Avaya Scopia® Desktop Server Administrator Guide

Release 8.3.3
For Solution 8.3
Issue 1
August 2015

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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: http://support.avaya.com 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 a 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 IF YOU PURCHASE A 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, HTTP://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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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. 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 Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. 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.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use 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").

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

Each product has its own ordering code and license types. Note 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: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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.

Note to Service Provider

The product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

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: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://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: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: About Scopia® Desktop

Scopia® Desktop is a desktop videoconferencing system turning Windows PCs, Apple Macintosh computers and mobile devices into videoconferencing endpoints. It includes the latest in video technology including support for HD video, NetSense for video quality optimization, Scalable Video Coding (SVC) for unsurpassed error resiliency and H.264 when viewing both meeting participants and data collaboration. Its audio system provides echo cancellation, background noise suppression, and is highly resilient to network errors common on the Internet.

Scopia® Desktop is comprised of the Scopia® Desktop server and a lightweight Scopia® Desktop Client which turns a PC or Mac into a videoconferencing endpoint. Scopia® Mobile users can also access the Scopia® Desktop server from their iOS and Android devices. For more information on Scopia® Mobile, see the *User Guide for Scopia® Mobile*.

Related Links

[About Scopia® Desktop server](#) on page 7
[About Components of the Scopia® Desktop server](#) on page 9
[About Scopia® Desktop Client](#) on page 9

About Scopia® Desktop server

Scopia® Desktop is a desktop videoconferencing system turning Windows PCs, Apple Macintosh computers and mobile devices into videoconferencing endpoints. It includes the latest in video technology including support for HD video, NetSense for video quality optimization, Scalable Video Coding (SVC) for unsurpassed error resiliency and H.264 when viewing both meeting participants and data collaboration. Its audio system provides echo cancellation, background noise suppression, and is highly resilient to network errors common on the Internet.

Scopia® Desktop server is the component which manages the Scopia® Desktop Clients and Scopia® Mobile endpoints participating in a videoconference. It includes firewall traversal features to ensure call connectivity and quality videoconferencing. Additionally, Scopia® Desktop server supports advanced videoconferencing features such as H.239 data collaboration, PIN protected meetings, conference moderation, SIP point-to-point communication between Scopia® Desktop Clients, and full authentication and authorization.

The Scopia® Desktop server requires Scopia® Elite MCU as part of its deployment.

Scopia® Desktop offers the following additional features:

- Integration with Microsoft Outlook

Users can send invitations to videoconferences directly from Microsoft Outlook using the Scopia® Add-in for Microsoft Outlook. The 32 bit version works directly with the Scopia® Desktop server, while the 64 bit version works directly with Scopia® Management. For more information, see *User Guide for Scopia® Add-in for Microsoft Outlook*.

- Chat messages to meeting participants

  Users can send public or private chat messages to meeting participants, including those connecting via dedicated endpoints or room systems.

- High quality video and audio even with limited bandwidth or poor network conditions, by using H.264 High Profile for compression.

  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.

- Service provider (multi-tenant) support

  Scopia® Desktop works alongside Avaya Scopia® Management to support service provider deployments which cater for multiple organizations (tenants). In a multi-tenant deployment, each Scopia® Desktop meeting is associated with only one tenant. Multi-tenant features include:

  - All Scopia® Desktop Clients only see contacts (users or endpoints) belonging to their own organization.
  - When browsing or searching a recording, Scopia® Desktop Clients only see recordings belonging to their own organization.

- Scopia® Desktop server has extensive support for security, both standard encryption with certificates and a proprietary secure protocol between the client and server. For more information, see Minimum Requirements and Specifications of Scopia® Desktop server on page 14.

- Scalability with an external load balancer

  Scopia® Desktop works with load balancers like F5 BIG-IP Load Traffic Manager and Radware's AppDirector, providing unlimited scalability, high availability and redundancy for large deployments.

- Microsoft Lync support

  With Scopia® Video Gateway in your deployment, Scopia® Desktop Clients can invite Microsoft Lync users to a meeting.

- Streaming and recording

  Streaming and recording with the Scopia® Desktop serveris available up to Version 8.3.1 of the Scopia® Solution. From Version 8.3.2 Avaya has packaged the streaming and recording functionality into the Avaya Scopia® Streaming and Recording server.

Related Links

About Scopia® Desktop on page 7

About Components of the Scopia® Desktop server

Scopia® Desktop server includes several different servers, each fulfilling its own function.

- Scopia® Desktop server

  At the center of Scopia® Desktop, the conference server creates conferences with Scopia® Desktop Clients and Scopia® Mobile devices, relaying media to the MCU to enable transparent connectivity with H.323 and SIP endpoints.

- Scopia® Desktop Application Server (Tomcat)

  The underlying Scopia® Desktop web server and application server is implemented by Tomcat. It serves as the login server, the update server, the recording server, the Scopia® Content Slider server and the Scopia® Desktop web portal.

- Scopia® Content Slider server

  Part of the Tomcat Application Server, it stores the data already presented in the videoconference and makes it available for participants to view during the meeting.

- Avaya Scopia® Content Center Recording server

  The server support recording and streaming video conferences. Using the streaming feature, you can broadcast live video conferences to stakeholders who cannot join the video conference.

- Avaya Scopia® Web Collaboration server

  The server supports sharing content in video conferences, such as documents, presentations, and whiteboards.

Related Links

About Scopia® Desktop on page 7

About Scopia® Desktop Client

The Avaya Scopia® Desktop Client is a simple web browser plug-in for interactive videoconferencing. With Scopia® Desktop client you can experience high definition videoconferencing, connecting you with other participants who may be using dedicated endpoints, room systems or even telepresence systems, all from your PC or Mac. Scopia® Desktop Client is part of Avaya Scopia® Solution for SMBs (small and medium businesses) which includes Scopia® Desktop and Avaya Scopia® XT Series with its built-in MCU which endpoints and room systems use to connect.

Clients can be centrally managed and deployed without complex licensing fees or installation issues. Users receive a web link in their invitation to join a videoconference, and in moments they are connected and participating. The Scopia® Desktop Client includes the main videoconference client with a built-in chat window and presentation viewing abilities (Figure 1: The Scopia® Desktop Client user interface on page 10).

Figure 1: The Scopia® Desktop Client user interface

Scopia® Desktop Client supports a number of algorithms and standards to make the most efficient use of bandwidth, including:

- 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.

- NetSense

  NetSense is a proprietary Scopia® Solution technology which optimizes the video quality according to the available bandwidth to minimize packet loss.

A Scopia® Add-in for Microsoft Outlook enables easy scheduling of meetings directly from within Microsoft Outlook. You can install the add-in together with Scopia® Desktop Client.

Related Links

About Scopia® Desktop on page 7

What's new in Scopia® Desktop

Elevated Quality

The new version adds Full HD 1080p everywhere:

- Full HD 1080p mobile user support with Scopia® Desktop

  Mobile users on their laptops, tablet PCs, and desktops can participate with the Full 1080p HD video quality previously available only on room systems, executive desktops, or hardware-based personal systems.

- Additionally, Avaya's cloud service, AvayaLive™ Video, provides Full HD 1080p support for meeting participants.

Enhanced Streaming and Recording

The new version phases out the Scopia Content Center streaming and recording solution (used up to version 8.3.1) and offers the following features:

- Streaming and recording delivered as one appliance for installation simplicity
- Scopia® Desktop and users can initiate recording with one click
- Notifications to users that the meeting is being recorded, thus complying with legal and privacy requirements
- Playback of previous recordings
- Streaming of meetings, townhalls and trainings, without involving specialized IT personnel
- Excellent scalability with up to 100,000 live viewers

Enhanced User Experience

The new version introduces the following improvements:

- Wireless presentation support with Scopia video room systems

  Avaya Scopia users now have the ability to wirelessly present from their laptop (either PC or Mac) with Avaya ScreenLink.

- Mobile meeting continuity between Scopia® Desktop Client, Scopia® Mobile, and room systems

  With Avaya Mobile Link, the user's mobile device automatically pairs and transfers the meeting to the room system, with the added benefit of enjoying the room system's crystal-clear audio, HD camera and large display.

- Network Quality Indicator

  The user gets a real-time indication of the quality of the connection, just as on the mobile phone. The call statistics button is still available to open a window with more detailed information about the call.

- Enhanced Gallery Layout

  The Gallery Layout (mixed video and presentation) is now available to any XT Series endpoint without the need to register with Scopia® Management.

- Virtual Knock on the Door

With this feature, late arrivers with Scopia® Desktop, Scopia® Mobile, and room systems have to ask for permission to join the meeting and the meeting host (moderator) can let them in.

- Outlook Scheduling Enhancements

  The new version phases out Scopia® Desktop add-in in favor of Avaya Scopia® Management plug-in providing:

  - Installation from desktop
  - Connection to Avaya Scopia® Desktop server (no need to be on VPN)
  - Support of HTTPS redirect
  - Two-mode usage: a simplified one like Scopia® Desktop, and an advanced one leveraging Scopia® Management's sophisticated capabilities including the ability to reserve resources such as MCU ports, and automatically invite room system endpoints.
  - Scopia® Management awareness of all system meeting.

- Advanced Web Collaboration Option

  The new version adds the following improvements:

  - Integrated Avaya Aura Conferencing (AAC) capabilities for more feature-rich, content-sharing capabilities

    Version 8.3 incorporates the rich web/data collaboration experience from Avaya's AAC solution within the Scopia® Solution. Features include white boarding, application sharing, selecting the screen to share with multiple monitors – which is becoming more prevalent with users docking their PC tablets and ultrabooks and using both displays. Also, this enables remote desktop control – where a user sharing the desktop can also share keyboard and mouse with one other meeting participant.
  - Data collaboration gateway functionality for room system interoperability (H.323 and SIP systems)
  - Web collaboration delivered as an appliance for installation simplicity:
    - Web collaboration supported by Scopia® Desktop Clients
    - Using web collaboration to present from Scopia® Desktop Clients requires users to download the new web collaboration plug-in from the Scopia® Desktop portal
    - Scopia® Mobile experience as today
    - Avaya Scopia® Web Collaboration server transcodes web collaboration presentation to/from H.239/BFCP with XT Series room systems and third party endpoints
    - Per service configuration. Standard presentation (H.239) is used in case web collaboration is disabled for the service.

- Unified Avaya User Interface Client Style

  Scopia® Desktop and Scopia® Mobile display the unified look and feel which user experience across all the Avaya offerings. With a clean gallery layout, the product line has the same look and feel as other Avaya solutions including Avaya Aura Conferencing.

Chapter 2: Planning your Avaya Scopia® Desktop Deployment

When planning your Avaya Scopia® Desktop deployment, consider the following:

- 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:

Related Links

Minimum Requirements and Specifications of Scopia® Desktop server on page 14
Planning your Topology for Scopia® Desktop server on page 16
Deploying Scopia® Desktop server with Dual-NIC on page 28
Estimating and Planning your Bandwidth Requirements on page 29
Ports to Open on Scopia® Desktop on page 37

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

The following add-ins for Scopia® Desktop integrate it with various third-party products. For more information, see the relevant add-in documentation.

- The Scopia® Connector for IBM Lotus Sametime Connect works with IBM Lotus Sametime 8.0, 8.0.1, 8.0.2, 8.0.5, 8.5, 8.5.1, and IBM Lotus Notes 8.0.
- The Scopia® Connector for IBM Lotus Sametime Web Conferencing works with IBM Lotus Sametime versions 8.0, 8.0.1, 8.0.2, and 8.0.5.
- Scopia® Add-in for Microsoft Outlook (64 bit) requires Office 2007 or later, and access to the Avaya Scopia® 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 Scopia® Management. Table 1: Call capacity and hardware requirements for Scopia® Desktop server on page 15 lists the minimum hardware requirements and call capacity for the Scopia® Desktop server.

Table 1: Call capacity and hardware requirements for Scopia® Desktop server

Product name	Recommended server hardware
Scopia® Desktop on dedicated server	Intel ® Xeon ® Processor E3-1270v2 @ 3.50 GHz RAM: 4GB Disk space: 80Gb 4 virtual cores NIC: 1000Mb
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 Scopia® 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 55876-00002: 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 Defining Scopia® Desktop server Public Address and Other Client Connection Settings on page 58.
- 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 Scopia® 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
  - 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 Scopia® Management.

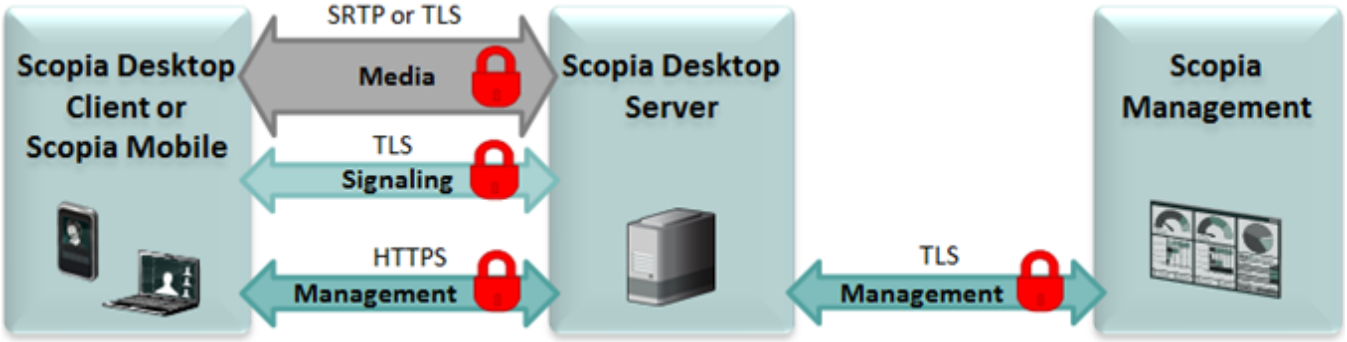


Figure 2: Securing Scopia® Desktop server communications

Related Links

Planning your Avaya Scopia® Desktop Deployment on page 13

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
- 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 Scopia® 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 Scopia® Streaming and Recording server* and *Administering the Avaya Scopia® Streaming and Recording server* at the Avaya Support website: https://support.avaya.com/.

For more information about the Scopia® Desktop components, see About Components of the Scopia® Desktop server on page 9.

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

Planning your Avaya Scopia® Desktop Deployment on page 13
Topology for Small Scopia® Desktop server Deployment on page 17
Medium Scopia® Desktop server Deployment with Dedicated Servers on page 19
Large Scopia® Desktop server Deployment with Dedicated Servers on page 21
Sizing your Scopia® Desktop server Deployment on page 25

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 3: Typical small deployment of Scopia® Desktop server on page 18):

- 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. For a detailed list of all Scopia® Desktop components, see About Components of the Scopia® Desktop server on page 9.
- Avaya Scopia® Management, an application used to control your video network devices and schedule videoconferences. Avaya Scopia® Management includes a built-in gatekeeper.

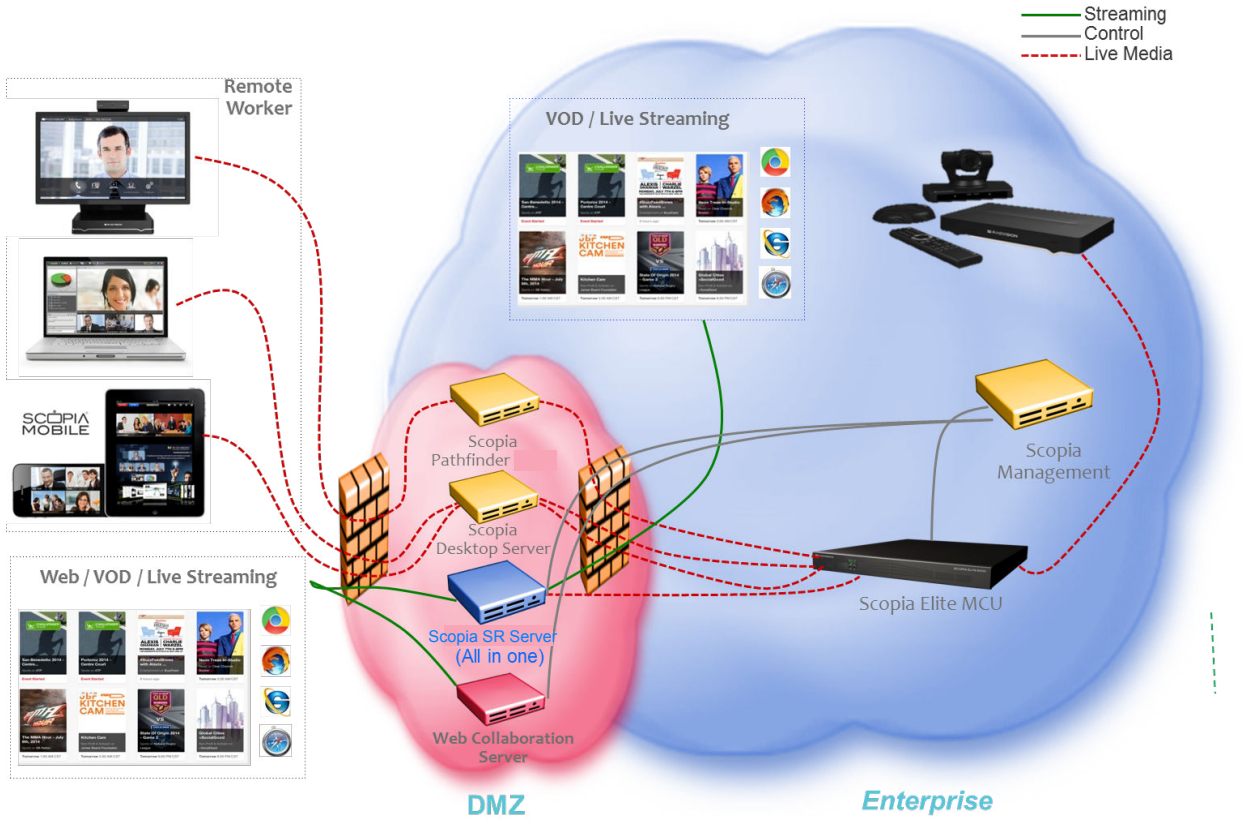


Figure 3: Typical small deployment of Scopia® Desktop server

In addition to Avaya Scopia® Desktop server your organization can choose to deploy optional components: Avaya Scopia® 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 Scopia® Streaming and Recording server* and *Administering the Avaya Scopia® 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 14.

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 19).

Scopia® Desktop server deployments require an MCU to host videoconferences, and Scopia® Management to control your video network devices and schedule videoconferences.

Related Links

Planning your Topology for Scopia® Desktop server on page 16

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 14. For more information about the Scopia® Desktop components, see About Components of the Scopia® Desktop server on page 9.

In addition to Avaya Scopia® Desktop server your organization can choose to deploy optional components: Avaya Scopia® 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 Scopia® Streaming and Recording server* and *Administering the Avaya Scopia® Streaming and Recording server* at the Avaya Support website: https://support.avaya.com/.

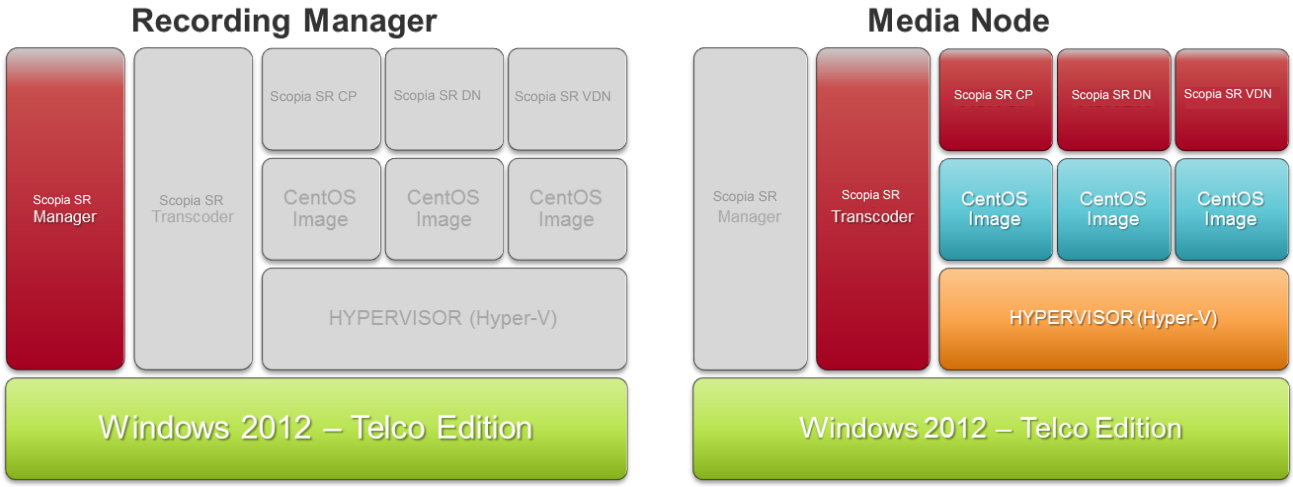


Figure 4: Typical medium-sized deployment

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 5: Deploying dedicated Scopia® Desktop servers in the DMZ on page 20). 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 Scopia® Desktop on page 37.

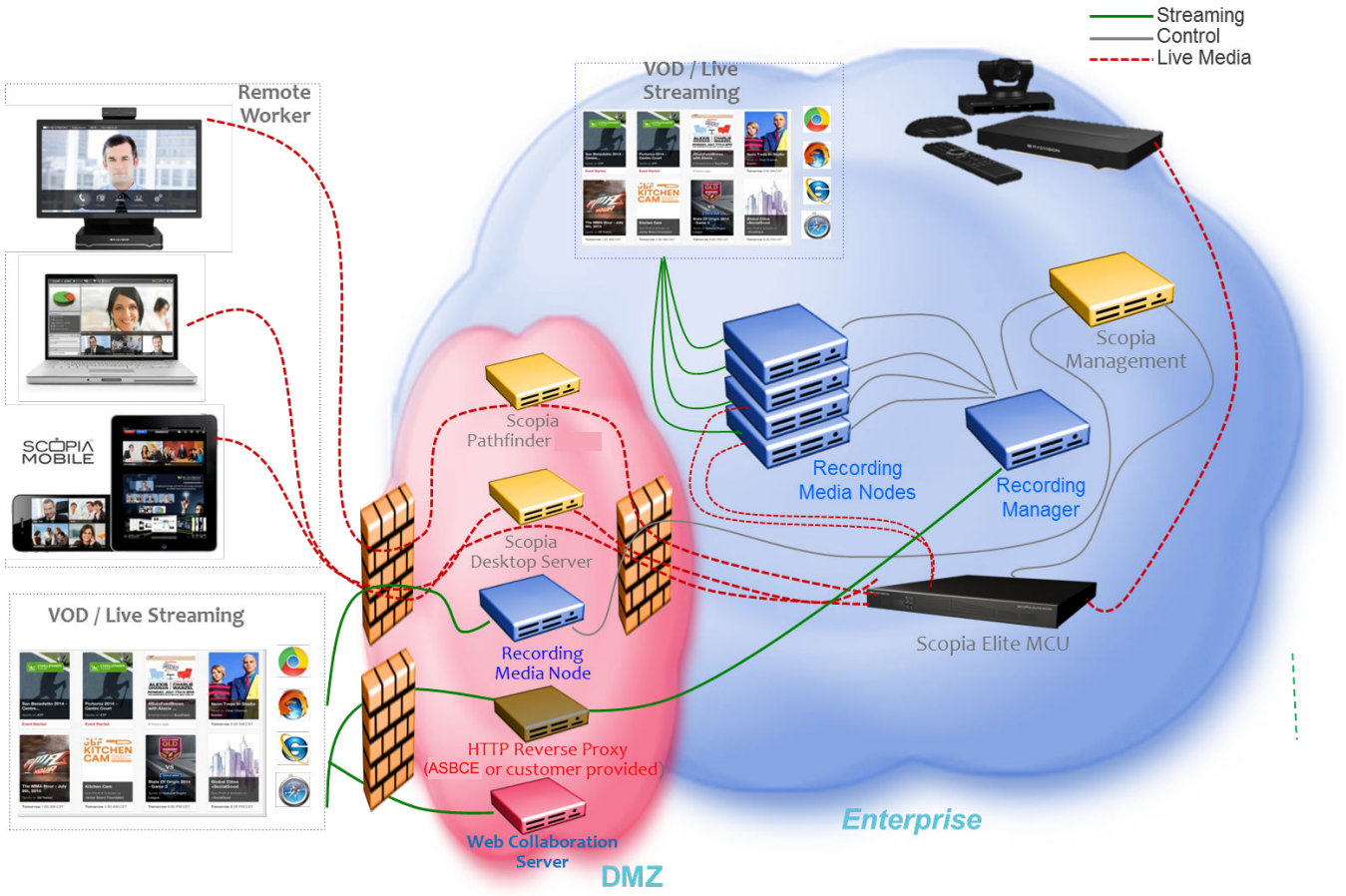


Figure 5: Deploying dedicated Scopia® Desktop servers in the DMZ

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 21. Smaller deployments, on the other hand, might install all components on the same Scopia® Desktop server with a Scopia® Management (see Topology for Small Scopia® Desktop server Deployment on page 17).

Scopia® Desktop server deployments require an MCU to host videoconferences, and Scopia® Management to control your video network devices and schedule videoconferences.

For more information about Scopia® Solution deployments, see the *Solution Guide for Scopia® Solution*.

Related Links

Planning your Topology for Scopia® Desktop server on page 16

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 23.

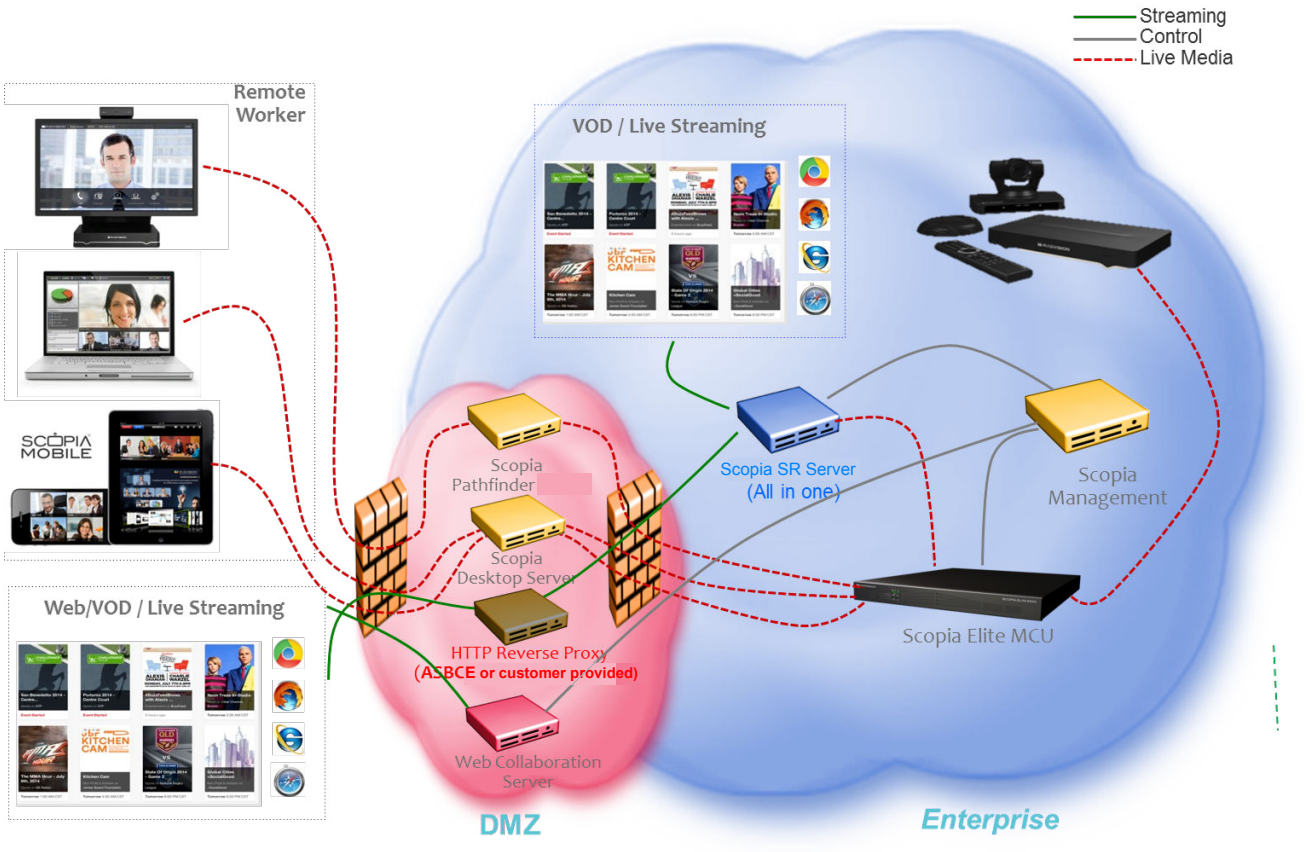


Figure 6: Typical large deployment

In addition to Avaya Scopia® Desktop server your organization can choose to deploy optional components: Avaya Scopia® 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 Scopia® Streaming and Recording server* and *Administering the Avaya Scopia® 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 7: Large Scopia® Desktop server Deployment with Dedicated Servers on page 22).

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.

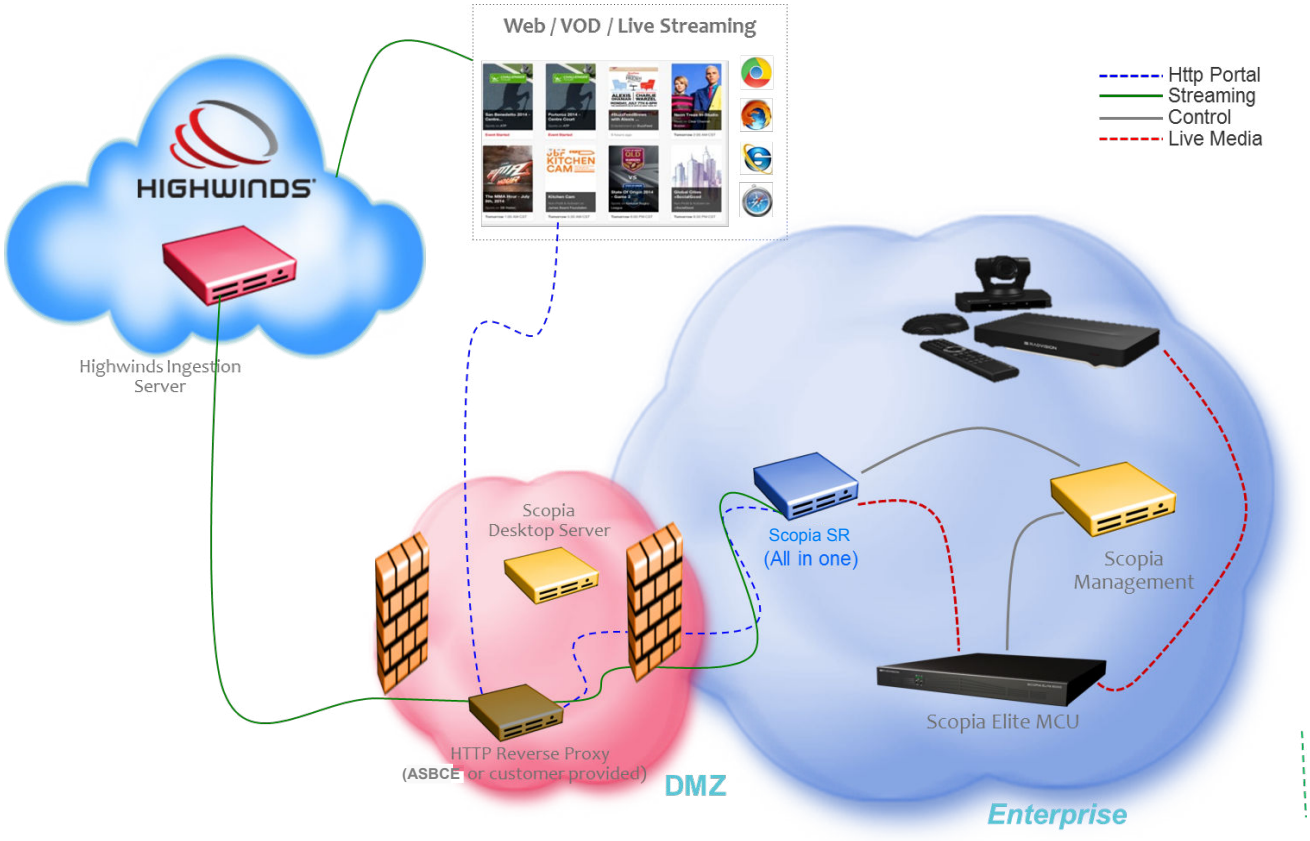


Figure 7: Large Scopia® Desktop server Deployment with Dedicated Servers

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 Scopia® 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 14.

