# Deployment Guide for Avaya Scopia Web Collaboration server


Release 8.3.2
Issue 8.3.2
May 2015

**Notice**

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

**Documentation disclaimer**

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

**Link disclaimer**

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

**Warranty**

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

**Hosted Service**

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

**Licenses**

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

**License types**

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

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

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

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

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

**Copyright**

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

**Virtualization**

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

**Third Party Components**

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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

**Note to Service Provider**

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

**Preventing Toll Fraud**

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

**Avaya Toll Fraud intervention**

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

**Downloading Documentation**

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

**Contact Avaya Support**

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

**Trademarks**

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

Avaya is a registered trademark of Avaya Inc.

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

# Contents

# Chapter 1: About Scopia® Web Collaboration server

The Scopia® Web Collaboration server is a new video network device that provides the advanced content sharing functionality for your Avaya Scopia® Solution. Before this product was introduced, Avaya Scopia® Solution offered standard content sharing capabilities. Avaya Scopia® Desktop streamed presentations as video, which led to the following restrictions: only one person presenting and annotating at a time while other participants can only passively watch the presentation. When the new Scopia® Web Collaboration server is deployed, the following content sharing features are available:

- 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.

This creates a very rich experience, much like when people meet in the same room to share and discuss ideas.

Scopia® Web Collaboration server is compatible with Avaya Aura® Communicator, and customers using the Avaya Aura® Communicator client can also take part in Scopia® Desktop meetings and enjoy content sharing capabilities.

Scopia® Web Collaboration server transfers presentations between Scopia® Desktop Clients as JPEG images instead of video as with content sharing powered by Scopia® Desktop. As a result, user experience is improved and presentations consume less bandwidth. Participants using videoconferencing endpoints and room systems, like Avaya Scopia® XT Series, can view shared content. To support these users, Scopia® Web Collaboration server sends a presentation as video in the legacy H.239 format via Scopia® Elite MCU. These participants can view the presentation, but cannot annotate it.

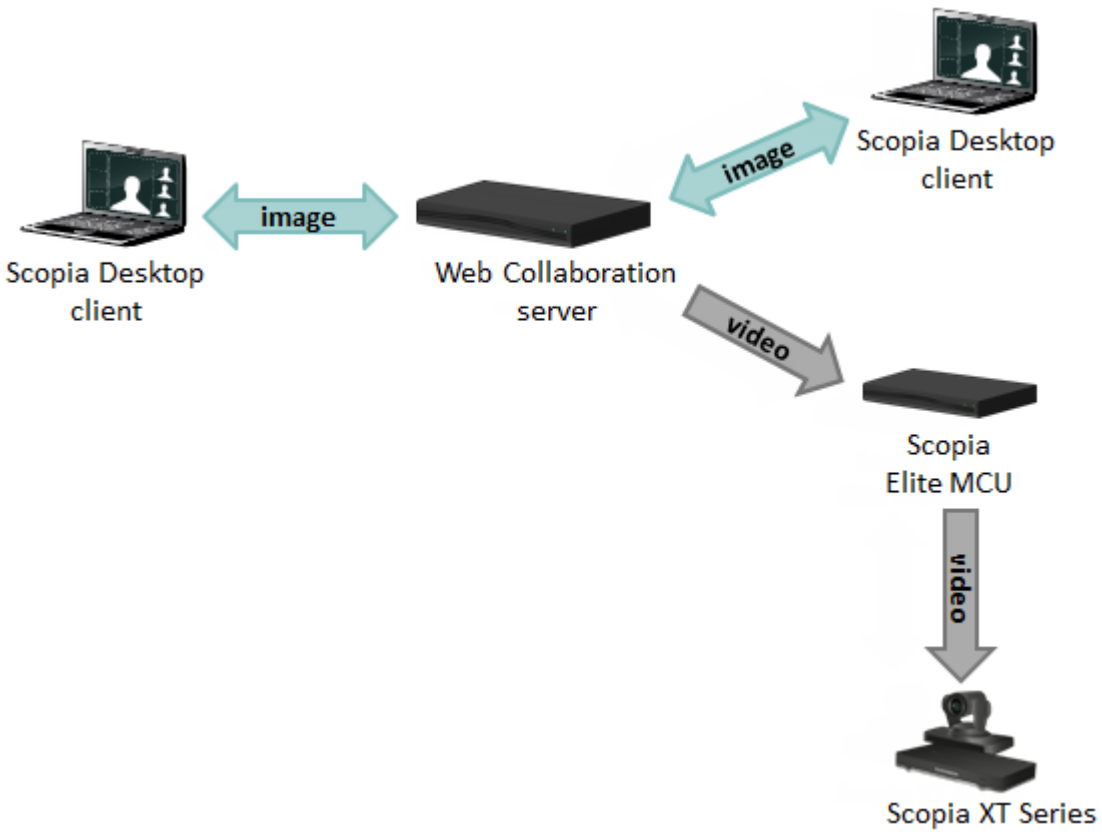


**Figure 1: Transferring a presentation as images or video**

Scopia® Web Collaboration server is normally located in the DMZ so that all users, both from inside and outside your network, can access it.

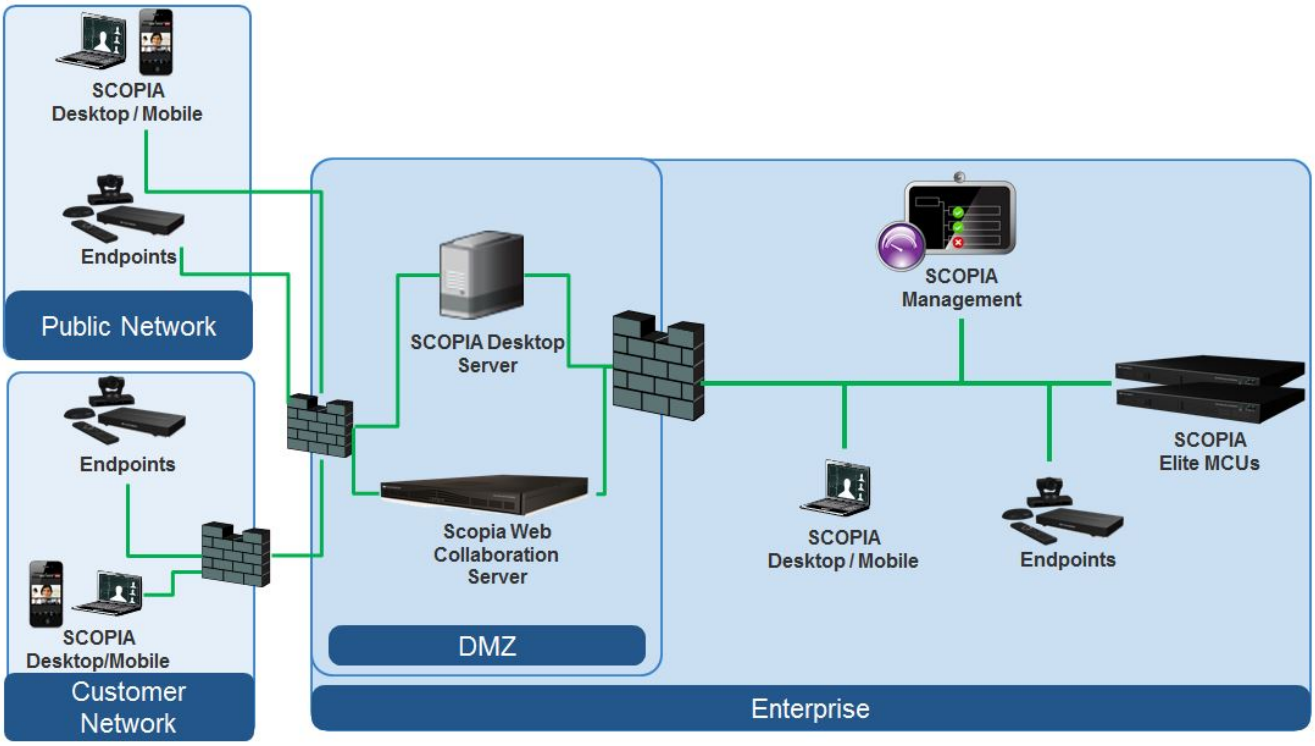


**Figure 2: Locating Scopia® Web Collaboration server in your deployment**

### Related Links

Technical Specifications on page 7

# Technical Specifications

This section lists important information about the Avaya Scopia® Web Collaboration server you purchased. Refer to this information when preparing system setup and afterwards to verify that the environment still complies with these requirements.

