RADVISION®
an Avaya company

Port Security for Scopia Solution

Reference Guide

Version 8.2

For Solution 8.2

All product and company names herein may be trademarks of their registered owners.

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 Port Security for Scopia Solution Version 8.2, July 3, 2013

http://www.radvision.com

Table of Contents

Chapter 1: About Port Security in Video Networks

Chapter 2: Implementing Port Security for Scopia Management

Chapter 3: Implementing Port Security for the Scopia Elite MCU

Chapter 4: Implementing Port Security for Scopia Desktop

Chapter 5: Implementing Port Security for Scopia PathFinder

Chapter 6: Implementing Port Security for the Scopia Video Gateway and the Radvision SIP Gateway

Chapter 7: Implementing Port Security for Scopia ECS Gatekeeper

Chapter 8: Implementing Port Security for the Scopia XT Desktop Server

Chapter 9: Implementing Port Security for the Scopia XT Series

Chapter 10: Implementing Port Security for the Scopia VC240

Chapter 11: Implementing Port Security for the Scopia Gateway

Chapter 12: Implementing Port Security for the Scopia 3G Gateway

Chapter 13: Implementing Port Security for the Scopia MCU

Chapter 1 | About Port Security in Video Networks

This document provides the information you need to know to implement port security, including details of TCP/IP/UDP ports used throughout the SCOPIA Solution, organized by product name. To determine which ports you should open to enable optimal product functionality, see the port entries for the specific product. To maximize security, consult the procedures in each section that describe how to configure ports, limit port ranges, and configure security modes.

The various components of the SCOPIA Solution can be combined to fit the existing network topology and the video requirements of the organization. For more information, see the Deployments of the Scopia Solution section of the *Scopia Solution Guide*.

Each port entry includes the following information:

- **Port Range**: Specifies the TCP/IP/UDP port/port range.
- **Direction**: Specifies the direction of traffic through the port/port range, relative to the Scopia Solution product (in or out of the Scopia Solution product, or bidirectional).
- **Protocol**: Specifies the protocol used by the port/port range.
- **Destination**: Specifies the recipient (client or server) of the traffic.
- **Functionality**: Specifies the function of the port/port range.
- **Result of Blocking Port**: Specifies the system limitations that occur when this port/port range is blocked.
- **Required**: Specifies whether opening this port/port range is mandatory, recommended, or optional, relative to the standard usage of the Scopia Solution product. To obtain the functionality described for a particular port/port range, it is mandatory to open the particular port/port range.

Chapter 2 | Implementing Port Security for Scopia Management

Scopia Management is a set of management, control and scheduling applications that provide robust network management and easy-to-use conference scheduling.

Scopia Management is located in the enterprise (internal) network and is connected to the DMZ and public network via firewalls.

Scopia Management can connect to H.323 endpoints in public and partner networks via Scopia PathFinder, and to H.323 and SIP endpoints located in the enterprise network. For a list of TCP/IP/UDP ports supported by Scopia Management, see Ports to Open on Scopia Management on page 8.

Ports to Open on Scopia Management

Scopia Management is typically deployed in the enterprise network or the DMZ.

When opening ports to and from Scopia Management, use the following as a reference:

- For ports both to and from Scopia Management, see Table 1: Bidirectional Ports to Open on Scopia Management on page 9.
- For outbound ports from Scopia Management, see Table 2: Outbound Ports to Open from Scopia Management on page 10.
- For inbound ports into Scopia Management, see Table 3: Inbound Ports to Open on Scopia Management on page 13.

Important:

Choose the specific firewalls to open ports, depending on where your Scopia Management and other Scopia Solution products are deployed.

Table 1: Bidirectional Ports to Open on Scopia Management

Port Range	Protocol	Source/ Destination	Functionality	Result of Blocking Port	Required
23	Telnet (TCP)	Sony PCS address book, MCM, Endpoints	Enables you to use Sony PCS address book, retrieve element logs, and control MCM and endpoints.	Cannot use Sony PCS address book feature or retrieve logs from various devices (such as MCM).	Recommended
80	HTTP (TCP)	Web client	**In**: Provides access to the Scopia Management web user interface. When installed with the gatekeeper, this port defaults to 8080. **Out**: Provides access to the Scopia Management web user interface, TANDBERG MXP management (XML API via HTTP) and Scopia Elite MCU.	Cannot manage TANDBERG MXP and Scopia Elite MCU from the Scopia Management administrator portal.	Mandatory This can be configured during installation. For more information, see the How to Install Scopia Management in the *Installation Guide for Scopia Management*.
161	SNMP (UDP)	Any managed element	Enables SNMP configuration	Cannot operate the SNMP service with devices, and forward trap events do not function.	Mandatory
162	SNMP (UDP)	Any third-party SNMP manager	Enables sending SNMP trap events from any managed element	Cannot operate the SNMP service with devices, and forward trap events do not function.	Recommended
389	LDAP (TCP)	LDAP servers	Enables connection to LDAP servers	Cannot work with LDAP Servers	Mandatory for LDAP authentication
3342	SOCKS (TCP)	Scopia Management	Enables synchronization between multiple redundant Scopia Management installations	Cannot operate redundancy	Mandatory in deployments with a redundant Scopia Management server.
3346	XML(TLS)	Scopia Management	Enable secure XML Connection to Scopia Management	Cannot open secure XML connection to SScopia Management	Mandatory for any XML secure clients
5060	SIP (TCP/ UDP)	B2B/ Other SIP components	Enables SIP signaling	Cannot connect SIP calls	Mandatory

Port Range	Protocol	Source/ Destination	Functionality	Result of Blocking Port	Required
5061	SIP (TLS)	B2B/ Other SIP components	Enables secure SIP signaling	No TLS connection available	Mandatory
5432	TCP	Scopia Management	Enables master/slave data synchronization (used for Scopia Management redundant deployments with a PostgreSQL internal database)	Cannot synchronize data between the master and slave servers	Mandatory for redundancy deployments with a PostgreSQL internal database
7800-7802	UDP	Scopia Management	Enables master/slave data synchronization (used for Scopia Management redundant deployments)	Redundancy functionality is not available	Mandatory for redundancy deployments This can be configured during redundancy configuration. For more information, see the Configuring Redundancy Mode in the *Administrator Guide for Scopia Management*.
8011	HTTP (TCP)	Web client	Provides access to the internal ECS web user interface	Scopia Management client cannot access internal ECS web user interface	Mandatory for accessing the ECS web user interface

Table 2: Outbound Ports to Open from Scopia Management

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
7	Echo (TCP)	Video Network Devices	Detects online status of video network devices	Cannot detect online status of video network devices	Mandatory
21	FTP (TCP)	Scopia Management	Enables downloading logs from ECS or other devices that allow logs to be downloaded via FTP. Enables importing and exporting TANDBERG Local Address Book. Enables software upgrade.	Cannot download logs from ECS or from other devices via FTP, import or export TANDBERG Local Address Book, or perform software upgrades.	Mandatory

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
22	SSH (TCP)	Scopia Management	Detects LifeSize endpoints. Enables downloading Scopia PathFinder Server logs. Detects and manages Scopia VC240.	Cannot detect LifeSize endpoints, download Scopia PathFinder Server logs, or detect/ manage Scopia VC240	Mandatory
24	Telnet (TCP)	Polycom endpoints	Enables you to control Polycom endpoints	Cannot control Polycom endpoints	Optional
25	SMTP (TCP)	SMTP server	Enables connection to SMTP server for sending email notifications	Cannot send email notifications	Mandatory
53	DNS (UDP)	DNS server	Enables DNS queries	Cannot parse domain names	Mandatory
445	NTLM (TCP/UDP)	Active Directory Server	Enables connection to the Active Directory Server	NTLM SSO does not function	Mandatory
636	LDAP over SSL	Directory Server	Enables connection to the Directory Server	Cannot connect to the Directory Server	Mandatory
3089	TCP	Scopia PathFinder	Detects endpoints via Scopia PathFinder	Cannot detect endpoints via Scopia PathFinder	Mandatory
3336	XML (TCP)	Scopia Video Gateway/ SIP Gateway/ MCU	Enables connection to the Scopia Video Gateway/ SIP Gateway/ MCU via the moderator's XML API (used for managing meetings via Scopia Management)	Cannot connect to the Scopia Video Gateway/ SIP Gateway/ MCU via the XML API	Mandatory if deployed with Scopia Video Gateway/ SIP Gateway/ MCU
3338	XML (TCP)	Scopia Video Gateway/ SIP Gateway	Enables connection to Scopia Video Gateway/ SIP Gateway via the administrator's XML API (used for configuring devices via Scopia Management)	Cannot perform configuration for Scopia Video Gateway/ SIP Gateway via the XML API	Mandatory if deployed with Scopia Video Gateway/ SIP Gateway
3339	XML (TCP)	B2B	Enables you to use the Scopia Management XML API	Cannot communicate with the B2BUA component via Scopia Management XML API	Mandatory
3340	TCP/TLS	Scopia Desktop	Enables connection to Scopia Desktop	Scopia Desktop cannot use Scopia Management to place or manage calls	Mandatory if deployed with Scopia Desktop

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3346	XML (TLS)	Scopia Video Gateway/ SIP Gateway	Enables secure connection to the Scopia Video Gateway/ SIP Gateway via the moderator's XML API (used for managing meetings via Scopia Management)	Cannot securely connect to the Scopia Video Gateway/ SIP Gateway/ MCU via the XML API	Mandatory for a secure XML API connection with Scopia Video Gateway/ SIP Gateway
3348	XML (TLS)	Scopia Video Gateway/ SIP Gateway	Enables secure connection to Scopia Video Gateway/ SIP Gateway via the administrator's XML API (used for configuring devices via Scopia Management)	Cannot securely connect to the Scopia Video Gateway/ SIP Gateway/ MCU via the administrator's XML API	Mandatory for a secure XML API connection with Scopia Video Gateway/ SIP Gateway
8089	XML (TCP)	Scopia PathFinder Server	Enables connection to Scopia PathFinder Server (v7.0 and later) via Scopia PathFinder Server XML API	Cannot connect to Scopia PathFinder Server via Scopia PathFinder Server XML API	Optional
50000	Telnet (TCP)	Sony endpoints	Enables you to control Sony endpoints	Cannot control Sony endpoints	Optional
55003	TCP	Scopia XT1000	Enables connection to the Scopia XT1000	Cannot connect to the Scopia XT1000	Mandatory if deployed with Scopia XT1000
63148	DIIOP (TCP)	Domino server	Enables connection with the Domino server	Cannot connect to the Domino Server	Mandatory if Scopia Management works with Domino Server

Table 3: Inbound Ports to Open on Scopia Management

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
443	HTTPS (TCP)	Web client	Enables Tomcat to run over SSL	Cannot access Scopia Management web user interface via HTTPS	Mandatory if using HTTPS
3341	TCP	IBM Sametime	Enables connection to IBM Sametime application	Cannot work with IBM Sametime	Mandatory if Scopia Management works with IBM Sametime
8080	HTTP (TCP)	Web client	Provides access to the Scopia PathFinder and Scopia Management web user interface	Cannot access the Scopia PathFinder web user interface	Mandatory if deployed with Scopia PathFinder or Scopia Management internal Gatekeeper. This can be configured during installation. For more information, see the How to Install Scopia Management in the *Installation Guide for Scopia Management*.

Chapter 3 | Implementing Port Security for the Scopia Elite MCU

The Scopia Elite MCU is a hardware unit that houses videoconferences from multiple endpoints, both H.323 and SIP.

This section details the ports used for the Scopia Elite 6000 Series MCU and Scopia Elite 5000 Series MCU, and the relevant configuration procedures:

Navigation

Ports to Open for the Scopia Elite 6000 Series MCU

The Scopia Elite 6000 Series MCU is typically located in the enterprise network and is connected to the DMZ. When opening ports on the Scopia Elite MCU, use the following as a reference:

- If you are opening ports that are both in and out of the Scopia Elite 6000 Series MCU, see Table 4: Bidirectional Ports to Open on the Scopia Elite 6000 Series MCU on page 15.
- If you are opening ports inbound to the Scopia Elite 6000 Series MCU, see Table 5: Inbound Ports to Open to the Scopia Elite 6000 Series MCU on page 16.

Important:

The specific firewalls you need to open ports on depends on where your MCU and other Scopia Solution products are deployed.

Table 4: Bidirectional Ports to Open on the Scopia Elite 6000 Series MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
1024-1324	H.245 (TCP)	Any H.323 device	Enables H.245 signaling	Cannot connect H.323 calls	Mandatory To configure, see Configuring the TCP Port Range for H.245 on the Scopia Elite MCU on page 23
1719	RAS (UDP)	H.323 gatekeeper	Enables RAS signaling	Cannot communicate with H.323 gatekeeper	Mandatory To configure, see Configuring the UDP Port for RAS on the Scopia Elite MCU on page 25 and Configuring the UDP Port for the Gatekeeper on the Scopia Elite MCU on page 26
1720	Q.931 (TCP)	Any H.323 device	Enables Q.931 signaling	Cannot connect H.323 calls	Mandatory To configure, see Configuring the TCP Port Q.931 on the Scopia Elite MCU on page 27
3336	XML (TCP)	Conference Control web client endpoint, Scopia Management, or third-party controlling applications	Enables you to manage the MCU via the XML API	Cannot use MCU Conference Control web user interface. Cannot use XML API to control MCU.	Mandatory if deployed with Scopia Management
3337	XML (TCP)	Other MCUs	Enables use of MCU Cascading XML API	Cannot cascade between two MCUs	Mandatory if multiple MCUs are deployed with Scopia Management
3338	XML (TCP)	Scopia Management, or third-party configuration applications	Enables you to configure the MCU via the XML API	Cannot configure MCU via the XML API	Mandatory if deployed with Scopia Management
3400-3580	SIP BFCP (TCP)	Any SIP video network device	Enables SIP content sharing	Cannot share SIP contents	Mandatory if using content sharing with SIP over TCP To configure, see Configuring the TCP Port Range for SIP BFCP on the Scopia Elite MCU on page 29

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
5060	SIP (TCP/ UDP)	Any SIP video network device	Enables SIP signaling	Cannot connect SIP calls	Mandatory if using SIP over TCP/ UDP To configure, see Configuring the TCP/UDP/TLS Port for SIP on the Scopia Elite MCU on page 28
5061	SIP (TLS)	Any SIP video network device	Enables secure SIP signaling	Cannot connect SIP calls over TLS	Mandatory if using SIP over TLS To configure, see Configuring the TCP/UDP/TLS Port for SIP on the Scopia Elite MCU on page 28
12000-13200 16384-16984	RTP/ RTCP/ SRTP (UDP)	Any H.323 or SIP media-enabled video network device	Enables real-time delivery of video and audio media	Cannot transmit/ receive video media streams	Mandatory To configure, see Configuring the UDP Port Ranges for RTP/RTCP on the Scopia Elite MCU on page 22

Table 5: Inbound Ports to Open to the Scopia Elite 6000 Series MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
21	FTP (TCP)	FTP Server	Enables audio stream recording	Cannot record audio streams	Optional
22	SSH (TCP)	SSH Client	Enables you to view logs	Cannot view logs in real-time (logs are collected on the compact flash card)	Optional
80	HTTP (TCP)	Web client	Provides access to the MCU Administrator and Conference Control web user interfaces; used for software upgrade	Cannot configure MCU	Mandatory if using HTTP To configure, see Configuring the HTTP Port on the Scopia Elite MCU on page 24
443	HTTPS (HTTP over SSL)	Web client	Provides secure access to the MCU Administrator and Conference Control web user interfaces; used for software upgrade	Cannot configure MCU	Mandatory if using HTTPS

Ports to Open for the Scopia Elite 5100 Series MCU

The Scopia Elite 5100 Series MCU is typically located in the enterprise network and is connected to the DMZ. When opening ports on the Scopia Elite 5100 Series MCU, use the following as a reference:

- If you are opening ports that are both in and out of the Scopia Elite 5100 Series MCU, see Table 6: Bidirectional Ports to Open on the Scopia Elite 5100 Series MCU on page 17.
- If you are opening ports outbound from the Scopia Elite 5100 Series MCU, see Table 7: Outbound Ports to Open from the Scopia Elite 5100 Series MCU on page 18.
- If you are opening ports inbound to the Scopia Elite 5100 Series MCU, see Table 8: Inbound Ports to Open to the Scopia Elite 5100 Series MCU on page 19.

Important:

The specific firewalls you need to open ports on depends on where your MCU and other Scopia Solution products are deployed.

Table 6: Bidirectional Ports to Open on the Scopia Elite 5100 Series MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
1024-1324	H.245 (TCP)	Any H.323 device	Enables H.245 signaling	Cannot connect H.323 calls	Mandatory To configure, see Configuring the TCP Port Range for H.245 on the Scopia Elite MCU on page 23
1719	RAS (UDP)	H.323 gatekeeper	Enables RAS signaling	Cannot communicate with H.323 gatekeeper	Mandatory To configure, see Configuring the UDP Port for RAS on the Scopia Elite MCU on page 25 and Configuring the UDP Port for the Gatekeeper on the Scopia Elite MCU on page 26.
1720	Q.931 (TCP)	Any H.323 device	Enables Q.931 signaling	Cannot connect H.323 calls	Mandatory To configure, see Configuring the TCP Port Q.931 on the Scopia Elite MCU on page 27.

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3336	XML (TCP)	Conference Control web client endpoint, Scopia Management, or third-party controlling applications	Enables you to manage the MCU via the XML API	Cannot use MCU Conference Control web user interface. Cannot use XML API to control MCU.	Mandatory if deployed with Scopia Management
3337	XML (TCP)	Other MCUs	Enables use of MCU Cascading XML API	Cannot cascade between two MCUs	Mandatory if multiple MCUs are deployed with Scopia Management
3338	XML (TCP)	Scopia Management, or third-party configuration applications	Enables you to configure the MCU via the XML API	Cannot configure MCU via the XML API	Mandatory if deployed with Scopia Management
5060	SIP (TCP/ UDP)	Any SIP video network device	Enables SIP signaling	Cannot connect SIP calls	Mandatory if using SIP over TCP/ UDP To configure, see Configuring the TCP/UDP/TLS Port for SIP on the Scopia Elite MCU on page 28.
5061	SIP (TLS)	Any SIP video network device	Enables secure SIP signaling	Cannot connect SIP calls over TLS	Mandatory if using SIP over TLS To configure, see Configuring the TCP/UDP/TLS Port for SIP on the Scopia Elite MCU on page 28.
12000-13200 16384-16984	RTP/ RTCP/ SRTP (UDP)	Any H.323 or SIP media-enabled video network device	Enables real-time delivery of video and audio media	Cannot transmit/ receive video media streams	Mandatory To configure, see Configuring the UDP Port Ranges for RTP/RTCP on the Scopia Elite MCU on page 22.

Table 7: Outbound Ports to Open from the Scopia Elite 5100 Series MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
162	SNMP (UDP)	Scopia Management or any SNMP manager station	Enables sending SNMP Trap events	Cannot send SNMP Traps	Recommended

Table 8: Inbound Ports to Open to the Scopia Elite 5100 Series MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
21	FTP (TCP)	FTP Server	Enables audio stream recording	Cannot record audio streams	Optional
22	SSH (TCP)	SSH Client	Enables you to view logs	Cannot view logs in real-time (logs are collected on the compact flash card)	Optional
80	HTTP (TCP)	Web client	Provides access to the MCU Administrator and Conference Control web user interfaces; used for software upgrade	Cannot configure MCU	Mandatory if using HTTP To configure, see Configuring the HTTP Port on the Scopia Elite MCU on page 24.
161	SNMP (UDP)	Scopia Management or any SNMP manager station	Enables you to configure and check the MCU status	Cannot configure or check the MCU status	Recommended
443	HTTPS (HTTP over SSL)	Web client	Provides secure access to the MCU Administrator and Conference Control web user interfaces; used for software upgrade	Cannot configure MCU	Mandatory if using HTTPS

Ports to Open on the Scopia Elite 5200 Series MCU

The Scopia Elite 5200 Series MCU is typically located in the enterprise network and is connected to the DMZ. When opening ports on the Scopia Elite 5200 Series MCU, use the following as a reference:

- If you are opening ports that are both in and out of the Scopia Elite 5200 Series MCU, see Table 9: Bidirectional Ports to Open on the Scopia Elite 5200 Series MCU on page 20.
- If you are opening ports outbound from the Scopia Elite 5200 Series MCU, see Table 10: Outbound Ports to Open from the Scopia Elite 5200 Series MCU on page 21.
- If you are opening ports inbound to the Scopia Elite 5200 Series MCU, see Table 11: Inbound Ports to Open to the Scopia Elite 5200 Series MCU on page 22.

Important:

The specific firewalls you need to open ports on depends on where your Scopia Elite MCU and other Scopia Solution products are deployed.

Table 9: Bidirectional Ports to Open on the Scopia Elite 5200 Series MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
1024-1324	H.245 (TCP)	Any H.323 device	Enables H.245 signaling	Cannot connect H.323 calls	Mandatory To configure, see Configuring the TCP Port Range for H.245 on the Scopia Elite MCU on page 23.
1719	RAS (UDP)	H.323 gatekeeper	Enables RAS signaling	Cannot communicate with H.323 gatekeeper	Mandatory To configure, see Configuring the UDP Port for RAS on the Scopia Elite MCU on page 25 and Configuring the UDP Port for the Gatekeeper on the Scopia Elite MCU on page 26.
1720	Q.931 (TCP)	Any H.323 device	Enables Q.931 signaling	Cannot connect H.323 calls	Mandatory To configure, see Configuring the TCP Port Q.931 on the Scopia Elite MCU on page 27.
3336	XML (TCP)	Conference Control web client endpoint, Scopia Management, or third-party controlling applications	Enables you to manage the MCU via the XML API	Cannot use MCU Conference Control web user interface. Cannot use XML API to control MCU.	Mandatory if deployed with Scopia Management
3337	XML (TCP)	Other MCUs	Enables use of MCU Cascading XML API	Cannot cascade between two MCUs	Mandatory if multiple MCUs are deployed with Scopia Management
3338	XML (TCP)	Scopia Management, or third-party configuration applications	Enables you to configure the MCU via the XML API	Cannot configure MCU via the XML API	Mandatory if deployed with Scopia Management

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
5060	SIP (TCP/ UDP)	Any SIP video network device	Enables SIP signaling	Cannot connect SIP calls	Mandatory if using SIP over TCP/ UDP To configure, see Configuring the TCP/UDP/TLS Port for SIP on the Scopia Elite MCU on page 28.
5061	SIP (TLS)	Any SIP video network device	Enables secure SIP signaling	Cannot connect SIP calls over TLS	Mandatory if using SIP over TLS To configure, see Configuring the UDP Port Ranges for RTP/ RTCP on the Scopia Elite MCU on page 22.
12000-13200	RTP/ RTCP (UDP)	Any RTP/RTCP media- enabled video network device	Enables real-time delivery of video media (lower blade only)	Cannot transmit /receive video media streams	Mandatory To configure, see Configuring the UDP Port Ranges for RTP/ RTCP on the Scopia Elite MCU on page 22.
16384-16984	RTP/ RTCP (UDP)	Any H.323 or SIP media-enabled video network device	Enables real-time delivery of audio media (upper blade only)	Cannot transmit /receive audio media streams	Mandatory To configure, see Configuring the UDP Port Ranges for RTP/ RTCP on the Scopia Elite MCU on page 22.

Table 10: Outbound Ports to Open from the Scopia Elite 5200 Series MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
162	SNMP (UDP)	Scopia Management, or any SNMP manager station	Enables sending SNMP Trap events	Cannot send SNMP Traps	Recommended

Table 11: Inbound Ports to Open to the Scopia Elite 5200 Series MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
21	FTP (TCP)	FTP Server	Enables audio stream recording	Cannot record audio streams	Optional
22	SSH (TCP)	SSH Client	Enables you to view logs	Cannot view logs in real-time (logs are collected on the compact flash card)	Optional
80	HTTP (TCP)	Web client	Provides access to the MCU Administrator and Conference Control web user interfaces; used for software upgrade	Cannot configure MCU	Mandatory if using HTTP To configure, see Configuring the HTTP Port on the Scopia Elite MCU on page 24.
161	SNMP (UDP)	Scopia Management, or any SNMP manager station	Enables you to configure and check the MCU status	Cannot configure or check the MCU status	Recommended
443	HTTPS (HTTP over SSL)	Web client	Provides secure access to the MCU Administrator and Conference Control web user interfaces; used for software upgrade	Cannot configure MCU	Mandatory if using HTTPS

Configuring Ports on All Models of the Scopia Elite MCU

This section provides instructions of how to configure the following ports and port ranges on all models of the Scopia Elite MCU:

Navigation

- Configuring the UDP Port Ranges for RTP/RTCP on the Scopia Elite MCU on page 22
- Configuring the TCP Port Range for H.245 on the Scopia Elite MCU on page 23
- Configuring the HTTP Port on the Scopia Elite MCU on page 24
- Configuring the UDP Port for RAS on the Scopia Elite MCU on page 25
- Configuring the UDP Port for the Gatekeeper on the Scopia Elite MCU on page 26
- Configuring the TCP Port Q.931 on the Scopia Elite MCU on page 27
- Configuring the TCP/UDP/TLS Port for SIP on the Scopia Elite MCU on page 28
- Configuring the TCP Port Range for SIP BFCP on the Scopia Elite MCU on page 29

Configuring the UDP Port Ranges for RTP/RTCP on the Scopia Elite MCU

About this task

The Scopia Elite 6000 Series MCU has designated UDP ports 12000-13200 (for video) and 16384-16984 (for audio) for RTP/RTCP.

While the number of ports required for this protocol remain fixed, you can determine the exact port numbers occupied by the MCU by defining the lower end of the port range, known as the base port.

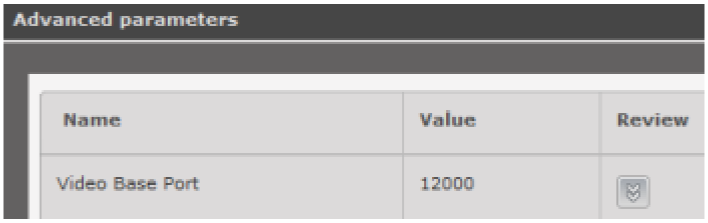
The Scopia Elite 6000 Series MCU uses 360 ports for audio and 1080 ports for video.

Important:

You cannot reduce the number of UDP ports occupied by the MCU for RTP/RTCP.

Procedure

1. Navigate to the MCU **Advanced Commands** section by doing the following:
   a. Select the 🛠 icon.
   b. Select **Advanced parameters**.
   c. Locate **Video Base Port** or the **Audio Base Port** entry in the **Name** column to change the video or audio port values respectively (see Figure 1: Defining the base port for video on page 23).



Advanced parameters

Name	Value	Review
Video Base Port	12000	⏬

Figure 1: Defining the base port for video

2. Select the ⏬ icon in the **Review** column.
3. Enter the new lower end port value in the field.
4. Select **Apply**.
5. Select **Close**.

Configuring the TCP Port Range for H.245 on the Scopia Elite MCU

About this task

The Scopia Elite 6000 Series MCU has designated TCP ports 1024-1324 for H.245. You can set the base port, which is the lower end of the port range. H.245 is a Control Protocol used for multimedia communication that enables transferring information about the device capabilities, as well as opening/closing the logical channels that carry media streams.

