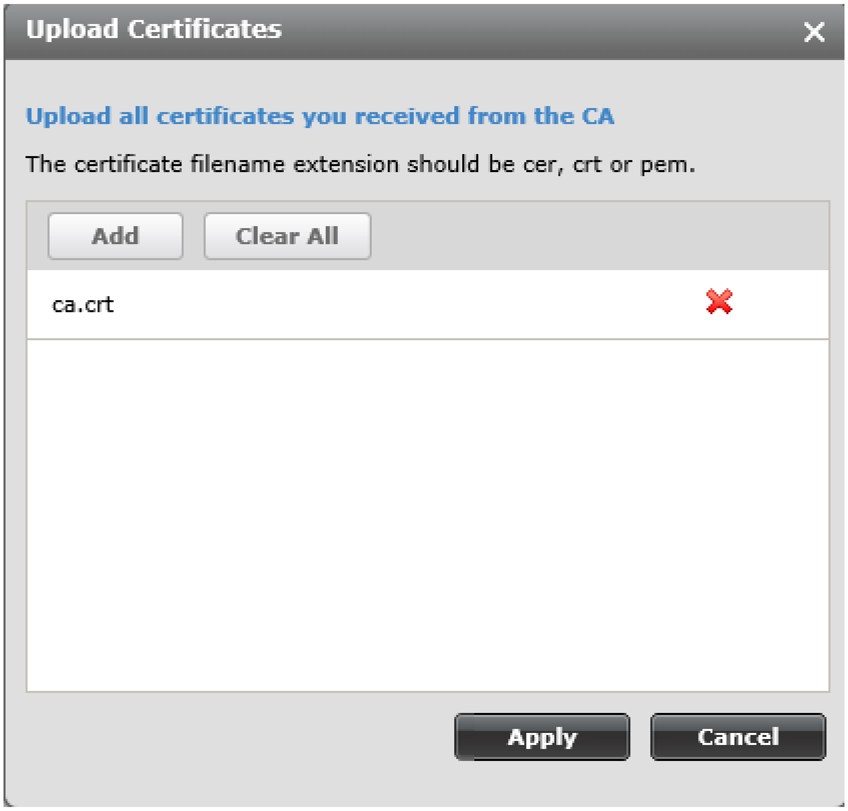
Upload certificates

Upload all certificates you received from the CA

The certificate filename extension should be cer, crt or pem.

Figure 64: Upload Certificates Dialog Box

8. Select **Add** to browse for the certificate. The certificate you select displays in the **Upload Certificates** dialog box.



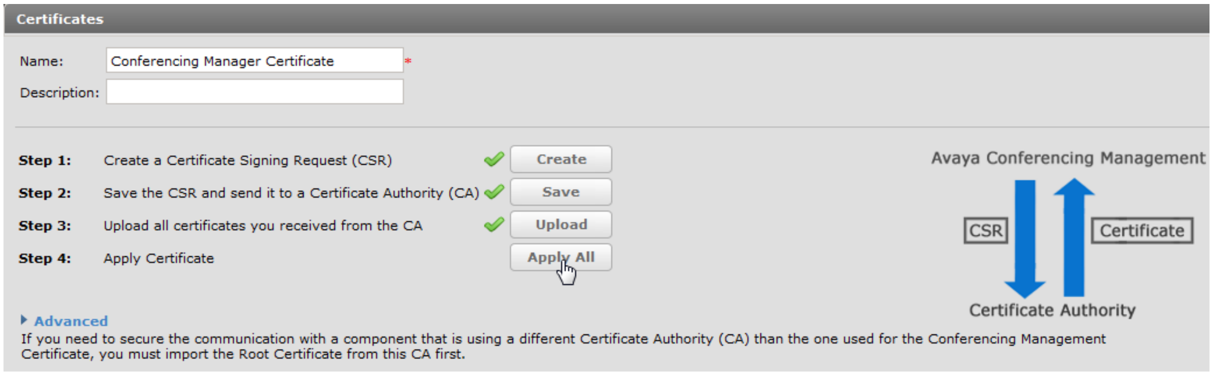
Upload all certificates you received from the CA

The certificate filename extension should be cer, crt or pem.

ca.crt

Figure 65: Upload Certificates Dialog Box

9. Select **Apply** to upload the indicated certificate to Equinox Management. A green check mark appears next to **Step 3**, and the **Apply All** button is enabled.



Name: Conferencing Manager Certificate *

Description:

Step 1: Create a Certificate Signing Request (CSR) ✓

Step 2: Save the CSR and send it to a Certificate Authority (CA) ✓

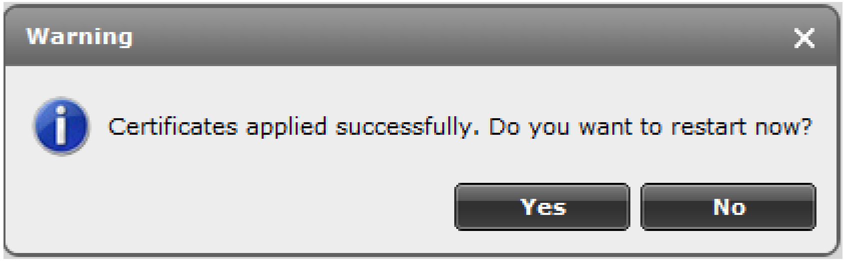
Step 3: Upload all certificates you received from the CA ✓

Step 4: Apply Certificate

If you need to secure the communication with a component that is using a different Certificate Authority (CA) than the one used for the Conferencing Management Certificate, you must import the Root Certificate from this CA first.

Figure 66: Certificates Page — Apply All Button

10. Select **Apply All** to apply the certificate. A dialog box appears, prompting you to restart the server.



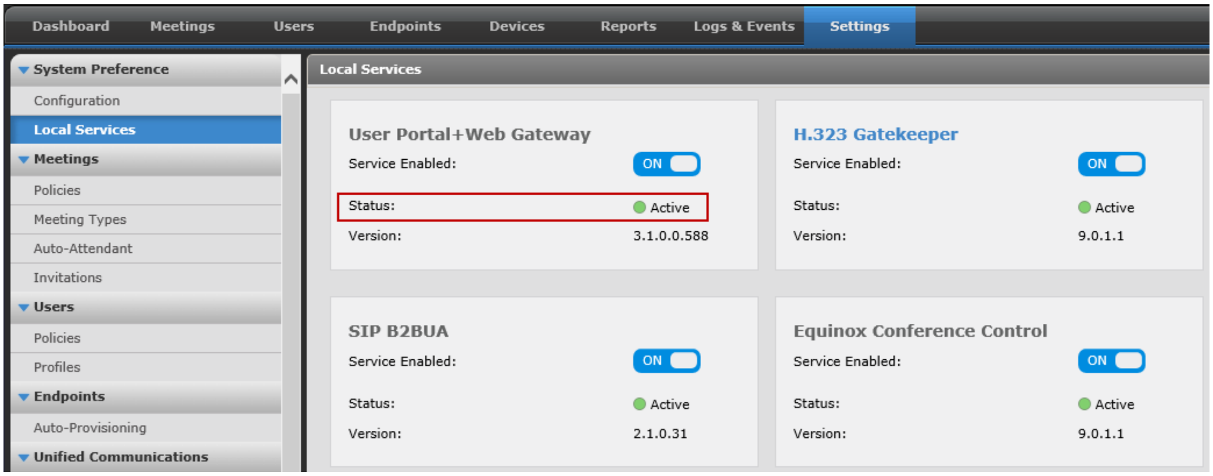
Warning

Certificates applied successfully. Do you want to restart now?

Figure 67: 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**.



Local Services

User Portal+Web Gateway
Service Enabled: ON
Status: Active
Version: 3.1.0.0.588

H.323 Gatekeeper
Service Enabled: ON
Status: Active
Version: 9.0.1.1

SIP B2BUA
Service Enabled: ON
Status: Active
Version: 2.1.0.31

Equinox Conference Control
Service Enabled: ON
Status: Active
Version: 9.0.1.1

Figure 68: Local Services Page — User Portal + Web Gateway Status

Related links

Securing Connections With Equinox Management on page 121

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

About this task

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.

Note:

This step is optional.

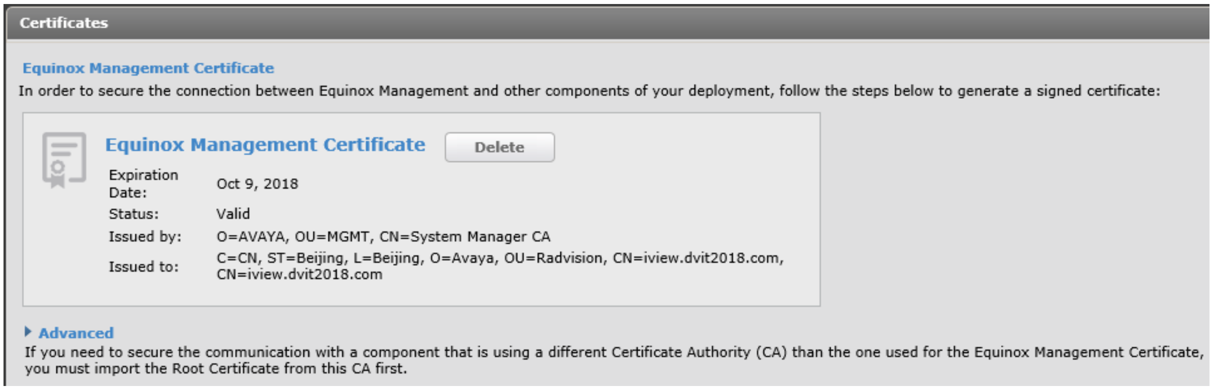
Before you begin

Ensure that you have set up the distributed Equinox Management server, as described in Configuring the Distributed Equinox Management Server as an H.323 Gatekeeper on page 112.

Procedure

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

   The **Certificates** page appears.



Certificates

Equinox Management Certificate

In order to secure the connection between Equinox Management and other components of your deployment, follow the steps below to generate a signed certificate:

Equinox Management Certificate Delete

Expiration Date: Oct 9, 2018

Status: Valid

Issued by: O=AVAYA, OU=MGMT, CN=System Manager CA

Issued to: C=CN, ST=Beijing, L=Beijing, O=Avaya, OU=Radvision, CN=iview.dvit2018.com, CN=iview.dvit2018.com

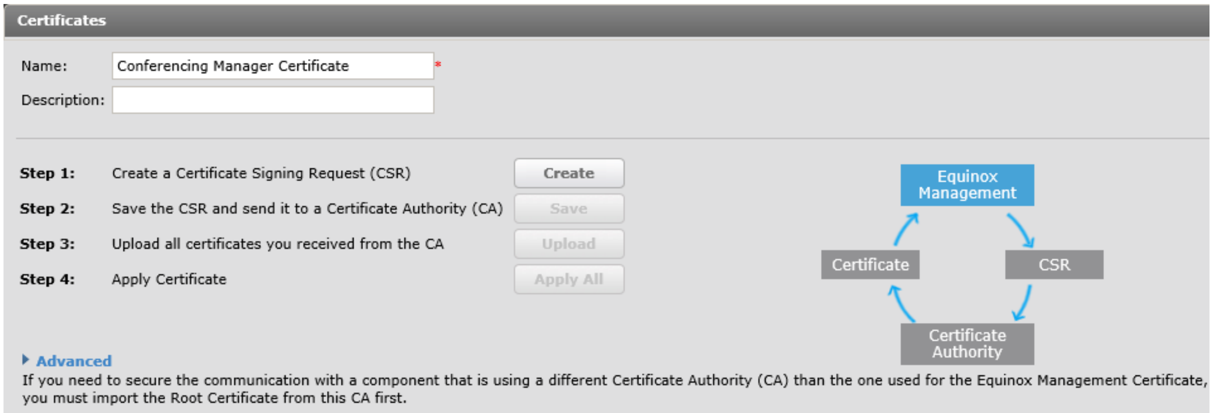
▸ Advanced

If you need to secure the communication with a component that is using a different Certificate Authority (CA) than the one used for the Equinox Management Certificate, you must import the Root Certificate from this CA first.

Figure 69: 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.



Certificates

Name: Conferencing Manager Certificate *

Description:

Step 1: Create a Certificate Signing Request (CSR) Create

Step 2: Save the CSR and send it to a Certificate Authority (CA) Save

Step 3: Upload all certificates you received from the CA Upload

Step 4: Apply Certificate Apply All

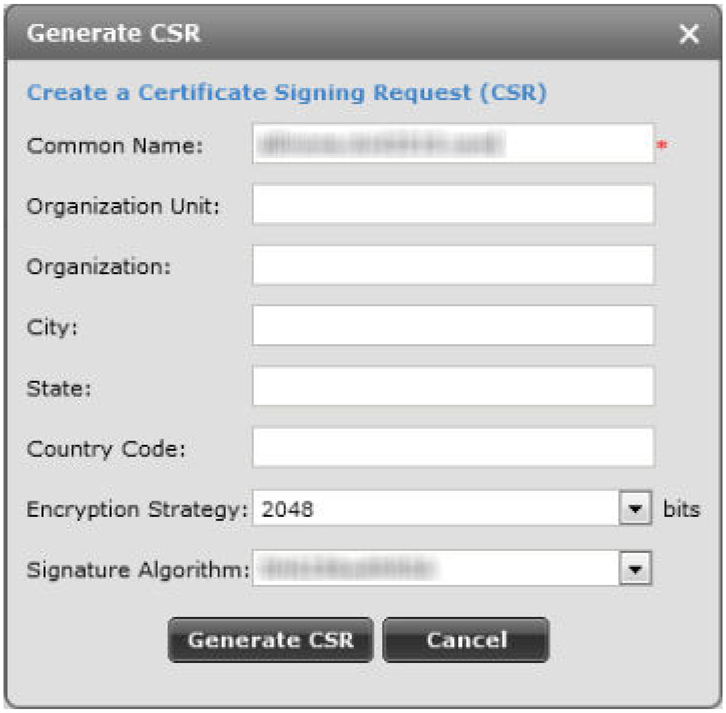
▸ Advanced

If you need to secure the communication with a component that is using a different Certificate Authority (CA) than the one used for the Equinox Management Certificate, you must import the Root Certificate from this CA first.

Figure 70: Certificates Page

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

   The **Generate CSR** dialog box opens.



Generate CSR

Create a Certificate Signing Request (CSR)

Common Name: [redacted] *

Organization Unit:

Organization:

City:

State:

Country Code:

Encryption Strategy: 2048 bits

Signature Algorithm: [redacted]

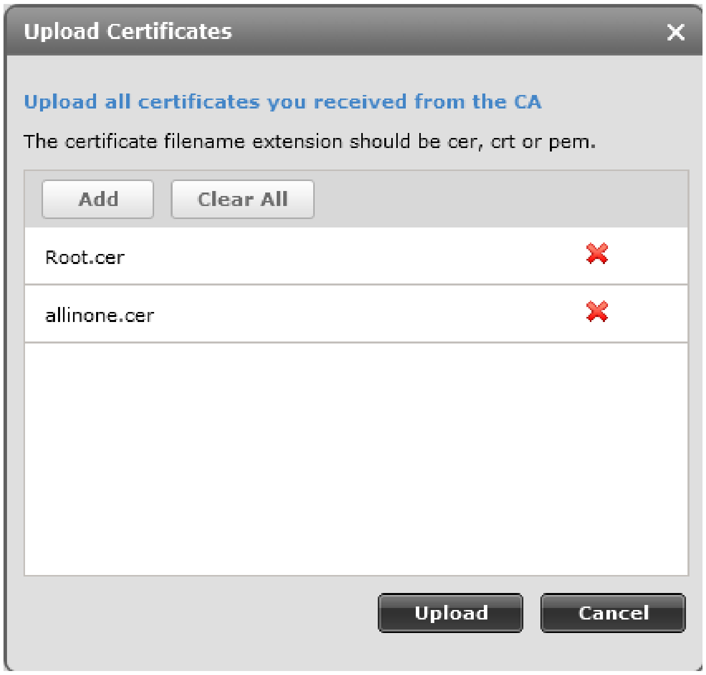
Figure 71: Generate CSR Dialog Box

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. Select **Upload** to upload the certificate to Equinox Management. Ensure that you upload both the CA root certificate (**Root.cer**) and the all-in-one certificate (**allinone.cer**).



Upload all certificates you received from the CA

The certificate filename extension should be cer, crt or pem.

Root.cer

allinone.cer

Figure 72: Upload Certificates Dialog Box

7. Select **Upload**.
8. Select **Apply All** to apply the certificate. The resulting dialog box prompts you to restart your machine.
9. Select **Yes** and wait 3–5 minutes for your machine to restart.

Related links

Securing Connections With Equinox Management on page 121

Installing the CA Certificate for Avaya Equinox Meetings for Web

About this task

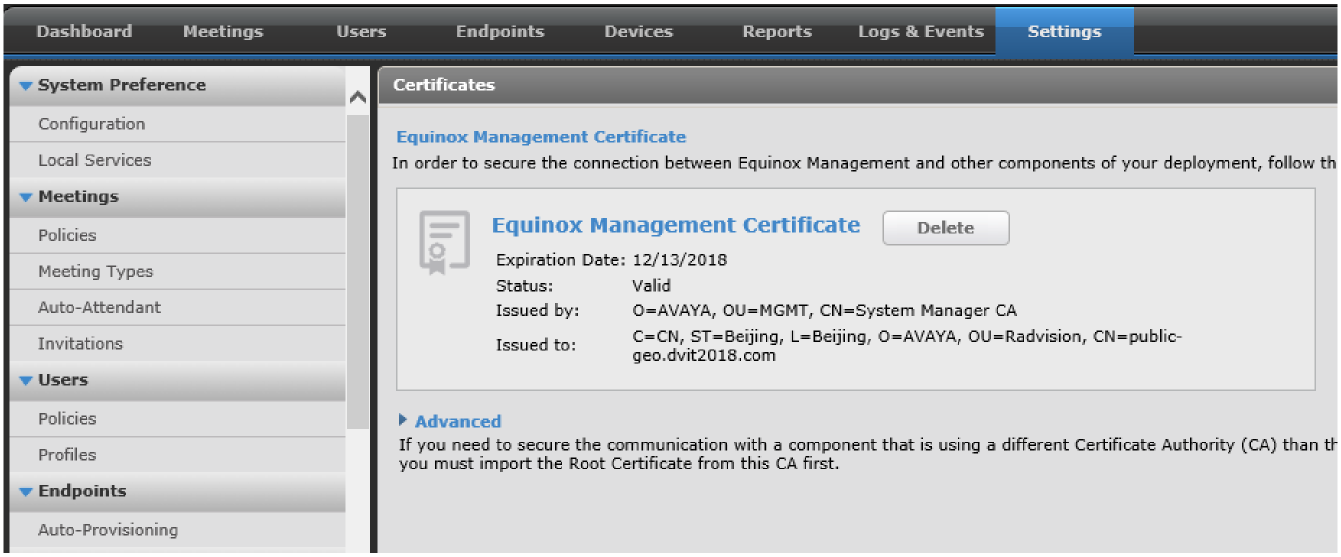
This task describes the procedure for configurations that must be done on the user's local PC during virtual deployment of Equinox Management. If you used the Avaya System Manager to sign the certificate created during configuration of the all-in-one Equinox Management server deployment (see Applying a Third-Party Certificate to the All-in-One Equinox Management Server on page 122) or if you used the internally signed certificate, you must install the root certificate on your client PC 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 85), 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 110).
- 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 **Certificates** page opens.



Equinox Management Certificate

In order to secure the connection between Equinox Management and other components of your deployment, follow th

Equinox Management Certificate

Expiration Date: 12/13/2018

Status: Valid

Issued by: O=AVAYA, OU=MGMT, CN=System Manager CA

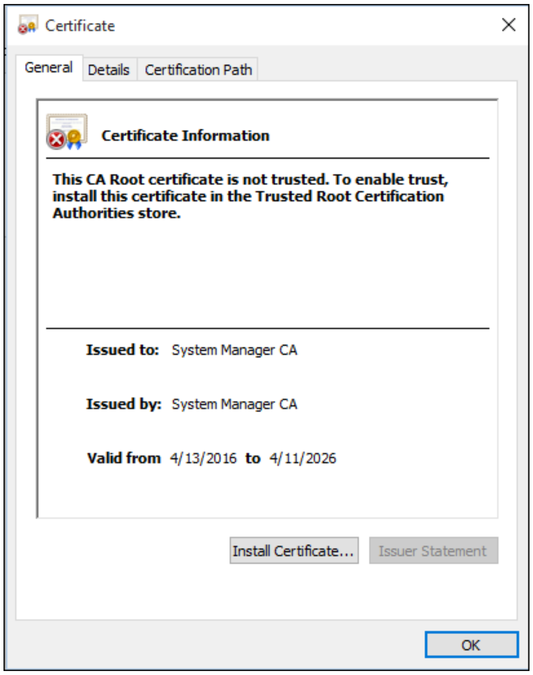
Issued to: C=CN, ST=Beijing, L=Beijing, O=AVAYA, OU=Radvision, CN=public-geo.dvit2018.com

If you need to secure the communication with a component that is using a different Certificate Authority (CA) than th you must import the Root Certificate from this CA first.

Figure 73: Certificates Page

3. Select the **Equinox Management Certificate** link, and select **Open**.

   The **Certificate** page appears.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: System Manager CA

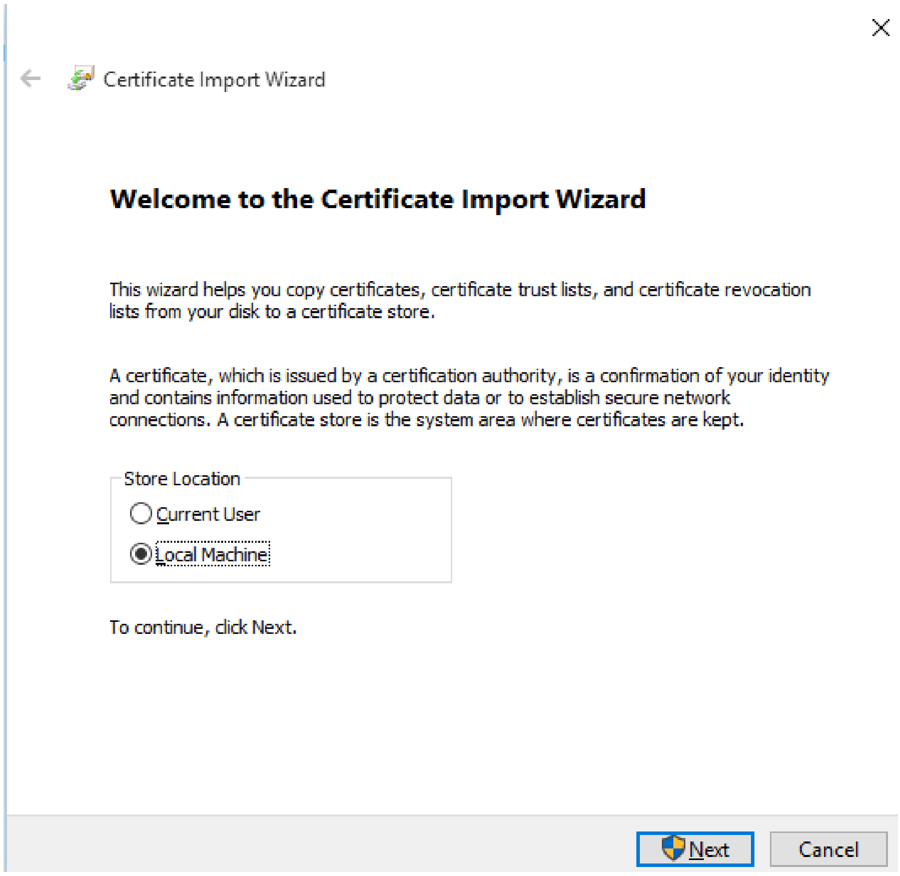
Issued by: System Manager CA

Valid from 4/13/2016 to 4/11/2026

Figure 74: Certificate Page

4. Select the **Install Certificate** button.

   The **Certificate Import Wizard** opens.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

○ Current User

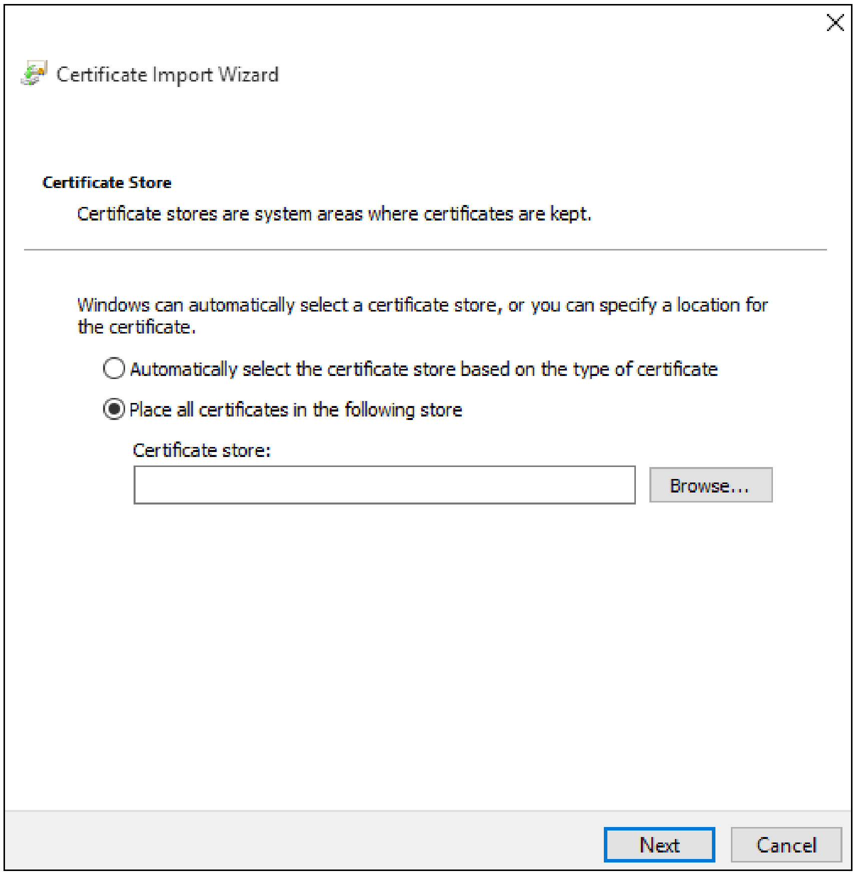
● Local Machine

To continue, click Next.

Figure 75: Certificate Import Wizard — Page 1

5. Select **Local Machine** and then select **Next**.

   The second page of the wizard opens.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

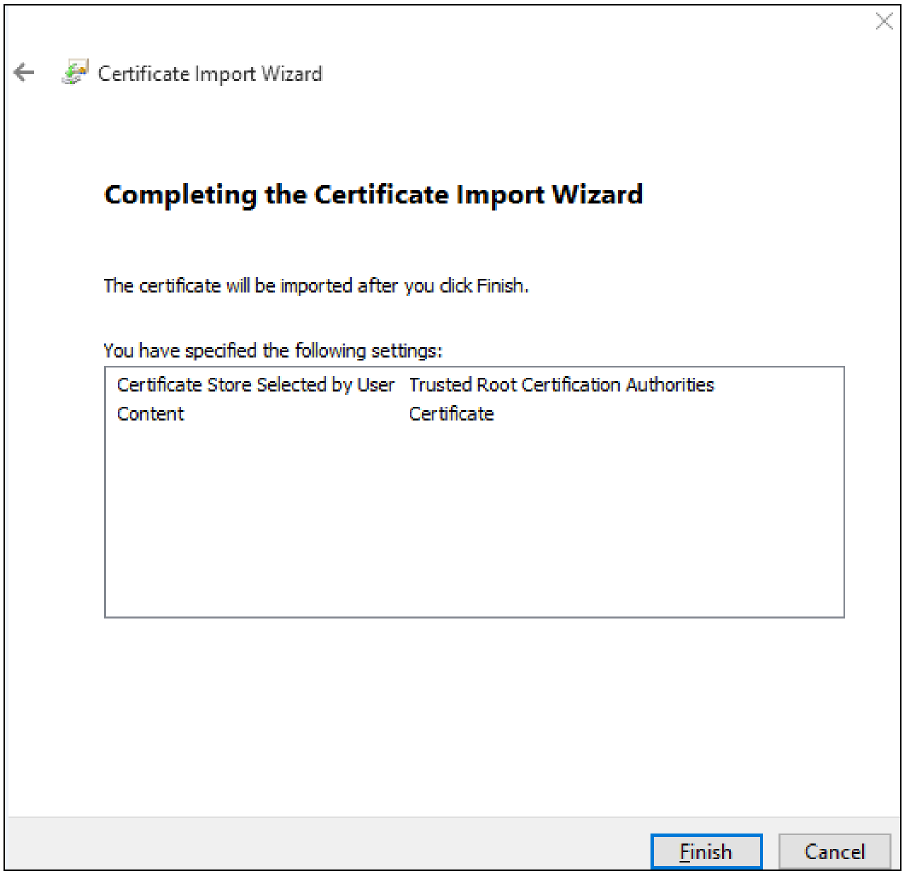
● Place all certificates in the following store

Certificate store:

Figure 76: Certificate Import Wizard — Page 2

6. Select **Place all certificates in the following store** and then select **Browse** to browse for a certificate store. Select **Trusted Root Certification Authorities**.
7. Select **Next**.

   The **Completing the Certificate Import Wizard** page opens.



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

Figure 77: Completing the Certificate Import Wizard Page

8. Verify that your information is correct, and select **Finish**.
9. Open a Chrome browser window and 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/`

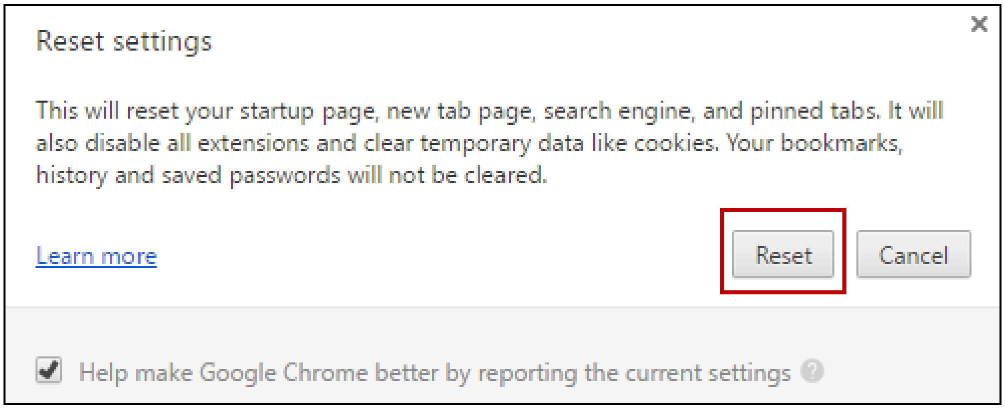
   ⚠ **Warning:**

   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.
10. Access the local Unified Portal URL (`https://<your local server FQDN>:8443/portal/tenants/default`).
11. Enter the **Virtual Room Number** in the relevant field and select **Join In Meeting** to join the meeting from your client.

    Note:

    To delete the Equinox Management certificate and re-create a Certificate Signing Request (CSR) to upload your new CA certificate after restarting Equinox Management, select **Reset Settings** in your Chrome browser window (select the **Customize** icon ⋮

and select **Settings** > **Advanced Settings** > **Reset Settings**, and select **Reset** in the **Reset Settings** dialog box).



Reset settings

This will reset your startup page, new tab page, search engine, and pinned tabs. It will also disable all extensions and clear temporary data like cookies. Your bookmarks, history and saved passwords will not be cleared.

×
Learn more
Reset
Cancel
☑ Help make Google Chrome better by reporting the current settings

Figure 78: Reset Settings Dialog Box

12. Restart the management server OVA, all media servers, and the gateway OVA.

Related links

Securing Connections With Equinox Management on page 121

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 122.

Procedure

1. Access the Equinox Management administrator portal.
2. Navigate to **Settings** > **Devices** > **User Portal / Web Gateway**. The **User Portal / Web Gateway Setting** page opens.
3. Configure the fields on the page, as described in the following table:

Table 15: User Portal / Web Gateway Setting Fields

Section	Field	Description
General	**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.
	Allow csa guest access	Select to enable a csa user to access Equinox Management as a guest.
	Enable uploading picture	Select to enable users to upload their picture into the system.
	Enable SSO	Select to enable automatic login to the Unified Portal after logging into Equinox Management.
	Client Ranking	Select the order in which Equinox Clients are chosen to host a meeting. The options are: • **Equinox Desktop Client, Equinox Mobile Client and Web Client** • **Equinox Desktop Client and Equinox Mobile Client** • **Scopia Desktop Client, Scopia Mobile Client and Web Client** • **Scopia Desktop Client and Scopia Mobile Client** ✱ **Note:** The **Equinox Mobile Client and Web Client** option is currently not supported.
	Equinox Management Web Access URL	Enter the URL to access Equinox Management on the web.
	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

Table continues…

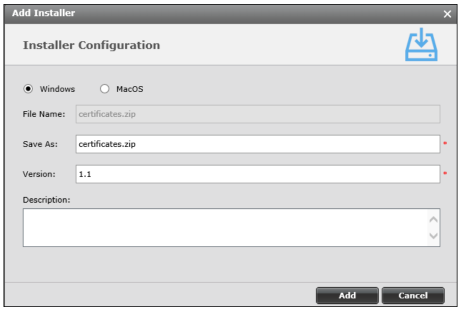
Section	Field	Description
		• Key Tab File
Avaya Equinox Client	**Use Microsoft Exchange Web Services (EWS)**	Select to enable Equinox Client to connect with the EWS.
	SSO with Equinox Client	Select to enable automatic login to EWS when logging into Equinox Client.
	Exchange Server Address	Enter the address of the exchange server.
	Exchange Server Domain	Enter the domain of the exchange server.
	Upload the Installer	Select this button to select an installer file to upload. The **Add Installer** dialog box appears, where you select the operating system, the name you wish to save the file as, the version, and (optionally) a description.  ● Windows ○ MacOS File Name: certificates.zip Save As: certificates.zip * Version: 1.1 * Description: **Figure 79: Add Installer Dialog Box**
Portal Setting	**Client Connection Frontend Scheme**	Select **https**
	Client Connection Frontend FQDN	Verify that the value is the same as that specified during OVA deployment.
	Client Connection Frontend Port	Enter **8443**
	Client Connection Frontend UPC Base URL	Enter the path for the Unified Portal, typically **/portal**
	Client Connection Frontend UPS Base URL	Enter the path for the Unified Portal server, typically **/ups**
	Client Connection Frontend SWC Base URL	Enter the path for the WebRTC client, typically **/uwd/dist**
	Client Connection Web Gateway Base URL	Enter the path for the Web Gateway, typically **/csa**
	Management Connection Frontend Scheme	Select **https**
	Management Connection Frontend FQDN	Enter the FQDN of the Web Gateway.
	Management Connection Frontend Port	Enter **8445** (or **8446** for cores).
	Management Connection API Base URL	Enter **/csaconfig/resources/settings**

Table continues…

Section	Field	Description
Web Gateway Setting	**Video Bandwidth (Kbps)**	Enter **1280**; the bandwidth value specified represents the maximum allowed by the Avaya Aura® Web Gateway. To disable video, enter **0**.
	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.
Advanced Settings	**Period to check for client updates (days)**	Enter the interval (in days) upon which the system checks for client updates.
	RTP Port Range	Enter the range of RTP ports. The default value is **5004–5203**
	BFCP UDP Port Range	Enter the range of PFCP UDP ports. The default value is **5204–5224**

4. 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.

Updating a User License

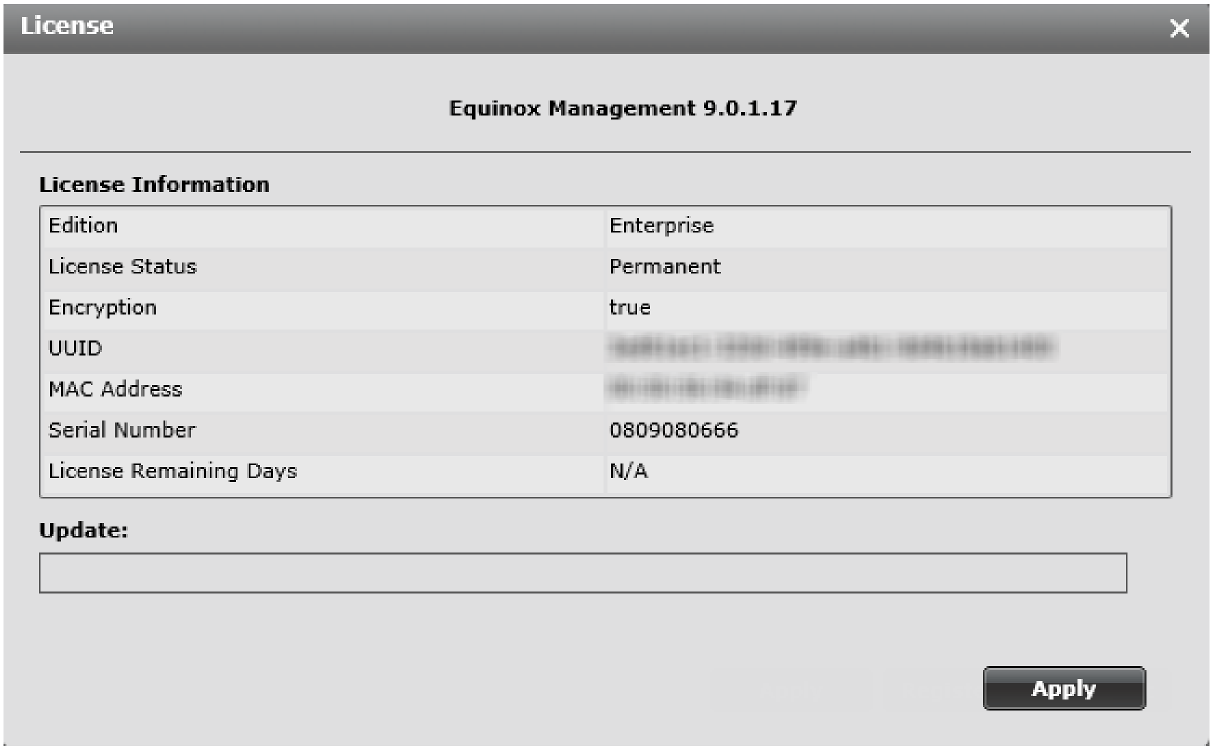
About this task

This task describes how to update user license information.

Procedure

1. In Avaya Equinox Management, select ≡ > **Licensing**.

    The **License Information** page appears.



License

Equinox Management 9.0.1.17

License Information

Edition	Enterprise
License Status	Permanent
Encryption	true
UUID	[redacted]
MAC Address	[redacted]
Serial Number	0809080666
License Remaining Days	N/A

Update:

Figure 80: License Information Page

An explanation of the fields on this page appears in Table 16: License Information Page on page 139.

Table 16: 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 (**true**) or non-encrypted (**false**).
UUID	Together with the **MAC Address**, used to generate the user based license.
MAC Address	Together with the **UUID**, used to generate the user based license.
Serial Number	The license'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. Select **Apply**.

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 Recording deployment* 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 select **Advanced Parameters**. The **Advanced Parameters** page opens.
2. In the **Unit Notify Level** section, modify the value to **100**, and select **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.

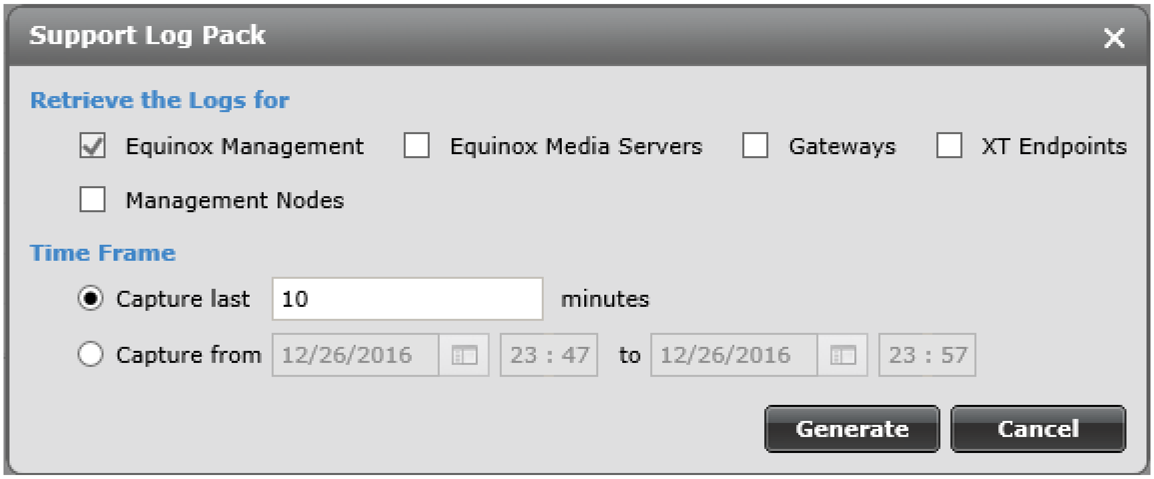
When a **Device is Not Available** message is generated for a Scopia MCU (5K or 6K) or for a UC-GW, the reason may be one of the following:

- 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, select the **Settings** icon and select **Support Log Pack**. The **Support Log Pack** dialog box opens.



Support Log Pack

Retrieve the Logs for

☑ Equinox Management □ Equinox Media Servers □ Gateways □ XT Endpoints

□ Management Nodes

Time Frame

● Capture last 10 minutes

○ Capture from 12/26/2016 23 : 47 to 12/26/2016 23 : 57

Figure 81: Support Log Pack Page

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. Select **Generate**.

Chapter 9: Equinox Management Deployment for Team Engagement (TE) 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 90	
2	Deploy the Equinox Management server	Deploying the Equinox Management Server on page 91 **Note:** The User Portal + Web Gateway component referenced in this topic is external to Equinox Management and is	

Table continues…

#	Action	Link/Notes	✔
		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 105	
4	Configure Equinox Management	Configuring the All-In-One Equinox Management Server on page 110 **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	Configuring the Distributed Equinox Management Server as an H.323 Gatekeeper on page 112	
6	Manage Licenses	Managing Licenses Via the Web-based License Manager (WebLM) on page 145	
7	Secure Connections	Securing Connections With Equinox Management on page 121	
8	Integrate Avaya Aura® Web Gateway and Equinox Management	Deploying the Avaya Aura Web Gateway on page 145	
9	Deploy and configure the Equinox Management environment	Deploying and Configuring the Equinox Management Environment on page 139	
10	Add Avaya Aura® users into Equinox Management	Integrating Avaya Aura Users Into Equinox Management Via System Manager on page 153	
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 161	
12	Configure Equinox Management to work with Avaya Aura®	Configuring Equinox Management for Interoperability with Avaya Aura on page 164	

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.

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 145

Installing the User License On the External WebLM Server on page 149

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 91.

Procedure

1. Log into your local WebLM server, using the following URL: `https://<Your Server IP>:9443/WebLM/LicenseServer`.

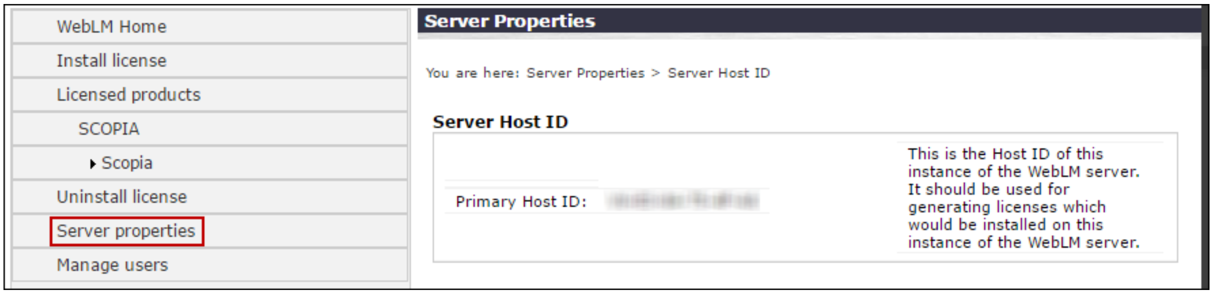
   The default login credentials are:

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

   After initial login, you are prompted to change your password.

2. On the local WebLM server UI, select **Server properties**.

   The **Server Properties** page appears, with the server's host ID which you use to get a license from the PLDS site.



You are here: Server Properties > Server Host ID

Server Host ID

Primary Host ID: [redacted]

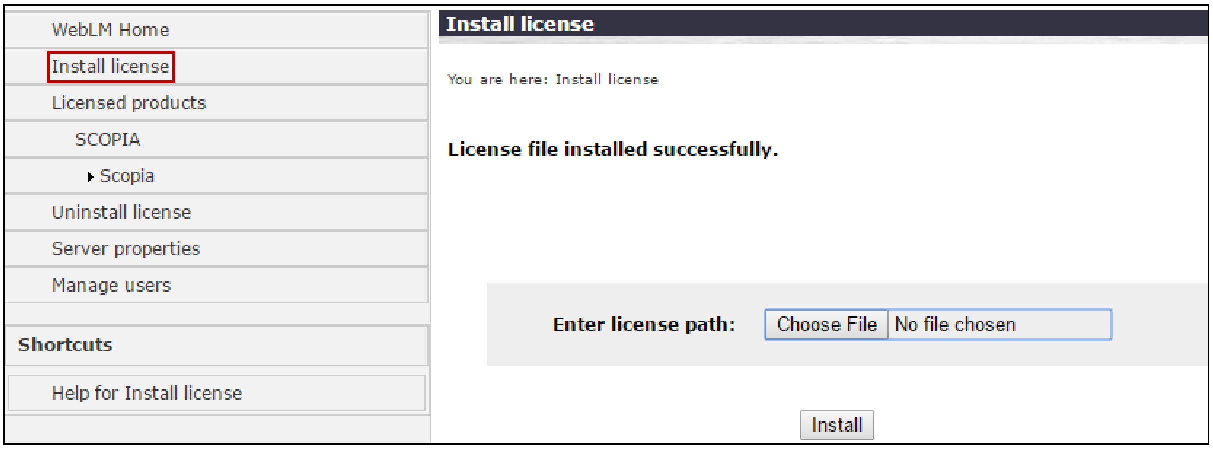
This is the Host ID of this instance of the WebLM server. It should be used for generating licenses which would be installed on this instance of the WebLM server.

Figure 82: 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. Select **Install license** on the WebLM server UI.

   The **Install License** page appears.



Install license

You are here: Install license

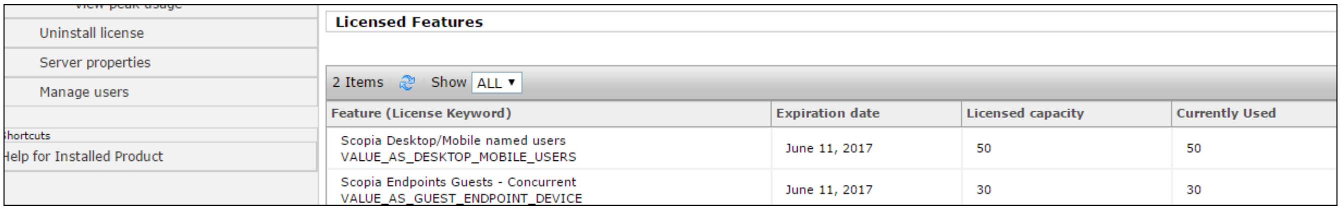
License file installed successfully.

Enter license path: No file chosen

Figure 83: Install License Page

5. Select **Choose File** in the **Enter license path** field, and after choosing your license file, select **Install** to install the license file.

   The **Licensed Features** page appears, where you verify the license status.



Licensed Features

2 Items

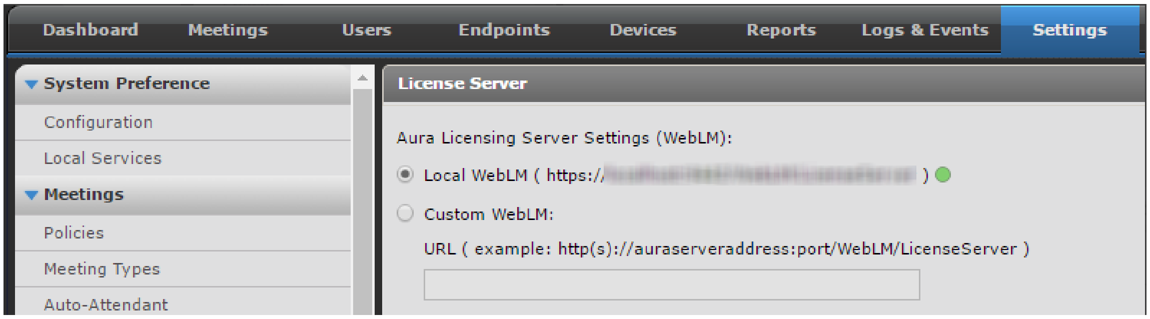
Feature (License Keyword)	Expiration date	Licensed capacity	Currently Used
Scopia Desktop/Mobile named users VALUE_AS_DESKTOP_MOBILE_USERS	June 11, 2017	50	50
Scopia Endpoints Guests - Concurrent VALUE_AS_GUEST_ENDPOINT_DEVICE	June 11, 2017	30	30

Figure 84: Licensed Features Page

6. Verify the license in Equinox Management, as follows:

   a. In the Equinox Management administrator portal, select **Settings** > **Servers** > **License Server**.

      The **License Server** page appears.



License Server

Aura Licensing Server Settings (WebLM):

● Local WebLM (https:/[redacted]) ●

○ Custom WebLM:

URL (example: http(s)://auraserveraddress:port/WebLM/LicenseServer)

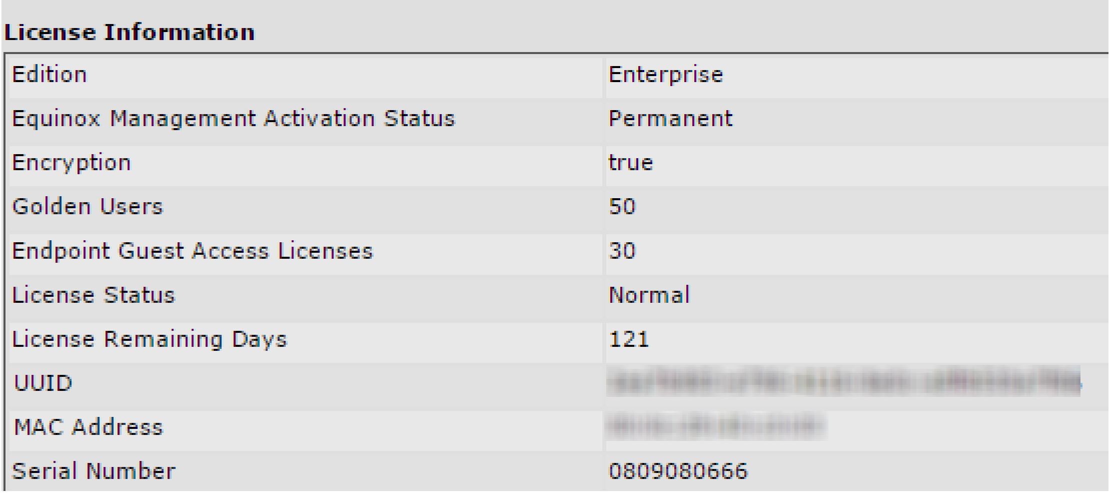
Figure 85: License Server Page

   b. Select **Apply**.

   c. Select ☰ > **Restart** to restart the Equinox Management server OVA.

      The local WebLM status displays with a green icon (active).

d. To verify license installation, select ☰ > **Licensing**. The **License Information** page appears, 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	[redacted]
MAC Address	[redacted]
Serial Number	0809080666

Figure 86: License Information Page

An explanation of the fields on this page appears in Table 17: License Information Page on page 148.

Table 17: 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**).
Golden Users	The number of users who have recording privileges. Golden users also have their own virtual meeting room.
Endpoint Guest Access Licenses	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.

Table continues…

Field Name	Description
	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	Together with the **MAC Address**, used to generate the user based license.
MAC Address	Together with the **UUID**, used to generate the user based license.
Serial Number	The license's serial number.

Related links

Managing Licenses Via the Web-based License Manager (WebLM) on page 145

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 91.

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:

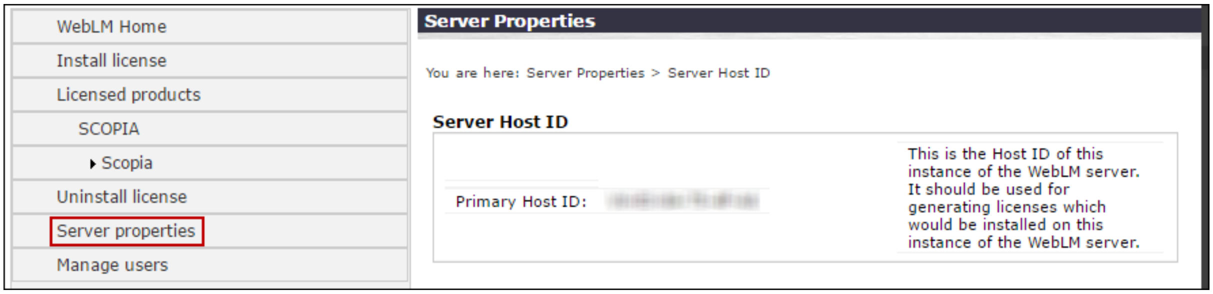
   - Username: **admin**

   - Password: **weblmadmin**

   After initial login, you are prompted to change your password.

3. On the WebLM server UI, select **Server properties**.

   The **Server Properties** page appears with the server's host ID, which you use to get a license from the PLDS site.



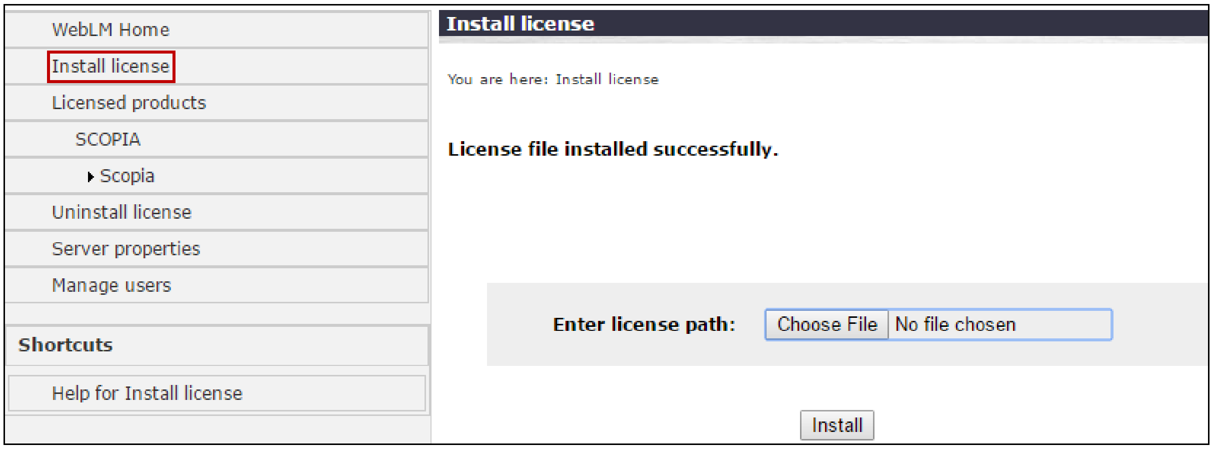
Primary Host ID: [redacted]

This is the Host ID of this instance of the WebLM server. It should be used for generating licenses which would be installed on this instance of the WebLM server.

Figure 87: 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. Select **Install license** on the WebLM server UI.

   The **Install License** page appears.

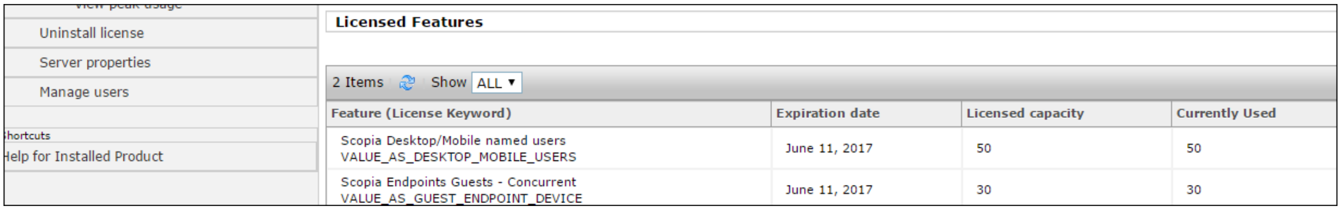


License file installed successfully.

Figure 88: Install License Page

6. Select **Choose File** in the **Enter license path** field, and after choosing your license file, select **Install** to install the license file.

   The **Licensed Features** page appears, where you verify the license status.



Feature (License Keyword)	Expiration date	Licensed capacity	Currently Used
Scopia Desktop/Mobile named users VALUE_AS_DESKTOP_MOBILE_USERS	June 11, 2017	50	50
Scopia Endpoints Guests - Concurrent VALUE_AS_GUEST_ENDPOINT_DEVICE	June 11, 2017	30	30

Figure 89: Licensed Features Page

7. In the Equinox Management administrator portal, select **Settings** > **Servers** > **License Server**, and select the **Apply** button.

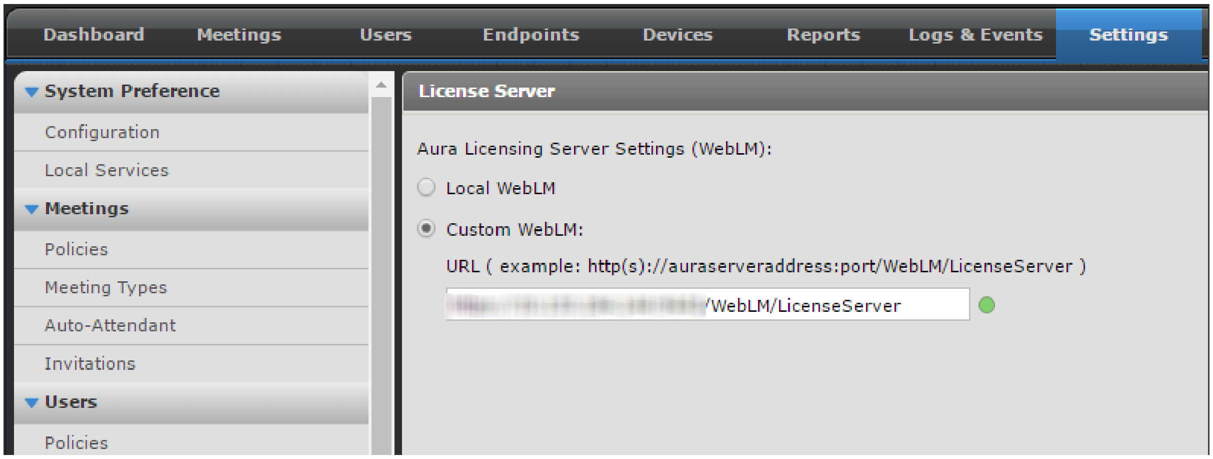
   The **License Server** page appears.

8. Select **Custom WebLM** and enter the URL of your external WebLM server.

   The remote WebLM server status displays next to the URL field with a red icon (inactive).

9. Select **Apply** to restart and activate the server.

   The remote WebLM server status displays with a green icon (active).



License Server

Aura Licensing Server Settings (WebLM):

○ Local WebLM

● Custom WebLM:

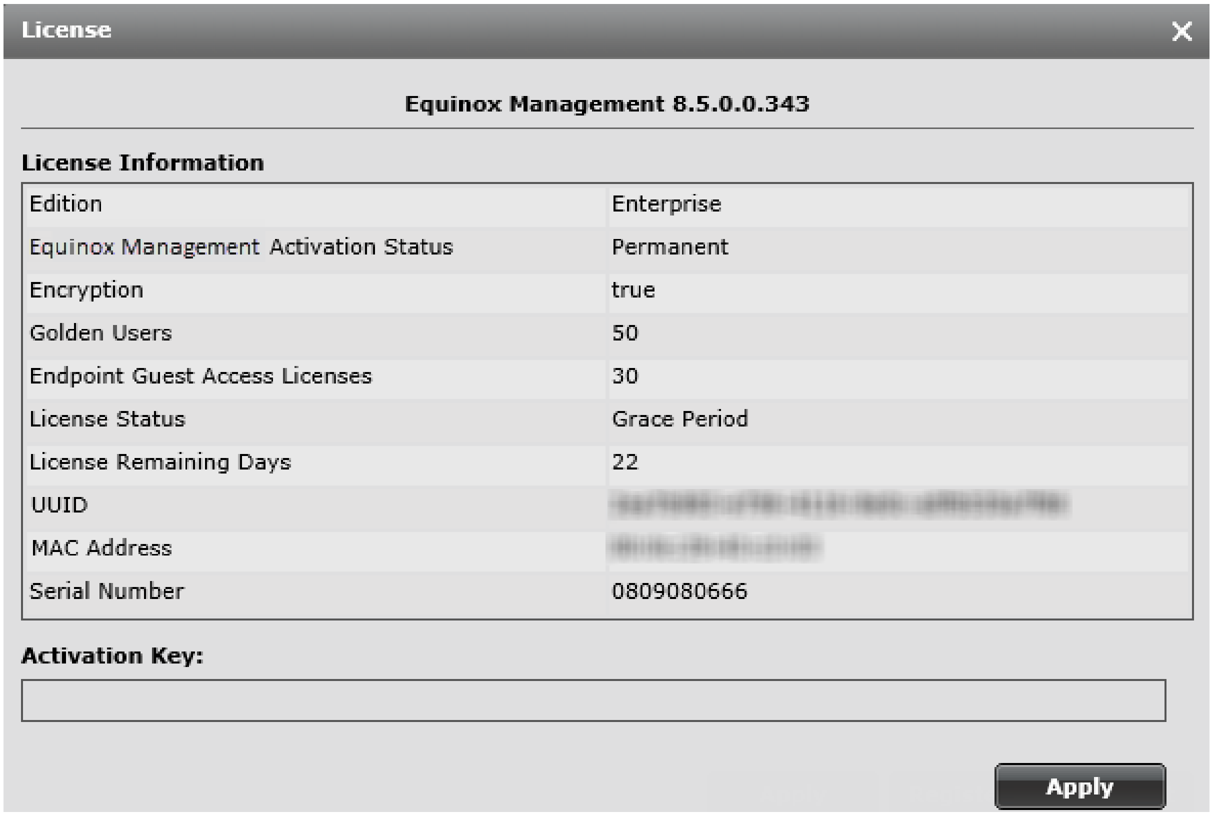
URL (example: http(s)://auraserveraddress:port/WebLM/LicenseServer)

[redacted]/WebLM/LicenseServer ●

Figure 90: License Server Page

10. Verify license installation by selecting ≡ > **License Information**.

    The **License Information** page appears, displaying information on the installed license.



