

# Port Security

## SCOPIA Solution Version 7.0



## NOTICE

© 2000-2009 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.

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.

Port Security

Publication 19, June 2009 (SCOPIA Solution version 7.0)

<http://www.radvision.com>

# 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:

- MCU
- Gateway
- 3G Gateway
- MSP-324M (Multimedia Streaming proxy)
- IVP (Interactive Video Platform)
- MSP-IVP (for Interactive Video Platform)
- MVP (Media Video Processor)
- MVP/M II SP (Media Video Processor)
- ECS (Enhanced Communication Server)
- DCS (Data Collaboration Server)
- iVIEW Suite
- iVIEW Network Manager
- PathFinder
- SCOPIA Desktop

---

**Note** 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.

---

## MCU

## MCU

Table 1 lists the ports supported by the MCU.

**Table 1** Ports Supported by the MCU

Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Source/Destination
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, iVIEW Suite or any other SNMP manager station
162	SNMP (UDP)	SNMP Trap events	Out	Cannot receive Traps	iVIEW Network Manager, iVIEW 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
2010	MPI (TCP)	MP control protocol	Both	Cannot use external MP	Any standalone MP units (MCUs configured to be MPs in clustering mode)
2944	MVP control (TCP)	MVP control protocol	Both	Cannot use external MVP	MVP
2945	MVP control (TCP)	MVP control protocol	Both	Cannot use external MVP	MVP

**Table 1** *Ports Supported by the MCU (continued)*

Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Source/Destination
3333	DTI (TCP)	DCS control protocol	Both	Cannot use external DCS	DCS
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, iVIEW 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	
5060 (configurable)	SIP (TCP/UDP)	SIP signaling	Both	Cannot connect SIP calls	Any SIP entities
10000-11000 (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](#), RADVISION MCUs offer configurable security access levels enabling and disabling Telnet, FTP, SNMP and ICMP (ping) services, as shown in [Table 2](#).

**Table 2** *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

## Gateway

### GATEWAY

Table 3 and Table 4 list the ports supported by the Gateway.

**Table 3** Gateway-supported Ports—Incoming Connections

Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Source/Destination
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

**Table 3** Gateway-supported Ports—Incoming Connections (continued)

Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Source/Destination
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
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 4** Gateway-supported Ports—Outgoing Connections

Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Source/Destination
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 3](#) and [Table 4](#), 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 5](#).

**Table 5** 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 6 lists the ports supported by the 3G Gateway.

**Table 6** Ports Supported by the 3G Gateway

Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Source/Destination
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, iVIEW Suite or any other SNMP manager station
162	SNMP (UDP); in use	SNMP Trap events	Out	Cannot receive Traps	iVIEW Network Manager, iVIEW 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

## 3G Gateway

**Table 6** *Ports Supported by the 3G Gateway (continued)*

<b>Port</b>	<b>Protocol/Use</b>	<b>Functionality</b>	<b>Direction</b>	<b>Result of Blocking Port on Firewall</b>	<b>Source/Destination</b>
3336	TCP; in use	Conference control	Both	Cannot use Gateway Conference Control web user interface.	Conference Control web client terminal, iVIEW Suite or third-party controlling applications
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

Table 7 lists the ports supported by the MSP-324M.

**Table 7** *MSP-324M-supported Ports*

Port	Protocol/Use	Functionality	Direction	Blocking in Application
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

## IVP

Table 8 lists the ports supported by the IVP Linux Server.

**Table 8** IVP Server-supported Ports

IVP Server Port	External Server Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Source/Destination (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

**Table 8**      *IVP Server-supported Ports (continued)*

<b>IVP Server Port</b>	<b>External Server Port</b>	<b>Protocol/Use</b>	<b>Functionality</b>	<b>Direction</b>	<b>Result of Blocking Port on Firewall</b>	<b>Source/Destination (External Server)</b>
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
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**

Table 9 lists the ports supported by the MSP for IVP.

**Table 9** *MSP-supported Ports*

Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Source/Destination
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**

Table 10 lists the ports supported by the MVP.

**Table 10** MVP-supported Ports

Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Source/Destination
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, iVIEW Suite or any other SNMP manager station
2944, 2945	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 streams	Any RTP/RTCP media enabled entity

**MVP/M II SP**

Table 11 lists the ports supported by the MVP/M II SP.

**Table 11** MVP/M II-supported Ports

Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Source/Destination
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, iVIEW 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

Table 12 and Table 13 list the ports supported by the ECS.