The Scopia Elite 6000 Series MCU uses 300 ports.

Procedure

1. Navigate to the MCU **Advanced Commands** section by doing the following:

   a. Select the 🛠 icon.

   b. Select **Advanced parameters**.

   c. Locate the **CLI** section and select **More** (see Figure 2: CLI Section on page 24).

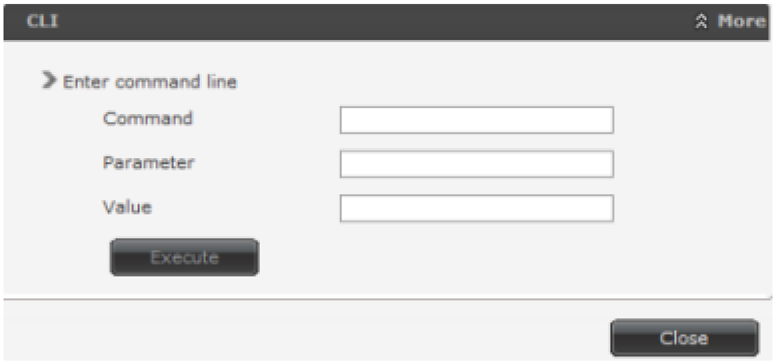


Figure 2: CLI Section

2. Enter the **h245baseport** command in the **Command** field.

   Important:

   To see the current port value, select **Execute**.

3. Modify the port value in the **Value** field.

4. Select **Execute**.

5. Select **Close.**

Configuring the HTTP Port on the Scopia Elite MCU

About this task

The Scopia Elite 6000 Series MCU has designated port 80 for HTTP. You can configure a different port to use HTTP if necessary in your environment.

Procedure

1. Navigate to the MCU **Advanced Commands** section by doing the following:

   a. Select the 🛠 icon.

   b. Select **Advanced parameters**.

c. Locate the **CLI** section and select **More** (see Figure 3: CLI Section on page 25).

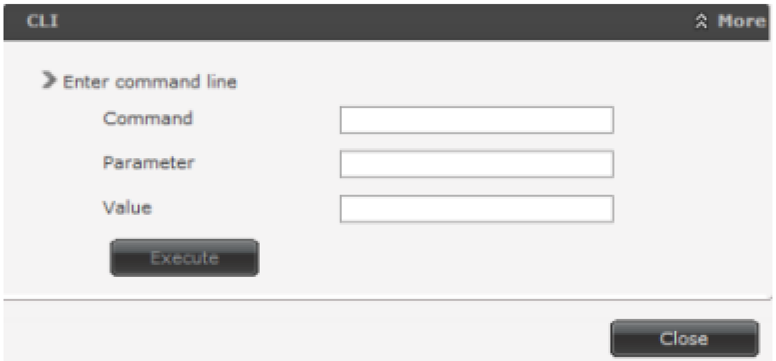


Figure 3: CLI Section

2. Enter the **webserverport** command in the **Command** field.

   Important:

   To see the current port value, select **Execute**.

3. Enter the port value in the **Value** field.
4. Select **Execute**.

   Important:

   After selecting **Execute**, a warning message appears, notifying you that the unit will be reset and any active conferences will be disconnected.

5. Select **Yes** to continue.
6. Select **Close.**

   Important:

   After applying the new port value, you must enter it as a suffix to the MCU IP address in order to access the web server.

   For example, if your new HTTP port value is 8080, access the web server by entering *http://<URL>:8080*

Configuring the UDP Port for RAS on the Scopia Elite MCU

About this task

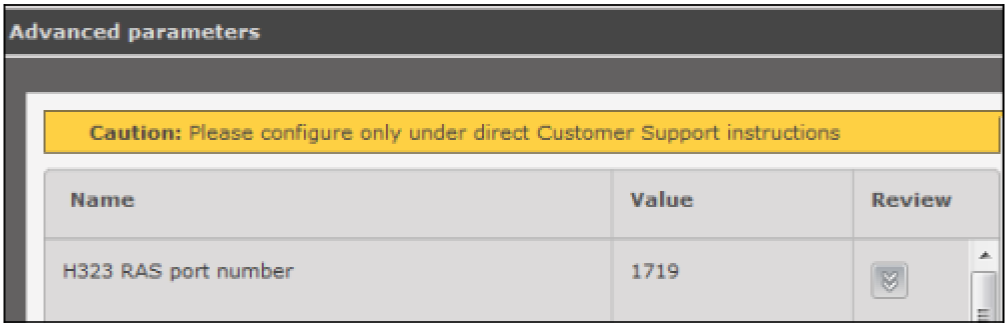
The Scopia Elite 6000 Series MCU has designated port 1719 for RAS. You can configure a different port to use RAS (for example, if port 1719 is busy). Port 1719 is also used to communicate with the gatekeeper (to configure the UDP port for the gatekeeper, see Configuring the UDP Port for the Gatekeeper on the Scopia Elite MCU on page 26).

Important:

If you close port 1719, you must configure another port for both RAS and the gatekeeper. If you configure a different port for RAS, you do not need to configure a different port for the gatekeeper.

Procedure

1. Navigate to the MCU **Advanced Commands** section by doing the following:
   a. Select the 🛠 ▾ icon.
   b. Select **Advanced parameters**.
   c. Locate the **H323 RAS port number** in the **Name** column (see Figure 4: RAS Port Configuration on page 26).



Advanced parameters

Caution: Please configure only under direct Customer Support instructions

Name	Value	Review
H323 RAS port number	1719	⌄

Figure 4: RAS Port Configuration

2. Select the ⌄ icon in the **Review** column.
3. Enter the port value in the **H323 RAS port number** field.
4. Select **Apply**.
5. Select **Close.**

Configuring the UDP Port for the Gatekeeper on the Scopia Elite MCU

About this task

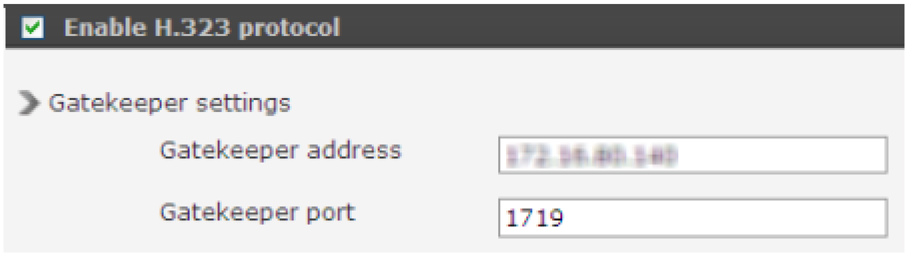
The Scopia Elite 6000 Series MCU has designated port 1719 for gatekeeper use. You can configure a different port to enable communication with the gatekeeper (for example, if port 1719 is busy). Port 1719 is also used for RAS (to configure the UDP port for RAS, see Configuring the UDP Port for RAS on the Scopia Elite MCU on page 25).

Important:

If you close port 1719, you must configure another port for both the gatekeeper and RAS. If you configure a different port for the gatekeeper, you do not need to configure a different port for RAS.

Procedure

1. Navigate to the MCU **H.323 Protocol** section by selecting **Configuration > Protocols**.
2. Locate the **Enable H.323 protocol** section (see Figure 5: H.323 Protocol section of the Protocols tab on page 27).



☑ Enable H.323 protocol

Gatekeeper settings

Gatekeeper address: [redacted]

Gatekeeper port: 1719

Figure 5: H.323 Protocol section of the Protocols tab

3. Enter the port value in the **Gatekeeper port** field.
4. Select **Apply**.

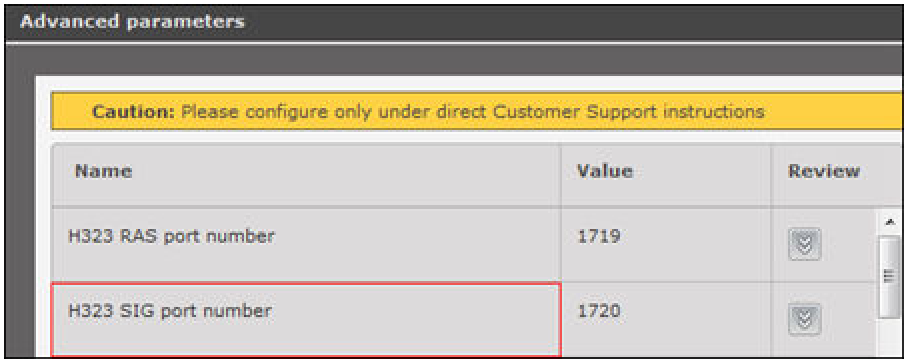
Configuring the TCP Port Q.931 on the Scopia Elite MCU

About this task

The Scopia Elite 6000 Series MCU has designated port 1720 for Q.931. You can configure a different port to use Q.931 (for example, if port 1720 is busy). Q.931 is a telephony protocol used for establishing and terminating the connections in H.323 calls.

Procedure

1. Navigate to the MCU **Advanced Commands** section by doing the following:
   a. Select the 🛠 icon.
   b. Select **Advanced parameters**.
   c. Locate the **H323 SIG port number** in the **Name** column (see Figure 6: H.323 Signaling Port Configuration on page 28).



Advanced parameters

Caution: Please configure only under direct Customer Support instructions

Name	Value	Review
H323 RAS port number	1719	⌄
H323 SIG port number	1720	⌄

Figure 6: H.323 Signaling Port Configuration

2. Select the ⌄ icon in the **Review** column.
3. Enter the port value in the **H323 SIG port number** field.
4. Select **Apply**.
5. Select **Close.**

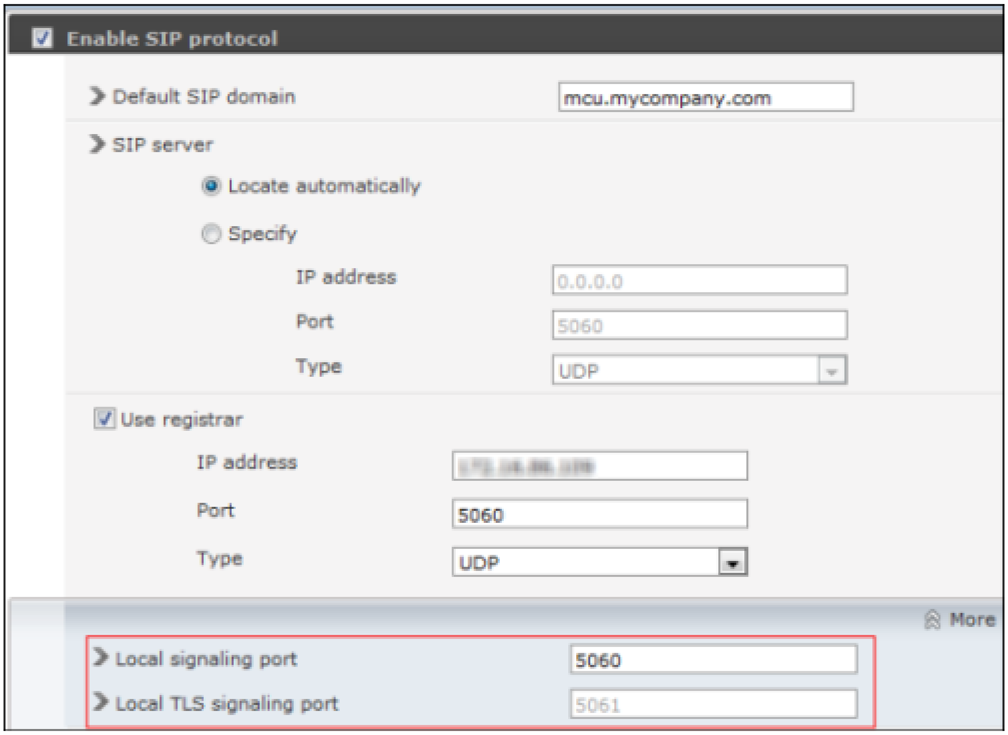
Configuring the TCP/UDP/TLS Port for SIP on the Scopia Elite MCU

About this task

The Scopia Elite 6000 Series MCU has designated ports 5060 and 5061 for SIP. You can configure a different port to use SIP (for example, if port 5060 or 5061 is busy).

Procedure

1. Navigate to the MCU **SIP Protocol** section by selecting **Configuration > Protocols**.
2. Locate the **Enable SIP protocol** section and select **More** (see Figure 7: SIP Port Configuration on page 29).



☑ Enable SIP protocol

Default SIP domain: mcu.mycompany.com

SIP server

● Locate automatically

○ Specify

IP address: 0.0.0.0

Port: 5060

Type: UDP

☑ Use registrar

IP address: [redacted]

Port: 5060

Type: UDP

Local signaling port: 5060

Local TLS signaling port: 5061

Figure 7: SIP Port Configuration

3. Do one of the following:
   - If your SIP server or Registrar is not configured with TLS, enter the port value in the **Local signaling port** field.
   - If your SIP server or Registrar is configured with TLS, enter the port value in the **Local TLS signaling port** field.

     Important:

     If your SIP server or Registrar is configured with TLS, you can also configure the port value for TCP/UDP traffic by modifying the **Local signaling port** field.
4. Select **Apply**.

Configuring the TCP Port Range for SIP BFCP on the Scopia Elite MCU

About this task

The Scopia Elite 6000 Series MCU has designated TCP ports 3400-3580 for SIP BFCP.

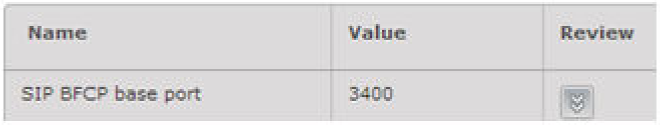
While the number of ports required for this protocol remain fixed, you can determine the exact port numbers occupied by the MCU by defining the lower end of the port range, known as the base port.

Procedure

Navigate to the MCU **Advanced Commands** section by doing the following:

a. Select the icon.

b. Locate **SIP BFC Base Port** entry in the **Name** column to change the port value (see Figure 8: Defining the base port for SIP BFCP on page 30).



Name	Value	Review
SIP BFCP base port	3400	⌄

Figure 8: Defining the base port for SIP BFCP

c. Select the icon in the **Review** column.

d. Enter the new lower end port value in the field.

e. Select **Apply**.

f. Select **Close**.

Configuring Security Access Levels for the Scopia Elite MCU

About this task

The Scopia Elite MCU offers configurable security access levels that enable and disable SSH, FTP, SNMP and ICMP (ping) protocols.

By default, the security access level is set to **High**. It is recommended to set your security access level to **Maximum** (which disables these protocols), except for the following situations:

- If you are performing either debugging or troubleshooting operations, SSH should be enabled.
- If you are customizing your language settings, FTP should be enabled.
- If you would like control or error response messages to be sent, ICMP (ping) should be enabled.
- If you are performing configuration procedures or would like to receive traps, SNMP should be enabled.

Important:

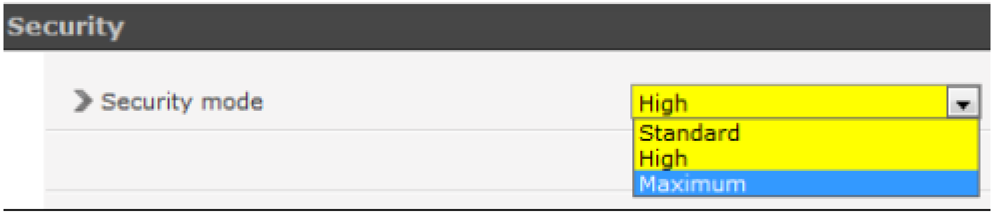
You can view trap events in the **Events** tab of the web user interface.

Important:

Using encryption is subject to local regulation. In some countries it is restricted or limited for usage. For more information, consult your local reseller.

Procedure

1. Access the MCU security settings by selecting **Configuration** > **Setup**.
2. Locate the **Security** section.
3. Select the access level from the **Security Mode** list (see Figure 9: Security Access Level Settings on page 31). Table 12: MCU Security Access Levels on page 31 lists the protocol status when each security access level is applied.



Security

Security mode: High

Figure 9: Security Access Level Settings

Table 12: MCU Security Access Levels

Security Access Level	SSH	FTP	SNMP	ICMP (ping)
Standard	Enabled	Enabled	Enabled	Enabled
High	Disabled	Disabled	Enabled	Enabled
Maximum	Disabled	Disabled	Disabled	Disabled

4. Select **Apply.**

Chapter 4 | Implementing Port Security for Scopia Desktop

Scopia Desktop is a software based endpoint, a client/server application that extends a room system conferencing application to remote and desktop users for voice, video and data communications. The system provides automatic firewall traversal to allow anyone to participate, regardless of where they are.

This section details the ports used for the Scopia Desktop Server and Scopia Desktop clients, and the relevant port configuration procedures:

Navigation

- Ports to Open on Scopia Desktop on page 32
- Limiting Port Ranges on the Scopia Desktop Server on page 39

Ports to Open on Scopia Desktop

The Scopia Desktop Server is typically located in the DMZ (see Figure 10: Locating the Scopia Desktop Server in the DMZ on page 33) and is therefore connected to both the enterprise and the public networks. Scopia Desktop Clients can be located in the internal enterprise network, in the public network, or in a partner network.

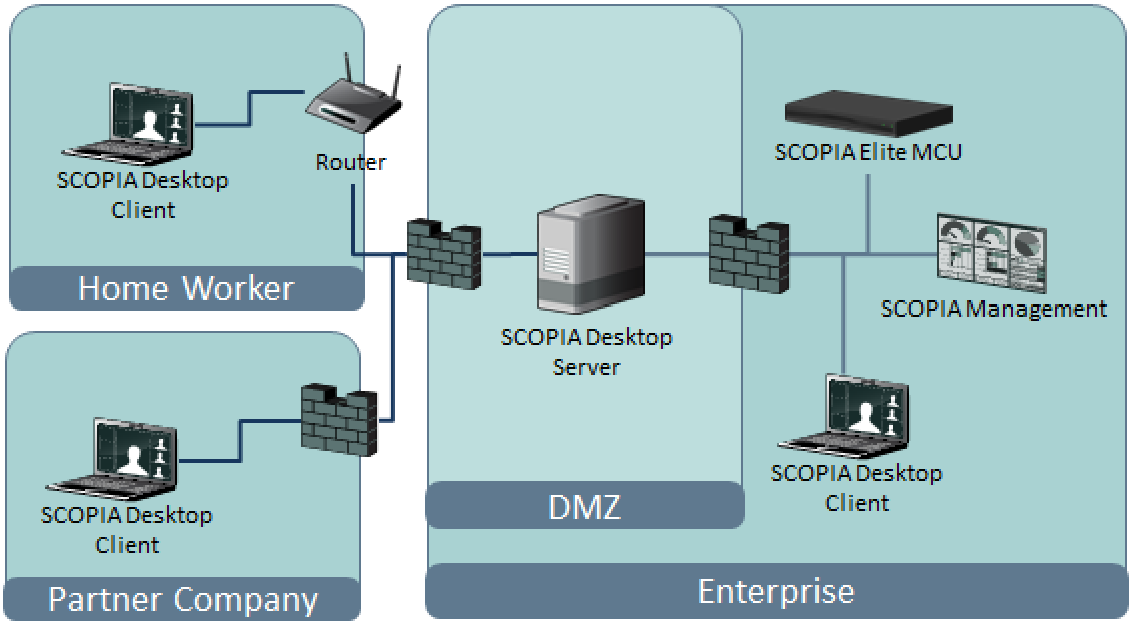


Figure 10: Locating the Scopia Desktop Server in the DMZ

When opening ports between the DMZ and the enterprise on the Scopia Desktop Server, use the following as a reference:

- When opening ports that are both in and out of the Scopia Desktop Server, see Table 13: Bidirectional Ports to Open Between the Scopia Desktop Server and the Enterprise on page 34.
- When opening ports that are outbound from the Scopia Desktop Server, see Table 14: Outbound Ports to Open from the Scopia Desktop Server to the Enterprise on page 34.
- When opening ports that are inbound to the Scopia Desktop Server, see Table 15: Inbound Ports to Open from the Enterprise to the Scopia Desktop Server on page 36.

When opening ports between the DMZ and the public on the Scopia Desktop Server, use the following as a reference:

- When opening ports that are both in and out of the Scopia Desktop Server, see Table 16: Bidirectional Ports to Open Between the Scopia Desktop Server and the Public on page 36.
- When opening ports that are inbound from the Scopia Desktop Server, see Table 17: Inbound Ports to Open from the Public to the Scopia Desktop Server on page 37.

When opening ports to and from the XMPP server (which is necessary when the XMPP server is separated by a firewall from the Scopia Desktop Server), use the following as a reference:

- When opening outbound ports from the XMPP server, see Table 18: Outbound Ports to Open from the XMPP Server on page 37.
- When opening inbound ports to the XMPP server, see Table 19: Inbound Ports to Open on the XMPP Server on page 38.

When opening bidirectional ports between Scopia Desktop Clients, see Table 20: Bidirectional Ports to Open Between Scopia Desktop Clients on page 38.

When opening inbound ports from the Scopia Desktop Clients to the STUN server, see Table 21: Inbound Ports to Open from the Scopia Desktop Client to the STUN Server on page 38.

Important:

The specific firewalls you need to open ports on depends on where your Scopia Desktop and other Scopia Solution products are deployed.

Table 13: Bidirectional Ports to Open Between the Scopia Desktop Server and the Enterprise

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
7640	TCP	Content Center Server	Enables connection between the Scopia Desktop Server and the Content Center Server, when installed on different servers.	Cannot communicate with the Content Center Server and some capabilities (such as recording and streaming) do not function properly	Mandatory
1024- 65535	TCP (H.245/ Q.931)	MCU or ECS, depending on deployment	Enables connection to Scopia Desktop meetings.	Cannot connect to the meeting	Mandatory To limit range, see Limiting the TCP Port Range for H.245/Q.931 on the Scopia Desktop Server on page 40
10000-65535	UDP (RTP)	MCU or Scopia Desktop Client	Enables media connection to the MCU, and the Scopia Desktop Client or Scopia Mobile.	Media cannot be passed from the MCU to Scopia Desktop Clients. Also, connection is tunneled via TCP port 443 resulting in a drop in performance.	Mandatory To limit range, see Limiting the UDP Port Range for RTP/RTCP on the Scopia Desktop Server on page 39

Table 14: Outbound Ports to Open from the Scopia Desktop Server to the Enterprise

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
137,138	UDP	Active Directory	Enables auto-discovery and authentication	Cannot perform auto-discovery and authentication	Recommended for performing Active Directory authentication
139,445	TCP	Active Directory	Enables auto-discovery and authentication	Cannot perform auto-discovery and authentication	Recommended for Active Directory authentication

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
1719	UDP (RAS)	Scopia ECS Gatekeeper or the internal gatekeeper in Scopia Management	Enables communication with Scopia ECS Gatekeeper or the internal gatekeeper in Scopia Management	Cannot connect to the meeting	Mandatory
1720	TCP	MCU or ECS, depending on deployment	Enables connection to Scopia Desktop meetings.	Cannot connect to the meeting	Mandatory
3337	TCP (XML)	MCU	Enables meeting cascading connection to the	Meeting cascading connection is disabled	Mandatory
5269	TCP	XMPP Server	Enables sever-to-server connections in cases where multiple Jabber servers are deployed as a federation or cluster.	Scopia Desktop Clients cannot login and use the contact list.	Mandatory only in deployments of two or more Jabber servers deployed as a federation or cluster which must communicate via a firewall
6972- 65535	UDP	Streaming Server	Enables media connection to the Scopia Desktop Streaming Server, if separated from Scopia Desktop Server by a firewall.	Cannot connect to the Scopia Desktop Streaming server.	Mandatory To avoid opening these ports, place the Scopia Desktop Server in the same zone as the streaming server.

Table 15: Inbound Ports to Open from the Enterprise to the Scopia Desktop Server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
80	TCP (HTTP)	Web client	Provides access to the Scopia Desktop Server Web Portal (you can configure port 443 instead)	Cannot access the Scopia Desktop Server Web Portal	Mandatory if using HTTP. You can configure this port during installation. For more information, see *Installation Guide for Scopia Desktop Server*.
443	TCP (TLS)	Scopia Desktop Clients and Scopia Mobile	Enables sending control messages between the Scopia Desktop Server and Clients, and is also used to tunnel RTP media if the UDP ports are blocked	Scopia Desktop Client or Scopia Mobile cannot connect to the Scopia Desktop Server	Mandatory
3340	TCP	Scopia Management	Enables meeting control connection with Scopia Management	Meeting control connection to Scopia Management is disabled	Mandatory
7070	TCP	Streaming Server	Enables Scopia Desktop Clients to send tunneled RTSP traffic	Scopia Desktop Clients cannot receive video streams	Mandatory To configure, see Configuring the TCP Streaming Port on the Scopia Desktop Server on page 40

Table 16: Bidirectional Ports to Open Between the Scopia Desktop Server and the Public

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
10000-65535	UDP (RTP/RTCP)	Scopia Desktop Client or Scopia Mobile	Enables media connection with the Scopia Desktop Client or Scopia Mobile	Connection is tunneled via TCP port 443 and performance is not optimal	Recommended To configure, see Limiting the UDP Port Range for RTP/RTCP on the Scopia Desktop Server on page 39

Table 17: Inbound Ports to Open from the Public to the Scopia Desktop Server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
80	TCP (HTTP)	Web client	Provides access to the web user interface (you can configure port 443 instead)	Cannot access the web user interface	Mandatory if using HTTP. You can configure this port during installation. For more information, see *Installation Guide for Scopia Desktop Server*.
443	TCP (TLS)	Scopia Desktop Clients and Scopia Mobile	Enables sending control messages between the Scopia Desktop Server and Clients, and is also used to tunnel RTP media if the UDP ports are blocked	Scopia Desktop Clients cannot connect to the Scopia Desktop Server	Mandatory
7070	TCP	Streaming Server	Enables Scopia Desktop Clients to send tunneled RTSP traffic	Scopia Desktop Clients cannot receive video streams	Mandatory To configure, see Configuring the TCP Streaming Port on the Scopia Desktop Server on page 40.

Table 18: Outbound Ports to Open from the XMPP Server on page 37 and Table 19: Inbound Ports to Open on the XMPP Server on page 38 list the ports that should be opened on the XMPP Presence server, if the XMPP server is separated by a firewall from the Scopia Desktop Server.

