

RADVISION Port Security

Reference Guide

Version 7.5

SCÖPIA[®]
ELITE 5000



SCÖPIA[®]
MANAGEMENT



SCÖPIA[®]
DESKTOP

SCÖPIA[®]
VC240



SCÖPIA[®]
MOBILE



SCÖPIA[®]
XT 1000 SERIES

© 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.

Reference Guide for RADVISION Port Security Version 7.5, September 16, 2010 11:22 am

<http://www.radvision.com>

1

RADVISION Port Security Reference Guide

This document details RADVISION use of TCP/IP/UDP ports throughout the company's NBU product range.

This information in this document is organized according to product name and port number. Each port entry includes a description of the protocol used by the specific port, the role that the port serves, the direction of traffic through the port (in, out or both), and the results of blocking the port on the firewall.

The following RADVISION products are described in this document:

- [SCOPIA Elite 5200 Series MCU](#) page 4
- [Secondary Media Blade for SCOPIA Elite 5200 Series MCU](#) page 6
- [SCOPIA Elite 5100 Series MCU](#) page 6
- [SCOPIA MCU](#) page 8
- [Media Video Processor for SCOPIA MCU](#) page 10
- [Gateway](#) page 11
- [3G Gateway](#) page 13
- [MSP-324M \(Multimedia Streaming proxy\)](#) page 15
- [IVP \(Interactive Video Platform\)](#) page 16
- [MSP-IVP \(for Interactive Video Platform\)](#) page 18
- [MVP/M II SP \(Media Video Processor\)](#) page 19
- [ECS \(SCOPIA ECS Gatekeeper\)](#) page 20
- [DCS \(Data Collaboration Server\)](#) page 22
- [SCOPIA iVIEW Management Suite](#) page 23
- [iVIEW Network Manager](#) page 25
- [SCOPIA PathFinder](#) page 26
- [SCOPIA Desktop](#) page 32
- [SCOPIA XT Desktop Server](#) page 36
- [SCOPIA XT1000](#) page 37
- [SCOPIA VC240](#) page 39

RADVISION takes no responsibility for ports required by additional servers such as LDAP, SQL, Oracle or CDR servers. Always check which ports your back-end servers require and open only these ports.

SCOPIA Elite MCU

SCOPIA Elite 5200 Series MCU

Table 1-1 lists the ports supported by the SCOPIA Elite 5200 Series MCU.

Table 1-1 Ports Supported by SCOPIA Elite 5200 Series MCU

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Description
21	FTP (TCP)	Audio stream recording	Out	Cannot record audio streams	FTP Server
22	SSH (TCP)	MCU	Both	Cannot view logs in real time (logs are collected on the compact flash card)	SSH Client
80 (configurable)	HTTP (TCP)	MCU Administrator and Conference Control web user interfaces	Both	Cannot administer MCU	Web client Used for software upgrade
161	SNMP (UDP)	Configuration and status	Both	Cannot configure or check the status of the MCU via SNMP	iVIEW Network Manager, SCOPIA iVIEW Management Suite or any other SNMP manager station
162	SNMP (UDP)	SNMP Trap events	Out	Cannot receive Traps	iVIEW Network Manager, SCOPIA iVIEW Management Suite or any other SNMP manager station
443	HTTPS (TCP)	Secure web interface	Both	Cannot administer MCU	
1024-1324	H.245 (TCP)	H.245 signaling	Both	Cannot connect H.323 calls	Any H.323 entity
1719 (configurable)	RAS (UDP)	RAS signaling	Both	Cannot communicate with H.323 gatekeeper	H.323 gatekeeper
1720 (configurable)	Q.931 (TCP)	Q.931 signaling	Both	Cannot connect H.323 calls	Any H.323 entity
2900	Secondary Media Blade control (TCP)	Secondary Media Blade control protocol	Both	Can be blocked—traffic is internal to the chassis only	Secondary Media Blade
3336	XML (TCP)	MCU version 3 XML API	Both	Cannot use MCU Conference Control web user interface. Cannot use version 3 XML API to control MCU	Conference Control web client terminal, SCOPIA iVIEW Management Suite or third-party controlling applications

Table 1-1 Ports Supported by SCOPIA Elite 5200 Series MCU

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Description
3337	XML (TCP)	MCU version 3 Cascading XML API	Both	Cannot cascade between two MCUs	Other MCUs
3338	XML (TCP)	Administration XML API	Both	Cannot be blocked	
5060 (configurable)	SIP (TCP/UDP)	SIP signaling	Both	Cannot connect SIP calls	Any SIP entities
16384-16984 (configurable)	RTP/RTCP (UDP)	RTP media	Both	Cannot transmit/receive media streams	Any H.323 or SIP media enabled entity

In addition to the ports listed in [Table 1-1](#), RADVISION MCUs offer configurable security access levels enabling and disabling Telnet, FTP, SNMP and ICMP (ping) services, as shown in [Table 1-2](#).

Table 1-2 MCU Security Mode

Security Mode	Telnet	FTP	SNMP	ICMP (ping)
Standard	Active	Active	Active	Active
High	Inactive	Inactive	Active	Active
Maximum	Inactive	Inactive	Inactive	Inactive

Secondary Media Blade for SCOPIA Elite 5200 Series MCU

Table 1-3 lists the ports supported by the Secondary Media Blade of the SCOPIA Elite 5200 Series MCU.

Table 1-3 Secondary Media Blade-supported Ports (SCOPIA Elite 5200 Series MCU)

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Description
21	TCP (FTP)	Software upgrade and video stream recording	Both	Cannot record video streams. Upgrade traffic is internal to the chassis only.	FTP server
22	(TCP) SSH	MCU	Both	Cannot view logs in real time (logs are collected on the compact flash card)	SSH Client
2900	TCP (Secondary Media Blade control)	Secondary Media Blade control protocol	Both	Can be blocked—traffic is internal to the chassis only	Primary Media Blade
12000-13200 (configurable)	UDP (RTP/RTCP)	RTP/RTCP media	Both	Cannot transmit/receive media streams	Any RTP/RTCP media enabled entity

SCOPIA Elite 5100 Series MCU

Table 1-4 lists the ports supported by the SCOPIA Elite 5100 Series MCU and SCOPIA Elite 5215 MCU version 7.0 and later.