Equinox Management 8.5.0.0.343

License Information

Edition	Enterprise
Equinox Management Activation Status	Permanent
Encryption	true
Golden Users	50
Endpoint Guest Access Licenses	30
License Status	Grace Period
License Remaining Days	22
UUID	[redacted]
MAC Address	[redacted]
Serial Number	0809080666

Activation Key:

Figure 91: License Information Page

An explanation of the fields on this page appears in Table 18: License Information Page on page 152.

Table 18: 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**).
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.

Table continues…

Field Name	Description
	When the license status is **Restricted**, the administrator must request a new license and apply it to the license server.
Golden Users	The number of users who have recording privileges. Golden users also have their own virtual meeting room.
Endpoint Guest Access Licenses	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	Together with the **MAC Address**, used to generate the user based license.
MAC Address	Together with the **UUID**, used to generate 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. Select **Apply** to apply the activation key.

Related links

Managing Licenses Via the Web-based License Manager (WebLM) on page 145

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 154
Configuring SSO for Equinox Conferencing on page 157
Adding Avaya Aura Users in Equinox Management on page 160

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.

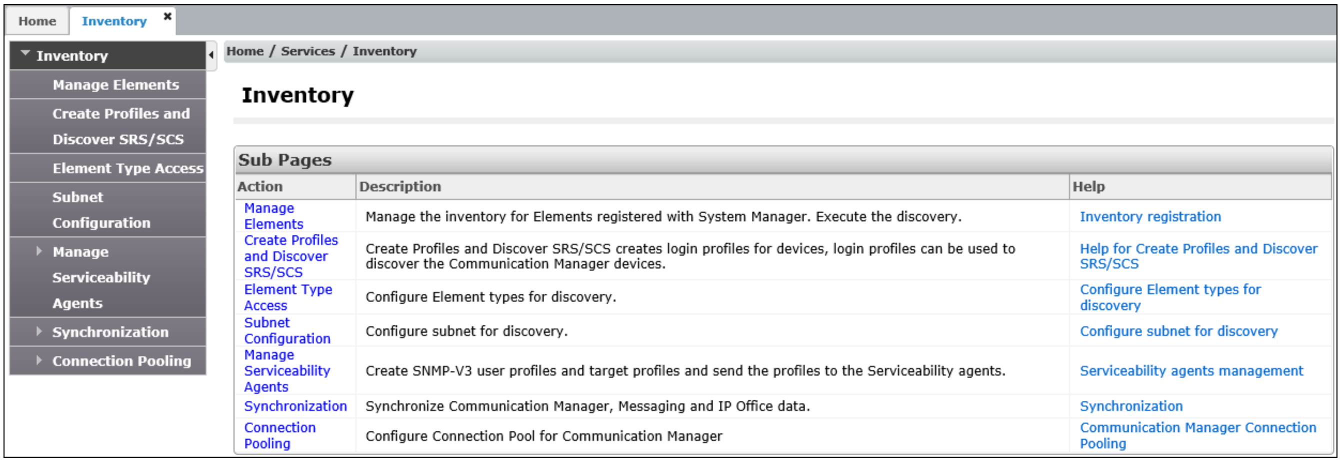
Note:

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.



Inventory

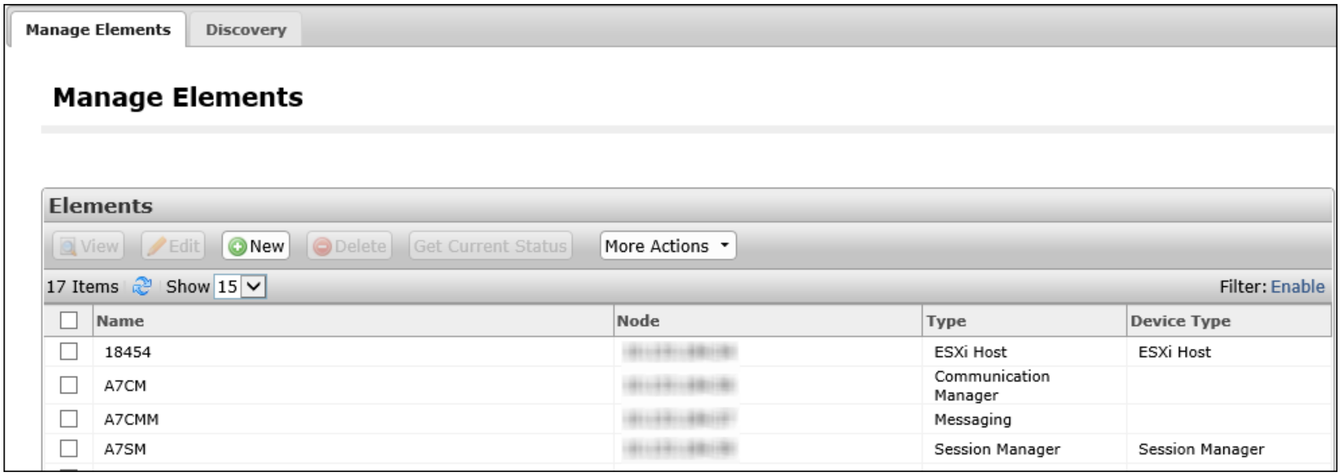
Sub Pages

Action	Description	Help
Manage Elements	Manage the inventory for Elements registered with System Manager. Execute the discovery.	Inventory registration
Create Profiles and Discover SRS/SCS	Create Profiles and Discover SRS/SCS creates login profiles for devices, login profiles can be used to discover the Communication Manager devices.	Help for Create Profiles and Discover SRS/SCS
Element Type Access	Configure Element types for discovery.	Configure Element types for discovery
Subnet Configuration	Configure subnet for discovery.	Configure subnet for discovery
Manage Serviceability Agents	Create SNMP-V3 user profiles and target profiles and send the profiles to the Serviceability agents.	Serviceability agents management
Synchronization	Synchronize Communication Manager, Messaging and IP Office data.	Synchronization
Connection Pooling	Configure Connection Pool for Communication Manager	Communication Manager Connection Pooling

Figure 92: System Manager — Inventory Page

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

   The **Manage Elements** page appears.



Manage Elements

Elements

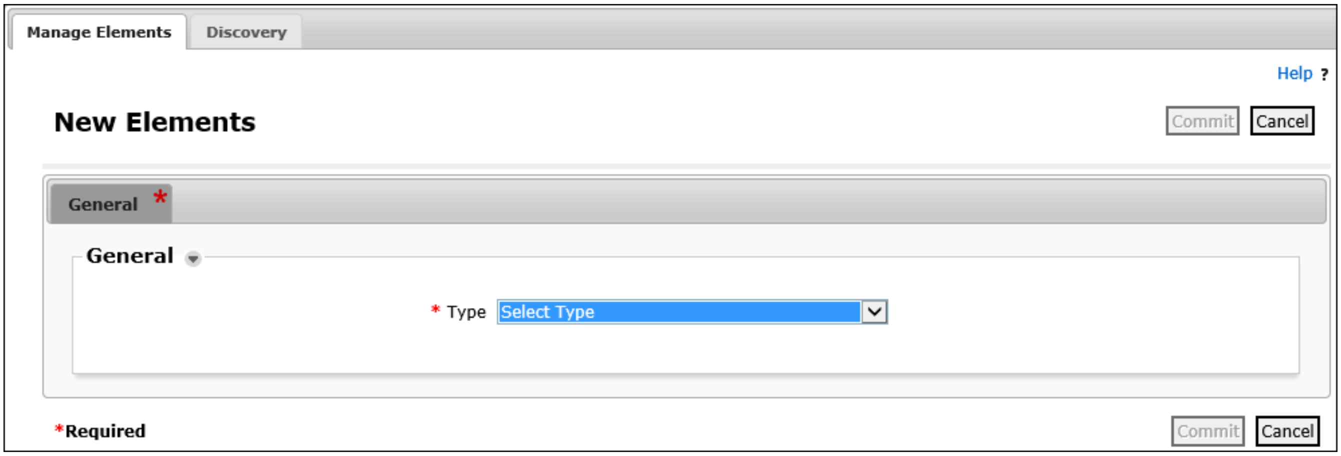
17 Items Show 15 Filter: Enable

□	Name	Node	Type	Device Type
□	18454	[redacted]	ESXi Host	ESXi Host
□	A7CM	[redacted]	Communication Manager	
□	A7CMM	[redacted]	Messaging	
□	A7SM	[redacted]	Session Manager	Session Manager

Figure 93: System Manager — Manage Elements Page

3. Select **New**.

   The **New Elements** page appears.



New Elements

General *

General

* Type Select Type

*Required

Figure 94: System Manager — New Elements Page

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

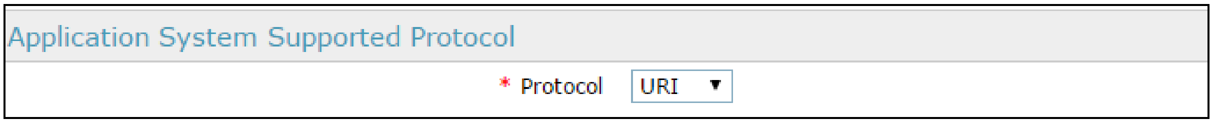
   The **New Equinox Conferencing** page appears.

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.



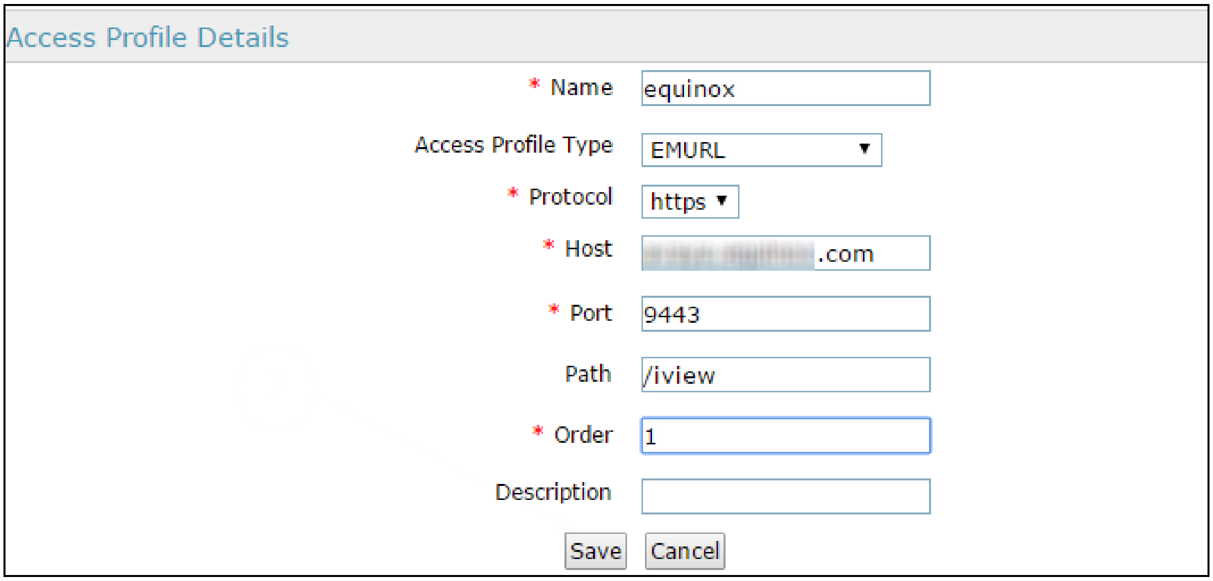
Application System Supported Protocol

* Protocol: URI

Figure 95: Application System Supported Protocol Section

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

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



Access Profile Details

* Name: equinox

Access Profile Type: EMURL

* Protocol: https

* Host: [redacted].com

* Port: 9443

Path: /iview

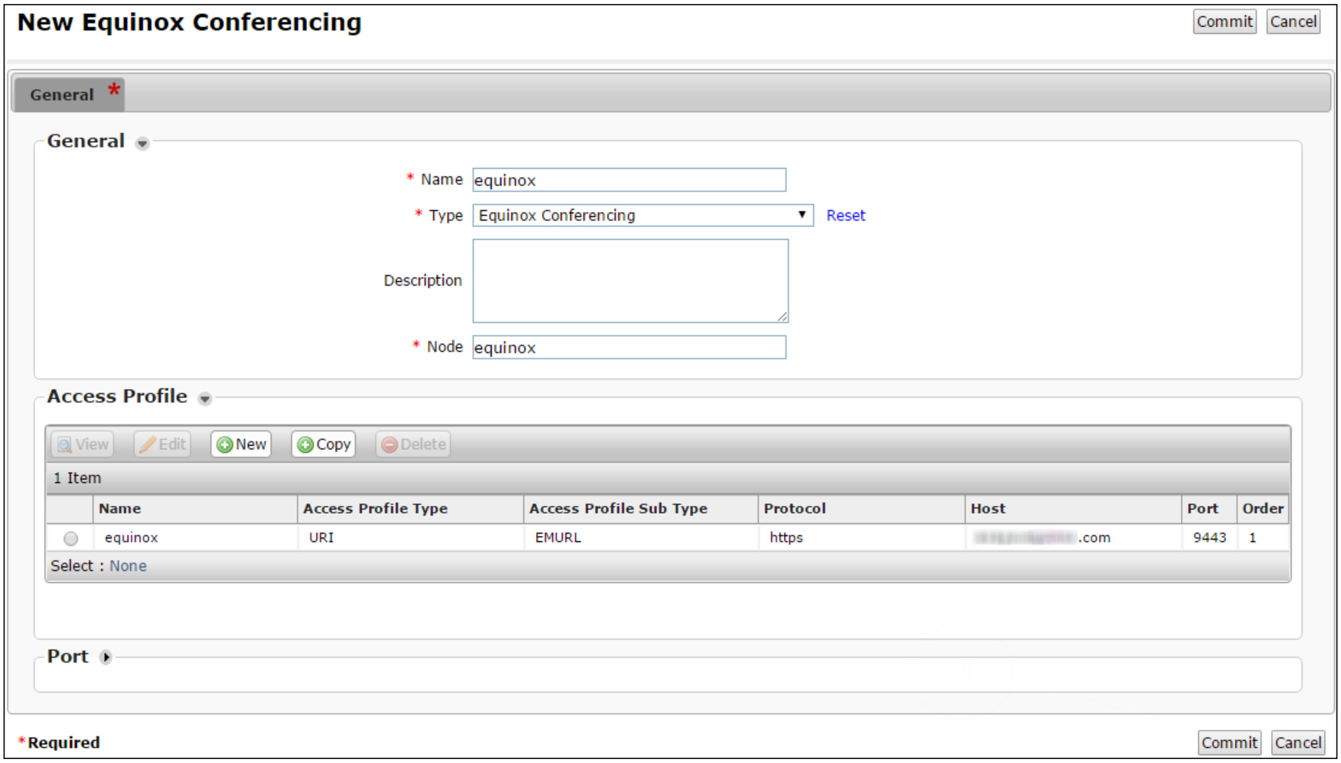
* Order: 1

Description:

Figure 96: 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.



General

* Name: equinox

* Type: Equinox Conferencing ▼ Reset

Description:

* Node: equinox

Access Profile

1 Item

	Name	Access Profile Type	Access Profile Sub Type	Protocol	Host	Port	Order
○	equinox	URI	EMURL	https	[redacted].com	9443	1

Select : None

Port

*Required

Figure 97: 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 157.

Related links

Integrating Avaya Aura Users Into Equinox Management Via System Manager on page 153

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 153
Downloading the System Manager CA Root Certificate on page 158
Exchanging CA Certificates Between System Manager and Avaya Equinox Management on page 158
Configuring SSO in Avaya Equinox Management on page 159

Downloading the System Manager CA Root Certificate

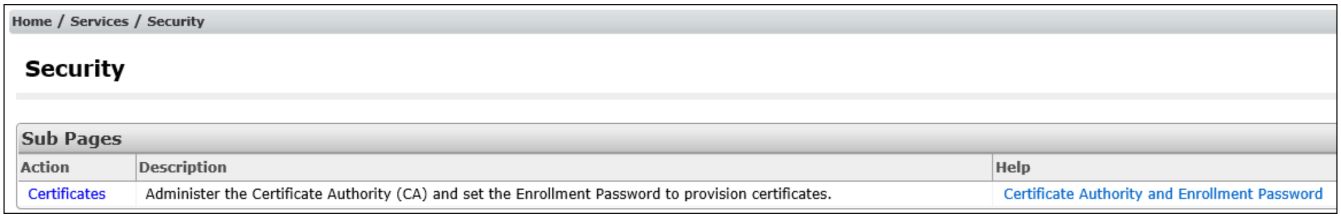
About this task

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.



Home / Services / Security

Security

Sub Pages

Action	Description	Help
Certificates	Administer the Certificate Authority (CA) and set the Enrollment Password to provision certificates.	Certificate Authority and Enrollment Password

Figure 98: 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 157

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 158.

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

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

   b. On the **Manage Elements** page, select the System Manager certificate and select **More Actions** > **Manage Trusted Certificates**.

   c. On the **Manage Trusted Certificates** page, select **Add**.

   d. On the **Add Trusted Certificates** page, select **Import as PEM Certificate**.

   e. Copy the content of the Avaya Equinox Management CA certificate and paste it in the field on the **Add Trusted Certificates** page.

   f. Select **Commit**.

Related links

Configuring SSO for Equinox Conferencing on page 157

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 158.

Procedure

1. Navigate to `/opt/Avaya/iview/tomcat/webapps/iview/WEB-INF/classes/sso_config/securityServerConfig.properties`, and edit the file properties, as follows:

```
openssoclient.config.folder=../config
com.iplanet.am.cookie.name=<FQDN of your System Manager>
security.server.fqdn=<FQDN of your System Manager>
```

2. Navigate to`/opt/Avaya/iview/tomcat/config/vcs-core.properties`, and add the `vnex.auth.smgr.sso=true` property.

3. Before restarting Tomcat, navigate to `/opt/Avaya/iview/tomcat/config/` and delete the `OpenSSOClient` directory.

4. To restart Tomcat, do one of the following:

   - On the shell, run the `service avaya.iview restart` command.
   - On the Avaya Equinox Management UI, select ☰ > **Restart**.

Related links

Configuring SSO for Equinox Conferencing on page 157

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 157.

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 153

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 Recording deployment* 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:

```
http://<FQDN_of_SystemManager>
```

Related links

Adding a SIP Entity for the Equinox B2BUA Component on page 161
Adding a SIP Entity Link/SIP Trunk For the Equinox B2BUA Component on page 162
Adding Routing Policies For the Equinox B2BUA Component on page 163
Adding Dial Patterns for the Equinox B2BUA Component on page 163

Adding a SIP Entity for the Equinox B2BUA Component

Before you begin

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

```
http://<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 19: 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 161

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:

```
http://<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 20: 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 **TCP**
Port	Enter **5060**
SIP Entity 2	Select the Equinox B2BUA component.
Port	Enter **5060**

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 161

Adding Routing Policies For the Equinox B2BUA Component

Before you begin

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

```
http://<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 161

Adding Dial Patterns for the Equinox B2BUA Component

Before you begin

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

```
http://<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 21: Dial Pattern Field Descriptions

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

Table continues…

Field Name	Description
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 161

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:

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

Note:

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

Related links

Adding a SIP Trunk from the Equinox B2BUA Component to Session Manager on page 164
Changing the Default SIP Domain in Equinox Management on page 165

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:

```
http://<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 164

Adding a SIP Trunk in Equinox Management on page 165

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 22: 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 **5060**
Transport Type	Enter **TCP**
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 164

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 the Settings icon ☰ on the top right side of the page, and select **Advanced Parameters**. The **Advanced Parameters** dialog box appears.
3. Enter values for the displayed fields, as indicated in the following table:

Table 23: Advanced Parameters Field Descriptions

Field Name	Value
Property Name	`vnex.vcms.core.conference.defaultDomain`
Property Value	`<SIP domain administered in Avaya Aura`®

4. Select **Apply**. You can verify the new SIP domain by typing `defaultDomain` in the **Search** field.

Related links

Configuring Equinox Management for Interoperability with Avaya Aura on page 164

Chapter 10: Migrating from Avaya Aura to Avaya Equinox

Introduction to migrating AAC8 data

This section is intended for Avaya Aura Conferencing 8.0 (AAC8) customers who need to migrate their deployment data to OTT or TE Equinox Solutions .

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 has these 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 VRM, AAC8 and user already have one VRM, 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 will be applied to determine location

For migration to non-Aura Equinox data is migrated directly from AAC8 to Equinox Management.

For migration to Aura Equinox, data is also migrated directly from AAC8 to Equinox Management for Release 9.0. In future releases, data will be migrated through Aura System Manager (SMGR). The tool generates XML files for the SMGR bulk import tool so all required data are imported to SMGR, and SMGR pushes all required data to Equinox Management. The current version of Equinox SMGR 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 SMGR user profile will not have the Equinox profile checkbox set and the administrator should be aware of this. When the Equinox SMGR EP bulk import tool is ready, those XML files can be used with the **Merge** option so the Equinox profile will be populated on SMGR as well.

Migration of user base profiles

The migration tool imports existing user fields from AAC User Base Profiles, creates users on Avaya 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
Enable Video	Whether video is enabled	User - Default Meeting Type Virtual Room - Meeting Type ✱ **Note:** Check Equinox Management default meeting type. The administrator should select the

Table continues…

Data field name in AAC	Description	Mapping in Equinox Management
		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, so if the Moderator Passcode is empty for user, then her/his moderator access code will be used. The list of such users will be shown in 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 8.0

About this task

Use the following procedure to export your existing data from Avaya Aura® Conferencing 8.0 (AAC8).

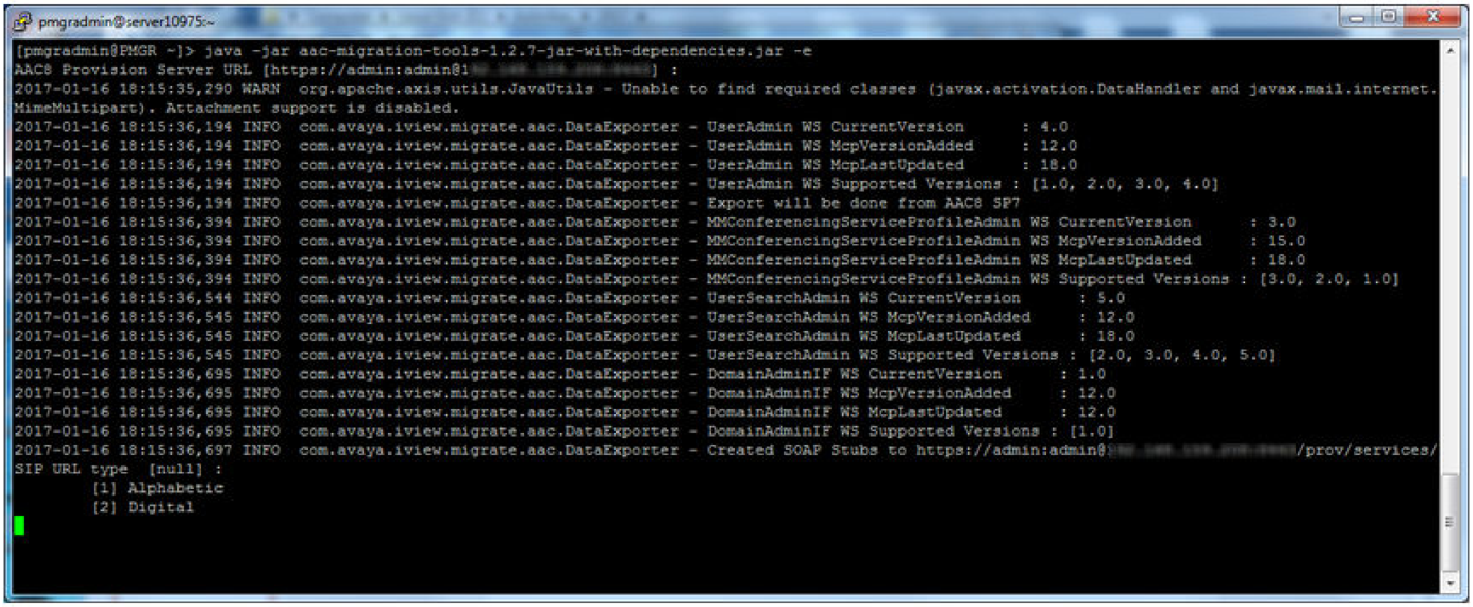
Before you begin

- Contact Customer Support for information on downloading the latest version of the migration tool. Chat with live agents to get answers to questions, or request an agent to connect you to a support team for additional expertise.
- Make sure you have your administrator credentials ready.

Procedure

1. Run:

   ```
   java -jar aac-migration-tools-1.2.7-jar-with-dependencies.jar -e
   ```



```
[pmgradmin@PMGR ~]> java -jar aac-migration-tools-1.2.7-jar-with-dependencies.jar -e
AAC8 Provision Server URL [https://admin:admin@1[redacted]] :
2017-01-16 18:15:35,290 WARN  org.apache.axis.utils.JavaUtils - Unable to find required classes (javax.activation.DataHandler and javax.mail.internet.
MimeMultipart). Attachment support is disabled.
2017-01-16 18:15:36,194 INFO  com.avaya.iview.migrate.aac.DataExporter - UserAdmin WS CurrentVersion      : 4.0
2017-01-16 18:15:36,194 INFO  com.avaya.iview.migrate.aac.DataExporter - UserAdmin WS McpVersionAdded     : 12.0
2017-01-16 18:15:36,194 INFO  com.avaya.iview.migrate.aac.DataExporter - UserAdmin WS McpLastUpdated      : 18.0
2017-01-16 18:15:36,194 INFO  com.avaya.iview.migrate.aac.DataExporter - UserAdmin WS Supported Versions : [1.0, 2.0, 3.0, 4.0]
2017-01-16 18:15:36,194 INFO  com.avaya.iview.migrate.aac.DataExporter - Export will be done from AAC8 SP7
2017-01-16 18:15:36,394 INFO  com.avaya.iview.migrate.aac.DataExporter - MMConferencingServiceProfileAdmin WS CurrentVersion      : 3.0
2017-01-16 18:15:36,394 INFO  com.avaya.iview.migrate.aac.DataExporter - MMConferencingServiceProfileAdmin WS McpVersionAdded     : 15.0
2017-01-16 18:15:36,394 INFO  com.avaya.iview.migrate.aac.DataExporter - MMConferencingServiceProfileAdmin WS McpLastUpdated      : 18.0
2017-01-16 18:15:36,394 INFO  com.avaya.iview.migrate.aac.DataExporter - MMConferencingServiceProfileAdmin WS Supported Versions : [3.0, 2.0, 1.0]
2017-01-16 18:15:36,544 INFO  com.avaya.iview.migrate.aac.DataExporter - UserSearchAdmin WS CurrentVersion      : 5.0
2017-01-16 18:15:36,545 INFO  com.avaya.iview.migrate.aac.DataExporter - UserSearchAdmin WS McpVersionAdded     : 12.0
2017-01-16 18:15:36,545 INFO  com.avaya.iview.migrate.aac.DataExporter - UserSearchAdmin WS McpLastUpdated      : 18.0
2017-01-16 18:15:36,545 INFO  com.avaya.iview.migrate.aac.DataExporter - UserSearchAdmin WS Supported Versions : [2.0, 3.0, 4.0, 5.0]
2017-01-16 18:15:36,695 INFO  com.avaya.iview.migrate.aac.DataExporter - DomainAdminIF WS CurrentVersion      : 1.0
2017-01-16 18:15:36,695 INFO  com.avaya.iview.migrate.aac.DataExporter - DomainAdminIF WS McpVersionAdded     : 12.0
2017-01-16 18:15:36,695 INFO  com.avaya.iview.migrate.aac.DataExporter - DomainAdminIF WS McpLastUpdated      : 12.0
2017-01-16 18:15:36,695 INFO  com.avaya.iview.migrate.aac.DataExporter - DomainAdminIF WS Supported Versions : [1.0]
2017-01-16 18:15:36,697 INFO  com.avaya.iview.migrate.aac.DataExporter - Created SOAP Stubs to https://admin:admin@[redacted]/prov/services/
SIP URL type  [null] :
        [1] Alphabetic
        [2] Digital
```

Figure 99: Data exporting procedure

2. 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.

3. Enter the SIP URL type to be added 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.

4. Select `Y` to start exporting.

   The tool exports data from AAC8 and saves it in the AAC8Data.ser file.

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

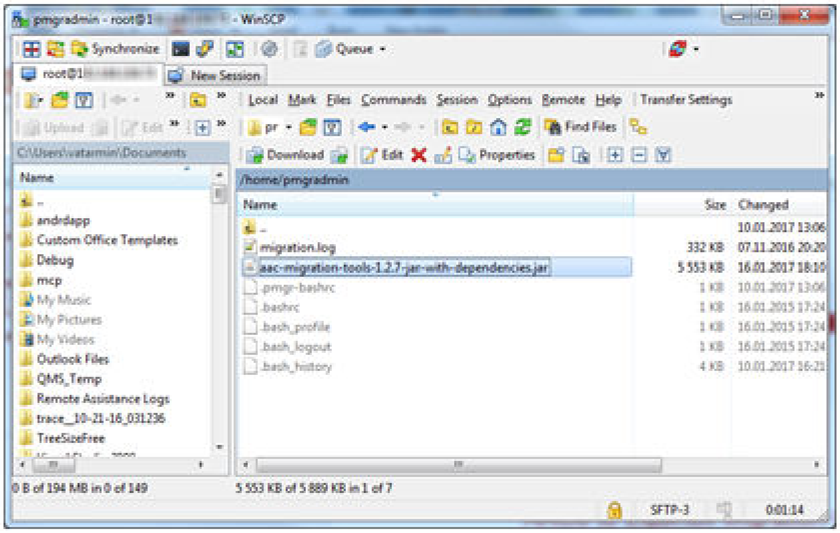
- Make sure you exported AAC8 data.
- (Optional. Only for multi-tenancy) Equinox Management has multi-tenant and enterprise versions. Multi-tenancy means there are multiple different members and organizations, each one with its member ID. AAC is enterprise only. Make sure you have your member ID as you 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-1.2.7-jar-with-dependencies.jar and AAC8Data.ser to Equinox Management as root.



Name
..
andrdapp
Custom Office Templates
Debug
mcp
My Music
My Pictures
My Videos
Outlook Files
QMS_Temp
Remote Assistance Logs
trace_10-21-16_031236
TreeSizeFree

0 B of 194 MB in 0 of 149

Name	Size	Changed
..		10.01.2017 13:06
migration.log	332 KB	07.11.2016 20:20
aac-migration-tools-1.2.7-jar-with-dependencies.jar	5 553 KB	16.01.2017 18:10
.pmgr-bashrc	1 KB	10.01.2017 13:06
.bashrc	1 KB	16.01.2015 17:24
.bash_profile	1 KB	16.01.2015 17:24
.bash_logout	1 KB	16.01.2015 17:24
.bash_history	4 KB	10.01.2017 16:21

5 553 KB of 5 889 KB in 1 of 7

Figure 100: Uploading the migration tool

2. Execute `java -jar aac-migration-tools-1.2.7-jar-with-dependencies.jar -i`

3. Select your deployment type.

   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 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.
`[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 System Manager (SMGR) 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 theEquinox 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 will be 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 will be 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.

13. Enter the relevant user password 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 password is stored on the LDAP server. For Local users, the password will be reset to default after migration. You cannot get the user's plain password from AAC8.

You will be prompted whether to use the participant code, or passcode, or telephone number as a password.

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 user password 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 participant code will be used.

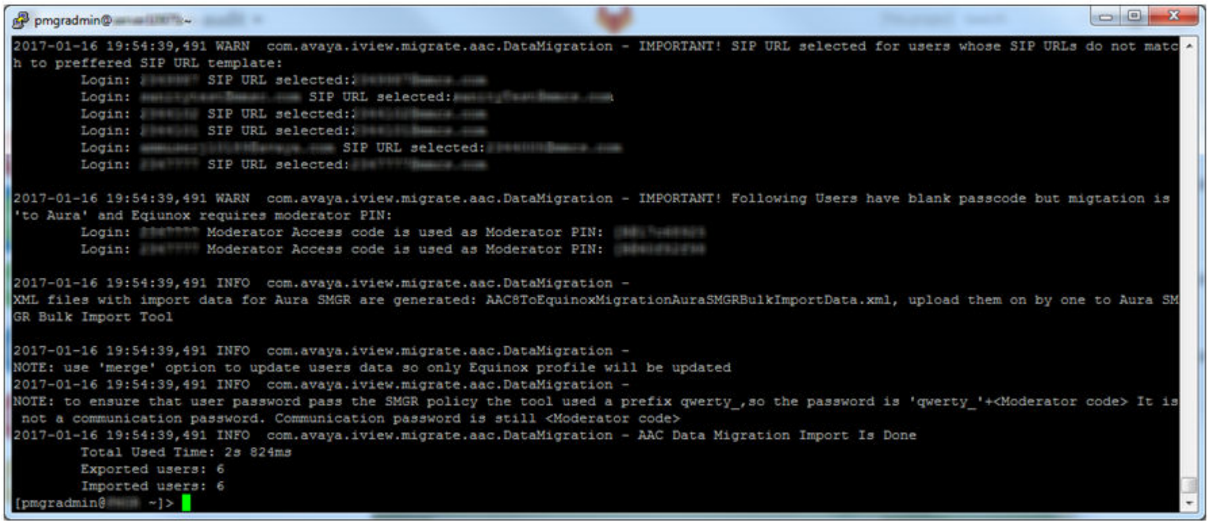
15. (Only if the migration tool runs on Equinox Management) Enter `Y` to have the system retrieve the prefix of the Virtual Room number automatically from the Equinox Management configuration file; otherwise, enter `N` and then enter the prefix manually.

    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, this message typically appears on the display.

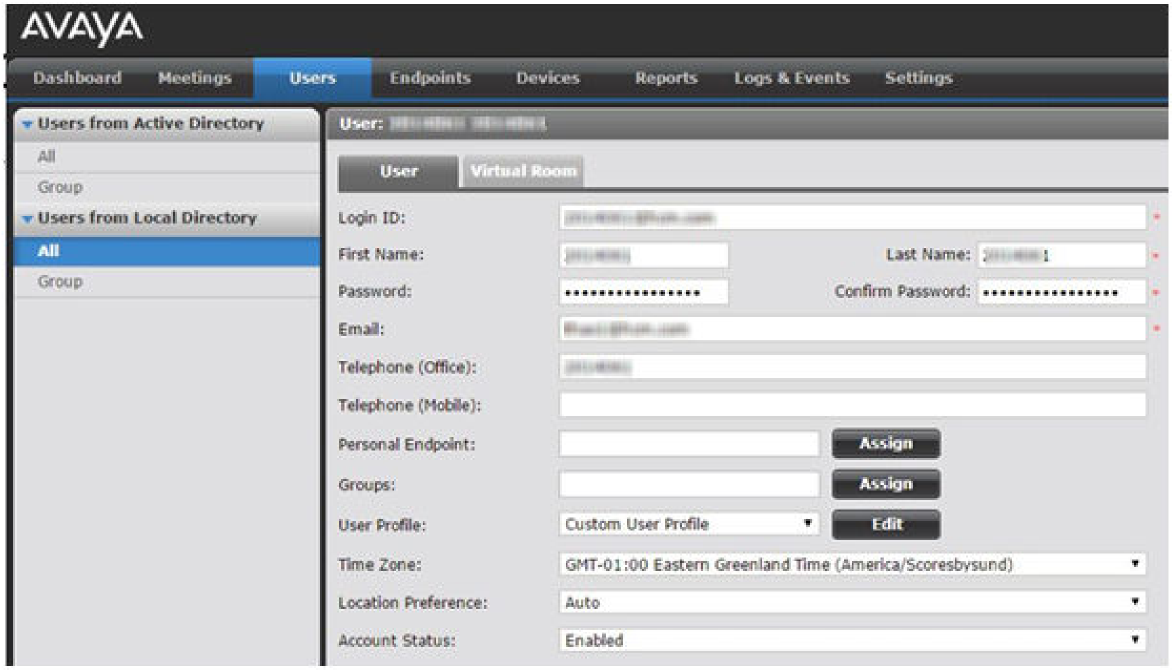


```
2017-01-16 19:54:39,491 WARN  com.avaya.iview.migrate.aac.DataMigration - IMPORTANT! SIP URL selected for users whose SIP URLs do not matc
h to preffered SIP URL template:
        Login: [redacted] SIP URL selected:[redacted]
        Login: [redacted] SIP URL selected:[redacted]
        Login: [redacted] SIP URL selected:[redacted]
        Login: [redacted] SIP URL selected:[redacted]
        Login: [redacted] SIP URL selected:[redacted]
        Login: [redacted] SIP URL selected:[redacted]

2017-01-16 19:54:39,491 WARN  com.avaya.iview.migrate.aac.DataMigration - IMPORTANT! Following Users have blank passcode but migtation is
'to Aura' and Eqiunox requires moderator PIN:
        Login: [redacted] Moderator Access code is used as Moderator PIN: [redacted]
        Login: [redacted] Moderator Access code is used as Moderator PIN: [redacted]

2017-01-16 19:54:39,491 INFO  com.avaya.iview.migrate.aac.DataMigration -
XML files with import data for Aura SMGR are generated: AAC8ToEquinoxMigrationAuraSMGRBulkImportData.xml, upload them on by one to Aura SM
GR Bulk Import Tool

