RADVISION®
an Avaya company

Scopia XT5000 Server for IP Office

Installation Guide

Version 3.2

For Avaya IP Office 8.1

3.2

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

Installation Guide for Scopia XT5000 Server for IP Office Version 3.2, June 3, 2013

http://www.radvision.com

Table of Contents

Chapter 7: Securing your Scopia XT Server for IP Office

Chapter 8: Troubleshooting the Scopia XT Server for IP Office

Chapter 1 | About the Scopia XT Server for IP Office

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

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

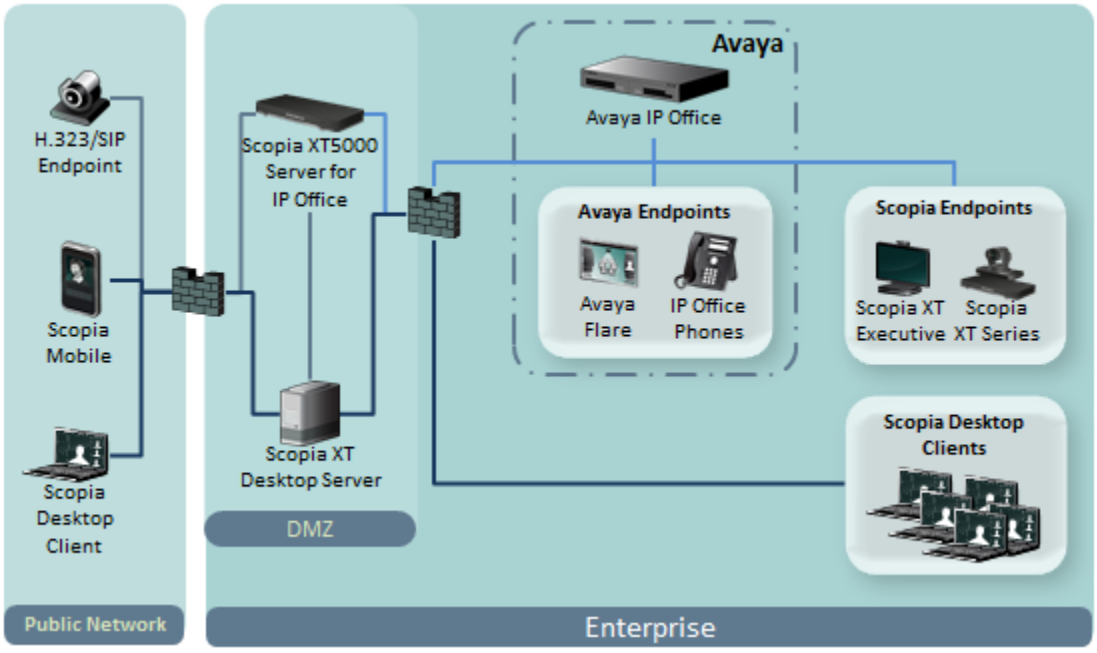


Figure 1: A typical Scopia XT Server for IP Office deployment

This section provides an overview of the general features and capabilities available in the Scopia XT Server 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 Server 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.
- 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 (requires license).
- For an even better experience, Scopia Control enables you to place a call using the intuitive touch interface of an Apple® iPad® (requires license).
- 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 Server 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 7.
- 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 9.

Table 1: Physical device specifications on page 7 refers to the physical details of the device.

Table 1: Physical device specifications

	Scopia XT Server 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)

	Scopia XT Server for IP Office
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)

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 Server 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)
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	This is relevant only if you connected a monitor, as described in Connecting a Monitor to the XT Server on page 25. 1920 x 1080 @ 25, 30, 50, 60fps (optional) 1280 x 720 @ 50, 60fps

	Scopia XT Server for IP Office
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 9 lists the XT Server's network interface and firewall traversal information.

Table 3: Network and security capabilities

	Scopia XT Server 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 | Installation Workflow for Scopia XT Server for IP Office

About this task

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

Procedure

1. Decide how to incorporate the XT Server into your deployment, as described in Planning the Topology of the Scopia XT Server for IP Office Deployment on page 12.

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

2. Read through and familiarize yourself with the safety information (see Complying with Safety Regulations on page 23).

3. Inspect the XT Server to verify that no shipping damage occurred, as described in Inspecting the Product on page 23.

4. To quickly connect your XT Server, refer to the *Quick Setup Guide for Scopia XT Server for IP Office*. For more detailed information on connecting the XT Server, see Setting up the Scopia XT Server for IP Office on page 24, which includes:

   - Mounting the XT Server
   - Connecting the XT Server to the network
   - Connecting a monitor (optional)
   - Placing batteries in the XT Remote Control Unit, if you are connecting a display and configuring from the endpoint interface.

5. If you are configuring from the web interface only, retrieve the system's IP address, as described in Retrieving the IP Address of the XT Server on page 29.

6. Read through and familiarize yourself with how to control the XT Server and access both the endpoint and web interface, as described in How to Control the XT Server on page 28. To use the XT Remote Control Unit to manage the system, you must first connect a monitor, as described in Connecting a Monitor to the XT Server on page 25. Otherwise, you can manage the system from the web interface only (see Managing your XT Server from the Web Interface on page 28).

7. Register your license to activate the XT Server, as described in Registering and Enabling your Scopia XT Server for IP Office license on page 47.

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

8. Perform the basic required configuration necessary to use the XT Server, such as the network and gatekeeper settings, as described in Performing Basic Configuration on page 52.

9. Perform additional basic configuration, such as setting the time zone and date, as described in Setting Basic System Information on page 66.

10. Configure the system to work with the IP Office Proxy/Registrar, as described in Registering the XT Server 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.

11. Disable local video and audio, as described in Configuring Call Settings on page 63.

12. If you connected a monitor and are configuring from the endpoint, you can modify the default administrator PIN code as described in Setting the Administrator PIN Code for the XT Server on page 71 (recommended).

13. If necessary for your deployment, configure your advanced network and call settings, as described in Configuring Network Settings on page 76.

    For more information about deployment setups, see Planning the Topology of the Scopia XT Server for IP Office Deployment on page 12 and the *Scopia Solution Guide*.

14. (Optional) If necessary for your organization, you can secure videoconference sessions via encrypted connections and TLS certificates (see Securing your Scopia XT Server for IP Office on page 88).

    Important:

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

Chapter 3 | Planning the Topology of the Scopia XT Server for IP Office Deployment

There are a number of ways that the Scopia XT Server 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 Server for IP Office Embedded MCU

The Scopia XT Server for IP Office includes an embedded MCU, allowing XT Server to host videoconferences locally, with up to 8 participants.

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 Server for IP Office on page 13 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 Server for IP Office

Maximum Resolution	XT Server
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.

Since the Scopia XT Server for IP Office is used only as an MCU for hosting videoconferences, block the audio and video input from this Scopia XT Server for IP Office during the meeting. For details, see Configuring Call Settings on page 63.

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

Scopia XT Server 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 Server 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 Server for IP Office include:

- Remote users can easily connect to a meeting hosted by the built-in MCU on the XT Server, 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 Server for IP Office includes the following:

- Full SMB9 - Advanced MCU level, with up to 8 participants:
  - Eight endpoints

    Or

  - Seven mixed endpoints and PC clients

Figure 2: Scopia XT Server for IP Office Deployment on page 14 shows a typical topology for the Scopia XT Server for IP Office solution. For more information, see the *Solution Guide for Scopia Solution*.

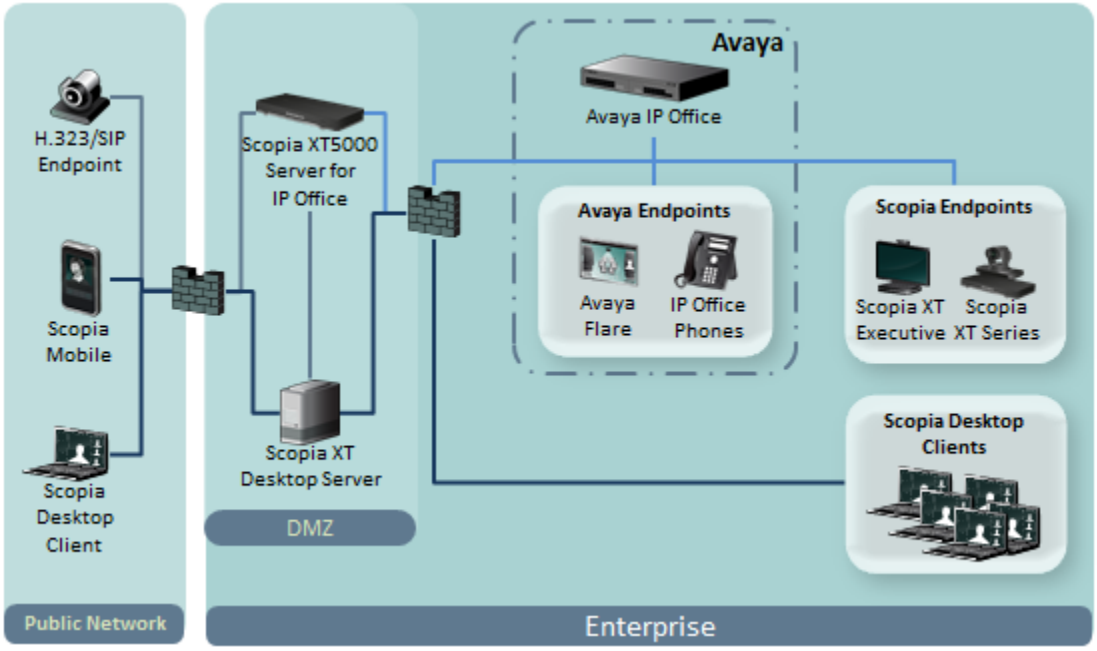


Figure 2: Scopia XT Server for IP Office Deployment

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

The Scopia XT Server 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 Server:

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

  When the XT Server hosts a videoconference with endpoints outside the enterprise (Figure 3: Using an HTTP/STUN Server for NAT and Firewall Traversal on page 15), 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.

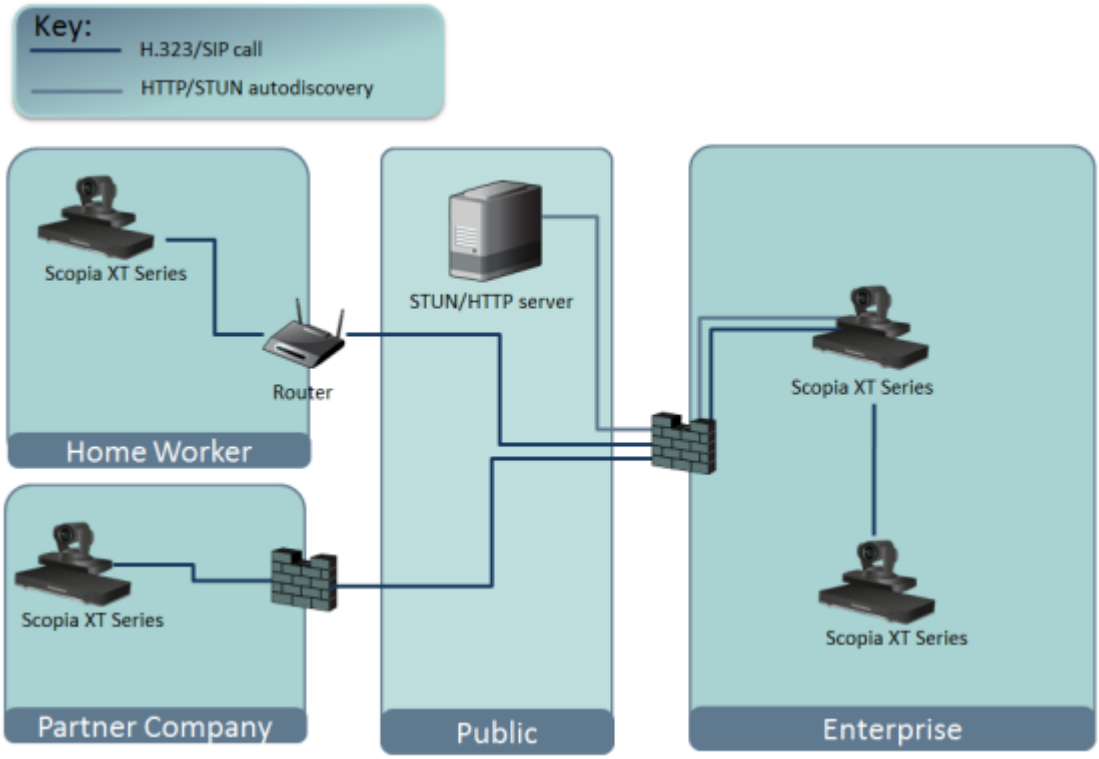


Figure 3: Using an HTTP/STUN Server for NAT and Firewall Traversal

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

- Using the XT Server for NAT and firewall traversal

  In cases where your organization has no sophisticated firewall protection, the XT Server can straddle the two network zones using the two network ports provided on the XT Codec Unit (see Figure 4: Using XT Server for NAT and Firewall Traversal on page 16).

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

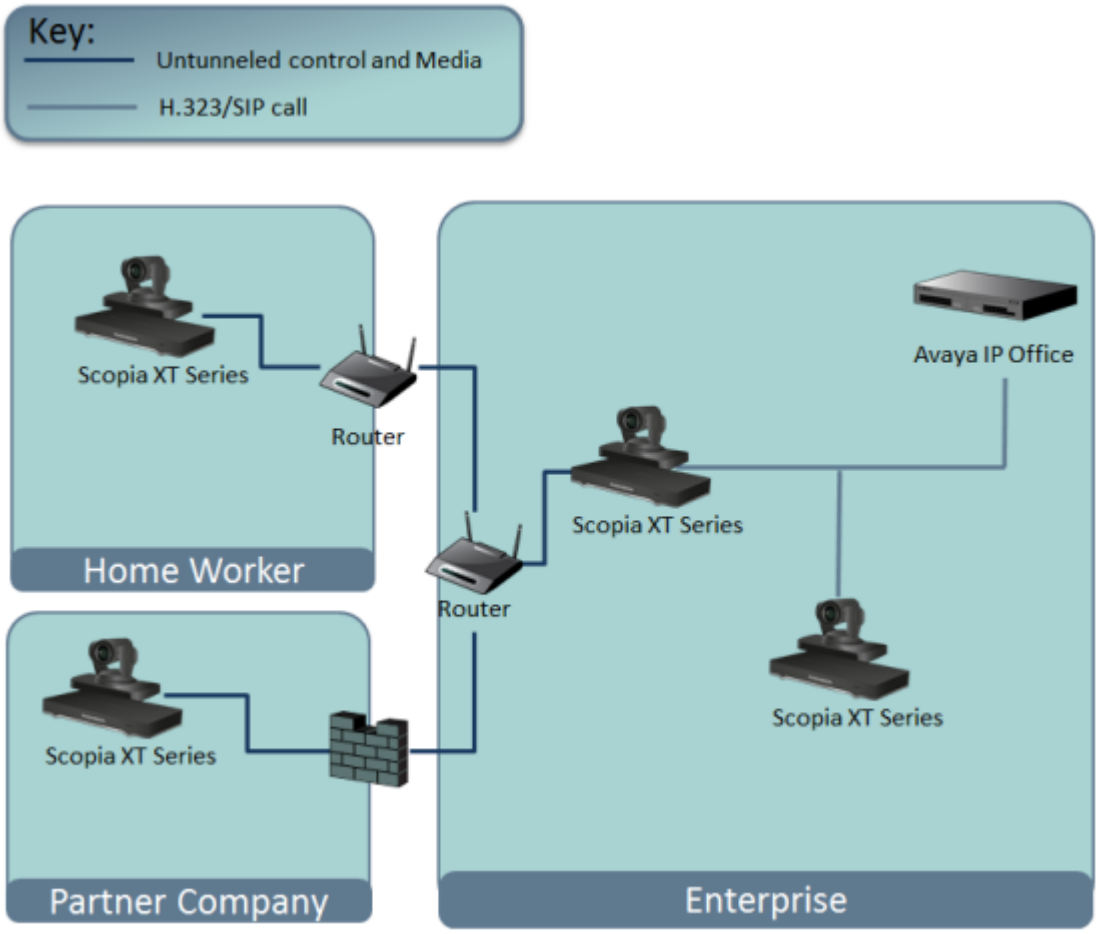


Figure 4: Using XT Server for NAT and Firewall Traversal

Regarding GLAN1 and GLAN2 configuration, the XT Server communicates simultaneously with the public and private network endpoints using IP addresses (see Figure 4: Using XT Server for NAT and Firewall Traversal on page 16).

