

Scopia XT5000 Series

Installation Guide

Version 3.2

For Solution 7.7, 8.0.x, 8.2



© 2000-2013 RADVISION Ltd. All intellectual property rights in this publication are owned by RADVISION Ltd and are protected by United States copyright laws, other applicable copyright laws and international treaty provisions. RADVISION Ltd retains all rights not expressly granted.

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

This publication is RADVISION confidential. No part of this publication may be reproduced in any form whatsoever or used to make any derivative work without prior written approval by RADVISION Ltd.

No representation of warranties for fitness for any purpose other than what is specifically mentioned in this guide is made either by RADVISION Ltd or its agents.

RADVISION Ltd reserves the right to revise this publication and make changes without obligation to notify any person of such revisions or changes. RADVISION

Ltd may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this publication, it is furnished under a license agreement included with the product as a separate document. If you are unable to locate a copy, please contact RADVISION Ltd and a copy will be provided to you.

Unless otherwise indicated, RADVISION registered trademarks are registered in the United States and other territories. All registered trademarks recognized.

For further information contact RADVISION or your local distributor or reseller.

Installation Guide for Scopia XT5000 Series Version 3.2, May 30, 2013

<http://www.radvision.com>

Table of Contents

Chapter 1: About the Scopia XT Series

About the Models in the Scopia XT Series Product Line	8
Comparing Between Scopia XT Series Models	12
Technical Specifications	13

Chapter 2: Installation Workflow for Scopia XT Series

Chapter 3: Planning the Topology of the Scopia XT Series Deployment

Topology for Scopia XT Series as Endpoints	19
About the Scopia XT Series Embedded MCU	20
Planning the Topology for the Scopia XT Series with Scopia XT Desktop	21
Planning NAT and Firewall Traversal with Scopia XT Series	22
Supporting ISDN Connectivity	25
Implementing External API Control	27
Implementing Port Security for the Scopia XT Series	27
Ports to Open on the XT Series	27
Configuring the TCP or UDP Port Range on the Scopia XT Series	30

Chapter 4: Prerequisites for Setting up the System

Complying with Safety Regulations	32
Inspecting the Product	32
Planning the Optimal Conference Room Setup	32

Chapter 5: Setting up the Scopia XT Series

Mounting the XT Codec Unit	35
Connecting Scopia XT Series to Your Network	35
Connecting a Computer to the Scopia XT Series	36
Selecting the Computer Display Resolution	38
Connecting Audio Equipment to the Scopia XT Series	39

Deciding on the Audio Setup for the Scopia XT Series	39
About the Microphone Pod	40
Connecting the Three-Way Microphone Pod	42
Connecting the One-Way Microphone Pod and other Analog Microphones	43
Connecting an Analog Sound System	45
Connecting the Video Equipment to the Scopia XT Series	47
Connecting the Primary XT Premium Camera	47
Connecting the Optional USB Camera	49
Connecting the Optional XT Premium Camera	50
Connecting Cameras for Controlling the Optional XT Premium Camera with the XT Remote Control Unit	51
Connecting the Optional Scopia XT Camera Switch	53
Connecting a DVD or Blu-ray Player	58
Connecting Analog Video Equipment	58
Installing the Batteries of the XT Remote Control Unit	59

Chapter 6: Initial Configuration

How to Control the XT Series	61
Managing your XT Series from the Web Interface	61
Accessing XT Series Web Interface	62
Enabling Remote Management on the Scopia XT Series	63
Configuring Remote Upgrade Settings	65
Managing your XT Series Locally from the Endpoint	66
Accessing the Scopia XT Series Main Menu	67
Using the XT Remote Control Unit	68
Pairing an XT Remote Control Unit with a XT Codec Unit	71
Maintaining the Scopia XT Series Locally from the Endpoint	73
Registering and Enabling your Scopia XT Series license	75
Registering the Scopia XT Series to Obtain a License Key	75
Installing and Enabling Licenses which Extend System Functionality	76
Remotely Enabling the License from the Web Interface	78
Enabling the License from the Scopia XT Series Endpoint	80
Performing Basic Configuration	82
Accessing the Quick Setup Procedure	82
Setting the System Name and Language	84
Adjusting the Image Position	85
Configuring Network Settings	87
Configuring Gatekeeper Settings	89
Setting Basic System Information	90

Remotely Setting the System Name and Language	90
Modifying the System's Name on the Titlebar	91
Setting the Administrator PIN Code for the XT Series	94
Setting Date and Time	95
Setting the Time Zone	96
Remotely Setting Regional Information	97
Configuring the Screen Saver to Start Automatically	98
Configuring Video Connections	99
Configuring the Camera Connection	100
Setting up the Monitor Display Modes	105
Configuring Audio Connections	109
Configuring the Microphone	110
Configuring Analog Audio Connections	111
Configuring Audio Outputs	113
Configuring the Echo Canceller	116
Configuring Network Settings	117
Configuring GLAN Use	117
Configuring IP Addresses	118
Configuring Network Connectivity	120
Enabling NAT and Firewall Traversal with Scopia XT Series	122
Determining the Priority of Audio versus Video Quality	124
Registering the Scopia XT Series with a Gatekeeper	125
Registering the XT Series to a SIP Server	128
Configuring Call Settings	131
Configuring Scopia XT Series Endpoints to use an LDAP Directory	135

Chapter 7: Securing your Scopia XT Series

Securing Connections to the XT Series Using TLS	140
Generating a Certificate Signing Request for XT Series	141
Uploading XT Series Certificates	143
Backing Up and Restoring XT Series Certificates	145
Deleting XT Series Certificates	146
Enabling the TLS Connection in XT Series	147
Enabling Encryption for Videoconferences	149

Chapter 8: Troubleshooting the Scopia XT Series

Viewing System Information for Customer Support	152
---	-----

Resolving Problems with Audio 154

Echo Cancelling on HDMI Monitors 156

Resolving Monitor Display Problems 158

Resolving Camera Issues 160

Resolving IP Address Problems 162

Resolving XT Remote Control Unit Problems 164

Restoring Default User Settings 165

Glossary of Terms for Scopia Solution

Chapter 1 | About the Scopia XT Series

Scopia XT Series endpoints incorporate state-of-the-art video technology for high definition (HD) conferencing. All models of the XT Series include the XT Codec Unit which performs the bulk of the professional videoconferencing, an elegant remote control which gives intuitive access to its features, and a camera, which varies depending on the specific model.

This section provides an overview of the general features and capabilities available in the different Scopia XT Series models ([Figure 1: Scopia XT Series products](#) on page 8):

- Ability to host videoconferences locally with a high-capacity embedded MCU, without requiring an external MCU deployment (selected models only).
- Excellent video quality, with resolutions of up to 1080p at an unprecedented 60 frames per second (fps), depending on the model.
- Support for dual HD video streams, allowing presentations and video clips to be shared in resolutions of up to 1080p 60 fps, depending on the model.

This includes either video input from two cameras, or one video stream from the camera, and one presentation stream from the PC.

- Allows to easily share data and presentations with third-party endpoints.
- DVD-quality audio with up to 48 kHz sampling rate audio encoding capability, depending on the model. The sampling rate is a measure of the accuracy of the audio when it is digitized. As the frequency with which the audio data is collected, or "sampled", increases, so does the audio quality.

Audio input is provided with either a dedicated 3-way/1-way Microphone Pod, or a microphone embedded in the camera, depending on the model.

- High quality video and audio even with limited bandwidth or poor network conditions, by using two compression methods:
 - H.264 Scalable Video Coding Technology (SVC, in selected models only).
SVC dramatically increases error resiliency and video quality without the need for higher bandwidth. It is especially effective over networks with high packet loss (like wireless networks) which deliver low quality video.
 - H.246 High Profile, which is a video compression standard used for bandwidth efficiency. This allows quality video at much lower bit rates (selected models only).
- Ability to record videoconferences using a USB drive (may require license, depending on the model).
- For an even better experience, Scopia Control enables you to select and control the camera for the videoconference, by using the pan, tilt, and zoom features, and place a call using the intuitive touch interface of an Apple® iPad® (may require license, depending on the model).
- Secure point-to-point video calls and videoconferences, via encrypted connections or using TLS certificates. You can have up to three remote encrypted participants in a videoconference.

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.

[Figure 1: Scopia XT Series products](#) on page 8 shows the different Scopia XT Series endpoints available.



SCOPIA XT5000



SCOPIA XT Telepresence



SCOPIA XT Executive



SCOPIA XT1200



SCOPIA XT Meeting Center



SCOPIA XT4200

Figure 1: Scopia XT Series products

For more information about the specific models in the Scopia XT Series product line:

Navigation

- [About the Models in the Scopia XT Series Product Line](#) on page 8
- [Comparing Between Scopia XT Series Models](#) on page 12
- [Technical Specifications](#) on page 13

About the Models in the Scopia XT Series Product Line

Scopia XT Series endpoints incorporate state-of-the-art video technology for high definition (HD) conferencing. All models of the XT Series include the XT Codec Unit which performs the bulk of the professional videoconferencing, an elegant remote control which gives intuitive access to its features, and a camera, which varies depending on the specific model.

This section provides an overview of each model in the Scopia XT Series product line. For more information about the features and capabilities available for Scopia XT Series endpoints, see [About the Scopia XT Series](#) on page 7. To easily compare the different Scopia XT Series endpoints, see [Comparing Between Scopia XT Series Models](#) on page 12.

The Scopia XT Series includes the following models:

- Scopia XT5000 Series

With HD video resolution of up to 1080p video at 60 frames per second (fps), Scopia XT5000 sets the standard for an exceptional videoconferencing experience, and is designed for easy setup and control.

The 3-way Microphone Pod provides superb signal-to-noise ratios, which isolates speakers' voices over background noise and gives a crisp high quality sound. You can also add a second microphone for unparalleled large room coverage.

The XT5000 720 provides HD video resolution of 720p at 60 fps and 5x optical zoom, with the option to upgrade to 1080p at 60fps and 10x optical zoom.



Figure 2: Scopia XT5000 Series

- Scopia XT4000 Series

Experience cost-effective HD videoconferencing with the Scopia XT4000 Series, which was designed specifically for small meeting rooms. The included camera has 5x with an option to upgrade to 10x.



Figure 3: Scopia XT4200

- Scopia XT1200

The Scopia XT1200 room-system uses the previous generation XT Codec Unit to provide excellent video and audio quality:

- Includes a high-quality camera (10x optical zoom, and an additional 4x digital zoom)
- The 3-way Microphone Pod provides superb signal-to-noise ratios. You can also add a second microphone for unparalleled large room coverage.



Figure 4: Scopia XT1200

- Scopia XT Telepresence

Experience the immersive feeling of telepresence using the Scopia XT Telepresence platform. The excellent video quality in each of the three cameras, combined with high-quality audio, give the feeling of an in-person meeting.

Depending on the XT Codec Unit used in your XT Telepresence deployment, you can inherit the features of the Scopia XT1200 or the Scopia XT5000.



Figure 5: Scopia XT Telepresence

- Scopia XT Executive

Designed as a professional personal endpoint, the Scopia XT Executive is an all-in-one HD videoconferencing desktop endpoint and PC monitor. The Scopia XT Executive fully integrates with your PC or Mac. Using a unique control application, you can place calls, join videoconferences, and navigate the system menus with your computer's keyboard and mouse. The XT Remote Control Unit can be used as well.

The Scopia XT Executive has a built-in, high-quality HD camera with a maximum resolution of 1080p at 30 frames per second (fps) together with the display. To fit your videoconferencing needs, you can also connect an optional XT Premium Camera with PTZ capability.



Figure 6: Scopia XT Executive

- Scopia XT Meeting Center

The Scopia XT Meeting Center is a high performance HD videoconferencing system, designed to quickly convert a regular meeting room into a videoconferencing room: it includes single or dual 55-inch high-quality monitors mounted on a mobile stand. This system uses the powerful XT5000 Series codec.



Figure 7: Scopia XT Meeting Center

The XT5000, Scopia XT1200, and Scopia XT Executive can also locally host HD continuous presence videoconferences with their built-in MCU. You can choose a license of up to 4 or 9 participants.

Depending on your deployment and the model, you can locally host videoconferences with other endpoints (including H.323, SIP, Scopia XT Desktop clients, Scopia Mobile, and ISDN endpoints, if your

deployment includes an ISDN gateway such as Scopia 100 Gateway) without relying on an external MCU. You can locally host videoconferences with the following editions:

- Scopia XT Series MCU Edition

The Scopia XT Series MCU Edition allows you to host videoconferences with standard H.323, SIP, and ISDN (via Scopia 100 Gateway) endpoints on your chosen XT Series model.

- Scopia XT Series SMB Edition

The Scopia XT Series SMB Edition allows you to host videoconferences with a variety of different endpoints on your chosen XT Series model: Scopia XT Desktop clients, Scopia Mobile clients, H.323, SIP, and ISDN (via Scopia 100 Gateway) endpoints.

It includes the software of the Scopia XT Desktop Server which must be deployed in the DMZ.

! Important:

If your license allows 9 participants, you can include up to 8 remote endpoints.

If any participants in the videoconference connect from Scopia XT Desktop clients or devices running Scopia Mobile, you can include up to 7 remote endpoints, since one port is reserved for connecting to the Scopia XT Desktop Server.

For more information on the SMB Solution deployment, see *Solution Guide for Scopia Solution*.

Comparing Between Scopia XT Series Models

Scopia XT Series endpoints incorporate state-of-the-art video technology for high definition (HD) conferencing. All models of the XT Series include the XT Codec Unit which performs the bulk of the professional videoconferencing, an elegant remote control which gives intuitive access to its features, and a camera, which varies depending on the specific model.

This section provides a comparison between the models of the Scopia XT Series product line. For an overview of each model, see [About the Models in the Scopia XT Series Product Line](#) on page 8. To see details about the features and capabilities of Scopia XT Series endpoints, see [About the Scopia XT Series](#) on page 7.

[Table 1: Differences in features for models in the Scopia XT Series](#) on page 12 summarizes the differences between each of the models in the Scopia XT Series.

Table 1: Differences in features for models in the Scopia XT Series

Feature	Scopia XT5000 	Scopia XT5000 720 	Scopia XT4000 Series 	Scopia XT1200 	Scopia XT Telepresence 	Scopia XT Executive 
Maximum HD Resolution	1080p 60fps	720p 60 fps (1080p optional)	720p 60fps	1080p 30fps	1080p x3 at 60 or 30 fps	720p 30fps/60 fps (1080p optional)
Hosting with internal MCU	Can host video-conferences (optional)	Can host video-conferences (optional)	—	Can host video-conferences (optional)	—	Can host video-conferences (optional)

Feature	Scopia XT5000 	Scopia XT5000 720 	Scopia XT4000 Series 	Scopia XT1200 	Scopia XT Telepresence 	Scopia XT Executive 
Camera	PTZ camera	PTZ camera	PTZ camera	PTZ camera	—	Built-in camera (PTZ camera optional)
Optical Zoom	10x optical zoom	5x optical zoom (10x optional)	5x optical zoom (10x optional)	10x optical zoom	10x optical zoom	10x optical zoom for optional camera
Total Zoom (Optical x Digital)	40x total zoom	40x total zoom (optional)	40x total zoom (optional)	10x total zoom (40x optional)	—	40x total zoom for optional camera
Dual Video Resolution	Dual video at 1080p 60 fps	Dual video at 720p 60 fps (1080p optional)	Dual video at 720p 60fps	Dual video at 1080p 30fps	Dual video at 1080p 60/30 fps	Dual video at 1080p 60 fps
High network error resilience	SVC & H.264 High Profile	SVC & H.264 High Profile	SVC & H.264 High Profile	—	SVC & H.264 High Profile (optional)	SVC & H.264 High Profile
High-quality audio	48 kHz sampling rate	48 kHz sampling rate	48 kHz sampling rate	48 kHz sampling rate	48 kHz sampling rate	48 kHz sampling rate
Type of Microphone	3-way Microphone Pod	3-way Microphone Pod	1-way Microphone Pod	3-way Microphone Pod	3-way Microphone Pod	Built-in microphone (Microphone Pod optional)
Additional Ethernet connection speed	10/100/1000 Mbps	10/100/1000 Mbps (optional)	10/100/1000 Mbps (optional)	10/100 Mbps (optional)	10/100 or 10/100/1000 Mbps	10/100/1000 Mbps
Scopia Control	Scopia Control	Scopia Control (optional)	Scopia Control (optional)	Scopia Control (optional)	Scopia Control	Scopia Control (optional)
Recording	Can record on USB disk	Can record on USB disk (optional)	Can record on USB disk (optional)	—	—	Can record on USB disk (optional)

Technical Specifications

This section details the system specifications of the Scopia XT Series you purchased. Refer to this data when preparing system setup and afterwards as a means of verifying that the environment still complies with these requirements:

- For physical details of the system, such as the power requirements and weight of each component, see [Table 2: Physical device specifications](#) on page 14.
- For specific video, audio, and control features of the system, such as supported codecs and web browsers, see [Table 3: Video, audio and control capabilities](#) on page 14.
- For network information of the system, such as network interface cards, see [Table 4: Network and security capabilities](#) on page 16.

[Table 2: Physical device specifications](#) on page 14 refers to the physical details of the device.

Table 2: Physical device specifications

	Scopia XT5000 Series	Scopia XT4000 Series	Scopia XT Executive
System power requirements	100-240 VAC, 50/60 Hz, 1.8 A Max.		100-240 VAC, 50/60 Hz, 1 A Max.
Maximum power consumption	60W (205 BTU/h)		
Operating temperature	0°C to 40°C (32°F to 104°F)		
Relative humidity	5% to 90% non-condensing		
Storage temperature	-40°C to 70°C (-40°F to 158°F), ambient		
Physical dimensions and Net Weight	Height: 4cm (1.6"), Width: 29cm (11.4"); Depth 16.5cm (6.5") Weight: 2.4 kg (5.3 lb)		Height: 49.5cm (19.5"), Width: 54.5cm (21.5"); Depth 25cm (9.9") Weight: 10 kg (22.1 lb)
Camera Physical dimensions and Net weight	Height: 15,2cm (6.0"), Width: 25cm (9.8"); Depth 13.5cm (5.3") Weight: 1.6 kg (3.5 lb)		Includes a built-in camera (can connect optional HDMI camera)
Microphone Pod Physical dimensions and Net weight	Diameter: 14cm (5.5"), Weight: 0.3 kg (0.7 lb)	Diameter: 12cm (4.7"), Weight: 0.4 kg (0.9 lb)	Includes a built-in microphone (can connect optional Microphone Pod)
Microphone Pod capabilities	3-way Microphone Pod: 360° range Up to 2 cascaded pods	1-way Microphone Pod: 180° range Optional 3-way Microphone Pod	Optional 3-way Microphone Pod: 360° range
	Frequency response: 50 – 22,000 Hz		

[Table 3: Video, audio and control capabilities](#) on page 14 lists the protocols and software requirements.

Table 3: Video, audio and control capabilities

	Scopia XT5000 Series	Scopia XT4000 Series	Scopia XT Executive
Signaling protocols	H.323, SIP, ISDN (in conjunction with Scopia Gateway)		
Video codecs	H.263, H.263+, H.263++, H.264, H.264 SVC, H.264 High Profile, H.264 High Profile SVC		
Dual video	H.239 (H.323); BFCP (SIP)		

	Scopia XT5000 Series	Scopia XT4000 Series	Scopia XT Executive
HDMI input formats	1920 x 1080 @ 25, 30, 50, 60fps (optional for XT5000 720) 1280 x 720 @ 25, 30, 50, 60fps 720 x 576 @ 50fps 720 x 480 @ 60fps 640 x 480 @ 60fps		
Live video resolution	1920 X 1080 @ 25, 30, 50, 60fps: HD1080p25, 30, 50, 60 (optional for XT5000 720)	-	1920 X 1080 @ 25, 30, 50, 60fps: HD1080p25, 30, 50, 60 (optional)
	1280 x 720 @ 25, 30, 50, 60fps: HD720p25, 30, 50, 60 1024 x 576 @ 25, 30fps: w576p 768 x 448 @ 25, 30fps: w448p 704 x 576 @ 25, 30fps: 4CIF 704 x 480 @ 25, 30fps: 4SIF 576 x 336 @ 25, 30fps 512 x 288 @ 25, 30fps: wCIF 400 x 224 @ 25, 30fps 352 x 288 @ 25, 30fps: CIF 352 x 240 @ 25, 30fps: SIF		
Presentation video resolution	1920 x 1080 @ 25, 30, 50, 60fps (optional for XT5000 720) 1440 x 900 @ 60fps: WSXGA 1280 x 1024 @ 60fps: SXGA	-	1920 x 1080 @ 25, 30, 50, 60fps 1440 x 900 @ 60fps: WSXGA 1280 x 1024 @ 60fps: SXGA
	1280 x 720 @ 25, 30, 50, 60fps 1280 x 768 @ 60fps: WXGA 1024 x 768 @ 60fps: XGA 800 x 600 @ 60fps: SVGA 640 x 480 @ 60fps: VGA		
HDMI output formats	1920 x 1080 @ 25, 30, 50, 60fps (optional for XT5000 720) 1280 x 720 @ 50, 60fps	1280 x 720 @ 50, 60fps	1920 x 1080 @ 25, 30, 50, 60fps 1280 x 720 @ 50, 60fps
Video bandwidth	Up to 12Mbps for a multipoint call (optional) Up to 6Mbps for 1080p in a point-to-point call (720p for XT5000 720)	Up to 4Mbps for 720p	Up to 12Mbps for a multipoint call (optional) Up to 6Mbps for a point-to-point call

	Scopia XT5000 Series	Scopia XT4000 Series	Scopia XT Executive
Camera resolution	1080p 60fps	720p 60fps	720p 30fps (1080p optional)
Audio codecs	G.711, G.722, G.722.1, G.722.1 Annex C, G.719, AAC-LD (G.728, G.729A optional)		
Web browser support	• Internet Explorer version 8 or later • Google Chrome version 11 or later • Mozilla Firefox version 3.6 or later • Apple Safari version 5 or later • Opera version 11 or later		

[Table 4: Network and security capabilities](#) on page 16 lists the XT Series's network interface and firewall traversal information.

Table 4: Network and security capabilities

	Scopia XT5000 Series	Scopia XT4000 Series	Scopia XT Executive
Network Interfaces	2 x 10/100/1000 Base-T full-duplex (RJ-45)		
	2nd GLAN enabled by default (optional for XT5000 720)	2nd GLAN is optional	2nd GLAN enabled by default
Firewall Traversal	Auto NAT discovery HTTP and STUN H.460.18, H.460.19		

Chapter 2 | Installation Workflow for Scopia XT Series

About this task

To safely set up and perform the required initial settings to start using the Scopia XT Series, follow the recommended workflow described below.

Procedure

1. Decide how to incorporate the XT Series into your deployment, as described in [Planning the Topology of the Scopia XT Series Deployment](#) on page 19.

For example, decide whether to enable license options such as a built-in MCU, where to deploy the XT Series, and the ports to open.

2. Read through and familiarize yourself with the safety information (see [Complying with Safety Regulations](#) on page 32).
3. Inspect the XT Series to verify that no shipping damage occurred, as described in [Inspecting the Product](#) on page 32.
4. Decide where to place your XT Series, depending on the room setup (see [Planning the Optimal Conference Room Setup](#) on page 32).

5. To quickly connect your XT Series, refer to the *Quick Setup Guide for Scopia XT Series*. For more detailed information on connecting the XT Series, see [Setting up the Scopia XT Series](#) on page 35, which includes:

- Mounting the XT Series
- Connecting the XT Series to the network
- Connecting a computer
- Connecting the audio equipment, such as the Microphone Pod
- Connecting the video equipment, such as the camera
- Placing batteries in the XT Remote Control Unit

6. Read through and familiarize yourself with how to control the XT Series and access both the endpoint and web interface, as described in [How to Control the XT Series](#) on page 61.
7. Register your license to activate the XT Series, as described in [Registering and Enabling your Scopia XT Series license](#) on page 75.

If you do not yet have your license key, you can set up the system in demo mode for a period of 24 hours. After this time, you must enable your license key to use the system.

8. Perform the basic required configuration necessary to use the XT Series, such as the network and gatekeeper settings, as described in [Performing Basic Configuration](#) on page 82.

9. Perform additional basic configuration, such as setting the time zone and date, as described in [Setting Basic System Information](#) on page 90.
10. You can modify the default administrator PIN code as described in [Setting the Administrator PIN Code for the XT Series](#) on page 94 (recommended).
11. Configure your camera and microphone settings, as described in:
 - [Configuring Video Connections](#) on page 99
 - [Configuring Audio Connections](#) on page 109
12. If necessary for your deployment, configure your advanced network and call settings, as described in [Configuring Network Settings](#) on page 117.

For more information about deployment setups, see [Planning the Topology of the Scopia XT Series Deployment](#) on page 19 and the *Scopia Solution Guide*.
13. (Optional) If necessary for your organization, you can secure videoconference sessions via encrypted connections and TLS certificates (see [Securing your Scopia XT Series](#) on page 140).

 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.

Chapter 3 | Planning the Topology of the Scopia XT Series Deployment

There are a number of ways that the Scopia XT Series can be deployed in a network, depending on whether you use it as a room system endpoint or a conference hosting system, and the type of the endpoints connecting to the unit.

Navigation

- [Topology for Scopia XT Series as Endpoints](#) on page 19
- [About the Scopia XT Series Embedded MCU](#) on page 20
- [Planning the Topology for the Scopia XT Series with Scopia XT Desktop](#) on page 21
- [Planning NAT and Firewall Traversal with Scopia XT Series](#) on page 22
- [Supporting ISDN Connectivity](#) on page 25
- [Implementing External API Control](#) on page 27
- [Implementing Port Security for the Scopia XT Series](#) on page 27

Topology for Scopia XT Series as Endpoints

A Scopia XT Series without a built-in MCU is an endpoint and requires an external MCU such as the Scopia Elite MCU to host videoconferences ([Figure 8: Scopia XT Series as Endpoints](#) on page 20):

- The MCU performs media processing for endpoints in all locations, including Scopia XT Series, Scopia XT Executive and compatible third-party endpoints.
- The MCU can handle multiple videoconferences simultaneously.
- Videoconferences are in high-quality, with maximum resolutions of 1080p and 720p, and include network error resilience using H.264 Scalable Video Coding (SVC) and high profile H.264 (for details about these features, see [About the Scopia XT Series](#) on page 7).

Scopia XT Executive integrates advanced videoconferencing into a high resolution 24-inch multimedia LED monitor.

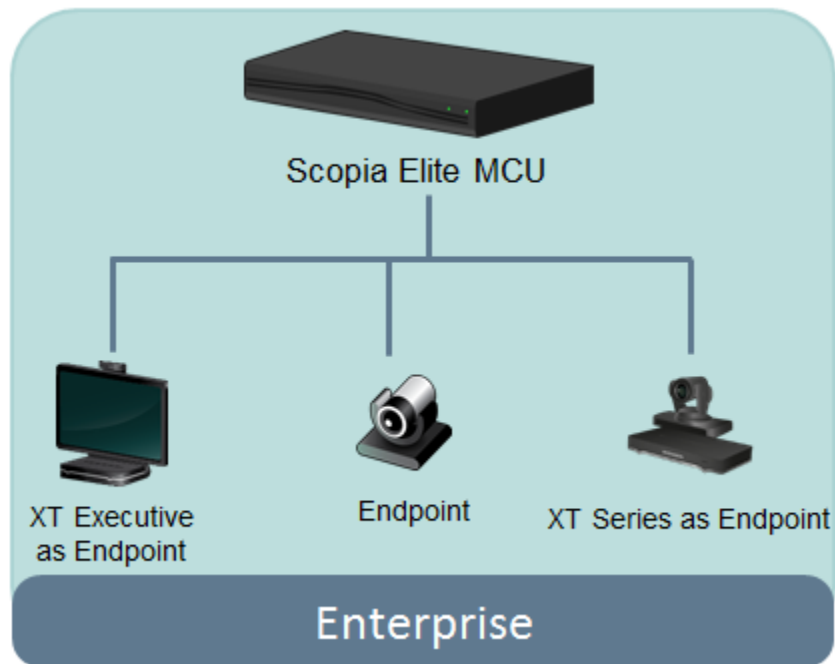


Figure 8: Scopia XT Series as Endpoints

About the Scopia XT Series Embedded MCU

The Scopia XT Series MCU Edition includes an embedded MCU, allowing Scopia XT Series to host videoconferences locally.

The built-in MCU is available as a license option for the Scopia XT5000, Scopia XT1200, and Scopia XT Executive models only. Activate the MCU capability by registering the XT Codec Unit, as described in [Registering the Scopia XT Series to Obtain a License Key](#) on page 75.

The following Scopia XT Series MCU Edition options are available, depending on the XT Series model:

- MCU4 - Host videoconferences with up to 4 participants (1 Local and 3 Remote).
- MCU9 - Host videoconferences with up to 9 Participants (1 Local and 8 Remote).

The embedded MCU can host both standard definition (SD) and high definition (HD) endpoints simultaneously (see [Table 5: Video capabilities for participants hosted by Scopia XT Series MCU Edition](#) on page 21 for details):

- The MCU processes video streams from all endpoints to ensure the video displays correctly for all possible layouts, regardless of the endpoint resolution or picture format.
- The presence of SD endpoints does not affect the quality received by HD endpoints. SD endpoints receive SD video streams and HD endpoints receive HD video streams.
- Both wide-screen (16:9) and standard formats (4:3) are incorporated into the continuous presence (CP) video layout.

Table 5: Video capabilities for participants hosted by Scopia XT Series MCU Edition

Maximum Resolution	XT5000	Scopia XT1200	Scopia XT Executive
Displayed and transmitted resolution (max)	1080p	720p	720p (1080p optional)
Resolution of single participant's video in layout (max)	448p		

! Important:

For MCU9, the capabilities depend on the selected CP layout.

For the best experience when using the Scopia XT Series MCU Edition, we recommend:

- Enabling the High Bandwidth Option (12Mbps), available as a separate license (for details, see [Installing and Enabling Licenses which Extend System Functionality](#) on page 76). Otherwise, the MCU sends out a lower resolution at the standard 6Mbps total bandwidth.
- If the Scopia XT Series is used only as an MCU for hosting videoconferences, block the audio and video input from this Scopia XT Series during the meeting. For details, see [Configuring Call Settings](#) on page 131.

As you add more XT Series endpoints, you can manage them centrally with Scopia Management. This would enable centralized updating, backing up and control.

Planning the Topology for the Scopia XT Series with Scopia XT Desktop

Scopia XT Series SMB Edition enables you to locally host videoconferences using its built-in MCU, and extends your videoconferences to participants joining from a computer (with Scopia Desktop Client) or a mobile device (using Scopia Mobile).

For example, when you start a videoconference with the XT Series hosting the call, you can add other participants by asking them to connect via a web link to the Scopia XT Desktop Server, which would automatically install and launch Scopia Desktop Client on their computers, or Scopia Mobile on their mobile devices.

The main features of the Scopia XT Series SMB Edition include:

- Remote users can easily connect to a meeting hosted by the built-in MCU on the XT Series, by connecting via the Scopia XT Desktop Server.
The deployment has very few components. You do not need additional hardware like an external MCU, Scopia PathFinder for firewall traversal, or Scopia ECS Gatekeeper for routing calls.
- The included Scopia XT Desktop provides built-in NAT and firewall traversal functionality, enabling secure remote connections from Scopia Mobile and Scopia Desktop Clients.

You can enable this functionality via the XT Series license.

The Scopia XT Series SMB Edition includes the following options:

- Full SMB4 - Basic MCU level with up to four participants: 1 local and 3 remote mixed endpoints and PC clients.
- Full SMB9 - Advanced MCU level, with up to 9 participants:
 - One local and eight remote endpoints
 - Or
 - One local and seven mixed endpoints and PC clients

[Figure 9: Scopia XT Series SMB Edition Deployment](#) on page 22 shows a typical topology for the Scopia XT Series SMB Edition solution. For more information, see the *Solution Guide for Scopia Solution*.

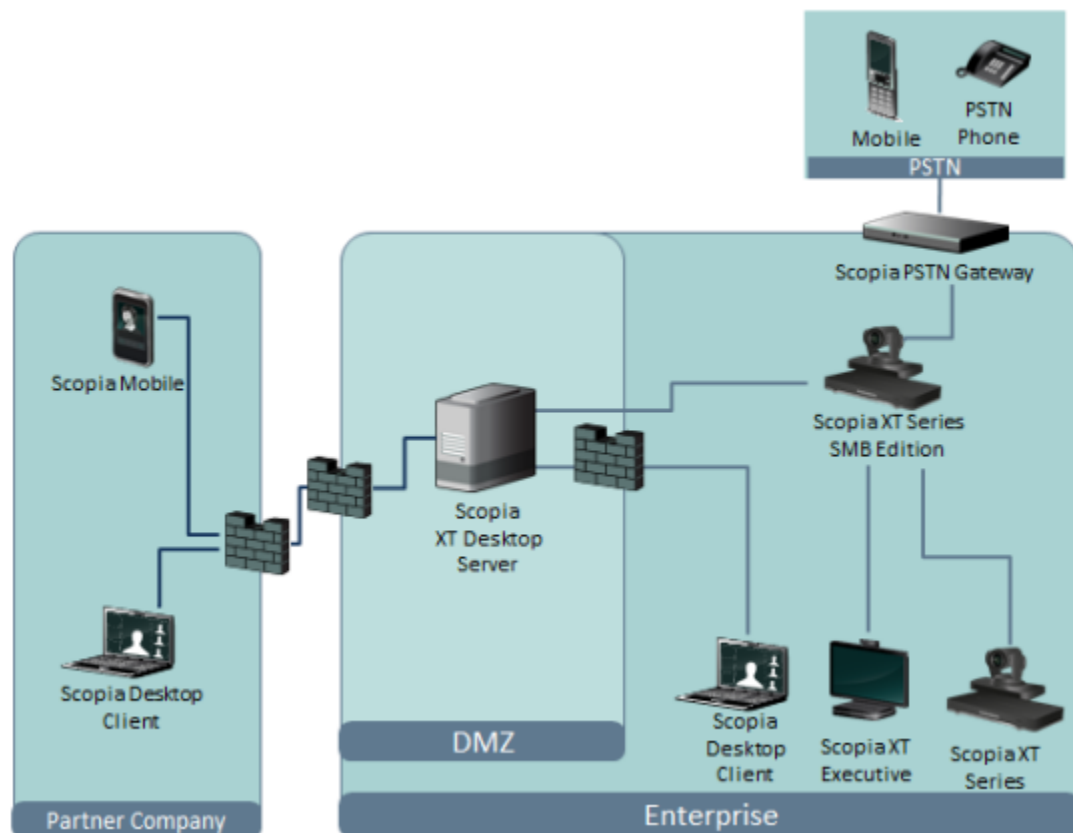


Figure 9: Scopia XT Series SMB Edition Deployment

Planning NAT and Firewall Traversal with Scopia XT Series

The Scopia XT Series fully supports NAT and firewall traversal, enabling you to place the unit behind a NAT router or firewall and connect with other endpoints seamlessly. This section describes the available methods to incorporate NAT and firewall traversal with XT Series:

- Using a Radvision HTTP server or a STUN public server for NAT and firewall traversal

When the XT Series hosts a videoconference with endpoints outside the enterprise ([Figure 10: Using an HTTP/STUN Server for NAT and Firewall Traversal](#) on page 23), it first queries the

HTTP or STUN server to discover its public IP address, then sends it to any external endpoints wishing to join the conference. The external endpoints then answer the call using the IP address provided. Configure the XT Codec Unit for HTTP or STUN autodiscovery.

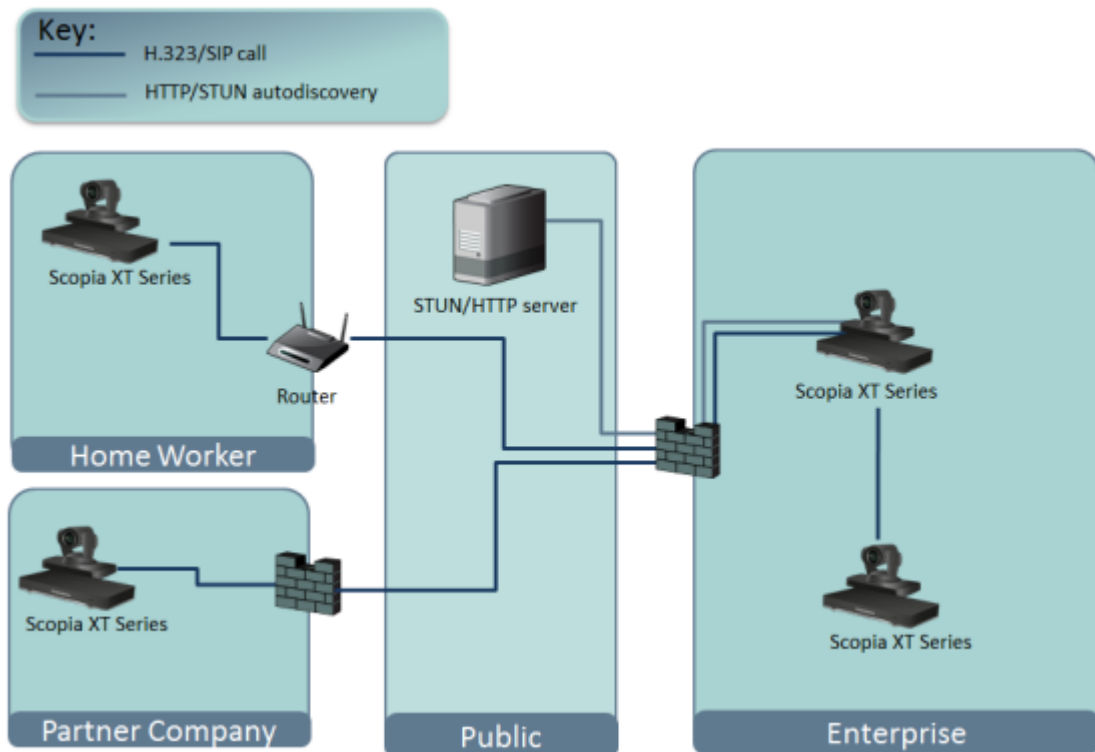


Figure 10: Using an HTTP/STUN Server for NAT and Firewall Traversal

This approach works well in simple NAT and firewall traversal deployments, typically used by home offices and Small Medium Businesses (SMBs).

