

SCOPIA Desktop Server

Installation Guide

Version 7.5



© 2000-2010 RADVISION Ltd. All intellectual property rights in this publication are owned by RADVISION Ltd and are protected by United States copyright laws, other applicable copyright laws and international treaty provisions. RADVISION Ltd retains all rights not expressly granted.

This publication is RADVISION confidential. No part of this publication may be reproduced in any form whatsoever or used to make any derivative work without prior written approval by RADVISION Ltd.

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.

Unless otherwise indicated, RADVISION registered trademarks are registered in the United States and other territories. All registered trademarks recognized.

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

Installation Guide for SCOPIA Desktop Server Version 7.5, September 2010

<http://www.radvision.com>

Table of Contents

1 About RADVISION SCOPIA Desktop Server

2 Prerequisites for Installing the SCOPIA Desktop Server

Verifying Server Requirements.....	3
Providing Sufficient Bandwidth	7
Using SCOPIA Desktop Server In a Dual-NIC Deployment	10
Selecting the Required Servers for Your Deployment	11
Verifying Operating System Requirements.....	12
Verifying Browser Requirements.....	12

3 Installing SCOPIA Desktop Server

Obtaining the SCOPIA Desktop License keys.....	13
Installing SCOPIA Desktop Server	15

4 Activating SCOPIA Desktop Presence Server and Authentication

Enabling SCOPIA Desktop User Authentication in iVIEW Suite.....	17
Configuring User Authentication Using Internal Directory	20
Configuring User Authentication Using Active Directory	21
Configuring User Authentication Using IBM Lotus Domino	24

5 Configuring Your Deployment

Logging In to the Administration Interface	28
Configuring SCOPIA Desktop to Work with a Single SCOPIA MCU	28
Configuring SCOPIA Desktop to Work With iVIEW Suite	30
Enabling Point-to-Point Functionality.....	32
Defining the Local Administrator Account	33
Verifying Component Communication and Status.....	34

1

About RADVISION SCOPIA Desktop Server

RADVISION SCOPIA Desktop is a video conferencing solution that makes your video network accessible to anyone using the SCOPIA network infrastructure. SCOPIA Desktop enables collaboration in point to point or multiparty conferences regardless of the devices connected.

SCOPIA Desktop is easy to use and includes built-in presence, invitation and firewall traversal features to ensure call connectivity and quality video conferencing. Additionally, SCOPIA Desktop supports advanced video conferencing features such as Continuous Presence video, H.239 data collaboration, PIN protected meetings, conference moderation, full authentication and authorization, and SIP point-to-point communication between SCOPIA Desktop clients.

The SCOPIA Desktop Server acts as a gateway from SCOPIA Desktop clients to a RADVISION MCU and handles all media connections. Optional SCOPIA Desktop Server components can be installed on the same or alternate servers for managing streaming, recording, and presence features.

The SCOPIA Desktop client is a simple web conferencing client for interactive conferencing using high definition or standard definition broadcasting. The client includes a control panel, a contact list, and an Outlook Add-In for scheduling meetings. A SCOPIA Desktop Pro license is also available to enable point-to-point conferencing.

As a major component of the RADVISION unified video communication solution, SCOPIA Desktop can be integrated with other RADVISION video communication components depending on your specific network topology and deployment strategy.



2

Prerequisites for Installing the SCOPIA Desktop Server

This section provides pre-installation guidelines for the SCOPIA Desktop Server. For detailed information regarding configurations for video network security, high availability, load balancing, and redundancy, refer to the *RADVISION Solution Deployment Guide*.

The topics included in this section are:

- [Verifying Server Requirements](#)..... page 3
- [Providing Sufficient Bandwidth](#) page 7
- [Using SCOPIA Desktop Server In a Dual-NIC Deployment](#) page 10
- [Selecting the Required Servers for Your Deployment](#) page 11
- [Verifying Browser Requirements](#)..... page 12
- [Verifying Browser Requirements](#)..... page 12

Verifying Server Requirements

Observe these guidelines when preparing a server for the SCOPIA Desktop Server installation:

- Use the right duplex configuration on your Ethernet NIC cards. It is essential for optimizing the videoconferencing experience.
- Use 100 Mb full duplex NIC settings for the switch and the SCOPIA Solution server.
- If you use a Gigabit NIC and switch, set the duplex setting to auto-sense. Do not use the auto-sense setting if you are not using a Gigabit NIC and switch because auto-sense might cause significant packet loss.
- Verify that the server you intend to use meets the requirements listed in [Table 2-1](#) or [Table 2-2](#).
- Only use a 32-bit operating system for iVIEW Suite installation. 64-bit operating systems are not supported at this time.
- Verify that the operating system is Windows[®] 2003 with the latest Service Releases.

[Table 2-1](#) describes server requirements for deployments where SCOPIA Desktop Server, iVIEW Suite, and Enhanced Communication Server are installed on the same server. Additionally, these requirements are based on calls made at the bandwidth of 384 Kbps.

Note: When this configuration initiates a 1 MB high definition call, scalability is reduced by fifty percent.

Table 2-1 Requirements for Single Server Installations

Deployment	Maximum number of connections	SCOPIA Desktop Server, iVIEW Suite, and ECS on the same server
For Interactive Conferencing, Watching Webcasts, and Recorded Meetings		
SCOPIA Desktop 25	25 interactive 75 streaming and playback 1 recording	RAM: 2G Disk: 20G CPU: Intel Single Core 2 Duo 915 or equivalent, 2.8GHz, 800MHz FSB, 2x2MB Cache NIC: 100 Mbit OS: Windows 2003 Server - Standard OS Language Supported: English
SCOPIA Desktop 50	50 interactive 150 streaming and playback 3 recording	RAM: 2G Disk: 20G CPU: Intel Single Quad 2 Core 915, 2.8GHz, 800MHz FSB, 2x2MB Cache NIC: 1GB OS: Windows 2003 Server - Standard OS Language Supported: English
SCOPIA Desktop 75	75 interactive 225 streaming and playback 3 recording	RAM: 3GB DDR II SDRAM - 400 MHz (PC23200) Disk: 20G CPU: Intel X3430, 2.40GHz 800MHz FSB, NIC: 1 GB with Full Duplex OS: Windows 2003 Server - Standard OS Language Supported: English
SCOPIA Desktop 100	100 interactive 300 streaming and playback 5 recording	RAM: 3GB - DDR II SDRAM - 400 MHz (PC23200) Disk: 20G CPU: Intel X3440, 2.53GH, 800MHz FSB NIC: 1 GB with Full Duplex OS: Windows 2003 Server - Standard OS Language Supported: English

Table 2-2 describes server requirements for deployments where SCOPIA Desktop Server, iVIEW Suite, and Enhanced Communication Server are installed on separate servers.