2017-01-16 19:54:39,491 INFO  com.avaya.iview.migrate.aac.DataMigration -
NOTE: use 'merge' option to update users data so only Equinox profile will be updated
2017-01-16 19:54:39,491 INFO  com.avaya.iview.migrate.aac.DataMigration -
NOTE: to ensure that user password pass the SMGR policy the tool used a prefix qwerty_,so the password is 'qwerty_'+<Moderator code> It is
 not a communication password. Communication password is still <Moderator code>
2017-01-16 19:54:39,491 INFO  com.avaya.iview.migrate.aac.DataMigration - AAC Data Migration Import Is Done
        Total Used Time: 2s 824ms
        Exported users: 6
        Imported users: 6
[pmgradmin@[redacted] ~]>
```

Figure 101: Typical migration completed message

- Warnings are printed like failed users, no SIP URL matches selected template, email is blank, or passcode encrypted.
- Summary is printed 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 following was migrated from AAC8 and created in the Equinox Management database:
    - Local user basic data and their virtual rooms



User: [redacted]

Login ID: [redacted]

First Name: [redacted] Last Name: [redacted]

Password: •••••••••••••••• Confirm Password: ••••••••••••••••

Email: [redacted]

Telephone (Office): [redacted]

Telephone (Mobile):

Personal Endpoint:

Groups:

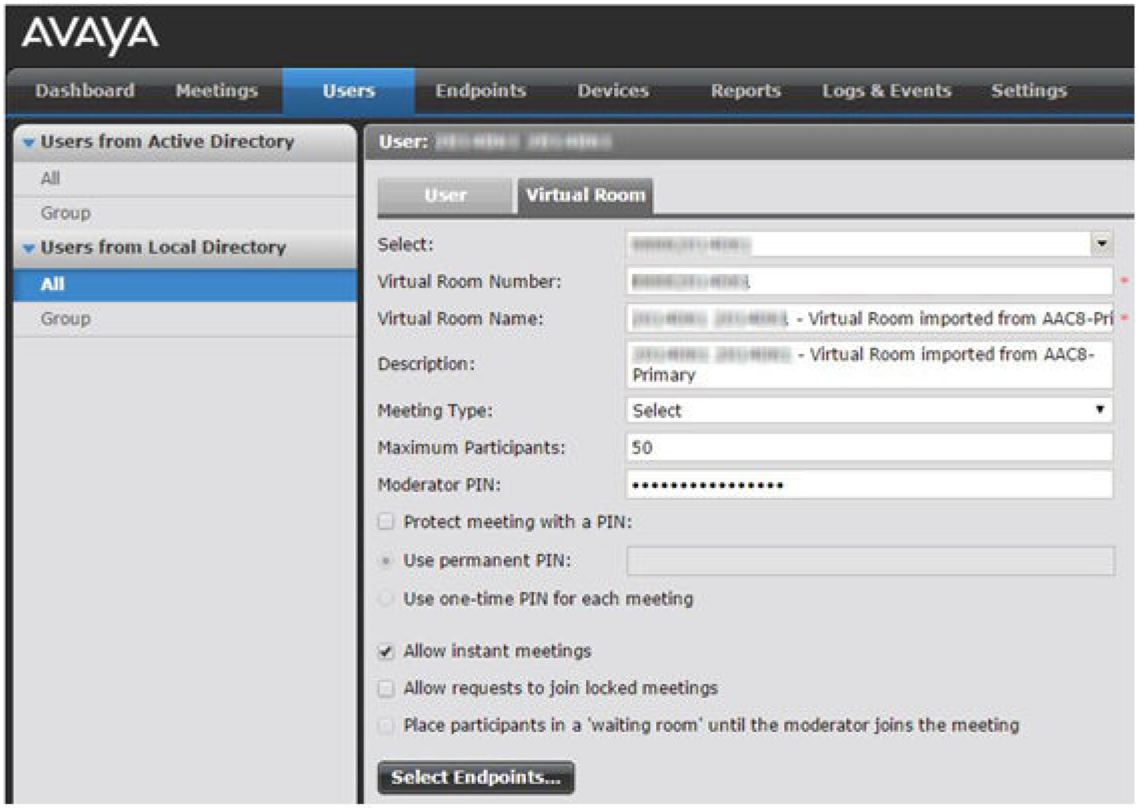
User Profile: Custom User Profile

Time Zone: GMT-01:00 Eastern Greenland Time (America/Scoresbysund)

Location Preference: Auto

Account Status: Enabled

Figure 102: Example of user basic data in Equinox Management after migration



User: [redacted]

Select: [redacted]

Virtual Room Number: [redacted]

Virtual Room Name: [redacted] - Virtual Room imported from AAC8-Pri

Description: [redacted] - Virtual Room imported from AAC8-Primary

Meeting Type: Select

Maximum Participants: 50

Moderator PIN: ••••••••••••••••

□ Protect meeting with a PIN:

● Use permanent PIN:

○ Use one-time PIN for each meeting

☑ Allow instant meetings

□ Allow requests to join locked meetings

□ Place participants in a 'waiting room' until the moderator joins the meeting

Figure 103: User's virtual room in Equinox Management after migration

Chapter 11: Equinox Media Server deployment

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 • WebRTC gateway
Web collaboration server	Web collaboration

Equinox Media Server processes all media on the server CPU and does not need media accelerator blades. 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.

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. Equinox Media Server is required in the Over The Top and Team Engagement deployments of Avaya Equinox.

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

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

Equinox Media Server deployment checklist

#	Action	Link/Notes	✔
1	Download the Equinox Media Server software from PLDS.	See Downloading software from PLDS on page 90	
2	Deploy the Equinox Media Server virtual machine.	See Deploying the Equinox Media Server virtual machine on page 185	
3	Start the Equinox Media Server virtual machine.	See Starting the Equinox Media Server virtual machine on page 190	
4	Configure the Equinox Media Server IP addresses using vSphere Client Console. This step is required only if you do not use vCenter.	See Configuring the Equinox Media Server IP addresses using vSphere Client Console on page 190	
5	Configure the Equinox Media Server virtual machine automatic startup settings.	See Configuring the virtual machine automatic startup settings on page 192	
6	Add Equinox Media Server in Equinox Management	See Adding Equinox Media Server in Equinox Management on page 192	
7	Configure the Equinox Media Server network settings.	See Configuring the Equinox Media Server network settings on page 195	

Equinox Media Server video conferencing mode administration checklist

Use this checklist to administration the activate Equinox Media Server as a media server for video conferencing and web collaboration.

No.	Task	Link/Notes	✔
1	Deploy the Equinox Media Server virtual machine.	See Deploying the Equinox Media Server virtual machine on page 185	
2	Start the Equinox Media Server virtual machine.	See Starting the Equinox Media Server virtual machine on page 190	
3	Configure the Equinox Media Server IP addresses using vSphere Client Console. This step is required only if you do not use vCenter.	See Configuring the Equinox Media Server IP addresses using vSphere Client Console on page 190	
4	Add Equinox Media Server in Equinox Management	See Adding Equinox Media Server in Equinox Management on page 192	

Table continues…

No.	Task	Link/Notes	✔
5	Update the Equinox Media Server video conferencing and web collaboration license.	See Adding or updating the Equinox Media Server licenses on page 197	

Equinox Media Server audio-only conferencing mode administration checklist

Use this checklist to administration the activate Equinox Media Server as a media server for audio-only conferencing and web collaboration.

No.	Task	Link/Notes	✔
1	Deploy the Equinox Media Server virtual machine.	See Deploying the Equinox Media Server virtual machine on page 185	
2	Start the Equinox Media Server virtual machine.	See Starting the Equinox Media Server virtual machine on page 190	
3	Configure the Equinox Media Server IP addresses using vSphere Client Console. This step is required only if you do not use vCenter.	See Configuring the Equinox Media Server IP addresses using vSphere Client Console on page 190	
4	Add Equinox Media Server in Equinox Management.	See Adding Equinox Media Server in Equinox Management on page 192	
5	Update the Equinox Media Server audio-only conferencing and web collaboration license.	See Adding or updating the Equinox Media Server licenses on page 197	
6	Install security certificates for TLS.	See Creating security certificates on page 200 and Uploading security certificates on page 201	
7	Secure the connection between Equinox Media Server and Equinox Management.	See Securing the connection with Equinox Management using TLS on page 202	
8	Change the working mode of Equinox Media Server to High Capacity Audio + Web Collaboration.	See Changing the Equinox Media Server working mode on page 198	
9	Upload the audio prompts.	See Customizing audio messages on page 199	

Equinox Media Server web collaboration mode administration checklist

Use this checklist to administration the activate Equinox Media Server as a media server for only web collaboration.

No.	Task	Link/Notes	✔
1	Deploy the Equinox Media Server virtual machine.	See Deploying the Equinox Media Server virtual machine on page 185	
2	Start the Equinox Media Server virtual machine.	See Starting the Equinox Media Server virtual machine on page 190	
3	Configure the Equinox Media Server IP addresses using vSphere Client Console. This step is required only if you do not use vCenter.	See Configuring the Equinox Media Server IP addresses using vSphere Client Console on page 190	
4	Add Equinox Media Server in Equinox Management.	See Adding Equinox Media Server in Equinox Management on page 192	
5	Update the Equinox Media Server web collaboration-only license.	See Adding or updating the Equinox Media Server licenses on page 197	

Equinox Media Server WebRTC gateway administration checklist

Use this checklist to administration the activate Equinox Media Server as a WebRTC gateway.

No.	Task	Link/Notes	✔
1	Deploy the Equinox Media Server virtual machine.	See Deploying the Equinox Media Server virtual machine on page 185	
2	Start the Equinox Media Server virtual machine.	See Starting the Equinox Media Server virtual machine on page 190	
3	Configure the Equinox Media Server IP addresses using vSphere Client Console. This step is required only if you do not use vCenter.	See Configuring the Equinox Media Server IP addresses using vSphere Client Console on page 190	
4	Add Equinox Media Server as a gateway in Equinox Management.	See Adding Equinox Media Server as a gateway on page 194	

Table continues…

No.	Task	Link/Notes	✔
5	Update the Equinox Media Server WebRTC-only license.	See Adding or updating the Equinox Media Server licenses on page 197	
6	Install security certificates for TLS.	See Creating security certificates on page 200 and Uploading security certificates on page 201	
7	Secure the connection between Equinox Media Server and Equinox Management.	See Securing the connection with Equinox Management using TLS on page 202	

Technical specifications

- 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.
- 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 and Web Collaboration mode, the maximum supported ports for audio in each deployment type also includes support for web collaboration.

Deployment configuration-wise hardware server requirement

Requirement	Ultra High configuration	High configuration	Medium configuration	Low configuration
Server CPU (processor * physical cores)	2.5 GHz * 24 cores	2.5 GHz * 16 cores	2.0 GHz * 12 cores	2.0 GHz * 6 cores
RAM in GB	64	32	24	12
2.5” SAS hard disk capacity in GB	120	120	120	120
Maximum licenses applicable in Over The Top deployments	4	2	1	Audio-only licenses
Maximum supported ports	40 ports for 720p*30fps video or 2000 ports for audio	20 ports for 720p*30fps video or 1000 ports for audio	10 ports for 720p*30fps video or 500 ports for audio	200 ports for audio

Deployment configuration-wise virtual machine requirement

Requirement	Ultra High configuration	High configuration	Medium configuration	Low configuration
Server CPU (processor speed * physical cores)	2.5 GHz * 24 cores	2.5 GHz * 16 cores	2.0 GHz * 12 cores	2.0 GHz * 6 cores
Virtual cores	48	32	12	6
CPU reservation in MHz	55000	35000	21900	9900
RAM reservation in GB	58	20	14	10
Disk space reservation in GB	120	120	120	120
NIC	2	2	2	2
Maximum licenses applicable in Over The Top deployment	4	2	1	Audio-only licenses
Maximum supported ports	40 ports for 720p*30 video or 2000 ports for audio	20 ports for 720p*30 video or 1000 ports for audio	10 ports for 720p*30 video or 500 ports for audio	200 ports for audio

Capacity and scalability

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.

<table>
<tr><th rowspan="2">Port-based licenses for Over The Top deployments</th><th rowspan="2">User-based licenses for Avaya Aura® Power Suite deployments</th><th colspan="3">Video</th><th rowspan="2">Audio using G.711 codec</th><th rowspan="2">Web collaboration</th><th rowspan="2">Deployment configuration</th></tr>
<tr><th>1080p*30fps using H.264 codec or 720p*30fps using VP8 codec</th><th>720p*30fps using H.264 codec or 480p*30fps using VP8 codec</th><th>480p*30fps using H.264 codec</th></tr>
<tr><td>4</td><td>16</td><td>20</td><td>40</td><td>80</td><td>80</td><td>80</td><td>Ultra High</td></tr>
<tr><td>3</td><td>12</td><td>15</td><td>30</td><td>60</td><td>60</td><td>60</td><td>Ultra High</td></tr>
<tr><td>2</td><td>8</td><td>10</td><td>20</td><td>40</td><td>40</td><td>40</td><td>High</td></tr>
<tr><td>1</td><td>4</td><td>5</td><td>10</td><td>20</td><td>20</td><td>20</td><td>Medium</td></tr>
</table>

High Capacity Audio 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.

Port-based licenses for Over The Top deployments	User-based licenses for Avaya Aura® Power Suite deployments	Audio using G.711 codec	Web collaboration	Deployment configuration
4	16	2000	2000	Ultra High
3	12	1500	1500	Ultra High
2	8	1000	1000	High
1	4	500	500	Medium
Migrations from existing Avaya Aura® Conferencing deployments	—	200	200	Low

Downloading software from PLDS

When you place an order for an Avaya PLDS-licensed software product, PLDS creates the license entitlements of the order and sends an email notification to you. The email includes a license activation code (LAC) and instructions for accessing and logging into PLDS. Use the LAC to locate and download the purchased license entitlements.

In addition to PLDS, you can download the product software from http://support.avaya.com using the **Downloads and Documents** tab at the top of the page.

Note:

Only the latest service pack for each release is posted on the support site. Previous service packs are available only through PLDS.

Procedure

1. Enter http://plds.avaya.com in your Web browser to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS home page, select **Assets**.
4. Click **View Downloads**.
5. Click on the search icon (magnifying glass) for **Company Name**.
6. In the **%Name** field, enter **Avaya** or the Partner company name.
7. Click **Search Companies**.
8. Locate the correct entry and click the **Select** link.
9. Enter the Download Pub ID.
10. Click **Search Downloads**.
11. Scroll down to the entry for the download file and click the **Download** link.
12. In the **Download Manager** box, click the appropriate download link.

    Note:

    The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.
13. If you use Internet Explorer and get an error message, click the **install ActiveX** message at the top of the page and continue with the download.
14. Select a location where you want to save the file and click **Save**.
15. If you used the Download Manager, click **Details** to view the download progress.

Deploying the Equinox Media Server virtual machine

About this task

The Equinox Media Server virtual machine software for VMware is available in the .OVA package format. You can install the OVA file using vSphere Client. The virtual machine 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 server.

Before you begin

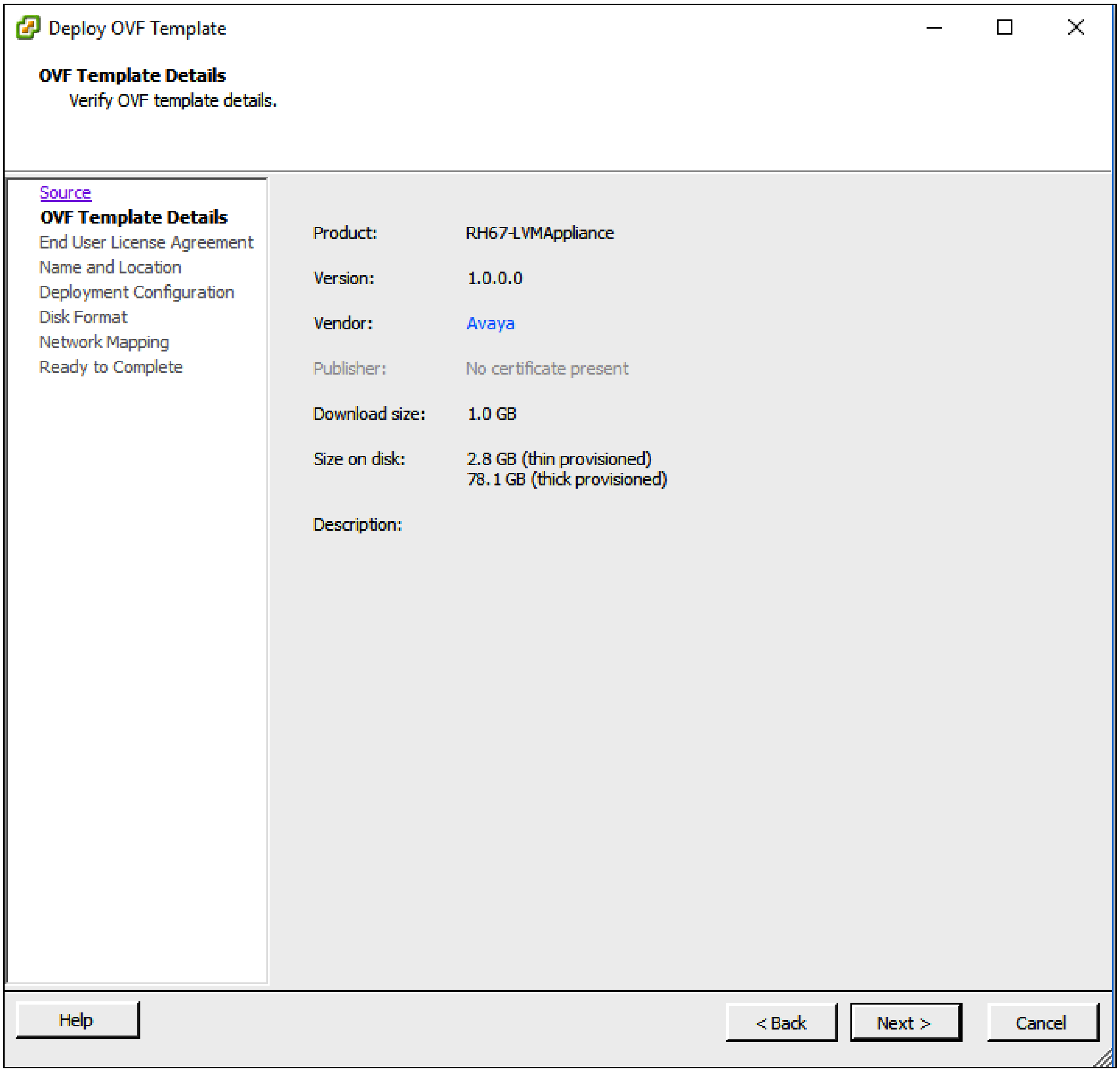
- Download the Equinox Media Server OVA to your computer.
- Ensure that the VMware ESXi host server software is Release 5.5 or 6.0.

Procedure

1. Log in to vSphere Client.
2. Select the host ESXi server to deploy the Equinox Media Server virtual machine.

   If you do not choose a host server before deploying the virtual machine, vSphere Client prompts you for the host or cluster name to deploy the virtual machine.
3. Click **File** > **Deploy OVF Template**.
4. Do one of the following to deploy the Equinox Media Server OVF package:
   - Click **Browse** and provide the Equinox Media Server OVA file location.
   - In the **Deploy from a file or URL** field, enter the full URL of the HTTP server where the Equinox Media Server 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**.



Deploy OVF Template

OVF Template Details

Verify OVF template details.

Product: RH67-LVMAppliance

Version: 1.0.0.0

Vendor: Avaya

Publisher: No certificate present

Download size: 1.0 GB

Size on disk: 2.8 GB (thin provisioned)
78.1 GB (thick provisioned)

Description:

7. Read the license agreement, and click **Accept**.
8. Click **Next**.
9. In the **Name** field, enter the name of the new virtual machine.
10. Select **Inventory Location** from the inventory location tree where you want this virtual machine to reside.
11. Select the deployment capacity from the **Configuration** drop-down list.

    The deployment capacity must be within the server hardware limits and the license capacity.
12. Click **Next** to display the Storage window.

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. Click **Next** to display the Disk Format window.
15. Select **Thin Provision**, and 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.
16. **(Optional)** From the **Destination Network** drop-down list, select a network option, and click **Next**.

    vSphere Client displays the Properties window.
17. Configure the following IP addresses:

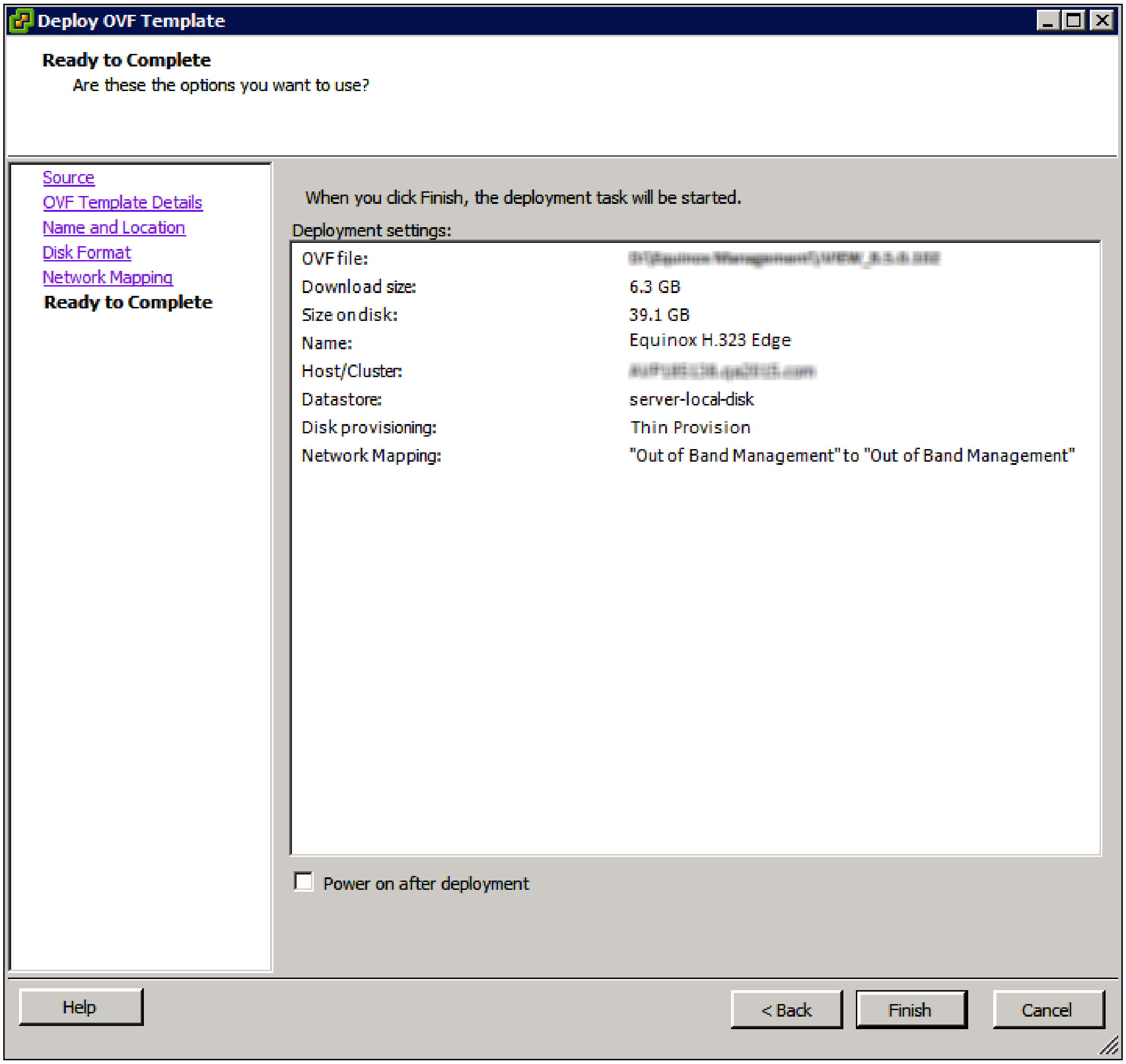
    - **Default Gateway**
    - **Public IP Address**
    - **Public Netmask**

    This configuration is for the internal network. To configure IP separation, you must configure the secondary IP addresses for the external network in Equinox Management after the deployment.

    Note:

    vSphere Client displays the Properties window to configure IP addresses only if you use vCenter. If you do not use vCenter, you must configure the IP addresses in the vSphere console only after the Equinox Media Server virtual machine deployment is complete.

18. Click **Next** to display the Ready to Complete window.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	[redacted]
Download size:	6.3 GB
Size on disk:	39.1 GB
Name:	Equinox H.323 Edge
Host/Cluster:	[redacted]
Datastore:	server-local-disk
Disk provisioning:	Thin Provision
Network Mapping:	"Out of Band Management" to "Out of Band Management"

☐ Power on after deployment

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

Result

vSphere Client starts the Equinox Media Server OVA deployment.

Related links

Configuring the Equinox Media Server IP addresses using vSphere Client Console on page 190

Configuring the Equinox Media Server network settings on page 195

Starting the Equinox Media Server virtual machine

Before you begin

Deploy the Equinox Media Server virtual machine.

Procedure

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

   The Equinox Media Server virtual machine starts.

Configuring the Equinox Media Server IP addresses using vSphere Client Console

About this task

If you do not use vCenter, you must configure the IP addresses in vSphere Client Console after the Equinox Media Server virtual machine deployment is complete

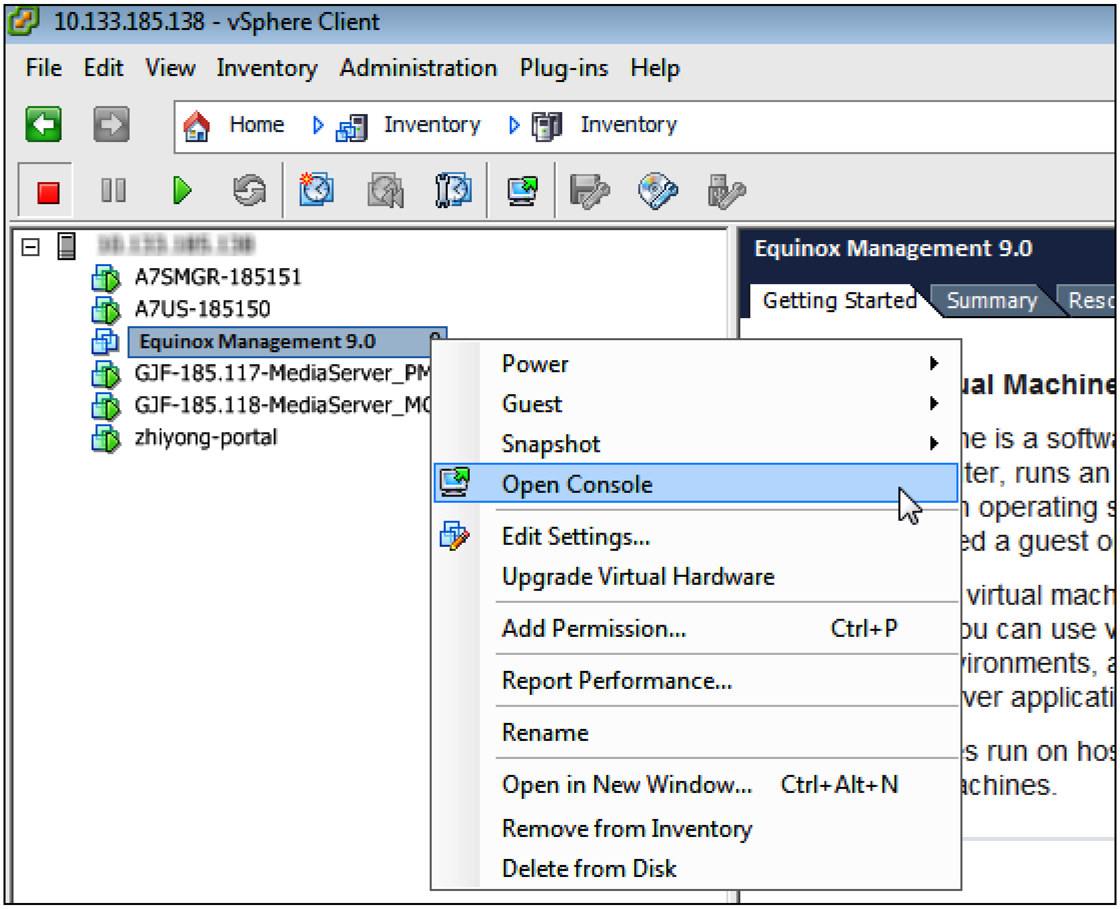
Before you begin

Start the Equinox Media Server virtual machine.

Procedure

1. Log in to vSphere Client.
2. Click **Inventory** > **Hosts and Clusters**.

3. Right-click the virtual machine, and click **Open Console**.



vSphere Client displays the main menu of the console.

4. Type `N` to configure the network port values.
5. Type `2` to configure the IP addresses.
6. Configure the IP addresses, and type `Q` to quit the console.

Result

vSphere Client restarts the virtual machine.

Related links

Configuring the Equinox Media Server network settings on page 195

Configuring the virtual machine automatic startup settings

About this task

This procedure does not apply for deployments and upgrades of applications running on Appliance Virtualization Platform.

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**.

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.

Related links

Adding or updating the Equinox Media Server licenses on page 197

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.

Table continues…

Name	Description
	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.
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.
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.
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	FQDN of Equinox Media Server. The local FQDN must be identical to the service FQDN.

Table continues…

Name	Description
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 The transport type must be UDP.
Turn/Stun Servers	The IP address of the session border controller. This field is relevant only if you deploy Equinox Media Server as a WebRTC gateway.

Adding or updating the Equinox Media Server licenses

About this task

Update license keys when you increase the Equinox Media Server capacity or increase the number of ports with a flexible license.

Before you begin

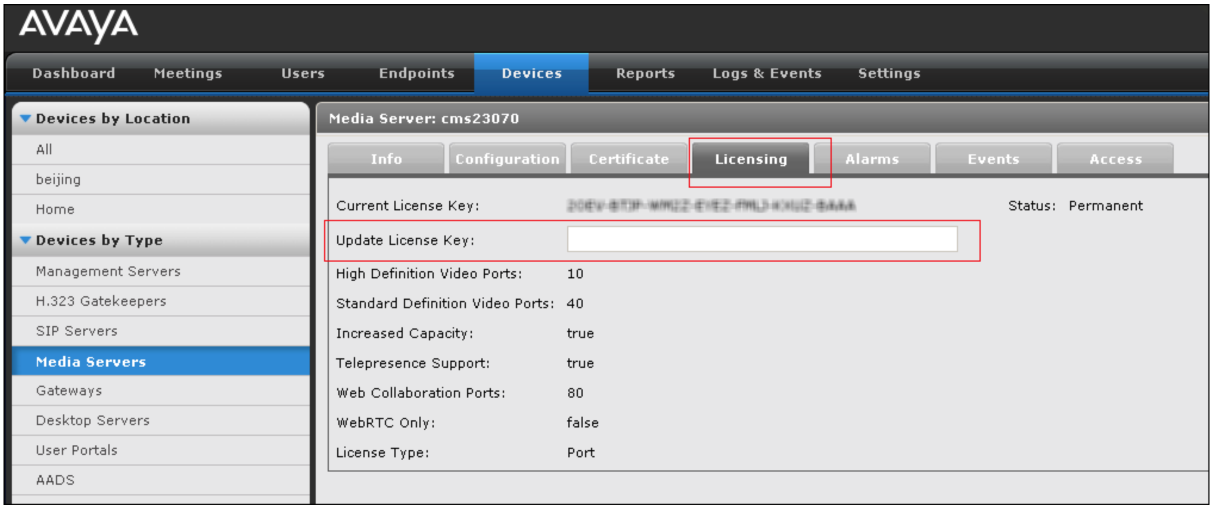
- Get the License Authentication Code (LAC) file from the Avaya customer email.
- Download the upgrade package at https://plds.avaya.com/. If you upgrade Equinox Media Server to a major version, you need a new license key.

Procedure

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

   Equinox Management displays the Equinox Media Server instance page.

3. Click the **Licensing** tab.



Media Server: cms23070

Current License Key: [redacted] Status: Permanent

Update License Key:

High Definition Video Ports: 10

Standard Definition Video Ports: 40

Increased Capacity: true

Telepresence Support: true

Web Collaboration Ports: 80

WebRTC Only: false

License Type: Port

4. In **Update License Key**, copy and paste or type the license key.
5. Click **Apply**.

Result

Equinox Management activates the new Equinox Media Server license.

Changing the Equinox Media Server working mode

Before you begin

Add the Media Server license to the Equinox Media Server instance.

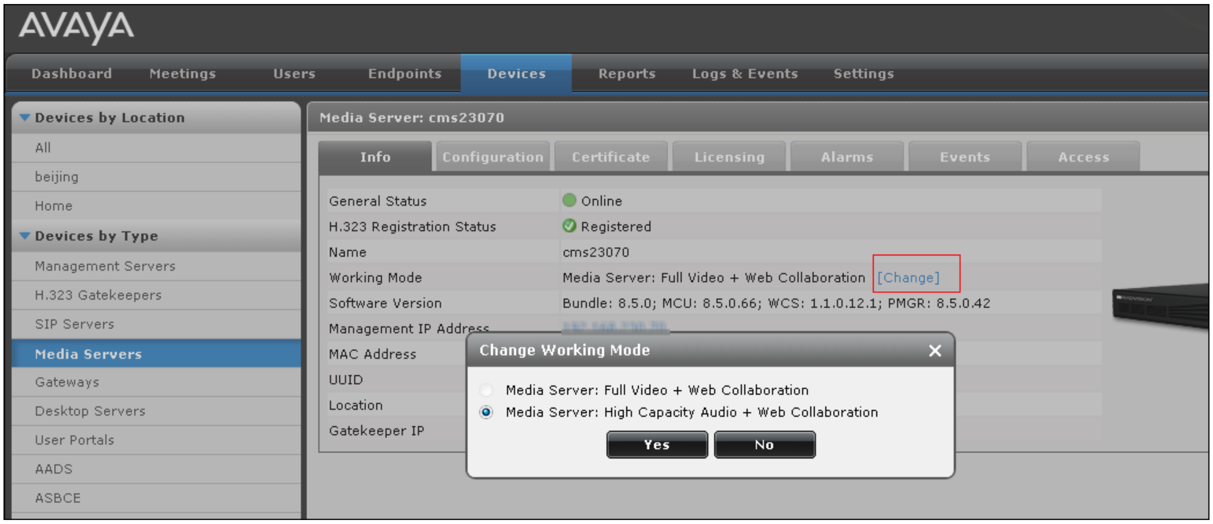
Procedure

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 + Web Collaboration



Media Server: cms23070

General Status	Online
H.323 Registration Status	✓ Registered
Name	cms23070
Working Mode	Media Server: Full Video + Web Collaboration [Change]
Software Version	Bundle: 8.5.0; MCU: 8.5.0.66; WCS: 1.1.0.12.1; PMGR: 8.5.0.42
Management IP Address	[redacted]
MAC Address	
UUID	
Location	
Gatekeeper IP	

Change Working Mode

○ Media Server: Full Video + Web Collaboration

● Media Server: High Capacity Audio + Web Collaboration

Yes No

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. Click **Update**, 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.
5. 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.

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**
   - **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.

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.

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 12: 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.

An MCU, or Multipoint Control Unit, connects several endpoints to a single videoconference. It manages the audio mixing and creates the video layouts, adjusting the output to suit each endpoint's capabilities.

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.	See *Rack Mounting Guide for Avaya Scopia® Elite 6000 MCU*	

Table continues…

#	Action	Link/Notes	✔
	- 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.		
2	Configure the Scopia® Elite 6000 MCU IP addresses and IP separation.	See Configuring the Device IP Addresses on page 210 and Configuring IP separation on page 215	
3	Update the Scopia® Elite 6000 MCU license	See Adding or updating licenses on page 220	
4	Configure the ports on Scopia® Elite 6000 MCU	See Configuring Ports on All Models of the MCU on page 221	
5	Verify the installation of the Scopia® Elite 6000 MCU server	See Verifying the Installation on page 227	

Technical specifications

This section details the system specifications of the MCU you purchased. Refer to this data when preparing system setup and afterwards as a means of verifying that the environment still complies with these requirements.

Hardware requirements

The following table refers to the physical details of the device:

Table 24: Physical device specifications

	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

Table continues…

	Scopia Elite MCU 6105, 6110 and 6120	**Scopia Elite MCU 6140**
Maximum power consumption at 35°C	200W, 250VA (682 BTU/h)	360W, 450VA (1228 BTU/h)
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

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

- Signaling protocols:
  - H.323
  - SIP
  - H.320 (in conjunction with Scopia H.320 Gateways)
- Audio support:
  - 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 support:
  - 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
- Web browser support:
  - Microsoft Internet Explorer version 6 and later

- Microsoft Edge
- Mozilla Firefox version 3.3 and later
- 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.

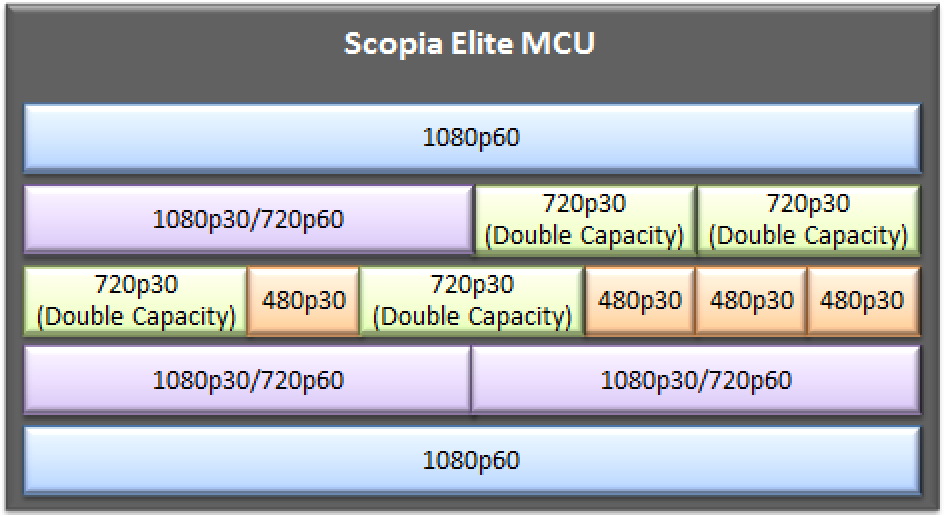


Figure 104: A connection uses its proportion of resources on the MCU

Important:

To enable connections at 720p at 30fps to use half the capacity of a 1080p 30fps connection, install the Double Capacity license. For more information, see Adding or updating licenses on page 220.

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 25: 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). 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). For more information on enabling switching, see *Administrator Guide for Scopia Elite 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 Scopia Elite 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 26: 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 28: 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 26: 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 222
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 223 and Configuring the UDP port for the gatekeeper on Scopia® Elite 6000 MCU on page 224
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 225
3336	XML (TCP)	Conference Control web client endpoint, Equinox Managemen	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

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
		t, or third-party controlling applications			
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
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 226
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 225
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 225
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 221

Table 27: 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 28: 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 223
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 105: Rear panel of the device on page 212). 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.

You must choose how you want to deploy the two network ports of this device: network redundancy or IP separation.

By default, the NICs are paired as a primary NIC and a redundant NIC. To separate them into media and management (IP separation) first define the IP address of both NICs as detailed in this section, and then perform the IP separation.

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.

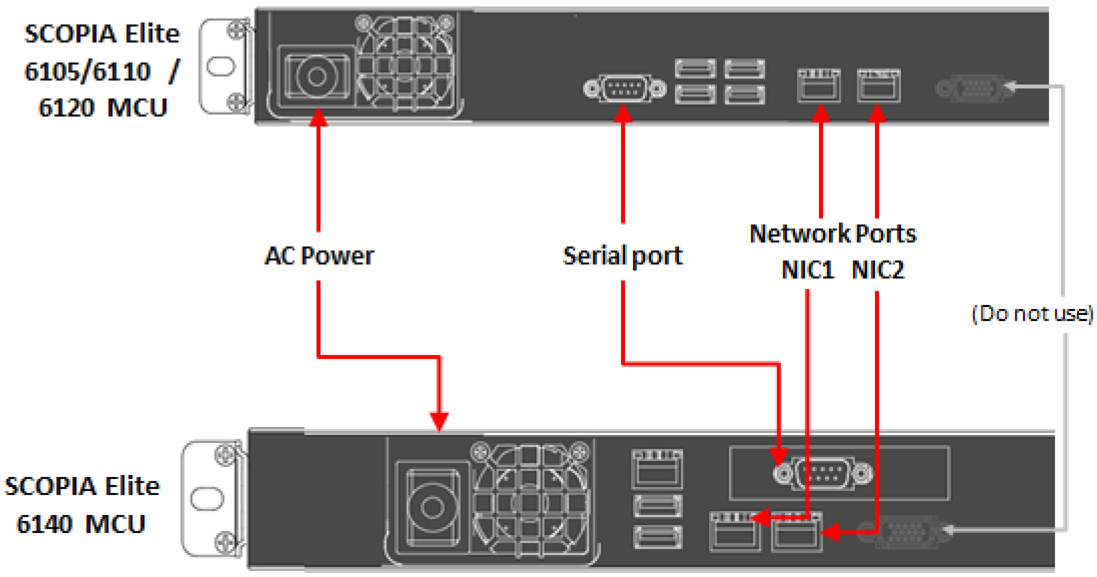


Figure 105: Rear panel of the device

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 29: Configuring the communication settings on page 212):

Table 29: Configuring the communication settings

Field Name	Value
Baud Rate	9600
Data bits	8
Parity	None
Stop bits	1
Flow Control	None

5. Power the device (see Figure 106: Device front panel on page 213).

   Verify the power LED is lit green (Figure 106: Device front panel on page 213).

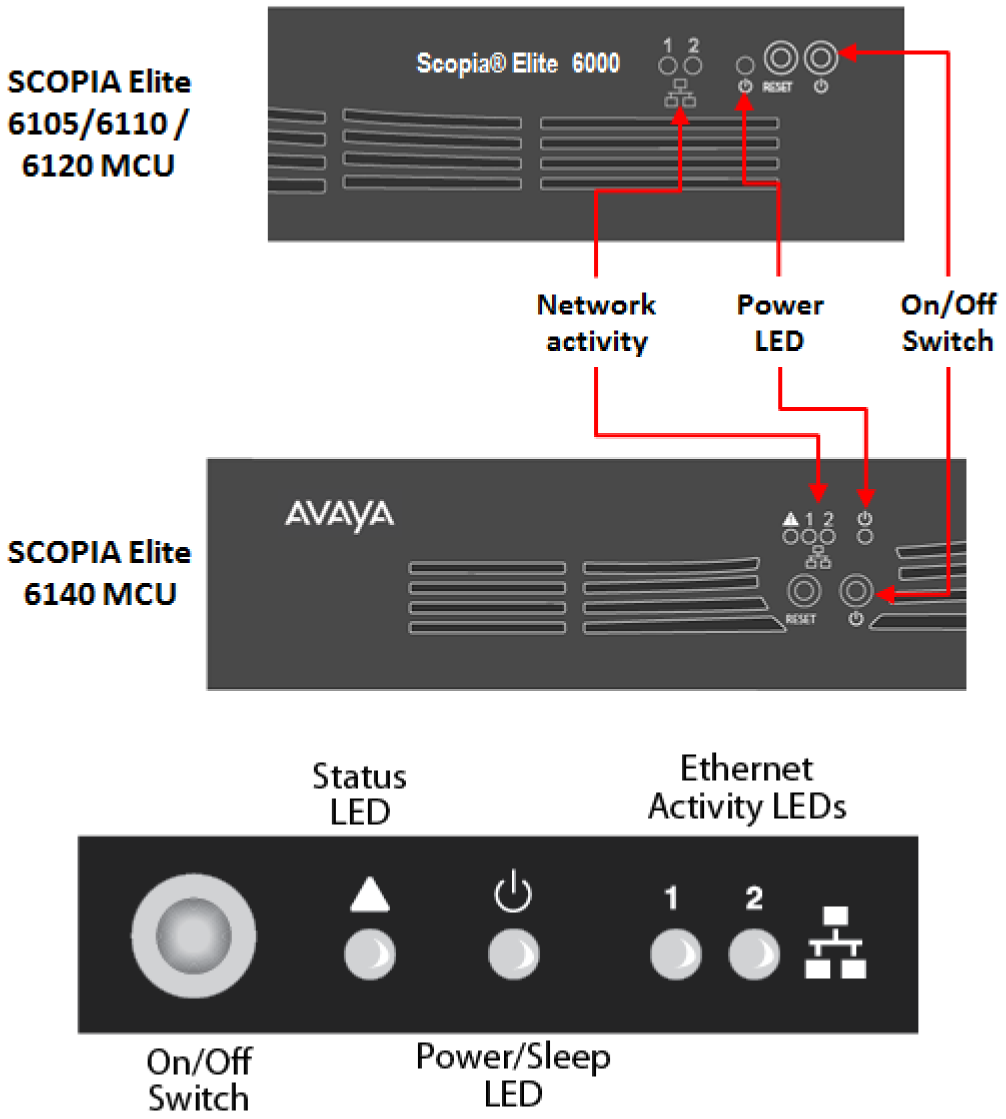


Figure 106: Device front panel

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 30: Configuring network settings on page 214).

   Table 30: 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

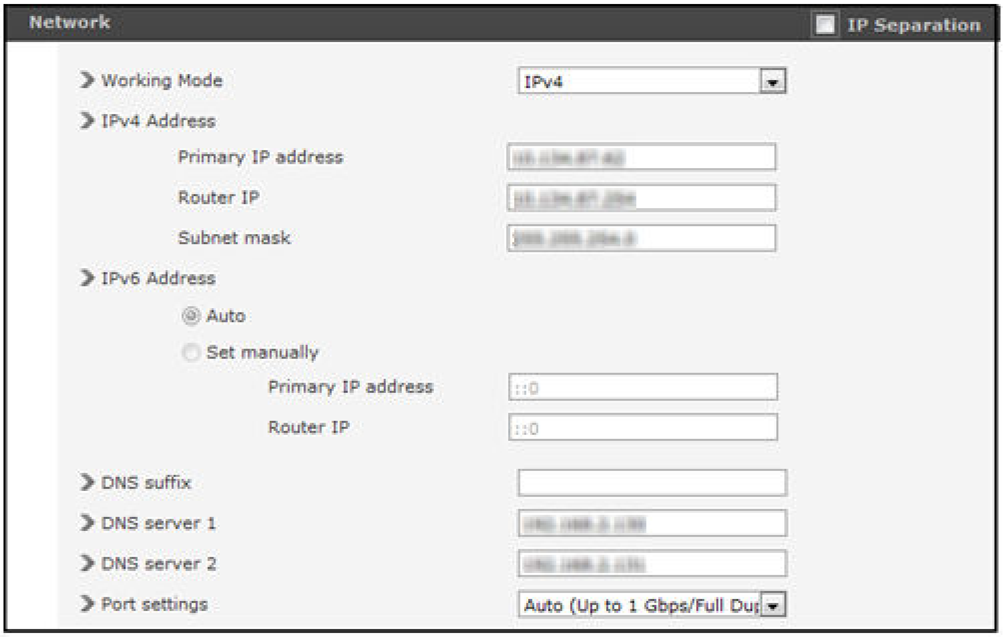
   Important:

   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 or IP separation, 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.
    - To achieve IP separation for separating management and media traffic, connect NIC1 to the management subnet and NIC2 to the media and signaling subnet. For more information, see Configuring IP separation on page 215.
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 107: Configuring the MCU throughput on page 215).



Network □ IP Separation

Working Mode: IPv4

IPv4 Address

Primary IP address: [redacted]

Router IP: [redacted]

Subnet mask: [redacted]

IPv6 Address

● Auto

○ Set manually

Primary IP address: ::0

Router IP: ::0

DNS suffix:

DNS server 1: [redacted]

DNS server 2: [redacted]

Port settings: Auto (Up to 1 Gbps/Full Du

Figure 107: Configuring the MCU throughput

14. To configure the following IPv6 and DNS server IP addresses, navigate to **Configuration** > **Network** (Figure 107: Configuring the MCU throughput on page 215).

    - **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 IP separation

About this task

You can configure IP separation on each network port (dual-NIC), improving security by placing the management data on a separate subnet from the media and signaling traffic.

Separating these types of data on different subnets improves security because management data typically remains on subnets within the enterprise, while the media of video calls is often required to traverse firewalls and reach endpoints outside the enterprise.

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.

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.

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.

Before you begin

- You must choose how you want to deploy the two network ports of this device: network redundancy or IP separation.

  By default, the NICs are paired as a primary NIC and a redundant NIC. To separate them into media and management (IP separation) first define the IP address of both NICs, and then perform the IP separation.
- Make sure you have the management interface IPv4 addresses ready for use: Management IP Address, Management Router, Management Subnet Mask.
- Make sure you have the IPv4 addresses of the media and signaling interface ready for use: Media/Signaling IP Address, Media/Signaling Router, Media/Signaling Subnet Mask.
- If you need management access from another branch with its own network, make sure you have the IPv4 address of that branch ready for configuration.
- Make sure no videoconferences are running on the MCU, as you need to restart it at the end of the procedure.

Procedure

1. If you previously had the MCU in a redundant dual-NIC setup and now you want to use to use dual NIC for IP separation, disconnect the network cables from the network switch.
2. Connect the network cable of the management subnet to the left ethernet port (NIC1).

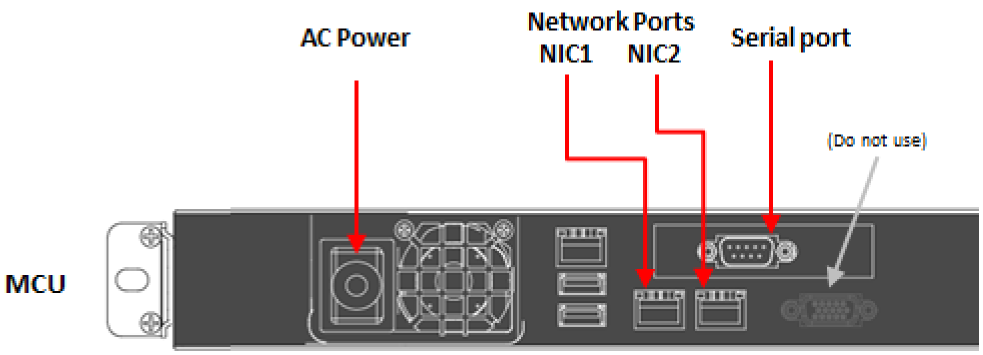


Figure 108: The device's management connections

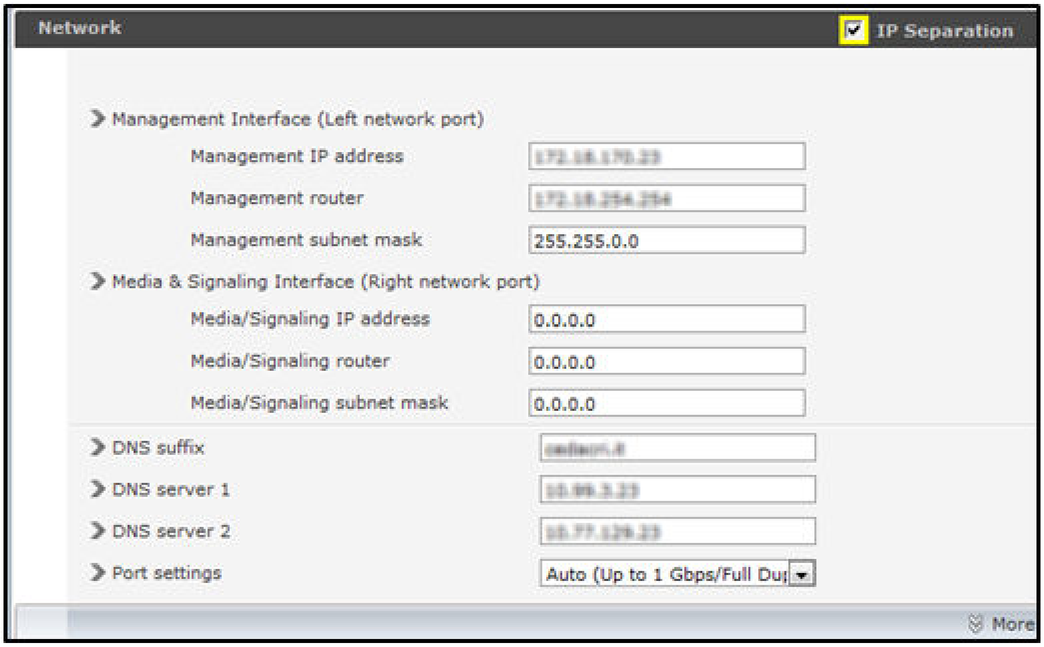
Important:

Do *not* connect the network cable of the media subnet until you restart the device at the end of this procedure.

3. Log in to Equinox Management.
4. Click **Devices**.
5. In the left pane, click **Media Servers**.
6. Click the name of the media server instance.

   Equinox Management displays the page of the media server instance.
7. In the **Info** tab, click the IP address of the media server.

   Equinox Management display the management UI in a new window.
8. Select the **Configuration** Configuration tab.
9. Select the **IP Separation** check box to expand that section of the page.



Management Interface (Left network port)

Management IP address: [redacted]

Management router: [redacted]

Management subnet mask: 255.255.0.0

Media & Signaling Interface (Right network port)

Media/Signaling IP address: 0.0.0.0

Media/Signaling router: 0.0.0.0

Media/Signaling subnet mask: 0.0.0.0

DNS suffix: [redacted]

DNS server 1: [redacted]

DNS server 2: [redacted]

Port settings: Auto (Up to 1 Gbps/Full Du

Figure 109: Configuring IP separation with two network connections

10. Configure the IP addresses of each interface.

Table 31: Configuring the IP addresses of each network interface

Field	Description
Management IP address	IP address of the MCU management interface (left ethernet port) as configured via serial port. This is the IP used to access this web interface.
Management router	IP address of the management subnet router
Management subnet mask	IP address of the management subnet mask
Media/Signaling IP address	IP address of the MCU media and signaling interface (right ethernet port belonging to a different subnet)
Media/Signaling router	IP address of the media and signaling subnet router
Media/Signaling subnet mask	IP address of the media and signaling subnet mask

11. Select **Apply** at the bottom of the page.
12. Select **Yes** to restart the MCU.
13. Connect the network cable of the media subnet cable to the right ethernet port (NIC2).

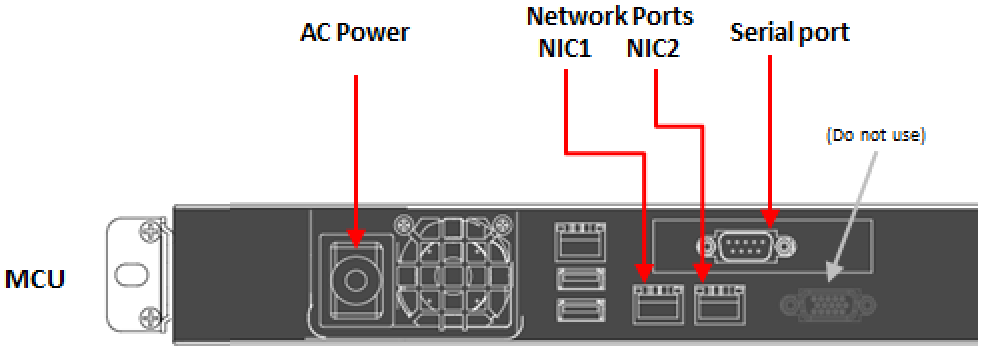


Figure 110: The device's media and signaling connections

14. (Optional) Depending on your deployment, you may need to access the MCU management interface from another network.

    For example, if your MCU is located on network 123.x.x.x and your browser is on the same network (123.x.x.x), you can access the administrator web interface to reach this web page. You can then configure IP separation of management and media as detailed in this procedure, where management communications stay in this network (123.x.x.x) while media is routed to a different network: 456.x.x.x. However, if you need management access from another branch with its own network, for example 789.x.x.x, you can configure the 789.x.x.x management traffic to be routed via 123.x.x.x, and then onwards to 789.x.x.x.

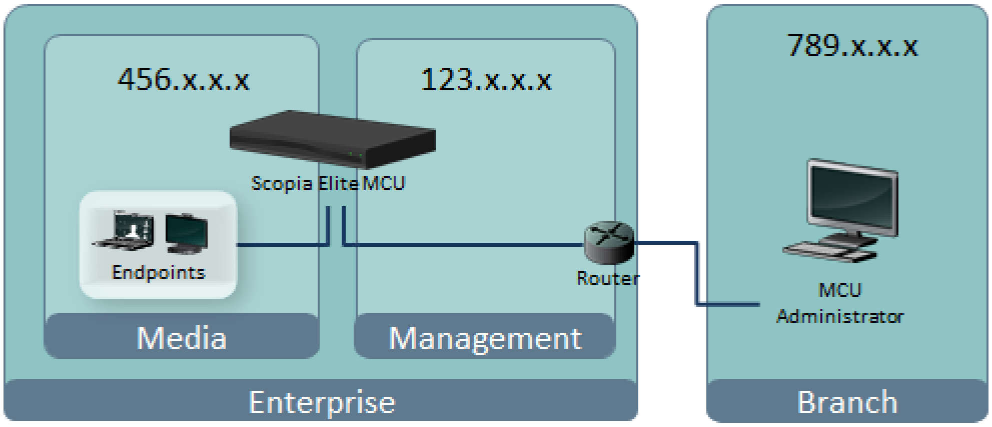


Figure 111: Example of additional management network

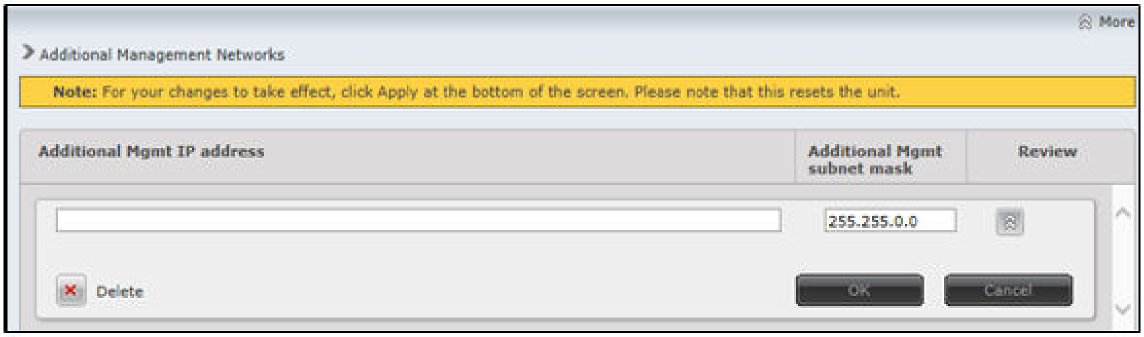
Use the following steps to configure an additional management network:

a. Select **More** at the bottom of the expanded section.

   The **Additional Management Networks** section opens.

b. Select **Add Management Network**.

c. Configure the access to the MCU management subnet.



Additional Management Networks

Note: For your changes to take effect, click Apply at the bottom of the screen. Please note that this resets the unit.

Additional Mgmt IP address	Additional Mgmt subnet mask	Review
	255.255.0.0	

Figure 112: Adding a new network for management access

Table 32: Configuring the additional network interfaces

Field	Description
IP address	IP address of the additional network to access the management of the MCU
Subnet mask	IP address of the additional management subnet mask

d. Select **OK**.

Adding or updating licenses

About this task

Update license keys when you increase the Scopia® Elite 6000 MCU capacity or increase the number of ports with a flexible license.

Scopia® Elite 6000 MCU has several pre-installed licenses. You can purchase more licenses, such as the option to increase the port capacity when you set the video quality to 720p with 30 frames per second.

Important:

If you add a non-encryption license, you cannot revert to a standard license that supports encryption.

Before you begin

- Get the License Authentication Code (LAC) file from the Avaya customer email.
- Download the upgrade package at https://plds.avaya.com/. If you upgrade Scopia® Elite 6000 MCU to a major version, you must have a new license key.

Procedure

1. Log in to Equinox Management.
2. Click **Devices**, and select the Scopia® Elite 6000 MCU instance.

Equinox Management displays the Scopia® Elite 6000 MCU 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 Scopia® Elite 6000 MCU license.

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 221
Configuring the TCP Port Range for H.245 on Scopia® Elite 6000 MCU on page 222
Configuring the HTTP port on Scopia® Elite 6000 MCU on page 223
Configuring the UDP port for RAS on Scopia® Elite 6000 MCU on page 223
Configuring the UDP port for the gatekeeper on Scopia® Elite 6000 MCU on page 224
Configuring the TCP port for Q.931 on Scopia® Elite 6000 MCU on page 225
Configuring the TCP, UDP, and TLS port for SIP on page 225
Configuring the TCP port range for SIP BFCP on Scopia® Elite 6000 MCU on page 226

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 221

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 221

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 221

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 221

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 223).

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.

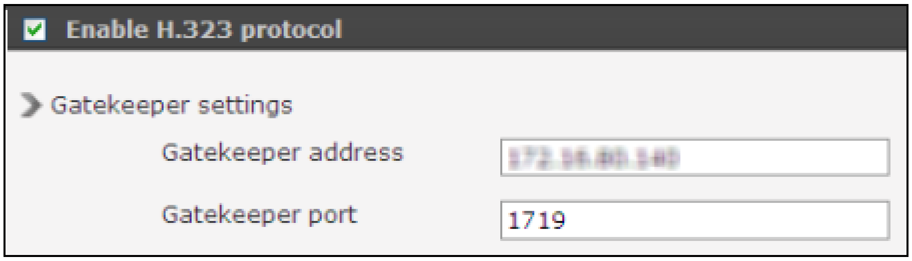
Procedure

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 113: H.323 Protocol section of the Protocols tab on page 225).



☑ Enable H.323 protocol

Gatekeeper settings

Gatekeeper address: [redacted]

Gatekeeper port: 1719

Figure 113: 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 221

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 221

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 221

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 221

Verifying the MCU Equinox H.323 Edge 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.

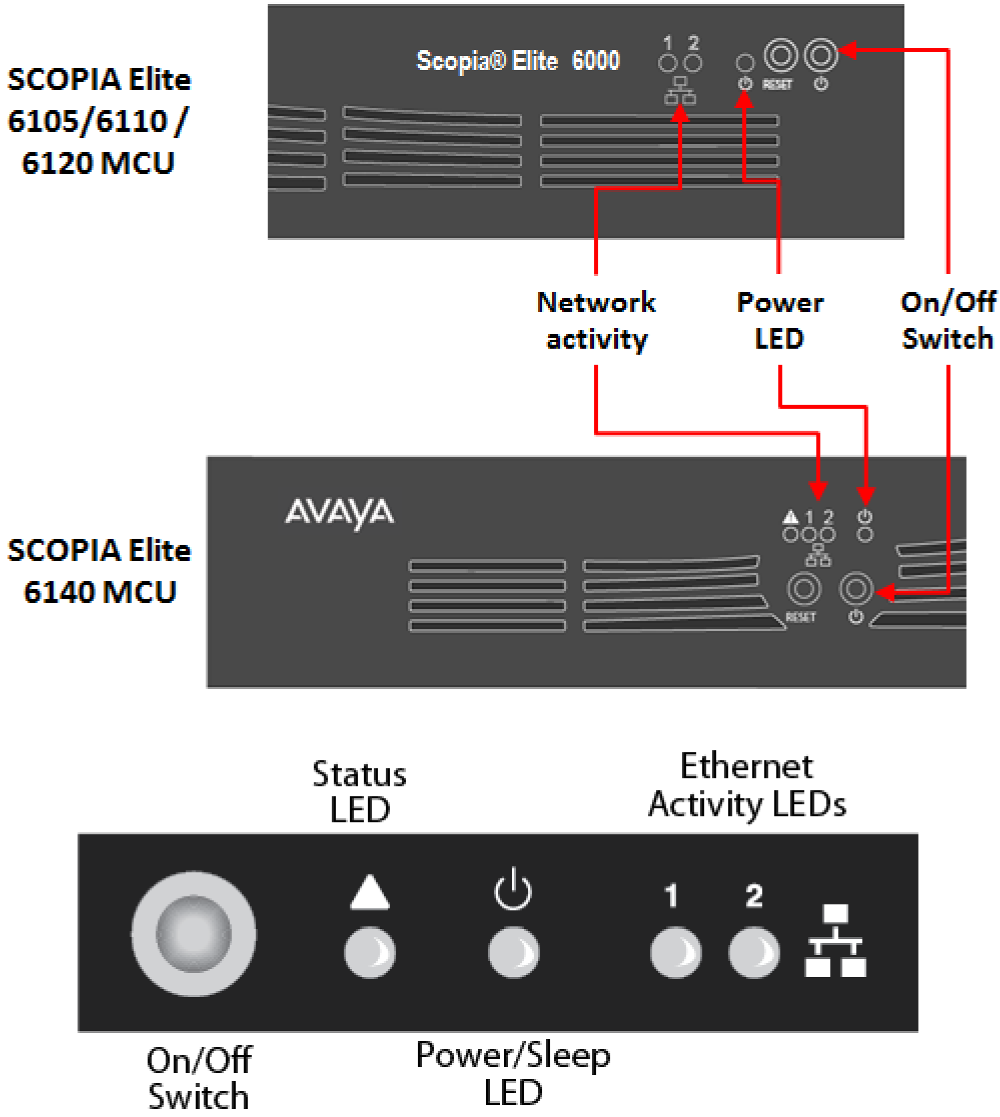


Figure 114: Locating the front panel LEDs

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.

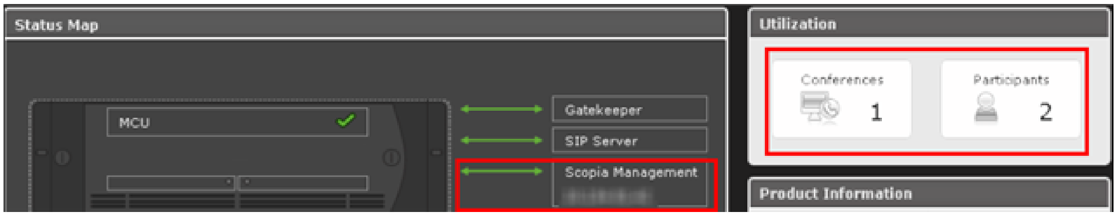
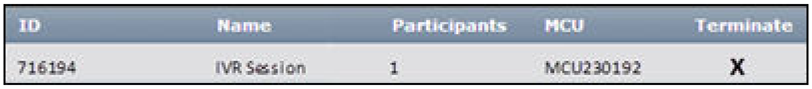


Figure 115: The MCU Status Map

       - The Equinox Management **Dashboard** which shows the details of the current videoconference.



ID	Name	Participants	MCU	Terminate
716194	IVR Session	1	MCU230192	X

Figure 116: The Equinox Management Dashboard status

    f. Exit the videoconference by disconnecting the call.

Chapter 13: Avaya Aura deployment

Deploying Avaya Aura components

The following table lists the related documents for Avaya Aura components that are part of the Team Engagement deployment. Download the documents from http://support.avaya.com. Each document has a Documentation chapter with a list of other related documents that will help you in the deployment.

The Avaya Support website also includes the latest information about product compatibility, ports, and Avaya Aura® releases.

Title	Description
Avaya Aura® Session Manager Overview and Specifications	Describes the key features of Session Manager (SM) and of the co-resident option, Avaya Aura Device Services (AADS)
Avaya Aura® System Manager Overview and Specification	Describes the key features of System Manager (SMGR).
Deploying and Updating Avaya Aura® Media Server Appliance	Describes the deployment, updates and troubleshooting of Avaya Aura® Media Server appliances deployed in the VMware® virtualized environment or on Avaya Common Server. Can function as a WebRTC to SIP gateway for converting from WebRTC media to SIP-friendly media and support video codec transcoding as well.
Avaya WebRTC Snap-in Reference	Describes the Avaya WebRTC Snap-in. Enables 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.
Avaya Aura® Communication Manager Overview and Specification	Describes the key features of Communication Manager.
Avaya Aura® Presence Service Overview and Specification	Describes the key features of Presence Services.
Avaya Multimedia Messaging Overview and Specification	Describes the Avaya Multimedia Messaging product and its features, as well as technical requirements for the server.

Chapter 14: Avaya Session Border Controller deployment

Overview of the Avaya Session Border Controller for Enterprise

The Avaya SBCE delivers security to a SIP-based Unified Communications network. It is available in two versions: Advanced Services and Basic Services.

Advanced Services is a highly specialized Unified Communications (UC) security product that protects all IP-based real-time multimedia applications, endpoints and network infrastructure from potentially catastrophic attacks and misuse. It provides the real-time flexibility to harmonize and normalize all types of enterprise communications traffic to maintain the highest levels of network efficiency and security.

Basic Services provides a subset of the functionality of the Advanced Services offer. It has all the functionality required for an enterprise to terminate SIP trunks without the complexity and higher price associated with typical SBCs.

ASBCE can be deployed in enterprise communications and in service provider networks.

For more information, see the relevant documentation at http://support.avaya.com.

ASBCE deployment checklist

This chapter describes how to configure the ASBCE for conferencing with Equinox Meet Me and Meetings for Web clients.

Guest clients who need to participate in conferences have to interact with multiple components. 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. The URL rewriting can be used in all Equinox deployments.

For a full explanation on configuring the ASBCE, download the following documents from the Avaya Support website at http://support.avaya.com

- *Deploying Avaya Session Border Controller in Virtualized Environment*

- *Administering Avaya Session Border Controller for Enterprise*

Use this checklist to deploy and configure the ASBCE for URL rewriting.

Table 33: Checklist for deploying the ASBCE

No.	Task	Link/Notes	✔
1	Deploy the ASBCE in a virtualized environment	See Deploying the ASBCE in a virtualized environment on page 231	
2	Configure licenses for ASBCE deployment	See Configuring licenses for ASBCE deployment on page 237	
3	Configure ASBCE TLS certificates	See Configuring ASBCE TLS management certificates on page 237	
4	Associate a certificate with client and server profiles	See Associating a certificate with the TLS Client and Server Profiles on page 238	
5	Configure the ASBCE interfaces	See Configuring the ASBCE interfaces on page 239	
6	Configure multiple server access using a single FQDN, a single IP address, and port 443	See Configuring the ASBCE for remote access to multiple servers using a single FQDN and a single IP address on page 240	
7	Configure the ASBCE STUN TURN Server	See Configuring the ASBCE STUN TURN server on page 246	
8	Configure the ASBCE in Avaya Equinox Management	See Configuring the ASBCE in Equinox Management on page 247	

Deploying the ASBCE in a virtualized environment

About this task

To install the ASBCE, you must download the .ova file and install it, using the following procedure.

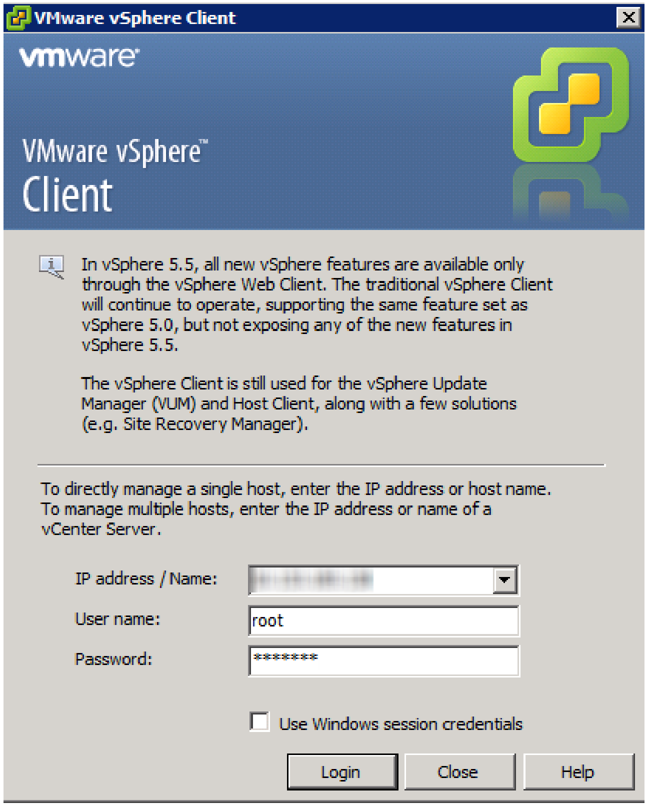
For additional details on virtual deployment, refer to *Deploying the Avaya Session Border Controller in Virtualized Environment* and *Administering Avaya Session Border Controller for Enterprise*.

Before you begin

Ensure that you have successfully installed the Equinox Management server .ova (see Deploying the Equinox Management Server on page 91).

Procedure

1. Copy the ASBCE .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.



VMware vSphere Client

vmware

VMware vSphere™
Client

In vSphere 5.5, all new vSphere features are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0, but not exposing any of the new features in vSphere 5.5.

The vSphere Client is still used for the vSphere Update Manager (VUM) and Host Client, along with a few solutions (e.g. Site Recovery Manager).

To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.

IP address / Name: [redacted]

User name: root

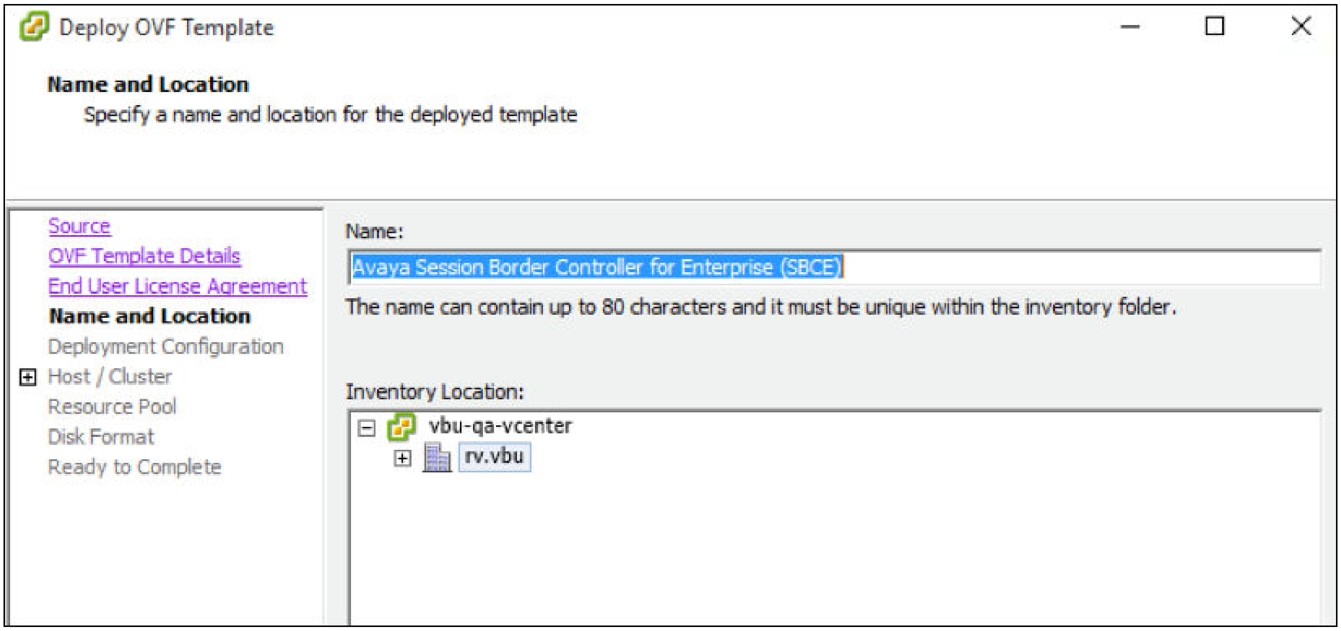
Password: ********

□ Use Windows session credentials

Figure 117: vSphere Client

3. Select **Login**. The vSphere Client page opens, where you select **File** > **Deploy OVF Template** to upload the .ova file.
4. Select the local ASBCE .ova file, and select **Next** to open the **Deploy OVF Template** wizard. The **OVF Template Details** page opens, displaying the product information.
5. Verify that the information is correct, and select **Next**.

   The **End User License Agreement** page opens.
6. Select **Accept** to accept the license agreement, and select **Next**. The **Name and Location** page opens.



Name and Location

Specify a name and location for the deployed template

Name: Avaya Session Border Controller for Enterprise (SBCE)

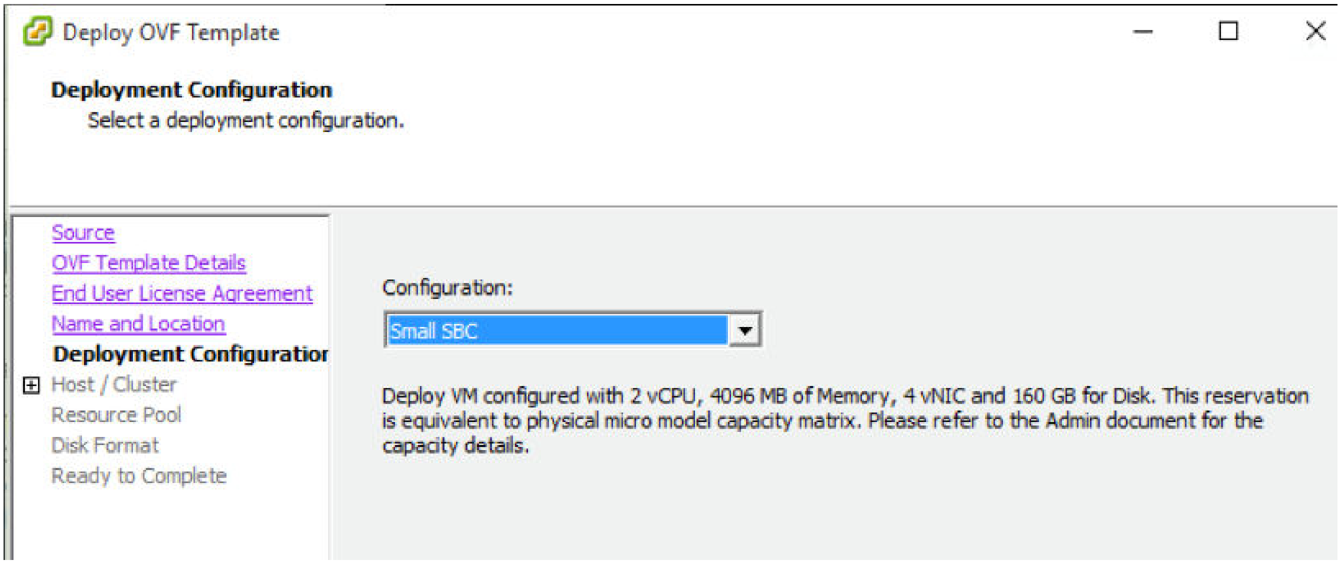
The name can contain up to 80 characters and it must be unique within the inventory folder.

Inventory Location:

Figure 118: Name and Location Page

7. Enter a name for the ASBCE machine in the **Name** field, and select **Next**.

   The **Deployment Configuration** page opens.



Deployment Configuration

Select a deployment configuration.

Configuration: Small SBC

Deploy VM configured with 2 vCPU, 4096 MB of Memory, 4 vNIC and 160 GB for Disk. This reservation is equivalent to physical micro model capacity matrix. Please refer to the Admin document for the capacity details.

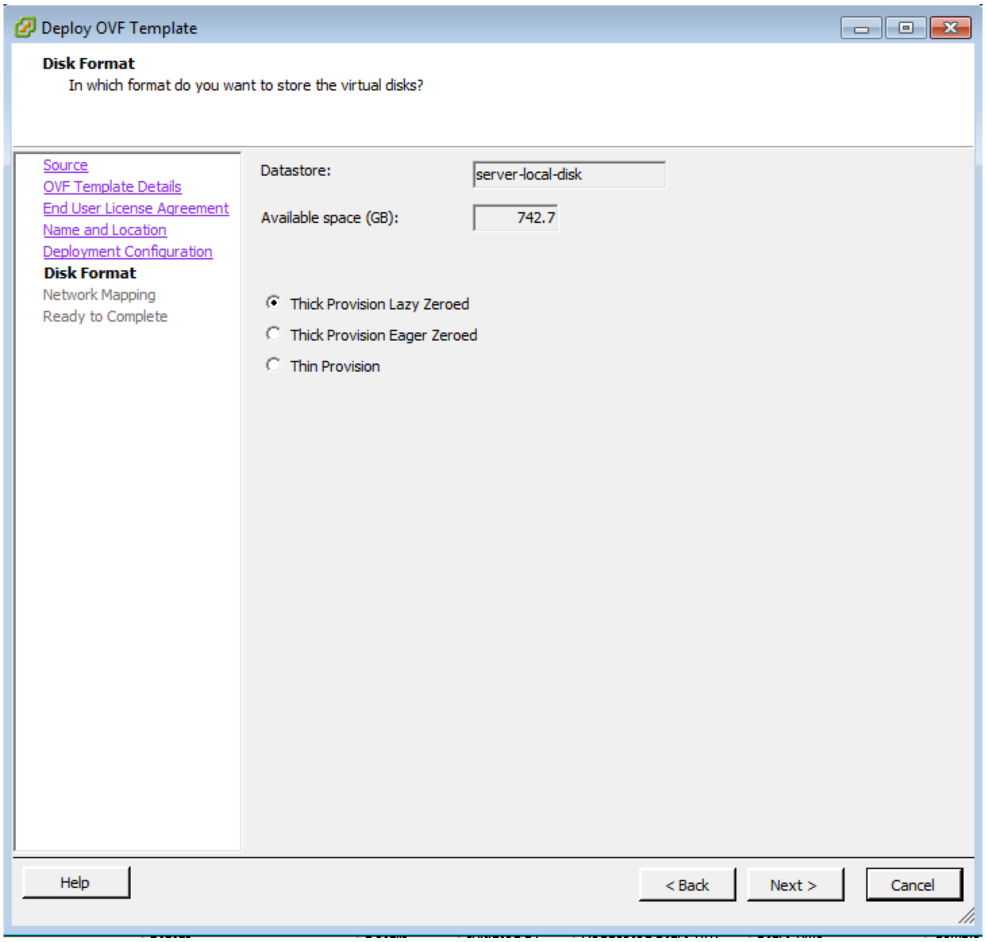
Figure 119: Deployment Configuration Page

8. In the **Configuration** field, select the relevant Equinox Management server based on your environment's needs. Select from the following:

   - **Small SBC**: For smaller deployments reserved with minimum resources. With the **Small SBC** option, you can achieve lower capacity, but some features such as HA will not work. For the Small SBC deployment option, the M1, A1, A2, and B1 interfaces are available.

- **Large SBC**: For large deployments reserved with maximum resources. Using the **Large SBC** option is preferable when you require features such as HA. For the Large SBC deployment option, the M1, M2, B1, B2, A1 and A2 interfaces are available.

9. Select **Next**. The **Disk Format** page opens.



Deploy OVF Template

Disk Format

In which format do you want to store the virtual disks?

Datastore: server-local-disk

Available space (GB): 742.7

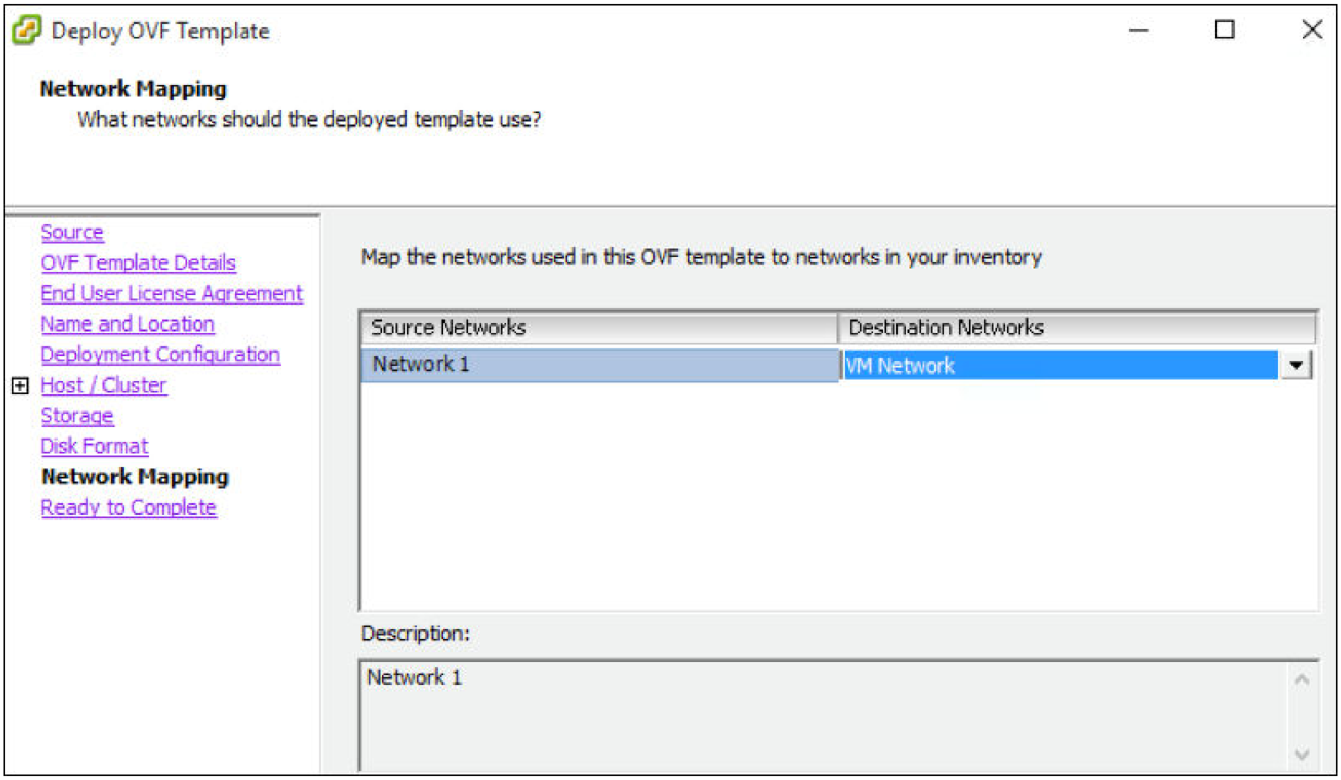
● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

Figure 120: Disk Format Page

10. Select **Thick Provision Lazy Zeroed** and select **Next**. The **Network Mapping** page opens.



Deploy OVF Template

Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

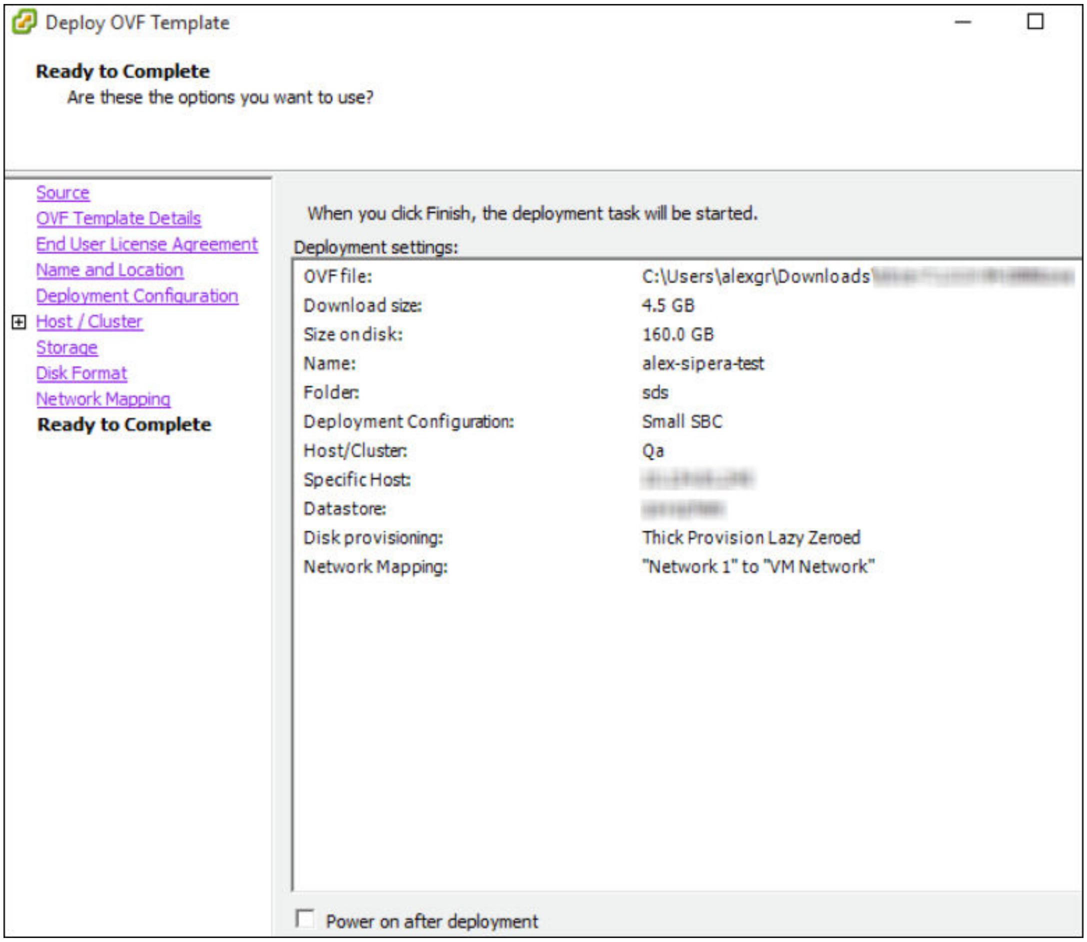
Source Networks	Destination Networks
Network 1	VM Network

Description:

Network 1

Figure 121: Network Mapping Page

11. Select a network that is accessible for the administrator, and select **Next**. The **Ready to Complete** page opens, displaying your deployment settings.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\Users\alexgr\Downloads[redacted]
Download size:	4.5 GB
Size on disk:	160.0 GB
Name:	alex-sipera-test
Folder:	sds
Deployment Configuration:	Small SBC
Host/Cluster:	Qa
Specific Host:	[redacted]
Datastore:	[redacted]
Disk provisioning:	Thick Provision Lazy Zeroed
Network Mapping:	"Network 1" to "VM Network"

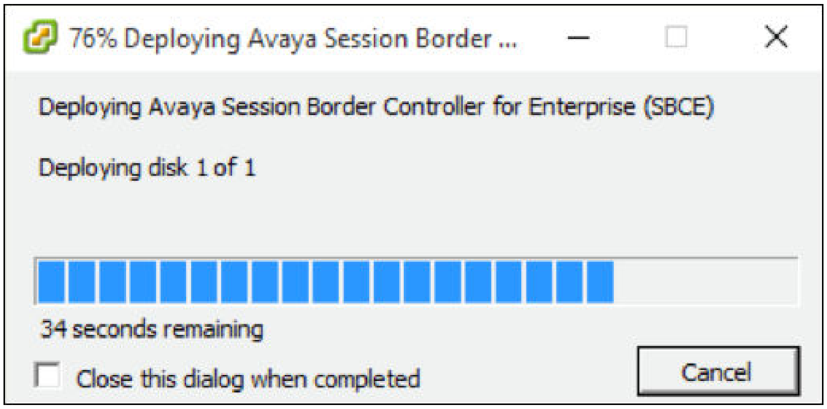
□ Power on after deployment

Figure 122: Ready to Complete Page

Optionally, select the **Power on after deployment** check box to activate the ASBCE server after completing deployment.

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

    The system deploys the .ova to the ASBCE host server.



Deploying Avaya Session Border Controller for Enterprise (SBCE)

Deploying disk 1 of 1

34 seconds remaining

□ Close this dialog when completed

Figure 123: Deploying the OVA

Configuring licenses for ASBCE deployment

About this task

This procedure enables you to configure a license for ASBCE using a web browser.

For additional details on configuration, refer to the sections in *Administering Avaya Session Border Controller for Enterprise* that explain the following concepts:

- Administrative user accounts
- Device configuration
- Domain policy, routing, and message flow administration
- System configuration

For details on licensing requirements, refer to the *Deploying Avaya Session Border Controller in Virtualized Environment* guide.

Procedure

1. Enter the following in a browser window:

   ```
   https://<IP Address>
   ```

   or

   ```
   https://<FQDN>
   ```

   If the certificate is not recognized by the system, accept it and proceed when prompted. The Avaya Session Border Controller for Enterprise login page appears.

2. Enter your login credentials. You are prompted to change your password when logging in for the first time.

   The **Dashboard** appears.

3. Select **System Management**.

   The **Licensing** tab page appears.

4. In the **External WebLM Server URL** field, enter a license.
5. Select **Save** and then **Refresh**.

   Your license is added.

6. Navigate to **System Management** > **Devices** and select **Install**.

Configuring ASBCE TLS management certificates

About this task

This procedure enables you to deploy and install an identity certificate on ASBCE. For details on certificates, refer to TLS Management in *Administering Avaya Session Border Controller for Enterprise*.

Procedure

1. In the ASBCE UI, select **TLS Management** > **Certificates**.

   The **Certificates** tab page appears.

2. Select the **Generate CSR** button.

   The **TLS Management Generate CSR** window appears.

3. Enter the relevant information in the TLS Management Generate CSR window and select **Generate CSR**.

   Ensure that the **Key Encipherment** and **Digital Signature** check boxes are selected.

Associating a certificate with the TLS Client and Server Profiles

About this task

After you deploy and install an ASBCE identity certificate, you must associate the certificate with the ASBCE Client and Server Profiles.

There are two types of certificates to install in the ASBCE: the third party certificate and the self-signed CA (Certificate Authority) certificate. Before installing the third party certificate, you need to create a Certificate Signing Request (CSR), send the CSR to the external CA for signing, and then upload the signed certificate to the ASBCE from its Certificates page. When the third party certificate is installed, you can view it in the page’s Installed Certificates section. After you install the self-signed certificates, you can view them in the page’s Installed CA Certificates section.

The ASBCE acts as a server for processing a connection from a remote client calling into the browser and uses the third-party certificate for the connection. The ASBCE acts as a client when connecting to other components in the deployment, like the User Portal, Web Gateway, Management, and media server. The self-signed CA certificates are used for these connections.

For detailed information on certificates and TLS profile management, refer to *Administering Avaya Session Border Controller for Enterprise*.

Procedure

1. On the ASBCE UI, select **TLS Management** > **Client Profiles** and select **Add**.
2. In the **Profile Name** field, enter a name for the profile.
3. In the **Certificate** field, select the installed CA certificate that you want to associate with the profile.
4. Configure information in the remaining fields, as needed, and select **Next**.
5. Select the relevant TLS versions, as needed, and select **Finish**.

   The client profile appears on the **Client Profile** page.

6. Select **TLS Management** > **Server Profiles** and select **Add**.

7. In the **Profile Name** field, enter a name for the profile.
8. In the **Certificate** field, select the installed certificate that you want to associate with the profile.
9. Configure information in the remaining fields, as needed, and select **Next**.
10. Select the relevant TLS versions, as needed, and select **Finish**.

    The server profile appears on the **Server Profile** page.

Configuring the ASBCE interfaces

About this task

Refer to 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. On the ASBCE UI, navigate to **Device Specific Settings** > **Network Management**.

   For the examples used in the deployment described in this chapter, you need:

   - One IP address for the external interface (B1, 150.50.0.1)
   - One IP address for the internal interface (A1, 10.0.0.21)
   - One IP address for listeners on the internal interface (A1, 10.0.0.22)

   Configure the fields as follows:

   - On the **Interfaces** page, under **Status**, mark at least two interfaces as **Enabled**.
   - OIn the **Networks** page, configure the IP Addresses for each ASBCE network interface.
2. Navigate to **Device Specific Settings** > **Signaling Interface** and select **Add**.

   Configure the internal and external signaling interfaces fields as follows:

   - In the **Name** field, enter a name for the signaling interface.
   - In the **IP Address** field, select an interface in the upper dropdown box, and an IP address protocol in the lower dropdown box.
   - In the **TLS Port**, enter `5061`
   - In the **TLS Profile**, select the ASBCE profile.

3. Navigate to **Device Specific Settings** > **Media Interface** and select **Add**.

   Configure the external and internal media interface fields as follows.

   - In the **Name** field, enter a name for the external media interface (B1).
   - In the **IP Address** field, select an interface in the upper dropdown box, and an IP address protocol in the lower dropdown box.
   - In the **Port Range** field, enter the port range `53001 — 55000`.

4. Navigate to **Device Specific Settings** > **End Point Flows** > **Server Flows** and select **Add**.

   Configure the fields as follows:

   - In the **Flow Name** field, enter the flow name.
   - In the **Server Configuration** field, select the server name.
   - In the **Received Interface** field, select the internal signaling interface.
   - In the **Signaling Interface** field, select the internal signaling interface.
   - In the **Media Interface** field, select the external media interface.
   - Select the relevant **Endpoint Policy Group**.
   - Leave other fields with their default values.

5. Navigate to **Device Specific Settings** > **Session Flows** and select **Add**.

   Configure the fields as follows:

   - In the **Flow Name** field, enter the flow name.
   - Ensure that the **Has Remote SBC** check box is unchecked.
   - Leave other fields with their default values.

Configuring the ASBCE for remote access to multiple servers using a single FQDN and a single IP address

Guest clients who need to participate in conferences have to interact with multiple components. Each component has its own IP address and FQDN. The URL rewriting method solves this interfacing complexity by enabling 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.

The following is an example of requirements when implementing the URL rewriting method.

Servers and services

These servers and services utilize HTTPS:

- User Portal (part of the Avaya Aura® Web Gateway server). This example describes a centric OTT deployment, so the User Portal is part of the Equinox Management Server.
- Equinox Conference Control (also called UCCS, part of the Equinox Management Server).
- Web Collaboration Server (WCS). It can be part of the audio and video Equinox Media Server, the high capacity audio Equinox Media Server, or be a standalone WCS. Multiple WCSs are deployed for scalability and high capacity. Each server has a unique IP address and unique FQDN. The Equinox Management Server is doing the load balancing among the multiple WCSs.
- Avaya Session Border Controller for Enterprise (ASBCE). The server is used for its three functionalities: reverse proxy, SBC, and STUN/TURN.

The following table lists the details of the servers used in this example.

Table 34: Defining server IP addresses and FQDNs

Type of server	Server IP address	Server FQDN	Listening port
Equinox Management Server 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	
ASBCE	150.50.0.1	equinox.mydomain.com	

Note:

- 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.

The numerous guests behind the firewall can access the User Portalthat listens to queries on port 443. The Equinox Management Server NGinx acts as a reverse proxy for the server and forwards the User Portal traffic to the portal's internal port and the UCCP traffic to Equinox Conference Control. The WCS always uses port 443.

Firewall traversal

The setup uses a split horizon DNS and the reverse proxy for firewall traversal, and the same URL for both internal and external calls. In this example, the internal DNS resolves wcs1.mydomain.com to 10.0.0.11, while the external DNS resolves the same FQDN to reach the reverse proxy external leg.

URLs

Each service uses a different path in its URL. 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.

Related links

Configuring multiple server access using URL rewriting on page 242

Configuring multiple server access using URL rewriting

About this task

The URL rewriting method enables using a single FQDN and a single IP address for accessing multiple media and management servers, via port 443. This procedure explains how to configure the components used in the deployment.

Before you begin

You must set up and configure the solution components as described in the server documentation. The following procedure is an example of configuration and describes only a few of the Equinox Management, WCS, and ASBCE settings that are required for the deployment.

Procedure

1. Configure Equinox Conference Control and the User Portal/Web Gateway in Equinox Management.
    a. To configure Equinox Conference Control, navigate to **Dashboard > ☰ > Advanced Parameters** and enter the following parameters in the fields:
        - **Property Name**: scroll down the **Core Properties** list and select `com.visionnex.vcms.core.uccp.customizedUCCPURL`.
        - **Property Value**: enter `https://equinox.mydomain.com:443/uwd/ws?ticket=`

    b. To configure client access from the User Portal/Web Gateway, navigate to **Settings > User Portal/Web Gateway > Portal Setting > Client Connection** and enter the following parameters in the fields:
        - **Frontend FQDN** : `equinox.mydomain.com`
        - **Frontend Port**: `443`

    c. To configure a management connection, navigate to **Settings > User Portal/Web Gateway > Portal Setting > Management Connection** and enter the following parameters in the fields:
        - **Frontend FQDN** : `app.mydomain.com`
        - **Frontend Port** : `8446`
2. To configure WCS1 in Equinox Management, navigate to **Devices > Devices by Type > WCS1 (or WCS1 media server) > Configuration** and enter the following parameters in the fields:
    - **Service FQDN** and **Local FQDN**: `wcs1.mydomain.com`
    - **Public URL Branch**: `equinox.mydomain.com`

Repeat the configuration for each WCS (or WCS media server) that is part of the deployment. The Public URL Branch setting is identical for every additional WCS.

3. Configure the external and internal rules in the ASBCE UI.

   ✱ **Note:**

   - As a pre-requisite, 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.

   a. Navigate to **System Management > Device Specific Settings > DMZ Services > Relay Services > Reverse Proxy**.

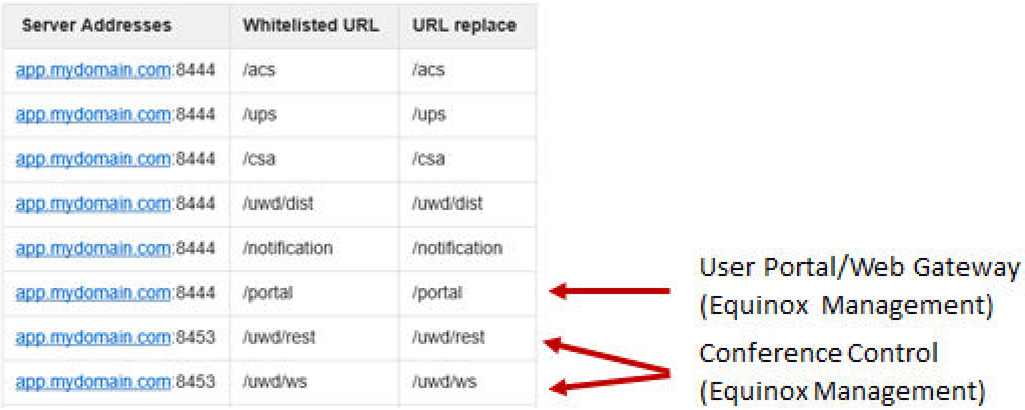
   b. Select **Add** to create the external Reverse Proxy Profile.

      Configure the following parameters:

      - **Name**: enter a descriptive name.
      - **Listen IP**: select the external media interface and the ASBCE external leg IP address (**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 (**10.0.0.21**) .
      - **Server TLS Profile**: select **client**.
      - Enable the **Rewrite Rule** checkbox.

   c. 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.



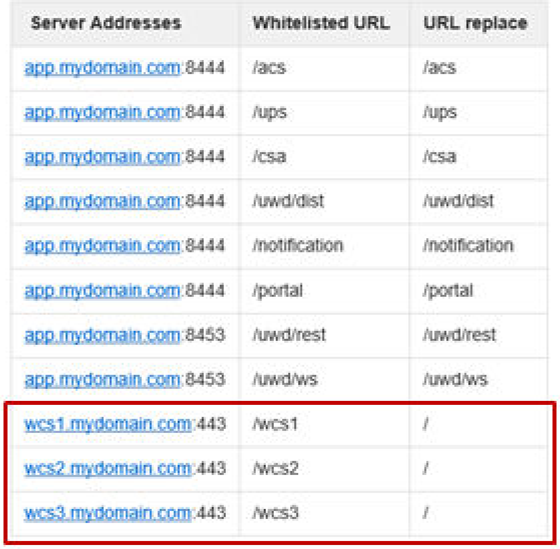
Server Addresses	Whitelisted URL	URL replace
app.mydomain.com:8444	/acs	/acs
app.mydomain.com:8444	/ups	/ups
app.mydomain.com:8444	/csa	/csa
app.mydomain.com:8444	/uwd/dist	/uwd/dist
app.mydomain.com:8444	/notification	/notification
app.mydomain.com:8444	/portal	/portal
app.mydomain.com:8453	/uwd/rest	/uwd/rest
app.mydomain.com:8453	/uwd/ws	/uwd/ws

Figure 124: Creating external URL rewrite rules for the User Portal/Web Gateway and Equinox Conference Control

d. Select **Add** at the bottom of the page to create an external rewriting rule for WCS1 (or WCS1 media server).

Configure parameters as shown in the figure below. In the **URL replace** column, enter a trailing slash (/). The system replaces the whitelisted URL parameter with the server address.

Repeat the configuration for each WCS (or WCS media server) that is part of the deployment.



Server Addresses	Whitelisted URL	URL replace
app.mydomain.com:8444	/acs	/acs
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:8453	/uwd/rest	/uwd/rest
app.mydomain.com:8453	/uwd/ws	/uwd/ws
wcs1.mydomain.com:443	/wcs1	/
wcs2.mydomain.com:443	/wcs2	/
wcs3.mydomain.com:443	/wcs3	/

Figure 125: Creating an external URL rewrite rule for WCS1 (or WCS1 media server)

e. Select **Finish** to save the external rules.

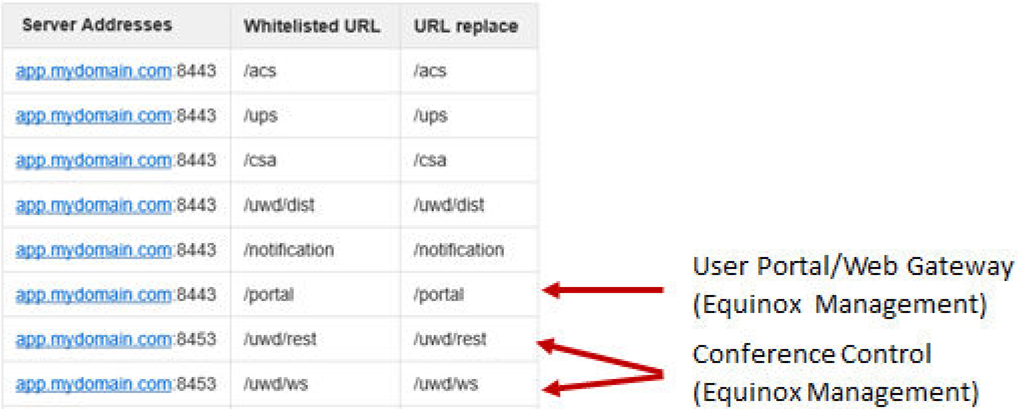
f. In the **Reverse Proxy** tab, select **Add** to create the internal Reverse Proxy Profile.

Configure the following parameters:

- **Name**: enter a descriptive name.
- **Listen IP**: select the internal media interface and the ASBCE internal leg IP address (**10.0.0.22**).
- **Connect IP**: select the internal media interface and select the ASBCE internal leg IP address (**10.0.0.21**).
- Configure the **Listen Port**, **Listen TLS Profile**, **Server TLS Profile**, and **Rewrite Rule** fields, as explained for the external Reverse Proxy Profile above.

g. 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 figure below. The system appends the parameter in the **URL replace** column to the server address.



Server Addresses	Whitelisted URL	URL replace
app.mydomain.com:8443	/acs	/acs
app.mydomain.com:8443	/ups	/ups
app.mydomain.com:8443	/csa	/csa
app.mydomain.com:8443	/uwd/dist	/uwd/dist
app.mydomain.com:8443	/notification	/notification
app.mydomain.com:8443	/portal	/portal
app.mydomain.com:8453	/uwd/rest	/uwd/rest
app.mydomain.com:8453	/uwd/ws	/uwd/ws

User Portal/Web Gateway (Equinox Management)

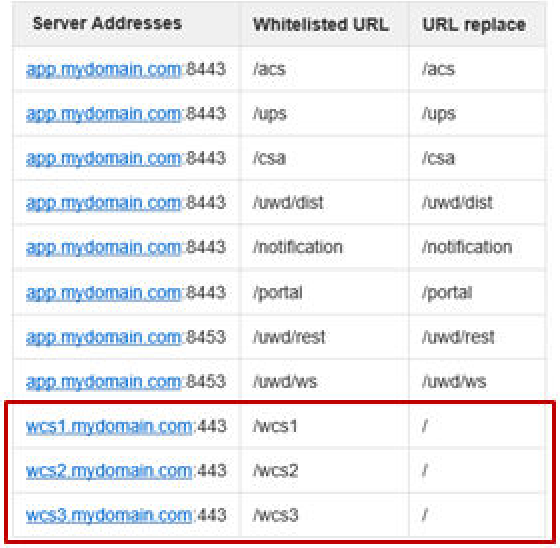
Conference Control (Equinox Management)

Figure 126: Creating internal URL rewrite rules for the User Portal/Web Gateway and Equinox Conference Control

h. Select **Add** at the bottom of the page to create an internal rewriting rule for WCS1 (or WCS1 media server).

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 (or WCS media server) that is part of the deployment.



Server Addresses	Whitelisted URL	URL replace
app.mydomain.com:8443	/acs	/acs
app.mydomain.com:8443	/ups	/ups
app.mydomain.com:8443	/csa	/csa
app.mydomain.com:8443	/uwd/dist	/uwd/dist
app.mydomain.com:8443	/notification	/notification
app.mydomain.com:8443	/portal	/portal
app.mydomain.com:8453	/uwd/rest	/uwd/rest
app.mydomain.com:8453	/uwd/ws	/uwd/ws
wcs1.mydomain.com:443	/wcs1	/
wcs2.mydomain.com:443	/wcs2	/
wcs3.mydomain.com:443	/wcs3	/

Figure 127: Creating an internal URL rewrite rule for WCS1 (or WCS1 media server)

i. Select **Finish** to save the internal rules.

Related links

Configuring the ASBCE for remote access to multiple servers using a single FQDN and a single IP address on page 240

Configuring the ASBCE STUN TURN server

About this task

This procedure describes how to configure the ASBCE STUN TURN server that Equinox Meetings for Web (WebRTC) clients use for media connection. Refer to the *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 Settings**.
2. Select **Add**.

   The **Modify TURN STUN Server Configuration** page opens.
3. In the **List Port** field, enter `3478`.
4. In the **Media Relay Port Range** field, enter the port range.
5. In the **Alternate Server** fields, enter the IP address to be used by the server, as needed.

6. Configure other fields as required, and select **Finish**.

   The results display on the **TURN STUN Configuration** page.

7. Select **Add Listen/Relay IP Pair** and configure the network's Listen IP and Media Relay IP addresses through which data will pass.
8. Save your configurations.

Configuring the ASBCE in Equinox Management

About this task

This procedure describes how to add the ASBCE to Equinox Management.

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*.

Procedure

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

   The **Add ASBCE** page appears.

3. In the **Name** field, enter a name for the ASBCE server.
4. In the **IP Address** field, enter the IP address of the ASBCE management interface (M1).
5. In the **Location** field, select the location of the ASBCE server, as defined in Equinox Management.
6. Select **OK**.

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

7. Select the ASBCE name in the ASBCE list and configure additional settings.

   The **Update ASBCE** page appears.

8. Configure the 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 ASBCE server's internal IP address (A1)
   - **SIP protocol**: select TLS

- **SIP port**: enter 5061
- **Check status IP**: enter the ASBCE server’s internal IP address (A1)
- **Check status protocol**: select **Http** or **Https**.

9. Select **OK**.

Chapter 15: Equinox H.323 Edge deployment

Equinox H.323 Edge 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.

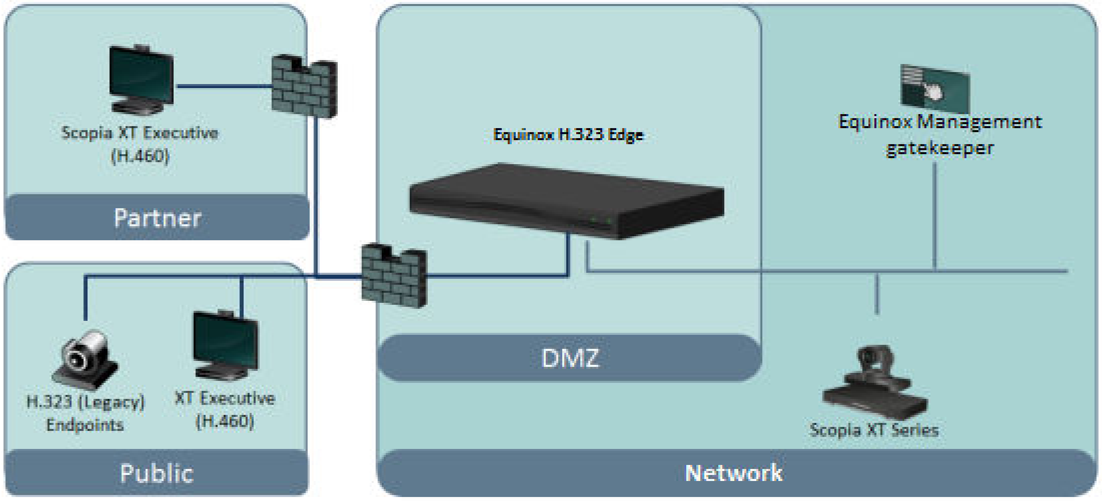
Note:

Deploy Equinox H.323 Edge only in legacy Avaya Scopia solution deployments which use the H.323 protocol.

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 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.

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 hardware server deployment checklist

#	Action	Link/Notes	✔
1	• Check the site to ensure that the site is suitable for the Equinox H.323 Edge server installation. • Unpack the Equinox H.323 Edge server and check for damages. • Mount the Equinox H.323 Edge server onto the rack.	See *Rack Mounting Guide for Avaya Equinox H.323 Edge*	

#	Action	Link/Notes	✔
	• Connect the power and serial cables to the Equinox H.323 Edge server.		

Equinox H.323 Edge virtual server deployment checklist

#	Action	Link/Notes	✔
1	Download the Equinox H.323 Edge software from PLDS	See Downloading software from PLDS on page 90	
2	Deploy the Equinox H.323 Edge virtual server	See Deploying the Equinox H.323 Edge virtual server on page 258	
3	Start the Equinox H.323 Edge virtual server	See Starting the Equinox H.323 Edge virtual server on page 259	
4	Configure the Equinox H.323 Edge virtual server automatic startup settings	See Configuring the virtual machine automatic startup settings on page 192	

Equinox H.323 Edge initial configuration checklist

No.	Task	Link/Notes	✔
1	Configure IP separation of the internal and external network traffic on the Equinox H.323 Edge hardware server.	See Configuring the IP addresses on page 260	
2	Add more networks to the Equinox H.323 Edge virtual server.	See Adding networks to the Equinox H.323 Edge virtual server on page 264	
3	Configure IP separation of the internal and external network traffic on the Equinox H.323 Edge virtual server	See Configuring IP separation of the Equinox H.323 Edge virtual server on page 266	
4	Configure the ports on Equinox H.323 Edge	See Configuring Ports on Equinox H.323 Edge on page 268	
5	Configure the gatekeeper	See Integrating with the gatekeeper on page 270	
6	Configure NAT	See Integrating with NAT on page 270	
7	Configure the NTP server	See Configuring the NTP server on page 271	

Table continues…

No.	Task	Link/Notes	✔
8	Configure access to calls to H.323 legacy endpoints	See Configuring access for calls to H.323 legacy endpoints on page 272	
9	Configure URI-based dialing	See URI Dialing Functionality on page 273	
10	Configure IP address-based dialing	See Configuring IP address-based dialing to external endpoints on page 276	
11	Secure the connection with Equinox Management	See Secure connection with Equinox Management on page 279	
12	Update the Equinox H.323 Edge license	See Adding or updating licenses on page 283	
13	Configure remote access to administer Equinox H.323 Edge from Equinox Management	See Configuring remote access on page 284	
14	Configure QoS	See Configuring QoS for audio and video on page 286	

Technical specifications of the Equinox H.323 Edge server

This section lists important information about the device you purchased. Refer to this information when preparing system setup and afterwards to verify that the environment still complies with these requirements.

This information lists the technical specifications of the Equinox H.323 Edge server.

- System power requirements:
    - 600W, 100-240VAC input, 50/60Hz auto-switched
- Environmental requirements:
    - Operating temperature: 5°C to 35°C (41°F to 95°F)
    - Humidity: 8% to 90% non-condensing
    - Storage and transit temperature: -40°C to 60°C (-40°F to 140°F)
- Physical dimensions:
    - Size: 437mm (17.2”) width x 43mm (1.7”) height x 650mm (25.6”) depth
    - Weight: ~16.3kg (~36lbs)
- External interfaces:
    - Dual Gigabit NICs
    - 1 x DB9 serial port connector

  - 4 x USB 2.0 connectors
- Communications:
  - H.323
  - IPv4
  - Bit rate: up to 4Mbps per call
- Call capacity:
  - Up to 100 concurrent calls
  - Up to 600 registered devices
- Load balancers for clusters:
  - 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 includes an installation of Equinox H.323 Edge Client, you can tunnel communication through the firewall securely by routing traffic via Equinox H.323 Edge Client.
- Security:
  - H.235 for call privacy in all traversal modes (H.460, tunneling, 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 128: H.323 connections to Equinox H.323 Edge on page 254).

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 128: H.323 connections to Equinox H.323 Edge on page 254).

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).

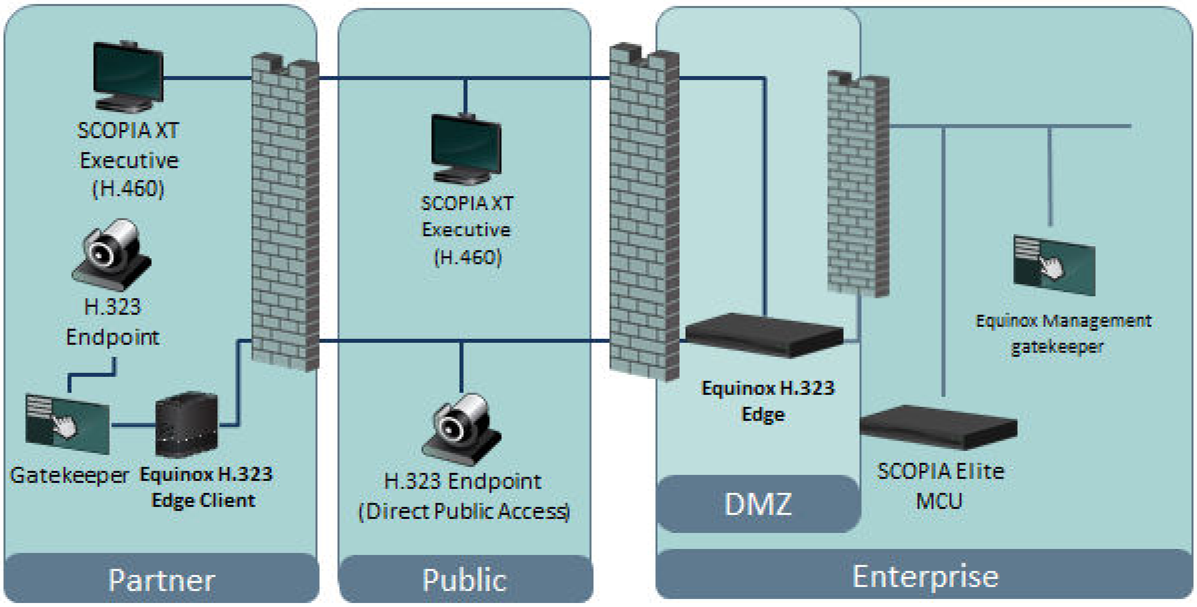

SCOPIA XT Executive (H.460)
H.323 Endpoint
Gatekeeper
Equinox H.323 Edge Client
Partner
SCOPIA XT Executive (H.460)
H.323 Endpoint (Direct Public Access)
Public
Equinox H.323 Edge
DMZ
Equinox Management gatekeeper
SCOPIA Elite MCU
Enterprise

Figure 128: 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 35: Bidirectional Ports to Open Equinox H.323 Edge on page 255.
- If opening ports that are both to and from Equinox H.323 Edge Client, see Table 36: Bidirectional Ports to Open on the Equinox H.323 Edge Client on page 257.

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 129: Contacting Equinox H.323 Edge from within the enterprise on page 255), you must do one of the following:

- Install Equinox H.323 Edge Client within the enterprise
- Use H.460-enabled endpoints
- Open the internal firewall to Equinox H.323 Edge (12000 to 15000, bidirectional)

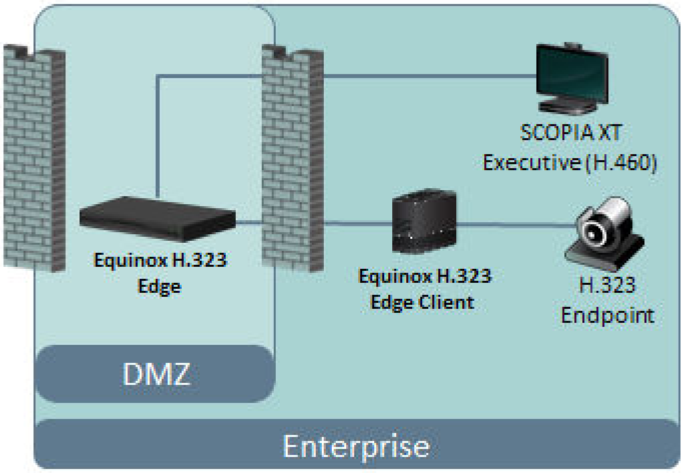


Figure 129: Contacting Equinox H.323 Edge from within the enterprise

Important:

The specific firewalls to open ports depends on where Equinox H.323 Edge Client and other Avaya Equinox Solution components are deployed.

Table 35: Bidirectional Ports to Open Equinox H.323 Edge

Port Range	Protocol	Source	Functionality	Result of Blocking Port	Required
22	SSH/SFTP (TCP)	SSH client endpoint	Enables initial configuration, log download and server upgrade	Cannot initialize the server, download logs and upgrade the server	Mandatory for configuring Equinox H.323 Edge
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
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	H.460.18 endpoints cannot register through Equinox H.323 Edge or set up logical channels. Firewall traversal function based on H.460.18 and H.	Mandatory for H. 460 endpoints

Table continues…

Port Range	Protocol	Source	Functionality	Result of Blocking Port	Required
				460.19 cannot function.	
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 268
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 36: 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

When you place an order for an Avaya PLDS-licensed software product, PLDS creates the license entitlements of the order and sends an email notification to you. The email includes a license activation code (LAC) and instructions for accessing and logging into PLDS. Use the LAC to locate and download the purchased license entitlements.

In addition to PLDS, you can download the product software from http://support.avaya.com using the **Downloads and Documents** tab at the top of the page.

Note:

Only the latest service pack for each release is posted on the support site. Previous service packs are available only through PLDS.

Procedure

1. Enter http://plds.avaya.com in your Web browser to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS home page, select **Assets**.
4. Click **View Downloads**.
5. Click on the search icon (magnifying glass) for **Company Name**.

6. In the **%Name** field, enter **Avaya** or the Partner company name.
7. Click **Search Companies**.
8. Locate the correct entry and click the **Select** link.
9. Enter the Download Pub ID.
10. Click **Search Downloads**.
11. Scroll down to the entry for the download file and click the **Download** link.
12. In the **Download Manager** box, click the appropriate download link.

    Note:

    The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.
13. If you use Internet Explorer and get an error message, click the **install ActiveX** message at the top of the page and continue with the download.
14. Select a location where you want to save the file and click **Save**.
15. If you used the Download Manager, click **Details** to view the download progress.

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, the wizard prompts you to associate networks specified in the OVA with networks available on the host.

Important:

- Ensure that you configure the internal network only to the physical NIC with the eth0 interface. Verify that the MAC addresses of eth0 and the network adapter match.
- If you want to configure Equinox H.323 Edge with a single NIC, do not enable the eth1 interface.

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 **Thin Provision**.
12. Click **Next** to display the Ready to Complete window.
13. Verify the deployment settings.

    If you need to modify any of the settings, use the **Back** option.
14. 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

This procedure does not apply for deployments and upgrades of applications running on Appliance Virtualization Platform.

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

Configuring the IP addresses of the Equinox H.323 Edge hardware server

About this task

There are two network cards (NICs) in Equinox H.323 Edge to enable deploying it with better security and management of network traffic:

- NIC 1 (Ethernet port defined as *eth0*) always supports the external traffic.
- NIC 2 (Ethernet port defined as *eth1*) is always dedicated to the internal network traffic.

For a highly secure dual-NIC deployment we recommend to also configure the management role to *eth1*. This procedure describes how to configure this type of topology. Figure 130: The role of the dual-NIC Equinox H.323 Edge in a deployment on page 261 illustrates these roles.

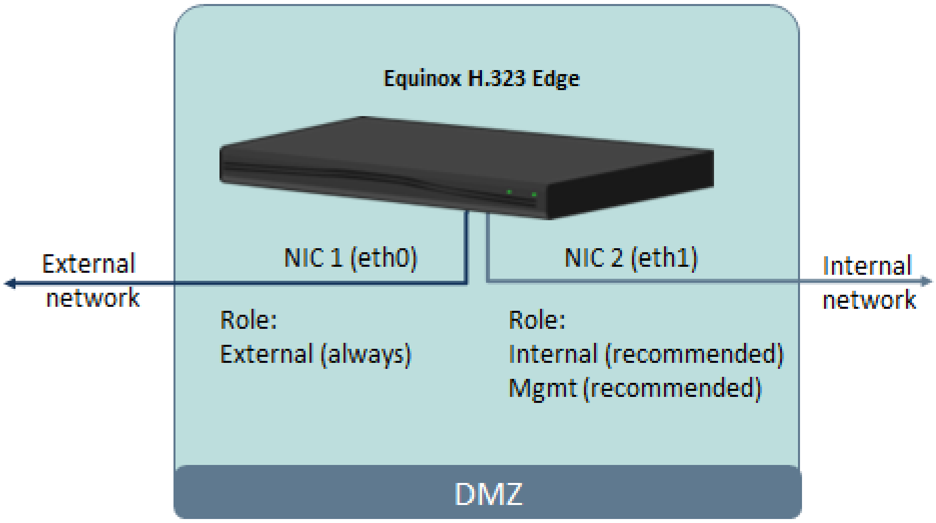


Figure 130: The role of the dual-NIC Equinox H.323 Edge in a deployment

Before you begin

Make sure you have these items:

- A PC with available serial port
- Serial cable provided with your Equinox H.323 Edge. Use the serial port on the server's rear panel to assign the new IP addresses.
- A client program to configure the administration console of your Equinox H.323 Edge using an SSH connection. We recommend using PuTTY. You can download this free application from http://www.chiark.greenend.org.uk/~sgtatham/putty/
- IP address of each NIC in Equinox H.323 Edge
- Dedicated subnet mask for Equinox H.323 Edge

  Important:

  In a dual-NIC deployment, you must connect the NICs to two different subnets.
- IP address of the default router Equinox H.323 Edge uses to communicate over the network
- IP address of the DNS server
- Fully Qualified Domain Name (FQDN) for Equinox H.323 Edge

Procedure

1. Login to the administration shell menu of your Equinox H.323 Edge.
   a. Start PuTTY on your PC
   b. Select the **Serial** page in the **PuTTY Configuration** dialog box.

c. Verify that the connection fields are setup as follows:

Field Name	**Value**
Serial line to connect to	COM1
Speed (baud)	9600
Data bits	8
Stop bits	1
Parity	None
Flow Control	None

d. Turn on the power to your Equinox H.323 Edge.

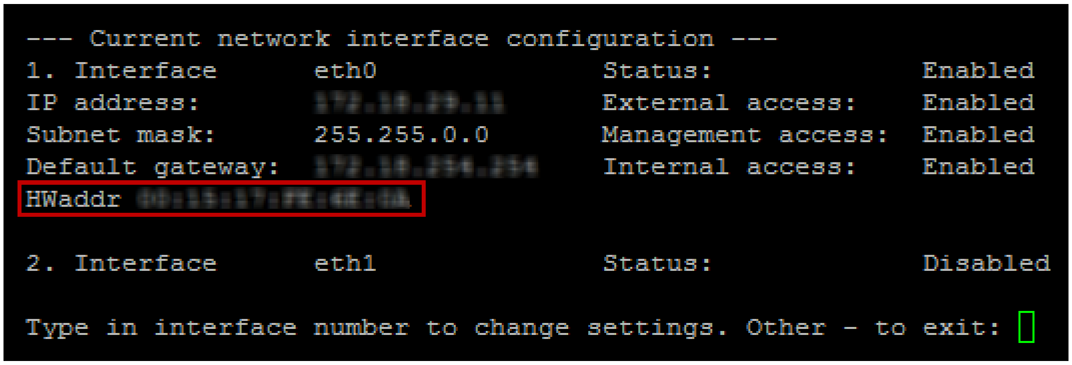
e. When prompted, enter a user name and password to login to Equinox H.323 Edge. The password is encrypted with a 2048-bit key. The default user name and password are both **admin**.

2. Configure the NIC interfaces.

a. Once in the **Main Menu**, enter **2** to access the **Network administration menu**.

b. Enter **2** to access the **Change network configuration menu** (Figure 131: Configuring NIC 0 (external NIC) on page 262).

The display shows the current network interface configuration. The **HWaddr** field displays the MAC address of *eth0*.



