RADVISION®
an Avaya company

Scopia Desktop Server

Installation Guide

Version 8.2.1

For Solution 8.2

David: Hi Dona!

Dona: Hi David, Did you send me your forecast for next quarter?

Yes. I sent it yesterday

8.2.1

No representation of warranties for fitness for any purpose other than what is specifically mentioned in this guide is made either by RADVISION Ltd or its agents.

RADVISION Ltd reserves the right to revise this publication and make changes without obligation to notify any person of such revisions or changes. RADVISION Ltd may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this publication, it is furnished under a license agreement included with the product as a separate document. If you are unable to locate a copy, please contact RADVISION Ltd and a copy will be provided to you.

For further information contact RADVISION or your local distributor or reseller.

Installation Guide for Scopia Desktop Server Version 8.2.1, July 16, 2013

http://www.radvision.com

Table of Contents

Chapter 1: About Scopia Desktop

Chapter 2: Planning your Scopia Desktop Server Deployment

Chapter 3: Installing Scopia Desktop

Chapter 4: Configuring Your Deployment

Chapter 5: Securing Your Scopia Desktop Deployment

Chapter 6: Deploying Multiple Scopia Desktop Servers with a Load Balancer

Glossary of Terms for Scopia Solution

Chapter 1 | About Scopia Desktop

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

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

Navigation

- About Scopia Desktop Server on page 5
- About Components of the Scopia Desktop Server on page 6
- About Scopia Desktop Client on page 7

About Scopia Desktop Server

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

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

Scopia Desktop offers the following additional features:

- Integration with Microsoft Outlook

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

- Streaming and recording

  You can create webcasts for others to view your videoconference, and you can record meetings for later viewing.

- Chat messages to meeting participants

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

- Service provider (multi-tenant) support

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

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

- Scopia Desktop Server has extensive support for security, both standard encryption with certificates and a proprietary secure protocol between the client and server. For more information, see Minimum Requirements and Specifications of Scopia Desktop Server on page 9.
- Scalability with an external load balancer

  Scopia Desktop works with load balancers like F5 BIG-IP Load Traffic Manager and Radware's AppDirector, providing unlimited scalability, high availability and redundancy for large deployments.
- High quality video and audio even with limited bandwidth or poor network conditions, by using H.264 High Profile for compression.

  H.264 High Profile is a standard for compressing video by up to 25% over the H.264 Baseline Profile, enabling high definition calls to be held over lower call speeds. It requires both sides of the transmission (sending and receiving endpoints) to support this protocol.
- Microsoft Lync support

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

About Components of the Scopia Desktop Server

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

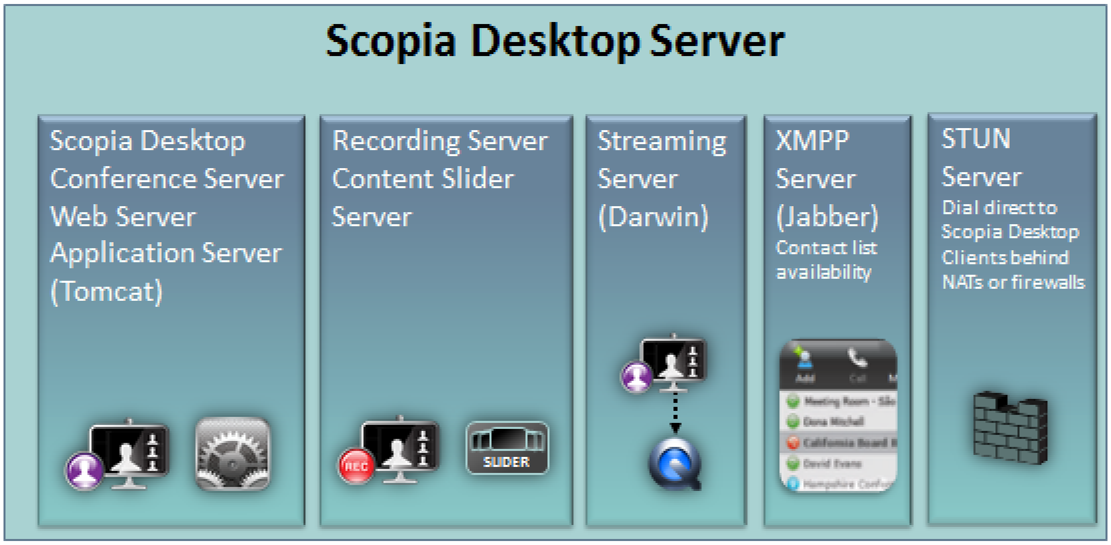

Scopia Desktop Server
Scopia Desktop Conference Server Web Server Application Server (Tomcat)
Recording Server Content Slider Server
REC
SLIDER
Streaming Server (Darwin)
XMPP Server (Jabber) Contact list availability
STUN Server Dial direct to Scopia Desktop Clients behind NATs or firewalls

Figure 1: Components of the Scopia Desktop Server

- Scopia Desktop Conference Server

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

- Scopia Desktop Application Server (Tomcat)

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

- Scopia Desktop Recording Server

  Part of the Tomcat Application Server, this service is responsible for recording meetings, storing the recordings and providing HTTP access to the recordings.

- Scopia Content Slider server

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

- Scopia Desktop Streaming Server (Darwin)

  Responsible for streaming webcasts.

- Scopia Desktop Presence (XMPP) Server (Jabber)

  Maintains a live list of contacts which are available or unavailable for video chat or videoconference. This information is presented in the Contact List of Scopia Desktop Pro. The XMPP server is also responsible for user authentication, and it is used for attendee registration and invitations.

- STUN Server

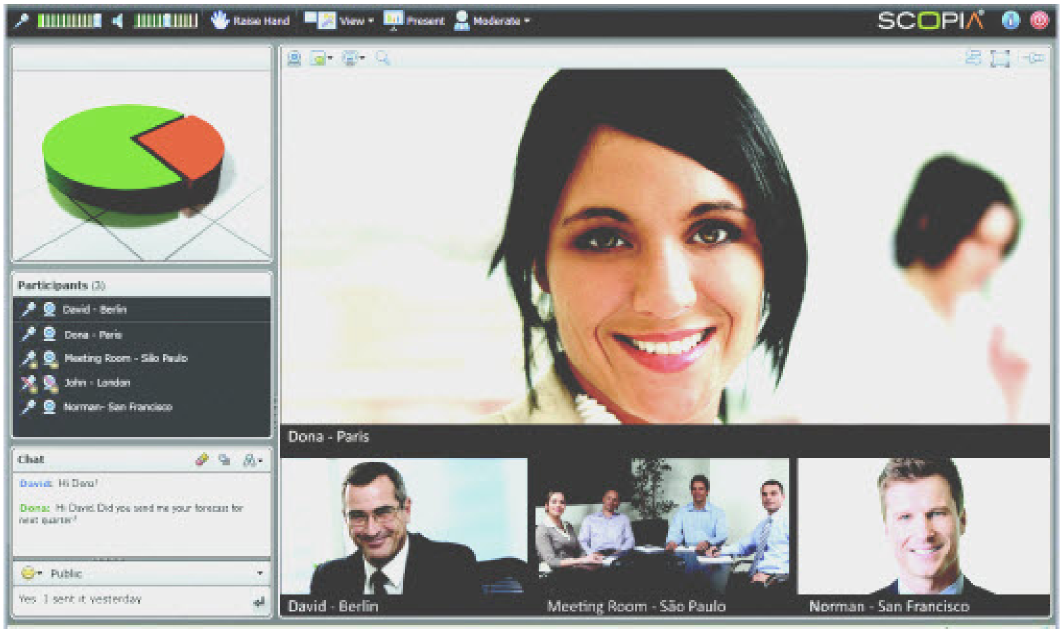
  Enables you to directly dial a Scopia Desktop Client behind a NAT or firewall in point-to-point implementations by giving that computer’s public internet address. Scopia Desktop also supports third-party STUN servers.

  Place the STUN Server in the DMZ, accessible by the Scopia Desktop Clients participating in a call. The STUN Server should have its own public IP address, not a NAT address.

About Scopia Desktop Client

The Scopia Desktop Client is a simple web browser plug-in for interactive videoconferencing using high definition or standard definition with superb quality. It is part of Scopia Desktop, the desktop videoconferencing solution which provides the client/server application that extends videoconferencing to remote and desktop users for voice, video and data communications.

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 2: The Scopia Desktop Client user interface on page 8).



David: Hi Dona!

Dona: Hi David. Did you send me your forecast for next quarter?

Yes. I sent it yesterday

Figure 2: The Scopia Desktop Client user interface

Users must have a login to have a virtual room to invite people to meetings. Scopia Desktop Client also includes support for 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.

A Scopia Add-in for Microsoft Outlook enables easy scheduling of meetings directly from within Microsoft Outlook. There are two types of Scopia Add-in for Microsoft Outlook: the 32 bit version works directly with the Scopia Desktop Server, while the 64 bit version works directly with Scopia Management. The 32 bit version of Scopia Add-in for Microsoft Outlook is installed together with Scopia Desktop Client, as described in Installing Scopia Desktop Client Locally on a PC on page 92. You can also configure the 64 bit version to install together with Scopia Desktop Client, or run a standalone installation. For more information, see the *User Guide for Scopia Add-in for Microsoft Outlook*.

Chapter 2 | Planning your Scopia Desktop Server Deployment

When planning your Scopia Desktop Server deployment, consider the following:

- How many users will be simultaneously connecting to videoconferences?
- Will most Scopia Desktop Clients connect to videoconferences from within the enterprise, or from outside? For example, if there are many internal Scopia Desktop Clients, consider placing a dedicated Conference Server in the enterprise.
- If reliability is a requirement, consider deploying redundant Scopia Desktop Servers.
- How often will your organization record videoconferences? How often will those recordings be viewed? Are there likely to be many simultaneous viewers?

  For example, if recording is a major part of your videoconferencing experience, you may decide to deploy a dedicated Recording Server.
- Will most users join videoconferences as participants, or view webcasts of meetings?
- What is your network's security policy?

  Depending on where you deploy the Scopia Desktop Server and other video network devices, you may need to open different ports on the firewall.
- How much internal and external bandwidth is required, based on the number of simultaneous users joining videoconferences? Consider also whether most users will be joining in standard or high definition.

Based on the factors above, decide whether to deploy all Scopia Desktop Server components on one server or on multiple dedicated servers. See the following sections for details on the different deployment options and how to plan your bandwidth:

Navigation

Minimum Requirements and Specifications of Scopia Desktop Server

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

Scopia Desktop Server Software Requirements

The minimum software requirements for the Scopia Desktop Server are:

Operating systems:

- Windows® 2008 SP2 or Windows® 2008 R2, 32 and 64 bit (English, Japanese)
- Windows® 2008 Datacenter or Enterprise Edition (English) with more than 4GB of RAM, or Windows® 2008 Standard Edition (English) with 4GB of RAM
- Windows® Server 2012

Important:

Scopia Desktop Servers should be deployed on a physical server, not virtual machines like VMware.

Web browsers (for the Scopia Desktop Server Administration):

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

- Internet Explorer 6 or later (Windows)
- Firefox 20 or later (Mac and Windows)
- Safari 5 or later (Mac and Windows)
- Google Chrome 25 or later (Mac and Windows)

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

- The Scopia Connector for IBM Lotus Sametime Connect works with IBM Lotus Sametime 8.0, 8.0.1, 8.0.2, 8.0.5, 8.5, 8.5.1, and IBM Lotus Notes 8.0.
- The Scopia Connector for IBM Lotus Sametime Web Conferencing works with IBM Lotus Sametime versions 8.0, 8.0.1, 8.0.2, and 8.0.5.
- The following versions of the Scopia Add-in for Microsoft Outlook:
  - 32 bit version of Scopia Add-in for Microsoft Outlook that can be installed from Scopia Desktop (does not work with Office 64 bit).
  - 64 bit version of Scopia Add-in for Microsoft Outlook that requires Office 2007 or later, and access to the Scopia Management user portal.

Scopia Desktop Server Hardware Requirements

Table 1: Call capacity and minimum hardware requirements for Scopia Desktop Server on page 11 lists the minimum hardware requirements and call capacity for the Scopia Desktop Server.

Important:

- All hard disks should have a minimum of 20Gb.
- The NIC card on the Scopia Desktop Server should be 1Gb full duplex, except for the Scopia Desktop 25 product, which can use a 100Mb NIC.
- If the server PC is not strong enough for the maximum number of connections, you can limit the number of calls in the Scopia Desktop Server. For more information, see Defining Scopia Desktop Server Public Address and Other Client Connection Settings on page 80.

Table 1: Call capacity and minimum hardware requirements for Scopia Desktop Server

Product name	Deployment	Maximum ports available	Minimum server hardware required
Scopia Desktop 25	On the same computer with Scopia Management	25 interactive participants 5 Scopia Content Slider sessions 75 streaming sessions 1 recording session	Intel® Xeon® Processor E3-1270, 3.50 GHz RAM: 4GB for Scopia Desktop Server 4 virtual cores 100Mb NIC
Scopia Desktop 50	On the same computer with Scopia Management	50 interactive participants 10 Scopia Content Slider sessions 150 streaming sessions 3 recording sessions	Intel® Xeon® Processor E3-1270, 3.50 GHz RAM: 4GB for Scopia Desktop Server (8GB when installed with Scopia Management) 4 virtual cores
Scopia Desktop 75	On the same computer with Scopia Management	75 interactive participants 15 Scopia Content Slider sessions 225 streaming sessions 3 recording sessions	Intel® Xeon® Processor E3-1270, 3.50 GHz RAM: 4GB for Scopia Desktop Server (8GB when installed with Scopia Management) 4 virtual cores
Scopia Desktop 100	On the same computer with Scopia Management	100 interactive participants 20 Scopia Content Slider sessions 300 streaming sessions 5 recording sessions	Intel® Xeon® Processor E3-1270, 3.50 GHz RAM: 4GB for Scopia Desktop Server (8GB when installed with Scopia Management) 4 virtual cores
Scopia Desktop 150	Dedicated conference server for Scopia Desktop	150 interactive participants	Intel® Xeon® Processor E3-1270, 3.50 GHz RAM: 4GB 4 virtual cores
Scopia Desktop 200	Dedicated conference server for Scopia Desktop	200 interactive participants	Intel® Xeon® Processor E3-1270, 3.50 GHz RAM: 4GB 4 virtual cores
Scopia Desktop 250	Dedicated conference server for Scopia Desktop	250 interactive participants	Intel® Xeon® Processor E3-1270, 3.50 GHz RAM: 4GB 4 virtual cores

Product name	Deployment	Maximum ports available	Minimum server hardware required
Content Center Server 300/10	Dedicated server for recording, streaming, and content slider	20 Scopia Content Slider sessions 300 streaming sessions 10 recording sessions	Intel® Xeon® Processor E3-1270, 3.50 GHz RAM: 4GB 4 virtual cores
Content Center Server 600/10	Dedicated server for recording, streaming, and content slider	40 Scopia Content Slider sessions 600 streaming sessions 10 recording sessions	Intel® Xeon® Processor E3-1270, 3.50 GHz RAM: 8GB 4 virtual cores
Scopia Content Slider Server	Dedicated server for content slider	100 Scopia Content Slider sessions	Intel® Xeon® Processor E3-1270, 3.50 GHz RAM: 8GB 4 virtual cores

You can store recordings locally on the Content Center Server or on any network server visble from the Content Center Server. Configure the location of recordings during the server installation (see Installing the Content Center for Scopia Desktop on a Dedicated Server on page 58).

Use the following formula to calculate the space required for recordings:

```
Recording Bandwidth (in megabytes) × Time (in seconds) + 20% Overhead
```

For example, for a call of 1 hour at 384 kbps (standard definition), calculate as follows:

```
384 kbps × (60 minutes × 60 seconds) = 1382400 kilobits
1382400 ÷ 1024 = 1350 megabits
1350 ÷ 8 = 168.75 megabytes (MB)
168.75 × 20% = 33.75MB (overhead)
Total is 168.75 + 33.75 = 202.5MB (including overhead)
```

Scopia Desktop Server Audio and Video Specifications

Scopia Desktop interoperates with both SIP and H.323 endpoints to provide a seamless user experience joining the ease of use of Scopia Desktop Clients and Scopia Mobile devices with dedicated endpoints like Scopia XT Executive and the Scopia XT Series.

- Audio support:
  - G.722.1 codec
  - DTMF tone detection (in-band, H.245 tones, and RFC2833)
- Video support:
  - High Definition (HD) Continuous Presence video with a maximum resolution of 720p at 30 frames per second (fps).
  - Video codec: H.264 with SVC (Scalable Video Coding) and H.264 High Profile
  - Video send resolutions: Up to HD 720p
  - Video receive resolution: HD 720p
  - Video bandwidth: HD up to 4Mbps for 720p resolutions; standard definition up to 448 kbps for 352p or lower

  - Presentation video: H.239 dual stream
  - Scopia Content Slider can function with presentation set to H.263 or H.264 on the MCU.

Scopia Desktop Server Security Specifications

Scopia Desktop Server has extensive support for security, both standard encryption with certificates and a proprietary secure protocol between the client and server:

- HTTPS protocol between Scopia Desktop Client and Scopia Desktop Server.
- SRTP encryption between Scopia Desktop Client/Scopia Mobile and Scopia Desktop Server
- TLS encryption between Scopia Desktop Server and Scopia Management

Planning your Topology for Scopia Desktop Server

You can deploy the Scopia Desktop components in various ways, depending on factors such as the number of videoconferencing users in your organization. For guidelines on how to assess your deployment's capacity, refer to Sizing your Scopia Desktop Server Deployment on page 23.

Scopia Desktop includes the following components:

- Conference Server for Scopia Desktop, to create videoconferences with Scopia Desktop Clients and Scopia Mobile devices
- Streaming Server for Scopia Desktop (Darwin), to stream webcasts
- Recording Server for Scopia Desktop (Tomcat), to record videoconferences
- Scopia Content Slider (Tomcat) to store data already presented in the videoconference, allowing participants to view previously shared content during the meeting
- STUN Server for Scopia Desktop to directly dial a Scopia Desktop Client behind a NAT or firewall in point-to-point implementations
- XMPP Presence Server (Jabber) for Scopia Desktop to maintain the contact list

For more information about the Scopia Desktop components, see About Components of the Scopia Desktop Server on page 6.

Depending on the size and capacity of your deployment, you can deploy these components on a single Scopia Desktop Server or install specific components on dedicated servers. See the following sections for the different deployment options:

Navigation

- Topology for Small Scopia Desktop Server Deployment on page 13
- Medium Scopia Desktop Server Deployment with Dedicated Servers on page 15
- Large Scopia Desktop Server Deployment with Dedicated Servers on page 17

Topology for Small Scopia Desktop Server Deployment

In a standard Scopia Desktop Server installation, you deploy a single all-in-one server with the following installed (see Figure 3: Typical small deployment of Scopia Desktop Server on page 14):

- A complete Scopia Desktop installation, which includes the Conference Server, as well as any other Scopia Desktop components used in your organization.

  Scopia Desktop Server includes various components, such as the Streaming Server, which allows users to view the videoconference webcast. For a detailed list of all Scopia Desktop components, see About Components of the Scopia Desktop Server on page 6.
- Scopia Management, an application used to control your video network devices and schedule videoconferences. Scopia Management includes a built-in gatekeeper.

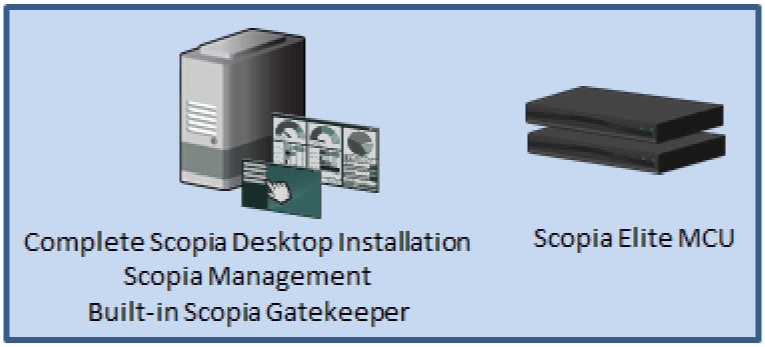

Complete Scopia Desktop Installation
Scopia Management
Built-in Scopia Gatekeeper
Scopia Elite MCU

Figure 3: Typical small deployment of Scopia Desktop Server

For information on the capacity of a single server, see Minimum Requirements and Specifications of Scopia Desktop Server on page 9.

The all-in-one server is typically deployed in the DMZ (see Figure 4: Deploying a Single Scopia Desktop Server in a Small Centralized Topology on page 14). Scopia Desktop Clients can connect from the internal enterprise network, a public network, or from a partner network.

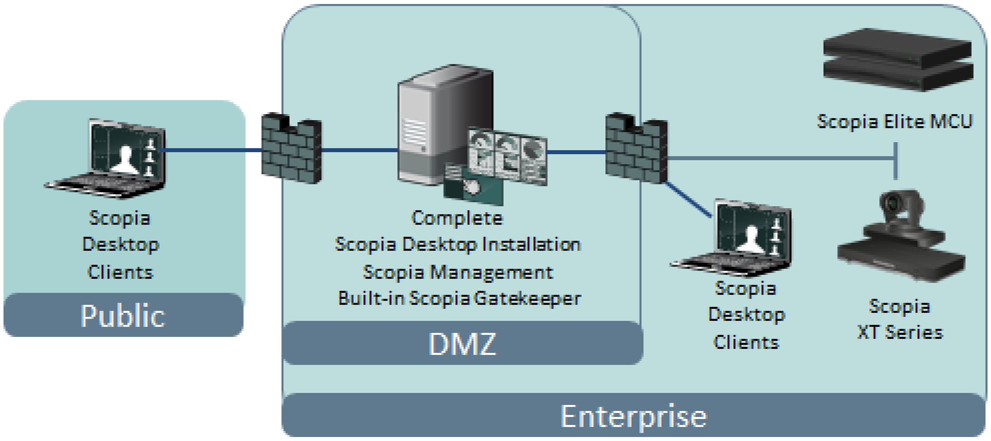


Figure 4: Deploying a Single Scopia Desktop Server in a Small Centralized Topology

This topology serves as the baseline deployment and is typically used for smaller organizations. To increase capacity, you can install Scopia Desktop components on dedicated servers (see Medium Scopia Desktop Server Deployment with Dedicated Servers on page 15).

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

Medium Scopia Desktop Server Deployment with Dedicated Servers

To increase the capacity of the deployment, you can dedicate a server for specific Scopia Desktop components, as follows:

- A dedicated Conference Server for Scopia Desktop, which includes the Conference Server and Web Server.
- A dedicated Content Center Server, which includes the recording, streaming, and content slider components. Depending on how these functions are used in your organization, you can deploy them separately. For example, if recording is a major part of your videoconferencing experience, you may decide to deploy a dedicated Recording Server.
- A dedicated XMPP Presence (Jabber) and STUN Server

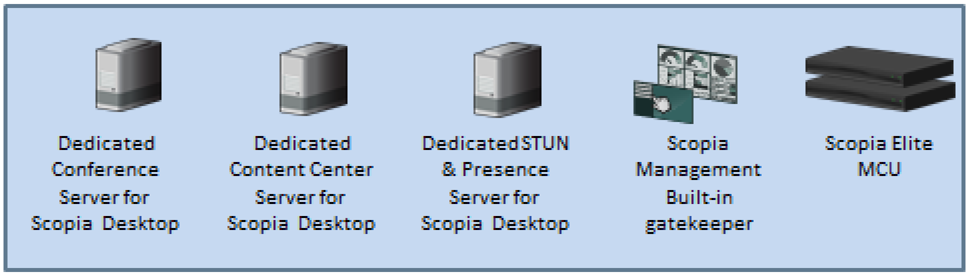

Dedicated Conference Server for Scopia Desktop
Dedicated Content Center Server for Scopia Desktop
Dedicated STUN & Presence Server for Scopia Desktop
Scopia Management Built-in gatekeeper
Scopia Elite MCU

Figure 5: Typical medium-sized deployment

Each Scopia Desktop Server deployed should match the minimum requirements detailed in Minimum Requirements and Specifications of Scopia Desktop Server on page 9. For more information about the Scopia Desktop components, see About Components of the Scopia Desktop Server on page 6.

Typically, you deploy the dedicated Scopia Desktop Servers in the DMZ, to provide connection to participants and webcast viewers connecting from both the internal and external networks (Figure 6: Deploying dedicated Scopia Desktop Servers in the DMZ on page 16). You can also deploy an additional server in the enterprise, so that internal participants do not need to connect through the firewall.

Depending on where you deploy the dedicated servers, you may need to open additional ports. For details, see Ports to Open on Scopia Desktop on page 38.

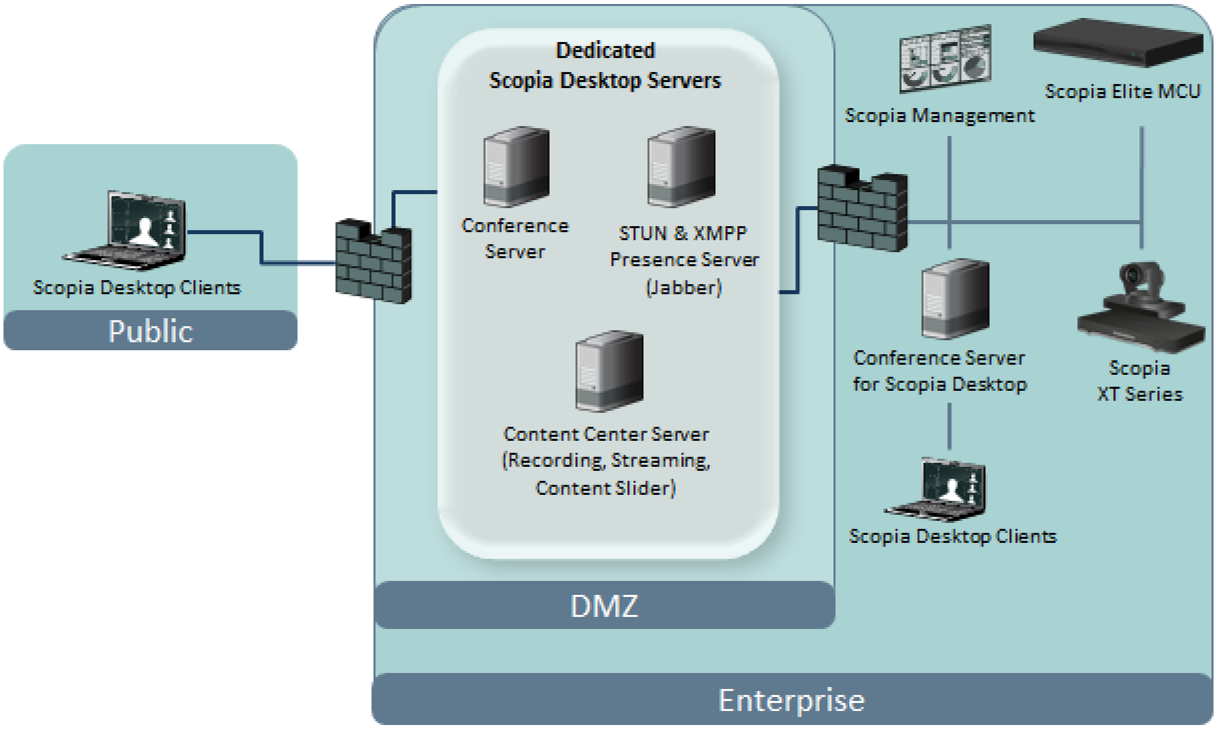


Figure 6: Deploying dedicated Scopia Desktop Servers in the DMZ

This is typically relevant for larger deployments. You can also cluster the Scopia Desktop Servers behind a load balancer, as described in Large Scopia Desktop Server Deployment with Dedicated Servers on page 17. Smaller deployments, on the other hand, might install all components on the same Scopia Desktop Server with a Scopia Management (see Topology for Small Scopia Desktop Server Deployment on page 13).

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

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

When deciding which components are suitable for your organization, refer to Table 2: Deploying dedicated Scopia Desktop Servers on page 17.

Table 2: Deploying dedicated Scopia Desktop Servers

Dedicated Scopia Desktop Server	Function
Dedicated Conference Server for Scopia Desktop	Mandatory Responsible for creating videoconferences with Scopia Desktop Clients and Scopia Mobile devices, and connects to the MCU for connectivity with H.323 and SIP endpoints. Also provides access to the Scopia Desktop web portals for the user and administrator.
Dedicated Content Center Server for Scopia Desktop	Optional (install for the functionality listed below) Install a dedicated Content Center Server with one or more of the following components: • Recording: To record meetings, perform user authentication, and provide access to the web portal. • Streaming: To stream live webcasts of videoconferences. • Content Slider: To allow participants to catch up with previously presented slides. For increased capacity, you can deploy the recording or streaming components on two different servers. If installing the Scopia Content Slider, install it on the Recording Server. Scopia Content Slider can function with presentation set to H.263 or H.264 on the MCU. If you have more than one Recording Server, you access each one to view the recordings stored by that specific server. For example, if you want to access a recording stored on Recording Server A, you must connect to Recording Server A. You cannot access it from Recording Server B.
Dedicated XMPP Presence Server & STUN Server for Scopia Desktop	Optional (install for the functionality listed below) Install a dedicated server with the following components: • XMPP Presence: To maintain a live list of contacts which are available or unavailable for video chat or videoconference. • STUN: To enable users to directly dial a Scopia Desktop Client or Server behind a NAT or firewall in point-to-point implementations.

Large Scopia Desktop Server Deployment with Dedicated Servers

Large deployments, such as service providers or large organizations, typically deploy multiple dedicated Scopia Desktop Servers. To provide scalability and high availability, with service preservation for up to 100,000 registered users, you can cluster several dedicated Conference Servers behind a load balancer as described in Deploying Scopia Desktop with a Load Balancer on page 20.

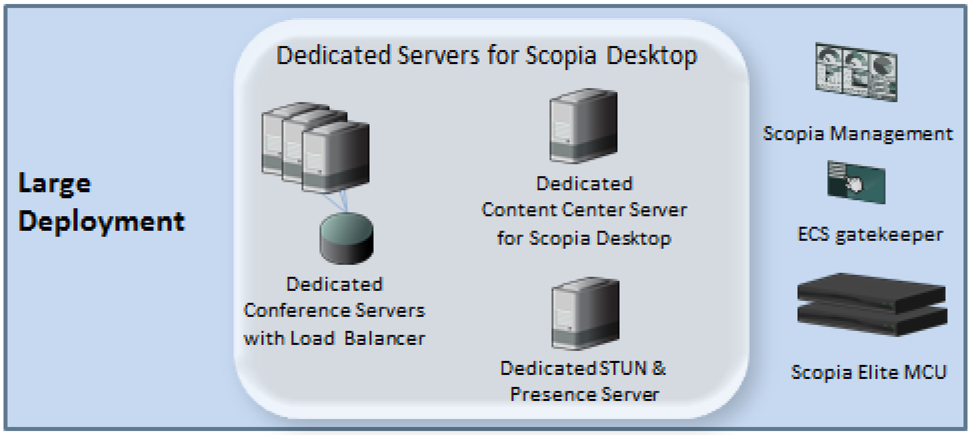

Large Deployment
Dedicated Servers for Scopia Desktop
Dedicated Conference Servers with Load Balancer
Dedicated Content Center Server for Scopia Desktop
Dedicated STUN & Presence Server
Scopia Management
ECS gatekeeper
Scopia Elite MCU

Figure 7: Typical large deployment

The videoconferencing infrastructure, including the Scopia Desktop Server, is typically deployed in the DMZ to provide connection to participants and webcast viewers connecting from both the internal and external networks (Figure 8: Large Scopia Desktop Server Deployment with Dedicated Servers on page 18).

You can also deploy an additional Conference Server in the enterprise, so that participants in internal videoconferences do not need to connect through the firewall.

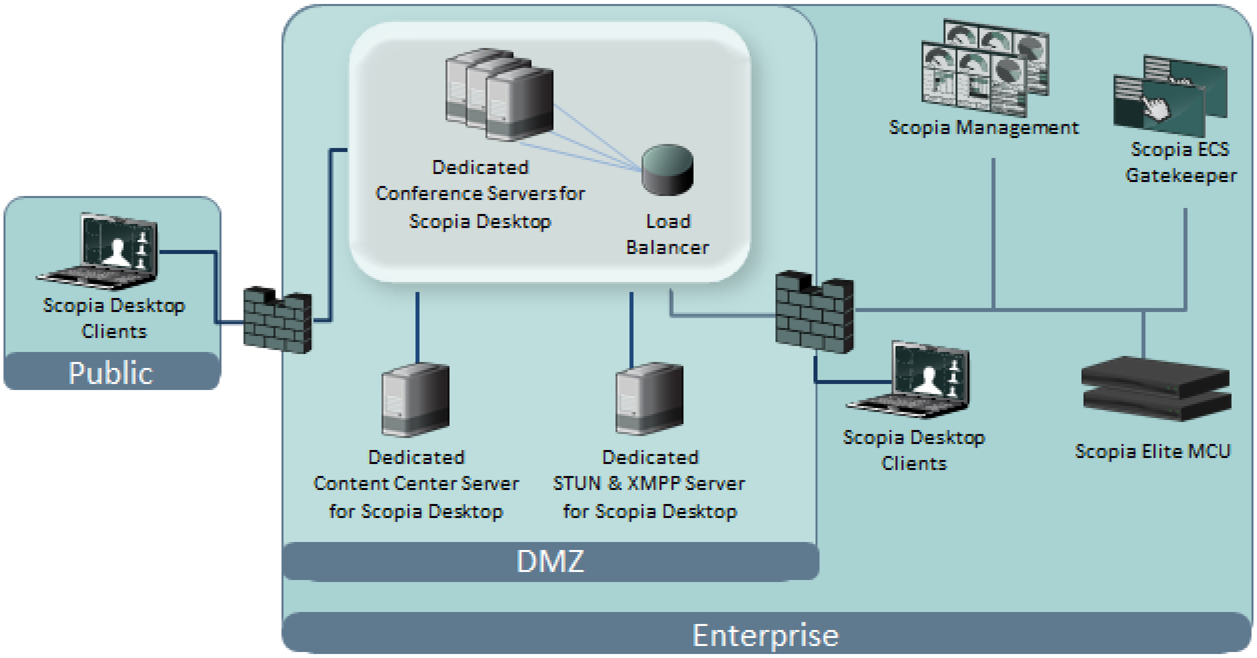

Dedicated Conference Servers for Scopia Desktop
Load Balancer
Scopia Management
Scopia ECS Gatekeeper
Scopia Desktop Clients
Public
Dedicated Content Center Server for Scopia Desktop
Dedicated STUN & XMPP Server for Scopia Desktop
Scopia Desktop Clients
Scopia Elite MCU
DMZ
Enterprise

Figure 8: Large Scopia Desktop Server Deployment with Dedicated Servers

Enterprises can deploy the videoconferencing infrastructure in more than one location. This can be done either for redundancy or, if there are many customers in different regions of the world, you can deploy a full set of videoconferencing infrastructure in the headquarters, and another set of infrastructure in a branch.

See the *Solution Guide for Scopia Solution* for detailed information about different ways to deploy your videoconferencing infrastructure.

When deciding which components are suitable for your organization, refer to Table 3: Deploying dedicated Scopia Desktop Servers on page 19.

Table 3: Deploying dedicated Scopia Desktop Servers

Dedicated Scopia Desktop Server	Function
Dedicated Conference Server for Scopia Desktop	Mandatory Responsible for creating videoconferences with Scopia Desktop Clients and Scopia Mobile devices, and connects to the MCU for connectivity with H.323 endpoints. Also provides access to the Scopia Desktop web portals for the user and administrator.
Dedicated Content Center Server for Scopia Desktop	Optional Install a dedicated Content Center Server with one or more of the following components: • Recording: To record meetings, perform user authentication, and provide access to the web portal. • Streaming: To stream live webcasts of videoconferences. • Content Slider: To allow participants to catch up with previously presented slides. For increased capacity, you can deploy the recording or streaming components on two different servers. If installing the Scopia Content Slider, install it on the Recording Server. Scopia Content Slider can function with presentation set to H.263 or H.264 on the MCU. If you have more than one Recording Server, you access each one to view the recordings stored by that specific server. For example, if you want to access a recording stored on Recording Server A, you must connect to Recording Server A. You cannot access it from Recording Server B.
Dedicated XMPP Presence Server & STUN Server for Scopia Desktop	Optional (install for the functionality listed below) Install a dedicated server with the following components: • XMPP Presence: To maintain a live list of contacts which are available or unavailable for video chat or videoconference. • STUN: To enable users to directly dial a Scopia Desktop Client or Server behind a NAT or firewall in point-to-point implementations.

Each Scopia Desktop Server deployed should match the minimum requirements detailed in Minimum Requirements and Specifications of Scopia Desktop Server on page 9.

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

Deploying Scopia Desktop with a Load Balancer

For increased reliability and scalability, you can deploy multiple Scopia Desktop Servers behind a load balancer such as Radware's AppDirector or another load balancer (Figure 10: Typical load balanced Scopia Desktop deployment on page 21).

A load balancer groups together a set (or cluster) of servers to give them a single IP address, known as a virtual IP address. It distributes client service requests amongst a group of servers. It distributes loads according to different criteria such as bandwidth, CPU usage, or cyclic (round robin). Load balancers are also known as application delivery controllers (ADC).

