

Scopia Elite 6000 Series MCU

Administrator Guide

Version 8.2

For Solution 8.2



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

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

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

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

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

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

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

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

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

*Administrator Guide for Scopia Elite 6000 Series MCU
Version 8.2, July 11, 2013*

<http://www.radvision.com>

Table of Contents

Chapter 1: About the Scopia Elite MCU

About Scopia Elite 6000 Series MCU	5
Minimum Requirements and Specifications	7

Chapter 2: Planning your MCU Deployment

Planning a Centralized or Distributed Topology (Cascading) for MCU	10
About the Capacity of the MCU	13
Ports to Open for the Scopia Elite 6000 Series MCU	14

Chapter 3: Maintaining the Scopia Elite MCU

Adding a License to the MCU	17
Configuring a New MCU Meeting Type	19
Regulating Bandwidth Usage of a Meeting Type	23
Applying a Meeting Type to a Videoconference	25
Configuring the Auto-Attendant Service	26
Securing MCU and Scopia Management Connection with TLS	27
Securing MCU with TLS in a SIP Environment	27
Uploading TLS Certificates to the MCU	28
Configuring Security Access Levels for the Scopia Elite MCU	33
Configuring IP Separation on the MCU	34
Managing Scopia Elite MCU User Profiles	38
Adding a User Profile	39
Changing a User Password	40
Deleting a User Profile	40
Adding a Power Supply Unit to the MCU	41
Removing a Power Supply Unit from the MCU	43
Backing Up Your Scopia Elite MCU Configuration	45
Restoring Your Scopia Elite MCU Configuration	45
Upgrading Scopia Elite 6000 Series MCU Software	46
Restoring a Previous Software Version	48
Configuring Ports on All Models of the Scopia Elite MCU	50

Configuring the UDP Port Ranges for RTP/RTCP on the Scopia Elite MCU	50
Configuring the TCP Port Range for H.245 on the Scopia Elite MCU	51
Configuring the HTTP Port on the Scopia Elite MCU	52
Configuring the UDP Port for RAS on the Scopia Elite MCU	53
Configuring the UDP Port for the Gatekeeper on the Scopia Elite MCU	54
Configuring the TCP Port Q.931 on the Scopia Elite MCU	55
Configuring the TCP/UDP/TLS Port for SIP on the Scopia Elite MCU	56
Configuring the TCP Port Range for SIP BFCP on the Scopia Elite MCU	57
Customizing the Logo Displayed in MCU Conferences	58
Customizing MCU Audio Messages	60

Chapter 4: Moderating a Videoconference from the MCU

Creating a New Videoconference from the MCU	64
Muting and Unmuting Participants	66
Changing the Video Layout of an Ongoing Videoconference	67
Personalizing Video Layouts for Participants	69
Blocking Access to a Videoconference	73
Viewing Participant Call Information	73
Displaying Participant Names in the Video Layout	77
Ending a Videoconference from the MCU	79

Chapter 5: Troubleshooting the Scopia Elite MCU

Defining an Advanced Command on the MCU	80
Resolving MCU Failure to Register with the Gatekeeper	81
MCU Cannot Start a Videoconference	82
MCU Does Not Allow Access an Existing Videoconference	83
Poor Quality in Cascaded Videoconferences	84
Endpoints Unexpectedly Disconnect from Videoconferences	84
Videoconference Ends Unexpectedly	84
Resolving Presentation Issues	86
SIP Call Disconnected Unexpectedly	87
Resolving Poor Video Quality	88
Resolving Poor Audio Quality	91
Resolving a Video Display Issue	92

Chapter 1 | About the Scopia Elite MCU

The Scopia Elite MCU is Scopia Solution's flagship platform for high definition multi-party videoconferencing. The MCU supports communications in the board room, at the desktop, in the home, or on the road over wireless.

Navigation

- [About Scopia Elite 6000 Series MCU](#) on page 5
- [Minimum Requirements and Specifications](#) on page 7

About Scopia Elite 6000 Series MCU

The Scopia Elite MCU is Scopia Solution's flagship platform for high definition multi-party videoconferencing.

An MCU, or Multipoint Control Unit, connects many endpoints to a single videoconference. It typically manages the audio mixing and video layouts, adjusting the output to suit each endpoint's capabilities.

The Scopia Elite MCU harnesses revolutionary processing power for the most demanding videoconferencing applications using the latest DSP technologies. It supports dual channels of Full HD 1080p at 60 frames per second for video and content, H.264 High Profile for bandwidth efficiency, H.264 Scalable Video Coding (SVC) for high network error resiliency, and full support for many telepresence systems, bringing an uncompromised videoconferencing experience.

With the Scopia Elite MCU, each videoconference participant receives a quality experience optimized to their individual capabilities from wireless mobile devices to HD room systems and immersive telepresence systems. The Scopia Elite MCU leads in video interoperability, working with the broadest range of video systems on the market from leading UC clients to mobile devices and telepresence systems.

The Scopia Elite MCU also features a patented, distributed architecture approach known as the Virtual MCU or cascaded videoconferences, which bring unparalleled scalability to its superb videoconferencing experience.

The MCU's feature list includes:

- Revolutionary video processing power

The Scopia Elite MCU brings unmatched power and capacity in a single unit, enabling dual-channel Full HD 1080p resolution at 60 frames per second for video and content, simultaneous H.264 High Profile and H.264 SVC, and support for multi-stream telepresence.

- Dynamic resource allocation

A meeting can support a mix of SD and HD users, making most efficient use of available resources. Video and audio processing is carried out per user rather than per meeting, with resolutions ranging from QCIF to 1080p in the same meeting. Each user connects using unique, optimized audio and video settings to enjoy the best audio and video quality supported by their endpoint and network, without affecting the other participants in a conference.

- Intuitive and easy to use

Video menus make it easy to set up or enter a videoconference, and the intuitive web interface makes administration easy.

- Massive scalability

The Scopia Elite MCU's Virtual MCU enables a unique scalability in both local and distributed architectures to combine the capacity of multiple MCU devices in the same meeting. The number of supported connections depends on your license.

- Seamless interoperability

The Scopia Elite MCU is built on the solid foundation of Radvision's H.323 and SIP software, ensuring full compliance and broad-ranging interoperability with IP, ISDN, and 3G endpoints. It also enables H.323 and SIP endpoints to collaborate in the same videoconference. See [Figure 1: Endpoints in the same videoconference](#) on page 6.

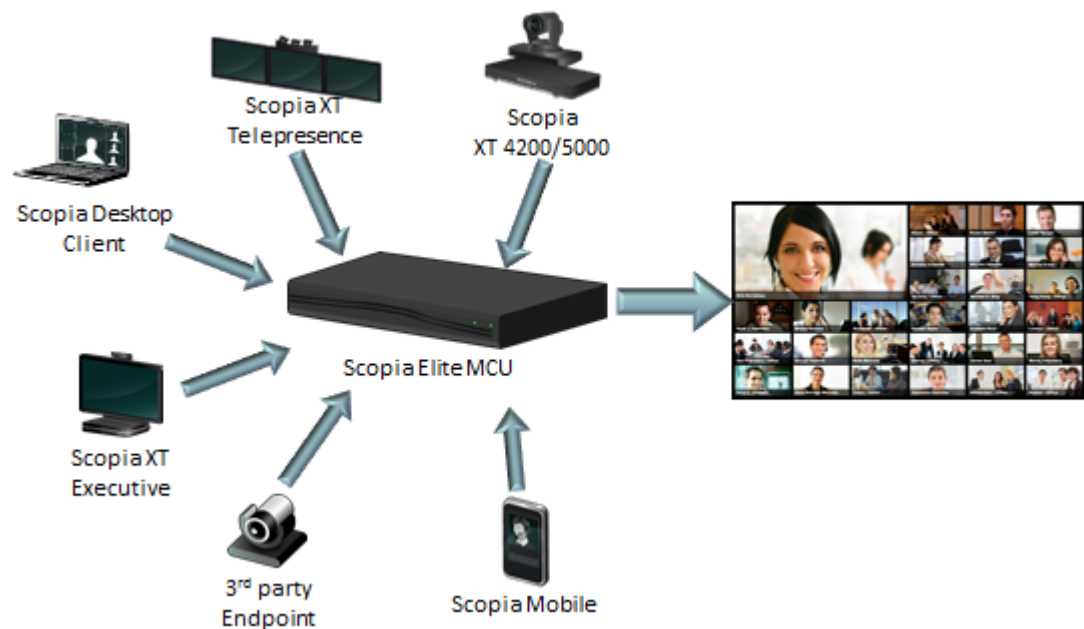


Figure 1: Endpoints in the same videoconference

The Scopia Elite MCU also easily integrates telepresence systems with regular videoconferencing systems, even within the same meeting. It is compatible with telepresence systems from Cisco, Tandberg, Polycom, and LifeSize/Logitech.

When used with Scopia Solution gateways, the deployment can even add ISDN, V.35 and other endpoints to the same meeting.

- Content sharing with SIP and H.323

The Scopia Elite MCU supports sharing presentations and other content via SIP (using the BFCP standard) and H.323 (using the H.239 standard). A user can connect to a meeting from either type of endpoint to share content such as presentations, spreadsheets, documents, and movies.

- Video quality

The Scopia Elite MCU delivers enterprise quality video and audio processing, using latest industry standards including state-of-the-art DSP hardware and software. This video quality is supported by:

- The Scopia Elite MCU supports SVC error resiliency for unmanaged networks using Temporal Scalability and Forward Error Correction (FEC).

Forward Error Correction (FEC) is a proactive method of sending redundant information in the video stream to preempt quality degradation. SVC extends the H.264 codec standard to dramatically increase error resiliency and video quality without the need for higher bandwidth.

- Frame rates can reach 60 frames per second, ensuring smooth video movement.
- A choice of 24 video layouts
- Bitrate (data speed) of up to 12 megabits per second on each stream without affecting capacity. Bitrate is the speed of data flow. Higher video resolutions require higher bitrates to ensure the video is constantly updated, thereby maintaining smooth motion.

- Security and privacy

The Scopia Elite MCU can encrypt communications with endpoints to create secure connections with H.235-based encryption for H.323 endpoints and SRTP and TLS encryption for SIP endpoints.

In addition, the Scopia Elite MCU features administrator and operator password protection for accessing the web interface. It also features optional PIN protection for joining a videoconference, and additional PIN protection for moderator control.

- Support for IP Separation

The Scopia Elite MCU enhances security within the enterprise by routing media and management traffic to two different subnets.

- Intuitive web-based management and control

You can configure both the Scopia Elite MCU and its videoconference sessions through an intuitive web interface offering easy, high-level conference control and administrative flexibility for an enhanced user experience.

- In-meeting indicators

A range of messages and icons are displayed on the endpoint during meetings as events occur. For example, participants are notified when someone joins or leaves the meeting.

- Personalized video layouts per meeting or per participant

You can choose from 24 video layouts for all participants or each participant can customize their own view. You can view up to 28 participants on your screen.

- Easy creation of logs for Customer Support

You can easily create a file containing logs and settings which you can send to Customer Support for troubleshooting.

- Recording via moderator menu

Moderators can record meetings using the Scopia Elite MCU moderator menu in deployments which include the Scopia Desktop recording option.

- In-conference control

During a videoconference, participants can use their endpoint remote control or keypad to perform actions such as mute, volume control, changing video layouts and inviting participants. These options are presented in the in-meeting menu overlaid on the video layout.

- Interactive Voice Response (IVR) messages

The Scopia Elite MCU includes pre-recorded greetings to participants and announcements as each new participant joins a meeting. You can record messages to provide custom greetings and announcements, but typically Scopia Management supplies these messages across all MCUs in the organization.

Minimum Requirements and Specifications

This section details the system specifications of the Scopia Elite 6000 Series MCU 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.

Hardware requirements

[Table 1: Physical device specifications](#) on page 8 refers to the physical details of the device.

Table 1: Physical device specifications

	Scopia Elite MCU 6105, 6110 and 6120	Scopia Elite MCU 6140
System power requirements	100-240 VAC, 50/60 Hz	100-240 VAC, 50/60 Hz with hot-swap redundant AC power supply and feed (optional)
Maximum power consumption	200W (682 BTU/h)	360W (1228 BTU/h)
Operating temperature	10°C to 35°C (50°F to 95°F)	
Relative humidity	5% to 90% non-condensing	
Storage temperature	-40°C to 70°C (-40°F to 158°F), ambient	
Physical dimensions	Height: 43mm (1.7"), width: 437mm (17.2"); depth 664mm (26.1")	Height: 43mm (1.7"), width: 437mm (17.2"); depth 790mm (31.1")
Net weight	Approx 11kg (24.25lbs)	Approx 14.5kg (32lbs) with one power supply.
Gross weight (with packaging)	17kg (37.5lbs)	21kg (46.3lbs)
Rack mounting	19-inch rack-mountable with flanges	
Acoustics	Low noise fan speed control	

Software Specifications

The technical specifications of the protocols and software requirements apply to all Scopia Elite 6000 Series MCU models:

- Signaling protocols:
 - H.323
 - SIP
 - H.320 (in conjunction with Scopia H.320 Gateways)
- Audio support:
 - Codecs: MPEG4 AAC-LC, G.711, G.722, G.722.1, G.729, Polycom® Siren14™/G.722.1 Annex C
 - DTMF tone detection (in-band, H.245 tones and RFC2833)

- Video support:
 - High Definition Continuous Presence video with a resolution of 1080p at up to 60fps
 - Codecs: H.263, H.263+, H.264, H.264 SVC, H.264 High Profile
 - Live video resolutions: QCIF up to 1080p
 - Presentation video resolution: VGA, SVGA, SXGA, XGA, 720p, 1080p, WUXGA
 - Video bandwidth: up to 12Mbps for 1080p resolutions and up to 6Mbps for 720p or lower

- Web browser support:

- Microsoft Internet Explorer versions 6, 7, 8 and 9
- Mozilla Firefox version 3.3 and above
- Google Chrome
- Apple Safari

- Call capacity:

For information on the default capacity of your MCU and how to increase it, see [About the Capacity of the MCU](#) on page 13.

Chapter 2 | Planning your MCU Deployment

When planning your MCU deployment, it is important to consider both bandwidth usage and port security, as described in the following sections:

Navigation

- [Planning a Centralized or Distributed Topology \(Cascading\) for MCU](#) on page 10
- [About the Capacity of the MCU](#) on page 13
- [Ports to Open for the Scopia Elite 6000 Series MCU](#) on page 14

Planning a Centralized or Distributed Topology (Cascading) for MCU

When your organization has more than one site, like a headquarters and several branches, the Scopia Solution offers a unique method of cutting video bandwidth costs, known as cascaded meetings.

A cascaded videoconference is a meeting distributed over more than one physical MCU, where a master MCU connects to one or more slave MCUs to create a single videoconference. It increases the meeting capacity by combining the resources of several MCUs. This can be especially useful for distributed deployments across several locations, reducing bandwidth usage.

Without cascading, if you choose a centralized MCU deployment, frequent videoconferences between branches can be expensive ([Figure 2: Centralized MCU deployment, where all branches use the HQ MCU](#) on page 11).

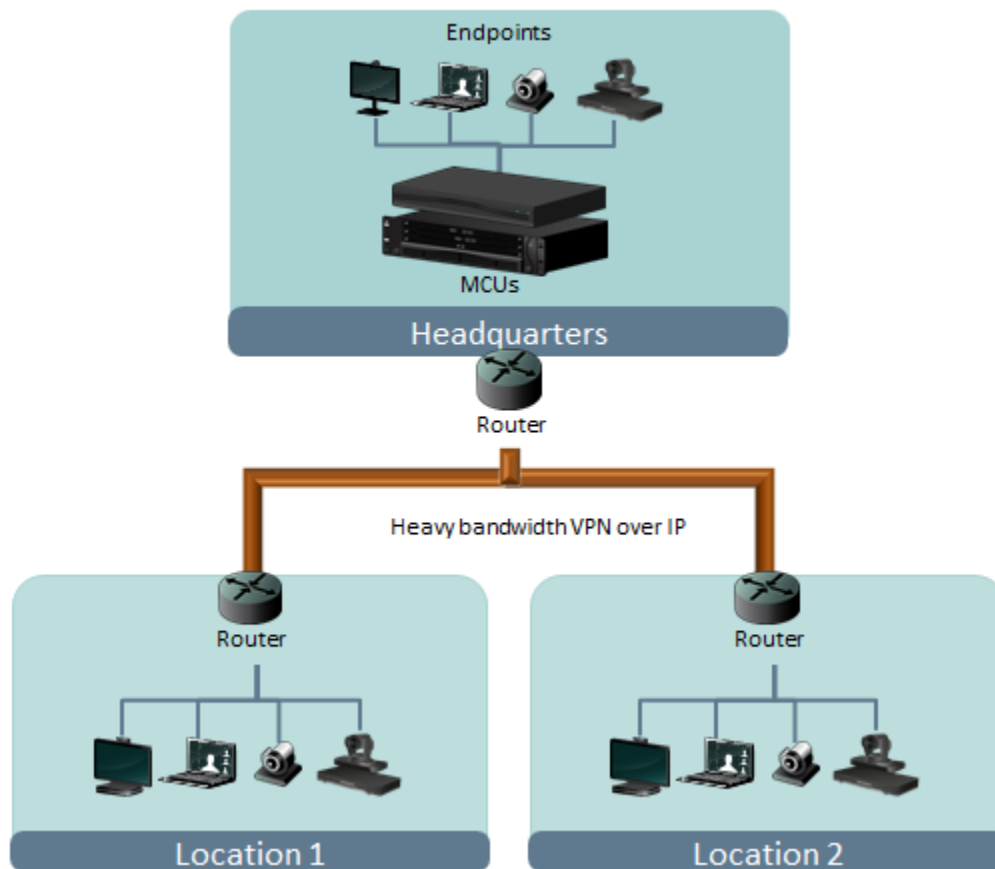


Figure 2: Centralized MCU deployment, where all branches use the HQ MCU

To reduce cross-site bandwidth costs, a distributed MCU deployment ([Figure 3: Distributed MCU deployment cascading meetings for reduced WAN bandwidth](#) on page 12) can perform cascaded conferences. Local participants connect to their local MCU, and the conference is cascaded by connecting between the MCUs using a fraction of the bandwidth compared to the centralized deployment.

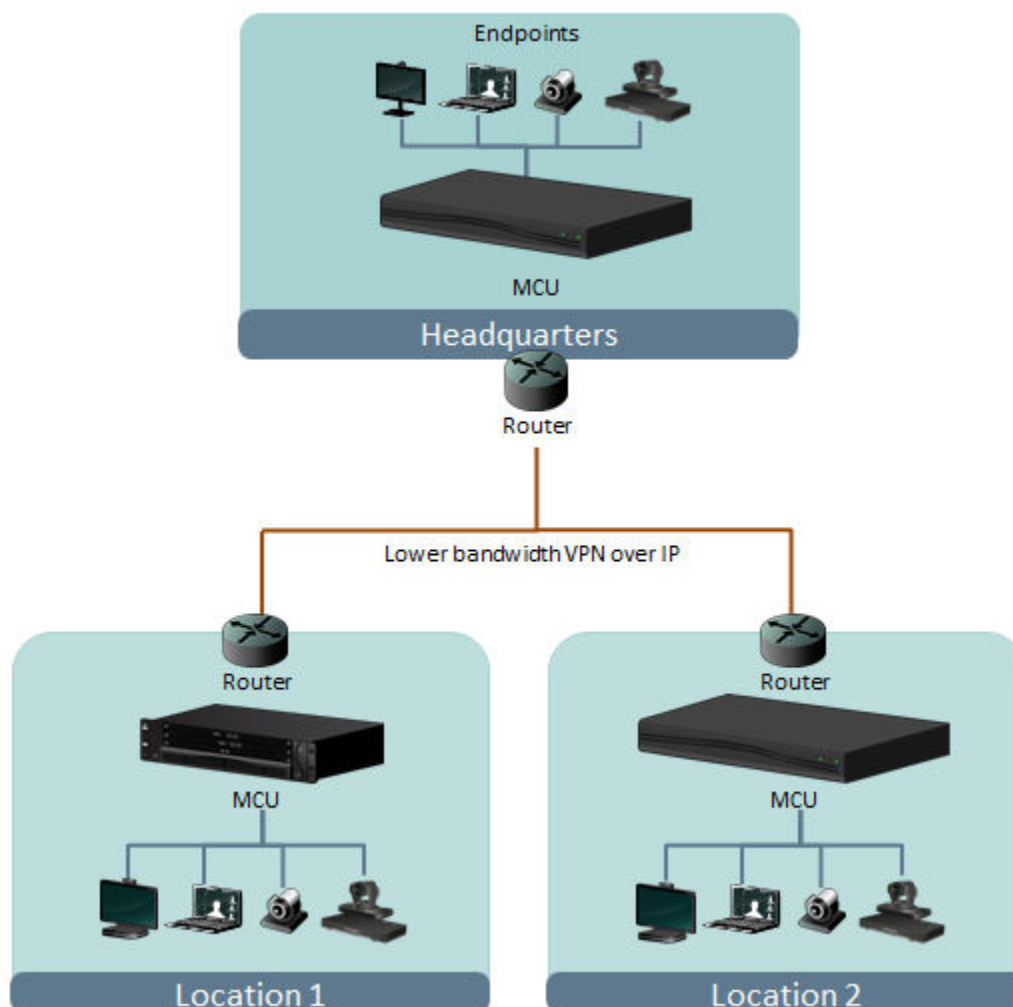


Figure 3: Distributed MCU deployment cascading meetings for reduced WAN bandwidth

The same principles apply to an MCU in the same location, thus increasing call capacity by cascading conferences between them.