Table 2-2 Requirements for Multi-Server Installation

Deployment	Maximum number of connections	SCOPIA Desktop Server, iVIEW Suite, and ECS on separate servers
For Interactive Conferencing		
SCOPIA Desktop 150	150 interactive	RAM: 3GB - DDR II SDRAM - 400 MHz (PC23200) Disk: 20G CPU: Intel X3430, 2.40GHz, 800MHz FSB NIC: 1 GB Full Duplex OS: Windows 2003 Server - Standard OS Language Supported: English
SCOPIA Desktop 200	200 interactive	RAM: 3GB - DDR II SDRAM - 400 MHz (PC23200) Disk: 20G CPU: Intel X3430, 2.53 GHz, 800MHz FSB, NIC: 1 GB Full Duplex OS: Windows 2003 Server - Standard OS Language Supported: English
SCOPIA Desktop 250	250 interactive	RAM: 8GB - 1333 Single Ranked UDIMM Disk: 20G CPU: Dual X5570, 2.93 GHz, 800MHz Front Side Bus: Intel QuickPath Interconnect QPI @6.GT/s NIC: 1 GB Full Duplex OS: Windows 2003 Server Data Center or Enterprise OS Language Supported: English
For Viewing Webcasts and Recorded Meetings		

Deployment	Maximum number of connections	SCOPIA Desktop Server, iVIEW Suite, and ECS on separate servers
SCOPIA Desktop 300/10	300 streaming or playback 10 recording	RAM: 3GB - DDR II SDRAM - 400 MHz Disk: 20G CPU: 2xIntel Xeon, 3.2GHz, or Intel X3440, 2.53GHz 800MHz FSB, NIC: 1 GB Full Duplex OS: Windows 2003 Server - Standard OS Language Supported: English
SCOPIA Desktop 600/10	600 streaming and playback 10 recording	RAM: 5GB SDRAM - 400 MHz Disk: 20G CPU: 4xIntel Xeon, 3.66GHz, 800MHz FSB, NIC: 1 GB Full Duplex OS: Windows 2003 Data Center OS Language Supported: English and Japanese

Providing Sufficient Bandwidth

SCOPIA Desktop Server acts as a SCOPIA Gateway between participating SCOPIA Desktop clients and the SCOPIA MCU. [Table 2-3](#) shows the bandwidth resources required to enable between 10 and 250 users to connect to the system and initiate hundreds of streaming sessions. We recommend that you use the data provided in [Table 2-4](#) to plan your deployment and NIC card requirements.

Note: Use bonded 100 Mbit NICs or a Gigabyte NIC. Default settings are 384 Kbps (interactive), 256 Kbps (streaming).

The SCOPIA Desktop Server manages the throughput of each video conferencing session according to the following workflow:

- SCOPIA Desktop Client sends media to SCOPIA Desktop Server.
- SCOPIA Desktop Server forwards media to SCOPIA MCU.
- SCOPIA MCU returns media to SCOPIA Desktop Server.
- SCOPIA Desktop Server sends media to SCOPIA Desktop Client.

Therefore, the formula for calculating the bandwidth required for interactive sessions is:

Bandwidth = Bandwidth Required for One Connection × 4 × Number of Connections

Thus, for a 384 Kbps call there is 1536 Kbps of media going through the SCOPIA Desktop Server for each client.

Streaming connections send media from the SCOPIA Desktop Server to SCOPIA Desktop Clients. The formula for calculating the bandwidth required for streaming sessions is as follows:

Bandwidth = Bandwidth Required for One Connection × Number of Connections

For high definition conferencing, SCOPIA Desktop Server sends 512 Kbps and receives 1 Mb, which doubles the bandwidth required for the 384 Kbps standard definition call, for which SCOPIA Desktop Server sends and receives 384 Kbps totaling 768 Kbps. As a result, high definition conferencing reduces the number of supported interactive connections by fifty percent as shown by [Table 2-3](#) and [Table 2-4](#).

Table 2-3 Required Bandwidth Resources—Standard Definition Connections

Interactive Connections	Streaming Connections	Bandwidth for Interactive Connections (Kbps)	Bandwidth for Streaming Connections (Kbps)	Total Bandwidth (Kbps)
1		384	384	
10	30	15360	11520	26880
25	75	38400	28800	57200
50	150	76800	57600	134400
100	300	153600	115200	268800
150	450	230400	172800	N/A (install streaming server on separate computer)
200	600	307200	230400	N/A (install streaming server on separate computer)
250	0	38400	0	N/A (install streaming server on separate computer)

Table 2-4 Required Bandwidth Resources—High Definition Connections

Interactive Connections	Streaming Connections	Bandwidth for Interactive Connections (Kbps)	Bandwidth for Streaming Connections (Kbps)	Total Bandwidth (Kbps)
1		768/1024	384	
5	15	17920	11520	26880
12	36	38400	28800	57200
25	75	76800	57600	134400
50	150	153600	115200	268800
75	225	230400	172800	N/A (install streaming server on separate computer)
100	300	307200	230400	N/A (install streaming server on separate computer)
125	600	38400	0	N/A (install streaming server on separate computer)

Note:

Using SCOPIA Desktop clients in HD mode requires larger bandwidth as well as a more powerful SCOPIA Desktop Server.

The Recording Server is managed separately. You should set the maximum bandwidth for recording and playback based on the server hardware capabilities. In deployments where the Recording Server is installed on the same server as the SCOPIA Desktop Server, users watching recorded meetings consume SCOPIA Desktop bandwidth which can be used for other purposes, such as meetings.

You use the Playback Bandwidth panel in the SCOPIA Desktop Administration interface to configure bandwidth usage. Set the **Total Bandwidth Allowed** value to define a total amount of bandwidth SCOPIA Desktop uses for playing back recorded meetings.

For example, if you set the **Total Bandwidth Allowed** value to 100 Mbps, SCOPIA Desktop allows a bandwidth of 100 Mbps if one user watches a recording, and a bandwidth of 50 Mbps for each user if two users watch recordings. Set the **Minimum Bandwidth Required for Download** value to prevent too many users watching recordings at the same time.

In general, you should not allow a total bandwidth of more than 350 Mbps for interactive, streaming and recording connections on the server.

Using SCOPIA Desktop Server In a Dual-NIC Deployment

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.

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 Clients to connect to. In this case you must configure the SCOPIA Desktop network interface address to represent the NIC behind the firewall, and then in the Public Address field enter a DNS name which resolves to the NIC outside the firewall and is accessible both inside and outside the corporate network.

For single NIC deployments, the network interface address represents the SCOPIA Desktop Server IP address that clients use to connect to SCOPIA Desktop Server. In single NIC deployments with both internal and external clients, this value represents an external, statically-mapped SCOPIA Desktop Server IP address.

SCOPIA Desktop Clients can connect to the SCOPIA Desktop Server either by an IP or a DNS name. If a DNS name is not specified in the Public Address field, the SCOPIA Desktop Server network interface address is used. However, in many deployments the SCOPIA Desktop Server network interface address is not accessible to clients outside the intranet due to NAT or firewall restrictions. Therefore, it is recommended that you specify the Public Address, which must be a DNS name resolving to the correct SCOPIA Desktop Server IP address both inside and outside the corporate network.