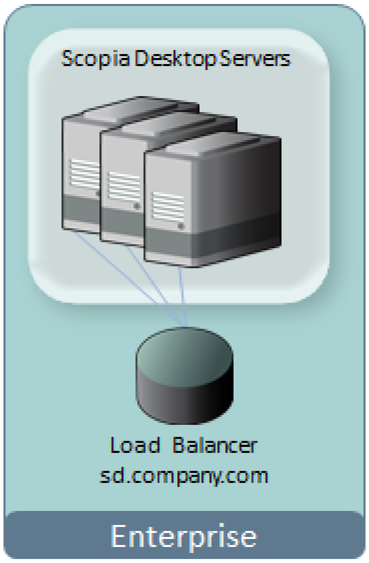


Figure 9: Deploying Scopia Desktop with a Load Balancer

All servers in the cluster should have identical functionality enabled, since one server must take over if another is overloaded or fails. If you deploy dedicated servers for the different components of Scopia Desktop (for example, a dedicated recording or streaming server), these dedicated servers should be located outside the cluster. For more information, see Configuring Streaming and Recording in a Load Balancing Environment on page 119.

Typically, the Scopia Desktop cluster is deployed in the DMZ, to enable both internal and external participants to join the videoconference. If many videoconferences include only internal participants, consider deploying an additional Conference Server in the enterprise, or, for increased capacity, an additional cluster with a load balancer.

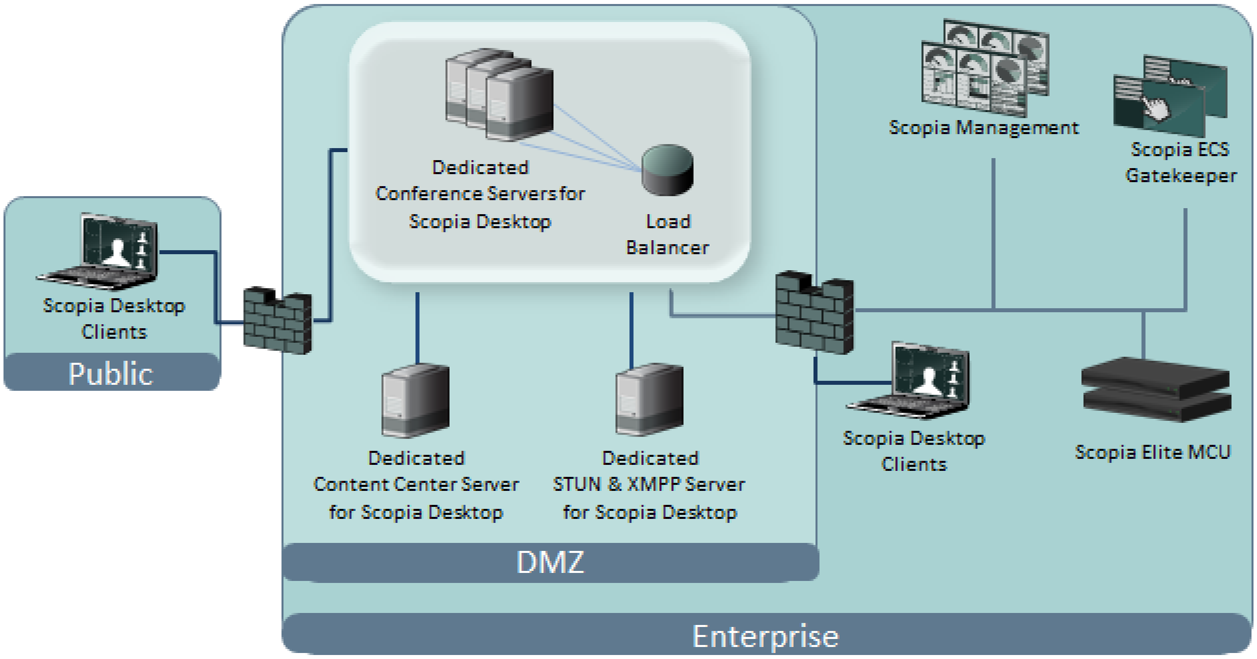


Figure 10: Typical load balanced Scopia Desktop deployment

When clustering multiple Scopia Desktop Servers in your deployment, all servers must be configured with the same security mode. When a device establishes a secure connection with another component, it sends a signed certificate verifying its identity. The signature on the certificate must be from a known (trusted) certification authority (CA). For more information about security, see Securing a Load Balanced Environment on page 122.

Important:

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

You can configure the load balancer to route all network traffic or only part of it, depending on the load balancer's capacity and your deployment requirements (Figure 11: Media can either bypass or travel via the load balancer (example) on page 22):

- In full load balancing deployments, all network traffic between servers and clients, including the media (audio, video, data presentations), is routed via the load balancer. This is best for powerful load balancer servers, and has the added security advantage of withholding the private IP of a Scopia Desktop Server to the outside world.
- In partial load balancing deployments, the media data travels directly between client and server, bypassing the load balancer, while signaling and management still travel via the load balancer. This is better for less powerful load balancer computers, but directly exposes the servers' private IP addresses to the outside world.

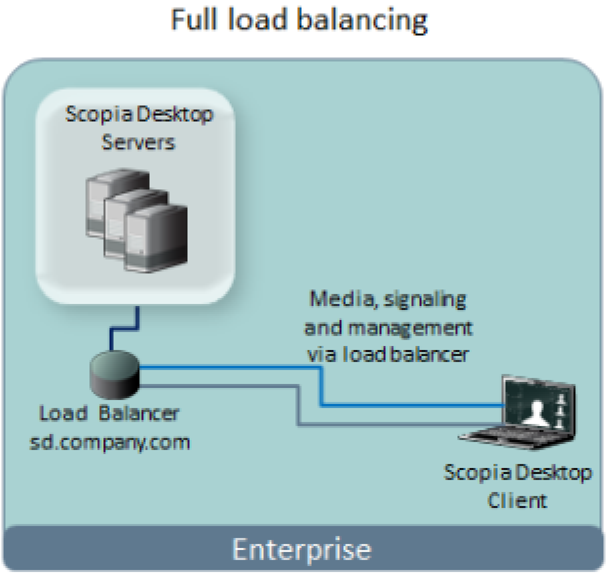

Full load balancing
Partial load balancing
Scopia Desktop Servers
Media, signaling and management via load balancer
Load Balancer sd.company.com
Scopia Desktop Client
Enterprise
Scopia Desktop Servers
Media connection direct to server
Signaling and management via load balancer
Load Balancer sd.company.com
Scopia Desktop Client
Enterprise

Figure 11: Media can either bypass or travel via the load balancer (example)

If your deployment includes dedicated servers for streaming and/or recording in a load balancing environment, you can choose one of the following deployments:

- Point all Scopia Desktop Servers in the cluster to a single dedicated streaming and/or recording server outside the cluster. The playback client communicates directly with the dedicated server.
- Enable streaming capabilities in each Scopia Desktop Server in the cluster.

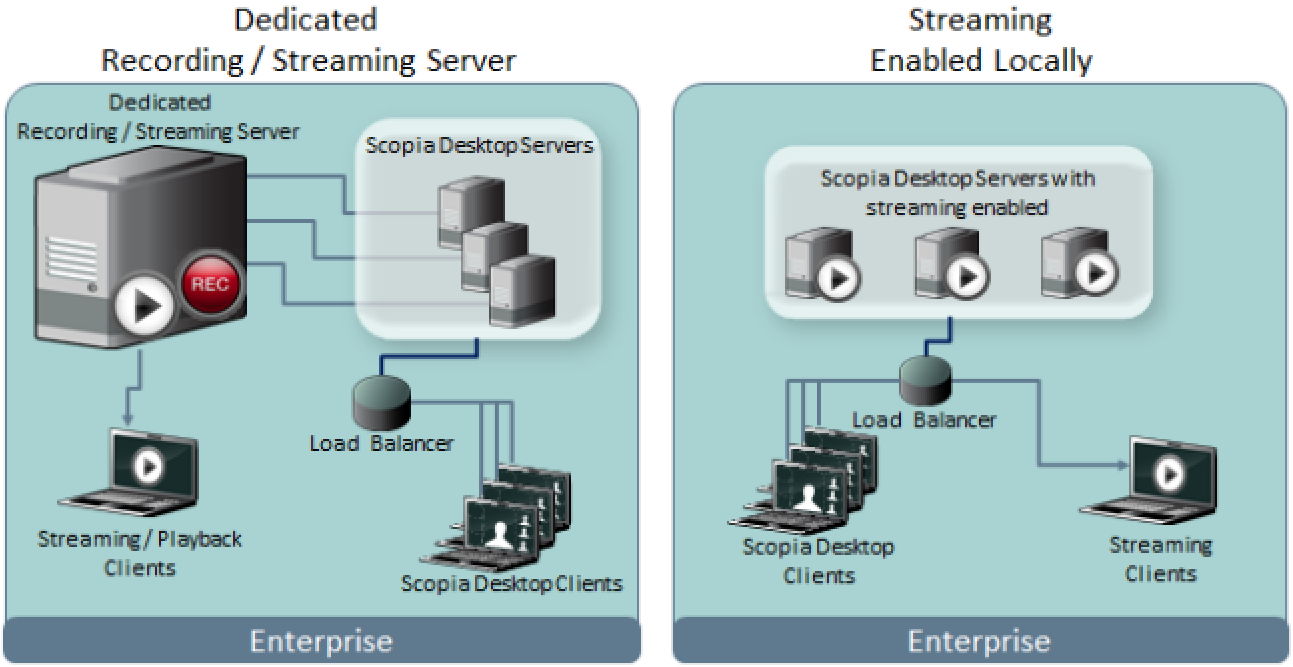

Dedicated Recording / Streaming Server
Streaming Enabled Locally
Dedicated Recording / Streaming Server
Scopia Desktop Servers
REC
Load Balancer
Streaming / Playback Clients
Scopia Desktop Clients
Enterprise
Scopia Desktop Servers with streaming enabled
Load Balancer
Scopia Desktop Clients
Streaming Clients
Enterprise

Figure 12: Deploying either a dedicated recording/streaming server, or enabling local streaming

For details about configuring load balancing, see Deploying Multiple Scopia Desktop Servers with a Load Balancer on page 105.

Sizing your Scopia Desktop Server Deployment

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

- Topology for Small Scopia Desktop Server Deployment on page 13
- Medium Scopia Desktop Server Deployment with Dedicated Servers on page 15
- Large Scopia Desktop Server Deployment with Dedicated Servers on page 17

Figure 13: Typical Scopia Desktop Server setups based on size of deployment on page 23 illustrates typical deployments for small, medium, and large organizations. For details on the complete deployment, including other video infrastructure devices such as Scopia PathFinder Server, see *Solution Guide for Scopia Solution*.

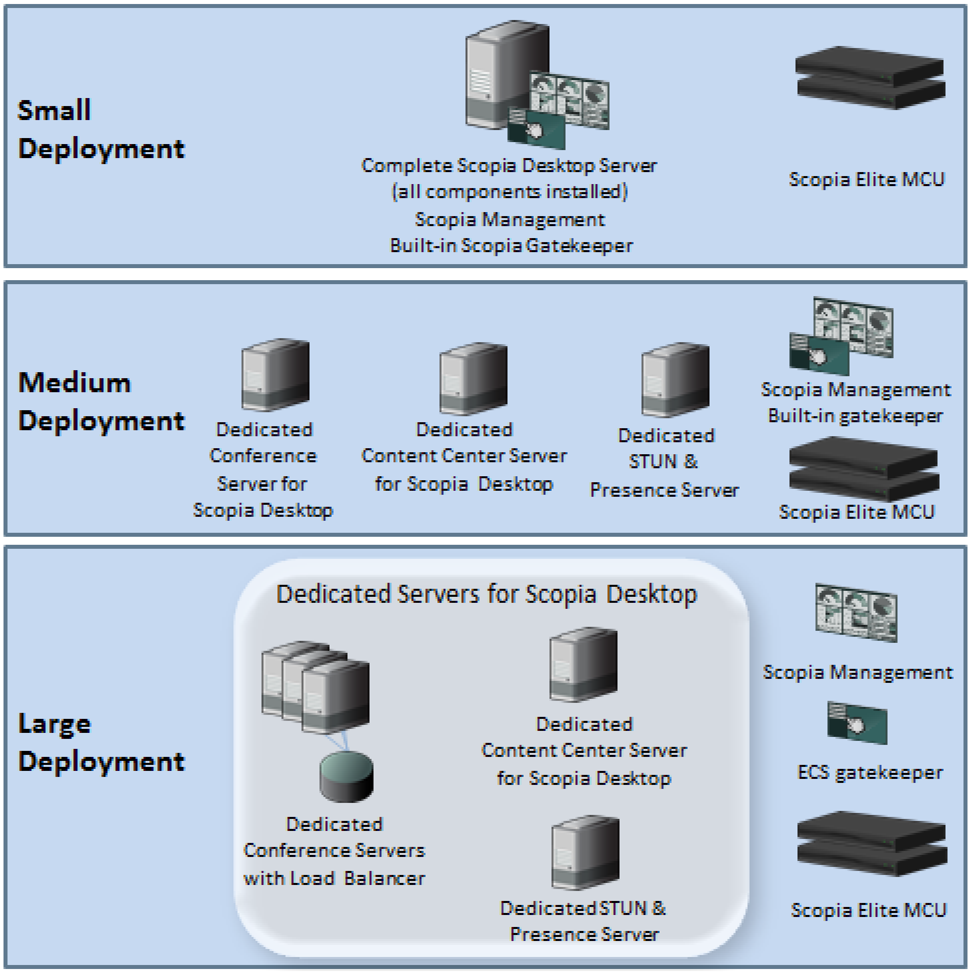

Small Deployment
Complete Scopia Desktop Server
(all components installed)
Scopia Management
Built-in Scopia Gatekeeper
Scopia Elite MCU
Medium Deployment
Dedicated Conference Server for Scopia Desktop
Dedicated Content Center Server for Scopia Desktop
Dedicated STUN & Presence Server
Scopia Management
Built-in gatekeeper
Scopia Elite MCU
Large Deployment
Dedicated Servers for Scopia Desktop
Dedicated Conference Servers with Load Balancer
Dedicated Content Center Server for Scopia Desktop
Dedicated STUN & Presence Server
Scopia Management
ECS gatekeeper
Scopia Elite MCU

Figure 13: Typical Scopia Desktop Server setups based on size of deployment

Choose a Scopia Desktop Server deployment based on factors such as number of users and bandwidth efficiency. Refer to Table 4: Sizing your Scopia Desktop Server deployment on page 24 for details.

When sizing your deployment and planning the number of MCUs required, it is also important to consider the number of simultaneous users that are connecting in standard definition (SD) and high definition (HD). Your chosen video resolution (and bandwidth), places demands on your MCU to supply that video resolution for each connection, which determines how many users can simultaneously connect to the MCU. For more information, see Planning the Bandwidth for Scopia Desktop Clients Based on MCU Capacity on page 27. For details on planning your MCU deployment and determining the number of simultaneous participants based on the video resolution, see *Installation Guide for Scopia Elite MCU*.

Table 4: Sizing your Scopia Desktop Server deployment

Number of Simultaneous Participants	Deployment	Number of Scopia Desktop Servers	Bandwidth Considerations
Up to 100	Single all-in-one Scopia Desktop Server with Scopia Management (small centralized deployment)	One To increase reliability, you can deploy a redundant server. To increase the number of users, you can deploy an additional Conference Server for Scopia Desktop.	In centralized deployments, all calls are directed to the MCUs located in one place. This puts a strain on bandwidth if videoconferences involve many remote endpoints. For details on ensuring sufficient bandwidth for your deployment, and planning your bandwidth to suit your MCU capacity, see Planning your Bandwidth Requirements on page 26.
Up to 250 per server	Dedicated Servers for medium organizations (large centralized deployment)	Typically two Conference Servers for Scopia Desktop. One of these servers may include the Content Center Server.	
	Dedicated servers for service providers (large centralized deployment)	Typically three servers, depending on how the Scopia Desktop components are allocated. Can be deployed as a cluster behind a load balancer.	
	Dedicated servers for service providers (distributed deployment)	One server or cluster in each location.	Distributed deployments save bandwidth in large videoconferences including many remote endpoints. However, smaller videoconferences might be unnecessarily cascaded between different MCUs and therefore use more bandwidth. For details on ensuring sufficient bandwidth for your deployment, and planning your bandwidth to suit your MCU capacity, see Planning your Bandwidth Requirements on page 26.

You can store recordings locally on the Content Center Server or on any network server visible from the dedicated Content Center Server. Configure the location of recordings during the server installation (see Installing the Content Center for Scopia Desktop on a Dedicated Server on page 58).

Use the following formula to calculate the space required for recordings:

```
Recording Bandwidth (in megabytes) × Time (in seconds) + 20% Overhead
```

For example, for a call of 1 hour at 384 kbps (standard definition), calculate as follows:

```
384 kbps × (60 minutes × 60 seconds) = 1382400 kilobits
1382400 ÷ 1024 = 1350 megabits
1350 ÷ 8 = 168.75 megabytes (MB)
168.75 × 20% = 33.75MB (overhead)
Total is 168.75 + 33.75 = 202.5MB (including overhead)
```

Deploying Scopia Desktop Server with Dual-NIC

Scopia Desktop Server can be installed on servers with multiple Network Interface Cards (NICs). Depending on the deployment and network configuration, you may want to control which NIC is used for various server communications.

Important:

Use bonded 100 Mbit NICs or a Gigabyte NIC. The default settings are 384 kbps for every participant connection, and 256 kbps for webcast viewers.

For example, in secure multiple NIC deployments you can use a NIC configured behind the firewall to communicate with various servers, while using another NIC for Scopia Desktop Client connections (Figure 14: Scopia Desktop Server with a dual-NIC deployment on page 26). In this case, configure the Scopia Desktop IP address to represent the NIC behind the firewall. For the Scopia Desktop public address, use a DNS name which resolves to the NIC outside the firewall, and is accessible both inside and outside the enterprise.

For more information and to configure the public address, see Defining Scopia Desktop Server Public Address and Other Client Connection Settings on page 80.

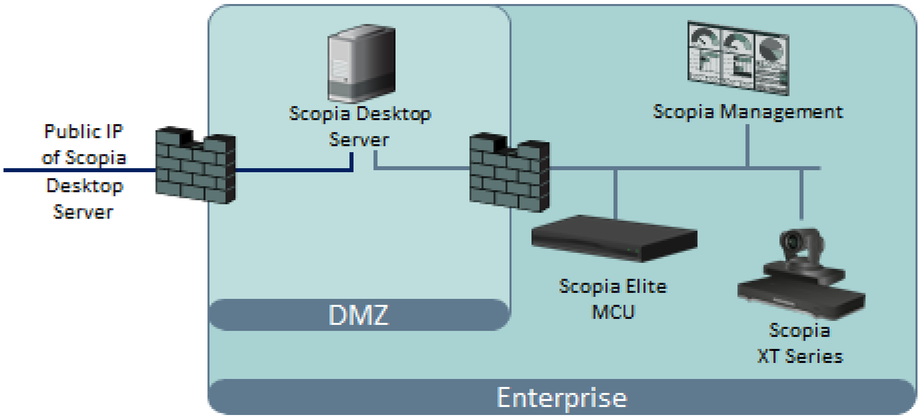


Figure 14: Scopia Desktop Server with a dual-NIC deployment

Scopia Desktop Clients can connect to the Scopia Desktop Server either by an IP address or a DNS name. In many deployments the Scopia Desktop Server IP address is not accessible to clients outside the enterprise due to NAT or firewall restrictions. Therefore, Scopia Desktop Server has a public address, which must be a DNS name resolving to the correct Scopia Desktop Server IP address both inside and outside the corporate network.

Planning your Bandwidth Requirements

The Scopia Solution supports a number of technologies designed to minimize the bandwidth used in videoconferences. For more information on the bandwidth-saving features of Scopia Solution, see *Scopia Solution Guide*. Even so, there are policy decisions you can make to reduce bandwidth further by deciding on the location of video network components and setting bandwidth management policies in your organization. You can estimate the total bandwidth required for Scopia Desktop, which includes:

- Bandwidth consumed by videoconference participants connecting to the Scopia Desktop Server (Scopia Desktop Clients and Scopia Mobile devices)
- Bandwidth consumed by viewers of videoconference webcasts
- Bandwidth consumed by users downloading a recorded videoconference

Use your Scopia Desktop bandwidth estimation to do the following:

- Calculate your bandwidth costs, for both external and internal bandwidth (see Calculating the Bandwidth Used by Scopia Desktop Participants on page 30).

  For example, to reduce bandwidth, you may decide that all calls going outside your organization are limited to standard definition (SD), or that all calls are SD by default.
- Use Scopia Management to define the bandwidth policies for different user profiles.

  For example, company executives are usually allocated more bandwidth. For details, see *Administrator Guide for Scopia Management*.
- Define the maximum bandwidth of MCU meeting types (also known as services), which define the videoconference parameters, including the bandwidth.

  For example, you can define a dial prefix which restricts the meeting to audio-only or SD, to consume much less bandwidth than an HD videoconference. For details, see *Administrator Guide for Scopia Elite MCU*.
- Decide how many users can actively participate or watch the videoconference as a webcast only.

Participants take up four times the bandwidth of webcast viewers. For details, see Calculating Scopia Desktop Bandwidth in a Centralized Deployment on page 31 and Calculating Scopia Desktop Bandwidth in a Distributed Deployment on page 32.

Important:

The bandwidth used by each Scopia Desktop Client indirectly determines the capacity of your deployed MCUs. Your chosen video resolution (and bandwidth), places demands on your MCU to supply that video resolution for each connection, which determines how many users can simultaneously connect to the MCU. For more information, see Planning the Bandwidth for Scopia Desktop Clients Based on MCU Capacity on page 27.

When calculating the total bandwidth required for videoconferencing, you need to also consider the bandwidth required by other Scopia Solution products included in your deployment, such as the MCU and Scopia XT Series.

Figure 15: Planning your Scopia Desktop bandwidth

For details on how to calculate the bandwidth, see the following sections:

Navigation

- Planning the Bandwidth for Scopia Desktop Clients Based on MCU Capacity on page 27
- Calculating the Bandwidth Used by Scopia Desktop Participants on page 30
- Allocating Bandwidth for Downloading Recordings on page 36
- Calculating the Total Required Bandwidth for Scopia Desktop on page 37

Planning the Bandwidth for Scopia Desktop Clients Based on MCU Capacity

As part of planning your bandwidth requirements, decide the maximum bandwidth to be used by each Scopia Desktop Client (measured as its bitrate). The bandwidth used by each Scopia Desktop Client indirectly determines the capacity of your deployed MCUs. Your chosen video resolution (and bandwidth), places demands on your MCU to supply that video resolution for each connection, which determines how many users can simultaneously connect to the MCU.

Bitrate is the speed of data flow. Higher video resolutions require higher bitrates to ensure the video is constantly updated, thereby maintaining smooth motion. The bandwidth determines how fast the data can be transferred.

When planning the maximum bitrate, it is important to consider the following factors, as illustrated in Figure 16: Planning the maximum bandwidth on page 29:

- The desired video resolution

  High definition (HD) videoconferences require a higher bitrate than standard definition (SD) videoconferences. If you lower the bitrate, you lower the quality of the video. For example, each Scopia Desktop Client requires at least 384 kbps for a SD videoconference at 480p, or at least 512 kbps for an HD videoconference at 720p (depending on the MCU model).

- The MCU capacity

  The MCU capacity determines how many users can simultaneously connect to a videoconference with a given video resolution. As you increase the video resolution, the number of users that can be supported by the MCU decreases. The capacity is based on the number of MCU ports used per Scopia Desktop Client.

  For example, for a 480p videoconference, each Scopia Desktop Client uses 1/4 port on the Scopia Elite 6000 Series MCU. For a 720p videoconference, however, each Scopia Desktop Client uses either 1/2 or 1 port (depending on your license). For more information, see the *Installation Guide for Scopia Elite MCU*.

- The compression capabilities of the MCU and Scopia Desktop

  The Scopia Elite 6000 Series MCU and Scopia Desktop offer H.264 High Profile encoding, allowing a higher resolution at a lower bitrate than other MCUs. 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.

  If your deployment also includes an MCU without H.264 High Profile (such as the Scopia Elite 5000 Series MCU), endpoints connecting to this MCU may use a lower resolution for the same bandwidth.

When planning the maximum call rate for Scopia Desktop, use the information provided in Table 5: Bandwidth and capacity requirements for each Scopia Desktop Client on page 29, as well as the other sections described in Planning your Bandwidth Requirements on page 26. To define the maximum call rate, see Defining Bandwidth Settings in Scopia Desktop Server on page 79.

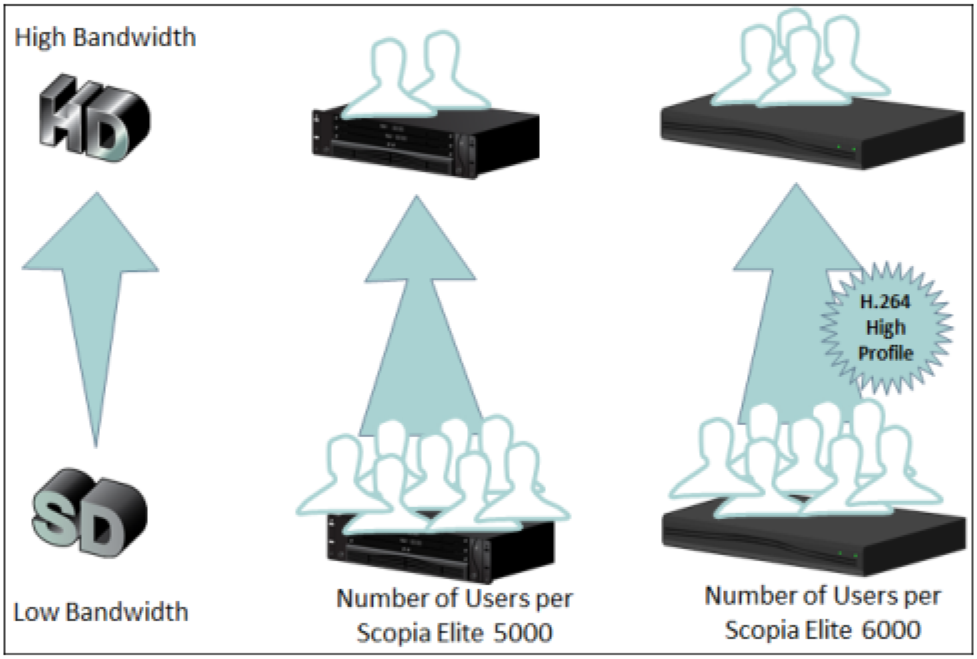


Figure 16: Planning the maximum bandwidth

Table 5: Bandwidth and capacity requirements for each Scopia Desktop Client on page 29 lists the bitrate (in kbps) and the number of required ports on the MCU per Scopia Desktop Client, based on specific video resolutions. The table illustrates how the same resolution in the newer MCU model requires less bandwidth and fewer ports because of H.264 High Profile.

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

Video Resolution	Scopia Elite 5000 Series MCU		Scopia Elite 6000 Series MCU with H.264 High Profile	
	Bitrate	**Capacity**	**Bitrate**	**Capacity**
352p	384 kbps	Each Scopia Desktop Client uses 1/4 port	256 kbps	Each Scopia Desktop Client uses 1/4 port
480p	512 kbps	Each Scopia Desktop Client uses 1 port (or 1/2 port with the MCU's double capacity license, see *Installation Guide for Scopia Elite MCU* for more information)	384 kbps	Each Scopia Desktop Client uses 1/4 port
720p	768 kbps	Each Scopia Desktop Client uses 1 port	512 kbps	Each Scopia Desktop Client uses 1 port (or 1/2 port with the MCU's double capacity license, see *Installation Guide for Scopia Elite MCU* for more information)

The number of participants that can be hosted by a single MCU depends on the MCU model. For more information, see *Installation Guide for Scopia Elite MCU*.

Calculating the Bandwidth Used by Scopia Desktop Participants

This section describes how to calculate the bandwidth required for videoconferences with Scopia Desktop participants and webcast viewers (both Scopia Desktop Clients and Scopia Mobile devices).

The Scopia Desktop Server coordinates videoconferences between Scopia Desktop Clients/Scopia Mobile devices and the MCU.

Typically, Scopia Desktop Servers are deployed in the same location as the MCU, hence the bandwidth between the Scopia Desktop Servers and the MCU is internal. However, if your deployment is set up with the Scopia Desktop Servers in a different location than the MCU, you also need to consider the bandwidth between the Scopia Desktop Servers and the MCU when considering bandwidth costs. For more information about distributed deployments, see *Solution Guide for Scopia Solution*.

❗ **Important:**

The bandwidth used by the Recording Server is managed separately, as described in Allocating Bandwidth for Downloading Recordings on page 36, except when it is installed on the same PC as other Scopia Desktop components. In such cases, users watching recorded meetings would consume bandwidth which would otherwise be used by videoconferences.

Table 6: Default bandwidth used for one connection on page 30 lists the default bandwidth used for each connection between the participant/webcast viewer and the Scopia Desktop Server.

Table 6: Default bandwidth used for one connection

Type of connection	Default bandwidth required
Upload bandwidth for one SD participant	384 kbps
Download bandwidth for one SD participant	384 kbps
Download bandwidth for one SD webcast viewer	384 kbps
Upload bandwidth for one HD participant	1024 kbps
Download bandwidth for one HD participant	1024 kbps
Download bandwidth for one HD webcast viewer	1024 kbps

❗ **Important:**

The actual bandwidth consumed for a specific video resolution depends on the compression capabilities of your MCU. For example, Scopia Elite 6000 Series MCU includes H.264 High Profile encoding, therefore allowing a higher resolution at a lower bitrate than other MCUs. For more information, see Planning the Bandwidth for Scopia Desktop Clients Based on MCU Capacity on page 27.

Depending on your deployment, see the following sections to calculate the bandwidth for Scopia Desktop calls:

Navigation

- Calculating Scopia Desktop Bandwidth in a Centralized Deployment on page 31
- Calculating Scopia Desktop Bandwidth in a Distributed Deployment on page 32

Calculating Scopia Desktop Bandwidth in a Centralized Deployment

This topic describes how to calculate the bandwidth required for Scopia Desktop calls when the Scopia Desktop Server is deployed in the same physical location as the MCU (also known as a centralized deployment).

If the Scopia Desktop Server is deployed in a different location than the MCU (also known as a distributed deployment), or if your deployment requires cascading between multiple branches, see Calculating Scopia Desktop Bandwidth in a Distributed Deployment on page 32.

Figure 17: Upload and download bandwidths for centralized deployments on page 31 illustrates the bandwidth to take into account when planning your resources.

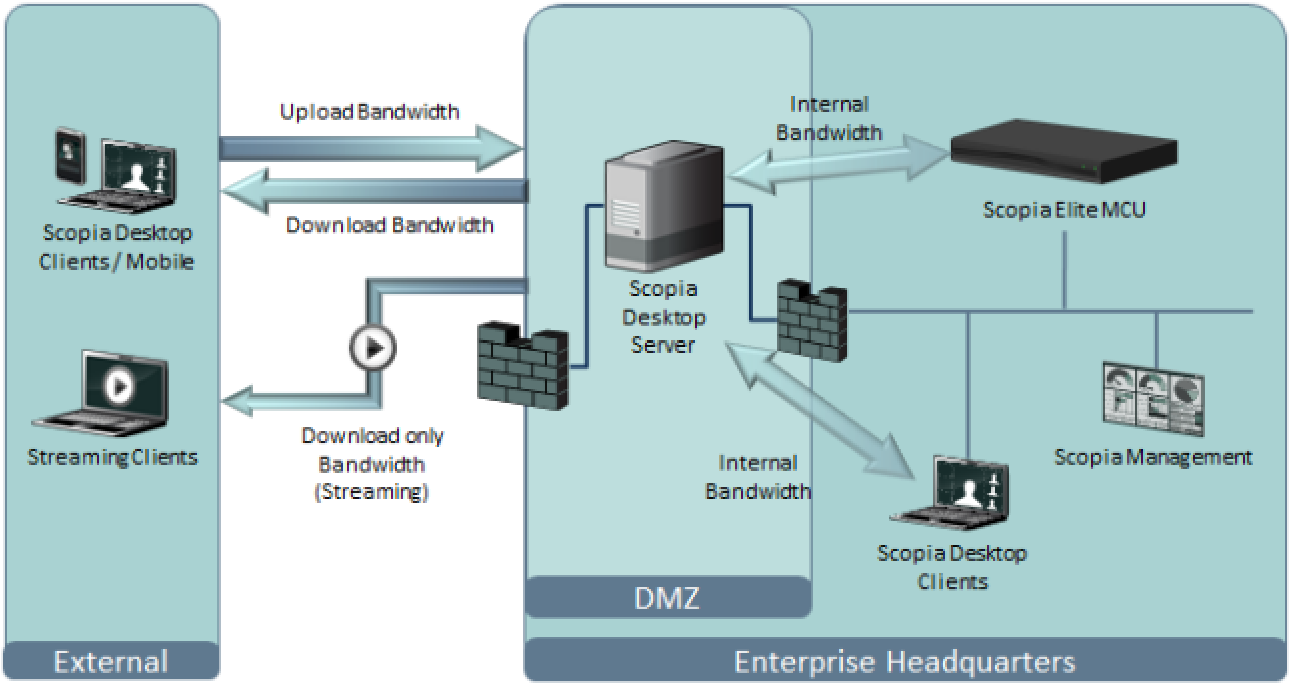
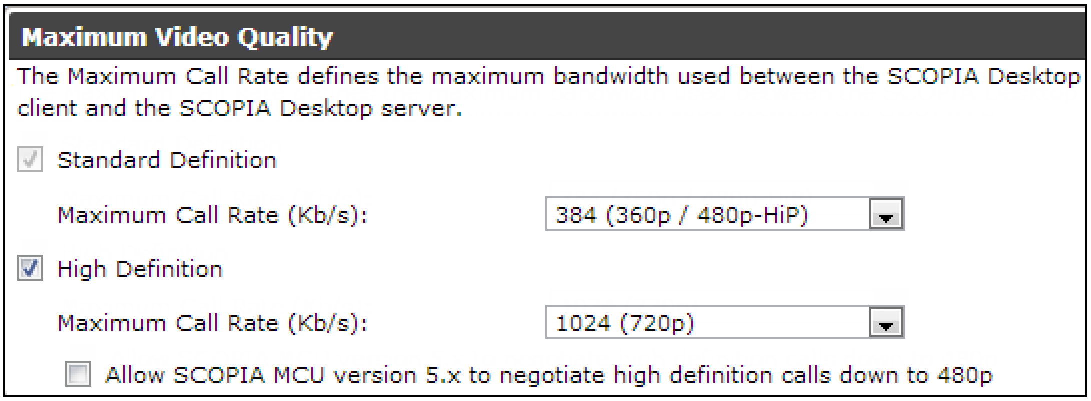


Figure 17: Upload and download bandwidths for centralized deployments

The bandwidth used for each Scopia Desktop Client participant is defined in the server settings (see Figure 18: Setting bandwidth defaults for Standard and High Definition on page 32). For viewing streamed videoconferences, there is only the download bandwidth to consider. For more information on defining these settings, see Defining Bandwidth Settings in Scopia Desktop Server on page 79.



Maximum Video Quality

The Maximum Call Rate defines the maximum bandwidth used between the SCOPIA Desktop client and the SCOPIA Desktop server.

☑ Standard Definition

Maximum Call Rate (Kb/s): 384 (360p / 480p-HiP)

☑ High Definition

Maximum Call Rate (Kb/s): 1024 (720p)

□ Allow SCOPIA MCU version 5.x to negotiate high definition calls down to 480p

Figure 18: Setting bandwidth defaults for Standard and High Definition

The formula is:

```
Total upload bandwidth = upload bandwidth per participant × num of internet participants
Total download bandwidth = download bandwidth per participant
                           × (num of internet participants + num of internet webcast viewers)
```

For example, if the defined call rate is 384 kbps, each participant uses 384 kbps for uploading and 384 kbps for downloading. So if 10 Scopia Desktop participants connect to a videoconference at 384 kbps, the bandwidth for these participants is 3,840 kbps for upload and 3840 kbps for download. 50 users is 19,200 kbps (or 19 Mbps) for uploads and 19 Mbps for downloads.

You should also consider whether the participants and webcast viewers are connecting from the internal or external network, to ensure there is sufficient internal and external bandwidth. For example, if your organization typically has 100 simultaneous participants connecting in SD, you require 38,400 kbps of bandwidth for uploading and 38,400 kbps for downloading. If 80 of these participants are connecting from the public network, you need to increase your organization's external bandwidth by an additional 30,720 kbps for both uploading and downloading media.

To calculate the total bandwidth required for Scopia Desktop, including both the bandwidth consumed by participants/webcast viewers, and downloading recordings, see Calculating the Total Required Bandwidth for Scopia Desktop on page 37.

Calculating Scopia Desktop Bandwidth in a Distributed Deployment

This topic describes how to calculate the bandwidth required for Scopia Desktop calls in distributed deployments. For centralized deployments, see Calculating Scopia Desktop Bandwidth in a Centralized Deployment on page 31.

There are several types of distributed Scopia Desktop deployment:

- Standard distributed deployment with cascading
- Distributed deployments without cascading
- Fragmented distributed deployments

A cascaded videoconference is a meeting distributed over more than one physical 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.

In each case, the external bandwidth costs vary significantly because of the cascading or the location of video network components in your deployment. The list below identifies the bandwidth formula for each distributed deployment type.