Table 1-4 Ports Supported by SCOPIA Elite 5100 Series MCU and SCOPIA Elite 5215 MCU version 7.0 and later

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Description
21	FTP (TCP)	Audio stream recording	Out	Cannot record audio streams	FTP Server
22	SSH (TCP)	MCU logs	Both	Cannot view logs in real time (logs are collected on the Compact Flash card)	SSH client
80 (configurable)	HTTP (TCP)	MCU Administrator and Conference Control web user interfaces	Both	Cannot administer MCU	Web client Used for software upgrade
161	SNMP (UDP)	Configuration and status	Both	Cannot configure or check the status of the MCU via SNMP	iVIEW Network Manager, SCOPIA iVIEW Management Suite or any other SNMP manager station

Table 1-4 Ports Supported by SCOPIA Elite 5100 Series MCU and SCOPIA Elite 5215 MCU version 7.0 and later (continued)

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Description
162	SNMP (UDP)	SNMP Trap events	Out	Cannot receive Traps	iVIEW Network Manager, SCOPIA iVIEW Management Suite or any other SNMP manager station
443	HTTPS (TCP)	Secure web interface	Both	Cannot administer MCU	
1024-1174	H.245 (TCP)	H.245 signaling	Both	Cannot connect H.323 calls	Any H.323 entity
1719 (configurable)	RAS (UDP)	RAS signaling	Both	Cannot communicate with H.323 gatekeeper	H.323 gatekeeper
1720 (configurable)	Q.931 (TCP)	Q.931 signaling	Both	Cannot connect H.323 calls	Any H.323 entity
2900	Secondary Media Blade control (TCP)	Secondary Media Blade control protocol	Both	Can be blocked—traffic is internal to the chassis only	Secondary Media Blade
3336	XML (TCP)	MCU version 3 XML API	Both	Cannot use MCU Conference Control web user interface. Cannot use version 3 XML API to control MCU	Conference Control web client terminal, SCOPIA iVIEW Management Suite or third-party controlling applications
3337	XML (TCP)	MCU version 3 Cascading XML API	Both	Cannot cascade between two MCUs	Other MCUs
3338	XML (TCP)	Administration XML API	Both	Cannot be blocked	
3339	XML (TCP)	CLI to MCU	Both	Can be blocked—traffic is internal to the chassis only	
3340	XML (TCP)	CLI to the media audio processor	Both	Can be blocked—traffic is internal to the chassis only	
3341	XML (TCP)	CLI to MVP	Both	Can be blocked—traffic is internal to the chassis only	
5060 (configurable)	SIP (TCP/UDP)	SIP signaling	Both	Cannot connect SIP calls	Any SIP entities
12000-13200 16384-16984 (configurable)	RTP/RTCP (UDP)	RTP media	Both	Cannot transmit/receive media streams	Any H.323 or SIP media enabled entity

SCOPIA MCU

SCOPIA MCU Blade

Table 1-5 lists the ports supported by the SCOPIA MCU.

Table 1-5 Ports Supported by SCOPIA MCU

Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Description
21	FTP (TCP)	Audio stream recording	Out	Cannot record audio stream	Upgrade Utility or FTP Server
23	Telnet (TCP)	MCU logs and initial configuration	Both	Cannot view logs	Telnet client
80 (configurable)	HTTP (TCP)	MCU Administrator and Conference Control web user interfaces	Both	Cannot administer MCU	Web client
161	SNMP (UDP)	Configuration and status	Both	Cannot configure or check the status of the MCU via SNMP	iVIEW Network Manager, SCOPIA iVIEW Management Suite or any other SNMP manager station
162	SNMP (UDP)	SNMP Trap events	Out	Cannot receive Traps	iVIEW Network Manager, SCOPIA iVIEW Management Suite or any other SNMP manager station
443	HTTPS (TCP)	Secure web interface	Both	Cannot administer MCU	
1024-4999	H.245 (TCP)	H.245 signaling	Both	Cannot connect H.323 calls	Any H.323 entity
1719 (configurable)	RAS (UDP)	RAS signaling	Both	Cannot communicate with H.323 gatekeeper	H.323 gatekeeper
1720 (configurable)	Q.931 (TCP)	Q.931 signaling	Both	Cannot connect H.323 calls	Any H.323 entity
1809	RPC		Both	Cannot transmit/receive audio stream	
2010	MPI (TCP)	MP control protocol	Both	Cannot use external MP	Any standalone MP units (MCUs configured to be MPs in clustering mode)
2946	MVP control (TCP)	MVP control protocol	Both	Cannot use external MVP	MVP
3333	DTI (TCP)	DCS control protocol	Both	Cannot use external DCS	DCS

Table 1-5 Ports Supported by SCOPIA MCU (continued)

Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Description
3336	XML (TCP)	MCU version 3 XML API	Both	Cannot use MCU Conference Control web user interface. Cannot use version 3 XML API to control MCU	Conference Control web client terminal, SCOPIA iVIEW Management Suite or third-party controlling applications
3337	XML (TCP)	MCU version 3 Cascading XML API	Both	Cannot cascade between two MCUs	Other MCUs
5060 (configurable)	SIP (TCP/UDP)	SIP signaling	Both	Cannot connect SIP calls	Any SIP entities
6000-6999 (configurable)	RTP/RTCP (UDP)	RTP/RTCP audio	Both	Cannot transmit/receive audio stream	Any RTP/RTCP media enabled entity
10000-11000 (configurable)	RTP/RTCP (UDP)	RTP media	Both	Cannot transmit/receive media stream	Any H.323 or SIP media enabled entity

In addition to the ports listed in [Table 1-6](#), RADVISION MCUs offer configurable security access levels enabling and disabling Telnet, FTP, SNMP and ICMP (ping) services, as shown in [Table 1-6](#).

Table 1-6 SCOPIA MCU Security Modes

Security Mode	Telnet	FTP	SNMP	ICMP (ping)
Standard	Active	Active	Active	Active
High	Inactive	Inactive	Active	Active
Maximum	Inactive	Inactive	Inactive	Inactive

Table 1-7 lists the ports supported by the MVP.

Table 1-7 MVP-supported Ports

Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Description
21	FTP (TCP)	Software upgrade and video stream recording	Both	Cannot upgrade version	Upgrade Utility
23	Telnet (TCP)	MVP online log	Both	Cannot view logs	Telnet client
161 (for future use)	SNMP (UDP)	Configuration and status	Both	Cannot configure or check the status of the MCU via SNMP	iVIEW Network Manager, SCOPIA iVIEW Management Suite or any other SNMP manager station
2946	MEGACO (TCP)	Control protocol between MCU and MVP	Both	MVP cannot connect to MCU	MEGACO (H.248) Protocol
3340	Font file client (TCP)	For receiving extended font files from the MCU.	Both	Cannot work with different fonts	Font client software
10000-10575 (configurable from version 2.5)	RTP/RTCP (UDP)	RTP/RTCP media	Both	Cannot transmit/receive media stream	Any RTP/RTCP media enabled entity

Gateway

Table 1-8 and Table 1-9 list the ports supported by the Gateway.

