Port Security for Avaya Scopia® Solution Reference Guide

Release 8.3.2
Issue 1
April 2015

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface

with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Note to Service Provider

The product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

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 Avaya Scopia® Management

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

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

Avaya Scopia® Management can connect to H.323 endpoints in public and partner networks via Avaya Scopia® PathFinder, and to H.323 and SIP endpoints located in the enterprise network. For a list of TCP/IP/UDP ports supported by Avaya Scopia® Management, see Ports to Open on Avaya Scopia® Management on page 9.

Related Links

Ports to Open on Avaya Scopia® Management on page 9

Ports to Open on Avaya Scopia® Management

Avaya 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 10.
- For outbound ports from Scopia® Management, see Table 2: Outbound Ports to Open from Scopia® Management on page 12.
- For inbound ports into Scopia® Management, see Table 3: Inbound Ports to Open on Scopia® Management on page 14.

Important:

Choose the specific firewalls to open ports, depending on where your Avaya 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 You can configure this port during installation (see *Installation Guide for Avaya 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
3336	XML (TCP)	Scopia® Management/ Scopia® Video Gateway / TIP Gateway/ SIP Gateway / MCU	Enables communication between Scopia® Management and the Scopia® Video Gateway/ TIP Gateway / SIP Gateway/ MCU via	Scopia® Management cannot connect to the Scopia® Video Gateway/ TIP Gateway /	Mandatory if deployed with Scopia® Video Gateway/ TIP Gateway / SIP Gateway/ MCU

Table continues…

Port Range	Protocol	Source/ Destination	Functionality	Result of Blocking Port	Required
			the moderator's XML API (used for managing meetings via Scopia® Management)	SIP Gateway/ MCU via the XML API	
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 Scopia® Management	Mandatory for any XML secure clients
5060	SIP (TCP/ UDP)	B2B/ Other SIP components	Enables SIP signaling	Cannot connect SIP calls	Mandatory
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 an internal database)	Cannot synchronize data between the master and slave servers	Mandatory for redundancy deployments with an internal database
5556	TCP	Avaya Scopia® Web Collaboration server	Enables Scopia® Management to receive alarms from Scopia® Web Collaboration server.	Scopia® Web Collaboration server cannot send alarms to Scopia® Management.	Mandatory when Scopia® Web Collaboration server is in your deployment.
7800-7802	UDP	Scopia® Management	Enables data synchronization between redundant Scopia® Management servers	Redundancy functionality is not available	Mandatory for redundancy deployments
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
22	SSH (TCP)	Scopia® Management	Detects LifeSize endpoints. Enables downloading Avaya Scopia® PathFinder server logs. Detects and manages Scopia® VC240.	Cannot detect LifeSize endpoints, download Avaya 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	Avaya Scopia® PathFinder	Detects endpoints via Avaya Scopia® PathFinder	Cannot detect endpoints via Avaya Scopia® PathFinder	Mandatory
3338	XML (TCP)	MCU/ Scopia® Video Gateway / TIP	Enables connection to MCU/ Scopia® Video Gateway / TIP Gateway/ SIP Gateway via the	Cannot perform configuration for MCU/ Scopia® Video Gateway /	Mandatory if deployed with MCU/ Scopia® Video

Table continues…

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

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
55003	TCP	XT Series	Enables connection to the XT Series	Cannot connect to the XT Series	Mandatory if deployed with XT Series
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 Avaya Scopia® PathFinder and Scopia® Management web user interface	Cannot access the Avaya Scopia® PathFinder web user interface	Mandatory if deployed with Avaya Scopia® PathFinder or Scopia® Management internal Gatekeeper. You can configure this port during installation (see *Installation Guide for Avaya Scopia® Management*).
9443	HTTPS (TCP)	Web client	Enables Tomcat to run over SSL	Cannot access Scopia® Management web user interface via HTTPS	Mandatory if using HTTPS. You can configure this port as part of setting up HTTPS (see *Administrator Guide for Avaya Scopia® Management*).

Related Links

Implementing Port Security for Avaya Scopia® Management on page 9

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:

Related Links

Ports to Open for the Scopia® Elite 6000 Series MCU on page 15
Ports to Open for the Scopia® Elite 5100 Series MCU on page 18
Ports to Open on the Scopia® Elite 5200 Series MCU on page 21
Configuring Ports on All Models of the Scopia® Elite MCU on page 24
Configuring Security Access Levels for the Scopia® Elite MCU on page 32

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 16.
- If you are opening ports inbound to the Scopia® Elite 6000 Series MCU, see Table 6: Inbound Ports to Open to the Scopia® Elite 6000 Series MCU on page 18.

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 26
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 28 and Configuring the UDP Port for the Gatekeeper on the Scopia® Elite MCU on page 29
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 29
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	Enables SIP content sharing	Cannot share SIP contents	Mandatory if using content sharing with SIP over TCP

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
		network device			To configure, see Configuring the TCP Port Range for SIP BFCP on the Scopia® Elite MCU on page 31
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 30
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 30
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 25

Table 5: Outbound ports to open from Scopia® Elite 6000 Series MCU

Port range	Protocol	Destination	Function	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
53	DNS (TCP/UDP)	DNS server	Enable querying DNS for FQDN	DNS is disabled	Mandatory

Table 6: 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 27
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

Related Links

Implementing Port Security for the Scopia® Elite MCU on page 15

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 7: Bidirectional Ports to Open on the Scopia® Elite 5100 Series MCU on page 19.
- If you are opening ports outbound from the Scopia® Elite 5100 Series MCU, see Table 8: Outbound Ports to Open from the Scopia® Elite 5100 Series MCU on page 20.
- If you are opening ports inbound to the Scopia® Elite 5100 Series MCU, see Table 9: Inbound Ports to Open to the Scopia® Elite 5100 Series MCU on page 20.

Important:

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

Table 7: 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 26
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 28 and Configuring the UDP Port for the Gatekeeper on the Scopia® Elite MCU on page 29.
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 29.
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	Enables SIP signaling	Cannot connect SIP calls	Mandatory if using SIP over TCP/ UDP

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
		network device			To configure, see Configuring the TCP/UDP/TLS Port for SIP on the Scopia® Elite MCU on page 30.
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 30.
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 25.

Table 8: Outbound Ports to Open from the Scopia® Elite 5100 Series MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
53	DNS (TCP)	DNS server	Enables querying DNS for FQDN	DNS is disabled	Mandatory
162	SNMP (UDP)	Scopia® Management or any SNMP manager station	Enables sending SNMP Trap events	Cannot send SNMP Traps	Recommended

Table 9: 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	Cannot configure MCU	Mandatory if using HTTP

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
			Conference Control web user interfaces; used for software upgrade		To configure, see Configuring the HTTP Port on the Scopia® Elite MCU on page 27.
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

Related Links

Implementing Port Security for the Scopia® Elite MCU on page 15

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 10: Bidirectional Ports to Open on the Scopia® Elite 5200 Series MCU on page 22.
- If you are opening ports outbound from the Scopia® Elite 5200 Series MCU, see Table 11: Outbound Ports to Open from the Scopia® Elite 5200 Series MCU on page 23.
- If you are opening ports inbound to the Scopia® Elite 5200 Series MCU, see Table 12: Inbound Ports to Open to the Scopia® Elite 5200 Series MCU on page 24.

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 10: 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 26.
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 28 and Configuring the UDP Port for the Gatekeeper on the Scopia® Elite MCU on page 29.
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 29.
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

Table continues…

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 30.
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 25.
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 25.
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 25.

Table 11: Outbound Ports to Open from the Scopia® Elite 5200 Series MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
53	DNS (TCP)	DNS server	Enables querying DNS for FQDN	DNS is disabled	Mandatory
162	SNMP (UDP)	Scopia® Management, or any SNMP manager station	Enables sending SNMP Trap events	Cannot send SNMP Traps	Recommended

Table 12: 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 27.
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

Related Links

Implementing Port Security for the Scopia® Elite MCU on page 15

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:

Related Links

Implementing Port Security for the Scopia® Elite MCU on page 15
Configuring the UDP Port Ranges for RTP/RTCP on the Scopia® Elite MCU on page 25
Configuring the TCP Port Range for H.245 on the Scopia® Elite MCU on page 26

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 (Figure 1: Defining the base port for video on page 25).

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**.

Related Links

Configuring Ports on All Models of the Scopia® Elite MCU on page 24

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** (Figure 2: CLI Section on page 26).

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**.

Related Links

Configuring Ports on All Models of the Scopia® Elite MCU on page 24

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** (Figure 3: CLI Section on page 27).

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*

Related Links

Configuring Ports on All Models of the Scopia® Elite MCU on page 24

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 29).

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 (Figure 4: RAS Port Configuration on page 28).

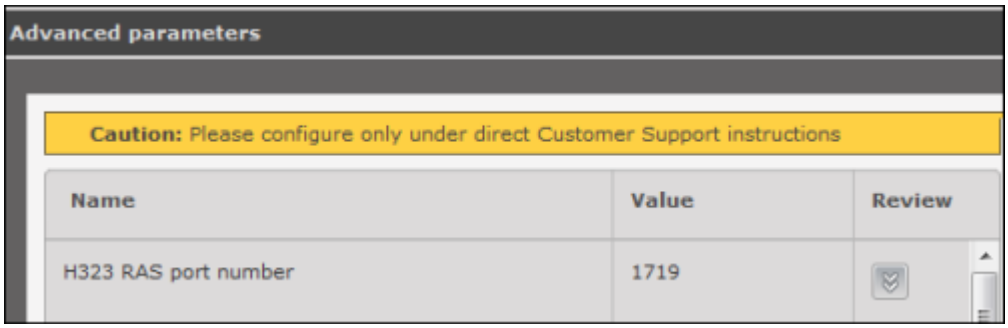

Figure 4: RAS Port Configuration

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**.

Related Links

Configuring Ports on All Models of the Scopia® Elite MCU on page 24

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 28).

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 (Figure 5: H.323 Protocol section of the Protocols tab on page 29).

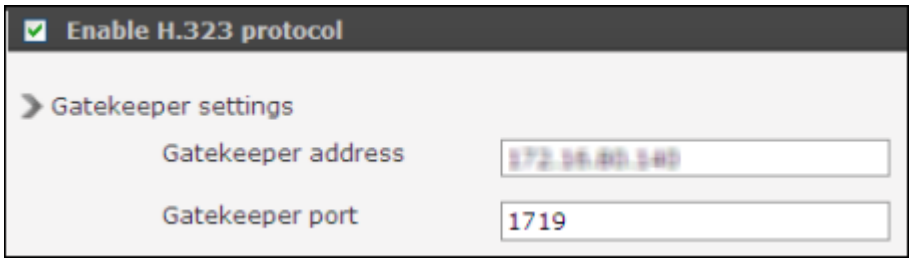

Figure 5: H.323 Protocol section of the Protocols tab

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

Related Links

Configuring Ports on All Models of the Scopia® Elite MCU on page 24

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 (Figure 6: H.323 Signaling Port Configuration on page 30).

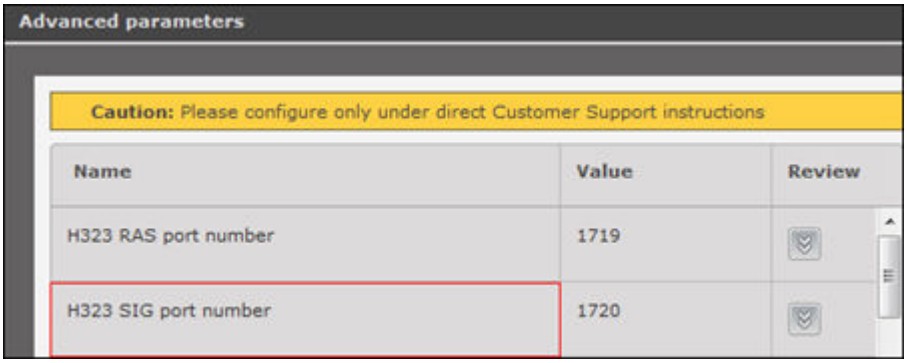

Figure 6: H.323 Signaling Port Configuration

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**.

Related Links

Configuring Ports on All Models of the Scopia® Elite MCU on page 24

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** (Figure 7: SIP Port Configuration on page 31).

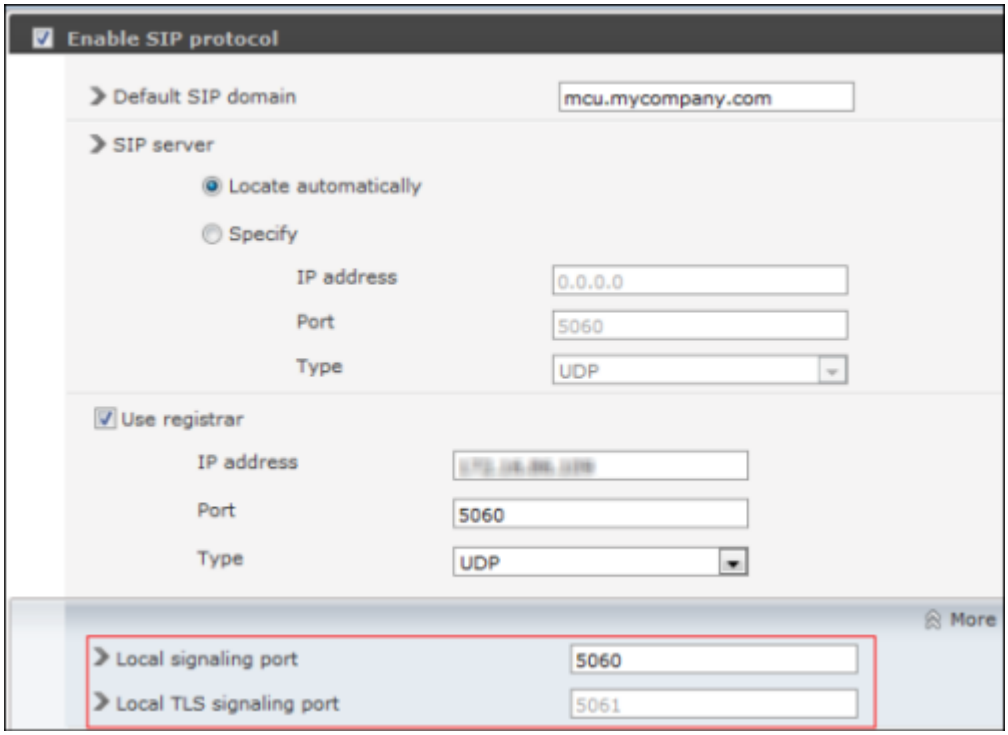

Figure 7: SIP Port Configuration

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**.

Related Links

Configuring Ports on All Models of the Scopia® Elite MCU on page 24

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.

BFCP is a protocol which coordinates shared videoconference features in SIP calls, often used by one participant at a time. For example, when sharing content to others in the meeting, one

participant is designated as the presenter, and is granted the floor for presenting. All endpoints must be aware that the floor was granted to that participant and react appropriately.

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 (Figure 8: Defining the base port for SIP BFCP on page 32).

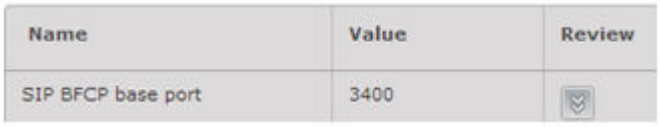

Figure 8: Defining the base port for SIP BFCP

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**.

Related Links

Configuring Ports on All Models of the Scopia® Elite MCU on page 24

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, 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.

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 33). Table 13: MCU Security Access Levels on page 33 lists the protocol status when each security access level is applied.

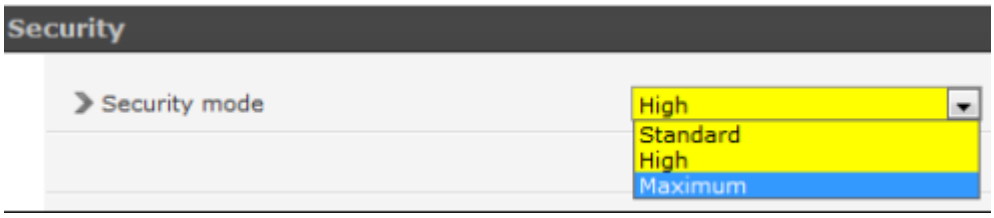

Figure 9: Security Access Level Settings

Table 13: MCU Security Access Levels

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

4. Select **Apply**.

Related Links

Implementing Port Security for the Scopia® Elite MCU on page 15

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:

Related Links

Ports to Open on Scopia® Desktop on page 34
Limiting Port Ranges on the Scopia® Desktop server on page 41

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 35) 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.

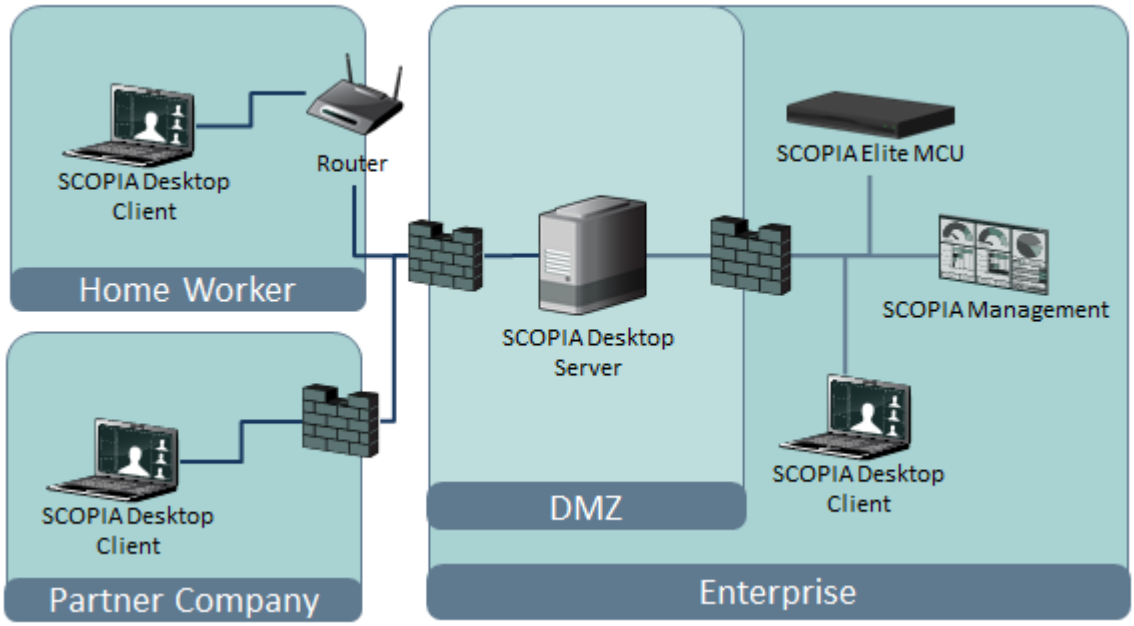

Figure 10: Locating the Scopia® Desktop server in the DMZ

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 14: Bidirectional Ports to Open Between the Scopia® Desktop server and the Enterprise on page 36.
- When opening ports that are outbound from the Scopia® Desktop server, see Table 15: Outbound Ports to Open from the Scopia® Desktop server to the Enterprise on page 37.
- When opening ports that are inbound to the Scopia® Desktop server, see Table 16: Inbound Ports to Open from the Enterprise to the Scopia® Desktop server on page 38.