For further information about the functionality and installation of SCOPIA Desktop Server in a dual-NIC deployment, refer to the RADVISION Solution Deployment Guide.

Selecting the Required Servers for Your Deployment

Depending on the features you require, SCOPIA Desktop may consist of a variety of different servers, each of which fulfills its own function:

- SCOPIA Desktop Server—Responsible for SCOPIA Desktop Client download and admission center, middleware, gateway media server, directory and user settings cache.

Note: The SCOPIA Desktop Server caches information from iVIEW Suite about the global directory and virtual rooms. If you restart the SCOPIA Desktop Server and it cannot reconnect to iVIEW Suite, this information is lost.

- SCOPIA Desktop Streaming Server—Responsible for streaming webcasts. This server functionality is available for all deployment types.
- SCOPIA Desktop Recording Server—Responsible for recording meetings, storing recordings, providing HTTP access to the recordings, and serving the SCOPIA Desktop Content Slider content. This server functionality is available for all deployment types except point-to-point deployments.
- SCOPIA Desktop Presence Server—Controls user authentication and user presence status information. Apart from enabling presence features, it is also used for attendee registration and invitations. The presence server that must be configured separately after the initial SCOPIA Desktop installation in order to activate it. This server functionality is only available for point-to-point and advanced deployments.
- STUN Server—Supports SCOPIA Desktop Client point-to-point media via SIP. The STUN Server is used to detect NATs and provide endpoints with the NAT public internet address. Depending on a specific deployment, the STUN server can perform these functions:
 - Figuring out if the SCOPIA Desktop Clients are on the same local network or separated by one or more NATs.
 - Figuring out which addresses are valid between the Clients.
 - Opening the NATs if applicable.

The SCOPIA Solution supports different scenarios:

- One endpoint is behind a Full Cone NAT—SIP point-to-point call succeeds.
- Both endpoints are located behind NATs.
- One endpoint is behind a Full Cone NAT—SIP point-to-point call succeeds.
- Other NATs are deployed—The call falls back to UDP/Relay hosted on SCOPIA Desktop Server.

Note: Some NATs or firewalls are SIP-aware and may act as a full cone NAT for SIP and allow point-to-point connections.

- A firewall blocks UDP ports required by a SCOPIA Desktop Client.—A call falls back to TCP/tunnelled/Relay hosted on SCOPIA Desktop Server for SCOPIA Desktop Clients that need it.
- Encryption/SRTP is forced.—A call is hosted on Relay Server.

Deployments where a STUN Server is used has these restrictions:

- You cannot use a NAT address on the STUN Server and expose it via static or dynamic public IP address. Instead you must configure STUN Server with a public IP address.
- You must place STUN Server at a location which is accessible by both SCOPIA Desktop Clients participating in a call.
- SCOPIA Desktop Clients can use different STUN Servers provided that the STUN Servers are situated on the Internet outside the Clients' NAT.
- Third-party STUN Servers are supported.

Verifying Operating System Requirements

The following operating systems are supported with this release of SCOPIA Desktop Server:

- Windows 2003 (English)
- Windows 2008 (English)
- Windows 2008 Standard 64 Bit (English)
- Windows 2008 Enterprise (English)

Verifying Browser Requirements

The following browsers are supported by SCOPIA Desktop Server:

- Internet Explorer 6.x, 7.x & 8.0 (Windows)
- Firefox 3.0, 3.5, and 4.0 (Windows)
- Chrome 5.0 (Windows)
- Safari 3.0, 4.0, and 5

3

Installing SCOPIA Desktop Server

The topics included in this section are:

- [Obtaining the SCOPIA Desktop License keys](#)..... page 13
- [Installing SCOPIA Desktop Server](#) page 15

Obtaining the SCOPIA Desktop License keys

A SCOPIA Desktop Server license key is required for the installation and operation of the SCOPIA Desktop Server. To obtain the SCOPIA Desktop Server license key, navigate to <http://www.radvision.com/sdreg> and fill in the required information. The SCOPIA Desktop license key will be sent to you by e-mail within a few business days.

To use point-to-point functionality for video communication between two clients, you must install iVIEW Suite and obtain a SCOPIA Desktop Pro license.

[Table 3-1](#) describes each of the SCOPIA Desktop client features.

Table 3-1 Description of SCOPIA Desktop Clients

Feature	SCOPIA Desktop	SCOPIA Desktop Pro
Access to the portal/plug-in installation	v	v
Schedule a meeting from Microsoft Outlook	v	v
Attend a group meeting hosted on MCU	v	v
Share and annotate documents	v	v
Invite an IP phone or a room system by its number	v	v
Watch a recorded meeting	v	v
Watch a webcast	v	v
Configure a virtual room using the SCOPIA Desktop portal		v
Publish one's presence to other meeting participants		v
Use the contact list to call people		v
Desktop-to-desktop calling		v
Invite from directory or from favorites		v

A recording serial key is required to activate SCOPIA Desktop 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 evaluation mode, limiting recording to a one five-minute session at a time.

Installing SCOPIA Desktop Server

You can install all of the SCOPIA Desktop Server components on one server or on separate servers. During the installation, you will perform a basic configuration to define which components SCOPIA Desktop Server uses based on your functionality requirements. Follow these recommendations when installing SCOPIA Desktop Server: correctly:

- For deployments of more than 100 users in which streaming or recording is heavily used, or for deployments in which port 80 is used for streaming, either install the Streaming and Recording Server together on a different server, or install each server on separate machines.
- The default SCOPIA Desktop Web Server port is 80. If other applications are using port 80, the installer prompts you to specify a different port.

If you wish to use port 80, access the Services panel on your computer and disable the IIS Administration, HTTP SSL, and World Wide Web Publishing services. You can do this before installing the SCOPIA Desktop Server software or when you receive the "ip address/ port is in use" error during installation.

After disabling these services, installation completes normally and SCOPIA Desktop clients can connect to the SCOPIA Desktop server using port 80.

- If you wish to use the HTTPS protocol for security, configure the SCOPIA Desktop web server to port 443 after the installation is completed.

- The SCOPIA Desktop Streaming Server is always installed under C:\Program Files, even if other components of SCOPIA Desktop are installed in a different location.
- The default SCOPIA Desktop Streaming Server port is 7070. If you select a different port, change the default port value in the Streaming Server configuration files accordingly.

Note: Do not install the SCOPIA Desktop Client on the SCOPIA Desktop Server.

Before You Begin

Obtain these license keys:

- SCOPIA Desktop Server license key
- (Optional) Recording serial key
- To use point-to-point functionality, you must install IVIEW Suite with the SCOPIA Desktop Pro license

Procedure

- Step 1** Navigate to the setup.exe file and double-click to launch the installer.
- Step 2** Select **Run** in the Security Warning window.
- Step 3** Select the installation language in the Choose Setup Language window, and select **OK**.
- Step 4** Select **Next** in the Welcome window.
- Step 5** Read the agreement in the License Agreement window, choose **I accept the terms in the license agreement**, and then select **Next**.
- Step 6** Define which SCOPIA Desktop servers to install and specify the installation location in the Custom Setup window, and then select **Next**.