Scopia® Desktop server deployments require an MCU to host videoconferences, and Scopia® Management to control your video network devices and schedule videoconferences.

Related Links

Planning your Topology for Scopia® Desktop server on page 16

Deploying Scopia® Desktop with a Load Balancer on page 23

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 9: Typical load balanced Scopia® Desktop deployment on page 24).

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).

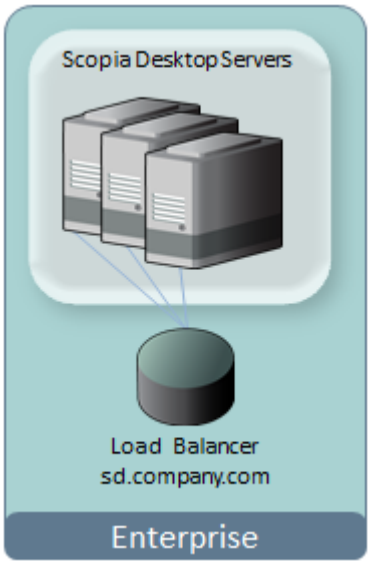


Figure 8: Deploying Scopia® Desktop with a Load Balancer

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.

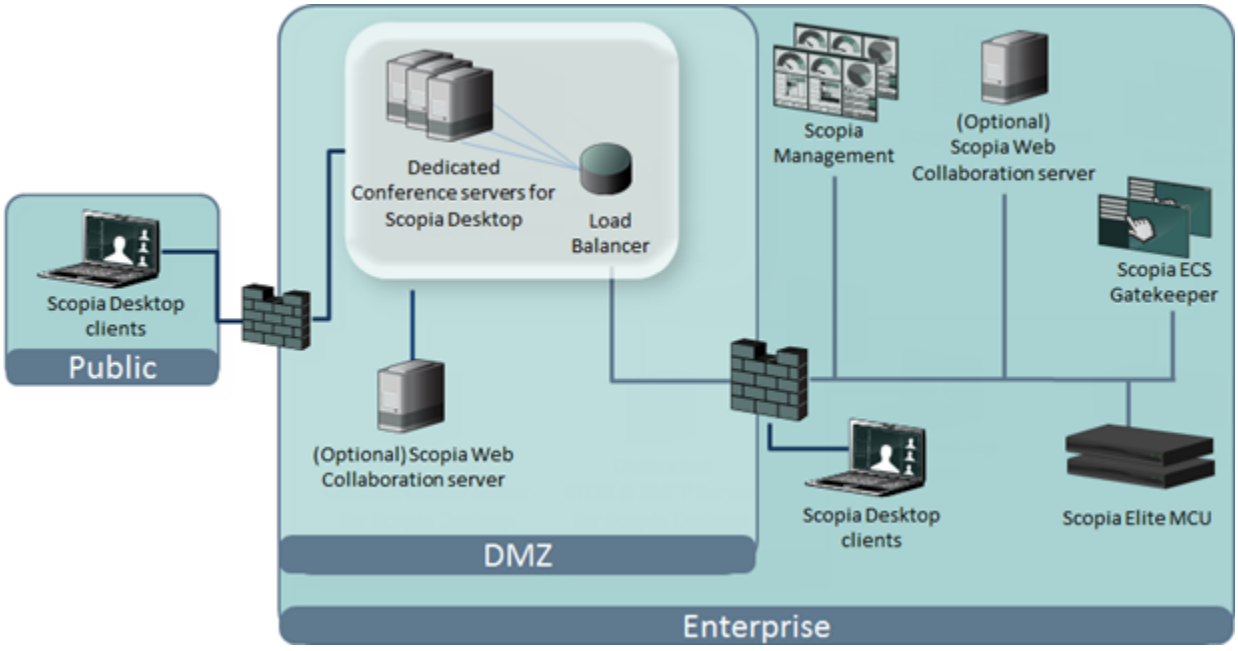


Figure 9: Typical load balanced Scopia® Desktop deployment

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 Securing a Load Balanced Environment on page 116.

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 10: Media can either bypass or travel via the load balancer (example) on page 25):

- 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.

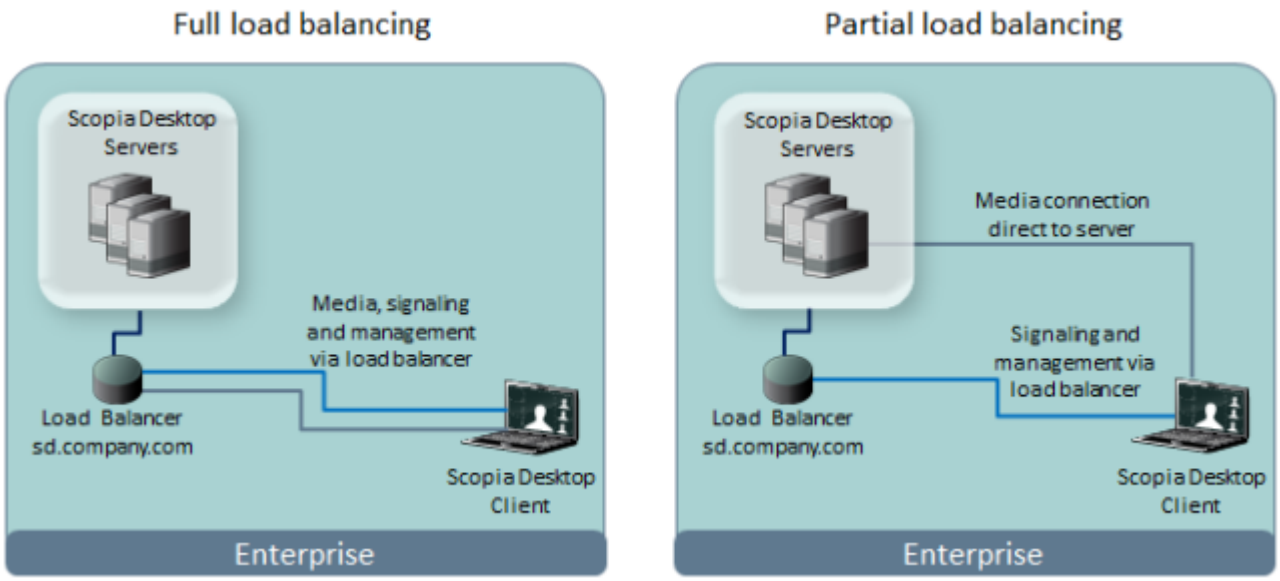


Figure 10: Media can either bypass or travel via the load balancer (example)

For details about configuring load balancing, see Deploying Multiple Scopia® Desktop servers with a Load Balancer on page 102.

Related Links

Large Scopia® Desktop server Deployment with Dedicated Servers on page 21

Sizing your Scopia® Desktop server Deployment

Based on your organization's requirements, you can choose to deploy your Scopia® Desktop server in one of the following ways:

- Topology for Small Scopia® Desktop server Deployment on page 17
- Medium Scopia® Desktop server Deployment with Dedicated Servers on page 19
- Large Scopia® Desktop server Deployment with Dedicated Servers on page 21

Figure 11: Typical Scopia® Desktop server setups based on size of deployment on page 26 illustrates typical deployments for small, medium, and large organizations. For details on the complete deployment, including other video infrastructure devices such as Avaya Scopia® PathFinder server, see *Solution Guide for Scopia® Solution*.

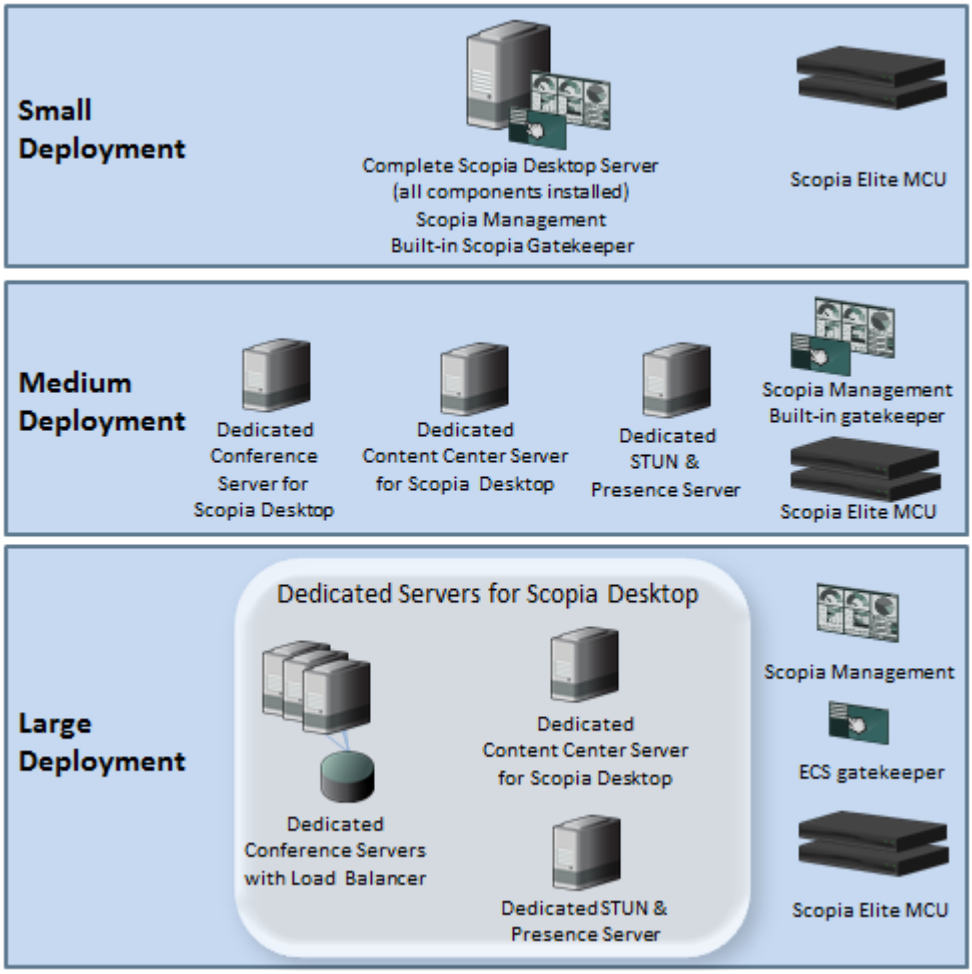


Figure 11: Typical Scopia® Desktop server setups based on size of deployment

Choose a Scopia® Desktop server deployment based on factors such as number of users and bandwidth efficiency. Refer to Table 4: Sizing your Scopia® Desktop server deployment on page 27 for details.

When sizing your deployment and planning the number of MCUs required, it is also important to consider the number of simultaneous users that are connecting in standard definition (SD) and high definition (HD). 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. For more information, see Calculating the Bandwidth Used by Avaya Scopia® Desktop Participants on page 30. For details on planning your MCU deployment and determining the number of simultaneous participants based on the video resolution, see *Installation Guide for Scopia® Elite MCU*.

Table 4: Sizing your Scopia® Desktop server deployment

Number of Simultaneous Participants	Deployment	Number of Scopia® Desktop servers	Bandwidth Considerations
Up to 100	Single all-in-one Scopia® Desktop server with Scopia® Management (small centralized deployment)	One To increase reliability, you can deploy a redundant server. To increase the number of users, you can deploy an additional Conference Server for Scopia® Desktop.	In centralized deployments, all calls are directed to the MCUs located in one place. This puts a strain on bandwidth if videoconferences involve many remote endpoints. For details on ensuring sufficient bandwidth for your deployment, and planning your bandwidth to suit your MCU capacity, see Estimating and Planning your Bandwidth Requirements on page 29.
Up to 250 per server	Dedicated Servers for medium organizations (large centralized deployment)	Typically two Conference Servers for Scopia® Desktop. One of these servers may include the Content Center Server.	
	Dedicated servers for service providers (large centralized deployment)	Typically three servers, depending on how the Scopia® Desktop components are allocated. Can be deployed as a cluster behind a load balancer.	
	Dedicated servers for service providers (distributed deployment)	One server or cluster in each location.	Distributed deployments save bandwidth in large videoconferences including many remote endpoints. However, smaller videoconferences might be unnecessarily cascaded between different MCUs and therefore use more bandwidth. For details on ensuring sufficient bandwidth for your deployment, and planning your bandwidth to suit your MCU capacity, see Estimating and Planning your Bandwidth Requirements on page 29.

You can store recordings locally on the Content Center Server or on any network server visible from the dedicated Content Center Server. Configure the location of recordings during the server installation (see *Installation Guide for Scopia® Desktop server*).