**Table 12** ECS-supported Ports—Incoming Connections (ECS as Server)

Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Source/Destination
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
1024-4999	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
1024-65535 (allocated by operating system, upper limit configurable)	RTP (UDP)—regular capacity	ECS Firewall Proxy Solution	Both	No ECS Firewall Proxy Solution functionality	Any H.323 terminal
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 12** *ECS-supported Ports—Incoming Connections (ECS as Server) (continued)*

<b>Port</b>	<b>Protocol/Use</b>	<b>Functionality</b>	<b>Direction</b>	<b>Result of Blocking Port on Firewall</b>	<b>Source/Destination</b>
20000 and above (overrides existing ports)	RTP (UDP)—increased capacity	ECS Firewall Proxy Solution	Both	No ECS Firewall Proxy Solution functionality	Any H.323 terminal

**Table 13** *ECS-supported Ports—Outgoing Connections (ECS as Client)*

<b>Port</b>	<b>Protocol/Use</b>	<b>Functionality</b>	<b>Direction</b>	<b>Result of Blocking Port on Firewall</b>	<b>Source/Destination</b>
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
389 (configurable)	LDAP (TCP)	LDAP queries and modifications	Both	Cannot use LDAP	LDAP server
1719 (configurable)	RAS (UDP)	Sending LRQ messages to Neighbor Gatekeepers	Both	No RAS	Neighbor Gatekeepers
1812 (configurable)	RADIUS (UDP)	Authentication	Both	No RADIUS authentication	RADIUS server
1813 (configurable)	RADIUS (UDP)	Accounting	Both	No RADIUS accounting	RADIUS server
Configurable	ECS XML (TCP)	External XML authorization server	Both	Can be blocked	XML authorization server

**Table 13** *ECS-supported Ports—Outgoing Connections (ECS as Client) (continued)*

<b>Port</b>	<b>Protocol/Use</b>	<b>Functionality</b>	<b>Direction</b>	<b>Result of Blocking Port on Firewall</b>	<b>Source/Destination</b>
Configurable	CDR (TPKT/TCP)	Sends CDRs to the server	Both	Can be blocked	Billing server

**DCS**

Table 14 lists the ports supported by the DCS.

**Table 14** DCS-supported Ports

Port	Protocol/Use	Functionality	Direction	Blocking in Application	Source/Destination
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

**iVIEW SUITE**

Table 15 lists the ports supported by iVIEW Suite.

**Table 15** *iVIEW Suite-supported Ports*

<b>Port</b>	<b>Protocol/Use</b>	<b>Functionality</b>	<b>Direction</b>	<b>Result of Blocking Port on Firewall</b>	<b>Source/Destination</b>
23	Telnet (TCP)	Sony PCS address book	Both	Cannot use Sony PCS address book feature.	Telnet clients or Sony PCS
80 (configurable)	HTTP (TCP)	iVIEW Suite web user interface	Both	Cannot view iVIEW Suite web interface	Web client
53	TCP, UDP	LDAP, SSO, DNS for resolving FQDN to IP addresses	Both	Cannot support domain name calls and dialing by URI.	DNS server
443	TCP	Tomcat/JBoss SSL	Both	Cannot view iVIEW Suite web interface via HTTPS	Web client with SSL
3271	TCP	ECS authorization and third-party call control (for example, for point-to-point calls)	Both	No ECS authorization	ECS
3336	TCP	MCU XML Proxy API	Both	Cannot use MCU XML Proxy API	TCP client using the iVIEW Suite MCU Proxy API
3344	TCP/UDP	Synchronization of object data between multiple iVIEW Suite installations. Only used in distributed environments.	Both	iVIEW cannot operate in a distributed deployment.	iVIEW Suite

**Table 15** *iVIEW Suite-supported Ports (continued)*

Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Source/Destination
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 iVIEW Suite locally. iVIEW Suite cannot function if the port is occupied by another application.	iVIEW Suite internal
5060	SIP (TCP/UDP)	SIP signaling	Both	Cannot connect SIP calls	Any SIP entities
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 iVIEW Suite locally. iVIEW Suite cannot function if the port is occupied by another application.	iVIEW Suite internal

## iVIEW NETWORK MANAGER

Table 16 lists the ports supported by the iVIEW Network Manager.

**Table 16** *iVIEW Network Manager-supported Ports*

Port	Protocol/Use	Functionality	Direction	Blocking in Application	Source/Destination
7	TCP	Element online status detection.	Out	Cannot be blocked	
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)	Endpoint control (v2.0)	Out	Can be blocked (v2.0)	
80	HTTP (TCP)	Web interface	Both	Cannot be blocked	Web client terminal

**Table 16** *iVIEW Network Manager-supported Ports*

<b>Port</b>	<b>Protocol/Use</b>	<b>Functionality</b>	<b>Direction</b>	<b>Blocking in Application</b>	<b>Source/Destination</b>
161	SNMP	SNMP configuration	Both	Cannot be blocked	To any managed element
162	SNMP	SNMP Trap events	Both	Can be blocked	From any managed element to any third-party SNMP manager
443	HTTPS (TCP)	Alternate web interface (for future use)	Both	Can be blocked	
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	PathFinder Server
8089	XML (TCP)	PathFinder server XML API port for connecting to PathFinder Server v7.0 and later	Out	Can be blocked	PathFinder Server

## PATHFINDER

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

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

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

### PATHFINDER SERVER AS SERVER

Table 17 lists the ports supported by PathFinder Server functioning as a server.

