

SCOPIA iVIEW Management Suite

Troubleshooting 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.

Troubleshooting Guide for SCOPIA iVIEW Management Suite Version 7.5, September 2010

<http://www.radvision.com>

Table of Contents

1 Troubleshooting SCOPIA iVIEW Management Suite Version 7.5

Resolving Browser Authentication Issues.....	2
Recognizing a Local Intranet Site.....	2
Enabling Single Sign-on.....	2
Configuring Outlook Add-on for Single Sign-on.....	2
Connecting the iCM Microsoft Outlook Add-on to iCM	3
Collecting Logs	3
Collecting iVIEW Network Manager Logs	3
Viewing Logs for a Selected Element	3
Defining iVIEW Network Manager Logging Activity.....	4
Saving Element Logs	4
Collecting Logs from a Cisco IOS H.323 Gatekeeper Element.....	5
Collecting SCOPIA Desktop Logs	5
Resolving User Experience Issues.....	6
Enabling Internet Explorer Pop-ups	6
Navigating Between Pages.....	6
Configuring Maximum Time Period for Recurring Meetings.....	6
Correcting Web Page and Pop-up Window Display.....	6
Resolving Administration Issues.....	7
Database Unavailable	7
Using Double-Byte Characters in the MCU Service Template	7
Configuring Terminal Area Codes.....	7
Assigning DID Numbers	7
Resolving IVR Issues.....	8
Resolving Virtual Service Issue	8

Resolving Video IVR Issue	9
Resolving Auto Route Incoming Calls Issue	10
Resolving a Port Conflict	11
Resolving a Scheduling Failure	11
Resolving a Failed Terminal Invitation	12
Resolving a Meeting Creation Failure	13
Resolving No Video Output	14
Resolving Poor Video Quality	14
Resolving No Audio Output	14
Synchronizing SCOPIA Desktop Server with iVIEW Suite	14
Updating the IP Address on the Streaming Server	15
Changing IP Address of the SCOPIA Desktop Server	15
Recording Does Not Start Automatically	16

1

Troubleshooting SCOPIA iVIEW Management Suite Version 7.5

RADVISION has your productivity and satisfaction in mind when creating this troubleshooting guide. It is meant to provide quick answers to common problems concerning your video conferencing network operations. This guide contains answers to problems that SCOPIA iVIEW Communications Manager administrators can utilize with minimal hassle.

The following sections might help you identify problems with your installation or configuration of iVIEW Communications Manager or related network components:

- [Resolving Browser Authentication Issues](#) page 2
- [Connecting the iCM Microsoft Outlook Add-on to iCM](#) page 3
- [Collecting Logs](#) page 3
- [Resolving User Experience Issues](#) page 6
- [Resolving Administration Issues](#) page 7
- [Resolving IVR Issues](#) page 8
- [Resolving a Port Conflict](#) page 11
- [Resolving a Scheduling Failure](#) page 11
- [Resolving a Failed Terminal Invitation](#) page 12
- [Resolving a Meeting Creation Failure](#) page 13
- [Synchronizing SCOPIA Desktop Server with iVIEW Suite](#) page 14
- [Resolving No Video Output](#) page 14
- [Resolving No Video Output](#) page 14
- [Resolving No Audio Output](#) page 14
- [Updating the IP Address on the Streaming Server](#) page 15
- [Changing IP Address of the SCOPIA Desktop Server](#) page 15
- [Recording Does Not Start Automatically](#) page 16

Resolving Browser Authentication Issues

Recognizing a Local Intranet Site

Problem The browser does not recognize iVIEW Communications Manager as a local Intranet site and an authentication window appears.

Solution

- Provide users with a link to iVIEW Management Suite that includes the necessary fully qualified domain name (FDQN), rather than only the iVIEW Communications Manager IP address.
- Configure the browser for the user so that iVIEW Communications Manager is a local Intranet site.

Enabling Single Sign-on

Problem iVIEW Management Suite web pages always require that you enter a user name and password.

Solution Use Single Sign-on (SSO). SSO enables users to access iVIEW Management Suite web pages without having to enter a user name or password. Users are authenticated transparently using domain account and password credentials.

To enable Single Sign-on, during installation select the **Single Sign-on** check box. You must also add the iVIEW Management Suite host server to the trusted site of the client browser.