```
--- Current network interface configuration ---
1. Interface      eth0                 Status:              Enabled
IP address:       [redacted]           External access:     Enabled
Subnet mask:      255.255.0.0          Management access:   Enabled
Default gateway:  [redacted]           Internal access:     Enabled
HWaddr [redacted]

2. Interface      eth1                 Status:              Disabled

Type in interface number to change settings. Other - to exit:
```

Figure 131: Configuring NIC 0 (external NIC)

c. Enter **1** to configure *eth0*(external NIC 1).

d. Enter the IP address of *eth0*(NIC 1).

e. Enter the IP address of the subnet mask to which *eth0* belongs.

f. Enter the IP address of the default gateway.

The window displays the new settings. The **External access**, **Management access**, and **Internal access** fields are automatically enabled.

External access is enabled so that the NIC can communicate with the external network. Traffic on the NIC typically comprises H.460, tunneling, DNS query traffic, and H.323.

Management access and internal access are automatically disabled after you enable these fields in *eth1*(NIC 2).

g. Enter **2** to configure *eth1*(internal NIC 2).

h. Enter **y** in the **Interface status** to enable *eth1*.

i. Enter the IP address of *eth1*(NIC 2).

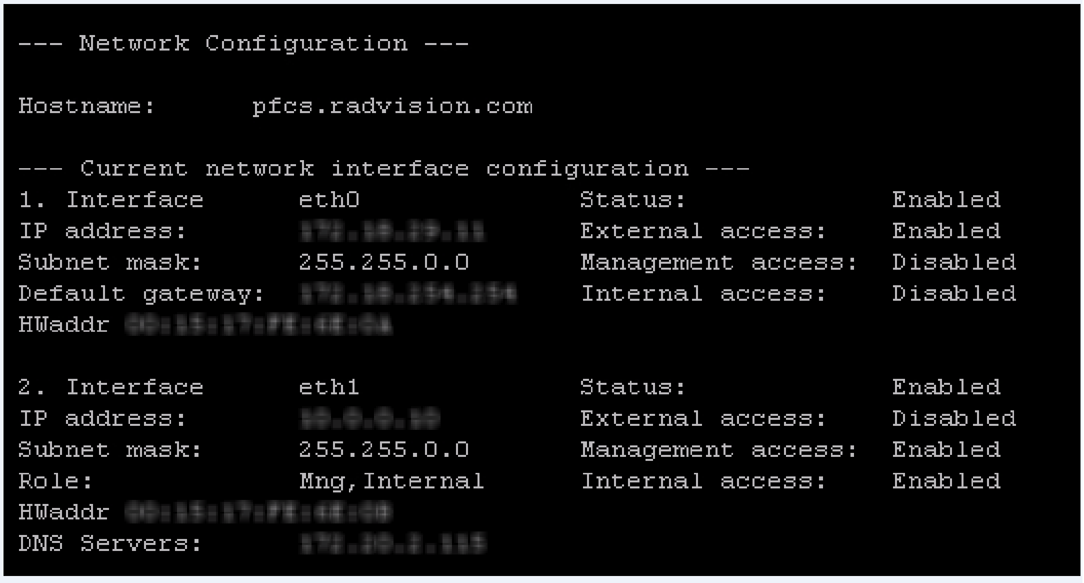
j. Enter the IP address of the subnet mask to which *eth1* belongs.

k. Enter **y** to enable the **Management role** of *eth1*.

l. Enter **y** to enable the **Internal role** of *eth1*.

Field	Description
Internal access	Enable this field so that the NIC can handle standard H. 323 traffic in the internal network.
Management access	Enable this field for the NIC's handling of management traffic such as: • SSH, required for accessing the shell administration menu of Equinox H.323 Edge • SFTP, for uploading or downloading resources of Equinox H.323 Edge • XML over TCP, required for third-party management interface.

The system automatically disables the external role of *eth1*. The window displays the NIC configuration as illustrated in Figure 132: The network interface configuration screen on page 263.



```
--- Network Configuration ---

Hostname:       pfcs.radvision.com

--- Current network interface configuration ---
1. Interface        eth0              Status:              Enabled
IP address:         [redacted]        External access:     Enabled
Subnet mask:        255.255.0.0       Management access:   Disabled
Default gateway:    [redacted]        Internal access:     Disabled
HWaddr [redacted]

2. Interface        eth1              Status:              Enabled
IP address:         [redacted]        External access:     Disabled
Subnet mask:        255.255.0.0       Management access:   Enabled
Role:               Mng,Internal      Internal access:     Enabled
HWaddr [redacted]
DNS Servers:        [redacted]
```

Figure 132: The network interface configuration screen

3. Configure the DNS server as your enterprise DNS server.
    a. In the **Network administration** menu enter **3** to access the DNS configuration menu.
    b. Enter **A** to add a DNS server.
    c. Enter the IP address of the new server.
4. Configure the new FQDN.
    a. In the **Network administration menu**, enter **4** to access the FQDN configuration menu.
    b. Enter the FQDN of Equinox H.323 Edge. The system displays the host name and domain name, as well as the new FQDN of Equinox H.323 Edge.
5. Add a static route to define call paths so that they are redirected from Equinox H.323 Edge to H.323 Gatekeeper and internal endpoints on other subnets.

    A static route is required if the internal network has many subnets. For example:

    - If the internal NIC is in network 168.168.1.10, and all internal endpoints and the H.323 Gatekeeper are also located in network 168.168.1.0, there is no need for a static route.
    - If the internal network has many subnets (such as 168.168.2.0, 172.16.0.0), you need to configure the static route so that Equinox H.323 Edge can communicate with devices inside subnets other than 168.168.1.0.

    a. In the **Network administration** menu enter **6** to access the static route configuration menu.
    b. Enter **A** to add a new static route.
    c. Enter the routing rule as: `<host_ip|network_ip/prefix> via <gateway>>`
6. Close the SSH session.

Adding networks to the Equinox H.323 Edge virtual server

About this task

Add more networks to the Equinox H.323 Edge virtual server to configure:

- IP separation for the external and internal networks.
- Separate subnets for different networks.

This procedure is relevant only if you have a dual NIC deployment of Equinox H.323 Edge.

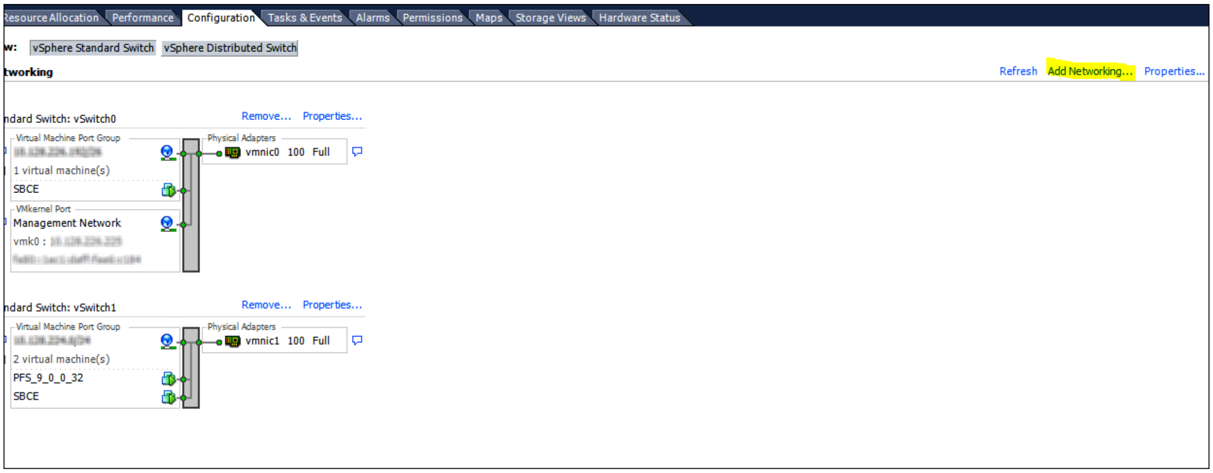
Before you begin

Connect a network cable to the second NIC of the host server.

Procedure

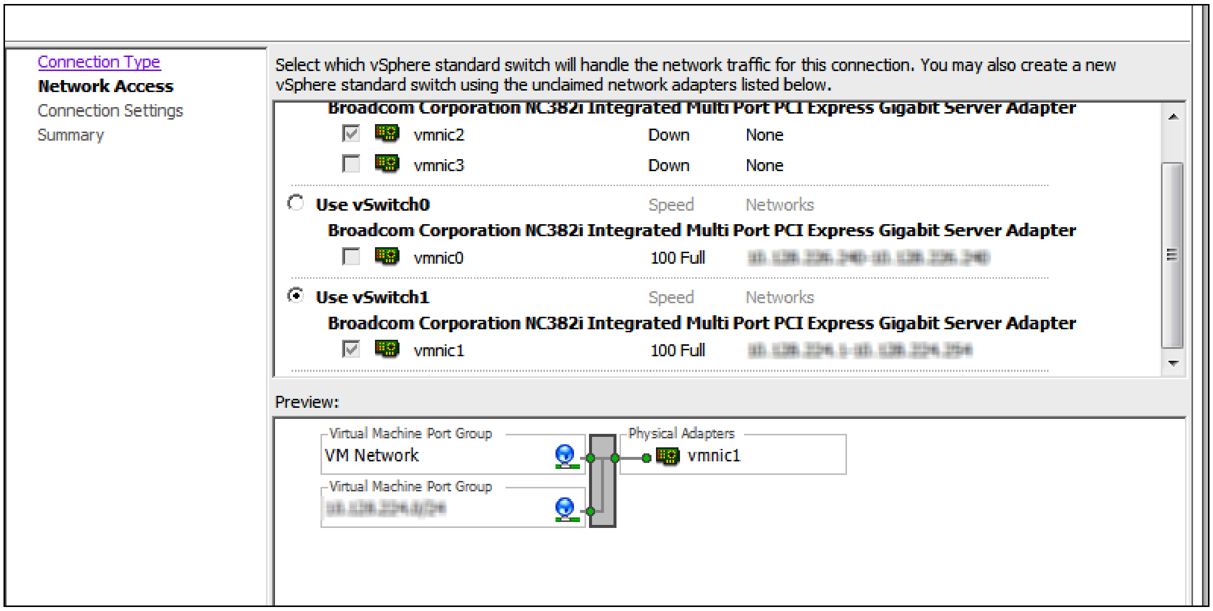
1. Log in to vSphere Client.
2. In the vSphere Client inventory, select the host where you deployed the Equinox H.323 Edge virtual server.

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**.



Select which vSphere standard switch will handle the network traffic for this connection. You may also create a new vSphere standard switch using the unclaimed network adapters listed below.

Broadcom Corporation NC382i Integrated Multi Port PCI Express Gigabit Server Adapter

☑	vmnic2	Down	None
□	vmnic3	Down	None

○ **Use vSwitch0** Speed Networks

Broadcom Corporation NC382i Integrated Multi Port PCI Express Gigabit Server Adapter

□	vmnic0	100 Full	[redacted]

● **Use vSwitch1** Speed Networks

Broadcom Corporation NC382i Integrated Multi Port PCI Express Gigabit Server Adapter

☑	vmnic1	100 Full	[redacted]

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

Configure IP separation.

Configuring IP separation of the Equinox H.323 Edge virtual server

About this task

Configure a different IP address and subnet for the second virtual NIC of Equinox H.323 Edge to process the external traffic.

This procedure is relevant only if you have a dual NIC deployment of Equinox H.323 Edge.

Before you begin

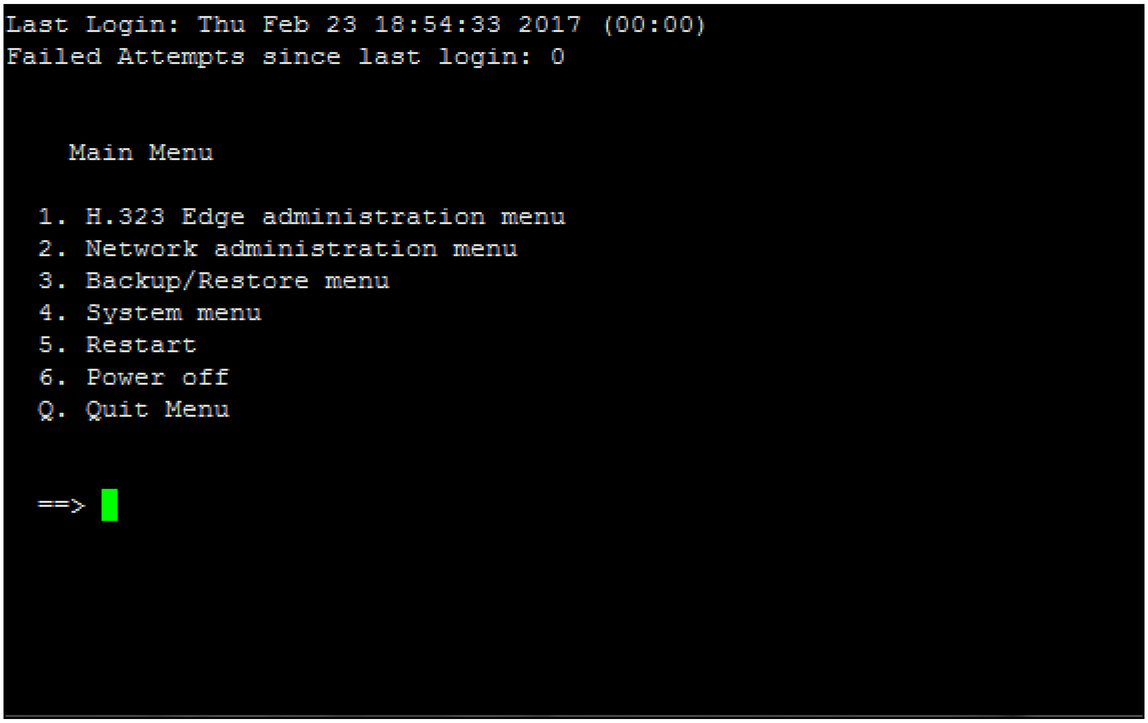
Add another network to the Equinox H.323 Edge virtual server.

Procedure

1. Log in to vSphere Client.
2. In the vSphere Client inventory, select the virtual machine.
3. Click the **Console** tab.
4. Login in as administrator.

   The default login credentials are:

   - user: admin
   - password: admin



```
Last Login: Thu Feb 23 18:54:33 2017 (00:00)
Failed Attempts since last login: 0


    Main Menu

  1. H.323 Edge administration menu
  2. Network administration menu
  3. Backup/Restore menu
  4. System menu
  5. Restart
  6. Power off
  Q. Quit Menu