Users of distributed MCU deployments do not need to choose a specific MCU. The powerful functionality of virtual rooms enables you to dial the same number anywhere in the world, while the Scopia Solution infrastructure transparently directs you to the correct meeting on the correct MCU.

The bandwidth used by a cascaded link is equivalent to only a single client connection in each direction: upload and download. The bandwidth value is determined by the MCU meeting type (or service), which is invoked when choosing a dial prefix for the meeting. You define the maximum bandwidth for each meeting type in the MCU. For more information on defining meeting types, see [Regulating Bandwidth Usage of a Meeting Type](#) on page 23.

Users do not enable cascading when creating meetings. This is performed transparently by Scopia Management. Its sophisticated cascading algorithms enable administrators to customize the priority given to cascading in a distributed topology.

The maximum supported number of participants in a single videoconference is 270 for both the centralized and distributed MCU deployment.

There are a number of factors that might influence when the system chooses to cascade to a different MCU. For example, if the maximum bandwidth threshold is breached, the system would attempt cascading with a different MCU.

! Important:

- Telepresence endpoints in cascaded meetings must always connect to the master MCU.

There is a limitation when cascading a Scopia Elite MCU with an older Scopia MCU. The older Scopia MCU behaves as a single endpoint, not an MCU.

You can customize the cascading priorities in Scopia Management in a number of ways:

- Default to using a local MCU first, and only cascade conferences if required.
- Prioritize cascading wherever possible, to keep bandwidth costs to an absolute minimum.
- Avoid cascading as often as possible.

For more information on implementing cascading in Scopia Management, see *Administrator Guide for Scopia Management*.

About the Capacity of the MCU

The MCU's capacity is measured in terms of the maximum number of simultaneous connections to a videoconference supported by this device.

The impact of a connection on the MCU's capacity depends on the bandwidth of the connection, which in turn is dependent on the resolution and frame rate of that connection. Therefore the same meeting can support a mix of HD and SD connections.

For example, a connection at 1080p at 30fps or 720p at 60fps uses half the capacity of a 1080p connection at 60fps. Similarly, a connection at 480p at 30fps uses a quarter of the resources of a 1080p connection at 30fps, or one-eighth of the resources of a 1080p 60fps connection.

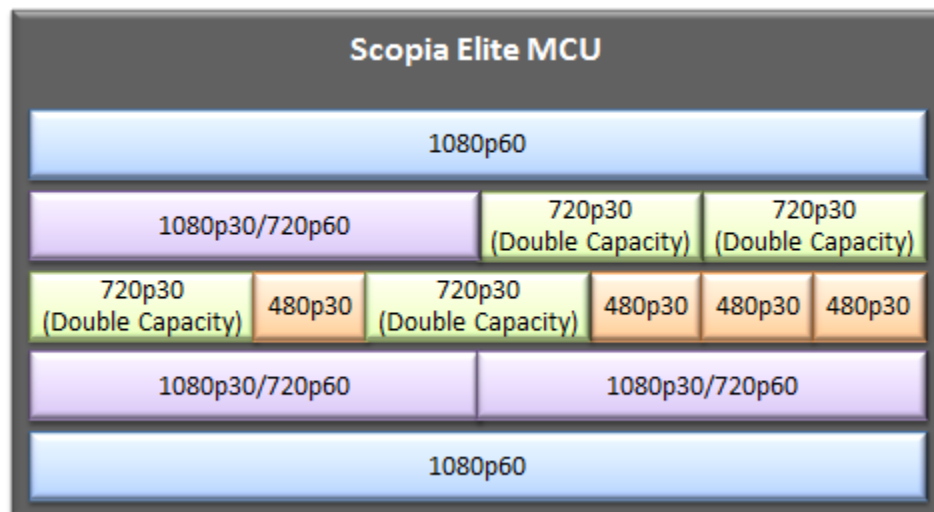


Figure 4: A connection uses its proportion of resources on the MCU

! Important:

To enable connections at 720p at 30fps to use half the capacity of a 1080p 30fps connection, install the Double Capacity license. For more information, see [Adding a License to the MCU](#) on page 17.

The following table details the number of simultaneous connections available for each of the devices when all the connections have the same video resolution and frame rate.

Table 2: Simultaneous connections available at different video quality settings

Scopia Elite 6000 Series MCU Model	1080p at 60fps	1080p at 30fps, 720p at 60fps, 720p at 30fps (no double capacity license)	720p at 30fps (with double capacity license)	480p at 30fps
Scopia Elite MCU 6105	3 connections	5 connections	10 connections	20 connections
Scopia Elite MCU 6110	5 connections	10 connections	20 connections	40 connections
Scopia Elite MCU 6120	10 connections	20 connections	40 connections	80 connections
Scopia Elite MCU 6140	20 connections	40 connections	80 connections	160 connections

If you want to limit the resolution and frame rate of all connections to a meeting, define a meeting type (MCU service) in the MCU and place the limit there. For more information, see [Configuring a New MCU Meeting Type](#) on page 19. Alternatively, you can limit the bandwidth using the global bandwidth policies in Scopia Management.

Ports to Open for the Scopia Elite 6000 Series MCU

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

- If you are opening ports that are both in and out of the Scopia Elite 6000 Series MCU, see [Table 3: Bidirectional Ports to Open on the Scopia Elite 6000 Series MCU](#) on page 15.
- If you are opening ports inbound to the Scopia Elite 6000 Series MCU, see [Table 4: Inbound Ports to Open to the Scopia Elite 6000 Series MCU](#) on page 16.

Important:

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

Table 3: Bidirectional Ports to Open on the Scopia Elite 6000 Series MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
1024-1324	H.245 (TCP)	Any H.323 device	Enables H.245 signaling	Cannot connect H.323 calls	Mandatory To configure, see Configuring the TCP Port Range for H.245 on the Scopia Elite MCU on page 51
1719	RAS (UDP)	H.323 gatekeeper	Enables RAS signaling	Cannot communicate with H.323 gatekeeper	Mandatory To configure, see Configuring the UDP Port for RAS on the Scopia Elite MCU on page 53 and Configuring the UDP Port for the Gatekeeper on the Scopia Elite MCU on page 54
1720	Q.931 (TCP)	Any H.323 device	Enables Q.931 signaling	Cannot connect H.323 calls	Mandatory To configure, see Configuring the TCP Port Q.931 on the Scopia Elite MCU on page 55
3336	XML (TCP)	Conference Control web client endpoint, Scopia Management, or third-party controlling applications	Enables you to manage the MCU via the XML API	Cannot use MCU Conference Control web user interface. Cannot use XML API to control MCU.	Mandatory if deployed with Scopia Management
3337	XML (TCP)	Other MCUs	Enables use of MCU Cascading XML API	Cannot cascade between two MCUs	Mandatory if multiple MCUs are deployed with Scopia Management
3338	XML (TCP)	Scopia Management, or third-party configuration applications	Enables you to configure the MCU via the XML API	Cannot configure MCU via the XML API	Mandatory if deployed with Scopia Management
3400-3580	SIP BFCP (TCP)	Any SIP video network device	Enables SIP content sharing	Cannot share SIP contents	Mandatory if using content sharing with SIP over TCP To configure, see Configuring the TCP Port Range for SIP BFCP on the Scopia Elite MCU on page 57

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
5060	SIP (TCP/UDP)	Any SIP video network device	Enables SIP signaling	Cannot connect SIP calls	Mandatory if using SIP over TCP/UDP To configure, see Configuring the TCP/UDP/TLS Port for SIP on the Scopia Elite MCU on page 56
5061	SIP (TLS)	Any SIP video network device	Enables secure SIP signaling	Cannot connect SIP calls over TLS	Mandatory if using SIP over TLS To configure, see Configuring the TCP/UDP/TLS Port for SIP on the Scopia Elite MCU on page 56
12000-13200 16384-16984	RTP/RTCP/SRTP (UDP)	Any H.323 or SIP media-enabled video network device	Enables real-time delivery of video and audio media	Cannot transmit/receive video media streams	Mandatory To configure, see Configuring the UDP Port Ranges for RTP/RTCP on the Scopia Elite MCU on page 50

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

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
21	FTP (TCP)	FTP Server	Enables audio stream recording	Cannot record audio streams	Optional
22	SSH (TCP)	SSH Client	Enables you to view logs	Cannot view logs in real-time (logs are collected on the compact flash card)	Optional
80	HTTP (TCP)	Web client	Provides access to the MCU Administrator and Conference Control web user interfaces; used for software upgrade	Cannot configure MCU	Mandatory if using HTTP To configure, see Configuring the HTTP Port on the Scopia Elite MCU on page 52
443	HTTPS (HTTP over SSL)	Web client	Provides secure access to the MCU Administrator and Conference Control web user interfaces; used for software upgrade	Cannot configure MCU	Mandatory if using HTTPS

Chapter 3 | Maintaining the Scopia Elite MCU

Maintaining the MCU includes tasks like ensuring secure communications, maintaining the hardware chassis performance, user profiles, backup and restore, license management, and standard configurations of the device.

This section includes the following maintenance procedures:

Navigation

- [Adding a License to the MCU](#) on page 17
- [Configuring a New MCU Meeting Type](#) on page 19
- [Regulating Bandwidth Usage of a Meeting Type](#) on page 23
- [Applying a Meeting Type to a Videoconference](#) on page 25
- [Configuring the Auto-Attendant Service](#) on page 26
- [Securing MCU and Scopia Management Connection with TLS](#) on page 27
- [Configuring Security Access Levels for the Scopia Elite MCU](#) on page 33
- [Configuring IP Separation on the MCU](#) on page 34
- [Managing Scopia Elite MCU User Profiles](#) on page 38
- [Adding a Power Supply Unit to the MCU](#) on page 41
- [Removing a Power Supply Unit from the MCU](#) on page 43
- [Backing Up Your Scopia Elite MCU Configuration](#) on page 45
- [Restoring Your Scopia Elite MCU Configuration](#) on page 45
- [Upgrading Scopia Elite 6000 Series MCU Software](#) on page 46
- [Restoring a Previous Software Version](#) on page 48
- [Configuring Ports on All Models of the Scopia Elite MCU](#) on page 50
- [Customizing the Logo Displayed in MCU Conferences](#) on page 58
- [Customizing MCU Audio Messages](#) on page 60

Adding a License to the MCU

About this task

Your MCU comes with several licenses pre-installed.

You can purchase and install additional license options, for example the option to double port capacity when you set the video quality to 720p with 30 frames per second (see [About the Capacity of the MCU](#) on page 13).

This section details how to incorporate a purchased license into your MCU.

Procedure

1. Open the customer letter you received when you purchased the license. Locate the new product key in the letter.
2. Access the MCU administrator web interface.
3. Make a note of the device's serial number, located in the center right pane of the main screen (Figure 5: Locating the serial number of the MCU on page 18).

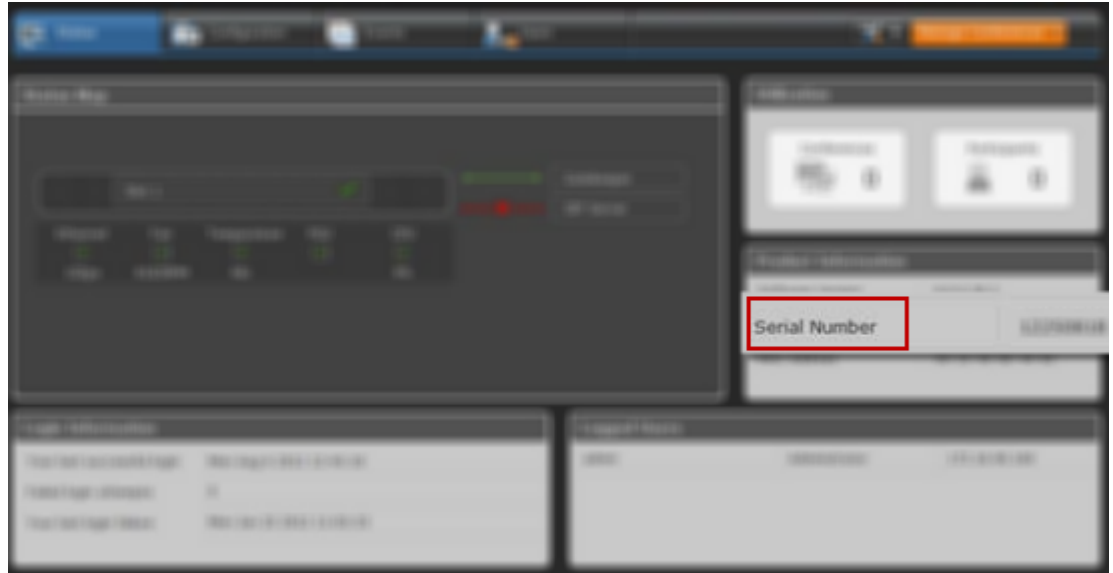


Figure 5: Locating the serial number of the MCU

4. Navigate to the licensing portal at <http://licensing.radvision.com>
5. Enter the product key from your customer letter.
6. Enter the serial number of the device.
7. Generate your new license key.
8. Return to the MCU screen.
9. Select **Maintenance**  > **Licensing and Registration**.
The **Licensing and Registration** window opens.

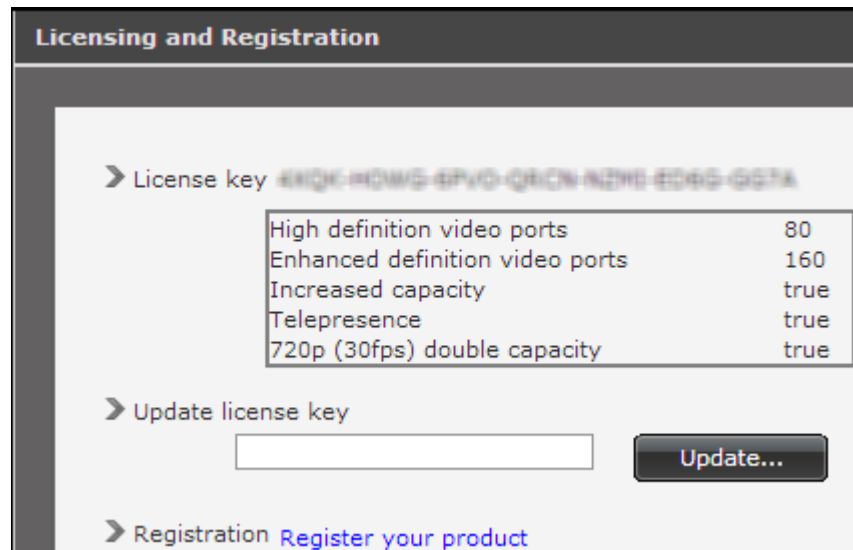


Figure 6: Licensing and Registration Window

10. Enter the new license key in the **Update license key** field.
11. Select **Update**.
12. Continue by enabling the feature activated by this license. For example, to enable 720p at 30fps, see [About the Capacity of the MCU](#) on page 13.

Configuring a New MCU Meeting Type

About this task

Meeting types (also known as MCU services) are meeting templates which determine the core characteristics of a meeting. For example, they determine if the meeting is audio only or audio and video, they determine the default video layout, the type of encryption, PIN protection and many other features. Meeting types are created in the MCU. You can invoke a meeting type by dialing its prefix in front of the meeting ID.

In organizations deploying multiple MCUs, Scopia Management enables you to define meeting types in one MCU, and then sync this device with the other MCUs in your deployment. For more information, see *Administrator Guide for Scopia Management*.

To define a meeting type, choose a unique dial prefix in the organization which would invoke this type of meeting, give it a descriptive name, and then define its parameters.

Procedure

1. Access the MCU administrator web interface.
2. Select **Configuration > Conferences**, then select **Add new service** ([Figure 7: Defining a new meeting type](#) on page 20).

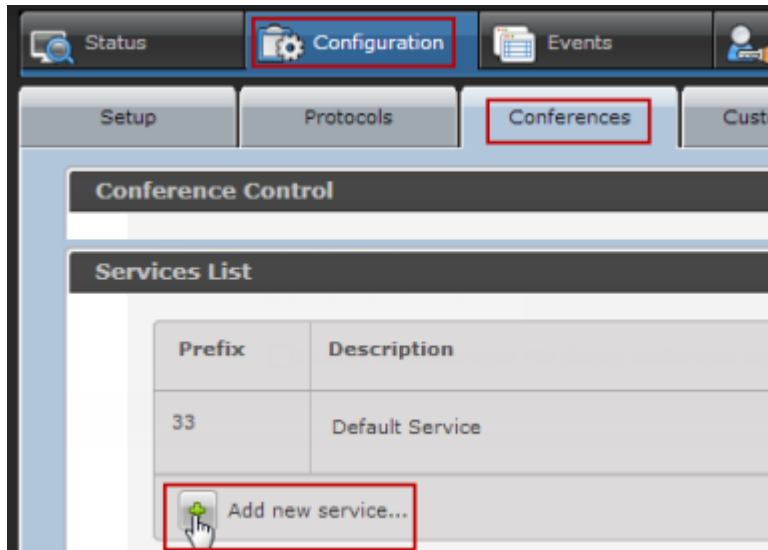


Figure 7: Defining a new meeting type

3. Enter a unique dial prefix to invoke this meeting type ([Figure 8: Defining basic properties of a meeting type](#) on page 20).

This prefix precedes the meeting ID when dialling the videoconferencing number. For example if the meeting ID is 9495, and the new service dial prefix is 88, the meeting ID to give participants is 889495.

4. Enter a description of the new meeting type ([Figure 8: Defining basic properties of a meeting type](#) on page 20).
5. Select **Audio only** if the meeting type is audio only, thereby gaining the largest savings on bandwidth ([Figure 8: Defining basic properties of a meeting type](#) on page 20).
6. Select **Switched video** to conserve bandwidth for this service by viewing only one participant at a time ([Figure 8: Defining basic properties of a meeting type](#) on page 20).

For more information, see [Regulating Bandwidth Usage of a Meeting Type](#) on page 23.

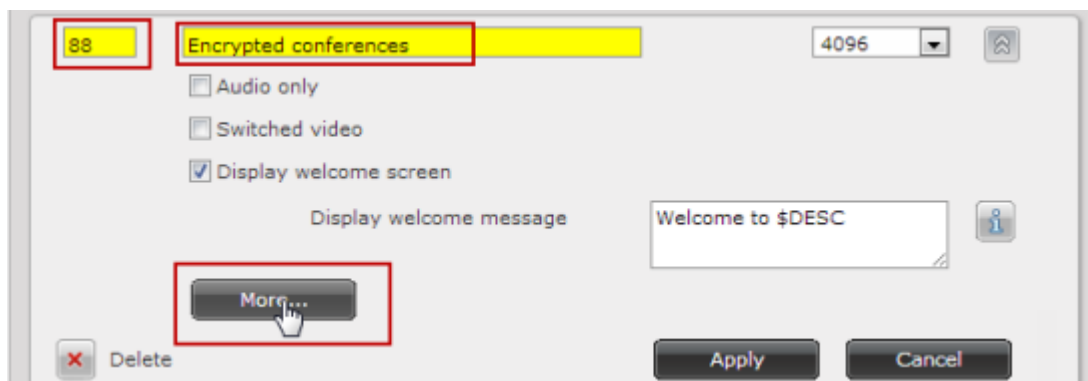


Figure 8: Defining basic properties of a meeting type

7. Select **More** to define more parameters of this meeting type ([Figure 8: Defining basic properties of a meeting type](#) on page 20).
8. Enter the following fields as detailed in [Table 5: Detailed properties of a meeting type](#) on page 21.