Table 1-8 Gateway-supported Ports—Incoming Connections

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Description
21	FTP (TCP)	File Transfer Protocol	Both	Cannot upgrade version or extract recordings	Upgrade Utility
23	Telnet (TCP)	Log	Both	Cannot view logs	Telnet client
80 (configurable via SNMP)	HTTP (TCP)	Web interface	Both	Cannot view Gateway web user interface	Web client
161	SNMP (UDP)	Configuration and status	Both	Cannot configure or check the status of the Gateway via SNMP	iVIEW Network Manager or any other SNMP manager station
443	HTTPS (TCP)	Secure web interface	Both	Cannot administer the Gateway	
1024-4999	H.245 (TCP)	H.245	Both	No H.245	H.323 entity
1503	TCP	T.120 data collaboration	Both	Cannot establish a T.120 connection to/from the Gateway	Any T.120 endpoint
1619	RAS (UDP)—IVR	RAS (receiving Gatekeeper notifications)	Both	No RAS capabilities	Gatekeeper
1620	Q.931 (TCP)—IVR	Q.931	Both	No signaling capabilities	H.323 entity
1719	RAS (UDP)	RAS (receiving Gatekeeper notifications)	Both	No RAS capabilities	Gatekeeper
1820 (configurable via SNMP/web)	Q.931 (TCP)	Q.931 (receiving Setup)	Both	No signaling capabilities	H.323 entity
7222-7422 (even numbers only)	RTP (UDP)	RTP IVR (audio)	Both	Cannot open audio	H.323 entity
7223-7421 (odd numbers only)	RTCP (UDP)	RTCP IVR (audio)	Both	Cannot open audio	H.323 entity
7622-7822 (even numbers only)	RTP (UDP)	RTP IVR (video)	Both	Cannot open video	H.323 entity
7623-7821 (odd numbers only)	RTCP (UDP)	RTCP IVR (video)	Both	Cannot open video	H.323 entity

Table 1-8 Gateway-supported Ports—Incoming Connections (continued)

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Description
12002-12952 (even numbers only)	RTP (UDP)	For terminals connected to the Gateway and not to the IVR.	Both	Cannot open media	H.323 entity
12003-12951 (odd numbers only)	RTCP (UDP)	For terminals connected to the Gateway and not to the IVR.	Both	Cannot open media	H.323 entity

Table 1-9 Gateway-supported Ports—Outgoing Connections

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Description
162	SNMP traps (UDP)	Sending traps to server	Outgoing	Cannot send traps	Gateway
1719	RAS (UDP)	RAS (sending RRQ/ARQ messages)	Both	No RAS capabilities	H.323 entity
1720	Q.931 (TCP)	Q.931 (sending Setup/Connect messages)	Both	No Q.931 capabilities	H.323 entity

In addition to the ports listed in [Table 1-8](#) and [Table 1-9](#), RADVISION Gateways offer the following features:

- The ability to conceal a caller ID for both IP-to-ISDN and ISDN-to-IP calls.
- Configurable security access levels enabling and disabling Telnet, FTP, SNMP and ICMP (ping) services, as shown in [Table 1-10](#).

Table 1-10 Gateway Security Modes

Security Mode	Telnet	FTP	SNMP	ICMP (ping)
Low	Active	Active	Active	Active
Medium	Inactive	Inactive	Active	Active
High	Inactive	Inactive	Inactive	Inactive

3G Gateway

Table 1-11 lists the ports supported by the 3G Gateway.

Table 1-11 Ports Supported by the 3G Gateway

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Description
21	FTP (TCP); in use	File Transfer Protocol	Both	Cannot upgrade version	Upgrade Utility
23	Telnet (TCP); in use	Gateway logs and initial configuration	Both	Cannot view logs	Telnet client
80 (configurable)	HTTP (TCP)	Gateway Administrator and Call Control web user interfaces	Both	Cannot administer MCU	Web client
161	SNMP (UDP); in use	Configuration and status	Both	Cannot configure or check the status of the Gateway via SNMP	iVIEW Network Manager, SCOPIA iVIEW Management Suite or any other SNMP manager station
162	SNMP (UDP); in use	SNMP Trap events	Out	Cannot receive Traps	iVIEW Network Manager, SCOPIA iVIEW Management Suite or any other SNMP manager station
443	HTTPS (TCP); in use	Secure web interface	Both	Cannot administer the Gateway	
1024-4999	H.245 (TCP); in use	H.245 signaling. TCP connection to the SIU.	Both	Cannot connect H.323 calls; no connection to SIU.	Any H.323 entity
1719 (configurable)	RAS (UDP)	RAS signaling	Both	Cannot communicate with H.323 gatekeeper	H.323 gatekeeper
1820 (configurable)	Q.931 (TCP)	Q.931 signaling	Both	Cannot connect H.323 calls	Any H.323 entity
2944	MVP control (TCP); in use	MVP control protocol	Both	Cannot use external MVP	MVP
2945	MVP control (TCP); in use	MVP control protocol	Both	Cannot use external MVP	MVP
3336	TCP; in use	Conference control	Both	Cannot use Gateway Conference Control web user interface.	Conference Control web client terminal, SCOPIA iVIEW Management Suite or third-party controlling applications

Table 1-11 Ports Supported by the 3G Gateway (continued)

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Description
5060 (configurable)	SIP (TCP/UDP); in use	SIP signaling	Both	Cannot connect SIP calls	Any SIP entities
6000-7000 (configurable)	RTP/RTCP (UDP); in use	RTP media	Both	Cannot transmit/receive media streams	Any H.323 or SIP media enabled entity
12000-13000 (non- configurable)	RTP/RTCP	RTP media	Both	Cannot transmit/receive media streams	Any H.323 or SIP media enabled entity
123	NTP (UDP)	Network time protocol	Incoming	The Gateway will not have the most accurate time settings.	NTP server

MSP-324M (Multimedia Streaming proxy)

Table 1-12 lists the ports supported by the MSP-324M.

Table 1-12 MSP-324M-supported Ports

Port Range	Protocol	Functionality	Direction
1024-5000 (may vary according to operating system configuration)	RTSP, H.323	Dynamically allocated to ports	
1720	H.323	Signaling	Both
7000-9000 (configurable within maximum range of 5000-65535)	RTP (UDP)	RTP transmission	

IVP (Interactive Video Platform)

Table 1-13 lists the ports supported by the IVP Linux Server.

Table 1-13 IVP Server-supported Ports

IVP Server Port	External Server Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Description (External Server)
80		HTTP	IVP administration	Both	IVP Manager is not accessible.	Administrator's PC
162		SNMP	SNMP trap events	Both	SNMP traps cannot be sent to/from the external trap server.	External trap server
1099 (configurable)		TCP	IVP Controller Management API	Both	Cannot maintain a clustered IVP system. Cannot administer IVP from an external NMS.	Redundant IVP Controller; external iVIEW Network Manager
1100 (configurable)		TCP	IVP Monitor Management API	Both	Cannot maintain a clustered IVP system. Cannot administer IVP from an external NMS.	Redundant IVP Controller; external iVIEW Network Manager
1500 (configurable)		HTTP	IVP Controller Push API	Both	V2XML applications that based on the Push API from an external server will not function properly.	Application server hosting IVP application
5060 (configurable)		SIP (TCP, UDP)	B2BUA SIP signaling	Both	SIP calls cannot be established.	Any SIP entity
8080		HTTP	Tomcat web server	Both	Tomcat web applications are not accessible from the external server	Administrator's PC; users of web applications hosted on IVP server
8127		Telnet	IVP Controller Telnet logging	Both	No Telnet logging of IVP Controller.	Administrator's PC
Dynamically allocated	161	SNMP	SNMP configuration	Both	IVP components cannot be managed by IVP Manager.	MCU, ECS, MSP
Dynamically allocated	3271 (ECS)	TCP (XML)	ECS XML API	Both	H.323 calls cannot be established.	ECS
Dynamically allocated	3336 (MCU)	TCP (XML)	MCU XML API	Both	Calls cannot be established.	MCU

Table 1-13 IVP Server-supported Ports (continued)

IVP Server Port	External Server Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Description (External Server)
Dynamically allocated	3339 (internal)	TCP (XML)	B2BUA XML API	Both	Not affected in standard setup (internal connection).	N/A
Dynamically allocated	64010 (MSP)	TCP (XML)	MSP XML API	Both	Cannot play media through external MSP.	MSP

MSP-IVP (for Interactive Video Platform)

Table 1-14 lists the ports supported by the MSP for IVP.