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 17: Bidirectional Ports to Open Between the Scopia® Desktop server and the Public on page 38.
- When opening ports that are inbound from the Scopia® Desktop server, see Table 18: Inbound Ports to Open from the Public to the Scopia® Desktop server on page 39.

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 19: Outbound Ports to Open from the XMPP Server on page 39.
- When opening inbound ports to the XMPP server, see Table 20: Inbound Ports to Open on the XMPP Server on page 40.

When opening bidirectional ports between Scopia® Desktop Clients, see Table 21: Bidirectional Ports to Open Between Scopia® Desktop Clients on page 40.

When opening inbound ports from the Scopia® Desktop Clients to the STUN server, see Table 22: Inbound Ports to Open from the Scopia® Desktop Client to the STUN Server on page 40.

Important:

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

Table 14: 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 42
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 41

Table 15: 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
1719	UDP (RAS)	Avaya Scopia® ECS Gatekeeper or the internal gatekeeper in Scopia® Management	Enables communication with Avaya 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 16: 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 .
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 43

Table 17: 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 41

Table 18: 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 .
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 43.

Table 19: Outbound Ports to Open from the XMPP Server on page 39 and Table 20: Inbound Ports to Open on the XMPP Server on page 40 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 19: 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®	Users cannot login to the XMPP Server	Mandatory for Scopia® Management authentication if there is a firewall between XMPP

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
			Management authentication		and Scopia® Desktop server

Table 20: 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 21: 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 22: 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 43.

Related Links

Implementing Port Security for Scopia® Desktop on page 34

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:

Related Links

Implementing Port Security for Scopia® Desktop on page 34
Limiting the UDP Port Range for RTP/RTCP on the Scopia® Desktop server on page 41
Limiting the TCP Port Range for H.245/Q.931 on the Scopia® Desktop server on page 42
Configuring the TCP Streaming Port on the Scopia® Desktop server on page 43

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 42).

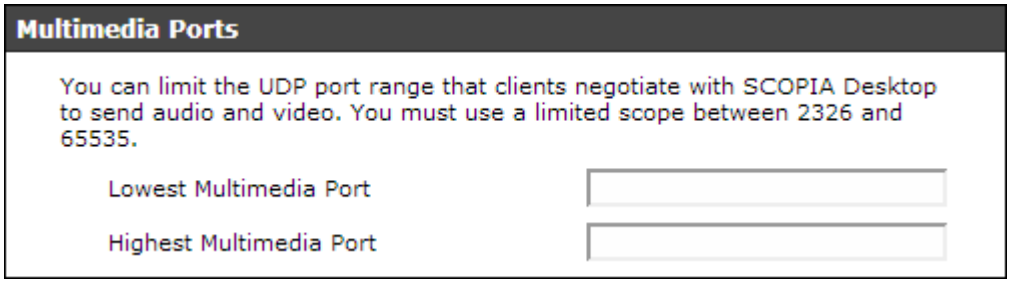

Figure 11: Multimedia Ports Area

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**.

Related Links

Limiting Port Ranges on the Scopia® Desktop server on page 41

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.

Related Links

Limiting Port Ranges on the Scopia® Desktop server on page 41

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 43).

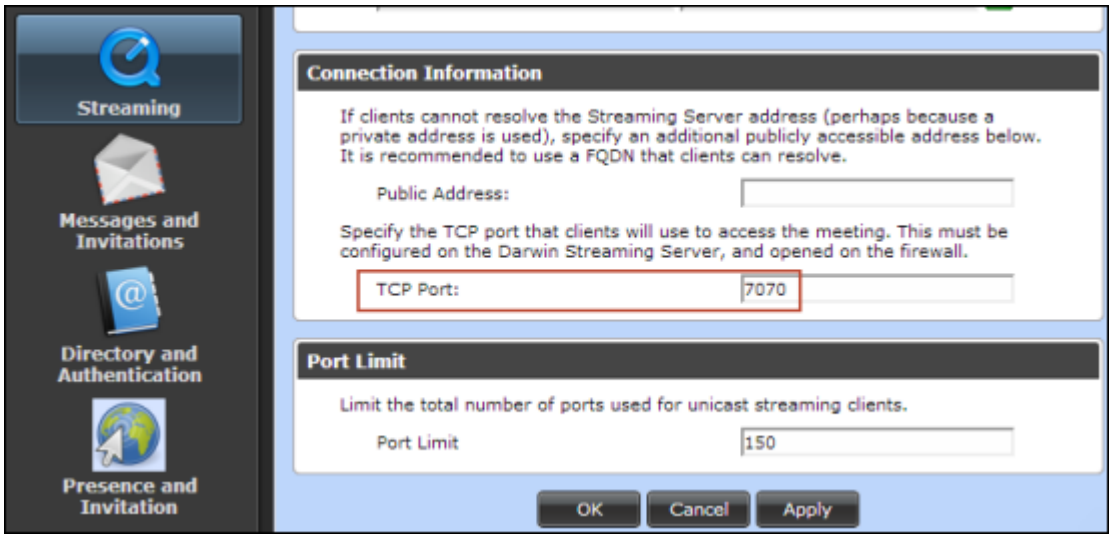

Figure 12: Setting the streaming port for Scopia® Desktop server

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.

Related Links

Limiting Port Ranges on the Scopia® Desktop server on page 41

Chapter 5: Implementing Port Security for Avaya Scopia® PathFinder

Avaya Scopia® PathFinder is Scopia® Solution's answer to firewall traversal. The Avaya 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 Avaya Scopia® PathFinder server and the Scopia® PathFinder client , and the relevant port configuration procedures:

Related Links

Ports to Open on Scopia® PathFinder on page 45
Configuring Ports on the PathFinder server on page 50

Ports to Open on Scopia® PathFinder

Avaya Scopia® PathFinder is Scopia® Solution's answer to firewall traversal. The PathFinder server is an H.460 server, typically deployed in the DMZ, while the Scopia® PathFinder client is a tunneling client, typically deployed outside the enterprise firewall alongside the remote H.323 endpoint (see Figure 13: H.323 connections to PathFinder server on page 46).

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 PathFinder server in the DMZ (see Figure 13: H.323 connections to PathFinder server on page 46).

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 PathFinder server using direct port access (ports 4000-5000).

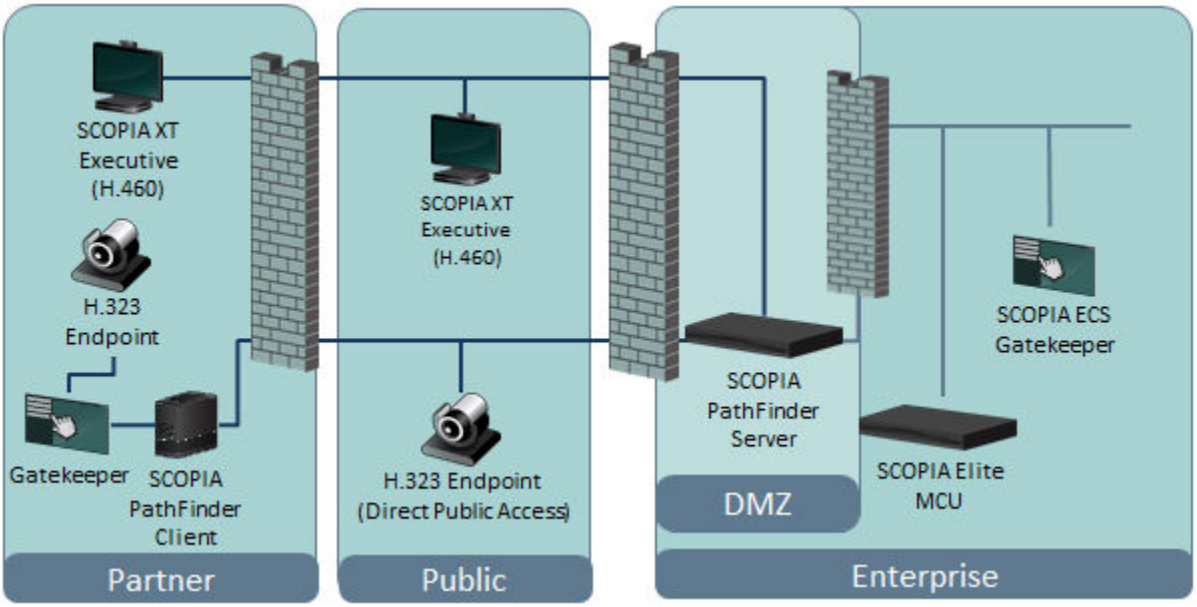

Figure 13: H.323 connections to PathFinder server

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

- If opening ports that are both to and from the PathFinder server, see Table 23: Bidirectional Ports to Open the PathFinder server on page 47.
- If opening ports that are both to and from the Scopia® PathFinder client , see Table 24: Bidirectional Ports to Open on the Scopia® PathFinder client on page 49.

Important:

In order for an H.323 endpoint (or other H.323 device) within the enterprise to successfully connect to the PathFinder server in the DMZ via the enterprise firewall (see Figure 14: Contacting PathFinder server from within the enterprise on page 47), 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 PathFinder server (1024-65535, bidirectional)

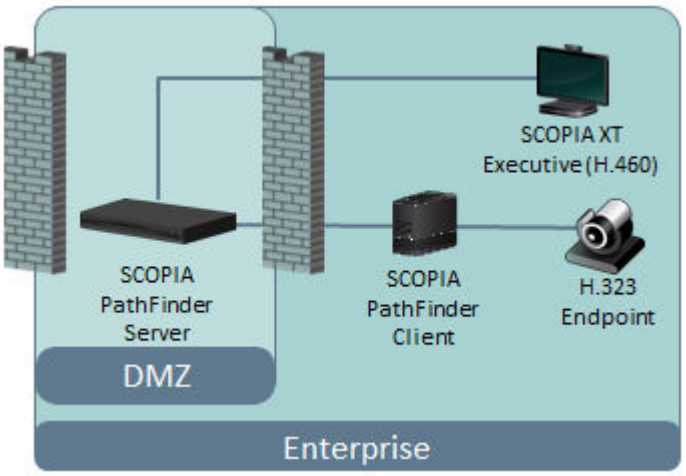

Figure 14: Contacting PathFinder server from within the enterprise

Important:

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

Table 23: Bidirectional Ports to Open the 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 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 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 PathFinder server on page 50
1720	TCP	Any H.323 device using Q. 931 signaling in DPA mode	Enables IP call signaling	No signaling capabilities: guest users cannot dial	Mandatory if in DPA mode

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
				into internal endpoints	
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 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 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	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

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
					TCP/UDP Port Range for H.323 Direct Access Calls on the PathFinder server on page 50
8080	HTTP (TCP)	Web client/ browser	Provides access to the web user interface	Cannot configure PathFinder server	Mandatory for configuring the Scopia® PathFinder application
8089	XML (TCP)	XML API Client	Enables managing PathFinder server via XML API	The External Management System cannot get PathFinder server status or receive traps from PathFinder server	Optional

Table 24: 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 .

Related Links

Implementing Port Security for Avaya Scopia® PathFinder on page 45

Configuring Ports on the PathFinder server

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

Related Links

Implementing Port Security for Avaya Scopia® PathFinder on page 45
Configuring the UDP Port for RAS on the PathFinder server on page 50
Limiting the TCP/UDP Port Range for H.323 Direct Access Calls on the PathFinder server on page 50

Configuring the UDP Port for RAS on the PathFinder server

About this task

The Avaya Scopia® PathFinder server assumes the gatekeeper uses 1719 as the designated port 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 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 50).

Figure 15: Gatekeeper Settings

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

Related Links

Configuring Ports on the PathFinder server on page 50

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

About this task

The Avaya 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 PathFinder server. To provide additional security for your firewall, you can limit this range.

To calculate approximately how many ports the 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 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 51).

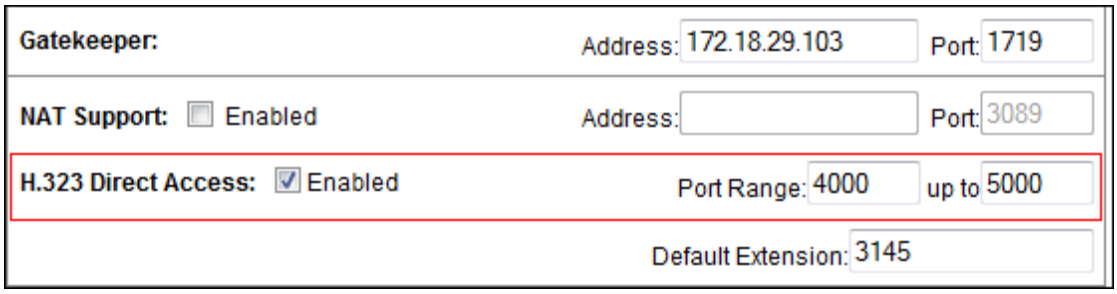

Figure 16: H.323 Direct Access Settings

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

Related Links

Configuring Ports on the PathFinder server on page 50

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

This section details the ports required for the Avaya Scopia® 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 Avaya Scopia® SIP Gateway, together with the relevant configuration procedures:

Related Links

Ports to Open on the Scopia® Video Gateway, the Avaya Scopia® SIP Gateway, and the Avaya Scopia® TIP Gateway on page 52

Configuring Ports on the Scopia® Video Gateway, Avaya Scopia® SIP Gateway and the Avaya Scopia® TIP Gateway on page 56

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

The Scopia® Video Gateway, the Avaya Scopia® SIP Gateway, and the Avaya 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 25: Bidirectional Ports to Open on the Scopia® Video Gateway, Avaya Scopia® SIP Gateway, and the Avaya Scopia® TIP Gateway on page 53.
- If you are opening ports outbound from either gateway, see Table 26: Outbound Ports to Open from the Scopia® Video Gateway and the Avaya Scopia® SIP Gateway on page 56.
- If you are opening ports inbound to either gateway, see Table 27: Inbound Ports to Open to the Scopia® Video Gateway, Avaya Scopia® SIP Gateway, and the Avaya Scopia® TIP Gateway on page 56.

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 25: Bidirectional Ports to Open on the Scopia® Video Gateway, Avaya Scopia® SIP Gateway, and the Avaya 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, Avaya Scopia® SIP Gateway, and Avaya Scopia® TIP Gateway on page 57
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 Avaya Scopia® TIP Gateway on page 60
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 Avaya Scopia® TIP Gateway on page 61

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
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
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 Avaya Scopia® TIP Gateway on page 58
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 Avaya Scopia® TIP

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
					Gateway on page 58
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 Avaya Scopia® TIP Gateway on page 58
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 Avaya Scopia® TIP Gateway on page 58
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 Avaya Scopia® TIP Gateway on page 58
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 Avaya Scopia® TIP Gateway on page 58

Table 26: Outbound Ports to Open from the Scopia® Video Gateway and the Avaya Scopia® 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 27: Inbound Ports to Open to the Scopia® Video Gateway, Avaya Scopia® SIP Gateway, and the Avaya 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

Related Links

Implementing Port Security for the Scopia® Video Gateway and the Avaya Scopia® SIP Gateway on page 52

Configuring Ports on the Scopia® Video Gateway, Avaya Scopia® SIP Gateway and the Avaya Scopia® TIP Gateway

This section provides instructions of how to configure the following ports and port ranges on the Scopia® Video Gateway,Avaya Scopia® SIP Gatewayand theAvaya Scopia® TIP Gateway.

Related Links

Implementing Port Security for the Scopia® Video Gateway and the Avaya Scopia® SIP Gateway on page 52
Limiting TCP Port Range for H.245 on the Scopia® Video Gateway, Avaya Scopia® SIP Gateway, and Avaya Scopia® TIP Gateway on page 57
Configuring RTP/RTCP/SRTP Ports on the Scopia® Video Gateway, SIP Gateway and Avaya Scopia® TIP Gateway on page 58
Configuring UDP Port for RAS on the Scopia® Video Gateway, SIP Gateway and Avaya Scopia® TIP Gateway on page 60

Configuring TCP Port for Q.931 on the Scopia® Video Gateway, SIP Gateway, and Avaya Scopia® TIP Gateway on page 61

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

About this task

The Scopia® Video Gateway, Avaya Scopia® SIP Gateway and Avaya 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 57).

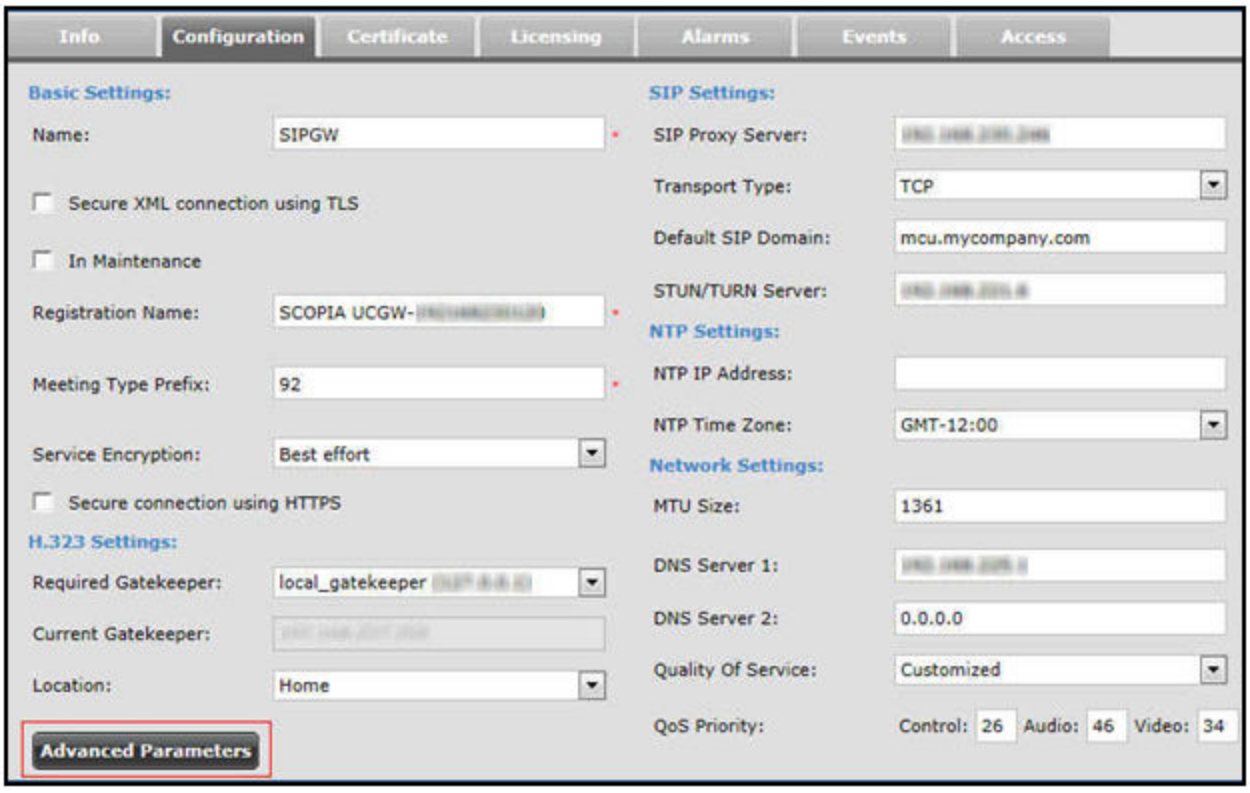

Figure 17: Configuring a gateway from Scopia® Management

5. Select **Advanced Parameters**. The **Advanced Parameters** dialog box appears (see Figure 17: Configuring a gateway from Scopia® Management on page 57).
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**

Related Links

Configuring Ports on the Scopia® Video Gateway, Avaya Scopia® SIP Gateway and the Avaya Scopia® TIP Gateway on page 56

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

About this task

The Scopia® Video Gateway, Avaya Scopia® SIP Gateway and Avaya 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 57).
6. Select **Advanced Parameters Settings**. The **Advanced Parameters** dialog box appears (see Figure 17: Configuring a gateway from Scopia® Management on page 57).

