

SCOPIA Desktop Server

Administration 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.

Administration Guide for SCOPIA Desktop Server Version 7.5, September 2010

<http://www.radvision.com>

Table of Contents

1 Configuring SCOPIA Desktop Clients

Defining Client Video Quality and Connection Parameters	1
Defining Meeting Features.....	4

2 Rolling-Out SCOPIA Desktop to End Users

Meeting SCOPIA Desktop Client System Requirements.....	7
Installing SCOPIA Desktop Client	8
Testing Desktop Connectivity	11
Sending Meeting Invitations to End Users.....	11
Sending Administrator Messages to End Users	13
Configuring Dial String Rules	15
Manipulating Dial Strings.....	15
Adding a Dial String Rule.....	20
Editing a Dial String Rule.....	22
Delete a Dial String Rule	23

3 Maintaining the SCOPIA Desktop DeploymentSCOPIA Desktop Server

Upgrading the SCOPIA Desktop Server License	24
Upgrading SCOPIA Desktop Server Recordings	25
Backing Up Configuration Settings	25
Restoring Configuration Settings	26
Enabling Integrated Windows Authentication	27
Enabling Microsoft Internet Explorer for Integrated Windows Authentication.....	28

Integrating SCOPIA Desktop with Sametime	29
Preserving SCOPIA Desktop Presence Server Configuration	29
Working with the Content Slider.....	30
Accessing Log Files.....	32

4 Configuring SCOPIA Desktop to Manage Recording Features

Adding a Recording Server	34
Calculating Space Needed for Recording	34
Defining SCOPIA Desktop Recording Settings	35

5 Managing Recordings

Viewing Recording Information	38
Editing Recording Attributes	40
Managing Categories.....	42
Creating Categories for Multiple Recordings.....	43
Selecting Recording Owners.....	44
Recording Meetings	45
Stopping a Recording in Progress	46
Deleting a Recording	47

6 Configuring SCOPIA Desktop Server to Manage Streaming Features

Defining the Streaming Server Settings	49
--	----

7 Customizing the SCOPIA Desktop User Interface

Replacing Images.....	52
Modifying Strings	53
Saving or Restoring Branding- Related Changes	54
Restoring Default Images and Strings	55

8 Configuring SCOPIA Desktop Servers for Scalability and High Availability

Scalability with Round Robin DNS	56
--	----

Round Robin DNS Functionality	56
Round Robin DNS Limitations	58
Scalability with Generic Load Balancer	58
Generic Load Balancer Functionality	58
How to Configure Round Robin DNS and Generic Load Balancers	59
Configuring DNS Settings for Round Robin DNS	60
Configuring DNS Settings for Generic Load Balancers	60
Configuring the Tomcat Cluster	60
Configuring SCOPIA Desktop in a Cluster	61
Configuring Multiple NIC Servers.....	63
Configuring Streaming and Recording for Scalability.....	64
Configuring Load Balancer Routing Rules.....	64
Generic Load Balancer Limitations.....	65
Scalability with Radware WSD	65
Radware WSD Functionality	65
How to Configure Radware WSD	65
Configuring Network Interfaces in WSD.....	66
Configuring Routing in WSD.....	66
Configuring the Central Server Farm.....	67
Configuring Remaining Servers in the Farm.....	67
Configuring Layer 4 Policies	68
Configuring Servers of the Central Server Farm.....	68
Configuring a Single Server Farm Server.....	69
Configuring Cookie Persistency.....	70
Radware WSD Limitations.....	70

9 Securing Your SCOPIA Desktop Deployment

Enabling SCOPIA Desktop Server to Use HTTPS	71
Configuring SCOPIA Desktop Server with a Certificate.....	72
Configuring SCOPIA Desktop Clients to Accept Certificates.....	73
Enabling Encryption.....	74

10 Troubleshooting Common Issues

Viewing Status of Servers and Directory	75
---	----

Viewing Server Status and Port Resource Usage.....	75
Viewing Directory Status	78
Viewing Recording Server Status.....	79
Viewing Content Slider Status.....	81
Recording Does Not Start Automatically	81
Synchronizing SCOPIA Desktop Server with iVIEW Management Suite.....	82
Updating the IP Address on the Recording or Streaming Server	82
Changing IP Address of the SCOPIA Desktop Server	83
Upgrading SCOPIA Desktop Server Recordings.....	83
Enabling a User to Sign In.....	84

1

Configuring SCOPIA Desktop Clients

You configure SCOPIA Desktop clients in order to define the parameters related to the video quality, connection addresses, and meeting functionality. The topic included are:

- [Defining Client Video Quality and Connection Parameters.....](#) page 1
- [Defining Meeting Features.....](#) page 4

Defining Client Video Quality and Connection Parameters

During this procedure you define the maximum bandwidth used between the SCOPIA Desktop client and the SCOPIA Desktop Server. The video quality options include:

- **Standard Definition**
This option limits the client to standard definition video connection at the maximum call rate you specify. If you define a service on the MCU that enables H.323 endpoints to use a higher bandwidth rate or high definition without enabling high definition on SCOPIA Desktop, calls using this service are transcoded down to the lower rate at standard definition (CIF resolution). If you select a MCU service with a bandwidth rate lower than the value set in the Maximum Call Rate list, then the latter is used for the standard definition call to the SCOPIA Desktop client. The default value is 384K.
- **High Definition**
This option allows SCOPIA Desktop clients to connect to a conference in high definition mode. If you select this option, select a maximum call rate of at least 1024 Kbps or greater to enable the conference to continue in 720p high definition video resolution for all clients. For

deployments using SCOPIA MCU, you may want to allow SCOPIA Desktop to reduce the video resolution from 720p to 480p if you set the call rate to 1024 Kbps and there is a bandwidth congestion during a conference.

The SCOPIA Desktop Client sends up to 512 Kbps of 480p video resolution and receives the maximum call rate or rate of the service selected (the lower value of the two) of 720p video resolution. If you select a lower maximum call rate, you force the high definition service to send 480p to all clients at the lower bandwidth.

When SCOPIA Desktop is set to high definition mode and connected to a high definition service in deployments using MCU, SCOPIA Desktop limits fast update requests to avoid degradation of video quality or frame rate to all the connected endpoints.

If SCOPIA Desktop connects to a standard definition service, or if there are no high definition ports left for the high definition service, then the standard definition maximum call rate is used during a SCOPIA Desktop conference.

You can also configure the maximum transmission unit (MTU) size the SCOPIA Desktop client uses for communicating with SCOPIA Desktop. The default value is 1360. This setting should match the setting on the MCU and your network settings to avoid fragmentation.

If you need to limit UDP ports that are opened on the firewall to allow SCOPIA Desktop clients to send RTP to SCOPIA Desktop, you must define a multimedia port range. We recommend that you use a limited range between 2326 and 65535. If this option is used, each client connection uses eleven ports; to define the range, multiply the number of connections allowed by your license by eleven.

If the Streaming Server resides behind a NAT, the clients might not resolve the Streaming Server IP address. In this case the clients use the public address to connect to the Streaming Server.

If a server on which the SCOPIA Desktop Server is installed is not powerful enough to support two hundred calls, you can use the call limit setting to reduce the number of allowed calls to limit the resources used by the system.

During this procedure you also configure the SCOPIA Desktop public address which SCOPIA Desktop clients use to connect to the SCOPIA Desktop Server. To allow clients from the public network to connect, use a FQDN they can resolve. In deployments using SCOPIA iVIEW Management Suite, if clients cannot send messages to the Presence Server directly because no ports are open, the SCOPIA Desktop Server tunnels the XMPP messages using this public address.

Before You Begin

Navigate to the SCOPIA Desktop Server Administration web user interface.

Procedure

Step 1 Select the **Client** icon in the sidebar.

Figure 1-1 Scopia Desktop Administration Client Icon



Step 2 Select the **Settings** tab.

Step 3 To configure settings for standard definition, select a bandwidth rate from the Maximum Call Rate list.

Step 4 To configure settings for high definition:

Figure 1-2 Maximum Call Rate Section

The screenshot shows a configuration window titled "Maximum Video Quality". It contains the following text and controls:

- Text: "The Maximum Call Rate defines the maximum bandwidth used between the SCOPIA Desktop client and the SCOPIA Desktop server."
- Control: Standard Definition
- Control: Maximum Call Rate (Kb/s): 448 (352p) [dropdown arrow]
- Control: High Definition
- Control: Maximum Call Rate (Kb/s): 1024 (720p) [dropdown arrow]
- Control: Allow SCOPIA MCU version 5.x to negotiate high definition calls down to 480p

- Select the High Definition check box.
- Select a bandwidth rate from the Maximum Call Rate list.
- If necessary, select the Allow SCOPIA MCU version 5.x to negotiate high definition calls down to 480p check box.

Step 5 Enter a value in the MTU Size field.

Figure 1-3 MTU Size Section

The screenshot shows a configuration window titled "MTU Size". It contains the following text and controls:

- Text: "The MTU Size specifies the maximum transmission unit size the client will use when communicating with SCOPIA Desktop."
- Control: MTU Size: 1360 [input field]

Step 6 If necessary, configure a multimedia port range by entering values for the lowest multimedia port and the highest multimedia port.

Step 7 Insert the public address.

Figure 1-4 Connection Information

The screenshot shows a configuration window titled "Connection Information". It contains the following text and controls:

- Text: "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."
- Control: Public Address: sdbeta.RADVISION.com [input field]

Step 8 Enter a value in the Call Limit field.

Figure 1-5 Call Limit Section

The screenshot shows a configuration window titled "Call Limit". It contains the following text and controls:

- Text: "Limit the total number of ports used for group or relayed point to point calls."
- Control: Call Limit: [input field]

Step 9 Select OK or Apply.

Defining Meeting Features

This section describes how each of the meeting features affect SCOPIA Desktop administration and the end user experience:

When the Desktop Sharing option is enabled, the SCOPIA Desktop Server participants can present applications and share their desktops with other participants. You can optionally allow only moderators to share their desktops. When desktop sharing is not enabled, the Present button does not appear, but the other sections are still available.

The Raise Hand feature allows a muted user to request the permission to speak. For deployments with multiple SCOPIA Desktop Servers, we recommend that you clear this check box. As a result, moderators will not see requests made by participants using a different SCOPIA Desktop Server.

You can enable the Custom Panel option to display an additional custom panel in the SCOPIA Desktop Live Meeting Console. The custom panel location is preconfigured and cannot be changed.

The URL parameters are passed to the custom URL as follows: `?meetingid=NNN&nickname=XXX`, where NNN is the ID of the meeting the user is connected to, and XXX is the nickname of the connected user. You can also use the custom panel URL to specify additional URL parameters. You must use the URL-encoding for the additional URL parameters. For example, if the custom panel URL is `"http://www.mycustompanel.com/myservlet?arg1"` and the SCOPIA Desktop entry page or conference room is launched with the additional argument `"?CUSTOM=arg2%26arg3% 3D123"`, the custom panel opens to the URL `"http://www.mycustompanel.com/myservlet?arg1&arg2&arg3=123"`.

Configure the Push to Talk option to define how participants use the microphone button in the SCOPIA Desktop Live Meeting Console:

- Allow users to join a meeting with their microphone on—The microphone is on and the audio output is sent when participants enter a meeting. The participants must select the microphone button to mute themselves.
- Force users to join a meeting with their microphone off—The microphone is off and the audio output is not sent when participants enter a meeting. The participants must select the microphone button to unmute themselves.
- Force users to hold down their microphone button while speaking—Participants must select and hold down the microphone button to activate their microphones and to send their audio output.

You can also configure these security features:

- sRTP media encryption between SCOPIA Desktop clients and the SCOPIA Desktop—Encrypting media (audio, video, presentation) between SCOPIA Desktop Server and the SCOPIA Desktop client may be used, for example, in a corporate deployment where the SCOPIA Desktop Server is used to invite people outside of your network. Since this option only enables secure encryption of the media, you need to secure the web portal.
- SCOPIA Desktop Callback—Choosing the **Allow Users to have SCOPIA Desktop Server call them back** option enables the video device callback option on the SCOPIA Desktop user entry page. When users select Use my computer for presentation only on connecting to a meeting, the Callback my video device number option becomes available. The Callback my video device number provides the option to call back the H.323 device when the users connect, so users can connect in “data only” mode to a meeting from their computers and automatically connect their H.323 devices at the same time.

Note:

In "data only" mode users can see the participant list, moderate, chat, and show or view presentations. Users can view or send neither audio nor video.

The H.323 device can be disconnected automatically when users disconnect their computers from the call.

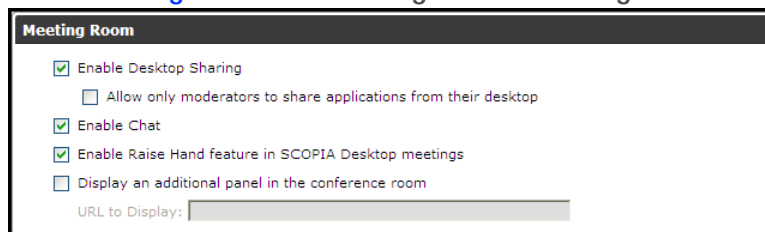
Before You Begin

Navigate to the SCOPIA Desktop Server Administration web user interface.

Procedure

- Step 1** Select the Client icon in the sidebar.
- Step 2** Select the Meeting Features tab.
- Step 3** In the Meeting Room section, configure the Desktop Sharing option as desired.

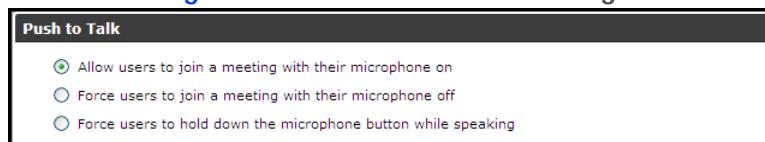
Figure 1-6 Meeting Room Settings



- Step 4** Configure the Chat option as required.

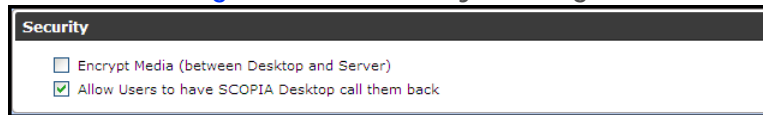
For deployments with multiple SCOPIA Desktop Servers, it is recommended that you do not enable the Chat option. A participant using one SCOPIA Desktop Server cannot join the chat started by a participant using another SCOPIA Desktop Server.
- Step 5** Configure the Raise Hand option as desired.
- Step 6** Define the additional custom panel option as desired:
 - a. Select the Display an additional panel in the conference room check box to enable the option.
 - b. Enter the URL in the field.
- Step 7** Define the Push to Talk option as desired.

Figure 1-7 Push to Talk Settings



Step 8 Define security options as desired.

Figure 1-8 Security Settings



Step 9 Select OK or Apply.

2

Rolling-Out SCOPIA Desktop to End Users

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

- [Meeting SCOPIA Desktop Client System Requirements.....](#) page 7
- [Installing SCOPIA Desktop Client](#) page 8
- [Testing Desktop Connectivity](#) page 11
- [Sending Meeting Invitations to End Users.....](#) page 11
- [Sending Administrator Messages to End Users.....](#) page 13
- [Configuring Dial String Rules](#) page 15

SCOPIA DesktopSCOPIA Desktop Server

Meeting SCOPIA Desktop Client System Requirements

Observe these guidelines when preparing a SCOPIA Desktop client installations:

- Requirements for interactive connections using Standard Definition video settings:
 - PC Intel[®] Pentium 4, 3.0 GHz or faster
 - PC AMD[®] Athlon 64 GHz or faster
 - PC Intel[®] Centrino Mobile Processor 1.8 GHz or faster
 - Mac[®] with Intel Core 2 Duo 1.9 GHz or faster
 - Notebook - Intel[®] Atom Processor 1.6 GHz or faster
 - 1 GB RAM or more
- Requirements for interactive connections using High Definition video settings:
 - PC Intel[®] Core 2 Duo 2.4 GHz or faster
 - PC AMD[®] Phenom IIx4 910 - 2.6 GHz or faster
 - Mac with Intel Core 2 Duo 2.7 GHz or faster
 - Minimum 2 GB RAM, 3 GB RAM or more recommended

- Best platform is i5 or i
- Best platform for laptop is i5 or i7
- Operating System:
 - Windows® XP (SP3 recommended for 32 Bit machines)
 - Windows® Vista (SP2 or higher for 64 Bit machines)
 - Windows® 7
 - Macintosh OS X version 10.5 (leopard) or higher Intel CPU only
- OS Languages Supported:
 - English
 - Japanese
- Supported Browsers:
 - Internet Explorer® 7 or above
 - Firefox® 3.6
 - Safari 4.0 (Mac)

Observe these guidelines when viewing webcasts or recorded meetings only:

- Operating System:
 - Windows® 7
 - Windows® 2003
 - Windows® Vista, SP2
 - Windows® XP, SP2, SP3
 - Mac® OS X 10.4-10.6
- Web Browsers:
 - Internet Explorer® 7 or 8
 - Firefox® 2, 3, or 3.5
 - Safari® 3.1

Installing SCOPIA Desktop Client

The Scopia Desktop client installation portal provides an automatic download and update manager. When you select the Updates link, the Updates Manager allows you to view any currently installed components and versions, and to install optional components, including the Outlook Add-In and the Contact List.

In addition to automatic downloads, Administrators can push SCOPIA Desktop client to end users in two ways:

- Active Directory Scripting Administrative Push - RADVISION provides scripts that can be run on Active Directory to push the client component installation on the desktops that are part of a domain. For more information see the RADVISION whitepaper Active Directory Scripting.
- System Management Server (SMS) Push - Allows IT administrators to centrally install, configure and monitor client installations. For more information the RADVISION whitepaper System Management Server.

Note: You must be logged into the portal in order to install all components at once. If you are not logged in then you can only install the client - not the Contact List or Outlook plugin. These components are reserved for authenticated users to access corporate systems to schedule and make calls.

