RADVISION®
an Avaya company

Scopia XT5000 Endpoint with Embedded Server for IP Office

Administrator Guide

Version 3.2

For Avaya IP Office 8.1



3.2

© 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.

Administrator Guide for Scopia XT5000 Endpoint with Embedded Server for IP Office Version 3.2, June 3, 2013

http://www.radvision.com

Table of Contents

Chapter 1: About the Scopia XT Endpoint for IP Office

Technical Specifications 7

Chapter 2: Planning the Topology of the Scopia XT Endpoint for IP Office Deployment

About the Scopia XT Endpoint for IP Office Embedded MCU 11
Planning the Topology of Scopia XT Endpoint for IP Office with Scopia XT Desktop 12
Planning NAT and Firewall Traversal with Scopia XT Endpoint for IP Office 13
Supporting ISDN Connectivity 15
Implementing External API Control 16
Implementing Port Security for the Scopia XT Endpoint for IP Office 17
Ports to Open on the XT Endpoint 17
Configuring the TCP or UDP Port Range on the Scopia XT Endpoint for IP Office 20

Chapter 3: Getting Started with Managing the XT Endpoint

Initial Workflow for Administrators 22
Managing your XT Endpoint from the Web Interface 24
Accessing XT Endpoint Web Interface 24
Enabling Remote Management on the Scopia XT Endpoint for IP Office 25
Configuring Remote Upgrade Settings 27
Managing your XT Endpoint Locally from the Endpoint 29
Accessing the Main Menu of the XT Endpoint 29
Using the XT Remote Control Unit 30
Pairing an XT Remote Control Unit with a XT Codec Unit 33
Maintaining the XT Endpoint Locally from the Endpoint 35

Chapter 4: Initial Configuration

Registering and Enabling your Scopia XT Endpoint for IP Office license 38
Registering the Scopia XT Endpoint for IP Office to Obtain a License Key 38
Installing and Enabling Licenses which Extend System Functionality 39
Remotely Enabling the License from the Web Interface 40

Enabling the License from the Scopia XT Endpoint for IP Office 43
Performing Basic Configuration 44
Accessing the Quick Setup Procedure 45
Setting the System Name and Language 46
Adjusting the Image Position 48
Configuring Network Settings 49
Configuring Gatekeeper Settings 51
Setting Basic System Information 52
Remotely Setting the System Name and Language 53
Modifying the System's Name on the Titlebar 54
Setting Date and Time 57
Setting the Time Zone 58
Remotely Setting Regional Information 59
Configuring the Screen Saver to Start Automatically 61
Registering the XT Endpoint to IP Office 61
Configuring Video Connections 64
Configuring the Camera Connection 64
Setting up the Monitor Display Modes 68
Configuring Audio Connections 73
Configuring the Microphone 74
Configuring Analog Audio Connections 75
Configuring the Echo Canceller 77
Configuring Audio Outputs 79
Configuring Network Settings 81
Configuring GLAN Use 81
Configuring IP Addresses 81
Configuring Network Connectivity 84
Enabling NAT and Firewall Traversal with Scopia XT Endpoint for IP Office 86
Determining the Priority of Audio versus Video Quality 88
Registering the Scopia XT Endpoint for IP Office with a Gatekeeper 89
Configuring Call Settings 92
Configuring Scopia XT Endpoint for IP Office to use an LDAP Directory 96

Chapter 5: Securing your Scopia XT Endpoint for IP Office

Securing Connections to the XT Endpoint Using TLS 100
Generating a Certificate Signing Request for XT Endpoint 101
Uploading XT Endpoint Certificates 103
Backing Up and Restoring XT Endpoint Certificates 105

Deleting XT Endpoint Certificates 106
Enabling the TLS Connection in XT Endpoint 107
Enabling Encryption for Videoconferences 109

Chapter 6: Maintaining the Scopia XT Endpoint for IP Office

Setting the Administrator PIN Code for the XT Endpoint 112
Setting the User PIN Code for the Scopia XT Endpoint for IP Office 113
Modifying the Username and Password for the XT Endpoint Web Interface 114
Preparing for a Video Call or Videoconference 116
Saving a Camera Position 116
Saving a Camera Position from the Web Interface 118
Setting Your Recording Preferences 119
Setting a Time Limit for Videoconferences 121
Updating Software for Scopia XT Endpoint for IP Office 123
Configuring Remote Upgrade Settings 123
Upgrading the Software Using a PC 125
Upgrading the Scopia XT Endpoint for IP Office Software Using a USB Drive 127

Chapter 7: Troubleshooting the Scopia XT Endpoint for IP Office

Viewing System Information for Customer Support 129
Resolving Problems Connecting Calls 131
Resolving Problems with Audio 132
Echo Cancelling on HDMI Monitors 134
Resolving Monitor Display Problems 136
Resolving Lip Sync Problem 140
Resolving Camera Issues 142
Resolving IP Address Problems 144
Resolving Problems with PC Presentations 146
Resolving XT Remote Control Unit Problems 146
Resolving Problems with Displaying Video 147
How to Retrieve Scopia XT Endpoint for IP Office Logs 149
Retrieving Network Traffic Logs 149
Retrieving System Logs 150
USB Software Upgrade Failure 151
Restoring Default User Settings 152

Chapter 1 | About the Scopia XT Endpoint for IP Office

The Scopia XT Endpoint for IP Office incorporates state-of-the-art video technology for high definition (HD) conferencing, allowing you to locally host videoconferences with the built-in MCU. Videoconferences can include a variety of different endpoints: H.323, SIP, Scopia XT Desktop clients and Scopia Mobile clients (with the Scopia XT Desktop Server), and ISDN endpoints (via Scopia 100 Gateway).

Avaya IP Office connects to the Scopia XT Endpoint for IP Office as a SIP server, allowing to host videoconferences and add Avaya endpoints to videoconferences. Figure 1: A typical Scopia XT Endpoint for IP Office deployment on page 6 shows a typical deployment integrating Scopia XT Endpoint for IP Office with Avaya IP Office.

You can use the Scopia XT Endpoint for IP Office as an MCU only, or as an endpoint by connecting a monitor, camera, and microphone.

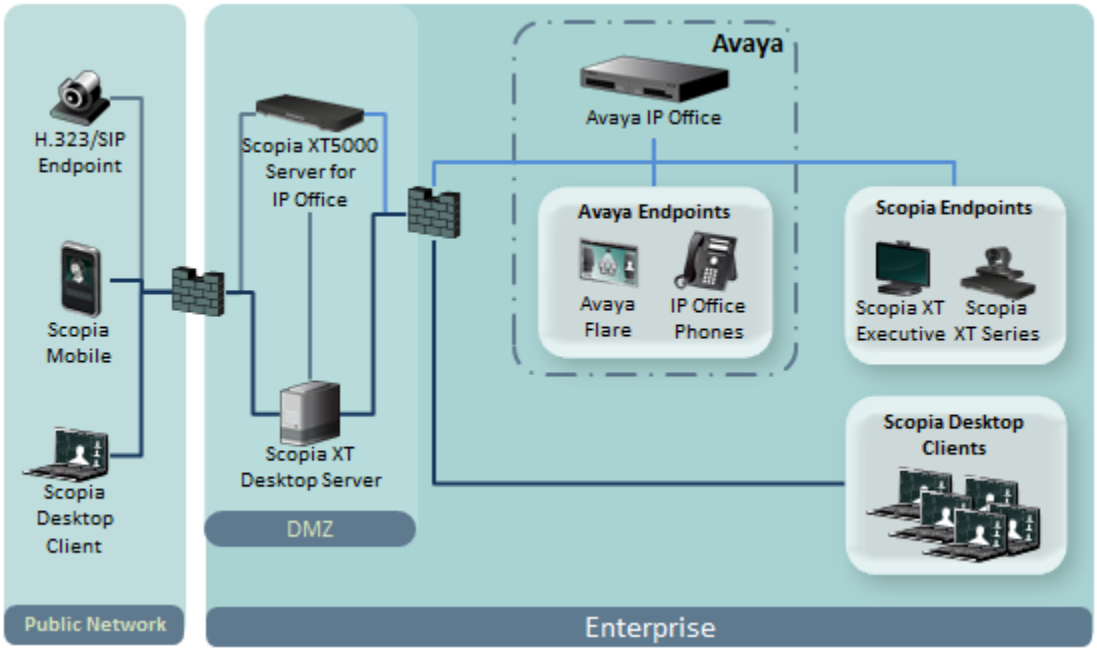


Figure 1: A typical Scopia XT Endpoint for IP Office deployment

This section provides an overview of the general features and capabilities available in the Scopia XT Endpoint for IP Office:

Important:

If you do not register to IP Office, you cannot host videoconferences or use the full functionality of the system. See Registering the XT Endpoint to IP Office on page 61 for details.

- Ability to host videoconferences locally with a high-capacity embedded MCU, without requiring an external MCU deployment.
- Excellent video quality, with resolutions of 720p, and up to 1080p at an unprecedented 60 frames per second (fps), depending on the license.

- 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 license.

  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. 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 a dedicated 3-way Microphone Pod.
- 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).

    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.
- Ability to record videoconferences .
- 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® .
- 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.

Technical Specifications

This section details the system specifications of the Scopia XT Endpoint for IP Office 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 1: Physical device specifications on page 8.
- For specific video, audio, and control features of the system, such as supported codecs and web browsers, see Table 2: Video, audio and control capabilities on page 8.
- For network information of the system, such as network interface cards, see Table 3: Network and security capabilities on page 10.

Table 1: Physical device specifications on page 8 refers to the physical details of the device.

Table 1: Physical device specifications

	Scopia XT Endpoint for IP Office
System power requirements	100-240 VAC, 50/60 Hz, 1.8 A Max. for XT Codec Unit and AC direct for the monitor
Maximum power consumption	100W, AC input 115VA (341 BTU/hr) at 40°C
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: 49.5cm (19.5"), Width: 54cm (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)
Microphone Pod Physical dimensions and Net weight	Diameter: 14cm (5.5"), Weight: 0.3 kg (0.7 lb)
Microphone Pod capabilities	3-way Microphone Pod: 360º range Up to 2 cascaded pods
	Frequency response: 50 – 22,000 Hz

Table 2: Video, audio and control capabilities on page 8 lists the protocols and software requirements.

Table 2: Video, audio and control capabilities

	Scopia XT Endpoint for IP Office
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)
HDMI input formats	1920 x 1080 @ 25, 30, 50, 60fps (optional) 1280 x 720 @ 25, 30, 50, 60fps 720 x 576 @ 50fps 720 x 480 @ 60fps 640 x 480 @ 60fps

	Scopia XT Endpoint for IP Office
Live video resolution	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) 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) 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 (with license; otherwise 720p)
Camera resolution	Up to 1080p 60fps
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 3: Network and security capabilities on page 10 lists the XT Endpoint's network interface and firewall traversal information.

Table 3: Network and security capabilities

	Scopia XT Endpoint for IP Office
Network Interfaces	2 x 10/100/1000 Base-T full-duplex (RJ-45) 2nd GLAN enabled by default
Firewall Traversal	Auto NAT discovery HTTP and STUN H.460.18, H.460.19

Chapter 2 | Planning the Topology of the Scopia XT Endpoint for IP Office Deployment

There are a number of ways that the Scopia XT Endpoint for IP Office 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

- About the Scopia XT Endpoint for IP Office Embedded MCU on page 11
- Planning the Topology of Scopia XT Endpoint for IP Office with Scopia XT Desktop on page 12
- Planning NAT and Firewall Traversal with Scopia XT Endpoint for IP Office on page 13
- Supporting ISDN Connectivity on page 15
- Implementing External API Control on page 16
- Implementing Port Security for the Scopia XT Endpoint for IP Office on page 17

About the Scopia XT Endpoint for IP Office Embedded MCU

The Scopia XT Endpoint for IP Office includes an embedded MCU, allowing XT Endpoint to host videoconferences locally, with up to 9 participants (1 Local and 8 Remote).

If you do not register to IP Office, you cannot host videoconferences or use the full functionality of the system.

The embedded MCU can host both standard definition (SD) and high definition (HD) endpoints simultaneously (see Table 4: Video capabilities for participants hosted by Scopia XT Endpoint for IP Office on page 12 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 4: Video capabilities for participants hosted by Scopia XT Endpoint for IP Office

Maximum Resolution	XT Endpoint
Displayed and transmitted resolution (max)	720p (can be upgraded to 1080p)
Resolution of single participant's video in layout (max)	448p

Important:

The capabilities depend on the selected CP layout.

If the Scopia XT Endpoint for IP Office is used only as an MCU for hosting videoconferences, block the audio and video input from this Scopia XT Endpoint for IP Office during the meeting. For details, see Configuring Call Settings on page 92.

Planning the Topology of Scopia XT Endpoint for IP Office with Scopia XT Desktop

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

For example, when you start a videoconference with the XT Endpoint 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 XT Desktop Client on their computers, or Scopia Mobile on their mobile devices.

If you do not register to IP Office, you cannot host videoconferences or use the full functionality of the system.

The main features of the Scopia XT Endpoint for IP Office include:

- Remote users can easily connect to a meeting hosted by the built-in MCU on the XT Endpoint, 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 XT Desktop Clients.

The Scopia XT Endpoint for IP Office includes the following:

- 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 2: Scopia XT Endpoint for IP Office Deployment on page 13 shows a typical topology for the Scopia XT Endpoint for IP Office solution. For more information, see the *Solution Guide for Scopia Solution*.

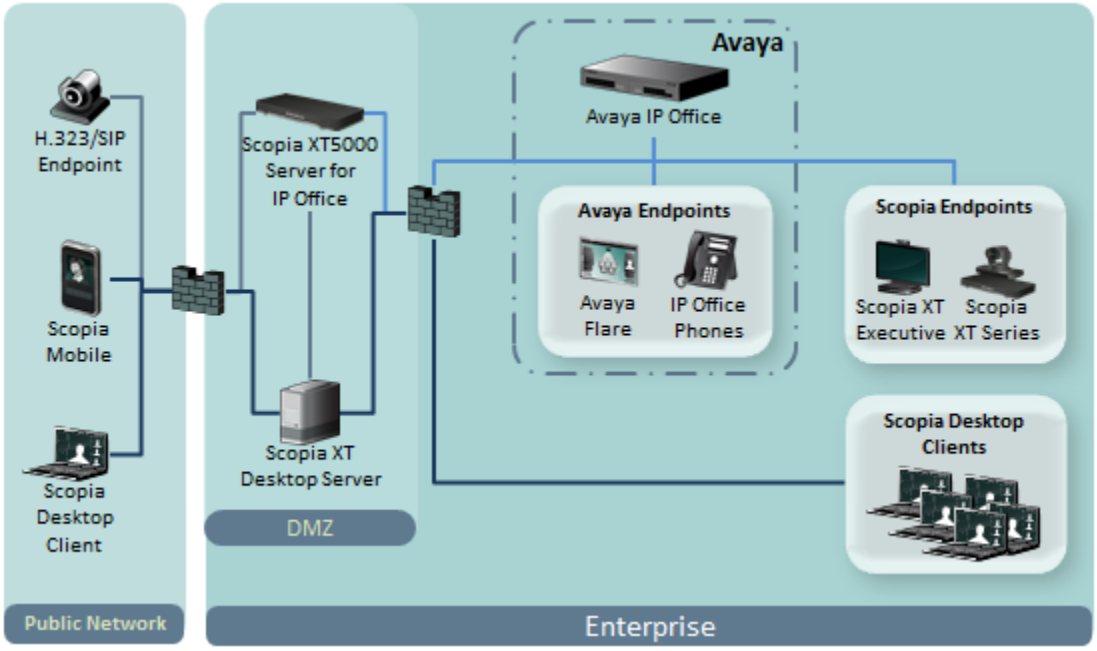


Figure 2: Scopia XT Endpoint for IP Office Deployment

Planning NAT and Firewall Traversal with Scopia XT Endpoint for IP Office

The Scopia XT Endpoint for IP Office 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 Endpoint:

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

  When the XT Endpoint hosts a videoconference with endpoints outside the enterprise (Figure 3: Using an HTTP/STUN Server for NAT and Firewall Traversal on page 14), 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.

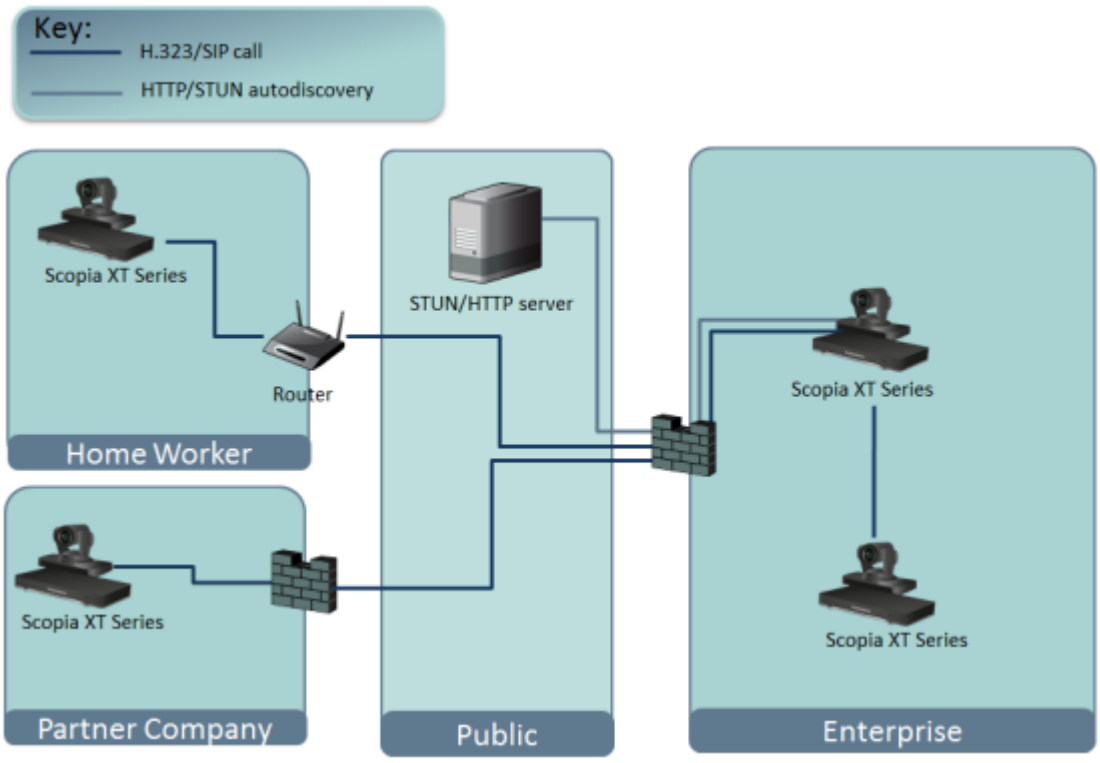


Figure 3: Using an HTTP/STUN Server for NAT and Firewall Traversal

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

- Using the XT Endpoint for NAT and firewall traversal

  In cases where your organization has no sophisticated firewall protection, the XT Endpoint can straddle the two network zones using the two network ports provided on the XT Codec Unit (see Figure 4: Using XT Endpoint for NAT and Firewall Traversal on page 15).

  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 Endpoint which acts as the virtual conference room for all the endpoints.

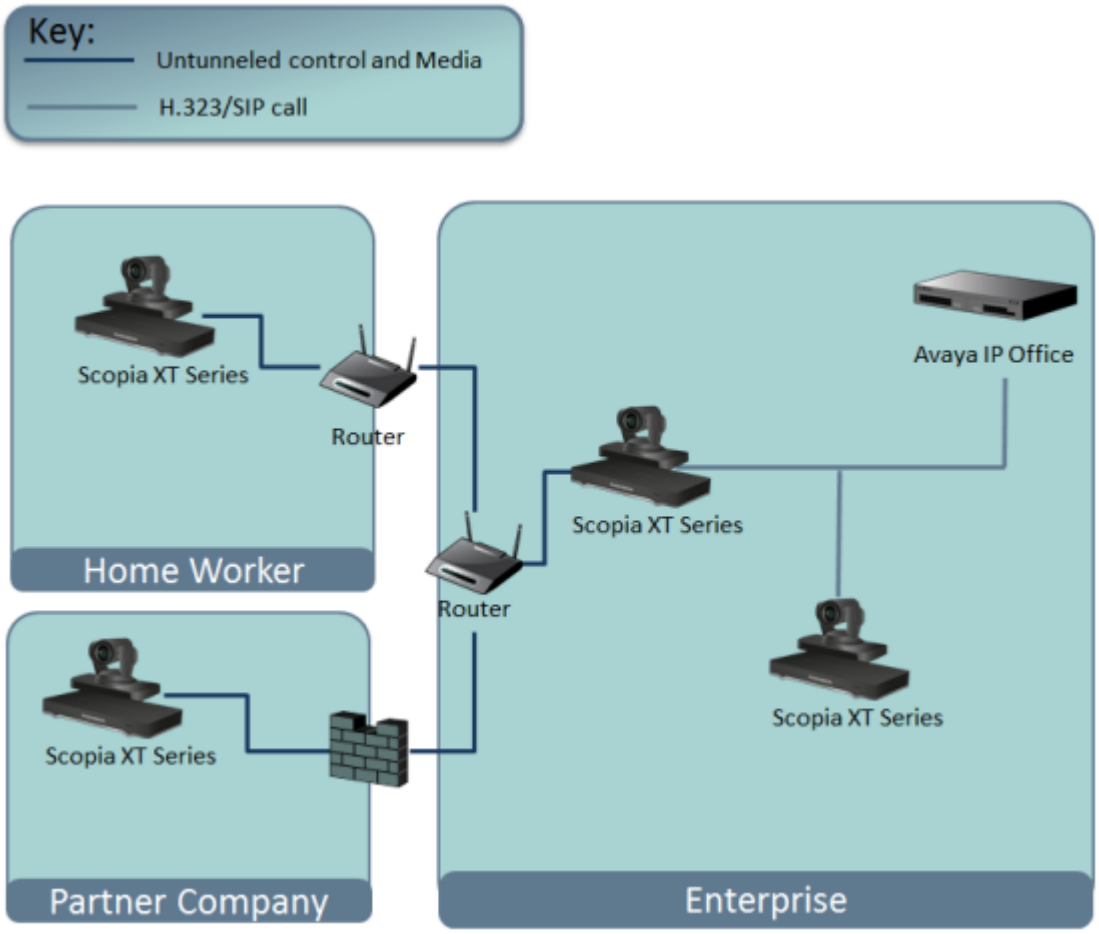


Figure 4: Using XT Endpoint for NAT and Firewall Traversal

Regarding GLAN1 and GLAN2 configuration, the XT Endpoint communicates simultaneously with the public and private network endpoints using IP addresses (see Figure 4: Using XT Endpoint for NAT and Firewall Traversal on page 15).

Supporting ISDN Connectivity

About this task

The Scopia XT Endpoint for IP Office supports ISDN connectivity, allowing calls from endpoints to be routed to the relevant videoconference via the Scopia Gateway for ISDN.

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 Endpoint for IP Office 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 Endpoint web interface, as described in Accessing XT Endpoint Web Interface on page 24.
2. Select **Administrator Settings > Protocols > ISDN**.
3. Configure the IDSN settings as described below:

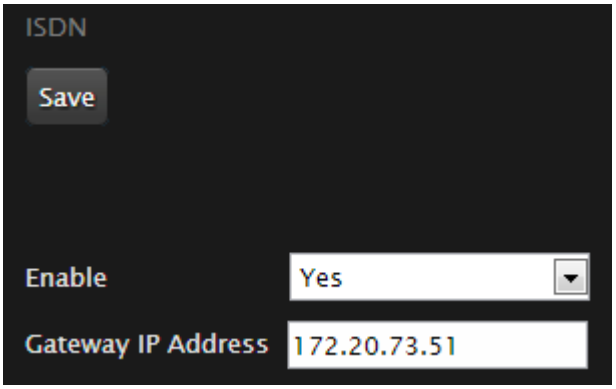


Figure 5: Enabling ISDN connectivity

Table 5: Supporting ISDN Connectivity

Field	Description
Enable	Select **Yes** to allow this Scopia XT Endpoint for IP Office 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 Endpoint for IP Office API (requires integration with AMX, Creston, or Extron control devices). Contact Radvision customer support to receive the

Reference Guide for Scopia XT Endpoint for IP Office API, which includes the list of commands over the Ethernet interface.

Implementing Port Security for the Scopia XT Endpoint for IP Office

The Scopia XT Endpoint for IP Office 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 Endpoint for IP Office and the relevant configuration procedures:

Navigation

- Ports to Open on the XT Endpoint on page 17
- Configuring the TCP or UDP Port Range on the Scopia XT Endpoint for IP Office on page 20

Ports to Open on the XT Endpoint

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

- If you are opening ports that are both to and from the XT Endpoint, see Table 6: Bidirectional Ports to Open on the XT Endpoint on page 18.
- If you are opening outbound ports from the XT Endpoint, see Table 7: Outbound Ports to Open from the Scopia XT Endpoint for IP Office on page 20.

Important:

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

Table 6: Bidirectional Ports to Open on the XT Endpoint

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)	An SNMP manager station	Enables you to discover the system IP address via SNMP	Cannot discover the IP address 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	Optional (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 Endpoint for IP Office on page 20
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 Endpoint for IP Office on page 20

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3338	XML Commands (TCP)	Scopia Control, Scopia XT Desktop Server	Enables communication with Scopia Control and Scopia XT Desktop Server by sending commands and receiving responses	Cannot communicate with Scopia Control application or and Scopia XT Desktop Server	Optional
3478, 3479	STUN (UDP)	STUN Server	Enables endpoints to automatically discover the presence of a firewall or NAT, and to determine their public IP address.	Cannot automatically discover the presence of a firewall or NAT (only manual configuration available)	Optional
5060	SIP (TCP)	Avaya IP Office and any SIP-enabled video network device	Enables SIP call signaling	Cannot connect SIP calls over TCP	Mandatory
5060	SIP (UDP)	Avaya IP Office and any SIP-enabled video network device	Enables SIP call signaling	Cannot connect SIP calls over UDP	Mandatory
5070	BFCP (TCP)	Avaya IP Office and any SIP-enabled video network device	Enables SIP video content (presentation) signaling	No SIP video content available	Mandatory
55003	AT Commands (TCP)	An external controlling device	Enables you to remotely manage the XT Endpoint via API	Cannot send/ receive commands	Optional
55099	Software Upgrade (TCP)	XT Endpoint 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 7: Outbound Ports to Open from the Scopia XT Endpoint for IP Office

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
162	SNMP (UDP)	An SNMP manager station	Enables discovering the system IP address via SNMP	You cannot discover the system IP address via SNMP	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	Optional (recommended if using a gatekeeper)
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 Endpoint for IP Office

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 Endpoint for IP Office 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 Endpoint for IP Office 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 XT Endpoint Locally from the Endpoint on page 35.

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**.

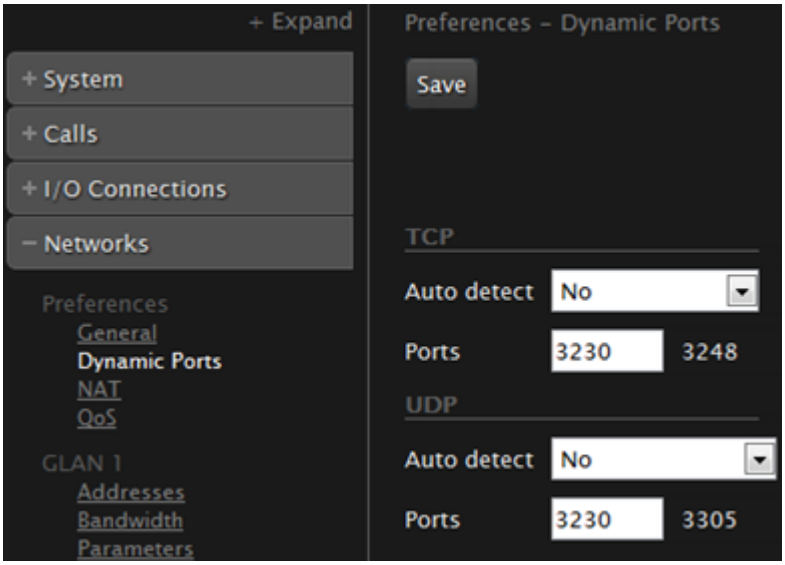


Figure 6: Configuring the TCP or UDP port range from the web interface

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 3 | Getting Started with Managing the XT Endpoint

To get started with configuring the XT Endpoint and customizing it to fit your network requirements, we recommend following the workflow described in Initial Workflow for Administrators on page 22.