- Standard distributed deployment with cascading

  Each location has its own MCU and Scopia Desktop Server, so any local videoconference would not incur external bandwidth costs. Meetings which cross locations are created via a cascaded link between the two local MCUs, thereby using much less bandwidth, enabling all local clients to participate in the same meeting (Figure 19: Cascading meetings in a distributed deployment: clients connect to local MCU on page 33).

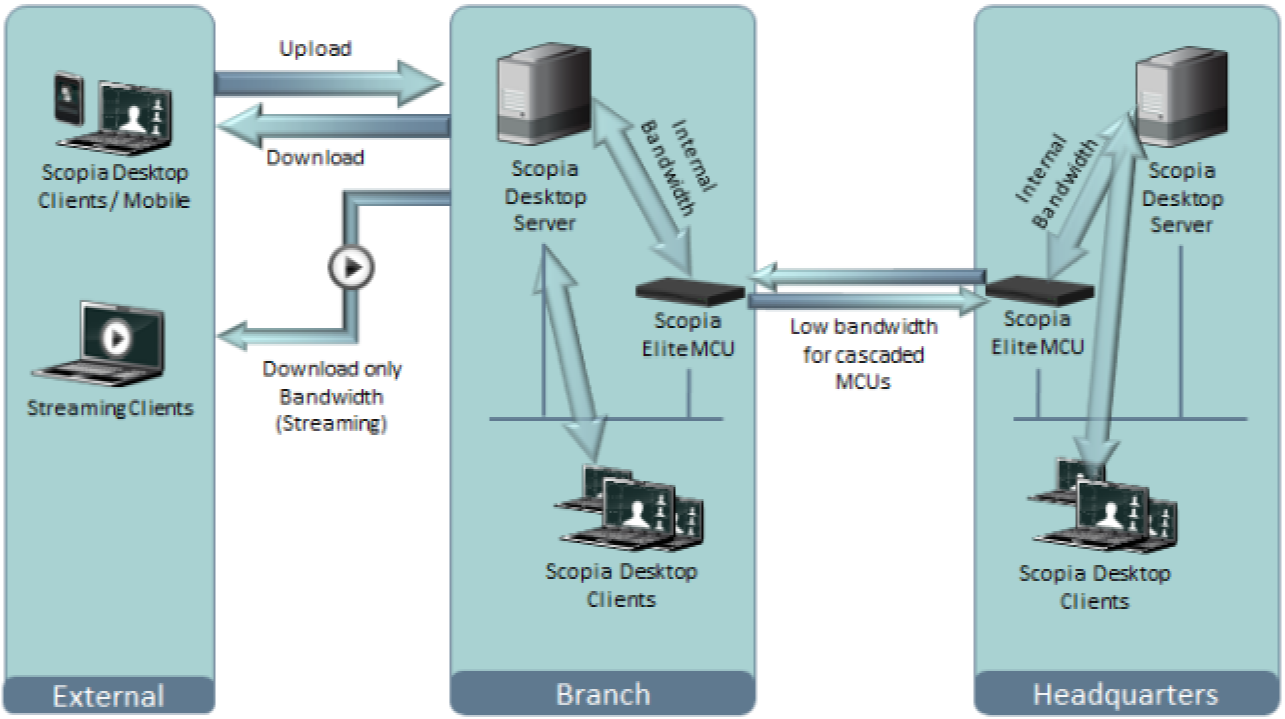
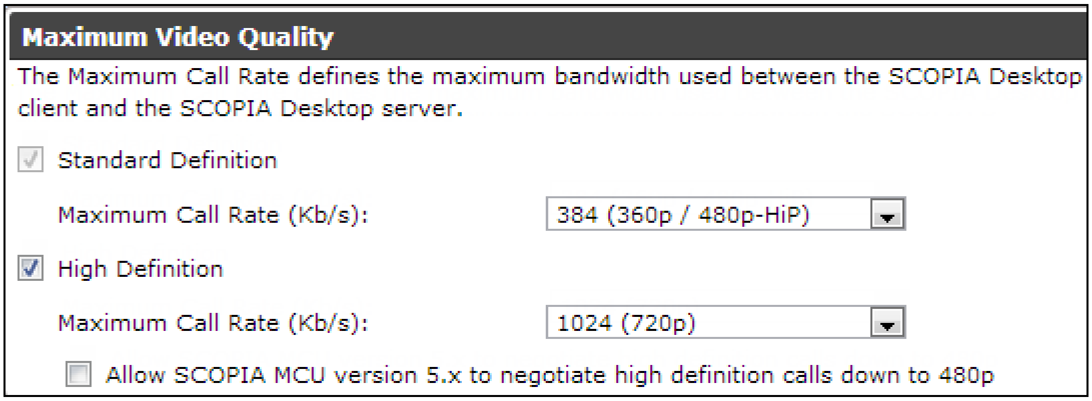


Figure 19: Cascading meetings in a distributed deployment: clients connect to local MCU

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

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

Each external Scopia Desktop Client connects with its own bandwidth usage as defined in the server settings (see Figure 20: Setting bandwidth defaults for Standard and High Definition on page 34). For viewing streamed videoconferences, there is only the download bandwidth to consider. For more information on defining these settings, see Defining Bandwidth Settings in Scopia Desktop Server on page 79.



Maximum Video Quality

The Maximum Call Rate defines the maximum bandwidth used between the SCOPIA Desktop client and the SCOPIA Desktop server.

☑ Standard Definition

Maximum Call Rate (Kb/s): 384 (360p / 480p-HiP)

☑ High Definition

Maximum Call Rate (Kb/s): 1024 (720p)

☐ Allow SCOPIA MCU version 5.x to negotiate high definition calls down to 480p

Figure 20: Setting bandwidth defaults for Standard and High Definition

The formula is to calculate external bandwidth usage is:

```
Total upload bandwidth = (upload bandwidth per participant × num of internet participants)
                       + (upload bandwidth of cascading MCU service × num simultaneous cascaded links)

Total download bandwidth = (download bandwidth per participant × num of internet participants)
                         + (download bandwidth of cascaded MCU service × num of cascaded links)
                         + (download bandwidth per participant × num of internet streaming viewers)
```

- Distributed deployments without cascading

  Without cascading, internal meetings still only use internal bandwidth, but when participants connect to a meeting hosted in another location, each client uses the same bandwidth as though they were connecting externally (Figure 21: Participants connect to a remote server on page 34).

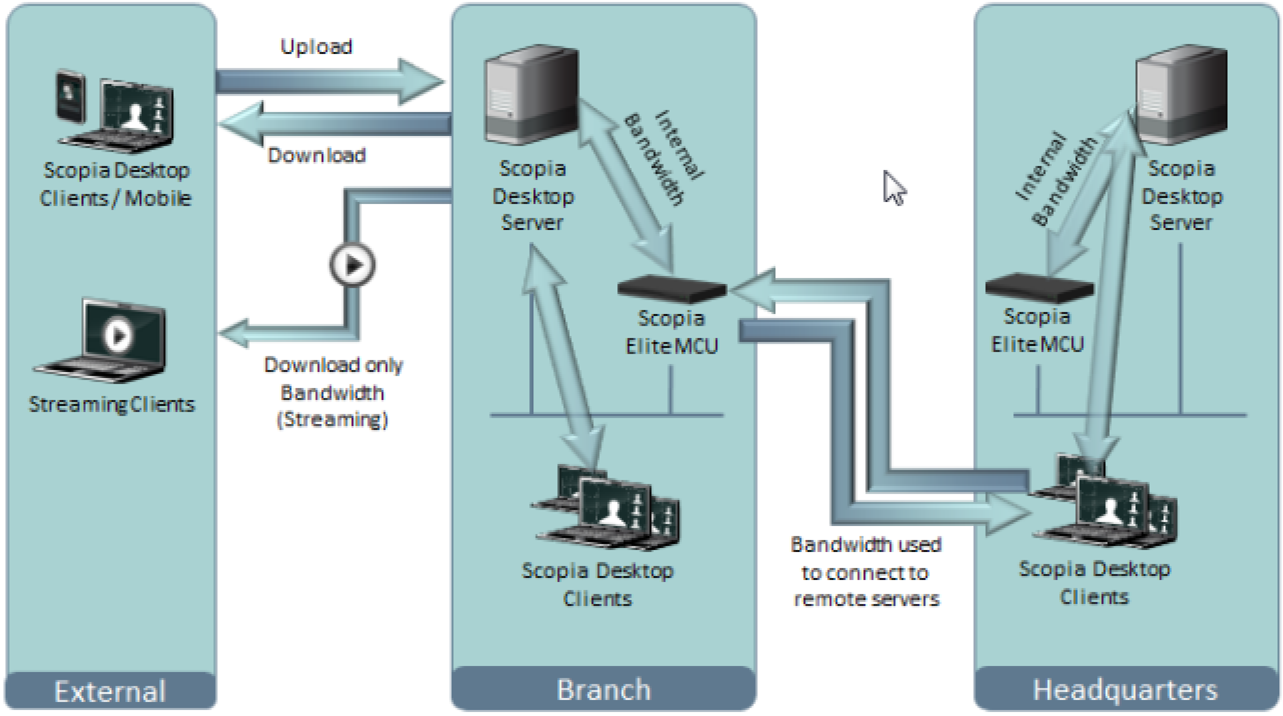


Figure 21: Participants connect to a remote server

The bandwidth used for each Scopia Desktop Client participant (external or in a different branch) connecting to a remote server is defined in the server settings (see Figure 20: Setting bandwidth defaults for Standard and High Definition on page 34). For viewing streamed videoconferences, there is only the download bandwidth to consider.

The formula is to calculate external bandwidth usage is:

```
Total upload bandwidth = upload bandwidth per participant x
                         (num of branch participants + num of internet participants)

Total download bandwidth = download bandwidth per participant
                         × (num of branch participants + num of internet participants + num of internet
stream viewers)
```

- Fragmented distributed deployments

  In fragmented deployments, each location houses different components of the deployment, making it the most bandwidth-intensive solution. External bandwidth costs are incurred for every participant, and furthermore, each connection's media is relayed again externally between the Scopia Desktop Server and the MCU (Figure 22: Fragmented distributed deployment requires more external bandwidth on page 35).

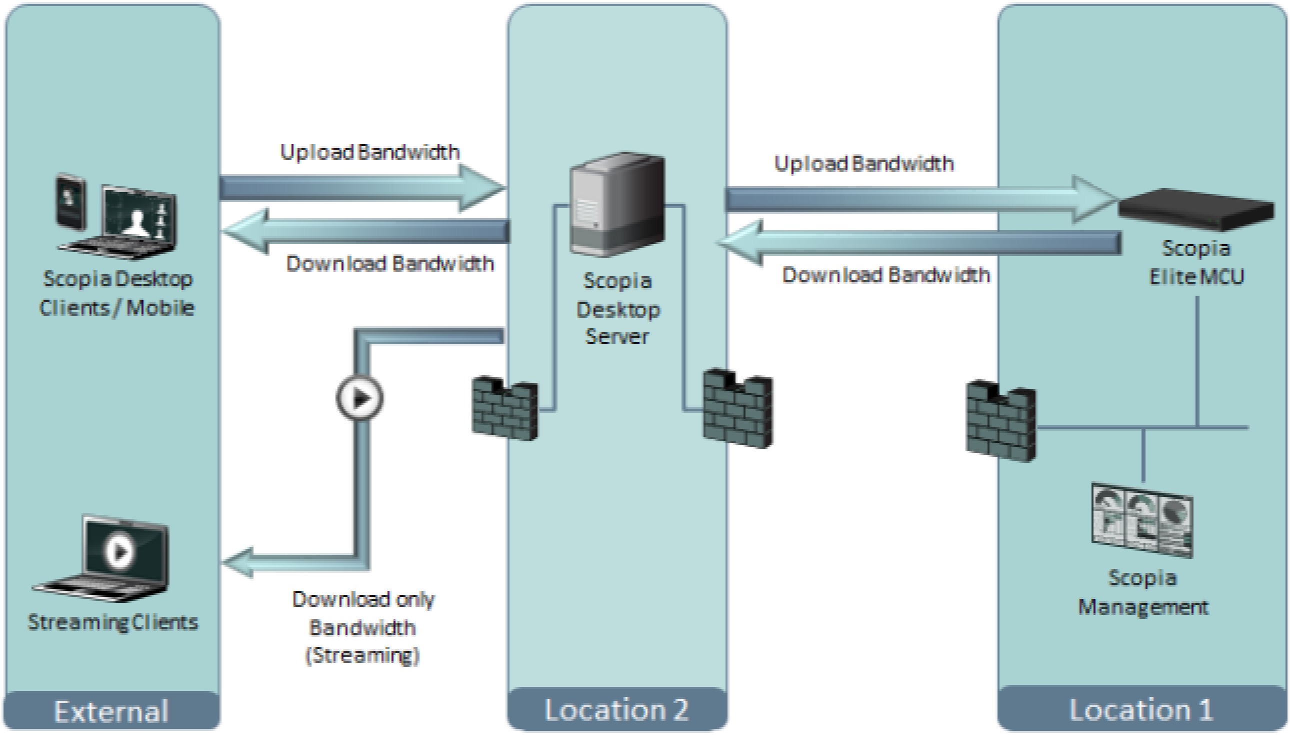


Figure 22: Fragmented distributed deployment requires more external bandwidth

In this case, the bandwidth for each participant's upload or download is double the bandwidth defined on the server (Figure 20: Setting bandwidth defaults for Standard and High Definition on page 34), because it needs to be transmitted twice, once from the client to server and another between the server and the MCU. Even Scopia Desktop Clients in the same location as the MCU must upload and download twice, since everything must be routed via the Scopia Desktop Server which is in a different location.

The formula is to calculate external bandwidth usage is:

```
Total upload bandwidth = 2 x (upload bandwidth per participant x num of participants)
Total download bandwidth = (2 x download bandwidth per participant x num of participants)
                         + (download bandwidth per participant x num of streaming viewers)
```

To calculate the total bandwidth required for Scopia Desktop, including both the bandwidth consumed by participants/webcast viewers, and downloading recordings, see Calculating the Total Required Bandwidth for Scopia Desktop on page 37.

Allocating Bandwidth for Downloading Recordings

This section describes how to allocate bandwidth to users who download recorded videoconferences.

Typically, the bandwidth used for playback of recordings is managed separately from the bandwidth of videoconference participation and webcast viewing. Server hardware capabilities often determine the maximum bandwidth for playback, since the quality of playback is directly related to the number of people viewing the playback at the same time. For more information on hardware requirements, see Minimum Requirements and Specifications of Scopia Desktop Server on page 9.

If the Recording Server is installed on the same server as the other components of the Scopia Desktop Server, users playing back recorded meetings consume part of the same bandwidth which might have been used for other purposes, such as videoconferences.

The bandwidth allocated for recording is divided between the number of users who simultaneously watch a recording. For example, if you allocate 100 Mbps for recording bandwidth, Scopia Desktop allows all 100 Mbps if one user watches a recording, or 50 Mbps per user if two users watch recordings simultaneously. To prevent too many users from watching recordings at the same time, you can define the minimum bandwidth that must be available before a user starts watching a recording.

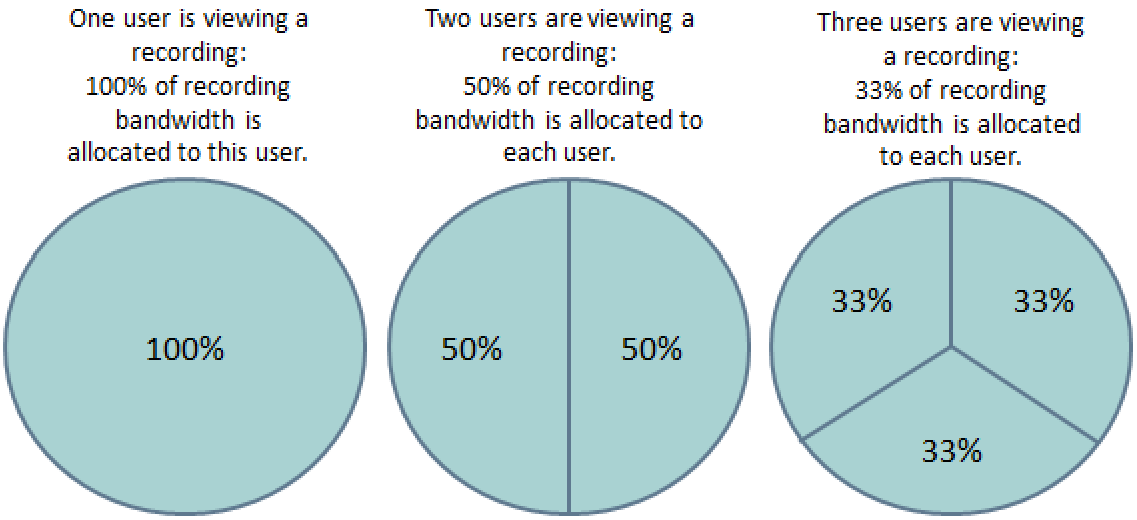
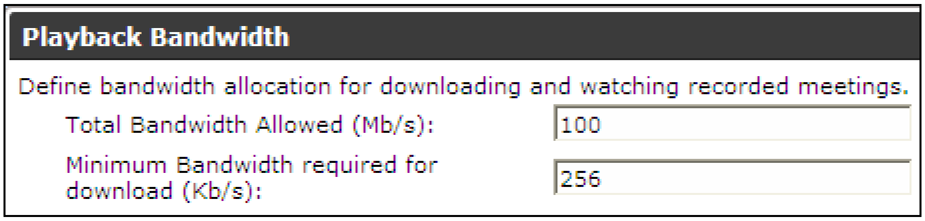


Figure 23: Allocating Recording Bandwidth

Estimate the number of remote and internal users who would simultaneously download recordings, to calculate the required internal and external bandwidth.

You can configure the recording bandwidth in the Scopia Desktop Server, by defining both the total bandwidth allocated for downloading recordings, and limit how many users can download recordings at the same time (Figure 24: Defining playback bandwidth on page 37). For details, see *Administrator Guide for Scopia Desktop Server*.


Playback Bandwidth

Define bandwidth allocation for downloading and watching recorded meetings.

Total Bandwidth Allowed (Mb/s): 100

Minimum Bandwidth required for download (Kb/s): 256

Figure 24: Defining playback bandwidth

To calculate the total bandwidth required for Scopia Desktop, including both the bandwidth consumed by participants/webcast viewers, and downloading recordings, see Calculating the Total Required Bandwidth for Scopia Desktop on page 37.

Calculating the Total Required Bandwidth for Scopia Desktop

The total bandwidth required for Scopia Desktop requires differentiating between internal bandwidth, which has its own cost considerations, and external bandwidth which is used when Scopia Desktop usage crosses site boundaries.

You should also consider whether the participants and webcast viewers are connecting from the internal or external network, to ensure there is sufficient internal and external bandwidth. For example, if your organization typically has 100 simultaneous participants connecting in SD, you require 38,400 kbps of bandwidth for uploading and 38,400 kbps for downloading. If 80 of these participants are connecting from the public network, you need to increase your organization's external bandwidth by an additional 30,720 kbps for both uploading and downloading media.

Upload and download bandwidths can comprise of the following components:

- Bandwidth consumed by videoconference participants connecting to the Scopia Desktop Server (Scopia Desktop Clients and Scopia Mobile devices)
- Bandwidth consumed by viewers of videoconference webcasts
- Bandwidth consumed by users downloading a recorded videoconference

Total bandwidth is calculated as follows:

```
Total Upload Bandwidth = Total upload bandwidth from participants

Total Download Bandwidth = Total download bandwidth from participants
                         + Total download bandwidth from webcast viewers
                         + Total download bandwidth from viewers replaying recordings
```

To calculate bandwidth required by participants and webcast viewers, see Calculating the Bandwidth Used by Scopia Desktop Participants on page 30. To calculate the bandwidth used to play back recordings, see Allocating Bandwidth for Downloading Recordings on page 36.

You can allocate the bandwidth depending on the specific needs of your organization. For example, if your organization has many participants connecting in standard definition and very few users downloading recordings, you may decide to increase the default rate for SD calls from 384 kbps, and decrease the bandwidth allocated for recordings.

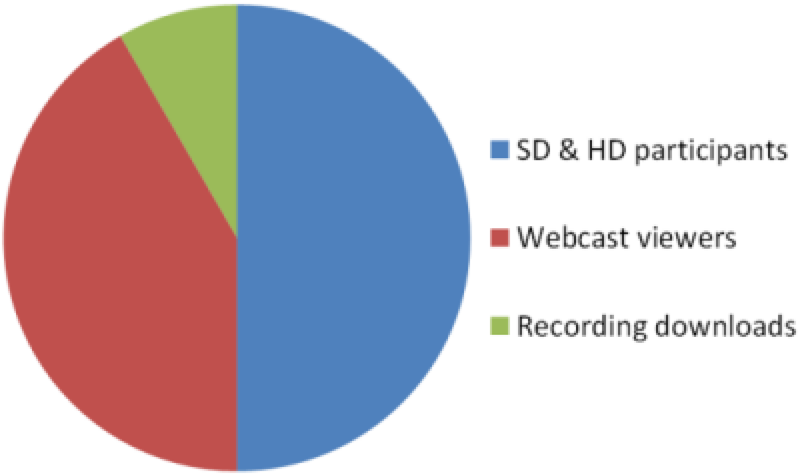


Figure 25: Total bandwidth for Scopia Desktop (example)

After calculating the total bandwidth, define your Scopia Desktop bandwidth settings as follows:

- Define the default call rates used by Scopia Desktop Clients, for standard and high definition (see Defining Bandwidth Settings in Scopia Desktop Server on page 79).
- Define the default call rates used to stream webcasts, for standard and high definition (see *Administrator Guide for Scopia Desktop Server*).
- Define the bandwidth used for downloading recordings (see *Administrator Guide for Scopia Desktop Server*).
- Define a default meeting type in your MCU with the correct bandwidth limit. For more information, see *Administrator Guide for Scopia Elite MCU*.

❗ Important:

The actual bandwidth consumed for a specific video resolution depends on the compression capabilities of your MCU. For example, Scopia Elite 6000 Series MCU includes H.264 High Profile encoding, therefore allowing a higher resolution at a lower bitrate than other MCUs. For more information, see Planning the Bandwidth for Scopia Desktop Clients Based on MCU Capacity on page 27.

The bandwidth used by each Scopia Desktop Client indirectly determines the capacity of your deployed MCUs. Your chosen video resolution (and bandwidth), places demands on your MCU to supply that video resolution for each connection, which determines how many users can simultaneously connect to the MCU. For more information, see Planning the Bandwidth for Scopia Desktop Clients Based on MCU Capacity on page 27.

Ports to Open on Scopia Desktop

The Scopia Desktop Server is typically located in the DMZ (see Figure 26: Locating the Scopia Desktop Server in the DMZ on page 39) and is therefore connected to both the enterprise and the public networks. Scopia Desktop Clients can be located in the internal enterprise network, in the public network, or in a partner network.

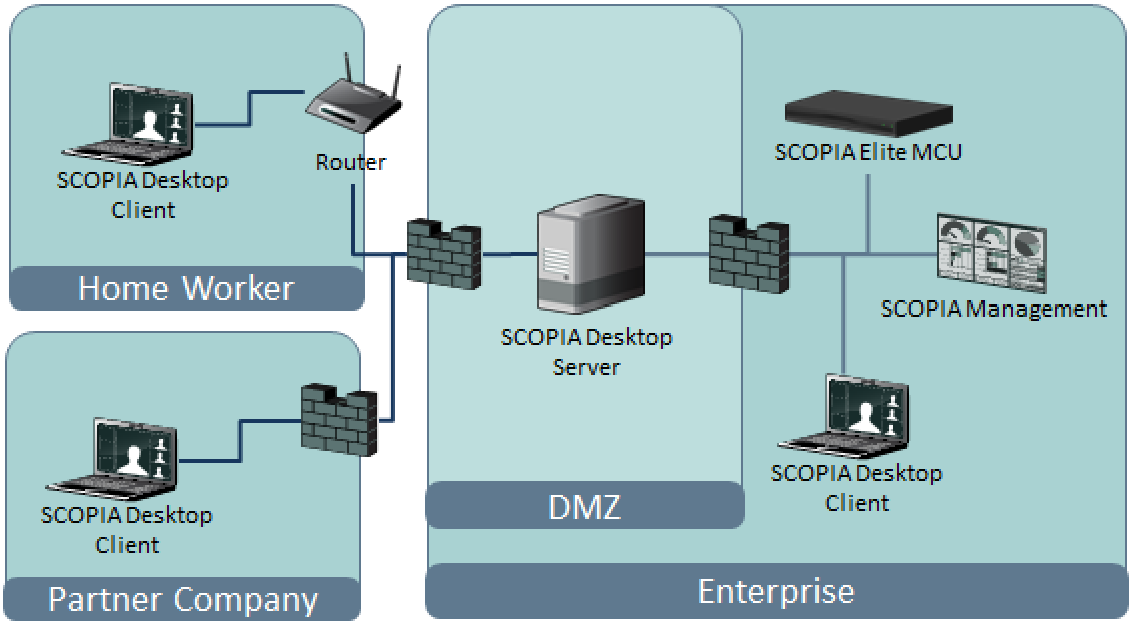


Figure 26: Locating the Scopia Desktop Server in the DMZ

When opening ports between the DMZ and the enterprise on the Scopia Desktop Server, use the following as a reference:

- When opening ports that are both in and out of the Scopia Desktop Server, see Table 7: Bidirectional Ports to Open Between the Scopia Desktop Server and the Enterprise on page 40.
- When opening ports that are outbound from the Scopia Desktop Server, see Table 8: Outbound Ports to Open from the Scopia Desktop Server to the Enterprise on page 40.
- When opening ports that are inbound to the Scopia Desktop Server, see Table 9: Inbound Ports to Open from the Enterprise to the Scopia Desktop Server on page 42.

When opening ports between the DMZ and the public on the Scopia Desktop Server, use the following as a reference:

- When opening ports that are both in and out of the Scopia Desktop Server, see Table 10: Bidirectional Ports to Open Between the Scopia Desktop Server and the Public on page 42.
- When opening ports that are inbound from the Scopia Desktop Server, see Table 11: Inbound Ports to Open from the Public to the Scopia Desktop Server on page 43.

When opening ports to and from the XMPP server (which is necessary when the XMPP server is separated by a firewall from the Scopia Desktop Server), use the following as a reference:

- When opening outbound ports from the XMPP server, see Table 12: Outbound Ports to Open from the XMPP Server on page 43.
- When opening inbound ports to the XMPP server, see Table 13: Inbound Ports to Open on the XMPP Server on page 44.

When opening bidirectional ports between Scopia Desktop Clients, see Table 14: Bidirectional Ports to Open Between Scopia Desktop Clients on page 44.

When opening inbound ports from the Scopia Desktop Clients to the STUN server, see Table 15: Inbound Ports to Open from the Scopia Desktop Client to the STUN Server on page 44.

Important:

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

Table 7: Bidirectional Ports to Open Between the Scopia Desktop Server and the Enterprise

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
7640	TCP	Content Center Server	Enables connection between the Scopia Desktop Server and the Content Center Server, when installed on different servers.	Cannot communicate with the Content Center Server and some capabilities (such as recording and streaming) do not function properly	Mandatory
1024- 65535	TCP (H.245/ Q.931)	MCU or ECS, depending on deployment	Enables connection to Scopia Desktop meetings.	Cannot connect to the meeting	Mandatory To limit range, see Limiting the TCP Port Range for H.245/Q.931 on the Scopia Desktop Server on page 46
10000-65535	UDP (RTP)	MCU or Scopia Desktop Client	Enables media connection to the MCU, and the Scopia Desktop Client or Scopia Mobile.	Media cannot be passed from the MCU to Scopia Desktop Clients. Also, connection is tunneled via TCP port 443 resulting in a drop in performance.	Mandatory To limit range, see Limiting the UDP Port Range for RTP/RTCP on the Scopia Desktop Server on page 45

Table 8: Outbound Ports to Open from the Scopia Desktop Server to the Enterprise

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
137,138	UDP	Active Directory	Enables auto-discovery and authentication	Cannot perform auto-discovery and authentication	Recommended for performing Active Directory authentication
139,445	TCP	Active Directory	Enables auto-discovery and authentication	Cannot perform auto-discovery and authentication	Recommended for Active Directory authentication

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
1719	UDP (RAS)	Scopia ECS Gatekeeper or the internal gatekeeper in Scopia Management	Enables communication with Scopia ECS Gatekeeper or the internal gatekeeper in Scopia Management	Cannot connect to the meeting	Mandatory
1720	TCP	MCU or ECS, depending on deployment	Enables connection to Scopia Desktop meetings.	Cannot connect to the meeting	Mandatory
3337	TCP (XML)	MCU	Enables meeting cascading connection to the MCU	Meeting cascading connection is disabled	Mandatory
5269	TCP	XMPP Server	Enables sever-to-server connections in cases where multiple Jabber servers are deployed as a federation or cluster.	Scopia Desktop Clients cannot login and use the contact list.	Mandatory only in deployments of two or more Jabber servers deployed as a federation or cluster which must communicate via a firewall
6972- 65535	UDP	Streaming Server	Enables media connection to the Scopia Desktop Streaming Server, if separated from Scopia Desktop Server by a firewall.	Cannot connect to the Scopia Desktop Streaming server.	Mandatory To avoid opening these ports, place the Scopia Desktop Server in the same zone as the streaming server.

Table 9: Inbound Ports to Open from the Enterprise to the Scopia Desktop Server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
80	TCP (HTTP)	Web client	Provides access to the Scopia Desktop Server Web Portal (you can configure port 443 instead)	Cannot access the Scopia Desktop Server Web Portal	Mandatory if using HTTP. You can configure this port during installation. For more information, see Installing Scopia Desktop on page 50.
443	TCP (TLS)	Scopia Desktop Clients and Scopia Mobile	Enables sending control messages between the Scopia Desktop Server and Clients, and is also used to tunnel RTP media if the UDP ports are blocked	Scopia Desktop Client or Scopia Mobile cannot connect to the Scopia Desktop Server	Mandatory
3340	TCP	Scopia Management	Enables meeting control connection with Scopia Management	Meeting control connection to Scopia Management is disabled	Mandatory
7070	TCP	Streaming Server	Enables Scopia Desktop Clients to send tunneled RTSP traffic	Scopia Desktop Clients cannot receive video streams	Mandatory To configure, see Configuring the TCP Streaming Port on the Scopia Desktop Server on page 47

Table 10: Bidirectional Ports to Open Between the Scopia Desktop Server and the Public

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
10000-65535	UDP (RTP/ RTCP)	Scopia Desktop Client or Scopia Mobile	Enables media connection with the Scopia Desktop Client or Scopia Mobile	Connection is tunneled via TCP port 443 and performance is not optimal	Recommended To configure, see Limiting the UDP Port Range for RTP/RTCP on the Scopia Desktop Server on page 45

Table 11: Inbound Ports to Open from the Public to the Scopia Desktop Server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
80	TCP (HTTP)	Web client	Provides access to the web user interface (you can configure port 443 instead)	Cannot access the web user interface	Mandatory if using HTTP. You can configure this port during installation. For more information, see Installing Scopia Desktop on page 50.
443	TCP (TLS)	Scopia Desktop Clients and Scopia Mobile	Enables sending control messages between the Scopia Desktop Server and Clients, and is also used to tunnel RTP media if the UDP ports are blocked	Scopia Desktop Clients cannot connect to the Scopia Desktop Server	Mandatory
7070	TCP	Streaming Server	Enables Scopia Desktop Clients to send tunneled RTSP traffic	Scopia Desktop Clients cannot receive video streams	Mandatory To configure, see Configuring the TCP Streaming Port on the Scopia Desktop Server on page 47.

Table 12: Outbound Ports to Open from the XMPP Server on page 43 and Table 13: Inbound Ports to Open on the XMPP Server on page 44 list the ports that should be opened on the XMPP Presence server, if the XMPP server is separated by a firewall from the Scopia Desktop Server.

Table 12: Outbound Ports to Open from the XMPP Server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
389	TCP (LDAP)	LDAP Server	Enables LDAP communication for user authentication, if the XMPP Server is configured for LDAP server (either Active Directory or Domino)	Users cannot login to the XMPP Server	Mandatory for LDAP authentication, if there is a firewall between XMPP and Scopia Desktop Server
3336	TCP (XML)	Scopia Management	Enables XML communication for user authentication, if the XMPP Server is configured for Scopia Management authentication	Users cannot login to the XMPP Server	Mandatory for Scopia Management authentication if there is a firewall between XMPP and Scopia Desktop Server

Table 13: Inbound Ports to Open on the XMPP Server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
5222	TCP	Scopia Desktop Client	Enables direct connection between Scopia Desktop Client and XMPP server	Scopia Desktop Client tries to use port 443 for tunnelled connection to the Scopia Desktop Server	Recommended if there is a firewall between XMPP and Scopia Desktop Server
5269	TCP	Scopia Desktop Client	Enables direct XMPP connections between Scopia Desktop Clients and the XMPP server	Scopia Desktop Clients need to proxy XMPP connections via Scopia Desktop Server	Recommended if there is a firewall between the XMPP server and Scopia Desktop Clients

Table 14: Bidirectional Ports to Open Between Scopia Desktop Clients

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
5060	UDP (SIP)	Scopia Desktop Client	Establishes direct SIP point-to-point connections between two Scopia Desktop Clients	Calls are routed via the Scopia Desktop Server	Recommended
1025-65535	UDP	Scopia Desktop Client	Establishes direct SIP point-to-point connections between two Scopia Desktop Clients	Calls are routed via the Scopia Desktop Server	Recommended

Table 15: Inbound Ports to Open from the Scopia Desktop Client to the STUN Server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3478	UDP	Scopia Desktop Clients	Enables connection between the STUN Server and Scopia Desktop Clients when making a point-to-point call. To connect point-to-point calls directly between two Scopia Desktop Clients, open the UDP ports (10000-65535, 6972-65535, 3478).	Scopia Desktop Client cannot connect to the STUN server and uses the Scopia Desktop Server as a relay agent.	Optional

❗ **Important:**

Some firewalls are configured to block packets from the streaming server. You can either configure the firewall to allow streaming packets, or reconfigure the streaming server and client to use different network protocols that cross the firewall boundary.

The Streaming Server uses the IETF RTSP/RTP protocols. RTSP runs over TCP, while RTP runs over UDP. The streaming server can tunnel RTSP/RTP traffic through standard HTTP. Some firewalls may inspect traffic on port 80 and not allow the tunneled RTSP/RTP on that port. We therefore recommend using the QuickTime standard port 7070 as the alternate TCP port for HTTP tunneling. This is configured in the streaming server by default as long as you specify the port as part of the streaming server virtual address, as described in Configuring the TCP Streaming Port on the Scopia Desktop Server on page 47.

Limiting Port Ranges on the Scopia Desktop Server

About this task

This section provides instructions of how to limit the following port ranges on the Scopia Desktop Server:

Navigation

- Limiting the UDP Port Range for RTP/RTCP on the Scopia Desktop Server on page 45
- Limiting the TCP Port Range for H.245/Q.931 on the Scopia Desktop Server on page 46
- Configuring the TCP Streaming Port on the Scopia Desktop Server on page 47

Limiting the UDP Port Range for RTP/RTCP on the Scopia Desktop Server

About this task

The Scopia Desktop Server has designated 10000-65535 as the default port range for UDP (RTP/RTCP). To provide additional security for your firewall, you can limit this range.

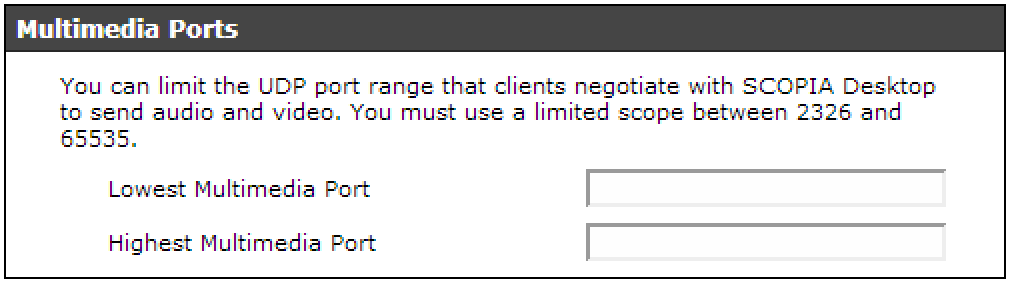
To calculate approximately how many ports the Scopia Desktop Server uses, multiply the number of license connections by 14, which amounts to reserving 14 ports per client.

In addition, add extra ports if your deployment includes:

- Add 6 ports per recording in your deployment.
- Add an extra 6 ports per conference which activates streaming.

Procedure

1. Log in to the Scopia Desktop Server Administrator web user interface.
2. Select **Client > Settings.**
3. Locate the **Multimedia Ports** section (see Figure 27: Multimedia Ports Area on page 46).



Multimedia Ports

You can limit the UDP port range that clients negotiate with SCOPIA Desktop to send audio and video. You must use a limited scope between 2326 and 65535.

Lowest Multimedia Port

Highest Multimedia Port

Figure 27: Multimedia Ports Area

4. Configure your port range (using any values between 2326 and 65535) by doing the following:

   a. Enter the base port value in the **Lowest Multimedia Port** field.

   b. Enter the upper port value in the **Highest Multimedia Port** field.

