RADVISION®
an Avaya company

Scopia Elite 6000 Series MCU

Installation Guide

Version 8.2
For Solution 8.2

8.2

Table of Contents

Chapter 1: About the Scopia Elite MCU

Chapter 2: Planning your MCU Deployment

Chapter 3: Preparing the MCU Setup

Chapter 4: Setting up the MCU

Chapter 5: Performing the MCU Initial Configuration

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

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.
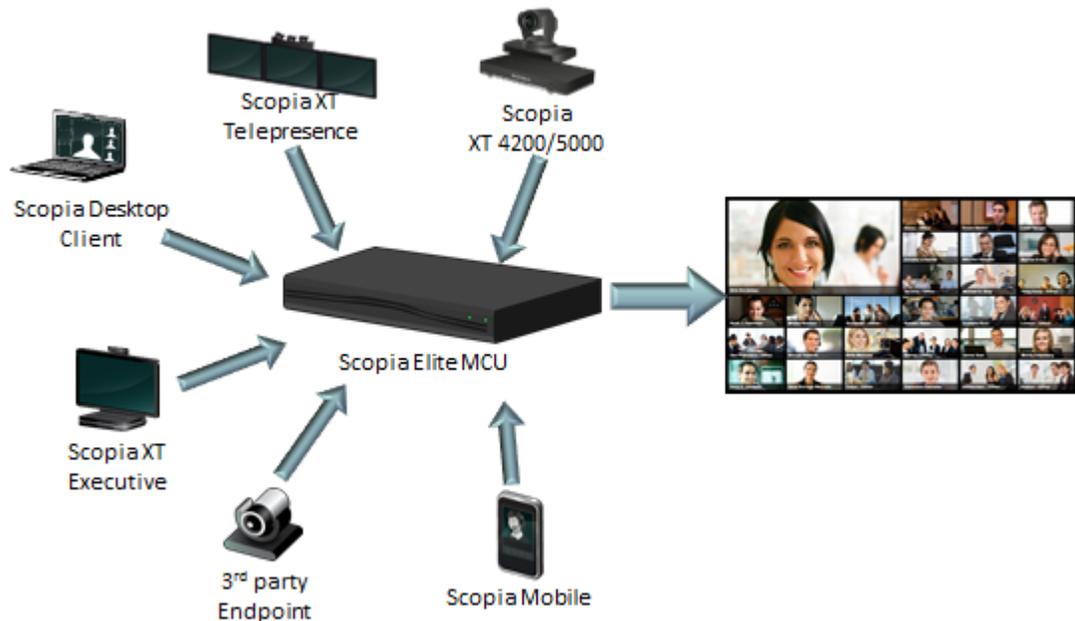
Figure 1: Endpoints in the same videoconference

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 increases 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 Managementsupplies 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

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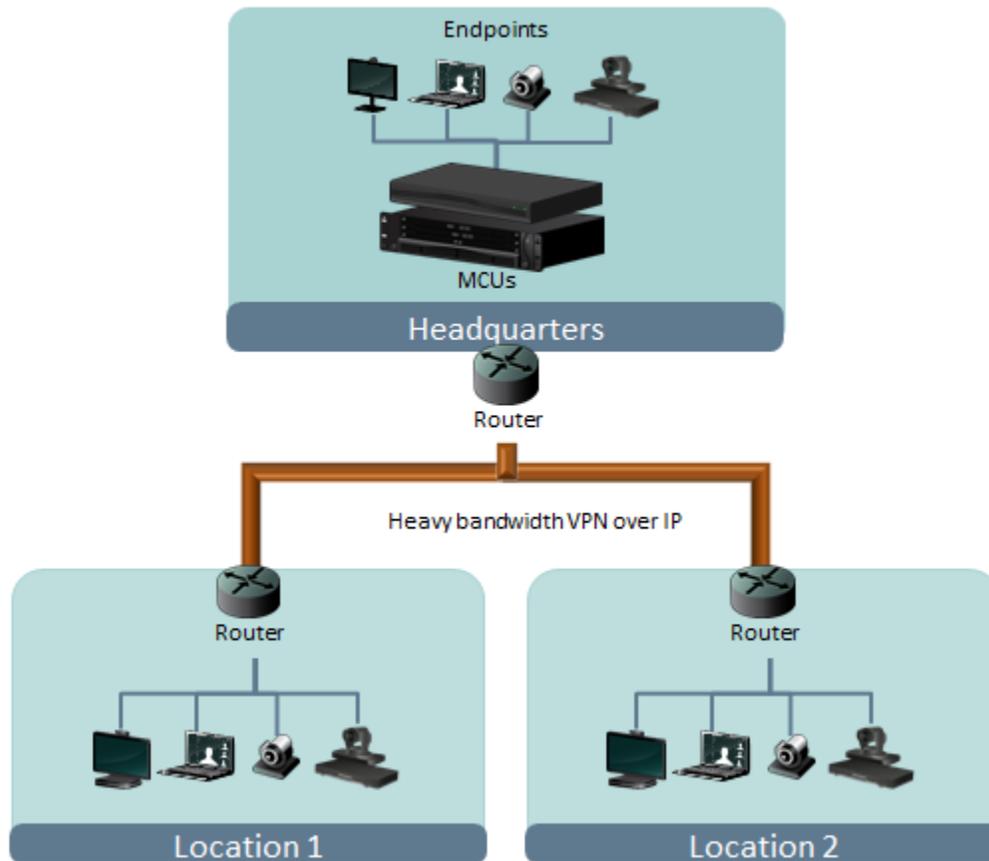
Figure 2: Centralized MCU deployment, where all branches use the HQ MCU

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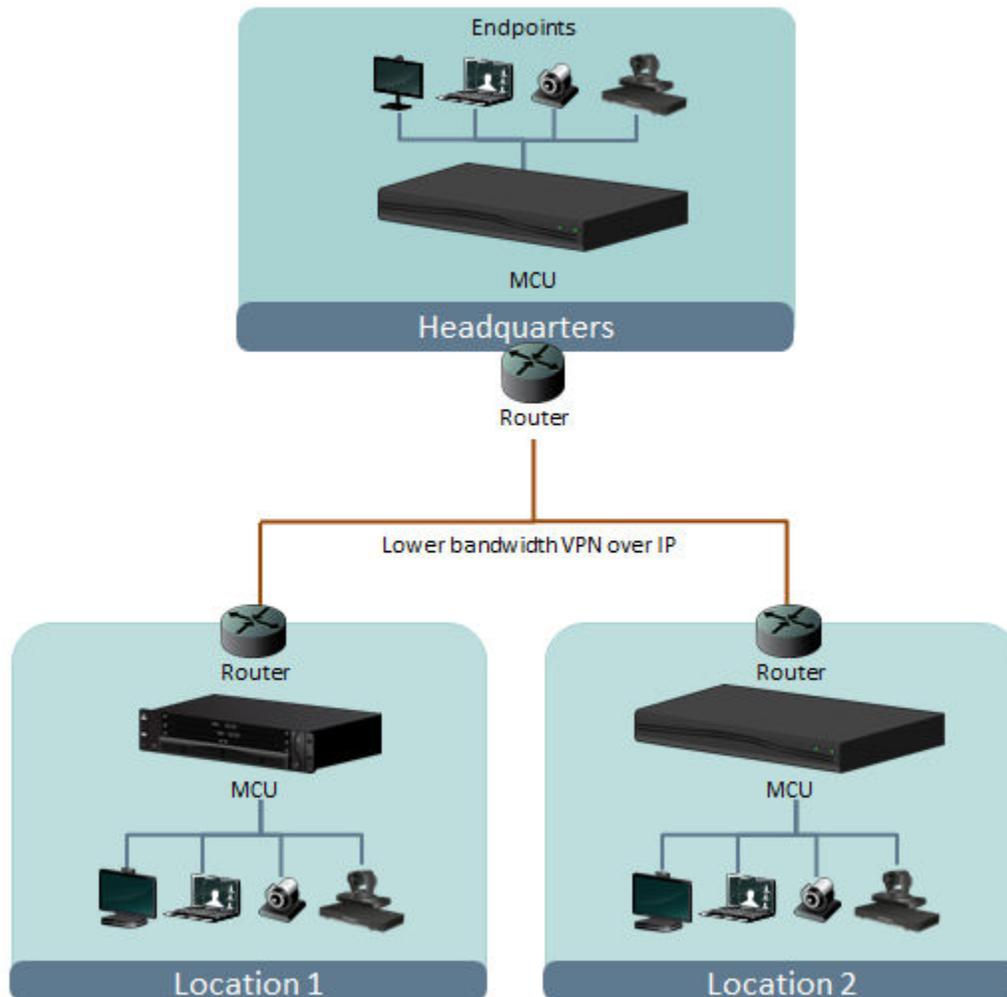
Figure 3: Distributed MCU deployment cascading meetings for reduced WAN bandwidth

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 *Administrator Guide for Scopia Elite MCU*.