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**.

Related Links

Configuring Ports on the Scopia® Video Gateway, Avaya Scopia® SIP Gateway and the Avaya Scopia® TIP Gateway on page 56

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

About this task

The Scopia® Video Gateway, Avaya Scopia® SIP Gateway and the Avaya 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 57).
6. Select **Advanced Parameters Settings**. The **Advanced Parameters** dialog box appears (see Figure 17: Configuring a gateway from Scopia® Management on page 57).
   a. Select **h323rasport** from the **Command ID** list.
   b. Enter the port value in the **Value** field.
   c. Select **Save**.
   d. Select **Close**.

Related Links

Configuring Ports on the Scopia® Video Gateway, Avaya Scopia® SIP Gateway and the Avaya Scopia® TIP Gateway on page 56

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

About this task

The Scopia® Video Gateway, Avaya Scopia® SIP Gateway, and Avaya 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 57).
6. Select **Advanced Parameters Settings**. The **Advanced Parameters** dialog box appears (see Figure 17: Configuring a gateway from Scopia® Management on page 57).
   a. Select **h323sigport** from the **Command ID** list.
   b. Enter the port value in the **Value** field.
   c. Select **Save**.
   d. Select **Close**.

Related Links

Configuring Ports on the Scopia® Video Gateway, Avaya Scopia® SIP Gateway and the Avaya Scopia® TIP Gateway on page 56

Chapter 7: Implementing Port Security for Avaya Scopia® ECS Gatekeeper

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

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

Related Links

Ports to Open on Avaya Scopia® ECS Gatekeeper on page 62
Configuring Ports on Avaya Scopia® ECS Gatekeeper on page 64

Ports to Open on Avaya Scopia® ECS Gatekeeper

Avaya 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 28: Bidirectional Ports to Open on Avaya Scopia® ECS Gatekeeper on page 62.
- If you are opening ports that are outbound from the ECS, see Table 29: Outbound Ports to Open from Avaya Scopia® ECS Gatekeeper on page 64.

Important:

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

Table 28: Bidirectional Ports to Open on Avaya 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

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
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 Avaya Scopia® ECS Gatekeeper on page 66
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 Avaya Scopia® ECS Gatekeeper on page 65
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 Avaya Scopia® ECS Gatekeeper on page 65
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	External management servers cannot connect to ECS	Mandatory if deployed with Scopia® Management

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
			to the ECS via XML messages		
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 29: Outbound Ports to Open from Avaya 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

Related Links

Implementing Port Security for Avaya Scopia® ECS Gatekeeper on page 62

Configuring Ports on Avaya Scopia® ECS Gatekeeper

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

Related Links

Implementing Port Security for Avaya Scopia® ECS Gatekeeper on page 62
Limiting the TCP Port Range for H.245/Q.931 on Avaya Scopia® ECS Gatekeeper on page 65
Configuring the HTTP Port on Avaya Scopia® ECS Gatekeeper on page 66
Configuring the TCP Port for the Alternate Gatekeeper Protocol on Avaya Scopia® ECS Gatekeeper on page 67
Configuring the UDP Port for SNMP Traps on Avaya Scopia® ECS Gatekeeper on page 69

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

About this task

Avaya Scopia® ECS Gatekeeper uses the same TCP port range as the underlying Windows system TCP port ranges for H.245/Q.931, which depends on the version of Windows you are running:

- If you have Windows XP or Windows Server 2003, ECS uses the Windows default dynamic port range: 1025-5000.
- If you have Windows Vista or Windows Server 2008 or 2012, ECS uses the Windows default dynamic port range: 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** on a 32-bit Windows system.
   - **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\RADVISION\Enhanced Communication Server\Storage\Config\Stack** on a 64-bit Windows system.
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. Verify the **PortMax** value is within the Windows port range:
   - On Windows XP or Windows Server 2003, navigate to **HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services\Tcpip\Parameters**.

     If **MaxUserPort** is not defined there, its default is **5000**. To change the system's default maximum port number, define and set a value for **MaxUserPort**. Then restart the computer.
   - On Windows Vista, Windows 7, Windows Server 2008 and Windows Server 2012, check the system's maximum port value in a command line window by entering:

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

     To change the system's default maximum, open the command line prompt as an administrator by right-clicking on **cmd** and selecting **Run as administrator**, and enter the following command:

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

     Enter the **show** command to verify the maximum port has changed.

   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`.

   In either case, **PortMax** should be lower than the system's maximum port number.
7. Access the Windows Services and start the **ECS service**.

Related Links

Configuring Ports on Avaya Scopia® ECS Gatekeeper on page 64

Configuring the HTTP Port on Avaya Scopia® ECS Gatekeeper

About this task

Avaya 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 67).

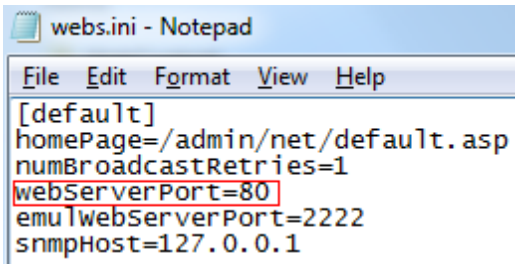

Figure 18: webs.ini File

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

Related Links

Configuring Ports on Avaya Scopia® ECS Gatekeeper on page 64

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

About this task

Avaya 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 68).

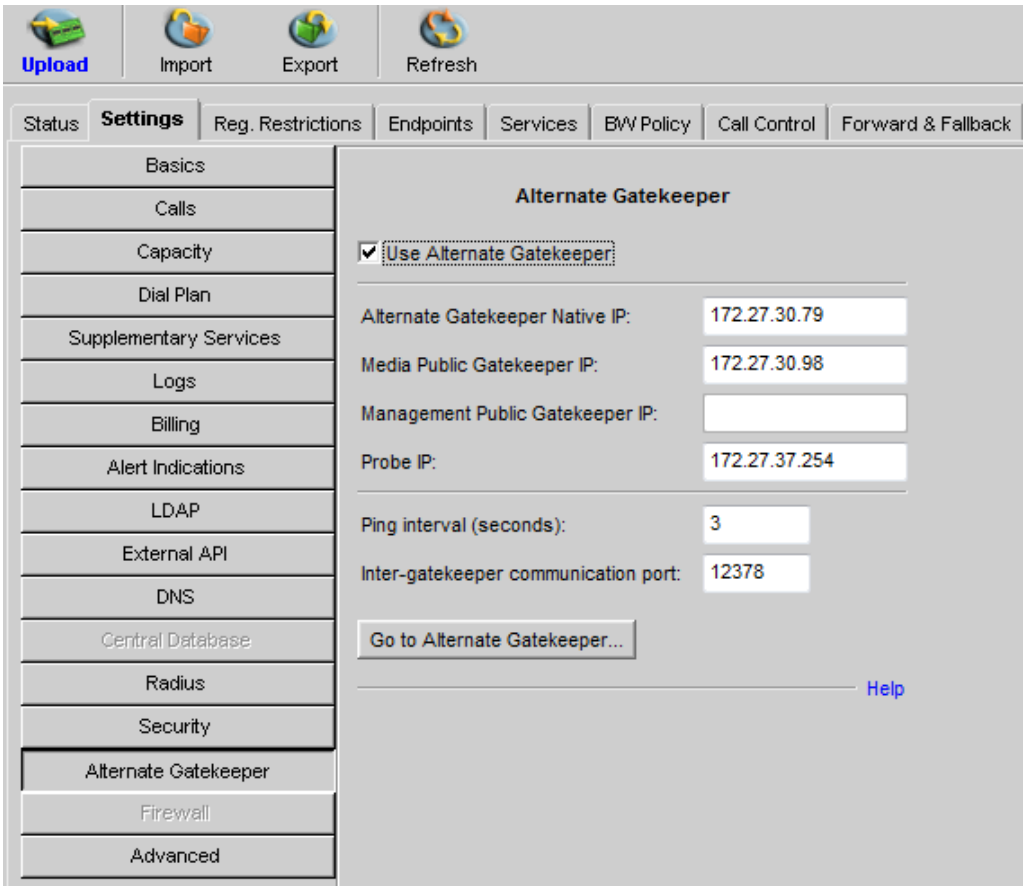

Figure 19: Alternate Gatekeeper Settings

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**.

Related Links

Configuring Ports on Avaya Scopia® ECS Gatekeeper on page 64

Configuring the UDP Port for SNMP Traps on Avaya Scopia® ECS Gatekeeper

About this task

Avaya 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 69).

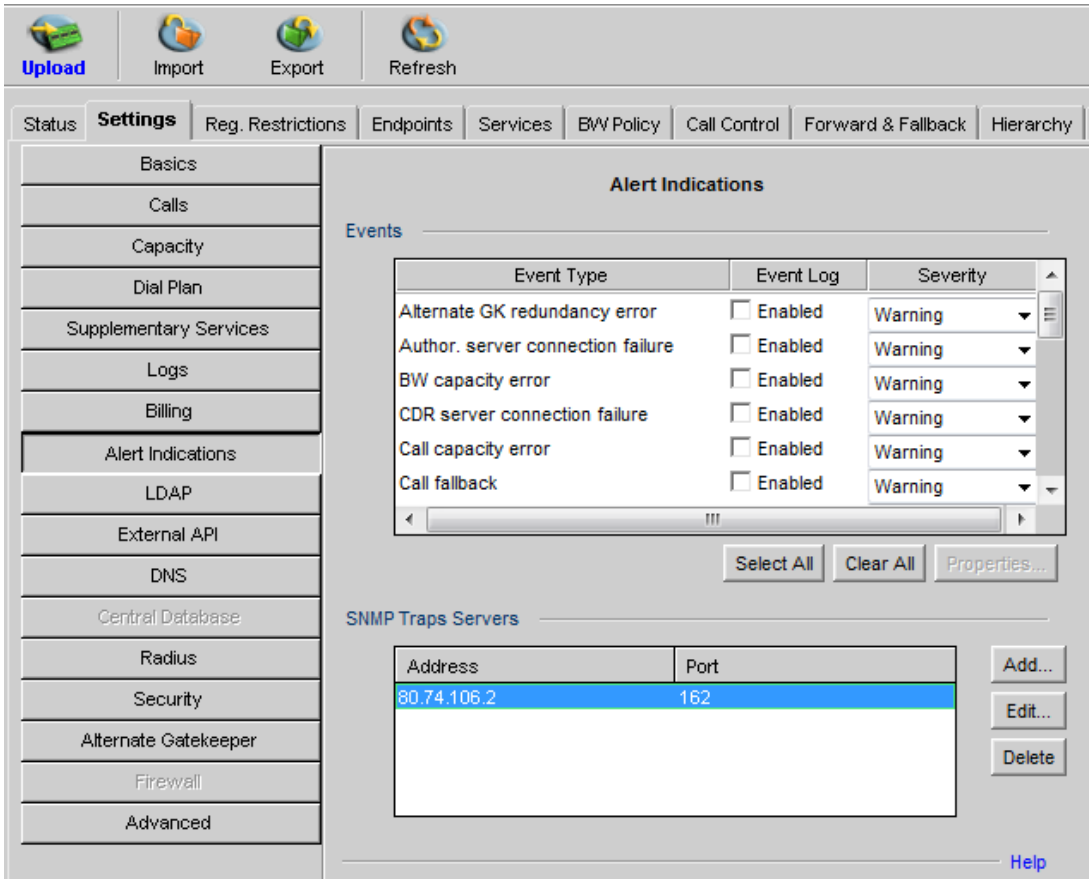

Figure 20: Alert Indications Settings

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 70).

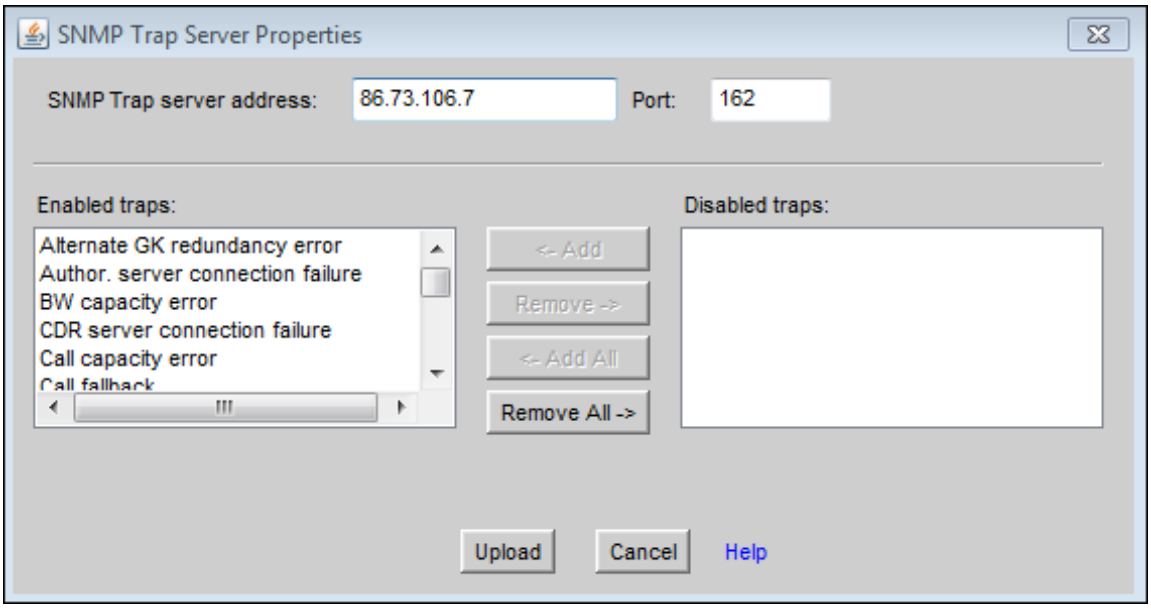

Figure 21: SNMP Trap Server Properties

6. Modify the port value in the **Port** field.
7. Select **Upload**.
8. To log out of the web user interface, select **Logout**.

Related Links

Configuring Ports on Avaya Scopia® ECS Gatekeeper on page 64

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:

Related Links

Ports to Open for the Scopia® XT Desktop server on page 71
Limiting Port Ranges on the Scopia® XT Desktop server on page 74

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 30: Bidirectional Ports to Open Between the Scopia® XT Desktop server and the Enterprise on page 72.
- For a list of outbound ports from the Scopia® XT Desktop server, see Table 31: Outbound Ports to Open from the Scopia® XT Desktop server to the Enterprise Scopia® Desktop on page 72.
- For a list of inbound ports to the Scopia® XT Desktop server, see Table 32: Inbound Ports to Open from the Enterprise to the Scopia® XT Desktop server on page 73.

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 33: Bidirectional Ports to Open Between the Scopia® XT Desktop server and the Public on page 73.
- For a list of inbound ports to the Scopia® XT Desktop server, see Table 34: Inbound Ports to Open from the Public to the Scopia® XT Desktop server on page 74.

Table 30: 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® XT1200	Enables H.323 traffic between the Scopia® XT Desktop server and the Scopia® XT1200	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 75Limiting the TCP Port Range on the Scopia® XT Desktop server on page 75
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 75

Table 31: Outbound Ports to Open from the Scopia® XT Desktop server to the Enterprise Scopia® Desktop

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3336, 3337	XML (TCP)	Scopia® XT1200	Enables cascading/ XML control connections between Scopia® XT Desktop server and Scopia® XT1200	Scopia® XT Desktop calls do not work	Mandatory

Table 32: 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 33: 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 75

Table 34: 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

Related Links

Implementing Port Security for the Scopia® XT Desktop server on page 71

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:

Related Links

Implementing Port Security for the Scopia® XT Desktop server on page 71
Limiting the TCP Port Range on the Scopia® XT Desktop server on page 75
Limiting the UDP Port Range on the Scopia® XT Desktop server on page 75

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.

Related Links

Limiting Port Ranges on the Scopia® XT Desktop server on page 74

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 76).

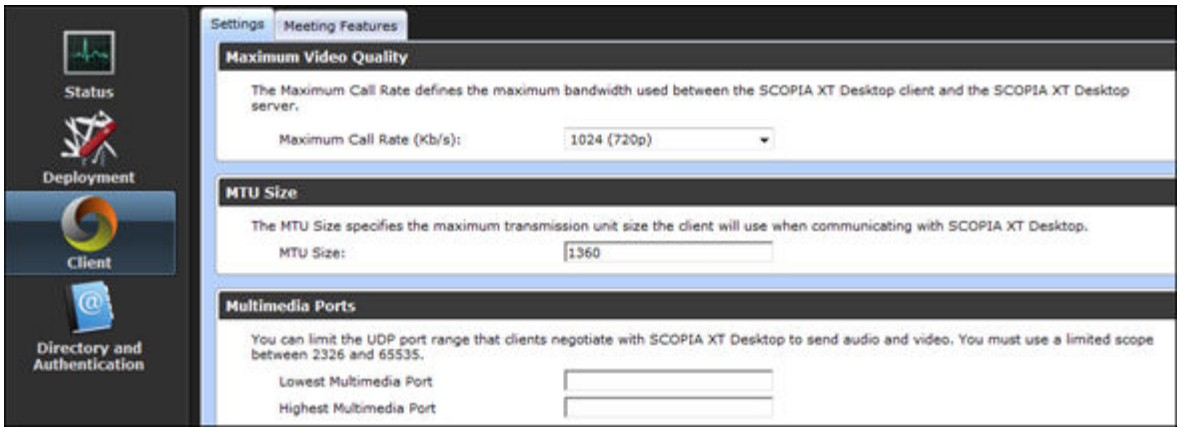

Figure 22: UDP Multimedia Ports

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**.

Related Links

Limiting Port Ranges on the Scopia® XT Desktop server on page 74

Chapter 9: Implementing Port Security for the Avaya Scopia® XT Series

The Avaya 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).