Supporting ISDN Connectivity

About this task

The Scopia XT Server 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 Server 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 Server web interface, as described in Accessing XT Server Web Interface on page 34.
2. Select **Administrator Settings > Protocols > ISDN**.
3. Configure the IDSN settings as described below:

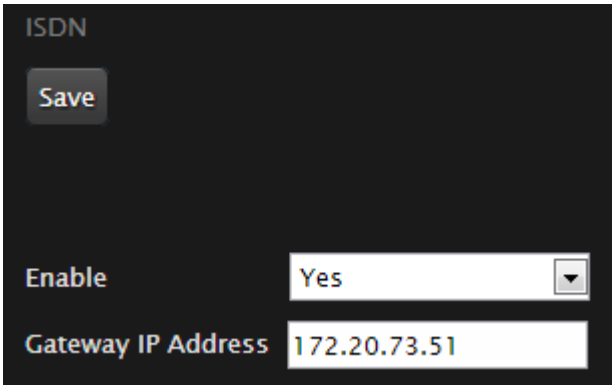


Figure 5: Enabling ISDN connectivity

Table 5: Supporting ISDN Connectivity

Field	Description
Enable	Select **Yes** to allow this Scopia XT Server 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 Server 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 Server for IP Office API, which includes the list of commands over the Ethernet interface.

Implementing Port Security for the Scopia XT Server for IP Office

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

Navigation

- Ports to Open on the XT Server on page 18
- Configuring the TCP or UDP Port Range on the Scopia XT Server for IP Office on page 21

Ports to Open on the XT Server

The Scopia XT Server 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 Server for IP Office, use the following as a reference:

- If you are opening ports that are both to and from the XT Server, see Table 6: Bidirectional Ports to Open on the XT Server on page 19.
- If you are opening outbound ports from the XT Server, see Table 7: Outbound Ports to Open from the Scopia XT Server for IP Office on page 20.

Important:

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

Table 6: Bidirectional Ports to Open on the XT Server

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 Server for IP Office on page 21
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 Server for IP Office on page 21
3338	XML Commands (TCP)	Scopia Control, Scopia XT Desktop Server	Enables communication with Scopia Control and Scopia XT Desktop Server by sending commands and receiving responses	Cannot communicate with Scopia Control application or and Scopia XT Desktop Server	Optional

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3478, 3479	STUN (UDP)	STUN Server	Enables endpoints to automatically discover the presence of a firewall or NAT, and to determine their public IP address.	Cannot automatically discover the presence of a firewall or NAT (only manual configuration available)	Optional
5060	SIP (TCP)	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 Server via API	Cannot send/ receive commands	Optional
55099	Software Upgrade (TCP)	XT Server 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 Server 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 Server 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 Server 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 Server 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).

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**.

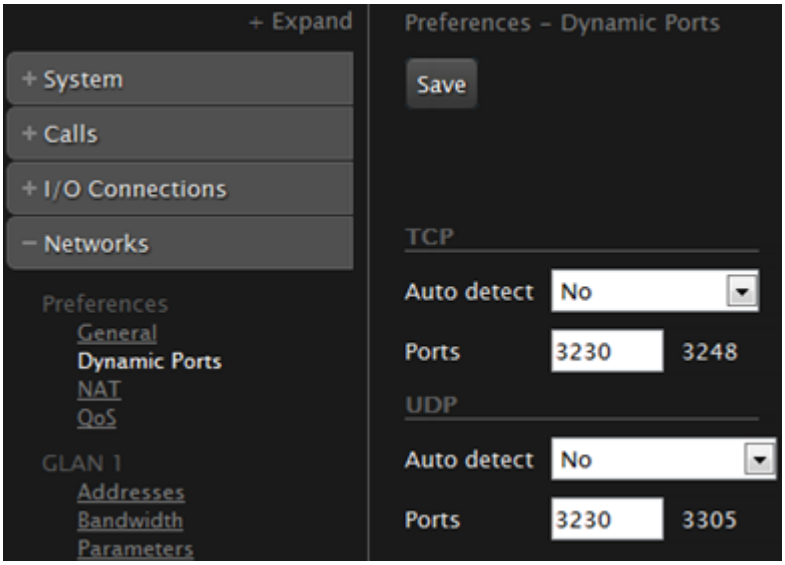


Figure 6: Configuring the TCP or UDP port range from the web interface

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 4 | Prerequisites for Setting up the System

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

Navigation

Complying with Safety Regulations

For detailed safety information consult the Scopia XT Server for IP Office Safety Instructions leaflet enclosed in the delivery package.

Inspecting the Product

Inspect the contents of the package for shipping damages.

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

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

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

Chapter 5 | Setting up the Scopia XT Server for IP Office

After reading the section Prerequisites for Setting up the System on page 23, you can install the Scopia XT Server for IP Office. These sections describe how to install the XT Codec Unit and connect its accessories:

Navigation

Mounting the XT Codec Unit

About this task

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

Procedure

Place the XT Codec Unit following these guidelines:

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

⚠ Caution:

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

Connecting Scopia XT Server for IP Office to Your Network

About this task

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

You can use both ports for connecting to the private and public network, however we recommend that you always connect the private network to the second GLAN port, whether one router interfaces with the Scopia XT Server for IP Office or multiple routers interface with the Scopia XT Server for IP Office (Figure 7: Connecting the XT Codec Unit to a private and a public network on page 25).

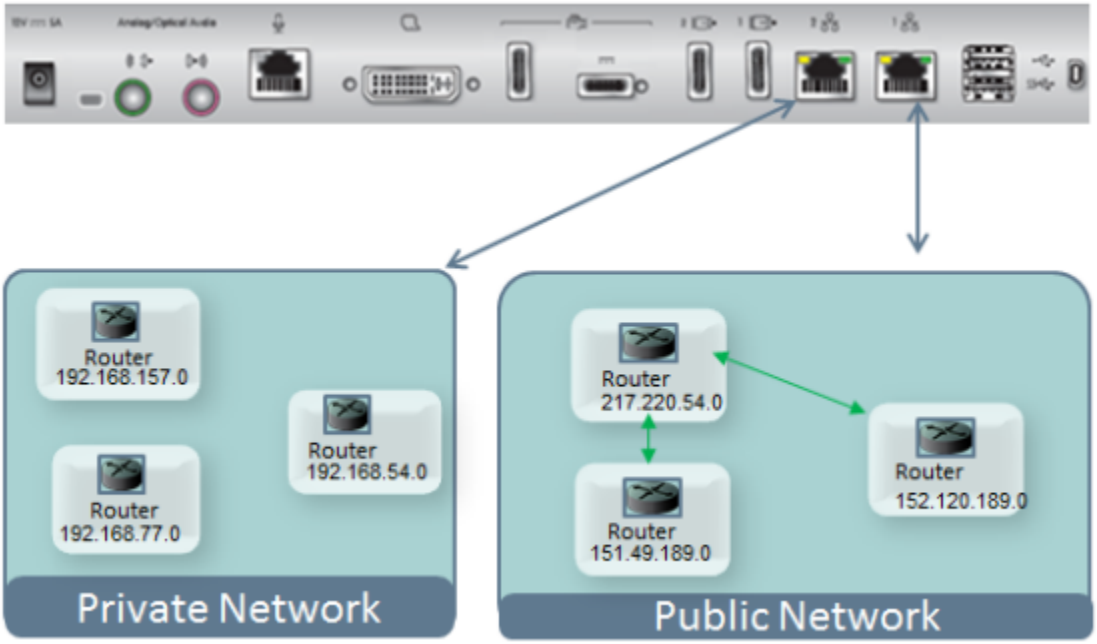


Figure 7: Connecting the XT Codec Unit to a private and a public network

For more information, see Planning NAT and Firewall Traversal with Scopia XT Server for IP Office on page 14.

Connecting a Monitor to the XT Server

About this task

To configure and manage your system using the XT Remote Control Unit, you must first connect a monitor as described below. Otherwise, configure the system from the web interface, as described in Managing your XT Server from the Web Interface on page 28.

Before you begin

You need an HDMI cable to connect the monitor to the XT Server:

Figure 8: HDMI cable

Procedure

1. Connect the cable to the HD1 port on the XT Codec Unit:

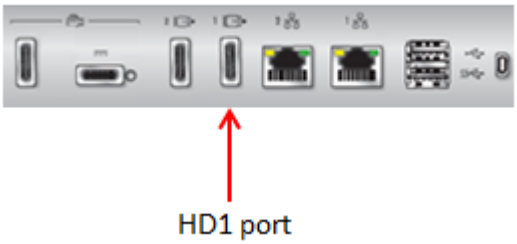


Figure 9: Connecting a monitor to the XT Server

2. Connect the cable to the HDMI port on the monitor.

Installing the Batteries of the XT Remote Control Unit

About this task

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

- Half-charged Battery
- Low Battery

Important:

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

For battery disposal information refer to the Safety Instructions leaflet.

Procedure

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

Chapter 6 | Initial Configuration

After connecting the system and powering it on as described in Setting up the Scopia XT Server for IP Office on page 24, perform the initial configuration as described in these sections:

Navigation

How to Control the XT Server

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

- From the endpoint's main menu, using your XT Remote Control Unit (see Using the XT Remote Control Unit on page 40 and Accessing the Main Menu of the XT Server on page 39).

  To use the XT Remote Control Unit to manage the system, you must first connect a monitor, as described in Connecting a Monitor to the XT Server on page 25. Otherwise, you can manage the system from the web interface only (see Managing your XT Server from the Web Interface on page 28).

- From the XT Server's web interface (see Accessing XT Server Web Interface on page 34).

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

Navigation

Managing your XT Server from the Web Interface

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

- Perform administrative tasks, such as:
  - Monitoring the status
  - Backing up the endpoint's configuration files
- Change basic settings, such as the interface language (for details, see Performing Basic Configuration on page 52)

You can also configure the XT Server from the endpoint itself by first connecting a monitor (see Connecting a Monitor to the XT Server on page 25), and enabling advanced configuration, as described in Maintaining the XT Server Locally from the Endpoint on page 45.

By default, all computers in the network can manage and upgrade the XT Server remotely. To limit access to specific computers in the network, see Enabling Remote Management on the Scopia XT Server for IP Office on page 35.

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

Navigation

- Retrieving the IP Address of the XT Server on page 29
- Accessing XT Server Web Interface on page 34
- Enabling Remote Management on the Scopia XT Server for IP Office on page 35
- Configuring Remote Upgrade Settings on page 37

Retrieving the IP Address of the XT Server

You can manage the XT Server from its web interface. To access the web interface and configure settings, you must first retrieve the IP address, in one of the following ways:

Navigation

- Retrieving the XT Server IP Address via Bonjour on page 29
- Retrieving the XT Server IP Address via SNMP Discovery on page 30
- Retrieving the XT Server IP Address via Serial Port Query on page 31

Tip:

We recommend using the Bonjour discovery method, since it is the simplest.

To configure the XT Server without retrieving the IP address, connect a monitor and manage the system from the endpoint's own interface, as described in Managing your XT Server Locally from the Endpoint on page 39.

Retrieving the XT Server IP Address via Bonjour

About this task

This procedure describes how to retrieve the XT Server's IP address using Bonjour, a protocol that enables automatic discovery of devices on the local network. After retrieving the IP address, you can configure the XT Server from its web interface.

Your network policies may prevent Bonjour discovery of devices that are located on a different subnet than your computer. In this case, retrieve the IP address using one of the other methods available:

- Retrieving the XT Server IP Address via SNMP Discovery on page 30
- Retrieving the XT Server IP Address via Serial Port Query on page 31

To configure the XT Server without retrieving the IP address, connect a monitor and manage the system from the endpoint's own interface, as described in Managing your XT Server Locally from the Endpoint on page 39.

Before you begin

Download the latest Apple Safari Internet Browser, which has embedded Bonjour support.

If necessary, you can use another internet browser such as Firefox and download the Bonjour plugin. For more information, see http://www.apple.com/support/bonjour/.

Procedure

1. Open Safari and navigate to the bookmarks.
2. Select **Bonjour** from the menu on the left.

   A list of all devices in your network appear.

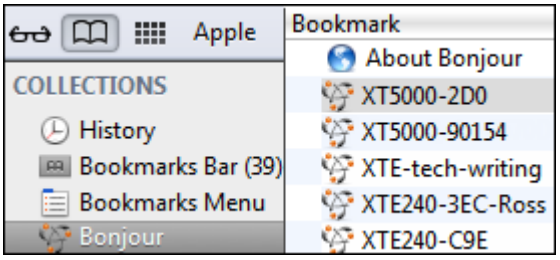


Figure 10: Retrieving the XT Server IP address via Bonjour

3. Find and double-click on your XT Server.

   The web interface opens. You can log in as described in Accessing XT Server Web Interface on page 34.

   Important:

   The initial IP assigned to the XT Server is a dynamic IP address. When you first start configuring the system, we recommend assigning a static IP address by performing the procedure described in Configuring IP Addresses on page 77.

Retrieving the XT Server IP Address via SNMP Discovery

About this task

This procedure describes how to retrieve the XT Server's IP address using SNMP Agent Discovery, a tool that allows discovery of SNMP agents on the network. This method is useful when the device is on a different subnet than your computer. After retrieving the IP address, you can configure the XT Server from its web interface.

This method is recommended for administrators only. Alternatively, you can also retrieve the IP address using one of the other methods available:

- Retrieving the XT Server IP Address via Bonjour on page 29
- Retrieving the XT Server IP Address via Serial Port Query on page 31

To configure the XT Server without retrieving the IP address, connect a monitor and manage the system from the endpoint's own interface, as described in Managing your XT Server Locally from the Endpoint on page 39.

Before you begin

Make sure you have an SNMP scanner tool, typically included in SNMP monitoring software.

Procedure

1. Launch the SNMP scanner tool used in your organization.

   A list of all devices in your network appear.

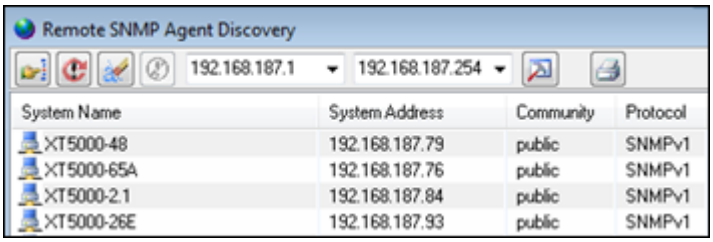


Figure 11: Retrieving the XT Server IP address via SNMP agent discovery

2. Find your XT Server.
3. Open a web browser and enter the IP address.

   The web interface opens. You can log in as described in Accessing XT Server Web Interface on page 34.

   Important:

   The initial IP assigned to the XT Server is a dynamic IP address. When you first start configuring the system, we recommend assigning a static IP address by performing the procedure described in Configuring IP Addresses on page 77.

Retrieving the XT Server IP Address via Serial Port Query

About this task

This procedure describes how to retrieve the XT Server's IP address using a serial port query, with no additional software required on your computer. This method is useful because it does not require any additional software on your computer, and can detect devices on a different subnet than your computer. After retrieving the IP address, you can configure the XT Server from its web interface.

This method is recommended for administrators only. Alternatively, you can also retrieve the IP address using one of the other methods available:

- Retrieving the XT Server IP Address via Bonjour on page 29
- Retrieving the XT Server IP Address via SNMP Discovery on page 30

To configure the XT Server without retrieving the IP address, connect a monitor and manage the system from the endpoint's own interface, as described in Managing your XT Server Locally from the Endpoint on page 39.

Before you begin

Verify that you have the following:

- An RS232 serial port cable for XT Server, provided with the basic cable kit.

Figure 12: Serial port cable

- A serial port terminal application, such as SecureCRT or PuTTY.

Procedure

1. Connect the serial port cable as follows:

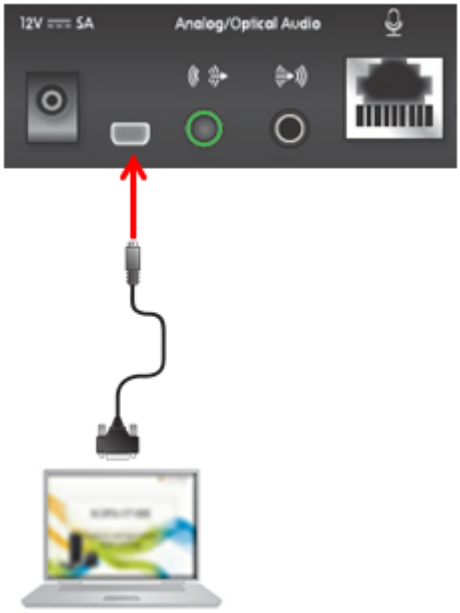


Figure 13: Connecting a serial port cable

   a. Connect the mini-USB end of the cable to the serial port on the XT Codec Unit.

   b. Connect the DB (9 pin) end of the cable to the serial port on the computer.