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.

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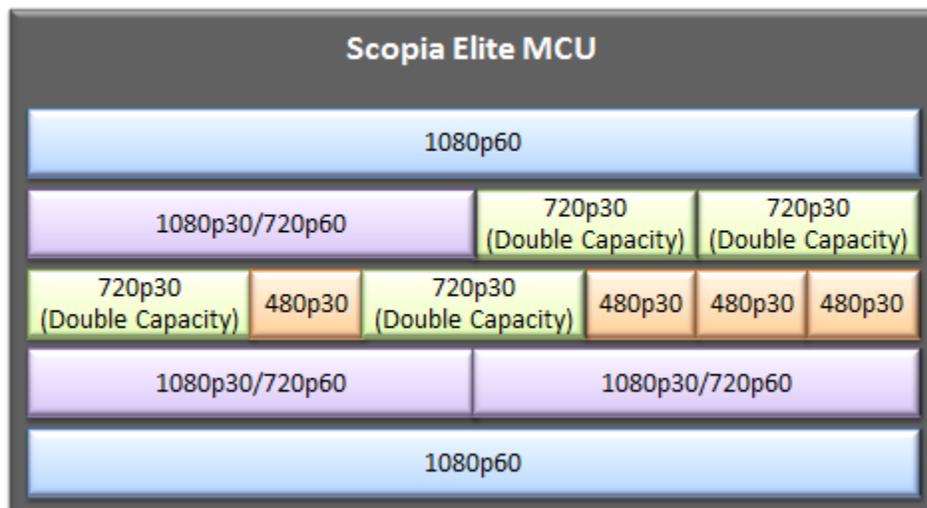
Figure 4: A connection uses its proportion of resources on the MCU

❶ 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 32.

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 *Administrator Guide for Scopia Elite MCU.* 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 47
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 49 and Configuring the UDP Port for the Gatekeeper on the Scopia Elite MCU on page 50
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 51
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 53

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 52
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 52
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 46

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 48
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 | Preparing the MCU Setup

Perform procedures in this section to prepare the site and device for installation.

Navigation

Checking Site Suitability

Prior to setting up your device, you need to verify your site suitability for:

- System power requirements
- System environmental requirements
- The device physical dimensions.

For more information, see Minimum Requirements and Specifications on page 7 to learn about these requirements. Ensure the site conforms to the listed requirements.

Unpacking the Device

About this task

We strongly recommend that you follow safety guidelines described in this section during unpacking.

Procedure

1. Inspect the shipping box to verify that it is not seriously damaged during shipping.

2. Place the shipping box on a horizontal surface paying attention to the This Side Up symbol on the shipping box. See Figure 5: This Side Up symbol on page 18.

Figure 5: This Side Up symbol

⚠ **Caution:**

The accessories kit is situated on top of the device inside the shipping box and can be damaged if the box is placed upside down. Pay attention to the This Side Up symbol on the shipping box to handle the box correctly at all times.

⚠ **Caution:**

To prevent injury and equipment damage, follow lifting guidelines described in the Safety Guide when lifting or moving the shipping box.

3. Cut the plastic straps.

⚠ **Caution:**

The plastic straps are tightly stretched and can hit you when you cut them. To avoid this, make sure you do not face the side of the box secured by the straps before you cut the straps.

4. Cut the strapping tape.

5. Open the shipping box.

6. Take the accessories kit out of the shipping box.

7. Take the device out of the shipping box.

8. Carefully open the additional boxes, remove the packing material, and remove the drives and other contents.

🛈 **Important:**

We recommend that you keep the packaging materials in case you need to repack the device.

9. After opening the shipping box, check the shipment is complete. Compare the contents of the shipment with your packing list.

Inspecting for Damage

After you verify that all of the equipment is included, carefully examine the cards, power supplies and cables for any damage resulting from shipping. If you suspect any damage from shipping, contact your local freight carrier for procedures on damage claims. If you observe any physical defects in the items you ordered, contact Radvision Technical Support for Return Material Authorization (RMA) form.

❗ Important:

Before proceeding with the installation, verify that all of the ordered parts are present and in good condition. Keep a record of the parts and serial numbers. If any parts are missing or damaged, contact your sales representative.

Chapter 4 | Setting up the MCU

Mount the device onto its rails within a 19" square-hole rack.

These sections describe how to set up the device:

Navigation

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 *Administrator Guide for Scopia Elite MCU*.

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.
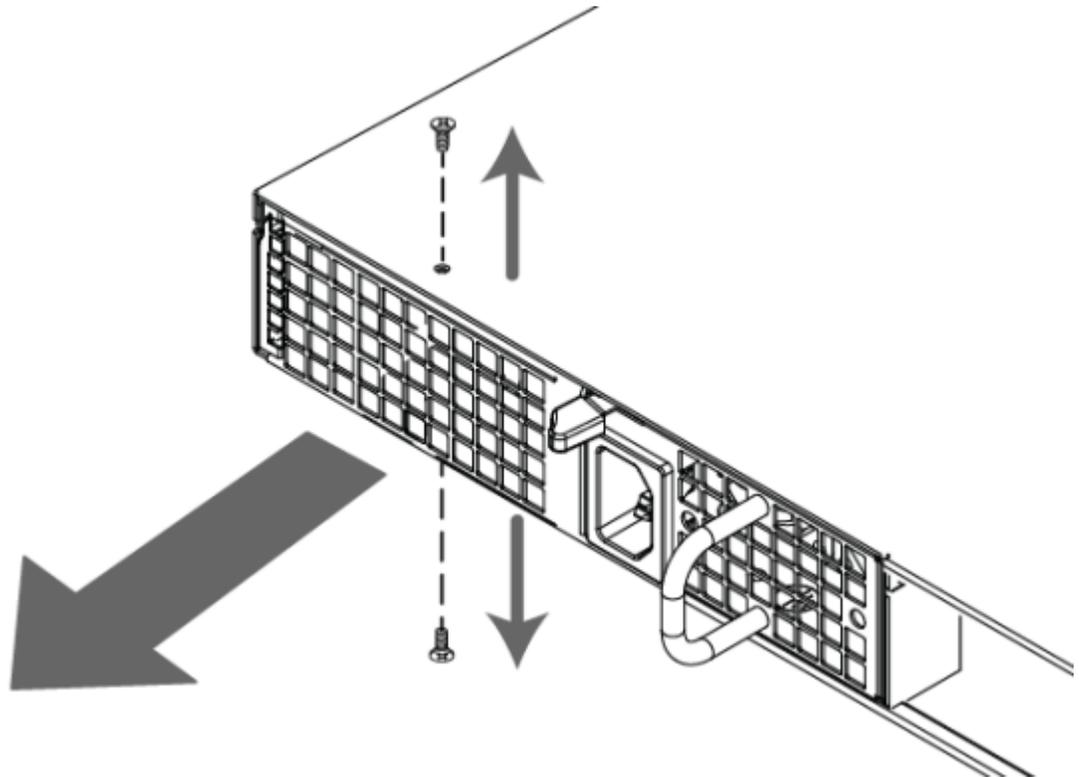
Figure 6: Removing cover of second PSU slot in Scopia Elite MCU 6140

2. Insert the new PSU into position and secure it by pressing it firmly into place until the release tab clicks.
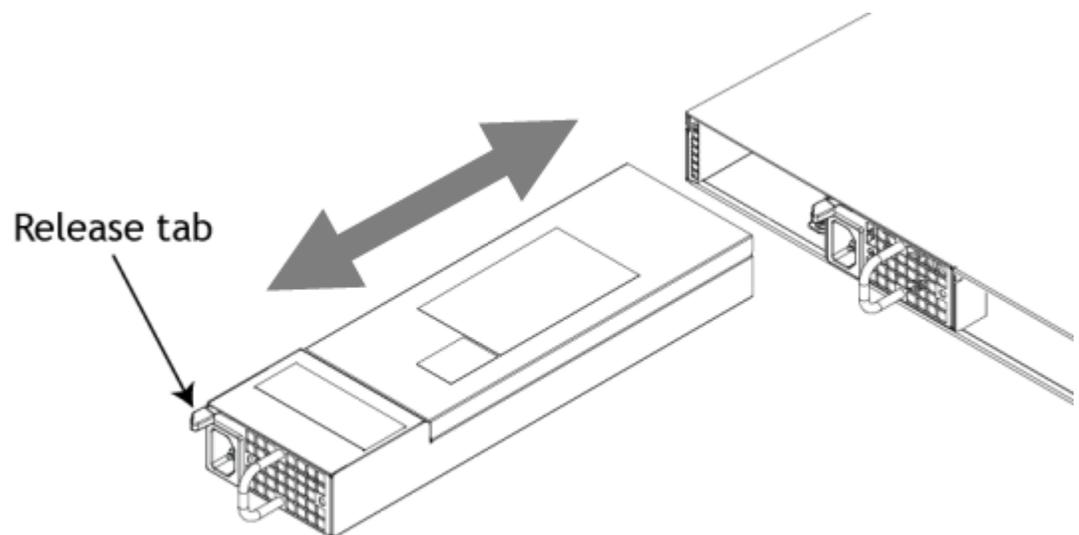
Figure 7: Adding a PSU in Scopia Elite MCU 6140

3. Reconnect the power cord.

Mounting the MCU onto the Rack Using Rails

Rails support the MCU inside the rack. Use cage nuts and screws to fix the rails and the MCU front panel to the rack posts.

