SCOPIA Elite 5100 Series MCU

Administrator Guide

Version 7.7

1 Table of Contents

1 About the SCOPIA Elite MCU

The SCOPIA Elite MCU enables multimedia, multiparty collaboration in applications such as group conferencing, distance learning, training and video telephony. The MCU supports multimedia, multiparty communications in the board room, at the desktop, in the home, or on the road over wireless.

Main Features of the SCOPIA Elite MCU

The SCOPIA Elite MCU is a hardware unit which houses videoconferences from multiple endpoints, both H.323 and SIP. It includes many powerful features including:

- Video processing

  Video and audio processing is carried out per user rather than per conference. 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.

- Seamless interoperability

  The MCU is built on the solid foundation of RADVISION's H.323 and SIP software, ensuring full compliance and unmatched interoperability with IP, ISDN, and 3G networks.

  The MCU unites H.323 and SIP devices in the same conference session.

  When used with the series of SCOPIA Gateways, the MCU also enables ISDN, V.35, and 3G handsets to participate in the same conference session. See Figure 1-1 on page 2.

Figure 1-1 Various devices are used in the same conference
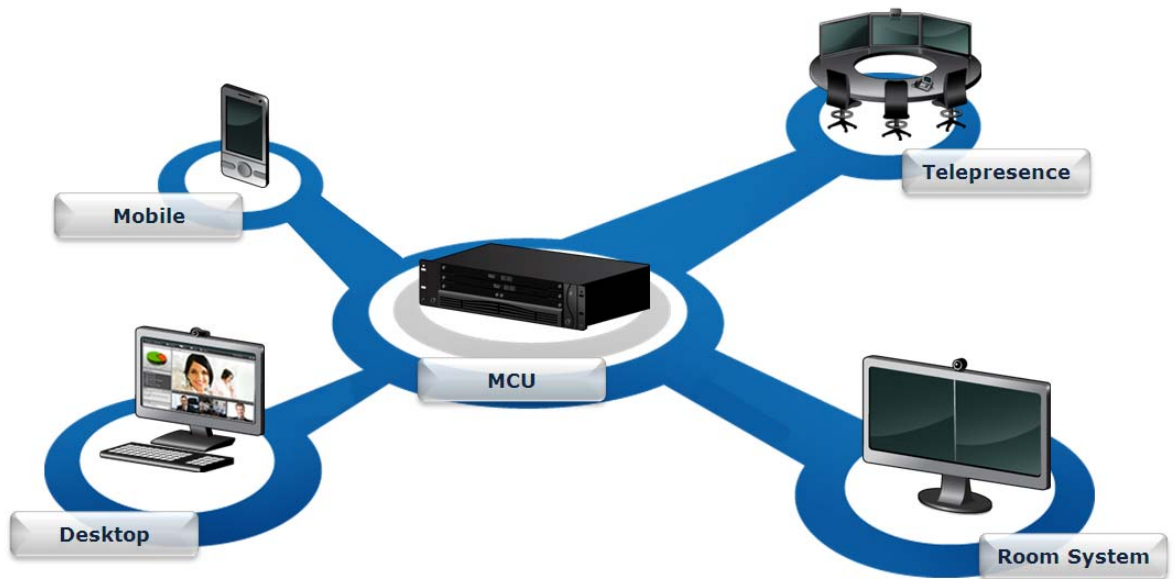
- Seamless interoperability with leading telepresence systems

  The MCU can easily connect to telepresence systems and combine them with regular videoconferencing systems, even within the same call. The MCU is compatible with telepresence systems from Cisco, Tandberg, Polycom, and LifeSize/Logitech. Enhanced video layouts were specifically designed for telepresence systems.

Note: Cisco telepresence systems can participate in conferences, but only as regular endpoints. Full telepresence functionality is not supported for Cisco telepresence systems.

- SIP and H.323-based content sharing

  The 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 a SIP or H.323 endpoint to share content such as presentations, spreadsheets, documents, and movies.

- Video quality

  The MCU delivers high quality video and audio processing, using latest industry standards and upgradeable DSP chip software. This state-of-the-art video quality is supported by:

  - H.264 SVC error resiliency

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

    The FEC component improves video quality and reduces the number of video freezes in packet loss conditions.

  - Error concealment mechanism: Maintains video quality when 3rd party endpoints are connected to the MCU over lossy networks.

  - High definition and standard definition participants in the same conference.

- A choice of 24 video layouts

- H.263 and H.264 in the same conference

- Resolutions from QCIF to 1080p in the same conference

- Framerate of up to 60 fps for 720p resolution and 30 fps for other resolutions

- Up to 12Mbps on each stream without affecting capacity

- MCU's bandwidth estimation package improves call quality over Internet connections. The available bandwidth is estimated at the beginning of each call and adjusts accordingly during the call.

- Security and privacy

  The MCU features administrator and operator password protection for accessing the MCU web interface. It also features optional PIN protection for joining a conference and web access, and additional PIN protection for conference Moderator Control.

  To achieve secure communication with endpoints, the MCU uses H.235-based encryption for H.323 endpoints and SRTP and TLS encryption for SIP endpoints.

  The SCOPIA Elite MCU is certified by the Joint Interoperability Test Command (JITC).

- Intuitive web-based management and control

  Both the MCU system and actual conference sessions are managed, configured, and dynamically modified through an intuitive, web-based interface that offers easy, high-level conference control and administrative flexibility for an enhanced user experience.

- Unlimited number of conferences

  The number of supported conferences depends on the number of ports provided by your license. The SCOPIA Elite MCU supports a dynamic port capacity that enables extra calls to be connected even after maximum call capacity is reached. By downspeeding existing 1080p calls to 720p, the MCU can accept additional calls within a single meeting.

  Participants defined as VIP users in SCOPIA iVIEW Management Suite will not have their resolution downspeeded.

- In-meeting indicators

  A range of messages and icons are displayed on the endpoint monitor during conferences when certain events occur. For example, conference participants are notified when a participant joins or leaves a conference, an audio-only participant speaks, or a participant's personal video layout changes.

- Personal layouts per participant

  You can choose from 24 video layouts for each conference participant. You can view up to 28 participants on your screen.

- Single LAN connection

  Only a single Ethernet connection is required for the entire MCU chassis. The connection is via the upper blade. The upper Media Blade manages the platform, including call signaling and processing, application interface, network management, and audio and video processing.

- Snapshot files for Customer Support

  One-click creation of a file of bundled logs and configuration files which you can send to Customer Support for debugging.

- In-conference control

  During a conference, 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 displayed on top of the video layout.

- Optional no self see

  The no self-see (NSS) option is enabled by default, but can be disabled with an advanced command. This feature enables more effective use of the video screen.

- Interactive Voice Response (IVR) messages

  The MCU includes pre-recorded greetings to conference participants and announcements as each new participant joins the conference. You can record messages to provide custom greetings and announcements.

Note: If your MCU deployment includes iVIEW Management Suite, use the IVR from your iVIEW Management Suite.

- Video switching

  The MCU supports the switching of HD resolutions 720p and 1080p at the capacity of up to 120 calls, depending on the video resolution and call bitrate. Video switching is available for H.264 and H.261 video codecs.

  When using switched video, all endpoints in the conference must support the same resolution. If a network experiences high packet loss, switched video might not be displayed properly for all endpoints in the conference.

- Dual NIC support

  The MCU enhances security within the enterprise by routing media and management traffic to two different subnets. For more information, see the Configuring a Dual NIC MCU section in the *Installation Guide of SCOPIA Elite MCU*.

- Recording via moderator menu

  Moderators can record meetings using the MCU moderator menu.

Note: This feature is only relevant if your SCOPIA Desktop deployment includes the recording option.

Technical Specifications

This section lists important data about the system 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.

- System power requirements:
  - 90-264VAC input, 50/60Hz
  - Single 400W AC power supply (default) / 48V DC power supply
  - Power consumption of a media blade: max. 250W (50°C)
  - Power consumption of an MCU including the chassis, control blade, and AC power supply: max. 85W (50°C)
  - Power consumption of an MCU including the chassis, control blade, two media blades and AC/DC power supply: AC 700VA (50°C), DC 585W (50°C)
  - Maximum power consumption: DC 335W (50°C), AC 392VA (50°C)
  - Heat dissipation: BTU/Hr (50°C)1445 BTU/Hr (50°C)
- Grounding and electrostatic discharge:
  - External 4mm grounding stud per TUV requirement
- Environmental requirements:
  - Operating temperature: 0°C to 45°C (32°F to 113°F)
  - Humidity: 5% to 90% non-condensing
  - Storage and transit temperature: -25°C to 70°C (-13°F to 158°F), ambient
  - Acoustics: 56dBA
- Physical dimensions:
  - Size: 448mm (17.6″) width x 133.35mm (5.25″) height x 400mm(15.75″) depth
  - Size: 448mm (17.6″) width x 44mm (1.73″) height x 480mm (18.9″) depth
  - Weight: ~13kg (~28.7lbs)
- Signaling protocols:
  - H.323
  - SIP
  - H.320 (in conjunction with SCOPIA H.320 Gateways)
  - H.324M (in conjunction with SCOPIA 3G Gateways)
- Audio support:
  - Codecs—G.711. G.722, G.722.1, G.729, MPEG4 AAC-LC, 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 30fps
  - Video with 720p resolution is sent and received at up to 60fps

- Codecs—H.261, H.263, H.263+, H.264, H.264 SVC

- Live video resolutions—QCIF up to 1080p

- Presentation video resolution—VGA, SVGA, SXGA, 720p, 1080p, WUXGA

- Video bandwidth—up to 12Mbps for 1080p resolutions and up to 6Mbps for 720p or lower

- Call capacity:

  See Table 1-1 on page 6 for the list of MCU call capacity licenses.

  - If you have the Increased Capacity license option installed, the MCU should be pre-configured to either X2 or X4 capacity:

    If you enable X2 capacity, resolutions of 480p and lower use only half a port, while higher resolutions use 1 port (except for 1080p, which uses 2 ports).

    If you enable X4 capacity, resolutions of 352p use 1/4 a port, and higher resolutions use 1 port (except for 1080p, which uses 2 ports).

    For more information, contact Customer Support.

  - If you do not have the Increased Capacity license option, resolutions of 720p and lower use 1 port, and resolutions of 1080p use 2 ports.

Note: By default, all conferences are in Continuous Presence mode, which supports different layouts and endpoints with various resolutions.

To increase your call capacity, you can configure your conference for video switching (see the Configuring the Conference Mode section in the *Administrator Guide of SCOPIA Elite MCU*).

Table 1-1   Call Capacity

Call Resolution	Ports per Call	SCOPIA Elite MCU 5105 (1U) Capacity	SCOPIA Elite MCU 5110 (1U) Capacity	SCOPIA Elite MCU 5115 (1U) Capacity
Basic Product Capacity				
HD (1080p) continuous presence	2 ports per call	3 ports	5 ports	7 ports
HD (720p) continuous presence	1 port per call	5 ports	10 ports	15 ports
HD video switching	1/4 - Four times the number of calls	20 ports	40 ports	60 ports
Increased Capacity License option				
ED (480p) continuous presence (if X2 capacity is enabled)	1/2 - Double the number of calls	10 ports	20 ports	30 ports
ED (352p) continuous presence (if X4 capacity is enabled)	1/4 - Four times the number of calls	20 ports	40 ports	60 ports

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:

Planning your Distributed or Centralized Topology for MCU

When your organization has more than one site, like a headquarters and several branches, RADVISION offers a unique method of cutting video bandwidth costs. Administrators can choose whether to place all MCUs centrally in the headquarters (Figure 2-1 on page 8), or they can opt for a distributed deployment, where multiple MCUs are spread over multiple sites (Figure 2-2 on page 9).

Centralized MCU deployments can be expensive for frequent conferences between branches with multiple participants from each site, since each participant must utilize extra bandwidth on the WAN connection between sites (Figure 2-1 on page 8).

Figure 2-1 Centralized MCU deployment, where all branches use the HQ MCU
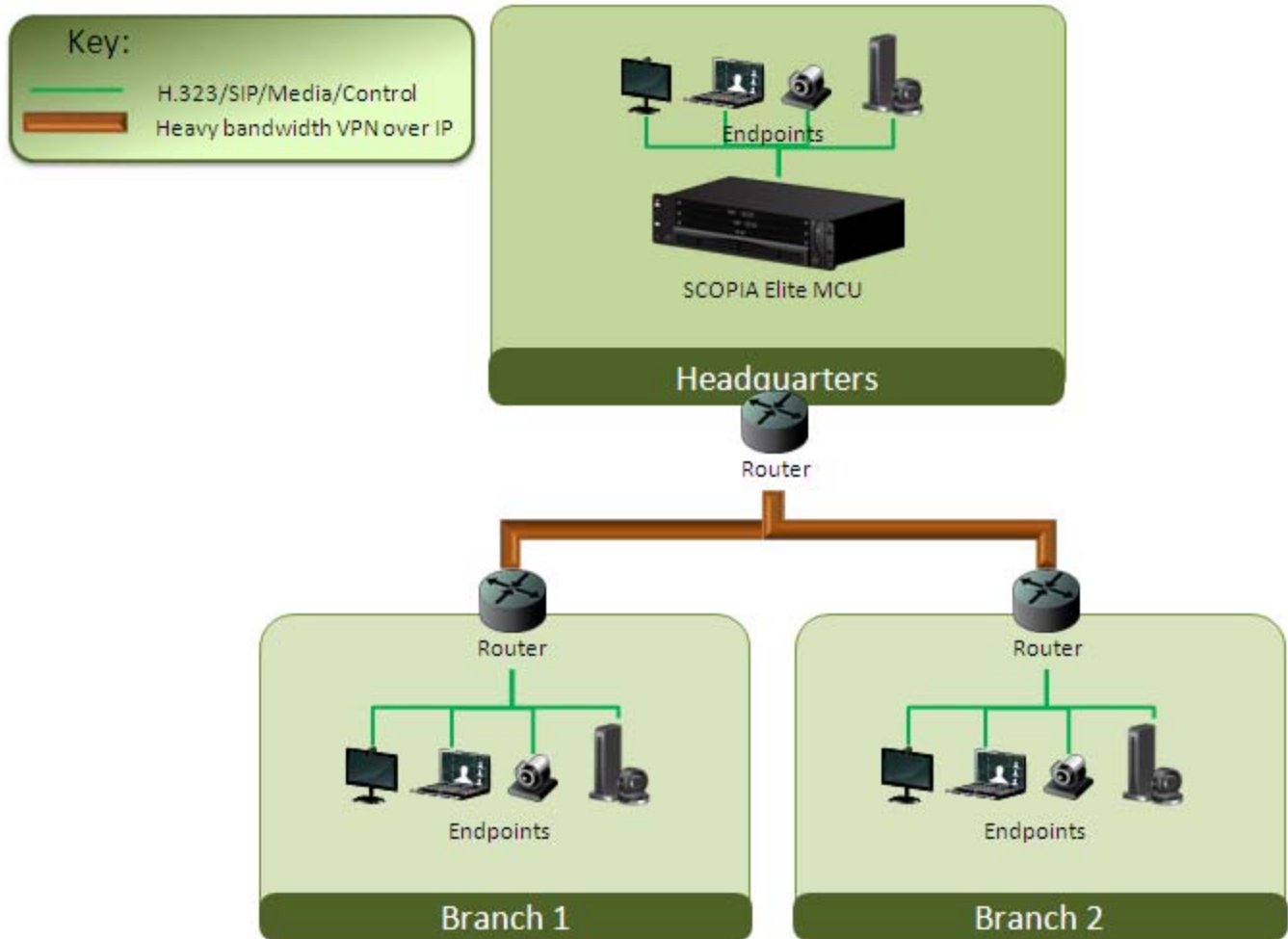
To reduce cross-site bandwidth costs, a distributed MCU deployment (Figure 2-2 on page 9) can perform cascaded conferences, where local participants connect to their local MCU, and the conference is cascaded by connecting between the MCUs using a fraction of the bandwidth compared to the centralized deployment.