You can manage the XT Endpoint as follows:

- From the endpoint

  You can perform all maintenance from the endpoint itself using the XT Remote Control Unit. To do so, you must first enable advanced configuration (see Maintaining the XT Endpoint Locally from the Endpoint on page 35).

- From the web interface

  You can perform all maintenance from the web interface. To do so, remote management must be enabled, as described in Managing your XT Endpoint from the Web Interface on page 24.

For information on configuring settings, such as the language and network settings, see Initial Configuration on page 38.

Navigation

- Initial Workflow for Administrators on page 22
- Managing your XT Endpoint from the Web Interface on page 24
- Managing your XT Endpoint Locally from the Endpoint on page 29

Initial Workflow for Administrators

About this task

To configure the Scopia XT Endpoint for IP Office and customize it for your network requirements, follow the recommended workflow described below. For example, you can secure videoconferences by enabling encryption.

Before you begin

Activate the Scopia XT Endpoint for IP Office and perform the required basic settings, as described in the *Quick Setup Guide for Scopia XT Endpoint for IP Office*.

Procedure

1. Decide how to incorporate the XT Endpoint into your deployment, as described in Planning the Topology of the Scopia XT Endpoint for IP Office Deployment on page 11.

For example, decide where to deploy the XT Endpoint, and the ports to open.

2. Read through and familiarize yourself with the different ways to manage your endpoint from both the web interface and from the endpoint itself, as described in Getting Started with Managing the XT Endpoint on page 22.

3. Register your license to activate the XT Endpoint, as described in Registering and Enabling your Scopia XT Endpoint for IP Office license on page 38.

   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.

4. Configure the endpoint's basic information as described in Initial Configuration on page 38.

   This includes, for example, performing the quick setup wizard, setting your endpoint's time zone, and configuring the network settings.

   Important:

   You may have already performed some of these tasks as part of the initial setup and configuration described in the *Quick Setup Guide for the Scopia XT Endpoint for IP Office* and the *Installation Guide for the Scopia XT Endpoint for IP Office*.

5. Configure the system to work with the IP Office Proxy/Registrar, as described in Registering the XT Endpoint to IP Office on page 61. If you do not register to IP Office, you cannot host videoconferences or use the full functionality of the system.

6. You can prevent users from changing settings you customized for your organization by changing the default administrator PIN code (recommended). See Setting the Administrator PIN Code for the XT Endpoint on page 112.

   To change the default login settings for the XT Endpoint web interface, see Modifying the Username and Password for the XT Endpoint Web Interface on page 114.

   Additionally, you can also set a user PIN code, which is required to access basic settings, such as the endpoint name and time (see Setting the User PIN Code for the Scopia XT Endpoint for IP Office on page 113). By default, a user PIN code is not required to access these settings.

7. You can save the optimal position before the meeting, as described in Preparing for a Video Call or Videoconference on page 116.

8. Configure your camera and microphone settings, as described in:

   - Configuring Video Connections on page 64
   - Configuring Audio Connections on page 73

9. (Optional) If necessary for your organization, you can secure videoconference sessions via encrypted connections and TLS certificates (see Securing your Scopia XT Endpoint for IP Office on page 100).

   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.

10. To update your software, see Updating Software for Scopia XT Endpoint for IP Office on page 123.

If the upgrade requires a license key, see Registering and Enabling your Scopia XT Endpoint for IP Office license on page 38).

Managing your XT Endpoint from the Web Interface

You can configure and control the XT Endpoint 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 Endpoint for IP Office*)
- Change basic settings, such as the interface language (for details, see Performing Basic Configuration on page 44)

You can also configure the XT Endpoint from the endpoint itself by first enabling advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

By default, all computers in the network can manage and upgrade the XT Endpoint remotely. To limit access to specific computers in the network, see Enabling Remote Management on the Scopia XT Endpoint for IP Office on page 25.

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

Navigation

- Accessing XT Endpoint Web Interface on page 24
- Enabling Remote Management on the Scopia XT Endpoint for IP Office on page 25
- Configuring Remote Upgrade Settings on page 27

Accessing XT Endpoint Web Interface

About this task

This procedure describes how to access the XT Endpoint web interface. The XT Endpoint 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 Endpoint login page opens.

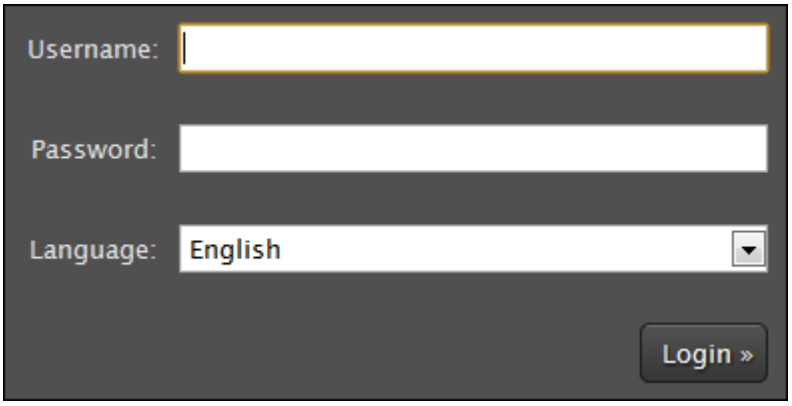


Figure 7: Logging into the XT Endpoint web interface

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 Modifying the Username and Password for the XT Endpoint Web Interface on page 114.

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

4. Select **Login**.

Enabling Remote Management on the Scopia XT Endpoint for IP Office

About this task

Remote management on your Scopia XT Endpoint for IP Office is enabled by default. You can configure the XT Endpoint 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 Endpoint web interface.

To remotely upgrade the XT Endpoint, you must also enable remote downloads, as described in Configuring Remote Upgrade Settings on page 27.

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

See Maintaining the Scopia XT Endpoint for IP Office on page 112 for information on maintenance tasks to configure and manage your XT Endpoint.

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 XT Endpoint Locally from the Endpoint on page 35.

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

Procedure

1. Access the remote management settings, as follows:
   - From the XT Endpoint 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.

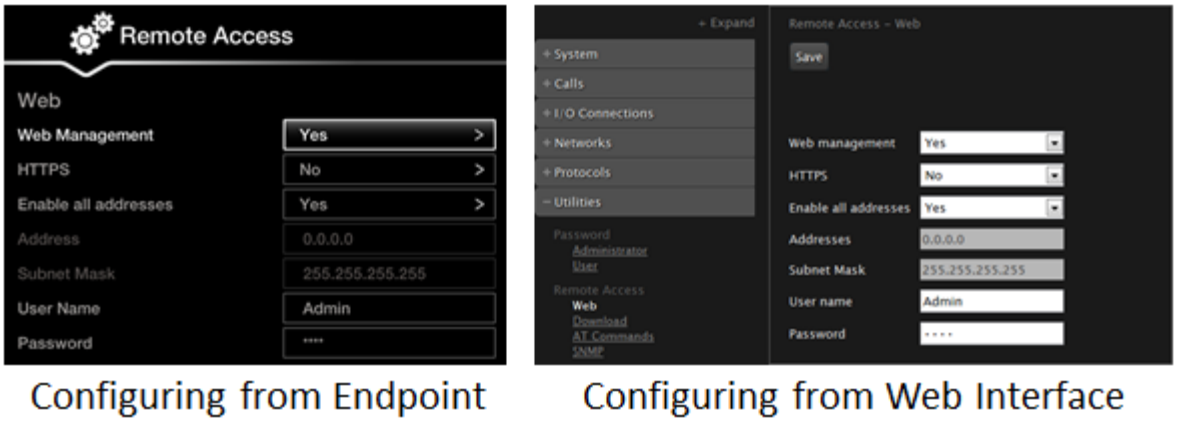


Figure 8: Configuring remote management on XT Endpoint

2. Set the fields as described in Table 8: Configuring remote management on XT Endpoint on page 26.

Table 8: Configuring remote management on XT Endpoint

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 XT Endpoint from its web interface. • Select **No** to disable remote management of the XT Endpoint 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 XT Endpoint 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.

Field Name	Description
Enable all addresses	Allow access to remote management for all or specific PCs, as follows: • Select **Yes** to enable access to XT Endpoint 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 XT Endpoint.
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 XT Endpoint remotely.

3. From the web interface only, select **Save**.
4. To perform remote upgrades, enable remote downloads as described in Configuring Remote Upgrade SettingsConfiguring Remote Upgrade Settings on page 0 .

Configuring Remote Upgrade Settings

About this task

In order to upgrade your Scopia XT Endpoint for IP Office 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 Endpoint web interface.

Before you begin

- If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.
- 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 Endpoint for IP Office on page 25.

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 Endpoint web interface, select **Configure** > **Advanced** > **Utilities** > **Remote Access** > **Download**.

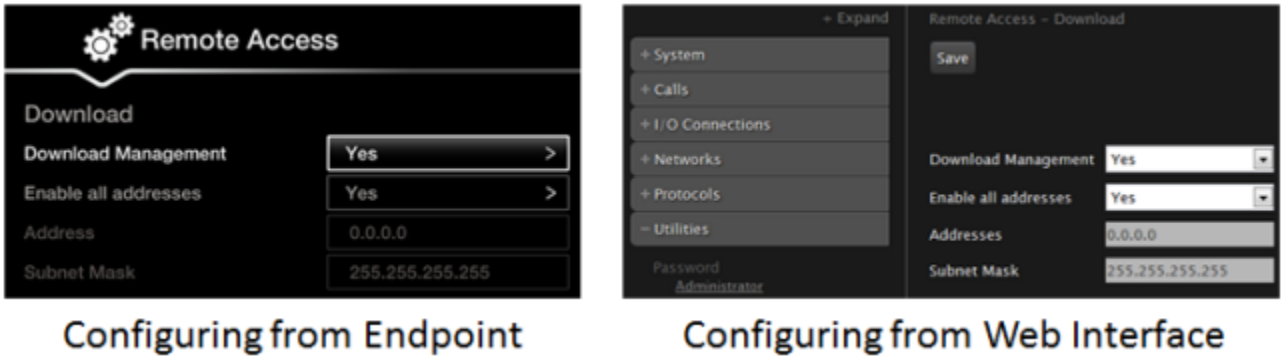


Figure 9: Enabling remote access to the XT Endpoint

2. Set the fields as described in Table 9: Enabling remote upgrade on page 28.

Table 9: 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, as follows: • Select **Yes** to enable remote downloads to the XT Endpoint. • Select **No** to disable remote downloads to the XT Endpoint.
Enable all addresses	Allow access to the XT Codec Unit from all or specific PCs, as follows: • Select **Yes** to enable access to XT Endpoint 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.

Field Name	Description
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 XT Endpoint.
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.

3. From the web interface only, select **Save**.
4. To upgrade the XT Endpoint, see Updating Software for Scopia XT Endpoint for IP Office on page 123.

Managing your XT Endpoint Locally from the Endpoint

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

To perform advanced configuration XT Endpoint from the endpoint itself, you must first enable advanced configuration as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

See the following topics for more information:

Navigation

- Accessing the Main Menu of the XT Endpoint on page 29
- Using the XT Remote Control Unit on page 30
- Maintaining the XT Endpoint Locally from the Endpoint on page 35

Accessing the Main Menu of the XT Endpoint

About this task

After switching on the XT Endpoint, 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 (license required)
- 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 XT Endpoint 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 30).

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 (license required)
   - **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 45).

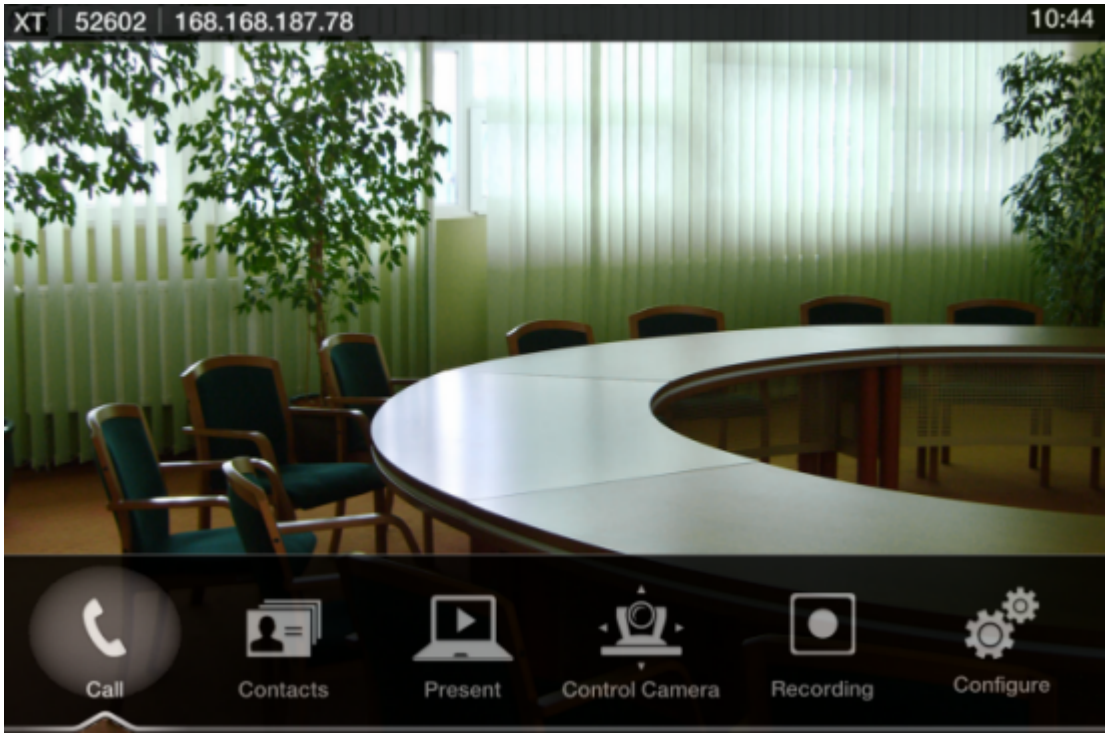


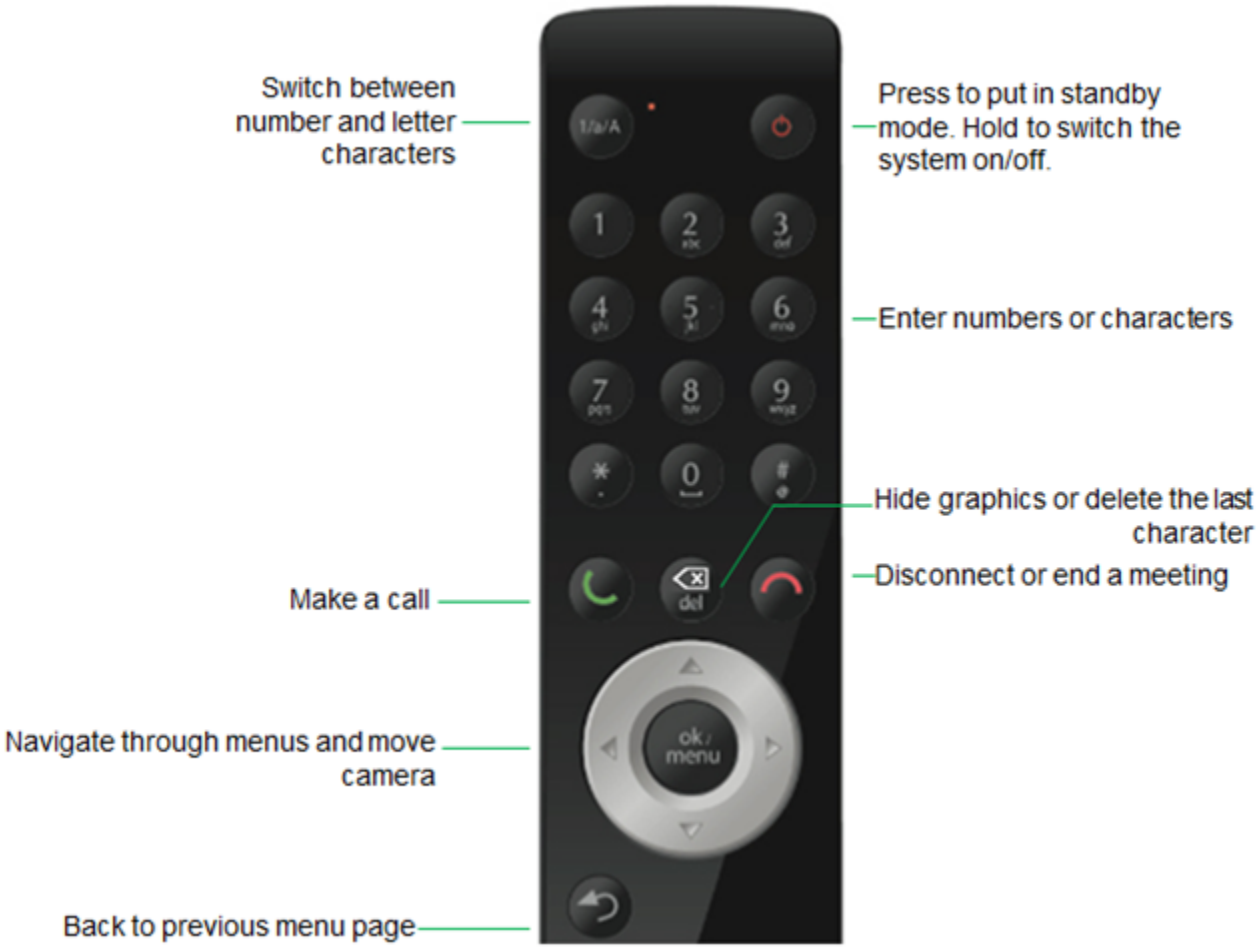
Figure 10: Main menu

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 11: The new XT Remote Control Unit on page 31 describes the functions of the XT Remote Control Unit.



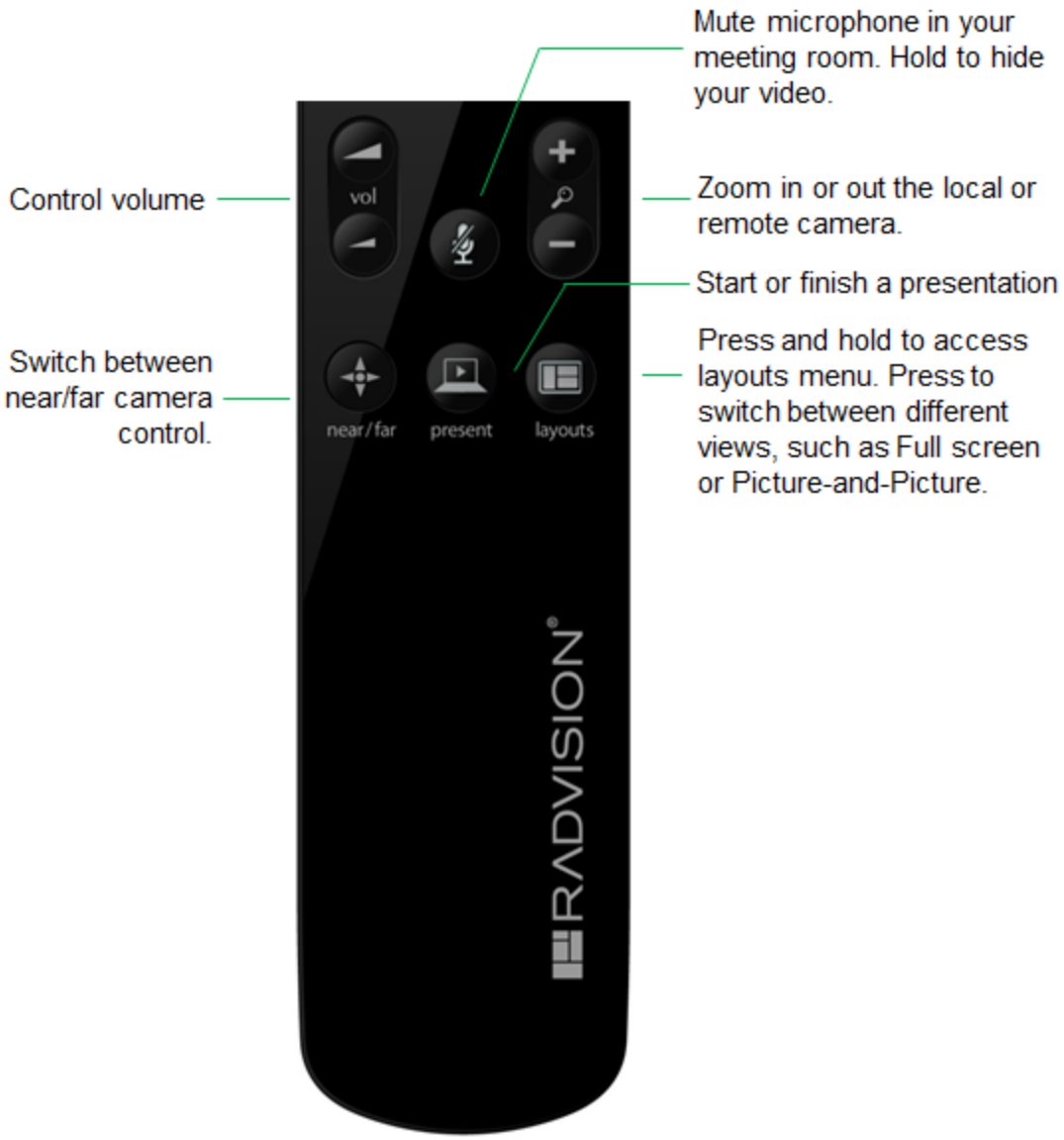


Figure 11: The new XT Remote Control Unit

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.

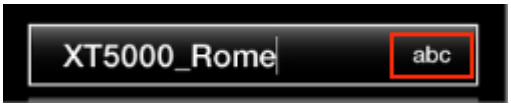
  Important:

  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 Endpoint 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**.

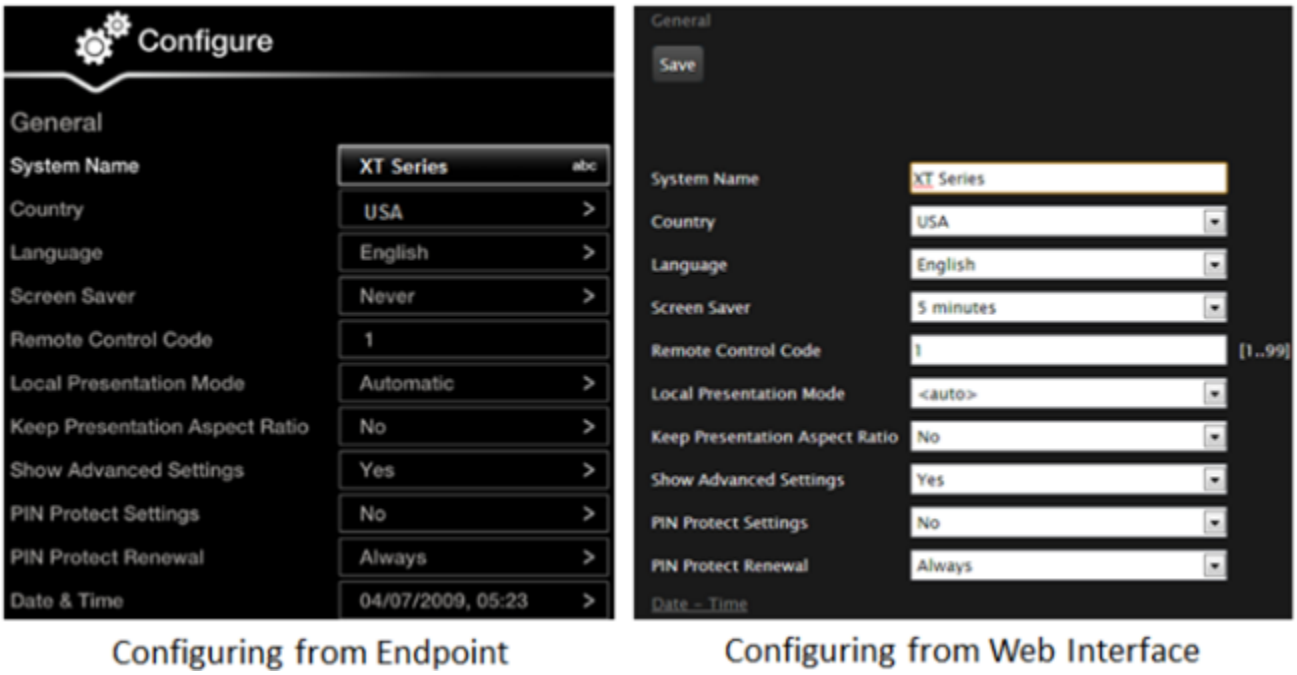


Figure 12: Setting the XT Remote Control Unit Code

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 13: 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 XT Endpoint Locally from the Endpoint

About this task

To perform advanced configuration and maintain the Scopia XT Endpoint for IP Office from the endpoint itself, you must first perform this procedure to access advanced settings. For example, you can upgrade the XT Endpoint. For more information about maintaining the XT Endpoint, see Maintaining the Scopia XT Endpoint for IP Office on page 112.

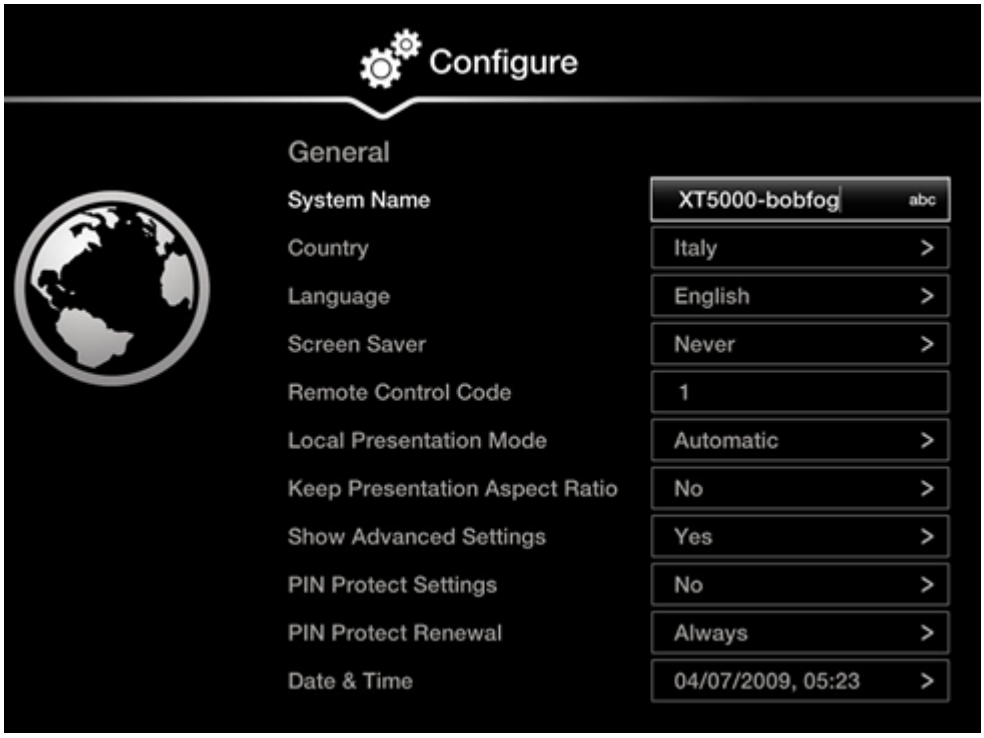
You can also perform advanced configuration from the web interface. See Managing your XT Endpoint from the Web Interface on page 24 for details.