2. Launch a serial port terminal application such as SecureCRT.

3. Establish the connection between the computer and the XT Server by configuring the settings as follows:

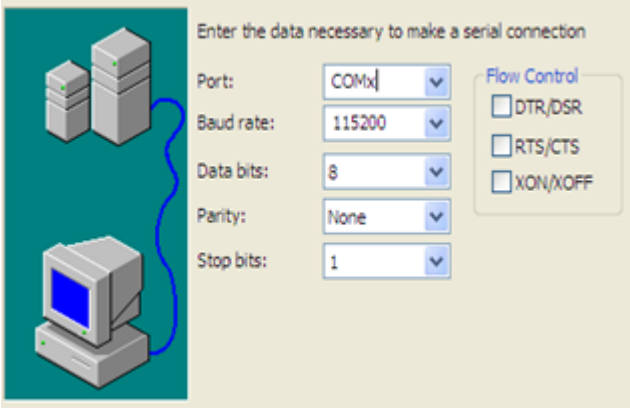


Figure 14: Establishing a serial connection

Table 8: Establishing a serial connection

Field	Value
Port	Enter the serial port number on your computer to which you connected the cable, for example **COM1**. If you are unsure of which serial port, consult your computer's documentation.
Baud rate	Set to **115200**.
Data bits	Set to **8**.
Parity	Set to **None**.
Stop bits	Set to **1**.

The PC connects to the XT Server.

4. In the console:
   a. Type `cd lan`.
   b. Type `read IP`.
      The IP address is displayed.

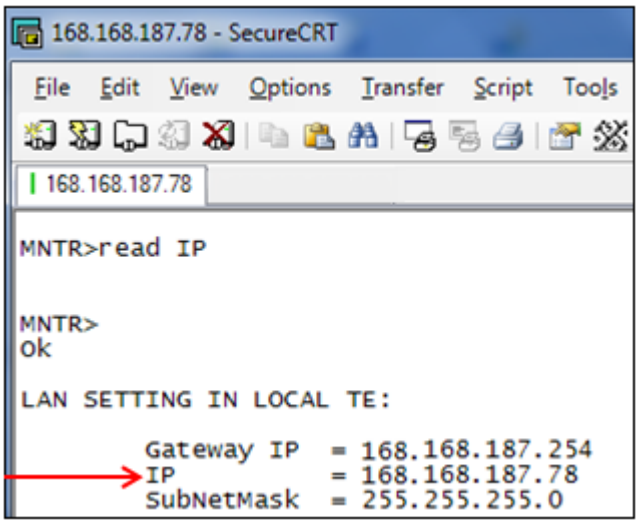


Figure 15: Retrieving the XT Server IP address via serial port query

5. Open a web browser and enter the IP address.

   The web interface opens. You can log in as described in Accessing XT Server Web Interface on page 34.

   Important:

   The initial IP assigned to the XT Server is a dynamic IP address. When you first start configuring the system, we recommend assigning a static IP address by performing the procedure described in Configuring IP Addresses on page 77.

Accessing XT Server Web Interface

About this task

This procedure describes how to access the XT Server web interface. The XT Server 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

Before you begin

Retrieve the system's IP address, as described in Retrieving the IP Address of the XT Server on page 29.

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 Server login page opens.

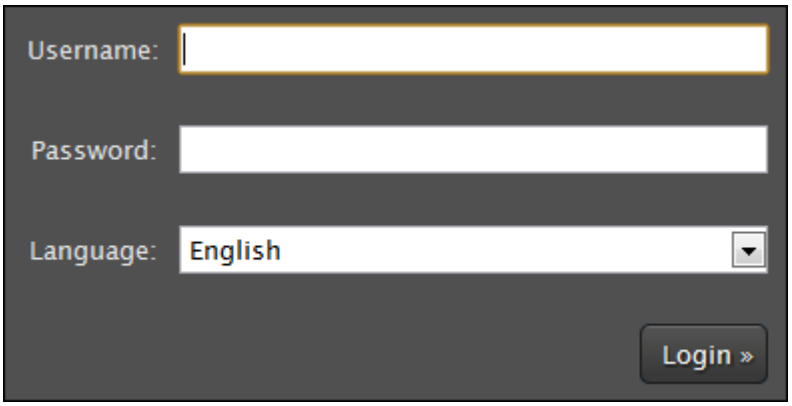


Figure 16: Logging into the XT Server web interface

2. Enter the username and password.

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

   Important:

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

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

4. Select **Login**.

Enabling Remote Management on the Scopia XT Server for IP Office

About this task

Remote management on your Scopia XT Server for IP Office is enabled by default. You can configure the XT Server 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 Server web interface. If you are not connecting a monitor to the XT Server, you can perform this procedure from the web only.

To remotely upgrade the XT Server, you must also enable remote downloads, as described in Configuring Remote Upgrade Settings on page 37.

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

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

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 Server Locally from the Endpoint on page 45.

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

Procedure

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

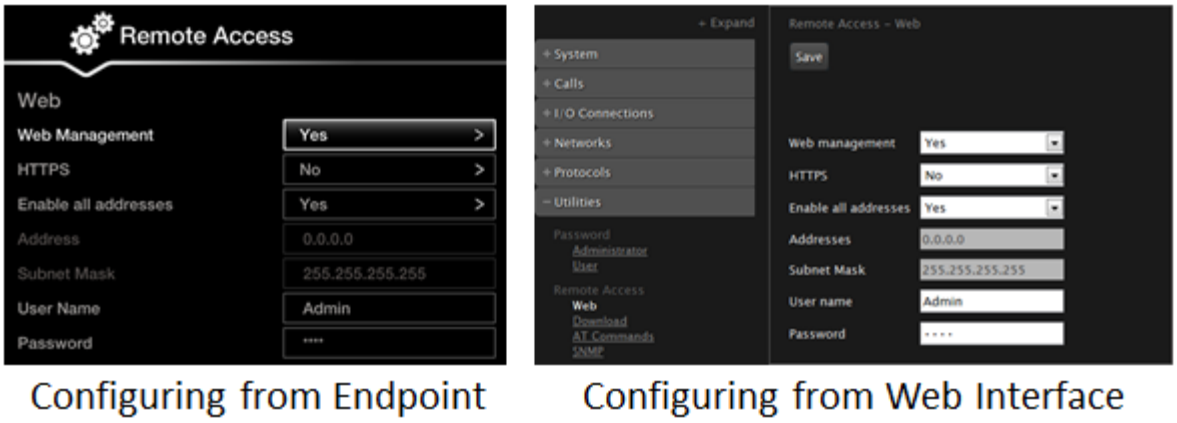


Figure 17: Configuring remote management on XT Server

2. Set the fields as described in Table 9: Configuring remote management on XT Server on page 36.

Table 9: Configuring remote management on XT Server

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

3. From the web interface only, select **Save**.
4. To perform remote upgrades, enable remote downloads as described in Configuring Remote Upgrade Settings on page 37.

Configuring Remote Upgrade Settings

About this task

In order to upgrade your Scopia XT Server 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 Server web interface. If you are not connecting a monitor to the XT Server, you can perform this procedure from the web only.

Before you begin

- If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Server Locally from the Endpoint on page 45.
- 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 Server for IP Office on page 35.

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

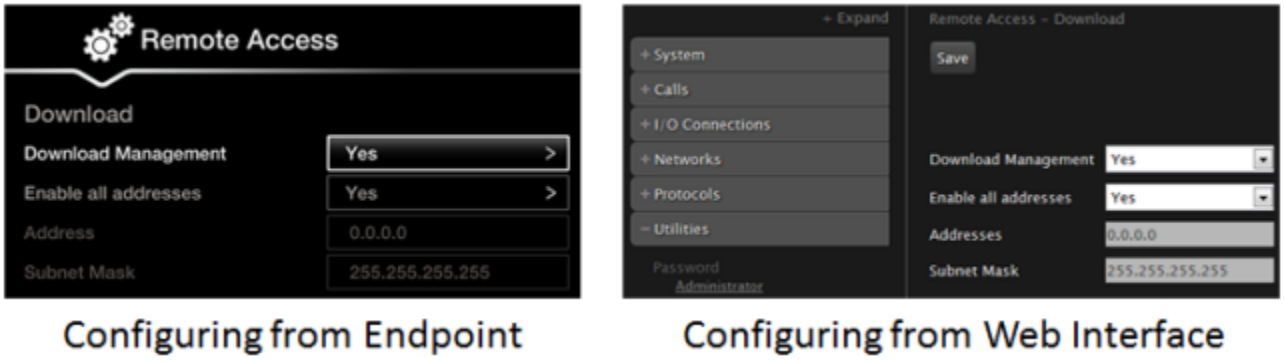


Figure 18: Enabling remote access to the XT Server

2. Set the fields as described in Table 10: Enabling remote upgrade on page 38.

Table 10: 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 Server. • Select **No** to disable remote downloads to the XT Server.
Enable all addresses	Allow access to the XT Codec Unit from all or specific PCs, as follows: • Select **Yes** to enable access to XT Server 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 Server.
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 Server, see *Administrator Guide for Scopia XT Server for IP Office*.

Managing your XT Server Locally from the Endpoint

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

This is only relevant if you connected a monitor to your system, as described in Connecting a Monitor to the XT Server on page 25.

To perform advanced configuration XT Server from the endpoint itself, you must first enable advanced configuration as described in Maintaining the XT Server Locally from the Endpoint on page 45.

See the following topics for more information:

Navigation

Accessing the Main Menu of the XT Server

About this task

After switching on the XT Server, the main menu appears and you can configure the system and check the status.

To make calls, record videoconferences, share content, and control the camera, you must first connect a camera, monitor, and microphone.

You navigate XT Server 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 40).

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 configure the system and check the 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 53).

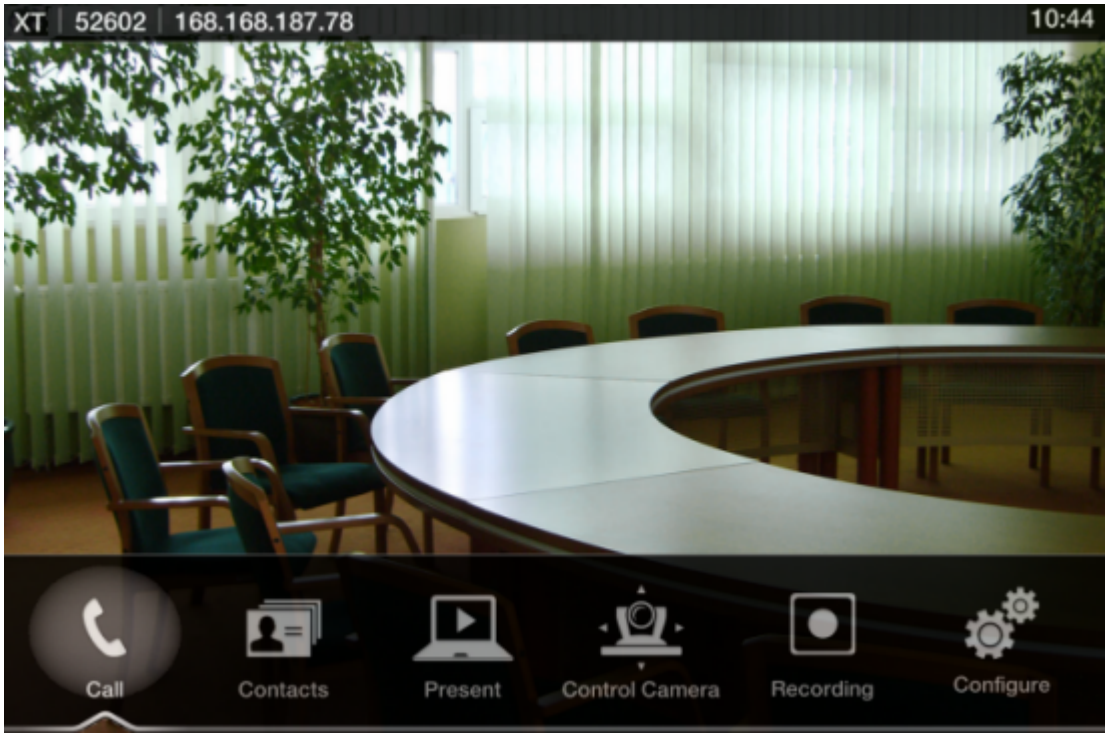


Figure 19: Main menu

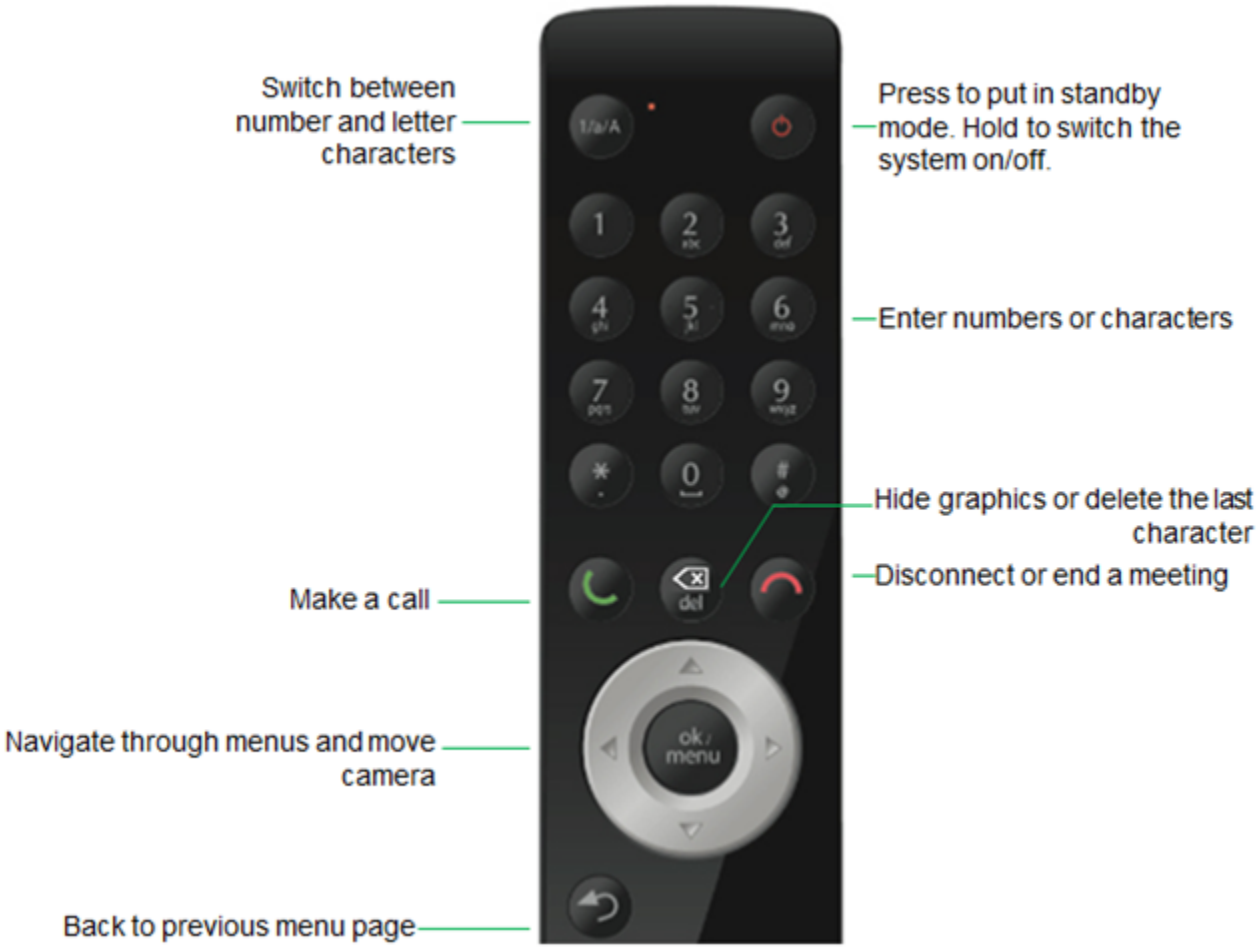
4. Select one of the options using the arrow keys of the XT Remote Control Unit.

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.

To use the XT Remote Control Unit to manage the system, you must first connect a monitor, as described in Connecting a Monitor to the XT Server on page 25. Otherwise, you can manage the system from the web interface only (see Managing your XT Server from the Web Interface on page 28).

The XT Remote Control Unit has an improved design and increases usability to give you a smoother and more efficient videoconferencing experience. Figure 20: The new XT Remote Control Unit on page 41 describes the functions of the XT Remote Control Unit.