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)
```

Related Links

Planning your Topology for Scopia® Desktop server on page 16

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 12: Scopia® Desktop with a dual-NIC deployment on page 29). 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 Defining Scopia® Desktop server Public Address and Other Client Connection Settings on page 58.

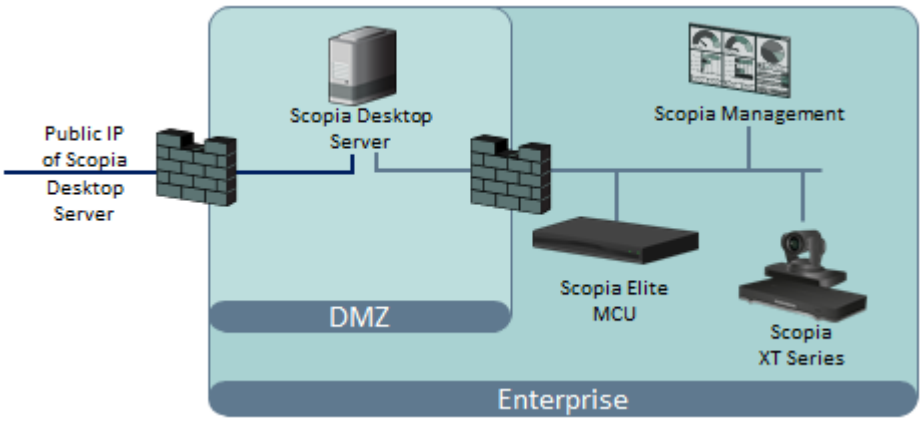


Figure 12: Scopia® Desktop with a dual-NIC deployment

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.

Related Links

Planning your Avaya Scopia® Desktop Deployment on page 13

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 13: 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 Scopia® Solution Guide.

Related Links

Planning your Avaya Scopia® Desktop Deployment on page 13
Calculating the Bandwidth Used by Avaya Scopia® Desktop Participants on page 30

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 Scopia® Management. You can also set the maximum bandwidth for guest users in Scopia® 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 Scopia® 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 14: Scopia® Management user profiles within maximum bandwidth set by Scopia® Desktop server on page 31).

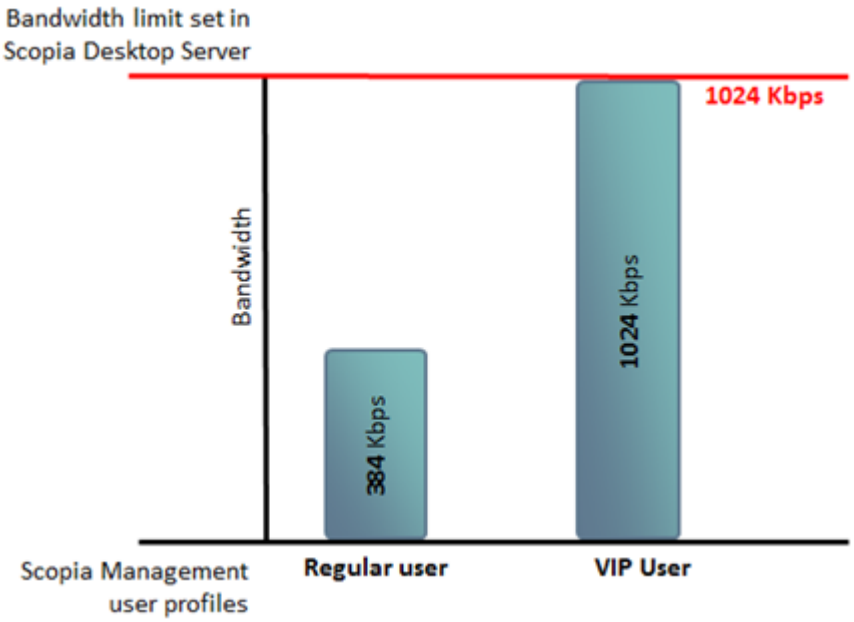


Figure 14: Scopia® Management user profiles within maximum bandwidth set by Scopia® Desktop server

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, as shown in Figure 15: External bandwidth required for centralized deployments on page 32:

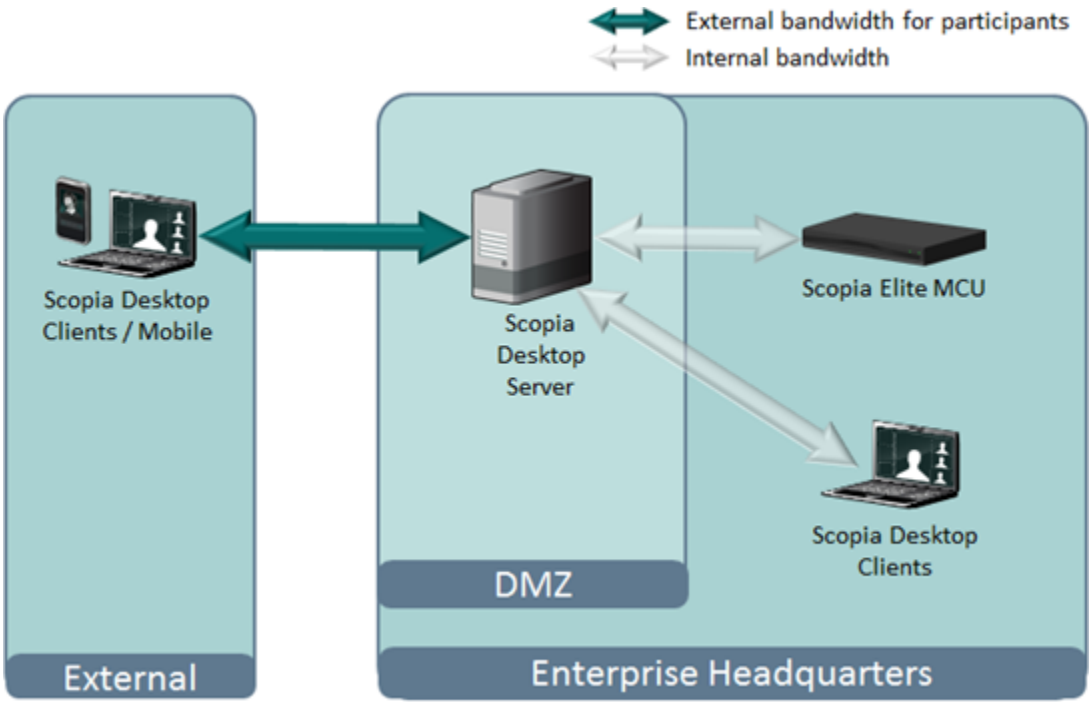


Figure 15: External bandwidth required for centralized deployments

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 16: External bandwidth required for distributed deployments on page 33:

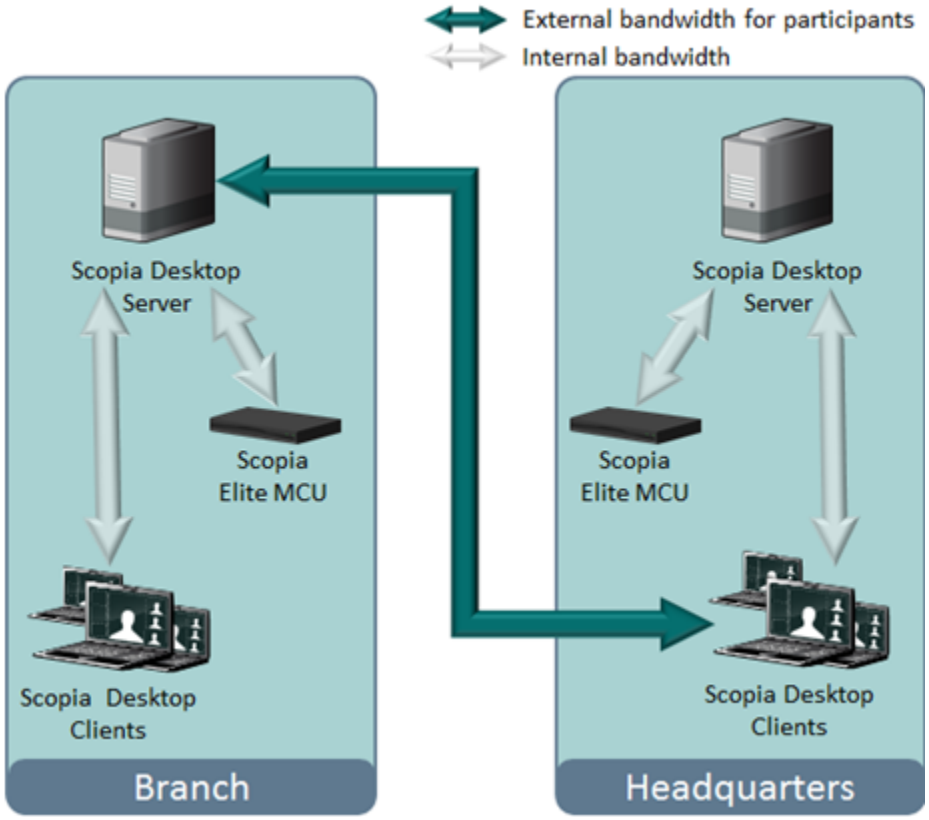


Figure 16: External bandwidth required for distributed deployments

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 31 and 2 on page 32.

   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 Series 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 17: Planning the maximum bandwidth based on MCU capacity on page 34.

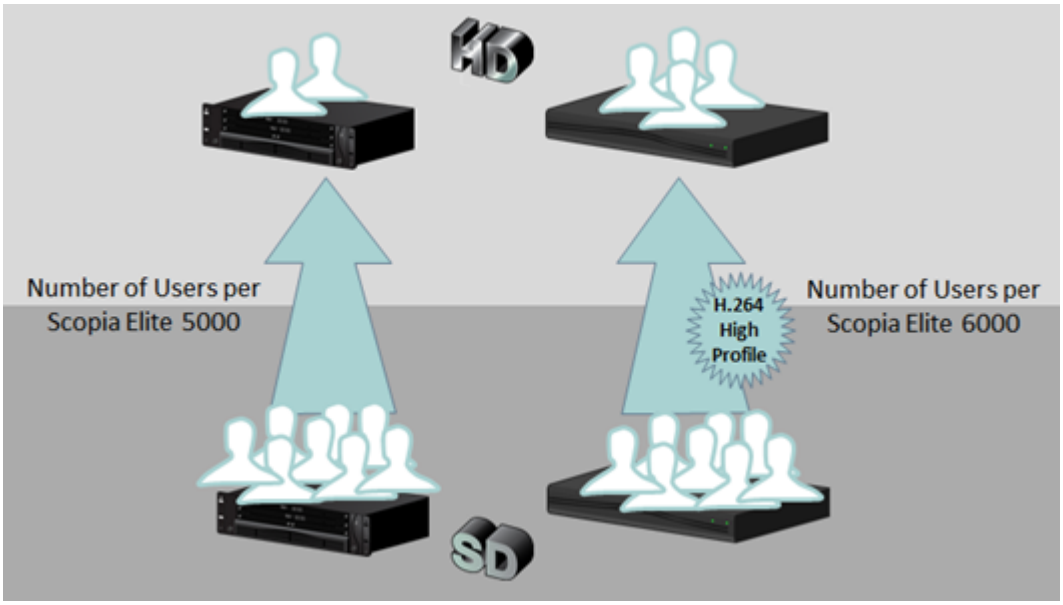


Figure 17: Planning the maximum bandwidth based on MCU capacity

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 Scopia® Solution:

   - The compression capabilities of the MCU and Avaya Scopia® Desktop

     The Scopia® Elite 6000 Series 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 5: Bandwidth and capacity requirements for each Scopia® Desktop Client on page 35 illustrates how the same resolution in the newer MCU model requires less bandwidth and fewer ports because of H.264 High Profile.

Table 5: Bandwidth and capacity requirements for each Scopia® Desktop Client

Video Resolution	Scopia® Elite 5000 Series MCU		Scopia® Elite 6000 Series 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, where a master MCU connects to one or more slave MCUs to create a single videoconference. It increases the meeting capacity by combining the resources of several MCUs. This can be especially useful for distributed deployments across several locations, reducing bandwidth usage.

You can configure Scopia® Management to determine whether your distributed MCUs form cascaded meetings. For more information, see *Administrator Guide for Scopia® Management*.

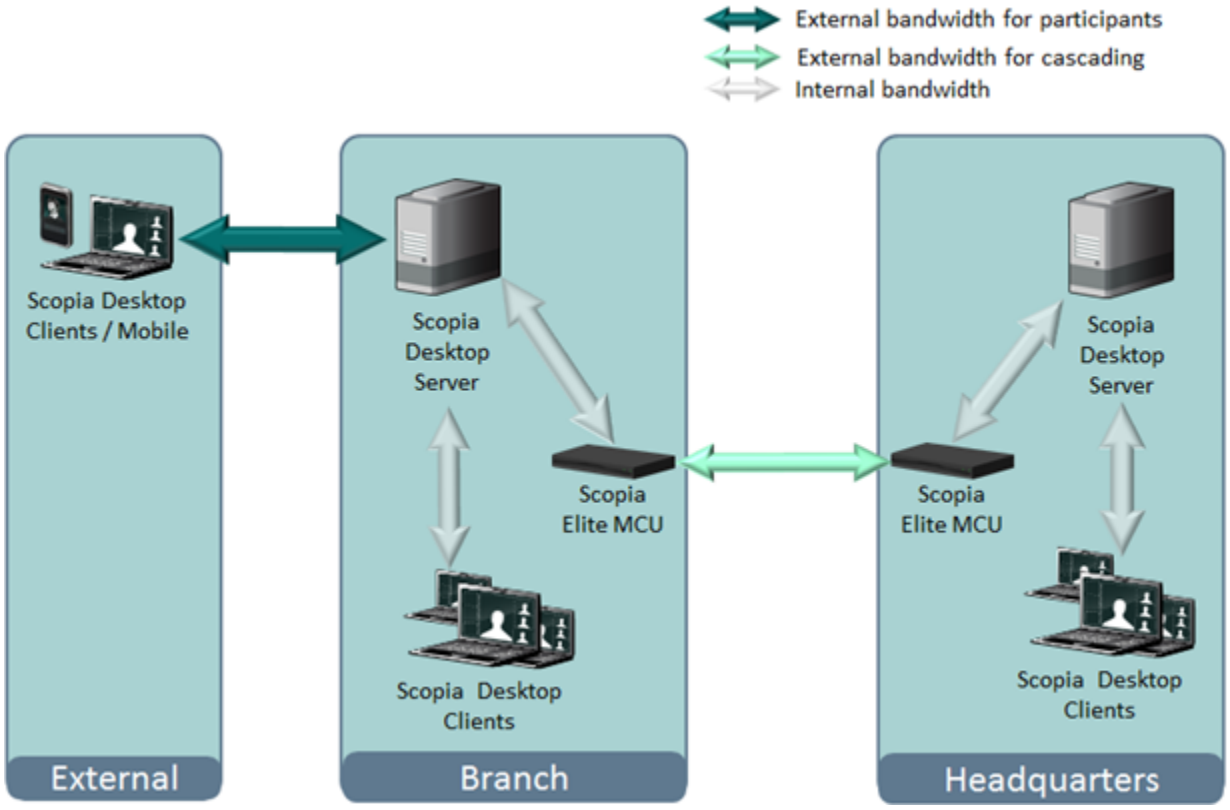


Figure 18: Using cascading to reduce bandwidth usage

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 Series MCU*.

- Setting bandwidth limits for Scopia® Desktop users.

  You can define different maximum bandwidth for Scopia® Desktop authenticated users and guests using Scopia® Management. The maximum bandwidth configured in Scopia® Management cannot exceed the maximum bandwidth configured on a Scopia® Desktop server to which the users connect. For more information see *Administrator Guide for Scopia® 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 29

Ports to Open on Scopia® Desktop

The Scopia® Desktop server is typically located in the DMZ (see Figure 19: Locating the Scopia® Desktop server in the DMZ on page 37) 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.

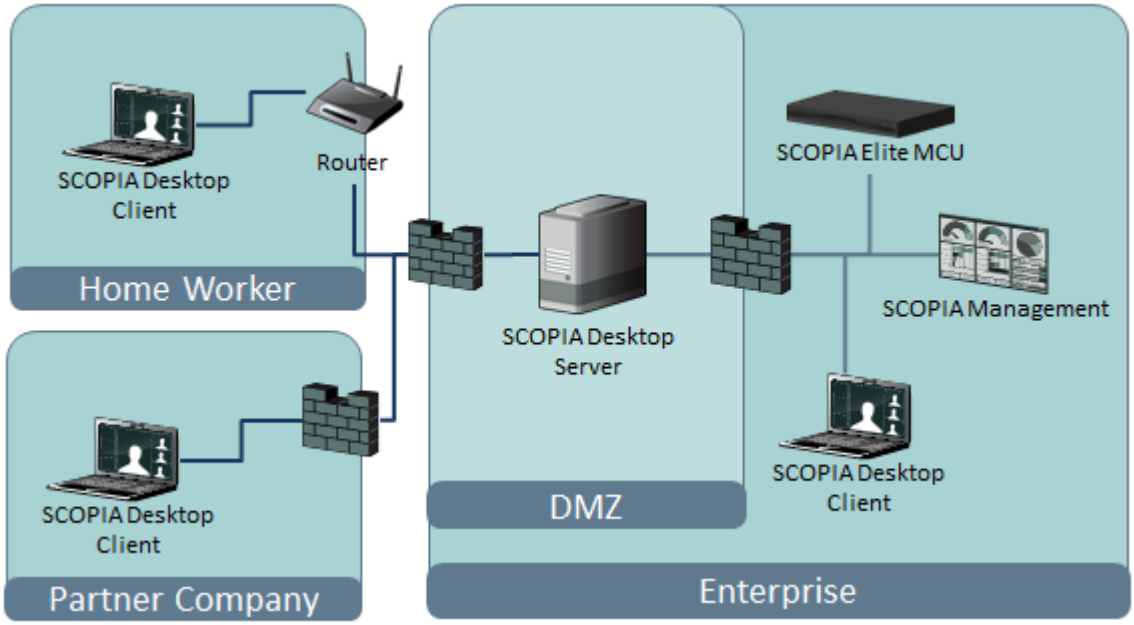


Figure 19: Locating the Scopia® Desktop server in the DMZ

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 6: Bidirectional Ports to Open Between the Scopia® Desktop server and the Enterprise on page 38.
- When opening ports that are outbound from the Scopia® Desktop server, see Table 7: Outbound Ports to Open from the Scopia® Desktop server to the Enterprise on page 39.
- When opening ports that are inbound to the Scopia® Desktop server, see Table 8: Inbound Ports to Open from the Enterprise to the Scopia® Desktop server on page 40.

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 9: Bidirectional Ports to Open Between the Scopia® Desktop server and the Public on page 40.
- When opening ports that are inbound from the Scopia® Desktop server, see Table 10: Inbound Ports to Open from the Public to the Scopia® Desktop server on page 41.

When opening bidirectional ports between Scopia® Desktop Clients, see Table 11: Bidirectional Ports to Open Between Scopia® Desktop Clients on page 41.

When opening inbound ports from the Scopia® Desktop Clients to the STUN server, see Table 12: Inbound Ports to Open from the Scopia® Desktop Client to the STUN Server on page 41.

Important:

The specific firewalls you need to open ports on depends on where your Scopia® Desktop and other Scopia® Solution products are deployed.

Table 6: 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 ECS, 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 43
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 port 443 resulting in a drop in performance.	Mandatory To limit range, see Limiting the UDP Port Range for RTP/RTCP on the Scopia® Desktop server on page 42

Table 7: 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)	Avaya Scopia® ECS Gatekeeper or the internal gatekeeper in Scopia® Management	Enables communication with Avaya Scopia® ECS Gatekeeper or the internal gatekeeper in Scopia® Management	Cannot connect to the meeting	Mandatory
1720	TCP	MCU or ECS, 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
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 8: 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 *Installation Guide for Scopia® Desktop server*.
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	Scopia® Management	Enables meeting control connection with Scopia® Management	Meeting control connection to Scopia® 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 BROKEN LINK: #unique_21

Table 9: 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 42

Table 10: 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 *Installation Guide for Scopia® Desktop server*.
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 Clients cannot connect to the Scopia® Desktop server	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 BROKEN LINK: #unique_21.

Table 11: 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 12: 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	Scopia® Desktop Client cannot connect to the STUN server and	Optional

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
			between two Scopia® Desktop Clients, open the UDP ports (10000-65535, 6972-65535, 3478).	uses the Scopia® Desktop server as a relay agent.	

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 BROKEN LINK: #unique_21.

Related Links

Planning your Avaya Scopia® Desktop Deployment on page 13
Limiting Port Ranges on the Scopia® Desktop server on page 42

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 Scopia® Desktop on page 37
Limiting the UDP Port Range for RTP/RTCP on the Scopia® Desktop server on page 42
Limiting the TCP Port Range for H.245/Q.931 on the Scopia® Desktop server on page 43

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.

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 20: Multimedia Ports Area on page 43).

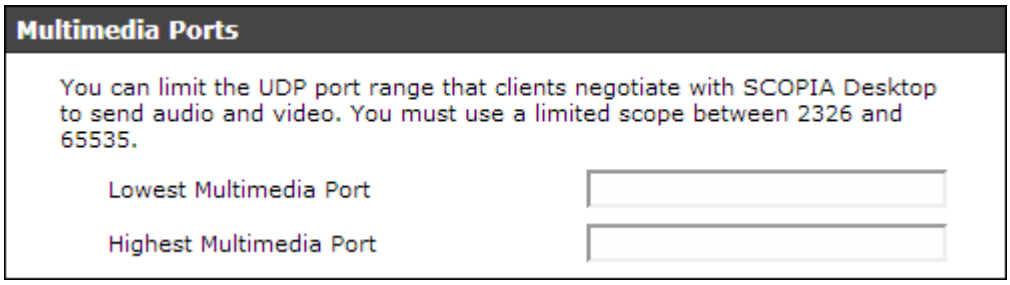


Figure 20: Multimedia Ports Area

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 42

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 42

Chapter 3: Configuring Core Features of Scopia® Desktop server

You can quickly configure the Scopia® Desktop server for initial use during the installation of the product, which defines all the server's settings with their default values.

This section details how to change the default settings of the core server features.

Related Links

Accessing the Scopia® Desktop server Web Administration Interface on page 45
Defining a Local Administrator Account on page 46
Connecting Scopia® Desktop server with Video Network Devices on page 47
Verifying Scopia® Desktop server Installation and Connection with Other Components on page 49
Adding and Modifying Scopia® Desktop server in Avaya Scopia® Management on page 52
Enabling Scopia® Desktop Registered Users in Scopia® Management on page 54
Defining Bandwidth Settings in Scopia® Desktop server on page 57
Defining Scopia® Desktop server Public Address and Other Client Connection Settings on page 58
Enabling Scopia® Desktop Client Features on page 60
Rolling-Out Scopia® Desktop Client to End Users on page 63

Accessing the Scopia® Desktop server Web Administration Interface

About this task

The Scopia® Desktop server web administration interface is a web-based application to configure the settings of your Scopia® Desktop server.

Perform this procedure to access the administration web interface.

Important:

In a service provider (multi-tenant) deployment the tenant's organization administrator cannot be granted access to the administration web interface.

Procedure

1. Access the Scopia® Desktop server Administration web interface in a browser at *http://<server_name>/scopia/admin*

   where *<server_name>* is the FQDN of your Scopia® Desktop server. If you have deployed a non-standard port to access the Scopia® Desktop server, enter the port number in the standard way: *<server_name>:<port_number>*. If you have implemented secure access to the server, use the *https://* prefix.

2. Enter your username and password.

   The default username is **admin** and the password is **admin**.

3. Select **Sign In**.

Related Links

Configuring Core Features of Scopia® Desktop server on page 45

Defining a Local Administrator Account

About this task

You can define a username and password for a local administrator to access Scopia® Desktop server Administration web interface. The local administrator cannot sign into the Scopia® Desktop user portal using credentials defined during this procedure.

In point-to-point-only and advanced deployments where the authentication option is enabled in Scopia® Management, Scopia® Management administrators can access the Scopia® Desktop Administration web interface.

Procedure

1. Select **Directory and Authentication** in the sidebar.

   The **Settings** tab is displayed.

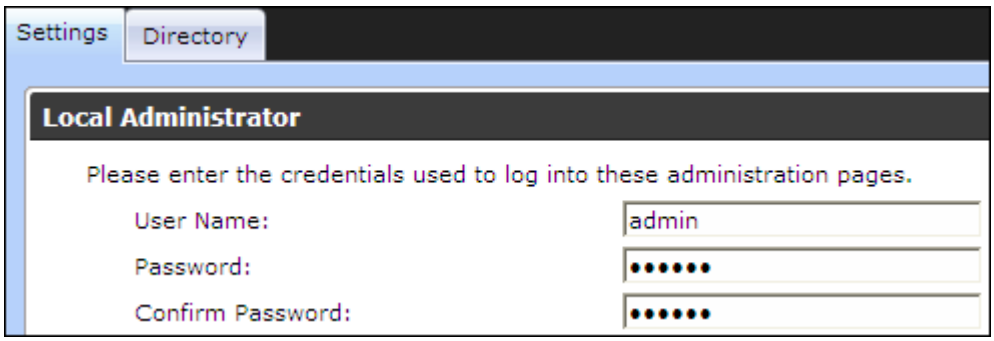


Figure 21: Configuring the local administrator credentials

2. Enter a **User Name** and **Password** in the **Local Administrator** section.
3. Select **OK**.

Related Links

Configuring Core Features of Scopia® Desktop server on page 45

Connecting Scopia® Desktop server with Video Network Devices

About this task

This section describes how to connect Scopia® Desktop server with the following servers in your video network:

- Avaya Scopia® Management which manages this Scopia® Desktop server
- A gatekeeper like Avaya Scopia® Gatekeeper (built-in to Scopia® Management) or Avaya Scopia® ECS Gatekeeper
- A dedicated Recording Server for Scopia® Desktop
- A dedicated Streaming Server for Scopia® Desktop

This window is also displayed when you access the Scopia® Desktop server for the first time.

Ensure that Scopia® Desktop server has Scopia® Management's IP address, and conversely Scopia® Management has Scopia® Desktop server's IP address. For more information on how to add Scopia® Desktop server's IP address to Scopia® Management, see Adding and Modifying Scopia® Desktop server in Avaya Scopia® Management on page 52.

To connect your Scopia® Desktop server to Microsoft Outlook, install the Scopia® Add-in for Microsoft Outlook. For more information, see the *User Guide for Scopia® Add-in for Microsoft Outlook*. To connect Scopia® Desktop server to IBM Sametime, install the Scopia® Connector. For more information, see the *Installation Guide for Scopia® Connector for IBM Sametime*.

Procedure

1. Access the Scopia® Desktop server administration web interface.
2. Select **Deployment** in the sidebar.
3. Enter the fields as described in Table 13: Defining addresses of other servers in the network on page 48.

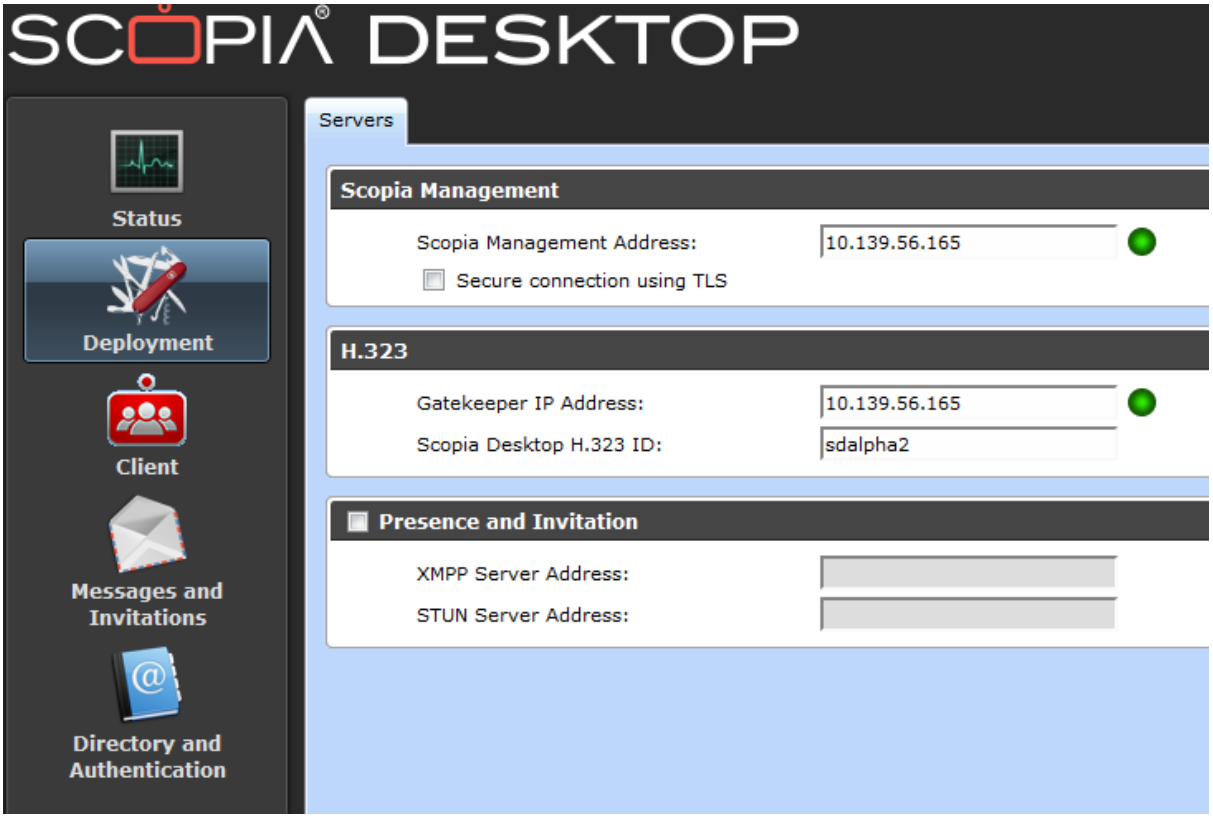


Figure 22: Connections to other servers including Scopia® Management

Table 13: Defining addresses of other servers in the network

Field	Description
Scopia® Management	Enter the IP address of Scopia® Management, for integrated user management, bandwidth policies, and stronger integration with the full range of Scopia® Solution features. By default, Scopia® Management uses port 8080.
Secure connection using TLS	Select this check box to encrypt communications between Scopia® Desktop server and Scopia® Management. This functionality requires installing certificates signed by a recognized CA on both Scopia® Management and Scopia® Desktop server. For more information on installing Scopia® Management certificates, see *Administrator Guide for Scopia® Management*. For more information on installing certificates on Scopia® Desktop server, see Adding and Modifying Scopia® Desktop server in Avaya Scopia® Management on page 52.

Table continues…

Field	Description
	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.
Gatekeeper IP Address	Enter the address of the gatekeeper. If you are using Scopia® Management's built-in gatekeeper, enter the IP address of Scopia® Management.
Scopia® Desktop H.323 ID	Enter the name (H.323 alias) which Scopia® Management uses to identify this Scopia® Desktop server's clients, and then route them to the appropriate MCU. This can have any of the following formats: • H.323 alias. For example, `username`. • IP address of an H.323 endpoint. For example, *10.133.184.195*. • URI dialing for H.323 or SIP endpoints. For example, *user@company.com* • E.164 dialing for H.323 or SIP endpoints. For example, *881234*. **Note:** In a deployment with multiple Scopia® Desktop servers, ensure that each Scopia® Desktop server has a unique alias.
Presence and Invitation	Select this check box if your deployment includes a presence and STUN server, used to maintain the contact list and point-to-point functionality of Scopia® Desktop Pro.
XMPP Server Address	Enter the IP address of the presence server, used to maintain the presence information of the contact list in Scopia® Desktop Pro.
STUN Server Address	Enter the IP address of the STUN server, used to ensure a point-to-point call can be made from a remote Scopia® Desktop Client to one inside the organization, finding the correct address via the firewall.

Related Links

Configuring Core Features of Scopia® Desktop server on page 45

Verifying Scopia® Desktop server Installation and Connection with Other Components

About this task

The Scopia® Desktop Administrator web interface displays the connectivity status of your deployment. The indicators next to each link shows whether or not the connection or registration to the target server is successful. When the indicator is red, hover over the indicator to view the tooltip containing the error details.

Configuration options which do not apply to your deployment are not displayed.

Procedure

1. To verify that Scopia® Desktop Server is connected to the necessary video network devices, select **Status** in the sidebar.
2. View the connection status for each server or component. If necessary, select any red indicators to view further error information.

Figure 23: Viewing the connection status with Scopia® Desktop server

3. In a service provider (multi-tenant) deployment, select the **Directory** tab, and select the organization whose policies you want to check.

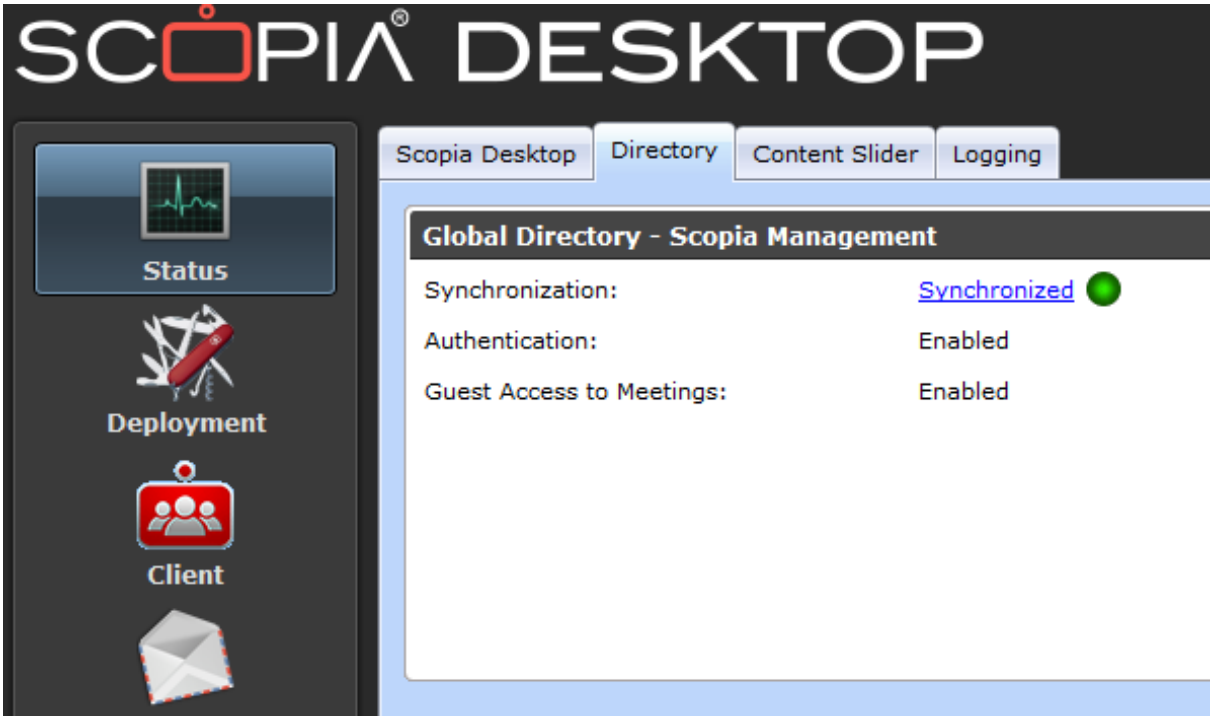


Figure 24: Viewing an organization's status in a multi-tenant deployment

4. For Scopia® Management deployments, Scopia® Desktop server must synchronize with Scopia® Management to download information about users, virtual rooms, and global policy. Select the **Directory** tab and verify synchronization with Scopia® Management.

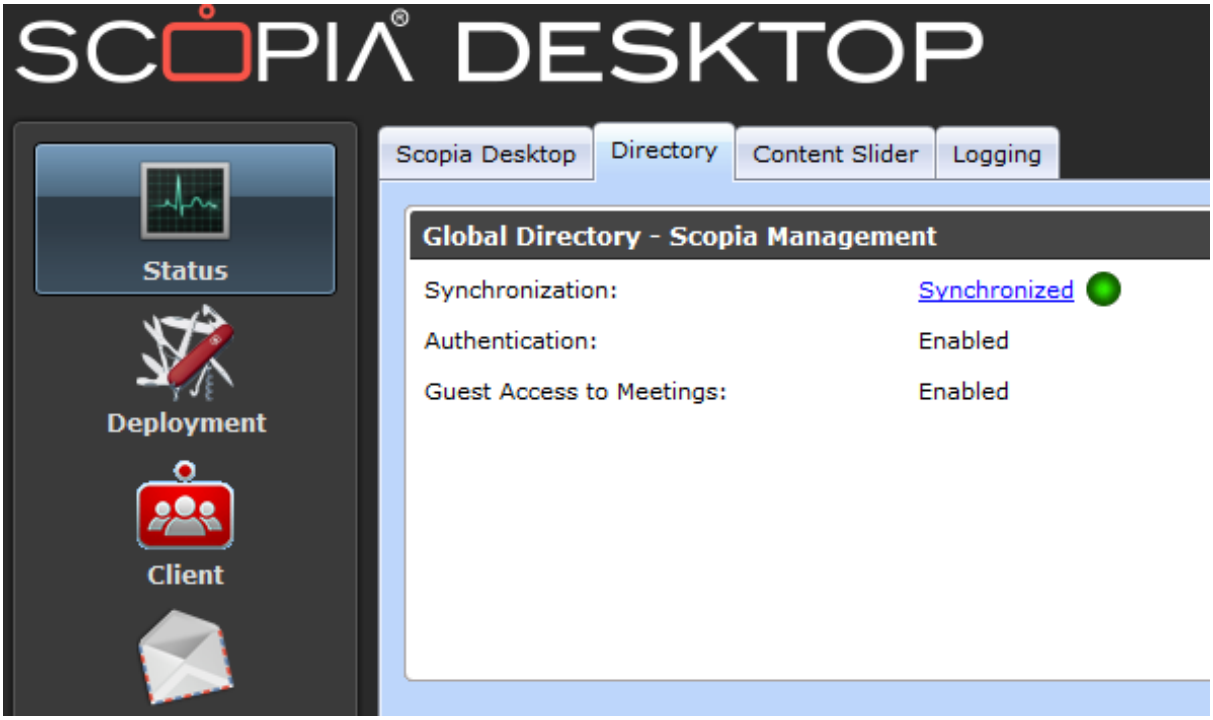


Figure 25: Status of LDAP synchronization

5. **(Optional)** View the connection status of the Scopia® Content Slider by selecting the **Content Slider** tab. For more information on the Content Slider, see About Components of the Scopia® Desktop server on page 9.
6. If necessary, select any red indicators to view further error information.

Related Links

Configuring Core Features of Scopia® Desktop server on page 45

Adding and Modifying Scopia® Desktop server in Avaya Scopia® Management

About this task

The Scopia® Desktop server uses Scopia® Management to retrieve the list of users from the corporate directory, and also query information about current and scheduled meetings, including the participant names in a meeting. Scopia® Desktop server profiles are manually added to Scopia® Management.

Ensure that Scopia® Desktop server has Scopia® Management's IP address, and conversely Scopia® Management has Scopia® Desktop server's IP address. For more information on how to add Scopia® Management's IP address to the Scopia® Desktop server, see Connecting Scopia® Desktop server with Video Network Devices on page 47.

Procedure

1. Access the Scopia® Management administrator portal.
2. In the **Devices** tab, select **Desktop Servers**.
3. Select the link in the **Name** column for the Scopia® Desktop server you require, or select **Add** to create a new Scopia® Desktop server profile. The **Add Scopia® Desktop server** page appears (Figure 26: Adding a Scopia® Desktop profile on page 53).

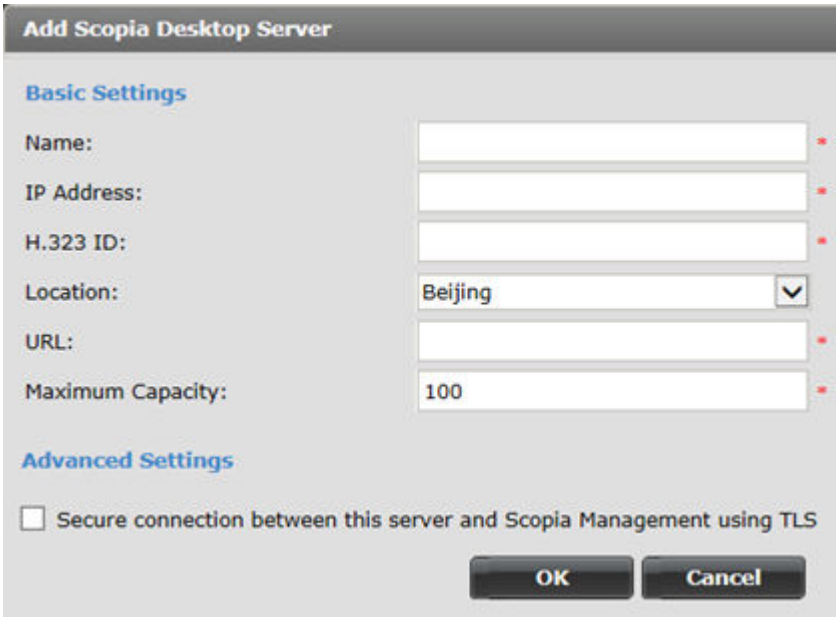


Figure 26: Adding a Scopia® Desktop profile

4. Enter the required information (Table 14: Configuring Scopia® Desktop server on page 53).

Table 14: Configuring Scopia® Desktop server

Field Name	Description
Name	Enter a name to identify this Scopia® Desktop server. This name is displayed in the list of Scopia® Desktop servers.
IP address	Enter the management IP address of Scopia® Desktop server.
H.323 ID	Enter the H.323 ID used to identify connections from Scopia® Desktop server in MCU conferences. This must match the H.323 ID that is configured in the Scopia® Desktop administrator web interface. Configuring this field allows Scopia® Management to route calls from this Scopia® Desktop server based on the predefined IP topology. The ID can have one of the following formats: • H.323 alias. For example, `username`. • IP address of an H.323 endpoint. For example, *10.133.184.195*.

Table continues…

Field Name	Description
	• URI dialing for H.323 or SIP endpoints. For example, *user@company.com* • E.164 dialing for H.323 or SIP endpoints. For example, *881234*. **Note:** In a deployment with multiple Scopia® Desktop servers, ensure that each Scopia® Desktop server has a unique alias.
Location	This is only relevant for service providers or deployments with multiple locations. Select the Scopia® Desktop server's location.
URL	Enter the URL used to access the Scopia® Desktop server. The URL must be in the format *http://<web URL>:<port number>/scopia*.
Maximum Capacity	Enter the maximum number of simultaneous connections you want to allow for your Scopia® Desktop server, based on computing power.
Secure connection between this server and Scopia® Management using TLS	To use the Transport Layer Security (TLS) protocol to secure the transport link between Scopia® Management and Scopia® Desktop, select this checkbox. For more information, see *Administrator Guide for Scopia® Management*.

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

Related Links

Configuring Core Features of Scopia® Desktop server on page 45

Enabling Scopia® Desktop Registered Users in Scopia® Management

About this task

When Scopia® Desktop server is managed by Scopia® Management, you must enable the functionality of registered Scopia® Desktop users in Scopia® Management. Registered users can login to the Scopia® Desktop Web Portal and have access to their own virtual room.

Depending on the privileges granted to different user groups in Scopia® Management, registered Scopia® Desktop users can access meetings, record meetings, watch recordings and webcasts, and invite new participants to meetings.

Assign licenses to groups of users via their user profile in Scopia® Management. For more information on defining user profiles, see *Administrator Guide for Scopia® Management*. This procedure includes how to customize the profile for a single user to add a license.

Before you begin

If you intend to use Scopia® Management authentication in point-to-point deployments, ensure you have a Scopia® Desktop Pro license. By default, Scopia® Management is installed with an evaluation license for five users.

Procedure

1. Access the Scopia® Desktop server Administrator web user interface.
2. Verify that the Scopia® Desktop server is connected to Scopia® Management:
   a. Select the **Status** icon in the sidebar.
   b. Verify the Scopia® Desktop server and Scopia® Management connection status in the Scopia® Desktop Components section.

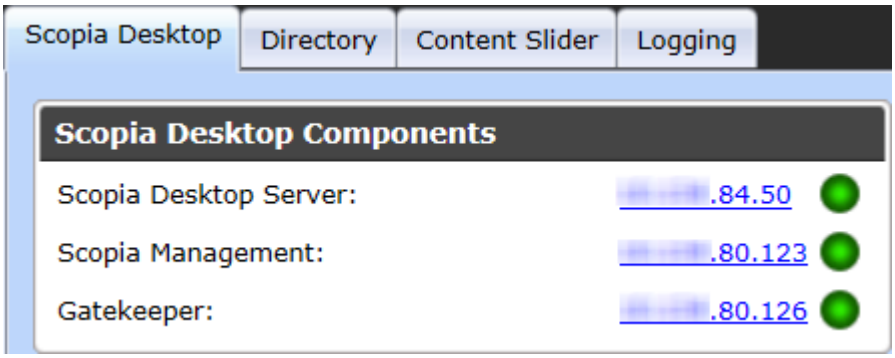


Figure 27: Verifying the Scopia® Management connection in Scopia® Desktop server

3. In Scopia® Management, verify that the Scopia® Desktop server is added as a connected server:
   a. Access the Scopia® Management web administrator portal.
   b. Select the **Devices** tab.

Figure 28: Verifying the Scopia® Desktop server connection in Scopia® Management

   c. Verify that the required Scopia® Desktop server appears in the table of connected servers.

4. Enable user authentication for Scopia® Desktop:
   a. Login to Scopia® Management.
   b. Select the **Settings** tab and navigate to **Users** > **Policies** in the sidebar menu.
   c. Select the **Allow Scopia® Desktop user authentication** check box.

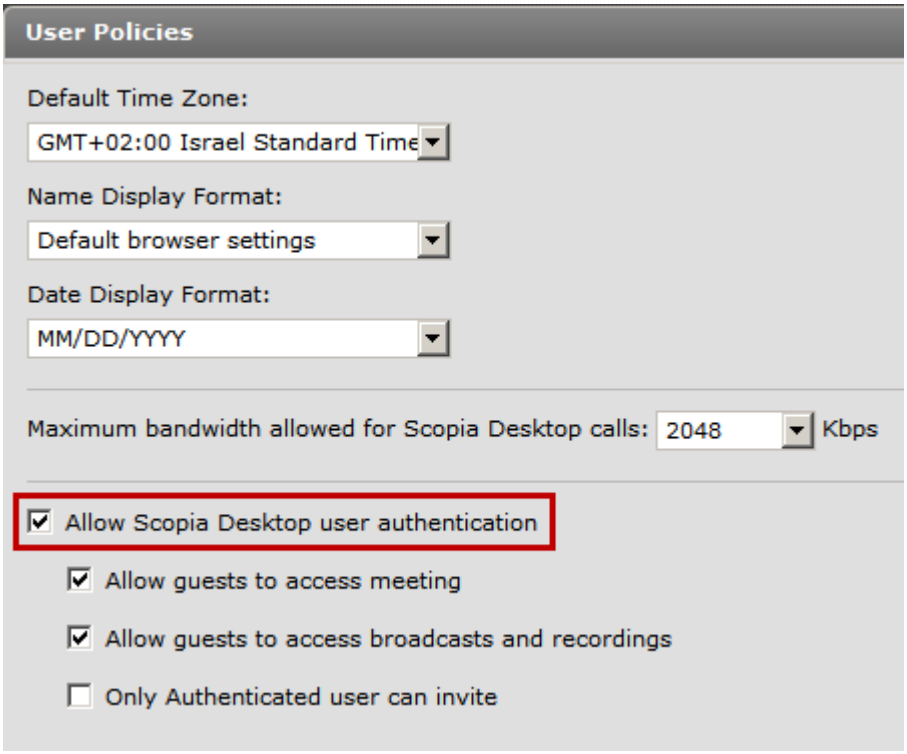


Figure 29: Enabling registered users in Scopia® Desktop

   d. Select authorization options for unregistered users (known as guests) as required. You can enable the following features for guests in your deployment:
      - Access meetings without logging in to Scopia® Desktop server
      - Access broadcasts and recordings without logging in to Scopia® Desktop server
      - Invite participants to a videoconference without logging in to Scopia® Desktop server.
5. Select **Servers** > **LDAP Servers** in the sidebar menu, and verify the type of directory to which Scopia® Management connects for user authentication using LDAP as an authentication method:
   - Internal Directory
   - Microsoft Active Directory
   - IBM Lotus Domino

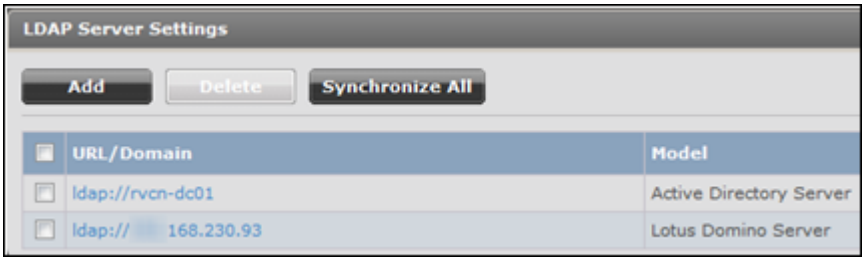


Figure 30: Examples of user directory server listed in Scopia® Management