Table 1-14 MSP-supported Ports

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Description
161	SNMP (UDP)	Receiving SNMP requests and sending responses	Both	No effect	IVP Network Manager or other SNMP manager station
Allocated by operating system	SNMP (UDP)	Sending SNMP traps	Out	No effect	IVP Network Manager or other SNMP manager station
2049	UDP	Remote file access (NFS)	Both	Cannot access media files located on server outside the firewall (setup not recommended)	NFS—remote file system
5070	SIP (TCP\UDP)	Sending and receiving SIP messages	Both	No effect	B2B UA/SIP entities
64010	XML Management (TCP)	XML API	Both	No effect	IVP Controller
6000-9000	RTP/RTCP (UDP)	Sending and receiving RTP packets	Both	Cannot transmit/receive media streams	RTSP streaming servers, RTSP entities
Allocated by operating system	RTSP (TCP)	Used for RTSP negotiation	Both	Cannot connect RTSP sessions	RTSP streaming servers, RTSP entities

MVP/M II SP (Media Video Processor)

Table 1-15 lists the ports supported by the MVP/M II SP.

Table 1-15 MVP/M II-supported Ports

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Description
21	FTP (TCP)	Software upgrade and video stream recording	Both	Cannot upgrade version	Upgrade Utility
23	Telnet (TCP)	MVP/M II online log	Both	Cannot view logs	Telnet client
161	SNMP (UDP)	Configuration and status	Both	Cannot configure or check the status of the Gateway via SNMP	iVIEW Network Manager, SCOPIA iVIEW Management Suite or any other SNMP manager station
3340	Font file client (TCP)	For receiving extended font files from the MCU	Both	Cannot work with different fonts	Font client software
10000-10240 (configurable from version 2.5)	RTP/RTCP (UDP)	RTP/RTCP media	Both	Cannot transmit/receive media streams	Any RTP/RTCP media enabled entity
21	FTP (TCP)	Software upgrade and video stream recording	Both	Cannot upgrade version	Upgrade Utility

ECS (SCOPIA ECS Gatekeeper)

Table 1-16 and Table 1-17 list the ports supported by the ECS.

Table 1-16 ECS-supported Ports—Incoming Connections (ECS as Server)

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Description
21	FTP (TCP)	File Transfer Protocol for offline viewing of ECS logs and CDRs	Both	Cannot view logs or retrieve CDR files	FTP client/CDR server
80 (configurable via <i>webs.ini</i> file)	HTTP (TCP)	Web interface	Both	Cannot view ECS web user interface	Web client terminal
161	SNMP (UDP)	Configuration and status	Both	Cannot configure or check the status of the ECS	iVIEW Network Manager, or any other SNMP manager station
1024-5000	H.245 (TCP)	H.245 routed calls	Both	No H.245 (except in Q.931 routed and direct mode)	Any H.323 entity H.245 port The actual port range is controlled by Windows OS. Verify that no other application nor any administrative action has modified values in range. The upper barrier is controlled by the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\MaxUserPort registry key. When this key is missing from the registry, a default value of 5000 is used by Windows OS.
1719	RAS (UDP)	RAS	Both	No RAS capabilities	Any H.323 entity using RAS signaling
1720	Q.931 (TCP)	Q.931 routed calls	Both	No signaling capabilities (except in direct mode)	Any H.323 entity using Q.931 signaling
3271	ECS XML	Incoming XML connection	Both	No incoming XML connection	XML server
12378 (configurable)	Alternate Gatekeeper protocol	Synchronization and negotiation between Alternate Gatekeepers	Both	No Alternate Gatekeeper functionality	Alternate Gatekeeper

Table 1-17 ECS-supported Ports—Outgoing Connections (ECS as Client)

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Description
23	Telnet (TCP)	Control of Sony endpoints	Both	No control over endpoints	Sony endpoint
53	DNS (TCP)	Query DNS for domains per call	Both	DNS disabled	DNS server
162 (configurable)	SNMP (UDP)	SNMP Trap events	Out	No traps are sent	To iVIEW Network Manager, or to any other SNMP manager station
1719	RAS (UDP)	Sending LRQ messages to Neighbor Gatekeepers	Both	No RAS	Neighbor Gatekeepers

DCS (Data Collaboration Server)

Table 1-18 lists the ports supported by the DCS.

Table 1-18 DCS-supported Ports

Port Range	Protocol	Functionality	Direction	Blocking in Application	Description
21	FTP (TCP)	Offline viewing of DCS logs	Both	Can be blocked	
23	Telnet (TCP)	Real-time viewing of DCS logs	Both	Can be blocked	
80	HTTP (TCP)	DCS configuration and monitoring via the web	Both	Can be blocked	Web client terminal
161	SNMP (UDP)	SNMP configuration	Both	Can be blocked by stopping the Windows SNMP service	iVIEW Network Manager, or any other SNMP manager station
162	SNMP (UDP)	SNMP Trap events	Out	Can be blocked by stopping the Windows SNMP service	To iVIEW Network Manager, or to any other SNMP manager station
1503	T.120 (TCP)	DCS configuration	Both	Can be blocked—blocking disables DCS functionality	Any T.120 terminal
3333	DTI (TCP)	For use when the DCS works with an MCU	Both	Can be blocked when the MCU is located on the LAN	MCU DTI port 3333.
9000-9099	T.120 (TCP)	DCS configuration	Both	Can be blocked—blocking disables DCS functionality	Any T.120 terminal

SCOPIA iVIEW Management Suite

Table 1-19 lists the ports supported by SCOPIA iVIEW Management Suite.