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**.



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 14: Advanced configuration screen

6. We recommend changing the default administrator password, as described in Setting the Administrator PIN Code for the XT Endpoint on page 112.

Chapter 4 | Initial Configuration

After connecting the system and powering it on as described in *Installation Guide for Scopia XT Endpoint for IP Office*, perform the initial configuration as described in these sections:

Navigation

- Registering and Enabling your Scopia XT Endpoint for IP Office license on page 38
- Performing Basic Configuration on page 44
- Registering the XT Endpoint to IP Office on page 61
- Configuring Video Connections on page 64
- Configuring Audio Connections on page 73
- Configuring Network Settings on page 81

Registering and Enabling your Scopia XT Endpoint for IP Office license

About this task

To activate the features of your XT Endpoint, 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 Endpoint for IP Office to Obtain a License Key on page 38.
2. Enable the license from either the endpoint or the web interface:
   - Remotely Enabling the License from the Web Interface on page 40
   - Enabling the License from the Scopia XT Endpoint for IP Office on page 43
3. If you are enabling licenses with additional features, such as upgrading the video resolution, see Installing and Enabling Licenses which Extend System Functionality on page 39.

Registering the Scopia XT Endpoint for IP Office to Obtain a License Key

About this task

Register your XT Endpoint 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 39.

Procedure

1. Open the envelope that came with the XT Endpoint.
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 40
   - Enabling the License from the Scopia XT Endpoint for IP Office on page 43

Installing and Enabling Licenses which Extend System Functionality

About this task

You can purchase licenses to extend the functionality of the Scopia XT Endpoint for IP Office, such as upgrading the video resolution.

Table 10: Scopia XT Endpoint for IP Office Software Options on page 40 lists the various license options available for purchase to extend the system's functionality.

Table 10: Scopia XT Endpoint for IP Office Software Options

Feature	Option/Reference	Description
Video resolution	55111-00937 Full HD (1080p)	Higher quality video at 1080p 60 fps instead the default 720p 60fps.
Recording Videoconferences	55111-00933 USB Recording License	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 109 or contact your administrator. When recording a videoconference, you can include up to 5 remote endpoints.
Scopia Control	55111-00917 Scopia Control	Enables controlling the Scopia XT Endpoint for IP Office using the Scopia Control Application (iPad).
Zoom	55111-10922 Scopia XT Endpoint for IP Office Zoom Upgrade	Upgrade to 40x digital zoom (10x optical and 4x digital).

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 40
   - Enabling the License from the Scopia XT Endpoint for IP Office on page 43

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 Endpoint for IP Office on page 43.

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 Endpoint for IP Office as described in Registering the Scopia XT Endpoint for IP Office to Obtain a License Key on page 38 or, if you are enabling a license option to extend Scopia XT Endpoint for IP Office functionality, see Installing and Enabling Licenses which Extend System Functionality on page 39.

Procedure

1. Access the XT Endpoint web interface, as described in Accessing XT Endpoint Web Interface on page 24.
2. From the Home page, select **Enable License**, or, navigate to **Administrator Settings** > **Utilities** > **Licenses**.

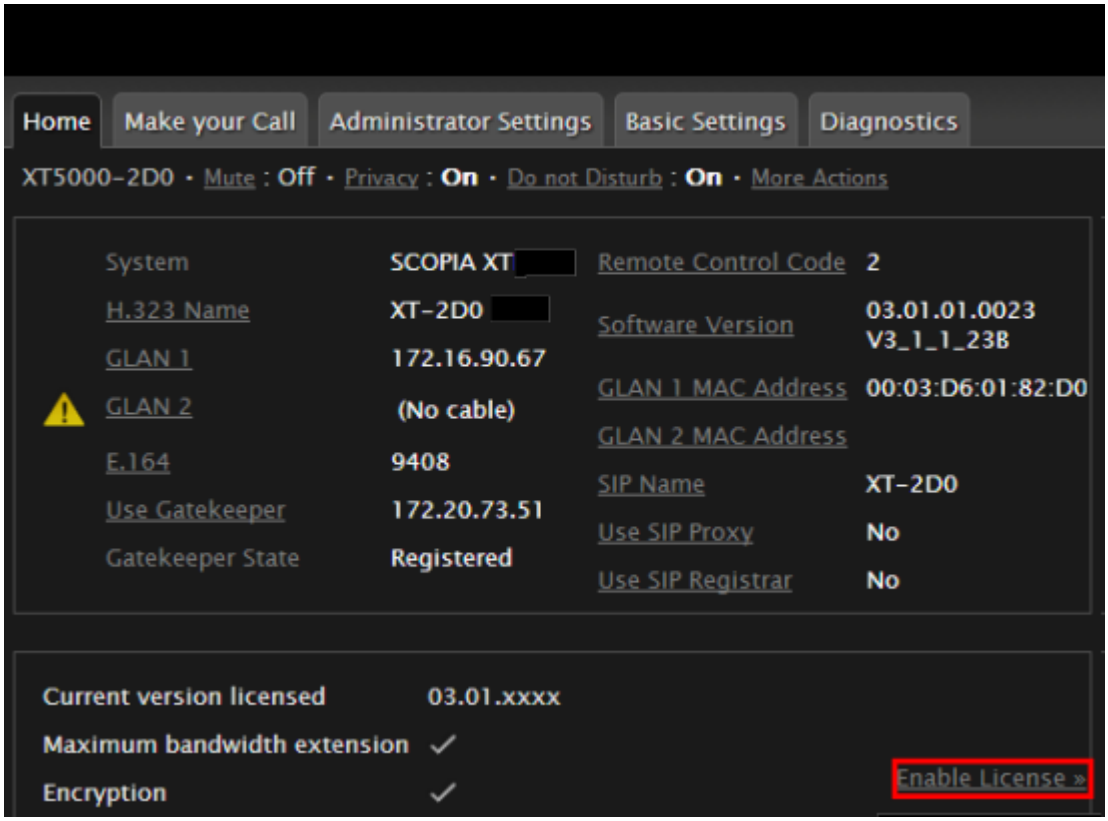


Figure 15: Accessing licenses from the Scopia XT Endpoint for IP Office home page

The **Licenses** page appears.

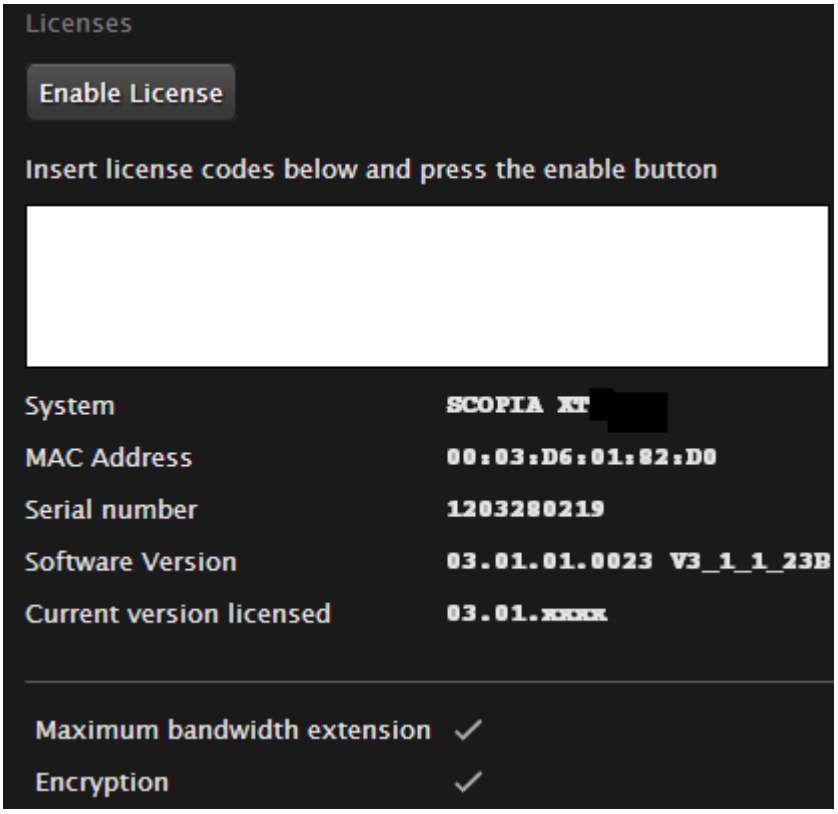


Figure 16: Enabling the license from the web interface

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.

Enabling the License from the Scopia XT Endpoint for IP Office

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 40.

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 Endpoint for IP Office as described in Registering the Scopia XT Endpoint for IP Office to Obtain a License Key on page 38 or, if you are enabling a license option to extend Scopia XT Endpoint for IP Office functionality, see Installing and Enabling Licenses which Extend System Functionality on page 39.
- If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

Procedure

1. Access the Scopia XT Endpoint for IP Office'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.

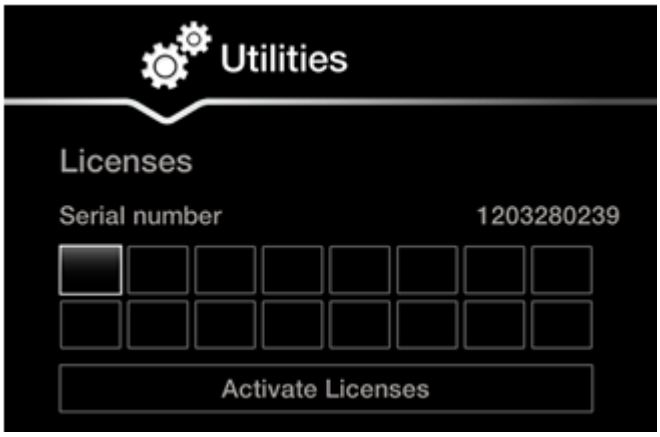


Figure 17: Activating a license

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.

Performing Basic Configuration

Before you perform basic configuration for the XT Endpoint, your system administrator should install and activate your XT Endpoint (for details, see the *Quick Setup Guide for Scopia XT Endpoint for IP Office*,

the *Installation Guide for Scopia XT Endpoint for IP Office*, and *Safety Instructions leaflet for Scopia XT Endpoint for IP Office*.

To start using your XT Endpoint, first define basic settings, such as the system's name, language, 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 Endpoint endpoint.

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

- Remotely defining the settings from the XT Endpoint web interface (see Accessing XT Endpoint Web Interface on page 24).

  Your administrator may define some settings remotely, such as for the network or gatekeeper (see Configuring Network Settings on page 81 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.

Navigation

- Accessing the Quick Setup Procedure on page 45
- Setting Basic System Information on page 52

Accessing the Quick Setup Procedure

About this task

Access the quick setup procedure to define basic settings for your Scopia XT Endpoint for IP Office, such as the system's name, language, 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 Endpoint web interface.

Before you begin

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.

Procedure

1. The quick setup wizard automatically appears the first time you access the Scopia XT Endpoint for IP Office, 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.

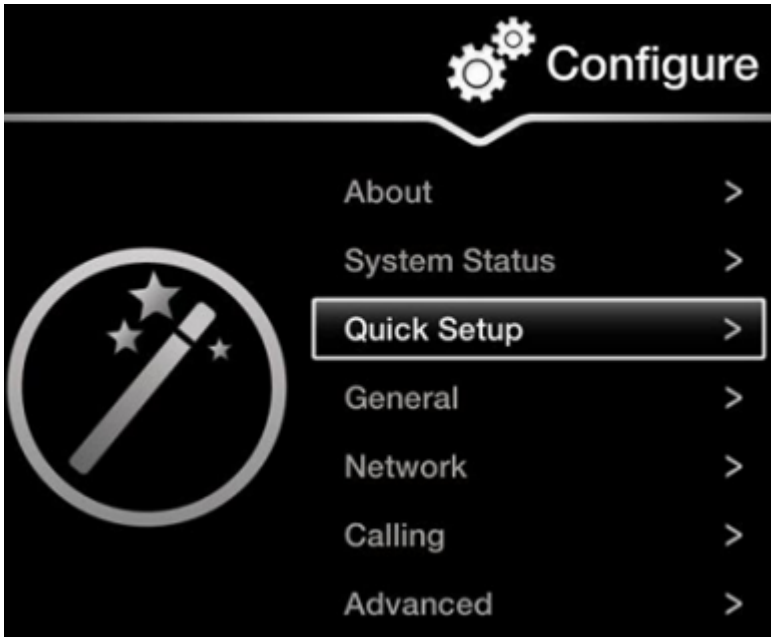


Figure 18: Accessing the Quick Setup

2. The quick setup wizard guides you through these basic configuration tasks:
   - Setting the System Name and Language on page 46: Define your system's name, your country, and preferred language for the interface.
   - Adjusting the Image Position on page 48: 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 49: Define your system's network settings to allow you to place and receive calls.
   - Configuring Gatekeeper Settings on page 51: If your Scopia XT Endpoint for IP Office works in conjunction with a gatekeeper, configure gatekeeper-related settings.

     This is typically not relevant for IP Office deployments. Configure only if you are using a gatekeeper in your deployment.

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 54.

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 53.

Before you begin

Access the quick setup wizard from the endpoint or web interface, as described in Accessing the Quick Setup Procedure on page 45.

Procedure

1. Enter the name of the XT Endpoint 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 30).



Figure 19: 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 48.

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 46.

Access the quick setup wizard from the endpoint, as described in Accessing the Quick Setup Procedure on page 45.

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 20: Examining the image position

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

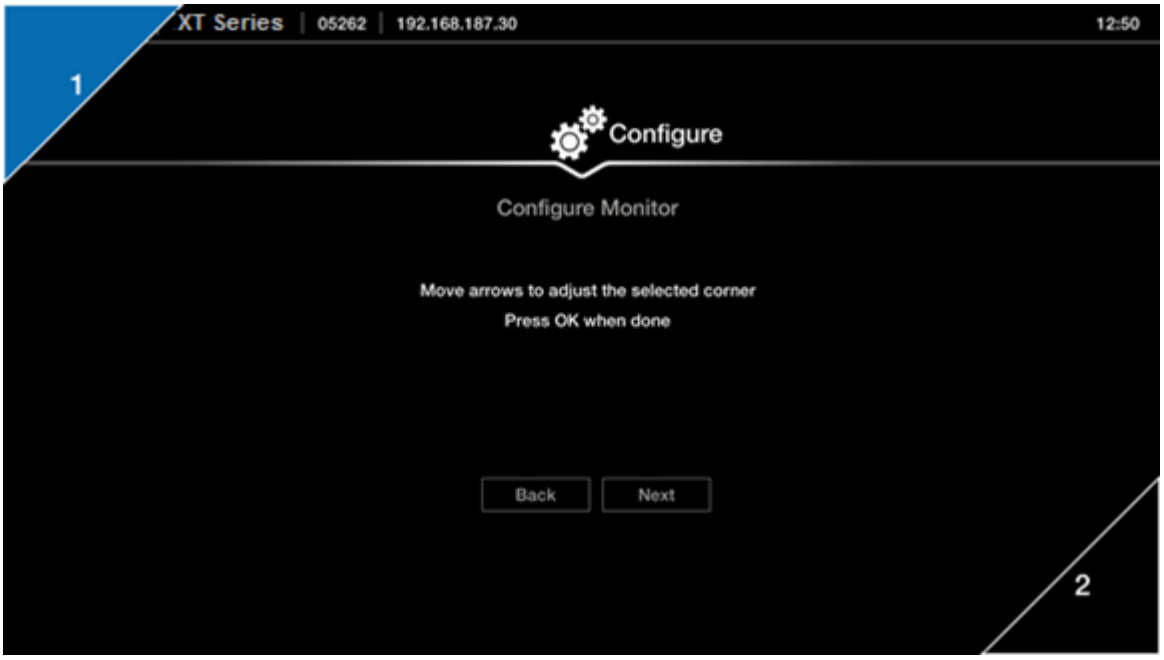


Figure 21: Adjusting the image position

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 49.

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 81.

Before you begin

This procedure is performed as part of the Quick Setup Wizard, after Adjusting the Image Position on page 48. 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 45.

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 DCHP).

     The **IP address**, **Subnet mask**, **Gateway**, and **DNS** fields appear as read-only. See Table 11: Configuring IP addresses on page 51 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 Endpoint 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 11: Configuring IP addresses on page 51.

     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 Endpoint Using TLS on page 100.



Figure 22: Defining IP Settings

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

Table 11: 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.

3. To configure your gatekeeper's settings, select **Next** and continue with Configuring Gatekeeper Settings on page 51.

   If you are not using a gatekeeper in your deployment, select **Next > Done**.

Configuring Gatekeeper Settings

About this task

This is typically not relevant for IP Office deployments. Configure only if you are using a gatekeeper in your deployment.

If you are not using a gatekeeper in your deployment, select **Done**.

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 Endpoint for IP Office 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 Endpoint for IP Office with a Gatekeeper on page 89.

Before you begin

This procedure is performed as part of the basic configuration after Configuring Network Settings on page 49. 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 45.

Procedure

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

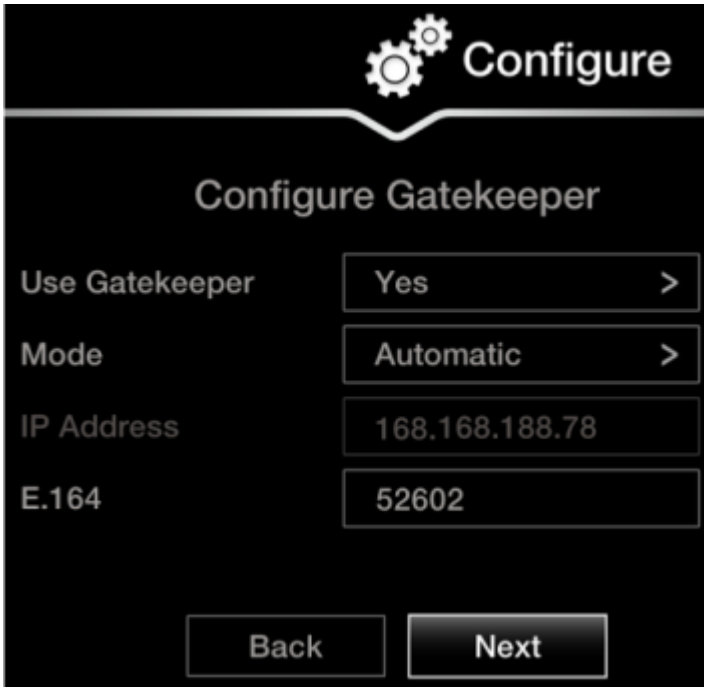


Figure 23: Gatekeeper settings

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 Endpoint for IP Office 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 53
- Setting Date and Time on page 57
- Setting the Time Zone on page 58
- Remotely Setting Regional Information on page 59
- Configuring the Screen Saver to Start Automatically on page 61

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 46.

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 54.

Procedure

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

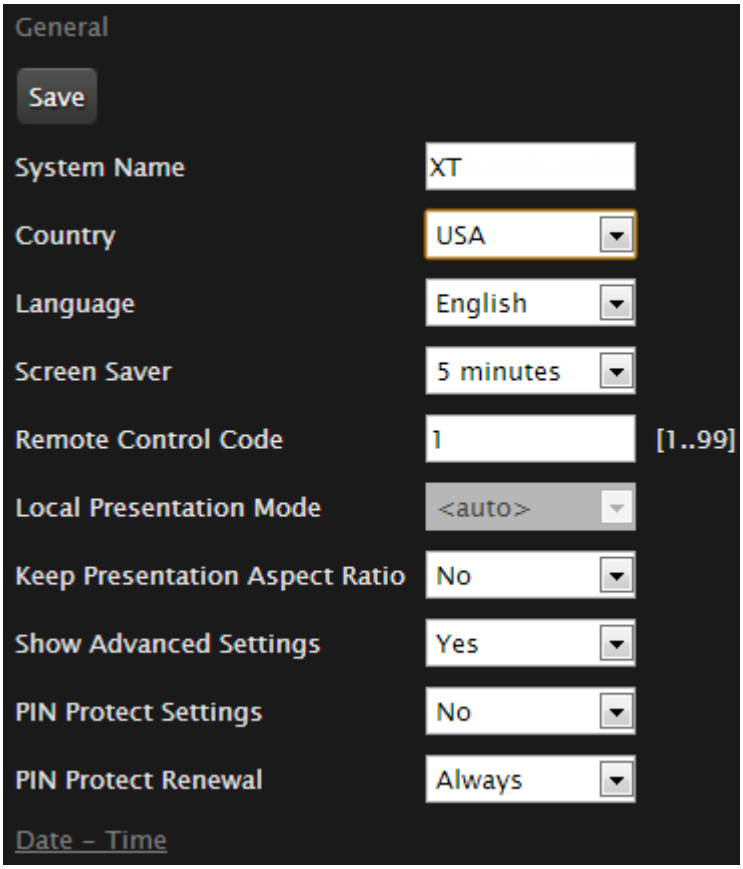


Figure 24: Basic Settings page

2. Enter the name of the XT Endpoint 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 25: Scopia XT Endpoint for IP Office's titlebar on page 55). 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 46.

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 Endpoint to IP Office on page 61 and Registering the Scopia XT Endpoint for IP Office with a Gatekeeper on page 89.



Figure 25: Scopia XT Endpoint for IP Office's titlebar

Procedure

1. Access the system name settings:
   - From the XT Endpoint 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.

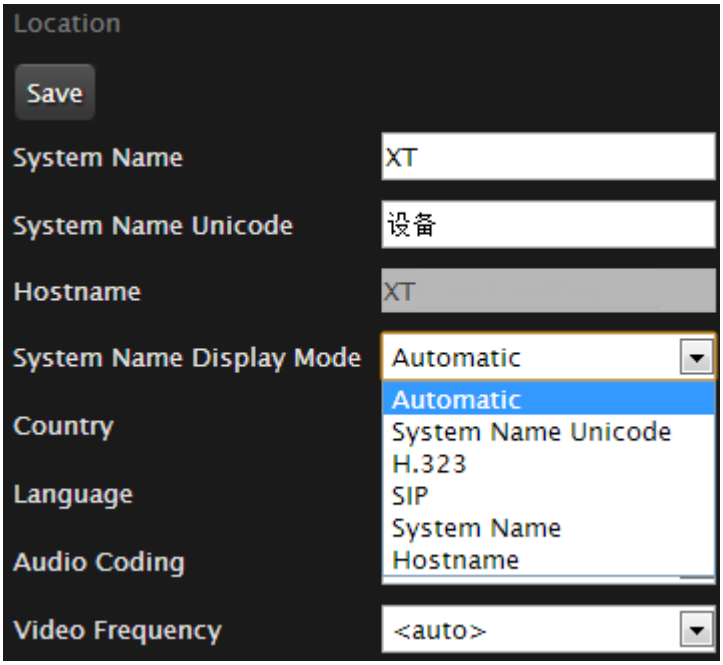


Figure 26: Selecting the system name

2. Enter the following settings:

Table 12: 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 Endpoint to IP Office on page 61. • **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 Endpoint for IP Office with a Gatekeeper on page 89. • **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 46). 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 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 XT Endpoint Locally from the Endpoint on page 35.

Procedure

1. Access the date and time settings as follows:
   - From the XT Endpoint 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 13: Configuring date and time settings on page 57.

   Important:

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

Table 13: 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.

3. 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 XT Endpoint web interface.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

Procedure

1. Access the time zone settings as follows:
   - From the XT Endpoint 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.
2. Configure settings as described in Table 14: Configuring time zone related settings on page 59.

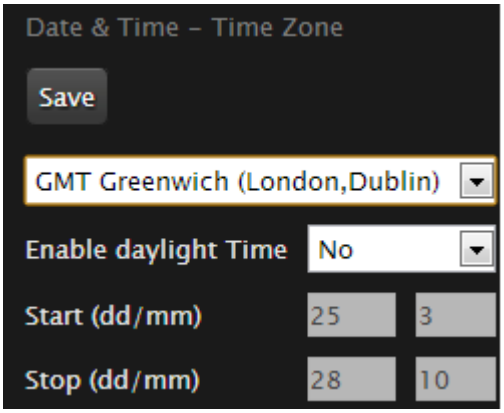


Figure 27: Setting the time zone

Table 14: 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.

3. 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 45). You can modify these settings at any time from the endpoint or the web interface.

Procedure

1. Access the XT Endpoint web interface, as described in Accessing XT Endpoint Web Interface on page 24.
2. Select **Administrator Settings > System > Location**.

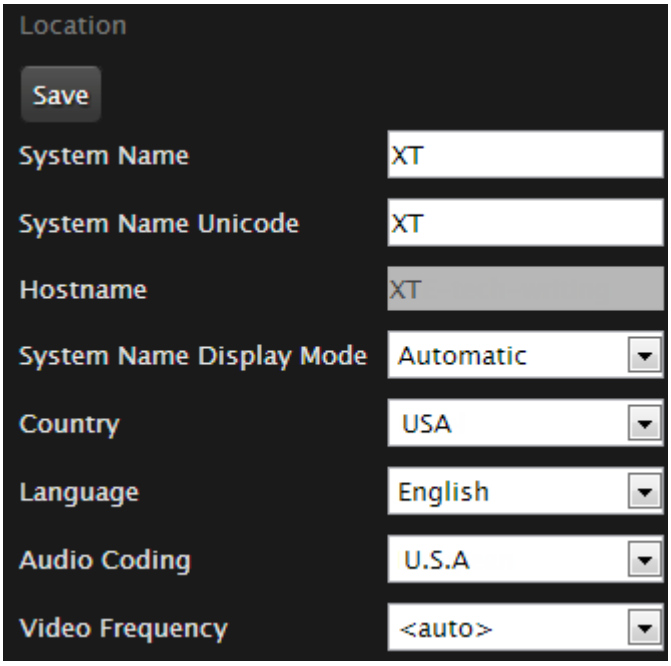


Figure 28: Setting regional information

3. Define regional settings as described in Table 15: Configuring regional information on page 60.

Table 15: 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 Endpoint 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 Endpoint for IP Office for a relatively short period of time. You can do this procedure from the endpoint itself or from the XT Endpoint web interface.

Procedure

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

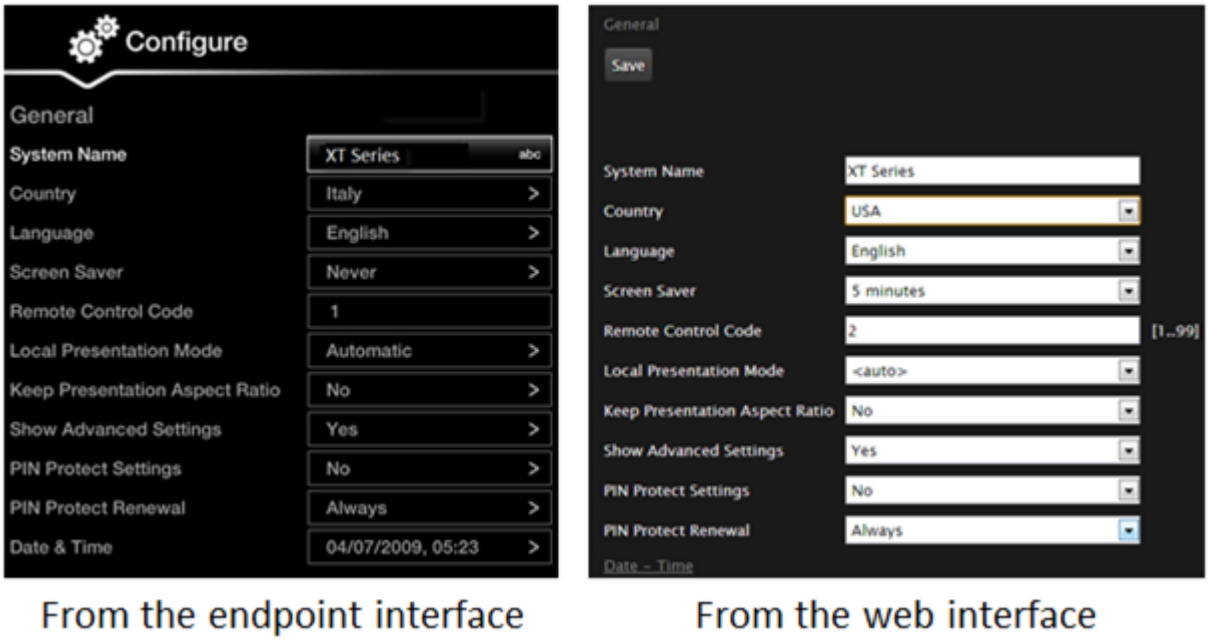


Figure 29: Configuring screen saver settings

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**.