Table 18: Outbound Ports to Open from the XMPP Server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
389	TCP (LDAP)	LDAP Server	Enables LDAP communication for user authentication, if the XMPP Server is configured for LDAP server (either Active Directory or Domino)	Users cannot login to the XMPP Server	Mandatory for LDAP authentication, if there is a firewall between XMPP and Scopia Desktop Server
3336	TCP (XML)	Scopia Management	Enables XML communication for user authentication, if the XMPP Server is configured for Scopia Management authentication	Users cannot login to the XMPP Server	Mandatory for Scopia Management authentication if there is a firewall between XMPP and Scopia Desktop Server

Table 19: Inbound Ports to Open on the XMPP Server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
5222	TCP	Scopia Desktop Client	Enables direct connection between Scopia Desktop Client and XMPP server	Scopia Desktop Client tries to use port 443 for tunnelled connection to the Scopia Desktop Server	Recommended if there is a firewall between XMPP and Scopia Desktop Server
5269	TCP	Scopia Desktop Client	Enables direct XMPP connections between Scopia Desktop Clients and the XMPP server	Scopia Desktop Clients need to proxy XMPP connections via Scopia Desktop Server	Recommended if there is a firewall between the XMPP server and Scopia Desktop Clients

Table 20: Bidirectional Ports to Open Between Scopia Desktop Clients

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
5060	UDP (SIP)	Scopia Desktop Client	Establishes direct SIP point-to-point connections between two Scopia Desktop Clients	Calls are routed via the Scopia Desktop Server	Recommended
1025-65535	UDP	Scopia Desktop Client	Establishes direct SIP point-to-point connections between two Scopia Desktop Clients	Calls are routed via the Scopia Desktop Server	Recommended

Table 21: Inbound Ports to Open from the Scopia Desktop Client to the STUN Server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3478	UDP	Scopia Desktop Clients	Enables connection between the STUN Server and Scopia Desktop Clients when making a point-to-point call. To connect point-to-point calls directly between two Scopia Desktop Clients, open the UDP ports (10000-65535, 6972-65535, 3478).	Scopia Desktop Client cannot connect to the STUN server and uses the Scopia Desktop Server as a relay agent.	Optional

Important:

Some firewalls are configured to block packets from the streaming server. You can either configure the firewall to allow streaming packets, or reconfigure the streaming server and client to use different network protocols that cross the firewall boundary.

The Streaming Server uses the IETF RTSP/RTP protocols. RTSP runs over TCP, while RTP runs over UDP. The streaming server can tunnel RTSP/RTP traffic through standard HTTP. Some firewalls may inspect traffic on port 80 and not allow the tunneled RTSP/RTP on that port. We therefore recommend using the QuickTime standard port 7070 as the alternate TCP port for HTTP tunneling. This is configured in the streaming server by default as long as you specify the port as part of the streaming server virtual address, as described in Configuring the TCP Streaming Port on the Scopia Desktop Server on page 40.

Limiting Port Ranges on the Scopia Desktop Server

About this task

This section provides instructions of how to limit the following port ranges on the Scopia Desktop Server:

Navigation

- Limiting the UDP Port Range for RTP/RTCP on the Scopia Desktop Server on page 39
- Limiting the TCP Port Range for H.245/Q.931 on the Scopia Desktop Server on page 40
- Configuring the TCP Streaming Port on the Scopia Desktop Server on page 40

Limiting the UDP Port Range for RTP/RTCP on the Scopia Desktop Server

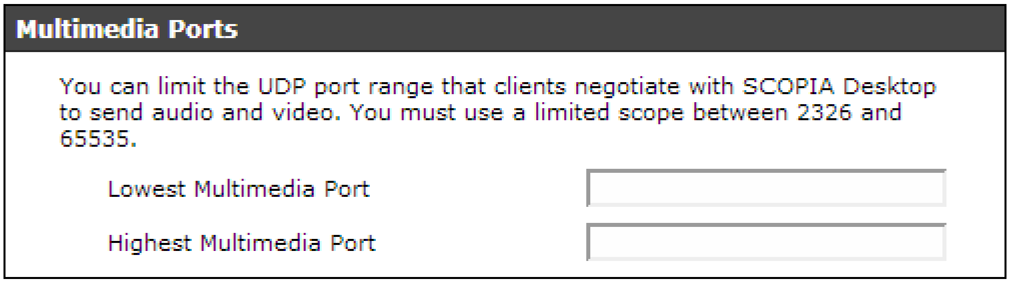
About this task

The Scopia Desktop Server has designated 10000-65535 as the default port range for UDP (RTP/RTCP). To provide additional security for your firewall, you can limit this range.

To calculate approximately how many ports the Scopia Desktop Server uses, multiply the number of license connections by 14, which amounts to reserving 14 ports per client.

Procedure

1. Log in to the Scopia Desktop Server Administrator web user interface.
2. Select **Client > Settings.**
3. Locate the **Multimedia Ports** section (see Figure 11: Multimedia Ports Area on page 40).


Multimedia Ports

You can limit the UDP port range that clients negotiate with SCOPIA Desktop to send audio and video. You must use a limited scope between 2326 and 65535.

Lowest Multimedia Port

Highest Multimedia Port

Figure 11: Multimedia Ports Area

4. Configure your port range (using any values between 2326 and 65535) by doing the following:

   a. Enter the base port value in the **Lowest Multimedia Port** field.

   b. Enter the upper port value in the **Highest Multimedia Port** field.

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

Limiting the TCP Port Range for H.245/Q.931 on the Scopia Desktop Server

About this task

The Scopia Desktop Server has designated ports 1024-65535 for TCP for H.245 and Q.931 signaling. To provide additional security for your firewall, you can limit this range.

For each conference, the Scopia Desktop Server uses 2 ports. In addition, add extra ports for:

- Add 2 ports for each participating Scopia Desktop Client client.
- Add 1 port per conference when presenting using the content slider.

Procedure

1. Navigate to *<Scopia Desktop install_dir>\ConfSrv*.

2. Edit the *config.val* file as follows:

   a. Locate the text `1 system`.

   b. At the bottom of that section, add two lines:

   ```
   2 portFrom = <lowest range limit>
   2 portTo = <highest range limit>
   ```

   Where `<lowest range limit>` is the base port of your port range and `<highest range limit>` is the upper value of your port range.

3. Access the Windows services and restart the **Scopia Desktop - Conference Server** service.

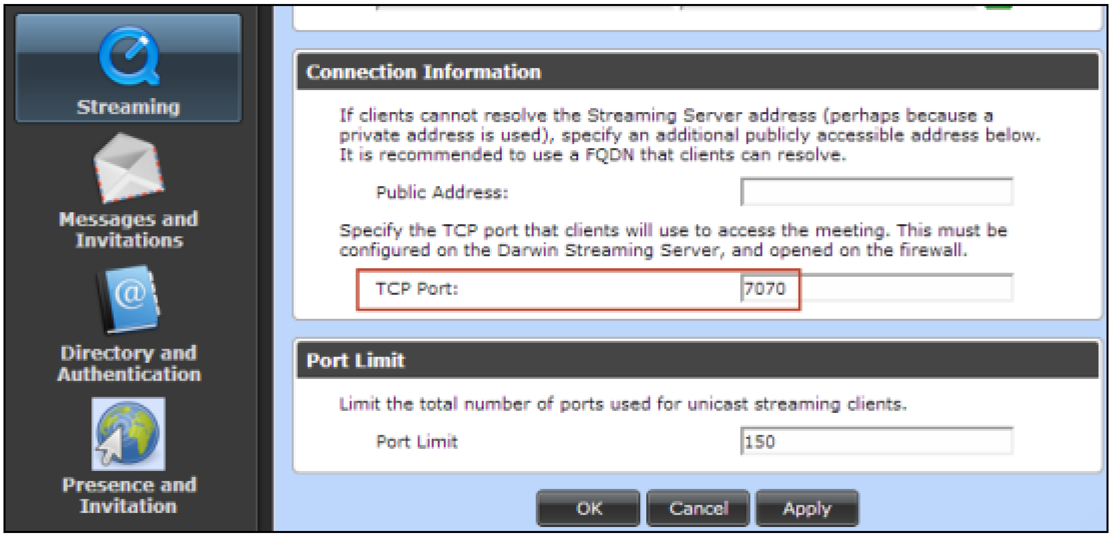
Configuring the TCP Streaming Port on the Scopia Desktop Server

About this task

The Streaming Server that is deployed with your Scopia Desktop Server is configured by default to use the QuickTime standard port 7070 as the alternate TCP port for HTTP tunneling. If your firewall is configured to block packets from the Streaming Server, you must reconfigure the Streaming Server and client to use different network protocols which can cross the firewall boundary.

Procedure

1. Log in to the Scopia Desktop Server Administrator web user interface.
2. Select **Streaming**. The **Settings** page for the Streaming Server appears (see Figure 12: Setting the streaming port for Scopia Desktop Server on page 41).



Connection Information

If clients cannot resolve the Streaming Server address (perhaps because a private address is used), specify an additional publicly accessible address below. It is recommended to use a FQDN that clients can resolve.

Public Address:

Specify the TCP port that clients will use to access the meeting. This must be configured on the Darwin Streaming Server, and opened on the firewall.

TCP Port: 7070

Port Limit

Limit the total number of ports used for unicast streaming clients.

Port Limit 150

Figure 12: Setting the streaming port for Scopia Desktop Server

3. Locate the **Connection Information** area.
4. Modify the port value in the **TCP Port** field.

   Important:

   The Streaming Server uses the IETF RTSP/RTP protocols. RTSP runs over TCP, while RTP runs over UDP. Many firewalls are configured to restrict TCP packets by port number and are very restrictive on UDP. The Streaming Server can tunnel RTSP/RTP traffic through standard HTTP. Some firewalls may inspect traffic on port 80 and not allow the tunneled RTSP/RTP on that port. We therefore recommend using the QuickTime standard port 7070 as the alternate TCP port for HTTP tunneling.

5. Select **OK** or **Apply**.
6. Do the following on the Scopia Desktop Server:

   a. Navigate to the following directory: C:\Program Files\Darwin Streaming Server.

   b. Open the *streamingserver.xml* file.

c. Locate the list of ports for the RTSP protocol by finding the text `LIST-PREF NAME="rtsp_port"` in the file.

```
<CONFIGURATION>
  <SERVER>
    <LIST-PREF NAME="rtsp_port" TYPE="UInt16" >
      <VALUE> 7070 </VALUE>
    </LIST-PREF>
```

d. Within this section, add a new entry of `<VALUE> xxxx </VALUE>`, where `xxxx` is the new port value.

e. Save the file.

f. Restart the Darwin Streaming Server.

g. Restart the **Darwin Streaming Server** service.

Chapter 5 | Implementing Port Security for Scopia PathFinder

Scopia PathFinder is Scopia Solution’s answer to firewall traversal. The Scopia PathFinder Server is an H.460 server, while the Scopia PathFinder Client is an H.460 client. H.460 enables firewall and NAT traversal for H.323 media and signaling.

This section details the ports used for the Scopia PathFinder Server and the Scopia PathFinder Client, and the relevant port configuration procedures:

Navigation

- Ports to Open on Scopia PathFinder on page 43
- Configuring Ports on the Scopia PathFinder Server on page 47

Ports to Open on Scopia PathFinder

Scopia PathFinder is Scopia Solution’s answer to firewall traversal. The Scopia PathFinder Server is an H.460 server, typically deployed in the DMZ, while the Scopia PathFinder Client is an H.460 client, typically deployed outside the enterprise firewall with the H.323 endpoint (see Figure 13: H.323 connections to Scopia PathFinder Server on page 44).

Many recent H.323 endpoints have built-in H.460 functionality (which enables secure communication), thereby avoiding the need for a Scopia PathFinder Client. If an H.323 endpoint located in a partner company does not have H.460 capabilities, it must communicate via the Scopia PathFinder Client to access the Scopia PathFinder Server in the DMZ (see Figure 13: H.323 connections to Scopia PathFinder Server on page 44).

Important:

There must be no firewall between the H.323 endpoint (device) and the Scopia PathFinder Client.

An H.323 endpoint in the public network can also directly dial the Scopia PathFinder Server using direct port access (ports 4000-5000).

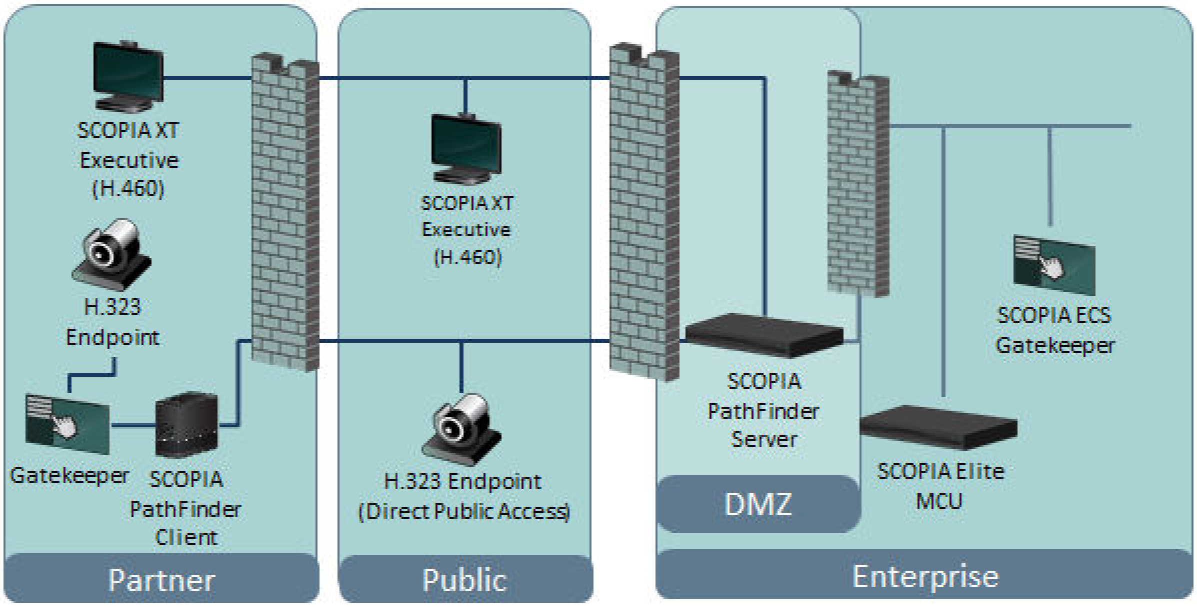


Figure 13: H.323 connections to Scopia PathFinder Server

When opening ports to and from Scopia PathFinder Server, use the following as a reference:

- If opening ports that are both to and from the Scopia PathFinder Server, see Table 22: Bidirectional Ports to Open the Scopia PathFinder Server on page 45.
- If opening ports that are both to and from the Scopia PathFinder Client, see Table 23: Bidirectional Ports to Open on the Scopia PathFinder Client on page 47.

Important:

In order for an H.323 endpoint (or other H.323 device) within the enterprise to successfully connect to the Scopia PathFinder Server in the DMZ via the enterprise firewall (see Figure 14: Contacting Scopia PathFinder Server from within the enterprise on page 45), you must do one of the following:

- Install a Scopia PathFinder Client within the enterprise
- Use H.460-enabled endpoints
- Open the internal firewall to the Scopia PathFinder Server (1024-65535, bidirectional)

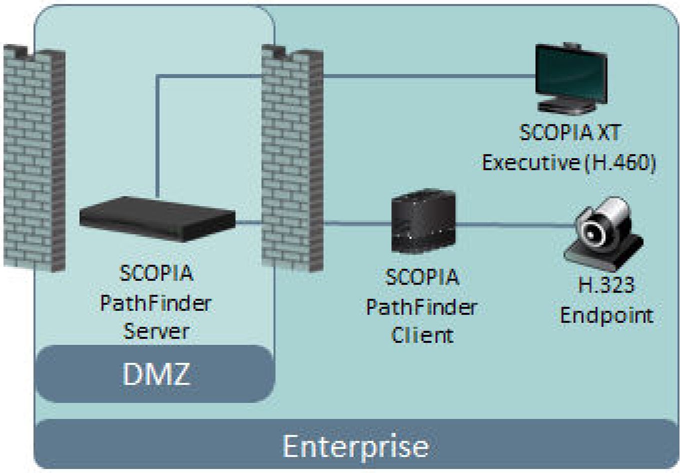


Figure 14: Contacting Scopia PathFinder Server from within the enterprise

Important:

The specific firewalls you need to open ports on depends on where your Scopia PathFinder Server, Scopia PathFinder Client, and other Scopia Solution products are deployed.

Table 22: Bidirectional Ports to Open the Scopia PathFinder Server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
22	SSH/SFTP (TCP)	SSH client endpoint	Enables initial configuration, log download and server upgrade	Cannot initialize the server, download logs and upgrade the server	Mandatory for configuring the Scopia PathFinder Server
53	DNS (UDP)	DNS server	Enables querying the DNS for domains per call	Cannot support domain name calls and dialing by URI	Mandatory if using URI dialing
1719	UDP	H.460.18 endpoint/ H.460.18 client gatekeeper	Enables H.460.18 RAS capabilities	H.460.18 endpoints cannot register through Scopia PathFinder Server, firewall traversal function based on H.460.18 and H.460.19 cannot function.	Mandatory for H.460 endpoints To configure, see Configuring the UDP Port for RAS on the Scopia PathFinder Server on page 47
1720	TCP	Any H.323 device using Q.931 signaling in DPA mode	Enables IP call signaling	No signaling capabilities: guest users cannot dial into internal endpoints	Mandatory if in DPA mode

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
2776	TCP, UDP	H.460.18 endpoint/ H.460.18 client gatekeeper	Enables H.460.18 Call Signaling, H.460.19 Multiplex Media Channel	H.460.18 endpoints cannot register through Scopia PathFinder Server or set up logical channels. Firewall traversal function based on H.460.18 and H.460.19 cannot function.	Mandatory for H.460 endpoints
2777	TCP, UDP	H.460.18 endpoint/ H.460.18 client gatekeeper	Enables H.460.18 and H.460.19 Call Control, H.460.19 Multiplex Media Control Channel	H.460.18 endpoints cannot set up Call Control channels or logical channels. Firewall traversal function based on H.460.18 and H.460.19 cannot function.	Mandatory for H.460 endpoints
3089	TCP, UDP	Scopia PathFinder Client	Enables signaling and media traversal	If the TCP port is blocked, Scopia PathFinder Client cannot connect to Scopia PathFinder Server. Legacy H.323 endpoints behind the Scopia PathFinder Client cannot call external endpoints. If the UDP port is blocked, Scopia PathFinder Client can only traverse media via TCP.	Mandatory if using Scopia PathFinder Client
3089	TCP, UDP	Scopia PathFinder Server	Enables signaling and media connection to neighbor server	Cannot connect or traverse media to neighbor server	Mandatory if using a neighbor server
4000-5000	TCP, UDP	Any H.323 device using Q.931 signaling in DPA mode	Enables Direct Public Access (DPA) for H.323 call signaling, control and media traversal	Cannot setup/ connect DPA mode calls	Mandatory if in DPA mode To limit range, see Limiting the TCP/UDP Port Range for H.323 Direct Access Calls on the Scopia PathFinder Server on page 48

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
8080	HTTP (TCP)	Web client/ browser	Provides access to the web user interface	Cannot configure Scopia PathFinder Server	Mandatory for configuring the Scopia PathFinder application
8089	XML (TCP)	XML API Client	Enables managing Scopia PathFinder Server via XML API	The External Management System cannot get Scopia PathFinder Server status or receive traps from Scopia PathFinder Server	Optional

Table 23: Bidirectional Ports to Open on the Scopia PathFinder Client

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3478	STUN (UDP)	STUN server	Enables an endpoint located in the remote network to send a STUN Binding Request when connecting to another endpoint in the same network	Scopia PathFinder Client cannot determine its public IP address. Smart Direct Media Connect cannot function.	Recommended

❗ **Important:**

If there is a firewall between the H.323 client and the Scopia PathFinder Client, all high ports must be opened in both directions (1024-65535). We therefore recommend no firewall between the endpoint and the Scopia PathFinder Client.

Configuring Ports on the Scopia PathFinder Server

This section provides instructions of how to configure the following ports and port ranges on the Scopia PathFinder Server:

Navigation

- Configuring the UDP Port for RAS on the Scopia PathFinder Server on page 47
- Limiting the TCP/UDP Port Range for H.323 Direct Access Calls on the Scopia PathFinder Server on page 48

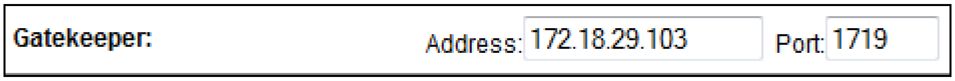
Configuring the UDP Port for RAS on the Scopia PathFinder Server

About this task

The Scopia PathFinder Server has designated port 1719 for RAS (communication with the gatekeeper). You can configure a different port for RAS (if, for example, port 1719 is busy).

Procedure

1. Access the Scopia PathFinder Server Administrator web interface.
2. Log in to the Scopia PathFinder web user interface.
3. Select **Settings > General**.
4. Locate the Gatekeeper area (see Figure 15: Gatekeeper Settings on page 48).



Gatekeeper: Address: 172.18.29.103 Port: 1719

Figure 15: Gatekeeper Settings

5. Modify the port range in the **Port** field.
6. Select **Save**.

Limiting the TCP/UDP Port Range for H.323 Direct Access Calls on the Scopia PathFinder Server

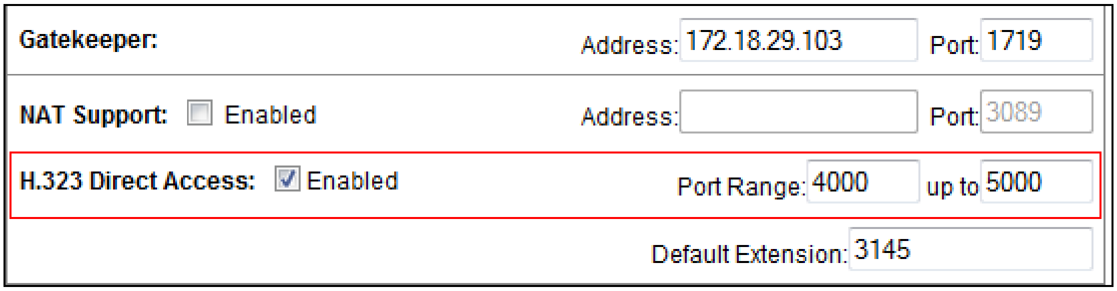
About this task

The Scopia PathFinder Server has designated ports 4000-5000 for H.323 Direct Public Access (DPA), which allows non-H.460 public endpoints to call internal endpoints without being registered to the Scopia PathFinder Server. To provide additional security for your firewall, you can limit this range.

To calculate approximately how many ports the Scopia PathFinder Server uses, multiply the number of simultaneous DPA calls by 10. The multiplication factor is lower for audio-only calls and higher for calls with dual video. We recommend using 10 as an approximation.

Procedure

1. Access the Scopia PathFinder Server Administrator web interface.
2. Select **Settings > General**.
3. Enable H.323 Direct Access by selecting the checkbox next to **H.323 Direct Access** (Figure 16: H.323 Direct Access Settings on page 49).



Gatekeeper: Address: 172.18.29.103 Port: 1719

NAT Support: □ Enabled Address: Port: 3089

H.323 Direct Access: ☑ Enabled Port Range: 4000 up to 5000

Default Extension: 3145

Figure 16: H.323 Direct Access Settings

4. Modify the port range in the **Port Range** fields.
5. Select **Save**.

Chapter 6 | Implementing Port Security for the Scopia Video Gateway and the Radvision SIP Gateway

This section details the ports required for the Radvision SIP Gateway and the Scopia Video Gateway, two gateways which serve as a bridge between H.323-based video networks and other protocols. With the right gateway deployed into your existing solution, you use the two separate video networks as one: making video calls from H.323 endpoints to clients from the other protocol and vice versa.

This section details the ports used for the Scopia Video Gateway or the Radvision SIP Gateway, together with the relevant configuration procedures:

Navigation

- Ports to Open on the Scopia Video Gateway , the Radvision SIP Gateway, and the Scopia TIP Gateway on page 50
- Configuring Ports on the Scopia Video Gateway, Radvision SIP Gateway and the Scopia TIP Gateway on page 53

Ports to Open on the Scopia Video Gateway , the Radvision SIP Gateway, and the Scopia TIP Gateway

The Scopia Video Gateway , the Radvision SIP Gateway, and the Scopia TIP Gateway are typically deployed in the enterprise network. When opening ports on either device, use the following as a reference:

- If you are opening ports that are both in and out of either gateway, see Table 24: Bidirectional Ports to Open on the Scopia Video Gateway , Radvision SIP Gateway , and the Scopia TIP Gateway on page 51.
- If you are opening ports outbound from either gateway, see Table 25: Outbound Ports to Open from the Scopia Video Gateway and the Radvision SIP Gateway on page 53.
- If you are opening ports inbound to either gateway, see Table 26: Inbound Ports to Open to the Scopia Video Gateway , Radvision SIP Gateway, and the Scopia TIP Gateway on page 53.

Important:

Choosing the specific firewalls where ports need to be opened depends on where your gateway and your other Scopia Solution products are deployed.