  ==>
```

vSphere Client displays the Main Menu window.

5. Type `2`.

   vSphere Client displays the Network administration menu window.

6. Type `1`.

   vSphere Client displays the Current network interface configuration window.

7. Note the MAC address of the eth0 interface.

   You need this MAC address to determine the network adapter corresponding to eth0 when you assign the external network to the adaptor.

8. In the vSphere Client inventory, select the virtual machine.
9. On the **Getting Started** tab, click **Edit virtual machine settings**.

   vSphere Client displays the Virtual Machine Properties window.

10. Do the following:

    a. Click **Network adapter 1**, and select the external network in **Network Connection**.

    b. Click **Network adapter 2**, and select the internal network in **Network Connection**.

    Important:

    Verify that **Network adapter 1** has the same MAC address as the eth0 MAC address.

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 268

Configuring the TCP/UDP port range on the internal interface on page 268

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.

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**
   - **Port Range Minimum Port**
   - **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 268

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 268

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 270
Integrating Equinox H.323 Edge with NAT on page 270

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 legacy 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.

Note:

In the settings of the gatekeeper, add the IP address of Equinox H.323 Edge at port 1719 as the gatekeeper's neighbor, as described in Configuring URI-based dialing to external endpoints on page 274.

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 269

Integrating Equinox H.323 Edge with NAT

About this task

If the external NIC of Equinox H.323 Edgeuses 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.
3. Click the **Configuration** tab.
4. In the **NAT Support** section, select **Enabled**.
5. Enter the IP address in **Public IP Address**.

   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 269

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. In **NTP Configuration**, type the IP address of the NTP server in **NTP Server Address**.
5. Click **Apply**.

Enabling Internal Endpoints to Call External Endpoints

Endpoints in the organization call external endpoints using their IP address (including dialing the device, then # or ##, then the meeting ID) or URI. If the external endpoint is registered to the H.323 Gatekeeper, it can also dial the endpoint's E.164 number. Since external endpoints are typically not registered to the gatekeeper, this requires the gatekeeper to work with the Avaya Equinox H.323 Edge server to complete the call.

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. The H.323 Gatekeeper provides address resolution functionality in H.323 networks and also manages video traffic over IP networks. When the destination address is located in another network, the gatekeeper forwards the request to the Equinox H.323 Edge server to complete the call and resolve the destination.

You must configure both the Equinox H.323 Edge server and the H.323 Gatekeeper to support IP and URI dialing, as described in the following topics:

Related links

Configuring access for calls to H.323 legacy endpoints on page 272
URI Dialing Functionality on page 273
Configuring URI-based dialing to external endpoints on page 274
Configuring IP address-based dialing to external endpoints on page 276

Configuring access for calls to H.323 legacy endpoints

About this task

Direct Public Access supports a direct connection to Equinox H.323 Edge for calls to external H.323 legacy endpoints. To set up this connection, you need to configure:

- Equinox H.323 Edge to process H.323 calls.
- H.323 Gatekeeper to Equinox H.323 Edge instances to process the routing of the calls.

For more information about configuring H.323 Gatekeeper, see *Reference Guide for H.323 Gatekeeper*.

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**
    - **Port Range Minimum Port**
    - **Port Range Maximum Port**

Table 37: Configuring Access for H.323 Legacy Endpoints

Field	Description
Port Range	Define the range of ports used for direct H.323 calls in the field. **Important:** If the external NIC of the Equinox H.323 Edge server is located behind a firewall, this range of port must also be opened in the firewall, as well as port 1720 for H.323 signaling.
Default Extension	Enter the default extension that you usually configure to the MCU IVR (Interactive Voice Response). Equinox H.323 Edge redirects a call to the default extension when the endpoint dials only the server's IP address without any extension.

6. Click **Apply**.

    Equinox Management displays a confirmation message.

7. Click **Yes**.

Related links

Enabling Internal Endpoints to Call External Endpoints on page 271

URI Dialing Functionality

The Equinox Solution fully supports URI dialing, a dial format for contacting endpoints outside your organization.

URI is an address format used to locate a SIP device on a network, 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. For example,<*endpoint name*>@<*server_domain_name*>. When dialing URI between organizations, the server might often be the Avaya Equinox H.323 Edge of the organization.

All Equinox Solution endpoints work transparently with URI dials, including the Avaya Scopia® XT Series. You can also perform URI dials from the conference control of Avaya Equinox Management.

URI dialing is compatible with Avaya Equinox H.323 Edge (for H.323 endpoint) and other third party firewall traversal systems such as SBCs (for SIP endpoints). Dialing an endpoint from one organization to another requires first traversing your own firewall with Avaya Equinox H.323 Edge, out through the internet, and then into the firewall of the recipient's organization using their firewall traversal system (Figure 133: Example of URI dialing between two enterprises using Avaya Equinox H.323 Edge on page 273).

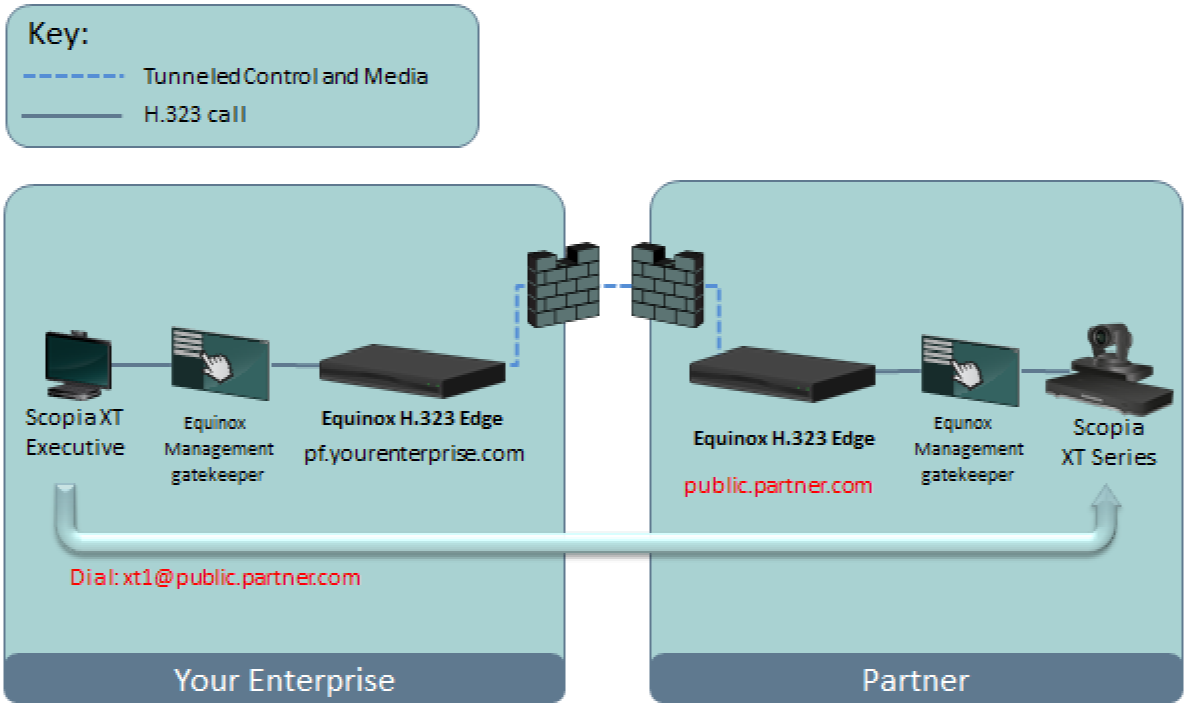


Figure 133: Example of URI dialing between two enterprises using Avaya Equinox H.323 Edge

To access an endpoint in the other company, the URI's domain name is the second company's firewall traversal system, like the name of their Equinox H.323 Edge server, or the organization's domain name. For example, in Figure 133: Example of URI dialing between two enterprises using Avaya Equinox H.323 Edge on page 273, dialing to the partner company requires knowing the following:

- The name or number of the endpoint, in this example *xt1*
- The domain name of the Equinox H.323 Edge server of that company, *public.partner.com* in this example, or the organization's domain name, *partner.com*.

❗ **Important:**

As with regular web domain names, the name of the Equinox H.323 Edge server resolves to an IP address via standard DNS lookup if it has been allocated a global DNS name. If the server's IP address does not have a DNS name, the URI dial should directly specify the server's IP address instead. For example, the URI *xt1@123.456.789.1* specifies the alias followed by the server's IP address.

To set up this connection, you need to configure the Equinox H.323 Edge server to accept H.323 calls and forward them. You also need to configure the H.323 Gatekeeper to define one or more Equinox H.323 Edge servers as H.323 Gatekeeper's neighbor, to facilitate the routing of these calls.

Related links

Enabling Internal Endpoints to Call External Endpoints on page 271

Configuring URI-based dialing to external endpoints

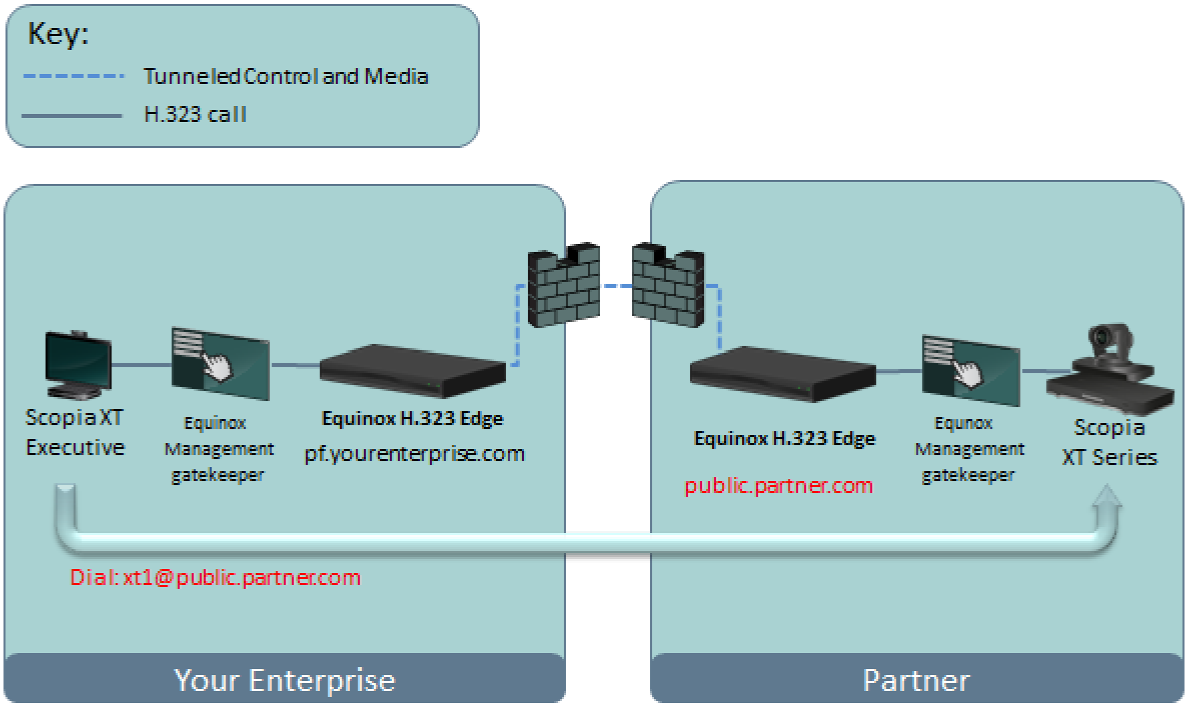
About this task

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. The H.323 Gatekeeper provides address resolution functionality in H.323 networks and also manages video traffic over IP networks.

URI is an address format used to locate a SIP device on a network, 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. For example,<*endpoint name*>@<*server_domain_name*>. When dialing URI between organizations, the server might often be the Avaya Equinox H.323 Edge of the organization.

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 URI-based calls from internal endpoints to external endpoints in another enterprise through Equinox H.323 Edge. The internal gatekeeper must 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 in calls can be legacy H.323–based and H.460–based endpoints.

When the internal gatekeeper detects a URI address that refers to an external destination, the gatekeeper forwards the request to Equinox H.323 Edge to complete the call and resolve the destination.



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 legacy endpoints. Using Direct Public Access, internal endpoints can call external legacy 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 external endpoints to communicate with 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. Click the **Configuration** tab.

4. Configure the following fields in the **URI Dialing Settings** section:
    - **Local Domain Name**
    - **Strip Domain Name**
5. Click **Settings**.
6. On the left pane, under **System Preferences**, click **Local Services**.

    Equinox Management displays the Local Services page.
7. Click **H.323 Gatekeeper**.

    Equinox Management displays the internal H.323 gatekeeper page.
8. Click **Neighbors** > **Add**.

    Equinox Management displays the Add Neighbors window.
9. Configure the following fields:
    - **Prefix**
    - **Description**
    - **IP Address**
    - **Port**
10. Click **OK**.
11. Click **Apply**.

Result

Equinox Management adds Equinox H.323 Edge as a neighbor of the internal gatekeeper.

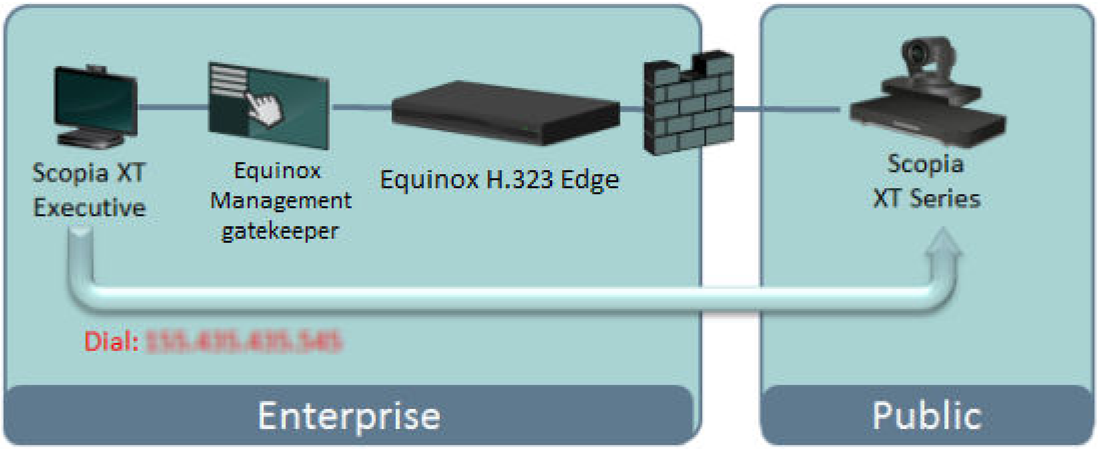
Related links

Enabling Internal Endpoints to Call External Endpoints on page 271

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 H.323–based legacy endpoints. Using Direct Public Access, internal endpoints can call external legacy 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.

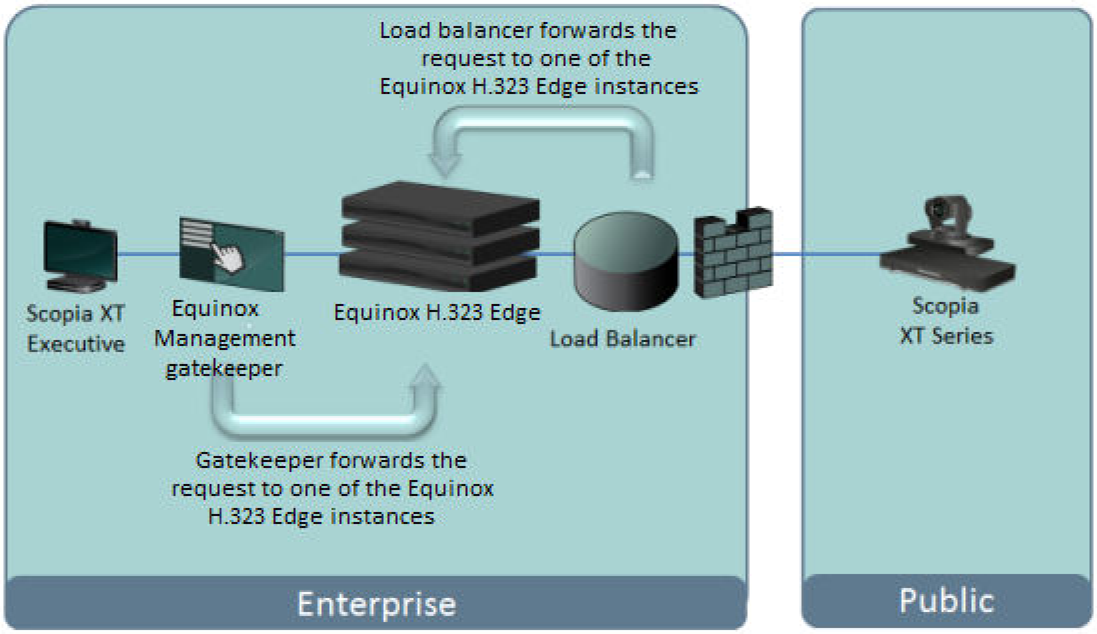
- If the enterprise deployment has multiple Equinox H.323 Edge instances, verify that the correct redundancy policy is configured between the internal gatekeeper of Equinox Management and each Equinox H.323 Edge instance.

  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 set 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.


Load balancer forwards the request to one of the Equinox H.323 Edge instances
Scopia XT Executive
Equinox Management gatekeeper
Equinox H.323 Edge
Load Balancer
Scopia XT Series
Gatekeeper forwards the request to one of the Equinox H.323 Edge instances
Enterprise
Public

Procedure

1. Log in to Equinox Management.
2. Click **Settings**.
3. On the left pane, under **System Preferences**, click **Local Services**.

   Equinox Management displays the Local Services page.
4. Click **H.323 Gatekeeper**.

   Equinox Management displays the internal H.323 gatekeeper page.
5. Click **Route IP calls**, and select **Route IP calls to H.323 Edge Server**.
6. Click **Add**.

   Equinox Management displays the Add IP Calls window.
7. Configure the following fields:
   - **IP Address**
   - **Port**
8. 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

Enabling Internal Endpoints to Call External Endpoints on page 271

Secure connection with Equinox Management

Equinox H.323 Edge supports the following three-layer security certificate chain to ensure the authentication and encryption of the network connection with Equinox Management:

- Product certificate
- Root certificate
- Intermediate certificate

You can upload the security certificates using one of the following two methods:

- Individually: Upload each security certificate from the individual section on the Certificate tab of the Equinox H.323 Edge instance page on Equinox Management. There is no order of uploading the security certificates individually.
- Simultaneously: Upload all the security certificates together by pasting the text of all the certificates in one text file and uploading the text file by using one of the Upload options on the Certificate tab.

Restrictions

The security certificate mechanism has the following restrictions:

- Equinox Management updates the root certificate and intermediate certificate only if you upload the product certificate first.
- Equinox Management displays all the security certificates only if you upload all the three security certificates. For example, if you upload only the product certificate and the root certificate, Equinox Management displays only the product certificate.

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.

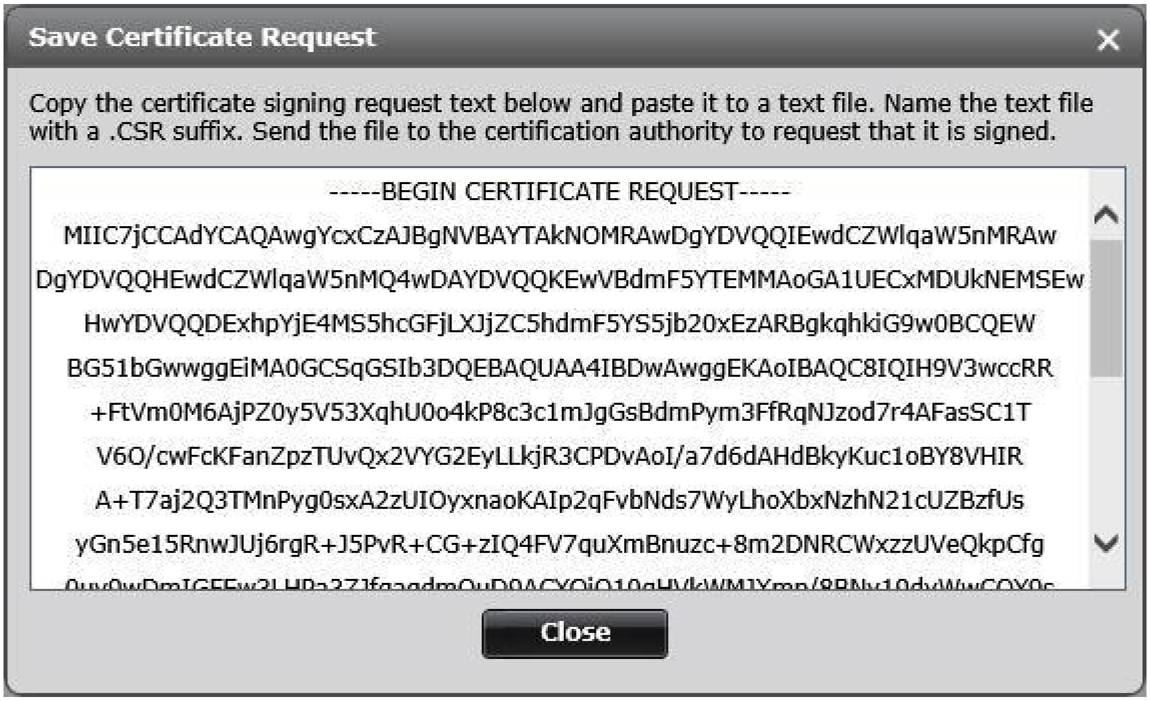
Procedure

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 a New CSR**.

   Equinox Management displays the Save Certificate Request window.



Save Certificate Request

Copy the certificate signing request text below and paste it to a text file. Name the text file with a .CSR suffix. Send the file to the certification authority to request that it is signed.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC7jCCAdYCAQAwgYcxCzAJBgNVBAYTAkNOMRAwDgYDVQQIEwdCZWlqaW5nMRAw
DgYDVQQHEwdCZWlqaW5nMQ4wDAYDVQQKEwVBdmF5YTEMMAoGA1UECxMDUkNEMSEw
HwYDVQQDExhpYjE4MS5hcGFjLXJjZC5hdmF5YS5jb20xEzARBgkqhkiG9w0BCQEW
BG51bGwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC8IQIH9V3wccRR
+FtVm0M6AjPZ0y5V53XqhU0o4kP8c3c1mJgGsBdmPym3FfRqNJzod7r4AFasSC1T
V6O/cwFcKFanZpzTUvQx2VYG2EyLLkjR3CPDvAoI/a7d6dAHdBkyKuc1oBY8VHIR
A+T7aj2Q3TMnPyg0sxA2zUIOyxnaoKAIp2qFvbNds7WyLhoXbxNzhN21cUZBzfUs
yGn5e15RnwJUj6rgR+J5PvR+CG+zIQ4FV7quXmBnuzc+8m2DNRCWxzzUVeQkpCfg
```

5. Copy the text in the Save Certificate Request window to a text file and save the file with a `.CSR` extension.
6. Send the text file to the certification authority for signing.
7. Click **Close**.

Result

The certification authority will send back a signed certificate.

Next steps

Upload the certificates.

Uploading product 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.

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

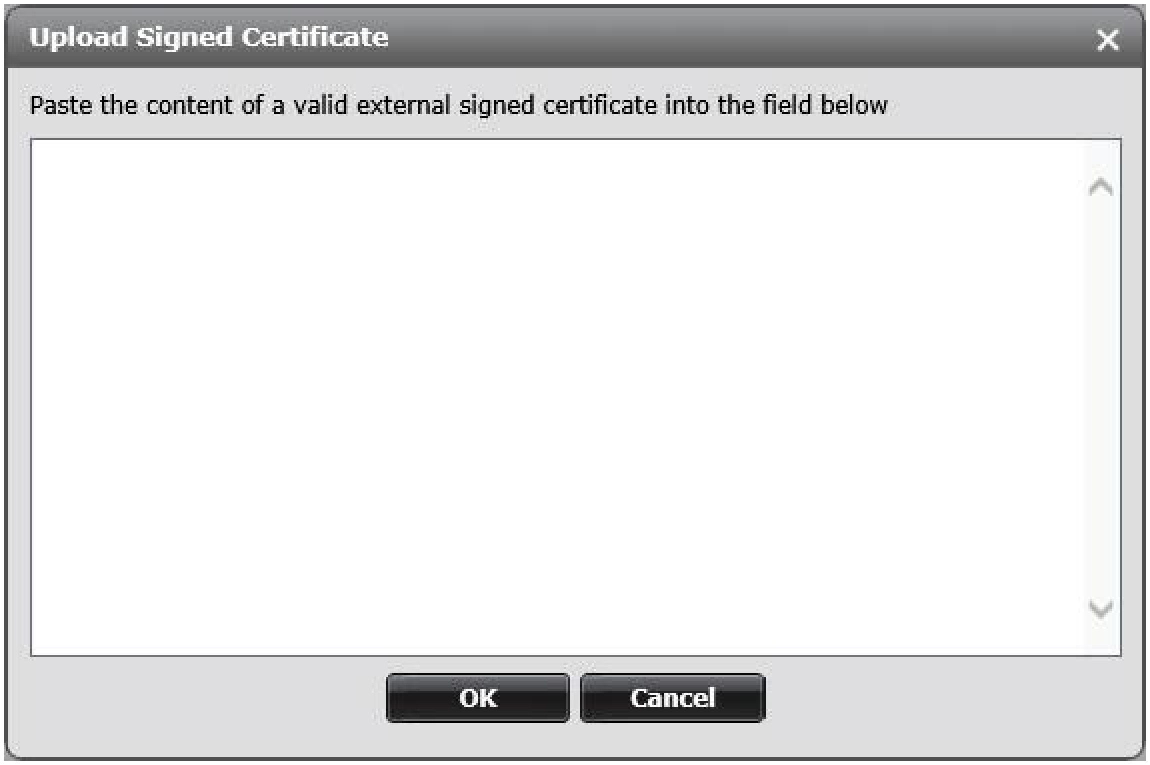
Generate the certificates.

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 a Certificate**.

   Equinox Management displays the Upload Signed Certificate window.



Upload Signed Certificate

Paste the content of a valid external signed certificate into the field below

5. Paste the content of the security certificate that the certification authority sent, and click **OK**.
6. Restart Equinox H.323 Edge.

Result

Equinox Management uploads the security certificate to Equinox H.323 Edge.

Next steps

Enable the secure connection between Equinox H.323 Edge and Equinox Management.

Uploading root certificates

About this task

The root certificate from the certification authority must be uploaded to Equinox H.323 Edge 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

Get the root certificate.

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** in the Certificate Authority (CA) Root Certificate section.

   Equinox Management displays the Upload CA Root Certificate window.
5. Paste the content of the root certificate that the certification authority sent, and click **OK**.
6. Restart Equinox H.323 Edge.

Result

Equinox Management uploads the root certificate to Equinox H.323 Edge.

Uploading intermediate certificates

About this task

The intermediate certificate from the certification authority must be uploaded to Equinox H.323 Edge 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

Get the intermediate security certificate.

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** in the Certificate Authority (CA) Intermediate Certificate section.

   Equinox Management displays the Upload CA Intermediate Certificate window.
5. Paste the content of the intermediate certificate that the certification authority sent, and click **OK**.
6. Restart Equinox H.323 Edge.

Result

Equinox Management uploads the intermediate certificate to Equinox H.323 Edge.

Next steps

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 **Configuration**.
4. Select the check box next to **Secure XML connection using TLS**,
5. Type the timeout duration in seconds in **Timeout**.

Result

The connection between Equinox H.323 Edge and Equinox Management is secured using TLS.

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/.

- 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.

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. Type the login credentials and ports for the following administrator profiles:
   - **Collaborator Access**
   - **SSH/SFTP Access**
   - **HTTP Access**
5. **(Optional)** In **Secure Access**, select **Prefer Secure XML connection using TLS** to secure the connection between Equinox H.323 Edge and Equinox Management.
6. Click **Apply**.

Access field descriptions

Name	Description
Collaborator Access	
Name	The user name of the collaborator. This profile is required to send XML API requests to Equinox H.323 Edge. The user name must match the name configured for the collaborator in Equinox H.323 Edge. The default name of the collaborator is *Collab*.
Login Password	The password of the collaborator. The password must match the password configured for the collaborator in Equinox H.323 Edge. The default password of the collaborator is *balloC*.
Port	The firewall port that the collaborator uses to gain access to Equinox H.323 Edge.
Secure Access	
Prefer Secure XML connection using TLS	The option to secure the connection between Equinox H.323 Edge and Equinox Management using TLS certificates. Equinox Management connects to Equinox H.323 Edge using TLS. If the TLS-based secure connection fails, Equinox Management connects using the TCP-based connection.
SSH/SFTP Access	
Name	The user name of the SSH and SFTP client. You cannot change this name. The SSH client gains access to the shell administration menu of Equinox H.323 Edge, and the SFTP client uploads and downloads Equinox H.323 Edge resources.
Login Password	The password of the SSH and SFTP clients. The default password is *admin*.
HTTP Access These fields are application only to Equinox H.323 Edge releases earlier than Release 9.0.	
Name	The user name of the Equinox H.323 Edge web interface administrator. The default user name is *admin*.
Login Password	The password of the Equinox H.323 Edge web interface administrator.

Table continues…

Name	Description
	The default password is *admin*.
Port	The firewall port for the HTTP access. The default port is 8080.

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, 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. Signaling occurs before the control aspect of call setup.
  - 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. 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.
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**

Chapter 16: Avaya Scopia Desktop Server deployment

Planning your Avaya Scopia Desktop Server deployment

Planning your Avaya Scopia Desktop Deployment

When planning your Avaya Scopia Desktop deployment, consider the following:

- Is yours an Over The Top solution (OTT) or a Team Engagement (TE) solution? Avaya Scopia Desktop is mandatory for OTT, but optional for TE.
- How many users will be simultaneously connecting to videoconferences?
- Will most Scopia Desktop Clients connect to videoconferences from within the enterprise, or from outside? For example, if there are many internal Scopia Desktop Clients, consider placing a dedicated Conference Server in the enterprise.
- If reliability is a requirement, consider deploying redundant Scopia Desktop Servers.
- How often will your organization record videoconferences? How often will those recordings be viewed? Are there likely to be many simultaneous viewers?

  For example, if recording is a major part of your videoconferencing experience, you may decide to deploy a dedicated Recording Server.
- Will most users join videoconferences as participants, or view webcasts of meetings?
- What is your network's security policy?

  Depending on where you deploy the Scopia Desktop Server and other video network devices, you may need to open different ports on the firewall.
- How much internal and external bandwidth is required, based on the number of simultaneous users joining videoconferences? Consider also whether most users will be joining in standard or high definition.

Based on the factors above, decide whether to deploy all Scopia Desktop Server components on one server or on multiple dedicated servers. See the following sections for details on the different deployment options and how to plan your bandwidth:

Minimum Requirements and Specifications of Scopia Desktop Server

This section details the system specifications of your Scopia Desktop Server. Refer to this data when preparing system setup and afterwards as a means of verifying that the environment still complies with these requirements.

Scopia Desktop Server Software Requirements

The minimum software requirements for the Scopia Desktop Server are:

Operating systems:

- Windows® 2012 Server and Windows® 2012 R2 Server (English)
- Windows® 2008 SP2 or Windows® 2008 R2, 32 and 64 bit (English, Japanese)
- Windows® 2008 Datacenter or Enterprise Edition (English) with more than 4GB of RAM, or Windows® 2008 Standard Edition (English) with 4GB of RAM

Important:

Scopia Desktop Servers can be deployed using the VMware Sphere v5.5 virtual machine.

Web browsers for the Scopia Desktop Server administration:

Scopia Desktop is tested with the latest internet browser versions available at the time of release.

- Microsoft Internet Explorer 8 and later for Windows
- Mozilla Firefox 37 or later for Apple OS and Windows
- Apple Safari 6 or later for Apple OS
- Google Chrome 41 or later for Apple OS and Windows
- Microsoft Edge 38 or later (EdgeHTML v14)

The following add-ins for Scopia Desktop integrate it with various third-party products. For more information, see the relevant add-in documentation.

- The Avaya Scopia Connector for IBM Lotus Notes 8.5.2, 8.5.3, and 9.0.
- Avaya Equinox Add-in for Microsoft Outlook (64 bit) requires Office 2013 or later, and access to the Avaya Equinox Management user portal.

Scopia Desktop Server Hardware Requirements

Depending on your deployment, you can install the Scopia Desktop Server on a dedicated server or on the same server as Equinox Management. Table 38: Call capacity and hardware requirements for Scopia Desktop Server on page 290 lists the minimum hardware requirements and call capacity for the Scopia Desktop Server.

Table 38: Call capacity and hardware requirements for Scopia Desktop Server

Product name	Recommended server hardware	Call capacity
Scopia Desktop on dedicated server	Intel ® Xeon ® Processor E3-1270v2 @ 3.50 GHz RAM: 4GB Disk space: 80Gb 4 virtual cores NIC: 1000Mb	Up to 250 1080p@1280Kbps calls are supported in a non-virtualized deployment. **Note:** In VMware deployments, call capacity is reduced due to virtualization. The following capacities are supported: Up to 150 480p@384Kbps calls or lower or Up to 100 1080p@1280Kbps calls or lower or For bandwidth settings higher than 1Mbps per call, use the following formula: `Max calls = 100/[call rate in Mbps]` **Note:** HD calls use twice as much bandwidth as regular calls. As a result, call capacity may be reduced in deployments that make large numbers of HD calls.
Avaya Scopia Content Slider Server (on dedicated server)	Intel ® Xeon ® Processor E3-1270v2 @ 3.50 GHz (4 virtual cores) RAM: 4GB Disk space: 80Gb 4 virtual cores NIC: 1000Mb	
Scopia Desktop and Equinox Management on the same server	CPU: Intel Xeon E3-1270v2 Quad Core @ 3.5 GHz RAM: 8Gb NIC: 1000 Mb Disk: 80 GB **Important:** If using Application Server P/N 55876-00003: 40 GB is sufficient, but clean up log files and upgrade packages on a regular basis to ensure that there is enough disk space.	

Important:

- If you upgrade your Scopia Desktop Server but maintain the same hardware platform, the new version has the same capacity as the previous version. You do not need to upgrade the hardware for this update.
- If the server PC is not strong enough for the maximum number of connections, you can limit the number of calls in the Scopia Desktop Server. For more information, see *Administrator Guide for Scopia Desktop Server*.
- When you initiate a 1MB high definition call, scalability is reduced by fifty percent.

Scopia Desktop Server Audio and Video Specifications

Scopia Desktop interoperates with both SIP and H.323 endpoints to provide a seamless user experience joining the ease of use of Scopia DesktopClients and Scopia Mobile devices with dedicated endpoints like XT Executive and the Avaya Scopia® XT Series.

- Audio support:
  - G.722.1 codec
  - DTMF tone detection (in-band, H.245 tones, and RFC2833)
- Video support:
  - High Definition (HD) video with a maximum resolution of 720p at 30 frames per second (fps)
  - Video codec: H.264 with SVC (Scalable Video Coding) and H.264 High Profile
  - Video send resolutions: Up to HD 720p
  - Video receive resolution: 1080p if bandwidth is higher than 1280 kbps
  - Video bandwidth: HD up to 4Mbps for 720p resolutions; standard definition up to 448 kbps for 352p or lower
  - Presentation video: H.239 dual stream
  - Avaya Scopia Content Slider can function with presentation set to H.263 or H.264 on the MCU.

Scopia Desktop Server Security Specifications

Scopia Desktop Server has extensive support for security inside private networks as well as across sites. In addition to a proprietary secure protocol between the client and server, Scopia Desktop Server has the following security specifications:

- Using HTTPS protocol for protecting signaling, management and media over TCP data streams between Scopia DesktopClient/Scopia Mobile and Scopia Desktop Server.
- Using SRTP encryption for protecting media over UDP data stream between Scopia DesktopClient/Scopia Mobile and Scopia Desktop Server.
- Using TLS encryption to protect all traffic between Scopia Desktop Server and Equinox Management.

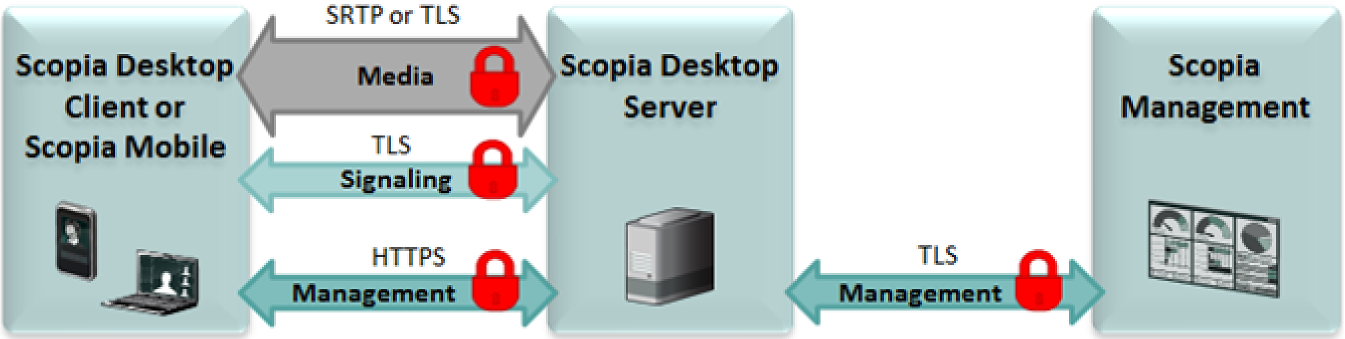


Figure 134: Securing Scopia Desktop Server communications

Planning your Topology for Scopia Desktop Server

You can deploy the Scopia Desktop components in various ways, depending on factors such as the number of videoconferencing users in your organization.

Scopia Desktop includes the following components:

- Conference Server for Scopia Desktop, to create videoconferences with Scopia Desktop Clients and Scopia Mobile devices
- Avaya Scopia Content Slider (Tomcat) to store data already presented in the videoconference, allowing participants to view previously shared content during the meeting

In addition to Avaya Scopia Desktop Server your organization can choose to deploy optional components: Avaya Equinox Streaming and Recording Server for recording meetings and Avaya Scopia® Web Collaboration server for advance content sharing. For more information about deploying these components, see *Installing the Avaya Equinox Streaming and Recording Server* and *Administering the Avaya Equinox Streaming and Recording Server* at the Avaya Support website: https://support.avaya.com/.

Depending on the size and capacity of your deployment, you can deploy these components and applications on a single Scopia Desktop Server or install specific components and applications on dedicated servers. See the following sections for the different deployment options:

Related links

Topology for Small Scopia Desktop Server Deployment on page 292
Medium Scopia Desktop Server Deployment with Dedicated Servers on page 294
Large Scopia Desktop Server Deployment with Dedicated Servers on page 296

Topology for Small Scopia Desktop Server Deployment

In a standard Scopia Desktop Server installation, you deploy a single all-in-one server with the following installed (see Figure 135: Typical small deployment of Scopia Desktop Server on page 293):

- A complete Scopia Desktop installation, which includes the Conference Server, as well as any other Scopia Desktop components used in your organization.

  Scopia Desktop Server includes various components.
- Avaya Equinox Management, an application used to control your video network devices and schedule videoconferences. Avaya Equinox Management includes a built-in gatekeeper.

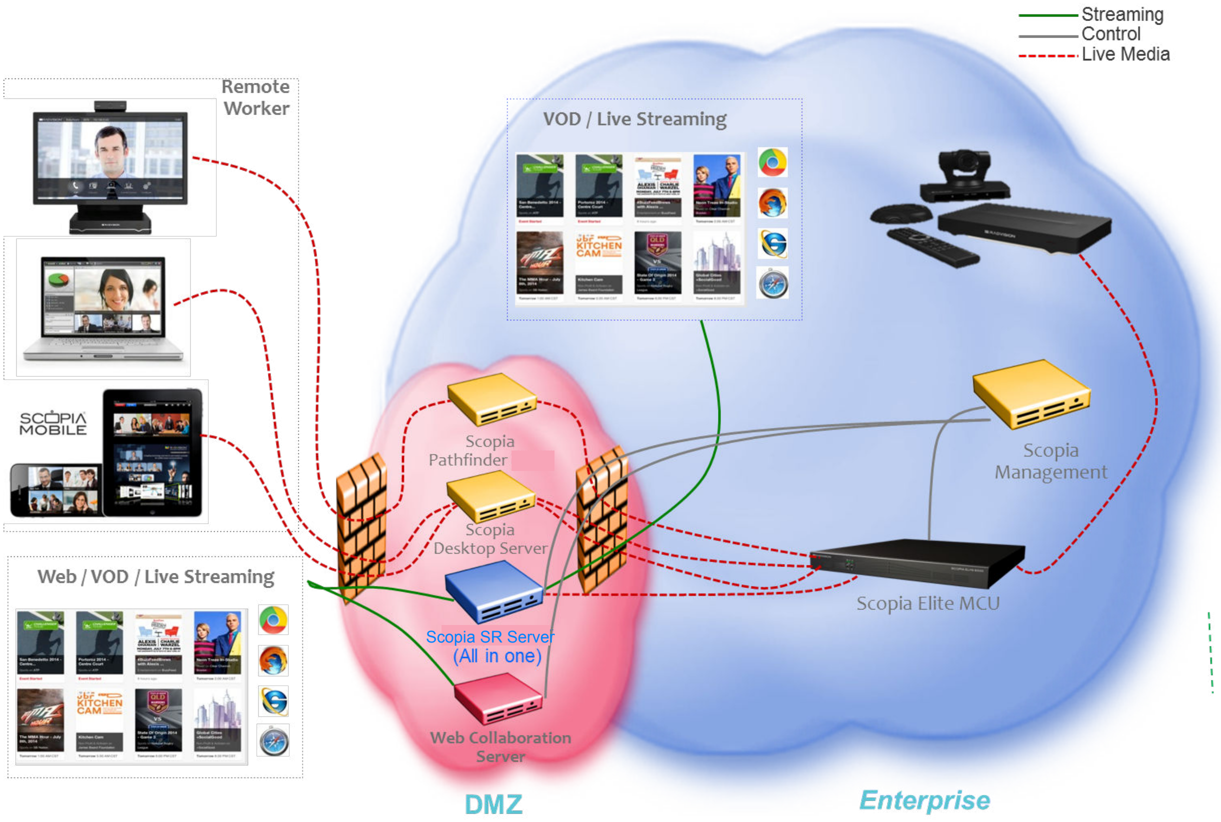


Figure 135: Typical small deployment of Scopia Desktop Server

In addition to Avaya Scopia Desktop Server your organization can choose to deploy optional components: Avaya Equinox Streaming and Recording Server for recording meetings and Avaya Scopia® Web Collaboration server for advance content sharing. For more information about deploying these components, see *Installing the Avaya Equinox Streaming and Recording Server* and *Administering the Avaya Equinox Streaming and Recording Server* at the Avaya Support website: https://support.avaya.com/.

For information on the capacity of a single server, see Minimum Requirements and Specifications of Scopia Desktop Server on page 289.

The all-in-one server is typically deployed in the DMZ. Scopia Desktop Clients can connect from the internal enterprise network, a public network, or from a partner network.

This topology serves as the baseline deployment and is typically used for smaller organizations. To increase capacity, you can install Scopia Desktop components on dedicated servers (see Medium Scopia Desktop Server Deployment with Dedicated Servers on page 294).

Scopia Desktop Server deployments require an MCU to host videoconferences, and Equinox Management to control your video network devices and schedule videoconferences.

Related links

Planning your Topology for Scopia Desktop Server on page 292

Medium Scopia Desktop Server Deployment with Dedicated Servers

To increase the capacity of the deployment, you can dedicate a Conference Server for Scopia Desktop, which includes the Conference Server and Web Server.

Each Scopia Desktop Server deployed should match the minimum requirements detailed in Minimum Requirements and Specifications of Scopia Desktop Server on page 289. .

In addition to Avaya Scopia Desktop Server your organization can choose to deploy optional components: Avaya Equinox Streaming and Recording Server for recording meetings and Avaya Scopia® Web Collaboration server for advance content sharing. For more information about deploying these components, see *Installing the Avaya Equinox Streaming and Recording Server* and *Administering the Avaya Equinox Streaming and Recording Server* at the Avaya Support website: https://support.avaya.com/.

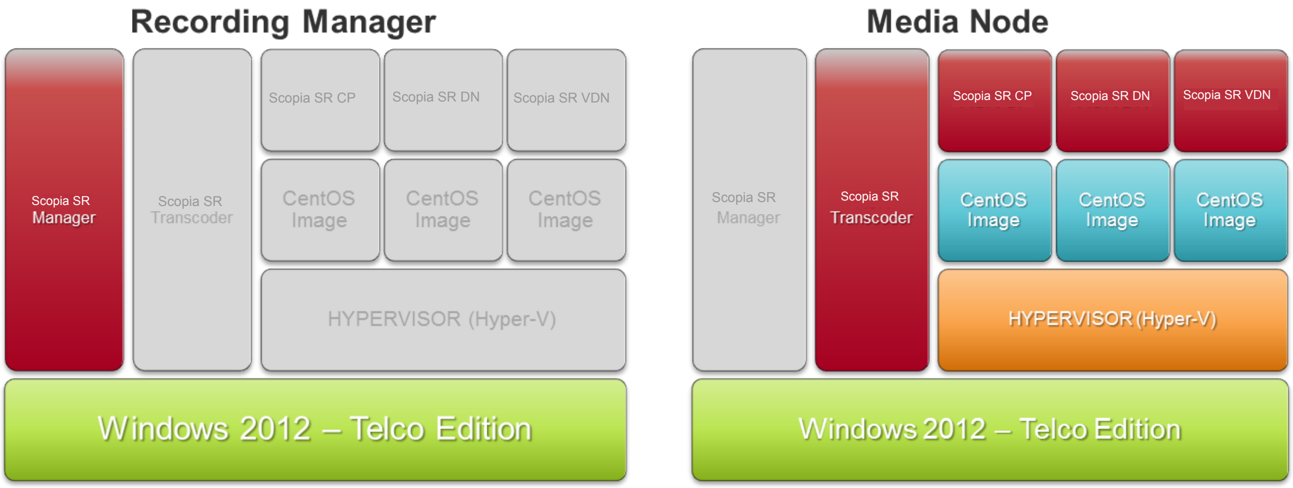


Figure 136: Typical medium-sized deployment

This example of a medium deployment shows a dedicated management server and a separate server that houses the media node. This distributed configuration adds capacity to the system.

Typically, you deploy the dedicated Scopia Desktop Servers in the DMZ, to provide connection to participants and webcast viewers connecting from both the internal and external networks (Figure 137: Deploying dedicated Scopia Desktop Servers in the DMZ on page 295). You can also deploy an additional server in the enterprise, so that internal participants do not need to connect through the firewall.

Depending on where you deploy the dedicated servers, you may need to open additional ports. For details, see Ports to Open on Avaya Scopia Desktop on page 309.

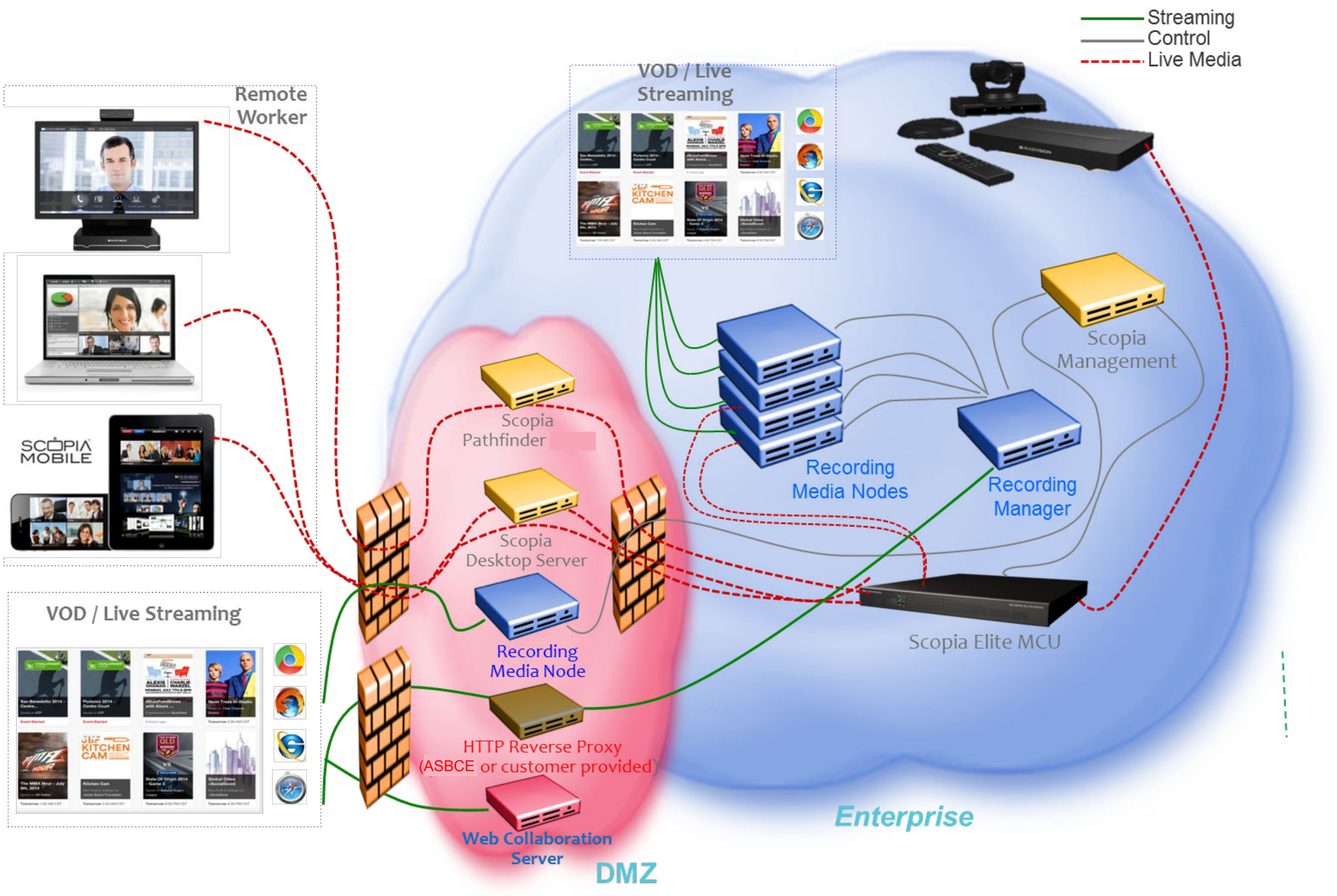


Figure 137: Deploying dedicated Scopia Desktop Servers in the DMZ

This is typically relevant for larger deployments. You can also cluster the Scopia Desktop Servers behind a load balancer, as described in Large Scopia Desktop Server Deployment with Dedicated Servers on page 296. Smaller deployments, on the other hand, might install all components on the same Scopia Desktop Server with a Equinox Management (see Topology for Small Scopia Desktop Server Deployment on page 292).

Scopia Desktop Server deployments require an MCU to host videoconferences, and Equinox Management to control your video network devices and schedule videoconferences.

For more information about Equinox Solution deployments, see the *Solution Guide for Equinox Solution*.

Related links

Planning your Topology for Scopia Desktop Server on page 292

Large Scopia Desktop Server Deployment with Dedicated Servers

Large deployments, such as service providers or large organizations, typically deploy multiple dedicated Scopia Desktop Servers. To provide scalability and high availability, with service preservation for up to 100,000 registered users, you can cluster several dedicated Conference Servers behind a load balancer as described in Deploying Scopia Desktop with a Load Balancer on page 298.

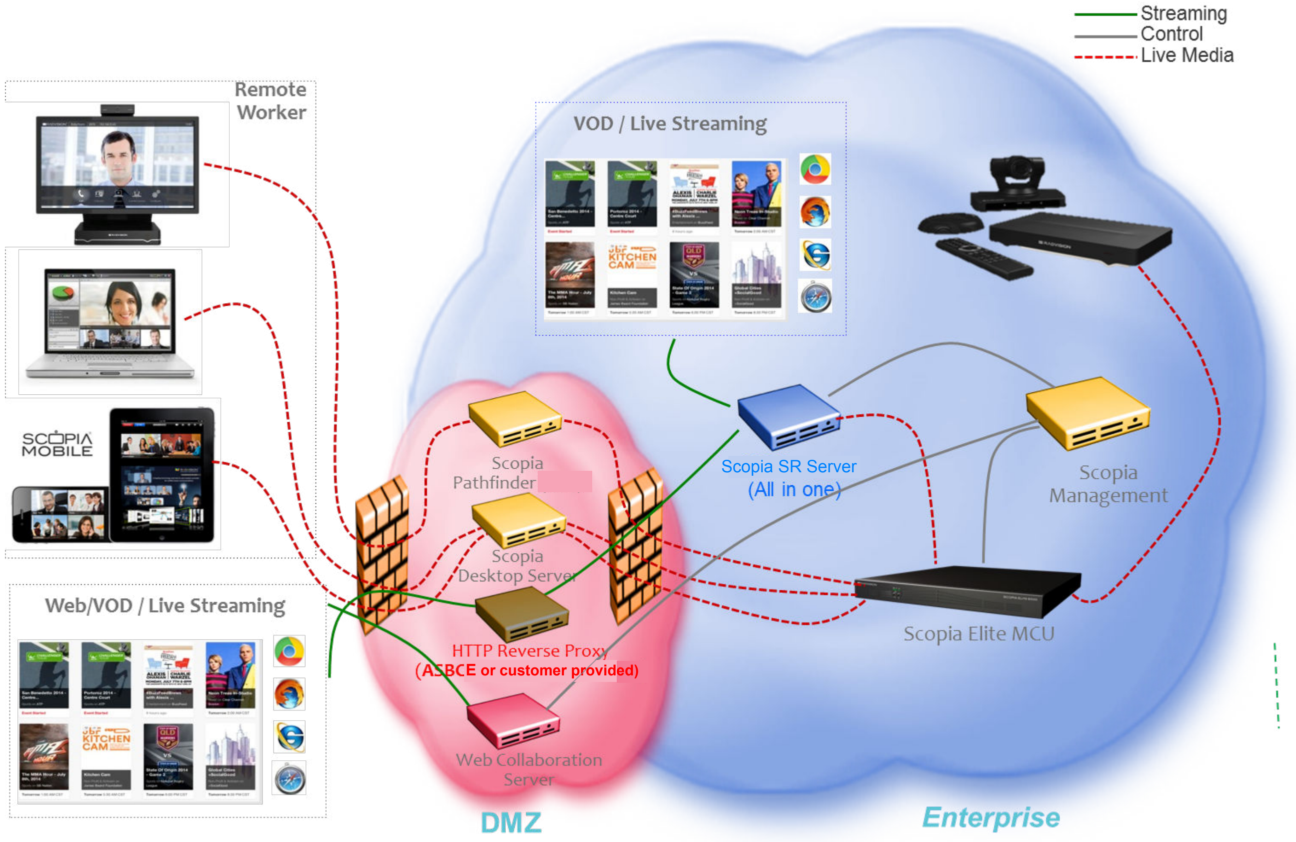


Figure 138: Typical large deployment

In addition to Avaya Scopia Desktop Server your organization can choose to deploy optional components: Avaya Equinox Streaming and Recording Server for recording meetings and Avaya Scopia® Web Collaboration server for advance content sharing. For more information about deploying these components, see *Installing the Avaya Equinox Streaming and Recording Server* and *Administering the Avaya Equinox Streaming and Recording Server* at the Avaya Support website: https://support.avaya.com/.

The videoconferencing infrastructure, including the Scopia Desktop Server, is typically deployed in the DMZ to provide connection to participants and webcast viewers connecting from both the internal and external networks (Figure 139: Large Scopia Desktop Server Deployment with Dedicated Servers on page 297).

You can also deploy an additional Conference Server in the enterprise, so that participants in internal videoconferences do not need to connect through the firewall.

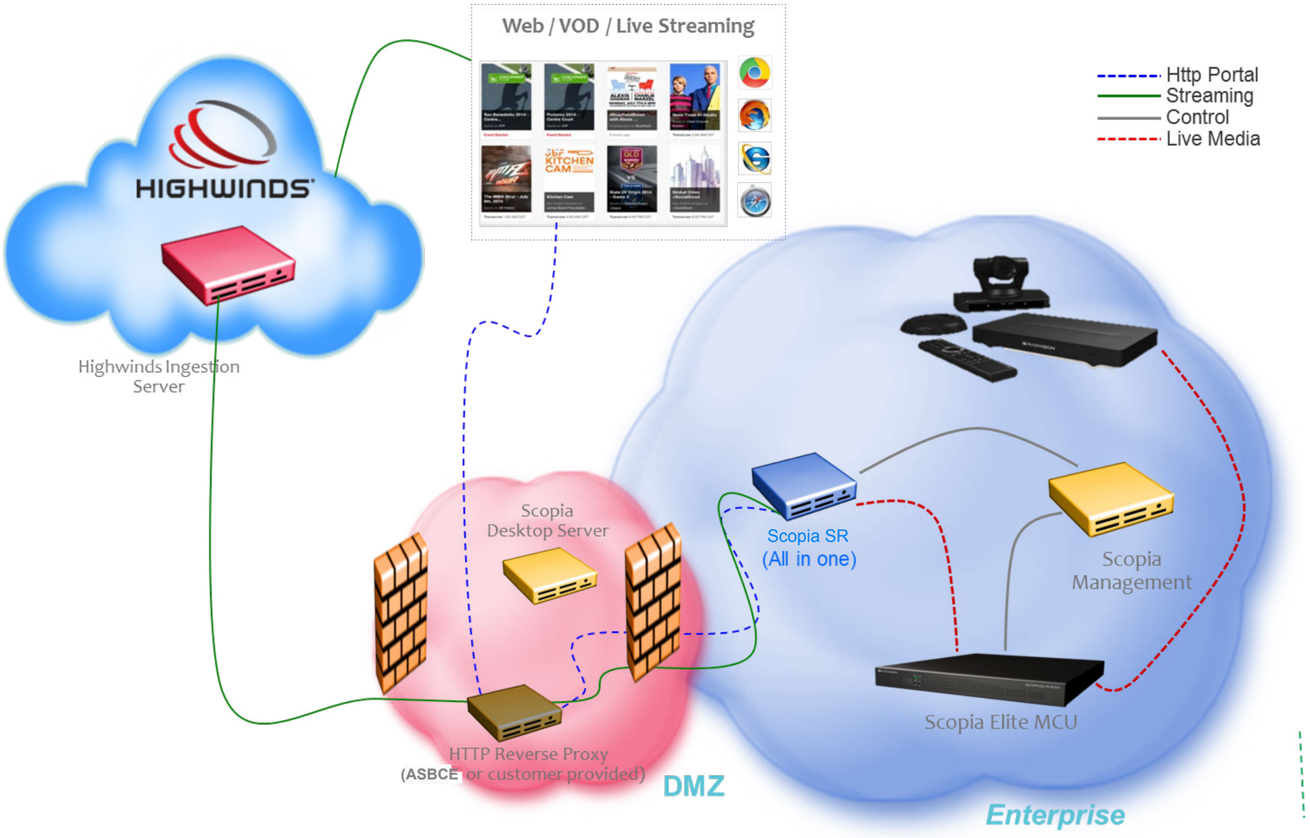


Figure 139: Large Scopia Desktop Server Deployment with Dedicated Servers

Enterprises can deploy the videoconferencing infrastructure in more than one location. This can be done either for redundancy or, if there are many customers in different regions of the world, you can deploy a full set of videoconferencing infrastructure in the headquarters, and another set of infrastructure in a branch.

See the *Solution Guide for Equinox Solution* for detailed information about different ways to deploy your videoconferencing infrastructure.

Each Scopia Desktop Server deployed should match the minimum requirements detailed in Minimum Requirements and Specifications of Scopia Desktop Server on page 289.

Scopia Desktop Server deployments require an MCU to host videoconferences, and Equinox Management to control your video network devices and schedule videoconferences.

Related links

Planning your Topology for Scopia Desktop Server on page 292

Deploying Scopia Desktop with a Load Balancer on page 298

Deploying Scopia Desktop with a Load Balancer

For increased reliability and scalability, you can deploy multiple Scopia Desktop Servers behind a load balancer such as Radware's AppDirector or another load balancer (Figure 141: Typical load balanced Scopia Desktop deployment on page 299).

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).

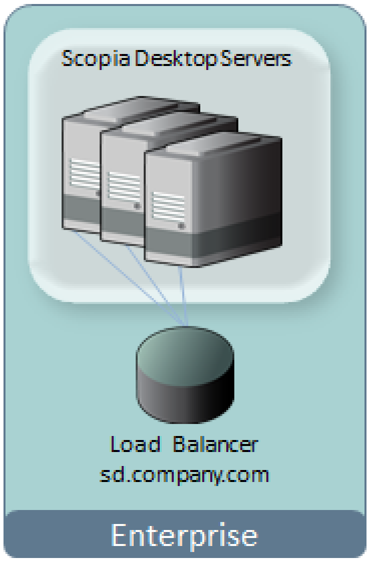


Figure 140: Deploying Scopia Desktop with a Load Balancer

All servers in the cluster should have identical functionality enabled, since one server must take over if another is overloaded or fails. If you deploy dedicated servers for the different components of Scopia Desktop (for example, a dedicated recording or streaming server), these dedicated servers should be located outside the cluster. For more information, see *Installation Guide for Scopia Desktop Server*.

Typically, the Scopia Desktop cluster is deployed in the DMZ, to enable both internal and external participants to join the videoconference. If many videoconferences include only internal participants, consider deploying an additional Conference Server in the enterprise, or, for increased capacity, an additional cluster with a load balancer.