Registering the XT Endpoint to IP Office

About this task

The procedure in this section explains how to register your XT Endpoint to the IP Office SIP Registrar and how to configure the SIP Proxy connection. If you do not register to IP Office, you cannot host videoconferences or use the full functionality of the system.

The XT Endpoint 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 Avaya IP Office server.
- The transport port used in your SIP environment.
- Credentials for authenticating XT Endpoint to the Avaya IP Office server.

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

Procedure

1. Access the SIP settings as follows:
   - From the XT Endpoint web interface, select **Administrator Settings > Protocols > SIP.**
   - From the endpoint's main menu, select **Configure > Advanced > Protocols > SIP**.

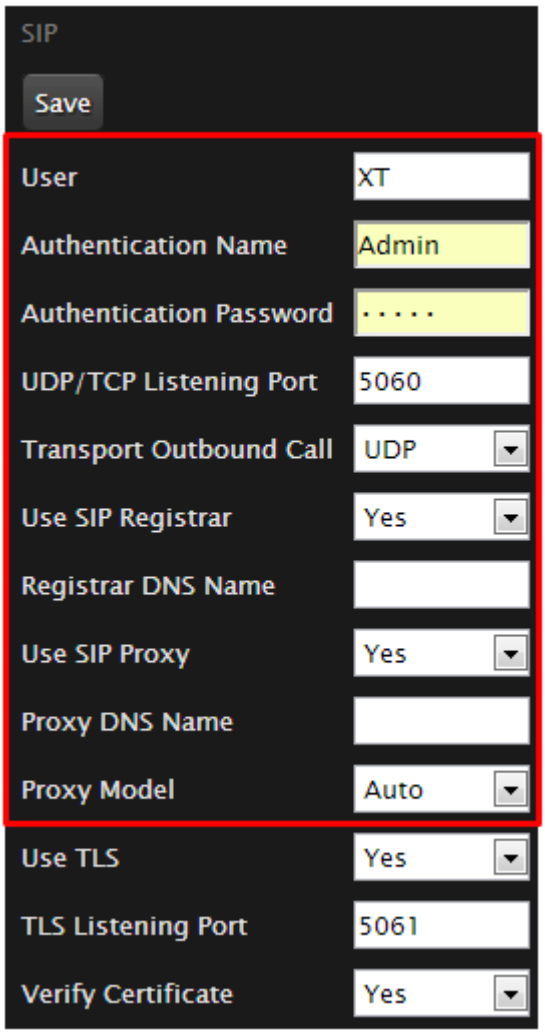


Figure 30: Configuring SIP settings

2. Configure parameters as described in Table 16: Configuring SIP-related parameters on page 63.

Table 16: Configuring SIP-related parameters

Parameter	Description
User	Enter the extension number of the user, as configured in IP Office. When connecting over SIP, this name is displayed on the monitors participating in the videoconference.
Authentication Name	Enter the user's **Name**, as configured in IP Office.
Authentication Password	Enter the user's **Login Code**, as configured in IP Office.
UDP/TCP Listening Port	Enter the same port number used by IP Office for receiving inbound SIP calls. By default, port 5060 is used.
Transport Outbound Call	Select **UDP**.

Parameter	Description
Use SIP Registrar	Select **Yes**.
Registrar DNS Name	Enter the DNS name or IP address of the IP Office server.
Use SIP Proxy	Select **Yes**.
Proxy DNS Name	Enter the DNS name or IP address of the IP Office server.
Proxy Model	Select **Auto**.

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 Endpoint Using TLS on page 100.

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 64
- Setting up the Monitor Display Modes on page 68

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 Endpoint web interface.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

Connect the video equipment, as described in *Installation Guide for Scopia XT Endpoint for IP Office*.

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 Endpoint web interface, select **Administrator settings > I/O connections > Cameras > General**.

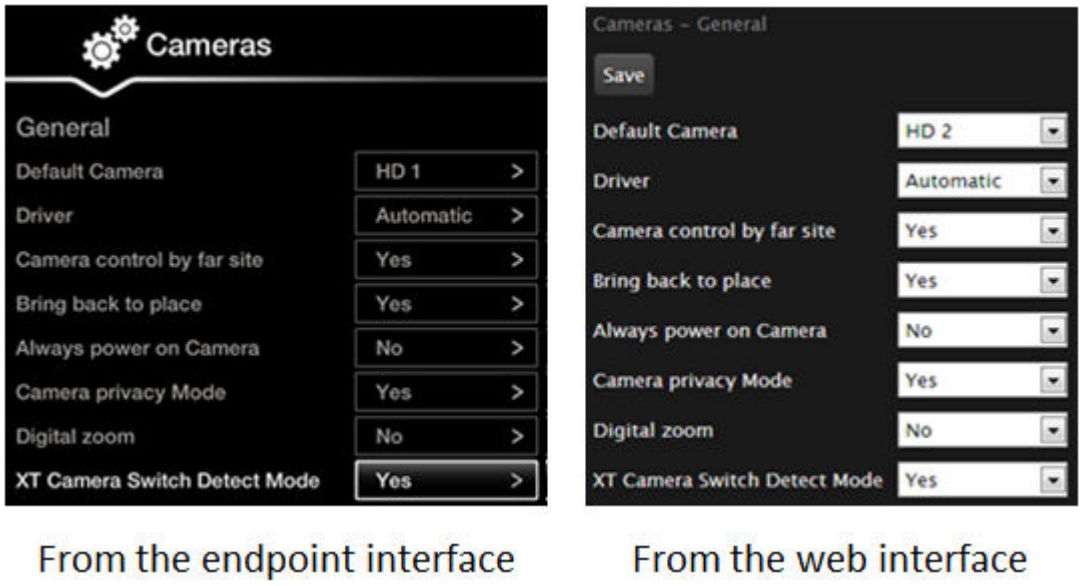


Figure 31: Configuring general camera settings from the web interface

2. Configure the camera connection as described in Table 17: Configuring general camera settings on page 66:

Table 17: 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 32: 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 *Installation Guide for Scopia XT Endpoint for IP Office*. **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 *Installation Guide for Scopia XT Endpoint for IP Office*.
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 *Installation Guide for Scopia XT Endpoint for IP Office*.

3. From the web interface only, select **Save**.
4. 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 Endpoint web interface, select **Administrator settings > I/O connections > Cameras**.

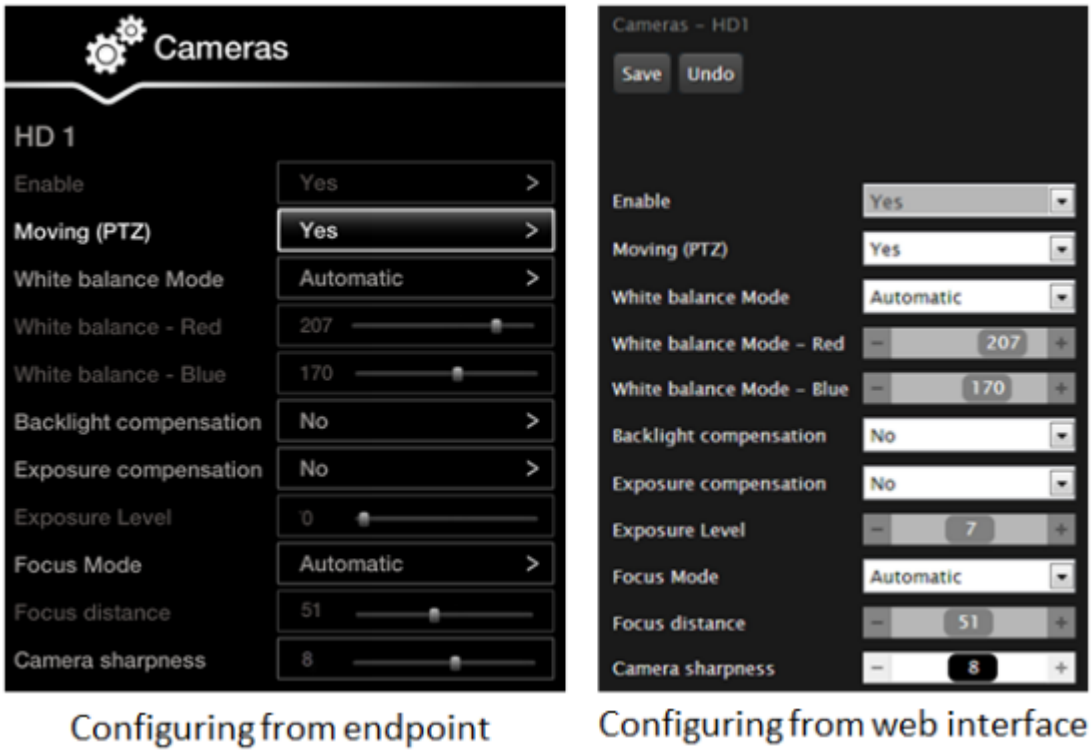


Figure 33: Configuring the camera settings from the web interface

5. Define the following camera settings:

Table 18: 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 *Installation Guide for Scopia XT Series*. 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 18: Configuring advanced camera settings on page 68 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 Endpoint 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 Endpoint for IP Office 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 136.

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 XT Endpoint Locally from the Endpoint on page 35.

Procedure

1. Access the monitor settings:
   - From the endpoint's main menu, select **Configure > Advanced > I/O connections > Monitor**.
   - From the XT Endpoint 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.

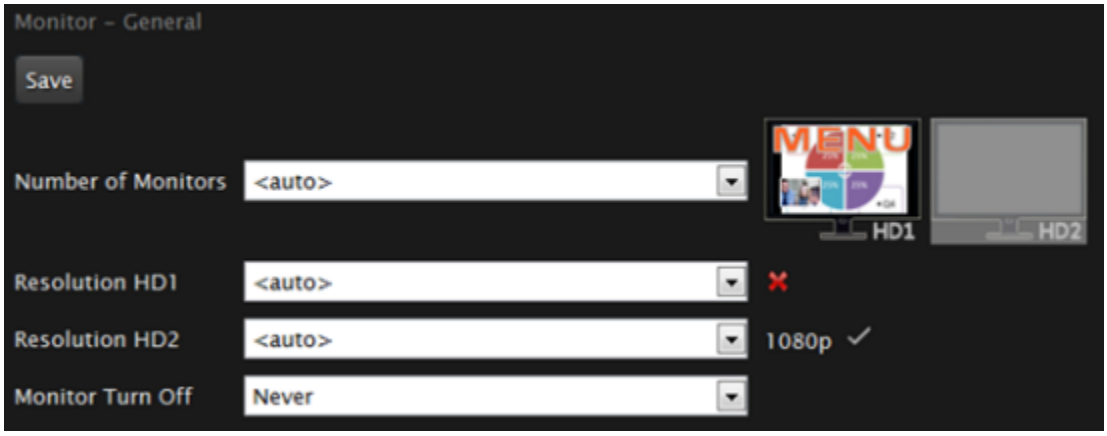


Figure 34: Configuring the general monitor settings from the web interface

b. Configure the general settings:

Table 19: 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**.

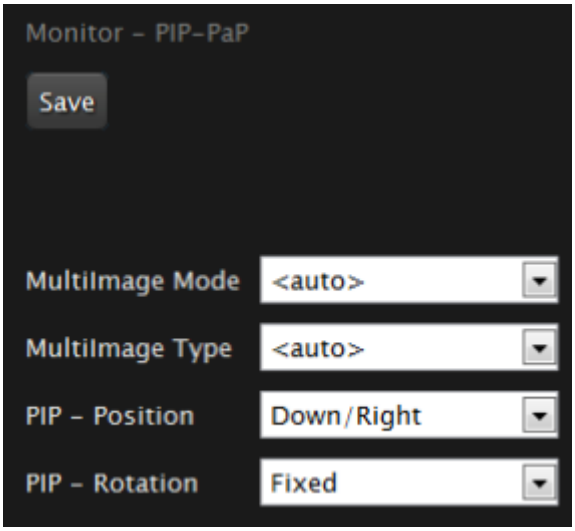


Figure 35: Setting PIP-PaP option

b. Configure the PiP and PaP options as described in Table 20: Configuring PIP-PaP option on page 73.

   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 Endpoint for IP Office User Guide*.

Table 20: 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 74
- Configuring Analog Audio Connections on page 75
- Configuring the Echo Canceller on page 77
- Configuring Audio Outputs on page 79

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 *Installation Guide for Scopia XT Endpoint for IP Office* 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 *Installation Guide for Scopia XT Endpoint for IP Office*. To plan your audio setup, see *Installation Guide for Scopia XT Endpoint for IP Office*.

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

Procedure

1. Access the microphone settings:
   - From the endpoint's main menu, select **Configure > Advanced > I/O connections > Audio - Input**.
   - From the XT Endpoint 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**.

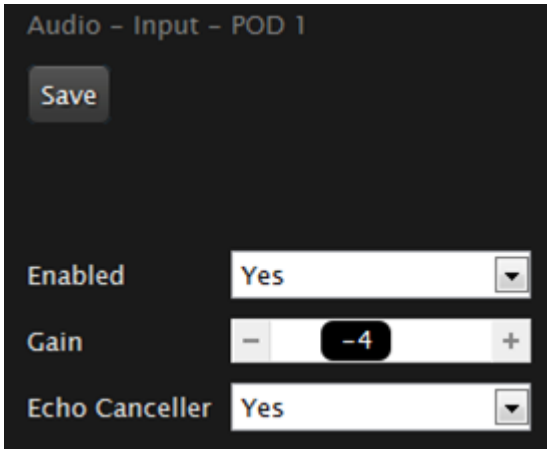


Figure 36: Configuring the microphone settings from the web interface

3. Set the fields as described in Table 21: Configuring the microphone connection on page 75.

Table 21: 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 77, 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 37: The analog/optical audio port on the XT Endpoint

Before you begin

Connect the analog audio equipment as described in *Installation Guide for Scopia XT Endpoint for IP Office* .

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

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 Endpoint web interface, select **Administrator settings > I/O connections > Audio - Input > Analog**.
2. Set the fields as required.

Table 22: 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 77. To hear the audio also locally, see Configuring Audio Outputs on page 79. 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 22: Configuring analog audio connections on page 76), 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 Endpoint web interface, select **Administrator Settings** > **I/O Connections** > **Cameras** > **DVI**.

   b. Verify that **Enabled** is set to **Yes**.

Configuring the Echo Canceller

About this task

If your Scopia XT Endpoint for IP Office 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 74.

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

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 Endpoint web interface, select **Administrator settings > I/O connections > Echo Canceller**.

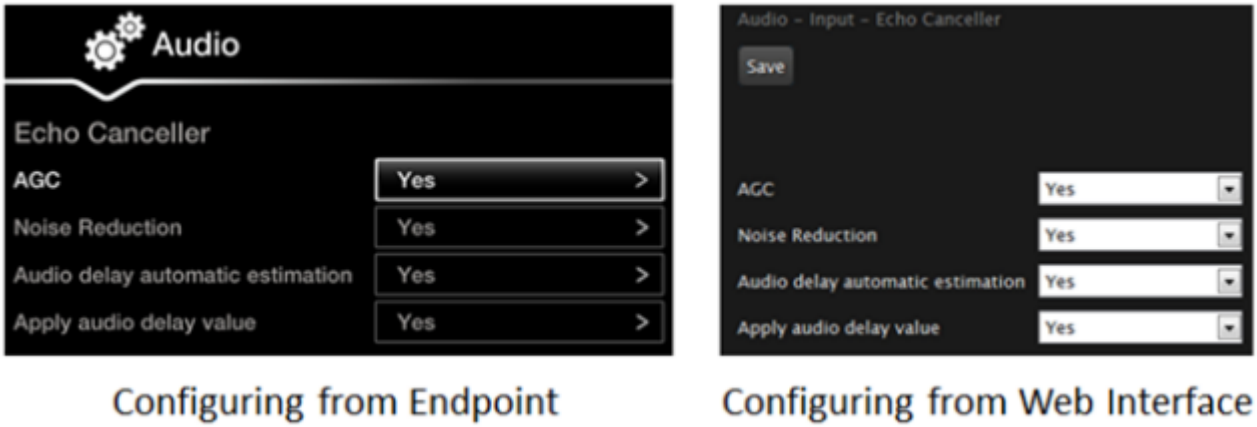


Figure 38: Configuring the Echo Canceller

2. Set the fields as required.

Table 23: 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 Audio Outputs

About this task

The Scopia XT Endpoint for IP Office 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 Endpoint for IP Office system menus (Figure 39: Defining the routing of the audio outputs on page 80).

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 39: Defining the routing of the audio outputs on page 80, 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 XT Endpoint Locally from the Endpoint on page 35.

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 Endpoint web interface, select **Administrator settings > I/O connections > Audio - Outputs > General**.

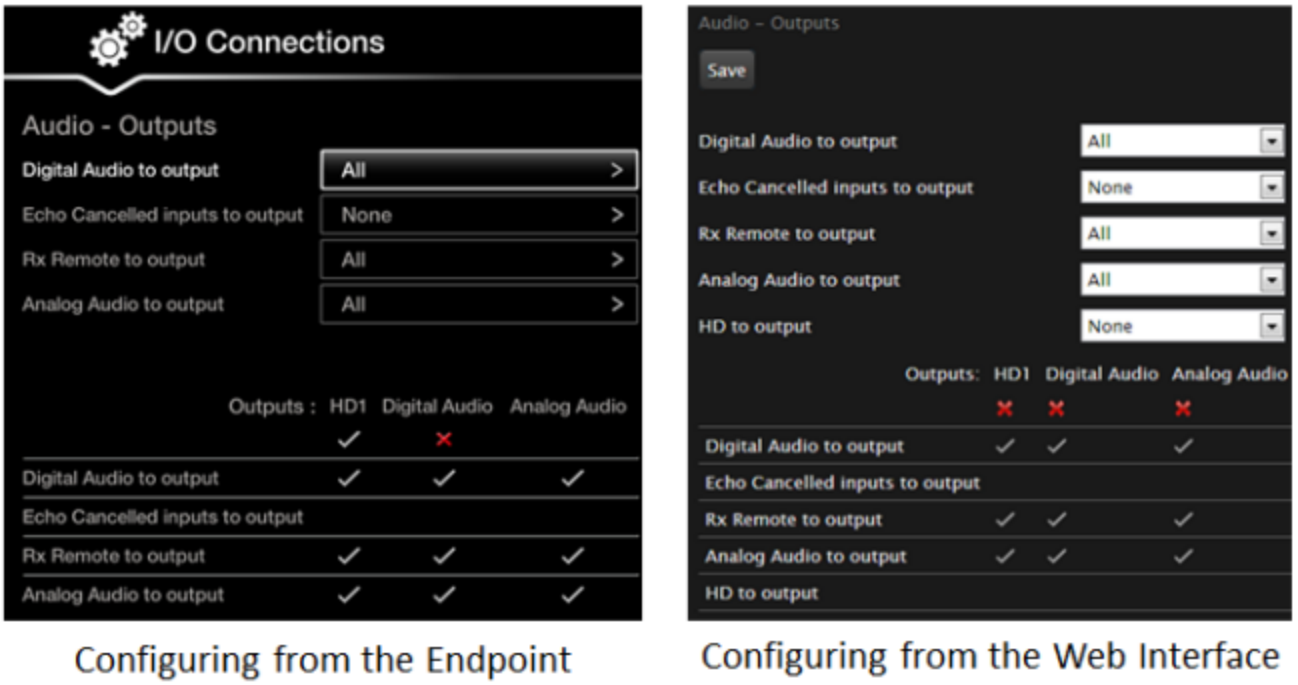


Figure 39: Defining the routing of the audio outputs

2. Set the fields as required.

Table 24: 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.

Field Name	Description
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.

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 81
- Registering the Scopia XT Endpoint for IP Office with a Gatekeeper on page 89
- Configuring Call Settings on page 92
- Configuring Scopia XT Endpoint for IP Office to use an LDAP Directory on page 96

Configuring GLAN Use

You can configure GLAN use for Scopia XT Endpoint for IP Office.

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 81
- Configuring Network Connectivity on page 84
- Enabling NAT and Firewall Traversal with Scopia XT Endpoint for IP Office on page 86
- Determining the Priority of Audio versus Video Quality on page 88

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 XT Endpoint Locally from the Endpoint on page 35.

Procedure

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

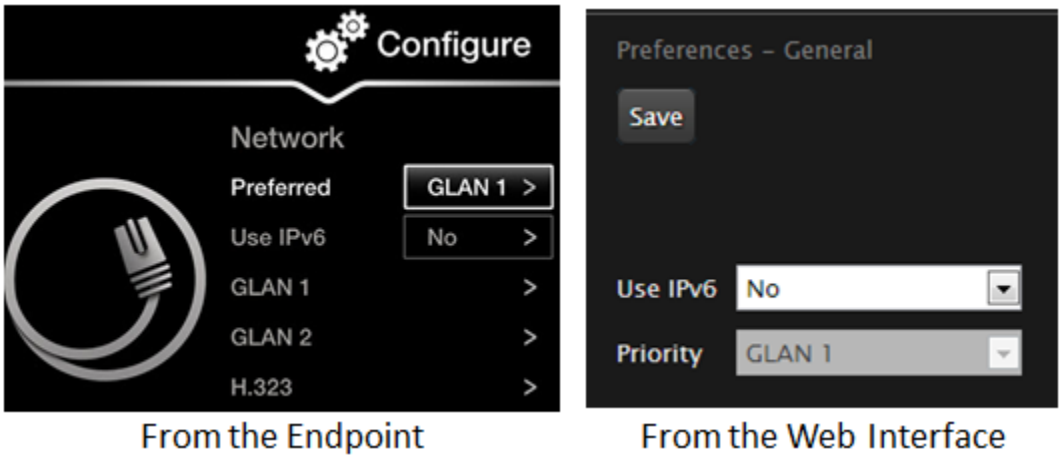


Figure 40: Enabling IPv6 mode

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**.

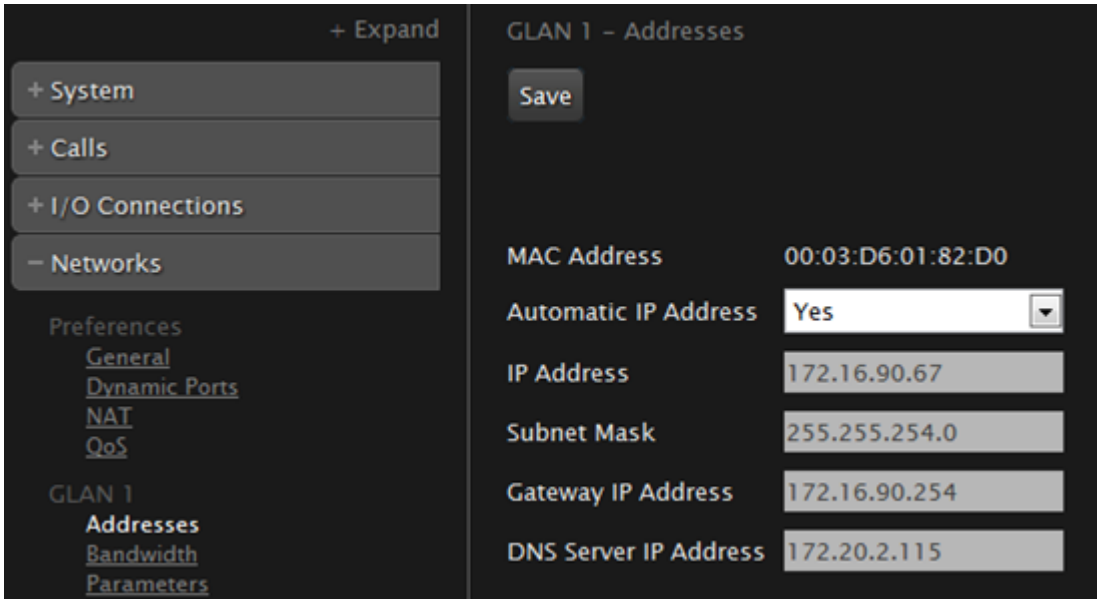


Figure 41: Configuring IP addresses from the web interface

5. Set the fields as described in Table 25: Configuring IP addresses on page 83.

Table 25: 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 Endpoint 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 Endpoint Using TLS on page 100.
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.
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.

Field Name	Description
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 Endpoint using TLS certificates and you now modified the IP address, you must generate the CSR again, as described in Generating a Certificate Signing Request for XT Endpoint on page 101.

Configuring Network Connectivity

About this task

This procedure describes how to configure the GLAN1 and GLAN2 ports.

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 XT Endpoint Locally from the Endpoint on page 35.

Procedure

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

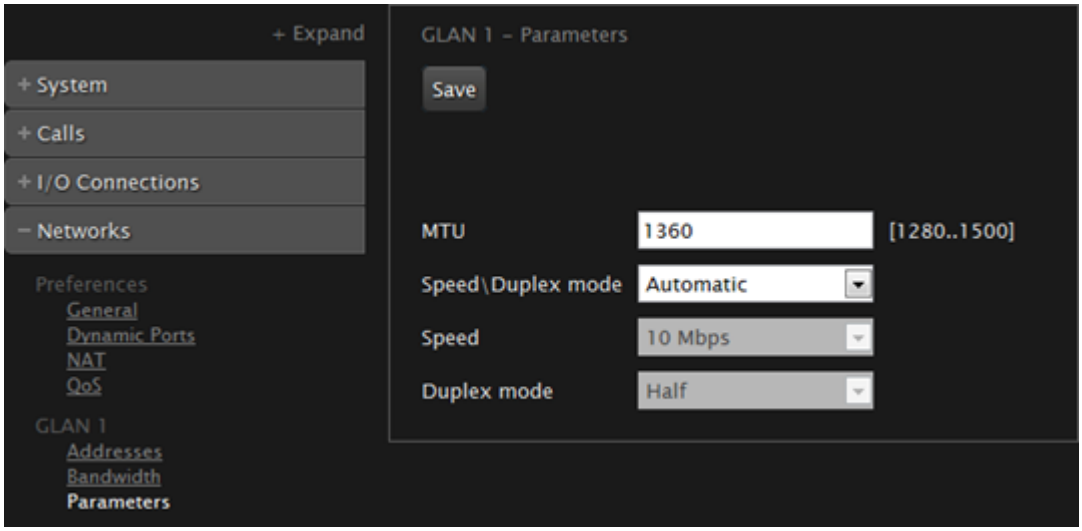


Figure 42: Configuring the GLAN parameters from the web interface

3. Set the field as described in Table 26: Configuring network connectivity on page 85.

   To avoid connectivity issues, match these settings to the equivalent settings in the network.