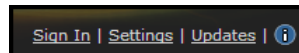
Before You Begin

- 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 required audio device to your computer, i.e., headset or speaker and microphone, or a USB audio device.
- Connect a video camera or web cam to your computer.

Procedure

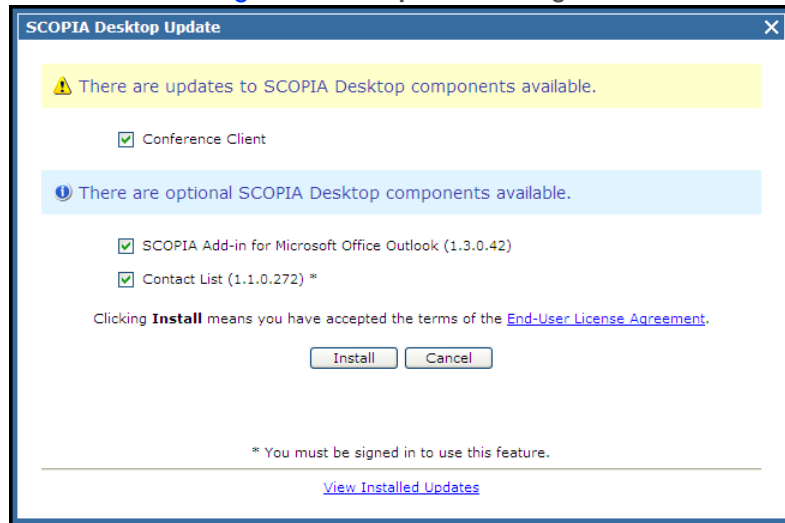
- Step 1** To activate SCOPIA Desktop for the first time, go to the SCOPIA Desktop portal page at: <http://sd.company.com>.
- Step 2** Select **Update**


Figure 2-1 Client Download and Update Link



Step 3 Select the check box next to any optional components.

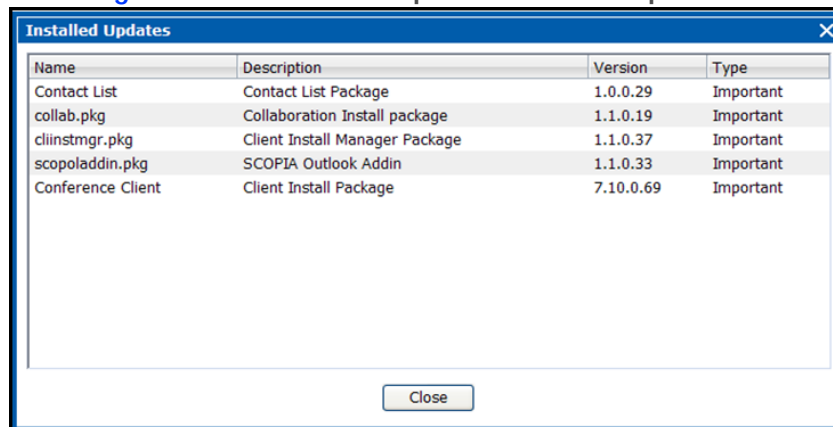
Figure 2-2 Update Manger



Step 4 Select **Install**. When the SCOPIA Desktop installation is complete, you should see the following icon in the task tray at the lower right corner of the screen: 

Step 5 To verify that any optional components were installed, select the **View Installed Updates** link. A list of installed components appears.

Figure 2-3 Installed Updates and Components



Testing Desktop Connectivity

As a best practice, after configuring your SCOPIA Desktop deployment, you should install the client on a local computer and attempt to enter a meeting room to verify connectivity. This section describes how to check whether or not a client is connected to SCOPIA Desktop Server.

Procedure

- Step 1** Verify that your video and audio peripheral equipment is connected to your desktop PC and configured correctly.
- Step 2** From a client machine (with Windows XP Service Pack 2 or higher), connect to SCOPIA Desktop Server via the following URL:
http://<FQDN>/scopia
- Step 3** You are prompted to install SCOPIA Desktop client.

Note: If you have not yet installed SCOPIA Desktop client or if you need to update your version of SCOPIA Desktop client, a yellow message displays on SCOPIA Desktop Server entry page. Select the link to access the page from which you can install SCOPIA Desktop client.

- Step 4** After installing SCOPIA Desktop client, enter a meeting ID in SCOPIA Desktop Server that starts with one of the following:
- The prefix configured on your SCOPIA MCU for the SCOPIA Desktop service.
 - A valid iVIEW Management Suite virtual room ID.
- The SCOPIA Desktop client loads and your own video stream is displayed.

Note: Ensure there is no firewall enabled on your machine that might block the SCOPIA Desktop client.

Sending Meeting Invitations to End Users

This section describes how to view and edit the default instructions for joining a meeting that the SCOPIA Desktop Server Outlook add-on sends to invitees, and how to modify the contents of these e-mail invitations.

While modifying the contents of e-mail invitations, you can define these links:

- Meeting URL—For connecting to a SCOPIA Desktop meeting.
- Portal URL—For watching a webcast or a recorded meeting.

If you have multiple SCOPIA Desktop Servers and want participants to know about them, insert link information for each of them into each SCOPIA Desktop e-mail configuration.

For example, if you have one SCOPIA Desktop Server in Europe, one in Asia, and another in the US, you could place the following information in your e-mail:

“From Europe, connect to <http://europe.server.com/scopia?ID=1234>

From Asia, connect to <http://asia.server.com/scopia?ID=1234>

From the US, connect to <http://us.server.com/scopia?ID=1234>

Before You Begin

Navigate to the SCOPIA Desktop Administration web user interface.

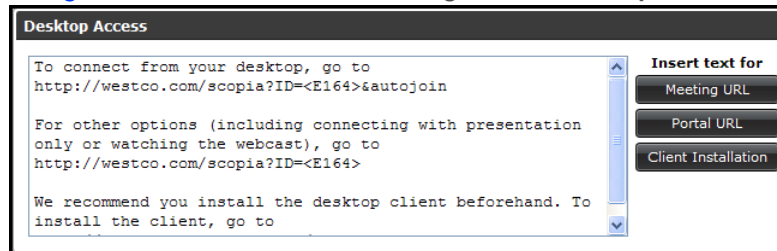
Procedure

Step 1 Select **Messages and Invitations** in the sidebar.

Step 2 Select the **Invitations** tab.

The default instructions for accessing the meeting from a desktop, phone or video conferencing device appear in the screen.

Figure 2-4 Invitation Message for Desktop Access



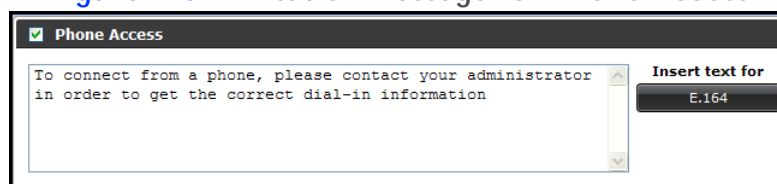
Step 3 In the Desktop Access section:

- Select **Meeting URL** to insert a link to the meeting.
- Select **Portal URL** to insert a link to the SCOPIA Desktop portal entry page.
- Select **Client Installation** to insert a link used to ensure that the SCOPIA Desktop client is installed and up-to-date.

Note: The automatically inserted server address is the SCOPIA Desktop Server Fully Qualified Domain Name specified during installation.

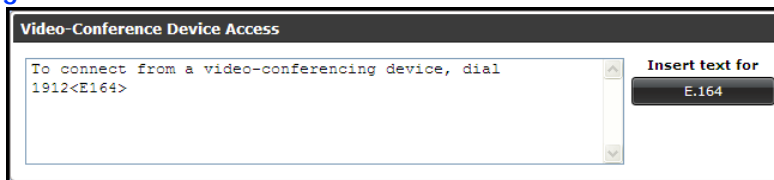
Step 4 In the Phone Access area, select **E.164** to insert the required E.164 alias. If your deployment does not include a gateway, leave the checkbox unchecked and the gateway information will not be included in Outlook.

Figure 2-5 Invitation Message for Phone Access



Step 5 In the Video-Conference Device Access area, select E.164 to insert the required E.164 alias.

Figure 2-6 Invitations for Video Communication Devices



Step 6 Select OK or Apply.

Sending Administrator Messages to End Users

You can use the Administrative message appearing on the SCOPIA Desktop Server portal entry page to post important information such as: system status, scheduled shutdown, or configuration tips. This section describes how to edit the Administrator and Dial Plan messages.

The Dial Plan message appears in the Invitation dialog box. You can use this message to provide users with dialing tips, for example, explain what prefixes they should use for gateways of different types.

These tags and attributes are supported in the administrator messages text editor:

- ``
- ``
- `<iframe src="http*"></iframe>`
- ``
- `<u></u>`
- `<i></i>`
- ``
- `
</br>`
- ``
- ``
- ``
- `<p></p>`
- `<div></div>`

You must fix a width and height of the `<iframe>` tag according to the style sheet of the corresponding page. For example, for the portal entry page, the style sheet looks like this:

```
<style>
    .motd iframe
```

```
        {  
            width: 100%;  
            height: 150px;  
        }  
    </style>
```

The administrator message text editor replaces single ‘&’ characters with ‘&’; it also replaces ‘<’ and ‘>’ of invalid tags with ‘<’ and ‘>’ respectively.

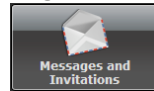
Before You Begin

Navigate to the SCOPIA Desktop Server Administration web user interface.

Procedure

Step 1 Select the **Messages and Invitations** icon in the sidebar.

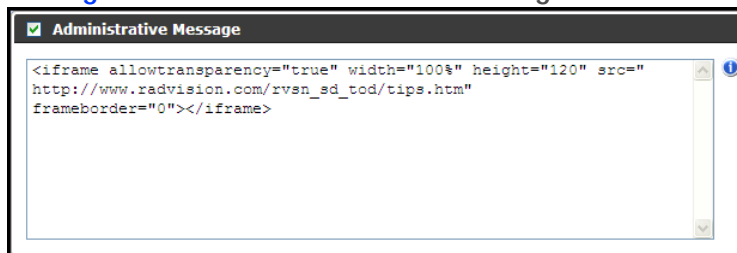
Figure 2-7 Messages and Invitations Icon



Step 2 Select the **Messages** tab.

Step 3 Select the **Administrative Message** check box.

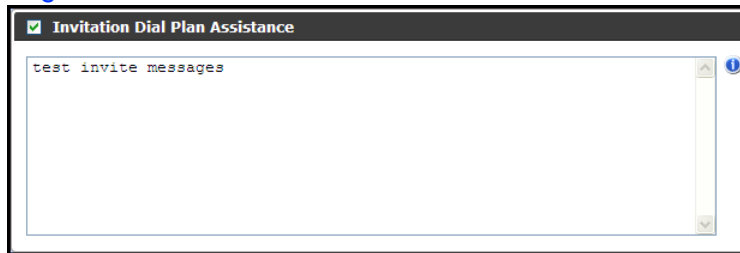
Figure 2-8 Administrative Messages Section



Step 4 Modify the text of the entry page message as required.

Step 5 Select the Invitation Dial Plan Assistance check box.

Figure 2-9 Invitation Dial Plan Assistance Section



Step 6 Modify the text of the invitation message as required.

Step 7 Select OK or Apply.

Configuring Dial String Rules

This section describes how to configure dial string rules which SCOPIA Desktop applies for inviting by E.164 or IP phones. Dial string rules cause the SCOPIA Desktop Server to replace a prefix or strip it off and to add a suffix.

- [Manipulating Dial Strings](#)..... page 15
- [Adding a Dial String Rule](#)..... page 20
- [Editing a Dial String Rule](#)..... page 22
- [Delete a Dial String Rule](#) page 23

Manipulating Dial Strings

In SCOPIA Solution deployments dial string manipulation is necessary in the following scenarios:

- When a call must be routed to local H.323 PSTN or ISDN gateways. In this case SCOPIA Desktop needs to detect phone numbers and modify the prefix to add routing information.
- When there is a SIP PBX either in enterprise premises or a remote location which SCOPIA Desktop must use to dial phone numbers. In this case SCOPIA Desktop needs to detect phone numbers in the directory and append the SIP URL to forward it to the right gateway.

There are several methods SCOPIA Desktop uses to perform dial string manipulation:

- string normalization
- prefix or suffix substitution
- prefix or suffix addition
- prefix stripping

You must configure rules according to which SCOPIA Desktop manipulates dial strings.

Notice that during substitution this logic is used:

- SCOPIA Desktop performs dial string normalization prior to applying other string manipulation rules. During normalization any non-numeric characters except “+” are removed. See [Table 2-1](#).

Table 2-1 Examples of Dial String Normalization

Initial String	Normalized String
1 (603) 407-5956	1603407-5956
+1 (603) 407-5956	+16034075956
+44 (141) 776-9462	+441417769462

- There is a certain order in which SCOPIA Desktop applies the rules. For example, it first applies more restrictive rules like those that cause SCOPIA Desktop to match long strings combining specific and non-specific characters.
- If during the rule configuration you leave the replacement string blank, SCOPIA Desktop strips the prefix from the address. In order to keep the string, configure this string as the replacement string.

In the following example, consider what kind of manipulation is necessary:

- Change any phone number that starts with the New Hampshire area code +1603, 1603, or 603 and followed by exactly seven digits to the gatekeeper/gateway prefix of 1370 followed by the seven digits for the local phone extension.
- Route any other long distance number indicated by +1 and followed by 10-digit phone number to the New Jersey gatekeeper/gateway by substituting 11701 for the +1 and keeping the 10 digits.
- Route the international England country prefix of +44 followed by any random number of digits to the 10700 London gateway.

[Table 2-2](#) shows what rules are configured for the required dial string manipulation.

Table 2-2 Rule settings

Match Prefix	Replacement	Optional Suffix	Comments
+1603xxxxxxx	1370		603 routed to local call gateway
1603xxxxxxx	1370		603 routed to local call gateway
603xxxxxxx	1370		603 routed to local call gateway
+1xxxxxxxxxx	11701		All other long distance calls routed to other gateway.
+44	10700		International calls to England go to the London local call gateway

When SCOPIA Desktop applies these rule, it results in this dial string manipulation:

Table 2-3 Dial String Manipulation Result

Normalized String	Substituted String
16034725956	13704725956
+16034725956	13704725956
+15081234567	117015081234567
+441417769462	107001417769462

Table 2-4 provides an example of the H.323 gateway dial plan where:

- 13—Prefix for the New Hampshire gatekeeper/gateway
- 11—Prefix for the New Jersey gatekeeper/gateway
- 10—Prefix for the London gatekeeper/gateway
- 15—Prefix for the Hong King gatekeeper/gateway
- 70—Prefix for audio gateway

Table 2-4 Example of H.323 Gateway Dial Plan

Match prefix	Replacement	Optional Suffix	Comments
Fixed string length examples			
+91508xxxxxxx	13701508		Use New Hampshire gateway for MA calls
+1508xxxxxxx	13701508		Use New Hampshire gateway for MA calls
1508xxxxxxx	13701508		Use New Hampshire gateway for MA calls
508xxxxxxx	13701508		Use New Hampshire gateway for MA calls
91603xxxxxxx	1370		Use New Hampshire gateway (local call seven digits)
+1603xxxxxxx	1370		Use New Hampshire gateway (local call seven digits)
1603xxxxxxx	1370		Use New Hampshire gateway (local call seven digits)
603xxxxxxx	1370		Use New Hampshire gateway (local call seven digits)
91xxxxxxxxxx	11701		Use New Jersey gateway for long distance calls
+1xxxxxxxxxx	11701		Use New Jersey gateway for long distance calls
1xxxxxxxxxx	11701		Use New Jersey gateway for long distance calls
Variable string examples			
01144	10700		Use London gateway (needs extra 0)
+44	10700		Use London gateway (needs extra 0)
011852	1570		Use Hong Kong gateway for local calls (without extra 0)
+852	1570		Use Hong Kong gateway for local calls (without extra 0)
011	1170011		Use New Jersey for other international calls

In the following example, consider what kind of manipulation is necessary:

- Route any phone number that starts with the New Hampshire area code +1603, 1603 or 603 and then followed by exactly seven digits to New Hampshire SIP gateway by adding the “@sipgateway.nh.com” suffix to the remaining seven digits.
- Route any other long distance number indicated by +1 and followed by 10-digit phone number to the New Jersey SIP gateway by adding the “@sipgateway.nj.com” suffix to the 10 digits.
- Route the international Israel country prefix of +44 followed by any random number of digits to the 10700 London gateway by replacing the prefix with 0 and adding the “@sipgateway.london.com” suffix.

Table 2-2 shows what rules are configured for the required dial string manipulation.