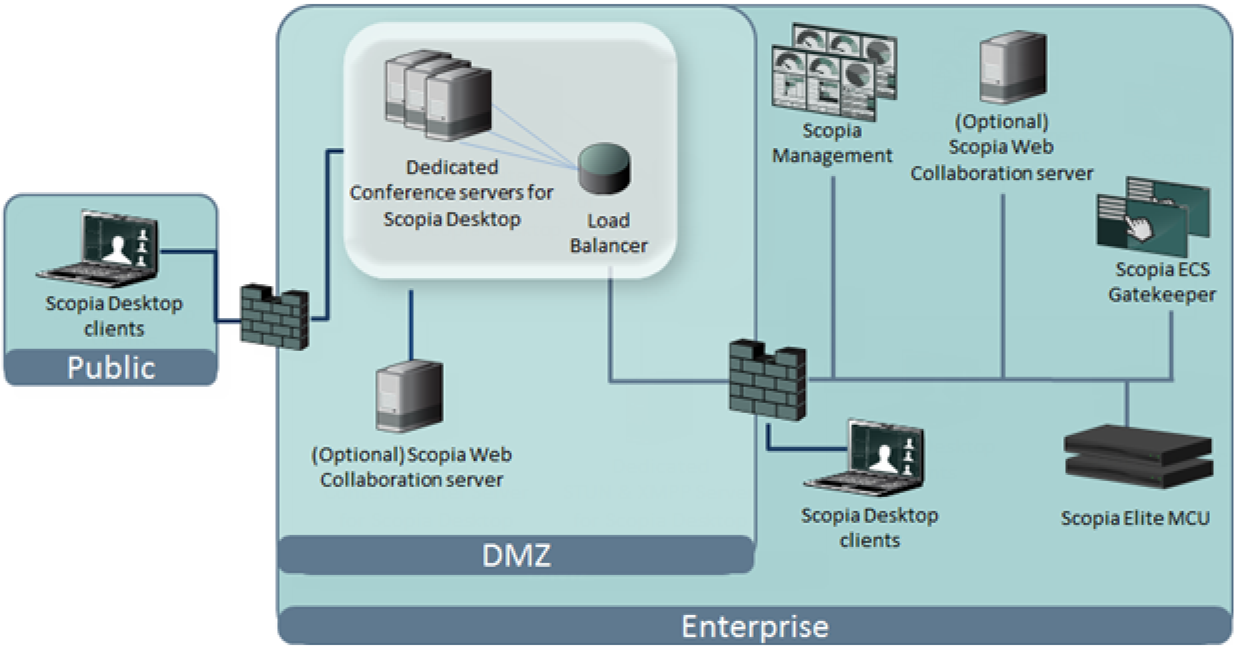

Dedicated Conference servers for Scopia Desktop
Load Balancer
Scopia Management
(Optional) Scopia Web Collaboration server
Scopia ECS Gatekeeper
Scopia Desktop clients
Public
(Optional) Scopia Web Collaboration server
Scopia Desktop clients
Scopia Elite MCU
DMZ
Enterprise

Figure 141: Typical load balanced Scopia Desktop deployment

When clustering multiple Scopia Desktop Servers in your deployment, all servers must be configured with the same security mode. When a device establishes a secure connection with another component, it sends a signed certificate verifying its identity. The signature on the certificate must be from a known (trusted) certification authority (CA). For more information about security, see *Installation Guide for Scopia Desktop Server*.

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.

You can configure the load balancer to route all network traffic or only part of it, depending on the load balancer's capacity and your deployment requirements (Figure 142: Media can either bypass or travel via the load balancer (example) on page 300):

- In full load balancing deployments, all network traffic between servers and clients, including the media (audio, video, data presentations), is routed via the load balancer. This is best for powerful load balancer servers, and has the added security advantage of withholding the private IP of a Scopia Desktop Server to the outside world.
- In partial load balancing deployments, the media data travels directly between client and server, bypassing the load balancer, while signaling and management still travel via the load balancer. This is better for less powerful load balancer computers, but directly exposes the servers' private IP addresses to the outside world.

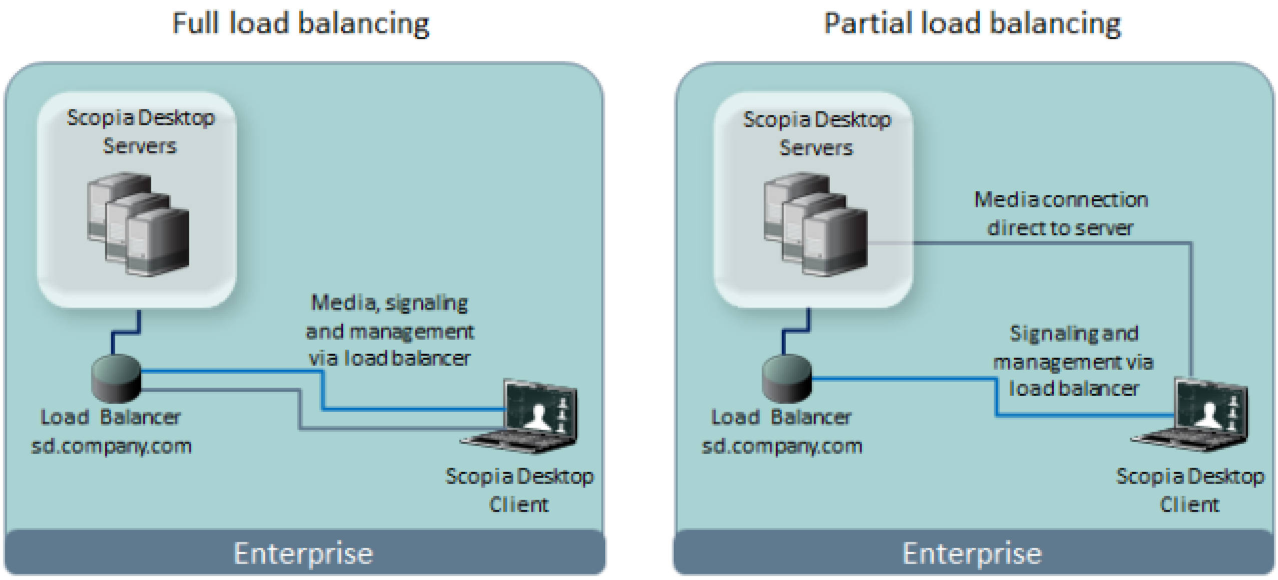


Figure 142: Media can either bypass or travel via the load balancer (example)

For details about configuring load balancing, see *Installation Guide for Scopia Desktop Server*.

Related links

Large Scopia Desktop Server Deployment with Dedicated Servers on page 296

Deploying Scopia Desktop Server with Dual-NIC

Scopia Desktop Server can be installed on servers with multiple Network Interface Cards (NICs). Depending on the deployment and network configuration, you may want to control which NIC is used for various server communications.

Important:

Use bonded 100 Mbit NICs or a Gigabyte NIC. The default settings are 384 kbps for every participant connection, and 256 kbps for webcast viewers.

For example, in secure multiple NIC deployments you can use a NIC configured behind the firewall to communicate with various servers , while using another NIC for Scopia Desktop Client connections (Figure 143: Scopia Desktop with a dual-NIC deployment on page 301). In this case, configure the Scopia Desktop IP address to represent the NIC behind the firewall. For the Scopia Desktop public address, use a DNS name which resolves to the NIC outside the firewall, and is accessible both inside and outside the enterprise.

For more information and to configure the public address, see *Administrator Guide for Scopia Desktop Server*.

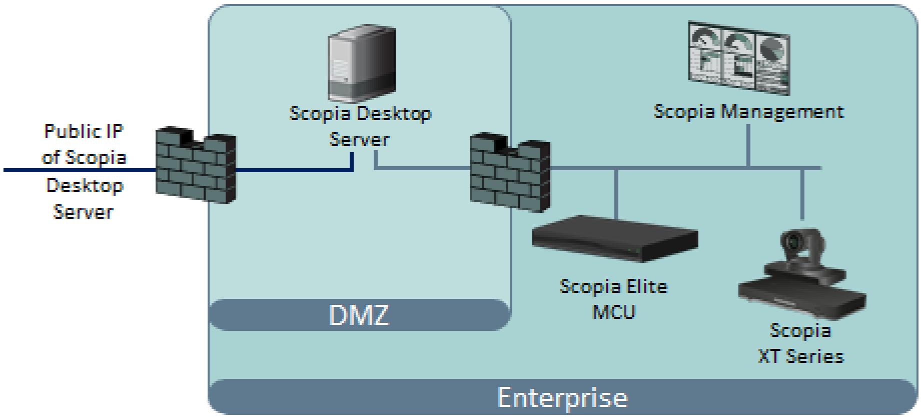


Figure 143: Scopia Desktop with a dual-NIC deployment

Scopia Desktop Clients can connect to the Scopia Desktop Server either by an IP address or a DNS name. In many deployments the Scopia Desktop Server IP address is not accessible to clients outside the enterprise due to NAT or firewall restrictions. Therefore, Scopia Desktop Server has a public address, which must be a DNS name resolving to the correct Scopia Desktop Server IP address both inside and outside the corporate network.

Estimating and Planning your Bandwidth Requirements

We recommend estimating Scopia Desktop's impact on bandwidth to determine if your current infrastructure needs updating. Planning bandwidth may help reduce costs in your organization.

This section explains how to estimate the bandwidth for external Scopia Desktop users connecting to your network.

Important:

You do not need to estimate bandwidth required by users who connect from within the internal network, because, typically, internal bandwidth is sufficient for videoconferencing.

You can allocate the bandwidth depending on the needs of your organization. For example, if your organization uses many HD videoconferences and has few users downloading recordings, you may decide to increase the bandwidth for participants, and decrease the bandwidth allocated for recordings.

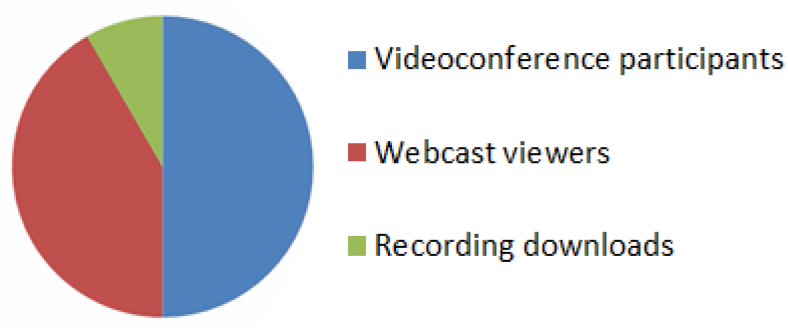


Figure 144: Example of allocating bandwidth in an organization

Since the Scopia Desktop coordinates videoconferences between Scopia Desktop Clients/Scopia Mobile devices and the MCU, you must plan bandwidth required by the Scopia Desktop Server and by the MCU jointly. Consider the MCU resources when planning your Scopia Desktop bandwidth. The bandwidth used by each Scopia Desktop Client indirectly determines the capacity of your deployed MCUs. Your chosen video resolution (and bandwidth), places demands on your MCU to supply that video resolution for each connection, which determines how many users can simultaneously connect to the MCU.

To assess the overall bandwidth for the videoconferencing solution including other types of endpoints, refer to the Avaya Equinox Solution Guide.

Related links

Calculating the Bandwidth Used by Avaya Scopia Desktop Participants on page 302

Calculating the Bandwidth Used by Avaya Scopia Desktop Participants

About this task

Videoconference participants consume most of the bandwidth in your Avaya Scopia Desktop deployment, because they both upload and download live media.

This section explains how to estimate the bandwidth for external Scopia Desktop users connecting to your network.

Important:

You do not need to estimate bandwidth required by users who connect from within the internal network, because, typically, internal bandwidth is sufficient for videoconferencing.

The amount of bandwidth consumed by participants mainly depends on the chosen topology and the maximum bandwidth you allow per participant. You configure the maximum bandwidth per participant in the Scopia Desktop Server which is the maximum possible bandwidth for any participant connecting to this server.

However, you can allow different maximum bandwidth for authenticated users by configuring user profiles and their maximum bandwidth in Avaya Equinox Management. You can also set the maximum bandwidth for guest users in Equinox Management. The maximum bandwidth for user profiles and guest users cannot exceed the maximum bandwidth configured in the Scopia Desktop Server. For example, you create a user profile on Equinox Management whose maximum bandwidth is less then the value you configured in the Scopia Desktop Server. In this case a user belonging to this profile uses the maximum bandwidth configured for the profile, not the possible maximum bandwidth of the Scopia Desktop Server (Figure 145: Equinox Management user profiles within maximum bandwidth set by Scopia Desktop Server on page 303).

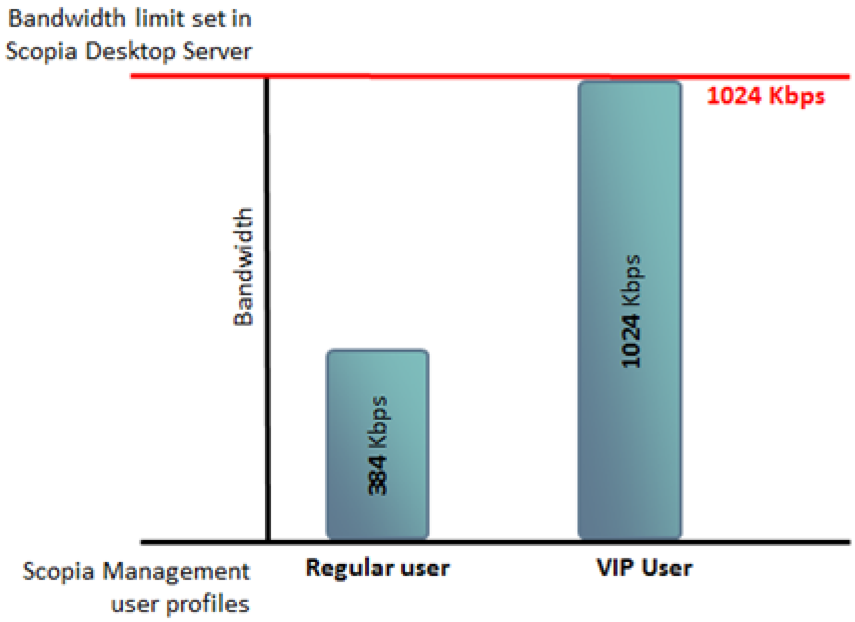


Figure 145: Equinox Management user profiles within maximum bandwidth set by Scopia Desktop Server

You calculate the maximum bandwidth used by Avaya Scopia Desktop participants in the following steps:

Procedure

1. Estimate the number of Avaya Scopia Desktop participants connecting externally.

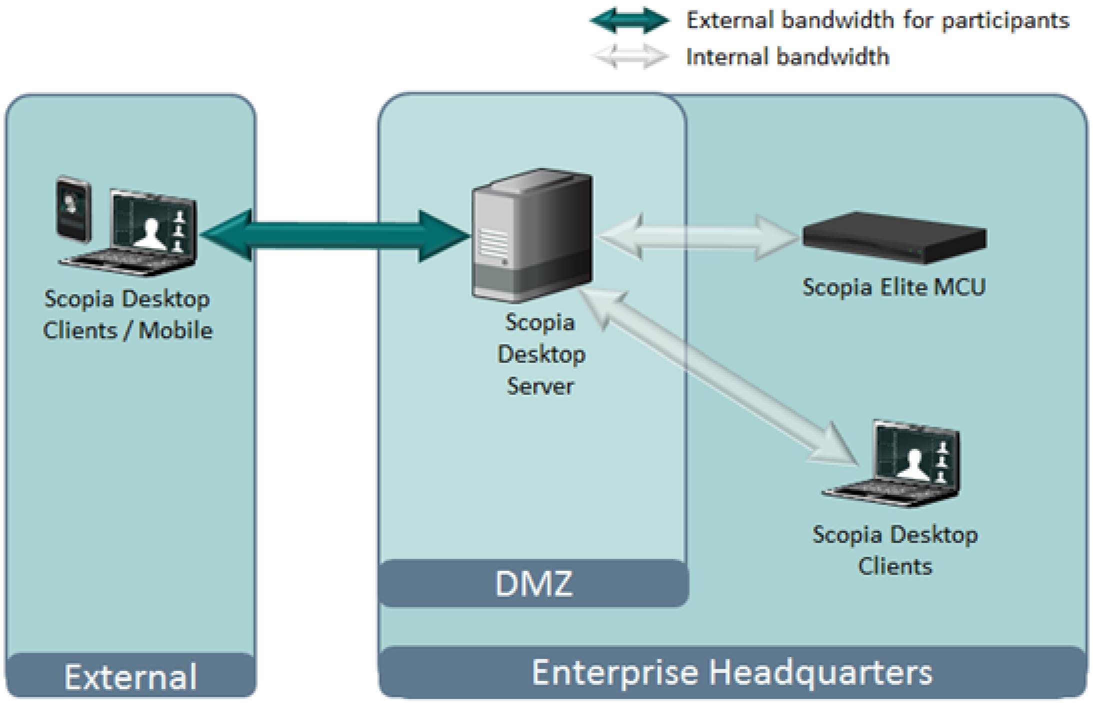


Figure 146: External bandwidth required for centralized deployments

2. (Optional for a distributed deployment) Estimate the number of Avaya Scopia Desktop participants connecting to the Scopia Desktop Server from other branches of your organization, as shown in Figure 147: External bandwidth required for distributed deployments on page 305:

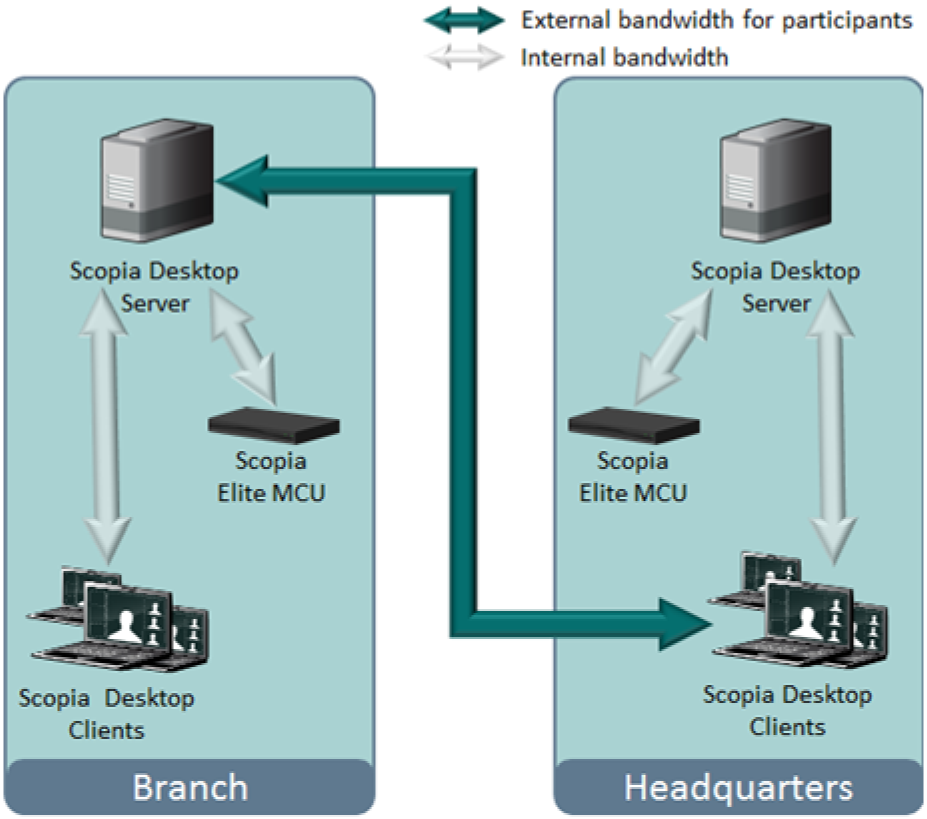


Figure 147: External bandwidth required for distributed deployments

3. (Optional for a distributed deployment) Calculate the total number of participants using external bandwidth by adding the numbers you acquired in steps 1 on page 303 and 2 on page 304.

   To illustrate how to estimate bandwidth, we shall use an example of 200 external participants: 100 external participants and 100 participants connecting from other branches.

4. Define the ratio of participants in concurrent videoconferences to all Avaya Scopia Desktop participants.

   A typical ratio for Avaya Scopia Desktop and Scopia Mobile is between 1/20 and 1/10, so that on average, one of every 10 or 20 users participate in a videoconference at the same time.

5. Estimate the peak usage for participants connecting from the external network and from other branches.

   This value represents the maximum number of participants connecting to your Scopia Desktop Server simultaneously. Use the following formula to calculate it:

   ```
   Peak usage = total number of participants / ratio
   ```

   For example, if there are 200 external participants and the ratio is 20, the peak usage is 10.

6. Decide on the maximum bandwidth per Scopia Desktop Client (measured as its bitrate).

Consider the following factors:

- Sharing bandwidth between live video and presentation

  When one of the participants is presenting during a videoconference, presentation uses the bandwidth you defined for Scopia Desktop participants. Typically, presentation uses 384 kbps. For example, if the maximum bandwidth you define for participants is 768 kbps, it decreases to 384 kbps after presentation is started. To ensure the video quality, add 384 kbps required for presentation to the bandwidth for participants.

- The desired video resolution

  Increasing video resolution requires higher bitrate. For example, each Scopia Desktop Client requires at least 384 kbps for a SD videoconference at 480p, or at least 512 kbps for an HD videoconference at 720p (depending on the MCU model).

- The MCU capacity

  The MCU capacity determines how many users can simultaneously connect to a videoconference with a given video resolution. As you increase the video resolution, the number of users that can be supported by the MCU decreases. For example, for a 480p videoconference, each Scopia Desktop Client users 1/4 port on the Scopia® Elite 6000 MCU. For a 720p videoconference, however, each Scopia Desktop Client uses either 1/2 or 1 port, depending on your license. For more information, see the *Installation Guide for Scopia Elite MCU*. See Figure 148: Planning the maximum bandwidth based on MCU capacity on page 306.

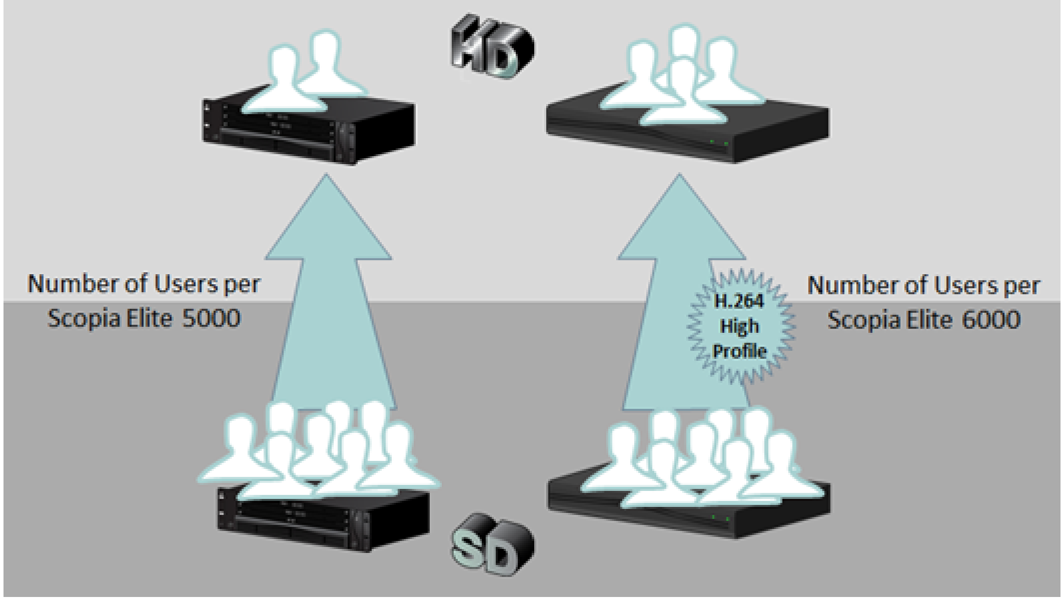

HD
Number of Users per Scopia Elite 5000
H.264 High Profile
Number of Users per Scopia Elite 6000
SD

Figure 148: Planning the maximum bandwidth based on MCU capacity

The number of participants that can be hosted by a single MCU depends on the MCU model. For more information, see *Installation Guide for Scopia Elite MCU*.

7. Calculate the peak bandwidth according to the following formula:

```
Peak bandwidth = peak usage x maximum bandwidth per participant
```

In our example of the Avaya Scopia Desktop deployment, where the peak usage is 10 and the chosen maximum bandwidth is 768 Kbps, the peak bandwidth equals 7680 kbps. This is the rough estimation of the bandwidth required for videoconference participants.

8. Fine-tune your estimation by deciding on the following bandwidth effective policies supported in Equinox Solution.

   - The compression capabilities of the MCU and Avaya Scopia Desktop

     The Scopia® Elite 6000 MCU and Avaya Scopia Desktop offer H.264 High Profile encoding, allowing a higher resolution at a lower bitrate than other MCUs.

     If your deployment also includes an MCU without H.264 High Profile (such as the Scopia® Elite 5000 Series MCU), endpoints connecting to this MCU may use a lower resolution for the same bandwidth.

     Table 41: Bandwidth and capacity requirements for each Scopia Desktop Client on page 307 illustrates how the same resolution in the newer MCU model requires less bandwidth and fewer ports because of H.264 High Profile.

Table 41: Bandwidth and capacity requirements for each Scopia Desktop Client

Video Resolution	Scopia® Elite 5000 Series MCU		Scopia® Elite 6000 MCU with H.264 High Profile	
	Bitrate	**Capacity**	**Bitrate**	**Capacity**
352p	384 kbps	Each Scopia Desktop Client uses 1/4 port	256 kbps	Each Scopia Desktop Client uses 1/4 port
480p	512 kbps	Each Scopia Desktop Client uses 1 port (or 1/2 port with the MCU's double capacity license, see *Installation Guide for Scopia Elite MCU* for more information)	384 kbps	Each Scopia Desktop Client uses 1/4 port
720p	768 kbps	Each Scopia Desktop Client uses 1 port	512 kbps	Each Scopia Desktop Client uses 1 port (or 1/2 port with the MCU's double capacity license, see *Installation Guide for Scopia Elite MCU* for more information)
1080p			1280 kbps	Each Scopia Desktop Client uses 1 port

   - Cascading for using bandwidth and resources more effectively

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

You can configure Equinox Management to determine whether your distributed MCUs form cascaded meetings. For more information, see *Administrator Guide for Equinox Management*.

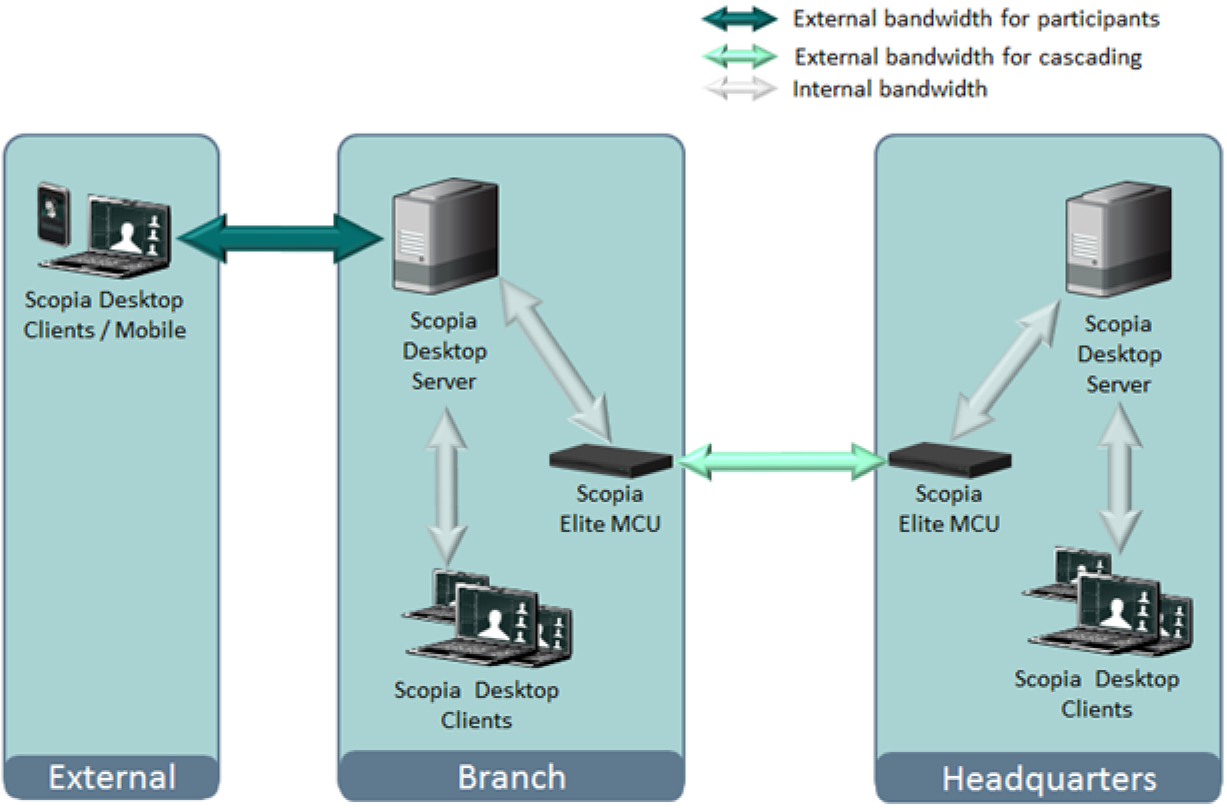


Figure 149: Using cascading to reduce bandwidth usage

The bandwidth used by a cascaded link is equivalent to only a single client connection in each direction: upload and download. The bandwidth value is determined by the MCU meeting type (or service), which is invoked when choosing a dial prefix for the meeting. You define the maximum bandwidth for each meeting type in the MCU. For more information on defining meeting types, see *Administrator Guide for Scopia® Elite 6000 MCU*.

- Setting bandwidth limits for Scopia Desktop users.

  You can define different maximum bandwidth for Scopia Desktop authenticated users and guests using Equinox Management. The maximum bandwidth configured in Equinox Management cannot exceed the maximum bandwidth configured on a Scopia Desktop to which the users connect. For more information see *Administrator Guide for Equinox Management*.

9. Add margins to make sure that even in poor network conditions video quality does not drop below the standard you decided on.

Important:

An average margin is 20% of your fine-tuned estimation.

Related links

Estimating and Planning your Bandwidth Requirements on page 301

Ports to Open on Avaya Scopia Desktop

The Scopia Desktop Server is typically located in the DMZ (see Figure 150: Locating the Scopia Desktop Server in the DMZ on page 309) and is therefore connected to both the enterprise and the public networks. Scopia Desktop Clients can be located in the internal enterprise network, in the public network, or in a partner network.

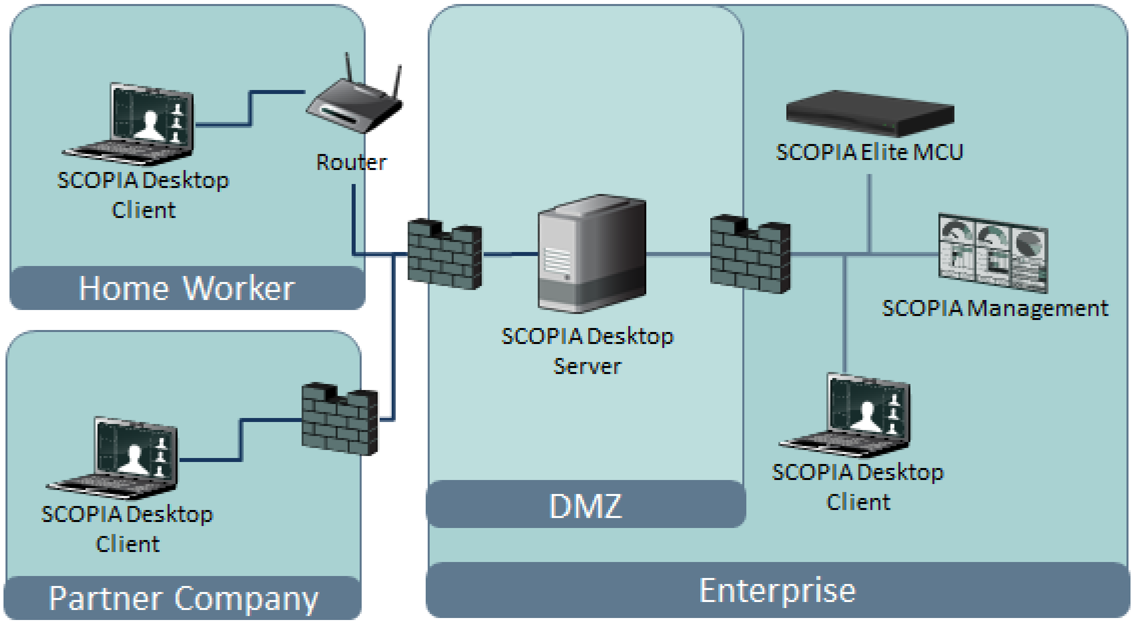


Figure 150: Locating the Scopia Desktop Server in the DMZ

When opening ports between the DMZ and the enterprise on the Scopia Desktop Server, use the following as a reference:

- When opening ports that are both in and out of the Scopia Desktop Server, see Table 42: Bidirectional Ports to Open Between the Scopia Desktop Server and the Enterprise on page 310.
- When opening ports that are outbound from the Scopia Desktop Server, see Table 43: Outbound Ports to Open from the Scopia Desktop Server to the Enterprise on page 311.
- When opening ports that are inbound to the Scopia Desktop Server, see Table 44: Inbound Ports to Open from the Enterprise to the Scopia Desktop server on page 312.

When opening ports between the DMZ and the public on the Scopia Desktop Server, use the following as a reference:

- When opening ports that are both in and out of the Scopia Desktop Server, see Table 45: Bidirectional Ports to Open Between the Scopia Desktop server and the Public on page 313.
- When opening ports that are inbound from the Scopia Desktop Server, see Table 46: Inbound Ports to Open from the Public to the Scopia Desktop server on page 313.

When opening bidirectional ports between Scopia Desktop Clients, see Table 47: Bidirectional Ports to Open Between Scopia Desktop Clients on page 314.

When opening inbound ports from the Scopia Desktop Clients to the STUN server, see Table 48: Inbound Ports to Open from the Scopia Desktop Client to the STUN Server on page 314.

Important:

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

Table 42: Bidirectional Ports to Open Between the Scopia Desktop Server and the Enterprise

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
7640	TCP	Content Center Server	Enables connection between the Scopia Desktop Server and the Content Center Server, when installed on different servers.	Cannot communicate with the Content Center Server and some capabilities (such as recording and streaming) do not function properly	Mandatory
1024- 65535	TCP (H. 245/ Q. 931)	MCU or H.323 Gatekeeper, depending on deployment	Enables connection to Scopia Desktop meetings.	Cannot connect to the meeting	Mandatory To limit range, see Limiting the TCP Port Range for H. 245/Q.931 on the Scopia Desktop Server on page 315
10000-65535	UDP (RTP)	MCU or Scopia Desktop Client	Enables media connection to the MCU , and the Scopia Desktop Client or Scopia Mobile.	Media cannot be passed from the MCU to Scopia Desktop Clients. Also, connection is tunneled via TCP	Mandatory To limit range, see Limiting the UDP Port

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
				port 443 resulting in a drop in performance.	Range for RTP/RTCP on the Scopia Desktop Server on page 315

Table 43: Outbound Ports to Open from the Scopia Desktop Server to the Enterprise

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
137,138	UDP	Active Directory	Enables auto-discovery and authentication	Cannot perform auto-discovery and authentication	Recommended for performing Active Directory authentication
139,445	TCP	Active Directory	Enables auto-discovery and authentication	Cannot perform auto-discovery and authentication	Recommended for Active Directory authentication
1719	UDP (RAS)	H.323 Gatekeeper or the internal gatekeeper in Equinox Management	Enables communication with H.323 Gatekeeper or the internal gatekeeper in Equinox Management	Cannot connect to the meeting	Mandatory
1720	TCP	MCU or H.323 Gatekeeper, depending on deployment	Enables connection to Scopia Desktop meetings.	Cannot connect to the meeting	Mandatory
3337	TCP (XML)	MCU	Enables meeting cascading connection to the MCU	Meeting cascading connection is disabled	Mandatory
5269	TCP	XMPP Server	Enables sever-to-server connections in cases where multiple Jabber servers are deployed as a federation or cluster.	Scopia Desktop Clients cannot login and use the contact list.	Mandatory only in deployments of two or more Jabber servers deployed as a federation or cluster which must communicate via a firewall

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
6972-65535	UDP	Streaming Server	Enables media connection to the Scopia Desktop Streaming Server, if separated from Scopia Desktop server by a firewall.	Cannot connect to the Scopia Desktop Streaming server.	Mandatory To avoid opening these ports, place the Scopia Desktop server in the same zone as the streaming server.

Table 44: Inbound Ports to Open from the Enterprise to the Scopia Desktop server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
80	TCP (HTTP)	Web client	Provides access to the Scopia Desktop server Web Portal (you can configure port 443 instead)	Cannot access the Scopia Desktop server Web Portal	Mandatory if using HTTP. You can configure this port during installation. For more information, see Installing or upgrading your Avaya Scopia Desktop deployment on page 318.
443	TCP (TLS)	Scopia Desktop Clients and Scopia Mobile	Enables sending control messages between the Scopia Desktop server and Clients, and is also used to tunnel RTP media if the UDP ports are blocked	Scopia Desktop Client or Scopia Mobile cannot connect to the Scopia Desktop server	Mandatory
3340	TCP	Equinox Management	Enables meeting control connection with Equinox Management	Meeting control connection to Equinox Management is disabled	Mandatory
7070	TCP	Streaming Server	Enables Scopia Desktop Clients to send tunneled RTSP traffic	Scopia Desktop Clients cannot receive video streams	Mandatory To configure, see Configuring the TCP Streaming Port on the Scopia Desktop Server on page 316

Table 45: Bidirectional Ports to Open Between the Scopia Desktop server and the Public

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
10000-65535	UDP (RTP/ RTCP)	Scopia Desktop Client or Scopia Mobile	Enables media connection with the Scopia Desktop Client or Scopia Mobile	Connection is tunneled via TCP port 443 and performance is not optimal	Recommended To configure, see Limiting the UDP Port Range for RTP/RTCP on the Scopia Desktop Server on page 315

Table 46: Inbound Ports to Open from the Public to the Scopia Desktop server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
80	TCP (HTTP)	Web client	Provides access to the web user interface (you can configure port 443 instead)	Cannot access the web user interface	Mandatory if using HTTP. You can configure this port during installation. For more information, see Installing or upgrading your Avaya Scopia Desktop deployment on page 318.
443	TCP (TLS)	Scopia Desktop Clients and Scopia Mobile	Enables sending control messages between the Scopia Desktop server and Clients, and is also used to tunnel RTP media if the UDP ports are blocked	Scopia DesktopClients cannot connect to the Scopia Desktop server	Mandatory
7070	TCP	Streaming Server	Enables Scopia Desktop servers to send tunneled RTSP traffic	Scopia Desktop Clients cannot receive video streams	Mandatory To configure, see Configuring the TCP Streaming Port on the Scopia Desktop Server on page 316.

Table 47: Bidirectional Ports to Open Between Scopia Desktop Clients

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
5060	UDP (SIP)	Scopia Desktop Client	Establishes direct SIP point-to-point connections between two Scopia Desktop Clients	Calls are routed via the Scopia Desktop server	Recommended
1025-65535	UDP	Scopia Desktop Client	Establishes direct SIP point-to-point connections between two Scopia Desktop Clients	Calls are routed via the Scopia Desktop server	Recommended

Table 48: Inbound Ports to Open from the Scopia Desktop Client to the STUN Server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3478	UDP	Scopia Desktop Clients	Enables connection between the STUN Server and Scopia Desktop Clients when making a point-to-point call. To connect point-to-point calls directly between two Scopia Desktop Clients, open the UDP ports (10000-65535, 6972-65535, 3478).	Scopia Desktop Client cannot connect to the STUN server and uses the Scopia Desktop Server as a relay agent.	Optional

Important:

Some firewalls are configured to block packets from the streaming server. You can either configure the firewall to allow streaming packets, or reconfigure the streaming server and client to use different network protocols that cross the firewall boundary.

The Streaming Server uses the IETF RTSP/RTP protocols. RTSP runs over TCP, while RTP runs over UDP. The streaming server can tunnel RTSP/RTP traffic through standard HTTP. Some firewalls may inspect traffic on port 80 and not allow the tunneled RTSP/RTP on that port. We therefore recommend using the QuickTime standard port 7070 as the alternate TCP port for HTTP tunneling. This is configured in the streaming server by default as long as you specify the port as part of the streaming server virtual address, as described in Configuring the TCP Streaming Port on the Scopia Desktop Server on page 316.

Related links

Limiting Port Ranges on the Scopia Desktop Server on page 314

Limiting Port Ranges on the Scopia Desktop Server

About this task

This section provides instructions of how to limit the following port ranges on the Scopia Desktop Server:

Related links

Ports to Open on Avaya Scopia Desktop on page 309

Limiting the UDP Port Range for RTP/RTCP on the Scopia Desktop Server on page 315

Limiting the TCP Port Range for H.245/Q.931 on the Scopia Desktop Server on page 315
Configuring the TCP Streaming Port on the Scopia Desktop Server on page 316

Limiting the UDP Port Range for RTP/RTCP on the Scopia Desktop Server

About this task

The Scopia Desktop Server has designated 10000-65535 as the default port range for UDP (RTP/RTCP). To provide additional security for your firewall, you can limit this range.

To calculate approximately how many ports the Scopia Desktop Server uses, multiply the number of license connections by 14, which amounts to reserving 14 ports per client.

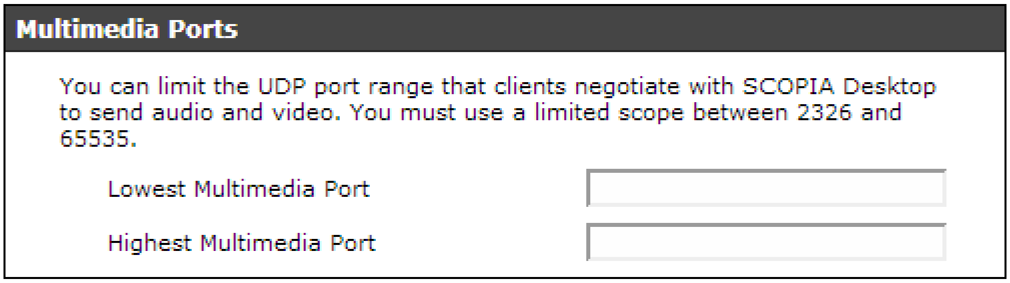
The minimum port range allowed on Scopia Desktop server is 100 ports.

In addition, add extra ports if your deployment includes:

- Add 6 ports per recording in your deployment.
- Add an extra 6 ports per conference which activates streaming.

Procedure

1. Log in to the Scopia Desktop Server Administrator web user interface.
2. Select **Client** > **Settings**.
3. Locate the **Multimedia Ports** section (see Figure 151: Multimedia Ports Area on page 315).



Multimedia Ports

You can limit the UDP port range that clients negotiate with SCOPIA Desktop to send audio and video. You must use a limited scope between 2326 and 65535.

Lowest Multimedia Port

Highest Multimedia Port

Figure 151: Multimedia Ports Area

4. Configure your port range (using any values between 2326 and 65535) by doing the following:
    a. Enter the base port value in the **Lowest Multimedia Port** field.
    b. Enter the upper port value in the **Highest Multimedia Port** field.
5. Select **OK** or **Apply**.

Related links

Limiting Port Ranges on the Scopia Desktop Server on page 314

Limiting the TCP Port Range for H.245/Q.931 on the Scopia Desktop Server

About this task

The Scopia Desktop Server has designated ports 1024-65535 for TCP for H.245 and Q.931 signaling. To provide additional security for your firewall, you can limit this range.

For each conference, the Scopia Desktop Server uses 2 ports. In addition, add extra ports for:

- Add 2 ports for each participating Scopia Desktop Client client.
- Add 2 ports per conference when recording.
- Add 2 ports per conference when streaming.
- Add 1 port per conference when presenting using the content slider.

Procedure

1. Navigate to <*Scopia Desktop install_dir*>*\ConfSrv*.
2. Edit the *config.val* file as follows:
    a. Locate the text `1 system`.
    b. At the bottom of that section, add two lines:

    ```
    2 portFrom = <lowest range limit>
    2 portTo = <highest range limit>
    ```

    Where `<lowest range limit>` is the base port of your port range and `<highest range limit>` is the upper value of your port range.
3. Access the Windows services and restart the **Scopia Desktop - Conference Server** service.

Related links

Limiting Port Ranges on the Scopia Desktop Server on page 314

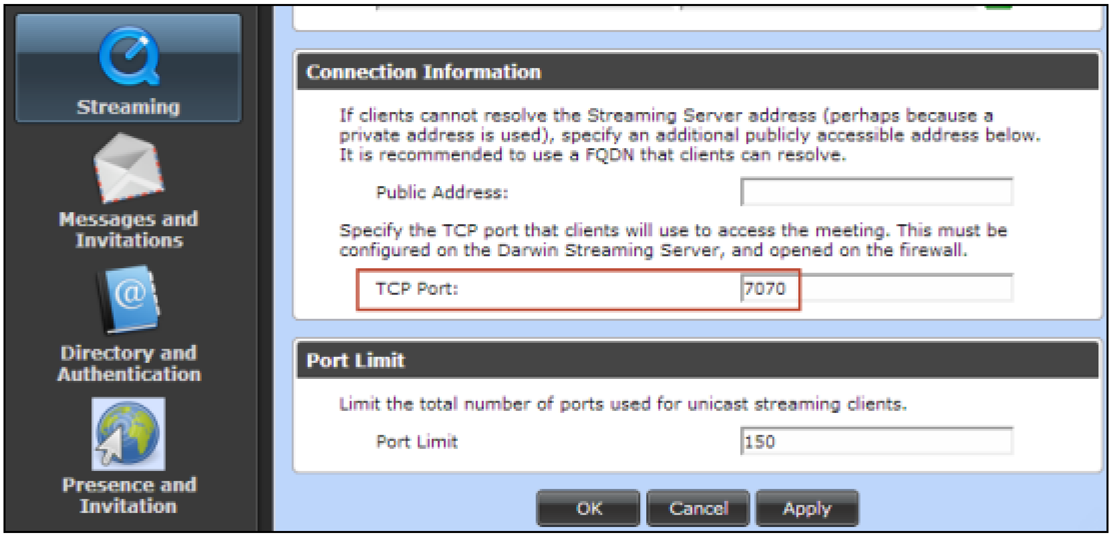
Configuring the TCP Streaming Port on the Scopia Desktop Server

About this task

The Streaming Server that is deployed with your Scopia Desktop Server is configured by default to use the QuickTime standard port 7070 as the alternate TCP port for HTTP tunneling. If your firewall is configured to block packets from the Streaming Server, you must reconfigure the Streaming Server and client to use different network protocols which can cross the firewall boundary.

Procedure

1. Log in to the Scopia Desktop Server Administrator web user interface.
2. Select **Streaming**. The **Settings** page for the Streaming Server appears (see Figure 152: Setting the streaming port for Scopia Desktop Server on page 317).



Connection Information

If clients cannot resolve the Streaming Server address (perhaps because a private address is used), specify an additional publicly accessible address below. It is recommended to use a FQDN that clients can resolve.

Public Address:

Specify the TCP port that clients will use to access the meeting. This must be configured on the Darwin Streaming Server, and opened on the firewall.

TCP Port: 7070

Port Limit

Limit the total number of ports used for unicast streaming clients.

Port Limit 150

Figure 152: Setting the streaming port for Scopia Desktop Server

3. Locate the **Connection Information** area.
4. Modify the port value in the **TCP Port** field.

   Important:

   The Streaming Server uses the IETF RTSP/RTP protocols. RTSP runs over TCP, while RTP runs over UDP. Many firewalls are configured to restrict TCP packets by port number and are very restrictive on UDP. The Streaming Server can tunnel RTSP/RTP traffic through standard HTTP. Some firewalls may inspect traffic on port 80 and not allow the tunneled RTSP/RTP on that port. We therefore recommend using the QuickTime standard port 7070 as the alternate TCP port for HTTP tunneling.
5. Select **OK** or **Apply**.
6. Do the following on the Scopia Desktop Server:
   a. Navigate to the following directory: C:\Program Files\Darwin Streaming Server.

   b. Open the *streamingserver.xml* file.

   c. Locate the list of ports for the RTSP protocol by finding the text `LIST-PREF NAME="rtsp_port"` in the file.

   ```
   <CONFIGURATION>
     <SERVER>
       <LIST-PREF NAME="rtsp_port" TYPE="UInt16" >
         <VALUE> 7070 </VALUE>
       </LIST-PREF>
   ```

   d. Within this section, add a new entry of `<VALUE> xxxx </VALUE>`, where `xxxx` is the new port value.

   e. Save the file.

   f. Restart the Darwin Streaming Server.

g. Restart the **Darwin Streaming Server** service.

Related links

Limiting Port Ranges on the Scopia Desktop Server on page 314

Installing Avaya Scopia Desktop Server

Installing or upgrading your Avaya Scopia Desktop deployment

Since Scopia Desktop Server has several components, you can choose to install all the components on the same computer, or choose to have some installed on a dedicated server. Typical configurations are:

- All components on one computer (Scopia Desktop Server).
- Dedicated servers for different components, often split as follows:
  - Dedicated Conference Server for Scopia Desktop.
  - Dedicated Content Center for Scopia Desktop.

For more information on the reasons for choosing dedicated servers versus a single server, see *Deploying Avaya Equinox Solution*, which is available from https://support.avaya.com/.

The dedicated Content Center Server for Scopia Desktop is the older system for streaming and recording videoconferences. Avaya continues to support this legacy system.

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 next generation HD streaming and recording platform. The Avaya Equinox Streaming and Recording Server replaces the Avaya Scopia Content Center Recording Server (SCC) server.

If you are upgrading from a version of the Equinox Solution that uses Content Center to a version of the Scopia solution that uses Equinox Streaming and Recording, you must ensure that you migrate the existing recordings from Content Center to Equinox Streaming and Recording. If you do not migrate the existing recordings from Content Center to Equinox Streaming and Recording, the recordings will not be available in the new system. If Content Center is on a standalone server, you can remove Content Center and repurpose that server after you migrate your recordings from Content Center to Equinox Streaming and Recording.

This section also discusses how to distribute Scopia Desktop Clients throughout your organization and how to access the Scopia Desktop Server Administrator web interface.

Installing All Scopia Desktop Components on a Single Server

About this task

Scopia Desktop Server includes various components which you can install on the same server for small deployments.

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 next generation HD streaming and recording platform. The Avaya Equinox Streaming and Recording Server replaces the Avaya Scopia Content Center Recording Server (SCC) server.

Tip:

> If you are installing all components on the same server, Avaya recommends the **Typical Install**. The **Typical Install** has fewer steps than the **Custom Install**. The **Typical Install** does not include Content Center or the Invitation and Presence server. For this reason, you can also choose the **Typical Install** when you want to install the conference server on a dedicated server. For informational purposes, this section describes the **Custom Install**.

For medium and large size deployments where you need power devoted to each component of the server, you can deploy a dedicated server devoted just one component of the Scopia Desktop Server, or you can choose a set of components on the same computer.

Follow these recommendations when installing the Scopia Desktop Server components:

- Do not install the Scopia Desktop Client on the same PC as any Scopia Desktop component.
- If you want to encrypt communication with HTTPS, configure the Conference Server for Scopia Desktop to port 443 after the installation is completed.

  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.

Follow this procedure to install the Scopia Desktop Server .

Before you begin

- Before installing, verify the computer meets the minimum hardware requirements for the number of intended users. For more information, see Minimum Requirements and Specifications of Scopia Desktop Server on page 289.
- Make sure you have enough space on the local hard drive to install all Scopia Desktop components.
- Ensure you have the correct license information.

  Important:

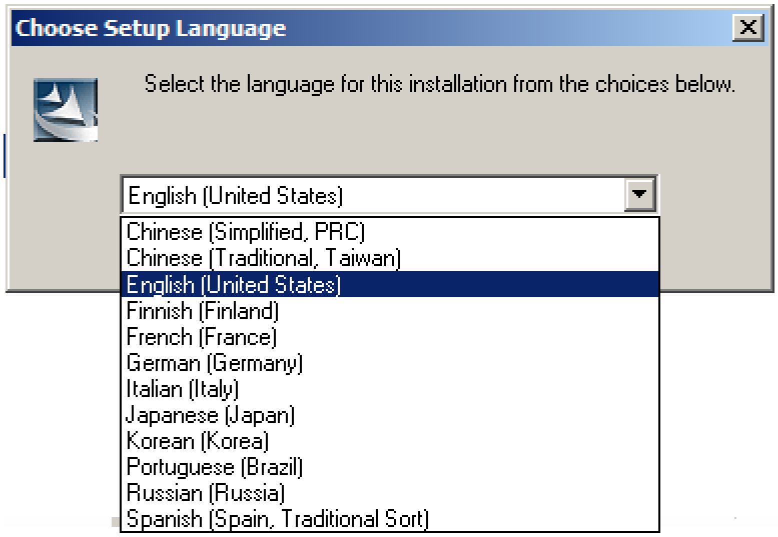
  > To use point-to-point functionality, you must install Equinox Management with the Avaya Scopia Desktop Pro license.

- By default, the older recording application, the Scopia Desktop Content Center (SCC) Server uses port 7070 streaming play. If you select a different port, change the default port value as explained in *Administration Guide for Scopia Desktop* and the *Port Security for the Avaya Equinox Solution Reference Guide*, which are available on https://support.avaya.com/.

- By default, the older recording application, Scopia Desktop Content Center (SCC) Server uses port 80 for recording play and download. If other applications on this PC use port 80, and you nevertheless want to use this port, access the Services panel in Windows and disable the IIS Administration, HTTP SSL, and World Wide Web Publishing services before installing the Conference Server.

Procedure

1. Launch the *setup.exe* file to start the Scopia Desktop Setup Wizard.
2. Select the installation language in the **Choose Setup Language** window, and select **OK**.



Choose Setup Language

Select the language for this installation from the choices below.

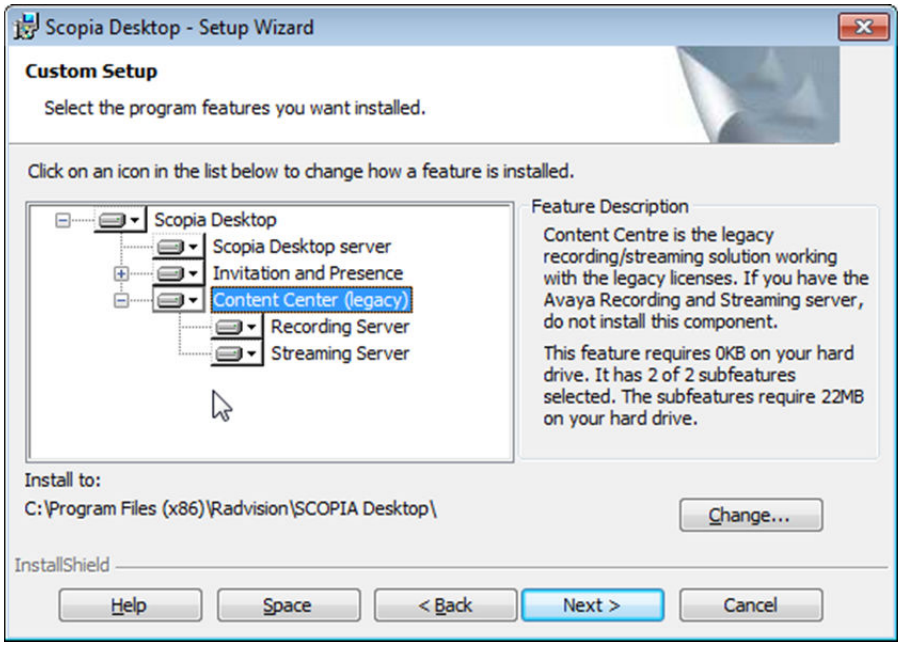
English (United States)

Figure 153: Choosing language for the installation

   Scopia Desktop starts the installation wizard.

3. Click **Next**, accept the license agreement, and click **Next**.
4. Select **Custom Install**, and click **Next**.
5. Choose the components that you want to install by clicking on each component icon and selecting **This feature will be installed on local hard drive** or **This feature will not be available**.

   For example, to install all components on a single server, including the legacy Content Center system, you can click on each component icon and select **This feature will be installed on local hard drive**. You only require the legacy Content Center system if you have existing recordings or want to support Content Center in the new installation.



Scopia Desktop - Setup Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- Scopia Desktop
  - Scopia Desktop server
  - Invitation and Presence
  - Content Center (legacy)
    - Recording Server
    - Streaming Server

Feature Description

Content Centre is the legacy recording/streaming solution working with the legacy licenses. If you have the Avaya Recording and Streaming server, do not install this component.

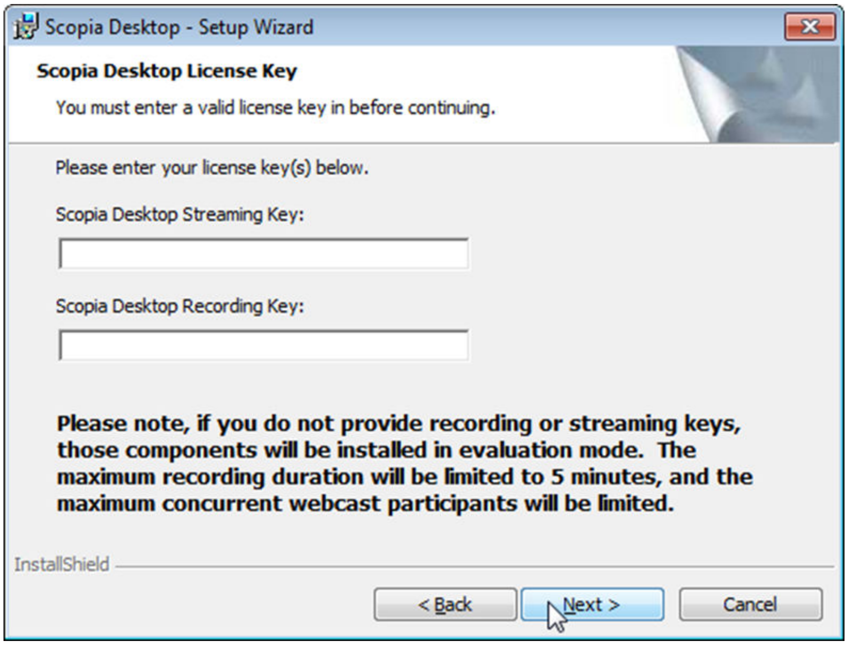
This feature requires 0KB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 22MB on your hard drive.

Install to:

C:\Program Files (x86)\Radvision\SCOPIA Desktop\

Figure 154: All components selected, including the legacy Content Center

6. **(Optional)** If you have chosen to install the legacy Content Center system, you must enter license keys for the recording component and the streaming component and click **Next**.



Scopia Desktop - Setup Wizard

Scopia Desktop License Key

You must enter a valid license key in before continuing.

Please enter your license key(s) below.

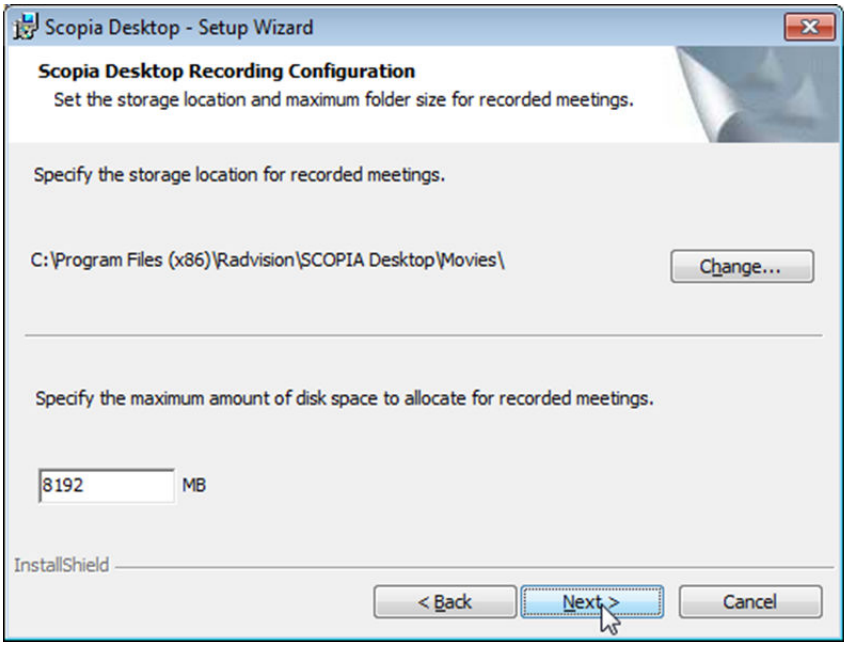
Scopia Desktop Streaming Key:

Scopia Desktop Recording Key:

Please note, if you do not provide recording or streaming keys, those components will be installed in evaluation mode. The maximum recording duration will be limited to 5 minutes, and the maximum concurrent webcast participants will be limited.

Figure 155: License keys for legacy Content Center system

7. **(Optional)** If you have chosen to install the legacy Content Center system, you must specify the storage location for recordings and the maximum allowed space for recordings and click **Next**.



Scopia Desktop - Setup Wizard

Scopia Desktop Recording Configuration

Set the storage location and maximum folder size for recorded meetings.

Specify the storage location for recorded meetings.

