Avaya Scopia® Desktop Client User Guide

Release 8.3.3
For Solution 8.3 FP3
October 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.

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 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 with continuous presence, 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 8).

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 Components of Scopia® Desktop Client on page 9

About Components of Scopia® Desktop Client

Scopia® Desktop Client is a lightweight program that turns your PC and Mac into a videoconferencing endpoint. With Scopia® Desktop client you can experience high definition videoconferencing with continuous presence, 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 has several components (Figure 2: Components of Scopia® Desktop Client on page 10):

- The Scopia® Desktop videoconferencing window displays a virtual room containing the video images of participants and a presentation if it is being shared. You can also browse the list of participants, chat to others, control the video layout, and adjust volume and camera settings.
- The Scopia® Desktop system tray icon provides easy access to all components of the Scopia® Desktop Client.

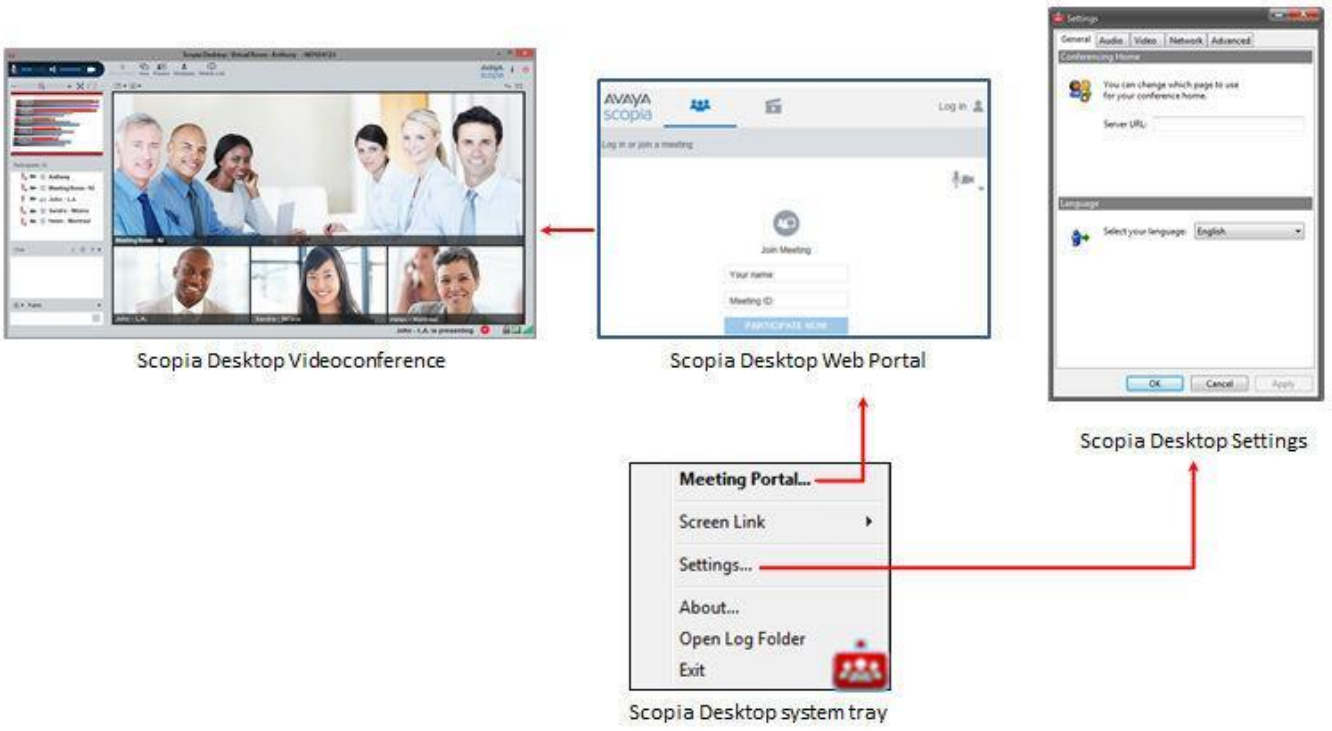


Figure 2: Components of Scopia® Desktop Client

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.

Related Links

About Scopia® Desktop Client on page 8

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 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: Getting Started with Scopia® Desktop Client

This section explains how to prepare your Scopia® Desktop Client for using it for the first time. Scopia® Desktop Client does not need any configurations to be used but there are some procedures that can make your videoconferencing experience better and to allow you to use the product's full functionality.

Related Links

Minimum Requirements for Scopia® Desktop Client on page 13 Installing Scopia® Desktop Client Locally on a PC on page 15 Accessing the Scopia® Desktop Web Portal on page 17 Logging in to the Scopia® Desktop Web Portal on page 18 Checking Audio and Video Configurations for your Scopia® Desktop Client on page 20 Customizing Your Virtual Room on page 23

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)

Important:

QuickTime 10 is not supported.

Related Links

Getting Started with Scopia® Desktop Client on page 13

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.
- 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*.

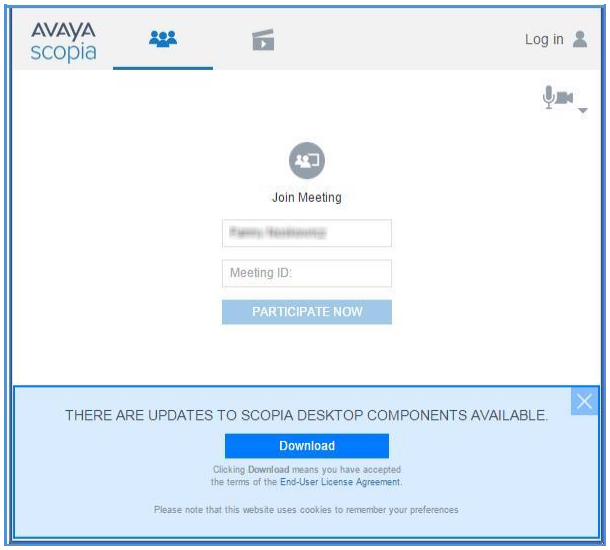


Figure 3: Installing Scopia® Desktop Client

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 Clientweb 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.

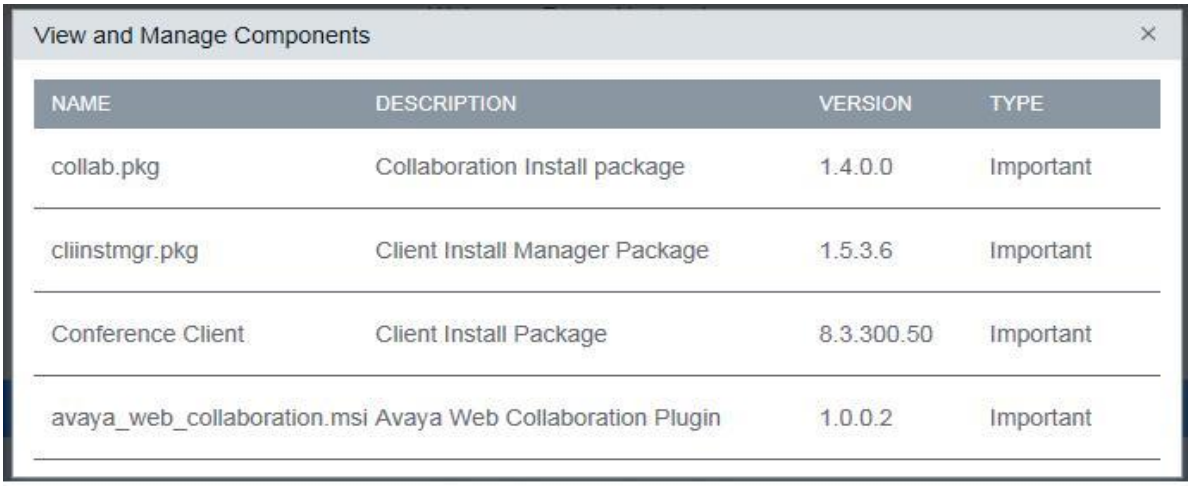


Figure 4: Viewing and managing installed components

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

Getting Started with Scopia® Desktop Client on page 13

Accessing the Scopia® Desktop Web Portal

About this task

The Scopia® Desktop web portal is the entry point to start or join a meeting. You can also use the web portal to access Scopia® Desktop Client settings.

Procedure

Enter the Scopia® Desktop public address in your Internet browser. For example, *http:// sd.company.com*

Or

Right-click the Scopia® Desktop icon in the Windows system tray, and then select **Meeting Portal**.

The Scopia® Desktop web portal opens at the **Join Meeting** screen.

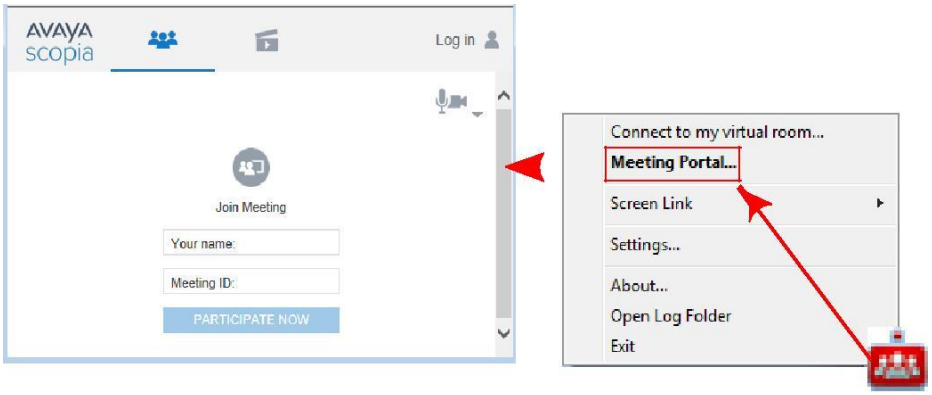


Figure 5: Scopia® Desktop web portal

Important:

Unless you change the default settings, the Scopia® Desktop web portal always opens at the **Join Meeting** screen.

Related Links

Getting Started with Scopia® Desktop Client on page 13

Logging in to the Scopia® Desktop Web Portal

About this task

You can log in to the Scopia® Desktop web portal to get access to your own virtual room and the complete Scopia® Desktop functionality.

Before you begin

Contact your video network administrator to find out your Scopia® Desktop credentials.

Procedure

1. Access the Scopia® Desktop web portal, as described in Accessing the Scopia® Desktop Web Portal on page 17.
2. Ensure that the **Join Meeting** screen is displayed.

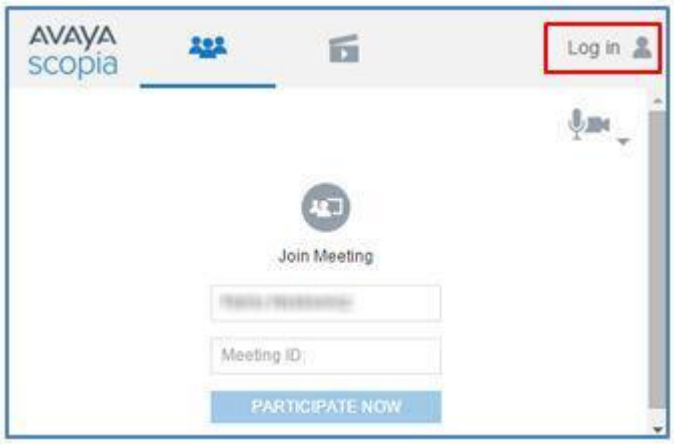
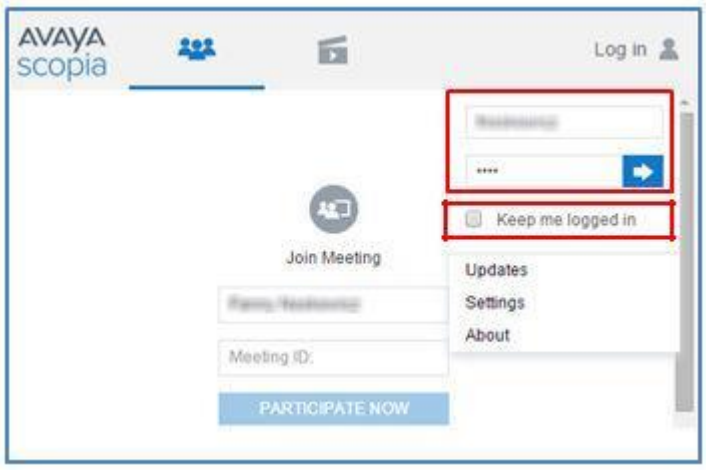


Figure 6: Join Meeting screen with the Log In link

3. Select **Log In**.
4. Enter your user name.



5. Enter your password.
6. (Optional) Select **Keep me logged in** to automatically log in the next time you launch the web portal.
7. Select .

Related Links

Getting Started with Scopia® Desktop Client on page 13

Checking Audio and Video Configurations for your Scopia® Desktop Client

About this task

This section explains how to configure your Scopia® Desktop Client before you use it for the first time.

Before you begin

If the **Virtual Room** window is open on your computer, close it. You cannot change settings of the Scopia® Desktop Client if the **Virtual Room** window is in open.

Procedure

1. Ensure that the web camera is connected and fully installed on your computer.
2. Ensure that the headphones or speakers are connected to your computer.
3. Ensure that the microphone is connected to your computer.

   Important:

   We recommend that you use headphones with a connected microphone for optimal videoconferencing experience.

   We do not recommend to use the microphone of the webcam to guarantee high quality sound.
4. Access the Scopia® Desktop web portal as described in Accessing the Scopia® Desktop Web Portal on page 17.
5. Ensure the **Join Meeting** screen is displayed.

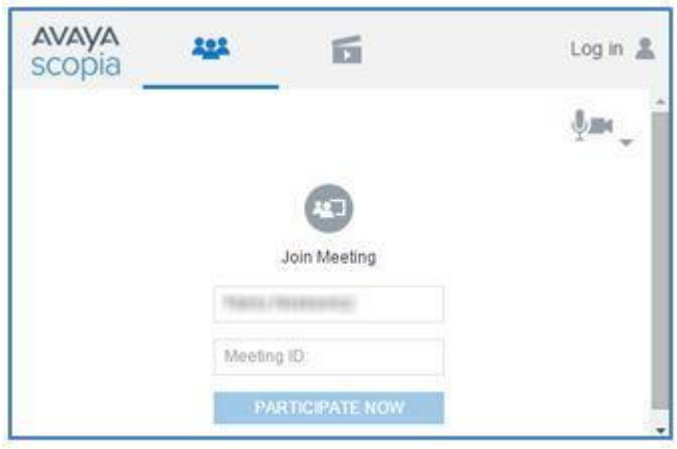


Figure 7: Join Meeting screen

6. Select the audio and video dropdown list.

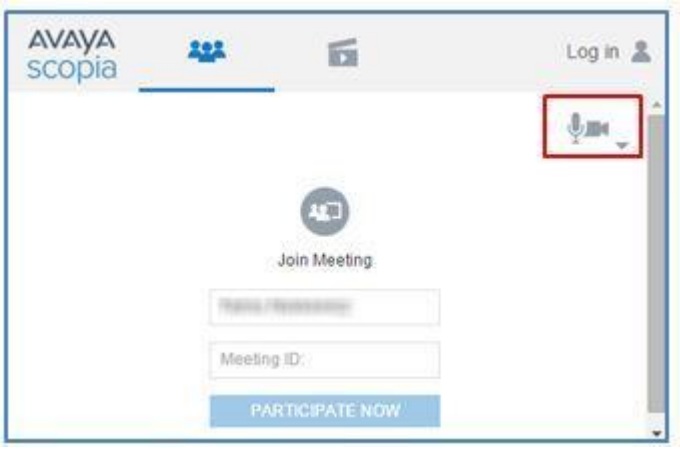


Figure 8: Selecting the audio and video dropdown list

7. Select **Adjust audio and video devices**. The **Audio** tab opens.

Figure 9: Checking the audio configuration for Scopia® Desktop Client

8. Select **Start audio test**.
9. Speak into the microphone and ensure that you can hear yourself and that the volume scales move when you speak.

   If you cannot hear yourself or if the quality of sound is not satisfactory, choose **Default Communication Device** from the **Device** lists in the **Record** and **Playback** sections of the **Audio** tab.

Important:

Most webcams include a built-in microphone. However, if the microphone is located too far away from your face, it is more likely to pick up background noise.

10. Select **OK**.
11. Select the **Video** tab in the **Settings** window.

Figure 10: Checking the video configuration for Scopia® Desktop Client

12. Select **Preview** and ensure that you can see yourself and that the quality of the video is satisfactory.

    If you cannot see yourself, select an alternative camera from the **Device** list and repeat this step to check the video quality.

    Important:

    To change the quality of the picture, use the software accompanying the camera.

13. Select **OK**.

Related Links

Getting Started with Scopia® Desktop Client on page 13

Customizing Your Virtual Room

About this task

A virtual room in Scopia® Desktop and Scopia® Mobile offers a virtual meeting place for instant or scheduled videoconferences. All registered users with a login have their own virtual room.

Most people use the default settings of their virtual rooms.

This procedure explains how to customize your virtual room for optimal videoconferencing experience.

Before you begin

To see your virtual room, you must be logged in. To make changes, ensure your virtual room is not in a meeting.

Procedure

1. Access the Scopia® Desktop web portal as described in Accessing the Scopia® Desktop Web Portal on page 17.
2. Log in to your virtual room as described in Logging in to the Scopia® Desktop Web Portal on page 18.
3. Select **Settings**.

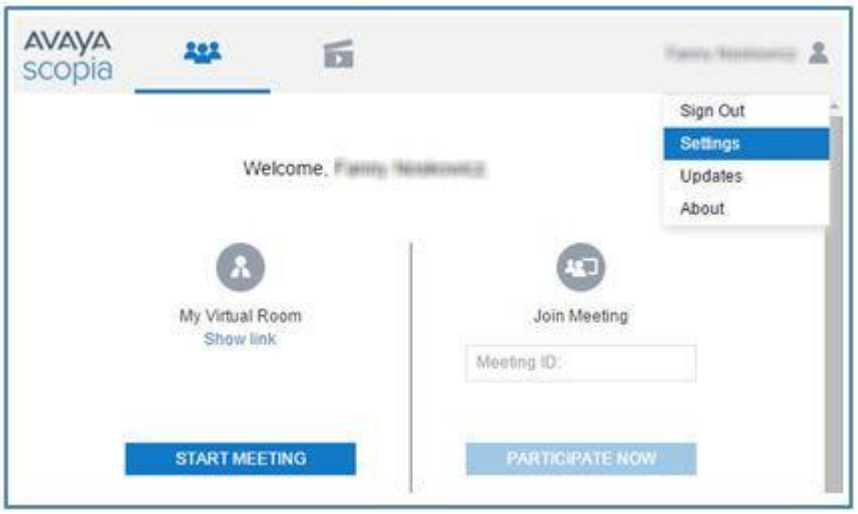


Figure 11: Link to Scopia® Desktop settings

4. Select the **Virtual Room** tab.

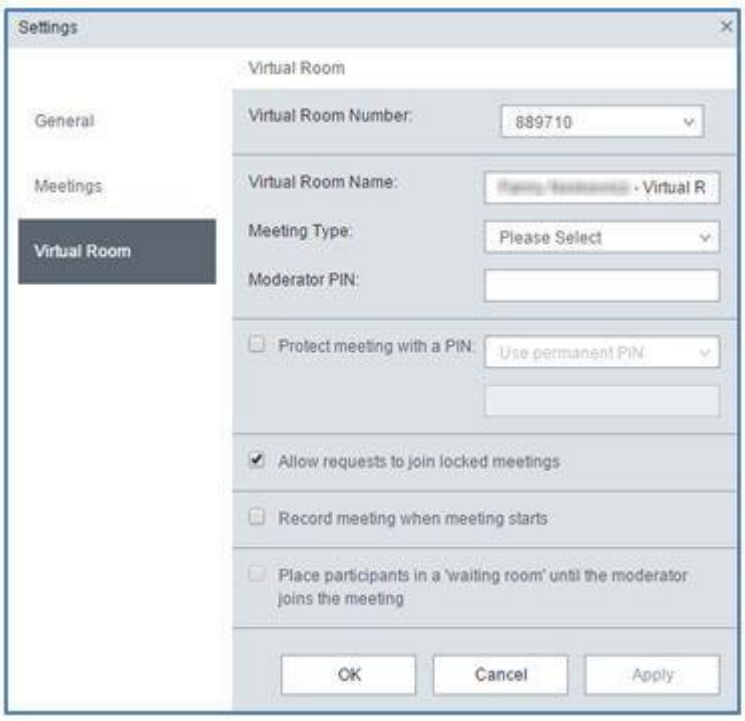


Figure 12: Virtual Room tab of the Settings window

5. Customize your virtual room as described in Table 1: Customizing your virtual room on page 24.

Table 1: Customizing your virtual room

To	Do this
Select your virtual room number from the dropdown list	If you have another virtual room.
Set the name of your virtual room that appears in the title bar of the Virtual Room window as shown in below.	Enter the name in the **Virtual Room Name** field.