To enable an external XT Series endpoint to communicate with Scopia® Solution components within the organization's network, you need to open firewall ports between the external XT Series endpoint and the organization. This section details the ports used for the Avaya Scopia® XT Series and the relevant configuration procedures:

Related Links

Opening Ports for the XT Series on page 77
Configuring the TCP or UDP Port Range on the Avaya Scopia® XT Series on page 86

Opening Ports for the XT Series

You can deploy Avaya Scopia® XT Series endpoints either inside or outside the enterprise network. When Scopia® Solution components are located inside the network, and one or more XT Series endpoints are outside the network, you must open ports in the firewall to enable the endpoint's functionality.

Since the location of the XT Series is not fixed, the ports' source and destination differ depending on your XT Series topology. There are two main deployment topologies for the XT Series, each with optional additional components:

- XT Series as an endpoint (standard topology)
- XT Series with Scopia® XT Desktop (Avaya Scopia® XT Series SMB Edition)

Typically, XT Series endpoints connect to a conference managed by Scopia® Management, and hosted on the Scopia® Elite MCU. XT Series endpoints may be both within and outside the enterprise. See Figure 23: Standard topology for Avaya Scopia® XT Series on page 78.

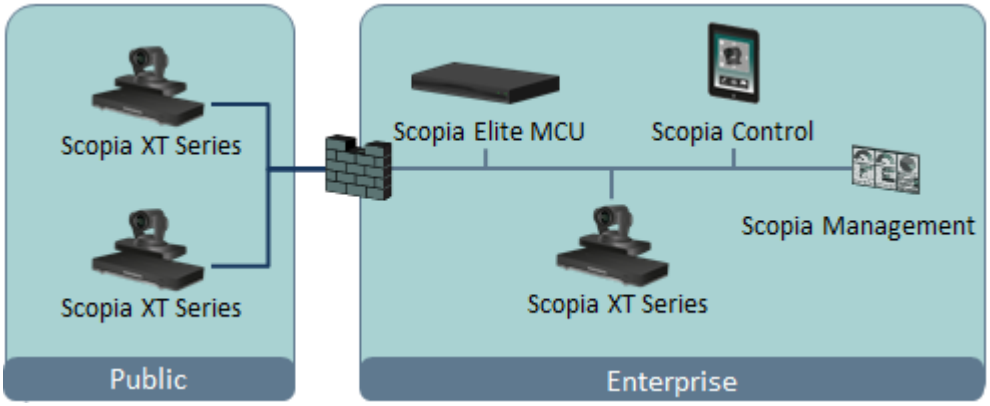

Figure 23: Standard topology for Avaya Scopia® XT Series

In contrast, in the Avaya Scopia® XT Series SMB Edition topology, Scopia® Desktop Clients join the conference via Scopia® XT Desktop server, located in the DMZ. The Scopia® XT Desktop server then connects to an XT Series endpoint with built-in MCU located inside the enterprise. External and internal XT Series endpoints connect directly to the XT Series endpoint with built-in MCU. See Figure 24: Avaya Scopia® XT Series SMB Edition topology on page 78.

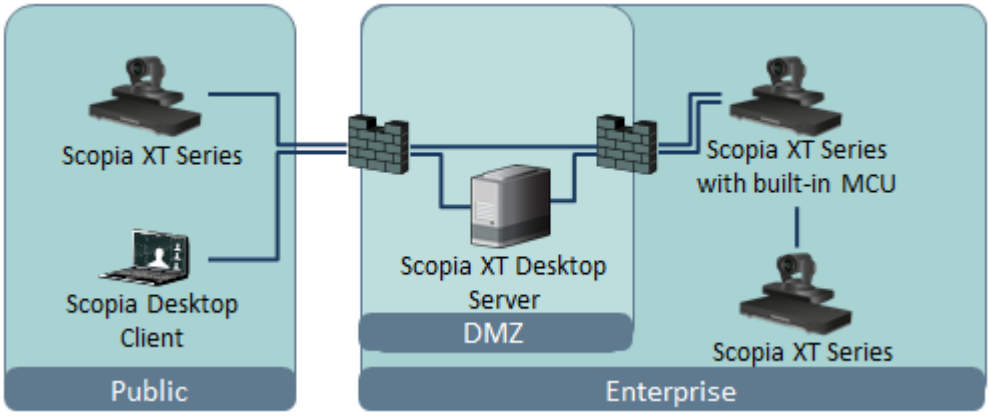

Figure 24: Avaya Scopia® XT Series SMB Edition topology

Avaya Scopia® PathFinder provides a complete firewall and NAT traversal solution for H.323 deployments, enabling secure connectivity between enterprise networks and remote sites. Scopia® PathFinder enables registered external endpoints to traverse the firewall without requiring you to open any dedicated ports for the XT Series. See Figure 25: XT Series deployment with Scopia® PathFinder on page 79

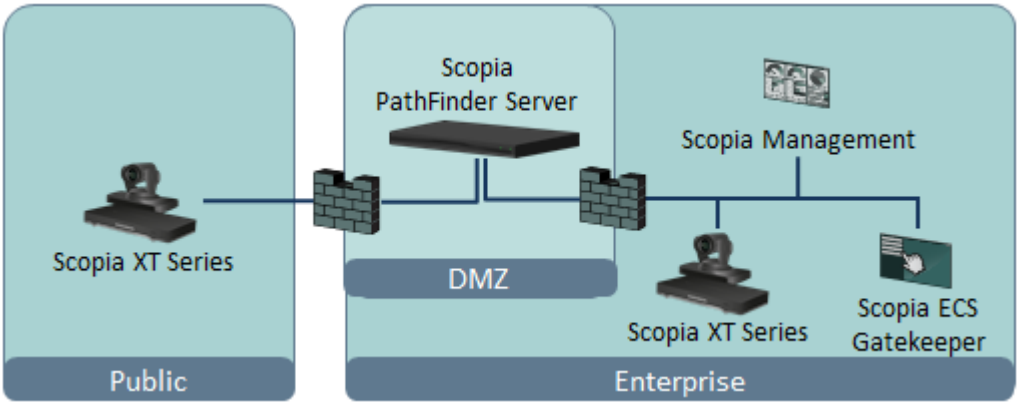

Figure 25: XT Series deployment with Scopia® PathFinder

In each of the topologies, the XT Series can be located either inside or outside the enterprise. You need to open different ports depending on the topology, and the location of the endpoints. The source for a port is the sender of data packets, and the destination is the receiver. There are two types of ports which require opening (see Figure 26: Inbound and outbound ports for the XT Series on page 79):

- Bidirectional ports, which allow the XT Series to send and receive data packets on the same port.
- Unidirectional ports, which allow the XT Series to either initiate communication or receive data packets.

  For a unidirectional port, you must designate it as inbound or outbound. A port is inbound if its source is sending to a destination protected by the firewall (for example, data sent from an external XT Series to Scopia® Management). A port is outbound if its destination is receiving data from a source protected by the firewall (for example, data sent from Scopia® Management to an external XT Series).

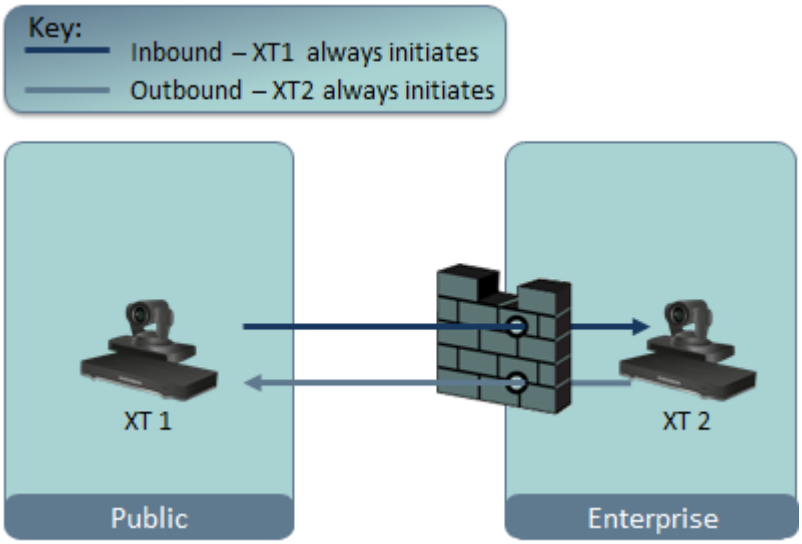

Figure 26: Inbound and outbound ports for the XT Series

Depending on the location of the XT Series, a unidirectional port might be inbound to the organization or outbound from the organization. For example:

- Port 161 is an outbound port from Scopia® Management or an SNMP management server to an external XT Series.
- Port 162 is an inbound port from an external XT Series to Scopia® Management or an SNMP management server.

Important:

On stateful firewalls, ports are left open to response data for an allocated period of time after the initial request. For unidirectional ports, this response is the only data allowed through in the opposite direction. On bidirectional ports, data can be initiated and sent through in both directions.

If you are opening unidirectional ports for the XT Series, see Table 35: Unidirectional ports to open for the XT Series on page 80. You need to determine if they are inbound or outbound depending on the source and destination.

If you are opening bidirectional ports for the XT Series, see Table 36: Bidirectional ports to open for the XT Series on page 85.

Table 35: Unidirectional ports to open for the XT Series

Port Range	Protocol	Source	Destination	Functionality	Result of Blocking Port	Required
69	TFTP (TCP)	XT Series	TFTP server	Enables the XT Series to send configuration, log, and other system files to a TFTP server.	The XT Series cannot send files to a TFTP server.	Optional
80	HTTP (TCP)	Web client (HTTP) / Scopia® Desktop Client	XT Series	Enables you to remotely manage the XT Series via the XT Series web user interface using HTTP. Enables you to manually activate Screen Link to share content from your computer to the XT Series without having a physical connection between the two.	You cannot access the XT Series web server using HTTP. You cannot manually activate Screen or Mobile Link. Acoustic pairing detection can still activate Screen or Mobile Link automatically even if this port is closed.	Recommended if accessing the XT Series remotely via a web browser using HTTP. Recommended if using Screen Link or Mobile Link.

Table continues…

Port Range	Protocol	Source	Destination	Functionality	Result of Blocking Port	Required
				Enables you to manually activate Mobile Link to transfer a meeting from a Scopia Mobile device or Scopia® Desktop Client to an XT Series endpoint.		
80	HTTP (TCP)	XT Series	Web servers on the internet / Scopia® Desktop server Proxy	Enables the XT Series to perform NAT auto-discovery and detect its location via HTTP. This enables the XT to select the appropriate system language. Enables you to use Mobile Link to transfer a meeting from a Scopia Mobile device or Scopia® Desktop Client to an XT Series endpoint.	The XT Series cannot perform NAT auto-discovery or detect its location via HTTP. You cannot transfer a meeting from a Scopia Mobile device or Scopia® Desktop Client to an XT Series endpoint.	Recommended
123	SNTP (UDP)	XT Series	SNTP Server	Enables the XT Series to receive the Internet UTC time.	The XT Series cannot receive the Internet UTC time from the SNTP server.	Recommended
161	SNMP (UDP)	Scopia® Management/ SNMP server	XT Series	Enables you to check the system status via SNMP.	You cannot check the status of the system via SNMP.	Mandatory if using Scopia® Management or an SNMP server to manage the XT Series.
162	SNMP (UDP)	XT Series	Scopia® Management/ SNMP server	Enables the XT Series to send SNMP traps.	The XT Series cannot send SNMP traps.	Mandatory if using Scopia® Management or an SNMP server to

Table continues…

Port Range	Protocol	Source	Destination	Functionality	Result of Blocking Port	Required
						manage the XT Series.
389	LDAP (TCP)	XT Series	Scopia® Management/ LDAP directory	Enables the XT Series to request contact information from the LDAP server.	The XT Series cannot request contact information from the remote directory.	Mandatory if using a remote directory.
443	HTTPS (TCP)	Web client (HTTPS) / Scopia® Desktop Client	XT Series	Enables you to remotely perform management tasks using the XT Series web user interface via HTTPS. Enables you to manually activate Screen Link to share content from your computer to the XT Series without having a physical connection between the two. Enables you to manually activate Mobile Link to transfer a meeting from a Scopia Mobile device or Scopia® Desktop Client to an XT Series endpoint.	A web client cannot access the XT Series web server via HTTPS. You cannot manually activate Screen or Mobile Link. Acoustic pairing detection can still activate Screen or Mobile Link automatically even if this port is closed.	Recommended if accessing the XT Series via a web browser using HTTPS. Recommended if using Screen Link or Mobile Link.
443	HTTPS	XT Series	Scopia® Desktop server Proxy	Enables you to use Mobile Link to transfer a meeting from a Scopia Mobile device or Scopia® Desktop Client to an XT Series endpoint.	You cannot transfer a meeting from a Scopia Mobile device or Scopia® Desktop Client to an XT Series endpoint.	Recommended
1718	H. 225.0/RAS (UDP)	XT Series	Multicast IP address 224.0.0.41	Enables the XT Series to automatically	You must define the gatekeeper manually since	Optional

Table continues…

Port Range	Protocol	Source	Destination	Functionality	Result of Blocking Port	Required
			(all gatekeepers)	identify the correct gatekeeper to use.	the XT Series cannot automatically identify the correct gatekeeper to use.	
1719	H. 225.0/RAS (UDP)	XT Series	H.323 gatekeeper	Enables H.323 call signaling and gatekeeper services.	The XT Series cannot use gatekeeper services.	Mandatory for H.323 deployments.
3336	XML (TCP)	XT Series	Scopia® Management	Enables an XT Series endpoint to request a list of meetings scheduled for it on that day from Scopia® Management.	XT Series endpoints cannot send Scopia® Management requests about meeting information.	Recommended
3336-3337	XML (TCP)	Scopia® XT Desktop server	XT Series	Enables Scopia® XT Desktop server to request and receive the XT Series' status information.	Scopia® XT Desktop clients cannot connect to the XT Series.	Mandatory if using Scopia® XT Desktop server.
3338	XML (TCP)	Scopia® Control	XT Series	Enables Scopia® Control to communicate with XT Series.	Scopia® Control cannot communicate with the XT Series.	Mandatory if using Scopia® Control.
3339	XML (TCP)	Scopia® Control	XT Series	Enables Scopia® Control to request and receive system status messages from the XT Series.	Scopia® Control cannot receive system status messages from the XT Series, and cannot function.	Mandatory if using Scopia® Control.
3341	XML (TCP)	Scopia® Management	XT Series	Enables XT Series to receive notifications from Scopia® Management with its daily list of meetings, meeting participants, and any meeting updates.	XT Series endpoints cannot receive meeting information from Scopia® Management.	Recommended

Table continues…

Port Range	Protocol	Source	Destination	Functionality	Result of Blocking Port	Required
3478-3479	STUN (UDP)	XT Series	STUN server	Enables XT Series endpoints to automatically discover the presence of a firewall or NAT, via the STUN server, and to determine their public IP address.	XT Series endpoints cannot automatically discover the presence of a firewall or NAT (only manual configuration is available).	Optional
8554	RTSP (TCP)	XT Series	Scopia® Desktop Client	Enables you to use Screen Link to share content from your computer to the XT Series without having a physical connection between the two.	You cannot share content from your computer to the XT Series.	Recommended (required to share content from a computer with a personal firewall)
55000	TCP	Scopia® XT Control	XT Series	Enables you to control the Scopia® XT Executive using a PC keyboard and mouse.	You cannot use Scopia® XT Control to manage the Scopia® XT Executive.	Mandatory if using Scopia® XT Control to manage the Scopia® XT Executive using a PC keyboard and mouse from a computer with a personal firewall.
55001	UDP	Scopia® XT Control	XT Series	Enables you to control the Scopia® XT Executive using a PC keyboard and mouse.	You cannot use Scopia® XT Control to manage the Scopia® XT Executive.	Mandatory if using Scopia® XT Control to manage the Scopia® XT Executive using a PC keyboard and mouse from a computer with a personal firewall.
55003	AT commands (TCP)	Scopia® Management/ Remote	XT Series	Enables Scopia® Management and the remote	Scopia® Management and the remote	Mandatory if using Scopia® Management or

Table continues…

Port Range	Protocol	Source	Destination	Functionality	Result of Blocking Port	Required
		management console (Creston/ Extron)		management console to remotely manage the XT Series.	management console cannot manage the XT Series.	the remote management console to manage the XT Series.
55099	Software upgrade (TCP)	Scopia® Management/ XT Series Software Upgrade application	XT Series	Enables you to remotely upgrade XT Series software.	You cannot upgrade XT Series software using Scopia® Management or a standalone XT Series software upgrade application.	Mandatory to upgrade XT Series software remotely.
60123	Telnet (TCP)	Telnet client	XT Series	Enables you to remotely manage the XT Series using the CLI application via Telnet.	Telnet cannot access the XT Series CLI application, and cannot remotely manage it.	Optional

Important:

Since source and destination are not fixed on bidirectional ports, we refer to them here as *Connection Points*. Each connection point can be both the source and the destination.

Table 36: Bidirectional ports to open for the XT Series

Port Range	Protocol	Connection Points	Functionality	Result of Blocking Port	Required
1720	H.225.0 /Q. 931	XT Series, Any H.323 endpoint	Enables H.323 call signaling (Q.931) for the XT Series.	The XT Series cannot connect H.323 calls.	Mandatory
3230-3250	H.225.0 / Q931, H.245, SIP (TCP)	XT Series, Any SIP or H.323 endpoint	Enables H.323 call control signaling (Q. 931), media control signaling (H.245), SIP (TCP) call signaling, and BFCP signaling. These are dynamic TCP ports which the XT Series uses to connect simultaneous H.323 and SIP calls.	The XT Series cannot connect SIP or H.323 calls.	Mandatory to support H.323 calls, and to support SIP calls on TCP. To configure, see Configuring the TCP or UDP Port Range on the Avaya Scopia® XT

Table continues…

Port Range	Protocol	Connection Points	Functionality	Result of Blocking Port	Required
					Series on page 86.
3230-3313	RTP, RTCP (UDP)	XT Series, Any SIP or H.323 endpoint	Enables H.323 and SIP media (audio, video, H.224/data RTP) and media control (RTCP). These are dynamic UDP ports which the XT Series uses to connect simultaneous H.323 and SIP calls.	No media can be exchanged in H.323 or SIP calls.	Mandatory to support H.323 and SIP calls. To configure, see Configuring the TCP or UDP Port Range on the Avaya Scopia® XT Series on page 86.
5060	SIP (TCP/UDP)	XT Series, Any SIP endpoint	Enables SIP call signaling for TCP and UDP.	The XT Series cannot connect SIP calls over TCP and UDP.	Mandatory to support SIP calls over TCP and UDP.
5061	SIP (TCP)	XT Series, Any SIP endpoint	Enables SIP call signaling for TLS.	The XT Series cannot securely connect SIP calls over TCP with TLS.	Mandatory to support secure SIP calls over TCP with TLS.
5070	BFCP (TCP/UDP)	XT Series, Any SIP endpoint	Enables SIP video content (presentation) signaling.	Video content (presentation) is not available for SIP.	Mandatory to support video content in SIP calls.