Configuring Outlook Add-on for Single Sign-on

Problem iVIEW Communications Manager authentication fails when working with SSO and iVIEW Communications Manager Microsoft Outlook Add-on.

Solution Perform the procedure in this section.

Procedure

Step 1 Select **Tools > Options > iVIEW Management Suite Meeting Settings**.

Step 2 Enter a link to iVIEW Management Suite that includes the necessary fully qualified domain name (FDQN), rather than only the Resource Manager IP address.

Step 3 Configure the browser for the user so that iVIEW Communications Manager is a local Intranet site. iVIEW Communications Manager automatically performs authentication using the domain account/password credentials.

Connecting the iVIEW Microsoft Outlook Add-on to iVIEW Communications Manager

Problem	The iVIEW Communications Manager Microsoft Outlook Add-on fails to connect to iVIEW Communications Manager.
Solution	After installing the iVIEW Communications Manager Microsoft Outlook Add-on, go to Tools > Options > iVIEW Management Suite Meetings and enter the URL of your server in the Web Site field.

Collecting Logs

- [Collecting iVIEW Network Manager Logs](#) page 3
- [Collecting SCOPIA Desktop Logs](#) page 5

Collecting iVIEW Network Manager Logs

- [Viewing Logs for a Selected Element](#) page 3
- [Defining iVIEW Network Manager Logging Activity](#)..... page 4
- [Saving Element Logs](#) page 4
- [Collecting Logs from a Cisco IOS H.323 Gatekeeper Element](#)..... page 5

Viewing Logs for a Selected Element

The information displayed on the Logs tab is dependent on the type of element that is selected in the tree.

A log of operations is not available for endpoints supported by the iVIEW Network Manager. A log tab is not available for endpoints when selected in the Network Tree view.

Procedure

- Step 1** Select **Network Tree** in the sidebar menu.
- Step 2** Select the required network element.
- Step 3** Select **Logs**.
- Step 4** Define the log details for the selected network element.
- Step 5** Select **Open log view** to view the logs directory for the selected network element. If you are viewing logs for ECS, select **Open elements logs directory**.

Defining iVIEW Network Manager Logging Activity

Procedure

- Step 1** Select **Settings** in the sidebar menu.
- Step 2** Select **Logging**.
- Step 3** Select **Network Manager Logs**.
- Step 4** Select **Save iView Manager log** to enable logging.
- Step 5** (Optional) Define the log file name, the maximum file size, the number of backup files to maintain, and the level of log detail in the relevant fields.
The maximum log file size is 5,120 KB.
The maximum number of log files is 50.
iVIEW Network Manager
- Step 6** Select the **View log directory** link to view a list of links to log files for iVIEW Network Manager and managed network elements.
- Step 7** Select **Upload** to save your changes.

Saving Element Logs

iVIEW Network Manager can locally save log files for those elements, such as MCUs, SCOPIA PathFinder Servers and Gateways, that do not maintain a log of their own.

Procedure

- Step 1** Select **Settings** in the sidebar menu.
- Step 2** Select **Logging**.
- Step 3** Select **Element Logs**.
- Step 4** Define the maximum size of each log file and the number of backup files to maintain in the relevant fields.
- Step 5** Select **Upload** to save your changes.

Collecting Logs from a Cisco IOS H.323 Gatekeeper Element

Procedure

- Step 1** Select **Network Tree** in the sidebar menu.
- Step 2** Select the Cisco IOS H.323 Gatekeeper you require in the tree.
- Step 3** Select **Debug Flags**.
- Step 4** Select **Add**.
- Step 5** Enter **debug ip icmp** in the Debug Command field to generate traffic and confirm logging is configured properly.
- Step 6** Enter **Enable ip icmp debugging** in the Description field.
- Step 7** Select **Enable**.
- Step 8** Select **OK**.
A new alarm appears in the Alarms tab.
- Step 9** Select **Logs**.
- Step 10** Select **Save logs**.
- Step 11** Enter a file name and set the log level to **Debugging**.
- Step 12** Ping the Cisco IOS H.323 Gatekeeper to generate traffic to capture logs.
- Step 13** Select **Open log view** to verify the result.