Table 1-19 SCOPIA iVIEW Management Suite-supported Ports

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall
23	Telnet (TCP)	Sony PCS address book	Both	SCOPIA iVIEW Management Suite cannot use Sony PCS address book feature.
25	TCP	Connect SMTP server for sending email notifications	Out	SCOPIA iVIEW Management Suite cannot send email notifications.
80 (configurable)	HTTP (TCP)	SCOPIA iVIEW Management Suite web user interface	In	SCOPIA iVIEW Management Suite cannot view SCOPIA iVIEW Management Suite web interface
161/162	SNMP	Network management of any element	Out	SCOPIA iVIEW Management Suite cannot operate the SNMP service with devices
389	TCP	LDAP servers communication	Both	SCOPIA iVIEW Management Suite cannot work with LDAP Servers
443	TCP	Tomcat/JBoss SSL	In	SCOPIA iVIEW Management Suite cannot view SCOPIA iVIEW Management Suite web interface via HTTPS
445	TCP/UDP	Connection to Active Directory Server	Out	NTLM SSO does not work
636	LDAP over SSL	Connection to Directory Server	Out	SCOPIA iVIEW Management Suite cannot connect to the Directory Server.
3336	TCP	Communication to XMPP server	Both	Cannot authenticate users from XMPP/SCOPIA Desktop Contact List
3339	TCP	SCOPIA iVIEW Management Suite XML API	Out	SCOPIA iVIEW Management Suite XML cannot communicate with the B2BUA component
3340	TCP/TLS	Connection to SCOPIA Desktop	Out	SCOPIA Desktop cannot use SCOPIA iVIEW Management Suite to place or manage calls
3341	TCP	This port is used only when SCOPIA iVIEW Management Suite needs to integrate with the IBM Sametime. IBM Sametime application uses this port to connect to SCOPIA iVIEW Management Suite.	In	SCOPIA iVIEW Management Suite cannot work with IBM Sametime.
3344	TCP/UDP	Synchronization of object data between multiple SCOPIA iVIEW Management Suite installations. Only used in distributed environments.	Both	SCOPIA iVIEW Management Suite cannot operate in a distributed deployment.

Table 1-19 SCOPIA iVIEW Management Suite-supported Ports (continued)

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall
4444, 4445	TCP	Required by the JBoss application server for correct JBoss operation.	Both	The port is not connected from a remote host; it is used by SCOPIA iVIEW Management Suite locally. SCOPIA iVIEW Management Suite cannot function if the port is occupied by another application.
5060	SIP (TCP/UDP)	SIP signaling	In	Cannot connect SIP calls
5061	TLS	SIP signaling	Both	No TLS connection will be available.
7800-7802 Configurable	TCP	Used for SCOPIA iVIEW Management Suite redundant deployments, for master/slave data synchronization	Both	No redundancy
8011	TCP	Provides web interface for internal ECS	Both	SCOPIA iVIEW Management Suite client cannot access internal ECS web.
11098/11099	TCP	Required by the JBoss application server for correct JBoss operation.	Both	The port is not connected from a remote host; it is used by SCOPIA iVIEW Management Suite locally. SCOPIA iVIEW Management Suite cannot function if the port is occupied by another application.
63148	DIIOIP	Only used when SCOPIA iVIEW Management Suite works with Domino Server	Out	The Domino Server may not be connected with SCOPIA iVIEW Management Suite successfully.

Table 1-20 lists the ports supported by the iVIEW Network Manager.

Table 1-20 iVIEW Network Manager-supported Ports

Port Range	Protocol	Functionality	Direction	Blocking in Application
7	TCP	Element online status detection.	Out	Cannot be blocked
21	TCP	Downloading logs from ECS or from other devices which allow logs to be downloaded via FTP Importing and Exporting TANDBERG Local Address Book Upgrading software	Out	
22	TCP	LifeSize endpoint detection Downloading PathFinder Server logs Detect and manage SCOPIA VC240	Out	
23	Telnet (TCP)	Element logs (v1.0), MCM control (v2.0) and endpoint control (v2.0).	Out	Can be blocked (v2.0)
24, 50000	Telnet (TCP)	24—Polycom endpoint control 50000—Sony endpoint control	Out	Can be blocked (v2.0)
53	UDP	DNS query	Out	Cannot parse domain name
80	HTTP (TCP)	Web interface This is also used for TANDBERG MXP management (XML API via HTTP)	Both	Cannot be blocked
161	SNMP	SNMP configuration to any managed element	Both	Cannot be blocked
162	SNMP	SNMP Trap events: from any managed element to any third-party SNMP manager	Both	Can be blocked
443	HTTPS (TCP)	Alternate web interface (for future use)	Both	Can be blocked
3089	TCP	Endpoint detection via PathFinder	Out	
3336	XML (TCP)	MCU XML API port for connecting to MCU v4.0 and later	Out	Can be blocked
8080	HTTP (TCP)	PathFinder Server web interface	Out	Can be blocked
8089	XML (TCP)	PathFinder server XML API port for connecting to PathFinder Server v7.0 and later	Out	Can be blocked
55003	TCP	SCOPIA XT1000	Out	

SCOPIA PathFinder

SCOPIA PathFinder is a Client/Server system rather than a single program. The SCOPIA PathFinder Server is the key component of the system; it receives requests from SCOPIA PathFinder Client, H.323 entities (gatekeepers & endpoints) and other utilities such as SSH and SFTP.

The SCOPIA PathFinder Client can only receive PDUs from H.323 entities. There must be no firewall or NAT between these H.323 entities and the SCOPIA PathFinder Client when the SCOPIA PathFinder Client functions as a server.

When the SCOPIA PathFinder Client functions as a client, its communication targets are H.323 entities, SCOPIA PathFinder Server and a public STUN server.

SCOPIA PathFinder Server as Server

Table 1-21 lists the ports supported by SCOPIA PathFinder Server functioning as a server.

Table 1-21 Ports Supported by SCOPIA PathFinder Server as Server

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Recipient Client or Server Type
22	SSH/SFTP (TCP)	Initial configuration, log download and upgrade	Client to SCOPIA PathFinder Server	Cannot initialize the server, download log and upgrade the server.	SSH client terminal
1719	UDP	H.460.18 RAS	Client to SCOPIA PathFinder Server	H.460.18 endpoints cannot register through Pathfinder server, firewall traversal function based on H.460.18 and H.460.19 cannot function.	H.460.18 endpoint/ H.460.18 client gatekeeper
2776	TCP	H.460.18 Call Signaling	Client to SCOPIA PathFinder Server	H.460.18 endpoints cannot register through Pathfinder server.	H.460.18 endpoint/ H.460.18 client gatekeeper
2776	UDP	H.460.19 Multiplex Media Channel	Client to SCOPIA PathFinder Server	H.460.18 endpoints cannot set up logical channels, media exchange of calls which traverse the firewall using H.460.18 and H.460.19 cannot function when using multiplexing.	H.460.18 endpoint/ H.460.18 client gatekeeper
2777	TCP	H.460.18 and H.460.19 Call Control	Client to SCOPIA PathFinder Server	H.460.18 endpoints cannot set up Call Control channel, firewall traversal function based on H.460.18 and H.460.19 cannot function.	H.460.18 endpoint/ H.460.18 client gatekeeper

Table 1-21 Ports Supported by SCOPIA PathFinder Server as Server (continued)