> Default layout

☒ Dynamically adjusted

Max displayed streams

☐ Static:

 Select

☒ Enable personal layout

☒ Display participant names

☒ Constantly

☐ On location changes for seconds

> Video quality preference

☒ Sharpness

☐ Motion

☒ Enable presentation view

Presentation video codec

☐ Encryption:

Encryption mode

☐ Auto mute joining participants

☒ Auto mute first joining participant

☐ Automatically reconnect dropped participants

☐ Force conference PIN protection

☐ Ask for conference PIN on invite

Figure 9: Defining detailed properties of a meeting type

Table 5: Detailed properties of a meeting type

Field Name	Description
Default layout	Determines the default video layout of this meeting type. Choose from the following values: • Dynamically adjusted changes the video layout automatically based on the number of participants in the videoconference. Choose from Max displayed streams to optionally limit the maximum number of participants simultaneously visible in the same layout. The default value is the device's maximum. • Static enables you to fix the default video layout of this meeting type.

Field Name	Description
Enable personal layout	Enables moderators to personalize any participant's video layout to be different from others in the same videoconference. For more information on this functionality within the MCU, see Personalizing Video Layouts for Participants on page 69.
Display participant names	Determines whether the video layout also displays the name under each participant by default. Choose from the following values: • Constantly always displays the name for the duration of the meeting. • On location changes for displays the name only for the first few seconds and refreshes whenever the location of the image in the video layout changes. For more information on performing this on the MCU for a single meeting, see Displaying Participant Names in the Video Layout on page 77.
Video quality preference	Determines whether the priority of the MCU processor power should be devoted more to image sharpness or speedy rendering of moving images.
Enable presentation view	Determines whether this type of meeting can include presentations (data content) alongside the other streams. Choose the protocol which is supported by all endpoints participating in the videoconference: • Auto automatically selects the data sharing protocol supported by all endpoints in the videoconference. • H.264 forces data sharing to take place over H.264, supported by newer endpoints for better compression and higher resolutions. • H.263 forces data sharing to take place over H.263 for legacy endpoints which do not support H.264.
Encryption	Specifies whether the meeting is encrypted, and the type of encryption used. Choose from: • Best effort indicates the system will attempt to encrypt the meeting transmissions, provided the encryption is supported by the endpoint. If an endpoint does not support encrypted media, transmissions to that endpoint are sent unencrypted. • Strong encryption (AES-128) required indicates the system demands AES-128 strong encryption. Endpoints not supporting this standard would not be able to connect to meetings of this type.  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.

Field Name	Description
Auto mute joining participants	Automatically mutes the sound of joining participants. This is helpful in eliminating background noise, like clicking keyboards and other distractions from an endpoint.
Auto mute first joining participant	When enabled, all conference participants are muted when joining the conference, except for the first participant.
Automatically reconnect dropped participants	The system automatically tries to reestablish a link if the connection to one of the endpoints has been dropped.
Force conference PIN protection	Determines whether meetings of this type always require participants to enter a PIN before gaining access to the meeting.
Ask for conference PIN on invite	Moderators setting up a meeting of this type are required to enter the meeting PIN to allow them to send invitations.

Regulating Bandwidth Usage of a Meeting Type

About this task

Depending on your network capacity, you may need to adjust bandwidth usage by defining how much bandwidth each meeting type requires. Meeting types (also known as MCU services) are meeting templates which determine the core characteristics of a meeting.

Then you can activate a meeting type by dialing its prefix before the conference number.

Examples of bandwidth limitation are:

- Limiting the maximum bit rate of a meeting type.
- Limiting the meeting type to audio only.
- Limiting video layouts to support showing only one participant's image at a time.

Procedure

1. Select **Configuration**.
2. Select **Conferences**.
3. Locate the **Services List** section.

Services List			
Prefix	Description	Max call rate (Kbps)	Review
7788	audio only	64	
9966	Default Service [Auto attendant service]	2048	
 Add new service...			

Figure 10: Service List Section of the Conferences Tab

4. Select **Review**  for a meeting type.
5. Select the required value from the list under **Max call rate (Kbps)**.

Prefix	Description	Max call rate (Kbps)	Rev
9966	Default Service Set as the Auto attendant service ☐ Audio only ☐ Switched video ☐ Display welcome screen Display welcome message: Welcome to \$DESC More... Delete	4096 64 128 192 256 320 384 512 768 936 1000 1024 1288 1472 1500 2048 2250 3072 4096 5120 6144	
33	Default Service [Auto attendant service]		

Figure 11: Service Settings Section

6. Select **Audio only** to conserve bandwidth by making the service audio-only.
7. Select **Switched video** to conserve bandwidth for this service by viewing only one participant at a time.

Switching is the process of redirecting video as-is without transcoding, so you see only one endpoint's image at a time, usually the active speaker, without any video layouts or continuous presence (CP). Using video switching increases the port capacity of the MCU by four times.

! Important:

Use switched video only when all endpoints participating in the videoconference support the same resolution. If a network experiences high packet loss, switched video might not be displayed properly for all endpoints in the videoconference.

By default, all videoconferences display video in Continuous Presence mode, which supports all layouts and endpoints with various resolutions. Continuous Presence video is processed by the MCU.

8. Select **Apply**.

Applying a Meeting Type to a Videoconference

About this task

You can apply a meeting type (service) to a videoconference by dialing the specified prefix followed by the videoconference number.

You can edit a service prefix if needed.

Procedure

1. Select **Configuration**.
2. Select **Conferences**.
3. Locate the **Services List** section.



Prefix	Description	Max call rate (Kbps)	Review
7788	audio only	64	
9966	Default Service [Auto attendant service]	2048	

 Add new service...

Figure 12: Service List Section of the Conferences Tab

4. Select the **Review**  button for the service you want to configure.

5. Change the dial prefix for this service by editing the numeric field to the left of the service description.
6. Select **Apply**.

Configuring the Auto-Attendant Service

About this task

The auto-attendant service allows MCU users to create or join a conference even if they do not know the MCU service number or the meeting ID number. The auto-attendant number serves as a preconfigured number a user can dial to access the MCU to either create a new conference or join a conference currently hosted at this MCU.

Before you begin

Procedure

1. Select **Configuration**.
2. Select **Conferences**.
3. Locate the **Services List** section.

Services List			
Prefix	Description	Max call rate (Kbps)	Review
7788	audio only	64	
9966	Default Service [Auto attendant service]	2048	
 Add new service...			

Figure 13: Service List Section of the Conferences Tab

4. Select **Review**  for the service you want to use as the auto attendant service.
5. Select the **Set as the Auto attendant service** link.

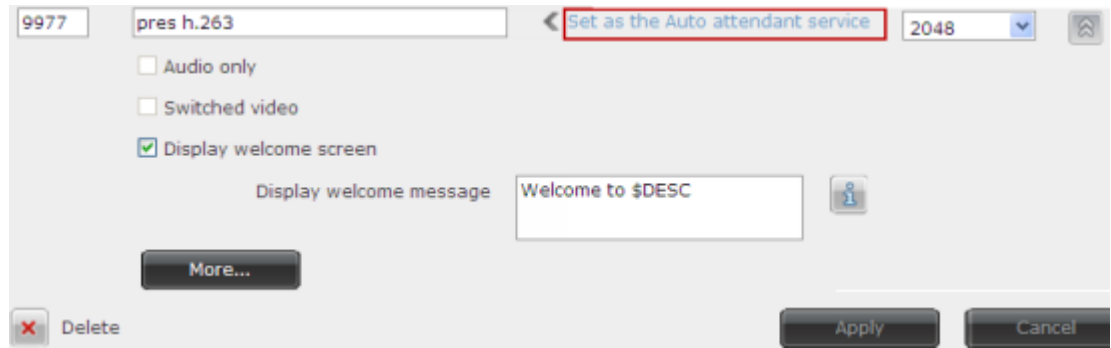


Figure 14: Service Setting Section

6. Select **Apply**.

Securing MCU and Scopia Management Connection with TLS

TLS is a standard method of authentication and encryption of SIP application signalling, using public-key cryptographic system. To allow a secure connection between the MCU and Scopia Management, the SIP server must be configured to support TLS, and a TLS certificate must be uploaded to the MCU, to provide TLS public and private keys for an encrypted network connection.

! 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.

Navigation

- [Securing MCU with TLS in a SIP Environment](#) on page 27
- [Uploading TLS Certificates to the MCU](#) on page 28

Securing MCU with TLS in a SIP Environment

About this task

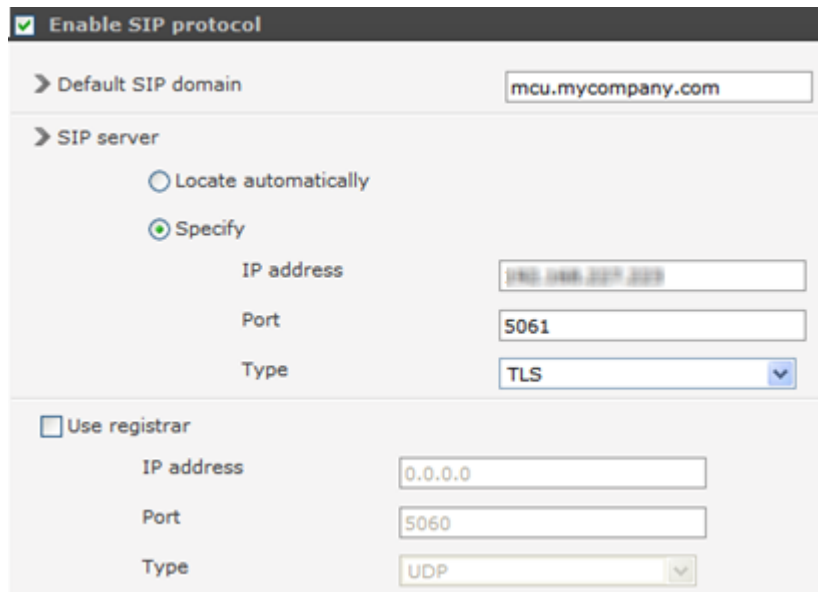
The first step to allow a secure connection between MCU and Scopia Management is to enable TLS support on the MCU SIP server. Once MCU SIP server is TLS enabled, a certificate must be uploaded to the MCU to provide identification and encryption keys (see [Uploading TLS Certificates to the MCU](#) on page 28).

! Important:

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

Procedure

1. Log in to the MCU.
2. Select **Configuration > Protocols > Enable SIP Protocol**.
3. Select **Specify**.
4. Set the **IP address** as the IP address of the Scopia Management server.
5. Set **Port** to the same port defined in Scopia Management. The default value is **5061**.
6. Set **Type** as **TLS**.



The screenshot shows the 'Enable SIP protocol' configuration window. The title bar indicates the window is titled 'Enable SIP protocol'. The main content area is divided into two sections. The first section, 'SIP server', has a radio button for 'Specify' selected. Below this, there are three fields: 'IP address' with the value '192.168.222.222', 'Port' with the value '5061', and 'Type' with a dropdown menu set to 'TLS'. The second section, 'Use registrar', has an unchecked checkbox. Below it, there are three fields: 'IP address' with the value '0.0.0.0', 'Port' with the value '5060', and 'Type' with a dropdown menu set to 'UDP'.

Figure 15: Enabling the SIP Protocol on the MCU

7. Restart the MCU.

Uploading TLS Certificates to the MCU

About this task

TLS certificates, issued by a trusted Certificate Authority (CA) contains the server's public encryption keys, that are used over the network to ensure authentication and encryption of the network connection.

! Important:

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

Procedure

1. Log in to the MCU.
2. Select **Configuration**.
3. Select **Manage** in the **Security** section.

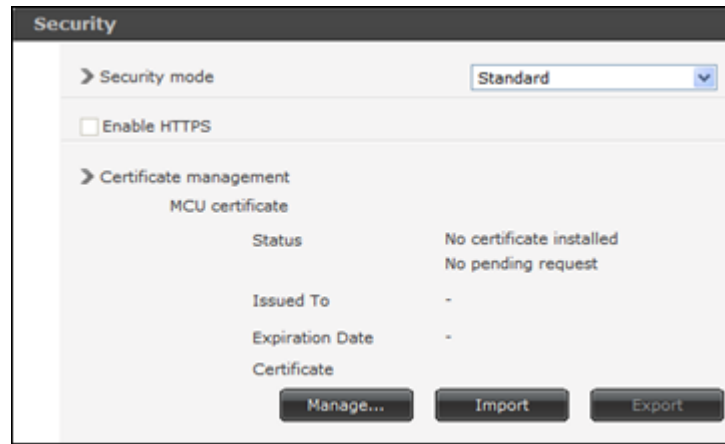


Figure 16: Security Section

4. Select **Create a new certificate request**. For example:

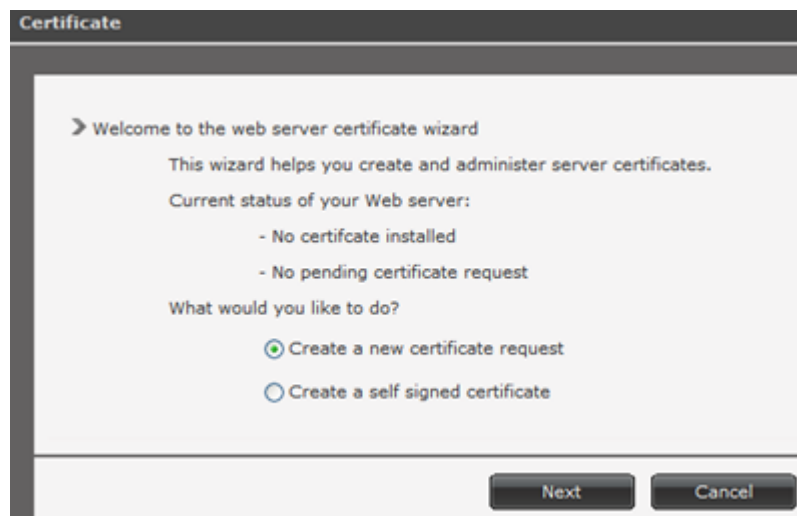


Figure 17: Create New Certificate Request

5. Select **Next**.
6. Enter the **Organization**, **Organizational Unit**, **Email** and **Common name**. For example:
 - **Organization:** *Company_Name*
 - **Organizational Unit:** *IT*
 - **Email:** *joe@companyname.com*
 - **Common name:** *video.mycompany.com* (unique for each MCU)

> **Organizational Information**

Your certificate must include information about your organization distinguishes it from other organizations.

Type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

Organization:

Organizational Unit:

Email:

The common name is the fully qualified domain name e.g video.mycompany.com. If the common name changes you will need to obtain new certificate

Common name:

Figure 18: Organization Details

7. Select **Next**.
 8. Enter the geographical information as required. For example:
 - **Country/Region:** *US*
 - **State/Province:** *New York*
 - **City/Locality:** *New York*
 9. Select **Next**.
- The **Certificate Request Summary** is displayed.

> **Certificate Request Summary**

You have chosen to create certificate request.

Your request contains the following information:

Issued To:

Country/Region:

State/Province:

City/Locality:

Organization:

Organizational Unit:

To generate a certificate request, click Next.

Figure 19: Certificate Request Summary

10. To generate a certificate request, select **Next**. Copy certificate request text in text area and paste it to a file (for example, *mcu_ca_request.txt*). Then select **Finish**.



Figure 20: Save Certificate Request

11. Submit this file to your Certification Authority (CA) by e-mail or any other method supported by your organization for your Enterprise CA.

You will receive a signed certificate from the CA, for example and the root certificate, for example `ca_root.cert`.

To install the signed certificate:

12. Select **Manage**.
13. Select **Process the pending request and install the certificate**.

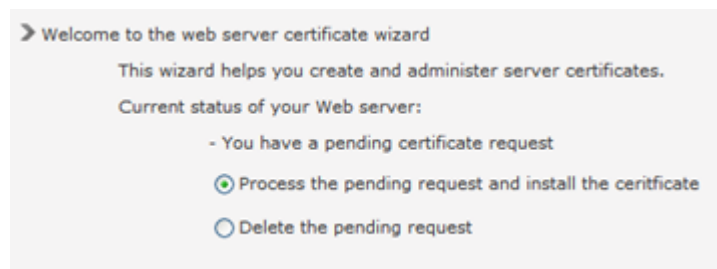


Figure 21: Certificate Status

14. Select **Next**.
15. Open the signed certificate, and copy-paste the content of the signed certificate.

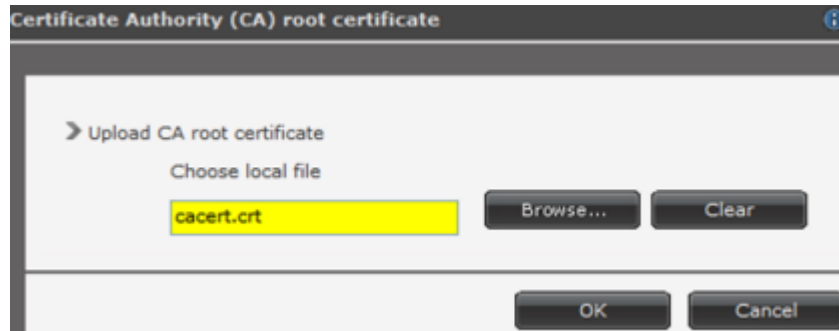


Figure 24: Browse for the CA Root Certificate

20. Select **OK**.
21. Copy the certificates to the B2BUA's CA directory (for example: *mcu_ca.cert* and *ca_root.cert*).

Configuring Security Access Levels for the Scopia Elite MCU

About this task

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

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

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

❗ Important:

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

❗ Important:

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

Procedure

1. Access the MCU security settings by selecting **Configuration > Setup**.
2. Locate the **Security** section.

3. Select the access level from the **Security Mode** list (see [Figure 25: Security Access Level Settings](#) on page 34). [Table 6: MCU Security Access Levels](#) on page 34 lists the protocol status when each security access level is applied.

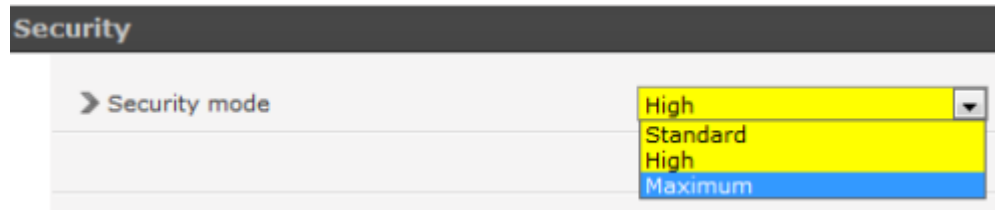


Figure 25: Security Access Level Settings

Table 6: MCU Security Access Levels

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

4. Select **Apply**.

Configuring IP Separation on the MCU

About this task

You can configure IP separation on the MCU using both network ports (dual-NIC), improving security by enabling the management data to be on a separate subnet from the media and signaling.

Separating these types of data on different subnets improves security because management data typically remains on subnets within the enterprise, while the media of video calls is often required to traverse firewalls and reach endpoints outside the enterprise.

Management refers to the administration messages sent between components of the Scopia Solution as they manage and synchronize data between them. Management also includes front-end browser interfaces configuring server settings on the server. Management messages are usually transmitted via protocols like HTTP, SNMP, FTP or XML. For example, Scopia Management uses management messages to monitor the activities of an MCU, or when it authorizes the MCU to allow a call to proceed.

Media refers to the live audio, video and shared data streams sent during a call. The shared data stream, like a presentation, is also known as dual video. Far end camera control (FECC) is another example of information carried on the data stream. Media is transmitted via the RTP and RTCP protocols in both SIP and H.323 calls.