Collecting SCOPIA Desktop Logs

Procedure

- Step 1** Access the SCOPIA Desktop Server.
- Step 2** Select the Conference Server icon on the taskbar to view the log in the Console window.
- Step 3** If necessary, save the log files located at these locations:
 - C:\Program Files\Radvision\SCOPIA Desktop\ConfSrv\cs.log
 - C:\Program Files\Radvision\SCOPIA Desktop\logs*.xml
 - C:\Program Files\SCOPIA Desktop\tomcat\logs\stdout.log, stderr.log

Resolving User Experience Issues

Enabling Internet Explorer Pop-ups

Problem Internet Explorer Pop-up Blocker blocks pop-ups for the SCOPIA iVIEW Communications Manager site.

Solution If you are using Microsoft Windows XP SP2 or Windows 2003 Service Pack 1, and you enable Internet Explorer Pop-up Blocker, add the iVIEW Communications Manager site to the list of allowed sites.

Procedure

Step 1 In the Internet Explorer window, select **Tools > Internet Options > Privacy**.

Step 2 Select the **Block Pop-ups** check box in the Pop-up Blocker area.

Step 3 Select **Settings**.

Step 4 Enter the iVIEW Communications Manager site address and select **Add**.

Step 5 Select **Close**.

Step 6 Select **OK**.

Navigating Between Pages

Problem Internet Explorer browser navigation buttons (Back, Forward and Refresh) do not work correctly in the iVIEW Management Suite user interface.

Solution Use the Next and Back buttons in iVIEW Management Suite to navigate between pages.

Configuring Maximum Time Period for Recurring Meetings

Problem You want to schedule recurring meetings for a period longer than that allowed in the iVIEW Management Suite Web user interface.

Solution Use the iVIEW Management Suite Configuration Tool to schedule recurring meetings for up to 730 days.

Correcting Web Page and Pop-up Window Display

- Problem** Some Web pages and pop-up windows do not display normally.
- Solution** Set the screen resolution to a standard resolution such as 800 x 600 pixels or 1024 x 768 pixels. The minimum recommended resolution is 800 x 600 pixels and the recommended font size is Normal or Large.

Resolving Administration Issues

Database Unavailable

- Problem** No database is available when iVIEW Management Suite is initially started.
- Solution** Restart the service when the database is ready. If the connection between the database and iVIEW Management Suite is lost after initially starting iVIEW Management Suite, iVIEW Management Suite works normally when the database is operating.

Using Double-Byte Characters in the MCU Service Template

- Problem** Unicode and other double-byte characters (such as Chinese, Japanese, Korean, and Hebrew characters) cause device exception in MCU service template Name, Description, Terminal Name and Gateway Service Prefix fields.
- Solution** Use only ASCII text in these fields.

Configuring Terminal Area Codes

- Problem** Terminal area codes are incorrectly defined.
- Solution** Do not include domestic long-distance prefixes in terminal area codes.

Assigning DID Numbers

Problem	Cannot change Direct Inward Dialing (DID) numbers
Solution	DID numbers are assigned on a per-endpoint basis rather than on a per-meeting basis. This is an internal configuration that cannot be changed via the Configuration Tool or the iVIEW Management Suite Web interface. To manually change the host name, perform the following procedure.

Procedure

- Step 1** Go to C:\Program Files\RADVISION\iVIEW Suite\iCM\jboss\bin where C is the local drive.
- Step 2** Make a backup copy of the vcs-config.xml file.
- Step 3** Open the vcs-config.xml file with a text editing tool and modify the <host-url> element to the required value.
- Step 4** Save the file in the text editor.
- Step 5** Restart iVIEW Management Suite.

Resolving IVR Issues

- [Resolving Virtual Service Issue](#) page 8
- [Resolving Video IVR Issue](#) page 9
- [Resolving Auto Route Incoming Calls Issue](#) page 10

Resolving Virtual Service Issue

Problem	If iVIEW Management Suite is in the standalone mode and a user is configured with a virtual services prefix only on iVIEW Management Suite, a call cannot be routed to Video IVR when the user calls a virtual conference ID.
Solution	Perform the procedure in this section.

Procedure

- Step 1** Login to SCOPIA ECS Gatekeeper.
- Step 2** Navigate to Gatekeeper > Endpoints > Endpoints tab.
- Step 3** Select **Add Predefined**.