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

Limiting the TCP Port Range for H.245/Q.931 on the Scopia Desktop Server

About this task

The Scopia Desktop Server has designated ports 1024-65535 for TCP for H.245 and Q.931 signaling. To provide additional security for your firewall, you can limit this range.

For each conference, the Scopia Desktop Server uses 2 ports. In addition, add extra ports for:

- Add 2 ports for each participating Scopia Desktop Client client.
- Add 2 ports per conference when recording.
- Add 2 ports per conference when streaming.
- Add 1 port per conference when presenting using the content slider.

Procedure

1. Navigate to <*Scopia Desktop install_dir*>*ConfSrv*.

2. Edit the *config.val* file as follows:

   a. Locate the text `1 system`.

   b. At the bottom of that section, add two lines:

   ```
   2 portFrom = <lowest range limit>
   2 portTo = <highest range limit>
   ```

   Where `<lowest range limit>` is the base port of your port range and `<highest range limit>` is the upper value of your port range.

3. Access the Windows services and restart the **Scopia Desktop - Conference Server** service.

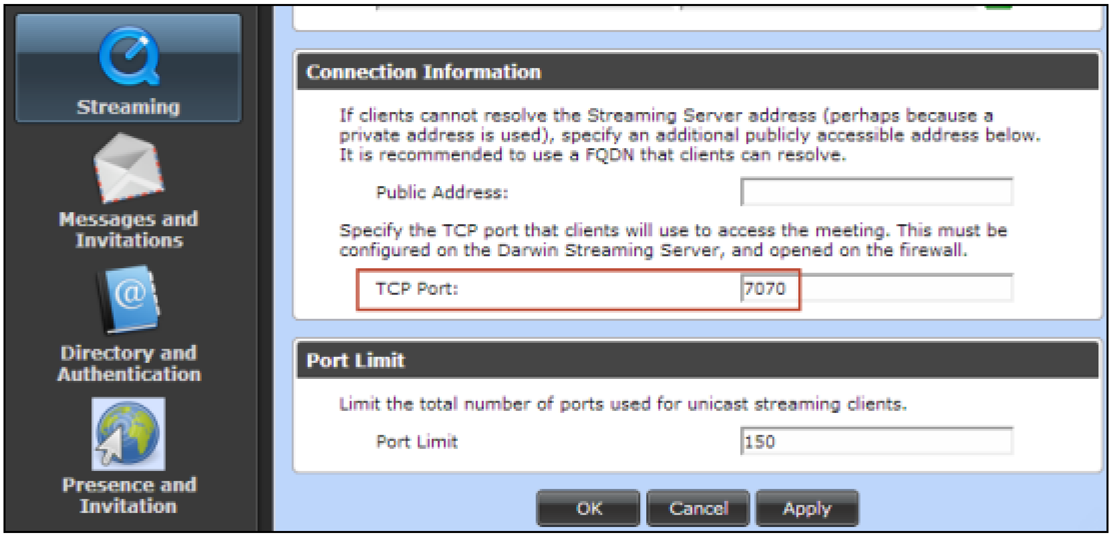
Configuring the TCP Streaming Port on the Scopia Desktop Server

About this task

The Streaming Server that is deployed with your Scopia Desktop Server is configured by default to use the QuickTime standard port 7070 as the alternate TCP port for HTTP tunneling. If your firewall is configured to block packets from the Streaming Server, you must reconfigure the Streaming Server and client to use different network protocols which can cross the firewall boundary.

Procedure

1. Log in to the Scopia Desktop Server Administrator web user interface.
2. Select **Streaming**. The **Settings** page for the Streaming Server appears (see Figure 28: Setting the streaming port for Scopia Desktop Server on page 47).



Connection Information

If clients cannot resolve the Streaming Server address (perhaps because a private address is used), specify an additional publicly accessible address below. It is recommended to use a FQDN that clients can resolve.

Public Address:

Specify the TCP port that clients will use to access the meeting. This must be configured on the Darwin Streaming Server, and opened on the firewall.

TCP Port: 7070

Port Limit

Limit the total number of ports used for unicast streaming clients.

Port Limit 150

Figure 28: Setting the streaming port for Scopia Desktop Server

3. Locate the **Connection Information** area.
4. Modify the port value in the **TCP Port** field.

   Important:

   The Streaming Server uses the IETF RTSP/RTP protocols. RTSP runs over TCP, while RTP runs over UDP. Many firewalls are configured to restrict TCP packets by port number and are very restrictive on UDP. The Streaming Server can tunnel RTSP/RTP traffic through standard HTTP. Some firewalls may inspect traffic on port 80 and not allow the tunneled RTSP/RTP on that port. We therefore recommend using the QuickTime standard port 7070 as the alternate TCP port for HTTP tunneling.

5. Select **OK** or **Apply**.
6. Do the following on the Scopia Desktop Server:

   a. Navigate to the following directory: C:\Program Files\Darwin Streaming Server.

b. Open the *streamingserver.xml* file.

c. Locate the list of ports for the RTSP protocol by finding the text `LIST-PREF NAME="rtsp_port"` in the file.

```
<CONFIGURATION>
  <SERVER>
    <LIST-PREF NAME="rtsp_port" TYPE="UInt16" >
      <VALUE> 7070 </VALUE>
    </LIST-PREF>
```

d. Within this section, add a new entry of `<VALUE> xxxx </VALUE>`, where `xxxx` is the new port value.

e. Save the file.

f. Restart the Darwin Streaming Server.

g. Restart the **Darwin Streaming Server** service.

Obtaining the Scopia Desktop License keys

You need license keys to install and operate the Scopia Desktop Server, the Recording Server, the Streaming Server, and Scopia Mobile device access. To obtain license keys, carefully read the instructions enclosed in the customer support letter you received when you purchased the product. Then navigate to http://licensing.radvision.com and enter the required information.

The recording key is required to activate Scopia Desktop Server recording and playback functionality, as well as enabling the Scopia Content Slider feature. You can choose to install the recording server without a license key. If so, the recording server is installed in demo mode, which limits recording to a one five-minute session at a time.

The streaming key is required to activate Scopia Desktop Server streaming functionality. You can choose to install the streaming server without a license key. If so, the streaming server is installed in demo mode and only allows up to 5 webcast watchers in a given call. If you are upgrading from an earlier release where you already had streaming installed, you are not prompted to enter the streaming key.

To use Scopia Mobile with full functionality, you must install Scopia Management and obtain a Scopia Mobile license as well.

Table 16: Features offered by Scopia Desktop and Scopia Desktop Pro Licenses on page 48 lists the features that Scopia Desktop and Scopia Desktop Pro licenses offer to customers.

Table 16: Features offered by Scopia Desktop and Scopia Desktop Pro Licenses

Feature	Scopia Desktop	Scopia Desktop Pro
Access to the portal/plug-in installation	Yes	Yes
Schedule a meeting from Microsoft Outlook	Yes	Yes
Attend a group meeting hosted on MCU	Yes	Yes
Share and annotate documents	Yes	Yes
Invite a phone or a room system by its number	Yes	Yes

Feature	Scopia Desktop	Scopia Desktop Pro
View a previously recorded meeting	Yes	Yes
View a webcast	Yes	Yes
Configure your virtual room from the Web Portal		Yes
Publish your presence to other meeting participants		Yes
Use the Contact List to call people		Yes
Desktop-to-desktop calling, seamless escalation to multi-party calls		Yes
Invite users or rooms from favorites, directory or by number		Yes

A guest user with no login can connect to existing meetings (unless Scopia Management is configured to restrict such feature) from Scopia Desktop Client or Scopia Mobile.

Chapter 3 | Installing Scopia Desktop

Since Scopia Desktop Server has several components, you can choose to install all the components on the same computer, or choose to have some installed on a dedicated server. Typical configurations are:

- All components on one computer (Scopia Desktop Server).
- Dedicated servers for different components, often split as follows:
  - Dedicated Conference Server for Scopia Desktop.
  - Dedicated Content Center for Scopia Desktop.
  - Dedicated Presence and Invitation Server for Scopia Desktop.

For more information on the reasons for choosing dedicated servers versus a single server, see Planning your Topology for Scopia Desktop Server on page 13.

This section also discusses how to distribute Scopia Desktop Clients throughout your organization and how to access the Scopia Desktop Server Administrator web interface.

Navigation

Installing All Scopia Desktop Components on a Single Server

About this task

Scopia Desktop Server includes various components (see About Components of the Scopia Desktop Server on page 6) which you can install on the same server for small deployments (see Topology for Small Scopia Desktop Server Deployment on page 13).

For medium and large size deployments where you need power devoted to each component of the server, you can deploy a dedicated server devoted just one component of the Scopia Desktop Server, or you can choose a set of components on the same computer (see Planning your Topology for Scopia Desktop Server on page 13).

Follow these recommendations when installing the Scopia Desktop Server components:

- Do not install the Scopia Desktop Client on the same PC as any Scopia Desktop component.
- If you want to encrypt communication with HTTPS, configure the Conference Server for Scopia Desktop to port 443 after the installation is completed (see Securing Web Connections and Media Traffic to Scopia Desktop Server on page 97).

❗ **Important:**

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

Follow this procedure to install the Scopia Desktop components.

Before you begin

- Before installing, verify the computer meets the minimum hardware requirements for the number of intended users. For more information, see Minimum Requirements and Specifications of Scopia Desktop Server on page 9.
- Make sure you have enough space on the local hard drive to install all Scopia Desktop components as they require 117MB.

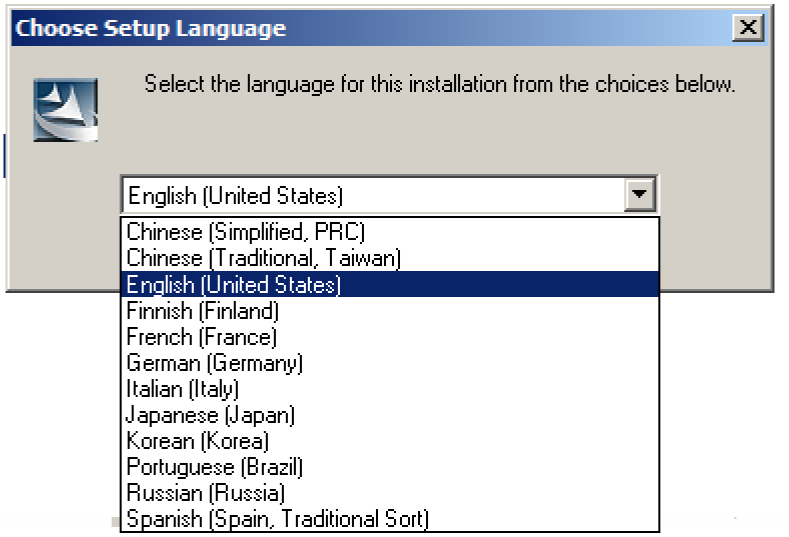
  If you want to store recordings locally, a typical recording for a one-hour meeting at 384 kbps takes up to 200MB. Alternatively, you can use a storage server in the enterprise. For more information, see Allocating Bandwidth for Downloading Recordings on page 36.
- Ensure you have the correct license information (see Obtaining the Scopia Desktop License keys on page 48).

  ❗ **Important:**

  To use point-to-point functionality, you must install Scopia Management with the Scopia Desktop Pro license.
- The Scopia Desktop Streaming Server uses port 7070 by default for communicating with Scopia Desktop Clients. If you select a different port, change the default port value as explained in *Administration Guide for Scopia Desktop*.
- By default, Scopia Desktop Clients access the Scopia Desktop Server via port 80. If other applications on this PC use port 80, and you nevertheless want to use this port, access the Services panel in Windows and disable the IIS Administration, HTTP SSL, and World Wide Web Publishing services before installing the Conference Server.

Procedure

1. Launch the *setup.exe* file to start the Scopia Desktop Setup Wizard.
2. Select the installation language in the **Choose Setup Language** window, and select **OK**.



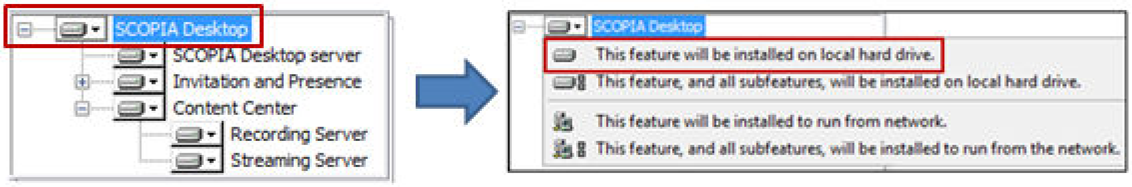
Choose Setup Language

Select the language for this installation from the choices below.

Figure 29: Choosing language for the installation

3. Select **Next** and accept the license agreement.

4. In the **Custom Setup** window select the **Scopia Desktop** icon. Always use the default option (**This feature will be installed on the local hard drive**).



SCOPIA Desktop
SCOPIA Desktop server
Invitation and Presence
Content Center
Recording Server
Streaming Server
SCOPIA Desktop
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will be installed to run from network.
This feature, and all subfeatures, will be installed to run from the network.

Figure 30: Installing all the Scopia Desktop components on the dedicated server

5. Change the installation folder if required, and select **Next**.

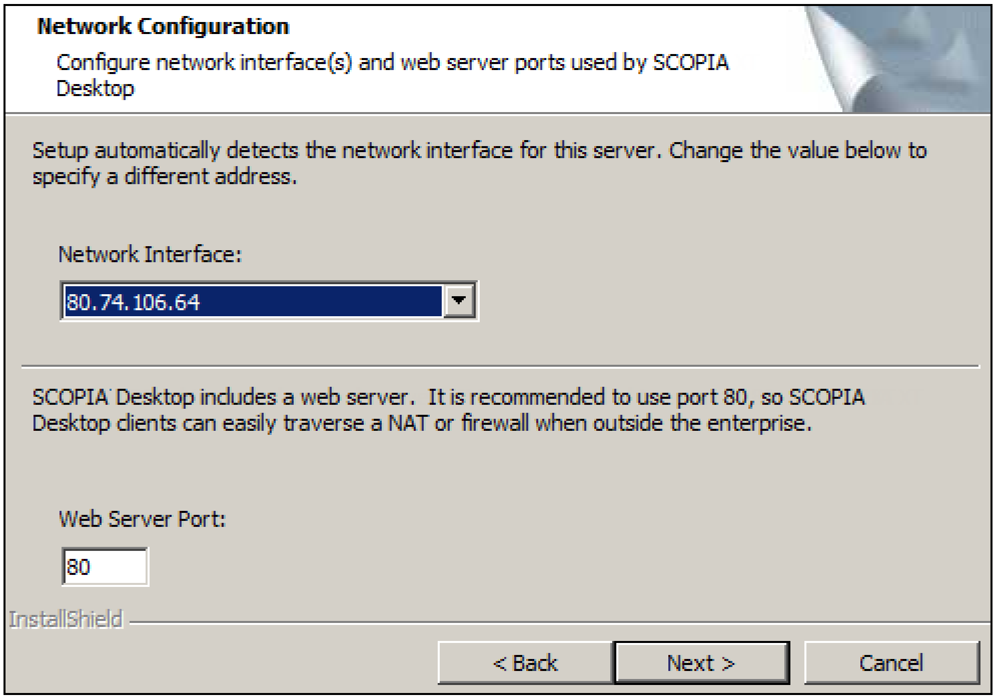
6. In the **License Key** window enter the Scopia Desktop, Streaming, and Recording license keys and select **Next**.

   ❗ **Important:**

   If you do not enter the streaming and/or recording license key, the corresponding server is installed in demo mode which limits recordings to 5 minutes and only allows up to 5 webcast viewers in a videoconference.

7. In the **Network Configuration** window, select the IP address used for communicating with the MCU.

   If the server has one NIC card, the **Network Interface** field has only one value to choose, the IP of the NIC. For dual-NIC servers, select the network IP address pointing to the internal firewall. For more information on dual-NIC setups, see Deploying Scopia Desktop Server with Dual-NIC on page 25



Network Configuration

Configure network interface(s) and web server ports used by SCOPIA Desktop

Setup automatically detects the network interface for this server. Change the value below to specify a different address.

Network Interface: 80.74.106.64

SCOPIA Desktop includes a web server. It is recommended to use port 80, so SCOPIA Desktop clients can easily traverse a NAT or firewall when outside the enterprise.

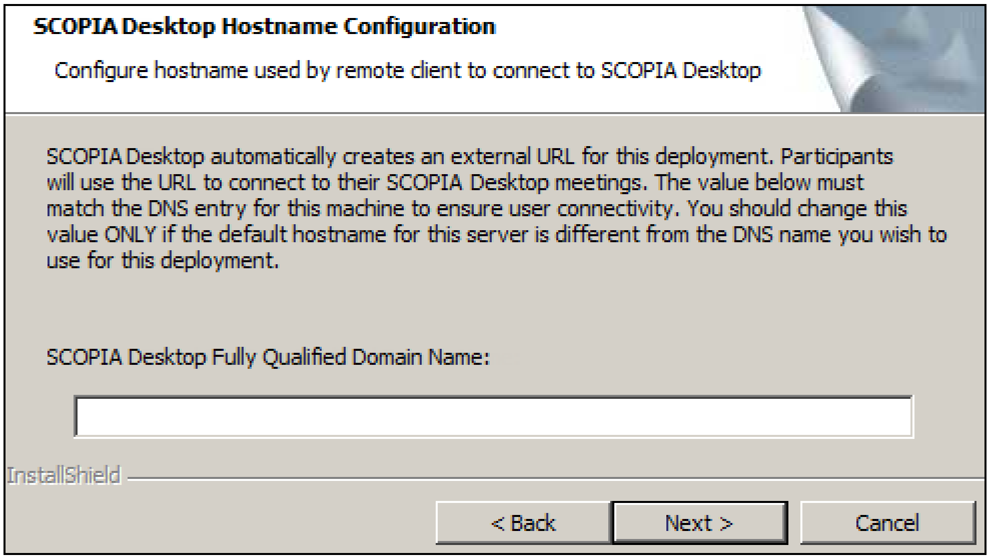
Web Server Port: 80

Figure 31: Selecting the NIC pointing to the internal network

8. Change the default web server port if required, and then select **Next**.

   For more information on port changes, see Ports to Open on Scopia Desktop on page 38

9. In the **Hostname Configuration** window specify the public name of the Scopia Desktop Server, to be used later as part of the URL sent to Scopia Desktop Clients to connect to videoconferences.



SCOPIA Desktop Hostname Configuration

Configure hostname used by remote client to connect to SCOPIA Desktop

SCOPIA Desktop automatically creates an external URL for this deployment. Participants will use the URL to connect to their SCOPIA Desktop meetings. The value below must match the DNS entry for this machine to ensure user connectivity. You should change this value ONLY if the default hostname for this server is different from the DNS name you wish to use for this deployment.

SCOPIA Desktop Fully Qualified Domain Name:

Figure 32: Defining the public address of the Scopia Desktop Server

Important:

An external Scopia Desktop Client must be able to resolve the server's hostname to the correct IP address from its location outside the enterprise. For example, do not use an internal DNS name if you have clients connecting from the public Internet.

10. In the **Recording Configuration** window, select the storage location for recorded meetings and specify the maximum amount (in MB) of disk space needed for storing recorded meetings. One hour of Scopia Desktop recording (384kbps) is 200MB.

    Use the following formula to calculate the space required for recordings:

    ```
    Recording Bandwidth (in megabytes) × Time (in seconds) + 20%
    Overhead
    ```

    For example, for a call of 1 hour at 384 kbps (standard definition), calculate as follows:

    ```
    384 kbps × (60 minutes × 60 seconds) = 1382400 kilobits
    1382400 ÷ 1024 = 1350 megabits
    1350 ÷ 8 = 168.75 megabytes (MB)
    168.75 × 20% = 33.75MB (overhead)
    Total is 168.75 + 33.75 = 202.5MB (including overhead)
    ```

    Important:

    You can enter a local pathname or a pathname of any storage server visible in the enterprise.

    Then select **Next**.

11. Select **Install** in the **Ready to Install the Program** window.

12. Select **Finish**.

13. To change the Content Center settings, run the Setup Wizard again and navigate to the relevant window.

Installing the Conference Server for Scopia Desktop on a Dedicated Server

About this task

This section details how to install a dedicated Conference Server for Scopia Desktop on a separate PC from the other server components (see About Components of the Scopia Desktop Server on page 6).

For medium and large size deployments where you need power devoted to each component of the server, you can deploy a dedicated server devoted just one component of the Scopia Desktop Server, or you can choose a set of components on the same computer (see Planning your Topology for Scopia Desktop Server on page 13).

Follow these recommendations when installing the Scopia Desktop Server components:

- Do not install the Scopia Desktop Client on the same PC as any Scopia Desktop component.
- If you want to encrypt communication with HTTPS, configure the Conference Server for Scopia Desktop to port 443 after the installation is completed (see Securing Web Connections and Media Traffic to Scopia Desktop Server on page 97).

  Important:

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

Before you begin

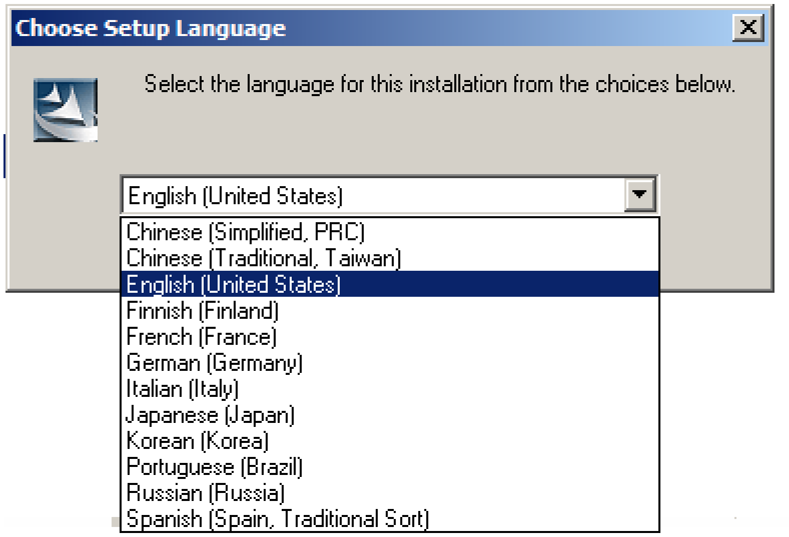
- Before installing, verify the computer meets the minimum hardware requirements for the number of intended users. For more information, see Minimum Requirements and Specifications of Scopia Desktop Server on page 9.
- Make sure you have enough space on the local hard drive to install the Scopia Desktop Server component as it requires 222MB.
- Ensure you have the correct license information (see Obtaining the Scopia Desktop License keys on page 48).

  Important:

  To use point-to-point functionality, you must install Scopia Management with the Scopia Desktop Pro license.
- By default, Scopia Desktop Clients access the Scopia Desktop Server via port 80. If other applications on this PC use port 80, and you nevertheless want to use this port, access the Services panel in Windows and disable the IIS Administration, HTTP SSL, and World Wide Web Publishing services before installing the Conference Server.

Procedure

1. Launch the *setup.exe* file to start the Scopia Desktop Setup Wizard.
2. Select the installation language in the **Choose Setup Language** window, and select **OK**.



Choose Setup Language

Select the language for this installation from the choices below.

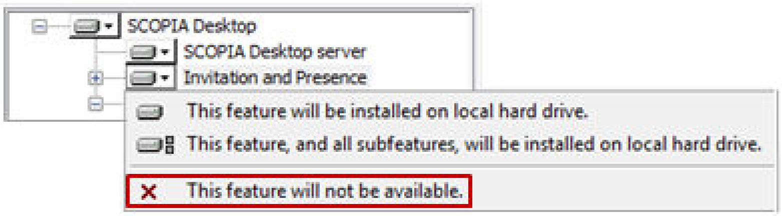
English (United States)

Chinese (Simplified, PRC)
Chinese (Traditional, Taiwan)
English (United States)
Finnish (Finland)
French (France)
German (Germany)
Italian (Italy)
Japanese (Japan)
Korean (Korea)
Portuguese (Brazil)
Russian (Russia)
Spanish (Spain, Traditional Sort)

Figure 33: Choosing language for the installation

3. Select **Next** and accept the license agreement.

4. In the **Custom Setup** window disable the **Invitation and Presence** by selecting **> This feature will not be available** (Figure 34: Installing the Scopia Desktop component on the dedicated server on page 56). Repeat for the **Content Center**.



SCOPIA Desktop
SCOPIA Desktop server
Invitation and Presence

This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
✕ This feature will not be available.

Figure 34: Installing the Scopia Desktop component on the dedicated server

5. Ensure that **Scopia Desktop Server**, which is the option for the Conference Server, remains selected for local installation.

   Important:

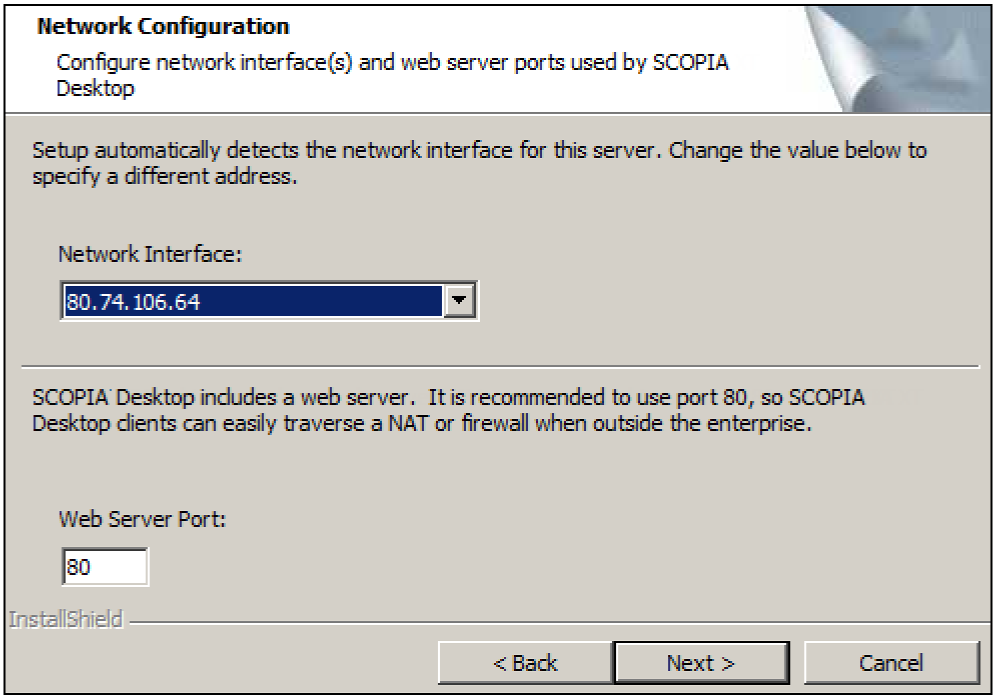
   When installing a component, always use the default option (**This feature will be installed on the local hard drive**).

6. Change the installation folder if required, and select **Next**.

7. In the **License Key** window enter the Scopia Desktop license key and select **Next**.

8. In the **Network Configuration** window, select the IP address used for communicating with the MCU.

   If the server has one NIC card, the **Network Interface** field has only one value to choose, the IP of the NIC. For dual-NIC servers, select the network IP address pointing to the internal firewall. For more information on dual-NIC setups, see Deploying Scopia Desktop Server with Dual-NIC on page 25



Network Configuration

Configure network interface(s) and web server ports used by SCOPIA Desktop

Setup automatically detects the network interface for this server. Change the value below to specify a different address.

Network Interface: 80.74.106.64

SCOPIA Desktop includes a web server. It is recommended to use port 80, so SCOPIA Desktop clients can easily traverse a NAT or firewall when outside the enterprise.

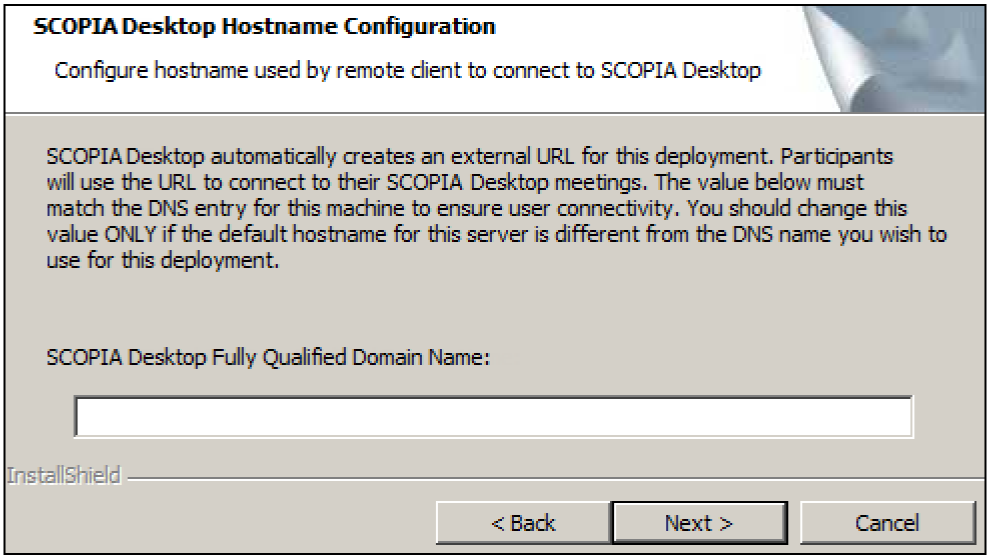
Web Server Port: 80

Figure 35: Selecting the NIC pointing to the internal network

9. Change the default web server port if required, and then select **Next**.

   For more information on port changes, see Ports to Open on Scopia Desktop on page 38

10. In the **Hostname Configuration** window specify the public name of the Scopia Desktop Server, to be used later as part of the URL sent to Scopia Desktop Clients to connect to videoconferences.



SCOPIA Desktop Hostname Configuration

Configure hostname used by remote client to connect to SCOPIA Desktop

SCOPIA Desktop automatically creates an external URL for this deployment. Participants will use the URL to connect to their SCOPIA Desktop meetings. The value below must match the DNS entry for this machine to ensure user connectivity. You should change this value ONLY if the default hostname for this server is different from the DNS name you wish to use for this deployment.

SCOPIA Desktop Fully Qualified Domain Name:

Figure 36: Defining the public address of the Scopia Desktop Server

Important:

An external Scopia Desktop Client must be able to resolve the server's hostname to the correct IP address from its location outside the enterprise. For example, do not use an internal DNS name if you have clients connecting from the public Internet.

11. Select **Install** in the **Ready to Install the Program** window.
12. Select **Finish**.

Installing the Content Center for Scopia Desktop on a Dedicated Server

About this task

This section details how to install a dedicated Content Center Server for Scopia Desktop on a separate PC from the other server components (see About Components of the Scopia Desktop Server on page 6). The Content Center Server includes the recording, streaming and content slider components.

For medium and large size deployments where you need power devoted to each component of the server, you can deploy a dedicated server devoted just one component of the Scopia Desktop Server, or you can choose a set of components on the same computer (see Planning your Topology for Scopia Desktop Server on page 13).

Follow these recommendations when installing the Scopia Desktop Server components:

- Do not install the Scopia Desktop Client on the same PC as any Scopia Desktop component.
- If you want to encrypt communication with HTTPS, configure the Conference Server for Scopia Desktop to port 443 after the installation is completed (see Securing Web Connections and Media Traffic to Scopia Desktop Server on page 97).

Important:

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

Before you begin

- Before installing, verify the computer meets the minimum hardware requirements for the number of intended users. For more information, see Minimum Requirements and Specifications of Scopia Desktop Server on page 9.
- Make sure you have enough space on the hard drive to install the component. The Streaming Server and the Recording Server require 26MB on the hard drive.

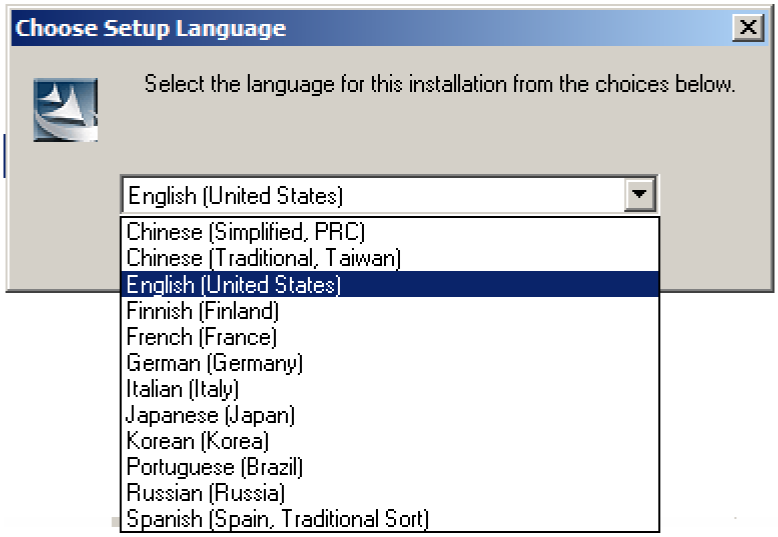
  If you want to store recordings locally, a typical recording for a one-hour meeting at 384 kbps takes up to 200MB. Alternatively, you can use a storage server in the enterprise. For more information, see Allocating Bandwidth for Downloading Recordings on page 36.
- Ensure you have the correct license information (see Obtaining the Scopia Desktop License keys on page 48).

  Important:

  When installing all components of the Content Center, you do not need a Scopia Desktop license key.
- The Scopia Desktop Streaming Server uses port 7070 by default for communicating with Scopia Desktop Clients. If you select a different port, change the default port value as explained in *Administration Guide for Scopia Desktop*.

Procedure

1. Launch the *setup.exe* file to start the Scopia Desktop Setup Wizard.
2. Select the installation language in the **Choose Setup Language** window, and select **OK**.



Choose Setup Language

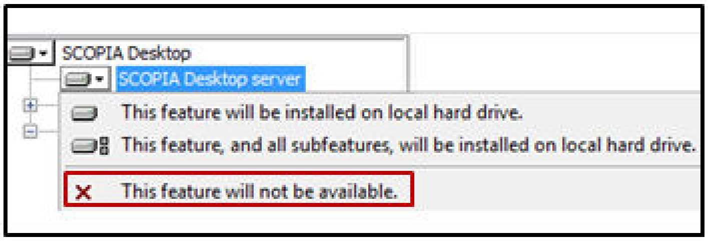
Select the language for this installation from the choices below.

English (United States)

Figure 37: Choosing language for the installation

3. Select **Next** and accept the license agreement.

4. In the **Custom Setup** window disable the **Scopia Desktop Server** by selecting ▭ **> This feature will not be available**. Repeat for the **Invitation and Presence**.



SCOPIA Desktop

SCOPIA Desktop server

This feature will be installed on local hard drive.

This feature, and all subfeatures, will be installed on local hard drive.

This feature will not be available.

Figure 38: Disabling a Scopia Desktop component on a dedicated server

5. Ensure the **Content Center** item remains selected to be installed.

   Important:

   When installing a component, always use the default option (**This feature will be installed on the local hard drive**).

6. Change the installation folder if required, and select **Next**.

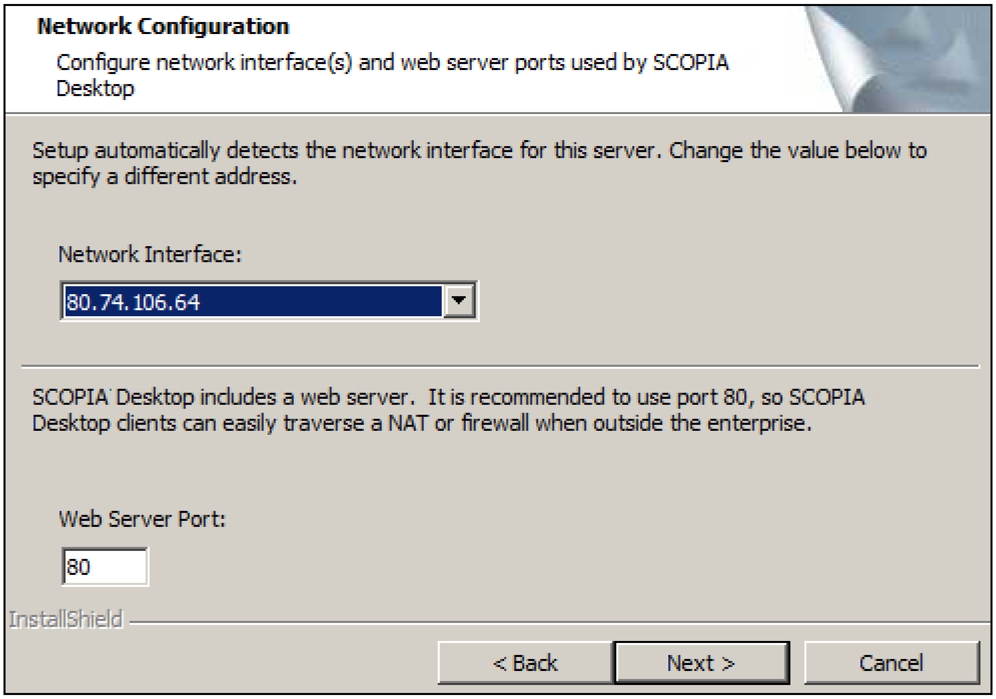
7. In the **License Key** window enter the relevant license key and select **Next**.

   Important:

   If you do not enter the Content Center license keys, the system installs the server in demo mode which limits recordings to 5 minutes and only allows up to 5 webcast viewers in a videoconference.