Related Links

Implementing Port Security for the Avaya Scopia® XT Series on page 77

Configuring the TCP or UDP Port Range on the Avaya 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 Avaya Scopia® XT Series uses dynamic TCP ports 3230-3250 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 Avaya 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).

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in *Deployment Guide for Avaya Scopia® XT Series*.

Procedure

1. Access the port settings. From the XT Series web interface, select **Administrator Settings** > **Networks** > **Preferences** > **Dynamic Ports**. From the endpoint's main menu, select **Configure** > **Advanced** > **Networks** > **Preferences** > **Dynamic Ports**.

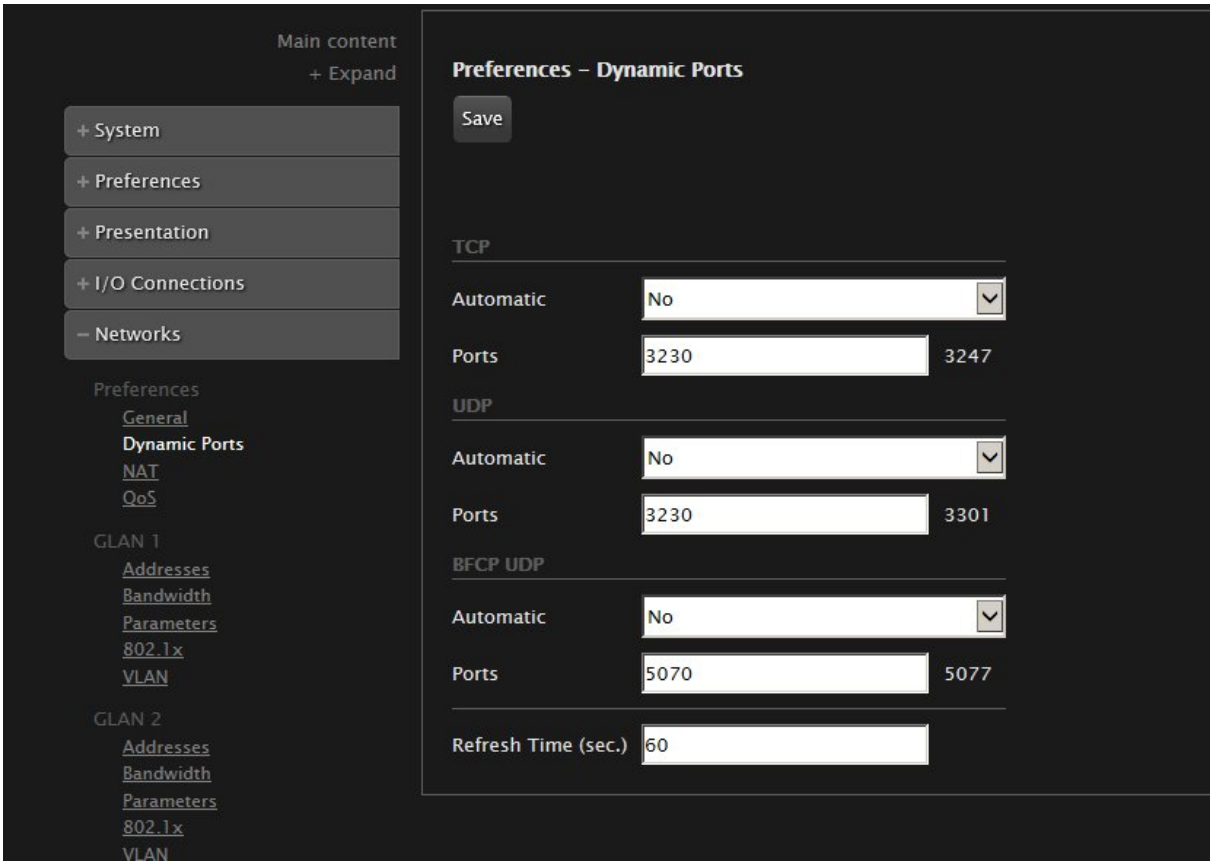

Figure 27: Configuring the TCP or UDP port range from the web interface

2. Define how the XT Series 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 **Automatic** 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**.

Related Links

Implementing Port Security for the Avaya Scopia® XT Series on page 77

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:

Related Links

Ports to Open for Scopia® VC240 on page 89
Configuring Port Ranges on the Scopia® VC240 on page 92

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 37: Bidirectional Ports to Open on the Scopia® VC240 on page 90.
- If opening outbound ports from the Scopia® VC240, see Table 38: Outbound Ports to Open from the Scopia® VC240 on page 91.
- If opening inbound ports to the Scopia® VC240, see Table 39: Inbound Ports to Open to the Scopia® VC240 on page 91.

Important:

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

Table 37: 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
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 92
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 92
4000	RV shell cmd (UDP)	Scopia® Management	Internal use Enables connection to Scopia® Management	Cannot connect to Scopia® Management	

Table continues…

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
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 38: 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 39: 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

Related Links

Implementing Port Security for the Scopia® VC240 on page 89

Configuring Port Ranges on the Scopia® VC240

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

Related Links

Implementing Port Security for the Scopia® VC240 on page 89
Configuring the TCP Port Range for H.245 on the Scopia® VC240 on page 92
Configuring the UDP Port Range for RTP/RTCP on the Scopia® VC240 on page 92

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**.

Related Links

Configuring Port Ranges on the Scopia® VC240 on page 92

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**.

Related Links

Configuring Port Ranges on the Scopia® VC240 on page 92

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:

Related Links

Ports to Open on the Scopia® Gateway on page 93
Configuring Ports on the Scopia® Gateway on page 96
Configuring Security Access Levels for the Scopia® Gateway on page 101

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 40: Bidirectional Ports to Open on the Scopia® Gateway on page 94.
- If opening outbound ports from the Scopia® Gateway, see Table 41: Outbound Ports to Open from the Scopia® Gateway on page 96.
-

Important:

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

Table 40: 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
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 96
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

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
					To configure, see Configuring the Gatekeeper Port on the Scopia® Gateway on page 97
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 98
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 98
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®	Cannot transmit/ receive media streams	Mandatory

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
			Gateway and not to the IVR		
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 41: 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

Related Links

Implementing Port Security for the Scopia® Gateway on page 93

Configuring Ports on the Scopia® Gateway

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

Related Links

Implementing Port Security for the Scopia® Gateway on page 93
Configuring the HTTP Port on the Scopia® Gateway on page 96
Configuring the Gatekeeper Port on the Scopia® Gateway on page 97
Configuring the TCP Port for Q.931 on the Scopia® Gateway on page 98

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 28: Scopia® Gateway Web Settings on page 97).

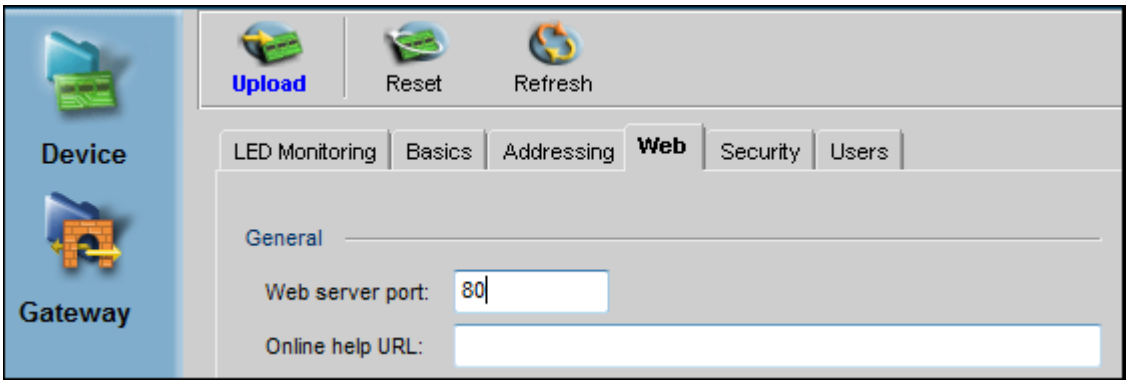

Figure 28: Scopia® Gateway Web Settings

4. Select **Upload**.

Related Links

Configuring Ports on the Scopia® Gateway on page 96

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 29: Gatekeeper Port Settings on page 98).

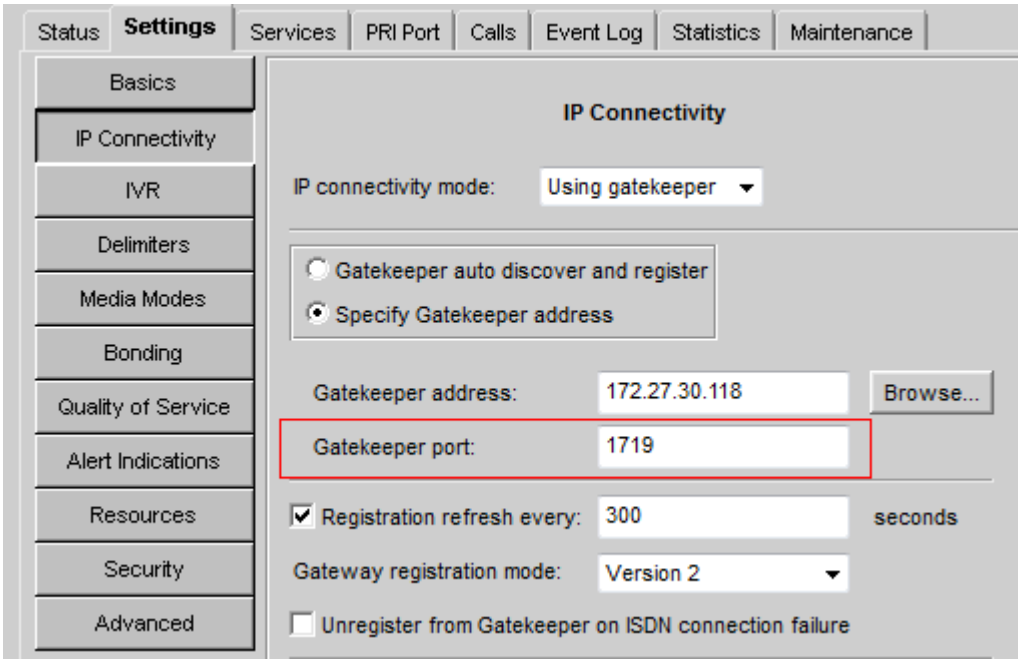

Figure 29: Gatekeeper Port Settings

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

Related Links

Configuring Ports on the Scopia® Gateway on page 96

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 30: Scopia® Gateway Advanced Settings on page 99).

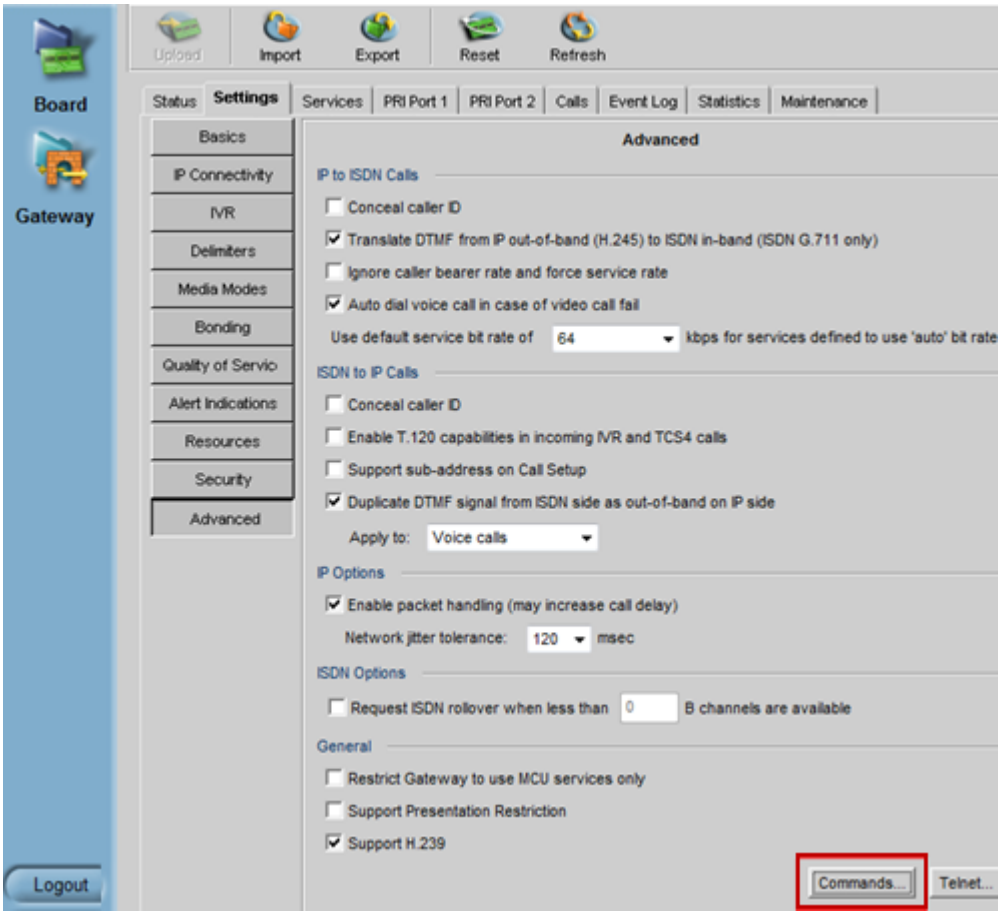

Figure 30: Scopia® Gateway Advanced Settings

3. Select **Commands**. The **Advanced Commands** dialog box appears (see Figure 31: Scopia® Gateway Advanced Commands on page 100).

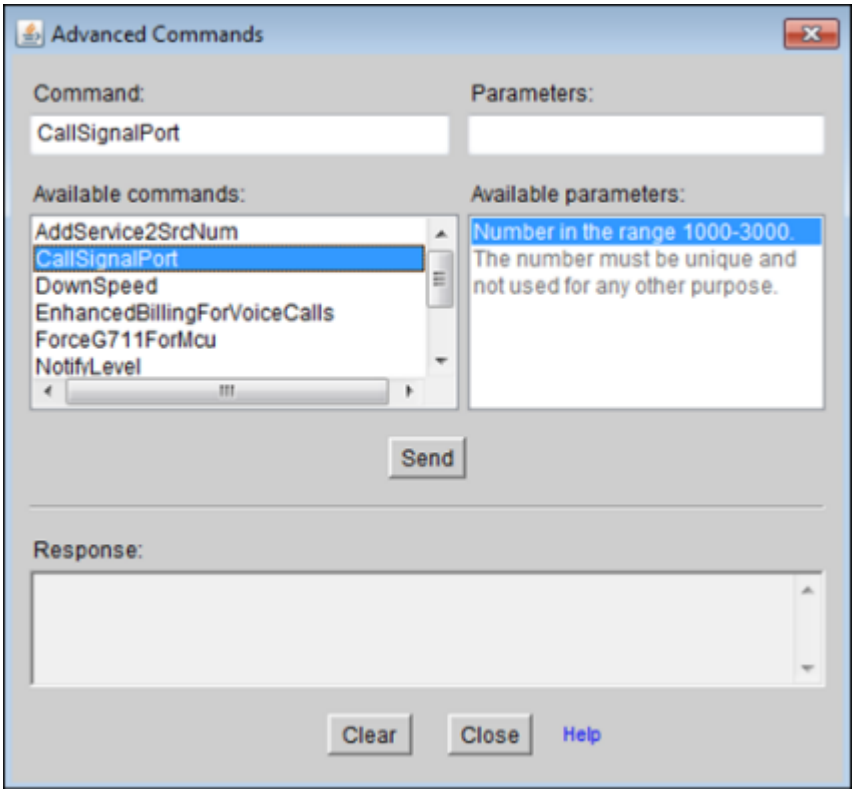

Figure 31: Scopia® Gateway Advanced Commands

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**.

Related Links

Configuring Ports on the Scopia® Gateway on page 96

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 32: Scopia® Gateway Security Settings on page 101). Table 42: Scopia® Gateway Security Access Levels on page 101 lists the protocol status when each security access level is applied.

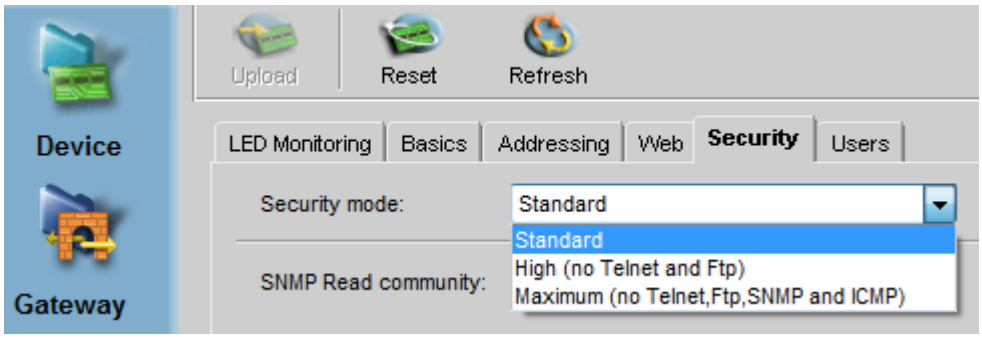

Figure 32: Scopia® Gateway Security Settings

Table 42: 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**.

Related Links

Implementing Port Security for the Scopia® Gateway on page 93

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:

Related Links

Ports to Open on the Scopia 3G Gateway on page 102
Configuring Ports on the Scopia 3G Gateway on page 104
Configuring Security Access Levels for the Scopia 3G Gateway on page 109
Ports to Open on the Scopia 3G Gateway SP for Media Blade on page 110

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 43: Bidirectional Ports to Open on the Media Blade on page 103.
- If opening outbound ports from the Media Blade, see Table 44: Outbound Ports to Open from the Media Blade on page 104.
- If opening inbound ports to the Media Blade, see Table 45: Inbound Ports to Open to the Media Blade on page 104.

Important:

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

Table 43: 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
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 105
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 105
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 107
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

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
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 108
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 44: 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 45: 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

Related Links

Implementing Port Security for the Scopia 3G Gateway on page 102

Configuring Ports on the Scopia 3G Gateway

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

Related Links

Implementing Port Security for the Scopia 3G Gateway on page 102

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 33: Scopia 3G Gateway HTTP Settings on page 105).