C:\Program Files (x86)\Radvision\SCOPIA Desktop\Movies\

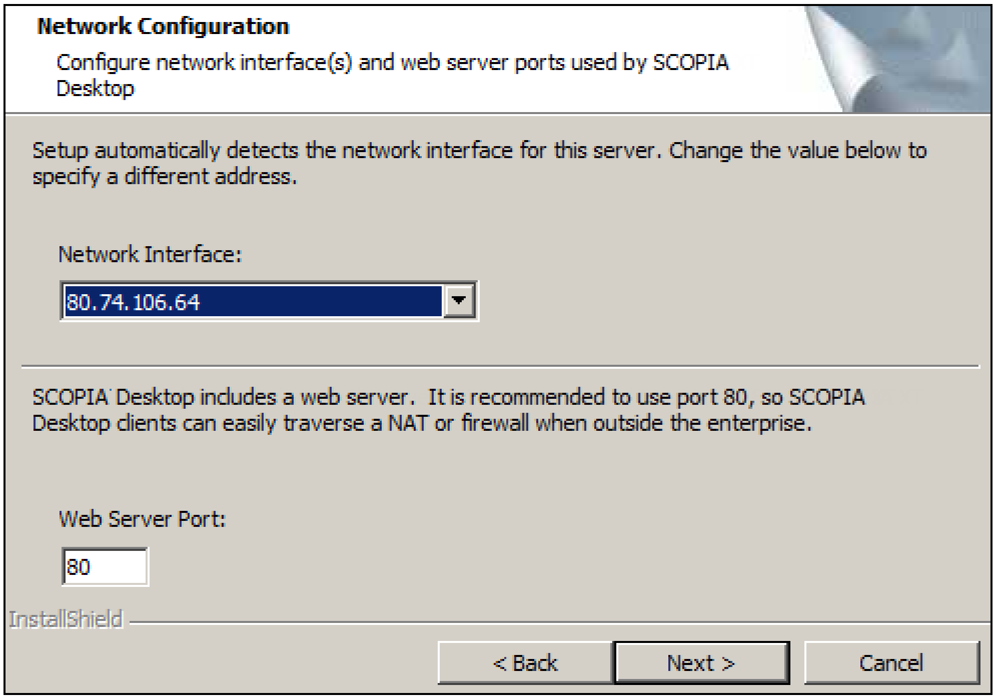
Specify the maximum amount of disk space to allocate for recorded meetings.

8192 MB

Figure 156: Storage details for legacy Content Center system recordings

8. In the **Network Configuration** window, select the IP address used for communicating with the MCU.

   If the server has one NIC card, the **Network Interface** field has only one value to choose, the IP of the NIC. For dual-NIC servers, select the network IP address pointing to the internal firewall.



Network Configuration

Configure network interface(s) and web server ports used by SCOPIA Desktop

Setup automatically detects the network interface for this server. Change the value below to specify a different address.

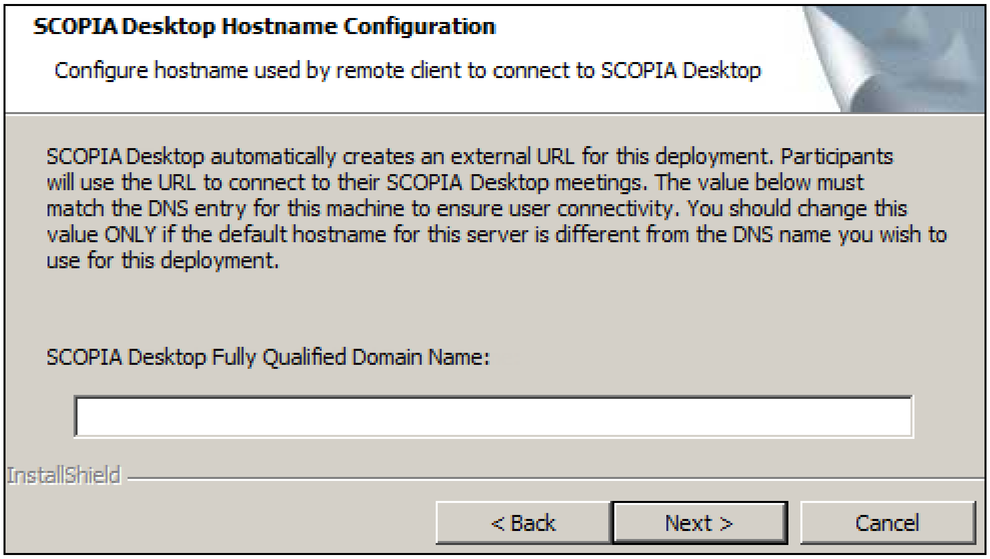
Network Interface: 80.74.106.64

SCOPIA Desktop includes a web server. It is recommended to use port 80, so SCOPIA Desktop clients can easily traverse a NAT or firewall when outside the enterprise.

Web Server Port: 80

Figure 157: Selecting the NIC pointing to the internal network

9. Change the default web server port if required, and then select **Next**.
10. In the **Hostname Configuration** window specify the public name of the d, to be used later as part of the URL sent to Scopia Desktop Clients to connect to videoconferences.



SCOPIA Desktop Hostname Configuration

Configure hostname used by remote client to connect to SCOPIA Desktop

SCOPIA Desktop automatically creates an external URL for this deployment. Participants will use the URL to connect to their SCOPIA Desktop meetings. The value below must match the DNS entry for this machine to ensure user connectivity. You should change this value ONLY if the default hostname for this server is different from the DNS name you wish to use for this deployment.

SCOPIA Desktop Fully Qualified Domain Name:

Figure 158: Defining the public address of the Scopia Desktop Server

> **Important:**
>
> An external Scopia Desktop Client must be able to resolve the server's hostname to the correct IP address from its location outside the enterprise. For example, do not use an internal DNS name if you have clients connecting from the public Internet.

11. Select **Install** in the **Ready to Install the Program** window.
12. Select **Finish**.
13. To change the Content Center settings, run the Setup Wizard again and navigate to the **Custom Setup** dialog.

Installing the Conference Server for Scopia Desktop on a Dedicated Server

About this task

This section details how to install a dedicated Conference Server for Scopia Desktop on a separate PC from the other server components.

For medium and large size deployments where you need power devoted to each component of the server, you can deploy a dedicated server devoted just one component of the Scopia Desktop Server, or you can choose a set of components on the same computer.

Follow these recommendations when installing the Scopia Desktop Server components:

- Do not install the Scopia Desktop Client on the same PC as any Scopia Desktop component.
- If you want to encrypt communication with HTTPS, configure the Conference Server for Scopia Desktop to port 443 after the installation is completed.

  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

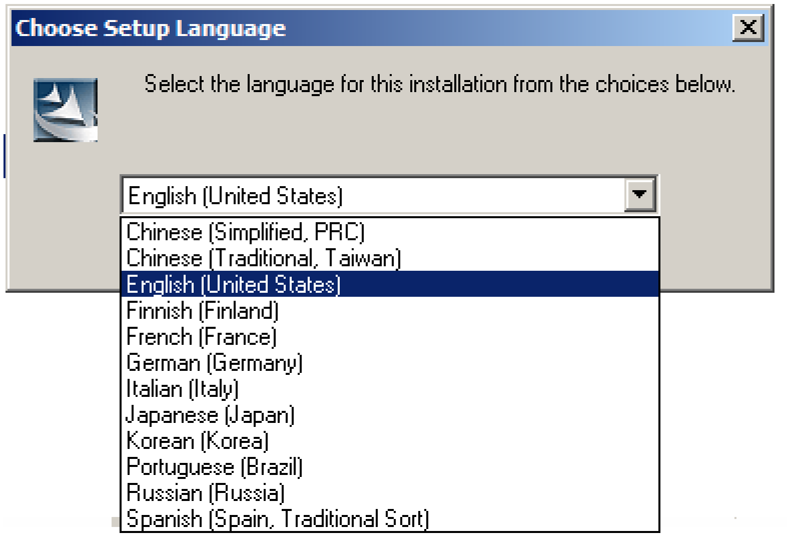
- Before installing, verify the computer meets the minimum hardware requirements for the number of intended users. For more information, see Minimum Requirements and Specifications of Scopia Desktop Server on page 289.
- Make sure you have enough space on the local hard drive to install the Scopia Desktop Server component as it requires 222MB.
- Ensure you have the correct license information.

  Important:

  To use point-to-point functionality, you must install Equinox Management with the Avaya Scopia Desktop Pro license.
- By default, the older recording application, Scopia Desktop Content Center (SCC) Server uses port 80 for recording play and download. If other applications on this PC use port 80, and you nevertheless want to use this port, access the Services panel in Windows and disable the IIS Administration, HTTP SSL, and World Wide Web Publishing services before installing the Conference Server.

Procedure

1. Launch the *setup.exe* file to start the Scopia Desktop Setup Wizard.
2. Select the installation language in the **Choose Setup Language** window, and select **OK**.



Select the language for this installation from the choices below.

Figure 159: Choosing language for the installation

Scopia Desktop starts the installation wizard.

3. Click **Next**, accept the license agreement, and click **Next**.
4. Select **Custom Install**, and click **Next**.
5. In the **Custom Setup** window, all components with the exception of Scopia Desktop Server are disabled.

   Verify that the various components are disabled. If they are not, disable the **Invitation and Presence** by selecting > **This feature will not be available** (Figure 160: Installing the Scopia Desktop component on the dedicated server on page 325). Repeat for the **Content Center**. For more information on the **Content Center** options, see Installing All Scopia Desktop Components on a Single Server on page 319.

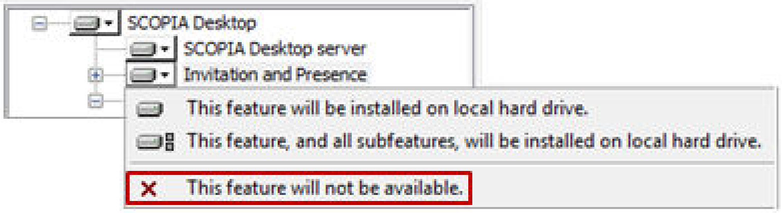

SCOPIA Desktop
SCOPIA Desktop server
Invitation and Presence
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.

Figure 160: Installing the Scopia Desktop component on the dedicated server

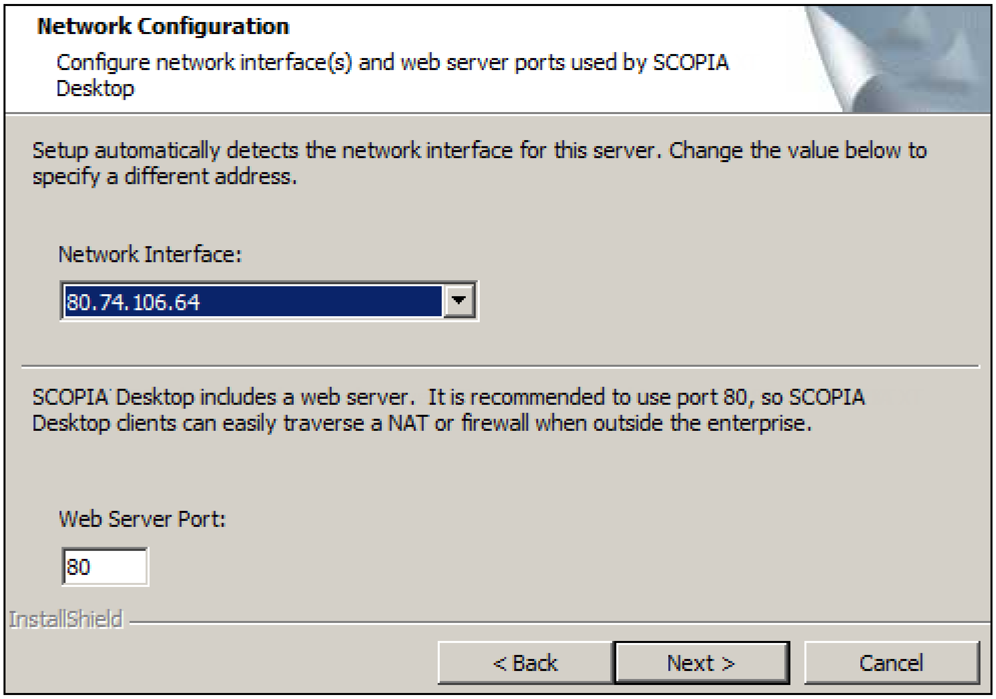
6. Ensure that **Scopia Desktop Server**, which is the option for the Conference Server, remains selected for local installation.

   Important:

   When installing a component, always use the default option (**This feature will be installed on the local hard drive**).

7. Change the installation folder if required, and select **Next**.
8. In the **Network Configuration** window, select the IP address used for communicating with the MCU.

   If the server has one NIC card, the **Network Interface** field has only one value to choose, the IP of the NIC. For dual-NIC servers, select the network IP address pointing to the internal firewall.



Network Configuration

Configure network interface(s) and web server ports used by SCOPIA Desktop

Setup automatically detects the network interface for this server. Change the value below to specify a different address.

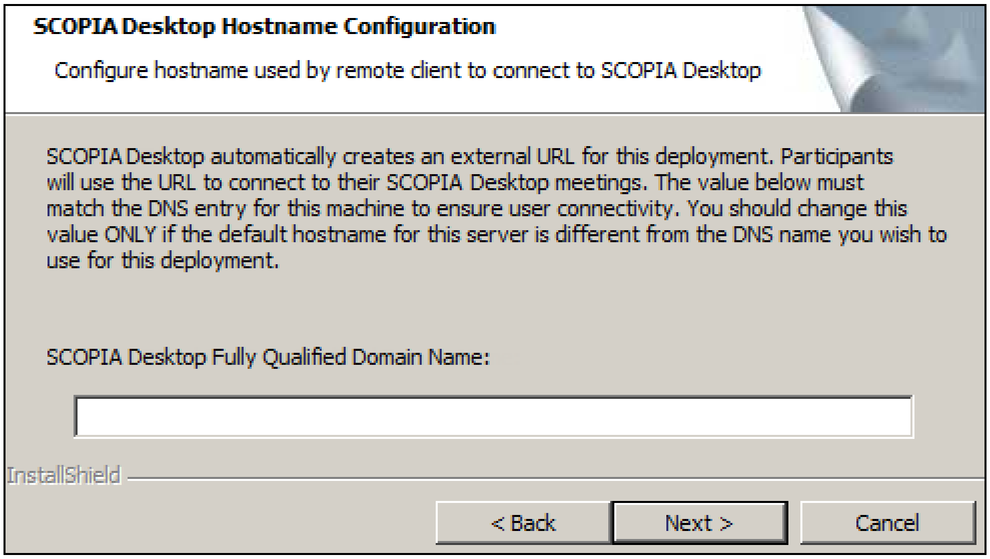
Network Interface: 80.74.106.64

SCOPIA Desktop includes a web server. It is recommended to use port 80, so SCOPIA Desktop clients can easily traverse a NAT or firewall when outside the enterprise.

Web Server Port: 80

Figure 161: Selecting the NIC pointing to the internal network

9. Change the default web server port if required, and then select **Next**.
10. In the **Hostname Configuration** window specify the public name of the d, to be used later as part of the URL sent to Scopia Desktop Clients to connect to videoconferences.



SCOPIA Desktop Hostname Configuration

Configure hostname used by remote client to connect to SCOPIA Desktop

SCOPIA Desktop automatically creates an external URL for this deployment. Participants will use the URL to connect to their SCOPIA Desktop meetings. The value below must match the DNS entry for this machine to ensure user connectivity. You should change this value ONLY if the default hostname for this server is different from the DNS name you wish to use for this deployment.

SCOPIA Desktop Fully Qualified Domain Name:

Figure 162: Defining the public address of the Scopia Desktop Server

Important:

An external Scopia Desktop Client must be able to resolve the server's hostname to the correct IP address from its location outside the enterprise. For example, do not use an internal DNS name if you have clients connecting from the public Internet.

11. Select **Install** in the **Ready to Install the Program** window.
12. Select **Finish**.

Installing the Content Center for Scopia Desktop on a Dedicated Server

About this task

This section details how to install a dedicated Content Center Server for Scopia Desktop on a separate PC from the other server components. The Content Center Server includes the recording, streaming and content slider components.

The dedicated Content Center Server for Scopia Desktop is the older system for streaming and recording videoconferences. Avaya continues to support this legacy system.

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 next generation HD streaming and recording platform. The Avaya Equinox Streaming and Recording Server replaces the Avaya Scopia Content Center Recording Server (SCC) server.

If you are upgrading from a version of the Equinox Solution that uses Content Center to a version of the Scopia solution that uses Equinox Streaming and Recording, you must ensure that you migrate the existing recordings from Content Center to Equinox Streaming and Recording. If you do not migrate the existing recordings from Content Center to Equinox Streaming and Recording, the recordings will not be available in the new system. If Content Center is on a standalone server, you can remove Content Center and repurpose that server after you migrate your recordings from Content Center to Equinox Streaming and Recording.

For medium and large size deployments where you need power devoted to each component of the server, you can deploy a dedicated server devoted just one component of the Scopia Desktop Server, or you can choose a set of components on the same computer.

Follow these recommendations when installing the Scopia Desktop Server components:

- Do not install the Scopia Desktop Client on the same PC as any Scopia Desktop component.

Before you begin

- Before installing, verify the computer meets the minimum hardware requirements for the number of intended users. For more information, see Minimum Requirements and Specifications of Scopia Desktop Server on page 289.
- Make sure you have enough space on the hard drive to install the component. The Streaming Server and the Recording Server require 26MB on the hard drive.

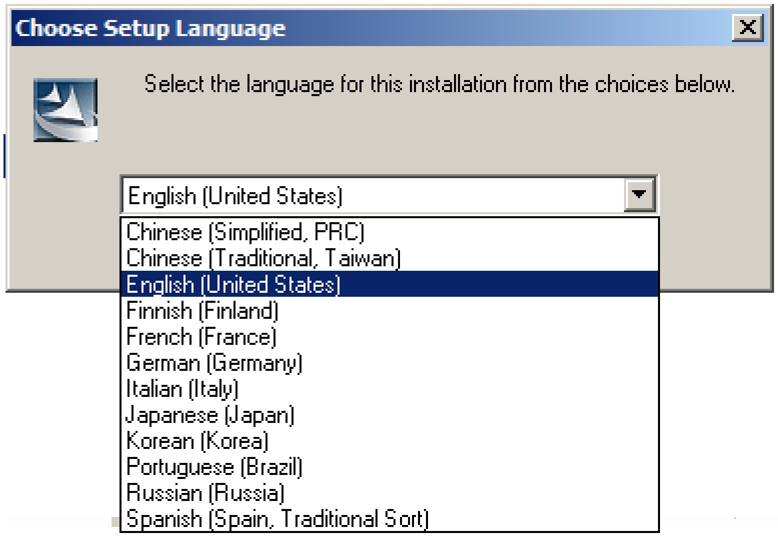
  If you want to store recordings locally, a typical recording for a one-hour meeting at 384 kbps takes up to 200MB. Alternatively, you can use a storage server in the enterprise.
- Ensure you have the correct license information.

  Important:

  When installing all components of the Content Center, you do not need a Scopia Desktop license key.
- By default, the older recording application, the Scopia Desktop Content Center (SCC) Server uses port 7070 streaming play. If you select a different port, change the default port value as explained in *Administration Guide for Scopia Desktop* and the *Port Security for the Avaya Equinox Solution Reference Guide*, which are available on https://support.avaya.com/.

Procedure

1. Launch the *setup.exe* file to start the Scopia Desktop Setup Wizard.
2. Select the installation language in the **Choose Setup Language** window, and select **OK**.



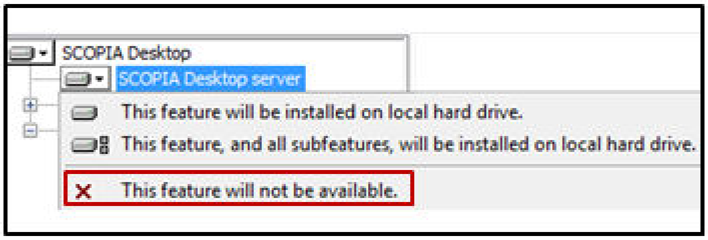
Choose Setup Language

Select the language for this installation from the choices below.

Figure 163: Choosing language for the installation

Scopia Desktop starts the installation wizard.

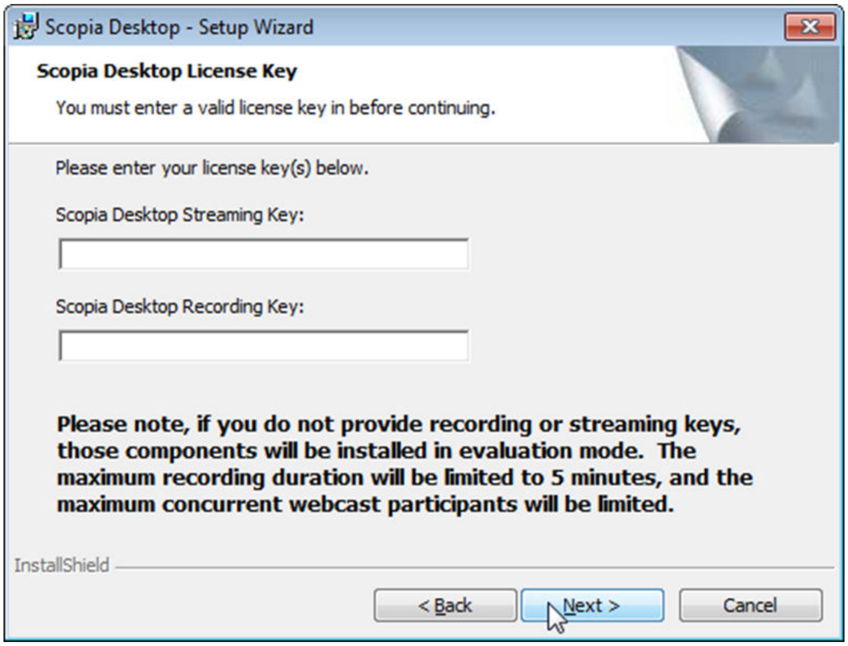
3. Click **Next**, accept the license agreement, and click **Next**.
4. Select **Custom Install**, and click **Next**.
5. In the **Custom Setup** window disable the **Scopia Desktop Server** by selecting > **This feature will not be available**. Repeat for the **Invitation and Presence** option.



SCOPIA Desktop
SCOPIA Desktop server
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.

Figure 164: Disabling a Scopia Desktop component on a dedicated server

6. Enable the **Content Center** item by selecting > **This feature will be installed on local hard drive**.
7. Change the installation folder if required, and select **Next**.
8. **(Optional)** If you have chosen to install the legacy Content Center system, you must enter license keys for the recording component and the streaming component and click **Next**.



Scopia Desktop - Setup Wizard

Scopia Desktop License Key

You must enter a valid license key in before continuing.

Please enter your license key(s) below.

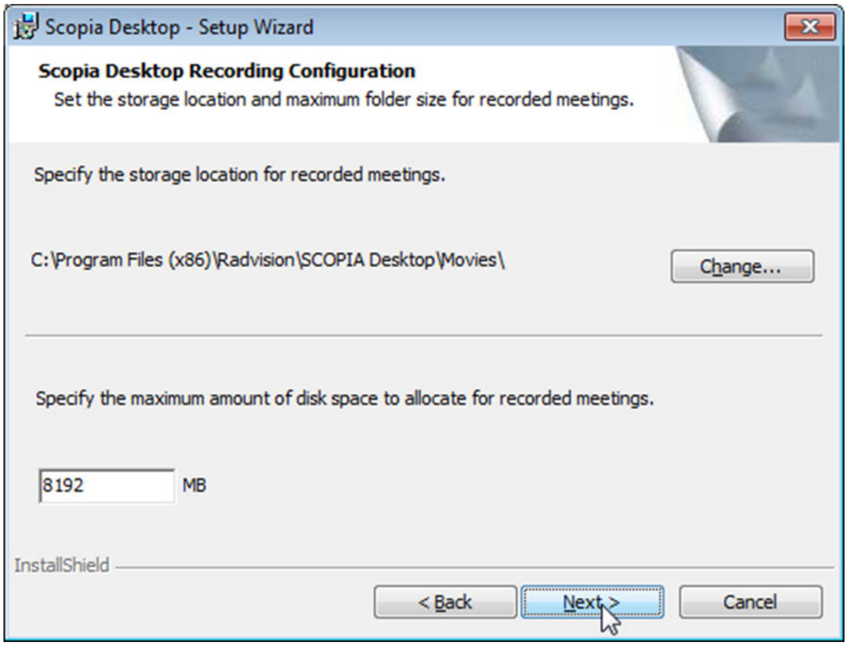
Scopia Desktop Streaming Key:

Scopia Desktop Recording Key:

Please note, if you do not provide recording or streaming keys, those components will be installed in evaluation mode. The maximum recording duration will be limited to 5 minutes, and the maximum concurrent webcast participants will be limited.

Figure 165: License keys for legacy Content Center system

9. **(Optional)** If you have chosen to install the legacy Content Center system, you must specify the storage location for recordings and the maximum allowed space for recordings and click **Next**.



Scopia Desktop - Setup Wizard

Scopia Desktop Recording Configuration

Set the storage location and maximum folder size for recorded meetings.

Specify the storage location for recorded meetings.

C:\Program Files (x86)\Radvision\SCOPIA Desktop\Movies\

Specify the maximum amount of disk space to allocate for recorded meetings.

8192 MB

Figure 166: Storage details for legacy Content Center system recordings

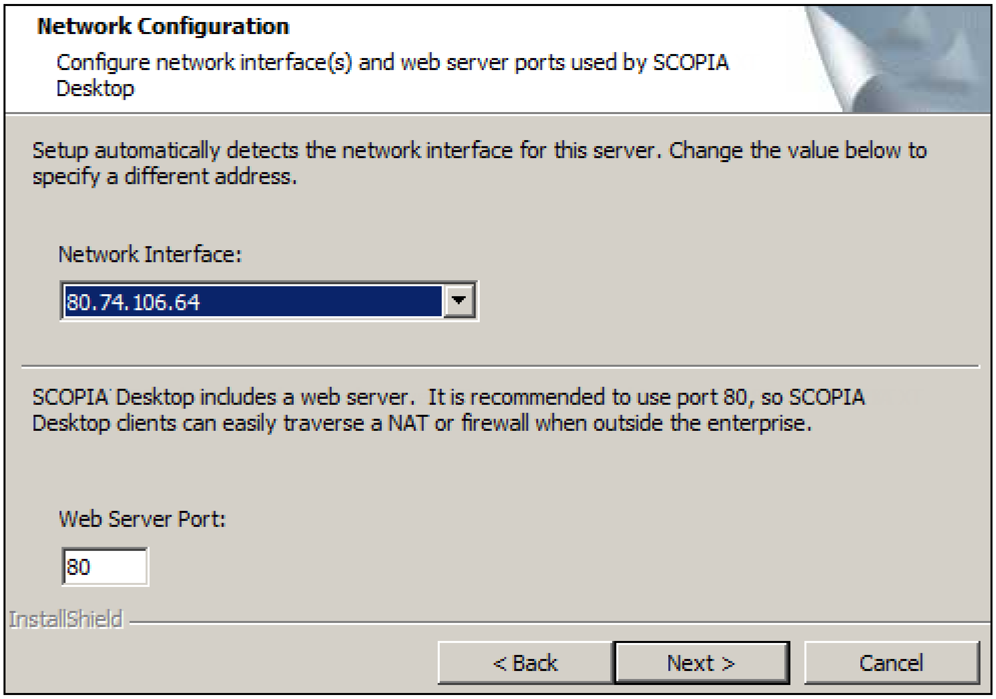
10. In the **License Key** window enter the relevant license key and select **Next**.

Important:

If you do not enter the Content Center license keys, the system installs the server in demo mode which limits recordings to 5 minutes and only allows up to 5 webcast viewers in a videoconference.

11. In the **Network Configuration** window, select the IP address used for communicating with the MCU.

    If the server has one NIC card, the **Network Interface** field has only one value to choose, the IP of the NIC. For dual-NIC servers, select the network IP address pointing to the internal firewall.



Network Configuration

Configure network interface(s) and web server ports used by SCOPIA Desktop

Setup automatically detects the network interface for this server. Change the value below to specify a different address.

Network Interface:

80.74.106.64

SCOPIA Desktop includes a web server. It is recommended to use port 80, so SCOPIA Desktop clients can easily traverse a NAT or firewall when outside the enterprise.

Web Server Port:

80

Figure 167: Selecting the NIC pointing to the internal network

12. In the **Recording Configuration** window, select the storage location for recorded meetings and specify the maximum amount (in MB) of disk space needed for storing recorded meetings. One hour of Scopia Desktop recording (384kbps) is 200MB.

    Use the following formula to calculate the space required for recordings:

```
Recording Bandwidth (in megabytes) × Time (in seconds) + 20% Overhead
```

    For example, for a call of 1 hour at 384 kbps (standard definition), calculate as follows:

```
384 kbps × (60 minutes × 60 seconds) = 1382400 kilobits
1382400 ÷ 1024 = 1350 megabits
1350 ÷ 8 = 168.75 megabytes (MB)
168.75 × 20% = 33.75MB (overhead)
Total is 168.75 + 33.75 = 202.5MB (including overhead)
```

> **Important:**
>
> You can enter a local pathname or a pathname of any storage server visible in the enterprise.

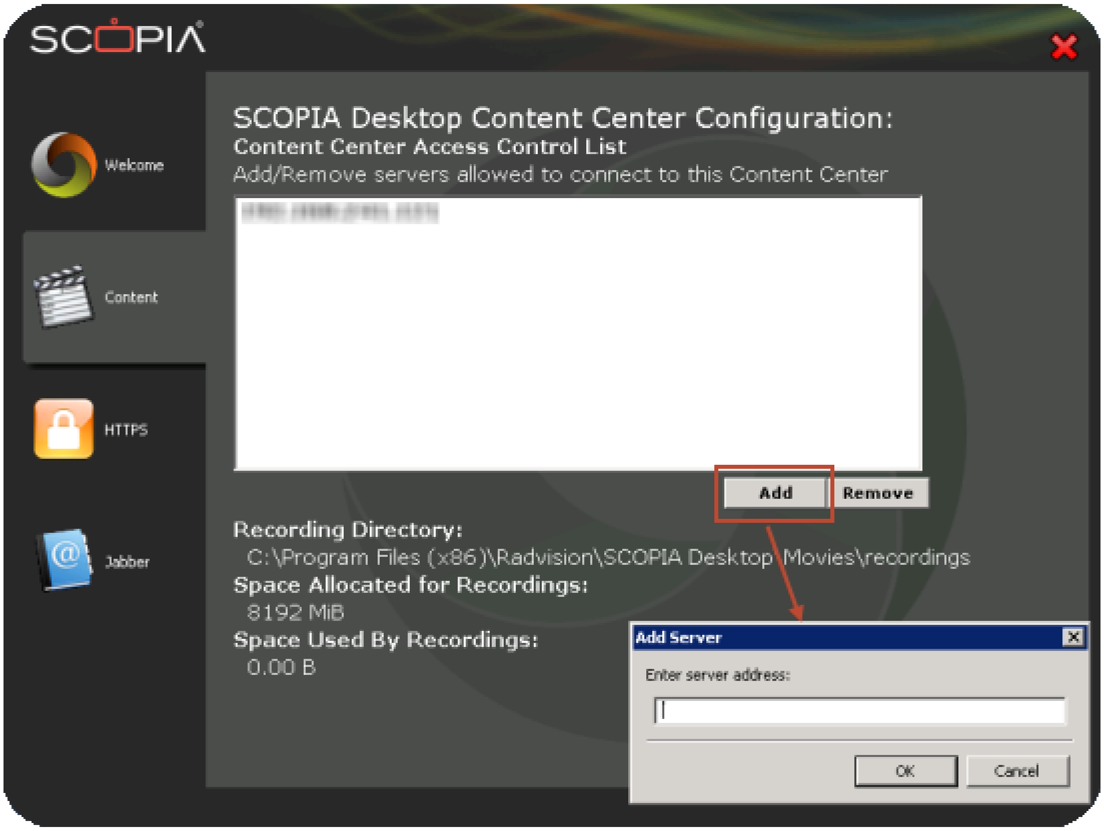
Then select **Next**.

13. Enter the IP address (or FQDN) of the Scopia Desktop Server which must communicate with this server and select **Next**.
14. Select **Install** in the **Ready to Install the Program** window.
15. Select **Finish**.
16. To change the Content Center settings, run the Setup Wizard again and navigate to the **Custom Setup** dialog.
17. For any Scopia Desktop Server accessing a dedicated Content Center Server (recording or streaming), enter each Scopia Desktop Server IP address in the access control list using the Scopia Desktop Server Configuration Tool.

    a. On the dedicated Content Server for Scopia Desktop, select **Start** > **Programs** > **Scopia Desktop** > **ConfigTool**.

    b. Select **Content** in the sidebar.

    The system lists the IP addresses of the Scopia Desktop Servers allowed to access this Dedicated Content Server, as shown below.



SCOPIA Desktop Content Center Configuration:
Content Center Access Control List
Add/Remove servers allowed to connect to this Content Center

[redacted]

Recording Directory:
C:\Program Files (x86)\Radvision\SCOPIA Desktop Movies\recordings
Space Allocated for Recordings:
8192 MiB
Space Used By Recordings:
0.00 B

Figure 168: Enabling multiple Scopia Desktop Servers to access a Dedicated Content Server

c. Select **Add** to add the IP address of each Scopia Desktop Server using this Content Server.

d. Select **OK**.

Installing the Invitation and Presence Server for Scopia Desktop on a Dedicated Server

About this task

This section details how to install a dedicated Invitation and Presence Server for Scopia Desktop on a separate PC from the other server components. The Invitation and Presence Server includes the XMPP (Jabber) server which updates a user's status in the contact list, and a STUN server which allows you to directly dial a Scopia Desktop Client which is located behind a firewall.

Scopia Desktop Server includes various components which you can install on the same server for small deployments.

For medium and large size deployments where you need power devoted to each component of the server, you can deploy a dedicated server devoted just one component of the Scopia Desktop Server, or you can choose a set of components on the same computer.

Follow these recommendations when installing the Scopia Desktop Server components:

- Do not install the Scopia Desktop Client on the same PC as any Scopia Desktop component.
- If you want to encrypt communication with HTTPS, configure the Conference Server for Scopia Desktop to port 443 after the installation is completed.

  Important:

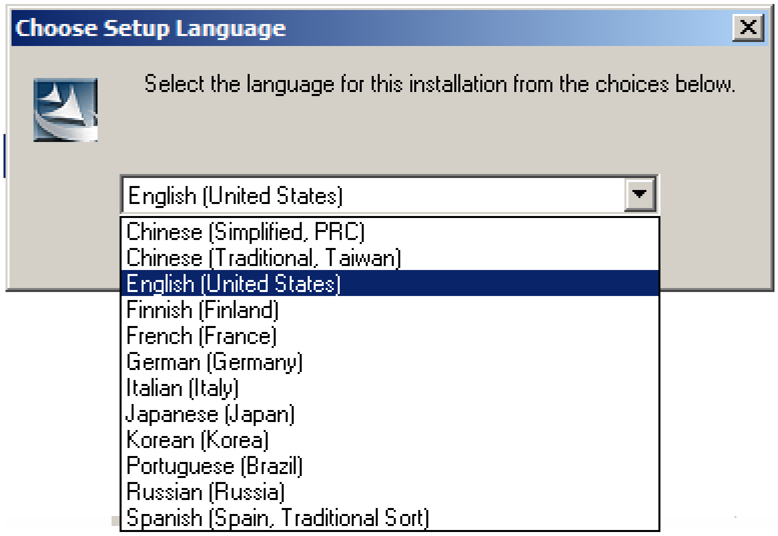
  Using encryption is subject to local regulation. In some countries it is restricted or limited for usage. For more information, consult your local reseller.

Before you begin

- Before installing, verify the computer meets the minimum hardware requirements for the number of intended users. For more information, see Minimum Requirements and Specifications of Scopia Desktop Server on page 289.
- Make sure you have enough space on the hard drive to install the component. The invitation and Presence Server require 26MB on the hard drive.
- To use point-to-point functionality, you must install Equinox Management with the Avaya Scopia Desktop Pro license.

Procedure

1. Launch the *setup.exe* file to start the Scopia Desktop Setup Wizard.
2. Select the installation language in the **Choose Setup Language** window, and select **OK**.



Choose Setup Language

Select the language for this installation from the choices below.

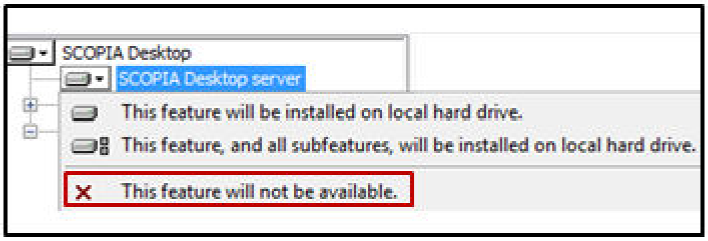
English (United States)

Chinese (Simplified, PRC)
Chinese (Traditional, Taiwan)
English (United States)
Finnish (Finland)
French (France)
German (Germany)
Italian (Italy)
Japanese (Japan)
Korean (Korea)
Portuguese (Brazil)
Russian (Russia)
Spanish (Spain, Traditional Sort)

Figure 169: Choosing language for the installation

   Scopia Desktop starts the installation wizard.

3. Click **Next**, accept the license agreement, and click **Next**.
4. Select **Custom Install**, and click **Next**.
5. In the **Custom Setup** window disable the **Scopia Desktop Server** by selecting > **This feature will not be available**. Repeat for the **Content Center** and select **Next**.



SCOPIA Desktop
SCOPIA Desktop server
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.

Figure 170: Disabling a Scopia Desktop component on a dedicated server

6. Ensure the **Invitation and Presence** component is selected for local installation.

   Important:

   When installing a component, always use the default option (**This feature will be installed on the local hard drive**).

7. Change the installation folder if required, and select **Next**.
8. Select **Install** in the **Ready to Install the Program** window.
9. Select **Finish**.

Centrally Deploying Scopia Desktop Clients in your Organization

About this task

You can push Scopia Desktop Clients simultaneously to end users using one of these standard Microsoft server tools:

- Microsoft Active Directory (AD)

  For more information, see the Knowledge Base article ADMN113188 on https://support.avaya.com

- Microsoft Systems Management Server (SMS)

  For more information, see the Knowledge Base article ADMN113919 on https://support.avaya.com

Upgrading Scopia Desktop

About this task

Scopia Desktop Server includes various components which you can install on the same server for small deployments.

For medium and large size deployments where you need power devoted to each component of the server, you can deploy a dedicated server devoted just one component of the Scopia Desktop Server, or you can choose a set of components on the same computer.

Follow these recommendations when installing the Scopia Desktop Server components:

- Do not install the Scopia Desktop Client on the same PC as any Scopia Desktop component.
- If you want to encrypt communication with HTTPS, configure the Conference Server for Scopia Desktop to port 443 after the installation is completed.

  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.

Follow this procedure to upgrade the Scopia Desktop components.

Before you begin

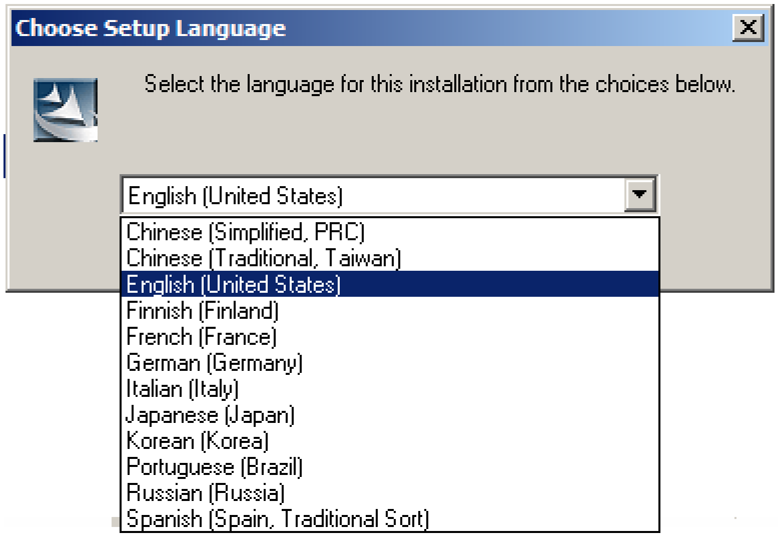
- Before installing, verify the computer meets the minimum hardware requirements for the number of intended users. For more information, see Minimum Requirements and Specifications of Scopia Desktop Server on page 289.
- Make sure you have enough space on the local hard drive to install all Scopia Desktop components.
- Ensure you have the correct license information.

  Important:

  To use point-to-point functionality, you must install Equinox Management with the Avaya Scopia Desktop Pro license.
- By default, the older recording application, the Scopia Desktop Content Center (SCC) Server uses port 7070 streaming play. If you select a different port, change the default port value as explained in *Administration Guide for Scopia Desktop* and the *Port Security for the Avaya Equinox Solution Reference Guide*, which are available on https://support.avaya.com/.
- By default, the older recording application, Scopia Desktop Content Center (SCC) Server uses port 80 for recording play and download. If other applications on this PC use port 80, and you nevertheless want to use this port, access the Services panel in Windows and disable the IIS Administration, HTTP SSL, and World Wide Web Publishing services before installing the Conference Server.

Procedure

1. Launch the *setup.exe* file to start the Scopia Desktop Setup Wizard.
2. Select the installation language in the **Choose Setup Language** window, and select **OK**.



Choose Setup Language

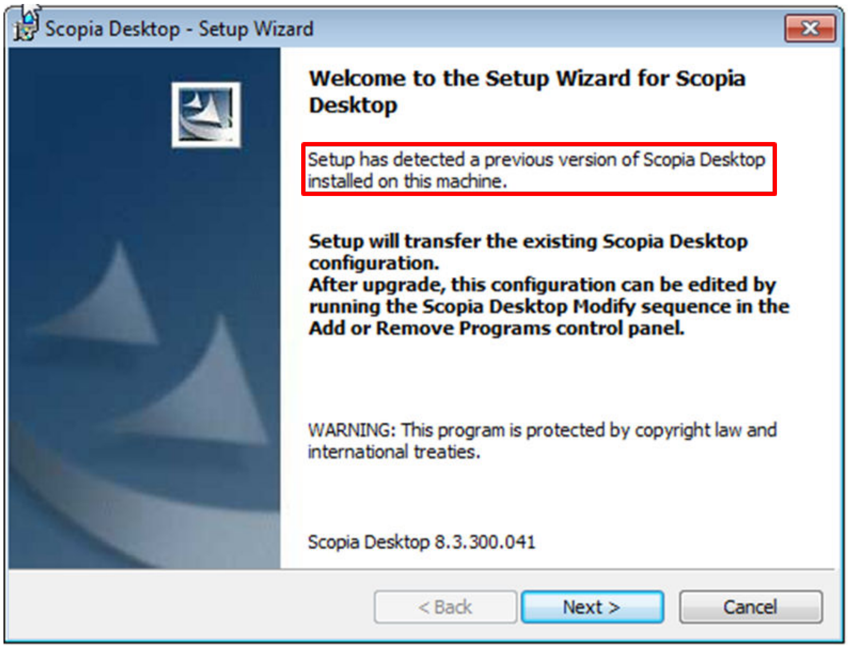
Select the language for this installation from the choices below.

English (United States)

Figure 171: Choosing language for the installation

Scopia Desktop starts the installation wizard.

3. Ensure that the installation wizard detects the existing version of the Scopia Desktop Server and click **Next**.



Scopia Desktop - Setup Wizard

Welcome to the Setup Wizard for Scopia Desktop

Setup has detected a previous version of Scopia Desktop installed on this machine.

Setup will transfer the existing Scopia Desktop configuration.
After upgrade, this configuration can be edited by running the Scopia Desktop Modify sequence in the Add or Remove Programs control panel.

WARNING: This program is protected by copyright law and international treaties.

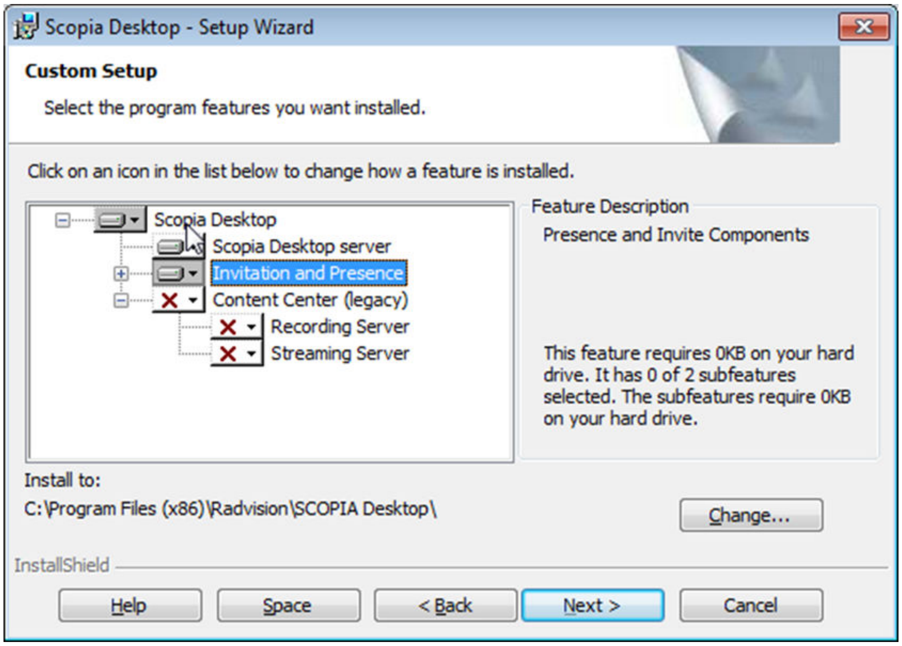
Scopia Desktop 8.3.300.041

Figure 172: Detection of previous version

4. Click **Next**, accept the license agreement, and click **Next**.

5. Choose the components that you want to install by clicking on each component icon and selecting **This feature will be installed on local hard drive** or **This feature will not be available**.

For example, to install all of the components on a single server, except the legacy Content Center system, you can click on the **Scopia Desktop Server** and **Invitation and Presence** icons and select **This feature will be installed on local hard drive**. On the **Content Center (legacy)** icon, select **This feature will not be available**.



Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- Scopia Desktop
  - Scopia Desktop server
  - Invitation and Presence
  - ☒ Content Center (legacy)
    - ☒ Recording Server
    - ☒ Streaming Server

Feature Description

Presence and Invite Components

This feature requires 0KB on your hard drive. It has 0 of 2 subfeatures selected. The subfeatures require 0KB on your hard drive.

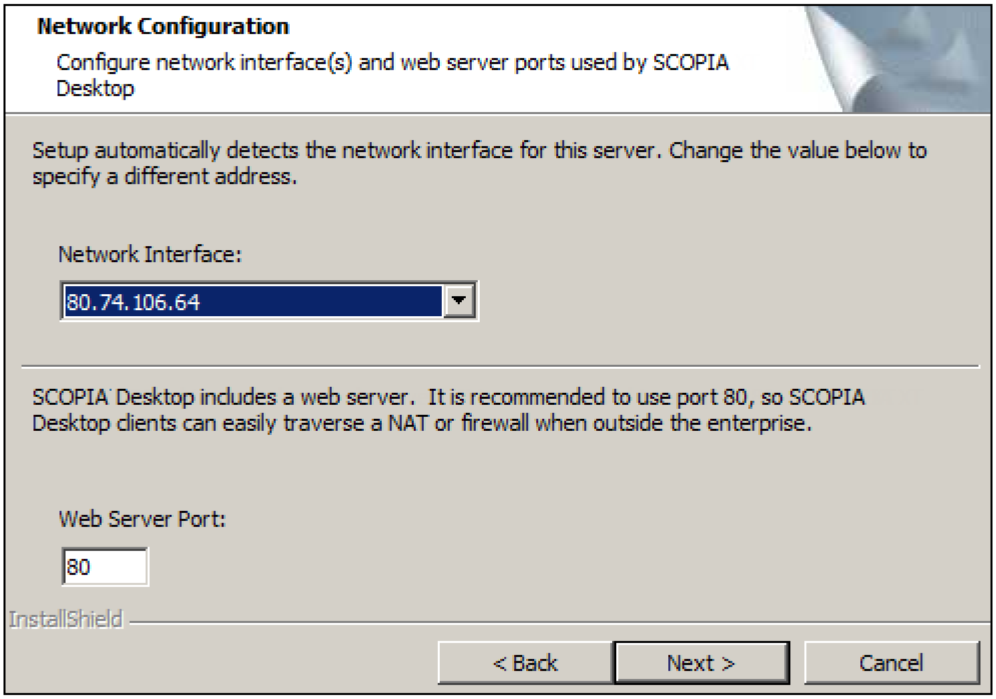
Install to:

C:\Program Files (x86)\Radvision\SCOPIA Desktop\

Figure 173: All components with the exception of Content Center (legacy)

6. In the **Network Configuration** window, select the IP address used for communicating with the MCU.

   If the server has one NIC card, the **Network Interface** field has only one value to choose, the IP of the NIC. For dual-NIC servers, select the network IP address pointing to the internal firewall.



Network Configuration

Configure network interface(s) and web server ports used by SCOPIA Desktop

Setup automatically detects the network interface for this server. Change the value below to specify a different address.

Network Interface:

80.74.106.64

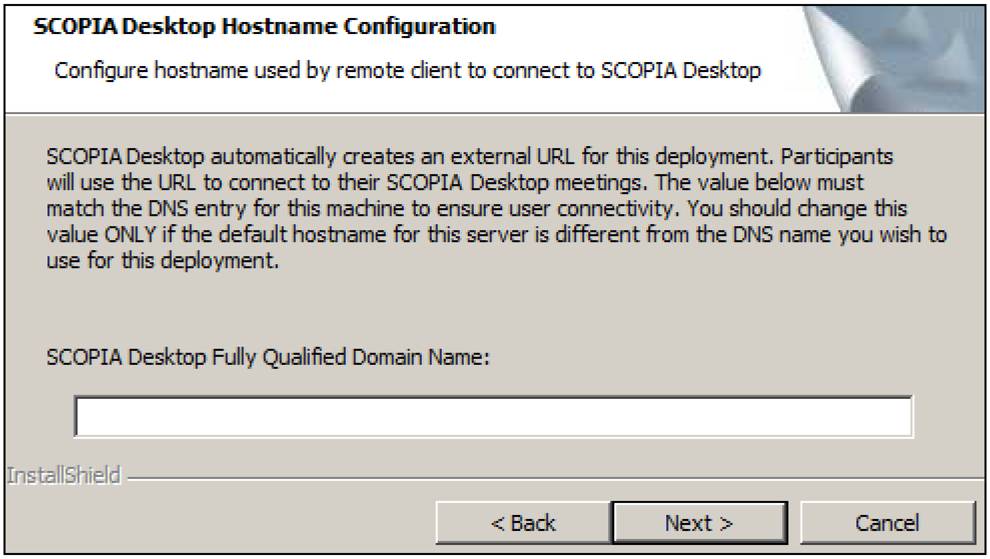
SCOPIA Desktop includes a web server. It is recommended to use port 80, so SCOPIA Desktop clients can easily traverse a NAT or firewall when outside the enterprise.

Web Server Port:

80

Figure 174: Selecting the NIC pointing to the internal network

7. Change the default web server port if required, and then select **Next**.
8. In the **Hostname Configuration** window specify the public name of the d, to be used later as part of the URL sent to Scopia Desktop Clients to connect to videoconferences.



SCOPIA Desktop Hostname Configuration

Configure hostname used by remote client to connect to SCOPIA Desktop

SCOPIA Desktop automatically creates an external URL for this deployment. Participants will use the URL to connect to their SCOPIA Desktop meetings. The value below must match the DNS entry for this machine to ensure user connectivity. You should change this value ONLY if the default hostname for this server is different from the DNS name you wish to use for this deployment.

SCOPIA Desktop Fully Qualified Domain Name:

Figure 175: Defining the public address of the Scopia Desktop Server

Important:

An external Scopia Desktop Client must be able to resolve the server's hostname to the correct IP address from its location outside the enterprise. For example, do not use an internal DNS name if you have clients connecting from the public Internet.

9. Select **Install** in the **Ready to Install the Program** window.
10. Select **Finish**.

Chapter 17: 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 next generation HD streaming and recording platform. The Avaya Equinox Streaming and Recording Server replaces the Avaya Scopia Content Center Recording Server (SCC) server.

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[2] 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 Scopia® 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 Equinox Streaming and Recording consists of the following components:

- Equinox Streaming and Recording Conference Point™ (CP)

[2] 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 Delivery Node™ (DN)
- Equinox Streaming and Recording Virtual Delivery Node™ (VDN)
- Equinox Streaming and Recording Manager™
- Avaya 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 Windows Media or .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 480pm, or up to 60 360p recordings, or 75 audio-only 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 Windows Media™ format or H.264/AAC MP4/MPEGTS/HLS formats.

- Operating Systems: The transcoder runs on the Windows Server 2012 R2 64-bit operating system with Hyper-V (an add-on to Windows Server 2012 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.

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
- Video, audio, and web collaboration conferences

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 a Avaya Equinox Recording Gateway. You can deploy the Avaya Equinox Recording Gateway using the Avaya Equinox Management interface. The Avaya 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 two additional meeting types - Audio Service and Audio Service with 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, Avaya 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. Avaya Equinox Management also determines the most appropriate capture rate, resolution, frame rate, and encode rate for the Equinox Streaming and Recording Conference Point.

The Avaya Equinox Recording Gateway does not require a separate license. When you buy a media node, you receive an Avaya Equinox Recording Gateway as well. For more information on adding the gateway to Avaya Equinox Management and for information on configuring the meeting types, see *Administering Avaya Equinox Management*, which is available on support.avaya.com.

Related links

Example of a direct DMZ deployment on page 345

Example of a reverse proxy deployment on page 346

Example of a distributed deployment on page 347

Example of a cloud deployment on page 350

System requirements on page 350

Example of a direct DMZ deployment

Figure 176: Example of a Direct DMZ Deployment on page 346 displays an example of a 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.

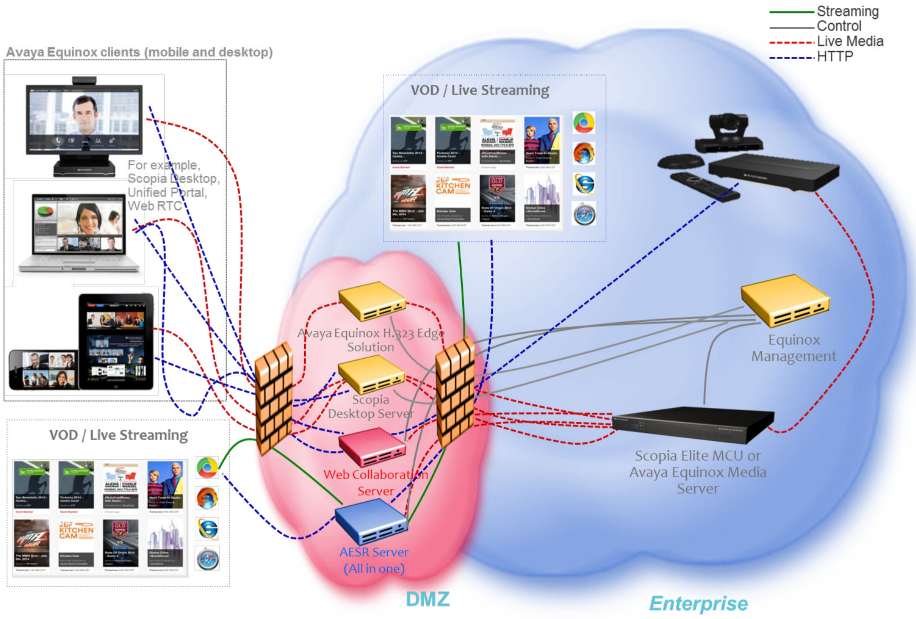

Streaming
Control
Live Media
HTTP
Avaya Equinox clients (mobile and desktop)
For example, Scopia Desktop, Unified Portal, Web RTC
VOD / Live Streaming
VOD / Live Streaming
Avaya Equinox H.323 Edge Solution
Scopia Desktop Server
Web Collaboration Server
AESR Server (All in one)
Equinox Management
Scopia Elite MCU or Avaya Equinox Media Server
DMZ
Enterprise

Figure 176: Example of a Direct DMZ Deployment

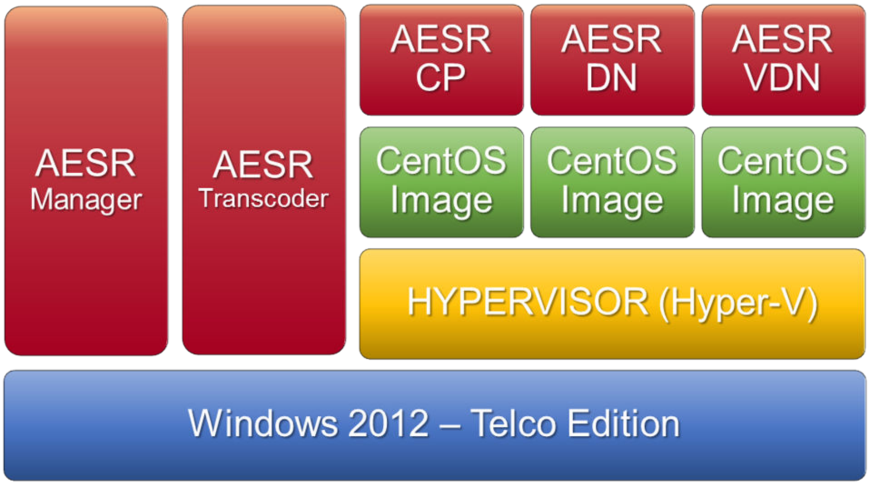


Figure 177: Components in an All-In-One Deployment with Virtual Software

Related links

Avaya Equinox Streaming and Recording Server on page 341

Example of a reverse proxy deployment

Figure 178: Example of a Reverse Proxy Deployment on page 347 displays an example of a Equinox Streaming and Recording deployment that includes a reverse proxy server. The deployment is a centralized or all-in-one solution.

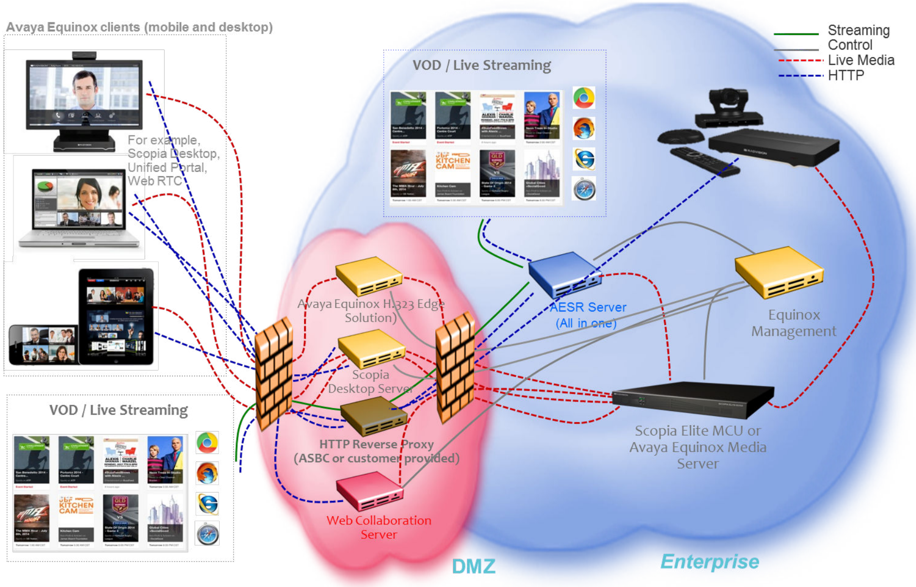

Avaya Equinox clients (mobile and desktop)
For example, Scopia Desktop, Unified Portal, Web RTC
VOD / Live Streaming
VOD / Live Streaming
Streaming
Control
Live Media
HTTP
Avaya Equinox H.323 Edge Solution)
Scopia Desktop Server
HTTP Reverse Proxy (ASBC or customer provided)
Web Collaboration Server
AESR Server (All in one)
Equinox Management
Scopia Elite MCU or Avaya Equinox Media Server
DMZ
Enterprise

Figure 178: Example of a Reverse Proxy Deployment

Related links

Avaya Equinox Streaming and Recording Server on page 341

Example of a distributed deployment

Figure 179: Example of a Distributed Deployment on page 348 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.

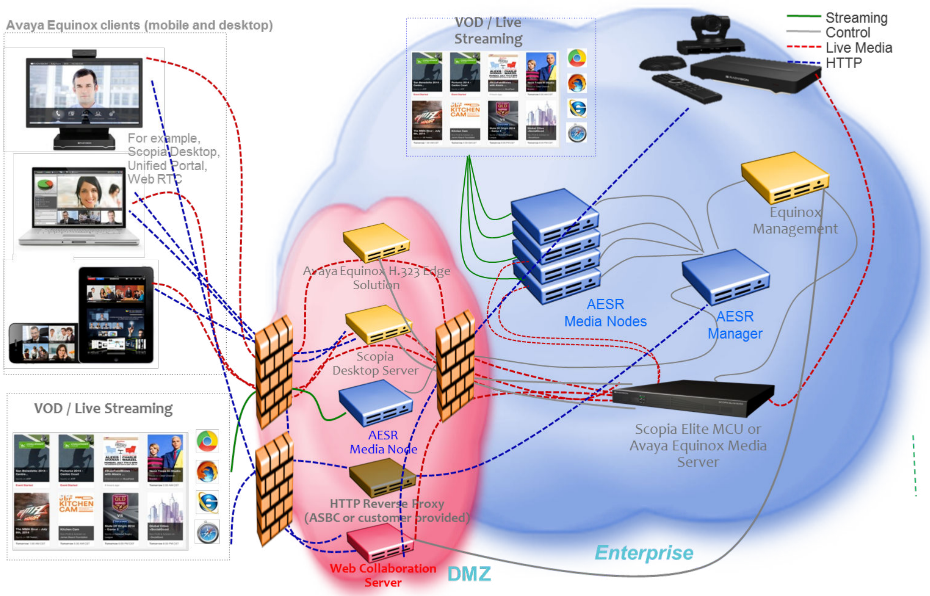

Avaya Equinox clients (mobile and desktop)
For example, Scopia Desktop, Unified Portal, Web RTC
VOD / Live Streaming
VOD / Live Streaming
Streaming
Control
Live Media
HTTP
Avaya Equinox H.323 Edge Solution
Scopia Desktop Server
AESR Media Node
HTTP Reverse Proxy (ASBC or customer provided)
Web Collaboration Server
DMZ
AESR Media Nodes
AESR Manager
Equinox Management
Scopia Elite MCU or Avaya Equinox Media Server
Enterprise

Figure 179: Example of a Distributed Deployment

Related links

[Avaya Equinox Streaming and Recording Server](#) on page 341

[Deployment choices for centralized and distributed solutions](#) on page 348

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**.