The steps for mounting the MCU are:

Navigation

- Mounting the Rails on page 22
- Mounting the MCU onto the Rails on page 24

Mounting the Rails

About this task

Before mounting the rails, adjust their length to correspond to the depth of the rack. For that purpose each rail has two parts that slide one inside the other.

Procedure

1. Adjust the length of the rail and align the rail holes with the left front and rear posts (see Figure 8: Adjusting rail length and attaching to rack on page 22).

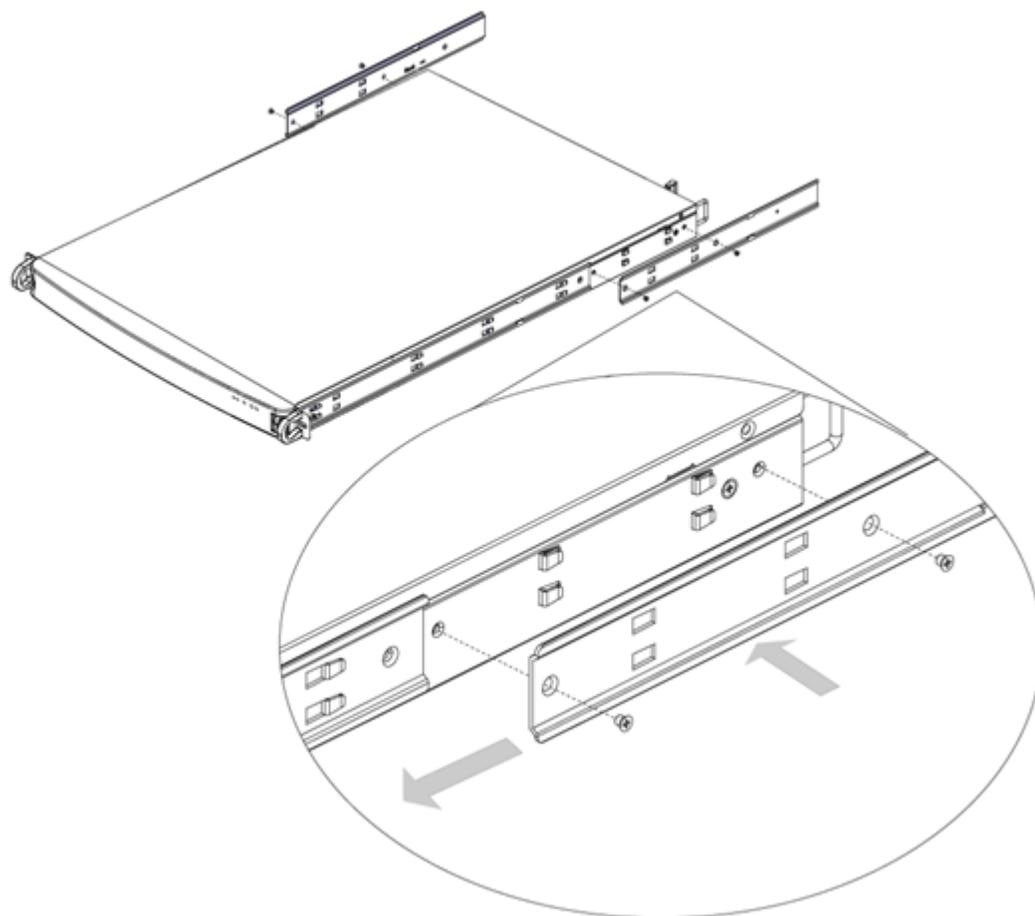   Ask someone to hold the rail while you extend it.
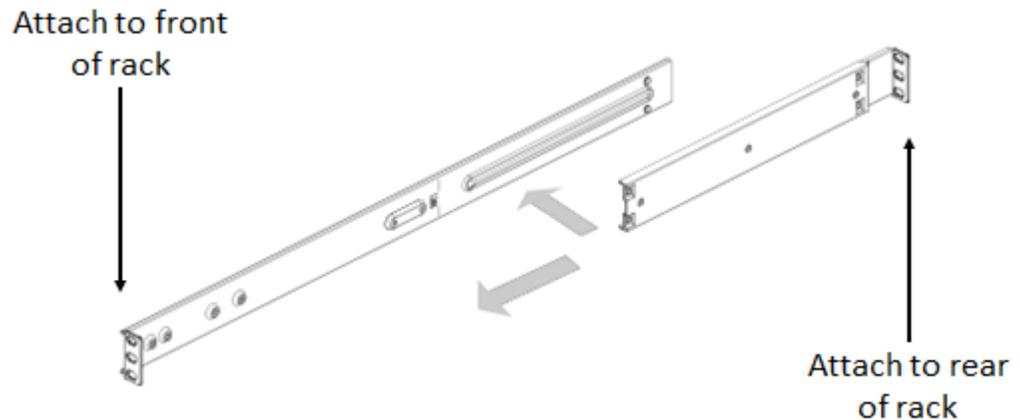
Figure 8: Adjusting rail length and attaching to rack

2. Attach the rail to the posts using the screws provided (see Figure 9: Attaching the rails to the rack on page 23).
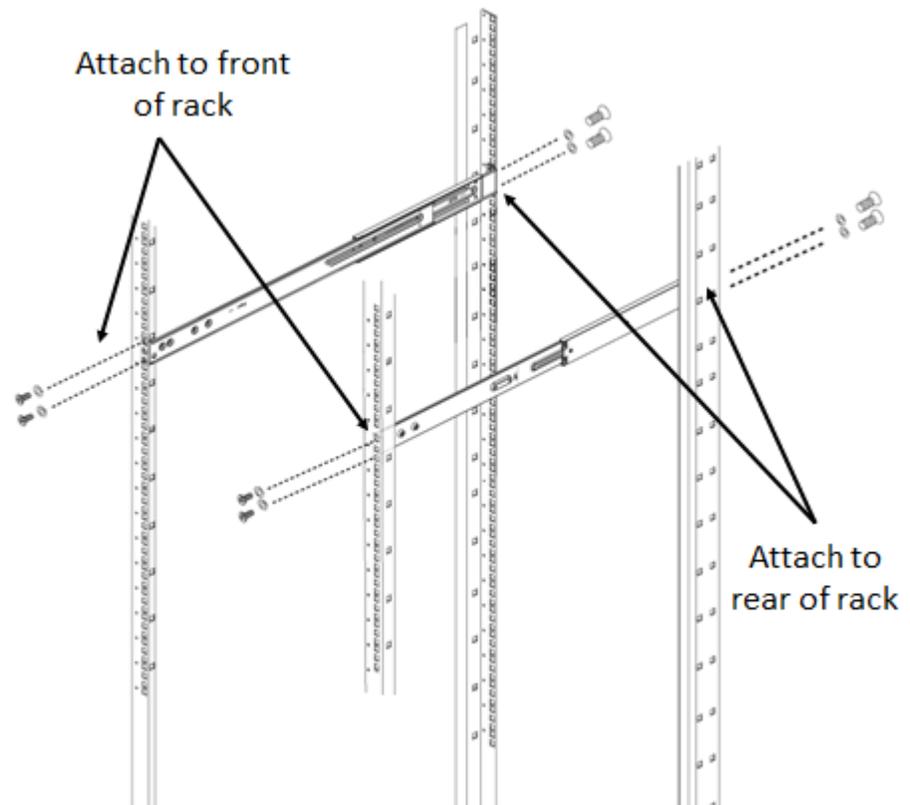
Figure 9: Attaching the rails to the rack