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Recipient Client or Server Type
2777	UDP	H.460.19 Multiplex Media Control Channel	Client to SCOPIA PathFinder Server	H.460.18 endpoints cannot set up logical channels, media exchange of calls which traverse the firewall using H.460.18 and H.460.19 cannot function when using multiplexing.	H.460.18 endpoint/ H.460.18 client gatekeeper
3089	TCP	Signaling and media traversal	Client to SCOPIA PathFinder Server	SCOPIA PathFinder Client cannot connect to SCOPIA PathFinder Server. Legacy H.323 endpoints behind the SCOPIA PathFinder Client cannot call external endpoints.	SCOPIA PathFinder Client
3089	UDP	Media traversal	Client to SCOPIA PathFinder Server	Cannot use UDP to traverse media; can only use TCP to traverse media.	SCOPIA PathFinder Client
8080	HTTP (TCP)	Web interface	Client to SCOPIA PathFinder Server	Cannot configure SCOPIA PathFinder Server.	Web client/browser
8089	XML (TCP)	PathFinder version 7.0 XML API service	Client to SCOPIA PathFinder Server	The External Management System cannot get SCOPIA PathFinder Server status or receive traps from SCOPIA PathFinder Server.	XML API Client
1024-65535	TCP, UDP	Standard H.323 communication	Client to SCOPIA PathFinder Server	Cannot communicate with server-side endpoints.	H.323 entity
1720	TCP, DPA	IP call signaling	External H.323 endpoint to SCOPIA PathFinder Server	No signaling capabilities: guest users cannot dial into internal endpoints	Any H.323 entity using a Q.931 signaling in DPA mode

Table 1-21 Ports Supported by SCOPIA PathFinder Server as Server (continued)

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Recipient Client or Server Type
2777	UDP	H.460.19 Multiplex Media Control Channel	Client to SCOPIA PathFinder Server	H.460.18 endpoints cannot set up logical channels, media exchange of calls which traverse the firewall using H.460.18 and H.460.19 cannot function when using multiplexing.	H.460.18 endpoint/H.460.18 client gatekeeper
3089	TCP	Signaling and media traversal	Client to SCOPIA PathFinder Server	SCOPIA PathFinder Client cannot connect to SCOPIA PathFinder Server. Legacy H.323 endpoints behind the SCOPIA PathFinder Client cannot call external endpoints.	SCOPIA PathFinder Client
3089	UDP	Media traversal	Client to SCOPIA PathFinder Server	Cannot use UDP to traverse media; can only use TCP to traverse media.	SCOPIA PathFinder Client
8080	HTTP (TCP)	Web interface	Client to SCOPIA PathFinder Server	Cannot configure SCOPIA PathFinder Server.	Web client/browser
8089	XML (TCP)	PathFinder version 7.0 XML API service	Client to SCOPIA PathFinder Server	The External Management System cannot get SCOPIA PathFinder Server status or receive traps from SCOPIA PathFinder Server.	XML API Client
1024-65535	TCP, UDP	Standard H.323 communication	Client to SCOPIA PathFinder Server	Cannot communicate with server-side endpoints.	H.323 entity
1720	TCP, DPA	IP call signaling	External H.323 endpoint to SCOPIA PathFinder Server	No signaling capabilities: guest users cannot dial into internal endpoints	Any H.323 entity using a Q.931 signaling in DPA mode

Table 1-21 Ports Supported by SCOPIA PathFinder Server as Server (continued)

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Recipient Client or Server Type
4000-5000	TCP	H.323 call signaling and call control	External H.323 endpoint to SCOPIA PathFinder Server	Cannot setup/connect DPA mode calls	Any H.323 entity using a Q.931 signaling in DPA mode
4000-5000	UDP	H.323 call media traversal	External H.323 endpoint to SCOPIA PathFinder Server	Cannot setup/connect DPA mode calls	Any H.323 entity

SCOPIA PathFinder Server as Client

Table 1-22 lists the ports supported by SCOPIA PathFinder Server functioning as the client.

Table 1-22 Ports Supported by SCOPIA PathFinder Server as Client

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Recipient Client or Server Type
53	DNS (UDP)	Query DNS for domain per call	SCOPIA PathFinder Server to another Server	Cannot support domain name calls and dialing by URI.	DNS server
1024-65535	UDP and TCP	Standard H.323 communication	SCOPIA PathFinder Server to H.323 entities	Cannot communicate with server-side H.323 entities. Cannot communicate with external H.323 entities through DPA.	H.323 entity
1719	RAS (UDP)	Communication with gatekeeper	SCOPIA PathFinder Server to the main gatekeeper	Cannot relay H.323 communication.	Gatekeeper
1720	TCP	H.323 IP call signaling	SCOPIA PathFinder Server to external SCOPIA PathFinder Server	No signaling capabilities: guest users cannot dial into internal endpoints	Any H.323 entity using a Q.931 signaling in DPA mode
3089	TCP	Neighbor server signaling and media connection	SCOPIA PathFinder Server to another Server	Cannot connect to neighbor server.	PathFinder Server
3089	UDP	Neighbor server media connection	SCOPIA PathFinder Server to another Server	Cannot traverse media to neighbor server using UDP.	PathFinder Server
4000-5000	TCP	H.323 call signaling and call control	SCOPIA PathFinder Server to external SCOPIA PathFinder Server	Cannot setup/connect DPA mode calls with external SCOPIA PathFinder Server	Any H.323 entity using a Q.931 signaling in DPA mode
4000-5000	UDP	H.323 call media traversal	SCOPIA PathFinder Server to external SCOPIA PathFinder Server	Cannot setup/connect DPA mode calls with external SCOPIA PathFinder Server	Any H.323 entity

Pathfinder Client as Server

Table 1-23 lists the ports supported by a SCOPIA PathFinder Client functioning as a server.

Table 1-23 Ports Supported by SCOPIA PathFinder Client as Server

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Recipient Client or Server Type
1719	RAS (UDP)	H.323 entity registration, admission and status communication	H.323 entity to SCOPIA PathFinder Client	H.323 endpoints cannot register to SCOPIA PathFinder Client. The enterprise Gatekeeper cannot locate external endpoints through PathFinder.	H.323 entity
1025-65535	TCP and UDP	H.323 Call Signaling, Call Control and Media Communication	H.323 entity to SCOPIA PathFinder Client	H.323 entities cannot set up calls through SCOPIA PathFinder.	H.323 entity

SCOPIA PathFinder Client as Client

Table 1-24 lists the ports supported by the SCOPIA PathFinder Client functioning as a client.

Table 1-24 Ports Supported by SCOPIA PathFinder Client as Client

Port Range	Protocol	Functionality	Direction	Result of Blocking Port on Firewall	Recipient Client or Server Type
3089	TCP and UDP	PathFinder tunneling service	SCOPIA PathFinder Client to Server	SCOPIA PathFinder Client cannot connect to the SCOPIA PathFinder Server. Legacy H.323 endpoints behind the SCOPIA PathFinder Client cannot call external endpoints.	PathFinder Server
3478	STUN (UDP)	STUN Binding Request	SCOPIA PathFinder Client to Server	SCOPIA PathFinder Client cannot determine its public IP address. Smart Direct Media Connect cannot function.	STUN server
1024-65535	TCP and UDP	H.323 Call Signaling, Call Control and Media Communication	SCOPIA PathFinder Client to H.323 entities	H.323 entities cannot set up calls through SCOPIA PathFinder.	H.323 entity

SCOPIA Desktop

[Table 1-25](#) lists the ports that need to be opened between the SCOPIA Desktop Server and the internal network.

[Table 1-26](#) lists the ports that need to be opened between the SCOPIA Desktop Server and the public internet.

[Table 1-28](#) lists the ports that need to be opened between the SCOPIA Desktop Server and XMPP Server.