Table 26: 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 81. 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 Endpoint for IP Office

About this task

Scopia XT Endpoint for IP Office 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 Endpoint for IP Office 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 Endpoint for IP Office on page 13.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

Procedure

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

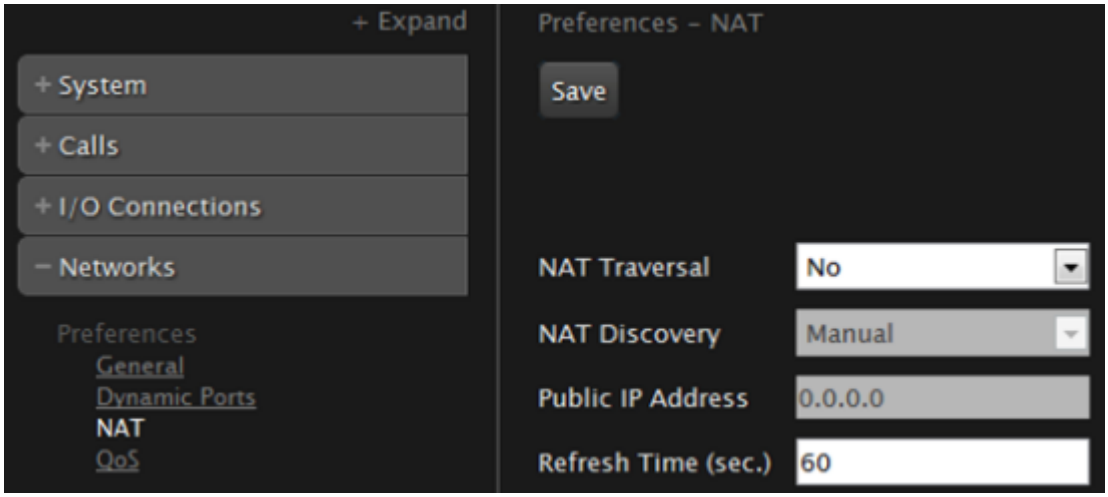


Figure 43: Configuring NAT traversal settings from the web interface

2. Set the fields as described in Table 27: Configuring NAT-related settings on page 87.

Table 27: 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 Endpoint for IP Office on page 20.

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 Endpoint for IP Office on page 129.

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 XT Endpoint Locally from the Endpoint on page 35.

Procedure

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

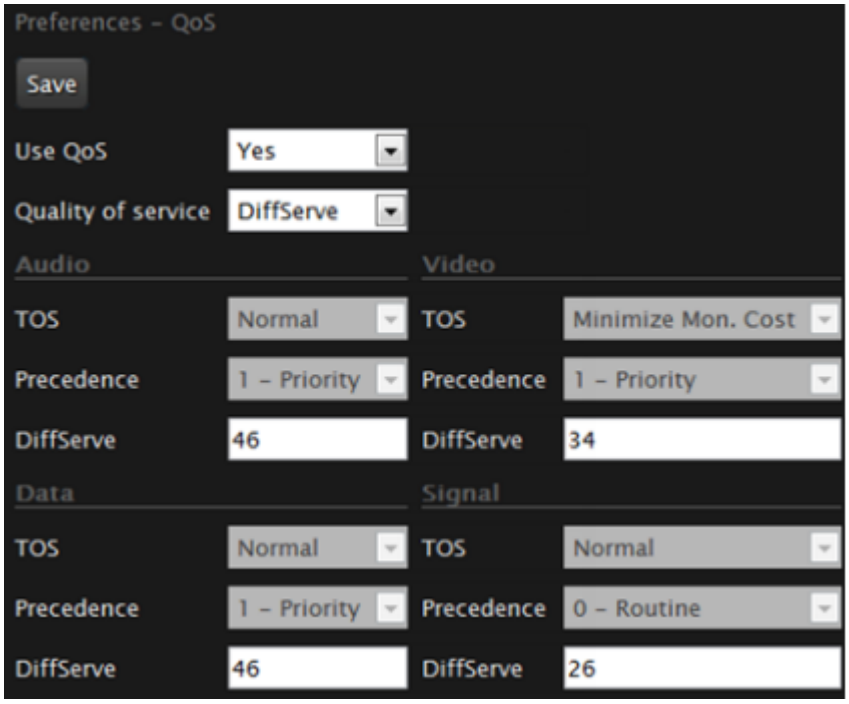


Figure 44: Configuring QoS settings

2. Set the fields as described in Table 28: Configuring QoS settings on page 89.

Table 28: 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.

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

Registering the Scopia XT Endpoint for IP Office with a Gatekeeper

About this task

This is typically not relevant for IP Office deployments. Configure only if you are using a gatekeeper in your deployment.

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 XT Endpoint Locally from the Endpoint on page 35.

Procedure

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

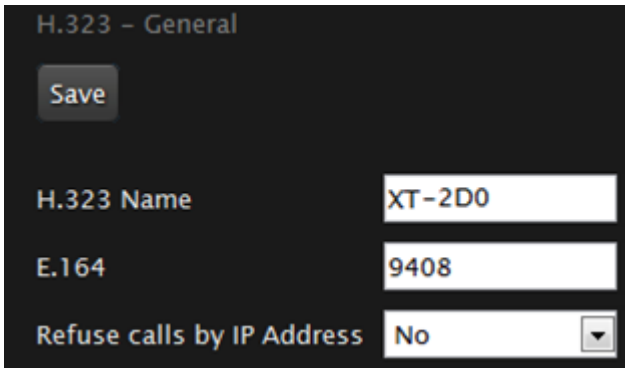


Figure 45: Configuring H.323 settings from the web interface

2. Set the fields as described in Table 29: Configuring H.323 settings on page 91.

Table 29: 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.

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

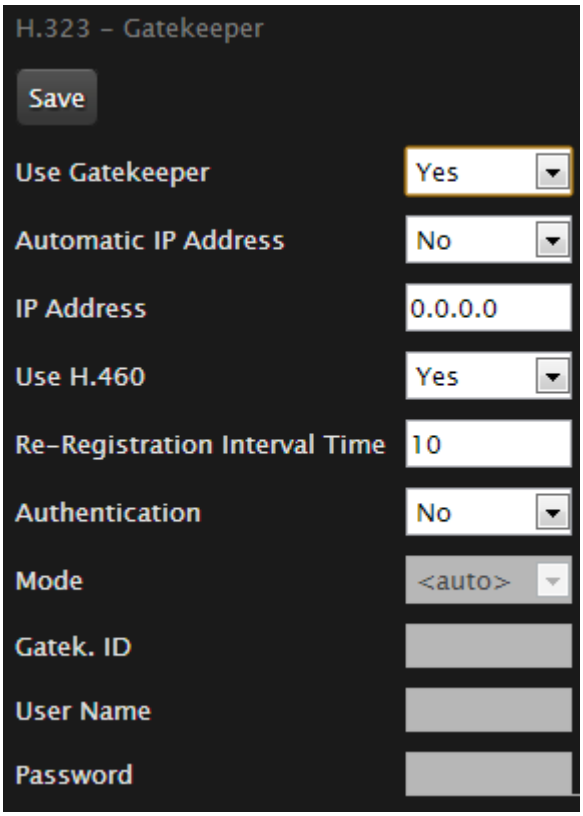


Figure 46: Configuring the Gatekeeper settings from the web interface

5. Set the fields as described in Table 30: Configuring the gatekeeper on page 92.

Table 30: 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**.

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 XT Endpoint Locally from the Endpoint on page 35.

Procedure

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

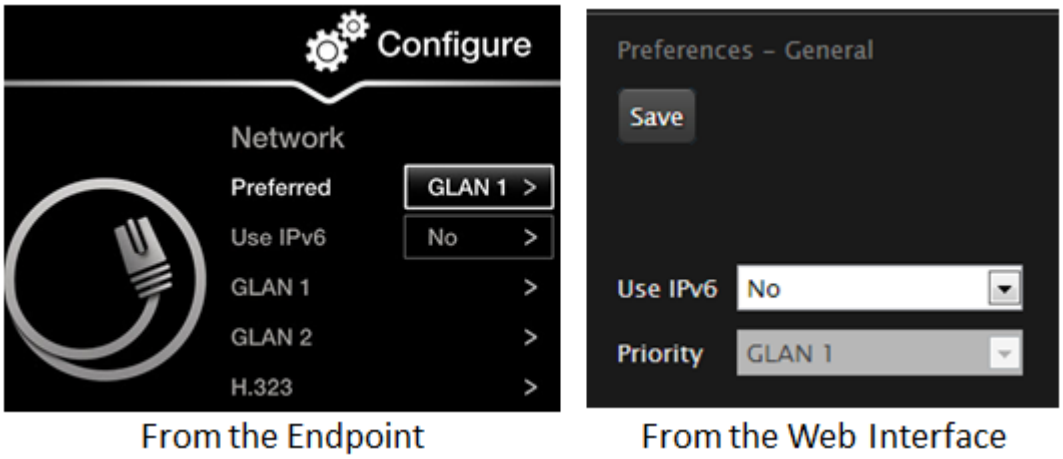


Figure 47: Configuring the Priority setting from the web interface

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**.

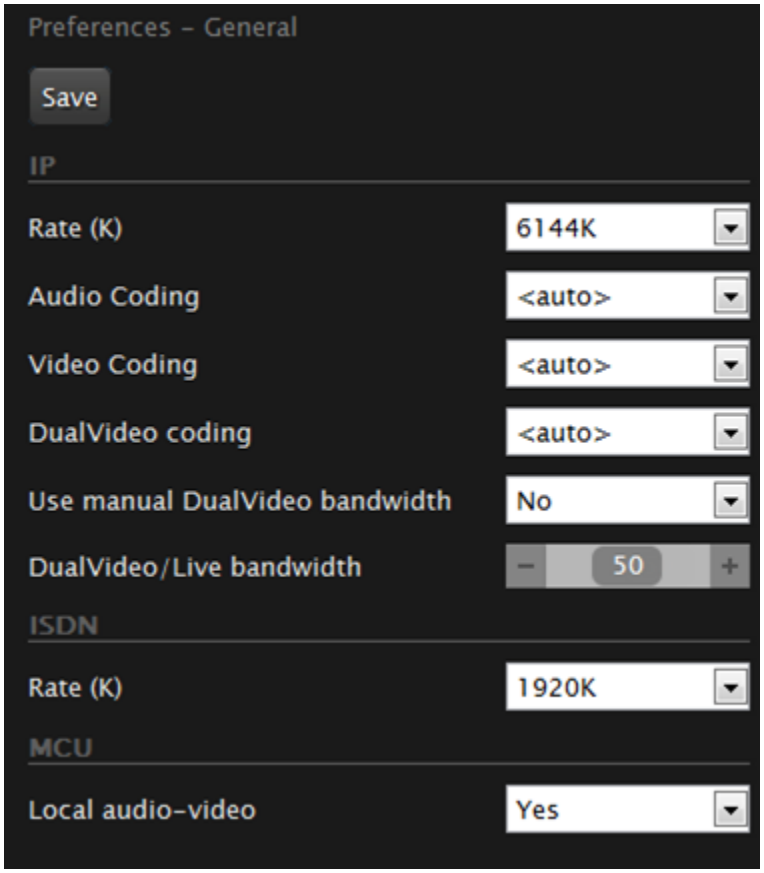


Figure 48: Configuring general call settings

5. Set the fields as described in Table 31: Configuring general call settings on page 94.

Table 31: 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**.

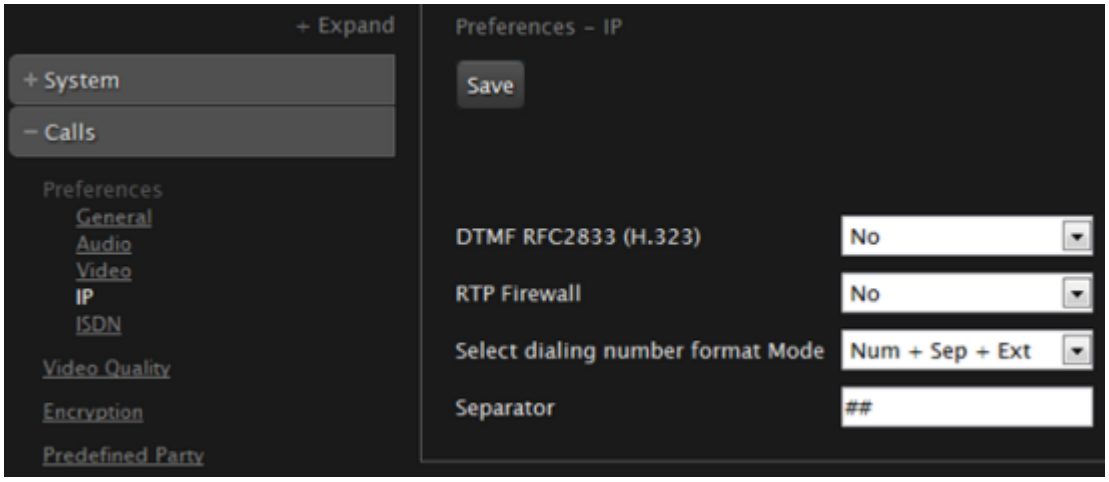


Figure 49: Configuring the IP settings from the web interface

8. Set the fields as described in Table 32: Configuring the IP-related call settings on page 95.

Table 32: 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 Endpoint for IP Office 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 50: Viewing and editing contacts in Local LDAP server on page 96).



Figure 50: Viewing and editing contacts in Local LDAP server

You can define these 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 50: Viewing and editing contacts in Local LDAP server on page 96). The local LDAP server has a password which can be changed if needed.

Important:

You cannot remove the local LDAP server.

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

  The contacts are read-only when browsing a remote XT Endpoint'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.

- 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 Endpoint works both as an H.323 and a SIP endpoint, all XT Endpoint **commObject**s 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 33: 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)
    ```

    where `commUniqueId` refers to the **commObject** ID

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

Procedure

1. Access the LDAP settings, as follows:
   - From the endpoint's main menu, select **Configure > Advanced > System > LDAP**.
   - From the XT Endpoint web interface, select **Administrator Settings > System > LDAP**.

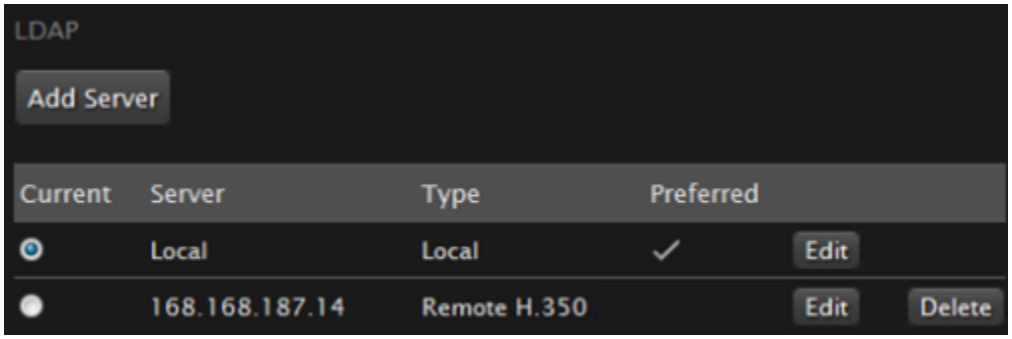


Figure 51: Configuring LDAP settings from the web interface

2. Select **Add Server**.

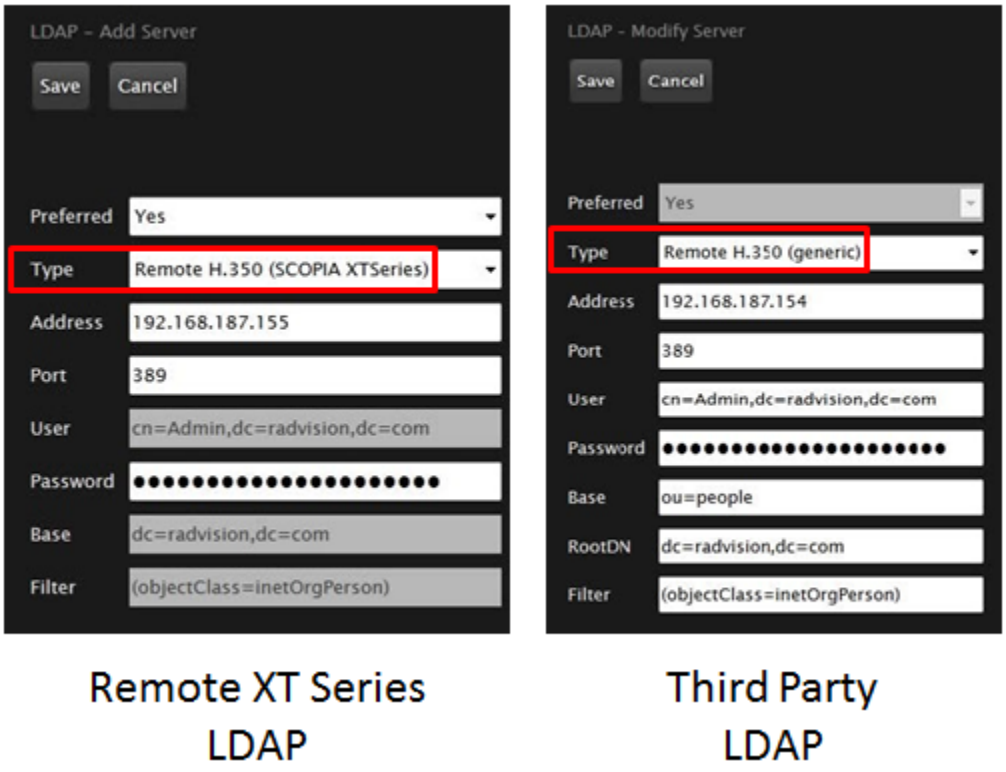


Figure 52: Adding each type of LDAP server from the web interface

3. Configure the LDAP server settings as described in Table 34: Configuring LDAP server settings on page 99.

Table 34: 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 Endpoint)**: An external XT Endpoint'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.
Port	Enter the port used to connect to the LDAP server. The default port is 389.
User **Password**	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). 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 Endpoint as the LDAP server, this value cannot be modified, since the LDAP user of a XT Endpoint 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 Endpoint, and cannot be modified.
Root DN	For third party LDAP servers, enter the mandatory H.350 Root DN. For XT Endpoint 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 Endpoint.

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

Chapter 5 | Securing your Scopia XT Endpoint for IP Office

You can secure the connection between video network devices and your Scopia XT Endpoint for IP Office 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 Endpoint for IP Office, see:

Navigation

- Securing Connections to the XT Endpoint Using TLS on page 100
- Enabling Encryption for Videoconferences on page 109

Securing Connections to the XT Endpoint 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 Endpoint and other video network devices.

The TLS protocol is based on a public and private keys for authorization and encryption, exchanged between the XT Endpoint 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 Endpoint 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 Endpoint 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 Endpoint and other devices. Perform these tasks in the order listed below:

1. Perform Generating a Certificate Signing Request for XT Endpoint on page 101.
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 Endpoint.

3. Perform Uploading XT Endpoint Certificates on page 103.
4. Perform Enabling the TLS Connection in XT Endpoint on page 107 .
5. To encrypt the media (audio, video, presentation) of videoconferences using the SRTP protocol, perform Enabling Encryption for Videoconferences on page 109.

Generating a Certificate Signing Request for XT Endpoint

About this task

This section details how to generate a certificate signing request (CSR) for the XT Endpoint, 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 Endpoint to other components in the network, and can also facilitate encrypted communications with those components.

Important:

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

To restore previously uploaded certificates, see Backing Up and Restoring XT Endpoint Certificates on page 105. To delete the certificates, see Deleting XT Endpoint Certificates on page 106.

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 81.

Procedure

1. Access the XT Endpoint web interface, as described in Accessing XT Endpoint Web Interface on page 24.
2. Select **Administrator Settings > Utilities > Certificates**.
3. Enter your organization's details and your email.

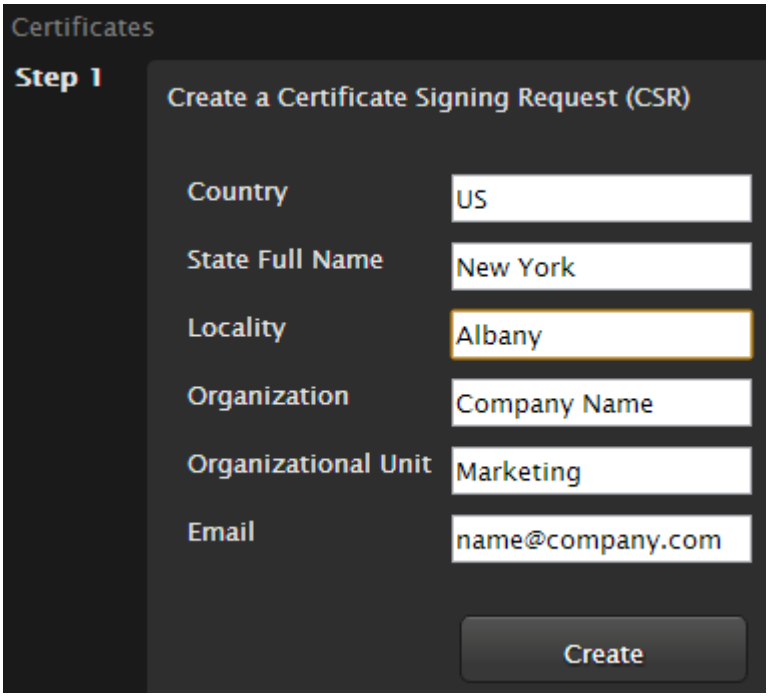


Figure 53: Generating a CSR for Scopia XT Endpoint for IP Office

Table 35: 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.

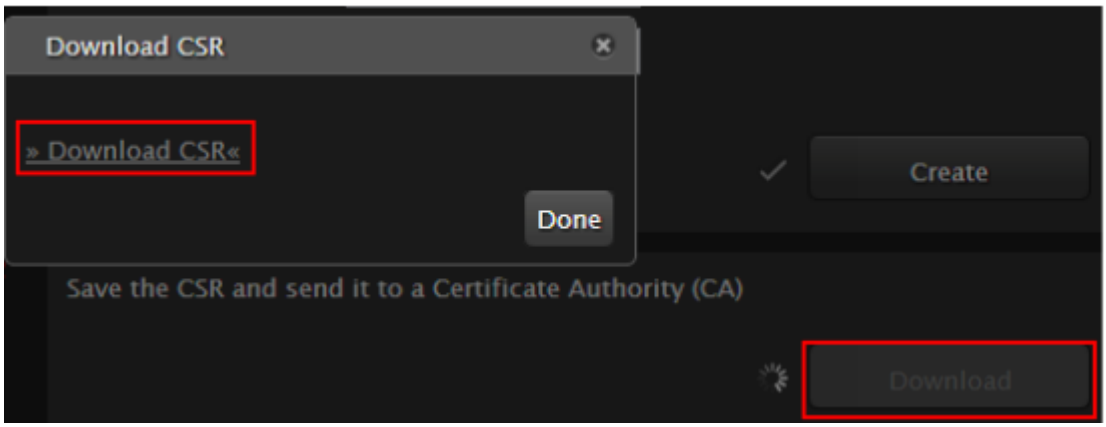


Figure 54: Downloading the CSR

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 Endpoint also have their own certificates, we recommend using a common CA for all certificates for a more efficient implementation.
8. Continue with Uploading XT Endpoint Certificates on page 103.

Uploading XT Endpoint Certificates

About this task

This procedure describes how to upload certificates which confirm the identity of an XT Endpoint, 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 Endpoint requires two certificates to be uploaded: a signed certificate identifying the XT Endpoint 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 Endpoint, it sends its identity certificate to the XT Endpoint to establish a secure connection.

To restore previously uploaded certificates or to back up certificates after uploading, see Backing Up and Restoring XT Endpoint Certificates on page 105. To delete the certificates, see Deleting XT Endpoint Certificates on page 106.

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 Endpoint (see Generating a Certificate Signing Request for XT Endpoint on page 101 for details on generating the CSR).

Procedure

1. Access the XT Endpoint web interface, as described in Accessing XT Endpoint Web Interface on page 24.
2. Select **Administrator Settings > Utilities > Certificates**.
3. Import the Certificate Authority (CA) root certificate as follows:

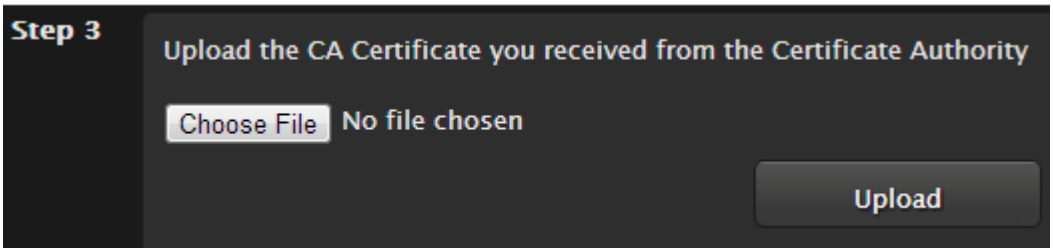


Figure 55: Uploading the CA root certificate

   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:

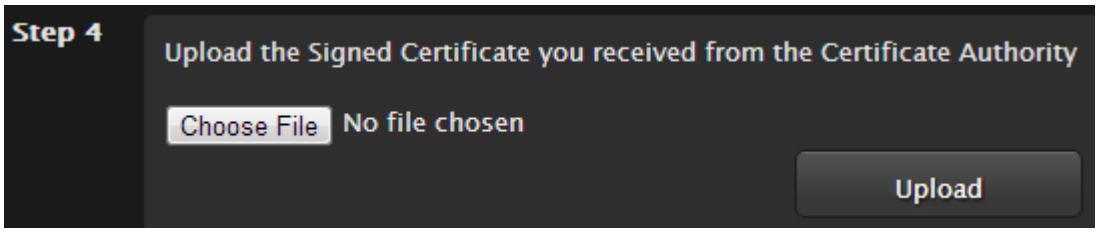


Figure 56: Uploading the signed certificate

   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 57: Signed certificate from the CA on page 105).

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 57). You can start using this certificate at the time indicated by the **notBefore** value in the signed certificate.



Figure 57: Signed certificate from the CA

5. Continue with Enabling the TLS Connection in XT Endpoint on page 107.

Backing Up and Restoring XT Endpoint 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 Endpoint Certificates on page 106.

Procedure

1. Connect a USB key to the upper USB port of the XT Codec Unit (Figure 58: Connecting a USB Key to the XT Codec Unit on page 106).

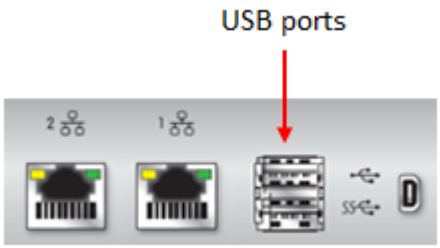


Figure 58: Connecting a USB Key to the XT Codec Unit

2. To back up a certificate to the USB key, select **Advanced > Utilities > Certificates > Backup** (Figure 59: Backing up or restoring certificates on page 106).

   The system copies the certificates and associated keys to the root folder of your USB key.



Figure 59: 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 59: Backing up or restoring certificates on page 106). This automatically restores the certificates and associated keys to the system.

Deleting XT Endpoint Certificates

About this task

This section explains how to remove or uninstall a certificate from the XT Endpoint 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:

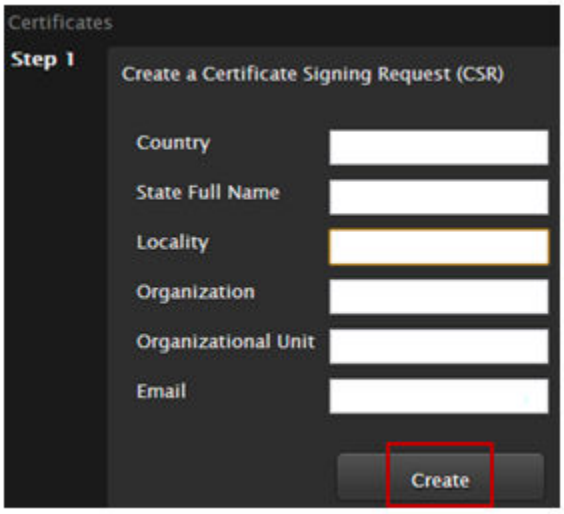
To secure SIP connections using TLS certificates, your system must have a static IP address, since the system generates the certificate request using its IP address as the Common Name (CN).

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 Endpoint Certificates on page 105.

Procedure

1. Access the XT Endpoint web interface, as described in Accessing XT Endpoint Web Interface on page 24.
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 60: Removing Current Certificates



Enabling the TLS Connection in XT Endpoint

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 Endpoint.

Before you begin

Upload the required certificates to the XT Endpoint, as described in Uploading XT Endpoint Certificates on page 103.

Procedure

1. Access the XT Endpoint web interface, as described in Accessing XT Endpoint Web Interface on page 24.
2. Select **Administrator Settings > Protocols > SIP**.
3. Select **Yes** from the **Use TLS** list to accept incoming calls using TLS.