3. Attach the inner rails to the rear of the device (see Figure 10: Attaching inner rails to the device on page 24).

Figure 10: Attaching inner rails to the device

Mounting the MCU onto the Rails

About this task

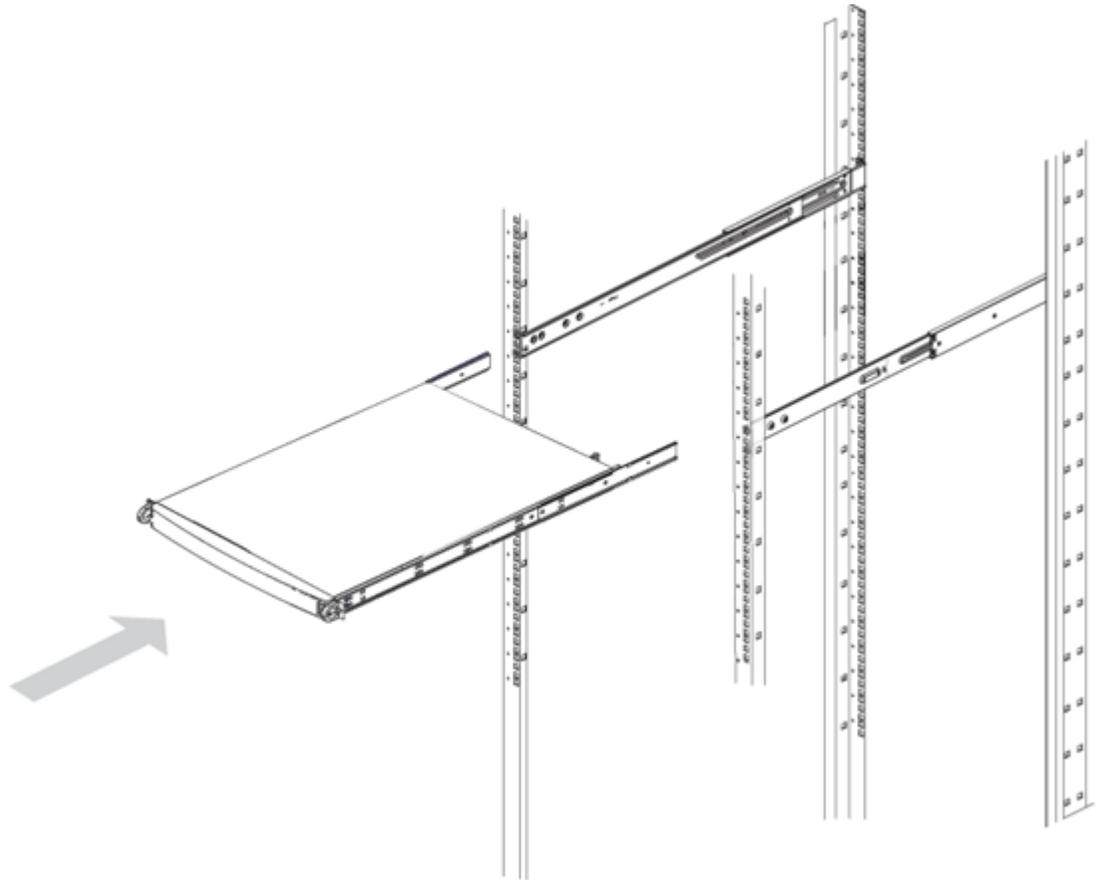After you have attached the rails to form a support, you can mount the MCU onto the rack. Before mounting the MCU, read the Safety Guidelines described in the Safety Guide.

> ⚠ **Caution:**
>
> The MCU is heavy. Ask someone to help you lift it.

Procedure

1. Ensure the rack breaks are locked or the rack is stabilized.

2. Slide the MCU onto the rails until the holes on the MCU front panel align with the front posts. See

Figure 11: Sliding the MCU onto the rails

3. Attach the device to the front posts of the rack.

Connecting Cables to the Device

About this task

Follow the safety guidelines described in the Safety Guide during this procedure, and follow this procedure to connect the power, network, and serial cables supplied with the accessories kit.

⚠ **Caution:**

Do no connect a network cable to the MCU at this stage. The device is shipped with a static IP address which may clash with an existing address on your network. To define a new MCU IP address, see Configuring the Device IP Addresses on page 26

Procedure

1. On the rear side of the device, connect the power cable to the AC power connector (see Figure 12: Rear panel of the device on page 26).
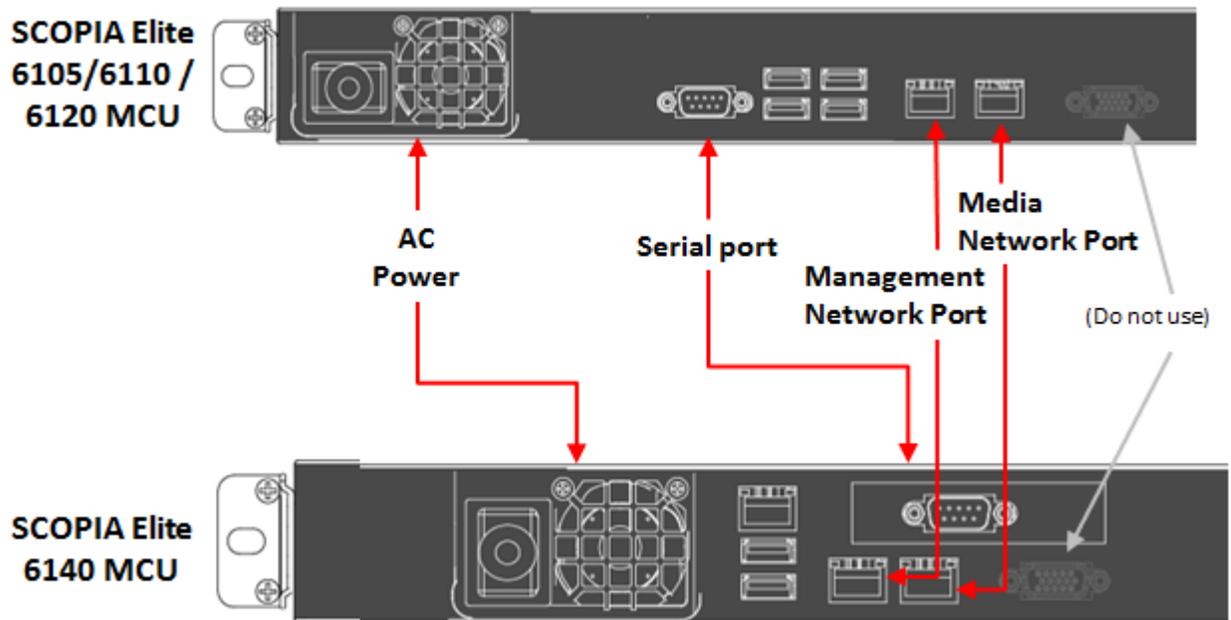
Figure 12: Rear panel of the device

2. Connect the other end of the power cable to the mains.

3. Use a serial cable to connect a PC to the device's serial port. This connection is required for local configuration and maintenance.

   🛈 **Important:**

   Do not connect a screen or a keyboard to the device directly. Define the device's basic settings via the serial connection only.

Configuring the Device IP Addresses

About this task

The MCU supports the following format of IP addresses:

- IPv4 (default)
- Both IPv4/IPv6 (Internet Protocol Version 6). This dual mode allows deploying servers using both protocols in your solution.

⚠️ **Caution:**

The device is shipped with a static IP address, which might conflict with an existing address on your network. Configure the MCU to its new IPv4 address before connecting the MCU to the network.

Configure the IPv4/IPv6 dual mode after the MCU has its new IPv4 address.

The MCU supports dual NIC. This procedure describes how to configure the management IP address. You will use this address to access the MCU web interface. To configure the media IP address, change

the management IP address, or add the IP address of a new management network, see

Before you begin

Make sure you have these items:

- Dedicated IP address for the device
- Dedicated subnet mask for the device
- IP address of the default router which the device uses to communicate over the network
- A PC with an available serial port. It should have a terminal emulator software installed like SecureCRT or PuTTY.
- Power, network, and serial cables supplied with the device accessories kit.