Note: For a single server installation, install all components. When you install the STUN server on a separate machine located outside the NAT/Firewall, run the SCOPIA Desktop installation and select to install STUN only.

- Step 7** Enter the SCOPIA Desktop key and the Recording key numbers in the SCOPIA Desktop License Key window, and select **Next**.

Note: If you enter the recording key, the Recording Server will be installed in demo mode. Also, you are not prompted for recording key if you did not choose the recording server in the previous screen.

- Step 8** Configure the SCOPIA Desktop Network Interface and SCOPIA Desktop web server port in the SCOPIA Desktop Network Configuration window, and select **Next**.

Step 9 Specify the hostname of the server that clients should use to connect to the SCOPIA Desktop in the SCOPIA Desktop Hostname Configuration window.

Note: Make sure that you specify the hostname that clients can resolve.

Step 10 If you chose to install the Recording Server component, specify the storage location and the maximum amount of disk space allocated for recorded meetings in the SCOPIA Desktop Recording Configuration window.

Note: Make sure to allocate enough space. A typical recording for a one-hour meeting at 384Kbps takes up to 200MB.

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

Step 12 Select **Finish**.

4

Activating SCOPIA Desktop Presence Server and Authentication

You can only configure user authentication for deployments that include point-to-point functionality or iVIEW Suite. To support the authentication feature, install and configure the following components:

- iVIEW Suite
- SCOPIA Desktop Server
- SCOPIA Desktop Presence Server

- [Enabling SCOPIA Desktop User Authentication in iVIEW Suite](#) page 17
- [Configuring User Authentication Using Internal Directory](#)..... page 20
- [Configuring User Authentication Using Active Directory](#) page 21
- [Configuring User Authentication Using IBM Lotus Domino](#)..... page 24

Enabling SCOPIA Desktop User Authentication in iVIEW Suite

For deployments that utilize iVIEW Suite or point-to-point functionality, iVIEW Suite must be enabled for SCOPIA Desktop user authentication. This feature allows authentication of SCOPIA Desktop user upon accessing the SCOPIA Desktop portal.

Once authenticated, users can access enhanced SCOPIA Desktop functionality according to the authorization rules defined on iVIEW Suite: accessing and recording meetings, watching recordings and webcasts, and inviting new participants to meetings.

Before You Begin

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

Procedure

Step 1

In the iVIEW Suite Administrator web user interface, verify that SCOPIA Desktop Server is added:

- a. Select the **Resource Management** icon in the sidebar.

Figure 4-1 iVIEW Suite Resource Management Icon



- b. Select the **SCOPIA Desktop** tab.
- c. Verify that the required SCOPIA Desktop Server appears in the table of connected servers.

Step 2

In the SCOPIA Desktop Administrator web user interface, select the **Status** icon in the sidebar, and verify that the SCOPIA Desktop Server is connected to iVIEW Suite.

Figure 4-2 SCOPIA Desktop and iVIEW Suite Connection Status

SCOPIA Desktop Components		
SCOPIA Desktop Server:	192.168.114.236	●
iVIEW Suite:	192.168.114.236	●

Step 3

Enable user authentication for SCOPIA Desktop:

- a. In the iVIEW Suite Administrator web user interface, navigate to the **General User Policies** section by selecting **Advanced Settings > Default User Settings**.
- b. Select the **Enable SCOPIA Desktop user authentication** check box.

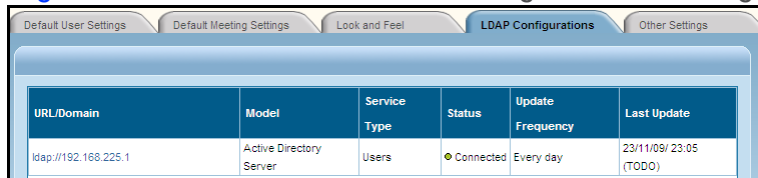
Figure 4-3 iVIEW Suite General User Policies

General User Policies:	
<input checked="" type="checkbox"/>	Enable SCOPIA Desktop user authentication
<input checked="" type="checkbox"/>	Allow guests to access meetings
<input type="checkbox"/>	Allow guests to access webcasts
<input type="checkbox"/>	Allow guests to start recording
<input type="checkbox"/>	Allow guests to access recordings
<input type="checkbox"/>	Only authenticated users can invite
<input checked="" type="checkbox"/>	Display all meeting records on My Meetings screen

- c. Select authorization options as required:

- Step 4** Navigate to **Advanced Settings > LDAP Configurations** and verify which authentication method iVIEW Suite is configured to use either:
- Internal Directory
 - Active Directory
 - IBM Lotus Domino

Figure 4-4 iVIEW Suite LDAP Configuration Settings



URL/Domain	Model	Service Type	Status	Update Frequency	Last Update
ldap://192.168.225.1	Active Directory Server	Users	Connected	Every day	23/11/09/ 23:05 (TODO)

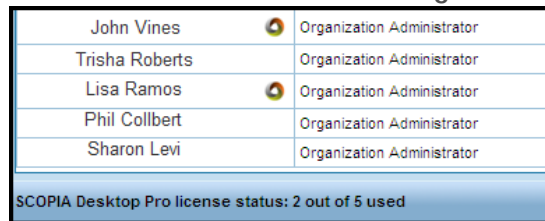
- Step 5** Select the **User Management** icon in the sidebar.



Figure 4-5 iVIEW Suite User Management Icon



- Step 6** Check the total number of licensed users displayed at the bottom of the tab. Each user who has an enabled license has a license icon next to their name.

Figure 4-6 iVIEW Suite User Management Panel



John Vines		Organization Administrator
Trisha Roberts		Organization Administrator
Lisa Ramos		Organization Administrator
Phil Colbert		Organization Administrator
Sharon Levi		Organization Administrator

SCOPIA Desktop Pro license status: 2 out of 5 used

- Step 7** If necessary, enable a Pro license for each user requiring point-to-point functionality by selecting the user, expanding the Advanced section, and verifying that the SCOPIA Desktop Pro license is enabled.

This procedure can also be done via group provisioning. You can either put users in groups that you define, or they can be in different groups in Active Directory / Domino, and then you can make settings for all users in that group at once.

Figure 4-7 iVIEW User Profile Advanced Configuration

Advanced	
User Type:	Organization Administrator
Telephone(Office):	5669
Telephone(Mobile):	+86 13701083586
LDAP Server:	ldap://192.168.225.1
Default Terminal:	<input type="text"/> <input type="button" value="Select"/>
Allowed Meeting Types:	Non Video Conference, Pt <input type="button" value="Select"/>
Groups:	<input type="text"/> <input type="button" value="Select"/>
Time Zone:	GMT+08:00 China Standard Time (Asia/Chongqing)
Recording Policy:	Allow user to record meetings
Location Preference:	Auto
SCOPIA Desktop Pro license:	SCOPIA Desktop Pro license disabled
	SCOPIA Desktop Pro license enabled
SCOPIA Desktop Pro license status: 2 out of 5 use SCOPIA Desktop Pro license disabled	

Configuring User Authentication Using Internal Directory

When the authentication method configured in iVIEW Suite is set to Internal Directory, iVIEW Suite imports the users and their passwords stored in an internal directory.