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.

Figure 2-2 Distributed MCU deployment enabling reduced WAN bandwidth
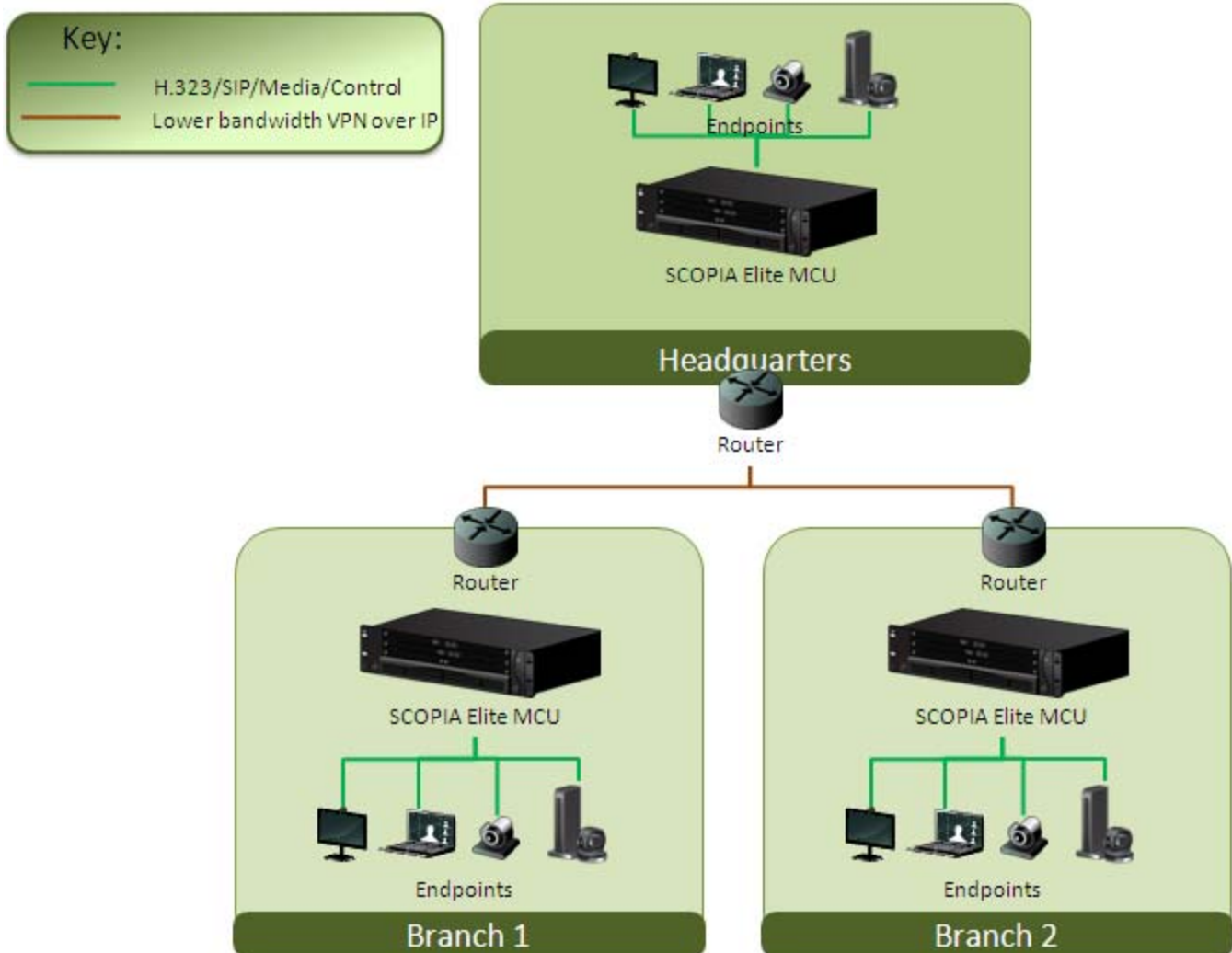
SCOPIA iVIEW Management Suite's sophisticated cascading algorithms enable administrators to customize the priority given to cascading in a distributed topology.

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.

The priorities of cascading can be customized 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 details on configuring cascading conferences, see the *Administrator Guide for SCOPIA iVIEW Management Suite*.

Ports to Open for the SCOPIA Elite 5100 Series MCU

The SCOPIA Elite 5100 Series MCU is typically located in the enterprise network and is connected to the DMZ. When opening ports on the SCOPIA Elite 5100 Series MCU, use the following as a reference:

- If you are opening ports that are both in and out of the SCOPIA Elite 5100 Series MCU, see Table 2-1.
- If you are opening ports outbound from the SCOPIA Elite 5100 Series MCU, see Table 2-2.
- If you are opening ports inbound to the SCOPIA Elite 5100 Series MCU, see Table 2-3.

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

Table 2-1   Bidirectional Ports to Open on the SCOPIA Elite 5100 Series MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
1024-1324	H.245 (TCP)	Any H.323 device	Enables H.245 signaling	Cannot connect H.323 calls	Mandatory To configure, see "Configuring the TCP Port Range for H.245 on the SCOPIA Elite MCU" on page 35
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 37 and "Configuring the UDP Port for the Gatekeeper on the SCOPIA Elite MCU" on page 38
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 39

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3336	XML (TCP)	Conference Control web client endpoint, iVIEW Management Suite, 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 iVIEW Management Suite
3337	XML (TCP)	Other MCUs	Enables use of MCU Cascading XML API	Cannot cascade between two MCUs	Mandatory if multiple MCUs are deployed with iVIEW Management Suite
3338	XML (TCP)	iVIEW Management Suite, 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 iVIEW Management Suite
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 40
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 40
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 "Limiting the UDP Port Ranges for RTP/RTCP on the SCOPIA Elite MCU" on page 33

Table 2-2   Outbound Ports to Open from the SCOPIA Elite 5100 Series MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
162	SNMP (UDP)	iVIEW Network Manager, iVIEW Management Suite, or any SNMP manager station	Enables sending SNMP Trap events	Cannot send SNMP Traps	Recommended

Table 2-3   Inbound Ports to Open to the SCOPIA Elite 5100 Series MCU

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
21	FTP (TCP)	FTP Server	Enables audio stream recording	Cannot record audio streams	Optional
22	SSH (TCP)	SSH Client	Enables you to view logs	Cannot view logs in real-time (logs are collected on the compact flash card)	Optional
80	HTTP (TCP)	Web client	Provides access to the MCU Administrator and 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 36
161	SNMP (UDP)	iVIEW Network Manager, iVIEW Management Suite, or any SNMP manager station	Enables you to configure and check the MCU status	Cannot configure or check the MCU status	Recommended
443	HTTPS (HTTP over SSL)	Web client	Provides secure access to the MCU Administrator and Conference Control web user interfaces; used for software upgrade	Cannot configure MCU	Mandatory if using HTTPS

3 Maintaining the SCOPIA Elite 5100 Series MCU

Securing MCU and iVIEW Management Suite 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 iVIEW Management Suite, 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.

Securing MCU with TLS in a SIP Environment

The first step to allow a secure connection between MCU and iVIEW Management Suite 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).

Procedure

Step 1   Log in to the MCU.

Step 2   Select **Enable SIP Protocol**.

Step 3   Select **Specify**.

Step 4   Set the **IP address** as the IP address of the iVIEW Management Suite server.

Step 5   Set **Port** to the same port defined in iVIEW Management Suite. The default value is **5061**.

Step 6   Set **Type** as **TLS**.

Figure 3-1   Enabling the SIP Protocol on the MCU

**Step 7**   Restart the MCU.

Uploading TLS Certificates

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.

Procedure

Step 1   Log in to the MCU.

Step 2   Select **Configuration**.

Step 3   Select **Manage** in the Security section.

Figure 3-2   Security Section
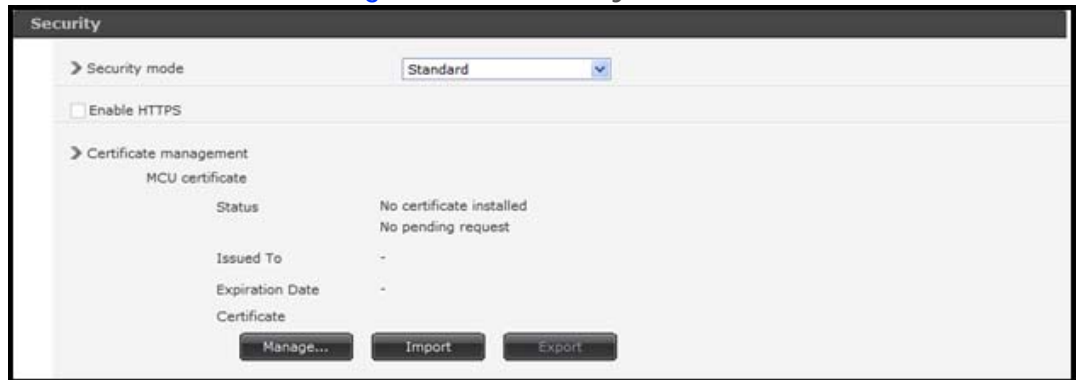
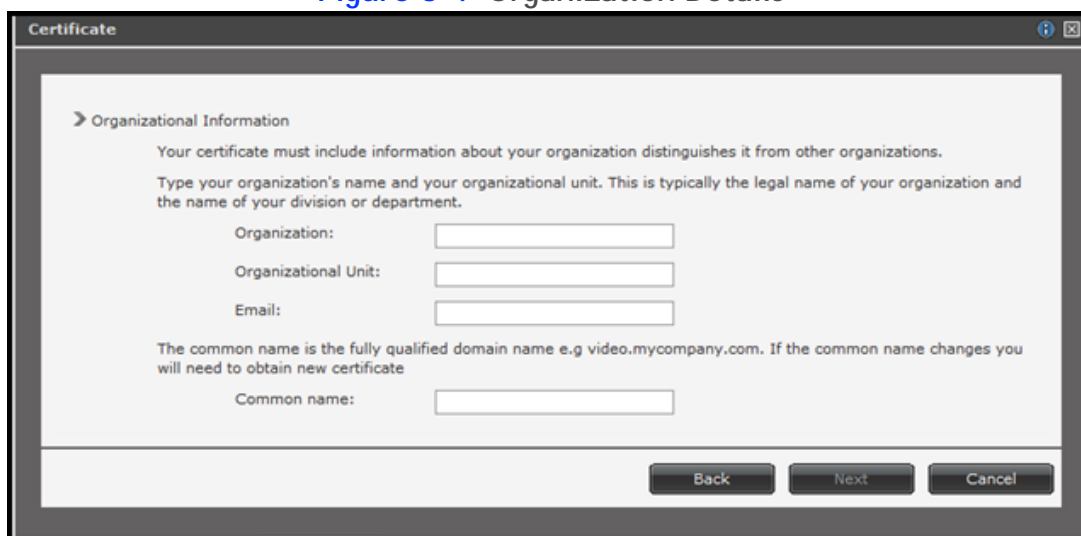**Step 4**   Select **Create a new certificate request**. For example:

Figure 3-3   Create New Certificate Request

Step 5   Select **Next**.

Step 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)

Figure 3-4 Organization Details

Step 7   Select **Next**.

Step 8   Enter the geographical information as required. For example:

- Issued To: Company_Name
- Country/Region: United States
- State/Province: New York
- City/Locality: New York

Step 9   Select **Next**.

The Certificate Request Summary appears.

Figure 3-5 Certificate Request Summary
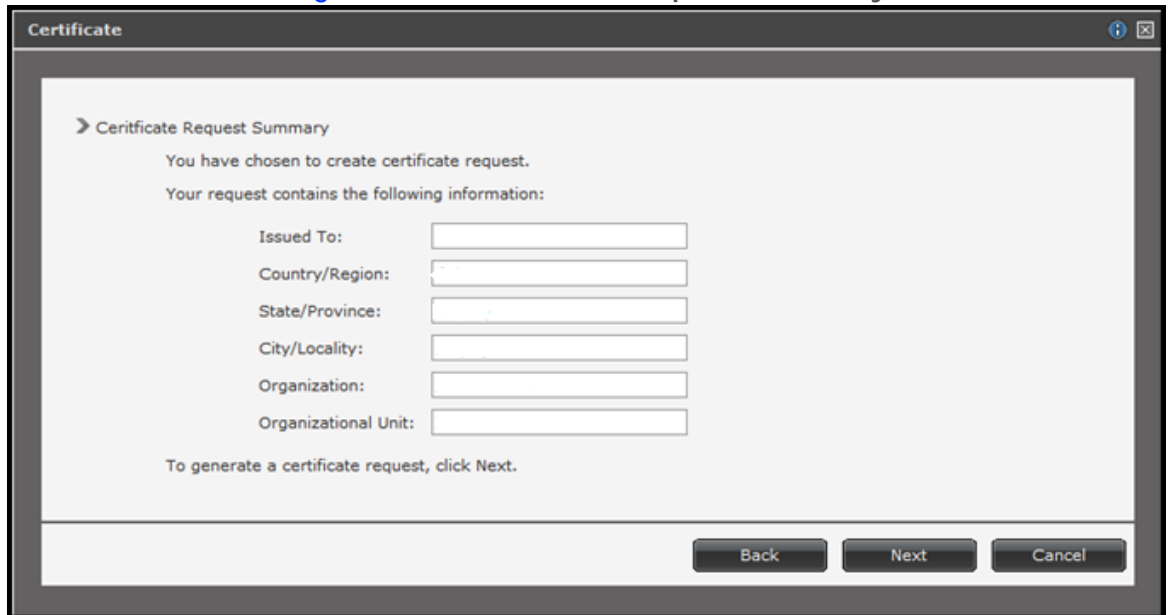
Step 10   To generate a certificate request, select **Next**. Copy certificate request text in text area and paste it to a file. For example, mcu_ca_request.txt.