Table 24: Bidirectional Ports to Open on the Scopia Video Gateway , Radvision SIP Gateway , and the Scopia TIP Gateway

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
443 (Scopia Video Gateway only)	STUN (TCP)	Microsoft STUN Server	Enables remote SIP , ICE connectivity.	Cannot connect remote endpoints	Mandatory
1024-1174	H.245 (TCP)	Any H.323 device	Enables H.245 signaling	Cannot connect H.323 calls	Mandatory To limit range, see Limiting TCP Port Range for H.245 on the Scopia Video Gateway, Radvision SIP Gateway, and Scopia TIP Gateway on page 54
1719	RAS (UDP)	H.323 gatekeeper	Enables RAS signaling	Cannot communicate with H.323 gatekeeper	Mandatory To configure, see Configuring UDP Port for RAS on the Scopia Video Gateway, SIP Gateway and Scopia TIP Gateway on page 57
1720	Q.931 (TCP)	Any H.323 device	Enables Q.931 signaling	Cannot connect H.323 calls	Mandatory To configure, see Configuring TCP Port for Q.931 on the Scopia Video Gateway, SIP Gateway, and Scopia TIP Gateway on page 58
3336	XML (TCP)	Scopia Management	Enables you to manage this gateway via the XML API	Cannot use the XML API to manage the gateway	Mandatory
3338	XML (TCP)	Scopia Management, or any third-party configuration applications	Enables you to configure the gateway via the XML API	Cannot use the XML API to configure the gateway	Mandatory
3346	XML (TLS)	Scopia Management	Enables you to manage Scopia Video Gateway via the XML API	Cannot use the XML API to manage Scopia Video Gateway	Mandatory if using TLS

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3348	XML (TLS)	Scopia Management, or any third-party configuration applications	Enables you to configure Scopia Video Gateway via the XML API	Cannot use the XML API to configure Scopia Video Gateway	Mandatory if using TLS
3478	STUN (UDP)	STUN Server	Enables remote endpoint to connect	Cannot connect remote endpoints	Mandatory
5060	SIP (TCP/ UDP)	Any SIP device	Enables SIP signaling	Cannot connect SIP calls	Mandatory
5061	SIP (TLS)	Any SIP device	Enables secure SIP signaling	Cannot connect SIP calls via TLS	Mandatory if using TLS
12000-13200 (SIP Gateway and Scopia Video Gateway only)	RTP/ RTCP / SRTP(UDP)	UDP for any H.323 or SIP media connection	Video: Enables real-time delivery of video media	Cannot transmit/ receive video media streams	Mandatory To configure, see Configuring RTP/ RTCP/SRTP Ports on the Scopia Video Gateway, SIP Gateway and Scopia TIP Gateway on page 55
12000-12718 (TIP Gateway only)	RTP/ RTCP / SRTP(UDP)	UDP for any H.323 or SIP media connection	Video: Enables real-time delivery of video media	Cannot transmit/ receive video media streams	Mandatory To configure, see Configuring RTP/ RTCP/SRTP Ports on the Scopia Video Gateway, SIP Gateway and Scopia TIP Gateway on page 55
16384-17584 (SIP Gateway and Scopia Video Gateway only)	RTP/ RTCP / SRTP (UDP)	UDP for any H.323 or SIP media connection	Audio: Enables real-time delivery of audio media	Cannot transmit/ receive audio media streams	Mandatory To configure, see Configuring RTP/ RTCP/SRTP Ports on the Scopia Video Gateway, SIP Gateway and Scopia TIP Gateway on page 55
16384-17280 (TIP Gateway only)	RTP/ RTCP / SRTP (UDP)	UDP for any H.323 or SIP media connection	Audio: Enables real-time delivery of audio media	Cannot transmit/ receive audio media streams	Mandatory To configure, see Configuring RTP/ RTCP/SRTP Ports on the Scopia Video Gateway, SIP Gateway and Scopia TIP Gateway on page 55

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
20000-29000 (Scopia Video Gateway only)	RTP/ RTCP / SRTP (TCP)	TCP for H.323 or SIP media connection. Microsoft Lync uses both UDP and TCP to ensure the widest compatibility.	Audio: Enables real-time delivery of audio media in TCP.	Cannot transmit/ receive audio media streams	Mandatory To configure, see Configuring RTP/ RTCP/SRTP Ports on the Scopia Video Gateway, SIP Gateway and Scopia TIP Gateway on page 55
40000-46200 (Scopia Video Gateway only)	RTP/ RTCP / SRTP (TCP)	TCP for H.323 or SIP media connection. Microsoft Lync uses both UDP and TCP to ensure the widest compatibility.	Video: Enables real-time delivery of video media in TCP.	Cannot transmit/ receive audio media streams	Mandatory To configure, see Configuring RTP/ RTCP/SRTP Ports on the Scopia Video Gateway, SIP Gateway and Scopia TIP Gateway on page 55

Table 25: Outbound Ports to Open from the Scopia Video Gateway and the Radvision SIP Gateway

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
162	SNMP (UDP)	Scopia Management, Scopia Management, or any SNMP manager station	Enables sending SNMP Trap events	Cannot send Traps via a Network Manager	Recommended

Table 26: Inbound Ports to Open to the Scopia Video Gateway , Radvision SIP Gateway, and the Scopia TIP Gateway

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
21	FTP (TCP)	FTP Server	Enables audio stream recording	Cannot record audio streams	Optional
22	SSH (TCP)	SSH Client	Enables you to view logs for the gateway in real-time	Cannot view logs in real- time (logs are collected on local storage device)	Optional
80	HTTP (TCP)	Web client	Enables you to upgrade the gateway and download customer support information	Cannot upgrade the gateway or download customer support information	Mandatory

Configuring Ports on the Scopia Video Gateway, Radvision SIP Gateway and the Scopia TIP Gateway

This section provides instructions of how to configure the following ports and port ranges on the Scopia Video Gateway, Radvision SIP Gateway and the Scopia TIP Gateway:

Navigation

- Limiting TCP Port Range for H.245 on the Scopia Video Gateway, Radvision SIP Gateway, and Scopia TIP Gateway on page 54
- Configuring RTP/RTCP/SRTP Ports on the Scopia Video Gateway, SIP Gateway and Scopia TIP Gateway on page 55
- Configuring UDP Port for RAS on the Scopia Video Gateway, SIP Gateway and Scopia TIP Gateway on page 57
- Configuring TCP Port for Q.931 on the Scopia Video Gateway, SIP Gateway, and Scopia TIP Gateway on page 58

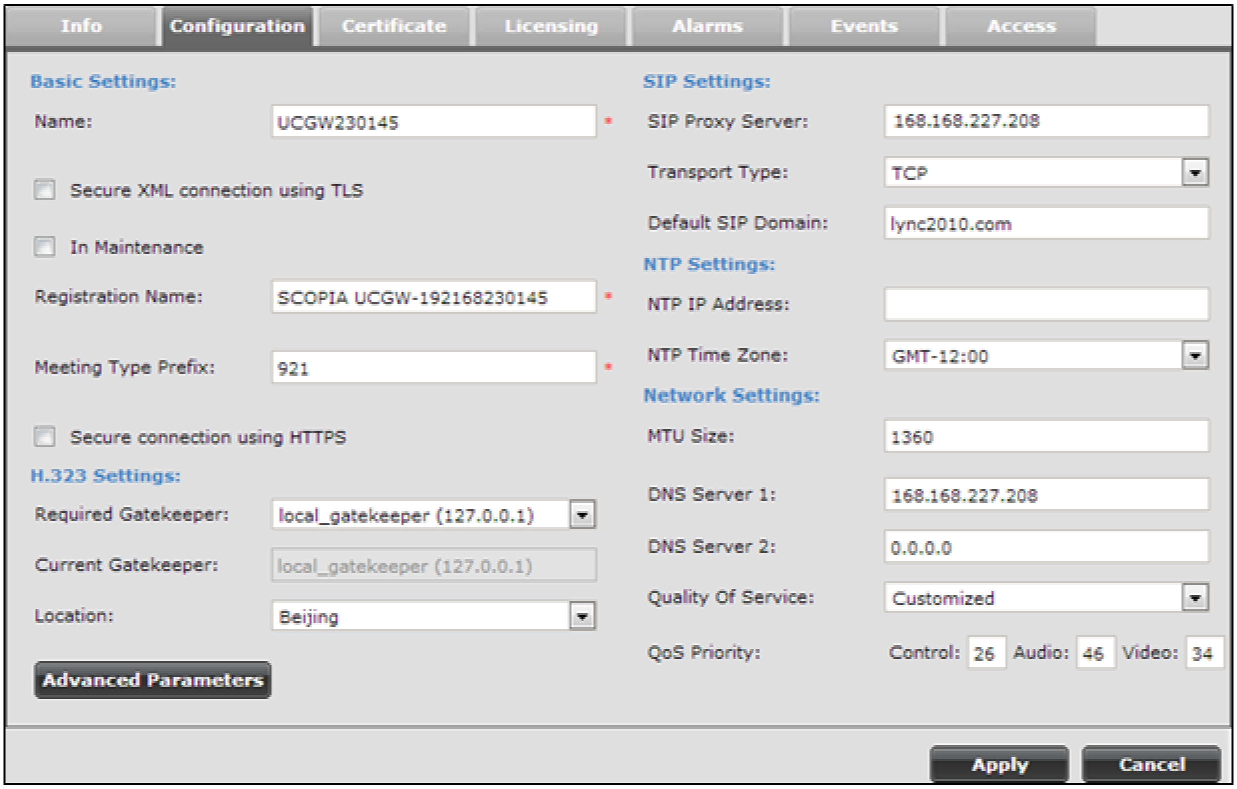
Limiting TCP Port Range for H.245 on the Scopia Video Gateway, Radvision SIP Gateway, and Scopia TIP Gateway

About this task

The Scopia Video Gateway, Radvision SIP Gateway and Scopia TIP Gateway designate ports 1024-1174 for H.245 (signaling). H.245 is a control protocol used for multimedia communications that enables transferring information about the device capabilities, as well as opening/closing the logical channels that carry media streams. To provide additional security for your firewall, you can limit this range.

Procedure

1. Log in to the Scopia Management administrator portal.
2. Select **Devices > Devices by Type > Gateways**.
3. Select the relevant gateway from the **Gateways** list.
4. Select the **Configure** tab (see Figure 17: Configuring a gateway from Scopia Management on page 55).



Basic Settings:

Name: UCGW230145 *

□ Secure XML connection using TLS

□ In Maintenance

Registration Name: SCOPIA UCGW-192168230145 *

Meeting Type Prefix: 921 *

□ Secure connection using HTTPS

H.323 Settings:

Required Gatekeeper: local_gatekeeper (127.0.0.1)

Current Gatekeeper: local_gatekeeper (127.0.0.1)

Location: Beijing

SIP Settings:

SIP Proxy Server: 168.168.227.208

Transport Type: TCP

Default SIP Domain: lync2010.com

NTP Settings:

NTP IP Address:

NTP Time Zone: GMT-12:00

Network Settings:

MTU Size: 1360

DNS Server 1: 168.168.227.208

DNS Server 2: 0.0.0.0

Quality Of Service: Customized

QoS Priority: Control: 26 Audio: 46 Video: 34

Figure 17: Configuring a gateway from Scopia Management

5. Select **Advanced Parameters**. The **Advanced Parameters** dialog box appears (see Figure 17: Configuring a gateway from Scopia Management on page 55).

6. To set the base port for the H.245 control channel protocol, do the following:

   a. Clear the values before proceeding to the next step.

   b. Enter **h245baseport** in the **Command ID** field.

   c. Enter the port value in the **Value** field.

   d. Select **Save**.

   e. Select **Close**

7. To set the port range for H.245, do the following:

   a. Clear the values before proceeding to the next step.

   b. Enter **h245portrange** in the **Command ID** field.

   c. Enter the port value in the **Value** field.

   d. Select **Save**.

   e. Select **Close**

Configuring RTP/RTCP/SRTP Ports on the Scopia Video Gateway, SIP Gateway and Scopia TIP Gateway

About this task

The Scopia Video Gateway, Radvision SIP Gateway and Scopia TIP Gateway designate ports 16384-17584 for UDP audio media, and 12000-13200 for UDP video media.

In addition, the Scopia Video Gateway uses ports 20000-29000 for TCP audio and 40000-46200 for TCP video.

Procedure

1. Log in to the Scopia Management administrator portal.
2. Select **Devices**.
3. Select **Gateways** in the sidebar menu.
4. Select the relevant gateway from the **Gateways** list.
5. Select the **Configure** tab (see Figure 17: Configuring a gateway from Scopia Management on page 55).
6. Select **Advanced Parameters Settings**. The **Advanced Parameters** dialog box appears (see Figure 17: Configuring a gateway from Scopia Management on page 55).
7. Set the UDP video base port by doing the following:

   a. For SIP Gateway and TIP Gateway deployments: Enter the **advcmdmvpsetval** command in the **Command** field.

   b. For Scopia Video Gateway deployments: Enter the **advcmdmpcsetval** command in the **Command** field.

   c. Enter the **mf.BasePort** parameter in the **Parameter** field to set the UDP video base port.

   Important:

   For Scopia Video Gateway deployments: To set the TCP video base port, enter **mf.MvpTcpBasePort** in the **Parameter** field.

   d. Enter the port value in the **Value** field.

   e. Select **Save**.
8. For SIP Gateway and TIP Gateway deployments: Complete the video base port configuration as follows:

   a. Enter the **mvpconfigcompletedcommand** command in the **Command** field.

   b. Enter **1** in the **Value** field.

   c. Select **Save**.

   d. Clear the value in the **Parameter** field before proceeding to the next step.
9. For SIP Gateway and TIP Gateway deployments: Set the audio base port by doing the following:

   a. Enter the **advcmdmapsetval** command in the **Command** field.

   b. Enter the **mf.UdpBasePort** parameter in the **Parameter** field.
   c. Enter the port value in the **Value** field.
   d. Select **Save**.
   e. Enter the **mapconfigcompleted** command in the **Command** field.
   f. Enter **1** in the **Value** field.
   g. Select **Save**.

10. For Scopia Video Gateway deployments: Set the UDP audio base port by doing the following:
    a. Enter the **setmprtpbaseport** command in the **Command** field.
    b. Modify the port value in the **Value** field.
    c. Select **Save**.

11. For Scopia Video Gateway deployments: Set the TCP audio base port by doing the following:
    a. Enter the **setmptcpbaseport** command in the **Command** field.
    b. Modify the port value in the **Value** field.
    c. Select **Save**.

12. Select **Close**.

Configuring UDP Port for RAS on the Scopia Video Gateway, SIP Gateway and Scopia TIP Gateway

About this task

The Scopia Video Gateway, Radvision SIP Gateway and the Scopia TIP Gateway designate port 1719 for RAS, the protocol for signaling messages. You can configure a different port for RAS (if, for example, port 1719 is busy).

Procedure

1. Log in to the Scopia Management administrator portal.

2. Select **Devices**.

3. Select **Gateways** in the sidebar menu.

4. Select the relevant gateway from the **Gateways** list.

5. Select the **Configure** tab (see Figure 17: Configuring a gateway from Scopia Management on page 55).

6. Select **Advanced Parameters Settings**. The **Advanced Parameters** dialog box appears (see Figure 17: Configuring a gateway from Scopia Management on page 55).
   a. Select **h323rasport** from the **Command ID** list.
   b. Enter the port value in the **Value** field.

c. Select **Save**.
d. Select **Close**.

Configuring TCP Port for Q.931 on the Scopia Video Gateway, SIP Gateway, and Scopia TIP Gateway

About this task

The Scopia Video Gateway, Radvision SIP Gateway, and Scopia TIP Gateway designate port 1720 for Q.931. Q.931 is a telephony protocol used for establishing and terminating the connections in H.323 calls. You can configure a different port for Q.931 (if, for example, port 1720 is busy).

Procedure

1. Log in to the Scopia Management administrator portal.
2. Select **Devices**.
3. Select **Gateways** in the sidebar menu.
4. Select the relevant gateway from the **Gateways** list.
5. Select the **Configure** tab (see Figure 17: Configuring a gateway from Scopia Management on page 55).
6. Select **Advanced Parameters Settings**. The **Advanced Parameters** dialog box appears (see Figure 17: Configuring a gateway from Scopia Management on page 55).
   a. Select **h323sigport** from the **Command ID** list.
   b. Enter the port value in the **Value** field.
   c. Select **Save**.
   d. Select **Close**.

Chapter 7 | Implementing Port Security for Scopia ECS Gatekeeper

Scopia ECS Gatekeeper is a management component that provides standalone address resolution functionality in H.323 networks.

This section details the ports used for Scopia ECS Gatekeeper and the relevant configuration procedures:

Navigation

Ports to Open on Scopia ECS Gatekeeper

Scopia ECS Gatekeeper is typically deployed in enterprise network or the DMZ.

When opening ports to and from the ECS, use the following as a reference:

- If you are opening ports that are both in and out of the ECS, see Table 27: Bidirectional Ports to Open on Scopia ECS Gatekeeper on page 59.
- If you are opening ports that are outbound from the ECS, see Table 28: Outbound Ports to Open from Scopia ECS Gatekeeper on page 61.

Important:

The specific firewalls you need to open ports on depends on where your Scopia ECS Gatekeeper and other Scopia Solution products are deployed.

Table 27: Bidirectional Ports to Open on Scopia ECS Gatekeeper

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
21	FTP (TCP)	FTP client/ CDR server	Enables offline viewing of ECS logs and CDRs	Cannot view logs or retrieve CDR files offline	Recommended
80	HTTP (TCP)	Web client	Provides access to the ECS web user interface	Cannot view ECS web user interface	Recommended To configure, see Configuring the HTTP Port on Scopia ECS Gatekeeper on page 63

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
161	SNMP (UDP)	Scopia Management, web client, or any SNMP manager station	Enables you to configure and check the ECS status	Cannot configure or check the ECS status	Mandatory
1025-5000 (for Windows XP or earlier)	H.245/ Q.931 (TCP)	Any H.323 device	Enables H.245/ Q.931 signaling	No H.245/ Q.931 signaling capabilities	Mandatory if ECS is not in direct mode To limit range, see Limiting the TCP Port Range for H.245/Q.931 on Scopia ECS Gatekeeper on page 61
49152-65535 (Windows Vista or Windows Server 2008)	H.245/ Q.931 (TCP)	Any H.323 device	Enables H.245/ Q.931 signaling	No H.245/ Q.931 signaling capabilities	Mandatory if ECS is not in direct mode To limit range, see Limiting the TCP Port Range for H.245/Q.931 on Scopia ECS Gatekeeper on page 61
1719	RAS (UDP)	Any H.323 device using RAS signaling or Neighbor Gatekeepers	Enables RAS signaling and sending LRQ messages to Neighbor Gatekeepers	No RAS signaling capabilities, cannot send LRQ messages between Neighbor Gatekeepers	Mandatory
1720	Q.931 (TCP)	Any H.323 device using Q.931 signaling	Enables Q.931 signaling	No signaling capabilities (except in direct mode)	Mandatory if ECS is not in direct mode
3271	ECS XML (TCP)	XML server	Enables external management servers (such as Scopia Management) to connect to the ECS via XML messages	External management servers cannot connect to ECS	Mandatory if deployed with Scopia Management
12378	Alternate Gatekeeper protocol (TCP)	Redundant (Alternate) Gatekeeper	Enables master/slave data synchronization and negotiation between redundant (Alternate) gatekeepers separated by a firewall	Redundancy functionality is not available	Recommended if gatekeepers are separated by a firewall

Table 28: Outbound Ports to Open from Scopia ECS Gatekeeper

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
23	Telnet (TCP)	Sony endpoint	Enables control of Sony endpoints	No control over Sony endpoints	Optional
53	DNS (TCP)	DNS server	Enables querying DNS for domains per call	DNS is disabled	Optional
162	SNMP (UDP)	Scopia Management or any SNMP manager station	Enables sending SNMP Trap events	Cannot send traps	Recommended
1719	RAS (UDP)	Neighbor Gatekeepers	Enables sending LRQ messages to Neighbor Gatekeepers	Cannot send LRQ messages between Neighbor Gatekeepers	Mandatory

Configuring Ports on Scopia ECS Gatekeeper

This section provides instructions of how to configure the following ports and port ranges on Scopia ECS Gatekeeper:

Navigation

- Limiting the TCP Port Range for H.245/Q.931 on Scopia ECS Gatekeeper on page 61
- Configuring the HTTP Port on Scopia ECS Gatekeeper on page 63
- Configuring the TCP Port for the Alternate Gatekeeper Protocol on Scopia ECS Gatekeeper on page 64
- Configuring the UDP Port for SNMP Traps on Scopia ECS Gatekeeper on page 65

Limiting the TCP Port Range for H.245/Q.931 on Scopia ECS Gatekeeper

About this task

Scopia ECS Gatekeeper uses one of the following TCP port ranges for H.245/Q.931, depending on the version of Windows you are running:

- If you have Windows XP, ECS uses 1025-5000.
- If you have Windows Vista or Windows Server 2008, ECS uses 49152-65535.

To provide additional security for your firewall, you can limit this range. To calculate how many ports the ECS uses, multiply the maximum calls allowed by your license by four.

Q.931 is a telephony protocol used for establishing and terminating the connections in H.323 calls, and H.245 is a Control Protocol used for multimedia communication that enables transferring information about the device capabilities, as well as opening/closing the logical channels that carry media streams.

Procedure

1. Access the Windows Services and stop the **ECS Service**.

2. Open the **Windows registry**.

3. Navigate to: **HKEY_LOCAL_MACHINE\SOFTWARE\RADVISION\Enhanced Communication Server\Storage\Config\Stack**.

   Important:

   If you are using Windows Server 2008 64-bit, navigate to: **HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node\RADVISION\Enhanced Communication Server\Storage \Config\Stack**.

4. Create a new string, as follows:

   a. Right-click the **Stack** folder and select **New > String Value**.

   b. Name the new string **PortMin**.

   c. Right-click **PortMin** and select **Modify**.

   d. In the **Value data** field, enter the value of the minimum port number the ECS should use.

5. Create a new string, as follows:

   a. Right-click the **Stack** folder and select **New > String Value**.

   b. Name the new string **PortMax**.

   c. Right-click **PortMax** and select **Modify**.

   d. In the **Value data** field, enter the value of the maximum port number the ECS should use.

6. Access the Windows Services and start the **ECS service**.

7. If you have Windows XP, check the Windows global maximum port by doing the following:

   a. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip \Parameters**.

   b. Verify that the Windows global maximum port, displayed in **MaxUserPort**, is higher than the ECS port you defined in **PortMax**.

      Important:

      If **MaxUserPort** is not defined, its default value is 5000.

   c. If the value you defined in **PortMax** is higher than the value in **MaxUserPort**, do one of the following:

      - If **MaxUserPort** is defined, right-click, select **Modify**, and enter a value that is higher than the value in **PortMax**. Restart your computer.
      - If **MaxUserPort** is not defined, right-click, select **New > DWORD** value, and enter a value that is higher than the value in **PortMax**. Restart your computer.

8. If you have Windows Vista or Windows Server 2008, your default Windows TCP port range is 49152-65535. If the port values you defined for the ECS are outside of this range, modify your Windows TCP port range by doing the following:

Important:

The Windows TCP port range must be compliant with the port requirements of all programs running on that server, as well as Scopia Solution products (such as Scopia Desktop or Scopia Management) communicating with this computer.

a. Open the command line prompt as an administrator by right-clicking on **cmd** and selecting **Run as administrator**.

b. Enter the following command:

```
netsh int ipv4 set dynamicportrange protocol=tcp
startport=1025 numberofports=3975
```

Important:

If the value you defined in **PortMax** is higher than 5000, increase the value of the number of ports in the command. For example, if you defined the value of **PortMax** as 6000, change the value of `numberofports` in the command to `4975`.

c. Verify that your default Windows TCP port range is updated by entering the following command:

```
netsh int ipv4 show dynamicportrange protocol=tcp
```

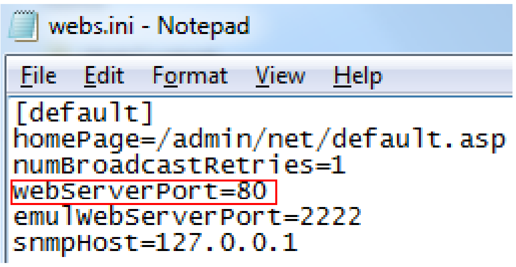
Configuring the HTTP Port on Scopia ECS Gatekeeper

About this task

Scopia ECS Gatekeeper has designated port 80 for HTTP. You can configure a different port to use HTTP (for example, if port 80 is busy).

Procedure

1. Navigate to: **C:\Program Files\RADVISION\Shared Applications\WebServer**.
2. Open the **webs.ini** file.
3. Locate the line that begins with `webserverport=` and modify the port value (see Figure 18: webs.ini File on page 64).



```
[default]
homePage=/admin/net/default.asp
numBroadcastRetries=1
webServerPort=80
emulWebServerPort=2222
snmpHost=127.0.0.1
```

Figure 18: webs.ini File

4. Access the Windows Services and restart the **ECS Web Service**.

Configuring the TCP Port for the Alternate Gatekeeper Protocol on Scopia ECS Gatekeeper

About this task

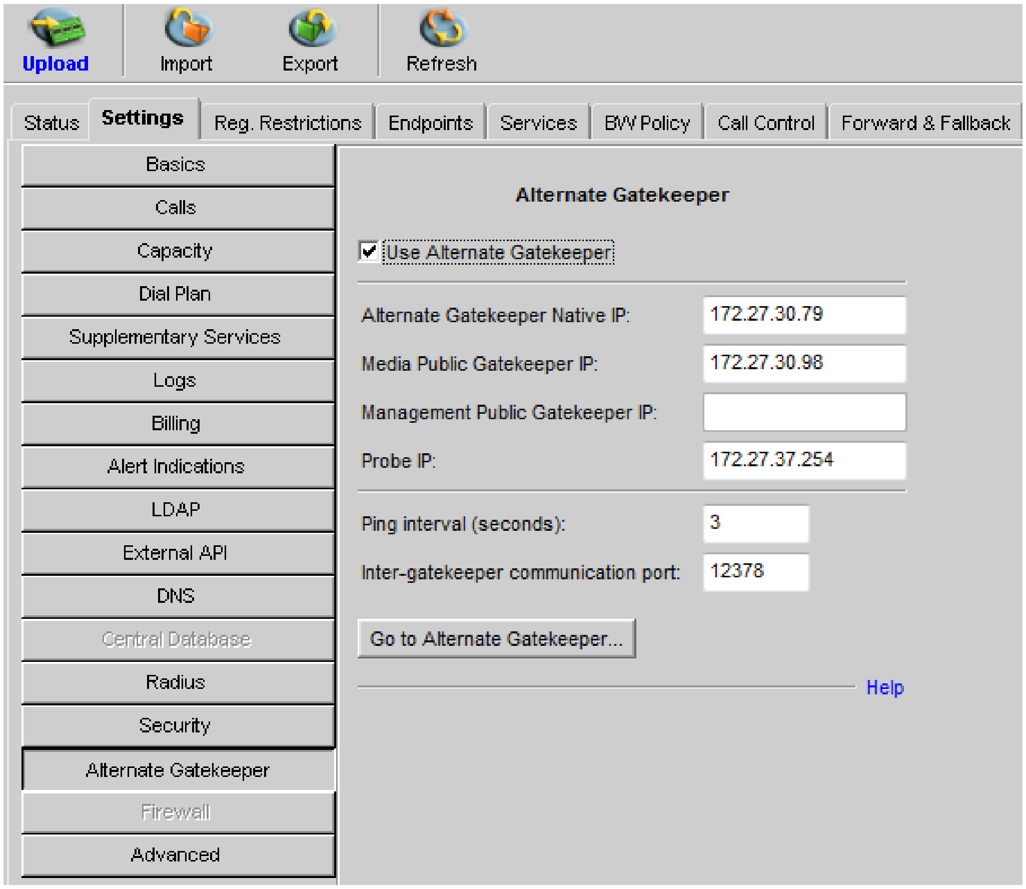
Scopia ECS Gatekeeper has designated port 12378 for the proprietary Alternate Gatekeeper protocol. You can configure a different port to use the Alternate Gatekeeper protocol (for example, if port 12378 is busy).

Important:

Opening or configuring this port is only relevant when your redundant (alternate) gatekeeper is separated from the main gatekeeper by a firewall.

Procedure

1. Log in to the ECS.
2. Select the **Settings** tab.
3. Select **Alternate Gatekeeper** (see Figure 19: Alternate Gatekeeper Settings on page 65).



Alternate Gatekeeper

☑ Use Alternate Gatekeeper

Alternate Gatekeeper Native IP: 172.27.30.79

Media Public Gatekeeper IP: 172.27.30.98

Management Public Gatekeeper IP:

Probe IP: 172.27.37.254

Ping interval (seconds): 3

Inter-gatekeeper communication port: 12378

Figure 19: Alternate Gatekeeper Settings

4. Modify the port value in the **Inter-gatekeeper communication port** field.
5. Select **Upload**.
6. Select **Go to Alternate Gatekeeper**. A new window opens, displaying the web user interface of the alternate gatekeeper.
7. Select the **Settings** tab in the web user interface of the alternate gatekeeper.
8. Select **Alternate Gatekeeper**.
9. Enter the same port value that you gave to the other gatekeeper in the **Inter-gatekeeper communication port** field.
10. Select **Upload**.
11. To log out of the web user interface, select **Logout**.