Table 2-5 Rule settings

Match Prefix	Replacement	Optional Suffix	Comments
+1603xxxxxxx		@sipgateway.nh.com	603 routed to local call gateway
1603xxxxxxx		@sipgateway.nh.com	603 routed to local call gateway
603xxxxxxx		@sipgateway.nh.com	603 routed to local call gateway
+1xxxxxxxxxx	1	@sipgateway.nj.com	All other long distance calls routed to the New Jersey gateway.
+44	0	@sipgateway.london.com	International calls to England go to the London international gateway

When SCOPIA Desktop applies these rule, it results in this dial string manipulation:

Table 2-6 Dial String Manipulation Result

Normalized String	Substituted String
16034725956	4725956@@sipgateway.nh.com
+16034725956	4725956@sipgateway.nh.com
+15081234567	15081234567@sipgateway.nj.com
+441447769462	1447769462@sipgateway.london.com

Table 2-7 provides an example of the SIP gateway dial plan where:

- 13—Prefix for the New Hampshire gatekeeper/gateway
- 11—Prefix for the New Jersey gatekeeper/gateway
- 10—Prefix for the London gatekeeper/gateway
- 15—Prefix for the Hong King gatekeeper/gateway
- 70—Prefix for audio gateway

Table 2-7 Example of SIP Gateway Dial Plan

Match prefix	Replacement	Optional Suffix	Comments
Fixed string length examples			
+91508xxxxx xx	1508	@sipgateway.nh.co m	Use New Hampshire gateway for MA calls
+1508xxxxxx x	1508	@sipgateway.nh.co m	Use New Hampshire gateway for MA calls
1508xxxxxxx	1508	@sipgateway.nh.co m	Use New Hampshire gateway for MA calls
508xxxxxxx	1508	@sipgateway.nh.co m	Use New Hampshire gateway for MA calls
91603xxxxxx x		@sipgateway.nh.co m	Use New Hampshire gateway for New Hampshire calls
+1603xxxxxx x		@sipgateway.nh.co m	Use New Hampshire gateway for New Hampshire calls
1603xxxxxxx		@sipgateway.nh.co m	Use New Hampshire gateway for New Hampshire calls
603xxxxxxx		@sipgateway.nh.co m	Use New Hampshire gateway for New Hampshire calls
91xxxxxxxxx x	1	@sipgateway.nj.co m	Use New Jersey gateway for long distance calls
+1xxxxxxxxx x	1	@sipgateway.nj.co m	Use New Jersey gateway for long distance calls
1xxxxxxxxxx	1	@sipgateway.nj.co m	Use New Jersey gateway for long distance calls
Variable string examples			
01144	0	@sipgw.london.com	Use London gateway (needs extra 0)
+44	0	@sipgw.london.com	Use London gateway (needs extra 0)
011852		@sipgw.hk.com	Use Hong Kong gateway for local calls (without extra 0)
+852		@sipgw.hk.com	Use Hong Kong gateway for local calls (without extra 0)
011	011	@sipgw.nj.com	Use New Jersey for other international calls

Adding a Dial String Rule

The prefix matches the beginning of a dialed string. To correctly represent the number of digits in a string, use the "x" character as a wildcard to match any digit. For example, "603" matches any dial string that begins with "603", while "603xxxxxxx" matches only a dial string beginning with "603" and consisting of ten digits. You cannot use any other characters, such as a space, a dash or a parenthesis.

Before You Begin

Navigate to the SCOPIA Desktop Administration web user interface.

Procedure

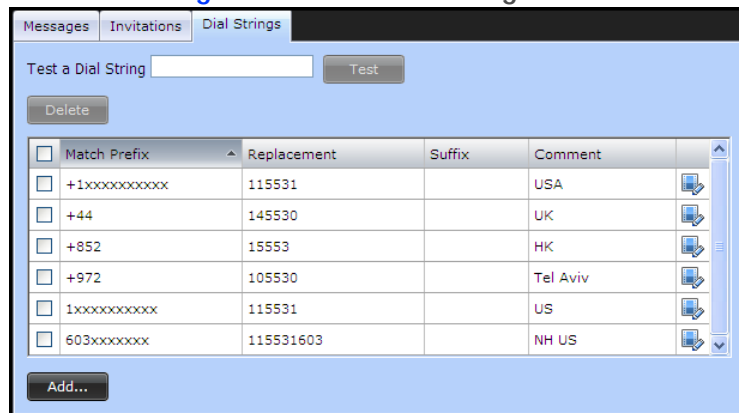
Step 1 Select the Messages and Invitations icon in the sidebar.

Figure 2-10 Messages and Invitations Icon



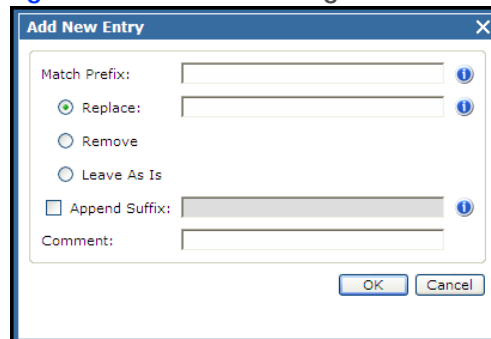
Step 2 Select the Dial Strings tab.

Figure 2-11 Dial Strings Tab



Step 3 Select Add.
The Add New Entry window opens.

Figure 2-12 Dial Strings New Entry



Step 4 Enter the prefix in the Match Prefix field.

- Step 5** Select one of these options:
- **Replace**—A string matching the prefix is replaced with another string.
 - **Remove**—A string matching the prefix is stripped from the dial string.
 - **Leave As Is**—A string matching the prefix is left as is.
- Step 6** If you selected the Replace option, enter the replacing prefix in the field.
- Step 7** To add a suffix, select the **Append Suffix** check box, and then enter the suffix in the field.
- Step 8** Enter a comment.
- Step 9** Select **OK**.
- Step 10** To test the new dial string rule:
- Enter a string in the Test a Dial String field.

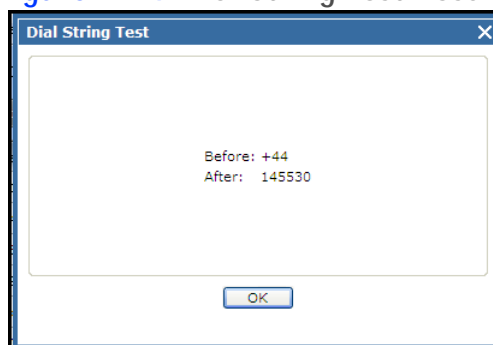
Figure 2-13 Dial String Test



- Select the check box for the rule you want to apply to this string.
- Select **Test**.

The Dial String Test window appears displaying the dial string after the rule is applied.

Figure 2-14 Dial String Test Results



Editing a Dial String Rule

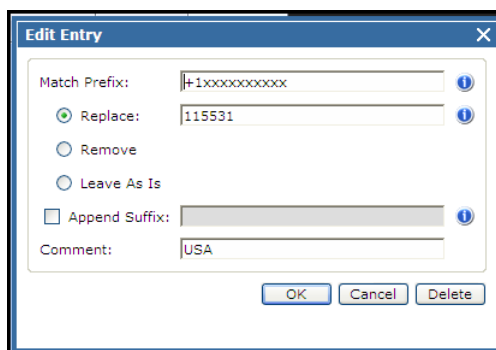
Before You Begin

Navigate to the SCOPIA Desktop Administration web user interface.

Procedure

- Step 1** Select **Messages and Invitations** in the sidebar.
- Step 2** Select the **Dial Strings** tab.

- Step 3** Select the Edit icon.
The Edit Entry window opens.



- Step 4** Edit the dial string as required.
Step 5 Select OK.

Delete a Dial String Rule

Before You Begin

Navigate to the SCOPIA Desktop Administration web user interface.

Procedure

- Step 1** Select Messages and Invitations in the sidebar.
Step 2 Select the Dial Strings tab.
Step 3 Locate the rule you need to edit and select the check box next to it.
Step 4 Select Delete.
Step 5 Select OK in the confirmation message.

3

Maintaining the SCOPIA Desktop DeploymentSCOPIA Desktop Server

Occasional system upgrades and infrastructure changes in your network may require additional system maintenance activities to maintain your SCOPIA Desktop deployment. This section includes the following topic to assist you in maintaining your deployment:

- [Maintaining the SCOPIA Desktop DeploymentSCOPIA Desktop Server](#) page 24
- [Upgrading SCOPIA Desktop Server Recordings](#)..... page 25
- [Backing Up Configuration Settings](#) page 25
- [Restoring Configuration Settings](#) page 26
- [Enabling Integrated Windows Authentication](#) page 27
- [Enabling Microsoft Internet Explorer for Integrated Windows Authentication](#)..... page 28

Upgrading the SCOPIA Desktop Server License

You need to update the SCOPIA Desktop Server license in these cases:

- If you upgrade the SCOPIA Desktop Server by adding the recording feature or increasing the number of simultaneous recordings which requires a new or updated recording serial key
- If you upgrade SCOPIA Solution components by adding SCOPIA MCUs and additional ports on the SCOPIA Desktop Server

Before You Begin

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

Procedure

- Step 1** Select **Start > Settings > Control Panel**.
- Step 2** Double-click **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 window, enter updated keys, and then select **Next**.
- Step 8** Follow on-screen instructions to complete installation configuration.

Upgrading SCOPIA Desktop Server Recordings

If there are recordings created using SCOPIA Desktop Server version 5.x, upgrade them by performing these steps:

Note: You can upgrade recordings at any time.

Procedure

- Step 1** Install QuickTime version 7.6.2 or higher. You can download QuickTime at <http://www.apple.com/quicktime/download/>.
- Step 2** On the SCOPIA Desktop Server, navigate to the <INSTALLDIR>\config location.
- Step 3** Double-click the recording_converter.exe file.
- Step 4** Follow the on-screen instructions. Depending of the size and amount of recordings, the upgrade may take time.
- Step 5** The recordings are converted and the log files are created in this folder.
- Step 6** Verify that the recordings are converted correctly.
- Step 7** Delete backed up recordings.

Backing Up Configuration Settings

Certain configuration files used by SCOPIA Desktop should be backed up regularly to allow recovery from catastrophic system failure or instances of corrupted files. During this backup procedure you copy the xml files which contain these settings:

- dial string rules
- administrative message
- invitation message
- Presence Server database
- local database

Procedure

- Step 1** Navigate to the following directory: `<installdir>\data`.
- Step 2** Copy the relevant files into a location outside the installation directory:
- `motd.html`—for administrator message
 - `dialplanhelp.html`—for invitation message
 - `members.xml`—for local database
 - `dial_string_manipulators.xml`—for dial string rules

Note: The `members.xml` is created only if you use SCOPIA Desktop without SCOPIA iVIEW Management Suite and add terminals to a local directory (using Directory section in admin GUI).

Restoring Configuration Settings

You may need to restore some of the configuration files used by SCOPIA Desktop to allow recovery from catastrophic system failure or instances of corrupted files.

Procedure

- Step 1** Stop the service "SCOPIA Desktop - Apache Tomcat".
- Step 2** Navigate to the following directory: `<installdir>\data`.
- Step 3** Replace the relevant file with the backup file:
- `motd.html`—for administrator message
 - `dialplanhelp.html`—for invitation message
 - `members.xml`—for local database
 - `dial_string_manipulators.xml`—for dial string rules
- Step 4** Start the service "SCOPIA Desktop - Apache Tomcat".

Note: The `members.xml` is created only if you use SCOPIA Desktop without SCOPIA iVIEW Management Suite and add terminals to a local directory (using Directory section in admin GUI).

Enabling Integrated Windows Authentication

When SCOPIA Desktop Server is enabled to use Integrated Windows Authentication, the user name and password are verified before being sent across the network. The client browser proves its knowledge of the password through a cryptographic exchange with your Web server. By default, the current Windows user information on the client is used for authentication.

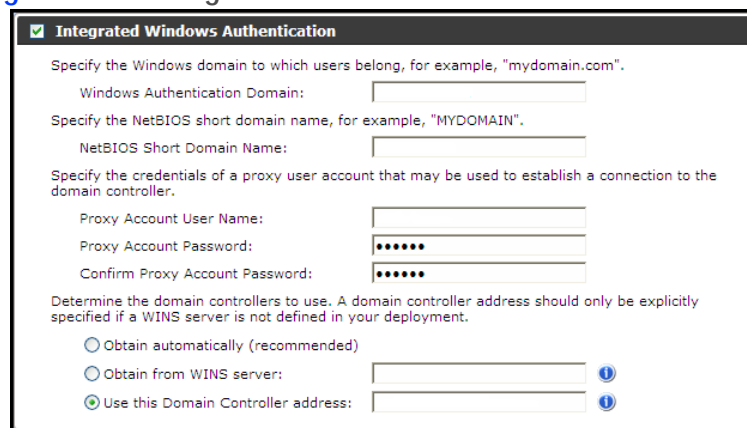
Before You Begin

Ensure that authentication settings are configured for iVIEW Management Suite. Navigate to the SCOPIA Desktop Administration web user interface.

Procedure

- Step 1** Select the **Directory and Invitations** icon in the sidebar.
The **Settings** tab is displayed.
- Step 2** Select the **Use Integrated Windows Authentication** check box.

Figure 3-1 Integrated Windows Authentication Settings



The screenshot shows a web form titled "Integrated Windows Authentication" with a checked checkbox. The form contains several sections:

- Specify the Windows domain to which users belong, for example, "mydomain.com".**
Windows Authentication Domain: [text input field]
- Specify the NetBIOS short domain name, for example, "MYDOMAIN".**
NetBIOS Short Domain Name: [text input field]
- Specify the credentials of a proxy user account that may be used to establish a connection to the domain controller.**
Proxy Account User Name: [text input field]
Proxy Account Password: [password input field with dots]
Confirm Proxy Account Password: [password input field with dots]
- 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: [text input field] ⓘ
 - Use this Domain Controller address: [text input field] ⓘ

- Step 3** Enter the windows domain to which users belong.
- Step 4** Enter the NetBIOS short domain name.

Note: The NetBIOS short domain name field is case sensitive.

- Step 5** Enter the Proxy account user name.
- Step 6** Enter the Proxy account password.
- Step 7** If a WINS server is not defined, enter the domain controller address.

Related Topics

- SCOPIA Solution Deployment Guide

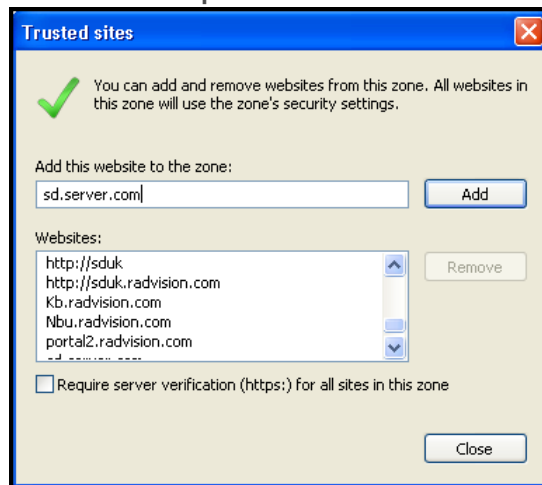
Enabling Microsoft Internet Explorer for Integrated Windows Authentication

For SCOPIA Desktop to work properly with Integrated Windows Authentication, the SCOPIA Desktop Server must be either located in the Intranet zone or be in the list of trusted sites. You must perform this procedure on SCOPIA Desktop client computers to enable Integrated Windows Authentication.

Procedure

- Step 1** Verify whether Integrated Windows Authentication is enabled for your Internet Explorer:
- In the Internet Explorer window, from Tools menu select **Internet Options**.
 - Select the **Advanced** tab.
 - Under Security section, verify that **Enable Integrated Windows Authentication** checkbox is selected.
- Step 2** To add SCOPIA Desktop Server to the list of Internet Explorer trusted sites:
- In the Internet Explorer window, from Tools menu select **Internet Options**.
 - Select the **Security** tab.
 - Select **Trusted Sites**, and then select **Sites**.

Figure 3-2 Internet Explorer Trusted Sites Configuration



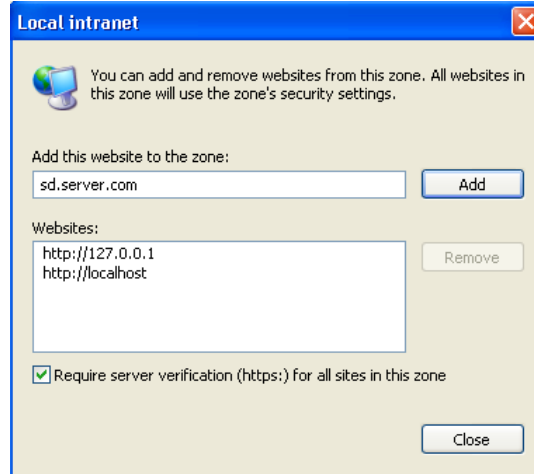
- Enter the SCOPIA Desktop Server site address, for example "sd.server.com" ., and then select **Add**.
- Select **Custom level**.
- Under User Authentication section, select the **Automatic logon with current user name and password** option.
- Select **OK**.

Step 3 To add SCOPIA Desktop Server to the Internet Explorer Intranet zone:

- In the Internet Explorer window, from Tools menu select **Internet Options**.

- b. Select the **Security** tab.
- c. Select **Local Intranet**.
- d. Select **Sites**.
- e. Select **Advanced**.

Figure 3-3 Internet Explorer Advanced Security Settings



- f. Enter the SCOPIA Desktop Server site address, for example "sd.server.com" ., and then select **Add**.
- g. Select **Custom level**.
- h. Under User Authentication section, select the **Automatic logon only in Intranet zone** option.
- i. Select **OK**.

Integrating SCOPIA Desktop with Sametime

For SCOPIA Desktop deployments working with Lotus Sametime Web Conferencing plug-in, you must configure Sametime-related administrative settings. For information about configuring Sametime settings, refer to the SCOPIA Connector for IBM Lotus Sametime Installation Guide.

Preserving SCOPIA Desktop Presence Server Configuration

Perform the procedure described in this section to preserve the SCOPIA Desktop Presence Server configuration to solve the issue.

Procedure

Step 1

Backup the current Presence Server configuration:

- a. Save the ejabberd.cfg file at the ...\Jabber\conf location into a different location.

- b. Save any folders under the ...\\Jabber\\database folder into a different location.
- Step 2** Navigate to the ...\\Jabber\\install location and double-click the ejabberd-2.0.3-windows-installer.exe file.
The Installation wizard opens.
- Step 3** Modify the installation directory in the Installation Directory window to be C:\\Program Files\\Radvision\\SCOPIA Desktop\\Jabber, and then select **Next**.
- Step 4** Leave the default domain in the ejabberd server domain window, and then select **Next**.
The default domain is changed either via the Jabber Config tool or by replacing the ejabberd.cfg file after installation, and then select **Next**.
- Step 5** Leave the default admin name in the Administrator user name window, and then select **Next**.
- Step 6** Enter the administrator password and re-enter it for confirmation in the Administrator password window, and then select **Next**.
- Step 7** Select the required option in the Cluster window, and then select **Next**.
- Step 8** After the installation is complete, perform this:
- Restore the database and ejabberd.cfg file.
 - Set the service to automatic.

Working with the Content Slider

The Content Slider allows SCOPIA Desktop users to browse presentations and is compatible with both SCOPIA Desktop and Mobile users.