- Using a NAT/firewall traversal server supporting H.460

The endpoints in the private network communicate with the endpoints located in the public network via an H.460 NAT/firewall traversal server, like the Scopia PathFinder (see [Figure 11: Using a NAT and Firewall Traversal Server](#) on page 24). Endpoints in the public network can join a conference hosted in the private network via the traversal server if there is an open connection through the firewall. Verify the duration of the firewall pinhole and configure that time in the XT Codec Unit.

Having a dedicated NAT/firewall traversal server like the Scopia PathFinder offers external endpoints a static address when joining conferences hosted in your organization. You can dial 1234@pathfinder.company.com to access from outside the firewall, or you can dial 1234 directly if you are a H.460 client logged in to the Scopia PathFinder Server.

H.460 is an extension of the H.323 protocol used for NAT and firewall traversal, employing ITU-T standards. The traversal server can be a Scopia PathFinder or a third-party ITU-T compliant server.

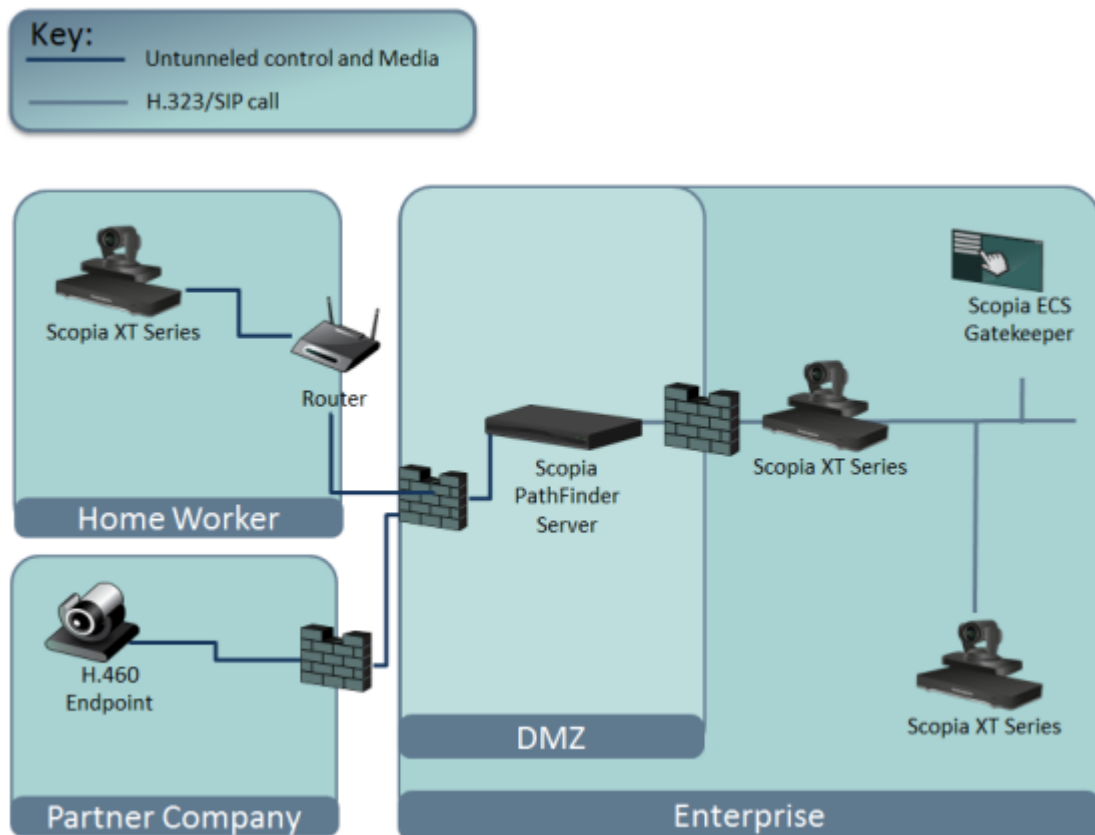


Figure 11: Using a NAT and Firewall Traversal Server

Configure the traversal server as the XT Codec Unit gatekeeper and enable the H.460 option. Configure the XT Codec Unit to the IP address of the traversal server Scopia PathFinder.

- Using the XT Series for NAT and firewall traversal

In cases where your organization has no sophisticated firewall protection, the XT Series can straddle the two network zones using the two network ports provided on the XT Codec Unit (see [Figure 12: Using XT Series for NAT and Firewall Traversal](#) on page 25).

Use the GLAN ports of the XT Codec Unit simultaneously and connect one port to the public network and the other to your private network. All communication passes through the XT Series which acts as the virtual conference room for all the endpoints.

! Important:

The second GLAN is an optional feature for selected models (for details, see [Installing and Enabling Licenses which Extend System Functionality](#) on page 76).

For deployments without a gatekeeper, you can dial ISDN endpoints by simply dialing the ISDN number. To do so, you must first configure the endpoint with your Scopia Gateway for ISDN, as described below. The system then automatically and transparently takes care of setting the bit rate and call routing through the Scopia Gateway.

A single gateway can serve multiple endpoints. For example, if your organization needs to enable 5 Scopia XT Series endpoints with ISDN connectivity (at a speed of 256bps), you can use one the Scopia Gateway for ISDN, which supports 5 concurrent calls of 256bps each.

With the gateway approach less communication lines are needed. As all gateways do not connect at the same time and not all calls are ISDN, many more endpoints can share the same ISDN connection and gateway.

Before you begin

Enable Peer-to-Peer mode in the Scopia Gateway for ISDN. For more information, see the Scopia Gateway documentation.

Procedure

1. Access the XT Series web interface, as described in [Accessing XT Series Web Interface](#) on page 62.
2. Select **Administrator Settings > Protocols > ISDN**.
3. Configure the ISDN settings as described below:



Figure 13: Enabling ISDN connectivity

Table 6: Supporting ISDN Connectivity

Field	Description
Enable	Select Yes to allow this Scopia XT Series to quickly dial ISDN endpoints via the Scopia Gateway for ISDN.
Gateway IP Address	Enter the IP address of the Scopia Gateway for ISDN used by your organization.

4. Select **Save**.

Implementing External API Control

You can control the XT Codec Unit using the Scopia XT Series API (requires integration with AMX, Creston, or Extron control devices). Contact Radvision customer support to receive the *Reference Guide for Scopia XT Series API*, which includes the list of commands over the Ethernet interface.

Implementing Port Security for the Scopia XT Series

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

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

Navigation

- [Ports to Open on the XT Series](#) on page 27
- [Configuring the TCP or UDP Port Range on the Scopia XT Series](#) on page 30

Ports to Open on the XT Series

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

- If you are opening ports that are both to and from the XT Series, see [Table 7: Bidirectional Ports to Open on the XT Series](#) on page 28.
- If you are opening outbound ports from the XT Series, see [Table 8: Outbound Ports to Open from the Scopia XT Series](#) on page 29.

Important:

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

Table 7: Bidirectional Ports to Open on the XT Series

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
69	TFTP (UDP)	TFTP client or server	Enables sending and receiving files via TFTP	Cannot send or receive files via TFTP	Optional
80	HTTP (TCP)	Web server	Enables you to remotely perform management tasks via the web user interface, enables NAT auto-discovery via HTTP	In: Cannot access the web server Out: Cannot access the web server and NAT auto-discovery via HTTP does not function	Recommended
123	SNTP (UDP)	SNTP client	Gets the Internet UTC time	Cannot get the Internet UTC time	Recommended
161	SNMP (UDP)	Scopia Management or an SNMP manager station	Enables you to configure and check the system status	Cannot configure or check the status of the system via SNMP	Mandatory if using SNMP manager station
1719	H.225.0/ RAS (UDP)	Any H.323 video network device	Enables H.323 call signaling to a gatekeeper; H.323 endpoints can use gatekeeper services.	H.323 endpoints cannot use gatekeeper services	Mandatory if using a gatekeeper
1720	H.225.0/ Q.931 (TCP)	Any H.323 video network device	Enables H.323 call signaling (Q.931)	Cannot connect H.323 calls	Mandatory
3230-3248	H.225.0/Q.931/ H.245/ SIP (TCP)	Any H.323/SIP video network device	Enables H.323 call control signaling (Q.931), media control signaling (H.245), SIP (TCP) call signaling, and BFCP signaling. Ephemeral TCP ports are used to connect simultaneous H.323 and SIP calls.	Cannot connect SIP/H.323 calls	Mandatory To configure, see Configuring the TCP or UDP Port Range on the Scopia XT Series on page 30
3230-3305	RTP and RTCP (UDP)	Any H.323 video network device	Enables H.323 and SIP media (audio, video, H.224/data RTP) and media control (RTCP). Ephemeral UDP ports are used to connect simultaneous H.323 and SIP media calls.	No media exchanged in H.323 or SIP calls	Mandatory To configure, see Configuring the TCP or UDP Port Range on the Scopia XT Series on page 30
3338	XML Commands (TCP)	Scopia Control, Scopia XT Desktop Server	Enables communication with Scopia Control and Scopia XT Desktop Server by sending commands and receiving responses	Cannot communicate with Scopia Control application or and Scopia XT Desktop Server	Optional

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3478, 3479	STUN (UDP)	STUN Server	Enables endpoints to automatically discover the presence of a firewall or NAT, and to determine their public IP address.	Cannot automatically discover the presence of a firewall or NAT (only manual configuration available)	Optional
5060	SIP (TCP)	Any SIP-enabled video network device	Enables SIP call signaling	Cannot connect SIP calls over TCP	Mandatory
5060	SIP (UDP)	Any SIP-enabled video network device	Enables SIP call signaling	Cannot connect SIP calls over UDP	Mandatory
5070	BFCP (TCP)	Any SIP-enabled video network device	Enables SIP video content (presentation) signaling	No SIP video content available	Mandatory
55003	AT Commands (TCP)	Scopia Management	Enables you to remotely manage the XT Series via API	Cannot send/receive commands	Optional
55099	Software Upgrade (TCP)	Scopia Management/ XT Series Software Upgrade application	Enables software upgrade	Cannot upgrade software	Recommended
60123	Telnet (TCP)	Telnet server	Enables remote management via Telnet	No Telnet access	Optional

Table 8: Outbound Ports to Open from the Scopia XT Series

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

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

About this task

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

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

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

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

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

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

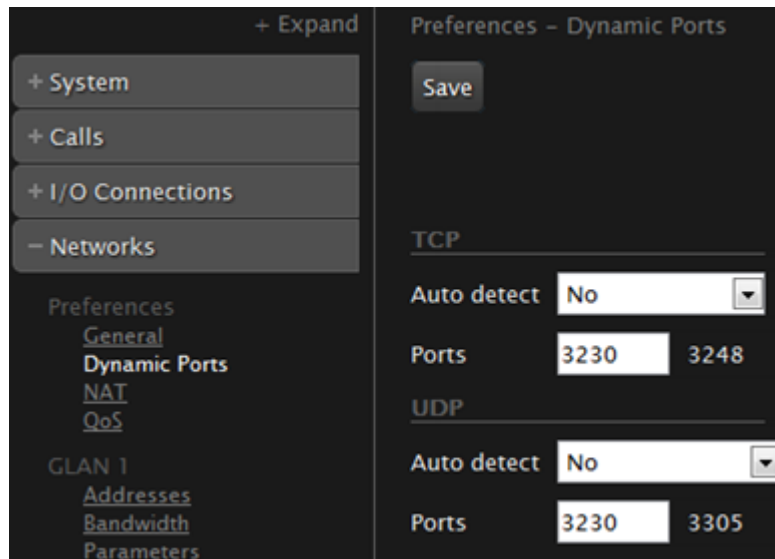


Figure 14: Configuring the TCP or UDP port range from the web interface

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

! Important:

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

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

Chapter 4 | Prerequisites for Setting up the System

Before beginning the installation of the system, you must read the safety regulations for a safe use of the system, verify the conference room setup, and check that the product corresponds to your order. The setup prerequisites are described in these sections:

Navigation

- [Complying with Safety Regulations](#) on page 32
- [Inspecting the Product](#) on page 32
- [Planning the Optimal Conference Room Setup](#) on page 32

Complying with Safety Regulations

For detailed safety information consult the Scopia XT Series Safety Instructions leaflet enclosed in the delivery package.

Inspecting the Product

Inspect the contents of the package for shipping damages.

For a list of package contents see the invoice shipped with your order.

Report any damage or missing items to your distributor or reseller.

Keep the package and its contents for inspection resulting from loss or damage claim.

Planning the Optimal Conference Room Setup

For optimal videoconferencing experience, follow the recommended guidelines described in this section when setting up the conference room.

To see additional information on designing a videoconferencing room, such as the best lighting for optimal video, see <http://blog.radvision.com/videooverenterprise/2010/05/11/ask-the-expert-designing-your-conference-room/>.

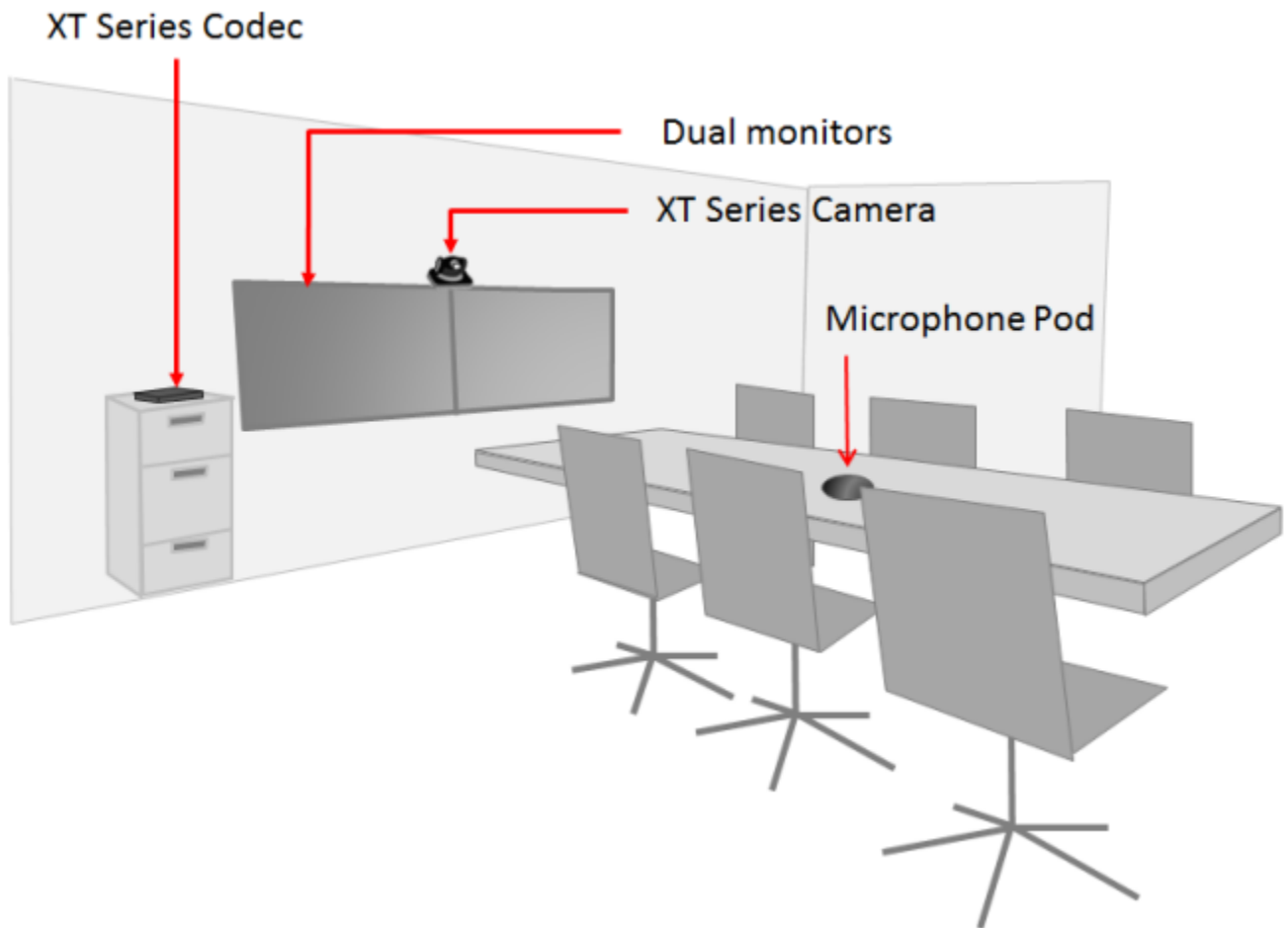


Figure 15: Suggested Room Setup

- When deciding where to place the XT Codec Unit and the camera, ensure that the Infra-Red (IR) sensors of both the XT Codec Unit and the camera, located on the front panels, are not facing sunlight or inverter fluorescent lamps.

This is necessary so that the XT Series can receive IR commands of the XT Remote Control Unit sent from the IR receivers of both the XT Codec Unit and the XT Premium Camera.

The IR commands are sent via VISCA control, which allows you to control your both the camera and the XT Codec Unit using the XT Remote Control Unit.

- Place the XT Codec Unit anywhere within 5 meter reach of the camera cables. Leave enough space for air circulation and for connecting cables easily.
- Place the camera(s) in a position to ensure eye contact between local and remote participants.

We recommend positioning the camera either directly below or directly above the monitors, in central position, at a distance which enables capture of the entire table. For the USB camera, we recommend placing the camera and adjusting the zoom so that the frame is filled with the head and upper body of the user.

⚠ Caution:

Do not place the camera on top of the XT Codec Unit. It can cause the system to overheat.

- Place chairs so that you and other participants appear in the middle of the monitors.
- Place the Microphone Pod at the center of the table, in front of the participants.

To prevent echo cancellation, we recommend positioning the Microphone Pod as far as possible from loudspeakers and other noise sources (for example, computer fans). Do not place paper or other objects in front of the Microphone Pod.

Use 2 Microphone Pods for large conference tables (selected models). Distribute them evenly on the table.

- Avoid white walls as they can introduce an effect-like backlight: a white wall increases the illumination behind the person. Avoid glass walls, as well as patterns and textures on the walls as they may cause disturbances to visual effects. We recommend to have plain walls of neutral color. Also, in order to avoid reverberations, we recommend to use heavy curtains of neutral color and carpets.
- The conference room should be air-conditioned and kept at a cool temperature to avoid the XT Codec Unit switching on its fan.
- The conference room should be well and uniformly lit, avoiding a mixture of natural and artificial light. Light should come from the top of the conference table, the front and the rear (for depth of field). If only ceiling light is available, it should contribute to maintain a pleasant environment and generate as less heat as possible.

Chapter 5 | Setting up the Scopia XT Series

After reading the section [Prerequisites for Setting up the System](#) on page 32, you can install the Scopia XT Series. These sections describe how to install the XT Codec Unit and connect its accessories:

Navigation

- [Mounting the XT Codec Unit](#) on page 35
- [Connecting Scopia XT Series to Your Network](#) on page 35
- [Connecting a Computer to the Scopia XT Series](#) on page 36
- [Selecting the Computer Display Resolution](#) on page 38
- [Connecting Audio Equipment to the Scopia XT Series](#) on page 39
- [Connecting the Video Equipment to the Scopia XT Series](#) on page 47
- [Installing the Batteries of the XT Remote Control Unit](#) on page 59

Mounting the XT Codec Unit

About this task

Follow the guidelines in this section to correctly place the XT Codec Unit.

Procedure

Place the XT Codec Unit following these guidelines:

- Place the XT Codec Unit on a horizontal surface which stands firmly on its base.
- The surface must be dry and free of dust, oil and other residues.
- Leave enough space for air circulation and for connecting cables easily.
- Place the XT Codec Unit anywhere within 5 meter reach of the camera cables.

Caution:

Do not place the camera on top of the XT Codec Unit. It can cause the system to overheat.

Connecting Scopia XT Series to Your Network

About this task

Your Scopia XT Series has two GLAN 10/100/1000 ports for connecting to the network.

❗ Important:

GLAN2 is available in selected models only. For more information, refer to [Comparing Between Scopia XT Series Models](#) on page 12 and [Installing and Enabling Licenses which Extend System Functionality](#) on page 76.

You can use both ports for connecting to the private and public network, however we recommend that you always connect the private network to the second GLAN port, whether one router interfaces with the Scopia XT Series or multiple routers interface with the Scopia XT Series ([Figure 16: Connecting the XT Codec Unit to a private and a public network](#) on page 36).

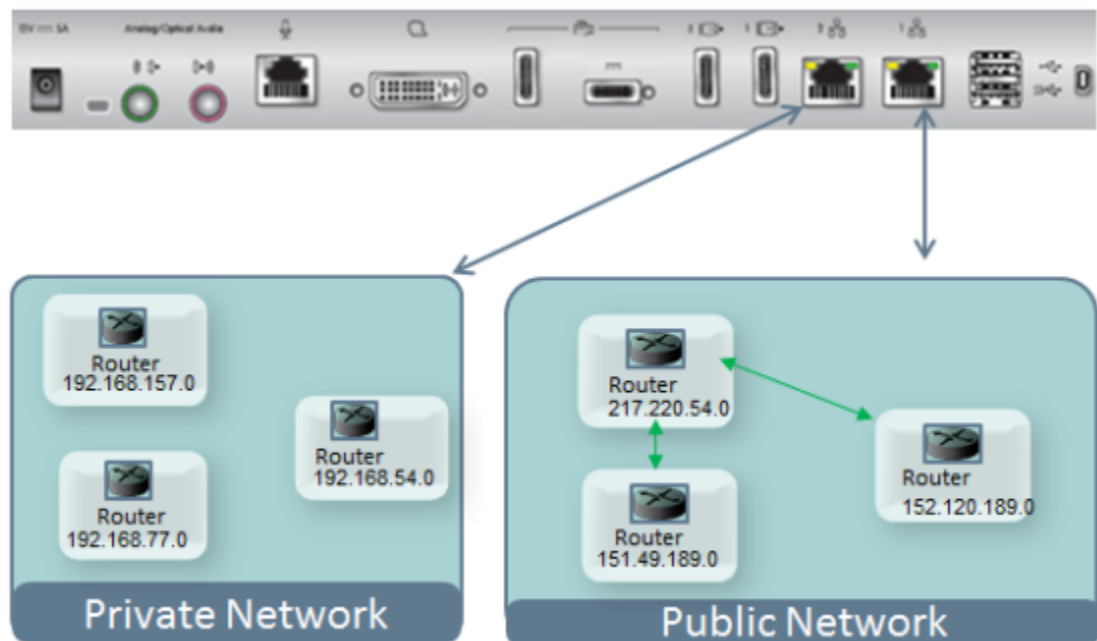


Figure 16: Connecting the XT Codec Unit to a private and a public network

For more information, see [Planning NAT and Firewall Traversal with Scopia XT Series](#) on page 22.

Connecting a Computer to the Scopia XT Series

About this task

Use a computer to share a presentation or other PC content during a call. This procedure describes how to connect computers that are equipped with a DVI-out or VGA-out connector.

Procedure

1. Connect your computer to the XT Codec Unit:
 - For computers and laptops with a DVI out connector, connect the DVI cable to the DVI-I socket of the XT Codec Unit and connect the other end of the cable to the computer.



Figure 17: Connecting a computer to Scopia XT Series

- For computers with a VGA output connector, use the included DVI to VGA adapter.
 - a. Connect the DVI-VGA adapter to the DVI-IN socket of the XT Codec Unit.
 - b. Connect a VGA cable to the adapter. This cable is not supplied with the system.
 - c. Connect the VGA cable to the PC/Laptop VGA out socket.
2. Connect the computer audio to the XT Codec Unit.

When you share content from the PC during a call, remote participants hear the computer's audio output as well as the audio from the Microphone Pod.

! Important:

The audio input port supports both analog and digital optical audio.



Figure 18: Connecting the computer's audio to the XT Codec Unit

3. Continue with setting the display resolution, as described in [Selecting the Computer Display Resolution](#) on page 38.

Selecting the Computer Display Resolution

About this task

For optimal display quality, and to prevent the screen from flickering during the videoconference, set the computer display to one of the supported picture resolutions and refresh frequencies. This procedure assumes computers running Microsoft Windows.

Procedure

1. From the Windows **Control Panel**, navigate to the screen resolution settings.
2. Select the desired screen resolution. See [Table 9: DVI input formats supported by XT Codec Unit](#) on page 38 for the list of resolutions supported by the XT Codec Unit.

Table 9: DVI input formats supported by XT Codec Unit

Name	Resolution
1080p	1920x1080
SXGA	1280x1024
HD+ (900p)	1600x900
WSGA	1440x900
UVGA	1280x960

Name	Resolution
WXGA	1280x768/ 1280x800
720p	1280x720
XGA	1024x768
SVGA	800x600
VGA	640x480

3. Select **Apply**.
4. Select the refresh frequency rate from the **Screen refresh rate** field. See [Table 10: Resolution and refresh rates](#) on page 39 for the supported resolution and refresh rates.

Table 10: Resolution and refresh rates

Name	Resolution	Digital Refresh Rate (Hz)	Analog Refresh Rate Frequency (Hz)
1080p	1920x1080	60	60
SXGA	1280x1024	60, 75	60, 75
HD+ (900p)	1600x900	60	N/A
WSGA	1440x900	60	60
UVGA	1280x960	60, 85	60, 85
WXGA	1280x768 / 1280x800	60	60
720p	1280x720	60	60
XGA	1024x768	60, 70, 75	60, 70, 75
SVGA	800x600	60, 72, 75	60, 72, 75
VGA	640x480	72, 75	72, 75

5. Select **Apply**.

Connecting Audio Equipment to the Scopia XT Series

These sections describe how to connect audio equipment, such as a microphone, to the XT Codec Unit:

Navigation

- [Deciding on the Audio Setup for the Scopia XT Series](#) on page 39
- [Connecting the Three-Way Microphone Pod](#) on page 42
- [Connecting the One-Way Microphone Pod and other Analog Microphones](#) on page 43
- [Connecting an Analog Sound System](#) on page 45

Deciding on the Audio Setup for the Scopia XT Series

Typically, you connect a three-way Microphone Pod to the Scopia XT Series. Alternatively, if you connected the USB camera, you can use the built-in microphone (see [Connecting the Optional USB Camera](#) on page 49 for details).

When sharing audio content such as a movie file from a PC, you need to connect the computer's audio output to the XT Codec Unit (for details, see [Connecting a Computer to the Scopia XT Series](#) on page 36). Remote participants hear the audio content from your computer and the Microphone Pod. If no content is being shared, they hear the audio from the Microphone Pod.

For larger rooms, you may want to connect the following (see [Figure 19: Options for connecting audio equipment](#) on page 40):

- An additional three-way Microphone Pod for enhanced room coverage.
 - If the three-way Microphone Pod is insufficient, you can connect an analog microphone, such as the one-way Microphone Pod, and use it with or without the three-way Microphone Pod.
- When connected, you cannot share audio content from your PC with remote participants, since the port used to connect your PC's audio output is also used to connect an external microphone.
- An external loudspeaker for stronger audio output.



Figure 19: Options for connecting audio equipment

About the Microphone Pod

The following Microphone Pods are available for the XT Series:

- Three-way Microphone Pod

Typically used for larger meeting rooms, the three-way Microphone Pod includes digital audio input from all sides for more enhanced coverage (360° range).

- One-way Microphone Pod

Typically used for smaller meeting rooms, the one-way analog Microphone Pod includes analog audio input from one side (180° range).

! Important:

The type of Microphone Pod available depends on your XT Series model. A second Microphone Pod is available for selected models only. For details, see [Technical Specifications](#) on page 13. You cannot use more than two Microphone Pods for one system.

The Microphone Pod performance varies with room characteristics, background noise levels, and loudness and position of speakers.

When used in typical settings, the Microphone Pod can cover a radius of 3 meters (about 10 feet). See [Figure 20: Microphone range of audio input](#) on page 42.

In the current version release, the XT Codec Unit does not encode/decode stereo signals.

For optimal results, place the Microphone Pod as described in [Planning the Optimal Conference Room Setup](#) on page 32.

To connect the Microphone Pod, see [Connecting the Three-Way Microphone Pod](#) on page 42 or [Connecting the One-Way Microphone Pod and other Analog Microphones](#) on page 43.

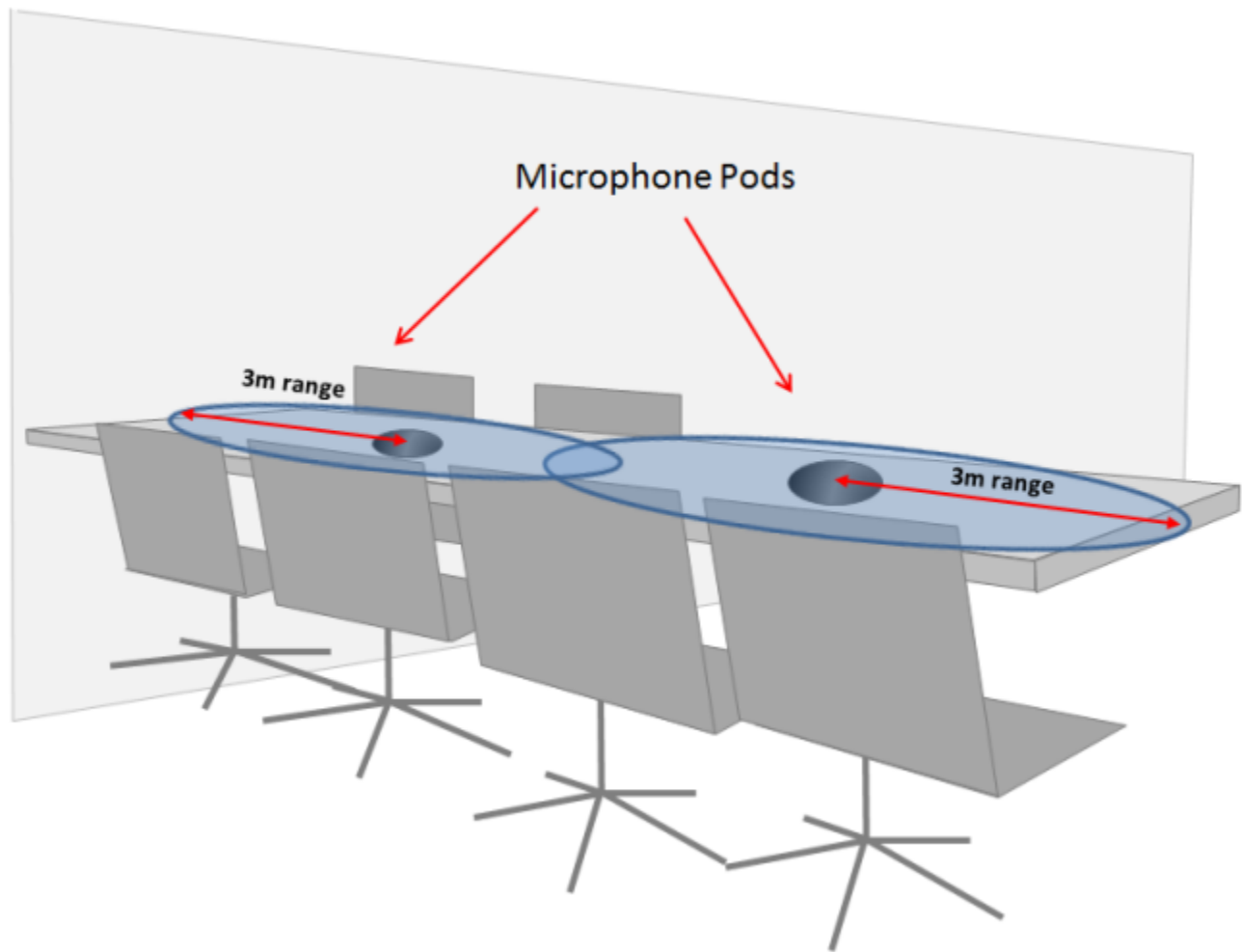


Figure 20: Microphone range of audio input

Connecting the Three-Way Microphone Pod

About this task

Connect the three-way Microphone Pod as described in this procedure. For more information about the Microphone Pod, see [About the Microphone Pod](#) on page 40.

To connect the one-way Microphone Pod, see [Connecting the One-Way Microphone Pod and other Analog Microphones](#) on page 43. For more information about typical audio configurations for the XT Series, see [Deciding on the Audio Setup for the Scopia XT Series](#) on page 39.

Before you begin

For optimal results, place the Microphone Pod as described in [Planning the Optimal Conference Room Setup](#) on page 32.

Procedure

1. Connect the Microphone Pod output  to the rear panel of the XT Codec Unit.



Figure 21: Connecting the Microphone Pods to the XT Codec Unit

2. (Optional) Connect the second Microphone Pod output  to the first Microphone Pod input .



Figure 22: Connecting an additional 3-way Microphone Pod

Connecting the One-Way Microphone Pod and other Analog Microphones

About this task

You can connect the one-way Microphone Pod. For details about the Microphone Pod, see [About the Microphone Pod](#) on page 40.

When the Microphone Pod is not sufficient for covering the room, you can use an external analog/optical microphone. This is typically only done for large-room configurations.

When connecting either the one-way Microphone Pod or another analog/optical microphone, you cannot share audio content from your PC with remote participants, since the port used to connect your PC's audio output is also used to connect an external microphone. To hear both the audio from your computer and the Microphone Pod, either connect the three-way Microphone Pod and your computer output, or use an external mixer device.

Important:

The XT Codec Unit's analog audio input supports either a balanced or unbalanced line microphone. A balanced line microphone reduces audio disruptions from other devices such as cellular phones.

For more information about typical audio configurations for the XT Series, see [Deciding on the Audio Setup for the Scopia XT Series](#) on page 39. To connect the three-way Microphone Pod, see [Connecting the Three-Way Microphone Pod](#) on page 42.

Before you begin

- For optimal results, place the Microphone Pod as described in [Planning the Optimal Conference Room Setup](#) on page 32.
- For very large conference rooms using multiple microphones, or to share both audio output from the computer and audio from the microphone during a call, you need to acquire audio mixers from third-parties. An audio mixer can connect multiple microphones, mix them, cancel the echo and generate a single audio stream that feeds into the audio inputs of your XT Codec Unit.

You can use, for example, Clear One audio mixers, which have been tested with the XT Series:

http://www.clearone.com/professional_conference_system.html

Make sure the microphone mixer provides these connectors: an analog audio I/O (mini jack 3.5") connector and a digital optical connector with a mini-TOSlink adapter.

Procedure

1. Connect the one-way Microphone Pod to the analog audio input ([Figure 23: Connecting the one-way Microphone Pod](#) on page 45).

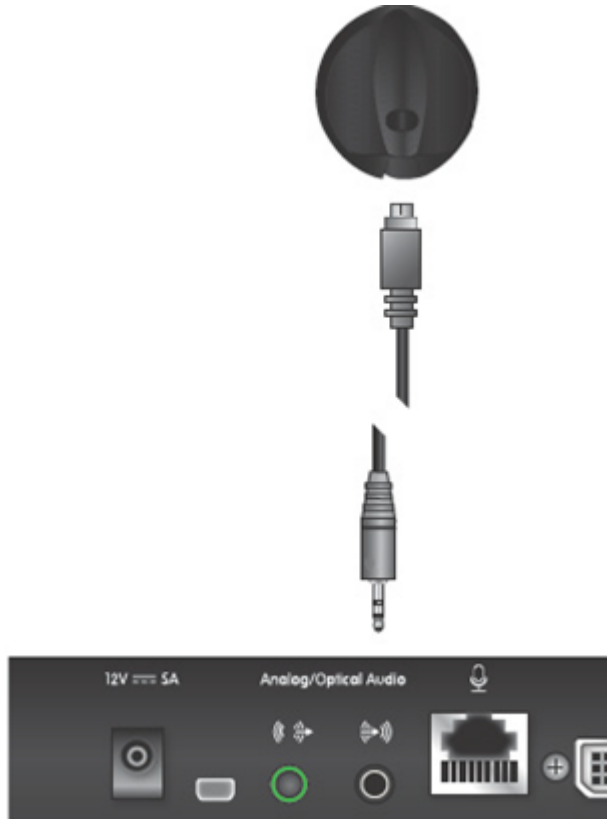


Figure 23: Connecting the one-way Microphone Pod

2. When using a microphone system other than the Microphone Pod, configure the echo cancellation settings:
 - a. Enable/disable echo cancellation as described in [Configuring Analog Audio Connections](#) on page 111:
 - For analog/optical microphone systems that do not contain echo cancellation, enable the echo canceller.
 - For external mixers that handle echo cancellation externally, disable echo cancellation. The echo canceller is automatically disabled when connected to a computer.

! Important:

This is not relevant for the Microphone Pod, which supports echo cancellation automatically.

- b. If you enabled echo cancellation, configure settings as described in [Configuring Analog Audio Connections](#) on page 111.

Connecting an Analog Sound System

About this task

If the room size requires stronger audio output, you can connect analog audio equipment (for example, an external amplifier) to the analog connector of the XT Codec Unit. This procedure specifically describes how to connect an external amplifier.