Before You Begin

Ensure user authentication is enabled on iVIEW Suite.

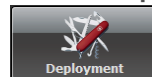
Procedure

Step 1

Configure user authentication on SCOPIA Desktop Server:

- a. Select the **Deployment** icon in the sidebar.

Figure 4-8 SCOPIA Desktop Deployment Icon



- b. Select the **Presence and Invitation** check box.

Figure 4-9 Presence and Invitation Panel

<input checked="" type="checkbox"/> Presence and Invitation	
XMPP Server Address:	<input type="text" value="192.168.212.23"/>
STUN Server Address:	<input type="text" value="88.211.26.134"/>

- c. Enter the XMPP Server and STUN Server IP addresses.

Step 2

Start SCOPIA Presence Server configuration tool by selecting **Start > All Programs > SCOPIA Desktop > Config Tool**.

Step 3

Select the **Jabber** Tab.

Step 4

Configure the SCOPIA Presence Server to use iVIEW Suite with internal directory:

- a. Select iVIEW Suite from the **Authentication Type** list, and then select **Add Host**.

Figure 4-10 SCOPIA Presence Server Authentication Type



The window displays the iVIEW tab.

- b. Enter the Jabber domain.

The Jabber domain you use must be identical to the domain set when enabling user authentication on SCOPIA Desktop Server.

- c. Enter the IP address of iVIEW Suite in the Remote Address field.
- d. Enter the IP address of Jabber Server in the Local Bind Address field.

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

Step 5 Select **Apply**.

Configuring User Authentication Using Active Directory

When iVIEW Suite uses Active Directory authentication, iVIEW Suite imports users from a single Active Directory Server or multiple Active Directory Servers.

Before You Begin

Ensure user authentication is enabled on iVIEW Suite.

Procedure

Step 1 In the iVIEW Suite Administrator web user interface, navigate to the LDAP Configuration page to see the Active Directory Servers configured for iVIEW Suite.

Figure 4-11 iVIEW Suite LDAP Configuration Tab

URL/Domain	Model	Service Type	Status	Update Frequency	Last Update
ldap://192.168.225.1	Active Directory Server	Users	Connected	Every day	23/11/09/ 23:05 (TODO)

Step 2 An Active Directory user group is referred to as “search base” in the SCOPIA Desktop web user interface. If necessary, specify one or more search bases.

- a. In the SCOPIA Desktop Administrator web user interface, select Presence and Invitation on the sidebar.

Figure 4-12 Scopia Presence and Invitation Icon



The directory servers configured on iVIEW Suite appears.

- Step 3** Connect the Active Directory Server to the XMPP Server:
- Select a check box for the SCOPIA Presence Server you want to use.

Figure 4-13 Scopia Domain Mapping and Presence Panel

Additional search base fields are displayed representing the groups of users imported from iVIEW Suite.

- For each group, specify a XMPP domain name.

-or-

- Step 4** To allow all users imported from the Active Directory to use the Active Directory domain as the XMPP domain, clear the check box for this directory.

- Step 5** Select **OK** or **Apply**.

- Step 6** Start the SCOPIA Presence Server configuration tool by selecting **Start > All Programs > SCOPIA Desktop > SCOPIA Presence Server Config**.

- Step 7** If you connected the Active Directory Server to an XMPP Server, create a profile for each Active Directory server:

- Select **Active Directory** from the Authentication Type dropdown list, then select **Add Host**.

Figure 4-14 SCOPIA Presence Server Authentication Type

The window displays the directory tab.

- Enter the SCOPIA Presence domain that matches the XMPP domain displayed on the Presence and Invitation page.

Figure 4-15 SCOPIA Presence Configuration Panel



The screenshot shows a configuration panel with the following fields:

- Jabber Domain: [Empty text box]
- Active Directory Address: 192.168.212.178
- LDAP search base: [Empty text box]
- Proxy Account User Name (must have READ permission to directory): [Empty text box]
- Password: [Masked text box with 8 dots]
- Confirm Password: [Masked text box with 8 dots]
- LDAP Port: 389

- c. Enter the Active Directory address that matches the Active Directory address displayed on the Presence and Invitation page.
- d. To define at what level of the Active Directory tree SCOPIA Presence Server should start searching for users to validate, enter the relevant value in the LDAP search base.
- e. Enter the Admin user and password for users who will be able to browse the Active Directory database.
- f. In case the Active Directory is configured with a port different from the default port 389, change the LDAP port value.

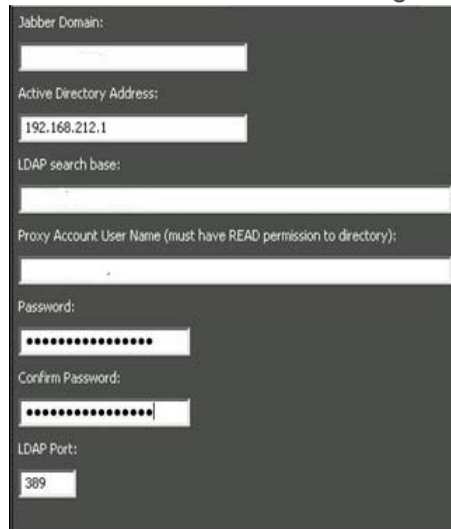
-or-

Step 8

If you chose to use the Active Directory domain as the XMPP domain, create a profile for this Active Directory:

- a. Select Active Directory from the Authentication Type list, and then select Add Host.
The window displays the directory tab.

Figure 4-16 SCOPIA Presence-XMPP Configuration Pane for AD



Jabber Domain:

Active Directory Address:

LDAP search base:

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

Password:

Confirm Password:

LDAP Port:

- b. Enter the Active Directory domain in the SCOPIA Presence Domain.
- c. Enter the Active Directory name in the AD Address. The Active Directory name must match the Active Directory name displayed on the Presence and Invitation page.
- d. To define at what level of the Active Directory tree SCOPIA Presence Server will start searching for users to validate, enter the relevant value in the LDAP search base. Use the root for all users in this domain.
- e. Enter the Admin username and password for users who will be able to browse the Active Directory database.
- f. If the Active Directory is configured with a port other than the default port 389, change the LDAP port value.

Step 9

Select **Apply**.

The SCOPIA Presence service is started.

Configuring User Authentication Using IBM Lotus Domino

Perform this procedure when iVIEW Suite is configured to import and authenticate users from IBM Lotus Domino.

Before You Begin

Ensure user authentication is enabled on iVIEW Suite.

Procedure

Step 1

In the iVIEW Suite Administrator web user interface, navigate to the LDAP Configuration page to see the Domino servers configured for iVIEW Suite.

A Domino user group is referred to as “search base” in the iVIEW Suite web user interface.

Step 2

If necessary, you can specify one or more search bases.