The Content Slider is a part of the recorder component, from both an installation and admin management perspective. Slider functionality is tied to your recording license, and shares the same base configuration (such as network address, gatekeeper/MCU, etc.). They also re-use the same TCP connection for control channel and share the ACL/TLS configuration.

Make note of these considerations when using the Content Slider:

- Generated slides are stored as files in a folder on a local or network mounted drive.
- For every slider session, SCOPIA Desktop specifies a slide folder, a slide set name, slide size and compression rate.
- SCOPIA Desktop saves slides using a base slide set name and incremental indexing.

For deployments with a single SCOPIA Desktop Server, these scenarios are supported:

- All-in-one. All components are installed on the same box. Recorder/slider share SCOPIA Desktop resources with live calls and webcasts.
- Separate box install. The recorder/slider is installed on a separate box and has a dedicated SCOPIA Desktop Server.

Note: The recorder and slider always shares SCOPIA Desktop resources and disk space for generated recordings/slides.

For deployments with multiple SCOPIA Desktop Servers, these options are available:

- Centralized recorder/slider. Owners of a single recording license install one recorder server. All SCOPIA Desktop Servers point to that recorder. Recordings are served for playback from the central site, while slides are downloaded to and served from a local SCOPIA Desktop.
- Distributed recorders/sliders. Owners of separate recording licenses for each recorder server install a recorder on each site. This provides distribution where licenses are not counted as a pool (separate number for each recorder); recordings are only available from the SCOPIA Desktop Server they are made from.

Figure 3-4 displays the Content Slider tab and all slider sessions currently in progress, and provides details about the server(s) where there are non-active sessions.

Figure 3-4 Content Slider Tab



If there are errors with a slider session, notices appear as links (per server) in the Problems column. Details are available by selecting the problem link.

Accessing Log Files

SCOPIA Desktop automatically maintains extensive logs to help maintain your deployment and troubleshoot problems. By accessing the Logging tab, you can turn on enhanced logging, which provides network trace on the server (with or without media, depending on your selection) as well as extended middleware logging.

Note: Enabling enhanced logging for extended periods of time adds large log files to the system. However, you can turn this feature on/off at anytime.

Before You Begin

Navigate to the SCOPIA Desktop Server Administration web user interface.

Procedure

Step 1 Select the Status icon in the sidebar.

Step 2 Select the Logging tab.

Figure 3-5 Logging Tab



Step 3 To download a zipped version of current log files, select the Download button.

Step 4 (Optional) To enable enhanced logging, select the Enable button.

The Logging Summary displays the current status of enhanced logging - enabled or disabled.

4

Configuring SCOPIA Desktop to Manage Recording Features

SCOPIA Desktop allows users to record meetings and to view recorded meetings. A recording includes all media types: audio, video and presentation.

Servers used for recording meetings must have a recording license installed on them. SCOPIA Desktop supports up to 10 simultaneous recordings. If you did not provide the Recording Server license key during SCOPIA Desktop Server installation, a default evaluation license allows you to record one five-minute meeting at a time.

In advanced deployments where authentication is enabled on iVIEW Management Suite, recordings may be designated as public or private. Public recordings are available for all users, including authenticated and guest users. Authenticated users can record private recordings, automatically becoming the recording's owner. Only recording owners can watch private recordings. By default all recordings are public. Recordings made by guest users are always public.

Note: Recordings made using SCOPIA Desktop version 5.x appear as public in SCOPIA Desktop version 7.5.

This section describes how to configure recording settings as well as manage recordings if a SCOPIA Desktop Server is configured to manage recording.

- [Adding a Recording Server](#) page 34
- [Calculating Space Needed for Recording](#) page 34
- [Defining SCOPIA Desktop Recording Settings](#) page 35

Adding a Recording Server

If during the SCOPIA Desktop Server installation the Recording Server was not installed and users recorded meetings using the evaluation license, you can add the Recording Server to the deployment.

Before You Begin

Prior to modifying the SCOPIA Desktop installation, acquire the recording license and make sure you have the license key for the Recording Server.

Procedure

- Step 1** Open the Control Panel.
- Step 2** Select the SCOPIA Desktop Server and select **Change**.
The SCOPIA Desktop Server Installation Wizard opens.
- Step 3** Select a language and select **OK**.
The Welcome screen is displayed.
- Step 4** Select **Next**.
- Step 5** Select **Modify**, and then select **Next**.
The Custom Setup screen opens.
- Step 6** Select the **Recording Server** icon and select the **This feature will be installed on local hard drive** option.
- Step 7** Select **Next**.
The SCOPIA Desktop License Key screen opens.
- Step 8** Enter the license key for the Recording Server, and then select **Next**.
The Network Configuration screen opens.
- Step 9** Select **Next** in the rest of the configuration screens.
- Step 10** In the Ready to Modify the Program screen, select **Install**.

Calculating Space Needed for Recording

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

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

For example, for a call of 1 hour at 384 Kbps, calculate as follows:

$384 \text{ Kbps} \times (60 \text{ minutes} \times 60 \text{ seconds}) = 1382400 \text{ Kbits}$
 $1382400 \div 1024 = 1350$

$1350 \div 8 = 168.75 \text{ Mbytes}$
 $168.75 \times 20\% = 33.75 \text{ (overhead)}$

$168.75 + 33.75 = 202.5 \text{ Mbytes (including overhead)}$

Defining SCOPIA Desktop Recording Settings

You can configure recording settings as well as manage recordings if you select this server to manage recording.

The public address you define during this procedure performs a similar role to the public address defined for the SCOPIA Desktop Server. If the SCOPIA Desktop Recording Server resides behind a NAT, the clients may not resolve the SCOPIA Desktop Recording Server IP address. In this case the clients use the public address to connect to the SCOPIA Desktop Recording Server.

If SCOPIA iVIEW Management Suite is configured to work with the SCOPIA Desktop Server, recording policies configured on SCOPIA iVIEW Management Suite determine whether users are allowed to record meetings or not. However, for deployments without iVIEW Management Suite, you need to define the recording policy on SCOPIA Desktop Server by enabling the recording option for SCOPIA Desktop users.

You also define the following parameters during this configuration:

- Video size and Recording bit rate—These parameters are used to control the quality of recordings.
Setting the recording bit rate to a value lower than 256 Kbps can affect the quality and framerate of the H.239 Data in the live connection and streaming modes.
- Maximum Recording Duration—The value set for this parameter controls maximum allowed duration for any recording.
- Send tone periodically during recording—This parameter defines the frequency of the sound signal played during a recording which serves to remind users that their meeting is being recorded.

In deployments where the Recording Server is installed on the same server as the SCOPIA Desktop Server, users watching recorded meetings take up SCOPIA Desktop bandwidth which can be used for other purposes, such as meetings. Use the Playback Bandwidth area to configure bandwidth usage for such deployments. Set the Total Bandwidth Allowed value to define a total amount of bandwidth SCOPIA Desktop uses for playing back recorded meetings.

You can use the iVIEW Management Suite to automatically record either a virtual room or a scheduled meeting when the meeting begins.

If the deployment in use comprises multiple SCOPIA Desktop Servers, automatic recording is performed on all SCOPIA Desktop Servers and several identical recordings are created. In this case we recommend that you allow one of the SCOPIA Desktop Servers to perform automatic recording, while disabling the SCOPIA MCU automatic recording feature on the rest of the SCOPIA Desktop Servers in the deployment. The procedure in this section describes how to disable the automatic recording feature on a SCOPIA Desktop Server.

For example, if you set the Total Bandwidth Allowed value to 100 Mb/s, then SCOPIA Desktop allows 100 Mb/s bandwidth if one user watches a recording and 50 Mb/s bandwidth for each user if two users watch recordings. You need to set the Minimum Bandwidth required for download value to prevent too many users from watching recordings at the same time.

When you enable high definition recording in deployments using SCOPIA MCU, SCOPIA Desktop Server starts recording in high definition. If the attempt to record in high definition fails, the SCOPIA Desktop Server automatically switches to standard definition and continues recording.

Before You Begin

- Navigate to the SCOPIA Desktop Server Administration web user interface.
- Select **Deployment** in the sidebar, and verify that the **Recording** check box is selected.
- Select **Status** in the sidebar, and verify that the IP address in the **Recording Server Address** field is correct.

Procedure

Step 1 Select Recording in the sidebar.

Figure 4-1 SCOPIA Desktop Recording Icon



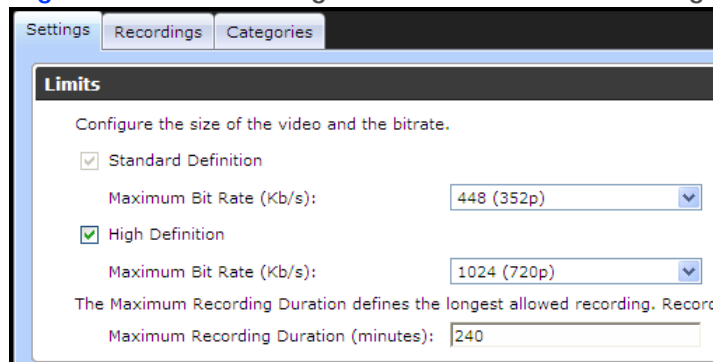
The Settings tab is displayed.

Step 2 To configure standard definition recording, in the Limits section select a value from the Maximum Bit Rate list under Standard Definition.

Step 3 To configure high definition recording, in the Limits section:

- a. Select the **High Definition** check box.
- b. Select a value from the Maximum Bit Rate list under High Definition.

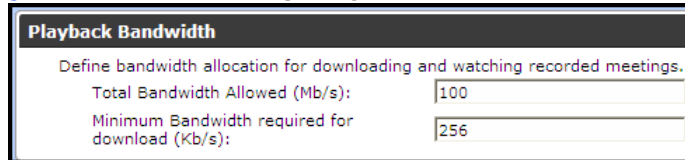
Figure 4-2 Recording Video and Bitrate Settings



Step 4 Enter a value in the Maximum Recording Duration field.

Step 5 In the Playback Bandwidth section, enter a value in the **Total Bandwidth Allowed** field.

Figure 4-3 Recording Playback Bandwidth Settings



The screenshot shows a configuration window titled "Playback Bandwidth". Below the title is a subtitle: "Define bandwidth allocation for downloading and watching recorded meetings." There are two input fields: "Total Bandwidth Allowed (Mb/s):" with the value "100" and "Minimum Bandwidth required for download (Kb/s):" with the value "256".

Step 6 Enter a value in the Minimum Bandwidth required for download field.

Step 7 In the Policies section, choose an option from the **Send tone periodically during recording list**.

Step 8 To disable automatic recording feature, clear the **Allow virtual rooms and scheduled meetings to be recorded automatically** check box.

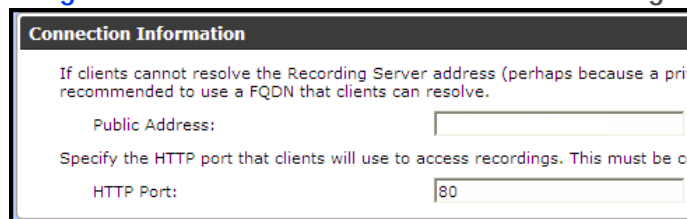
Step 9 For deployments without iVIEW Management Suite, select the **Allow meeting participants to record** check box to enable recording for SCOPIA Desktop users.

For deployments using iVIEW Management Suite, this setting cannot be modified in SCOPIA Desktop since iVIEW Management Suite controls the recording policies.

Step 10 In the Connection Information section, enter a FQDN in the Public Address field.

We recommend that you use a FQDN that clients can resolve.

Figure 4-4 Connection Information Settings



The screenshot shows a configuration window titled "Connection Information". Below the title is a subtitle: "If clients cannot resolve the Recording Server address (perhaps because a priv recommended to use a FQDN that clients can resolve." There are two input fields: "Public Address:" and "HTTP Port:" with the value "80".

Step 11 Enter the HTTP port.

This port is used by clients to access the recording. You must configure the HTTP port on the Recording Server and open this port on the firewall

Step 12 Select **OK** or **Apply**.

Related Topics

- SCOPIA Solution Deployment Guide

5

Managing Recordings

This section provides instruction for creating and managing recordings within SCOPIA Desktop. The topic included are:

- [Viewing Recording Information](#) page 38
- [Editing Recording Attributes](#) page 40
- [Managing Categories](#)..... page 42
- [Creating Categories for Multiple Recordings](#)..... page 43
- [Selecting Recording Owners](#)..... page 44
- [Recording Meetings](#) page 45
- [Stopping a Recording in Progress](#) page 46
- [Deleting a Recording](#) page 47

Viewing Recording Information

You can review the list of recordings made on this SCOPIA Desktop using the Recordings tab. The following information is displayed:

- Meeting ID
- Name
- Start Time
- Duration

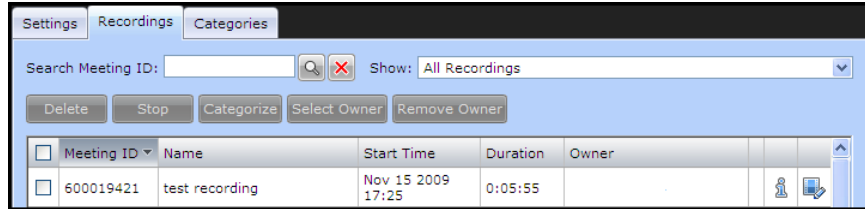
Note: For meetings that are currently being recorded, the “In progress” indication is displayed.

- PIN-protected indicator
- Owner (only in advanced deployments where authentication is enabled on iVIEW Management Suite)

You can also access for the following additional information for a specific recording:

- Description
- Categories—Keywords associated with recordings
- Recording URL

Figure 5-1 Scopia Desktop Administration - Recordings Tab



Before You Begin

Navigate to the SCOPIA Desktop Server Administration web user interface.

Procedure

Step 1 Select Recording icon in the sidebar.

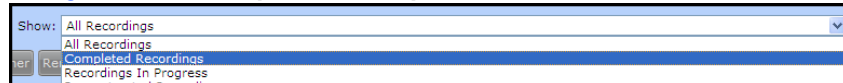


Step 2 Select the Recordings tab.

The Recordings tab is displayed showing a list of recordings. By default all recordings are displayed.

Step 3 To filter recordings, select a category from the Show list.

Figure 5-2 Scopia Desktop Administration - Show List



Step 4 To sort recordings, select the column according to which you want to sort.

Step 5 To search for a specific recording by an attribute:

- Meeting ID—Select the Meeting ID column, enter the meeting ID in the Search field, and then select the Search button.
- Owner—Select the Owner column, enter the owner name in the Search field, and then select the Search button.
- Meeting Name—Select any column except the Meeting ID and Owner columns, enter the meeting name in the Search field, and then select the Search button.

Figure 5-3 Recording Tab Search Box




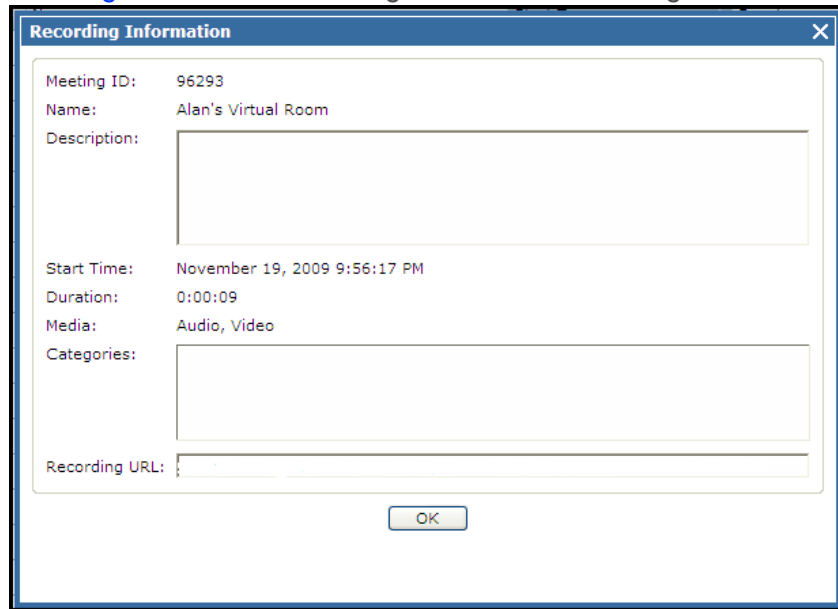
Step 6 To display additional information for a specific recording, select the Information icon:  The Meeting Information window opens.

Figure 5-4 Recording Information Dialogue Box



The image shows a 'Recording Information' dialog box with the following fields:

- Meeting ID: 96293
- Name: Alan's Virtual Room
- Description: (empty text area)
- Start Time: November 19, 2009 9:56:17 PM
- Duration: 0:00:09
- Media: Audio, Video
- Categories: (empty text area)
- Recording URL: (empty text field)

An 'OK' button is located at the bottom center of the dialog box.

Editing Recording Attributes

You can assign either an owner or an access PIN for recording security. The access PIN is optional and is used for viewing recordings. In the list of recorded meetings, recordings protected by an access PIN are marked by a key icon. If you assign an owner to a recording, only the owner can edit it. There are no PINs for recordings assigned to owners.

Before You Begin

Navigate to the SCOPIA Desktop Server Administration web user interface.