- System power requirements:
  - 100-240VAC input, 50/60Hz auto-switched
- Power consumption:
  - 946W (230V/4.3A or 115V/8.6A)
- Environmental requirements:
  - Operating temperature: 10°C to 35°C (50°F to 95°F)
  - Humidity: 90% non-condensing at 35°
  - Storage and transit temperature: -40°C to 70°C (-40°F to 158°F), ambient

- Physical dimensions:
  - Size: 430mm (16.9”) width x 43mm (1.7”) height x 690mm (27.2”) depth
  - 19-inch rack-mountable with flanges
- Ethernet connection requirement:
  - 1Gbps
- Communications:
  - Web Socket
  - IPv4
  - HTTP/HTTPS
  - Bit rate: up to 0.5Mbps per call
  - SIP — for connecting to other Avaya Scopia® Solution components
- Content sharing
  - JPEG/PNG at up to 720p5/1080p5
- Call capacity

  Up to 50 conferences

  Up to 160 participants in all conferences
- Scalability

  Multiple scalability with Scopia® Web Collaboration server together with associated MCU

  **Note:**

  A single Scopia® Web Collaboration server hosts a videoconference, all its participants connect to the same unit for collaboration features, cascading not supported.
- Security
  - Secure Real-time Transport Protocol (SRTP)
  - Transport Layer Security (TLS)
  - HTTPS for secure management
- Interfaces
  - RJ-45, dual gigabit Ethernet
  - RJ-45 serial port connector

**Related Links**

About Scopia® Web Collaboration server on page 5

# Chapter 2: Preparing the Scopia® Web Collaboration server Setup

Perform procedures in this section to prepare the site and device for installation.

**Related Links**

Checking Site Suitability on page 9
Unpacking the Device on page 9
Inspecting for Damage on page 10

## Checking Site Suitability

Prior to setting up your device, you need to verify your site suitability for:

- System power requirements
- System environmental requirements
- The device physical dimensions.

For more information, see Technical Specifications on page 7 to learn about these requirements. Ensure the site conforms to the listed requirements.

**Related Links**

Preparing the Scopia® Web Collaboration server Setup on page 9

## Unpacking the Device

### About this task

We strongly recommend that you follow safety guidelines described in this section during unpacking.

### Procedure

1. Inspect the shipping box to verify that it is not seriously damaged during shipping.
2. Place the shipping box on a horizontal surface paying attention to the This Side Up symbol on the shipping box (Figure 3: This Side Up symbol on page 10).

**Figure 3: This Side Up symbol**

**Caution:**

The accessories kit is situated on top of the device inside the shipping box and can be damaged if the box is placed upside down. Pay attention to the This Side Up symbol on the shipping box to handle the box correctly at all times.

**Caution:**

To prevent injury and equipment damage, follow the lifting guidelines described in the Safety Guide when lifting or moving the shipping box.

3. Cut the plastic straps.

   **Caution:**

   The plastic straps are tightly stretched and can hit you when you cut them. To avoid this, make sure you do not face the side of the box secured by the straps before you cut the straps.

4. Cut the strapping tape.
5. Open the shipping box.
6. Take the accessories kit out of the shipping box.
7. Take the device out of the shipping box.
8. Carefully open the additional boxes, remove the packing material, and remove the drives and other contents.

   **Important:**

   We recommend keeping the packaging materials in case you need to repack the device.

9. Remove the cellophane wrapping from the server case.
10. After opening the shipping box, check the shipment is complete. Compare the contents of the shipment with the packing list included in the box.

**Related Links**

Preparing the Scopia® Web Collaboration server Setup on page 9

# Inspecting for Damage

After you verify that all of the equipment is included, carefully examine the , power supplies and cables for any damage resulting from shipping. If you suspect any damage from shipping, contact

your local freight carrier for procedures on damage claims. If you observe any physical defects in the items you ordered, contact Technical Support for Return Material Authorization (RMA) form.

**Important:**

Before proceeding with the installation, verify that all of the ordered parts are present and in good condition. Keep a record of the parts and serial numbers. If any parts are missing or damaged, contact your sales representative.

**Related Links**

Preparing the Scopia® Web Collaboration server Setup on page 9

# Chapter 3: Setting up the Device

These sections describe how to set up the device:

**Related Links**

Verifying Rack Suitability on page 12
Mounting the Device onto the Rack Using a Shelf on page 15
Connecting Cables to the Device on page 22
Configuring the Device IP Addresses on page 23
Verifying the Device Installation on page 25

## Verifying Rack Suitability

There are some critical requirements that you must meet when choosing a rack and before mounting the device into it.

**Related Links**

Setting up the Device on page 12
Choosing the Type of Rack on page 12
Making space for the Device on page 13

### Choosing the Type of Rack

There are many types of racks on the market. The installation instructions in this guide are intended for a 19” rack.

- Verify that the 19” rack meets the EIA-310 standards. This standard includes precise definitions of the shape of the holes, their size, the depth of the rack and other features. For more information on the EIA-310 standard, see http://electronics.ihs.com/collections/eia/index.htm.
- Notice that the vertical square holes on the rack posts are not spaced equally. They form a repeating pattern of two holes close together, then one hole separate, then two holes close together and so on. See Figure 4: Hole distribution on 19” rack on page 13.

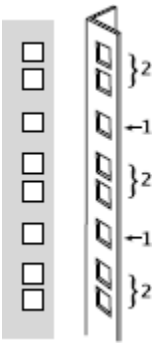


**Figure 4: Hole distribution on 19” rack**

**Related Links**

Verifying Rack Suitability on page 12

## Making space for the Device

When checking for an empty space to setup the device, be aware of its physical dimensions.

- Install the device in an open rack whenever possible. If installation in an enclosed rack is unavoidable, ensure that the rack has adequate ventilation.
- Avoid placing the device in an overly congested rack or directly next to another equipment rack. Otherwise, the heated exhaust air from other equipment can enter the inlet air vents and cause the device to overheat.
- Maintain a minimum clearance of 3 inches (7.62 cm) on the left and right of the device for the cooling air inlet and exhaust vents.
- Find a space on the rack which is at least 7 empty square holes in height on the rack posts.

  The Scopia® Web Collaboration server takes up 3 holes (1U) on the posts. You need at least 2 additional holes to slide the device into the rack.

  See Figure 5: Height of the device in the rack on page 14.

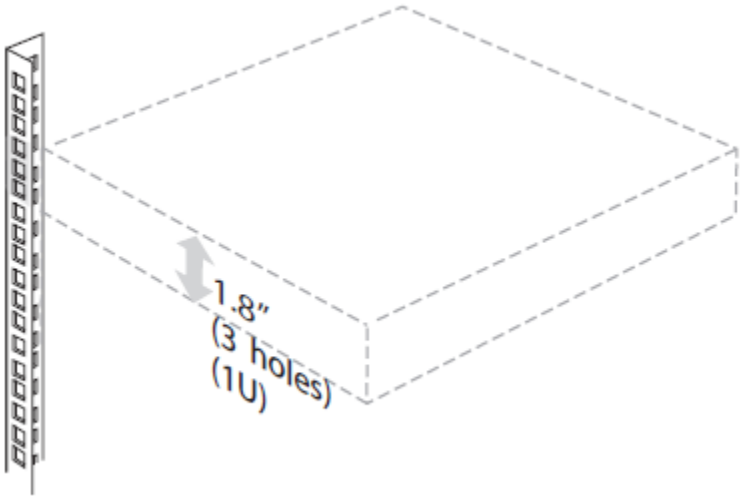


**Figure 5: Height of the device in the rack**

- To mount the device between two posts, the width between the inner sides of the two posts must be at least 17.7 inches (45 cm). See Figure 6: Width between inner sides of posts on page 14.