Figure 3-6 Save Certificate Request
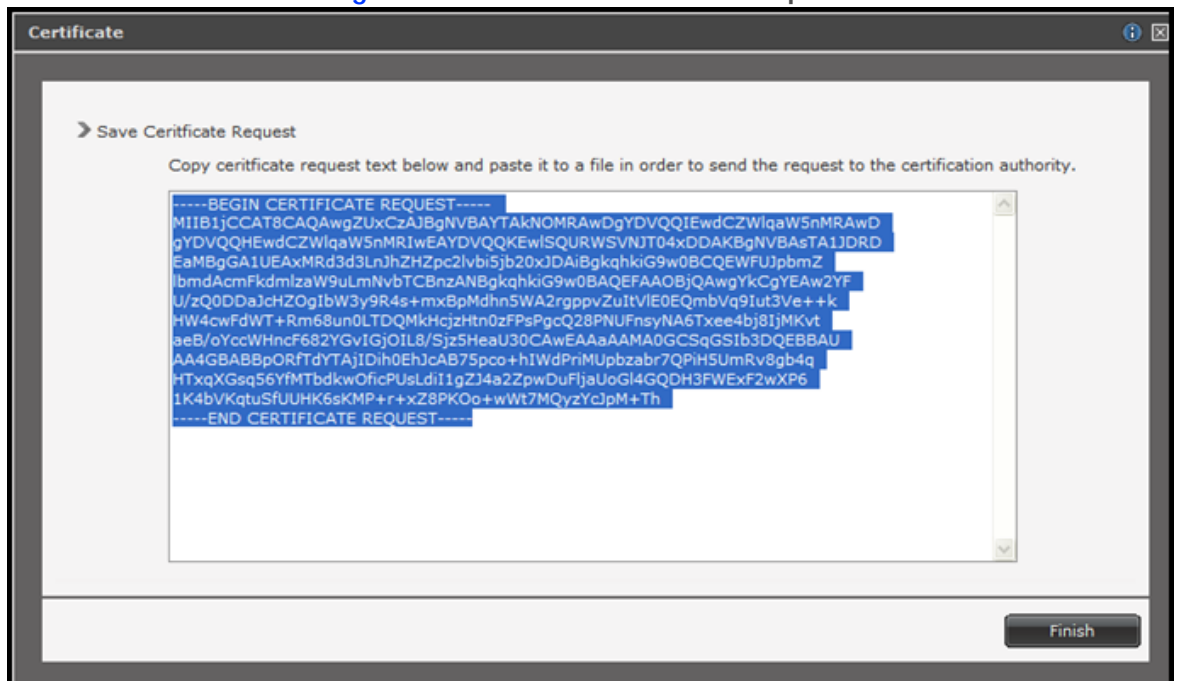
Step 11 Submit this file to your Certification Authority (CA) by e-mail or any other method supported by your organization for your Enterprise CA.

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:

Step 12 Select **Manage**.

Step 13 Select **Process the pending request and install the certificate**.

Figure 3-7 Certificate Status
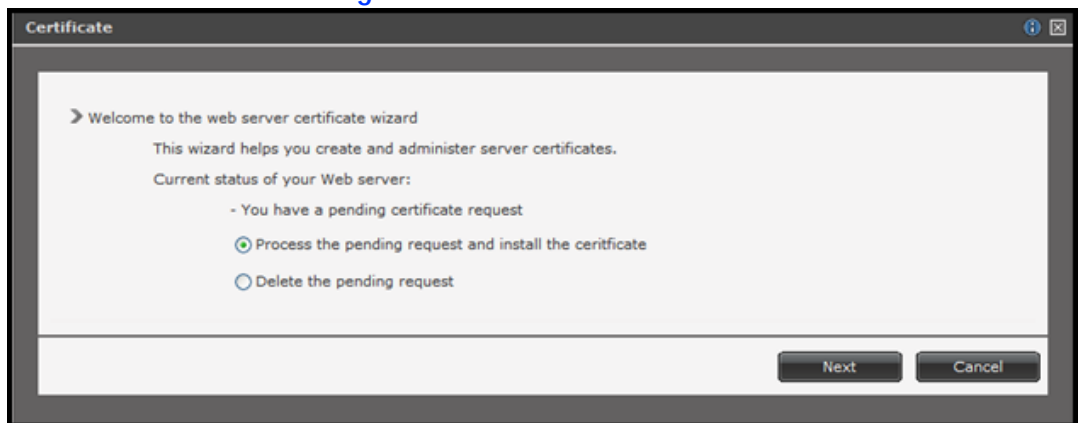
Step 14 Select **Next**.

Step 15 Open the signed certificate, and copy-paste the content of the signed certificate.

Figure 3-8 Process a Pending Request

Step 16 Select **Next**.

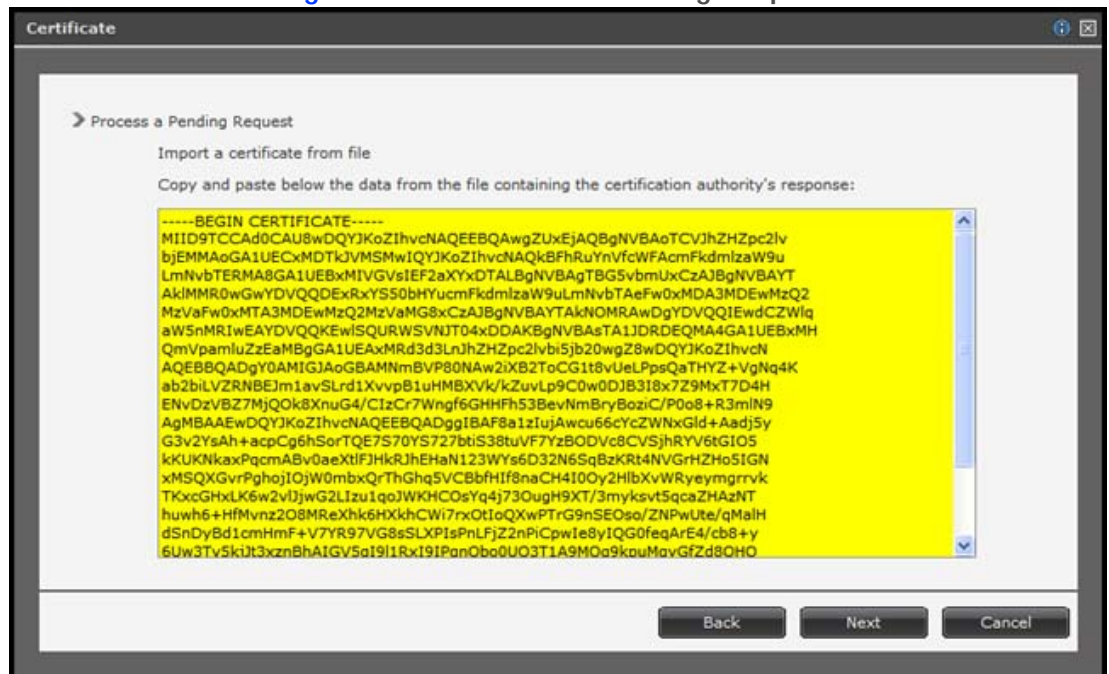**Step 17**   If data is correct, select **Finish** and the MCU certificate is uploaded successfully. If the data is not correct, select **Back** to enter the correct data.

Figure 3-9 Successful Certificate Upload
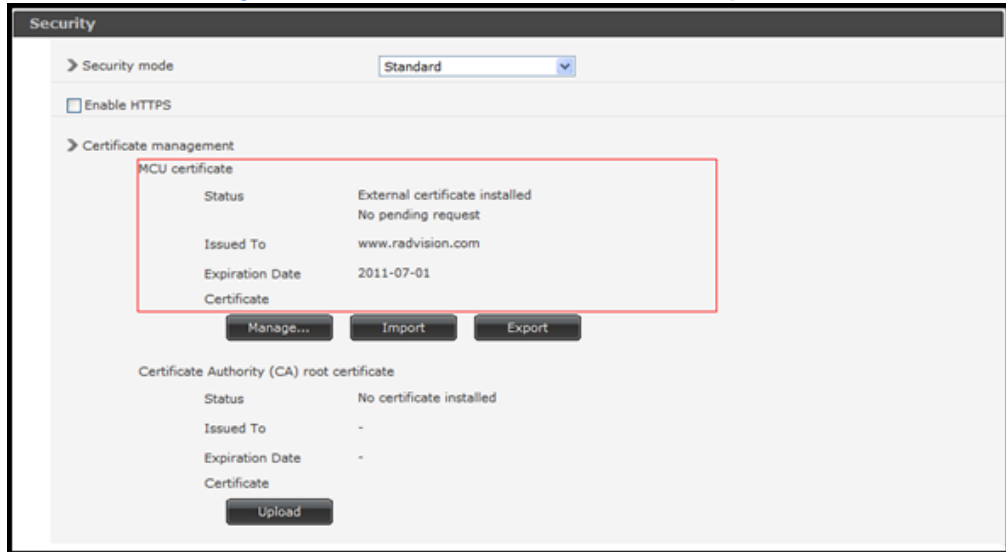
Step 18   Upload the CA root certificate by selecting **Upload** from the Security section.

Step 19   Select **Browse** to select the CA root certificate.

Figure 3-10 Browse for the CA Root Certificate

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

Regulating Bandwidth Usage

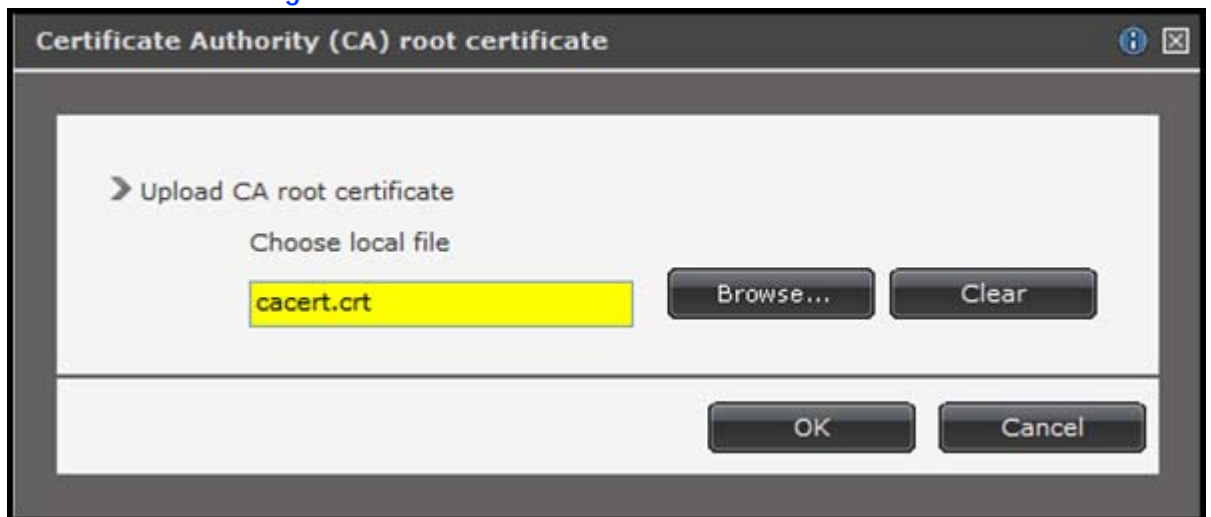Depending on your network capacity, you may need to adjust bandwidth usage by defining how much bandwidth each call will require.

Procedure
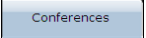
Step 1   Select **Configuration** [Configuration] .

Step 2   Select **Conferences** [Conferences] .

Step 3   Locate the Services list section.

Figure 3-11 Service List Section of the Conferences Tab

Step 4   Select the **Review** button [⌄] next to the service.

Step 5   Select the required value from the list under **Max call rate (Kbps)**.

Figure 3-12 Service Settings Section

Step 6   Select **Apply**.

Configuring the Conference Mode

The default conference mode is Continuous Presence. To increase your call capacity or conserve bandwidth, you can configure a service to apply one of the following conference modes to your conference:

- Audio only
- Switched video

Procedure

Step 1   Select **Configuration** [Configuration] .
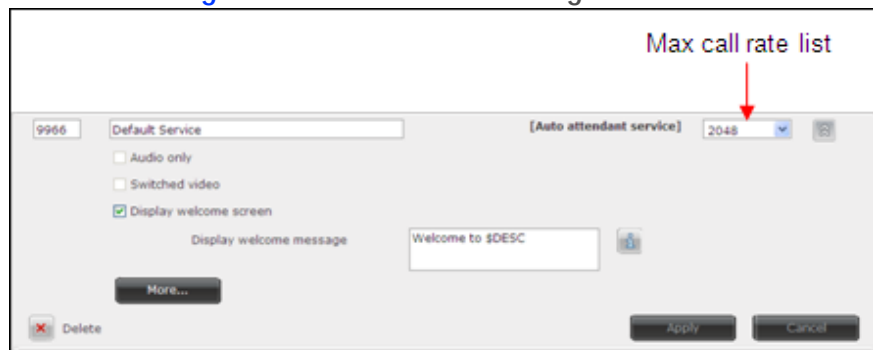
Step 2   Select **Conferences** [Conferences] .

Step 3   Locate the **Services List** section.

Figure 3-13   Service List Section of the Conferences Tab

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

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

Step 5   Select one of the following conference mode options (see Figure 3-14 on page 22):

- **Audio only**: This conference does not contain any video and therefore requires less bandwidth.
- **Switched video**: The video displayed in this conference is not processed by the MCU and therefore only supports a single screen layout with the active speaker, and cannot display video on endpoints with varying resolutions and codecs. If a network experiences high packet loss, switched video might not be displayed properly for all endpoints in the conference.Video switching enables you to have a higher HD call capacity.

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

Figure 3-14 Service Setting Section
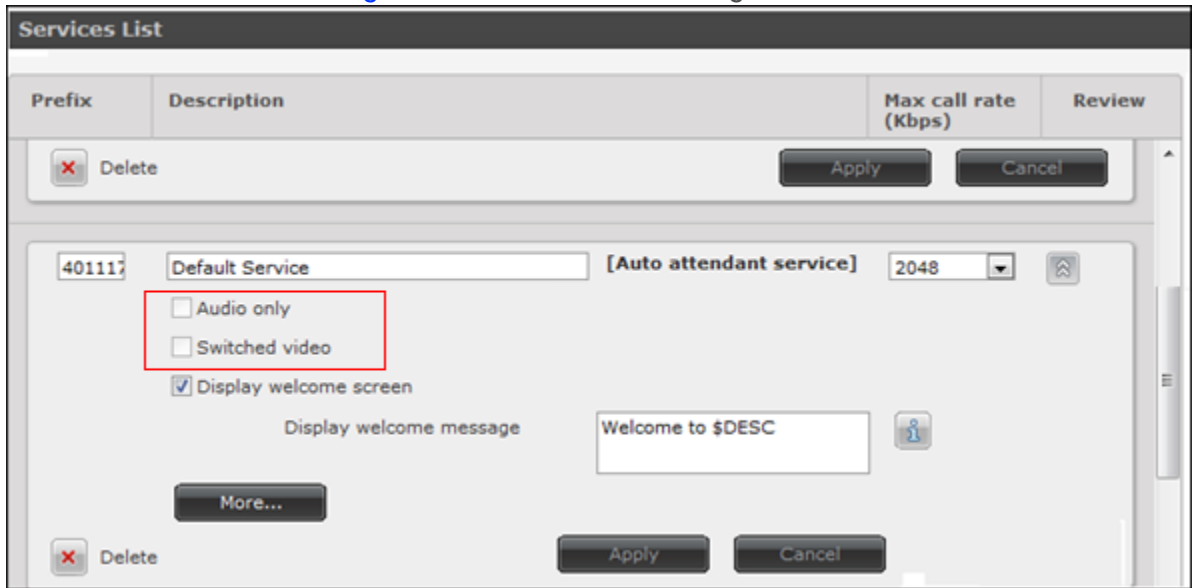
Step 6   Select **Apply**.

Configuring the Auto Attendant Service

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 then either create a new conference or join a conference currently hosted at this MCU.

Procedure
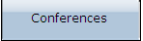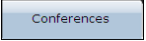
Step 1   Select **Configuration** [Configuration].