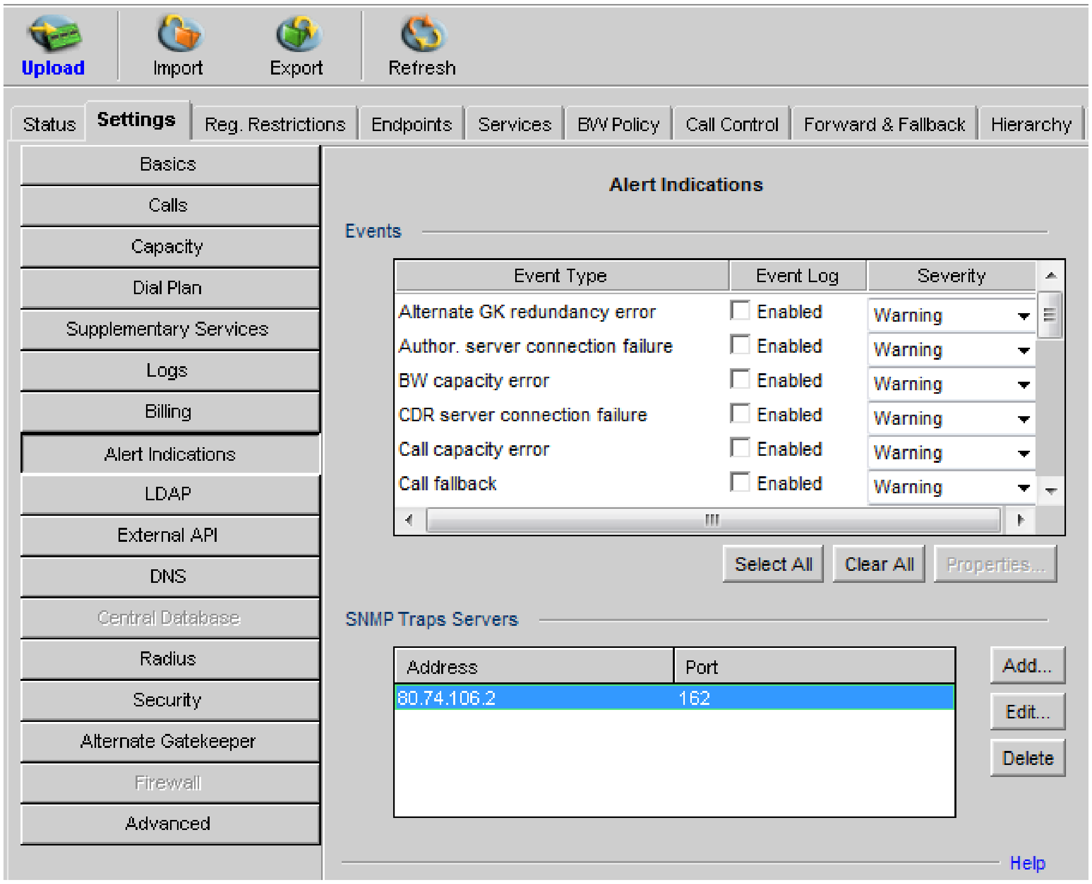
Configuring the UDP Port for SNMP Traps on Scopia ECS Gatekeeper

About this task

Scopia ECS Gatekeeper has designated port 162 for SNMP traps, to manage statuses and error log handling. You can configure a different port to use SNMP traps (for example, if port 162 is busy).

Procedure

1. Log in to the ECS.
2. Select the **Settings** tab.
3. Select **Alert Indications** (see Figure 20: Alert Indications Settings on page 66).



Alert Indications

Events

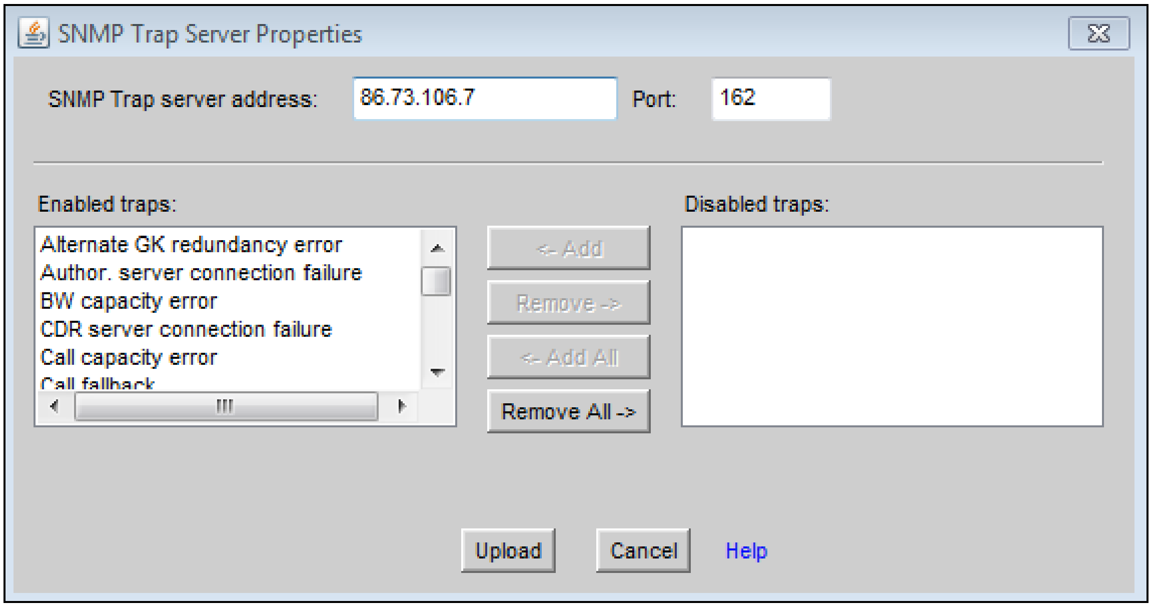
Event Type	Event Log	Severity
Alternate GK redundancy error	□ Enabled	Warning
Author. server connection failure	□ Enabled	Warning
BW capacity error	□ Enabled	Warning
CDR server connection failure	□ Enabled	Warning
Call capacity error	□ Enabled	Warning
Call fallback	□ Enabled	Warning

SNMP Traps Servers

Address	Port
80.74.106.2	162

Figure 20: Alert Indications Settings

4. Locate the **SNMP Traps Servers** area and select the IP address of the computer that receives traps.
5. Select **Edit**. The **SNMP Trap Server Properties** dialog box appears (see Figure 21: SNMP Trap Server Properties on page 67).



SNMP Trap Server Properties

SNMP Trap server address: 86.73.106.7

Port: 162

Enabled traps:

Alternate GK redundancy error
Author. server connection failure
BW capacity error
CDR server connection failure
Call capacity error
Call fallback

Disabled traps:

Figure 21: SNMP Trap Server Properties

6. Modify the port value in the **Port** field.

7. Select **Upload**.

8. To log out of the web user interface, select **Logout**.

Chapter 8 | Implementing Port Security for the Scopia XT Desktop Server

This section details the ports used for the Scopia XT Desktop Server and the relevant configuration procedures:

Navigation

Ports to Open for the Scopia XT Desktop Server

The Scopia XT Desktop Server is typically located in the DMZ, and is connected to the enterprise and public networks.

When opening ports between the DMZ and the enterprise, use the following as a reference:

- For a list of ports that are both to and from the Scopia XT Desktop Server, see Table 29: Bidirectional Ports to Open Between the Scopia XT Desktop Server and the Enterprise on page 69.
- For a list of outbound ports from the Scopia XT Desktop Server, see Table 30: Outbound Ports to Open from the Scopia XT Desktop Server to the EnterpriseScopia Desktop on page 69.
- For a list of inbound ports to the Scopia XT Desktop Server, see Table 31: Inbound Ports to Open from the Enterprise to the Scopia XT Desktop Server on page 70.

When opening ports between the DMZ and the public, use the following as a reference:

- For a list of ports that are both to and from the Scopia XT Desktop Server, see Table 32: Bidirectional Ports to Open Between the Scopia XT Desktop Server and the Public on page 70.
- For a list of inbound ports to the Scopia XT Desktop Server, see Table 33: Inbound Ports to Open from the Public to the Scopia XT Desktop Server on page 71.

Table 29: Bidirectional Ports to Open Between the Scopia XT Desktop Server and the Enterprise

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
1025-65535	H.245/ Q.931 (TCP)	Scopia XT1000 Series	Enables H.323 traffic between the Scopia XT Desktop Server and the Scopia XT1000 Series	Scopia XT Desktop calls do not work	Mandatory To limit range, see Limiting the TCP Port Range on the Scopia XT Desktop Server on page 71Limiting the TCP Port Range on the Scopia XT Desktop Server on page 71
10000-65535	RTP/RTCP (UDP)	Scopia XT Desktop Client	Enables media connection with the Scopia XT Desktop Client	Connection is tunneled via TCP port 443 and performance is not optimal	Recommended To limit range, see Limiting the UDP Port Range on the Scopia XT Desktop Server on page 72

Table 30: Outbound Ports to Open from the Scopia XT Desktop Server to the EnterpriseScopia Desktop

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3336, 3337	XML (TCP)	Scopia XT1000 Series	Enables cascading/ XML control connections between Scopia XT Desktop Server and Scopia XT1000 Series	Scopia XT Desktop calls do not work	Mandatory

Table 31: Inbound Ports to Open from the Enterprise to the Scopia XT Desktop Server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
80	HTTP (TCP)	Web client	Provides access to the Scopia XT Desktop web user interface (you can configure port 443 instead)	Cannot access the web user interface	Mandatory if using HTTP. You can configure this port during installation. For more information, see the Installing Scopia XT Desktop Server section in the *Installation Guide for Scopia XT Desktop Server.*
443	HTTPS (TCP)	Scopia XT Desktop Client	Enables sending control messages between the Scopia XT Desktop client and server, and is also used to tunnel RTP media if the UDP ports are blocked	Scopia XT Desktop client cannot connect to the Scopia XT Desktop Server	Mandatory

Table 32: Bidirectional Ports to Open Between the Scopia XT Desktop Server and the Public

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
10000-65535	RTP/ RTCP (UDP)	Scopia XT Desktop Client	Enables media connection to the Scopia XT Desktop Client	Connection is tunneled via TCP port 443 and performance is not optimal	Recommended To limit range, see Limiting the UDP Port Range on the Scopia XT Desktop Server on page 72

Table 33: Inbound Ports to Open from the Public to the Scopia XT Desktop Server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
80	HTTP (TCP)	Web client	Provides access to the Scopia XT Desktop Server web user interface (you can configure port 443 instead)	Cannot access the web user interface	Mandatory if using HTTP. You can configure this port during installation. For more information, see the Installing Scopia XT Desktop Server section in the *Installation Guide for Scopia XT Desktop Server.*
443	HTTPS (TCP)	Scopia XT Desktop Client	Enables connection to the Scopia XT Desktop Client	Cannot connect to the Scopia XT Desktop Client	Mandatory

Limiting Port Ranges on the Scopia XT Desktop Server

This section provides instructions of how to limit the following port ranges on the Scopia XT Desktop Server:

Navigation

- Limiting the TCP Port Range on the Scopia XT Desktop Server on page 71
- Limiting the UDP Port Range on the Scopia XT Desktop Server on page 72

Limiting the TCP Port Range on the Scopia XT Desktop Server

About this task

The Scopia XT Desktop Server has designated ports 1025-65535 for TCP (H.245 and Q.931 signaling). To provide additional security for your firewall, you can limit this range.

For each conference, the Scopia XT Desktop Server uses 2 ports for the conference and an additional 2 ports for each participating Scopia XT Desktop client.

Procedure

1. Navigate to **C:\Program Files\Radvision\Scopia XT Desktop\ConfSrv**.
2. Edit the **config.val** file as follows:

   a. Locate the **[1 system]** section.

   b. At the bottom of that section, add two lines:

   ```
   2 portFrom = <lowest range limit>
   2 portTo = <highest range limit>
   ```

   Where `<lowest range limit>` is the base port of your port range and `<highest range limit>` is the upper value of your port range.
3. Access the Windows services and restart the **Scopia XT Desktop Server - Conference Server** service.

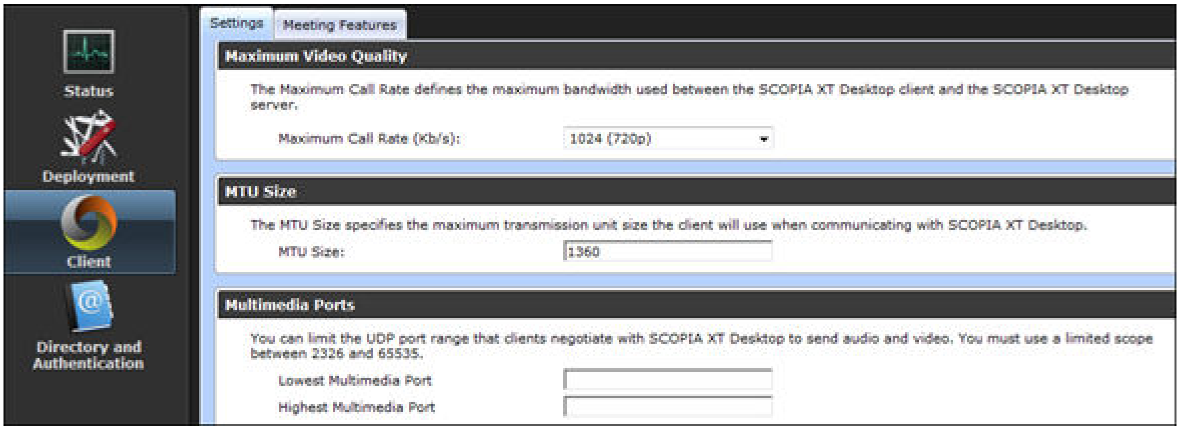
Limiting the UDP Port Range on the Scopia XT Desktop Server

About this task

The Scopia XT Desktop Server has designated 10000-65535 as the default port range for UDP. At full capacity, the SCOPIA XT1009 requires 76 ports. To provide additional security for your firewall, you can limit this range.

Procedure

1. Log in to the Scopia XT Desktop Server Administrator web user interface.
2. Select **Client > Settings.**
3. Locate the **Multimedia Ports** section (see Figure 22: UDP Multimedia Ports on page 72).



Maximum Video Quality

The Maximum Call Rate defines the maximum bandwidth used between the SCOPIA XT Desktop client and the SCOPIA XT Desktop server.

Maximum Call Rate (Kb/s): 1024 (720p)

MTU Size

The MTU Size specifies the maximum transmission unit size the client will use when communicating with SCOPIA XT Desktop.

MTU Size: 1360

Multimedia Ports

You can limit the UDP port range that clients negotiate with SCOPIA XT Desktop to send audio and video. You must use a limited scope between 2326 and 65535.

Lowest Multimedia Port

Highest Multimedia Port

Figure 22: UDP Multimedia Ports

4. Configure your port range (using any values between 2326 and 65535) by doing the following:

    a. Enter the base port value in the **Lowest Multimedia Port** field.

    b. Enter the upper port value in the **Highest Multimedia Port** field.

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

Chapter 9 | Implementing Port Security for the Scopia XT Series

The Scopia XT Series provides video technology for room conferencing, including support for dual stream 1080p video, high quality data sharing, high quality full band audio and a high-capacity embedded MCU (selected models).

This section details the ports used for the Scopia XT Series and the relevant configuration procedures:

Navigation

- Ports to Open on the XT Series on page 74
- Configuring the TCP or UDP Port Range on the Scopia XT Series on page 76

Ports to Open on the XT Series

The Scopia XT Series is typically located in the enterprise network and is connected to the DMZ. When opening ports to and from the Scopia XT Series, use the following as a reference:

- If you are opening ports that are both to and from the XT Series, see Table 34: Bidirectional Ports to Open on the XT Series on page 74.
- If you are opening outbound ports from the XT Series, see Table 35: Outbound Ports to Open from the Scopia XT Series on page 76.

Important:

The specific firewalls you need to open ports on depends on where your XT Series and other Scopia Solution products are deployed.

Table 34: Bidirectional Ports to Open on the XT Series

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
69	TFTP (UDP)	TFTP client or server	Enables sending and receiving files via TFTP	Cannot send or receive files via TFTP	Optional
80	HTTP (TCP)	Web server	Enables you to remotely perform management tasks via the web user interface, enables NAT auto-discovery via HTTP	**In**: Cannot access the web server **Out**: Cannot access the web server and NAT auto-discovery via HTTP does not function	Recommended

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
123	SNTP (UDP)	SNTP client	Gets the Internet UTC time	Cannot get the Internet UTC time	Recommended
161	SNMP (UDP)	Scopia Management or an SNMP manager station	Enables you to configure and check the system status	Cannot configure or check the status of the system via SNMP	Mandatory if using SNMP manager station
1719	H.225.0/ RAS (UDP)	Any H.323 video network device	Enables H.323 call signaling to a gatekeeper; H.323 endpoints can use gatekeeper services.	H.323 endpoints cannot use gatekeeper services	Mandatory if using a gatekeeper
1720	H.225.0/ Q.931 (TCP)	Any H.323 video network device	Enables H.323 call signaling (Q.931)	Cannot connect H.323 calls	Mandatory
3230-3248	H.225.0/Q.931/ H.245/ SIP (TCP)	Any H.323/SIP video network device	Enables H.323 call control signaling (Q.931), media control signaling (H.245), SIP (TCP) call signaling, and BFCP signaling. Ephemeral TCP ports are used to connect simultaneous H.323 and SIP calls.	Cannot connect SIP/H.323 calls	Mandatory To configure, see Configuring the TCP or UDP Port Range on the Scopia XT Series on page 76
3230-3305	RTP and RTCP (UDP)	Any H.323 video network device	Enables H.323 and SIP media (audio, video, H.224/data RTP) and media control (RTCP). Ephemeral UDP ports are used to connect simultaneous H.323 and SIP media calls.	No media exchanged in H.323 or SIP calls	Mandatory To configure, see Configuring the TCP or UDP Port Range on the Scopia XT Series on page 76
3338	XML Commands (TCP)	Scopia Control, Scopia XT Desktop Server	Enables communication with Scopia Control and Scopia XT Desktop Server by sending commands and receiving responses	Cannot communicate with Scopia Control application or and Scopia XT Desktop Server	Optional
3478, 3479	STUN (UDP)	STUN Server	Enables endpoints to automatically discover the presence of a firewall or NAT, and to determine their public IP address.	Cannot automatically discover the presence of a firewall or NAT (only manual configuration available)	Optional
5060	SIP (TCP)	Any SIP-enabled video network device	Enables SIP call signaling	Cannot connect SIP calls over TCP	Mandatory
5060	SIP (UDP)	Any SIP-enabled video network device	Enables SIP call signaling	Cannot connect SIP calls over UDP	Mandatory

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
5070	BFCP (TCP)	Any SIP-enabled video network device	Enables SIP video content (presentation) signaling	No SIP video content available	Mandatory
55003	AT Commands (TCP)	Scopia Management	Enables you to remotely manage the XT Series via API	Cannot send/ receive commands	Optional
55099	Software Upgrade (TCP)	Scopia Management/ XT Series Software Upgrade application	Enables software upgrade	Cannot upgrade software	Recommended
60123	Telnet (TCP)	Telnet server	Enables remote management via Telnet	No Telnet access	Optional

Table 35: Outbound Ports to Open from the Scopia XT Series

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
162	SNMP (UDP)	Scopia Management or an SNMP manager station	Enables sending SNMP trap events	Endpoints cannot send SNMP events	Optional
1718	H.225.0/ RAS (UDP)	Multicast IP address 224.0.1.41 (all gatekeepers)	Enables H.323 endpoints to automatically identify the gatekeeper to register with	H.323 endpoints can only register with a predefined gatekeeper	Recommended
3339, 3340	XML HINTS (TCP)	Scopia Control, Scopia XT Desktop Server	Enables receiving system status alerts	Cannot send system status alerts; Scopia Control and Scopia XT Desktop Server cannot function.	Optional

Configuring the TCP or UDP Port Range on the Scopia XT Series

About this task

You can configure the TCP or UDP port range by setting the base port, which is the lower end of the port range (if, for example, port 3230 is busy).

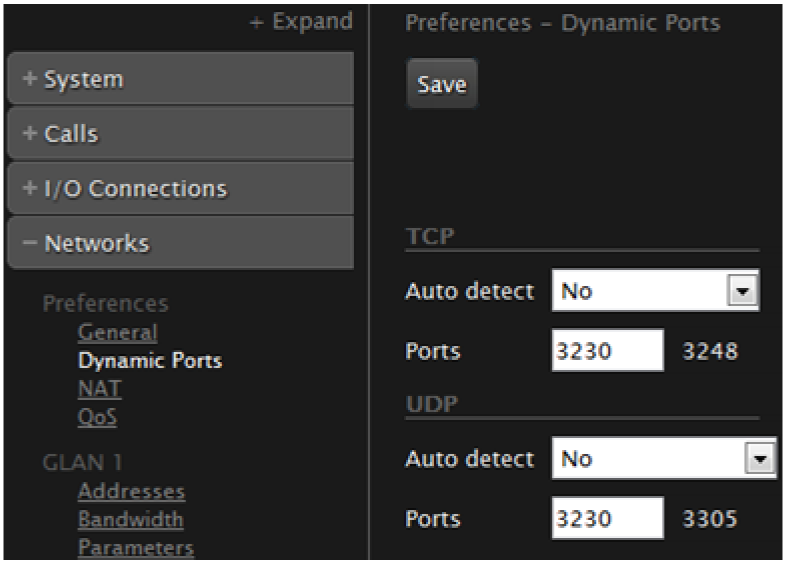
The Scopia XT Series uses dynamic TCP ports 3230-3248 for the following:

- H.225.0: An H.323 protocol that specifies the messages and procedures used by gatekeepers to set up calls.
- Q.931:A telephony protocol used for establishing and terminating the connection in H.323 calls.
- H.245: A Control Protocol used for multimedia communication; enables transferring information about the device capabilities, as well as opening/closing the logical channels that carry media streams.
- SIP: A signaling protocol used for creating, modifying, or terminating multimedia connections between two or more participants.

The Scopia XT Series uses dynamic UDP ports 3230-3248 for enabling real-time H.323 and SIP media, including audio, video, and H.224/data (RTP), and media control (RTCP).

Procedure

1. Access the port settings as follows:
   - From the web interface, select **Administrator Settings > Networks > Preferences > Dynamic Ports.**
   - From the endpoint interface, select **Configure > Advanced > Networks > Preferences > Dynamic Ports**.



Preferences - Dynamic Ports

TCP

Auto detect: No

Ports: 3230 3248

UDP

Auto detect: No

Ports: 3230 3305

Figure 23: Configuring the TCP or UDP port range from the web interface

2. Define how the XT Codec Unit assigns ports by selecting one of the following from **Auto detect**:
   - **No**: The XT Codec Unit uses the range of dynamic ports indicated and allows you to define the base port (default and recommended setting).
   - **Yes**: The XT Codec Unit assigns ports randomly, and you cannot define the base port.
3. If you selected **No** in the **Auto detect** list, you can modify the TCP or UDP base port in the **Ports** field.

Important:

You can configure the base port to any value between 1024-65535. The number of ports is calculated automatically by the system, depending on whether you have an MCU license and its type.

4. From the web interface only, select **Save**.

Chapter 10 | Implementing Port Security for the Scopia VC240

The Scopia VC240, an H.460 endpoint, is a high resolution desktop monitor with integrated HD videoconferencing. It can be located in the enterprise (internal), public, or partner networks.

This section details the ports used for the Scopia VC240 and the relevant port configuration procedures:

Navigation

Ports to Open for Scopia VC240

The Scopia VC240 is typically located in the public or enterprise network.

When opening ports to and from the Scopia VC240, use the following as a reference:

- If opening ports that are both to and from the Scopia VC240, see Table 36: Bidirectional Ports to Open on the Scopia VC240 on page 79.
- If opening outbound ports from the Scopia VC240, see Table 37: Outbound Ports to Open from the Scopia VC240 on page 80.
- If opening inbound ports to the Scopia VC240, see Table 38: Inbound Ports to Open to the Scopia VC240 on page 81.

Important:

The specific firewalls you need to open ports on depends on where your Scopia VC240 and other Scopia Solution products are deployed.

Table 36: Bidirectional Ports to Open on the Scopia VC240

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
22	SSH (TCP)	SSH Server	Enables remote software upgrades via Scopia Management	Cannot connect to Scopia Management	Recommended for software upgrades
23	Telnet (TCP)	Scopia Management	Enables you to configure the Scopia VC240 via Scopia Management	Cannot connect to Scopia Management	Recommended

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
69	TFTP (UDP)	TFTP Server	Enables software upgrade via device menus	Cannot perform software upgrades via TFTP	Optional
1719	RAS (UDP)	H.323 gatekeeper	Enables RAS signaling	Cannot communicate with H.323 gatekeeper	Recommended
1720	Q.931 (TCP)	Any H.323 device	Enables Q.931 signaling	Cannot connect H.323 calls	Recommended
3230-3241	H.245 (TCP)	Any H.323 device	Enables H.245 signaling	Cannot connect H.323 calls	Mandatory To configure base port, see Configuring the TCP Port Range for H.245 on the Scopia VC240 on page 81
3230-3251	RTP/ RTCP (UDP)	Any H.323 or SIP media- enabled video network device	Enables delivery of real-time media	Cannot transmit/ receive media streams	Mandatory To configure base port, see Configuring the UDP Port Range for RTP/RTCP on the Scopia VC240 on page 81
4000	RV shell cmd (UDP)	Scopia Management	Internal use Enables connection to Scopia Management	Cannot connect to Scopia Management	
5060	SIP (TCP/UDP)	Any SIP video network device	Enables SIP signaling	Cannot connect SIP calls	Mandatory if using SIP
22444	HTTP (TCP)	Web application or open API-based application	Provides access to the web user interface, enables use of open APIs (for remote access and remote software upgrades)	Cannot access the web user interface or use open APIs	Mandatory if performing web-based software upgrades

Table 37: Outbound Ports to Open from the Scopia VC240

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
162	SNMP (UDP)	Scopia Management, Scopia Management or any SNMP manager station	Enables sending SNMP trap events	Cannot send traps	Mandatory if using a Network Manager

Table 38: Inbound Ports to Open to the Scopia VC240

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
161	SNMP (UDP)	Scopia Management, Scopia Management or any SNMP manager station	Enables you to configure and check the endpoint status	Cannot configure or check the endpoint status via SNMP	Mandatory if using a Network Manager
22445	HTTPS (TCP)	Web application or open API-based application	Provides secure access to the web user interface and enables use of open APIs	Cannot access the web user interface via HTTPS or use open APIs	Mandatory if using HTTPS

Configuring Port Ranges on the Scopia VC240

This section provides instructions of how to configure the following port ranges on the Scopia VC240:

Navigation

- Configuring the TCP Port Range for H.245 on the Scopia VC240 on page 81
- Configuring the UDP Port Range for RTP/RTCP on the Scopia VC240 on page 81

Configuring the TCP Port Range for H.245 on the Scopia VC240

About this task

The Scopia VC240 has designated ports 3230-3242 for H.245. You can configure the base port (for example, if port 3230 has another application running on it). The Scopia VC240 uses 12 ports for H.245. H.245 is a Control Protocol used for multimedia communication that enables transferring information about the device capabilities, as well as opening/closing the logical channels that carry media streams.

Procedure

1. Using your remote control, select **Setup > Network > Port Configuration**.
2. Modify the base port using your remote control in the **TCP** field on your screen.
3. Select **OK**.

Configuring the UDP Port Range for RTP/RTCP on the Scopia VC240

About this task

The Scopia VC240 has designated ports 3230-3251 for RTP/RTCP. You can configure the base port (for example, if port 3230 has another application running on it). The Scopia VC240 uses 22 ports for RTP/RTCP.

Procedure

1. Using your remote control, select **Setup > Network > Port Configuration**.
2. Modify the base port using your remote control in the **UDP** field on your screen.
3. Select **OK**.