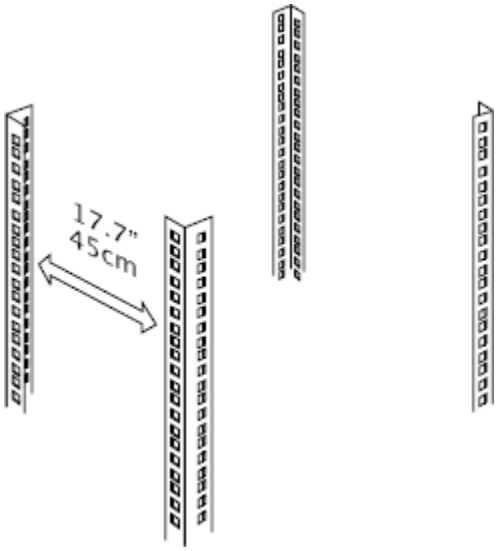


**Figure 6: Width between inner sides of posts**

## Related Links

Verifying Rack Suitability on page 12

# Mounting the Device onto the Rack Using a Shelf

This section describes how to mount the unit on to your rack:

**Related Links**

Setting up the Device on page 12
Locating a Shelf in the Rack on page 15
Checking the Accessories Required for Mounting on page 16
Attaching Brackets to the Device on page 17
Marking the Location of the Device-fixing Cage Nuts on page 19
Removing the Cage Nut Screws on page 19
Mounting the Device-fixing Cage Nuts on page 20
Mounting the Device onto the Rack Using a Shelf on page 20

## Locating a Shelf in the Rack

### About this task

Before choosing a shelf that will support the device, follow this procedure.

### Procedure

1. Read Verifying Rack Suitability on page 12, which contains important positioning and spacing information.
2. Prepare masking tape or a felt-tip pen to mark the location of the device-fixing cage nuts. If the holes on the rack are marked with numbers, write down the numbers on a piece of paper.
3. If you choose to mount the shelf, see the manufacturer's guidelines for mounting a shelf.

   When looking for a location on the rack (see Locating a shelf in the rack on page 16):

   - Choose a shelf on a rack with at least 1.73 inches (4.4 cm) of empty space above.
   - Verify that the shelf you want to use is properly mounted and secured.
   - Verify that the shelf can support the device weight. See Technical Specifications on page 7.
   - Verify a hole is present 0.75 inches (2 cm) above the shelf (measured from the center of the hole).

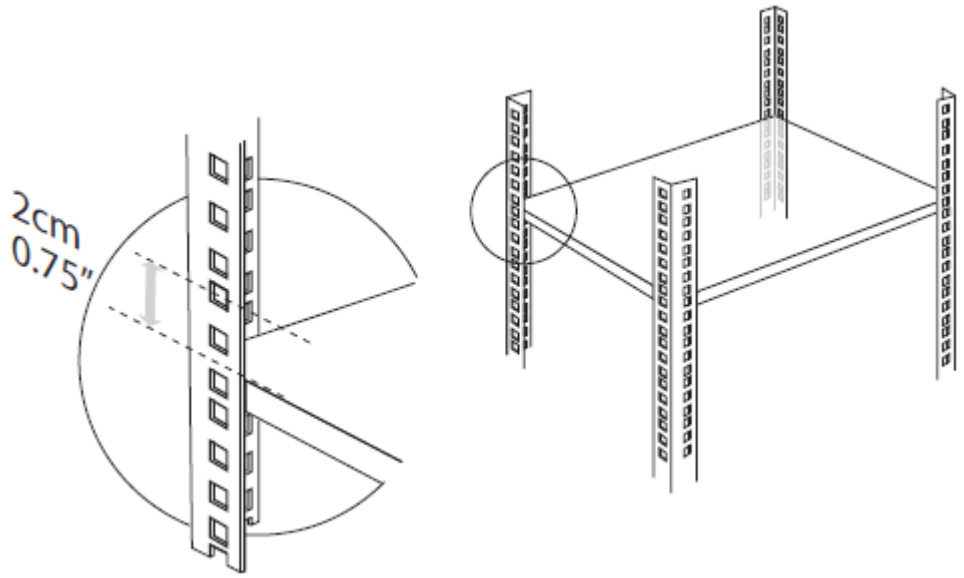


**Figure 7: Checking the location of the shelf in the rack**

4. Ensure the shelf is positioned horizontally in the rack.
5. Ensure the rack breaks are locked or the rack is stabilized.

**Related Links**

Mounting the Device onto the Rack Using a Shelf on page 15

## Checking the Accessories Required for Mounting

Check you have the accessories necessary for mounting the device (see Figure 8: Accessories required for mounting on page 17):

- 2 mounting brackets (left and right)
- 2 cage nuts (M6) each with its hexagon socket cap screw (M6x10, DIN 7984)
- 4 Phillips screws already mounted on the device.

**Important:**

Make sure you have a ruler, an Allen wrench (4 mm diameter), and a screwdriver (Nr. 1 tip) ready to hand before you start the setup.

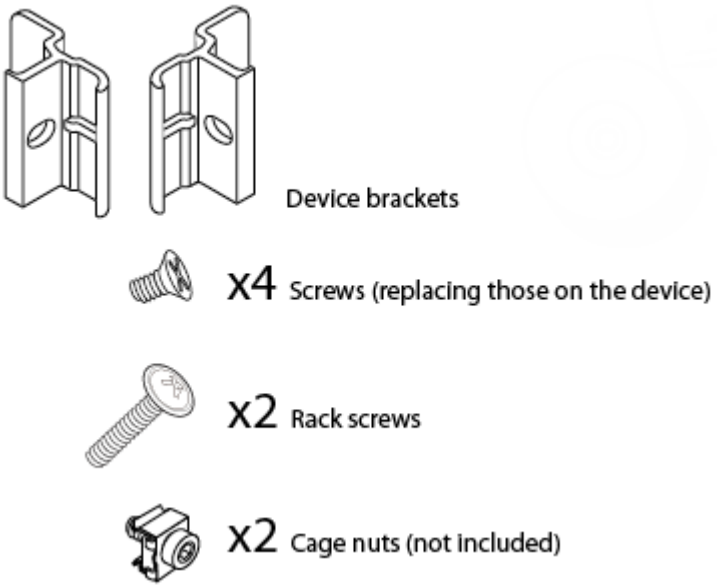


**Figure 8: Accessories required for mounting**

**Related Links**

Mounting the Device onto the Rack Using a Shelf on page 15

# Attaching Brackets to the Device

## About this task

The brackets serve to secure the device to the rack's front posts.

## Procedure

1. Position the device on a flat, horizontal surface. Make sure the device front panel faces toward you.
2. Unscrew the two Phillips screws on either side of the device. They hold the front panel in place. See Figure 9: Removing the Phillips screws on the side panel on page 18.

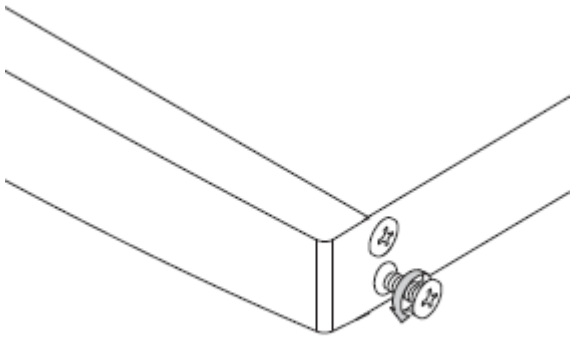

**Figure 9: Removing the Phillips screws on the side panel**

3. Attach the brackets on each side of the device side panel with the Phillips screws. See Figure 10: Aligning the bracket with the device front panel on page 18.