Step 2   Select **Conferences** [Conferences].

Step 3   Locate the **Services List** section.

Figure 3-15 Service List Section of the Conferences Tab

Step 4   Select **Review** [⌄] for the service you want to use as the auto attendant service.

Step 5   Select the **Set as the Auto attendant service** link.

Figure 3-16 Service Setting Section
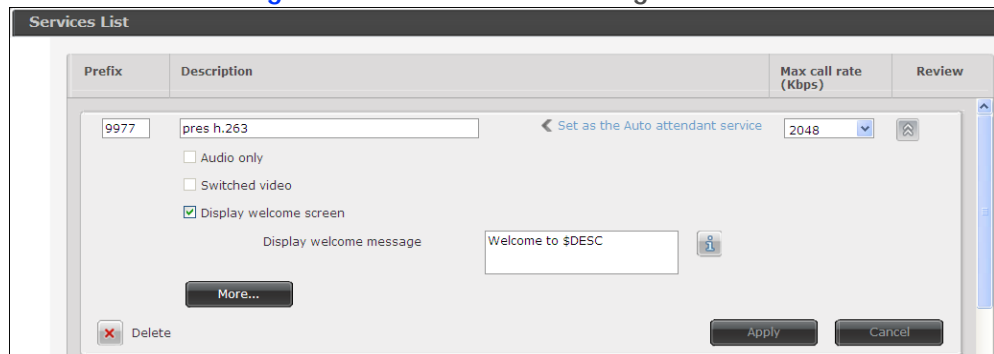
Step 6   Select **Apply**.

Customizing the Logo Displayed in MCU Conferences

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

Procedure

Step 1   Select **Configuration** [Configuration] .

Step 2   Select **Customization**.

Step 3   Locate the **Images pack** area ().

Figure 3-17 Customizing the Images Pack
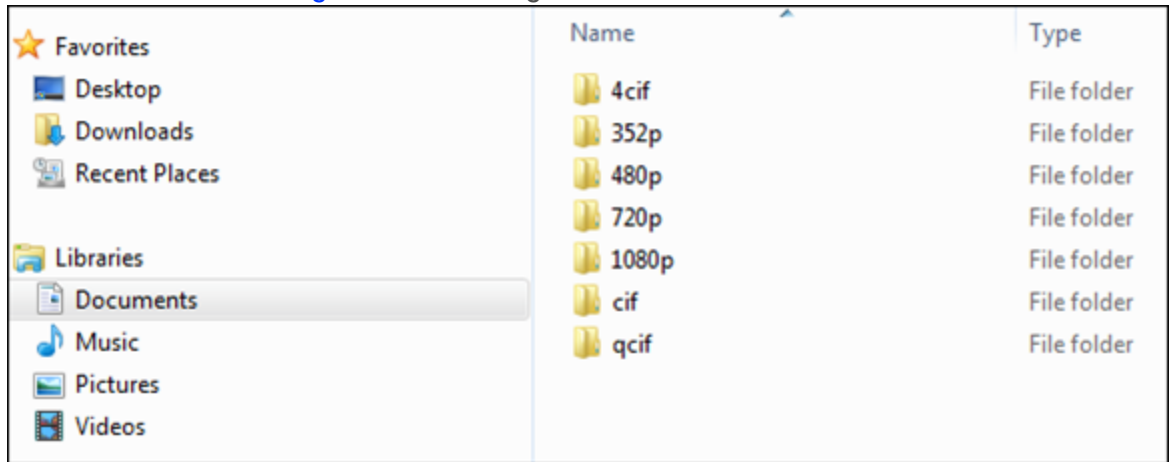
Step 4   Select **Save** and save the .zip file with the current images to your local drive.

Step 5   Navigate to the location where you saved the .zip file.

Step 6 Add your logo image to each folder, as follows:

Note: 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 3-18 on page 24). 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.

Figure 3-18 Image Pack Folder Structure

a.   Ensure that your logo image has the correct dimensions (see Table 3-1 for the requirements).

Table 3-1   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

Step 7   Update the Image pack file by selecting **Browse** and navigating to your updated .zip file.

Step 8   Select **Apply**.

Step 9   Select the ⚒▾ icon.

Step 10   Select **Advanced Parameters**.

Step 11   Locate the **Default vendor logo** in the **Name** column (see Figure 3-19 on page 25).

Figure 3-19 Advanced Commands Section
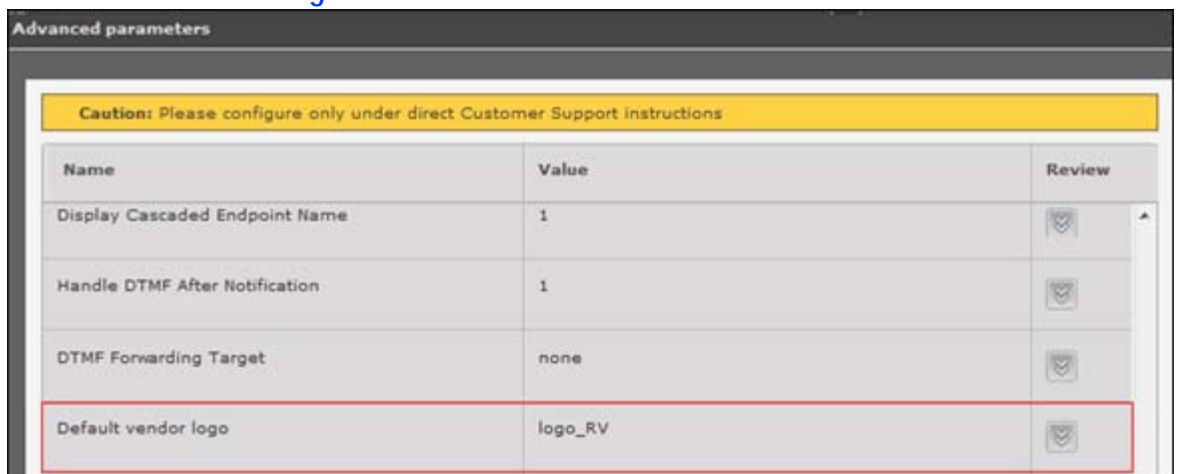
Step 12   Select the ⌄ icon in the **Review** column.

Step 13   Enter the filename of the logo you added in Step 6.

Step 14   Select **Apply**.
Step 15   Select **Close**.

How to Manage SCOPIA Elite MCU User Profiles

Only administrators can manage MCU user profiles.

About SCOPIA Elite MCU User Types

There are two types of users who can access the SCOPIA Elite MCU administration interface: administrators and operators.

As an administrator, you have these privileges:

- Full access to the MCU Administrator interface.
- Full Operator-level access to the Conference Control interface.
- SSH access to the MCU.
- You can assign Administrator authorization to up to ten users.

As an operator, you have these privileges:

- Access to the Conference Control interface using the Create Conference window.
- Access to view details of all conferences hosted on the MCU and to cascaded conferences hosted on participating MCU units.
- Ability to create a new conference from the Conference Control access window, the Create Conference window, or the Conference Control interface.
- Moderator-level access to all conferences while moderator controls are simultaneously held by other users.
- Ability to invite other participants to a conference.
- You can assign Operator authorization to up to 50 users.

Adding a User Profile

Only administrators can add user profiles.
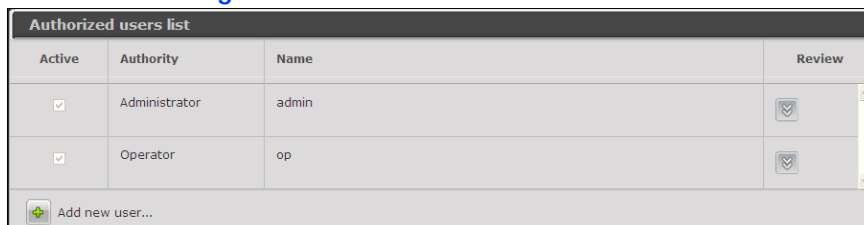
You can create up to ten administrator profiles and up to 50 operator profiles.

Procedure

Step 1   Access the MCU Administrator interface.

Step 2   Select **Users** .

Figure 3-20   Authorized Users List
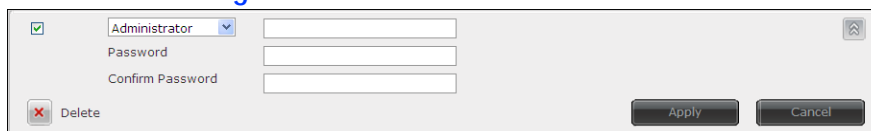
Step 3   Select **Add new user**.

Figure 3-21   User Profile Section

Step 4   Select an authority level from the list.

Step 5   Enter a user name.

Step 6   Enter a password and confirm it.

Step 7   Select **Apply**.

Changing a User Password

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

Step 1   Access the MCU Administrator interface.

Step 2   Select **Users** .

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

Step 4   Enter the new password in the **Password** and the **Confirm Password** fields.

Step 5   Select **Apply**.

Deleting a User Profile

Only administrators can delete user profiles.

You can delete user profiles at any time.

Procedure

Step 1   Access the MCU Administrator interface.

Step 2   Select **Users** ![Users icon](.) .

Figure 3-22 Authorized Users List

Step 3   Select the **Review** button ![button](.) for the user profile you want to remove.

Figure 3-23 User Profile Section

Step 4   Select **Delete**.

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

Backing Up Your SCOPIA Elite MCU Configuration

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

Step 1   Select the ![icon](.) icon in the MCU administrator interface.

Step 2   Select **Backup configuration**.

Step 3   Save the configuration settings file to your chosen location.
The .zip extension is automatically appended to the file name.

Restoring Your Configuration

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.

Note: 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

Step 1 Select the ⚒ icon in the MCU administrator interface.

Step 2 Select **Restore configuration**.

Step 3 Select **Browse**.

Step 4 Navigate to and select the configuration file (.zip) you want to import.

Step 5 Select **Restore**.

Step 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.

Step 7 Select **OK** to complete the restore procedure.

Upgrading Software

Perform this procedure to upgrade from version 7.1 to version 7.5 or from version 7.5/7.6 to later versions.

Do not upgrade MCU software remotely. The MCU and the computer you are using to upgrade should be on the same physical network.

Upgrading from version 7.1 to version 7.5 requires a new license key. If you do not have the license key, you can still upgrade and use a 30-day temporary license. You must update the MCU with the permanent license before this period of time expires. Contact RADVISION Customer Support for obtaining a license key.

Upgrading from version 7.1 to version 7.5 may take up to 30 minutes. Upgrading from version 7.5/7.6 to a later version normally takes 15 minutes.

If you are upgrading from version 7.0, contact Customer Support.

Before You Begin

Verify that there are no active conferences hosted on the MCU.

Procedure

Step 1   (Recommended) Save the current MCU configuration by doing the following:

a. In the web user interface, select the ⚒ icon.

b. Select **Backup configuration**.

c. Save the generated .zip file.

Step 2   If you are upgrading from version 7.1 to version 7.5, do the following:

a. Run the Software Update tool.

b. Select the **Upgrade to version 7.5** tab.

The upgrade process may take up to 45 minutes, depending on your system. Do not use the system or restart during the upgrade process.

Step 3   If you are upgrading from version 7.5/7.6 to a later version, do the following:

a. In the web user interface, select the ⚒ icon.

b. Select **Update software**.

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

A message is displayed informing you that a temporary license is used for the upgrade. After the upgrade, the license is permanent.

d. Click **OK**.

e. Select **Update**.

The system shuts down for a few minutes and then restarts automatically.

All active conferences are disconnected.

f. 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.

Step 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. Press 0 to create a new conference.

c. At a prompt, enter the meeting ID and press #.

The MCU creates the conference and you see the Conference window.

d. Exit the conference by disconnecting the call.

Restoring a Previous Software Version

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

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

Before You Begin

- If you need to restore version 7.5 or 7.6: On the Status tab, verify that the MCU is connected to the network by checking the Ethernet icon.

Figure 3-24 Status Map Section of the Status Tab
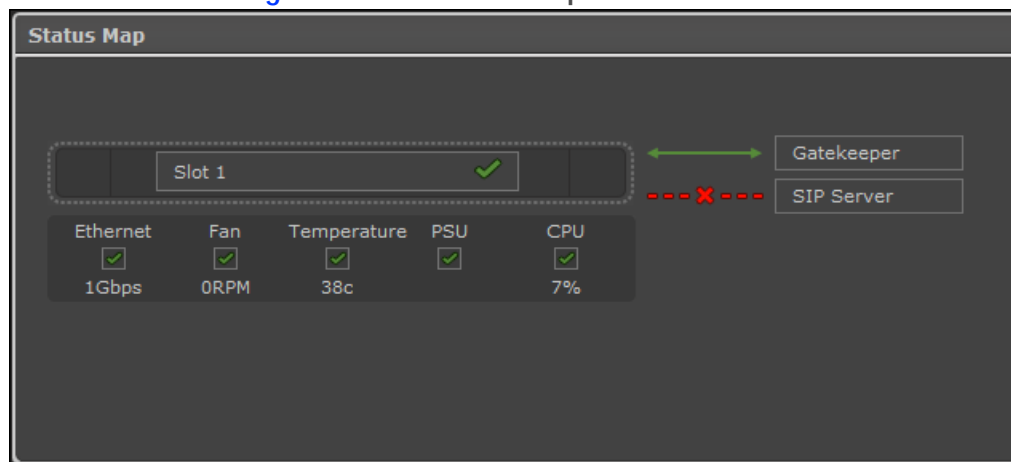
- Verify that there are no active conferences hosted on the MCU by selecting Manage Conferences [Manage Conferences >] and checking that no conferences appear in the Conference List.

Procedure

Step 1   (Recommended) Save the current MCU custom configuration by performing these steps:

    a. In the MCU web user interface, select the maintenance icon.

    b. Select Backup configuration and save the generated .zip file.

Step 2   To restore MCU version 7.5 or 7.6, perform the following steps:

    a. In the MCU Administrator interface, select the maintenance icon.

    b. Select **Rollback software**.

> **Note:** Restoring the previous version may take up to 15 minutes.

Step 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.

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

Step 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. Press 0 to create a new conference.

c. At a prompt, enter the meeting ID and press #.

The MCU creates the conference and you see the Conference window.

d. Exit the conference by disconnecting the call.

Updating a SCOPIA Elite 5100 Series MCU License

If you use a temporary license, you need to obtain a permanent license key and install it on the MCU.

Procedure

Step 1   Obtain a permanent license:

a. Access the RADVISION Internet customer page: www.radvision.com/Support.

b. Select **Product Upgrade**.

c. Select MCU Upgrade.

d. Enter information and select **Submit**.

The permanent license key will be sent to you.

Step 2   Access the MCU Administrator interface.

Step 3   Select the **Maintenance** button .

Step 4   Select **Licensing and Registration**.

The Licensing and Registration window opens.