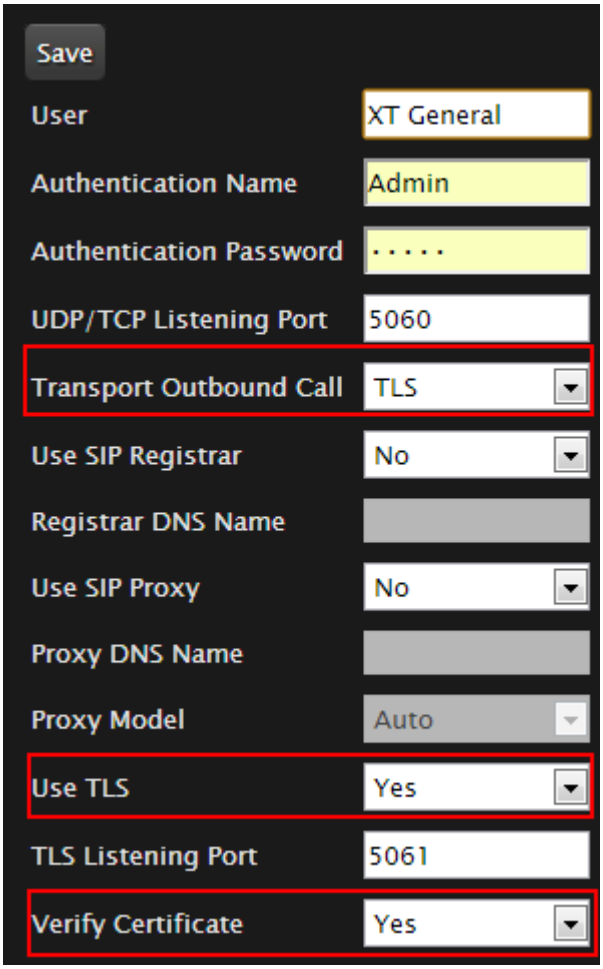


Figure 61: Enabling TLS

4. Define the following settings:

Table 36: 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 Endpoint for IP Office. • **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 Endpoint for IP Office.

5. Select **Save**.
6. (Optional) If required by your organization's security policies, continue with Enabling Encryption for Videoconferences on page 109.

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 Endpoint 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 XT Endpoint Locally from the Endpoint on page 35.

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 Endpoint Using TLS on page 100). If TLS is not enabled, only SIP calls to other XT Endpoint endpoints are encrypted, using a proprietary encryption protocol.

Procedure

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

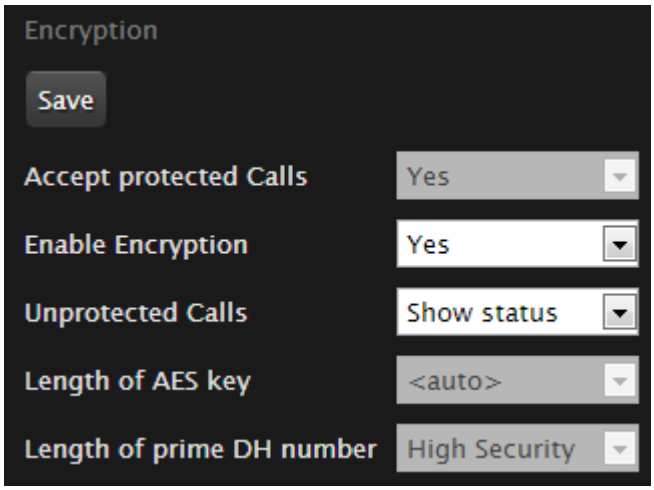


Figure 62: Encrypting calls from the web interface

2. Select **Yes** from the **Enable encryption** field.
3. Set the fields as described in Table 37: Configuring settings for securing calls on page 111.

Table 37: 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 6 | Maintaining the Scopia XT Endpoint for IP Office

This chapter details the maintenance tasks required by administrators for ongoing use of the Scopia XT Endpoint for IP Office.

Navigation

- Setting the Administrator PIN Code for the XT Endpoint on page 112
- Setting the User PIN Code for the Scopia XT Endpoint for IP Office on page 113
- Modifying the Username and Password for the XT Endpoint Web Interface on page 114
- Preparing for a Video Call or Videoconference on page 116
- Updating Software for Scopia XT Endpoint for IP Office on page 123

Setting the Administrator PIN Code for the XT Endpoint

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 Endpoint 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 Setting the User PIN Code for the Scopia XT Endpoint for IP Office on page 113. To modify the web username and password for the XT Endpoint, see Modifying the Username and Password for the XT Endpoint Web Interface on page 114.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

To modify the PIN, you must be connected via HTTPS (see Enabling Remote Management on the Scopia XT Endpoint for IP Office on page 25).

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 Endpoint web interface, select **Administrator Settings > Utilities > PIN Protect Settings > Administrator**.



Figure 63: 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 the User PIN Code for the Scopia XT Endpoint for IP Office

About this task

You can set a PIN code to access basic settings, such as the language displayed on the interface. If set, you are required to enter this code before viewing or modifying any basic settings. You can do this procedure from the endpoint itself or from the XT Endpoint web interface.

By default, you do not need to enter any PIN to access and modify basic settings.

You can also modify the administrator PIN code, required to access and modify advanced settings, such as defining camera settings. To modify the web username and password for the XT Endpoint, see Modifying the Username and Password for the XT Endpoint Web Interface on page 114.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

To modify the PIN, you must be connected via HTTPS (see Enabling Remote Management on the Scopia XT Endpoint for IP Office on page 25).

Procedure

1. Access the user PIN settings, as follows:
   - From the endpoint's main menu, select **Configure** > **Advanced > Utilities > PIN Protect Settings > Basic Settings**.

     You need to enter the PIN required to access the **Advanced** settings. The default PIN is 1234.
   - From the XT Endpoint web interface, select **Administrator Settings > Utilities > PIN Protect Settings > Basic**.



Figure 64: Modifying the user PIN

2. Set **Enable** to **Yes**.
3. If you previously set a user PIN, enter it in the **Old PIN Code** field.
4. Enter your new 4 digit PIN code.

   From the web interface only, re-enter your new PIN in the **Confirm PIN Code** field.
5. Save your changes as follows:
   - From the endpoint, select **Done**.
   - From the web interface, select **Save**.

   Use this new PIN the next time you are required access basic settings.

Modifying the Username and Password for the XT Endpoint Web Interface

About this task

This procedure describes how to change the username and password used to access the XT Endpoint web interface. We strongly recommend that you change the default credentials first time you access the XT Endpoint remotely (for more information, see Enabling Remote Management on the Scopia XT Endpoint for IP Office on page 25). You can do this procedure from the endpoint itself or from the XT Endpoint web interface.

The default credentials for remote access are:

- username - Admin
- password - 1234

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

Procedure

1. Access the remote management settings, as follows:
   - From the XT Endpoint web interface, select **Administrator Settings** > **Utilities** > **Remote Access** > **Web** (see Figure 8: Configuring remote management on XT Endpoint on page 26).
   - From the endpoint's main menu, select **Configure** > **Advanced** > **Utilities** > **Remote Access** > **Web**.

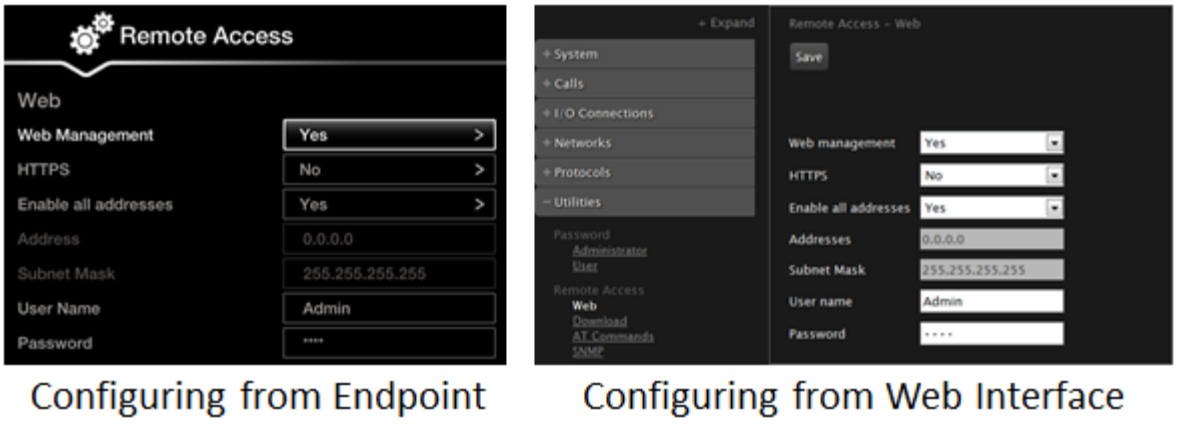


Figure 65: Modifying the username and password for the web interface

2. Modify the **User Name** and **Password** fields.

Important:

All characters can be used.

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

Preparing for a Video Call or Videoconference

This section gives recommendations on how to prepare your Scopia XT Endpoint for IP Office for a video call or videoconference.

If you need an additional HD camera, make sure it is correctly connected as described in the *Installation Guide for Scopia XT Endpoint for IP Office*.

Navigation

- Saving a Camera Position on page 116
- Saving a Camera Position from the Web Interface on page 118
- Setting Your Recording Preferences on page 119
- Setting a Time Limit for Videoconferences on page 121

Saving a Camera Position

About this task

You can change the camera position before or during a call and save that position for later use as one of several presets.

To move the camera to a previously saved position, press and hold the number corresponding to the camera position on the XT Remote Control Unit. The camera moves to the stored position.

This procedure describes how to position your local camera or another Scopia XT Endpoint for IP Office endpoint's camera, and store up to 10 camera positions from the endpoint. You can store many more positions from the web interface, as described in Saving a Camera Position from the Web Interface on page 118.

Important:

You can control a remote camera when connected to it, as long as it is configured to be remotely managed.

Procedure

1. Position the camera:
   a. Select **Control Camera** from the Main menu (or from the In-Call menu, during a call).

      Important:

      To position the remote camera, press **ok/menu** and select **Control Far**.

b. Move the camera position using the arrow keys, alter the zoom with the zoom keys, .

Important:

To switch to a different camera, press **ok/menu** on the XT Remote Control Unit and select **Video Source** (Figure 66: Storing camera presets on page 117).

2. To save this position for future use:

a. Press **ok/menu** on the XT Remote Control Unit and select **Presets** (Figure 66: Storing camera presets on page 117).

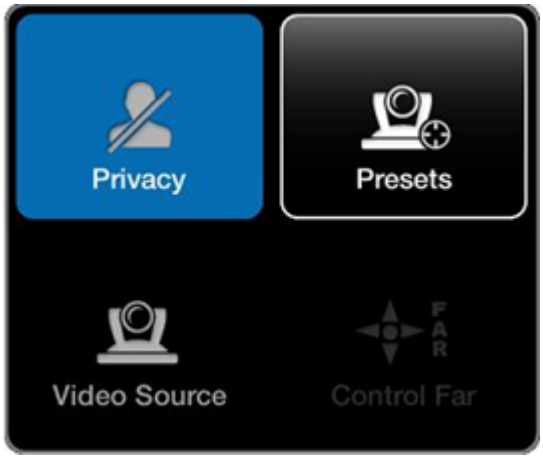


Figure 66: Storing camera presets

b. Press a number between 0-9 on the XT Remote Control Unit to store a position.

Important:

To delete a previously stored position, press its ID and the **Delete** key using the XT Remote Control Unit.

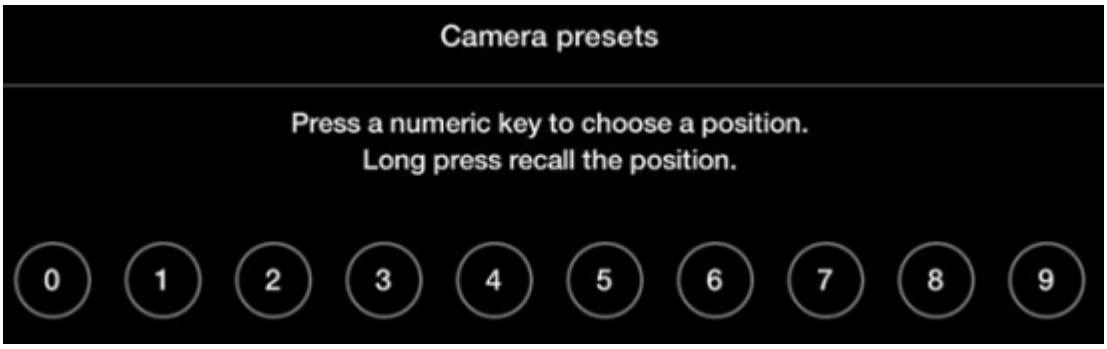


Figure 67: Selecting the camera position

3. Press **ok/menu**.

The number of the preset is now blue, indicating that it was successfully stored. Use the camera position ID in the future to quickly adjust your camera.



Figure 68: Camera position stored successfully

Saving a Camera Position from the Web Interface

About this task

You can change the camera position before or during a call and save that position for later use as one of several presets.

This procedure describes how to position your local camera, and store dozens of camera positions from the web interface. You can store up to 10 positions from the endpoint interface, as described in Saving a Camera Position on page 116.

Important:

You can control another Scopia XT Endpoint for IP Office endpoint's camera when connected to it, as long as it is configured to be remotely managed.

Procedure

1. Access the XT Endpoint web interface, as described in Accessing XT Endpoint Web Interface on page 24.
2. Select **More Actions** > **Camera Control**.

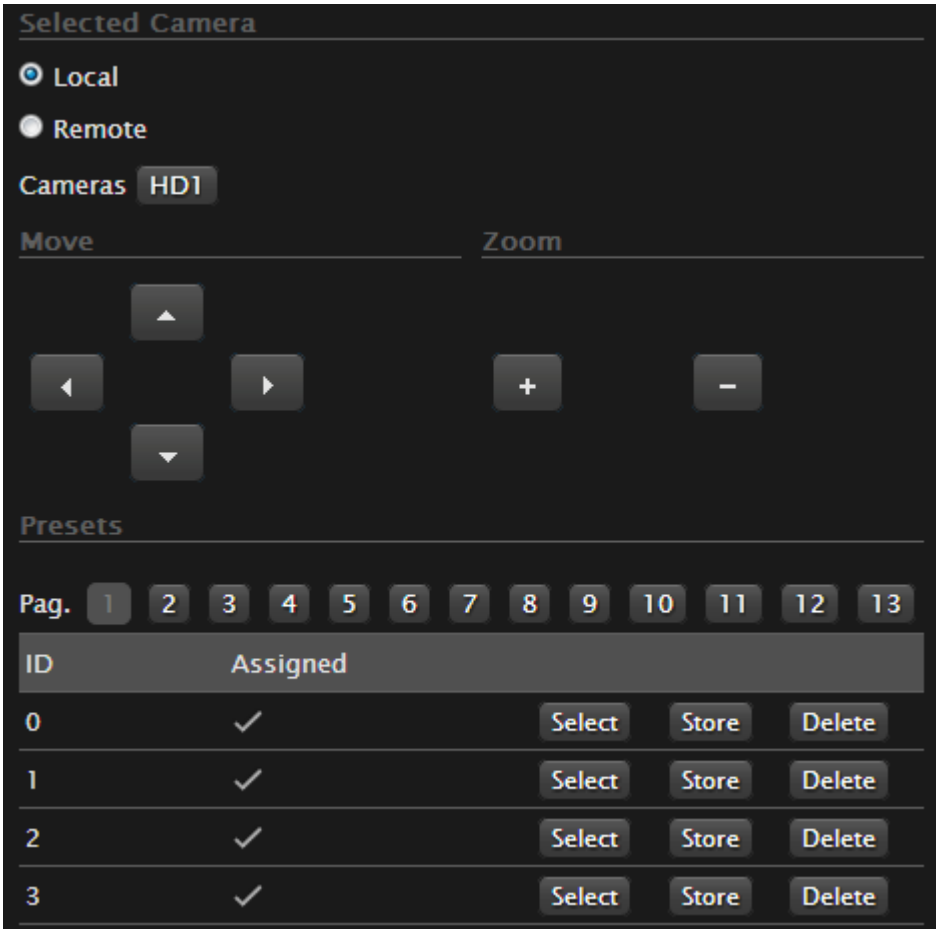


Figure 69: Camera Control page

3. To move the camera to a previously saved position, choose the ID of the camera position and choose **Select**.

   The camera moves to the preset position.

4. Move the camera position using the arrow and zoom icons.

5. To store the position, select a number between 0-121 to identify the camera position, and select **Store**.

   The position is now stored. Use the camera position ID in the future to quickly adjust your camera.

Setting Your Recording Preferences

About this task

You can record videoconferences and store them to a connected USB storage device. This procedure describes how to configure your recording preferences, such as the video resolution and bitrate. This is useful, for example, to increase the time available for recording on your USB storage device. You can do this procedure from the endpoint itself or from the XT Endpoint web interface.

This may require a license, depending on your model. For more information, see Installing and Enabling Licenses which Extend System Functionality on page 39.

You can play the recordings using any standard media player. The system saves the file as an MP4, and records the video in H.264 format and audio in AAC-LC format.

You cannot record videoconferences when encryption is enabled. For more information, see Enabling Encryption for Videoconferences on page 109 or contact your administrator. When recording a videoconference, you can include up to 5 remote endpoints.

Procedure

1. Access the recording settings:
   - From the XT Endpoint web interface, select **Basic Settings > Recording > General.**
   - From the endpoint's main menu, select **Configure > Recording**.

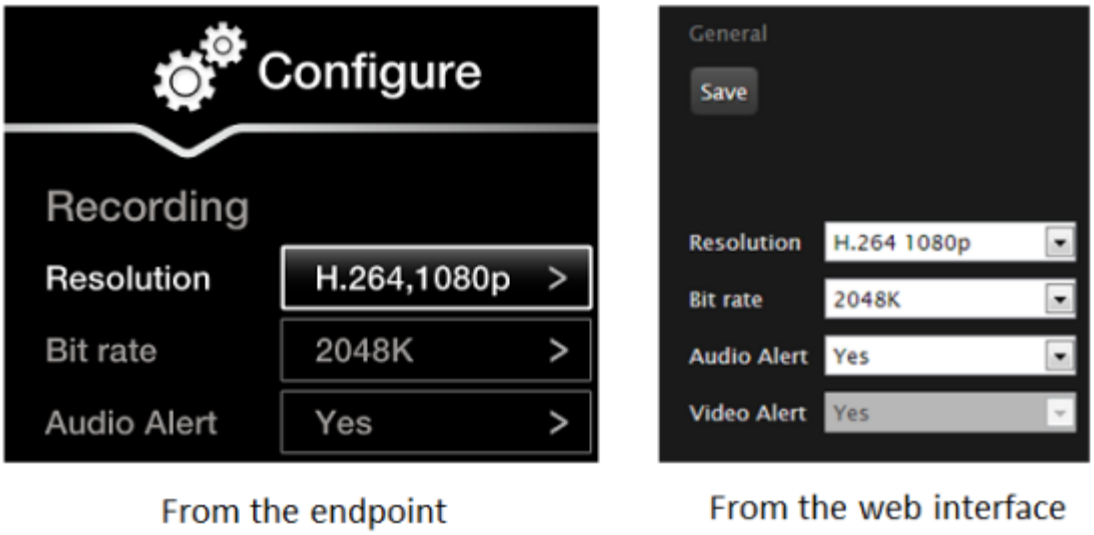


Figure 70: Setting your recording preferences

2. Define the following recording settings:

Table 38: Configuring recording settings

Field	Description
Resolution	Select the video resolution to use for recording from the list. The frame rate is limited to 25 frames per second. For the best quality, we recommend using the default video resolution, 1080p. You can lower the video resolution during a recording if the media player or device used to view recordings does not support all video resolutions. When you change the resolution, the system automatically selects the optimal bitrate for this resolution.
Bit rate	Select the recording bitrate to determine the file size of the recording. To use less space on your USB storage device for recordings, select a lower bitrate. For the best results, use the default value for your chosen resolution. 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. To estimate the space you need for the recording, see Table 39: Typical file sizes based on the bitrate on page 121. You can see how much recording time is available on your USB storage device when you access the **Recording** menu (for details, see Starting a Recording).
Audio Alert	Select **Yes** to enable an audio message alert at the beginning of the videoconference, indicating to all participants that the meeting is being recorded. This alert is also sent to late participants.

Table 39: Typical file sizes based on the bitrate

Bitrate	File size for 1 minute recording	File size for 30 minute recording	File size for 1 hour recording
6144K	45 MB	1,350 MB	2,700 MB
4096K	30 MB	900 MB	1,800 MB
2048K	15 MB	450 MB	900 MB
1024	7.5 MB	225 MB	450 MB
512	3.75 MB	112.5 MB	225 MB
384	3 MB	85 MB	169 MB

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

Setting a Time Limit for Videoconferences

About this task

Set a time limit for videoconferences to alert users that the time allocated for the meeting is about to end, and to end open videoconferences that were not properly disconnected.

Once you set a time limit:

- An alert appears during the videoconference when the time limit is reached. The user can then decide to do one of the following:
  - Disconnect the videoconference
  - Postpone the reminder and extend the meeting for another hour
  - Remove the limit for this videoconference
- The meeting is automatically disconnected if there is no response to the alert for 30 seconds.

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

Procedure

1. Access call settings:
   - From the XT Endpoint web interface, select **Administrator Settings > Call > Preferences > General**.
   - From the endpoint's main menu, select **Configure > Advanced > Calls > Preferences > General**.

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

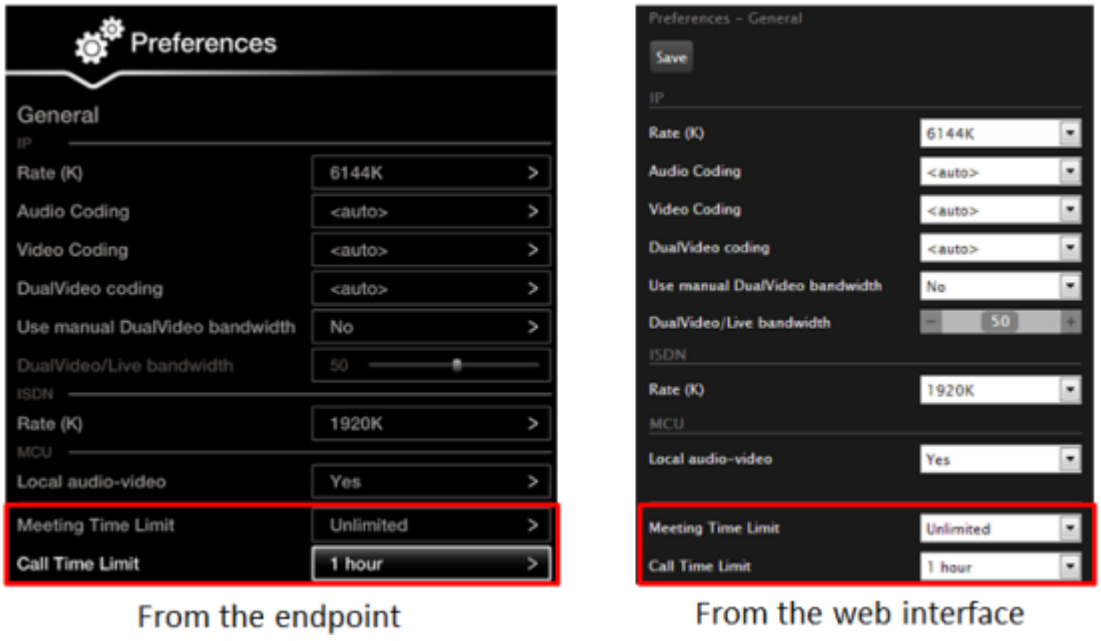


Figure 71: Setting a Time Limit for Videoconferences

2. Define the time limit for meetings with multiple participants in the **Meeting Time Limit** field.

By default, the time limit is **Unlimited**. The maximum limit you can set is 24 hours.

3. Define the time limit for point-to-point calls in the **Call Time Limit** field.

   By default, the time limit is **Unlimited**. The maximum limit you can set is 24 hours.

Updating Software for Scopia XT Endpoint for IP Office

This section describes how to upgrade the software running on the XT Codec Unit.

Important:

Any software version, even if it is restricted by a license, can run in a temporary mode for 24 hours. After that, you must enter a new license key or download the previous allowed version.

The software version 3.0 does not need a license.

The software update package is an auto-extracting file containing a software version, usually with a filename indicating the exact version number (for example: XT5000_V3_0_115.exe). You can update the software version in one of the following ways:

- Upgrading the Software Using a PC on page 125: Download and run a new software package from the Radvision web or FTP site.

  Downloading the update package from the Radvision web or FTP site ensures you get the latest available version.

  For more information, see http://licensing.radvision.com/.

- Upgrading the Scopia XT Endpoint for IP Office Software Using a USB Drive on page 127: Run the software package on the USB key that is shipped together with the product.

  You need to first download the latest upgrade available to your USB.

During the software upgrade, you cannot use the XT Codec Unit to make calls or perform configurations. All the configuration settings and user data are preserved in the update process.

Upgrading to a major version requires a new license key. The first and second digits in the version number indicate the major version number. For example, in version 3.1.0.005, the major version number is “3.1”.

Important:

You can always downgrade the system to a previous version. Call customer support for help.

Navigation

- Configuring Remote Upgrade Settings on page 123
- Upgrading the Software Using a PC on page 125
- Upgrading the Scopia XT Endpoint for IP Office Software Using a USB Drive on page 127

Configuring Remote Upgrade Settings

About this task

In order to upgrade your Scopia XT Endpoint for IP Office 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 Endpoint web interface.

Before you begin

- If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.
- 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 Endpoint for IP Office on page 25.

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 Endpoint web interface, select **Configure** > **Advanced** > **Utilities** > **Remote Access** > **Download**.

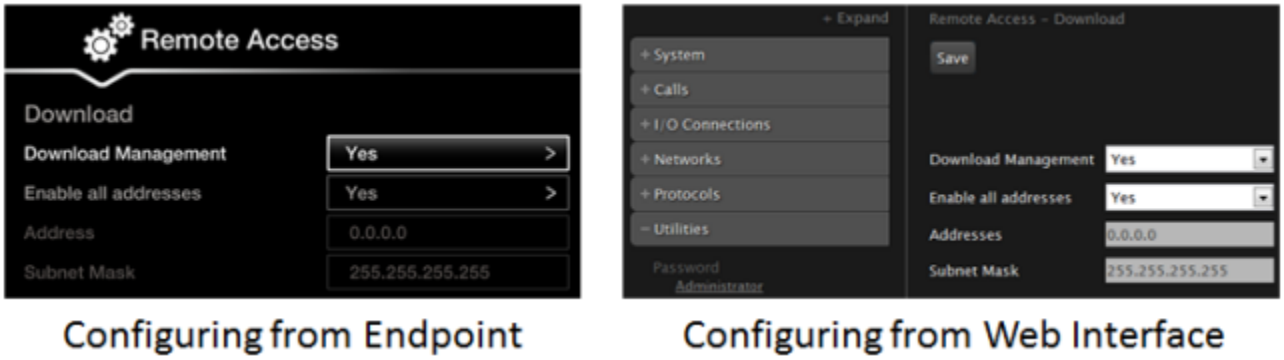


Figure 72: Enabling remote access to the XT Endpoint

2. Set the fields as described in Table 40: Enabling remote upgrade on page 125.

Table 40: 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, as follows: • Select **Yes** to enable remote downloads to the XT Endpoint. • Select **No** to disable remote downloads to the XT Endpoint.
Enable all addresses	Allow access to the XT Codec Unit from all or specific PCs, as follows: • Select **Yes** to enable access to XT Endpoint 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 XT Endpoint.
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.

3. From the web interface only, select **Save**.
4. To upgrade the XT Endpoint, see Updating Software for Scopia XT Endpoint for IP Office on page 123.