Table continues…

To	Do this
Select which meeting type your Scopia® Desktop Client uses. Meeting types (also known as MCU services) are meeting templates which determine the core characteristics of a meeting.	Select a value from the **Meeting Type** list. **Important:** We strongly recommend to consult your video network administrator before changing this setting.
Set the moderator PIN so only users with the PIN can perform moderator actions in your virtual room.	Enter a value in the **Moderator PIN** field. Refer to Protecting Videoconferences in Your Virtual Room on page 77.
Set the access PIN so only users with the PIN can access meetings in your virtual room.	Select **Protect meeting with a PIN**, and then select one of the following: • **Use permanent PIN** This PIN is the access PIN for all videoconferences held in your virtual room. • Use one-time PIN for each meeting Enter a new access PIN at the beginning of every videoconference you create in your virtual room, as described in Starting a New Scopia® Desktop Videoconference in Your Virtual Room on page 37. For more information, see Protecting Videoconferences in Your Virtual Room on page 77.
To not allow participants ask for permission to join locked meetings in your virtual room	Unselect **Allow requests to join locked meetings**. A user trying to join a locked meeting gets a message prompting that the meeting is locked. If you select the checkbox, a user trying to join a locked meeting can send a joining request to the videoconference moderator. For more information see Barring New Participants from Joining Videoconferences on page 80.
To automatically record all videoconferences in your virtual room	Select **Record meeting when meeting starts**. **Important:** You must define the moderator PIN before you select this feature.

Table continues…

To	Do this
To let other participants enter your virtual room only after you join the videoconference	Select **Place participants in a 'waiting room' until the moderator joins the meeting**. **Important:** You must define the moderator PIN before you select this feature.

6. Select **OK**.
7. (Optional) To use your computer for data sharing only, select **Use my computer for presentation only** in the web portal. Your computer does not send video or audio, but you can view the participant list, moderate, chat, and share content.

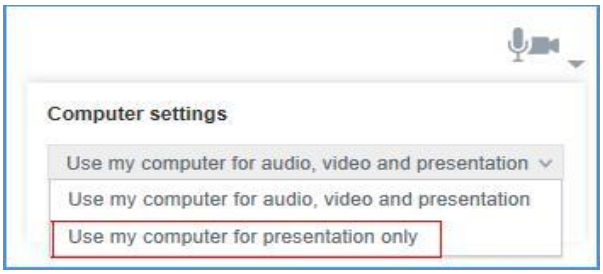


Figure 13: Using your computer for presentation only

8. (Optional) To have the conference video and audio on another endpoint while you are using your computer for data sharing:
   a. Select **Callback my video device number**.
   b. Enter the endpoint number.

   Scopia® Desktop calls the endpoint using this number and you are connected to the conference.

Related Links

Getting Started with Scopia® Desktop Client on page 13

Chapter 3: Scheduling Videoconferences Using Scopia® Add-in for Microsoft Outlook

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

Scheduling a Videoconference Using the Scopia® Add-in for Microsoft Outlook on page 27 Cancelling an Outlook Meeting on page 36

Modifying a Scopia® Add-in for Microsoft Outlook Invitation on page 36

Scheduling a Videoconference Using the Scopia® Add-in for Microsoft Outlook

About this task

When scheduling a videoconference, the options available to you are determined by your user profile:

- Basic meeting settings

  Schedule a meeting without reserving resources (see Scheduling a Videoconference Without Reserving Resources on page 28 for more information). This options suits starting ad-hoc, instant meetings, but has the risk of not having enough bandwidth or available ports on the video network devices to hold your videoconference in high quality.
- Advanced meeting settings

  Schedule a meeting and reserve the required video network resources (see Scheduling a Videoconference and Reserving Network Resources on page 30 for more information). This ensures your meeting has the enough resources to deliver quality videoconferencing. You can also modify advanced meeting settings, such as whether to record the meeting, and using a meeting PIN to restrict access.

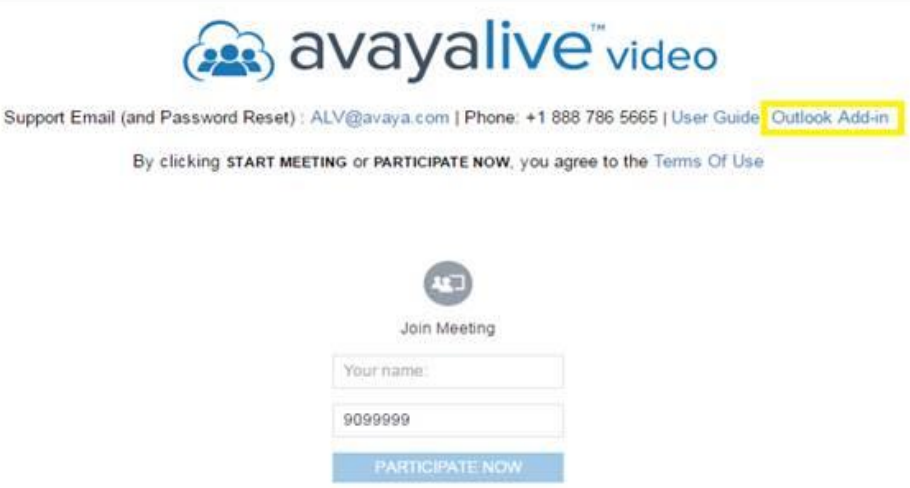
Important:

The meeting options available to you depend on your user profile in Scopia® Management. For more information, contact your administrator, or see *User Guide for Scopia® Management*.

Before you begin

Download Scopia® Add-in for Microsoft Outlook :

Install Scopia® Add-in for Microsoft Outlook from the Meeting home page by clicking on the "Outlook Add- In"



Procedure

1. Select **Scopia Meeting** in Microsoft Outlook.

Figure 14: Locating the Scopia® Add-in for Microsoft Outlook icon at the Outlook ribbon

The scheduling window appears, showing either advanced settings, or basic outlook meeting settings.

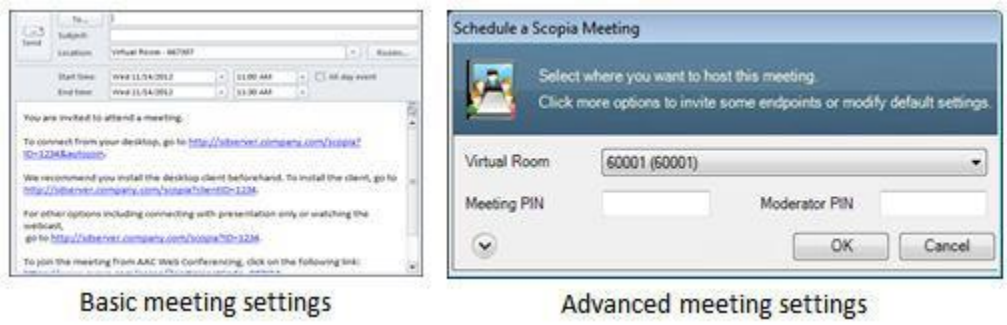


Figure 15: Scopia Meeting Settings

Related Links

Scheduling Videoconferences Using Scopia® Add-in for Microsoft Outlook on page27

Scheduling a Videoconference Without Reserving Resources

About this task

This procedure describes how to schedule a videoconference using the 64 bit version of Scopia® Add-in for Microsoft Outlook without reserving ports. If enabled for your user profile, you can schedule a videoconference with reserved resources, as described in Scheduling a Videoconference and Reserving Network Resources on page 30.

Important:

The meeting options available to you depend on your user profile in Scopia® Management. For more information, contact your administrator, or see *User Guide for Scopia® Management*.

Before you begin

Install Scopia® Add-in for Microsoft Outlook as described in *User Guide for Scopia® Add-in for Microsoft Outlook*.

Procedure

1. Access **Scopia Meeting** add-on in Microsoft Outlook (see Scheduling a Videoconference Using the Scopia® Add-in for Microsoft Outlook on page 27).
2. Specify meeting participants in the **To** field.

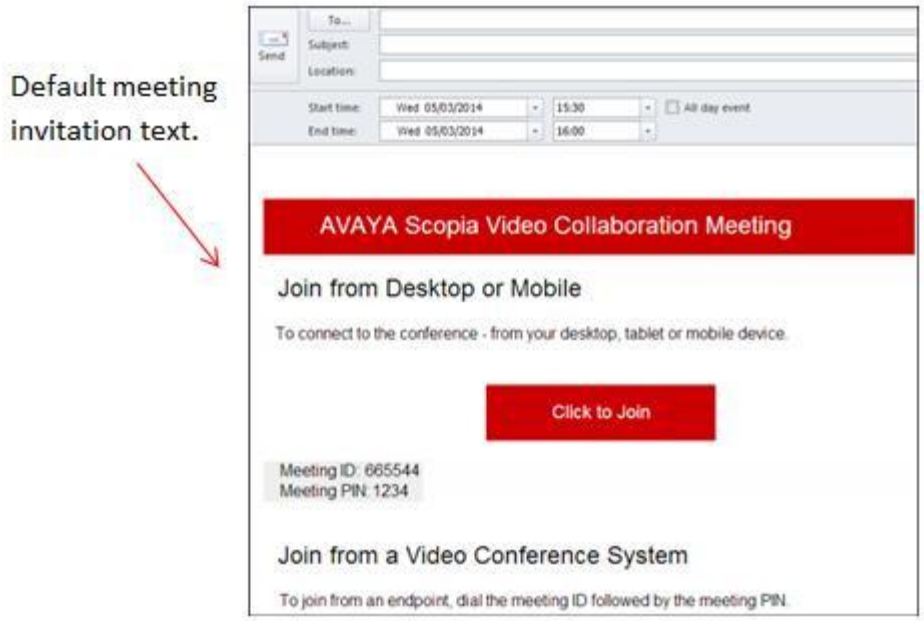


Figure 16: Scheduling a meeting

3. You can modify the text if you prefer.

   The meeting invitation is similar to a regular Microsoft Outlook meeting request, but it already contains text in the body of the invitation with web links (URLs) for the recipients to easily and quickly access your virtual meeting.

   The default template text is defined in Scopia® Management. To change this template to something different, ask your administrator.

Important:

The body of a message sent using the Scopia® Add-in for Microsoft Outlook can contain a maximum of 2000 characters. Any characters beyond the 2000th character are not saved when the message is sent.

4. Select **Send** to send the meeting request to Scopia® Management.

Related Links

Scheduling a Videoconference Using the Scopia® Add-in for Microsoft Outlook on page 27

Scheduling a Videoconference and Reserving Network Resources

About this task

If enabled by your user profile settings in Scopia® Management, you can schedule a videoconference and define advanced settings for your meeting using the 64 bit version of Scopia® Add-in for Microsoft Outlook.

For example, you can reserve ports to ensure that the meeting has sufficient resources, invite endpoints, or restrict the meeting by requiring participants to enter a PIN. To schedule a meeting without reserving resources, see Scheduling a Videoconference Without Reserving Resources on page 28.

Important:

The meeting options available to you depend on your user profile in Scopia® Management. For more information, contact your administrator, or see *User Guide for Scopia® Management*.

Before you begin

Install Scopia® Add-in for Microsoft Outlook as described in *User Guide for Scopia® Add-in for Microsoft Outlook*.

Procedure

1. Access **Scopia Meeting** add-on in Microsoft Outlook (see Scheduling a Videoconference Using the Scopia® Add-in for Microsoft Outlook on page 27).
   If you already have a virtual room defined, some detailed information and default settings are displayed.

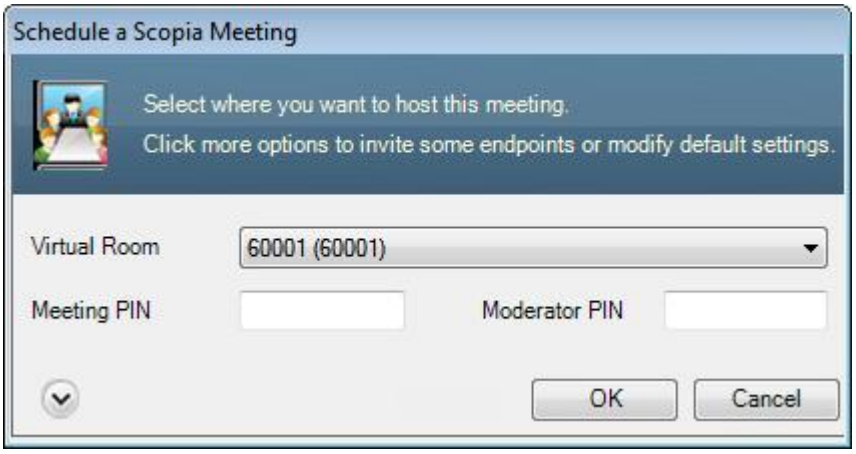


Figure 17: Advanced meeting settings

2. To use a virtual room different from your default virtual room:
   - Select another virtual room belonging to you as shown in Figure 18: Virtual room list on page 31.

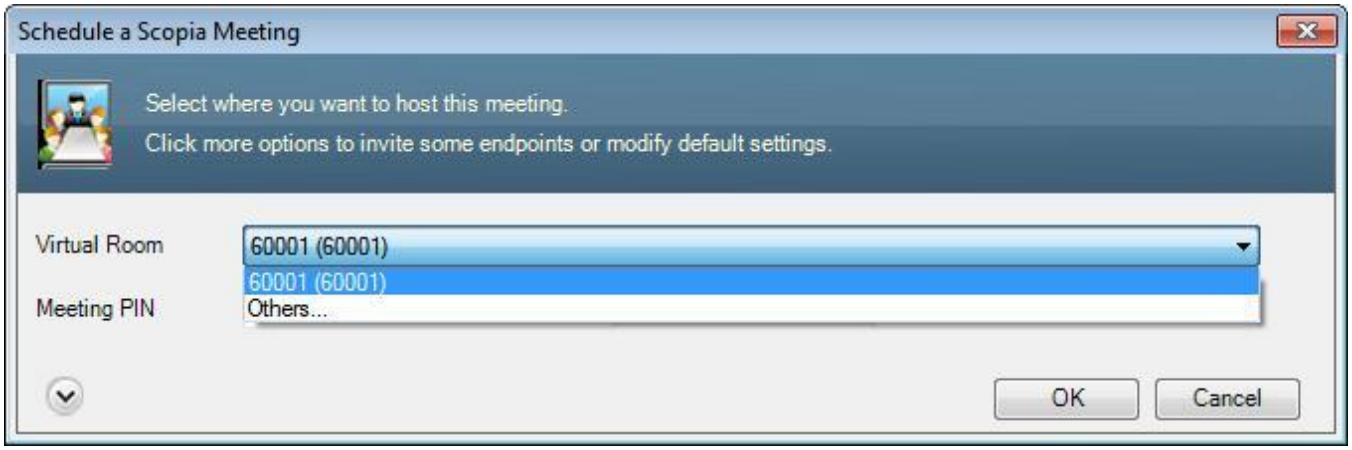


Figure 18: Virtual room list

   - Or

     Select a virtual room belonging to another user:

     a. From the **Virtual Room** list (see Figure 18: Virtual room list on page 31), select **Others**.

        The Others window opens.

     b. Select the **Virtual Room** tab.

     c. Enter the name of the other participant whose virtual room you want to use as shown in Figure 19: Selecting other user's virtual room on page 32.

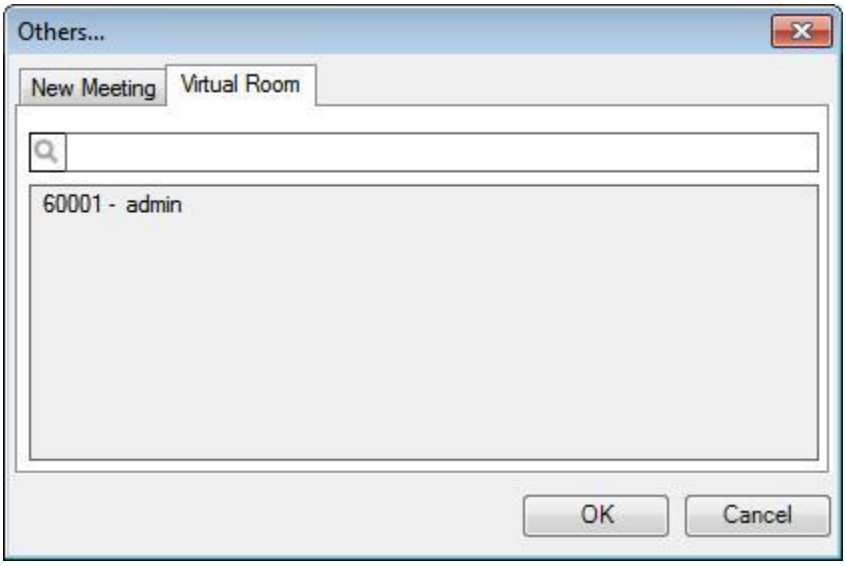


Figure 19: Selecting other user's virtual room

d. Select a virtual room from the virtual rooms assigned to this user.

Important:

You may not able to select another user's virtual room for your meeting if the administrator did not enable this feature for you.

3. (Optional) Enter a PIN to restrict access to your meeting.

   Participants will be required to enter this PIN when accessing the meeting.

4. (Optional) Enter a PIN to restrict meeting moderator capabilities, such as inviting additional participants.

   Participants will be required to enter this PIN to access moderator functions.

5. To use a meeting type other than the default one defined in your virtual room settings, select **Others** from the **Virtual Room** list as shown in Figure 18: Virtual room list on page 31, choose the **Meeting Type** from the list, and select **OK**.

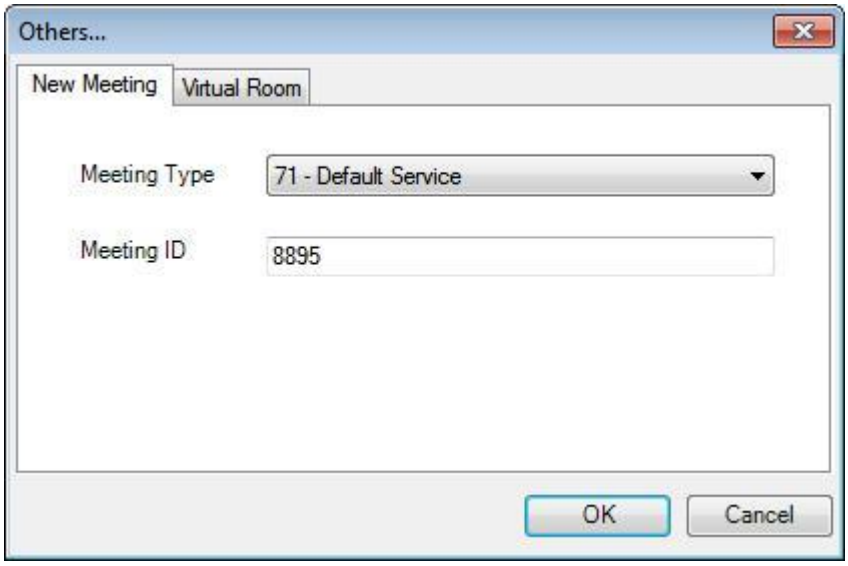


Figure 20: Modifying the meeting type

6. (Optional) Access the endpoint list and advanced options as shown in Figure 21: Accessing advanced options on page 33 and configure advanced settings for your meeting:

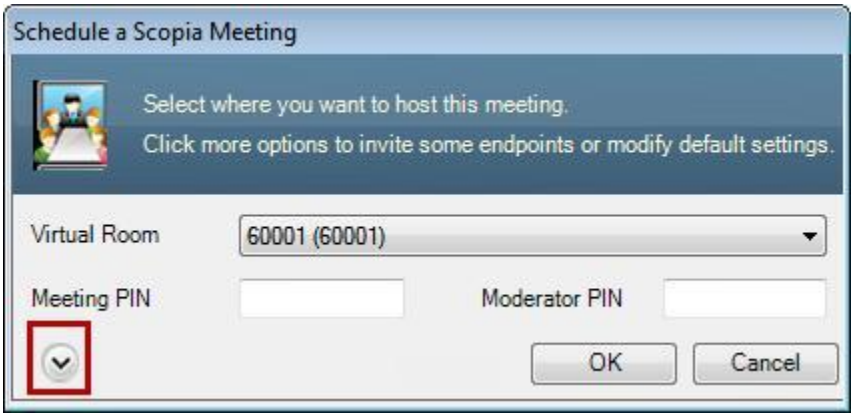


Figure 21: Accessing advanced options

a. Search for specific endpoints to invite, either **By Directory** or **By Address**, and select **Add**.

b. Select the **Advanced** tab to reserve ports and to customize the virtual room settings for this meeting:

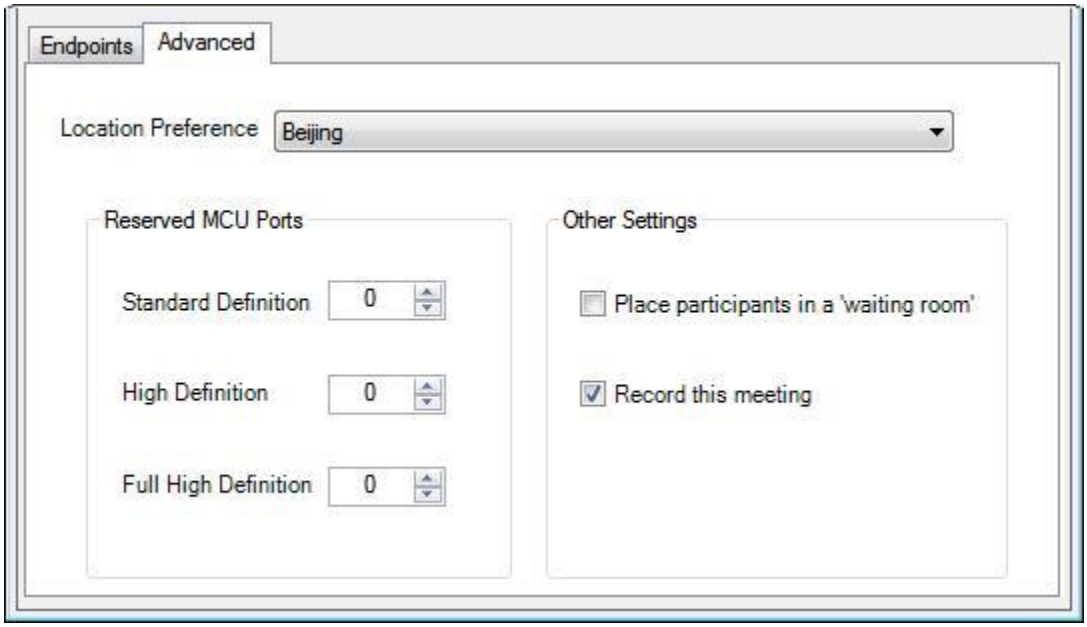


Figure 22: Advanced settings for the meeting

Define the settings based on the following table:

Table 2: Advanced settings for the Meeting

Field Name	Description
Location Preference	Select the meeting location, which is used by Avaya Scopia® Management when assigning the videoconference to a specific MCU (available only in deployments with more than one location). If you select **Auto**, Scopia® Management knows the endpoints' location and can thus automatically select the MCU closest to the endpoints. For example, if only one endpoint in the meeting is in Europe while the remainder are in the Far East, Scopia® Management selects an MCU located in the Far East. We strongly recommend selecting **Auto** to let the system choose the optimal settings matching your organization's bandwidth policies. This ensures efficient bandwidth use and maximum quality for the videoconference.
Reserved MCU Ports	You can reserve ports to ensure you have sufficient resources for the videoconference, according to the endpoint's video capabilities: • **Standard Definition**: Endpoints that support resolutions of 352p and lower. • **High Definition**: Endpoints that support resolutions of 720p and lower.