Signaling, also known as call control, sets up, manages and ends a connection or call. These messages include the authorization to make the call, checking bandwidth, resolving endpoint addresses, and routing the call through different servers. Signaling is transmitted via the H.225.0/Q.931 and

H.225.0/RAS protocols in H.323 calls, or by the SIP headers in SIP calls. Signaling occurs before the control aspect of call setup.

Before you begin

- Configure the MCU's management IP address before connecting to the network, as explained in *Installation Guide for Scopia Elite MCU*.
- Make sure no videoconferences are running on the MCU, as you need to restart it at the end of the procedure.

Procedure

1. Connect the network cable of the management subnet to the left ethernet port.

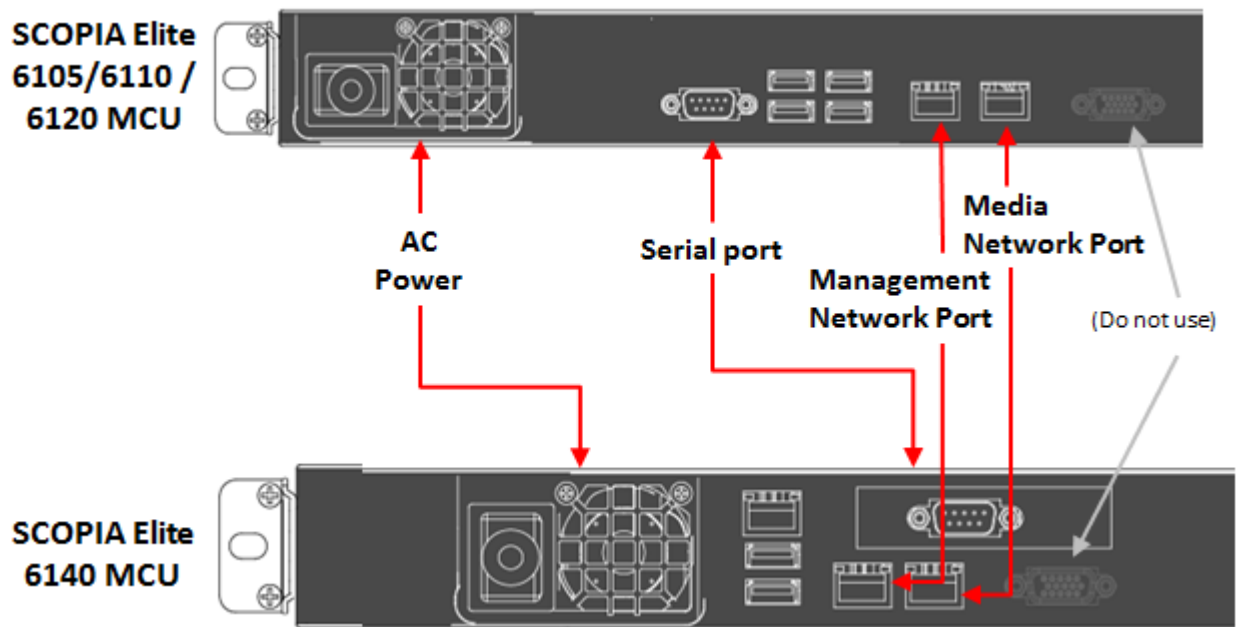


Figure 26: The MCU management and media connections

! Important:

Do *not* connect the network cable of the media subnet until you restart the MCU at the end of this procedure.

2. Access the MCU administrator web interface using the management IP you configured via serial cable (*Installation Guide for Scopia Elite MCU*).
3. Select the **Configuration**  **Configuration** tab.
4. Select the **Advanced IP Configuration** check box to expand that section of the page [Figure 27: Configuring IP separation with two network connections](#) on page 36).

Network ☒ **Advanced IP Configuration**

> **Management Interface**

Primary IP address: 192.168.0.10

Router IP: 192.168.0.254

Subnet mask: 255.255.255.0

> **Media & Signaling Interface**

Primary IP address: 10.0.0.1

Router IP: 192.168.0.254

Subnet mask: 255.255.0.0

> **DNS suffix**

> **DNS server 1**

> **DNS server 2**: 0.0.0.0

> **Port settings**: Auto (Up to 1 Gbps/Full Du)

[More](#)

Figure 27: Configuring IP separation with two network connections

5. Configure the IP addresses of each interface ([Table 7: Configuring the IP addresses of each network interface](#) on page 36).

Table 7: Configuring the IP addresses of each network interface

Field	Description
Management Interface > IP address	IP address of the MCU management interface (left ethernet port) as configured via serial port. This is the IP used to access this web interface.
Management Interface > Router IP	IP address of the management subnet router
Management Interface > Subnet mask	IP address of the management subnet mask
Media & Signaling Interface > IP address	IP address of the MCU media and signaling interface (right ethernet port)
Media & Signaling Interface > Router IP	IP address of the media and signaling subnet router
Media & Signaling Interface > Subnet mask	IP address of the media and signaling subnet mask

6. Select **Apply** at the bottom of the page.
7. Select **Yes** to restart the MCU.
8. Connect the network cable of the media subnet cable to the right ethernet port ([Figure 26: The MCU management and media connections](#) on page 35).
9. (Optional) Depending on your deployment, you may need to access the MCU management interface from another network.

For example, if your MCU is located on network 123.x.x.x and your browser is on the same network (123.x.x.x), you can access the administrator web interface to reach this web page and configure IP separation of management and media as detailed in this procedure, where management communications stay in this network (123.x.x.x) while media is routed to a different network: 456.x.x.x (see [Figure 28: Example of additional management network](#) on page 37). However, if you need management access from another branch with its own network, for example 789.x.x.x, you can configure the 789.x.x.x management traffic to be routed via 123.x.x.x, and then onwards to 789.x.x.x (see [Figure 28: Example of additional management network](#) on page 37).

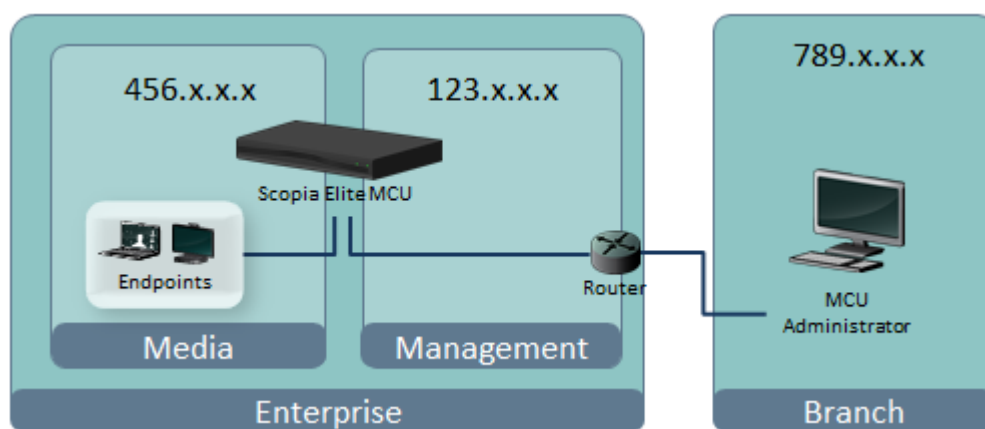


Figure 28: Example of additional management network

Use the following steps to configure an additional management network:

- a. Select **More** at the bottom of the expanded section ([Figure 27: Configuring IP separation with two network connections](#) on page 36).
The **Additional Management Networks** section opens.
- b. Select **Add Management Network**.
- c. Configure the access to the MCU management subnet ([Figure 29: Adding a new network for management access](#) on page 38 and [Table 8: Configuring the additional network interfaces](#) on page 38).

Figure 29: Adding a new network for management access

Table 8: Configuring the additional network interfaces

Field	Description
IP address	IP address of the additional management network
Subnet mask	IP address of the additional management subnet mask

d. Select **OK**.

Managing Scopia Elite MCU User Profiles

The MCU has two types of users:

- Administrators (up to 10 users)
- Operators (up to 50 users).

As an administrator, you have the following privileges:

- Full access to the MCU administrator interface.
- Full Operator-level access to the Conference Control interface.
- Full access to the Manage Conferences interface.
- SSH access to the MCU.
- Manage user profiles.

As an operator, your privileges are mostly limited to the Conference Control interface.

! Important:

You can configure meetings from the MCU's Conference Control interface only in standalone mode, when the MCU is not part of a Scopia Management deployment. In Scopia Management deployments, the conference control is managed by Scopia Management.

You can:

- View details of ongoing videoconferences hosted on the MCU and to cascaded conferences involving this MCU.
- Create a new videoconference.
- Moderate videoconferences.
- Invite participants to a videoconference.

Navigation

- [Adding a User Profile](#) on page 39
- [Changing a User Password](#) on page 40
- [Deleting a User Profile](#) on page 40

Adding a User Profile

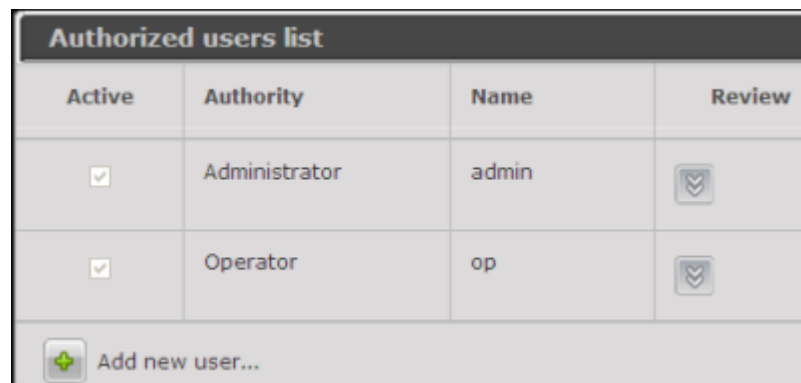
About this task

MCU administrators can create a new user on the MCU.

You can create up to 10 administrator profiles and up to 50 operator profiles.

Procedure

1. Access the MCU administrator web interface.
2. Select **Users** .



Authorized users list			
Active	Authority	Name	Review
☒	Administrator	admin	
☒	Operator	op	
 Add new user...			

Figure 30: Authorized Users List

3. Select **Add new user**.



The dialog box for creating or modifying a user profile. It features a green checkmark icon in the top left corner. A dropdown menu is set to 'Administrator'. Below it are three input fields labeled 'Password', 'Confirm Password', and an empty field. At the bottom left is a red 'X' icon with the text 'Delete'. At the bottom right are 'Apply' and 'Cancel' buttons. A small icon with an upward arrow is in the top right corner.

Figure 31: User Profile Section

4. Choose **Administrator** or **Operator** as the type of user.
5. Enter the new username.
6. Enter a password and its confirmation.
7. Select **Apply**.

Changing a User Password

About this task

Only administrators can change a password.

The MCU comes with two preconfigured users: an administrator and an operator. The password for both preconfigured users is 'password'. We highly recommend that you change the default user password for security.

You can change a user password at any time.

Procedure

1. Access the MCU administrator web interface.
2. Select **Users** .
3. Select the **Review** button  for the user profile you want to modify.
4. Enter the new password in the **Password** and the **Confirm Password** fields.
5. Select **Apply**.

Deleting a User Profile

About this task

Only administrators can delete user profiles.

You can delete user profiles at any time.

Procedure

1. Access the MCU administrator web interface.
2. Select **Users** .

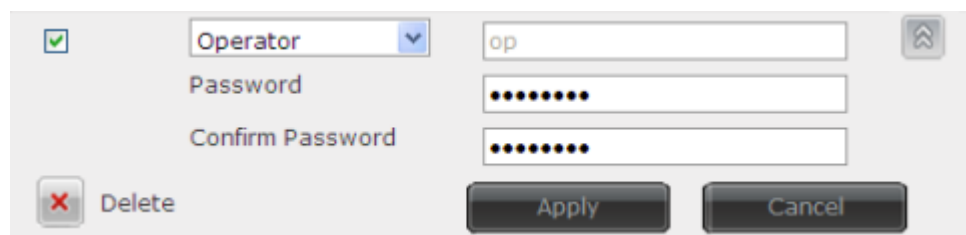


Authorized users list			
Active	Authority	Name	Review
☒	Administrator	admin	
☒	Operator	op	

 Add new user...

Figure 32: Authorized Users List

3. Select the **Review** button  for the user profile you want to remove.



☒ Operator  op 

Password

Confirm Password

 Delete Apply Cancel

Figure 33: User Profile Section

4. Select **Delete**.
5. Select **Yes** in the message that appears.
The user profile is removed from the authorized users list.

Adding a Power Supply Unit to the MCU

About this task

This section details how to set up an additional power supply unit (PSU) of the Scopia Elite MCU 6140, which can house two PSUs.

! Important:

This applies to the 6140 model only. For details of replacing a PSU of the Scopia Elite 5200 Series MCU, see the *Administrator Guide of Scopia Elite 5200 Series MCU version 7.7*.

If one of the PSUs fails, the remaining PSU takes the full load of the system to enable continued operation without interruption. PSUs can be hot-swapped, enabling you to replace the power unit without powering down the device.

To remove an existing PSU from the device, see [Removing a Power Supply Unit from the MCU](#) on page 43.

Procedure

1. Remove the cover of the PSU slot if it is there.

The MCU is shipped with only one PSU fitted, while the second slot is covered by a metal grid. Remove the grid by unscrewing the two screws, one above and one below the device.

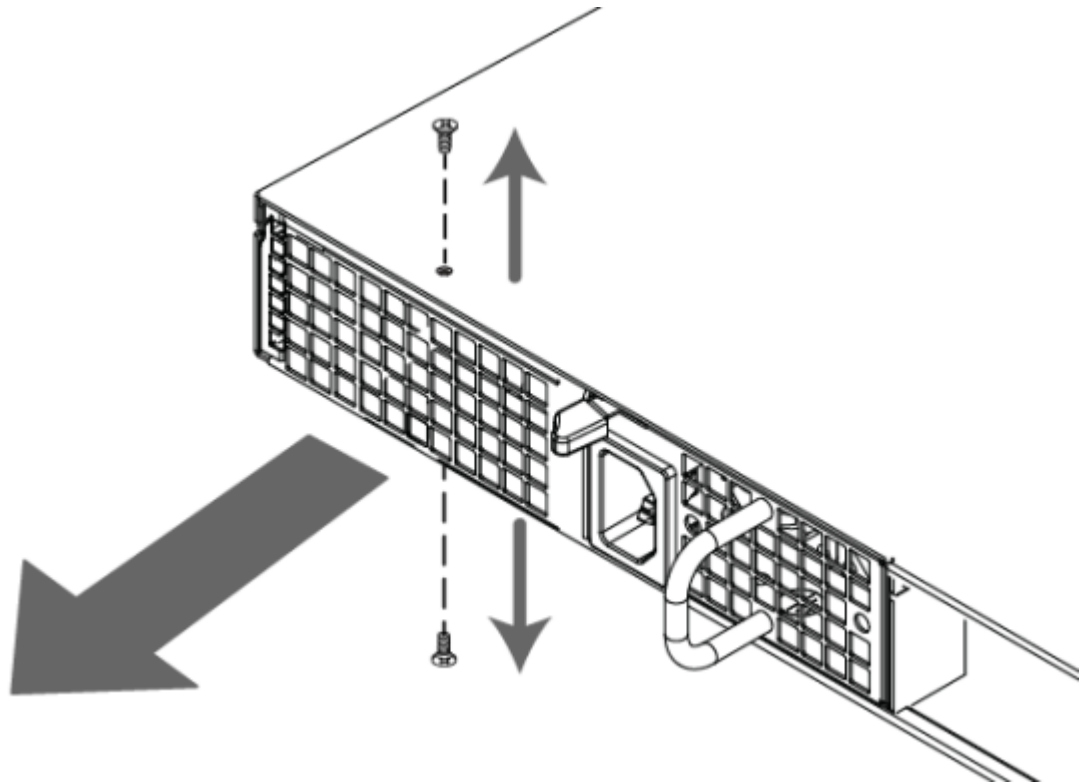


Figure 34: Removing cover of second PSU slot in Scopia Elite MCU 6140

2. Insert the new PSU into position and secure it by pressing it firmly into place until the release tab clicks.

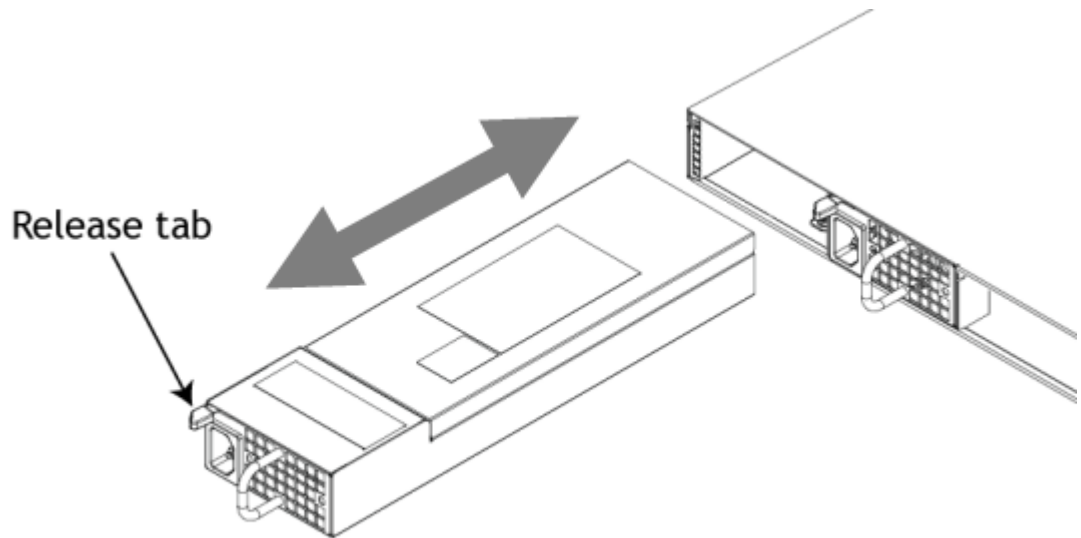


Figure 35: Adding a PSU in Scopia Elite MCU 6140

3. Reconnect the power cord.

Removing a Power Supply Unit from the MCU

About this task

This section details how to remove one of the power supply units (PSUs) from the Scopia Elite MCU 6140, which can house two PSUs.

Important:

This applies to the 6140 model only. For details of replacing a PSU of the Scopia Elite 5200 Series MCU, see the *Administrator Guide of Scopia Elite 5200 Series MCU version 7.7*.

If one of the PSUs fails, the remaining PSU takes the full load of the system to enable continued operation without interruption. PSUs can be hot-swapped, enabling you to replace the power unit without powering down the device.

To add a new PSU, see [Adding a Power Supply Unit to the MCU](#) on page 41.

Procedure

1. Disconnect the AC power cord of that PSU.

! Important:

If a second PSU is actively powering the MCU, this PSU can be removed without powering down the device. However, if the only active PSU is the one you need to replace, first power down the device, then remove the power cord.