Switch between number and letter characters
Press to put in standby mode. Hold to switch the system on/off.
Enter numbers or characters
Hide graphics or delete the last character
Disconnect or end a meeting
Make a call
Navigate through menus and move camera
Back to previous menu page
1/a/A
del
ok / menu

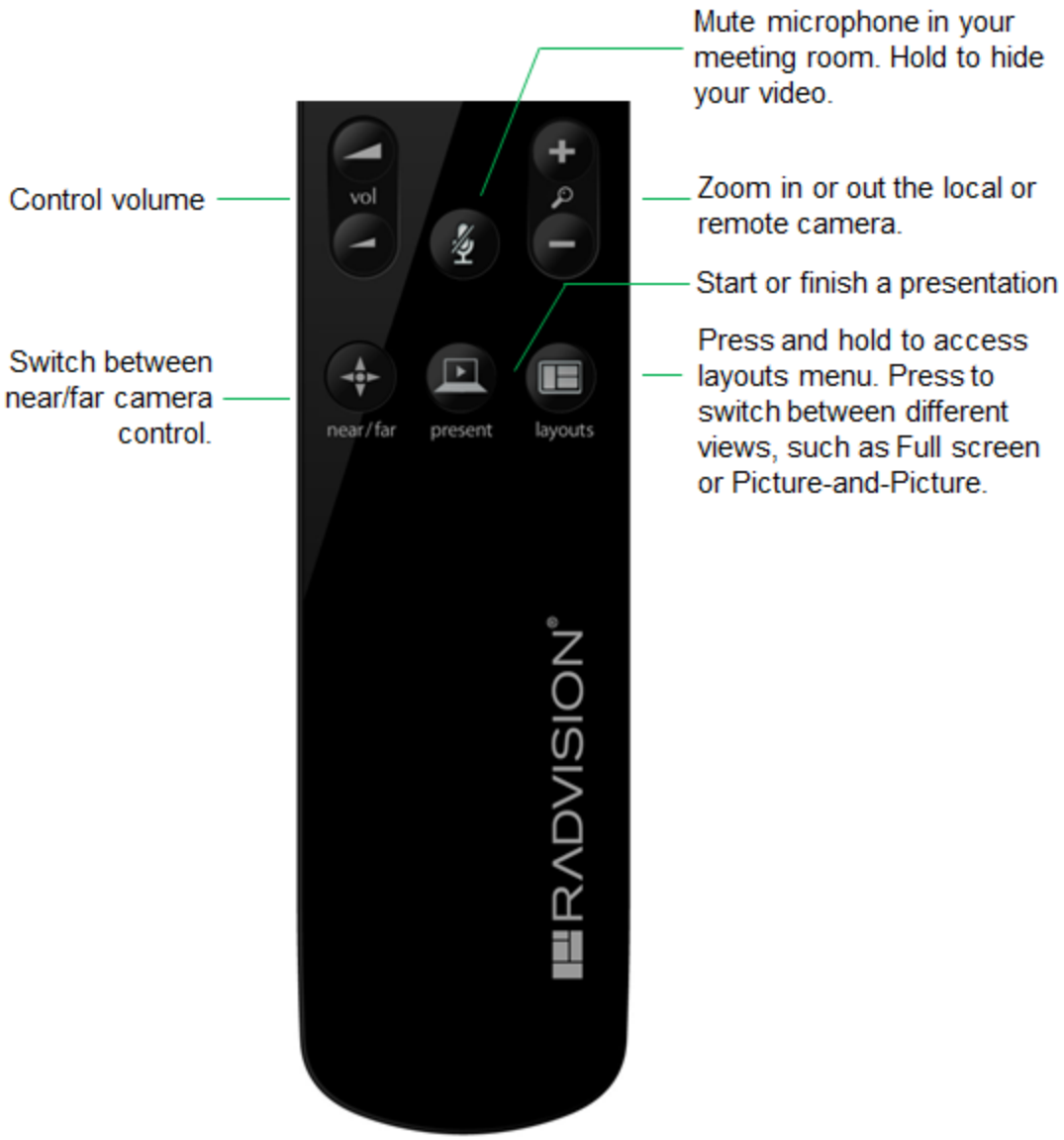


Figure 20: The new XT Remote Control Unit

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.

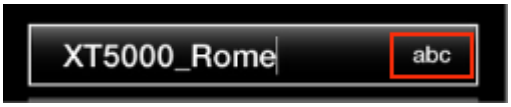
  Important:

  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 Server 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**.

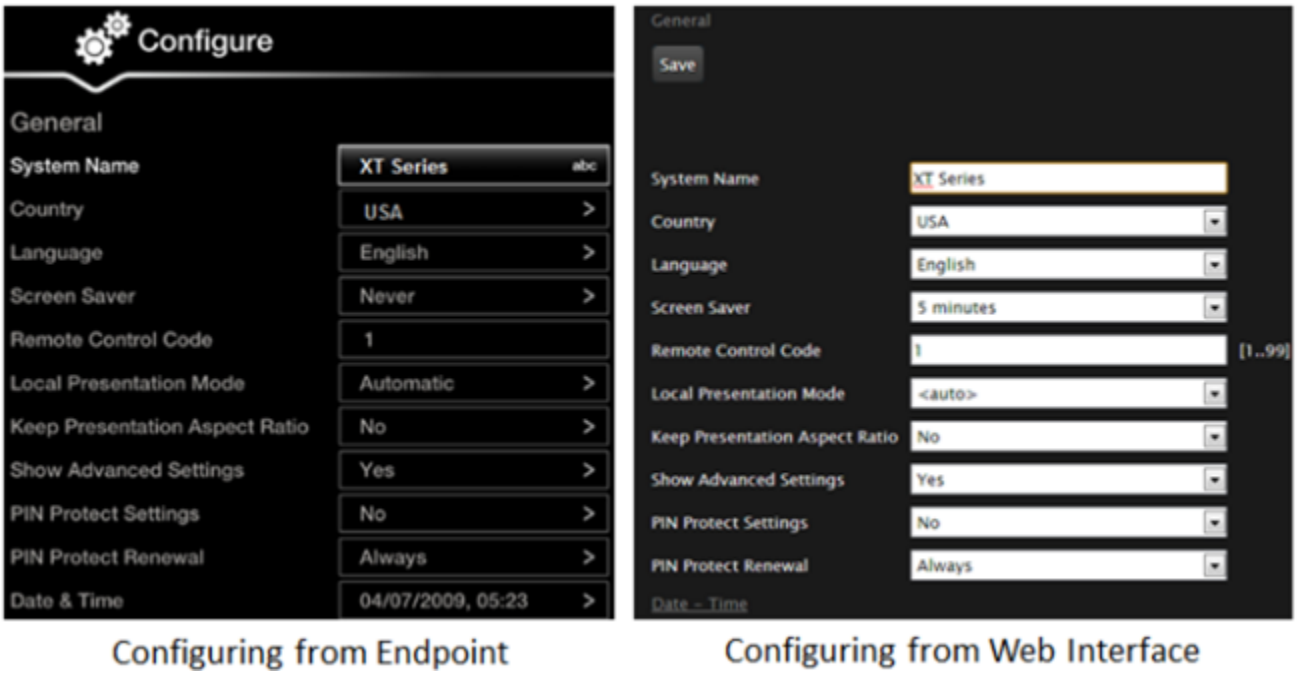


Figure 21: Setting the XT Remote Control Unit Code

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 22: 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 Server Locally from the Endpoint

About this task

To perform advanced configuration and maintain the Scopia XT Server for IP Office from the endpoint itself, you must first perform this procedure to access advanced settings. For example, you can upgrade the XT Server. For more information about maintaining the XT Server, see *Administrator Guide for Scopia XT Server for IP Office*.

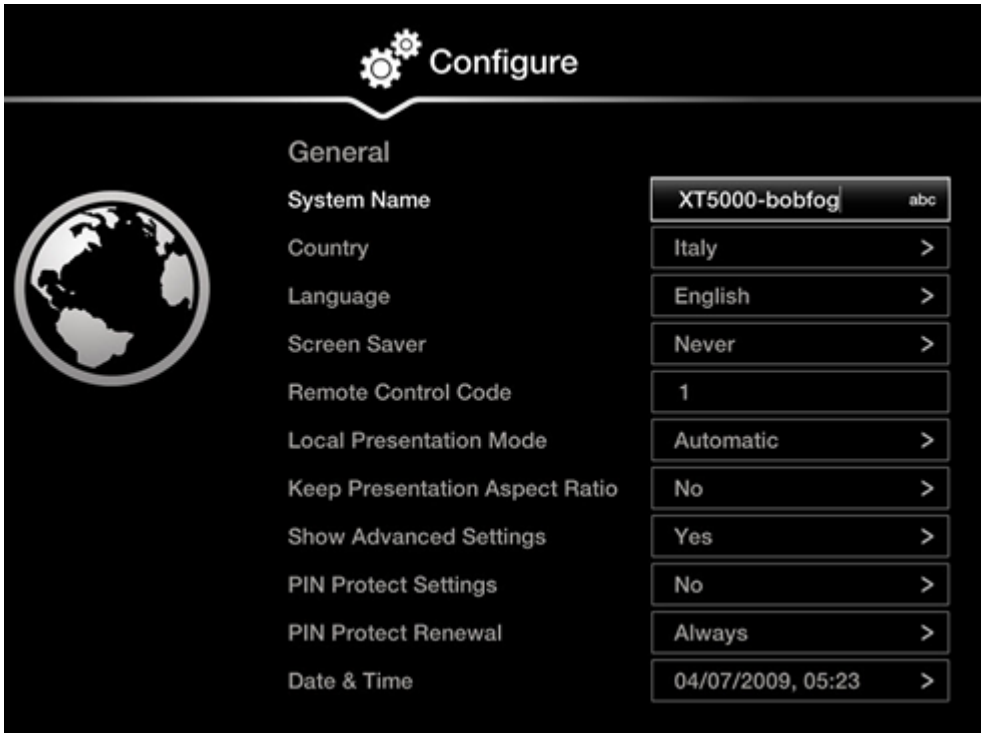
To use the XT Remote Control Unit to manage the system, you must first connect a monitor, as described in Connecting a Monitor to the XT Server on page 25. Otherwise, you can manage the system from the web interface only (see Managing your XT Server from the Web Interface on page 28).

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 23: Advanced configuration screen

6. We recommend changing the default administrator password, as described in Setting the Administrator PIN Code for the XT Server on page 71.

Registering and Enabling your Scopia XT Server for IP Office license

About this task

To activate the features of your XT Server, 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 Server for IP Office to Obtain a License Key on page 48.
2. Enable the license from either the endpoint or the web interface:
   - Remotely Enabling the License from the Web Interface on page 49
   - Enabling the License from the Scopia XT Server for IP Office on page 51
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 48.

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

About this task

Register your XT Server 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 48.

Procedure

1. Open the envelope that came with the XT Server.
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 49
   - Enabling the License from the Scopia XT Server for IP Office on page 51

Installing and Enabling Licenses which Extend System Functionality

About this task

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

Table 11: Scopia XT Server for IP Office Software Options on page 49 lists the various license options available for purchase to extend the system's functionality.

Table 11: Scopia XT Server 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 97 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 Server for IP Office using the Scopia Control Application (iPad).

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 49
   - Enabling the License from the Scopia XT Server for IP Office on page 51

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 Server for IP Office on page 51.

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 Server for IP Office as described in Registering the Scopia XT Server for IP Office to Obtain a License Key on page 48 or, if you are enabling a license option to extend Scopia XT Server for IP Office functionality, see Installing and Enabling Licenses which Extend System Functionality on page 48.

Procedure

1. Access the XT Server web interface, as described in Accessing XT Server Web Interface on page 34.
2. From the Home page, select **Enable License**, or, navigate to **Administrator Settings** > **Utilities** > **Licenses**.

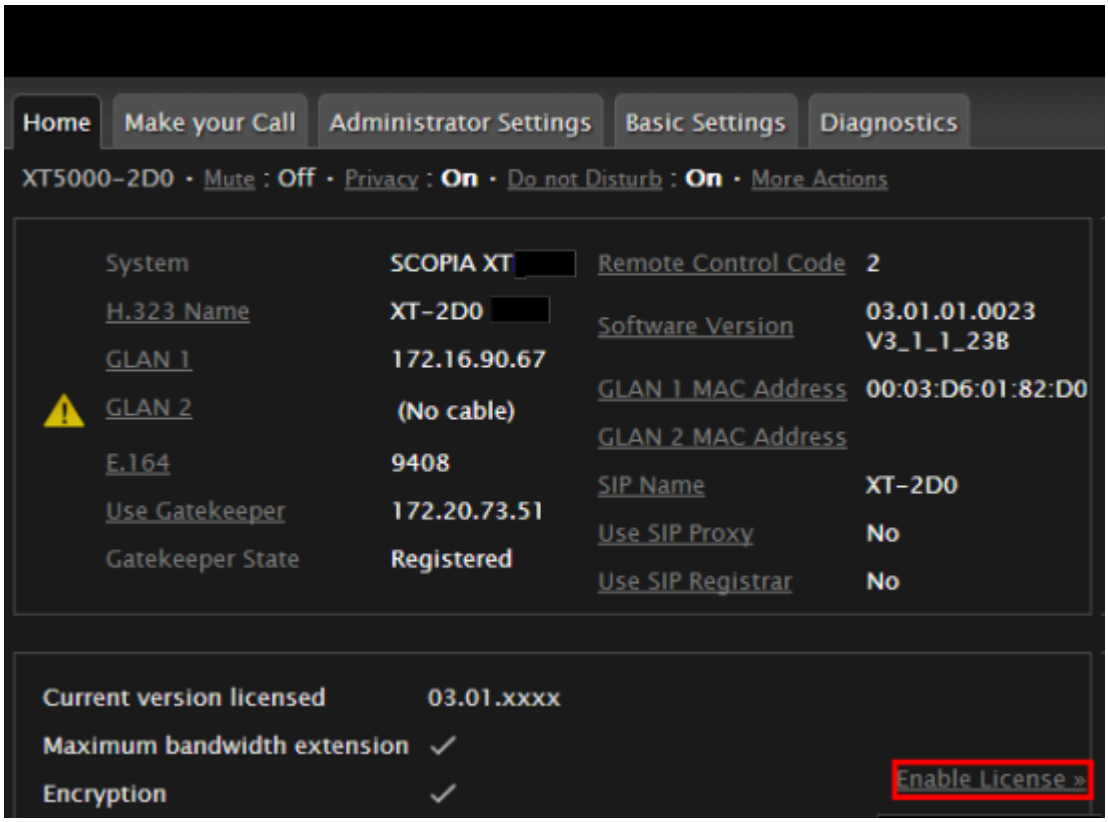


Figure 24: Accessing licenses from the Scopia XT Server for IP Office home page

The **Licenses** page appears.

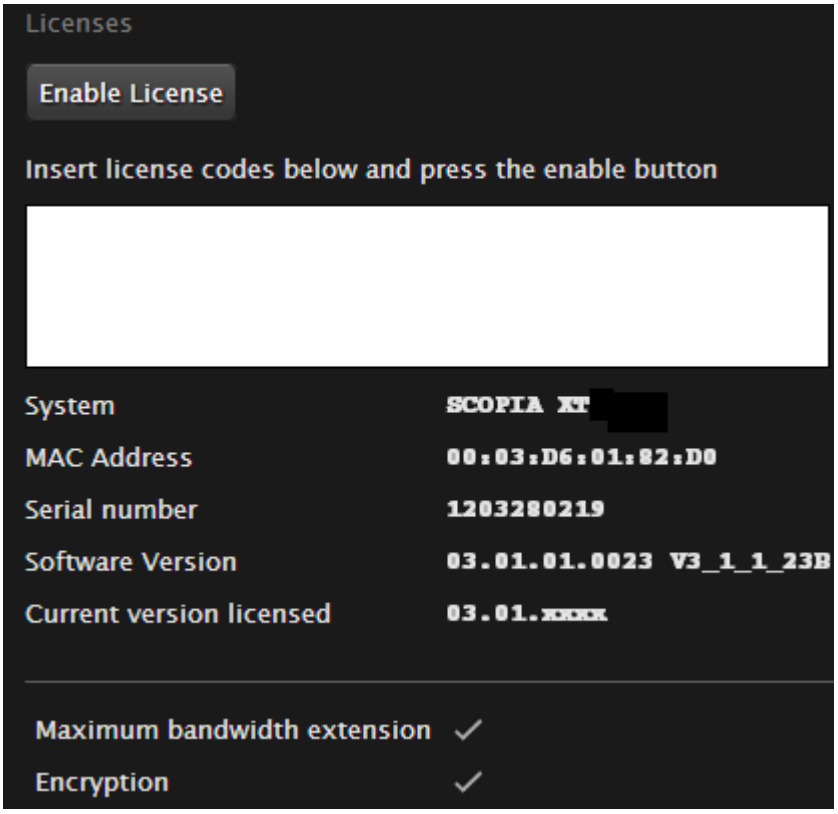


Figure 25: Enabling the license from the web interface

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 Server 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 49.