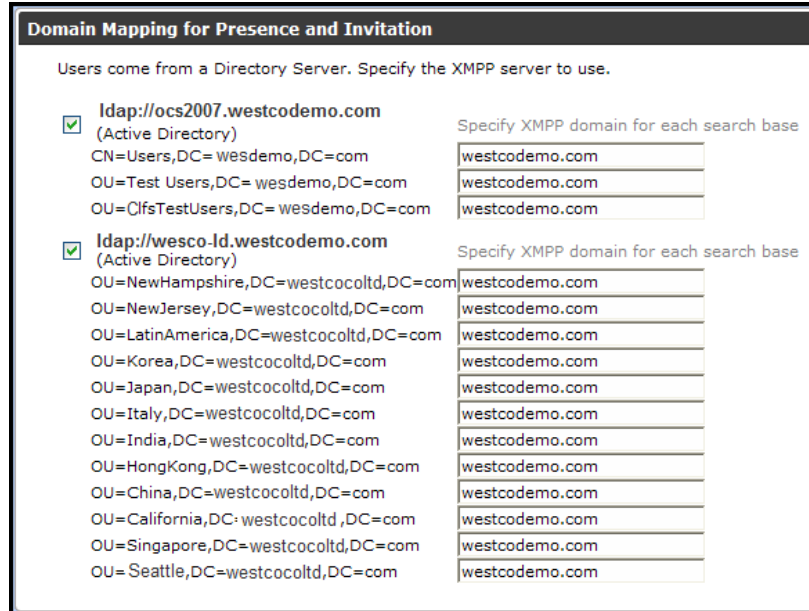
Step 3 In the SCOPIA Desktop Administrator interface, select **Presence and Invitation** on the sidebar.

Figure 4-17 SCOPIA Desktop Presence and Invitation Icon



The directory servers configured on iVIEW Suite appear on the page.

Figure 4-18 SCOPIA Desktop Domain Mapping Panel



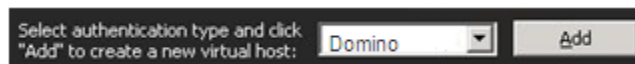
- Step 4** Configure Domino Servers to connect to an XMPP Server:
- Select a check box for the Domino Server you want to use.
Additional search base fields are displayed representing user groups imported from iVIEW Suite.
 - For each group specify a XMPP domain name.

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

Step 6 Start the SCOPIA Presence Server configuration tool by selecting **Start > All Programs > SCOPIA Desktop > SCOPIA Presence Config**.

- Step 7** Create a profile for each IBM Lotus Domino server:
- Select Domino from the Authentication Type dropdown list, and then select **Add**.

Figure 4-19 SCOPIA Presence Server Authentication Type



The window displays the directory tab.

- Enter the SCOPIA Presence Server domain that matches the XMPP domain displayed on the Presence and Invitation page.

- c. Enter the IBM Lotus Domino address that matches the address displayed on the Presence and Invitation page.
- d. To define at what level of the IBM Lotus Domino tree SCOPIA Presence Server will start searching for users to validate, enter the relevant value in the LDAP search base.
- e. Enter the Admin username and password for users who will be able to browse the Active Directory database.
- f. In case the Active Directory is configured with a port different from the default port 389, change the LDAP port value.

Step 8

Select **Apply**.

The SCOPIA Presence Server service is started.

5

Configuring Your Deployment

After completing the SCOPIA Desktop Server installation, you must login to the SCOPIA Desktop Administration web page 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 Administration interface, configure your deployment of choice, define a local administrator account, and verify that the SCOPIA Solution components are successfully connected.

Note:

If you intend to configure multicast streaming, before configuring SCOPIA Desktop, you should:

- Ensure multicast is enabled on the deployment routers and firewalls. Verify the number of packet hops to correctly define the Time to Live value.
- Obtain the internal IP address range of accessible SCOPIA Desktop Clients to define clients that will be able to watch multicasts.

-
- [Logging In to the Administration Interface](#) page 28
 - [Configuring SCOPIA Desktop to Work with a Single SCOPIA MCU](#) page 28
 - [Configuring SCOPIA Desktop to Work With iVIEW Suite](#) page 30
 - [Enabling Point-to-Point Functionality](#) page 32
 - [Defining the Local Administrator Account](#) page 33
 - [Verifying Component Communication and Status](#) page 34

Logging In to the Administration Interface

The SCOPIA Desktop Server Administration interface is a web-based application. To login:

Procedure

- Step 1** Open the Internet browser.
- Step 2** Enter the following URL:
`http://<host>[:<port>]/scopia/admin`
where <host> is the location of your corporate SCOPIA Desktop Server.
- Step 3** On the Administration page, enter your username and password.
- Step 4** Select Sign In.
The default username and password are both "admin"

Configuring SCOPIA Desktop to Work with a Single SCOPIA MCU

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

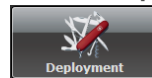
Before You Begin

- Login to the SCOPIA Desktop Server Administration web user interface.
- 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

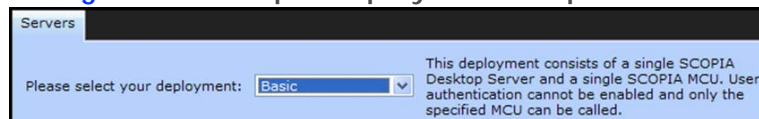
- Step 1** Select the **Deployment** icon in the sidebar.

Figure 5-1 SCOPIA Desktop Deployment Icon



- Step 2** Select **Basic** from the deployment dropdown list.

Figure 5-2 Scopia Deployment Dropdown List



Step 3 Enter the MCU IP address.

Figure 5-3 MCU IP Address Field

The screenshot shows the SCOPIA MCU configuration page. It has a dark header with the text "SCOPIA MCU". Below the header, there are several input fields and a checkbox. The "Management Address" field is highlighted in yellow. Below it is a checkbox labeled "Use a different address for media and signaling". Underneath the checkbox is the "Media and Signaling Address" field, which is currently greyed out. Below that are three more input fields: "User Name:", "Password:", and "Confirm:", each with a corresponding text box.

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.

Step 4 Enter a user name and password for accessing the MCU Administration web user interface.

Step 5 Re-enter the password in the Confirm field.

The default user name is "admin". There is no default password for SCOPIA Classic MCU; for SCOPIA Elite MCU the default password is "password".

Step 6 If SCOPIA Desktop Server is configured with multiple IP addresses, select the relevant address from the SCOPIA Desktop Network Interface list.

Step 7 To enable recording:

- a. Select the **Recording** check box.
- b. Enter the Recording Server address.

Figure 5-4 Recording and Streaming Server Check Boxes

The screenshot shows the Recording and Streaming configuration sections. The "Recording" section has a checked checkbox and a "Recording Server Address" field containing "192.111.111.111" with a green status indicator. The "Streaming" section has a checked checkbox, a "Darwin Streaming Server Address" field containing "192.111.111.111" with a green status indicator, a checked checkbox for "Use a different address for media and signaling", and a "Media and Signaling Address" field highlighted in yellow.