2. Push the release tab sideways towards the handle of the PSU to eject the unit from the device.

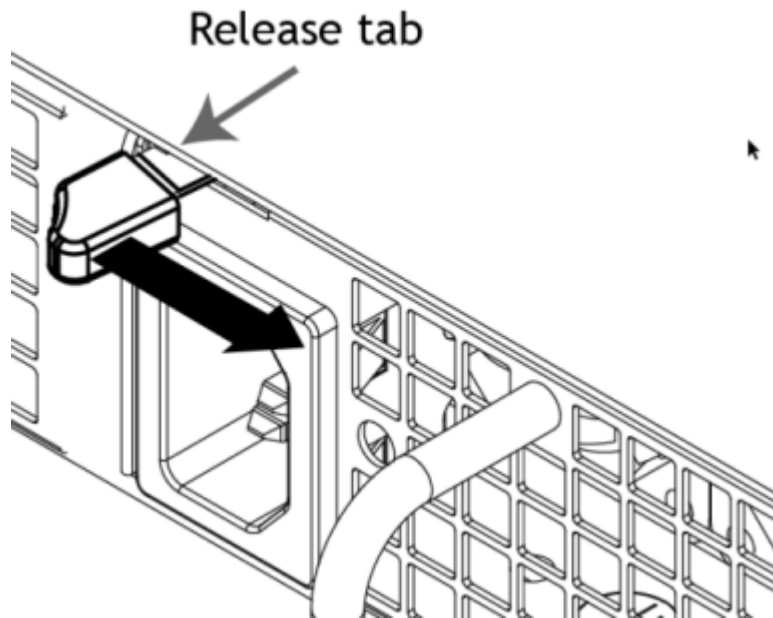


Figure 36: Ejecting the PSU with the release tab

3. Use the PSU handle to remove it from the device.

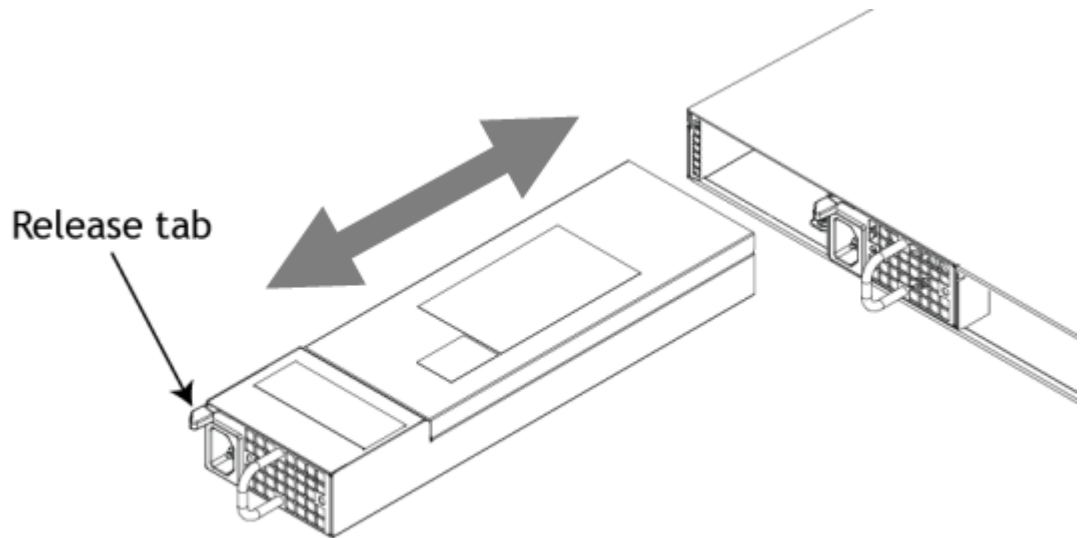


Figure 37: Removing a PSU from the device

Backing Up Your Scopia Elite MCU Configuration

About this task

You can save MCU configuration settings to a file and then export this file to a storage device on your network. You can use the saved configuration file to restore the settings to the current MCU or to configure a similar MCU.

The exported file is a *.zip* file that includes a *.val* file and a *.xml* file.

Procedure

1. Access the MCU administrator web interface.
2. Select  > **Backup configuration**.
3. Save the configuration settings file to your chosen location.
The *.zip* extension is automatically appended to the filename.

Restoring Your Scopia Elite MCU Configuration

About this task

You can import the settings of a saved MCU configuration file from a storage device on your network. You can use the saved configuration file to restore the settings to the current MCU or to configure another MCU.

The imported file is a `.zip` file that includes a `.val` file and a `.xml` file.

Important:

If you are importing a configuration setup from a different MCU that has different login credentials, you will need to enter these new credentials to access the MCU.

Procedure

1. Access the MCU administrator web interface.
 2. Select  > **Restore configuration**.
 3. Select **Browse**.
 4. Navigate to and select the configuration file (`.zip`) you want to import.
 5. Select **Restore**.
 6. Select **Continue** to upload the new configuration settings.

The restore procedure causes all current configuration to be permanently lost.

The system restarts automatically.

All active conferences are disconnected.
 7. Select **OK** to complete the restore procedure.
-

Upgrading Scopia Elite 6000 Series MCU Software

About this task

This section details the software upgrade procedure for the Scopia Elite 6000 Series MCU. You can upgrade the MCU in one of several ways:

- Upgrade via the MCU administrator web interface, by following the steps in this section.
- Remotely upgrade via Scopia Management, where you can centralize all MCU upgrades. For more information, see *the Administrator Guide for SCOPIA Management*.
- Upgrade the device itself by inserting a USB flash drive. Contact your local Radvision representative to receive the upgrade via USB flash drive.

To implement the USB flash drive upgrade, follow the instructions you received with your flash drive.

Upgrading may take up to 40 minutes. The procedure below details how to upgrade via the MCU web interface.

Before you begin

Before starting the upgrade procedure, verify:

- You have backed up the current device configuration (see [Backing Up Your Scopia Elite MCU Configuration](#) on page 45).
- There are no active conferences hosted on the MCU.

Procedure

1. Access the MCU administrator web interface.

2. Select  > **Update software**.

3. Select **Browse** and navigate to the required MCU upgrade package.

A message informs you a temporary license is used for the upgrade. After the upgrade, the license is permanent.

4. Select **OK**.

5. Select **Update**.

The system shuts down for a few minutes and then restarts automatically. All active conferences are disconnected.

6. Select **Continue**.

As soon as the update process has finished, the MCU reboots and reloads with the new software version. The upgrade process keeps the existing configuration and you do not need to import the saved configuration.

7. Verify that the MCU functions properly:

a. From an endpoint dial the MCU IP address.

You access the MCU auto attendant service which plays the video and audio prompts.

b. Select **0** to create a new conference.

c. At the prompt, enter the meeting ID and then #.

The MCU creates a new conference and the Conference window is displayed.

d. Exit the conference by disconnecting the call.

8. Verify the device is ready.

a. Configure this MCU in Scopia Management as explained in *Administrator Guide for Scopia Management*.

b. Take other MCUs offline (if any) to make sure you hold the videoconference on this MCU.

c. From an endpoint dial the IP address (or the Auto-Attendant number if configured).

d. Press **0** to create a new conference.

e. At the prompt, enter the meeting ID followed by #.

The MCU creates the videoconference. If it is successful, the MCU is properly installed and configured.

You can view the videoconference status in these pages:

- The MCU's **Status Map** which shows the connection to Scopia Management and conference use statistics.

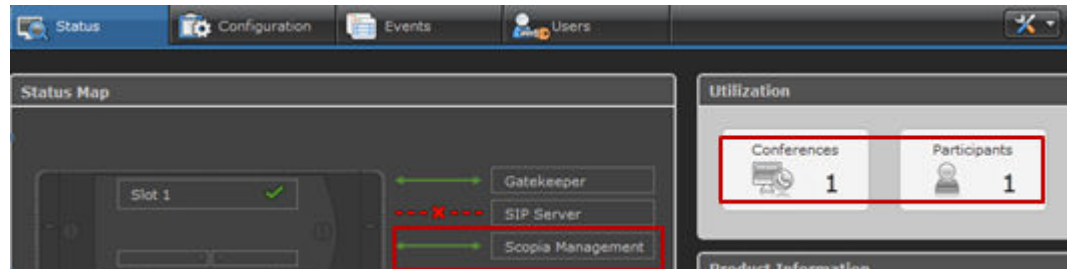


Figure 38: The MCU Status Map

- The Scopia Management **Dashboard** which shows the details of the current videoconference.

ID	Name	Participants	MCU	Terminate
716194	IVR Session	1	MCU230192	X

Figure 39: The Scopia Management Dashboard status

f. Exit the videoconference by disconnecting the call.

Restoring a Previous Software Version

About this task

Perform this procedure to downgrade to the previous MCU software version.

! Important:

You cannot downgrade the Scopia Elite 6000 Series MCU to a version prior to 8.0.

We highly recommend that you contact Radvision Customer Support prior to restoring a previous software version.

Before you begin

- Verify you have backed up the current device configuration (see [Backing Up Your Scopia Elite MCU Configuration](#) on page 45).
- On the **Status** tab, verify that the MCU is connected to the network by checking the **Ethernet** icon ([Figure 40: Status Map Section of the Status Tab](#) on page 49).

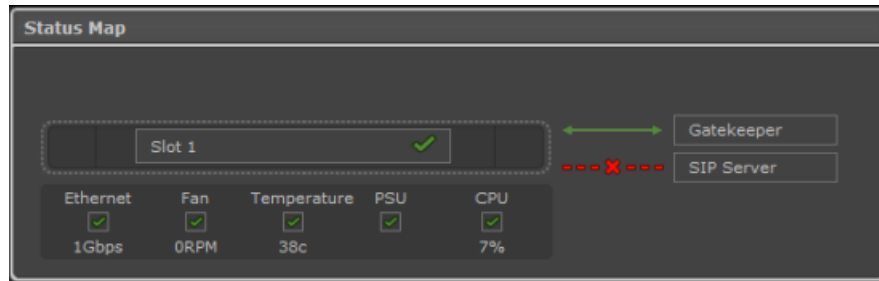


Figure 40: Status Map Section of the Status Tab

- Verify that there are no active videoconferences hosted on the MCU by selecting **Manage Conferences** **Manage Conferences >** and checking that no conferences appear in the **Conference List**.

Procedure

1. Access the MCU web Administrator interface.
2. Select  > **Rollback software**.
Restoring the previous version may take up to 15 minutes.
3. After reset, the previous release is installed on the MCU.
The downgrade process returns the MCU configuration back to the previous version, with the values used prior to the last upgrade.

Important:

Do not import a saved configuration to the MCU after the downgrade. An older version of the MCU configuration might not support the new configuration values.

4. Verify that the MCU functions properly:
 - a. From an endpoint dial the MCU IP address.
You access the MCU auto attendant service which plays the video and audio prompts.
 - b. Select **0** to create a new conference.
 - c. At a prompt, enter the meeting ID and then #.
The MCU creates a new conference and the Conference window is displayed.
 - d. Exit the conference by disconnecting the call.
5. Verify the device is ready.
 - a. Configure this MCU in Scopia Management as explained in *Administrator Guide for Scopia Management*.
 - b. Take other MCUs offline (if any) to make sure you hold the videoconference on this MCU.
 - c. From an endpoint dial the IP address (or the Auto-Attendant number if configured).
 - d. Press **0** to create a new conference.
 - e. At the prompt, enter the meeting ID followed by #.
The MCU creates the videoconference. If it is successful, the MCU is properly installed and configured.

You can view the videoconference status in these pages:

- The MCU's **Status Map** which shows the connection to Scopia Management and conference use statistics.

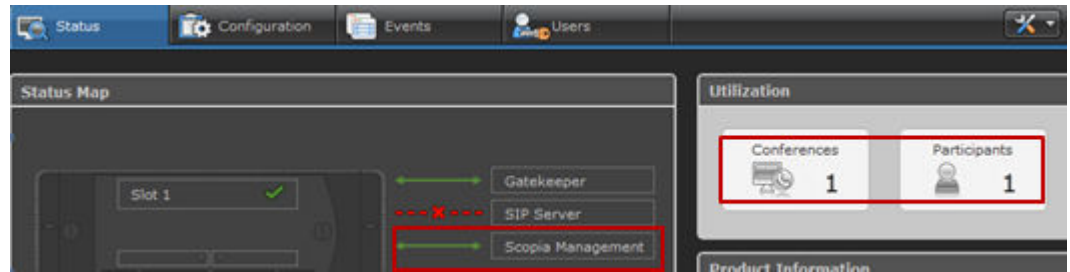


Figure 41: The MCU Status Map

- The Scopia Management **Dashboard** which shows the details of the current videoconference.

ID	Name	Participants	MCU	Terminate
716194	IVR Session	1	MCU230192	X

Figure 42: The Scopia Management Dashboard status

f. Exit the videoconference by disconnecting the call.

Configuring Ports on All Models of the Scopia Elite MCU

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

Navigation

- [Configuring the UDP Port Ranges for RTP/RTCP on the Scopia Elite MCU](#) on page 50
- [Configuring the TCP Port Range for H.245 on the Scopia Elite MCU](#) on page 51
- [Configuring the HTTP Port on the Scopia Elite MCU](#) on page 52
- [Configuring the UDP Port for RAS on the Scopia Elite MCU](#) on page 53
- [Configuring the UDP Port for the Gatekeeper on the Scopia Elite MCU](#) on page 54
- [Configuring the TCP Port Q.931 on the Scopia Elite MCU](#) on page 55
- [Configuring the TCP/UDP/TLS Port for SIP on the Scopia Elite MCU](#) on page 56
- [Configuring the TCP Port Range for SIP BFCP on the Scopia Elite MCU](#) on page 57

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

About this task

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

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

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

 Important:

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

Procedure

1. Navigate to the MCU **Advanced Commands** section by doing the following:
 - a. Select the  icon.
 - b. Select **Advanced parameters**.
 - c. Locate **Video Base Port** or the **Audio Base Port** entry in the **Name** column to change the video or audio port values respectively (see [Figure 43: Defining the base port for video](#) on page 51).



Advanced parameters		
Name	Value	Review
Video Base Port	12000	

Figure 43: Defining the base port for video

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

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

About this task

The Scopia Elite 6000 Series MCU has designated TCP ports 1024-1324 for H.245. You can set the base port, which is the lower end of the port range. H.245 is a Control Protocol used for multimedia

communication that enables transferring information about the device capabilities, as well as opening/closing the logical channels that carry media streams.

The Scopia Elite 6000 Series MCU uses 300 ports.

Procedure

1. Navigate to the MCU **Advanced Commands** section by doing the following:
 - a. Select the  icon.
 - b. Select **Advanced parameters**.
 - c. Locate the **CLI** section and select **More** (see [Figure 44: CLI Section](#) on page 52).



Figure 44: CLI Section

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

Important:

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

3. Modify the port value in the **Value** field.
4. Select **Execute**.
5. Select **Close**.

Configuring the HTTP Port on the Scopia Elite MCU

About this task

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

Procedure

1. Navigate to the MCU **Advanced Commands** section by doing the following:
 - a. Select the  icon.
 - b. Select **Advanced parameters**.

- c. Locate the **CLI** section and select **More** (see [Figure 45: CLI Section](#) on page 53).



Figure 45: CLI Section

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

! Important:

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

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

4. Select **Execute**.

! Important:

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

5. Select **Yes** to continue.

6. Select **Close**.

! Important:

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

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

Configuring the UDP Port for RAS on the Scopia Elite MCU

About this task

The Scopia Elite 6000 Series MCU has designated port 1719 for RAS. You can configure a different port to use RAS (for example, if port 1719 is busy). Port 1719 is also used to communicate with the gatekeeper (to configure the UDP port for the gatekeeper, see [Configuring the UDP Port for the Gatekeeper on the Scopia Elite MCU](#) on page 54).

! Important:

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

Procedure

1. Navigate to the MCU **Advanced Commands** section by doing the following:
 - a. Select the  icon.
 - b. Select **Advanced parameters**.
 - c. Locate the **H323 RAS port number** in the **Name** column (see [Figure 46: RAS Port Configuration](#) on page 54).

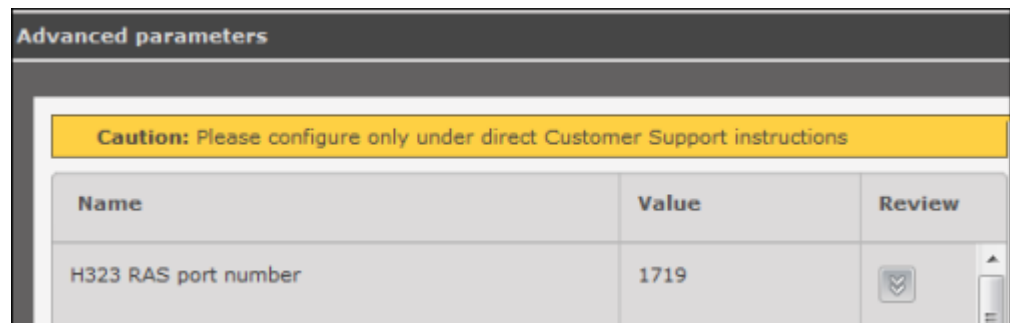


Figure 46: RAS Port Configuration

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

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

About this task

The Scopia Elite 6000 Series MCU has designated port 1719 for gatekeeper use. You can configure a different port to enable communication with the gatekeeper (for example, if port 1719 is busy). Port 1719 is also used for RAS (to configure the UDP port for RAS, see [Configuring the UDP Port for RAS on the Scopia Elite MCU](#) on page 53).

! Important:

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

Procedure

1. Navigate to the MCU **H.323 Protocol** section by selecting **Configuration > Protocols**.
2. Locate the **Enable H.323 protocol** section (see [Figure 47: H.323 Protocol section of the Protocols tab](#) on page 55).

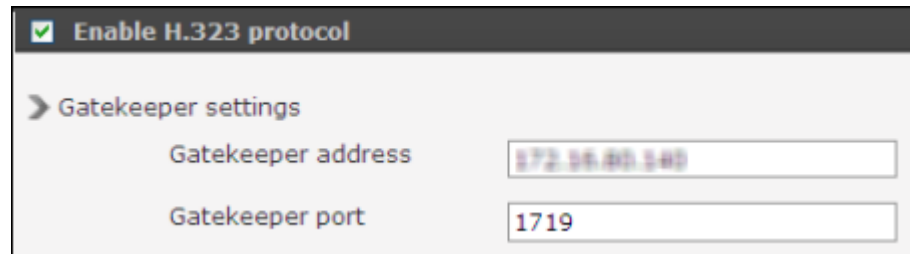


Figure 47: H.323 Protocol section of the Protocols tab

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

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

About this task

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

Procedure

1. Navigate to the MCU **Advanced Commands** section by doing the following:
 - a. Select the  icon.
 - b. Select **Advanced parameters**.
 - c. Locate the **H323 SIG port number** in the **Name** column (see [Figure 48: H.323 Signaling Port Configuration](#) on page 56).



Figure 48: H.323 Signaling Port Configuration

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

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

About this task

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

Procedure

1. Navigate to the MCU **SIP Protocol** section by selecting **Configuration > Protocols**.
2. Locate the **Enable SIP protocol** section and select **More** (see [Figure 49: SIP Port Configuration](#) on page 57).

☒ Enable SIP protocol

> Default SIP domain

> SIP server

☒ Locate automatically

☐ Specify

IP address

Port

Type

☒ Use registrar

IP address

Port

Type

> Local signaling port

> Local TLS signaling port

More

Figure 49: SIP Port Configuration

3. Do one of the following:

- If your SIP server or Registrar is not configured with TLS, enter the port value in the **Local signaling port** field.
- If your SIP server or Registrar is configured with TLS, enter the port value in the **Local TLS signaling port** field.

! Important:

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

4. Select **Apply**.

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

About this task

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

BFCP is a protocol which coordinates shared videoconference features in SIP calls, often used by one participant at a time. For example, when sharing content to others in the meeting, one participant is designated as the presenter, and is granted the floor for presenting. All endpoints must be aware that the floor was granted to that participant and react appropriately.

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

Procedure

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

- a. Select the  icon.
- b. Locate **SIP BFC Base Port** entry in the **Name** column to change the port value (see [Figure 50: Defining the base port for SIP BFCP](#) on page 58).

Name	Value	Review
SIP BFCP base port	3400	

Figure 50: Defining the base port for SIP BFCP

- c. Select the  icon in the **Review** column.
- d. Enter the new lower end port value in the field.
- e. Select **Apply**.
- f. Select **Close**.

Customizing the Logo Displayed in MCU Conferences

About this task

Perform the procedure in this section to customize the default logo displayed in the auto-attendant and the MCU conference screens.

Procedure

1. Select **Configuration** .
2. Select **Customization**.
3. Locate the **Images pack** area ([Figure 51: Customizing the Images Pack](#) on page 58).