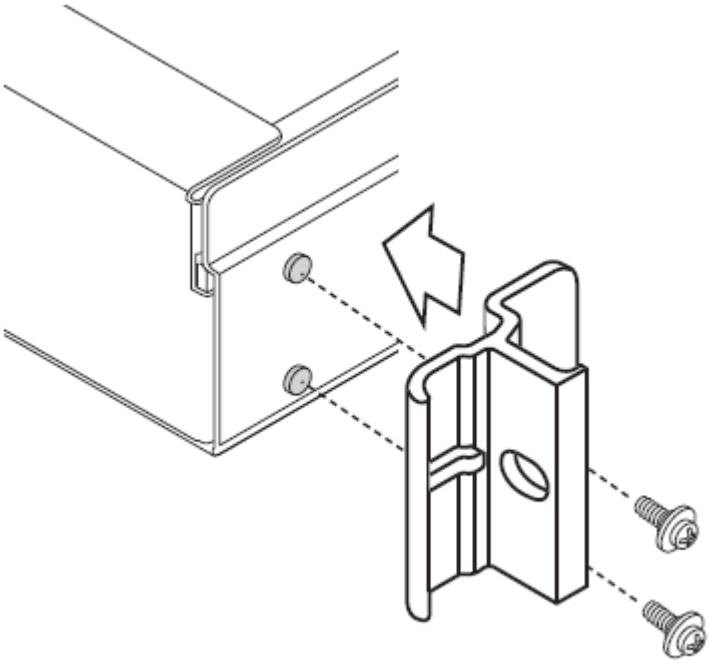

**Figure 10: Aligning the bracket with the device front panel**

## Related Links

Mounting the Device onto the Rack Using a Shelf on page 15

## Marking the Location of the Device-fixing Cage Nuts

### About this task

There is a pair of cage nuts, one for each front-facing rack post. You need these cage nuts to fix the device brackets to the post.

### Procedure

1. From inside the front-facing rack post, mark the location of the device-fixing cage nut measured at 0.75 inches (2 cm) above the shelf. See Figure 11: Marking the location of the device-fixing cage nut on the rack on page 19.

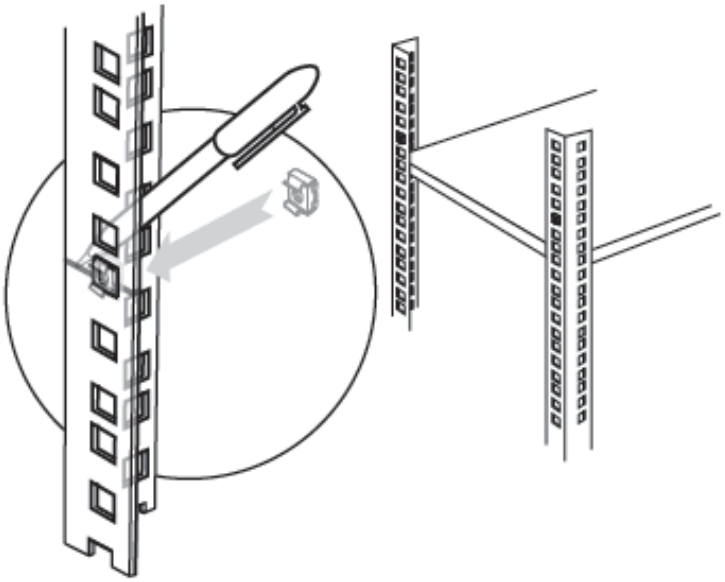

**Figure 11: Marking the location of the device-fixing cage nut on the rack**

2. Repeat this procedure for the other front-facing post.

### Related Links

Mounting the Device onto the Rack Using a Shelf on page 15

## Removing the Cage Nut Screws

### About this task

The cage nuts are supplied with pre-mounted screws. Remove the screws and put them aside for later. See Figure 12: Removing the cage nut screw on page 20.

**Figure 12: Removing the cage nut screw**

**Related Links**

Mounting the Device onto the Rack Using a Shelf on page 15

# Mounting the Device-fixing Cage Nuts

## About this task

After you have marked the location of these cage nuts on the front-facing posts, you can mount them into the rack. Insert each cage nut on each of the posts where you have placed marks on the rack.

## Procedure

1. Rotate the bottom cage nut so that its wings are on the top and bottom sides of the cage nut. See Figure 11: Marking the location of the device-fixing cage nut on the rack on page 19.
2. Compress the wings. From the back side of the post, insert first the wide wing, then the narrow wing into the marked square hole. Release the wings after the nut is in position.

**Related Links**

Mounting the Device onto the Rack Using a Shelf on page 15

# Mounting the Device onto the Rack Using a Shelf

## About this task

After you have inserted the cage nuts onto the posts, you can mount the device onto the rack. Before mounting the device, read the Safety Guidelines described in the Safety Guide. Secure the device on the rack's posts to prevent it from moving around or falling.

**Caution:**

The device is heavy and we recommend that you ask someone to help you lift it.

## Procedure

1. Lift the device.
2. Slide the device onto the shelf until the holes on the device's brackets align with the cage nuts you mounted previously. See Figure 13: Sliding the device onto the shelf on page 21.

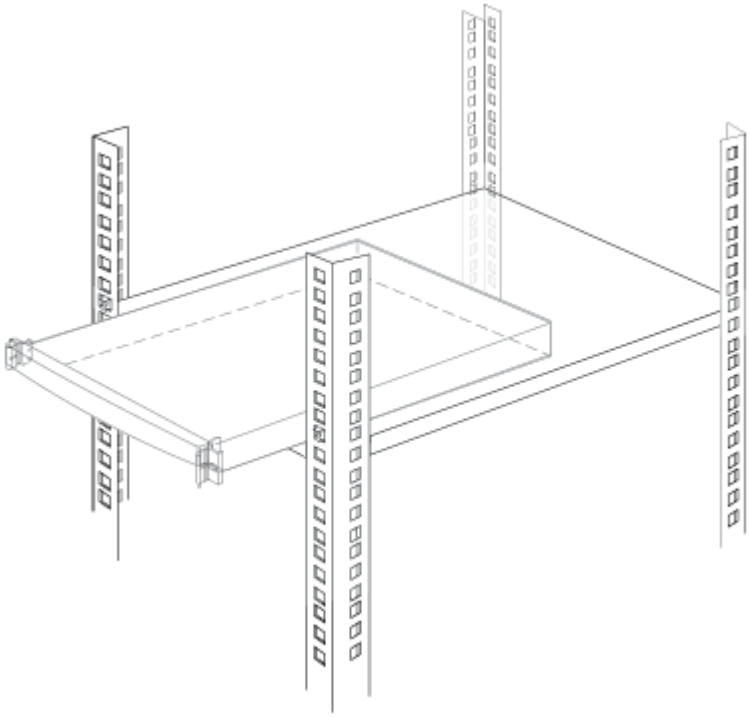

**Figure 13: Sliding the device onto the shelf**

3. Insert the two long rack screws provided with the product through the bracket holes into the cage nuts in the rack. Using the Allen wrench tighten the screws to secure the device to the front posts. See Figure 14: Securing the device to the rack on page 21.

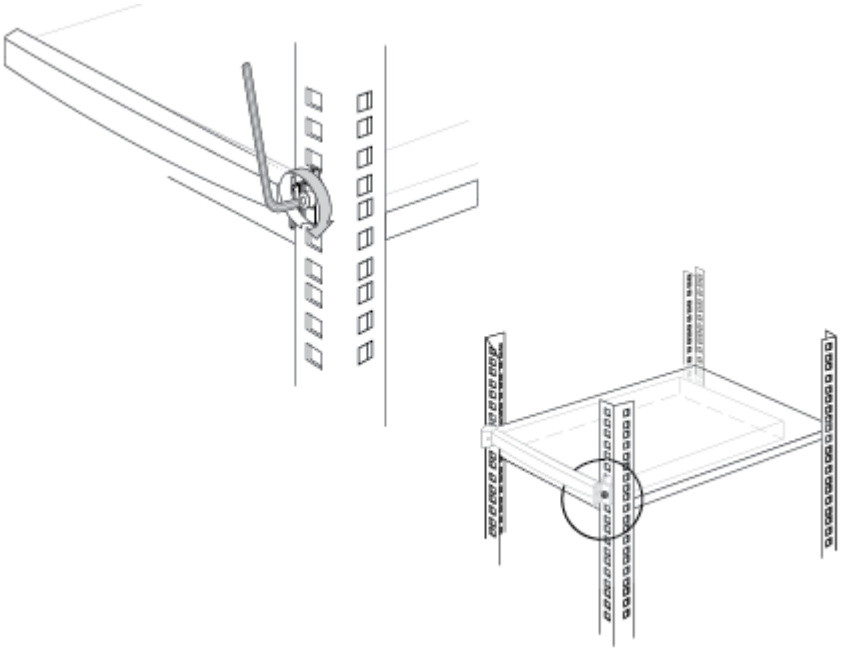

**Figure 14: Securing the device to the rack**

**Related Links**

Mounting the Device onto the Rack Using a Shelf on page 15

# Connecting Cables to the Device

## About this task

Follow this procedure to connect the power and serial cable supplied with the accessories kit.