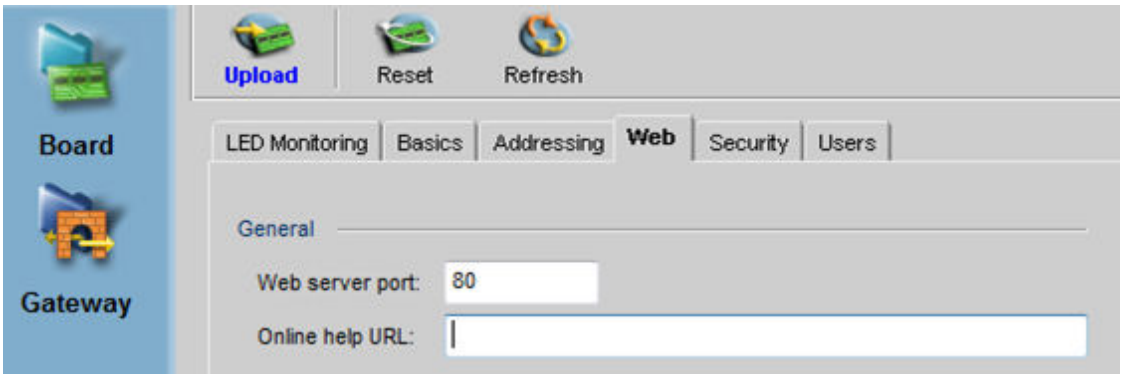

Figure 33: Scopia 3G Gateway HTTP Settings

4. Select **Upload**.

Related Links

Configuring Ports on the Scopia 3G Gateway on page 104

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 34: Scopia 3G Gateway Gatekeeper Settings on page 106).

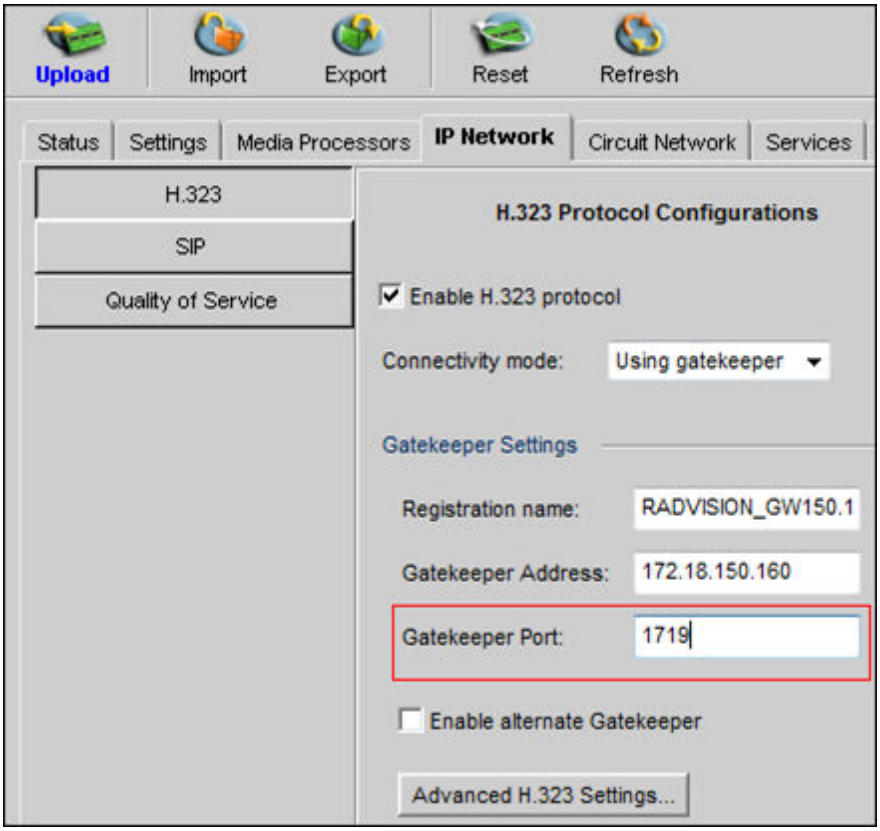

Figure 34: Scopia 3G Gateway Gatekeeper Settings

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 35: Advanced H.323 Settings on page 107).

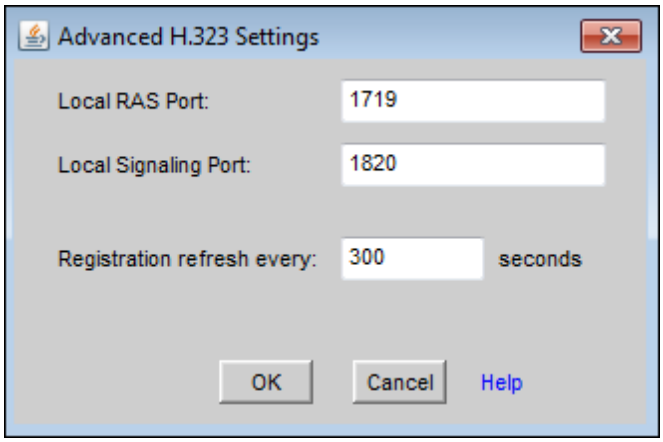

Figure 35: Advanced H.323 Settings

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

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

Related Links

Configuring Ports on the Scopia 3G Gateway on page 104

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 36: Advanced H.323 Settings on page 108).

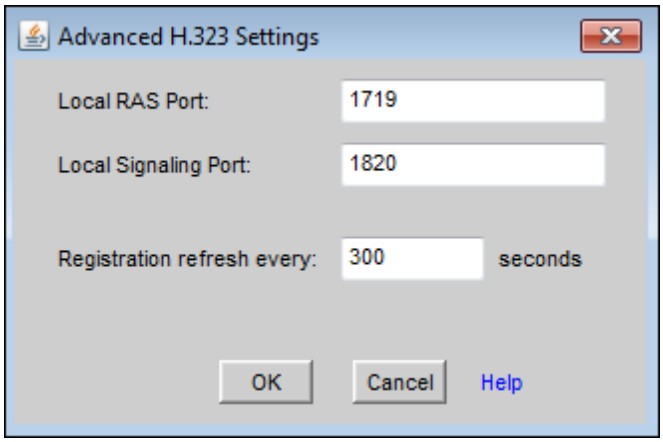

Figure 36: Advanced H.323 Settings

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

Related Links

Configuring Ports on the Scopia 3G Gateway on page 104

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 37: Scopia 3G Gateway SIP Settings on page 109).

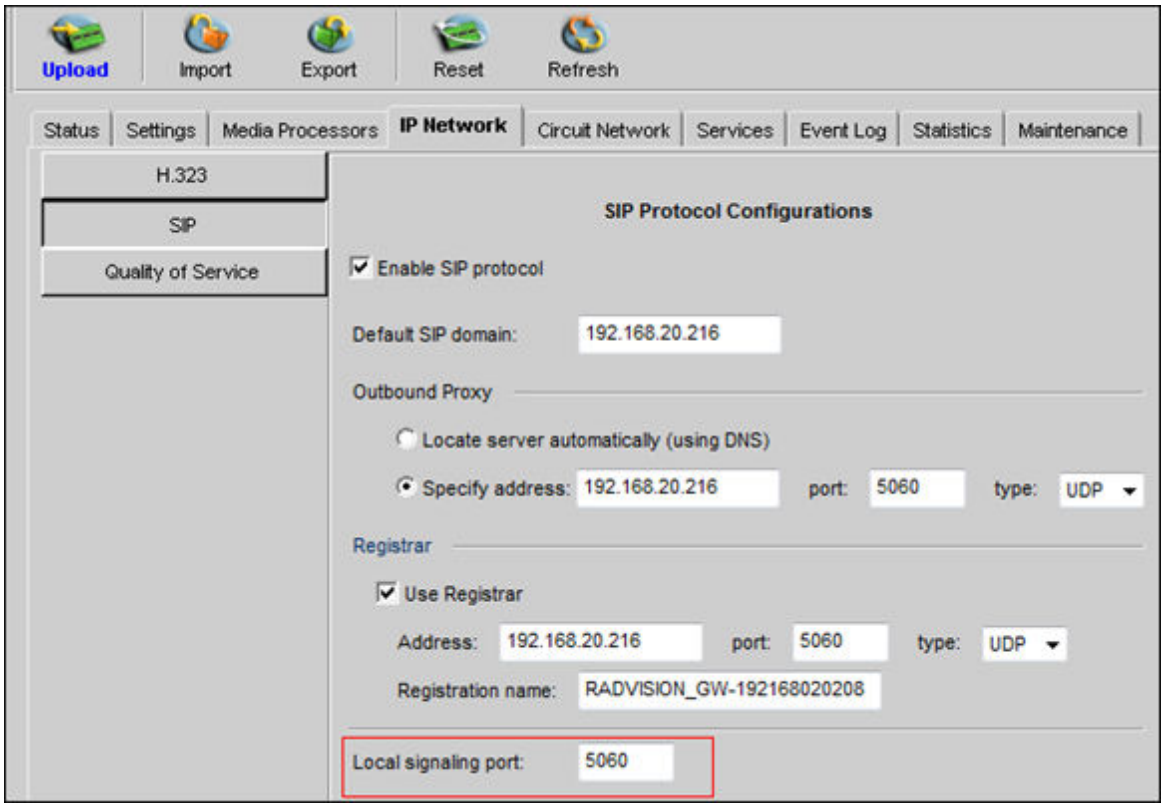

Figure 37: Scopia 3G Gateway SIP Settings

5. Select **Upload**.

Related Links

Configuring Ports on the Scopia 3G Gateway on page 104

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 38: Enabled Management Protocols Area on page 110). We recommend enabling these protocols.

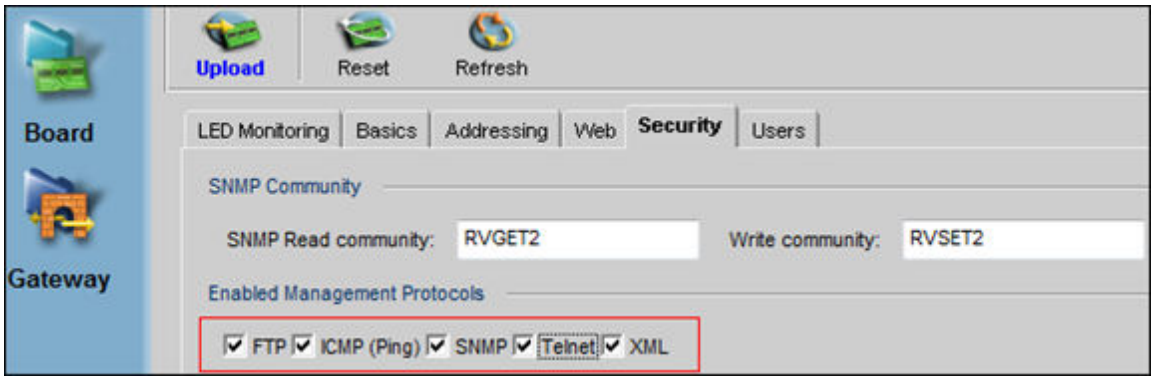

Figure 38: Enabled Management Protocols Area

3. Select **Upload**.

Related Links

Implementing Port Security for the Scopia 3G Gateway on page 102

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 46: Bidirectional Ports to Open on the Scopia 3G Gateway SP for Media Blade on page 111 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 46: Bidirectional Ports to Open on the Scopia 3G Gateway SP for Media Blade

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

Related Links

Implementing Port Security for the Scopia 3G Gateway on page 102

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:

Related Links

Ports to Open on the Scopia® MCU Blade on page 112
Configuring Ports on the Scopia® MCU Blade on page 115
Configuring Security Access Levels for the Scopia® MCU Blade on page 125
Ports to Open on the MVP for Scopia® MCU on page 126
Configuring UDP Ports for RTP/RTCP on the MVP for Scopia® MCU on page 127

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 47: Bidirectional Ports to Open on the Scopia® MCU Blade on page 113.
- If you are opening outbound ports from the Scopia® MCU blade, see Table 48: Outbound Ports to Open from the Scopia® MCU Blade on page 115.

Important:

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

Table 47: 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 115
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 116
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 119
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

Table continues…

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
					Scopia® MCU Blade on page 120
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
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 122
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 123

Table 48: 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

Related Links

Implementing Port Security for the Scopia® MCU on page 112

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:

Related Links

Implementing Port Security for the Scopia® MCU on page 112
Configuring the HTTP Port on the Scopia® MCU Blade on page 115
Limiting the TCP Port Range for H.245 on the Scopia® MCU Blade on page 116
Configuring the UDP Port for RAS on the Scopia® MCU Blade on page 119
Configuring the TCP Port for Q.931 on the Scopia® MCU Blade on page 120
Configuring the SIP Port on the Scopia® MCU Blade on page 122
Configuring the UDP Port for RTP/RTCP on the Scopia® MCU Blade on page 123

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 39: Scopia® MCU Web Settings on page 116).

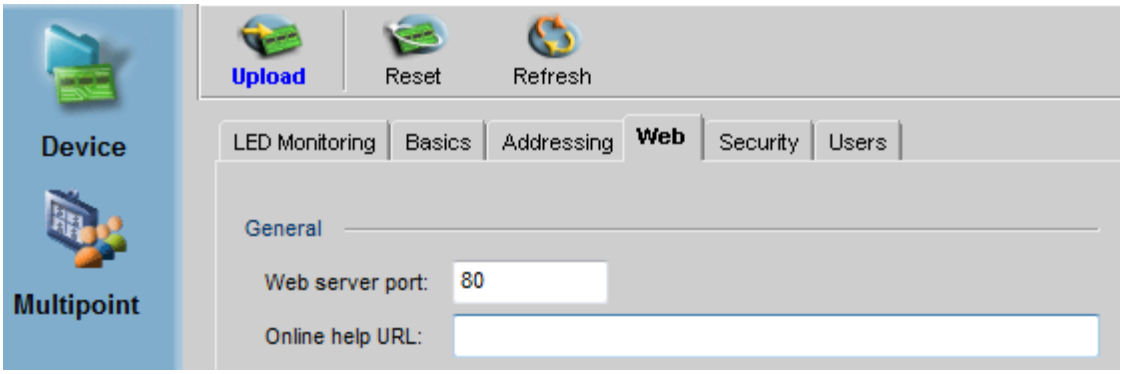

Figure 39: Scopia® MCU Web Settings

4. Select **Upload**.

Related Links

Configuring Ports on the Scopia® MCU Blade on page 115

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 40: MCU Advanced Settings on page 117).

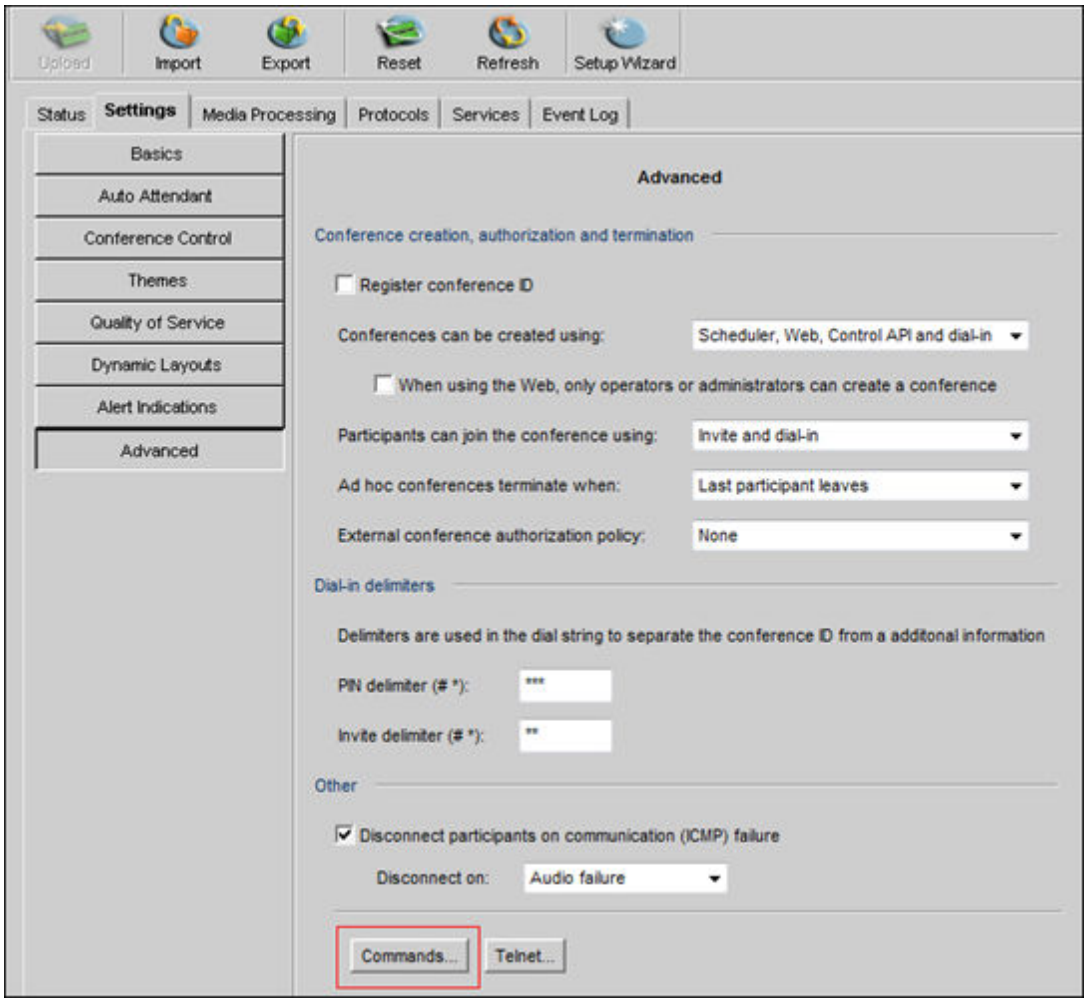

Figure 40: MCU Advanced Settings

b. Select **Commands**. The **Advanced Commands** dialog box opens (see Figure 41: MCU Advanced Commands Section on page 118).

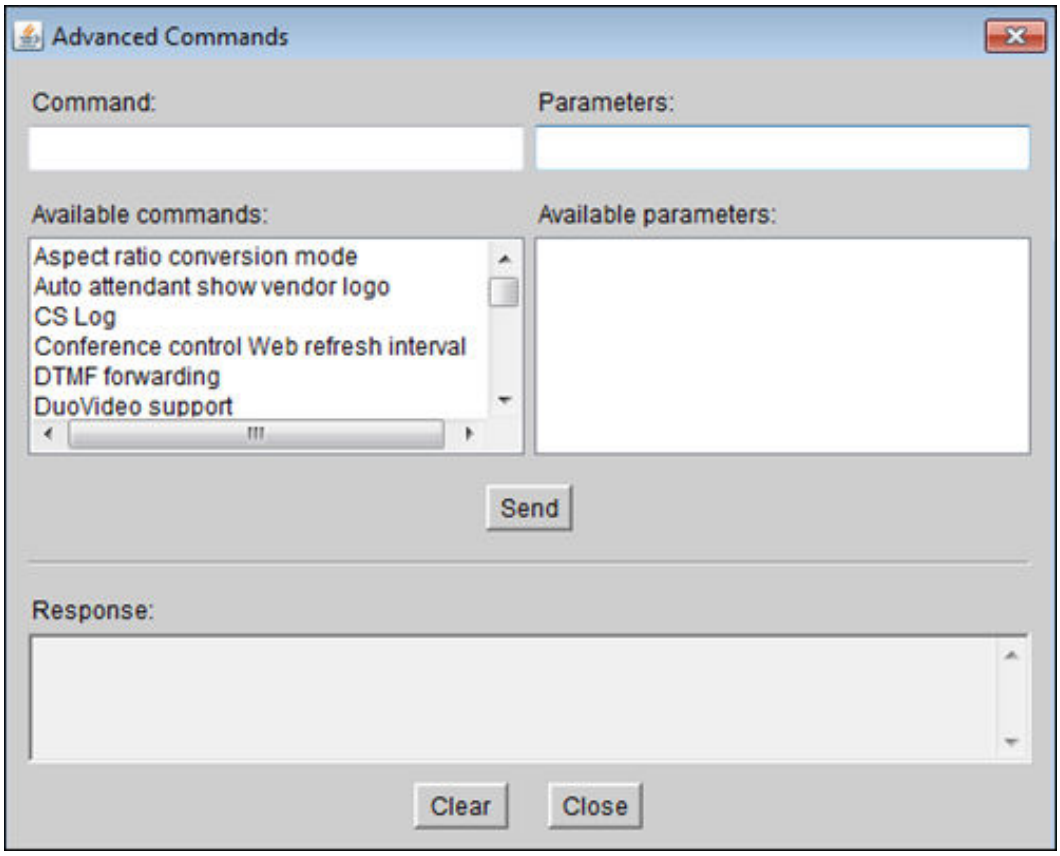

Figure 41: MCU Advanced Commands Section

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**.