Procedure


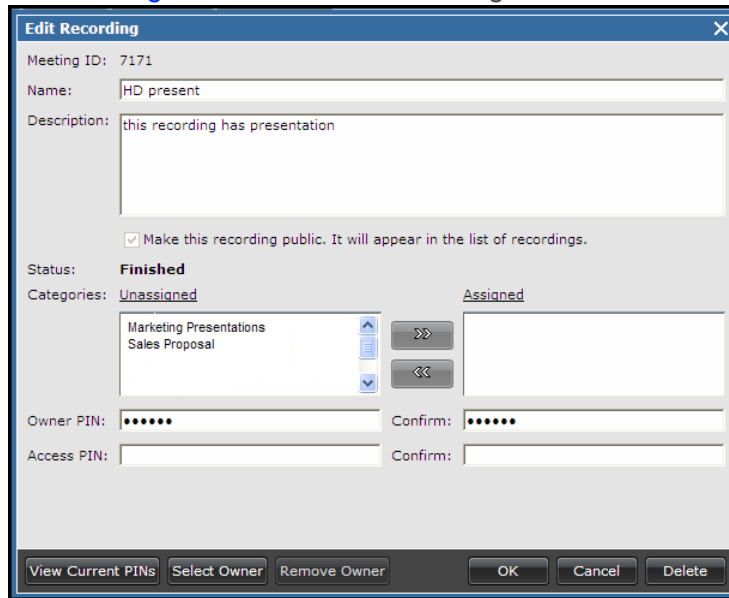
- Step 1** Select Recording icon the sidebar.
- Step 2** Select the Recordings tab.
- Step 3** Select the Manage Recording button for the required recording in the list: 
The Edit Recording window is displayed.

Figure 5-5 Edit Recording Window



- Step 4 To modify the recording name and description, enter new text in relevant fields.
- Step 5 If necessary, select the check box to make the recording public.
- Step 6 If you enabled user authentication, you can select or remove a recording owner.
- Step 7 To modify categories for the recording, select a category in the relevant pane and select the Transfer button.
- Step 8 To set the owner PIN for the recording, enter the owner PIN.
- Step 9 To set the access PIN, enter the access PIN.
- Step 10 Select OK.

Managing Categories

Apart from standard attributes like an ID, name, and duration, SCOPIA Desktop provides a category—a special attribute that can help organizing and searching recordings. Both users and administrators can assign categories to recordings. Administrators manage categories by modifying a list of existing categories, while users can only select categories from this list to associated them with recordings.

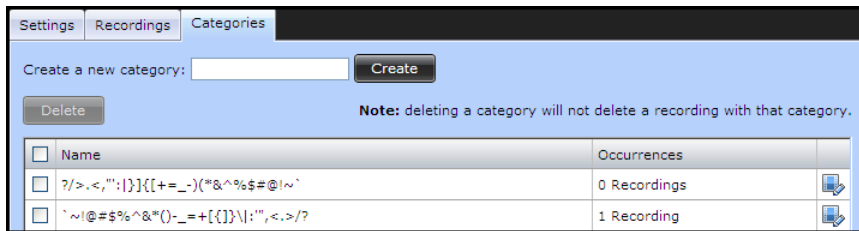
If you rename an existing category, SCOPIA Desktop automatically updates attributes for all recordings belonging to the modified category. Deleting a category does not cause SCOPIA Desktop to delete recordings belonging to the deleted category.

Before You Begin

Navigate to the SCOPIA Desktop Server Administration web user interface.

Procedure

- Step 1 Select the **Recording** icon in the sidebar.
- Step 2 Select the **Categories** tab.



- Step 3 To create a new category:
 - a. In the Create a new category field, enter the name.
 - b. Select **Create**.The new category appears in the list.

- Step 4 To edit an existing category:
 - a. Select the **Edit** icon:
 - b. Enter the new name for the category.
 - c. Select **OK**.

- Step 5 To delete an existing category:
 - a. Select the **Delete** icon.
 - b. Select **Yes**.

Creating Categories for Multiple Recordings

You can create categories for multiple recordings at once. For example, you may want to group a specific presenter's recordings and save them separately from recordings of other presenters.

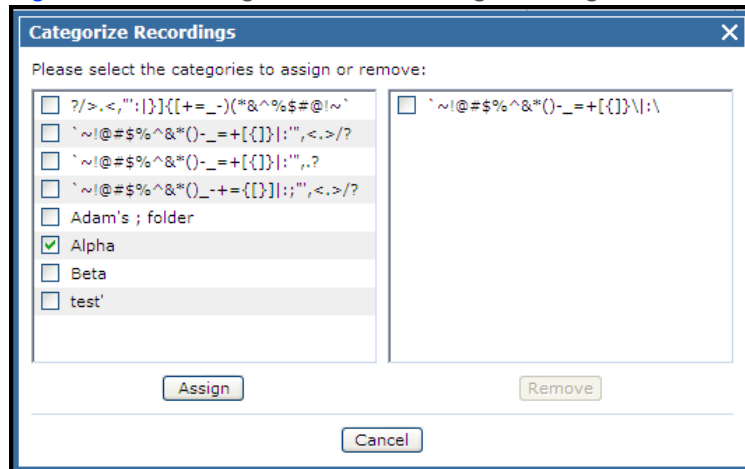
Before You Begin

Navigate to the SCOPIA Desktop Server Administration web user interface.

Procedure

- Step 1** Select Recording in the sidebar.
- Step 2** Select the Recordings tab.
- Step 3** In the recording list, select check boxes for required recordings.
- Step 4** Select the Categorize button.
The Categorize Recordings window opens.

Figure 5-6 Categorize Recordings Dialogue Window



- Step 5** To assign a category, which is not currently assigned to selected recordings:
 - a. In the left pane, select the check box for this category.
 - b. Select **Assign**.
- Step 6** To remove a category, which is currently assigned to selected recordings:
 - a. In the right pane, select the check box for this category.
 - b. Select **Remove**.

Selecting Recording Owners

You can assign ownership to recordings when you want to grant administrative control for a recording to a specific user.

Before You Begin

Navigate to the SCOPIA Desktop Server Administration web user interface.

Procedure

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

Step 2 Select the **Recordings** tab.

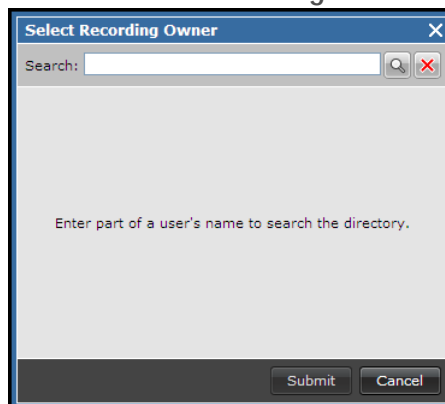
Step 3 In the recording list, select check boxes for each recording you want to assign to an owner.

<input checked="" type="checkbox"/>	7123	Large Meeting January 21 4pm	Jan 21 2010 22:52	1:16:49	Adam Pitcher
-------------------------------------	------	------------------------------	----------------------	---------	--------------

Step 4 Select **Select Owner**.

The Select Recording Owner window opens.

Figure 5-7 Select Recording Owner Window



Step 5 Select the owner name from the Search field.

Step 6 Select **Submit**.

Step 7 To remove an owner which is currently assigned to selected recordings:

- a. Select the check box for the recording in the list.
- b. Select **Remove**.

Recording Meetings

You can record meetings using the SCOPIA Desktop Server Administration web user interface.

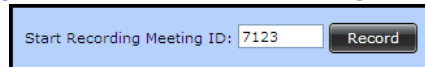
Before You Begin

- Verify that you have the ID of a meeting you wish to record.
- Navigate to the SCOPIA Desktop Server Administration web user interface.

Procedure

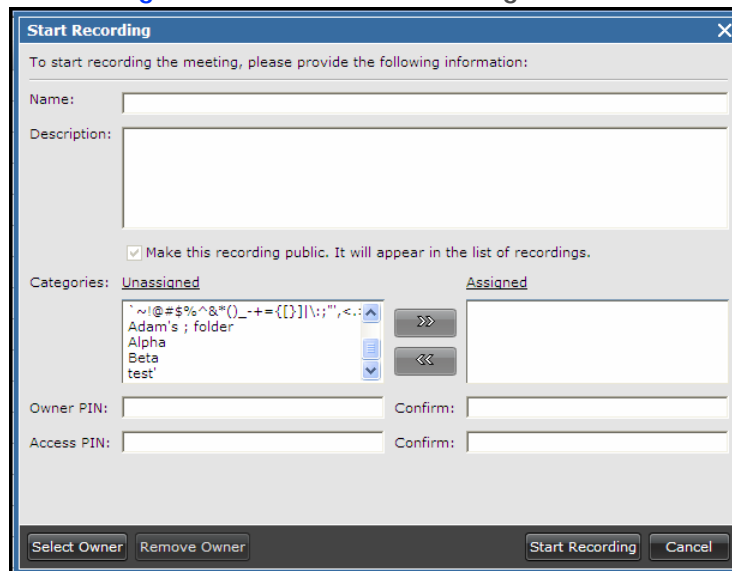
- Step 1** Select the Recording icon in the sidebar.
- Step 2** Select the Recordings tab.
- Step 3** In the Start recording meeting ID field, enter ID.

Figure 5-8 Start Recording Button



- Step 4** Select Record.
- The Start Recording window is displayed.

Figure 5-9 Start Recording Window

A screenshot of a "Start Recording" dialog box. The title bar says "Start Recording" with a close button (X). The main text says "To start recording the meeting, please provide the following information:". Below this are several fields: "Name:" with a text input field; "Description:" with a larger text area; a checked checkbox labeled "Make this recording public. It will appear in the list of recordings."; "Categories:" with two lists: "Unassigned" (containing a regex pattern, "Adam's ; folder", "Alpha", "Beta", "test") and "Assigned" (empty). There are right and left arrow buttons between the lists. Below the categories are "Owner PIN:" and "Access PIN:" fields, each with a "Confirm:" field to its right. At the bottom are buttons for "Select Owner", "Remove Owner", "Start Recording", and "Cancel".

- Step 5** Enter recording name and description.
- Step 6** Assign categories as necessary.
- Step 7** To set the owner PIN for the recording:
- a. Choose either the Use the moderator PIN as the Owner PIN or Specify an Owner PIN option.
 - b. Enter the owner PIN.
 - c. Enter the owner PIN in the Confirm field.

- Step 8** To set the meeting PIN:
 - a. Choose the **Use the meeting PIN as the Access PIN** or **Specify an Owner PIN** option.
 - b. Enter the access PIN.
 - c. Enter the access PIN in the Confirm field.
- Step 9** To set an owner for the meeting, select **Select Owner**.
- Step 10** If you set an owner for the meeting, select the **Make this recording private** check box.
- Step 11** Select **Start Recording**.
The meeting appears in the list, and its duration is indicated as "In Progress".

Stopping a Recording in Progress

You can stop any recording which is in progress. When you do so, meeting participants are notified that the recording is stopped. The meeting moderator receives a notification that the recording is stopped by the administrator.

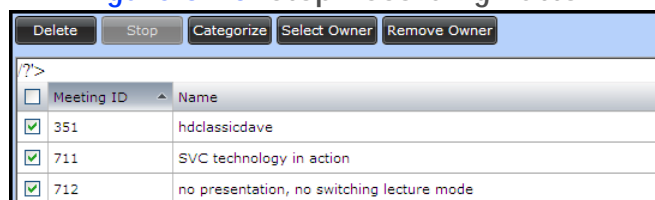
Before You Begin

Navigate to the SCOPIA Desktop Server Administration web user interface.

Procedure

- Step 1** Select **Recording** in the sidebar
- Step 2** Select the **Recordings** tab.
- Step 3** In the recording list, select the check box for recordings you wish to stop.

Figure 5-10 Stop Recording Button



- Step 4** Select **Stop**.
- Step 5** Select **Yes** in the confirmation message.

Deleting a Recording

You can permanently remove a recording from SCOPIA Desktop by deleting it from the recording list.

When you delete a recording which is in progress, the meeting participants are notified that the recording is stopped. Also, the meeting moderator receives a notification that the recording was deleted by the administrator.

Before You Begin

Navigate to the SCOPIA Desktop Server Administration web user interface.

Procedure

- Step 1** Select **Recording** in the sidebar.
- Step 2** Select the **Recordings** tab.
- Step 3** In the recording list, select the check box for recordings you wish to delete.
- Step 4** Select **Delete**.
- Step 5** Select **Yes** in the confirmation message.

6

Configuring SCOPIA Desktop Server to Manage Streaming Features

This section describes how to configure SCOPIA Desktop streaming settings. Streaming can be managed either by a single SCOPIA Desktop Server or by multiple SCOPIA Desktop Servers. If a single SCOPIA Desktop Server is set to manage streaming, all other participants are directed to this server. If multiple SCOPIA Desktop Server are configured to manage streaming, each manages streaming independently.

To designate a single SCOPIA Desktop Server to manage streaming, enable streaming on this SCOPIA Desktop Server. In this case you must disable streaming on other SCOPIA Desktop Servers in the same deployment. However, you can configure those servers to allow the viewing of webcasts from the SCOPIA Desktop Server on which streaming is enabled. To enable multiple SCOPIA Desktop Servers for managing streaming, enable streaming on each SCOPIA Desktop Server in this deployment.

The iVIEW Communications Manager Streaming feature requires an additional license.

[Table 6-1](#) compares deployments using a single SCOPIA Desktop Server to deployments using multiple SCOPIA Desktop Server for streaming.

Table 6-1 Comparison of Streaming Server Deployment Types

Characteristic	Single SCOPIA Desktop Server enabled for streaming	Multiple SCOPIA Desktop Servers enabled for streaming
HTTP performance	Slower HTTP performance over the Internet between dispersed sites and the designated SCOPIA Desktop Server.	Faster HTTP performance within local sites.
Load on Streaming Server	Many streaming clients at different sites sharing the resources of a single streaming server.	Streaming clients at individual sites share a local streaming server.
SCOPIA Desktop Server management	Single location for managing streaming.	Streaming must be enabled or disabled on each individual SCOPIA Desktop Server.
Participant count	All participants connected to the central SCOPIA Desktop Server are shown in the meeting display.	Only participants connected to a specific local SCOPIA Desktop Server are shown.

This section includes a single topic:

- [Defining the Streaming Server Settings..... page 49](#)

Defining the Streaming Server Settings

You need to perform the procedure described in this section only if you enabled streaming during deployment configuration.

The public address you define during this procedure performs a similar role to the public address defined for the SCOPIA Desktop Server. If the Streaming Server resides behind a NAT, the clients might not resolve the Streaming Server IP address. In this case, the clients use the public address to connect to the Streaming Server.

You can enable and configure multicast streaming to allow an unlimited number of simultaneous streaming connections. Multicast streaming in SCOPIA Desktop is performed without Streaming Server support. If the IP address of a client computer is not within the multicast IP address range you configured, this client will use a unicast streaming connection.

During multicast configuration you also need to define the Time to Live value—the number of transmissions of a multicast packet that SCOPIA Desktop propagates throughout the network. Setting this value to 1 means that a multicast packet stays within a local network. The change in the multicast streaming configuration applies only to meetings created after the change takes place; the change does not effect meetings in progress.

By default, the maximum number of ports used for streaming is 600. However, we recommend that you adjust the number of ports value to match the supported number of streaming ports based on the CPU and Memory system requirements.

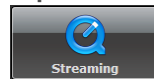
Before You Begin

- Navigate to the SCOPIA Desktop Server Administration web user interface.
- Select Deployment in the sidebar and verify that streaming is enabled on the Servers page.

Procedure

Step 1 Select the **Streaming** icon in the sidebar.

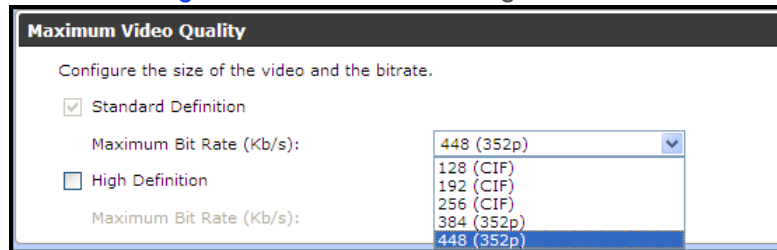
Figure 6-1 Scopia Desktop Administration Streaming Icon



Step 2 Select the **Settings** tab.

Step 3 To configure standard definition recording, select a value from the Maximum Bit Rate list under Standard Definition.

Figure 6-2 Video Settings Section

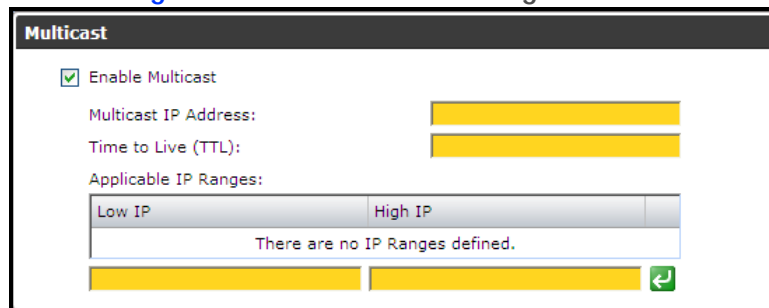


Step 4 To configure high definition recording, perform the following:

- a. Select the **High Definition** check box.
- b. Select a value from the Maximum Bit Rate list under High Definition.

Step 5 If necessary, configure multicast settings:

Figure 6-3 Multicast Settings Section



- a. Check the **Enable Multicast** option.

b. Enter the multicast IP address.

The valid multicast IP address is in the range of 224.0.0.1 and 239.255.255.255.

c. Enter the Time to Live value.

d. Define clients that will be able to watch multicasts by entering IP range in the fields and selecting the Arrow button.

Step 6 Enter a public address.

We recommend to use a public address that clients can resolve.

Step 7 Enter a TCP streaming port.

The default port is 7070.

Note: If you use a TCP port different from the default value of 7070, you must open this port on the firewall. For more information about configuring a UDP connection, refer to the “Configuring Streaming or Playback using the UDP connection” section of the SCOPIA Solution Deployment Guide.

Step 8 Enter a value for the maximum number of ports you want to use for unicast streaming clients.

Figure 6-4 Port Settings Section



The screenshot shows a dialog box titled "Port Limit" with a dark header. Below the header, there is a line of text: "Limit the total number of ports used for unicast streaming clients." Underneath this text, there is a label "Port Limit" followed by a text input field containing the number "600".

Step 9 Select OK or Apply.