Procedure

1. Connect the power cable but do not switch on the device.

2. Connect the device serial port to a PC with the terminal emulator software installed.

3. Start the terminal emulation application on the PC.

4. Set the communication settings in the terminal emulation application on the PC as follows (Table 5: Configuring the communication settings on page 27):

Table 5: Configuring the communication settings

Field Name	Value
Baud Rate	9600
Data bits	8
Parity	None
Stop bits	1
Flow Control	None

5. Power the device (see Figure 13: Device front panel on page 28).

   Verify the power LED is lit green (Figure 13: Device front panel on page 28).
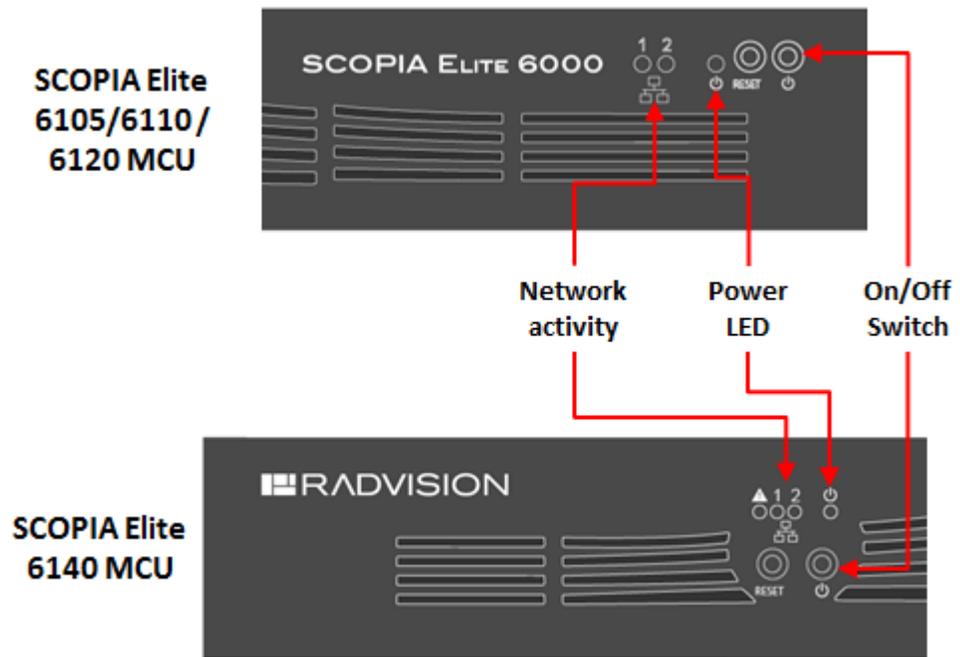
Figure 13: Device front panel

A log of the auto-boot events is displayed in the terminal emulator.

6. When the message `Press any key to start configuration` appears on the screen, press a key and wait for the following message:

```
Main menu
```

```
Main menu
N: Configure network port values
R: Restore to factory defaults
T: Set the XML connection mode to TCP (Reboot is not required)
S: Set Board Security Level
Q: Quit
```

If you do not see this output, contact customer support.

7. Enter **N** at the prompt to configure network port values.

The terminal displays the following message:

```
Configure network port values
1: Show current network configuration
2: Change network configuration
0: Return to main menu

Select:
```

8. Enter **2** to change the network configuration.

9. Enter the new settings at each prompt (Table 6: Configuring network settings on page 29).

Table 6: Configuring network settings

Field	Description
IP Address	Management IP address of the device
Subnet mask	IP address of the subnet mask to which the device belongs. If you are not using a subnet mask, press **Enter**.
Default router	IP address of the default router the device uses to communicate over the network

10. Allow the device to complete the reboot process. A new emulator session begins.

11. Close the terminal emulator session.

12. Connect the network cable to the left ethernet connector on the rear panel of the device (see).

   > 🛈 **Important:**
   >
   > Use both ethernet connectors for dual-NIC deployments. A dual-NIC deployment raises security by using different subnets for media versus management. Use the left ethernet connector for management and the right connector for media ().

13. (Recommended) Set the network switch to 1Gbps Auto Negotiation full duplex, if it can support this configuration.

   The throughput of the network switch should always be the same as the setting in the MCU, whose default value is also 1Gbps.

   You can change the default value from the MCU administrator web interface by navigating to **Configuration > Network > Port Settings**.

Figure 14: Configuring the MCU throughput

> ❗ **Important:**
>
> To access the web interface, you need an IP address as explained in Configuring the Device IP Addresses on page 26.

14. (Optional) To comply with the requirements of your deployment, configure the IPv4/IPv6 mode from the MCU administrator web interface by navigating to **Configuration > Network** (Figure 14: Configuring the MCU throughput on page 30).

15. Select **Apply** at the bottom of the page.

16. Make sure no videoconferences are running on the MCU, and select **Yes** to restart the device.

Chapter 5 | Performing the MCU Initial Configuration

When you finish installing the MCU, you need to perform the initial configuration during which you configure the basic features. After the initial configuration the MCU should be ready for use.

Navigation

Accessing the MCU Administrator Web Interface

About this task

The MCU interface is available in these languages:

- English
- Chinese
- Japanese
- Portuguese
- Spanish
- Russian

The default language of the MCU interface is English. When you access the MCU interface, the login screen is in English unless you choose a different language.

Procedure

1. Launch your browser and enter the IP address or the name of the MCU.

2. If you need to change the MCU interface language, select a language from the **Language** list.

   The login screen is displayed in the language you selected.

3. Enter the administrator user name and password in the appropriate fields and select **Go**.

   The default global user name is **admin**. The default password is **password**.

   > ❶ **Important:**
   >
   > If you try to sign in as an administrator and another administrator is currently signed in, the MCU signs you in as a read only user. The words **Read Only** appear at the top of the window and a pop-up displays the IP address of the administrator already signed in. Read only users cannot edit MCU settings.

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**.

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 15: Locating the serial number of the MCU on page 33).
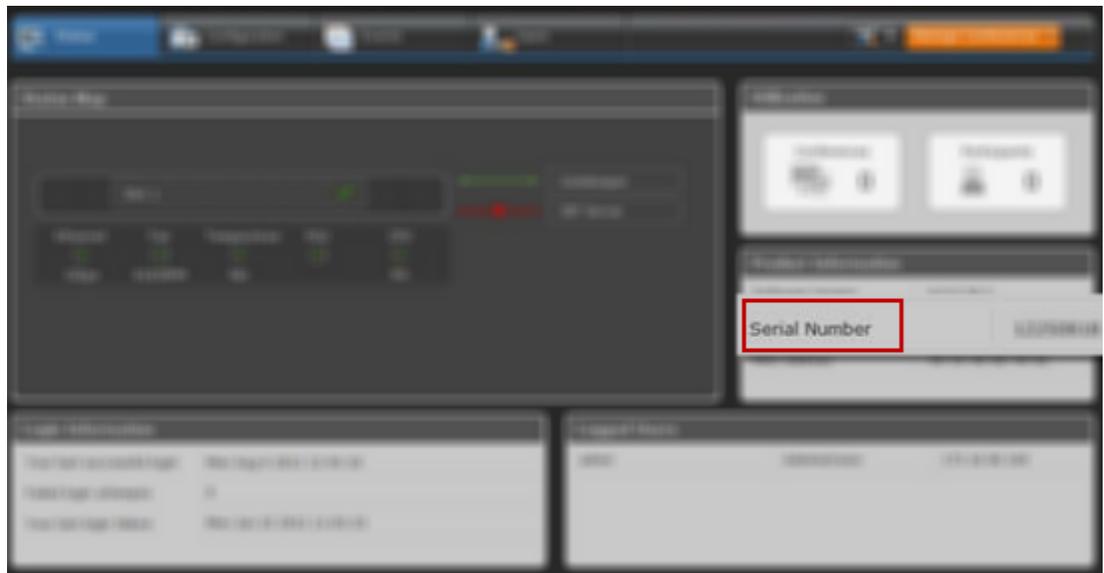
Figure 15: Locating the serial number of the MCU

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** [icon] > **Licensing and Registration**.