Figure 3-25 Licensing and Registration Window
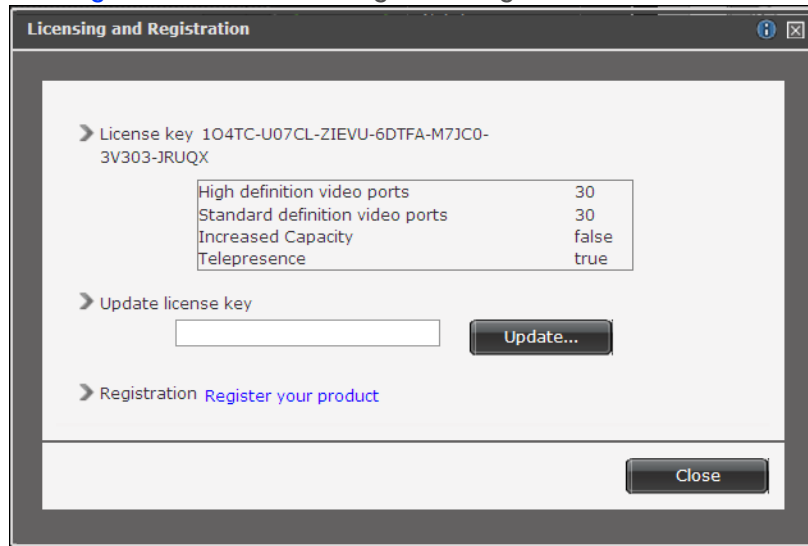
Step 5   Enter the permanent license key.

Step 6   Select **Update**.

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 the SCOPIA Elite MCU 5000 Series, including the SCOPIA Elite 5100 Series MCU and the SCOPIA Elite 5200 Series MCU:

Limiting the UDP Port Ranges for RTP/RTCP on the SCOPIA Elite MCU

The SCOPIA Elite MCU 5000 Series has designated UDP ports 12000-13200 (for video) and 16384-16984 (for audio) for RTP/RTCP. To provide additional security for your firewall, you can limit these ranges.

Every call uses two audio ports and six video ports. For highly utilized systems (above 90%), we recommend multiplying the number of total ports (for all calls) by a factor of 1.5.

Using its full capacity, the SCOPIA Elite 5100 Series MCU uses 180 ports for audio and 540 ports for video, and the SCOPIA Elite 5200 Series MCU uses 360 ports for audio and 1080 ports for video (except for the SCOPIA Elite MCU 5215, which has the same capacity as the SCOPIA Elite 5100 Series MCU).

Procedure

Step 1   Navigate to the MCU **Advanced Commands** section by doing the following:

a.   Select the [icon] icon.

b.   Select **Advanced parameters**.

c.   Locate the **CLI** section and select **More** (see).

Figure 3-26 CLI Section

Step 2   Set the video base port by doing the following:

a.   Enter the **advcmdmpcsetval** command in the **Command** field.

b.   Enter the **mf.BasePort** parameter in the **Parameter** field.

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

d.   Select **Execute**.

e.   Clear the value in the **Parameter** field before proceeding to the next step.

Step 3   Set the audio base port by doing the following:

a.   Enter the **setmprtpbaseport** command in the **Command** field.

b.   Modify the port value in the **Value** field.

c.   Select **Execute**.

Step 4   Select **Close**.

The SCOPIA Elite MCU 5000 Series 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 5100 Series MCU uses 150 ports for H.245, while the SCOPIA Elite 5200 Series MCU uses 300 ports (except for the SCOPIA Elite MCU 5215, which has the same capacity as the SCOPIA Elite 5100 Series MCU).

Procedure

Step 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 3-26 on page 34).

Figure 3-27 CLI Section

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

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

Step 3   Modify the port value in the **Value** field.

Step 4   Select **Execute**.

Step 5   Select **Close**.

The SCOPIA Elite MCU 5000 Series has designated port 80 for HTTP. You can configure a different port to use HTTP if necessary in your environment.
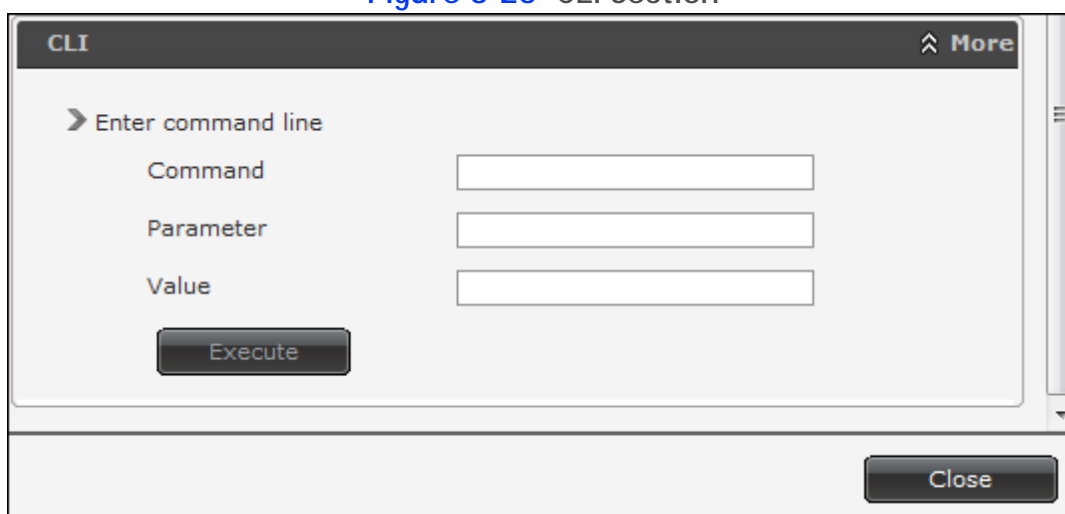
Procedure

Step 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 3-26 on page 34).

<div align="center">Figure 3-28 CLI Section</div>

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

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

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

Step 4   Select **Execute**.

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

Step 5   Select **Yes** to continue.

Step 6   Select **Close**.

> **Note:** 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 the following:
>
> **http://<URL>:8080**

Configuring the UDP Port for RAS on the SCOPIA Elite MCU

The SCOPIA Elite MCU 5000 Series 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 38).

> **Note:** 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.
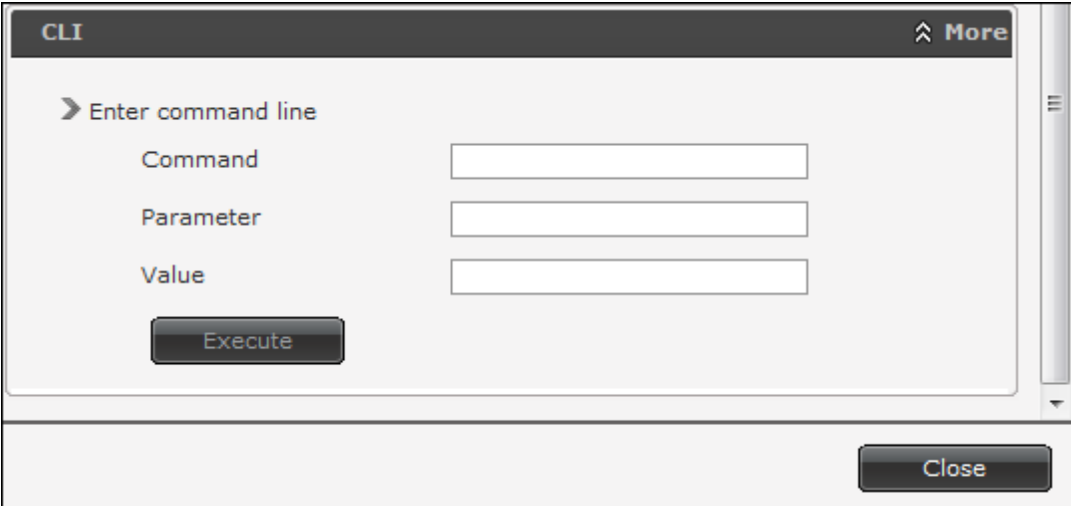
Procedure

Step 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 3-29 on page 38).

Figure 3-29 RAS Port Configuration
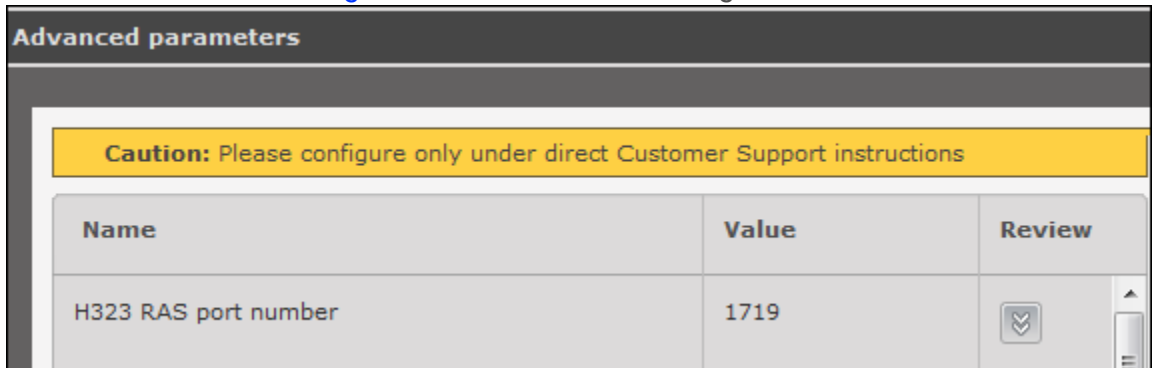
Step 2   Select the ⬇ icon in the **Review** column.

Step 3   Enter the port value in the **H323 RAS port number** field.

Step 4   Select **Apply**.

Step 5   Select **Close**.

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

The SCOPIA Elite MCU 5000 Series 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 37).

Note: 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

Step 1   Navigate to the MCU **H.323 Protocol** section by selecting **Configuration** > **Protocols**.

Step 2   Locate the **Enable H.323 protocol** section (see Figure 3-30 on page 38).

Figure 3-30 H.323 Protocol section of the Protocols tab
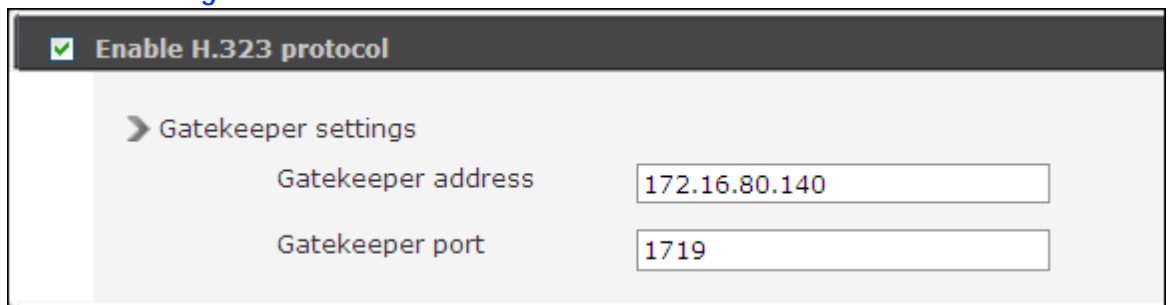
Step 3   Enter the port value in the **Gatekeeper port** field.

Step 4   Select **Apply**.

The SCOPIA Elite MCU 5000 Series 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.
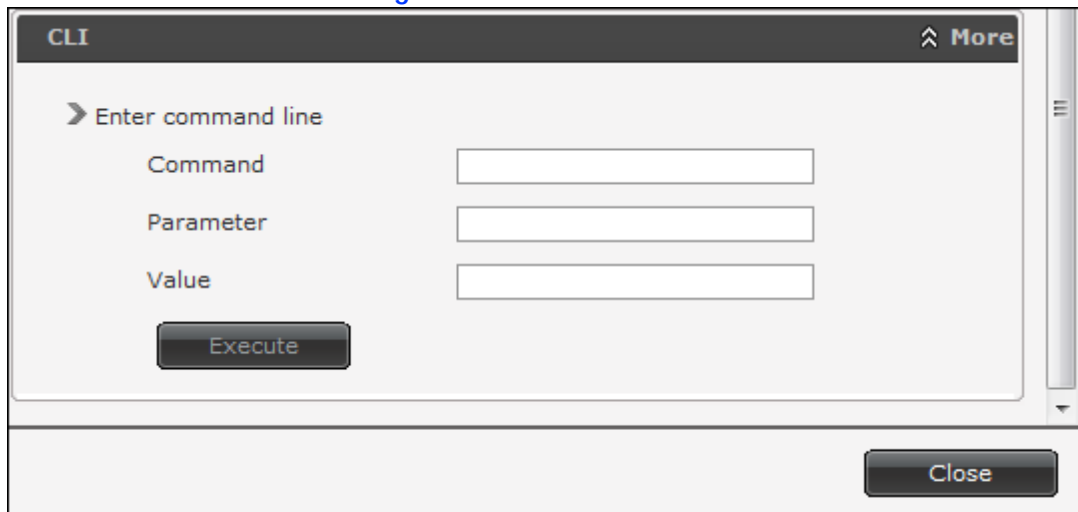
Procedure

Step 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 3-31 on page 39).

Figure 3-31 H.323 Signaling Port Configuration

Step 2   Select the ⌄ icon in the **Review** column.

Step 3   Enter the port value in the **H323 SIG port number** field.

Step 4   Select **Apply**.

Step 5   Select **Close**.

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

The SCOPIA Elite MCU 5000 Series 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

Step 1   Navigate to the MCU **SIP Protocol** section by selecting **Configuration** > **Protocols**.

Step 2   Locate the **Enable SIP protocol** section and select **More** (see).

Figure 3-32 SIP Port Configuration

Step 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.

Note: 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.

Step 4   Select **Apply**.

Configuring Security Access Levels for the SCOPIA Elite MCU

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 **Standard**. 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.

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

Procedure

Step 1   Access the MCU security settings by selecting **Configuration** > **Setup**.

Step 2   Locate the **Security** section.

Step 3   Select the access level from the **Security Mode** list (see Figure 3-33 on page 41). Table 3-2 lists the protocol status when each security access level is applied.

Figure 3-33 Security Access Level Settings
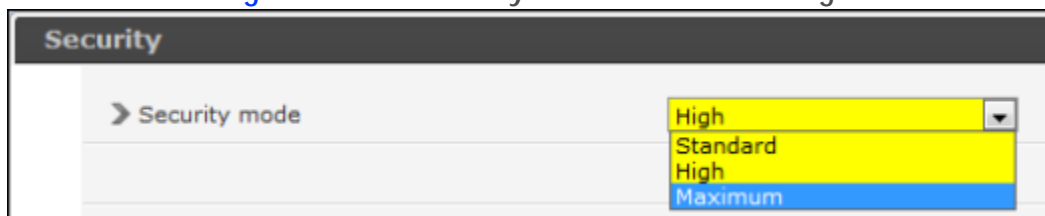
Table 3-2   MCU Security Access Levels

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

Step 4   Select **Apply**.

4 How to Moderate a Conference as an Operator

As an operator, you can modify a conference using the Conference Control interface.

Conference Control Interface

Use the SCOPIA Elite MCU Conference Control interface to perform these tasks:

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

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.

Note: We recommend that you use the full screen mode (1024 x 768 fps) when using the Conference Control interface.

Note: You can view multiple Conference Control interface browser windows at the same time to monitor different conferences. We recommend, however, that you close windows you are not currently viewing to avoid confusion and carrying out operations in the wrong conference.