Step 8 To enable streaming:

- a. Select the **Streaming** check box.
- b. Enter the Darwin Streaming Server address.
- c. (Optional) To use a different address for media and signaling, select the **Use a different address for media and signaling** check box and enter the address.

Step 9 Select OK.

The Settings page appears.

Configuring SCOPIA Desktop to Work With iVIEW Suite

This section describes how to configure SCOPIA Desktop to work with iVIEW Suite and the Enhanced Communication Server gatekeeper.

The source H.323 ID is used to allow iVIEW Suite to identify SCOPIA Desktop. iVIEW Suite contains a corresponding field and uses the source H.323 ID to identify clients from a particular SCOPIA Desktop Server, and then route clients to the appropriate MCU.

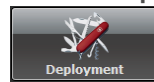
Before You Begin

Navigate to the SCOPIA Desktop Administration web user interface.

Procedure

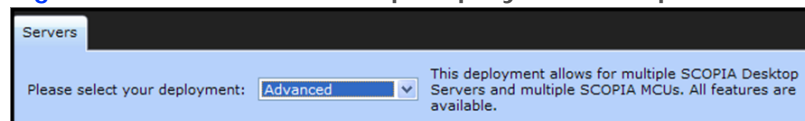
Step 1 Select **Deployment** in the sidebar.

Figure 5-5 SCOPIA Desktop Deployment Icon



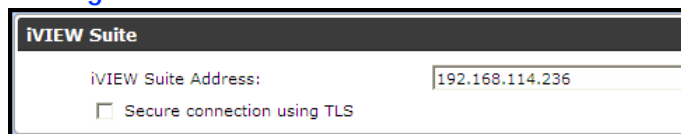
Step 2 Select **Advanced** from the deployment dropdown list.

Figure 5-6 SCOPIA Desktop Deployment Dropdown List



Step 3 Enter the address of iVIEW Suite.

Figure 5-7 iVIEW Suite IP Address Field



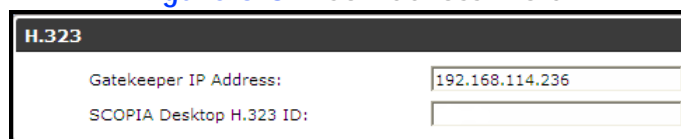
Step 4 To use secure connection between iVIEW Suite and SCOPIA Desktop Server, select the **Secure connection using TLS** check box.

Ensure the check box is also selected on iVIEW Suite.

Step 5 If the SCOPIA Desktop Server is configured with multiple IP addresses, select the relevant address from the SCOPIA Desktop Network Interface list.

Step 6 Enter IP address of the gatekeeper.

Figure 5-8 ECS Address Field

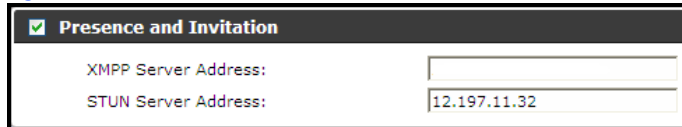


Step 7 Enter the source H.323 ID of the SCOPIA Desktop Server.
The H.323 ID must match the SCOPIA Desktop H.323 ID configured on iVIEW Suite.

Step 8 To enable presence and invitation features:

- Select the Presence and Invitation check box.
- Enter the XMPP Server address.
- Enter the STUN Server address.

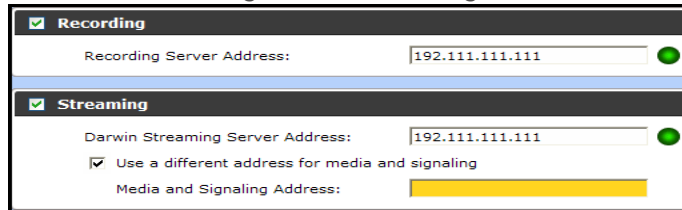
Figure 5-9 Presence and Invitation Check Boxes



<input checked="" type="checkbox"/> Presence and Invitation	
XMPP Server Address:	<input type="text"/>
STUN Server Address:	<input type="text" value="12.197.11.32"/>

Step 9 To enable recording, select the Recording check box, and then enter the Recording Server address.

Figure 5-10 Recording and Streaming Server Check Boxes



<input checked="" type="checkbox"/> Recording	
Recording Server Address:	<input type="text" value="192.111.111.111"/> ●
<hr/>	
<input checked="" type="checkbox"/> Streaming	
Darwin Streaming Server Address:	<input type="text" value="192.111.111.111"/> ●
<input checked="" type="checkbox"/> Use a different address for media and signaling	
Media and Signaling Address:	<input style="background-color: yellow;" type="text"/>

Step 10 To enable streaming, select the Streaming check box, and then enter the Streaming Server address.

Step 11 Select OK.
The Settings page appears.

Related Topics

- SCOPIA Solution Deployment Guide

Enabling Point-to-Point Functionality

This section describes how to enable point-to-point functionality when SCOPIA Desktop is configured to work with iVIEW Suite. When you set the deployment type to Advanced or Point-to-Point-Only, the Integrated Windows Authentication area is displayed on the Settings tab under Authentication and Directory.

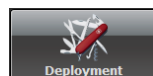
Before You Begin

Login to the SCOPIA Desktop Administration web user interface.

Procedure

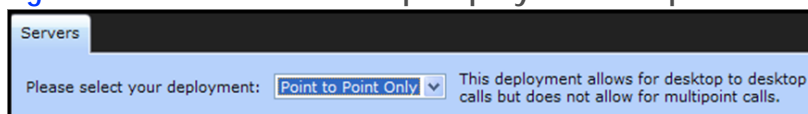
Step 1 Select Deployment icon in the side bar.

Figure 5-11 SCOPIA Desktop Deployment Icon



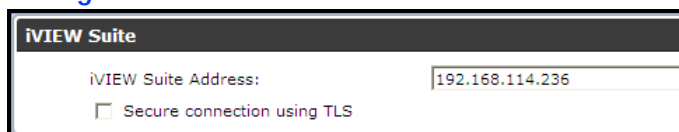
Step 2 Select Point-to-Point Only from the deployment dropdown list.

Figure 5-12 SCOPIA Desktop Deployment Dropdown List



Step 3 Enter the address of iVIEW Suite.

Figure 5-13 iVIEW Suite IP Address Field



Step 4 To use a secure connection between iVIEW Suite and SCOPIA Desktop Server, select the Secure connection using TLS check box.

Ensure the check box is also selected on iVIEW Suite.

Step 5 If the SCOPIA Desktop Server is configured with multiple IP addresses, select the relevant address from the SCOPIA Desktop Network Interface list.

Step 6 Enter the XMPP Server address.

Figure 5-14 Presence and Invitation Settings



Step 7 Enter the STUN Server address.

Step 8 Select OK
The SCOPIA Desktop Settings page appears.