- Step 4** Configure settings as follows:
- Endpoint type: Terminal
 - Registration IP: 127.0.0.1 Port: 1719
 - Call signaling IP: 127.0.01 Port: 1719
 - Aliases:
 - Value: Virtual Services; Type: Name
 - Value: Your auto virtual services prefix number; Type: Phone number
- Step 5** Select **Upload**.
- Step 6** Navigate to **Gatekeeper > Services > Services** tab.
- Step 7** Select **Add**.
- Step 8** Configure settings as follows:
- Prefix: Your auto virtual services prefix number
 - Prefix type: phone number
 - Description: Virtual Services
 - Conference Hunting: Enabled
 - Global Service: No
 - Allow access for:
 - In-zone non-predefined endpoints: enabled
 - Out-of-zone endpoints: enabled
- Step 9** Select **Upload**.

Resolving Video IVR Issue

Problem If iVIEW Management Suite is in a standalone mode and a user is configured with an auto-attendant number on iVIEW Management Suite only, a call to the auto-attendant number is not routed to Video IVR.

Solution Perform the procedure in this section.

Procedure

- Step 1** Login to SCOPIA ECS Gatekeeper.
- Step 2** Navigate to **Gatekeeper > Endpoints > Endpoints** tab.
- Step 3** Select **Add Predefined**.

- Step 4** Configure settings as follows:
- Endpoint type: Terminal
 - Registration IP: 127.0.0.1 Port: 0
 - Call signaling IP: 127.0.01 Port: 0
 - Aliases:
 - IVR Number; Type: Name
 - Your auto attendant number; Type: Phone number
- Step 5** Select **Upload**.
- Step 6** Navigate to **Gatekeeper > Services > Services** tab.
- Step 7** Select **Add**.
- Step 8** Configure settings as follows:
- Prefix: Your auto attendant number
 - Prefix type: phone number
 - Description: End Point
 - Conference Hunting: Enabled
 - Global Service: No
 - Allow access for:
 - In-zone non-predefined endpoints: enabled
 - Out-of-zone endpoints: enabled
- Step 9** Select **Upload**.

Resolving Auto Route Incoming Calls Issue

Problem If iVIEW Management Suite is in the standalone mode and a user is configured with auto route incoming calls only on iVIEW Management Suite, a call cannot be routed to Video IVR when the user calls an auto route incoming call number.

Solution Perform the procedure in this section.

Procedure

- Step 1** Login to SCOPIA ECS Gatekeeper.
- Step 2** Navigate to **Gatekeeper > Endpoints > Endpoints** tab.
- Step 3** Select **Add Predefined**.

- Step 4** Configure settings as follows:
- Endpoint type: Terminal
 - Registration IP: 127.0.0.1 Port: 5
 - Call signaling IP: 127.0.01 Port: 5
 - Aliases:
 - Value: Routing Number; Type: Name
 - Value: Your auto route incoming calls number; Type: Phone number
- Step 5** Select **Upload**.
- Step 6** Navigate to **Gatekeeper > Services > Services** tab.
- Step 7** Select **Add**.
- Step 8** Configure settings as follows:
- Prefix: Your auto route incoming calls number
 - Prefix type: phone number
 - Description: Virtual Services
 - Conference Hunting: Enabled
 - Global Service: No
 - Allow access for:
 - In-zone non-predefined endpoints: enabled
 - Out-of-zone endpoints: enabled
- Step 9** Select **Upload**.

Resolving a Port Conflict

- Problem** A port conflict occurs when you try to install or run certain applications.
- Solution** Ensure that ports 11098 and 11099 are free. Run the "netstat" command in the DOS window to determine which applications (if any) occupy ports 11098 and 11099.

Resolving a Scheduling Failure

- Problem** In iVIEW Communications Manager, in My Meetings or Meeting Monitoring, on the Current tab, if Failed appears, if you Select Failed, the message that opens reads: "Unable to create the meeting as scheduled. Please check your meeting settings."
- Solution** A scheduling failure may occur if a meeting type is downloaded, and then the meeting type is changed on the MCU but the iVIEW Communications Manager does not update the meeting types.