Table continues…

Field Name	Description
	• **Full High Definition**: Endpoints that support resolutions of 1080p and lower.
Place participants in a 'waiting room'	Select this option to place all participants in a virtual 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. This is available only if you entered a moderator PIN.

7. Select **OK** to save the Scopia® Management scheduling request and close the **Scopia Meeting** window.

   The name of the virtual room appears in the **Location** field of the appointment or meeting request.
8. Specify meeting participants in the **To** field.
9. You can modify the text if you prefer.

   The meeting invitation is similar to a regular Microsoft Outlook meeting request, but it already contains text in the body of the invitation with web links (URLs) for the recipients to easily and quickly access your virtual meeting.

   The default template text is defined in Scopia® Management. To change this template to something different, ask your administrator.

   Important:

   The body of a message sent using the Scopia® Add-in for Microsoft Outlook can contain a maximum of 2000 characters. Any characters beyond the 2000th character are not saved when the message is sent.
10. Select **Send** to send the meeting request to Scopia® Management.

Related Links

Scheduling a Videoconference Using the Scopia® Add-in for Microsoft Outlook on page 27

Cancelling an Outlook Meeting

About this task

Cancelling a meeting scheduled via one of the Scopia® Management plug-ins for Microsoft Outlook is the same as cancelling a regular Outlook meeting.

Procedure

1. Select the meeting in the Outlook calendar.
2. Select **Delete**.
3. Select **Send cancellation and delete meeting**.
4. Select **Send**.

Related Links

Scheduling Videoconferences Using Scopia® Add-in for Microsoft Outlook on page 27

Modifying a Scopia® Add-in for Microsoft Outlook Invitation

About this task

You can modify an invitation created using the 64 bit version of Scopia® Add-in for Microsoft Outlook from within Outlook in just the same way as you would an ordinary meeting.

Procedure

1. Open the meeting from the Microsoft Outlook calendar.
2. Select **Scopia Meeting**.
3. Modify the meeting settings as required. For more information on each of the meeting settings, see Scheduling a Videoconference and Reserving Network Resources on page 30 or Scheduling a Videoconference Without Reserving Resources on page 28.
4. Select **Send Update**.

Related Links

Scheduling Videoconferences Using Scopia® Add-in for Microsoft Outlook on page 27

Chapter 4: Participating in a Scopia® Desktop Videoconference

This section describes how to create a new videoconference or join an existing one as well as actions you may want to perform while participating in a videoconference.

Notice that you need to sign into the Scopia® Desktop web portal to get access to complete Scopia® Desktop functionality.

If a videoconference is taking place in another participants' virtual room which is protected, you need to know the moderator PIN to perform moderation tasks, like controlling other participants in the videoconference.

Related Links

Starting a New Scopia® Desktop Videoconference in Your Virtual Room on page 37
Starting a New Videoconference in Another User's Virtual Room on page 39
Inviting Participants to an Ongoing Videoconference on page 40
Joining an Ongoing Scopia® Desktop Videoconference on page 47
Transferring a videoconference to an Avaya Scopia® XT Series on page 50
About Sharing Content on page 51
Changing Your Video Layout during a Videoconference on page 64
Moderating Other Participants on page 67
Granting permission to a participant to join a locked videoconference on page 69
Blocking Your Audio and Video during a Scopia® Desktop Videoconference on page 70
Using Text Chat during a Videoconference on page 71
About Lecture Mode on page 72
Leaving or Ending a Scopia® Desktop Videoconference on page 75

Starting a New Scopia® Desktop Videoconference in Your Virtual Room

About this task

Typically, you start new videoconferences in your own virtual room. You start the unscheduled (ad-hoc) and scheduled videoconferences in the same way.

If necessary, you may also create videoconferences in another participants' virtual rooms as described in Starting a New Videoconference in Another User's Virtual Room on page 39. To learn about scheduling videoconferences, read Scheduling Videoconferences Using Scopia® Add-in for Microsoft Outlook on page 27.

Procedure

1. Select **Connect to my virtual room** from the system tray icon.

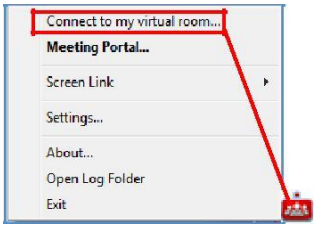


Figure 23: Link to your virtual room in the task tray menu

Or

2. Start a videoconference from the Scopia® Desktop portal:
   a. Access the Scopia® Desktop web portal as described in Accessing the Scopia® Desktop Web Portal on page 17.
   b. Log in to the Scopia® Desktop web portal as described in Logging in to the Scopia® Desktop Web Portal on page 18.
   c. Verify that the **Join Meeting** screen is displayed.
   d. To create a videoconference in your own virtual room, select **Start Meeting** .

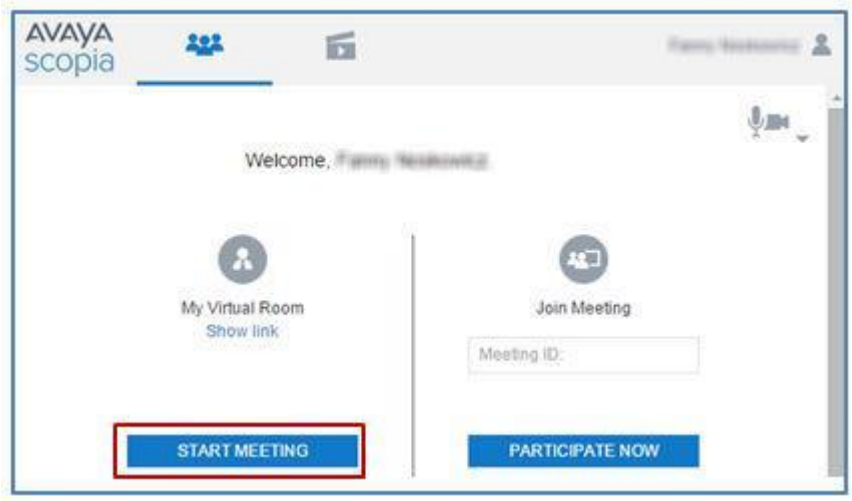


Figure 24: Start a meeting in your virtual room

If the virtual room is protected with a one-time access PIN, enter it in the field and select **OK**.

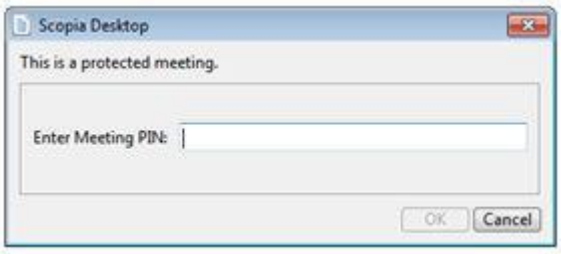


Figure 25: Entering the one-time PIN at the beginning of a videoconference

The Virtual Room window opens. You can invite other participants to your conference now.

Related Links

Participating in a Scopia® Desktop Videoconference on page 37

Starting a New Videoconference in Another User's Virtual Room

About this task

Usually you start a videoconference in your own virtual room, but, if necessary, you can also use somebody else's virtual room as described in this section.

You start unscheduled (ad-hoc) and scheduled videoconferences in the same way. To learn about scheduling videoconferences, read Scheduling Videoconferences Using Scopia® Add-in for Microsoft Outlook on page 27.

Before you begin

Make sure you know the meeting ID of this virtual room.

If the virtual room you want to use is protected, ask the owner of this virtual room to send you the moderator PIN. For more information about protected virtual rooms, refer to Protecting Videoconferences in Your Virtual Room on page 77.

Procedure

1. Access the Scopia® Desktop web portal as described in Accessing the Scopia® Desktop Web Portal on page 17.
2. Verify that the **Join Meeting** screen is displayed.

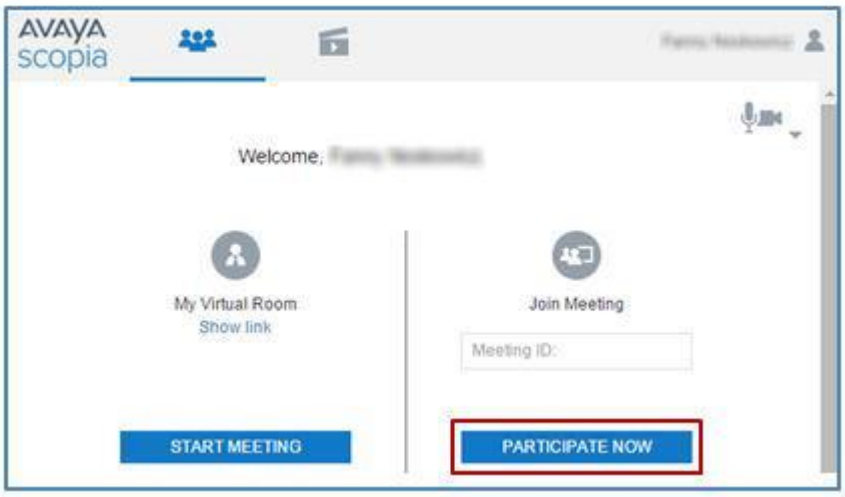


Figure 26: Join Meeting screen

3. Enter the meeting ID of another user's virtual room in the **Meeting ID** field.
4. Select **Participate Now**.

   The **Virtual Room** window opens and your videoconference is created. Continue by inviting participants as described in Inviting Participants to an Ongoing Videoconference on page 40.
5. If the virtual room is protected, enter the moderator PIN and select **OK**.

   The Virtual Room window opens. You can invite other participants to your conference now.

Related Links

Participating in a Scopia® Desktop Videoconference on page 37

Inviting Participants to an Ongoing Videoconference

This section explains how to invite participants to an ongoing videoconference. You can also invite participants to a scheduled videoconference before it starts, as described in Scheduling Videoconferences Using Scopia® Add-in for Microsoft Outlook on page 27.

Participants can also invite others unless moderating rights in this virtual room are protected. For more information about protected virtual rooms see Protecting Videoconferences in Your Virtual Room on page 77.

As described in Figure 27: Ways of inviting users to an ongoing videoconference on page 41, you can invite a new participant in the following ways:

Figure 27: Ways of inviting users to an ongoing videoconference

- Sending the link or dial-in information via an mail or IM

  When the participant clicks the link, the Scopia® Desktop Client opens and the participant joins the meeting. Sending the link best suits participants using Scopia® Desktop Clients or Scopia® Mobile.

  All participants, no matter what device they have, can use the dial-in information to dial into your videoconference or to access it from the Scopia® Desktop web portal. Refer to Accessing the Scopia® Desktop Web Portal on page 17.

  See Inviting Participants by Sending a Link or Dial-in Information on page 45 for operational information.

- Sending an invitation using the Scopia® Desktop Client

  The invited participant receives an invitation message on the computer or the videoconferencing endpoint. When the participant accepts the invitation, the Scopia® Desktop **Virtual Room** window opens and this participant joins the meeting.

  See Inviting Participants Using Scopia® Desktop Client on page 42 for operational information.

- Calling or sending a text message to the participant with the meeting ID of the videoconference.

  The meeting ID is displayed in the title bar of the **Virtual Room** window as shown in Figure 28: Meeting ID displayed at the title bar of the Virtual Room window on page 42

Figure 28: Meeting ID displayed at the title bar of the Virtual Room window

The participant accesses the Scopia® Desktop web portal and connects to the videoconference using the meeting ID you forwarded.

Related Links

Participating in a Scopia® Desktop Videoconference on page 37
Inviting Participants Using Scopia® Desktop Client on page 42
Inviting Participants by Sending a Link or Dial-in Information on page 45

Inviting Participants Using Scopia® Desktop Client

About this task

The procedure in this section explains how you can invite users to an ongoing Scopia® Desktop videoconference from any endpoint. You can invite both individual users or people in meeting rooms equipped with room systems. Scopia® Desktop Client allows you to invite participants by using

- the participant's name from the organization's directory
- the number of the room system or of the dedicated endpoint (like Avaya Scopia® XT Executive)
- the IP address, phone number, or the E.164 address or SIP address of the room system or dedicated endpoint

You must have moderator's rights to invite participants. By default, any Scopia® Desktop participant in a videoconference can be a moderator, unless a virtual room is protected by its owner. You still may be able to invite other users to a videoconference if the owner of the videoconference shares the moderator PIN with you.

Before you begin

If you know that the virtual room is protected with a moderator PIN, ask the owner to send the PIN to you using the **Chat** pane. We recommend that the PIN is sent privately. For more information about using text messages in Scopia® Desktop Client, see Using Text Chat during a Videoconference on page 71.

If the Scopia® Desktop deployment in your organization does not support directory, ensure you know which device or endpoint participants you want to invite use and what is the phone number or address of this device.

Procedure

1. In the **Virtual Room** window, select **Moderate**.

   This option is only available to registered users who logged in.

2. If necessary, enter the moderator PIN and select **OK**.
3. Select **Invite**.
4. Select the relevant invitation method and enter dialing information as described in Table 3: Choosing the invitation method and entering the connection information on page 43.

Table 3: Choosing the invitation method and entering the connection information

To invite by	Perform these steps
The user's name (as it appears in the directory)	a. Select **Invite a user from the directory** from the **Invitation Method** list. See Figure 29: Invitation method list in the Scopia® Desktop Invite window on page 44. b. Enter the user's name or part of the name into the search field next to the **Invitation Method** list, and select **Search**  The window displays all search results. See Figure 29: Invitation method list in the Scopia® Desktop Invite window on page 44. c. Select the user's name. d. Select **Invite**.
The number of the room system or of the dedicated endpoint	a. From the **Invitation Method** list, select **Invite a terminal from the directory** (Figure 29: Invitation method list in the Scopia® Desktop Invite window on page 44). b. If the list of endpoints is too long and not all endpoints appear, enter the first digits of the endpoint number in the **Search** field to narrow the search. c. Select the endpoint from the list. d. Select **Invite**.
The IP address, phone number, or the E.164 address or SIP address of the room system or dedicated endpoint	a. Select **Invite by address** from the **Invitation Method** list (Figure 29: Invitation method list in the Scopia® Desktop Invite window on page 44).

Table continues…

To invite by	Perform these steps
	b. Enter the number or the address of the endpoint or mobile device in the **Address** field. c. Select **Invite**.

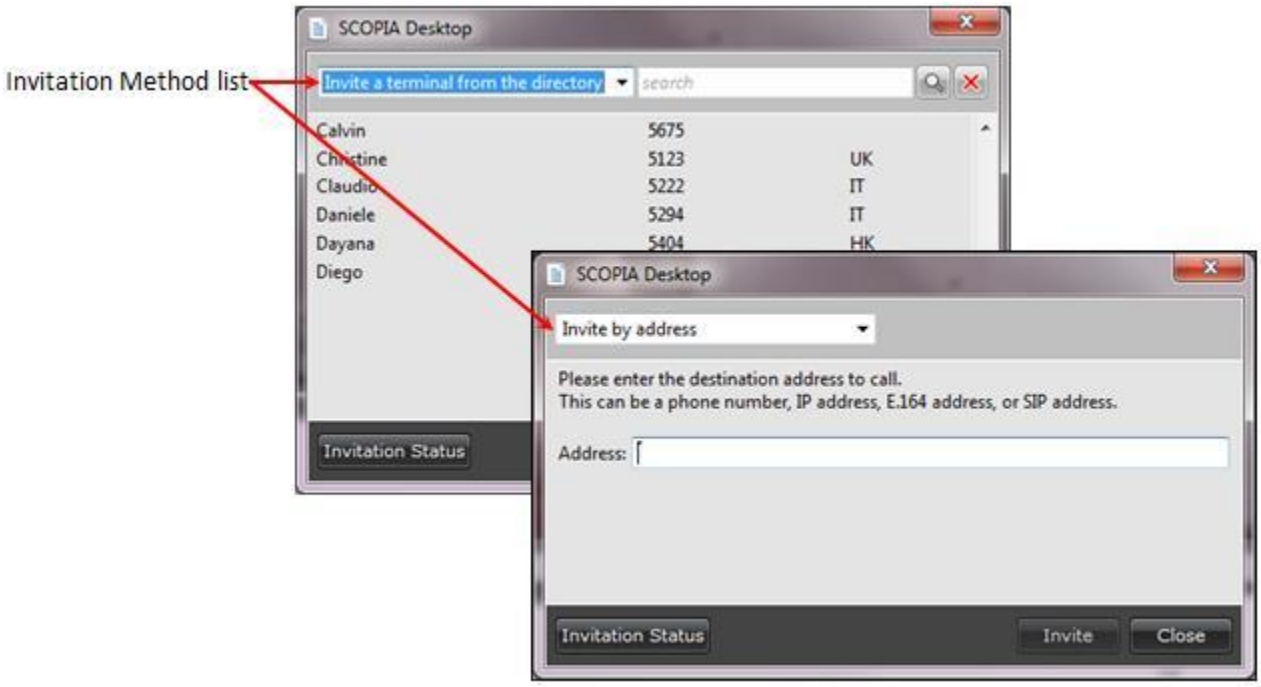


Figure 29: Invitation method list in the Scopia® Desktop Invite window

The **Invite** window shows the status of your recent invitations as shown in Figure 30: Invite window showing invitation status on page 44.