**Table 17** Ports Supported by PathFinder Server as Server

Port	Protocol/Use	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 PathFinder	Cannot initialize the server, download log and upgrade the server.	SSH client terminal
1719	UDP	H.460.18 RAS	Client to PathFinder	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 PathFinder	H.460.18 endpoints cannot register through Pathfinder server.	H.460.18 endpoint/ H.460.18 client gatekeeper

**Table 17** *Ports Supported by PathFinder Server as Server (continued)*

<b>Port</b>	<b>Protocol/Use</b>	<b>Functionality</b>	<b>Direction</b>	<b>Result of Blocking Port on Firewall</b>	<b>Recipient Client or Server Type</b>
2776	UDP	H.460.19 Multiplex Media Channel	Client to PathFinder	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 PathFinder	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
2777	UDP	H.460.19 Multiplex Media Control Channel	Client to PathFinder	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

## PathFinder

**Table 17** *Ports Supported by PathFinder Server as Server (continued)*

<b>Port</b>	<b>Protocol/Use</b>	<b>Functionality</b>	<b>Direction</b>	<b>Result of Blocking Port on Firewall</b>	<b>Recipient Client or Server Type</b>
3089	TCP	Signaling and media traversal	Client to PathFinder	PathFinder Client cannot connect to PathFinder Server. Legacy H.323 endpoints behind the PathFinder Client cannot call external endpoints.	Pathfinder Client
3089	UDP	Media traversal	Client to PathFinder	Cannot use UDP to traverse media; can only use TCP to traverse media.	Pathfinder Client
8080	HTTP (TCP)	Web interface	Client to PathFinder	Cannot configure PathFinder server.	Web client/browser
8089	XML (TCP)	PathFinder version 7.0 XML API service	Client to PathFinder	The External Management System cannot get PathFinder Server status or receive traps from PathFinder Server.	XML API Client
1024-65535	TCP, UDP	Standard H.323 communication	Client to PathFinder	Cannot communicate with server-side endpoints.	H.323 entity

**PATHFINDER SERVER  
AS CLIENT**

Table 18 lists the ports supported by PathFinder Server functioning as the client.

**Table 18** *Ports Supported by PathFinder Server as Client*

<b>Port</b>	<b>Protocol/Use</b>	<b>Functionality</b>	<b>Direction</b>	<b>Result of Blocking Port on Firewall</b>	<b>Recipient Client or Server Type</b>
53	DNS (UDP)	Query DNS for domain per call	PathFinder to Server	Cannot support domain name calls and dialing by URI.	DNS server
1024-65535	UDP and TCP	Standard H.323 communication	Both	Cannot communicate with server-side H.323 entities.	H.323 entity
1719	RAS (UDP)	Communication with gatekeeper	Both	Cannot relay H.323 communication.	Gatekeeper
3089	TCP	Neighbor server signaling and media connection	PathFinder to Server	Cannot connect to neighbor server.	PathFinder Server
3089	UDP	Neighbor server media connection	PathFinder to Server	Cannot traverse media to neighbor server using UDP.	PathFinder Server

**PATHFINDER CLIENT  
AS SERVER**

Table 19 lists the ports supported by a PathFinder Client functioning as a server.

**Table 19** *Ports Supported by PathFinder Client as Server*

<b>Port</b>	<b>Protocol/Use</b>	<b>Functionality</b>	<b>Direction</b>	<b>Result of Blocking Port on Firewall</b>	<b>Recipient Client or Server Type</b>
1719	RAS (UDP)	H.323 entity registration, admission and status communication	Client to PathFinder	H.323 endpoints cannot register to 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	Both	H.323 entities cannot set up calls through PathFinder.	H.323 entity

**PATHFINDER CLIENT  
AS CLIENT**

[Table 20](#) lists the ports supported by the PathFinder Client functioning as a client.