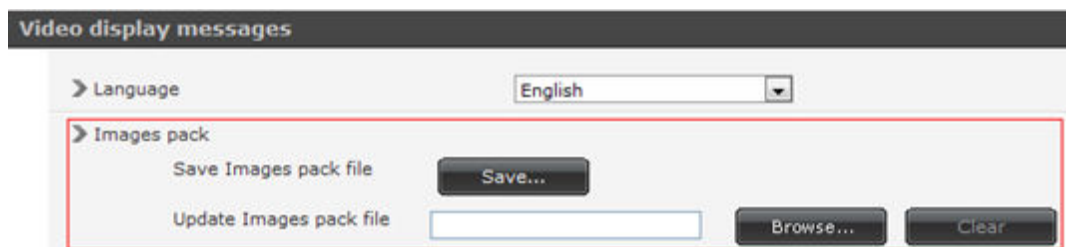


Figure 51: Customizing the Images Pack

4. Select **Save** and save the .zip file with the current images to your local drive.

5. Navigate to the location where you saved the .zip file.
6. Add your logo image to each folder, as follows:

+ Tip:

It is easier to do this procedure if you open the zip file in Windows Explorer. Images are separated into folders according to resolution ([Figure 52: Image Pack Folder Structure](#) on page 59). You need to save the desired logo with each of the specified resolutions to the relevant folder.

If any of the images are missing or not in the correct format, the default system logo is used.

Name	Type
4cif	File folder
352p	File folder
480p	File folder
720p	File folder
1080p	File folder
cif	File folder
qcif	File folder

Figure 52: Image Pack Folder Structure

- a. Ensure that your logo image has the correct dimensions (see [Table 9: Logo Image Dimensions](#) on page 59 for the requirements).

Table 9: Logo Image Dimensions

Resolution	File Dimension (in Pixels)
4CIF	216 x 44
1080p	312 x 64
352p	132 x 24
480p	132 x 24
720p	216 x 44
CIF	132 x 24
QCIF	96 x 16

- b. Give your image a filename in the following format (maximum characters allowed in the filename is 32):

logo_XX

7. Update the Image pack file by selecting **Browse** and navigating to your updated .zip file.
8. Select **Apply**.
9. Select the  icon.
10. Select **Advanced Parameters**.
11. Locate the **Default vendor logo** in the **Name** column (see [Figure 53: Advanced Commands Section](#) on page 60).

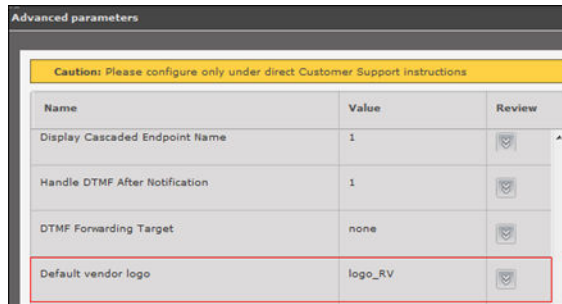


Figure 53: Advanced Commands Section

12. Select the icon in the **Review** column.
13. Enter the filename of the logo you added in [6](#).
14. Select **Apply**.
15. Select **Close**.

Customizing MCU Audio Messages

About this task

You can change the default audio messages in your MCU to have your own wording. You can upload a single customized audio message, or you can upload a zip file containing all the messages customized. You can also download the existing messages pack of the MCU to inspect the naming convention of each filename.

Sound files must be in .wav format, encoded with G.711 (CCITT), 8-bit, 8kHz mono.

Procedure

1. Access the MCU administrator web interface.
2. Select **Configuration > Customization > Audio messages**.

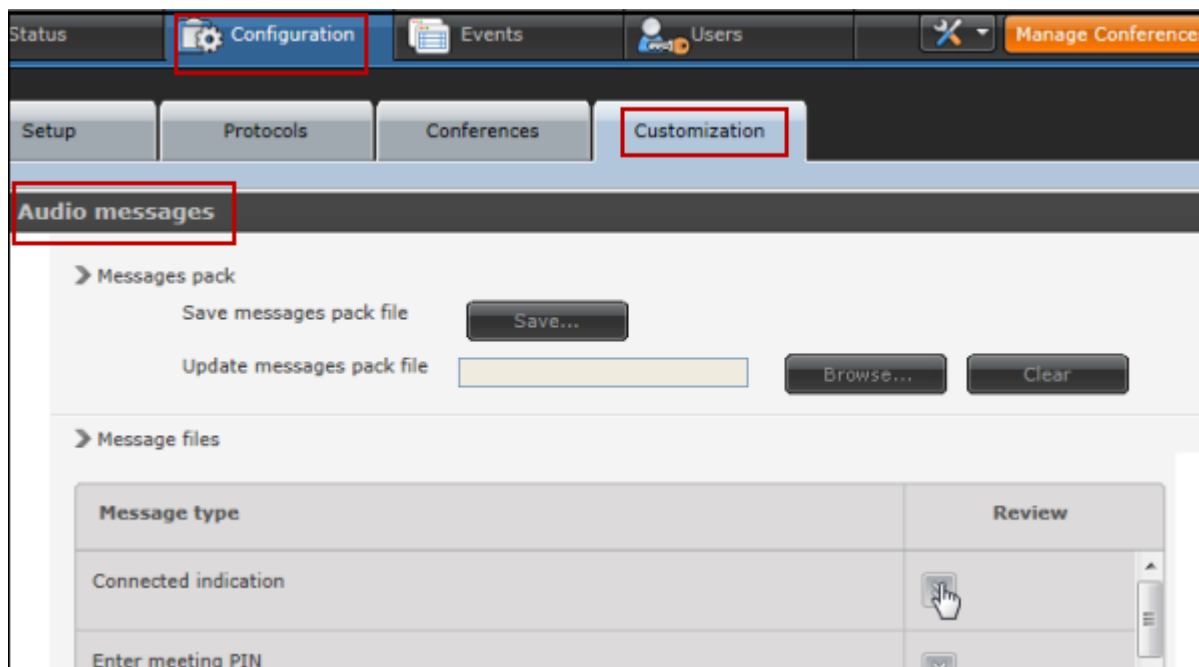


Figure 54: Customizing audio messages

3. To upload a single message, locate the specific message to be customized in the **Message files** section and select the  icon in the **Review** column.
4. To upload a pack of messages, locate the **Messages pack** section.
 Message packs are sound files grouped together in a standard zip file. File uploads must be less than 3Mb.
 Before uploading your customized pack of sound files, we recommend first downloading the existing message pack by selecting **Save** (see [Figure 54: Customizing audio messages](#) on page 61), then replace the sound files you want to customize from the downloaded zip file.
5. Select **Browse** and locate the sound file.
6. Select **Save**.
7. Select **Apply**.

Chapter 4 | Moderating a Videoconference from the MCU

About this task

Use the Scopia Elite MCU Conference Control interface in standalone MCU deployments to perform these tasks:

- View active conferences hosted on the MCU or on cascaded MCUs.
- View participant details.
- Create conferences.
- Moderate conference participants.
- Monitor and manage conference behavior.

Important:

You can configure meetings from the MCU's Conference Control interface only in standalone mode, when the MCU is not part of a Scopia Management deployment. In Scopia Management deployments, the conference control is managed by Scopia Management.

While all users can use the Conference Control interface, access to conference management features is controlled by authorization access levels: Administrator, Operator, Moderator and User.

[Figure 55: Conference Control Page](#) on page 63 shows the layout of the Conference Control page, which may vary depending on whether you are a moderator or not. If you are not a moderator, you do not have access to moderator tasks. Figures in this section show all interface elements including those which are available for moderators only.

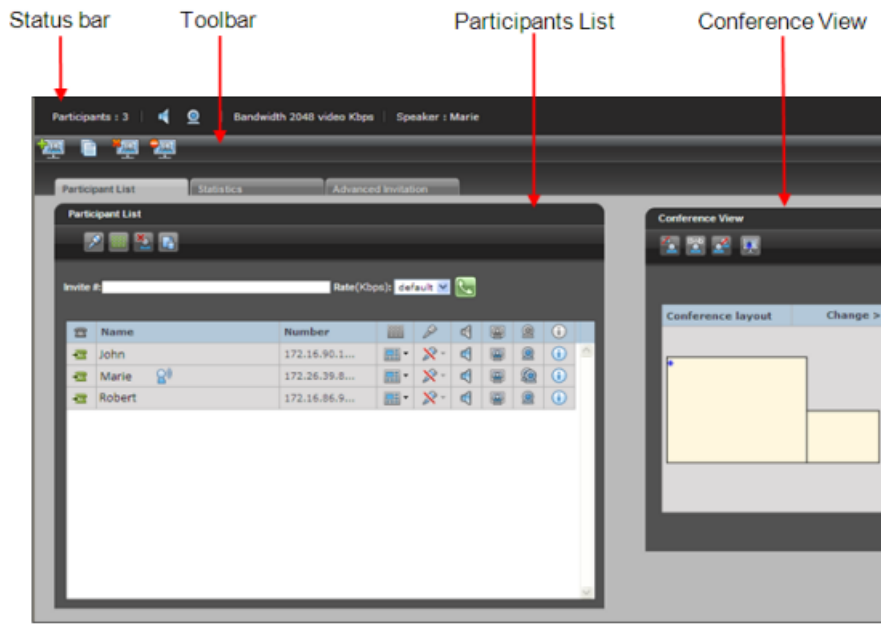


Figure 55: Conference Control Page

The Conference Control page consists of the following elements:

- The status bar displays the number of participants, the bandwidth used, the active speaker, and whether video and voice are enabled for this videoconference.
- The toolbar enables you to create a new videoconference, block admission or become a moderator.
- The **Participant List** lists the current participants, and enables moderators to control their experience of the videoconference. You can also invite new participants in this pane.
- The **Conference View** displays the current video layout and enables you to change it.

Administrators and Operators can jointly be moderators simultaneously. This procedure details how to assume moderator rights in the Conference Control interface.

Procedure

1. Access the Conference Control interface by selecting **Manage Conferences >**. The system displays a list of ongoing videoconferences.
Select any meeting to access its details.
2. Select **Become Moderator**  to take control of that conference.
3. A dialog box requesting a PIN might appear if Moderator access is PIN-protected. Enter the PIN.
4. To release control of the conference, select **Stop Moderation** .

Navigation

- [Creating a New Videoconference from the MCU](#) on page 64
- [Muting and Unmuting Participants](#) on page 66
- [Changing the Video Layout of an Ongoing Videoconference](#) on page 67
- [Personalizing Video Layouts for Participants](#) on page 69

- [Blocking Access to a Videoconference](#) on page 73
- [Viewing Participant Call Information](#) on page 73
- [Displaying Participant Names in the Video Layout](#) on page 77
- [Ending a Videoconference from the MCU](#) on page 79

Navigation

- [Creating a New Videoconference from the MCU](#) on page 64
- [Muting and Unmuting Participants](#) on page 66
- [Changing the Video Layout of an Ongoing Videoconference](#) on page 67
- [Personalizing Video Layouts for Participants](#) on page 69
- [Blocking Access to a Videoconference](#) on page 73
- [Viewing Participant Call Information](#) on page 73
- [Displaying Participant Names in the Video Layout](#) on page 77
- [Ending a Videoconference from the MCU](#) on page 79

Creating a New Videoconference from the MCU

About this task

Moderators, Operators, and Administrators can create a new conference either from the login window or from the Conference Control interface.

From the login window, you can select the **Create/Manage** link to create a meeting.

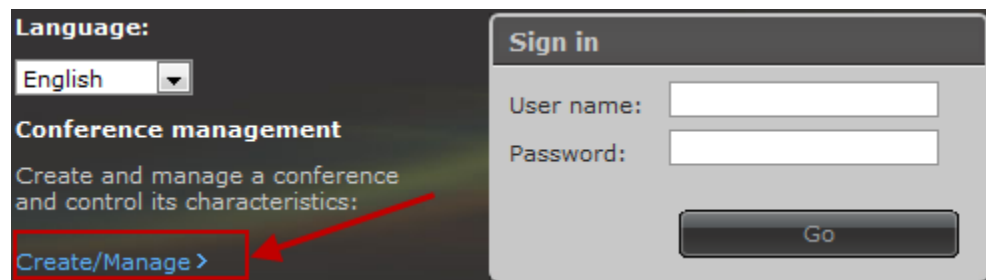


Figure 56: Creating a videoconference from the Scopia Elite MCU login window

This section details how to create a meeting from the Conference Control interface.

! Important:

You can configure meetings from the MCU's Conference Control interface only in standalone mode, when the MCU is not part of a Scopia Management deployment. In Scopia Management deployments, the conference control is managed by Scopia Management.

Procedure

1. Access the Conference Control interface by selecting **Manage Conferences >**. The system displays a list of ongoing videoconferences.
Select any meeting to access its details.

2. Select **Become Moderator**  to take control of that conference.

3. Select **Create Conference**  on the toolbar.

4. Select a meeting type and its dial prefix from the list.

Meeting types (also known as MCU services) are meeting templates which determine the core characteristics of a meeting. For example, they determine if the meeting is audio only or audio and video, they determine the default video layout, the type of encryption, PIN protection and many other features. Meeting types are created in the MCU. You can invoke a meeting type by dialing its prefix in front of the meeting ID.

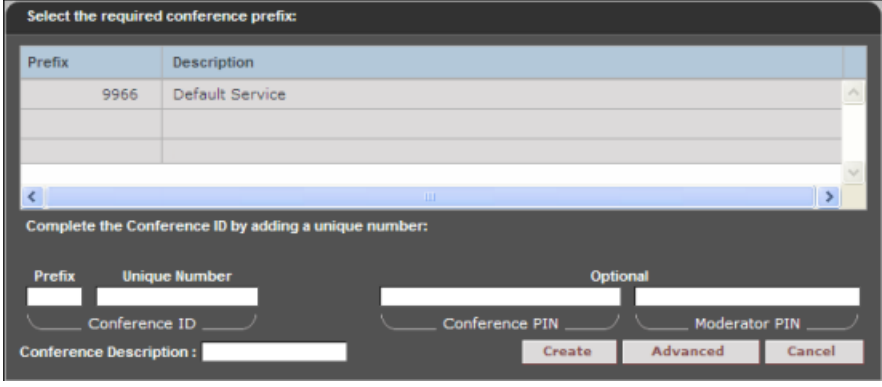


Figure 57: Create Conference Page

5. Configure the videoconference settings as defined in

Table 10: Fields to create a new videoconference

Field Name	Description
Prefix	The dial prefix for the meeting is determined by the meeting type (service).
Unique Number	Assign a meeting ID for this videoconference.
Conference PIN	If you want to protect entrance to this videoconference, enter an access PIN.
Moderator PIN	If you want to protect moderator functions in this videoconference, enter a moderator PIN. ! Important: You can also define a default moderator PIN for a meeting type.

Field Name	Description
Conference Description	Enter a description of the meeting.
Advanced	Select to define additional properties of the videoconference such as duration, time-out and dialing policy settings.

6. Select **Create** to start the meeting.

Muting and Unmuting Participants

About this task

Moderators can mute or unmute an individual participant in an ongoing videoconference.

Important:

You can configure meetings from the MCU's Conference Control interface only in standalone mode, when the MCU is not part of a Scopia Management deployment. In Scopia Management deployments, the conference control is managed by Scopia Management.

Procedure

1. Access the Conference Control interface by selecting **Manage Conferences >**. The system displays a list of ongoing videoconferences.
Select any meeting to access its details.
2. Select **Become Moderator**  to take control of that conference.
3. To mute a single participant, select that person's microphone  to toggle the mute/unmute of that endpoint.

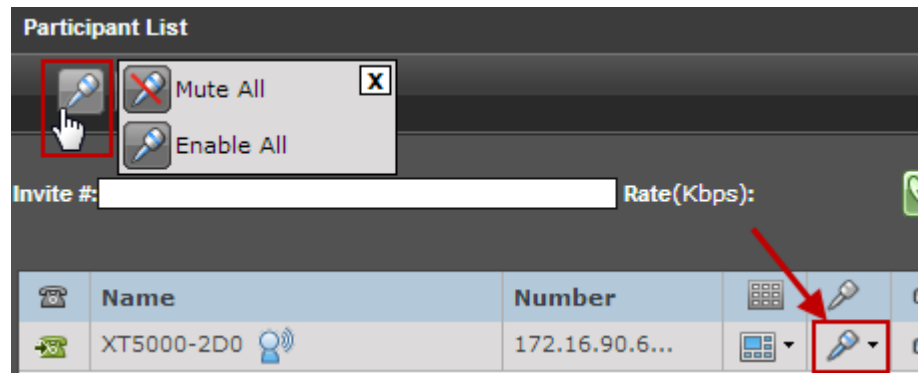


Figure 58: Muting one participant or all participants in a videoconference

4. To mute all participants, select the microphone  in the toolbar. It displays a submenu enabling you to mute or unmute all participants.

Changing the Video Layout of an Ongoing Videoconference

About this task

Moderators can change the video layout of an ongoing videoconference from the Conference Control interface. The MCU supports video layouts for up to 28 participants.



Figure 59: Available video layouts up to 28 participants

❗ Important:

You can configure meetings from the MCU's Conference Control interface only in standalone mode, when the MCU is not part of a Scopia Management deployment. In Scopia Management deployments, the conference control is managed by Scopia Management.

Procedure

1. Access the Conference Control interface by selecting **Manage Conferences >**. The system displays a list of ongoing videoconferences.
Select any meeting to access its details.
2. Select **Become Moderator**  to take control of that conference.
3. In the **Conference View** section of the **Participant List** tab, select **Change**.

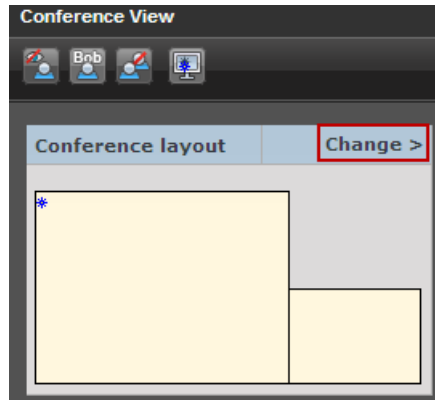


Figure 60: Conference View Section

The layout menu appears, displaying a list of available layouts for the current conference.

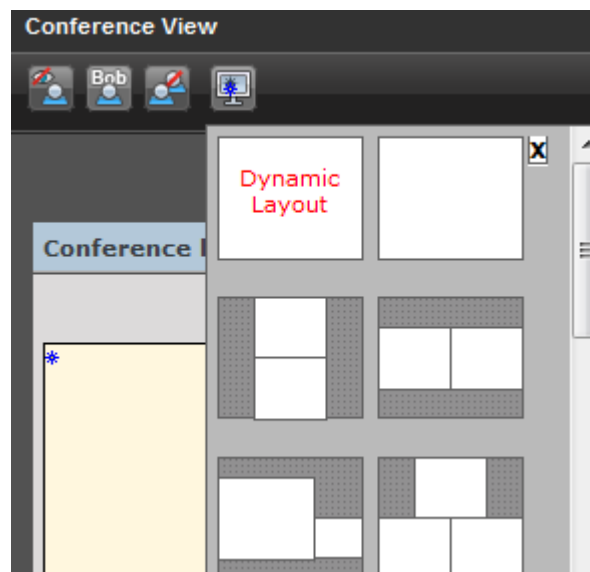


Figure 61: Changing the video layout

4. Select the layout of your choice.

! Important:

You can display up to 28 participants in a single layout. Layouts that display up to 16 participants are supported by all resolutions, while layouts that display 21 or 28 participants are supported only by resolutions of 480p or higher.

The videoconference adjusts to the new selection.

Personalizing Video Layouts for Participants

About this task

Moderators can customize different video layouts for any of the meeting participants from the Conference Control interface. A video layout is the arrangement of participant images as they appear on the monitor in a videoconference. You can assign a video layout to the whole videoconference, or you can assign a layout to an individual participant.



Figure 62: Available video layouts up to 28 participants

Important:

You can configure meetings from the MCU's Conference Control interface only in standalone mode, when the MCU is not part of a Scopia Management deployment. In Scopia Management deployments, the conference control is managed by Scopia Management.

Personalized layouts must be enabled in the meeting type definition. For more information, see [Configuring a New MCU Meeting Type](#) on page 19.

By default a single video layout is assigned to all participants in a videoconference.

Personalized video layouts are marked with different icons.