Table 1-25 Port Security—SCOPIA Desktop Server and Internal Network

Port Range	Protocol	Severity	Functionality
80	TCP	Optional	GUI—The alternative is to configure the GUI to run on port 443.
8080	TCP	Optional	GUI access to SCOPIA iVIEW Management Suite web pages if SCOPIA iVIEW Management Suite is deployed on the same PC as SCOPIA Desktop.
443	TCP	Mandatory	Control connection between the SCOPIA Desktop Client and the SCOPIA Desktop Server.
3340	TCP	Mandatory	Meeting control connection between SCOPIA iVIEW Management Suite and the SCOPIA Desktop Server.
3337	TCP	Mandatory	Meeting cascading connection between the SCOPIA Desktop Server and the SCOPIA MCU.
139/445	TCP	Recommended for performing Active Directory authentication.	From SCOPIA Desktop to Active Directory in order to do auto discovery and authentication.
10000-65535 (Configurable)	UDP	Mandatory	Media connection between the SCOPIA Desktop Server and the SCOPIA MCU. Also open these ports between the SCOPIA Desktop Server and the MVP.
5269	UDP	Optional	SCOPIA Desktop Server to XMPP Server for performing proxy XMPP Client connections.
1719	UDP	Mandatory	ECS Gatekeeper
1720 (configurable)	TCP	Mandatory	SCOPIA Desktop Server to ECS or MCU
137/138	UDP	Recommended for performing Active Directory authentication.	From SCOPIA Desktop to Active Directory in order to do auto discovery and authentication.

Table 1-25 Port Security—SCOPIA Desktop Server and Internal Network (continued)

Port Range	Protocol	Severity	Functionality
1024-65535 (Configurable)	TCP	Mandatory	<p>In deployments where the SCOPIA Desktop Server works in conjunction with the MCU only, this port range is used for establishing connection from SCOPIA Desktop Server to MCU.</p> <p>In deployments where the SCOPIA Desktop Server works in conjunction with the SCOPIA iVIEW Management Suite, this port range is used for establishing connection from SCOPIA Desktop Server to ECS.</p>
1025-65535	TCP	Mandatory	H.323 traffic between the SCOPIA Desktop Server and the SCOPIA MCU.
10000-65535	UDP	Recommended	<p>Media connection between the SCOPIA Desktop Client and Server. If not open, the connection will be tunneled via TCP port 443 and performance will not be optimal.</p> <p>An administrator can also control the range of the of the multimedia ports using the SCOPIA Desktop Server Administrator web interface (Client > Settings tab > Multimedia Ports area).</p>
6972-65535	UDP	Mandatory	Media connection between the SCOPIA Desktop Server and the SCOPIA Desktop Darwin server, if separated.
7070	TCP	Optional	Client-to-Server port for tunneled RTSP streaming.
10000-65535	UDP	Optional	<p>Limit UDP ports opened on the firewall to allow SCOPIA Desktop to send RTP to the internal network (MCU).</p> <p>We recommend that you use a limited range between 2326 and 65535.</p> <p>If this option is used:</p> <ul style="list-style-type: none"> • Each Client-to-SCOPIA Desktop connection uses 2 UDP ports. • Each SCOPIA Desktop Server-to-MCU connection uses 6 UDP ports. • Each conference uses 6 UDP ports for server-to-server communication. <p>Reserve 11 ports per user. To define the range, multiply the number of connections allowed by your license by 11.</p> <p>Add up to 60 ports to support the maximum of ten simultaneous recordings.</p>
3478	UDP	Optional	The STUN access is for the SCOPIA Desktop client to communicate with the STUN Server. To acquire the true SIP PTP, open the UDP ports (10000-65535, 6972-65535, 10000-65535, 3478). If the UDP ports are not open, the STUN server will use the SCOPIA Desktop Server as a relay agent.

Table 1-26 Port Security—SCOPIA Desktop Server and Public Internet

Port Range	Protocol	Severity	Functionality
80	TCP	Optional	GUI access. The alternative is to configure the GUI to run on port 443.
8080	TCP	Optional	GUI access to an optional SCOPIA iVIEW Management Suite.
443	TCP	Mandatory	Control connection between the SCOPIA Desktop Client and Server.
10000-65535	UDP	Recommended	<p>Media connection between the SCOPIA Desktop Client and Server. If not open, the connection will be tunneled via TCP port 443 and performance will not be optimal.</p> <p>Limit UDP ports opened on the firewall to allow conference clients to send RTP to SCOPIA Desktop.</p> <p>We recommend that you use a limited range between 10000 and 65535. If this option is used:</p> <ul style="list-style-type: none"> Each Client-to-SCOPIA Desktop connection uses 2 UDP ports. Each SCOPIA Desktop Server-to-MCU connection uses 6 UDP ports. Each conference uses 6 UDP ports for server-to-server communication. <p>We recommend that you reserve 11 ports per user. To define the range, multiply the number of connections allowed by your license by 11.</p> <p>Recordings use 6 ports per recording. Add up to 60 ports to support the maximum of ten simultaneous recordings.</p> <p>You can modify the media port range using the SCOPIA Desktop Server Administrator interface: Client > Settings tab > Multimedia Ports section.</p>
7070	TCP	Mandatory	Client-to-Server port for tunneled RTSP streaming.

You can configure the incoming pinholes only after outgoing pinholes are initiated.

Table 1-27 Port Security—SCOPIA Desktop Client-to-Client connection

Port Range	Protocol	Severity	Functionality
5060	SIP UDP		For establishing SIP PTP connection.
1025-65535	UDP		

Table 1-28 Port Security—SCOPIA Desktop Server and XMPP Server

Port Range	Protocol	Severity	Functionality	Result of Blocking in Application
5222	TCP		Direct SCOPIA Desktop Client to XMPP connection.	The SCOPIA Desktop Client tries to use port 443 for tunnelled connection to the SCOPIA Desktop Server.
5269	TCP		XMPP Server for supporting proxy XMPP connections from SCOPIA Desktop Server for SCOPIA Desktop Clients.	From SCOPIA Desktop Server
3336	TCP	Mandatory for SCOPIA iVIEW Management Suite authentication	If XMPP Server is configured for SCOPIA iVIEW Management Suite authentication, it uses this port for XML communications.	Users would not be able to log into XMPP Server.
389	TCP	Mandatory for LDAP authentication	If XMPP Server is configured for LDAP server (either Active Directory or Domino), XMPP Server uses this port for LDAP communication for user authentication.	Users would not be able to log into XMPP Server.

SCOPIA XT Desktop Server

Table 1-29 lists ports that need to be open on SCOPIA XT Desktop Server.