7

Customizing the SCOPIA Desktop User Interface

Customers can change logos and strings which contain the default RADVISION or SCOPIA Desktop branding to brand the user interface with their own logos and strings. You can change images and strings using the SCOPIA Desktop Branding application.

- [Replacing Images](#)..... page 52
- [Modifying Strings](#) page 53
- [Saving or Restoring Branding- Related Changes](#) page 54
- [Restoring Default Images and Strings](#) page 55

Replacing Images

You can replace images appearing in the SCOPIA Desktop user interface by using the Branding application on SCOPIA Desktop Server. Replacement takes affect immediately, therefore we recommend that you should not replace images on a server that is currently in service. Replacement does not affect the proper function of the SCOPIA Desktop user interface. Most web browsers store local copies of images to accelerate future views of the same image. This practice is called caching. Any browser that has previously loaded an image that you replace may display its local copy of the old image rather than your replacement image. If an image in the SCOPIA Desktop user interface does not appear to be the same as the one displayed as the currently installed image, then you must clear your browser's cache. SCOPIA Desktop Server is released with a set of default images which you can restore at any time.

Procedure

- Step 1** Select Start.
- Step 2** Choose Programs > SCOPIA Desktop > Branding Application.
The branding application starts.

Step 3 Select the **Images** tab.
The images that can be replaced are displayed together with the recommended size and a brief description of each image.

Note: If an image has a transparent background, it appears with a gray and white “checkerboard” background in the preview fields.

Step 4 From the list, choose the image you want to replace.
A brief description of the image is displayed along with the recommended image size. The Default image area shows the image that was originally distributed with the product. The Currently installed image shows the image that appears in the user interface.

Step 5 Select **Select File**, and then choose the replacement image.
A preview of the image is displayed. If you use an image that the application indicates as not properly sized, a warning appears below the image description. Using an image that does not match the original image size might result in incorrect image display.

Step 6 If you use an image that is not properly sized, verify that the image is displayed correctly:

- Verify that the SCOPIA Desktop Server is running.
- Review the SCOPIA Desktop user interface after replacement in order to verify that the image appears correctly.

Step 7 Select **Install Image** to use the replacement image. This image is replaced.

Note: If an old image still appears, see your browser's documentation for information about removing temporary internet files.

Step 8 To restore a default image, select **Restore Original Image**.

Step 9 Repeat [Step 4](#) through [Step 7](#) for other images.

Modifying Strings

You can modify some strings appearing in the SCOPIA Desktop user interface. New string values you set using the Branding application appear in the user interface only after SCOPIA Desktop Server starts and reads these values. Therefore, you can see modified strings only after the changes are applied and after the server is restarted if it was running when you made the changes.

Procedure

Step 1 Select **Start**.

Step 2 Choose **Programs > SCOPIA Desktop > Branding Application**.

- Step 3** Select the **Strings** tab.
The strings that can be replaced are displayed along with their values:
- The **Rebranded Value** column displays values that are currently saved. When the SCOPIA Desktop Server is restarted, these are the values that appear in the user interface.
 - The **Default Value** column displays values that are the original strings that were distributed with SCOPIA Desktop.
- Step 4** Select the relevant cell in the **New Value** column and type in the new string you want to use.
Or
Double-click a value in the **Rebranded Value** column or the **Default** column to copy it into the **New Value** column.
- Step 5** Repeat [Step 4](#) for other strings if necessary.
- Step 6** Select **Apply**.
The new values are saved. The modified values appear in the **Rebranded Value** column.
- Step 7** Restart the “SCOPIA Desktop - Apache Tomcat” service for the changes to take effect.
- Step 8** To restore default strings:
- a. Select **Restore All Default Strings**.
 - b. Select **Apply**.
 - c. Restart the “SCOPIA Desktop - Apache Tomcat” service for the changes to take effect.

Saving or Restoring Branding- Related Changes

You can save modified images and strings by exporting them to a file. You can later use this file to import values from it, thus restoring them.

Procedure

- Step 1** Select **Start**.
- Step 2** Choose **Programs > SCOPIA Desktop > Branding Application**.
- Step 3** To save modified images and strings:
- a. From the **File** menu, choose **Export**.
 - b. Specify the location in which you want to save the file.
 - c. Select **Save**.
- Step 4** To restore the modified images and strings from the file:
- a. From the **File** menu, choose **Import**.
 - b. Navigate to the export file.
 - c. Select **Import**.
- Step 5** Restart the “SCOPIA Desktop - Apache Tomcat” service for the changes to take effect.

Restoring Default Images and Strings

SCOPIA Desktop Server is released with a set of default images and string values. You can restore both default images and default string values at once. Restoring default images and strings overwrites currently used images and string values with the default settings.

Procedure

- Step 1** Select **Start**.
- Step 2** Choose Programs > SCOPIA Desktop > Branding Application.
- Step 3** From the File menu, choose **Restore all**.
- Step 4** Restart the “SCOPIA Desktop - Apache Tomcat” service for the changes to take affect.

8

Configuring SCOPIA Desktop Servers for Scalability and High Availability

- [Scalability with Round Robin DNS](#) page 56
- [Scalability with Generic Load Balancer](#) page 58
- [Scalability with Radware WSD](#) page 65

Scalability with Round Robin DNS

SCOPIA Desktop Servers can be configured for scalability and high availability by placing several of them in a Tomcat cluster and using a Round Robin DNS on the DNS server to route requests to the different servers within the cluster.

- [Round Robin DNS Functionality](#) page 56
- [Round Robin DNS Limitations](#) page 58

Round Robin DNS Functionality

In a deployment with Round Robin DNS, a single DNS name resolves to multiple IP addresses defined by the network administrator. Each request is resolved to one of the SCOPIA Desktop Servers in the cluster.

Usually the same SCOPIA Desktop Servers in the cluster would have different IP addresses depending on whether they are contacted by a user outside the network compared to inside the network. Users always enter the same DNS name, like SD.company.com, but depending on the location of the user, that DNS name resolves to a different list of IP addresses.

For each client request, the DNS name is resolved to one of the defined IP addresses.

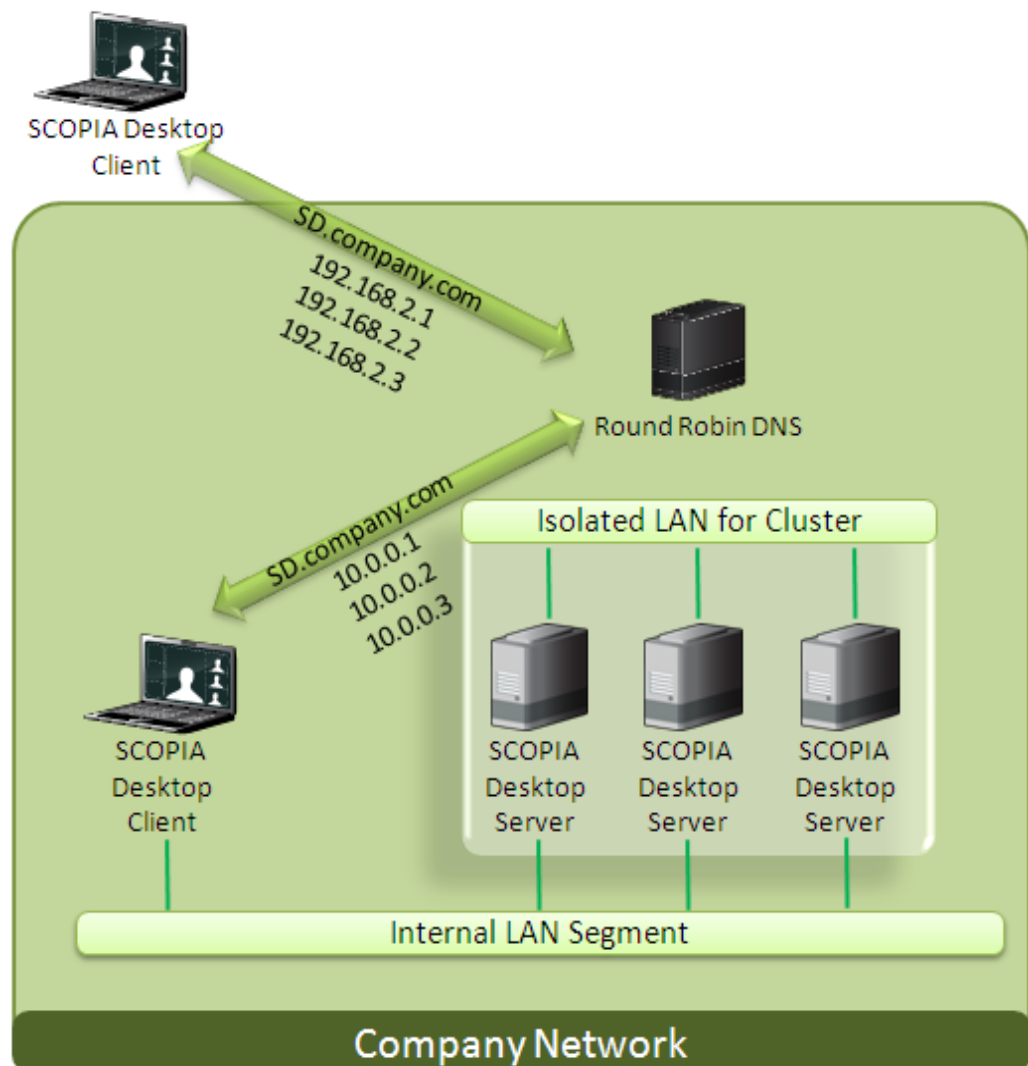
When the client PC's browser resolves the DNS name, it caches the list of IPs in the order they were returned by the Round Robin DNS. If connection to the first one fails, it will try the next in the list. Unless the DNS cache on the client is flushed, the browser uses the same IP address list for subsequent requests, unless a connection fails, then it will try the next in the list as before.

Servers in the cluster are recommended to have two network cards, one to connect to an isolated network behind the load balancer and a second card to connect to the company network.

The integrity of authenticated HTTP sessions is maintained when requests are routed to different servers, enabling rerouting to different SCOPIA Desktop Servers within the cluster without requiring another login.

Figure 8-1 on page 57 demonstrates how a single address can be resolved to different IP addresses depending on whether the client request came from inside or outside the company network. Each SCOPIA Desktop Server has two IP addresses, one for each NIC, where the internal address for one of the servers would be 10.0.0.1 while its external IP would be 192.168.2.1.

Figure 8-1 Round Robin DNS sends a list of IP addresses to a client. The client tries each one in turn to access a SCOPIA Desktop Server.



Round Robin DNS Limitations

Users in the same meeting could be routed to different SCOPIA Desktop Servers. This can be costly, as each SCOPIA Desktop Server occupies an extra port, thereby increasing the number of servers per meeting, reducing the efficiency of port usage.

Spreading meeting participants over more than one server also implies that participants on other servers lose chat and raising hand functionality.

There is no guarantee that the load is distributed evenly when using Round Robin DNS.

Scalability with Generic Load Balancer

SCOPIA Desktop Servers in a Tomcat cluster can also be managed using a generic load balancer. This topology has the added advantage of continued service even when one or more of the servers have failed.

- [Generic Load Balancer Functionality](#) page 58
- [How to Configure Round Robin DNS and Generic Load Balancers](#) page 59
- [Generic Load Balancer Limitations](#) page 65

Generic Load Balancer Functionality

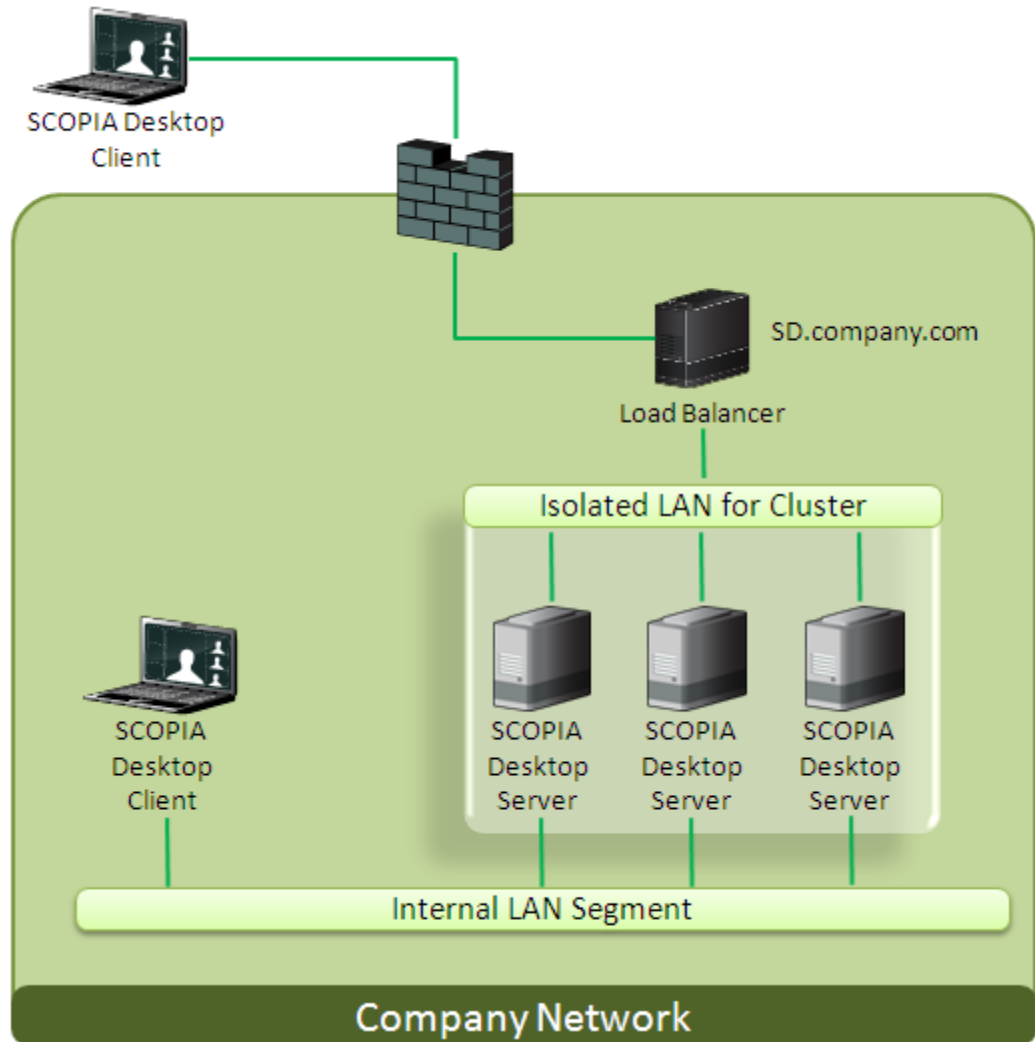
Generic load balancers offer the continued service of a cluster when one or more of the units are unresponsive, due to the health checks that take place in the background. If one or more of the servers are not able to respond, the load balancer reroutes requests to the remaining active servers.

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

External clients access the IP address of the cluster, like SD.company.com, which points directly to the load balancer via the firewall. The load balancer resolves the request to one of the servers in the cluster (as opposed to offering several IPs and leaving it to the client browser to cycle through them).

Internal clients type the same address, SD.company.com, which is also resolved directly to the load balancer, this time with its internal address.

Figure 8-2 Ensuring high availability of SCOPIA Desktop Servers using a load balancer to resolve the IP address



The firewall must be configured with a static IP mapping.

Note: Scalability cannot be currently extended to streaming servers.

How to Configure Round Robin DNS and Generic Load Balancers

A Tomcat cluster enables users to access the SCOPIA Desktop Servers using a single DNS name, for example `sdcluster.x.com`, routing to several servers each with their own IP address.

- [Configuring DNS Settings for Round Robin DNS](#) page 60
- [Configuring DNS Settings for Generic Load Balancers](#) page 60
- [Configuring the Tomcat Cluster](#) page 60
- [Configuring SCOPIA Desktop in a Cluster](#) page 61

- [Configuring Multiple NIC Servers.....](#) page 63
- [Configuring Streaming and Recording for Scalability.....](#) page 64
- [Configuring Load Balancer Routing Rules.....](#) page 64

Configuring DNS Settings for Round Robin DNS

Procedure

- Step 1** Define a single DNS name for the multiple IP addresses in the cluster.
- Step 2** Define a DNS name for each of the servers in the cluster, each associated with that server’s IP address.

Note: This DNS name must be available from all locations that might request access to the SCOPIA Desktop Servers.

Configuring DNS Settings for Generic Load Balancers

Procedure

- Step 1** Define a single DNS name for the a single IP address that represents the cluster.
- Step 2** Define a DNS name for each of the servers in the cluster, each associated with that server’s IP address.

Note: This DNS name must be available from all locations that might request access to the SCOPIA Desktop Servers.

Configuring the Tomcat Cluster

This procedure configures the Tomcat cluster as a simple TCP cluster with full memory replication of sessions. On each of the servers in the cluster, perform the following steps.

Procedure

- Step 1** Open the file server.xml on each SCOPIA Desktop Server located at c:\Program Files\Radvision\SCOPIA Desktop\tomcat\conf.
- Step 2** Locate the line

```
<Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster" channelSendOptions="8">
```

Step 3 Replace that line with the following code:

```
<Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"
channelSendOptions="8"><Manager
className="org.apache.catalina.ha.session.DeltaManager"expireSessionsOn
Shutdown="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.PooledParallelSende
r"/></Sender><Interceptor
className="org.apache.catalina.tribes.group.interceptors.TcpFailureDete
ctor"/><Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDispatc
h15Interceptor"/></Channel><Valve
className="org.apache.catalina.ha.tcp.ReplicationValve"filter=""/><Valv
e
className="org.apache.catalina.ha.session.JvmRouteBinderValve"/><Deploy
er
className="org.apache.catalina.ha.deploy.FarmWarDeployer"tempDir="/tmp/
war-temp/"deployDir="/tmp/war-deploy/"watchDir="/tmp/war-listen/"watchE
nabled="false"/><ClusterListener
className="org.apache.catalina.ha.session.JvmRouteSessionIDBinderListen
er"/><ClusterListener
className="org.apache.catalina.ha.session.ClusterSessionListener"/></Cl
uster>
```

Step 4 Open the file web.xml in \tomcat\webapps\scopia\WEB-INF\.