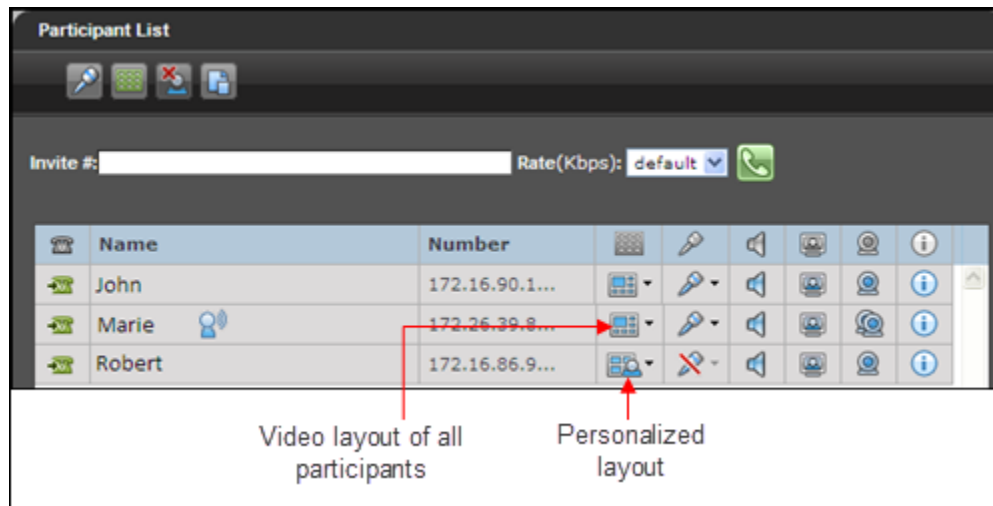


Figure 63: Personalizing video layouts

Procedure

1. Access the Conference Control interface by selecting **Manage Conferences >**. The system displays a list of ongoing videoconferences.
Select any meeting to access its details.
2. Select **Become Moderator** [Icon] to take control of that conference.
3. To change the view for an individual participant:
 - a. Select **Change View** [Icon] for this participant.

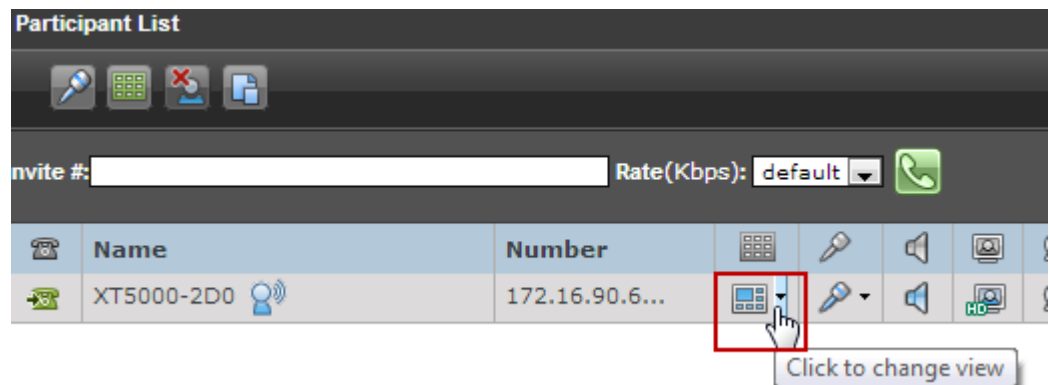


Figure 64: Change Participant's View button in the Participant List Tab

- b. From the submenu, select the new video layout.

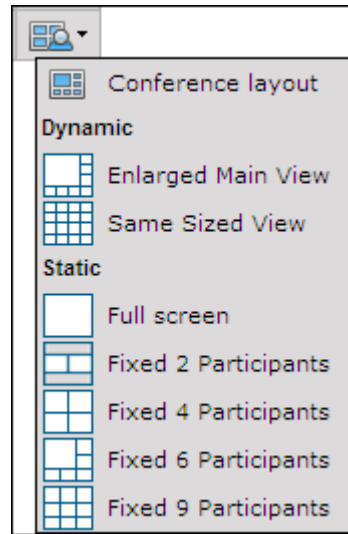


Figure 65: Participant View Submenu

! Important:

You can display up to 28 participants in a single layout. Layouts that display up to 16 participants are supported by all resolutions, while layouts that display 21 or 28 participants are supported only by resolutions of 480p or higher.

4. To change the view for more than one participant at the same time:
 - a. Select the participants from the list of names while holding down the CTRL key.
 - b. In the toolbar of the **Participant List** pane, select the **Change View** button.

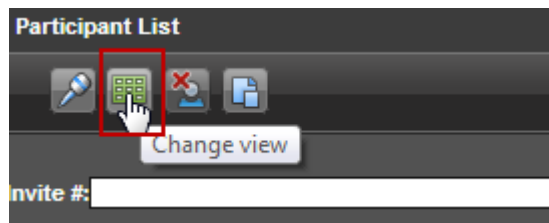


Figure 66: Changing the layout of several participants

- c. In the **Change view** pop-up, choose **Selected participants**.

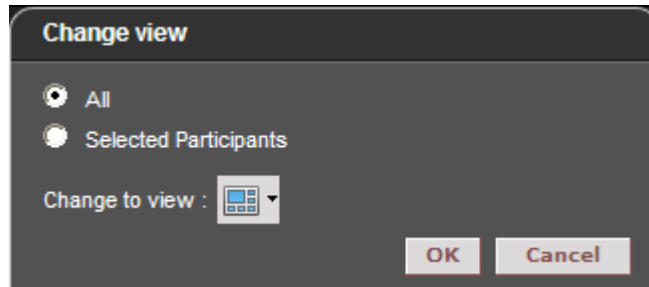


Figure 67: Change view dialog box

You can also change the video layout of all the participants at once by selecting **All**. For a more complete list of video layouts for all participants, see [Changing the Video Layout of an Ongoing Videoconference](#) on page 67.

- d. From the **Change to view**  list, select the new video layout.
- e. Select **OK**.

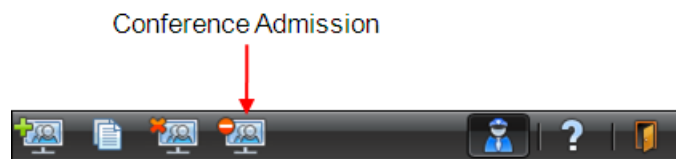
Blocking Access to a Videoconference

About this task

Moderators can block the admission of additional participants in a conference in the Conference Control interface. As a result, no further participants can join the conference.

Procedure

1. Access the Conference Control interface by selecting **Manage Conferences** . The system displays a list of ongoing videoconferences.
Select any meeting to access its details.
2. Select **Become Moderator**  to take control of that conference.
3. On the main toolbar, select **Conference Admission**.



To re-admit participants, select **Conference Admission** again.

Viewing Participant Call Information

About this task

Moderators of a videoconference can view detailed information about any of the participants, including information about the endpoint, and technical details about the audio, video and data streams flowing to and from this endpoint.

Procedure

1. Access the Conference Control interface by selecting **Manage Conferences >**. The system displays a list of ongoing videoconferences.
Select any meeting to access its details.
2. Select **Become Moderator**  to take control of that conference.
3. Select the required participant in the **Participant List** tab.

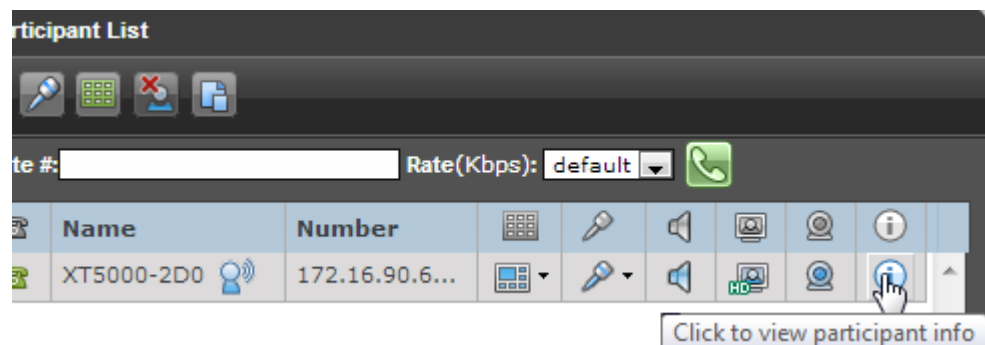


Figure 68: Viewing participant information

4. Select **Information**  for the selected participant.

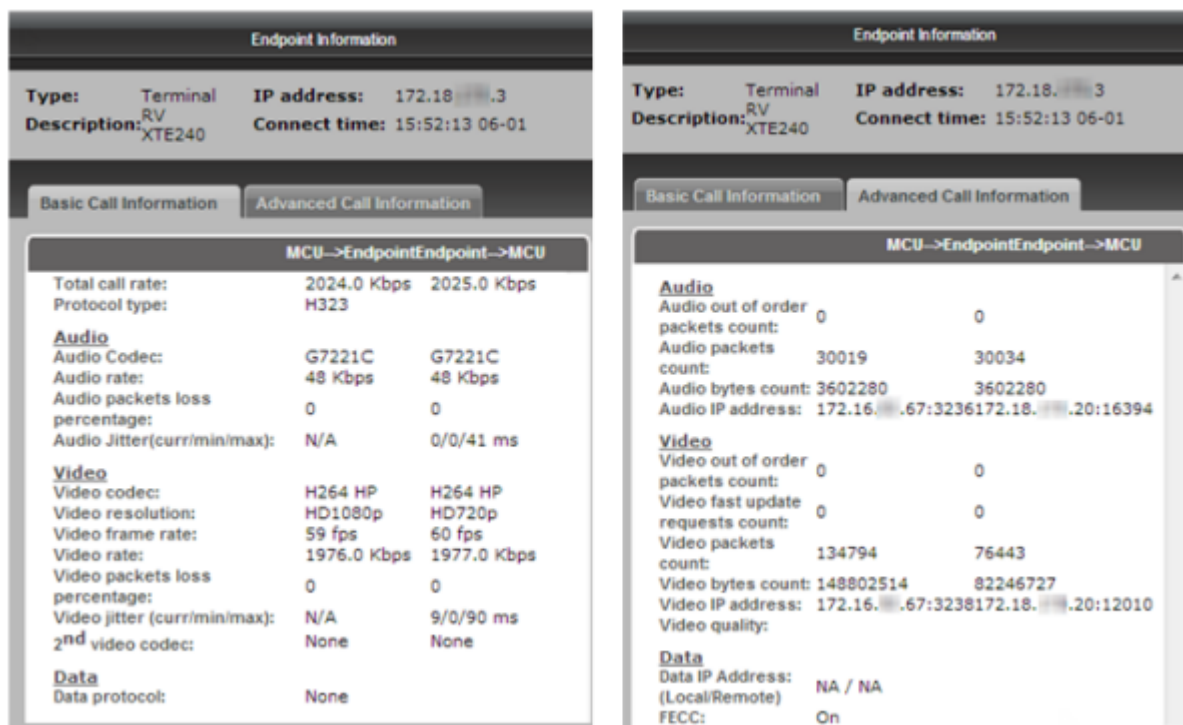


Figure 69: Detailed connection information of an endpoint

! Important:

You need to enable pop-up windows to see the information view.

The participant's **Call Information** window is displayed with two tabs: basic and advanced call information. There are two columns of data, one for values sent by the MCU to the endpoint, and other column for data sent by the endpoint to the MCU. The following table lists the fields in each tab.

Group	Field	Description
Endpoint Information	Type	The type of endpoint used by this participant to connect to the videoconference. Dedicated videoconferencing endpoints are listed as Terminal .
	IP address	The participant endpoint's IP address.
	Description	Displays the endpoint vendor identifier, if available.
	Connect time	The time stamp showing when the participant connected to the conference.
Basic Call Information		
Audio	Total call rate	The total of the audio and video bandwidth sent to and received by this endpoint.
	Protocol type	The protocol used to connect with this endpoint.

Group	Field	Description
	Audio Codec	The audio codecs used in sending to and receiving from the participant.
	Audio rate	Bandwidth used in sending and receiving audio from this endpoint.
	Audio Packet loss percentage	Percentage of lost audio packets sent to and received by this endpoint.
	Audio Jitter (curr/min/max)	A measure of the variance in the arrival time of audio packets sent over the network. High variance leads to disjointed sound output. Three values are displayed, separated by a slash (/): the current variance, the minimum value during this connection, and the maximum value.
Video	Video codec	The video codecs used in sending to and receiving from this endpoint.
	Video resolution	Video resolution sent and received by the endpoint.
	Video frame rate	Frame rate of the video sent to and received by the endpoint. Measured in frames per second (fps).
	Video rate	Bandwidth used in sending and receiving video from this endpoint.
	Video packets loss percentage	Percentage of lost video packets sent to and received by this endpoint.
	Video jitter (curr/min/max)	A measure of the variance in the arrival time of video packets sent over the network. High variance leads to disjointed video output. Three values are displayed, separated by a slash (/): the current variance, the minimum value during this connection, and the maximum value.
	2nd video codec	If there are two video streams between this MCU and the endpoint (for example, two cameras), this field displays the video codec sent to and received by the endpoint in this stream.
Data	Data protocol	The protocol used for data transmissions if the participant is sharing data.
Advanced Call Information		

Group	Field	Description
Audio	Audio out of order packets count	Total audio packets sent to and received from the participant's endpoint which were out of sequence. When data is carried via network packets over a complex topology, a packet may arrive earlier than its predecessor. For clear audio, the packets must be reassembled in the correct order.
	Audio packets count	Total audio packets sent and received by the participant's endpoint.
	Audio bytes count	Total audio bytes sent and received by the participant.
	Audio IP address	IP address and port of the endpoint where audio is sent and received.
Video	Video out of order packets count	Total video packets sent to and received from the participant out of sequence.
	Video fast update requests count	Total number of Video Fast Update requests sent and received by the endpoint. Video Fast Update (VFU) is a request for a refreshed video frame, sent when the received video is corrupted by packet loss. In response to a VFU request, the broadcasting endpoint sends a new intra-frame to serve as the baseline for the ongoing video stream.
	Video packets count	Total video packets sent and received by the endpoint.
	Video bytes count	The number of bytes of video sent and received by the endpoint.
	Video IP address	IP address and port of the endpoint where video is sent and received.
	Video quality	Not in use.
Data	Data IP address (Local/Remote)	IP address and port of the endpoint used to send data. The two addresses are separated by a slash (/).
	FECC	Indicates whether Far End Camera Control is enabled for this endpoint.

Displaying Participant Names in the Video Layout

About this task

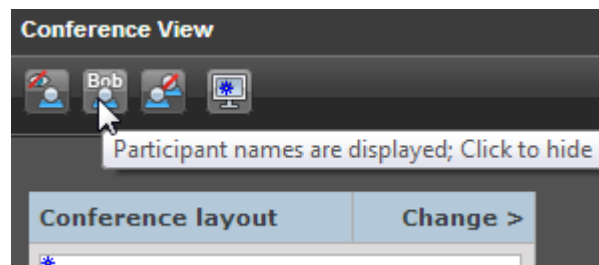
Moderators can configure the display of the names of endpoints or participants in the video layout using the Conference Control interface.

! Important:

You can configure meetings from the MCU's Conference Control interface only in standalone mode, when the MCU is not part of a Scopia Management deployment. In Scopia Management deployments, the conference control is managed by Scopia Management.

Procedure

1. Access the Conference Control interface by selecting **Manage Conferences >**. The system displays a list of ongoing videoconferences.
Select any meeting to access its details.
2. Select **Become Moderator**  to take control of that conference.
3. Select **Display names**  in the **Conference View** section.



The names are displayed at the bottom of the participants' frames in a conference ([Figure 70: Names Displayed in Conference \(Example\)](#) on page 78).



Figure 70: Names Displayed in Conference (Example)

Ending a Videoconference from the MCU

About this task

You can terminate an ongoing videoconference at any time. This action disconnects all participants from the meeting and deletes it from the list of conferences.

! Important:

You can configure meetings from the MCU's Conference Control interface only in standalone mode, when the MCU is not part of a Scopia Management deployment. In Scopia Management deployments, the conference control is managed by Scopia Management.

Procedure

1. Access the Conference Control interface by selecting **Manage Conferences >**. The system displays a list of ongoing videoconferences.
Select any meeting to access its details.
2. Select **Become Moderator**  to take control of that conference.
3. Select **Terminate Conference**  from the toolbar.

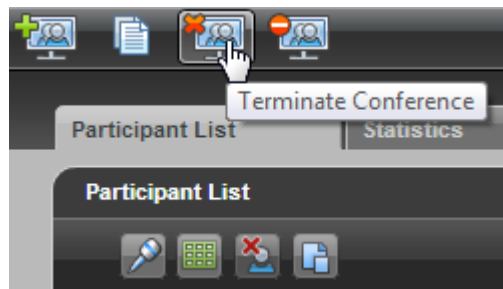


Figure 71: Terminate Conference Button on the Toolbar

4. Select **OK** to confirm.
All participants are disconnected and the videoconference is closed.

Chapter 5 | Troubleshooting the Scopia Elite MCU

These tips list useful hardware and software troubleshooting solutions. If the MCU still malfunctions, contact your local Radvision support representative for help.

Navigation

- [Defining an Advanced Command on the MCU](#) on page 80
- [Resolving MCU Failure to Register with the Gatekeeper](#) on page 81
- [MCU Cannot Start a Videoconference](#) on page 82
- [MCU Does Not Allow Access an Existing Videoconference](#) on page 83
- [Poor Quality in Cascaded Videoconferences](#) on page 84
- [Endpoints Unexpectedly Disconnect from Videoconferences](#) on page 84
- [Videoconference Ends Unexpectedly](#) on page 84
- [Resolving Presentation Issues](#) on page 86
- [SIP Call Disconnected Unexpectedly](#) on page 87
- [Resolving Poor Video Quality](#) on page 88
- [Resolving Poor Audio Quality](#) on page 91
- [Resolving a Video Display Issue](#) on page 92

Defining an Advanced Command on the MCU

Problem How to enter an advanced command in the MCU. Often this instruction may come from a conversation with your local customer support representative.

Possible Causes Advanced configuration of some of the less commonly accessed settings are managed with **Advanced Command** settings on the MCU.

Solution Navigate to the advanced commands entry by performing the following steps.

Procedure

1. Select the  icon.
2. Select **Advanced parameters**.
3. Locate the **CLI** section and select **More** (see [Figure 72: CLI section in MCU](#) on page 81).

Figure 72: CLI section in MCU

4. Enter the advanced command in the **Command** field.
5. Enter the value of the command in the **Value** field.
6. Select **Execute**.

Resolving MCU Failure to Register with the Gatekeeper

Problem The Scopia Elite MCU fails to register with the gatekeeper.

- Possible Causes**
- The gatekeeper address is set incorrectly.
 - There is a TCP/IP setup issue.
 - There is a LAN or cable issue.
 - The ECS is in the Predefined mode.

Solution If the gatekeeper IP address is incorrect, verify the gatekeeper IP address and reconfigure the gatekeeper IP address on the MCU.

Solution If the problem is caused by a TCP/IP setup issue, perform these steps:

- Verify that the MCU is assigned a unique IP address.
- Verify that the subnet mask and default gateway subnet mask are set correctly.
- Attempt to ping the MCU from the gatekeeper to verify whether the MCU is reachable.
- Ensure the IP address assigned to the MCU is unique and not duplicated anywhere on the network.

Solution If the problem is caused by a LAN or cable issue, perform these steps:

- Verify the switch port settings.
- Verify that the Ethernet cable is straight through.
- Try another Ethernet cable.
- Verify if the Link and Activity LEDs on the switch port are lit.

Solution If the ECS is in **Predefined** mode, verify that the MCU is predefined on the ECS.

MCU Cannot Start a Videoconference

Problem Users cannot create new conferences.

Possible Causes

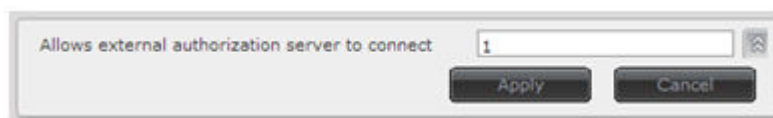
- In ad hoc conferences, the ECS is set to reject all calls.
- The MCU is set to work with an external authorization server, but no authorization server is configured.
- The MCU is set to work with an external authorization server, but the authorization server is not configured properly to work with the MCU.
- There are endpoint-related interoperability issues
- There are not enough MCU resources available for the desired conference.

Solution If the problem is caused by the ECS rejecting all calls, verify that the **Accept calls** option is checked in **ECS > Settings > Calls**.