8. In the **Network Configuration** window, select the IP address used for communicating with the MCU.

   If the server has one NIC card, the **Network Interface** field has only one value to choose, the IP of the NIC. For dual-NIC servers, select the network IP address pointing to the internal firewall. For more information on dual-NIC setups, see Deploying Scopia Desktop Server with Dual-NIC on page 25



Network Configuration

Configure network interface(s) and web server ports used by SCOPIA Desktop

Setup automatically detects the network interface for this server. Change the value below to specify a different address.

Network Interface: 80.74.106.64

SCOPIA Desktop includes a web server. It is recommended to use port 80, so SCOPIA Desktop clients can easily traverse a NAT or firewall when outside the enterprise.

Web Server Port: 80

Figure 39: Selecting the NIC pointing to the internal network

9. In the **Recording Configuration** window, select the storage location for recorded meetings and specify the maximum amount (in MB) of disk space needed for storing recorded meetings. One hour of Scopia Desktop recording (384kbps) is 200MB.

   Use the following formula to calculate the space required for recordings:

   ```
   Recording Bandwidth (in megabytes) × Time (in seconds) + 20%
   Overhead
   ```

   For example, for a call of 1 hour at 384 kbps (standard definition), calculate as follows:

   ```
   384 kbps × (60 minutes × 60 seconds) = 1382400 kilobits
   1382400 ÷ 1024 = 1350 megabits
   1350 ÷ 8 = 168.75 megabytes (MB)
   168.75 × 20% = 33.75MB (overhead)
   Total is 168.75 + 33.75 = 202.5MB (including overhead)
   ```

   Important:

   You can enter a local pathname or a pathname of any storage server visible in the enterprise.

   Then select **Next**.

10. Enter the IP address (or FQDN) of the Scopia Desktop Server which must communicate with this server and select **Next**.

11. Select **Install** in the **Ready to Install the Program** window.

12. Select **Finish**.

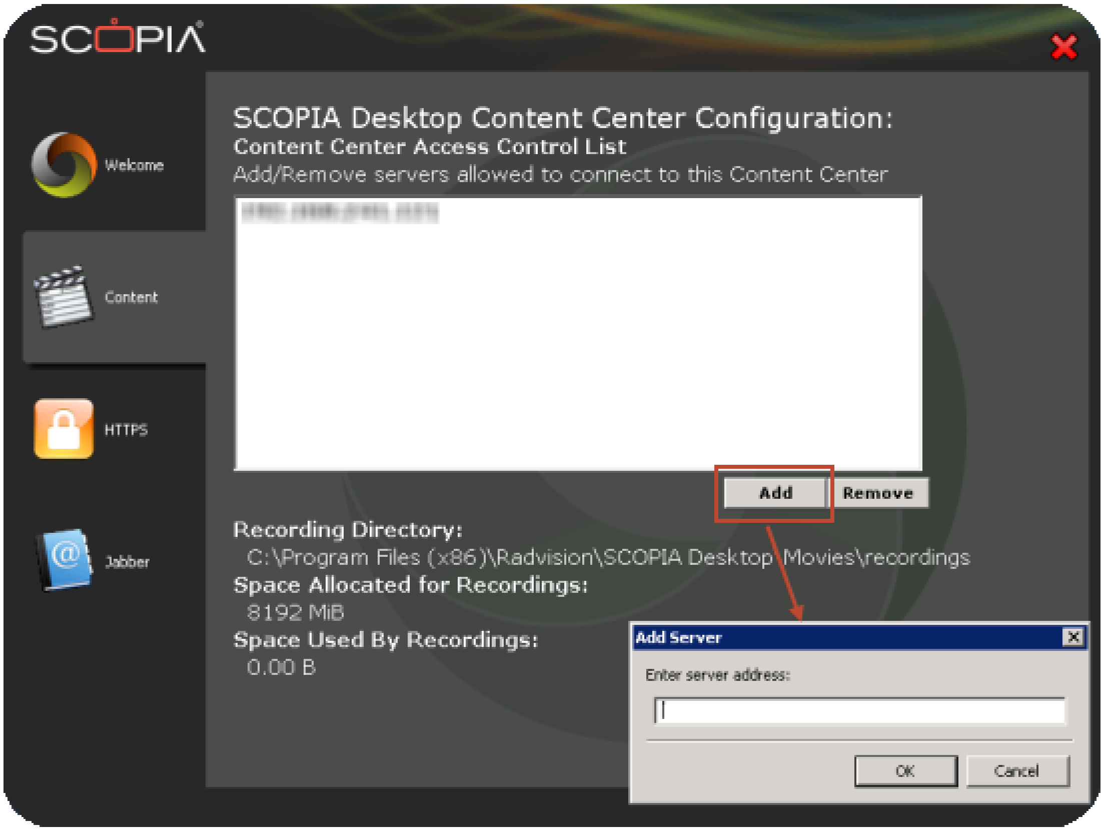
13. To change the Content Center settings, run the Setup Wizard again and navigate to the relevant window.

14. For any Scopia Desktop Server accessing a dedicated Content Center Server (recording or streaming), enter each Scopia Desktop Server IP address in the access control list using the Scopia Desktop Server Configuration Tool.

   a. On the dedicated Content Server for Scopia Desktop, select **Start > Programs > Scopia Desktop > ConfigTool**.

   b. Select **Content** in the sidebar.

   The system lists the IP addresses of the Scopia Desktop Servers allowed to access this Dedicated Content Server, as shown below.



SCOPIA Desktop Content Center Configuration:
Content Center Access Control List
Add/Remove servers allowed to connect to this Content Center

[redacted]

Recording Directory:
C:\Program Files (x86)\Radvision\SCOPIA Desktop\Movies\recordings
Space Allocated for Recordings:
8192 MiB
Space Used By Recordings:
0.00 B

Add Server
Enter server address:

Figure 40: Enabling multiple Scopia Desktop Servers to access a Dedicated Content Server

   c. Select **Add** to add the IP address of each Scopia Desktop Server using this Content Server.

   d. Select **OK**.

Installing the Invitation and Presence Server for Scopia Desktop on a Dedicated Server

About this task

This section details how to install a dedicated Invitation and Presence Server for Scopia Desktop on a separate PC from the other server components (see About Components of the Scopia Desktop Server on page 6). The Invitation and Presence Server includes the XMPP (Jabber) server which updates a user's status in the contact list, and a STUN server which allows you to directly dial a Scopia Desktop Client which is located behind a firewall.

Scopia Desktop Server includes various components (see About Components of the Scopia Desktop Server on page 6) which you can install on the same server for small deployments (see Topology for Small Scopia Desktop Server Deployment on page 13).

For medium and large size deployments where you need power devoted to each component of the server, you can deploy a dedicated server devoted just one component of the Scopia Desktop Server, or you can choose a set of components on the same computer (see Planning your Topology for Scopia Desktop Server on page 13).

Follow these recommendations when installing the Scopia Desktop Server components:

- Do not install the Scopia Desktop Client on the same PC as any Scopia Desktop component.
- If you want to encrypt communication with HTTPS, configure the Conference Server for Scopia Desktop to port 443 after the installation is completed (see Securing Web Connections and Media Traffic to Scopia Desktop Server on page 97).

Important:

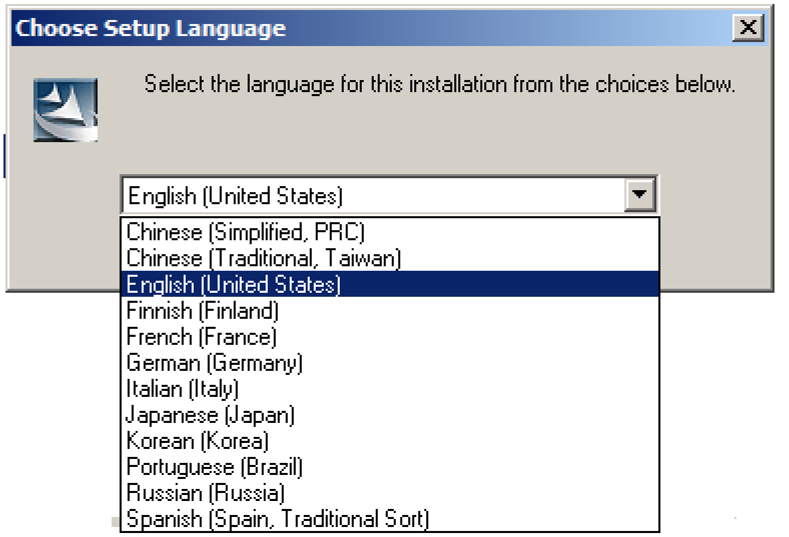
Using encryption is subject to local regulation. In some countries it is restricted or limited for usage. For more information, consult your local reseller.

Before you begin

- Before installing, verify the computer meets the minimum hardware requirements for the number of intended users. For more information, see Minimum Requirements and Specifications of Scopia Desktop Server on page 9.
- Make sure you have enough space on the hard drive to install the component. The invitation and Presence Server require 26MB on the hard drive.
- To use point-to-point functionality, you must install Scopia Management with the Scopia Desktop Pro license.

Procedure

1. Launch the *setup.exe* file to start the Scopia Desktop Setup Wizard.
2. Select the installation language in the **Choose Setup Language** window, and select **OK**.



Choose Setup Language

Select the language for this installation from the choices below.

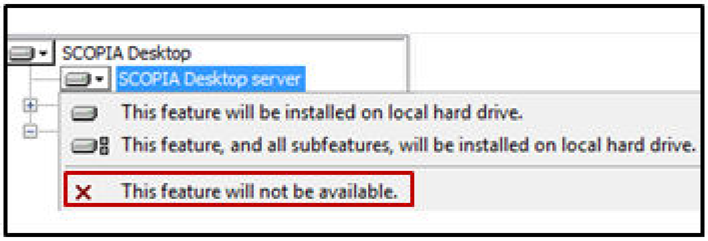
English (United States)

- Chinese (Simplified, PRC)
- Chinese (Traditional, Taiwan)
- English (United States)
- Finnish (Finland)
- French (France)
- German (Germany)
- Italian (Italy)
- Japanese (Japan)
- Korean (Korea)
- Portuguese (Brazil)
- Russian (Russia)
- Spanish (Spain, Traditional Sort)

Figure 41: Choosing language for the installation

3. Select **Next** and accept the license agreement.

4. In the **Custom Setup** window disable the **Scopia Desktop Server** by selecting 🖴 **> This feature will not be available**. Repeat for the **Content Center** and select **Next**.



SCOPIA Desktop

SCOPIA Desktop server

- This feature will be installed on local hard drive.
- This feature, and all subfeatures, will be installed on local hard drive.
- ✗ This feature will not be available.

Figure 42: Disabling a Scopia Desktop component on a dedicated server

5. Ensure the **Invitation and Presence** component is selected for local installation.

   Important:

   When installing a component, always use the default option (**This feature will be installed on the local hard drive**).

6. Change the installation folder if required, and select **Next**.

7. Select **Install** in the **Ready to Install the Program** window.

8. Select **Finish**.

Centrally Deploying Scopia Desktop Clients in your Organization

About this task

You can push Scopia Desktop Clients simultaneously to end users using one of these standard Microsoft server tools:

- Microsoft Active Directory (AD)
- Microsoft Systems Management Server (SMS).

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

Chapter 4 | Configuring Your Deployment

After completing the Scopia Desktop Server installation, you must login to the Scopia Desktop Administration from your browser and complete the Configuration Wizard before the system is usable. The configuration wizard is automatically activated when you first access the Scopia Desktop Administration interface.

This section describes how to access the Scopia Desktop Administration web interface, configure your deployment, define a local administrator account, and verify that the Scopia Solution components are successfully connected.

Important:

If you intend to configure streaming videoconferences, before configuring Scopia Desktop, you should:

- Ensure streaming multicasts are enabled on the deployment routers and firewalls.
- Obtain the internal IP address range of accessible Scopia Desktop Clients to define clients that will be able to watch streamed meetings.

Navigation

Accessing the Scopia Desktop Server Web Administration Interface

About this task

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

Perform this procedure to access the administration web interface.

Important:

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

Procedure

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

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

2. Enter your username and password.

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

3. Select **Sign In**.

Defining a Local Administrator Account

About this task

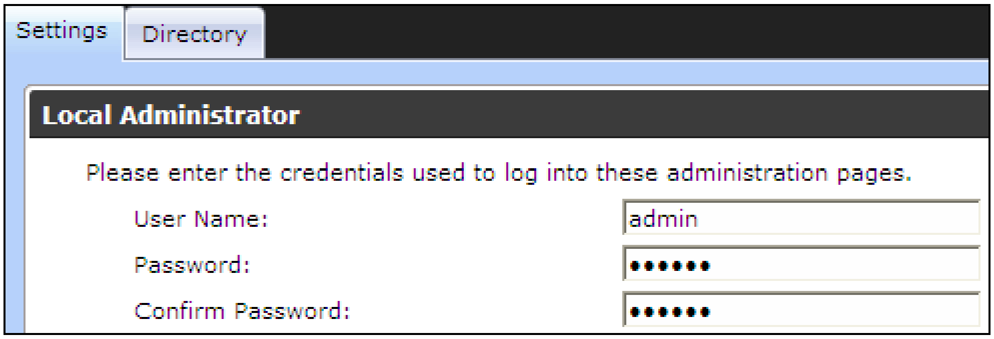
You can define a username and password for a local administrator to access Scopia Desktop Server Administration web interface. The local administrator cannot sign into the Scopia Desktop user portal using credentials defined during this procedure.

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

Procedure

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

   The **Settings** tab is displayed.



Local Administrator

Please enter the credentials used to log into these administration pages.

User Name: admin

Password: ••••••

Confirm Password: ••••••

Figure 43: Configuring the local administrator credentials

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

Connecting Scopia Desktop Server with Video Network Devices

About this task

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

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

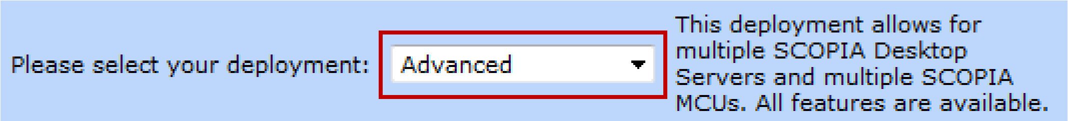
This window is also displayed when you access the Scopia Desktop Server for the first time.

Ensure that Scopia Desktop Server has Scopia Management's IP address, and conversely Scopia Management has Scopia Desktop Server's IP address. For more information on how to add Scopia Desktop Server's IP address to Scopia Management, see Adding and Modifying Scopia Desktop Server in Scopia Management on page 73.

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

Procedure

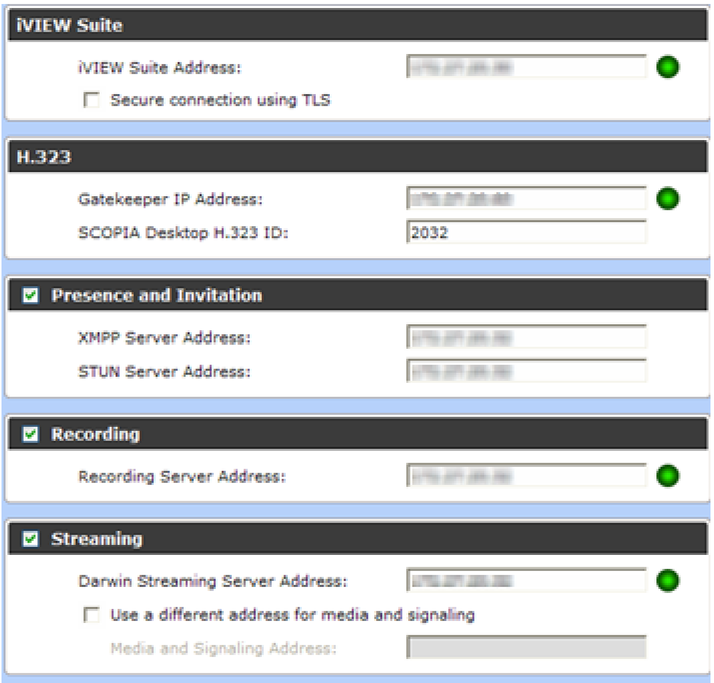
1. Access the Scopia Desktop Server administration web interface.
2. Select **Deployment** in the sidebar.
3. Select **Advanced** if your network includes Scopia Management (Figure 44: Determining whether to include Scopia Management in deployment on page 69).



Please select your deployment: Advanced ▾

This deployment allows for multiple SCOPIA Desktop Servers and multiple SCOPIA MCUs. All features are available.

Figure 44: Determining whether to include Scopia Management in deployment



iVIEW Suite

iVIEW Suite Address: [redacted] ●

□ Secure connection using TLS

H.323

Gatekeeper IP Address: [redacted] ●

SCOPIA Desktop H.323 ID: 2032

☑ **Presence and Invitation**

XMPP Server Address: [redacted]

STUN Server Address: [redacted]

☑ **Recording**

Recording Server Address: [redacted] ●

☑ **Streaming**

Darwin Streaming Server Address: [redacted] ●

□ Use a different address for media and signaling

Media and Signaling Address:

Figure 45: Connections to other servers including Scopia Management

4. Enter the fields as described in Table 17: Defining addresses of other servers in the network on page 70.

Table 17: Defining addresses of other servers in the network

Field	Description
iVIEW Suite Address	Enter the IP address of Scopia Management, for integrated user management, bandwidth policies, and stronger integration with the full range of Scopia Solution features. By default, Scopia Management uses port 8080.
Secure connection using TLS	Select this check box to encrypt communications between Scopia Desktop Server and Scopia Management. This functionality requires installing certificates signed by a recognized CA on both Scopia Management and Scopia Desktop Server. For more information on installing Scopia Management certificates, see *Administrator Guide for Scopia Management*. For more information on installing certificates on Scopia Desktop Server, see Securing Scopia Desktop Server's Connection to other Components on page 99. ❗ **Important:** Using encryption is subject to local regulation. In some countries it is restricted or limited for usage. For more information, consult your local reseller.
Gatekeeper IP Address	Enter the address of the gatekeeper. If you are using Scopia Management's built-in gatekeeper, enter the IP address of Scopia Management.
Scopia Desktop H.323 ID	Enter the name (H.323 alias) which Scopia Management uses to identify this Scopia Desktop Server's clients, and then route them to the appropriate MCU. This can have any of the following formats: • H.323 alias. For example, `username`. • IP address of an H.323 endpoint. For example, 123.45.678.9. • URI dialing for H.323 or SIP endpoints. For example, user@company.com • E.164 dialing for H.323 or SIP endpoints. For example, 881234.
Presence and Invitation	Select this check box if your deployment includes a presence and STUN server, used to maintain the contact list and point-to-point functionality of Scopia Desktop Pro.
XMPP Server Address	Enter the IP address of the presence server, used to maintain the presence information of the contact list in Scopia Desktop Pro.
STUN Server Address	Enter the IP address of the STUN server, used to ensure a point-to-point call can be made from a remote Scopia Desktop Client to one inside the organization, finding the correct address via the firewall.
Recording	Select this check box to enable recording in your deployment. This requires a valid license key for recording.
Recording Server Address	Enter the IP address of the Recording Server and Scopia Content Slider Server. You can install the recording server on the same computer as the other Scopia Desktop Server components, or you can deploy it as a dedicated server.
Streaming	Select this check box to enable streaming in your deployment. This requires a valid license key for streaming.

Field	Description
Streaming Server Address	Enter the IP address of the streaming server. You can install the streaming server on the same computer as the other Scopia Desktop Server components, or you can deploy it as a dedicated server.
Use a different address for media and signaling	Select this check box when you install the Streaming Server to configure it on one IP address but users view webcasts on another IP address.

Verifying Scopia Desktop Server Installation and Connection with Other Components

About this task

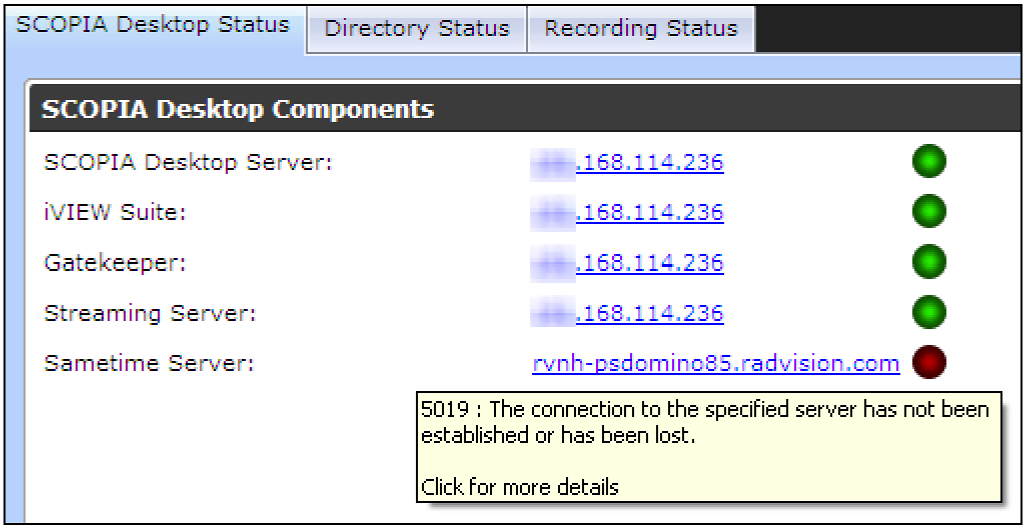
The Scopia Desktop Administrator web interface displays the connectivity status of your deployment. The indicators next to each link shows whether or not the connection or registration to the target server is successful. When the indicator is red, hover over the indicator to view the tooltip containing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

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

Procedure

1. To verify that Scopia Desktop Server is connected to the necessary video network devices, select **Status** in the sidebar.

2. View the connection status for each server or component. If necessary, select any red indicators to view further error information.



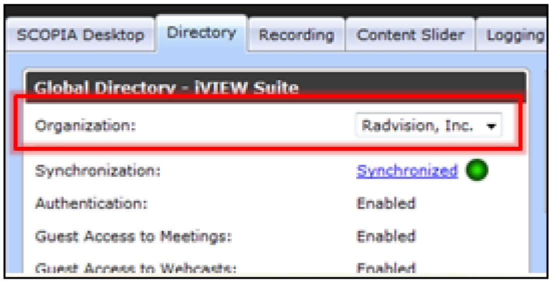
SCOPIA Desktop Server: [redacted].168.114.236 ●
iVIEW Suite: [redacted].168.114.236 ●
Gatekeeper: [redacted].168.114.236 ●
Streaming Server: [redacted].168.114.236 ●
Sametime Server: rvnh-psdomino85.radvision.com ●

5019 : The connection to the specified server has not been established or has been lost.

Click for more details

Figure 46: Viewing the connection status with Scopia Desktop Server

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



Global Directory - iVIEW Suite

Organization: Radvision, Inc.

Synchronization: Synchronized

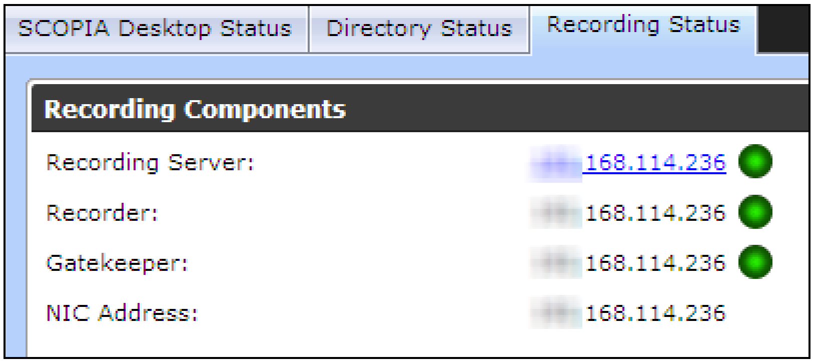
Authentication: Enabled

Guest Access to Meetings: Enabled

Guest Access to Webcasts: Enabled

Figure 47: Viewing an organization's status in a multi-tenant deployment

4. If you installed and configured a Scopia Desktop Recording Server, select the **Recording Status** tab to verify the connectivity status of the recording components.



Recording Components

Recording Server: [redacted]168.114.236

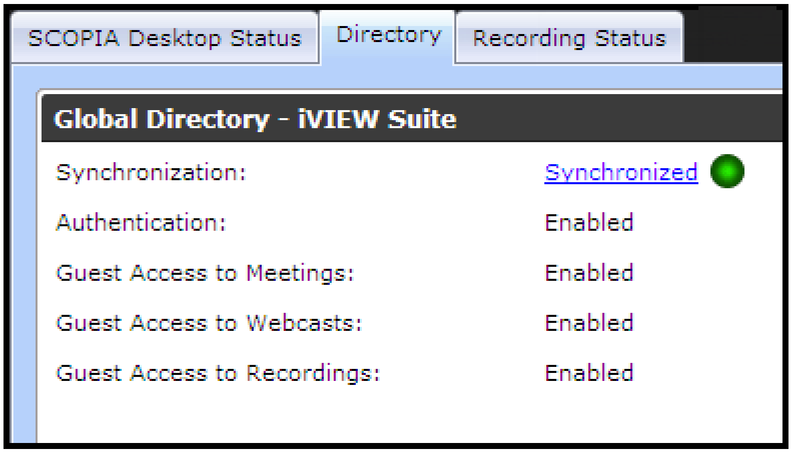
Recorder: [redacted]168.114.236

Gatekeeper: [redacted]168.114.236

NIC Address: [redacted]168.114.236

Figure 48: Viewing the connectivity

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



Global Directory - iVIEW Suite

Synchronization: Synchronized

Authentication: Enabled

Guest Access to Meetings: Enabled

Guest Access to Webcasts: Enabled

Guest Access to Recordings: Enabled

Figure 49: Status of LDAP synchronization

6. (Optional) View the connection status of the Scopia Content Slider by selecting the **Content Slider** tab. For more information on the Content Slider, see About Components of the Scopia Desktop Server on page 6.

7. If necessary, select any red indicators to view further error information.

Adding and Modifying Scopia Desktop Server in Scopia Management

About this task

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

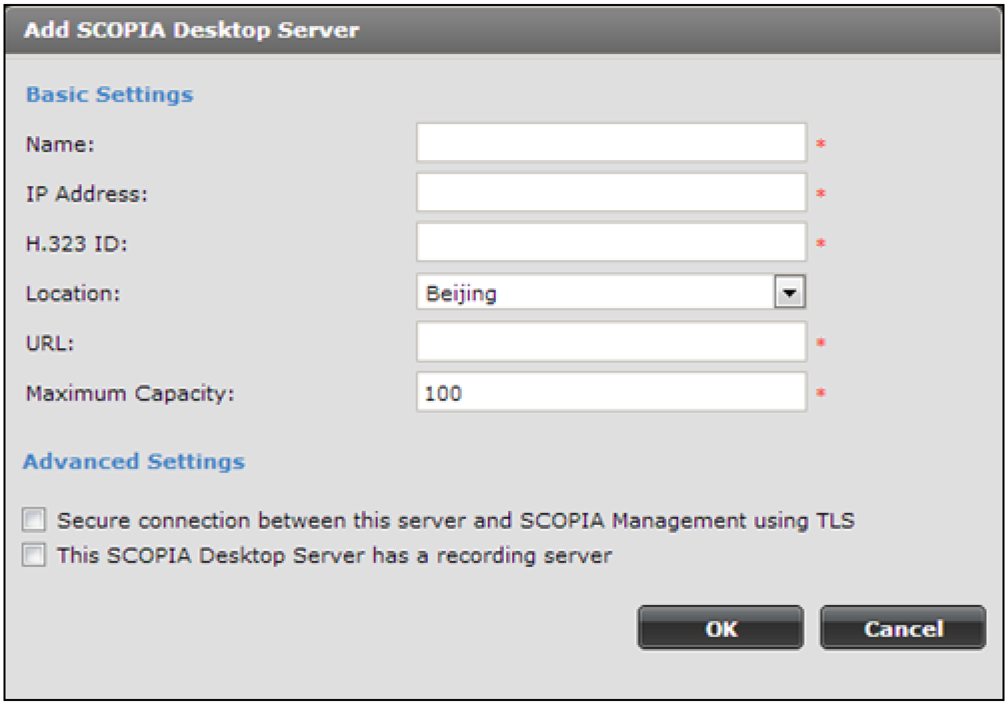
Ensure that Scopia Desktop Server has Scopia Management's IP address, and conversely Scopia Management has Scopia Desktop Server's IP address. For more information on how to add Scopia Management's IP address to the Scopia Desktop Server, see Connecting Scopia Desktop Server with Video Network Devices on page 68.

Procedure

1. Access the Scopia Management administrator portal.

2. In the **Devices** tab, select **Desktop Servers**.

3. Select the link in the **Name** column for the Scopia Desktop Server you require, or select **Add** to create a new Scopia Desktop Server profile. The **Add Scopia Desktop Server** page appears (Figure 50: Adding a Scopia Desktop profile on page 74).



Add SCOPIA Desktop Server

Basic Settings

Name: *

IP Address: *

H.323 ID: *

Location: Beijing

URL: *

Maximum Capacity: 100 *

Advanced Settings

□ Secure connection between this server and SCOPIA Management using TLS

□ This SCOPIA Desktop Server has a recording server

Figure 50: Adding a Scopia Desktop profile

4. Enter the required information (Table 18: Configuring Scopia Desktop Server on page 74).

Table 18: Configuring Scopia Desktop Server

Field Name	Description
Name	Enter a name to identify this Scopia Desktop Server. This name is displayed in the list of Scopia Desktop Servers.
IP address	Enter the management IP address of Scopia Desktop Server.
H.323 ID	Enter the H.323 ID used to identify connections from Scopia Desktop Server in MCU conferences. This must match the H.323 ID that is configured in the Scopia Desktop administrator web interface. Configuring this field allows Scopia Management to route calls from this Scopia Desktop Server based on the predefined IP topology. The ID can have one of the following formats: • H.323 alias. For example, `username`. • IP address of an H.323 endpoint. For example, 123.45.678.9. • URI dialing for H.323 or SIP endpoints. For example, user@company.com • E.164 dialing for H.323 or SIP endpoints. For example, 881234.
Location	This is only relevant for service providers or deployments with multiple locations. Select the Scopia Desktop Server's location.
URL	Enter the URL used to access the Scopia Desktop Server. The URL must be in the format *http://<web URL>:<port number>/scopia*.

Field Name	Description
Maximum Capacity	Enter the maximum number of simultaneous connections you want to allow for your Scopia Desktop Server, based on computing power.
Secure connection between this server and Scopia Management using TLS	To use the Transport Layer Security (TLS) protocol to secure the transport link between Scopia Management and Scopia Desktop, select this checkbox. For more information, see *Administrator Guide for Scopia Management*.
This Scopia Desktop Server has a recording server	Select this checkbox to configure this Scopia Desktop Server with a recording server.

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

Enabling Scopia Desktop Registered Users in Scopia Management

About this task

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

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

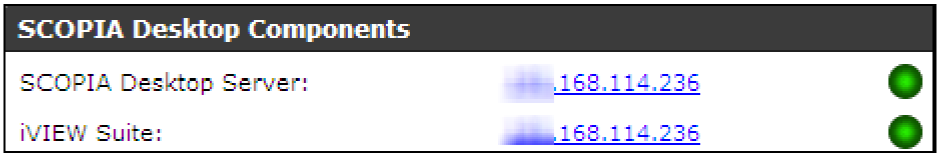
Assign licenses to groups of users via their user profile in Scopia Management. For more information on defining user profiles, see *Administrator Guide for Scopia Management*. This procedure includes how to customize the profile for a single user to add a license.

Before you begin

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

Procedure

1. Access the Scopia Desktop Server Administrator web user interface, as described in Accessing the Scopia Desktop Server Web Administration Interface on page 66.
2. Verify that the Scopia Desktop Server is connected to Scopia Management:
   a. Select the **Status** icon in the sidebar.
   b. Verify the Scopia Desktop Server and Scopia Management connection status in the Scopia Desktop Components section.



SCOPIA Desktop Components

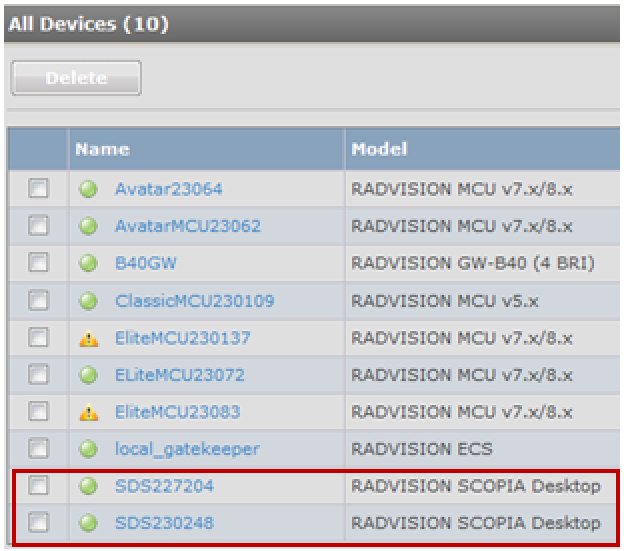
SCOPIA Desktop Server:	[redacted].168.114.236	●
iVIEW Suite:	[redacted].168.114.236	●

Figure 51: Verifying the Scopia Management connection in Scopia Desktop Server

3. In Scopia Management, verify that the Scopia Desktop Server is added as a connected server:

   a. Access the Scopia Management web administrator portal.

   b. Select the **Devices** tab.



All Devices (10)

	Name	Model
□	● Avatar23064	RADVISION MCU v7.x/8.x
□	● AvatarMCU23062	RADVISION MCU v7.x/8.x
□	● B40GW	RADVISION GW-B40 (4 BRI)
□	● ClassicMCU230109	RADVISION MCU v5.x
□	⚠ EliteMCU230137	RADVISION MCU v7.x/8.x
□	● ELiteMCU23072	RADVISION MCU v7.x/8.x
□	⚠ EliteMCU23083	RADVISION MCU v7.x/8.x
□	● local_gatekeeper	RADVISION ECS
□	● SDS227204	RADVISION SCOPIA Desktop
□	● SDS230248	RADVISION SCOPIA Desktop

Figure 52: Verifying the Scopia Desktop Server connection in Scopia Management

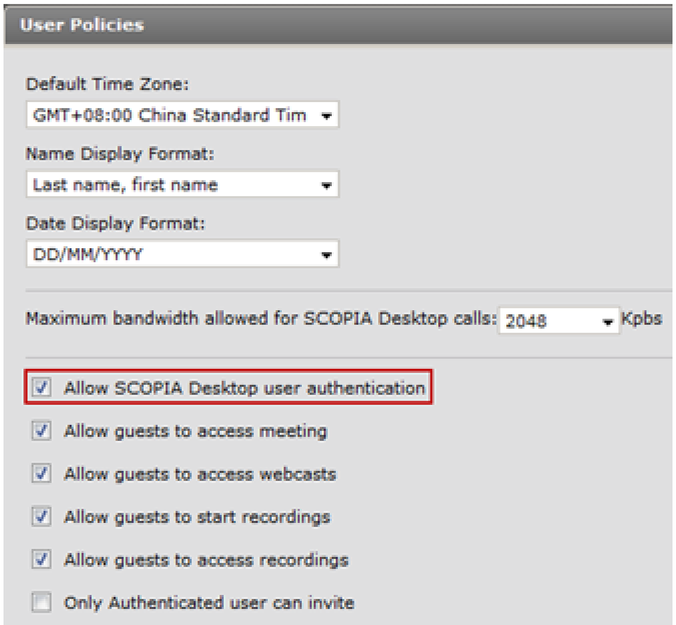
   c. Verify that the required Scopia Desktop Server appears in the table of connected servers.

4. Enable user authentication for Scopia Desktop:

   a. Login to Scopia Management.

   b. Select the **Settings** tab and navigate to **Users> Policies** in the sidebar menu.

   c. Select the **Allow Scopia Desktop user authentication** check box.



User Policies

Default Time Zone:
GMT+08:00 China Standard Tim

Name Display Format:
Last name, first name

Date Display Format:
DD/MM/YYYY

Maximum bandwidth allowed for SCOPIA Desktop calls: 2048 Kpbs

☑ Allow SCOPIA Desktop user authentication

☑ Allow guests to access meeting

☑ Allow guests to access webcasts

☑ Allow guests to start recordings

☑ Allow guests to access recordings

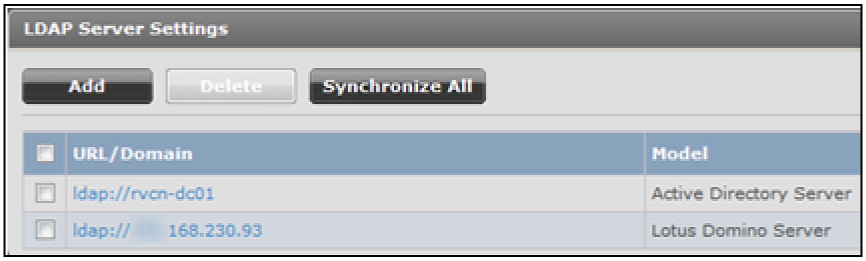
☐ Only Authenticated user can invite

Figure 53: Enabling registered users in Scopia Desktop

d. Select authorization options for unregistered users (known as guests) as required. You can enable the following features for guests in your deployment:

- Access meetings without logging in to Scopia Desktop Server
- Access meetings without logging in to Scopia Desktop Server
- Access webcasts without logging in to Scopia Desktop Server
- Start a recording of a videoconference without logging in to Scopia Desktop Server
- Access a public recording without logging in to Scopia Desktop Server
- Invite participants to a videoconference without logging in to Scopia Desktop Server.