Step 5 Add a line and enter <distributed/>.

Step 6 Save and close the file.

Step 7 Open the file context.xml in \tomcat\conf\.

Step 8 Locate the line containing <Manager pathname="" />.

Step 9 Delete this line.

Step 10 Save and close the file.

Step 11 Restart the server.

Configuring SCOPIA Desktop in a Cluster

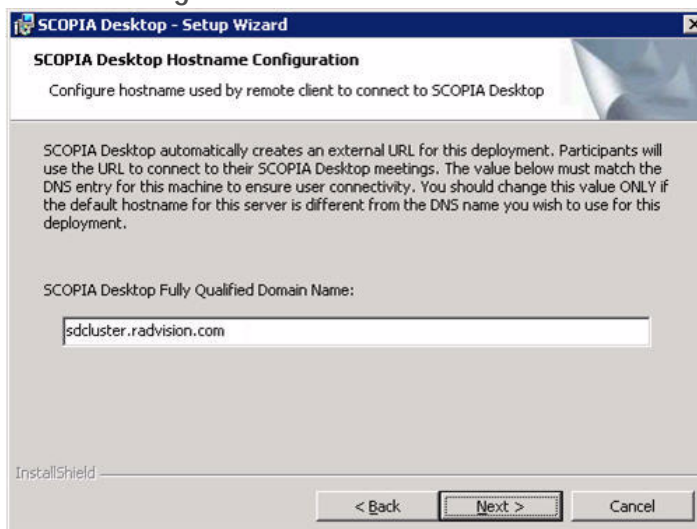
Procedure

Step 1 Enter the same DNS name for each of the servers in the cluster during installation.

a. Run the installation of the SCOPIA Desktop Server.

- b. Enter the DNS name in the SCOPIA Desktop Fully Qualified Domain Name field in the SCOPIA Desktop Hostname Configuration window, as in [Figure 8-3](#) on page 62.

Figure 8-3 Defining the DNS Name of a SCOPIA Desktop Server

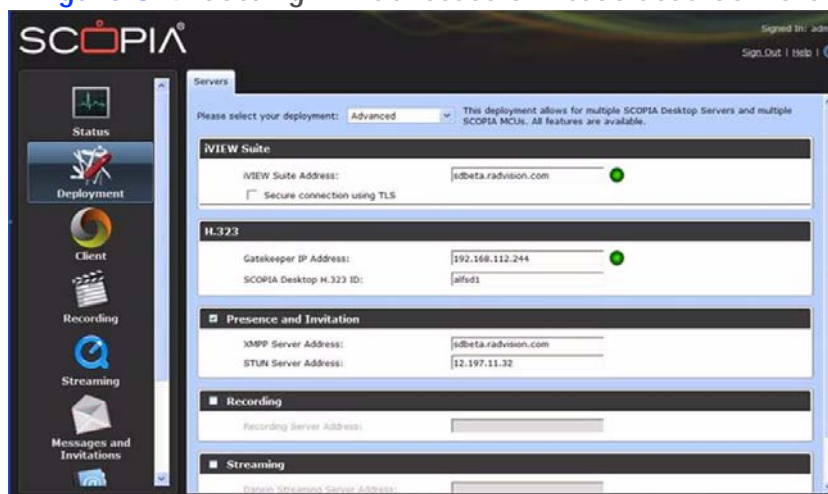


Step 2

Define the same IP address in the iVIEW Management Suite Address field for each of the servers in the cluster.

- a. Open the SCOPIA Desktop Server Administration Web User Interface.
- b. Select the Deployment section ([Figure 8-4](#) on page 62).

Figure 8-4 Setting IP Addresses of Associated Servers



- c. Enter the IP address in the iVIEW Management Suite Address field, identical to the other servers in the cluster.
- d. Ensure the Recording and Streaming sections are disabled.
- e. Repeat for each of the servers in the cluster.

Step 3

Repeat [Step 2](#) for the Gatekeeper IP Address field.

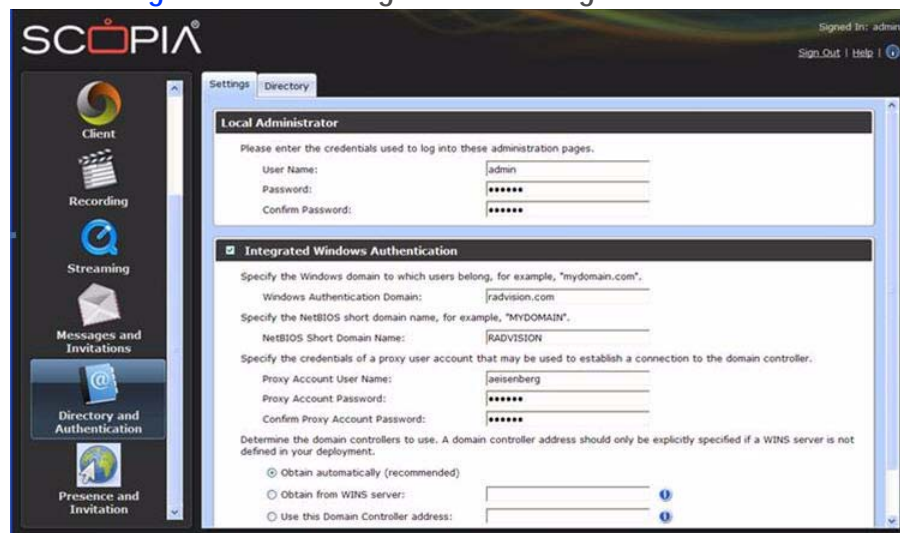
Step 4 Repeat [Step 2](#) for the XMPP Server Address field.

Note: Do not configure the Recording and Streaming sections of this window in this deployment.

Step 5 Enter the same usernames and passwords on all SCOPIA Desktop Servers in the cluster to integrate Windows authentication.

- Open the SCOPIA Desktop Server Administration Web User Interface.
- Select the **Directory and Authentication** section ([Figure 8-5](#)).
- Enter the Windows login information.

Figure 8-5 Setting Windows Login Credentials



Step 6 Configure point-to-point calls to use a specific SCOPIA Desktop Server address, not the generic address of the cluster.

- Open the SCOPIA Desktop Server Administration Web User Interface.
- Select the **Presence and Invitation** section ([Figure 8-5](#)).
- Select the check box **Use a different SCOPIA Desktop Server to host point to point calls**.
- Specify the address of the SCOPIA Desktop Server to host point-to-point calls.

Configuring Multiple NIC Servers

Procedure

Step 1 Open server.xml on each SCOPIA Desktop Server located at c:\Program Files\Radvision\SCOPIA Desktop\tomcat\conf.

Step 2 Locate the line

```
<Membership  
className="org.apache.catalina.tribes.membership.McastService
```

Step 3

"
Use the bind attribute to define the IP interface to restrict cluster membership multicast messages. For example:

```
<Membership  
className="org.apache.catalina.tribes.membership.McastService  
"address="228.0.0.4"port="45564"frequency="500"dropTime="3000  
"bind="10.0.0.2"/>
```

Configuring Streaming and Recording for Scalability

Currently there is no solution for recording when the SCOPIA Desktop Server is configured for scalability. Therefore recording functionality must be disabled on each SCOPIA Desktop Server used for interactive users (Figure 8-4 on page 62).

To support streaming functionality in the cluster, you can install dedicated SCOPIA Desktop Servers as streaming servers, and enable streaming as a policy on all scheduled meetings and Virtual rooms. The maximum number of streaming servers is the number of SCOPIA Desktop Servers deployed for interactive users.

To configure a dedicated streaming server, you can either point all interactive SCOPIA Desktop Servers to the same alternate streaming server, or assign one streaming server to each interactive SCOPIA Desktop Server as the alternate streaming server.

Procedure

- Step 1** Open the SCOPIA Desktop Server Administration Web User Interface.
- Step 2** Select the **Deployment** section (Figure 8-4 on page 62).
- Step 3** Select the **Streaming** check box.
- Step 4** Select the check box **Allow watching of webcasts from an alternate SCOPIA Desktop Server**
- Step 5** Enter the IP address of the dedicated streaming server.
- Step 6** Configure the SCOPIA iVIEW Management Suite to enable streaming for virtual rooms and scheduled meetings (see the *User Guide for SCOPIA iVIEW Management Suite for further details*).

Configuring Load Balancer Routing Rules

Procedure

- Step 1** Set the persistence based on JSESSIONID in HTTP header, otherwise on source IP.
- Step 2** Select sever based on least amount of traffic or fastest response time. This will insure that all servers are as evenly loaded as possible.

Generic Load Balancer Limitations

Users in the same meeting could be routed to different SCOPIA Desktop Servers. This can be costly, as each SCOPIA Desktop Server occupies an extra port, thereby increasing the number of servers per meeting, reducing the efficiency of port usage.

Spreading meeting participants over more than one server also implies that participants on other servers lose chat and raising hand functionality.

Scalability with Radware WSD

SCOPIA Desktop Servers can also be made scalable using Radware WSD. This configuration does not use Tomcat clustering. Configure each SCOPIA Desktop Server independently.

- [Radware WSD Functionality](#) page 65
- [How to Configure Radware WSD](#) page 65
- [Radware WSD Limitations](#)..... page 70

Radware WSD Functionality

Radware WSD's application, the App Director, can be configured to track the meeting ID, enabling it to route users in the same meeting to a single SCOPIA Desktop Server. The WSD routes one meeting to one server, and when one is full, it reroutes other meetings to one of the remaining servers.

When a request arrives to the main virtual IP address, the App Director inspects the cookie embedded within the URL to determine if this request is part of an existing session with its server location. If it is, the App Director redirects the HTTP request to that server.

When a new session is requested, the App Director can be configured to route requests to the server with the least amount of traffic.

The WSD does not require the use of an extra port for each meeting, since there is always only one server per meeting.

How to Configure Radware WSD

- [Configuring Network Interfaces in WSD](#) page 66
- [Configuring Routing in WSD](#)..... page 66
- [Configuring the Central Server Farm](#)..... page 67
- [Configuring Remaining Servers in the Farm](#)..... page 67
- [Configuring Layer 4 Policies](#) page 68
- [Configuring Servers of the Central Server Farm](#)..... page 68
- [Configuring a Single Server Farm Server](#) page 69
- [Configuring Cookie Persistency](#) page 70

Configuring Network Interfaces in WSD

Procedure

- Step 1** Open the App Director.
- Step 2** Select **Router**.
- Step 3** Select **IP Router**.
- Step 4** Select **Interface Parameters**.
- Step 5** Configure the IP interfaces for the device. One interface is the IP address to access the load balancer from outside and inside the network. The other interface is the load balancer's IP address on the isolated network of the SCOPIA Desktop Server farm.

Configuring Routing in WSD

Procedure

- Step 1** Open the App Director.
- Step 2** Select **Router**.
- Step 3** Select **Routing Table**.
- Step 4** Configure the routing table so that traffic that is destined for the SCOPIA Desktop Servers is routed through one interface, while all other traffic is routed through the other interface.

Note: Routes can only be defined when the interface is accessible.

Configuring the Central Server Farm

Procedure

- Step 1** Open the App Director.
- Step 2** Select Farms.
- Step 3** Select Farm Table.
- Step 4** Select Create.
- Step 5** Enter the central server farm name in the Farm Name field, for example Central_Server_Farm.
- Step 6** Enter 90000 in the Aging Time field.
- Step 7** Select Least Amount of Traffic in the Dispatch Method field.
- Step 8** Select Server Per Session in the Session Mode field.
- Step 9** Select TCP Port in the Connectivity Check Method field.
- Step 10** Select HTTP Redirection in the Redirection Mode field.
- Step 11** Select IP Mode in the HTTP Redirection Mode field.
- Step 12** Use the default values for the remaining fields.
- Step 13** Select Set.

Configuring Remaining Servers in the Farm

Perform the following procedure on each of the remaining servers in the farm.

Procedure

- Step 1** Open the App Director.
- Step 2** Select Farms.
- Step 3** Select Farm Table.
- Step 4** Select Create.
- Step 5** Enter the name of this server in the farm in the Farm Name field.
- Step 6** Enter 60 in the Aging Time field.
- Step 7** Select Least Amount of Traffic in the Dispatch Method field.
- Step 8** Select Server Per Session in the Session Mode field.
- Step 9** Select TCP Port in the Connectivity Check Method field.
- Step 10** Use the default values for the remaining fields.
- Step 11** Select Set.

Configuring Layer 4 Policies

Procedure

- Step 1** Open the App Director.
- Step 2** Select **Servers**.
- Step 3** Select **Layer 4 Farm Selection**.
- Step 4** Select **Layer 4 Policy Table**.
- Step 5** Select **Create**.
- Step 6** Enter the IP address of the central server farm in the **Virtual IP** field.
- Step 7** Select **Any** in the **L4 Protocol** field.
- Step 8** Enter a policy name in the **L4 Policy Name** field. For example, `Main_Policy`.
- Step 9** Enter the name of the central server farm in the **Farm Name** field. For example, `Central_Server_Farm`.
- Step 10** Use the default values for the remaining fields.
- Step 11** Select **Set**.

Configuring Servers of the Central Server Farm

Procedure

- Step 1** Open the App Director.
- Step 2** Select **File > Configuration > Receive From Device**.
- Step 3** Select **ASCII** as the file format
- Step 4** Select **Set**.

- Step 5** Search for the name of each farm and note its IP address.
For example, `rsWSDFarmName.0.0.0.2="S1_Farm"` denotes S1_Farm's IP address is 0.0.0.2
- Step 6** Open the App Director.
- Step 7** Select **Servers**.
- Step 8** Select **Application Servers**.
- Step 9** Select **Table**.
- Step 10** Select **Create**.
- Step 11** Enter the name of the central server farm in the **Farm Name** field. For example, `Central_Server_Farm`.
- Step 12** Enter the IP address of the server in the farm in the **Server Address** field (see [Step 5](#)).
- Step 13** Enter a name for this server in the **Server Name** field. For example, `S1-Redir_To_S1_Farm`.
- Step 14** Select **Local Farm** in the **Type** field.
- Step 15** Enter the IP address of the server's L4 policy in the **Redirect To** field.
- Step 16** Use the default values for the remaining fields.
- Step 17** Select **Set**.

Configuring a Single Server Farm Server

Procedure

- Step 1** Open the App Director.
- Step 2** Select **Servers**.
- Step 3** Select **Application Servers**.
- Step 4** Select **Table**.
- Step 5** Select **Create**.
- Step 6** Enter the name of the single server farm in the **Farm Name** field. For example, `S1_Farm`.
- Step 7** Enter the IP address of the server in the **Server Address** field.
- Step 8** Enter the name of the server in the **Server Name** field. For example, `S1`.
- Step 9** Use the default values for the remaining fields.
- Step 10** Select **Set**.

Note: You may configure an additional server as a backup server for a farm in case of server failure. On the backup server, select **Backup** in the **Operation Mode** field.

Procedure

- Step 1** Open the App Director.
- Step 2** Select **Layer 7 Server Persistency**.
- Step 3** Select **Text Match**.
- Step 4** Select **Create**.
- Step 5** Enter the name of the farm in the **Farm Name** field. For example, `Central_Server_Farm`.
- Step 6** Select **URL Cookie** in the **Lookup Mode** field.
- Step 7** Enter `CONFID` in the **Persistency Identifier** field.
- Step 8** Enter `&` in the **Stop Chars** field.
- Step 9** Enter `90000` in the **Select Enabled** in the **Inactivity Timeout [sec]** field.
- Step 10** Select **Enabled** in the **Inactivity Timeout [sec]** field.
- Step 11** Use the default values for the remaining fields.
- Step 12** Select **Set**.

Radware WSD Limitations

A redirected request does not maintain session authentication, since reroutes use specific IP addresses. This requires users to re-enter credentials when their requests are rerouted.

9

Securing Your SCOPIA Desktop Deployment

This section provides optional procedures for enhancing the security of your SCOPIA Desktop deployment. For example, you can configure secure access of SCOPIA Desktop clients to SCOPIA Desktop Servers or enable encryption for communication across the conferencing network. The topic in this section included:

- [Enabling SCOPIA Desktop Server to Use HTTPS](#) page 71
- [Configuring SCOPIA Desktop Server with a Certificate](#)..... page 72
- [Configuring SCOPIA Desktop Clients to Accept Certificates](#)..... page 73
- [Enabling Encryption](#) page 74

Enabling SCOPIA Desktop Server to Use HTTPS

It is not possible to configure SCOPIA Desktop web access to accept an SSL connection on the standard 443 port because that port is already used to accept tunnelled connections from SCOPIA Desktop Client. This procedure explains how to configure SCOPIA Desktop Server to forward HTTPS requests to its web server.

Procedure

- Step 1** Select **Start > All Programs > SCOPIA Desktop > Config Tool**.
- Step 2** Select the **Enable HTTPS** checkbox in the HTTPS tab.
- Step 3** Select **Apply**.
- Step 4** Update the start menu shortcut used to access the SCOPIA Desktop Administration web interface:
 - Select **Start > All Programs > SCOPIA Desktop**.
 - Right-click **SCOPIA Desktop - Administration** shortcut.
 - Select **Properties**.
 - Modify the value in the Target field from
`C:\WINDOWS\explorer.exe https://localhost:80/scopia/admin`
to
`C:\WINDOWS\explorer.exe http://your_IP/scopia/admin`

e. Select OK.

Step 5 Select **Add Certificate** to use an existing certificate, and follow the steps described in [Configuring SCOPIA Desktop Server with a Certificate page 72](#).

Step 6 Select **Restart Services**.

Step 7 Change URL in Invitations section of the SCOPIA Desktop Administration web interface:

- 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, modify all URLs to use https instead of http.

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

Configuring SCOPIA Desktop Server with a Certificate

SCOPIA Desktop Server forwards all HTTPS requests to a Tomcat Server. In order to configure SCOPIA Desktop with a certificate for HTTPS, import the certificate acquired from a Certificate Authority to SCOPIA Desktop Server.