Related Links

Configuring Ports on the Scopia® MCU Blade on page 115

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 42: Gatekeeper Port Settings on page 119).

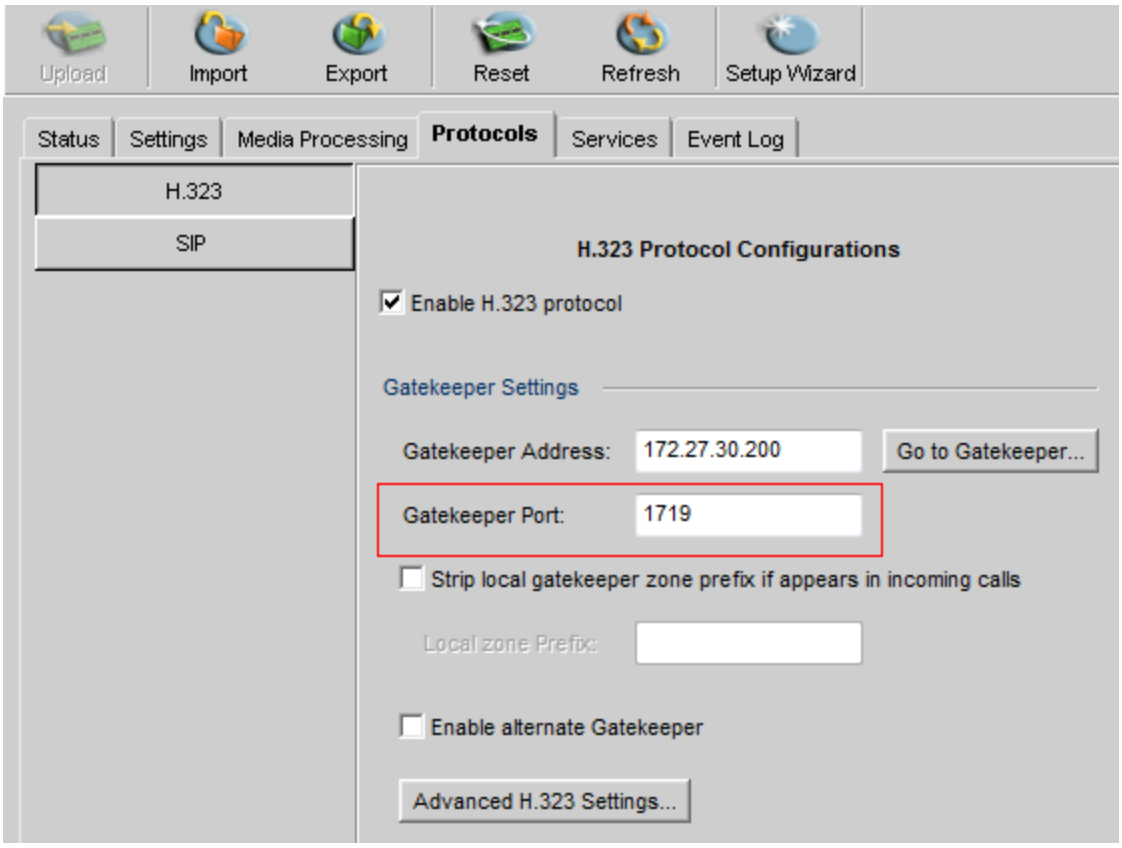

Figure 42: Gatekeeper Port Settings

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 43: Advanced H.323 Settings on page 120).

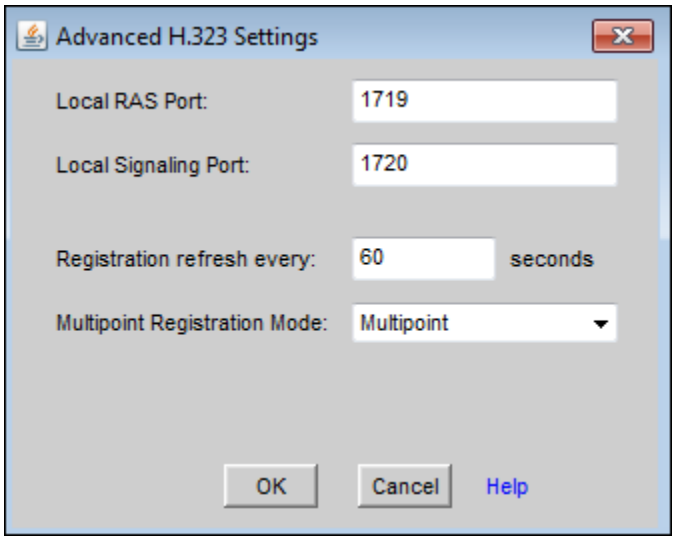

Figure 43: Advanced H.323 Settings

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

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

Related Links

Configuring Ports on the Scopia® MCU Blade on page 115

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 44: H.323 Settings on page 121).

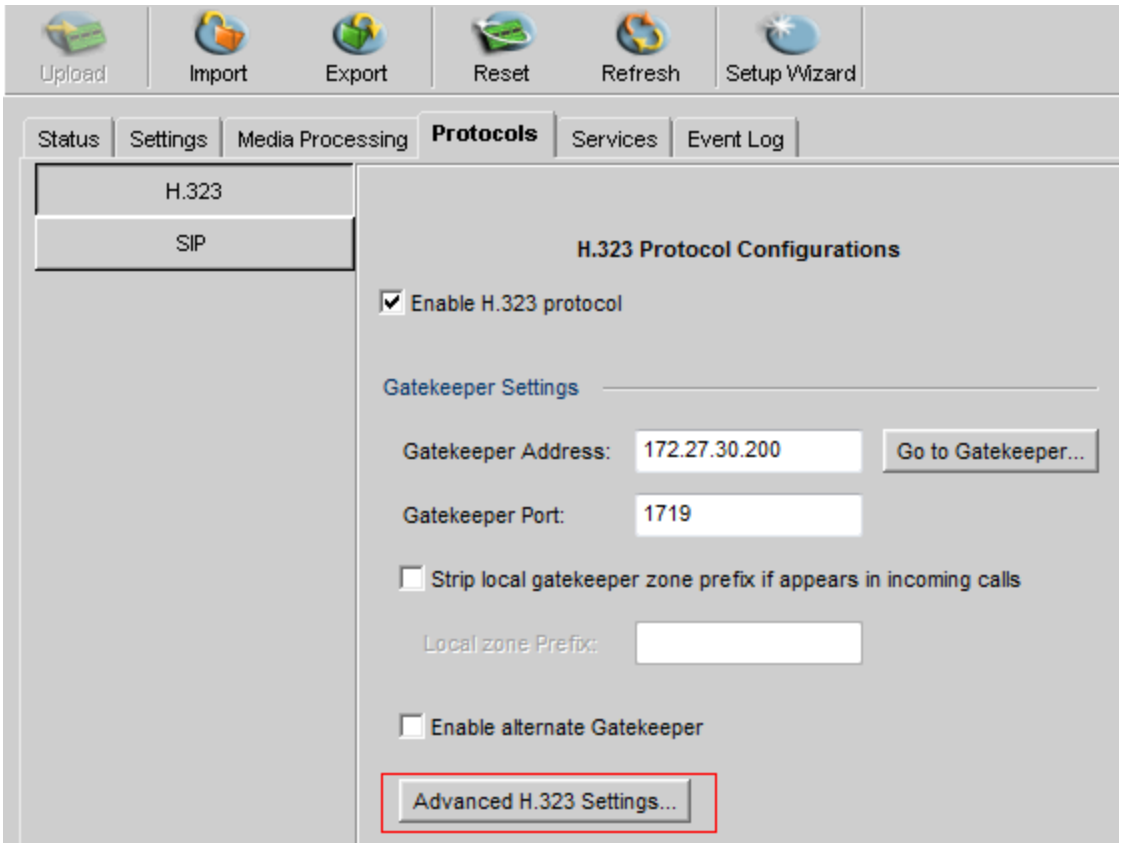

Figure 44: H.323 Settings

3. Select **Advanced H.323 Settings**. The Advanced H.323 Settings dialog box appears (see Figure 45: Advanced H.323 Settings on page 121).

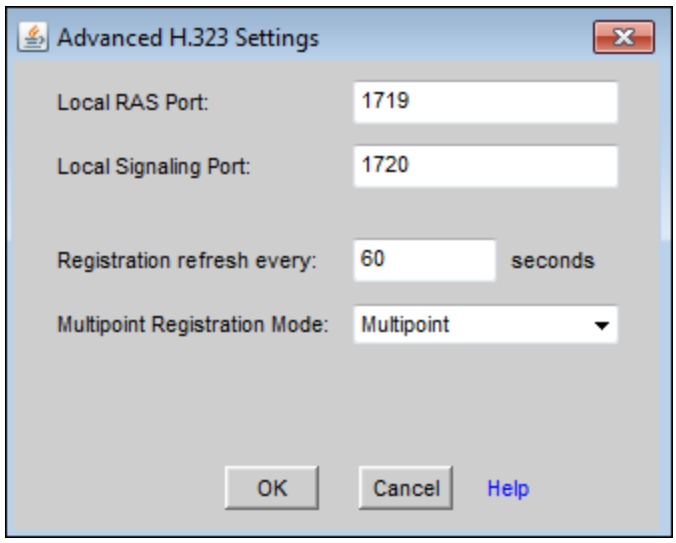

Figure 45: Advanced H.323 Settings

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

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

Related Links

Configuring Ports on the Scopia® MCU Blade on page 115

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 46: SIP Protocol Settings on page 123).

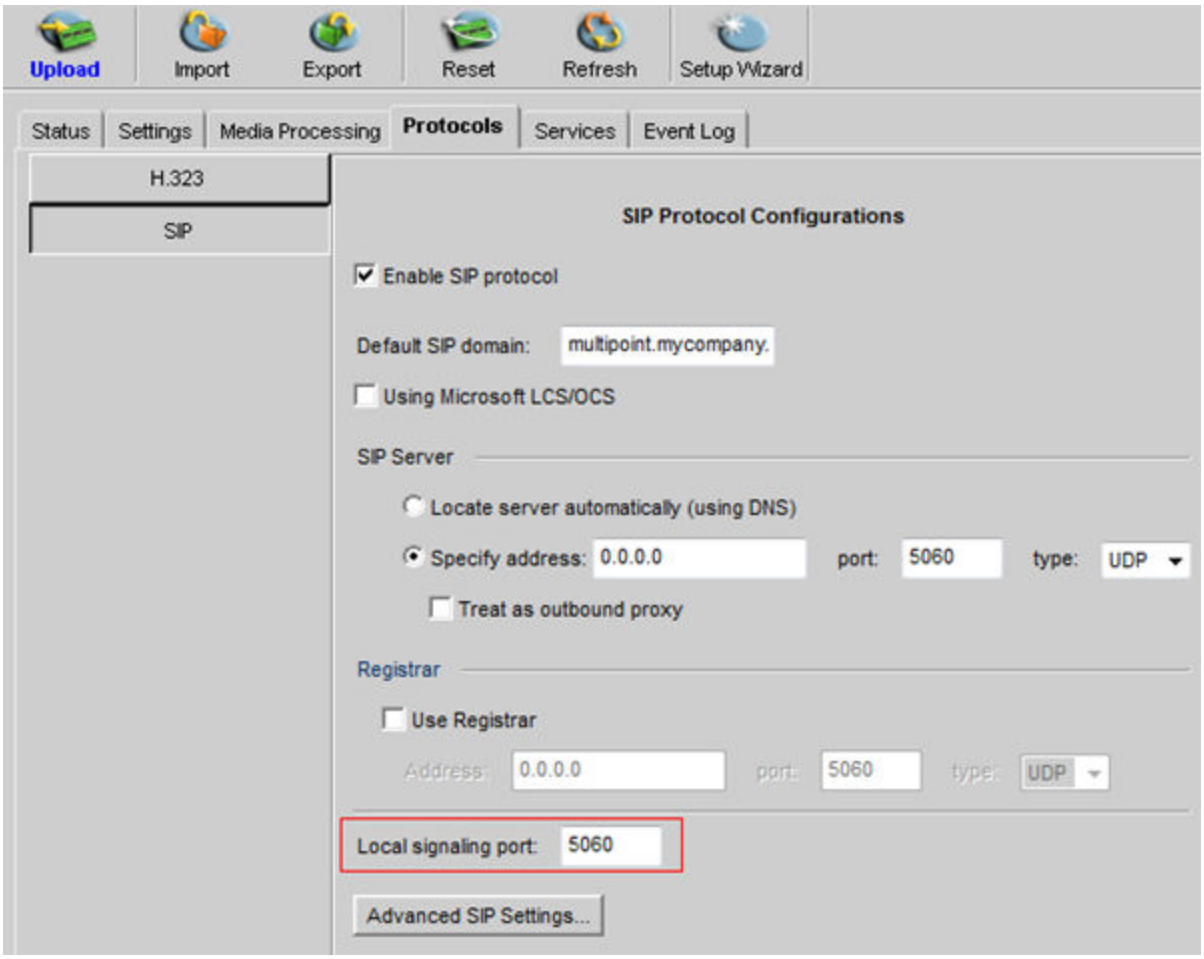

Figure 46: SIP Protocol Settings

5. Select **Upload**.

Related Links

Configuring Ports on the Scopia® MCU Blade on page 115

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 47: MCU Advanced Settings on page 124).

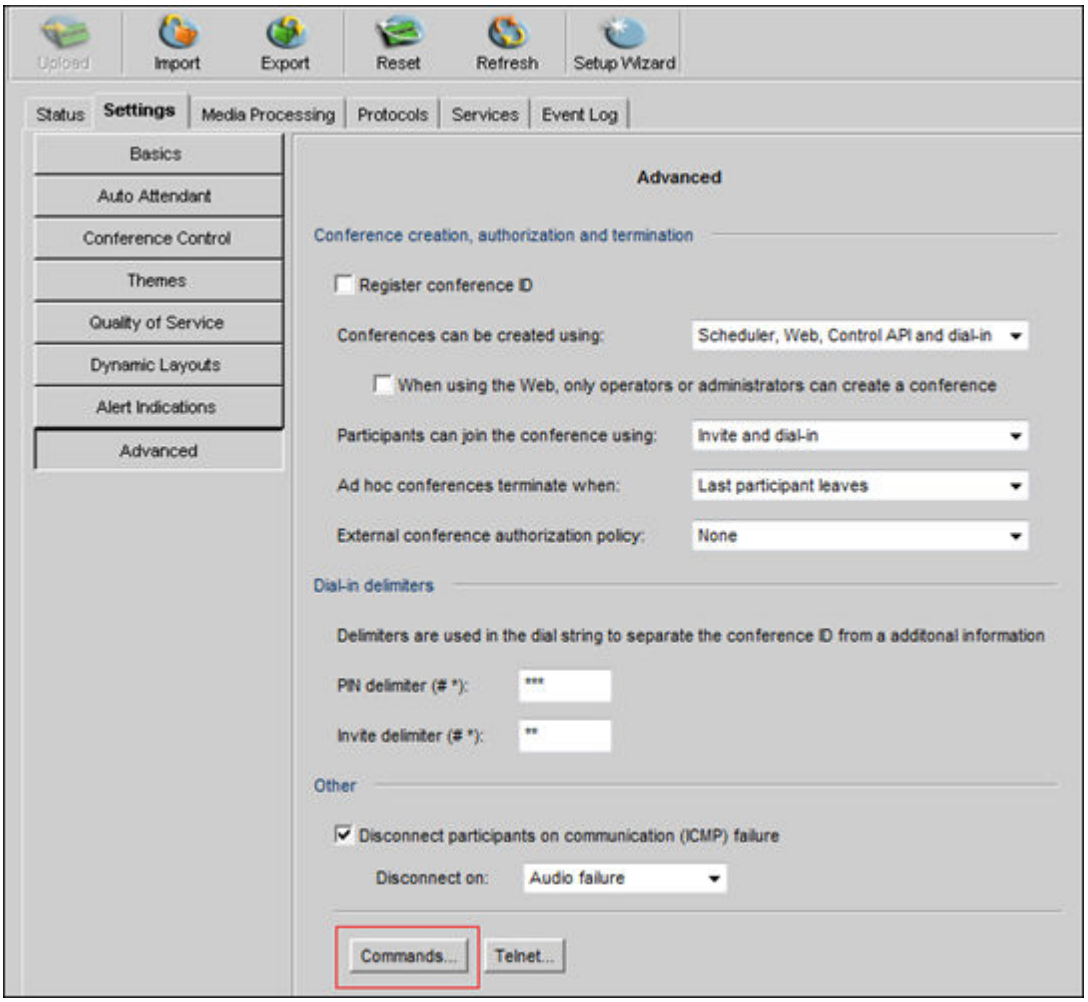

Figure 47: MCU Advanced Settings

3. Select **Commands**. The **Advanced Commands** section appears (see Figure 48: MCU Advanced Commands Section on page 125).