Solution If the MCU is set to work with an authorization server and no authorization server is configured, perform these steps: verify that the **External conference authorization policy** option is set to **None** in **Maintenance > Advanced parameters > External conference policy authorization**.

Procedure

1. Access the MCU administrator web interface.
 2. Select the **Maintenance options** button , and then select **Advanced parameters**.
The Advanced parameters window is displayed.
 3. Locate the **Allows external authorization servers to connect** parameter.
 4. Select the **Review** button .
- This parameter section is displayed.



Solution If the MCU is set to work with an authorization server, but the authorization server is not configured properly, verify that the MCU IP address is correctly configured in the authorization server.

Solution If there are endpoint-related interoperability issues, perform this procedure:

Procedure

1. Verify the MCU and the endpoint are registered properly:
 - For SIP endpoints, verify that both the MCU and the SIP endpoint are properly registered with the SIP proxy.

- For H.323 endpoints, verify that both the MCU and the H.323 endpoint are properly registered with the ECS.
- For 3G endpoints, verify that both the MCU and the 3G endpoint are properly registered with the SIP proxy and/or ECS.

2. If the registration is correct, collect logs and wireshark traces and send them to Radvision Customer Support.

Solution If the initiating LAN endpoint is not registered with the ECS, verify that the initiating endpoint appears in the ECS Endpoints table correctly.

Solution If the MCU service is not defined in the ECS Services table, perform these steps:

Procedure

1. Verify that the service is defined in the MCU.
2. Verify that the MCU service prefix appears in the ECS Services table. If it does not, add it manually.
3. Verify that the service prefix is not a subset of another service prefix.

Solution There are not enough MCU resources available, verify that current calls are not utilizing all resources by checking the available MCU capacity and then trying to disconnect other calls in order to find the problem.

MCU Does Not Allow Access an Existing Videoconference

Problem An endpoint cannot be invited to a conference or dial into the conference.

- Possible Causes**
- The ECS is set to reject all calls.
 - The endpoint is not registered with the ECS.
 - The MCU is configured to work with an authorization server, but the endpoint is not authorized and therefore the authorization server rejects the call.
 - The endpoint is currently in a call.
 - There are not enough MCU resources available for the desired conference.

Solution If the ECS is set to reject all calls, verify that the **Accept calls** option is checked in **ECS > Settings > Calls**.

Solution If the endpoint is not registered with the ECS, verify that the invited/dialing endpoint appears in the ECS table of registered endpoints. Also verify that the endpoint is online.

Solution If the MCU is configured to work with an authorization server, verify that the endpoint is authorized in the authorization server.

Solution If the endpoint is currently in a call, confirm that the endpoint is not busy/in a call.

Solution If there are not enough MCU resources, remove one of the current participants to verify that the endpoint can join successfully. Then verify whether cascading is enabled and if the meeting is scheduled for cascading.

Poor Quality in Cascaded Videoconferences

Problem A videoconference using several MCU devices (cascaded videoconference) suffers long delays or bad lip synchronization.

Possible Causes The topology used for the conference is not suitable; for example, a chain topology is used unnecessarily.

Solution One single central MCU should invite all other cascaded MCUs. We recommend that you do not have more than one level of cascaded MCUs. Use a star topology, where the central MCU is in the center of the star, and other cascaded MCU modules are on the arms of the star.

Endpoints Unexpectedly Disconnect from Videoconferences

Problem Endpoints unexpectedly drop out of the MCU conference.

Possible Causes The network connection is unreliable.

Solution Check network connection quality. Round trip time should be less than 300ms.

Videoconference Ends Unexpectedly

Problem A conference on the MCU unexpectedly terminates.

Possible Causes

- The MCU unexpectedly drops out of the ECS endpoints database.
- The Ad hoc conferences terminate when option at **Configuration > Conferences** is set to Conference creator leaves and the conference creator has left the conference.

Solution If the MCU drops out of the ECS endpoints database:

Procedure

1. Uncheck the **Check that endpoint is online every n seconds** option in **ECS > Settings > Advanced**.
2. Uncheck the **Check that call is alive every n seconds** option in **ECS > Settings > Calls**.
3. Uncheck the **TTL** option in **ECS > Settings > Advanced**.

Solution If a conference is terminated when the conference creator has left the conference, perform this procedure:

Procedure

1. Access the MCU administrator web interface.
2. Select the **Configuration** tab  **Configuration**.
3. Select the **Conferences** tab  **Conferences**.
4. In the **Conference Control** section, select **More**.
Additional conference control parameters are displayed.

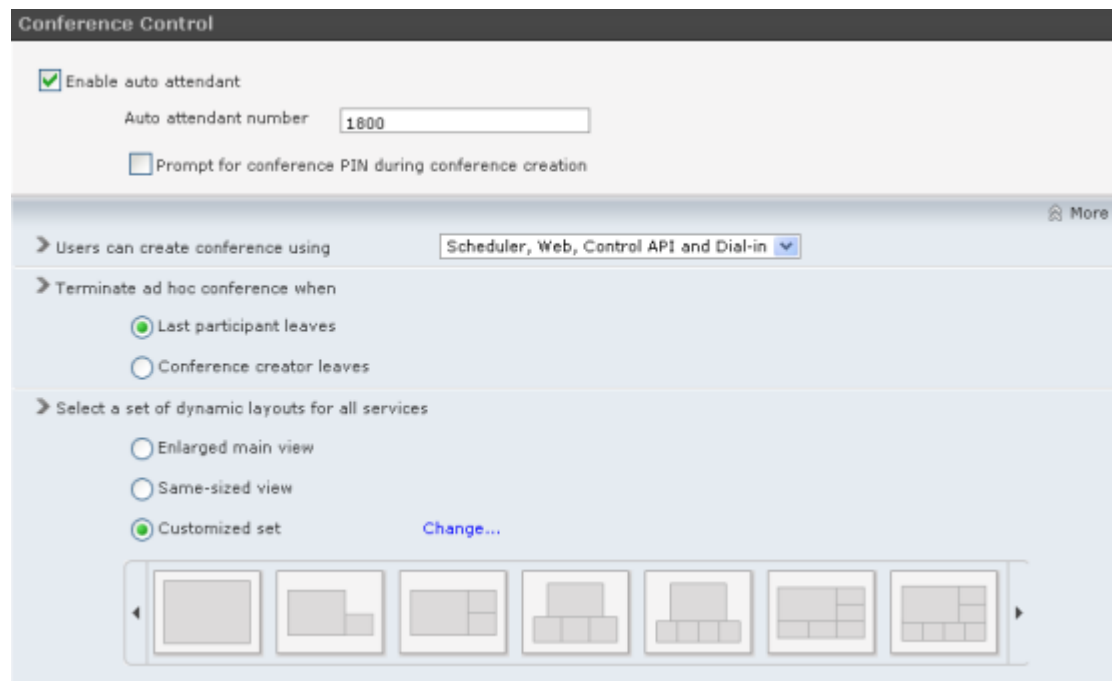


Figure 73: The Conference Control Section of the Conferences Tab

5. Enable the **Last participant leaves** option.
 6. Select **Apply**.
-

Resolving Presentation Issues

Problem A conference participant cannot start or receive a presentation.

Possible Causes

- H.239 functionality is not enabled on the endpoint.
- Presentation is not configured in the MCU service used in the conference.
- MCU presentation definitions in the service are not supported by the endpoint (frame rate, frame size, codec).

Solution If the H.239 functionality is not enabled on the participant's endpoint, verify that H.239 is enabled on the endpoint. Make a point-to-point call to another endpoint and verify that the participant can start a presentation.

Solution If presentation is not configured in the MCU, perform this procedure:

Procedure

1. Access the MCU administrator web interface.
2. Select the **Configuration** tab  Configuration.
3. Select the **Conferences** tab.
4. In the **Services List** section, select the service.
5. Select **More**.
Additional settings for this service are displayed.

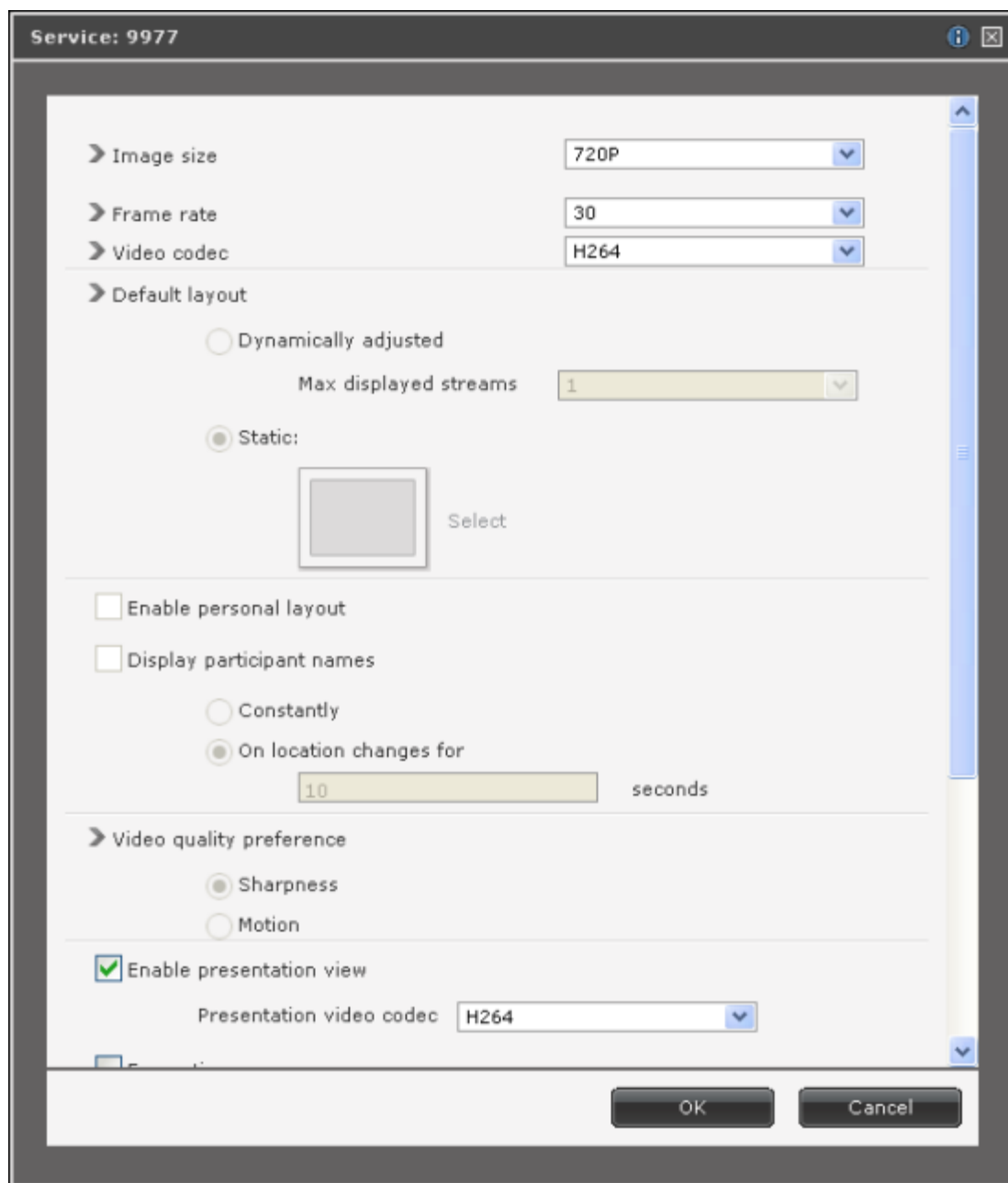


Figure 74: Additional Service Settings Window

6. Select **Enable presentation view**.

Solution If the problem is caused by inconsistency of presentation definitions, configure the endpoint to that it supports the frame size, frame rate and video codec as defined in the service.

SIP Call Disconnected Unexpectedly

Problem A SIP call unexpectedly disconnects after 30 seconds.

Possible Causes DNS is not fully configured on the MCU and user agents.

Solution Make sure that DNS is configured on user agent and MCU.

Resolving Poor Video Quality

Problem The quality of the video in a videoconference is poor.

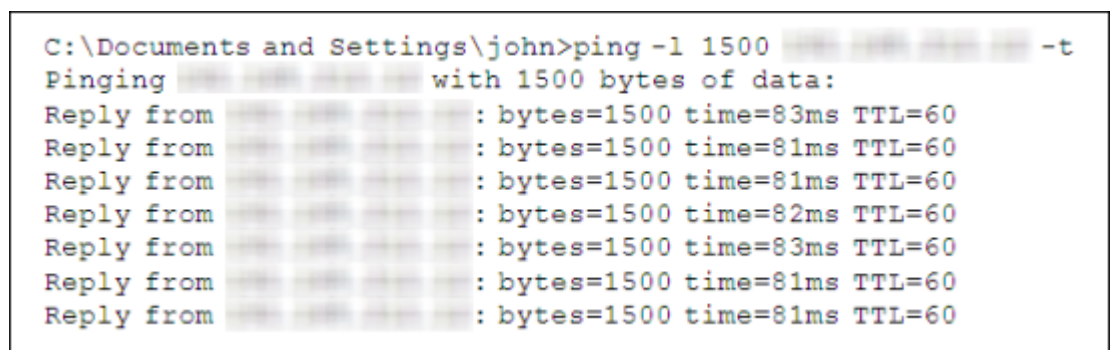
Solution Perform the procedure described in this section.

During this procedure a ping test is used to monitor connection general performance, although the ping test uses ICMP packets and not RTP packets used in video/audio protocols.

As part of this troubleshooting procedure, you check the general performance of the connection between the MCU and the endpoint.

Procedure

1. Connect a PC to the network segment to which the endpoint belongs.
2. Open a command line window.
3. Enter this command:
`ping -l 1500 <MCU remote IP address> -t`
4. Monitor the router response for at least 20 minutes.



```
C:\Documents and Settings\john>ping -l 1500 10.10.10.10 -t
Pinging 10.10.10.10 with 1500 bytes of data:
Reply from 10.10.10.10: bytes=1500 time=83ms TTL=60
Reply from 10.10.10.10: bytes=1500 time=81ms TTL=60
Reply from 10.10.10.10: bytes=1500 time=81ms TTL=60
Reply from 10.10.10.10: bytes=1500 time=82ms TTL=60
Reply from 10.10.10.10: bytes=1500 time=83ms TTL=60
Reply from 10.10.10.10: bytes=1500 time=81ms TTL=60
Reply from 10.10.10.10: bytes=1500 time=81ms TTL=60
```

Figure 75: Example of a Router Response in a Ping Test

5. To display the statistics, press CTRL + Space.

```
Ping statistics for 192.168.1.100:
  Packets: Sent = 65, Received = 65, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 80ms, Maximum = 91ms, Average = 82ms
Control-Break
```

Figure 76: Example of Router Statistics as Displayed in the Ping Test

Press CTRL+C to hide the statistics.

6. Use the router response to perform the following:
 - a. Verify that there is no packet loss.

The packet loss that is higher than 1-2% causes poor video quality.
 - b. Verify that the steady jitter (the difference between the minimum and maximum round trip times) is not higher than 30-50 msec.
 - c. Verify that the minimal delay (round trip time) for QoS-tagged packets is not higher than 300-400 msec.
7. Close the command line window.
8. Verify that enough bandwidth is dedicated to videoconferencing traffic and this bandwidth is available at all times.
9. Verify that there is enough bandwidth for daily activity traffic on WAN IP links apart from bandwidth dedicated to videoconferencing.
10. Use a network sniffing application to perform the following:
 - Verify that the one-way delay is not higher than 100-150 msec.
 - Verify that the delay is the same for both directions.
11. Verify that the Auto Negotiation preferred setting is selected for all routers and switches working in 100 Mbit/Full Duplex mode.
12. Verify that the MCU LAN ports are synchronized with the switch:
13. In deployments using a Scopia Gateway, verify that the Scopia Gateway LAN ports are synchronized with the switch:
 - a. Connect a PC to the Scopia Gateway.
 - b. Open a command line window.
 - c. Enter the sysLanStatusGet command to check the port status.
 - d. Enter the motFccErrorShow command to check that there are no CRC errors.
14. Verify that 10 Mbit/Half Duplex hubs are not used for videoconferencing traffic.
15. Verify that synchronization of the LAN endpoints with the LAN switches is set to 100 Mbit/Full Duplex.
 - a. Access the MCU administrator web interface.
 - b. Select the **Configuration** tab  Configuration.

The Setup tab is displayed.

- c. In the **Network** section, verify that the **Port settings** field is set to either the **Auto (Up to 1 Gbps/Full Duplex)** or **100 Mbps/Full Duplex** option.

The screenshot shows the 'Network' section of the 'Advanced IP Configuration' tab. It includes sections for IPv4 and IPv6 addresses, DNS settings, and port settings. The IPv4 section is expanded, showing fields for Primary IP address (172.16.88.125), Secondary IP address (172.16.88.132), Router IP (172.16.88.254), and Subnet mask (255.255.255.0). The IPv6 section is collapsed. The DNS suffix is empty. DNS server 1 is 172.16.2.115 and DNS server 2 is 172.16.2.114. The Port settings are set to 'Auto (Up to 1 Gbps/Full Duplex)'.

Section	Field	Value
IPv4 Address	Primary IP address	172.16.88.125
	Secondary IP address	172.16.88.132
	Router IP	172.16.88.254
	Subnet mask	255.255.255.0
IPv6 Address	Primary IP address	::0
	Secondary IP address	::0
	Router IP	::0
DNS	DNS suffix	
	DNS server 1	172.16.2.115
	DNS server 2	172.16.2.114
Port settings	Port settings	Auto (Up to 1 Gbps/Full Duplex)

Figure 77: Network Section of the Setup Tab

16. Verify that the MCU Quality of Service (QoS) settings are correct:
- In the **Setup** tab of the MCU administrator web interface, scroll down to the **QoS** section.
 - Select **More**.

The **QoS** section is displayed.

Figure 78: QoS Section of the Setup Tab

- c. Select **Custom**.
- d. Enter 34 in all fields.
- e. Select **Apply**.

17. Verify that the bandwidth on the WAN IP links dedicated to the videoconferencing traffic is enough.
18. On Cisco routers, make sure the assured forwarding policy is set to 41.

Resolving Poor Audio Quality

Problem The quality of a participant's audio received in a conference is poor.

Possible Causes Interoperability issues: an incorrect video format used by an endpoint or incorrect logical channel negotiation

Solution Perform the procedure in this section:

Procedure

1. Make a point-to-point call without Radvision products to verify that there are no issues related to endpoints used in a conference. In case there are problems related to endpoints, use the endpoint documentation to troubleshoot them.
2. If the problem is not endpoint-related verify that perform verification depending on the kind of endpoint used in the conference:
 - For a SIP endpoint, verify that both the MCU and the endpoint are properly registered with the SIP proxy.
 - For an H.323 endpoint, verify that both the MCU and the endpoint are properly registered with the ECS.

- For a 3G endpoint, verify that both the MCU and the endpoint are properly registered with SIP proxy and/or the ECS.

3. If registration is correct, collect logs and wireshark traces to Radvision Customer Support.

Resolving a Video Display Issue

Problem The video for a conference participant is not displayed in a conference view.

Possible Causes

- Interoperability issues: an incorrect video format used by an endpoint or incorrect logical channel negotiation
- Issues related to a camera or cables
- The media ports are blocked on the firewall

Solution If the problem is caused by interoperability issues, perform the procedure in this section:

Procedure

1. Make a point-to-point call without Radvision products to verify that there are no issues related to endpoints used in a conference. In case there are problems related to endpoints, use the endpoint documentation to troubleshoot them.
2. If the problem is not endpoint-related verify that perform verification depending on the kind of endpoint used in the conference:
 - For a SIP endpoint, verify that both the MCU and the endpoint are properly registered with the SIP proxy.
 - For an H.323 endpoint, verify that both the MCU and the endpoint are properly registered with the ECS.
 - For a 3G endpoint, verify that both the MCU and the endpoint are properly registered with SIP proxy and/or the ECS.
3. If registration is correct, collect logs and wireshark traces to Radvision Customer Support.

Solution If the problem is caused by the camera-related or cable-related issues, verify that the camera is connected properly.

Solution If the problem is caused by incorrect firewall configuration, open the necessary media ports on the firewall. Refer to the *Port Security Reference Guide* for information about ports.

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