For more information about typical audio configurations for the XT Series, see [Deciding on the Audio Setup for the Scopia XT Series](#) on page 39.

Before you begin

Verify you have a shielded stereo audio cable with a 3.5mm stereo audio plug:



Figure 24: Stereo audio cable

Procedure

Connect the analog device to the XT Series as follows:

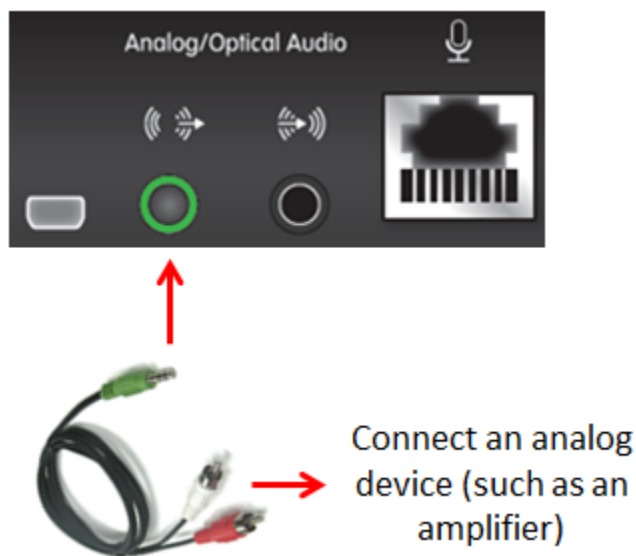


Figure 25: Connecting an Analog Device to the Analog Connector on the XT Series

- Insert the green plug into the green analog connector of the XT Codec Unit.
- Insert the white plug into the left audio device connector.
- Insert the red plug into the right audio device connector.

Connecting the Video Equipment to the Scopia XT Series

These sections describe how to connect the video devices to the XT Codec Unit.

Navigation

- [Connecting the Primary XT Premium Camera](#) on page 47
- [Connecting the Optional USB Camera](#) on page 49
- [Connecting the Optional XT Premium Camera](#) on page 50
- [Connecting Cameras for Controlling the Optional XT Premium Camera with the XT Remote Control Unit](#) on page 51
- [Connecting the Optional Scopia XT Camera Switch](#) on page 53
- [Connecting a DVD or Blu-ray Player](#) on page 58
- [Connecting Analog Video Equipment](#) on page 58

Connecting the Primary XT Premium Camera

About this task

This procedure describes how to connect the primary XT Premium Camera to the XT Series.

You can control and include more than one HDMI camera in your video by connecting them to the Scopia XT Camera Switch (purchased separately). Multiple cameras are typically used for larger meeting rooms or auditoriums. For example, you may want to zoom one camera to focus on the speaker, and use another camera for the audience. Connecting the Scopia XT Camera Switch also allows you use multiple cameras while still keeping the DVI port open to connect a computer and share content. For more information about connecting the Scopia XT Camera Switch, see [Connecting the Optional Scopia XT Camera Switch](#) on page 53.

For details about the camera's capabilities, see [Technical Specifications](#) on page 13.

Procedure

1. Place the camera in a position to ensure eye contact between local and remote participants.

We recommend positioning the camera either directly below or directly above the monitors, in central position, at a distance which enables capture of the entire table. For the USB camera, we recommend placing the camera and adjusting the zoom so that the frame is filled with the head and upper body of the user.

For more information about the room setup, see [Planning the Optimal Conference Room Setup](#) on page 32.

Caution:

Do not place the camera on top of the XT Codec Unit. It can cause the system to overheat.

2. Remove the camera stabilizing cartons.

⚠ Caution:

Failure to remove the camera stabilizing cartons before connecting the camera can cause damage to the system.

3. Insert these connectors on the camera cable to the ports on the back of the camera, as shown in [Figure 26: Connecting cables to the back of the camera](#) on page 48:

- The DVI connector to the DVI socket
- The 8-pin connector to the IN (RS232C) socket
- The power connector to the DC IN 12V socket



Figure 26: Connecting cables to the back of the camera

4. Check that the System Select switch on back panel of the camera is set to 7:



Figure 27: Checking the System Select switch

⚠ Caution:

To adjust the switch, you must first turn the camera off. Adjust it using a slotted 2.5 mm screwdriver.

5. Insert the two connectors on the camera cable to the ports on the XT Codec Unit, as shown in [Figure 28: Connecting the cables to the XT Codec Unit](#) on page 49:

- The HDMI connector to the vertical socket
- The power connector to the horizontal socket

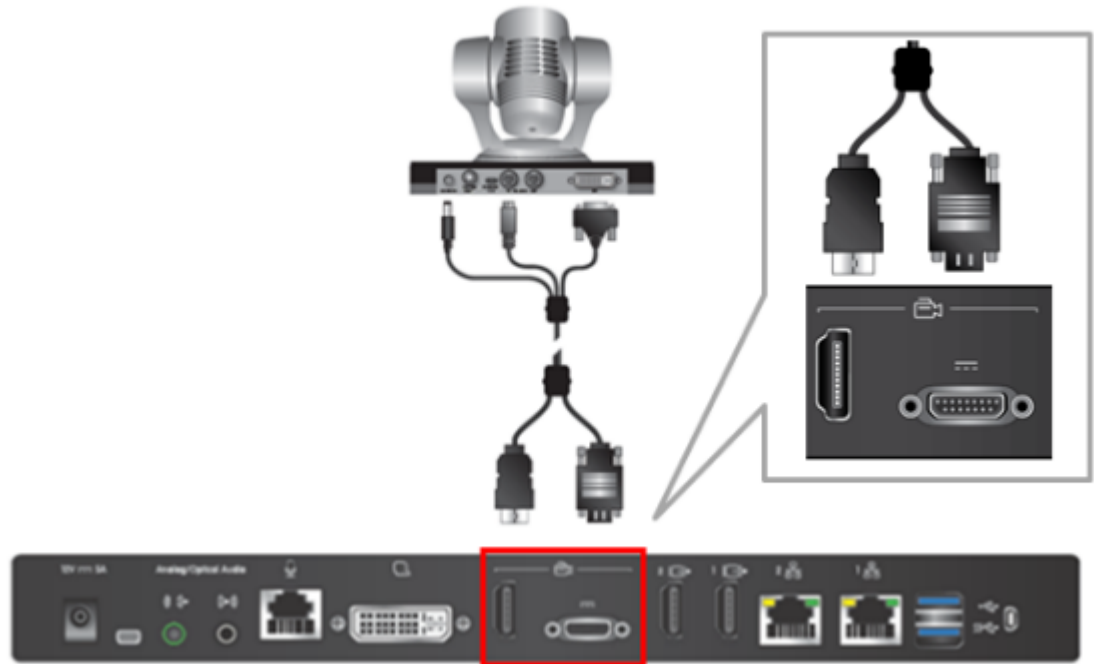


Figure 28: Connecting the cables to the XT Codec Unit

! Important:

If you connect a camera to the DVI-I input, the system manages it as PC content.

6. Enable the HD1 camera and configure its settings, as described in [Configuring the Camera Connection](#) on page 100.

Connecting the Optional USB Camera

About this task

You can connect the optional USB camera to the XT Codec Unit. Currently, the USB camera certified to work with the system is the Logitech C290 Webcam.

We recommend placing the camera and adjusting the zoom so that the frame is filled with the head and upper body of the user.

Procedure

1. Connect the USB cable attached to the camera to the **upper** USB port on the XT Codec Unit:

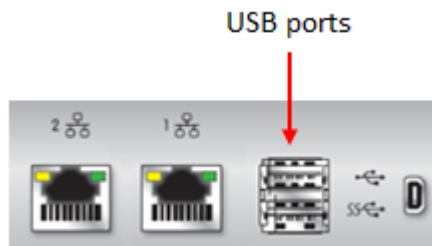


Figure 29: Connecting the USB camera to the XT Codec Unit

2. Enable the USB camera and configure its settings, as described in [Configuring the Camera Connection](#) on page 100.
3. Enable the built-in microphone and configure its settings, as described in [Configuring the Microphone](#) on page 110.

Connecting the Optional XT Premium Camera

About this task

You can connect the optional camera to the XT Codec Unit together with other devices to get the number of video streams that best fit your conference. Typically, you connect the main camera to the HD CAM connector and the optional camera to the DVI connector. For information about connecting a computer, see [Connecting a Computer to the Scopia XT Series](#) on page 36.

You can control and include more than one HDMI camera in your video by connecting them to the Scopia XT Camera Switch (purchased separately). Multiple cameras are typically used for larger meeting rooms or auditoriums. For example, you may want to zoom one camera to focus on the speaker, and use another camera for the audience. Connecting the Scopia XT Camera Switch also allows you use multiple cameras while still keeping the DVI port open to connect a computer and share content. For more information about connecting the Scopia XT Camera Switch, see [Connecting the Optional Scopia XT Camera Switch](#) on page 53.

There are two ways of controlling the XT Premium Camera:

- Using the XT Remote Control Unit provided with the XT Premium Camera kit.
- Using the XT Remote Control Unit. In that case you control both cameras, main and optional, using the same XT Remote Control Unit.

Before you begin

Verify that you have the following:

- An HDMI to DVI adapter, needed to connect the two cameras
- If the included video cables cannot be used for your system because of length requirements, ensure you have a video cable with 1080p60 support

The XT Premium Camera kit contains a camera, remote control, power supply, 5-meter DVI-HDMI cable, and 10-meter VISCA cross cable.

Procedure

1. Remove the camera stabilizing cartons.

⚠ Caution:

Always remove the camera stabilizing cartons before connecting the camera.

⚠ Caution:

Do not place the camera on top of the XT Codec Unit. It can cause the system to overheat.

2. Connect the camera to the DVI Input connector on the XT Codec Unit:



Figure 30: Connecting the optional XT Premium Camera for Scopia XT5000 Series

❗ Important:

If you connect a camera to the DVI-I input, the system manages it as PC content.

3. Connect the power supply cable to the DC IN connector on the camera.
4. Plug the power supply cable into one of the power sockets on the wall.
5. To enable controlling the camera using the XT Remote Control Unit, connect a crossed VISCA control cable to the RS-232C IN connector on the camera and to the RS-232C OUT connector on the main camera. For instructions, see [Connecting Cameras for Controlling the Optional XT Premium Camera with the XT Remote Control Unit](#) on page 51.
6. Apply power to the camera.

Connecting Cameras for Controlling the Optional XT Premium Camera with the XT Remote Control Unit

About this task

The optional camera is supported for selected models only.

You can control the optional camera using the XT Remote Control Unit instead of the camera remote control. To do this, you must connect a VISCA Cross cable between the main and the optional cameras.

Important:

The camera remote control is disabled when you connect the main and optional cameras using a VISCA Cross cable.

VISCA Control is a standard protocol to control PTZ Cameras. VISCA Control is implemented through the cable connection from the main camera to the CTRL CAM input of the XT Codec Unit. Through the VISCA interface, the XT Codec Unit sends commands that change the camera capture resolution, PTZ properties and more.

You can control and include more than one HDMI camera in your video by connecting them to the Scopia XT Camera Switch (purchased separately). Multiple cameras are typically used for larger meeting rooms or auditoriums. For example, you may want to zoom one camera to focus on the speaker, and use another camera for the audience. Connecting the Scopia XT Camera Switch also allows you use multiple cameras while still keeping the DVI port open to connect a computer and share content. For more information about connecting the Scopia XT Camera Switch, see [Connecting the Optional Scopia XT Camera Switch](#) on page 53.

Before you begin

- Buy a VISCA Cross cable, available in the optional cable kit. Alternatively, you can create a cable of the required length if you're planning to position the optional camera far away from the XT Codec Unit.
- If the XT Codec Unit is installed in a cabinet, the XT Codec Unit IR receiver cannot function properly. In this case, the IR sensor of the main camera (not the optional camera) receives the IR signals coming from the XT Remote Control Unit and sends them to the XT Codec Unit through the VISCA interface.

For this type of setup, enable the **Always power on camera** field in **Administrator settings > I/O Inputs > Cameras** (for details, see [Configuring the Camera Connection](#) on page 100).

Procedure

1. Measure the distance that separates the main camera from the optional camera, and cut the cable to the required length. The cable's maximal allowed length is 15m (50ft). Attach each end of the VISCA Cross cable to an 8-pin mini-DIN male connector.



Figure 31: 8-Pin Mini-DIN Connector

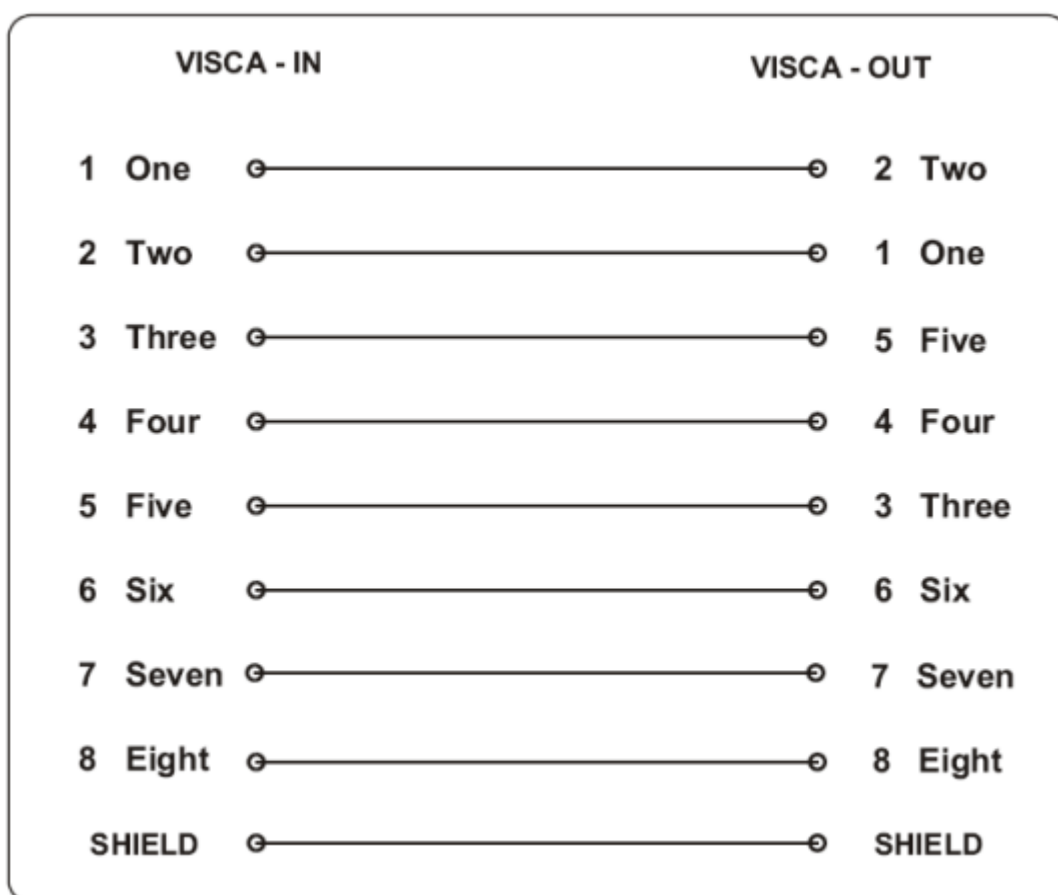


Figure 32: Pinout Diagram

2. Connect the VISCA Cross cable from the main camera VISCA OUT to the optional camera VISCA IN.

Check that the **SYSTEM SELECT** switch on the back panel of the camera is set to 7.

Connecting the Optional Scopia XT Camera Switch

About this task

You can control and include more than one HDMI camera in your video by connecting them to the Scopia XT Camera Switch (purchased separately). Multiple cameras are typically used for larger meeting rooms or auditoriums. For example, you may want to zoom one camera to focus on the

speaker, and use another camera for the audience. Connecting the Scopia XT Camera Switch also allows you use multiple cameras while still keeping the DVI port open to connect a computer and share content.

You can connect to the Scopia XT Camera Switch an XT Premium Camera or any other HD device with a supported resolution, included a DVD or Blu-ray player.

! Important:

You can only connect and use together cameras of the same model.

Before you begin

⚠ Caution:

- Make sure all units are switched off when connecting or disconnecting devices.
- Always remove the camera stabilizing cartons before connecting the camera.
- Do not place a camera on top of the XT Codec Unit. It can cause the system to overheat.

Procedure

1. Install the Scopia XT Camera Switch on a horizontal surface close to the XT Codec Unit. Maximum supplied cable length is 40cm (0.13ft).
2. Connect the following cables between the Scopia XT Camera Switch and the XT Codec Unit ([Figure 33: Connecting the Scopia XT Camera Switch to the XT Codec Unit](#) on page 54):
 - Connect one end of the HDMI cable to the **OUTPUT** socket on the Scopia XT Camera Switch and the other end to the vertical HDMI connector on the XT Codec Unit.
 - Connect one end of the USB cable to the USB socket on the Scopia XT Camera Switch and the other end to the upper USB connector on the XT Codec Unit.

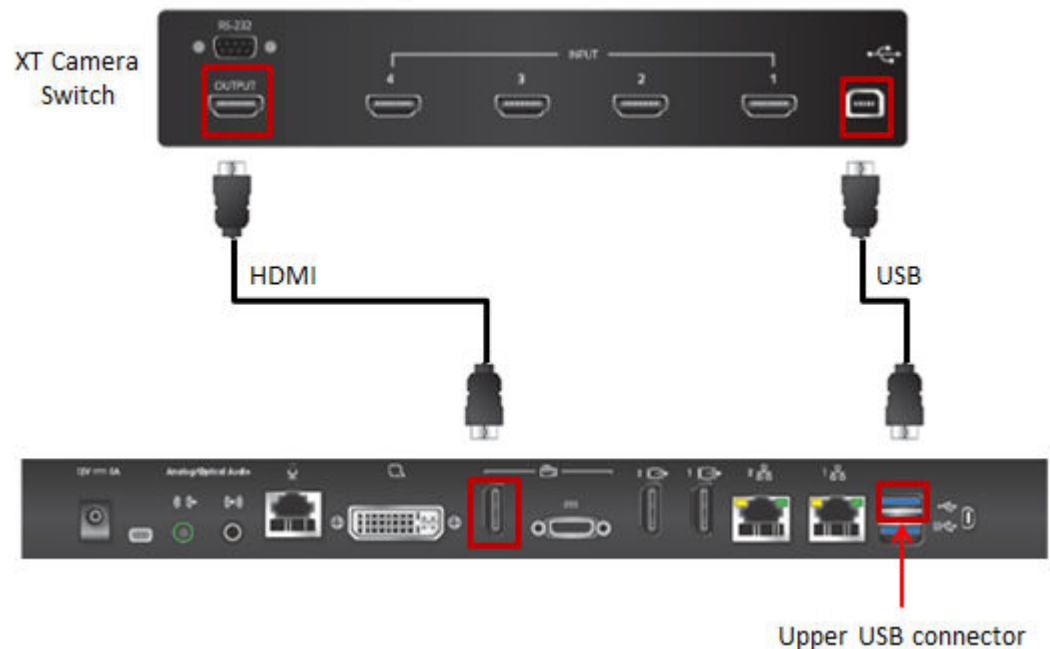


Figure 33: Connecting the Scopia XT Camera Switch to the XT Codec Unit

3. Insert the three connectors of the camera cable (3 connectors on one side, 2 connectors on the other side) to the sockets on the back of the camera, as shown in [Figure 26: Connecting cables to the back of the camera](#) on page 48:
 - The DVI connector to the **DVI** socket
 - The 8-pin connector to the **IN RS232C** socket
 - The power connector to the **DC IN 12V** socket



Figure 34: Connecting cables to the back of the camera

4. Attach the two connectors on the other end of the camera cable as shown in [Figure 35: Connecting cables to the Scopia XT Camera Switch](#) on page 56:
 - a. The HDMI connector to the HDMI socket labeled **1** on the Scopia XT Camera Switch.
 - b. The connector for power and serial control to the  horizontal socket on the XT Codec Unit.

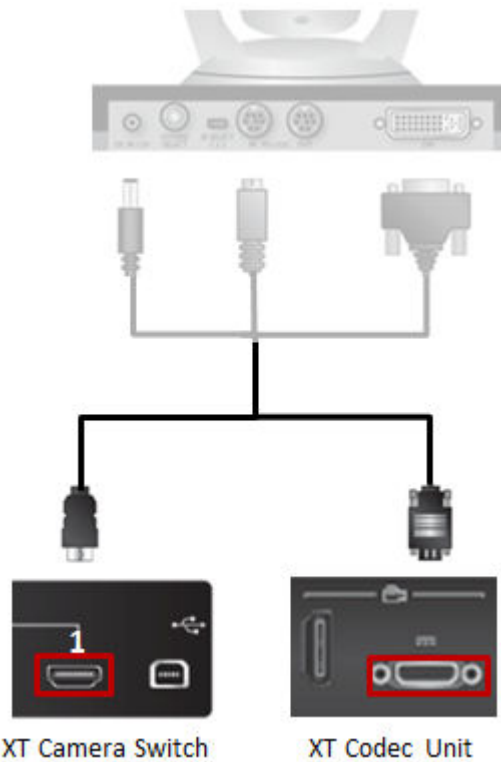


Figure 35: Connecting cables to the Scopia XT Camera Switch

5. Connect the second camera ([Figure 36: Connecting the second camera](#) on page 57):
 - a. Connect the 10-meter VISCA Control cable supplied with the camera kit.

! Important:

If you're planning to position the optional camera further away from the XT Codec Unit, you can create a cable of up to 15 meters (50 feet) by attaching each end of the VISCA Cross cable to an 8-pin mini-DIN male connector.

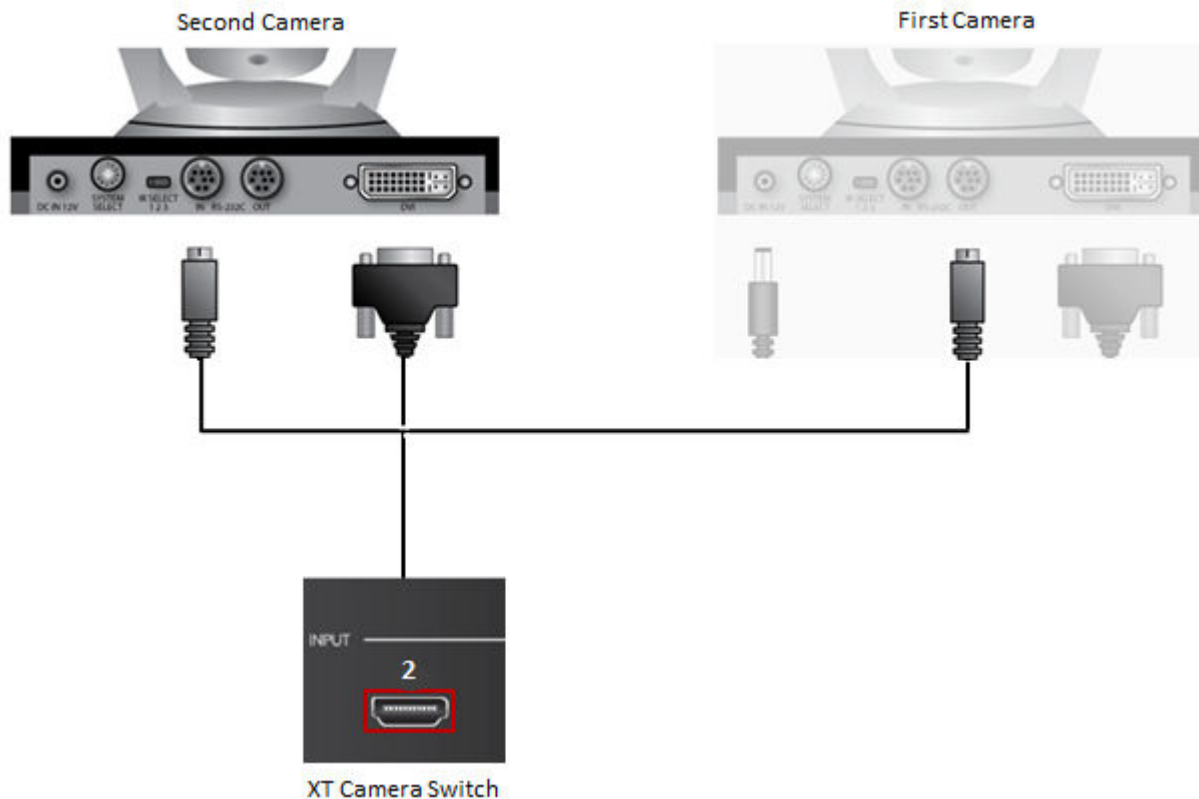


Figure 36: Connecting the second camera

- Attach one end of the VISCA control cable to the **IN RS-232C** connector on the second camera.
 - Attach the other end to the **OUT RS-232C** connector on the first camera.
- b. Connect the DVI-HDMI cable:
- Attach the DVI connector to the **DVI** socket on the second camera.
 - Attach the HDMI connector to the HDMI socket labeled **2** on the Scopia XT Camera Switch.

6. If required, repeat the above step for a third or fourth camera.

7. Check that the **SYSTEM SELECT** switch on the back panel of each camera is set to **7**:



Figure 37: Checking the SYSTEM SELECT switch

⚠ Caution:

To adjust the switch, you must first turn the camera off. Adjust it using a slotted 2.5 mm screwdriver.

8. Turn on the XT Codec Unit by pressing the  power key on the XT Remote Control Unit. This also turns on the Scopia XT Camera Switch.

9. Connect one end of the power supply cable to the **DC IN 12V** connector on the camera, and the other end into one of the power sockets on the wall.
 10. Configure the cameras' settings as explained in [Configuring the Camera Connection](#) on page 100.
- If required, connect the DVD or Blu-ray player to a socket on the Scopia XT Camera Switch using an HDMI cable.

Connecting a DVD or Blu-ray Player

About this task

You can connect a DVD or Blu-ray player to the Scopia XT Series to share its content during a videoconference. XT Series supports High-bandwidth Digital Content Protection (HDCP):

- You can only view digitally protected content on a device that supports HDCP.
- You cannot view digitally protected content on a device that copies HDCP content.
- You cannot send digitally protected content to non-HDCP devices.
- If the XT Codec Unit detects that non-compliant devices are attached to one of the HD CAM inputs, the video is locked.

Connect a DVD or Blu-ray player to the HD CAM or DVI inputs of the XT Codec Unit:



Connect DVD/ Blu-ray player
to one of these ports

Figure 38: Connecting a DVD or Blu-ray Player

Connecting Analog Video Equipment

About this task

As an alternative to the XT Premium Camera, you can connect an analog video device, such as an analog camera.

Before you begin

The XT Codec Unit features digital inputs and outputs. To connect an analog video device, you need an external analog-to-digital (or vice-versa) video converter.

Radvision has tested and certified these two video converters from Gefen:

- GTV-COMPSVID-2-HDMIS, Composite/S-Video to HDMI Scaler
- GTV-HDMI-2-COMPSVIDS, HDMI to Composite/S-Video Scaler

See the company's site for documentation.

Procedure

Connect the analog camera to either the HD CAM or DVI ports, using the Composite/S-Video to HDMI Scaler:

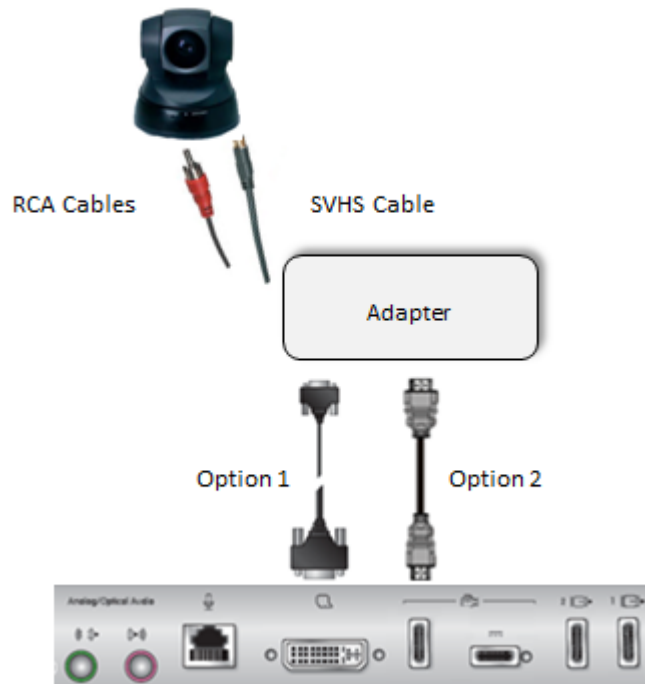


Figure 39: Connecting an Analog Camera

Installing the Batteries of the XT Remote Control Unit

About this task

The XT Remote Control Unit requires CR2025 Lithium batteries (3V). When the XT Remote Control Unit's battery power is low, an icon appears on the GUI letting you know that you should replace the battery:

-  Half-charged Battery
-  Low Battery

 Important:

When the Low Battery icon appears on the display, we recommend to change batteries immediately, to ensure proper functioning of the system.

For battery disposal information refer to the Safety Instructions leaflet.

Procedure

1. Slide the battery compartment cover open.
 2. Put the battery in, making sure the battery is positioned correctly.
 3. Slide the battery compartment cover back until you hear a click.
-

Chapter 6 | Initial Configuration

After connecting the system and powering it on as described in [Setting up the Scopia XT Series](#) on page 35, perform the initial configuration as described in these sections:

Navigation

- [How to Control the XT Series](#) on page 61
- [Registering and Enabling your Scopia XT Series license](#) on page 75
- [Performing Basic Configuration](#) on page 82
- [Setting Basic System Information](#) on page 90
- [Configuring Video Connections](#) on page 99
- [Configuring Audio Connections](#) on page 109
- [Configuring Network Settings](#) on page 117

How to Control the XT Series

You can set up and control your XT Series, as well as make calls, in the following ways:

- From the endpoint's main menu, using your XT Remote Control Unit (see [Using the XT Remote Control Unit](#) on page 68 and [Accessing the Scopia XT Series Main Menu](#) on page 67).
- From the XT Series's web interface (see [Accessing XT Series Web Interface](#) on page 62).

Before performing initial configuration, we recommend reading the following topics to familiarize yourself with how to control the XT Series:

Navigation

- [Managing your XT Series from the Web Interface](#) on page 61
- [Managing your XT Series Locally from the Endpoint](#) on page 66

Managing your XT Series from the Web Interface

You can configure and control the XT Series remotely using the web interface:

- Perform administrative tasks, such as:
 - Monitoring the status
 - Backing up the endpoint's configuration files
- Place a call (for details, see *User Guide for Scopia XT Series*)
- Change basic settings, such as the interface language (for details, see [Performing Basic Configuration](#) on page 82)

You can also configure the XT Series from the endpoint itself by first enabling advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

By default, all computers in the network can manage and upgrade the XT Series remotely. To limit access to specific computers in the network, see [Enabling Remote Management on the Scopia XT Series](#) on page 63.

For details on managing your XT Series from the web interface, see:

Navigation

- [Accessing XT Series Web Interface](#) on page 62
- [Enabling Remote Management on the Scopia XT Series](#) on page 63
- [Configuring Remote Upgrade Settings](#) on page 65

Accessing XT Series Web Interface

About this task

This procedure describes how to access the XT Series web interface. The XT Series supports the following internet browsers:

- Internet Explorer version 8 or later
- Google Chrome version 11 or later
- Mozilla Firefox version 3.6 or later
- Apple Safari version 5 or later
- Opera version 11 or later

Procedure

1. Open any of the supported internet browsers and enter the system's IP address.

For example, *http://1.2.3.4/*.

The XT Series login page opens.



Figure 40: Logging into the XT Series web interface

2. Enter the username and password.

The default username for the web interface is **Admin** and the default password is **1234**.

Important:

We recommend changing the default credentials after logging in for the first time, as described in the *Administrator Guide for Scopia XT Series*.

3. (Optional) Select the web interface language from the **Language** list.
 4. Select **Login**.
-

Enabling Remote Management on the Scopia XT Series

About this task

Remote management on your Scopia XT Series is enabled by default. You can configure the Scopia XT Series so that it can be remotely managed from any computer in the network, or from a specific computer only. You can do this procedure from the endpoint itself or from the XT Series web interface.

To remotely upgrade the Scopia XT Series, you must also enable remote downloads, as described in [Configuring Remote Upgrade Settings](#) on page 65.

We strongly recommend that you change the default credentials first time you access the Scopia XT Series remotely, described as part of the procedure below.

See *Administrator Guide for the Scopia XT Series* for information on maintenance tasks to configure and manage your Scopia XT Series.

Before you begin

To configure the network, contact your network administrator.

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

To modify the PIN, you must be connected via HTTPS (see below).

Procedure

1. Access the remote management settings, as follows:
 - From the XT Series web interface, select **Administrator Settings > Utilities > Remote Access > Web**.
 - From the endpoint's main menu, select **Configure > Advanced > Utilities > Remote Access > Web** from the Main menu.

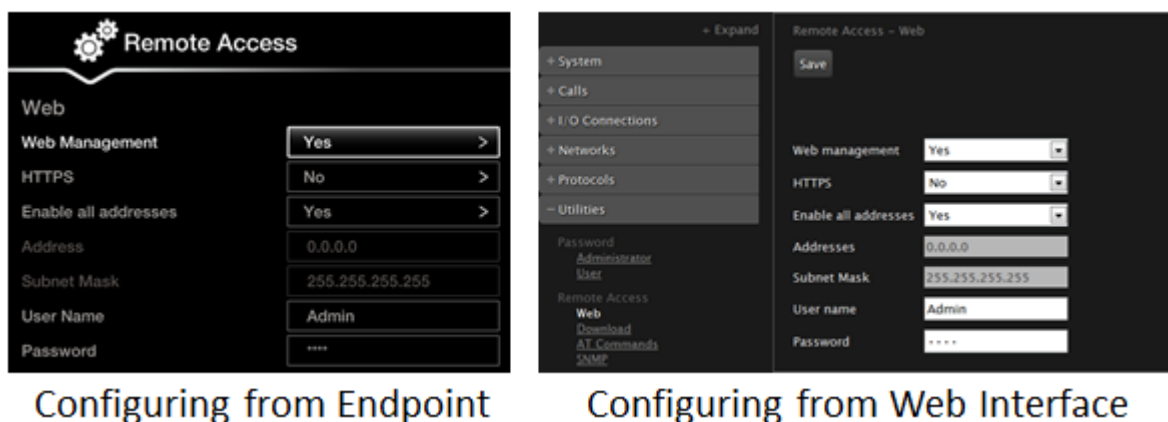


Figure 41: Configuring remote management on Scotia XT Series

2. Set the fields as described in [Table 11: Configuring remote management on Scotia XT Series](#) on page 64.

Table 11: Configuring remote management on Scotia XT Series

Field Name	Description
Web Management	Configure whether to allow remote management via the web interface, as follows: • Select Yes to enable remote management of the Scotia XT Series from its web interface. • Select No to disable remote management of the Scotia XT Series from its web interface.
HTTPS	Configure your web security settings, as follows: • Select Yes to enable secure HTTPS connection to the web when remotely managing the Scotia XT Series from its web interface. • Select No to disable secure HTTPS connection to the web. For example, if you remotely configure your endpoint only from within your network, it may not be necessary to use HTTPS.
Enable all addresses	Allow access to remote management for all or specific PCs, as follows: • Select Yes to enable access to Scotia XT Series from any IP address in a network. • Select No to allow access to specified computers only. If selected, you must also configure the Address and SubNet mask as described below.
Address	This field is only relevant if you set the Enable all addresses field to No. Enter the IP address or IP addresses of the computers allowed to access Scotia XT Series.

Field Name	Description
Subnet Mask	This field is only relevant if you set the Enable all addresses field to No . Enter the Subnet mask associated with the IP address or group of IP addresses specified above.
User Name	The current credentials for remote access are displayed.
Password	Modify the credentials here. You must be connected via HTTPS (see above). The default username for the web interface is Admin and the default password is 1234 . We strongly recommend that you change the default credentials the first time you access the Scopia XT Series remotely.

3. From the web interface only, select **Save**.
4. To perform remote upgrades, enable remote downloads as described in [Configuring Remote Upgrade Settings](#) on page 65.

Configuring Remote Upgrade Settings

About this task

In order to upgrade your Scopia XT Series from the web interface, remote upgrade must be enabled. This procedure describes how to:

- Enable/disable remote upgrades (it is enabled by default)
- Limit access to specific computers in the network. By default, all computers in the network can perform remote upgrades.

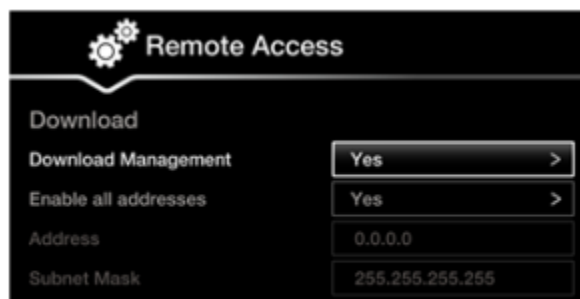
You can do this procedure from the endpoint itself or from the XT Series web interface.

Before you begin

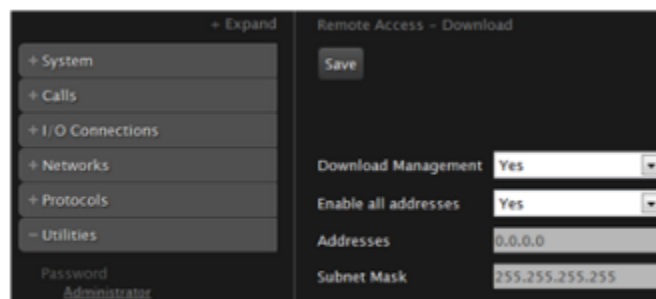
- If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.
- By default, remote management is enabled. If you changed this configuration, make sure that you enable it as described in [Enabling Remote Management on the Scopia XT Series](#) on page 63.