Figure 4-1 shows the Conference Control page. The layout of the Conference Control page may be different 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 4-1 Conference Control Page
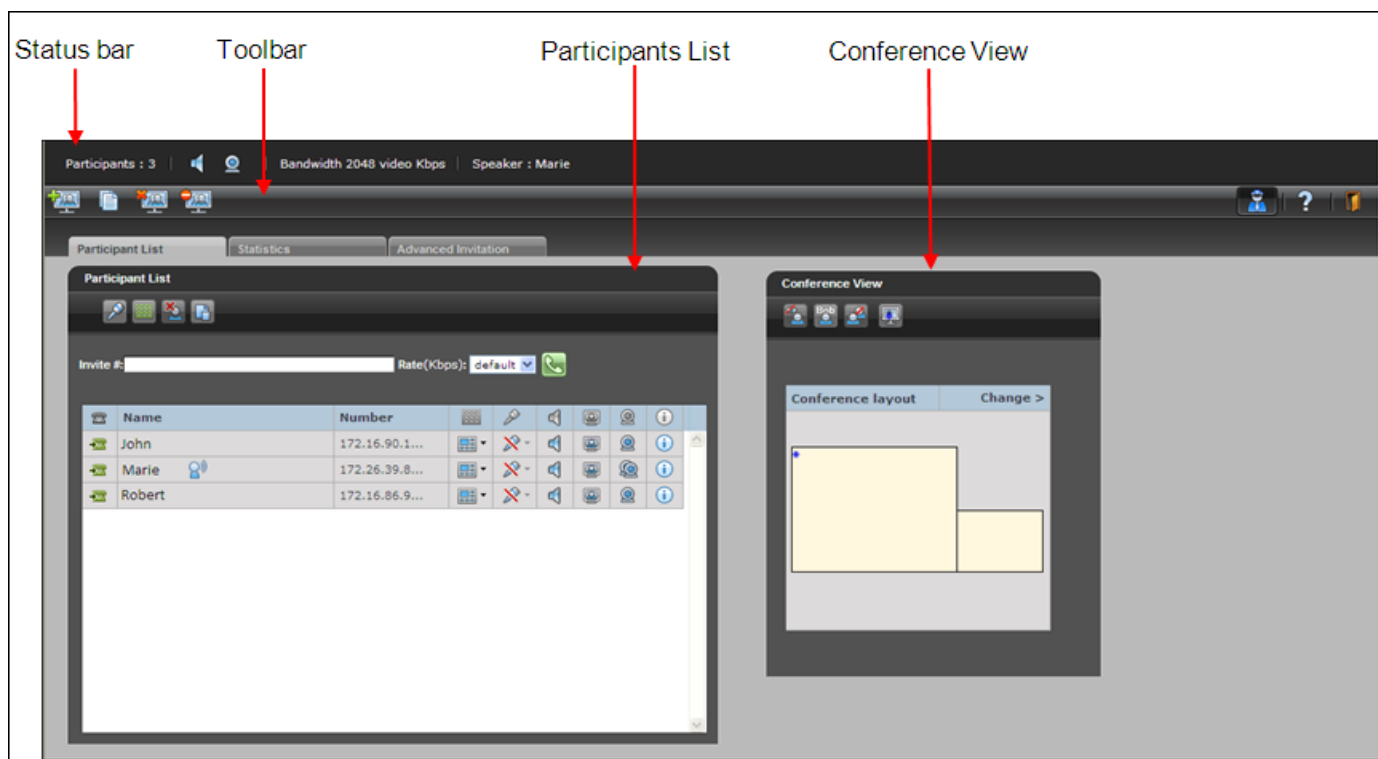
The Conference Control Page consists of the following elements:

- Status bar—Presents essential information about a conference: number of participants, used bandwidth, the active speaker, and whether video and voice are enabled for this conference.

- Toolbar—Provides access to conference-level tasks, such as creating a new conference, blocking admission to a conference or becoming a moderator.

- Participant List—Displays inclusive information about current conference participants. You use the Participant List section to control participants in the conference, as well as to invite new participants.

- Conference View—Displays the current conference video layout and provides controls for modifying it.

Becoming a Moderator and Stopping Moderation

Moderator access can be PIN-protected. Administrators and Operators can jointly be moderators simultaneously.

Procedure

Step 1   Access the Conference Control interface by clicking `Manage Conferences >`.

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

Step 3   A dialog box requesting a PIN might appear if Moderator access is PIN-protected. Enter the PIN.

Step 4   To release control of the conference, select **Stop Moderation**.

How to Control Participants in a Conference

As a moderator, you can control participants in a conference by performing the following tasks:

Creating a New Conference

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

Procedure

Step 1   To create a conference from the Login page:

    a. Launch your browser and enter the IP address of the MCU.

         The MCU login window appears.

Figure 4-2 SCOPIA Elite MCU Login Window
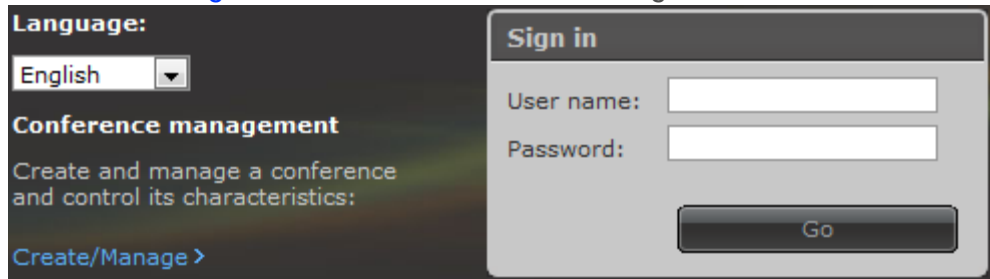
b. Select the **Create** link.

c. Select **Create Conference**.

-or-

Step 2   To create a conference from the Conference Control interface:

a. Access the Conference Control interface by selecting the **Manage Conferences** button `Manage Conferences >`.

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

Step 3   Select a service prefix from the list.

Figure 4-3 Create Conference Page
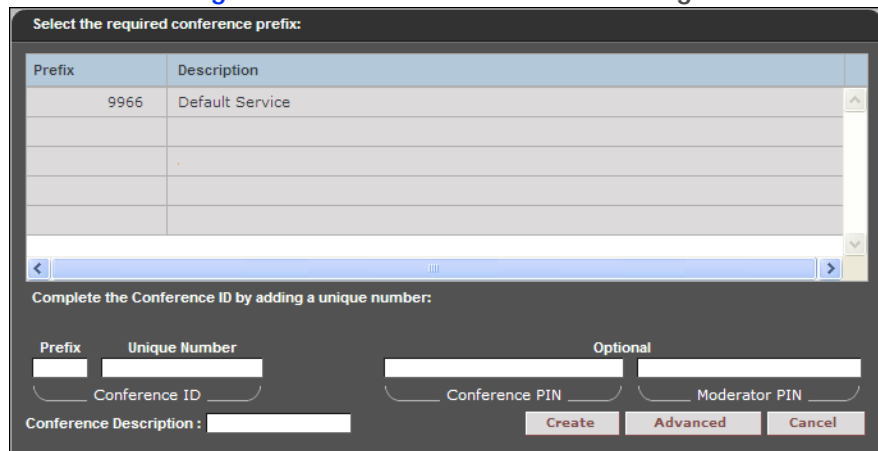
Step 4   Enter an ID number for this conference in the Unique Number field.

Note: You cannot use an existing meeting number.

Step 5   (Optional) Enter a PIN for accessing the conference in the Conference PIN field.

Step 6   (Optional) Enter a PIN for moderating the conference in the Moderator PIN field.

> **Note:** You can also configure a default moderator PIN for a service profile in the Administrator interface.

Step 7   (Optional) Enter a description of the meeting in the Conference Description field.

Step 8   (Optional) Select **Advanced** to configure additional settings for the conference such as duration, time-out and dialing policy settings.

Step 9   Select **Create** to launch your conference.

Muting and Unmuting Individual Participants

Moderators can mute or unmute an individual participant in a conference.

Procedure

Step 1   Access the Conference Control interface.

Step 2   In the Participants List section, select a participant.

Step 3   Select the microphone icon [icon] in the Participant List row.
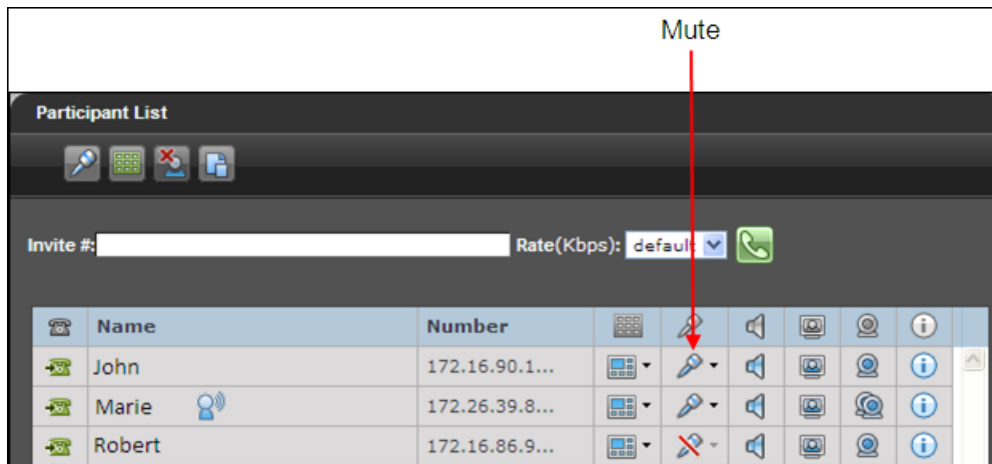
Muting and Unmuting All Participants

Users with moderator level access can mute or unmute all participants in the conference.

Procedure

Step 1   Access the Conference Control interface by selecting the **Manage Conferences** button `Manage Conferences >`.

Step 2   In the Participants List section, select **Mute All**.

Figure 4-4 Mute All Button in the Participant List Section
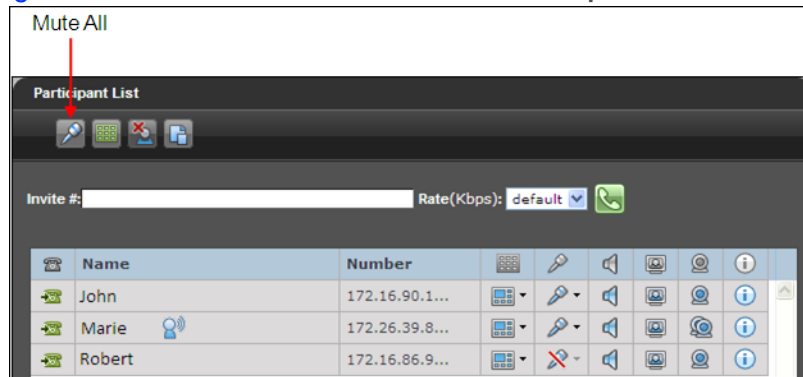
Submenu opens.

Figure 4-5 Mute All submenu
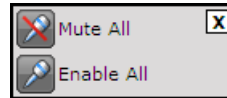
Step 3   Select the desired option.

Changing Participant Views

Moderators can define the video layout for meeting participants: how many participants they see, how large the participants' video frames are and so on. These views are preconfigured on the SCOPIA Elite MCU and can be assigned both to a conference, becoming a conference view, and to an individual participant, becoming a participant's view. If multiple views are enabled for a conference, you can assign different views to participants in the same conference.

By default the conference view is assigned to all participants in a conference.

In the Conference Control interface the participant's and conference views are marked with different icons.

Figure 4-6 Change Participant's View button in the Participant List Tab
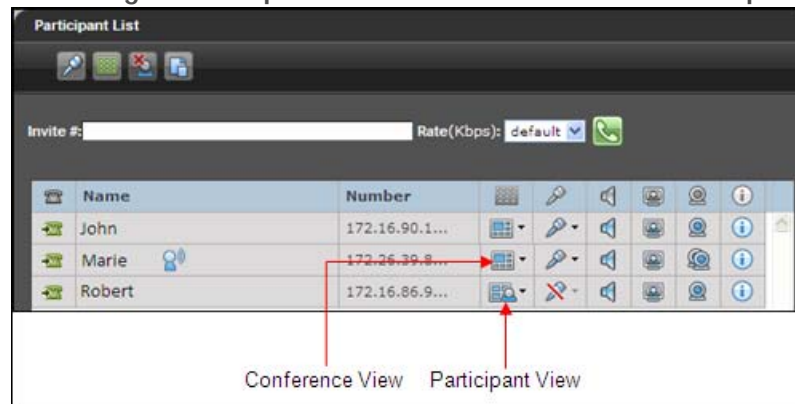
Procedure

Step 1 Access the Conference Control interface.

Step 2 To change the view for an individual participant, perform these steps:

a. Select the **Change Participant's View** button for this participant in the Participant List Tab.

Figure 4-7 Change Participant's View button in the Participant List Tab
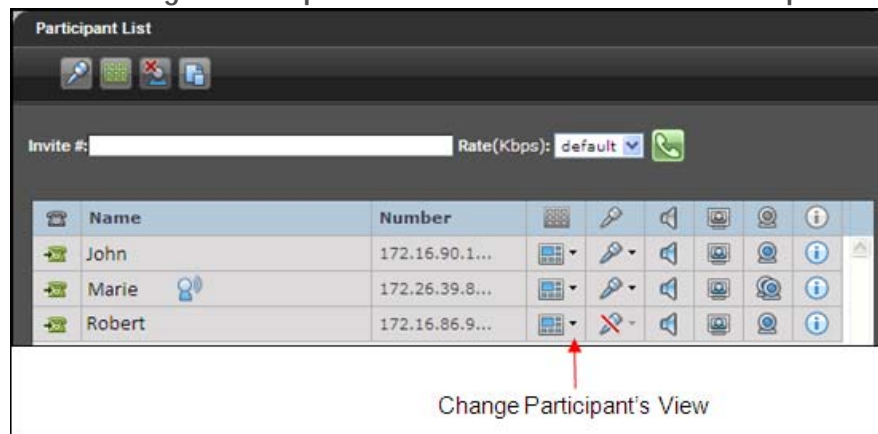
b. From the submenu, select the necessary option.

Figure 4-8 Participant View Submenu
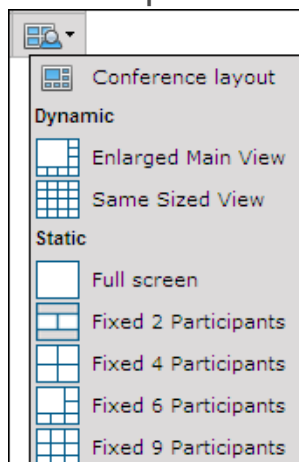
> **Note:** You can display up to 28 participants in a single layout. Layouts that display up to 16 participants are supported by all resolutions, while layouts that display 21 or 28 participants are supported only by resolutions of 480p or higher.

Step 3 To change the view for several participants or all participants, perform these steps:

a. If you want to change the view for several participants, select these participants in the Participant List by holding down the CTRL key and clicking participants' names.

b. In the Participant List Tab, select the **Change View** button.