Procedure

Step 1 Stop the service "SCOPIA Desktop- Conference Server. x.x.x".

Step 2 Navigate to this location:

`<SDINSTALLDIR>\Confsvr`

where <SDINSTALLDIR> is the default installation directory.

Step 3 Run the Certificate Configuration Utility by double-clicking *CertificateConfiguration.exe* file.

Step 4 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.

Step 5 If the certificate is in PKCS12 format:

- a. Select **Configure Certificate via File Name**.
- b. Browse to the PKCS12 certificate.

- c. Enter the private key password for the certificate.
- Step 6** Select **OK**.
- Step 7** Verify that the certificate information is listed in the Selected Certificate pane.
- Step 8** Select **Apply**.
- Step 9** Select **OK**.
- Step 10** Select **OK**.
- Step 11** Start the service "SCOPIA Desktop- Conference Server.x.x.x".

Configuring SCOPIA Desktop Clients to Accept Certificates

Perform this configuration procedure to install the SCOPIA Desktop Server Certificate on a SCOPIA Desktop client. If you try to connect to the server and the certificate is not installed on the client computer, the client issues a -734 error. View this error in the client call log:
 "#####get_verify_result error = 19, the peer certificate is invalid."

In cases of incorrect SCOPIA Desktop Server Certificate setting, the SCOPIA Desktop Client returns errors 21 or 26.

Procedure

- Step 1** Obtain a certificate from the administrator. If you are using a known Windows CA server, a CA certificate can be obtained as follows:
 - a. Connect to the Certificate Authority Server at this address: *http://<serverName>/certsrv*.
 - b. On the Welcome Page, select Download a CA certificate, certificate chain, or CRL.
 - c. Select Download CA certificate chain and save it to your hard disk.
- Step 2** Install the certificate on the computer using Microsoft Management Console:
 - a. Select **Start > Run**.
 - b. Type mmc and press enter.
 - c. From the File menu, select **Add/Remove Snap-in**.
 - d. Select **Add**.
 - e. Select Certificates, and then select **Add**.
 - f. Select **Computer Account** in the Certificates snap-in dialog box, and then select **Next**.
 - g. Select Local computer:(the computer this console is running on), and then select **Finish**.
 - h. Select **Close** and **OK**.
 - i. Verify that Microsoft Management Console shows the Certificates (Local Computer) certificate store.
 - j. Expand certificates by selecting **Certificates > Trusted Root Certification Authorities > Certificates**.
 - k. Right-click Certificates and select **All Tasks > Import**, and then select **Next**.

- I. Select **Browse**, and select **Certificate**.

By default it only shows X.509 Certificate file types, you must change this to Personal Information Exchange (*.pfx;*.p12) or All Files (*.*.), and select **Next**.

- m. Select **Place all certificates in the following store**, and then verify that the Certificate store: Trusted Root Certification Authorities option is selected.
- n. Select **Next**.
- o. Verify the information and select **Finish**.
- p. Verify that the Certificate Chain is located in the Trust Root Certification Authorities store.

Step 3

Verify that the SCOPIA Desktop Client can connect to the SCOPIA Desktop Server.

Enabling Encryption

Besides securing communication, enabling encryption guarantees data integrity which is tested as a part of the transport level message integrity check.

Note:

Encryption functionality is only available for deployments using iVIEW Suite.

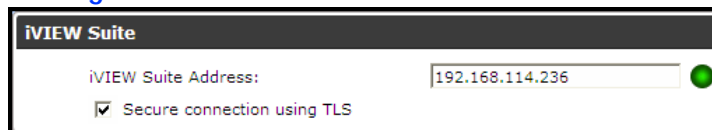
Procedure

Step 1

Enable encryption on the SCOPIA Desktop Server:

- a. Access the SCOPIA Desktop Administrator web user interface.
- b. Select the **Deployment** icon on the sidebar.
- c. Select the **Secure connection using TLS** check box in the iVIEW Management Suite section.

Figure 9-1 Secure Connection Check Box



- d. Select **OK**.

10

Troubleshooting Common Issues

Each of the following sections presents the symptoms of common problems that may occur during the use of the SCOPIA Desktop. Recommended actions for each symptom are also provided. For more information related to know issues, see the SCOPIA Desktop Version 7.5 Release Notes.

- [Viewing Status of Servers and Directory](#) page 75
- [Recording Does Not Start Automatically](#) page 81
- [Synchronizing SCOPIA Desktop Server with iVIEW Management Suite](#) page 82
- [Updating the IP Address on the Recording or Streaming Server](#) page 82
- [Changing IP Address of the SCOPIA Desktop Server](#) page 83
- [Enabling a User to Sign In](#) page 84

Viewing Status of Servers and Directory

Viewing the status of your SCOPIA Desktop deployment is a helpful way to assess resource availability and troubleshoot connectivity problems. The following sections provide useful information for utilizing the View Status functionality of SCOPIA Desktop.

- [Viewing Server Status and Port Resource Usage](#) page 75
- [Viewing Directory Status](#) page 78
- [Viewing Recording Server Status](#) page 79
- [Viewing Content Slider Status](#) page 81

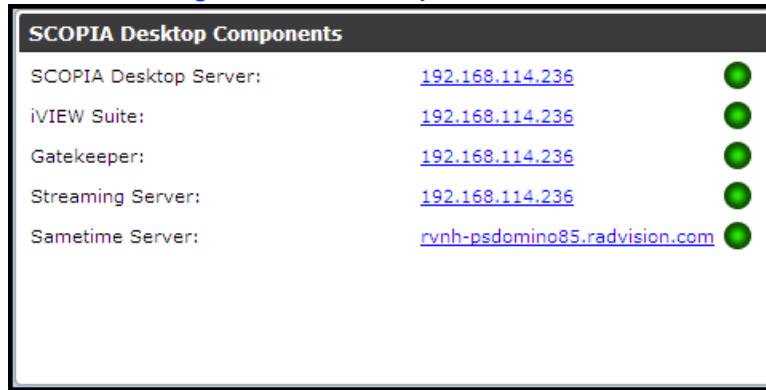
Viewing Server Status and Port Resource Usage

The SCOPIA Desktop Status tab displays status information about the SCOPIA Desktop Server and other servers with which it interacts:

- Gatekeeper—RADVISION ECS Server.
- Streaming—SCOPIA Desktop Server. This information appears only if the SCOPIA Desktop Server is configured to manage streaming.
- SCOPIA MCU—MCU. This information is displayed only for basic deployments.

- iVIEW Management Suite—iVIEW Management Suite. This information is displayed only for point-to-point and advanced deployments.
- Sametime Server—Sametime Community Server. This information appears if the SCOPIA Desktop Server is configured to work with IBM Lotus Sametime Web.

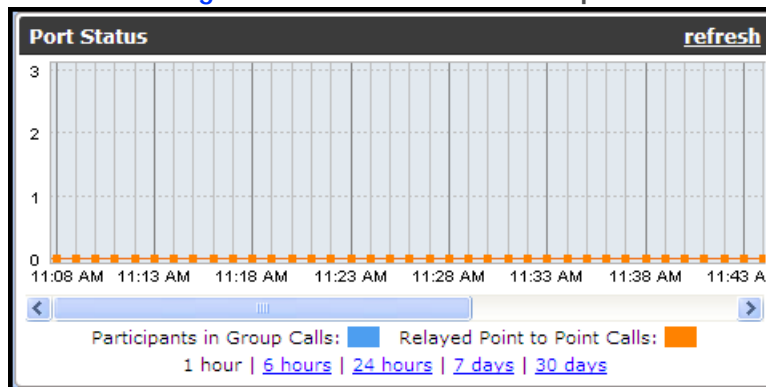
Figure 10-1 Component Status



The indicator next to each link shows whether or not the connection to the target server or registration with the Gatekeeper is successful. When the indicator is red, a tooltip containing error details is available. Click the red indicator to view further error information.

The SCOPIA Desktop Status tab also shows port usage statistics and presents port usage graphically.

Figure 10-2 Port Status Graph



Depending on your needs you may choose one of the graph reports described in [Table 10-1](#).

Note:

We recommend that you wait five minutes after you run the SCOPIA Desktop Server before you refresh the SCOPIA Desktop Status tab to acquire the updated port information.

Table 10-1 Graph Views Content

Graph Report	Data Collection Frequency	Number of Data Points Collected	Source
one hour	one minute	60	SCOPIA Desktop
6 hours	four minutes	90	Four data points from one hour report
24 hours	20 minutes	72	Five data points from 6 hour report
7 days	120 minutes	84	Six data points from 24 hour report
30 days	12 hours	60	Six data points from 7 day report

Depending on the deployment the SCOPIA Desktop Status tab also displays additional statistics:

- For deployment without iVIEW Management Suite
 - Number of participants in group calls
 - Number of streaming ports
- For deployments with enabled point-to-point-only functionality
 - Number of relayed point-to-point calls
- For advanced deployments
 - Number of total live ports
 - Number of relayed point-to-point calls
 - Number of participants in group calls
 - Number of streaming ports

Total Live Ports	
In Use 0	Allowed 250
Relayed Point to Point Calls	
Connected 0	Allowed 250
Participants in Group Calls	
Connected 0	Licensed 200
Streaming Ports	
In Use 0	Allowed 600

Sometimes point-to-point and group calls may exceed the allowed port limit because the limit is enforced at connecting time. If this happens, number of connected ports appears in red and the “Usage has exceeded the maximum allocated resources” warning is displayed.

If you set the call limit to a number lower than defined by the license, an error message is displayed next to the number of participants in group calls.


Viewing Directory Status

In deployments where SCOPIA Desktop is configured to work with iVIEW Management Suite, SCOPIA Desktop Server must synchronize with iVIEW Management Suite to download information about users, virtual rooms, and global policy. SCOPIA Desktop Server synchronizes with iVIEW Management Suite when it connects to it for the first time; then iVIEW Management Suite updates SCOPIA Desktop Server each time there is new or modified information. There are the following synchronization states:

- Synchronized—SCOPIA Desktop Server is synchronized with iVIEW Management Suite
- Synchronizing—SCOPIA Desktop Server is caching information from iVIEW Management Suite. Users cannot search for users and terminals in the contact list or in the Invite dialog box.
- Not Synchronized—SCOPIA Desktop Server functions using locally cached information. The SCOPIA Desktop functionality is not influenced except one feature: standard login is not available. In deployments where the Integrated Windows Authentication is enabled, users can still log in using Single Sign-On.
- Synchronization error—SCOPIA Desktop Server is not synchronized with iVIEW Management Suite, no information is cached. The SCOPIA Desktop functionality is reduced.

Select **Status > Directory Status** to display directory information.

Figure 10-3 Directory Status

Global Directory - iVIEW Suite	
Synchronization:	Synchronized 
Authentication:	Enabled
Guest Access to Meetings:	Enabled
Guest Access to Webcasts:	Enabled
Guest Access to Recordings:	Enabled

You can also view authentication settings and maximum call rate value configured at iVIEW Management Suite.

Figure 10-4 Maximum Call Rate Policy

Global User Policy
Maximum Call Rate (Kb/s):
1024




Viewing Recording Server Status

You can view the Recording Server Status information only if recording is enabled in your deployment.

The Recording Status tab displays this information:

- Recording Components:

Figure 10-5 Recording Components Status

Recording Components	
Recording Server:	192.168.114.236 
Recorder:	192.168.114.236 
Gatekeeper:	192.168.114.236 
NIC Address:	192.168.114.236

- Recording Server—Displays the address of the SCOPIA Desktop Recording Server.
- Recorder—Displays the connection status between the SCOPIA Desktop Recording Server and the SCOPIA Desktop Conference Server.
- Gatekeeper—Displays the address of the gatekeeper to which the Conference Server is registered. In the special case that the SCOPIA Desktop Recording Server is installed separately from the SCOPIA Desktop Server and has its own Conference Server, the Conference Server must be registered to the same gatekeeper as the SCOPIA Desktop Server.
- NIC Address—Displays the NIC address used by the SCOPIA Desktop Recording Server to communicate with MCU.

- Recording Server Information:

Figure 10-6 Recording Server Information

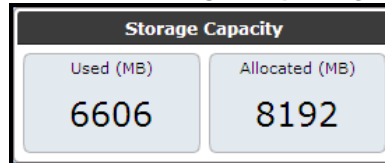


- Recordings Folder—Displays the location of the folder on the SCOPIA Desktop Recording Server used for storing recordings.
- Remaining Disk Space—Shows how much space is remaining on the disk on which recordings are stored.

If the remaining disk space is less than the disk space allocated for recordings, a warning icon is displayed. Click the icon for details.

- Storage Capacity—Shows the amount of disk space used by all recordings.

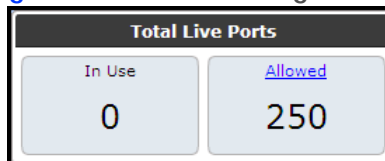
Figure 10-7 Storage Capacity Status



The maximum value is configured during installation. To change the maximum disk space, run the installer on the SCOPIA Desktop Recording Server in the modification mode.

- Recording Ports:

Figure 10-8 Port Usage Status



- In Use—Shows the number of recordings being recorded at the present moment. The maximum value appears as specified in the recording license installed for this SCOPIA Desktop.
- Licensed—Shows the number of recording ports defined by the license.

- Available Recordings:

Figure 10-9 Available Recordings Status



- Completed—Shows the total number of completed recordings available for watching.
- Reconstructed—Shows the number of reconstructed recordings.

SCOPIA Desktop saves actual recordings and recording attributes in different folders. If a user restores only a recording without restoring its attributes, the recording appears as reconstructed. In this case you need to manually define recording attributes, such as the name and the owner PIN, to finalize reconstruction of a recording. After the reconstruction is completed, the recording appears on Watch Recording page of the SCOPIA Desktop portal. If recording attributes are not reconstructed, the yellow attention icon is displayed. Click the icon for more information.

Select **Status > Recording Status** to access Recording Server information.

Viewing Content Slider Status

You can view the Content Server status information only if recording is enabled in your deployment.

The Content Slider Status tab displays this information:

Figure 10-10 Content Slider Status

Recording Servers	Sessions	Problems
107.63.132.88	660	44
190.172.196.141	0	19
21.74.179.154	0	10

Total Sessions	Total Problems
660	73

- Recording Server Status:
 - Recording Server—Displays the address of the SCOPIA Desktop Recording Server.
 - Sessions—All slider sessions currently in progress, with details on the server(s) that have sessions.

Problems—If there are problems with slider sessions, they appear (per server) in the problems column. To view details, select the link in the Problems column: Results show the date/time of the problem and a brief summary of the problem details.

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.
- 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.

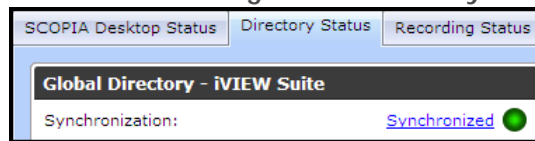
Synchronizing SCOPIA Desktop Server with iVIEW Management Suite

Problem The Directory Status - iVIEW Management Suite tab displays the 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.

Figure 10-11 iVIEW Management Suite Synchronization



Updating the IP Address on the Recording or Streaming Server

Problem The SCOPIA Desktop Status tab indicates that the Streaming or Recording 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, select **Programs > SCOPIA Desktop > ConfigTool**.
- Step 2** Select the **Content Center** tab.
- Step 3** Click the **Add** button and enter the new IP address of the SCOPIA Desktop Server.
- Step 4** Select the old IP address of SCOPIA Desktop Server, and click the **Remove** button to remove it from the list.

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-click **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**.

Upgrading SCOPIA Desktop Server Recordings

If there are recordings created using SCOPIA Desktop Server version 5.x, upgrade them by performing these steps:

Note: You can upgrade recordings at any time.

Procedure

- Step 1** Install QuickTime version 7.6.2 or higher. You can download QuickTime at <http://www.apple.com/quicktime/download/>.
- Step 2** On the SCOPIA Desktop Server, navigate to the <INSTALLDIR>\config location.
- Step 3** Double-click the recording_converter.exe file.
- Step 4** Follow the on-screen instructions. Depending of the size and amount of recordings, the upgrade may take time.
- Step 5** The recordings are converted and the log files are created in this folder.
- Step 6** Verify that the recordings are converted correctly.
- Step 7** Delete backed up recordings.

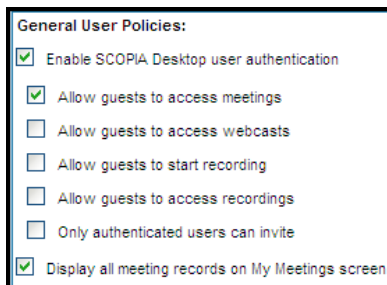
Enabling a User to Sign In

Problem A user cannot sign in.

Solution Verify that the following problems do not interfere with user signing in:

- Authentication is turned off on iVIEW Management Suite. In the SCOPIA Desktop Administrator web user interface, select **Status** in the sidebar, and then select the **Directory Status** tab. Verify that authentication is enabled.

Figure 10-12 General User Policies



- This particular user does not have a SCOPIA Desktop Pro license.
- If SCOPIA Desktop is enabled for Integrated Windows Authentication and the user does not use a valid proxy account. In the SCOPIA Desktop Administrator web user interface, select **Directory and Authentication** in the sidebar, check the proxy account configured in the Integrated Windows Authentication area.

Figure 10-13 Proxy Account Settings

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

Proxy Account User Name:	<input type="text" value="rvnh-know"/>
Proxy Account Password:	<input type="password" value="•••••"/>
Confirm Proxy Account Password:	<input type="password" value="•••••"/>

- If SCOPIA Desktop is not enabled for Integrated Windows Authentication and uses iVIEW Management Suite to authenticate, select **Status** in the sidebar and verify that SCOPIA Desktop Server is connected to iVIEW Management Suite.

Figure 10-14 SCOPIA Desktop and iVIEW Management Suite Connectivity

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



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