Procedure

1. Access the remote download settings, as follows:
 - From the endpoint's main menu, select **Administrator Settings > Utilities > Remote Access > Download**.
 - From the XT Series web interface, select **Configure > Advanced > Utilities > Remote Access > Download**.



Configuring from Endpoint



Configuring from Web Interface

Figure 42: Enabling remote access to the Scopia XT Series

- Set the fields as described in [Table 12: Enabling remote upgrade](#) on page 66.

Table 12: Enabling remote upgrade

Field Name	Description
Download Management	Configure whether to allow remotely downloading firmware or patches to the XT Codec Unit via a Windows PC upgrade program or Scopia Management, as follows: - Select Yes to enable remote downloads to the Scopia XT Series. - Select No to disable remote downloads to the Scopia XT Series.
Enable all addresses	Allow access to the XT Codec Unit from all or specific PCs or Scopia Management, as follows: - Select Yes to enable access to Scopia XT Series from any IP address in a network. - Select No to allow access to specified computers only. If selected, you must also configure the Address and SubNet mask as described below.
Address	This field is only relevant if you set the Enable all addresses field to No . Enter the IP address or IP addresses of the computers allowed to access Scopia XT Series.
Subnet Mask	This field is only relevant if you set the Enable all addresses field to No . Enter the Subnet mask associated with the IP address or group of IP addresses specified above.

- From the web interface only, select **Save**.
- To upgrade the Scopia XT Series, see *Administrator Guide for Scopia XT Series*.

Managing your XT Series Locally from the Endpoint

You can set up and control the Scopia XT Series from the endpoint's main menu, using your XT Remote Control Unit.

To perform advanced configuration XT Series from the endpoint itself, you must first enable advanced configuration as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

See the following topics for more information:

Navigation

- [Accessing the Scopia XT Series Main Menu](#) on page 67
- [Using the XT Remote Control Unit](#) on page 68
- [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73

Accessing the Scopia XT Series Main Menu

About this task

After switching on the Scopia XT Series, the main menu appears and you can do the following:

- Make audio and video calls
- View contacts in the phone book
- Start sharing content from your computer
- Adjust the camera position. You can also store the position to retrieve it later.
- Record your videoconferences
- Perform basic configuration, such as setting the interface language
- Set your preferences, such as activating the Do Not Disturb feature
- Check the system status

You navigate Scopia XT Series menus using arrow keys and pressing the **ok/menu** key on the XT Remote Control Unit (for details, see [Using the XT Remote Control Unit](#) on page 68).

Procedure

1. Verify that the LED on the front panel of the XT Codec Unit is blinking.
2. Turn on the XT Codec Unit by pressing the  Power key on the XT Remote Control Unit.
3. The system home page appears on the monitors, and you can access the following menus:
 - **Call**—make audio and video calls
 - **Contacts**—view, edit, and call contacts in the phonebook
 - **Present**—start sharing content from your computer
 - **Control Camera**—adjust camera position
 - **Recording**—start recording a videoconference
 - **Configure**—perform basic configuration and check the system status

! Important:

When you access the system for the first time only, the Quick Setup wizard is displayed (for details, see [Accessing the Quick Setup Procedure](#) on page 82).

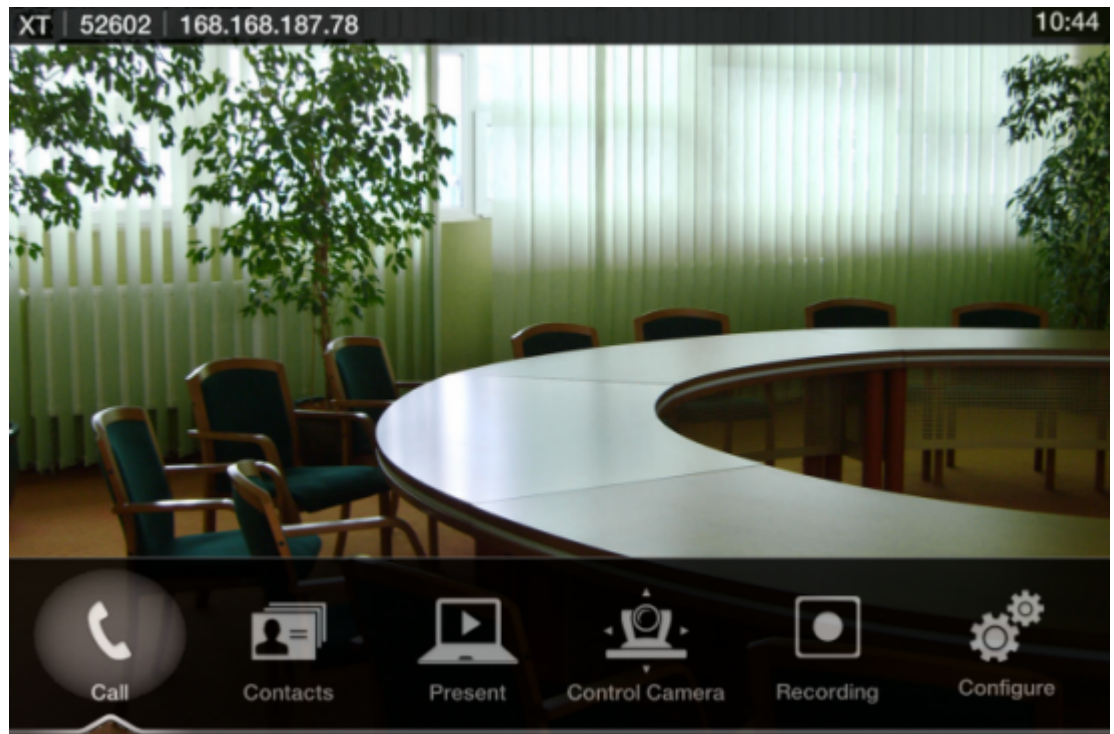


Figure 43: Main menu

4. Select one of the options using the arrow keys of the XT Remote Control Unit.

Using the XT Remote Control Unit

This section explains how to use the XT Remote Control Unit to navigate through the system menus, and lists the function of each key.

The XT Remote Control Unit has an improved design and increases usability to give you a smoother and more efficient videoconferencing experience. [Figure 44: The new XT Remote Control Unit](#) on page 69 describes the functions of the XT Remote Control Unit.



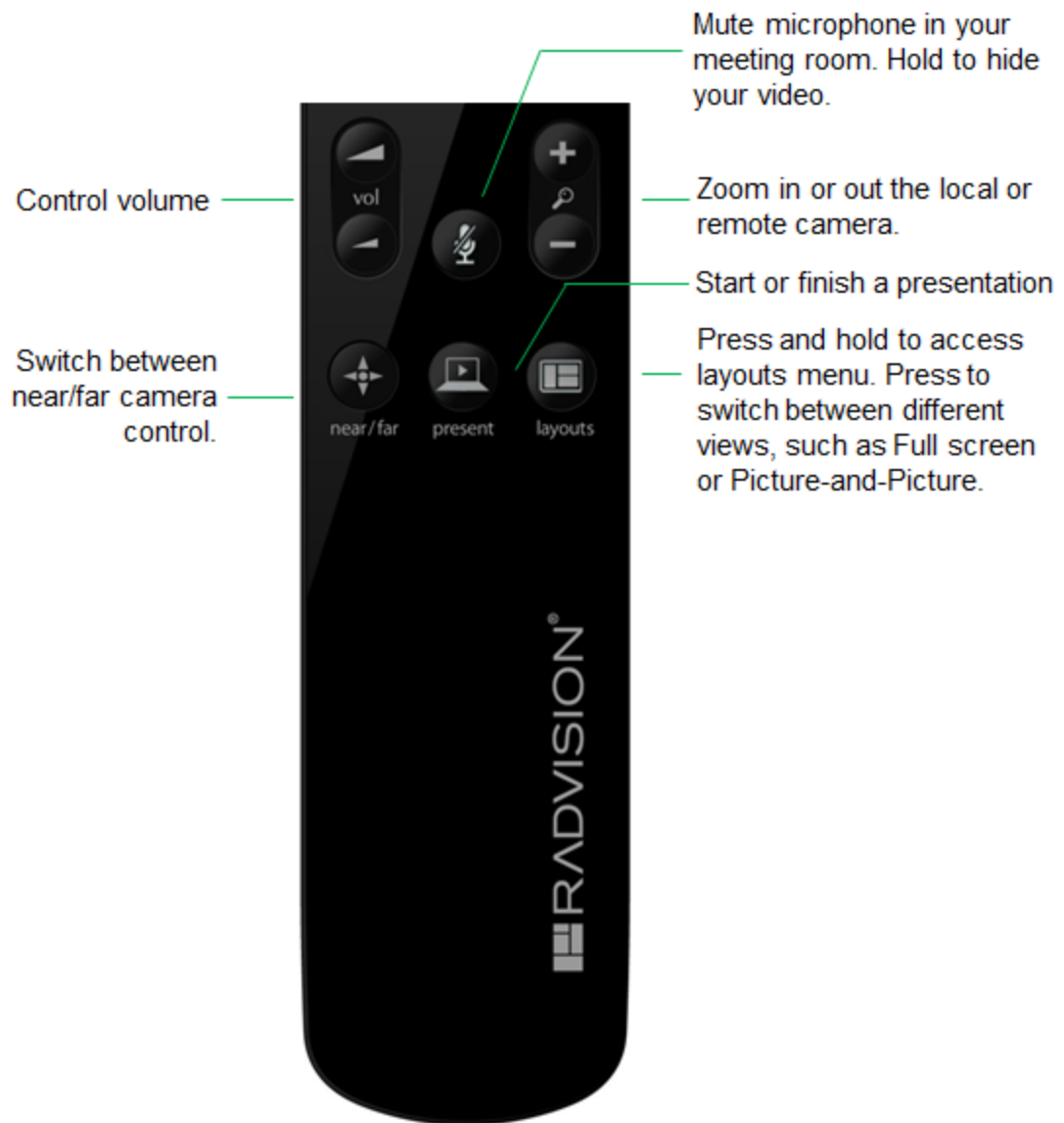


Figure 44: The new XT Remote Control Unit

Use the XT Remote Control Unit to navigate through system menus, as follows:

- Scroll through menus and options using the arrow keys and pressing the **ok/menu** key.

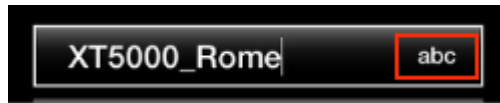
! Important:

Use the **ok/menu** key to select an item or a specific option, such as when choosing the interface language. If there are less than 5 options in a list, press **ok/menu** repeatedly to scroll through the options.

- Use the XT Remote Control Unit keypad to enter letters and digits.

The default input method is **abc1**: you must press the required character key on the XT Remote Control Unit repeatedly before entering a digit. To enter text in the XT Series interface, scroll to the input field and enter the required characters.

The current input method is displayed in the field you are in:



You can also switch between **ABC**, **abc**, and **123** input methods by pressing **1/a/A** repeatedly while the cursor is in the input field.

Pairing an XT Remote Control Unit with a XT Codec Unit

About this task

Multiple XT Codec Units can be set up in the conference room and controlled with different XT Remote Control Units.

Each XT Remote Control Unit is dedicated to one XT Codec Unit by pairing them. This is done by configuring the same numeric code in your XT Remote Control Unit and the system software.

An XT Remote Control Unit is configured with code 01 by default.

Before you begin

Decide what numeric code you want to use for your monitor and the XT Codec Unit. You can choose any value between 1-99.

Procedure

1. Access the general settings, as follows:
 - From the web interface, select **Basic Settings > General**.
 - From the endpoint's Main menu, select **Configure > General**.

Configure

General

System Name: XT Series

Country: USA

Language: English

Screen Saver: Never

Remote Control Code: 1

Local Presentation Mode: Automatic

Keep Presentation Aspect Ratio: No

Show Advanced Settings: Yes

PIN Protect Settings: No

PIN Protect Renewal: Always

Date & Time: 04/07/2009, 05:23

Configuring from Endpoint

General

Save

System Name: XT Series

Country: USA

Language: English

Screen Saver: 5 minutes

Remote Control Code: 1 [1..99]

Local Presentation Mode: <auto>

Keep Presentation Aspect Ratio: No

Show Advanced Settings: Yes

PIN Protect Settings: No

PIN Protect Renewal: Always

Date & Time

Configuring from Web Interface

Figure 45: Setting the XT Remote Control Unit Code

2. Enter the numeric code in the **Remote control code** field. You can choose any value between 1-99.
3. From the web interface only, select **Save**.
4. On the XT Remote Control Unit, press the * and # keys simultaneously until the red led blinks twice.



Figure 46: Setting the code on the XT Remote Control Unit

5. Using the keypad, type the number you just entered in the **Remote control code** field.

! Important:

You must always use two digits for a code. For example, to set the code to “1”, enter “01”.

The code of the XT Remote Control Unit is changed and the Remote Control  icon with the new Remote Control code appear at the top-right corner of the screen:



❗ Important:

The code and icon do not appear when the default code, **01**, is used.

6. Set the code and exit by doing one of the following:

- In the web interface, select **Finish**.
- In the endpoint, press **OK**.

Maintaining the Scopia XT Series Locally from the Endpoint

About this task

To perform advanced configuration and maintain the Scopia XT Series from the endpoint itself, you must first perform this procedure to access advanced settings. For example, you can enable AT commands to manage the endpoint (as described in *Administrator Guide for Scopia XT Series*).

You can also perform advanced configuration from the web interface. See [Managing your XT Series from the Web Interface](#) on page 61 for details.

Before you begin

Ensure that you have the password to access the **Advanced** settings. The default password is **1234**.

Procedure

1. From the endpoint's main menu, select **Configure > General**.



The image shows the 'Configure' screen for the Scopia XT5000 Series. It features a globe icon on the left and a list of settings on the right. The settings are as follows:

General	
System Name	XT5000-bobfog abc
Country	Italy >
Language	English >
Screen Saver	Never >
Remote Control Code	1
Local Presentation Mode	Automatic >
Keep Presentation Aspect Ratio	No >
Show Advanced Settings	Yes >
PIN Protect Settings	No >
PIN Protect Renewal	Always >
Date & Time	04/07/2009, 05:23 >

2. Set **Show Advanced Settings** to **Yes**.
3. Press the **Back** key  on the XT Remote Control Unit.
The **Advanced** section now appears in the **Configure** screen.
4. Select **Configure > Advanced**.
5. Enter the password required to access the **Advanced** settings. The default password is **1234**.
The **Advanced** screen appears.



Figure 47: Advanced configuration screen

6. We recommend changing the default administrator password, as described in [Setting the Administrator PIN Code for the XT Series](#) on page 94.

Registering and Enabling your Scopia XT Series license

About this task

To activate the features of your XT Series, you first register the product to obtain your license key, and then enable the license. Follow the workflow described in this section.

If you do not yet have your license key, you can set up the system in demo mode for a period of 24 hours. After this time, you must enable your license key to use the system.

Procedure

1. Register your system to activate your license key, as described in [Registering the Scopia XT Series to Obtain a License Key](#) on page 75.
2. Enable the license from either the endpoint or the web interface:
 - [Remotely Enabling the License from the Web Interface](#) on page 78
 - [Enabling the License from the Scopia XT Series Endpoint](#) on page 80
3. If you are enabling licenses with additional features, such as an embedded MCU or higher bandwidth, see [Installing and Enabling Licenses which Extend System Functionality](#) on page 76.

Registering the Scopia XT Series to Obtain a License Key

About this task

Register your XT Series to obtain your license key to activate the features of the XT Codec Unit, and receive a number of additional benefits:

- Notification of software updates and new features availability.
- Be the first to know about product support alerts.
- Access to Radvision's user-community.

You can obtain other license keys in the same way, when you need them to enable optional features in the XT Codec Unit, such as increased bandwidth or the embedded MCU, depending on the model. For details, see [Installing and Enabling Licenses which Extend System Functionality](#) on page 76.

Procedure

1. Open the envelope that came with the XT Series.
2. Locate the serial number and the product key in the letter inside the envelope. The serial number is printed on a label affixed at the back of the XT Codec Unit.
You can find the user code (and the serial number) by selecting **Configure > About** from the Main menu.
3. From your computer's Internet browser, navigate to <http://licensing.radvision.com/>.
4. Complete the online registration form and enter the serial number (or the user code) AND the product key.
The web registration form returns an active license key.
5. Write down the license key and keep it in a safe place for future use.
6. Use the license key to enable the software, as described in:
 - [Remotely Enabling the License from the Web Interface](#) on page 78
 - [Enabling the License from the Scopia XT Series Endpoint](#) on page 80

Installing and Enabling Licenses which Extend System Functionality

About this task

You can purchase licenses to extend the functionality of the Scopia XT Series, such as enabling the Scopia XT Series to host its own videoconferences with an embedded MCU, or enhancing the bandwidth capabilities.

[Table 13: Scopia XT Series Software Options](#) on page 77 lists the various license options available for purchase to extend the system's functionality.

Table 13: Scopia XT Series Software Options

Feature	Option/Reference	Description
Bandwidth and Network	55111-00904 Scopia XT Series 12MBPS Option	Increases total bandwidth to 12Mbps
Audio	55111-00948 Additional Audio Codec Pack	Adds G.728 and G.729A audio codecs.
Scopia XT Series MCU Edition Options	55111-00951 Full MCU4 License	Enables hosting videoconferences with up to 4 endpoints. For the XT5000 720, this option also includes a 2nd GLAN port.
	55111-00952 Full MCU9 License	Enables hosting videoconferences with up to 9 endpoints. For the XT5000 720, this option also includes a 2nd GLAN port.
Scopia XT Series SMB Edition Options	55111-00941 Full SMB4 License	Enables hosting videoconferences with up to 4 participants joining from an endpoint, a PC, web browser, or a mobile device. For the XT5000 720, this option also includes a 2nd GLAN port and Scopia Control.
	55111-00942 Full SMB9 License	Enables hosting videoconferences with up to 9 participants joining from an endpoint, a PC, web browser, or a mobile device. If any participants in the videoconference connect from a PC or mobile client, you can have up to 8 participants in the videoconference. For the XT5000 720, this option also includes a 2nd GLAN port and Scopia Control.
Video Resolution	55111-00937 Full HD (1080p)	This option is already included for the XT5000 and is available for the XT5000 720. Higher quality video at 1080p instead the default 720p.
Zoom	55111-10922 Scopia XT Series Zoom Upgrade	This option is already included for the XT5000 and is available for the XT5000 720. Upgrade to 40x digital zoom (10x optical and 4x digital).
Scopia Control	55111-00917 Scopia Control	This option is already included for the XT5000 and is available for the XT5000 720. Enables Scopia XT Series control using the Scopia Control Application (iPad).

Feature	Option/Reference	Description
Network	55111-00916 Scopia XT Series 2nd GLAN Port	This option is already included for the XT5000 and is available for the XT5000 720. Enables 10/100/1000 GLAN port.
Recording Videoconferences	55111-00933 USB Recording License	This option is already included for the XT5000 and is available for the XT5000 720. You can record videoconferences and store them to a connected USB storage device. You cannot record videoconferences when encryption is enabled. For more information, see Enabling Encryption for Videoconferences on page 149 or contact your administrator. When recording a videoconference on a system with an embedded MCU, you can include up to 6 remote endpoints. The Scopia XT Series SMB Edition edition can include up to 5 remote endpoints.

This procedure details how to register your extended license purchase, to convert your new user code and option key into an updated license key.

Procedure

1. Open the envelope that you obtained when you bought your license extension, or refer to the email you received after purchasing the license.
2. Locate the option key in the letter. Locate the serial number on the XT Codec Unit or the user code you received with the purchase.
You can also retrieve the user code and serial number by selecting **Configure > About** from the Main menu.
3. From your computer's Internet browser, navigate to <http://licensing.radvision.com/>.
4. Complete the online registration form and enter the serial number or the user code and the option key. The Web registration form returns a license key.
5. Write down the license key and keep it in a safe place for future use.
6. Use the license key to enable the software or the option you bought, as described in:
 - [Remotely Enabling the License from the Web Interface](#) on page 78
 - [Enabling the License from the Scopia XT Series Endpoint](#) on page 80

Remotely Enabling the License from the Web Interface

About this task

This procedure describes how to enable the software license of an XT Codec Unit remotely via the web interface. You can also enable the license from the endpoint's interface, as described in [Enabling the License from the Scopia XT Series Endpoint](#) on page 80.

If you do not yet have your license key, you can set up the system in demo mode for a period of 24 hours. After this time, you must enable your license key to use the system.

Before you begin

Obtain a license key for the Scopia XT Series as described in [Registering the Scopia XT Series to Obtain a License Key](#) on page 75 or, if you are enabling a license option to extend Scopia XT Series functionality, see [Installing and Enabling Licenses which Extend System Functionality](#) on page 76.

Procedure

1. Access the Scopia XT Series web interface.
2. From the Home page, select **Enable License**, or, navigate to **Administrator Settings > Utilities > Licenses**.

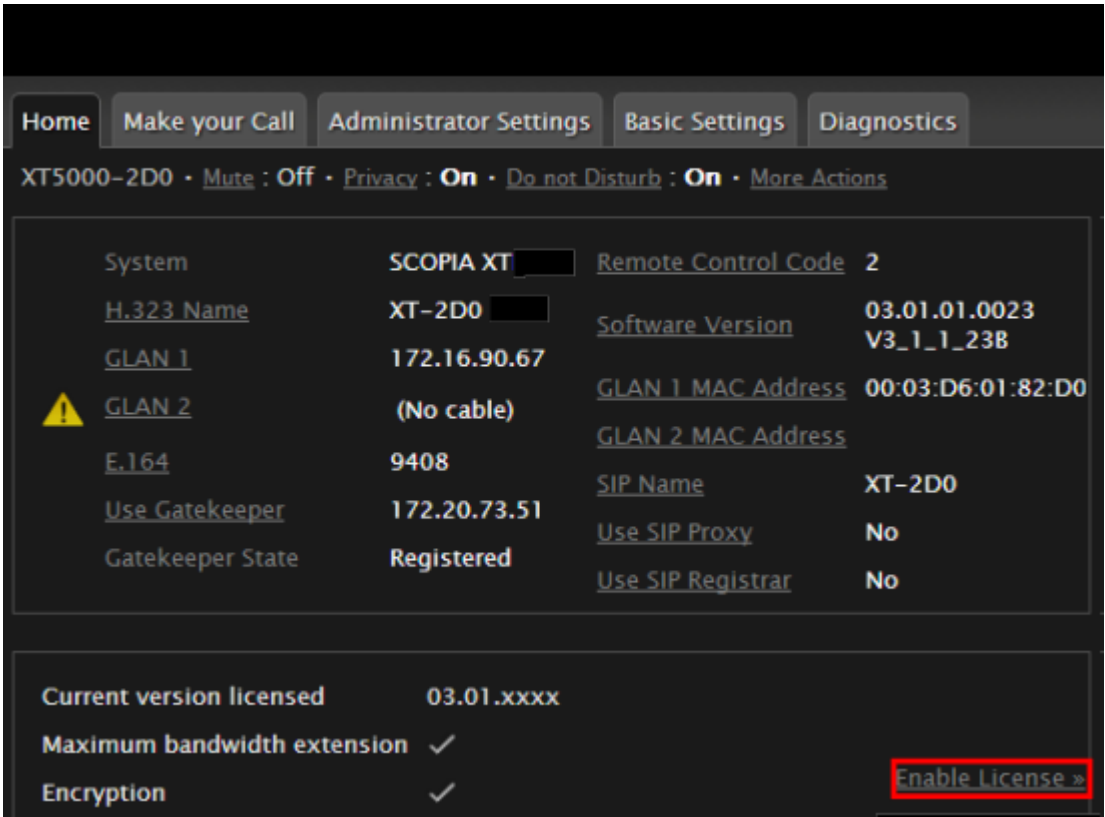


Figure 48: Accessing licenses from the Scopia XT Series home page

The **Licenses** page appears.

Licenses

Enable License

Insert license codes below and press the enable button

System	SCOPTA XT
MAC Address	00:03:D6:01:82:D0
Serial number	1203280219
Software Version	03.01.01.0023 V3_1_1_23B
Current version licensed	03.01.xxxxxx

Maximum bandwidth extension ✓

Encryption ✓

Figure 49: Enabling the license from the web interface

! Important:

The Web page shows the serial number (10-digit string) and user code. The user code corresponds to the system MAC address. These fields are not editable.

The serial number is also printed on a label affixed at the back of the XT Codec Unit.

3. Enter the active license key you received when registering the product. You can also enter license keys for optional features.
4. Select **Enable license**.

The license is automatically enabled.

! Important:

If you are enabling a second GLAN license option, the XT Codec Unit is restarted (see [Installing and Enabling Licenses which Extend System Functionality](#) on page 76 for details).

Enabling the License from the Scopia XT Series Endpoint

About this task

This procedure describes how to enable the software license of an XT Codec Unit via the endpoint's interface.

You can also enable the license from the web interface, as described in [Remotely Enabling the License from the Web Interface](#) on page 78.

If you do not yet have your license key, you can set up the system in demo mode for a period of 24 hours. After this time, you must enable your license key to use the system.

Before you begin

- Obtain a license key for the Scopia XT Series as described in [Registering the Scopia XT Series to Obtain a License Key](#) on page 75 or, if you are enabling a license option to extend Scopia XT Series functionality, see [Installing and Enabling Licenses which Extend System Functionality](#) on page 76.
- If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the Scopia XT Series's **Main** menu.
2. Select **Configure > Advanced > Utilities > Licenses**.

The **Licenses** screen appears, displaying the serial number (10-digit string) and user code. The user code corresponds to the system MAC address. These fields are not editable.

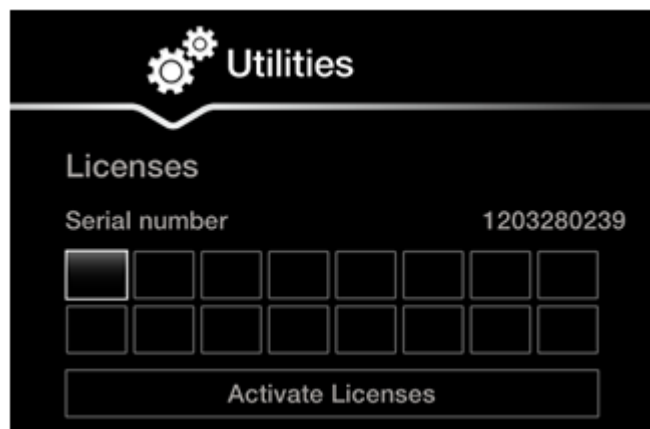


Figure 50: Activating a license

! Important:

The serial number is also printed on a label affixed at the back of the XT Codec Unit.

3. Enter the license key you received when registering the product. You can also enter license keys for optional features.
4. Select **Activate Licenses**.

The license is automatically enabled.

! Important:

If you are enabling a second GLAN license option, the XT Codec Unit is restarted (see [Installing and Enabling Licenses which Extend System Functionality](#) on page 76 for details).

Performing Basic Configuration

Before you perform basic configuration for the XT Series, your system administrator should install and activate your XT Series (for details, see the *Quick Setup Guide for Scopia XT Series*, the *Installation Guide for Scopia XT Series*, and *Safety Instructions leaflet for Scopia XT Series*).

To start using your XT Series, first define basic settings, such as the system's language, the name of this endpoint, and network settings. This is relevant for both new installations, and also after restoring default settings and re-installing software.

! Important:

Your system administrator might already have set these parameters for you and customized certain features described in this guide to suit the environment of your company. If your administrator set up PIN protection, you need the PIN number before continuing with the configuration.

You can define these settings as follows:

- Following the quick setup procedure on the XT Series endpoint.

We recommend this method to quickly start using your XT Series, since the quick setup wizard includes only the basic required settings.

- Remotely defining the settings from the XT Series web interface (see [Accessing XT Series Web Interface](#) on page 62).

Your administrator may define some settings remotely, such as for the network or gatekeeper (see [Configuring Network Settings](#) on page 117 for details). The quick setup is available from the web interface if you have not already completed the procedure from the endpoint.

You cannot remotely set the image on the monitor; this must be done from the endpoint itself.

Accessing the Quick Setup Procedure

About this task

Access the quick setup procedure to define basic settings for your Scopia XT Series, such as the system's language, the name of this endpoint, and network settings. Follow the tasks of the quick setup procedure in the order they are presented.

This is relevant for both new installations, and also after restoring default settings and re-installing software.

You can do this procedure from the endpoint itself or from the XT Series web interface.

Before you begin

Your system administrator might already have set these parameters for you. If your administrator set up PIN protection, you need the PIN number before continuing with the configuration.

Procedure

1. The quick setup wizard automatically appears the first time you access the Scopia XT Series, either by turning on the XT Codec Unit or logging in to the web interface.

If the quick setup wizard is not displayed automatically when you first turn on the XT Codec Unit, select **Configure > Quick Setup** from the Main Menu.



Figure 51: Accessing the Quick Setup

2. The quick setup wizard guides you through these basic configuration tasks:
 - [Setting the System Name and Language](#) on page 84: Define your system's name, your country, and preferred language for the interface.
 - [Adjusting the Image Position](#) on page 85: Adjust your monitor's image if necessary.

! Important:

This task is not available from the web interface. If you are configuring from the web interface, perform this procedure from the endpoint.

- [Configuring Network Settings](#) on page 87: Define your system's network settings to allow you to place and receive calls.
- [Configuring Gatekeeper Settings](#) on page 89: If your Scopia XT Series works in conjunction with a gatekeeper, configure gatekeeper-related settings.

Setting the System Name and Language

About this task

You can select the name of your XT Codec Unit, to be displayed on the monitors participating in the videoconference call (for example: **Hong-Kong**, or **9th-Floor-Room**, or **NY-Office**), and on the system's titlebar.

There is also a unicode version of the system name for users who want the name displayed on the titlebar to contain non-English characters. For more information, see [Modifying the System's Name on the Titlebar](#) on page 91.

You can also select the country in which the system is located and the language in which the system menus are displayed.

After initial setup, you can modify these settings by selecting **Configure > General** from the **Main** menu, or from the web interface as described in [Remotely Setting the System Name and Language](#) on page 90.

Before you begin

Access the quick setup wizard from the endpoint or web interface, as described in [Accessing the Quick Setup Procedure](#) on page 82.

Procedure

1. Enter the name of the Scopia XT Series in the **System Name** field. This name is also used for the SIP username and the H.323 name, which can be manually changed.

If you perform this task from the endpoint interface, use the alphanumeric keys of the XT Remote Control Unit (for more information, see [Using the XT Remote Control Unit](#) on page 68).



Figure 52: Setting Country and Language

2. Select the required country from the **Country** list. If performing this task from the endpoint interface, use the arrow keys and press **ok/menu**.
The system menu and the **Language** field automatically change to the language used in the selected country.
3. If you want to change the language of the system menus, select **Language**.
If performing this task from the endpoint interface, press **ok/menu** to display the list of languages. Scroll to the preferred language and press **ok/menu**.
4. To adjust the image on your monitor, select **Next** and continue with [Adjusting the Image Position](#) on page 85.
If performing the quick setup from the web interface, access the quick setup from the endpoint to adjust the image. This can be done at any time.

Adjusting the Image Position

About this task

If your monitor does not center the image correctly, perform this procedure. This can be done from the endpoint itself only.

Before you begin

This procedure is performed as part of the Quick Setup Wizard, after [Setting the System Name and Language](#) on page 84.

Access the quick setup wizard from the endpoint, as described in [Accessing the Quick Setup Procedure](#) on page 82.

Procedure

1. Examine the image on the monitor to decide if you need to adjust the image position.

The triangles in the top left corner and bottom right corner must be fully visible so that the white border of the triangle is fully visible on all sides.

If the image is centered correctly, skip this procedure and select **Next**.



Figure 53: Examining the image position

2. Press **1** to align the top left corner.

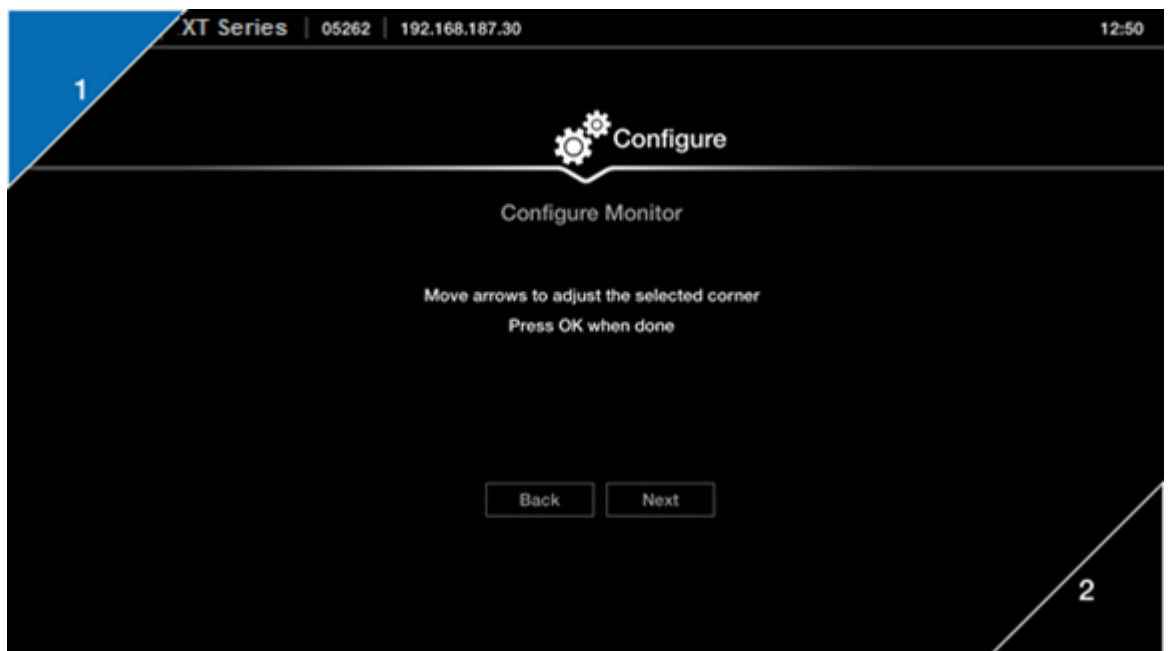


Figure 54: Adjusting the image position

3. Use the arrow keys on the XT Remote Control Unit to position the image, and then press **ok/menu**.
 4. Press **2** to align the bottom right corner.
 5. Use the arrow keys on the XT Remote Control Unit to position the image, and then press **ok/menu**.
 6. To configure network settings, select **Next** and continue with [Configuring Network Settings](#) on page 87.
-

Configuring Network Settings

About this task

This procedure describes how to set up the network settings and the IP address the system uses for placing a call.

If you are modifying the network settings after initial setup, navigate to **Configure > Network > GLAN 1** from the **Main** menu. For more information, see [Configuring GLAN Use](#) on page 117.

Before you begin

This procedure is performed as part of the Quick Setup Wizard, after [Adjusting the Image Position](#) on page 85. Consult with your network administrator to configure these fields.

Access the quick setup wizard from the endpoint or web interface, as described in [Accessing the Quick Setup Procedure](#) on page 82.

Procedure

1. Press **ok/menu** and select one of the following from the **IP Address Mode** list:
 - **Automatic:** (Default) Select this option if the system gets its IP address automatically (using DHCP).

The **IP address**, **Subnet mask**, **Gateway**, and **DNS** fields appear as read-only. See [Table 14: Configuring IP addresses](#) on page 88 for a description of these fields.

- **Manual:** Select this option if you require a static IP address. This is required, for example, if the XT Series is connected directly to the Internet, without any address translation, or when other external endpoints need to dial to this endpoint as an MCU. Enter the fields as described in [Table 14: Configuring IP addresses](#) on page 88.

To secure SIP connections using TLS certificates, your system must have a static IP address, since the system generates the certificate request using its IP address as the Common Name (CN). For more information, see [Securing Connections to the XT Series Using TLS](#) on page 140.

Figure 55: Defining IP Settings

- If you selected **Manual**, configure the following, as instructed by the system administrator:

Table 14: Configuring IP addresses

Field Name	Description
IP address	Enter the system static IP address here, used for accessing and managing the system. If the system retrieves its IP address automatically, this field displays the IP address assigned to the system.
Subnet mask	Enter the subnet mask associated with the IP address. If the system retrieves its IP address automatically, this field displays the subnet mask that has been assigned.
Gateway	Enter the default gateway static IP address. The gateway is used to route information between two subnets, for example, between the headquarters and a partner site. If the system gets its IP address automatically, this field displays the gateway IP address assigned to the system.
DNS	Enter the DNS server IP address. The DNS server in your network resolves domain names in your network and translates them into IP addresses. If the system gets its IP address automatically, this field displays the assigned DNS server IP address.

- To configure your gatekeeper's settings, select **Next** and continue with [Configuring Gatekeeper Settings](#) on page 89.

Configuring Gatekeeper Settings

About this task

A gatekeeper routes audio and video H.323 calls by resolving dial strings (H.323 alias or URI) into the IP address of an endpoint, and handles the initial connection of calls. If your Scopia XT Series works in conjunction with a gatekeeper, configure gatekeeper-related settings as described in this procedure.

This procedure completes the basic system configuration.

If you are modifying these settings after initial setup, navigate to **Configure > Network > H.323** from the **Main** menu. For more information, see [Registering the Scopia XT Series with a Gatekeeper](#) on page 125.