Chapter 11 | Implementing Port Security for the Scopia Gateway

The Scopia Gateway provides seamless connectivity between different networks and standards to deliver feature-rich, reliable, multimedia conferencing and communications.

This section details the ports used for the Scopia Gateway and the relevant configuration procedures:

Navigation

- Ports to Open on the Scopia Gateway on page 83
- Configuring Ports on the Scopia Gateway on page 85
- Configuring Security Access Levels for the Scopia Gateway on page 89

Ports to Open on the Scopia Gateway

The Scopia Gateway is typically located in the enterprise and ISDN networks.

When opening ports on the Scopia Gateway, use the following as a reference:

- If opening ports that are both to and from the Scopia Gateway, see Table 39: Bidirectional Ports to Open on the Scopia Gateway on page 83.
- If opening outbound ports from the Scopia Gateway, see Table 40: Outbound Ports to Open from the Scopia Gateway on page 85.
-

Important:

The specific firewalls you need to open ports on depends on where your Scopia Gateway and other Scopia Solution products are deployed.

Table 39: Bidirectional Ports to Open on the Scopia Gateway

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
21	FTP (TCP)	Upgrade Utility	Enables you to perform software upgrades	Cannot upgrade version or extract recordings	Mandatory
23	Telnet (TCP)	Telnet client	Enables you to view logs	Cannot view logs	Recommended

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
80	HTTP (TCP)	Web client	Provides access to the web user interface	Cannot view Scopia Gateway web user interface	Mandatory if using HTTP To configure, see Configuring the HTTP Port on the Scopia Gateway on page 86
161	SNMP (UDP)	Web client, Scopia Management or any SNMP manager station	Enables you to configure and check the Scopia Gateway status	Cannot configure or check the Scopia Gateway status via SNMP	Mandatory
443	HTTPS (TCP)		Provides secure access to the web user interface	Cannot administer the Scopia Gateway	Mandatory if using HTTPS
1024-4999	H.245 (TCP)	H.323 device	Enables H.245 signaling	No H.245	Mandatory if using H.245
1503	TCP	Any T.120 endpoint	Enables T.120 data collaboration	Cannot establish a T.120 connection to/from the Scopia Gateway	Optional
1619	RAS (UDP) — IVR	Gatekeeper	Enables RAS signaling (receiving Gatekeeper notifications)	No RAS signaling	Mandatory if communicating with the Gatekeeper
1620	Q.931 (TCP) — IVR	H.323 device	Enables Q.931 signaling	No signaling capabilities	Mandatory if using IVR functionality
1719	RAS (UDP)	Gatekeeper	Enables RAS signaling (receiving Gatekeeper notifications)	No RAS signaling	Mandatory if communicating with the Gatekeeper To configure, see Configuring the Gatekeeper Port on the Scopia Gateway on page 86
1719	RAS (UDP)	H.323 device	Enables RAS capabilities (sending RRQ/ARQ messages)	No RAS capabilities	Mandatory
1720	Q.931 (TCP)	H.323 device	Enables Q.931 capabilities (sending Setup/Connect messages)	No Q.931 capabilities	Mandatory if working in Peer-to-Peer mode To configure, see Configuring the TCP Port for Q.931 on the Scopia Gateway on page 87

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
1820	Q.931 (TCP)	H.323 device	Enables Q.931 signaling (receiving Setup messages)	No signaling capabilities	Mandatory if working with Gatekeeper To configure, see Configuring the TCP Port for Q.931 on the Scopia Gateway on page 87
7222-7422 (even numbers only)	RTP (UDP)	H.323 device	Enables delivery of IVR media (audio)	Cannot open IVR audio via RTP	Mandatory
7223-7421 (odd numbers only)	RTCP (UDP)	H.323 device	Enables delivery of IVR media (audio)	Cannot open IVR audio via RTCP	Mandatory
7622-7822 (even numbers only)	RTP (UDP)	H.323 device	Enables delivery of IVR media (video)	Cannot open IVR video via RTP	Mandatory
7623-7821 (odd numbers only)	RTCP (UDP)	H.323 device	Enables delivery of IVR media (video)	Cannot open IVR video via RTCP	Mandatory
12002-12952 (even numbers only)	RTP (UDP)	H.323 device	Enables real-time delivery of media to endpoints connected to the Scopia Gateway and not to the IVR	Cannot transmit/ receive media streams	Mandatory
12003-12951 (odd numbers only)	RTCP (UDP)	H.323 device	Enables real-time delivery of media to endpoints connected to the Scopia Gateway and not to the IVR	Cannot transmit/ receive media streams	Mandatory

Table 40: Outbound Ports to Open from the Scopia Gateway

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
162	SNMP traps (UDP)	Scopia Gateway	Enables sending traps	Cannot send traps	Mandatory

Configuring Ports on the Scopia Gateway

This section provides instructions of how to configure the following ports and port ranges on the Scopia Gateway:

Navigation

- Configuring the HTTP Port on the Scopia Gateway on page 86

- Configuring the Gatekeeper Port on the Scopia Gateway on page 86
- Configuring the TCP Port for Q.931 on the Scopia Gateway on page 87

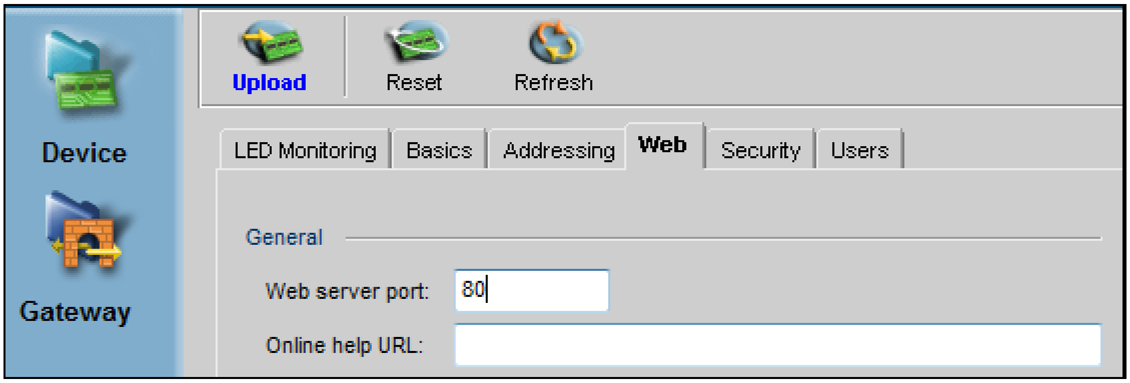
Configuring the HTTP Port on the Scopia Gateway

About this task

The Scopia Gateway has designated port 80 for HTTP. You can configure a different port to use HTTP (for example, if port 80 is busy).

Procedure

1. Log in to the Scopia Gateway.
2. Do one of the following, depending on how your Scopia Gateway is installed:
   - Select **Board** > **Web** if your Scopia Gateway is installed in the chassis.
   - Select **Device** > **Web** if your Scopia Gateway is installed as a standalone.
3. Modify the port value in the Web Server Port field (see Figure 24: Scopia Gateway Web Settings on page 86).



Web server port: 80

Online help URL:

Figure 24: Scopia Gateway Web Settings

4. Select **Upload**.

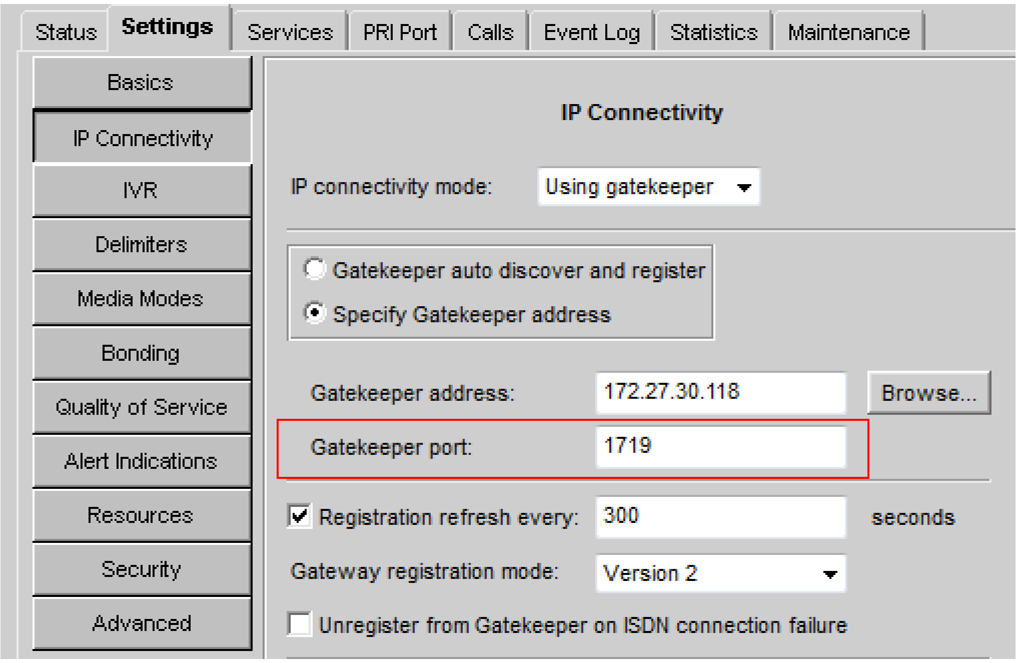
Configuring the Gatekeeper Port on the Scopia Gateway

About this task

The Scopia Gateway has designated port 1719 for the communication with the Gatekeeper. You can configure a different port to communicate with the Gatekeeper (for example, if port 1719 is busy).

Procedure

1. Log in to the Scopia Gateway.
2. Select **Gateway** > **Settings** tab.
3. Select **IP Connectivity** (see Figure 25: Gatekeeper Port Settings on page 87).



IP Connectivity

IP connectivity mode: Using gatekeeper

○ Gatekeeper auto discover and register

● Specify Gatekeeper address

Gatekeeper address: 172.27.30.118

Gatekeeper port: 1719

☑ Registration refresh every: 300 seconds

Gateway registration mode: Version 2

□ Unregister from Gatekeeper on ISDN connection failure

Figure 25: Gatekeeper Port Settings

4. Modify the port value in the **Gatekeeper port** field.
5. Select **Upload**.

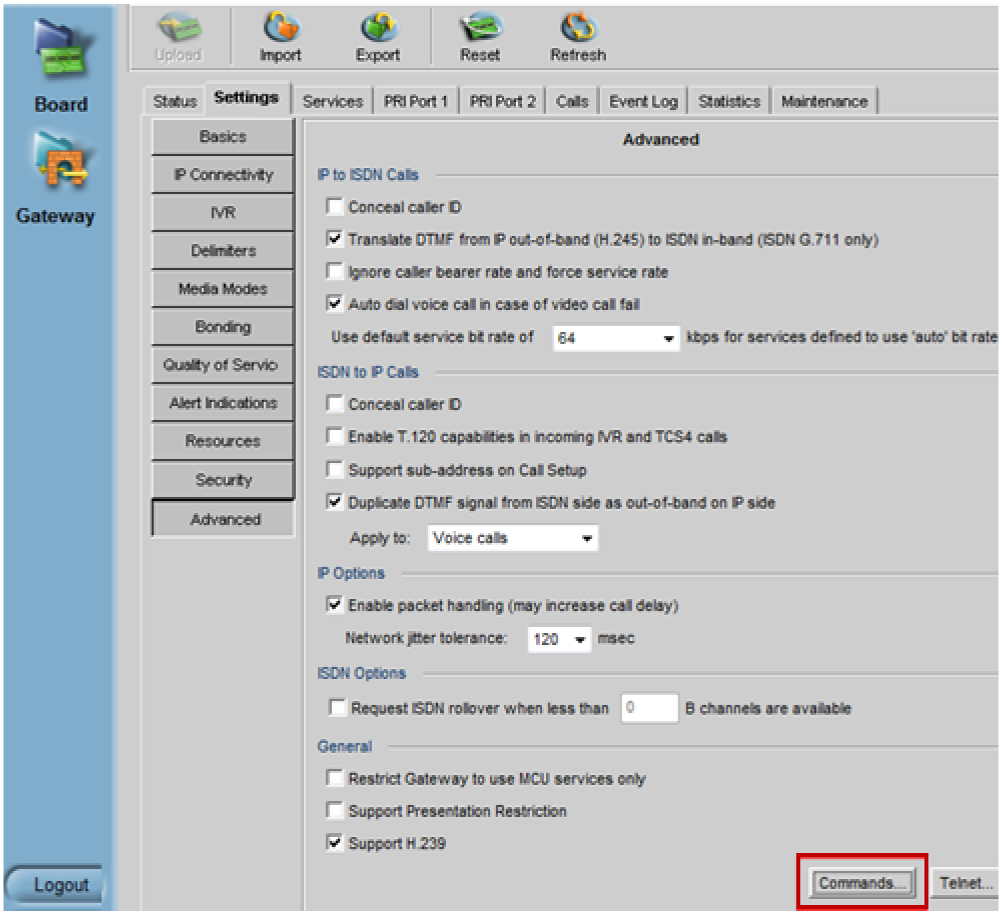
Configuring the TCP Port for Q.931 on the Scopia Gateway

About this task

The Scopia Gateway has designated ports 1720 or 1820 for Q.931 signaling, depending on deployment. Q.931 is a telephony protocol used for establishing and terminating the connections in H.323 calls. If you are working in peer-to-peer mode, with H.323 endpoints communicating with each other directly, the default port is 1720. If you are working with the gatekeeper, the default port is 1820. You can configure a different port for Q.931.

Procedure

1. Log in to the Scopia Gateway.
2. Select **Gateway** > **Settings** > **Advanced** (see Figure 26: Scopia Gateway Advanced Settings on page 88).



Advanced

IP to ISDN Calls

- □ Conceal caller ID
- ☑ Translate DTMF from IP out-of-band (H.245) to ISDN in-band (ISDN G.711 only)
- □ Ignore caller bearer rate and force service rate
- ☑ Auto dial voice call in case of video call fail

Use default service bit rate of 64 kbps for services defined to use 'auto' bit rate

ISDN to IP Calls

- □ Conceal caller ID
- □ Enable T.120 capabilities in incoming IVR and TCS4 calls
- □ Support sub-address on Call Setup
- ☑ Duplicate DTMF signal from ISDN side as out-of-band on IP side

Apply to: Voice calls

IP Options

- ☑ Enable packet handling (may increase call delay)

Network jitter tolerance: 120 msec

ISDN Options

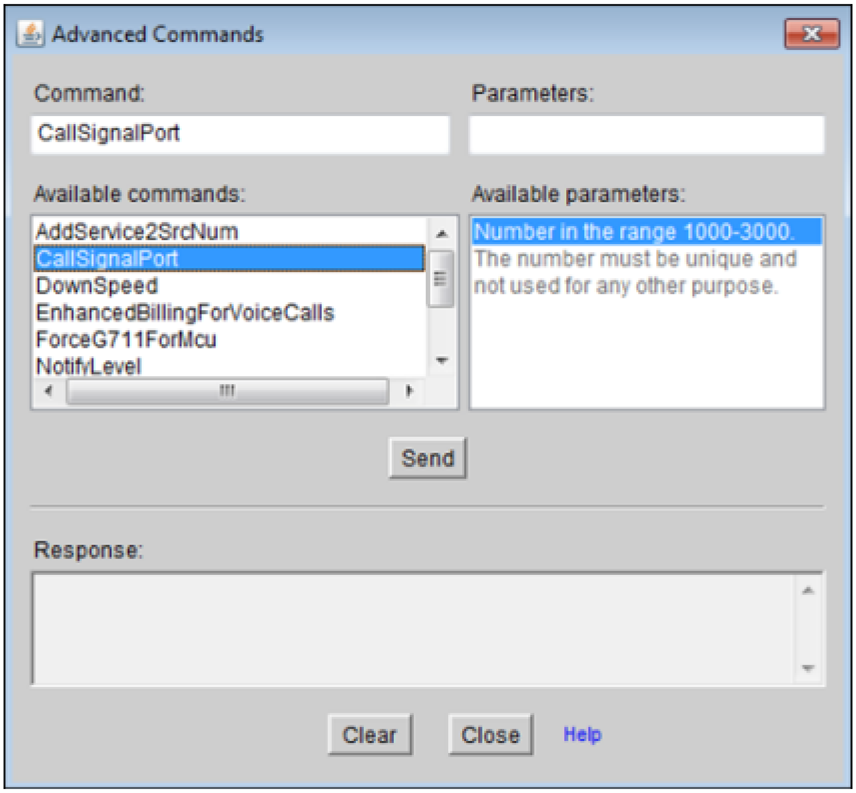
- □ Request ISDN rollover when less than 0 B channels are available

General

- □ Restrict Gateway to use MCU services only
- □ Support Presentation Restriction
- ☑ Support H.239

Figure 26: Scopia Gateway Advanced Settings

3. Select **Commands**. The **Advanced Commands** dialog box appears (see Figure 27: Scopia Gateway Advanced Commands on page 89).



Command: CallSignalPort

Parameters:

Available commands:

AddService2SrcNum
CallSignalPort
DownSpeed
EnhancedBillingForVoiceCalls
ForceG711ForMcu
NotifyLevel

Available parameters:

Number in the range 1000-3000.
The number must be unique and not used for any other purpose.

Response:

Figure 27: Scopia Gateway Advanced Commands

4. Select **CallSignalPort** from the **Available Commands** list.

5. Enter the port value in the **Parameters** field.

   Important:

   You can enter any value between **1000** to **3000**.

6. Select **Send**.

7. Select **Close**.

Configuring Security Access Levels for the Scopia Gateway

About this task

The Scopia Gateway offers configurable security access levels that enable and disable Telnet, FTP, SNMP and ICMP (ping) protocols, which enable you to do the following:

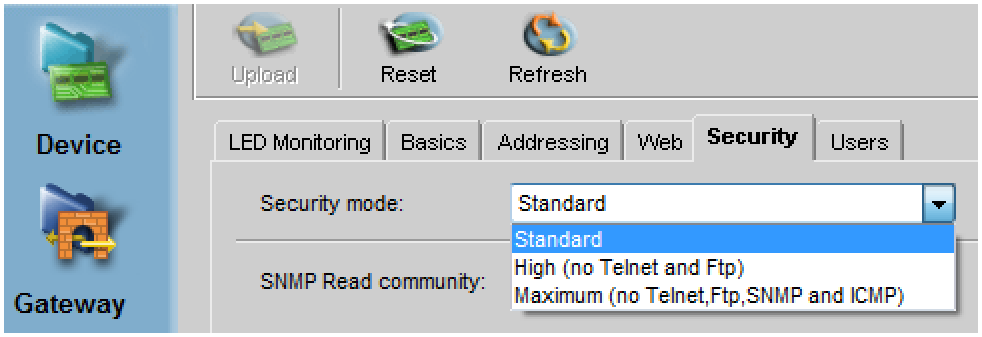
- Upgrade software via FTP.
- Access the web user interface and perform configuration procedures via SNMP.

- Access the Scopia Gateway CLI and receive logs directly via Telnet.
- Send control or error response messages via ICMP (ping).

It is recommended to enable these protocols by setting your security access level to **Standard**.

Procedure

1. Access the Scopia Gateway security settings by selecting **Device** > **Security** from the Scopia Gateway web user interface.
2. Select the access level from the **Security Mode** list (see Figure 28: Scopia Gateway Security Settings on page 90). Table 41: Scopia Gateway Security Access Levels on page 90 lists the protocol status when each security access level is applied.



Security mode: Standard

Standard
High (no Telnet and Ftp)
Maximum (no Telnet,Ftp,SNMP and ICMP)

SNMP Read community:

Figure 28: Scopia Gateway Security Settings

Table 41: Scopia Gateway Security Access Levels

Security Access Level	Telnet	FTP	SNMP	ICMP (ping)
Standard	Enabled	Enabled	Enabled	Enabled
High	Disabled	Disabled	Enabled	Enabled
Maximum	Disabled	Disabled	Disabled	Disabled

3. Select **Upload.**

Chapter 12 | Implementing Port Security for the Scopia 3G Gateway

The Scopia 3G Gateway bridges 3G-324M-based mobile devices with IP-based videoconferencing systems and infrastructure for the delivery of video services to a variety of handsets.

This section details the ports used for the Scopia 3G Gateway and the MVP/M II SP for Scopia 3G Gateway and the relevant configuration procedures:

Navigation

Ports to Open on the Scopia 3G Gateway

The Media Blade is typically located in the enterprise and is connected to the DMZ.

When opening ports to and from the Media Blade, use the following as a reference:

- If opening ports that are both to and from the Media Blade, see Table 42: Bidirectional Ports to Open on the Media Blade on page 91.
- If opening outbound ports from the Media Blade, see Table 43: Outbound Ports to Open from the Media Blade on page 93.
- If opening inbound ports to the Media Blade, see Table 44: Inbound Ports to Open to the Media Blade on page 93.

Important:

The specific firewalls you need to open ports on depends on where your Media Blade and other Scopia Solution products are deployed.

Table 42: Bidirectional Ports to Open on the Media Blade

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
21	FTP (TCP)	Upgrade Utility	Enables you to upgrade software	Cannot upgrade version	Recommended
23	Telnet (TCP)	Telnet client	Enables you to view Scopia 3G Gateway logs and perform initial configuration	Cannot view logs or perform initial configuration	Recommended

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
80	HTTP (TCP)	Web client	Provides access to the MVP/M II Administrator and Call Control web user interfaces	Cannot configure Scopia 3G Gateway	Mandatory To configure, see Configuring the HTTP Port on the Scopia 3G Gateway on page 93
161	SNMP (UDP)	Scopia Management, Scopia Management, or any SNMP manager station	Enables you to configure and check the Scopia 3G Gateway status	Cannot configure or check the status of the Scopia 3G Gateway via SNMP	Recommended
443	HTTPS (TCP)	Secure web client	Provides access to a secure web interface	Cannot configure the Scopia 3G Gateway	Mandatory if using HTTPS
1024-4999	H.245 (TCP)	Any H.323 device	Enables H.245 signaling and a TCP connection to the DSI SIU.	Cannot connect H.323 calls; no connection to DSI SIU.	Mandatory
1719	RAS (UDP)	H.323 gatekeeper	Enables RAS signaling	Cannot communicate with H.323 gatekeeper	Mandatory To configure, see Configuring the UDP Port for RAS on the Scopia 3G Gateway on page 94
1820	Q.931 (TCP)	Any H.323 device	Enables Q.931 signaling	Cannot connect H.323 calls	Mandatory To configure, see Configuring the TCP Port for Q.931 on the Scopia 3G Gateway on page 96
2944, 2945	MVP control (TCP)	MVP/M II SP	Enables MVP/M II SP to connect to Scopia 3G Gateway	Cannot use external MVP	Mandatory
3336	External Control (TCP)	Scopia Management	Enables Scopia 3G Gateway External Control	Cannot control Scopia 3G Gateway	Mandatory
5060	SIP (TCP/ UDP)	Any SIP video network device	Enables SIP signaling	Cannot connect SIP calls	Mandatory To configure, see Configuring the SIP Port on the Scopia 3G Gateway on page 96

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
6000-7000	RTP/ RTCP (UDP)	Any H.323 or SIP media- enabled video network device	Enables real-time delivery of audio media	Cannot transmit/ receive audio media streams	Mandatory
12000-13000	RTP/ RTCP	Any H.323 or SIP media- enabled video network device	Enables real-time delivery of video media	Cannot transmit/ receive video media streams	Mandatory

Table 43: Outbound Ports to Open from the Media Blade

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
162	SNMP (UDP)	Scopia Management, Scopia Management, or any SNMP manager station	Enables sending SNMP Trap events	Cannot send traps	Recommended

Table 44: Inbound Ports to Open to the Media Blade

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
123	NTP (UDP)	NTP server	Enables time synchronization	Time settings are inaccurate	Recommended

Configuring Ports on the Scopia 3G Gateway

This section provides instructions of how to configure the following ports on the Scopia 3G Gateway:

Navigation

- Configuring the HTTP Port on the Scopia 3G Gateway on page 93
- Configuring the UDP Port for RAS on the Scopia 3G Gateway on page 94
- Configuring the TCP Port for Q.931 on the Scopia 3G Gateway on page 96
- Configuring the SIP Port on the Scopia 3G Gateway on page 96

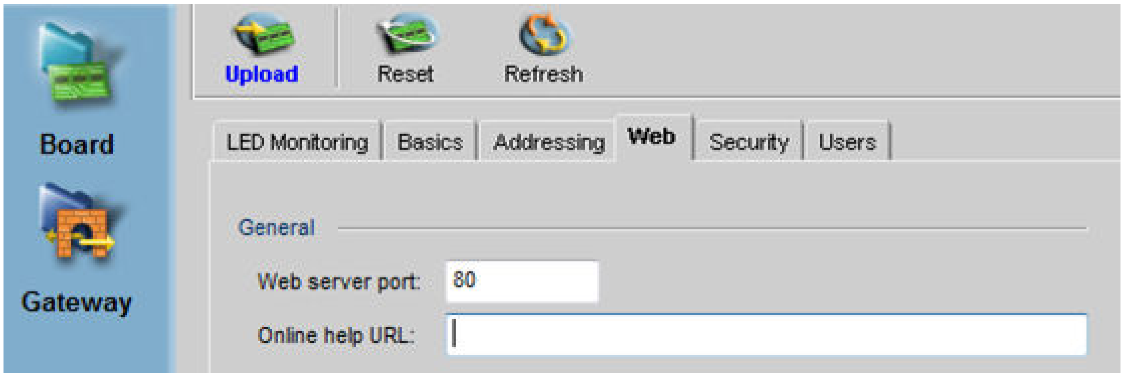
Configuring the HTTP Port on the Scopia 3G Gateway

About this task

The Scopia 3G Gateway has designated port 80 for HTTP. You can configure a different port to use HTTP (for example, if port 80 is busy).

Procedure

1. Log in to the Scopia 3G Gateway.
2. Select **Board** > **Web**.
3. Modify the port value in the **Web Server Port** field (see Figure 29: Scopia 3G Gateway HTTP Settings on page 94).