**Table 20** *Ports Supported by PathFinder Client as Client*

Port	Protocol/Use	Functionality	Direction	Result of Blocking Port on Firewall	Recipient Client or Server Type
3089	TCP and UDP	PathFinder tunneling service	PathFinder to Server	PathFinder Client cannot connect to the PathFinder Server. Legacy H.323 endpoints behind the PathFinder Client cannot call external endpoints.	PathFinder Server
3478	STUN (UDP)	STUN Binding Request	PathFinder to Server	PathFinder Client cannot determine its public IP address. Smart Direct Media Connect cannot function.	STUN server
1025-65535	TCP and UDP	H.323 Call Signaling, Call Control and Media Communication	Both	H.323 entities cannot set up calls through PathFinder.	H.323 entity

## SCOPIA DESKTOP

[Table 21](#) lists the ports that need to be opened between the SCOPIA Desktop Server and the internal network.

[Table 22](#) lists the ports that need to be opened between the SCOPIA Desktop Server and the public internet.

**Table 21** *Port Security—SCOPIA Desktop Server and Internal Network*

Protocol	Port Range	Severity	Purpose
TCP	80	Optional	GUI—The alternative is to configure the GUI to run on port 443.
TCP	8080	Optional	GUI access to iVIEW Suite web pages if iVIEW Suite is deployed on the same PC as SCOPIA Desktop.
TCP	443	Mandatory	Control connection between the SCOPIA Desktop Client and the SCOPIA Desktop Server.
TCP	3336	Mandatory	Meeting control connection between the SCOPIA Desktop Server and the SCOPIA MCU/iVIEW Suite.
TCP	3337	Mandatory	Meeting cascading connection between the SCOPIA Desktop Server and the SCOPIA MCU.
UDP	1025-65535	Mandatory	Media connection between the SCOPIA Desktop Server and the SCOPIA MCU. Also open these ports between the SCOPIA Desktop Server and the MVP.
UDP	1719	Mandatory	ECS Gatekeeper.
TCP	1025-65535	Mandatory	H.323 traffic between the SCOPIA Desktop Server and the SCOPIA MCU.

**Table 21** Port Security—SCOPIA Desktop Server and Internal Network

Protocol	Port Range	Severity	Purpose
UDP	1025-65535	Recommended	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.
UDP	6972-65535	Mandatory	Media connection between the SCOPIA Desktop Server and the SCOPIA Desktop Darwin server, if separated.
TCP	7070	Optional	Client-to-Server port for tunneled RTSP streaming.
UDP	2326-65535	Optional	<p>Limit UDP ports opened on the firewall to allow SCOPIA Desktop to send RTP to the internal network (MCU). We recommend that you use a limited range between 2326 and 65535. If this option is used:</p> <ul style="list-style-type: none"> <li>■ Each Client-to-SCOPIA Desktop connection uses 2 UDP ports.</li> <li>■ Each SCOPIA Desktop Server-to-MCU connection uses 6 UDP ports.</li> </ul> <p>Reserve 8 ports per user. To define the range, multiply the number of connections allowed by your license by 8.</p> <p>In addition, 6 UDP ports each are required for:</p> <ul style="list-style-type: none"> <li>■ every conference with SCOPIA Desktop users</li> <li>■ every recording channel.</li> </ul>

**Table 22** *Port Security—SCOPIA Desktop Server and Public Internet*

<b>Protocol</b>	<b>Port Range</b>	<b>Severity</b>	<b>Purpose</b>
TCP	80	Optional	GUI—The alternative is to configure the GUI to run on port 443.
TCP	8080	Optional	GUI access to an optional iVIEW Suite.
TCP	443	Mandatory	Control connection between the SCOPIA Desktop Client and Server.
UDP	1025-65535	Recommended	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.
TCP	7070	Mandatory	Client-to-Server port for tunneled RTSP streaming.
UDP	2326-65535	Optional	<p>Limit UDP ports opened on the firewall to allow conference clients to send RTP to SCOPIA Desktop. We recommend that you use a limited range between 2326 and 65535. If this option is used:</p> <ul style="list-style-type: none"> <li>■ Each Client-to-SCOPIA Desktop connection uses 2 UDP ports.</li> <li>■ Each SCOPIA Desktop Server-to-MCU connection uses 6 UDP ports.</li> </ul> <p>Reserve 8 ports per user. To define the range, multiply the number of connections allowed by your license by 8.</p>



[www.radvision.com](http://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](http://www.radvision.com)

---

USA/Americas  
T +1 201 689 6300  
F +1 201 689 6301  
[infoUSA@radvision.com](mailto:infoUSA@radvision.com)

EMEA  
T +44 20 3178 8685  
F +44 20 3178 5717  
[infoUK@radvision.com](mailto:infoUK@radvision.com)

APAC  
T +852 3472 4388  
F +852 2801 4071  
[infoAPAC@radvision.com](mailto:infoAPAC@radvision.com)