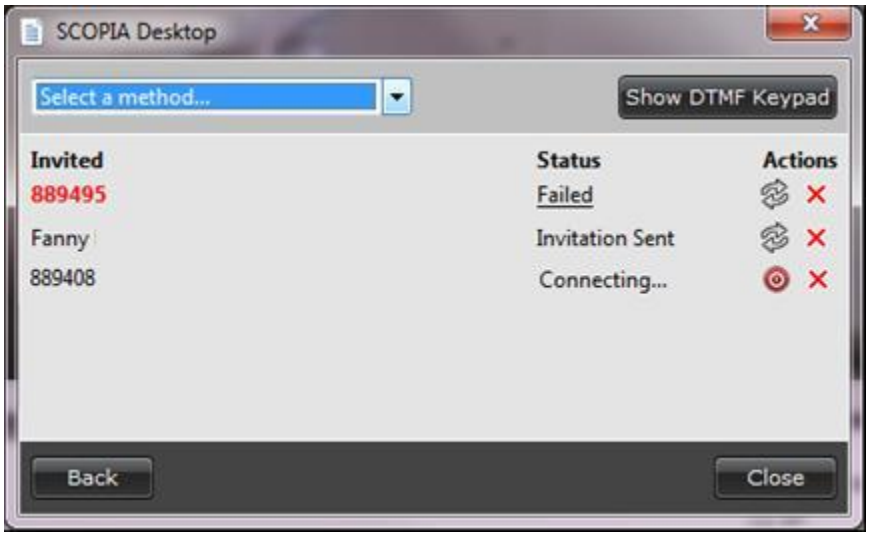


Figure 30: Invite window showing invitation status

5. If necessary, you can cancel the invitation by selecting **Cancel** . Or

   Resend the invitation by selecting **Re-invite**

   . Or

   Remove the invitation from the list by select **Remove**

   The invited user receives your invitation. An example of the invitation message is shown in Figure 31: Meeting Invitation message as displayed on a desktop on page 45.

Figure 31: Meeting Invitation message as displayed on a desktop

   The invitation message may look different depending on the endpoint.

Related Links

Inviting Participants to an Ongoing Videoconference on page 40

Inviting Participants by Sending a Link or Dial-in Information

About this task

The procedure in this section explains how to invite new participants to an ongoing videoconference by sending a link to it or information on how to dial into it.

Selecting the link takes any Scopia® Desktop Client or Scopia® Mobile user directly to the videoconference. Users without Scopia® Desktop Client (PC or mac) or Scopia® Mobile (iOS or Android) can automatically download the apps from the same location.

Dial-in information allows participants using any device (a desktop, tablet, mobile device, room system, dedicated endpoint or a regular phone) to connect to your videoconference.

Procedure

1. Send the link to your virtual room to the user you are inviting:

   a. Log in to the Scopia® Desktop Client web portal.

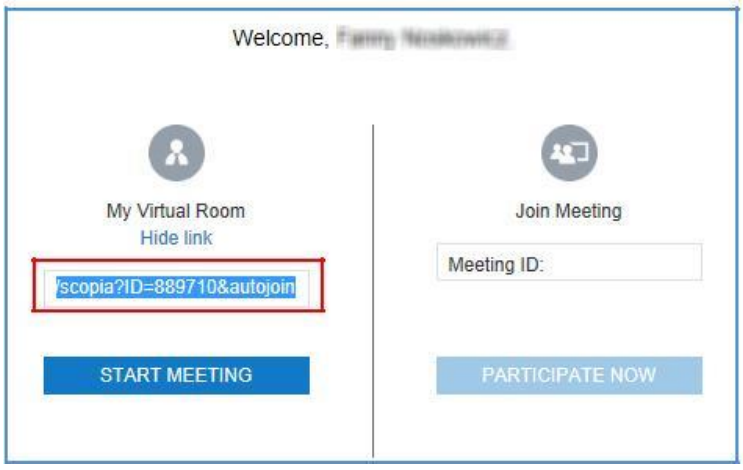


Figure 32: Sending the link to a meeting

b. Copy the link to your virtual room.

c. Paste it into an e-mail or an instant message and send it to the invited user.

2. Or, In the **Virtual Room** window, select **Information** in the upper right corner.

3. Select **Dial-in Information**.

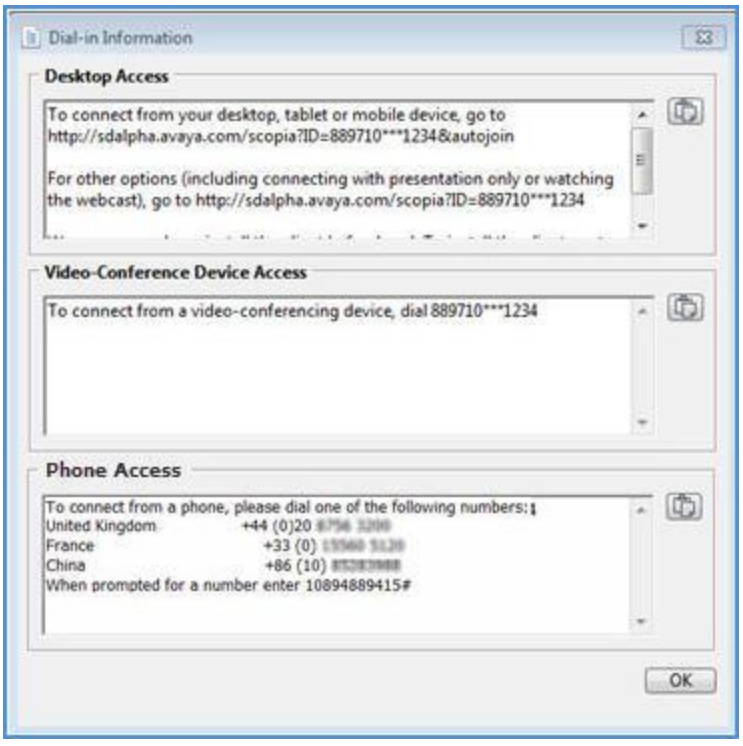


Figure 33: Dial-in Information window

4. Select **Copy to Clipboard** next to the information you want to copy.

5. Paste the copied text into an e-mail or an instant message and send it to the user you are inviting.

Related Links

Inviting Participants to an Ongoing Videoconference on page 40

Joining an Ongoing Scopia® Desktop Videoconference

About this task

You can join an ongoing Scopia® Desktop videoconference in several ways, depending on the way you were invited.

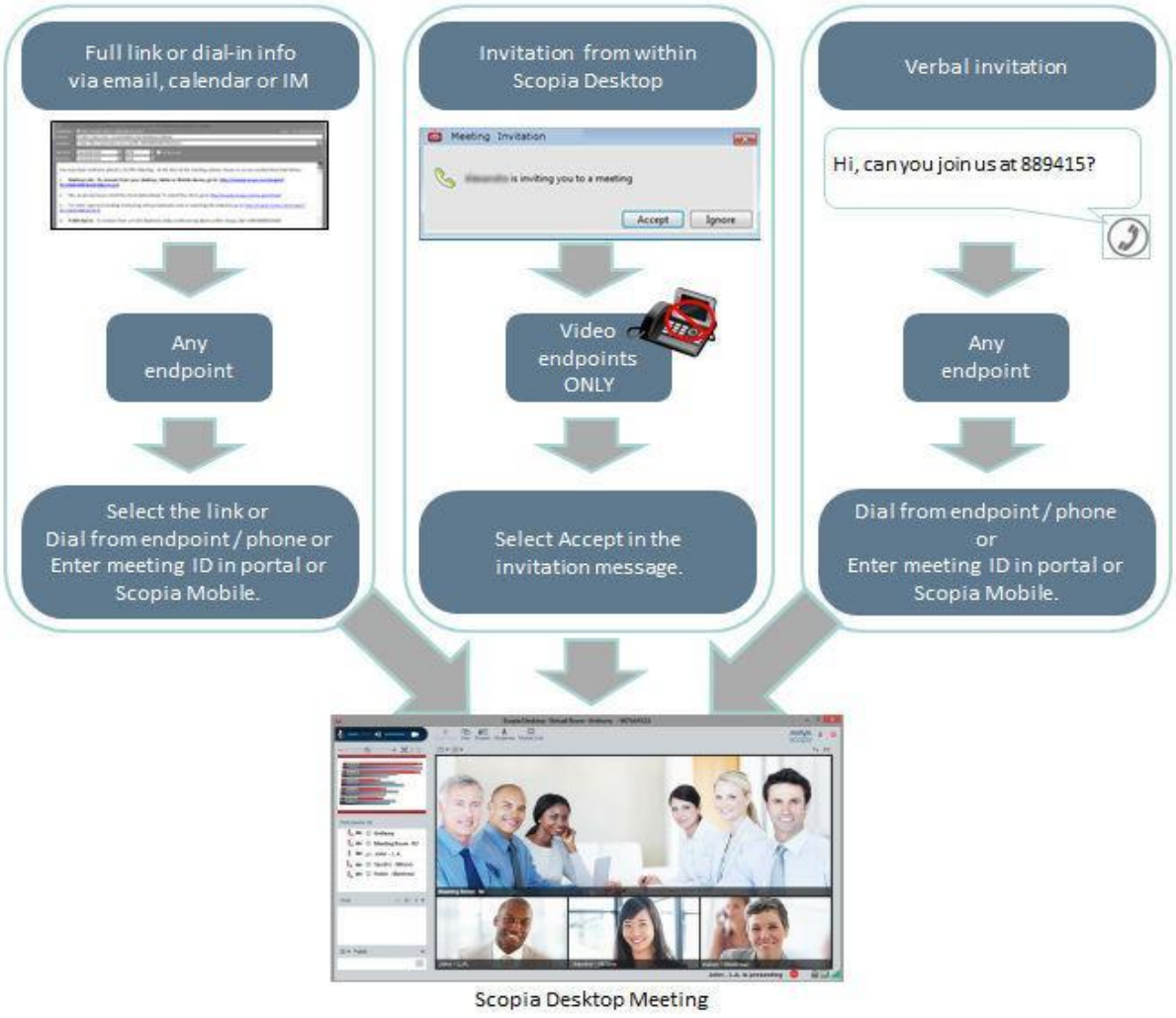


Figure 34: Joining a Scopia® Desktop videoconference

A meeting moderator can lock the meeting for new participants, but let new participants request permission to join the meeting. In this case the moderator decides if to grant you permission to join or not.

Procedure

Depending on your invitation type, join a videoconference as described in Table 4: Joining a videoconference on page 48.

Table 4: Joining a videoconference

Invitation type	Your endpoint	Do this
The link	A computer or mobile device	a. Open the invitation email or the IM message containing the link on your computer or mobile device. b. Click on the link. c. If the virtual room is protected , enter the access PIN and select **OK**. d. If the videoconference is locked, but you can request permission to join, do so either by: • Selecting **Yes** Or • (If the videoconference is protected with a PIN) Entering the access PIN and selecting **OK**. You are connected to the videoconference and the **Virtual Room** window opens. If the videoconference is locked, you are connected only if the moderator granted you permission to join.
Dial-in information	A room system or dedicated endpoint	a. Dial the number as instructed in the invitation email or IM message using the remote control of your room system or the digit keys of your phone. You are connected to the videoconference. b. If this videoconference is locked, but you can request permission to join, do so by pressing the pound key # or entering the access PIN and selecting **OK**. You are connected to the videoconference and the **Virtual Room** window opens. If the videoconference is locked, you are connected only if the moderator granted you permission to join. **Important:** When using a regular phone, you are connected only with audio.

Table continues…

Invitation type	Your endpoint	Do this
From the Scopia® Desktop Client	A room system or dedicated endpoint	Select **Accept** in the invitation message displayed on your computer, room system or dedicated endpoint.
Over the phone	A computer	a. Open the Scopia® Desktop web portal on your computer as described in Accessing the Scopia® Desktop Web Portal on page 17. Ensure that the **Join Meeting** screen is displayed. b. Enter the meeting ID in the **Meeting ID** field. c. Select **Participate Now**. d. If the videoconference is locked, but you can request permission to join, do so by: • Selecting **Yes** Or • (If the videoconference is protected with a PIN) Entering the access PIN and selecting **OK**. Your computer is now connected to the videoconference and the **Virtual Room** window opens. If the videoconference is locked, you are connected only if the moderator granted you permission to join.
Over the phone	A mobile device	a. Open the Scopia® Mobile application on your mobile device. b. Enter the meeting ID. c. Tap **Connect**. d. If the videoconference is locked, but you can request permission to join, do so by: • Selecting **Yes**. Or • (If the videoconference is protected with a PIN) Entering the access PIN and selecting **OK**. Your mobile device is connected to the videoconference. If the videoconference is locked, your mobile device is connected only if the moderator granted you permission to join.

Related Links

Participating in a Scopia® Desktop Videoconference on page 37

Transferring a videoconference to an Avaya Scopia® XT Series

About this task

Avaya Mobile Link allows users connected to a videoconference on a laptop to transfer the videoconference onto an XT Series endpoint without connecting the laptop to the endpoint with a cable. While XT Series endpoint is used for audio and video of the meeting, Avaya Scopia® Desktop Client still runs on the laptop in the Companion mode supporting moderation, Content Slider and chat.

Before you begin

To display your computer's content on the XT Series using Avaya Screen Link, your computer must have Scopia® Desktop Client installed and be in the same network as the endpoint. If the computer and endpoint are in different networks, make sure there is no NAT or firewall between them.

- For automatic pairing (using proximity sensing), the computer's speakers must be able to play audio at up to 19KHz.
- The proximity pairing is designed to work in proximity to the endpoint's microphone. The optimal distance is up to 1-1.5 m. The exact distance depends on the type of microphone pod used (one way or three way) and the computer's gain levels.
- When automatic proximity does not work, use manual pairing.

Procedure

1. In the Virtual Room, select **Mobile Link**.

Figure 35: Selecting Mobile Link

   The list of available XT Series endpoints is displayed.

2. Select the required XT Series endpoint.

   The videoconference is transferred onto the endpoint.

3. To transfer the videoconference back to your computer, select **Mobile Link** > **Stop Mobile Link**.

Related Links

Participating in a Scopia® Desktop Videoconference on page 37

About Sharing Content

Avaya Scopia® Solution helps to make collaborating with other participants easy and effective using its content sharing capabilities.

You can allow other participants to see the content of your screen by presenting during a videoconference. You can also decide to share any content on your screen, or limit it to either a part of the screen or to certain applications. For example, if you choose to only share the PowerPoint application, content from applications is not sent to other participants.

If your organization deploys the latest content sharing solution, the advanced content sharing features are available:

- All participants can share their screen one at a time
- All participants can annotate the shared content
- All participants can draw and write on the special blank slide (whiteboard), which is not part of the original presentation, to illustrate their point
- All participants can view previously displayed slides using a slider

If your organization deploys the legacy content sharing solution, you can use the standard content sharing features it offers:

- All participants can share their screen
- Only the participant who is currently presenting can annotate the shared content
- All participants can view previously displayed slides using a slider

In addition, if you have a Avaya Scopia® XT Series endpoint in your room, you can use it to present your content.

Related Links

Participating in a Scopia® Desktop Videoconference on page 37 Sharing Content during a Scopia® Desktop Videoconference on page 51
Viewing Presented Content during a Scopia® Desktop Videoconference on page 55
Annotating Shared Content during a Avaya Scopia® Desktop Videoconference on page 57 Collaborating with Participants Using Whiteboards on page 59
Presenting Content Using an Avaya Scopia® XT Series Endpoint on page 61

Sharing Content during a Scopia® Desktop Videoconference

About this task

This section explains how to annotate shared content in the new content sharing solution deploying Avaya Scopia® Web Collaboration server.

You can allow other participants to see the content of your screen by presenting during a videoconference. You can also decide to share any content on your screen, or limit it to either a part of the screen or to certain applications. For example, if you choose to only share the PowerPoint application, content from applications is not sent to other participants.

Note:

If your organization deploys a legacy solution for sharing content, some sharing options such as limiting sharing to certain applications on Mac-based clients or limiting sharing to a set area of the monitor are not available.

When you start sharing content, the video layout changes to provide the maximum space on your screen to the content you are sharing:

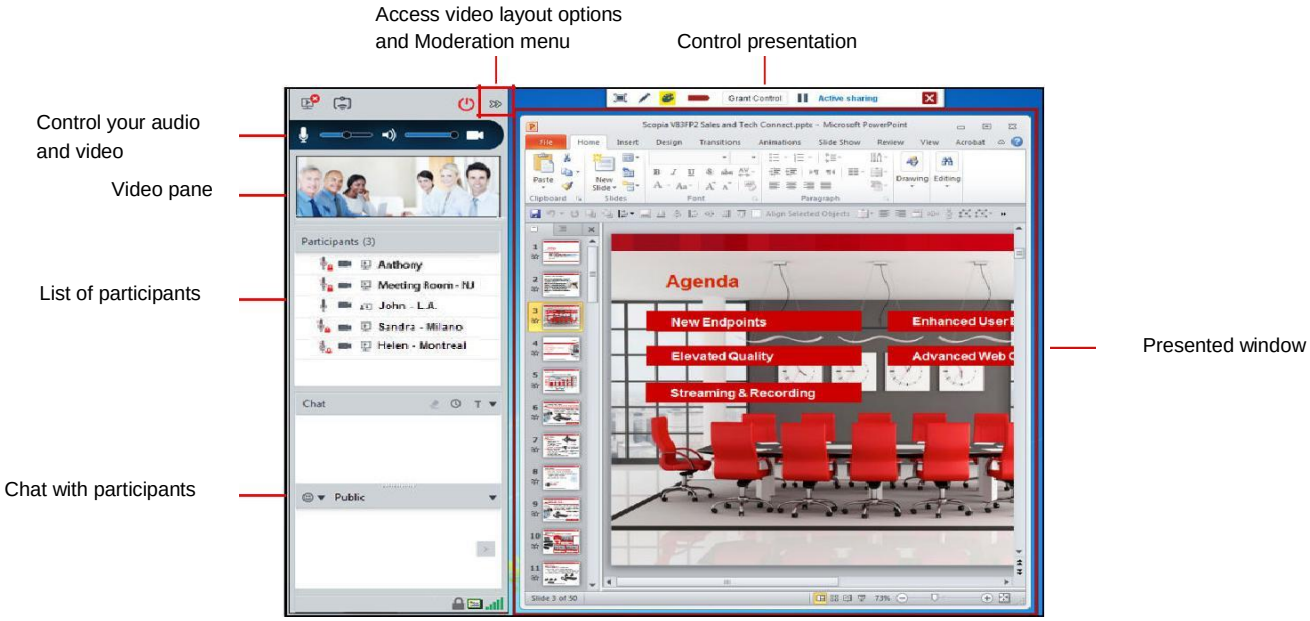


Figure 36: Video layout of the presenter as appears on a PC

Before you begin

In the new content sharing solution if another participant is currently presenting in this virtual room , select **Request Control**. You can start sharing your content after the virtual room owner or the current presenter grants permission.

Procedure

1. In the **Virtual Room** window, select **Present**.

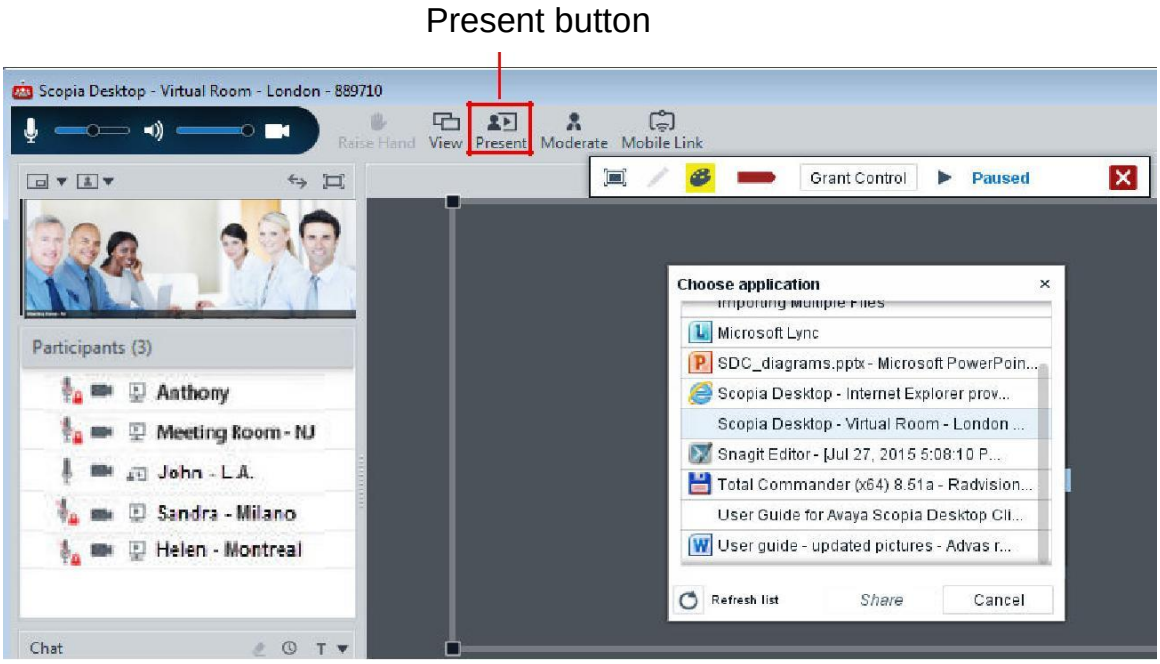


Figure 37: Starting a presentation in the Windows-based Scopia® Desktop Client

2. To share the content of any application visible on your screen, select **Full Screen**.
3. To share the content of specific applications only, select **Application**, select the desired application in the **Choose application** window, and then select **Share**.
4. To share the content within a set area of your monitor in the new content sharing solution:
   a. Select **Portion of screen**.