5. Select **Servers > LDAP Servers** in the sidebar menu, and verify the type of directory to which Scopia Management connects for user authentication using LDAP as an authentication method:
   - Internal Directory
   - Microsoft Active Directory
   - IBM Lotus Domino



☐	URL/Domain	Model
☐	ldap://rvcn-dc01	Active Directory Server
☐	ldap://[redacted]168.230.93	Lotus Domino Server

Figure 54: Examples of user directory server listed in Scopia Management

6. Select the **Users** tab to check the total number of Scopia Desktop Pro and/or Scopia Mobile licensed users displayed at the top of the tab. Users with Scopia Desktop Pro and/or Scopia

Mobile have a license icon next to their name (see Figure 55: Scopia Desktop Pro and Scopia Mobile licensed users in Scopia Management on page 78).

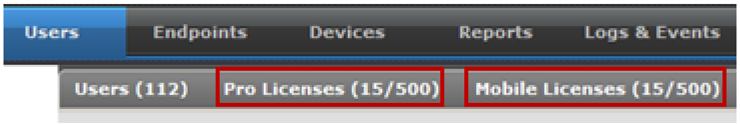


Figure 55: Scopia Desktop Pro and Scopia Mobile licensed users in Scopia Management

7. If necessary, enable a Scopia Desktop Pro license or Scopia Mobile for each person using point-to-point functionality or Scopia Mobile.
   a. In the **Users** tab, select the relevant user.
   b. Select **Edit** in the **User Profile** field.

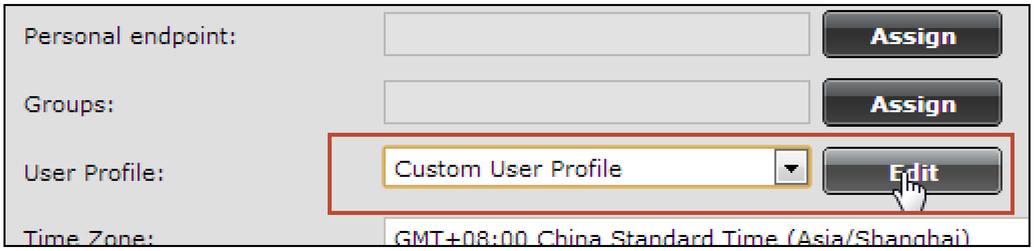


Figure 56: Customizing profile details of a user

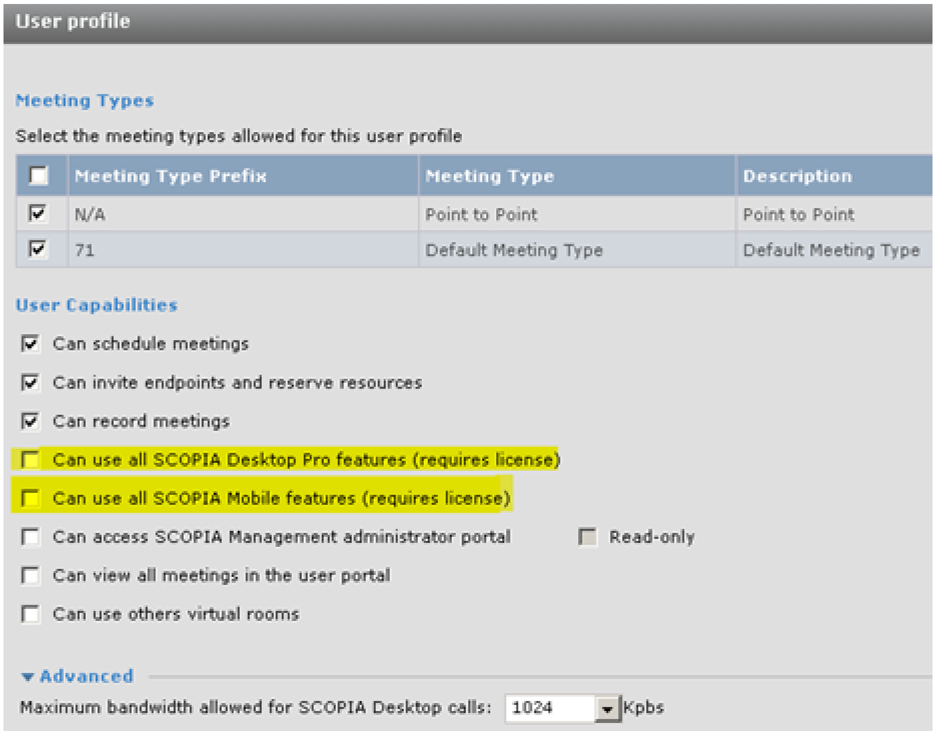
If this is a **View** button, it means you cannot change this profile from here, you can only view it. To edit the profile, you can do one of the following:

- To edit the profile for all its members (not just this user), select **Settings > Users > Profiles**.
- To customize the profile for this user only, change the **User Profile** field to **Custom User Profile**, then select **Edit**.

Important:

After you decouple this username from its profile, any future changes to the profile will not impact on this user, since now it has a custom profile.

   c. Select **Can use all Scopia Desktop Pro features** or **Can use all Scopia Mobile features**.


User profile

Meeting Types

Select the meeting types allowed for this user profile

□	Meeting Type Prefix	Meeting Type	Description
☑	N/A	Point to Point	Point to Point
☑	71	Default Meeting Type	Default Meeting Type

User Capabilities

☑ Can schedule meetings

☑ Can invite endpoints and reserve resources

☑ Can record meetings

□ Can use all SCOPIA Desktop Pro features (requires license)

□ Can use all SCOPIA Mobile features (requires license)

□ Can access SCOPIA Management administrator portal □ Read-only

□ Can view all meetings in the user portal

□ Can use others virtual rooms

▼ Advanced

Maximum bandwidth allowed for SCOPIA Desktop calls: 1024 Kpbs

Figure 57: Enabling Scopia Desktop Pro or Scopia Mobile licenses in Scopia Management

Defining Bandwidth Settings in Scopia Desktop Server

About this task

This section details how to define the maximum bandwidth used between the Scopia Desktop Client and the Scopia Desktop Server.

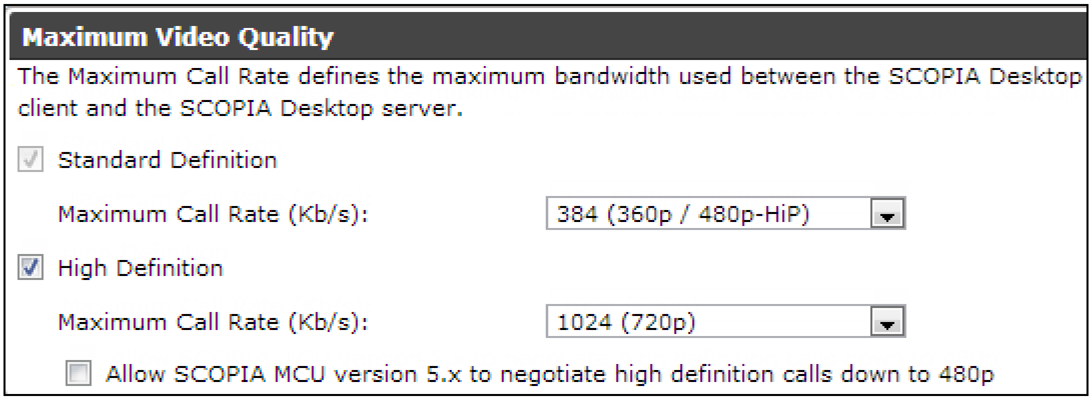
Maximum bandwidth is also defined in the MCU meeting type (service). You invoke a meeting type by entering its prefix before the meeting ID. For example, if 88 is the dial prefix defined MCU meeting type for HD meetings, users would enter 88 followed by the meeting ID to invoke that meeting type's parameters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

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

Procedure

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

4. Select the maximum call rate in the **Maximum Video Quality** section.
5. Configure call rate or bandwidth settings for standard definition (SD) and high definition (HD) video by selecting the bandwidth rate from the **Maximum Call Rate** list.



Maximum Video Quality

The Maximum Call Rate defines the maximum bandwidth used between the SCOPIA Desktop client and the SCOPIA Desktop server.

☑ Standard Definition

Maximum Call Rate (Kb/s): 384 (360p / 480p-HiP)

☑ High Definition

Maximum Call Rate (Kb/s): 1024 (720p)

☐ Allow SCOPIA MCU version 5.x to negotiate high definition calls down to 480p

Figure 58: Maximum Call Rate Section

SD video has a default resolution of 360p, with a default bandwidth value of 384 kbps. If your MCU uses a meeting type (service) defined for higher quality HD video, video is downgraded to SD.

HD video has a default resolution of 720p, with a default bandwidth of 1024 kbps. If your MCU uses a meeting type (service) defined for lower quality SD video or lower bandwidth, video is downgraded to those values.

Important:

The actual bandwidth consumed for a specific video resolution depends on the compression capabilities of your MCU. For example, Scopia Elite 6000 Series MCU includes H.264 High Profile encoding, therefore allowing a higher resolution at a lower bitrate than other MCUs. For more information, see Planning the Bandwidth for Scopia Desktop Clients Based on MCU Capacity on page 27.

The bandwidth used by each Scopia Desktop Client indirectly determines the capacity of your deployed MCUs. Your chosen video resolution (and bandwidth), places demands on your MCU to supply that video resolution for each connection, which determines how many users can simultaneously connect to the MCU. For more information, see Planning the Bandwidth for Scopia Desktop Clients Based on MCU Capacity on page 27.

Defining Scopia Desktop Server Public Address and Other Client Connection Settings

About this task

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

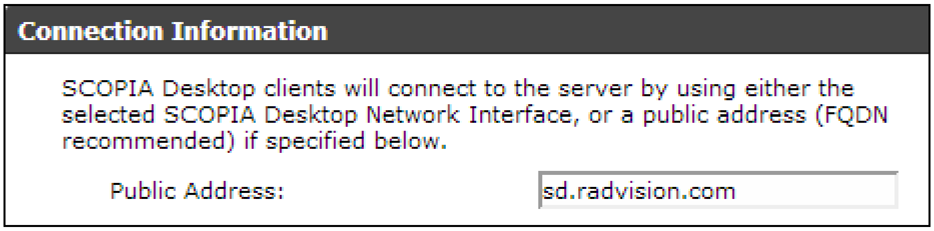
You can also define Scopia Desktop Server's size of network packets (MTU size). The MTU, or Maximum Transmission Unit, is the maximum size of data packets sent around your network.

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

Procedure

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

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

   Connection Information

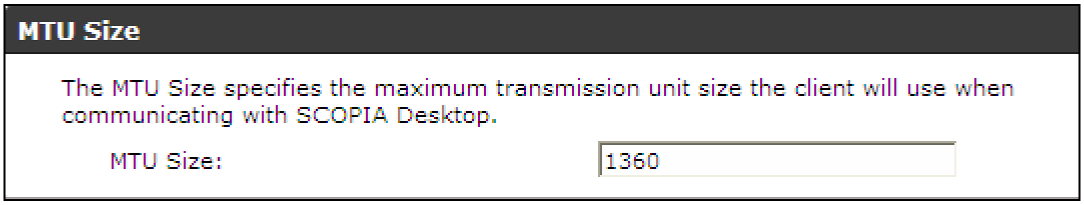
   SCOPIA Desktop clients will connect to the server by using either the selected SCOPIA Desktop Network Interface, or a public address (FQDN recommended) if specified below.

   Public Address: sd.radvision.com

   Figure 59: The public address for Scopia Desktop Clients to connect to the server

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

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

   MTU Size

   The MTU Size specifies the maximum transmission unit size the client will use when communicating with SCOPIA Desktop.

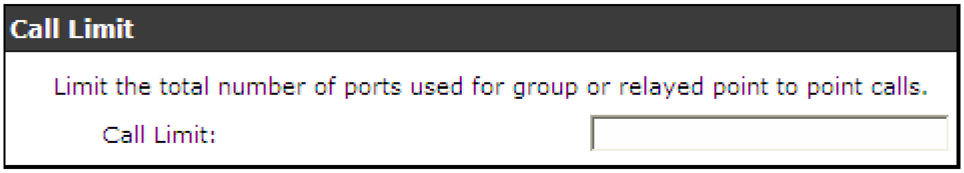
   MTU Size: 1360

   Figure 60: Setting the MTU size for Scopia Desktop Client

   Important:

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

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


Call Limit

Limit the total number of ports used for group or relayed point to point calls.

Call Limit:

Figure 61: Call Limit Section

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

Enabling or Disabling Scopia Desktop Client Features

About this task

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

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

  Important:

  Using encryption is subject to local regulation. In some countries it is restricted or limited for usage. For more information, consult your local reseller.
- Enable or disable call back for users who have an H.323 endpoint but also want to connect a dedicated PC to share presentations.
- Add a pane in the videoconferencing window containing web content for all users in your organization.

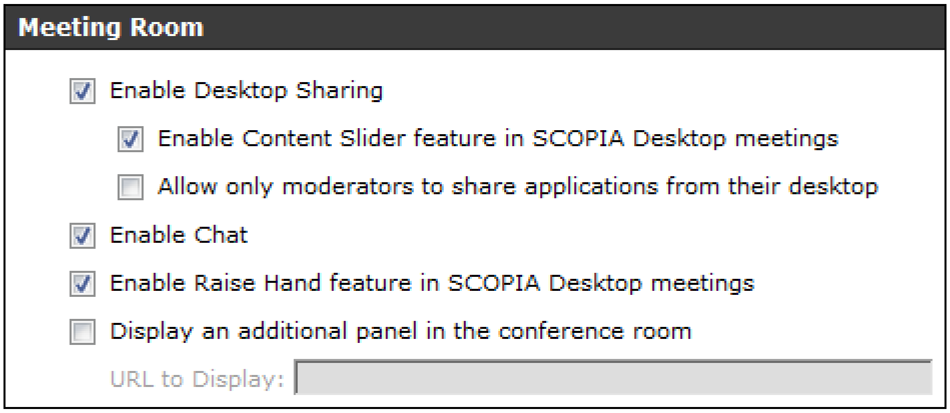
Users with a login to Scopia Desktop Server can define their own virtual room preferences in the Scopia Desktop Client (see *User Guide for Scopia Desktop Client*).

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

This section describes how to make global changes for the virtual rooms of all Scopia Desktop Server users.

Procedure

1. Access the Scopia Desktop Server Administration web interface.
2. Select the **Client** icon in the sidebar.
3. Select the **Meeting Features** tab.



Meeting Room

☑ Enable Desktop Sharing

☑ Enable Content Slider feature in SCOPIA Desktop meetings

☐ Allow only moderators to share applications from their desktop

☑ Enable Chat

☑ Enable Raise Hand feature in SCOPIA Desktop meetings

☐ Display an additional panel in the conference room

URL to Display:

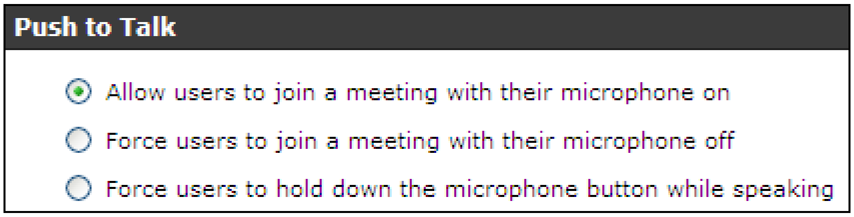
Figure 62: Enabling or disabling client videoconferencing features

4. Enter the fields as described in Table 19: Settings for the Scopia Desktop Client Virtual Room window on page 83.

Table 19: Settings for the Scopia Desktop Client Virtual Room window

Field	Description
Enable Desktop Sharing	Determines whether participants can share their PC desktop content with others in the videoconference. If desktop sharing disabled, the **Present** button does not appear in the Virtual Room window of Scopia Desktop Client.
Enable Content Slider feature in Scopia Desktop meetings	Determines whether participants can review content which has already been shared in the meeting by scrolling back and forth.
Allow only moderators to share applications from their desktop	Determines whether this feature is restricted to moderators of videoconferences only.
Enable Chat	Determines whether to display the chat window pane in the Virtual Room window of Scopia Desktop Client.
Enable Raise Hand feature in Scopia Desktop meetings	Determines whether a muted user (usually in lecture mode) can request permission to speak.
Display an additional panel in the conference room	Determines whether to display an additional pane in Scopia Desktop Client's Virtual Room window within your organization. The pane's contents are drawn from an external web address.
URL to Display	Enter the web address in this field. When the system accesses the web address, it automatically appends two parameters: the current meeting ID and the participant's nickname. This enables your external web content to relate to the meeting and participant if required. The parameters added are: `?meetingid=NNN&nickname=XXX`. If your external web content already takes different parameters in its URL, these parameters are appended to the URL string. Use standard URL-encoding in this field, for example '&' is `%26`, '=' is `%3D` and so on.

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



Push to Talk

● Allow users to join a meeting with their microphone on

○ Force users to join a meeting with their microphone off

○ Force users to hold down the microphone button while speaking

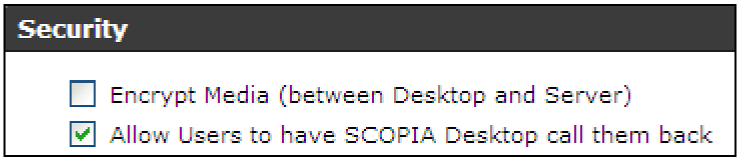
Figure 63: Push to Talk Settings

Enter the fields as described in Table 20: Defining microphone behavior during a meeting on page 84.

Table 20: Defining microphone behavior during a meeting

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

6. Configure the **Security** section to determine encryption parameters.



Security

□ Encrypt Media (between Desktop and Server)

☑ Allow Users to have SCOPIA Desktop call them back

Figure 64: Security Settings

Enter the fields as described in Table 21: Defining security settings between Scopia Desktop Server and Scopia Desktop Client on page 85.

Table 21: Defining security settings between Scopia Desktop Server and Scopia Desktop Client

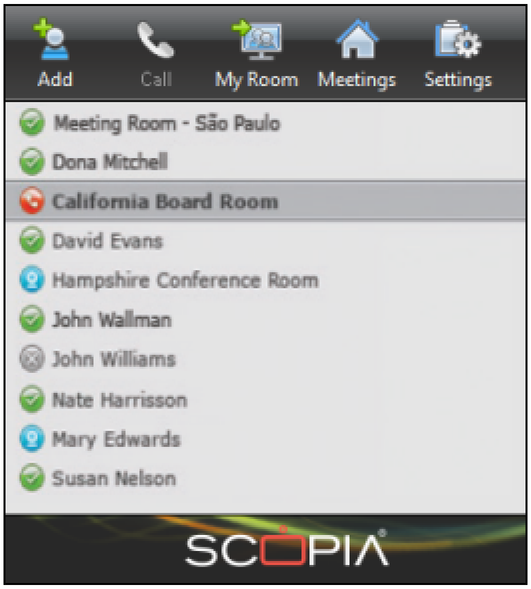
Field	Description
Encrypt Media	Determines whether to encrypt the media (audio, video and presentation) using SRTP between the Scopia Desktop Server and Scopia Desktop Client/Scopia Mobile. ❗ **Important:** Using encryption is subject to local regulation. In some countries it is restricted or limited for usage. For more information, consult your local reseller.
Allow Users to have Scopia Desktop call them back	When users with a dedicated videoconferencing endpoint connect their PC to the meeting for data sharing only, this field determines whether the system displays the check box for the system to call back their H.323 device to connect video from there. The check box is located on the Scopia Desktop web portal. Before connecting to a meeting, select **More Options > Use my computer for presentation only > Callback my video device number**. ❗ **Important:** When a computer connects as a dedicated data-only device, it cannot view or send video or audio, but you can view the participant list, moderate, chat, share content from the computer.

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

Synchronizing Contact Lists with a User Directory

About this task

One of the components in the Scopia Desktop Server is the Presence Server (see Figure 1: Components of the Scopia Desktop Server on page 6), which updates Scopia Desktop's Contact List, part of a Scopia Desktop Pro deployment. It maintains the status of a user's listed contacts, whether or not they are available.



✓ Meeting Room - São Paulo
✓ Dona Mitchell
California Board Room
✓ David Evans
Hampshire Conference Room
✓ John Wallman
John Williams
✓ Nate Harrisson
Mary Edwards
✓ Susan Nelson

Figure 65: Status icons appear next to each contact

Scopia Desktop's Presence (XMPP) Server is implemented by a service known as Jabber.

The Presence Server must therefore have access to a user directory, which it retrieves from Scopia Management, which in turn can take its list of users either from an external source, like Microsoft's Active Directory, or from Scopia Management's own internal directory.

This section describes how to configure the Presence Server with Scopia Management's user directory, both its own internal user directory or with an external LDAP directory.

Important:

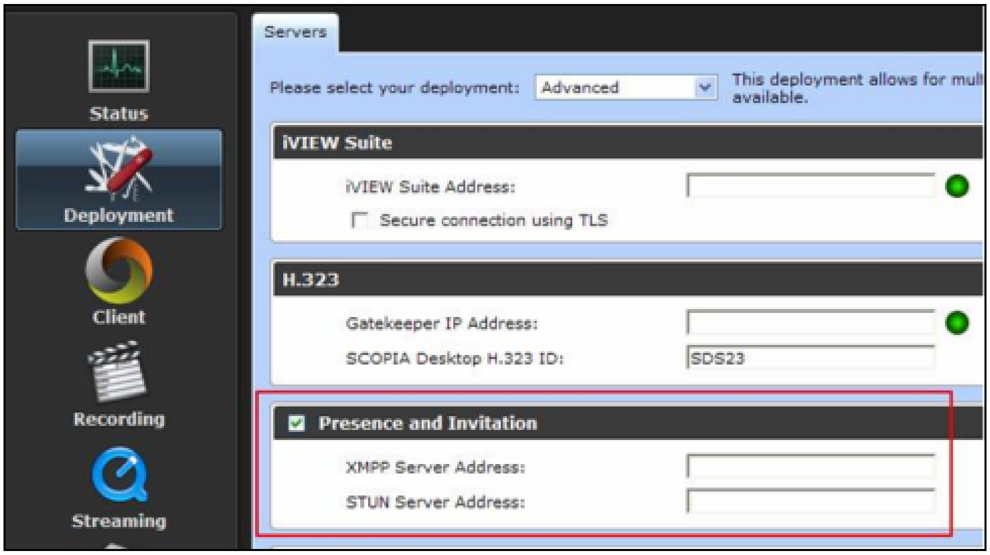
If your Scopia Management uses Domino as the source of its user directory, follow the same steps for an Active Directory source.

Before you begin

Ensure Scopia Management is connected to the Scopia Desktop Server and is sharing its user database. For more information, see Enabling Scopia Desktop Registered Users in Scopia Management on page 75.

Procedure

1. Access the Scopia Desktop web administration interface.
2. Select the **Deployment** icon in the sidebar.
3. Select the **Presence and Invitation** check box. (Figure 66: Connecting the Scopia Desktop Server to presence (XMPP) and STUN servers on page 87)



Please select your deployment: Advanced

This deployment allows for mul
available.

iVIEW Suite Address:

□ Secure connection using TLS

Gatekeeper IP Address:

SCOPIA Desktop H.323 ID: SDS23

☑ Presence and Invitation

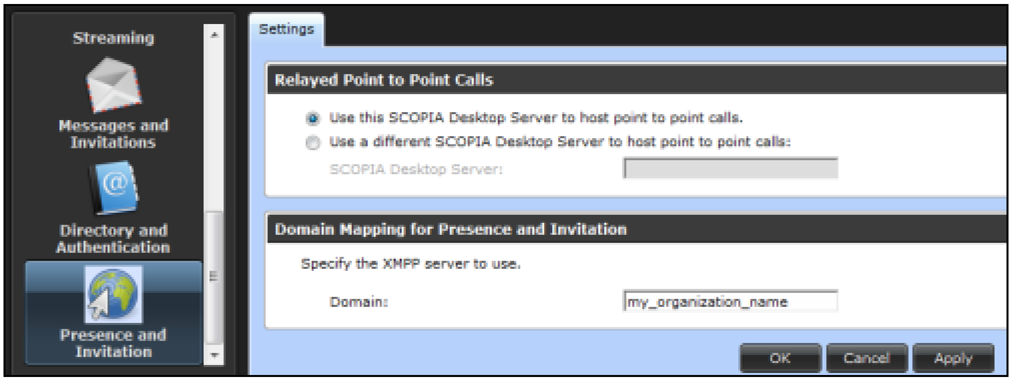
XMPP Server Address:

STUN Server Address:

Figure 66: Connecting the Scopia Desktop Server to presence (XMPP) and STUN servers

4. Enter the IP addresses of each of the servers in the **XMPP Server Address** and **STUN Server Address** fields (Figure 66: Connecting the Scopia Desktop Server to presence (XMPP) and STUN servers on page 87).

5. Select the **Presence and Invitation** icon in the sidebar (Figure 67: Defining the Jabber Domain on Scopia Desktop Server on page 87).


Streaming
Messages and Invitations
Directory and Authentication
Presence and Invitation
Settings
Relayed Point to Point Calls
Domain Mapping for Presence and Invitation
OK
Cancel
Apply

● Use this SCOPIA Desktop Server to host point to point calls.

○ Use a different SCOPIA Desktop Server to host point to point calls:

SCOPIA Desktop Server:

Specify the XMPP server to use.

Domain: my_organization_name

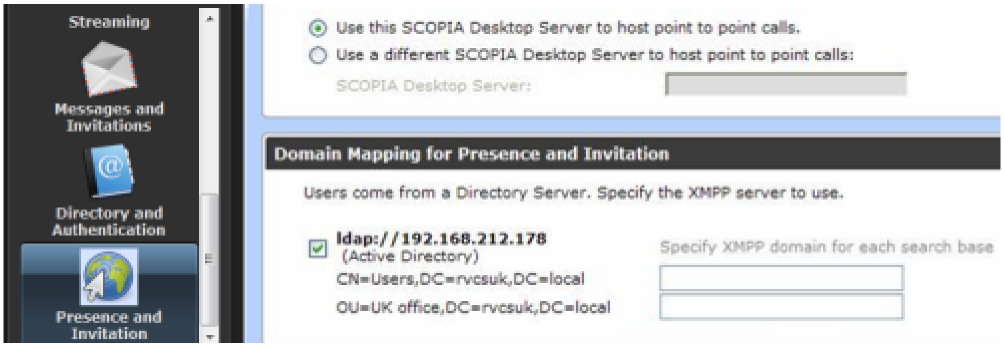
Figure 67: Defining the Jabber Domain on Scopia Desktop Server

6. If Scopia Management uses its internal directory as its list of users, set the **Domain** field (Figure 67: Defining the Jabber Domain on Scopia Desktop Server on page 87) to be the internal Jabber domain name for your organization. Make a note of this name as you will use it again later for the **Jabber Domain** field in the configuration tool in 10.

   ### Important:

   This is not a DNS domain. The **Domain** field here refers to an internal name for the Jabber service, responsible for presence services. We recommend, therefore, using a name that does not resolve to an IP address. For example, **my_organization_name**.

7. If your Scopia Management is configured to work with the Active Directory (Figure 68: Mapping Jabber domains to search bases in Active Directory on page 88):



● Use this SCOPIA Desktop Server to host point to point calls.

○ Use a different SCOPIA Desktop Server to host point to point calls:

SCOPIA Desktop Server:

Domain Mapping for Presence and Invitation

Users come from a Directory Server. Specify the XMPP server to use.

☑ **ldap://192.168.212.178** (Active Directory)

Specify XMPP domain for each search base

CN=Users,DC=rvcsuk,DC=local

OU=UK office,DC=rvcsuk,DC=local

Figure 68: Mapping Jabber domains to search bases in Active Directory

a. You can either choose specific user groups (search bases) within the LDAP user list to map to a Jabber domain, or map the whole database to a Jabber domain. To select parts of the LDAP database, select the check box of the LDAP database (Figure 68: Mapping Jabber domains to search bases in Active Directory on page 88).

   To choose the whole database, clear the check box.

b. For each search base (user group) you want the Presence Server (XMPP) to access, enter its internal Jabber domain. Make a note of these names as you will use them again later in this procedure for the **Jabber Domain** field in the configuration tool.

   Important:

   This is not a DNS domain. This **Domain** field refers to an internal name for the Jabber service, responsible for presence services. We recommend, therefore, using a name that does not resolve to an IP address. For example, **my_organization_name**.

   In a multi-tenant deployment, you can create a different mapping per organization.

8. On the Presence Server computer, start the Scopia Desktop Configuration Tool by selecting **Start > All Programs > Scopia Desktop > ConfigTool**.

9. Select the **Jabber** icon in the sidebar to configure the Presence Server.

10. If Scopia Management's user directory comes from its own internal directory:

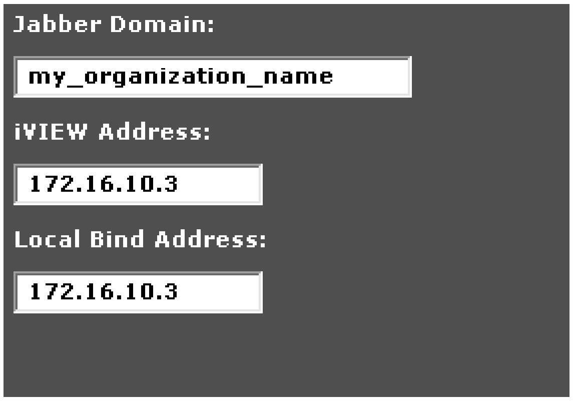
    a. Select **iVIEW** from the **Authentication Type** dropdown list at the top of the screen, and then select **Add**.

    b. In the **Jabber Domain** field, enter the same domain you used when enabling user authentication in the Scopia Desktop Server (Figure 69: Connecting the Presence Server to Scopia Management's internal directory on page 89).

       This domain must match the Jabber Domain entered earlier in this procedure.

       Important:

       This is not a DNS domain. The **Domain** field here refers to an internal name for the Jabber service, responsible for presence services. We recommend, therefore, using a name that does not resolve to an IP address. For example, **my_organization_name**.



Jabber Domain:

my_organization_name

iVIEW Address:

172.16.10.3

Local Bind Address:

172.16.10.3

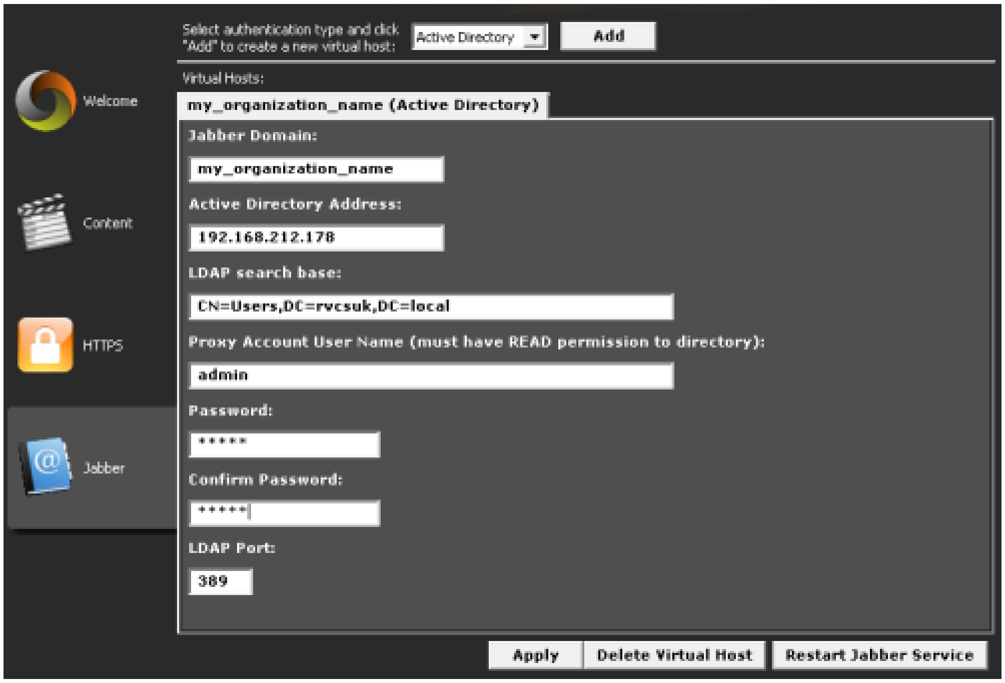
Figure 69: Connecting the Presence Server to Scopia Management's internal directory

c. Enter the IP Address of Scopia Management in the **iVIEW Address** field.

d. Enter the IP address of Scopia Desktop Server.

If the Jabber Server has multiple NICs, choose one of them for this configuration.

11. If your Scopia Management accesses its list of users from an external source like Microsoft's Active Directory (Figure 70: Connecting the Presence Server with the Active Directory on page 89):



Select authentication type and click "Add" to create a new virtual host: Active Directory

Virtual Hosts:

my_organization_name (Active Directory)

Jabber Domain:

my_organization_name

Active Directory Address:

192.168.212.178

LDAP search base:

CN=Users,DC=rvcsuk,DC=local

Proxy Account User Name (must have READ permission to directory):

admin

Password:

*****

Confirm Password:

*****

LDAP Port:

389

Figure 70: Connecting the Presence Server with the Active Directory

a. Select **Active Directory** from the **Authentication Type** dropdown list at the top of the screen, and then select **Add**.

For Domino implementations, select **Domino**.

b. Enter the IP address of the Active Directory server in the **Active Directory Address** field.

Important:

This domain must match the Active Directory address entered in the **Deployment** page (4).

c. To limit the scope to one or more user groups within the Active Directory, specify the search base in the **LDAP Search Base** field.

d. Enter the **Proxy Account User Name** and **Password** of a user with access to the Active Directory database.

e. In case the Active Directory is configured with a port other than default port 389, change the **LDAP Port** value.

12. If you have a service provider (multi-tenant) deployment, configure the XMPP domain for each organization.

    In a multi-tenant deployment the Jabber configuration tool displays many tabs, to enable a different configuration in each organization. Select the relevant tab to configure the authentication type per organization. See Figure 69: Connecting the Presence Server to Scopia Management's internal directory on page 89.

    Important:

    In a multi-tenant deployment, you can have a different Jabber domain for each organization, but all the organizations use the same Scopia Management, hence the **iVIEW Address** field becomes read-only in all the tabs after you have configured it for the first tab in one of the organizations.

13. Select **Apply**.

Rolling-Out Scopia Desktop Client to End Users

About this task

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

The section includes these topics:

Navigation

- Minimum Requirements for Scopia Desktop Client on page 90
- Installing Scopia Desktop Client Locally on a PC on page 92
- Centrally Deploying Scopia Desktop Clients in your Organization on page 93

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 (desktop mode, 32 and 64-bit)
  - Mac OS X version 10.6 (Snow Leopard) 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 25 and later)
  - Internet Explorer (version 6 and later, for windows)
  - Firefox (version 20 and later)

    - Safari (version 5 and later)
- Viewing live webcasts or recorded meetings
    - Mac: QuickTime 7.4.5 or later (version 7.7 recommended)
    - PC: QuickTime 7.4.5 minimum (version 7.7 recommended)

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 the 32 bit version of Scopia Add-in for Microsoft Outlook and the Contact List.

Important:

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

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

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

Before you begin

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

Procedure

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

   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. Select **Updates** in the top-right corner of the web portal.

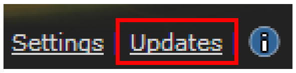
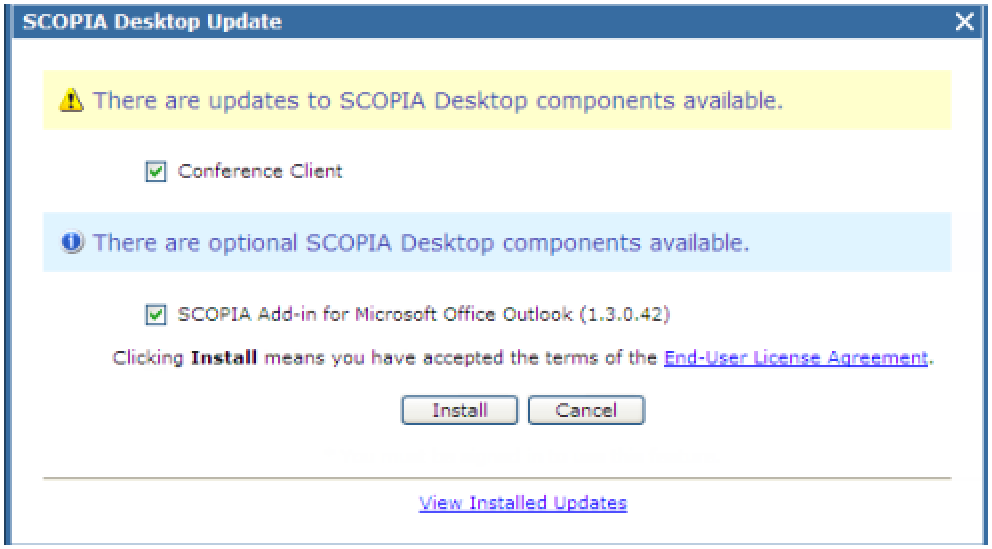


Figure 71: The Updates link in the top right corner of the web portal

The **Scopia Desktop Update** window opens.



There are updates to SCOPIA Desktop components available.