   The **Licensing and Registration** window opens.
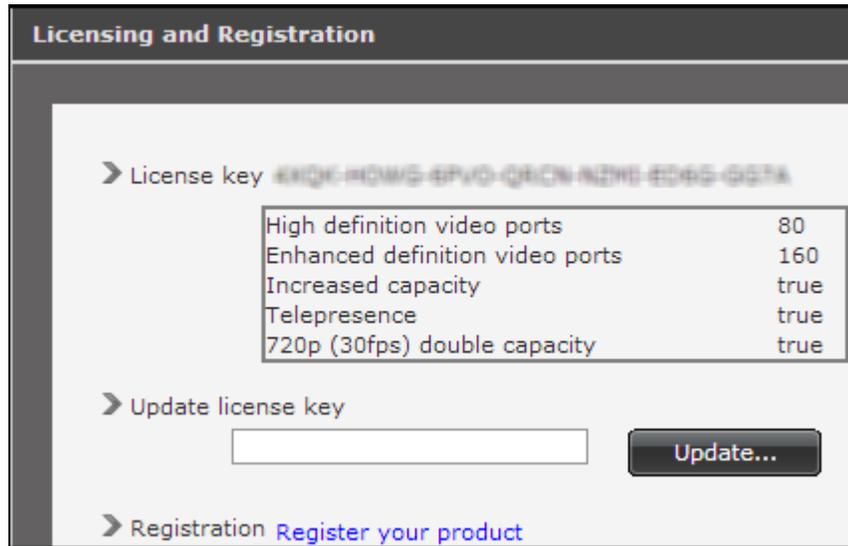
Figure 16: Licensing and Registration Window

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.

Changing the Default 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.

The MCU comes with a single predefined default meeting type (with prefix number 71). This default service is factory tuned to be suitable in most cases for audio and video calls. We recommend starting with this service and modifying it as necessary to suit your needs.

You can modify existing prefixes to suit your network dialing plan or define new services and add them to the list.

When choosing an alternative dial prefix, ensure that the service prefix numbers are not identical to the first digits of any of your network endpoint phone numbers or aliases.

Procedure

1. Access the MCU administrator web interface.

2. Select **Configuration** .

3. Select **Conferences**.

4. Locate the **Services** list section.

5. Select the **Review** button ⬇ next to the service.

6. Enter the new prefix number.

7. Select **Apply**.

Setting the MCU Interface Languages

The MCU supports a number of interface languages which can be set as part of its initial configuration.

Navigation

About Supported Languages

The MCU has three user interfaces:

- Administrator interface

  The web-based interface used by administrators for configuration and maintenance tasks.

- Conference Control interface

  The web-based interface used by administrators and operators for conference moderation and video layout control.

  ### ❶ Important:

  This interface is not available when the MCU is registered to Scopia Management.

- Text overlay on conference video

  The set of menus that appear in the conference video.

The Scopia Elite MCU supports the same languages for the Administrator and Conference Control interfaces, and a different set of languages for the text overlay.

Table 7: Supported Languages in the MCU Interface

Language	Administrator Interface	Conference Control Interface	Text Overlay on Conference Video
English	Yes	Yes	Yes
Chinese (simplified)	Yes	Yes	Yes
French			Yes

Language	Administrator Interface	Conference Control Interface	Text Overlay on Conference Video
Japanese	Yes	Yes	Yes
Portuguese	Yes	Yes	
Russian	Yes	Yes	
Spanish	Yes	Yes	
Hebrew			Yes

Setting the MCU User Interface Language
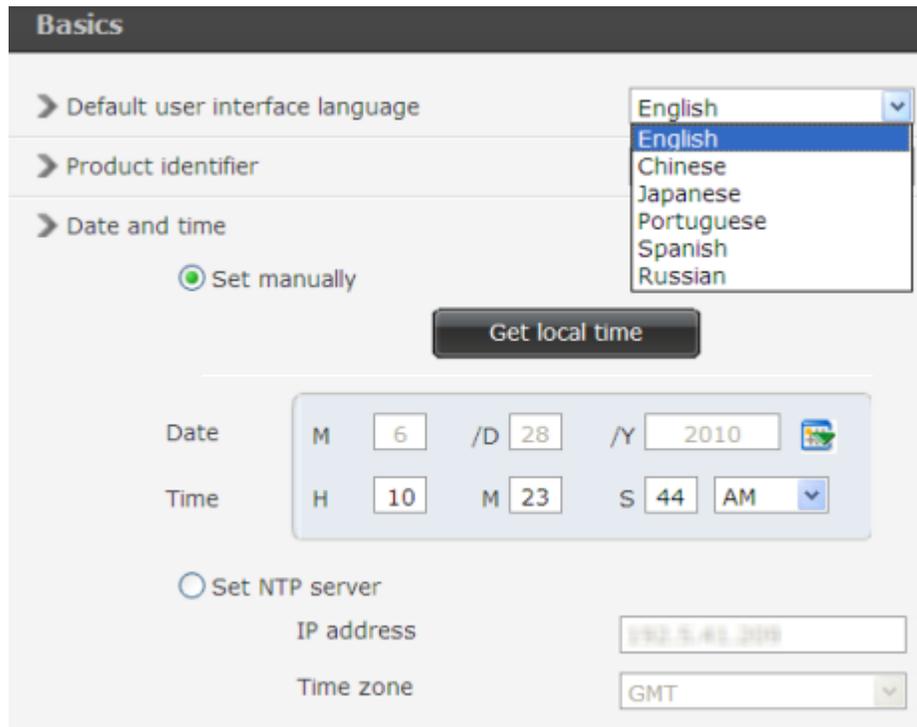
About this task

The procedure in this section explains how to set the language of the MCU administrator web interface and the Conference Control interface. By default, the interface language is set to English.

> **ⓘ Important:**
>
> To view Chinese or Japanese fonts properly in the Administrator interface, the computer on which the web browser is running must support the relevant languages. On a Microsoft Windows operating system, you can set the default language in **Control Panel > Regional and Language Options**.

Procedure

1. Access the MCU administrator web interface.

2. Select **Configuration** .

   The **Setup** tab is displayed.

3. Locate the **Basics** section.

4. Select a language in the **Default user interface language** list.

Figure 17: Setting the language of the device

     5. Select **Apply** at the bottom of the **Setup** tab.

Setting a Text Overlay Language

About this task

Perform the procedure in this section to set the language of the text overlay messages.

The text overlay feature is set to English by default.

Procedure

     1. Access the MCU administrator web interface.

     2. Select **Configuration** .

     3. Select **Customization**.

     4. Select the required language.

Figure 18: Setting text overlay language

5. Select **Apply**.

Configuring Network Protocols for the MCU

Before setting the protocols, ensure the network switch and the MCU have the same throughput. We recommend setting the network switch to 1Gbps Auto Negotiation full duplex, if it can support this configuration. The throughput of the network switch should always be the same as the setting in the MCU, whose default value is also 1Gbps.

You can change the default value from the MCU web administrator interface by navigating to **Configuration > Setup > Network > Port Settings**.

Set the MCU protocols by configuring it to work either with the H.323 gateway or with the SIP Proxy Server, or both. You can change the protocol-related settings at any time without resetting the MCU.

Navigation

- Connecting the MCU to the Gatekeeper on page 38
- Configuring SIP Server Settings on page 39

Connecting the MCU to the Gatekeeper

About this task

You can configure the H.323 protocol settings to determine how the MCU and the gatekeeper interact.

> ⚠ **Important:**
>
> Changing gatekeeper settings does not reset the MCU, but might disconnect active calls.
>
> Disabling the H.323 protocol in the MCU requires the device to restart.

Procedure

1. Select **Configuration** .

2. Select **Protocols**.

3. Locate the H.323 section.

Figure 19: H.323 protocol section of the Protocols tab

4. Select **H.323** to enable the MCU to operate with the H.323 protocol.

5. Enter the gatekeeper's FQDN or IP address and port number.

   The default port is **1719**.

6. Select **Apply**.

7. Login to the MCU Administrator web interface.

8. Locate the **Status Map** section.
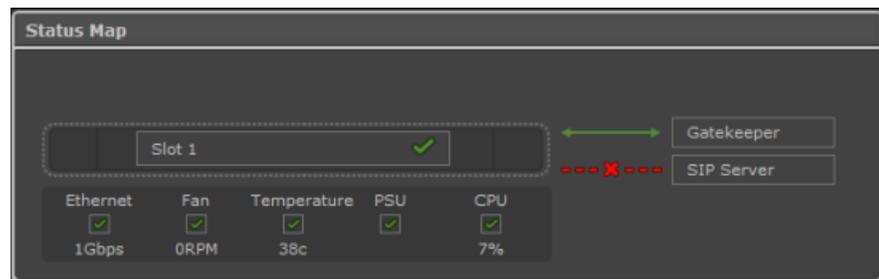
Figure 20: The Status Map showing the gatekeeper connection

9. Verify the MCU is connected to the Ethernet.

10. Verify the MCU is connected to the Gatekeeper.

Configuring SIP Server Settings

About this task

You can configure settings for SIP server profiles which set how the MCU and the registrar interact.

Depending on connection types supported by the SIP server, MCU supports these transport connection types for sending messages to SIP server:

- UDP
- TCP
- TLS

Procedure

1. Select **Configuration** ⚙ Configuration.

2. Select **Protocols**.

3. Select **Enable SIP protocol** to enable MCU communication with the SIP server.

4. Enter the SIP domain of the MCU in the **Default SIP domain** field as defined in the SIP server.

   An example of a SIP domain is company.com.