      The red box appears marking the shared area.

   b. Move the red box to the area that you want to share.
   c. If necessary, adjust the size of the shared area by resizing the red box.
5. If another participant is currently presenting, select **Yes** in the confirmation message. The content is displayed on other participants' screens.
6. If you use more than one monitor, make sure that the desired content is shared by selecting the **Change type of sharing** icon and then selecting **Screen 1** or **Screen 2**

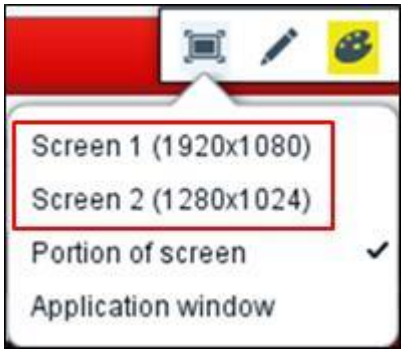


Figure 38: Selecting the monitor used to share content

7. Use the annotation feature to point at specific elements in your presentation as described in Annotating Shared Content on page 57.
8. To share content in full-screen mode, hide the Scopia® Desktop Client as shown below. The client minimizes as a tab. To maximize the client, select the minimized tab.

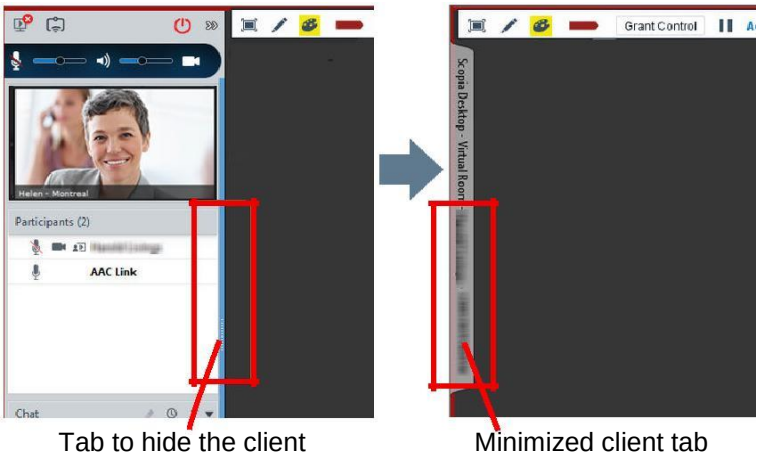


Figure 39: Sharing content in full-screen mode

9. To change the application you are sharing in the new content sharing solution:
   a. Select the **Change type of sharing** icon > **Application window** .
   b. From the **Choose application** window, select the desired application.
   c. Select **Share**.
10. To stop sharing, select in the control presentation toolbar.

Related Links

About Sharing Content on page 51

Viewing Presented Content during a Scopia® Desktop Videoconference

About this task

When another participant shares PC content during a videoconference, your video layout changes to display the presentation.

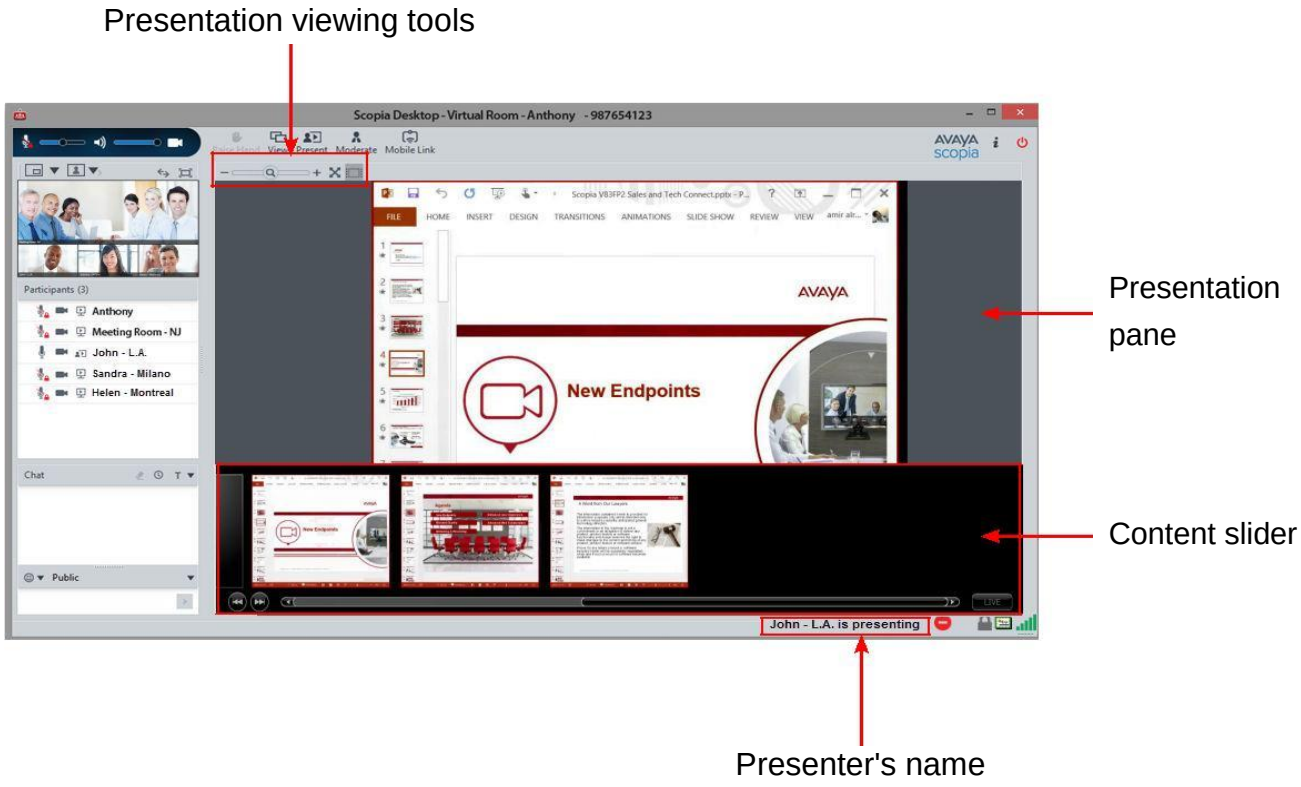


Figure 40: Video layout during a presentation

You can watch the presentation live (as it is sent to participants) or you can navigate through the previously shown slides using the **Content Slider** as described in this section. Content Slider displays all content presented during the video conference, including all annotated slides and whiteboards.

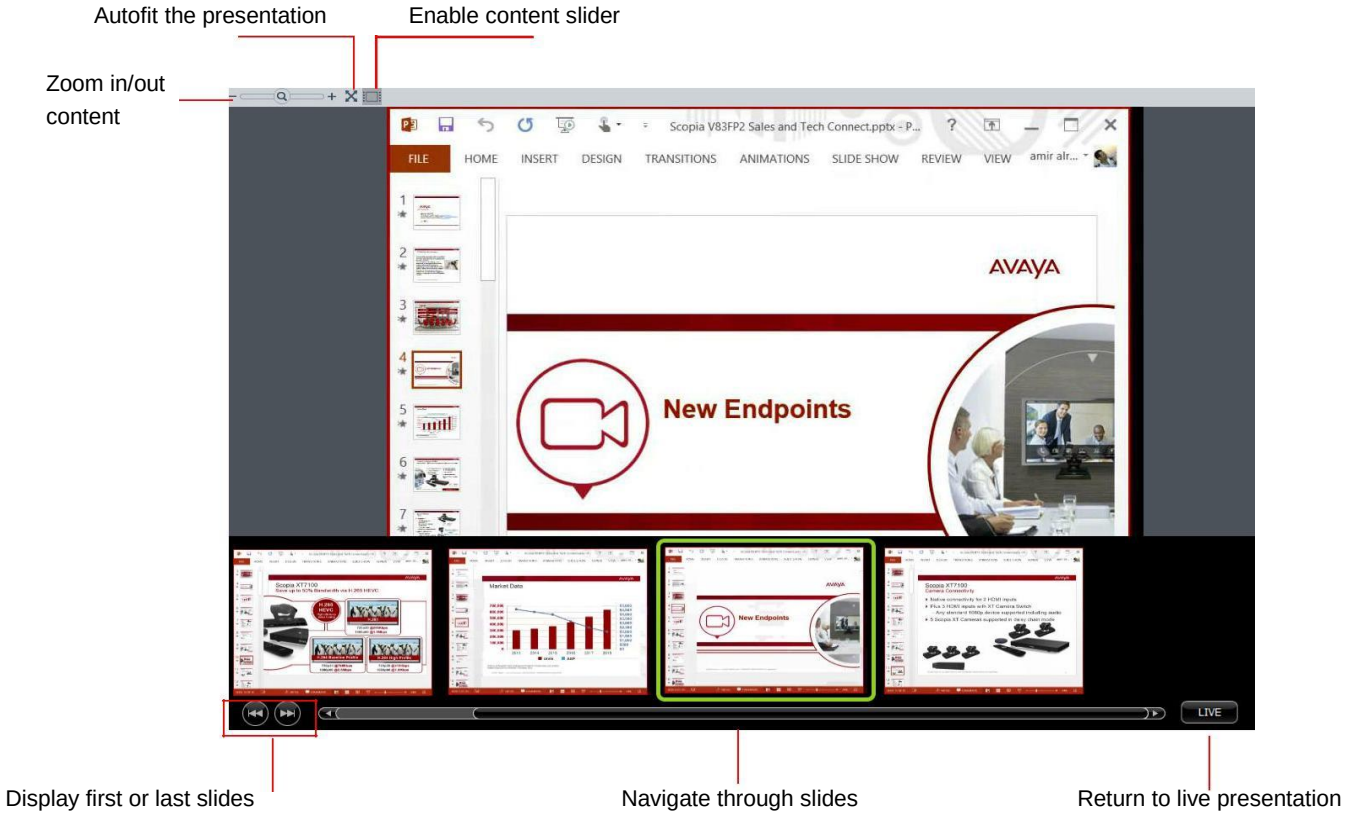


Figure 41: Navigating through a presentation

Procedure

Perform one of the following to navigate through a presentation:

- Swap positions of the video and presentation panes by selecting .

Figure 42: Swapping positions of the video and presentation panes

- Fit the presented content into the **Presentation** pane by selecting .
- Enable the content slider by selecting .
- Display the first slide by rolling the mouse over the bottom of the **Presentation** pane, and then selecting on the content slider.

Important:

If the content slider is hidden, select and try again.

- Display the last slide by rolling the mouse over the bottom of the **Presentation** pane, and then selecting on the content slider.

Important:

If the content slider is hidden, select and try again.

- Navigate through the slides by rolling the mouse over the bottom of the **Presentation** pane, and using the slider to find the slide you want.

Important:

If the content slider is hidden, select and try again.

- Go to the previous slide by scrolling the slider to the left.
- Go to the next slide by scrolling the slider to the right.
- Return to the live presentation by selecting while viewing the last slide in the presentation Or

  Rolling the mouse over the bottom of the **Presentation** pane, and then selecting **LIVE** on the content slider.

Important:

If the content slider is hidden, select and try again.

Related Links

About Sharing Content on page 51

Annotating Shared Content during a Avaya Scopia® Desktop Videoconference

About this task

This section explains how to annotate shared content in the new content sharing solution deploying Avaya Scopia® Web Collaboration server.

Use the annotation feature to point at specific elements in your presentation. When in annotation mode, you can draw over and highlight the presented content. Viewing Presented Content during a Videoconference on page 55 shows annotations as they appear for other participants.

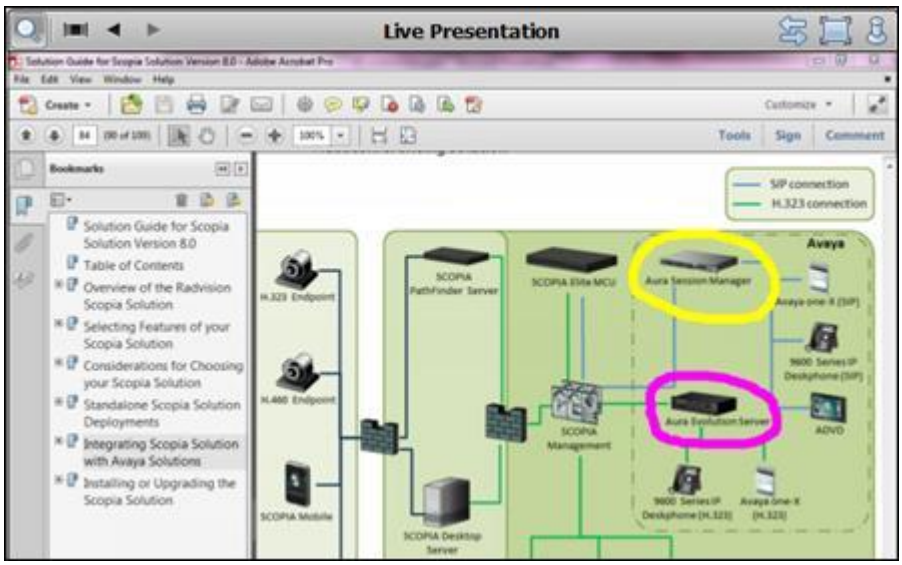


Figure 43: Annotations as they appear on a viewer's screen

Only the presenter can annotate. Their markup is displayed for all participants.

Procedure

1. From the **Presentation** pane, select **Palette tool** to choose color.

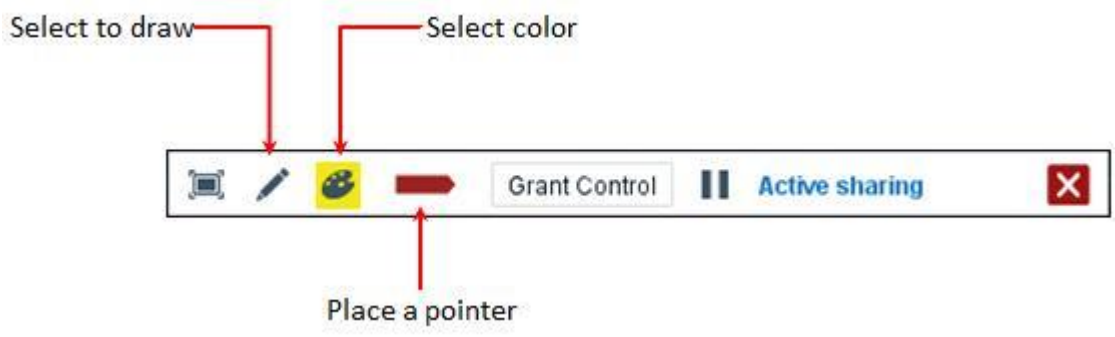


Figure 44: Presentation pane in the latest presentation solution

2. Select **Pen tool** to draw.
3. Select **Pointer tool** to place a pointer.
4. When finished, select **Pen tool** again to toggle off. All annotations you made are removed.

Related Links

About Sharing Content on page 51

Collaborating with Participants Using Whiteboards

About this task

The whiteboard feature allows all participants in the videoconference to successfully collaborate by illustrating their point.

Note:

Participants joining a videoconference from Avaya Scopia® XT Series endpoint, Avaya Scopia® Mobile or Avaya Scopia® Desktop Client not connected to the collaboration component (Avaya Scopia® Web Collaboration server), can see the whiteboard, but cannot draw on it.

When using this feature the layout of your virtual room changes to show the whiteboard area and its tools.

Figure 45: Video layout when using the whiteboard feature

Procedure

1. To create a new whiteboard, select **Present > Whiteboard**.

The whiteboard pane displays whiteboards saved from previous conferences, if any.

2. Select the required drawing or writing tool.

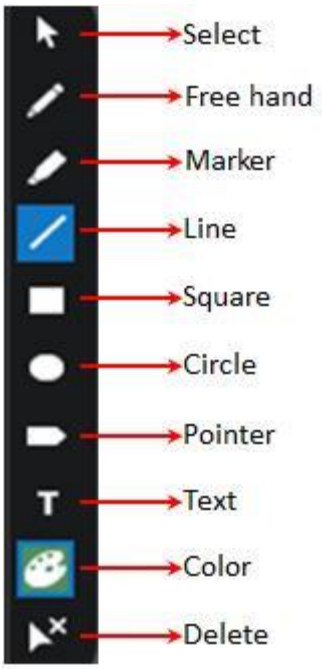


Figure 46: Drawing and writing tools

3. Illustrate your point in the **Shared** area.
4. To modify the way the whiteboard appears on your screen:
   - Use the **Zoom** slider to make the shared content of the whiteboard appear smaller or larger.
   - Use **Autofit** tool to resize the **Shared** area to fit the screen.
5. To delete the whiteboard, select the **Delete** tool, and then select **OK** in the confirmation message.

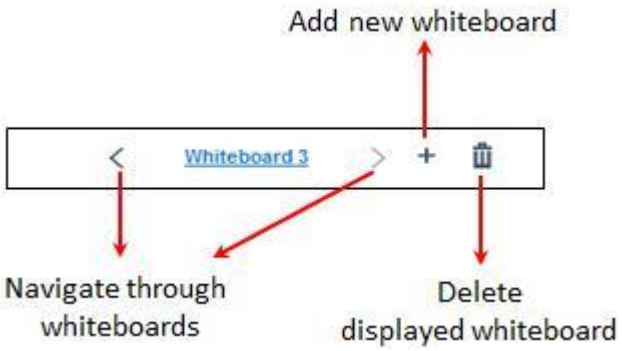


Figure 47: Navigating and managing your whiteboards

6. To add a new whiteboard, select the **Add** tool.

7. To navigate between your whiteboards, select the arrow buttons.
8. To save the whiteboard, create another one or select **Present > End Presentation**.

Related Links

About Sharing Content on page 51

Presenting Content Using an Avaya Scopia® XT Series Endpoint

About this task

Users can present content from a laptop on an XT Series monitor without connecting it to the XT Codec Unit, using the Avaya Screen Link feature. If you are also using the XT Series for a videoconference, the content is shared with all participants of the meeting, both located in the same room and remote.

Depending on its security configuration, an XT Series endpoint behaves in one of the following ways when you to connect to it:

- **Rejects Screen Link** — the endpoint does not allow anyone to connect to it for screen sharing.
- **Requires password** — the endpoint generates a one time password that you need to enter on your laptop to connect to it.
- **Seamlessly authenticates Scopia® Desktop Client and connects to it**

Before you begin

- If you want to present content to local participants only, make sure that the XT Series endpoint is not currently used for a videoconference. If you are using the endpoint for an audio-only call, you can share the presentation with participants in the meeting room.
- To present content from your laptop, bring the laptop into a videoconference room equipped with an XT Series endpoint.
- To display your computer's content on the XT Series using Avaya Screen Link, your computer must have Scopia® Desktop Client installed and be in the same network as the endpoint. If the computer and endpoint are in different networks, make sure there is no NAT or firewall between them.
  - For automatic pairing (using proximity sensing), the computer's speakers must be able to play audio at up to 19KHz.
  - The proximity pairing is designed to work in proximity to the endpoint's microphone. The optimal distance is up to 1-1.5 m. The exact distance depends on the type of microphone pod used (one way or three way) and the computer's gain levels.
  - When automatic proximity does not work, use manual pairing.

Procedure

1. Choose an XT Series endpoint from the list of endpoints found by Scopia® Desktop Client:
   a. Right-click the Scopia® Desktop icon and select **Screen Link > Start Screen Link**.

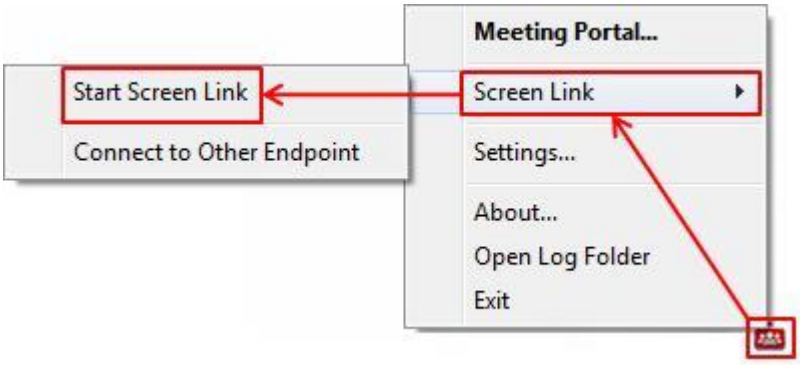


Figure 48: Starting to share content using the XT Series endpoint

Your Scopia® Desktop Client looks for accessible XT Series endpoints and displays a list of endpoints you can connect to.

b. Select the XT Series endpoint that you want to use.

c. If the endpoint you want to use does not appear in the list, connect to it as described in Step 2 on page 62.

2. Connect to the XT Series endpoint by its IP address:

a. Turn on the XT Codec Unit by pressing the Power key on the XT Remote Control Unit.