Upgrading the Software Using a PC

About this task

This section describes how to upgrade the software running on the XT Codec Unit by downloading the upgrade package to a computer in the network. If your network is configured so that only specified PCs can remotely manage the Scopia XT Endpoint for IP Office, make sure to download the upgrade package to this computer.

Before you begin

- If you upgrade to a major version, ensure you have a new license key (for details, see Registering the Scopia XT Endpoint for IP Office to Obtain a License Key on page 38).
- Verify that this PC is allowed to remotely manage this Scopia XT Endpoint for IP Office. By default, all PCs in a network can remotely manage the Scopia XT Endpoint for IP Office. See Enabling Remote Management on the Scopia XT Endpoint for IP Office on page 25 for more details.
- Enable the remote upgrade as described in Configuring Remote Upgrade Settings on page 27.

- Download the update as explained in Updating Software for Scopia XT Endpoint for IP Office on page 123, or contact Customer Support.
- Ensure that a computer in your network with Windows OS is available.

Procedure

1. Verify the XT Codec Unit is switched on, and is connected to the IP network interface.

   The network cable must be connected to the rightmost GLAN connector, GLAN1, on the back panel of the XT Codec Unit.

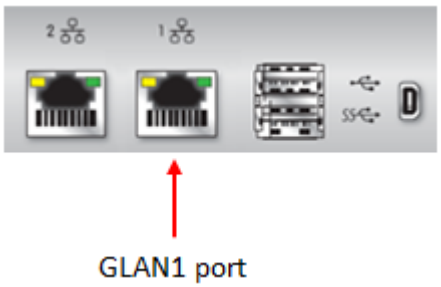


Figure 73: GLAN1 port

2. Verify that the network allows communication between the Codec Unit and the computer, and that a firewall does not block TCP port 55099.
3. Download the .exe file (for example, XT5000_Vxxx.exe) from the Radvision site to the computer.

   Important:

   The XT5000_Vxxx.exe upgrade package can be used to upgrade any Scopia XT Executive, XT4000, or XT Endpoint.

4. On the computer, launch the .exe upgrade file. It automatically starts the upgrade program.
5. Enter the IP address of the XT Codec Unit in the start screen and select **Start**.

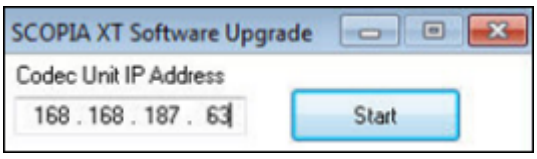


Figure 74: Upgrading the firmware of the Scopia XT Endpoint for IP Office

   The software is downloaded to the XT Codec Unit. You can view the progress on the Scopia XT Endpoint for IP Office.

   Caution:

   After download begins do not shut down the XT Codec Unit until download is completed. At the end of the update, the XT Codec Unit reboots automatically.

6. The upgrade procedure may automatically continue after the reboot, and therefore reboot again. Wait a few minutes to ensure that the upgrade procedure is completed.

Important:

Do not turn off the Scopia XT Endpoint for IP Office before the upgrade procedure is completed.

Upgrading the Scopia XT Endpoint for IP Office Software Using a USB Drive

About this task

Your Scopia XT Endpoint for IP Office comes with a USB drive containing the latest firmware version available at the time the system was shipped. We recommend that you always access the Radvision site to check if a later version is available.

Before you begin

Check if a later version is available by accessing the Radvision site as explained in Updating Software for Scopia XT Endpoint for IP Office on page 123.

If a later version is available, download it and copy onto the USB drive.

Procedure

1. Turn on the Scopia XT Endpoint for IP Office.
   Wait for the menus to appear on the monitor.
2. Insert the USB drive into one of the USB ports on the back panel of the XT Codec Unit.

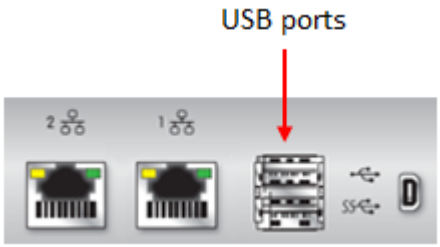


Figure 75: The USB ports on the back panel of the Scopia XT Endpoint for IP Office

The upgrade procedure begins automatically.

Caution:

After download begins do not shut down the XT Codec Unit until download is completed.

3. Follow the instructions displayed on the screen.
   The system restarts automatically after the upgrade procedure is completed.
4. The upgrade procedure may automatically continue after the reboot, and therefore reboot again. Wait a few minutes to ensure that the upgrade procedure is completed.

Important:

Do not turn off the Scopia XT Endpoint for IP Office before the upgrade procedure is completed.

5. If the upgrade fails, see USB Software Upgrade Failure on page 151.

Chapter 7 | Troubleshooting the Scopia XT Endpoint for IP Office

This section covers troubleshooting problems that may occur when setting up and using the Scopia XT Endpoint for IP Office.

Navigation

- Viewing System Information for Customer Support on page 129
- Resolving Problems Connecting Calls on page 131
- Resolving Problems with Audio on page 132
- Echo Cancelling on HDMI Monitors on page 134
- Resolving Monitor Display Problems on page 136
- Improving Call Video Resolution on page 138
- Resolving Lip Sync Problem on page 140
- Resolving Camera Issues on page 142
- Resolving IP Address Problems on page 144
- Resolving Problems with PC Presentations on page 146
- Resolving XT Remote Control Unit Problems on page 146
- Resolving Problems with Displaying Video on page 147
- How to Retrieve Scopia XT Endpoint for IP Office Logs on page 149
- USB Software Upgrade Failure on page 151
- Restoring Default User Settings on page 152

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:

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

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

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 Endpoint 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**.

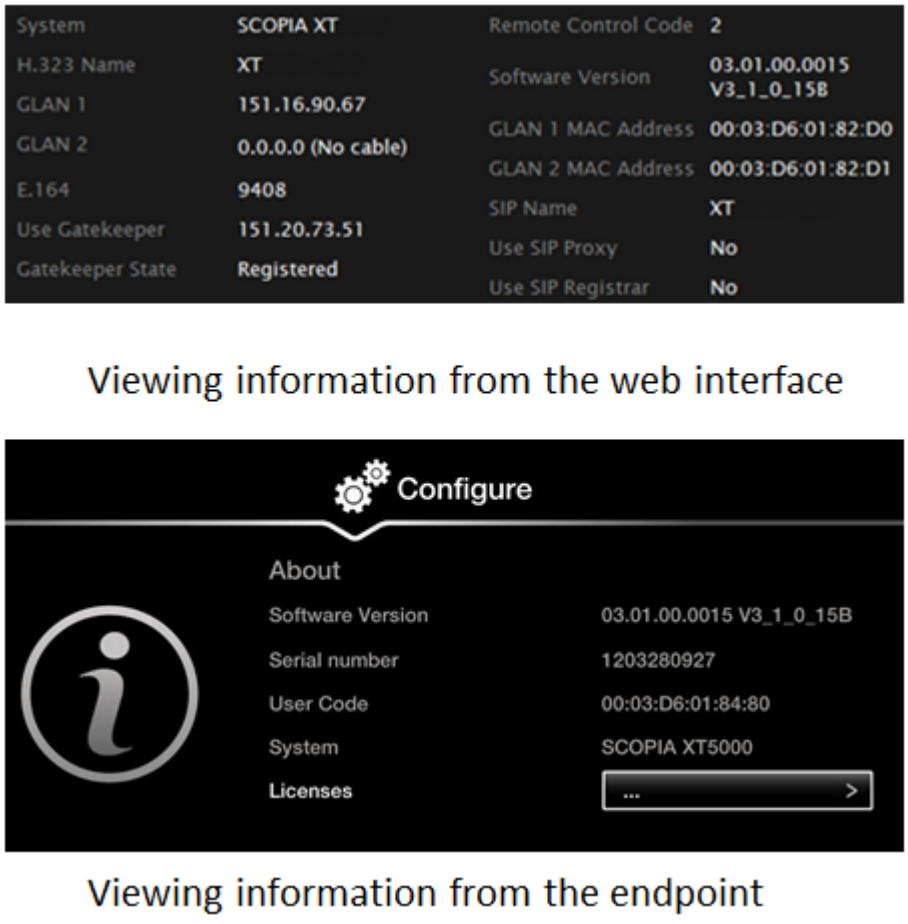


Figure 76: Viewing system information

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 77: Viewing system network information

Resolving Problems Connecting Calls

Problem	Cannot dial out or connect to an outgoing SIP or H.323 video call.
Solution	Verify you dialed the correct number or address.
Solution	Recheck the **Network Configuration**, **Network Preferences** and **H.323/SIP Proxy** settings, described in Configuring Network Settings on page 81.
Problem	Cannot receive a SIP or H.323 video call.
Solution	Verify the number/address used to connect to you is correct.
Solution	Recheck the **Network Configuration**, **Network Preferences** and **H.323/SIP Proxy** settings, described in Configuring Network Settings on page 81.
Solution	Make sure the Do Not Disturb (DND) function is not enabled. DND is indicated by the ⛔ icon in the top bar on the menu screens.
Problem	Cannot connect to a videoconference.
Solution	Check you dialed the correct conference number.
Solution	Check you are registered to the correct gatekeeper or SIP Proxy.

Problem The other party in a call cannot see or hear me.

Solution Make sure your Microphone Pod is correctly connected to the system.

Solution Make sure the **Video Privacy** and **Mute** functions are not enabled. You can see this in the top bar of the system's menus: No video or No audio .

Solution If the other site can hear, but not see, make sure your **Call Type** is set to **Audio & Video**, not **Audio Only**:

1. Disconnect the call.
2. Select **Call** from the Main menu, and press **ok/menu**.
3. Select the arrow to access the **Advanced Calling Options**.

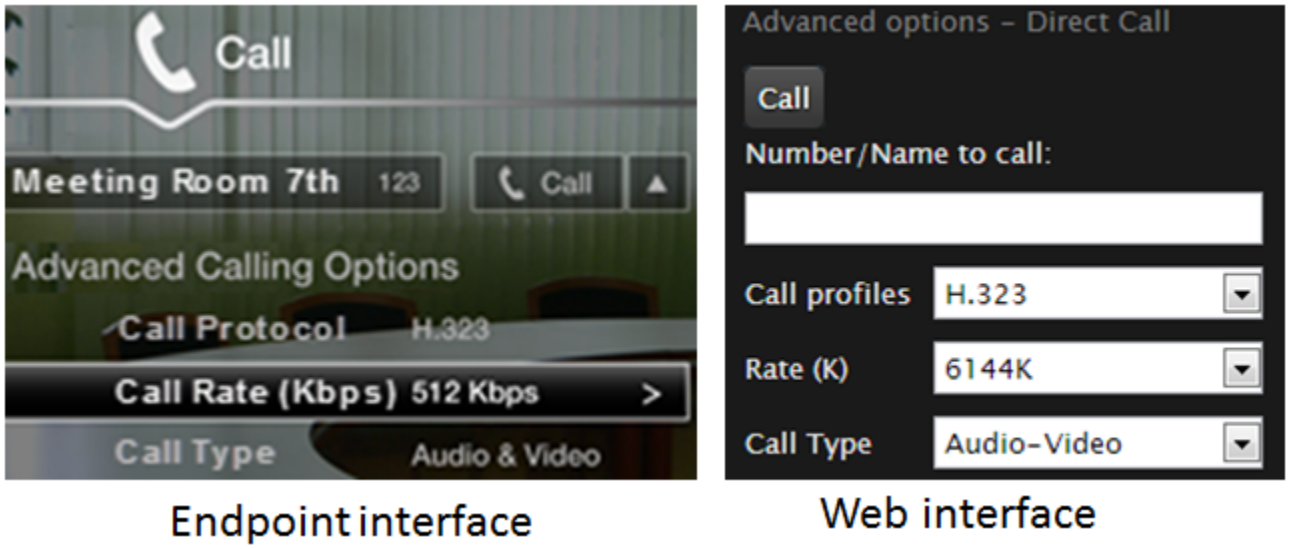


Figure 78: Changing advanced call settings

4. Check that the **Call Type** is set to **Audio & Video**.
5. Redial the same contact.

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**.

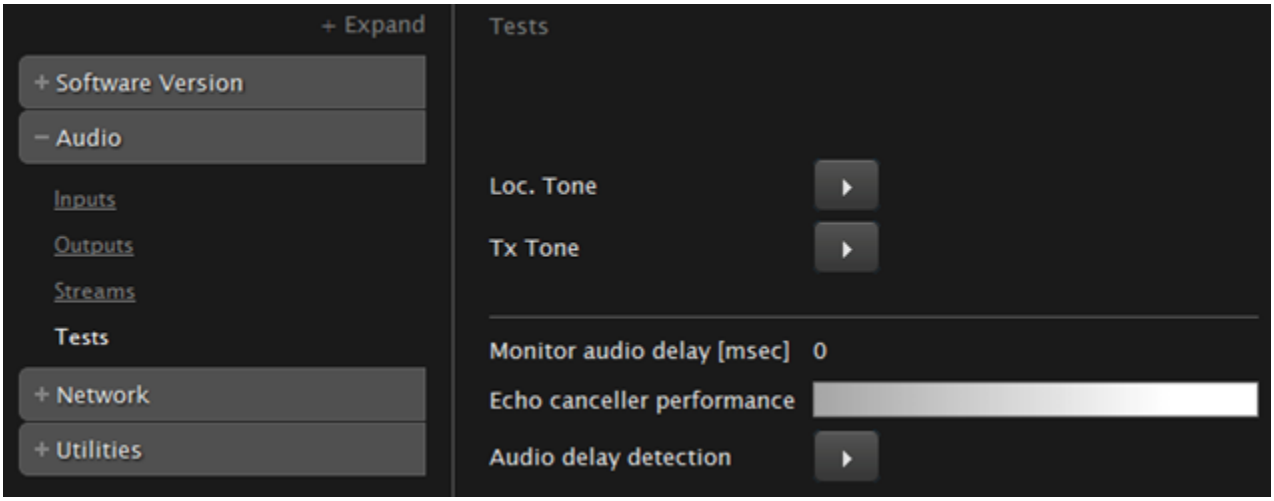


Figure 79: Performing the audio tests from the web interface

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

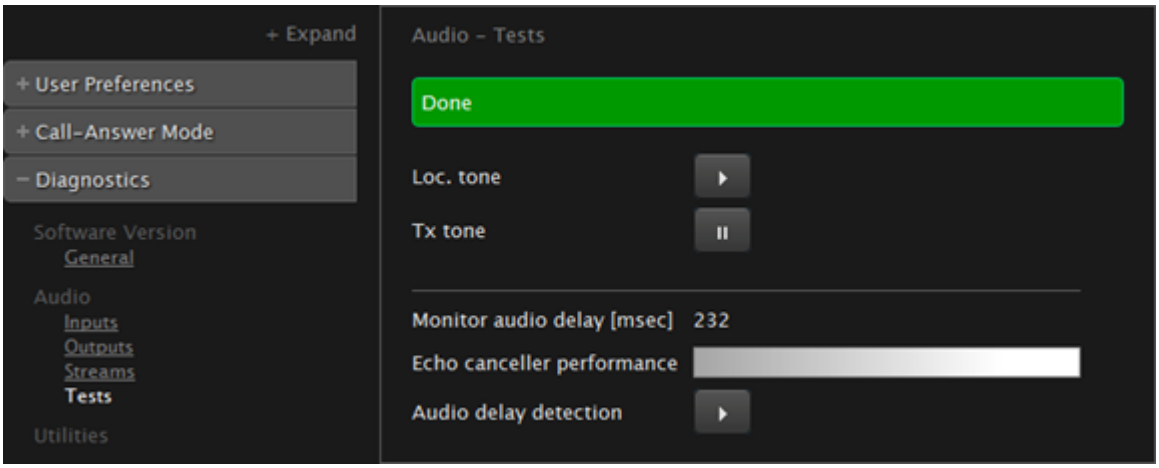


Figure 80: The audio test completed successfully from the web interface

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 XT Endpoint Locally from the Endpoint on page 35.

Procedure

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

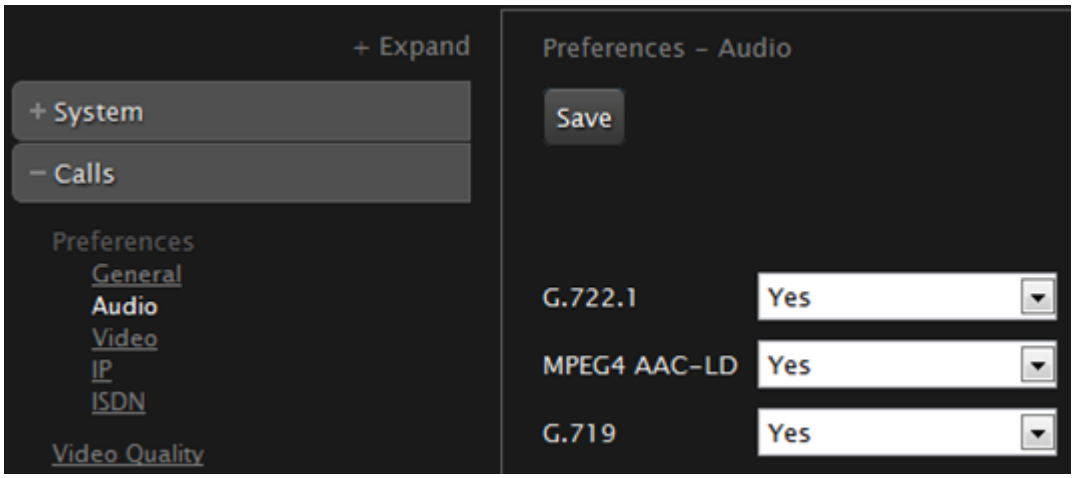


Figure 81: Configuring audio settings from the web interface

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 XT Endpoint Locally from the Endpoint on page 35.

Procedure

1. Access the echo cancellation settings, as follows:
   - From the Scopia XT Endpoint for IP Office 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**.

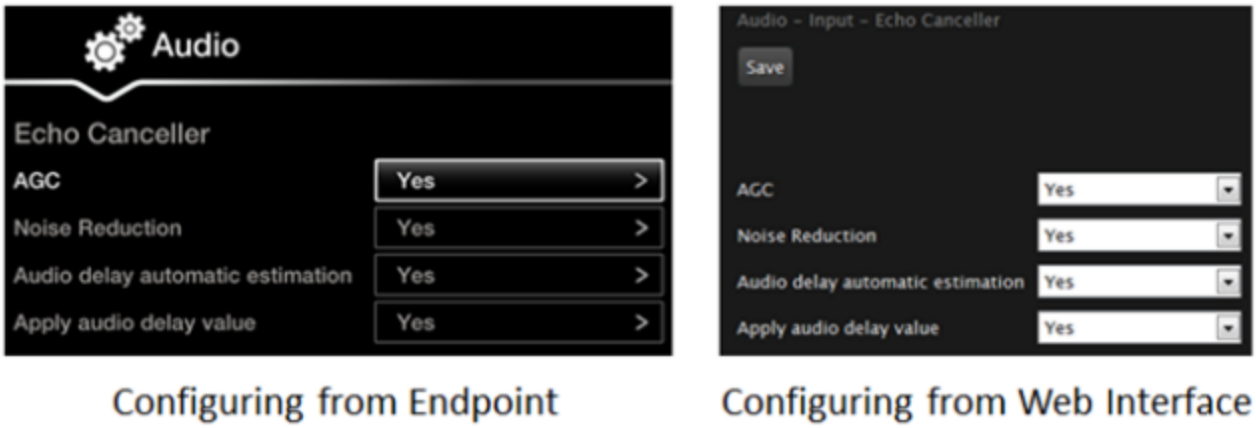


Figure 82: Configuring echo cancellation settings

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**.

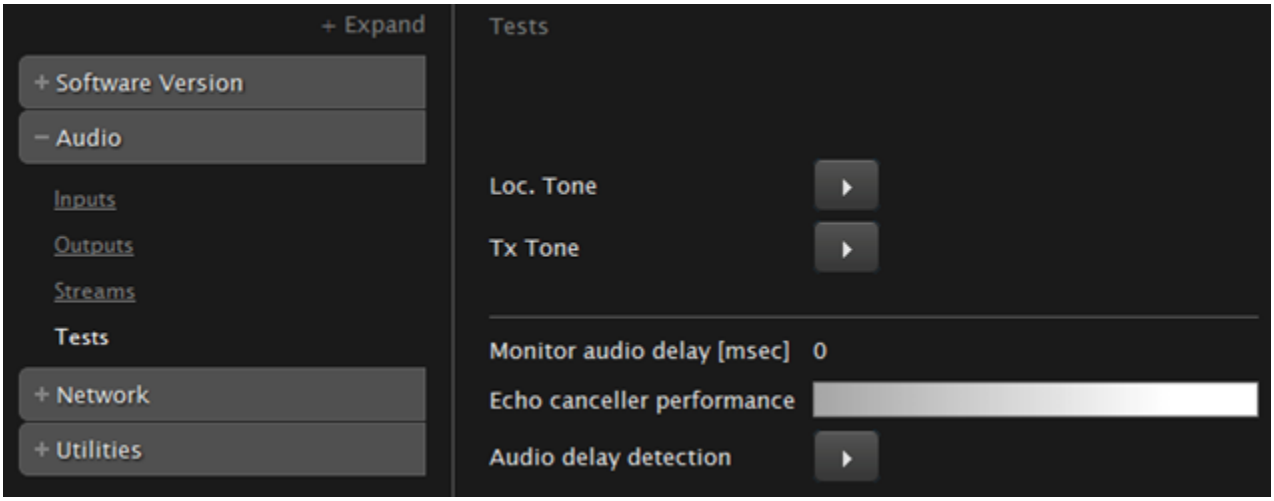


Figure 83: Testing the audio from the web interface

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 48 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 XT Endpoint Locally from the Endpoint on page 35.

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 Endpoint 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. **Important:** You can also adjust the image for the monitor displaying the system menu, in the quick setup
Left	

Option	Description
Bottom	wizard as described in Adjusting the Image Position on page 48.
Right	

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

Improving Call Video Resolution

Problem My call does not perform at 1080p, even though the camera is capable of 1080p and 1080p is enabled on the Scopia XT Endpoint for IP Office.

Solution Make sure the remote system also supports 1080p. Remote systems that are limited to 720p or less negotiate lower resolutions with the Scopia XT Endpoint for IP Office.

Solution Make sure the camera is connected to the HD CAM1 input port of the XT Codec Unit.

Solution Make sure the **Moving** setting is enabled as described below.

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

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 Scopia XT Endpoint for IP Office web interface, select **Administrator Settings** > **I/O connections** > **Cameras** > **HD1**.

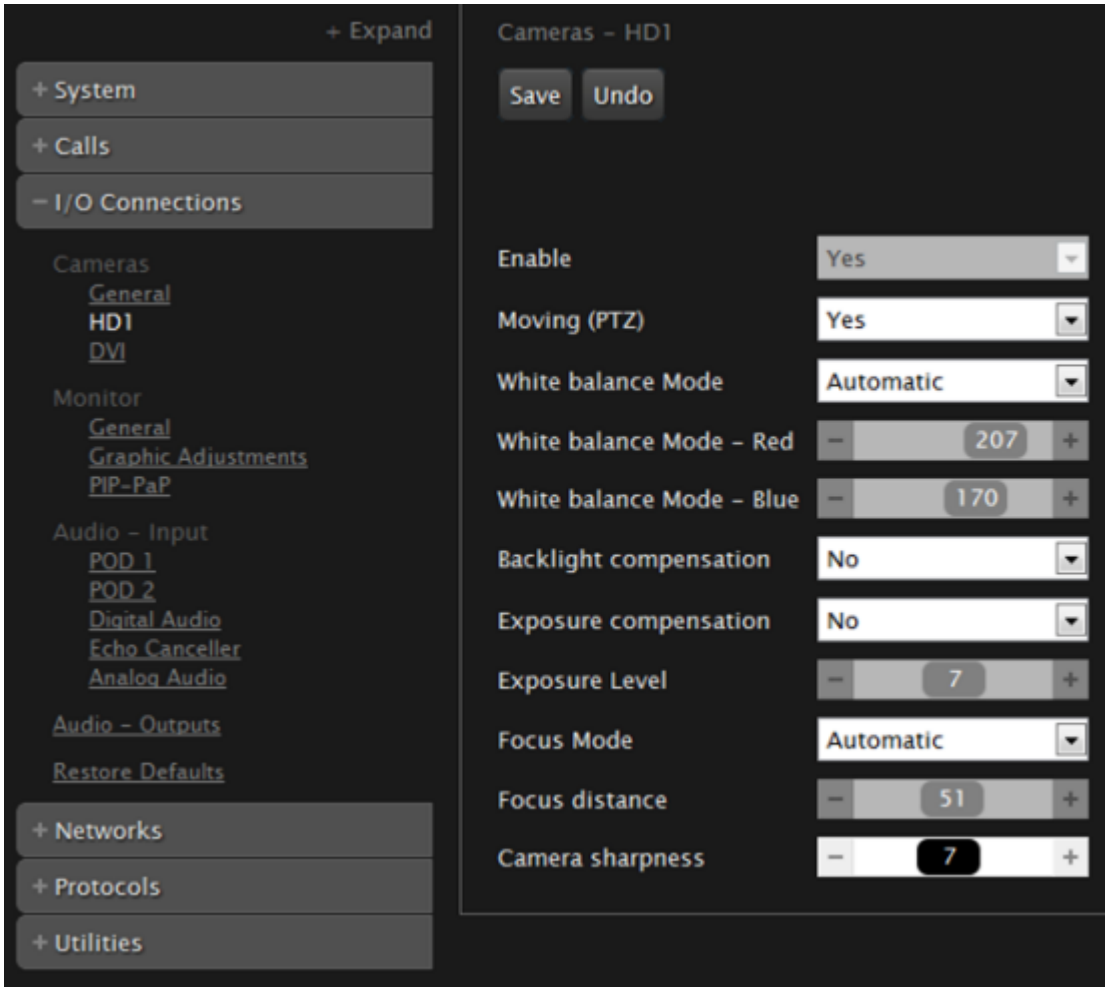


Figure 84: Enabling the Moving setting from the web interface

2. Make sure that the **Moving** field is set to **Yes**.
3. From the web interface only, select **Save**.

Solution

Make sure 1080p is enabled as described below.

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

1. Access the video settings by doing one of the following:
   - From the Scopia XT Endpoint for IP Office web interface, select **Administrator Settings** > **Calls** > **Preferences** > **Video**.