Table 1-29 Port Security—SCOPIA XT Desktop Server and Internal Network

Port Range	Protocol	Severity	Functionality
80	TCP	Optional	GUI—The alternative is to configure the GUI to run on port 443.
443	TCP	Mandatory	Control connection between the SCOPIA XT Desktop Client and the SCOPIA XT Desktop Server.
10000-65535	UDP	Mandatory	Media connection between the SCOPIA XT Desktop Server and the SCOPIA XT1000 Series.
1025-65535	TCP	Mandatory	H.323 traffic between the SCOPIA Desktop Server and the SCOPIA XT1000 Series.
3336, 3337	TCP	Mandatory	Cascade/XML control connections between SCOPIA Desktop Server and SCOPIA XT1000.
10000-65535	UDP	Recommended	<p>Media connection between the SCOPIA XT Desktop Client and Server. If not open, the connection will be tunneled via TCP port 443 and performance will not be optimal.</p> <p>Limit UDP ports opened on the firewall to allow conference clients to send RTP to SCOPIA Desktop.</p> <p>We recommend that you use a limited range between 10000 and 65535.</p> <p>If this option is used:</p> <ul style="list-style-type: none"> Each Client-to-SCOPIA Desktop connection uses 2 UDP ports. Each SCOPIA XT Desktop Server-to-MCU connection uses 6 UDP ports. Each conference uses 6 UDP ports for server-to-server communication. <p>We recommend that you reserve 11 ports per user. To define the range, multiply the number of connections allowed by your license by 11.</p>

Table 1-30 lists ports that need to be open on SCOPIA XT1000.

Table 1-30 Port Security—SCOPIA XT1000 and Internal Network

Port number	Protocol/Use	Port Type	Functionality	Direction	Result of Blocking Port on Firewall	Description/External Client
22	SSH	TCP	Secure Shell	Both	No secure shell	Remote management
23	Telnet	TCP	Telnet server	Both	No Telnet access	Remote management
69	TFTP	UDP	TFTP client or server	Both	Cannot send or receive files via TFTP	Send or receive files via TFTP
80	HTTP	TCP	WEB Server	Both	No WEB server	WEB remote management or use
123	SNTP	UDP	SNTP client	Both	Cannot get the Internet UTC time	Get the Internet UTC time
161	SNMP	UDP	SNTP Configuration and Status	Both	Cannot configure or check the status of the terminal via SNMP	Interface to iVIEW Network Manager or any other SNMP manager station
162	SNMP	UDP	SNTP Trap Events	Out	The terminal cannot send SNMP events	Interface to iVIEW Network Manager or any other SNMP manager station
55003	AT Commands	TCP	API for Remote Management	Both	Cannot send/receive commands	iVIEW Network Manager
55099	Software Upgrade	TCP	Software Upgrade	Both	Cannot upgrade software	iVIEW Network Manager/Landownload
3338	XML Commands	TCP	Remote Control	Both	Cannot send/receive commands. SCOPIA Control and SCOPIA XT Desktop Server are not operational.	SCOPIA Control; SCOPIA XT Desktop Server
3339; 3340	XML HINTS	TCP	Remote Control	Out	Cannot send hints. SCOPIA Control and SCOPIA XT Desktop Server are not operational.	SCOPIA Control; SCOPIA XT Desktop Server
1718	H.225.0/ RAS	UDP	H.323 call signaling to a GK for "Gatekeeper Automatic Discovery" procedure	Out to the multicast IP address 224.0.0.41 ("all GK")	The H.323 endpoint cannot automatically discover a gatekeeper (only manual configuration available).	The H.323 endpoint can automatically discover a gatekeeper.

Table 1-30 Port Security—SCOPIA XT1000 and Internal Network (continued)

Port number	Protocol/ Use	Port Type	Functionality	Direction	Result of Blocking Port on Firewall	Description/External Client
1719	H.225.0/ RAS	UDP	H.323 call signaling to a GK	Both	The H.323 endpoint cannot use the services of a gatekeeper.	The H.323 endpoint uses the services of a gatekeeper
1720	H.225.0/ Q.931	TCP	H.323 call signaling (Q.931)	Both	Cannot connect H.323 calls.	"Well known" H.323 service port.
5060	SIP	TCP	SIP call signaling	Both	Cannot connect SIP calls over TCP.	"Well known" SIP service port.
5060	SIP	UDP	SIP call signaling	Both	Cannot connect SIP calls over UDP.	"Well known" SIP service port.
3230- 3248	H.225.0/ Q.931 and H.245 and SIP	TCP	H.323 call control signaling (Q.931) and media control signaling (H.245) and SIP (TCP) call signaling and BFCP signaling	Both	Cannot connect H.323 calls. Cannot connect SIP calls on TCP transport.	Ephemeral TCP ports used to connect simultaneous H.323 and SIP calls. The range can be modified by the user interface.
5070	BFCP	TCP	SIP content (presentation) video signaling	Both	No SIP content video available.	"Well known" BFCP service port (used by SIP).
3230- 3287	RTP and RTCP	UDP	H.323 and SIP media (audio, video, H.224/data RTP) and media control (RTCP)	Both	No media exchanged in the H.323 or SIP call.	Ephemeral UDP ports used to connect simultaneous H.323 and SIP calls media.
3478- 3479	STUN	UDP	STUN client	Both	Cannot discover the presence of a firewall or NAT (only manual configuration available).	Discover the presence of a firewall or NAT and the public IP address. The range can be modified by the user interface.

SCOPIA VC240

Table 1-31 lists ports that need to be opened between SCOPIA VC240 and network devices.

Table 1-31 Ports supported by SCOPIA VC240

Port	Protocol/Use	Functionality	Direction	Result of Blocking on Firewall	Description
22	TCP (SSH)	SCOPIA iVIEW Management Suite	Both	SCOPIA iVIEW Management Suite does not communicate with the unit	SSH Server
23	TCP (Telnet)	SCOPIA iVIEW Management Suite and administration	Both	SCOPIA iVIEW Management Suite does not communicate with the unit	
80	HTTP (TCP)	Open APIs	Both	Web server and open APIs do not function	Web application or open API-based application
161	UDP (SNMP)	Configuration and status	Both	Cannot configure or check the status of the terminal via SNMP	iVIEW Network Manager, SCOPIA iVIEW Management Suite or any other SNMP manager station
162	UDP (SNMP)	SNMP trap events	Out	Cannot receive traps	iVIEW Network Manager, SCOPIA iVIEW Management Suite or any other SNMP manager station
443	HTTPS (TCP)	Open APIs	Both	Web server and open APIs do not function	Web application or open API-based application
1024-4999	TCP (H.245)	H.245 signaling	Both	Cannot connect H.323 calls	Any H.323 entity
1719	UDP (RAS)	RAS signaling	Both	Cannot communicate with H.323 gatekeeper	H.323 gatekeeper
1720	TCP (Q.931)	Q.931 signaling	Both	Cannot connect H.323 calls	Any H.323 entity
4000	RV shell cmd	Internal use	Both	SCOPIA iVIEW Management Suite does not communicate with the unit	Internal use

Table 1-31 Ports supported by SCOPIA VC240 (continued)

Port	Protocol/Use	Functionality	Direction	Result of Blocking on Firewall	Description
5060	TCP/UDP (SIP)	SIP signaling	Both	Cannot connect SIP calls	Any SIP entity
10000-10299	UDP (RTP/RTCP)	RTP media	Both	Cannot transmit/receive media streams	Any H.323 or SIP media enabled entity



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