The monitor displays this endpoint's IP address.

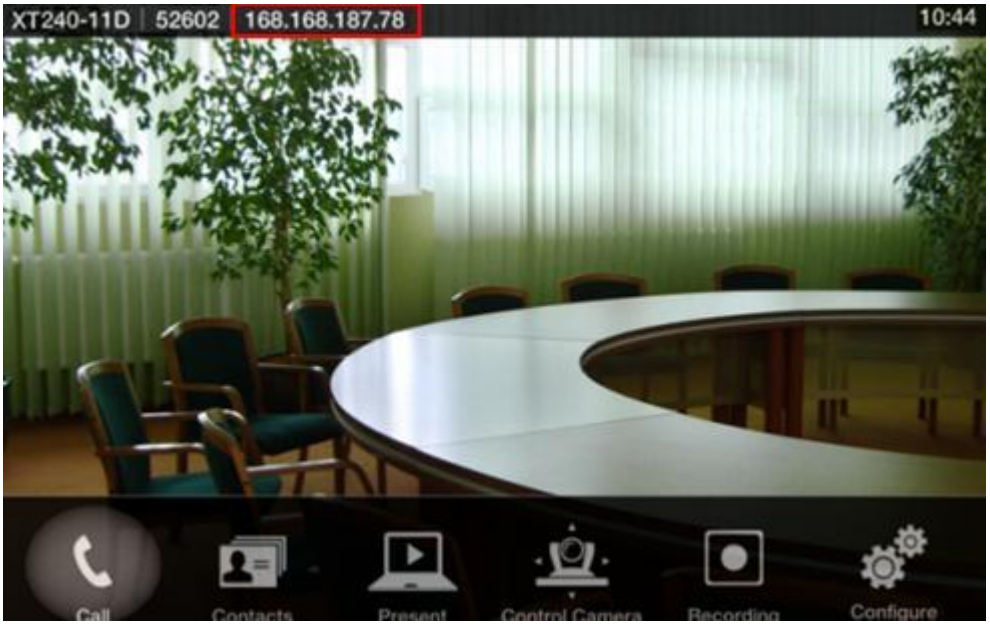


Figure 49: IP address displayed on the XT Series monitor

b. Right-click the Scopia® Desktop icon and select **Screen Link > Connect to Other Endpoint**.

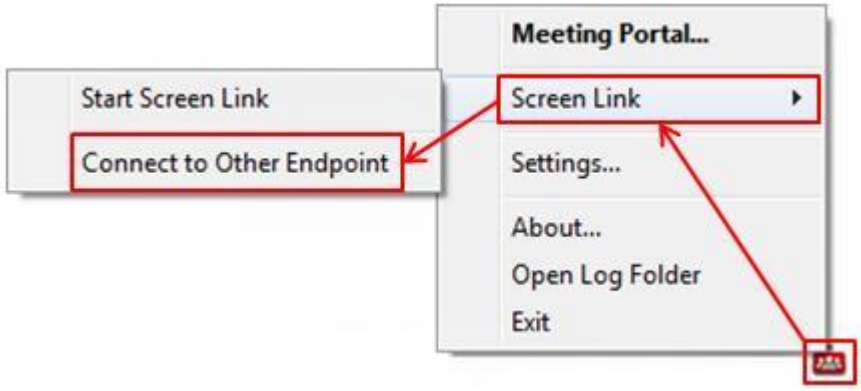


Figure 50: Connecting to an XT Series endpoint by its IP address

c. Enter the IP address of the endpoint on your laptop.

d. Select **OK**.

3. If the XT Series endpoint is protected with a password, enter the password displayed on the endpoint screen.

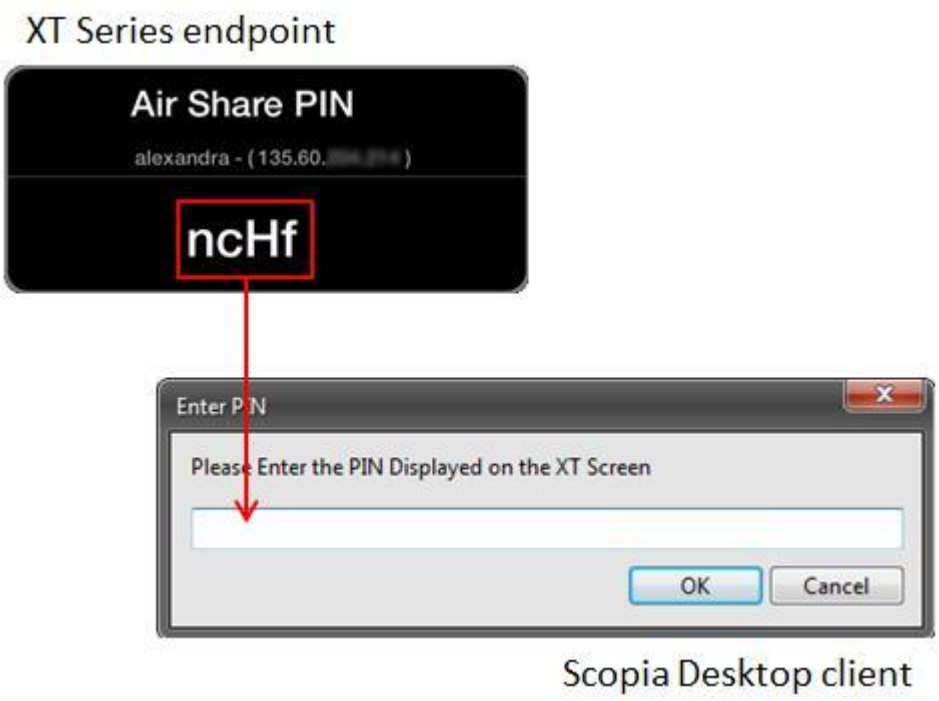


Figure 51: Entering the XT Series endpoint password

The content is displayed on the screen of the XT Series endpoint or the content is shared with remote participants.

4. To stop presenting your content on the endpoint screen, right-click the Scopia® Desktop icon and select **Screen Link > Stop Screen Link.**

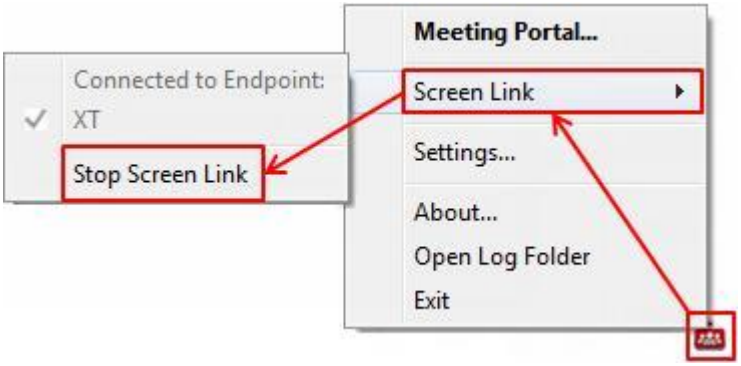


Figure 52: Stopping to share content using the XT Seriesendpoint

Related Links

About Sharing Content on page 51

Changing Your Video Layout during a Videoconference

About this task

A video layout is the arrangement of participant images as they appear on the monitor in a videoconference. If the meeting includes a presentation, a layout can also refer to the arrangement of the presentation image together with the meeting participants.

Scopia® Desktop offers a wide variety of video layouts and features that make your videoconferencing experience optimal.

The automatic video layout dynamically adjusts the number of frames displayed to the number of participants in the videoconference. When someone joins the videoconference, it automatically switches the layout by adding a new frame. It can display up to the maximum number of participants (28) in the same view, putting the active speaker in the larger frame. The automatic video layout is usually used as the default layout. Alternatively you can choose video layouts with a fixed number of shown participants. The change you make to your video layout, is not saved by your Scopia® Desktop Client so that when you access your virtual room next time the default layout is used.

You can use the Picture-in-Picture (PIP) and Self-See features to see your own video without transmitting it to other users. In addition, you can choose the position of the Picture-in-Picture frame so that it does not overlap important information on your screen.

Procedure

To change your video layout during a videoconference, perform one of the following:

- To swap positions of the video and presentation panes, select  .

Figure 53: Swapping positions of video and presentation frames

- To change your video layout, select  > **My Layout**, and then select the layout.

Access video layout options

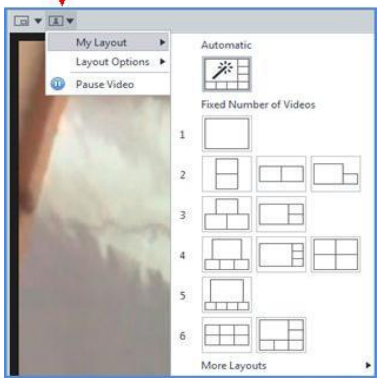


Figure 54: Changing the video layout

- To remove/add your own video from your video layout, select  > **Layout Options** > **Enable Self-See**.

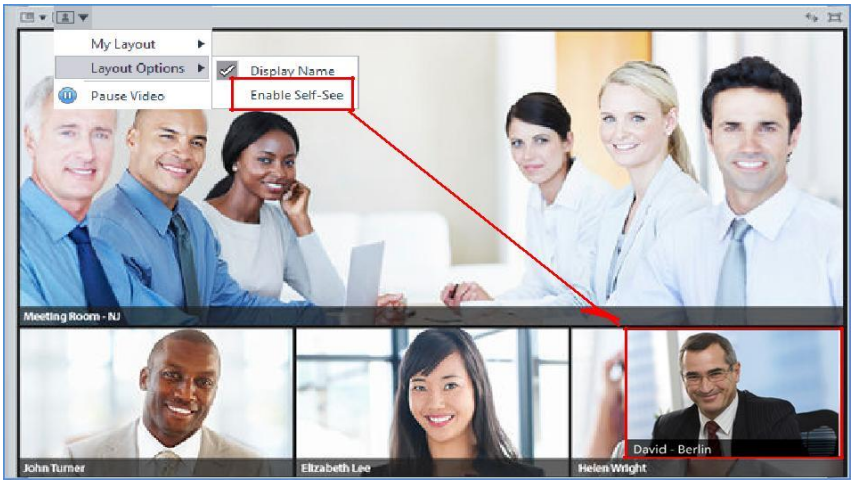


Figure 55: Enabling the Self-See pane

- See your own video in a Picture-in-Picture frame, select  and select the position of the Picture-in-Picture frame.

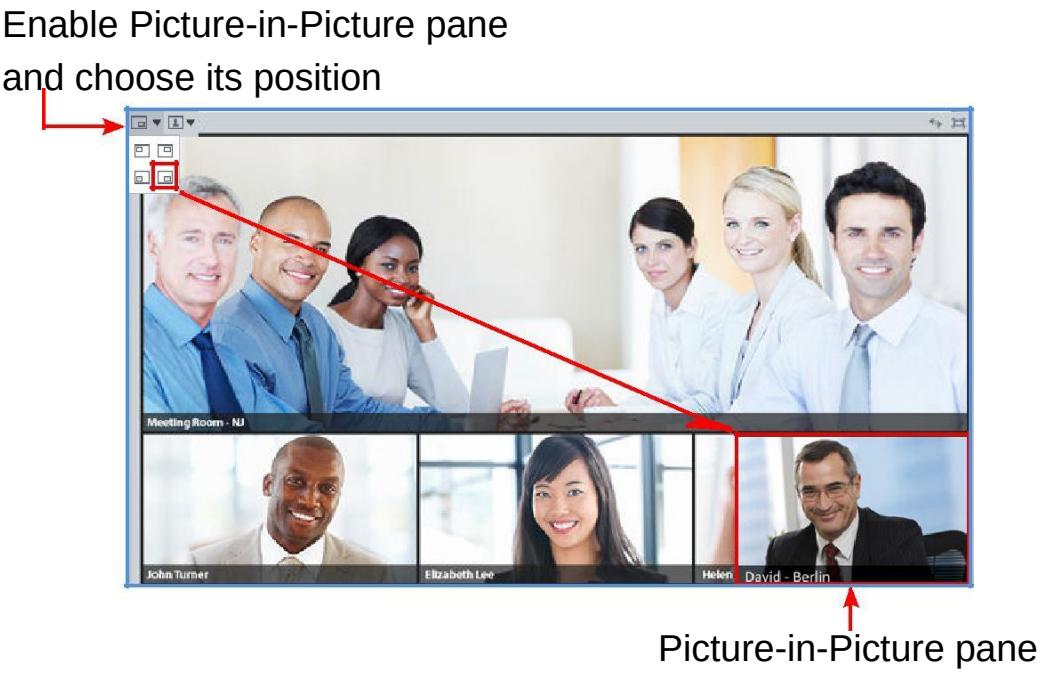


Figure 56: Enabling the PIP pane

- Display/hide participants' names, select  > **Layout Options** > **Display Name**.

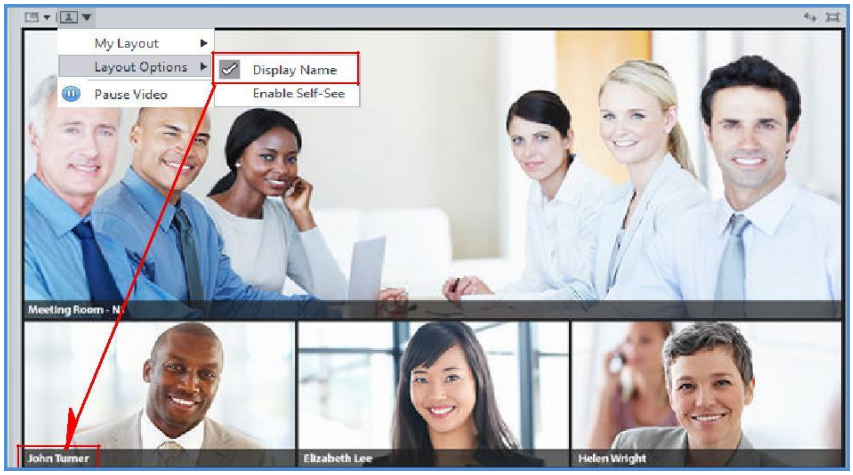


Figure 57: Displaying names in video frames

Related Links

Participating in a Scopia® Desktop Videoconference on page 37

Moderating Other Participants

About this task

Moderator is a participant who can control other participants in a videoconference, for example, to mute or disconnect them. By default, the owner of the virtual room always has moderation rights. Depending on your organization's policy virtual rooms can be protected with a moderator PIN which gives access to the moderation features. Any participant who enters the moderator PIN, can moderate.

You can moderate other participants during a videoconference in your virtual room by muting, blocking their cameras and disconnecting them from the videoconference.

If the videoconference takes place in another participant's virtual room which is protected, you cannot moderate other participants unless you know the moderation PIN.

Procedure

Control other participants by performing one of the following:

- To mute a participant, either right-click on this participant's name in the **Participants list** and select **Mute Participant** or select **Moderate** > **Mute** and select this participant's name. Alternatively, select the microphone icon next to the participant’s name.

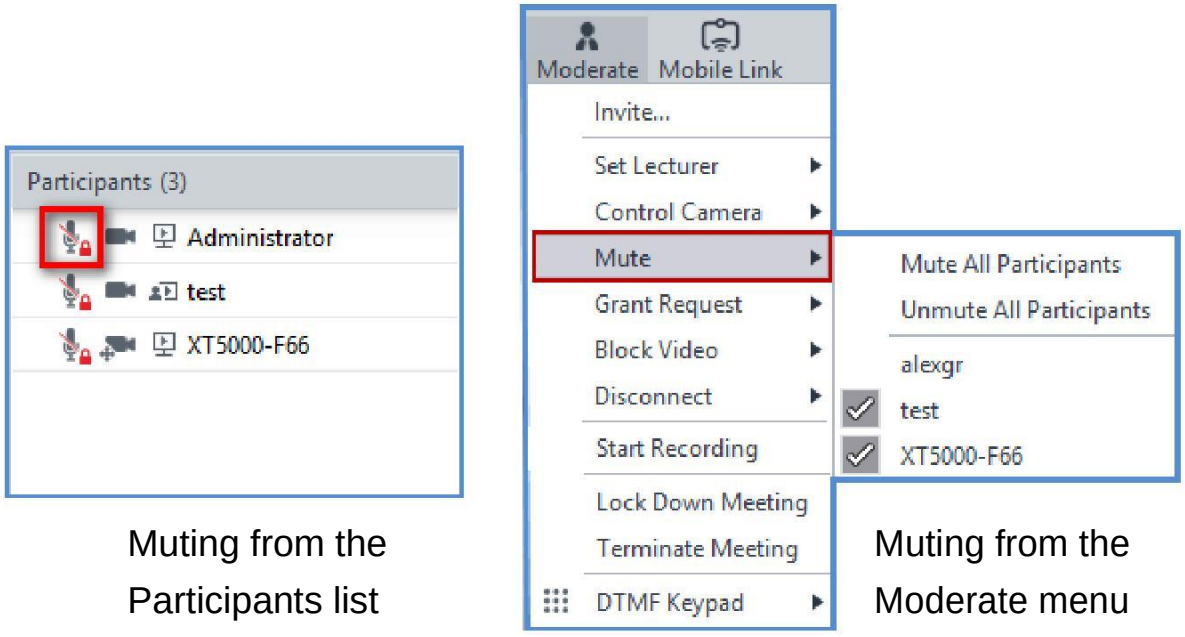


Figure 58: Muting a participant

- To block a participant's video, select the camera icon in the **Participants list** to toggle blocking a participant's video. Alternatively, right-click on this participant's name and select **Block Participant** or select **Moderate** > **Block Video** and select this participant's name.

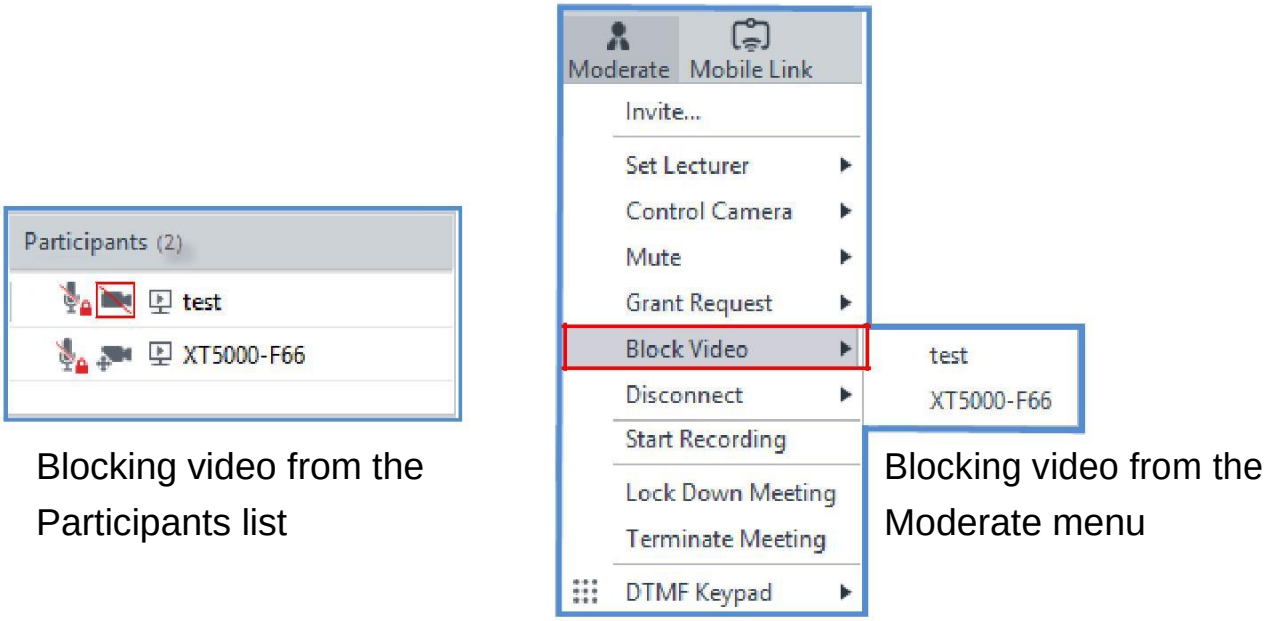


Figure 59: Blocking a participant

- To disconnect a participant, either right-click on this participant's name in the **Participants list** and select **Disconnect Participant** or select **Moderate** > **Disconnnect** and select this participant's name.