Web server port: 80

Online help URL:

Figure 29: Scopia 3G Gateway HTTP Settings

4. Select **Upload**.

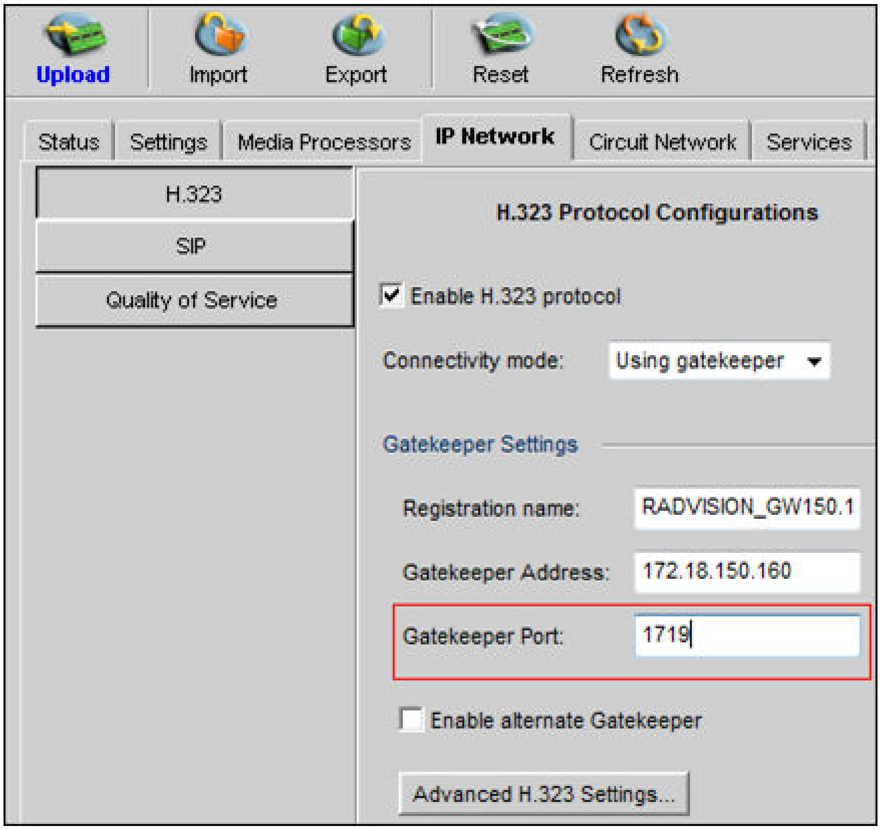
Configuring the UDP Port for RAS on the Scopia 3G Gateway

About this task

The Scopia 3G Gateway has designated port 1719 for RAS signaling (communication with the gatekeeper). You can configure a different port for RAS (for example, if port 1719 is busy).

Procedure

1. Log in to the Scopia 3G Gateway.
2. Select **IP Network** > **H.323**.
3. Configure the port that the Scopia 3G Gateway uses to communicate with the gatekeeper by modifying the value in the **Gatekeeper Port** field (see Figure 30: Scopia 3G Gateway Gatekeeper Settings on page 95).



H.323 Protocol Configurations

☑ Enable H.323 protocol

Connectivity mode: Using gatekeeper

Gatekeeper Settings

Registration name: RADVISION_GW150.1

Gatekeeper Address: 172.18.150.160

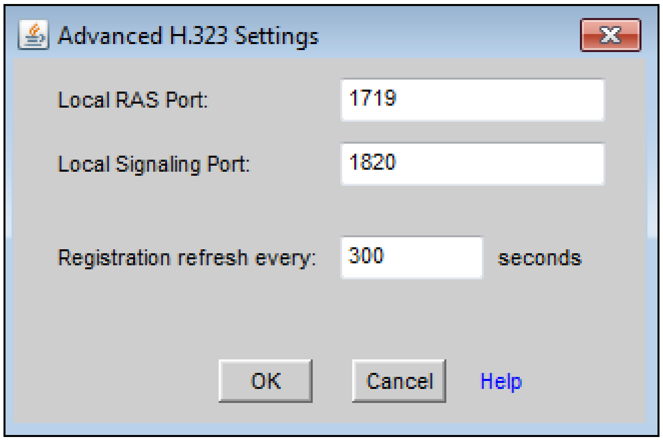
Gatekeeper Port: 1719

□ Enable alternate Gatekeeper

Figure 30: Scopia 3G Gateway Gatekeeper Settings

4. Configure the port that the gatekeeper uses to communicate with the Scopia 3G Gateway by doing the following:

   a. Select **Advanced H.323 Settings**. The **Advanced H.323 Settings** dialog box appears (see Figure 31: Advanced H.323 Settings on page 95).



Advanced H.323 Settings

Local RAS Port: 1719

Local Signaling Port: 1820

Registration refresh every: 300 seconds

Figure 31: Advanced H.323 Settings

   b. Modify the value in the **Local RAS Port field**.

5. Select **OK**.

6. Select **Upload**.

Configuring the TCP Port for Q.931 on the Scopia 3G Gateway

About this task

The Scopia 3G Gateway has designated port 1820 for Q.931 signaling. You can configure a different port for Q.931 (if, for example, port 1820 is busy). Q.931 is a telephony protocol used for establishing and terminating the connections in H.323 calls.

Procedure

1. Log in to the Scopia 3G Gateway.
2. Select **IP Network** > **H.323** > **Advanced H.323 Settings**. The Advanced H.323 Settings dialog box appears (see Figure 32: Advanced H.323 Settings on page 96).

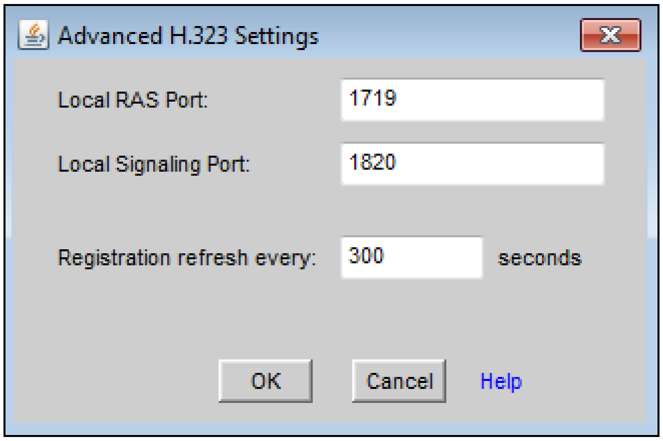

Local RAS Port: 1719
Local Signaling Port: 1820
Registration refresh every: 300 seconds

Figure 32: Advanced H.323 Settings

3. Modify the port value in the **Local Signaling Port** field.
4. Select **OK**.
5. Select **Upload**.

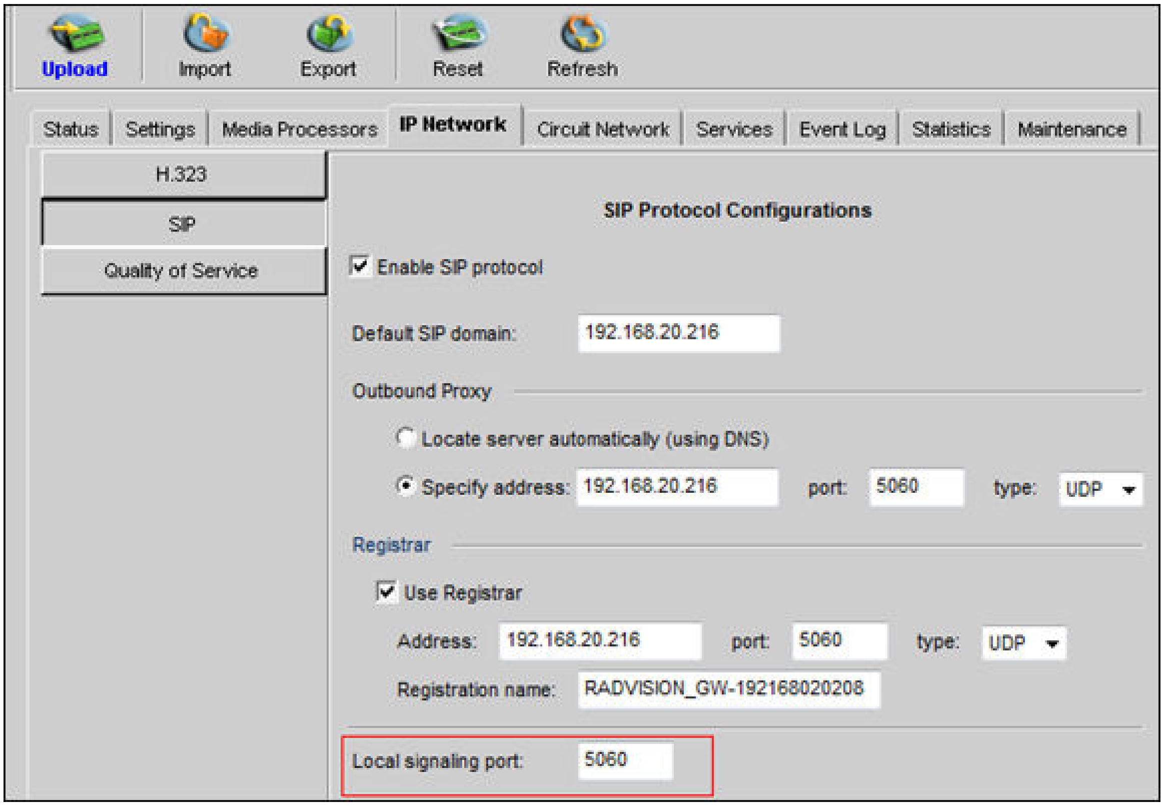
Configuring the SIP Port on the Scopia 3G Gateway

About this task

The Scopia 3G Gateway has designated port 5060 for SIP signaling. You can configure a different port for SIP (for example, if port 5060 is busy).

Procedure

1. Log in to the Scopia 3G Gateway.
2. Select **IP Network** > **SIP**.
3. Select the **Enable SIP protocol** checkbox (if cleared).
4. Modify the value in the **Local signaling port** field (see Figure 33: Scopia 3G Gateway SIP Settings on page 97).



SIP Protocol Configurations

☑ Enable SIP protocol

Default SIP domain: 192.168.20.216

Outbound Proxy

○ Locate server automatically (using DNS)

● Specify address: 192.168.20.216 port: 5060 type: UDP

Registrar

☑ Use Registrar

Address: 192.168.20.216 port: 5060 type: UDP

Registration name: RADVISION_GW-192168020208

Local signaling port: 5060

Figure 33: Scopia 3G Gateway SIP Settings

5. Select **Upload**.

Configuring Security Access Levels for the Scopia 3G Gateway

About this task

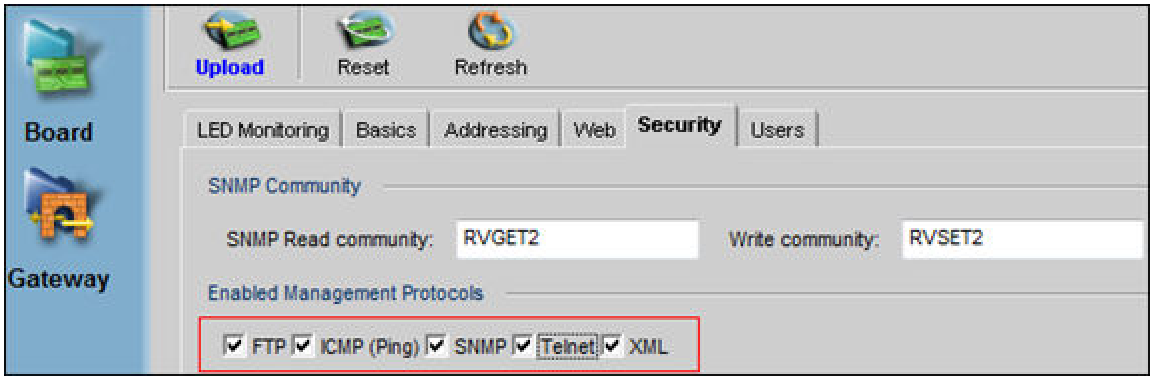
The Scopia 3G Gateway offers configurable security access levels that enable and disable Telnet, FTP, SNMP, XML, and ICMP (ping) protocols, which are used for the following:

- Upgrading software via FTP.
- Accessing the web user interface and performing configuration procedures via SNMP.
- Communication between Scopia Management and Scopia 3G Gateway.
- Accessing the Scopia 3G Gateway CLI and receive logs directly via Telnet.
- Sending control or error response messages via ICMP (ping).

Procedure

1. Access the Scopia 3G Gateway security settings by selecting **Board** > **Security** from the Scopia 3G Gateway web user interface.

2. Select the protocols you want to enable by selecting the checkbox next to each protocol in the **Enabled Management Protocols** Area (see Figure 34: Enabled Management Protocols Area on page 98). We recommend enabling these protocols.



SNMP Read community: RVGET2
Write community: RVSET2

☑ FTP ☑ ICMP (Ping) ☑ SNMP ☑ Telnet ☑ XML

Figure 34: Enabled Management Protocols Area

3. Select **Upload.**

Ports to Open on the Scopia 3G Gateway SP for Media Blade

The Scopia 3G Gateway SP (Media Video Processor for Mobile Software Package) is typically located in the enterprise and is connected to the DMZ. When opening ports to and from the MVP/M II, use Table 45: Bidirectional Ports to Open on the on page 99 as a reference.

Important:

The specific firewalls you need to open ports on depends on where your Scopia 3G Gateway and other Scopia Solution products are deployed.

Table 45: Bidirectional Ports to Open on the

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
21	FTP (TCP)	Upgrade Utility	Enables software upgrade and video stream recording	Cannot upgrade version	Recommended
23	Telnet (TCP)	Telnet client	Enables viewing MVP/M II online logs	Cannot view logs	Recommended
161	SNMP (UDP)	Scopia Management, Scopia Management, or any SNMP manager station	Enables you to configure and check the MVP/M II status	Cannot configure or check the status of the MVP/M II via SNMP	Recommended
3340	Font file client (TCP)	Font client software	Enables receiving extended font files from the MCU	Cannot work with different fonts	Optional
10000-10240	RTP/ RTCP (UDP)	Any RTP/RTCP media- enabled video network device	Delivers real-time media	Cannot transmit/ receive media streams	Mandatory

Chapter 13 | Implementing Port Security for the Scopia MCU

The Scopia MCU is a hardware unit that houses videoconferences from multiple endpoints, both H.323 and SIP.

This section details the ports used for the Scopia MCU, for both the blade and the MVP, and the relevant configuration procedures:

Navigation

Ports to Open on the Scopia MCU Blade

The Scopia MCU is typically located in the enterprise network and is connected to the DMZ. When opening ports on the Scopia MCU blade, use the following as a reference:

- If you are opening ports that are both to and from the Scopia MCU blade, see Table 46: Bidirectional Ports to Open on the Scopia MCU Blade on page 101.
- If you are opening outbound ports from the Scopia MCU blade, see Table 47: Outbound Ports to Open from the Scopia MCU Blade on page 102.

Important:

The specific firewalls you need to open ports on depends on where your Scopia MCU and other Scopia Solution products are deployed.

Table 46: Bidirectional Ports to Open on the Scopia MCU Blade

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
23	Telnet (TCP)	Telnet client	Enables you to view MCU logs and perform initial configuration tasks	Cannot view logs	Optional
80	HTTP (TCP)	Web client	Provides access to the MCU Administrator and Conference Control web user interfaces	Cannot administer MCU	Mandatory if using HTTP To configure, see Configuring the HTTP Port on the Scopia MCU Blade on page 103
161	SNMP (UDP)	Scopia Management, Scopia Management, or any SNMP manager station	Enables you to configure and check the MCU status	Cannot configure or check the MCU status via SNMP	Recommended
443	HTTPS (TCP)	Web client	Provides access to a secure web interface	Cannot administer MCU	Mandatory if using HTTPS
1024-4999	H.245 (TCP)	Any H.323 device	Enables H.245 signaling	Cannot connect H.323 calls	Mandatory To limit range, see Limiting the TCP Port Range for H.245 on the Scopia MCU Blade on page 103
1719	RAS (UDP)	H.323 gatekeeper	Enables RAS signaling	Cannot communicate with H.323 gatekeeper	Mandatory To configure, see Configuring the UDP Port for RAS on the Scopia MCU Blade on page 105
1720	Q.931 (TCP)	Any H.323 device	Enables Q.931 signaling	Cannot connect H.323 calls	Mandatory To configure, see Configuring the TCP Port for Q.931 on the Scopia MCU Blade on page 107
2010	MPI (TCP)	Any standalone MP units (MCUs configured to be MPs in clustering mode)	Enables connection to external MP	Cannot use external MP	Mandatory

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
2946	MVP control (TCP)	MVP	Enables connection to external MVP	Cannot use external MVP	Mandatory
3333	DTI (TCP)	DCS	Enables connection to external DCS	Cannot use external DCS	Optional; Mandatory if using DCS
3336	XML (TCP)	Conference Control web client endpoint, Scopia Management or third-party controlling applications	Enables you to manage the MCU via the XML API	Cannot use MCU Conference Control web user interface. Cannot control MCU via version 3 XML API.	Mandatory if deployed with Scopia Management
3337	XML (TCP)	Other MCUs	Enables you to cascade between MCUs (version 3) via XML API	Cannot cascade between two MCUs	Mandatory if multiple MCUs are deployed with Scopia Management
5060	SIP (TCP/ UDP)	Any SIP video network device	Enables SIP signaling	Cannot connect SIP calls	Mandatory To configure, see Configuring the SIP Port on the Scopia MCU Blade on page 109
6000-6999	RTP/ RTCP (UDP)	Any RTP/RTCP media-enabled video network device	Enables delivery of real-time audio media stream	Cannot transmit/ receive audio stream	Mandatory To configure, see Configuring the UDP Port for RTP/ RTCP on the Scopia MCU Blade on page 110

Table 47: Outbound Ports to Open from the Scopia MCU Blade

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
21	FTP (TCP)	Upgrade Utility or FTP Server	Enables audio stream recording	Cannot record audio streams	Optional
162	SNMP (UDP)	Scopia Management, Scopia Management, or any SNMP manager station	Enables sending SNMP Trap events	Cannot send traps	Recommended

Configuring Ports on the Scopia MCU Blade

This section provides instructions of how to configure the following ports and port ranges on the Scopia MCU:

Navigation

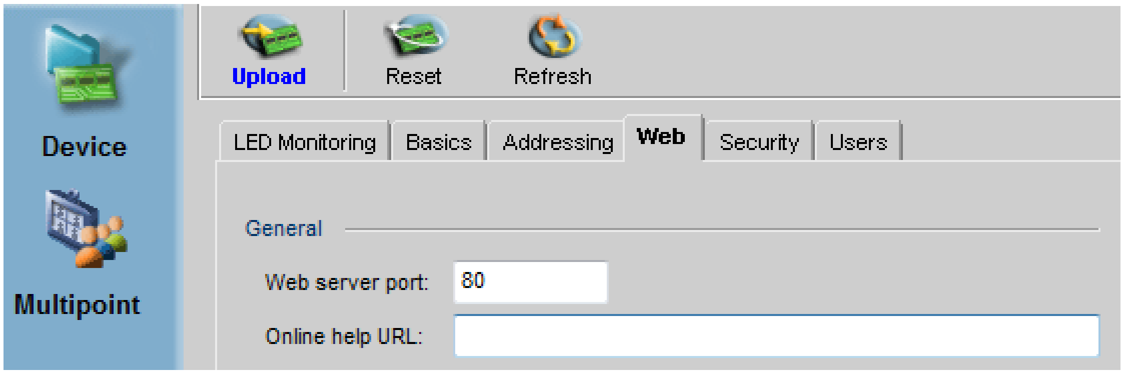
Configuring the HTTP Port on the Scopia MCU Blade

About this task

The Scopia MCU has designated port 80 for HTTP. You can configure a different port to use HTTP (for example, if port 80 is busy).

Procedure

1. Log in to the Scopia MCU.
2. Select **Device** > **Web**.
3. Modify the port value in the Web Server Port field (see Figure 35: Scopia MCU Web Settings on page 103).



Web server port: 80

Online help URL:

Figure 35: Scopia MCU Web Settings

4. Select **Upload**.

Limiting the TCP Port Range for H.245 on the Scopia MCU Blade

About this task

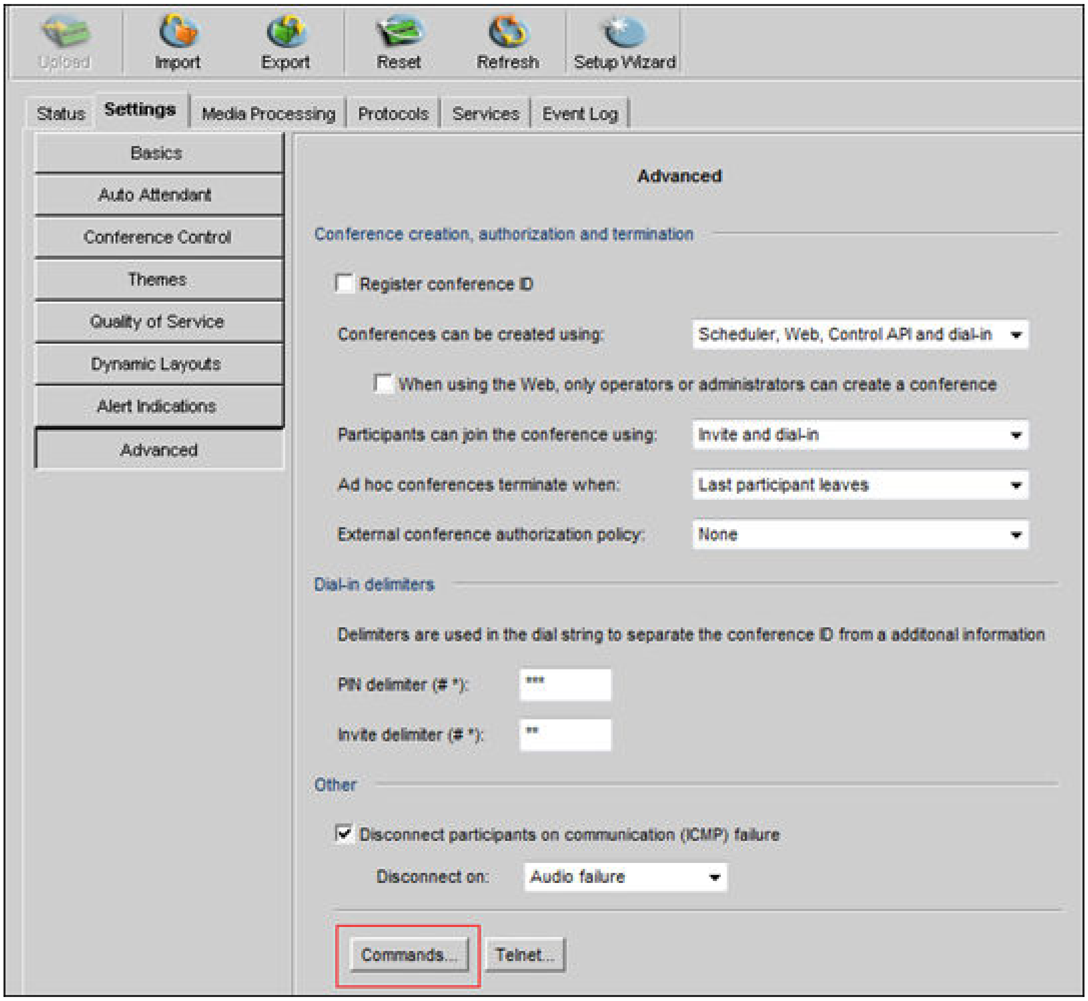
The Scopia MCU has designated ports 1024-4999 for H.245. To provide additional security for your firewall, you can limit this range. H.245 is a Control Protocol used for multimedia communication that enables transferring information about the device capabilities, as well as opening/closing the logical channels that carry media streams.

To calculate the number of ports you need to open, we recommend multiplying the number of total ports (for all calls) allowed by your license by a factor of 2.5.

Procedure

1. Log in to the Scopia MCU.
2. Navigate to the **Advanced Commands** section by doing the following:

   a. Select **Settings** > **Advanced** (see Figure 36: MCU Advanced Settings on page 104).



Advanced

Conference creation, authorization and termination

☐ Register conference ID

Conferences can be created using: Scheduler, Web, Control API and dial-in

☐ When using the Web, only operators or administrators can create a conference

Participants can join the conference using: Invite and dial-in

Ad hoc conferences terminate when: Last participant leaves

External conference authorization policy: None

Dial-in delimiters

Delimiters are used in the dial string to separate the conference ID from a additonal information

PIN delimiter (# *): ***

Invite delimiter (# *): **

Other

☑ Disconnect participants on communication (ICMP) failure

Disconnect on: Audio failure

Figure 36: MCU Advanced Settings

   b. Select **Commands.** The **Advanced Commands** dialog box opens (see Figure 37: MCU Advanced Commands Section on page 105).

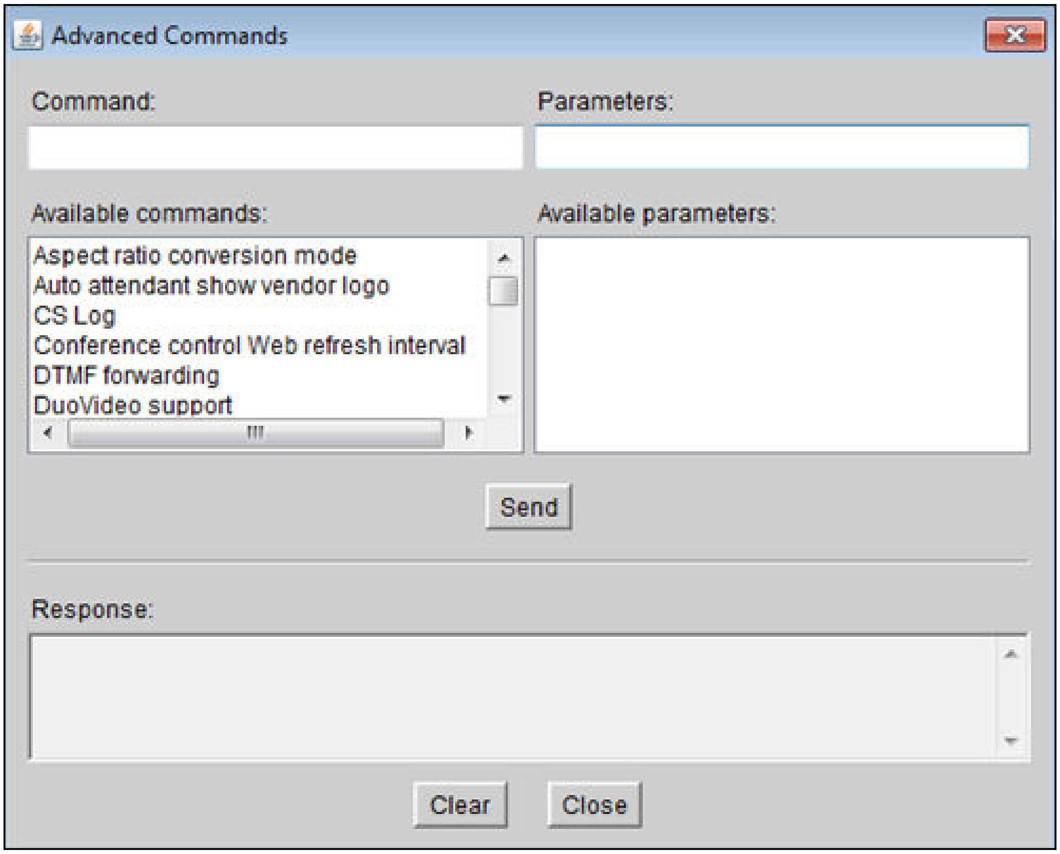


Figure 37: MCU Advanced Commands Section

3. Set the base port (the lower port) by typing **mc:h245portfrom** in the **Command** field and the base port value in the **Parameters** field.

   Important:

   You can configure the base port to any value between 1024-65535. To see the current port range, type **mc:h245portfrom** in the **Command** field and select **Send**.

4. Set the upper port by typing **mc:h245portto** in the **Command** field and the upper port value in the **Parameters** field.

   Important:

   You can configure the upper port to any value lower than or equal to 65535. To see the current port range, type **mc:h245portto** in the **Command** field and select **Send**.