**Important:**

The serial connection is used only for configuring the IP address of the device.

**Caution:**

During this procedure, follow the safety guidelines described in the Safety Guide.

## Procedure

1. On the rear panel, connect the power cable to the AC power connector (Figure 15: Rear panel of the device on page 22).


**Figure 15: Rear panel of the device**

2. Connect the other end of the power cable to the AC power.
3. Use a serial cable to connect a PC to the device's serial port. This connection is required for local configuration and maintenance.

   **Important:**

   Do not connect a screen or a keyboard to the device directly. Define the device's basic settings via the serial connection only.

**Related Links**

Setting up the Device on page 12

# Configuring the Device IP Addresses

## About this task

The device supports the IPv4 IP address format.

## Before you begin

Make sure you have these items:

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

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

## Procedure

1. Connect the power cable, but do not switch on the device.
2. Connect the device serial port to a PC with the terminal emulator software installed.
3. Start the terminal emulation application on the PC.
4. Set the communication settings in the terminal emulation application on the PC as follows (Table 1: Configuring the communication settings on page 23):

   **Table 1: Configuring the communication settings**

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

5. Power the device (see Figure 16: Device front panel on page 24).

   Verify the power LED is lit green (Figure 16: Device front panel on page 24).

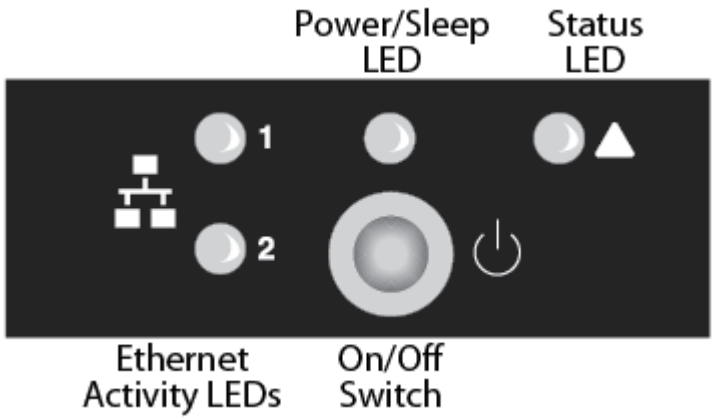


**Figure 16: Device front panel**

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

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

   `Main menu`

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

   Select:
   ```

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

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

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

   The terminal displays the following message:

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

   Select:
   ```

8. Enter **2** to change the network configuration.
9. Enter the new settings at each prompt (Table 2: Configuring network settings on page 25).

**Table 2: Configuring network settings**

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

**Important:**

The settings configure only the left NIC, because the right NIC is disabled.

10. Allow the device to complete the reboot process. A new emulator session begins.
11. Close the terminal emulator session.
12. Connect the network cable to the ethernet connector on the rear panel of the device (see Figure 15: Rear panel of the device on page 22).

**Related Links**

Setting up the Device on page 12

# Verifying the Device Installation

## About this task

After you installed Avaya Scopia® Web Collaboration server and performed its initial configuration, you need to verify that it is installed and configured correctly.

## Procedure

1. On the front panel, verify that the power LED is lit green.

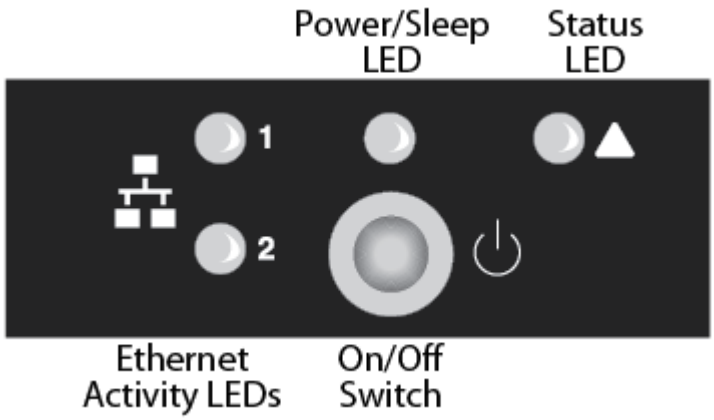


**Figure 17: Locating the front panel LEDs**

2. Verify that the status LED is lit green.
3. Check the network connection by verifying that the Ethernet activity LED is lit green.

**Related Links**

Setting up the Device on page 12

# Chapter 4: Planning and Configuring Scopia® Web Collaboration servers in Scopia® Management

This section describes how to configure and manage Avaya Scopia® Web Collaboration servers. Since Avaya Scopia® Web Collaboration servers do not have their own web interface, you configure them in Scopia® Management.

**Important:**

If you have not installed a Scopia® Web Collaboration server on your system, you should use the Avaya Scopia® Desktop server content sharing functionality. For further details, see Scopia® Desktop server documentation.

The Scopia® Web Collaboration server is a video network device that provides the advanced content sharing functionality for your Avaya Scopia® Solution.

You add Avaya Scopia® Web Collaboration servers to a specific organization or branch, according to pre-defined network topologies. For more information see the *Scopia® Solution Guide*.

**Related Links**

Adding Avaya Scopia® Web Collaboration server in Avaya Scopia® Management on page 27
Configuring the Scopia® Web Collaboration server in Scopia® Management on page 28
Changing an Avaya Scopia® Web Collaboration server's Location or Organization on page 30

## Adding Avaya Scopia® Web Collaboration server in Avaya Scopia® Management

Just like most other video network devices in your Avaya Scopia® Solution, you configure the Avaya Scopia® Web Collaboration server in Avaya Scopia® Management. You begin by adding the Avaya Scopia® Web Collaboration server in Avaya Scopia® Management, as described in *Adding Video Network Devices in Scopia® Management in Administrator Guide for Avaya Scopia® Management*

**Related Links**

Planning and Configuring Scopia® Web Collaboration servers in Scopia® Management on page 27

# Configuring the Scopia® Web Collaboration server in Scopia® Management

## About this task

This section explains how to configure the Avaya Scopia® Web Collaboration server settings in Scopia® Management. For example, you can configure whether the system uses HTTP or HTTPS to connect to the Scopia® Web Collaboration server.

**Important:**

If you have not installed a Scopia® Web Collaboration server on your system, you should use the Avaya Scopia® Desktop serversharing functionality . For further details, see Scopia® Desktop server documentation.

## Before you begin

Add the Scopia® Web Collaboration server to Scopia® Management by entering its basic settings, as described in *Administrator Guide for Avaya Scopia® Management*.

## Procedure

1. Access the Scopia® Management administrator portal.
2. Select **Devices** > **Devices by Type** > **Web Collaboration Servers**.
3. Select the Scopia® Web Collaboration server you are configuring.
4. Select the **Configuration** tab.