Related Links

Configuring Core Features of Scopia® Desktop server on page 45

Defining Bandwidth Settings in Scopia® Desktop server

About this task

This section details how to define the maximum bandwidth used between the Scopia® Desktop Client and the Scopia® Desktop server. Calculating the Bandwidth Used by Avaya Scopia® Desktop Participants on page 30 explains how to assess the maximum bandwidth per Scopia® Desktop Client.

This value determines the maximum bandwidth used by a Scopia® Desktop participant uploading and downloading media during a videoconference. A webcast viewer uses half of this bandwidth because media is only downloaded from the Scopia® Desktop server when a videoconference is streamed.

Maximum bandwidth is also defined in the MCU meeting type (service). You invoke a meeting type by entering its prefix before the meeting ID. For example, if 88 is the dial prefix defined MCU meeting type for HD meetings, users would enter 88 followed by the meeting ID to invoke that meeting type's parameters in the videoconference.

The bandwidth values defined here are subordinate to the bandwidth restrictions defined in the MCU meeting type.

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.

Before you begin

Decide on the maximum bandwidth per Scopia® Desktop Client as explained in Calculating the Bandwidth Used by Avaya Scopia® Desktop Participants on page 30.

Procedure

1. Access the Scopia® Desktop server Administration web interface.
2. Select the **Client** icon in the sidebar.
3. Select the **Settings** tab.

4. Select the maximum call rate in the **Maximum Video Quality** section.

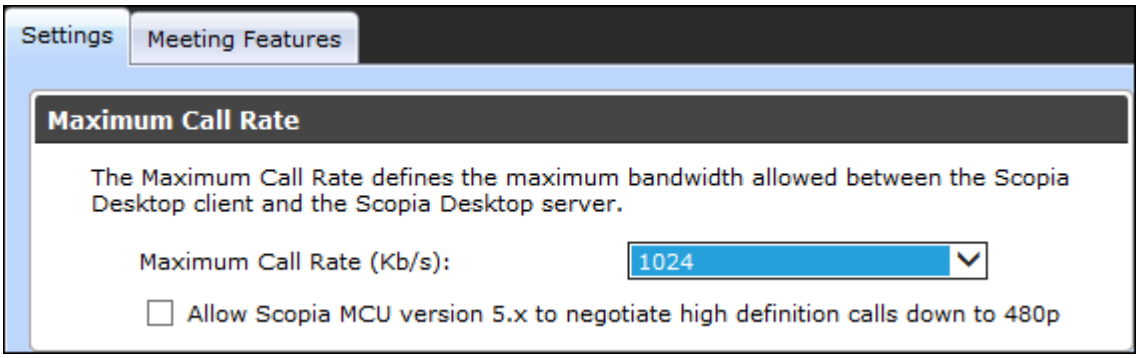


Figure 31: Maximum Call Rate Section

Important:

The actual bandwidth consumed for a specific video resolution depends on the compression capabilities of your MCU. For example, Scopia® Elite 6000 Series MCU includes H.264 High Profile encoding, therefore allowing a higher resolution at a lower bitrate than other MCUs. .

Related Links

Configuring Core Features of Scopia® Desktop server on page 45

Defining Scopia® Desktop server Public Address and Other Client Connection Settings

About this task

This section details how to define the public address of the Scopia® Desktop server, which is pushed to Scopia® Desktop Clients participating in a videoconference on that server.

You can also define Scopia® Desktop server's size of network packets (MTU size). The MTU, or Maximum Transmission Unit, is the maximum size of data packets sent around your network.

Furthermore, you can place arbitrary limits for the number of clients which can simultaneously connect to this server, in cases where the server's specifications are not powerful enough to manage the maximum number of connections.

Procedure

1. Access the Scopia® Desktop server Administration web interface.
2. Select the **Client** icon in the sidebar.
3. Select the **Settings** tab.
4. Insert the public address of the Scopia® Desktop server to be accessed by the client. Use a FQDN which Scopia® Desktop Clients can resolve from their location, to arrive at the correct IP address of the server.

If a DNS name is not specified in the **Public Address** field, the Scopia® Desktop server network interface address is used.

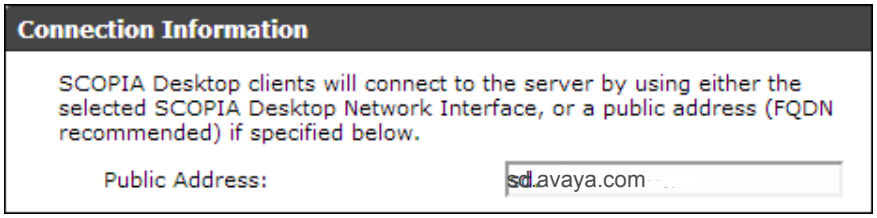


Figure 32: The public address for Scopia® Desktop Clients to connect to the server

If your deployment uses dedicated servers for one or more Scopia® Desktop server components, Scopia® Desktop Clients would connect via this public address if those dedicated servers cannot be reached due to NAT or firewall restrictions.

5. Define the **MTU Size** if your network routers and the MCU are configured to accept network packets of a different size. The default value is **1360**.

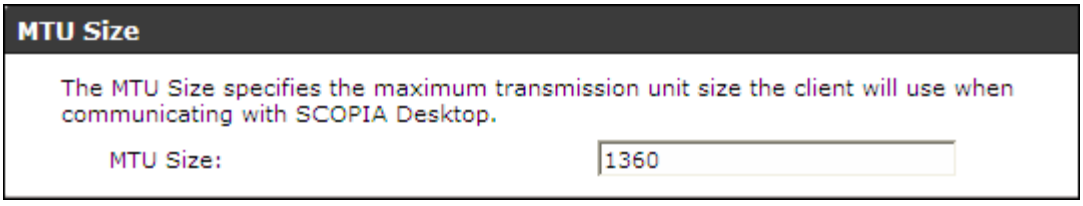


Figure 33: Setting the MTU size for Scopia® Desktop Client

Important:

This value must remain the same across all network components to guard against packet fragmentation.

6. Enter a value in the **Call Limit** field to limit the resources used by the system. Use this to limit bandwidth or when the Scopia® Desktop server computer is not powerful enough to support the maximum number of calls.

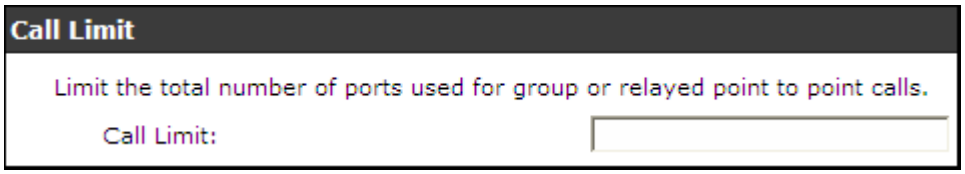


Figure 34: Call Limit Section

7. Select **OK** or **Apply**.

Related Links

Configuring Core Features of Scopia® Desktop server on page 45

Enabling Scopia® Desktop Client Features

About this task

This section describes how to enable or disable features in the **Virtual Room** window of the Scopia® Desktop Client for all users logged in to the Scopia® Desktop server. You can:

- Enable or disable presentations (desktop sharing).
- Enable or disable Scopia® Content Slider.
- Enable or disable text chat.
- Enable or disable raising hand feature in lecture mode.
- Enable or disable encryption.

  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.
- Enable or disable call back for users who have an H.323 endpoint but also want to connect a dedicated PC to share presentations.
- Add a pane in the videoconferencing window containing web content for all users in your organization.

Users with a login to Scopia® Desktop server can define their own virtual room preferences in the Scopia® Desktop Client (see *User Guide for Scopia® Desktop Client*).

Users with a Scopia® Management login can define the behavior of their virtual rooms in Scopia® Management (see *User Guide for Scopia® Management*).

The changes you make in this procedure are global and affect all Scopia® Desktop Clients connecting to this Scopia® Desktop server.

You can decide to encrypt the media sent over UDP between the Scopia® Desktop server and Scopia® Desktop Client/Scopia® Mobile. For more information about encryption see Encrypting Media over UDP between Scopia® Desktop server and Scopia® Desktop Client on page 93.

Procedure

1. Access the Scopia® Desktop server Administrator web user interface.
2. Select the **Client** icon in the sidebar.
3. Select the **Meeting Features** tab.

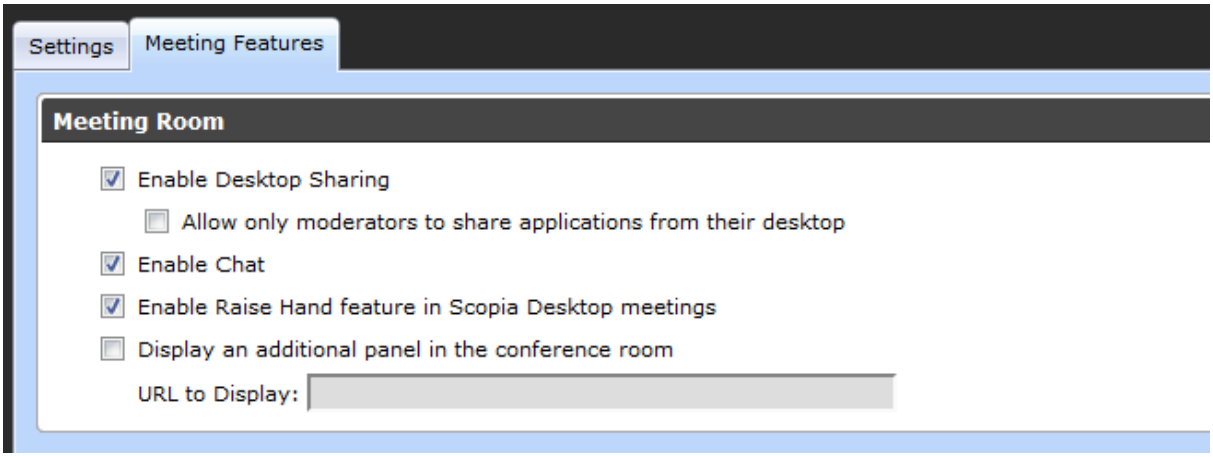


Figure 35: Enabling or disabling client videoconferencing features

4. Enter the fields as described in Table 15: Settings for the Scopia® Desktop Client Virtual Room window on page 61.

Table 15: Settings for the Scopia® Desktop Client Virtual Room window

Field	Description
Enable Desktop Sharing	Determines whether participants can share their PC desktop content with others in the videoconference. If desktop sharing disabled, the **Present** button does not appear in the **Virtual Room** window of Scopia® Desktop Client.
Enable Content Slider feature in Scopia® Desktop meetings	Determines whether participants can review content which has already been shared in the meeting by scrolling back and forth.
Allow only moderators to share applications from their desktop	Determines whether this feature is restricted to moderators of videoconferences only.
Enable Chat	Determines whether to display the chat window pane in the **Virtual Room** window of Scopia® Desktop Client.
Enable Raise Hand feature in Scopia® Desktop meetings	Determines whether a muted user (usually in lecture mode) can request permission to speak.
Display an additional panel in the conference room	Determines whether to display an additional pane in Scopia® Desktop Client's **Virtual Room** window within your organization. The pane's contents are drawn from an external web address.
URL to Display	Enter the web address in this field. When the system accesses the web address, it automatically appends two parameters: the current meeting ID and the participant's nickname. This enables your external web content to relate to the meeting and participant if required. The parameters added are: `?meetingid=NNN&nickname=XXX`. If your external web content already takes

Table continues…

Field	Description
	different parameters in its URL, these parameters are appended to the URL string. Use standard URL-encoding in this field, for example '&' is %26, '=' is %3D and so on.

5. Configure the **Push to Talk** section to define how participants use the microphone button in the **Virtual Room** window of Scopia® Desktop Client.

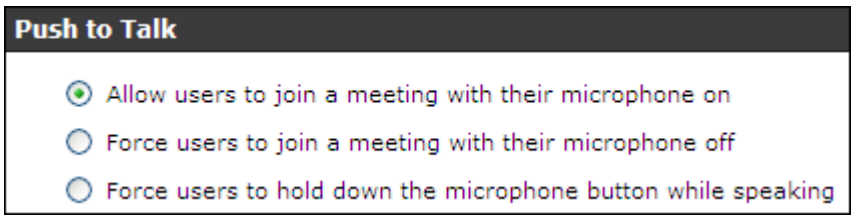


Figure 36: Push to Talk Settings

Enter the fields as described in Table 16: Defining microphone behavior during a meeting on page 62.

Table 16: Defining microphone behavior during a meeting

Field	Description
Allow users to join a meeting with their microphone on	When selected, this field enables the microphone by default, so participants must select the microphone button to mute themselves.
Force users to join a meeting with their microphone off	(Recommended) When selected, this field disables the microphone by default, so participants must select the microphone button to unmute themselves. This is eliminates background noise from a videoconference until the participant is ready to contribute.
Force users to hold down their microphone button while speaking	When selected, this field requires participants to select and hold down the microphone button to activate their microphones and send their audio.

6. Select **Encrypt Media** to encrypt audio and video over UDP between Scopia® Desktop server and Scopia® Desktop Client.

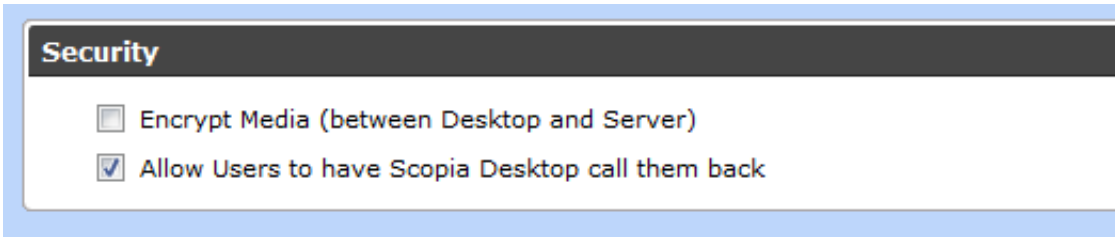


Figure 37: Security Settings

7. Select **Allow Users to have Scopia® Desktop call them back**. When users with a dedicated videoconferencing endpoint connect their PC to the meeting for data sharing only,

this field determines whether the system displays the check box for the system to call back their H.323 device to connect video from there.

The check box is located on the Scopia® Desktop web portal. Before connecting to a meeting, select **More Options** > **Use my computer for presentation only** > **Callback my video device number**.

Important:

When a computer connects as a dedicated data-only device, it cannot view or send video or audio, but you can view the participant list, moderate, chat, share content from the computer.

8. Select **OK** or **Apply**.

Related Links

Configuring Core Features of Scopia® Desktop server on page 45

Rolling-Out Scopia® Desktop Client to End Users

About this task

This section provides the recommended procedures for rolling-out your deployment to end users.

The section includes these topics:

Related Links

Configuring Core Features of Scopia® Desktop server on page 45
Minimum Requirements for Scopia® Desktop Client on page 63
Installing Scopia® Desktop Client Locally on a PC on page 65
Centrally Deploying Scopia® Desktop Clients in your Organization on page 67

Minimum Requirements for Scopia® Desktop Client

This section details the minimum hardware and software requirements of the Scopia® Desktop Client.

The minimum hardware requirements for the Scopia® Desktop Client depend on the video resolution.

- Standard definition hardware specifications:
  - PC Intel Pentium 4, 3.0 GHz or faster
  - PC AMD Athlon 3.0 GHz or faster
  - PC Intel Centrino Mobile Processor 1.8 GHz or faster
  - Mac with Intel Core Duo 1.8 GHz or faster
  - Netbook Intel Atom Processor 1.6 GHz or faster

- 1GB of RAM or more

- Enhanced definition hardware specifications:
  - PC Intel true dual core processors - Core 2 Duo 1.8 GHz or faster
  - PC AMD true dual core processors - e.g. Phenom IIx4 91- 2.X GHz or faster
  - Minimum 2GB of RAM
- High definition hardware specifications:
  - Intel PC architecture
    - 2nd Generation Intel® Core™ i3, i5 or i7 processors (Sandy Bridge) or newer

      Or
    - Any Intel generation with quad-core processors
    - i5 or i7 recommended
  - PC AMD Quad-Core Opteron
  - Mac with Intel Core 2 Duo 2.7 GHz or faster
  - Minimum 2GB of RAM, 3GB of RAM or more recommended

The minimum software requirements of the Scopia® Desktop Client are:

- Operating systems:
  - Windows XP (SP3, 32 and 64-bit)
  - Windows Vista (SP2 or higher, 32 and 64-bit)
  - Windows 7 (32 and 64-bit)
  - Windows 8 and 8.1 (desktop mode, 32 and 64-bit)
  - Windows 10 (32 and 64 bit)
  - Mac OS X version 10.7 (Lion) or higher, Intel CPU only

  We recommend using the latest service pack of the Windows operating systems listed in this section.
- Internet browsers:

  Scopia® Desktop is tested with the latest internet browser versions available at the time of release.

  Important:

  Internet Explorer must be installed on your Windows PC when using the Scopia® Desktop Client, even if you access meeting with other web browsers like Firefox or Chrome.

  - Google Chrome (version 30 and later)
  - Internet Explorer (version 8 and later, for windows)
  - Firefox (version 25 and later)

- Safari (version 5 and later)

- Viewing live webcasts or recorded meetings
  - Mac: QuickTime 7.4.5 or later (version 7.7 recommended)
  - PC: QuickTime 7.4.5 minimum (version 7.7 recommended)

Important:

QuickTime 10 is not supported.

Related Links

Rolling-Out Scopia® Desktop Client to End Users on page 63

Installing Scopia® Desktop Client Locally on a PC

About this task

The Scopia® Desktop Client web portal provides an automatic download and update manager. When you select the **Updates** link, it displays any currently installed components and versions, and enables you to install components, including Scopia® Add-in for Microsoft Outlook and the Contact List.

Important:

You must be logged in to the web portal to install all components at once. If you are not logged in, you can only install the client, not the Contact List or the Scopia® Add-in for Microsoft Outlook. These components are reserved for users who are authenticated to access corporate systems for scheduling and making calls.

For information about installing the 64 bit version of Scopia® Add-in for Microsoft Outlook, refer to *User Guide for Scopia® Add-in for Microsoft Outlook*.

In a service provider (multi-tenant) deployment the Contact List and the Scopia® Add-in for Microsoft Outlook are configured on installation with organization-specific URLs.

Before you begin

- Obtain login credentials. You may need to ask your Scopia® Desktop administrator for a user name and password if Scopia® Desktop is configured so that only authenticated users can participate in meetings, access webcasts, or watch recordings.
- Connect a headset or speaker and microphone to your computer, and ensure it is configured in the control panel or system settings.
- Connect a video camera or webcam to your computer.

Procedure

1. To activate Scopia® Desktop for the first time, go to the Scopia® Desktop web portal page at *http://<Scopia® Desktop domain name>/scopia*.

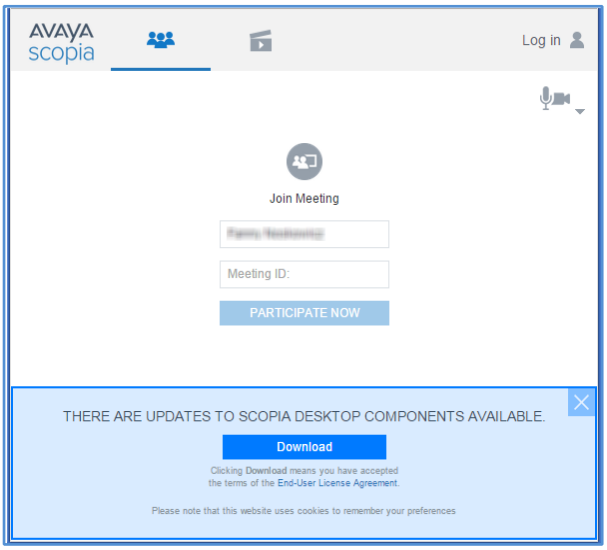


Figure 38: Installing Scopia® Desktop Client

For service provider (multi-tenant) deployments, access *http://<Scopia® Desktop domain name>/<tenant>* or *http://<Scopia® Desktop domain name>/scopia/mt/<tenant>*. For example, *http://sd.company.com/org1* or *http://sd.company.com/scopia/mt/org1*.

2. On the Scopia® Desktop Client web interface, click **Download**.

   Scopia® Desktop Client downloads the installation file.

3. Run the installation file.
4. Restart the browser.
5. If you are installing from Google Chrome or Firefox, click **Launch application** in the **External Protocol Request** dialog box.
6. Install the **Conference Client** to install or update the Scopia® Desktop Client.

   When the Scopia® Desktop Client installation is complete, you should see the Scopia® Desktop icon in the task tray at the lower right corner of the screen.

7. Install the **Web Collaboration** package to get the advanced content sharing functionality of your Avaya Scopia® Solution.
8. To verify which components were installed, select **View and Manage Components**. A list of installed components appears.

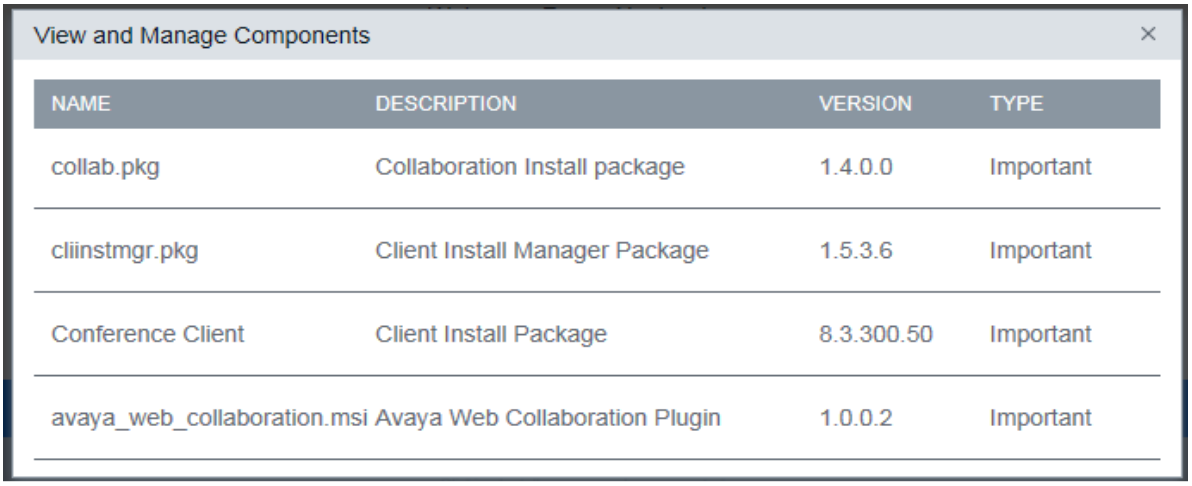


Figure 39: Viewing and managing installed components

9. To install Scopia® Add-in for Microsoft Outlook, log in to the Scopia® Desktop Client. This add-in allows you to schedule videoconferences from Microsoft Office Outlook.
10. If you installed the Scopia® Add-in for Microsoft Outlook, restart your Microsoft office Outlook.

Related Links

Rolling-Out Scopia® Desktop Client to End Users on page 63

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)
- Microsoft Systems Management Server (SMS).

Contact Customer Support to obtain pre-prepared scripts which can run using either of these infrastructures. There is also accompanying documentation on how to deploy throughout your organization using either of these infrastructures.

Related Links

Rolling-Out Scopia® Desktop Client to End Users on page 63

Chapter 4: Configuring Advanced Features of Scopia® Desktop server

Scopia® Desktop server is a highly flexible system with many settings which can be configured manually.

This section details how to change the default settings of the more advanced server features.

Related Links

Creating Meeting Invitation Templates for End Users on page 68
Managing Recordings from the Scopia® Desktop Web Portal on page 70
Displaying Administrator Messages to End Users on page 73
Configuring Dial String Rules on page 74
Branding your Scopia® Desktop User Interface on page 80

Creating Meeting Invitation Templates for End Users

About this task

This section describes how to create or edit the text automatically added to meeting invitations created with the Scopia® Add-in for Microsoft Outlook (32bit).

Important:

The text of the invitation for the 64bit version is configured in Scopia® Management. For more information, see *User Guide for Scopia® Add-in for Microsoft Outlook*.

Create the invitation text yourself, and use the buttons in this section to automatically insert the addresses which are configured for this server. Addresses use the FQDN configured in the server during installation.

Important:

In a service provider (multi-tenant) deployment the Contact List and the Scopia® Add-in for Microsoft Outlook are configured during installation with organization-specific URLs.

Procedure

1. Access the Scopia® Desktop server Administration web interface.
2. Select **Messages and Invitations** in the sidebar.

3. Select the **Invitations** tab.

   The default instructions for accessing the meeting from a desktop, phone or video conferencing device appear in the screen.

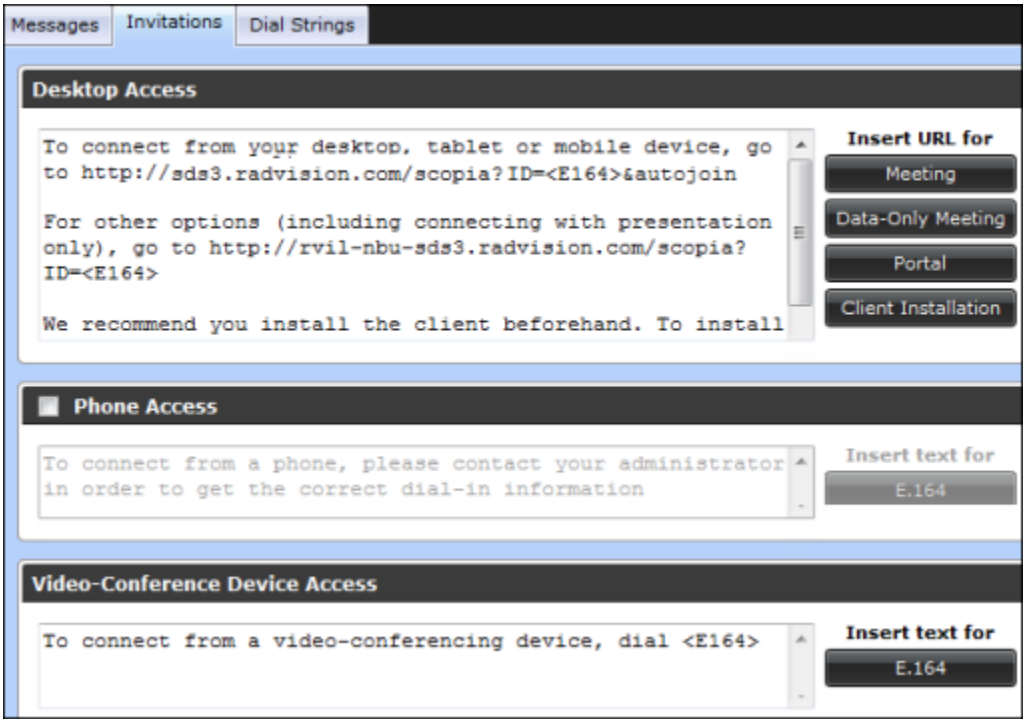


Figure 40: Creating invitation text for Scopia® Add-in for Microsoft Outlook (32bit)

4. Enter the invitation text, using the buttons to add web addresses as described in Table 17: Generating addresses for invitation text on page 69.

Table 17: Generating addresses for invitation text

Field	Description

Meeting	Inserts the web address to connect directly to the videoconference from Scopia® Desktop Clients.
	If you have multiple Scopia® Desktop servers and want participants to join from their local server to conserve bandwidth, insert the link information for each server. For example:
	`From Europe, connect to http://europe.server.com/scopia?ID=1234`
	`From Asia, connect to http://asia.server.com/scopia?ID=1234`
	`From the US, connect to http://us.server.com/scopia?ID=1234`

Data-Only Meeting	Inserts the web address for participants who connect their computer to share content on their screens separately from the video of a dedicated videoconferencing endpoint.
Portal	Inserts the address for the Scopia® Desktop web portal. Users would access this to enter a different meeting ID or access a recorded meeting.

Table continues…

Field	Description
Client Installation	Inserts the address to install Scopia® Desktop Client on your computer. The installation occurs within the web page.
Phone Access > **E. 164**	Insert the telephone number of the gateway enabling phones to join the videoconference. If your deployment does not include a gateway, de-select the **Phone Access** checkbox, so the gateway information is not included in Outlook.
Videoconference Device Access > **E. 164**	Inserts the number to dial from dedicated videoconferencing endpoints to join the meeting.

5. Select **OK** or **Apply**.

Related Links

Configuring Advanced Features of Scopia® Desktop server on page 68

Managing Recordings from the Scopia® Desktop Web Portal

About this task

You can protect and secure recordings by making them private or by limiting access to them. For more information about protected and private recordings see *User Guide for Scopia® Desktop*.

Before you begin

To manage a recording made by other users, you need to know their username and password.

Procedure

1. Access the Scopia® Desktop web portal, as described in *User Guide for Scopia® Desktop*.
2. Select the **Recordings and Events** tab.

   The list of available recordings is displayed.

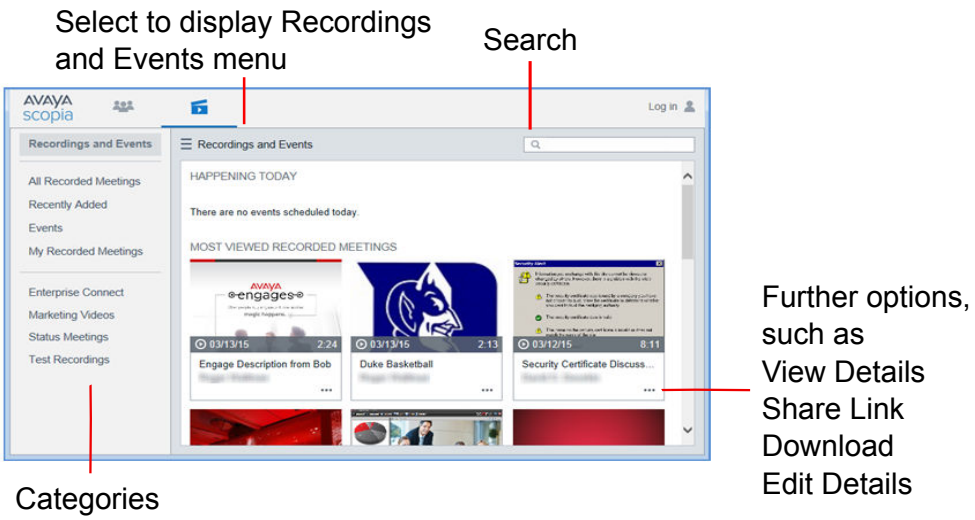


Figure 41: Recordings and Events tab of the Scopia® Desktop web portal

3. Find the recording:
   - To search by the meeting ID, name or owner, enter the value in the **Search** field and select **Search** .

     To return to the complete list of recordings, select **Recordings and Events** from the left-hand menu.
4. Select the **Further Options** button ... next to the recording.

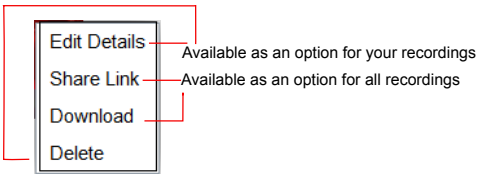


Figure 42: Further Options menu

5. Select **Edit Details**.

   The Edit details window opens.

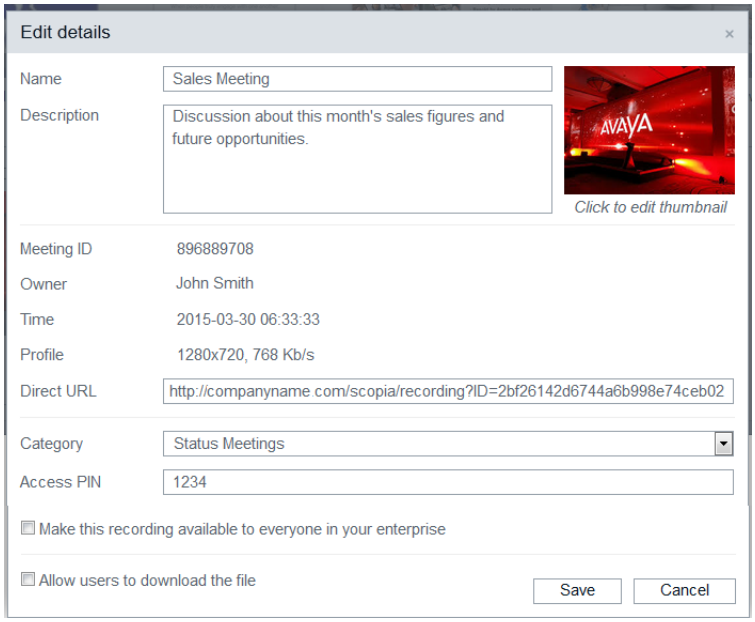


Figure 43: Edit details window

6. Change the recording's properties.

Table 18: Editing properties of a recording

Element	Description
Name	You can change the name which appears at the **Recordings and Events** tab of the Scopia® Desktop web portal.
Description	Edit the short description that appears in the Recording Information window (upon selecting the **View Details** button).
Category	Use the list to assign a category.
Access PIN	To protect the recording by limiting access to it, enter the access PIN. You can use any combination of alphanumeric characters.
Make this recording available to everyone in your enterprise	Select to make the recording public and clear it to make it private. **Note:** Even if a recording is private, users can still access it if they have the direct URL address of the recording.
Allow users to download the file	Select to enable users to save the file to their computer and clear it to prevent users from saving the file to their computer.
Thumbnail picture	You can change the default thumbnail by clicking on it. Your thumbnail should represent the program. It should be 4x3 aspect ratio, and ideally should be <100Kb. In terms of file types, Scopia® Desktop supports .png, .jpg, .gif.

7. Select **Save** to save the changes you made to the recording's properties.

Related Links

Configuring Advanced Features of Scopia® Desktop server on page 68

Displaying Administrator Messages to End Users

About this task

This section describes how to edit the administrator and dial plan messages. Use administrator messages on the Scopia® Desktop server Web Portal page to post important information like the system status, scheduled shutdowns, or configuration tips.

The dial plan message appears in the Invitation dialog box. You can use this to provide users with dialing tips, for example, to explain the prefixes to use for different gateways.

The following HTML tags and attributes are supported in the administrator messages text editor:

```
<a href="http*" target="_blank"></a>
<img src=”http*”>
<iframe src=”http*”></iframe>
<font color=#123456|red|green|blue|”></font>
<u>underlined text</u>
<i>italic text</i>
<b>bold text</b>
<br> to break a line
<ol><li>Ordered list items</li></ol>
<ul><li>Unordered list items</li></ul>
<p></p>
<div></div>
```

You must fix a width and height of the `<iframe>` tag according to the style sheet of the corresponding page. For example, for the portal entry page, the style sheet looks like this:

```
<style>
      .motd iframe
      {
         width: 100%
         height: 150px
      }
</style>
```

The administrator message text editor replaces single `&` characters with `&amp;`. It also replaces < and > of unrecognized tags with `<` and `>` respectively.

Procedure

1. Access the Scopia® Desktop server Administration web interface.
2. Select **Messages and Invitations** > **Messages**.
3. Select the **Administrative Message** check box.

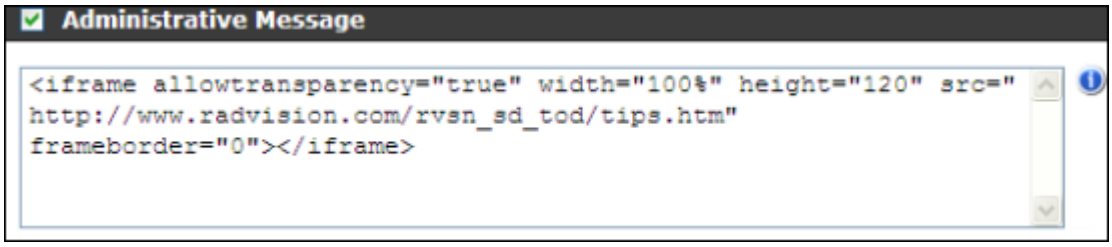


Figure 44: Modifying the entry-page message for end-users

4. Modify the text of the entry page message as required.

5. Select the **Invitation Dial Plan Assistance** check box.

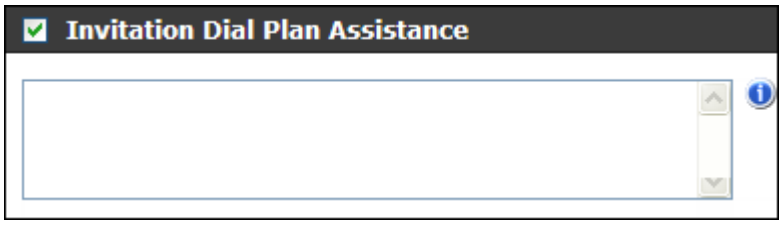


Figure 45: Modifying the invitation message for end-users

6. Modify the text of the invitation message as required.
7. Select **OK** or **Apply**.

Related Links

Configuring Advanced Features of Scopia® Desktop server on page 68

Configuring Dial String Rules

About this task

This section describes how to configure dial string rules in Scopia® Desktop. Dial string rules look for prefixes in the dial string, alter the string according to your organization's policy, and route the call to the correct gateway or gatekeeper.

Related Links

Configuring Advanced Features of Scopia® Desktop server on page 68
Planning Rules to Modify Dial Strings on page 74
Adding or Editing a Dial String Rule on page 76
Deleting a Dial String Rule on page 79

Planning Rules to Modify Dial Strings

About this task

Depending on the phone system of your organization, you may already have a prefix of '9' (or some other number) to call outside the organization. More specifically, a gateway reads and interprets the dial string, sees the '9', and routes the call to a gateway to reach an external phone line. It then alters the dial string by removing the '9', and sends the remainder of the number to the external phone exchange.

Similarly, you may also have a prefix of '1' or '0' to dial outside your city or state (long distance calls), and '00' or '011' for international calls. If you have branches in other locations, your gateways/gatekeepers may have dedicated prefixes to reach that branch's exchange. For example, all dial strings beginning with '5' may be routed to the Hong Kong office. In each case, your call system routes to different gateways or gatekeepers by reading and interpreting your dial prefixes.

In Scopia® Solution deployments, dial prefixes are interpreted and altered when:

- When a call is routed to a local H.323 PSTN or ISDN gateway. Scopia® Desktop modifies the prefix to add routing information.
- When there is a SIP PBX either on-site or at a remote location, Scopia® Desktop detects phone numbers in the directory and appends the SIP URL to forward it to the right gateway.

There are several methods to alter dial strings:

- String normalization removes all non-digits from a string (except '+'). For example: `+1 (603) 407-5956` becomes `16034075956`. This is always the first rule.
- Replace a prefix or suffix
- Add a prefix or suffix
- Remove a prefix by leaving the replacement string blank.

Important:

Dial rules are applied in the specific order they are listed in the table.

List your rules so that the more specific rules are applied first, followed by the more general. For example, a rule which replaces all `+1603` prefixes is more specific than a rule which replaces all `+1` prefixes. Therefore the more specific `+1603` rule should be executed first.

Table 19: Simplified example for local, national and international dial string rules on page 75 shows the rules required to edit the dial strings, where the rules are implemented in this order:

1. The first three rules replace the prefix `603`, `1603`, or `+1603` with `1370` when followed by exactly seven digits. `1370` routes it to a gatekeeper/gateway, while the remaining seven digits remain intact. Each of these rules are inserted so that the most specific rule is first.
2. The next rule replaces the `+1` of any other phone number with 8 digits. The new prefix is `11701`, the prefix of a different gatekeeper/gateway. The subsequent eight digits remain intact.
3. The final rule replaces prefix `+44` with `10700`, to route these numbers to a different gateway.

Table 19: Simplified example for local, national and international dial string rules

Match Prefix	Replace	Optional Suffix	Example Input String	Example Result String	Comments
603xxxxx	1370		60355555	137055555	Replace the prefix *603*, *1603*, or *+1603* with *1370* when followed by exactly seven digits.
1603xxxxx	1370		160355555	137055555	
+1603xxxxx	1370		+160355555	137055555	
+1xxxxxxxx	11701		+150855555	1170150855555	All other long distance calls routed to another gateway, accessed with the number 11701.
+44	10700		+4455566666	1070055566666	International calls to England go to the London local call gateway, accessed by the number 10700.

Table 20: Example dial rules to add a suffix to route to a SIP gateway on page 76 adds a suffix to route each prefix to a different SIP server, and removes or replaces the prefix:

1. The first three rules remove `603`, `1603`, or `+1603` prefixes when followed by exactly five digits and route them to the *aa* SIP gateway by adding *@sip_aa.z.com* as a suffix.
2. The next rule replaces the `+1` prefix to `1` when followed by exactly eight digits, and routes it to the *bb* SIP gateway by adding *@sip_bb.z.com* as a suffix.
3. The final rule replaces prefix `+44` with `0` and routes it to the *cc* SIP gateway by adding *@sip_cc.z.com* as a suffix.

Table 20: Example dial rules to add a suffix to route to a SIP gateway

Match Prefix	Replace	Optional Suffix	Example Input String	Example Result String	Comments
603xxxxx		@sip_aa.z.com	60355555	55555@sip_aa.acme.com	Remove the prefix of a phone number starting with `603`, `1603`, or `+1603` when followed by exactly five digits and route it to the *aa* SIP gateway by adding *@sip_aa.acme.com* as a suffix.
1603xxxxx		@sip_aa.z.com	16035555555	55555@sip_aa.acme.com	
+1603xxxxx		@sip_aa.z.com	+160355555	55555@sip_aa.acme.com	
+1xxxxxxx	1	@sip_bb.z.com	+150855555	150855555@sip_bb.acme.com	All other long distance (national) calls routed to the *bb* SIP gateway, replacing `+1` with `1`.
+44	0	@sip_cc.z.com	+4455566666	055566666@sip_cc.acme.com	International calls to the UK go to the *cc* SIP gateway, replacing `+44` with `0`.

Related Links

Configuring Dial String Rules on page 74

Adding or Editing a Dial String Rule

About this task

A dial string rule alters dial strings to reflect the routing policy of your organization. For example, a dial string that starts with ‘9’ can be defined to route to an outside line. The rule usually specifies a dial prefix which is replaced, or adds a suffix to the end of the dial string, so that it can be sent to the appropriate gateway/gatekeeper.

To correctly represent the number of digits in a string, use the 'x' character to denote ‘any number’.

For example, a rule which looks for `603` matches a dial string of any length beginning with `603`, while a rule looking for `603xxxxx` matches only a dial string which begins with `603` and is followed by five digits.

Important:

Do not use any other characters, such as a spaces, hyphens or brackets.

This section details how to create or edit a dial string rule.

Procedure

1. Access the Scopia® Desktop server Administration web interface.
2. Select **Messages and Invitations** > **Dial Strings**.

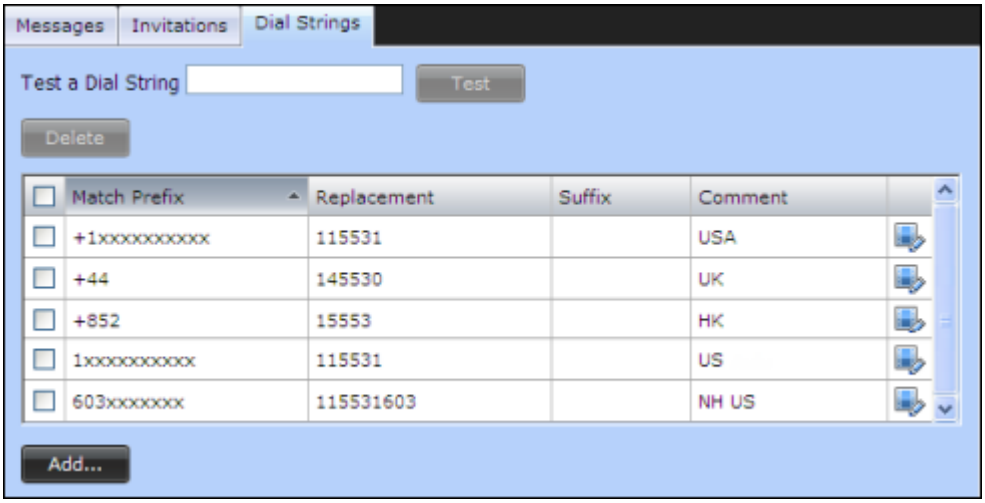


Figure 46: List of Dial string rules

3. Select **Add** to create a dial rule.

   To edit an existing rule, select the row's edit icon .

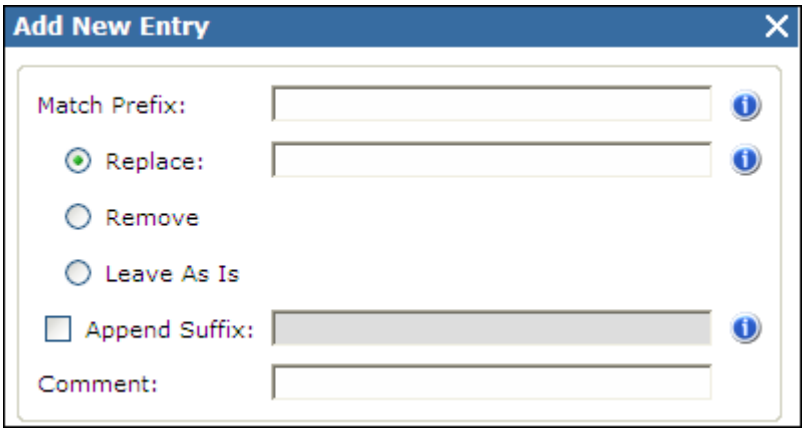


Figure 47: New dial string rule

4. Enter the fields as detailed in Table 21: Creating or editing a dial string rule on page 78.

Table 21: Creating or editing a dial string rule

Field	Description
Match Prefix	Insert the prefix which the system should identify to apply this rule. To make the rule even more specific to apply to dial strings with a specific length, add 'x' for each digit which must follow the prefix.
Replace	Select and enter the string to replace the **Match Prefix** string.
Remove	Select to delete the **Match Prefix** string.
Leave As Is	Select to identify dial strings which have the **Match Prefix** string at the beginning, but do not remove it.
Append Suffix	Select this option to add a suffix, and enter the suffix in the text box.
Comment	Optional, used to explain the reasoning behind this rule.

5. Select **OK**.
6. To test the new dial string rule:
   a. Enter a string in the **Test a Dial String** field.

Figure 48: Dial String Test

   b. Select the check box for the rule you want to apply to this string.
   c. Select **Test**.

   The **Dial String Test** window appears displaying the dial string after the rule is applied.

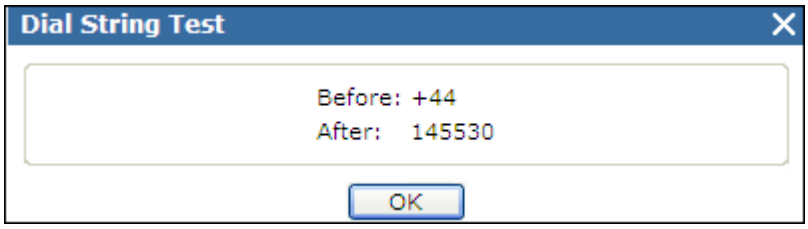


Figure 49: Dial String Test Results

Related Links

Configuring Dial String Rules on page 74

Deleting a Dial String Rule

About this task

A dial string rule is the method used to alter dial strings to reflect the routing policy of your organization. For example, a dial string that starts with ‘9’ can be defined to be routed to an outside line. The rule usually specifies a dial prefix, which the rule then replaces, or adds a suffix to the end of the dial string, so that it can be sent to the appropriate gateway/gatekeeper.

This section details how to remove an existing dial string rule.

Procedure

1. Access the Scopia® Desktop Administration web interface.
2. Select **Messages and Invitations** > **Dial Strings**.

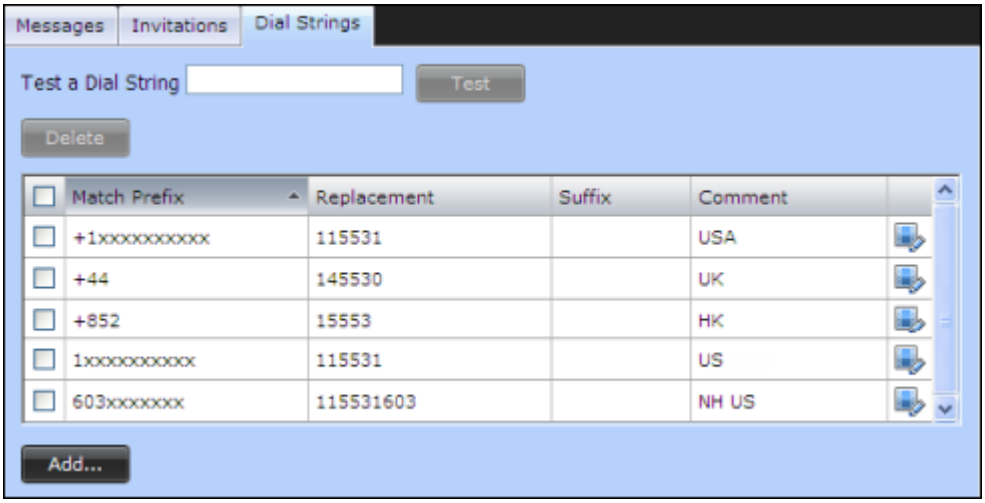


Figure 50: List of Dial string rules

3. Locate the rule you need to remove and select the check box next to it.

   The **Add** button changes to a **Delete** button.
4. Select **Delete**.
5. Select **OK** to confirm.

Related Links

Configuring Dial String Rules on page 74

Branding your Scopia® Desktop User Interface

Customers can change logos and text from the Avaya or Scopia® Desktop branding to their own custom branding. You can change images and strings using the Scopia® Desktop Branding application.

Important:

You can export or import all the customized images and text strings for your organization in the Scopia® Desktop Branding application, by selecting **File** > **Export** or **File** > **Import**.

To restore the default Scopia® Desktop GUI text and images, select **File** > **Restore All**.

Related Links

Configuring Advanced Features of Scopia® Desktop server on page 68
Replacing Brand Logos and Other Images on page 80
Customizing GUI Text Strings for your Organization on page 82

Replacing Brand Logos and Other Images

About this task

You can replace images appearing in the Scopia® Desktop user interface by using the Branding application on Scopia® Desktop server. Changes takes affect immediately, therefore we recommend not to replace images on a live server. Most web browsers store local cached copies of images, therefore to ensure an up-to-date view of the application, clear your browser's cache. Scopia® Desktop server is released with a set of default images which you can restore at any time.

Procedure

1. Select **Start** > **Programs** > **Scopia® Desktop** > **Branding Application**.
2. Select the **Images** tab.

Figure 51: Viewing and changing logos in the Scopia® Desktop GUI

Important:

If an image has a transparent background, it appears with a gray and white "checkerboard" background in the preview fields.

3. Choose the image you want to replace from the list at the top left of the window.

   A brief description of the image is displayed along with the recommended image size. The **Default image** area shows the image originally distributed with the product. The **Currently installed image** shows the image that appears in the user interface.

4. Select **Select File**, to choose the new logo.

   If you use an image that the application indicates as not properly sized, a warning appears below the image description.

5. If you use an image that is not properly sized, verify that the image is displayed correctly:
   a. Verify that the Scopia® Desktop server is running.
   b. Review the Scopia® Desktop user interface to verify that the image appears correctly.

6. Select **Install Image** to use the new image.

   Important:

   If an old image still appears, refresh your browser's cache.

7. To restore a default image, select **Restore Original Image**.

Related Links

Branding your Scopia® Desktop User Interface on page 80

Customizing GUI Text Strings for your Organization

About this task

You can modify some of the text displayed in the Scopia® Desktop user interface. If you update any text strings, you need to restart Scopia® Desktop server to see the effect of the update.

Procedure

1. Select **Start** > **Programs** > **Scopia® Desktop** > **Branding Application**.
2. Select the **Strings** tab.

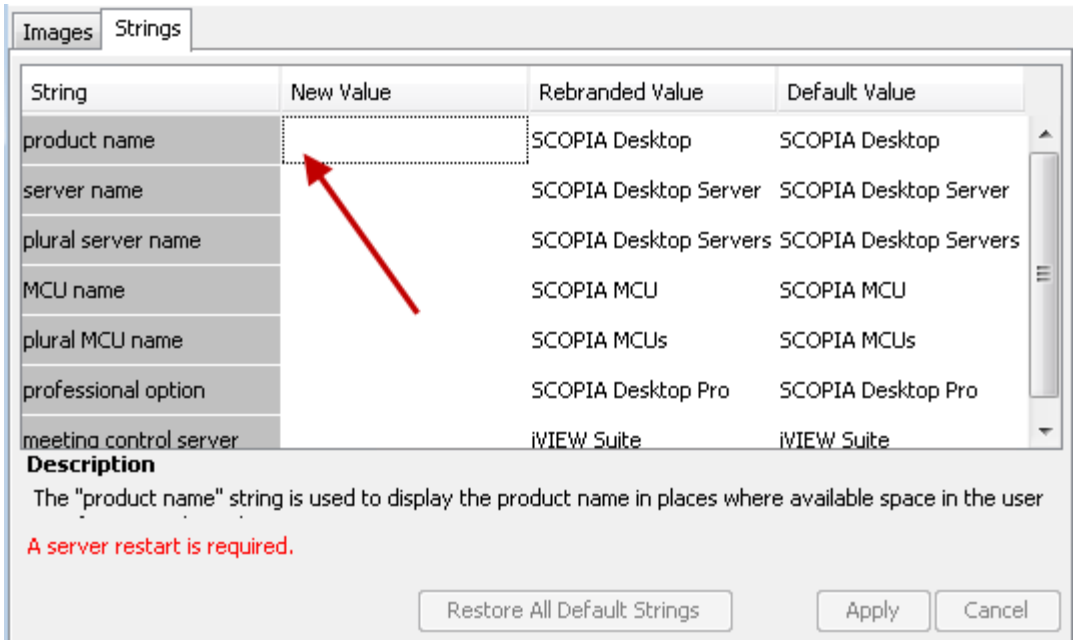


Figure 52: Creating replacement strings for Scopia® Desktop GUI

3. Enter the new text strings in the **New Value** column.

Table 22: Changing the GUI strings

Field	Description
String	The internal label of the string whose value is displayed in the GUI.
New Value	Insert the text you would like to display in place of the existing text.
Rebranded Value	This column displays the values that are currently saved. When the Scopia® Desktop server is restarted, these are the values which appear in the user interface. Double-click this value to copy it to the **New Value** column.
Default Value	This column displays the original text strings that were distributed with Scopia® Desktop.

4. Select **Apply**.

   The new values are saved and appear in the **Rebranded Value** column.

5. In the Windows Services panel, restart the **Scopia® Desktop - Apache Tomcat** service to apply the changes.
6. To restore default strings:
   a. Select **Restore All Default Strings**.
   b. Select **Apply**.
   c. Restart the **Scopia® Desktop - Apache Tomcat** service to apply the changes.

Related Links

Branding your Scopia® Desktop User Interface on page 80

Chapter 5: Securing Your Scopia® Desktop Deployment

This section describes how you can enhance the security of your Scopia® Desktop deployment by encrypting Scopia® Desktop communications and by protecting access to Scopia® Desktop server using Integrated Windows Authentication (IWA).

Important:

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

Related Links

Encrypting Scopia® Desktop server Communications on page 84
Securing Login Access to Scopia® Desktop server using IWA on page 94

Encrypting Scopia® Desktop server Communications

You can secure Scopia® Desktop server communications by encrypting its traffic.

There are several data streams between Scopia® Desktop server and Scopia® Desktop Client and then between Scopia® Desktop server and Scopia® Management which are transmitted using different protocols as shown in Figure 53: Protocols used in an unsecure environment on page 84:

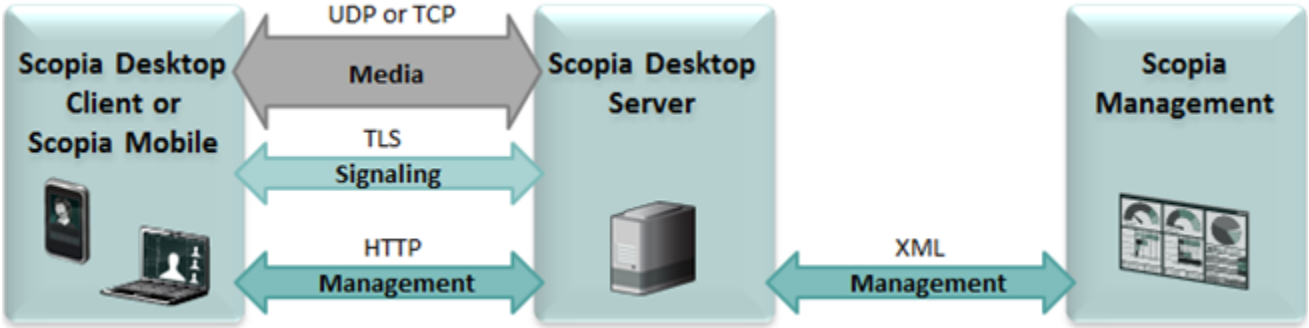


Figure 53: Protocols used in an unsecure environment

The media stream consists of audio, video and presentation. Audio and video are sent over UDP by default. If the UDP connection fails, for example, if the UDP port is closed, TCP is used instead. Presentation always uses TCP.

In a secure environment you encrypt Scopia® Desktop server communications as shown in Table 23: Protocols used for encrypting Scopia® Desktop server communications on page 85.

Table 23: Protocols used for encrypting Scopia® Desktop server communications

Data stream	Unsecure environment	Secure environment
Audio and video between Scopia® Desktop server and Scopia® Desktop Client	UDP	SRTP
	TCP	TLS
Signaling and presentation between Scopia® Desktop server and Scopia® Desktop Client	TCP	TLS
Management between Scopia® Desktop server and Scopia® Desktop Client	HTTP	HTTPS
Signaling and management between Scopia® Desktop server and Scopia® Management	XML	TLS

Make sure that you protect all data streams and have a secure environment as shown in Figure 54: Protocols used in a secure environment on page 85.

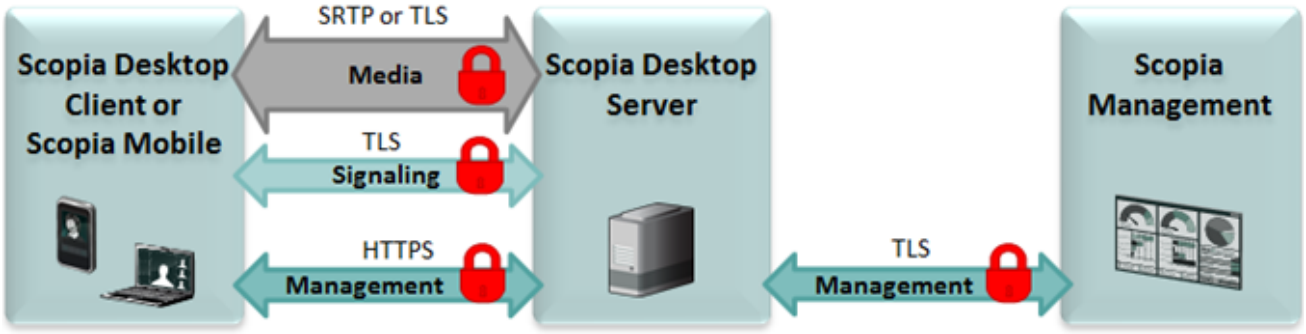


Figure 54: Protocols used in a secure environment

Related Links

Securing Your Scopia® Desktop Deployment on page 84
Encrypting Web Access to the Scopia® Desktop server on page 85
Encrypting Scopia® Desktop Media and Signaling and Connection with Scopia® Management on page 89
Encrypting Media over UDP between Scopia® Desktop server and Scopia® Desktop Client on page 93

Encrypting Web Access to the Scopia® Desktop server

About this task

You can secure access to the Scopia® Desktop server web administration interface and web portal by enabling HTTPS encryption of the management traffic. 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.

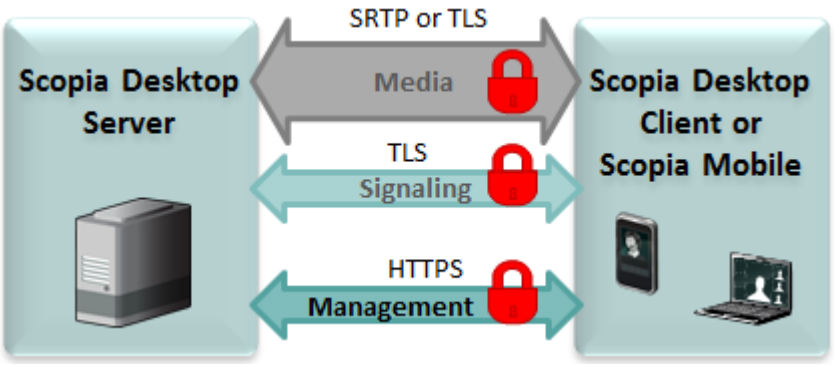


Figure 55: Encrypting communications between Scopia® Desktop server and Scopia® Desktop Client

Encrypting web access to the Scopia® Desktop server requires a signed certificate for it. Scopia® Desktop server comes with a non-unique certificate pre-installed on the Scopia® Desktop Conference Server, however, we recommend that you use a unique certificate for stronger authentication as described in the procedure below.

Before you begin

For stronger authentication, make sure you have a unique HTTPS certificate on the Scopia® Desktop Conference Server. Do not save the certificate in the Scopia® Desktop installation directory or any of its sub-directories, to avoid its accidental deletion during an upgrade.

Procedure

1. Select **Start** > **All Programs** > **Scopia® Desktop** > **ConfigTool**.
2. Select the **Enable HTTPS** check box in the **HTTPS** tab.

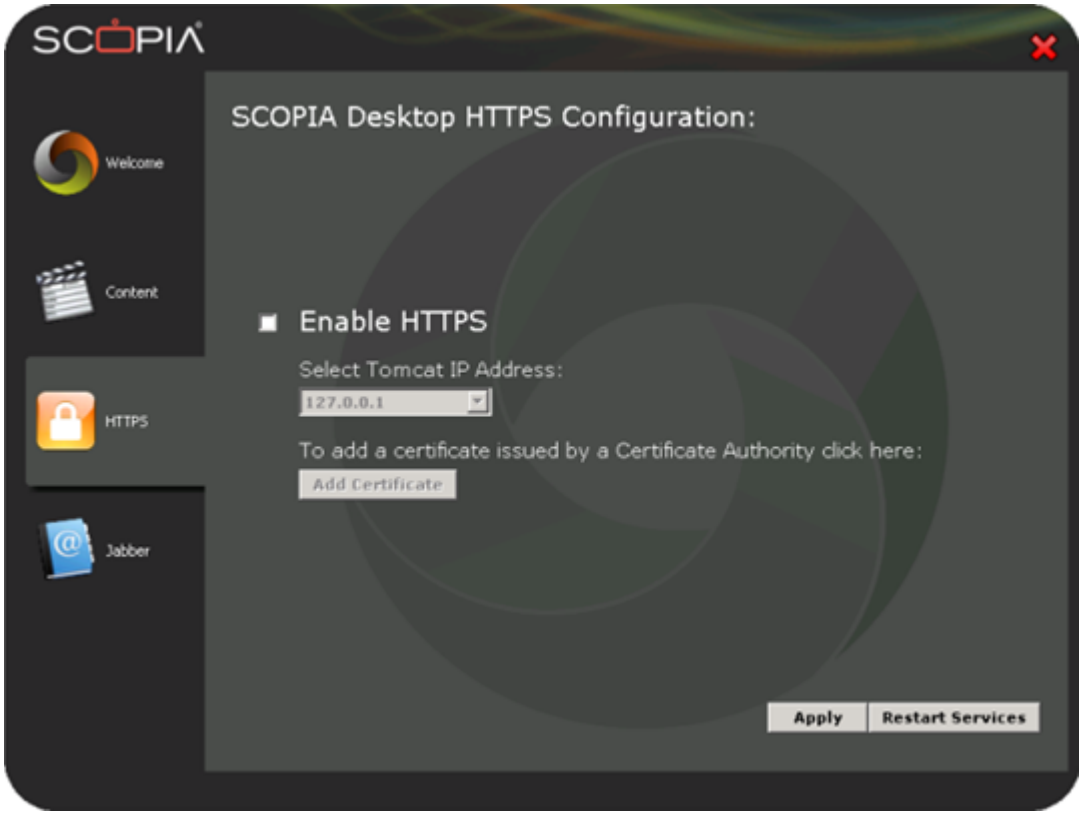


Figure 56: Adding a certificate to Scopia® Desktop server

3. Ensure that the real IP address of Scopia® Desktop server is displayed in the **Select Tomcat IP Address** list.
4. Select **Apply**.

   You have enabled HTTPS with the pre-installed non-unique certificate. For stronger authentication, use a unique certificate by following the rest of this procedure.
5. Select **Add Certificate** to upload an existing signed certificate.
6. If the certificate is installed in the local machine's Windows Certificate Store (WCS):
   a. Select the **Configure Certificate via Certificate Store**.

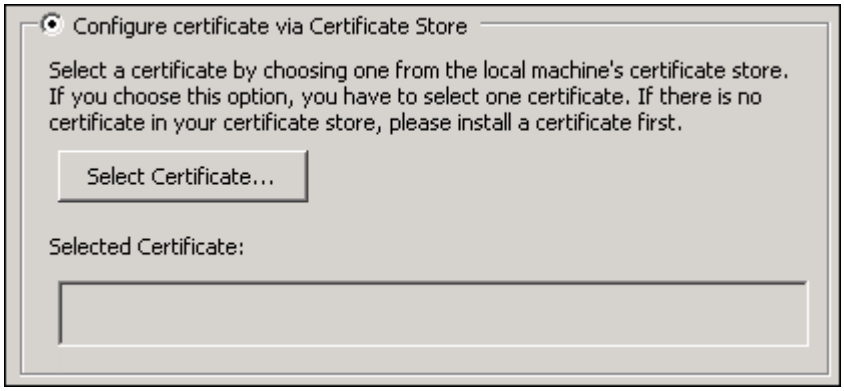


Figure 57: Configuring certificate using installed on the local machine

b. Select **Select Certificate** to browse the WCS.

c. Select the certificate from the list of certificates in the WCS.

7. To locate a certificate by its filename:

   a. Select **Configure Certificate via File Name**.

   Verify the certificate is not in the Scopia® Desktop installation directory or any of its sub-directories, to avoid its accidental deletion during an upgrade.

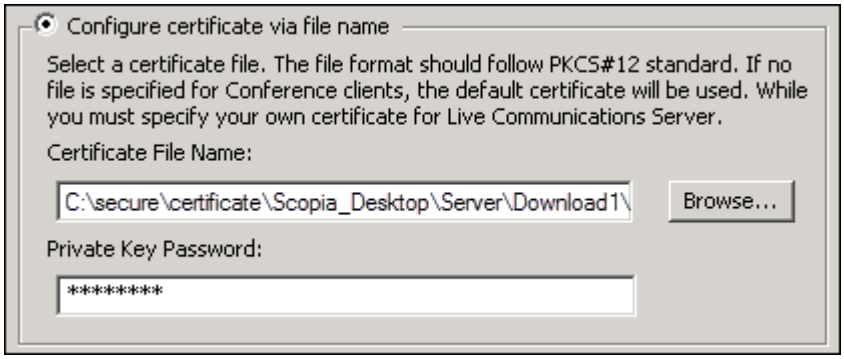


Figure 58: Configuring certificate using the file name

   b. Browse to the PKCS12 certificate and select it.

   c. Enter the private key password for the certificate.

8. Select **OK**.
9. Verify that the certificate information is listed in the **Selected Certificate** pane.
10. Select **Apply**.
11. Select **OK**, and then select **OK** again.
12. Select **Restart Services**.
13. Change the URL in the **Invitations** section of the Scopia® Desktop Administration web interface to use the secure HTTPS protocol:

    a. Log into the Scopia® Desktop Administration web interface.

b. Select **Messages and Invitations** on the sidebar.

c. Select the **Invitations** tab.

d. In the **Desktop Access** section, verify all URLs have the prefix of *https*.

Important:

By default, there are two URLs present in this section.

Related Links

Encrypting Scopia® Desktop server Communications on page 84

Encrypting Scopia® Desktop Media and Signaling and Connection with Scopia® Management

About this task

You can secure Avaya Scopia® Desktop's the traffic between Avaya Scopia® Desktop server and Avaya Scopia® Management using TLS encryption. TLS enables network devices to communicate securely using certificates, to provide authentication of the devices and encryption of the communication between them. This method also checks the data integrity of messages.

By default, audio and video between Scopia® Desktop server and Scopia® Desktop Client are transmitted using the UDP protocol. If Scopia® Desktop server fails to establish the UDP connection with its client, it sends media over TCP. If this is the case your media is protected using TLS together with other data streams between Scopia® Desktop server and Scopia® Desktop Client.

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.

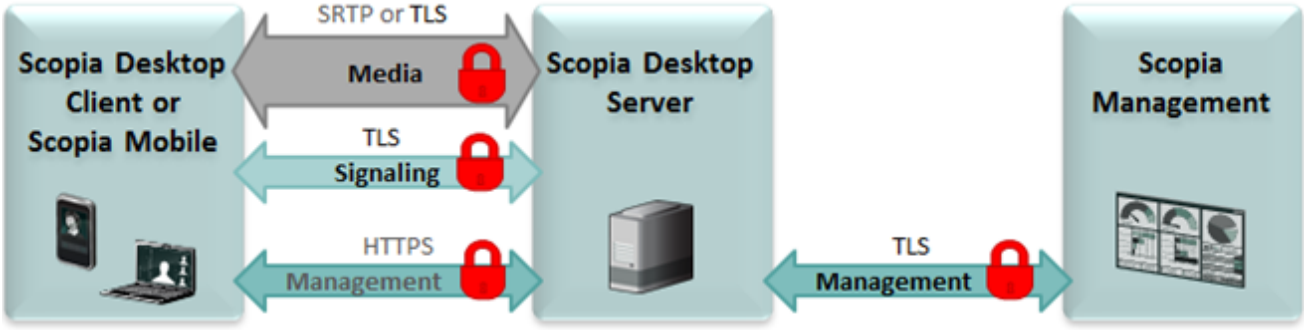


Figure 59: Encrypting communications using TLS

Each time a video network device starts the TLS communication session, it sends its own signed certificate together with the CA root certificate and requests the same certificates from the other devices to which it wants to connect. After both devices verify each other's identity, a secure TLS connection can be established. Exchanging certificates between devices is part of the TLS protocol; it happens in the background and is transparent to a user.

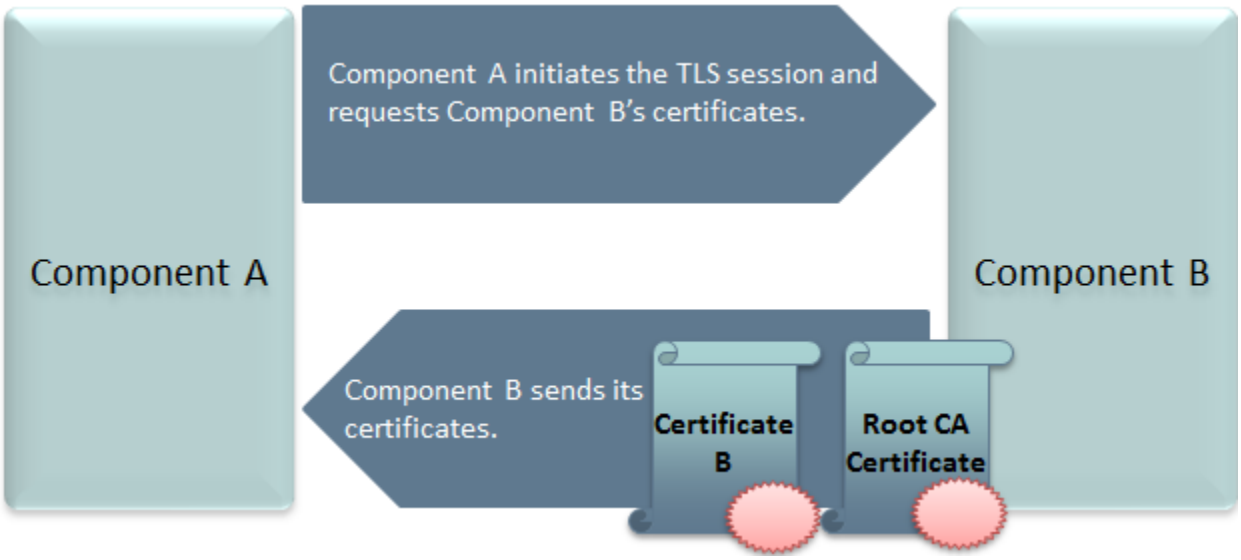


Figure 60: Establishing TLS connection

To establish the encrypted connection, Scopia® Desktop server and Scopia® Management use their TLS certificates for authentication as shown below.

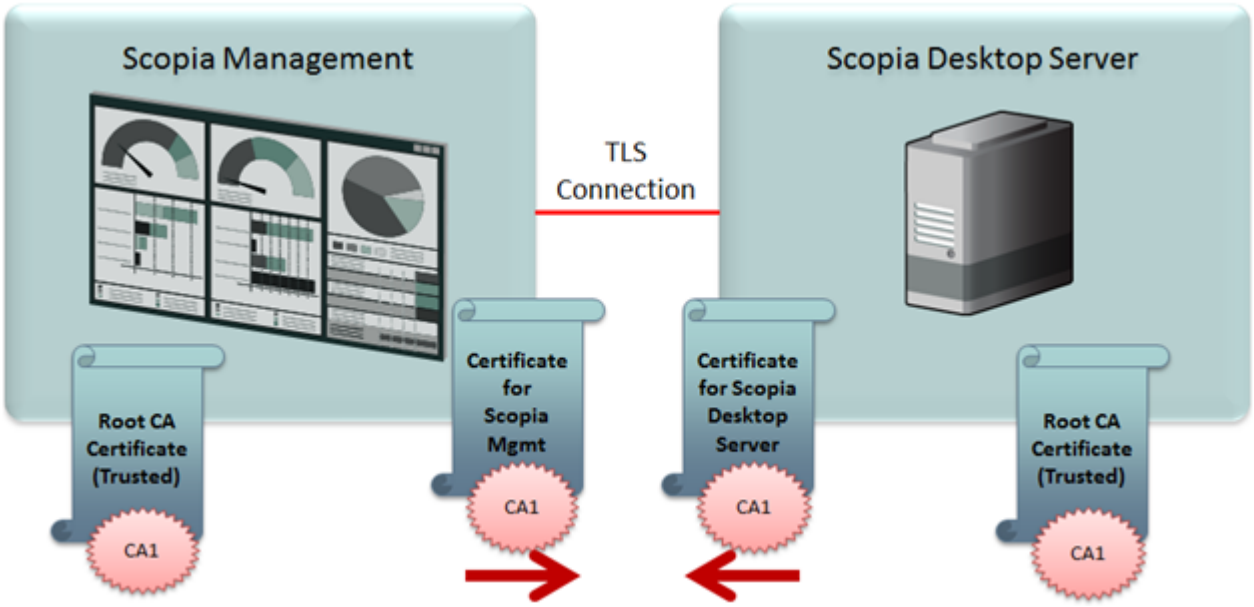


Figure 61: Typical TLS communication with a Scopia® Desktop server

Scopia® Desktop server is shipped with a pre-created and pre-installed certificate, but its encryption keys are non-unique. You can create a unique certificate for stronger authentication as described in this section.

You create a unique certificate by generating a certificate signing request (CSR) using the `keytool` utility and sending it to a certificate authority (CA) for signing. The `keytool` utility is part of the Java installation.

Important:

This section does not explain each of the parameters of the keytool command. For a full description of this Java utility, seehttp://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html.

For information on generating and uploading Scopia® Management certificates as well as enabling the TLS ecryption on Scopia® Management, see *Administration Guide for Scopia® Management.*

Procedure

1. Enable the management encryption on the Scopia® Desktop server side:
   a. Access the Scopia® Desktop server Administrator web user interface.
   b. Select the **Deployment** icon on the sidebar.
   c. Select the **Secure connection using TLS** check box in the **Scopia® Management** section.

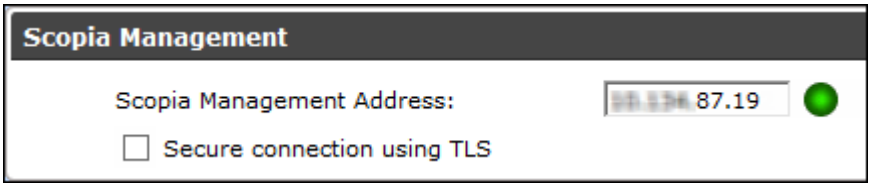


Figure 62: Secure Connection check box

   d. Select **OK**.
2. On Scopia® Management, enable the management encryption connection:
   a. Access the Scopia® Management Administrator portal.
   b. Select the **Devices** tab.
   c. Select the Scopia® Desktop server whose communications you want to encrypt.
   d. Select the check box **Secure connection between this server and Scopia® Management using TLS**.
   e. Select **OK**.

      For stronger authentication create a certificate with unique keys by following the steps below.
3. Stop the **Scopia® Desktop - Apache Tomcat** service.
4. Copy the `.keystore` file located in *<SD_install_dir>\data\sds.keystore* to a temporary working folder, for example *C:\cert*. The keystore file holds the certificates on each server. Currently they hold the default non-unique certificates.

   Important:

   The password on the `.keystore` file is `radvision`.
5. Open a command line window. The `keytool` utility is located in *<SD_install_dir>\JRE\bin*.

6. Use the `keytool` utility to remove the pre-installed certificate from the `.keystore` file with the `-delete` parameter. The default certificate has an alias of `default`:

```
keytool -delete -alias default -keystore sds.keystore -storepass radvision
```

7. Generate a unique key pair using an appropriate DN with the `-genkeypair` parameter:

```
keytool -genkeypair -keyalg RSA -alias sds -sigalg MD5withRSA -dname "CN=<FQDN of
server>"
-keystore sds.keystore -storepass radvision -validity 365 -keysize 1024
```

8. Create a certificate signing request file (CSR) for the newly generated key pair using the `-certreq` parameter:

```
keytool -certreq -alias sds -sigalg MD5withRSA -keystore sds.keystore -storepass
radvision
-file C:\cert\certreq.csr
```

9. Send the certificate request to a Certificate Authority.

   Important:

   Make sure that you use the same CA for signing certificates for both Scopia® Management and Scopia® Desktop server for a more efficient process.

10. The CA returns the certificate signed in form of .crt file, for example `signed_cert.crt`. It also returns a root certificate, `root_cert.crt`.

11. Import the root certificate of the CA into the keystore file using the `-import` parameter:

```
keytool -import -trustcacerts -alias root -file root_cert.crt -keystore sds.keystore
-storepass radvision
```

    where `root_cert.crt` is the trusted root certificate.

    The `trustcacerts` parameter instructs `keytool` to check both the specific and the system `.keystore` file for the root certificate.

12. Import the signed certificate into the keystore file. Use the same alias you used in step 8 on page 92.

```
keytool -import -trustcacerts -alias sds -file signed_cert.crt -keystore
sds.keystore
-storepass radvision
```

    `Keytool` issues a confirmation message if the certificate was uploaded successfully.

13. Copy the `.keystore` file back to its original location.

14. Restart the services on the Scopia® Desktop server.

15. Make sure that Scopia® Management has its certificate generated and uploaded as described in the *Administration Guide for Scopia® Management*.

16. Make sure that TLS encryption is enabled on Scopia® Management as described in the *Administration Guide for Scopia® Management*.

Related Links

Encrypting Scopia® Desktop server Communications on page 84

Encrypting Media over UDP between Scopia® Desktop server and Scopia® Desktop Client

About this task

By default, audio and video between Scopia® Desktop server and Scopia® Desktop Client are transmitted using the UDP protocol. You can configure your Scopia® Desktop server to encrypt this data stream using the SRTP protocol.

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.

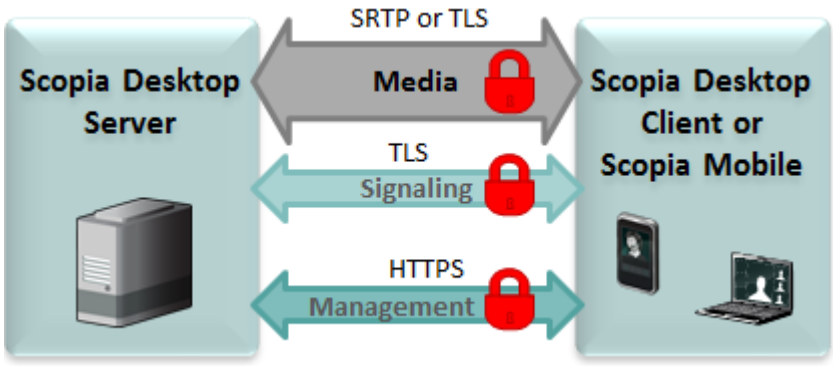


Figure 63: Encrypting media between Scopia® Desktop server and Scopia® Management

Important:

Encrypt signaling between Scopia® Desktop server and Scopia® Desktop Client to protect transmission of the symmetric key.

If Scopia® Desktop server fails to establish the UDP connection with its client, it sends media over TCP. If this is the case and you enabled HTTPS on the Scopia® Desktop server, your media is protected using HTTPS together with other data streams between Scopia® Desktop server and Scopia® Desktop Client.

Procedure

1. Access the Scopia® Desktop web administration interface.
2. Select the **Client** icon in the sidebar.
3. Select the **Meeting Features** tab.
4. Select **Encrypt Media** to encrypt audio and video over UDP between Scopia® Desktop server and Scopia® Desktop Client.

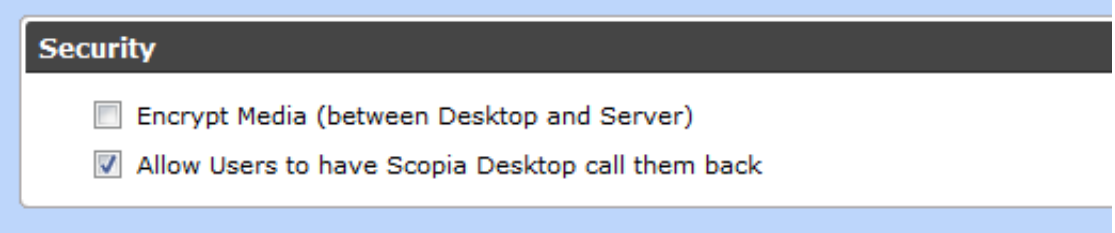


Figure 64: Security Settings

5. Select **OK** or **Apply**.

Related Links

Encrypting Scopia® Desktop server Communications on page 84

Securing Login Access to Scopia® Desktop server using IWA

About this task

Integrated Windows Authentication (IWA) enables Single Sign-On by allowing users to access the Scopia® Desktop Web Portal without entering a username and password, because they are automatically encrypted and sent by the client's browser. The information is verified on the server side by the LDAP (Active Directory), which stores user names and passwords under a Domain Controller (DC).

Microsoft Internet Explorer must be configured to enable IWA and access the Scopia® Desktop server as one of the trusted sites or as part of the Intranet zone.

Important:

This feature is only supported for organizations where all users are under one Domain Controller (DC).

You cannot enable Scopia® Desktop server IWA in service provider (multi-tenant) deployments.

Before you begin

Ensure that authentication settings are configured for Scopia® Management.

Procedure

1. Access the Scopia® Desktop Administration web interface.
2. Select the **Directory and Authentication** icon in the sidebar.

   The **Settings** tab is displayed.
3. Select the **Integrated Windows Authentication** check box.

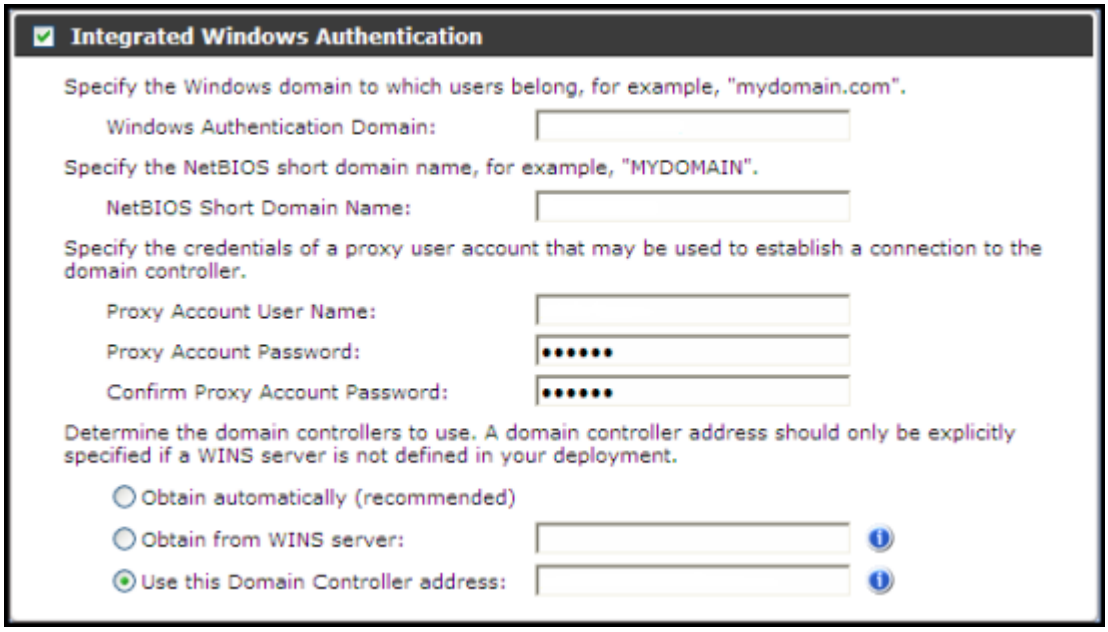


Figure 65: Enabling single sign-on with IWA

4. Configure the Integrated Windows Authentication as detailed in Table 24: Configuring IWA on page 95.

Table 24: Configuring IWA

Field	Description
Windows Authentication Domain	Enter the Windows domain used to authenticate logins. Usually this is the full name of the Domain Controllers (DC) in the LDAP directory which governs the users accessing this server. For example, if you have a DC=*com* and DC=*companyname*, the full domain would be *companyname.com*.
NetBIOS Short Domain Name	Enter the NetBIOS domain name, which is the `USERDOMAIN` environment variable. To view, open a command line window and enter `set u` at the prompt. The system lists environment variables beginning with 'u', including `USERDOMAIN`. This name is case sensitive.
Proxy Account User Name	Enter the username of a proxy account which can remotely access the Domain Controller to authenticate remote logins. Proxy accounts are sometimes set up to enable remote users to login.
Proxy Account Password **Confirm Proxy Account Password**	The password of the proxy account to remotely access the Domain Controller.

Table continues…

Field	Description
Obtain Automatically (recommended)	Select this option to use the current address used by Windows to access the Domain Controller for authenticating users. Typically this is the Active Directory server.
Obtain from WINS server	Select this option to enter the location of a WINS server deployed in your organization, with access details of the Domain Controller. A WINS server resolves NetBIOS names and domains into IP addresses. To enter more than one WINS server, enter each location separated by a comma.
Use this Domain Controller address	Manually specify the address of the Domain Controller to be used to authenticate usernames and passwords.

5. On the Scopia® Desktop Client, verify that Integrated Windows Authentication is enabled in Internet Explorer:
   a. In the Internet Explorer window, select **Tools** > **Internet Options** > **Advanced**.
   b. Under **Security** section, verify that **Enable Integrated Windows Authentication** is selected.
6. Add Scopia® Desktop server to the list of Internet Explorer trusted sites on Scopia® Desktop Client:
   a. In the Internet Explorer window, from **Tools** > **Internet Options** > **Security** > **Trusted Sites** > **Sites**.

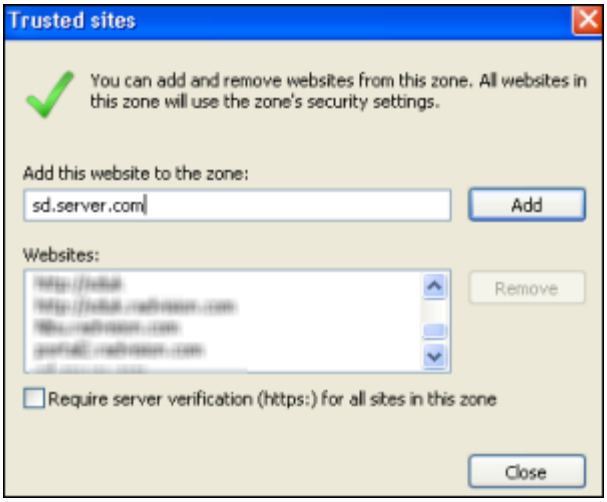


Figure 66: Adding Scopia® Desktop server as a trusted site

   b. Enter the Scopia® Desktop server site address, for example *sd.server.com* and then select **Add**.
   c. Select **Custom level**.
   d. Under the **User Authentication** section, select **Automatic logon with current user name and password**.

e. Select **OK**.

7. To add Scopia® Desktop server to the Internet Explorer intranet zone:

a. In the Internet Explorer window, from Tools menu select **Internet Options** > **Security** > **Local Intranet** > **Sites** > **Advanced**.

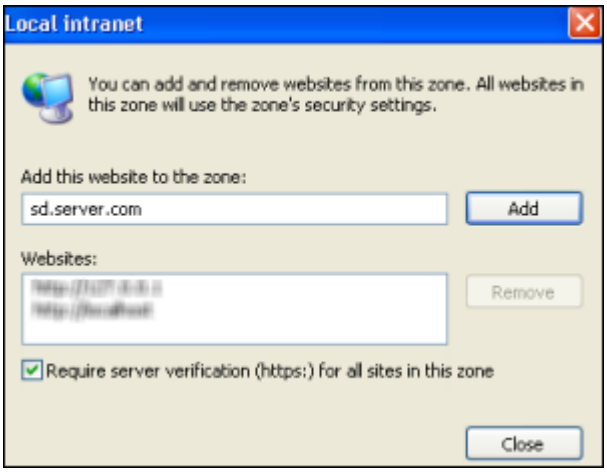


Figure 67: Adding Scopia® Desktop server as a trusted intranet site

b. Enter the Scopia® Desktop server site address, for example *sd.server.com* and then select **Add**.

c. Select **Custom level**.

d. Under User Authentication section, select **Automatic logon only in Intranet zone**.

e. Select **OK**.

Related Links

Securing Your Scopia® Desktop Deployment on page 84

Chapter 6: Maintaining the Scopia® Desktop Deployment

Occasional system upgrades and infrastructure changes in your network may require additional system maintenance activities to maintain your Scopia® Desktop deployment. This section includes the following topics to assist you in maintaining your deployment:

Related Links

Upgrading the Scopia® Desktop server License on page 98
Backing Up Scopia® Desktop server Configuration Settings on page 99
Restoring Scopia® Desktop server Configuration Settings on page 100
Accessing Scopia® Desktop server Log Files on page 100

Upgrading the Scopia® Desktop server License

About this task

You can update the Scopia® Desktop server license for:

- Increased call capacity

  If you upgrade your video network capacity, you can upgrade the maximum number of simultaneous calls on the Scopia® Desktop server with an updated license.

Before you begin

Obtain an Scopia® Desktop server license key and an optional recording serial key.

Procedure

1. Select **Start** > **Settings** > **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. From the list of programs, choose Scopia® Desktop, and then **Change**.

   The Setup Wizard opens.
4. In the Welcome screen select **Next**.
5. In the Program Maintenance screen, choose **Modify**, and select **Next**.
6. In the Custom Setup screen, select **Next**.

7. In the Scopia® Desktop Serial Key window, enter updated keys, and then select **Next**.
8. Follow on-screen instructions to complete installation configuration.

Related Links

Maintaining the Scopia® Desktop Deployment on page 98

Backing Up Scopia® Desktop server Configuration Settings

About this task

Certain configuration files used by Scopia® Desktop should be backed up regularly to allow recovery from catastrophic system failure or instances of corrupted files. During this backup procedure you copy the files which contain these settings:

- Dial string rules
- Administrative message
- Invitation message
- Local configuration

Procedure

1. Navigate to the following directory: *<installdir>\data*.
2. Copy the relevant files into a location outside the installation directory:
   - *ctmx.ini*—for the local configuration
   - *motd.html*—for the administrator message
   - *dialplanhelp.html*—for the invitation message
   - *dial_string_manipulators.xml*—for the dial string rules
   - *admit.dat*- for the content center access control list
   - *csagent.properties*- for the content center configuration

   Important:

   The list of files may vary depending on the configuration of the video network in your organization.

Related Links

Maintaining the Scopia® Desktop Deployment on page 98

Restoring Scopia® Desktop server Configuration Settings

About this task

You may need to restore some of the configuration files used by Scopia® Desktop to allow recovery from catastrophic system failure or instances of corrupted files.

Procedure

1. Stop the service **Scopia® Desktop - Apache Tomcat**.
2. Navigate to the following directory: *<install_dir>\data*.
3. Replace the relevant file with the backup file:
   - *ctmx.ini*—for the local configuration

     Important:

     If you upgraded your Scopia® Desktop server since the last backup, do not restore the ctmx.ini file to avoid overwriting the configuration with the settings of the previous version.
   - *motd.html*—for the administrator message
   - *dialplanhelp.html*—for the invitation message
   - *dial_string_manipulators.xml*—for the dial string rules
   - *admit.dat*- for the content center access control list
   - *recorder_config.xml*- for the recording settings
   - *csagent.properties*- for the content center configuration

   Important:

   The list of files may vary depending on the configuration of the video network in your organization.
4. Start the service **Scopia® Desktop - Apache Tomcat**.

Related Links

Maintaining the Scopia® Desktop Deployment on page 98

Accessing Scopia® Desktop server Log Files

About this task

Scopia® Desktop automatically maintains extensive logs to help maintain your deployment and troubleshoot problems. By accessing the **Logging** tab, you can enable enhanced logging, which provides a network trace on the server (with or without media, depending on your selection).

Important:

Enabling enhanced logging for extended periods of time adds large log files to the system.

Procedure

1. Navigate to the Scopia® Desktop server Administration web interface.
2. Select the **Status** icon in the sidebar.
3. Select the **Logging** tab.

Figure 68: Enabling enhanced logs

4. To download a zipped version of current log files, select **Download**.
5. **(Optional)** To enable enhanced logging, select **Enable**.

   The **Logging Summary** pane displays the current status of enhanced logging.

Related Links

Maintaining the Scopia® Desktop Deployment on page 98

Chapter 7: Deploying Multiple Scopia® Desktop servers with a Load Balancer

Scopia® Desktop is a scalable solution, enabling you to add more Scopia® Desktop servers to your deployment to increase server availability by making your solution resistant to server downtime, and increases the number of participants who can simultaneously connect to videoconferences.

You can deploy multiple Scopia® Desktop servers in a number of ways (see Planning your Avaya Scopia® Desktop Deployment on page 13), including managing a set of servers with a 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. In this way, other components in the solution relate to the cluster as though they were a single server (Figure 69: Scopia® Desktop servers with load balancer on page 102).

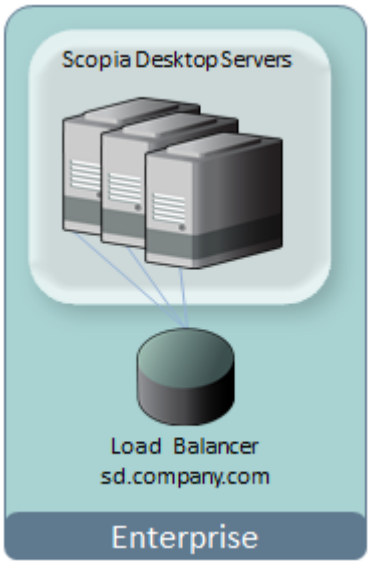


Figure 69: Scopia® Desktop servers with load balancer

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).

Important:

All servers in the deployment must be configured with the same functionality and the same security mode (http/https).

We recommend using the health checks of ICMP echo request and HTTP Web (TCP port 80) to monitor the cluster in your deployment.

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*.

This section guides you through deploying a load balancer with Scopia® Desktop. Perform these tasks in the order listed below:

Related Links

Configuring Scopia® Desktop server for Load Balancing on page 103
Configuring Radware AppDirector on page 107
Configuring Other Load Balancers on page 115
Securing a Load Balanced Environment on page 116

Configuring Scopia® Desktop server for Load Balancing

About this task

For scalability and high availability, you can deploy multiple Scopia® Desktop servers with a load balancer. This section focuses on configuring settings on the Scopia® Desktop servers. For configuring load balancer settings, see Configuring Radware AppDirector on page 107 or Configuring Other Load Balancers on page 115.

Load balancers must direct all participants in a videoconference to the same Scopia® Desktop server, even if this server has no longer enough resources to handle the calls.

When a participant requests to join a videoconference on an overflowing server, the server (not the load balancer, but the server itself) points to another server in the cluster, enabling the participant to join the same meeting from a second server. Redirecting participants in the same conference can only be done from within the Scopia® Desktop server which hosts the videoconference (Figure 70: Redirecting participants in a load balanced environment on page 104).

This is separate and distinct from the load balancer's redirection, which redirects traffic between different servers, not within the same videoconference.

For example, in a new videoconference the load balancer uses the configured load distribution algorithm (such as round robin or least traffic) to forward the first participant to server A (Figure 70: Redirecting participants in a load balanced environment on page 104). The load balancer then forwards subsequent participants of the same videoconference to the same server. If server A runs out of ports, configure it to redirect calls to the next server in the cluster (or farm):

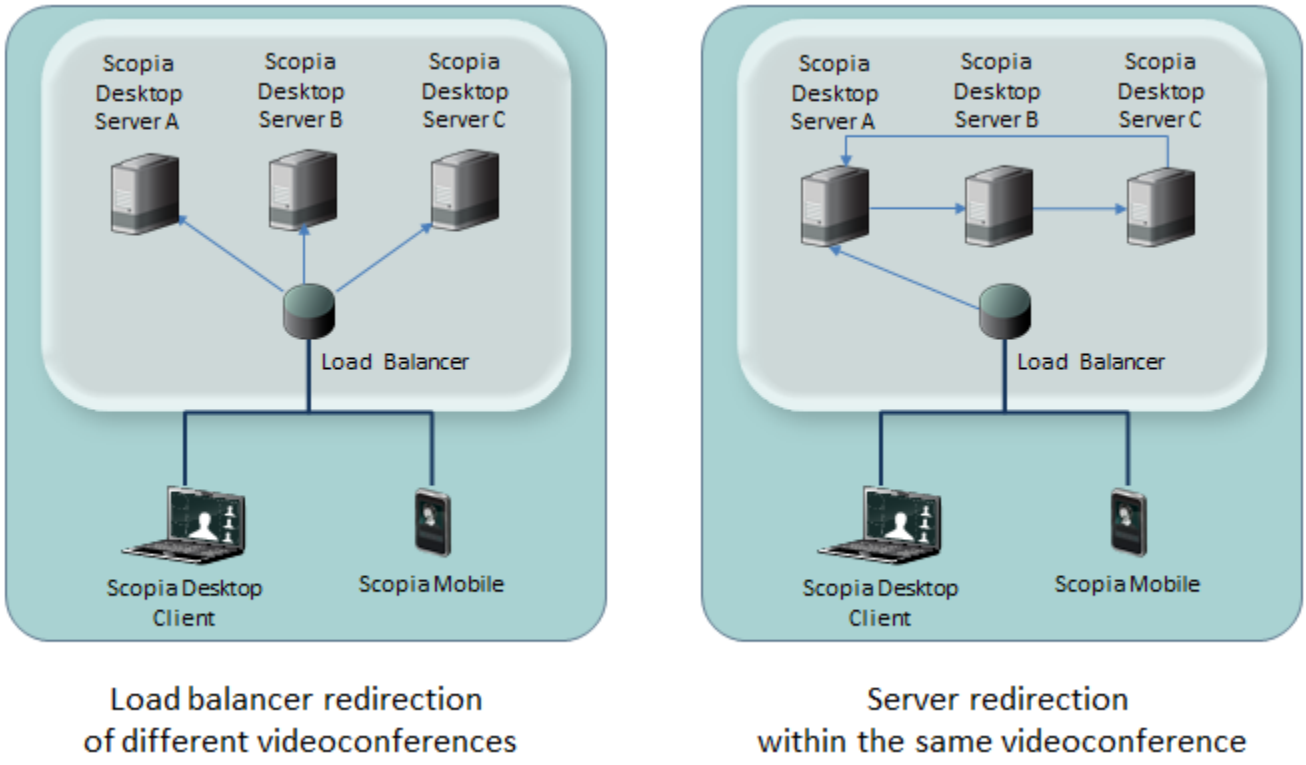


Figure 70: Redirecting participants in a load balanced environment

1. If server A is out of resources for the same videoconference, redirect participants to server B.
2. If server B is out of resources for the same videoconference, redirect participants to server C, and so on.

The Scopia® Solution allows both registered participants and guests to join a videoconference. To further improve registered user experience, all servers in the group must share the meeting login of registered users. Otherwise, participants might have to re-enter their credentials when the load balancer routes calls to other servers in the farm. Therefore, enable the underlying Tomcat clustering in each Scopia® Desktop server (About Components of the Scopia® Desktop server on page 9), so participants enter their username and password only once when they join the videoconference.

Important:

If all participants are guests with no logins, you do not need to set up Tomcat clusters.

This procedure describes how to configure Scopia® Desktop server redirection for participants within the same videoconference, for deployment with any type of load balancer.

Before you begin

1. Plan your load balancer deployment as part of your overall topology. For more information, see Planning your Avaya Scopia® Desktop Deployment on page 13.
2. Configure the Scopia® Desktop server's basic settings as described in Configuring Core Features of Scopia® Desktop server on page 45.

3. Read the overview on load balancing in the Scopia® Desktop deployment.
4. Remember to back up any settings file which you edit as part of this procedure.

Procedure

1. Open the *ctmx.ini* file located in *<install directory>\data*
2. Locate the `[redundancy]` section of the file (Figure 71: The redundancy section in the ctmx.ini file on page 105).

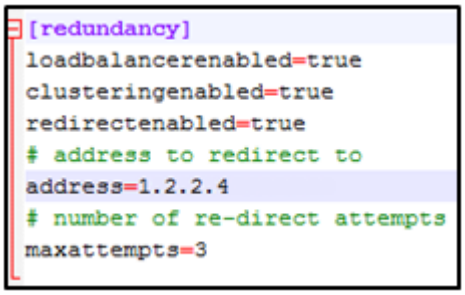


Figure 71: The redundancy section in the ctmx.ini file

3. Set `loadbalancerenabled` to `true` (Figure 71: The redundancy section in the ctmx.ini file on page 105).
4. Set `redirectenabled` to `true` (Figure 71: The redundancy section in the ctmx.ini file on page 105).
5. In the `address` line, enter the address (either IP or FQDN) of the server to which the system redirects a participant of the same call when this server is full. Redirect each server to the next one in line (Figure 70: Redirecting participants in a load balanced environment on page 104). You must specify only one redirection address in each server.

   For example, the server's address can be an IP address (`address=1.2.2.4`), an FQDN (`address=sds.company.com`) or an IP with port number (`address=1.2.2.4:8080`).
6. Enter the maximum number of redirections in `maxattempts` (Figure 71: The redundancy section in the ctmx.ini file on page 105). Keep this number consistent in all the servers across the deployment to ensure a predictable redirection behavior.

   To prevent an infinite loop, limit the total number of redirections to the total number of Scopia® Desktop servers in the deployment.
7. (Required only if you have registered Scopia® Desktop Client users with usernames and passwords.) Enable Tomcat clustering in Scopia® Desktop server with full memory replication of sessions. For more information, see http://tomcat.apache.org.
   a. In the same `[redundancy]` section, set `clusteringenabled` to `true` (Figure 71: The redundancy section in the ctmx.ini file on page 105).
   b. Save and close the *ctmx.ini* file.
   c. Open the *server.xml* file located in *<install directory>\tomcat\conf*
   d. Locate the text `<Cluster`(without the close bracket '>').

e. Verify this line is not commented out by removing the surrounding comment indicators (<!-- and -->).

f. Replace that element with the following code:

```
<Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"
channelSendOptions="8">
  <Manager className="org.apache.catalina.ha.session.DeltaManager"
             expireSessionsOnShutdown="false"
notifyListenersOnReplication="true"/>
  <Channel className="org.apache.catalina.tribes.group.GroupChannel">
    <Membership className="org.apache.catalina.tribes.membership.McastService"
address="228.0.0.4"
             bind="NIC IP" port="45564" frequency="500" dropTime="3000"/>
    <Receiver className="org.apache.catalina.tribes.transport.nio.NioReceiver"
             address="NIC IP" port="4000" autoBind="100" selectorTimeout="5000"
maxThreads="6"/>
    <Sender
className="org.apache.catalina.tribes.transport.ReplicationTransmitter">
      <Transport
className="org.apache.catalina.tribes.transport.nio.PooledParallelSender"/>
    </Sender>
    <Interceptor
className="org.apache.catalina.tribes.group.interceptors.TcpFailureDetector"/>
    <Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDispatch15Interce
ptor"/>
  </Channel>
  <Valve className="org.apache.catalina.ha.tcp.ReplicationValve" filter=""/>
  <Valve className="org.apache.catalina.ha.session.JvmRouteBinderValve"/>
  <Deployer className="org.apache.catalina.ha.deploy.FarmWarDeployer"
tempDir="/tmp/war-temp/"
             deployDir="/tmp/war-deploy/" watchDir="/tmp/war-listen/"
watchEnabled="false"/>
  <ClusterListener
className="org.apache.catalina.ha.session.JvmRouteSessionIDBinderListener"/>
  <ClusterListener
className="org.apache.catalina.ha.session.ClusterSessionListener"/>
</Cluster>
```

Important:

Clustered Tomcat servers communicate with each other via multicasting. If servers within the cluster are separated by routers, switches, firewalls or other network devices, you must configure them to forward multicast traffic.

Clustered Tomcat servers broadcast and listen on a default IP address of 228.0.0.4, much like a radio transceiver broadcasts and receives on a frequency. This underlying communication is distinct and separate from multicast videoconference streams, which you would configure in the Scopia® Desktop server.

g. Replace both mentions of ***NIC IP*** in the above code with the IP address of the network port of this Scopia® Desktop server.

If you enabled both network ports (dual-NIC) on this server, each belonging to a different subnet, replace both mentions of ***NIC IP*** with the address of the NIC whose subnet contains all the cluster servers. All the servers in the cluster must belong to the same subnet.

h. Save and close the file.

i. Open the *web.xml* file located in *\tomcat\webapps\scopia\WEB-INF*

j. Add a new line before the `</web-app>` line and enter `<distributable/>` in the line.

   This allows the server to distribute session information to other servers in the cluster.

k. Save and close the file.

l. Open the *context.xml* file in *\tomcat\conf* and locate the line containing `<Manager pathname="" />`. Verify the line is commented, or delete it.

m. Save and close the file.

8. Restart the **Scopia® Desktop– Apache Tomcat** service.
9. Repeat the above procedure for each Scopia® Desktop server in the group.
10. (Optional) To verify whether the cluster is correctly configured on all the servers, you can perform your own stress tests and capture network traces using the Wireshark filter `ip.dst filter==228.0.0.4` which presents the cluster's synchronization traffic (or "heartbeat").

    For example, enter the filter to verify that each server in the cluster broadcasts a message every 0.5 seconds to the specified IP address (Figure 72: Capturing network traces on page 107).

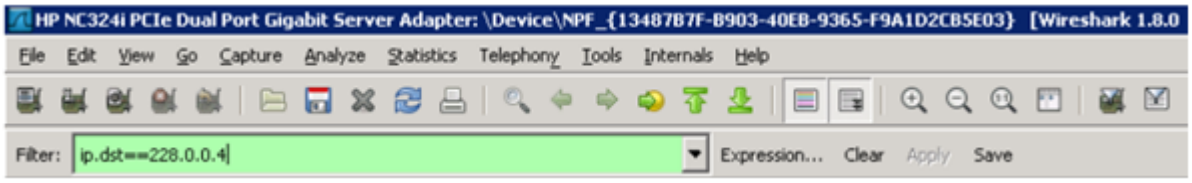


Figure 72: Capturing network traces

11. Configure the load balancer used in your deployment (see Configuring Radware AppDirector on page 107 or Configuring Other Load Balancers on page 115).

Related Links

Deploying Multiple Scopia® Desktop servers with a Load Balancer on page 102
Configuring Radware AppDirector on page 107

Configuring Radware AppDirector

About this task

For scalability and high availability you can cluster multiple Scopia® Desktop servers behind a load balancer such as Radware's AppDirector.

You can configure AppDirector to route all network traffic or part of it (Figure 73: Media can either bypass or travel via the load balancer on page 108) depending on your deployment requirements:

- 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.

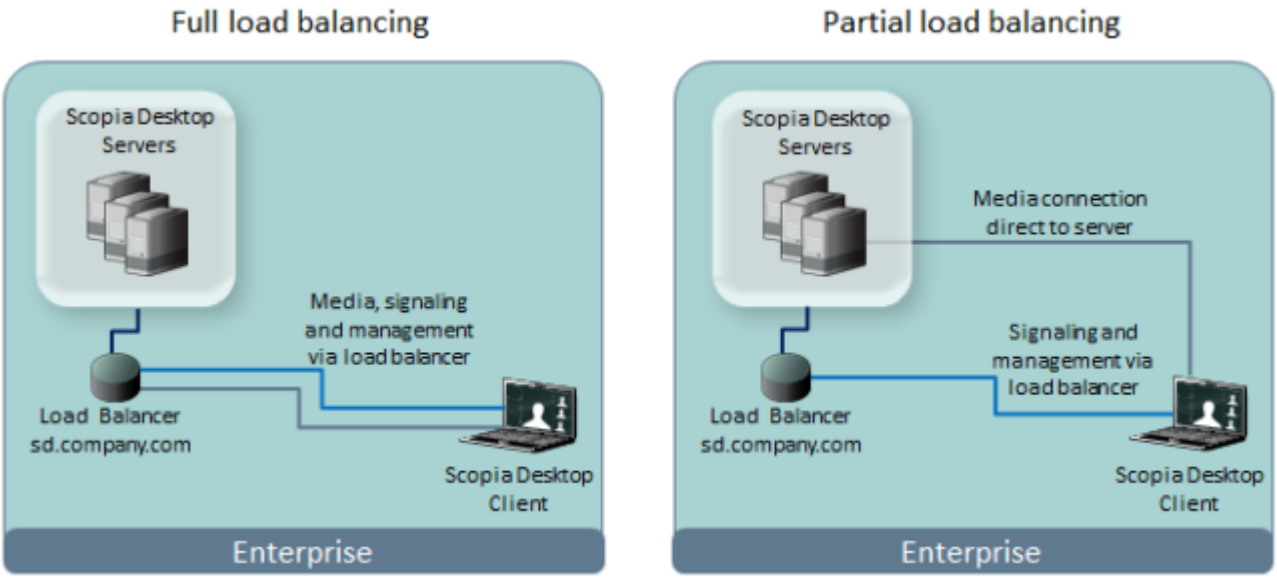


Figure 73: Media can either bypass or travel via the load balancer

Important:

You can set up your load balancer so the servers route everything via the load balancer, by defining the Scopia® Desktop server default gateway to be the load balancer. If you deploy servers whose only connection to the network is via the load balancer, then clearly there is no way for the media to bypass the load balancer.

This procedure describes how to configure AppDirector for a Scopia® Desktop deployment. For complete flexibility in AppDirector configuration, see AppDirector's documentation.

Important:

Only system integrators familiar with AppDirector should configure the load balancer.

Before you begin

1. Plan your load balancer deployment as part of your overall topology. For more information, see Planning your Avaya Scopia® Desktop Deployment on page 13.
2. Configure the Scopia® Desktop server's basic settings as described in Configuring Core Features of Scopia® Desktop server on page 45.
3. Read the overview on load balancing in the Scopia® Desktop deployment.
4. Follow the procedure in Configuring Scopia® Desktop server for Load Balancing on page 103 to configure settings on each Scopia® Desktop server.

Procedure

1. Login to AppDirector.

2. Configure the server farm in the load balancer. The farm is the AppDirector's terminology of a cluster of servers. It is a virtual entity that integrates one or more physical servers.
   a. Create a farm by selecting **AppDirector** > **Farms** > **Farm Table** > **Create**.
   b. Enter the basic settings for this server farm (Figure 74: Configuring the virtual farm on page 109 and Table 25: The virtual farm settings on page 109).

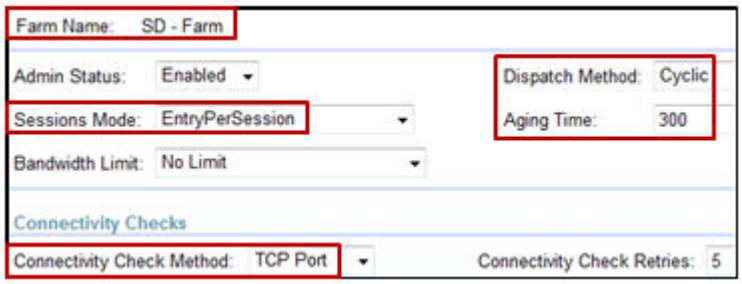


Figure 74: Configuring the virtual farm

Table 25: The virtual farm settings

Field Name	Description
Farm Name	Server farm name
Aging Time	Indicates the number of seconds before the Scopia® Desktop Client connection is timed out (disconnected). Set the aging time to a high value (for example, *90000*). Within that period of time, AppDirector routes the re-connecting client to that specific server.
Dispatch Method	Select the method the load balancer uses for distributing traffic among servers in this farm. For example, select **Cyclic** for the load balancer to direct traffic to each server in a round robin mode.
Sessions Mode	Select **EntryPerSession** for the load balancer to route packets from the same client to the same server throughout the duration of the videoconference.
Connectivity Check Method	Select **TCP Port** for AppDirector to check the Scopia® Desktop server availability during the videoconference.

3. Configure the Layer 4 rules (or policies) the load balancer uses to manage traffic. AppDirector uses the Layer 4 protocol and the request's destination port to select the farm.
   a. Create a policy by selecting **AppDirector** > **Layer 4 Traffic Redirection** > **Layer 4 Policies** > **Create**.
   b. Enter the basic settings for this policy (Figure 75: Configuring the Layer 4 Policies on page 110 and Table 26: The Layer 4 Policy settings on page 110).

Figure 75: Configuring the Layer 4 Policies

Table 26: The Layer 4 Policy settings

Field Name	Description
L4 Policy Name	Policy name
Virtual IP	Farm's virtual IP address. The load balancer uses the virtual IP to act as a single server to other components in the deployment.
L4 Protocol	Select **Any** for the Layer 4 traffic policy to support any IP protocol including TCP and UDP.
Farm Name	Select the name of the farm you previously created.

c. Configure the farm's virtual IP in the organization's firewalls to ensure communication with the farm.

4. (Optional) If you want the media traffic (audio, video, presentation data) to bypass the load balancer, verify the client NAT feature on the load balancer is disabled (default setting). The client NAT would re-route traffic destined for the Scopia® Desktop Client to go via the load balancer. Therefore to bypass it, client NAT must be disabled.

   a. Verify the **Client NAT** in **AppDirector** > **NAT** > **Client NAT** > **Global Parameters** is disabled (Figure 78: Enabling Client NAT on page 111).

Figure 76: Disabling Client NAT

   b. Configure Scopia® Desktop server to send its individual IP address (or FQDN) to Scopia® Desktop Clients, not its virtual IP address, so media can be sent directly between the client and server, bypassing the load balancer.

      In the Scopia® Desktop server's administration web interface, navigate to **Client** > **Connection Information**.

Figure 77: Configuring direct media traffic between client and server

c. Enter this server's IP address, not the virtual IP address. It sends this address to the client at call setup, so both client and server can route media traffic directly between them.

5. (Optional) If you want the media traffic (audio, video, presentation data) to route via the load balancer, enable the client NAT feature on the load balancer. Client NAT re-routes traffic destined for the Scopia® Desktop Client to go via the load balancer.

   a. Enable **Client NAT** in **AppDirector** > **NAT** > **Client NAT** > **Global Parameters** (Figure 78: Enabling Client NAT on page 111).

Figure 78: Enabling Client NAT

   With Client NAT enabled, the load balancer replaces Scopia® Desktop Client's IP address with the load balancer's IP address. The server uses this address to send replies to clients.

   b. Configure the range of client IP addresses on which the system performs NAT by selecting **Client NAT Intercept Table** (Figure 79: The Client NAT Intercept Table on page 111).

Figure 79: The Client NAT Intercept Table

   c. Configure the NAT IP addresses in **Client NAT Address Table** (Figure 80: The Client NAT Address Table on page 112). The load balancer replaces the client IP address calling into the farm with the load balancer IP address. Usually you configure both fields to the same IP address (the load balancer's IP address).

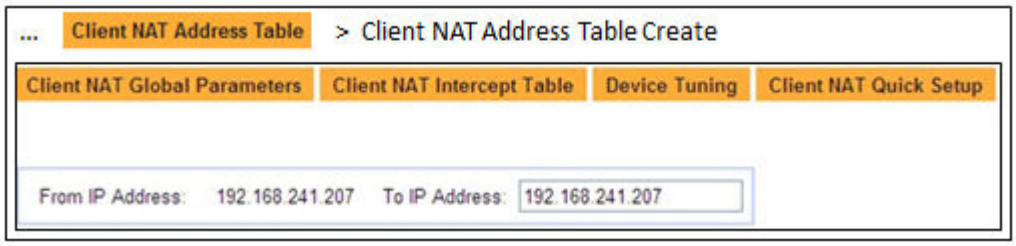


Figure 80: The Client NAT Address Table

d. Configure the Client NAT's basic settings in **Client NAT Quick Setup** (Figure 81: The Client NAT Quick Setup window on page 112.

Figure 81: The Client NAT Quick Setup window

Fill the fields as described in Table 27: The Client NAT Quick Setup settings on page 112.

Table 27: The Client NAT Quick Setup settings

Field Name	Description
Client NAT Range	Select the IP address in the list of configured Client NAT ranges.
Farm	Select the farm for which Client NAT is performed.
Apply for all client source IP addresses	Select to indicate the load balancer performs this IP replacement (re-routing) for all clients calling into this load balancer.

e. Configure Scopia® Desktop server to send the virtual IP address of the farm to Scopia® Desktop Clients, so media can be sent via the load balancer.

In the Scopia® Desktop server's administration web interface, navigate to **Client** > **Connection Information**.

Figure 82: Routing media traffic through the load balancer

f. Enter the farm's virtual IP address. Scopia® Desktop server sends this address to clients at call setup, so both client and server can route media via the load balancer.

6. Add each Scopia® Desktop server to the farm.

   a. Enter the server details in **AppDirector** > **Servers** > **Application Servers** > **Table** > **Create** (Figure 83: Configuring the server table on page 113 and Table 28: The server table settings on page 113).

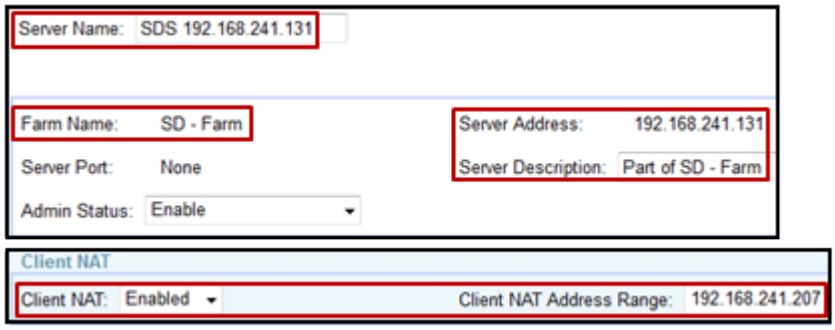


Figure 83: Configuring the server table

Table 28: The server table settings

Field Name	Description
Server Name	Scopia® Desktop server name
Farm Name	Select the name of the newly created farm.
Server Address	IP address of the Scopia® Desktop server
Server Description	A short text describing the Scopia® Desktop server
Client NAT	Set to **Enabled** when routing media as well as signaling through the load balancer.
Client NAT Address Range	Select the configured client NAT address.

   b. Repeat these steps for each Scopia® Desktop server in the farm.

7. Configure cookie persistency in the load balancer.

   The persistency rule routes clients of the same videoconference to the same server. The rule examines the HTTP persistent cookie sent by Scopia® Desktop Clients. The cookie has the format `CONFSESSIONID = <meeting number>`.

   a. Create the persistency rule in **AppDirector** > **Layer 7 Server Persistency** > **Text Match** > **Create**.

   b. Enter the rule's basic settings (Figure 84: Configuring session persistency on page 114 and Table 29: The session persistency settings on page 114).

Figure 84: Configuring session persistency

Table 29: The session persistency settings

Field Name	Description
Farm Name	Select the name of the farm grouping Scopia® Desktop servers.
Lookup Mode	Select **Cookie**. Configure the cookie name in the **Persistency Parameter** field.
Persistency Parameter	Enter *CONFSESSIONID*. The cookie is case sensitive.
Inactivity Timeout [sec]	Indicates how long AppDirector keeps linking a meeting ID to a specific server after the videoconference becomes inactive. If a client connects again within that period of time, AppDirector routes it to that specific server.
Learning Direction	Select **Client Request** for AppDirector to inspect the client request only for the HTTP persistent cookie.
Ignore Source IP	Select **Enabled** so AppDirector uses the meeting ID to forward the same videoconference to the same server.

Related Links

Deploying Multiple Scopia® Desktop servers with a Load Balancer on page 102
Configuring Scopia® Desktop server for Load Balancing on page 103
Configuring Other Load Balancers on page 115

Configuring Other Load Balancers

About this task

For scalability and high availability you can cluster several Scopia® Desktop servers behind a non-Radware load balancer. This allows continued service even when one or more of the servers fails.

This procedure describes how to configure load balancers other than AppDirector to correctly route calls to the Scopia® Desktop servers. If your deployment uses AppDirector, see Configuring Radware AppDirector on page 107.

Important:

Only experts familiar with the load balancing tool and HTTP protocol may set up this deployment.

Before you begin

- Plan your load balancer deployment as part of your overall topology. For more information, see Planning your Avaya Scopia® Desktop Deployment on page 13.
- Configure the Scopia® Desktop server's basic settings as described in Configuring Core Features of Scopia® Desktop server on page 45.
- Read the overview on load balancing in the Scopia® Desktop deployment.

Procedure

1. Define the load balancer settings, including defining the servers, their cluster or group name, and their virtual IP (VIP) address.

   Scopia® Desktop Clients use the VIP to reach that cluster.

2. Select a routing method for the load balancer.

   To optimize resource utilization, load balancers use different methods for rotating the load of calls among servers in the deployment. We tested load balancing with the round-robin method which ensures good load balancing and is widely used in the videoconferencing industry.

3. Configure a persistency rule in the load balancer so all the clients belonging to the same meeting are routed to the same server.

   The rule must examine the HTTP persistent cookie sent by Scopia® Desktop Clients. The cookie has the format `CONFSESSIONID = <meeting number>`.

   If an HTTP request arrives from the client and contains an HTTP cookie with a CONFSESSIONID key, the persistency rule must route as follows:

   - If the load balancer has previously routed an HTTP request with this cookie to a specific server, it must route the new request to the same server.
   - If the load balancer did not yet encounter a cookie with this value, it must route the request to the next available server and learn this cookie.

Important:

If you do not define these rules, the system uses ports less efficiently. In addition, some moderation features (such as muting participants) may fail. We strongly recommend to verify correct routing using a network tracing tool such as Wireshark.

4. Set the aging time of the persistency rule to a high value.

   The aging time indicates how long the load balancer keeps linking a meeting ID to a specific server after the videoconference becomes inactive. If a participant connects again to that videoconference within the specified period of time, the load balancer routes the call to that same server.

Related Links

Deploying Multiple Scopia® Desktop servers with a Load Balancer on page 102
Configuring Radware AppDirector on page 107
Securing a Load Balanced Environment on page 116

Securing a Load Balanced Environment

You can route the media of a videoconference via the load balancer if its computer is powerful enough, or the media can bypass the load balancer creating a direct flow from the server to the Scopia® Desktop Client (see Configuring Radware AppDirector on page 107).

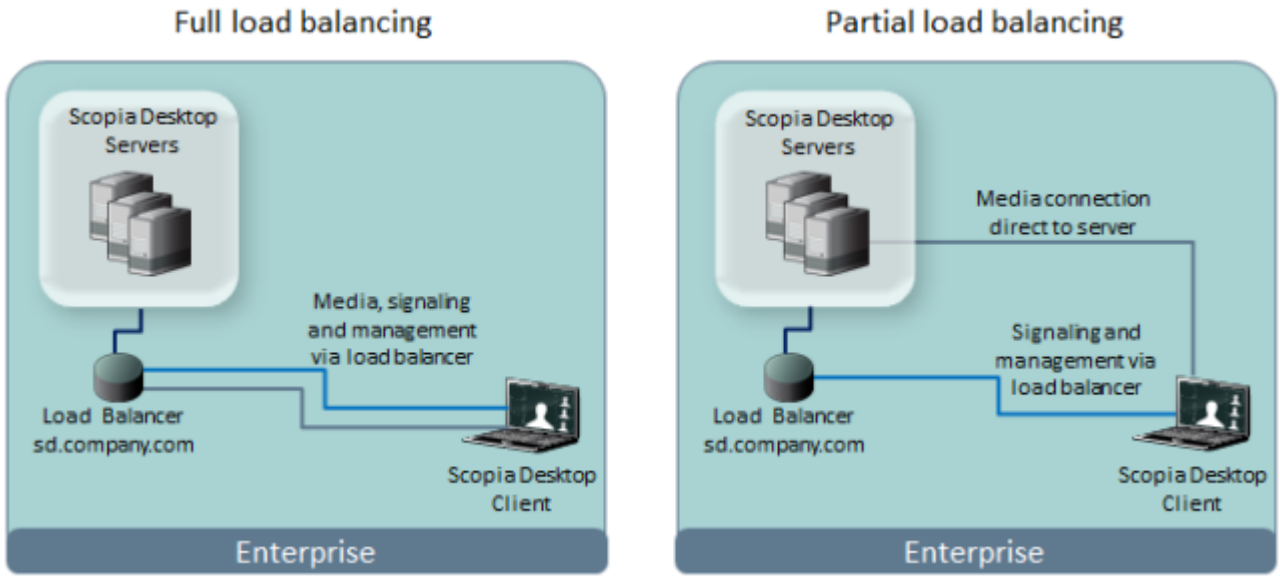


Figure 85: Media can either bypass or travel via the load balancer

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).

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.

- When media flows via the load balancer, install the Scopia® Desktop server certificates on the load balancer only (Figure 86: Encrypting communication with the load balancer certificate on page 117). If each server has its own certificate, install all of them on the load balancer. If they all share the same certificate, you only need to install it once.

  For more information on installing certificates on your load balancer, see the load balancer documentation.

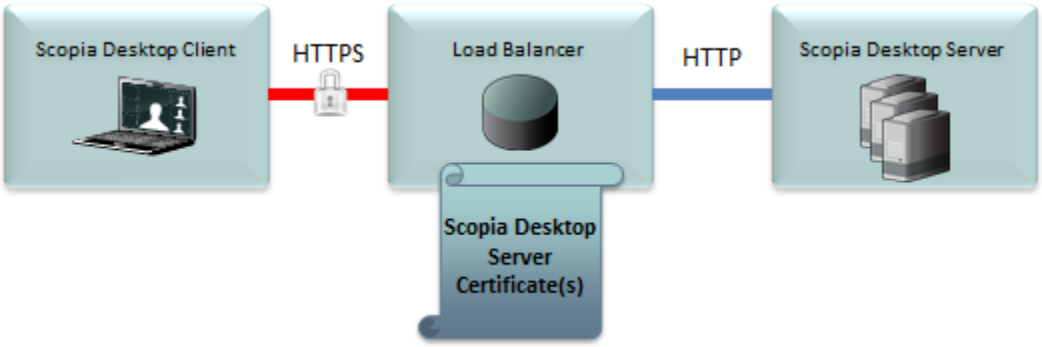


Figure 86: Encrypting communication with the load balancer certificate

- When media flows directly between client and server, bypassing the load balancer, install certificates both on the load balancer and the servers in the cluster (Figure 87: Encrypting communication with the load balancer and server certificates on page 117). As with the previous example, if all servers in the cluster share the same certificate, you only need to install that single certificate on the load balancer.

  For more information on installing Scopia® Desktop server certificates, see Securing Your Scopia® Desktop Deployment on page 84. To install certificates on your load balancer, see the load balancer documentation.

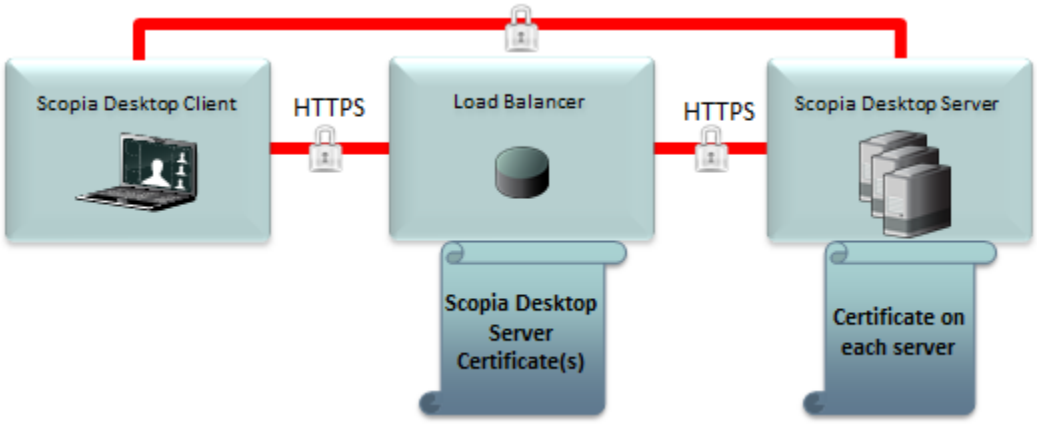


Figure 87: Encrypting communication with the load balancer and server certificates

Important:

All servers in the deployment must be configured with the same functionality and the same security mode (http/https).

Related Links

Deploying Multiple Scopia® Desktop servers with a Load Balancer on page 102
Configuring Other Load Balancers on page 115

Chapter 8: Troubleshooting Scopia® Desktop server

Each of the following sections presents the symptoms of common problems that may occur during the use of the Scopia® Desktop. Recommended actions for each symptom are also provided. For more information related to known issues, see the *Scopia® Desktop Release Notes*.

When Scopia® Desktop is part of a service provider (multi-tenant) deployment, you can view the connection and communication status for each of your organizations to isolate possible problems. Select the organization whose connection status you want to check.

This section includes the following topics:

Related Links

Viewing Status of Servers and Directory on page 119
Changing the IP Address of the Scopia® Desktop server on page 124
Client -734 Error and other Certificate Problems on page 125
Troubleshooting Scopia® Mobile on page 126
Upgrading Scopia® Desktop server Recordings on page 126
Enabling a User to Sign In on page 127

Viewing Status of Servers and Directory

Viewing the status of your Scopia® Desktop deployment is a helpful way to assess resource availability and troubleshoot connectivity problems. The following sections provide useful information for utilizing the View Status functionality of Scopia® Desktop.

Related Links

Troubleshooting Scopia® Desktop server on page 119
Viewing Server Status and Port Resource Usage on page 120
Viewing Directory Status on page 122
Viewing Content Slider Status on page 123

Viewing Server Status and Port Resource Usage

About this task

Select **Status** in the sidebar and select the **Scopia® Desktop** tab to view the status information about the Scopia® Desktop server and other connected video network devices.

Figure 88: Component Status

The **Scopia® Desktop Components** section includes the IP address and status of the following video network devices:

- **Scopia® Management** when Scopia® Management manages the Scopia® Desktop server.
- **Gatekeeper** when the server is registered to the built-in gatekeeper in Scopia® Management or the standalone Avaya Scopia® ECS Gatekeeper.
- **Scopia® MCU** if the Scopia® Desktop server is managed by an MCU rather than Scopia® Management.
- **Sametime Server** if the Scopia® Desktop server is configured to work with IBM Lotus Sametime Web.

The indicator next to each link shows whether or not the connection to the target device or registration with the gatekeeper is successful. When the indicator is red, hover the mouse pointer over the icon to view the error details. Select the red indicator to view further error information.

The **Scopia® Desktop** tab also shows port usage statistics and presents port usage graphically.

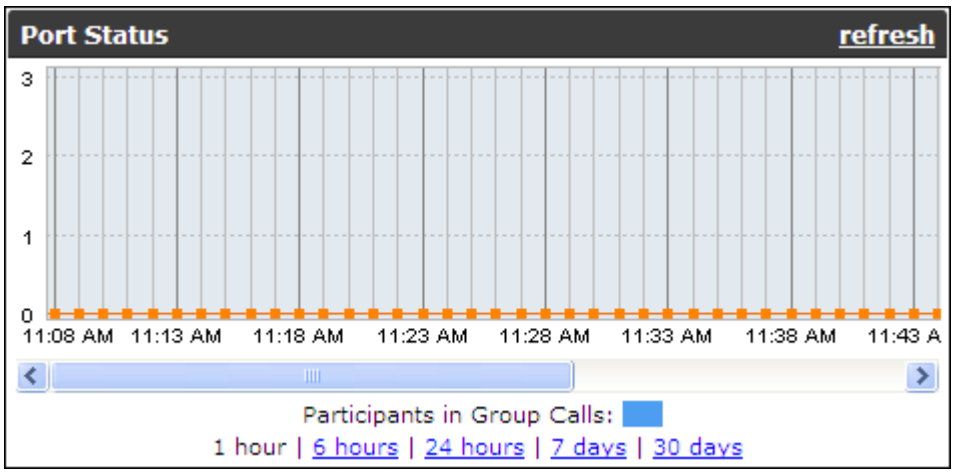


Figure 89: Port Status Graph

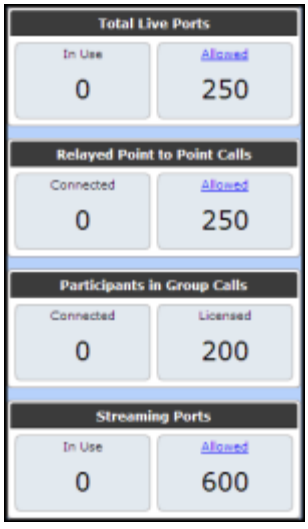
Depending on your needs you may choose one of the graph reports described in Viewing Server Status and Port Resource Usage on page 120.

Important:

We recommend waiting several minutes before refreshing the status information to view the updated port information.

Depending on the deployment the **Status** > **Scopia® Desktop** tab also displays additional statistics:

- For deployment without Scopia® Management
  - Number of participants in group calls
- For advanced deployments
  - Number of total live ports
  - Number of participants in group calls



If calls exceed the maximum allowed, the number of connected participants appears in red, with a warning that **Usage has exceeded the maximum allocated resources**.

If you set the call limit to a number lower than defined by the license, an error message is displayed next to the number of participants in group calls.

Related Links

Viewing Status of Servers and Directory on page 119

Viewing Directory Status

About this task

In deployments where Scopia® Desktop is configured to work with Scopia® Management, Scopia® Desktop server must synchronize with Scopia® Management to download information about users, virtual rooms, and global policy. Scopia® Desktop server synchronizes with Scopia® Management when it connects to it for the first time; then Scopia® Management updates Scopia® Desktop server each time there is new or modified information. These are the following synchronization states:

Field	Description
Synchronized	Scopia® Desktop server is synchronized with Scopia® Management.
Synchronizing	Scopia® Desktop server is caching information from Scopia® Management. You cannot search for users or endpoints in the Contact List or in the **Invite** dialog box.
Not Synchronized	Scopia® Desktop server uses locally cached information. During this time you can only login if the Integrated Windows Authentication (IWA) is enabled.
Synchronization error	Scopia® Desktop server is not synchronized with Scopia® Management, and no information is cached. This limits functionality until the synchronization issue is resolved.

Select **Status** > **Directory** to display an organization's directory information, defined in Scopia® Management.

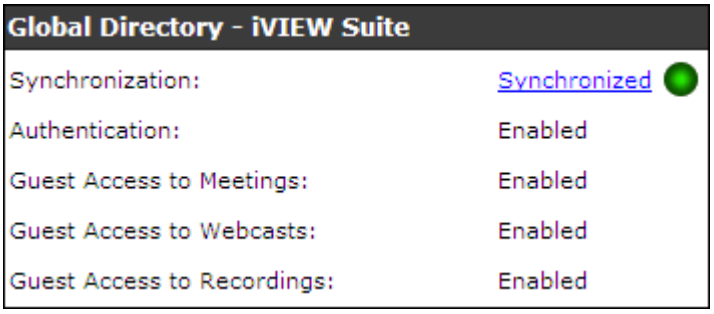


Figure 90: Viewing the directory status of an organization

In service provider (multi-tenant) deployments, view the status of each organization in your deployment by selecting it in the **Organization** field (Figure 91: Viewing the directory status of a company pertaining to multi-tenant deployment on page 123).

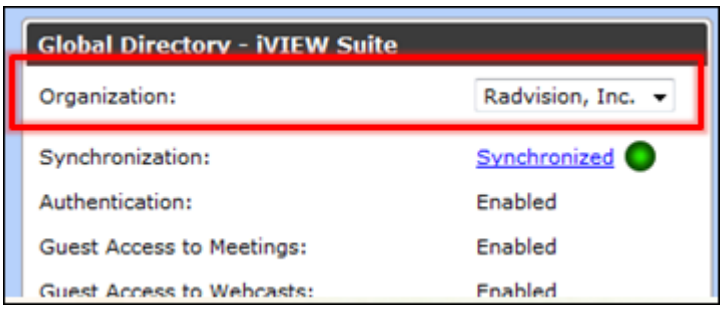


Figure 91: Viewing the directory status of a company pertaining to multi-tenant deployment

You can also view the maximum call rate value. This setting is configured in Scopia® Management.

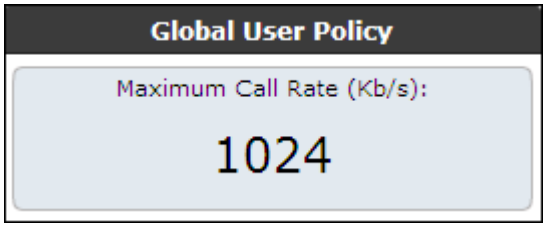


Figure 92: Viewing the maximum call rate policy

Related Links

Viewing Status of Servers and Directory on page 119

Viewing Content Slider Status

About this task

You can view the Content Server status information only if recording is enabled in your deployment.

The **Content Slider** tab displays the connection information and the number of ongoing sessions. You can use this panel to verify connection status and help troubleshoot problems.

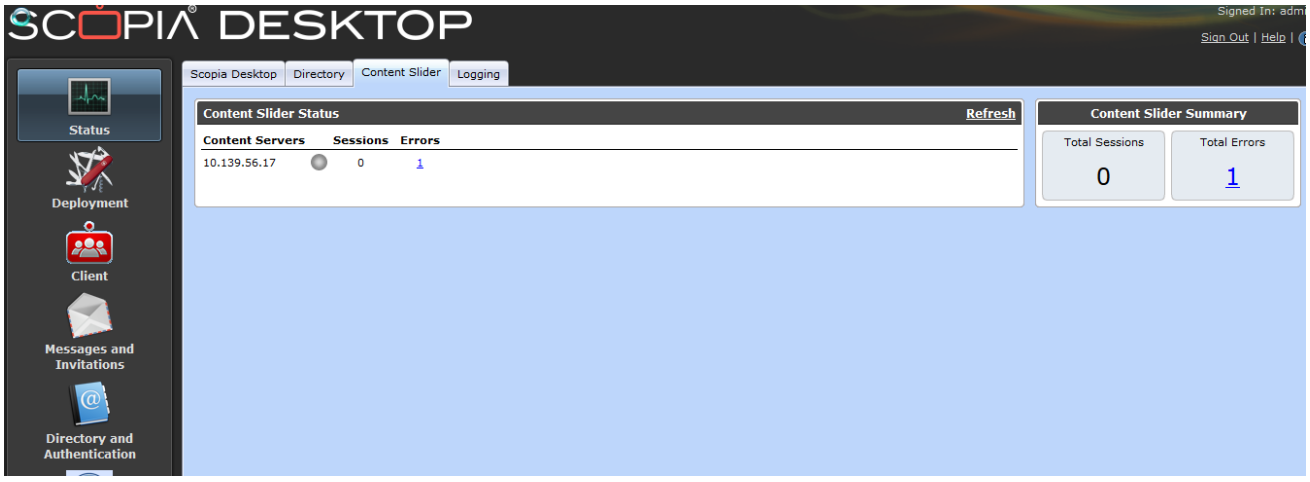


Figure 93: Status of Content Slider

Review the status as detailed in Table 30: Content Slider status fields on page 124.

Table 30: Content Slider status fields

Field	Description
Recording Servers	Displays the address of the Scopia® Desktop Recording Server.
Sessions	Displays the number of slider sessions currently in progress, with details on the server(s) that have sessions.
Problems	If there are problems with slider sessions, they appear per server in the **Problems** column. To view details, select the number of problems for that server. The system displays the date and time of the problem and a brief summary of the problem details. To view more information, select the problem summary.

Related Links

Viewing Status of Servers and Directory on page 119

Changing the IP Address of the Scopia® Desktop server

Problem

The **Status** > **Scopia® Desktop** tab indicates the Scopia® Desktop server is not connected.

Cause

If the IP address of the Scopia® Desktop server computer has changed, you must update Scopia® Desktop server components with its new IP address.

Solution

The installation process automatically detects the IP of the computer.

1. Select **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**.
2. From the list of programs, choose Scopia® Desktop, and then **Change**.

   The Setup Wizard opens.
3. In the **Welcome** screen select **Next**.
4. In the **Program Maintenance** screen, select **Modify**, then select **Next**.
5. In the **Custom Setup** screen, select **Next**.
6. In the **Scopia® Desktop Serial Key** screen, select **Next**.

7. In the **Scopia® Desktop Network Configuration** screen, it will automatically detect the current IP address of the server. Select **Next**.
8. In the **Scopia® Desktop Hostname Configuration** screen, select **Next**.
9. In the **Scopia® Desktop Recording Configuration** screen, select **Next**.
10. Select **Install**.

Related Links

Troubleshooting Scopia® Desktop server on page 119

Client -734 Error and other Certificate Problems

Problem

The client issues a -734 error, and the client call log states:

```
get_verify_result error = 19, the peer certificate is invalid
```

In cases of an incorrect Scopia® Desktop server certificate setting, the Scopia® Desktop Client returns errors 21 or 26.

Cause

The Scopia® Desktop Client is attempting to connect to the Scopia® Desktop server when the connection is encrypted but the server's certificate is signed by an unknown (untrusted) CA.

Solution

Install the root CA certificate on the Scopia® Desktop Client computer using the standard Microsoft Management Console.

1. Obtain the root certificate of the CA used to sign the certificate on the Conference Server.
2. Launch the Microsoft Management Console.
3. Select **File** > **Add/Remove Snap-in**.
4. Select **Add**.
5. Select **Certificates**, and then select **Add**.
6. Select **Computer Account** in the **Certificates snap-in** window, and then select **Next**.
7. Select **Local computer (the computer this console is running on)**, and then select **Finish**.
8. Select **Close** and **OK**.
9. Verify that the console shows the **Certificates (Local Computer)** in the main console window's left hand pane.
10. Expand the entry **Certificates (Local Computer)** and navigate to **Certificates (Local Computer)** > **Trusted Root Certification Authorities** > **Certificates**.
11. Right-click **Certificates** and select **All Tasks** > **Import**.
12. Select **Next**.

13. Select **Browse**, and select the signed certificate file you want to upload.

    By default the file type in the browse window is set to show only X.509 Certificates. Change this to Personal Information Exchange (*.pfx;*.p12) or All Files (*.*), and select **Next**.
14. Select **Place all certificates in the following store**, and then verify that the **Certificate store: Trusted Root Certification Authorities** option is selected.
15. Select **Next**.
16. Verify the information and select **Finish**.
17. Verify that the Certificate Chain is located in the **Trust Root Certification Authorities** store.

Related Links

Troubleshooting Scopia® Desktop server on page 119

Troubleshooting Scopia® Mobile

If Scopia® Mobile stops running (or crashes), a crash report is generated and copied to the computer the next time the device is synchronized with iTunes.

Two files are generated for each crash: *.crash* and *.plist*. You can find them in these locations, depending on the computer you are using:

- On an OSX device, search in *~/Library/Logs/CrashReporter/MobileDevice/<device_name>/SCOPIAMobile**
- On Windows Vista/Windows 7, search in *%APPDATA%\Roaming\Apple Computer\Logs\CrashReporter\MobileDevice\<device_name>\SCOPIAMobile**
- On Windows XP, search in *%APPDATA%\Apple Computer\Logs\CrashReporter\MobileDevice\<device_name>\SCOPIAMobile**

Related Links

Troubleshooting Scopia® Desktop server on page 119

Upgrading Scopia® Desktop server Recordings

About this task

If there are recordings created using Scopia® Desktop server version 5.x, upgrade them by performing these steps:

Important:

You can upgrade recordings at any time.

Procedure

1. Install QuickTime version 7.6.2 or higher. You can download QuickTime athttp://www.apple.com/quicktime/download/.
2. On the Scopia® Desktop server, navigate to the <INSTALLDIR>\config location.
3. Double-click the recording_converter.exe file.
4. Follow the on-screen instructions. Depending of the size and amount of recordings, the upgrade may take time.
5. The recordings are converted and the log files are created in this folder.
6. Verify that the recordings are converted correctly.
7. Delete backed up recordings.

Related Links

Troubleshooting Scopia® Desktop server on page 119

Enabling a User to Sign In

Problem

A user cannot sign in.

Solution

Verify that the following problems do not interfere with user signing in:

- Authentication is turned off on Scopia® Management. In the Scopia® Desktop server Administrator web interface, select **Status** in the sidebar, and then select the **Directory** tab. Verify that authentication is enabled.

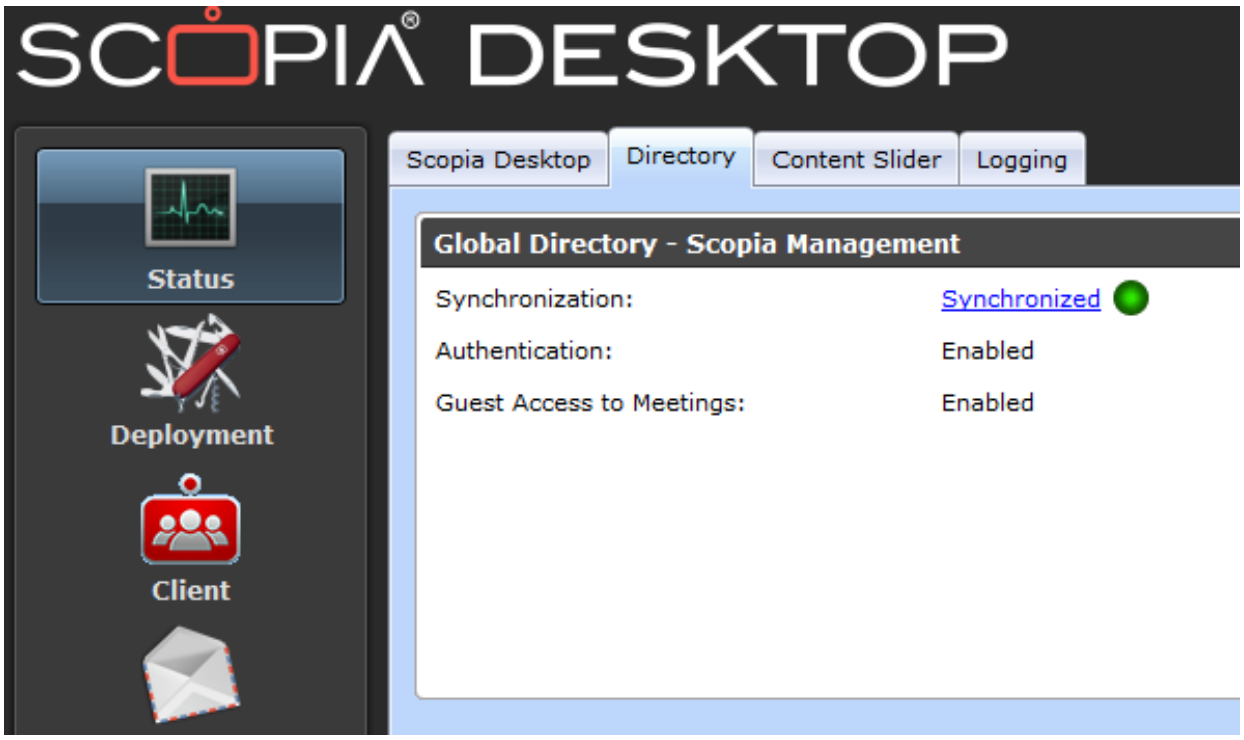


Figure 94: General User Policies

- This user does not have a Scopia® Desktop Pro license.
- If Scopia® Desktop is enabled for Integrated Windows Authentication and the user does not use a valid proxy account. In the Scopia® Desktop Administrator web interface, select **Directory and Authentication** in the sidebar, check the proxy account configured in the Integrated Windows Authentication area.

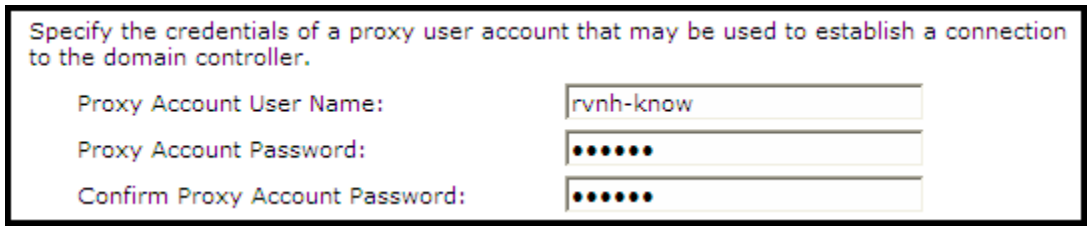


Figure 95: Proxy Account Settings

- If Scopia® Desktop is not enabled for Integrated Windows Authentication and uses Scopia® Management to authenticate, select **Status** in the sidebar and verify that Scopia® Desktop server is connected to Scopia® Management.

Figure 96: Scopia® Desktop and Scopia® Management Connectivity

Related Links

Troubleshooting Scopia® Desktop server on page 119

Glossary

1080p	See Full HD on page 134.
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 136.
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, also known as video IVR, offers quick access to meetings hosted on MCUs, via a set of visual menus. Participants can select menu options using standard DTMF tones (numeric keypad). Auto-Attendant works with both H.323 and SIP endpoints.
Avaya Scopia® Streaming and Recording Manager	The Avaya Scopia® Streaming and Recording Manager provides a web-based interface to configure and manage Scopia® Streaming and Recording server software, devices, services, and users. The Scopia® Streaming and Recording server Manager application resides on a single

	hardware platform and provides access to all content in the Scopia® Streaming and Recording server environment.
Avaya Scopia® Streaming and Recording Manager Portals	The Scopia® 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. The Manager also provides the Viewer portal. This portal is embedded within the Avaya Scopia® Desktop User portal. Use the User portal to schedule Scopia® Streaming and Recording server broadcasts.
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. In video recordings, the bitrate determines the file size for each minute of recording. Bitrate is often measured in kilobits per second (kbps).
Call Control	See Signaling on page 141.
Cascaded Videoconference	A cascaded videoconference is a meeting distributed over more than one physical Scopia® Elite MCU, where a master MCU connects to one or more slave MCUs to create a single videoconference. It increases the meeting capacity by combining the resources of several MCUs. This can be especially useful for distributed deployments across several locations, reducing bandwidth usage.
CDN	Scopia® SR 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 Scopia® 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 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.
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 132.
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, Scopia® XT Executive. It is listed in the organization's LDAP directory as associated exclusively with this user.
Delivery Node	The Avaya Scopia® 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). 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 Scopia® XT Executive, software endpoints like Scopia® Desktop Client, mobile device endpoints like Scopia® Mobile, room systems like XT Series, and telepresence systems like Scopia® XT Telepresence.
Endpoint Alias	See Alias on page 130.
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) 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 133.
FPS	See Frames Per Second on page 134.
Frame Rate	See Frames Per Second on page 134.
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. Scopia® Management includes a built-in Avaya Scopia® Gatekeeper, while ECS 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 TIP Gateway, or the Scopia® 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 135.

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 Scopia® 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 130.

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/NAT traversal, employing ITU-T standards. Endpoints which are already H.460 compliant can communicate directly with the PathFinder server, where the endpoint acts as an H.460 client to the PathFinder server which 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 136.

High Profile

See H.264 High Profile on page 135.

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 Scopia® Solution products.

Image Resolution

See Resolution on page 140.

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, IBM Sametime and others. 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.

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 Scopia® 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, Scopia® Management uses management messages to monitor the activities of an MCU, or when it authorizes the MCU 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 138.

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 132.
Meeting Type	Meeting types (also known as MCU 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 MCU, with additional properties in Scopia® 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 Scopia® Desktop server, endpoints like XT Series and other network devices like LDAP servers and 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, Scopia® 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 Scopia® 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 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 132.

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.
Scopia® Content Slider	See Content Slider on page 132.
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 service. See Meeting Type on page 138.
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 140.
SIP Server	A SIP server is a network device communicating via the SIP protocol.
SIP URI	See URI on page 144.
Slider	See Content Slider on page 132.
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 141.
Standard Definition	See SD on page 141.
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 Scopia® 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 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.
URI	URI is an address format used to locate a 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 Scopia® PathFinder server of the organization.
URI Dialing	Accessing a device via its URI on page 144.
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 144.
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 140.
Video Switching	See Switched video on page 143.
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 Scopia® 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 Scopia® 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 Scopia® 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 Scopia® 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 Avaya Scopia® ECS 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.