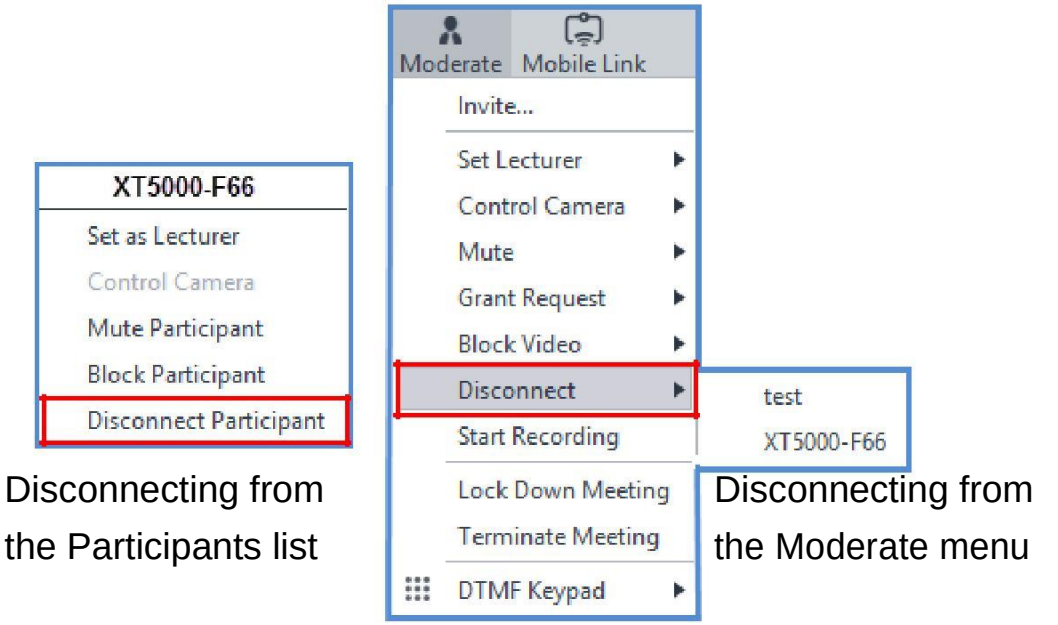


Figure 60: Disconnecting a participant

Related Links

Participating in a Scopia® Desktop Videoconference on page 37

Granting permission to a participant to join a locked videoconference

About this task

If you protected your videoconference by barring new participants from joining, they can ask permission to join the videoconference. This procedure describes how to grant permission to join a locked videoconference.

When a new participant asks permission to join your locked videoconference, the virtual room owner or the moderator of the videoconference receive an audio alert and a message.

The message is displayed until you answer it, it times out, or the user cancels the request. If there are several users requesting to join, the screen displays all the request messages.

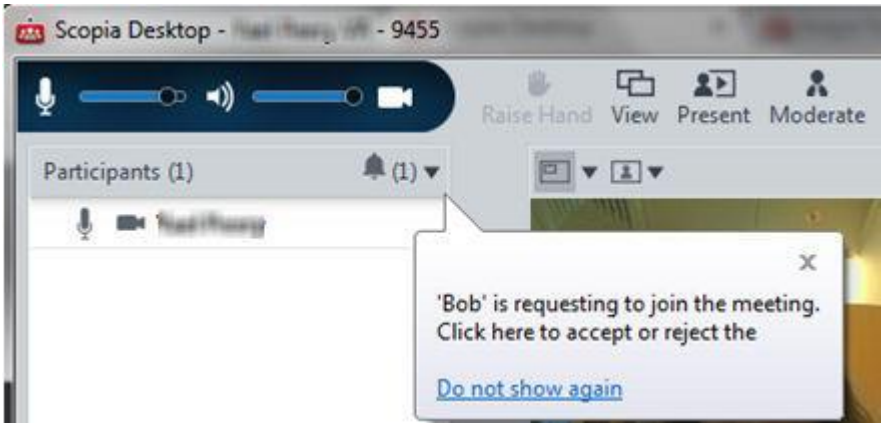


Figure 61: Requesting to join a meeting

Before you begin

If you want to grant permission to new participants from the videoconference that is held in another user's virtual room and this virtual room is protected with a moderator PIN, ask the owner to send the PIN. We recommend that the PIN is sent privately.

Make sure that the **Allow requests to join locked meetings** feature is enabled in your virtual room settings as described in Customizing Your Virtual Room on page 23.

Procedure

1. Grant permission to join:
   - For one participant, open the dropdown list under , select the participant's name, and then select **Admit to Meeting**.

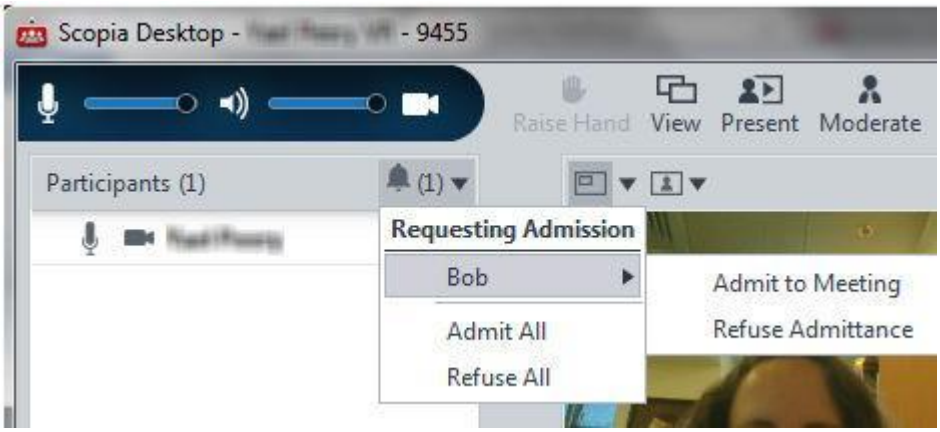


Figure 62: Admitting participants to a meeting

Or

- For multiple participants, select **Admit All**.

The new participants join the videoconference.

2. Reject permission to join:
   - For one participant, select the name of the participant requesting permission to join, and then select **Refuse Admittance**.

     Or
   - For multiple participants, select **Refuse All**.

   The new participants are barred from joining your videoconference.

Related Links

Participating in a Scopia® Desktop Videoconference on page 37

Blocking Your Audio and Video during a Scopia® Desktop Videoconference

About this task

You can adjust the volume of your microphone and speakers, and disable your camera as shown in Figure 63: Controlling Your Video and Audio on page 71.

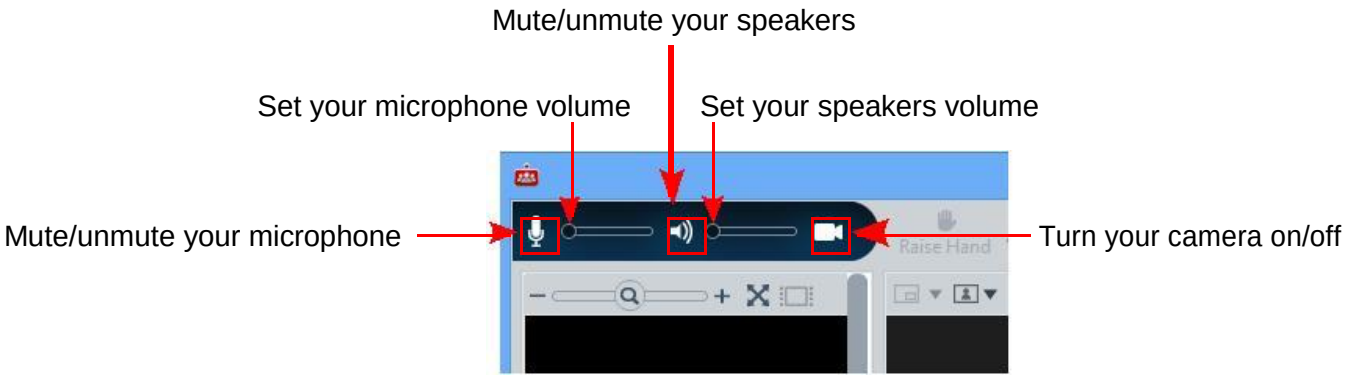


Figure 63: Controlling Your Video and Audio

You can also control other participants' audio and video, for more information see Moderating Other Participants on page 67.

Related Links

Participating in a Scopia® Desktop Videoconference on page 37

Using Text Chat during a Videoconference

About this task

In addition to audio, video, and data in a videoconference, you can also use the chat feature to send text messages. You can chat publicly (for all participants to see your messages) or privately (sending your messages to one participant only).

Procedure

1. From the list above the text insertion field, select **Public** or the name of the participant to whom you want to send your message. See Figure 64: Icons of the Chat pane on page 72.

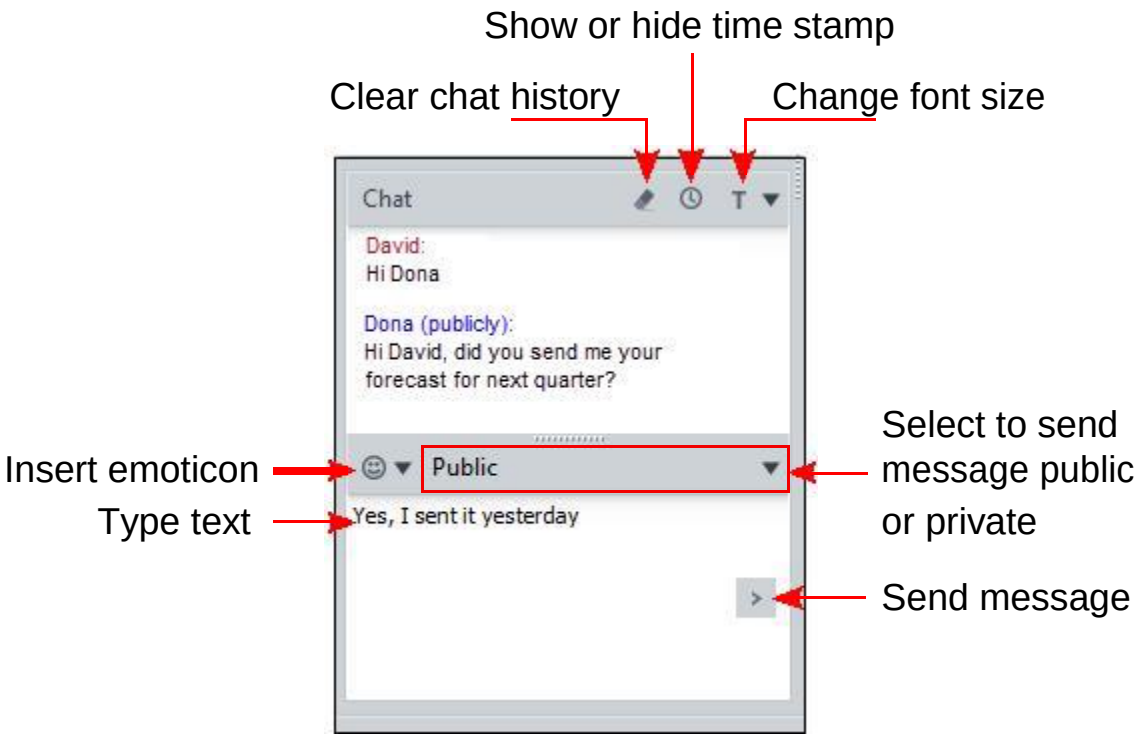


Figure 64: Icons of the Chat pane

2. Enter text in the text pane.
3. To insert an emoticon, select  and then select an emoticon.
4. Select **Send Message** or press Enter.

   The message is sent and appears in the chat history.
5. If necessary, customize the chat history:
   - Show or hide the time stamp by selecting **Time Stamp** (see Figure 64: Icons of the Chat pane on page 72).
   - Change the font size by selecting **Font Size** (see Figure 64: Icons of the Chat pane on page 72).
6. To remove the chat history, select **Clear Chat** and select **Yes** in the confirmation message.

Related Links

Participating in a Scopia® Desktop Videoconference on page 37

About 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.

The video layout of the Virtual Room window in lecture mode stays the same.

Related Links

Participating in a Scopia® Desktop Videoconference on page 37 Using Lecture Mode as a Lecturer on page 73
Requesting Permission to Speak in Lecture Mode on page 75

Using Lecture Mode as a Lecturer

About this task

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.

You need to have moderator's rights to set yourself or any other participant as a lecturer.

If a participant asks permission to speak, you see a notification and a hand icon next to the participant's name in the **Participants** list, as shown in Figure 66: Display of participant requesting to speak on page 74.

Before you begin

Always use your own virtual room and configure the moderator PIN as described in Protecting Videoconferences in Your Virtual Room on page 77.

Procedure

1. From the **Participants list**, right-click the name of the participant, and select **Set as Lecturer**. See Figure 65: Setting the lecturer during a videoconference on page 74. Or

   In the **Virtual Room** window, select **Moderate** > **Set Lecturer**, and then select the name of the participant.

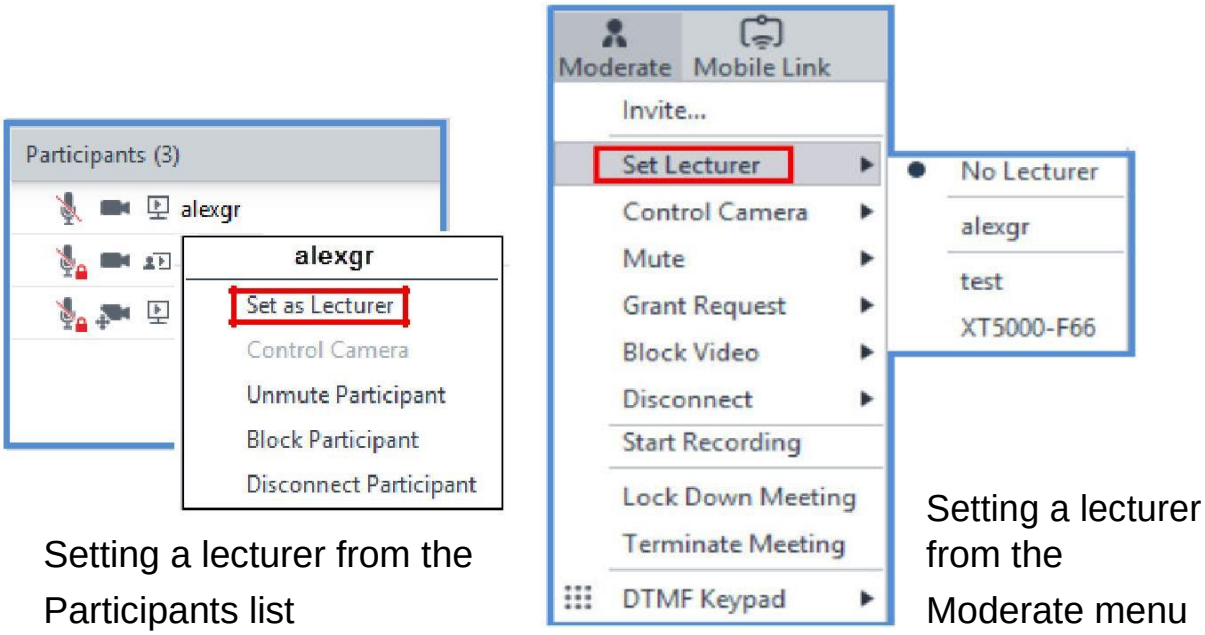


Figure 65: Setting the lecturer during a videoconference

2. To grant permission to speak when a participant requests permission, select the hand icon in the **Participants** list (Figure 66: Display of participant requesting to speak on page 74) and select **Yes** in the confirmation message.

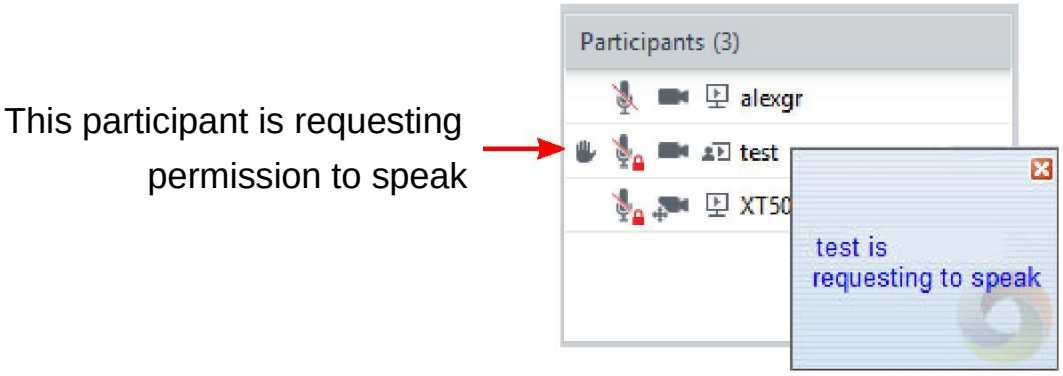


Figure 66: Display of participant requesting to speak

The participant is unmuted and can speak.

3. To leave the Lecture mode, select **Moderate** > **No lecturer** Or

   From the **Participants list**, right-click the name of the current lecturer and select **Unset as Lecturer**.

Related Links

About Lecture Mode on page 72

Requesting Permission to Speak in Lecture Mode

About this task

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.

When you are a participant in a videoconference, you can request permission from the lecturer to speak, as described below.

Procedure

If you are not a lecturer and you want to speak, select **Raise Hand**  .

The lecturer is notified and can unmute you.

Related Links

About Lecture Mode on page 72

Leaving or Ending a Scopia® Desktop Videoconference

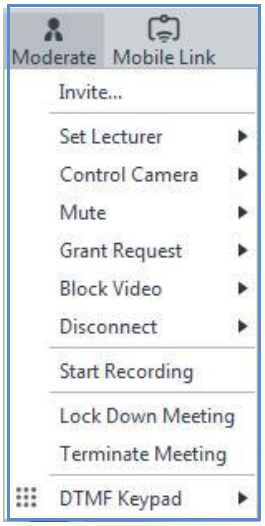
About this task

You can leave a videoconference at any moment. If you leave the videoconference as a participant, the videoconference goes on without you. If you are the moderator of the videoconference, you can also terminate the videoconference when you leave it, so that the virtual room closes and all participants are disconnected from the videoconference.

Table 5: Leaving a videoconference

To	Do this
Leave a videoconference	1. In the **Virtual Room** window, select **Leave Meeting**  2. Select **Yes** in the confirmation message. The **Virtual Room** window closes. You have left the videoconference.
Terminate a videoconference	1. In the **Virtual Room** window, select **Moderate**. 2. If necessary, enter the moderator PIN and select **OK**. 3. Select **Terminate Meeting** from the **Moderate** menu.

Table continues…

To	Do this
	 4. Select **Yes** in the confirmation message. The **Virtual Room** window closes. You have terminated the videoconference. All other participants receive a notification that the videoconference is terminated.

Related Links

Participating in a Scopia® Desktop Videoconference on page 37

Chapter 5: Securing your Scopia® Desktop Videoconference

You can secure your videoconferences to provide a safe place for communication by protecting your virtual room with PINs and by stopping new participants from joining an ongoing videoconference in your virtual room.

Related Links

Protecting Videoconferences from Your Virtual Room on page 77

Barring New Participants from Joining Scopia® Desktop Videoconferences on page80

Protecting Videoconferences from Your Virtual Room

About this task

Your organization can secure video communications by protecting all virtual rooms and defining user authorization centrally. This section explains how to protect your virtual room if no such protection was performed centrally.

By default, all users, both signed-in and guest users, can access and moderate videoconferences in any virtual room. However, you can protect your virtual room to a varying degree using PINs:

- Setting an access PIN restricts the number of participants to users who know the access PIN and can join a videoconference in this virtual room.
- Setting a moderator PIN restricts the number of participants who can moderate to users who know the moderator PIN of this virtual room.

Table 6: Protecting a virtual room on page 78 explains degrees of protection and the necessary configuration.

Table 6: Protecting a virtual room

Level of Protection	Description	Necessary Configuration
No protection	All users can access this virtual room and moderate Videoconferences in it.	Default configuration
Partial protection	Only users with the access PIN can access this virtual room. All signed-in participants can moderate a Videoconference held in this virtual room.	The owner of this virtual room must define the access PIN.
Partial protection	All users can access this virtual room ,but only users who have the moderator PIN can moderate. Guest users cannot moderate.	The owner of this virtual room must define the moderator PIN.
Full protection	Only signed-in users with the access and the moderator PINs can use this virtual room.	The owner of this virtual room must define both the moderator PIN and the access PIN.

If a virtual room is protected, its owner must share relevant PINs with other users to give them access to the videoconference or allow them to moderate in this virtual room.

In addition to protecting your videoconferences, you can lock videoconferences in progress so that no new participants can join as described in Barring New Participants from Joining Scopia® Desktop Videoconferences on page 80.

Before you begin

We recommend that you contact your video network organization to find out if your virtual room is protected centrally or not.

Procedure

1. Log in to your virtual room as described in Logging in to the Scopia® Desktop Web Portal on page 18.
2. Select **Settings**.