Figure 4-9 Change View button in the Participant List Tab
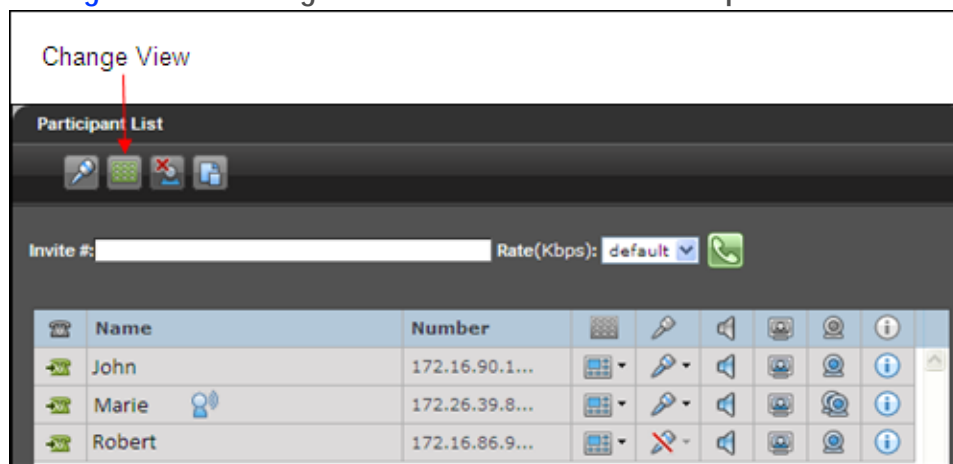
c. In the Change view dialog box, select **All** or **Selected participants**.

Figure 4-10 Change view dialog box
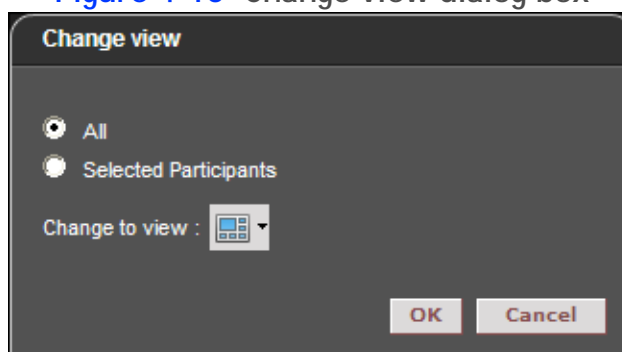
    d. From the Change to view list, select the desired view.

    e. Select **OK**.

Blocking Conference Admission

Users with moderator-level access 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

Step 1   Access the Conference Control interface by selecting the Manage Conferences button Manage Conferences >.

Step 2   On the toolbar, select **Conference Admission**.
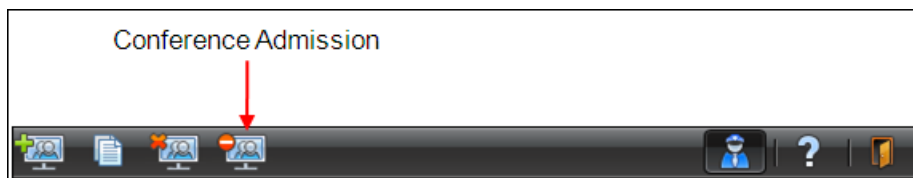
To re-admit participants, select **Conference Admission** again.

Viewing Participant Call Information

You can view participant call statistical information.

Procedure

Step 1   Access the Conference Control interface.

Step 2   Select the required participant in the Participant List tab.

Step 3   Select the information icon in the Participants List section for the selected participant.
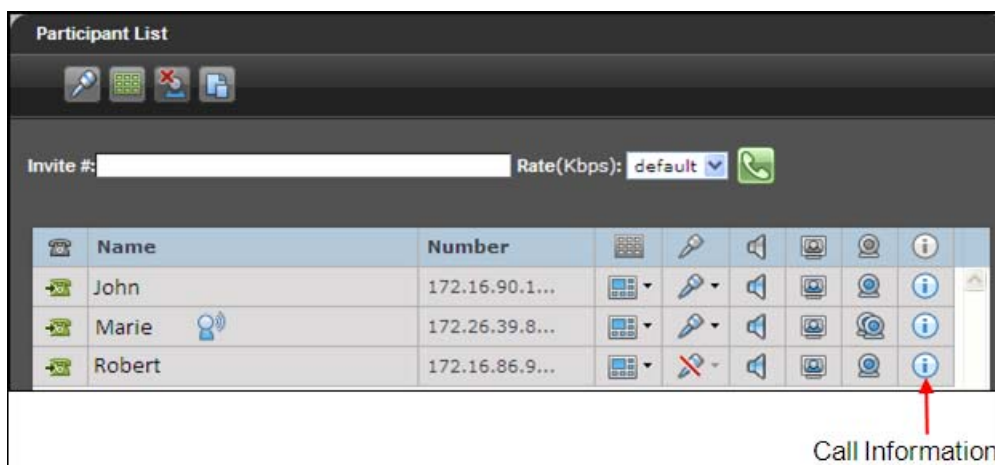
Call Information

The Call Information dialog box for the specified participant appears.

Table 4-1 lists the statistics displayed.

Table 4-1   Participant Information Statistics

Group	Field	Description
Endpoint Information	Type	Participant endpoint type.
	IP address	Participant endpoint IP address.
	Description	Participant description (displays the endpoint vendor identifier, if available).
	Connect time	Time at which the participant connected to the conference.
Basic Call Information		
Audio	Audio Codec	Audio codecs sent to and received by the participant.
	Audio rate	Total audio bandwidth sent and received by the participant.
	Audio Packets loss count	Total lost audio packets sent to and received by the participant.
	Audio Jitter (curr/min/max)	Accumulated audio packets sent to and received from the participant. Includes the current value and average values for the minimum and maximum number of packets sent to and received from the participant.

Group	Field	Description
Video	Video codec	Video codecs sent to and received by the participant.
	Video resolution	Picture size of video sent and received by the participant.
	Video frame rate	Frame rate of video sent to and received by the participant.
	Video rate	Total video bandwidth sent and received by the participant.
	Video packets loss count	Total lost video packets sent to and received by the participant.
	Video jitter (curr/min/max)	Accumulated video packets sent to and received from the participant. Includes the current value and average values for the minimum and maximum number of packets sent to and received from the participant.
	2nd video codec	The second video codec sent to and received by the participant (if used).
Data	Data protocol	Indicates whether the protocol used if the participant is participating in data sharing.
Advanced Call Information		
Audio	Audio out of order packets count	Total audio packets sent to and received from the participant out of sequence.
	Audio packets count	Total audio packets sent and received by the participant.
	Audio bytes count	Total audio bytes sent and received by the participant.
	Audio IP address	IP address and port to which audio is sent to the participant.

Group	Field	Description
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 Video Fast Update (VFU) requests sent and received by the participant.
	Video packets count	Total video packets sent and received by the participant.
	Video bytes count	Total video packets sent and received by the participant.
	Video IP address	IP address and port to which video is sent to the participant.
	Qualivision state	Encryption level used.
Data	Data IP address (Local/Remote)	IP address of the participant data sharing terminal.
	FECC	Indicates whether Far End Camera Control is in use.

Defining Conference Views

The following sections describe how to define the conference view using the Conference Control interface:

In the Conference View section, users with moderator-level access can change the main layout for the current conference.

Procedure

Step 1   Access the Conference Control interface by selecting the Manage Conferences button [Manage Conferences >].

Step 2   In the Conference View section of the Participant List tab, select **Change**.

Figure 4-11 Conference View Section
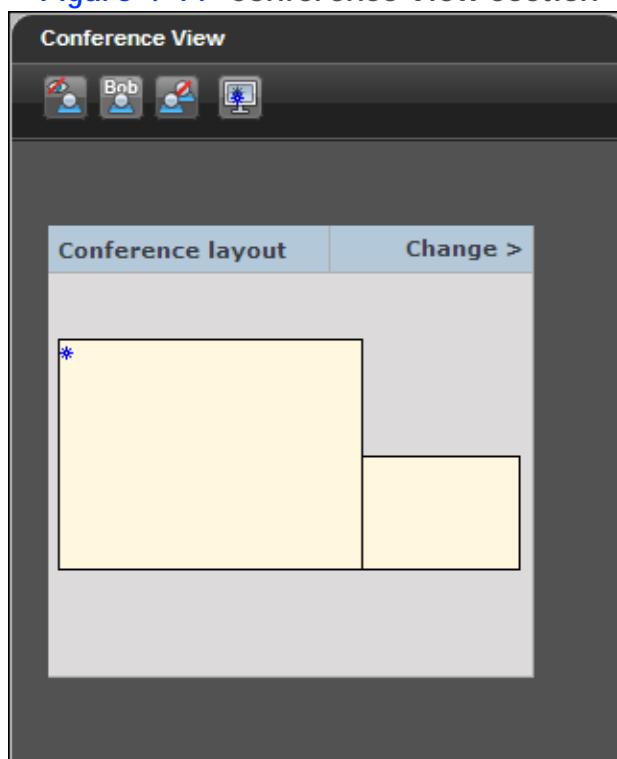
The layout menu appears, displaying a list of available layouts for the current conference.

Figure 4-12 Layout Menu Displayed in the Conference View Section
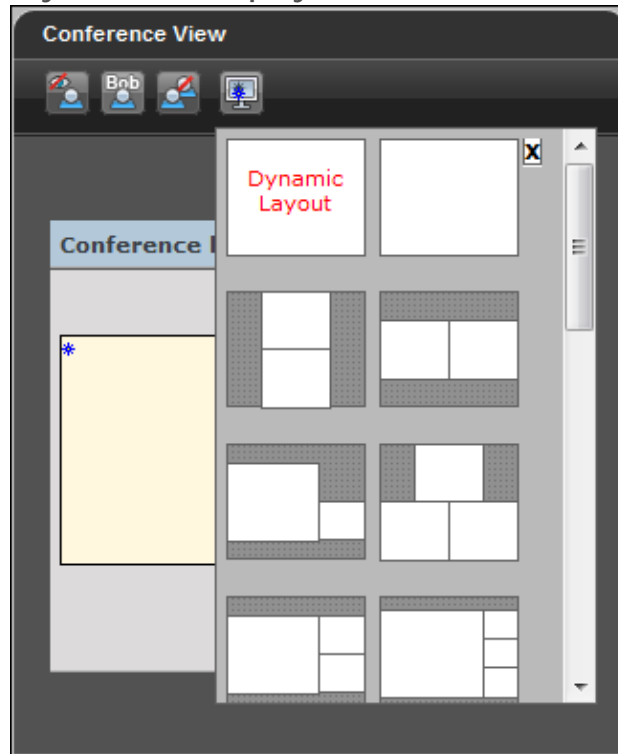
Step 3   Select the layout of your choice.

> **Note:** 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 conference adjusts to the new selection.

Displaying Participant Names in Frames

In the Conference View section, users with moderator-level access can optionally display the name of endpoints or participants in specific positions of the video layout frame.

Procedure

Step 1   Access the Conference View section of the Participant List tab.

Step 2   Select **Display names** button in the Conference View section.
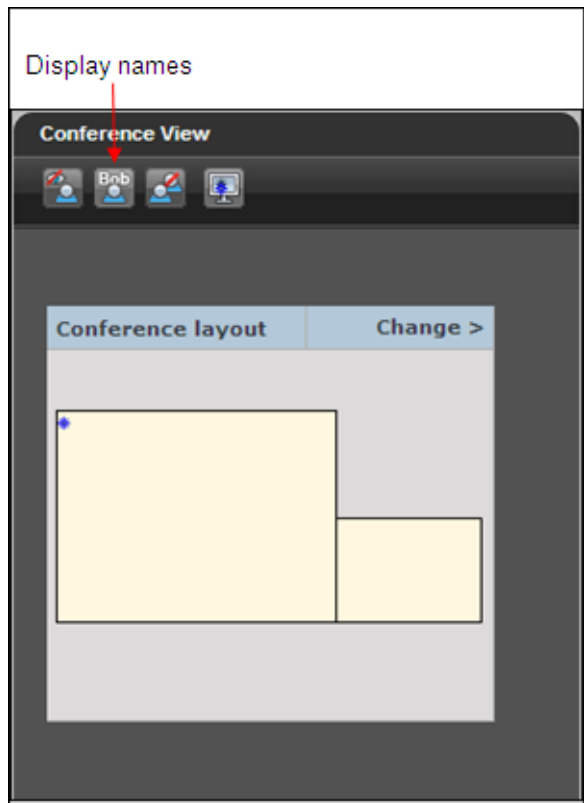
The names are displayed at the bottom of the participants' frames in a conference (Figure 4-13 on page 56).

Figure 4-13 Names Displayed in Conference (Example)

The self-see feature allows participants see their own video in a separate frame displayed as part of the conference video. By default, this feature is disabled.

Procedure

Step 1   Access the Conference View section of the Participant List tab.

Step 2   Select the **Self-see mode** button.
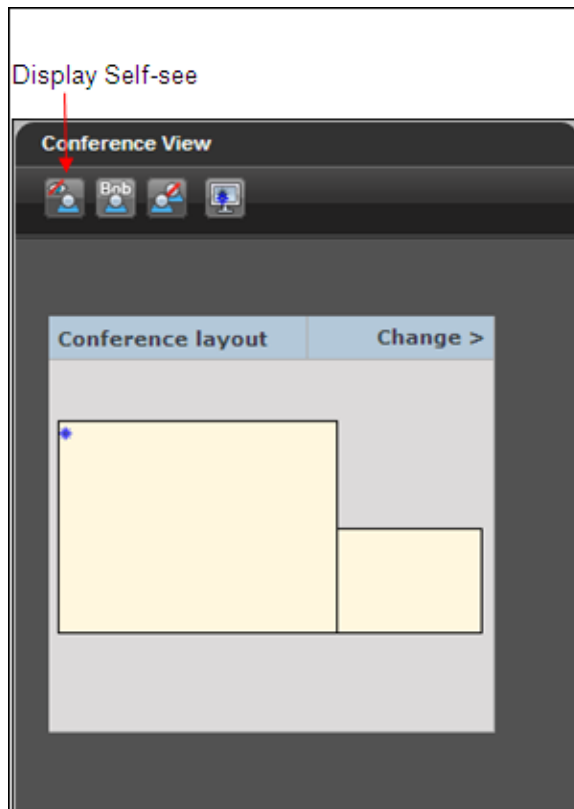
All participants using the conference view can see themselves in the conference video.

Terminating Conferences

You can terminate a conference at any time. This action disconnects all participants from the conference.

Procedure

Step 1   Access the Conference Control interface.

Step 2   Select **Terminate Conference**.

Figure 4-14 **Terminate Conference Button on the Toolbar**
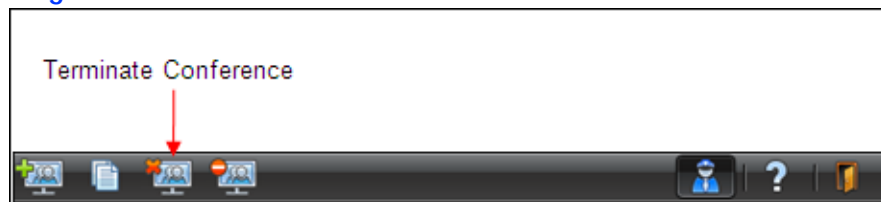
Step 3   Click **OK** in the confirmation message.
The conference is closed.

Troubleshooting the SCOPIA Elite MCU

These tips list useful hardware and software troubleshooting solutions. If the MCU still malfunctions, call RADVISION support for help.

Quick Troubleshooting Using the Front Panel LEDs of the SCOPIA Elite MCU

Problem   The STATUS LED on the front panel of the SCOPIA Elite MCU lights red.

Solution   The MCU contains an automatic reset mechanism to deal with most issues. Reset takes place automatically after a short while. If the STATUS LED continues to light red, manually reset the system by pressing the RESET button on the front panel.