Before you begin

This procedure is performed as part of the basic configuration after [Configuring Network Settings](#) on page 87. Consult with your network administrator to configure these fields.

Access the quick setup wizard from the endpoint or web interface, as described in [Accessing the Quick Setup Procedure](#) on page 82.

Procedure

1. Set the **Use Gatekeeper** list to **Yes**.



Use Gatekeeper	Yes >
Mode	Automatic >
IP Address	168.168.188.78
E.164	52602

Back Next

Figure 56: Gatekeeper settings

2. Set the **Mode** list to **Manual**.

 Important:

If the gatekeeper is configured to be automatically detected by endpoints, select **Automatic** (depends on the type of gatekeeper). Consult the network administrator.

3. Enter the IP address of the gatekeeper in the **Gatekeeper IP address** field.
4. Enter the H.323 number required to dial the XT Codec Unit in the **E.164** field.
5. Select **Done**.

The basic configuration of your Scopia XT Series is complete.

Setting Basic System Information

Set the system's basic information, such as the correct local time and date. We recommend modifying the default administrator PIN to prevent users from modifying advanced settings. For more information, see the following topics:

Navigation

- [Remotely Setting the System Name and Language](#) on page 90
- [Setting the Administrator PIN Code for the XT Series](#) on page 94
- [Setting Date and Time](#) on page 95
- [Setting the Time Zone](#) on page 96
- [Remotely Setting Regional Information](#) on page 97
- [Configuring the Screen Saver to Start Automatically](#) on page 98

Remotely Setting the System Name and Language

About this task

This procedure describes how to set the name and language of the endpoint from the web interface. You can also do this as part of the quick setup from the endpoint itself, as described in [Setting the System Name and Language](#) on page 84.

You can also configure the endpoint to use alternate system name, such as the SIP username, on both the titlebar and on the monitors participating in the videoconference call, as described in [Modifying the System's Name on the Titlebar](#) on page 91.

Procedure

1. Access the name and language settings:
 - From the XT Series web interface, select **Basic Settings > Preferences > General**.
 - From the endpoint's main menu, select **Configure > General**.

General

Save

System Name

Country

Language

Screen Saver

Remote Control Code [1..99]

Local Presentation Mode

Keep Presentation Aspect Ratio

Show Advanced Settings

PIN Protect Settings

PIN Protect Renewal

[Date - Time](#)

Figure 57: Basic Settings page

2. Enter the name of the Scopia XT Series in the **System Name** field.
3. Select the required language from the **Language** list.
4. From the web interface only, select **Save**.

Modifying the System's Name on the Titlebar

About this task

This procedure describes how to configure the endpoint to use an alternate system name, such as the SIP username, on the titlebar ([Figure 58: Scopia XT Series's titlebar](#) on page 92). You can also do this as part of the quick setup from the endpoint itself, as described in [Setting the System Name and Language](#) on page 84.

The name displayed on the monitors participating in the videoconference (for example: **John-Smith**, or **9th-Floor-Room**, or **NY-Office**) is based on the protocol of the call. If you are connecting over SIP, your system's SIP username is used, while if you are connecting over H.323, your system's H.323 name is used. For more information, see [Registering the XT Series to a SIP Server](#) on page 128 and [Registering the Scopia XT Series with a Gatekeeper](#) on page 125.

System name



Figure 58: Scopia XT Series's titlebar

Procedure

1. Access the system name settings:
 - From the XT Series web interface, select **Administrator Settings > System > Location**.
 - From the endpoint's main menu, select **Configure > Advanced > System > Location**.You need to enter the PIN required to access the **Advanced** settings. The default PIN is 1234.

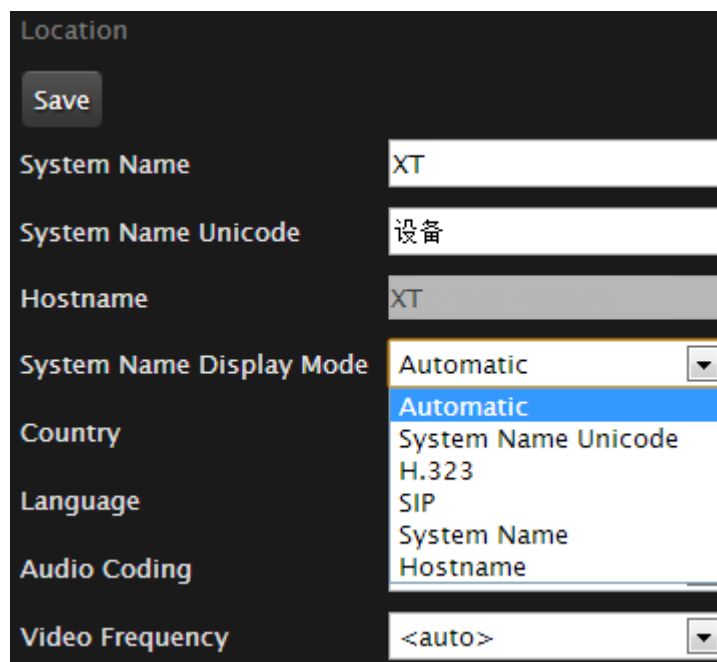


Figure 59: Selecting the system name

2. Enter the following settings:

Table 15: Setting the display name

Field	Description
System Name Display Mode	Select which name the system displays on the titlebar: • Automatic: The system selects the name to display by checking how the endpoint was registered, in the following order: – If the system is registered to a SIP registrar or proxy, the SIP username is displayed. – If the system is registered to a Gatekeeper, the H.323 name is displayed. – If the system is not registered at all, the System Name Unicode is displayed. • System Name Unicode: Select to display the contents of the System Name Unicode field, which allows non-alphanumeric characters such as Chinese or Japanese alphabets. • SIP: Select to display the SIP username, used to register your system to the SIP server. This is the same as the System Name, unless you change it manually as described in Registering the XT Series to a SIP Server on page 128. • H.323: Select to display the H.323 name, used to register your system to the gatekeeper. This is the same as the System Name, unless you change it manually as described in Registering the Scopia XT Series with a Gatekeeper on page 125. • System Name: Select to display the contents of the System Name field, which supports only alphanumeric characters. • Hostname: Select to display the contents of the system's Hostname field. This is typically the same as the System Name, unless the System Name includes characters that are not supported by the hostname standard. Invalid characters are replaced by the - character.
System Name	This field displays the initial name you entered for the system during the quick setup (as described in Setting the System Name and Language on page 84). If you selected this option from the System Name Display Mode list, you can modify the name you want to display in the titlebar (optional). You can only enter alphanumeric characters.
System Name Unicode	If you selected this option from the System Name Display Mode list, you can modify the name you want to display in the titlebar (optional). You can enter non-alphanumeric characters, such as Chinese or Japanese letters.
Hostname	You cannot modify the Hostname. This field displays the name used to register the system to the network. You may need the system's hostname, for example, if you are locating the device from a list of hostnames on an SNMP agent discovery tool. Typically, the Hostname is the same as the System Name, unless the System Name includes characters that are not supported by the hostname standard. Invalid characters are replaced by the - character.

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

Setting the Administrator PIN Code for the XT Series

About this task

You can modify the administrator PIN code required to access and modify advanced settings, such as defining camera or network settings. You can do this procedure from the endpoint itself or from the XT Series web interface.

The default PIN is **1234**. We recommend that you change the administrator PIN when starting the system configuration to prevent users from changing settings by mistake.

You can also set a user PIN code to access basic settings, such as the language displayed on the interface, as described in *Administrator Guide for Scopia XT Series*. To modify the web username and password for the XT Series, see *Administrator Guide for Scopia XT Series*.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

To modify the PIN, you must be connected via HTTPS (see [Enabling Remote Management on the Scopia XT Series](#) on page 63).

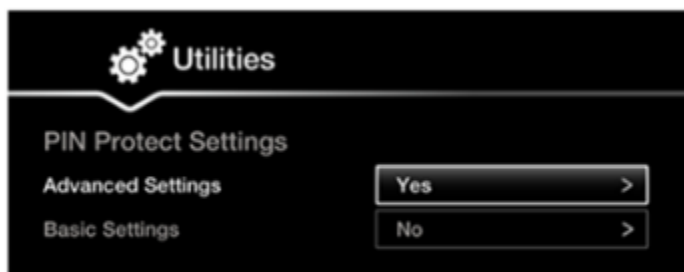
Procedure

1. Access the PIN settings, as follows:

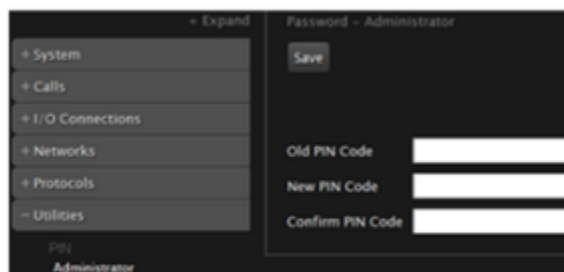
- From the endpoint's main menu, select **Configure > Advanced > Utilities > PIN Protect Settings > Advanced Settings > Choose a new PIN Code**.

You need to enter the PIN required to access the **Advanced** settings. The default PIN is 1234.

- From the XT Series web interface, select **Administrator Settings > Utilities > PIN Protect Settings > Administrator**.



Configuring from Endpoint



Configuring from Web Interface

Figure 60: Modifying the administrator PIN

2. Enter the current PIN code required to access the **Advanced** settings in the **Old PIN Code** field. The default PIN is 1234.
3. Enter your new 4 digit PIN code.

From the web interface only, re-enter your new PIN in the **Confirm PIN Code** field.

4. Save your changes as follows:
 - From the endpoint, select **Done**.
 - From the web interface, select **Save**.

Use this PIN the next time you are accessing advanced settings.

Setting Date and Time

About this task

You can set the date and time from either the endpoint or the web interface.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the date and time settings as follows:
 - From the XT Series web interface, select **Administrator Settings > System > Date & Time > General**.
 - From the endpoint's main menu, select **Configure > Advanced > System > Date & Time > General**.

You need to enter the PIN required to access the **Advanced** settings. The default PIN is 1234.

2. Set the date and time, as described in [Table 16: Configuring date and time settings](#) on page 95.

Important:

If you configure set **Internet time** to **Yes**, you cannot modify the date and time fields.

Table 16: Configuring date and time settings

Field Name	Description
Day	Enter the date.
Month	Enter the month.
Year	Enter the year.
Hour	Enter the hour.
Minutes	Enter the minutes.
Internet time	Select Yes to synchronize the system clock with the network clock, thus allowing you to align devices connected to the Internet using NTP.

Field Name	Description
Use Default NTP Server	If your organization uses an external Network Time Protocol (NTP) server for synchronizing the system clock, select Yes . If your organization uses one or two internal NTP servers for that purpose, select No and enter the server IP address in fields Server 1 and/or Server 2 .
Refresh time	Indicates the period of time after which the system contacts the NTP server to refresh the clock.

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

Setting the Time Zone

About this task

You can set the time zone from your endpoint or the Scopia XT Series web interface.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

- Access the time zone settings as follows:
 - From the XT Series web interface, select **Administrator Settings > System > Date & Time > Time Zone**.
 - From the endpoint's main menu, select **Configure > Advanced > System > Date & Time > Time Zone**.
You need to enter the PIN required to access the **Advanced** settings. The default PIN is 1234.
- Configure settings as described in [Table 17: Configuring time zone related settings](#) on page 97.

Figure 61: Setting the time zone

Table 17: Configuring time zone related settings

Field Name	Description
Time zone list	Select the time zone to which the system belongs.
Enable daylight time	Set the daylight or summer time field to Yes or No according to the current daylight-saving status of your time zone.
Start (dd/mm)	Set the day and month to indicate when daylight saving times start.
Stop (dd/mm)	Set the day and month to indicate when daylight saving times end.

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

Remotely Setting Regional Information

About this task

You must configure the region-related settings: the country and language. You also need to configure audio coding and video frequency, because your video network depends on the local infrastructure. The system suggests the optimal values for audio coding and video frequency when you enter the country value.

You may have set some of these fields in the Quick Setup procedure, since this is part of the basic required settings (for details, see [Accessing the Quick Setup Procedure](#) on page 82). You can modify these settings at any time from the endpoint or the web interface.

Procedure

- Access the XT Series web interface, as described in [Accessing XT Series Web Interface](#) on page 62.
- Select **Administrator Settings > System > Location**.

Figure 62: Setting regional information

3. Define regional settings as described in [Table 18: Configuring regional information](#) on page 98.

Table 18: Configuring regional information

Field Name	Description
System name	Enter the name that will appear in the local endpoint interface and in the remote endpoint interface (if connected).
Country	Select the country in which the local system is located. Once the country is selected, the other fields are populated automatically.
Language	Select the language used in the XT Series endpoint's interface.
Audio coding	Select the European or US coding.
Video frequency	The video refresh frequency depends on the country, and may assume the values of 50Hz or 60Hz . You can select the video frequency automatically or manually. If set to automatic, the system assigns the value depending upon the selected country. In Japan, the frequency depends on the country area (east or west); thus in Japan the system administrator must select manually the correct value related to the geographic location.

4. Select **Save**.

Configuring the Screen Saver to Start Automatically

About this task

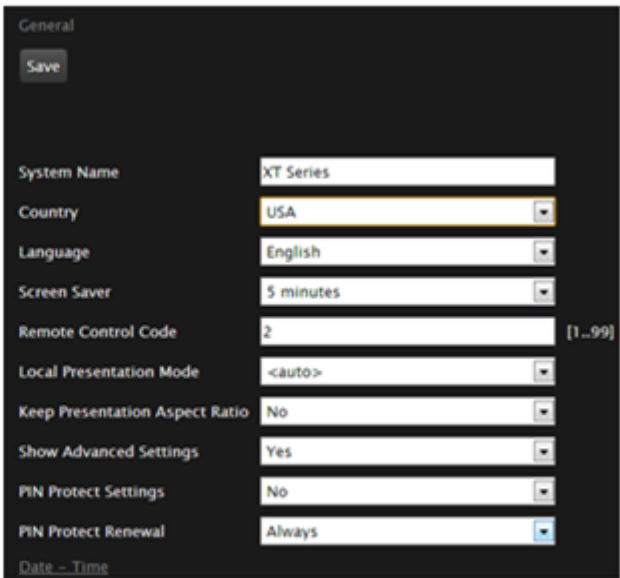
The screen saver helps to protect your monitor from burn-in without switching it off. This can be useful in situations when you stop using your Scopia XT Series for a relatively short period of time. You can do this procedure from the endpoint itself or from the XT Series web interface.

Procedure

1. Access the screen saver settings as follows:
 - From the endpoint's main menu, select **Configure > General**.
 - From the XT Series web interface, select the **Basic Settings** tab.



From the endpoint interface



From the web interface

Figure 63: Configuring screen saver settings

2. Select **Yes** from the **Screen Saver** list.
3. Set the time after which the screen saver automatically starts on the display in the **Minutes** field.
4. From the web interface only, select **Save**.

Configuring Video Connections

There are a number of settings which affect the way the camera accepts input and the way the monitors display video.

Navigation

- [Configuring the Camera Connection](#) on page 100
- [Setting up the Monitor Display Modes](#) on page 105

Configuring the Camera Connection

About this task

You configure the connection depending on the type of camera and its functionality. This includes configuring the Scopia XT Camera Switch. You can do this procedure from the endpoint itself or from the XT Series web interface.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

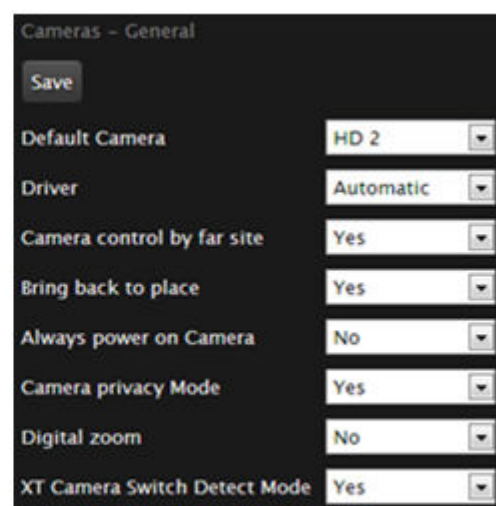
Connect the video equipment, as described in [Connecting the Video Equipment to the Scopia XT Series](#) on page 47.

Procedure

1. Access the camera settings as follows:
 - From the endpoint's main menu, select **Configure > Advanced > I/O connections > Cameras > General**.
 - From the XT Series web interface, select **Administrator settings > I/O connections > Cameras > General**.



From the endpoint interface



From the web interface

Figure 64: Configuring general camera settings from the web interface

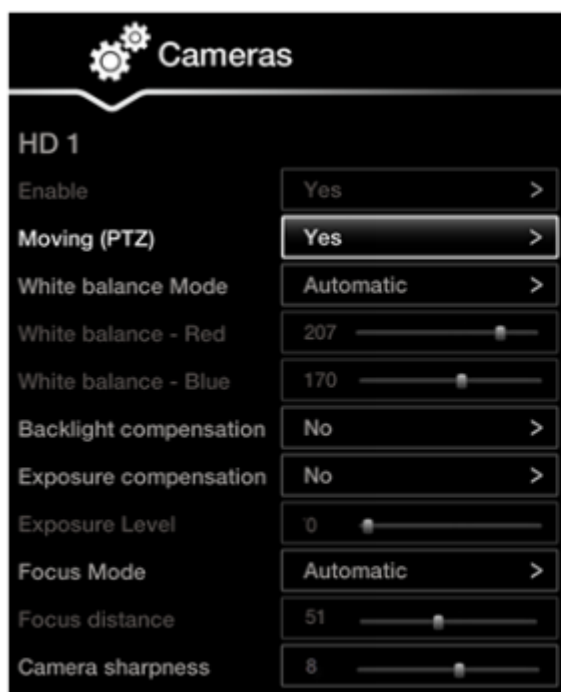
2. Configure the camera connection as described in [Table 19: Configuring general camera settings](#) on page 102:

Table 19: Configuring general camera settings

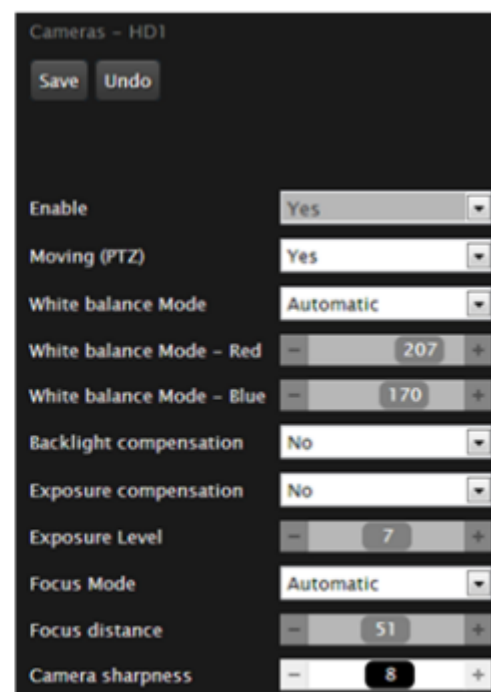
Field Name	Description
Default camera	Select the port of the XT Codec Unit which you connected the default camera, which is automatically activated when the system powers up.  Figure 65: Video inputs of the XT Codec Unit • HD1: Select if you connected the default camera to the HDMI input of the XT Codec Unit. This is the most common configuration. If you connected multiple cameras using the Scopia XT Camera Switch, select the HD port of the Scopia XT Camera Switch to which you connected the default camera, from HD1- HD4. • USB: Select if you connected the default camera to the USB input of the XT Codec Unit. • DVI: Select if you connected the default camera to the DVI input of the XT Codec Unit. For more information about connecting your camera to the XT Codec Unit, see Connecting the Video Equipment to the Scopia XT Series on page 47. ! Important: When using the Scopia XT Camera Switch, do not connect cameras to ports HD1 and USB on the XT Codec Unit, as these are used to connect the Scopia XT Camera Switch itself. For more information, see Connecting the Optional Scopia XT Camera Switch on page 53.
Driver	Select the camera driver for the connected camera. Automatic allows automatic identification of the correct driver at system start up. Automatic detection for HD camera is available only if the camera is connected using a VISCA Cross cable.
Camera control by far site	Enables/disable control of my camera(s) by the remote endpoint.
Bring back to place	If enabled, the system stores camera positions when the camera is switched off, and restores this position the next time the camera is switched on.

Field Name	Description
Always power on Camera	Ensures the camera does not automatically power off, enabling the system to be switched on via remote control, if the camera has an infrared receiver.
Camera privacy Mode	Places the camera in a sleep position, with the lens facing down and to the left, when the system is in screen saver or privacy mode (default).
Digital zoom	Enables digital zoom for cameras equipped with this feature.
XT Camera Switch Detect Mode	Enables the Scopia XT Camera Switch if you are using this device to control and include more than one camera in your video. Multiple cameras are typically used for larger meeting rooms or auditoriums. For more information, see Connecting the Optional Scopia XT Camera Switch on page 53.

- From the web interface only, select **Save**.
- Select the port to which you connected the camera you are configuring, such as **HD1**:
 - From the endpoint's main menu, select **Configure > Advanced > I/O connections > Cameras**.
 - From the XT Series web interface, select **Administrator settings > I/O connections > Cameras**.



Configuring from endpoint



Configuring from web interface

Figure 66: Configuring the camera settings from the web interface

- Define the following camera settings:

Table 20: Configuring advanced camera settings

Field Name	Description
Enable	Select Yes to enable this camera. Otherwise, you cannot use the video input from this camera. If you connected multiple cameras via the Scopia XT Camera Switch, enable each camera. You cannot disable the default camera.
Moving (PTZ)	Enable the camera pan, tilt and zoom functionality if it is supported by your camera, such as the XT Premium Camera. The camera must be connected via a VISCA cable, as described in Connecting Cameras for Controlling the Optional XT Premium Camera with the XT Remote Control Unit on page 51. Disable if you connected DVD devices or non-PTZ cameras.
White balance mode	This is not relevant for USB cameras. If the lighting in the room is not standard, you can adjust the colors of the image sent by the camera: • To allow the camera to automatically adjust colors to room lighting, set to Automatic. • To set the camera to adjust colors based on natural sunlight, select Outdoor. This could be used, for example, in a room with many large windows. • To set the camera to adjust colors based on artificial light, select Indoor. • To calibrate colors manually, set to Manual, and adjust the Red and Blue sliders. • To calibrate color temperature so that the image does not have blue or red color undertones, set to Customize.
Backlight compensation	Select to counteract silhouetting of subjects when the backlighting is excessive.
Exposure compensation	This is not relevant for USB cameras. If the lighting in the room is excessive, enable and define exposure compensation to manually reduce light intake.
Focus mode	Set the camera focus: • To set the camera focus automatically, select Automatic. • To adjust the camera focus manually, select Manual, and set the distance from the camera to the table.
Camera sharpness	Adjust the sharpness of the image from your camera.

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

7. Configure the settings described in [Table 20: Configuring advanced camera settings](#) on page 104 for each camera you are using.

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

Setting up the Monitor Display Modes

About this task

You can configure the monitor from the XT Series endpoint or web interface by:

- Setting its resolution
- Configuring the system to work with a single monitor or two monitors side-by-side.
- Modify the default video layout to define whether the user sees two or three video streams on the monitor(s): local video, remote video, and a data presentation.

For more information about video layouts, see *Scopia XT Series User Guide*.

! Important:

If your monitor crops the edges of the image shown in their displays, adjust it as described in [Resolving Monitor Display Problems](#) on page 158.

! Important:

You can return to the Default Auto settings at any time by pressing the **Layouts**  key and then **0** on the XT Remote Control Unit.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the monitor settings:
 - From the endpoint's main menu, select **Configure > Advanced > I/O connections > Monitor**.
 - From the XT Series web interface, select **Administrator settings > I/O connections > Monitor**.
2. Configure the general monitor settings as follows:
 - a. Select **General** to access the general settings.



Figure 67: Configuring the general monitor settings from the web interface

b. Configure the general settings:

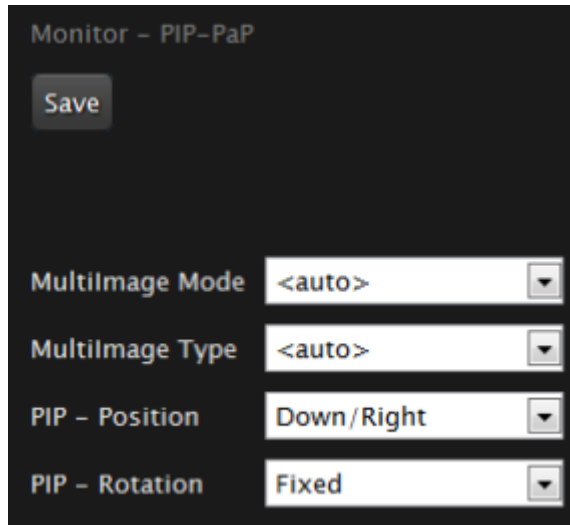
Table 21: Configuring general monitor settings

Field Name	Description
Number of monitors	Specifies the number of monitors connected to the XT Codec Unit. In a dual configuration, the selected layout is depicted as two pictures representing the two connected displays. • <auto> - The system automatically detects the number of connected monitors (recommended). • HD1/HD2 - When a single monitor is connected to the HD1/HD2 output socket of the XT Codec Unit. If two monitors are connected with this setting, the second monitor will appear as a black screen. • HD1 (Menu & Video Rx) + HD2 (Present) - Dual monitor configuration, where the system menus and remote video are displayed on the main monitor, while PC content is shown on the auxiliary monitor. This is the default mode with two connected monitors set to <auto>. • HD1 (Menu & Present) + HD2 (Video Rx) - Dual monitor configuration, where the system menus and PC content are displayed on the main monitor, while remote video is shown on the auxiliary monitor. • HD1 (Present) + HD2 (Menu & Video Rx) - Dual monitor configuration, where the system menus and Remote Video are displayed on the auxiliary monitor, while PC content is shown on the main monitor. • HD1 (Video Rx) + HD2 (Menu & Present) - Dual monitor configuration, where the system menus and PC content are displayed on the auxiliary monitor, while remote video is shown on the main monitor.
Resolution HD1/HD2	Defines how the XT Codec Unit sets the resolution of the connected main monitor (HD1)/auxiliary monitor (HD2). • <auto> - Sets 1080p as the default settings for both monitors. • 1080p - If the monitor supports 1080p, this setting will always keep the monitor resolution at 1080p. • 720p - If the monitor supports 720p, this setting will always keep the monitor resolution at 720p, even if the received resolution is higher.

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

3. Configure the monitor to show more than one video stream:

a. Select **PIP-PaP** under **Monitor**.



Monitor - PIP-PaP

Save

Multimage Mode <auto>

Multimage Type <auto>

PIP - Position Down/Right

PIP - Rotation Fixed

Figure 68: Setting PIP-PaP option

- b. Configure the PiP and PaP options as described in [Table 22: Configuring PIP-PaP option](#) on page 109.

The PiP (Picture In Picture) view shows a video image in the main screen, with an additional smaller image overlapping in the corner. The PaP (Picture and Picture) view shows two images of the same size, presented side by side.

For more information about video layouts, see *Scopia XT Series User Guide*.

Table 22: Configuring PIP-PaP option

Field Name	Description
Multi Image Mode	Sets PIP and PaP activation, depending on the number of video streams available. • auto: PIP and PaP are enabled only when needed. This occurs when the number of video streams is greater than the number of available monitors. The order of the video streams is set automatically, with precedence to the remote video streams. • On: PIP and PaP are enabled if at least two video streams are available. If there is one video stream, the image shows in full screen (for example, when the system is not connected). • Off: PIP and PaP are disabled.  Important: When you are using two monitors, PIP can be forced only if there are at least three different video streams.
Multi Image Type	Sets the PIP and PaP functions. • auto: Both PIP, PaP and PoP functions are enabled. Press the Layout  key to switch between PIP, PaP and PoP. • PIP: Only PIP is enabled. • PaP: Only PaP is enabled. • PoP: Only PoP is enabled.
PIP - Position	Sets the position of the small image on the monitor: upper left, upper right, lower left, lower right.
PIP - Rotation	Enables/disables image rotation and controls the direction in which the image rotates. Press the Layout  key to activate image rotation (if enabled). • Fixed: The image does not change position. • Clockwise: Image rotates clockwise to change position. • Counterclockwise: Image rotates counterclockwise to change position.

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

Configuring Audio Connections

Part of the initial configuration is ensuring the microphones and speakers are set up correctly, and that there is no noticeable echo across connections in a call or conference. The settings are detailed in these sections:

Navigation

- [Configuring the Microphone](#) on page 110
- [Configuring Analog Audio Connections](#) on page 111
- [Configuring Audio Outputs](#) on page 113
- [Configuring the Echo Cancellor](#) on page 116

Configuring the Microphone

About this task

Typically, you connect the Microphone Pod, which puts the focus on the speaker while isolating background noise. Alternatively, if you connected a USB camera, you can use the built-in microphone (see [Connecting the Optional USB Camera](#) on page 49 for details).

In larger rooms, use a second Microphone Pod.

Important:

A second Microphone Pod is only available for selected models.

Before you begin

Connect the microphone you are using, either the Microphone Pod or the microphone embedded in the USB camera, as described in [Setting up the Scopia XT Series](#) on page 35. To plan your audio setup, see [Deciding on the Audio Setup for the Scopia XT Series](#) on page 39.

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the microphone settings:
 - From the endpoint's main menu, select **Configure > Advanced > I/O connections > Audio - Input**.
 - From the XT Series web interface, select **Administrator settings > I/O connections > Audio - Input**.
2. Select the microphone you are using, such as **POD1** or **USB**.
If you are using a second Microphone Pod, select **POD2**.

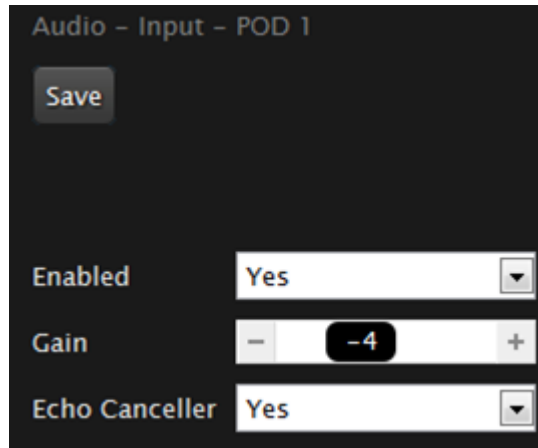


Figure 69: Configuring the microphone settings from the web interface

3. Set the fields as described in [Table 23: Configuring the microphone connection](#) on page 111.

Table 23: Configuring the microphone connection

Field Name	Description
Enabled	Enables/disables the microphone.
Gain	Use the slider to adjust the fixed Gain Control, setting the voice signal to the desired level. The AGC reduces the volume if the audio is strong and raises the volume if the audio is weak.
Echo canceller	Enable the echo canceller when working with an external microphone system that does not contain echo cancellation. If enabled check the field settings in Configuring the Echo Canceller on page 116, and configure if required. Disable this setting when working with an external mixer that handles echo cancellation.

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

Configuring Analog Audio Connections

About this task

You must perform this procedure if you are using the analog audio connections:



Figure 70: The analog/optical audio port on the XT Series

Before you begin

Connect the analog audio equipment as described in [Connecting an Analog Sound System](#) on page 45.

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the Microphone Pod settings:
 - From the endpoint's main menu, select **Configure > Advanced > I/O connections > Audio - Input > Analog**.
 - From the XT Series web interface, select **Administrator settings > I/O connections > Audio - Input > Analog**.
2. Set the fields as required.

Table 24: Configuring analog audio connections

Field Name	Description
Enabled	Enables/disables this audio input.
Gain	Set the voice signal to the desired level by using the slider.
Echo canceller	Enable the echo canceller when working with an external microphone system that does not contain echo cancellation. To configure the echo cancellation settings, see Configuring the Echo Canceller on page 116. To hear the audio also locally, see Configuring Audio Outputs on page 113. Disable this setting if you have an external mixer that handles its own echo cancellation or you are connecting to a computer.
Audio selection	Choose one of these settings: • Analog associated with DVI - Select this option when a PC is connected to the XT Codec Unit's DVI-I Input port and you want to hear the PC's audio only when you selected the DVI video input as your main video source or as the presentation. • Analog always - The audio coming from analog connection is always sent to remote participants, regardless of which video is selected.

Field Name	Description
Type	In a standalone microphone, power and audio can be supplied over the same wires; power is drawn from an external source but without a separate power supply. This is called phantom power. A built-in microphone, such as in a computer or the Scopia XT Executive, does not need phantom power since it gets power from the device itself, using the computer as its external power source, for example. When configuring these settings, verify the audio equipment connection method: a balanced line reduces external noise interference and allows to use very long cables. Choose one of these settings: • Line - Select this option for an analog audio input without phantom power. Then set the Mode field to Stereo or Mono input (see below). • Microphone - Select this option if the analog audio is coming from an analog balanced microphone that is using phantom power.
Mode	You can configure this field if you selected the Line setting. Choose one of these options: • Stereo - The input is an L/R stereo unbalanced line without phantom power. • Mono - The input is a mono balanced line without phantom power.

3. From the web interface only, select **Save**.
4. (Optional) If you selected **Analog associated with DVI** as the **Audio selection** (see [Table 24: Configuring analog audio connections](#) on page 112), verify the DVI video input is enabled as described below.

The remote endpoint hears the computer's audio.

- a. Access the DVI settings as follows:
 - From the endpoint's main menu, select **Configure > Advanced > I/O Connections > Cameras > DVI**.
 - From the XT Series web interface, select **Administrator Settings > I/O Connections > Cameras > DVI**.
- b. Verify that **Enabled** is set to **Yes**.

Configuring Audio Outputs

About this task

The Scopia XT Series allows you to combine audio from various inputs such as the XT Digital Microphone Array Pod, and route it to available audio outputs. The possible combination of inputs and

outputs forms a matrix, which is depicted in the Scopia XT Series system menus ([Figure 71: Defining the routing of the audio outputs](#) on page 115).

Sources of audio input include the following:

- XT Digital Microphone Array Pods
- Analog audio input
- Remote audio coming from other participants in the videoconference

Important:

The audio from the analog inputs and microphones can be mixed and echo-cancelled, and routed to one or more of the following audio outputs:

- Monitor speakers or other device connected to the HD1 port with an HDMI cable.
- The analog output or the analog/optical port connected to a speaker or a device like a recorder.

A typical audio configuration, depicted in [Figure 71: Defining the routing of the audio outputs](#) on page 115, would be:

- Route the remote audio to the speakers of one of the monitors (HD1), so you can hear the other conference participants.
- Typically, you do not route the local microphone to a speaker, since you can hear your own voices in the room. This will avoid feedback loops.
- If you are showing a presentation on your computer and it includes sound, route the sound of the computer to the analog input connector.

Before you begin

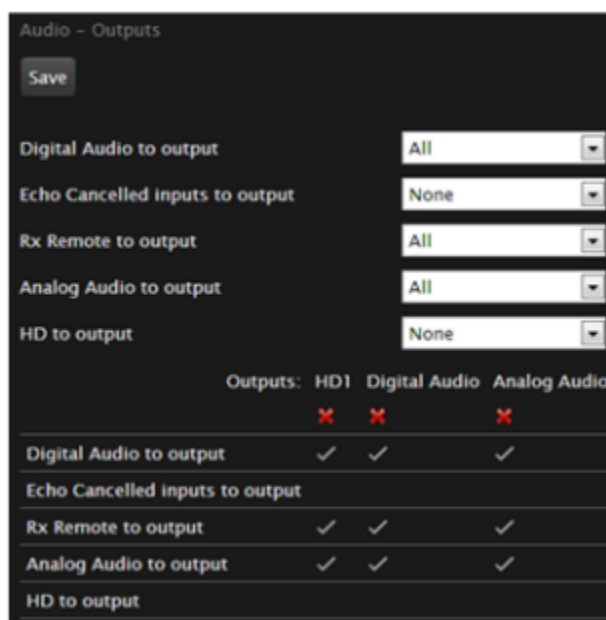
If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the audio output settings as follows:
 - From the endpoint's main menu, select **Configure > Advanced > I/O connections > Audio - Outputs > General**.
 - From the XT Series web interface, select **Administrator settings > I/O connections > Audio - Outputs > General**.



Configuring from the Endpoint



Configuring from the Web Interface

Figure 71: Defining the routing of the audio outputs

- Set the fields as required.

Table 25: Configuring audio output settings

Field Name	Description
Digital Audio to output	If enabled, it routes the digital audio input port to one or more of the system's audio output channels: HD1, digital audio and digital analog or all of the above.
Echo Cancelled inputs to output	This setting is disabled by default, to avoid echo effects and feedback loops when a monitor speaker is used. If enabled, sends the echo cancelled input from the microphones to one of the system's audio output channels: HD1, digital audio or analog output.
Rx remote to output	If enabled, sends the remote audio of other conference participants to one or more of the system's audio output channels: HD1, digital audio or analog output.
Analog to output	If enabled, it routes the analog input port to one or more of the system's audio output channels: HD1, digital audio or analog output.

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

Configuring the Echo Canceller

About this task

If your Scopia XT Series works with an external microphone system that does not contain echo cancellation, perform this procedure to cancel echo.

Before you begin

Enable echo cancellation as described in [Configuring the Microphone](#) on page 110.