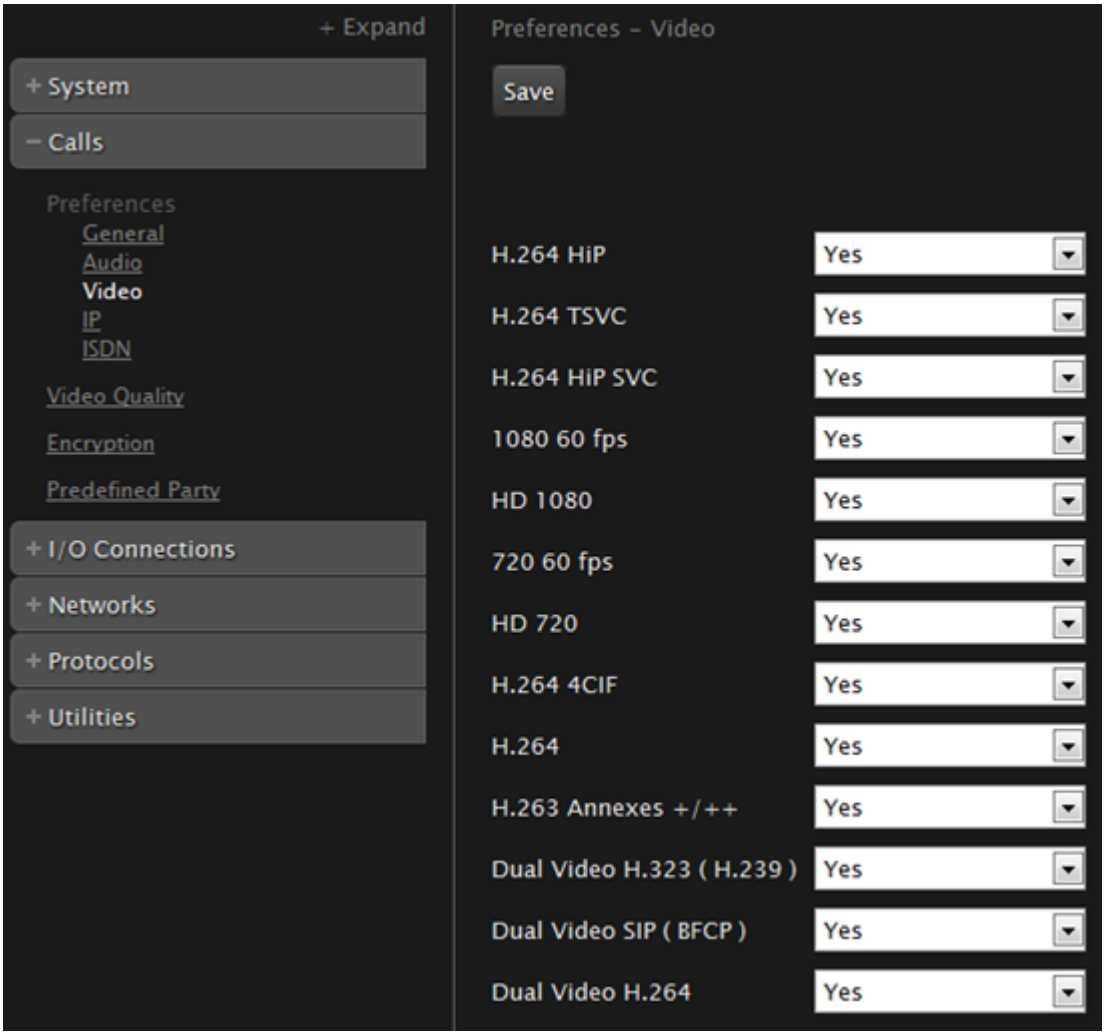


Figure 85: Enabling 1080p 60fps setting

- From the endpoint's Main menu, select **Configure** > **Advanced** > **Calls** > **Preferences** > **Video**.

2. Ensure that the **1080 60fps** field is set to **Yes**.
3. From the web interface only, select **Save**.

Solution Make sure the network connection to the remote endpoint has enough bandwidth. Low bandwidth conditions results in a reduction of resolution at the XT Codec Unit.

Solution Make sure the VISCA cable is connected to the VISCA IN port of the camera. The VISCA cable is part of the cable harness that connects the camera to the XT Codec Unit and is used to control the camera. A common mistake is to connect this cable to VISCA OUT instead of VISCA IN. This prevents the XT Codec Unit from setting the camera to the necessary resolution. For details, see *Installation Guide for Scopia XT Endpoint for IP Office*.

Resolving Lip Sync Problem

Problem There is a lack of synchronization between audio and video.

One of the optional video devices, an optional camera or a video converter, causes the video delay.

Solution Configure lip sync settings.

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

1. Access the video quality settings by doing one of the following:
   - From the XT Endpoint web interface, select **Administrator Settings** > **Calls** > **Video Quality** > **General**.
   - From the endpoint's main menu, select **Configure** > **Advanced** > **Calls** > **Video Quality**.

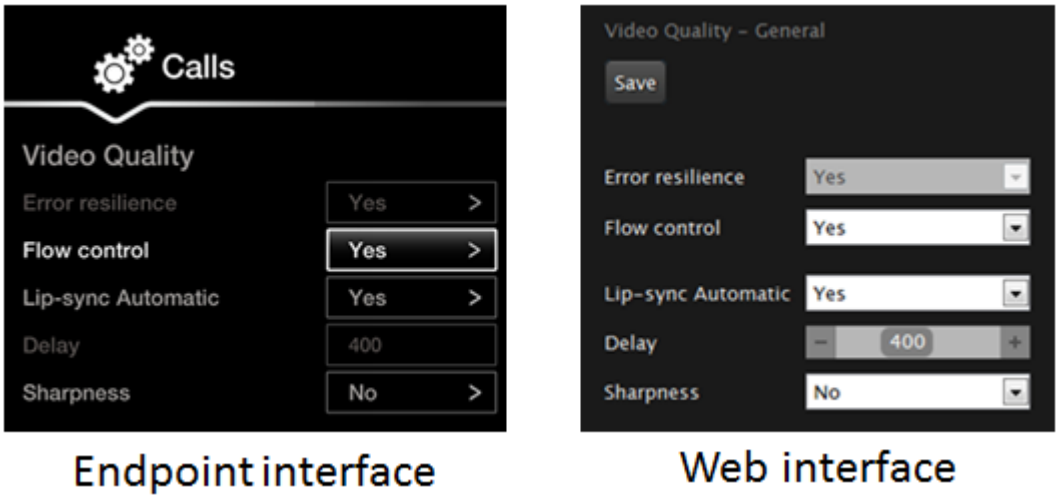


Figure 86: Configuring the lip sync settings via endpoint interface

2. Set the fields as described in Table 42: Configuring video quality settings on page 141

Table 42: Configuring video quality settings

Field Name	Description
Error resilience	Set to **Yes** to minimize error in case of packet loss (for example, due to network congestion).
Flow Control	If set to **Yes**, a Flow Control (bandwidth reduction) request is sent to the remote terminal in case of packet loss.
Error strategies	If set to **Yes**, you may set the number of allowed line errors before video is frozen.

Field Name	Description
Fluency	Indicates the number of allowed line errors, if the **Error strategies** field is set to **Yes**. Drag the slider to the required value. At minimum setting, video frames freeze at the first occurring error. At maximum setting, video frames never freeze and errors are allowed to pass through.
Lip-sync automatic	Allows synchronizing audio with video. To have a perfect synchronization between audio and video, you must adjust according to the type of connection. If set to **Yes**, the system will perform automatic synchronization (highly recommended setting). If set to **No**, adjust manually by dragging the **Delay** slider until you obtain the best synchronization.
Delay	Received audio delay in milliseconds. If **Lip-sync automatic** is set to **No**, drag the slider until you obtain the best synchronization.
Sharpness	Enable/disable video sharpness.

3. 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 Endpoint for IP Office web interface by selecting **More Actions > Web Video**:

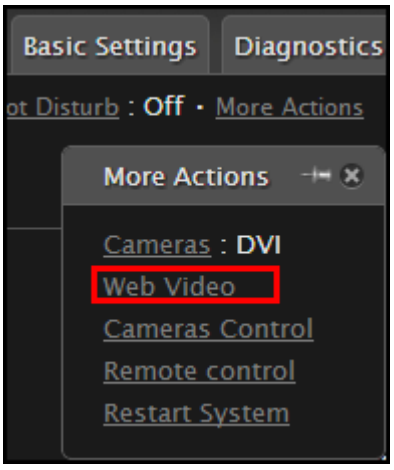


Figure 87: Remotely monitoring your camera's

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.

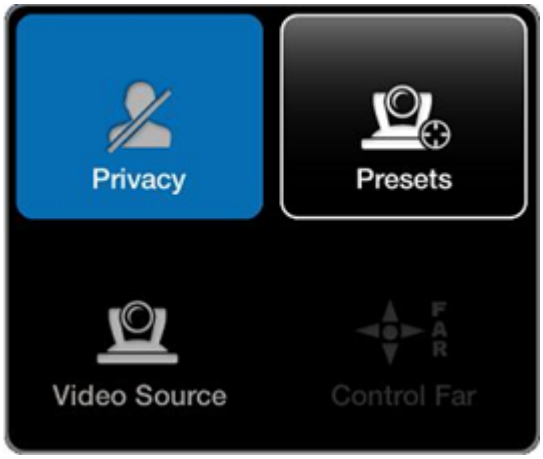


Figure 88: Selecting a video source

3. Select **Video Source**.

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

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

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Endpoint Locally from the Endpoint on page 35.

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 Endpoint web interface, select **Administrator Settings** > **I/O connections** > **Cameras** > **HD1**.

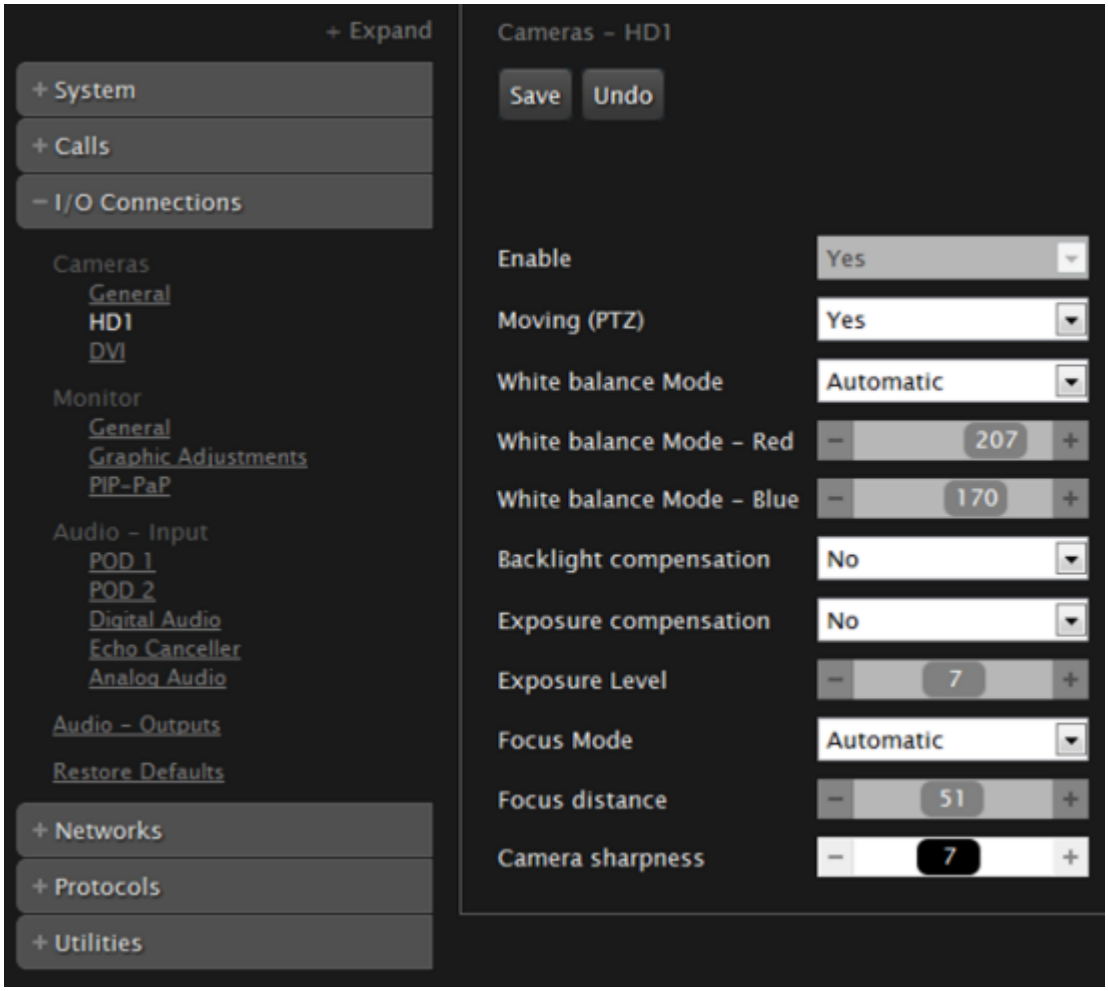


Figure 89: Enabling the Moving setting

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 129).

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 90: GLAN1 port on page 145.

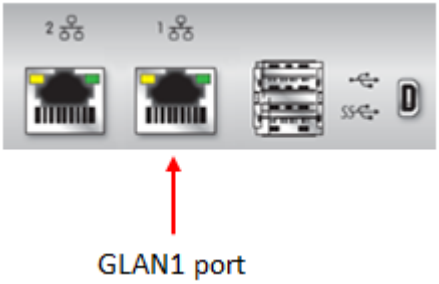


Figure 90: GLAN1 port

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 81.

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 XT Endpoint Locally from the Endpoint on page 35.

1. From the endpoint's main menu, select **Configure** > **Quick Setup**.
2. Press **Next** several times until the **Configure TCP/IP** screen appears.



Figure 91: 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 XT Endpoint Locally from the Endpoint on page 35.

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

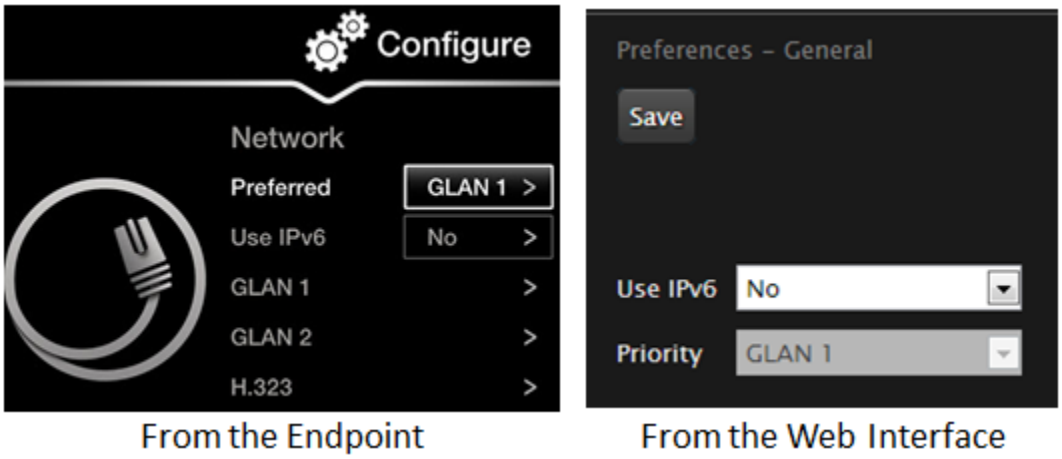


Figure 92: Setting network preferences

2. Set the **Use IPv6** field to **Yes**.
3. From the web interface only, select **Save**.

Resolving Problems with PC Presentations

Problem I cannot send a presentation from my PC.

Solution Make sure the VGA/DVI cable is properly connected between the PC and the XT Codec Unit, as described in *Installation Guide for Scopia XT Endpoint for IP Office*.

Solution Make sure the resolution of the PC output is supported by the XT Codec Unit (see *User Guide for Scopia XT Endpoint for IP Office*).

Resolving XT Remote Control Unit Problems

Problem The XT Remote Control Unit does not function.

Solution Replace the battery, as described in *Scopia XT Endpoint for IP Office Installation Guide*. 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 33).

Solution If you still experience problems, reconfigure the XT Remote Control Unit code to be a number between 01-04, inclusive.

Resolving Problems with Displaying Video

Problem You cannot send or receive video during a call.

You can monitor video remotely from the XT Endpoint web interface by selecting **More Actions > Web Video**:

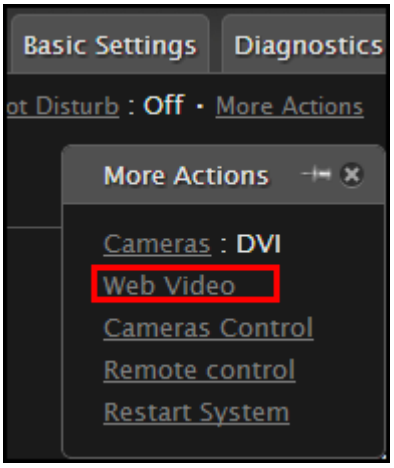


Figure 93: Remotely monitoring your camera

Possible Causes You may experience video problems when calling older endpoints that are not fully compliant with more recent standards, and thus not able to recognize and manage recent video protocols such as HD 1080 (full HD) or Dual Video SIP (BFCP).

Solution The endpoint administrator must disable specific video 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 XT Endpoint Locally from the Endpoint on page 35.

Procedure

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

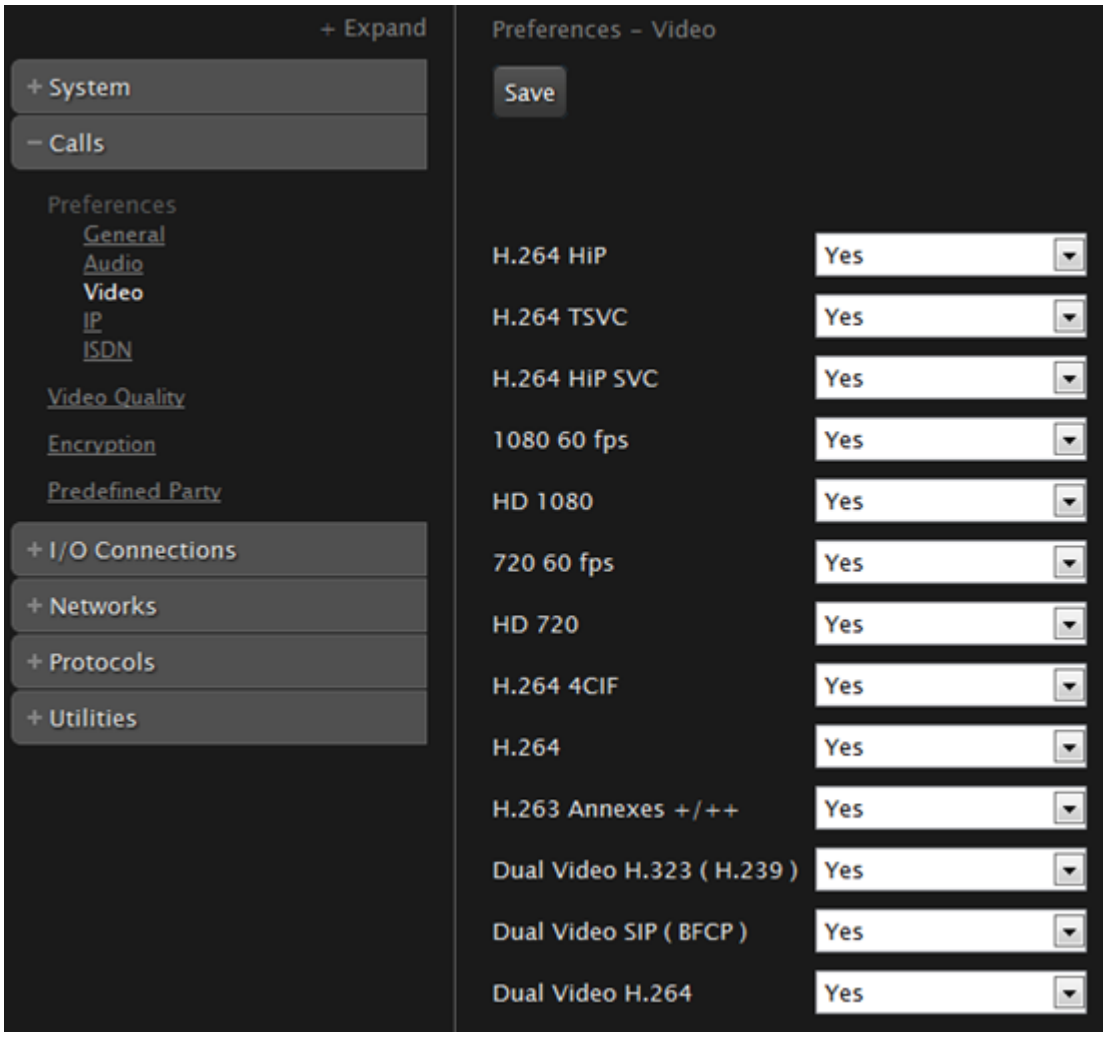


Figure 94: Configuring video settings from the web interface (example)

2. Disable specific video codecs by selecting **No** from the lists.

   Important:

   The video codecs available depends on your XT Endpoint model.

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

How to Retrieve Scopia XT Endpoint for IP Office Logs

When reporting a problem to customer support, you may be asked to retrieve and send logs of Scopia XT Endpoint for IP Office. There are two kinds of logs you can retrieve from the Scopia XT Endpoint for IP Office:

- Logs for analyzing network traffic—These log files provide information about network status.
- Internal system activities and memory dump logs—These log files are a snapshot of the system's memory at the moment of an error. These log files are analyzed by customer support only.

Navigation

- Retrieving Network Traffic Logs on page 149
- Retrieving System Logs on page 150

Retrieving Network Traffic Logs

About this task

This procedure describes how to retrieve log files that provide information about network status as you perform an action or during a specific call. This is necessary when contacting customer support with network traffic problems, such as poor video quality caused by increased packet loss.

The files are in the standard **libpcap** format supported by most network analysis tools.

Before you begin

- Ensure the computer you intend to use for retrieving logs is connected to the same network as the Scopia XT Endpoint for IP Office.
- We recommend cleaning old logs from the RAM. If there is not enough room on the RAM, retrieving logs is automatically stopped.

Procedure

1. Access the XT Endpoint web interface, as described in Accessing XT Endpoint Web Interface on page 24.
2. Select **Diagnostics** > **Utilities** > **Advanced Tools**.

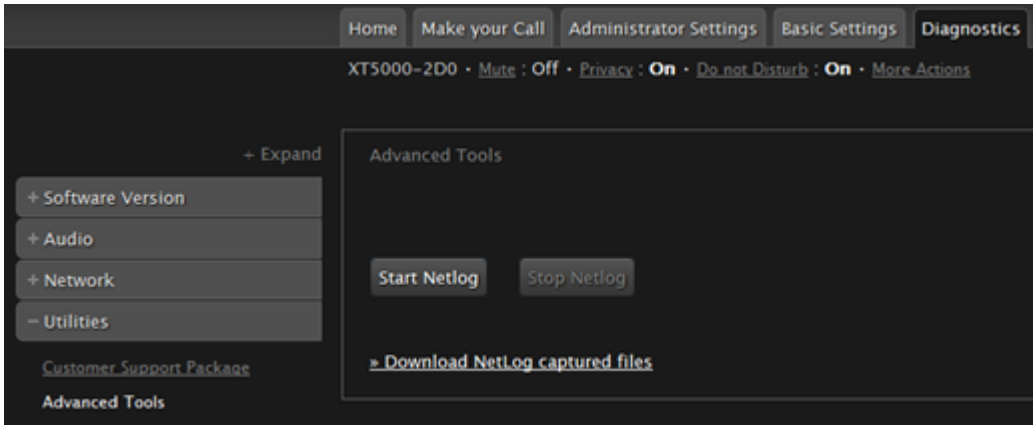


Figure 95: Retrieving netlog files

3. Start retrieving logs by selecting **Start Netlog**.
4. Reproduce the problem you want to report to customer support.
5. Stop retrieving logs by selecting **Stop Netlog**.
6. Access the logs as follows:
   a. Select **Download NetLog captured files**.

      The NetLog page appears.
   b. Enter the username and password.

      The default credentials are:
      - Username - CustomerSupport
      - Password - 5678
   c. Select the NetLog file to download it to your computer.



Figure 96: Downloading Netlog files

Retrieving System Logs

About this task

This procedure explains how to retrieve log files of Scopia XT Endpoint for IP Office internal system activities and memory dump.

Before you begin

Navigate to **Administrator Settings > Remote Access > Advanced**, and enable the following:

- **System Log**
- **Profiler**

Only enable these options while reporting the problem, as they can affect system performances if permanently enabled.

Procedure

1. Access the XT Endpoint web interface, as described in Accessing XT Endpoint Web Interface on page 24.
2. In the **Diagnostics** tab, select **Utilities > Customer Support Package**.

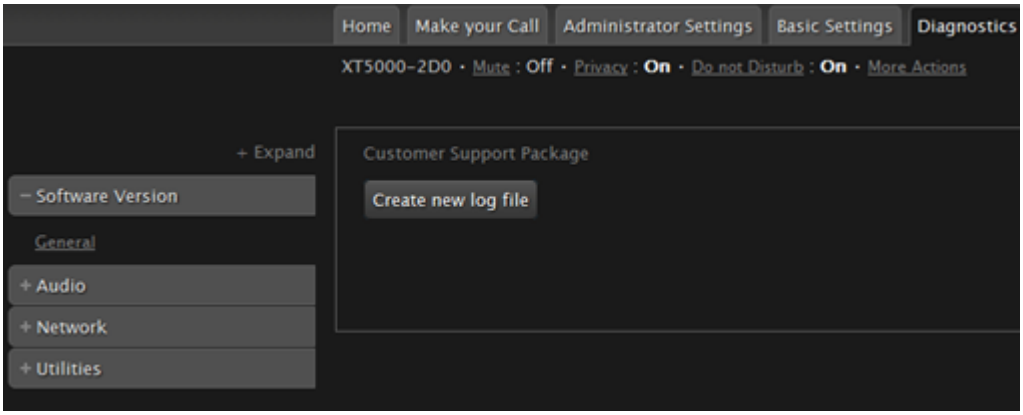


Figure 97: Retrieving system logs

3. Select **Create new log file**.
4. Wait for the system to create the log package file and display the link for downloading this file.
5. Select the link to download the log package file onto the computer.

USB Software Upgrade Failure

Problem The software upgrade from the USB drive fails.

Solution
1. Remove the USB drive from the USB port of the Scopia XT Endpoint for IP Office
2. Connect the USB drive to a computer.
3. Locate the **upgrade.log** file on the flash drive.
4. Send the log file to your local customer service representative.

Restoring Default User Settings

About this task

This procedure explains how to restore the default settings if necessary. You can do this from the endpoint itself only.

Before you begin

- Turn on the Scopia XT Endpoint for IP Office 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**.

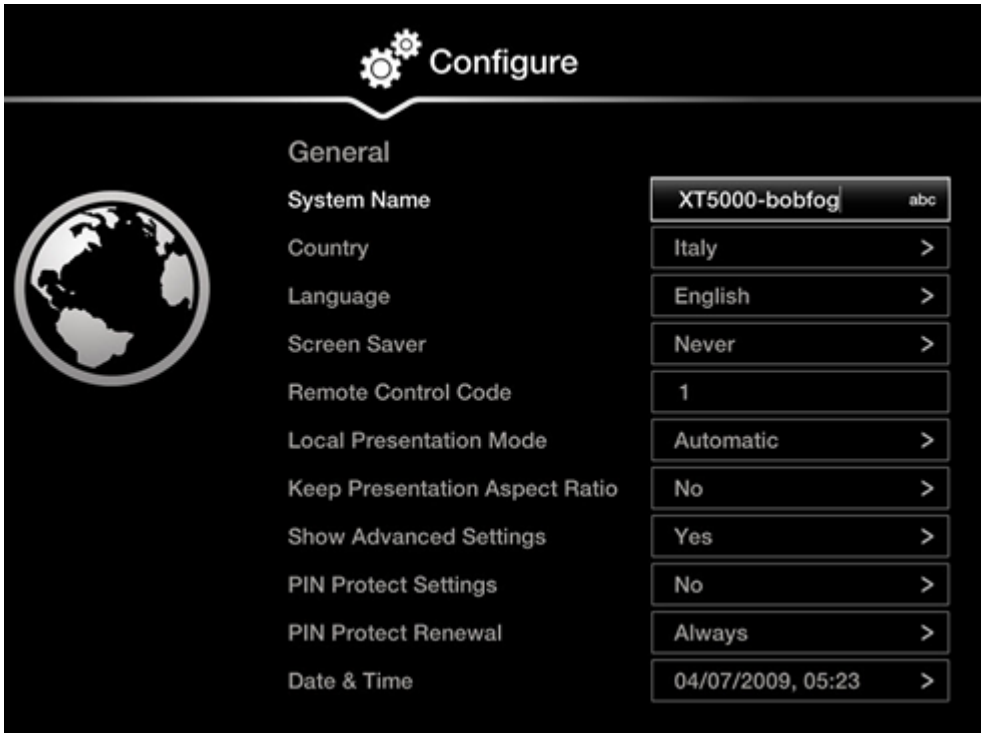


Figure 98: Enabling advanced settings

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 99: Restoring factory default settings

7. Press **ok/menu**, and select **Yes**.

   The default settings are restored.

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