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 Server for IP Office as described in Registering the Scopia XT Server for IP Office to Obtain a License Key on page 48 or, if you are enabling a license option to extend Scopia XT Server for IP Office functionality, see Installing and Enabling Licenses which Extend System Functionality on page 48.
- If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Server Locally from the Endpoint on page 45.

Procedure

1. Access the Scopia XT Server 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.

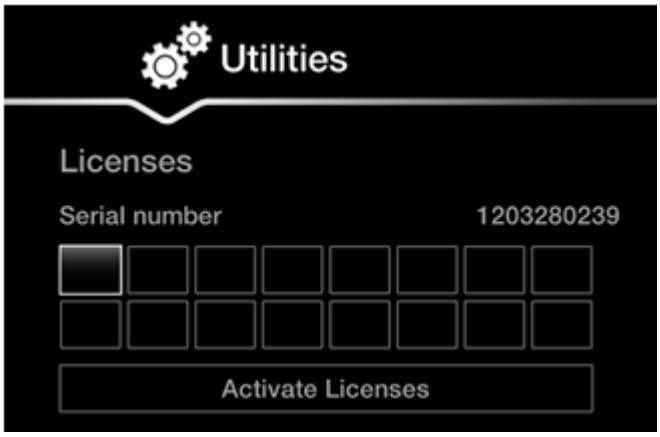


Figure 26: Activating a license

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 Server, your system administrator should install and activate your XT Server (for details, see the *Quick Setup Guide for Scopia XT Server for IP Office*, the

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

To start using your XT Server, 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 password protection, you need the password before continuing with the configuration.

If you are performing the quick setup from the web interface, retrieve the system's IP address, as described in Retrieving the IP Address of the XT Server on page 29.

You can define these settings as follows:

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

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

  This is only relevant if you connected a monitor to your system, as described in Connecting a Monitor to the XT Server on page 25.

- Remotely defining the settings from the XT Server web interface (see Accessing XT Server Web Interface on page 34).

  Your administrator may define some settings remotely, such as for the network or gatekeeper (see Configuring Network Settings on page 76 for details). The quick setup is available from the web interface if you have not already completed the procedure from the endpoint.

  If you did not connect a monitor to your system, you can perform the quick setup and configure your system from the web interface only.

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

Accessing the Quick Setup Procedure

About this task

Access the quick setup procedure to define basic settings for your Scopia XT Server 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 Server web interface. If you are not connecting a monitor to the XT Server, you can perform this procedure from the web only.

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 password protection, you need the password before continuing with the configuration.

If you are performing the quick setup from the web interface, retrieve the system's IP address, as described in Retrieving the IP Address of the XT Server on page 29.

Procedure

1. The quick setup wizard automatically appears the first time you access the Scopia XT Server 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.

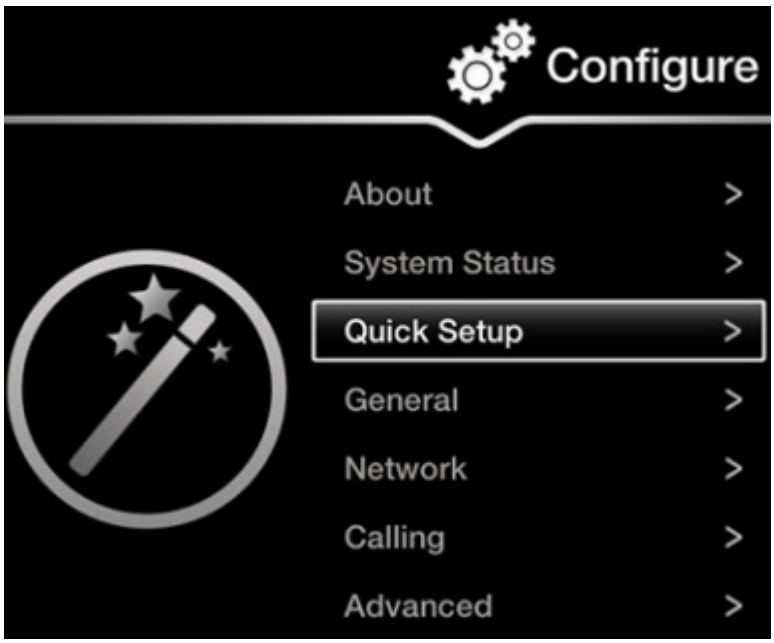


Figure 27: Accessing the Quick Setup

2. The quick setup wizard guides you through these basic configuration tasks:
   - Setting the System Name and Language on page 55: Define your system's name, your country, and preferred language for the interface.
   - Adjusting the Image Position on page 56: 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 58: Define your system's network settings to allow you to place and receive calls.
   - Configuring Gatekeeper Settings on page 60: If your Scopia XT Server 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 68.

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 66.

Before you begin

Access the quick setup wizard from the endpoint or web interface, as described in Accessing the Quick Setup Procedure on page 53.

Procedure

1. Enter the name of the XT Server 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 40).

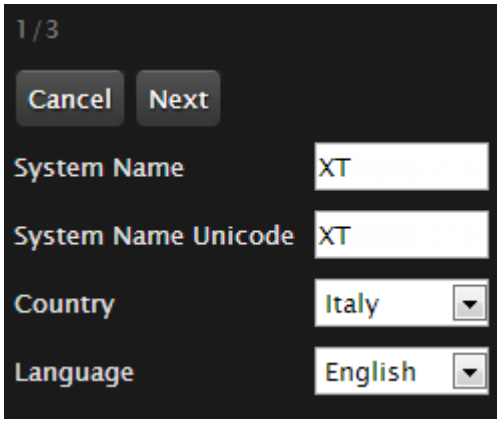


Figure 28: Setting Country and Language

2. To include non-ANSII characters such as Chinese or Japanese on the system's titlebar, enter the name in the **System Name Unicode** field. This can be configured from the web interface only.

   For more information about modifying the name on the system's titlebar, see Modifying the System's Name on the Titlebar on page 68.

3. 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.

4. 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**.

5. To adjust the image on your monitor, select **Next** and continue with Adjusting the Image Position on page 56.

   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.

This is only relevant if you connected a monitor to your system, as described in Connecting a Monitor to the XT Server on page 25.

Before you begin

This procedure is performed as part of the Quick Setup Wizard, after Setting the System Name and Language on page 55.

Access the quick setup wizard from the endpoint, as described in Accessing the Quick Setup Procedure on page 53.

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 29: Examining the image position

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

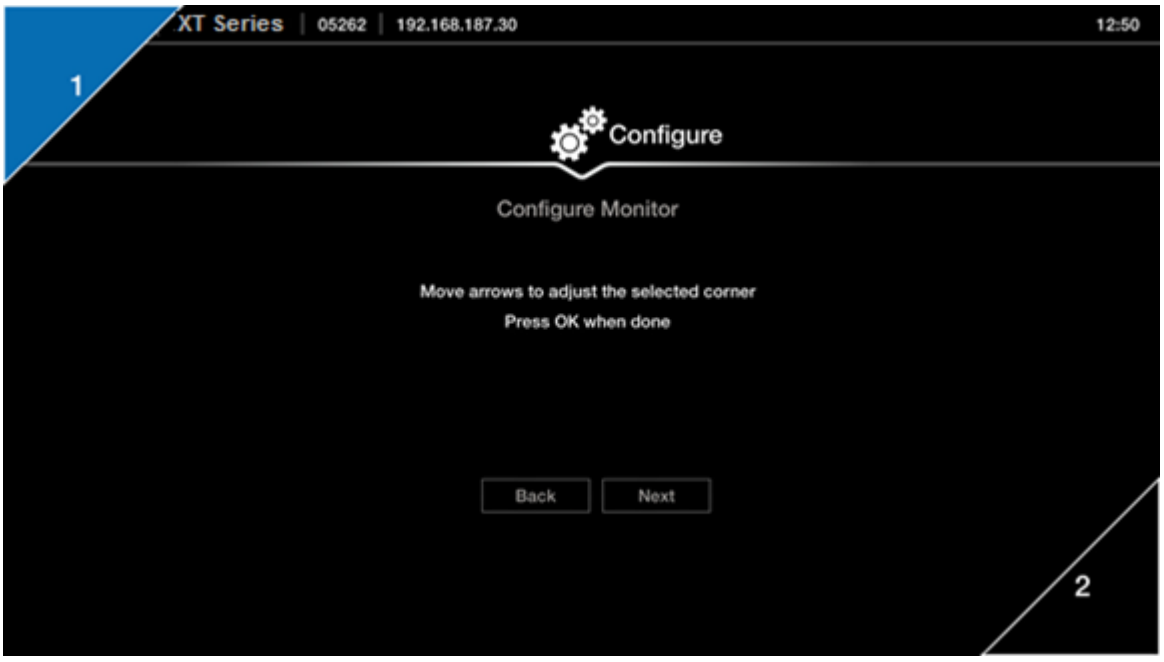


Figure 30: Adjusting the image position

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 58.

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 77.

Before you begin

This procedure is performed as part of the Quick Setup Wizard, after Adjusting the Image Position on page 56. 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 53.

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 12: Configuring IP addresses on page 59 for a description of these fields.
   - **Manual**: Select this option if you require a static IP address. We recommend this option since external endpoints need to dial to this endpoint as an MCU. Enter the fields as described in Table 12: Configuring IP addresses on page 59.

     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 Server Using TLS on page 88.

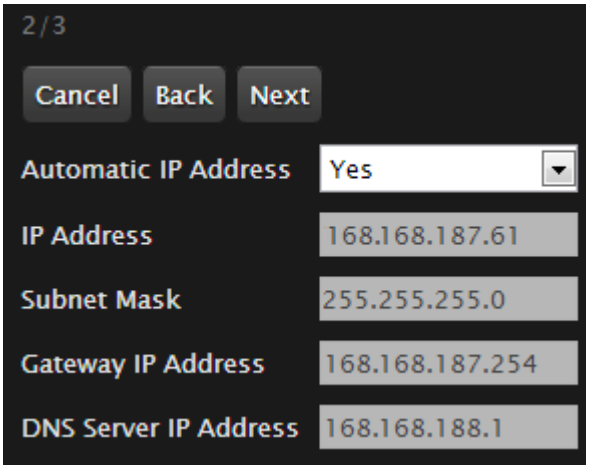


Figure 31: Defining IP Settings

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

Table 12: 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 60.

   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 Server 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 Server for IP Office with a Gatekeeper on page 84.

Before you begin

This procedure is performed as part of the basic configuration after Configuring Network Settings on page 58. 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 53.

Procedure

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

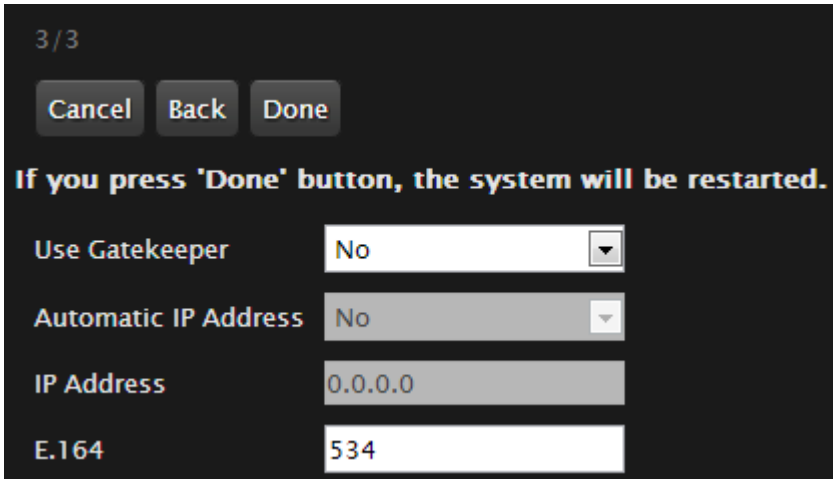


Figure 32: Gatekeeper settings

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 Server for IP Office is complete.

Registering the XT Server to IP Office

About this task

The procedure in this section explains how to register your XT Server 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 Server 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 Server to the Avaya IP Office server.

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Server Locally from the Endpoint on page 45.

Procedure

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

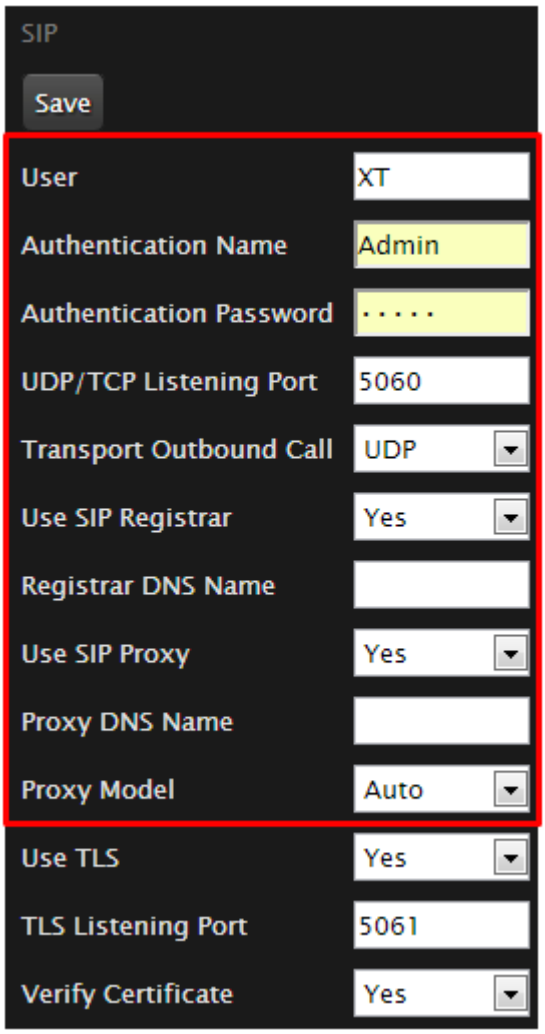


Figure 33: Configuring SIP settings

2. Configure parameters as described in Table 13: Configuring SIP-related parameters on page 62.

Table 13: 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 Server Using TLS on page 88.

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:

- Disable the local video and audio and use the system as an MCU only. See the **Local audio-video (MCU)** field in Table 14: Configuring general call settings on page 65, below.
- 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 Server Locally from the Endpoint on page 45.

Procedure

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

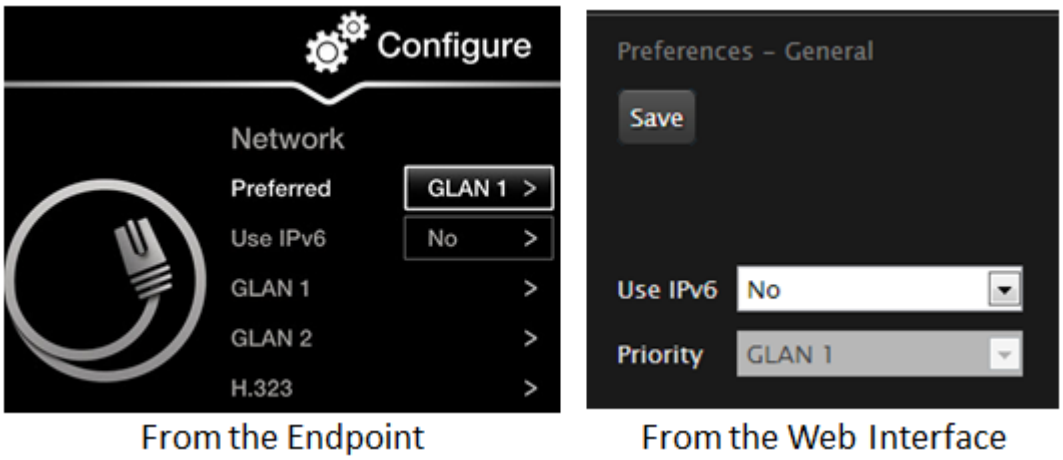


Figure 34: Configuring the Priority setting from the web interface

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**.