Procedure

- Step 1** To confirm that the reason for the failure is an incompatible meeting type, select **Admin > Meeting Types** and select **Download**.
- Step 2** If the meeting type that you specified appears in the Meeting Types (Service) Conflicts list, the reason for the scheduling failure is, at least in part, an incompatible meeting type.

Note: If a meeting is created even though the specified meeting type is incompatible, there may be resource-calculation errors.

- Step 3** To resolve the conflict, repeat the download of the meeting type you require.
- Solution** If actual MCU resources are changed after the MCU is added in iVIEW Communications Manager but iVIEW Communications Manager does not update or synchronize the actual MCU information, then the result may be an incompatible MCU.

Procedure

- Step 1** To determine which MCU is actually assigned to the meeting, select **Admin > Resource Management > MCU**.
- Step 2** Select the required MCU in the MCU column on the Current tab.
- Step 3** In the Modify MCU window, select **Synchronize**.
The MCU profile is updated.
- Step 4** Make sure the MCU registered gatekeeper is configured correctly.
- Step 5** Make sure the connection configuration in **Admin > Network Management > IP Topology** is correct.

Note: The Network Management section is hidden by default in iVIEW Communications Manager. Use the iVIEW Communications Manager Configuration Tool to change default settings in the user interface.

Resolving a Failed Terminal Invitation

Problem	You are not able to invite a terminal to a meeting.
Possible Causes	Incompatible gatekeeper registration. The MCU may be registered to a gatekeeper that is different than the one specified in the MCU profile in iVIEW Communications Manager.
Solution	Perform the procedure in this section.

Procedure

Step 1 In the MCU section of the SCOPIA MCU application, check that the ECS that is listed is the same as the one designated in iVIEW Communications Manager.

Step 2 If the gatekeeper is not the same, then in iVIEW Communications Manager, select the same gatekeeper to which the MCU is registered.

Possible Causes Authorization failure. ECS version 4.1.5.0 or later allows multiple iVIEW Communications Manager to connect as authorizer. However, if multiple iVIEW Communications Manager authorizes a single ECS, the iVIEW Communications Manager/ECS authorization logic does not work.

Solution Ensure that each ECS has only one iVIEW Communications Manager as its authorizer. If multiple iVIEW Communications Manager authorizes a single ECS, remove all other iVIEW Communications Manager authorization connections, and then restart ECS. Only after this does the remaining iVIEW Communications Manager work with this ECS properly in authorization mode.

Note: iVIEW Communications Manager initiates the authorization connection to the ECS. Ensure that the ECS server SNMP Community names are set correctly in the iVIEW Communications Manager user interface.

Possible Causes Unconnected IP location (at Network Management > IP Topology) for the MCU and a terminal.
If a meeting is set up on the MCU that belongs to a specific location defined at Network Management > IP Topology, a terminal is invited to a different location, the location to which the MCU is assigned may not be able to connect to the location to which the terminal is assigned.

Procedure

Step 1 In iVIEW Communications Manager, on the IP Topology tab, check that there is a link between the two different locations.

Step 2 Make sure that if there is a connection, that Bandwidth and Location are correctly defined.

Step 3 Alternatively, assign the MCU and the terminal to the same location.

Step 4 Make sure that the gatekeeper that the terminal is assigned to is in Authorization Mode.

Note: Cascading is set up in iVIEW Communications Manager in the Network Management section, on the IP Topology tab. If the IP Topology tab is hidden, in the iVIEW Management Suite Configuration Tool, in System Configuration > UI Settings, check **IP Topology** to activate the IP Topology tab.

Resolving a Meeting Creation Failure

Problem A meeting is successfully scheduled but cannot actually be created.

Procedure

Step 1 Make a point-to-point call.

Step 2 Ensure that the call is successful from within iVIEW Communications Manager. A successful point-to-point call indicates that the ECS and iVIEW Communications Manager are configured correctly.

Step 3 Create an endpoint-initiated MCU conference. If the endpoint connects, the MCU, ECS and iVIEW Communications Manager are configured properly. Schedule a meeting in iVIEW Communications Manager. If the meeting is scheduled successfully, wait for the meeting to start. If the meeting starts successfully, dial into the meeting using an endpoint.

Solution In the event that the troubleshooting procedures in this section do not resolve a meeting creation or meeting invitation issue, use the procedure in this section.

Procedure

Step 1 Attempt the same meeting creation or invitation directly on the MCU without using the iVIEW Communications Manager.