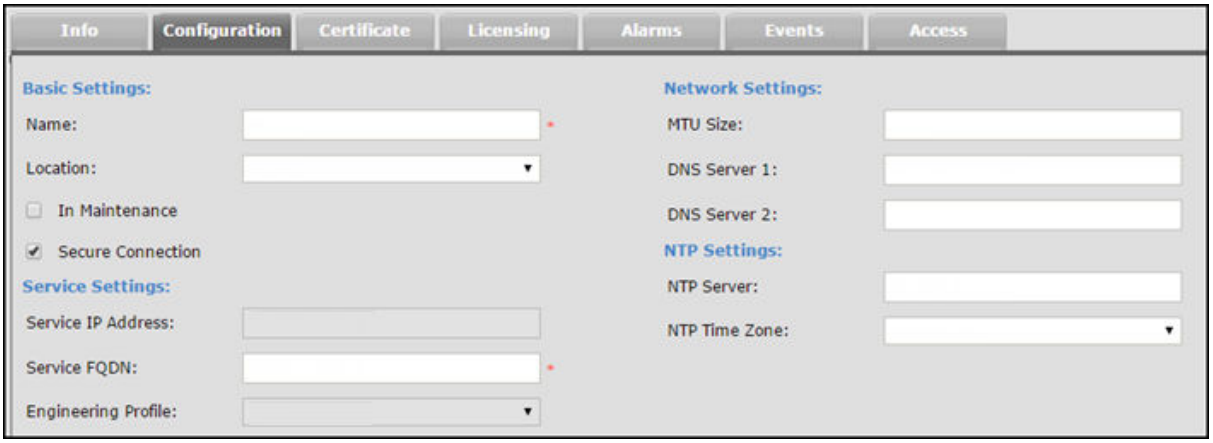


**Figure 18: Configuring the Scopia® Web Collaboration server**

5. Configure the Scopia® Web Collaboration server settings as described in Table 3: Configuring settings for the Avaya Scopia® Web Collaboration server on page 29.

**Table 3: Configuring settings for the Avaya Scopia® Web Collaboration server**

| Field Names | Description |
|---|---|
| **Name** | The name that identifies the Scopia® Web Collaboration server in Scopia® Management. |
| **Location** | If there is more than one location in your deployment, assign your Scopia® Web Collaboration server to a location by selecting an option from the list. |
| **In Maintenance** | Select if you are currently upgrading the Scopia® Web Collaboration server or if you are repairing it.<br><br>If you select this option, you can still configure settings and perform upgrades, but you cannot actively use this Scopia® Web Collaboration server. |
| **Secure Connection** | Select to securely access the Scopia® Web Collaboration server web interface using HTTPS, and to securely communicate between Scopia® Management and the Scopia® Web Collaboration server using TLS.<br><br>Before selecting HTTPS, you must generate the Scopia® Web Collaboration server certificates. To enable HTTP deselect the checkbox.<br><br>By default, Scopia® Management communicates with the Scopia® Web Collaboration server using TCP. For enhanced security, you can secure XML communication using TLS. You can only do this if you installed certificates for the Scopia® Web Collaboration server, either from Scopia® Management or from the Scopia® Web Collaboration server interface (see Scopia® Web Collaboration server documentation.) |
| **Service IP Address** | This (read-only) field displays the management IP address of the Scopia® Web Collaboration server. This is configured directly on the Scopia® Web Collaboration server. Verify that the IP address is correctly registered in the DNS server, and that the DNS is set in the Scopia® Web Collaboration server. For more information see the *Installation Guide for Avaya Scopia® Web Collaboration server*. |
| **Service FQDN** | The fully qualified domain name of the Scopia® Web Collaboration server. Verify that the FQDN address is correctly registered in the DNS server, and that the DNS is set in the Scopia® Web Collaboration server. |
| **MTU Size** | The size of the packets the Scopia® Web Collaboration server sends.<br><br>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 |

*Table continues…*

| Field Names | Description |
|---|---|
| | server, endpoints like XT Series and other network devices like LDAP servers and network routers.<br>Only change this setting for a router that uses a non-standard MTU size. |
| **DNS Server 1, 2** | The IP address(es) of the organization's DNS server(s). |
| **NTP Server** | The IP address of a Network Time Protocol server that sets the time for the Scopia® Web Collaboration server clock.<br>External NTP servers ensure the same clock throughout all devices on the network.<br>If you have no NTP server, enter **0.0.0.0**. |
| **NTP Time Zone** | The time zone of the NTP server. |

6. Select **Apply**.
7. Allow Scopia® Management to access the Scopia® Web Collaboration server:
   a. Select the **Access** tab.
   b. Enter the login name and password of the Scopia® Web Collaboration server. The default username is *admin* and the default password is *password*.
   c. Select **Apply**.

**Related Links**

Planning and Configuring Scopia® Web Collaboration servers in Scopia® Management on page 27

# Changing an Avaya Scopia® Web Collaboration server's Location or Organization

## About this task

This procedure is relevant for administrators of a distributed deployment.

Once you add the Scopia® Web Collaboration server to Scopia® Management, you can modify its location , according to your network requirements and topology.

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

## Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Devices** tab.
3. Select **Web Collaboration Servers**, located under **Devices by Type**.
4. Select the Scopia® Web Collaboration server you want to configure in the **Name** column.

5. Select the **Configure** tab.
6. Select the Scopia® Web Collaboration server's location from the **Location** list.
7. Select **OK** to save your changes.

**Related Links**

Planning and Configuring Scopia® Web Collaboration servers in Scopia® Management on page 27

# Chapter 5: Implementing Port Security for the Avaya Scopia® Web Collaboration server

The Avaya Scopia® Web Collaboration server is the component which hosts the web collaboration aspect of videoconferences.

This section details the ports used for the Avaya Scopia® Web Collaboration server.

**Related Links**

Ports to open for the Avaya Scopia® Web Collaboration server on page 32

## Ports to open for the Avaya Scopia® Web Collaboration server

The Avaya Scopia® Web Collaboration server (WCS) is typically located in the enterprise network and is connected to the DMZ.

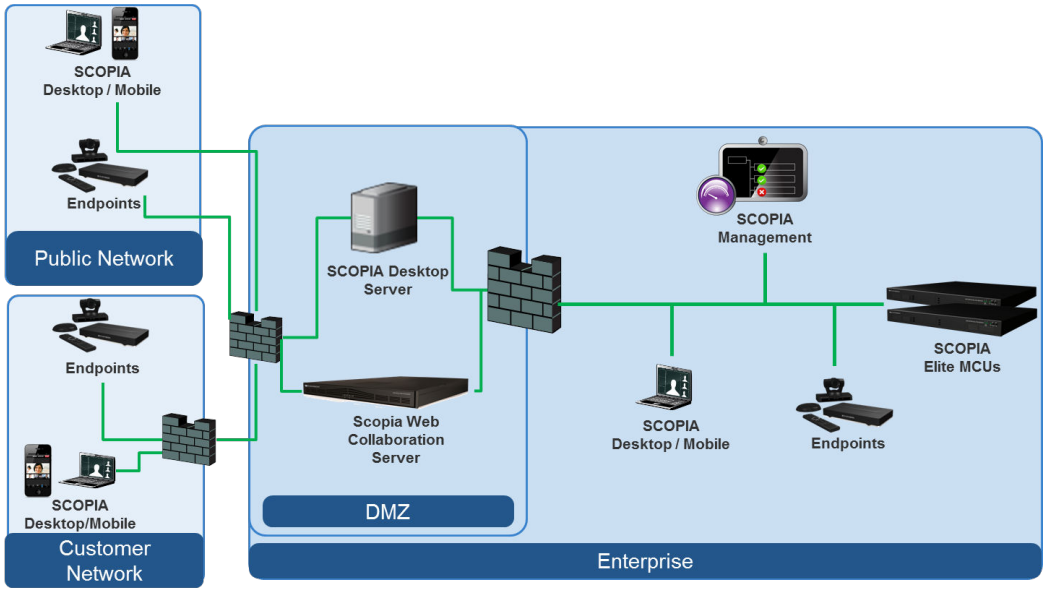


**Figure 19: Locating the Avaya Scopia® Web Collaboration server in the DMZ**

When opening ports on the Avaya Scopia® Web Collaboration server, use the following tables as a reference.