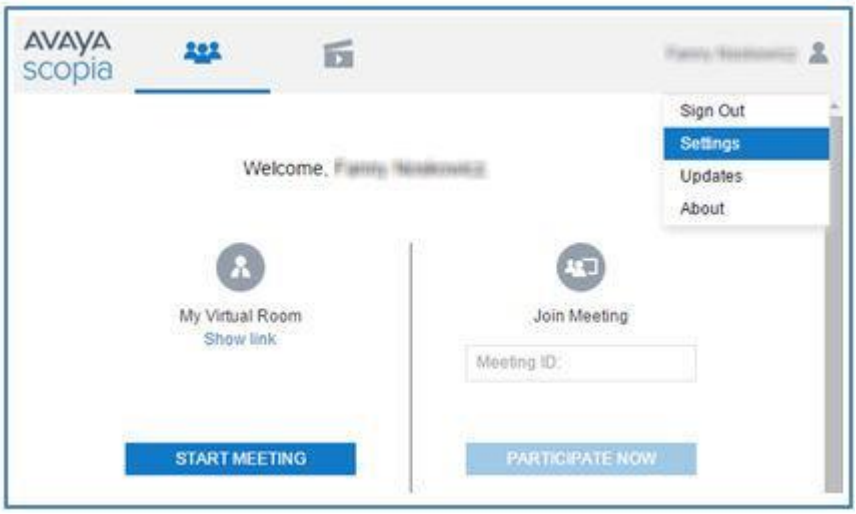


Figure 67: Accessing Scopia® Desktop Client settings

3. Select the **Virtual Room** tab.

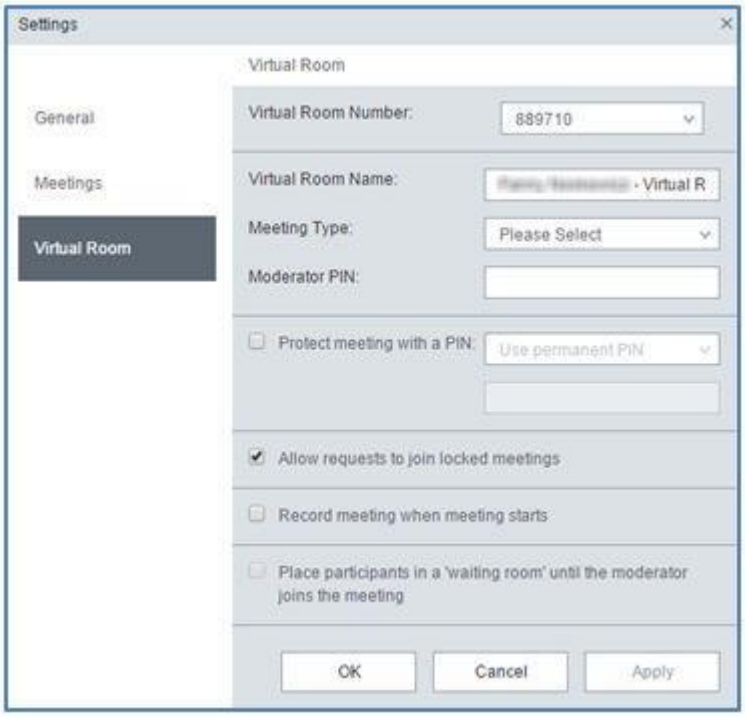


Figure 68: Virtual Room tab

4. To set the moderator PIN, enter a value in the **Moderator PIN** field.
5. To set the access PIN, select **Protect meeting with a PIN**, and then select one of the following:
   - **Use permanent PIN**

This PIN is the access PIN for all videoconferences held in your virtual room.

- **Use one-time PIN for each meeting**

  Enter a new access PIN at the beginning of every videoconference you create in your virtual room, as described in Starting a New Scopia® Desktop Videoconference in Your Virtual Room on page 37.

6. Select **OK**.

Related Links

Securing your Scopia® Desktop Videoconference on page 77

Barring New Participants from Joining Scopia® Desktop Videoconferences

About this task

You can secure your videoconference by barring new participants from joining a videoconference after everybody you wanted to join did so.

Before you begin

If you want to bar new participants from the videoconference that is held in another user's virtual room and this virtual room is protected with a moderator PIN, ask the owner to send the PIN. We recommend that the PIN is sent privately.

You can still allow new participants to request permission to join your videoconference and let them join or reject the request. For more information, see Granting permission to a participant to join a locked meeting on page 69.

Procedure

1. In the Virtual Room window, select **Moderate**.
2. If necessary, enter the moderator PIN and select **OK**.
3. Select **Lock Down Meeting**.

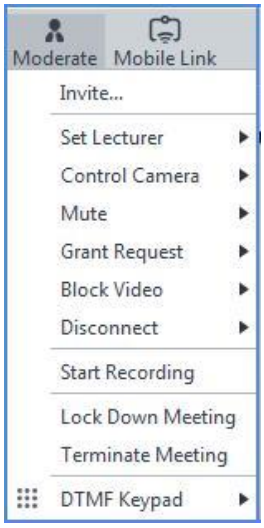


Figure 69: Moderate menu

The videoconference is locked, indicated by the icon on the status bar of the **Virtual Room** window.

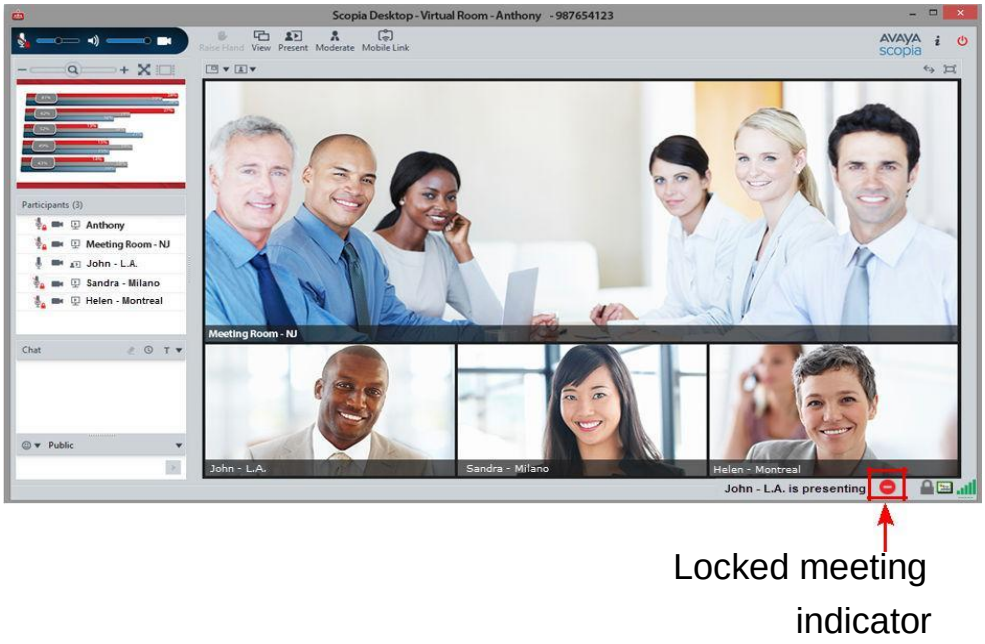


Figure 70: Locked meeting indicator shown in the Virtual Room window

4. To unlock the videoconference, select **Moderate** > **Lock Down Meeting** again to toggle off.

Related Links

Securing your Scopia® Desktop Videoconference on page 77

Chapter 7: Troubleshooting Scopia® Desktop Client

These tips list useful troubleshooting solutions. If the Scopia® Desktop Client still malfunctions, contact your local support representative for help.

Related Links

Hearing Other Participants in a Videoconference on page 82
Collecting Logs for Customer Support on page 85
Configuring Logging Parameters of your Scopia® Desktop Client on page86
Having Problems with Call Quality on page 87

Hearing Other Participants in a Videoconference

Problem

You cannot hear one or all of the participants.

Cause 1

This participant is muted.

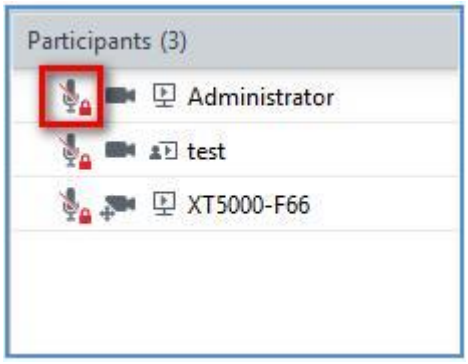


Figure 94: Participant marked as muted in the Virtual Room window

Solution 1

If you can moderate this videoconference, unmute the participant as described in Moderating Other Participants on page 67. If you do not have moderation rights, let this participant know about the problem using **Text Chat**. See Using Text Chat during a Videoconference on page 71.

Cause 2

The audio is muted or volume is set to too low.

Solution 2a

Make sure the volume control is not muted in your **Virtual Room** window as shown below.

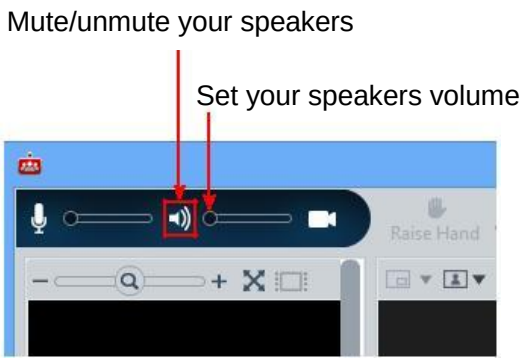


Figure 95: Controlling the speakers

Solution 2b

Make sure that the device you use to play audio (speakers, speakerphone, headphones) is not muted.

Cause 3

If there are several audio output devices connected to your computer, the system may be using the audio from a different device to the one used by your Scopia® Desktop Client .

Solution 3

Perform one of the following:

- Change Windows to use the same audio device as your Scopia® Desktop Client .
- Change the Scopia® Desktop Client settings to align with the computer's chosen audio device, as explained in Checking Audio and Video Configurations for your on page 20.

Cause 4

You computer audio settings are not configured correctly.

If this is the cause, you cannot hear any audio using other applications on your computer.

Solution 4

Check that the speakers/headphones volume is not too low: 1.

Try to play audio on another program or application.

2. If you cannot hear any audio on any application, you need to change the operating system's volume settings. For example, in Windows, on the **Windows System Tray**, select the **Speakers** icon as shown below.

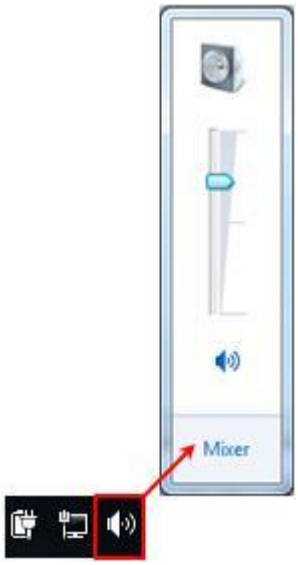


Figure 96: Adjusting the speakers volume from the System Tray

3. Move the slider up to adjust the volume.

Cause 5

Your audio device (headphones or speakerphone) is connected to the wrong socket.

Solution 5

Depending on the type of the device connector, perform one of the following:

- If your device has two audio connectors, one for audio in and one for audio out, check that you plugged these connectors into the corresponding sockets on your computer.
- If your device has a USB connector, check that it is plugged into a USB port which is directly connected the motherboard, not a USB hub.

  USB hub connectors may not transmit enough power for your audio device. USB ports which are directly connected to the motherboard are usually located next to other computer connectors like the VGA or HDMI socket. On a desktop computer, USB ports together with other connectors are typically located on the rear panel.

Related Links

Troubleshooting Scopia® Desktop Client on page 101

Collecting Logs for Customer Support

About this task

When reporting a problem to customer support, you may be asked to collect and send logs of your Scopia® Desktop Client.

Procedure

1. Right-click the Scopia® Desktop icon and select **Open Log Folder**.

Figure 97: Selecting Settings from the system tray menu

The **Windows Explorer** window opens.

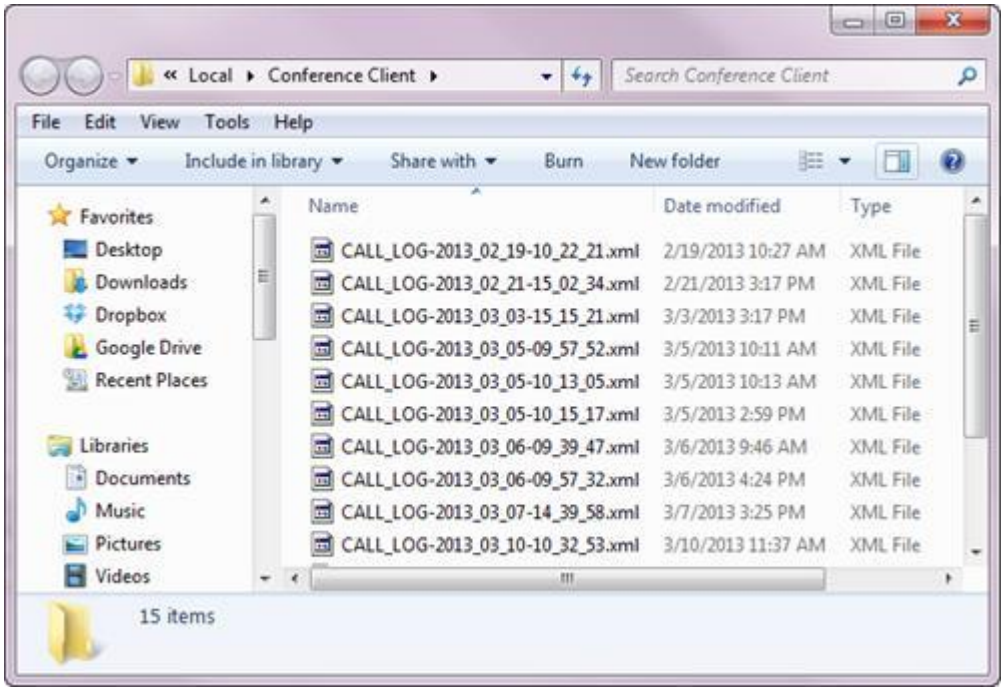


Figure 98: Log files showing in the Windows Explorer window

2. Select the relevant log file using its time stamp.

3. Copy the file and send it to Avaya customer support.

Related Links

Troubleshooting Scopia® Desktop Client on page 101

Configuring Logging Parameters of your Scopia® Desktop Client

About this task

You can customize the level of detail and back catalogue of Scopia® Desktop Client logs to submit to customer support if needed.

Procedure

1. Right-click the Scopia® Desktop icon and select **Settings**.

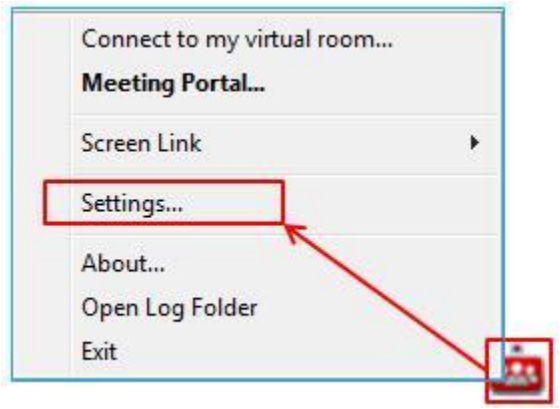


Figure 99: Selecting Settings from the system tray menu

The **Settings** window opens.

2. Select the **Advanced** tab.

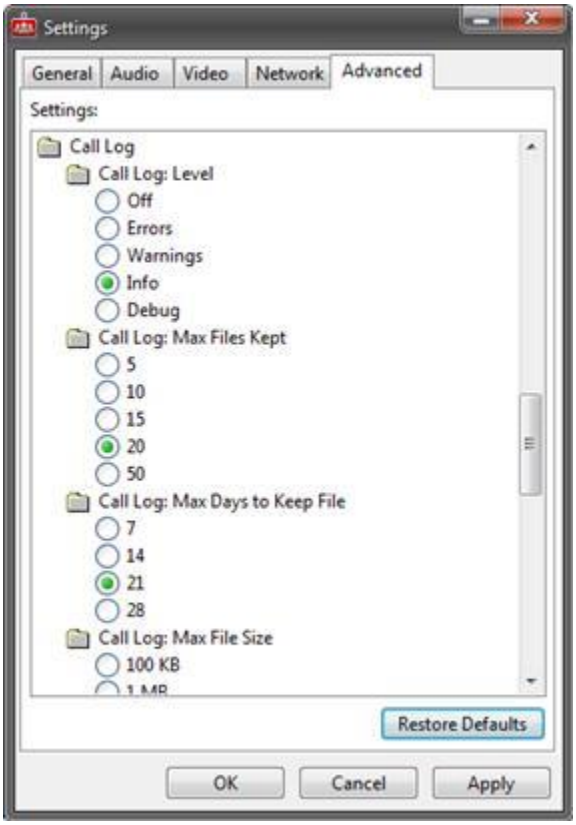


Figure 100: Setting the log level

3. Set the following details for logs:
   - **Level** determines the level of detail in the logs. Customer support may ask you to set this value to **Debug** during troubleshooting.
   - **Max Files Kept**, **Max Days to Keep File**, **Max File Size** and **Max Disk Used** determine the amount of space used by logs.
4. Select **OK**.

Related Links

Troubleshooting Scopia® Desktop Client on page 101

Having Problems with Call Quality

Problem

The quality of video or audio is poor from the beginning or degrades during the meeting. You cannot see or hear your other participants well or other participants cannot see you well.

Cause

There is not enough bandwidth or the signal on wireless networks is not strong enough. Good networking conditions are crucial for the videoconferencing experience because they define the quality of your audio, video and presentation in a meeting.

Solution

1. In the **Virtual Room** window, check the **Network Conditions** indicator in the lower right corner
2. Check if you have problems with network connection, as described in the Table 9: Checking the network conditions on page 107.

Table 9: Checking the network conditions

Indicator shows	Description
	Network conditions are optimal. The problems you experience with your call quality are not caused by the network conditions.
	There are minor network issues, but the call quality is not affected. The problems you experience with your call quality are not caused by the network conditions.
	There are minor network issues that may affect your meeting experience. Avaya Scopia® Desktopis trying to minimize the impact on your call quality.
	There are moderate network issues that may affect the call quality. Avaya Scopia® Desktopis trying to minimize the impact on your call quality.
	There are severe network issues that cause problems with your call quality . You may turn video off temporarily until the network conditions improve.

3. To see more details on your network connection, select the **Network Conditions** indicator. The **Current call** window opens, displaying details of your network connection.

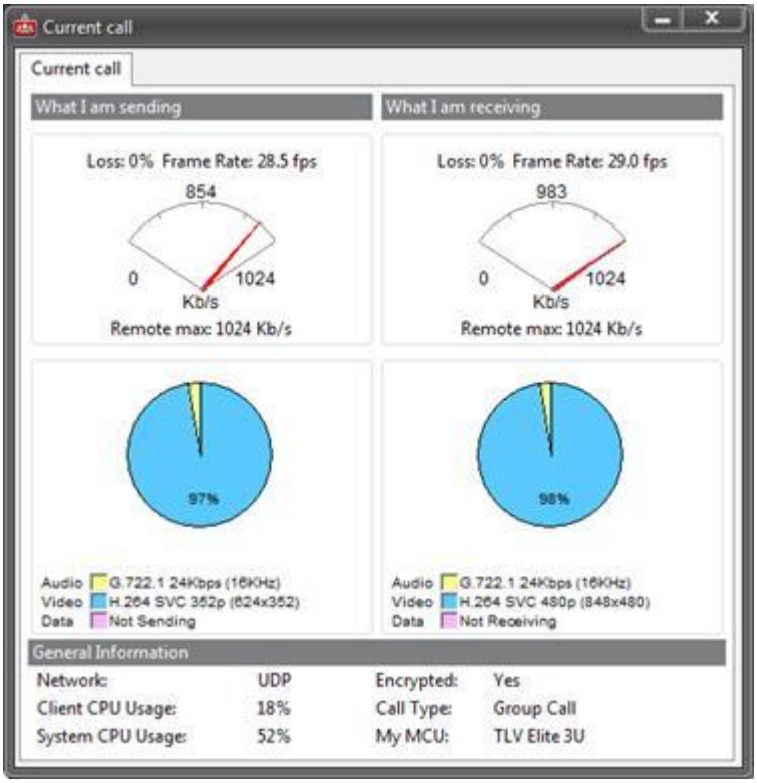


Figure 101: Network connection details in the Current call window

Related Links

Troubleshooting Scopia® Desktop Client on page 101

Glossary

1080p	See Full HD on page 113.
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 115.
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.

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.

Call Control

See Signaling on page 120.

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.

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).

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 111.
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.
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 109.
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 112.
FPS	See Frames Per Second on page 113.
Frame Rate	See Frames Per Second on page 113.
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 114.

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 109.

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 115.

High Profile See H.264 High Profile on page 114.

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 119.

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 117.

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 111.

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 111.
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.
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 111.
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 117.
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 119.

SIP Server A SIP server is a network device communicating via the SIP protocol.

SIP URI See URI on page 123.

Slider See Content Slider on page 111.

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 120.

Standard Definition See SD on page 120.

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 123.
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 123.
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 119.
Video Switching	See Switched video on page 122.
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.

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.
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.