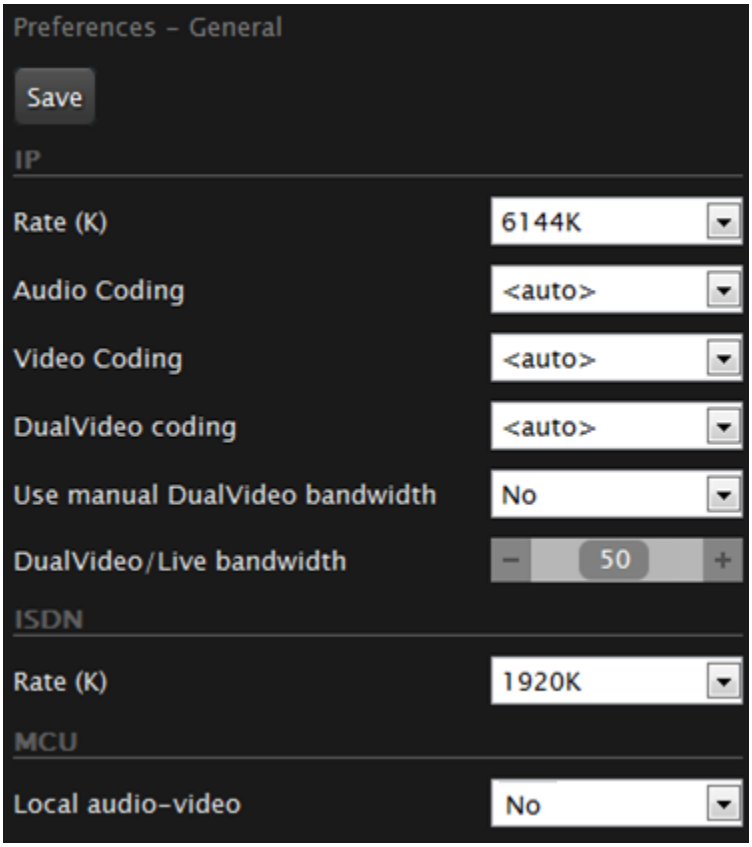


Figure 35: Configuring general call settings

5. Set the fields as described in Table 14: Configuring general call settings on page 65.

Table 14: 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.
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)	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**.

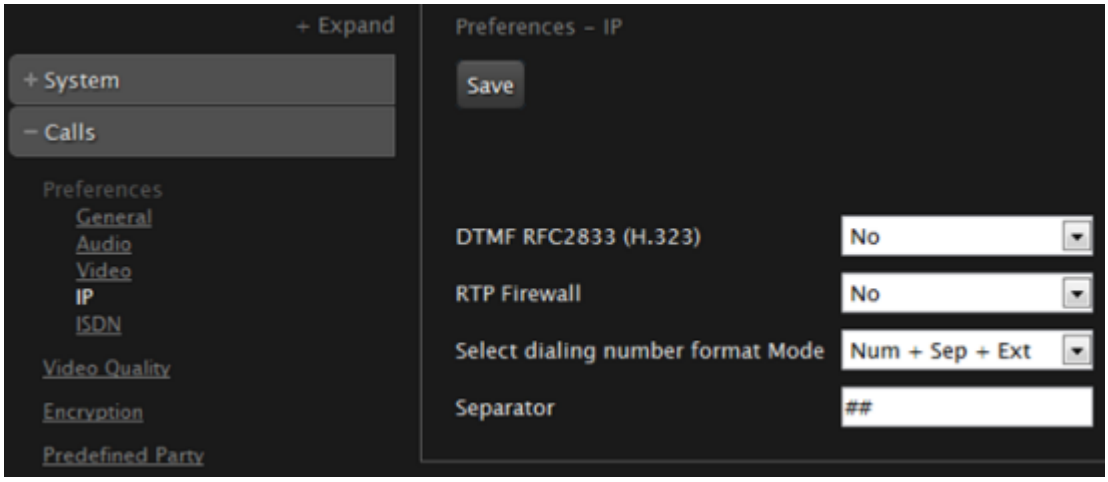


Figure 36: Configuring the IP settings from the web interface

8. Set the fields as described in Table 15: Configuring the IP-related call settings on page 66.

Table 15: 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.
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**.

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

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 55.

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 68.

Procedure

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

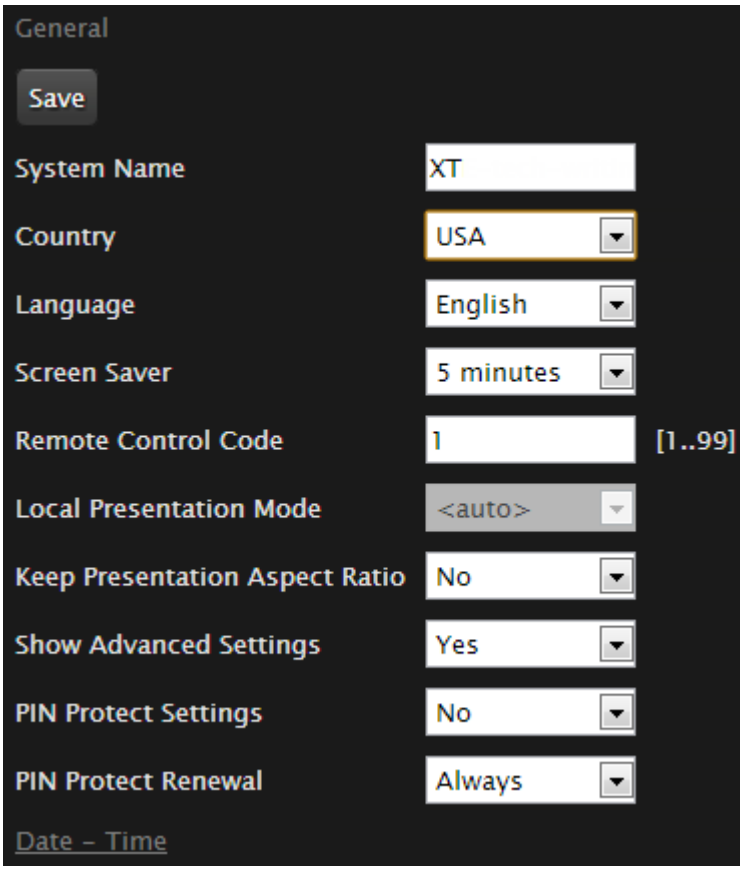


Figure 37: Basic Settings page

2. Enter the name of the XT Server 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 38: Scopia XT Server for IP Office's titlebar on page 68). 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 55.

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 Server to IP Office on page 61 and Registering the Scopia XT Server for IP Office with a Gatekeeper on page 84.

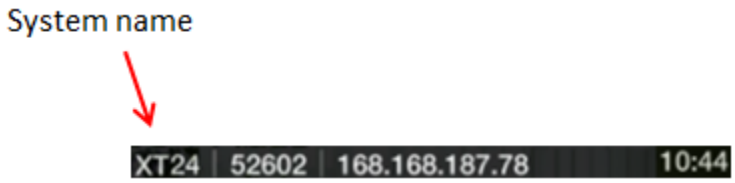


Figure 38: Scopia XT Server for IP Office's titlebar

Procedure

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

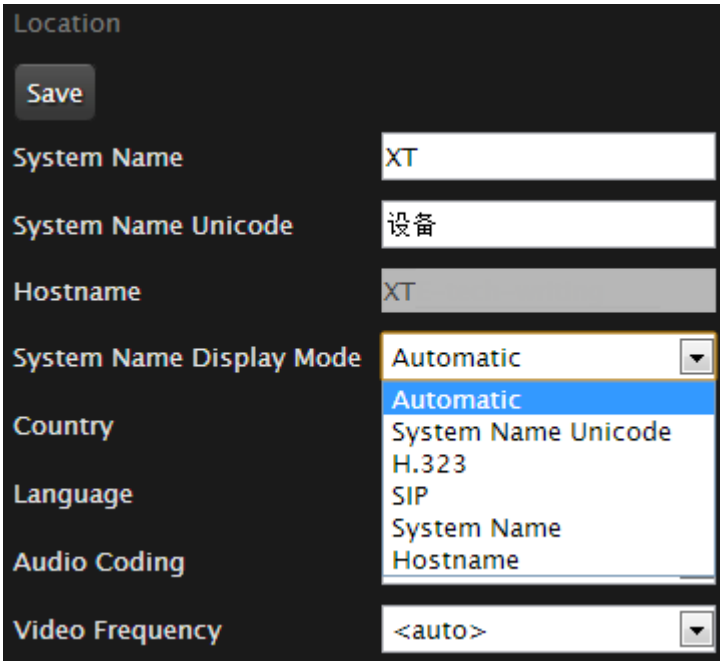


Figure 39: Selecting the system name

2. Enter the following settings:

Table 16: 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 Server 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 Server for IP Office with a Gatekeeper on page 84. • **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 55). If you selected this option from the **System Name Display Mode** list, you can modify the name you want to display in the titlebar (optional). You can only enter alphanumeric characters.
System Name Unicode	If you selected this option from the **System Name Display Mode** list, you can modify the name you want to display in the titlebar (optional). You can enter non-alphanumeric characters, such as Chinese or Japanese letters.
Hostname	You cannot modify the **Hostname**. This field displays the name used to register the system to the network. You may need the system's hostname, for example, if you are locating the device from a list of hostnames on an SNMP agent discovery tool. Typically, the **Hostname** is the same as the **System Name**, unless the **System Name** includes characters that are not supported by the hostname standard. Invalid characters are replaced by the **-** character.

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

Setting the Administrator PIN Code for the XT Server

About this task

This is only relevant if you connected a monitor to your system, as described in Connecting a Monitor to the XT Server on page 25.

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 Server web interface.

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

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

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Server Locally from the Endpoint on page 45.

To modify the PIN, you must be connected via HTTPS (see Enabling Remote Management on the Scopia XT Server for IP Office on page 35).

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

Figure 40: Modifying the administrator PIN

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

3. Enter your new 4 digit PIN code.

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

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

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

Setting Date and Time

About this task

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

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Server Locally from the Endpoint on page 45.

Procedure

1. Access the date and time settings as follows:
   - From the XT Server 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 17: Configuring date and time settings on page 72.

   Important:

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

Table 17: 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.

Field Name	Description
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.
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 Server web interface.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Server Locally from the Endpoint on page 45.

Procedure

1. Access the time zone settings as follows:
   - From the XT Server 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 18: Configuring time zone related settings on page 74.

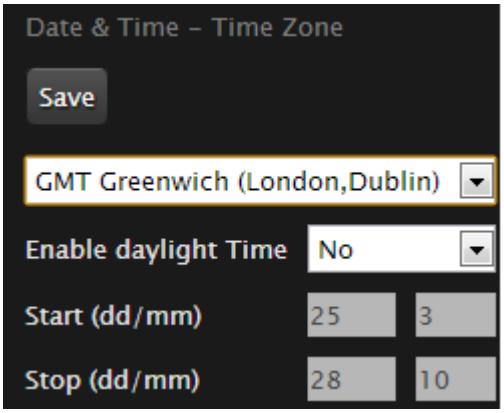


Figure 41: Setting the time zone

Table 18: 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 53). You can modify these settings at any time from the endpoint or the web interface.

Procedure

1. Access the XT Server web interface, as described in Accessing XT Server Web Interface on page 34.
2. Select **Administrator Settings > System > Location**.

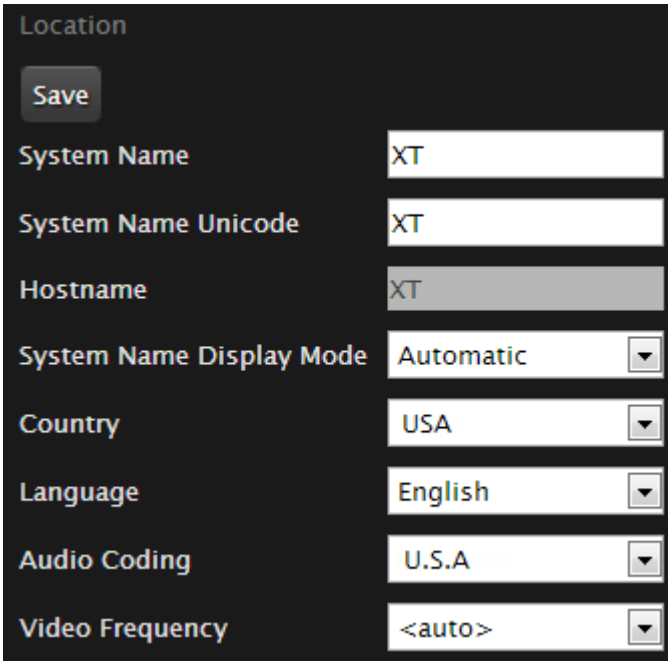


Figure 42: Setting regional information

3. Define regional settings as described in Table 19: Configuring regional information on page 75.

Table 19: 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 Server 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

This is only relevant if you connected a monitor to your system, as described in Connecting a Monitor to the XT Server on page 25.

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

Procedure

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

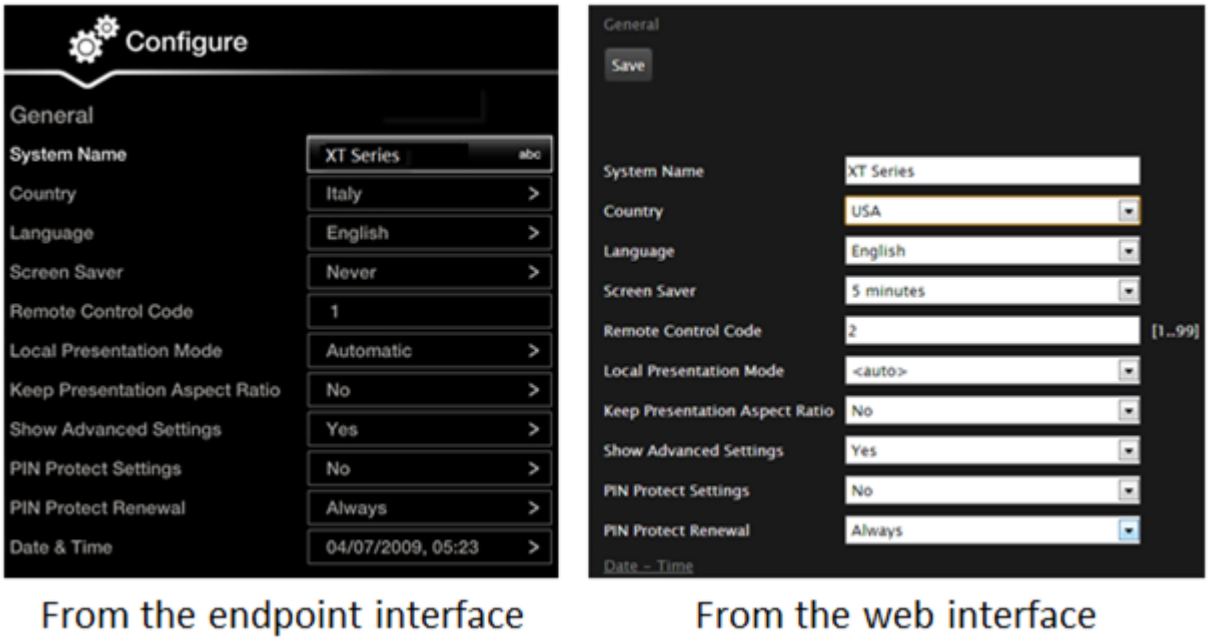


Figure 43: Configuring screen saver settings

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

Configuring 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 77
- Registering the Scopia XT Server for IP Office with a Gatekeeper on page 84

Configuring GLAN Use

You can configure GLAN use for Scopia XT Server 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 77
- Configuring Network Connectivity on page 79
- Enabling NAT and Firewall Traversal with Scopia XT Server for IP Office on page 81
- Determining the Priority of Audio versus Video Quality on page 83

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 Server Locally from the Endpoint on page 45.

Procedure

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

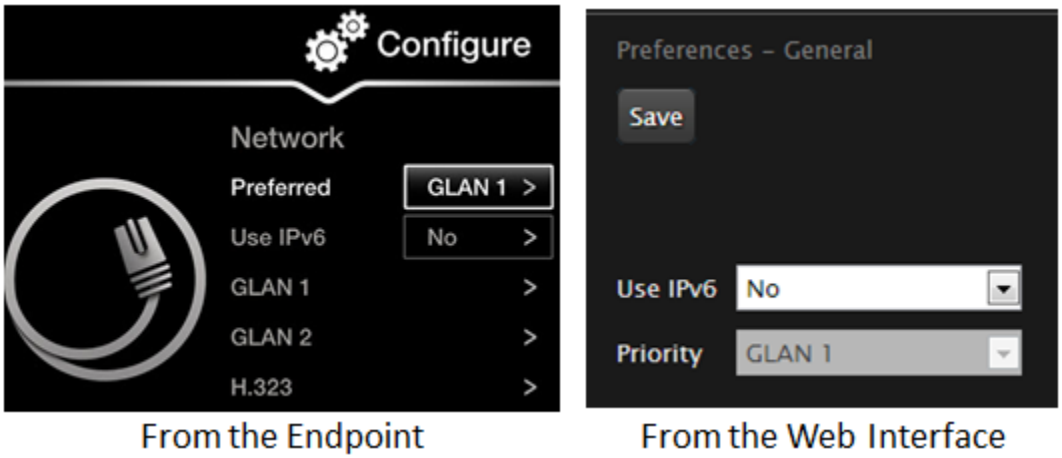


Figure 44: Enabling IPv6 mode

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**.