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 the 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 the Predefined mode, verify that the MCU is predefined on the ECS.

Resolving MCU Conference Initiation Failure

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.

1. Access the MCU Administrator interface.

2. Select the **Maintenance options** button ⚒▾, and then select **Advanced parameters**.

   The Advanced parameters window is displayed.

3. Locate the **Allows/Disallows external authorization servers to connect** parameter.

4. Select the **Review** button ⊗.

   This parameter section is displayed.
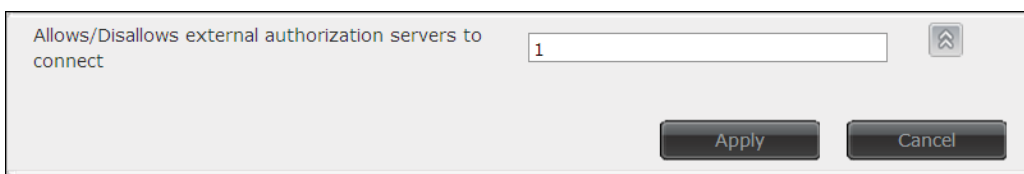
Allows/Disallows external authorization servers to connect	1		⊗
		Apply	Cancel

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

Step 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.

Step 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:

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.

Resolving Conference Access Failure

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 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.

Resolving Quality Issues in Cascaded Conferences

Problem A cascaded conference 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.

Resolving Endpoint Disconnection Issues

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 300 msec).

Resolving Unexpected Conference Termination

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, uncheck the **Check that endpoint is online every n seconds** option in ECS > Settings > Advanced. Uncheck the **Check that call is alive every n seconds** option in ECS > Settings > Calls. 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

Step 1 Access the MCU Administrator interface.

Step 2 Select the **Configuration** tab .

Step 3 Select the **Conferences** tab .

Step 4 In the Conference Control section, select **More**.

Additional conference control parameters are displayed.

Figure 5-1 The Conference Control Section of the Conferences Tab
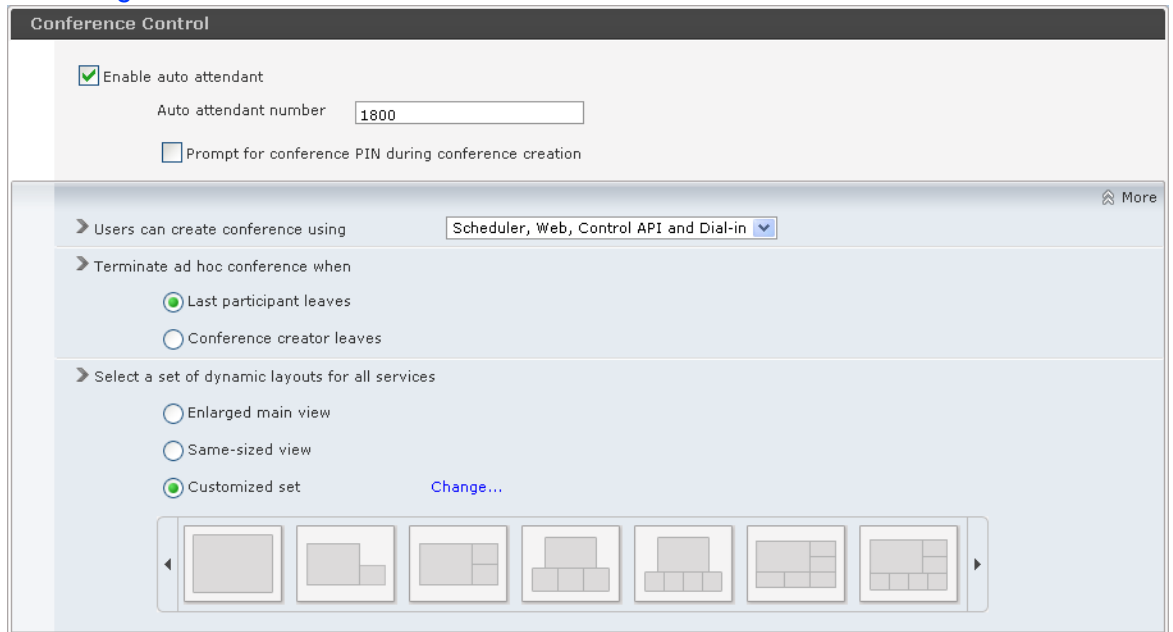
Step 5   Enable the **Last participant leaves** option.

Step 6   Select **Apply**.

Resolving Presentation Issues

Problem   A conference participant cannot start or receive a presentation.
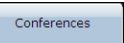
Possible Causes

- 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:
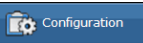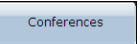
Procedure

Step 1   Access the MCU Administrator interface.

Step 2   Select the **Configuration** tab [Configuration].

Step 3   Select the **Conferences** tab [Conferences].

Step 4   In the Services List section, select the service.

Step 5   Select **More**.

Additional settings for this service are displayed.

Figure 5-2 Additional Service Settings Window
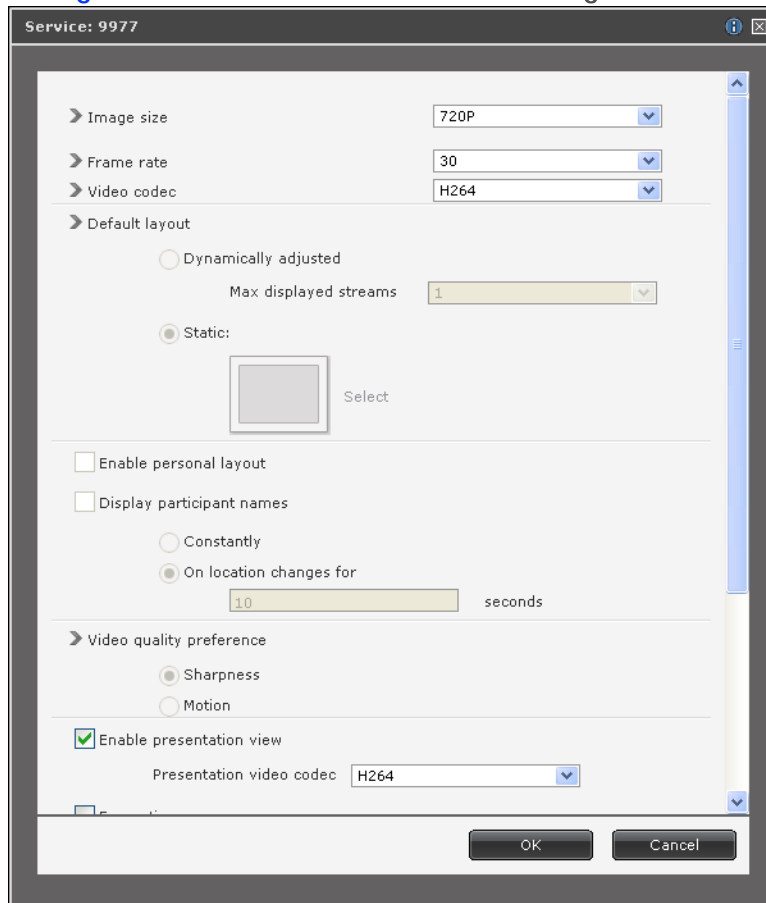
Step 6   Select **Enable presentation view**.

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.

Resolving Unexpected SIP Call Disconnection

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.

Recovering the Password

Problem	You forgot your MCU password.
Solution	Reassign a username and password directly on the MCU by connecting a computer to the device's serial port.

Procedure

Step 1   Make sure you have these items:

- IP address of the default router the MCU uses to communicate over the network
- PC with available serial port and terminal emulator software installed
- Serial cable

Step 2   Connect the power cable.

Step 3   Start the terminal emulation application on the PC.

Step 4   Set the communication settings in the terminal emulation application on the PC as follows:

- Baud rate: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Step 5   Turn on the power to the MCU.

A log of the auto-boot events scrolls across the computer monitor.

Step 6   When the message "Press any key to start configuration" appears on the screen, press any key within 10 seconds.

The network configuration Main menu appears:

```
Main menu

N: Configure network port values

P: Change the configuration software password

S: Configure network security mode

T: Configure TFTP servers list

A: Advanced configuration menu

Q: Quit
```

Caution   If you do not press a key before the countdown ends, the device continues its initialization and you will need to reboot the device to return to the network configuration Main menu.

Step 7   Enter **P** at the prompt to configure default network port values and press **Enter**.

Step 8   Enter the name that you want to use as the global user name at the Enter User name prompt and press **Enter**.

Step 9   Enter **Q** to save your changes and allow the device to complete the boot process.

Resolving a Poor Video Quality Issue

Problem   The quality of the video in a conference 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

Step 1   Connect a PC to the network segment to which the EP belongs.

Step 2   Open a command line window.

Step 3   Enter this command:

```
ping -l 1500 -t <remote IP address of the MCU>
```

Step 4   Monitor the router response for at least 20 minutes.

Figure 5-3 Example of a Router Response in a Ping Test

```
C:\Documents and Settings\john>ping -l 1500 192.168.212.12 -t
Pinging 192.168.212.12 with 1500 bytes of data:
Reply from 192.168.212.12: bytes=1500 time=83ms TTL=60
Reply from 192.168.212.12: bytes=1500 time=81ms TTL=60
Reply from 192.168.212.12: bytes=1500 time=81ms TTL=60
Reply from 192.168.212.12: bytes=1500 time=82ms TTL=60
Reply from 192.168.212.12: bytes=1500 time=83ms TTL=60
Reply from 192.168.212.12: bytes=1500 time=81ms TTL=60
Reply from 192.168.212.12: bytes=1500 time=81ms TTL=60
```

Step 5   (Optional) You may display statistics by pressing CTRL + Space.

Figure 5-4 Example of Router Statistics as Displayed in the Ping Test

```
Ping statistics for 192.168.212.12:
    Packets: Sent = 65, Received = 65, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 80ms, Maximum = 91ms, Average = 82ms
Control-Break
```

Press CTRL +C to hide statistics.

Step 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 in not higher than 300-400 msec.

Step 7   Close the command line window.

Step 8   Verify that enough bandwidth is dedicated to videoconferencing traffic and this bandwidth is available at all times.

Step 9   Verify that there is enough bandwidth for daily activity traffic on WAN IP links apart from bandwidth dedicated to videoconferencing.

Step 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.

Step 11   Verify that the Auto Negotiation preferred setting is selected for all routers and switches working in 100 Mbit/Full Duplex mode.

Step 12   Verify that the MCU LAN ports are synchronized with the switch:

Step 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.

Step 14 Verify that 10 Mbit/Half Duplex hubs are not used for videoconferencing traffic.

Step 15 Verify that synchronization of the LAN endpoints with the LAN switches is set to 100 Mbit/Full Duplex.
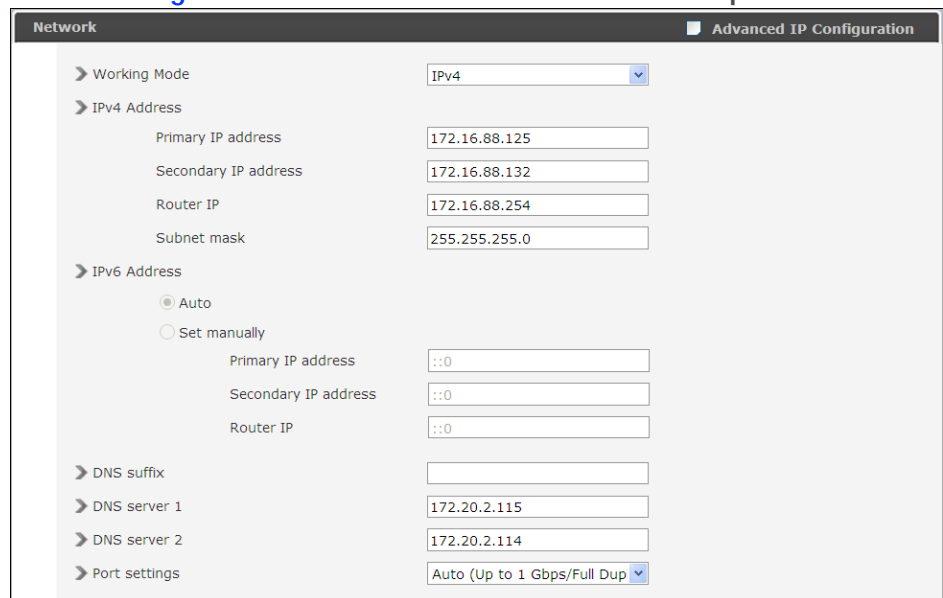
    a. Access the MCU Administrator interface.

    b. Select the **Configuration** tab [Configuration].

       The Setup tab is displayed.

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

Figure 5-5 Network Section of the Setup Tab

Step 16 Verify that the MCU Quality of Service (QoS) settings are correct:

    a. In the Setup Tab of the MCU Administrator interface, scroll down to the QoS section.

    b. Select **More**.

       The QoS section is displayed.

Figure 5-6 QoS Section of the Setup Tab

c. Select **Custom**.
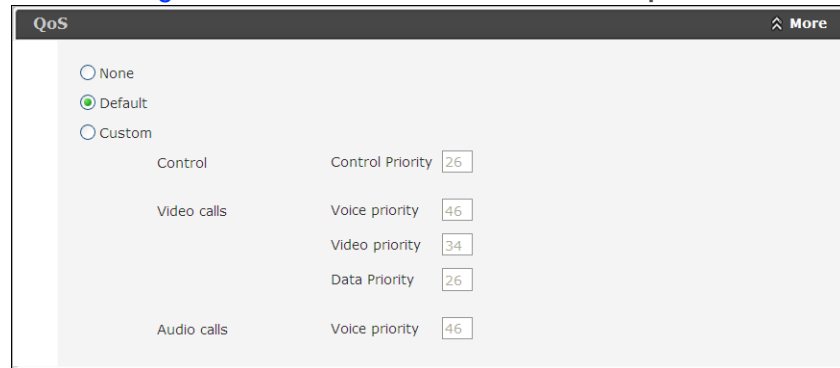
d. Enter 34 in all fields.

e. Select **Apply**.

Step 17 Verify that the bandwidth on the WAN IP links dedicated to the videoconferencing traffic is enough.

Step 18 (Optional) On Cisco routers, verify that assured forwarding policy is set to 41.

Resolving a Poor Audio Quality Issue

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

Step 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.

Step 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.

Step 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

Step 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.

Step 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.

Step 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.

About RADVISION

RADVISION (NASDAQ: RVSN) is the industry's leading provider of market-proven products and technologies for unified visual communications over IP, 3G and IMS networks. With its complete set of standards-based video communications solutions and developer toolkits for voice, video, data and wireless communications, RADVISION is driving the unified communications evolution by combining the power of video, voice, data and wireless – for high definition video conferencing systems, innovative converged mobile services, and highly scalable video-enabled desktop platforms on IP, 3G and emerging next generation IMS networks. To gain additional insights into our products, technology and opinions, visit blog.radvision.com. For more information about RADVISION, visit www.radvision.com

USA/Americas	EMEA	APAC
T +1 201 689 6300	T +44 20 3178 8685	T +852 3472 4388
F +1 201 689 6301	F +44 20 3178 5717	F +852 2801 4071
infoUSA@radvision.com	infoUK@radvision.com	infoAPAC@radvision.com

RADVISION®

Delivering the Visual Experience ®