5. Select **Send**.

6. Select **Close**.

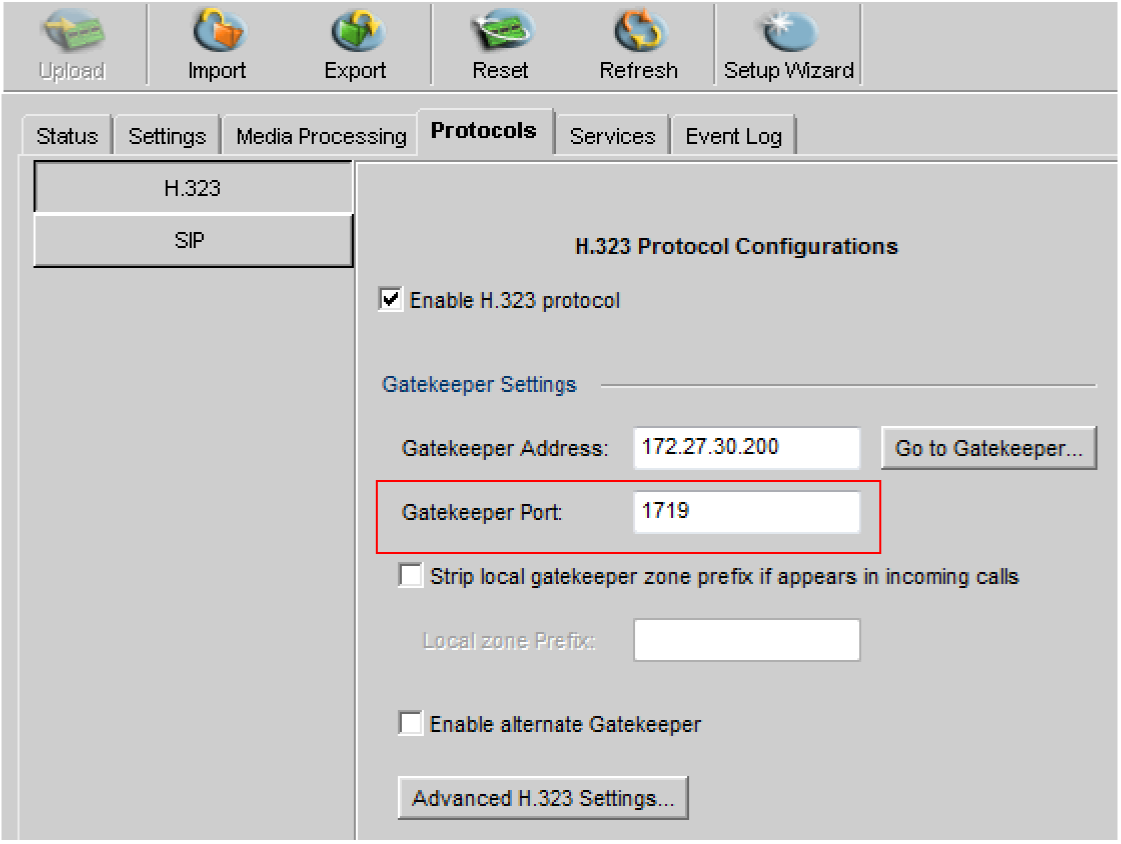
Configuring the UDP Port for RAS on the Scopia MCU Blade

About this task

The Scopia MCU has designated port 1719 for RAS signaling (communication with the gatekeeper). You can configure a different port for RAS (for example, if port 1719 is busy).

Procedure

1. Log in to the Scopia MCU.
2. Select **Protocols** > **H.323**.
3. Configure the port that the Scopia MCU uses to communicate with the gatekeeper by modifying the value in the **Gatekeeper Port** field (see Figure 38: Gatekeeper Port Settings on page 106).



H.323 Protocol Configurations

☑ Enable H.323 protocol

Gatekeeper Settings

Gatekeeper Address: 172.27.30.200

Gatekeeper Port: 1719

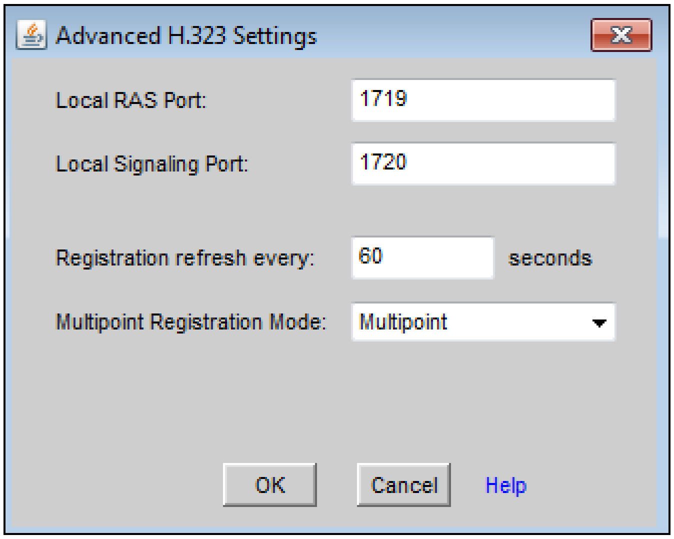
☐ Strip local gatekeeper zone prefix if appears in incoming calls

Local zone Prefix:

☐ Enable alternate Gatekeeper

Figure 38: Gatekeeper Port Settings

4. Configure the port that the gatekeeper uses to communicate with the Scopia MCU by doing the following:
   a. Select **Advanced H.323 Settings**. The Advanced H.323 Settings dialog box appears (see Figure 39: Advanced H.323 Settings on page 107).


Advanced H.323 Settings

Local RAS Port: 1719

Local Signaling Port: 1720

Registration refresh every: 60 seconds

Multipoint Registration Mode: Multipoint

Figure 39: Advanced H.323 Settings

b. Modify the value in the **Local RAS Port field**.

5. Select **OK**.
6. Select **Upload**.

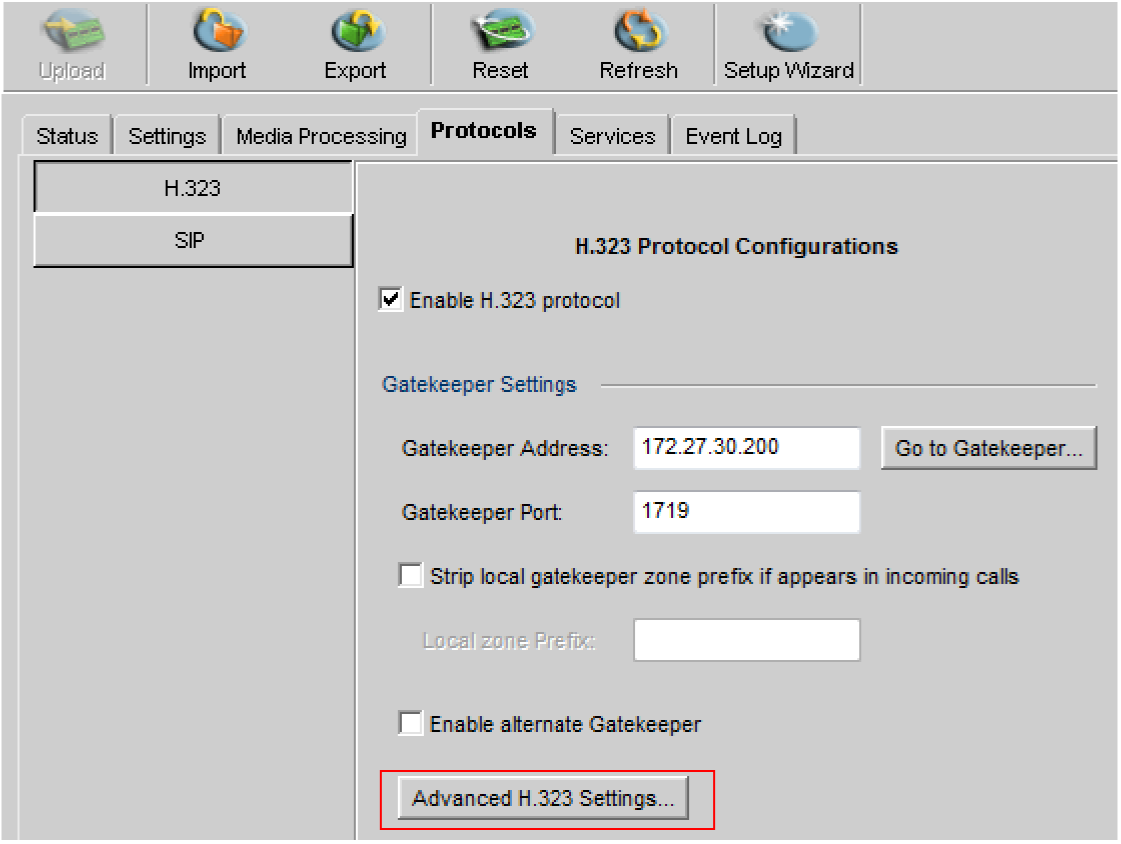
Configuring the TCP Port for Q.931 on the Scopia MCU Blade

About this task

The Scopia MCU has designated port 1720 for Q.931 signaling. You can configure a different port for Q.931 (for example, if port 1720 is busy). Q.931 is a telephony protocol used for establishing and terminating the connections in H.323 calls.

Procedure

1. Log in to the Scopia MCU.
2. Select **Protocols** > **H.323** (see Figure 40: H.323 Settings on page 108).



H.323 Protocol Configurations

☑ Enable H.323 protocol

Gatekeeper Settings

Gatekeeper Address: 172.27.30.200

Gatekeeper Port: 1719

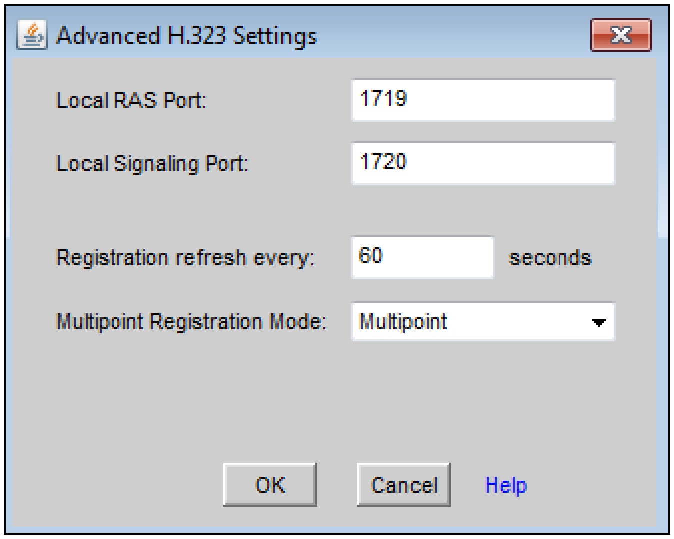
□ Strip local gatekeeper zone prefix if appears in incoming calls

Local zone Prefix:

□ Enable alternate Gatekeeper

Figure 40: H.323 Settings

3. Select **Advanced H.323 Settings**. The Advanced H.323 Settings dialog box appears (see Figure 41: Advanced H.323 Settings on page 108).



Local RAS Port: 1719

Local Signaling Port: 1720

Registration refresh every: 60 seconds

Multipoint Registration Mode: Multipoint

Figure 41: Advanced H.323 Settings

4. Modify the value in the **Local Signaling Port** field.

5. Select **OK**.

6. Select **Upload**.

Configuring the SIP Port on the Scopia MCU Blade

About this task

The Scopia MCU has designated port 5060 for SIP signaling. You can configure a different port for SIP (for example, if port 5060 is busy).

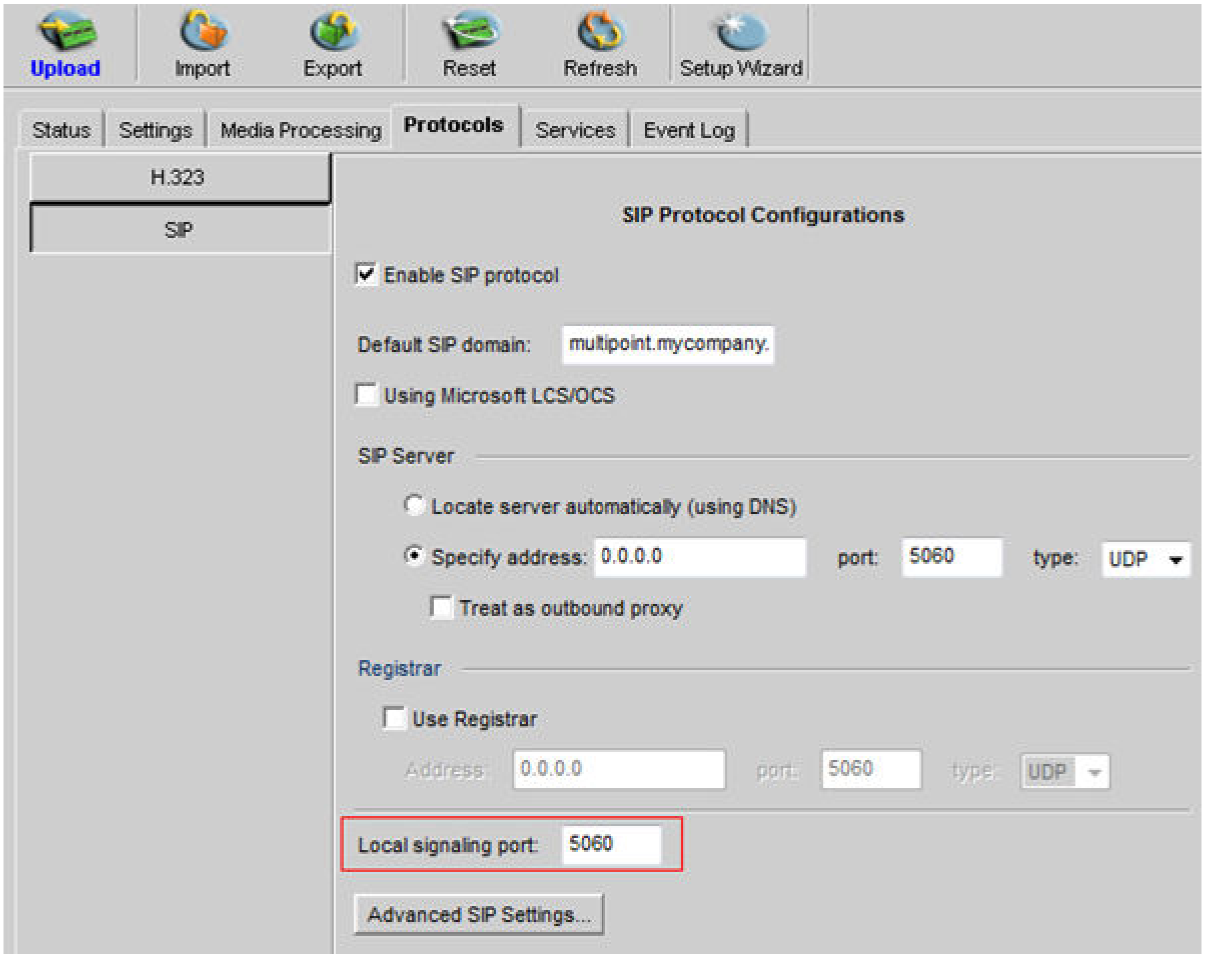
Procedure

1. Log in to the Scopia MCU.

2. Select **Protocols** > **SIP**.

3. Select the **Enable SIP protocol** checkbox (if cleared).

4. Modify the value in the **Local signaling port** field (see Figure 42: SIP Protocol Settings on page 110).



SIP Protocol Configurations

☑ Enable SIP protocol

Default SIP domain: multipoint.mycompany.

□ Using Microsoft LCS/OCS

SIP Server

○ Locate server automatically (using DNS)

● Specify address: 0.0.0.0 port: 5060 type: UDP

□ Treat as outbound proxy

Registrar

□ Use Registrar

Address: 0.0.0.0 port: 5060 type: UDP

Local signaling port: 5060

Figure 42: SIP Protocol Settings

5. Select **Upload**.

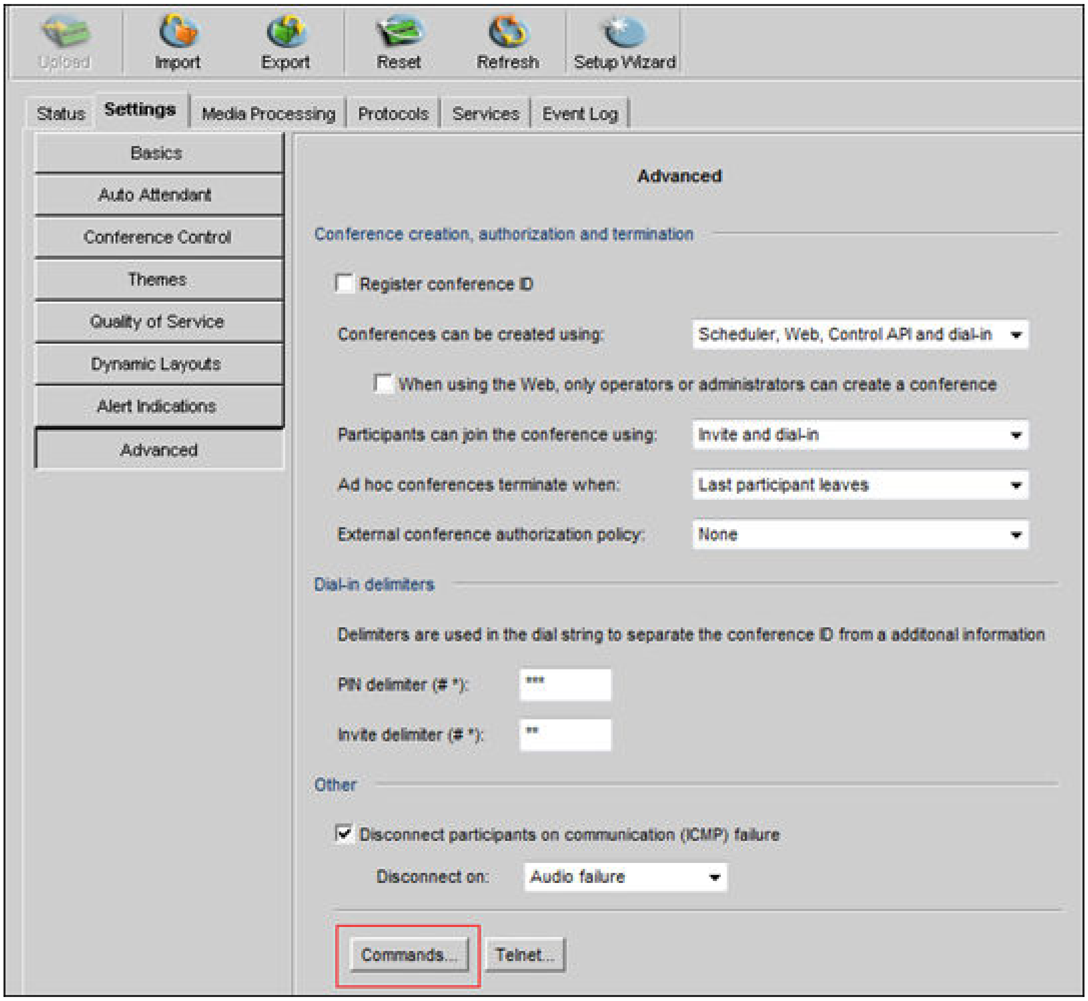
Configuring the UDP Port for RTP/RTCP on the Scopia MCU Blade

About this task

The Scopia MCU has designated ports 6000-6999 for RTP/RTCP (audio media). You can configure a different base port for RTP/RTCP (for example, if port 6000 is busy).

Procedure

1. Log in to the Scopia MCU.
2. Select **Settings** > **Advanced** (see Figure 43: MCU Advanced Settings on page 111).



Advanced

Conference creation, authorization and termination

□ Register conference ID

Conferences can be created using: Scheduler, Web, Control API and dial-in

□ When using the Web, only operators or administrators can create a conference

Participants can join the conference using: Invite and dial-in

Ad hoc conferences terminate when: Last participant leaves

External conference authorization policy: None

Dial-in delimiters

Delimiters are used in the dial string to separate the conference ID from a additonal information

PIN delimiter (# *): ***

Invite delimiter (# *): **

Other

☑ Disconnect participants on communication (ICMP) failure

Disconnect on: Audio failure

Figure 43: MCU Advanced Settings

3. Select **Commands**. The **Advanced Commands** section appears (see Figure 44: MCU Advanced Commands Section on page 112).

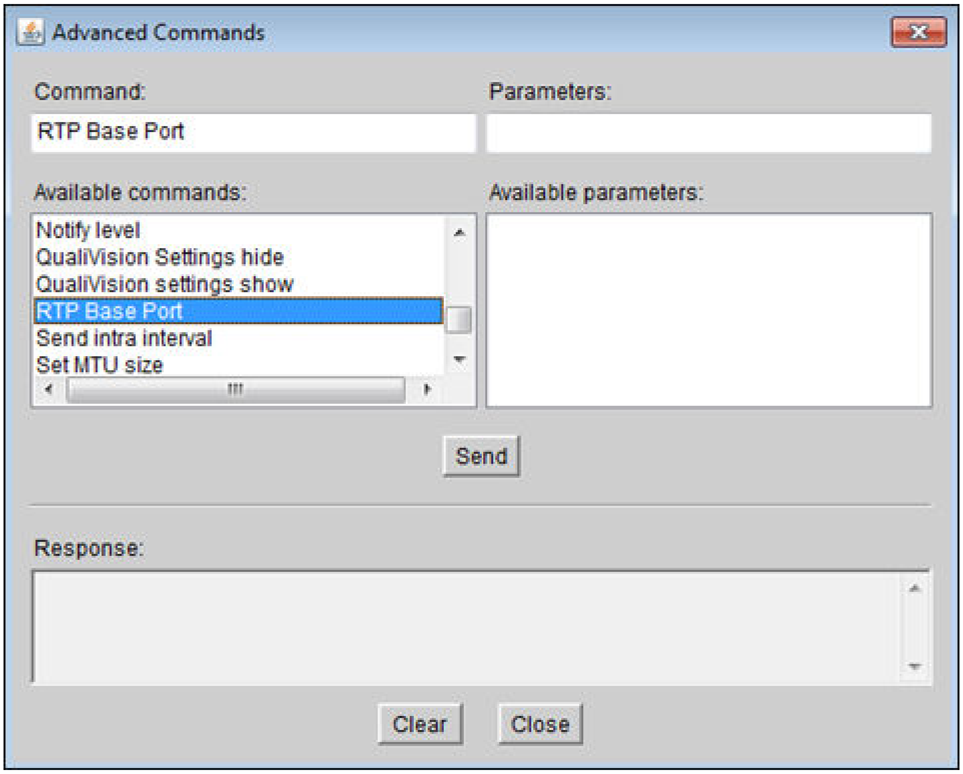


Figure 44: MCU Advanced Commands Section

4. Select **RTP Base Port** in the **Available Commands** list.
5. Enter the base port value, which is the lower end of the range, in the **Parameters** field.
6. Select **Send**.
7. Select **Close**.

Configuring Security Access Levels for the Scopia MCU Blade

About this task

The Scopia MCU offers configurable security access levels that enable and disable Telnet, FTP, SNMP and ICMP (ping) protocols.

By default, the security access level is set to **Standard**. It is recommended to set your security access level to **Maximum** (which disables these protocols), except for the following situations:

- If you are viewing logs, Telnet should be enabled.
- If you are customizing your language settings, FTP should be enabled.
- If you are performing configuration procedures or would like to receive traps, SNMP should be enabled.

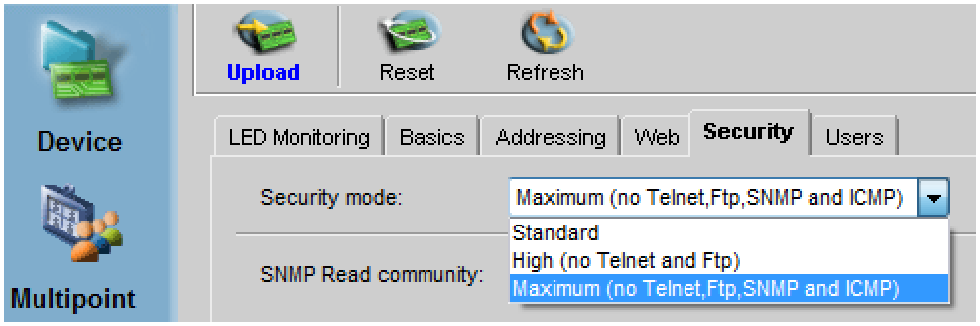
Important:

You can view trap events in the **Event Log** tab of the web user interface.

- If you would like control or error response messages to be sent, ICMP (ping) should be enabled.

Procedure

1. Access the Scopia MCU security settings by selecting **Device** > **Security**.
2. Select the access level from the **Security Mode** list (see Figure 45: MCU Security Settings on page 113). Table 48: Scopia MCU Security Modes on page 113 lists the behavior of each service when each security mode is applied.



Security mode: Maximum (no Telnet,Ftp,SNMP and ICMP)

SNMP Read community:

Figure 45: MCU Security Settings

Table 48: Scopia MCU Security Modes

Security Access Level	Telnet	FTP	SNMP	ICMP (ping)
Low	Enabled	Enabled	Enabled	Enabled
Medium	Disabled	Disabled	Enabled	Enabled
High	Disabled	Disabled	Disabled	Disabled

3. Select **Upload.**

Ports to Open on the MVP for Scopia MCU

The MVP, a component of the Scopia MCU, is typically located in the enterprise network and connected to the DMZ. When you are opening ports that are both in and out of the MVP, use Table 49: Bidirectional Ports to Open on the MVP on page 114 as a reference.

Important:

The specific firewalls that you need to open ports on depends on where your MVP and other Scopia Solution products are deployed.

Table 49: Bidirectional Ports to Open on the MVP

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
21	FTP (TCP)	Upgrade Utility	Enables software upgrade and video stream recording	Cannot upgrade version	Optional
23	Telnet (TCP)	Telnet client	Enables you to view MVP online logs	Cannot view logs	Optional
2946	MEGACO (TCP)	MEGACO (H.248) Protocol	Enables connection to MCU	Cannot connect to MCU	Mandatory
3340	Font file client (TCP)	Font client software	Enables receiving extended font files from the MCU	Cannot work with non-English fonts	Mandatory
10000-10575	RTP/ RTCP (UDP)	Any RTP/RTCP media-enabled video network device	Enables real-time delivery of video media	Cannot transmit/ receive video media stream	Mandatory To configure, see Configuring UDP Ports for RTP/ RTCP on the MVP for Scopia MCU on page 114

Configuring UDP Ports for RTP/RTCP on the MVP for Scopia MCU

About this task

The MVP has designated ports 10000-10575 for RTP/RTCP. You can configure the base port, which is the lower port value.

Procedure

1. Connect to the MVP IP via any telnet application.
2. Type **printCfgMenu** to display the configurations that can be modified.
3. Locate the **RTP Base Port** line and modify the value (the default value is 10000).
4. Type **q** to close and save.

   Important:

   The MVP restarts.

RADVISION®
an Avaya company

About Radvision
Radvision, an Avaya company, is a leading provider of videoconferencing and telepresence technologies over IP and wireless networks. We offer end-to-end visual communications that help businesses collaborate more efficiently. Together, Radvision and Avaya are propelling the unified communications evolution forward with unique technologies that harness the power of video, voice, and data over any network.
www.radvision.com