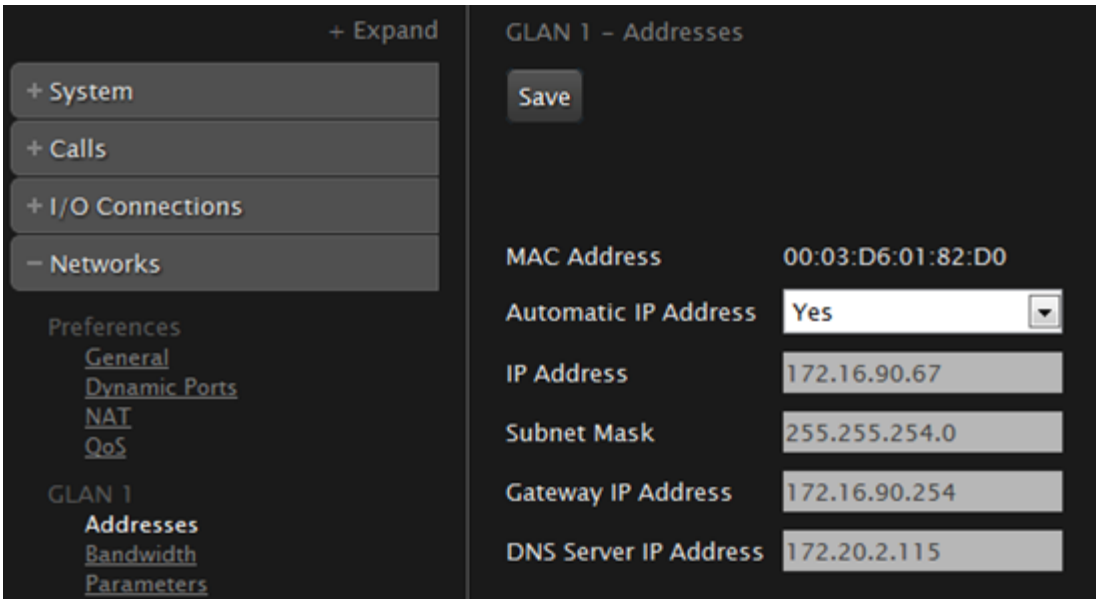


Figure 45: Configuring IP addresses from the web interface

5. Set the fields as described in Table 20: Configuring IP addresses on page 79.

Table 20: 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. We recommend this option since 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 Server Using TLS on page 88.
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.
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 Server 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 Server on page 89.

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 Server Locally from the Endpoint on page 45.

Procedure

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

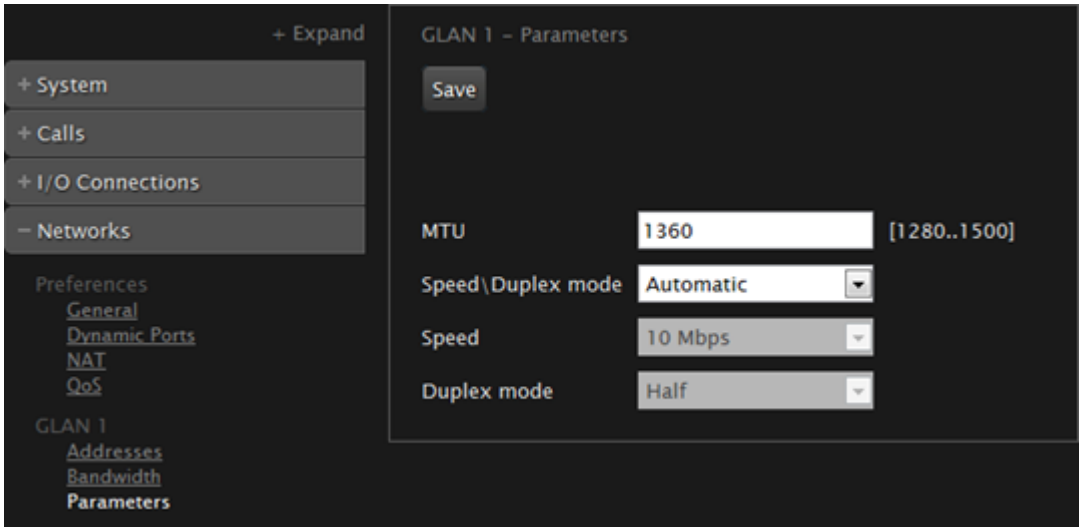


Figure 46: Configuring the GLAN parameters from the web interface

3. Set the field as described in Table 21: Configuring network connectivity on page 81.

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

Table 21: 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 77. 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.
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 Server for IP Office

About this task

Scopia XT Server 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 Server 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 Server for IP Office on page 14.

Before you begin

If configuring from the endpoint, you must first enable advanced configuration, as described in Maintaining the XT Server Locally from the Endpoint on page 45.

Procedure

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

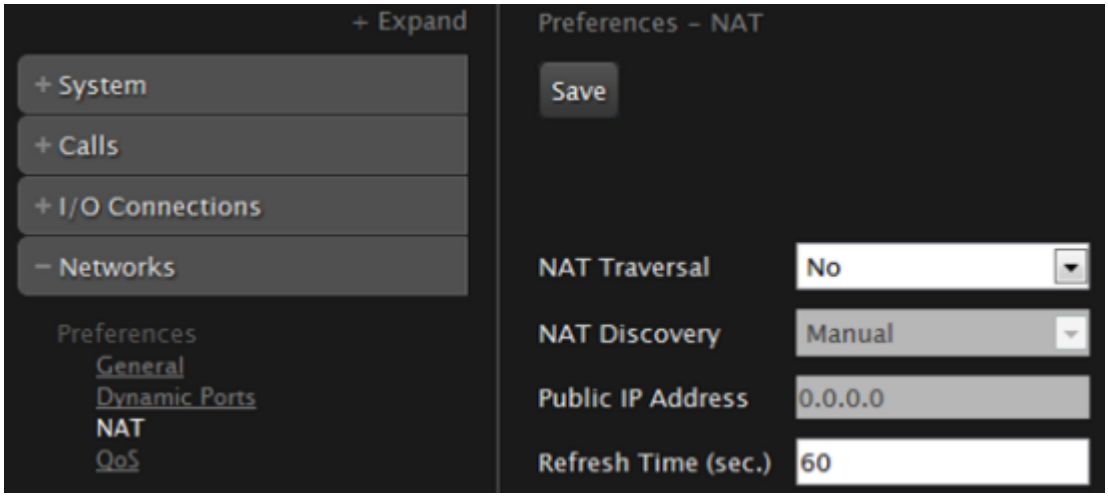


Figure 47: Configuring NAT traversal settings from the web interface

2. Set the fields as described in Table 22: Configuring NAT-related settings on page 82.

Table 22: 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.

Field Name	Description
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 Server for IP Office on page 21.

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 Server for IP Office on page 100.

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 Server Locally from the Endpoint on page 45.

Procedure

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

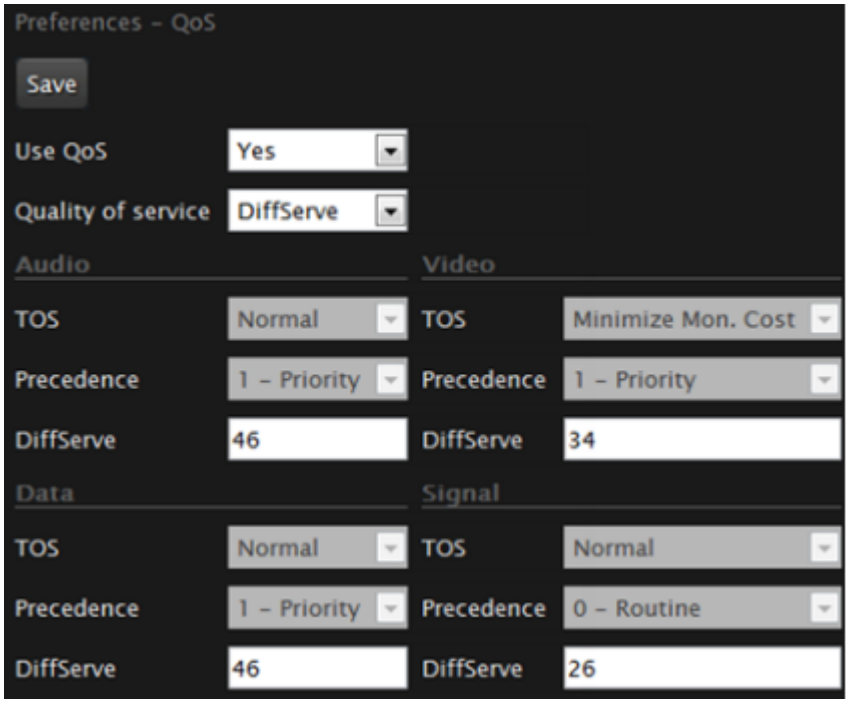


Figure 48: Configuring QoS settings

2. Set the fields as described in Table 23: Configuring QoS settings on page 84.

Table 23: 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 Server 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 Server Locally from the Endpoint on page 45.

Procedure

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

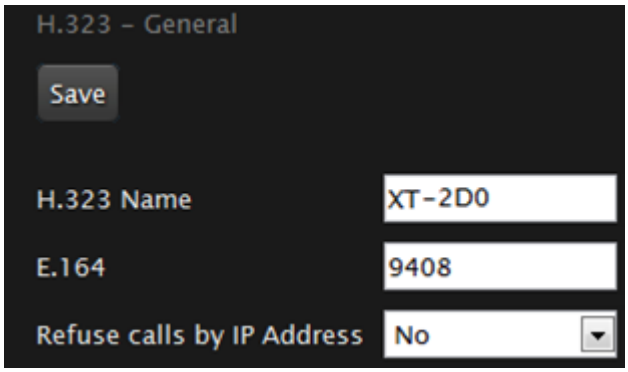


Figure 49: Configuring H.323 settings from the web interface

2. Set the fields as described in Table 24: Configuring H.323 settings on page 86.

Table 24: 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**.

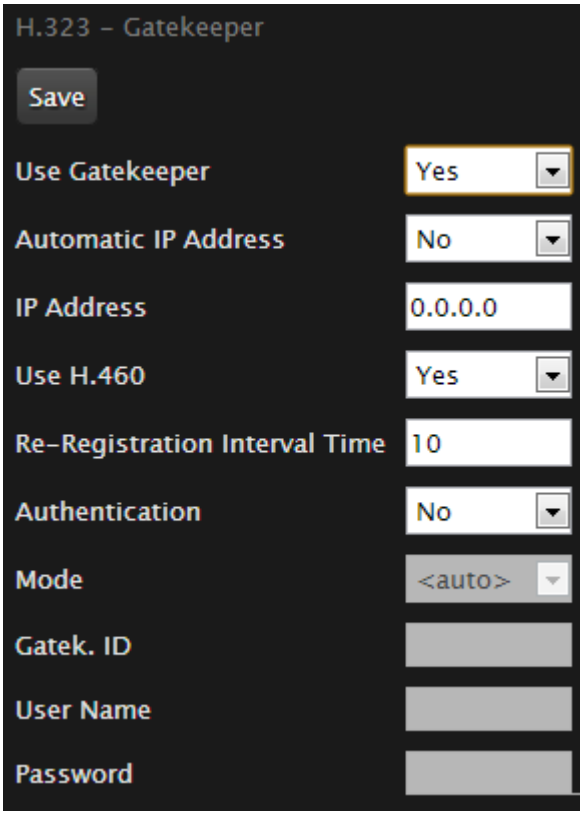


Figure 50: Configuring the Gatekeeper settings from the web interface

5. Set the fields as described in Table 25: Configuring the gatekeeper on page 87.

Table 25: 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**.

Chapter 7 | Securing your Scopia XT Server for IP Office

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

Navigation

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

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

1. Perform Generating a Certificate Signing Request for XT Server on page 89.
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 Server.

3. Perform Uploading XT Server Certificates on page 91.
4. Perform Enabling the TLS Connection in XT Server on page 95 .
5. To encrypt the media (audio, video, presentation) of videoconferences using the SRTP protocol, perform Enabling Encryption for Videoconferences on page 97.

Generating a Certificate Signing Request for XT Server

About this task

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

Important:

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

To restore previously uploaded certificates, see Backing Up and Restoring XT Server Certificates on page 93. To delete the certificates, see Deleting XT Server Certificates on page 94.

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 77.

Procedure

1. Access the XT Server web interface, as described in Accessing XT Server Web Interface on page 34.
2. Select **Administrator Settings > Utilities > Certificates**.
3. Enter your organization's details and your email.

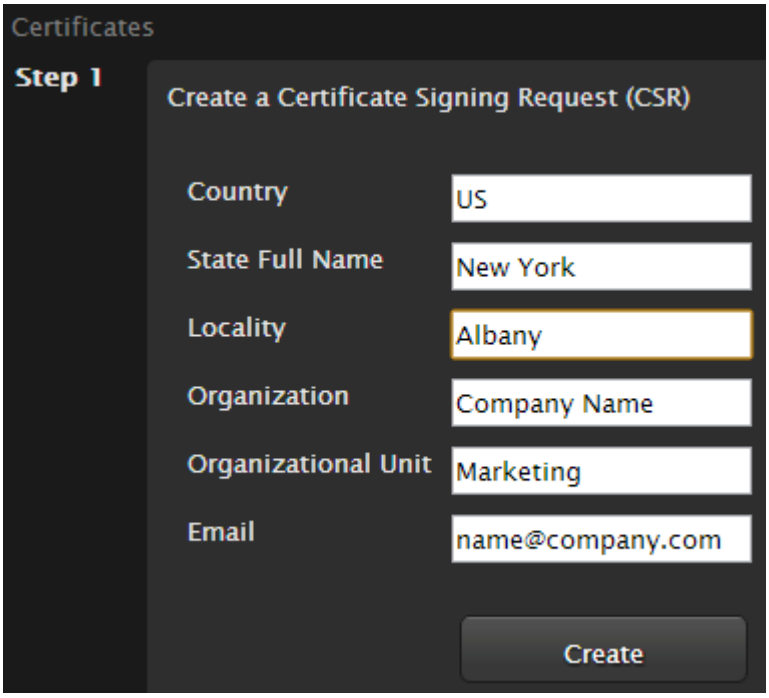


Figure 51: Generating a CSR for Scopia XT Server for IP Office

Table 26: 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.

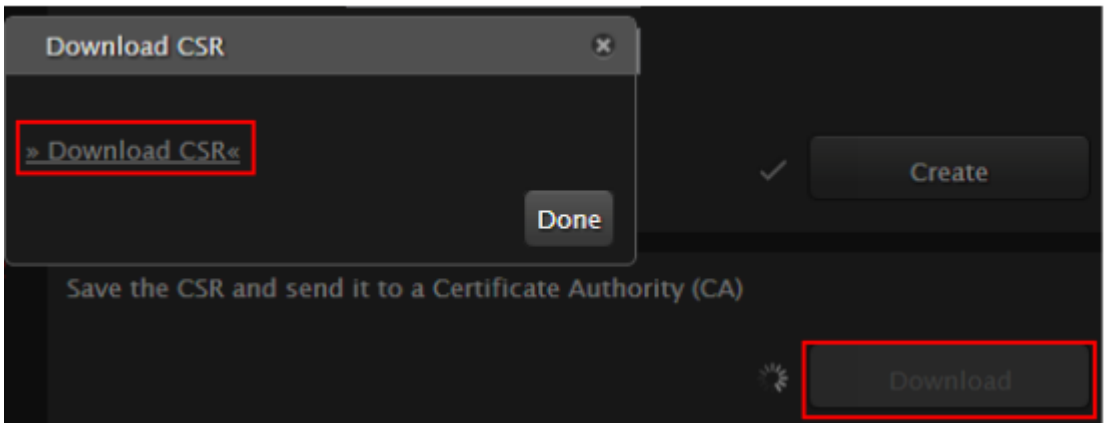


Figure 52: Downloading the CSR

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 Server also have their own certificates, we recommend using a common CA for all certificates for a more efficient implementation.
8. Continue with Uploading XT Server Certificates on page 91.

Uploading XT Server Certificates

About this task

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

To restore previously uploaded certificates or to back up certificates after uploading, see Backing Up and Restoring XT Server Certificates on page 93. To delete the certificates, see Deleting XT Server Certificates on page 94.

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 Server (see Generating a Certificate Signing Request for XT Server on page 89 for details on generating the CSR).