Step 2 If the same meeting creation or invitation does not succeed directly on the MCU, restart the MCU.

Step 3 If restarting the MCU does not resolve the issue, contact your MCU service representative.

Resolving No Video Output

Problem No video is seen during a call.

Solution In iVIEW Communications Manager:

- Check iVIEW in-meeting control and verify that the outgoing video channel is not blocked.
- Check if video packet is sent out to this caller.

Resolving Poor Video Quality

Problem End user computer is sending poor quality video.

Solution In iVIEW Communications Manager:

- Ensure there is enough bandwidth and the correct codecs in In-meeting control

For software endpoints:

- Ensure other applications do not occupy much CPU resources.

Resolving No Audio Output

Problem No audio is heard during a call.

Solution In iVIEW Communications Manager:

- First, verify the endpoint's self-audio; For software endpoints, play a clip to verify that audio can be heard. Or, for hardware endpoints, play a p2p call to verify each endpoint can hear each other.
- Check iVIEW Management Suite In-Meeting Control to verify if the outgoing audio channel is blocked.
- Verify that audio packets are sent out to this caller.
- Check if audio column is very slow.

Synchronizing SCOPIA Desktop Server with iVIEW Management Suite

Problem The Directory Status - iVIEW Management Suite tab displays a synchronization error.

Solution Perform the procedure.

Procedure

Step 1 Select the link on the Directory Status - iVIEW Management Suite tab.

The Directory tab opens.

Step 2 Select the **Synchronize** button.

Updating the IP Address on the Streaming Server

Problem The SCOPIA Desktop Status tab indicates that the Streaming Server is not connected. If you select the Streaming Server indicator, this error is displayed: "5003 Access denied error from proxy".

Solution When the Streaming or Recording components of SCOPIA Desktop are installed on their own server, separately from the SCOPIA Desktop Server, they are configured with the IP address of the SCOPIA Desktop Server which is allowed to connect to them. If the IP address of the SCOPIA Desktop Server changes, you need to update it on the Streaming and Recording Servers.

Procedure

- Step 1** From the Start menu, choose **Programs > SCOPIA Desktop > TCP Proxy Configuration**.
- Step 2** Run the listServers command to display the address of the SCOPIA Desktop Server which is allowed to access the Streaming or Recording Server.
- Step 3** If the SCOPIA Desktop Server address is incorrect, run the removeServer command to remove it.
- Step 4** Run the addServer command to add the correct address.
- Step 5** Follow on-screen directions to complete the procedure.

Changing IP Address of the SCOPIA Desktop Server

- Problem** The SCOPIA Desktop Status tab indicates that the SCOPIA Desktop Server is not connected.
- Solution** If the IP address of the server on which the SCOPIA Desktop Server is installed changes, you need to update SCOPIA Desktop Server components with its new IP address.

Procedure

- Step 1** Select **Start > Settings > Control Panel**.
- Step 2** Double-select **Add or Remove Programs**.
- Step 3** From the list of programs, choose SCOPIA Desktop, and then **Change**.
The Setup Wizard opens.
- Step 4** In the Welcome screen, select **Next**.
- Step 5** In the Program Maintenance screen, choose **Modify**, and select **Next**.
- Step 6** In the Custom Setup screen, select **Next**.
- Step 7** In the SCOPIA Desktop Serial Key screen, select **Next**.
- Step 8** In the SCOPIA Desktop Network Configuration screen, select **Next**.
- Step 9** In the SCOPIA Desktop Hostname Configuration screen, select **Next**.
- Step 10** In the SCOPIA Desktop Recording Configuration screen, select **Next**.
- Step 11** Select **Install**.

Recording Does Not Start Automatically

- Problem** iVIEW Management Suite configured to work with the SCOPIA Desktop Server does not record virtual room meetings or scheduled meetings automatically, even though iVIEW Management Suite is configured to do so.
- Solution** Verify that one of the following problems does not interfere with recording:

- There are not enough available recording ports on the SCOPIA Desktop at the time when the meeting is scheduled.
- The maximum number of simultaneous recordings is reached.
- Make sure that the **Allow virtual rooms and scheduled meetings to be recorded automatically** option is enabled on the SCOPIA Desktop Administration web user interface.



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