☑ Conference Client

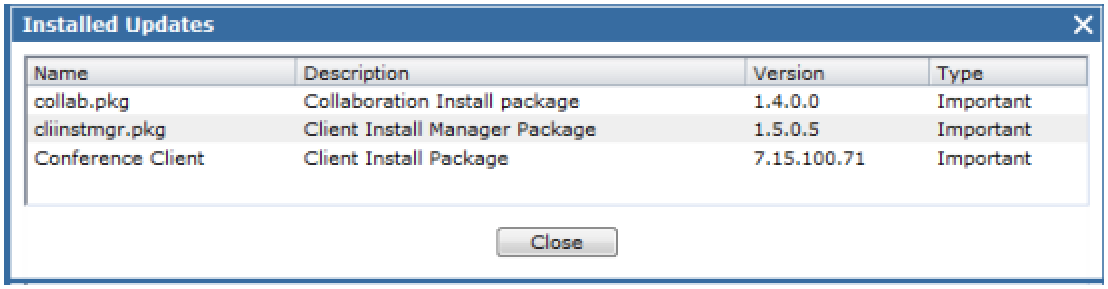
There are optional SCOPIA Desktop components available.

☑ SCOPIA Add-in for Microsoft Office Outlook (1.3.0.42)

Clicking **Install** means you have accepted the terms of the End-User License Agreement.

Figure 72: Updating Scopia Desktop Client

3. Select **Conference Client** to install or update the Scopia Desktop Client.
4. Select **Scopia Add-in for Microsoft Office Outlook** to install the add-in that allows you to schedule videoconferences from Microsoft Office Outlook.
5. Select **Install**. When the Scopia Desktop Client installation is complete, you should see the following icon in the task tray at the lower right corner of the screen:
6. To verify that any optional components were installed, select the **View Installed Updates** link. A list of installed components appears.



Name	Description	Version	Type
collab.pkg	Collaboration Install package	1.4.0.0	Important
cliinstmgr.pkg	Client Install Manager Package	1.5.0.5	Important
Conference Client	Client Install Package	7.15.100.71	Important

Figure 73: Installed Updates and Components

7. If you installed the Scopia Add-in for Microsoft Outlook, restart your Microsoft Office Outlook.

Centrally Deploying Scopia Desktop Clients in your Organization

About this task

You can push Scopia Desktop Clients simultaneously to end users using one of these standard Microsoft server tools:

- Microsoft Active Directory (AD)
- Microsoft Systems Management Server (SMS).

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

Upgrading the Scopia Desktop Server License

About this task

You can update the Scopia Desktop Server license for:

- Recording license

  If you want to add the recording feature or increase the number of simultaneous recordings, you need a new or updated recording serial key.

  A server with recording features enabled must have a valid recording license installed. Without a license, you are restricted to the default evaluation license allowing you to record one five-minute meeting at a time. Scopia Desktop Server supports up to 10 simultaneous recordings.
- Increased call capacity

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

Before you begin

Obtain an Scopia Desktop Server license key and an optional recording serial key.

Procedure

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

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

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

Configuring Scopia Desktop to Work with a Single Scopia MCU

About this task

This section describes how to configure Scopia Desktop to work with a single Scopia MCU.

Before you begin

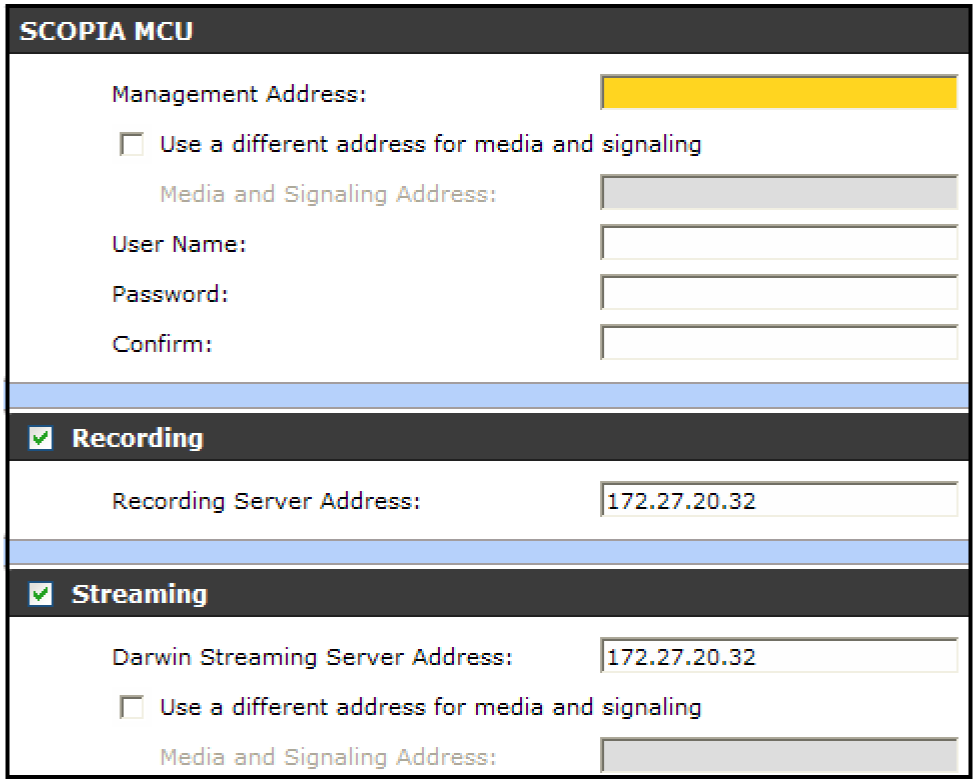
If the dual NIC support feature is enabled on the MCU, determine the IP addresses used for the MCU Management Interface and Media and Signaling Interface.

Procedure

1. Access to the Scopia Desktop Server Administration web interface.
2. Select the **Deployment** icon in the sidebar.
3. Select **Basic** from the deployment list.

   The deployment consists of a single Scopia Desktop Server and a single Scopia MCU. Only the Scopia MCU can be called.
4. Enter the MCU IP address in the **Management Address** field.

   If the dual NIC support feature is enabled on the MCU, select **Use a different interface for media and signaling**, and then enter IP addresses in the Management Address field and in the Media and Signaling Address field.



SCOPIA MCU

Management Address:

□ Use a different address for media and signaling

Media and Signaling Address:

User Name:

Password:

Confirm:

☑ Recording

Recording Server Address: 172.27.20.32

☑ Streaming

Darwin Streaming Server Address: 172.27.20.32

□ Use a different address for media and signaling

Media and Signaling Address:

Figure 74: Basic deployment configuration

5. Enter a user name and password for accessing the MCU Administration web user interface.

6. Re-enter the password in the **Confirm** field.

   The default user name is **admin**. There is no default password for Scopia MCU; for Scopia Elite MCU the default password is **password**.

7. If Scopia Desktop Server is configured with multiple IP addresses, select the relevant address from the Scopia Desktop Network Interface list.

8. To enable recording:

   a. Select the **Recording** check box.

   b. Enter the Recording Server address.

9. To enable streaming:

   a. Select the **Streaming** check box.

   b. Enter the Darwin Streaming Server address.

   c. If you use a different address for media and signaling, select the **Use a different address for media and signaling** check box and enter the address.

10. Select **OK**.

    The **Settings** page appears.

Chapter 5 | Securing Your Scopia Desktop Deployment

This section describes how you can enhance the security of your Scopia Desktop deployment by encrypting communications using the encryption keys held in certificates which are uploaded to the various deployment components.

Important:

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

There are two types of certificates which can be installed.

- Install certificates on the Conference Server to encrypt the media travelling between Scopia Desktop Clients and the Scopia Desktop Server. These certificates also secure all web traffic to the Scopia Desktop Server, for example, when you access the server's web administration user interface or when a user accesses their meeting portal.
- Install certificates in the server's keystore file, part of the Java installation, to secure communications with Scopia Management and other components. Mutual authentication requires a certificate stored on each side of the communication line.

The details of each certificate type and their configuration are detailed in the sections below:

Navigation

Securing Web Connections and Media Traffic to Scopia Desktop Server

About this task

This procedure explains how to secure all web traffic to the Scopia Desktop Server with HTTPS, including the administrator interface and user portals. This also secures the actual media (audio and video) of any videoconferences which take place.

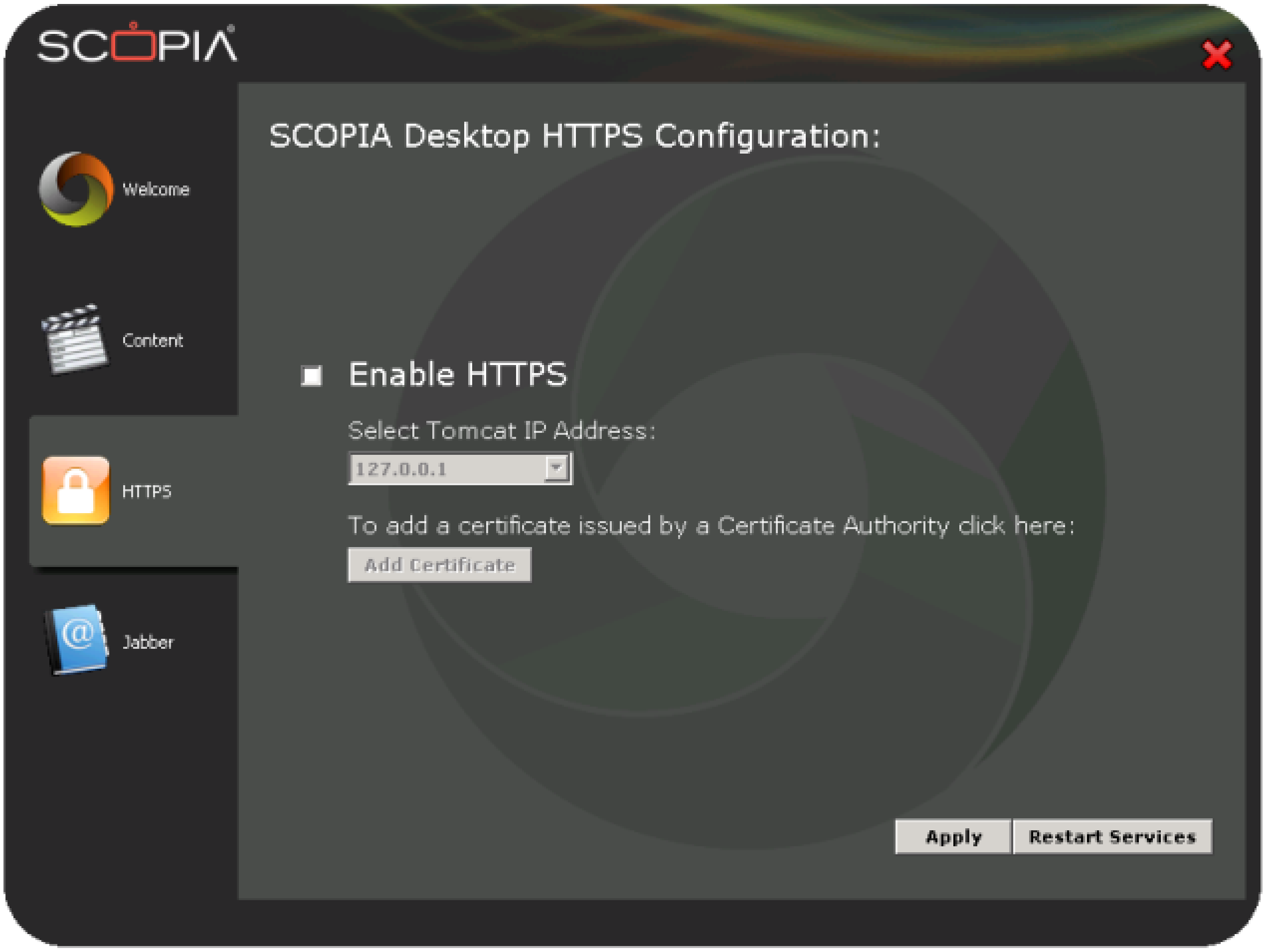
The certificate which secures web traffic and videoconference media is installed in the Scopia Desktop Conference Server.

Important:

This procedure requires a signed certificate ready for the Scopia Desktop Server. You can either use the certificate shipped with the server, or create your own unique certificate.

Procedure

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



SCOPIA Desktop HTTPS Configuration:

■ Enable HTTPS

Select Tomcat IP Address: 127.0.0.1

To add a certificate issued by a Certificate Authority click here:

Figure 75: Adding a certificate to Scopia Desktop Server

3. Select **Apply**.
4. Select **Add Certificate** to upload an existing signed certificate.
5. Stop the service **Scopia Desktop Conference Server**.
6. Navigate to *<SD_install_dir>\Confsrv*
7. Run the **Certificate Configuration Utility** by launching *CertificateConfiguration.exe* file.
8. If the certificate is installed in the local machine's certificate store:
   a. Select the **Configure Certificate via Certificate Store**
   b. Select **Select Certificate**.
   c. Select the certificate from the list.

9. If the certificate is in PKCS12 format:
    a. Select **Configure Certificate via File Name**.
    b. Browse to the PKCS12 certificate and select it.
    c. Enter the private key password for the certificate.
10. Select **OK**.
11. Verify that the certificate information is listed in the **Selected Certificate** pane.
12. Select **Apply**.
13. Select **OK**.
14. Select **OK**.
15. Start the service **Scopia Desktop Conference Server**.
16. Select **Restart Services**.
17. Change the URL in the **Invitations** section of the Scopia Desktop Administration web interface to use the secure HTTPS protocol:
    a. Log into the Scopia Desktop Administration web interface.
    b. Select **Messages and Invitations** on the sidebar.
    c. Select the **Invitations** tab.
    d. In the **Desktop Access** section, verify all URLs have the prefix of `https`.

    ❗ **Important:**

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

Securing Scopia Desktop Server’s Connection to other Components

About this task

You can secure the management communication sent between Scopia Desktop Server and other components like Scopia Management with TLS encryption. This method also checks the data integrity of messages.

Mutual authentication would require a certificate on each side of the connection. On Scopia Desktop Server, use the `keytool` utility, which is part of the Java installation. For more information about securing Scopia Management’s connections with other components, see the *Administration Guide for Scopia Management*.

To open a mutually authenticated TLS connection, each server authenticates the other by exchanging certificates.

Important:

Scopia Desktop Server is shipped with a pre-created and pre-installed certificate, but its encryption keys are non-unique.

To create certificates with unique keys for true authentication (step 3 onwards), you must first remove the pre-installed certificates held in `keytool`'s `.keystore` file, then generate and install new unique certificates.

The password on the `.keystore` file is `radvision`.

This section does not explain each of the parameters of the keytool command. For a full description of this Java utility, see http://java.sun.com/j2se/1.4.2/search.html.

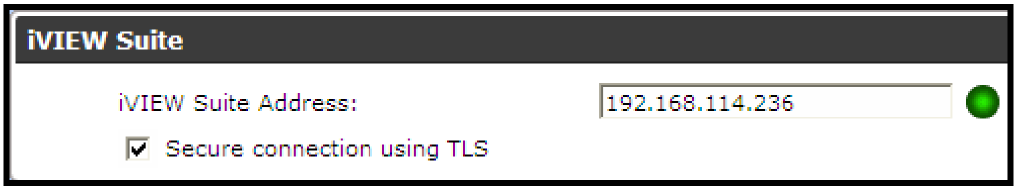
Procedure

1. Enable the management encryption on the Scopia Desktop Server side:

   a. Access the Scopia Desktop Server Administrator web user interface, as described in Accessing the Scopia Desktop Server Web Administration Interface on page 66.

   b. Select the **Deployment** icon on the sidebar.

   c. Select the **Secure connection using TLS** check box in the **iVIEW Suite** section.



iVIEW Suite

iVIEW Suite Address: 192.168.114.236

☑ Secure connection using TLS

Figure 76: Secure Connection Check Box

   d. Select **OK**.

2. On the side of Scopia Management, enable the management encryption connection:

   a. Access the Scopia Management Administrator portal.

   b. Select the **Devices** tab.

   c. Select the Scopia Desktop Server whose communications you want to encrypt.

   d. Select the check box **Secure connection between this server and Scopia Management using TLS**.

   e. Select **OK**.

3. Stop the **Scopia Desktop - Apache Tomcat** service.

4. Copy the `.keystore` file located in *<SD_install_dir>\data\sds.keystore* to a temporary working folder, for example *C:\cert*. The keystore file holds the certificates on each server. Currently they hold the default non-unique certificates.

5. Open a command line window. The `keytool` utility is located in *<SD_install_dir>\JRE\bin*.

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

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

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

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

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

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

9. Send the certificate request to a Certificate Authority.

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

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

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

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

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

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

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

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

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

14. Restart the services on the Scopia Management and Scopia Desktop Server computers.

Securing Login Access to Scopia Desktop Server using IWA

About this task

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

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

Important:

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

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

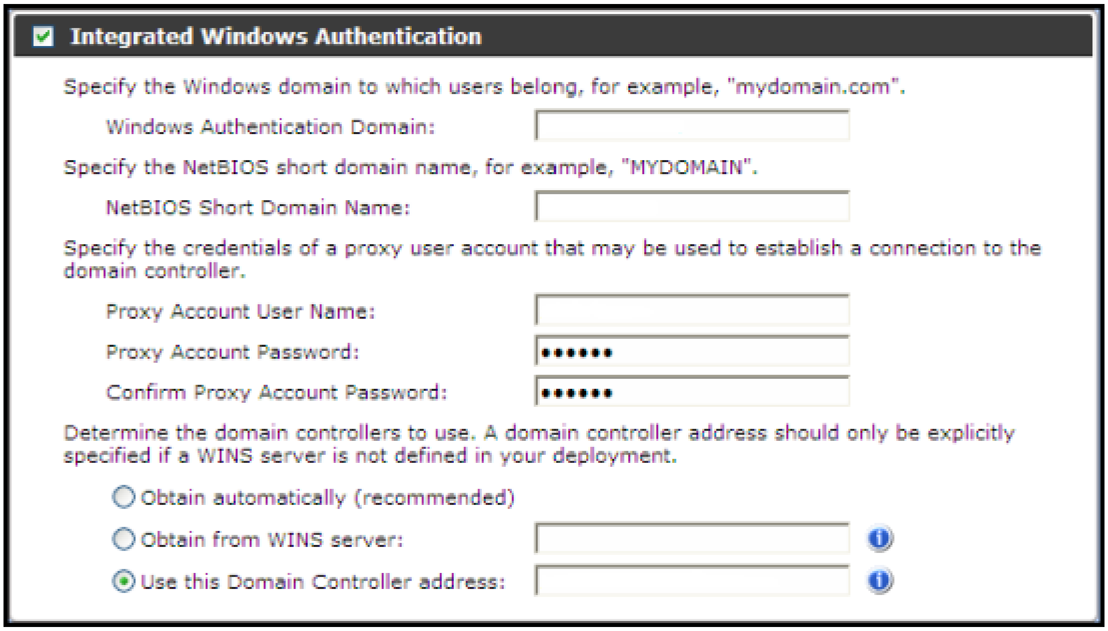
Before you begin

Ensure that authentication settings are configured for Scopia Management.

Procedure

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

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



☑ **Integrated Windows Authentication**

Specify the Windows domain to which users belong, for example, "mydomain.com".

Windows Authentication Domain:

Specify the NetBIOS short domain name, for example, "MYDOMAIN".

NetBIOS Short Domain Name:

Specify the credentials of a proxy user account that may be used to establish a connection to the domain controller.

Proxy Account User Name:

Proxy Account Password: ••••••

Confirm Proxy Account Password: ••••••

Determine the domain controllers to use. A domain controller address should only be explicitly specified if a WINS server is not defined in your deployment.

○ Obtain automatically (recommended)

○ Obtain from WINS server:

● Use this Domain Controller address:

Figure 77: Enabling single sign-on with IWA

4. Configure the Integrated Windows Authentication as detailed in Table 22: Configuring IWA on page 103.

Table 22: Configuring IWA

Field	Description
Windows Authentication Domain	Enter the Windows domain used to authenticate logins. Usually this is the full name of the Domain Controllers (DC) in the LDAP directory which governs the users accessing this server. For example, if you have a DC=*com* and DC=*companyname*, the full domain would be *companyname.com*.
NetBIOS Short Domain Name	Enter the NetBIOS domain name, which is the `USERDOMAIN` environment variable. To view, open a command line window and enter `set u` at the prompt. The system lists environment variables beginning with 'u', including `USERDOMAIN`. This name is case sensitive.
Proxy Account User Name	Enter the username of a proxy account which can remotely access the Domain Controller to authenticate remote logins. Proxy accounts are sometimes set up to enable remote users to login.
Proxy Account Password **Confirm Proxy Account Password**	The password of the proxy account to remotely access the Domain Controller.
Obtain Automatically (recommended)	Select this option to use the current address used by Windows to access the Domain Controller for authenticating users. Typically this is the Active Directory server.
Obtain from WINS server	Select this option to enter the location of a WINS server deployed in your organization, with access details of the Domain Controller. A WINS server resolves NetBIOS names and domains into IP addresses. To enter more than one WINS server, enter each location separated by a comma.
Use this Domain Controller address	Manually specify the address of the Domain Controller to be used to authenticate usernames and passwords.

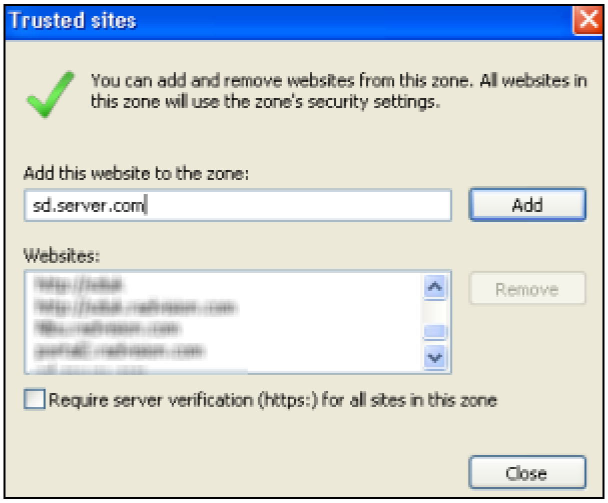
5. On the Scopia Desktop Client, verify that Integrated Windows Authentication is enabled in Internet Explorer:

   a. In the Internet Explorer window, select **Tools > Internet Options > Advanced**.

   b. Under **Security** section, verify that **Enable Integrated Windows Authentication** is selected.

6. Add Scopia Desktop Server to the list of Internet Explorer trusted sites on Scopia Desktop Client:

   a. In the Internet Explorer window, from **Tools > Internet Options > Security > Trusted Sites > Sites**.


Trusted sites

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone: sd.server.com

Websites:

□ Require server verification (https:) for all sites in this zone

Figure 78: Adding Scopia Desktop Server as a trusted site

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

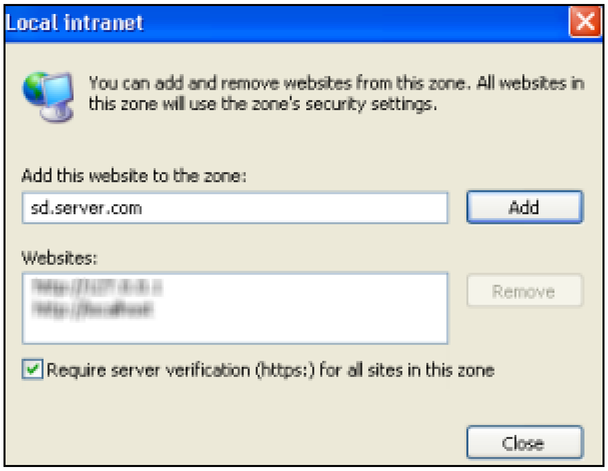
c. Select **Custom level**.

d. Under the **User Authentication** section, select **Automatic logon with current user name and password**.

e. Select **OK**.

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

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


Local intranet

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone: sd.server.com

Websites:

☑ Require server verification (https:) for all sites in this zone

Figure 79: Adding Scopia Desktop Server as a trusted intranet site

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

c. Select **Custom level**.

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

e. Select **OK**.

Chapter 6 | Deploying Multiple Scopia Desktop Servers with a Load Balancer

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

You can deploy multiple Scopia Desktop Servers in a number of ways (see Planning your Scopia Desktop Server Deployment on page 9), including managing a set of servers with a load balancer. A load balancer groups together a set (or cluster) of servers to give them a single IP address, known as a virtual IP address. In this way, other components in the solution relate to the cluster as though they were a single server (Figure 80: Scopia Desktop Servers with load balancer on page 105).

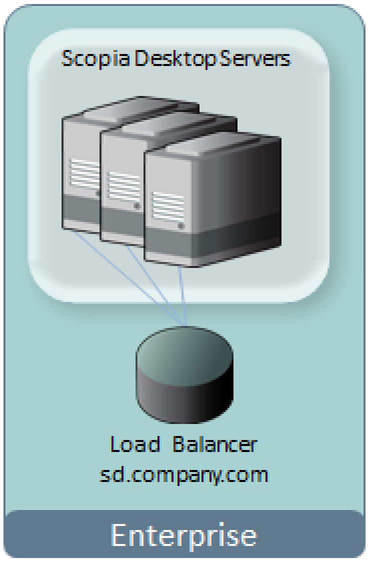


Figure 80: Scopia Desktop Servers with load balancer

A load balancer groups together a set (or cluster) of servers to give them a single IP address, known as a virtual IP address. It distributes client service requests amongst a group of servers. It distributes loads according to different criteria such as bandwidth, CPU usage, or cyclic (round robin). Load balancers are also known as application delivery controllers (ADC).

Important:

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

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

All servers in the cluster should have identical functionality enabled, since one server must take over if another is overloaded or fails. If you deploy dedicated servers for the different components of Scopia Desktop (for example, a dedicated recording or streaming server), these dedicated servers should be located outside the cluster. For more information, see Configuring Streaming and Recording in a Load Balancing Environment on page 119.

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

Navigation

1. Configuring Scopia Desktop Server for Load Balancing on page 106
2. Configuring Radware AppDirector on page 110
3. Configuring Other Load Balancers on page 117
4. Configuring Streaming and Recording in a Load Balancing Environment on page 119
5. Securing a Load Balanced Environment on page 122

Configuring Scopia Desktop Server for Load Balancing

About this task

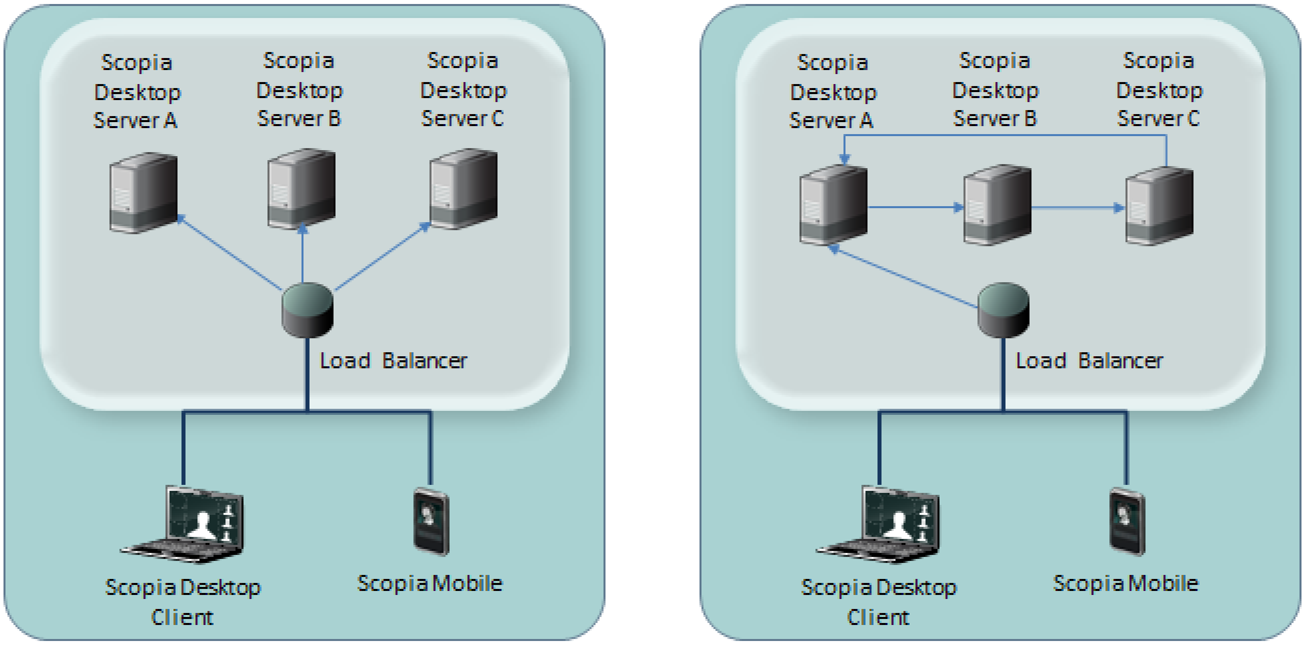
For scalability and high availability, you can deploy multiple Scopia Desktop Servers with a load balancer. This section focuses on configuring settings on the Scopia Desktop Servers. For configuring load balancer settings, see Configuring Radware AppDirector on page 110 or Configuring Other Load Balancers on page 117.

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

When a participant requests to join a videoconference on an overflowing server, the server (not the load balancer, but the server itself) points to another server in the cluster, enabling the participant to join the same meeting from a second server. Redirecting participants in the same conference can only be done from within the Scopia Desktop Server which hosts the videoconference (Figure 81: Redirecting participants in a load balanced environment on page 107).

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

For example, in a new videoconference the load balancer uses the configured load distribution algorithm (such as round robin or least traffic) to forward the first participant to server A (Figure 81: Redirecting participants in a load balanced environment on page 107). The load balancer then forwards subsequent participants of the same videoconference to the same server. If server A runs out of ports, configure it to redirect calls to the next server in the cluster (or farm):



Load balancer redirection of different videoconferences

Server redirection within the same videoconference

Figure 81: Redirecting participants in a load balanced environment

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

The Scopia Solution allows both registered participants and guests to join a videoconference. To further improve registered user experience, all servers in the group must share the meeting login of registered users. Otherwise, participants might have to re-enter their credentials when the load balancer routes calls to other servers in the farm. Therefore, enable the underlying Tomcat clustering in each Scopia Desktop Server (About Components of the Scopia Desktop Server on page 6), so participants enter their username and password only once when they join the videoconference.

Important:

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

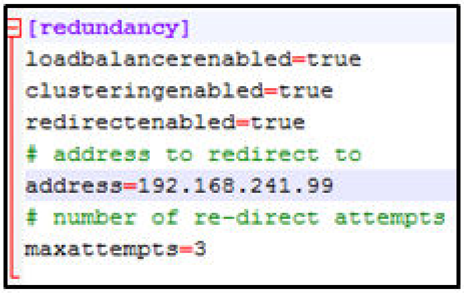
This procedure describes how to configure Scopia Desktop Server redirection for participants within the same videoconference, for deployment with any type of load balancer.

Before you begin

1. Plan your load balancer deployment as part of your overall topology. For more information, see Planning your Scopia Desktop Server Deployment on page 9.
2. Configure the Scopia Desktop Server's basic settings as described in *Administrator Guide for Scopia Desktop Server*.
3. Read Deploying Multiple Scopia Desktop Servers with a Load Balancer on page 105 for an overview on load balancing in the Scopia Desktop deployment.
4. Remember to back up any settings file which you edit as part of this procedure.

Procedure

1. Open the *ctmx.ini* file located in *<install directory>\data\*
2. Locate the `[redundancy]` section of the file (Figure 82: The redundancy section in the ctmx.ini file on page 108).



```
[redundancy]
loadbalancerenabled=true
clusteringenabled=true
redirectenabled=true
# address to redirect to
address=192.168.241.99
# number of re-direct attempts
maxattempts=3
```

Figure 82: The redundancy section in the ctmx.ini file

3. Set `loadbalancerenabled` to `true` (Figure 82: The redundancy section in the ctmx.ini file on page 108).
4. Set `redirectenabled` to `true` (Figure 82: The redundancy section in the ctmx.ini file on page 108).
5. In the `address` line, enter the address (either IP or FQDN) of the server to which the system redirects a participant of the same call when this server is full. Redirect each server to the next one in line (Figure 81: Redirecting participants in a load balanced environment on page 107). You must specify only one redirection address in each server.

   For example, the server's address has one of these formats:

   - IP address:

     ```
     address=192.168.241.99
     ```

   - FQDN:

     ```
     address=scopiaserver1.com
     ```

   - IP address with port when the port is not the default:

     ```
     address=192.168.241.99:8080
     ```

6. Enter the maximum number of redirections in `maxattempts` (Figure 82: The redundancy section in the ctmx.ini file on page 108). Keep this number consistent in all the servers across the deployment to ensure a predictable redirection behavior.

   To prevent an infinite loop, limit the total number of redirections to the total number of Scopia Desktop Servers in the deployment.

7. (Required only if you have registered SDC users with usernames and passwords.) Enable Tomcat clustering in Scopia Desktop Server with full memory replication of sessions. For more information, see http://tomcat.apache.org.

   a. In the same `[redundancy]` section, set `clusteringenabled` to `true` (Figure 82: The redundancy section in the ctmx.ini file on page 108).

b. Save and close the *ctmx.ini* file.

c. Open the *server.xml* file located in *<install directory>\tomcat\conf\*

d. Locate the text `<Cluster` (without the close bracket '>').

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

f. Replace that element with the following code:

```
<Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster" channelSendOptions="8">
  <Manager className="org.apache.catalina.ha.session.DeltaManager"
              expireSessionsOnShutdown="false" notifyListenersOnReplication="true"/>
  <Channel className="org.apache.catalina.tribes.group.GroupChannel">
    <Membership className="org.apache.catalina.tribes.membership.McastService"
              address="228.0.0.4" port="45564" frequency="500" dropTime="3000"/>
    <Receiver className="org.apache.catalina.tribes.transport.nio.NioReceiver"
              address="auto" port="4000" autoBind="100" selectorTimeout="5000" maxThreads="6"/>
    <Sender className="org.apache.catalina.tribes.transport.ReplicationTransmitter">
      <Transport className="org.apache.catalina.tribes.transport.nio.PooledParallelSender"/>
    </Sender>
    <Interceptor className="org.apache.catalina.tribes.group.interceptors.TcpFailureDetector"/>
    <Interceptor className="org.apache.catalina.tribes.group.interceptors.MessageDispatch15Interceptor"/>
  </Channel>
  <Valve className="org.apache.catalina.ha.tcp.ReplicationValve" filter=""/>
  <Valve className="org.apache.catalina.ha.session.JvmRouteBinderValve"/>
  <Deployer className="org.apache.catalina.ha.deploy.FarmWarDeployer"
              tempDir="/tmp/war-temp/" deployDir="/tmp/war-deploy/" watchDir="/tmp/war-listen/"
              watchEnabled="false"/>
  <ClusterListener className="org.apache.catalina.ha.session.JvmRouteSessionIDBinderListener"/>
  <ClusterListener className="org.apache.catalina.ha.session.ClusterSessionListener"/>
</Cluster>
```

g. Save and close the file.

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

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

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

j. Save and close the file.

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

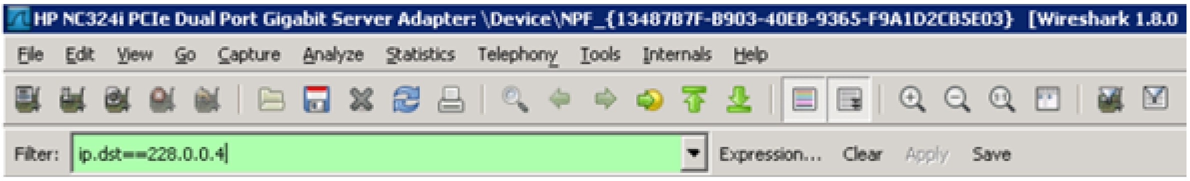
l. Save and close the file.

8. Restart the **Scopia Desktop – Apache Tomcat** service.

9. Repeat the above procedure for each Scopia Desktop Server in the group.

10. (Optional) To verify whether the cluster is correctly configured on all the servers, you can perform your own stress tests and capture network traces using the Wireshark filter `ip.dst filter==228.0.0.4` which presents the cluster's synchronization traffic (or "heartbeat").

    For example, enter the filter to verify that each server in the cluster broadcasts a message every 0.5 seconds to the specified IP address (Figure 83: Capturing network traces on page 110).



HP NC324i PCIe Dual Port Gigabit Server Adapter: \Device\NPF_{134B7B7F-B903-40EB-9365-F9A1D2CB5E03} [Wireshark 1.8.0

Filter: ip.dst==228.0.0.4

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Figure 83: Capturing network traces

11. Configure the load balancer used in your deployment (see Configuring Radware AppDirector on page 110 or Configuring Other Load Balancers on page 117).

Configuring Radware AppDirector

About this task

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

You can configure AppDirector to route all network traffic or part of it (Figure 84: Media can either bypass or travel via the load balancer on page 111) depending on your deployment requirements:

- In full load balancing deployments, all network traffic between servers and clients, including the media (audio, video, data presentations), is routed via the load balancer. This is best for powerful load balancer servers, and has the added security advantage of withholding the private IP of a Scopia Desktop Server to the outside world.
- In partial load balancing deployments, the media data travels directly between client and server, bypassing the load balancer, while signaling and management still travel via the load balancer. This is better for less powerful load balancer computers, but directly exposes the servers' private IP addresses to the outside world.