5. Select **Locate automatically** to instruct the MCU to automatically locate one of the SIP servers that are present in the domain,

   or

   Select **Specify** and enter the following:

   - An IP address or host name of the SIP server, for example *<sipserver>.<company>.com*.

Figure 21: SIP Protocol section of the Protocols tab

   - The communication port number of the SIP server address. The default port is **5060**.
   - The protocol from the **Type** field. The default is **UDP**.

   ⓘ **Important:**

   The Locate automatically option works only if you have configured a valid IP address at **Configuration > Setup > Network > DNS server1** or **DNS server2**.

6. To instruct the MCU to register with a SIP registrar and to send service information to the registrar, perform these steps:

   a. Select **Use registrar**.

   b. Enter the following information:

- The IP address or the host name of the SIP registrar in the **IP address** field.
- The communication port number of the SIP registrar address.
- The transport connection type for sending registration requests to the registrar according to the type supported by the SIP registrar.

    The default is UDP.

7. Select **More**.

    The **Local signaling port** section is displayed.

Figure 22: Local signaling port section

8. Enter the number of the signaling port on which the MCU communicates with the SIP server.

    The default is **5060**.

9. Select **Use proxy digest authentication** to enable MCU authentication with a SIP server using user name and password.

    Authentication is performed as defined in RFC 2617. This field is disabled by default.

    Enter the MCU user name and password. They must match those defined on the SIP server.

10. Select **Use registrar digest authentication** to enable MCU authentication with a SIP registrar using user name and password.

    Authentication is performed as defined in RFC 2617. This field is disabled by default.

    Enter the MCU user name and password. They must match those defined on the SIP server.

11. Select **Use 'Empty Invite' when sending Invite messages to endpoints** to enable the remote endpoint to indicate preferred audio and video channels.

12. Select **Apply**.

13. Check the MCU status using the MCU administrator web interface:

    a. Enter the MCU IP address or the MCU name into the Internet browser.

    b. Enter the Administrator user name and password in the appropriate fields and select **Go**.

    The default global user name is **admin**. The default password is **password**.

The **Status** tab of the Administrator interface opens.

c. Locate the **Status Map** section. This section is a graphic representation of the MCU chassis.
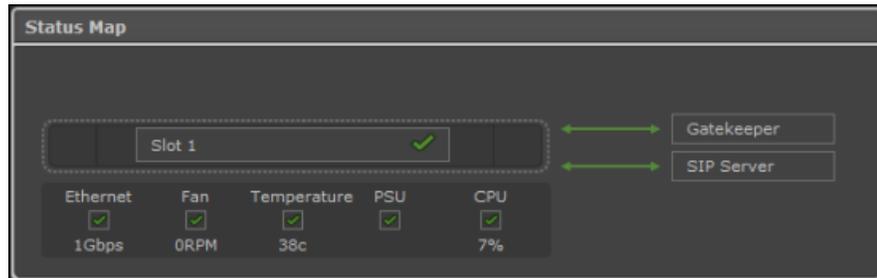
Figure 23: The Status Map section showing the SIP Server connection

d. Verify that the MCU is connected to the Ethernet.

e. If you registered the MCU with SIP registrar, verify that the MCU is connected to the SIP Server.

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 <u>Configuring the Device IP Addresses</u> on page 26.

- 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.
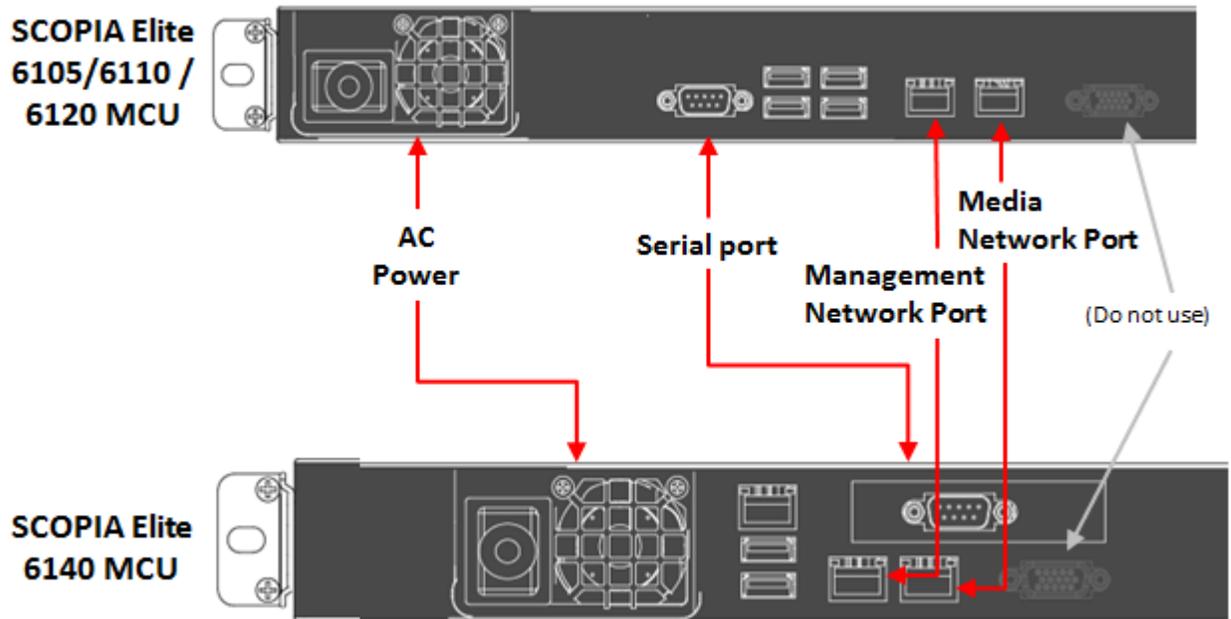
Figure 24: The MCU management and media connections

> ⚠ **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 (<u>Configuring the Device IP Addresses</u> on page 26).

3. Select the **Configuration** ⚙ Configuration tab.

4. Select the **Advanced IP Configuration** check box to expand that section of the page <u>Figure 25: Configuring IP separation with two network connections</u> on page 44).
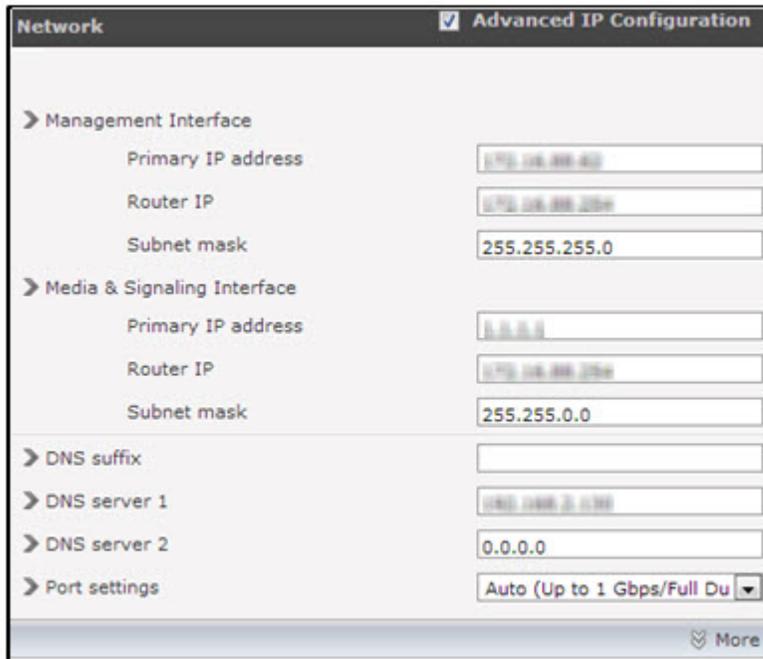
Figure 25: Configuring IP separation with two network connections

5. Configure the IP addresses of each interface (Table 8: Configuring the IP addresses of each network interface on page 44).

Table 8: 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 24: The MCU management and media connections on page 43).