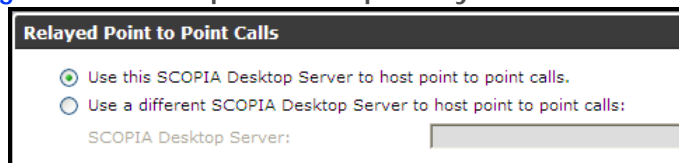
Step 9 -OR-
To deploy more than one SCOPIA Desktop Server, configure which server hosts point-to-point calls:
a. Select **Presence and Invitation** in the sidebar.

Figure 5-15 SCOPIA Desktop Presence and Invitation Icon



b. Select the relevant option in the Relayed Point to Point calls section.

Figure 5-16 Scopia Desktop Relayed Host Selection



c. If you select **Use a different SCOPIA Desktop Server to host point to point calls**, enter the server IP address in the field.
d. Select OK.
The SCOPIA Desktop Settings page appears.

Related Topics

- *SCOPIA Solution Deployment Guide*

Defining the Local Administrator Account

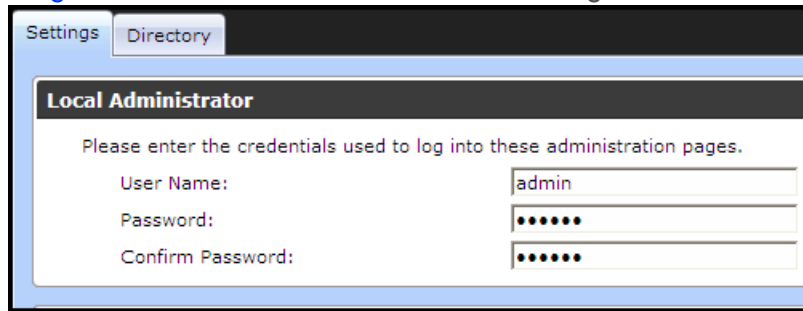
You can define a user and password for a local administrator to access SCOPIA Desktop Administration web user interface. The local administrator cannot sign in SCOPIA Desktop user portal using credentials defined during this procedure.

In point-to-point-only and advanced deployments where the authentication option is enabled on iVIEW Suite, iVIEW Suite administrators can access the SCOPIA Desktop Administration web user interface.

Procedure

Step 1 Select **Directory and Authentication** on the sidebar.
The **Settings** tab is displayed.

Figure 5-17 Local Administrator Configuration Panel



Step 2 Enter credentials in the Local Administrator area.

Step 3 Select OK.

The SCOPIA Desktop Status page opens.

Verifying Component Communication and Status

The SCOPIA Desktop user interface provides a page for reporting the connectivity status of your deployment. The indicators next to each link shows whether or not the connection to the target server or registration with a particular component is successful. When the indicator is red, a tooltip containing error details is available.

Note: Configuration options irrelevant for your deployment are hidden.

Procedure

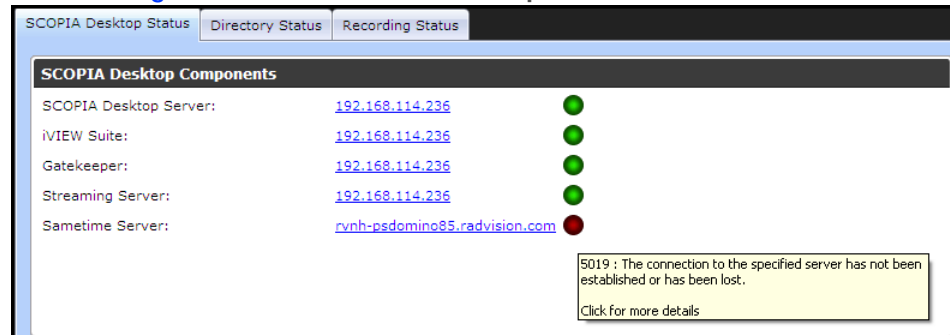
Step 1 To verify that SCOPIA Desktop Server is connected to the required servers and SCOPIA Solution components, select the Status icon in the sidebar.

Figure 5-18 SCOPIA Desktop Status Icon



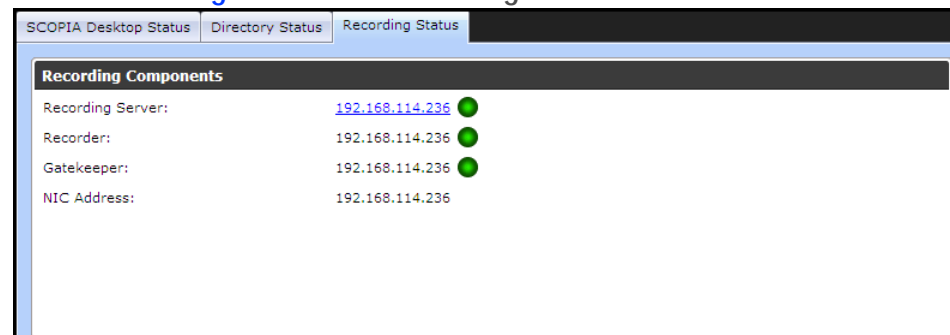
Step 2 View the connection status for each server or component. If necessary, select any red indicators to view further error information.

Figure 5-19 SCOPIA Desktop Status Indicator Tab



Step 3 If you installed and configured a SCOPIA Desktop Recording Server, select the Recording Status tab and verify connectivity for the recording components.

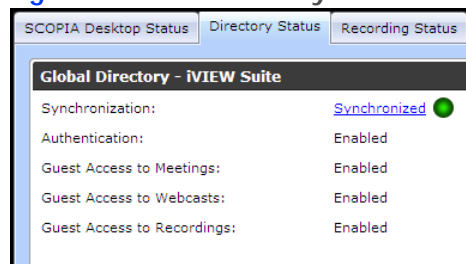
Figure 5-20 Recording Server Status Tab



Step 4 View the connection status for each recording server component. If necessary, select any red indicators to view further error information.

Step 5 If you installed and configured a SCOPIA Desktop to work with iVIEW Suite, SCOPIA Desktop Server must synchronize with iVIEW Suite to download information about users, virtual rooms, and global policy. Select the Directory Status tab and verify synchronization with iVIEW Suite.

Figure 5-21 Directory Status Tab



Step 6 (Optional) View the connection status of the Content Slider by selecting the Content tab.

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



www.radvision.com

About RADVISION

RADVISION (NASDAQ: RVSN) is the industry's leading provider of market-proven products and technologies for unified visual communications over IP and 3G networks. With its complete set of standards based video networking infrastructure and developer toolkits for voice, video, data and wireless communications, RADVISION is driving the unified communications evolution by combining the power of video, voice, data and wireless - for high definition video conferencing systems, innovative converged mobile services, and highly scalable video-enabled desktop platforms on IP, 3G and emerging next generation networks. For more information about RADVISION, visit www.radvision.com

USA/Americas

T +1 201 689 6300

F +1 201 689 6301

infoUSA@radvision.com

EMEA

T +44 20 3178 8685

F +44 20 3178 5717

infoUK@radvision.com

APAC

T +852 3472 4388

F +852 2801 4071

infoAPAC@radvision.com