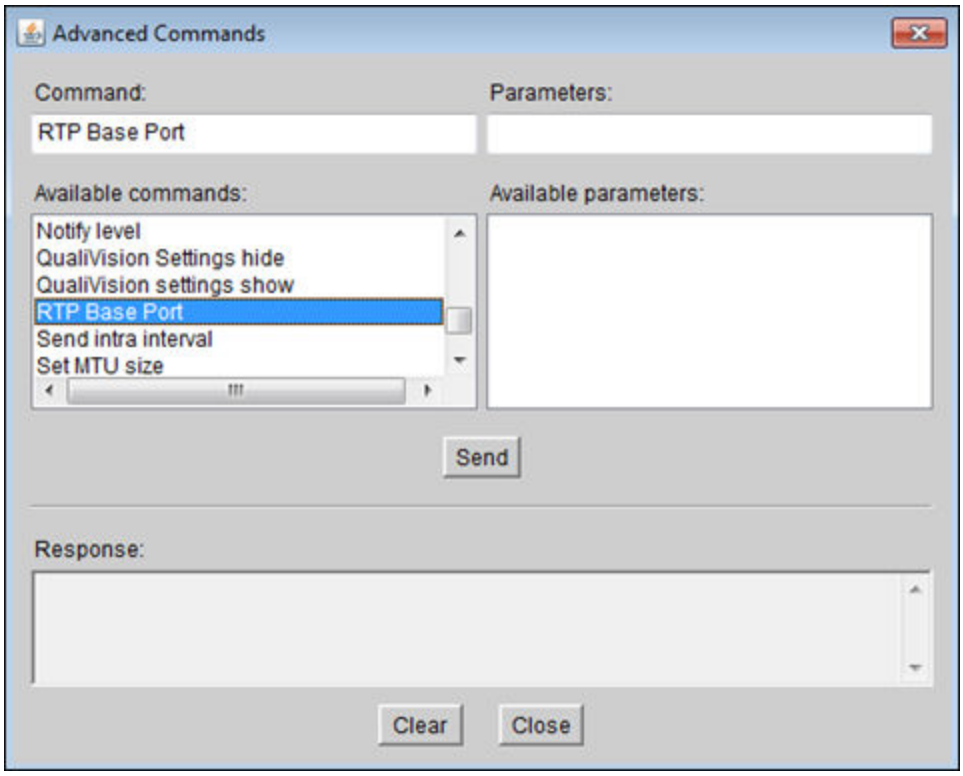

Figure 48: MCU Advanced Commands Section

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**.

Related Links

Configuring Ports on the Scopia® MCU Blade on page 115

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 49: MCU Security Settings on page 126). Table 49: Scopia® MCU Security Modes on page 126 lists the behavior of each service when each security mode is applied.

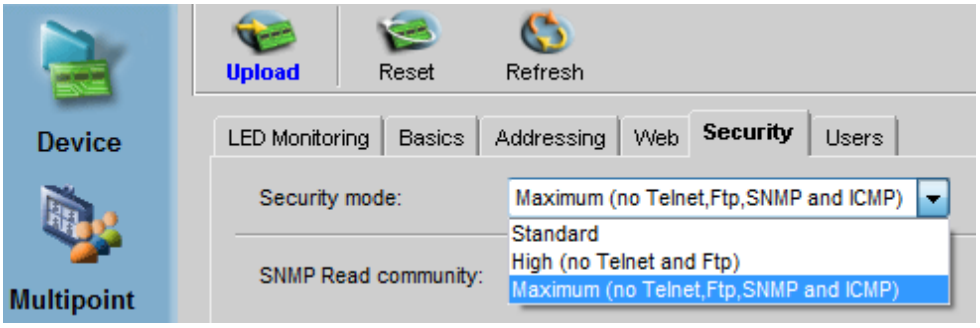

Figure 49: MCU Security Settings

Table 49: 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**.

Related Links

Implementing Port Security for the Scopia® MCU on page 112

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 50: Bidirectional Ports to Open on the MVP on page 127 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 50: 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 127

Related Links

Implementing Port Security for the Scopia® MCU on page 112

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.

Related Links

Implementing Port Security for the Scopia® MCU on page 112

Chapter 14: Implementing Port Security for the Avaya Scopia® Web Collaboration server

The Avaya Scopia® Web Collaboration server is the component which hosts the web collaboration aspect of videoconferences.

This section details the ports used for the Avaya Scopia® Web Collaboration server.

Related Links

Ports to open for the Avaya Scopia® Web Collaboration server on page 129

Ports to open for the Avaya Scopia® Web Collaboration server

The Avaya Scopia® Web Collaboration server (WCS) is typically located in the enterprise network and is connected to the DMZ.

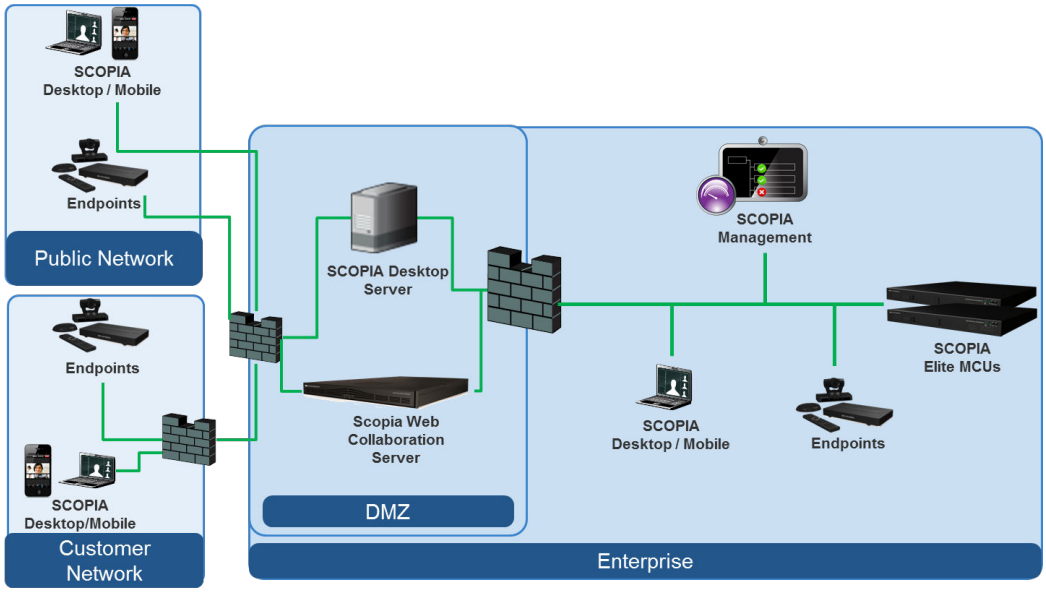

Figure 50: Locating the Avaya Scopia® Web Collaboration server in the DMZ

When opening ports on the Avaya Scopia® Web Collaboration server, use the following tables as a reference.

Important:

The specific firewalls you need to open ports on depends on where your Avaya Scopia® Web Collaboration server and other Scopia® Solution products are deployed.

Table 51: Bidirectional Ports to Open Between the Avaya Scopia® Web Collaboration server (WCS) and the Enterprise

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3336	TCP-TLS	Scopia® Management server	Facilitates WCS administration by Scopia® Management.	WCS connectivity issues	Mandatory
3338	TCP-TLS	Scopia® Management server	Facilitates WCS administration by Scopia® Management	WCS connectivity issues	Mandatory
3346	TCP-TLS	Scopia® Management server	Facilitates WCS administration by Scopia® Management	WCS connectivity issues	Mandatory
3348	TCP-TLS	Scopia® Management server	Facilitates WCS administration by Scopia® Management	WCS connectivity issues	Mandatory
5060	TCP/UDP	Scopia® Elite MCU and Scopia® Management server	SIP Protocol	WCS connectivity issues	Mandatory
5061	TCP-TLS	Scopia® Elite MCU and Scopia® Management server	SIP TLS Protocol	WCS connectivity issues	Mandatory
12000–12800	UDP	Scopia® Elite MCU	RTP presentation traffic	WCS connectivity issues	Mandatory
3400–3580	TCP/UDP	Scopia® Elite MCU	BFCP presentation traffic	WCS connectivity issues	Mandatory

Table 52: Inbound Ports to Open from the Enterprise to the Avaya Scopia® Web Collaboration server (WCS)

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
22	TCP	Avaya Scopia® Web Collaboration server	SSH	No debugging	Optional
80	TCP	From Avaya Scopia® Web Collaboration client to server	Controls web collaboration traffic	Issues relating to web collaboration functionality	Mandatory
443	TCP	From Avaya Scopia® Web Collaboration client to server	Controls web collaboration traffic	Issues relating to web collaboration functionality	Mandatory
843	TCP	From Avaya Scopia® Web Collaboration client to server	Controls the client's Flash policy server	Issues relating to web collaboration functionality	Mandatory
5556	TCP-TLS	From Scopia® Management to Avaya Scopia® Web Collaboration server	Facilitates WCS administration by Scopia® Management	WCS connectivity issues	Mandatory
8095	TCP-HTTP	From Scopia® Management to Avaya Scopia® Web Collaboration server	File transfer channel	WCS connectivity issues	Mandatory
8445	TCP-HTTPS	From Scopia® Management to Avaya Scopia® Web Collaboration server	File transfer channel	WCS connectivity issues	Mandatory

Table 53: Outbound Ports to Open from the Avaya Scopia® Web Collaboration server (WCS) to the Enterprise

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
53	UDP	DNS server	DNS	No FQDN resolution	Mandatory
8080	HTTP	Scopia® Management server	Controls web collaboration traffic	Issues relating to web collaboration functionality	Mandatory
9443	HTTPS	Scopia® Management server	Controls web collaboration traffic	Issues relating to web collaboration functionality	Mandatory

Table 54: Inbound Ports to Open from the Public to the Avaya Scopia® Web Collaboration server (WCS)

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
80	TCP	From Avaya Scopia® Web Collaboration client to server	Controls web collaboration traffic	Issues relating to web collaboration functionality	Mandatory
443	TCP	From Avaya Scopia® Web Collaboration client to server	Controls web collaboration traffic	Issues relating to web collaboration functionality	Mandatory
843	TCP	From Avaya Scopia® Web Collaboration client to server	Controls the client's Flash policy server	Issues relating to web collaboration functionality	Mandatory

Related Links

Implementing Port Security for the Avaya Scopia® Web Collaboration server on page 129

Chapter 15: Implementing Port Security for the Avaya Scopia® Streaming and Recording server

The Avaya Scopia® 8.3.2 solution introduces a new component, Avaya Scopia® Streaming and Recording server (Scopia® SR). Scopia® SR is the Avaya next generation HD streaming and recording platform, bringing significant enhancements to the Avaya Scopia® solution for streaming and recording. The Avaya Scopia® Streaming and Recording server replaces the Avaya Scopia® Content Center Recording server (SCC) server.

This section details the ports used for the Avaya Scopia® Streaming and Recording server.

Related Links

Ports to open for the Avaya Scopia Streaming and Recording server on page 133

Ports to open for the Avaya Scopia® Streaming and Recording server

If your network includes a firewall, and the Avaya Scopia® Streaming and Recording server and devices are on opposite sides of the firewall, you must open ports on the firewall to enable streaming between the Scopia® SR components. When opening ports on the Avaya Scopia® Streaming and Recording server, use the following tables as a reference.

Important:

The specific firewalls you need to open ports on depends on where your Avaya Scopia® Streaming and Recording server and other Scopia® Solution products are deployed.

The Avaya Scopia® Streaming and Recording server is a solution that consists of several components and these components can be deployed in a highly flexible way. You could place all of the components on a single server or you could place the components on a series of distributed servers. If you place all of the components on a single server, you do not have to open ports that facilitate communications between components of the Avaya Scopia® Streaming and Recording server. If you place some of the components outside of the firewall, you must open more ports. The

tables in this section list the ports for each of the individual components. You must know the location of each of the components before you configure the ports.

- Inbound port means that the device is listening on that port
- Outbound port means that the device is connecting to that port

Table 55: Ports to Open on the Scopia® SR Manager

Port Range	Protocol	Direction	Destination	Functionality	Required
80 443	TCP (HTML)	Inbound	From Scopia® SR client (the end-user's web browser) to Scopia® SR Manager. It is either 80 or 443, depending on how the system is configured.	Client systems access the Scopia® SR Manager HTML	Mandatory
443	TCP (HTTP)	Inbound	From Scopia® Management to Scopia® SR Manager	REST API for management communication	Mandatory
443	TCP (XML)	Inbound	From the Scopia® SR transcoder to Scopia® SR Manager	Communication	Mandatory
443	TCP	Bidirectional	Conference points (CP)	Scopia® SR Manager communicate with other Scopia® SR devices XML for communication, also pushes media files	Mandatory
443	TCP	Bidirectional	Delivery nodes (DN)	Scopia® SR Manager communicate with other Scopia® SR devices XML for communication, also pushes media files	Mandatory
443	TCP	Bidirectional	Virtual delivery node (VDN)	Scopia® SR Manager communicate with other Scopia® SR	Mandatory

Table continues…

Port Range	Protocol	Direction	Destination	Functionality	Required
				devices (typically on 443, not 80) XML for communication, also pushes media files	
25	TCP	Outbound	From Scopia® SR Manager to the SMTP server	SMTP mail server communication	Optional
8443	TCP (XML)	Outbound	From Scopia® SR Manager to the Scopia® SR transcoder.	Communication with the transcoder	Mandatory
8080	TCP (HTTP)	Outbound	From Scopia® SR Manager to Scopia® Management	REST API (the port is defined by iVIEW)	Mandatory

Table 56: Ports to Open on the Conference Points (CP)

Port Range	Protocol	Direction	Destination	Functionality	Required
443	TCP (XML)	Bidirectional	Scopia® SR Manager		Mandatory
80	TCP (Media)	Inbound	From the Scopia® SR transcoder to the CP	Transcoder pulls ASF streams from CP	Mandatory
80	TCP (Media)	Inbound	From the delivery node (DN) to the CP	RTP media (windows media streaming). CP gets raw RTP from Scopia® Elite MCU then sends it to the transcoder to encode to Windows Media. Then, it pulls back from the transcoder and makes it available to the DN	Mandatory
1025 — 65535 (default is 4100 — 4400)	UDP	Inbound	From Scopia® Elite MCU to the CP	RTP Audio/Video/ Presentation	Mandatory

Table continues…

Port Range	Protocol	Direction	Destination	Functionality	Required
				Note: This can be limited in the CP administration GUI.	
9090 -> 9XXX	TCP (Windows Media Stream)	Outbound	From the CP to the Scopia® SR transcoder	Transcoder communicates to the CP for transcoding and broadcasting from the transcoder. CP Pulls media from the transcoder	Mandatory
1719	UDP	Outbound	From the CP to the gatekeeper	RAS communication with the gatekeeper	Mandatory
1720	TCP	Outbound	From the CP to the gatekeeper	RAS communication with the gatekeeper, H. 323 call setup (H. 225/Q.931)	Mandatory
1025 — 65535	TCP	Outbound	From the CP to the gatekeeper	RAS communication with the gatekeeper, H. 323 call setup (H. 225/Q.931) – dynamic port range that can be limited on the gatekeeper	Mandatory
1025 —65535	UDP (RTP)	Outbound	From the CP to the Scopia® Elite MCU	RTP Audio/Video/ Presentation (this range can be limited on the MCU)	Mandatory
8443	TCP (XML)	Outbound	From the CP to the Scopia® SR transcoder	Communication between devices	Mandatory

Table 57: Ports to Open on the Transcoder

Port Range	Protocol	Direction	Destination	Functionality	Required
8443	TCP (XML)	Inbound	From the CP to the Scopia® SR transcoder	Communication between devices	Mandatory
8080 8443	TCP (HLS: 8080 or 8443)	Inbound	From the DN to the Scopia® SR transcoder	Communication between devices Access to HLS media	Mandatory
8443	TCP (XML)	Inbound	From the Scopia® SR Manager to the transcoder	Communication between devices	Mandatory
9090 — 9XXX	TCP (Windows Media Stream)	Inbound	From the CP to the Scopia® SR transcoder	Transcoder communicates to the CP for transcoding and broadcasting from the transcoder	Mandatory
9090 — 9XXX	UDP (AAC-LC)	Inbound	From the CP to the Scopia® SR transcoder	Transcoder communicates to the CP for transcoding and broadcasting from the transcoder	Mandatory
443	TCP (XML)	Outbound	From the Scopia® SR transcoder to the Scopia® SR Manager	Communication between devices	Mandatory
80	TCP (Media)	Outbound	From the Scopia® SR transcoder to the CP	Communication between devices	Mandatory
1755	TCP (Windows Media Stream)	Outbound	From the Scopia® SR transcoder to the CP	Transcoder communicates to the CP for transcoding and broadcasting from the transcoder	Mandatory

Table 58: Ports to Open on the Virtual Delivery Node (VDN)

Port Range	Protocol	Direction	Destination	Functionality	Required
80 443	TCP (HLS Media)	Inbound	From the CDN to the VDN.	DN streams media to client	Mandatory
80	TCP (HLS Media)	Inbound	From the Session Border	DN streams media to client	Mandatory

Table continues…

Port Range	Protocol	Direction	Destination	Functionality	Required
443			Controller (SBC) to the VDN		
21	TCP (FTP)	Outbound	From the VDN to the content delivery network (CDN)	File upload from the VDN to the CDN.	Mandatory
80 443	TCP (80, 443)	Outbound	From the VDN to the DN	DN communicate with other DN (HLS Media) – pull the stream from DN	Mandatory
443	TCP (XML)	Bidirectional	Scopia® SR Manager	Communications	Mandatory

Table 59: Ports to Open on the Delivery Node (DN)

Port Range	Protocol	Direction	Destination	Functionality	Required
80 443	TCP (HLS Media, Progressive Download)	Inbound	From the Scopia® SR clients to the DN	DN streams media to clients	Mandatory
80 554 1755	TCP (Windows Media)	Inbound	From the Scopia® SR clients to the DN	DN streams media to clients (windows media streaming)	Mandatory
80 443	TCP (Windows Media – 80, HLS – 80, 443)	Bidirectional	From DN to DN	DN communicates with other DN (HLS Media)	Mandatory
443	TCP (XML)	Bidirectional	Scopia® SR Manager		Mandatory
8080 8443	TCP	Outbound	From the DN to the transcoder		Mandatory
1024-5000 1755 80	UDP, TCP, HTTP (Windows Media)	Outbound	From the DN to the Scopia® SR clients	Client will try UDP between port 1024-5000 (Only open the necessary number of ports), then TCP on port 1755, then TCP on port 80	Mandatory

Table continues…

Port Range	Protocol	Direction	Destination	Functionality	Required
Multicast port range	UDP	Outbound	From the DN to the Scopia® SR clients	When using MMS and the network is multicast-capable, the standard port range for multicast will be used	Mandatory

Table 60: Additional Ports to Open

Port Range	Protocol	Direction	Destination	Functionality	Required
3389	UDP, TCP	Inbound	Remote Desktop	Microsoft Remote Desktop	Optional
53	UDP, TCP	Outbound	DNS server	DNS servers	Optional
123	UDP	Bidirectional	NTP source	NTP	Mandatory
514	TCP	Outbound	Syslog Server	Remote Syslog Server	Mandatory

Related Links

Implementing Port Security for the Avaya Scopia Streaming and Recording server on page 133
Limiting RTP/UDP Ports on the Conference Point on page 139

Limiting RTP/UDP Ports on the Conference Point

Procedure

1. Log in the conference point administration page.
   a. Type `https://<CP IP Address>` in a web browser.
   b. Log in using the following credentials:
      - Username: `administrator`
      - Password: `administrator`
2. Navigate to **System Configuration** > **Enable Services**.
3. In the RTP Ports panel, enter the base port value in the **From** field, and the upper port value in the **To** field.
4. Click **Save**.

Related Links

Ports to open for the Avaya Scopia Streaming and Recording server on page 133