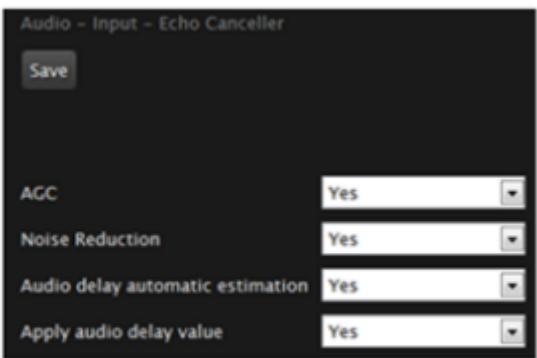
If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the echo canceller settings as follows:
 - From the endpoint's main menu, select **Configure > Advanced > I/O connections > Echo Canceller**.
 - From the XT Series web interface, select **Administrator settings > I/O connections > Echo Canceller**.



Configuring from Endpoint



Configuring from Web Interface

Figure 72: Configuring the Echo Canceller

2. Set the fields as required.

Table 26: Configuring echo canceller related settings

Field Name	Description
AGC	Enables/disables Automatic Gain Control (AGC), which is used to adjust the volume. The AGC reduces the volume if the audio is strong and raises when it is weak.
Noise reduction	Enables/disables reduction of ambient noise in a conference room (e.g.: coughing, paper rustling, etc.).

Field Name	Description
Audio delay automatic estimation	An HDMI monitor might insert delay in the audio, causing an echo. If you set this field to Yes , the XT Codec Unit improves its echo canceller performance automatically. We recommend this setting when you connect a new monitor to the XT Codec Unit. If you set this field to No , you can generate the audio delay manually and train the echo canceller to use the resulting audio for better performance.
Audio delay	Enables/disables the use of the audio delay value calculated when activating audio delay automatic estimation.

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

Configuring Network Settings

Part of the initial configuration is ensuring the network is properly set up. The settings are detailed in these sections:

Navigation

- [Configuring GLAN Use](#) on page 117
- [Registering the Scopia XT Series with a Gatekeeper](#) on page 125
- [Registering the XT Series to a SIP Server](#) on page 128
- [Configuring Call Settings](#) on page 131
- [Configuring Scopia XT Series Endpoints to use an LDAP Directory](#) on page 135

Configuring GLAN Use

You can configure GLAN use for Scopia XT Series.

Before you begin to configure GLAN use, you must prepare your network for videoconferencing. Consult your network administrator for more information.

These sections describe step-by-step procedures to configure settings for GLAN use:

Navigation

- [Configuring IP Addresses](#) on page 118
- [Configuring Network Connectivity](#) on page 120
- [Enabling NAT and Firewall Traversal with Scopia XT Series](#) on page 122
- [Determining the Priority of Audio versus Video Quality](#) on page 124

Configuring IP Addresses

About this task

To place calls, the system supports either IPv4-only mode, or dual IPv4 and IPv6 mode.

HTTP, SNMP, and AT commands management occurs in IPv4 only, even if you set the system to support dual mode. You can configure the IPv4 address manually or automatically.

Media streams in the same conference can be a mixture of IPv4 and IPv6.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the general network settings, as follows:
 - From the XT Series web interface, select **Administrator Settings > Networks > Preferences > General**.
 - From the endpoint's main menu, select **Configure > Network**.

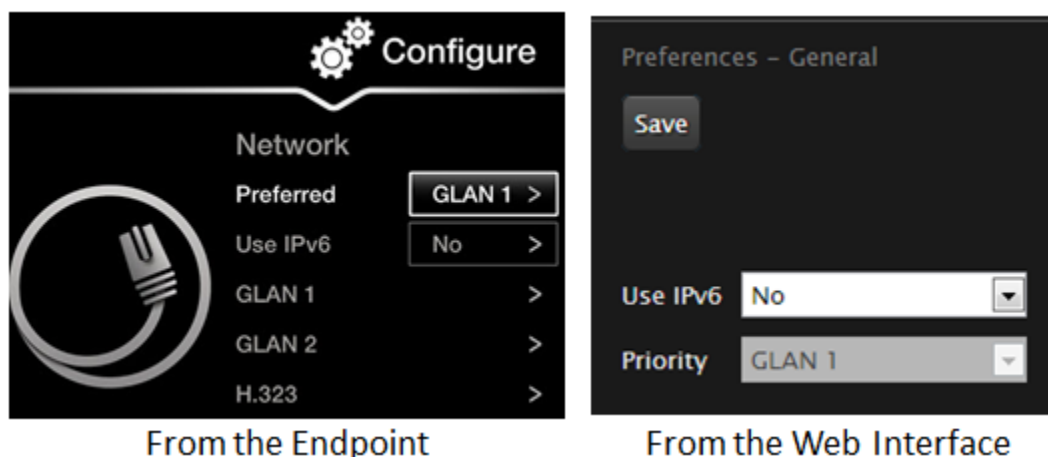


Figure 73: Enabling IPv6 mode

2. Set the **Use IPv6** field to enable or disable IPv6 support.
3. From the web interface only, select **Save**.
4. Access the IP address settings, as follows:
 - From the endpoint, select either **GLAN 1** or **GLAN 2**.
 - From the web interface, select **Addresses** under **GLAN 1** or **GLAN 2**.

! Important:

GLAN2 is available in selected models only. For more information, refer to [Comparing Between Scopia XT Series Models](#) on page 12 and [Installing and Enabling Licenses which Extend System Functionality](#) on page 76.

Figure 74: Configuring IP addresses from the web interface

5. Set the fields as described in [Table 27: Configuring IP addresses](#) on page 119.

Table 27: Configuring IP addresses

Field Name	Description
MAC Address	This setting cannot be changed.
Automatic IP Address	Set to Yes (default) if the system gets its IP address automatically. Set to No if you must set up a public IP address in the IP address field. The other fields in this page become configurable. This is required, for example, if the XT Series is connected directly to the Internet, without any address translation, or when other external endpoints need to dial to this endpoint as an MCU. To secure SIP connections using TLS certificates, your system must have a static IP address, since the system generates the certificate request using its IP address as the Common Name (CN). For more information, see Securing Connections to the XT Series Using TLS on page 140.
IP Address	If the system gets its IP address automatically, indicates the IP address assigned to the system. Otherwise, enter the system static IP address here.

Field Name	Description
Subnet Mask	If the system gets its IP address automatically, this field indicates the subnet mask assigned to the system. If you entered the system's IP address manually, type the subnet mask.
Gateway IP Address	If the system gets its IP address automatically, this field indicates the gateway IP address assigned to the system. If you entered the system's IP address manually, type the gateway IP address.
DNS Server IP Address	If the system gets its IP address automatically, this field indicates the DNS server IP address assigned to the system. If you entered the system's IP address manually, type the DNS server IP address.

6. From the web interface only, select **Save**.
7. If you secured your XT Series using TLS certificated and you now modified the IP address, you must generate the CSR again, as described in [Generating a Certificate Signing Request for XT Series](#) on page 141.

Configuring Network Connectivity

About this task

This procedure describes how to configure the GLAN1 and GLAN2 ports. The GLAN2 port is available only if it is enabled, depending on your model. For more information, refer to [Installing and Enabling Licenses which Extend System Functionality](#) on page 76.

You may want to enable both GLAN1 and GLAN2, for example, to use one network connection for control and another for videoconferences.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the network settings as follows:
 - From the XT Series web interface, select **Administrator Settings > Networks**.
 - From the endpoint's main menu, select **Configure > Advanced > Networks**.
2. Select **Parameters** under **GLAN**.

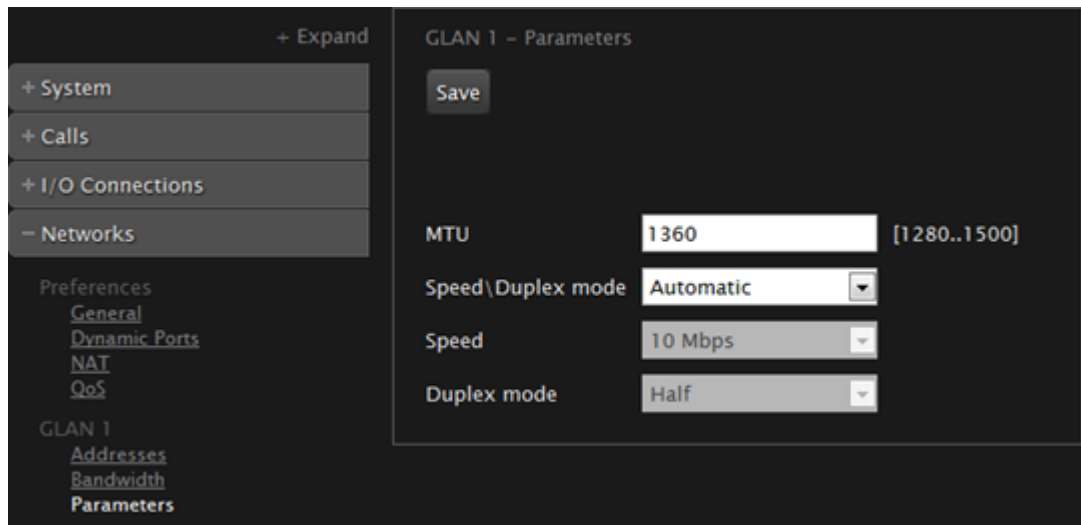


Figure 75: Configuring the GLAN parameters from the web interface

3. Set the field as described in [Table 28: Configuring network connectivity](#) on page 121.
To avoid connectivity issues, match these settings to the equivalent settings in the network.

Table 28: Configuring network connectivity

Field Name	Setting
MTU	Sets the maximum size of each IP packet the XT Codec Unit can send to the network. If the system or the remote endpoint transmits IP packets larger than the configured MTU size, they are dropped or fragmented. To avoid packet loss or fragmentation, decrease MTU. If packets are smaller than the configured MTU size, increase MTU. The maximum and minimum values you enter in this field depend on the mode selected for placing calls: IPv4 or IPv6. (These are configured in Configuring IP Addresses on page 118. Both for IPv4 and IPv6 MTU size is set by default to 1360 octets. You can set the MTU size to these ranges: • The minimum allowed value for IPv4 is 576 octets. • The minimum allowed value or IPv6 is 1280 octets. • The maximum allowed value for both is 1500 octets.
Speed/Duplex mode	Set the speed and transition mode as follows: • Automatic: The XT Codec Unit selects the Ethernet speed and transmission mode. We recommend this default mode. • Auto - up to 100/Full, Auto - up to 100/Half, Auto - up to 10/Full, Auto - up to 10/Half: If necessary for your network requirements, select one of these semi-automatic modes. The XT Codec Unit selects the Ethernet speed and transmission mode according to the specified values. • Manual: You must configure speed and transmission mode and know the network and remote endpoints requirements.

Field Name	Setting
Speed	Select the suitable Ethernet speed: 10, 100, or 1000 MBPs for GLAN. This field is read-only if you selected Automatic for Speed/Duplex mode .
Duplex mode	Select the data transmission mode that is defined for your network router or switch, either duplex or half-duplex mode. This field is read-only if you selected Automatic for Speed/Duplex mode .

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

Enabling NAT and Firewall Traversal with Scopia XT Series

About this task

Scopia XT Series fully supports NAT and firewall traversal, enabling you to place the unit behind a NAT router or firewall and connect with other endpoints seamlessly.

Perform this procedure to enable your Scopia XT Series to traverse NAT and firewall. For an explanation about NAT and firewall approaches, as well as examples of deployments, see [Planning NAT and Firewall Traversal with Scopia XT Series](#) on page 22.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the network settings as follows:
 - From the XT Series web interface, select **Administrator Settings > Networks > Preferences > NAT**.
 - From the endpoint's main menu, select **Configure > Advanced > Networks > Preferences > NAT**.

Figure 76: Configuring NAT traversal settings from the web interface

2. Set the fields as described in [Table 29: Configuring NAT-related settings](#) on page 123.

Table 29: Configuring NAT-related settings

Field Name	Description
NAT Traversal	Set to Yes to allow the system to be located behind a firewall/NAT. Set to No if the system is not located behind a firewall/NAT, but has a public IP address.
NAT Discovery	Manual method of setting the system's firewall/NAT public IP address. Enter the Public IP address for that setting. HTTP discovery - This method uses a Radvision HTTP server to discover the presence of a firewall/NAT and its public IP address (requires the endpoint to have internet access). STUN discovery - This method uses a public STUN server to discover the presence of a firewall/NAT and its public IP address. This is the suggested method.
Public IP Address	Firewall public IP address. The field is enabled if NAT Traversal is set to Yes .
Refresh Time (sec)	Sets the opening time, in seconds of the pinhole inside the firewall. Also used by H.460 as TTL (Time To Live) of registration requests.

! Important:

Set the ports in accordance with the settings detailed in [Configuring the TCP or UDP Port Range on the Scopia XT Series](#) on page 30.

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

Determining the Priority of Audio versus Video Quality

About this task

Quality of Service determines how your network handles IP packets sent to your system during a video conference. For example, you can set a higher priority to audio packets, so that when there is an issue with packet loss, audio quality is maintained over video.

Bandwidth and video quality settings also contribute to call quality. If you experience problems with call quality, refer to the [Troubleshooting the Scopia XT Series](#) on page 152.

Before you begin

Consult with your network administrator for more information about configuring Quality of Service.

Important:

For detailed information on QoS based on TOS, refer to RFC-1439.

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the network settings as follows:
 - From the XT Series web interface, select **Administrator Settings > Networks > Preferences > QoS**.
 - From the endpoint's main menu, select **Configure > Advanced > Networks > Preferences > QoS**.

Figure 77: Configuring QoS settings

- Set the fields as described in [Table 30: Configuring QoS settings](#) on page 125.

Table 30: Configuring QoS settings

Field Name	Description
Use QoS	Enable/Disable QoS. If you set Use QoS to Yes , you will provide different priority to different data stream, or guarantee a certain level of performance to a data stream. In particular, you may choose between Precedence/TOS and Differentiated Service .
Quality of service	Precedence/TOS - For each stream (Audio , Video , Data , Signal) sent to the system, you may define the Type Of Services and a Precedence to fit network capabilities. Precedence is priority. A higher number sets a higher priority. Used mainly to class router packets as high priority.
	Differentiated Service - For each stream (Audio , Video , Data , Signal) sent to the system, you may define a priority level to fit network capabilities.

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

Registering the Scopia XT Series with a Gatekeeper

About this task

Gatekeepers enable you to contact H.323 endpoints by entering an alias, rather than having to remember each endpoint's IP address. For example, you can dial "1234" or "joesmith" and the gatekeeper routes the call correctly.

To do this, the gatekeeper must register all endpoints to maintain the mapping list of aliases and endpoints to successfully route calls. It also registers gateways to ensure that a call can be routed to a non-H.323 entity, since gateways form the bridge from H.323 to other protocols, such as ISDN.

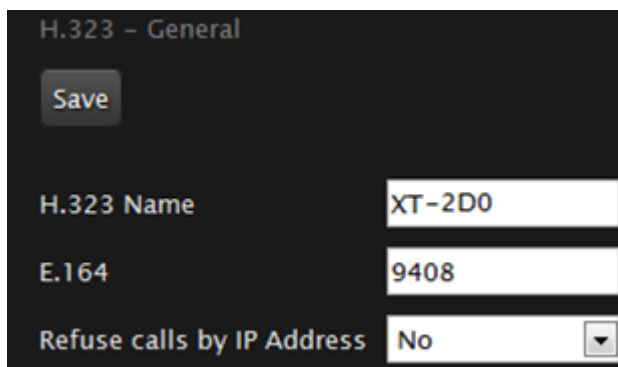
When registering with a gatekeeper like Scopia ECS Gatekeeper, the endpoint sends its IP and aliases. Registration occurs before any calls are attempted and may occur periodically, or once, such as during endpoint power-up.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the gatekeeper settings as follows:
 - From the XT Series web interface, select **Administrator Settings > Protocols > H.323 > General**.
 - From the endpoint's main menu, select **Configure > Advanced > Protocols > H.323 > General**.



H.323 - General	
Save	
H.323 Name	XT-2D0
E.164	9408
Refuse calls by IP Address	No

Figure 78: Configuring H.323 settings from the web interface

2. Set the fields as described in [Table 31: Configuring H.323 settings](#) on page 127.

Table 31: Configuring H.323 settings

Field Name	Description
H.323 Name	The H.323 name or ID (alias) used to register the unit with the gatekeeper. When connecting over H.323, this name is displayed on the monitors participating in the videoconference (for example: John-Smith , or 9th-Floor-Room , or NY-Office).
E.164	The E.164 number used to register the unit with the gatekeeper.
Refuse calls by IP Address	Select Yes to allow only endpoints registered to the gatekeeper to call your endpoint.

- From the web interface only, select **Save**.
- Select **Gatekeeper** under **H.323**.

H.323 - Gatekeeper

Save

Use Gatekeeper Yes

Automatic IP Address No

IP Address 0.0.0.0

Use H.460 Yes

Re-Registration Interval Time 10

Authentication No

Mode <auto>

Gatek. ID

User Name

Password

Figure 79: Configuring the Gatekeeper settings from the web interface

- Set the fields as described in [Table 32: Configuring the gatekeeper](#) on page 128.

Table 32: Configuring the gatekeeper

Field Name	Description
Use gatekeeper	Enables/disables the use of a gatekeeper. If No is selected, all the other fields are greyed. If Yes is selected, the XT Codec Unit can use the gatekeeper's services.
Automatic IP address	Automatic gatekeeper discovery. The XT Codec Unit searches for an available gatekeeper.
IP address	Enter the IP address of the gatekeeper, if you do not use Automatic IP address .
Use H.460	If set to Yes , the system uses H.460 firewall traversal features.
Re-registration interval time	This option is normally off and must be enabled only if the XT Codec Unit administrator is sure that the gatekeeper sends the IRQ messages (see the Gatekeeper's documentation for more information). Enter the time (in seconds) after which the system should re-register to the gatekeeper because the registration state was lost. This field is useful if you do not want to use the normal RAS lightweight registration procedure.
Authentication	If Authentication is enabled, the related fields must be defined. If it is not enabled, the four text fields (Mode , Gatek. ID , User name , Password) are greyed.
Mode	Automatic , MD5 , H.235 annex D - If set to Automatic , the XT Codec Unit selects the best mode according to the gatekeeper.
Gatek. ID	Gatekeeper H.323 identifier. Ask the network administrator.
User name	The network administrator must pre-configure the User name in the gatekeeper.
Password	The network administrator must pre-configure the Password in the gatekeeper.

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

Registering the XT Series to a SIP Server

About this task

The procedure in this section explains how to register your XT Series to the SIP Registrar and how to configure the SIP Proxy connection.

The XT Series can be configured to function in a SIP environment, where aliases are managed by SIP servers rather than gatekeepers. In a SIP environment, a user can contact an endpoint by entering its alias, rather than having to remember the endpoint's IP address. For example, you can dial "1234" or "joesmith" and the SIP server routes the call correctly. To do this, the SIP server must register all endpoints to maintain the mapping list of aliases and endpoints to successfully route calls.

Before you begin

Verify that you have the following information about your SIP environment:

- The DNS names or IP addresses of the SIP Proxy and SIP Registrar.
- The transport protocol and port used in your SIP environment.
- (Optional) The model of the SIP Proxy.
- For the SIP infrastructure that requires a SIP user authentication, credentials for authenticating XT Series to the SIP Proxy and SIP Registrar.

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the SIP settings as follows:

- From the XT Series web interface, select **Administrator Settings > Protocols > SIP**.
- From the endpoint's main menu, select **Configure > Advanced > Protocols > SIP**.

SIP

Save

User: XT

Authentication Name: Admin

Authentication Password:

UDP/TCP Listening Port: 5060

Transport Outbound Call: UDP

Use SIP Registrar: Yes

Registrar DNS Name:

Use SIP Proxy: Yes

Proxy DNS Name:

Proxy Model: Auto

Use TLS: Yes

TLS Listening Port: 5061

Verify Certificate: Yes

Figure 80: Configuring SIP settings

2. Configure parameters as described in [Table 33: Configuring SIP-related parameters](#) on page 130.

Table 33: Configuring SIP-related parameters

Parameter	Description
User	Enter the system user name (alias). The system is registered to the SIP Registrar under this name. When connecting over SIP, this name is displayed on the monitors participating in the videoconference (for example: John-Smith, or 9th-Floor-Room, or NY-Office).
Authentication Name	If necessary, enter the name for authenticating the XT Series with the SIP Proxy server and SIP Registrar. It can be the same as the User parameter.

Parameter	Description
Authentication Password	If necessary, enter the password for authenticating your XT Series with the SIP Proxy server and SIP Registrar.
UDP/TCP Listening Port	Enter the port number used by XT Series for receiving inbound SIP calls. By default, port 5060 is used.
Transport Outbound Call	Select the preferred transport protocol for outbound SIP calls: TCP or UDP .
Use SIP Registrar	Enable registering the system to the SIP Registrar by selecting Yes .
Registrar DNS Name	Enter the DNS name or IP address of the SIP Registrar.
Use SIP Proxy	Enable using the SIP Proxy by selecting Yes .
Proxy DNS Name	Enter the DNS name or IP address of the SIP Proxy.
Proxy Model	Select the model of the SIP Proxy server. Specifying the model can help to avoid potential interoperability issues. If the model is unknown or is not on the list, select Auto . Dual video streams are not supported for both Cisco UCM and BroadSoft proxy servers (BFCP is disabled). Presentations from a PC are sent instead of the video. For the BroadSoft proxy server, controlling remote cameras is also not supported (H.224 is disabled).

3. From the web interface only, select **Save**.
4. (Optional) If you are securing SIP connections using TLS certificates, continue with [Securing Connections to the XT Series Using TLS](#) on page 140.

Configuring Call Settings

About this task

To allow incoming and outgoing calls, configure the following system settings according to your network requirements, as described in this procedure:

- Network's preferred GLAN
- Call settings, such as defining calls as audio-only, or specifying the call rate
- IP settings, such as determining whether the XT Codec Unit checks the source of audio and video data packets

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the network priority settings as follows:
 - From the XT Series web interface, select **Administrator Settings > Networks > Preferences > General**.
 - From the endpoint's main menu, select **Configure > Advanced > Networks > Preferences > General**.

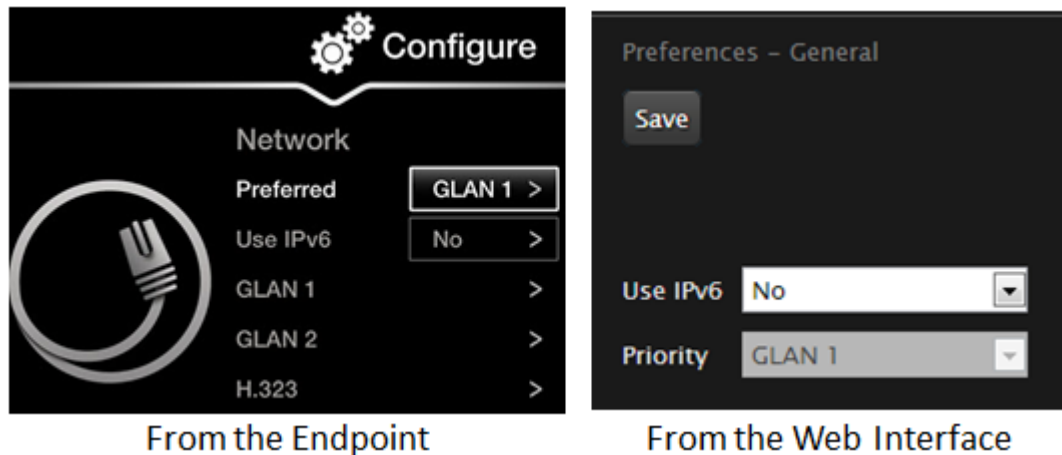


Figure 81: Configuring the Priority setting from the web interface

2. Set the **Priority** setting to the GLAN port that the preferred network uses. This field specifies in which order the system places outgoing calls.
3. From the web interface only, select **Save**.
4. Access the call settings as follows:
 - From the web interface, select **Administrator Settings > Calls > Preferences > General**.
 - From the endpoint, select **Configure > Advanced > Calls > Preferences > General**.

Preferences – General

Save

IP

Rate (K) 6144K

Audio Coding <auto>

Video Coding <auto>

DualVideo coding <auto>

Use manual DualVideo bandwidth No

DualVideo/Live bandwidth 50

ISDN

Rate (K) 1920K

MCU

Local audio-video Yes

Figure 82: Configuring general call settings

- Set the fields as described in [Table 35: Configuring the IP-related call settings](#) on page 134.

Table 34: Configuring general call settings

Field Name	Description
<auto>	(Recommended) This is the default and setting. It indicates that the system tries to choose the settings that best suit the local situation.
Rate K (IP)	Sets the maximum call rate that the system uses for all incoming or outgoing calls.
Audio Coding (IP)	Sets the preferred Audio Coding that the system tries to use for all incoming or outgoing calls, if the remote system supports the same Audio Coding.
Video Coding (IP)	Sets the preferred Video Coding that the system tries to use for all incoming or outgoing calls, if the remote system supports the same Video Coding.
DualVideoCoding (IP)	Sets the resolution for H.264 content video.
Use manual DualVideo bandwidth (IP)	If set to Yes allows to change bandwidth used for content and live video (DualVideo/Live bandwidth).
DualVideo/Live bandwidth (IP)	Sets more bandwidth on Live Video or Content.

Field Name	Description
Rate K (ISDN)	Sets the maximum call rate that the system uses for all incoming or outgoing calls in ISDN connectivity.
Local audio-video (MCU)	If using the system as an endpoint that can also host conferences on the embedded MCU, select Yes to include local video and audio in videoconferences. Select No to hide the local audio and video and use the system as an MCU.

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

7. Access the IP settings as follows:

- From the web interface, select **Administrator Settings > Calls > Preferences > IP**.
- From the endpoint interface, select **Configure > Advanced > Calls > Preferences > IP**.

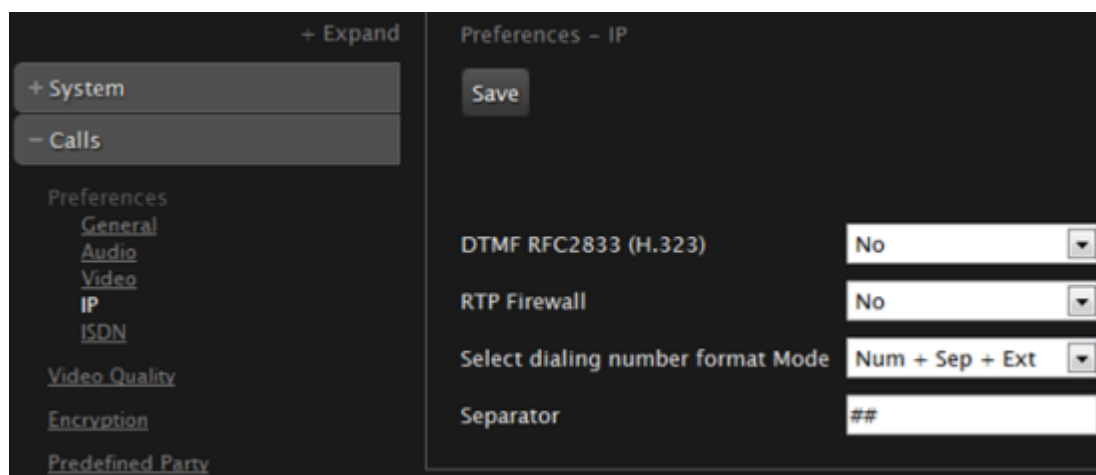


Figure 83: Configuring the IP settings from the web interface

8. Set the fields as described in [Table 35: Configuring the IP-related call settings](#) on page 134.

Table 35: Configuring the IP-related call settings

Field Name	Description
DTMF RFC2833 (H.323)	DTMF describes a method to send DTMF inside an audio stream. This method is normally used in SIP protocol but is uncommon in H.323. If set to Yes, the H.323 application in the XT Codec Unit can use DTMF transmission. Verify the remote endpoint supports RFC2833 before enabling this field.
RTP Firewall	If set to Yes, the XT Codec Unit checks the source of the RTP packets (audio, video, and presentation) it receives to verify that it matches the remote endpoint's IP address.

Field Name	Description
Select dialing number format mode	If your XT Codec Unit is not registered with an H.323 gatekeeper, you can still place a call to an endpoint registered with a gatekeeper. Check which format of dialing the gatekeeper accepts and configure it in this field: <gatekeeper number><separator> <extension of the called endpoint>, or <extension> <separator><number>. The default syntax is <number><separator><extension>.
Separator	Select the field separator accepted by the gatekeeper. The default separator is ##.

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

Configuring Scopia XT Series Endpoints to use an LDAP Directory

About this task

This procedure describes how to manage the contacts of your endpoint using any of a number of different types of LDAP servers.

LDAP servers are accessed using the H.350 protocol, which enhances the LDAP standard to include video endpoint information.

You can define up to 100 LDAP servers either from the endpoint itself or from the web interface. The LDAP servers visible from the Contacts page are only those labeled as Preferred. Select one of the preferred LDAP servers from the **Server** field in the contacts page to view its contacts ([Figure 84: Viewing and editing contacts in Local LDAP server](#) on page 135).



Figure 84: Viewing and editing contacts in Local LDAP server

You can define three types of LDAP servers:

- The local built-in LDAP server

You can define only one local LDAP server. When selected, you can edit, create or delete the details of any contacts stored locally ([Figure 84: Viewing and editing contacts in Local LDAP server](#) on page 135). The local LDAP server has a password which can be changed if needed.

! Important:

You cannot remove the local LDAP server.

- A remote XT Series's built-in LDAP server

The contacts are read-only when browsing a remote XT Series's LDAP server. You can define more than one of these LDAP servers, where each requires only the IP address of the remote endpoint and its LDAP password.

- Scopia Management's built-in LDAP server

The contacts of this server are read-only from the endpoint. You can define more than one such server, specifying each IP address, port, and its LDAP username and password. The resulting contact list is filtered to show only users registered to an endpoint.

! Important:

If the Scopia Management LDAP server has a Root DN defined, you must specify the **RootDN** field when defining that LDAP server.

- A third-party LDAP server, such as Microsoft Active Directory

The contacts of a third party LDAP are read-only from the endpoint. The LDAP tree must have the following specific structure and naming conventions:

- The Root DN must be defined. For example, **dc=company, dc=com**.
- All users (**inetOrgPerson** entities) must be located under an organizational unit (**ou**) in the LDAP tree. For example, **ou=people**.
- All endpoints (**commObject** entities) must be listed under an organizational unit called **h323Identity** if they are to work with H.323, and **SIPIdentity** if they are to work as SIP endpoints.

Since the XT Series works both as an H.323 and a SIP endpoint, all XT Series **commObjects** should be listed under both organizational units.

- Each endpoint is represented by a **commObject** with its **commUniqueid**. Each **commObject** contains the details of accessing this endpoint, and the user associated with it. Define the following fields:

Table 36: commObject fields

Field	Value	Comments
objectClass	commObject	Use this exact value
objectClass	h323Identity	Use this exact value
commOwner	uid=<x>,ou=people,dc=company,dc=com	The user ID associated with this endpoint
h323IdentityEndpointType	Terminal	Use this exact value for H.323 endpoints only
h323IdentitytransportID	<ip address>	At least one of these fields must be defined for an H.323 endpoint.
h323IdentitytransportDigits	<E/164 dial number>	
h323IdentitytransportNumber	<H.323 alias>	
h323Identityh323-ID	<H.323 alias>	
SIPIdentitySIPURI	<URI address of SIP endpoint>	SIP endpoints only.

- Each user (**inetOrgPerson** entity) must have its **commURI** field pointing to the user's endpoint (**commObject ID**).

For example:

```
ldap://123.456.789.012/ou=h323identity,dc=company,dc=com??sub?(commUniqueid=6)
```

Scopia XT5000

where commUniqueid refers to the **commObject ID**

A centralized solution like Scopia Management enables synchronizing the same list of contacts across all the endpoints in your organization, and has other benefits like remote centralized upgrading and backing up of all endpoints in your video network. In deployments without Scopia Management, you can use the local built-in LDAP server that comes within every XT Series unit.

! Important:

You can configure the XT Series to use Scopia Management as the LDAP directory also from the Scopia Management administrator portal (for details, see the *Administrator Guide for Scopia Management*).

Before you begin

- If you are using Scopia Management as the LDAP directory, associate LDAP contacts to video endpoints; otherwise these contacts are not displayed on the XT Series.

Each LDAP contact on the XT Series can only be mapped to a maximum of ten video endpoints.

- If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the LDAP settings, as follows:

- From the endpoint's main menu, select **Configure > Advanced > System > LDAP**.
- From the XT Series web interface, select **Administrator Settings > System > LDAP**.

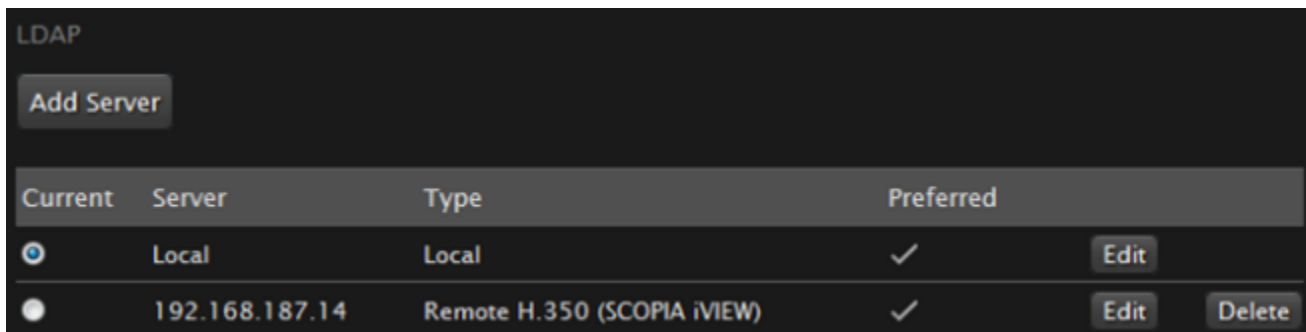


Figure 85: Configuring LDAP settings from the web interface

2. Select **Add Server**.

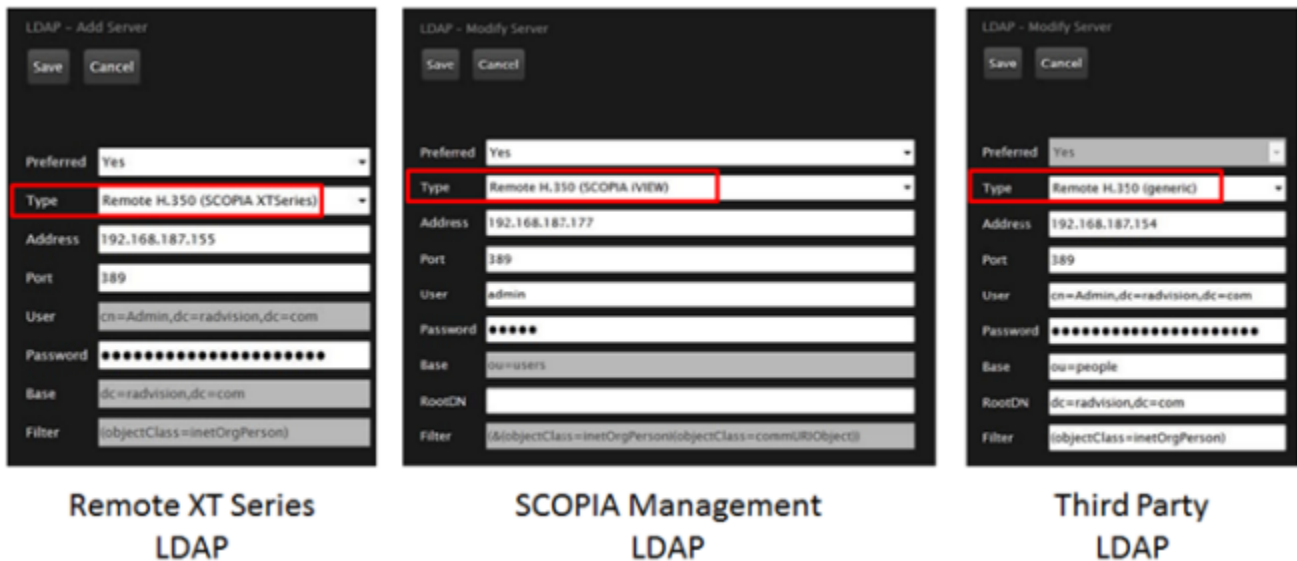


Figure 86: Adding each type of LDAP server from the web interface

3. Configure the LDAP server settings as described in [Table 37: Configuring LDAP server settings](#) on page 138.

Table 37: Configuring LDAP server settings

Field Name	Description
Preferred	To view contacts from this LDAP server from the Contacts page, select Yes . Users can then select one of these preferred LDAP servers to view the contacts in that LDAP database.
Type	Define the type of LDAP server you are configuring, as follows: • Local Server: The endpoint's built-in LDAP server. Users can add, modify and delete contacts, as well as call and browse contacts in the phone book. • Remote H.350 (XT Series): An external XT Series's built-in LDAP server. Users cannot make any changes to the contact list for this endpoint. • Remote H.350 (Scopia Management): Scopia Management's built-in LDAP server. Users cannot make any changes to the contact list for this endpoint. • Remote H.350 (generic): A third-party LDAP server, such as Microsoft Active Directory. Users cannot make any changes to the contact list for this endpoint.
Address	Enter the LDAP server address. If you are using Scopia Management as your LDAP directory, enter Scopia Management's IP address.
Port	Enter the port used to connect to the LDAP server. The default port is 389.
User	Enter the username and password required to access the LDAP server. The format of the username is in the form of a Distinguished Name (DN). Some standard components of DN are: domain controller (dc), organizational unit (ou), common name (cn), country (c), state or province (st), locality (l), organization (o).