**Important:**

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

**Table 4: Bidirectional Ports to Open Between the Avaya Scopia® Web Collaboration server (WCS) and the Enterprise**

| Port Range | Protocol | Destination | Functionality | Result of Blocking Port | Required |
|---|---|---|---|---|---|
| 3336 | TCP-TLS | Scopia® Management server | Facilitates WCS administration by Scopia® Management. | WCS connectivity issues | Mandatory |
| 3338 | TCP-TLS | Scopia® Management server | Facilitates WCS administration by Scopia® Management | WCS connectivity issues | Mandatory |
| 3346 | TCP-TLS | Scopia® Management server | Facilitates WCS administration by Scopia® Management | WCS connectivity issues | Mandatory |
| 3348 | TCP-TLS | Scopia® Management server | Facilitates WCS administration by Scopia® Management | WCS connectivity issues | Mandatory |
| 5060 | TCP/UDP | Scopia® Elite MCU and Scopia® Management server | SIP Protocol | WCS connectivity issues | Mandatory |
| 5061 | TCP-TLS | Scopia® Elite MCU and Scopia® Management server | SIP TLS Protocol | WCS connectivity issues | Mandatory |
| 12000–12800 | UDP | Scopia® Elite MCU | RTP presentation traffic | WCS connectivity issues | Mandatory |
| 3400–3580 | TCP/UDP | Scopia® Elite MCU | BFCP presentation traffic | WCS connectivity issues | Mandatory |

**Table 5: Inbound Ports to Open from the Enterprise to the Avaya Scopia® Web Collaboration server (WCS)**

| Port Range | Protocol | Destination | Functionality | Result of Blocking Port | Required |
|---|---|---|---|---|---|
| 22 | TCP | Avaya Scopia® Web Collaboration server | SSH | No debugging | Optional |
| 80 | TCP | From Avaya Scopia® Web Collaboration client to server | Controls web collaboration traffic | Issues relating to web collaboration functionality | Mandatory |
| 443 | TCP | From Avaya Scopia® Web Collaboration client to server | Controls web collaboration traffic | Issues relating to web collaboration functionality | Mandatory |
| 843 | TCP | From Avaya Scopia® Web Collaboration client to server | Controls the client's Flash policy server | Issues relating to web collaboration functionality | Mandatory |
| 5556 | TCP-TLS | From Scopia® Management to Avaya Scopia® Web Collaboration server | Facilitates WCS administration by Scopia® Management | WCS connectivity issues | Mandatory |
| 8095 | TCP-HTTP | From Scopia® Management to Avaya Scopia® Web Collaboration server | File transfer channel | WCS connectivity issues | Mandatory |
| 8445 | TCP-HTTPS | From Scopia® Management to Avaya Scopia® Web Collaboration server | File transfer channel | WCS connectivity issues | Mandatory |

**Table 6: Outbound Ports to Open from the Avaya Scopia® Web Collaboration server (WCS) to the Enterprise**

| Port Range | Protocol | Destination | Functionality | Result of Blocking Port | Required |
|---|---|---|---|---|---|
| 53 | UDP | DNS server | DNS | No FQDN resolution | Mandatory |
| 8080 | HTTP | Scopia® Management server | Controls web collaboration traffic | Issues relating to web collaboration functionality | Mandatory |
| 9443 | HTTPS | Scopia® Management server | Controls web collaboration traffic | Issues relating to web collaboration functionality | Mandatory |

**Table 7: Inbound Ports to Open from the Public to the Avaya Scopia® Web Collaboration server (WCS)**

| Port Range | Protocol | Destination | Functionality | Result of Blocking Port | Required |
|---|---|---|---|---|---|
| 80 | TCP | From Avaya Scopia® Web Collaboration client to server | Controls web collaboration traffic | Issues relating to web collaboration functionality | Mandatory |
| 443 | TCP | From Avaya Scopia® Web Collaboration client to server | Controls web collaboration traffic | Issues relating to web collaboration functionality | Mandatory |
| 843 | TCP | From Avaya Scopia® Web Collaboration client to server | Controls the client's Flash policy server | Issues relating to web collaboration functionality | Mandatory |

## Related Links

Implementing Port Security for the Avaya Scopia® Web Collaboration server on page 32

# Glossary

| | |
|---|---|
| **1080p** | See Full HD on page 40. |
| **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 41. |
| **AAC** | AAC is an audio codec which compresses sound but with better results than MP3. |
| **AGC (Automatic Gain Control)** | Automatic Gain Control (AGC) smooths audio signals through normalization, by lowering sounds which are too strong and strengthening sounds which are too weak. This is relevant with microphones situated at some distance from the speaker, like room systems. The result is a more consistent audio signal within the required range of volume. |
| **Alias** | An alias in H.323 represents the unique name of an endpoint. Instead of dialing an IP address to reach an endpoint, you can dial an alias, and the gatekeeper resolves it to an IP address. |
| **Auto-Attendant** | Auto-Attendant, also known as video IVR, offers quick access to meetings hosted on MCUs, via a set of visual menus. Participants can select menu options using standard DTMF tones (numeric keypad). Auto-Attendant works with both H.323 and SIP endpoints. |
| **Avaya Scopia® Streaming and Recording Manager** | The Avaya Scopia® Streaming and Recording Manager provides a web-based interface to configure and manage Scopia® Streaming and Recording server software, devices, services, and users. The Scopia® Streaming and Recording server Manager application resides on a single |

hardware platform and provides access to all content in the Scopia® Streaming and Recording server environment.

**Avaya Scopia® Streaming and Recording Manager Portals**

The Scopia® Streaming and Recording server Manager provides a portal for administering content. When you log in to the web interface, you can access the Administrator portal.

The Manager also provides the Viewer portal. This portal is embedded within the Avaya Scopia® Desktop User portal. Use the User portal to schedule Scopia® Streaming and Recording server broadcasts.

**Balanced Microphone**

A balanced microphone uses a cable that is built to reduce noise and interference even when the cable is long. This reduces audio disruptions resulting from surrounding electromagnetic interference.

**BFCP (Binary Floor Control Protocol)**

BFCP is a protocol which coordinates shared videoconference features in SIP calls, often used by one participant at a time. For example, when sharing content to others in the meeting, one participant is designated as the presenter, and is granted the floor for presenting. All endpoints must be aware that the floor was granted to that participant and react appropriately.

**Bitrate**

Bitrate is the speed of data flow. Higher video resolutions require higher bitrates to ensure the video is constantly updated, thereby maintaining smooth motion. If you lower the bitrate, you lower the quality of the video. In some cases, you can select a lower bitrate without noticing a significant drop in video quality; for example during a presentation or when a lecturer is speaking and there is very little motion. Bitrate is often measured in kilobits per second (kbps).

**Call Control**

See Signaling on page 47.

**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).

**Conference Point**

The Avaya Scopia® Streaming and Recording Conference Point is a video conferencing gateway appliance that captures standard or high definition video conferences. It transcodes, creates, and records the video conferences in a streaming media format. You can use it to capture H.323 video for instant video webcasting or on-demand publishing.

**Content Slider**

The Scopia® Content Slider stores the data already presented in the videoconference and makes it available for participants to view during the meeting.

**Continuous Presence**

Continuous presence enables viewing multiple participants of a videoconference at the same time, including the active speaker. This graphics-intensive work requires scaling and mixing the images together into one of the predefined video layouts. The range of video layouts depends on the type of media processing supported, typically located in the MCU.

**Control**

Control, or media control, sets up and manages the media of a call (its audio, video and data). Control messages include checking compatibility between endpoints, negotiating video and audio codecs, and other parameters like resolution, bitrate and frame rate. Control is communicated via H.245 in H.323 endpoints, or by SDP in SIP endpoints. Control occurs within the framework of an established call, after signaling.

**CP**

See Continuous Presence on page 38.

**Dedicated Endpoint**

A dedicated endpoint is a hardware endpoint for videoconferencing assigned to a single user. It is often referred to as a personal or executive endpoint, and serves as the main means of video communications for this user. For example, Scopia® XT Executive. It is listed in the organization's LDAP directory as associated exclusively with this user.

**Delivery Node**

The Avaya Scopia® Streaming and Recording Delivery Node provides on-demand and broadcast video delivery. You can use it alone or in a hierarchy of devices. It supports thousands of concurrent streams. The Delivery Node uses intelligent routing, content caching, and inherent redundancy to ensure transparent delivery of high-quality video.

**Dial Plan**

A dial plan defines a way to route a call and to determine its characteristics. In traditional telephone networks, prefixes often denote geographic locations. In videoconferencing deployments, prefixes are also used to define the type and quality of a call. For example, dial 8 before a number for a lower bandwidth call, or 6 for an audio-only call, or 5 to route the call to a different branch.

**Dial Prefix**

A dial prefix is a number added at the beginning of a dial string to route it to the correct destination, or to determine the type of call. Dial prefixes are defined in the organization's dial plan. For example, dial 9 for an outside line, or dial 6 for an audio only call.