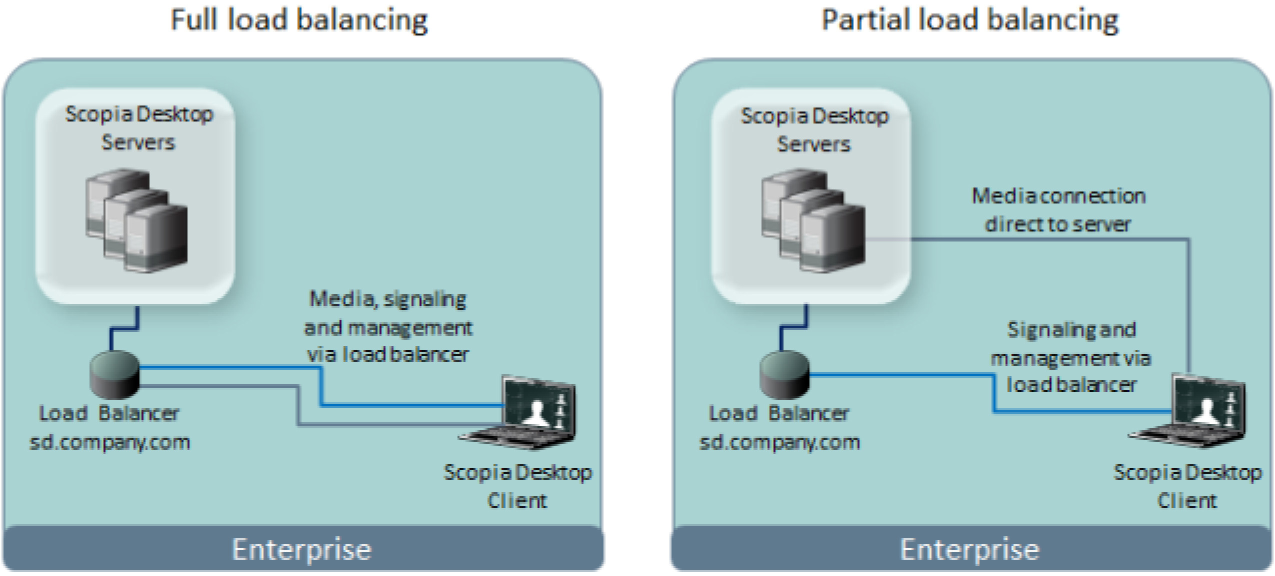

Full load balancing
Scopia Desktop Servers
Media, signaling and management via load balancer
Load Balancer sd.company.com
Scopia Desktop Client
Enterprise
Partial load balancing
Scopia Desktop Servers
Media connection direct to server
Signaling and management via load balancer
Load Balancer sd.company.com
Scopia Desktop Client
Enterprise

Figure 84: Media can either bypass or travel via the load balancer

Important:

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

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

Important:

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

Before you begin

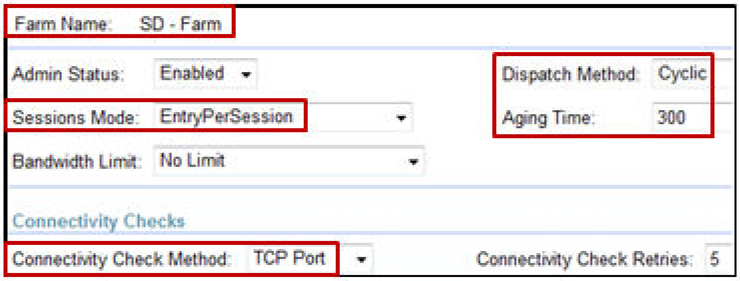
1. Plan your load balancer deployment as part of your overall topology. For more information, see Planning your Scopia Desktop Server Deployment on page 9.
2. Configure the Scopia Desktop Server's basic settings as described in *Administrator Guide for Scopia Desktop Server*.
3. Read Deploying Multiple Scopia Desktop Servers with a Load Balancer on page 105 for an overview on load balancing in the Scopia Desktop deployment.
4. Follow the procedure in Configuring Scopia Desktop Server for Load Balancing on page 106 to configure settings on each Scopia Desktop Server.

Procedure

1. Login to AppDirector.
2. Configure the server farm in the load balancer. The farm is the AppDirector's terminology of a cluster of servers. It is a virtual entity that integrates one or more physical servers.

   a. Create a farm by selecting **AppDirector > Farms > Farm Table > Create**.

b. Enter the basic settings for this server farm (Figure 85: Configuring the virtual farm on page 112 and Table 23: The virtual farm settings on page 112).



Farm Name: SD - Farm

Admin Status: Enabled

Sessions Mode: EntryPerSession

Bandwidth Limit: No Limit

Dispatch Method: Cyclic

Aging Time: 300

Connectivity Checks

Connectivity Check Method: TCP Port

Connectivity Check Retries: 5

Figure 85: Configuring the virtual farm

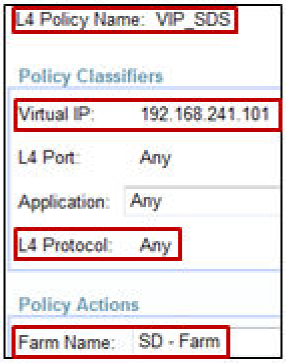
Table 23: The virtual farm settings

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

3. Configure the Layer 4 rules (or policies) the load balancer uses to manage traffic. AppDirector uses the Layer 4 protocol and the request’s destination port to select the farm.

   a. Create a policy by selecting **AppDirector > Layer 4 Traffic Redirection > Layer 4 Policies > Create**.

   b. Enter the basic settings for this policy (Figure 86: Configuring the Layer 4 Policies on page 113 and Table 24: The Layer 4 Policy settings on page 113).



L4 Policy Name: VIP_SDS

Virtual IP: 192.168.241.101

L4 Port: Any

Application: Any

L4 Protocol: Any

Farm Name: SD - Farm

Figure 86: Configuring the Layer 4 Policies

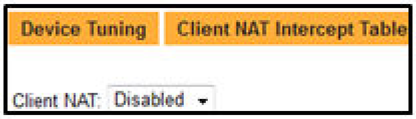
Table 24: The Layer 4 Policy settings

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

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

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

   a. Verify the **Client NAT** in **AppDirector > NAT > Client NAT > Global Parameters** is disabled (Figure 89: Enabling Client NAT on page 114).

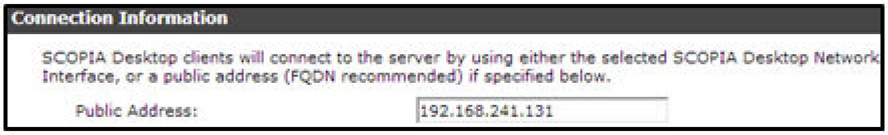


Client NAT: Disabled

Figure 87: Disabling Client NAT

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

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



Connection Information

SCOPIA Desktop clients will connect to the server by using either the selected SCOPIA Desktop Network Interface, or a public address (FQDN recommended) if specified below.

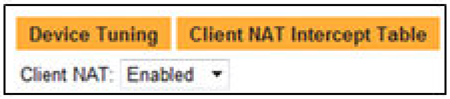
Public Address: 192.168.241.131

Figure 88: Configuring direct media traffic between client and server

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

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

a. Enable **Client NAT** in **AppDirector > NAT > Client NAT > Global Parameters** (Figure 89: Enabling Client NAT on page 114).

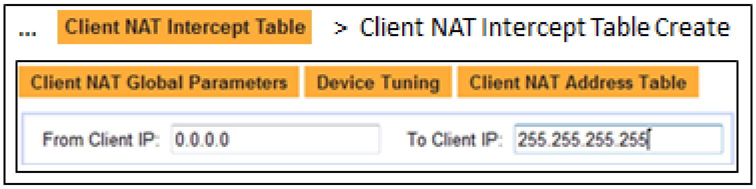


Client NAT: Enabled

Figure 89: Enabling Client NAT

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

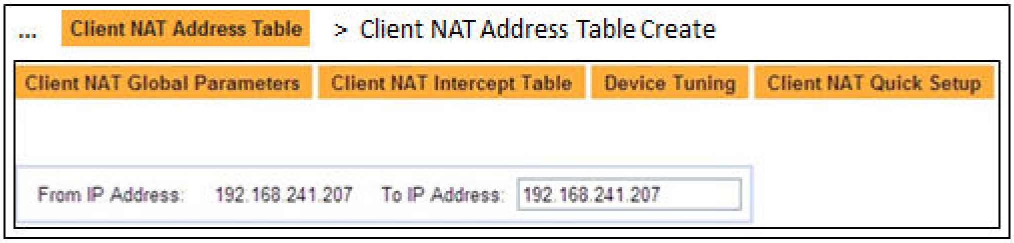
b. Configure the range of client IP addresses on which the system performs NAT by selecting **Client NAT Intercept Table** (Figure 90: The Client NAT Intercept Table on page 114).


...
Client NAT Intercept Table
> Client NAT Intercept Table Create
Client NAT Global Parameters
Device Tuning
Client NAT Address Table

From Client IP: 0.0.0.0 To Client IP: 255.255.255.255

Figure 90: The Client NAT Intercept Table

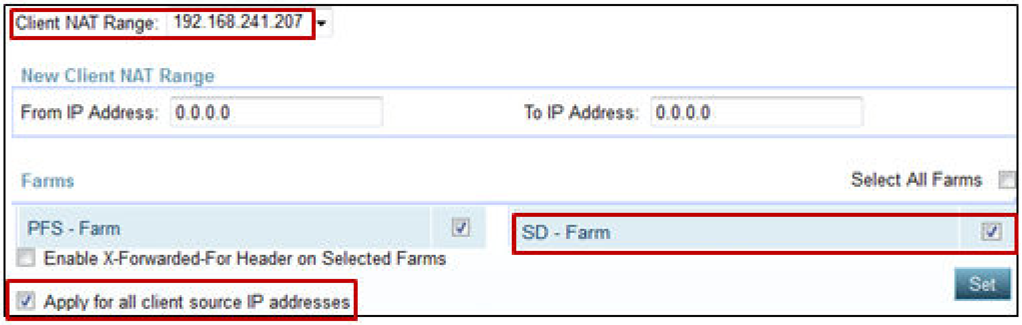
c. Configure the NAT IP addresses in **Client NAT Address Table** (Figure 91: The Client NAT Address Table on page 114). The load balancer replaces the client IP address calling into the farm with the load balancer IP address. Usually you configure both fields to the same IP address (the load balancer's IP address).


...
Client NAT Address Table
> Client NAT Address Table Create
Client NAT Global Parameters
Client NAT Intercept Table
Device Tuning
Client NAT Quick Setup

From IP Address: 192.168.241.207 To IP Address: 192.168.241.207

Figure 91: The Client NAT Address Table

d. Configure the Client NAT's basic settings in **Client NAT Quick Setup** (Figure 92: The Client NAT Quick Setup window on page 115.



Client NAT Range: 192.168.241.207

New Client NAT Range

From IP Address: 0.0.0.0

To IP Address: 0.0.0.0

Farms

Select All Farms □

PFS - Farm ☑

SD - Farm ☑

□ Enable X-Forwarded-For Header on Selected Farms

☑ Apply for all client source IP addresses

Figure 92: The Client NAT Quick Setup window

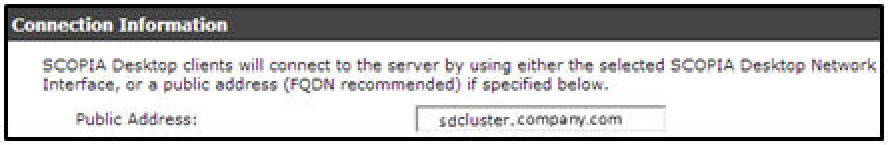
Fill the fields as described in Table 25: The Client NAT Quick Setup settings on page 115.

Table 25: The Client NAT Quick Setup settings

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

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

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



Connection Information

SCOPIA Desktop clients will connect to the server by using either the selected SCOPIA Desktop Network Interface, or a public address (FQDN recommended) if specified below.

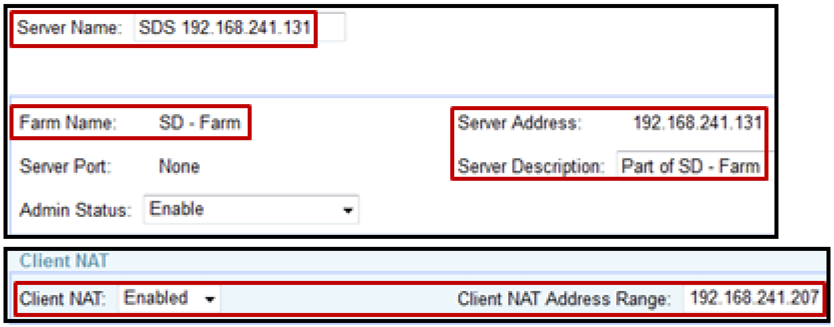
Public Address: sdcluster.company.com

Figure 93: Routing media traffic through the load balancer

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

6. Add each Scopia Desktop Server to the farm.

a. Enter the server details in **AppDirector > Servers > Application Servers > Table > Create** (Figure 94: Configuring the server table on page 116 and Table 26: The server table settings on page 116).



Server Name: SDS 192.168.241.131

Farm Name: SD - Farm

Server Port: None

Admin Status: Enable

Server Address: 192.168.241.131

Server Description: Part of SD - Farm

Client NAT

Client NAT: Enabled

Client NAT Address Range: 192.168.241.207

Figure 94: Configuring the server table

Table 26: The server table settings

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

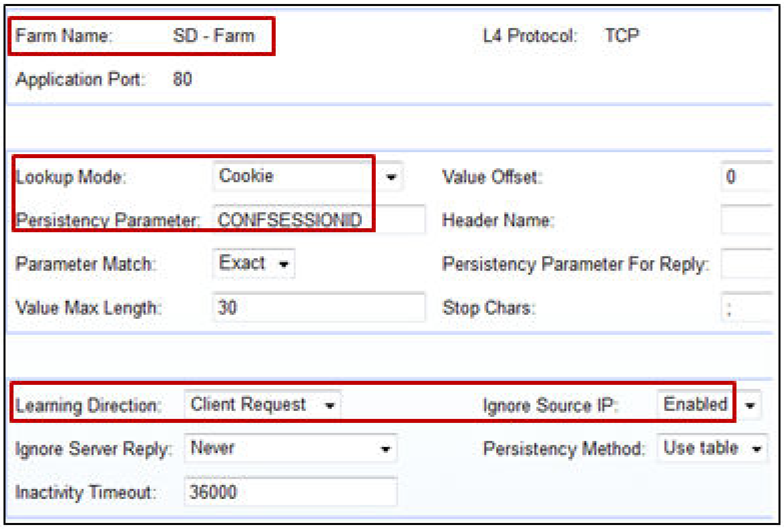
b. Repeat these steps for each Scopia Desktop Server in the farm.

7. Configure cookie persistency in the load balancer.

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

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

   b. Enter the rule's basic settings (Figure 95: Configuring session persistency on page 117 and Table 27: The session persistency settings on page 117).



Farm Name: SD - Farm
L4 Protocol: TCP
Application Port: 80

Lookup Mode: Cookie
Value Offset: 0
Persistency Parameter: CONFSESSIONID
Header Name:
Parameter Match: Exact
Persistency Parameter For Reply:
Value Max Length: 30
Stop Chars: ;

Learning Direction: Client Request
Ignore Source IP: Enabled
Ignore Server Reply: Never
Persistency Method: Use table
Inactivity Timeout: 36000

Figure 95: Configuring session persistency

Table 27: The session persistency settings

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

Configuring Other Load Balancers

About this task

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

This procedure describes how to configure load balancers other than AppDirector to correctly route calls to the Scopia Desktop Servers. If your deployment uses AppDirector, see Configuring Radware AppDirector on page 110.

Important:

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

Before you begin

- Plan your load balancer deployment as part of your overall topology. For more information, see Planning your Scopia Desktop Server Deployment on page 9.
- Configure the Scopia Desktop Server's basic settings as described in *Administrator Guide for Scopia Desktop Server*.
- Read Deploying Multiple Scopia Desktop Servers with a Load Balancer on page 105 for an overview on load balancing in the Scopia Desktop deployment.
- Perform the procedure in Configuring Scopia Desktop Server for Load Balancing on page 106.

Procedure

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

   Scopia Desktop Clients use the VIP to reach that cluster.

2. Select a routing method for the load balancer.

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

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

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

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

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

   Important:

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

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

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

Configuring Streaming and Recording in a Load Balancing Environment

About this task

Scopia Desktop Server allows users to record meetings and to view recorded meetings. A recorded Scopia Desktop videoconference can be played at any time. Recordings include audio, video, and shared data (if participants present data during the videoconference).

Scopia Desktop Server's streaming functionality enables viewers to watch a webcast. A Scopia Desktop webcast is a live broadcast of a Scopia Desktop videoconference over the internet. Viewers of the webcast cannot interact with other participants in the meeting.

To view a webcast, you can use any client that accepts Real Time Streaming Protocol (RTSP), such as Apple Quicktime.

Scopia Desktop Server includes the Recording and Streaming Server components. You can enable this functionality within Scopia Desktop Server, or you can deploy dedicated recording and streaming servers. For more information, see Medium Scopia Desktop Server Deployment with Dedicated Servers on page 15.

To configure a streaming and/or recording server in a load balancing environment, you can:

- Point all Scopia Desktop Servers in the cluster to a single dedicated streaming and/or recording server outside the cluster. The playback client communicates directly with the dedicated server.
- Enable streaming capabilities in each Scopia Desktop Server in the cluster.

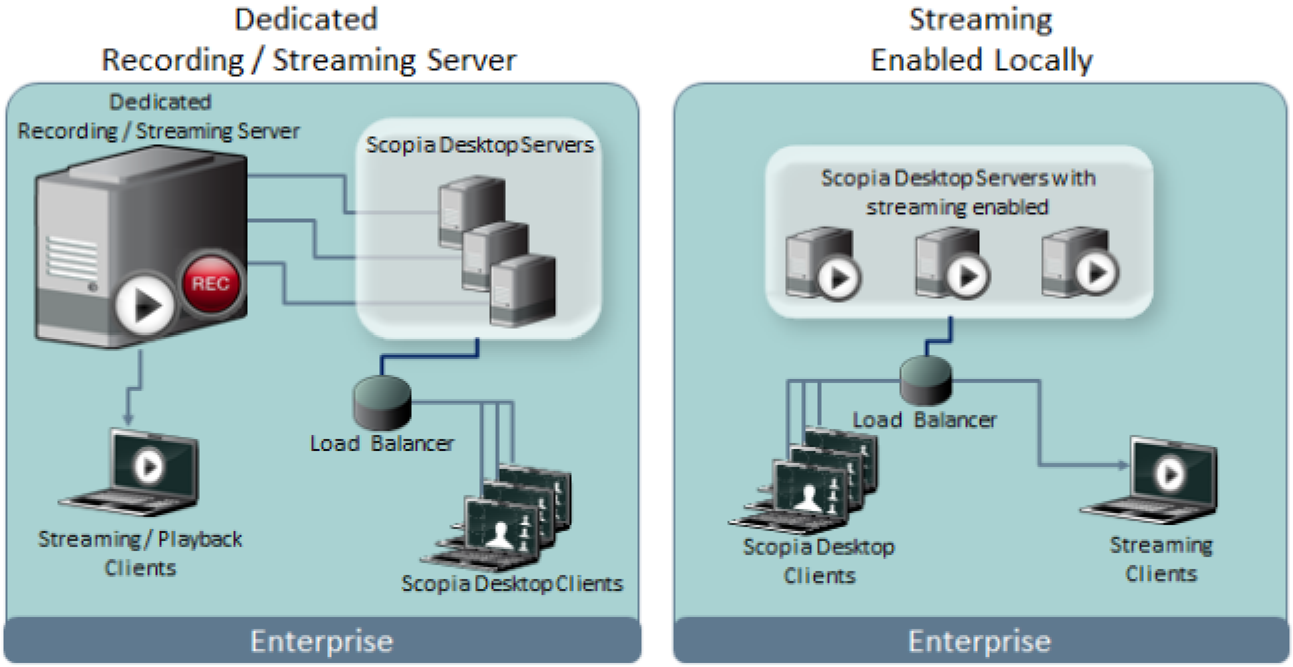


Figure 96: Dedicated recording/streaming, or local streaming

With a dedicated Recording or Streaming Server, you also need to list the Scopia Desktop Servers allowed to access it, by editing its access control list using the Scopia Desktop Server Configuration Tool. Furthermore, the number of simultaneous streaming and/or recording clients depends on the license enabled in the dedicated server. For example, if you install a 600-port streaming server, it can communicate with 600 streaming clients.

With streaming enabled locally, the number of simultaneous streaming clients depends on the number of licensed streams per server times the number of servers in the cluster. For example, if each streaming server has 600 ports and you install three of them, they can communicate with 1800 streaming clients.

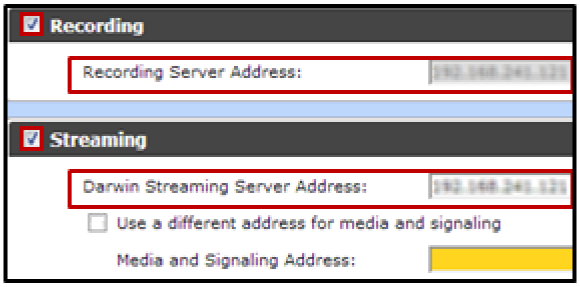
This section describes how to either point the servers to a dedicated streaming/recording server, or locally enable streaming on each server in the farm.

Before you begin

For an overview of the recording and streaming components in Scopia Desktop Servers, see About Components of the Scopia Desktop Server on page 6.

Procedure

1. Access the Scopia Desktop Server administrator portal.
2. Select **Deployment** in the sidebar menu (Figure 97: Recording and streaming on page 121).



☑ Recording

Recording Server Address: [redacted]

☑ Streaming

Darwin Streaming Server Address: [redacted]

□ Use a different address for media and signaling

Media and Signaling Address:

Figure 97: Recording and streaming

3. Enter the settings for the dedicated or local Scopia Desktop Server:

Table 28: Recording and streaming settings

Field Name	Description
Recording	Select the checkbox to enable recording in the dedicated server.
Streaming	Select the checkbox to enable streaming in the dedicated or local server.
Recording Server Address	Enter the IP address of the server used for recording (either this server or a dedicated recording server).
Darwin Streaming Server Address	Enter the IP address of the dedicated or local server.

4. Select **Ok** or **Apply**.

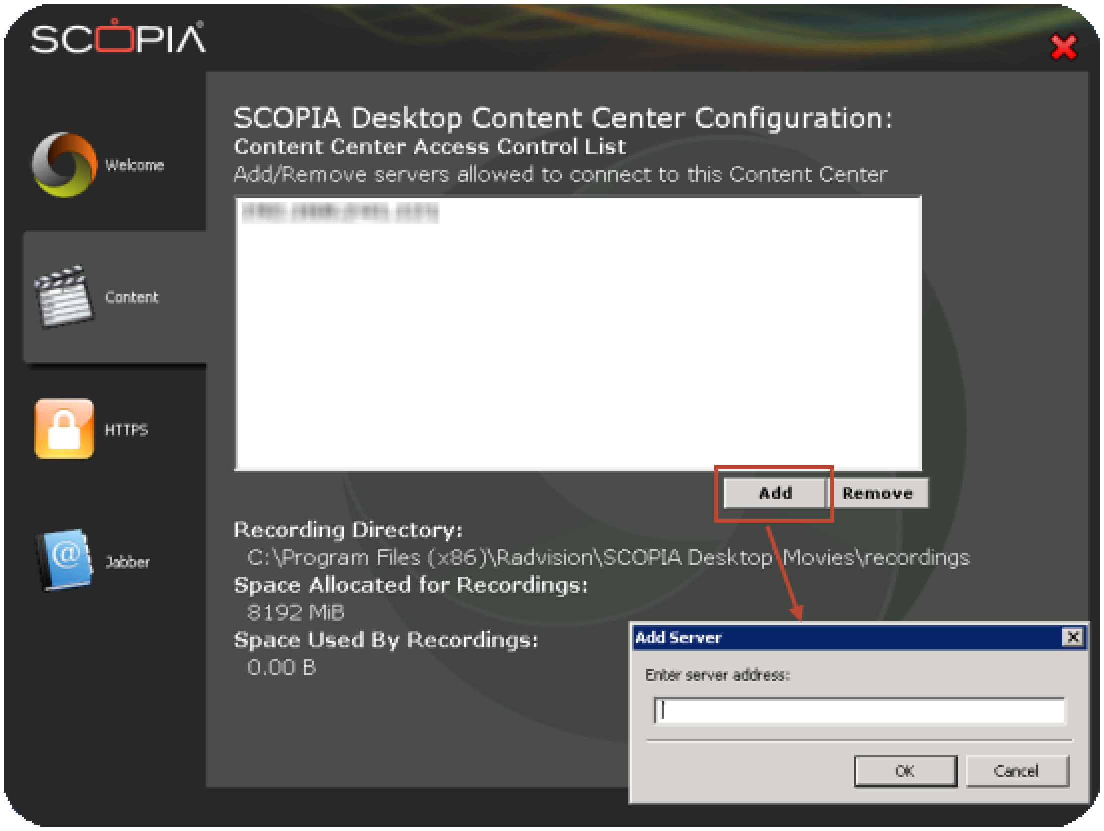
5. If you are configuring a streaming server locally, repeat the above steps for each Scopia Desktop Server in the cluster.

6. For any Scopia Desktop Server accessing a dedicated Content Center Server (recording or streaming), enter each Scopia Desktop Server IP address in the access control list using the Scopia Desktop Server Configuration Tool.

   a. On the dedicated Content Server for Scopia Desktop, select **Start > Programs > Scopia Desktop > ConfigTool**.

   b. Select **Content** in the sidebar.

   The system lists the IP addresses of the Scopia Desktop Servers allowed to access this Dedicated Content Server, as shown below.



SCOPIA Desktop Content Center Configuration:
Content Center Access Control List
Add/Remove servers allowed to connect to this Content Center

[redacted]

Recording Directory:
C:\Program Files (x86)\Radvision\SCOPIA Desktop\Movies\recordings
Space Allocated for Recordings:
8192 MiB
Space Used By Recordings:
0.00 B

Enter server address:

Figure 98: Enabling multiple Scopia Desktop Servers to access a Dedicated Content Server

c. Select **Add** to add the IP address of each Scopia Desktop Server using this Content Server.

d. Select **OK**.

Securing a Load Balanced Environment

You can route the media of a videoconference via the load balancer if its computer is powerful enough, or the media can bypass the load balancer creating a direct flow from the server to the Scopia Desktop Client (see Configuring Radware AppDirector on page 110).

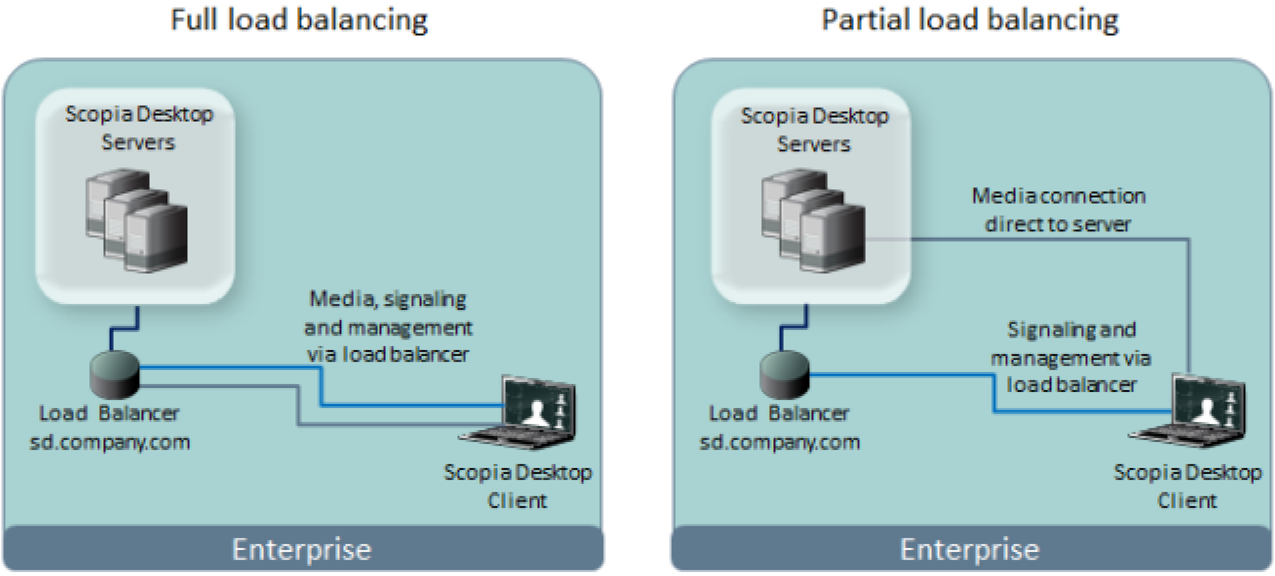

Full load balancing
Scopia Desktop Servers
Media, signaling and management via load balancer
Load Balancer sd.company.com
Scopia Desktop Client
Enterprise
Partial load balancing
Scopia Desktop Servers
Media connection direct to server
Signaling and management via load balancer
Load Balancer sd.company.com
Scopia Desktop Client
Enterprise

Figure 99: Media can either bypass or travel via the load balancer

When a device establishes a secure connection with another component, it sends a signed certificate verifying its identity. The signature on the certificate must be from a known (trusted) certification authority (CA).

Important:

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

- When media flows via the load balancer, install the Scopia Desktop Server certificates on the load balancer only (Figure 100: Encrypting communication with the load balancer certificate on page 123). If each server has its own certificate, install all of them on the load balancer. If they all share the same certificate, you only need to install it once.

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

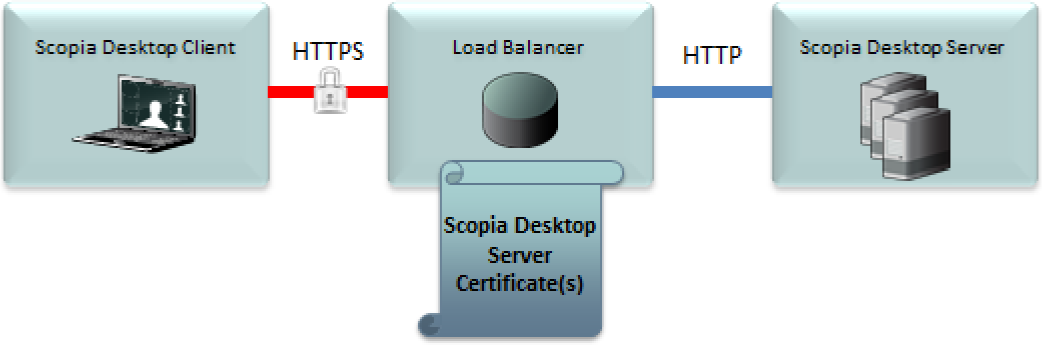


Figure 100: Encrypting communication with the load balancer certificate

- When media flows directly between client and server, bypassing the load balancer, install certificates both on the load balancer and the servers in the cluster (Figure 101: Encrypting communication with the load balancer and server certificates on page 124). As with the previous example, if all servers in the cluster share the same certificate, you only need to install that single certificate on the load balancer.

For more information on installing Scopia Desktop Server certificates, see Securing Your Scopia Desktop Deployment on page 97. To install certificates on your load balancer, see the load balancer documentation.

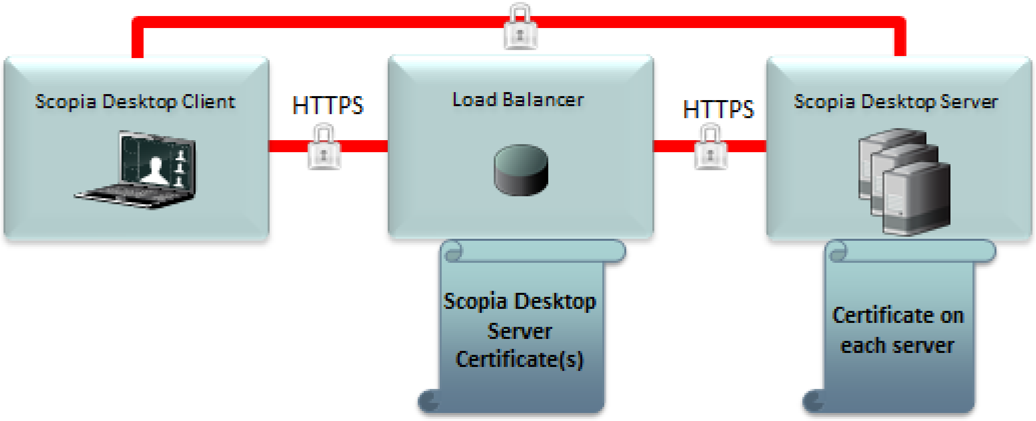


Figure 101: Encrypting communication with the load balancer and server certificates

❗ Important:

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

Glossary of Terms for Scopia Solution

1080p

See Full HD on page 129.

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 132.

AAC

AAC is an audio codec which compresses sound but with better results than MP3.

Alias

In H.323, an alias 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.

BFCP (Binary Floor Control Protocol)

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

Bitrate

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

Call Control

See Signaling on page 138.

Cascaded Videoconference

A cascaded videoconference is a meeting distributed over more than one physical 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 127.

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 various dial prefixes to determine the characteristics 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 to the start 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 28). 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 125.

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 endpoints, where the camera can be controlled remotely by another endpoint in the call.

Forward Error Correction

See FEC on page 128.

FPS

See Frames Per Second on page 129.

Frame Rate

See Frames Per Second on page 129.

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 participant or a composite of the other participants.

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 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 Scopia TIP Gateway, Radvision SIP Gateway, or the Scopia TIP Gateway.

GLAN

GLAN, or gigabit LAN, is the name of the network port on the Scopia 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.

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 131.

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 125.

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 Scopia PathFinder Server, where the endpoint acts as an H.460 client to the Scopia 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 132.

High Profile

See H.264 High Profile on page 131.

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 137.

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).

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.

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 many endpoints to a single videoconference. It typically manages the audio mixing and video layouts, adjusting the output to suit each endpoint's capabilities.

MCU service

See Meeting Type on page 134.

Media

Media refers to the live audio, video and shared data streams sent during a call. The shared data stream, like a presentation, is also known as dual video. Far end camera control (FECC) is another example of information carried on the data stream. Media is transmitted via the RTP and RTCP protocols in both SIP and H.323 calls.

Media Control

See Control on page 127.

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. Meeting types are created in the MCU. You can invoke a meeting type by dialing its prefix in front of the meeting ID.

Moderator

A moderator is a participant with special rights in a videoconference, including muting the sound and video of other participants, inviting new participants, disconnecting participants, defining a meeting PIN to restrict access, 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.

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 two images of the same size, presented side by side.

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. The image on the left is larger, with two smaller images on the right.

Prefix

See Dial Prefix on page 127.

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.

Recordings

A recording of a videoconference can be played back at any time. Recordings include audio, video and shared data (if presented). In Scopia Desktop, any participant with moderator rights can record a meeting. Users can access Scopia Desktop 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.

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.

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.

RTCP

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

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. During conversions from analog to digital sound, if you increase the frequency that audio data is collected, or "sampled", you increase the 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 126.

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 134.

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.

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 Scopia XT Series), an endpoint can be compatible with both protocols. As a protocol, it uses fewer resources than H.323.

SIP Server

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

SIP URI

See URI on page 142.

SIP Registrar

See Registrar on page 137.

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.

Slider

See Content Slider on page 126.

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.

SRTP

Secure Real-time Transport Protocol (SRTP) adds security to the standard RTP protocol, which is used to send video and audio data between devices in SIP calls using TLS. It offers security via encrypting, authenticating and ensuring message integrity.

SSO

See Single Sign On on page 139.

Standard Definition

See SD on page 138.

Streaming

Streaming is a method of delivering multimedia content in one direction. Streaming recipients cannot not use a microphone or camera to communicate back to the videoconference. The content can be a live videoconference, or it can be a stored recording.

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 increases 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.

SQCIF

SQCIF defines a video resolution of 128 x 96 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 MCU 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 like Scopia XT Telepresence 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.

TLS

TLS enables network devices to communicate securely by exchanging 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).

URI

URI is an address format to locate a device on a network. For a SIP call, the URI consists of the endpoint's name or number, followed by the SIP server domain name. For example, *<endpoint name>@<SIP server domain name>* or *user@domain_name.com*.

URI Dialing

Accessing a device via its URI on page 142.

VFU

See Video Fast Update (VFU) on page 142.

VGA

VGA defines a video resolution of 640 x 480 pixels.

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.

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 137.

Video Switching

See Switched video on page 141.

Virtual Room

A virtual room in Scopia Desktop and Scopia Mobile offers a virtual meeting place for ad-hoc 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.

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. A Scopia Desktop webcast becomes available when a participant in the videoconference enables the streaming feature. To invite users to the webcast, one of the participants attending the Scopia Desktop videoconference must send this information in an e-mail or an instant message:

- The link to the webcast

  or

- The 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 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.

RADVISION®
an Avaya company

About Radvision
Radvision, an Avaya company, is a leading provider of videoconferencing and telepresence technologies over IP and wireless networks. We offer end-to-end visual communications that help businesses collaborate more efficiently. Together, Radvision and Avaya are propelling the unified communications evolution forward with unique technologies that harness the power of video, voice, and data over any network.
www.radvision.com