Field Name	Description
Password	The login to third party LDAP servers is via a Simple Bind LDAP v3 operation.  Important: When using the endpoint's built-in LDAP server, you can modify the password here. When using an external XT Series as the LDAP server, this value cannot be modified, since the LDAP user of a XT Series is predefined.
Base	The root of the LDAP tree where the contacts' records are defined. Use this field for third party LDAP server connections to define the node under which all the inetOrgPerson entities are located. For example ou=people. This value is predefined when the LDAP server is an XT Series or Scopia Management, and cannot be modified.
Root DN	For third party LDAP servers, enter the mandatory H.350 Root DN. For a Scopia Management LDAP directory, if you defined the Root DN in Scopia Management, enter it here. For details, see the <i>Administrator Guide for Scopia Management</i>. For XT Series LDAPs, this field is not displayed.
Filter	The filter applied to the LDAP tree, so you view only the relevant contacts. This value is predefined when the LDAP server is an XT Series or Scopia Management.

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

Chapter 7 | Securing your Scopia XT Series

You can secure the connection between video network devices and your Scopia XT Series by configuring the network's components to communicate via the Transport Layer Security (TLS) protocol, and enabling encryption.

For details about securing your Scopia XT Series, see:

Navigation

- [Securing Connections to the XT Series Using TLS](#) on page 140
- [Enabling Encryption for Videoconferences](#) on page 149

Securing Connections to the XT Series Using TLS

You can configure your video network, whether it is a Scopia Solution or a third party deployment, to support Transport Layer Security (TLS) for the SIP protocol.

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.

TLS is used to secure the connection between the XT Series and other video network devices.

The TLS protocol is based on a public and private keys for authorization and encryption, exchanged between the XT Series and other video network devices to allow an authenticated and secure connection. You can create a pair of keys, public and private, by generating a certificate which must be signed by a certification authority. The public key is placed in a certificate and signed by a certification authority (CA).

As you configure your deployment for TLS, you need to generate a certificate signing request (CSR) for every XT Series that uses TLS in your deployment and send it to the CA to be signed. A CA has its own certificate, known as the CA root certificate. When the CA signed certificate is ready, you upload it into the XT Series for which it was created, together with the CA root certificate.

Each time a TLS connection is established, the video network device which starts the TLS communication session requests a signed certificate together with the CA root certificate. After the other device verifies its identity with these certificates, a secure connection can be established. Exchanging certificates between devices is part of the TLS protocol; it happens in the background and is transparent to a user.

The following set of procedures secure the connection between XT Series and other devices. Perform these tasks in the order listed below:

1. Perform [Generating a Certificate Signing Request for XT Series](#) on page 141.
2. Ensure you have the root certificate of the certificate authority your organization uses.
This root certificate is used when uploading signed certificates into the XT Series.
3. Perform [Uploading XT Series Certificates](#) on page 143.

4. Perform [Enabling the TLS Connection in XT Series](#) on page 147 .
5. To encrypt the media (audio, video, presentation) of videoconferences using the SRTP protocol, perform [Enabling Encryption for Videoconferences](#) on page 149.

Generating a Certificate Signing Request for XT Series

About this task

This section details how to generate a certificate signing request (CSR) for the XT Series, which must be signed by a certificate authority (CA). This is done from the web interface only.

Once properly signed, the certificate would confirm the identity of the XT Series to other components in the network, and can also facilitate encrypted communications with those components.

Important:

If you modify the XT Series's IP address, you must generate a new CSR.

To restore previously uploaded certificates, see [Backing Up and Restoring XT Series Certificates](#) on page 145. To delete the certificates, see [Backing Up and Restoring XT Series Certificates](#) on page 145.

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.

Before you begin

To secure SIP connections using TLS certificates, your system must have a static IP address, since the system generates the certificate request using its IP address as the Common Name (CN). For more information, see [Configuring IP Addresses](#) on page 118.

Procedure

1. Access the XT Series web interface, as described in [Accessing XT Series Web Interface](#) on page 62.
2. Select **Administrator Settings > Utilities > Certificates**.
3. Enter your organization's details and your email.

Certificates

Step 1

Create a Certificate Signing Request (CSR)

Country: US

State Full Name: New York

Locality: Albany

Organization: Company Name

Organizational Unit: Marketing

Email: name@company.com

Create

Figure 87: Generating a CSR for Scopia XT Series

Table 38: Entering the organization's details

Field	Description
Country	Enter the organization's country code. ! Important: Country must include two characters only. For more information about the country code to use, contact your Certificate Authority.
State Full Name	Enter the complete name of the organization's state or country.
Locality	Enter the organization's city.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of your specific department within the organization.
Email	Enter your email address.

4. Select **Create**.
The CSR is created.
5. Select **Download > Download CSR** to save the CSR.

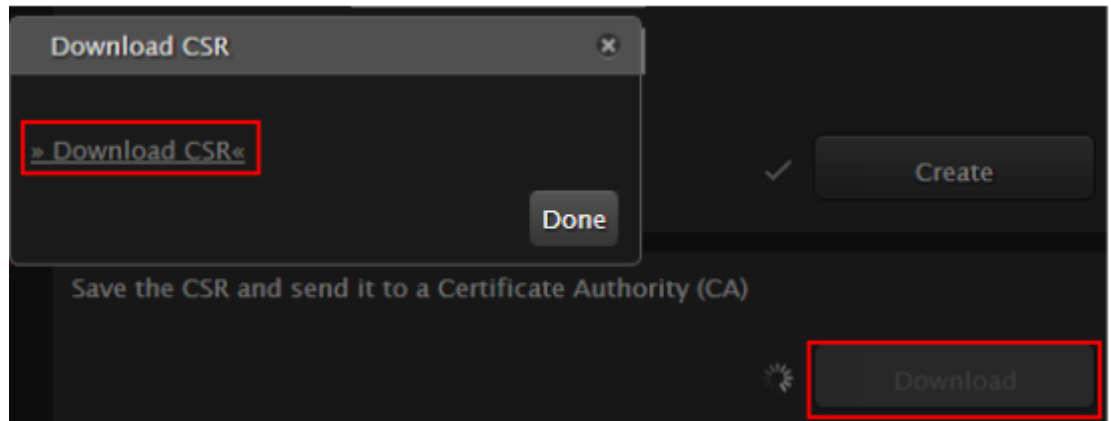


Figure 88: Downloading the CSR

The CSR is downloaded onto your computer, with the following filename:

<IP address>_csr.pem

6. Save the certificate in an appropriate folder. The certificate is saved as a text file compatible with Base-64 ASCII code, in .pem format.
7. Send the text file containing the certificate for signing as a certificate compatible with Base-64 ASCII code.

! Important:

The certificate must be signed as a certificate compatible with Base-64 ASCII code, in either .pem or .cer format.

If other components communicating with the XT Series also have their own certificates, we recommend using a common CA for all certificates for a more efficient implementation.

8. Continue with [Uploading XT Series Certificates](#) on page 143.

Uploading XT Series Certificates

About this task

This procedure describes how to upload certificates which confirm the identity of an XT Series, from its web interface.

! Important:

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

The XT Series requires two certificates to be uploaded: a signed certificate identifying the XT Series signed by a certification authority (CA) and that CA's root certificate. Each time a network device tries to establish a new TLS session with the XT Series, it sends its identity certificate to the XT Series to establish a secure connection.

To restore previously uploaded certificates or to back up certificates after uploading, see [Backing Up and Restoring XT Series Certificates](#) on page 145. To delete the certificates, see [Backing Up and Restoring XT Series Certificates](#) on page 145.

Before you begin

1. Ensure that you have the root certificate for the certificate authority that your organization uses. The root certificate must be compatible with the Base-64 ASCII code, in either .pem or .cer format.
2. Ensure that you have the signed certificate from the CA for the XT Series (see [Generating a Certificate Signing Request for XT Series](#) on page 141 for details on generating the CSR).

Procedure

1. Access the XT Series web interface, as described in [Accessing XT Series Web Interface](#) on page 62.
2. Select **Administrator Settings > Utilities > Certificates**.
3. Import the Certificate Authority (CA) root certificate as follows:

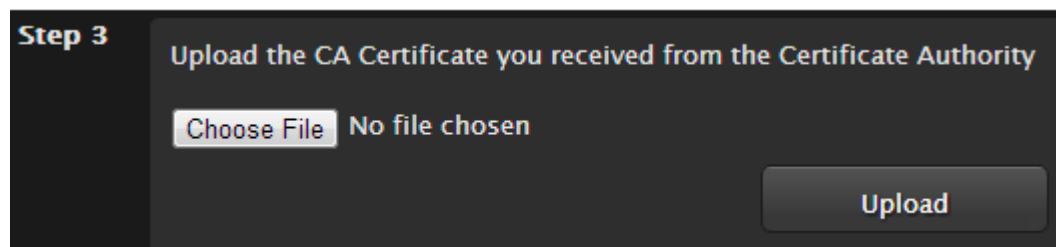


Figure 89: Uploading the CA root certificate

- a. Select **Choose File** (next to Step 3) and browse to the CA root certificate you received from the CA.
 - b. Select **Upload**.
4. Import the signed certificate you received from the CA, as follows:

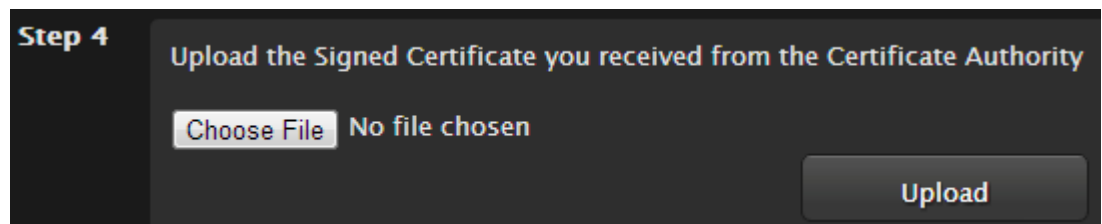


Figure 90: Uploading the signed certificate

- a. Select **Choose File** (next to Step 4) and browse to the signed certificate you received from the CA.
- b. Select **Upload**.

The certificate is validated and its details appear ([Figure 91: Signed certificate from the CA](#) on page 145).

+ Tip:

Verify that the system's time is synchronized with SNTP, otherwise you may need to wait a few hours before using this certificate (for details, see [Setting Date and Time](#) on page 95). You can start using this certificate at the time indicated by the **notBefore** value in the signed certificate.

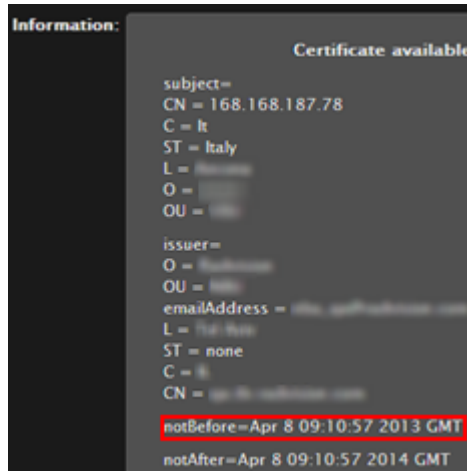


Figure 91: Signed certificate from the CA

5. Continue with [Enabling the TLS Connection in XT Series](#) on page 147.

Backing Up and Restoring XT Series Certificates

About this task

This section explains how to backup and restore certificates using a USB key to store the certificate information. You can only perform this procedure from the endpoint's interface. If you want to delete the certificates without first backing them up, proceed as explained in [Deleting XT Series Certificates](#) on page 146.

Procedure

1. Connect a USB key to the upper USB port of the XT Codec Unit ([Figure 92: Connecting a USB Key to the XT Codec Unit](#) on page 146).

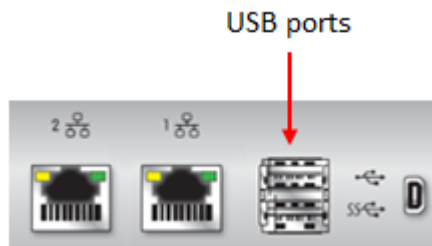


Figure 92: Connecting a USB Key to the XT Codec Unit

2. To back up a certificate to the USB key, select **Advanced > Utilities > Certificates > Backup** ([Figure 93: Backing up or restoring certificates](#) on page 146).
The system copies the certificates and associated keys to the root folder of your USB key.



Figure 93: Backing up or restoring certificates

3. If you select **Backup and Remove**, the system first copies the certificates and associated keys to the USB key and then removes them from the XT Codec Unit.
4. To restore a certificate into the system, select **Advanced > Utilities > Certificates > Restore** ([Figure 93: Backing up or restoring certificates](#) on page 146). This automatically restores the certificates and associated keys to the system.

Deleting XT Series Certificates

About this task

This section explains how to remove or uninstall a certificate from the XT Series using the web interface. You might need to remove certificates if:

- For privacy reasons, you do not want to keep your certificates on a shared endpoint.
- The system generated errors while creating the CSR and you want to replace it with a new one.
- You want to use a different CA for signing your certificates.
- You changed the system's IP address.

Important:

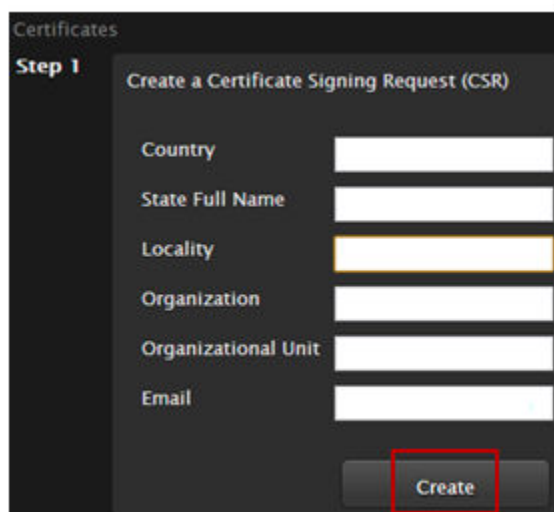
To secure SIP connections using TLS certificates, your system must have a static IP address, since the system generates the certificate request using its IP address as the Common Name (CN).

This procedure removes the current certificate by replacing it with a blank form. To back up a certificate before deleting it from the system, see [Backing Up and Restoring XT Series Certificates](#) on page 145.

Procedure

1. Access the XT Series web interface, as described in [Accessing XT Series Web Interface](#) on page 62.
2. Select **Administrator Settings > Utilities > Certificates**.
3. Leave all fields blank and select **Create** to start a new CSR procedure. This erases the previous certificates.

Figure 94: Removing Current Certificates



The screenshot shows a web interface titled 'Certificates' with a sub-header 'Step 1'. Below this is the instruction 'Create a Certificate Signing Request (CSR)'. There are six text input fields: 'Country', 'State Full Name', 'Locality', 'Organization', 'Organizational Unit', and 'Email'. The 'Locality' field is currently selected with a yellow border. At the bottom right of the form is a button labeled 'Create', which is highlighted with a red rectangular box.

Enabling the TLS Connection in XT Series

About this task

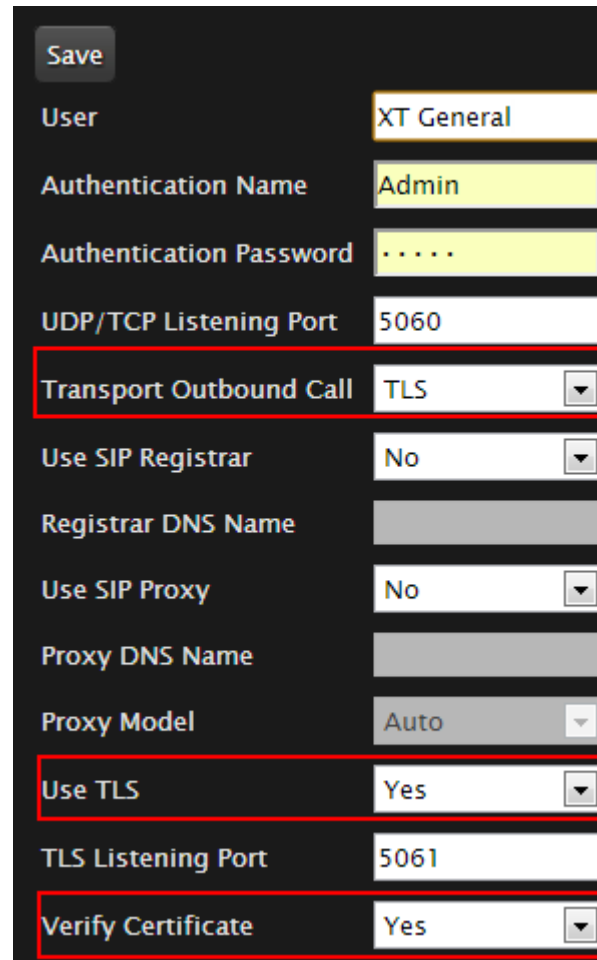
This procedure describes how to enable the system to use the TLS connection, which is required to secure communications between other video network devices and your XT Series.

Before you begin

Upload the required certificates to the XT Series, as described in [Uploading XT Series Certificates](#) on page 143.

Procedure

1. Access the XT Series web interface, as described in [Accessing XT Series Web Interface](#) on page 62.
2. Select **Administrator Settings > Protocols > SIP**.
3. Select **Yes** from the **Use TLS** list to accept incoming calls using TLS.



Save

User	XT General
Authentication Name	Admin
Authentication Password	
UDP/TCP Listening Port	5060
Transport Outbound Call	TLS
Use SIP Registrar	No
Registrar DNS Name	
Use SIP Proxy	No
Proxy DNS Name	
Proxy Model	Auto
Use TLS	Yes
TLS Listening Port	5061
Verify Certificate	Yes

Figure 95: Enabling TLS

4. Define the following settings:

Table 39: Configuring TLS Settings

Field	Description
Transport Outbound Call	Select TLS to secure outgoing calls via TLS.
Verify Certificate	Select one of the following: • Yes to connect to other devices via TLS only when the other device has certificates signed by the same Certificate Authority (CA) as the Scopia XT Series. • No to connect to any other device. The connection is only secured via TLS when the other device has certificates signed by the same Certificate Authority (CA) as the Scopia XT Series.

5. Select **Save**.

6. (Optional) If required by your organization's security policies, continue with [Enabling Encryption for Videoconferences](#) on page 149.

Enabling Encryption for Videoconferences

About this task

The system can secure videoconference sessions via encrypted connections, in both point-to-point calls and videoconferences, as follows:

- For SIP connections, you can encrypt the actual media of SIP connections via SRTP.
Secure Real-time Transport Protocol (SRTP) adds security to the standard RTP protocol, which is used to send video and audio data between devices in SIP calls using TLS. It offers security via encrypting, authenticating and ensuring message integrity.
- For H.323 connections, encryption is enabled via H.235.
H.235 is the protocol used to authenticate trusted H.323 endpoints and encrypt the media stream during meetings.

Configure settings for securing calls as described in the procedure below. You can have up to three remote encrypted participants in a videoconference.

You can do this procedure from the endpoint itself or from the XT Series web interface.

Important:

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

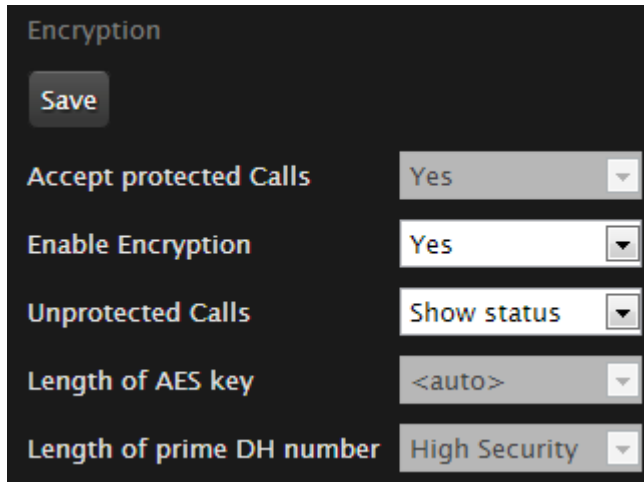
Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

To encrypt SIP calls using SRTP, you must also secure communication between your video network devices using TLS certificates and enable encryption (see [Securing Connections to the XT Series Using TLS](#) on page 140). If TLS is not enabled, only SIP calls to other XT Series endpoints are encrypted, using a proprietary encryption protocol.

Procedure

1. Access the security settings as follows:
 - From the XT Series web interface, select **Administrator Settings > Calls > Encryption**.
 - From the endpoint's main menu, select **Configure > Advanced > Calls > Encryption**.



Encryption	
<button>Save</button>	
Accept protected Calls	Yes
Enable Encryption	Yes
Unprotected Calls	Show status
Length of AES key	<auto>
Length of prime DH number	High Security

Figure 96: Encrypting calls from the web interface

2. Select **Yes** from the **Enable encryption** field.
3. Set the fields as described in [Table 40: Configuring settings for securing calls](#) on page 151.

Table 40: Configuring settings for securing calls

Field Name	Description
Accept protected calls	If encryption is enabled, the system automatically encrypts incoming calls and this field is read-only. If encryption is disabled, set to Yes to allow the system to use encryption when receiving an encrypted call.
Unprotected calls	Select the policy the system applies when a remote endpoint does not support protected calls: • Show Status: The system displays a warning message and an open padlock symbol is displayed on the status bar (the default option). • Disconnect: The system automatically disconnects the call. • Ask Confirmation: The system asks you to confirm that you want to establish an unprotected call. • Inform: The system displays a warning message.
Length of AES key	This value is always fixed at 128 bit, which is the standard H.323 value.
Length of Prime DH Number	This value is always fixed at 1024 bit, which is the standard H.323 value.

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



Chapter 8 | Troubleshooting the Scopia XT Series

This section covers troubleshooting problems that may occur when setting up and using the Scopia XT Series.

Navigation

- [Viewing System Information for Customer Support](#) on page 152
- [Resolving Problems with Audio](#) on page 154
- [Echo Cancelling on HDMI Monitors](#) on page 156
- [Resolving Monitor Display Problems](#) on page 158
- [Resolving Camera Issues](#) on page 160
- [Resolving IP Address Problems](#) on page 162
- [Resolving XT Remote Control Unit Problems](#) on page 164
- [Restoring Default User Settings](#) on page 165

Viewing System Information for Customer Support

About this task

When contacting customer support or your system administrator, you may need to provide information about the system. This procedure describes how to view the following system information from the endpoint or from the web interface:

- Software version
- User code (MAC address)
- IP addresses
- Serial number
- System name and model
- Licenses
- Network, gatekeeper, and SIP settings

Important:

The system serial number also appears on the label at the back of the XT Codec Unit.

Procedure

1. View system information as follows:

- From the XT Series web interface, log in. The system information is displayed in the **Home** tab.
- From the endpoint's main menu, select **Configure** > **About** using the XT Remote Control Unit.

! Important:

If your system is currently in a call, press **ok/menu** and select **Stats** > **Configure** > **About**.

System	SCOPIA XT5000	Remote Control Code	2
H.323 Name	XT5000-2D0	Software Version	03.01.00.0015 V3_1_0_15B
GLAN 1	172.16.90.67	GLAN 1 MAC Address	00:03:D6:01:82:D0
GLAN 2	0.0.0.0 (No cable)	GLAN 2 MAC Address	00:03:D6:01:82:D1
E.164	9408	SIP Name	XT5000-2D0
Use Gatekeeper	172.20.73.51	Use SIP Proxy	No
Gatekeeper State	Registered	Use SIP Registrar	No

Viewing information from the web interface



Viewing information from the endpoint

Figure 97: Viewing system information

2. To view additional system information such as IP addresses and the gatekeeper's registration status from the endpoint, press the  **Back** key and select **System Status**.

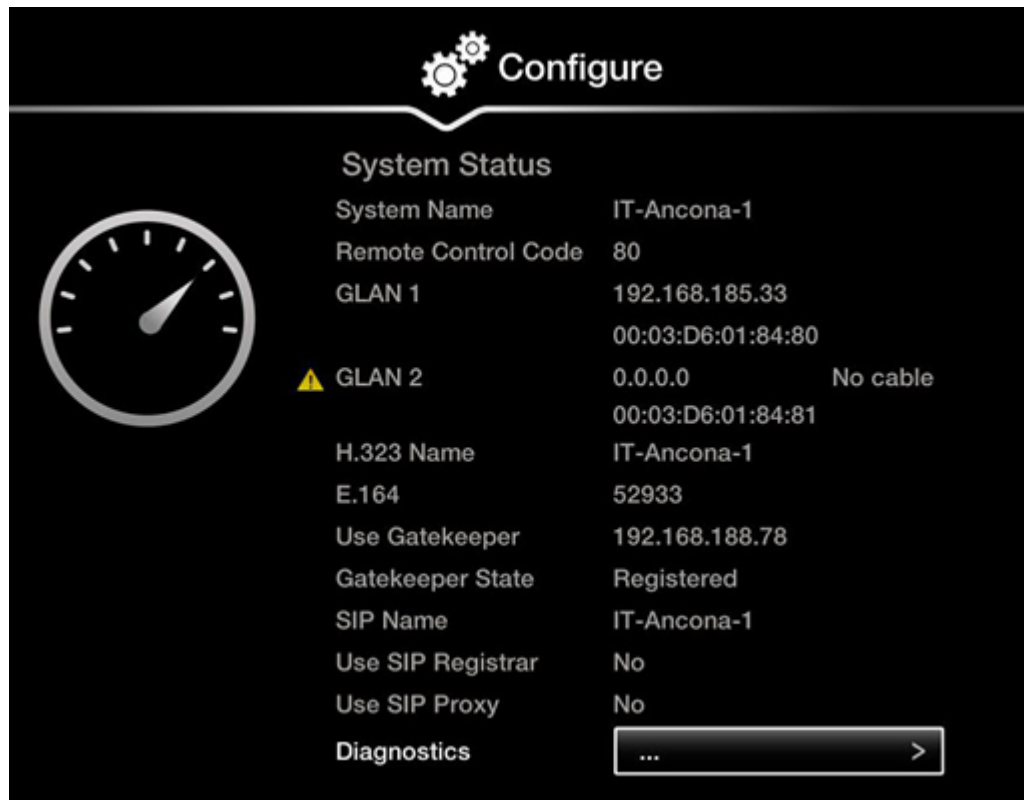


Figure 98: Viewing system network information

Resolving Problems with Audio

Problem I cannot hear audio after setting up the system.

Solution Make sure the monitor volume is not set to 0.

Solution Make sure the system volume is not set to 0 by activating  on the XT Remote Control Unit.

Solution While the system is in a call, perform the audio tests to verify that the audio input and output are in order:

1. Access audio tests as follows:
 - From the endpoint, select **Configure > System Status > Audio > Tests**.
 - From the web interface, select **Diagnostics > Audio > Tests**.

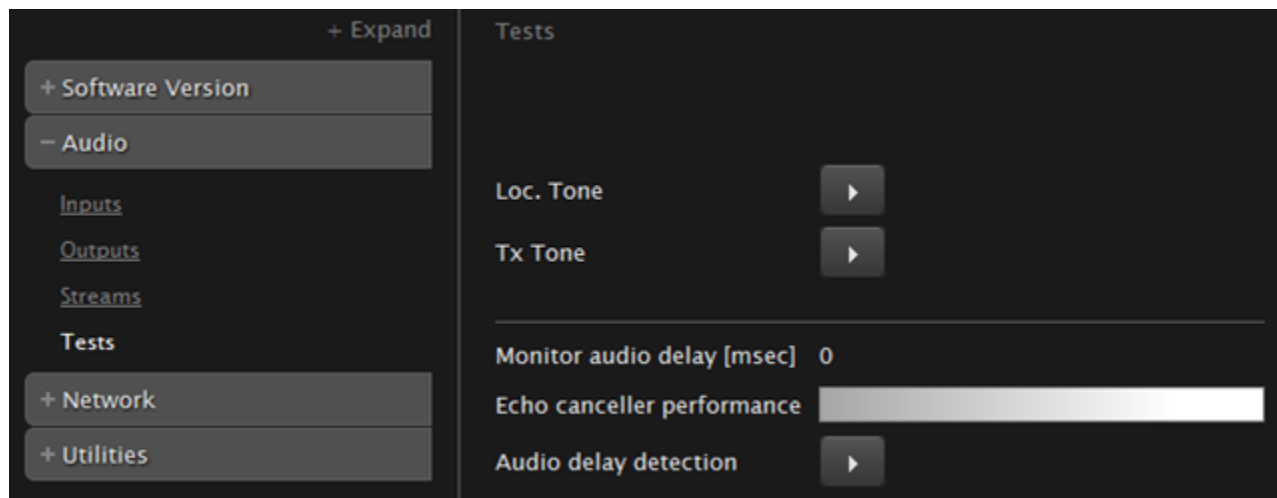


Figure 99: Performing the audio tests from the web interface

2. Select **Loc tone**  to check the audio input received by the endpoint. If the test is completed successfully, the **Done** message is displayed.

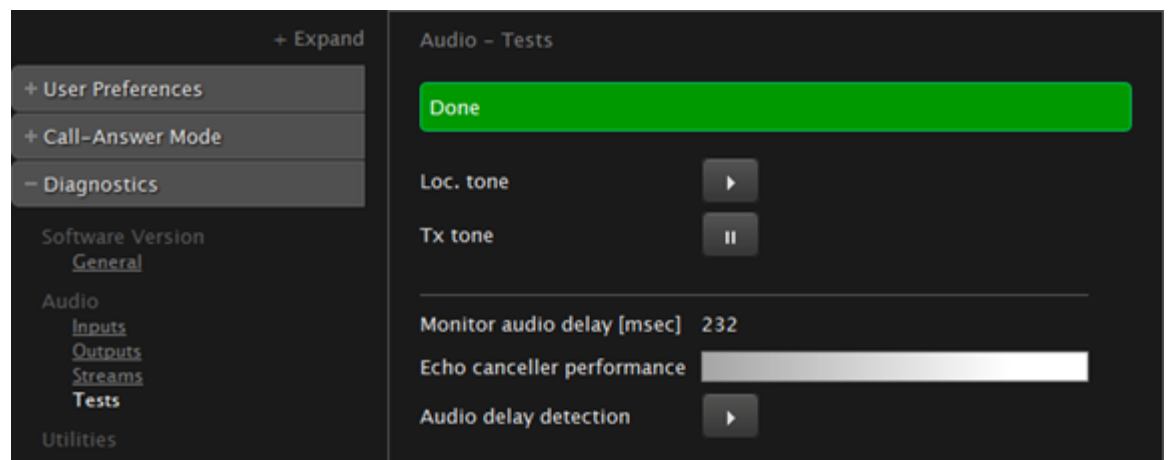


Figure 100: The audio test completed successfully from the web interface

3. Select **Tx tone**  to check the audio output sent from the local endpoint to the connected endpoint. If the test is completed successfully, the **Done** message is displayed.

Important:

If the tone level is not constant but increases and decreases (the tone is amplitude modulated), the HDMI monitor is incompatible with the XT Codec Unit or not set properly.

Possible Causes You may experience audio problems when calling older endpoints that are not fully compliant with more recent standards, and thus not able to recognize and manage recent audio protocols such as Audio G.719 (full band).

Solution The endpoint administrator should disable specific audio codec if there is any compliance issue with older endpoints.

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the audio settings as follows:
 - From the XT Series web interface, select **Administrator Settings > Calls > Preferences > Audio**.
 - From the endpoint's main menu, select **Configure > Advanced > Calls > Preferences > Audio**.

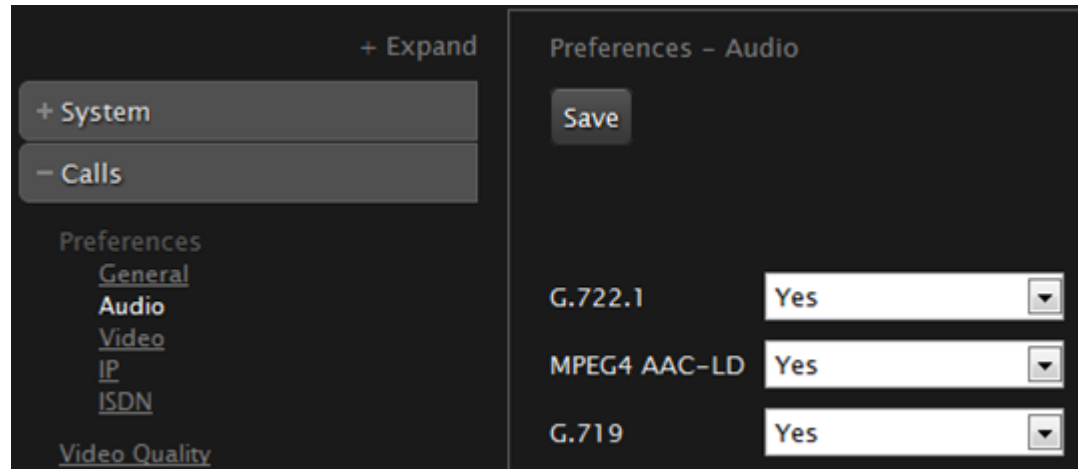


Figure 101: Configuring audio settings from the web interface

2. Disable specific audio codecs by selecting **No** from the lists.
3. From the web interface only, select **Save**.

Echo Cancelling on HDMI Monitors

About this task

An HDMI monitor might insert a delay in the audio, causing an echo.

To improve echo canceller performance, you can use automatic or manual estimation of the audio delay by the XT Codec Unit.

You can also generate the audio delay manually. Then you can train the echo canceller to use the manual estimation as described in this procedure.

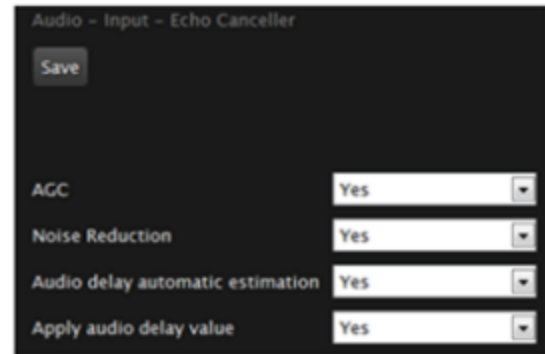
If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

Procedure

1. Access the echo cancellation settings, as follows:
 - From the Scopia XT Series web interface, select **Administrator Settings > I/O connections > Audio-Inputs > Echo canceller**.
 - From the endpoint's Main menu, select **Configure > Advanced > I/O connections > Audio-Inputs > Echo canceller**.



Configuring from Endpoint



Configuring from Web Interface

Figure 102: Configuring echo cancellation settings

2. Set the **Audio delay automatic estimation** field to **Yes**.
This enables the endpoint to constantly measure the audio delay.
3. Set the **Apply audio delay value** field to **Yes**.
This enables the system to fix problems with the audio delay.
4. From the web interface only, select **Save**.
5. If necessary to further fine tune audio delay, perform these steps:
 - a. Navigate to Audio tests as follows:
 - From the endpoint's Main menu, select **Configure > System Status > Diagnostics > Audio > Tests**.
 - From the web interface, select **Diagnostics > Audio > Tests**.

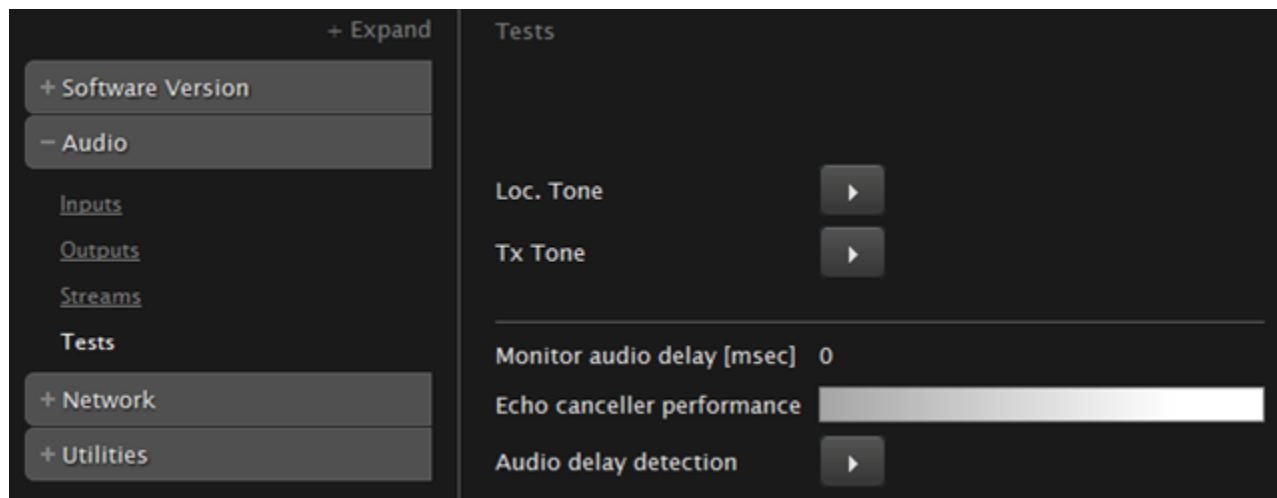


Figure 103: Testing the audio from the web interface

b. Bring the Microphone Pod at about 1 m (3 feet) from the monitor. Keep silent.

c. Navigate to **Audio delay detection**  and select **Yes**.

The monitor generates an evaluation noise and the Codec Unit estimates the audio delay introduced by the monitor. The display shows the audio delay in milliseconds.

The XT Codec Unit uses this manually adjusted delay to calculate the audio delay and improve the echo canceller performance.

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

Resolving Monitor Display Problems

Problem The system displays a flickering or blank screen.