**Distributed Deployment**

A distributed deployment describes a deployment where the solution components are geographically distributed in more than one network location.

**DNS Server** A DNS server is responsible for resolving domain names in your network by translating them into IP addresses.

**DTMF** DTMF, or touch-tone, is the method of dialing on touch-tone phones, where each number is translated and transmitted as an audio tone.

**Dual Video** Dual video is the transmitting of two video streams during a videoconference, one with the live video while the other is a shared data stream, like a presentation.

**Dynamic Video Layout** The dynamic video layout is a meeting layout that switches dynamically to include the maximum number of participants it can display on the screen (up to 9 on the XT Series, or up to 28 on Scopia® Elite MCU). The largest image always shows the active speaker.

**E.164** E.164 is an address format for dialing an endpoint with a standard telephone numeric keypad, which only has numbers 0 - 9 and the symbols: * and #.

**Endpoint** An endpoint is a tool through which people can participate in a videoconference. Its display enables you to see and hear others in the meeting, while its microphone and camera enable you to be seen and heard by others. Endpoints include dedicated endpoints, like Scopia® XT Executive, software endpoints like Scopia® Desktop Client, mobile device endpoints like Scopia® Mobile, room systems like XT Series, and telepresence systems like Scopia® XT Telepresence.

**Endpoint Alias** See Alias on page 36.

**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 39.

**FPS** See Frames Per Second on page 39.

**Frame Rate** See Frames Per Second on page 39.

**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. |
| **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 41.

**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 36.

**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 41.

**High Profile** See H.264 High Profile on page 41.

**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 46.

**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 43.

**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 38.

**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 38.

**PTZ Camera**

A PTZ camera can pan to swivel horizontally, tilt to move vertically, and optically zoom to devote all the camera's pixels to one area of the image. For example, the XT Standard Camera is a PTZ camera with its own power supply and remote control, and uses powerful lenses to achieve superb visual quality. In contrast, fixed cameras like webcams only offer digital PTZ, where the zoom crops the camera image, displaying only a portion of the original, resulting in fewer pixels of the zoomed image, which effectively lowers the resolution. Fixed cameras also offer digital pan and tilt only after zooming, where you can pan up to the width or length of the original camera image.

**Q.931**

Q.931 is a telephony protocol used to start and end the connection in H.323 calls.

**QCIF**

QCIF, or Quarter CIF, defines a video resolution of 176 × 144 pixels (PAL) or 176 x 120 (NTSC). It is often used in older mobile handsets (3G-324M) limited by screen resolution and processing power.

**Quality of Service (QoS)**

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

**Recordings**

A recording of a videoconference can be played back at any time. Recordings include audio, video and shared data (if presented). Users can access recordings from the Scopia® Desktop web portal or using a web link to the recording on the portal.

**Redundancy**

Redundancy is a way to deploy a network component, in which you deploy extra units as 'spares', to be used as backups in case one of the components fails.

**Registrar**

A SIP Registrar manages the SIP domain by requiring that all SIP devices register their IP addresses with it. For example, once a SIP endpoint

registers its IP address with the Registrar, it can place or receive calls with other registered endpoints.

**Resolution** Resolution, or image/video resolution, is the number of pixels which make up an image frame in the video, measured as the number of horizontal pixels x the number of vertical pixels. Increasing resolution improves video quality but typically requires higher bandwidth and more computing power. Techniques like SVC, H.264 High Profile and FEC reduce bandwidth usage by compressing the data to a smaller footprint and compensating for packet loss.

**Restricted Mode** Restricted mode is used for ISDN endpoints only, when the PBX and line uses a restricted form of communication, reserving the top 8k of each packet for control data only. If enabled, the bandwidth values on these lines are in multiples of 56kbps, instead of multiples of 64kbps.

**Room System** A room system is a hardware videoconferencing endpoint installed in a physical conference room. Essential features include its camera's ability to PTZ (pan, tilt, zoom) to allow maximum flexibility of camera angles enabling participants to see all those in the meeting room or just one part of the room.

**RTCP** Real-time Control Transport Protocol, used alongside RTP for sending statistical information about the media sent over RTP.

**RTP** RTP or Real-time Transport Protocol is a network protocol which supports video and voice transmission over IP. It underpins most videoconferencing protocols today, including H.323, SIP and the streaming control protocol known as RTSP. The secured version of RTP is SRTP.

**RTSP** RTSP or Real-Time Streaming Protocol controls the delivery of streamed live or playback video over IP, with functions like pause, fast forward and reverse. While the media itself is sent via RTP, these control functions are managed by RTSP

**Sampling Rate** The sampling rate is a measure of the accuracy of the audio when it is digitized. To convert analog audio to digital, it must collect or sample the audio at specific intervals. As the rate of sampling increases, it raises audio quality.

**SBC** A Session Border Controller (SBC) is a relay device between two different networks. It can be used in firewall/NAT traversal, protocol translations and load balancing.

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

| | |
|---|---|
| **Scopia® Content Slider** | See Content Slider on page 38. |
| **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 43. |
| **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 45. |
| **SIP Server** | A SIP server is a network device communicating via the SIP protocol. |
| **SIP URI** | See URI on page 49. |
| **Slider** | See Content Slider on page 38. |
| **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 47.

**Standard Definition**

See SD on page 47.

**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 49.

**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 50.

**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 46.

**Video Switching** See Switched video on page 48.

**Videoconference** A videoconference is a meeting of more than two participants with audio and video using endpoints. Professional videoconferencing systems can handle many participants in single meetings, and multiple simultaneous meetings, with a wide interoperability score to enable a wide variety of endpoints to join the same videoconference. Typically you can also share PC content, like presentations, to other participants.

**Viewer Portal** The Avaya Scopia® Streaming and Recording Viewer Portal is embedded in the Avaya Scopia® Desktopuser portal. To access the Viewer Portal, you can select **Recordings and Events** on the main Scopia® Desktop page. From the Viewer Portal, you can watch recordings and navigate through the categories.

**Virtual Delivery Node** The Avaya Scopia® Streaming and Recording Virtual Delivery Node (VDN) is a device to push content to an external Content Delivery Network (CDN). The method for publishing content to a CDN is tightly coupled to the Avaya Scopia® Streaming and Recording platform which allows a company's video assets to be managed from a central location.

If you want to use a VDN and a CDN, you must buy cloud storage and services from Highwinds™, with the appropriate bandwidth and capacity for your needs. You apply the credentials you receive from Highwinds in the Avaya Scopia® Streaming and Recording Manager to securely access the CDN.

**Virtual Room** A virtual room in Scopia® Desktop and Scopia® Mobile offers a virtual meeting place for instant or scheduled videoconferences. An administrator can assign a virtual room to each member of the organization. Users can send invitations to each other via a web link which brings you directly into their virtual room. Virtual meeting rooms are also dialed like phone extension numbers, where a user's virtual room number is often based on

that person's phone extension number. You can personalize your virtual room with PIN numbers, custom welcome slides and so on. External participants can download Scopia® Desktop or Scopia® Mobile free to access a registered user's virtual room and participate in a videoconference.

**VISCA Cable** A crossed VISCA cable connects two PTZ cameras to enable you to use the same remote control on both.

**Waiting Room** A waiting room is a holding place for participants waiting for the host or moderator to join the meeting. While waiting, participants see a static image with the name of the owner's virtual room, with an optional audio message periodically saying the meeting will start when the host arrives.

**Webcast** A webcast is a streamed live broadcast of a videoconference over the internet. Enable Scopia® Desktop webcasts by enabling the streaming feature. To invite users to the webcast, send an email or instant message containing the webcast link or a link to the Scopia® Desktop portal and the meeting ID.

**WUXGA** WUXGA defines a video resolution of 1920 x 1200 pixels.

**XGA** XGA defines a Video resolution of 1024 x 768 pixels.

**Zone** Gatekeepers like Avaya Scopia® ECS Gatekeeper split endpoints into zones, where a group of endpoints in a zone are registered to a gatekeeper. Often a zone is assigned a dial prefix, and usually corresponds to a physical location like an organization's department or branch.