Procedure

1. Access the XT Server web interface, as described in Accessing XT Server Web Interface on page 34.
2. Select **Administrator Settings > Utilities > Certificates**.
3. Import the Certificate Authority (CA) root certificate as follows:

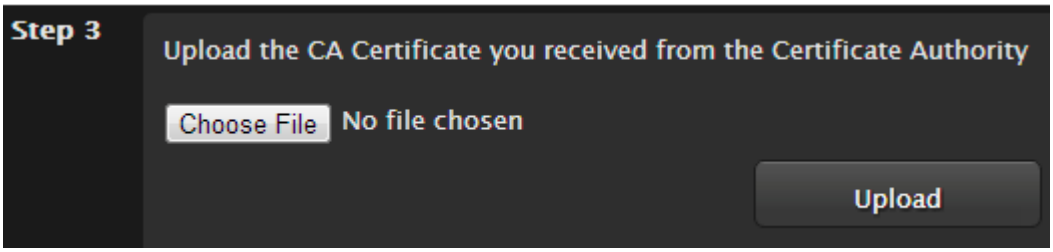


Figure 53: Uploading the CA root certificate

   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:

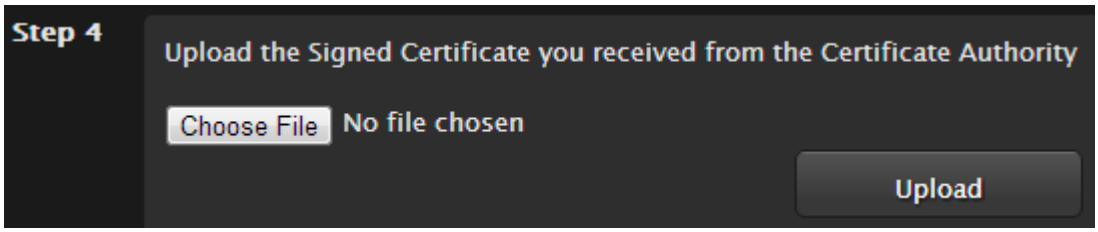


Figure 54: Uploading the signed certificate

   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 55: Signed certificate from the CA on page 93).

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

Figure 55: Signed certificate from the CA

5. Continue with Enabling the TLS Connection in XT Server on page 95.

Backing Up and Restoring XT Server 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 Server Certificates on page 94.

Procedure

1. Connect a USB key to the upper USB port of the XT Codec Unit (Figure 56: Connecting a USB Key to the XT Codec Unit on page 94).

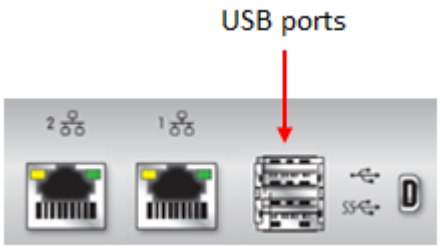


Figure 56: Connecting a USB Key to the XT Codec Unit

2. To back up a certificate to the USB key, select **Advanced > Utilities > Certificates > Backup** (Figure 57: Backing up or restoring certificates on page 94).

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

Figure 57: 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 57: Backing up or restoring certificates on page 94). This automatically restores the certificates and associated keys to the system.

Deleting XT Server Certificates

About this task

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

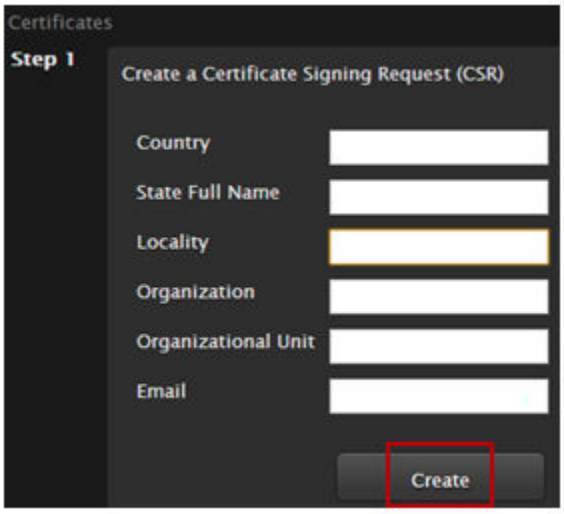
To secure SIP connections using TLS certificates, your system must have a static IP address, since the system generates the certificate request using its IP address as the Common Name (CN).

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 Server Certificates on page 93.

Procedure

1. Access the XT Server web interface, as described in Accessing XT Server Web Interface on page 34.
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 58: Removing Current Certificates



Enabling the TLS Connection in XT Server

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 Server.

Before you begin

Upload the required certificates to the XT Server, as described in Uploading XT Server Certificates on page 91.

Procedure

1. Access the XT Server web interface, as described in Accessing XT Server Web Interface on page 34.
2. Select **Administrator Settings > Protocols > SIP**.
3. Select **Yes** from the **Use TLS** list to accept incoming calls using TLS.

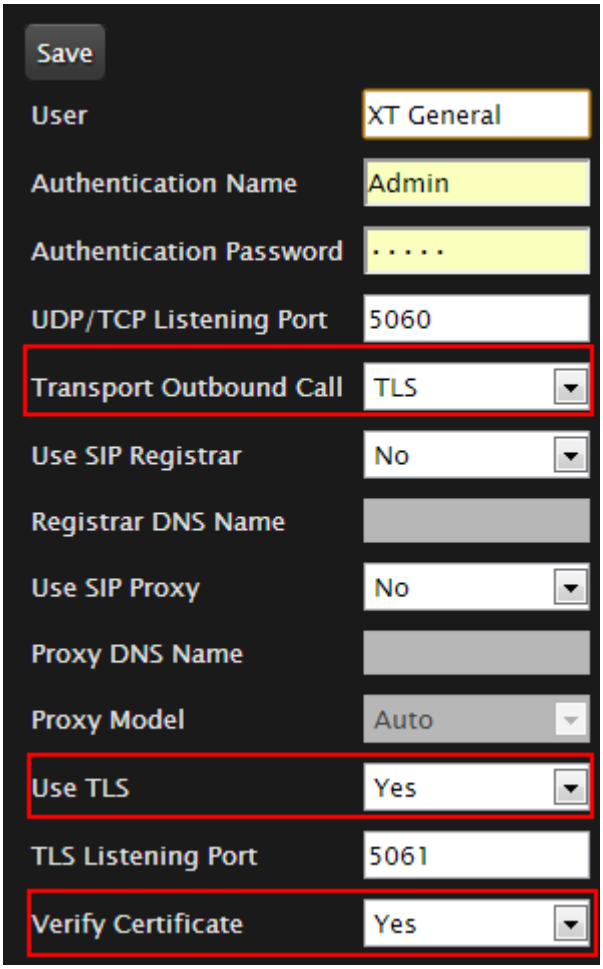


Figure 59: Enabling TLS

4. Define the following settings:

Table 27: 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 Server 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 Server for IP Office.

5. Select **Save**.
6. (Optional) If required by your organization's security policies, continue with Enabling Encryption for Videoconferences on page 97.

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 Server web interface. If you are not connecting a monitor to the XT Server, you can perform this procedure from the web only.

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 Server Locally from the Endpoint on page 45.

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 Server Using TLS on page 88). If TLS is not enabled, only SIP calls to other XT Server endpoints are encrypted, using a proprietary encryption protocol.

Procedure

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

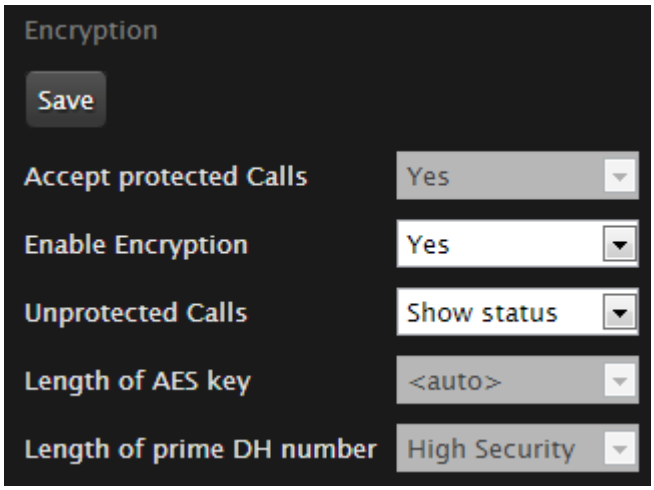


Figure 60: Encrypting calls from the web interface

2. Select **Yes** from the **Enable encryption** field.
3. Set the fields as described in Table 28: Configuring settings for securing calls on page 99.

Table 28: Configuring settings for securing calls

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

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

Chapter 8 | Troubleshooting the Scopia XT Server for IP Office

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

Navigation

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 Server web interface. If you are not connecting a monitor to the XT Server, you can perform this procedure from the web only.

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 Server 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**.

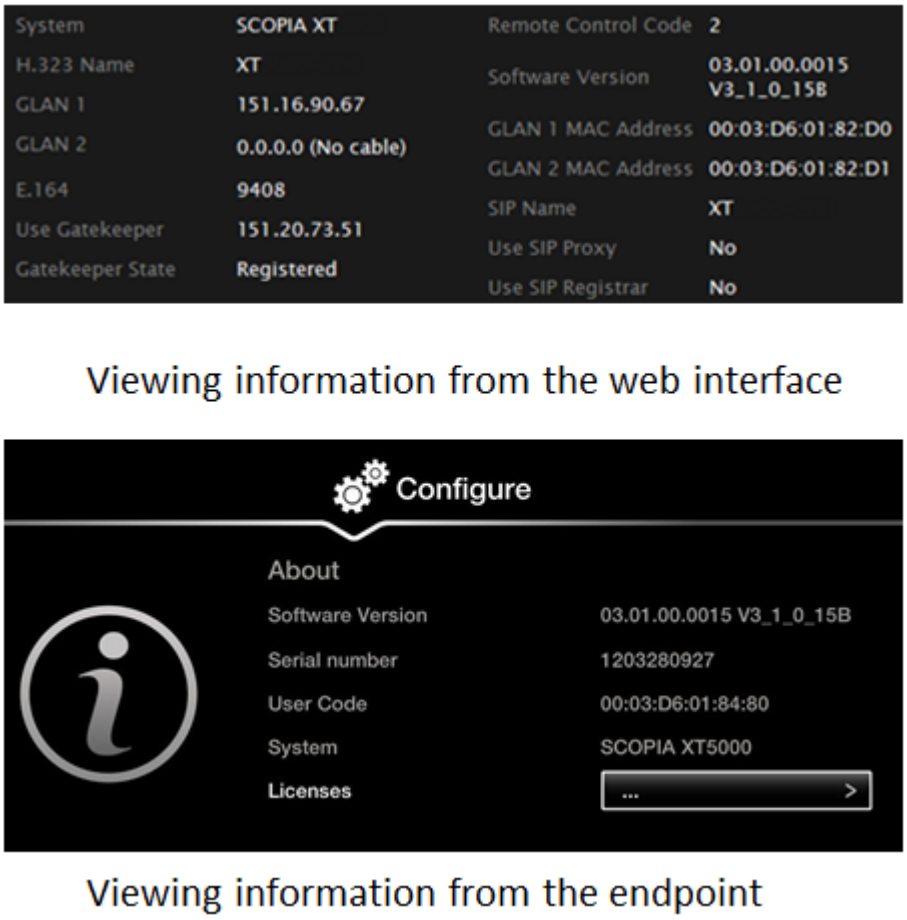


Figure 61: Viewing system information

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 62: Viewing system network information

Resolving Monitor Display Problems

Problem This is only relevant if you connected a monitor to your system, as described in Connecting a Monitor to the XT Server on page 25.

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 56 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 Server Locally from the Endpoint on page 45.

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 Server 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 29: 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 56.
Right	

4. 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 100).

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 63: GLAN1 port on page 104.

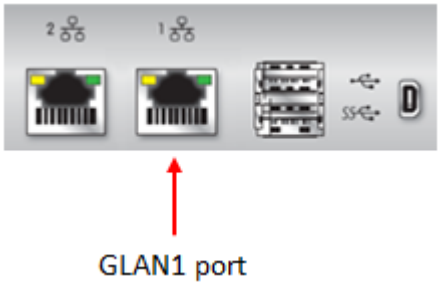


Figure 63: GLAN1 port

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 77.

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 Server Locally from the Endpoint on page 45.

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

Figure 64: 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 Server Locally from the Endpoint on page 45.

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

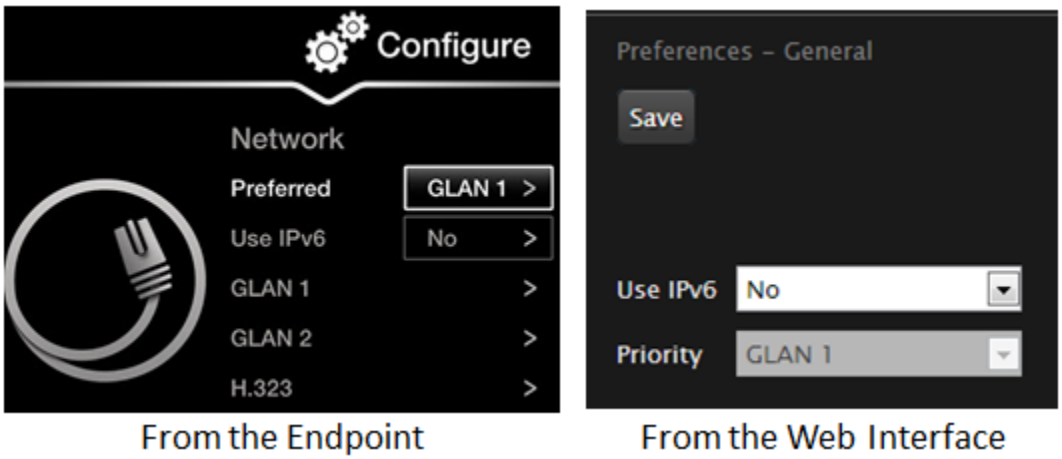


Figure 65: Setting network preferences

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

Resolving XT Remote Control Unit Problems

Problem The XT Remote Control Unit does not function.

Solution Replace the battery, as described in Installing the Batteries of the XT Remote Control Unit on page 26. 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 43).

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

Restoring Default User Settings

About this task

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

Before you begin

- Turn on the Scopia XT Server 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.
- Connect a monitor to system so that you can manage the system from the endpoint's own interface, as described in Connecting a Monitor to the XT Server on page 25.

Procedure

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

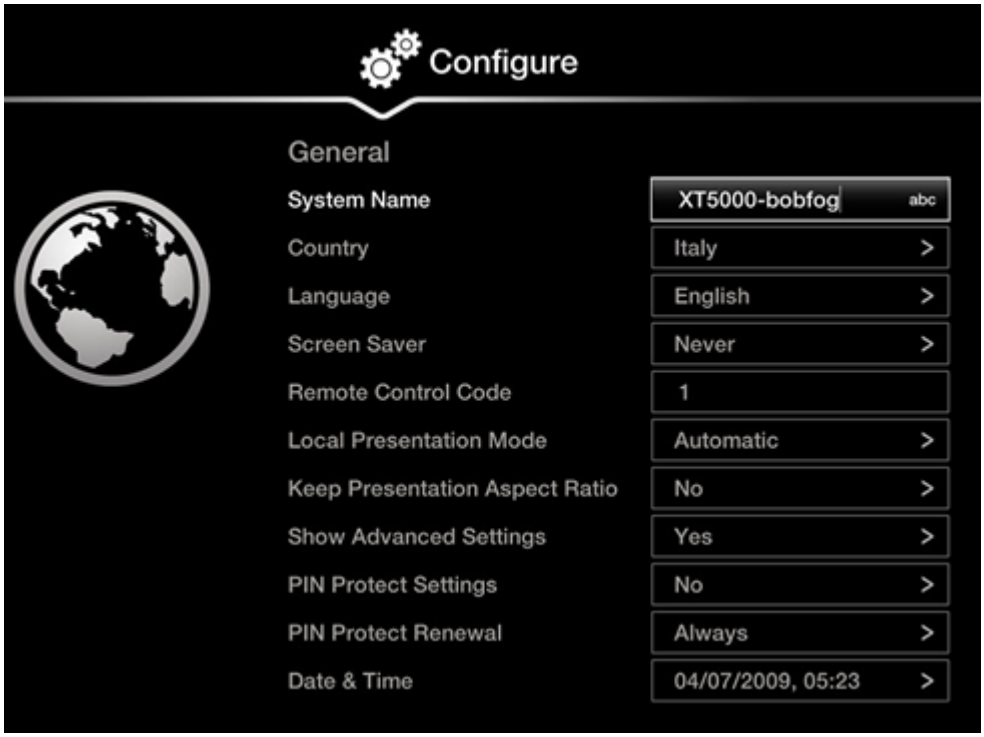


Figure 66: Enabling advanced settings

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 67: 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