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 347
All-in-one on page 349
Content Management components only on page 349
Media Node only on page 349

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.

Related links

Deployment choices for centralized and distributed solutions on page 348

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 348

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 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 348

Example of a cloud deployment

Example of a cloud deployment on page 350 displays an example of a 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.

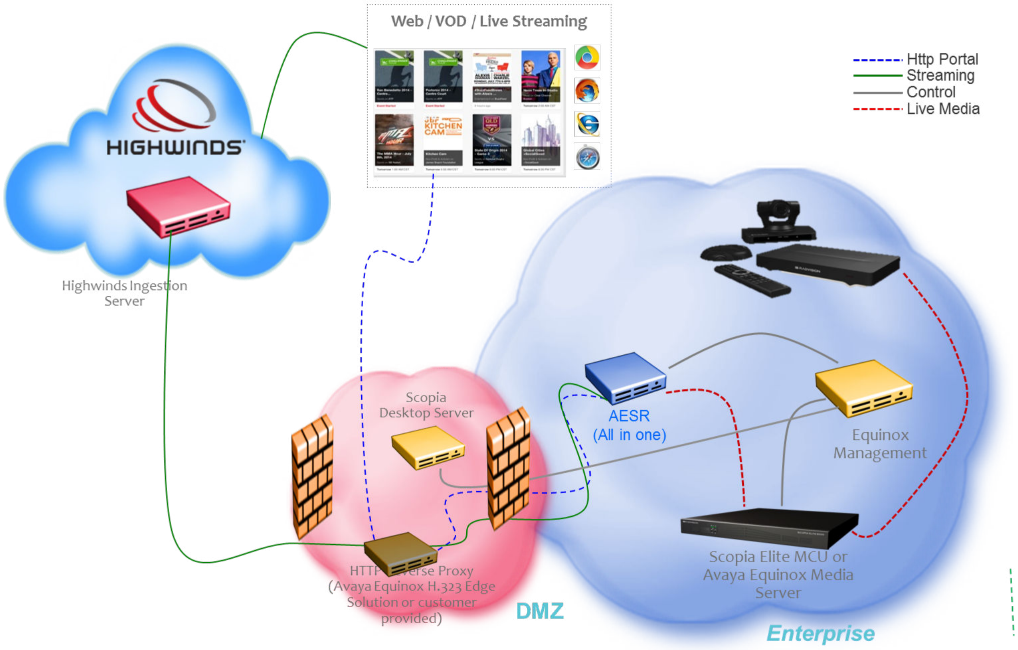

Web / VOD / Live Streaming
Http Portal
Streaming
Control
Live Media
HIGHWINDS
Highwinds Ingestion Server
Scopia Desktop Server
AESR
(All in one)
Equinox Management
Scopia Elite MCU or Avaya Equinox Media Server
HTTP Reverse Proxy (Avaya Equinox H.323 Edge Solution or customer provided)
DMZ
Enterprise

Figure 180: Example of a Cloud Deployment

Related links

Avaya Equinox Streaming and Recording Server on page 341

System requirements

Before you log on to Equinox Streaming and Recording Manager administration pages, your client system must meet the system requirements listed in Table 49: Requirements on page 350.

Table 49: Requirements

Component	Requirement
Operating system	• Mac OS X 10.7 (Lion) or later

Table continues…

Component	Requirement
	• Windows Vista™ • Windows 20XX • Windows 7™ (32 and 64 Bit) • Windows 8™ • Windows 10™
Web browser	• Microsoft Internet Explorer 8.0™ or later • Microsoft Edge™ • Mozilla Firefox 35™ or later (Mac or Windows) • Chrome 30™ or later (Mac or Windows) • Safari 6™ or later (Mac) JavaScript must be enabled.

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 50: Requirements on page 351.

Table 50: Requirements

Component	Requirement
Web browser	• Microsoft Internet Explorer 11.0™ or later • 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™ 7 (32 and 64 Bit) • Windows™ 8 • Windows™ 8.1 • Windows™ 10 • iOS N-1 or later • Android 4.0.3. or later
Media Player	Microsoft Windows Media Player™ Release 9.0, 10.0, or 11.0 to view programs.
Silverlight	Microsoft Silverlight™ player to view programs.

Table continues…

Component	Requirement
HTMLV5 Browsers	A select number of browsers support video playback directly for MP4 VoD files including: • Internet Explorer 9, 10, 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.

Related links

Avaya Equinox Streaming and Recording Server on page 341

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 Scopia® Streaming and Recording server on page 341		
2	• Connect the LAN cables, keyboard, mouse, and monitor for your new server. • Alternatively, you can purchase a Microsoft™	• Physically connecting the new server on page 354 • For more information about obtaining and installing the Equinox Streaming and		

Table continues…

No.	Task	Description	Notes	✔
	Windows Image (WIM) and install Equinox Streaming and Recording on your own server.	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 358	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 359		
5	Set the IP addresses and apply the licenses.	Licensing the new server on page 362		
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 369	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 371		
8	On the delivery node (DN), configure the parent delivery node.	Configuring delivery nodes on page 374		
9	On the conference point (CP), configure the gatekeeper IP and source DN.	Configuring conference points on page 380		
10	On Equinox Streaming and Recording, configure the network address for device communication.	Specifying polling intervals and the network address on page 381		

Table continues…

No.	Task	Description	Notes	✔
11	Register Equinox Streaming and Recording with Equinox Management.	Adding and Modifying Recording and Streaming servers in Scopia® Management on page 383		
12	Configure the Avaya Equinox Recording Gateway.	Configuring the Avaya Equinox Recording Gateway on page 385		

Physically connecting the new server

Before you begin

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 Avaya Equinox Streaming and Recording Server (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.

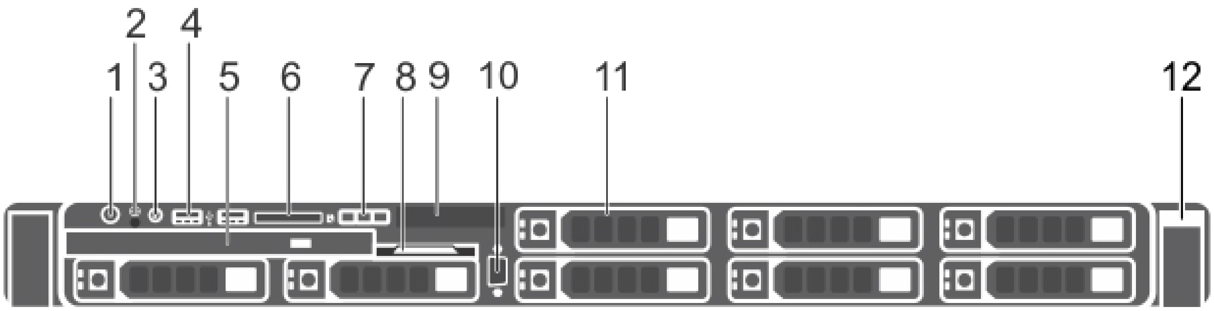
Next steps

Return to the Installation checklist on page 352 to see your next task.

Related links

Front view of Dell PowerEdge R630 Server on page 355
Back view of Dell PowerEdge R630 Server on page 356

Front view of Dell™ PowerEdge™ R630 Server



No.	Item	Icon	Description
1	Power-On Indicator, Power Button	⏻	The power-on indicator lights when the system power is on. The power button controls the power supply output to the system. **Note:** On ACPI-compliant operating systems, turning off the system using the power button causes the system to perform a graceful shutdown before power to the system is turned off.
2	NMI Button	⊖	Used to troubleshoot software and device driver errors when running certain operating systems. This button can be pressed using the end of a paper clip. Use this button only if directed to do so by qualified support personnel or by the operating system documentation.
3	System Identification Button	ⓘ	The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pressed, the LCD panel on the front and the system status indicator on the back flashes blue until one of the buttons are pressed again. Press to toggle the system ID on and off. If the system stops responding during POST, press and hold the system ID button for more than five seconds to enter BIOS progress mode. To reset the iDRAC (if not disabled in F2 iDRAC setup) press and hold the button for more than 15 seconds.
4	USB Connectors (2)	⭠	Allows you to insert USB devices to the system. The ports are USB 2.0-compliant.
5	Optical Drive		One DVD+/-RW drive. **Note:** DVD devices are data only.

Table continues…

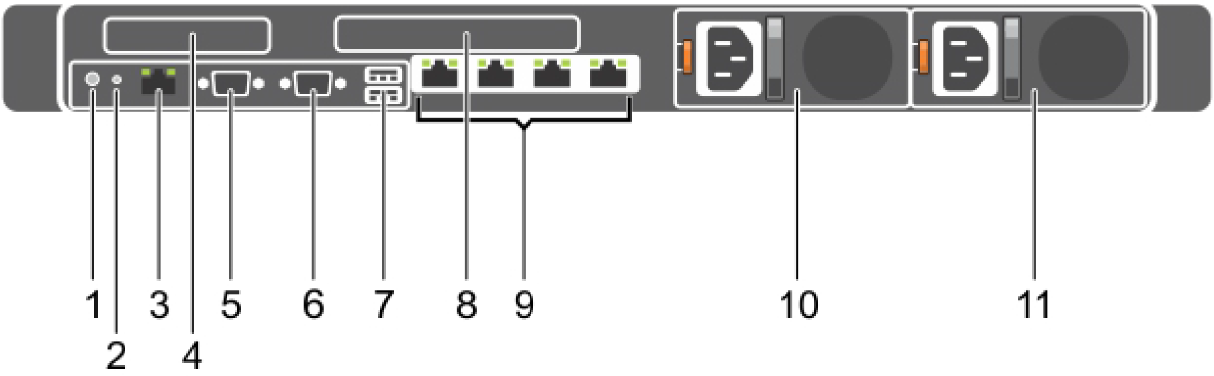
No.	Item	Icon	Description
6	vFlash Media Card Slot		Not used in Avaya configurations.
7	LCD Menu Buttons		Allows you to navigate the control panel LCD menu.
8	Information Tag		A slide-out label panel, which allows you to record system information, such as Service Tag, NIC, MAC address.
9	LCD Panel		Displays system ID, status information, and system error messages. The LCD lights blue during normal system operation. When the system needs attention, the LCD lights amber and the LCD panel displays an error code followed by descriptive text. **Note:** If the system is connected to AC power and an error is detected, the LCD lights amber regardless of whether the system is turned on or off.
10	Video Connector		Allows you to connect a VGA display to the system.
11	Hard Drives		Support for up to eight 2.5 inch hot-swappable hard drives.* * The first 2 HDDs are placed in the slots under the DVD Drive and read left to right, the remaining HDDs read top to bottom, left to right.
12	Quick Sync		Not used in Avaya configurations.

More information can be found in the *Front-panel features and indicators* section of the Dell Owner's Manual.

Related links

Physically connecting the new server on page 354

Back view of Dell™ PowerEdge™ R630 Server



No.	Item	Icon	Description
1	System Identification Button	ⓘ	The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pressed, the LCD panel on the front and the system status indicator on the back blink until one of the buttons are pressed again. Press to toggle the system ID on and off. If the system stops responding during POST, press and hold the system ID button for more than five seconds to enter BIOS progress mode. If you are directed by services to reset the iDRAC port, press and hold the button for more than 15 seconds.
2	System Identification Connector		Allows you to connect the optional system status indicator assembly through the optional cable management arm.
3	iDRAC8 Enterprise Port	🔧	Dedicated management port. **Note:** The port is available for iDRAC8 Express features only. Avaya systems do not come with an Enterprise license. (Not normally used in Avaya systems.)
4	PCIe Expansion Card Slot 1 (riser 2)		Allows you to connect a low profile PCIe expansion card. **Note:** If your server is equipped with 6 or 8 NIC ports this slot can contain two port 10/100/1000 Mbps NIC connectors or two 100 Mbps/ 1Gbps/10 Gbps SFP + connectors, 2 CPUs must be installed for this slot to be available for use.
5	Serial Connector	IOIOI	Allows you to connect a serial device to the system.
6	Video Connector	IOI	Allows you to connect a VGA display to the system.
7	USB Connectors (2)	⭠	Allows you to connect USB devices to the system. The ports are USB 3.0-compliant.
8	PCIe Expansion Card Slot 2 (riser 3)		Allows you to connect a full-height half-length PCIe expansion card. **Note:** If your server is equipped with 6 or 8 NIC ports this slot can contain two port 10/100/1000 Mbps NIC connectors or two 100 Mbps/ 1Gbps/10 Gbps SFP + connectors.
9	Ethernet Connectors (4)	🖧	Four integrated 10/100/1000 Mbps NIC connectors (Avaya Standard). **Note:** NIC port numbers are read from left to right, starting with Port 1, then continuing to Ports 2, 3, and 4.
10	Power Supply (PSU1)		Wattage and voltage type depends on configuration.

Table continues…

No.	Item	Icon	Description
11	Power Supply (PSU2)		Wattage and voltage type depends on configuration.

More information can be found in the *Back-panel features and indicators* section of the Dell Owner's Manual.

Related links

Physically connecting the new server on page 354

Starting the new server

If you have the Avaya-provided server (The Avaya Common Server), the Microsoft Windows™ 2012 R2 license is already configured on your server.

If you are providing your own hardware, Avaya provides a temporary license for Microsoft Windows™ 2012 R2, which you should replace with a permanent license after the installation. The Windows Imaging Format (WIM) prompts it after the boot.

Procedure

1. Start up the server.
2. Press Ctrl+Alt+Delete to log in.
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 352 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

This 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

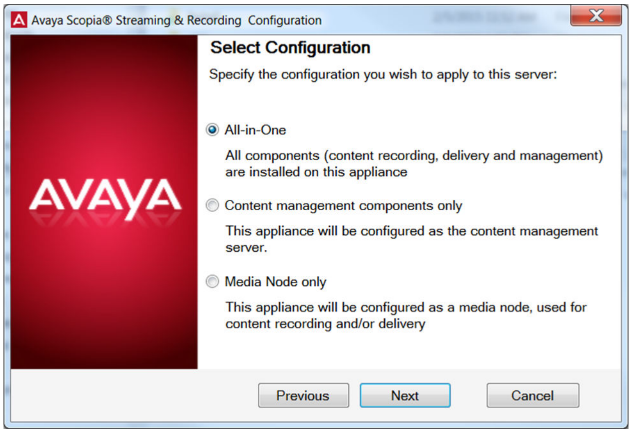
1. On the Choose Setup Language dialog, select your preferred language.
2. On the next screen, click **Next**.

   The first time you run the configuration utility, a Welcome screen is displayed.

   If you have not configured a delivery node (DN) and you run the configuration utility again, a Warning screen is displayed 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 348.



Avaya Scopia® Streaming & Recording Configuration

Select Configuration

Specify the configuration you wish to apply to this server:

● All-in-One

All components (content recording, delivery and management) are installed on this appliance

○ Content management components only

This appliance will be configured as the content management server.

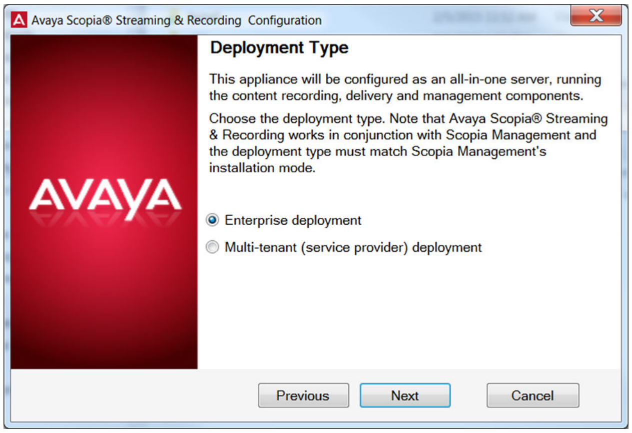
○ Media Node only

This appliance will be configured as a media node, used for content recording and/or delivery

Figure 181: 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.



Deployment Type

This appliance will be configured as an all-in-one server, running the content recording, delivery and management components.

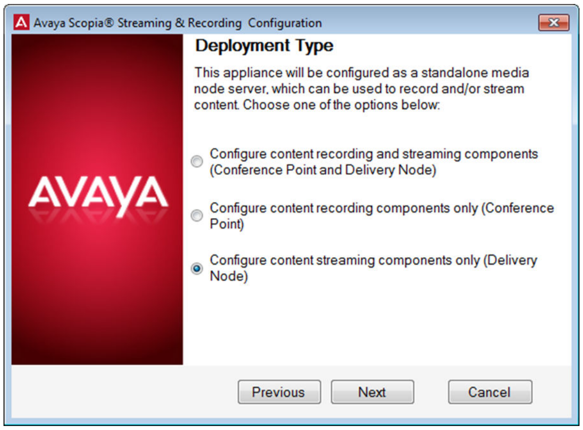
Choose the deployment type. Note that Avaya Scopia® Streaming & Recording works in conjunction with Scopia Management and the deployment type must match Scopia Management's installation mode.

● Enterprise deployment

○ Multi-tenant (service provider) deployment

Figure 182: 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 182: Deployment Type on page 361.
- 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**.



Deployment Type

This appliance will be configured as a standalone media node server, which can be used to record and/or stream content. Choose one of the options below:

○ Configure content recording and streaming components (Conference Point and Delivery Node)

○ Configure content recording components only (Conference Point)

● Configure content streaming components only (Delivery Node)

Figure 183: 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 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 352 to see your next task.

Licensing checklist

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 363 Setting the IP address of the delivery component (Delivery Node) on page 366		
2	Restart services.	Restarting services on page 366		
3	Apply the license to each of the components.	Applying the license to the management component on page 367 Applying the license to the recording component (Conference Point) on page 367 Applying the license to the delivery component (Delivery Node) on page 368	You must apply the license to all components.	

Related links

Setting the IP address of the recording component (Conference Point) on page 363

Setting the IP address of the delivery component (Delivery Node) on page 366

Restarting services on page 366

Applying the license to the management component on page 367

Applying the license to the recording component (Conference Point) on page 367

Applying the license to the delivery component (Delivery Node or Virtual Delivery Node) on page 368

Setting the IP address of the recording component (Conference Point)

The recording component is known as the conference point or CP.

About this task

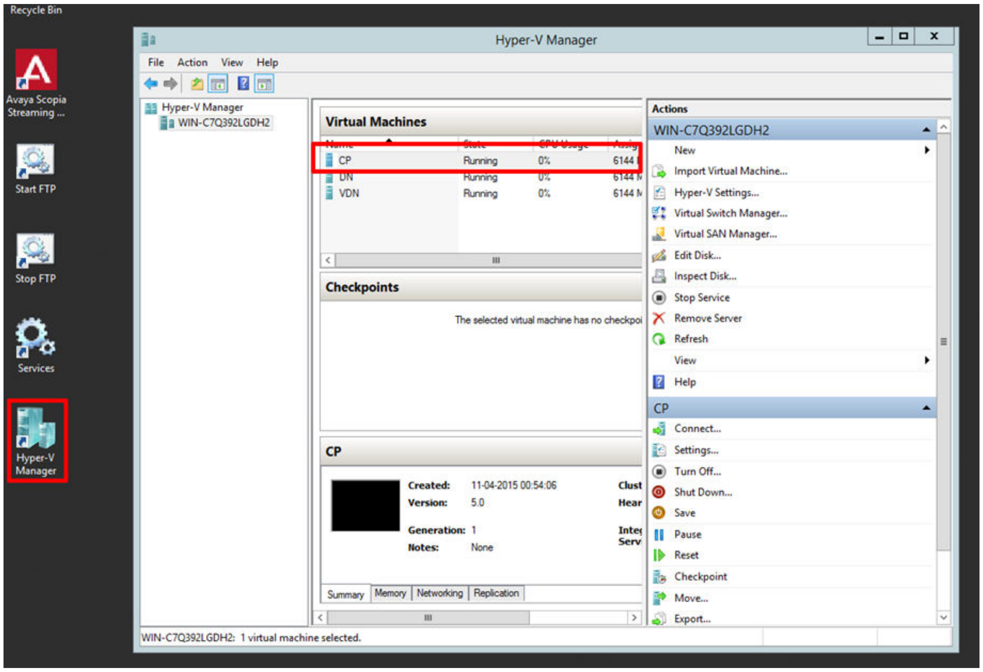
You should set an IPv4 address.

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.



Name	State	CPU Usage	Assig
CP	Running	0%	6144
DN	Running	0%	6144
VDN	Running	0%	6144

The selected virtual machine has no checkpoi

Created: 11-04-2015 00:54:06
Version: 5.0
Generation: 1
Notes: None

WIN-C7Q392LGDH2: 1 virtual machine selected.

Figure 184: Hyper-V Manager

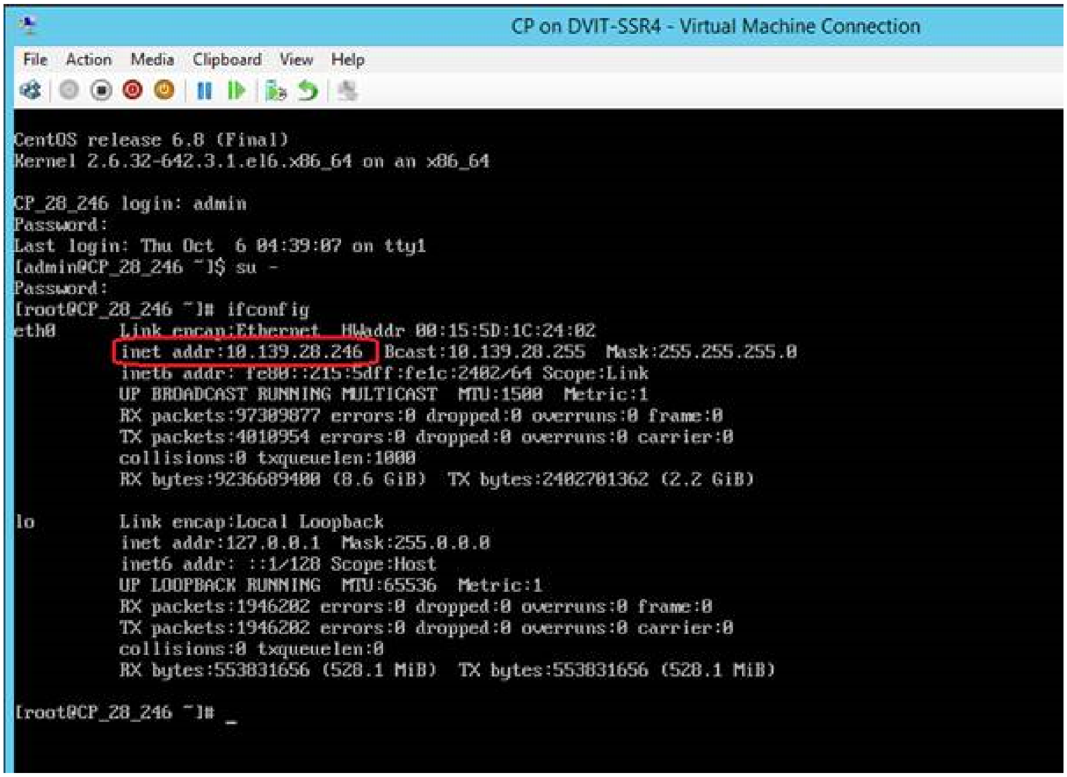
3. Log in to the Conference Point (CP) on the console as `admin`.

   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`.



CP on DVIT-SSR4 - Virtual Machine Connection
File Action Media Clipboard View Help

```
CentOS release 6.8 (Final)
Kernel 2.6.32-642.3.1.el6.x86_64 on an x86_64

CP_28_246 login: admin
Password:
Last login: Thu Oct  6 04:39:07 on tty1
[admin@CP_28_246 ~]$ su -
Password:
[root@CP_28_246 ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5D:1C:24:02
          inet addr:10.139.28.246  Bcast:10.139.28.255  Mask:255.255.255.0
          inet6 addr: fe80::215:5dff:fe1c:2402/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:97309877 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4010954 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9236689400 (8.6 GiB)  TX bytes:2402701362 (2.2 GiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1946202 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1946202 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:553831656 (528.1 MiB)  TX bytes:553831656 (528.1 MiB)

[root@CP_28_246 ~]# _
```

Figure 185: Retrieving the IP Address

5. Type `network` to open the configuration screens.
6. On the Terminal window, highlight **Device configuration** and press `Enter`.

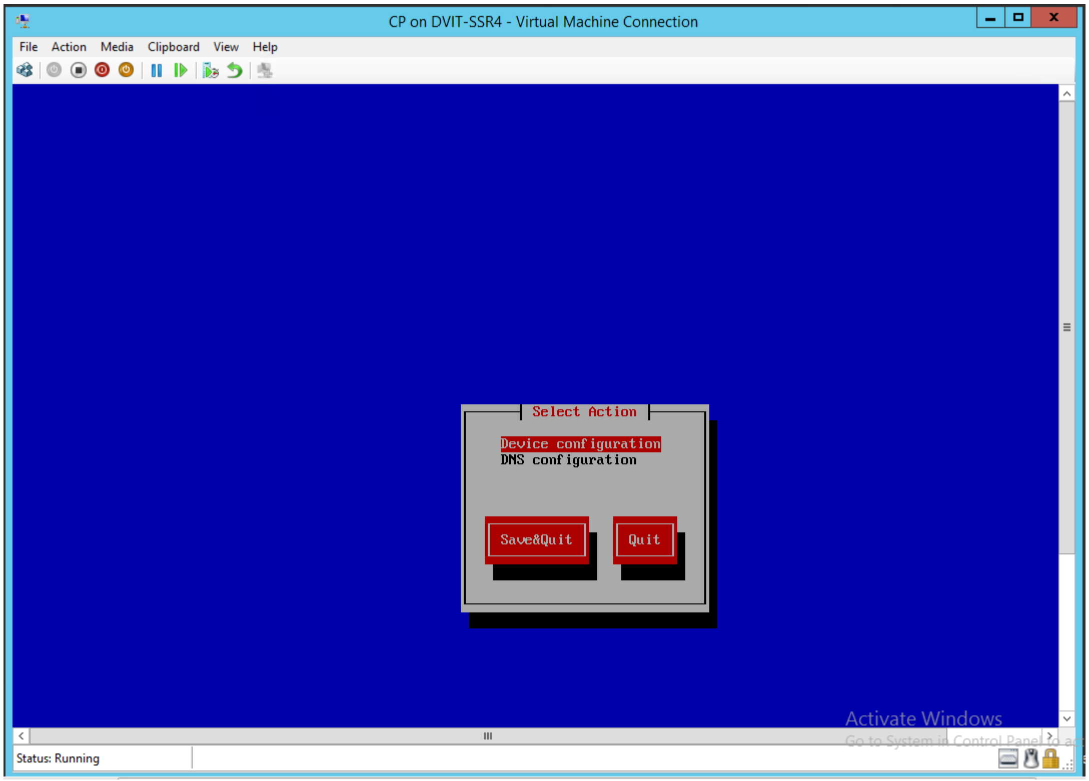
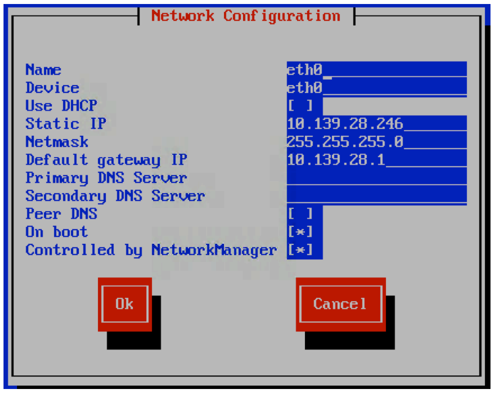

CP on DVIT-SSR4 - Virtual Machine Connection
File Action Media Clipboard View Help
Select Action
Device configuration
DNS configuration
Save&Quit
Quit
Status: Running
Activate Windows
Go to System in Control Panel to a

Figure 186: Device Configuration

7. On the Select A Device window, highlight **eth0** and press `Enter`.
8. Use the **Tab** key to highlight **Use DHCP** and press the **Spacebar** key to disable DHCP.
9. Use the **Tab** key to navigate to the other fields and enter the following details:
    - Static IP
    - Netmask
    - Default gateway IP
    - Primary DNS Server
    - Secondary DNS Server



```
Name                          eth0
Device                        eth0
Use DHCP                      [ ]
Static IP                     10.139.28.246
Netmask                       255.255.255.0
Default gateway IP            10.139.28.1
Primary DNS Server
Secondary DNS Server
Peer DNS                      [ ]
On boot                       [*]
Controlled by NetworkManager  [*]
```

Figure 187: Network Configuration

10. Use the **Tab** key to highlight **Ok** and press `Enter`.
11. On the Select A Device window, use the **Tab** key to highlight **Save** and press `Enter`.
12. On the Select Action window, use the **Tab** key to highlight **Save** and press `Enter`.
13. In the terminal window, type `service network restart` to restart network services.

Next steps

Return to the Licensing checklist on page 362 to see your next task.

Related links

Licensing checklist on page 362

Setting the IP address 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 of the recording component (Conference Point) on page 363.

Next steps

Return to the Licensing checklist on page 362 to see your next task.

Related links

Licensing checklist on page 362

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 362 to see your next task.

Related links

Licensing checklist on page 362

Applying the license to the management component

Procedure

1. Type `https://<Scopia 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 362 to see your next task.

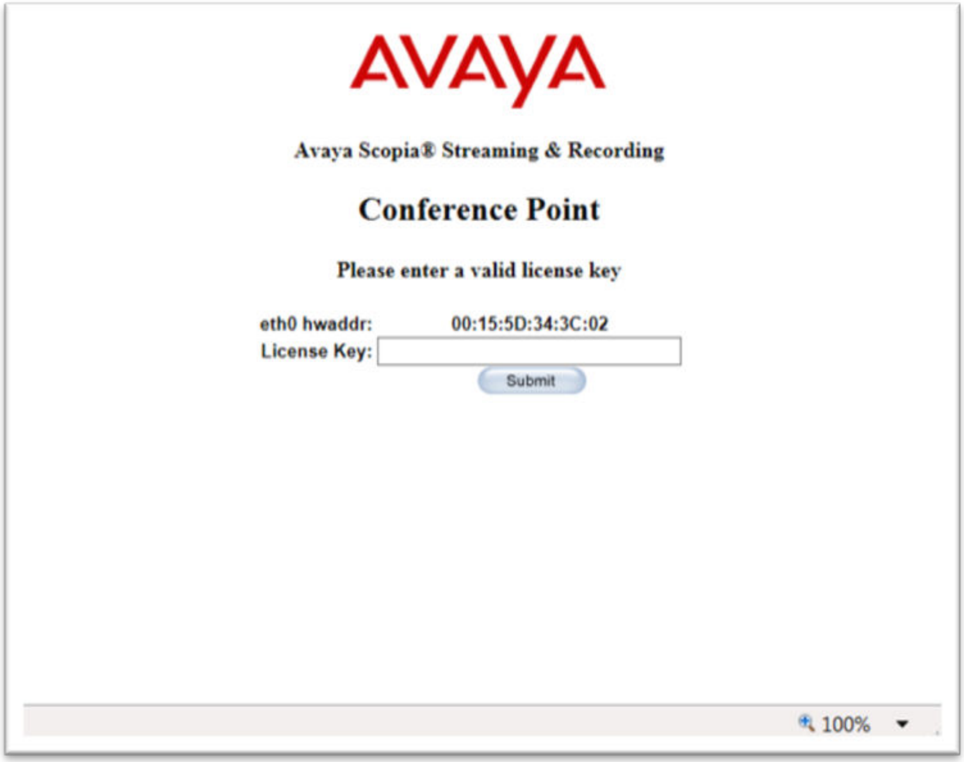
Related links

Licensing checklist on page 362

Applying the license to the recording component (Conference Point)

Procedure

1. Open a browser and type the Conference Point (CP) IP address or fully qualified domain name (FQDN).
2. On the Conference Point license screen, enter the license key in the **License Key** field and click **Submit**.



Avaya Scopia® Streaming & Recording

Conference Point

Please enter a valid license key

eth0 hwaddr: 00:15:5D:34:3C:02

License Key:

Figure 188: Conference Point

Next steps

Return to the Licensing checklist on page 362 to see your next task.

Related links

Licensing checklist on page 362

Applying the license to the delivery component (Delivery Node or Virtual Delivery Node)

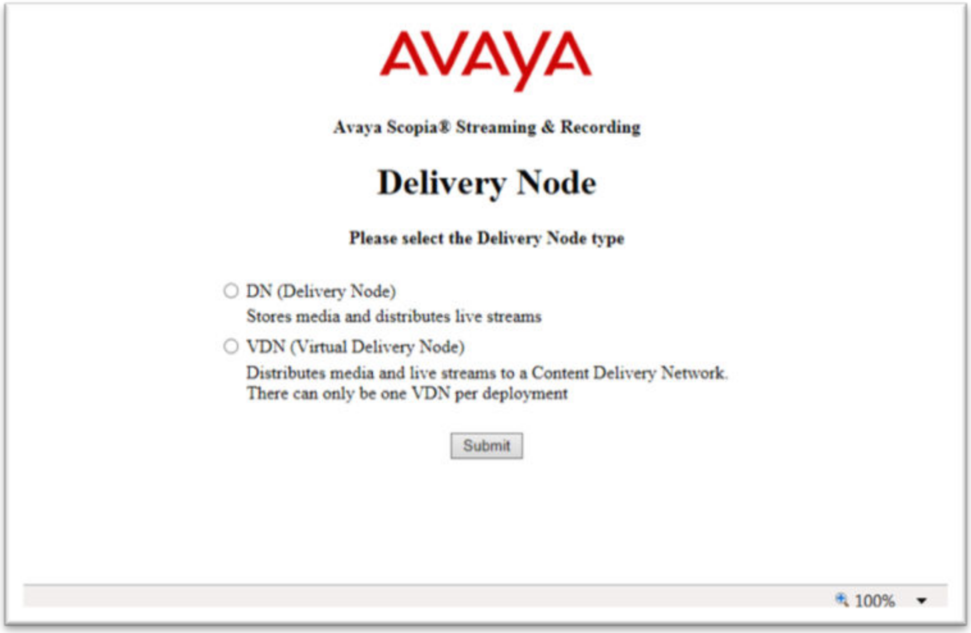
There can only be a single virtual delivery node (VDN) in a deployment.

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)



AVAYA

Avaya Scopia® Streaming & Recording

Delivery Node

Please select the Delivery Node type

○ DN (Delivery Node)
Stores media and distributes live streams

○ VDN (Virtual Delivery Node)
Distributes media and live streams to a Content Delivery Network.
There can only be one VDN per deployment

Figure 189: 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 352 to see your next task.

Related links

Licensing checklist on page 362

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 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. Enter the external address in the **External Address (optional)** field in the **Global Network Configuration** section.
   e. Click **Submit**.

2. 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. Enter 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**.

3. 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. Enter 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

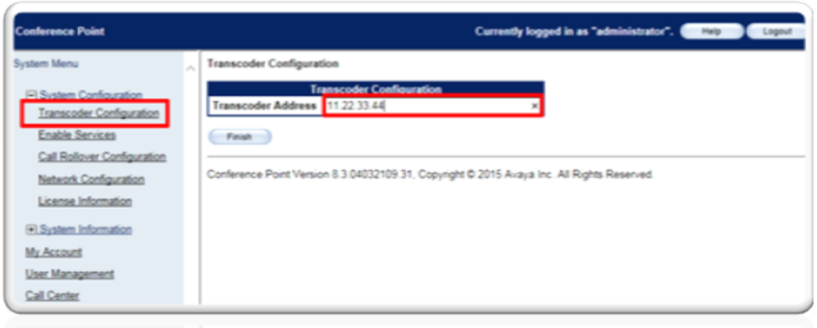
1. Type `https://<Equinox Streaming and Recording manager FQDN/IP address>:8445` in a web browser.
2. Log in to Equinox Streaming and Recording. The following credentials are the default credentials, but when you first log in, you are prompted to update your password:
    - Username: `admin`
    - Password: `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™ 2012 server. When you are securing the system with certificates, this address must match the address that you specify in the transcoder server certificate.



Transcoder Address: 11.22.33.44

Conference Point Version 8.3.04032109.31, Copyright © 2015 Avaya Inc. All Rights Reserved.

Figure 190: Transcoder Registration

Next steps

Return to the Installation checklist on page 352 to see your next task.

Related links

Unregistering each of the components on page 373

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 371

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.

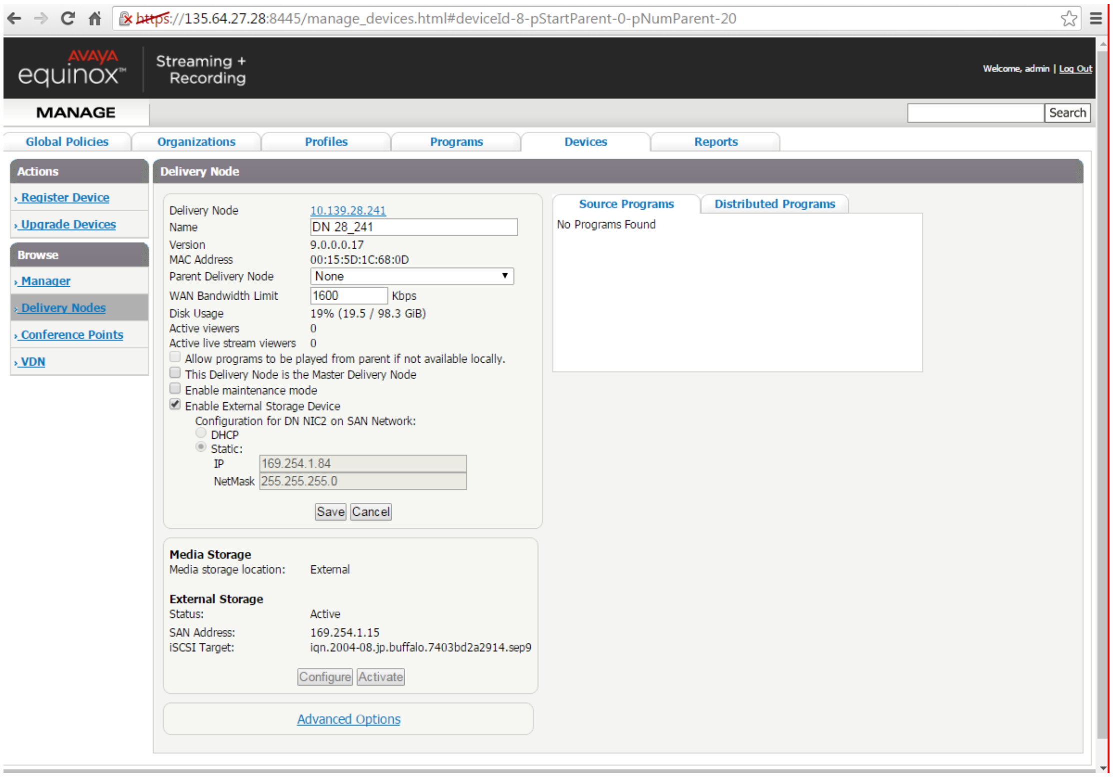
Equinox Streaming and Recording stops creating new recordings and triggers an alert when capacity on the master DN reaches 90%. Equinox Streaming and Recording stops any recordings in progress and triggers an alert when capacity on the master DN reaches 95%. If the capacity on an edge DN reaches 90%, 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.



~~https~~://135.64.27.28:8445/manage_devices.html#deviceId-8-pStartParent-0-pNumParent-20

No Programs Found

Delivery Node 10.139.28.241
Name DN 28_241
Version 9.0.0.0.17
MAC Address 00:15:5D:1C:68:0D
Parent Delivery Node None ▾
WAN Bandwidth Limit 1600 Kbps
Disk Usage 19% (19.5 / 98.3 GiB)
Active viewers 0
Active live stream viewers 0
☐ Allow programs to be played from parent if not available locally.
☐ This Delivery Node is the Master Delivery Node
☐ Enable maintenance mode
☑ Enable External Storage Device
Configuration for DN NIC2 on SAN Network:
○ DHCP
● Static:
IP 169.254.1.84
NetMask 255.255.255.0

Media Storage
Media storage location: External

External Storage
Status: Active
SAN Address: 169.254.1.15
iSCSI Target: iqn.2004-08.jp.buffalo.7403bd2a2914.sep9

Figure 191: Delivery Node Details

5. Configure the settings, as described in Table 51: Delivery Node Details on page 376.

Table 51: 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.
Active Viewers	You can view the number of users who are currently accessing recordings.
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

Table continues…

Field Name	Description
	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)** If you have configured your system to enable individual delivery nodes to specify the distribution policy, then an additional panel is displayed. Configure the settings, as described in Table 52: Override Default Distribution Policy Panel on page 377.

Table 52: Override Default Distribution Policy Panel

Field	Description
Unicast Only	Select to enable only unicasting from the source delivery node.
Multicast Only	Select to enable only multicasting from the source delivery node. If you select this option and the client technically supports the playing of multicast but the network location does not support multicasting, viewers cannot view the program.
Multicast and Unicast (Unicast Rollover if Multicast is Unsuccessful)	Select to enable the stream to be unicast from the source delivery node if the client does not support multicasting. If you select this option but multicast facilities are not available on the source delivery node, the unicast rollover does not occur.

Note:

These settings only impact MMS streams. You can specify **Multicast Only** and still deliver HLS streams.

7. **(Optional)** Click **Advanced Options** and configure the settings as described in Table 53: Advanced Options on page 377.

Table 53: Advanced Options

Field	Description
Distribute All Programs	Select to take all the programs in the system from other source nodes and copy them to this delivery node.

Table continues…

Field	Description
Replace with new DN	Use this setting when bringing on a replacement delivery node for an older or broken system.
Synchronize	Select to ensure that all programs are distributed to their assigned delivery nodes. Only perform this step if programs have indicated failure or pending for some time. When you click **Synchronize**, Equinox Streaming and Recording attempts to complete any failed or pending distributions for a given DN. You can check the progress of the synchronization by checking the DN program listing on the Delivery Node screen. This feature is useful when adding a new DN, or moving an existing DN within a DN hierarchy. The programs are not updated until you click **Synchronize** . You may also want to click **Synchronize** if a delivery node has been offline for some time and needs to synchronize programs that have occurred during this time.

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.

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 54: 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 600GB (Avaya Common Server 2) or 900GB (Avaya Common Server 3) at RAID level 1.
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.	
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.

6. 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 Windows Media or .MP4 format.

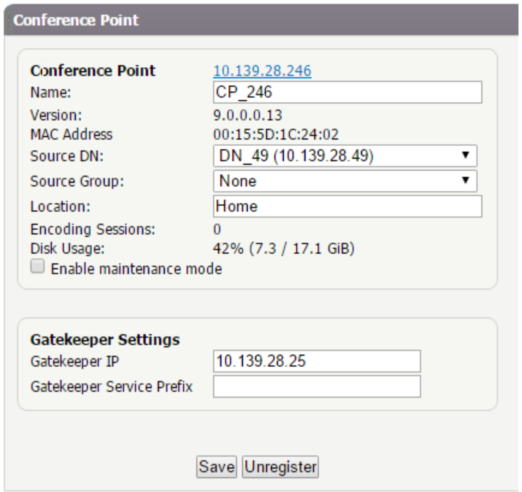
Each conference point must be associated with a delivery node. A delivery node streams and optionally archives the content captured by the conference point and delivers it to client systems.

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.



Conference Point

Conference Point: 10.139.28.246
Name: CP_246
Version: 9.0.0.0.13
MAC Address: 00:15:5D:1C:24:02
Source DN: DN_49 (10.139.28.49)
Source Group: None
Location: Home
Encoding Sessions: 0
Disk Usage: 42% (7.3 / 17.1 GiB)
□ Enable maintenance mode

Gatekeeper Settings
Gatekeeper IP: 10.139.28.25
Gatekeeper Service Prefix:

Figure 192: Conference Point Details

5. Configure the settings, as described in Table 55: Conference Point Details on page 381.

Table 55: 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.
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.
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 56: Polling Settings on page 382.

Table 56: Polling 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	

5. Click **Save**.

Configuring the recycle bin

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 57: Retain deleted recordings for: on page 383.

Table 57: 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.

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. For example, you can configure the URL of the Avaya Scopia Desktop Server that users connect to in order to see broadcasts.

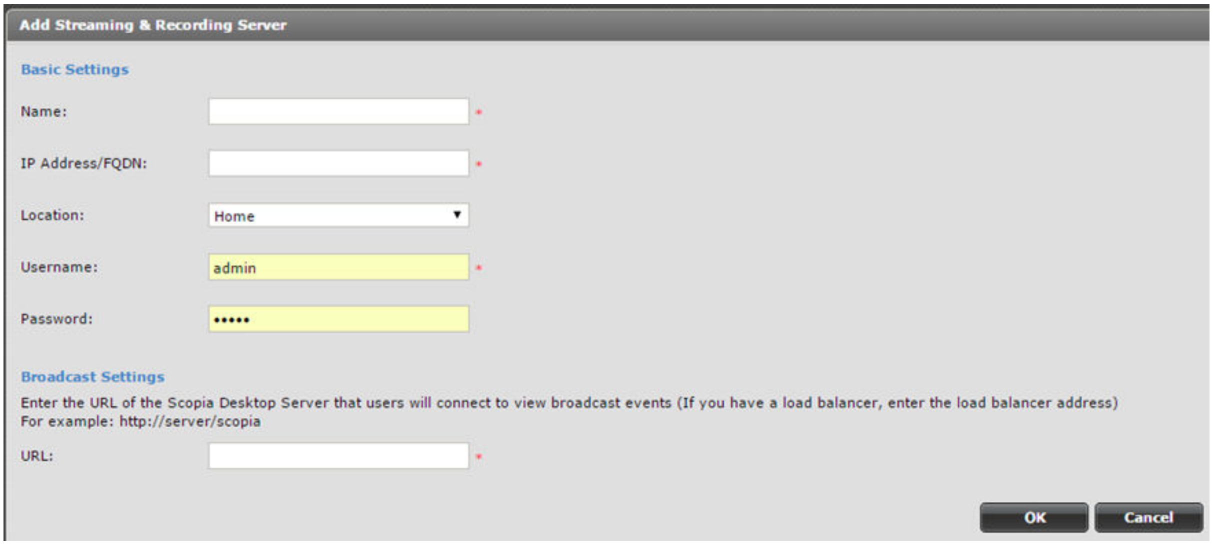
If you are using the Avaya Scopia Content Center Streaming and Recording Server, you need to configure and manage the servers using the Avaya Scopia Desktop Server. For more information, see the *Administrator Guide for Avaya Scopia Desktop Server*, which is from a previous release and is available on support.avaya.com.

Important:

Once you configure a Equinox Streaming and Recording Server you cannot revert back to the Scopia Content Center Streaming Server or the Scopia Content Center Recording Server.

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 193: Adding an Avaya Equinox Streaming and Recording server on page 384).



Add Streaming & Recording Server

Basic Settings

Name: *

IP Address/FQDN: *

Location: Home

Username: admin *

Password: •••••

Broadcast Settings

Enter the URL of the Scopia Desktop Server that users will connect to view broadcast events (If you have a load balancer, enter the load balancer address)
For example: http://server/scopia

URL: *

Figure 193: Adding an Avaya Equinox Streaming and Recording server

4. Configure the Equinox Streaming and Recording Server's settings, as described in (Table 58: Configuring the Avaya Equinox Streaming and Recording on page 384).

Table 58: 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. This is the address that clients use to access the Equinox Streaming and Recording Server portal within Scopia Desktop. 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 theEquinox Streaming and Recording Server portal. The default is **admin**. If you change the username in the Equinox Streaming and Recording Server, you must update the username here.
Password	Enter the administrative password used to login to the Equinox Streaming and Recording Server portal. The default is **admin**. If you change the password in the Equinox Streaming and Recording Server, you must update the password here.
Secure connection using HTTPS	❗ **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 screen, the

Table continues…

Field Name	Description
	option only becomes available if you have a regular license. If you have a non-encrypted license you cannot secure the connection. Select to enable HTTPS, which encrypts the communication between the Equinox Streaming and Recording Server and the client. It is important to be consistent. If the Avaya Scopia Desktop Server is configured for HTTPS, you must select this checkbox to ensure that the Equinox Streaming and Recording Server matches the Avaya Scopia Desktop Server. To enable HTTP deselect the checkbox. 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.
URL	Enter the URL of the Avaya Scopia Desktop Server you are using to view broadcasts. The URL must be in the format *http://<web URL>:<port number>/scopia*. If you are using a load balancer, enter the URL of the load balancer.

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 a Avaya Equinox Recording Gateway. You can deploy the Avaya Equinox Recording Gateway using the Avaya Equinox Management interface.

When a user records a conference, Avaya 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, Avaya Equinox Recording Gateway is not used.

About this task

This section summarizes the steps for configuring the Avaya 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 Avaya Equinox Management and for information on configuring the meeting types, see *Administering Avaya Equinox Management*, which is available on support.avaya.com.

Procedure

- Add the Avaya Equinox Recording Gateway as a gateway, in Avaya Equinox Management. There is a drop-down menu, called **Avaya Recording Gateway**.
- Upload the default audio prompts to the Avaya Equinox Recording Gateway.

- Verify that the two new meeting types are displayed in the Avaya Equinox Management interface.
- Ensure that you are logged into Avaya 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 18: Upgrading to the Avaya Equinox solution

Upgrading the Equinox Solution

Customers who run a Scopia 8.3 release can upgrade to OTT Equinox Solution 9.0. For detailed upgrade information, refer to the product administrator guides listed in the Documentation section of this guide.

Chapter 19: 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 Scopia® XT Series	Plan for and deploy Avaya Scopia® XT Series	Partners, Services, and Support personnel
Deployment Guide for XT Telepresence	Plan for and deploy XT Telepresence	Partners, Services, and Support personnel
Deployment Guide for Avaya Video Collaboration Solution for IP Office	Plan for and deploy Avaya Video Collaboration Solution for IP Office	Partners, Services, and Support personnel
Deployment Guide for Avaya Equinox Add-in for IBM Lotus Notes	Plan for and deploy Avaya Equinox Add-in for IBM Lotus Notes	Partners, Services, and Support personnel
Deployment Guide for Avaya Scopia® Video Gateway for Microsoft Lync	Plan for and deploy Avaya Scopia® Video Gateway for Microsoft Lync	Partners, Services, and Support personnel
OCS Deployment Guide for Avaya Scopia® Video Gateway for Microsoft Lync	Plan for and deploy Avaya Scopia® Video Gateway for Microsoft Lync	Partners, Services, and Support personnel
Deployment Guide for Avaya Scopia XT Desktop Server for IP Office	Plan for and deploy Avaya Scopia XT Desktop Server for IP Office	Partners, Services, and Support personnel

Table continues…

Title	Use this document to:	Audience
Deployment Guide for Avaya Scopia XT Desktop Server	Plan for and deploy Avaya Scopia XT Desktop Server	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
Installation Guide for Avaya Scopia XT Desktop Server	Install Avaya Scopia XT Desktop Server	Partners, Services, and Support personnel
Installation Guide for Avaya Scopia Desktop Server for Avaya Aura® Power Suite	Install Avaya Scopia Desktop Server for Avaya Aura® Power Suite	Partners, Services, and Support personnel
Installation Guide for Kerberos in Avaya Equinox Management	Install Kerberos in Avaya Equinox Management	Partners, Services, and Support personnel
Rack Mounting Guide for Avaya Scopia® Elite 6000 MCU	Install the Avaya Scopia® Elite 6000 MCU hardware	Partners, Services, and Support personnel
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 Application Server for Avaya Aura® Power Suite	Perform administration tasks for Avaya Equinox Application Server for Avaya Aura® Power Suite	System administrators
Administrator Guide for Avaya Equinox Streaming and Recording Server	Perform administration tasks for Avaya Equinox Streaming and Recording Server	System administrators

Table continues…

Title	Use this document to:	Audience
Administrator Guide for Avaya Scopia Desktop Server	Perform administration tasks for Avaya Scopia Desktop Server	System administrators
Administrator Guide for Avaya Scopia Desktop Server for Avaya Aura® Power Suite	Perform administration tasks for Avaya Scopia Desktop Server for Avaya Aura® Power Suite	System administrators
Quick Setup Guide for Avaya Scopia® XT5000 Codec Only	Perform administration tasks for the Avaya Scopia® XT5000 codec	System administrators
Avaya Scopia® XT5000 Codec Only	Perform administration tasks for the Avaya Scopia® XT5000 codec	System administrators
Avaya Scopia® XT Executive 240	Perform administration tasks for Avaya Scopia® XT Executive 240	System administrators
Avaya Scopia® XT5000 Server for IP Office	Perform administration tasks for Avaya Scopia® XT5000 Server for IP Office	System administrators
Avaya Scopia® XT Premium 3–way Microphone Pod	Perform administration tasks for Avaya Scopia® XT Premium 3–way Microphone Pod	System administrators
Avaya Scopia® XT4300	Perform administration tasks for Avaya Scopia® XT4300	System administrators
Avaya Scopia® XT4300 Codec Only	Perform administration tasks for the Avaya Scopia® XT4300 codec	System administrators
Avaya Scopia® XT7100 Codec Only	Perform administration tasks for the Avaya Scopia® XT7100 codec	System administrators
Avaya Scopia® XT Deluxe Camera	Perform administration tasks for Avaya Scopia® XT Deluxe Camera	System administrators
Avaya Scopia® XT Flex Camera	Perform administration tasks for Avaya Scopia® XT Flex Camera	System administrators
Quick Tips for Avaya Scopia® XT Series	Perform administration tasks for Avaya Scopia® XT Series	System administrators
Supporting		
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	System administrators, Customers, Partners,

Table continues…

Title	Use this document to:	Audience
	remote SNMP management client of its operational status	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
Purchasing Guide for AvayaLive™ Video	Understand how to purchase AvayaLive™ Video	System administrators, Customers, Partners, Services, and Support personnel
Using		
Using Avaya Equinox Unified Portal	Understand the features of and use Avaya Equinox Unified Portal	Customers
User Guide for Avaya Scopia® Elite 6000 MCU	Understand the features of and use Avaya Scopia® Elite 6000 MCU	Customers
Using Avaya Equinox Media Server	Understand the features of and use Avaya Equinox Media Server	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 Scopia® XT Series	Understand the features of and use Avaya Scopia® XT Series	Customers
User Guide for Avaya Equinox Management	Understand the features of and use Avaya Equinox Management	Customers
User Guide for Avaya Equinox Add-in for IBM Lotus Notes	Understand the features of and use Avaya Equinox Add-in for IBM Lotus Notes	Customers
User Guide for Avaya Equinox Add-in for Microsoft Outlook	Understand the features of and use Avaya Equinox Add-in for Microsoft Outlook	Customers
User Guide for Avaya Equinox Add-in for Microsoft Outlook for Avaya Aura® Power Suite	Understand the features of and use Avaya Equinox Add-in for Microsoft Outlook for Avaya Aura® Power Suite	Customers
User Guide for Avaya Scopia® Video Gateway for Microsoft Lync	Understand the features of and use Avaya Scopia® Video Gateway for Microsoft Lync	Customers
User Guide for Avaya Scopia® XT Desktop Client	Understand the features of and use Avaya Scopia® XT Desktop Client	Customers

Table continues…

Title	Use this document to:	Audience
User Guide for Avaya Scopia Mobile	Understand the features of and use Avaya Scopia Mobile	Customers
User Guide for Avaya Scopia® Control	Understand the features of and use Avaya Scopia® Control	Customers

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://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 an appropriate release number.
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 displays the documents only from the selected category.
7. Click **Enter**.

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

Table continues…

Course code	Course title
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 http://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.

Glossary

1080p See Full HD on page 398.

2CIF 2CIF describes a video resolution of 704 x 288 pixels (PAL) or 704 x 240 (NTSC). It is double the width of CIF, and is often found in CCTV products.

2SIF 2SIF describes a video resolution of 704 x 240 pixels (NTSC) or 704 x 288 (PAL). This is often adopted in IP security cameras.

4CIF 4CIF describes a video resolution of 704 x 576 pixels (PAL) or 704 x 480 (NTSC). It is four times the resolution of CIF and is most widespread as the standard analog TV resolution.

4SIF 4SIF describes a video resolution of 704 x 480 pixels (NTSC) or 704 x 576 (PAL). This is often adopted in IP security cameras.

720p See HD on page 400.

AAC AAC is an audio codec which compresses sound but with better results than MP3.

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 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.

Avaya Scopia Content Slider

See Content Slider on page 396.

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.

BFCP (Binary Floor Control Protocol)

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.

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 405.

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 Scopia 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 396.

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, XT Executive. 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.

E.164

E.164 is an address format for dialing an endpoint with a standard telephone numeric keypad, which only has numbers 0 - 9 and the symbols: * and #.

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 XT Executive, software endpoints like Scopia Desktop Client, mobile device endpoints like Scopia Mobile, room systems like XT Series, and telepresence systems like XT Telepresence.

Endpoint Alias

See Alias on page 394.

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 397.

FPS See Frames Per Second on page 398.

Frame Rate See Frames Per Second on page 398.

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 Equinox TIP Gateway, or the 100 Gateway.

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 399.

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 394.

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 400.

High Profile

See H.264 High Profile on page 399.

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 404.

KBps

Kilobytes per second (KBps) measures the bitrate in kilobytes per second, not kilobits, by dividing the number of kilobits by eight. Bitrate is normally quoted as kilobits per second (kbps) and then converted to kilobytes per second (KBps). Bitrate measures the throughput of data communication between two devices.

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).

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

Scopia Desktop's 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 might or might 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

An MCU, or Multipoint Control Unit, connects several endpoints to a single videoconference. It manages the audio mixing and creates the video layouts, adjusting the output to suit each endpoint's capabilities.

MCU service

See Meeting Type on page 402.

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 396.

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. In Scopia Desktop Client, 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 Scopia Desktop Server, 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.

Multicast Streaming

Multicast streaming sends a videoconference to multiple viewers across a range of addresses, reducing network traffic significantly. Scopia Desktop Server multicasts to a single IP address, and streaming clients must tune in to this IP address to view the meeting. Multicasts require that routers, switches and other equipment know how to forward multicast traffic.

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.

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.

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 396.

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.

Q.931

Q.931 is a telephony protocol used to start and end the connection in H.323 calls.

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.

Quality of Service (QoS)

Quality of Service (QoS) determines the priorities of different types of network traffic (audio, video and control/signaling), so in poor network conditions, prioritized traffic is still fully transmitted.

Recordings

A recording of a videoconference can be played back at any time. Recordings include audio, video and shared data (if presented). Users can access recordings from the Scopia Desktop web portal or using a web link to the recording on the portal.

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.

Scalability Scalability describes the ability to increase the capacity of a network device by adding another identical device (one or more) to your existing deployment. In contrast, a non-scalable solution would require replacing existing components to increase capacity.

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 402.

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 Scopia® 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 404.

SIP Server A SIP server is a network device communicating via the SIP protocol.

SIP URI See URI on page 408.

Slider See Content Slider on page 396.

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. For example, Scopia Desktop Client or Scopia Mobile.

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 405.

Standard Definition See SD on page 405.

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. There are two types of streaming supported in Equinox Solution: unicast which sends a separate stream to each viewer, and multicast which sends one stream to a range of viewers.

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 the Scopia Elite MCU and/or Equinox Media Server only by four times.

> **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.

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.

UC (Unified Communications)

UC, or unified communications deployments offer solutions covering a wide range of communication channels. These include audio (voice), video, text

(IM or chat), data sharing (presentations), whiteboard sharing (interactive annotations on shared data).

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 in Scopia Desktop Server. To save bandwidth, consider multicast 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 used to locate a SIP device on a network, 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. For example,<*endpoint name*>@<*server_domain_name*>. When dialing URI between organizations, the server might often be the Avaya Equinox H.323 Edge of the organization.

URI Dialing

Accessing a device via its URI on page 408.

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 Scopia Desktop and Scopia Mobile functionality, and allowed bandwidth for calls.

VFU

See Video Fast Update (VFU) on page 408.

VGA

VGA defines a video resolution of 640 x 480 pixels.

Video Fast Update (VFU)

Video Fast Update (VFU) is a request for a refreshed video frame, sent when the received video is corrupted by packet loss. In response to a VFU request, the broadcasting endpoint sends a new intra-frame to serve as the baseline for the ongoing video stream.

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 404.

Video Switching

See Switched video on page 407.

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 Avaya Scopia Desktopuser portal. To access the Viewer Portal, you can select **Recordings and Events** on the main Scopia Desktop page. 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 in Scopia Desktop and Scopia Mobile 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 download Scopia Desktop or Scopia Mobile free 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 Scopia Desktop 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 Scopia Desktop 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.