Solution The rear panel of the XT Codec Unit features 2 HD outputs for connecting a main and auxiliary screen. For cabling, see the cabling diagram in the *Quick Setup Guide*.

Your system administrator must configure the system for correct video resolution.

When you are not in a call, you can set the refresh frequency of the monitor display:

- Set to 50 Hz by pressing  then **5**.
- Set to 60 Hz by pressing  then **6**.

Problem The system displays a blank screen.

Solution Verify the power cord of the XT Codec Unit is connected properly at both ends.

Solution Verify the monitor's power cord is connected properly at both ends.

Solution Check that the monitor power switch is set to ON.

Solution Verify the XT Codec Unit's LED is on. If the LED is blinking, press the Power key  on the XT Remote Control Unit.

Solution Make sure the XT Codec Unit output is properly connected to the monitor input. Make sure the monitor/DVI cable is connected properly at both ends.

Problem The screen layout appears to be cropped.

Solution Configure the monitor layout as described below.

1. From the endpoint's main menu, select **Configure > Quick Setup**.
2. Select **Next** to navigate to the **Configure Monitor** page.
3. Follow the instructions on the screen to adjust the image.

If necessary, refer to [Adjusting the Image Position](#) on page 85 for operational information.

Problem The system menus or the remote presentation appears to be cropped.

Solution Adjust the way the image appears on the monitor. To see your adjustments in real-time, we recommend performing this procedure from the endpoint itself.

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

1. Access the monitor settings as follows:
 - From the endpoint's main menu, select **Configure > Advanced > I/O connections > Monitor > Graphic Adjustments**.
 - From the XT Series web interface, select **Administrator settings > I/O connections > Monitor > Graphic Adjustments**.
2. Navigate to the monitor requiring adjustment (**Monitor HD1** or **Monitor HD2**).
3. Select your preferred image view mode:

Table 41: Adjustment options for the monitor

Option	Description
Adjustment Mode	Select to adjust where the windows are displayed on the monitor: • Menu: Select to adjust the system menus only. • Menu, presentation (default): Select to adjust both the system menu and presentation, local or received.
Top	Drag the sliders to the required sizes until the menu or presentation borders are visible on the monitor.
Left	
	 Important: You can also adjust the image for the monitor displaying the system menu, in the quick setup

Option	Description
Bottom	wizard as described in Adjusting the Image Position on page 85.
Right	

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

Resolving Camera Issues

Problem I cannot see the camera's output after setting up.

You can also check the camera's output remotely from the Scopia XT Series web interface by selecting **More Actions > Web Video**:

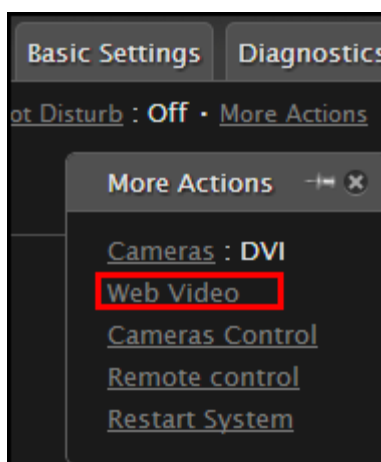


Figure 104: Remotely monitoring your camera's

Problem I can see the camera's output, but I cannot move the camera.

Solution Change the video source to the correct camera, as described below.

1. Select **Control Camera** from the Main menu (or from the In-Call menu, during a call) and press **ok/menu**.
2. Press **ok/menu** again.

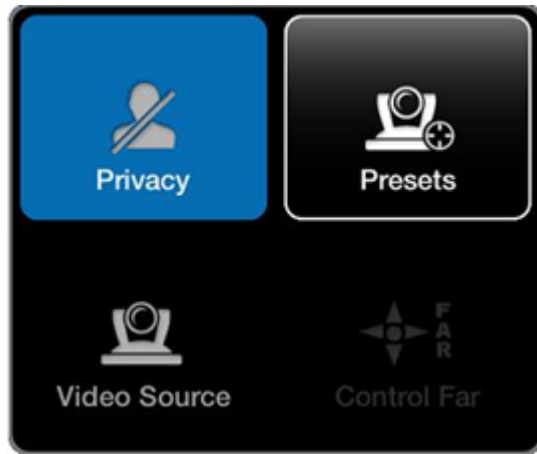


Figure 105: Selecting a video source

3. Select **Video Source**.

Solution Ensure the camera is correctly connected to the system. For details, see the *Installation Guide for the Scopia XT Series*.

Solution Make sure the **Moving** setting is enabled.

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

1. Access the general camera settings by doing one of the following:
 - From the endpoint's main menu, select **Configure > Advanced > I/O connections > Cameras > HD1** from the Main menu.
 - From the XT Series web interface, select **Administrator Settings > I/O connections > Cameras > HD1**.

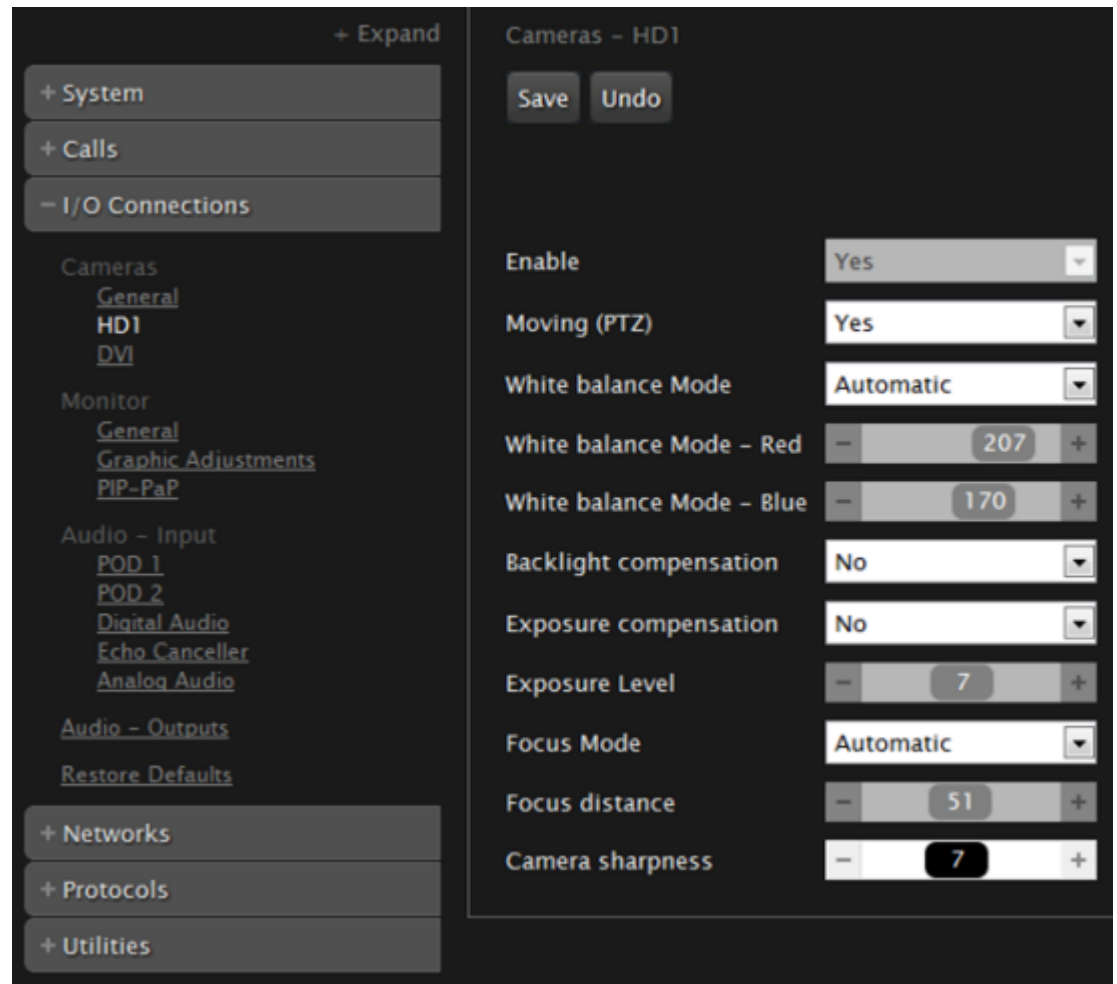


Figure 106: Enabling the Moving setting

2. Make sure that the **Moving** field is set to **Yes**.
3. From the web interface only, select **Save**.

Resolving IP Address Problems

Problem Cannot configure the IP address.

Possible Causes If the icon for no network connection  appears and the system displays 0.0.0.0 as its assigned IP address, the system is not connected to network or has an invalid IP address (for details on viewing the system's IP address, see [Viewing System Information for Customer Support](#) on page 152).

Solution Make sure the GLAN cable is connected properly at both ends: to the network socket and to the GLAN1 port of the XT Codec Unit, as shown in [Figure 107: GLAN1 port](#) on page 163.

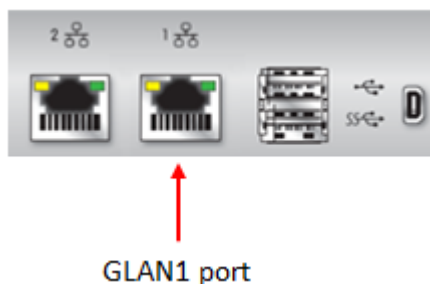


Figure 107: GLAN1 port

! Important:

If the GLAN2 port is enabled and in use, check that it is properly connected.

Solution Assign a valid IP address to the system on GLAN1 or GLAN2, as described in [Configuring IP Addresses](#) on page 118.

Possible Causes The system is capable of detecting IP/MAC addresses conflicts in a network. The conflict occurs with static IP addresses if administrators have inadvertently attributed the same IP addresses to devices or with dynamic IP addresses due to a DHCP server problem.

Solution Verify that another the IP address defined for this endpoint is unique in the network. If there is an address conflict, redefine the IP address.

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

1. From the endpoint's main menu, select **Configure > Quick Setup**.
2. Press **Next** several times until the **Configure TCP/IP** screen appears.



Figure 108: Configuring IP address

3. Enter the IP address.

4. Select **Next**.
5. Select **Done**.

Problem The system does not make calls due to a network error.

Possible Causes The network is based on IPv6 and the endpoint is configured to support only IPv4.

Solution Enable the endpoint to support IPv6.

If configuring from the endpoint, you must first enable advanced configuration, as described in [Maintaining the Scopia XT Series Locally from the Endpoint](#) on page 73.

1. Access the general network settings, as follows:
 - From the XT Series web interface, select **Administrator settings > Networks > Preferences > General**.
 - From the endpoint's main menu, select **Configure > Advanced > Networks > Preferences > General**.

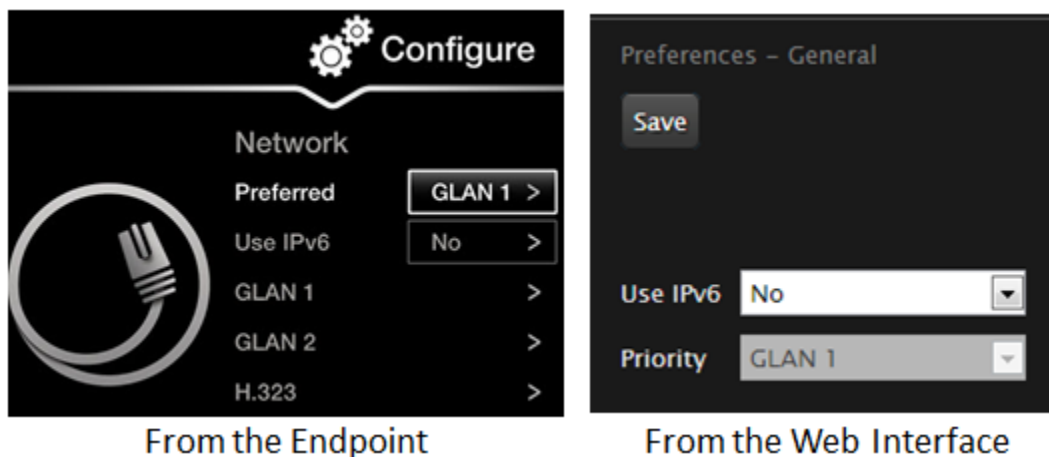


Figure 109: Setting network preferences

2. Set the **Use IPv6** field to **Yes**.
3. From the web interface only, select **Save**.

Resolving XT Remote Control Unit Problems

Problem The XT Remote Control Unit does not function.

Solution Replace the battery, as described in [Installing the Batteries of the XT Remote Control Unit](#) on page 59. When the XT Remote Control Unit's battery power is low, an icon appears in the system menus letting you know that you should replace the battery:

-  Half-charged Battery
-  Low Battery

Solution If the battery power is not low, configure the XT Remote Control Unit code on the XT Codec Unit to the same number that it is set on the XT Remote Control Unit, as described in [Pairing an XT Remote Control Unit with a XT Codec Unit](#) on page 71).

Solution If you still experience problems, reconfigure the XT Remote Control Unit code to be a number between 01-04, inclusive.

Restoring Default User Settings

About this task

This procedure explains how to restore the default settings if necessary, from the endpoint itself.

Before you begin

- Turn on the Scopia XT Series unit.
- Verify that you have the four-digit PIN code required to make changes to the system settings. The default PIN code is 1234.

Procedure

1. From the endpoint's main menu, select **Configure** > **General**.

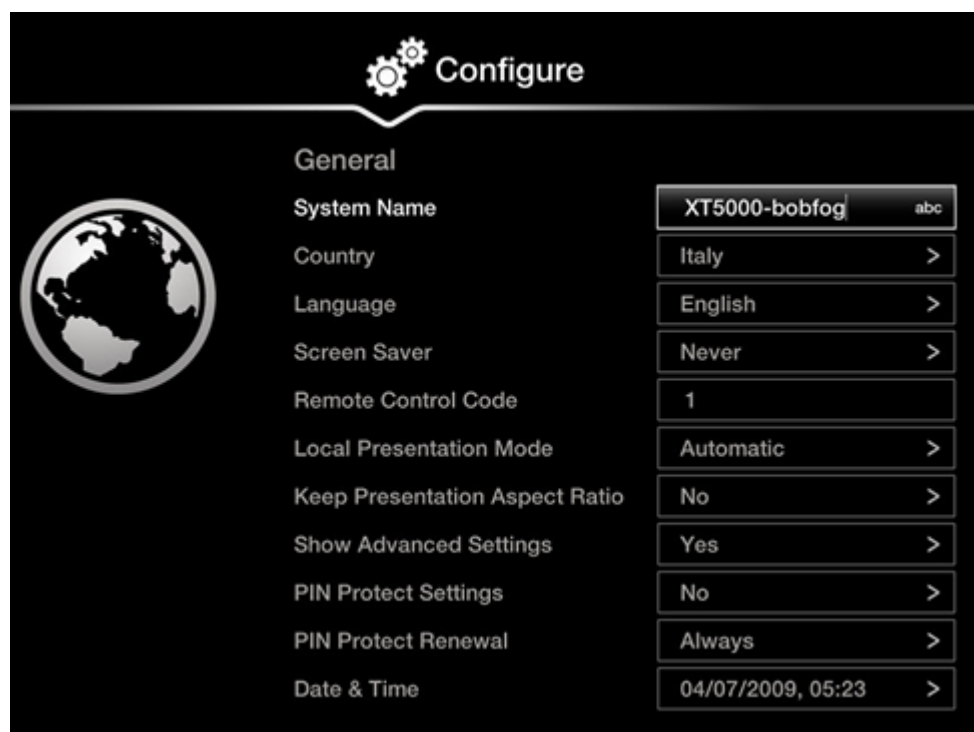


Figure 110: Enabling advanced settings

2. Set **Show Advanced Settings** to **Yes**.

3. Press the  Back key on the XT Remote Control Unit.
4. Select **Advanced**.
5. Enter your four-digit PIN code, and press **ok/menu**. The default PIN code is 1234.
6. Select **Utilities** > **Restore System** > **Factory Defaults**.



Figure 111: Restoring factory default settings

7. Press **ok/menu**, and select **Yes**.
The default settings are restored.

Glossary of Terms for Scopia Solution

1080p

See [Full HD](#) on page 170.

2CIF

2CIF describes a video resolution of 704 x 288 pixels (PAL) or 704 x 240 (NTSC). It is double the width of CIF, and is often found in CCTV products.

2SIF

2SIF describes a video resolution of 704 x 240 pixels (NTSC) or 704 x 288 (PAL). This is often adopted in IP security cameras.

4CIF

4CIF describes a video resolution of 704 x 576 pixels (PAL) or 704 x 480 (NTSC). It is four times the resolution of CIF and is most widespread as the standard analog TV resolution.

4SIF

4SIF describes a video resolution of 704 x 480 pixels (NTSC) or 704 x 576 (PAL). This is often adopted in IP security cameras.

720p

See [HD](#) on page 173.

AAC

AAC is an audio codec which compresses sound but with better results than MP3.

Alias

In H.323, an alias represents the unique name of an endpoint. Instead of dialling an IP address to reach an endpoint, you can dial an alias, and the gatekeeper resolves it to an IP address.

Auto-Attendant

Auto-Attendant, also known as video IVR, offers quick access to meetings hosted on MCUs, via a set of visual menus. Participants can select menu options using standard DTMF tones (numeric keypad).

BFCP (Binary Floor Control Protocol)

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.

Bitrate

Bitrate measures the speed of data flow, measured in kbps. Higher video resolutions require higher bitrates to ensure the video is constantly updated, thereby maintaining smooth motion. If you lower the bitrate, you lower the quality of the video. In some cases, you can select a lower bitrate without noticing a significant drop in video quality; for example during a presentation or when a lecturer is speaking and there is very little motion. In video recordings, the bitrate determines the file size for each minute of recording.

Cascaded videoconference

A cascaded videoconference is a meeting distributed over more than one physical MCU, where a master MCU connects to one or more slave MCUs to create a single videoconference. It increases the meeting capacity by combining the resources of several MCUs. This can be especially useful for distributed deployments across several locations, reducing bandwidth usage.

CIF

CIF, or Common Intermediate Format, describes a video resolution of 352 × 288 pixels (PAL) or 352 x 240 (NTSC). This is sometimes referred to as Standard Definition (SD).

Continuous Presence

Continuous Presence enables viewing multiple participants of a videoconference at the same time, including the active speaker. This graphics-intensive work requires scaling and mixing the images together into one of the predefined video layouts. The range of video layouts depends on the type of media processing supported, typically located in the MCU.

CP

See [Continuous Presence](#) on page 168.

Dedicated Endpoint

A dedicated endpoint is a hardware endpoint for videoconferencing assigned to a single user. It is often referred to as a personal or executive endpoint, and serves as the main means of video communications for this user. For example, Scopia XT Executive. It is listed in the organization's LDAP directory as associated exclusively with this user.

Dial Plan

A dial plan defines various dial prefixes to determine the characteristics of a call. For example, dial 8 before a number for a lower bandwidth call, or 6 for an audio-only call, or 5 to route the call to a different branch.

Dial Prefix

A dial prefix is a number added to the start of a dial string to route it to the correct destination, or to determine the type of call. Dial prefixes are defined in the organization's dial plan. For example, dial 9 for an outside line, or dial 6 for an audio only call.

Distributed Deployment

A distributed deployment describes a deployment where the solution components are geographically distributed in more than one network location.

DNS Server

A DNS server is responsible for resolving domain names in your network by translating them into IP addresses.

DTMF

DTMF, or touch-tone dialling, is the tones you hear when you dial on a touch-tone telephone.

E.164

E.164 is an address format for dialling an endpoint with a standard telephone numeric keypad, which only has numbers 0 - 9 and the symbols: * and #.

Endpoint

An endpoint is a tool through which people can participate in a videoconference. Its display enables you to see and hear others in the meeting, while its microphone and camera enable you to be seen and heard by others. Endpoints include dedicated endpoints, like Scopia XT Executive, software endpoints

like Scopia Desktop Client, mobile device endpoints like Scopia Mobile, room systems like XT Series, and telepresence systems like Scopia XT Telepresence.

Endpoint Alias

See [Alias](#) on page 167.

FEC

Forward Error Correction (FEC) is a proactive method of sending redundant information in the video stream to preempt quality degradation. FEC identifies the key frames in the video stream that should be protected by FEC. There are several variants of the FEC algorithm. The Reed-Solomon algorithm (FEC-RS) sends redundant packets per block of information, enabling the sender (like the Scopia Elite MCU) to manage up to ten percent packet loss in the video stream with minimal impact on the smoothness and quality of the video.

FECC

Far End Camera Control (FECC) is a feature of endpoints, where the camera can be controlled remotely by another endpoint in the call.

Forward Error Correction

See [FEC](#) on page 170.

FPS

See [Frames Per Second](#) on page 170.

Frame Rate

See [Frames Per Second](#) on page 170.

Frames Per Second

Frames Per Second (fps), also known as the frame rate, is a key measure in video quality, describing the number of image updates per second. The average human eye can register up to 50 frames per second. The higher the frame rate, the smoother the video.

Full HD

Full HD, or Full High Definition, also known as 1080p, describes a video resolution of 1920 x 1080 pixels.

Full screen Video Layout

The full screen view shows one video image. Typically, it displays the remote presentation, or, if there is no presentation, it displays the other participant or a composite of the other participants.

Gatekeeper

A gatekeeper routes audio and video H.323 calls by resolving dial strings (H.323 alias or URI) into the IP address of an endpoint, and handles the initial connection of calls. Gatekeepers also implement the dial plan of an organization by routing H.323 calls depending on their dial prefixes. Scopia Management includes a built-in Scopia Gatekeeper, while ECS is a standalone gatekeeper.

Gateway

A gateway is a component in a video solution which routes information between two subnets or acts as a translator between different protocols. For example, a gateway can route data between the headquarters and a partner site, or between two protocols like the Scopia TIP Gateway, Radvision SIP Gateway, or the Scopia TIP Gateway.

GLAN

GLAN, or gigabit LAN, is the name of the network port on the Scopia XT Series. It is used on the XT Series to identify a 10/100/1000MBit ethernet port.

H.225

H.225 is part of the set of H.323 protocols. It defines the messages and procedures used by gatekeepers to set up calls.

H.235

H.235 is the protocol used to authenticate trusted H.323 endpoints and encrypt the media stream during meetings.

H.239

H.239 is a widespread protocol used with H.323 endpoints, to define the additional media channel for data sharing (like presentations) alongside the videoconference, and ensures only one presenter at a time.

H.243

H.243 is the protocol used with H.323 endpoints enabling them to remotely manage a videoconference.

H.245

H.245 is the protocol used to control a remote endpoint from your local endpoint. It is part of the H.323 set of protocols.

H.261

H.261 is an older protocol used to compress CIF and QCIF video resolutions.

H.263

H.263 is an older a protocol used to compress video. It is an enhancement to the H.261 protocol.

H.264

H.264 is a widespread protocol used with SIP and H.323 endpoints, which defines video compression. Compression algorithms include 4x4 transforms and a basic motion comparison algorithm called P-slices. There are several profiles within H.264. The default profile is the H.264 Baseline Profile, but H.264 High Profile uses more sophisticated compression techniques.

H.264 Baseline Profile

See [H.264](#) on page 172.

H.264 High Profile

H.264 High Profile is a standard for compressing video by up to 25% over the H.264 Baseline Profile, enabling high definition calls to be held over lower call speeds. It requires both sides of the transmission (sending and receiving endpoints) support this protocol. H.264 High Profile uses compression algorithms like:

- CABAC compression (Context-Based Adaptive Binary Arithmetic Coding)
- 8x8 transforms which more effectively compress images containing areas of high correlation

These compression algorithms demand higher computation requirements, which are offered with the dedicated hardware available in Scopia Solution components. Using H.264 High Profile in videoconferencing requires that both the sender and receiver's endpoints support it. This is different from SVC which is an adaptive technology working to improve quality even when only one side supports the standard.

H.320

H.320 is a protocol for defining videoconferencing over ISDN networks.

H.323

H.323 is a widespread set of protocols governing the communication between endpoints in videoconferences and point-to-point calls. It defines the call signaling, control, media flow, and bandwidth regulation.

H.323 Alias

See [Alias](#) on page 167.

H.324M

H.324M is the videoconferencing standard for endpoints connecting via 3G mobile networks. Scopia Mobile, however, uses the same protocols as Scopia Desktop Client.

H.350

H.350 is the protocol used to enhance LDAP user databases to add video endpoint information for users and groups.

HD

A HD ready device describes its high definition resolution capabilities of 720p, a video resolution of 1280 x 720 pixels.

High Availability

Deploying additional servers ensures better service by protecting your organization from server downtime through various strategies including deployment of redundant servers managed by load balancing systems.

High Definition

See [HD](#) on page 173.

High Profile

See [H.264 High Profile](#) on page 172.

HTTPS

HTTPS is the secured version of the standard web browser protocol HTTP. It secures communication between a web browser and a web server through authentication of the web site and encrypting

communication between them. For example, you can use HTTPS to secure web browser access to the web interface of many Scopia Solution products.

Image Resolution

See [Resolution](#) on page 177.

kpbs

Kilobits per second (kbps) is the standard unit to measure bitrate, measuring the throughput of data communication between two devices. Since this counts the number of individual bits (ones or zeros), you must divide by eight to calculate the number of KB (kilobytes) per second.

LDAP

LDAP is a widespread standard database format which stores network users. The format is hierarchical, where nodes are often represented as *branch location > department > sub-department*, or *executives > managers > staff members*. The database standard is employed by most user directories including Microsoft Active Directory, IBM Sametime and others. H.350 is an extension to the LDAP standard for the videoconferencing industry.

Lecture Mode

Scopia Desktop's lecture mode allows the participant defined as the lecturer to see all the participants, while they see only the lecturer. All participants are muted except the lecturer, unless a participant asks permission to speak and is unmuted by the lecturer. This mode is tailored for distance learning, but you can also use it for other purposes like when an executive addresses employees during company-wide gatherings.

Load balancer

A load balancer groups together a set (or cluster) of servers to give them a single IP address, known as a virtual IP address. It distributes client service requests amongst a group of servers. It distributes loads according to different criteria such as bandwidth, CPU usage, or cyclic (round robin). Load balancers are also known as application delivery controllers (ADC).

Location

A location is a physical space (building) or a network (subnet) where video devices can share a single set of addresses. A distributed deployment places these components in different locations, often connected via a VPN.

MCU

An MCU, or Multipoint Control Unit, connects multiple endpoints into a single videoconference. It typically manages the audio mixing and video layouts, adjusting the output to suit each endpoint's capabilities.

MCU service

See [Meeting Type](#) on page 175.

Meeting Type

Meeting types (also known as MCU services) are meeting templates which determine the core characteristics of a meeting. For example, they determine if the meeting is audio only or audio and video, they determine the default video layout, the type of encryption, PIN protection and many other features. Meeting types are created in the MCU. You can invoke a meeting type by dialing its prefix in front of the meeting ID.

Moderator

A moderator is a participant with special rights in a videoconference, including muting the sound and video of other participants, inviting new participants, disconnecting participants, defining a meeting PIN to restrict access, determining video layouts, and closing meetings. In Scopia Desktop Client, an owner of a virtual room is the moderator when the room is protected by a PIN. Without this protection, any participant can assume moderator rights.

MTU

The MTU, or Maximum Transmission Unit, is the maximum size of data packets sent around your network. This value must remain consistent for all network components, including servers like the MCU and Scopia Desktop Server, endpoints like XT Series and other network devices like LDAP servers and network routers.

Multi-Point

A multi-point conference has more than two participants.

Multi-tenant

Service provider, or multi-tenant, deployments enable one installation to manage multiple organizations. All the organizations can reside as tenants within a single service provider deployment. For example, Scopia Management can manage a separate set of users for each organization, separate local administrators, separate bandwidth policies etc. all within a single multi-tenant installation.

NAT

A NAT, or Network Address Translation device, translates external IP addresses to internal addresses housed in a private network. This enables a collection of devices like endpoints in a private network, each with their own internal IP address, can be represented publicly by a single, unique IP address. The NAT translates between public and private addresses, enabling users to place calls between public network users and private network users.

NetSense

NetSense is a proprietary Radvision technology which optimizes the video quality according to the available bandwidth to minimize packet loss. As the available bandwidth of a connection varies depending on data traffic, NetSense's sophisticated algorithm dynamically scans the video stream, and then reduces or improves the video resolution to maximize quality with the available bandwidth.

Packet Loss

Packet loss occurs when some of the data transmitted from one endpoint is not received by the other endpoint. This can be caused by narrow bandwidth connections or unreliable signal reception on wireless networks.

PaP Video Layout

The PaP (Picture and Picture) view shows two images of the same size, presented side by side.

PiP Video Layout

The PiP (Picture In Picture) view shows a video image in the main screen, with an additional smaller image overlapping in the corner. Typically, a remote presentation is displayed in the main part of the screen, and the remote video is in the small image. If the remote endpoint does not show any content, the display shows the remote video in the main part of the screen, and the local presentation in the small image.

Point-to-Point

Point-to-point is a feature where only two endpoints are communicating with each other.

PoP Video Layout

The PoP (Picture out Picture) view shows up to three images of different size, presented side by side. The image on the left is larger, with two smaller images on the right.

Prefix

See [Dial Prefix](#) on page 169.

Q.931

Q.931 is a telephony protocol used to start and end the connection in H.323 calls.

QCIF

QCIF, or Quarter CIF, defines a video resolution of 176 × 144 pixels (PAL) or 176 × 120 (NTSC). It is often used in older mobile handsets (3G-324M) limited by screen resolution and processing power.

Redundancy

Redundancy is a way to deploy a network component, in which you deploy extra units as 'spares', to be used as backups in case one of the components fails.

Registrar

A SIP Registrar manages the SIP domain by requiring that all SIP devices register their IP addresses with it. For example, once a SIP endpoint registers its IP address with the Registrar, it can place or receive calls with other registered endpoints.

Resolution

Resolution, or image/video resolution, is the number of pixels which make up an image frame in the video, measured as the number of horizontal pixels x the number of vertical pixels. Increasing resolution improves video quality but typically requires higher bandwidth and more computing power. Techniques like SVC, H.264 High Profile and FEC reduce bandwidth usage by compressing the data to a smaller footprint and compensating for packet loss.

Room System

A room system is a hardware videoconferencing endpoint installed in a physical conference room. Essential features include its camera's ability to PTZ (pan, tilt, zoom) to allow maximum flexibility of camera angles enabling participants to see all those in the meeting room or just one part of the room.

RTP

RTP or Real-time Transport Protocol is a network protocol which supports video and voice transmission over IP. It underpins most videoconferencing protocols today, including H.323, SIP and the streaming control protocol known as RTSP. The secured version of RTP is SRTP.

RTCP

Real-time Control Transport Protocol, used alongside RTP for sending statistical information about the media sent over RTP.

RTSP

RTSP or Real-Time Streaming Protocol controls the delivery of streamed live or playback video over IP, with functions like pause, fast forward and reverse. While the media itself is sent via RTP, these control functions are managed by RTSP

Sampling Rate

The sampling rate is a measure of the accuracy of the audio when it is digitized. During conversions from analog to digital sound, if you increase the frequency that audio data is collected, or "sampled", you increase the audio quality.

SBC

A Session Border Controller (SBC) is a relay device between two different networks. It can be used in firewall/NAT traversal, protocol translations and load balancing.

Scalability

Scalability describes the ability to increase the capacity of a network device by adding another identical device (one or more) to your existing deployment. In contrast, a non-scalable solution would require replacing existing components to increase capacity.

SD

Standard Definition (SD), is a term used to refer to video resolutions which are lower than HD. There is no consensus defining one video resolution for SD.

Service

Also known as MCU service. See [Meeting Type](#) on page 175.

SIF

SIF defines a video resolution of 352 x 240 pixels (NTSC) or 352 x 288 (PAL). This is often used in security cameras and countries.

SIP

Session Initiation Protocol (SIP) is a signaling protocol for starting, managing and ending voice and video sessions over TCP, TLS or UDP. Videoconferencing endpoints typically are compatible with SIP or H.323, and in some cases (like Scopia XT Series), an endpoint can be compatible with both protocols. As a protocol, it uses fewer resources than H.323.

SIP Server

A SIP server is a network device communicating via the SIP protocol.

SIP URI

See [URI](#) on page 181.

SIP Registrar

See [Registrar](#) on page 177.

Single Sign On

Single Sign On (SSO) automatically uses your network login and password to access different enterprise systems. Using SSO, you do not need to separately login to each system or service in your organization.

SNMP

Simple Network Management Protocol (SNMP) is a protocol used to monitor network devices by sending messages and alerts to their registered SNMP server.

Software endpoint

A software endpoint turns a computer or portable device into a videoconferencing endpoint via a software application only. It uses the system's camera and microphone to send image and sound to the other participants, and displays their images on the screen. For example, Scopia Desktop Client or Scopia Mobile.

SRTP

Secure Real-time Transport Protocol (SRTP) adds security to the standard RTP protocol, which is used to send video and audio data between devices in SIP calls using TLS. It offers security via encrypting, authenticating and ensuring message integrity.

SSO

See [Single Sign On](#) on page 179.

Standard Definition

See [SD](#) on page 178.

Streaming

Streaming is a method of delivering multimedia content in one direction. Streaming recipients cannot not use a microphone or camera to communicate back to the videoconference. The content can be a live videoconference, or it can be a stored recording.

STUN

A STUN server enables you to directly dial an endpoint behind a NAT or firewall by giving that computer's public internet address.

SVC

SVC extends the H.264 codec standard to dramatically increases error resiliency and video quality without the need for higher bandwidth. It is especially effective over networks with high packet loss (like wireless networks) which deliver low quality video. It splits the video stream into layers, comprising a small base layer and then additional layers on top which enhance resolution, frame rate and quality. Each additional layer is only transmitted when bandwidth permits. This allows for a steady video transmission when available bandwidth varies, providing better quality when the bandwidth is high, and adequate quality when available bandwidth is poor.

SVGA

SVGA defines a video resolution of 800 x 600 pixels.

SQCIF

SQCIF defines a video resolution of 128 x 96 pixels.

Switched video

Switching is the process of redirecting video as-is without transcoding, so you see only one endpoint's image at a time, usually the active speaker, without any video layouts or continuous presence (CP). Using video switching increases the port capacity of the MCU by four times.

Important:

Use switched video only when all endpoints participating in the videoconference support the same resolution. If a network experiences high packet loss, switched video might not be displayed properly for all endpoints in the videoconference.

SXGA

SXGA defines a video resolution of 1280 x 1024 pixels.

Telepresence

A telepresence system combines of two or more endpoints together to create a wider image, simulating the experience of participants being present in the same room. For example, Scopia XT Telepresence.

TLS

TLS enables network devices to communicate securely by exchanging certificates, to provide authentication of the devices and encryption of the communication between them.

Transcoding

Transcoding is the process of converting video into different sizes, resolutions or formats. This enables multiple video streams to be combined into one view, enabling continuous presence, as in a typical videoconferencing window.

UC (Unified Communications)

UC, or unified communications deployments offer solutions covering a wide range of communication channels. These include audio (voice), video, text (IM or chat), data sharing (presentations), whiteboard sharing (interactive annotations on shared data).

URI

URI is an address format to locate a device on a network. For a SIP call, the URI consists of the endpoint's name or number, followed by the SIP server domain name. For example, *<endpoint name>@<SIP server domain name>* or *user@domain_name.com*.

URI Dialling

Accessing a device via its [URI](#) on page 181.

VFU

See [Video Fast Update \(VFU\)](#) on page 182.

VGA

VGA defines a video resolution of 640 x 480 pixels.

Videoconference

A videoconference is a meeting of more than two participants with audio and video using endpoints. Professional videoconferencing systems can handle many participants in single meetings, and multiple simultaneous meetings, with a wide interoperability score to enable a wide variety of endpoints to join the same videoconference. Typically you can also share PC content, like presentations, to other participants.

Video Fast Update (VFU)

Video Fast Update (VFU) is a request for a refreshed video frame, sent when the received video is corrupted by packet loss. In response to a VFU request, the broadcasting endpoint sends a new intra-frame to serve as the baseline for the ongoing video stream.

Video Layout

A video layout is the arrangement of participant images as they appear on the monitor in a videoconference. If the meeting includes a presentation, a layout can also refer to the arrangement of the presentation image together with the meeting participants.

Video Resolution

See [Resolution](#) on page 177.

Video Switching

See [Switched video](#) on page 180.

Virtual Room

A virtual room in Scopia Desktop and Scopia Mobile offers a virtual meeting place for videoconferences. An administrator can assign a virtual room to the organization's users and conference rooms. Users can send invitations to others with a link bringing participants directly into their virtual room. External participants can download Scopia Desktop or Scopia Mobile free to access a registered user's virtual room and participate in the videoconference.

Waiting Room

A waiting room is a holding place for participants waiting for the host or moderator to join the meeting. While waiting, participants see a static image with the name of the owner's virtual room, with an optional audio message periodically saying the meeting will start when the host arrives.

Webcast

A webcast is a streamed live broadcast of a videoconference over the internet. A Scopia Desktop webcast becomes available when a participant in the videoconference enables the streaming feature. To invite users to the webcast, one of the participants attending the Scopia Desktop videoconference must send this information in an e-mail or an instant message:

- The link to the webcast
 - or
 - The link to the Scopia Desktop portal and the meeting ID
-

WUXGA

WUXGA defines a video resolution of 1920 x 1200 pixels.

XGA

XGA defines a Video resolution of 1024 x 768 pixels.

Zone

Gatekeepers like Scopia ECS Gatekeeper split endpoints into zones, where a group of endpoints in a zone are registered to a gatekeeper. Often a zone is assigned a dial prefix, and usually corresponds to a physical location like an organization's department or branch.

RADVISION[®]

an Avaya company

About Radvision

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

www.radvision.com