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 26: Example of additional management network on page 45). 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 26: Example of additional management network on page 45).
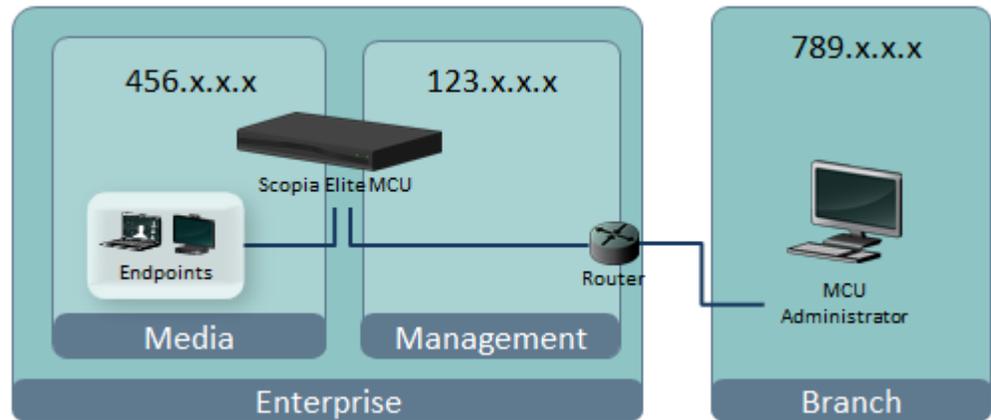
Figure 26: Example of additional management network

Use the following steps to configure an additional management network:

a. Select **More** at the bottom of the expanded section (Figure 25: Configuring IP separation with two network connections on page 44).

The **Additional Management Networks** section opens.

b. Select **Add Management Network**.

c. Configure the access to the MCU management subnet (Figure 27: Adding a new network for management access on page 46 and Table 9: Configuring the additional network interfaces on page 46).
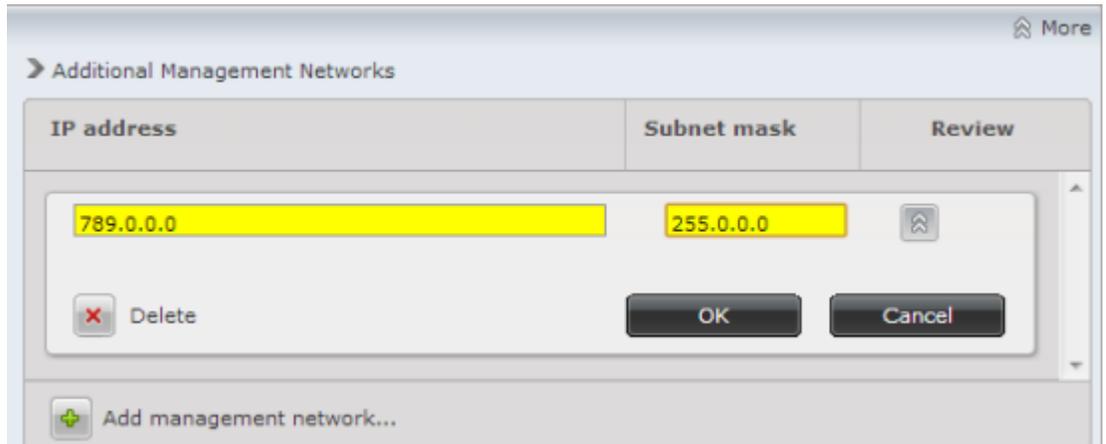
Figure 27: Adding a new network for management access

Table 9: 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**.

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 46
- Configuring the TCP Port Range for H.245 on the Scopia Elite MCU on page 47
- Configuring the HTTP Port on the Scopia Elite MCU on page 48
- Configuring the UDP Port for RAS on the Scopia Elite MCU on page 49
- Configuring the UDP Port for the Gatekeeper on the Scopia Elite MCU on page 50
- Configuring the TCP Port Q.931 on the Scopia Elite MCU on page 51
- Configuring the TCP/UDP/TLS Port for SIP on the Scopia Elite MCU on page 52
- Configuring the TCP Port Range for SIP BFCP on the Scopia Elite MCU on page 53

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 28: Defining the base port for video on page 47).

Figure 28: 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] icon.

    b. Select **Advanced parameters**.

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

Figure 29: 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] icon.

    b. Select **Advanced parameters**.

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

Figure 30: 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).

> **ⓘ 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] icon.

   b. Select **Advanced parameters**.

   c. Locate the **H323 RAS port number** in the **Name** column (see Figure 31: RAS Port Configuration on page 50).

Figure 31: RAS Port Configuration

2. Select the [icon] 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 49).

> **ⓘ 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 32: H.323 Protocol section of the Protocols tab on page 51).

Figure 32: 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 33: H.323 Signaling Port Configuration on page 52).

Figure 33: 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 34: 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).

Name	Value	Review
SIP BFCP base port	3400	⊻

Figure 35: 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**.

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.

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

> ❶ **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). lists the protocol status when each security access level is applied.

Figure 36: Security Access Level Settings

Table 10: 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.**

Verifying the MCU Installation

About this task

After you installed the device and performed its initial configuration, you need to verify that it is installed and configured correctly.

Procedure

1. On the front panel, verify that the power LED is lit green.
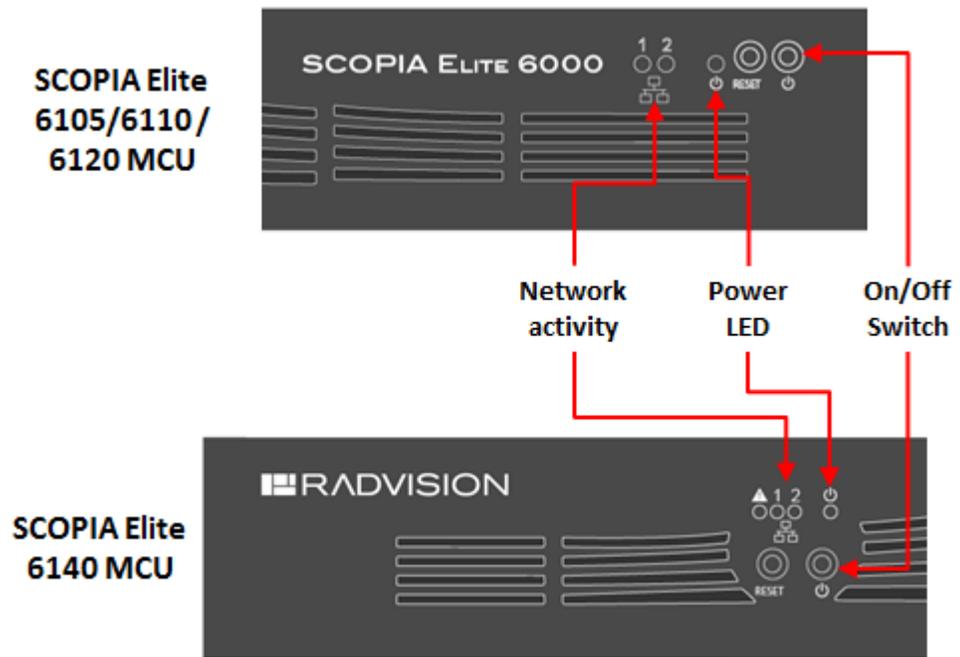
Figure 37: Locating the front panel LEDs

2. Verify that the status LED is lit green (selected models only).

3. Check the network connection by verifying that the Ethernet activity LED is lit green.

4. Verify the device is ready for use by creating a videoconference:

   a. From an endpoint dial the MCU IP address.

      The MCU Auto-Attendant service plays the video and audio prompts.

   b. Press **0** to create a new videoconference.

   c. At the prompt, enter the meeting ID followed by **#**.

      The MCU creates the conference and opens the Conference window.

   d. Exit the conference by disconnecting the call.

5. Access the MCU administrator web interface to verify all status icons are green on the home page.

6. 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.
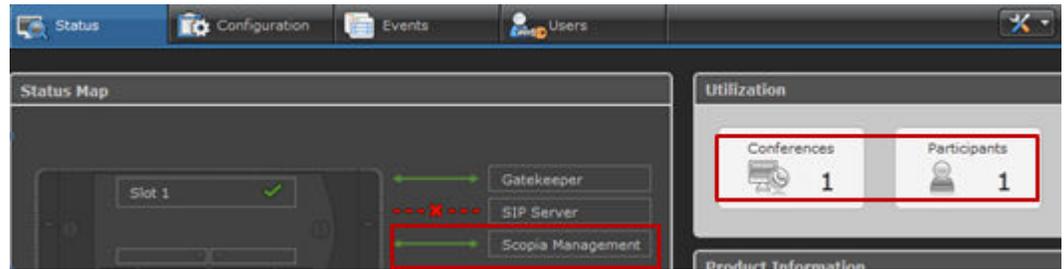
Figure 38: The MCU Status Map

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

Figure 39: The Scopia Management Dashboard status

f. Exit the videoconference by disconnecting the call.

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